

**Department of Defense
Unified Capabilities Requirements 2008 (UCR 2008)**



December 2008

**The Office of the Assistant Secretary of Defense
for
Networks and Information Integration / DoD Chief
Information Officer**

**DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2008 (UCR 2008)**

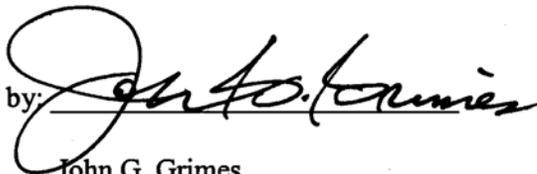
This document specifies technical requirements for certification of approved products supporting voice, video, and data applications services to be used in Department of Defense (DoD) networks to provide end-to-end Unified Capabilities (UC).

It conforms to Public Law 107-314 and is the basis for any future Unified Capabilities device acquisition, independent of the technology.

DISTRIBUTION STATEMENT A:

Approved for public release; distribution is unlimited.

Approved by:



John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Dated:

1/22/09

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
SECTION 1 – PURPOSE	1
SECTION 2 – APPLICABILITY AND SCOPE.....	3
2.1 Applicability	3
2.2 Scope of Document.....	4
SECTION 3 – POLICY	7
3.1 Introduction.....	7
3.2 Specific Policies Affecting UC.....	8
3.2.1 DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”	8
3.2.2 DoDD 8500.1, “Information Assurance (IA)”.....	8
3.2.3 DoDI 8510.01, “DOD Information Assurance Certification and Accreditation Process (DIACAP)”	9
3.2.4 CJCSI 6211.02C, “Defense Information System Network (DISN): Policy, Responsibilities and Processes”	10
3.2.5 DoDI 8100.3, “Department of Defense (DoD) Voice Networks”	11
3.2.6 CJCSI 6215.01C, “Policy for Department of Defense (DoD) Voice Networks with Real Time Services”	13
SECTION 4 – UNIFIED CAPABILITIES DESCRIPTION AND KEY PROCESSES	15
4.1. Unified Capabilities Services Description	15
4.1.1 Unified Capabilities Service Classes	17
4.2 Mission Capabilities	17
4.2.1 User Categories.....	17
4.2.2 Assured Services Features	20
4.3 Migration to Unified Capabilities	23
4.3.1 UC Migration Strategy Drivers.....	25
4.3.1.1 Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service- Oriented DoD Enterprise	27
4.3.1.2 Joint Net-Centric Operations Campaign Plan.....	29
4.3.1.3 Internet Protocol Version 6 Requirements.....	29
4.3.1.4 Critical Milestones and Actions for Complete Circuit-Switch Phase-Out.....	31

Table of Contents

4.3.2	Programs Migration to VVoIP.....	32
4.3.3	Migration Time Frames	40
4.3.3.1	Migration Time Frame – Fiscal Years 2008-2011.....	42
4.3.3.1.1	SBU Voice and Video Operational Services ...	43
4.3.3.1.2	SBU VVoIP Voice and Video Services Technology Insertions.....	44
4.3.3.2	Migration Time Frame – Fiscal Years 2012-2015.....	49
4.3.3.3	Migration Time Frame – Fiscal Years 2016-2020.....	50
4.4	Unified Capabilities System Description.....	50
4.4.1	IP-Based Design for Unified Capabilities	52
4.4.1.1	Overview of VVoIP 2008 System Design Attributes.....	54
4.4.1.1.1	Queuing Hierarchy for DISN IP Service Classes.....	56
4.4.1.1.2	Customer Edge Segment Design	57
4.4.1.1.2.1	Base/Post/Camp/Station VVoIP Design.....	57
4.4.1.1.2.2	Local Session Controller Designs – Voice	58
4.4.1.1.2.3	Local Session Controller Designs – Video.....	61
4.4.1.1.2.4	LAN and ASLAN Design 2008.....	63
4.4.1.1.3	Network Infrastructure End-to-End Performance (DoD Intranets and DISN Service Delivery Nodes).....	66
4.4.1.1.4	End-to-End Protocol Planes.....	68
4.4.1.1.5	ASAC System Component 2008	69
4.4.1.1.6	Voice/Video System Signaling Design.....	73
4.4.1.1.7	IA System Design	76
4.4.1.1.8	Network Management System Design.....	79
4.4.1.2	Relationship between SBU UC System Description and Products to be Tested for APL Certification	81
4.4.1.3	Classified VoIP System Design.....	84
4.4.1.4	VTC System Design	85
4.4.1.5	DISN Router Hierarchy	86
4.4.1.6	IPv6 System Design.....	87
4.4.2	TDM-Based SBU Voice (DSN) System Design	88
4.4.2.1	DSN Backbone Switches.....	89
4.4.2.2	Military and Agency Installation Configuration and Switch Types.....	90
4.4.2.3	End Office.....	91

	4.4.2.4	Small End Office	91
	4.4.2.5	Private Branch Exchange.....	91
	4.4.2.6	Remote Switching Unit.....	92
	4.4.2.7	Deployable Voice Exchange.....	93
	4.4.2.8	Deployable DSN PBX1	93
	4.4.2.9	DSN Backbone Signaling System	94
4.5	Unified Capabilities Approved Products List Process.....		94
	4.5.1	Unified Capabilities Approved Products Process and Products	94
	4.5.1.1	Overview of Approved Products	94
	4.5.1.2	Standard Process for Gaining APL Status	101
	4.5.1.3	Approval to Connect and IA Approval to Connect Processes.....	102
	4.5.1.4	Links to the UCCO and Unified Capabilities APL Web Pages.....	104
	4.5.2	Use of UC Approved Products in (Tailored) Information Support Plans.....	105
	4.5.3	APL Process for Deployment of IP-Based DISN Voice and Video Capabilities	106
	4.5.3.1	APL Process Modified for the VVoIP Assessment Prototype Phase.....	107
	4.5.3.2	APL Process Modified for the VVoIP Assessment Preproduction Phase	108
	4.5.3.3	APL Process Modified for the UC Spiral 1 or 2 Operational Testing Phase	109
	4.5.3.4	VVoIP Assessment and Deployment Timelines.....	109

SECTION 1 PURPOSE

1.1 The purpose of this “Unified Capabilities Requirements 2008 (UCR 2008)” document is to specify the technical requirements for certification of approved products to be used in Department of Defense (DoD) networks to provide end-to-end Unified Capabilities (UC).

1.2 The UCR 2008 replaces the UCR 2007 dated 21 December 2007.

1.3 The UCR 2008 is the governing requirements document for all DoD network infrastructures and services that provide or support UC end-to-end and it takes precedence over subordinate documents, DoD standards and commercial standards that address UC.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 2 APPLICABILITY AND SCOPE

2.1 APPLICABILITY

The UCR:

2.1.1 Is applicable to The Office of the Secretary of Defense, the Military Services, Chairman of the Joint Chiefs of Staff, combatant commands (COCOMs), the Office of the Inspector General of the Department of Defense (DoD), the Defense agencies, the DoD Field Activities and all other organizational entities in the Department of Defense (referred to hereafter collectively as “the DoD Components”) in peacetime, crisis situations, and wartime.

2.1.2 Is applicable to all DoD network infrastructures and services that provide or support UC end-to-end, over all phases of their life cycle from acquisition to operations.

2.1.2.1 Unified Capabilities are defined as the seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities. UC integrate standards-based communication and collaboration services including, but not limited to, the following:

- Messaging
- Voice, video, and Web conferencing
- Presence
- UC clients

2.1.2.2 These standards-based communication and collaboration services must integrate with available enterprise applications, both business and warfighting.

More specifically the UCR 2008 specifies technical requirements for assured interoperability and information assurance of the following set of UC, which will be expanded in the future:

- Voice and Video Services Point to Point
- Voice Conferencing
- Videoconferencing
- E-Mail/Calendar
- Unified Messaging
- Web Conferencing and Web Collaboration

Section 2 – Applicability and Scope

- Unified Conferencing
- Instant Messaging and Chat

2.1.3 Establishes the requirements needed by industry to develop requirements-compliant unified capability solutions.

2.1.4 Provides the foundation for the development of Unified Capability Test Plans (UCTPs) for Interoperability (IO) and Information Assurance (IA) testing. These tests are used to make the certification decisions necessary to place products on the UC Approved Products List (APL).

2.1.5 Provides IA requirements necessary for UC products to meet DoD IA policy to become approved products. These IA requirements will subsequently be used to assist in the development of the security technical implementation guides (STIGs) needed to operate properly UC approved products once installed.

2.1.6 Provides the foundation to support the collaborative development of Information Support Plans (ISPs) and Tailored Information Support Plans (TISPs) for programs that meet DoDI 4630.8 and CJCSI 6212.01D requirements.

2.1.7 Identifies only the MINIMUM requirements and features applicable to all DoD networks that support Unified Capabilities, which include voice and video operating in IP, converged networks with data services.

2.1.8 Does not contain a complete set of requirements for the commercial off-the-shelf (COTS) features that do not affect assured services but are of interest to users since these features do not require interoperability or information assurance requirements.

2.2 SCOPE OF DOCUMENT

The UCR 2008 consists of seven sections, as follows:

1. Section 1, Purpose, defines the purpose for the UCR 2008.
2. Section 2, Applicability and Scope, provides the scope of the UCR.
3. Section 3, Policy, provides a broad overview of policies that will be implemented in the UCR 2008 with emphasis on policies that govern Information Assurance (IA) and Interoperability (IO) verification and testing of systems and products used to provide DISN UC.

4. Section 4, Unified Capabilities Description and Key Processes, provides an overview of UC services, their relationship to Voice and Video Over IP (VVoIP), and the core processes needed for a vendor to gain placement on the DoD APL.
5. Section 5, Unified Capabilities Product Requirements, describes technical requirements, features, and test configurations of equipment used to achieve approval to appear on the UC APL.
6. Section 6 contains unique requirements: 6.1, Unique Tactical Requirements, and 6.2, Unique Classified VVoIP Requirements.
7. Section 7 contains a high-level requirements matrix, which is a summary of the requirements defined in Sections 5 and 6 for the UC products.
8. Appendix A, Definitions, Abbreviations and Acronyms, and References, contains the definitions, abbreviations and acronyms, and references applicable to the UCR 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 3 POLICY

3.1 INTRODUCTION

This section provides a broad overview of policies that will be implemented in the UCR 2008. The overview is focused on policies that govern IA and IO verification and testing of systems and components used in providing UC. The UCR 2008 translates the mission based requirements outlined by the major policies listed in Table 3.1-1, Major Policies Addressed by the UCR 2008, into requirements that allow vendors to develop the functionality needed to meet those mission based requirements and JITC to conduct the testing necessary to place those products on the Unified Capabilities Approved Product List (UC APL).

Table 3.1-1. Major Policies Addressed by UCR 2008

DoDD 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” Certified current as of April 23, 2007
DoDI 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” June 30, 2004
DoDD 8500.01E, “Information Assurance (IA),” April 23, 2007
DoDI 8510.01, “DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP),” November 28, 2007
DoDI 8100.3, “Department of Defense (DoD) Voice Networks,” January 16, 2004
CJCSI 6212.01D, “Interoperability and Supportability of Information Technology and National Security Systems,” 8 March 2006, Current as of 14 March 2007
CJCSI 6510.01E, “Information Assurance (IA) And Computer Network Defense (CND),” 15 August 2007
CJCSI 6211.02C, “Defense Information System Network (DISN): Policy and Responsibilities,” 9 July 2008
CJCSI 6215.01C, “Policy for Department of Defense (DoD) Voice Networks, with Real Time Services (RTS),” 9 November 2007
JROCM 202-02, “Global Information Grid (GIG), Mission Area Initial Capabilities Document (MA ICD),” 22 November 2002
JROCM 048-96, Memorandum For The Under Secretary Defense For Acquisition and Technology Subject: Validation of Defense Information System Network (DISN) Capstone Requirements Document (CRD), 15 April 1996

3.2 SPECIFIC POLICIES AFFECTING UC

In this section, specific policy extracts which are drivers of the UCR 2008 requirements are provided since they are the most demanding on the technologies that must be used to satisfy the requirements.

3.2.1 DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”

DoDI 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 30 June 2004 and CJCSI 6212.01D, “Interoperability and Supportability of Information Technology and National Security Systems” implement DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 05 May 2004 and establish:

1. Policies and procedures for developing, coordinating, reviewing, and approving IT and NSS Interoperability and Supportability (I&S) needs.
2. Procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems.
3. Procedures to perform I&S Certification and J-6 System Validation of ISPs for all non-ACAT and fielded programs/systems.
4. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).
5. Provides guidance for NR-KPP development and assessment.
6. Establishes procedures for JITC Joint Interoperability Test Certification.

3.2.2 DoDD 8500.1, “Information Assurance (IA)”

DoDD 8500.1, “Information Assurance (IA),” establishes policy and assigns responsibilities under Section 2224 of title 10, United States Code, “Defense Information Assurance Program,” to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. The following extract from this DoDD is applicable to the DSN and thereby assured voice services:

- “4.0 It is DoD policy that:
- “4.1 Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, Appendix III, DoD Directive 5000.1 and this Directive, and other IA-related DoD guidance, as issued.
- “4.2 All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness. For IA purposes all DoD information systems shall be organized and managed in the following four categories: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.”

3.2.3 DoDI 8510.01, “DOD Information Assurance Certification and Accreditation Process (DIACAP)”

DoDI 8510.01, “DOD Information Assurance Certification and Accreditation Process (DIACAP),” establishes the DIACAP for authorizing the operation of DoD Information Systems (ISs). The following extract from this DoDI is applicable to UC:

- “1.4. Establishes a C&A [Certification and Accreditation] process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.
- “1.5. Prescribes the DIACAP to satisfy the requirements of Reference (a) [Subchapter III of Chapter 35 of title 44, United States Code, “Federal Information Security Management Act (FISMA) of 2002”] and requires the Department of Defense to meet or exceed the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to Reference (a) and section 11331 of title 40, United States Code.

“It is DoD policy that:

- “4.1. The Department of Defense shall certify and accredit ISs through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls as defined in DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003. IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the GIG architecture and risk assessments that are conducted at DoD-wide, mission area (MA), DoD Component, and IS levels consistent with Reference (a).
- “4.2. The Department of Defense shall establish and use an enterprise decision structure for IA C&A that includes and integrates GIG MAs pursuant to DoD Directive (DoDD) 8115.01 and the DIACAP governance process prescribed in this Instruction.
- “4.3. The DIACAP shall support the transition of DoD ISs to GIG standards and a net-centric environment while enabling assured information sharing by:
 - “4.3.1. Providing a standard C&A approach.
 - “4.3.2. Providing guidance on managing and disseminating enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting.
 - “4.3.3. Accommodating diverse ISs in a dynamic environment.
- “4.4. All DoD-owned or -controlled ISs shall be under the governance of a DoD Component IA program in accordance with Reference (d). The DoD Component IA program shall be the primary mechanism for ensuring enterprise visibility and synchronization of the DIACAP.”

3.2.4 CJCSI 6211.02C, “Defense Information System Network (DISN): Policy, Responsibilities and Processes”

CJCSI 6211.02C, “Defense Information System Network (DISN): Policy, Responsibilities and Processes,” establishes policy, responsibilities, and connection approval process for subnetworks of the DISN. A subset of DISA responsibilities as applicable to UC in accordance with Enclosure B, Responsibilities, of this instruction is as follows:

- “5. The Director, DISA, will:
 - “5.h. Assess the technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN.
 - “(1) Add new DISN services and capabilities in response to validated and prioritized user requirements and planned technology insertion.
 - “(2) Analyze and satisfy requests for new DISN services in coordination with the CC/S/As.
 - “(3) Identify capability gaps to OASD(NII)/DOD CIO when the CC/S/A requirements cannot be met feasibly by new DISN services.
 - “5i. Approve DISN connections based on validated requirements. Ensure that the connection meets technical and interoperability requirements IAW DODI 4630.8..., CJCSI 6212.01..., and CJCSI 6215.01C....Additionally, ensure the IS is accredited IAW DODI 8510.01... or DCID 6/3
 - “5j. Accredit the DISN SIPRNET to process SECRET information, including North Atlantic Treaty Organization (NATO) information, IAW DODI 8510.01.”

3.2.5 DoDI 8100.3, “Department of Defense (DoD) Voice Networks”

The ASD(NII) issued DoDI 8100.3, “Department of Defense (DoD) Voice Networks,” to implement Section 353 of Public Law 107-314, “Bob Stump National Defense Authorization Act for Fiscal Year 2003,” and DoDD 8100.1, “Global Information Grid (GIG) Overarching Policy.” This instruction provides policy and procedures, and assigns responsibilities for test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches, switched data, and services on DoD voice networks, specifically the DSN and DRSN.

The following is an extract from this instruction:

“2. APPLICABILITY AND SCOPE

“This Instruction applies to:

Section 3 – Policy

- “2.1 The Office of the Secretary of Defense, the Military Services, the Chairman of the Joint Chiefs of Staff, the COCOMs, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as “the DoD Components”).
- “2.2 All telecommunication switches leased, procured (whether systems or services), or operated by any Component of the Department of Defense or by authorized non-DoD users (e.g., Combined or Coalition partners (upon ratification) and U.S. Government Departments and Agencies designated as Special Command and Control (C2) or C2 users) that are, or shall be, installed or connected to the DSN, DRSN or Public Switched Telecommunications Network (PSTN) to include:
- “2.2.1 The hardware or software for sending and receiving voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the DSN, DRSN or PSTN. For authorized non-DoD DSN users, only the telecommunications switch interfaces to the DSN are subject to this Instruction.
- “2.2.2 End-to-end (e.g., phone-to-phone. Video-to-video unit, fax-to-fax; Secure Terminal Equipment (STE)-to-STE) and tactical applications.
- “2.2.3 All technologies (i.e., circuit switch, Voice over Asynchronous Transfer Mode (VoATM) and Voice over Internet Protocol (VoIP)) that use DSN or DRSN telephone numbers and provide dial tone for origination and reception of voice, dial-up video and dial-up data for routine and precedence subscribers; or that are otherwise incorporated into the DSN or DRSN numbering and routing plan by means of area code, access code, address resolution scheme for origination and reception of voice, dial-up video and dial-up data for routine and precedence subscribers.

“4.0 POLICY

“It is DoD policy that:

- “4.1. Telecommunications switches (and associated software releases) leased, procured (whether systems or services), or operated by the DoD

Components, and connected or planned for connection to the DSN, shall be joint interoperability certified by the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) and granted information assurance certification and accreditation by the Defense Information System Network (DISN) Designated Approval Authorities (DAAs).”

3.2.6 CJCSI 6215.01C, “Policy for Department of Defense (DoD) Voice Networks with Real Time Services”

CJCSI 6215.01C, “Policy for Department of Defense (DoD) Voice Networks with Real Time Services,” establishes policy consistent with DoDI 8100.3 and prescribes responsibilities for use and operation of the DoD voice networks, to include, but not be limited to, the DSN, DRSN, DVS, and all DISN that provide Real Time Services (RTS).

This instruction is applicable to:

- “a. All telecommunications switches leased, procured (whether systems or services), or operated by any DOD Component of the Department of Defense.
- “b. The hardware or software for sending and receiving voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the DSN, DRSN or Public Switched Telephone Networks (PSTN).
- “c. End-to-End services (e.g., phone-to-phone, video-to-video units, fax-to-fax; Secure Terminal Equipment (STE-to-STE) to include tactical applications.
- “d. All technologies i.e. (circuit switch, voice over Asynchronous Transfer Mode, and Voice over Internet Protocol) that use DSN or DRSN telephone numbers; or that are otherwise incorporated into the DSN or DRSN numbering or routing plans via area code, access code, IP addressing scheme, etc. for the origination and reception of voice, dial-up video, and dial-up data for routine and precedence subscribers.
- “e. The DOD Component's planning, investment, development, operations, and management of telecommunications switches

Section 3 – Policy

connected to the DSN or DRSN for processing voice, dial-up video and dial-up data.

“f. All networks that provide DISN RTS.

“4. Policy. The DISN provides RTS via its router networks (NIPRNET, SIPRNET and the DISN Service Delivery Nodes) and via DSN, DRSN and DVS. DSN and DRSN are worldwide private-line telephone sub-networks of the DISN that provide long-haul secure and non-secure telecommunications services to DOD Component authorized users. They are the integral components of the Global Information Grid (GIG) that provide End-to-End services to critical users at the highest levels of Government. Connection approval shall follow the instructions and processes in CJCSI 6211.02C....”

“d. RTS are a subset of the four categories of services contained in the GIG Net Centric Implementation Document (NCID) v2, QoS (T300): Signaling, Inelastic/, Preferred Elastic and Elastic.

“(1) Signaling includes Network Control for managing the network.

“(2) Inelastic/ provide GIG users with live interactive telecommunications to include voice and video and the user signaling for setting up and taking down sessions over the network. They also include rapid delivery of critical C2 information involving weapons delivery capabilities. Inelastic RTS allows for the equivalent of “Face to Face” interactions in which both factual and emotional content of the interaction can be conveyed and the operation of surveillance and weapons systems that require rapid message delivery.

“(3) Preferred Elastic services include services such as instant messaging, user authentication imagery, video and audio streaming.

“(4) Elastic services include services such as, email, Web browsing, and document transfers.”

SECTION 4

UNIFIED CAPABILITIES DESCRIPTION AND KEY PROCESSES

4.1 UNIFIED CAPABILITIES SERVICES DESCRIPTION

This section describes UC, their relationship to VVoIP, and the core processes needed for a vendor to gain placement of their UC product on the DoD UC APL or for a DoD program to gain ISP or TISP Joint Staff approval. Use of products from the DoD UC APL or approved ISP/TISPs allows DoD Components to purchase and operate UC systems over all DoD network infrastructures. This section applies to both strategic and tactical systems.

Unified capabilities that are addressed in the UCR 2008 are as follows:

1. Voice and Video Services Point to Point. Provides for two voice and/or video users to be connected End Instrument (EI) to EI with services that can include capabilities such as voice mail, call forwarding, call transfer, call waiting, operator assistance and local directory services.
2. Voice Conferencing. Provides for multiple voice users to conduct a collaboration session.
3. Video Teleconferencing (VTC). Provides for multiple video users to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.
4. E-Mail/Calendaring. Provides for users to send messages to one or many recipients with features such as priority marking, reports on delivery status and delivery receipts, digital signatures and encryption. Calendaring allows the scheduling of appointments with one or many desired attendees.
5. Unified Messaging. Provides access to voice mail via e-mail or access to e-mail access via voice mail.
6. Web Conferencing and Web Collaboration. Provides for multiple users to collaborate with voice, video and data services simultaneously using Web page type displays and features.
7. Unified Conferencing. Provides for multiple users to collaborate with voice, Web, or videoconferencing integrated into a single, consolidated solution often as a collaboration application.

8. Instant Messaging and Chat. Provides real time interaction among two or more users who must collaborate to accomplish their responsibilities using messages to interact when they are jointly present on the network. For instant messaging, presence is displayed.
 - a. Instant Messaging (IM) provides the capability for users to exchange one-to-one ad-hoc text message over a network in real-time. This is different and not to be confused with signal or equipment messaging, in that IM is always user generated and user initiated.
 - b. Chat provides the capability for two or more users operating on different computers to exchange text messages in real-time. Distinguished from instant messaging by being focused on group chat, or room-based chat. Room persistence is typically a key feature of multi-user chat; in contrast with typically ad-hoc instant messaging capabilities.
 - c. Presence/Awareness is a status indicator that conveys ability and willingness of a potential user to communicate.

9. Mobility. Provides the ability to offer wireless and wired access, and applies to voice, e-mail, and many other communication applications. It includes devices such as personal digital assistants (PDAs) and smart telephones. In addition, it provides for users who move to gain access to enterprise services at multiple locations (e.g., your telephone number and desktop follow you).

In order to fully achieve the mission benefits of UC, all services must migrate to be IP based. Currently all services except voice and video are already IP. Therefore the UCR 2008 focuses on defining the standards and requirements needed to achieve multi-vendor assured secure interoperability for VVoIP with data in IP converged networks since they are the critical path to achieving UC. The set of UCs addressed will be expanded in future versions of the UCR to include:

- a. Consolidated Administration. Provides for a single point of administration, operation, and reporting for all organizations.

- b. Communicator Client. Provides a standard interface for all user communication functions via a consistent look and feel across fat, thin, and wireless mobile environments. Therefore, a common, integrated client interface application is used for telephony, voice, IM, and conferencing on a variety of platforms such as desktops, PDAs and smartphone screens.

- c. Rich-Presence Services. Allows contact to be achieved to individuals based on their availability as displayed by presence information from multiple sources, including IM, telephone, and mobile devices.
- d. Intelligent Assistants. Provide for simple access to multiple platforms and information sources from multiple platforms as well as flexible control over communication-routing options and rules.
- e. Notification Services. Provide methods and controls for sending alerts and different types of information across multiple systems to gain access to individuals or groups.

4.1.1 Unified Capabilities Service Classes

A number of UC are shown in the examples in [Figure 4-1](#), GIG End-to-End Service Class Definitions. UC include RTS such as voice and video that experience significant degradation in IP networks that are not designed to provide Quality of Service (QoS) which is needed to assure that end-to-end voice and video performance are clear, intelligible, not distorted nor degraded. Figure 4-1 identifies aggregate and granular service classes based on their need for QoS. It labels RTS as “inelastic” (e.g., intolerant of performance changes in the network) and non-RTS as “elastic” (e.g., tolerant of performance changes in the network.) In order for networks to provide the set of proper resources and performance needed by these service classes, they are identified to the network by the use of Differentiated Services Code Point (DSCP) markings.

4.2 MISSION CAPABILITIES

Assured Services Features (ASF) must be provided by UC networks based on the user category the network is serving. Based on the user category, there are users who need the full range of assured services, those that only need limited assured services, and those that need non-assured services. It must be noted that even if requirements for assured services do not apply to all users (e.g., users may be served by local area networks (LANs) with high, medium, or commercial availability, or wireless LAN users may go out of range), the IA features cannot be degraded.

4.2.1 User Categories

There are four mission based user categories, Special C2, C2, Non-C2, and Administrative. Assured services shall be used consistent with the mission of the users. For example, Special C2 users shall be provided the full range of assured services. A minimum set of assured services shall be provided to all to C2 users based on COCOM assessment of mission requirements. Non-C2 and Administrative users can receive non-assured services. Non-C2 and Administrative users shall use DoD UC networks as their first choice for purposes of cost effectiveness. The four user categories are as follows:

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	EXAMPLES
Control	Network Control & Signaling	Routing & QoS Signaling
Inelastic/Real Time	User Signaling	IP Telephony Signaling
	Short Message	Sensor-to-Shooter, UAV Control, Safety Critical Applications
	Voice	IP Telephony
	Video	Interactive Video Conferencing & Broadcast Video
Preferred Elastic	Low Latency Data	IM & User Authentication
	High Throughput Data	Imagery
	Multimedia Streaming	Video & Audio Streaming, Multimedia Conferencing
	OA&M	SNMP, Trap, & Syslog Files, Audit & Accounting Records
Elastic	Default/Best Effort	E-mail, Web Browsing, Document Transfers
LEGEND: IM Instant Messaging IP Internet Protocol OA&M Operations, Administration, and Management QoS Quality of Service		SNMP Simple Network Management Protocol Syslog System Log UAV Unmanned Aerial Vehicle

Figure 4-1. GIG End-to-End Service Class Definitions

1. Special C2 Users. A special class of user who has access to UC for origination and reception of essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among all DoD Components. Specifically, these special C2 users are identified through one or more; Chairman of the Joint Chiefs of Staff, COCOMs, Service, or DoD agency validation processes. The following are required capabilities of special C2 users:
 - a. Chairman of the Joint Staff-approved FLASH, FLASH OVERRIDE, or IMMEDIATE precedence origination.
 - b. COCOM-validated minimum-essential circuits.

- c. COCOM or Service-approved IMMEDIATE and PRIORITY precedence origination.
2. C2 Users. Users who have a requirement to originate and/or receive C2 communications but do not meet the criteria for the class of Special C2 user. C2 users can exercise authority and direction as a Joint Staff/CC/S/A properly designated commander over assigned and attached forces in the accomplishment of the mission. These Joint Staff/CC/S/A designated users can originate IMMEDIATE and/or PRIORITY precedence calls to issue or receive guidance or orders that direct, control, or coordinate military forces, whether said guidance or order is issued, received, or effected during peacetime or wartime. All C2 users are capable of receiving FO/F/I/P calls. C2 users can be re-designated by Joint Staff to originate FO/F calls or designated by the COCOM of the AOR to originate IMMEDIATE and PRIORITY calls if situation warrants. There are four (4) types of C2 users:
- a. Users approved by the Joint Staff or DoD Component for PRIORITY and ROUTINE precedence origination. These users shall be provided the full range of assured services.
 - b. DoD users with a military mission that may receive C2 communications for orders or direction at precedence above ROUTINE, even though they do not have a C2 mission for issuing guidance or orders. These users shall be provided a minimum set of assured services consistent with COCOM mission requirements.
 - c. Any Joint Staff/CC/S/A user that is authorized to originate ONLY Routine communications does not need to meet the availability or redundancy requirements of the Special C2 users or C2 users capable of originating I/P precedence. These users are categorized as C2(R).
 - d. Any non-DoD U.S. Government organization supporting Homeland Defense that requires assured services and the requirement has been validated by the Joint Staff and approved by the ASD(NII)/DoD CIO.
 - (1) The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.
3. Non-C2 Users. Those users, DoD, non-DoD, non-U.S. Government and foreign government users that have no missions or communications (equipment) requirements to

Section 4 – Unified Capabilities Description and Key Processes

originate or receive C2 communications under existing military scenarios. These users are provided access to the DoD networks for the economic benefit of the DoD. During a crisis or contingency, these users may be denied access to the DoD Networks.

4. Administrative Users. Users at DoD locations who have both local and long-distance requirements for communications with industry or the public.

4.2.2 Assured Services Features

The three GIG Assured Services are Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery, which are described as follows:

1. Assured System and Network Availability is achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.
2. Assured Information Protection applies to information in storage/at rest, as well as passing over networks, from the time it is stored and catalogued, until it is distributed to the users, operators, and decisions makers.
3. Assured Information Delivery provides information to users, operators, and decision makers in a timely manner.

DoD UC networks and services shall have the following Assured Services Features (ASF) in order to provide the three GIG Assured Services:

1. Survivable Service for System and Network Availability.

Supports C2 user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possesses the robustness to provide a surge capability when needed. The following objectives contribute to the survivability of the UC:

- a. No single point of vulnerability for the entire network, to include the NM facilities. No single point of vulnerability within a COCOM defined geographic region of the COCOM's theater
- b. No more than 15 percent of the bases, posts, camps, or stations within a COCOM defined geographic region of the COCOM's theater can be impacted by an outage in the network.

- c. System robustness through maximum use of alternative routing, redundancy and backup.
 - d. To the maximum extent possible, transport supporting major installations (base, post, camp, and station, leased or commercial sites/locations) will use physically diverse routes.
 - e. The National Military Command Center (NMCC) (and Alternate), COCOMs, or DoD Component headquarters will not be isolated longer than 30 minutes because of an outage in the backbone (long-haul) portion of the network.
 - f. Priorities, in order, by stress levels are:
 - (1) Crisis, Pre-Attack, and Theater Non-Nuclear War. Unified capabilities networks shall support all peacetime readiness (Priority 3) users, plus surge requirements for non-nuclear war and for the General War on Terrorism (GWOT). These capabilities are handled according to established precedence levels.
 - (2) Post-Attack. In the CONUS, UC networks shall possess the capability to reconstitute itself, from segments of the UC networks surviving a conventional or nuclear war, to support the NCS in reconstituting national communications. Overseas, UC networks shall possess the same capabilities to support the NCS after a non-nuclear war.
 - (3) Peacetime Readiness. Unified capabilities networks must support both C2 and non-C2 users.
 - (4) Early Trans-Attack (Few Weapons, Possible High-Altitude Electromagnetic Pulse (HEMP)). Unified capabilities networks will support C2 user traffic as able.
 - (5) Massive Nuclear Attack. Unified capabilities networks will support special C2 user traffic as able.
2. Assured Connectivity and Information Delivery.
- a. Assured connectivity ensures the connectivity from user-instrument-to-user-instrument across all DoD UC networks, including U.S. Government-controlled UC network infrastructures.

- b. DoD UC networks are required to provide assured information delivery of UC to C2 users. Assured delivery requires the ability of the DoD UC networks to optimize session completion rates for all C2 users despite degradation because of network disruptions, natural disasters, or surges during crisis or war. DoD UC networks shall be designed with the capability to assign resources on demand consistent with mission priorities. For voice and video sessions, precedence based assured service capability shall be provided to permit higher precedence users to preempt lower precedence sessions at the edge of the network. Precedence based assured service is not required in the Wide Area Network (WAN). Special C2 users (FLASH and FLASH OVERRIDE) shall be provided with non-blocking service (P.00 threshold) from user to user. (P.00 = out of every 100 calls, the probability is that zero sessions will be blocked.)

(1) Responsive Service and Assured Information Delivery.

- (a) Service must be responsive to the needs of C2 users. Special C2 users – FLASH and FLASH OVERRIDE – are provided non-blocking service.
- (b) Visibility and Rapid Reconfiguration. If blocking occurs to other C2 users sessions due to crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to situational awareness to ensure minimal blocking to services critical to the response. In response to STRATCOM JTF GNO, DISA shall possess read-access and limited/controlled write- access capabilities to all network components for providing visibility end-to-end and for modifying the configuration of network components as needed to respond to situational awareness. All actions shall be coordinated with DoD Components affected before such actions are taken if possible consistent with the “Operational Tempo” and after such actions are taken.

3. Surge Capacity and Assured Information Delivery.

- a. Mitigation of blocking of C2 users sessions that occur during short-term traffic surges shall be accomplished via MLPP.
- b. During times of surge or crisis, the CJCS can direct implementation of session controls to control the use of resources in the network to meet mission needs.,

- c. The long-haul portion of the network must be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.
5. Secure Service and Assured Information Protection. Secure EIs shall be used for the protection of classified and sensitive information being passed, to ensure its confidentiality, integrity, and authentication. The UC networks shall be configured to minimize attacks on the system that could result in denial or disruption of service. All hardware and software in the network must be information assurance accredited.
6. Interoperable Service and Assured Information Delivery. UC networks shall be designed with the capability to permit interconnection and interoperation with similar tactical, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable.
7. Voice, Video and Data Performance and Assured Information Delivery: Assure that end-to-end voice, video and data performance are clear, intelligible, not distorted nor degraded using commercial standards performance metrics. DoD UC networks in order to meet voice, video, and performance requirements shall be designed to provide QoS. Tactical UC networks can provide degraded performance consistent with meeting mission needs as compared to strategic UC network performance.

4.3 MIGRATION TO UNIFIED CAPABILITIES

Unified capabilities will migrate into a voice, video, and data converged infrastructure using an incremental approach consisting of three increments. [Figure 4-2](#), Unified Capabilities Incremental Approach, illustrates the notional incremental approach. Unified Capabilities Increment 1 focuses on VVoIP converged with data, Web, and e-mail applications. Unified Capabilities Increment 2 adds DISA NCES applications. Eventually, the IP convergence means that all different service classes E2E will be operational within the same Base/Post/Camp/Station (B/P/C/S) ASLAN/Intranet and the DISN SDNs/Transport.

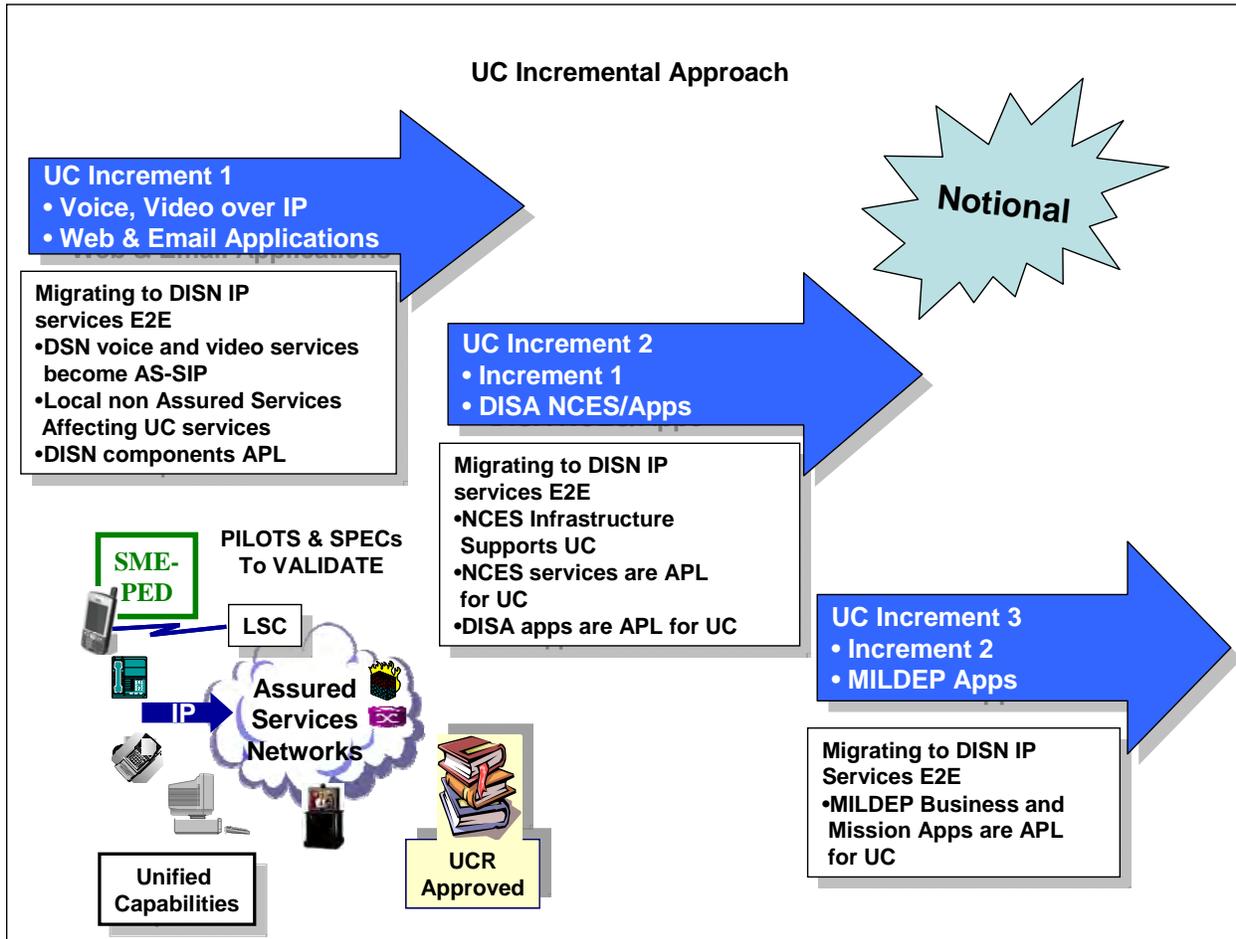


Figure 4-2. Unified Capabilities Incremental Approach

The scope of migrating toward the all IP environment for UC is illustrated in [Figure 4-3](#), Incremental Scope of Unified Capabilities Migration. The scope includes service types and infrastructure migration projected for each of the three increments. The service types, which include voice, video, collaboration, and applications, are shown across the top of the figure, with the infrastructures shown vertically on the left side of the figure.

Services →	Voice	Video	Collaboration	Applications
Infrastructure	UC Spiral 1		UC Spiral 2	
Networks	Increment 1	Increment 1	Increment 2	Increment 3
LANs	Increment 1	Increment 1	Increment 2	Increment 3
Intranets	Increment 1 SLA	Increment 1 SLA	Increment 2 Spec	Increment 3
WANs	Increment 1 SLA	Increment 1 SLA	Increment 2 Spec	Increment 3
SATCOM	Increment 1 SLA	Increment 1 SLA	Increment 2 Spec	Increment 3
Network Mgmt.	Increment 1	Increment 1	Increment 2	Increment 3
NCES Enterprise Servers			Increment 2	Increment 3
End Instruments	Increment 1	Increment 1	Increment 2	Increment 3
Wired	Increment 1	Increment 1	Increment 2	Increment 3
Wireless	Increment 1			Increment 3
Applications	Converged Ops	Converged Ops	Increment 2	Increment 3

Figure 4-3. Incremental Scope of Unified Capabilities Migration

Finally, [Figure 4-4](#), Unified Capabilities Enabled by an IP Infrastructure End to End, illustrates how UC at the user will be enabled over an end-to-end IP infrastructure.

4.3.1 UC Migration Strategy Drivers

The major drivers of the migration to UC and many of the technical requirements defined by the UCR 2008 are taken from “Department of Defense Global Information Grid Architectural Vision” the “Joint Net-Centric Operations Campaign Plan” (JNO). The purpose of the JNO CP is to provide a unifying strategy to better integrate and synchronize joint community transformation and maximize joint warfighting capabilities. The purpose of the Global Information Grid (GIG) Architectural Vision is to describe the target end state and provide direction for the development of GIG capabilities (DISN Services) that will support DoD missions, operations, and functions in the future.

In addition, CJCSI 6215.01C, “DoD Voice Networks with Real Time Services,” provides more detailed requirements for VVoIP. The DoDI 8510.01 on DIACAP is a major driver of UC migration as is the ASD(NII)/DoD CIO guidance on IPv6.

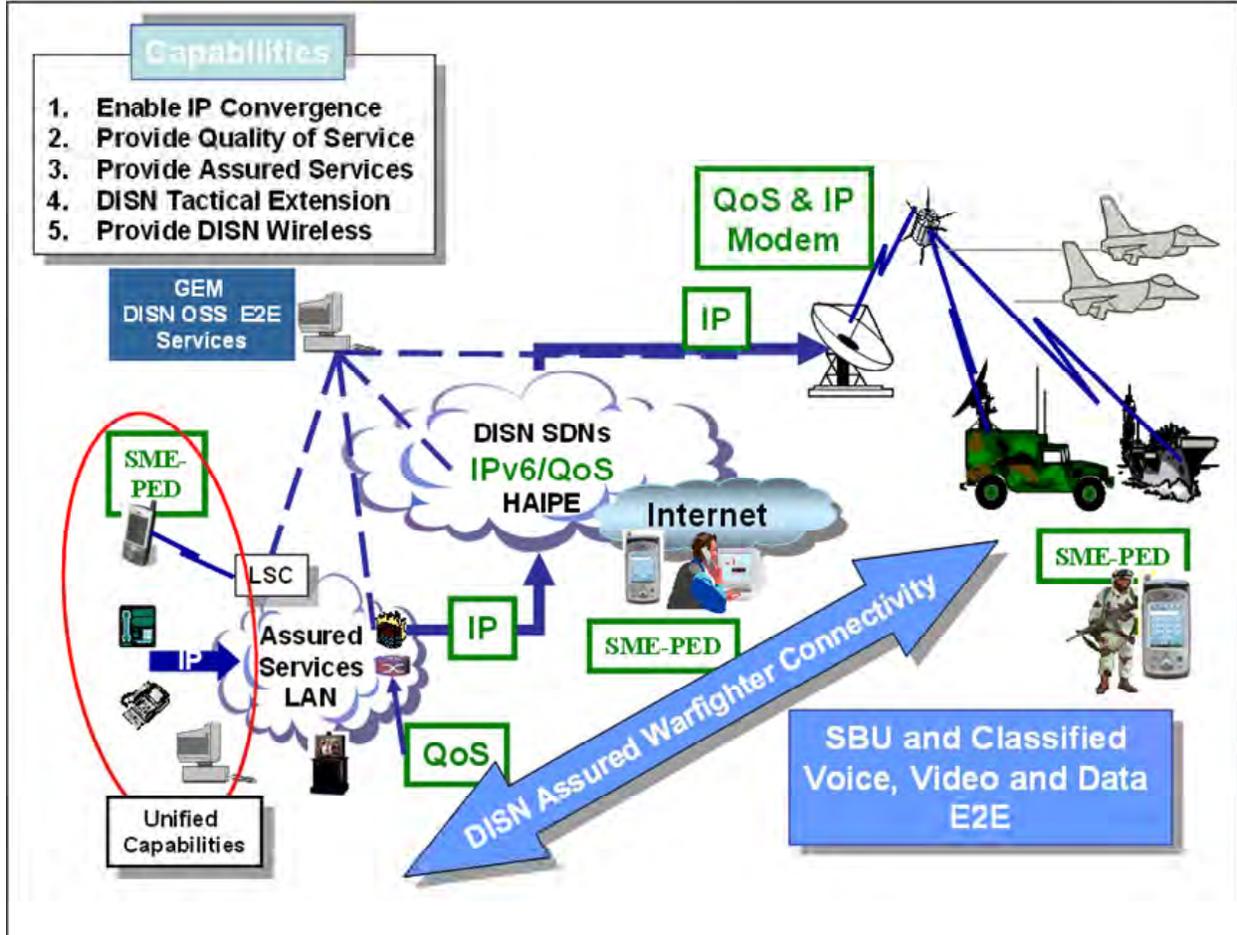


Figure 4-4. Unified Capabilities Enabled by an IP Infrastructure End to End

The most demanding set of requirements in these documents that drive the migration from legacy technologies to IP technologies involves those associated with the following:

- Information Assurance (IA) consistent with the DIACAP and STIGs that must change constantly due to attacks
- Assured services across hybrid circuit-switched and IP networks
- End-to-end interoperability among multiple vendors
- End-to-end interoperability between strategic and multiple tactical programs
- NetOps end-to-end voice and video performance over IP converged networks that simultaneously serve voice, video, and data

- NetOps UC Element Managers that can support situational awareness using Policy-based network management (PBNM) over IP converged networks that simultaneously serve voice, video, and data
- IPv6
- Fully leveraging COTS features associated with UC to enhance mission and combat support productivity

These requirements are the most demanding because IP-based technologies have inherent IA limitations that must be mitigated and were not originally designed for voice and video (or RTS) and thus require a variety of techniques to properly support voice and video. Thus, IP-based technologies require GIG end-to-end system engineering, development by industry, and test and evaluation by the JITC to satisfy the policies and meet the requirements. In addition, the technical challenges and MILDEP funding limitations prevent the ability to install a common IP technology base as a “flash cut.” Thus, networks based on hybrid technologies will be required for many years; therefore, the UCR 2008 covers technical requirements for both TDM and IP-based systems that support UC.

Several of these migration drivers are addressed in the subsequent sections.

4.3.1.1 Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise

“Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise,” defines nine DoD CIO target GIG attributes necessary to achieve the net-centric transformation of the GIG that require fundamental shifts and advances in technologies, architectures, systems, policies, processes, doctrines and culture. The target GIG attributes align to enable a dynamic and responsive end-to-end operational environment, where information is available; the means to produce, exchange, and use information are assured and protected; and resources such as bandwidth, spectrum, and computing power are dynamically allocated based on mission requirements and implemented using precedence, priority and resource allocation techniques. Like the Internet and the World Wide Web, the target GIG follows a many-to-many approach to sharing information. The GIG communication infrastructure is scalable, robust, and highly available based on packet switching that enables the interconnection of anyone, anywhere, at any time with any type of information such as voice, video, images, or text. Robust and dynamic IA capabilities are embedded across the target GIG to protect all information, every information transaction, and GIG software and hardware. A common IP-based packet communications layer transparently provides information transfer to users through dissimilar wireless and wired devices. More specifically the DoD GIG Architectural vision calls for,

1. General

“The Communications Infrastructure provides secure, agile, and survivable end-to-end connectivity and on-demand bandwidth that is dynamically allocated, based on operational priority and precedence among millions of space, air, sea, and terrestrial-based fixed, mobile, and moving users. This communications infrastructure supports those on the warfighting edge by enabling... (4) reliable delivery, and (5) an ability to dynamically extend connectivity as needed, which includes mission partners through controlled interfaces. It is an infrastructure that users can rely on—one that continues to function under physical, cyber, or electronic attack. Redundancy of paths, the ability to reallocate bandwidth based on path conditions, the commander’s policies and priorities, and automated routing alternatives are key to the high availability of this infrastructure.

“The communications infrastructure is achieved by integrating the Department’s diverse set of communications assets into a reliable, end-to-end communications capability. This integration is based upon adherence to a set of network interfaces, standards, and guidelines in key areas. These areas include: a common network IP, physical communication links, access protocols, routing protocols, consistent Quality of Service (QoS)/Class of Service (CoS), IA methodologies, ...”

2. Attributes

- a. Adapt the DISN with Internet standards that enhance “mobility, surety, and military unique features (e.g., precedence, preemption).”
- b. Provide QoS tailored DISN services: “voice, still imagery, video/moving imagery, data, and collaboration.”
- c. “...an IP-based network infrastructure [The Convergence Layer] is the foundation of end-to-end interoperability in the target GIG. All types of information such as telephony, multimedia services, video, and data are converged over this universal network.”

3. Secure and Available Information Transport/Trusted and Tailored Access

- a. “Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.”

- b. “Access to the information transport, info/data, applications and services linked to user’s role, identity and technical capability.”
4. Federated DoD Enterprise Architecture (EA). “Finally, realization of the operational benefits of the target GIG in enabling NCO [Net-Centric Operations] requires the development and implementation of new concepts of operations, tactics, business processes, and organizational changes for the Department. Training and experimentation are critical in identifying and validating the benefits and risks of information sharing, as well as its impact on NCO.”

4.3.1.2 Joint Net-Centric Operations Campaign Plan

The Joint Net-Centric Operations (JNO) Campaign Plan defines six Joint Community Warfighter (JCW) Chief Information Officer (CIO) goals necessary to make substantive progress toward achieving the full benefits of a networked force. [Table 4-1](#), Joint Community Warfighter CIO Goals, identifies four JCW CIO goals that are of primary relevance to the DISN mission. Effective network connectivity and interfaces improve the joint force ability to access key information transport capabilities that enable information sharing at all levels, from the “first tactical mile” across the entire DoD. Protecting information, defending the network, and keeping network services available are essential elements of Information Assurance (IA). A synchronized approach to developing, procuring, engineering, and fielding joint capabilities provides the DoD community with timely, coordinated information sharing. Enterprise NM enables the effective operation of systems and networks including their configuration, availability, performance, manageability, and enterprise connectivity.

4.3.1.3 Internet Protocol Version 6 Requirements

DoD CIO Memorandum “DoD IPv6 Definitions” dated June 26, 2008 provides the definitions of IPv6 Capable and Enabled as follows:

1. IPv6 Capable Products. Products (whether developed by commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/v6 environments. IPv6 Capable Products shall be able to interoperate with other IPv6 Capable Products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also:
 - a. Conform to the requirements of the DoD IPv6 Standard Profiles for IPv6 Capable Products document contained in the DISR.

Table 4-1. Joint Community Warfighter CIO Goals

GOAL		DESCRIPTION
1.1	Connect the Warfighter	It is essential that seamless communications services be available to joint warfighters and mission partners under all conditions and at every echelon—especially at the “first tactical mile.”
1.2	Secure the Network	Provide the warfighter an assured information environment, protected and defended throughout the battlespace and across the entire network.
1.3	Synchronize Delivery of Network Capabilities	Strengthen joint warfighting by synchronizing delivery of capabilities and ensuring integration of capabilities across the entire Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF)
1.4	Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access	Support JNO through improved GIG enterprise management, including electromagnetic spectrum management at all echelons.

- b. Possess a migration path and/or commitment to upgrade from the developer (company Vice President, or equivalent, letter) as the IPv6 standard evolves.
 - c. Ensure product developer IPv6 technical support is available.
 - d. Conform to National Security Agency (NSA) and/or Unified Cross Domain Management Office requirements for Information Assurance products.
2. IPv6 Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6 capable network shall be ready to have IPv6 enabled for operational use, when mission need or business case dictates. Specifically, an IPv6 Capable network must:
- a. Use IPv6 Capable Products.
 - b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.
 - c. Conform to DoD and NSA-developed IPv6 network security implementation guidance
 - d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

3. IPv6 Enabled Network. An IP network that is supporting operational IPv6 traffic, through the network, end-to-end.

4.3.1.4 Critical Milestones and Actions for Complete Circuit-Switch Phase-Out

A major aspect of the migration toward an end-to-end IP infrastructure for UC is the migration of voice and video services from DSN circuit switching to VVoIP over IP. The date for a complete phase-out of the TDM-based DSN is not predictable. This date is totally dependent on the success of test programs and DoD Component's and allied funding.

In order to expeditiously move forward on the vision of Net Centricity and to exploit what COTS and standards based IP technologies can deliver yet maintain affordable assured services for the warrior, we have elected to implement a less than perfect IP-based solution for FY 2008. This solution is referred to as a "70%" solution because it cannot do all that is needed but is a significant step forward in achieving the IP convergence vision.

Finally, the DSN circuit-switched network will phase out when:

1. UC Migration system design, system engineering, UCRs and test programs are completed. The FY 2008 System 70% Design and the UCR 2008 must be validated in the DISN Spiral deployment of capabilities. This will provide the VVoIP foundation upon which the migration to UC can be implemented using future versions of the UCR consistent with major policies and requirements for Net Centricity and NetOps that are continuing to be refined and matured.
2. DISN WAN and MILDEP Intranets Service Level Agreements for QoS Capabilities are available. Assured requirements capabilities projected to be available by FY 2010 include: assured service SLAs (e.g., non-blocking Grade of Service (GoS), voice and video quality, packet loss, jitter, latency, availability, DSCPs from the GIG QoS Working Group, PHB determined by supporting network based on VVoIP SLAs).
3. UC APL Assured Services Solutions are available. All IP solutions necessary to replace the circuit-switched services are on the APL.
4. Deployment is completed for Multifunction Softswitches or standalone Softswitches that allow for secure interoperability among multiple vendors and mixed technologies.
5. Joint Hawaii Information Transfer System (JHITS) becomes end-to-end IP. DoD funds, purchases, and installs the upgrade of the JHITS end to end based on Pacific Command's approval.

6. UC Master Plan is approved.
 - a. DoD plans and programs to fund, purchase, and install hybrid MFSSs and, ultimately, migrate to pure softswitches for SBU voice and video.
 - b. The DoD Components plan and program to fund, purchase, and install VVoIP Edge systems from the APL.
 - c. The DoD tactical community plans and programs to fund, purchase, and install VVoIP APL Edge systems or obtain a Joint Staff-approved Information Support Plan.
7. UC Master Plan is executed. Detailed joint transition and cutover planning unique to each theater and country will be required.

4.3.2 Programs Migration to VVoIP

The VVoIP subset of UC is currently provided by 1) the existing TDM-based DSN with SBU VoIP on the line side (at the telephone) over ASLANs but not end-to-end using the TDM transport layer of DISN; 2) the existing TDM-based DRSN with Multi Level Secure services using the TDM transport layer of DISN; 3) the VoSIP with Secret level services using the SIPRNet; 4) DVS VTC services via a mixture of DSN ISDN services and limited DVS video over IP for both SBU and Secret Level services, 5) Teleport and 6) Tactical Programs. The TDM-based services will migrate over a long period of time to IP-based assured services systems end-to-end over MILDEP ASLANs/Intranets, and the DISN SDNs/Transport. During the migration time frame, UC will be provided by a hybrid arrangement of both TDM- and IP-based systems. The VoSIP, DVS, Teleport, and Tactical Programs will upgrade their infrastructures using approved products based on the UCR 2008.

As a result of the number of programs and technologies that either will be replaced by the VVoIP technology insertion or will need to be augmented to support the migration, in subsequent paragraphs, the DISN, DSN, DRSN/VoSIP, DVS, and Tactical Programs migrations are addressed.

[Figure 4-5](#), DISN SDNs Migration, illustrates the migration of the DISN SDNs, which is critical to end-to-end performance of UC.

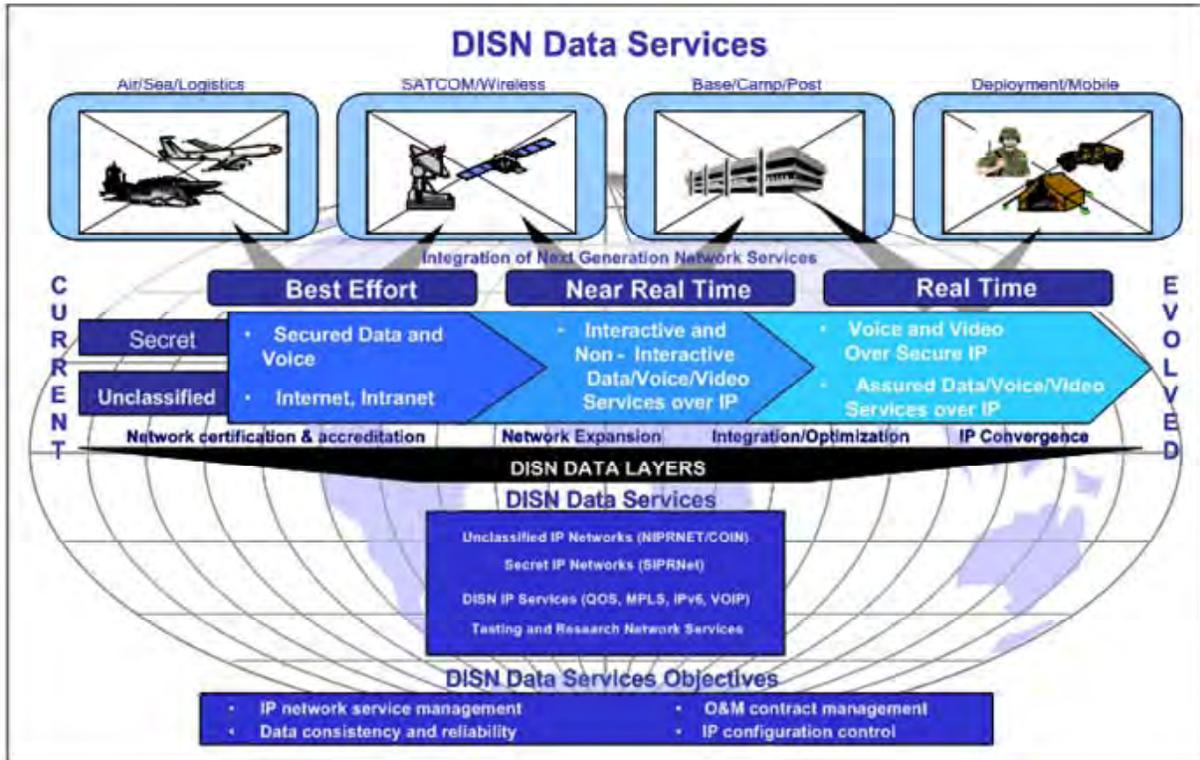


Figure 4-5. DISN SDNs Migration

A high-level view of the VVoIP technology insertion and migration is shown in [Figure 4-6](#), VVoIP Technology Insertion and Migration from Circuit Switching, which illustrates the phase-out of SBU voice circuit switch technologies based on MILDEP business cases and the initial insertion of VoIP to the telephone technologies, followed by the insertion of E2E VVoIP technologies based on MILDEP business cases.

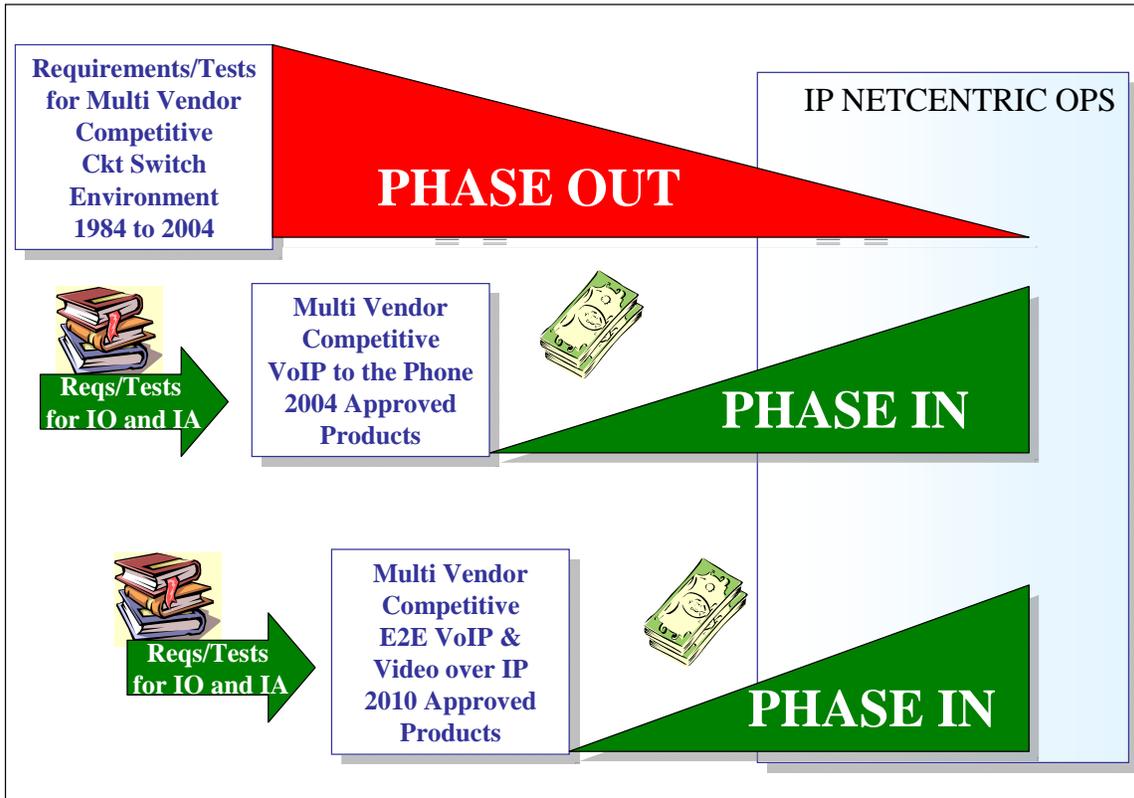


Figure 4-6. VVoIP Technology Insertion and Migration from Circuit Switching

Key to this migration will be a series of multiple Edge and WAN test programs. [Figure 4-7](#), SBU Voice and Video Migration to UC, illustrates a high-level overview of the migration approach for Sensitive but Unclassified Voice and Video.

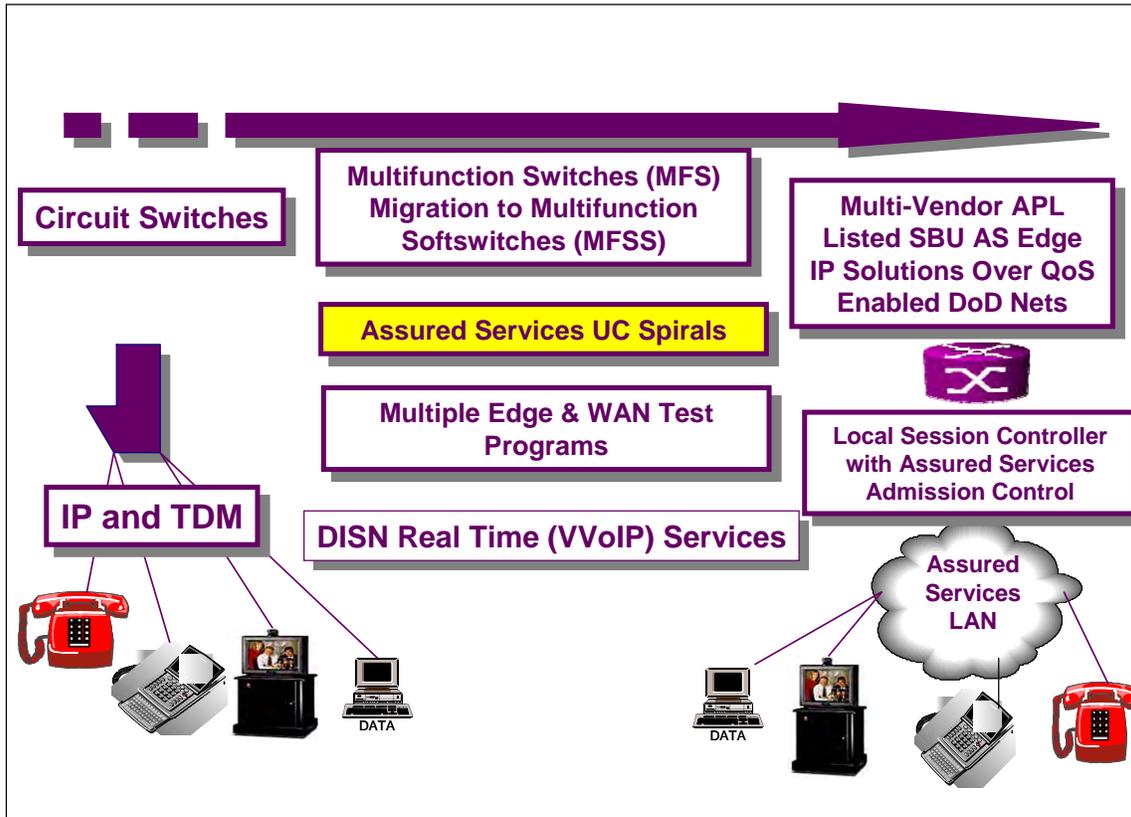


Figure 4-7. SBU Voice and Video Migration to UC

[Figure 4-8](#), Classified Voice and Video Migration to Classified UC, illustrates a high-level overview of the migration approach for Classified Voice and Video. This migration recognizes the need to sustain the DRSN technology for users with MLS and specialized conferencing capabilities. VoSIP will migrate to a set of capabilities based on the SBU VVoIP technologies.

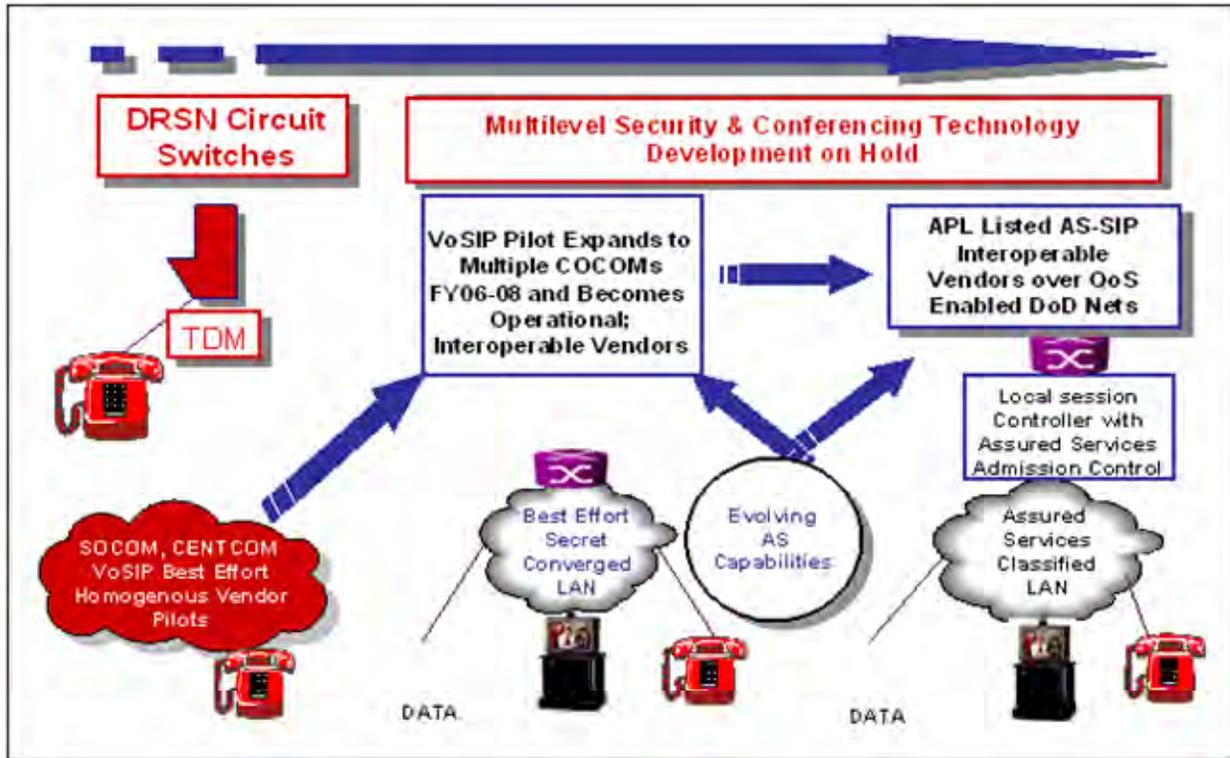


Figure 4-8. Classified Voice and Video Migration to Classified UC

The SBU VVoIP convergence migration strategy is illustrated in [Figure 4-9](#), SBU VVoIP Convergence Migration Strategy Overview. The left side of the figure shows the three network segments of the current UC architecture: Customer Edge, Network Edge, and Network Core. Across the top of the figure are the major time frames associated with the migration.

Today’s voice and video capabilities will be migrated from circuit-switched technologies to IP-based DISN VVoIP service converged with data services as follows for each of the system design’s main network segments:

1. At the Customer Edge network segment, the Edge components and systems will migrate from TDM with circuit switches to all IP infrastructures, and the current TDM-based MLPP functionality will be replaced by deploying IP-based Local Session Controllers with Assured Services Admission Control and ASLANs.
2. At the Network Edge and Core Network segments, migration will be accomplished by upgrades to DSN MFSSs to become MFSSs, and by migrating access and long-haul backbone transport from TDM to IP transport provided by the DISN Service Delivery Nodes and the MILDEP Intranets that must be enabled to provide QoS to meet the VVoIP SLA.

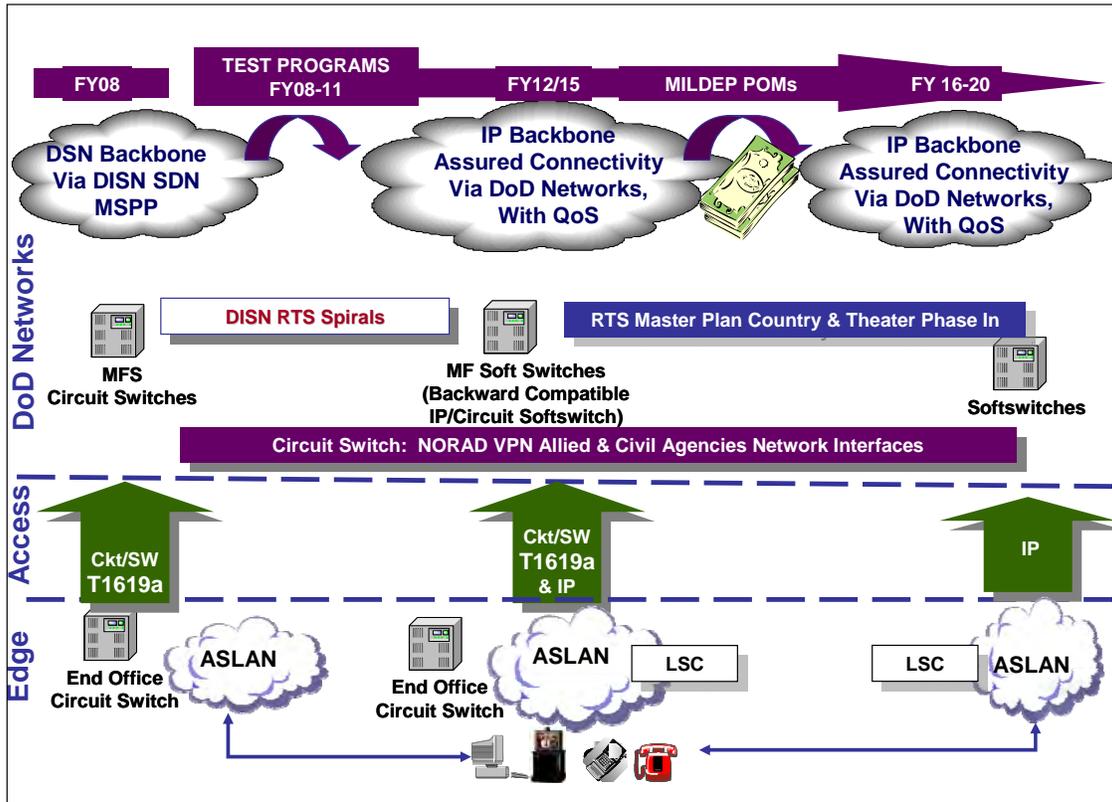


Figure 4-9. SBU VVoIP Convergence Migration Strategy Overview

[Figure 4-10](#), Classified VVoIP Convergence Migration Strategy as a Hybrid End State, illustrates the classified VVoIP convergence migration strategy as a hybrid end state.

Both SBU VVoIP and Classified VVoIP Edge systems will be the almost identical with the exception of a few features and with the exception of the Multifunction Softswitch (MFSS). SBU VVoIP needs a MFSS to bridge between the circuit switch and IP infrastructures. Classified VVoIP uses a Standalone Softswitch that uses dual IP signaling to bridge from its current infrastructure to AS SIP and bridges to the circuit-switched DRSN via a gateway.

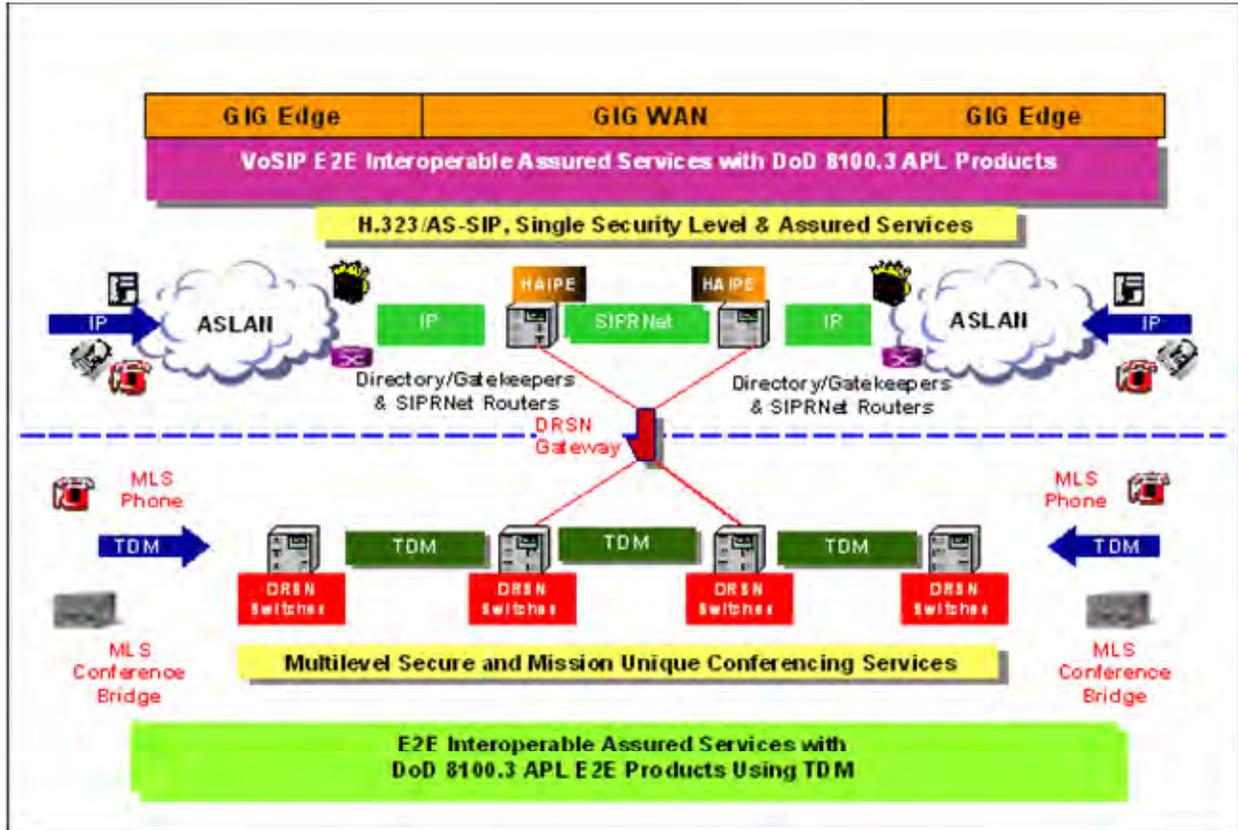


Figure 4-10. Classified VVoIP Convergence Migration Strategy as a Hybrid End State

Figure 4-11, Hybrid DVS VTC Services, illustrates the hybrid DVS VTC services that will exist until the DVS is able to migrate to the SBU system design and multilevel secure end user services can be accommodated by a next generation KIV-7 capable of IP operations.

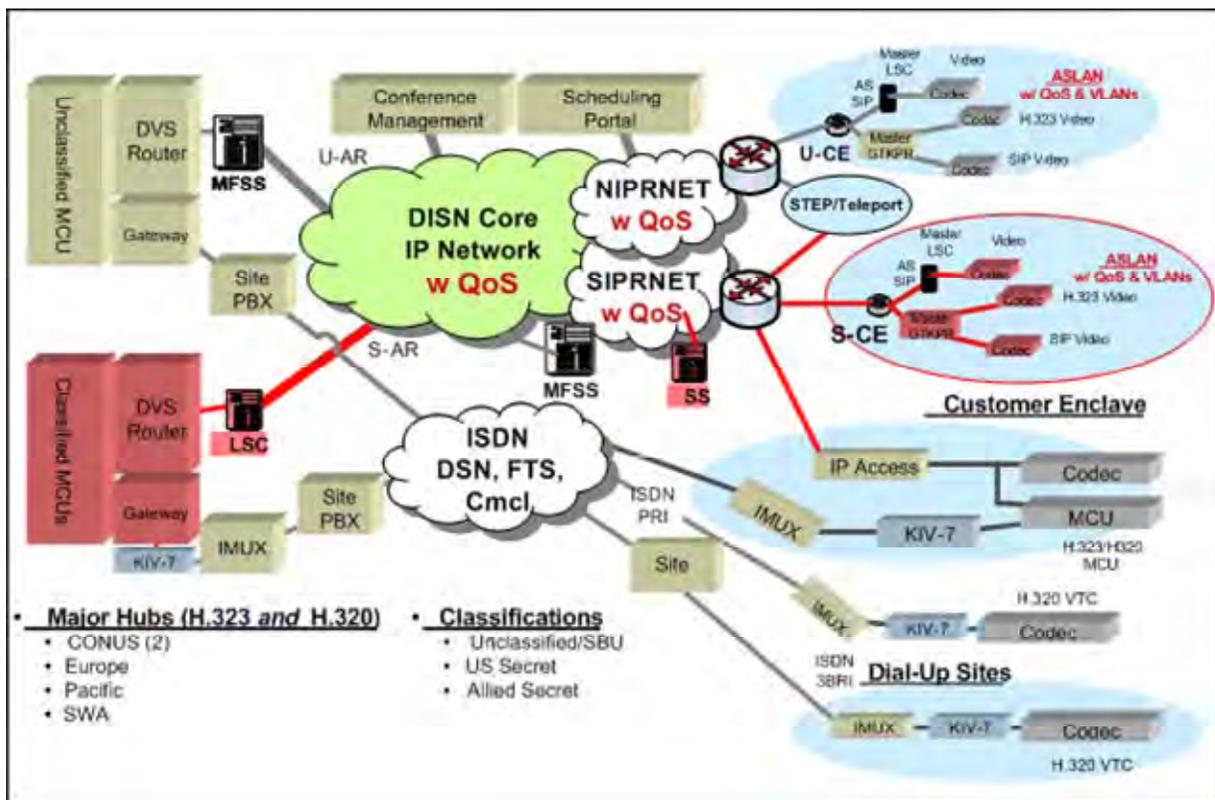


Figure 4-11. Hybrid DVS VTC Services

Figure 4-12, Tactical Component of the VVoIP Design, illustrates the Tactical component of the system design and the programs that are adopting the VVoIP system design as part of their migration.

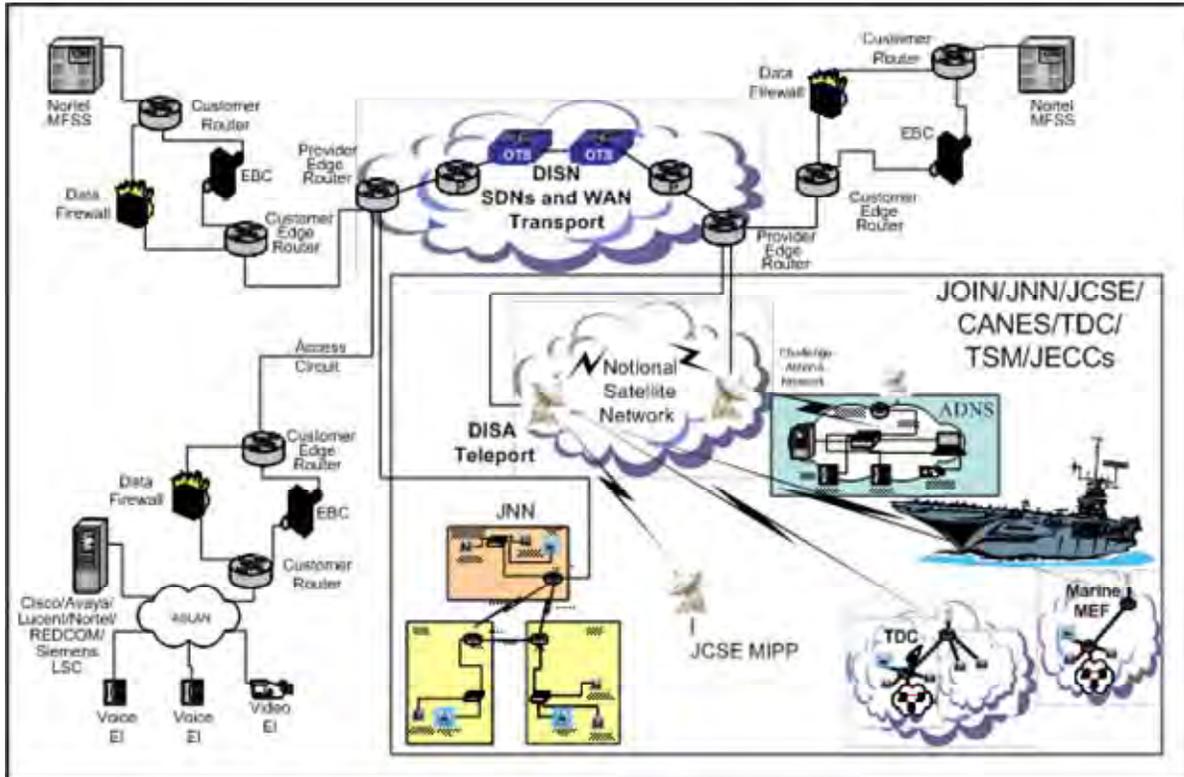


Figure 4-12. Tactical Component of the VVoIP Design

Figure 4-13, Migration of Both SBU VVoIP and Classified VVoIP from FY 2008’s IP Services to the Final Architecture, illustrates the complex migration of Both SBU and Classified VVoIP from today’s IP services to the final VVoIP architecture.

4.3.3 Migration Time Frames

This section describes major transition events and provides technical overviews of the transition architectures during the three major migration time frames, which are FY 2008-2011, FY 2012-2015, and FY 2016-2020. Due to funding and technology maturity, in all three time frames, VVoIP will be provided by a coexistence of three types of architectures: 1) TDM/circuit-switched WAN with hybrid edges of TDM and IP, 2) IP WAN with hybrid edges of TDM and IP, and 3) the goal architecture of IP end to end.

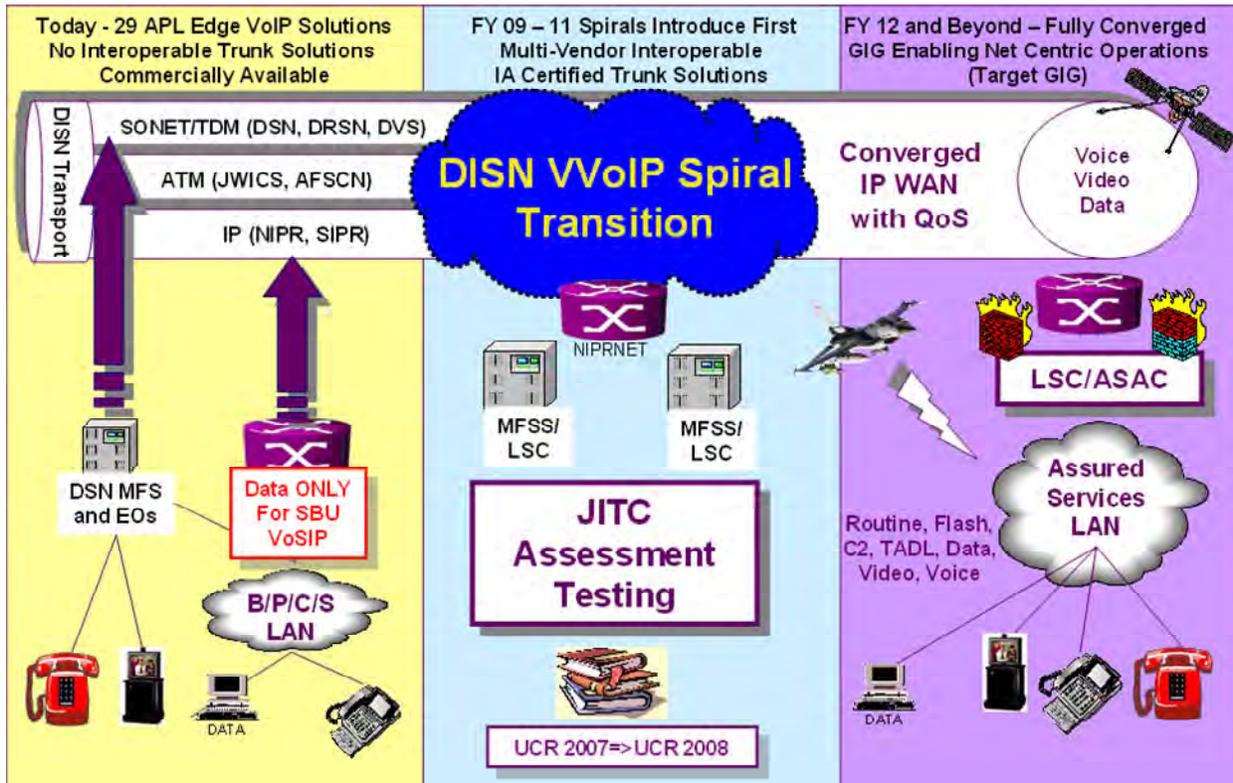


Figure 4-13. Migration of Both SBU VVoIP and Classified VVoIP from FY 2008’s IP Services to the Final Architecture

Figure 4-14, SBU Hybrid Circuit Switched and VVoIP Design, illustrates the SBU hybrid circuit-switched and IP VVoIP converged with data services system design that will exist for many years as the migration to SBU VVoIP is funded. The network migration planning strategy for hybrid operations will reflect the following approach: End-to-end voice quality must be maintained during the migration period when the network consists of both TDM and IP segments. Each time a call bearer stream converts between IP and TDM transport modes; there is a degradation of voice quality. Therefore, the network implementation approach will seek to minimize the number of IP-to-TDM-to-IP conversions for an end-to-end call. Planning considerations will follow a scenario where a call that originates in the TDM portion of the overall network will be routed on a TDM basis as far as possible toward an IP-based destination before being converted to IP.

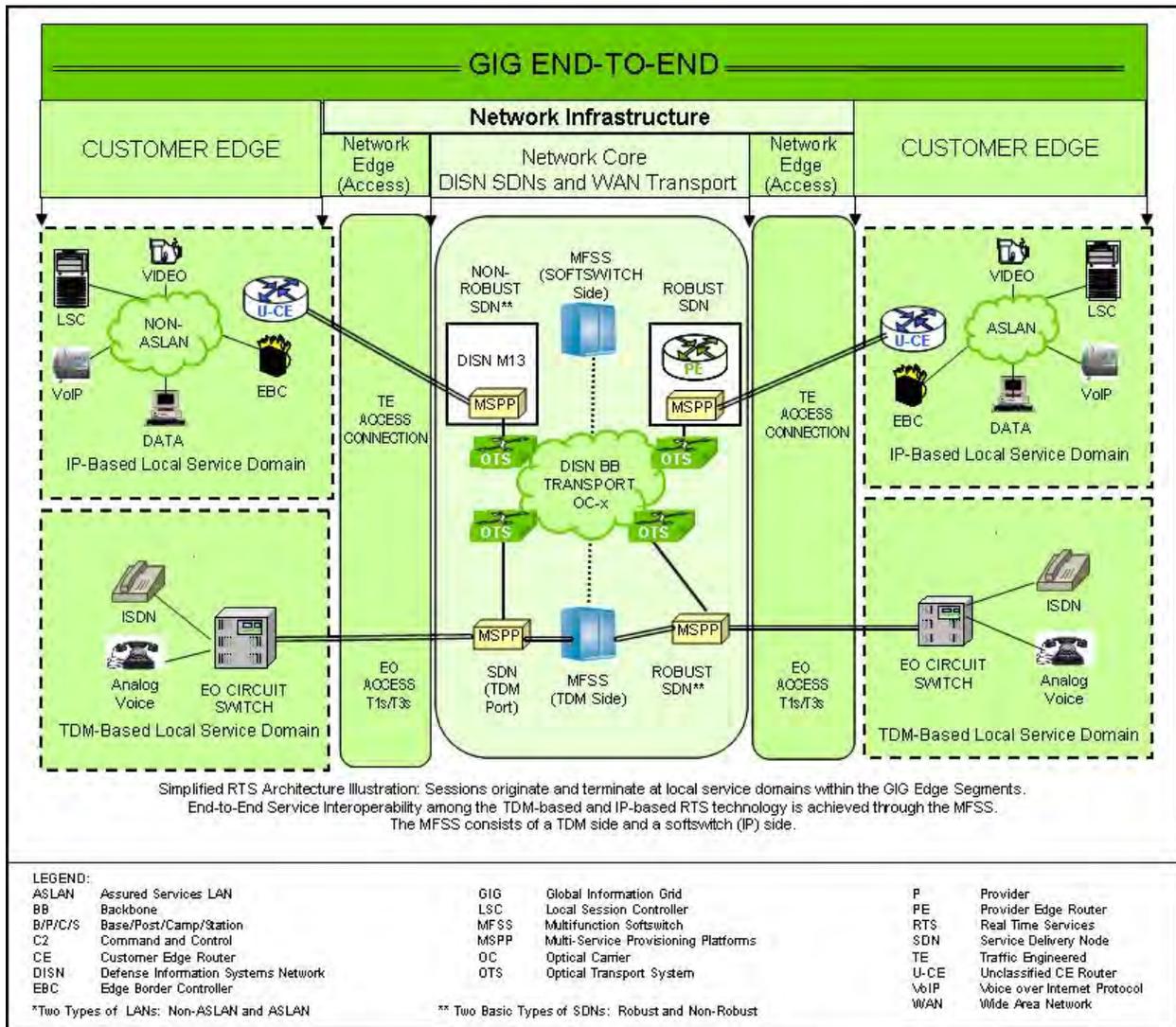


Figure 4-14. SBU Hybrid Circuit Switched and VVoIP Design

4.3.3.1 Migration Time Frame – Fiscal Years 2008-2011

In the FY 2008-2011 time frame, hybrid operations will begin when the new VVoIP End-to-End capabilities are deployed in technology Spirals while the DSN circuit-switched network provides operational services. DRSN is operational providing high quality Multi-level classified voice and conferencing services. VoSIP is operational providing Secret Level Best Effort voice services over SIPRNet. DVS is providing predominately ISDN based VTC services using DSN and a small number of Best Effort video services over both NIPRNet and SIPRNet. FY 2012 Architecture, System Design, and the UCR 2010 must begin in this time frame driven by the updates to JS and ASD(NII)/DoD CIO policies, and the maturity of network level techniques for providing assured services such as MPLS VPNs and HAIPE Discovery Servers.

4.3.3.1.1 SBU Voice and Video Operational Services

Operational SBU voice and video services will be provided by the DSN which will consist of MFSs that provide local (i.e., on-B/P/C/S) voice, dial-up video, and data services; and backbone (i.e., long-haul or WAN) circuit switching. Long-haul (WAN) transport between the MFSs is provided by TDM transport from the MILDEP bases to the DISN Service Delivery Nodes, then via the DISN SDNs MSPPs and DISN optical backbone transport.

The MFSs provide interfaces between the DSN and the following external networks:

- DRSN
- Enhanced Mobile Satellite Systems (EMSS)
- Allied networks (e.g., North American Treaty Organization (NATO), Canada, United Kingdom, Australia)
- Civil agencies (e.g., Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), State Department)
- Government Emergency Telecommunications Service (GETS)
- FTS
- PSTN

The Edge systems are a mixture of EO, SMEO, PBX1 circuit switches with both TDM EIs and VoIP EIs operating over ASLANs capable of MLPP. The DSN VoIP with MLPP to the telephone is available with over 22 Edge solutions on the DoD UC APL for MILDEPs to purchase and can be network-managed end to end. Video services are provided for point-to-point videos, distance learning and for Video Teleconferencing via DSN ISDN services. These systems are operating in accordance with the DSN VoIP STIG.

DRSN is operational providing high quality Multi-level classified voice and conferencing services. VoSIP is operational providing Secret Level Best Effort voice services over SIPRNet. DVS is providing predominately ISDN based VTC services using DSN and a small number of Best Effort video services over both NIPRNet and SIPRNet.

4.3.3.1.2 SBU VVoIP Voice and Video Services Technology Insertions

During FY 2008 thru FY 2010, a series of assessment tests will be conducted on prototype and preproduction systems that are capable of E2E assured SBU and Classified voice and video services. Assessment tests are being conducted at the JITC, the TJTJN JOIN test bed and other distributed test beds, in collaboration with multiple vendors. The SBU and Classified voice and video services are on their way to E2E DISN IP-based Assured/Secure VVoIP at the Edge, over the DISN SDNs and to Tactical users.

The FY 2008 architecture as a 70% E2E IP converged solution is underway for implementation. The UCR 2008 forms the basis of the DISN VVoIP deployment testing and for establishing the DoD UC APL. The VVoIP STIG will be completed. A full range of test programs is planned with multivendor E2E capability deployment. The Theater Joint Tactical Networks Configuration Control Board (TJTJNCCB) and industry are fully engaged. First realization of convergence is in the deployment of DISN VVoIP capabilities, which will introduce NETOPS Convergence with products on the DoD UC APL by FY 2010.

As these VVoIP technology insertion solutions emerge from the test bed assessment testing, RTS capabilities will be deployed using two deployment spirals as indicated in [Figure 4-15](#), UC Capabilities Deployment Way Forward:

1. Deployment Spiral 1. Under deployment Spiral 1, the following capabilities will be tested and verified:
 - a. Early local level UC
 - b. IA: DIACAP processes CA and DAA per location
 - c. MFSS to MFSS hybrid network operations– Monitor fault, configuration, accounting, performance, and security (FCAPS).
 - d. End-to-end strategic multivendor interoperability– Monitor FCAPS.

The completion of the above capabilities will result in successful vendors having their products placed on the APL. Only after the Spiral 1 participating vendors have been placed on the APL will vendors who did not participate be allowed to enter the normal APL process at JITC.

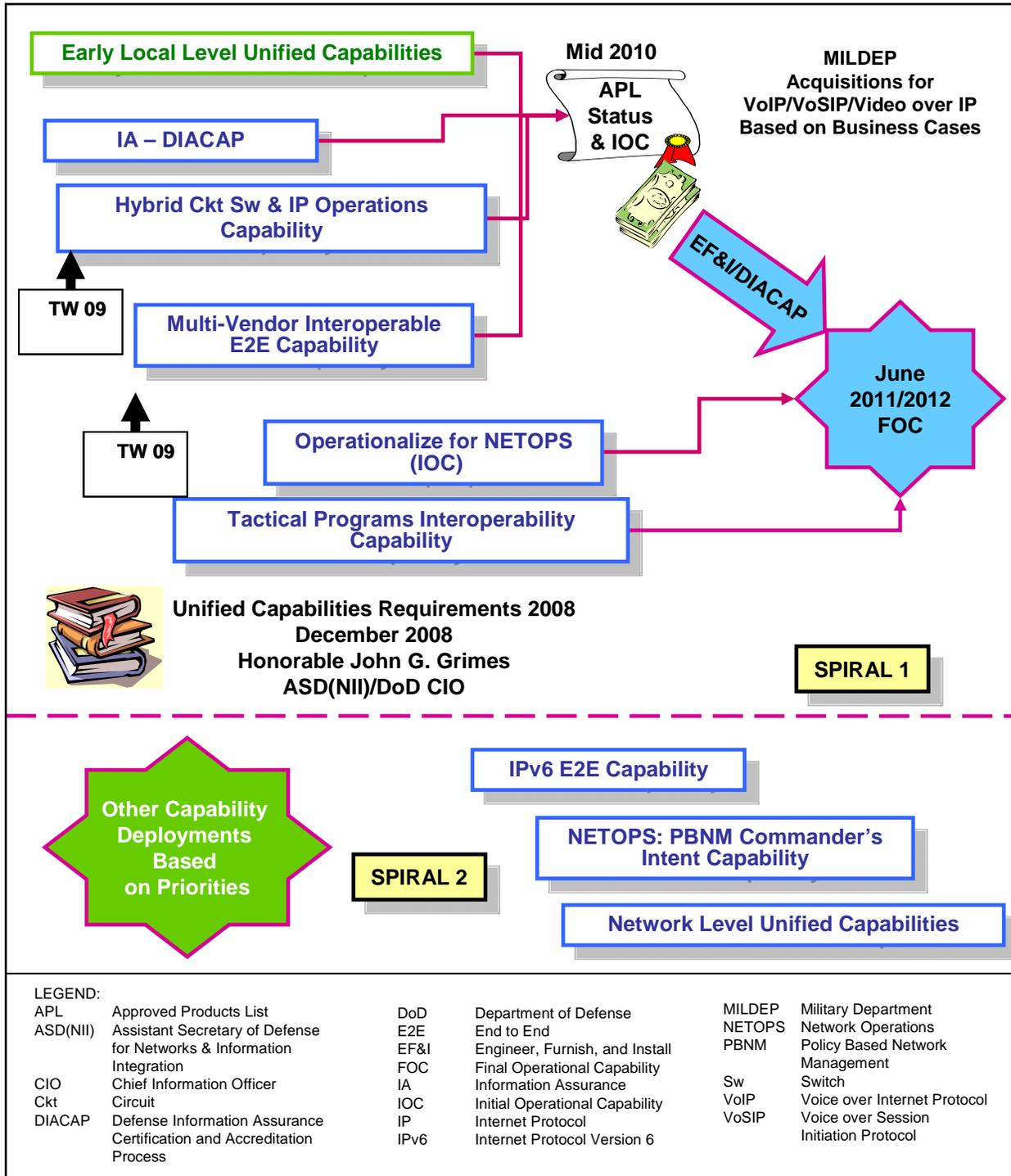


Figure 4-15. UC Capabilities Deployment Way Forward

Additional capabilities that will be deployed during deployment Spiral 1 include the following:

Section 4 – Unified Capabilities Description and Key Processes

1. Operationalization for NETOPS (Mid 2010). This capability ensures that E2E performance can be jointly managed by JTF GNO, DISA, and MILDEPs Network Operations Centers to ensure quality services and isolate causes of degradation for VVoIP deployment. This capability will include assessments of both the DISN SDNs and MILDEP Intranets capabilities to meet the VVoIP SLA.

At this point DISN VVoIP will have achieved IOC.

2. Strategic/Tactical Programs IO Capability. This capability, when implemented, represents Final Operational Capability (FOC) for DISN VVoIP capability deployment.

The completion of the above capabilities will result in successful Tactical Programs having their Tailored ISPs approved and their Tactical VVoIP equipment suite placed on the APL.

3. Deployment Spiral 2. Under deployment Spiral 2, the following capabilities will be tested and verified:
 - a. IPv6 E2E for Joint Staff criteria
 - b. NETOPS: PBNM Commander's intent for response to situational awareness (DISA CP-SIB Commander's intent)
 - c. Network-level unified communications

Spiral 1 participation includes four (4) Military Services with twelve (12) sites; TJTNCCB and five (5) Tactical programs; DISA, JTF GNO, JITC and Teleport; five (5) telephony vendors; two (2) router vendors; two (2) VVoIP firewall vendors.; three (3) video vendors and one (1) secure voice EI vendor.

During this period the IA challenges associated with the deployment of DISN voice and video operating in IP converged networks with data services will be resolved. Information Assurance certification and testing of the new, converged environment are faced with new challenges. The following are major factors:

1. VVoIP on the SBU backbone and DIACAP arrive about the same time.
2. Telephone/Video Codec/LAN connection to NIPRNet increases IA risk.

3. Current firewalls are not designed to securely process VoIP or Video over IP signaling and bearer streams. Opening up ports/protocols to support VoIP at the data firewalls increases risk for data networks
4. VVoIP aware dynamic stateful firewalls are required to mitigate the risk.
5. New VVoIP STIG in development and Operating System, Enclave, NOC, and Network STIGs must also be used.
6. IPv6 is included in all appropriate STIGs and there are currently no Intrusion Detection Systems (IDSs) that operate with IPv6.
7. DIACAP drives new processes in a higher risk IP world. Approval authority moves to the 3-star level, not local B/P/C/S DAA.
8. DISN and thus VVoIP falls under a PAA: DoD Deputy Chief Information Officer (DCIO) PAA Enterprise Information Environment Mission Area.
9. Eight DIACAP IA control areas must be jointly executed.
10. Each MILDEP is independently developing how it will meet DIACAP for VoIP and video over IP.
11. A DoD joint approach to DIACAP is needed with shared workload and results for VVoIP.

For Spiral 1, steps must be developed for extensive reuse of JITC and each MILDEP's DIACAP processes and results. [Figure 4-16](#), IA Controls Reuse Process, illustrates how the eight (8) DIACAP IA controls are grouped and how a joint, cooperative effort between the MILDEPs and JITC can develop effective processes that include reuse.

In order to deal with the IA challenges a DISN VVoIP governance structure will be established modeled after the NECC governance structure and includes the following:

- PAA Enterprise Information Environment Mission Area: DDCIO
- Designated Approval Authority: DISA
- Certification Authority: DISA Field Security Office (FSO)

Section 4 – Unified Capabilities Description and Key Processes

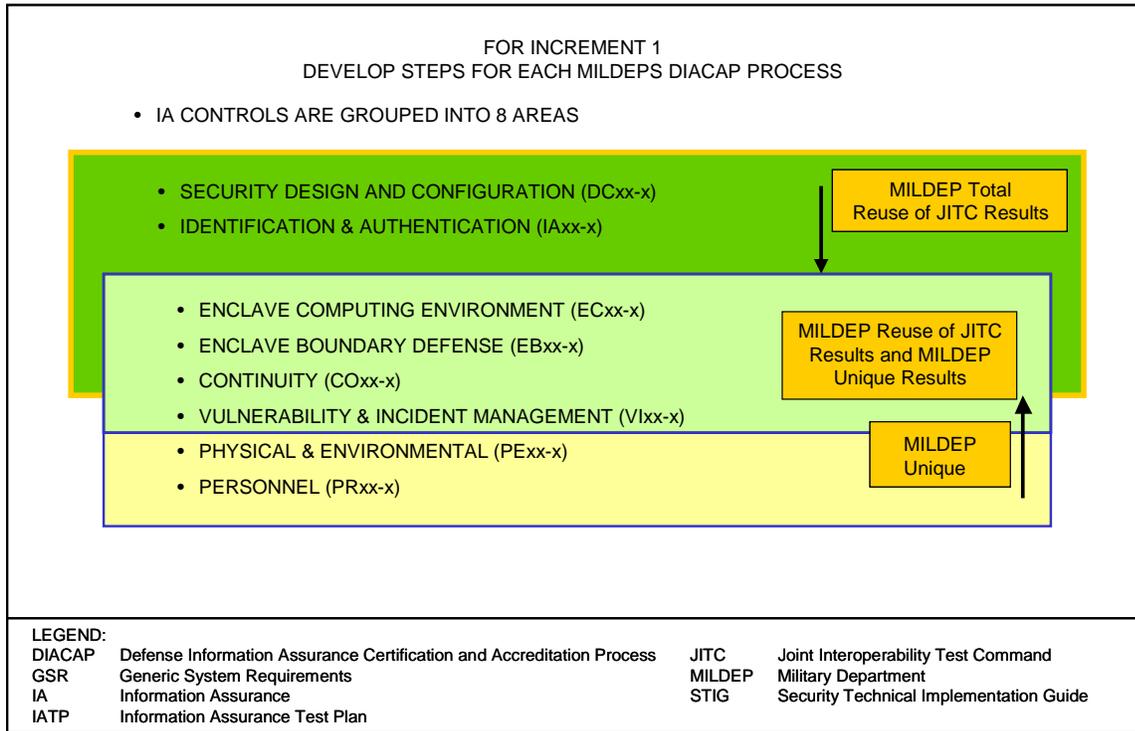


Figure 4-16. IA Controls Reuse Process

- Certification Approval Authorities (CAAs) (per MILDEP and agency): MILDEP/agency CAAs will leverage each other’s acquisitions and implementation of the IA controls for reuse and adoptions.
- JITC for IO and IA testing of all systems for the APL.

[Figure 4-17](#), IA Governance and DSAWG Relationship for VVoIP Deployment, illustrates the proposed relationship between DISN VVoIP Deployment IA Governance and the DISN Security Accreditation Working Group (DSAWG).

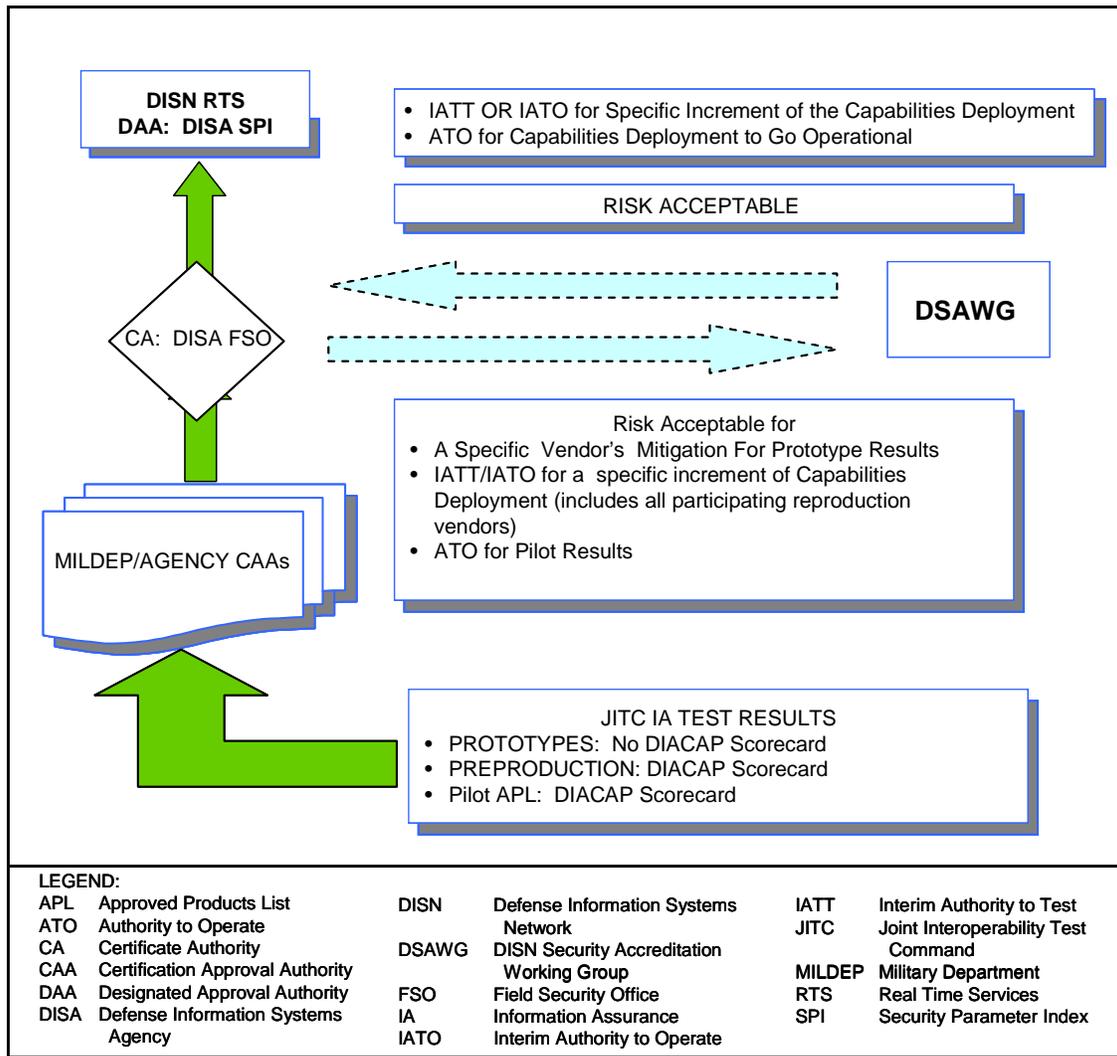


Figure 4-17. IA Governance and DSAWG Relationship for UC Deployment

4.3.3.2 Migration Time Frame – Fiscal Years 2012-2015

In the FY 2012-2015 time frame, the CC/S/As should begin to invest in the migration to Net Centricity using the products on the UC APL that were established during 2008 to 2011. This investment will begin with MFSS on a country-by-country basis in all four theaters. Edge systems will be purchased for force redeployments, BRAC sites, new buildings, and end of life circuit switches. Enclaves of E2E IP based UC services will be scattered around the globe. The network will begin hybrid operations on a global scale with few major sites. Spiral 2 will complete during this time frame and Spiral 3 will begin with a heavy focus on the full suite of UCs to finalize the FY 2012 Architecture and to validate the UCR 2010. New more powerful, robust, and cost-effective products will be on the UC APL for MILDEPs to acquire. FY2016 Architecture/System Design must begin, and the UCR 2014 must be completed in this time

frame driven by the updates to JS and ASD(NII)/DoD CIO policies and the need for network technologies for providing information assurance and real time situational awareness.

4.3.3.3 Migration Time Frame – Fiscal Years 2016-2020

In the FY 2016-2020 time frame, the CC/S/As should be well on the way to investing in the migration to Net Centricity using the products on the UC APL that were established during 2012-15. This investment will expand on a country-by-country basis in all four Theaters as circuit switching technologies become too expensive to sustain and the price of EIs drops. Entire countries of E2E IP based UC services will be established around the globe. The network operations will begin to be dominated by IP based services on a global scale with few circuit-switched sites. Spiral 3 will complete during this time frame and Spiral 4 will begin with a heavy focus on the full suite of UCs to finalize the FY 2016 Architecture and to validate the UCR 2014. FY 2020 Architecture/System Design must begin, and the UCR 2018 must be completed in this time frame driven by the updates to JS and ASD(NII)/DoD CIO policies and the need for network technologies for providing information assurance and real time situational awareness.

4.4 UNIFIED CAPABILITIES SYSTEM DESCRIPTION

This section provides a system-level overview of the E2E network designs that provide UC. The E2E IP system design is illustrated in [Figure 4-18](#), E2E IP System Description, that shows the major components of the design and the responsibilities. The edge is made up of the UC-approved products, which include the telephones, the video codecs, the ASLAN, the Local Session Controller, the Edge Boundary Controller, and the customer edge router. The edge is connected to the DISN SDNs and Transport via access circuits or via MILDEP intranets.

Currently, the SBU voice and ISDN video services subset of UC are provided by the existing TDM-based DSN and its components with VoIP assured LAN services provided to the telephone on ASLANs. The TDM-based services on the network backbone will migrate over a long period to IP-based assured services systems end-to-end over the MILDEP ASLANs, intranets, and the DISN Network infrastructure. During the migration time frame, SBU UC will be provided by a hybrid arrangement of both TDM- and IP-based systems. DRSN will remain based on circuit-switched technologies as the only technologies that can currently provide Multilevel Security. However, Classified VVoIP will migrate from the current VoSIP using the same system design as the SBU VVoIP with a few feature differences. In addition, the current DVS VTC services will be provided predominately by DSN ISDN TDM technologies with a few sites capable of video over IP for both SBU and Classified VTCs. Eventually SBU and Classified VTC services will migrate to the SBU IP system design. Since the Circuit Switched TDM based system is well established, the following subsections provide a UC system overview by first describing VVoIP subsystems followed by an overview of the TDM-based DSN design.

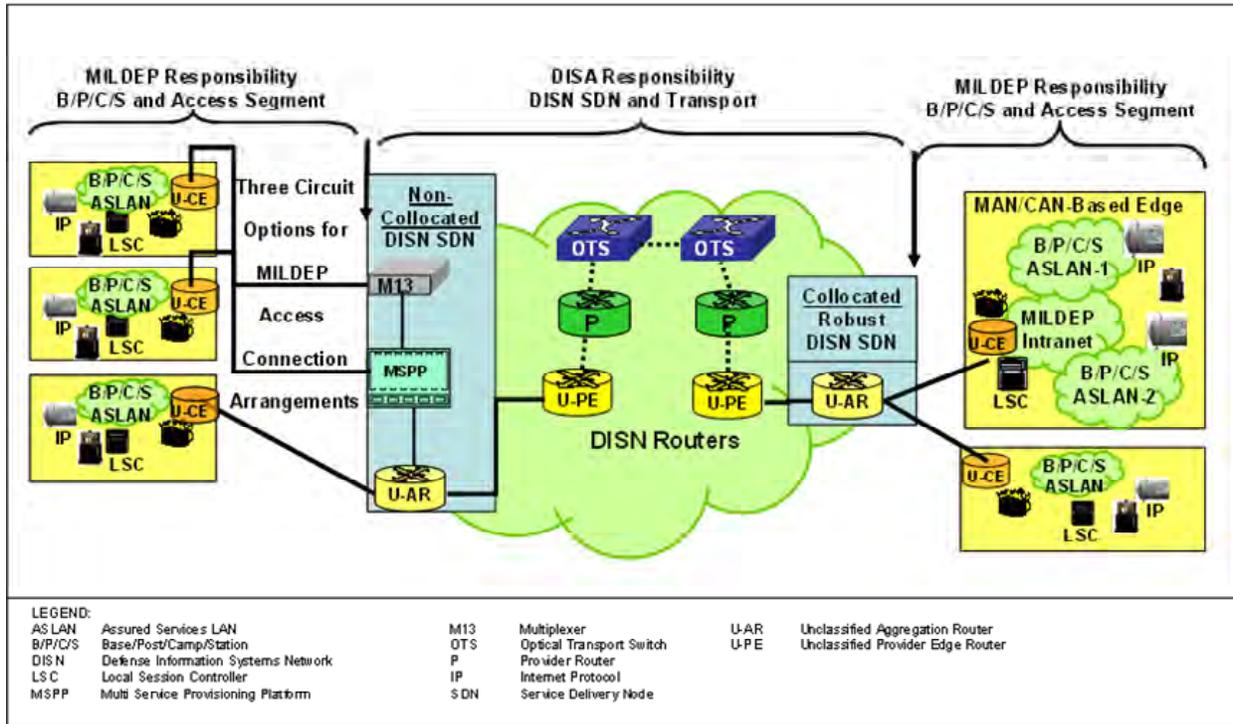


Figure 4-18. E2E IP System Description

The network segments comprising the hybrid TDM and IP-based end-to-end design are illustrated in [Figure 4-19](#), High-Level Hybrid Voice and Video Design Illustrating the Three Main Network Segments.

[Figure 4-19](#), High-Level Hybrid Voice and Video System Design Illustrating the Three Main Network Segments, shows the three major end-to-end network segments: Customer Edge, Network Edge, and the Network Core (DISN SDNs and WAN Transport) which are all part of the GIG end-to-end. End users attach to the Customer Edge Segment, consisting of either a TDM-based End Office, or the set of VVoIP components of LSC, EBC, Customer Edge (CE) Router, and ASLAN. The Network Edge and the DISN Network Infrastructure is either TDM or IP based on the technology of the Edge. Within the DISN MFSS the technology conversions necessary for the different technology edges to interoperate securely are performed.

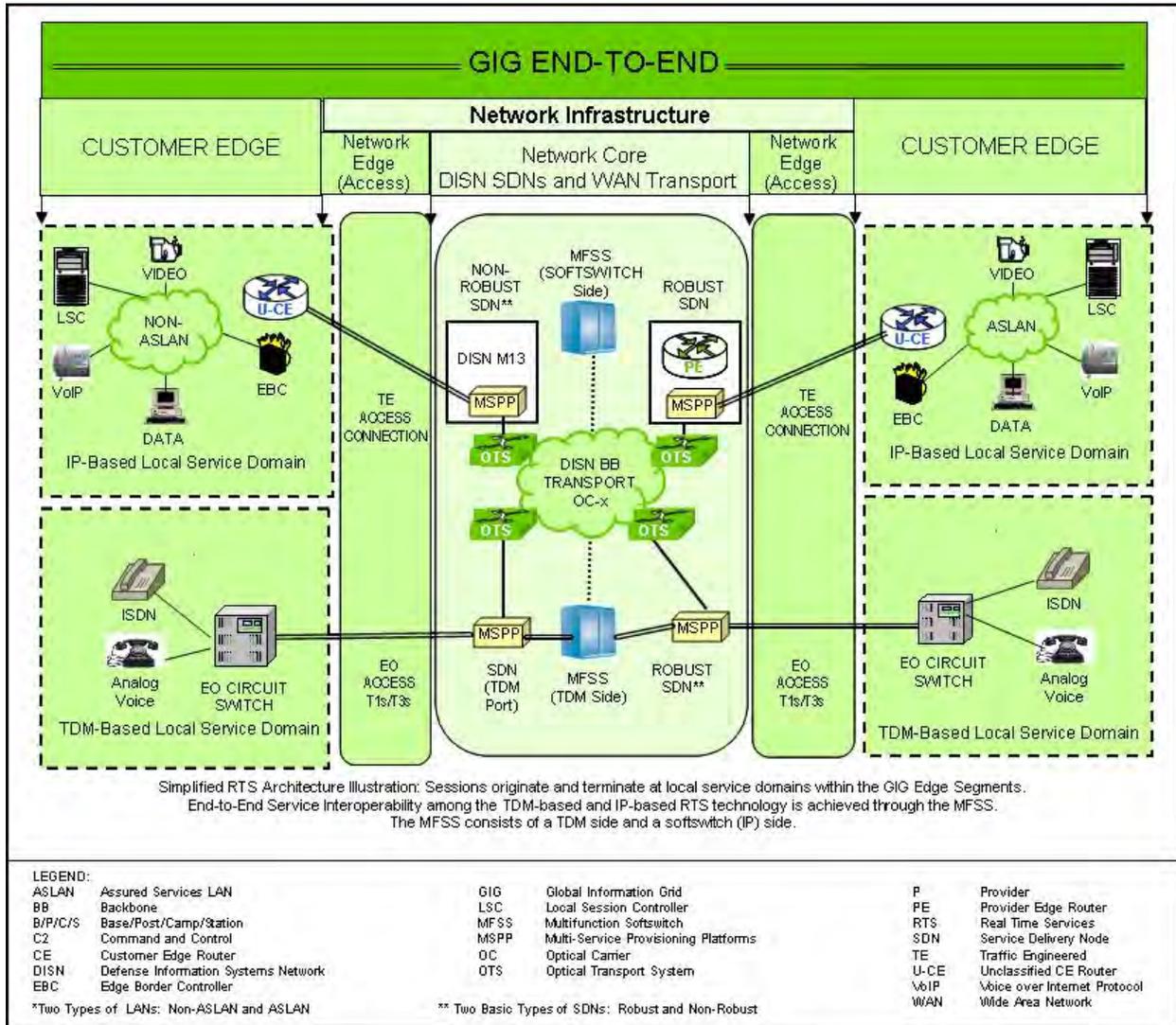


Figure 4-19. High-Level Hybrid Voice and Video System Design Illustrating the Three Main Network Segments

4.4.1 IP-Based Design for Unified Capabilities

This section provides a high-level overview of the FY 2008 VVoIP design within the context of the DoD network infrastructure. The focus of the description is on FY 2008. Because the details governing the complete VVoIP design and more specifically Assured Services are complex and consist of several components, individual sections are written within the UCR 2008 for each design component. The purpose of providing the high-level overview here is to give a consolidated view of the entire VVoIP as well as IM and Chat network infrastructures and services design.

There are two types of LANs: ASLAN and non-ASLAN. The mission of the subscriber (from both an origination and receiving role) determines which type of LAN to which they must attach.

The DISN consists of hundreds of worldwide Service Delivery Nodes (SDNs) interconnected by a highly robust, bandwidth-rich optical fiber cross-connected core with gigabit routers (i.e., the DISN Core). The customer is responsible for ensuring the aggregate access bandwidth on the Distribution Segment is sized to meet the busy hour traffic demand for each GIG service class and each of the four GIG traffic queues, plus a 25 percent (%) surge for voice and video traffic, plus a 10 percent (%) aggregate overhead for signaling, NM, and routing traffic.

Based on a site's C2 mission requirements, the site's access to the DISN WAN may be dual homed. The major aspects determining the dual-homing method required, i.e., the type of SDN that a user location shall connect to, the location of the U-CE Router in relation to the type of SDN, and the type of missions that the U-CE Router serves, are as follows:

- Types of SDN
 - Non-Robust – M13 multiplexer
 - Robust – Multi-Service Provisioning Platforms (MSPP) all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning)
 - Robust – MSPP and Unclassified Aggregation Router (AR)
- U-CE Router Location for the SDN
 - U-CE Router not at an SDN location
 - U-CE Router at a non-robust SDN location
 - U-CE Router at a robust SDN location
- Type of U-CE Router
 - Critical mission
 - Non-Critical Mission

As shown in [Figure 4-20](#), Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site, a non-critical mission U-CE Router may connect to the nearest SDN, while a critical mission U-CE Router must be dual homed to two separate robust types of SDNs. If a critical mission U-CE Router is located on the same base as an SDN, it still requires a second connection to another robust SDN.

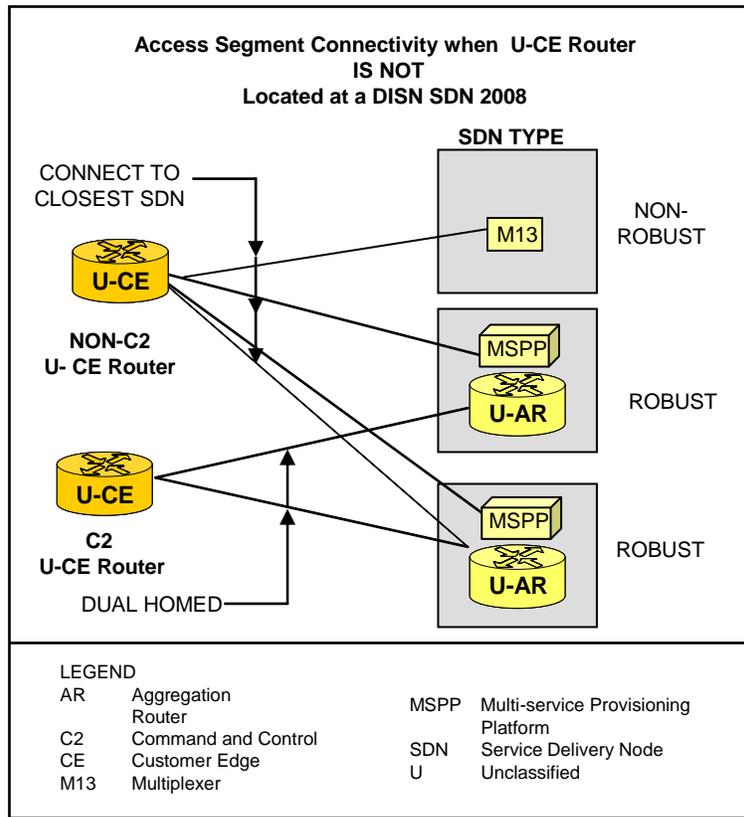


Figure 4-20. Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site

4.4.1.1 Overview of VVoIP 2008 System Design Attributes

The most important consideration for implementing the VVoIP technology insertion associated with the “VVoIP 2008 System Design” is not to degrade the capability to meet C2 voice, video and data services mission requirements. Preventing degradation begins with establishing a VVoIP 2008 System Design and requirements that meet currently defined policies and requirements. The requirements will be validated and updated via both assessment testing in DoD laboratories and via the UC Spiral testing on operational networks as described in [Section 4.3](#), Migration to Unified Capabilities.

Section 4 – Unified Capabilities Description and Key Processes

The logical location of the major VVoIP system attributes within the GIG End-to-End design for circa 2008 is shown in [Figure 4-21](#). The location of attributes in terms of the Customer Edge (B/P/C/S), the Network Edge, and the Network Core is depicted, and the differentiation between assured service and non-assured service is shown between the top half of the diagram and the bottom half of the diagram, respectively.

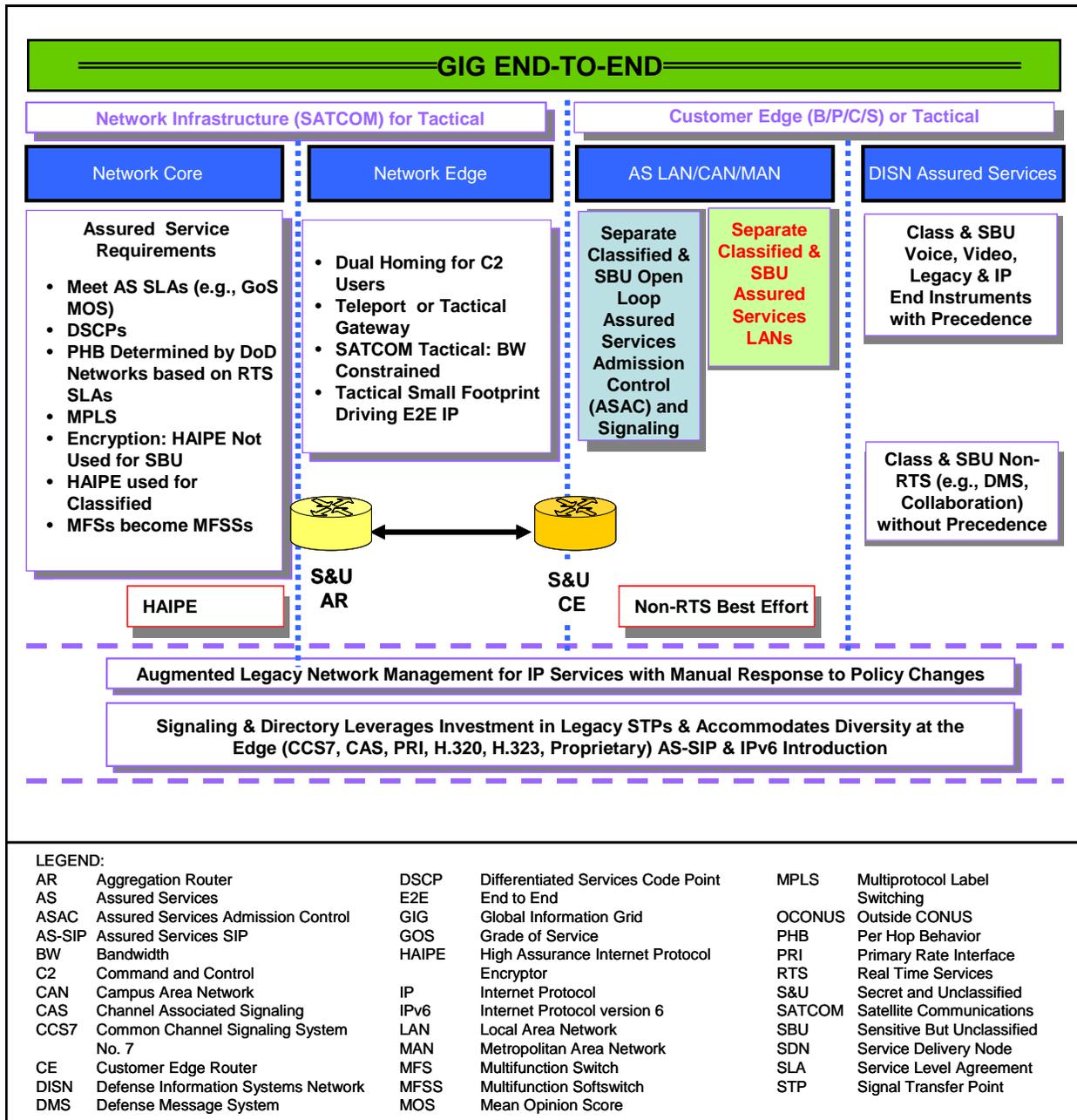


Figure 4-21. Overview of VVoIP System Attributes Circa 2008

The functions contained in the boxes located within the top half of [Figure 4-21](#), Overview of VVoIP System Attributes Circa 2008, constitute the scope of the Assured Services functions while the placement of the boxes indicates where in the overall design (WAN to Edge) the functions logically reside. Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while in FY 2008 only voice and video sessions are supported by Assured Services.

4.4.1.1.1 *Queuing Hierarchy for DISN IP Service Classes*

Section 5.3.3, Network Infrastructure E2E Performance Requirements, has defined four queues for the purposes of maintaining the required QoS for each UC Aggregate Class. Voice, signaling, and routing packets are placed in the Expedited Forwarding (EF) queue (a priority-forwarding queue). Video packets are placed in an Assured Forwarding (AF) fair weighted queue. Preferred data and NM packets are placed in a second AF fair weighted queue. All other packets (data and any other service) are placed in the best effort (default) queue. [Figure 4-22](#), Queuing for the Bearer Design Circa 2008, shows the queue structure and associated rules.

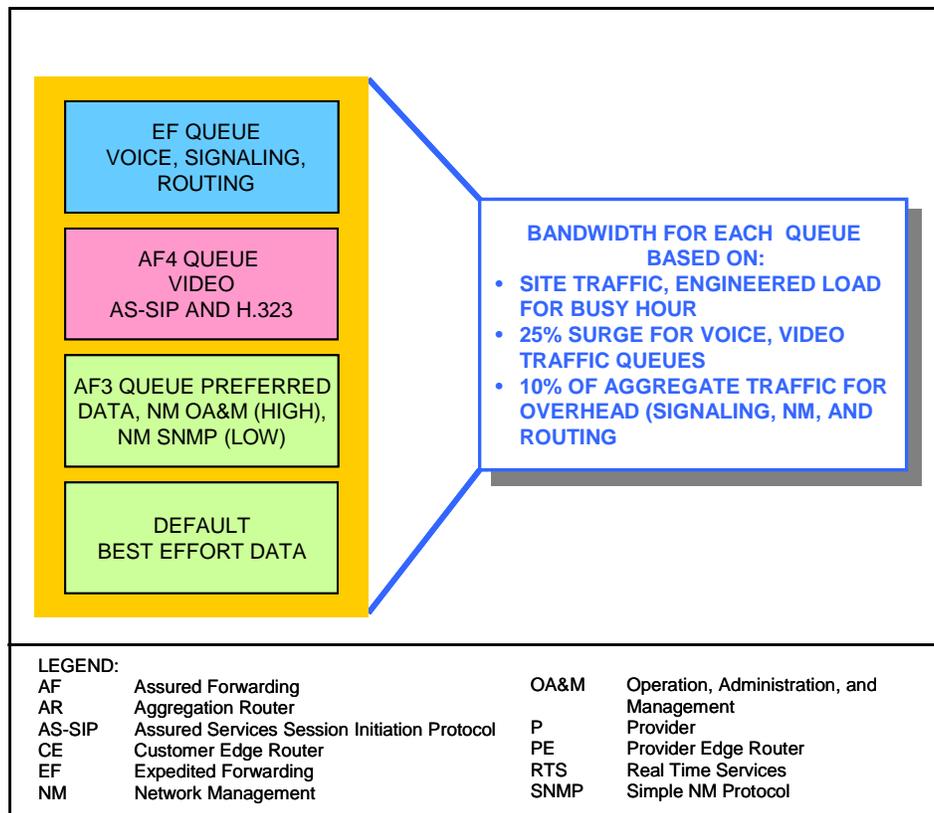


Figure 4-22. Queuing for the Bearer Design Circa 2008

The Assured Forwarding queues employ two separate drop probabilities.

The Assured Service Admission Control (ASAC) controlled video (both AS-SIP and H.323) and the non-ASAC controlled video (H.323 and Session Initiation Protocol (SIP)) will have the same drop probability. The higher drop probability in the AF4 queue may be used if necessary to differentiate various video or other AF4 queue assigned functions as defined locally.

In the second Assured Forwarding-3 (AF3) queue, NM and Simple Network Management Protocol (SNMP) packets will have the lower drop probability while Operation, Administration, and Management (OA&M) packets will have the higher drop probability.

The bandwidth for each queue must be provided based on a sound traffic engineering analysis, which includes the site budget settings, the site busy hour traffic load plus a 25 percent (%) surge for voice and video traffic, plus a 10 percent (%) aggregate overhead for signaling, NM, and routing traffic.

4.4.1.1.2 Customer Edge Segment Design

The Customer Edge Segment has the following attributes:

1. Non-Blocking ASLAN. At the Customer Edge, the 2008 design has an ASLAN that is designed as non-blocking for voice and video traffic.
2. Traffic Admission Control. The LSCs on a B/P/C/S employ an Open Loop ASAC technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit consistent with maintaining a voice quality, as described in UCR 2008, Section 5.3.3.15, Voice Service Quality.
3. Call Preemption. Lower precedence sessions will be preempted on the access circuit in order to accept the LSC setup of a higher precedence level outgoing or incoming session establishment request.
4. Traffic Service Classification and Priority Queues. In terms of the CE Router queuing structure, traffic will be assigned to the higher priority queues by an aggregated service class as described in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

4.4.1.1.2.1 Base/Post/Camp/Station VVoIP Design

The military B/P/C/S level design consists of an LSC complex that may consist of a redundant LSC, or several LSCs in a cluster arrangement, in a LAN, campus area network (CAN), metropolitan area network (MAN) structure. The LAN/CAN/MAN design may be tailored to a

single building or an entire base structure with varying degrees of robustness tailored to individual building mission requirements. Off-base connectivity to the long-haul DISN network infrastructure is provided through the EBC function. Interface to the local commercial telephone network is provided through a media gateway function within an LSC per local interface requirements. It is a MILDEP responsibility to design and fund the base infrastructure design.

4.4.1.1.2.2 Local Session Controller Designs – Voice

An LSC is a call stateful Voice, Video, and Signaling Server product at the B/P/C/S that directly serves IP EIs. The LSCs are the cornerstone of all DoD VVoIP signaling functions. The functions provided by the LSC are also found in the multifunction softswitch (MFSS). The LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC employs AS-SIP signaling. If the LSC interfaces to the PSTN or to legacy B/P/C/S TDM systems, it must also support Primary Rate Interface (PRI) using its Media Gateway (MG) and Media Gateway Controller (MGC). If the LSC supports C2 users, it provides precedence and preemption functions, such as supporting MLPP features of CAS and PRI and ASAC for IP.

[Figure 4-23](#), B/P/C/S Level LSC Voice Designs, shows examples of three possible configurations for connecting multiple LSCs on a B/P/C/S to the DISN WAN and the MFSS. The U-CE Routers are dual homed which is not shown for simplicity. At the top of the figure, the first case is shown where multiple LANs, each with its own LSC and U-CE Router, connecting via separate access circuits to the DISN WAN. Each LSC would have its own traffic engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from one LSC on the base to another LSC on the base must traverse the DISN WAN and use the MFSS to connect to another LSC. Should base connection to the DISN WAN or the MFSS be lost, then sessions from one base LSC to another on-base LSC could not be established. In addition, if one of the LSCs was not using all its traffic engineered bandwidth (Budget A), a second LSC (Budget B) could not use the unused bandwidth of the other LSC (Budget A).

The second case, shown in the middle of the diagram, allows sessions to be established through the U-CE Router when connection to the DISN WAN is lost. Naturally the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic engineered bandwidth for each individual LSC (i.e., $B = B_1 + B_2$). Again, if one LSC is not using all of its budget/bandwidth, the other LSC cannot use the unused budget/bandwidth. For one LSC to establish a session to the other LSC, without access to the MFSS, then each LSC must contain the directory information of all LSCs on the base.

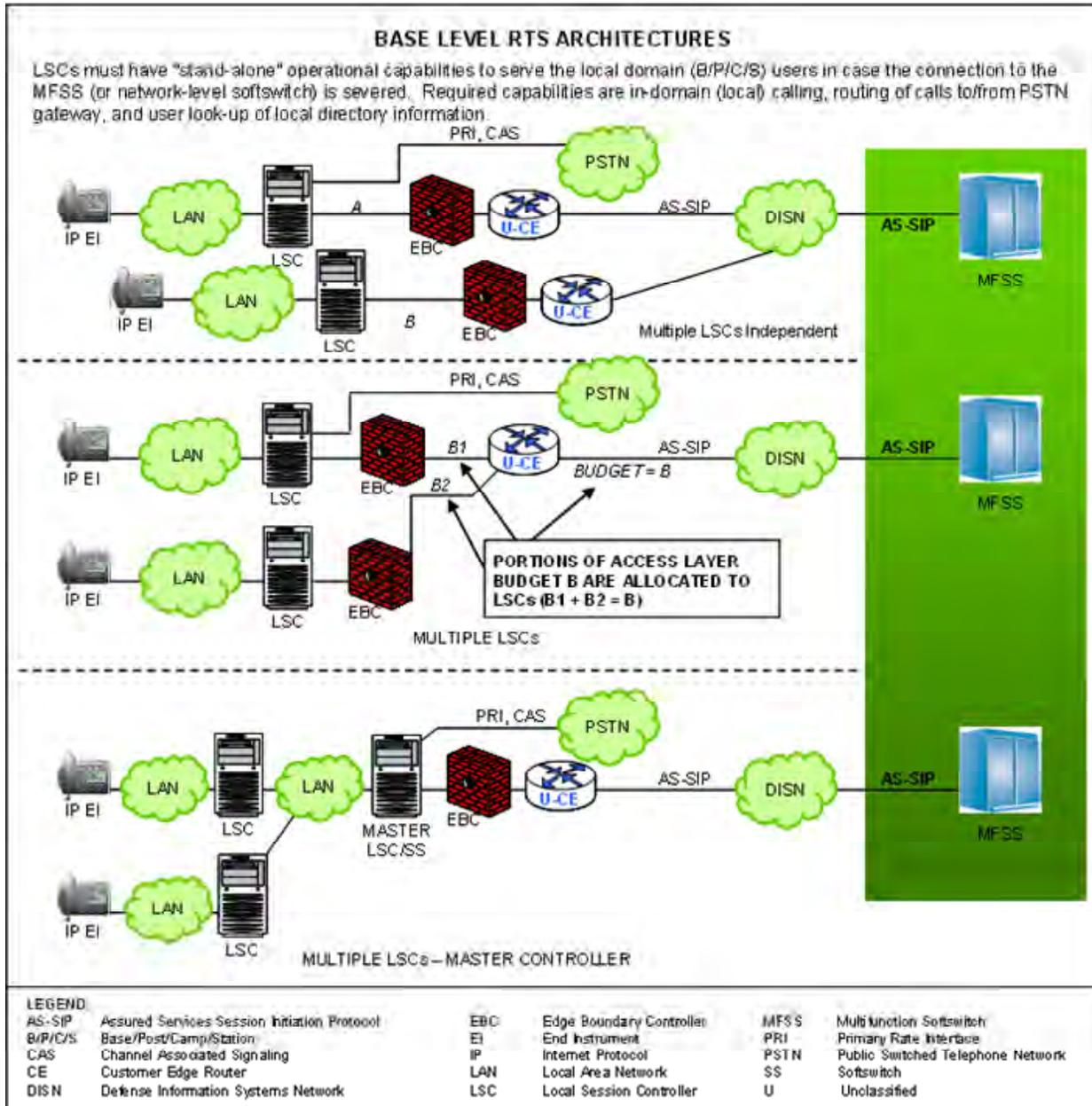


Figure 4-23. B/P/C/S-Level Voice over IP LSC Designs

The third case, shown in the lower part of the figure, solves these limitations of being able to use all the WAN access circuit bandwidth, and the establishment of on-base sessions without the need for DISN WAN connection or access to an MFSS.

The third case requires the design and implementation of an LSC cluster concept where a master LSC, as shown in the figure, has a master directory of all users on the base. Under this arrangement, service order activity at one LSC will be reflected automatically at all LSCs in the

cluster, including the master LSC. *Only the first case will be specified in detail in the UCR 2008.* The other two cases will require custom engineering of the base design (including the use of the LSC portion of an MFSS where an MFSS is located on a base) to ensure interoperability and acceptable performance between the various on-base LSC arrangements and vendors.

Some general rules to follow with respect to a master LSC and subtended LSCs are as follows:

1. End instruments served by a master LSC are treated like EIs served by subtended LSCs.
2. The master LSC adjudicates the enclave budget between the subtended LSCs.
3. Either of two methods is acceptable
 - a. Method 1 – master always ensures the highest priority sessions are served (up to the budget limit of the access link) regardless of the originating subtended LSC, for example,
 - (1) If the ASAC budget is 28.
 - (2) Each subtended LSC (three (3) total) allowed ten (10) voice sessions (ten (10) budgets).
 - (3) Master LSC performs preemptions to ensure higher precedence sessions succeed.
 - (4) Master LSC blocks Routine sessions from any LSC once access link budget is met.
 - b. Method 2 – master maintains a strict budget for subtended LSCs, for example,
 - (1) If the ASAC budget is 30.
 - (2) Each subtended LSC (three (3) total) with each allowed ten (10) sessions.
 - (3) Does not use unfilled LSC budget to service above Routine precedence sessions from another subtended LSC.
4. All LSCs directly connect to the E2E Element Management System at either a DISA Network Operations Centers (NOC) as part of the DISN OSS that supports the JTF GNO or at a MILDEP NOC that supports the JTF GNO.

5. The Master LSC is not required to provide an aggregated NM view of the subtended LSCs.
6. Master LSCs and subtended LSCs communicate using AS-SIP
 - a. All signaling destined external to the enclave passes through the master LSC.
 - b. Allows multiple vendors within the enclave.
7. Each LSC maintains two budget counts as follows:
 - a. Intra-enclave (based on local traffic engineering and not associated with access link budget).
 - b. Inter-enclave (ASAC controlled by each LSC).
8. It is desired that connections to the PSTN only be through the master LSC (simplifies location services).
9. When a subtended LSC directly connects to the PSTN (exception situation, not desired), then only EIs of the subtended LSC can originate and receive calls from that PSTN PRI/CAS trunk.
10. The Master LSC is the only connection to enclave TDM infrastructure (simplifies location services).

The choice of the B/P/C/S LSC configurations is dependent on the size of the B/P/C/S. Very small bases will only have one LSC so these configurations are not of concern. Larger B/P/C/Ss are most likely to have multiple Circuit Switches to replace, and might try to set up the LSC connections like their circuit switches which would lead to the undesirable configurations that don't employ Master LSCs. Only the Master configuration is recommended.

4.4.1.1.2.3 Local Session Controller Designs – Video

[Figure 4-24](#), B/P/C/S Video over IP LSC Designs, illustrates the LSC designs for video services. An LSC is a call stateful AS-SIP signaling appliance at the B/P/C/S that directly serves IP video-capable EIs. The video LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC employs AS-SIP signaling. A Gatekeeper is an appliance that processes calls to the WAN using H.323 or SIP signaling. If the LSC or Gatekeeper interfaces to the PSTN or to legacy B/P/C/S TDM appliances, it must also support PRI and CAS using its MG and MGC. If the LSC supports C2 users, it provides precedence and preemption functions, such as supporting MLPP features of CAS (conditional for LSC) and PRI and ASAC for IP.

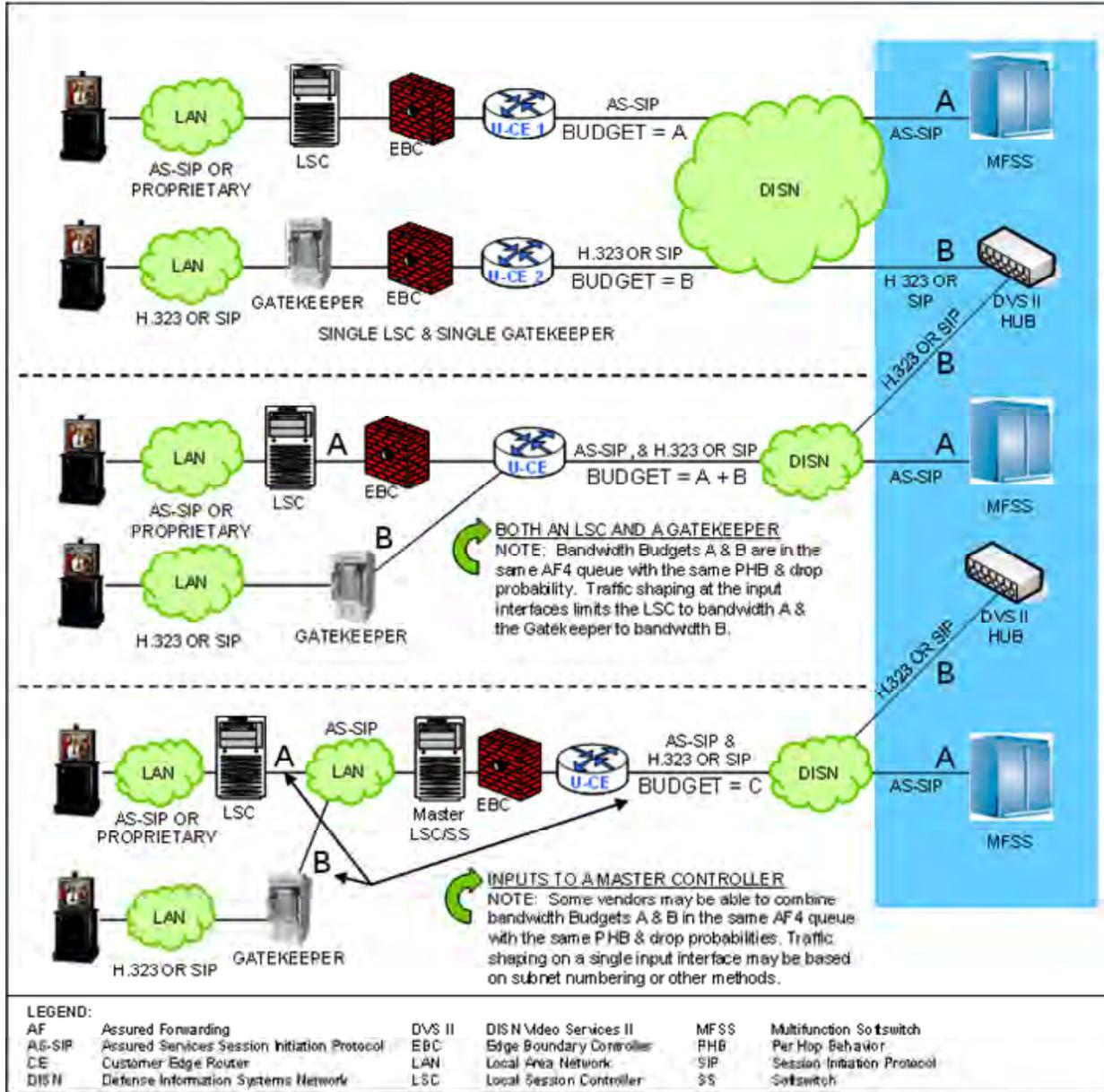


Figure 4-24. B/P/C/S Video over IP LSC Designs

Figure 4-24, B/P/C/S Video over IP LSC Designs, shows examples of three possible configurations for connecting multiple video-capable LSCs and Gatekeepers on a B/P/C/S to the DISN WAN and the MFSS.

The first case is, shown at the top of the figure, where multiple LANs, one with its own LSC and U-CE Router, and another LAN with a Gatekeeper and U-CE Router that connect via separate access circuits to the DISN WAN. The LSC and the Gatekeeper would each have its own traffic engineered access circuit bandwidth, which can support the predetermined number of sessions

(called a Budget in the figure). The limitation of this first case is that sessions from the LSC or Gatekeeper on the base will not be able to communicate with each other because of the different signaling protocols in use by each. However, the LSC and the Gatekeeper each will have separate bandwidths that act independently to each other.

The second case, shown in the middle of the figure, allows sessions to be established through the U-CE Router. In this case, both the LSC and the Gatekeeper will act independently as described in the first case, but both will connect to the same U-CE Router. However, the LSC video call and the Gatekeeper video call will connect to separate ports on the U-CE Router. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic-engineered bandwidth for each individual LSC (i.e., $B1 + B2$). Although each router port processing video calls acts independently in the AF4 queue, both customer calls must be treated equally when configured according to DoD policy.

The third case requires the designation and implementation of an LSC cluster concept as described for the voice design in the previous section.

With regard to the Gatekeeper interworking with the master LSC or Softswitch (SS) in the third case, some vendors may be able to manage the LSC-originated video call in addition to the Gatekeeper-originated call. In this case, the master LSC/SS will manage Budgets A and B to make a more efficient use of Budget C. Although the LSC video EI and the Gatekeeper EI will still not be able to communicate with each other because of different protocols utilized, the master LSC/SS will be able to process the calls into Budget C efficiently in the AF4 queue. All video calls leaving the master LSC/SS must be treated equally to comply with DoD Policy.

4.4.1.1.2.4 LAN and ASLAN Design 2008

Requirements for the B/P/C/S LAN designs are defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network. The principal LAN requirements are summarized in [Figure 4-25](#), ASLAN Requirements Summary.

 <p>DISN ASLAN GSR/UCTP/IATP</p>	<p>REQUIREMENTS</p> <ul style="list-style-type: none"> • MEET C2 SLAs (e.g., GOS OF NON-BLOCKING, MOS) • SERVICE CLASSES & PRECEDENCE MAPPED INTO DSCPs • QOS BY OVER-PROVISIONING/DSCPs • PACKET LOSS, JITTER, LATENCY • COMMERCIAL, MEDIUM, AND HIGH AVAILABILITY/POWER • VLAN FOR VOICE, VIDEO, DATA PERIPHERALS • NETWORK MANAGEMENT OF LAN 																								
<p>LEGEND</p> <table border="0"> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>IATP</td> <td>Information Assurance Test Plan</td> </tr> <tr> <td>C2</td> <td>Command and Control</td> <td>LAN</td> <td>Local Area Network</td> </tr> <tr> <td>DISN</td> <td>Defense Information Systems Network</td> <td>MOS</td> <td>Mean Opinion Score</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point</td> <td>SLA</td> <td>Service Level Agreement</td> </tr> <tr> <td>GOS</td> <td>Grade of Service</td> <td>UCTP</td> <td>Unified Capability Test Plan</td> </tr> <tr> <td>GSR</td> <td>Generic System Requirements</td> <td>VLAN</td> <td>Virtual Local Area Network</td> </tr> </table>		ASLAN	Assured Services Local Area Network	IATP	Information Assurance Test Plan	C2	Command and Control	LAN	Local Area Network	DISN	Defense Information Systems Network	MOS	Mean Opinion Score	DSCP	Differentiated Services Code Point	SLA	Service Level Agreement	GOS	Grade of Service	UCTP	Unified Capability Test Plan	GSR	Generic System Requirements	VLAN	Virtual Local Area Network
ASLAN	Assured Services Local Area Network	IATP	Information Assurance Test Plan																						
C2	Command and Control	LAN	Local Area Network																						
DISN	Defense Information Systems Network	MOS	Mean Opinion Score																						
DSCP	Differentiated Services Code Point	SLA	Service Level Agreement																						
GOS	Grade of Service	UCTP	Unified Capability Test Plan																						
GSR	Generic System Requirements	VLAN	Virtual Local Area Network																						

Figure 4-25. ASLAN Requirements Summary

There are two types of LANs, ASLAN and non-ASLAN, depending on the type of missions and users served by a LAN. The two LAN types and three categories along with user classes are illustrated in [Figure 4-26](#), Three Categories of LANs.

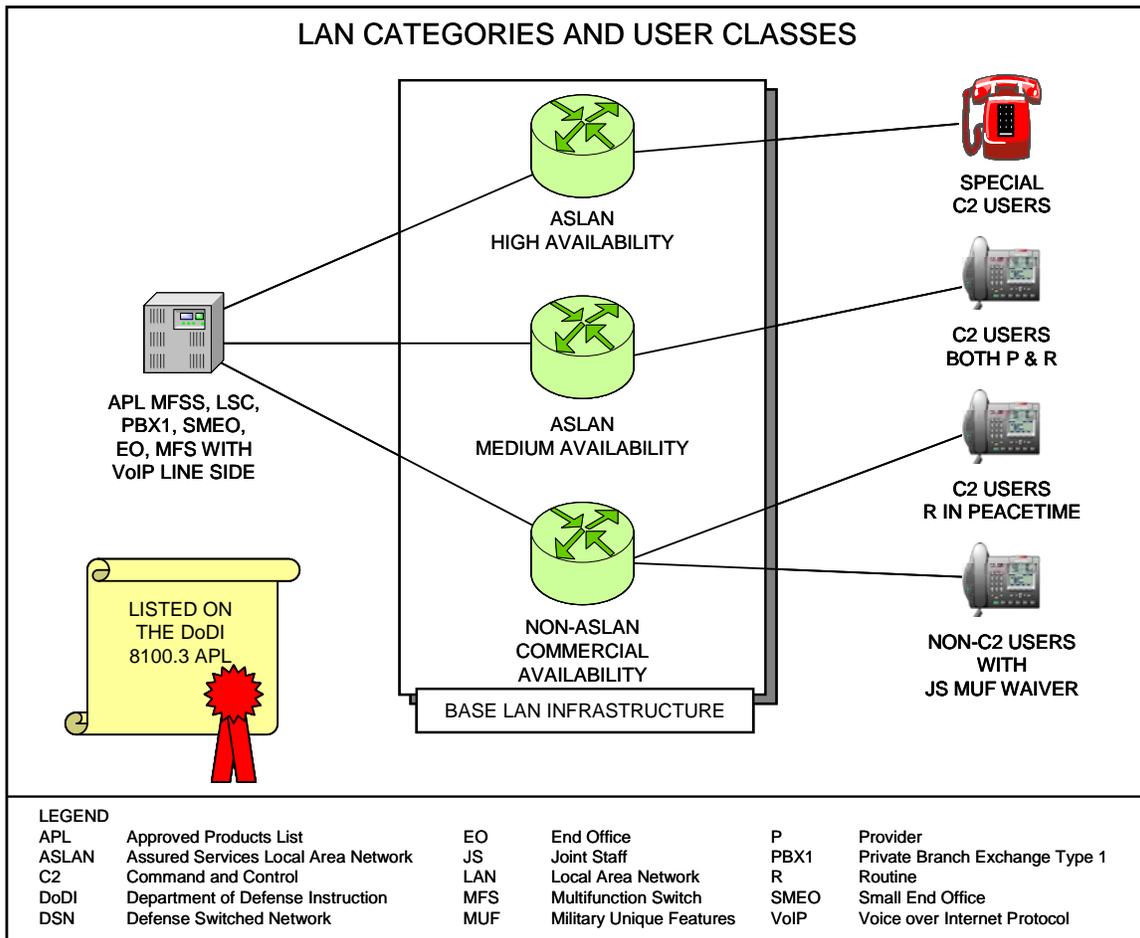


Figure 4-26. Three Categories of LANs

[Table 4-2](#), LAN Requirements Summary, shows the requirements needed based on subscriber mission category. *Requirements* are defined as necessary for the user while *Permitted* allows other user types to be served (such as a Special C2 user is Required to be served on a high availability ASLAN, and C2 and non-C2 users are Permitted on the same LAN). *Not Permitted* means that the user must not be served (such as a Special C2 user cannot be served by a medium availability or non-ASLAN). *Not Required* are requirements that do not have to be met for some users (such as requirements for diversity, redundancy, and power backup that are not required for C2(R) and non-C2 users).

The LAN has two configurations when it supports C2 or Special C2 users. An ASLAN that supports C2 users is classified as a Medium Availability ASLAN. An ASLAN that supports Special C2 users is classified as a High Availability ASLAN.

Table 4-2. LAN Requirements Summary

LAN REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	SPECIAL C2	C2	C2(R)	NON-C2
ASLAN High	R	P	P	P
ASLAN Medium	NP	R	P	P
Non-ASLAN	NP	NP	P	P
ASF	R	R	R	N
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
GOS p=	0.0	0.0	0.0	x.x
Availability	99.999	99.997	99.9	99.9
LEGEND				
ASF	Assured Services Features	NP	Not Permitted	
ASLAN	Assured Services LAN	NR	Not Required	
C2	Command and Control	P	Permitted	
GOS	Grade of Service	R	Required	
LAN	Local Area Network			

The actual LAN implementation will vary from base to base depending on building/facility locations, installed cable plant, and the location and type of missions being performed on the base. [Figure 4-27](#), An Example of a Potential CAN, is an example of one potential ASLAN implementation. It shows a CAN involving multiple buildings and types of mission users and how connectivity redundancy and backup power time requirement of 8, 2, or 0 hours are met in a cost-effective manner.

4.4.1.1.3 Network Infrastructure End-to-End Performance (DoD Intranets and DISN Service Delivery Nodes)

In 2008, DoD Intranets and the DISN SDNs serving SBU VVoIP traffic do not use High Assurance Internet Protocol Encryptors (HAIPES). The DISN SDNs are assumed to be bandwidth rich and robust. Since the ASLAN is required to be implemented as nonblocking for voice and video traffic, it has no bandwidth limit either. The access circuit, which can include a SATCOM link from the Edge to the DISN Core SDN, is the only potential bandwidth-limited resource due to funding, crisis traffic surges or damage. Therefore, the system design includes the use of ASAC to prevent session overload and subsequent voice and video performance degradation from the Customer Edge and to ensure that bandwidth is assigned to sessions based on precedence. The DISN WAN provides high availability (99.96 percent or greater) using dual-homed access circuits and the Multiprotocol Label Switching (MPLS) Fast Failure Recovery (FFR) in the Core.

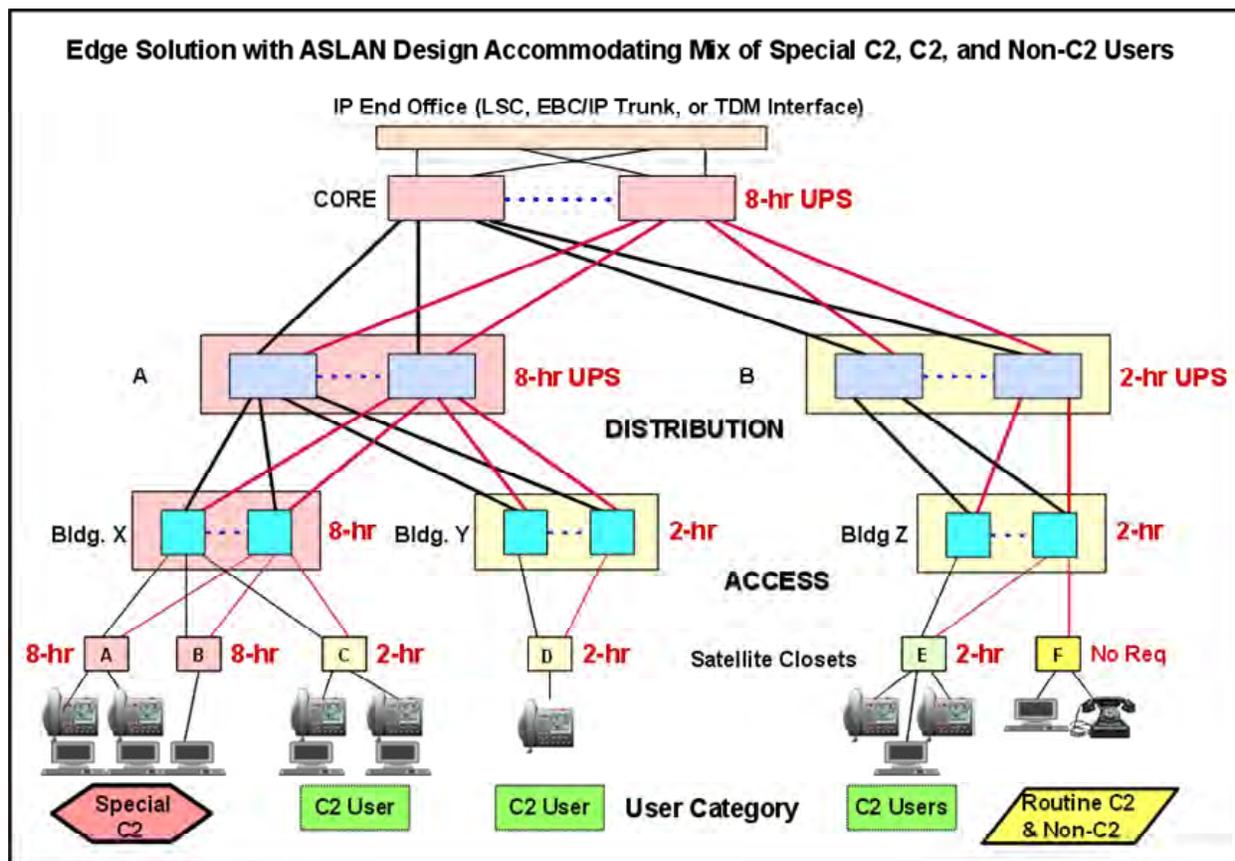


Figure 4-27. An Example of a Potential CAN

In order to ensure end-to-end voice and video services performance, a Service Level Agreement (SLA) must be established for the MILDEP Intranets and DISN SDNs, which are supporting IP-based voice, video, and data services. The SLA for voice and video is based on required Latency, Packet Loss, Jitter, and Availability, which is allocated to the MILDEP ASLANs and their associated customer edge router and EIs, to the MILDEP Intranets (called Metropolitan Area Networks (MAN) and Campus Area Networks (CAN)) and to the DISN SDNs. There are many techniques, such as MPLS, MPLS-TE, Queuing, mesh routing, and redundancy, which can be used by the networks to meet the SLAs. Currently, only the voice and video SLAs have been defined. Data application SLAs will be addressed in the future. In addition, the performance metrics for voice only (E-Model R-Factor) have been defined. The performance metric for video is under development. Measurement techniques for validating that the SLAs have been met and for isolating the portion of the end-to-end network, that is not meeting the SLA are also in development. [Figure 4-28](#), Measurement Points for Network Segments, illustrates the components of the end-to-end network where measurements will be made to ascertain compliance with the SLAs. The specific end-to-end network performance requirements are described in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

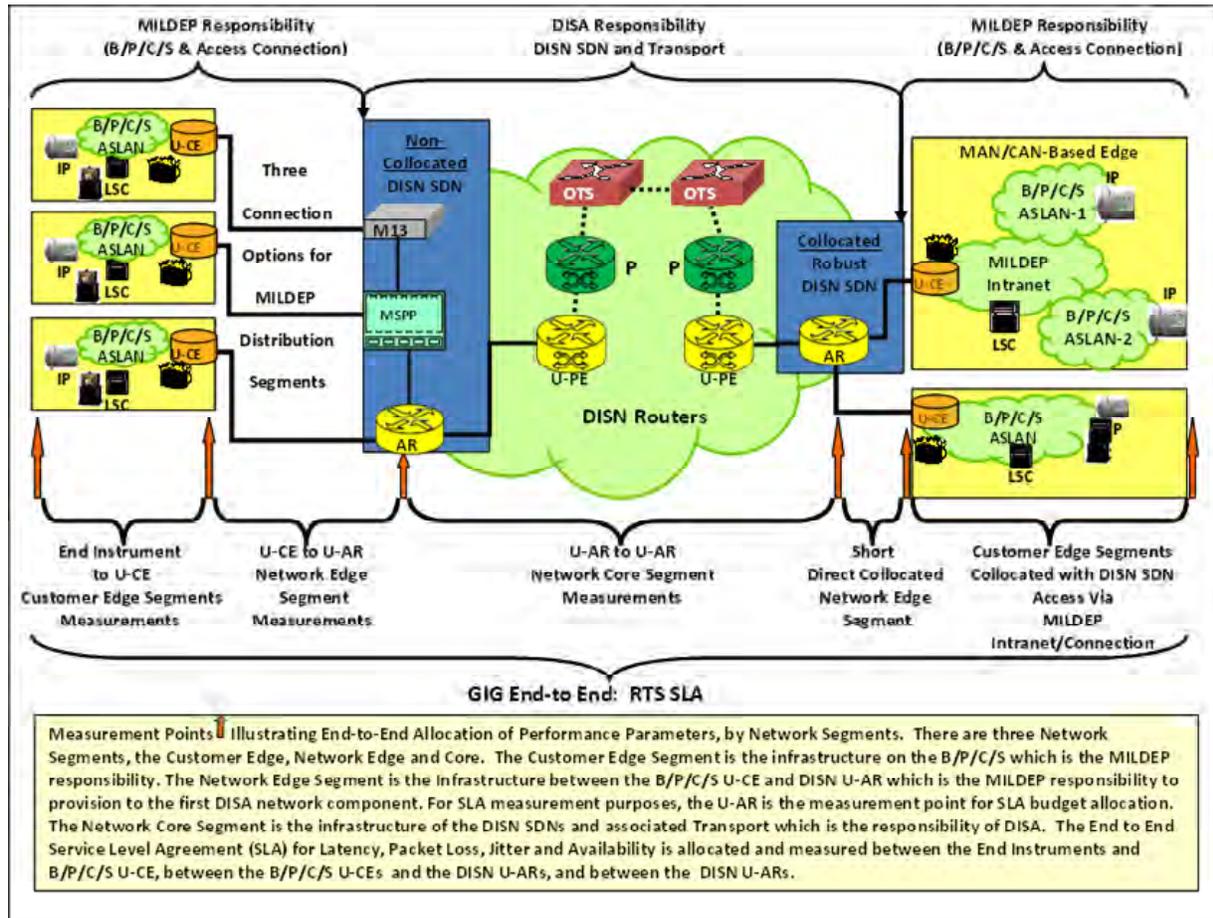


Figure 4-28. Measurement Points for Network Segments

4.4.1.1.4 End-to-End Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions and protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes. The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and Resource Reservation Protocol (RSVP). The bearer plane is associated with the bearer traffic and protocols, such as Secure Real-Time Transport Protocol (SRTP) and Real Time Control Protocol (RTCP). The NM plane is associated with NM protocols and is used to transfer status and configuration information between a NM system (NMS) and a network appliance. Network management protocols include the SNMP, Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

4.4.1.1.5 ASAC System Component 2008

The ASAC technique is the key VVoIP design component ensuring that end-to-end SLAs (grade of service voice quality, user assured service delivery, and call preemption to the EI) are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements end to end.

Figure 4-29, Assured Services System Functions, represents the first step in specifying the DISN assured services features by depicting a more detailed functional breakdown of the system components for 2008 than that shown in Figure 4-21, Overview of VVoIP System Attributes Circa 2008.

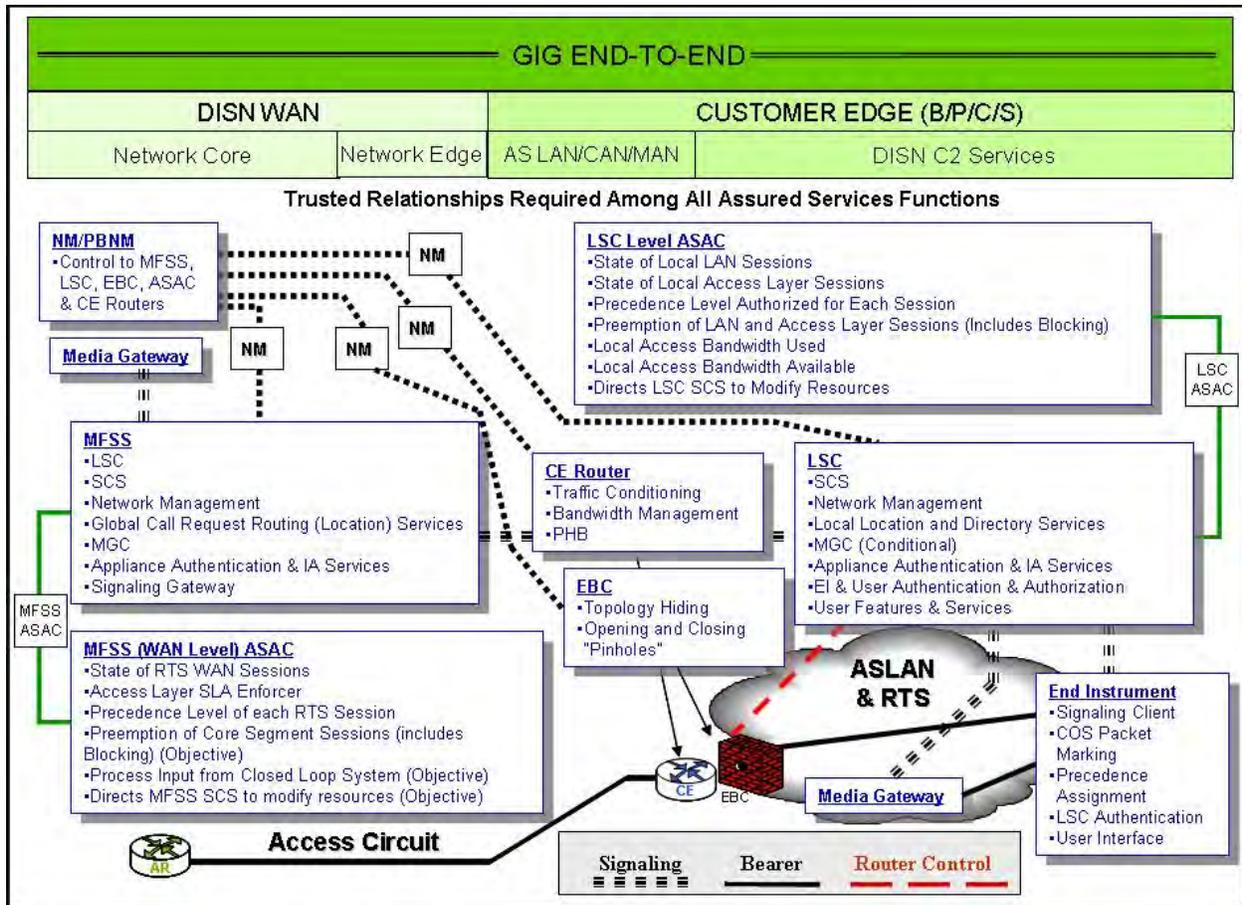


Figure 4-29. Assured Services System Functions

Detailed requirements for each of the functions contained in the boxes, the EBC, and the other components of the assured services features are contained within UCR 2008, Section 5.3.2, Assured Services Features Requirements.

The Open Loop ASAC design, depicted in [Figure 4-30](#), Open Loop ASAC System Design, is specified for 2008 as the method for achieving assured service end to end. The ASLAN connects via a local access circuit to a backbone network that consists of a Core MPLS-capable network.

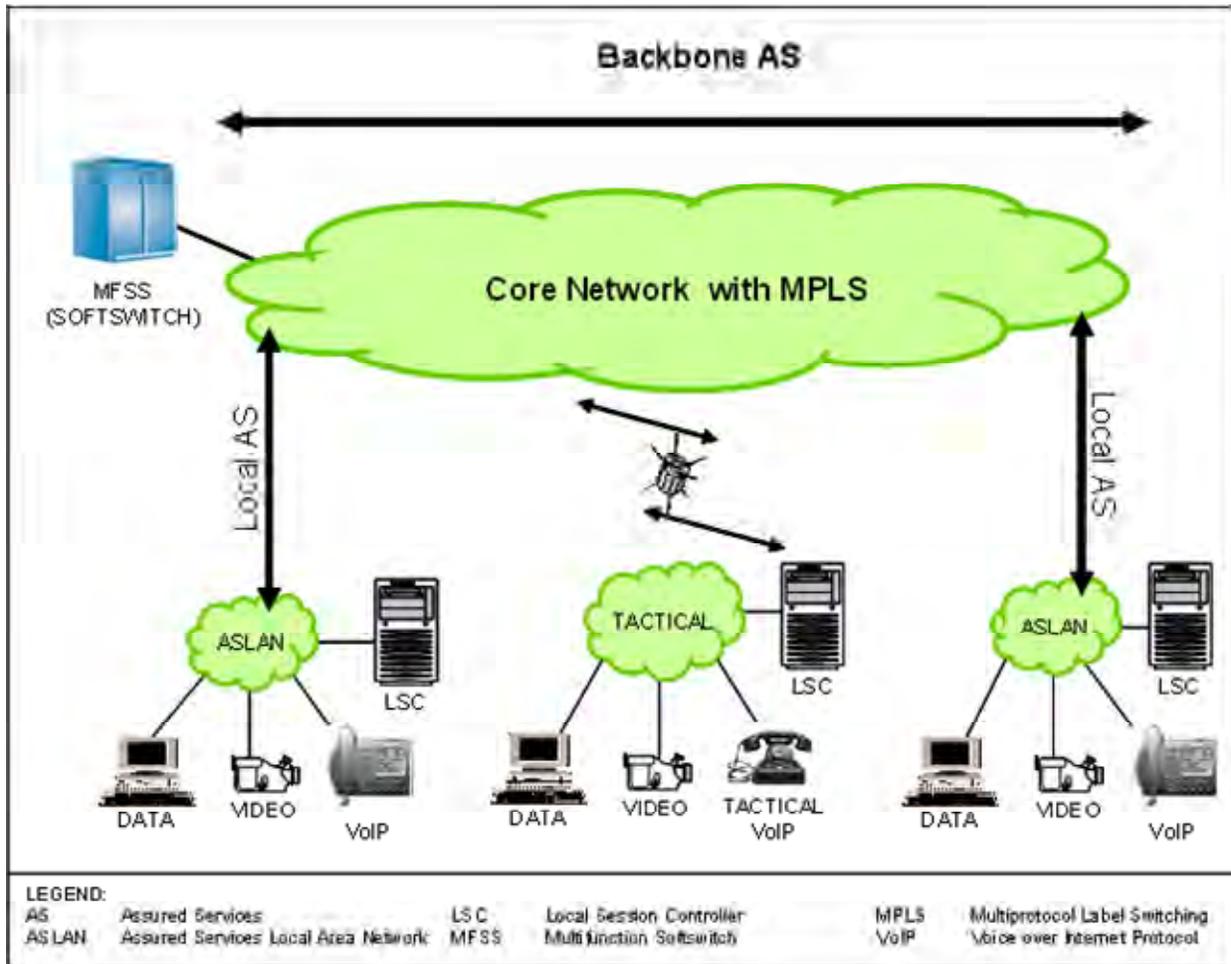


Figure 4-30. Open Loop ASAC System Design

The local assured service domain consists of an EI, ASLAN, LSC, and access circuit. Both the local assured service domains and the backbone assured service domains are realized with functionality in the signaling plane and the bearer plane to initiate and sustain a voice and video session.

NOTE: Tactical VoIP systems may connect via compressed satellite circuits to the DISN backbone and operate in a similar manner to strategic systems on an ASLAN.

The components of the 2008 Open Loop ASAC method are shown in [Figure 4-31](#), Open Loop ASAC for SBU Voice and Video for 2008. In the access circuit and the ASLAN, AS-SIP signaling (see UCR 2008, Section 5.3.4, AS-SIP General System Specification) is used by the LSC and MFSS to establish or preempt voice and video sessions based on precedence and engineered traffic levels on the access circuits (both origination and destination ends). In the bearer plane, the QoS/DSCP manages router per-hop behavior (PHB) based on the type of service class. Both the ASLAN and the backbone are assumed to be traffic engineered to be nonblocking for voice and video traffic. In the DISN Core, the DISN SLAs will support voice and video with assured service provided by QoS/DSCP, traffic engineering, and MPLS. Traffic with no marking will be treated as “Best Effort.”

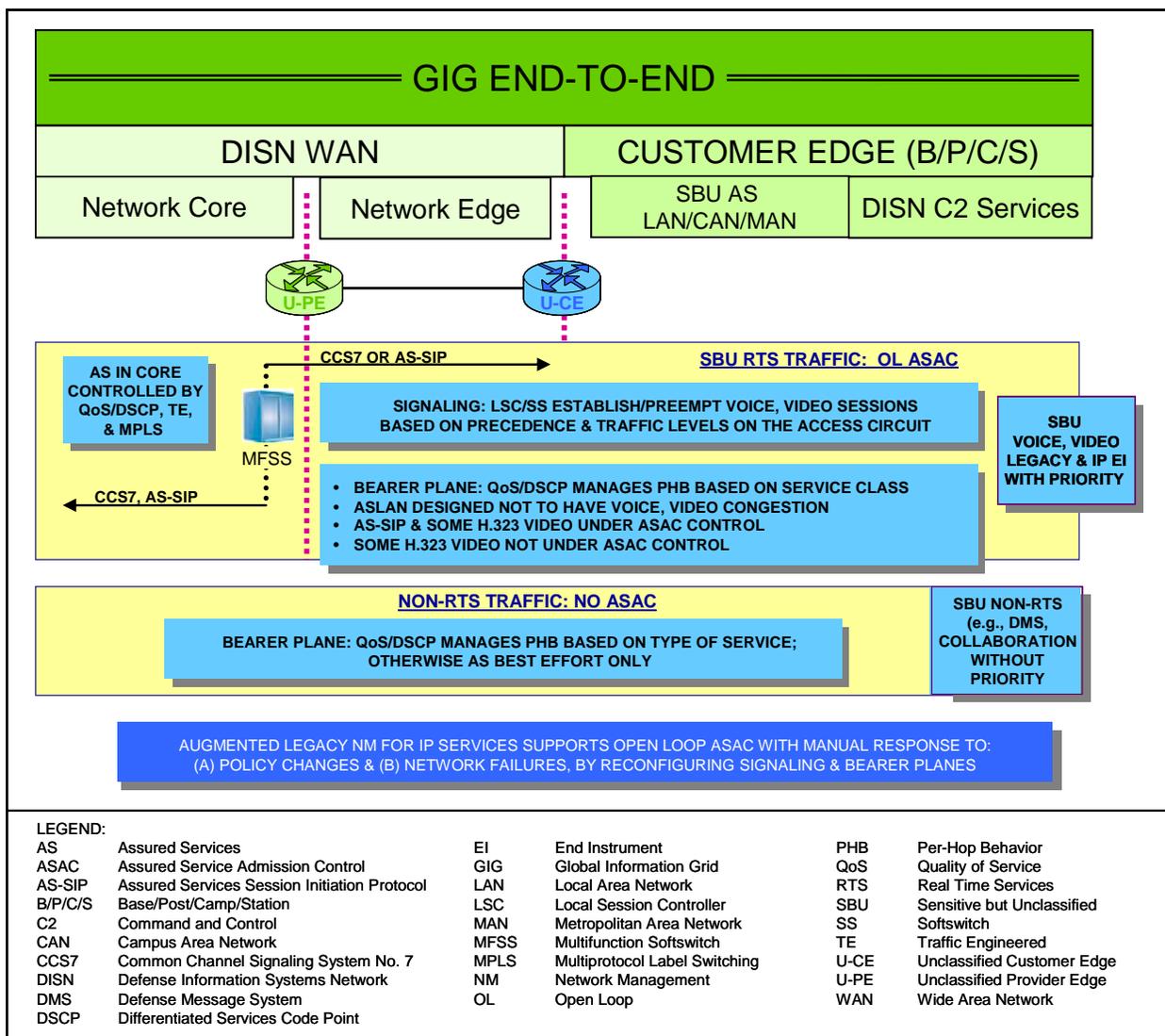


Figure 4-31. Open Loop ASAC for SBU Voice and Video for 2008

The LSC manages a budget for sessions determined by the voice and video traffic-engineered bandwidth of the associated access infrastructure. The Resource-Priority header portion of the AS-SIP signaling message conveys the precedence of the desired session establishment to the destination end LSC. Both the originating and destination LSCs independently manage their session budgets, so that sessions are permitted or established by precedence until the budget limit is reached. Then a new session can be allowed only if a lower precedence session is available to preempt. At the originating end, once preemption has taken place, if necessary, the origination request is sent to the destination upon which, once preemption has taken place, if necessary, the request acceptance is returned to the originating LSC. If the originating LSC is at its budget limit and has no lower precedence session to preempt, then a blocked session indication, in the form of a Blocked Precedence Announcement (BPA), will be sent to the originating EI. If the terminating LSC is at its budget limit and has no lower precedence session to preempt, then a Session Request Denied message will be returned to the originating LSC, which, in turn, will send a BPA to the EI. For Routine calls reaching the maximum budget limit, “fast busy” (120 impulses per minute (ipm)) will be sent to the originating EI. All AS-SIP voice users and some H.323 video users will come under Open Loop ASAC. Some H.323 video users on a base may choose to use a separate H.323 gatekeeper and not come under LSC Open Loop ASAC.

NOTE: Data traffic (non-voice and video) does not have any ASAC and is handled as best effort or preferred data, if the data application implements DSCP packet marking. Signaling between MFSSs may be either DSN Common Channel Signaling System Number 7 (CCS7) (for TDM-to-TDM trunking), or AS-SIP (for voice/video-to-voice/video over an IP WAN). [Figure 4-32](#), Converged VVoIP Design: Signaling, QoS, and Assured Service, shows the aspects of ASAC, signaling, and QoS (CE Router queues and PHB) in one diagram.

Session control processing to establish, maintain, and terminate sessions is performed by the Call Control Agent (CCA) part of the LSC and MFSS. Signaling is performed by the signaling gateway (used for CCS7), Media Gateway (for CAS) or the AS-SIP Signaling Appliance part of the LSC and MFSS depending on requirements for a particular session. Local subscriber directories are stored in the LSCs and network-level worldwide routing tables and addressing/numbering plans are stored in the MFSS.

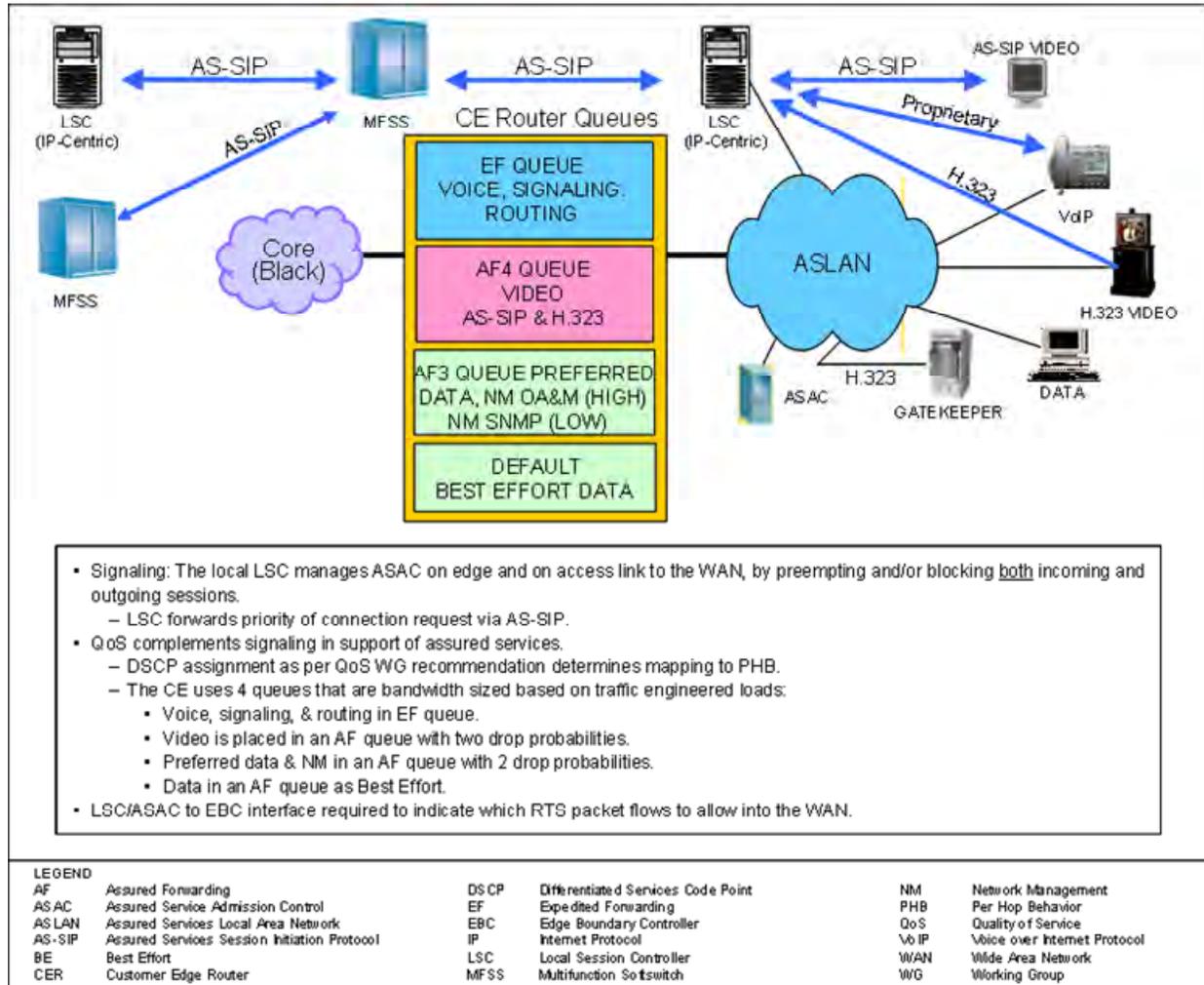


Figure 4-32. Converged VVoIP Design: Signaling, QoS, and Assured Service

4.4.1.1.6 Voice/Video System Signaling Design

The voice/video signaling design for SBU voice and video is shown in [Figure 4-33](#), SBU Voice/Video Services Signaling Design. For classified voice and video, only the AS-SIP signaling is used since classified VVoIP does not have a TDM legacy infrastructure embedded in the system design. Duration migration both H.323 and AS-SIP signaling will be employed in classified VVoIP. Classified VVoIP interfaces to the TDM DRSN via media and signaling gateways. A standalone softswitch will support AS-SIP signaling in the classified VVoIP network. For SBU voice and video, on the edge of the DISN IP WAN cloud, an LSC on the B/P/C/S signals via AS-SIP to the network-level softswitch part of the MFSS. The TDM EO signals via DSN CCS7 to the TDM switching part of the MFSS. The MFSSs use AS-SIP between themselves to set up IP-to-IP EI sessions across the DISN IP WAN.

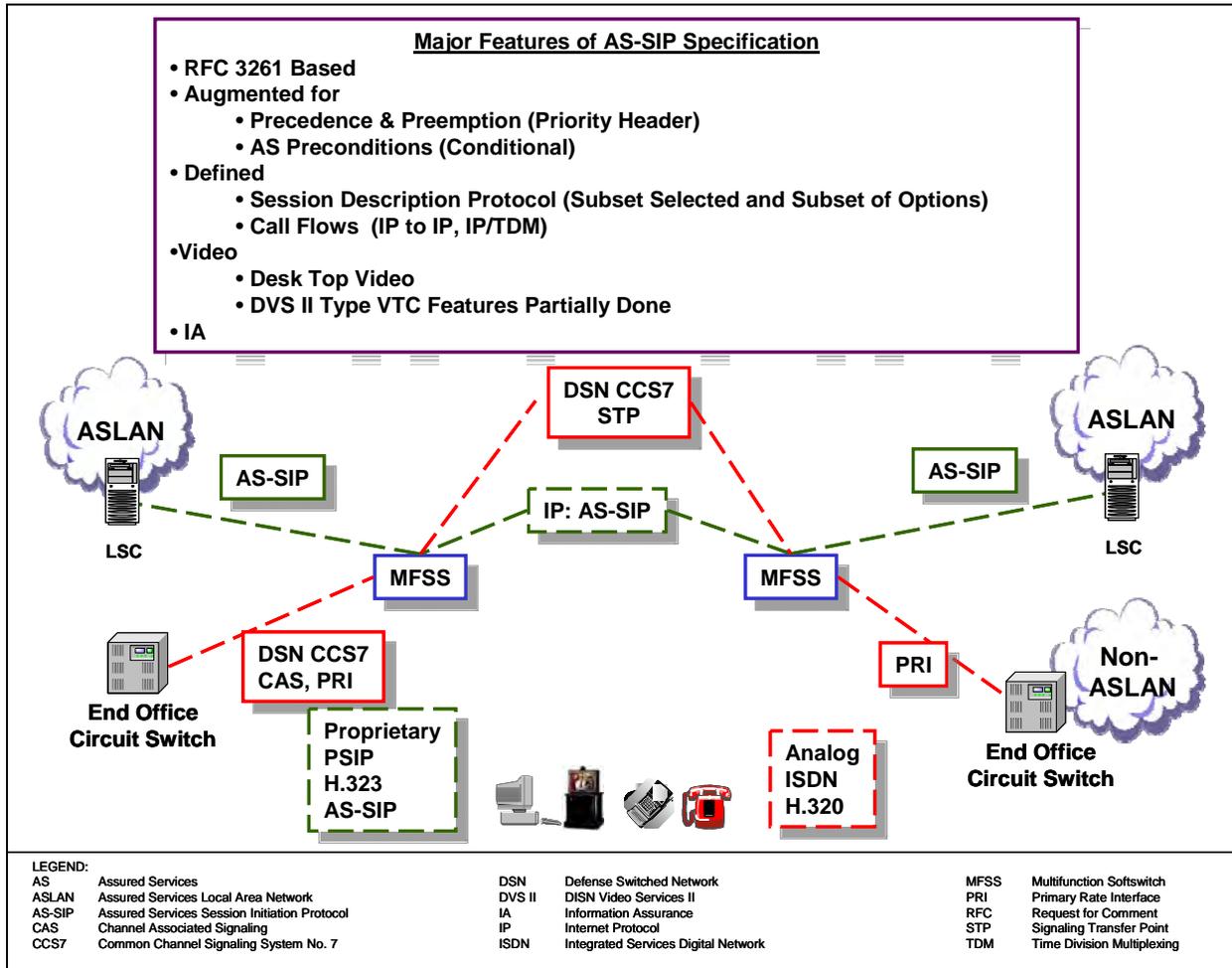


Figure 4-33. SBU Voice/Video Services Signaling Design

The MFSSs use DSN CCS7 to set up TDM-to-TDM EI sessions across the TDM trunking part of the DISN WAN. Both types of signaling are required to support a hybrid TDM and IP EI environment as the DISN voice/video system migrates to an all IP EI environment in the post-2016 time frame.

NOTE: The DSN CCS7 network needs to be supported as long as TDM EOs are still connected to the MFSSs. The MILDEPs will control the pace and timing of the phase-out of TDM EOs on the B/P/C/S.

The key rules and attributes of the signaling design are as follows:

1. Two-level signaling hierarchy: LSC and MFSS
 - a. LSC to MFSS to MFSS to LSC.

- b. LSC to MFSS to LSC.
2. LSCs are assigned a primary and backup MFSS for signaling robustness.
3. Signaling from IP EI to LSC may be proprietary.
4. AS-SIP will be specified in time for 2008 implementation.
5. LSC-to-LSC not permitted across the strategic WAN
 - a. Allowed for tactical theater.
 - b. Does not support GIG Policy-Based Network Management (PBNM) and NETOPS principles to manage bandwidth use.
6. LSC can set up:
 - a. On-base sessions when connection to MFSS is lost.
 - b. Sessions to PSTN trunks independent of MFSS.
7. LSC/MFSS Requirements
8. Signaling
 - a. TDM EO will signal via DSN CCS7, PRI, or CAS to MFSSs.
 - b. MFSSs will signal via CAS/PRI to the PSTN and to coalition gateways.

LSC to LSC signaling without a network level Soft Switch for other than deployed JTFs are under assessment. This assessment is necessary since this configuration has limitations with respect to managing traffic flows from the edge into the network for situational awareness responses of the JTF GNO NetOps and they have visibility limitations (except for cases involving intrabase where an LSC cluster with a master LSC is implemented or for some Tactical Programs under TISPs). Signaling from the LSC must pass through the network softswitch part of the MFSS or through a network level SS so that the MFSS/SS can implement PBNM controls and police the proper use of access circuit bandwidth. For bases that have a collocated MFSS, base-level access to the local PSTN can be provided through the LSC portion of the MFSS. At the network level, the MFSS will serve as the gateway to external networks, such as tactical networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as CAS/PRI signaling.

The end-to-end two-level SBU AS-SIP network signaling design is shown in [Figure 4-34](#), End-to-End Two-Level SBU AS-SIP Network Signaling Design. For classified networks the two level signaling uses standalone softswitches rather than MFSSs.

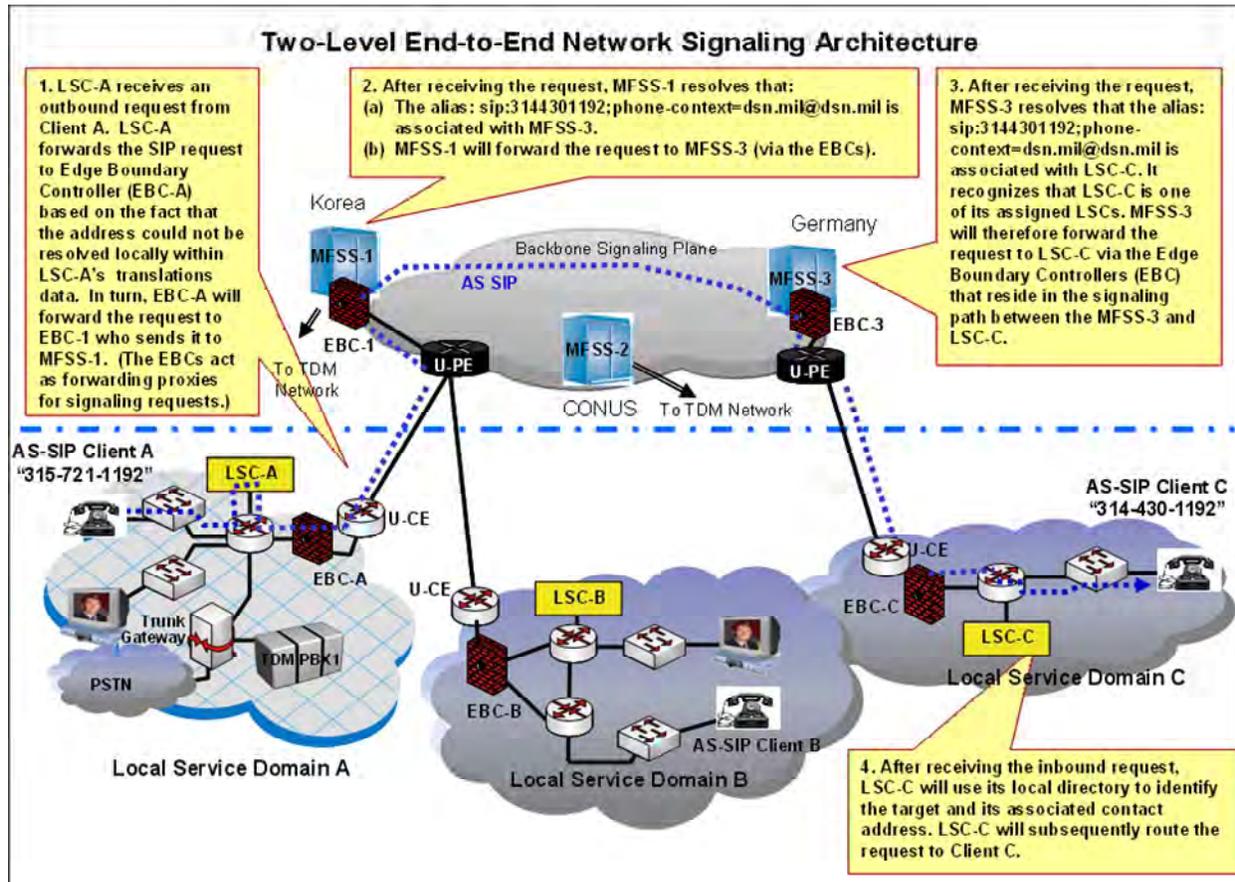


Figure 4-34. End-to-End Two-Level SBU AS-SIP Network Signaling Design

4.4.1.1.7 IA System Design

Information assurance is a key aspect in the design of any IP-based system. IP is inherently vulnerable to eavesdropping and a variety of denial of service attacks. VVoIP introduce avenues of attack due to its use of dynamically assigned UDP sessions that cannot be addressed by traditional data firewalls. Therefore, VVoIP are applications that use IP for transport and inherit the threats associated with IP as well as adding vulnerabilities that are unique to the VVoIP technology. A tailored VVoIP IA design is necessary and is addressed in detail in UCR 2008, Section 5.4, Information Assurance Requirements. The major components of the IA design include the protocols used, the interfaces of LSCs and MFSS to external control devices, and the design of the ASLAN. The methods for securing the VVoIP protocols are illustrated in [Figure](#)

4-35. IA Protocols. Key to the system design is a hop-by-hop security model for trust between the signaling appliances using the DoD PKI for authentication.

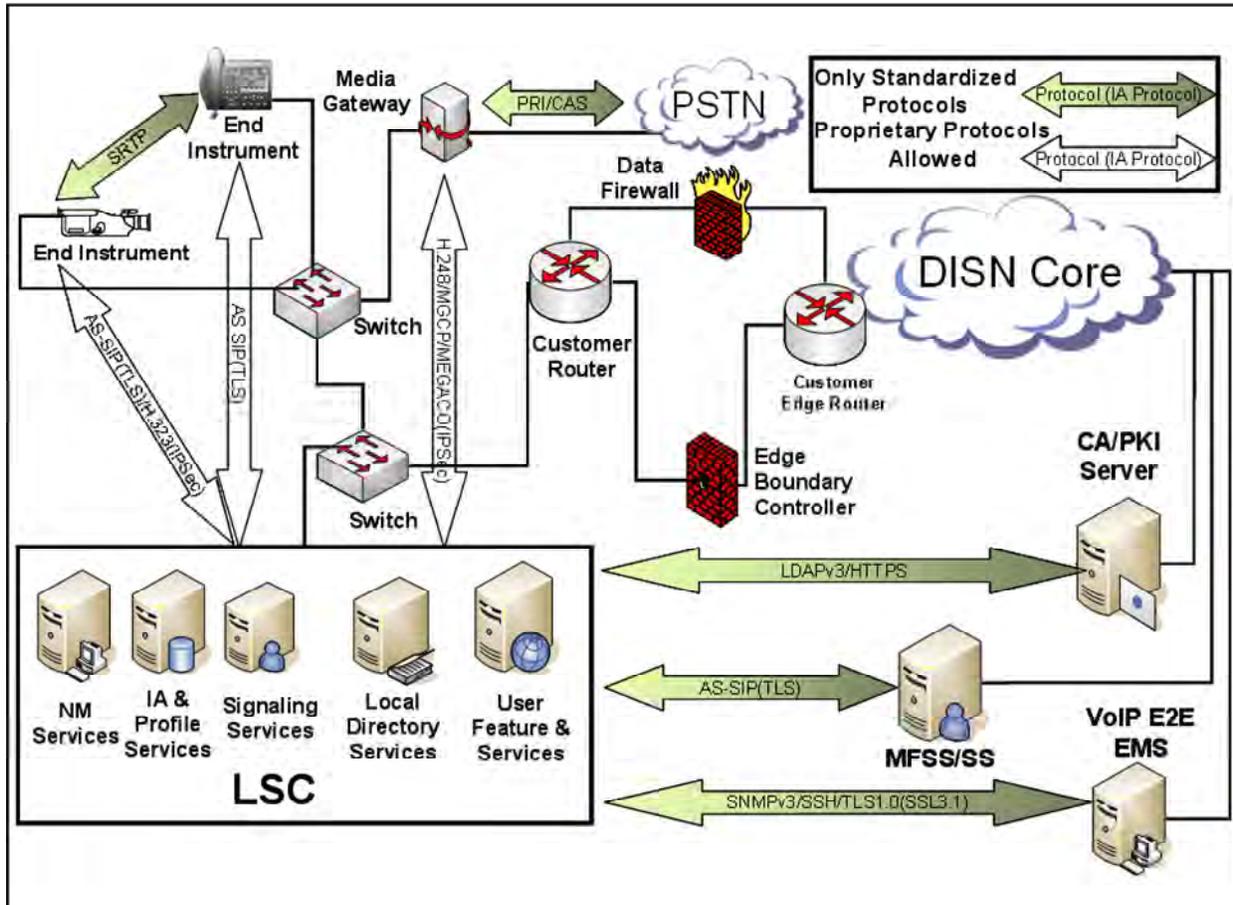


Figure 4-35. IA Protocols

Figure 4-36, IP External Interfaces to the LSC or MFSS, illustrates the IP interfaces to the LSC or MFSS by external remote access terminals such as the End-to-End Element Management System as well as to the other and the associated IA appliances.

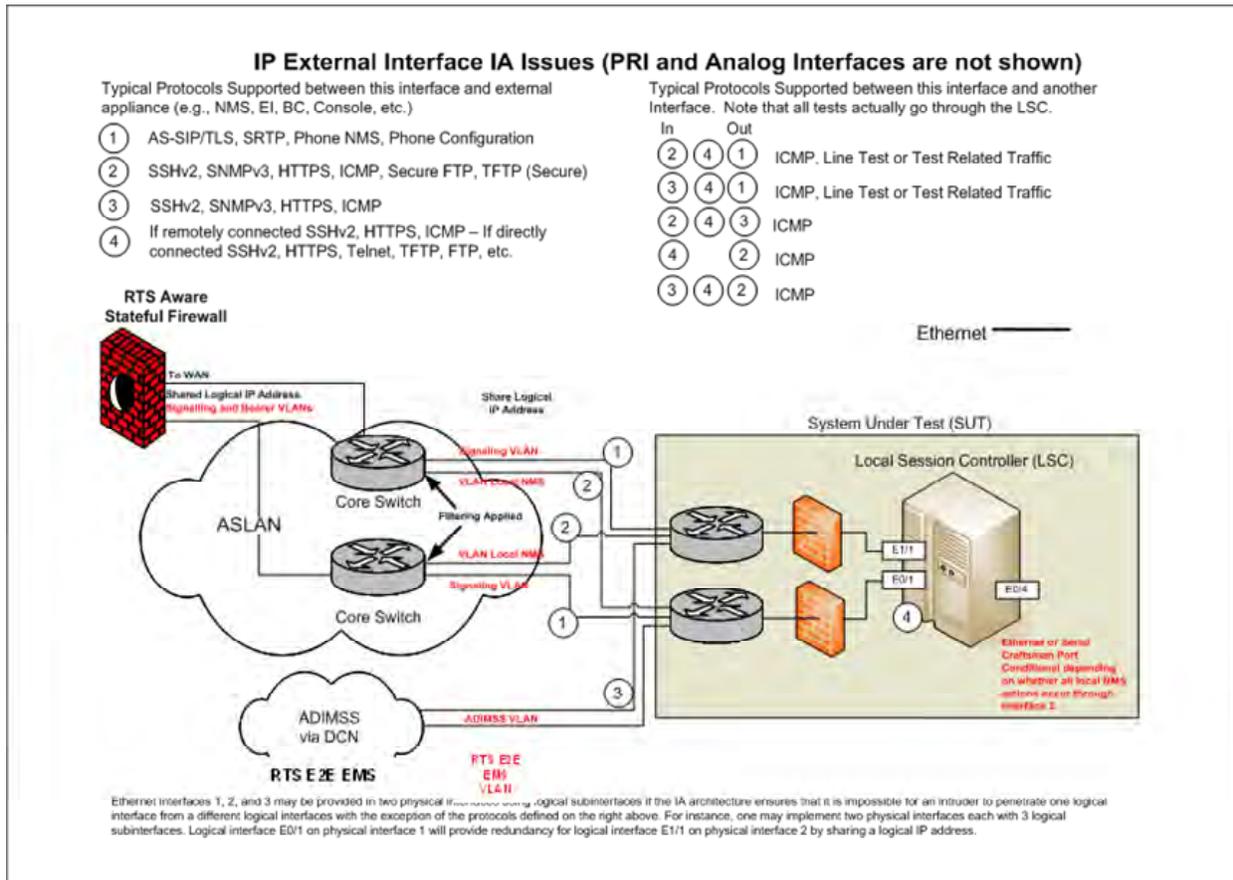


Figure 4-36. IP External Interfaces to the LSC or MFSS

[Figure 4-37](#), ASLAN Enclave Boundary Security Diagram, depicts a diagram of the IA system design needed as part of the ASLAN. The key feature of Figure 4-37 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice/video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice/video dynamic stateful AS-SIP aware application firewall, which provides Network Address Translation (NAT), MFSS failover, and port pinholes for individual voice and video sessions. An UC APL product called an Edge Boundary Controller (EBC) consisting of the voice/video firewall/border controller, which may be collocated on the same platform as the CE Router and the data firewall and has been defined and specified in Section 5.3.2, Assured Services Requirements.

The requirements for the IA functionality are provided in UCR 2008, Section 5.4, Information Assurance Requirements, which dictates the detailed methods by which all known security threats against the system have been mitigated.

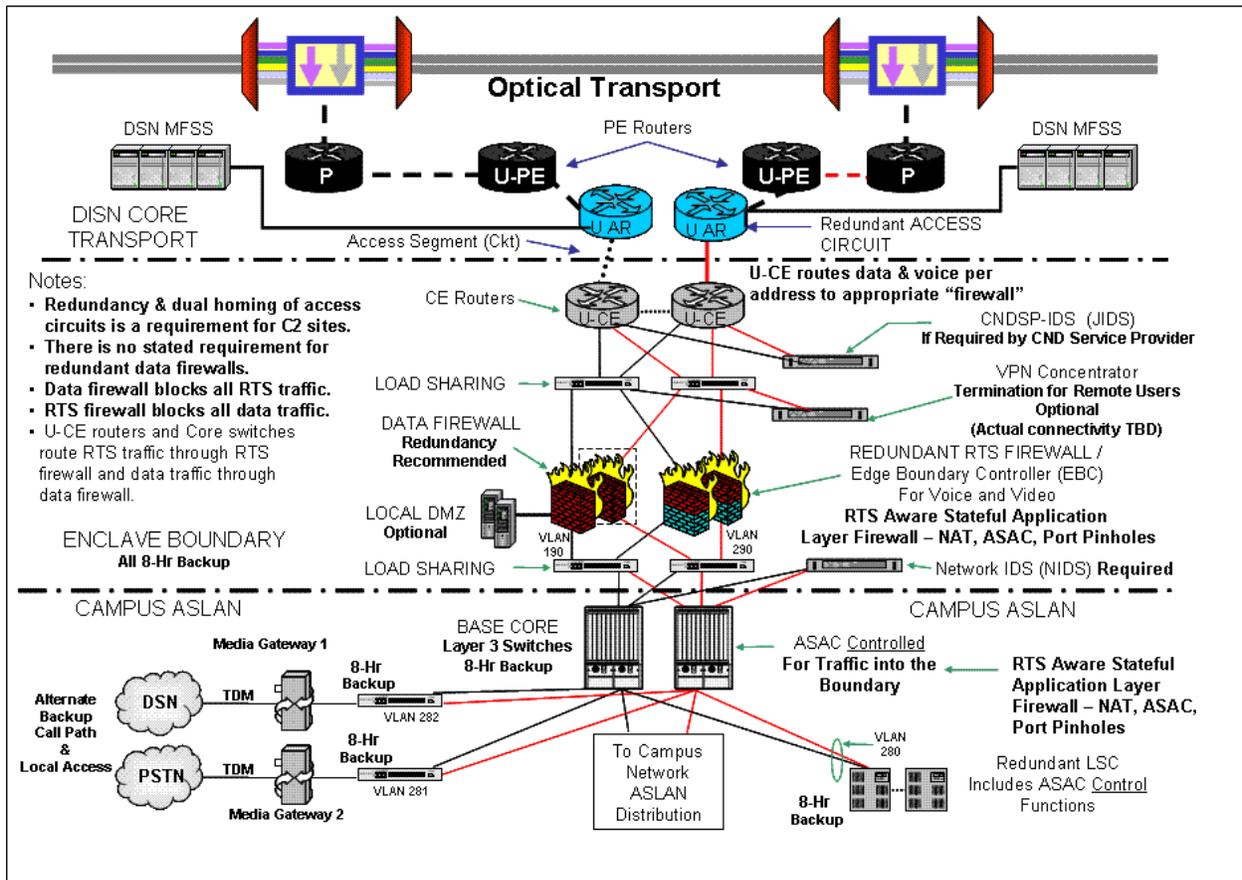


Figure 4-37. ASLAN Enclave Boundary Security Design

4.4.1.1.8 Network Management System Design

Network management of the VVoIP services end-to-end (E2E) is a critical component of NetOps. Since the VVoIP network will be a hybrid network for an extended period the NM system must continue to be provided by an Element Management System (EMS) via commanding and monitoring of the voice and video services for both circuit-switched and IP technologies as part of the DISN Operations Support System (OSS). This hybrid operation within the DISN OSS is illustrated in [Figure 4-38](#), Role of E2E RTS EMS in DISN OSS, where the EMS is shown at the bottom of the DISN OSS hierarchy.

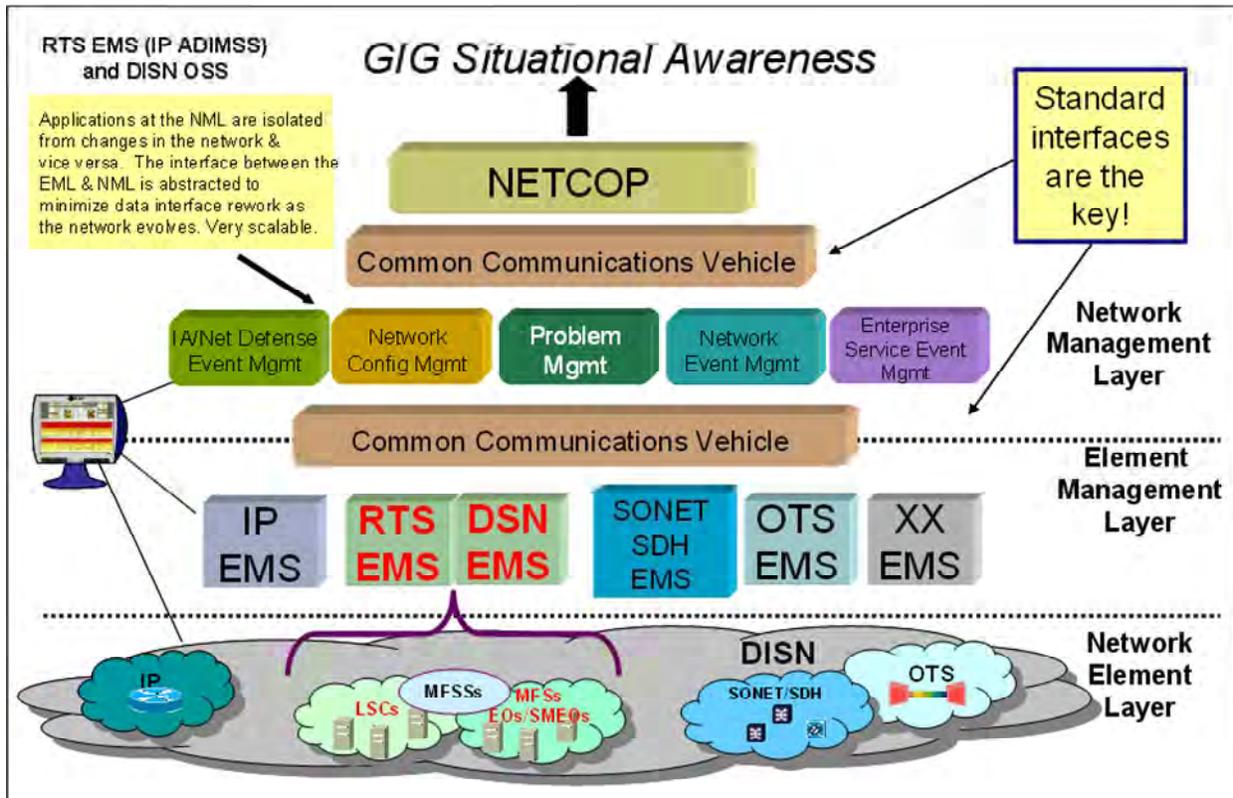


Figure 4-38. Role of E2E RTS EMS in DISN OSS

As part of the migration to NetOps GIG Element Management (GEM) the E2E RTS EMS must provide new interfaces for “Reading and Writing” to the edge appliances to support the JTF GNO in both visibility into the network and in reconfiguring the network and controlling the flow of sessions into the network in response to situational awareness. The system design for support of JTF GNO is illustrated in [Figure 4-39](#), E2E RTS EMS Command and Monitoring at the Edge. It should be noted that since the E2E VVoIP EMS is GOTS based on COTS it is available for the MILDEPs to use at their Network Operations Centers (NOC) as well.

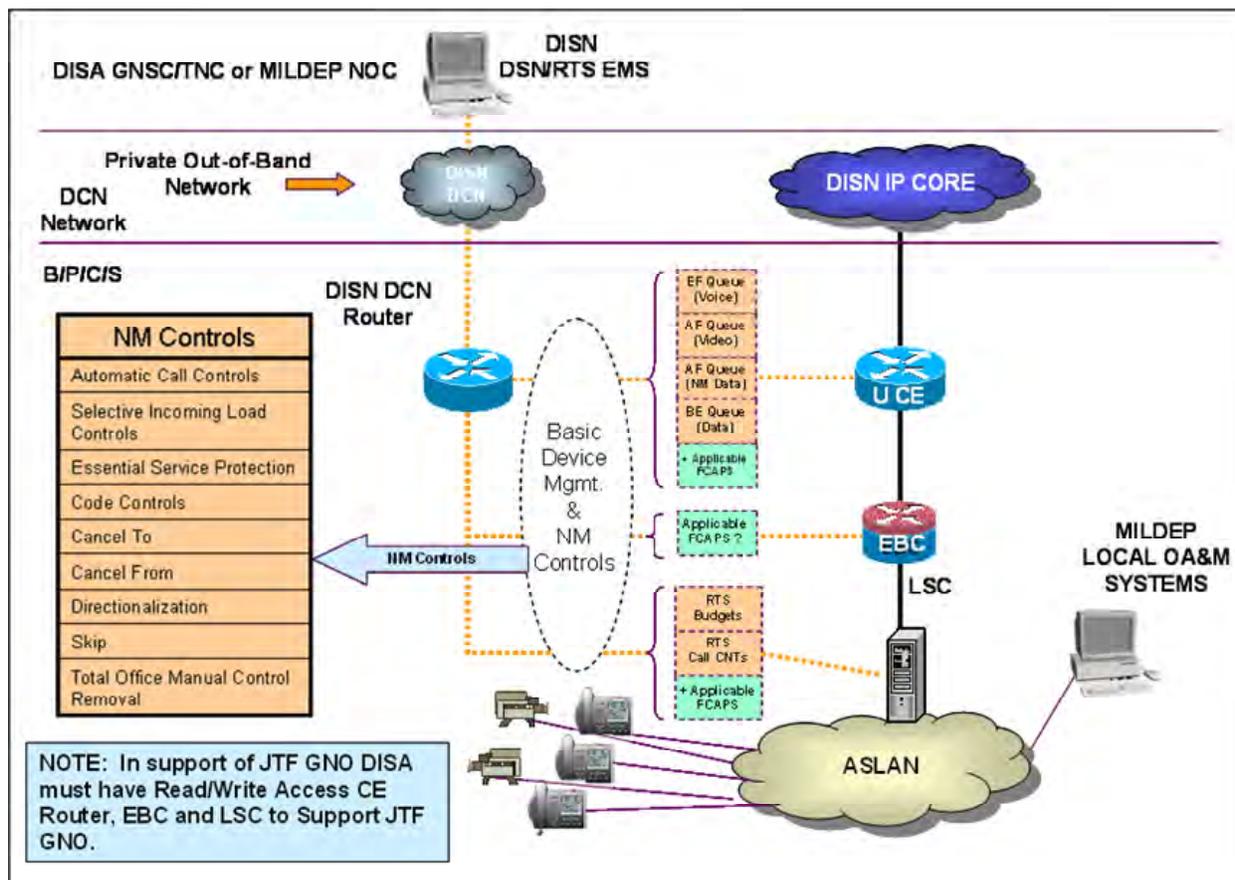


Figure 4-39. E2E RTS EMS Command and Monitoring at the Edge

4.4.1.2 Relationship between SBU UC System Description and Products to be Tested for APL Certification

This section describes relationships between voice and video architectural components, appliance functions, and UC products to be tested for APL certification. The term “appliance function” is introduced because the IP-based UC APL products will often consist of software functions and features (e.g., appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a TDM-based APL product, such as an End Office, consists of a single unit containing all required telephony functions. Appliances operate at the signaling, bearer, and NM planes. Appliance functions are described and referred to throughout the UCR 2008, but are not considered products for UC APL certification, but rather functions and features that form a part of a UC APL product. [Table 4-3](#), Summary of IP-Based Appliances and UC APL Products, provides a summary of IP-based appliances and APL Products. [Table 4-4](#), Summary of TDM-Based Appliances and UC APL Products, provides a summary of TDM-based APL products.

Table 4-3. Summary of IP-Based Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
End Instrument	Appliance	Appliance part of LSC
Media Gateway	Appliance	Media conversion function as part of the LSC and MFSS
Signaling Gateway	Appliance	Signaling conversion function as part of the LSC and MFSS
AS-SIP Signaling Appliance	Appliance	Appliance function within and LSC and MFSS that provides AS-SIP signaling capability
Call Connection Agent	Appliance	Appliance function within an LSC and MFSS that performs parts of session control and signaling functions
Registrar	Appliance	Appliance function that stores the location of a registrant and its profile
Registrant	Appliance	Appliance function used to register with the network to seek and gain authority to invoke services or resources from the network
LAN Switch/Router (Access, Distribution, and Core)	APL Products	APL products used in ASLAN
Secure End Instrument	APL Product	System consisting of a single appliance
Local Session Controller (LSC)	APL Product	System providing many local telephony functions
Multifunction Softswitch (MFSS)	APL Product	Large, complex system providing many local and WAN-related telephony functions
Edge Boundary Controller (EBC)	APL Product	System providing firewall functions
Customer Edge (CE) Router	APL Product	System providing routing functions at the enclave boundary
DISN WAN P/PE Router	APL Product	System providing routing of IP packets
DISN MSPP	APL Product	System providing transport access to the DISN WAN
M1-3 Multiplexer	APL Product	System providing transport interface to the DISN
DISN Optical Switch	APL Product	System serving as an optical transport node

Table 4-4. Summary of TDM-Based Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
Multifunction Switch (MFS)	APL Product	System providing local telephone service and tandem switching with full set of Assured Services Features, including network traffic management Controls
End Office	APL Product	System providing local telephone service and full set of Assured Services Features including network traffic management Controls
Small End Office	APL Product	Smaller version of the EO System providing local telephone service and full set of Assured Services Features
Private Branch Exchange (PBX) Type 1	APL Product	System providing local telephone service and MLPP capabilities
Private Branch Exchange (PBX) Type 2	APL Product	System providing local telephone service without MLPP capabilities
Remote Switching Unit (RSU)	APL Product	Small System providing local telephone service as an extension to an EO/SMEO or PBX.
Deployable Voice Exchange (DVX)	APL Product	System providing tactical telephone service with MLPP capabilities
Deployable DSN PBX1	APL Products	System providing tactical telephone service with PBX1 features

The architectural differences between TDM-based APL products and IP-based APL products are illustrated further in [Figure 4-40](#), Decomposition of a VVoIP Edge Solution into UC APL Products. The figure illustrates how several VVoIP appliance functions and APL products replace what is typically provided by a single TDM-based APL product (e.g., DSN EO) to provide voice/video service on a B/P/C/S.

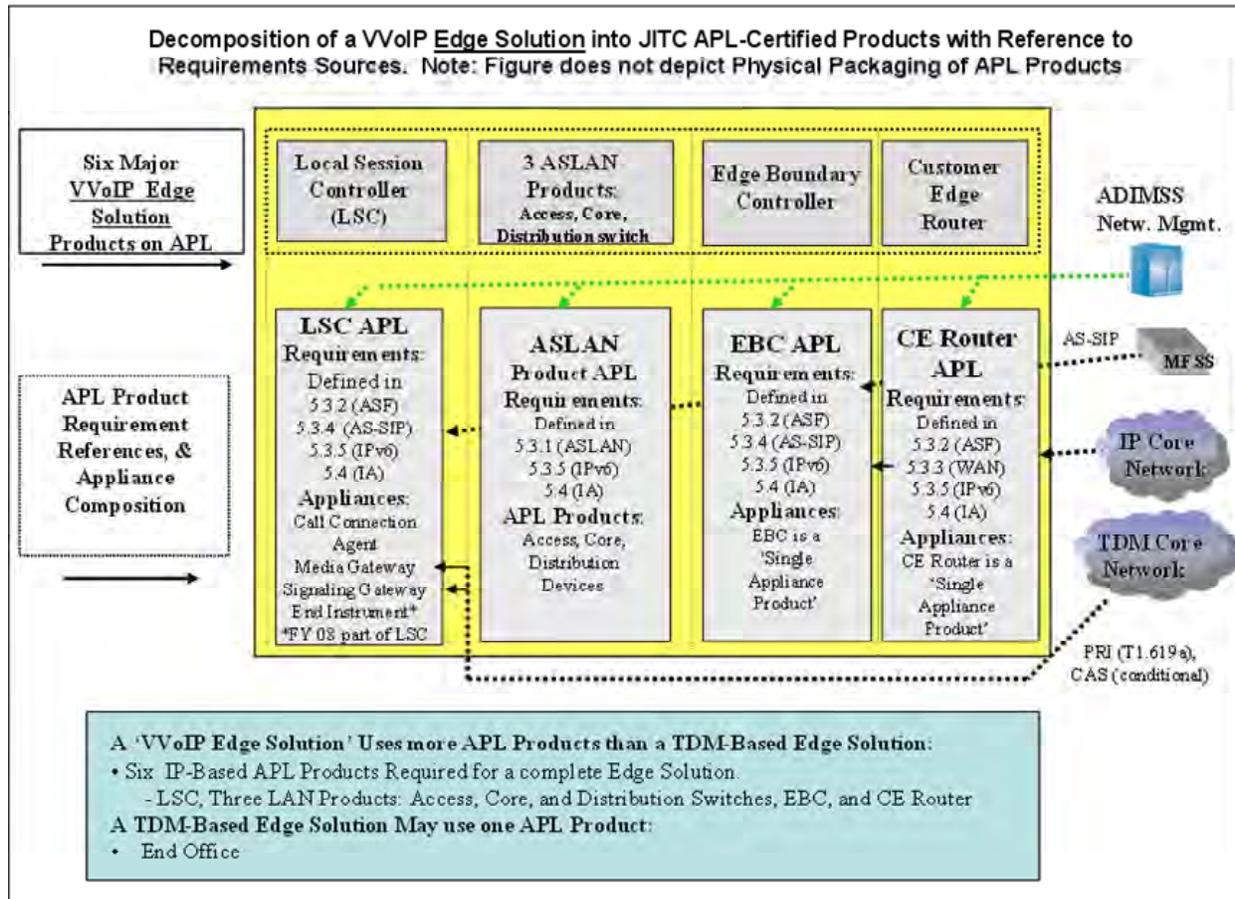


Figure 4-40. Decomposition of a VVoIP Edge Solution into UC APL Products

4.4.1.3 Classified VoIP System Design

Figure 4-41, Classified VoIP System Design Illustration, illustrates the Classified VoIP System Design. The approved product types are the same as the SBU approved product types with the exception of the MFSS, which is not needed for classified VoIP and is replaced with a dual signaling stand-alone softswitch capable of both H.323 and AS-SIP signaling which is described in UCR 2008, Section 6.2, Unique Classified Requirements.

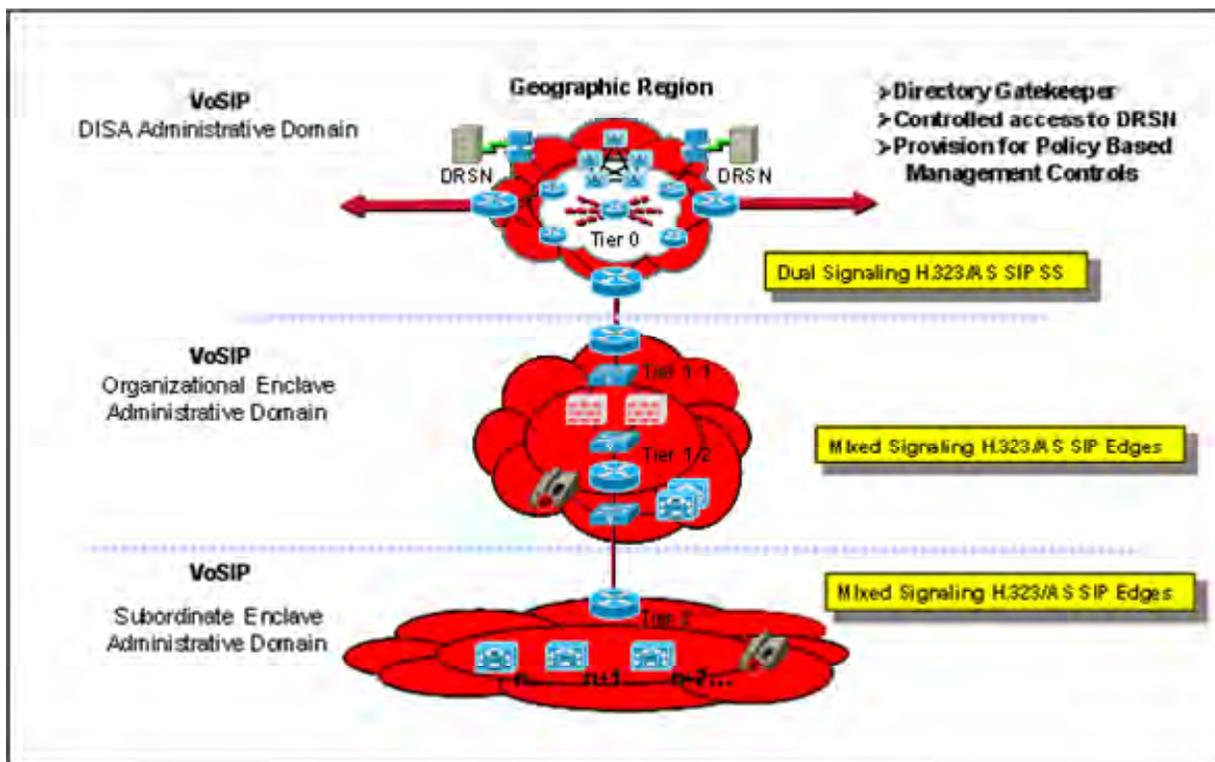


Figure 4-41. Classified VoIP System Design Illustration

4.4.1.4 VTC System Design

VTC systems both DVS and MILDEP VTCs will use both the SBU and Classified system designs and approved product types with the significant difference being that the MCUs employed will be capable of three types of signaling to support the migration of the end users systems. The three signaling types will be H.320, H.323, and AS-SIP. [Figure 4-42](#), Hybrid VTC Services System Description, illustrates the Hybrid VTC Services System Description.

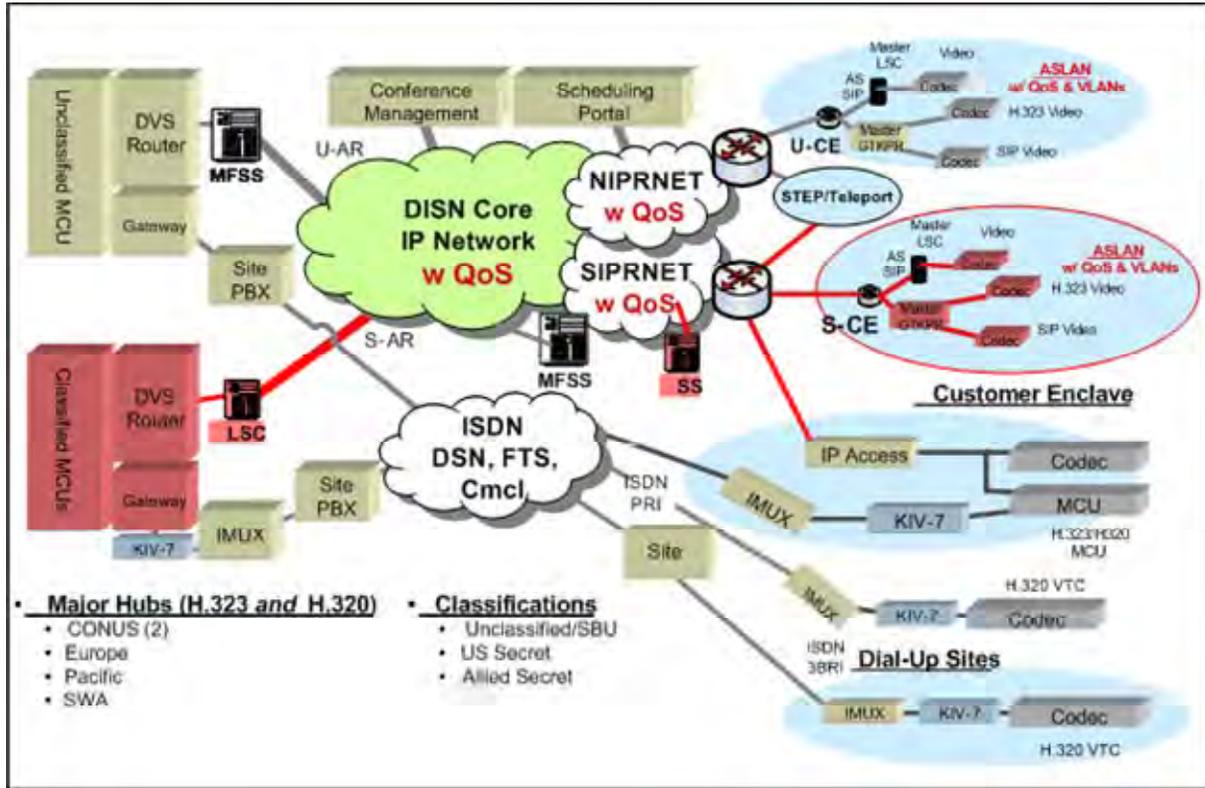


Figure 4-42. Hybrid VTC Services System Description

4.4.1.5 DISN Router Hierarchy

Figure 4-43, DISN Router Hierarchy for FY 2009, illustrates the DISN router hierarchy for FY 2009 for both the unclassified network and the Secret network. At this point, the NIPRNet and SIPRNet routers have been transformed to be Unclassified Aggregation Routers (ARs) and Secret ARs connected to the U-PE routers and C-PE routers.

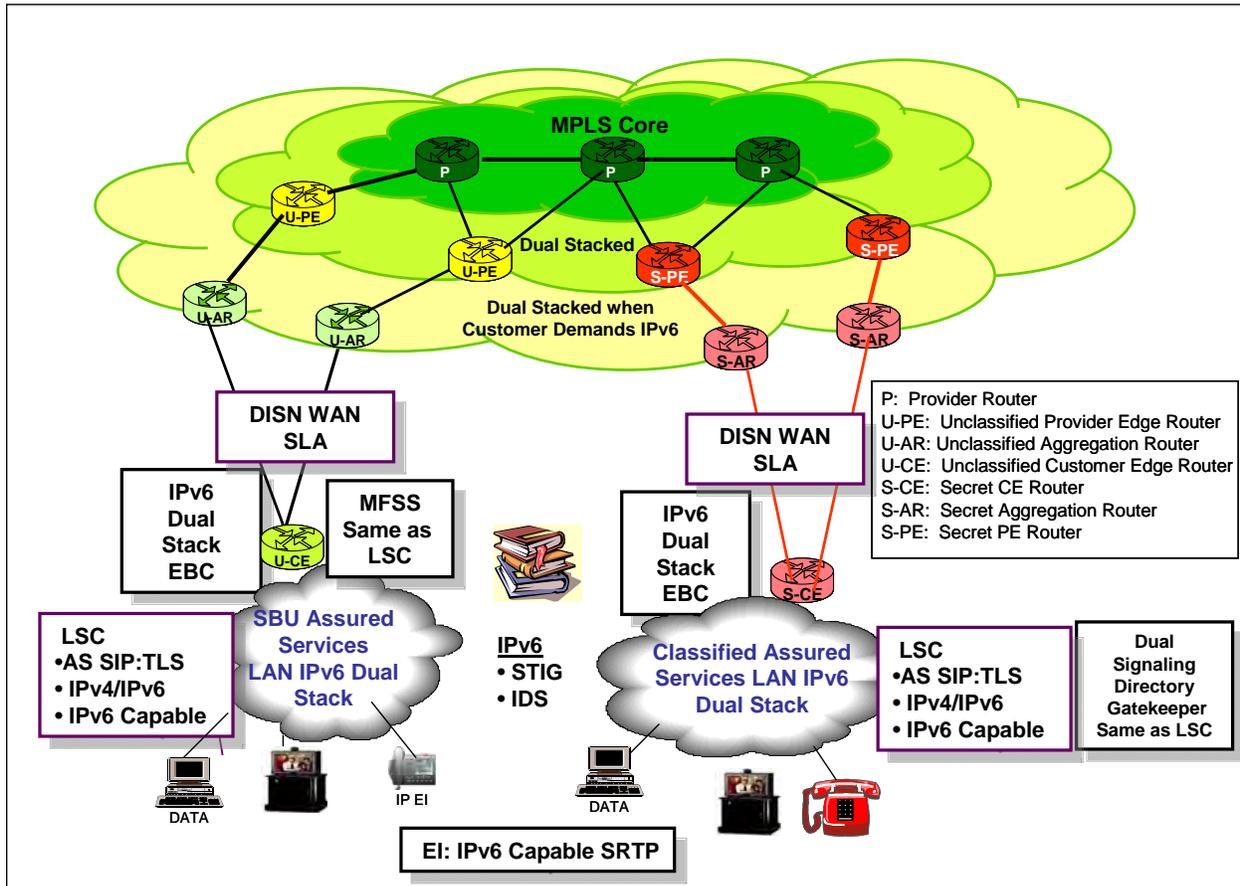


Figure 4-44. IPv6 Design for SBU and Classified VVoIP

4.4.2 TDM-Based SBU Voice (DSN) System Design

The Joint Staff Policy document CJCSI 6215.01C defines network performance and features required to ensure end-to-end global voice quality, interoperability for all voice C2 services. DISA is responsible for engineering, network design, and technical support. The DSN design meets the Joint Staff Policy mandate, shown in [Figure 4-45](#), DSN Design and Components.

The DSN design is a two-level network hierarchy consisting of DSN backbone switches and military or agency installation switches. The switches are connected by several types of trunks, as indicated in [Figure 4-45](#), DSN Design and Components.

Joint Staff policy and subscriber mission requirements determine which locations require the full set of MUFs and capabilities offered by the DSN. The DSN design therefore consists of several categories of switches. They may be used as outlined in the following paragraphs.

4.4.2.1 DSN Backbone Switches

The DSN backbone switches are integral to the DSN (and part of the GIG), which provides tandem switching for long-distance DSN services. The backbone switch types are the tandem switch (TS) and the MFS. These switches have the full set of MUFs as defined in the UCR 2008. The MFS contains both the End Office (EO) and TS functionalities. [Figure 4-45](#), DSN Design and Components, depicts the DSN SBU voice and video design and components

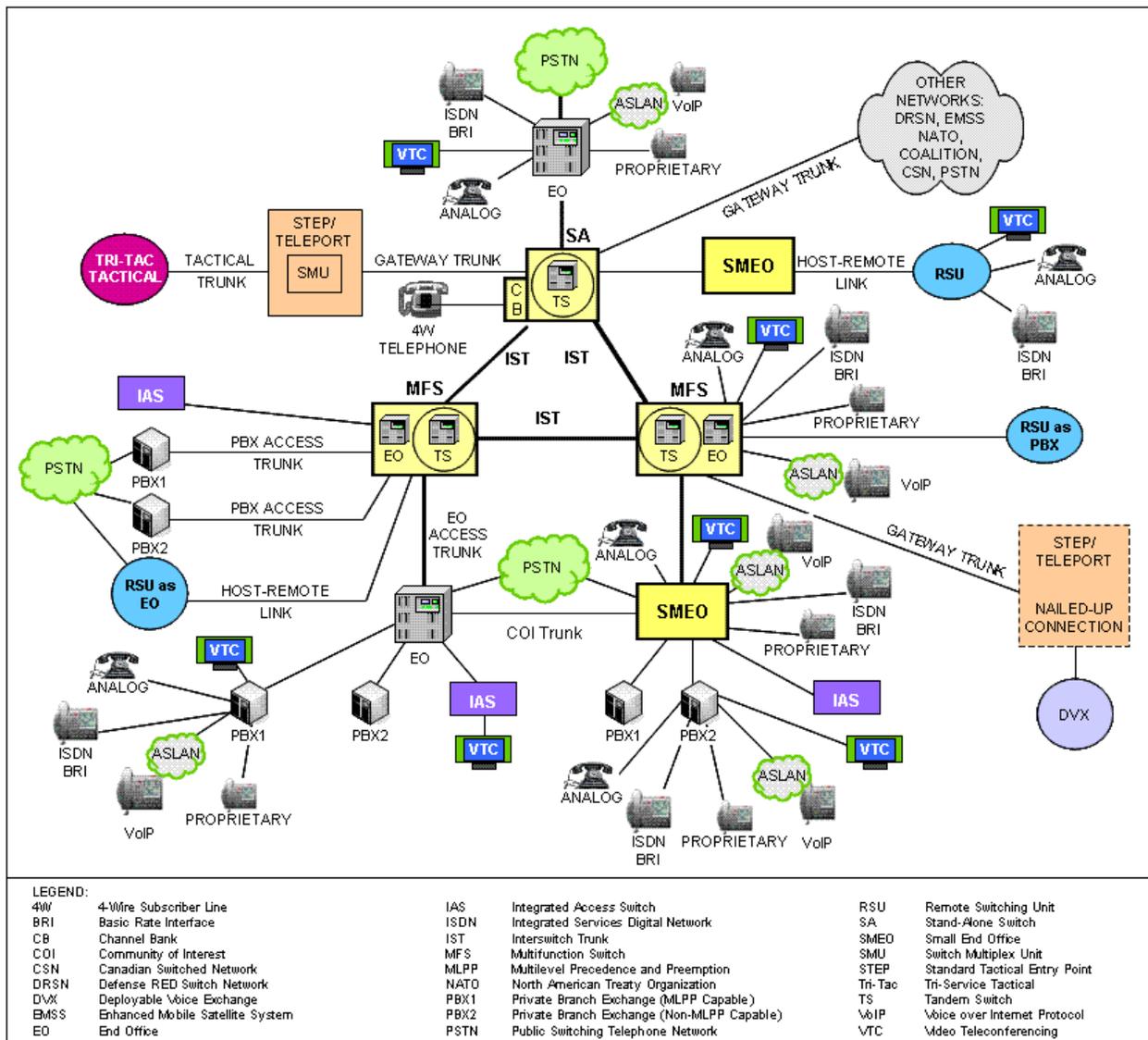


Figure 4-45. DSN Design and Components

4.4.2.2 Military and Agency Installation Configuration and Switch Types

Military and agency installation switch types are integral to the DSN (and part of the GIG) and provide origination and reception of DSN calls to the DSN user categories defined in the UCR. Because of the various degrees of mission support performed by the users at an installation, the following military/agency installation switch types are defined: End Office (EO), Small EO (SMEO), Private Branch Exchange 1 (PBX1), and Private Branch Exchange 2 (PBX2). [Figure 4-46](#), Example Installation Configurations, shows an example installation configuration. The intent is to allow for maximum flexibility consistent with satisfying the COCOM’s C2 mission requirements.

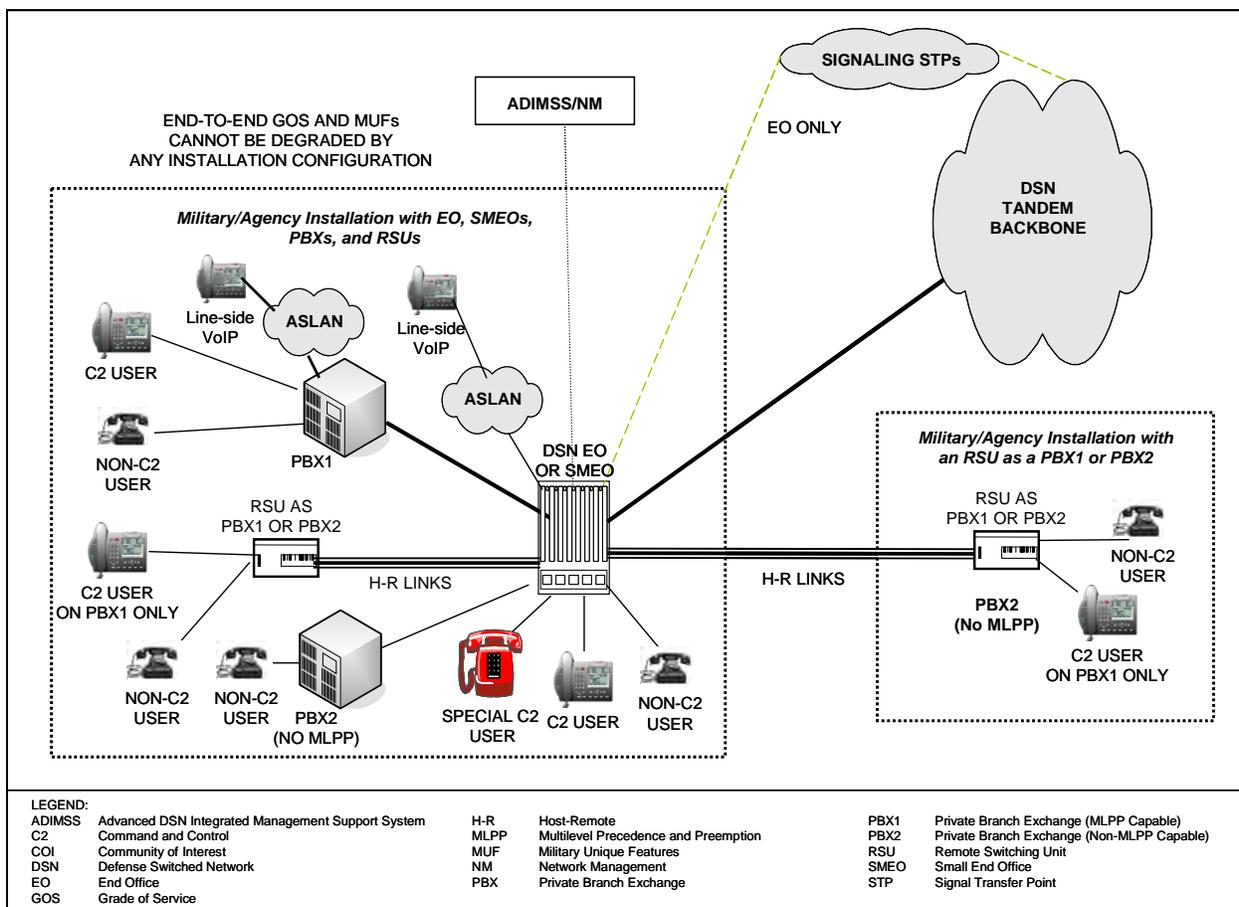


Figure 4-46. Example Installation Configurations

An installation configuration can vary from a single EO or SMEO with subtending Private Branch Exchanges (PBXs) or Remote Switching Units (RSUs) to an installation that for cost or operations considerations uses multiple switches, such as a mixture of EOs, SMEOs, PBX1s, PBX2s, and RSUs, depicted in [Figure 4-45](#), DSN Design and Components, interconnected in a hub, ring, mesh, or hybrid configuration (not depicted). When this is done, at least two

physically diverse access circuits must be used to connect to the DSN tandem backbone. Regardless of where terminated on the installation switches, the Special C2, C2, C2(R) user (originate ROUTINE only calls but can receive precedence calls), and the non-C2 users must be provided the grade of service (GOS) and ASFs as required for their class of user.

The NM capabilities defined by the UCR 2008 to support Special C2, C2, C2(R), and non-C2 users are required in all installation switching configurations. It is the responsibility of the installation manager to ensure that the installation configuration meets the approved product configurations posted on the UC APL.

4.4.2.3 *End Office*

End Office switches are integral to the DSN (and part of the GIG). They provide a significant amount of the intra-DoD communications to meet the mission requirements of a military or agency installation. An EO provides access to the long-haul backbone of the DSN by interconnection using EO access trunks. Where an installation's EO function is provided by an MFS, access to the long-haul DSN backbone is provided through the tandem portion of the MFS. A large installation could have multiple EO switches, where each of them provides a significant amount of DoD communications for the missions of that installation or tenants on the installation. An EO can serve all user categories.

4.4.2.4 *Small End Office*

Small End Office switches are integral to the DSN (and part of the GIG). They provide EO functions. The SMEO is used where a smaller DoD community requires DSN C2 services. The SMEO technology is based on a commercial Private Automatic Branch Exchange (PABX) with MLPP capabilities, thereby providing a lower-cost EO solution. The SMEO does not provide full DSN Network Traffic Management control capability. It offers limited performance reporting. The SMEO may not support CCS7 signaling.

4.4.2.5 *Private Branch Exchange*

Private Branch Exchanges are MILDEP-controlled elements of the DSN. In addition, they are part of the GIG because users can originate and receive DSN calls. The PBXs are therefore subject to all interoperability requirements of the GIG. Two categories of DSN PBX switches are Type 1 and Type 2, and described as follows:

1. PBX Type 1 (PBX1). A PBX Type 1 has MLPP capabilities. Based on mission requirements, this switch may serve those C2 users defined as DoD users having a military mission that might receive C2 calls for orders or direction at precedence levels above a ROUTINE precedence, even though they do not have a C2 mission for issuing guidance or

orders. Special C2 users must connect to an EO or SMEO and are not authorized to be served by a PBX1.

2. PBX Type 2 (PBX2). A PBX Type 2 has no MLPP capabilities and requires only one of several network interfaces specified for a DSN EO. This switch can serve only DoD, non-DoD, nongovernmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 communications under existing military scenarios. These users are provided access to the DSN for the economic or policy benefits of the DoD, when it is not in conflict with local Public Telephone and Telegraph (PTT) ordinances. During a crisis or contingency, they may be denied access to the DSN. C2 and Special C2 users are not authorized to be served by a PBX2.

4.4.2.6 Remote Switching Unit

The RSU is a switching capability that is connected to a host as a remote via an umbilical, dependent on the host switch for software control, some or all centralized OA&M, and it is integral to a Line Concentrating Module, or Remote Module that depends upon a host switch.

The RSU can best be described or envisioned as an installation of the host switch's internal "line and trunk cabinets" at a location within the confines of the Installation, B/P/C/S authorized boundaries, or at a related adjacent site, normally within a few miles of the host switch." During degraded operating conditions, only partial service may be available from the RSU. The RSUs line and trunk cabinets are of the same basic type and originally certified by the JITC during the "host switch's" MFS, EO, or SMEO certification process.

RSUs are cost effective ways to improve "reach" and extension of voice communications capabilities and services to users located in buildings that are some distance from the host switch. An RSU is an extension for the voice switch's previously certified DoD Components. For this reason:

1. RSUs retain legacy status even if the host switch is upgraded.
2. RSUs can be capacity upgraded, expanded, and moved within the authorized boundaries (within a reasonable distance of the Installation, B/P/C/S).
3. RSUs used to extend the host switches' capability do not require stand-alone (MUF) capability.
4. Stand-alone capability is only required if an RSU is utilized in EO/SMEO applications not within a reasonable distance of the host switch.

5. Line and trunk sizing does not trigger APL requirements.
6. CAS to PRI transitions do not trigger APL requirements.

4.4.2.7 Deployable Voice Exchange

The DVX is a tactical switch with ASF capabilities to support the assured service requirements of CJCSI 6215.01C used for rapid deployment situations and contingencies in the tactical environment. The DVXs can be either DVX COTS (DVX-C) or DVX legacy (DVX-L) tactical (TRI-TAC) systems. Normally, a DVX is connected to the DSN using gateway trunks routed through a standard tactical entry point (STEP)/Teleport location. It can be connected directly to the DSN (TS/MFS/EO/SMEO) if it is to be used as a temporary solution for either of the following:

1. An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.
2. A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

4.4.2.8 Deployable DSN PBX1

A strategic DSN PBX1 is connected to a DSN EO or SMEO switch; however, a deployable DSN PBX1 may need to connect through a STEP/Teleport to a DSN switch. This configuration includes some limitations, as follows:

1. The PBX1 functionality shall be limited only to those that were tested and certified by the JITC and as posted on the APL. The user assumes all limitations identified in the JITC test report.
2. The PBX1 was designed for connecting to only one supporting DSN switch. If connections to more than one switch are required, testing must verify this capability.
3. The PBX1 must not tandem and shall not have any subordinate switches or lateral connectivity.
4. Fewer variants may be available for PSTN/PTT connections.
5. The PBX1 requirements do not include the use of an attendant and this capability is not tested.

6. The PBX1s are not approved to support Special C2 (FLASH and FLASH OVERRIDE) users as their only means of communication. Special C2 users shall be supported by other means such as a long local.

4.4.2.9 DSN Backbone Signaling System

The DSN employs CCS7 throughout most parts of the backbone. The Signaling Transfer Points (STPs) used to relay signaling messages are system components that are subject to IA and interoperability testing and must appear on the APL. Requirements are specified in the UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

4.5 UNIFIED CAPABILITIES APPROVED PRODUCTS LIST PROCESS

This section addresses the UC approved products processes and products, the role of the UCR in the Information Support Plan (ISP)/Tailored ISP (TISP) process and the modifications of the APL process to support VVoIP technology and UC technologies insertion via the Spirals capability deployments addressed in the Migration sections.

4.5.1 Unified Capabilities Approved Products Process and Products

[Figure 4-47](#), JIC and IA Certification and Accreditation Process Overview, depicts an overview of the JIC and IA certification and accreditation process. This process shall be applied to all the UC products identified in the UCR.

The UCR 2008 defines the products and the requirements that must be met for those products to be placed on the UC Approved Products List. The process by which products gain APL status is also defined. This process is defined for mature products and for technology insertion products that are evaluated via assessment testing in DoD test labs and validated for NetOps via Spirals that deploy capabilities. These three areas APL products, APL processes for mature products and APL process for technology insertion products are in addressed in the subsequent sections.

4.5.1.1 Overview of Approved Products

The UCR covers six categories of Approved Products as follows:

1. SBU UC Products for IP E2E systems support SBU voice and video services
2. Ckt Switches with IP on EIs only that support SBU voice and video services

Section 4 – Unified Capabilities Description and Key Processes

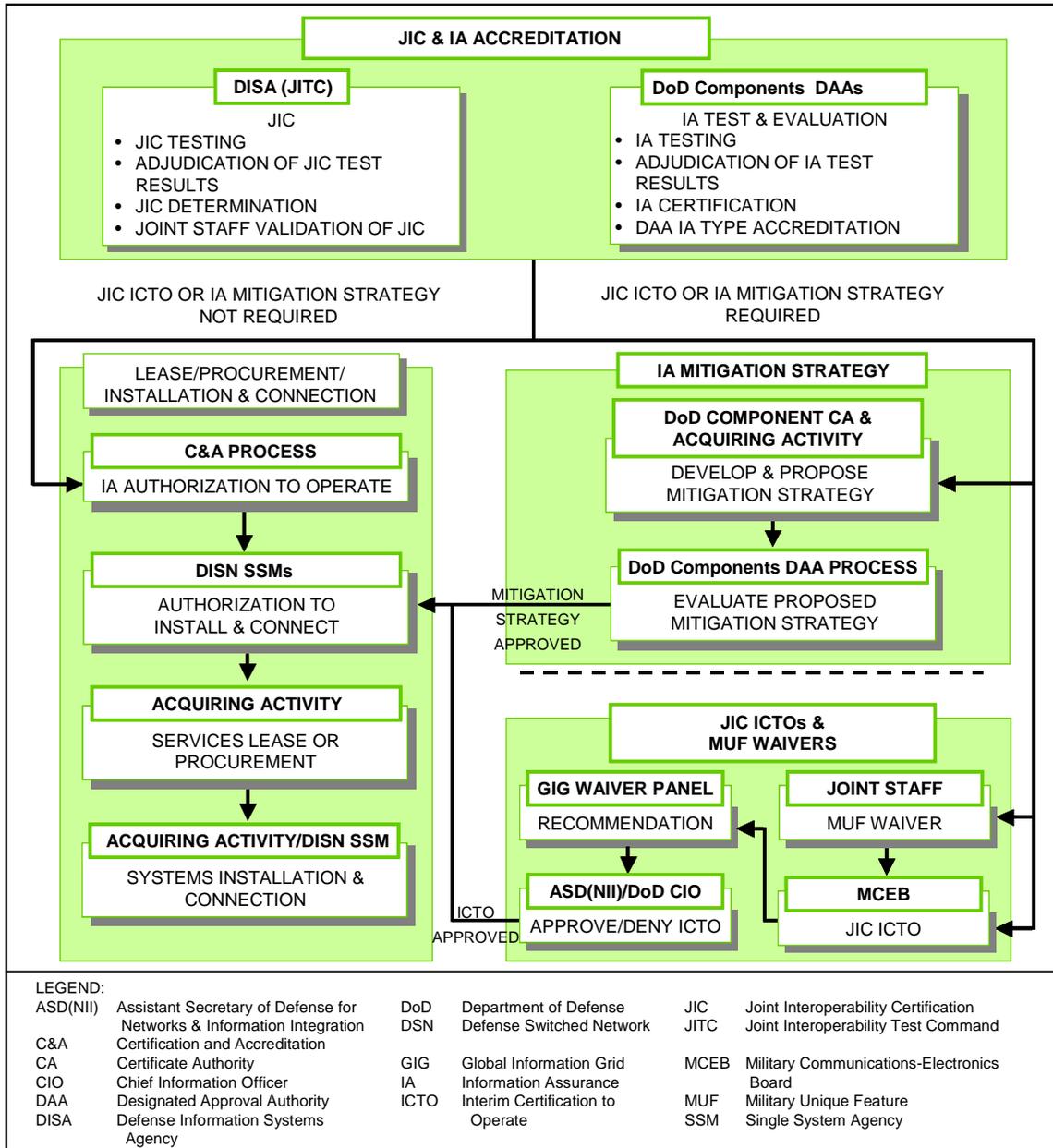


Figure 4-47. JIC and IA Certification and Accreditation Process Overview

3. Classified UC Products for IP E2E systems support SBU voice and video services
4. Network Infrastructure Products (e.g., DISN SDN /MILDEP Intranet and Terrestrial Transport Components Products).
5. Tactical Products

6. Encryption Products

Instant Messaging (IM) and Chat Collaboration UC are not considered to be stand-alone UC products; these are applications that create the possibility of real-time text-based communication between two or more participants over the network infrastructure. These UC features are included in the SBU UC Products for IP E2E systems support SBU voice and video services; Classified UC Products for IP E2E systems support SBU voice and video services; and in Tactical Products.

[Figure 4-48](#), Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each of the six UC product categories would be found under their appropriate section of the UC APL. Many UC products would show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE Routers, EBCs, and ASLANs that can be used for both SBU and Classified voice and video services.

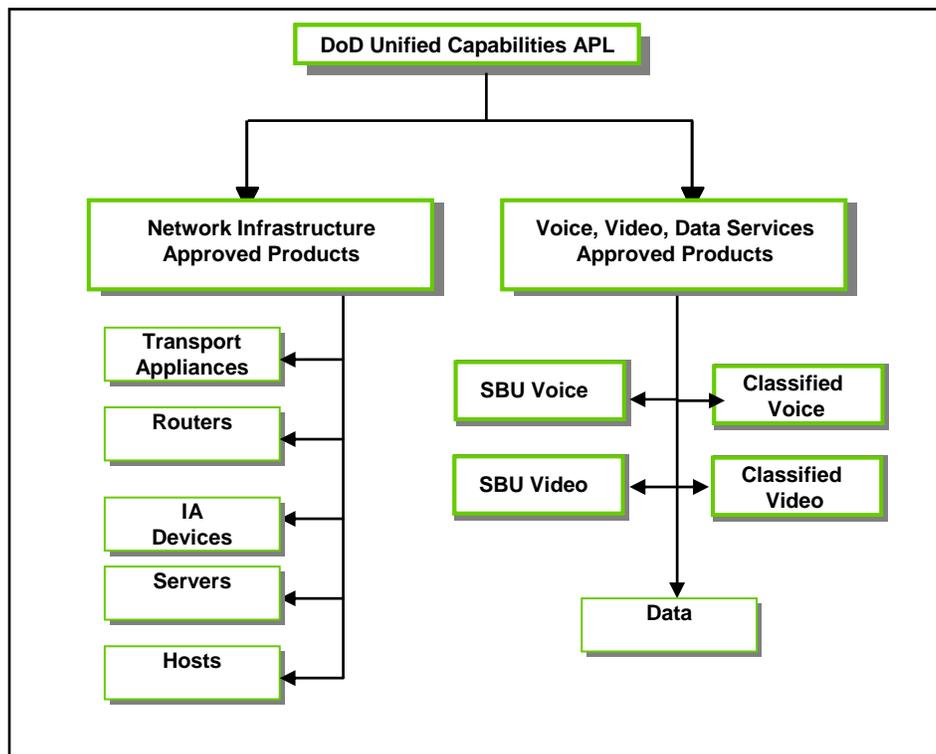


Figure 4-48. Overview of UC Product Categories within the DoD UC APL

[Figure 4-49](#), SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services, delineates the SBU UC products for IP E2E systems that support SBU voice

and video services. These UC products do not currently include video VTC MCUs but will in future updates.

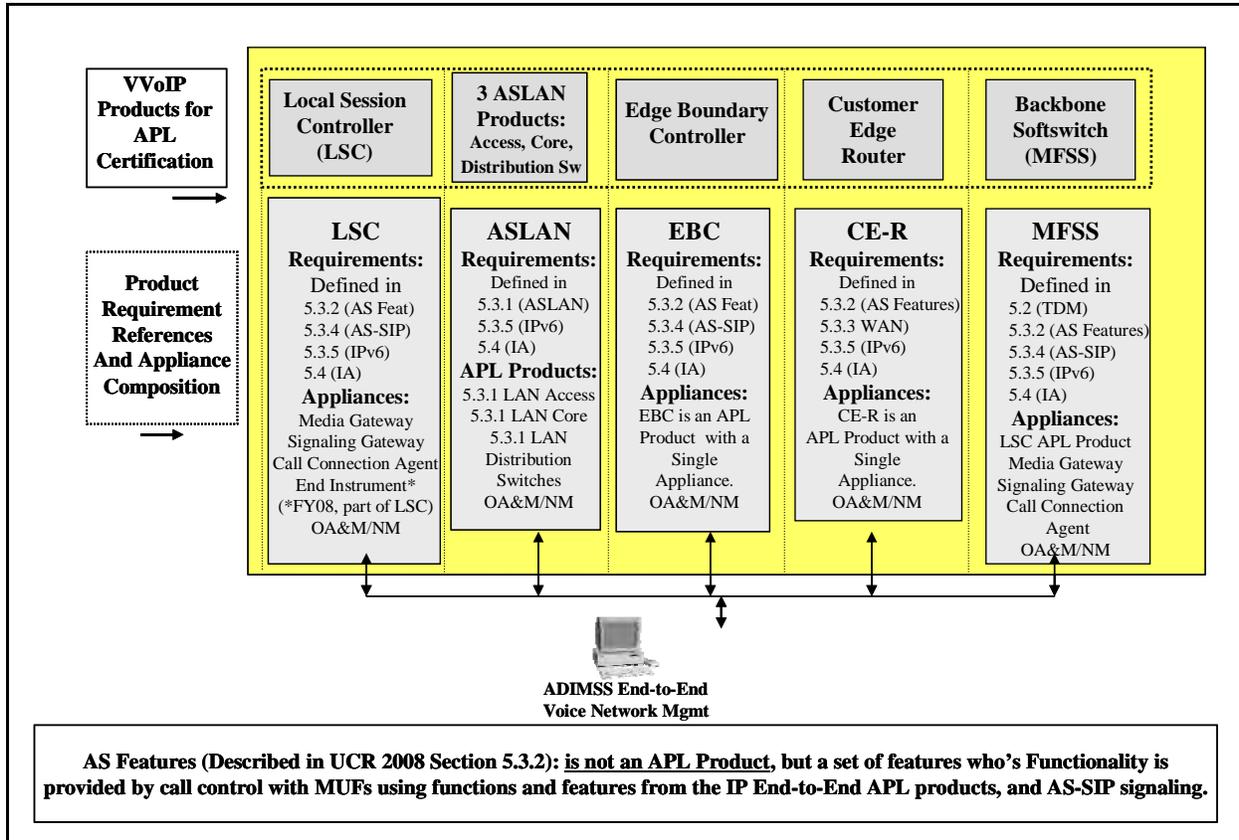


Figure 4-49. SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services

Table 4-5, UC Products for TDM-Based Switches with IP and EIs Only that Support SBU Voice and Video Services, delineates the UC products for TDM-based DSN Switches with IP on EIs only that support SBU voice and video services. Figure 4-50, Classified VoIP UC Products, delineates the Classified UC products.

Table 4-5. UC Products for TDM-Based Switches with IP on EIs Only that Support SBU Voice and Video Services

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
Multifunction Switch (MFS)	5.2	System providing local telephone service and tandem switching with full set of ASFs, including network traffic management Controls
End Office	5.2	System providing local telephone service and full set of ASFs including network traffic management Controls
Small End Office	5.2	Smaller version of the EO System providing local telephone service and full set of ASFs
Private Branch Exchange (PBX) Type 1	5.2	System providing local telephone service and MLPP capabilities
Private Branch Exchange (PBX) Type 2	5.2	System providing local telephone service without MLPP capabilities
Remote Switching Unit (RSU)	5.2	Small System providing local telephone service as an extension to an EO/SMEO or PBX.

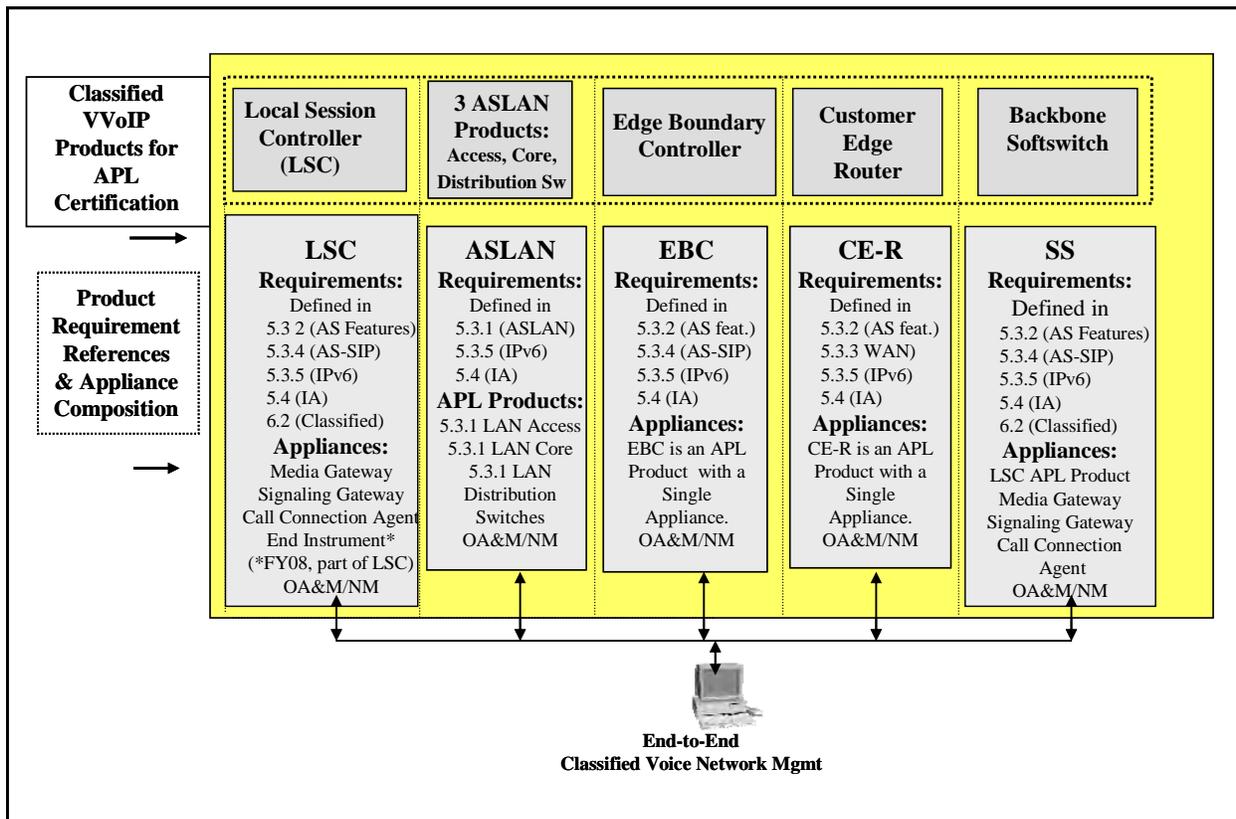


Figure 4-50. Classified VoIP UC Products

[Table 4-6](#), DISN Network Infrastructure UC Product Categories, delineates the Network infrastructure UC products, which can be used by all MILDEPs for their Intranets. These UC products do not currently include Data Firewalls but will in future updates.

Table 4-6. DISN Network Infrastructure UC Product Categories

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
M13	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
MSPP	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
Aggregation Router	5.5	System serving as a port expander for a PE Router
Provider Edge Router	5.5	System providing robust, high-capacity IP routing at the entry points to the DISN WAN
Provider Router	5.5	System providing robust, high-capacity IP routing in the DISN WAN
Optical Switch	5.5	Switching system providing high-speed optical transport in the DISN WAN
LEGEND DISN Defense Information Systems Network IP Internet Protocol MSPP Multi-Service Provisioning Platforms		PE Provider Edge WAN Wide Area Network

[Table 4-7](#), Tactical UC Product Categories and Paragraph Reference, delineates the Tactical UC products, and [Table 4-8](#), Encryption Products and Paragraph Reference, delineates the Encryption products. All of these UC products include IPv6 capability.

Table 4-7. Tactical UC Product Categories and Paragraph Reference

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	6.1.3	Tactical voice switch with ASF capabilities to support assured service requirements. This switch is used for rapid deployment situations and contingencies in the tactical environment
DVX Legacy (DVX-L)	6.1.3	Tactical voice switch with ASF capabilities to support assured service requirements. This switch is part of the TRI-TAC systems and thus termed Legacy
Deployable DSN PBX1	6.1.3	A DSN PBX1 used in the tactical arena When used in the tactical arena, the PBX1 is connected to a DSN EO through a STEP/Teleport
Tactical Network Elements	5.2.12.5 6.1.4	Network elements deployed in a tactical arena
Tactical LANs	5.3.1 6.1.5	LAN Deployed in a tactical arena
DCVX	6.1.6	Tactical cellular voice switch with ASF capabilities to support assured service requirements. This switch is used for rapid deployment situations and contingencies in the tactical environment
LEGEND ASF Assured Services Features COTS Commercial Off-the-Shelf DCVX Deployed Cellular Voice Exchange DSN Defense Switched Network DVX Deployable Voice Exchange DVX-C Deployable Voice Exchange–COTS DVX-L Deployable Voice Exchange–Legacy EO End Office LAN Local Area Network PBX1 Private Branch Exchange 1 STEP Standardized Tactical Entry Point TRI-TAC Tri-Service Tactical Communications		

Table 4-8. Encryption Products and Paragraph Reference

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
HAIPE	5.6	HAIPE is a programmable IP INFOSEC device with traffic protection, networking, and management features that provide IA services for IPv4 and IPv6 networks
Link Encryptors	5.6	Link Encryptors provide data security in a multitude of network elements, by encrypting point-to-point, netted, broadcast, or high-speed trunks.
LEGEND HAIPE High Assurance Internet Protocol Encryptor IA Information Assurance INFOSEC Information Security IPv4 Internet Protocol Version 4 IPv6 Internet Protocol Version 6		

4.5.1.2 Standard Process for Gaining APL Status

The standard process for gaining APL status for all of the UC Products identified in [Section 4.5.1.1](#), Overview of Approved Products, is shown in [Figure 4-51](#), Standard UC APL Product Certification Process. This process reflects that both IO and IA certifications are required for placement on the UC APL.

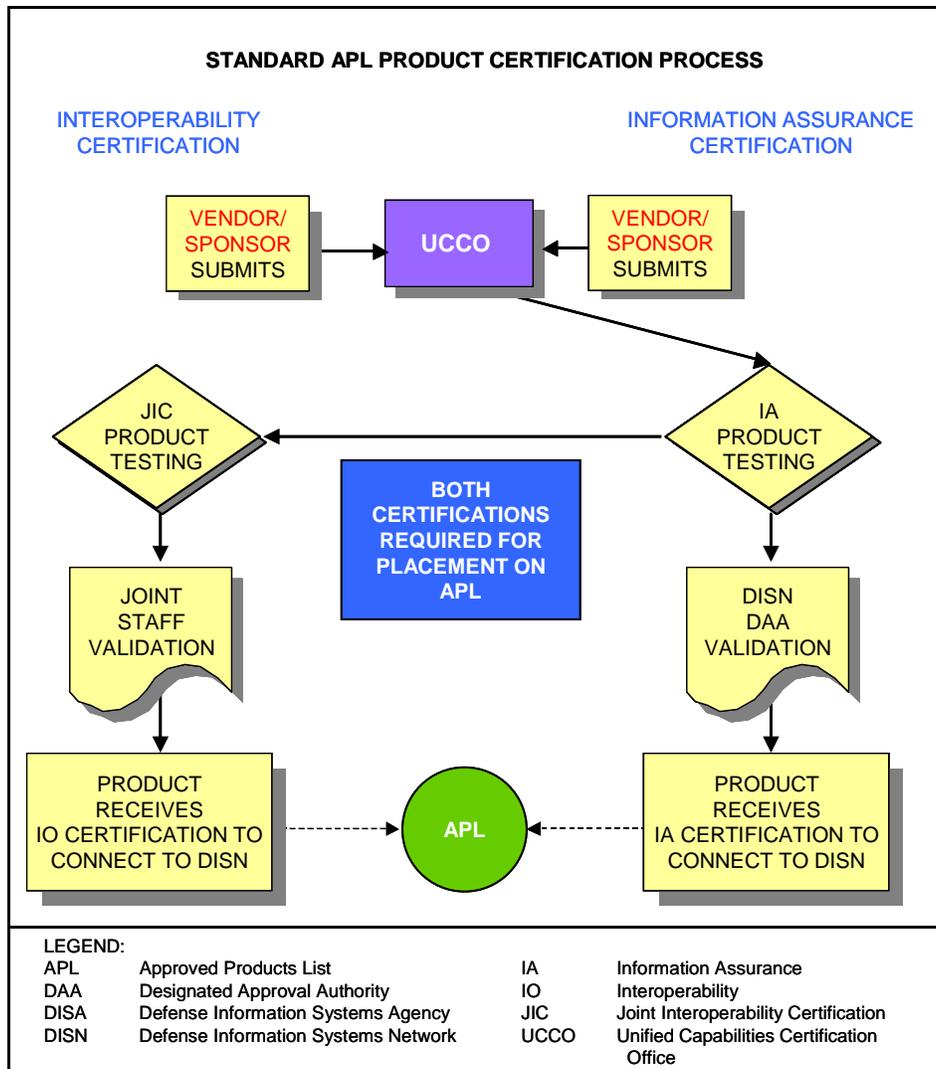


Figure 4-51. Standard UC APL Product Certification Process

The following set of rules applies to the standard APL process:

1. A product enters the UC APL process by obtaining sponsorship and providing both IA and IO information as shown in [Figure 4-51](#), Standard UC APL Product Certification Process.

Section 4 – Unified Capabilities Description and Key Processes

2. If a product successfully passed both the IA and IO portions of the testing, the product is placed on the UC APL. This listing is good for 3 years beginning as of the day the UCCO announces the vendor's APL status, if no product changes are made.
3. If software and/or hardware changes are made, the product must be recertified for new purchases.

Procedures allow for changing the requirements a product must meet to become UC APL certified. Changes can come about as a result of the following:

- New or evolving technology changes
- Policy changes
- Changes in operational environment obviating the need for an existing requirement (e.g., Mfg., Discontinued).

When a requirement addition/change/deletion has been approved as of the date the UCR is signed, one of three dispositions will occur as follows:

1. The vendors will have 18 months to develop it if it is new and not previously available. Vendors may provide it earlier.
2. If the requirement has been lessened, vendor compliance is immediate.
3. If warning of the requirements has been given before approval, the requirement compliance may be immediate.

Item 1 would be a new feature, not previously required, and the vendors did not have long-range knowledge of the requirement.

4.5.1.3 Approval to Connect and IA Approval to Connect Processes

Once a product is on the UC APL, authorization to connect to DISN should follow the following steps:

1. Conduct DIACAP.
 - a. Initiate and update C&A package.

2. Once ATO is achieved, each DoD Component site shall do the following to maintain the ATO:
 - a. Situational awareness
 - (1) Changes to infrastructure
 - (2) New security threats (IAVAs)
 - b. Continuous self-assessments
 - c. Monthly retina scans
 - d. Maintain assets in VMS
 - e. Prepare for reaccreditation
 - (1) Depends on length of accreditation OR if significant changes occur

3. Register with

- a. System/Network Approval Process (SNAP): NIPRNet Connection or Use existing registration User Service Information (USI) https://snap.dod.mil/cap_index.cfm
- b. SNAP: Register the LSC only in SNAP Uniform Resource Locator (URL):
<https://snap.dod.mil/dsn/capformpage1.cfm>
- c. Ports, Protocols, and Services Management (PPSM) registration:
<https://pnp.cert.smil.mil>
- d. Submit Authority to Connect (ATC) request for Voice/Video connection approval
URL: <http://www.disa.mil/dsn/jic/atcsubmittal.html>

NOTE: This should be the final step. At this step, the following information will be requested:

- (1) USI (for NIPR registration in SNAP)
- (2) USI (for LSC registration in SNAP)
- (3) Tracking number for PPSM registration

Acquisitions and installations shall use the general processes outlined as follows:

1. Acquisition organizations should structure their acquisitions to ask for the most current APL version of a system to be delivered at the time of scheduled installation.
2. A UC APL system that met STIGs at the time of purchase can continue to be purchased even if the STIGs have changed (often due to Information Assurance Vulnerability Alerts (IAVAs)) since the original APL status. Changes in STIGs shall be addressed at the time

when an Authority to Operate (ATO) is sought as part of the local DIACAP process used to install the system.

3. The retired UC APL allows organizations to continue to use the retired systems and they do not need to replace them after 3 years. Peripherals (e.g., telephones, interface cards) for systems on the retired list may still to be purchased even if the peripherals are retired.
4. DoD Components will install DSN systems and equipment in a manner that prevents unauthorized access to critical systems and equipment. Typically, this means that equipment will be placed in securely locked cabinets or in locked rooms providing access only to those individuals managing or supporting the system. Management systems and critical core equipment should be located in controlled access areas.
5. Furthermore, DoD Components will follow all applicable STIGs, as well as the deployment limitations, and vulnerability mitigations that are contained in the final IA security assessment report for the system. This report can be obtained from the Unified Capabilities Certification Office (UCCO) by e-mail request to:

ucco@disa.mil

Questions concerning the ATC process can be sent to:

ATCRequest@disa.mil.

General questions and other requests concerning the APL and ATC may be sent to:

ns534-Web@disa.mil

6. Additionally, DoD Components will follow DISA- or vendor-provided configuration guides, mitigation lists, and/or checklists that detail how to match the IA configuration that allowed the system to be IA certified and APL listed.
7. Installed systems will conform to the above security requirements and will be certified and accredited in accordance with processes and procedures outlined in the following paragraphs.

4.5.1.4 Links to the UCCO and Unified Capabilities APL Web Pages

Additional and current information concerning the APL process can be obtained from the following on-line sources:

1. DSN Connection Guide
 - a. http://www.disa.mil/gs/dsn/ops_connect.html
 - b. http://www.disa.mil/gs/dsn/Webfiles/dsn_connect_guide_05232005.pdf
2. DSN UC APL pages
 - a. http://www.disa.mil/gs/dsn/apl_process.html
 - b. <http://jtc.fhu.disa.mil/tssi/apl.html>

4.5.2 Use of UC Approved Products in (Tailored) Information Support Plans

(Tailored) Information Support Plans (TISP/ISPs) policies are defined in by CJCSI 6212.01D. In summary, TISPs take precedence over the APL process as follows: When the results from a TISP/ISP are approved by the Joint Staff, the program or device can interoperate with the DISN networks. The purpose of the Tailored ISP process is to provide a dynamic and efficient vehicle for certain programs to produce requirements necessary for Interoperability and Supportability Certification. Select program managers may request to tailor the content of their ISP. For programs not designated Office of the Secretary of Defense (OSD) Special Interest by ASD(NII)/DoD CIO, the Component will make the final decision of the details of the tailored plan subject to the minimums defined in CJCSI 6212.01D and any special needs identified by the J-6 for the Interoperability and Supportability Certification process. The final Component approved plan will be submitted to the DoD ISP (C4ISP) Assessment Tool via NIPRNET or SIPRNET for review by the Joint C4I Program Assessment Tool-Empowered (JCPAT-E).

Programs following the traditional three-stage ISP review process are not required to submit an ISP draft for review in advance of their Critical Design Review (CDR). Under the ASD(NII) ISP Pilot Program, the ISP review prior to the CDR is intended to give the PM another opportunity to influence system design and identify information related issues that can be resolved before the final development phase as well as provide a corresponding joint review prior to the Milestone C decision. Under the ISP Pilot Program, PMs still submit ISPs at Milestones B and C (IAW DoDI 5000.2 and DoDI 4630.8). The two-fold benefit of the ISP Pilot Program timing is to influence the CDR and to forestall late ISP submissions, which restrict comprehensive review prior to the Milestone C. [Figure 4-52](#), TISP/ISP Process, illustrates the TISP/ISP Process.

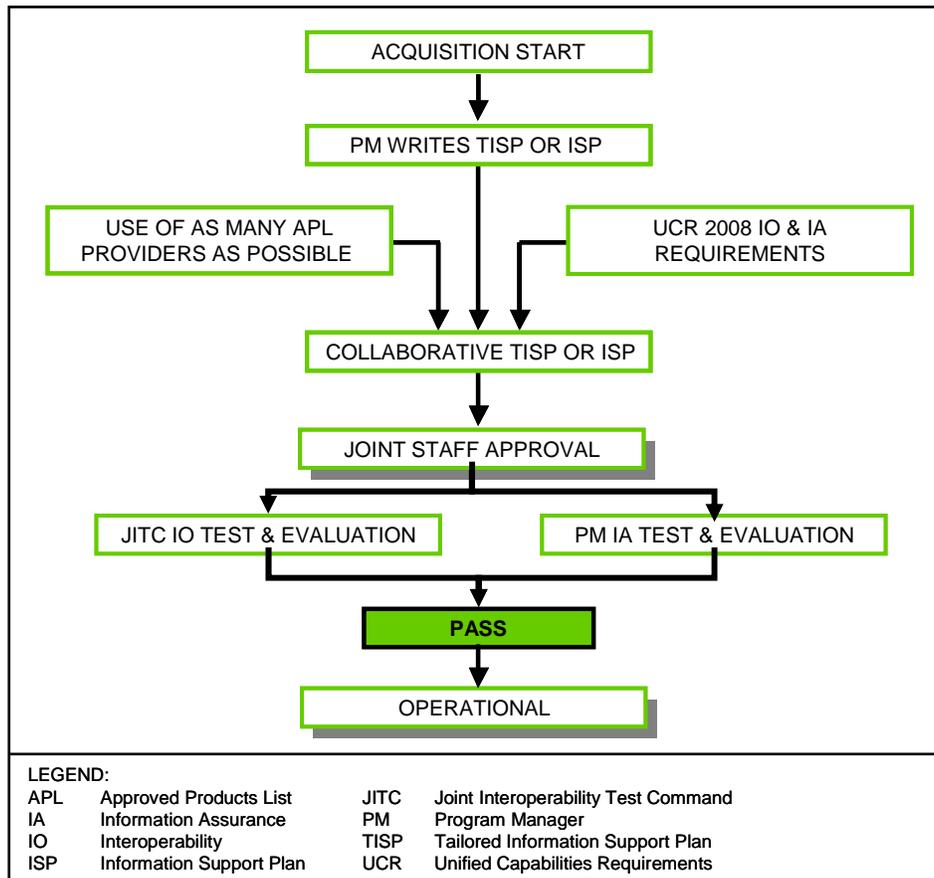


Figure 4-52. TISP/ISP Process

The UCR 2008 must be used and the TISP/ISP Program Management team must collaborate with the DISA UCR team to reach agreement on the IO and IA requirements to be used for the TISP/ISP. The Joint Staff will not approve and the JITC will not test a program that has not pre-coordinated with the DISA UC team.

4.5.3 APL Process for Deployment of IP-Based DISN Voice and Video Capabilities

The approach taken to achieve APL status for the new, converged IP-based voice and video and UC systems is a modification to the standard APL process. The modified approach will leverage the DISN VVoIP capabilities deployment processes outlined in the following sections. In summary, the standard APL process will be modified to reflect two deployment spirals and the following three test phases:

- UC Assessment Prototype Phase
- UC Assessment Preproduction Phase

- UC Spiral 1 or 2 Operational Testing Phase

4.5.3.1 APL Process Modified for the VVoIP Assessment Prototype Phase

Figure 4-53, APL Process Modified for the VVoIP Assessment Prototype Phase, illustrates the APL process as modified for the Assessment Prototype Phase. At the end of the JIC product and IA product testing, the tracking number will be retired and the prototype phase declared completed. The results are then reviewed by the DSAWG, and upon DISN Spirals DAA validation, the product receives authorization to proceed to preproduction.

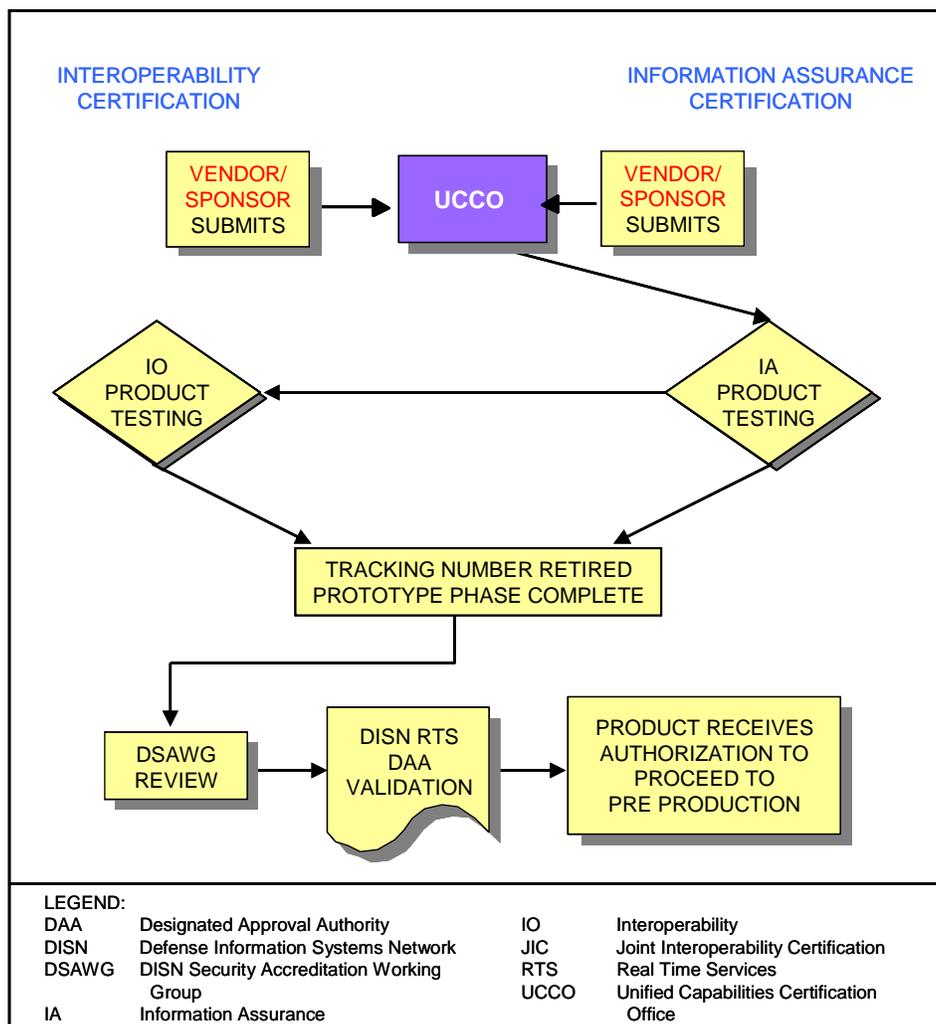


Figure 4-53. APL Process Modified for the VVoIP Assessment Prototype Phase

4.5.3.2 APL Process Modified for the VVoIP Assessment Preproduction Phase

Figure 4-54, VVoIP Assessment Preproduction Phase, illustrates the APL process as modified for the Deployment Assessment Preproduction Phase. At the end of this phase, we have a fully assessed VVoIP overlay, and the product is pre-approved to connect to DISN by receiving Interim Authority to Test (IATT) or Interim Authority to Operate (IATO) to connect. The product can then enter the live deployment.

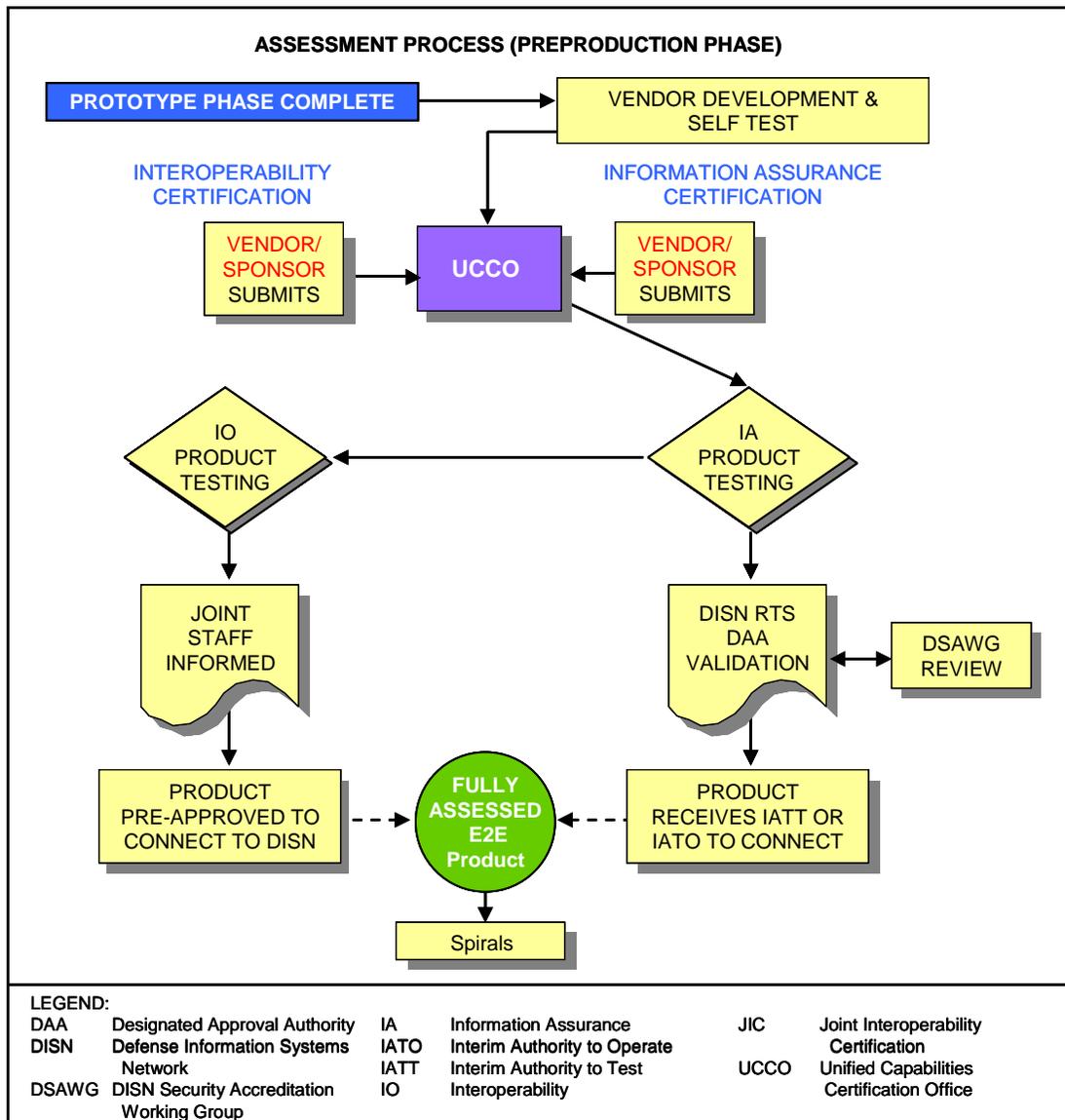


Figure 4-54. VVoIP Assessment Preproduction Phase

4.5.3.3 APL Process Modified for the UC Spiral 1 or 2 Operational Testing Phase

Figure 4-55, UC Spiral 1 or 2 Operational Testing Phase, illustrates the UC Spiral 1 or 2 Operational Testing Phase. At the end of the Spiral 1 or 2 Operational Testing Phase, and upon Joint Staff validation of the JIC test results and DAA validation, the product is placed on the APL.

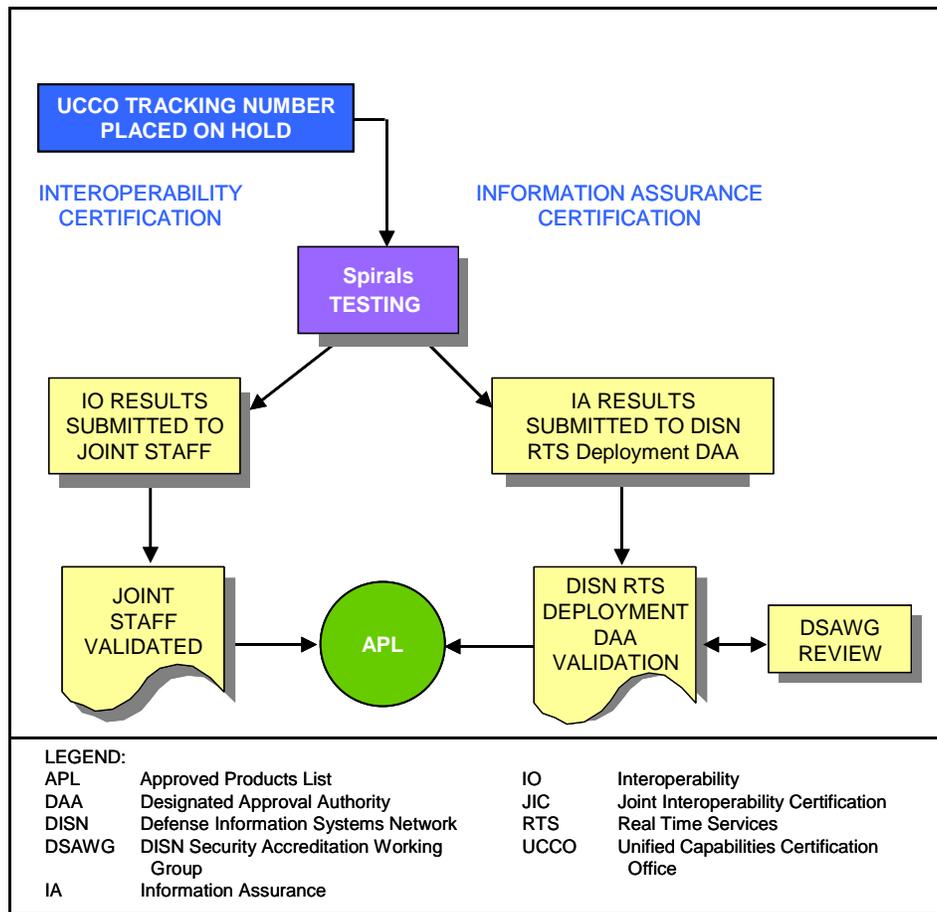


Figure 4-55. UC Spiral 1 or 2 Operational Testing Phase

4.5.3.4 VVoIP Assessment and Deployment Timelines

Figure 4-56, VVoIP Assessment Timeline, shows the VVoIP Assessment Timeline, and Figure 4-57, VVoIP Assessment Timeline (Post Fully Assessed Deployment Approval), shows the VVoIP Assessment Timeline (Post Fully Assessed Deployment Approval).

Section 4 – Unified Capabilities Description and Key Processes

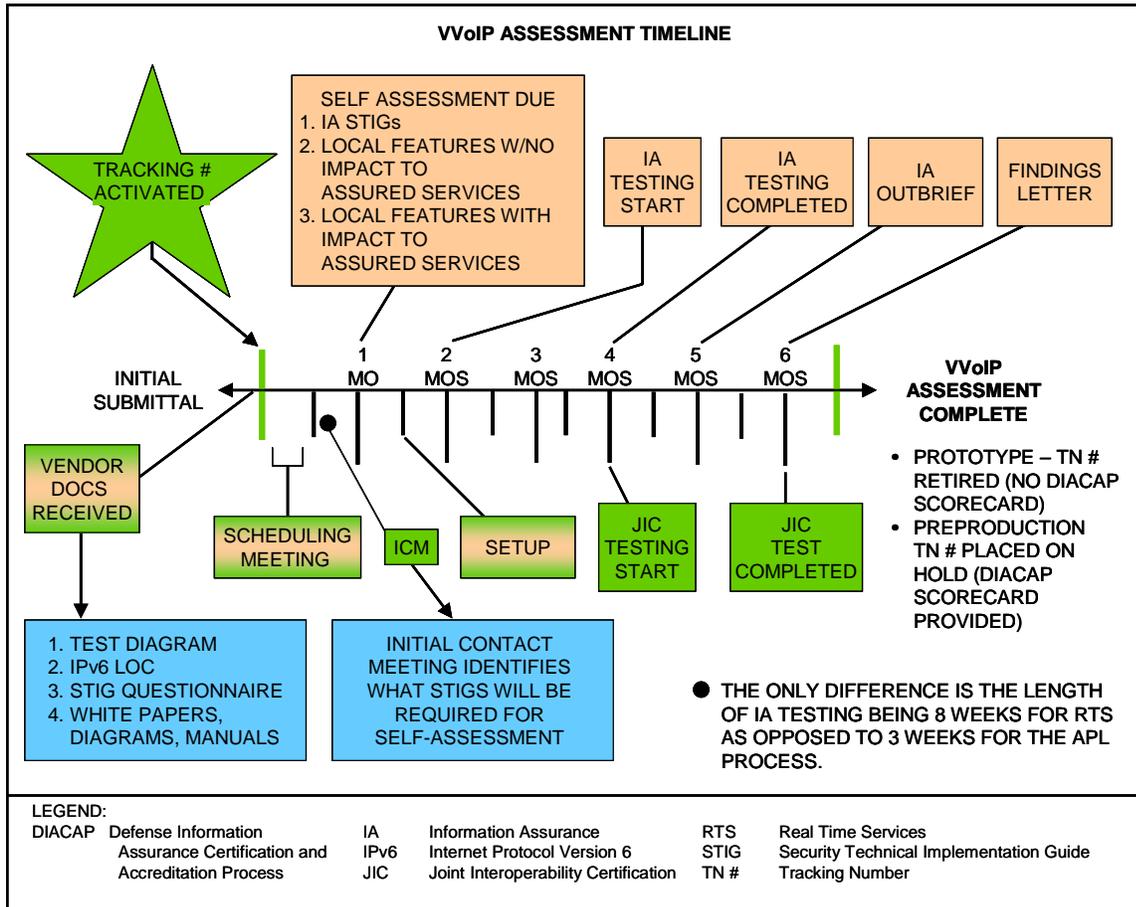


Figure 4-56. VVoIP Assessment Timeline

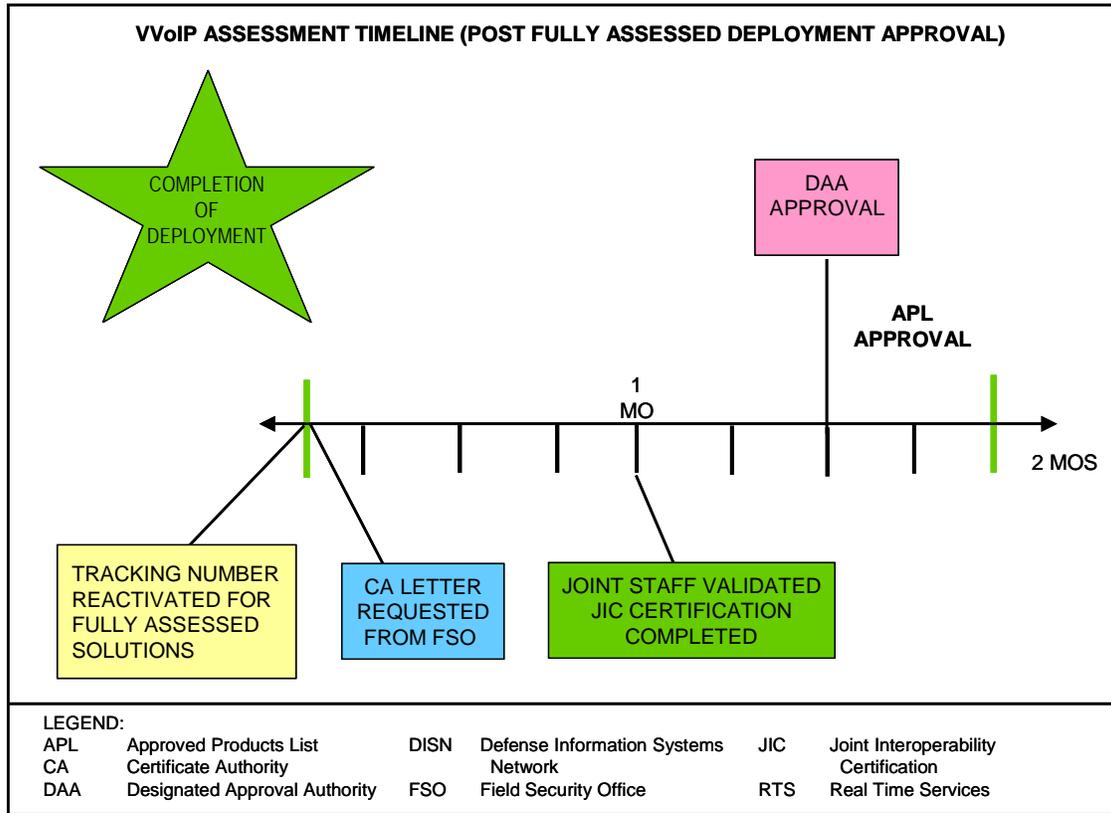


Figure 4-57. VVoIP Assessment Timeline (Post Fully Assessed Deployment Approval)

Once the Spiral 1 deployment is completed, UC solutions will enter the standard DoD UC APL process described in UCR 2008, [Section 4.5.1.2](#), Standard Process for Gaining APL Status.

THIS PAGE INTENTIONALLY LEFT BLANK