

**Department of Defense
Unified Capabilities Requirements 2008 (UCR 2008)
Change 1**

Final



January 2010

**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), CHANGE 1

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

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.

SIGNATURE TO BE INSERTED HERE

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
SECTION 1 – PURPOSE	1
SECTION 2 – APPLICABILITY, DEFINITION, AND SCOPE	3
2.1 Applicability	3
2.2 UC Definition.....	3
2.3 Scope of Document.....	4
SECTION 3 – POLICY	5
3.1 Introduction.....	5
3.1.1 UC Policy Documents	5
SECTION 4 – UNIFIED CAPABILITIES DESCRIPTION AND KEY PROCESSES	9
4.1 Overview.....	9
4.2 Unified Capabilities Services Description	9
4.3 Mission Capabilities.....	11
4.3.1 Assured Services Features	12
4.4 Migration to Unified Capabilities	15
4.5 Unified Capabilities E2E Networks Description	17
4.5.1 IP-Based Design for Unified Capabilities	20
4.5.1.1 Overview of VVoIP Network Design Attributes.....	22
4.5.1.1.1 Queuing Hierarchy for DISN IP Service Classes.....	24
4.5.1.1.2 Customer Edge Segment Design	25
4.5.1.1.3 Network Infrastructure E2E Performance (DoD Intranets and DISN SDNs).....	33
4.5.1.1.4 E2E Protocol Planes.....	35
4.5.1.1.5 ASAC Component	36
4.5.1.1.6 Voice and Video Signaling Design.....	40
4.5.1.1.7 Information Assurance Design	43
4.5.1.1.8 Network Management Design	46
4.5.1.2 Relationship between UC Network Description and Products to be Tested for APL Certification	48
4.5.1.3 Role of LSCs as Replacement for Existing Switching Systems	50
4.5.1.4 Classified VoIP Network Design.....	50
4.5.1.5 VTC Network Design	50
4.5.1.6 DISN Router Hierarchy	52

	4.5.1.7	IPv6 Network Design.....	52
4.5.2		Unified Communications.....	53
	4.5.2.1	UC Network-wide Collaboration Services	54
	4.5.2.2	UC Network-wide Collaboration Services Capability Increments.....	54
	4.5.2.3	UC Network-wide Collaboration Services Capability Interoperability.....	55
4.5.3		Service Portability.....	56
4.6		UC Products, APL Processes, and Connection Processes	58
	4.6.1	Overview of Approved Products	58
4.6.2		Overview of UC Interoperability and Information Assurance Processes	62
4.6.3		Unified Capabilities Certification Office Processes	65
	4.6.3.1	Standard Process for Gaining APL Status	66

LIST OF FIGURES

<u>FIGURE</u>	<u>PAGE</u>
3.1.1-1 UC Policy and Technical Reference Documents	6
4.4-1 DISN Evolution Spirals	16
4.5-1. E2E IP Network Description	18
4.5-2. High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments	20
4.5.1-1 Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site	22
4.5.1-2. Overview of VVoIP Network Attributes	23
4.5.1-3 Queuing for the Bearer Design	24
4.5.1-4 B/P/C/S-Level Voice over IP LSC Designs.....	27
4.5.1-5 B/P/C/S Video over IP LSC Designs.....	30
4.5.1-6 ASLAN Requirements Summary	31
4.5.1-7 Three Categories of ASLANs	32
4.5.1-8. An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users	34
4.5.1-9 Measurement Points for Network Segments.....	35
4.5.1-10 Assured Services Functions	36
4.5.1-11 Open Loop ASAC Network Design	37
4.5.1-12 Open Loop ASAC for SBU Voice and Video	38
4.5.1-13 Converged VVoIP Design: Signaling, QoS, and Assured Service	40
4.5.1-14 SBU Voice and Video Services Signaling Design	41
4.5.1-15 E2E Two-Level SBU AS-SIP Network Signaling Design	43
4.5.1-16 Information Assurance Protocols.....	44
4.5.1-17 IP External Interfaces to the LSC or MFSS.....	45
4.5.1-18 ASLAN Enclave Boundary Security Design.....	46
4.5.1-19 Role of RTS EMS in DISN OSS	47
4.5.1-20 RTS EMS Role in Providing E2E GEM.....	48
4.5.1-21 Classified VoIP Network Design Illustration	50
4.5.1-22 DISN DSMCU Design Hybrid Operations.....	51
4.5.1-23 DISN Router Hierarchy	52
4.5.1-24 IPv6 Design for SBU and Classified VVoIP	53
4.5.2-1 UC Network-Wide Collaboration Services Objectives	54
4.5.2-2 UC Pilot Increments.....	55
4.5.2-3 Interoperability/Federation of IM, Chat, and Presence.....	56
4.5.3-1 Mobile Warfighter’s Communication Dilemma.....	57
4.6.1-1 SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services	59

Table of Contents

4.6.1-2 Classified VoIP UC Products.....60
4.6.2-1 UC Requirements, Interoperability Certification, and Connection Approval Process 63
4.6.2-2 UC Information Assurance Certification and Accreditation Process64
4.6.3-1 Standard UC APL Product Certification Process67

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
3.1-1	Major Policies Addressed by UCR	5
4.5.1-1	LAN Requirements Summary	33
4.5.1-2	Summary of IP-Based Appliances and UC APL Products	49
4.6.1-1	DISN Network Infrastructure UC Product Categories	61
4.6.1-2	Deployable UC Product Categories and Paragraph References	61
4.6.1-3	Security Devices and Paragraph Reference	62
4.6.3-1	Service Complexity vs. Technology Maturity Matrix for Determination of Type of APL Process	66
4.6.3-2	New Features and Products in UCR for Which 18-Month Rule Applies	69

SECTION 1 PURPOSE

1.1 The “Department of Defense Unified Capabilities Requirements 2008 (UCR 2008) Change 1” (hereinafter referred to as “UCR 2008, Change 1”), specifies the technical requirements for certification of approved products to be used in Department of Defense (DoD) networks to provide end-to-end (E2E) Unified Capabilities (UC).

1.2 The UCR 2008, Change 1, augments UCR 2008, dated 22 January 2009.

1.3 The UCR establishes the governing policy for UC products and services supported on DoD networks.

1.4 The UC benefits of leveraging emerging technologies to the warfighter include the following:

- Global fixed and deployable E2E Interoperability over Internet Protocol (IP):
 - Resolution of Interoperability, Information Assurance, and performance issues.
 - Conducting DoD UC Operational Trial (Pilot) in Spirals.
- Network Operations (NETOPS): Enables integrated network management (NM) for performance monitoring (PM) and situational awareness (SA).
 - Enhanced situational assessments and information availability:
Proliferation of IP-addressed sensors, munitions, biosensors, and logistics tracking applications.
- Voice and Video management consolidates at Defense Information Systems Agency (DISA) and Service Network Operations and Security Centers (NOSCs).
- Potential cost savings: Reduced footprint, personnel, training, and operations and maintenance costs.
- Integrated operations: Ubiquitous, robust, and scalable E2E networks.
- Information Assurance specifications: Establishes rigorous specifications and governance to reduce exposure to threats.

Section 1 – Purpose

- New Information Assurance strategies that support mission assurance:
E2E security, authentication, and non-repudiation.
- Increased operations tempo: Rapid reorganizational capabilities, shared SA, and improved wireless and mobility support.
- Greater support for communications on the move.
- Improved multicasting: Dynamic formation of communities of interest (COIs).
- Real-time collaboration: Integrated voice, video, and data capabilities.
- SA using NETOPS COI information sharing.
- Quicker, more dynamic responses: Rapid and agile Information Technology (IT) infrastructures with the capability to “discover” adjacent networks and plug-n-play.
- Provision of approved products for Combatant Commanders/Services/Agencies (CC/S/As) to purchase.

SECTION 2 APPLICABILITY, DEFINITION, AND SCOPE

2.1 APPLICABILITY

The UCR applies to:

1. The Office of the Secretary of Defense (OSD), the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (COCOMs), the Office of the Inspector General of the DoD, the defense agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).
2. All equipment or software (hereinafter referred to as “UC products” or “products”) and services that provide or support UC during each phase of those products’ life cycles, from acquisition to operations, including:
 - a. All UC products and end-to-end voice, video, and data services acquired or operated by the DoD Components or by authorized non-DoD users (e.g., combined or coalition partners and U.S. Government departments and agencies). Authorized non-DoD network users are required to comply with approved interfaces contained in Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD Chief Information Officer (DoD CIO) publication, “DoD Unified Capabilities Requirements (UCR)”).
 - b. All products and technologies used to send and receive or to support voice, video, or data across DoD networks that provide UC services.
 - c. DoD Components’ planning, investment, development, acquisition, operations, and management of DoD networks that provide UC services.
3. DoD Components’ Programs of Record, specifically those governed by DoD Directive (DoDD) 5000.01, DoD Instruction (DoDI) 5000.02, and CJCS Instruction (CJCSI) 3170.01G are not subject to the provisions of this publication; however, are encouraged to use UC certified products in the development of programs, where appropriate.

2.2 UC DEFINITION

Unified Capabilities are the integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. Unified

Capabilities integrates standards-based communication and collaboration services including, but not limited to: messaging; voice, video, and web conferencing; and unified communication and collaboration applications or clients. These standards-based UC services are integrated with available enterprise applications, both business and warfighting.

2.3 SCOPE OF DOCUMENT

The UCR consists of the following seven sections:

1. Section 1, Purpose, for the UCR.
2. Section 2, Applicability, Definition, and Scope, of the UCR.
3. Section 3, Policy, provides a broad overview of policies that will be implemented in the UCR with emphasis on policies that govern Information Assurance and Interoperability requirements and testing of products used to provide DoD UC.
4. Section 4, Unified Capabilities Description and Key Processes, provides an overview of UC services and the core processes needed for a vendor's product to gain placement on the DoD UC Approved Products List (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 DoD UC APL. Section 5 also contains Change sheets that identify changes for which the 18-month rule applies.
6. Section 6 contains unique requirements: Section 6.1, Unique Requirements for Deployable Products, and Section 6.2, Unique Classified VVoIP Requirements.
7. Section 7, Product Categories Requirements Matrix, contains a high-level requirements matrix, which is a summary of the requirements defined in Sections 5 and 6 for the UC product categories and the products within those categories.
8. Appendix A, Definitions, Abbreviations and Acronyms, and References, contains the definitions, abbreviations, acronyms, and references applicable to the UCR.

Sections 1 through 4 are intended to serve as the summary of the UCR. Sections 5 and 6 are intended for product vendors and testers.

SECTION 3 POLICY

3.1 INTRODUCTION

This section provides a broad overview of policies that will be implemented in the UCR. The overview is focused on policies that govern Information Assurance and Interoperability verification and testing of systems and components used in providing UC. The UCR translates the mission-based requirements outlined by the major policies listed in [Table 3.1-1](#), Major Policies Addressed by the UCR, into requirements that allow vendors to develop the functionality needed to meet those mission-based requirements, and for the DoD Distributed Test Laboratories to conduct the testing necessary to place those products on the DoD UC APL.

Table 3.1-1. Major Policies Addressed by UCR

DoDI 8100.ee, “Department of Defense Unified Capabilities,” Draft, October 2009
DoDD 5144.1, “Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO),” May 2, 2005
DoDD 8000.01, “Management of the Department of Defense Information Enterprise,” February 10, 2009
DoDI 8100.3, “Department of Defense (DoD) Voice Networks,” January 16, 2004 (hereby canceled)
ASD/(NII) Memorandum, “Department of Defense Unified Capabilities Requirements,” current edition
DoDD 4630.05, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 5, 2004
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,” October 24, 2002
DoDI 8500.2, “Information Assurance Implementation,” February 6, 2003
DoDI 8510.01, “DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP),” November 28, 2007
DoDI 8410.02, “DoD NETOPS for the Global Information Grid (GIG),” December 19, 2008

3.1.1 UC Policy Documents

[Figure 3.1.1-1](#), UC Policy and Technical Reference Documents, illustrates the relationships among the documents that drive, execute, and implement UC migration and technology insertions.

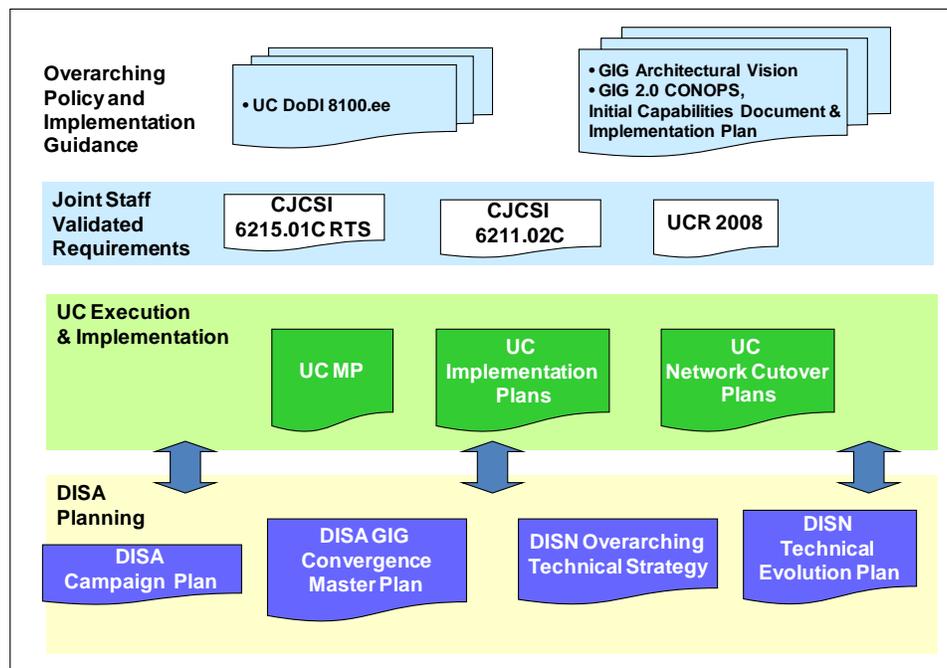


Figure 3.1.1-1. UC Policy and Technical Reference Documents

The overarching policy and implementation guidance for UC is provided by the ASD(NII)/DoD CIO “Global Information Grid (GIG) Architectural Vision” (hereinafter referred to as “GIG Architectural Vision”) and the Joint Staff “Global Information Grid 2.0 (GIG 2.0) Concept of Operations (CONOPS)” (hereinafter referred to as “GIG 2.0 CONOPS”) and “Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD),” (hereinafter to as “GIG 2.0 ICD”) and the “GIG 2.0 Implementation Plan” (hereinafter referred to as “GIG 2.0 Implementation Plan”). The major drivers of UC migration are the DoD objective enterprise architecture as defined by the “GIG Architectural Vision” and the Joint Staff-validated strategic requirements in the “GIG 2.0 ICD.” This objective enterprise architecture is driven by emerging IP and changing communications technologies, which recognizes evolving communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to a single device, wired to wireless, non-real time to real time, and scheduled to ad hoc.

The following five GIG 2.0 critical characteristics with the UC initiatives addressing them in parentheses are as follows:

- Global Authentication, Access Control, and Directory Services (UC Portable Assured Services in UC Pilots, UCR and APL Products)
- Information and Services “from the Edge” (UC Assured Services to Deployed Tactical Units Based on the UCR and APL Products)

- Joint Infrastructure (NETOPS to Enable Information Sharing across a Diverse Spectrum of Operational Requirements)
- Common Policies and Standards (UCR and Test Programs for UC Spirals and for APL Products)

- Unity of Command (NETOPS for UC Response to Situational Awareness)

Joint Staff-validated requirements for Real Time Services (RTS), which are critical UC, are initially addressed in CJCSI 6215.01C, “Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS).” CJCSI 6211.02C, “DISN: Policy and Responsibilities,” provides the connection approval processes for the Defense Information System Network (DISN), and is applicable to UC within the DISN. The ASD(NII)/DoD CIO document, “DoD Unified Capabilities Requirements (UCR) 2008,” contains the first comprehensive Joint Staff-validated requirements for UC.

Unified Capabilities execution and implementation documents essential to synchronizing investments across DoD by the DISA and other DoD Components are the UC MP, the UC implementation plans, and the UC network cutover plans (NCPs). The UC MP defines three spiral timeframes (i.e., near-, mid-, and far-term) to be used as context for DoD Components’ Program Objective Memorandum (POM) actions. The UC implementation plans synchronize the deployment of UC based on DoD Components’ acquisition plans by fiscal year (FY) quarter. The UC NCPs ensure the readiness of UC site installations as they become operational.

DISA has four major planning documents that are both driving and supporting the UC planning activities. The first is the “DISA Campaign Plan,” which identifies areas of focus with the UC initiatives addressing them in parentheses as follows:

- Enterprise Infrastructure (UCR and Test Programs for UC Spirals and for APL Products)
- Command and Control and Information Sharing (UCR and NETOPS)
- Operate and Assure (NETOPS and APL Products)

The second document is the DISA GIG Convergence Master Plan (DGCMP) that identifies four categories with the UC initiatives addressing them in parentheses as follows:

- Applications, Services, and Data (UC Collaboration Services Non-Assured Services (AS) with Quality of Service (QoS) and AS with QoS)
- Communications/Networks (UC E2E Assured Services via UCR and APL Products)

Section 3 – Policy

- Information Assurance (E2E Information Assurance UCR and Information Assurance Governance)
- NETOPS/Enterprise Management (NETOPS CONOPS/Joint Tactics, Techniques and Procedures (JTTPs), RTS Element Management System (EMS)/Probes)

The third and fourth documents are the “DISN Overarching Technical Strategy (DOTS)” and the “DISN Technology Evolution Plan (DTEP),” shown in Figure 3.1-1, UC Policy and Technical Reference Documents. The DOTS addresses “what” DISA is doing from a technology perspective for DISN. The DTEP addresses “how” and “when” for the DISN UC technical migration. The DTEP includes a section on DISN UC evolution and a section on DISN UC deployment. Both documents address the technology migrations outlined in the “DoD Unified Capabilities Requirements (UCR).” The “UC MP” is consistent with these DISN documents, as well as DoD Components’ UC technology implementation plans. The DOTS and the DTEP identify four key capabilities with the UC initiatives addressing them in parentheses as follows:

- Information Assurance (E2E Information Assurance UCR and Information Assurance Governance)
- Connectivity (UCR)
- Network Management (NETOPS CONOPS/JTTPs, RTS EMS/Probes)
- Interoperability (UCR and Test Programs for UC Spirals and for APL Products)

SECTION 4

UNIFIED CAPABILITIES DESCRIPTION AND KEY PROCESSES

4.1 OVERVIEW

This section describes UC services, E2E UC network designs, the UC products that support those designs, and the core processes needed for a vendor to gain placement of its UC products on the DoD UC APL. Use of products from the DoD UC APL allows DoD Components to purchase and operate UC products over all DoD network infrastructures. This section applies to both fixed and deployable products that support UC services on DoD networks.

4.2 UNIFIED CAPABILITIES SERVICES DESCRIPTION

The major drivers of mission needs for UC services are the DoD objective enterprise architecture as defined by the “GIG Architectural Vision” and the Joint Staff-validated requirements in the “GIG 2.0 ICD.” This objective enterprise architecture is driven by emerging IP and changing communications technologies, which recognizes evolving communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to single device, wired to wireless, non-real time to real time, and scheduled to ad hoc.

Assured UC services are required to meet the requirements of the IP-enabled battlefield of the future. Unified Capabilities will allow the DoD to achieve the following:

- Ubiquitous, robust, and scalable E2E networks, enabling integrated operations.
- Proliferation of IP-addressed sensors, munitions, biosensors, and logistics tracking applications, which will enhance situational assessments and information availability.
- End-to-end security, authentication, and non-repudiation, which will enable new Information Assurance strategies that support mission assurance.
- Increased operations tempo supported by rapid reorganizational capabilities, shared SA, and improved wireless and mobility support.
- Greater support for communications on the move.
- Dynamic formation of COIs supported by improved multicasting.

- Real-time collaboration using integrated voice, video, and data capabilities.
- SA using NETOPS COI information sharing.
- Rapid and agile IT infrastructures with the capability to “discover” adjacent networks and plug-n-play to facilitate quicker, more dynamic responses.

Unified Capabilities services that are addressed in the UCR 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/Calendar. 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. Calendar 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 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 (IM) 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 IM, presence is displayed.
 - a. Instant messaging 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 IM by being focused on group chat, or room-based chat. Typically, room persistence is a key feature of multiuser chat; in contrast with typically ad hoc IM capabilities.
 - c. Presence/Awareness is a status indicator that conveys ability and willingness of a potential user to communicate.
9. **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.
10. **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).

Each of these UC services need to be provided by networks that meet E2E performance standards for QoS, which are defined in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, for all DoD networks.

4.3 MISSION CAPABILITIES

Assured Services Features (ASFs) must be provided by UC networks based on the mission of the users consistent with their roles in peacetime, crisis, and war. 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. Even if requirements for assured services do not apply to all users at a site the Assured Information Protection features cannot be degraded.

In the operation of networks that provide UC services, the DoD Components shall comply with ASFs requirements, i.e., Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery) defined as follows:

1. **Assured System and Network Availability.** 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, failover, diversity, and elimination of critical failure points. This ASF supports user traffic during

peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed.

2. Assured Information Protection. Applies to information in storage, at rest, and passing over networks, from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers. Secure end devices shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication. The DoD networks that provide UC services 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 certified and accredited.
3. Assured Information Delivery. The requirement that DoD networks providing UC services have the ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war.

4.3.1 Assured Services Features

This section provides more specific mission capabilities associated with the three UC Assured Services of Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery. The DoD UC networks and services shall have the following ASF to provide these three UC Assured Services:

1. Assured System and Network Availability. Supports mission critical 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 (B/P/C/Ss) within a COCOM-defined geographic region of the COCOM's theater can be affected by an outage in the network.
 - c. Networks robustness through maximum use of alternative routing, redundancy, and backup.
 - d. To the maximum extent possible, transport supporting major installations (i.e., B/P/C/S, leased or commercial sites or 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.

2. Assured Information Protection.

- a. Secure EIs (SEIs) shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication.
- b. The UC networks shall be configured to minimize and protect against attacks that could result in denial or disruption of service.
- c. All hardware and software in the network must be Information Assurance certified and accredited and operated in accordance with (IAW) the most current Security Technical Implementation Guides (STIGs).

3. Assured 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, achieved under peacetime, crisis, and war situations.
- b. The DoD UC networks are required to provide precedence based assured services (PBAS) for delivery of UC services. Precedence based assured services (PBAS) requires the ability of the DoD UC networks to optimize session completion rates and, in some cases, prevent blocking of all mission-critical users' sessions despite degradation because of network disruptions, natural disasters, or surges during crisis or war. The DoD UC networks shall be designed with the capability to assign and reallocate resources on demand consistent with mission precedence. For voice and video sessions, PBAS shall allow higher precedence users to be provided with resources that had been allocated to lower precedence sessions. The PBAS is not required in the wide area network (WAN). Five precedence levels shall be provided. They are FLASH OVERRIDE (FO), FLASH (F), IMMEDIATE (I), PRIORITY (P), and ROUTINE (R). Authorization for origination of sessions that use these precedence levels to support mission-critical sessions shall be determined by the Joint Staff and COCOMs. All users shall be capable of receiving precedence UC services sessions since locations of crises and wars cannot be determine in advance.
- c. Unified Capabilities services must be responsive to the needs of FLASH and FLASH OVERRIDE sessions, that are provided nonblocking service (i.e., P.00 threshold) from user to user. (NOTE: P.00 is the probability that out of every 100 calls, the probability is that zero sessions will be blocked.)

- d. Precedence-based sessions placed to EIs that are busy with lower precedence-based sessions shall be absolutely assured completion to a live person. This shall be accomplished by immediate disconnection of the lower precedence session and immediate completion of the higher precedence session.
- e. **Visibility and Rapid Reconfiguration.** If blocking occurs to users' sessions caused by crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to SA to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock network operations centers (NOCs) that oversee voice, video, and data services. DISA shall oversee the DISN systems and shall have read-write access to DISN systems, which are shared with the military services for cost avoidance, such as the multifunction softswitch (MFSS) or WAN Softswitch (SS). All NOCs shall have EMSs that allow for read-write access for the systems for which they have direct responsibility. In addition, the Joint Task Force – Global Network Operations (JTF GNO)-sponsored NETOPS COI metadata standards and information sharing capabilities shall be used by all NOCs to share alarms, performance data, and trouble tickets. Information sharing shall allow for providing visibility E2E and for modifying the configuration of network components, as needed, to respond to SA. 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.
- f. Mitigation of blocking of sessions that occur during short-term traffic surges shall be accomplished via PBAS.
- g. During times of surge or crisis, the CJCS can direct implementation of session controls to allocate the use of resources in the network to meet mission needs.
- h. The global and theater networks 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.
- i. Unified Capabilities networks shall be designed with the capability to permit interconnection and interoperation with similar Services' deployable programs, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable.
- j. Unified Capabilities networks shall be designed to assure that E2E voice, video, and data performance are clear, intelligible, not distorted or degraded, using commercial standards performance metrics. The DoD UC networks shall be designed to meet

voice, video, and data performance requirements E2E. Deployed UC networks can provide degraded performance consistent with meeting mission needs as compared to fixed UC network performance.

4.4 MIGRATION TO UNIFIED CAPABILITIES

The DoD “UC MP” provides the details on the migration to UC services. This section provides an overview of that migration to assist the DoD Components acquisition organizations and product vendors in understanding how the products will be used to meet mission needs.

The purpose of the “UC MP” is to

1. Define DoD’s migration from the current legacy technologies to converged net-centric, IP-based voice, video, and data services.
2. Serve as a guideline to the DoD Components in the preparation of migration and acquisition plans for phasing out circuit-switched voice and video services and initially phasing in Voice and Video over IP (VVoIP) services, and other UC services that will operate in converged voice, video, and data networks. The “UC MP” addresses synchronization of life-cycle activities, from acquisition to operations, for networks that provide UC services.
3. Provide guidance for DoD Components’ POM submissions.

The challenges of UC migration and DoD Component budgets prevent the ability to install a common IP technology base as a global “flash cut.” Thus, networks based on hybrid technologies will be required for many years. The DISN Evolution Spirals (see Figure 4.4-1, DISN Evolution Spirals) have been structured to address these challenges.

The DoD UC migration strategy must be integrated with DISN and DoD Component implementation planning to sustain E2E capabilities in a hybrid technology environment. The “UC MP” is structured to synchronize the DoD Components’ migration to E2E voice, video, and data services as rapidly as resources allow, consistent with respective business cases and mission needs.

To support timely UC implementation, the migration strategy is structured to fully leverage DISN technical refreshment investments. The “UC MP” is based on the DISN Spiral timeframes to synchronize DISN and DoD Components investments. Figure 4.4-1, DISN Evolution Spirals, illustrates the Near-Term, Mid-Term, and Far-Term DISN Spirals that depict the evolution to the target capabilities and infrastructure. These three Spirals are as follows:

- Near-Term (FY 2008–2012) – Circuit-Switched to IP Convergence

- Mid-Term (FY 2013–2016) – Voice, Video, and Data to Shared IP Convergence
- Far-Term (FY 2017–2020) – Multiple Classifications to Unified IP Convergence

At the completion of each Spiral, UC services are implemented, both by the DoD Components and in the DISN infrastructure. As shown in Figure 4.4-1, network-oriented capabilities will evolve to enhanced service oriented capabilities.



Figure 4.4-1. DISN Evolution Spirals

Near-Term Spiral. This Spiral focuses on enhancing the DISN IP data and transport services to transition from asynchronous transfer mode (ATM) and time division multiplexing (TDM) circuit-switched technologies to IP-based networks. Ethernet will become the standard interface for all DISN services. Converged voice, video, and data services will begin during this Spiral.

Mid-Term Spiral. This spiral will focus on expanding converged voice, video, and data services by integrating service specific networks into a shared IP-based network using improved IP QoS, multicast, and session setup technologies. Ethernet-based transport services will support different classification levels. Command and control applications will remain separate from the IP networks for mission assurance. High Assurance Internet Protocol Encryptor (HAIPE) deployments will be expanding. The phaseout of separate legacy circuit-based voice, video, and data networks in the DISN Mid-Term Spiral will expand as customers migrate to enhanced DISN IP data services. Assured services will provide availability, information protection, and optimized information delivery.

Far-Term Spiral. This Spiral will focus on the DoD CIO's vision for net-centricity by establishing highly available, resilient, and secure IP-based networks, to include command and

control applications. This DISN spiral will support user-encrypted, IP-based voice, video, and data services at all classification levels over a unified customer interface.

4.5 UNIFIED CAPABILITIES E2E NETWORKS DESCRIPTION

This section provides a description of the E2E networks that use the UC products specified in Sections 5 and 6 that

- Establish the requirements needed by industry to develop requirements-compliant Unified Capability solutions,
- Provide the foundation for the development of Unified Capability Test Plans (UCTPs) for Interoperability and Information Assurance testing. These tests are used to make the certification decisions necessary to place products on the DoD UC APL.
- Provides Information Assurance requirements necessary for UC products to meet DoD Information Assurance policy to become approved products. Later, these Information Assurance requirements will be used to assist in the development of the STIGs needed to operate properly UC approved products once installed, and
- Identify only the MINIMUM requirements and features applicable to all DoD networks that support UC, which include voice and video operating in IP, converged networks with data services.

Sections 5 and 6 do 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, because these features do not provide interoperability with multiple vendors.

Specifically, this UCR specifies technical requirements for assured Interoperability and Information Assurance of products that provide the following set of UC, which will be expanded in the future:

- Voice and video services point-to-point
- Voice conferencing
- Videoconferencing
- E-mail/calendaring
- Unified messaging
- Web conferencing and web collaboration
- Unified conferencing
- Instant messaging and chat

differences. In addition, the current DISN Video Services (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 network design. Since the circuit-switched TDM-based network is well established, the following subsections provide a UC network overview by first describing VVoIP subsystems followed by an overview of the TDM-based DSN design.

[Figure 4.5-2](#) shows the three major E2E network segments: Customer Edge, Network Edge, and the Network Core (DISN SDNs and WAN Transport), which are all part of the UC E2E. End users attach to the Customer Edge Segment, consisting of either a TDM-based End Office (EO), or the set of VVoIP components of LSC, EBC, CE Router, and ASLAN. The Network Edge and the DISN Network Infrastructure are 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.

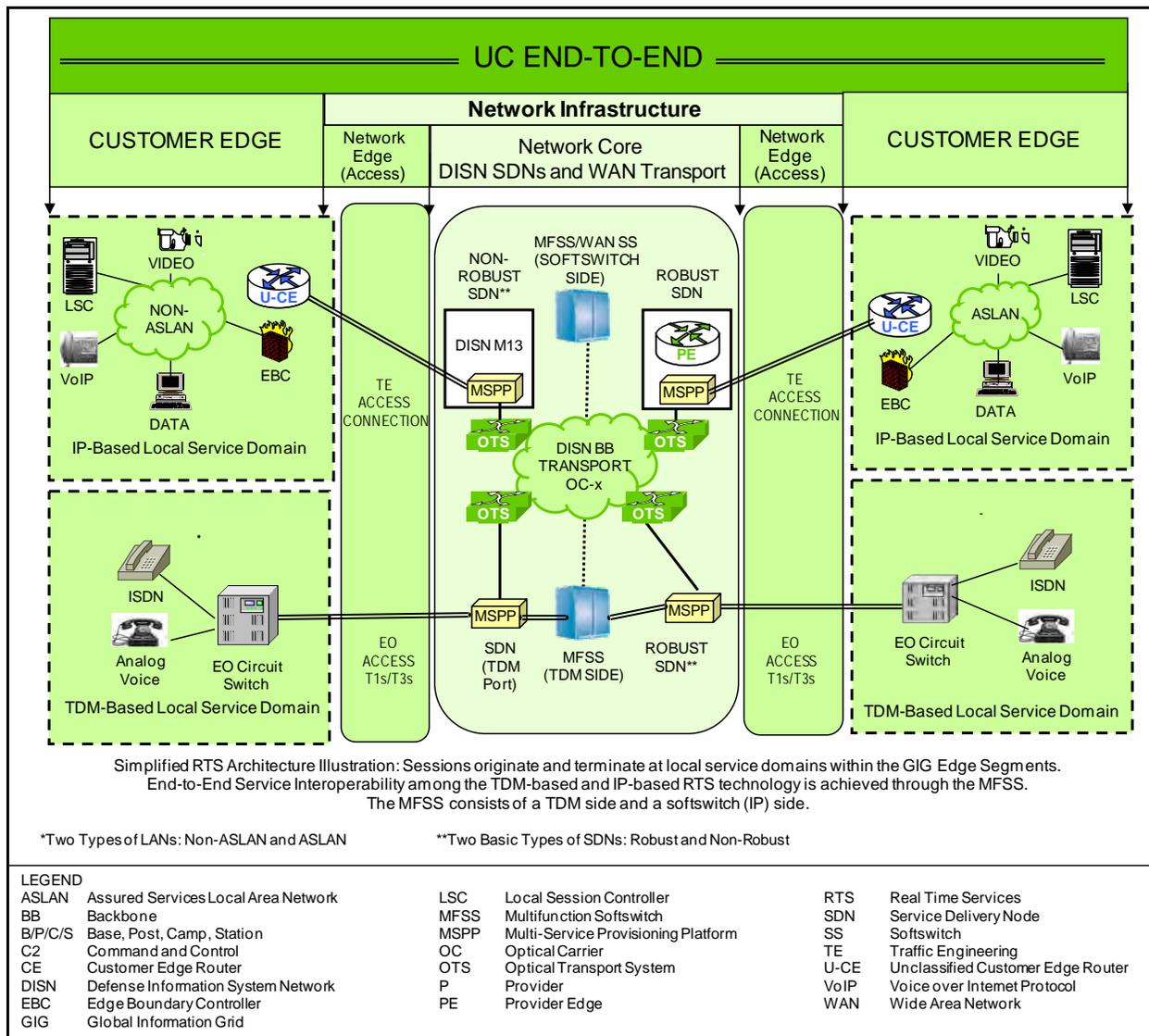


Figure 4.5-2. High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments

4.5.1 IP-Based Design for Unified Capabilities

This section provides a high-level overview of the VVoIP design within the context of the DoD network infrastructure. 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 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 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 Network Edge (Access) Segment is sized to meet the busy hour traffic demand for each service class and each of the four 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 DISN Subscription Services (DSS) designation as a mission-critical site, 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 Unclassified Customer Edge (U-CE) Router in relation to the type of SDN, and the type of missions that the U-CE Router serves), are as follows:

- Type of SDN
 - Non-Robust – M13 multiplexer
 - Robust – Multi-Service Provisioning Platform (MSPP) without Aggregation Router (AR) all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning)
 - Robust – MSPP with Unclassified Aggregation Router (U-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
 - Noncritical mission

As shown in [Figure 4.5.1-1](#), a noncritical mission U-CE Router may connect to the nearest SDN regardless of the type of 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.

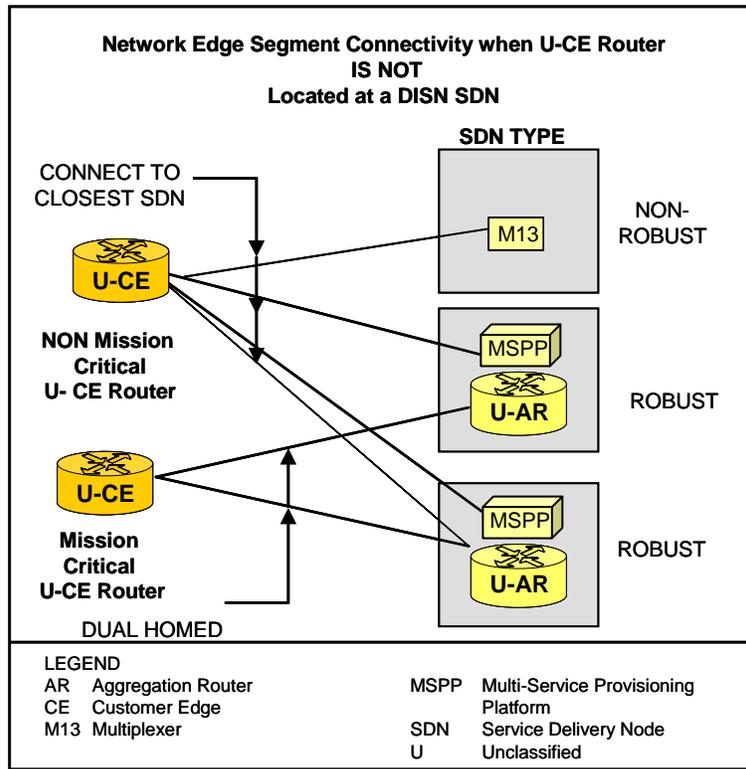


Figure 4.5.1-1. Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site

4.5.1.1 Overview of VVoIP Network Design Attributes

The most important consideration for implementing the VVoIP technology insertion associated with the “VVoIP Network Design” is not to degrade the capability to meet voice, video, and data services mission requirements. Preventing degradation begins with establishing a VVoIP Network 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 4.4](#), Migration to Unified Capabilities.

The logical location of the major VVoIP network attributes within the UC E2E design is shown in [Figure 4.5.1-2](#), Overview of VVoIP network Attributes. The location of attributes in terms of the Customer Edge (B/P/C/S), the Network Edge (Access), 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.

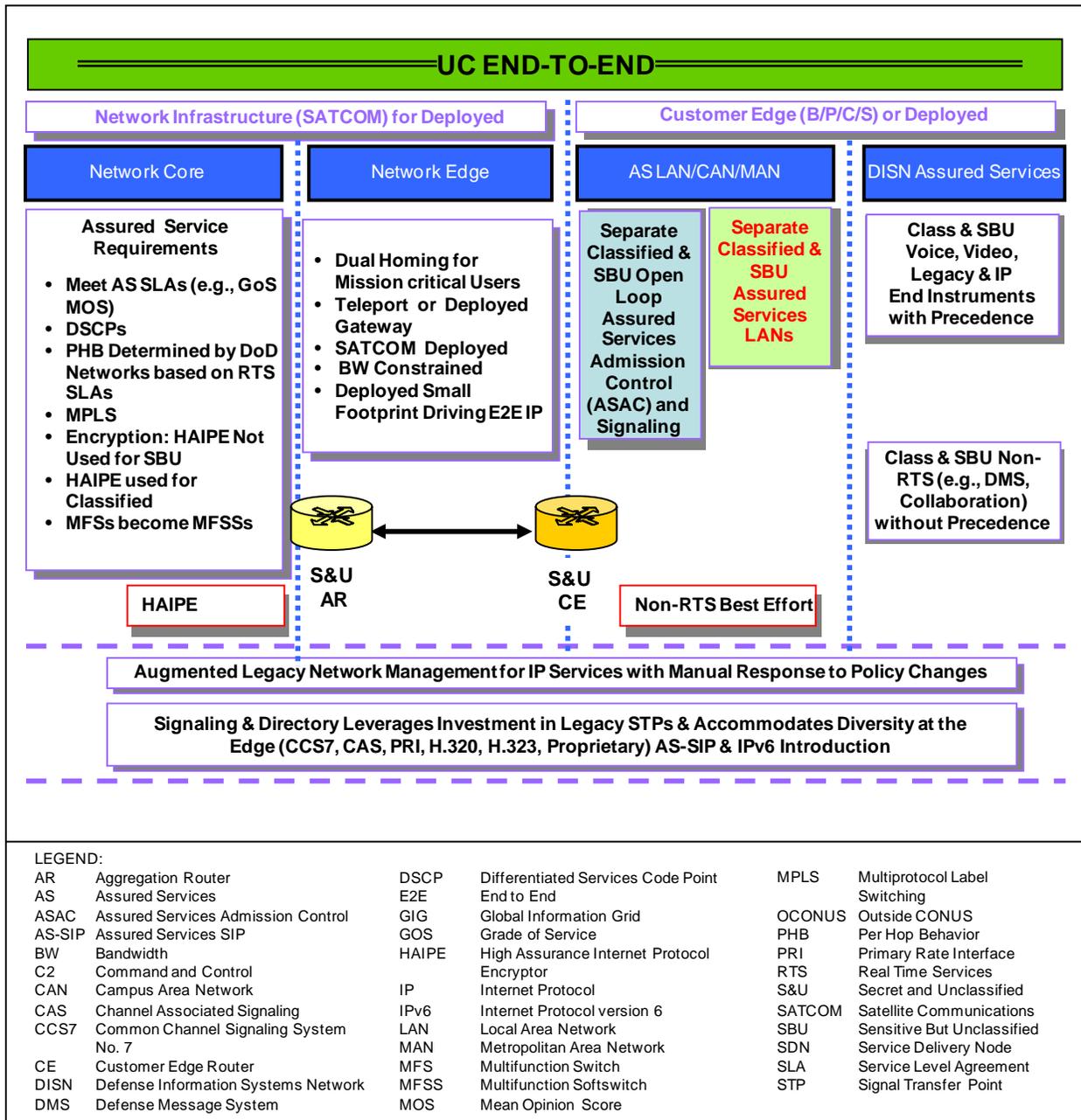


Figure 4.5.1-2. Overview of VVoIP Network Attributes

The functions contained in the boxes located within the top half of [Figure 4.5.1-2](#) 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 currently only voice and video sessions are supported by Assured Services.

4.5.1.1.1 Queuing Hierarchy for DISN IP Service Classes

Section 5.3.3, Network Infrastructure E2E Performance Requirements, defines a four-queue model for maintaining the required QoS for each UC Aggregate Service Class. Assured Voice, User Signaling, and Network Control Traffic are placed in the Expedited Forwarding (EF) queue. Assured Multimedia Conferencing (i.e., Video) traffic is placed in the Class 4 Assured Forwarding (AF4) queue. Preferred data, non-assured VVoIP; IM, Chat, and Presence; and Operations, Administration and Maintenance (OA&M) traffic is placed in the Class 3 Assured Forwarding (AF3) queue. All other traffic (data and any other service) are placed in the Best Effort (Default) queue. NOTE: User Signaling associated with non-assured VVoIP is placed in the EF queue. Figure 4.5.1-3 shows the queue structure and associated rules.

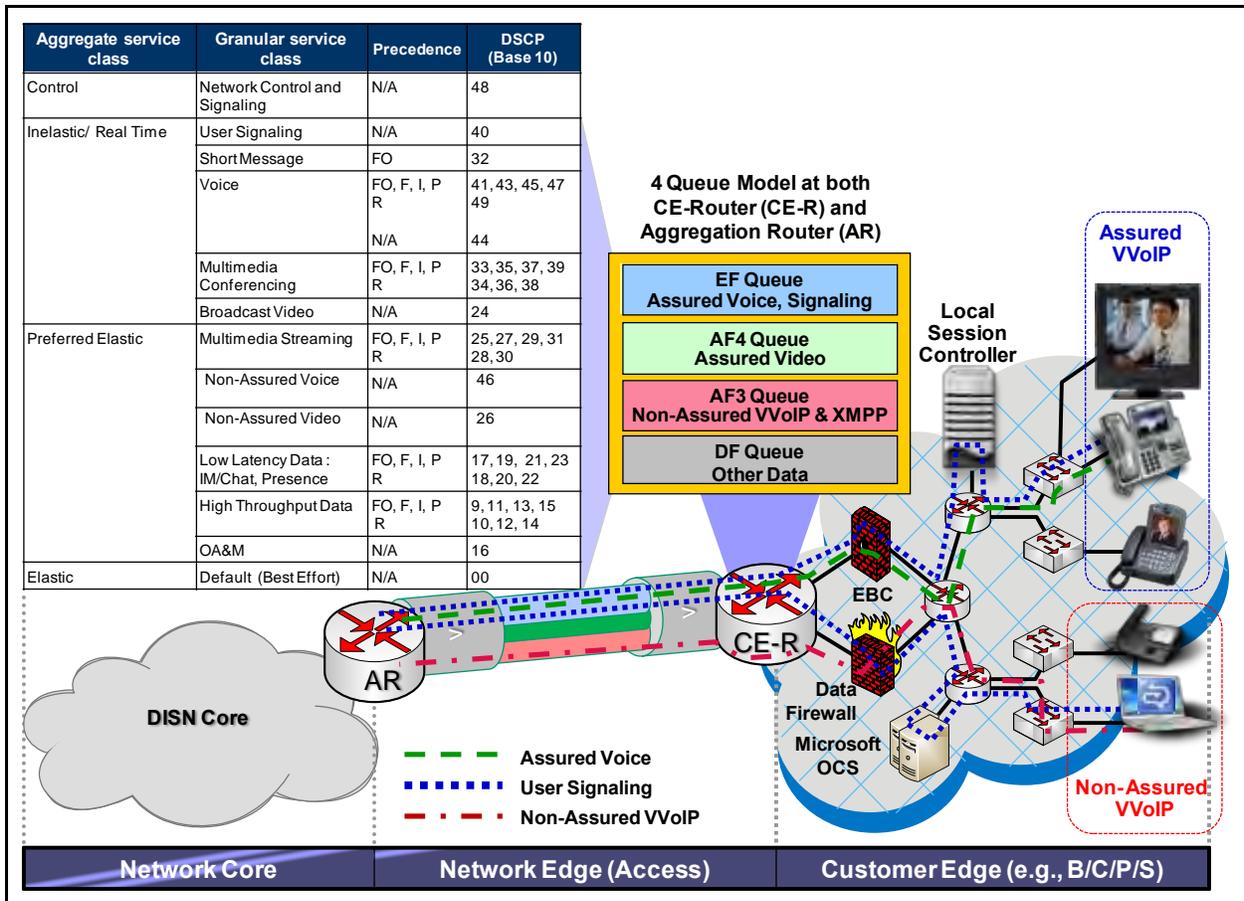


Figure 4.5.1-3. Queuing for the Bearer Design

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.

4.5.1.1.2 *Customer Edge Segment Design*

The Customer Edge Segment has the following attributes:

1. **Nonblocking ASLAN.** At the Customer Edge, the design has an ASLAN that is designed as nonblocking for voice and video traffic.
2. **Traffic Admission Control.** The LSCs on a B/P/C/S use an Open Loop Assured Service Admission Control (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 Section 5.3.3.15, Voice Service Quality.
3. **Call Preemption.** Lower precedence sessions will be preempted on the access circuit 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 Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.
5. **MPLS and MPLS VPNs.** Can be implemented in the ASLAN but cannot be extended to the DISN.

4.5.1.1.2.1 **B/P/C/S 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), or metropolitan area network (MAN) structure. The LAN, CAN, or 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 (MG) function within an LSC per local interface requirements. It is a MILDEP responsibility to design and fund the base infrastructure design.

4.5.1.1.2.2 **LSC Designs – Voice**

An LSC is a call stateful voice, video, and signaling server product at the B/P/C/S that directly serves IP and analog EIs. The LSCs are the cornerstone of all DoD VVoIP signaling functions. The functions provided by the LSC are found in the MFSS also. The LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC uses AS-SIP signaling. If the

LSC interfaces to the public switched telephone network (PSTN) or to legacy B/P/C/S TDM systems, it must support Primary Rate Interface (PRI) also, using its MG and Media Gateway Controller (MGC). All LSCs provide PBAS via AS-SIP/ASAC for IP and via T1.619a.

[Figure 4.5.1-4](#), B/P/C/S-Level Voice over IP 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 and not shown for simplicity. At the top of the figure, the first case shown is where multiple LANs, each with its own LSC and U-CE Router, connect 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 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.

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.* 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.

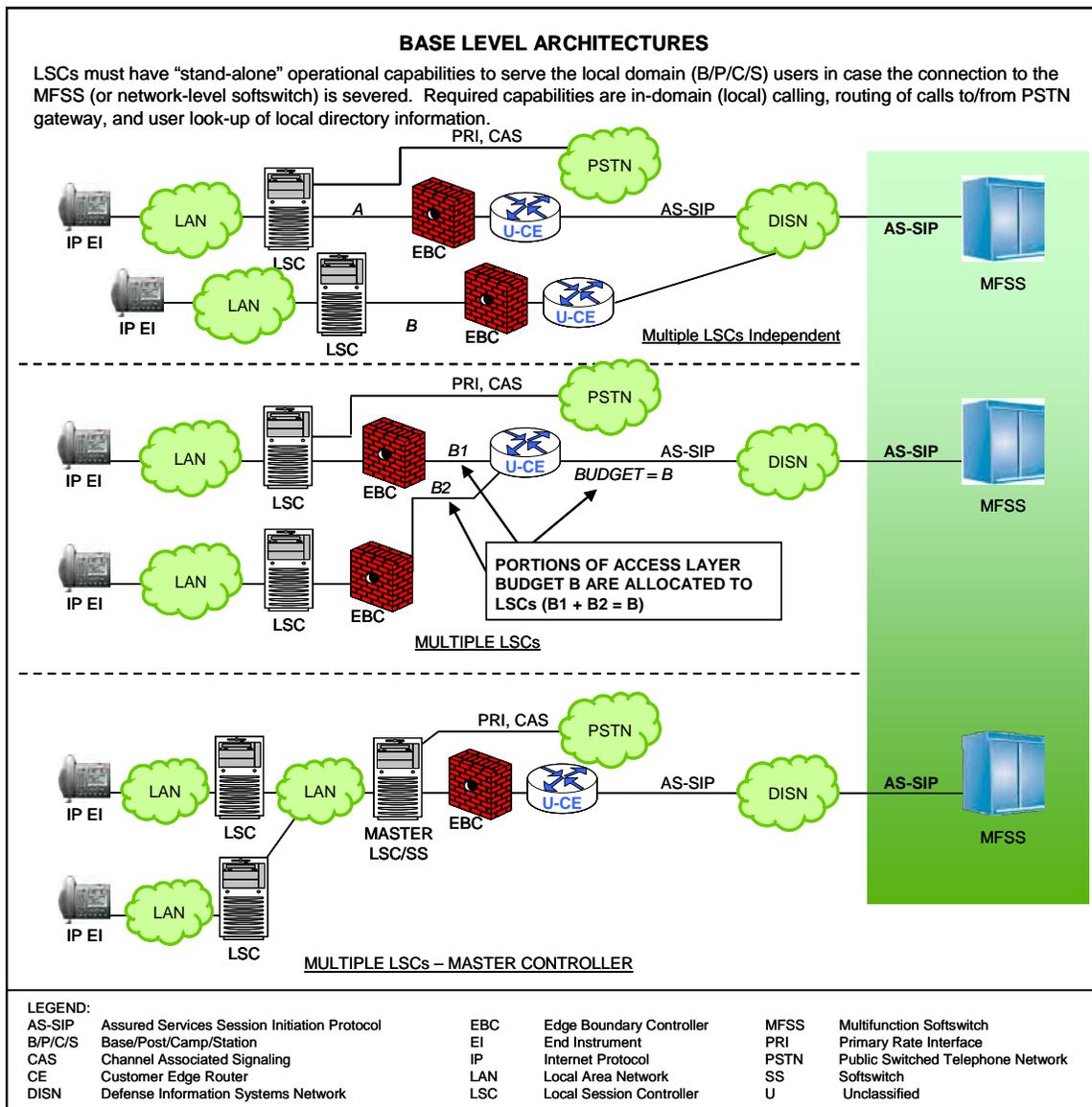


Figure 4.5.1-4. B/P/C/S-Level Voice over IP LSC Designs

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 the following two methods is acceptable:

Section 4 – UC Description and Key Processes

- a. Method 1 – the 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 (3 total) allowed 10 voice sessions (10 budgets).
 - (3) Master LSC performs preemptions to ensure higher precedence sessions succeed.
 - (4) Master LSC blocks ROUTINE precedence sessions from any LSC after the access link budget is met.
- b. Method 2 – the master maintains a strict budget for subtended LSCs, for example,
 - (1) If the ASAC budget is 30.
 - (2) Each subtended LSC (3 total) with each allowed 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 an EMS 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 and or proprietary signaling protocols if LSCs are from the same vendor.
 - a. All signaling destined external to the enclave passes through the master LSC.
 - b. Allows multiple vendors within the enclave or a single vendor integrated solution.
7. Each LSC maintains two budget counts as follows:
 - a. Intraenclave (based on local traffic engineering and not associated with the access link budget).
 - b. Interenclave (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 have only 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 do not use master LSCs. Only the master configuration is recommended.

4.5.1.1.2.3 LSC Designs – Video

[Figure 4.5.1-5](#), 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 uses AS-SIP signaling. A Gatekeeper is an appliance that processes calls to the WAN using H.323 or Session Initiation Protocol (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 channel-associated signaling (CAS) using its MG and MGC. All LSCs provide PBAS via AS-SIP/ASAC for IP and via MLPP for the PRI.

[Figure 4.5.1-5](#) 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

Section 4 – UC Description and Key Processes

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., $B_1 + B_2$). 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.

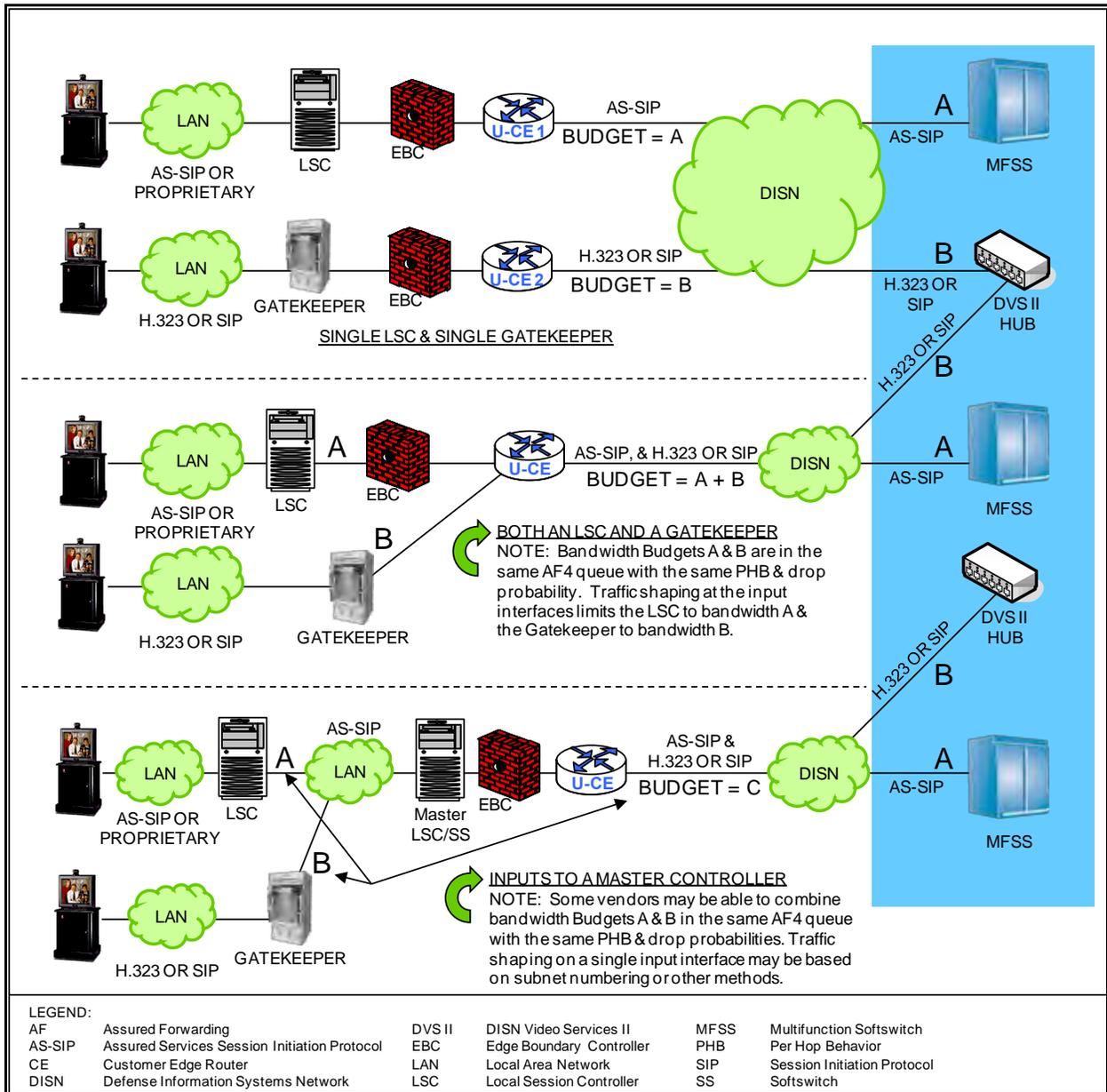


Figure 4.5.1-5. B/P/C/S Video over IP LSC Designs

The third case requires the designation and implementation of an LSC cluster concept as described for the voice design in [Section 4.5.1.1.2.2, LSC Designs–Voice](#).

With regard to the Gatekeeper interworking with the master LSC or 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 or 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 or SS will be able to process the calls into Budget C efficiently in the AF4 queue. All video calls leaving the master LSC or SS must be treated equally to comply with DoD policy.

4.5.1.1.2.4 LAN and ASLAN Design

Requirements for the B/P/C/S LAN designs are defined in Section 5.3.1, Assured Services Local Area Network. The principal LAN requirements are summarized in [Figure 4.5.1-6](#).

 ASLAN UCR/UCTP	REQUIREMENTS <ul style="list-style-type: none"> • MEET VOICE, VIDEO & DATA PERFORMANCE • SERVICE CLASSES & PRECEDENCE MAPPED INTO DSCPs • QoS BY OVER-PROVISIONING/DSCPs • PACKET LOSS, JITTER, LATENCY METRICS • COMMERCIAL, MEDIUM, AND HIGH AVAILABILITY/POWER • VLAN FOR VOICE, VIDEO, DATA PERIPHERALS • NETWORK MANAGEMENT OF LAN 												
LEGEND <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">ASLAN Assured Services Local Area Network</td> <td style="width: 50%;">IATP Information Assurance Test Plan</td> </tr> <tr> <td>C2 Command and Control</td> <td>LAN Local Area Network</td> </tr> <tr> <td>DISN Defense Information Systems Network</td> <td>MOS Mean Opinion Score</td> </tr> <tr> <td>DSCP Differentiated Services Code Point</td> <td>SLA Service Level Agreement</td> </tr> <tr> <td></td> <td>UCTP Unified Capability Test Plan</td> </tr> <tr> <td></td> <td>VLAN 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		UCTP Unified Capability Test Plan		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												
	UCTP Unified Capability Test Plan												
	VLAN Virtual Local Area Network												

Figure 4.5.1-6. ASLAN Requirements Summary

Two types of LANs are 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 4.5.1-7](#), Three Categories of LANs.

[Table 4.5.1-1](#), 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 user that is authorized FLASH OVERRIDE and FLASH precedence is required to be served on a High Availability ASLAN, and other users are permitted on the same LAN). *Not Permitted* means that the user must not be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence cannot be served by a Medium Availability ASLAN 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 users that only have ROUTINE precedence).

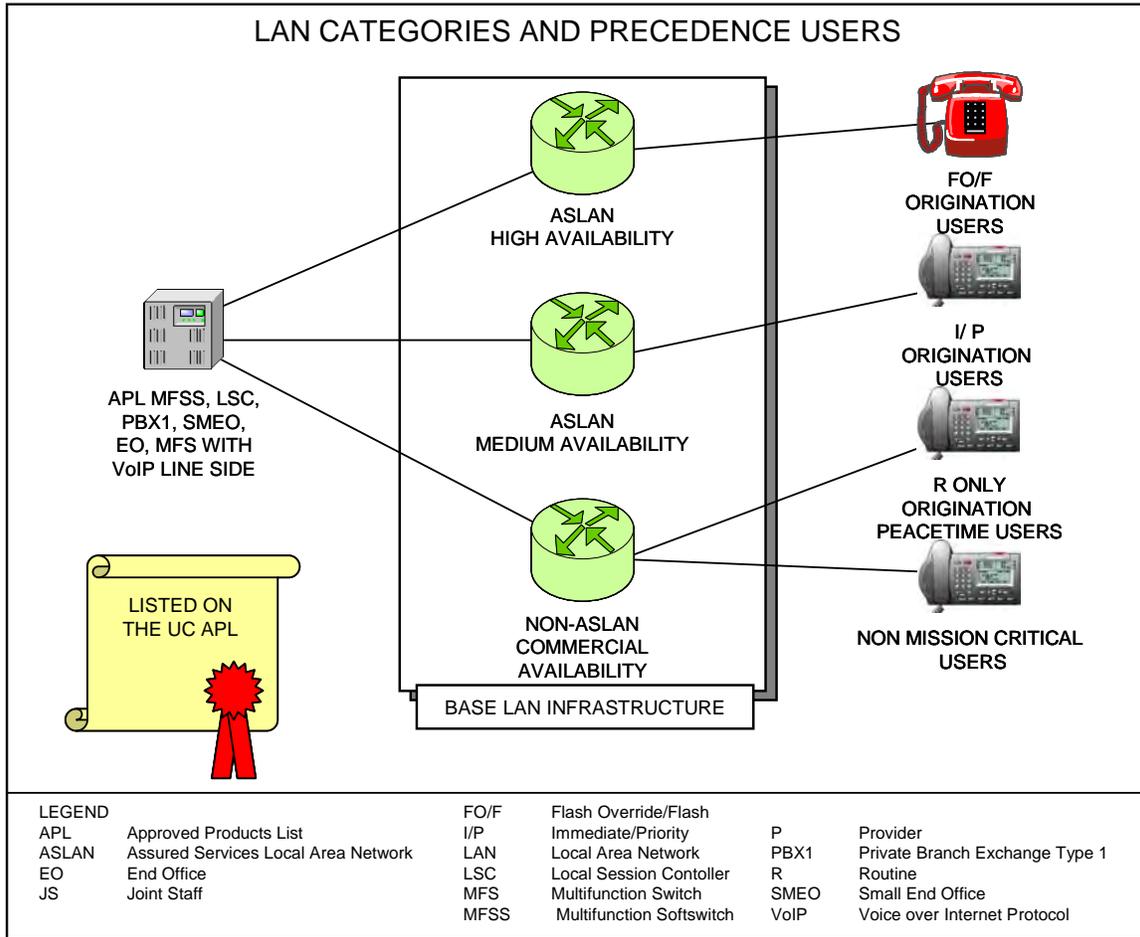


Figure 4.5.1-7. Three Categories of ASLANs

An ASLAN that supports users authorized I/P is classified as a Medium Availability ASLAN. An ASLAN that supports users authorized FO/F is classified as a High Availability ASLAN.

Table 4.5.1-1. LAN Requirements Summary

LAN REQUIREMENT ITEM	USER PRECEDENCE ORIENTATION AUTHORIZATION			
	FO/F	I/P	R	NOT MISSION CRITICAL
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	Note 1
Availability	99.999	99.997	99.9	99.9
LEGEND				
ASF	Assured Services Features		NP	Not Permitted
ASLAN	Assured Services LAN		NR	Not Required
FO/F	FLASH OVERRIDE/FLASH		P	Permitted
GOS	Grade of Service		R	Required
I/P	IMMEDIATE/PRIORITY		R	ROUTINE
LAN	Local Area Network			
Note 1 GOS is discretionary and shall be determined by DoD Components.				

The actual LAN implementation will vary from base to base depending on building or facility locations, installed cable plant, and the location and type of missions being performed on the base. [Figure 4.5.1-8](#), An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users, 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.

4.5.1.1.3 Network Infrastructure E2E Performance (DoD Intranets and DISN SDNs)

The DoD Intranets and the DISN SDNs serving SBU VVoIP traffic currently do not use 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 satellite communications (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 network 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.

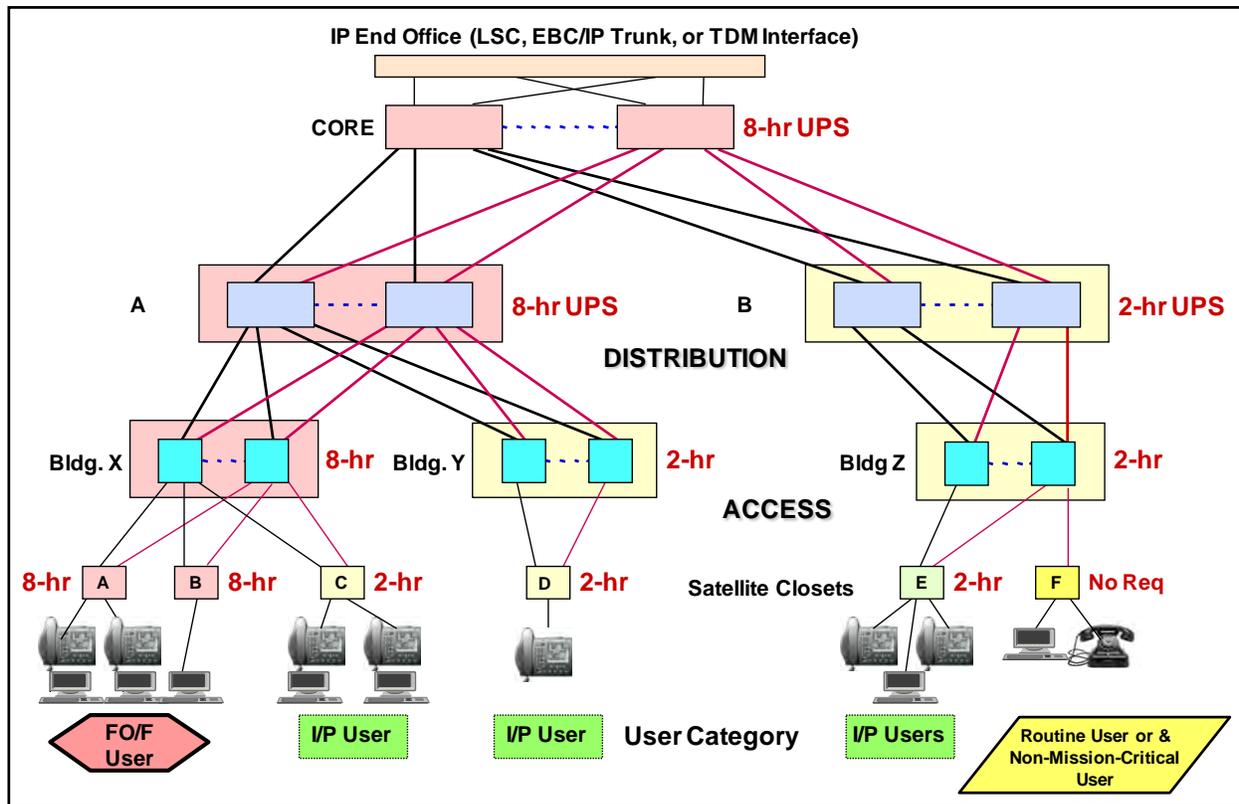


Figure 4.5.1-8. An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users

In order to ensure E2E voice and video services' performance, an allocation of performance must be established for the Services' Intranets and DISN SDNs, which are supporting IP-based voice, video, and data services. The performance requirements for voice and video is based on best commercial practices for latency, packet loss, jitter, and availability, which is allocated to the Services' ASLANs and their associated CE Router and EIs, to the Services' Intranets (called MANs and CANs) and to the DISN SDNs. Many techniques, such as MPLS, Multiprotocol Label Switching – Traffic Engineered (MPLS-TE), queuing, mesh routing, and redundancy; can be used by the networks to meet the performance allocations. Currently, only the voice and video performance metrics have been defined. Data application performance metrics will be addressed in the future. The performance metrics for voice (E-Model R-Factor) and video have been defined. Measurement techniques for validating that the performance allocations have been met and for isolating the portion of the E2E network, that is not meeting the allocations have been developed. [Figure 4.5.1-9](#), Measurement Points for Network Segments, illustrates the components of the E2E network where measurements will be made to ascertain compliance with

the Service Level Agreements (SLAs). The specific E2E network performance requirements are described in Section 5.3.3, Network Infrastructure E2E Performance Requirements.

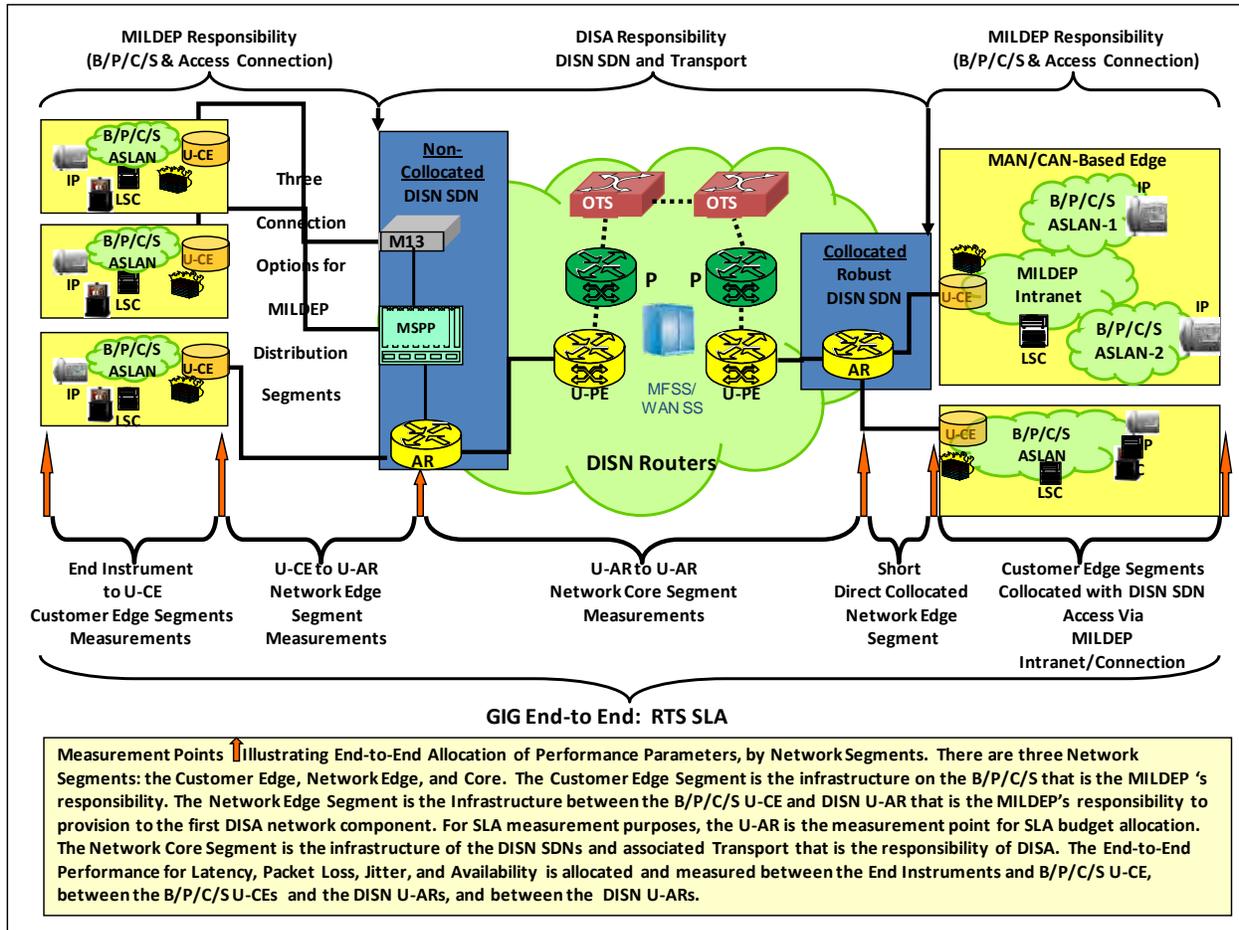


Figure 4.5.1-9. Measurement Points for Network Segments

4.5.1.1.4 E2E 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 an NM system (NMS) and a network appliance. Network management protocols include the Simple Network Management Protocol (SNMP), Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

4.5.1.1.5 ASAC Component

The ASAC technique is the key VVoIP design component ensuring that E2E SLAs (Grade of Service (GOS) 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 E2E.

Figure 4.5.1-10 represents the first step in specifying the DISN ASFs by depicting a more detailed functional breakdown of the components than that shown in Figure 4.5.1-2, Overview of VVoIP Network Attributes.

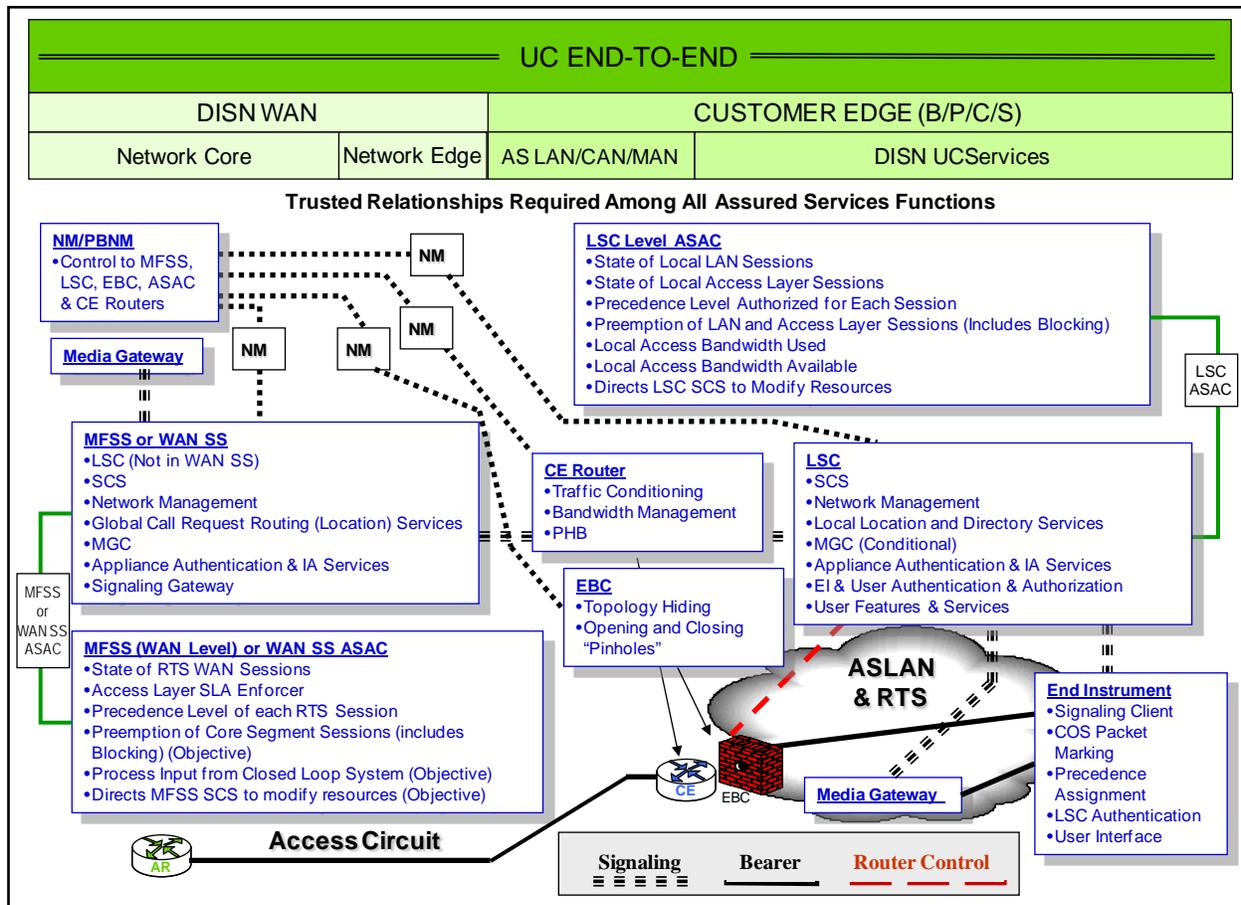


Figure 4.5.1-10. Assured Services Functions

Detailed requirements for each function contained in the boxes, the EBC, and the other components of the ASFs are contained in Section 5.3.2, Assured Services Features Requirements.

The Open Loop ASAC design, depicted in [Figure 4.5.1-11](#), Open Loop ASAC Network Design, is specified as the current method for achieving assured services E2E. The ASLAN connects via a local access circuit to a backbone network that consists of a Core MPLS-capable network.

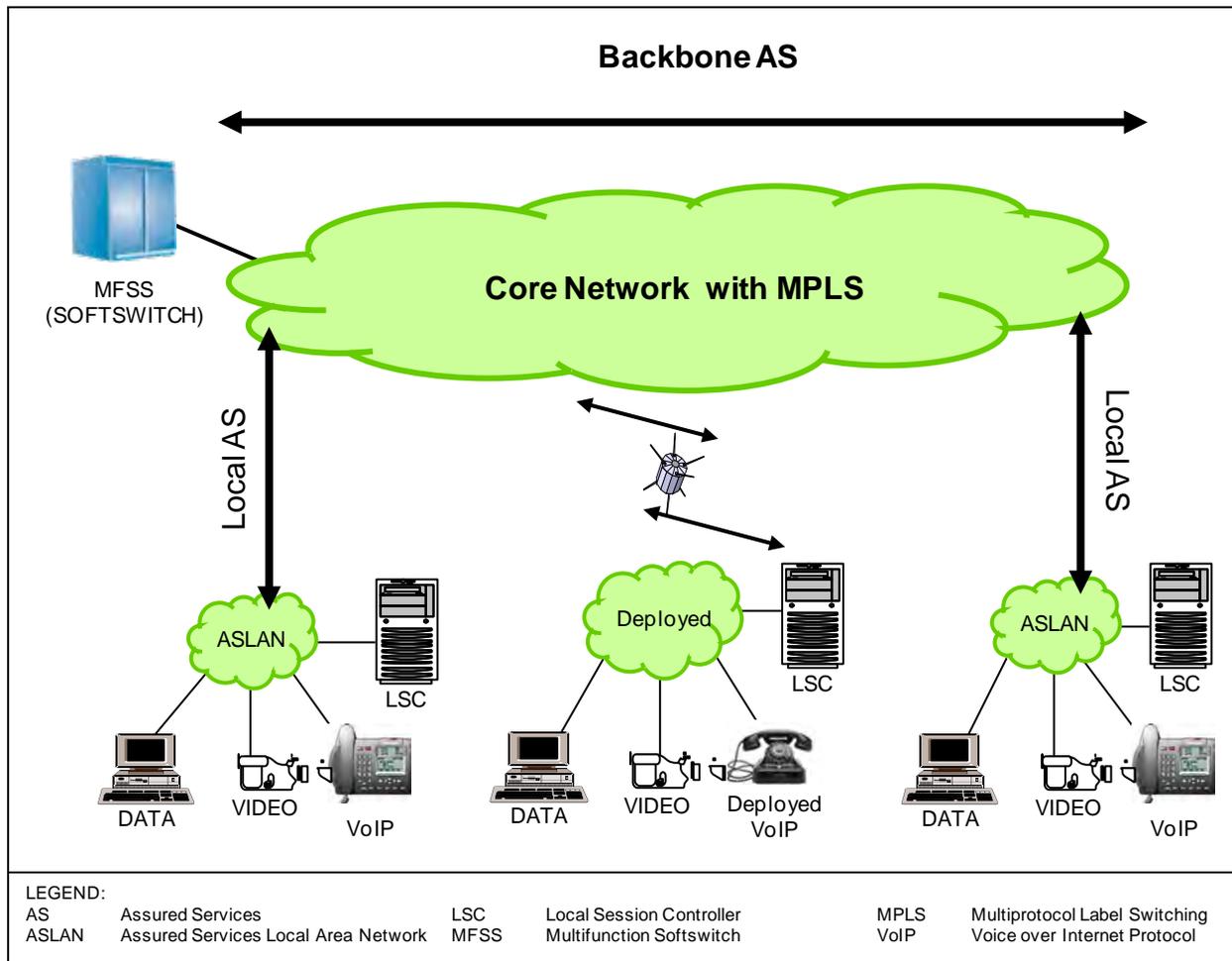


Figure 4.5.1-11. Open Loop ASAC Network Design

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

NOTE: Deployable VoIP products may connect via compressed satellite circuits to the DISN backbone and operate in a similar manner to fixed products on an ASLAN.

The components of the Open Loop ASAC method are shown in [Figure 4.5.1-12](#), Open Loop ASAC for SBU Voice and Video. In the access circuit and the ASLAN, AS-SIP signaling (see

Section 4 – UC Description and Key Processes

Section 5.3.4, AS-SIP General 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 services provided by QoS/Differentiated Service Code Point (DSCP), traffic engineering, and MPLS. Traffic with no marking will be treated as Best Effort.

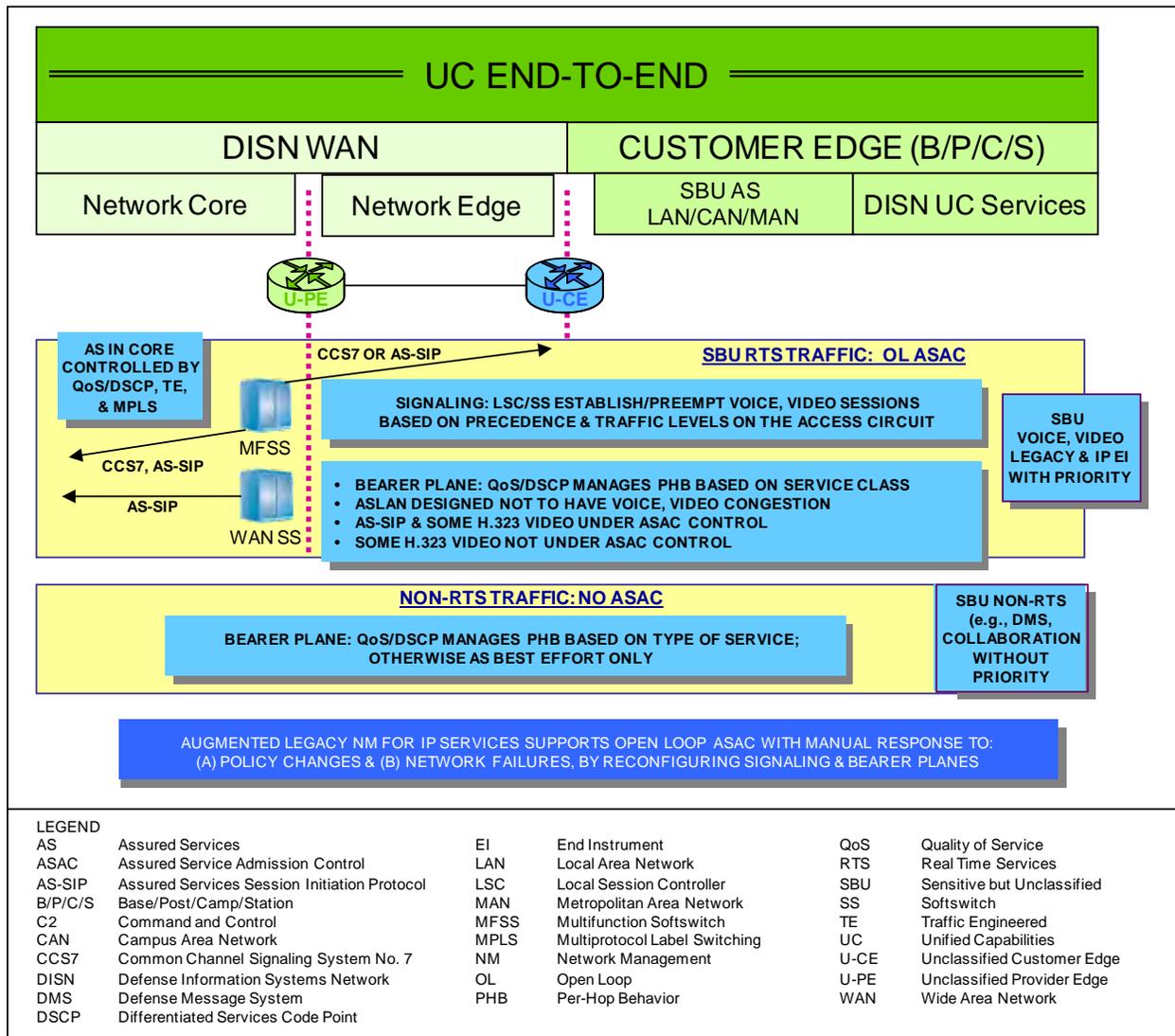


Figure 4.5.1-12. Open Loop ASAC for SBU Voice and Video

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 after preemption has taken place, if necessary, the origination request is sent to the destination upon which, after 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 precedence 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. [Figure 4.5.1-13](#), 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 Connection Agent (CCA) part of the LSC and MFSS. Signaling is performed by the Signaling Gateway (SG) (used for CCS7), the MG (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 and numbering plans are stored in the MFSS.

Section 4 – UC Description and Key Processes

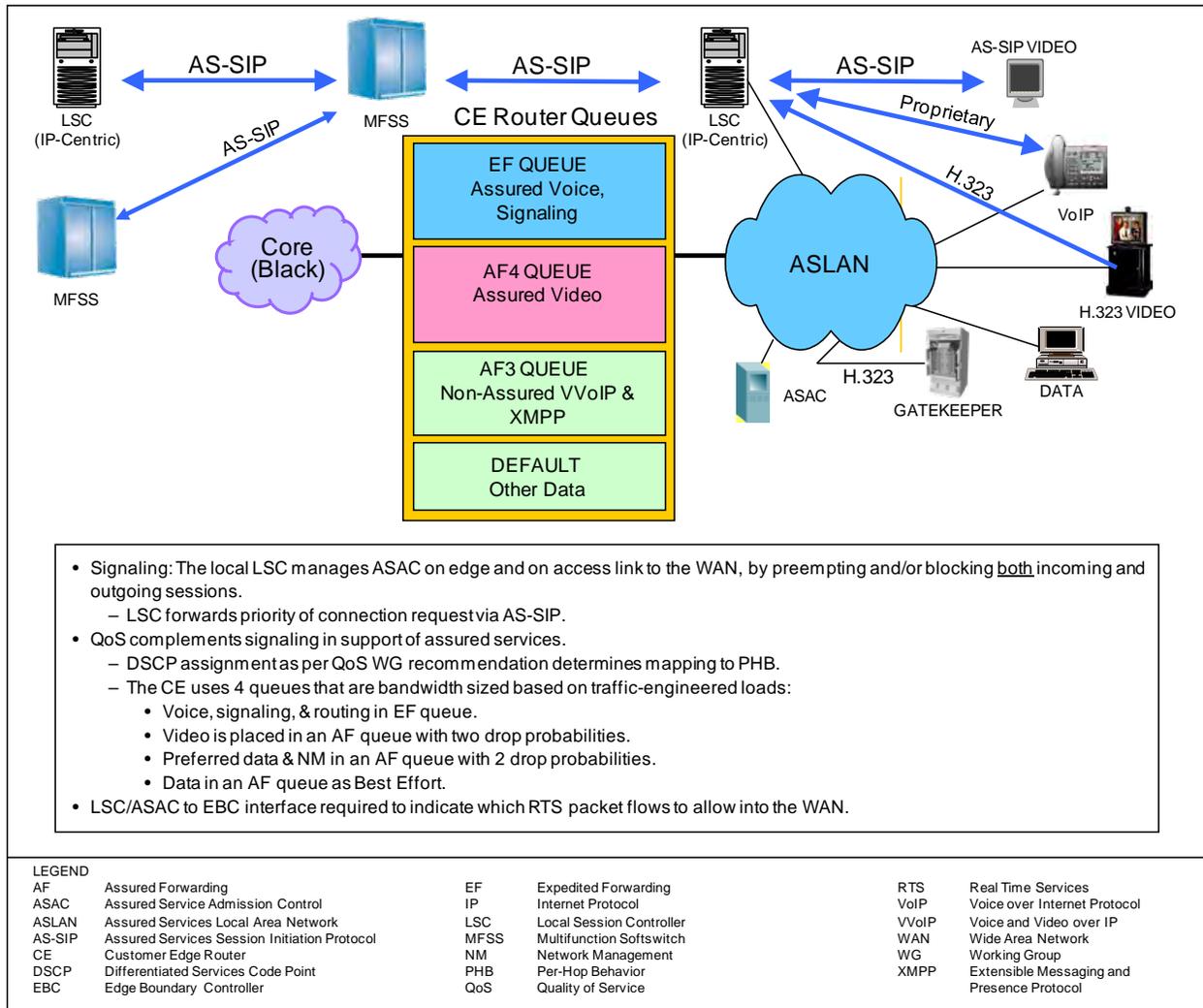


Figure 4.5.1-13. Converged VVoIP Design: Signaling, QoS, and Assured Service

4.5.1.1.6 Voice and Video Signaling Design

The voice and video signaling design for SBU voice and video is shown in [Figure 4.5.1-14](#), SBU Voice and 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 design. During migration, both H.323 and AS-SIP signaling will be used in classified VVoIP. Classified VVoIP interfaces to the TDM DRSN via MGs and SGs. A standalone SS 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 SS part of the MFSS. The TDM EOs 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.

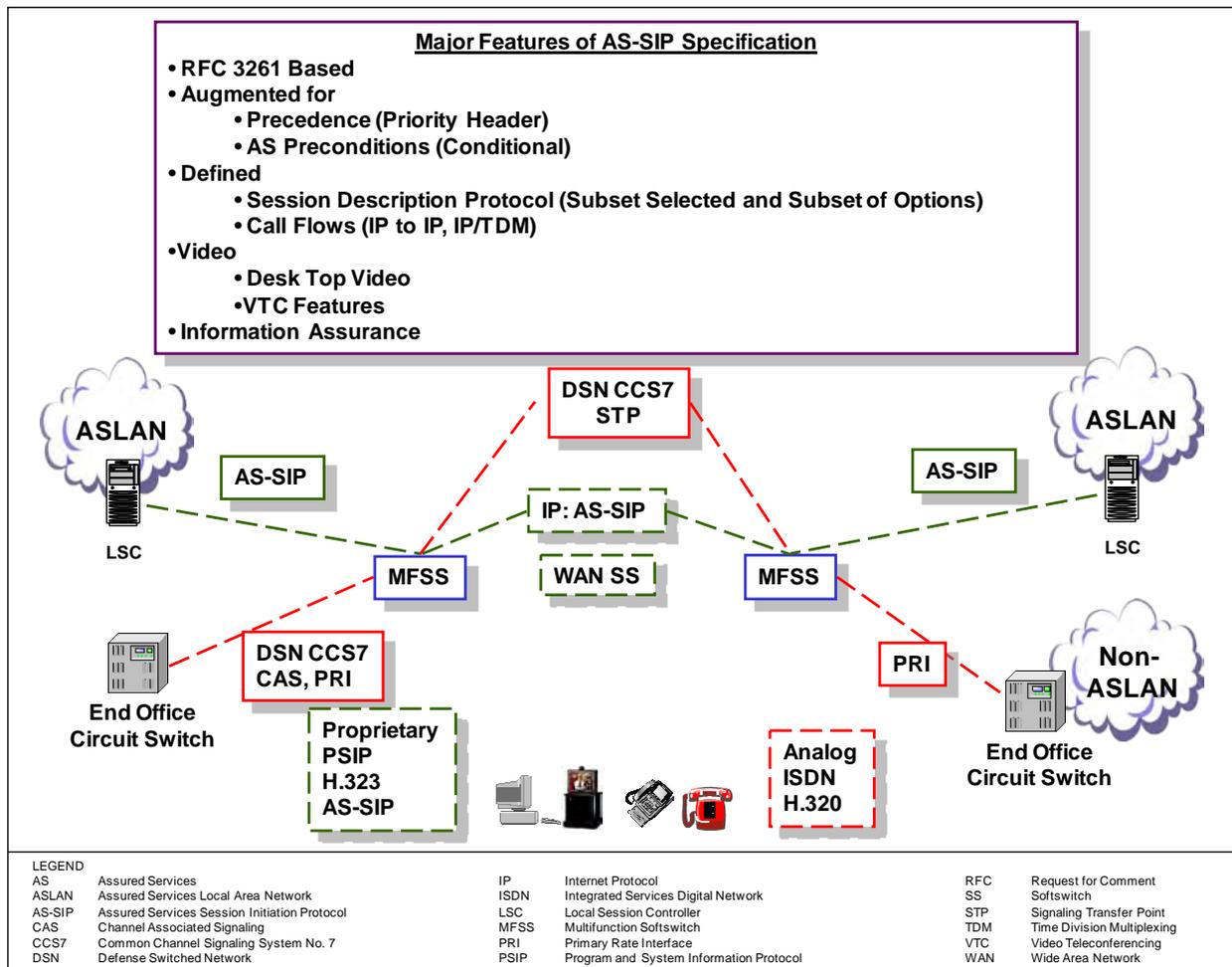


Figure 4.5.1-14. SBU Voice and Video Services Signaling Design

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 and video network migrates to an all IP EI environment in the post-2016 timeframe.

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 (or WAN SS).
 - a. LSC A to MFSS A to MFSS B to LSC B when the LSCs have different primary MFSSs.

- b. LSC A to MFSS A to LSC B when they have the same primary MFSS.
2. The LSCs are assigned a primary and backup MFSS for signaling robustness.
3. Signaling from an IP EI to an LSC may be proprietary.
4. AS-SIP will be specified in time for 2009 implementation.
5. The LSC-to-LSC signaling is not permitted external to the security enclave except for use in cases involving deployable products operating in a single area of operational responsibility network that is not the DISN.
6. The LSC can set up:
 - a. On-base sessions when a connection to an MFSS is lost.
 - b. Sessions to PSTN trunks independent of an MFSS.
7. The LSC and MFSS requirements.
8. Signaling.
 - a. A TDM EO will signal via DSN CCS7, PRI, or CAS to MFSSs.
 - b. The MFSSs will signal via CAS/PRI to the PSTN and to coalition gateways.

The LSC-to-LSC signaling without a network-level SS for other than deployed Joint Task Forces (JTFs) are under assessment. This assessment is necessary because this configuration has limitations with respect to managing traffic flows from the edge into the network for SA 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 Services' Deployable Programs under Tailored Information Support Plans (TISPs)). Signaling from the LSC must pass through the network SS part of the MFSS or through a network-level SS so the MFSS/SS can implement Precedence-Based Network Management (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 Services' Deployable Programs networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as CAS/PRI signaling.

The E2E, two-level SBU AS-SIP network signaling design is shown in [Figure 4.5.1-15](#), E2E Two-Level SBU AS-SIP Network Signaling Design. For classified networks, the two-level signaling uses WAN SSs rather than MFSSs.

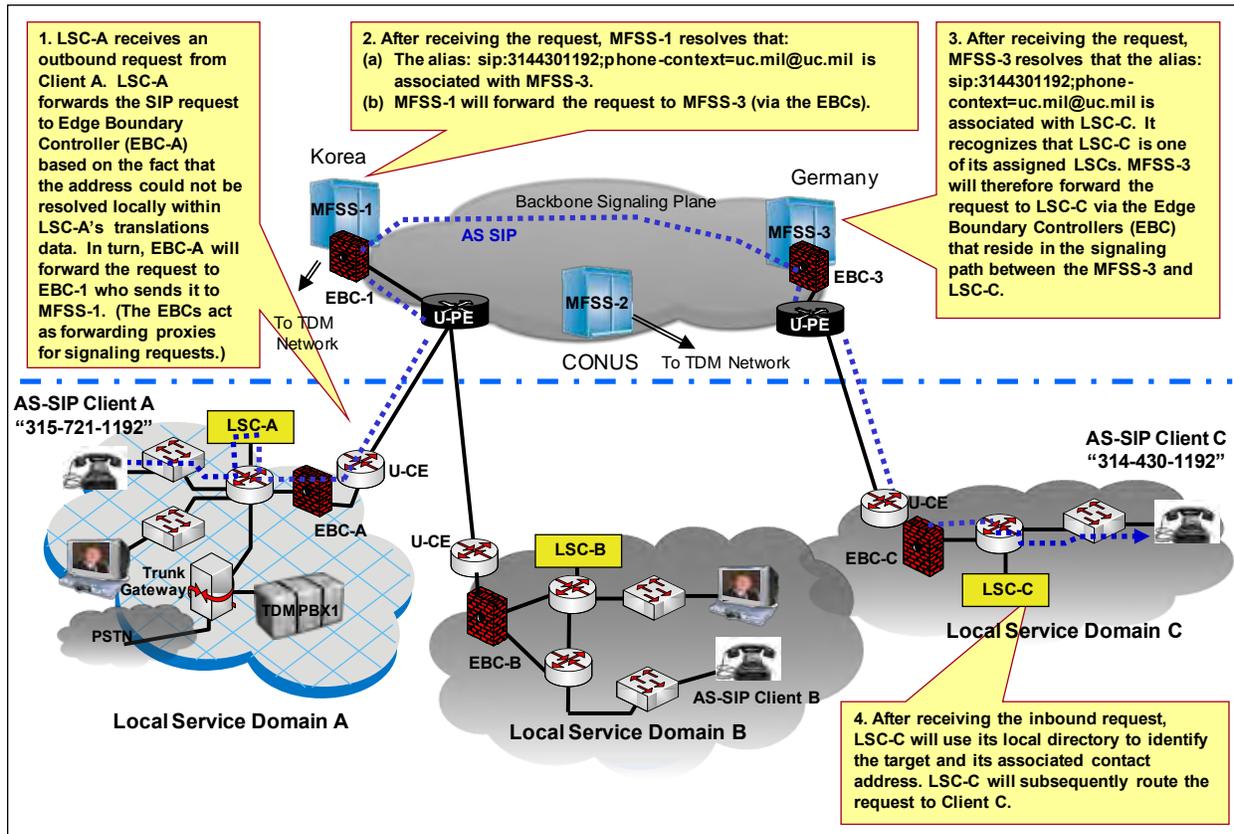


Figure 4.5.1-15. E2E Two-Level SBU AS-SIP Network Signaling Design

4.5.1.1.7 Information Assurance Design

Information Assurance is a key aspect in the design of any IP-based network. Internet Protocol is inherently vulnerable to eavesdropping and a variety of denial of service (DoS) attacks. Voice and Video over IP introduces avenues of attack due to its use of dynamically assigned User Datagram Protocol (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 Information Assurance design is necessary and is addressed in detail in Section 5.4, Information Assurance Requirements. The major components of the Information Assurance 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 4.5.1-16](#), Information Assurance Protocols. Key to the design is a hop-by-hop security model for trust between the signaling appliances using the DoD Public Key Infrastructure (PKI) for authentication.

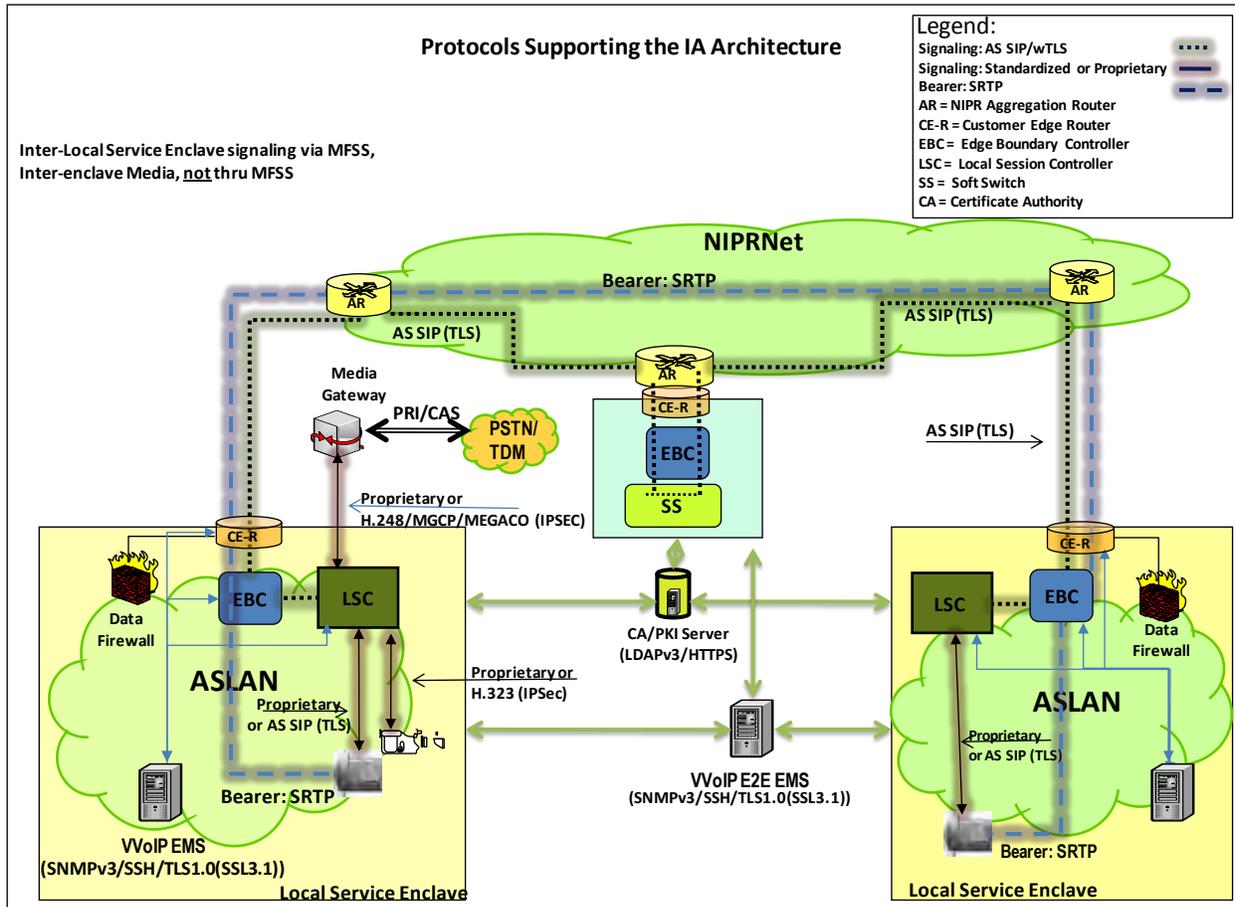


Figure 4.5.1-16. Information Assurance Protocols

Figure 4.5.1-17, IP External Interfaces to the LSC or MFSS, illustrates the IP interfaces to the LSC or MFSS to remote access terminals, such as the RTS EMS, local NMS, and the Ethernet connections for signaling and bearer traffic.

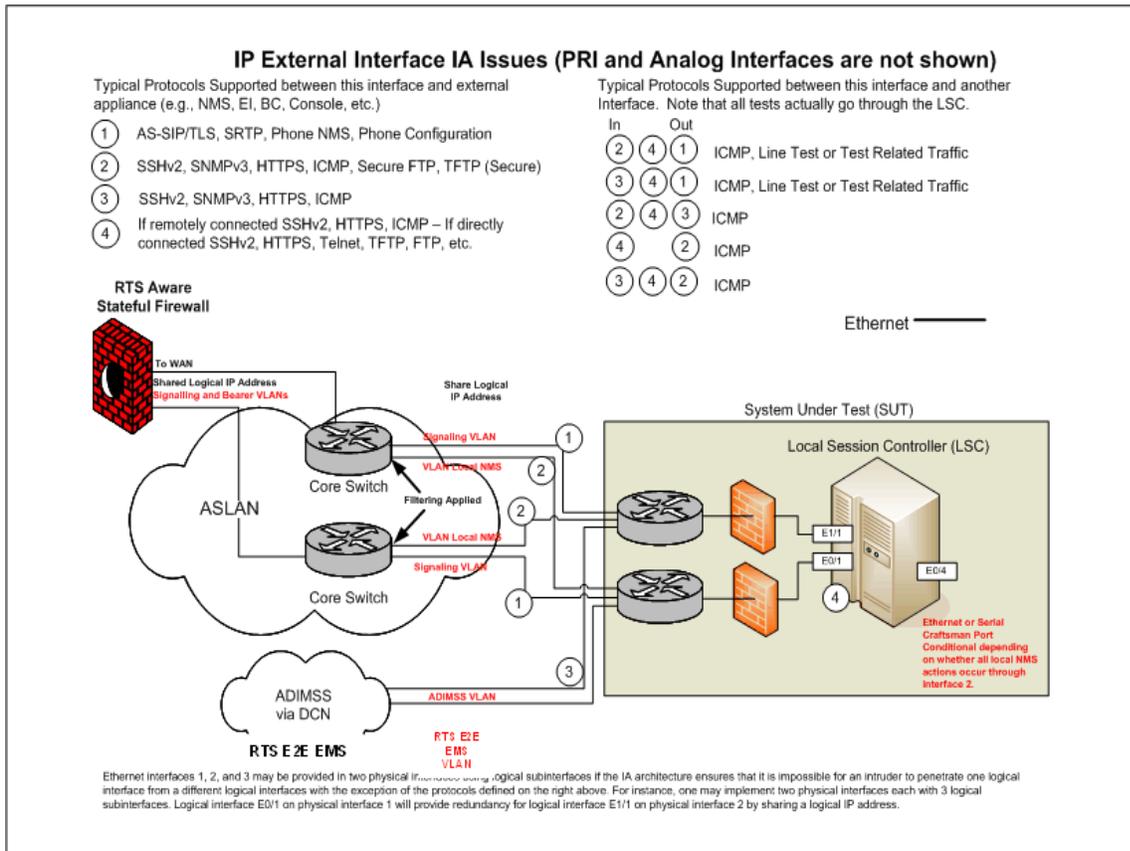


Figure 4.5.1-17. IP External Interfaces to the LSC or MFSS

[Figure 4.5.1-18](#), ASLAN Enclave Boundary Security Diagram, depicts a diagram of the Information Assurance design needed as part of the ASLAN. The key feature of Figure 4.5.1-18 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice and/or video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice and/or 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. A UC APL product called an Edge Boundary Controller (EBC) consisting of the voice and/or video firewall/border controller, has been defined and specified in Section 5.3.2, Assured Services Requirements.

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

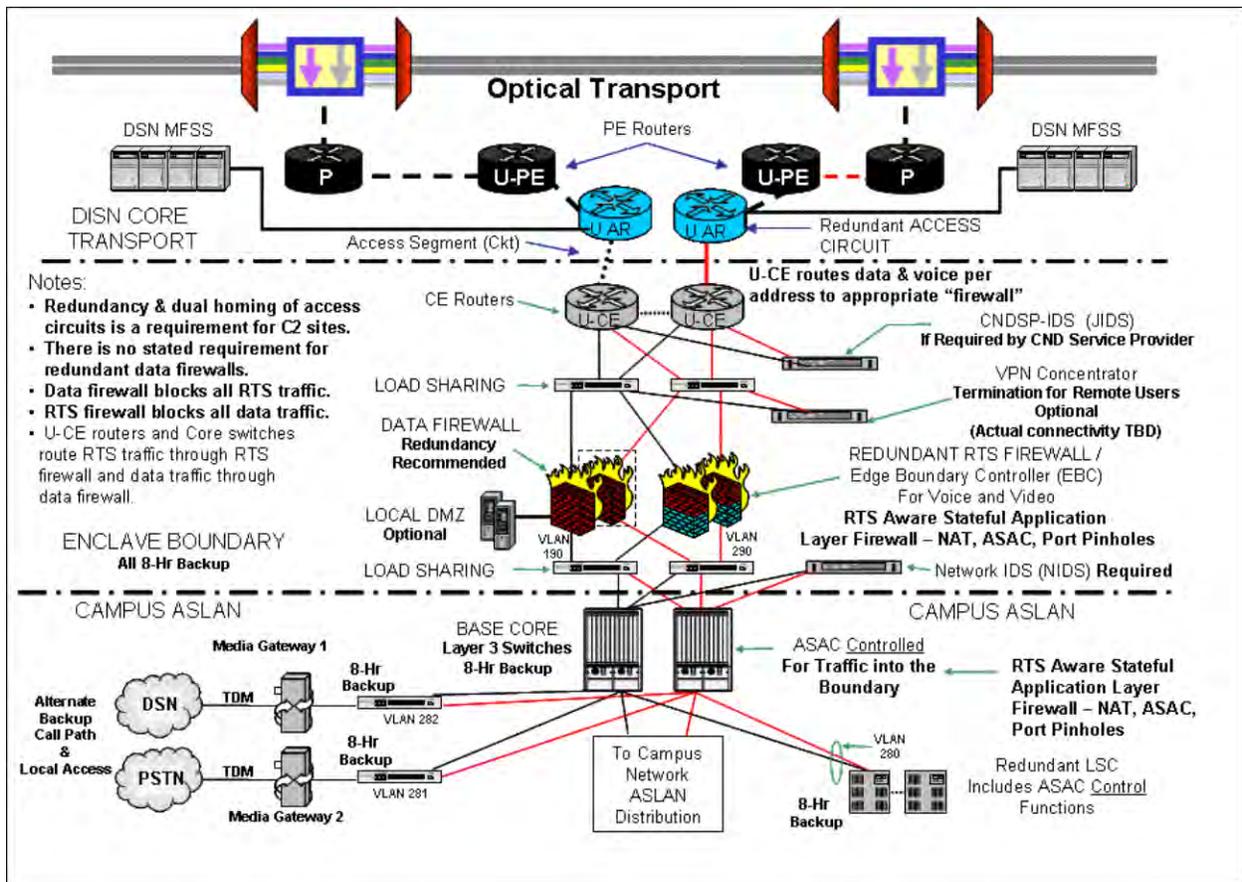


Figure 4.5.1-18. ASLAN Enclave Boundary Security Design

4.5.1.1.8 Network Management Design

Network management of the VVoIP services E2E is a critical component of NETOPS. Since the VVoIP network will be a hybrid network for an extended period, the NMS must continue to be provided by an EMS via commanding and monitoring of the voice and video services for both circuit-switched and IP technologies as part of the DISN OSS. This hybrid operation within the DISN Operational Support System (OSS) is illustrated in [Figure 4.5.1-19](#), Role of E2E RTS EMS in DISN OSS, where the EMS is shown at the bottom of the DISN OSS hierarchy.

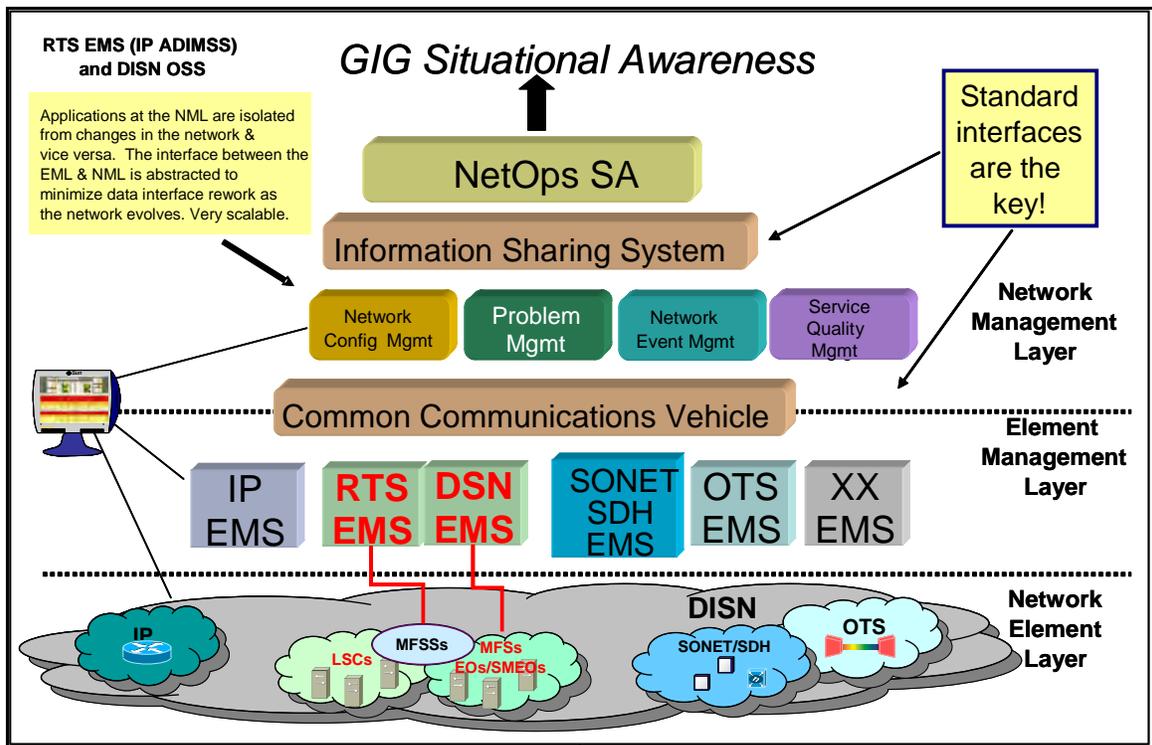


Figure 4.5.1-19. Role of RTS EMS in DISN OSS

In support of the Joint CONOPS for shared SA, and as an enabler of Net-Centric GIG Enterprise Management (GEM), the DoD Component EMS and RTS EMS must provide new machine-to-machine interfaces for “reading and writing” to the Services’ NMS to support the JTF-GNO in both visibility and reconfiguration of the network, and in controlling the flow of sessions. The design for support of JTF-GNO is illustrated in [Figure 4.5.1-20](#), RTS EMS Role in Providing E2E EMS. Since the RTS EMS is Government Off-the-Shelf (GOTS) based on COTS, it is available for the MILDEPs to use at their NOCs as well.

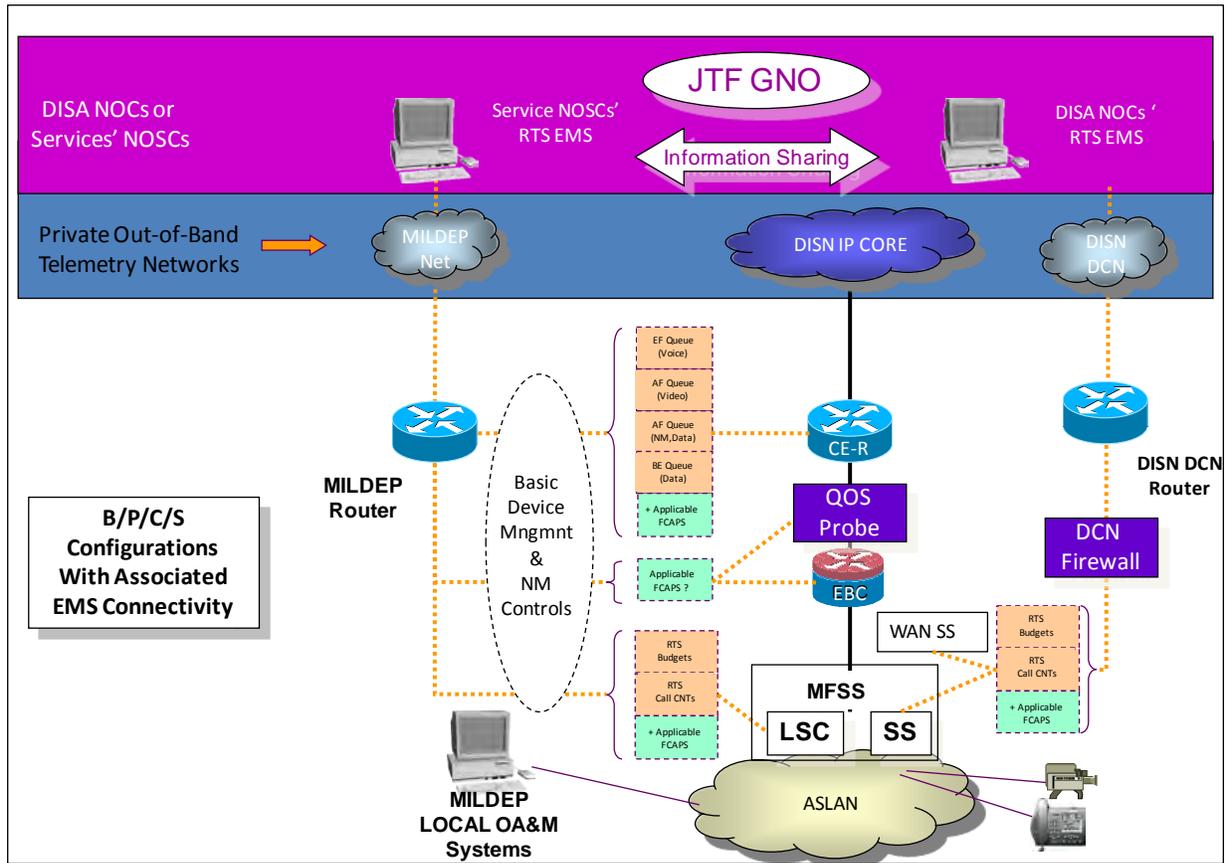


Figure 4.5.1-20. RTS EMS Role in Providing E2E GEM

4.5.1.2 Relationship between UC Network 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 EO, 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, but are not considered products for UC APL certification, but rather functions and features that form a part of a UC APL product. [Table 4.5.1-2](#), Summary of IP-Based Appliances and UC APL Products, provides a summary of IP-based appliances and APL products.

Table 4.5.1-2. Summary of IP-Based Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
End Instrument (EI)	Appliance	Appliance part of LSC
AS-SIP End Instrument (AEI)	APL Product	Product consisting of a single appliance
Media Gateway (MG)	Appliance	Media conversion function as part of the LSC and MFSS
Signaling Gateway (SG)	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 (CCA)	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 an ASLAN
Secure End Instrument (SEI)	APL Product	Product consisting of a single appliance
Local Session Controller (LSC)	APL Product	Product providing many local telephony functions
Multifunction Softswitch (MFSS)	APL Product	Large, complex product providing many local and WAN-related telephony functions
Wide Area Network Softswitch (WAN SS)	APL product	A standalone APL product that acts as an AS-SIP B2BUA within the UC architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS.
Dual-Signaling Softswitch (DSSS)	APL product	A WAN SS used in the classified network that has both H.323 and AS-SIP signaling
Dual-Signaling Multipoint Control Unit (DSMCU)	APL product	APL product that supports multiple video conferencing signaling protocols, H.320, H.323, and AS-SIP
Edge Boundary Controller (EBC)	APL Product	Product providing firewall functions
Customer Edge (CE) Router	APL Product	Product providing routing functions at the enclave boundary
DISN WAN Provider (P)/Provider Edge (PE) Router	APL Product	Product providing routing of IP packets
DISN Multi-Service Provisioning Platforms (MSPP)	APL Product	Product providing transport access to the DISN WAN
M13 Multiplexer	APL Product	Product providing transport interface to the DISN
DISN Optical Switch	APL Product	Product serving as an optical transport node

4.5.1.3 Role of LSCs as Replacement for Existing Switching Systems

When an LSC is placed on the APL, it is also listed as a PBX1 until UCR 2008 expires without additional testing. Going forward, all existing local B/P/C/S TDM switching systems (e.g., PBX2, PBX1, SMEO, and EO) will eventually be phased out and replaced by LSCs.

4.5.1.4 Classified VoIP Network Design

[Figure 4.5.1-21](#), Classified VoIP Network Design Illustration, illustrates the classified VoIP 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 WAN SS capable of both H.323 and AS-SIP signaling, which is described in Section 6.2, Unique Classified Requirements.

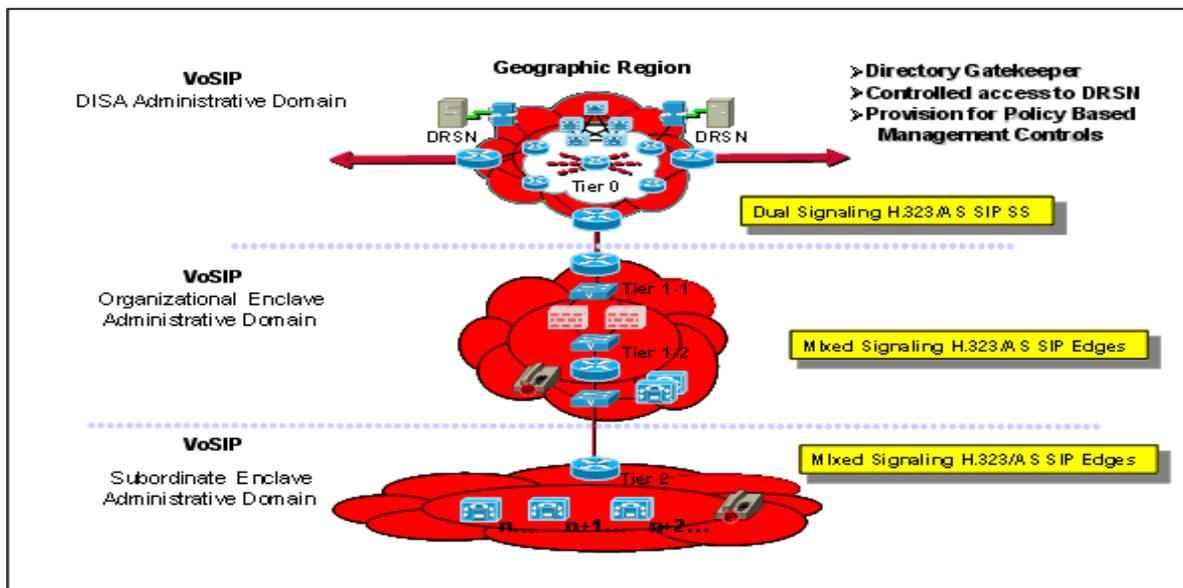
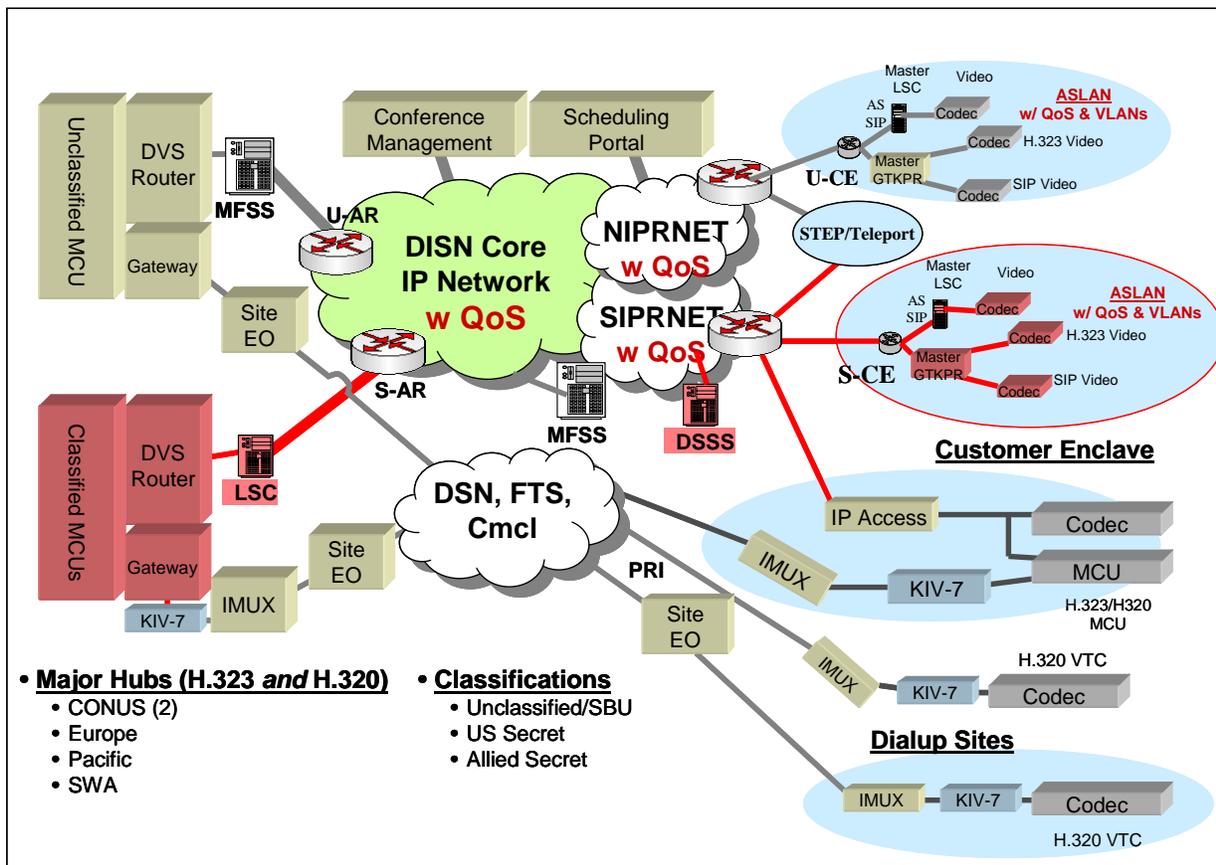


Figure 4.5.1-21. Classified VoIP Network Design Illustration

4.5.1.5 VTC Network Design

DISA provides VTC services as part of the DVS program for joint operations and the MILDEPs have their own VTCs for their unique COIs. The current Video Teleconferencing over IP (VTCoIP) E2E over both the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) does not provide assured

services. The current DoD VTC services use an IP signaling protocol, called H.323, that does not provide Assured Services. They also support video using a TDM protocol, H.320. Due to DoD Components' budgetary constraints and because the VTCoIP technology insertion must be determined by site-by-site business cases, current versions of DVS VTC and MILDEP VTC technologies will provide voice and video services over the DISN for many years. Therefore, the current DVS and MILDEP Multipoint Conferencing Units (MCUs), which use H.320 and H.323, will be augmented to become Dual Signaling MCUs (DSMCUs) supporting interoperability among H.323 and AS-SIP Edge video systems. Figure 4.5.1-22, DISN Dual Signaling MCU Design, illustrates the dual IP signaling involved in the VTC networks with backward compatibility to TDM video and the role of the DSMCU in that signaling.



H.323, and AS-SIP technology networks to set up video sessions among DoD Component sites with either non-assured or assured IP signaling technologies. The DSMCUs will support both classified VTC on SIPRNet and SBU VTC on NIPRNet.

4.5.1.6 DISN Router Hierarchy

[Figure 4.5.1-23](#), DISN Router Hierarchy, illustrates the DISN router hierarchy for FY 2009 for both the unclassified network and the classified network. At this point, the NIPRNet and SIPRNet routers have been transformed to be U-ARs and classified ARs connected to the Unclassified Provider Edge (U-PE) Routers and classified Provider Edge (C-PE) Routers.

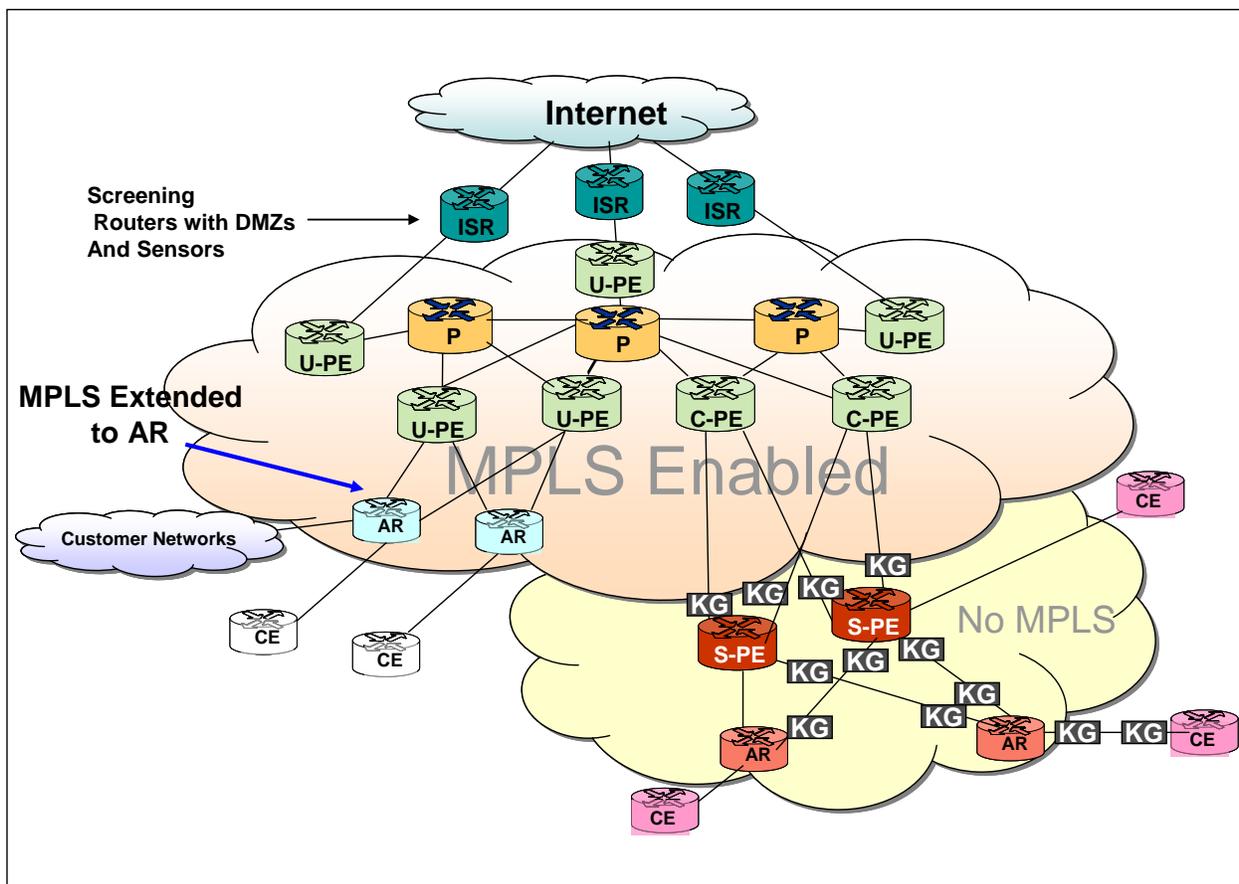


Figure 4.5.1-23. DISN Router Hierarchy

4.5.1.7 IPv6 Network Design

[Figure 4.5.1-24](#), IPv6 Design for SBU and Classified VVoIP, depicts the Internet Protocol version 6 (IPv6) network design for SBU and classified VVoIP and includes the DISN SDNs. All UC approved products will be IPv6 capable, and the VVoIP network will be an IPv6-enabled network during Spiral 2 of its capabilities deployments.

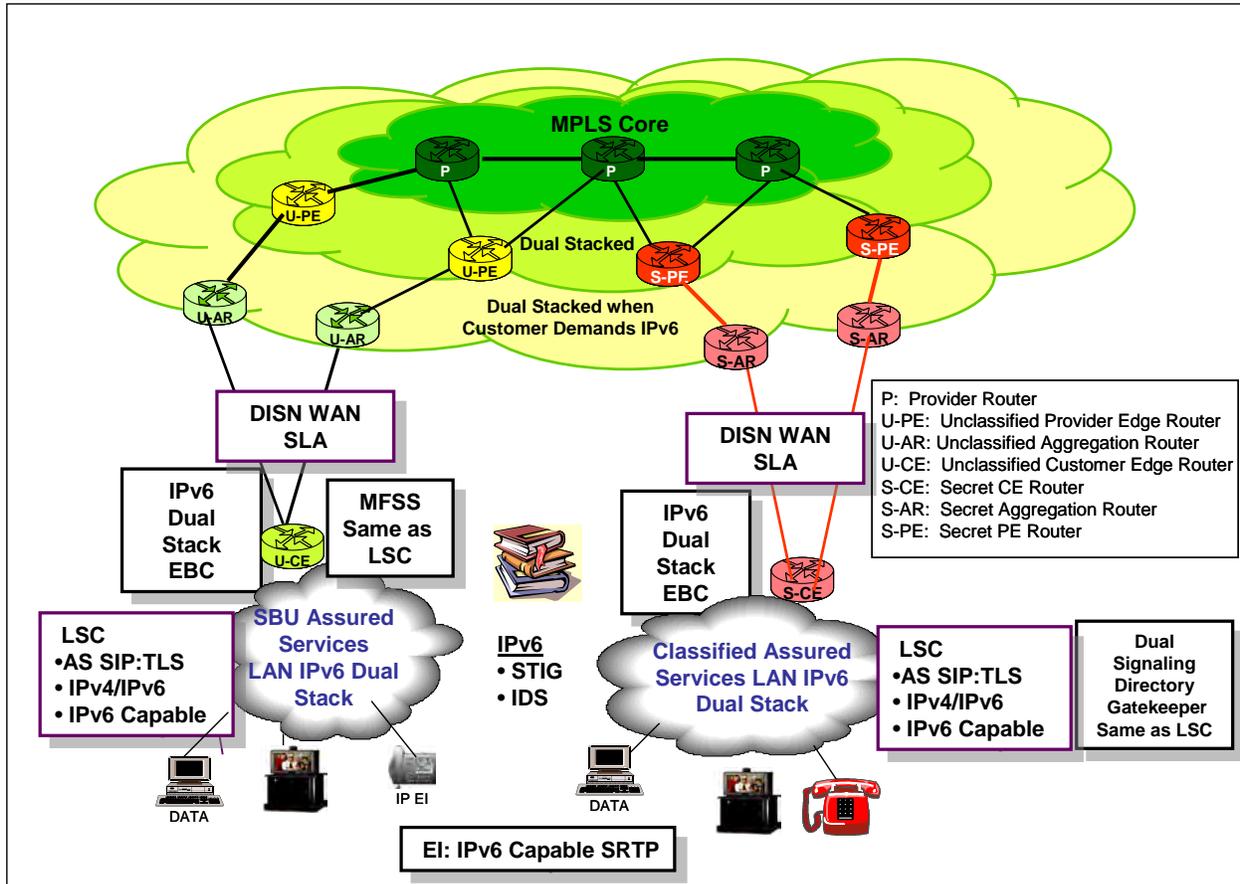


Figure 4.5.1-24. IPv6 Design for SBU and Classified VVoIP

4.5.2 Unified Communications

This section provides an overview of the initial system concepts for UC associated with network-wide collaboration services. The UC Collaboration services include multimedia or cross-media collaboration capabilities (including audio collaboration, video collaboration, text-based collaboration, and presence). The focus of the UC network-wide collaboration services is to go beyond local, intraenclave test events to implement and assess collaboration services and applications on an E2E, WAN-level basis. These UC network-wide collaboration services raise the need for new designs to address any potential performance, Information Assurance, or engineering/configuration issues associated with these different applications traversing the same ASLAN and Network Edge Segments.

4.5.2.1 UC Network-wide Collaboration Services

Leveraging the UCR 2008, Change 1, capabilities, the key UC network-wide collaboration services objectives are listed in [Figure 4.5.2-1](#), UC Network-wide Collaboration Services Objectives.

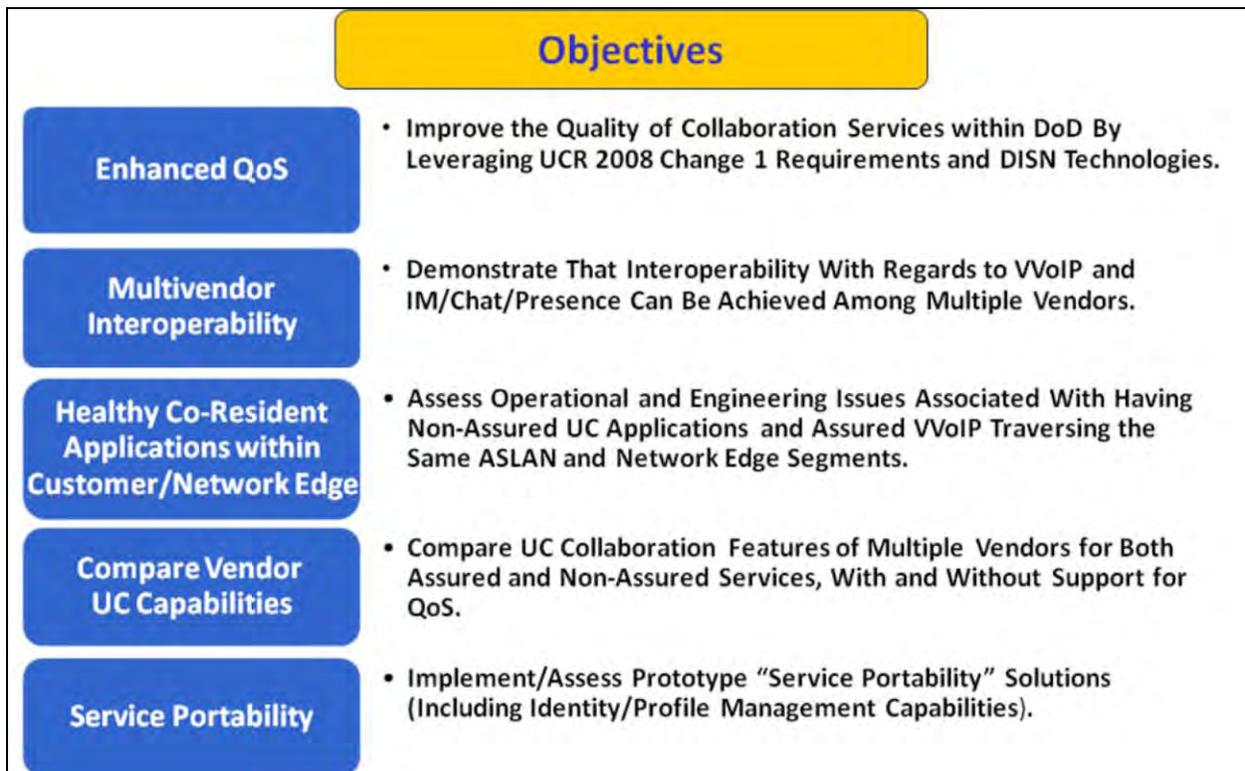


Figure 4.5.2-1. UC Network-Wide Collaboration Services Objectives

4.5.2.2 UC Network-Wide Collaboration Services Capability Increments

[Figure 4.5.2-2](#), UC Pilot Increments, shows the near-term, mid-term, and long-term network-wide collaboration services capability increments. The initial increment moves forward with the testing of COTS UC solutions that are not capable of individually “class marking” IP packets consistent with the DSCP Plan shown in Section 5.3.3.3, General Network Requirements. Next, is the implementation and assessment of products that can mark individual flows (i.e., voice, video, IM/Chat) as belonging to a particular traffic class per UCR 2008, Change 1, Differentiated Serviced (“DiffServ”) requirements. Longer term, path is mapped for how these UC applications can migrate to assured services to better support the needs of the mission-critical users.

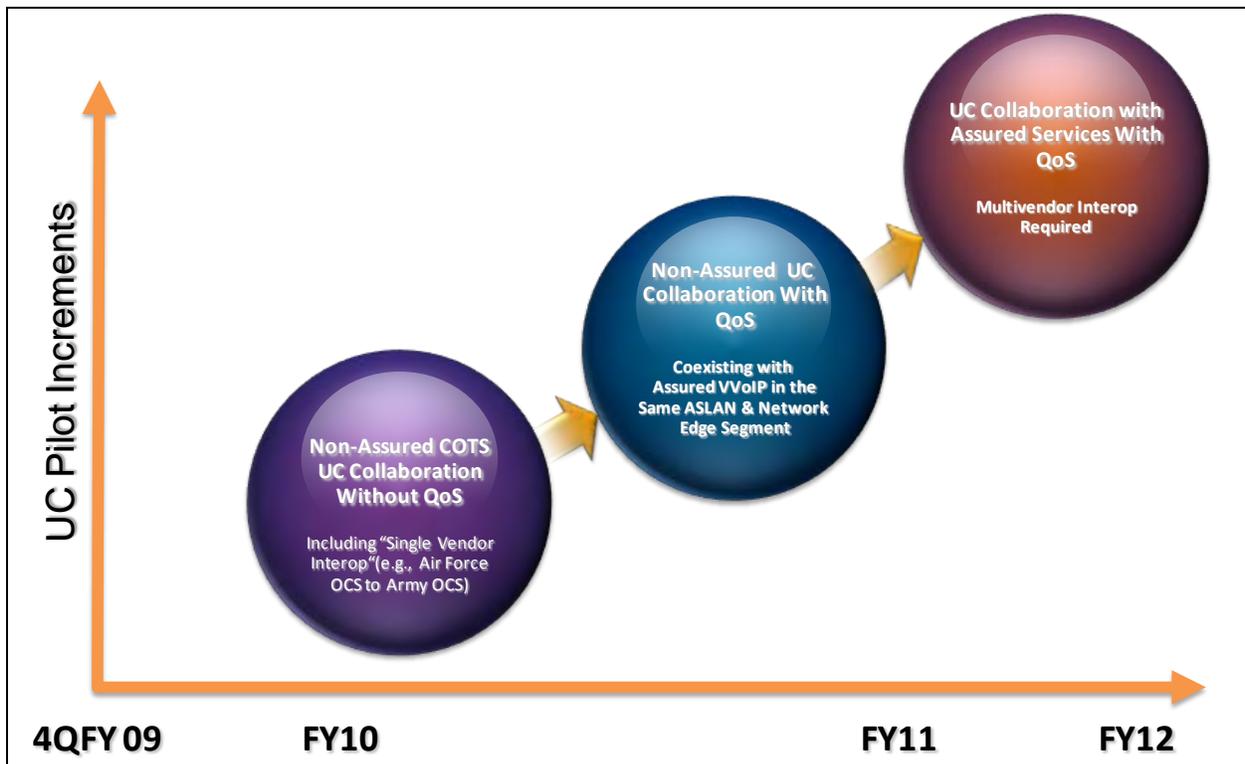


Figure 4.5.2-2. UC Pilot Increments

4.5.2.3 UC Network-wide Collaboration Services Capability Interoperability

Multivendor interoperability is needed to exploit the full potential of IM, Chat, and Presence across the DoD. Without multisystem, multivendor interoperability/federation, users can only exchange Presence information and IMs with users who belong to the same system or the same COI. With multisystem, multivendor interoperability, the DoD community can exploit the full potential of IM, Chat, and Presence. The concept of Federating simply refers to a server-to-server link that permits the exchange of Presence information and IM between the two systems.

Figure 4.5.2-3, Interoperability/Federation of IM, Chat, and Presence, illustrates the following IM, Chat, and Presence demonstrations:

- “Single vendor” interoperability (e.g., the ability to federate or bridge a vendor solution owned by the Air Force with the same vendor solution owned by another MILDEP)
- Multivendor interoperability

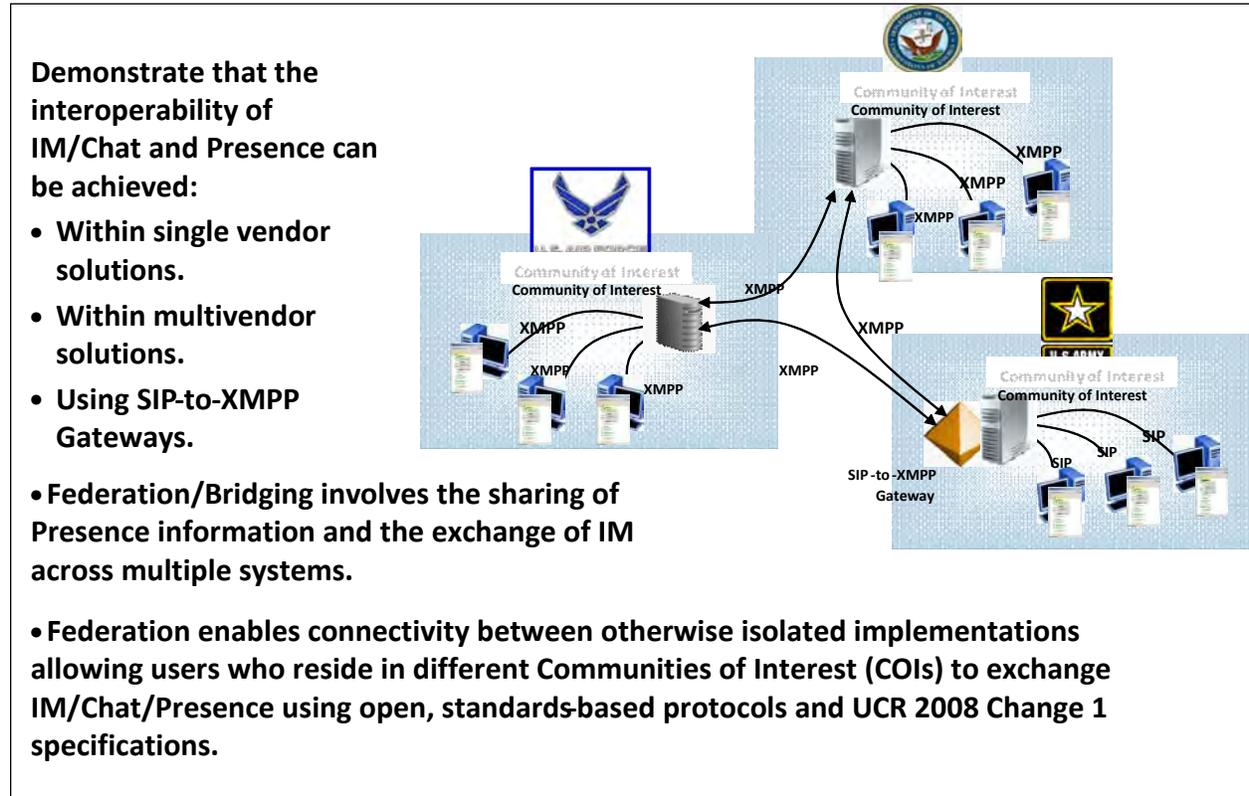


Figure 4.5.2-3. Interoperability/Federation of IM, Chat, and Presence

- The ability to federate native Extensible Messaging and Presence Protocol (XMPP) IM clients with native SIP/SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) IM clients through a SIP-to-XMPP gateway

4.5.3 Service Portability

Service portability is defined as the end user’s ability to obtain subscribed services in a transparent manner regardless of the end user’s point of attachment to the network. The key UC objective is to provide service continuity by ensuring mobile warfighters’ telephone numbers, e-mail addresses, and communication and collaboration tools remain constant as their mission and location change. [Figure 4.5.3-1](#), Mobile Warfighter’s Communication Dilemma, shows the problem service portability is trying to solve.



Figure 4.5.3-1. Mobile Warfighter's Communication Dilemma

To achieve this objective, the UC architecture needs to address the issues of service discovery, centralized authentication and authorization, and centralized directory integration and access. Service discovery is focused on allowing a roaming end user's client to discover the location of the service (i.e., LSC, e-mail server, XMPP server). Centralized authentication and authorization permits roaming users to access the network and receive their assigned privileges. Centralized directory integration and access is associated with ensuring a roaming user has access to end-user lookups (i.e., white pages) and to enable automatic user provisioning.

The near-term strategy is to deploy and assess prototype solutions in Spiral 1 and work with sponsoring MILDEPs to define test objectives, user requirements, and to resolve Information Assurance issues in order to complete a architecture. The lessons learned during Spiral 1 will be used to attain the mid-term strategy to incorporate the architecture and requirements into the UCR 2010. Based on the vendors implementing the architecture and requirements within their products and systems, the long-term strategy is to test and field the products and systems within the Deployed and S environments in the 2012–2013 timeframe.

4.6 UC PRODUCTS, APL PROCESSES, AND CONNECTION PROCESSES

This section provides an overview of the APL product categories and products with those categories. It defines the processes used to get the products placed on the APL and processes needed to gain connection approvals for the products. More detailed information is available at <http://www.disa.mil/ucco/>.

4.6.1 Overview of Approved Products

The UCR covers a broad variety of product categories and products within those categories that support UC. The two major product categories are network infrastructure and voice, video, and data services consistent with the definition of UC. Not all IT products are required to be on the APL. The DoD UC Steering Group advises ASD(NII)/DoD CIO with respect to which product categories and products should appear in the UCR, and thus, on the APL. APL products identified by the ASD(NII)/DoD CIO must be on the APL for DoD Components to acquire them. Products that have not been identified by the ASD(NII)/DoD CIO to be on the APL can be acquired by DoD Components. Still products must be granted a site Authority to Operate (ATO) and be operated IAW appropriate STIGs to gain DISN Authority to Connect (ATC).

Instant Messaging, Chat, Presence, and Collaboration UC Tool Suites are considered to be data UC products. These applications 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 that support SBU voice and video services; classified UC products for IP E2E systems that support SBU voice and video services; and in deployable products.

[Figure 4.6.1-1](#), 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.

[Figure 4.6.1-2](#), Classified VoIP UC Products, delineates the classified UC products.

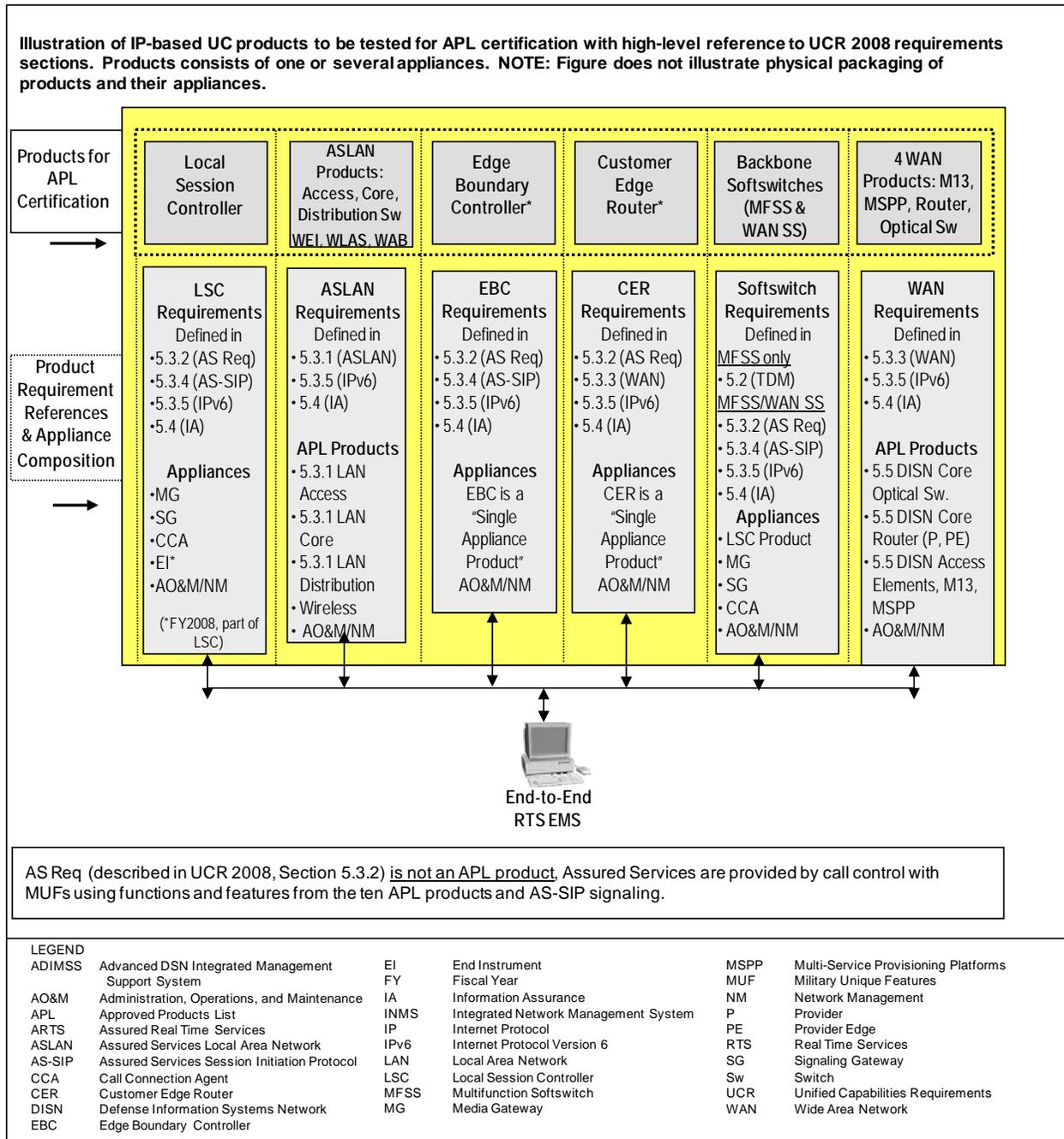


Figure 4.6.1-1. SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services

Section 4 – UC Description and Key Processes

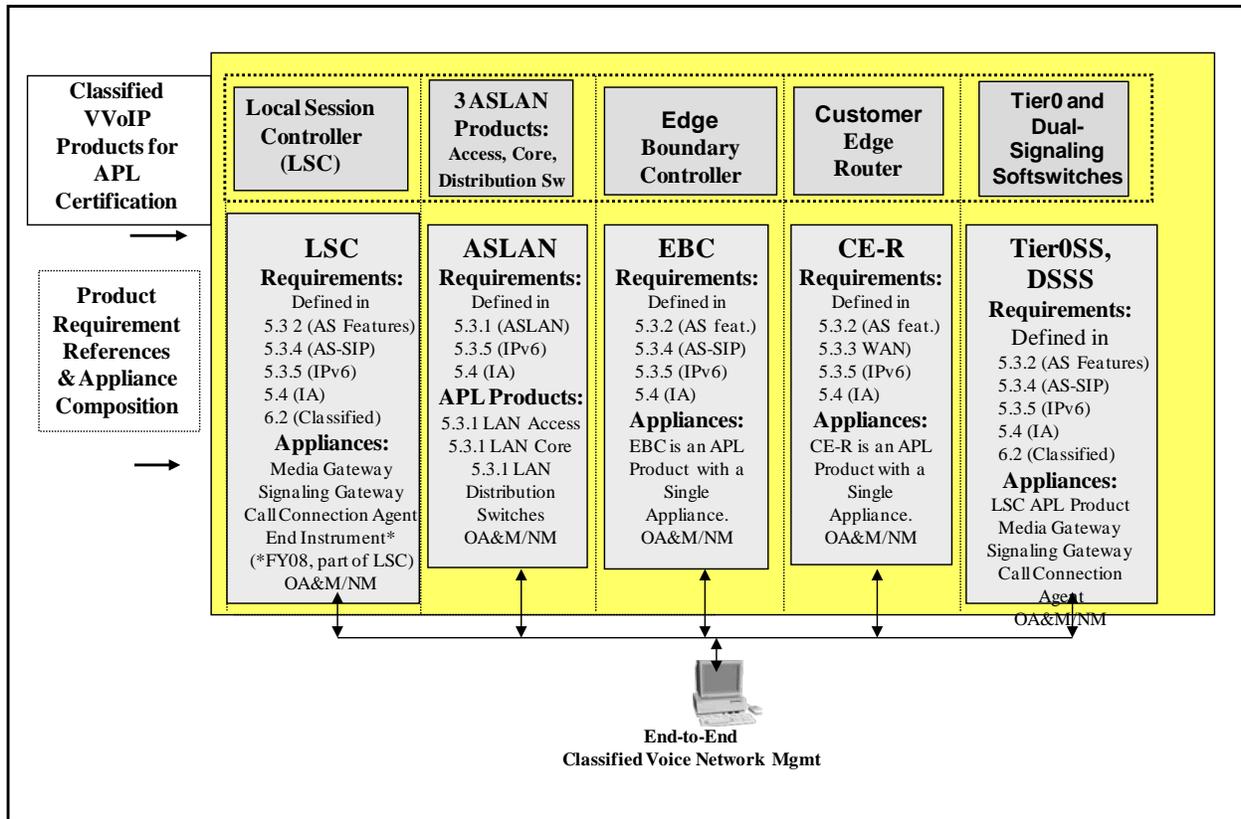


Figure 4.6.1-2. Classified VoIP UC Products

Table 4.6.1-1, DISN Network Infrastructure UC Product Categories, delineates the network infrastructure UC products that can be used by all MILDEPs for their Intranets. These UC products do not currently include data firewalls but will in future updates.

Table 4.6.1-1. DISN Network Infrastructure UC Product Categories

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

[Table 4.6.1-2](#) delineates the deployable UC products.

Table 4.6.1-2. Deployable UC Product Categories and Paragraph References

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	6.1.3	Deployable voice switch with ASF capabilities to support assured services requirements. This switch is used for rapid deployment situations and contingencies in the deployed environment.
Deployable NEs	5.9.3	NEs used in a deployed situations.
Deployable LANs	5.3.1 6.1.5	LAN used in deployed situations.
Deployed Tactical Radio	6.1.7	Deployable Radio systems used in a deployed situations.
DCVX	6.1.6	Deployable cellular voice switch with ASF capabilities to support assured services requirements. This switch is used for rapid deployment situations and contingencies.
LEGEND		
ASF	Assured Services Features	LAN Local Area Network
DCVX	Deployed Cellular Voice Exchange	NEs Network Elements
DVX-C	Deployable Voice Exchange – COTS	

[Table 4.6.1-3](#) delineates the encryption products. All these UC products include IPv6 capability.

Table 4.6.1-3. Security Devices 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 Information Assurance services for IPv4 and IPv6 networks. Encryption algorithms are not specified and are under the authority of NSA.															
Link Encryptors	5.6	Link Encryptors provide data security in a multitude of NEs, by encrypting point-to-point, netted, broadcast, or high-speed trunks. Encryption algorithms are not specified and are under the authority of NSA.															
FW	5.8	A product that blocks unauthorized access while permitting authorized communications.															
IPS	5.8	A product that detects unwanted attempts at accessing, manipulating, and/or disabling a computer system.															
VPN Concentrator	5.8	A product that sets up a secure link between an end user and an internal network.															
<table border="0"> <tr> <td colspan="2">LEGEND</td> <td></td> </tr> <tr> <td>HAIPE</td> <td>High Assurance Internet Protocol Encryptor</td> <td>IPv4 Internet Protocol Version 4</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>IPv6 Internet Protocol Version 6</td> </tr> <tr> <td>INFOSEC</td> <td>Information Security</td> <td>NSA National Security Agency</td> </tr> <tr> <td>IPS</td> <td>Intrusion Protection System</td> <td>VPN Virtual Private Network</td> </tr> </table>			LEGEND			HAIPE	High Assurance Internet Protocol Encryptor	IPv4 Internet Protocol Version 4	FW	Firewall	IPv6 Internet Protocol Version 6	INFOSEC	Information Security	NSA National Security Agency	IPS	Intrusion Protection System	VPN Virtual Private Network
LEGEND																	
HAIPE	High Assurance Internet Protocol Encryptor	IPv4 Internet Protocol Version 4															
FW	Firewall	IPv6 Internet Protocol Version 6															
INFOSEC	Information Security	NSA National Security Agency															
IPS	Intrusion Protection System	VPN Virtual Private Network															

The UC products acquired by the DoD Components, and connected or planned for connection to DoD networks, shall be both Interoperability and Information Assurance certified by DISA pursuant to the current UCR.

4.6.2 Overview of UC Interoperability and Information Assurance Processes

The UC Interoperability certification and connection approval processes are illustrated in [Figure 4.6.2-1](#), UC Requirements, Interoperability Certification, and Connection Approval Process. All UC products shall be tested and certified for Interoperability:

1. The ASD(NII)/DoD CIO provides overall policy and direction for development of UC requirements. DISA translates DoD Component functional requirements into engineering specifications for inclusion in the UCR. The ASD(NII)/DoD CIO approves the UCR for use in test and certification of UC products. The Joint Interoperability Test Command (JITC) develops the UC Test Plan (TP) based on the UCR. The UCR also may be used for UC product assessments and/or operational tests for emerging UC technology.

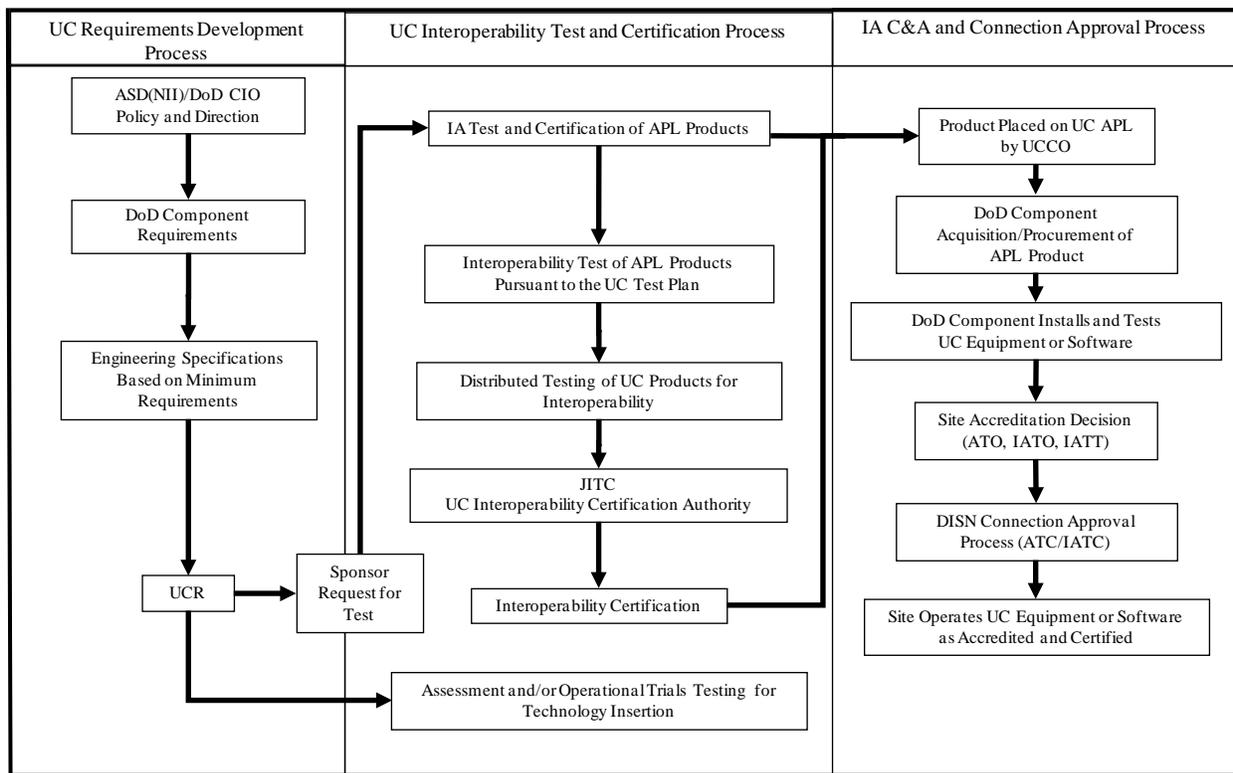


Figure 4.6.2-1. UC Requirements, Interoperability Certification, and Connection Approval Process

2. The JITC conducts Interoperability testing, adjudicates Interoperability test results, and provides certification, as appropriate. [Figure 4.6.2-1](#), UC Requirements, Interoperability Certification, and Connection Approval Process, depicts an overview of the UC requirements, Interoperability certification, and connection approval processes. The JITC uses distributed testing for UC Interoperability certification. The JITC serves as the UC Interoperability certifying authority.
3. The UC products certified for both Interoperability and Information Assurance shall be placed on the DoD UC APL by the UCCO. This APL is the single authoritative source for certified UC products on DoD networks. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless and until a waiver is approved. The DoD Components provide a site accreditation decision for the UC product to be installed. This accreditation decision may result in an ATO, Interim Authorization to Operate (IATO), or Interim Authorization to Test (IATT). DISA then provides an ATC or Interim Approval to Connect (IATC) to the DISN. When installed and connected, UC products shall be operated and maintained pursuant to DISA STIGs and the JITC Interoperability certified configuration.

The UC Information assurance certification, accreditation, and connection approval processes are illustrated in [Figure 4.6.2-2](#), UC Information Assurance Certification and Accreditation Process. The UC products on the DoD UC APL shall be granted Information Assurance certification by the DISA Certification Authority (CA).

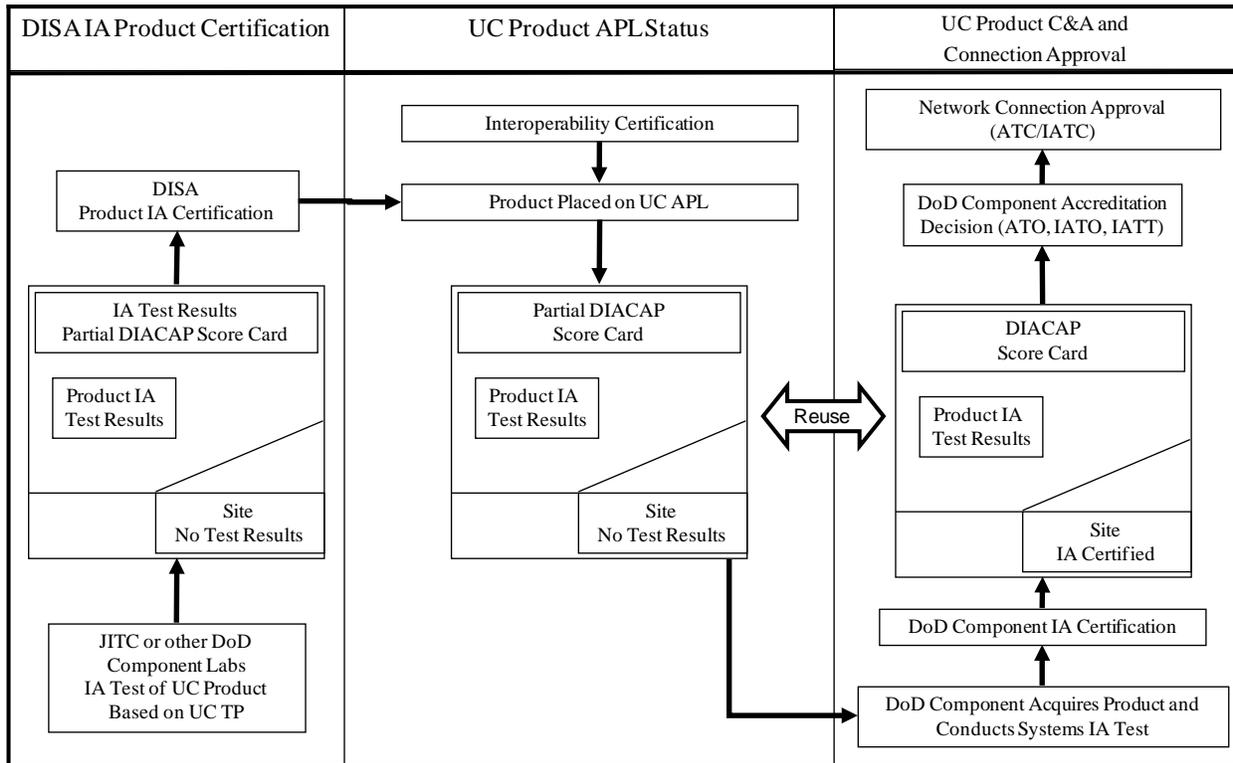


Figure 4.6.2-2. UC Information Assurance Certification and Accreditation Process

DISA oversees the Information Assurance certification process for UC products. The DoD Component Designated Accrediting Authorities (DAAs) certifies and accredits information systems (ISs).

1. DISA and other DoD Component test labs conduct Information Assurance testing and adjudicate Information Assurance test results for security features of products that provide UC services. The DISA CA issues Information Assurance certification. Once a UC product has received both Interoperability and Information Assurance certifications, that product is placed on the APL. [Figure 4.6.2-2](#) depicts the UC Information Assurance certification process.
2. The UC ISs are certified and accredited on a site-specific basis by the DoD Component DAA as part of the overall DoD Information Assurance Certification and Accreditation Process (DIACAP).

3. As an artifact of the Information Assurance test and certification process, the DoD Component test labs produce a partial DIACAP Score Card (as DoD Component test labs can completely test only a limited subset of Information Assurance controls, the remainder of the Information Assurance control tests must be completed on a site-specific basis, after Information Assurance certification). The partial DIACAP Score Card supports the Information Assurance certification and/or a type accreditation decision, and can assist a site in creating and implementing a security baseline, providing the foundation for obtaining an ATO. DISA maintains a repository of partial DIACAP Score Cards for reuse by the DoD Components.

4.6.3 Unified Capabilities Certification Office Processes

This section provides an overview of the UC approved products UCCO processes.

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. [Table 4.6.3-1](#) provides a matrix framework for deciding the maturity of technologies and the mission criticality of the features provided by the technologies. This matrix is used to determine which technologies need technology insertion assessment testing and DISN UC Spiral Deployment validations (i.e., prototype and preproduction assured and affecting assured services) and which are ready for product approval testing (i.e., APL or post APL testing of assured or affecting assured services). If the features are non-assured and do not affect Assured services, there is no need to test them and a vendor letter of compliance (LOC) will be accepted. Two processes, APL processes for mature products and APL process for technology insertion products, are addressed in the subsequent sections.

Table 4.6.3-1. Service Complexity vs. Technology Maturity Matrix for Determination of Type of APL Process

Services Complexity	Prototype	Pre-Production	APL Ready	Post APL
ASFs	<ul style="list-style-type: none"> • Full test • Or incremental test and/or desk-top review (DTR) if based on previously tested product 	<ul style="list-style-type: none"> • Full test • Or incremental test and/or DTR if based on previously tested product 	<ul style="list-style-type: none"> • Full test • Or incremental test and/or DTR if based on previously tested product 	<ul style="list-style-type: none"> • Full test for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product
Non ASFs Affecting ASFs	<ul style="list-style-type: none"> • Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor letter of compliance (LOC) of vendor tests of non assured services features meeting brochure claims 	<ul style="list-style-type: none"> • Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims 	<ul style="list-style-type: none"> • Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims 	<ul style="list-style-type: none"> • Partial test • Full test of interaction of features for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims
Non ASFs Not Affecting ASFs	<ul style="list-style-type: none"> • Random test of potential interactions 	<ul style="list-style-type: none"> • Random test of potential interactions 	<ul style="list-style-type: none"> • No test • Vendor LOC of vendor tests of features meeting brochure claims 	<ul style="list-style-type: none"> • No test • Vendor LOC of vendor tests of features meeting brochure claims

4.6.3.1 *Standard Process for Gaining APL Status*

The standard process for gaining APL status for all UC products is shown in [Figure 4.6.3-1](#). This process reflects that both Interoperability and Information Assurance certifications are required for placement on the UC APL.

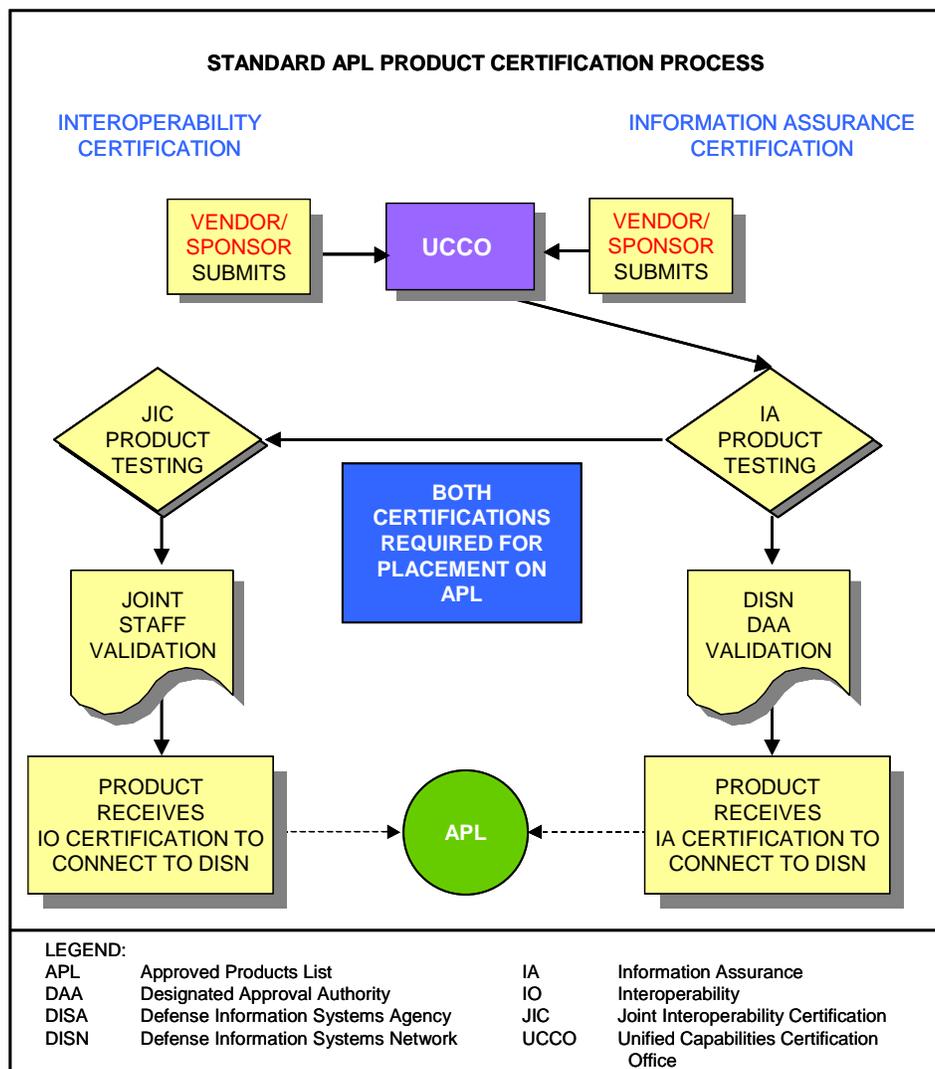


Figure 4.6.3-1. Standard UC APL Product Certification Process

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

1. A product enters the UC APL process by obtaining DoD Component sponsorship and providing both Interoperability and Information Assurance information as shown in [Figure 4.6.3-1](#).
2. If a product successfully passed both Interoperability and Information Assurance portions of the testing, the product is placed on the UC APL. This listing is good for 3 years beginning on the day the UCCO announces the vendor's APL status, if no product changes are made. After the 3-year period has finished, products are placed on the "Retired List."
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 because 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, or deletion has been approved on the date the UCR is signed, one of three dispositions will occur as follows:

1. The vendors will have 18 months to develop the requirement 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.

The 18-month period for development would apply to a new feature or a product not previously required, and the vendors did not have long-range knowledge of the requirement. New features or products in this version of the UCR are included in [Table 4.6.3-2](#), New Features and Products in UCR for Which 18-Month Rule Applies.

A change sheet for the Section 5, Unified Capabilities Product Requirements, will identify which changes are subject to the 18-month rule and which ones are not.

Table 4.6.3-2. New Features and Products in UCR for Which 18-Month Rule Applies

FEATURES	SECTION OF THE UCR
AS-SIP VTC Functionality	5.3.4.9.7.4
AS-SIP Generic End Instrument	5.3.2.6
V.150.1 Modem Relay Secure Telephone Support	5.3.2.21
AS-SIP TDM Gateway	5.3.2.7.4
AS-SIP IP Gateway	5.3.2.7.5
WAN SS	5.3.2.8.4
DSSS	6.2
Commercial Cost Avoidance	5.3.2.23
DSMCU	4.4.1.4
AS-SIP-Based Interfaces for Voicemail and Unified Messaging Systems	5.3.2.24
Information Assurance Requirements overlay for IM/Chat/Presence Awareness	5.7
IPv6 Profile 4.x Updates	5.3.5
SSH PKI Requirements	5.4
Deployed Tactical Radio	6.1.7

A new APL process has been introduced called Fast Track (FT). The FT process is intended to expedite products onto the APL. The FT process is structured to deal with the fact that DoD sponsors have a need for products for which they have reasonably well-established requirements, and in some cases, test results. Yet these products do not appear in the UCR that is published on an annual basis. If the UC Steering Group agrees that new product categories and/or new products should be in the UCR, the DoD sponsors and vendors do not have to wait for the next UCR to get tested and placed on the APL. The APL testing can begin based on existing requirements that will be placed in the next version of the UCR. Products that are candidates for the FT process are as follows:

- Products that are within existing UCR product categories with well-established requirements, and in some cases, the existing requirements can be augmented by current UCR requirements
- Products that have existing test results that can be reused
- Products that are currently fielded and successfully performing from both an Interoperability and Information Assurance perspective in operational networks
- Products that should be added to the UCR per the UC Steering Group

Three categories of FT products are as follows:

Section 4 – UC Description and Key Processes

1. Products within Current UCR Product Categories. Products that were tested by JITC before development of the product category or products that have existing requirements that are similar to those in the UCR that can be augmented with UCR requirements.
2. Operationally Validated. Products that are currently operating in DoD networks that have an IATO or ATO, are in compliance with appropriate STIGs, and are requesting APL status. Products may be end of life (i.e., retired APL status) or active (i.e., normal APL status).
3. New UCR Product Categories. Products that have existing DoD (non-UCR) requirements that can be used in the next version of the UCR and have been approved for the UCR by the UC Steering Group.

Additional and current information concerning the APL process can be obtained from the following online sources:

- UC APL Pages
 - UCCO Main Page: <http://www.disa.mil/ucco/>.
 - UCCO Policies and Procedures: This page contains important instructions and a breakdown of the UCCO Process (http://www.disa.mil/ucco/apl_process.html).
- ATC Pages
 - ATC Main Page: <http://www.disa.mil/connect/>.
 - ATC Policy, Guidance, and Procedures: <http://www.disa.mil/connect/library/index.html>.
 - ATC Process Overview: <http://www.disa.mil/connect/overview/index.html>.