Department of Defense

Unified Capabilities Requirements 2008, Change 3 (UCR 2008, Change 3)

Final

September 2011

The Office of the DoD Chief Information Officer

DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2008, CHANGE 3 (UCR 2008, CHANGE 3)

This document specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support Unified Capabilities (UC), and shall be used to support test, certification, acquisition, connection, and operation of UC devices.

This document fulfills the requirements specified in DoD Instruction (DoDI) 8100.04 for the development of a UC requirements document.

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 1
PURPOSE

1.1 The "Department of Defense Unified Capabilities Requirements 2008, Change 3 (UCR 2008, Change 3)" (hereinafter referred to as "UCR"), specifies the technical requirements for certification of approved products to be used in Department of Defense (DoD) networks to provide end-to-end Unified Capabilities (UC).

1.2 This document supersedes UCR 2008, Change 2.

1.3 The UCR specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may be used also for UC product assessments and/or operational tests for emerging UC technology. The Defense Information Systems Agency (DISA) translates DoD Component functional requirements into engineering specifications for inclusion into the UCR, which identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR also defines interoperability, Information Assurance, and interface requirements among products that provide UC. The information assurance portion of the UC Test Plan (TP) shall be based on the requirements of the UCR as derived from DoD Instruction (DoDI) 8500.2.

1.4 The UCR is based on commercial off-the-shelf (COTS) products' features, standards listed in the DoD Information Technology Standards Registry (DISR), and unique requirements needed to support DoD mission-critical needs.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 2
APPLICABILITY, DEFINITION, AND SCOPE

2.1 APPLICABILITY

Per DoDI 8100.04, 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 (JS), 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 (hereafter referred to collectively as the "DoD Components").

2. DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies (e.g., circuit-switched and/or Internet Protocol (IP)), and whether converged or non-converged, including 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.

3. Acquisition of services as described in DoD Directive (DoDD) 5000.01 and DoDI 5000.02.

2.2 UC DEFINITION

Unified Capabilities are the integration of voice, video, and/or 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.

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/Requirements, provides a broad overview of policies and requirements that will be implemented in the UCR with emphasis on policies and requirements that govern information assurance and interoperability requirements and testing of products used to provide DoD UC.

4. Section 4, Unified Capabilities Mission Requirements, E2E Network Descriptions, and Key Certification Processes, provides the Product Categories Requirements Matrix (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.

5. Section 5, Unified Capabilities Product Requirements, describes technical requirements, features, and test configurations of equipment used to achieve DoD UC Approved Products List (APL) status. 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 UC Requirements.

7. 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/REQUIREMENTS

3.1 POLICY AND REQUIREMENTS FRAMEWORK FOR UC IMPLEMENTATION

This section provides a broad overview of requirements for DoD Component planning, investment, development, acquisition, operations, sustainment, and management of DoD networks that provide UC.

UC provides the integration of voice, video, and/or 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. UC 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, including business, intelligence, and warfighting. Capabilities are provided to fixed and deployed users to include ground, airborne, and seaborne mobile/transportable platforms.

The UC requirements process addresses DoD-level warfighter and Intelligence Community needs based on approved DoD architectures and Joint Staff requirements. These UC requirements shall be reflected in DoD Unified Capabilities Requirements (UCR) document, the UC Master Plan (UC MP), the UC Operational Framework, and DoD Component UC implementation plans.

Per DoDI 8100.04, Subject DoD Unified Capabilities, implementation of UC across DoD is dependent on UC transport, which is the secure and highly available enterprise network infrastructure used to provide voice, video, and/or data services through a combination of DoD and commercial terrestrial, wireless, and satellite communications (SATCOM) capabilities.

Implementation of UC is required to meet the requirements of the IP-enabled battlefield of the future. UC allows the DoD to achieve the following warfighter needs:

- Ubiquitous, robust, and scalable DoD networks, enabling integrated operations

- IP-addressed sensors, munitions, biosensors, and logistics tracking applications, which shall enhance situational assessments and information availability

- End device-to-end device security, authentication, and non-repudiation, which shall enable new information assurance strategies that support mission assurance

- Increased operations tempo supported by rapid reorganizational capabilities, shared situational awareness, and improved wireless and mobility support

- Greater support for mobility and communications on the move

- Dynamic formation of a Community of Interest (COI) supported by improved multicasting

- Real-time collaboration using integrated voice, video, and data capabilities

- Situational awareness using Network Operations (NetOps) COI information sharing

- Rapid and agile information technology infrastructures with the capability to "discover" adjacent networks and plug and play to facilitate quicker, more dynamic responses

Figure 3.1, Policy, Requirements, and Planning Documentation, depicts the policy, requirements, and planning, documentation for UC implementation.

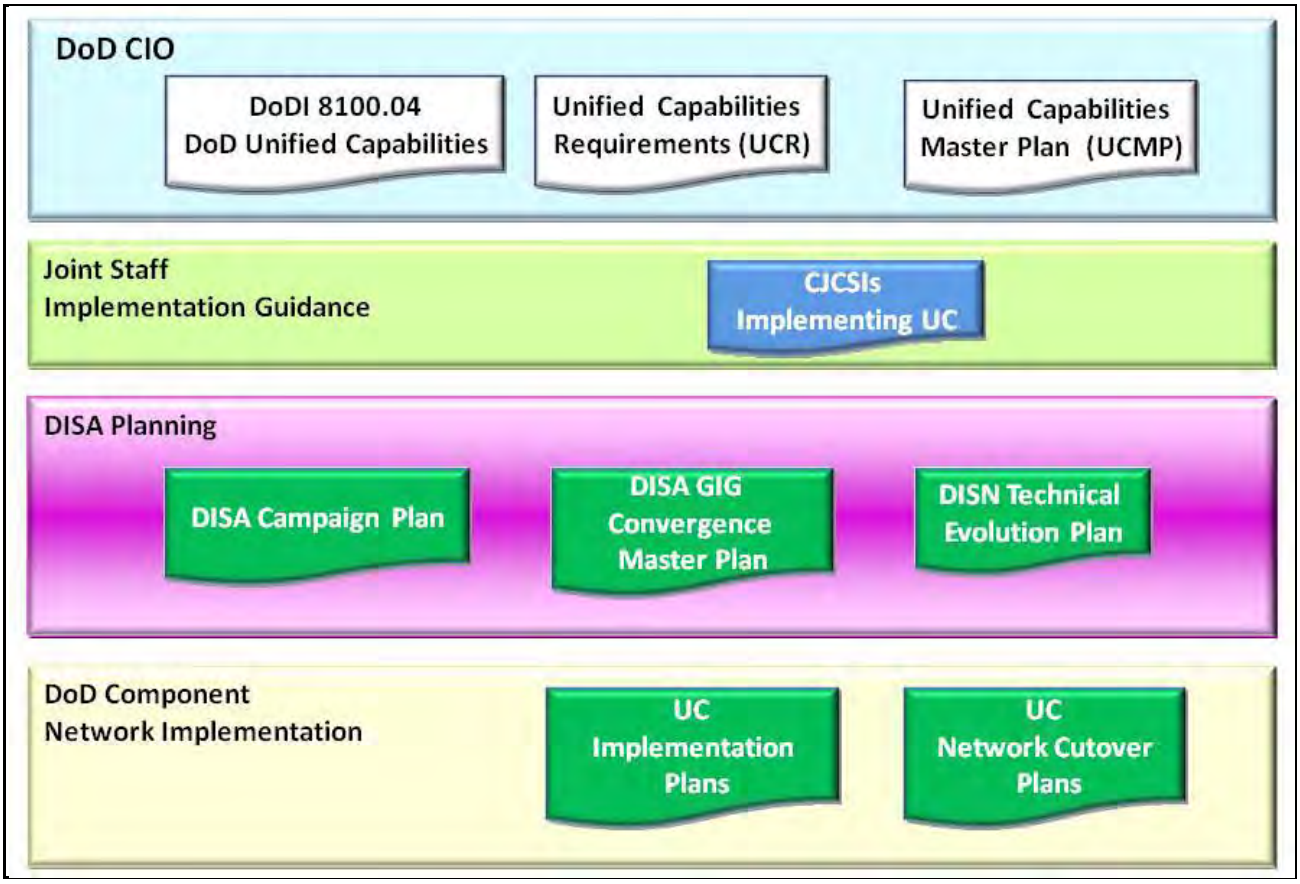


Figure 3.1. Policy, Requirements, and Planning Documentation

1. The four key DoD Chief Information Officer (DoD CIO) documents that drive UC implementation are:

   a. Secretary of Defense Memorandum, "Department of Defense (DoD) Efficiency Initiatives", which directs the Department to "consolidate DoD's Information Technology (IT) infrastructure where possible, to achieve greater economies of scale." The goals of this Memorandum are "to reduce duplication, overhead, and excess, and instill a culture of savings and restraint across the DoD." The Department shall achieve these goals and deliver a streamlined, rationalized, and simpler network by consolidating IT infrastructure across DoD. The UC MP addresses the enterprise UC supporting this Memorandum.

   b. DoDI 8100.4, which establishes policy, assigns responsibilities, and prescribes procedures for test; certification; acquisition, procurement, or lease; effective, efficient, and economical transport; connection; and operation of DoD networks to support UC. Additionally, it establishes the governing policy for UC products and services supported on DoD networks.

c. DoD UCR, which specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and supports test, certification, acquisition, connection, and operation of these devices.

d. The UC MP, which defines the UC operational framework and strategy for enterprise converged, net-centric, IP-based UC. It serves as a guideline to the DoD Components in the preparation of implementation plans and acquisition plans for phasing in enterprise UC. It initially focuses on UC that can be matured and fielded by Fiscal Year (FY) 2016 within the constraints of DoD Component resources, mission needs, and business cases. The UC MP will be updated biennially, as required.

2. The Joint Staff publishes, as appropriate, implementing instructions for UC based on DoD CIO's direction and guidance.

3. The major DISA planning documents driving and supporting UC activities are:

a. The "DISA Campaign Plan," which identifies three Lines of Operations: Enterprise Infrastructure; Command and Control (C2) and Information Sharing; and Operate and Assure, with specific tasks for UC implementation.

b. The "DISA Global Information Grid (GIG) Convergence Master Plan," which identifies five categories of DISA programs: Application, Services, and Data; Communications and Networks; Information Assurance; Network Operations and Enterprise Management; and Computing Infrastructure.

c. The "Defense Information Systems Network (DISN) Technical Evolution Plan (DTEP)," based on the DISN Overarching Technical Strategy (DOTS), addresses the plan for DISN UC technical implementation. The DTEP describes the plan for DISN technical refresh funds to augment and sustain the DISN. The DTEP also addresses technology implementation requirements outlined in the DoD UCR. The DTEP's four capability areas are Information Assurance, Connectivity, Network Management, and Interoperability.

4. Documents essential to synchronizing investments across DoD, by DoD Components, are:

a. The DoD Component UC implementation plans shall synchronize the specific deployments of UC from a converged, consolidated, and integrated family of commercial and DoD networks perspective, based on DoD Components' acquisition plans. DoD Component UC implementation plans shall be used to address detailed costs, funding, schedules and transition phases, and system designs to be implemented. DoD Component UC implementation plans shall be based on the

proven risk management process used for UC which includes the development of UC requirements based on collaboration with DoD Components and industry, DoD CIO sponsored and DISA hosted multi-vendor test events at DoD Component test laboratories, UC Spirals for operational validation based on DISN UC Concept of Operations (CONOPS) resulting in DoD UC approved products.

b. DoD Component UC Network Cutover Plans (NCPs) shall ensure site and transport readiness, security of mobile devices, and integration with DoD and commercial networks. DoD Components' UC NCPs shall be used to facilitate the DISN connection approval process to fulfill DoD Component UC service requests.

3.2 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.

3.2.1 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 Base/Post/Camp/Station (B/P/C/S) 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 or UC Transport) portion of the network.

2. Assured Information Protection.

   a. Secure End Instruments (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 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. Execution of PBAS is required on the sessions at the access and egress to the wide area network (WAN) to meet mission needs. The WAN is expected to provide Quality of Service (QoS) to the sessions allowed by PBAS to access the WAN. The WAN need not be involved in precedence and preemption of the sessions, which will be determined at access and egress. 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 JS and COCOMs. All users shall be capable of receiving precedence UC services sessions, since locations of crises and wars cannot be determined in advance.

   c. UC services must provide nonblocking service (i.e., P.00 threshold) from user to user for FLASH and FLASH OVERRIDE sessions. (NOTE: P.00 denotes that out of every 100 sessions, the probability is that zero sessions will be blocked.)

   d. Precedence-based sessions placed to end instruments (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 situational awareness (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 Element Management Systems (EMSs) that allow for read-write access for the systems for which they have direct responsibility. In addition, the U.S. Cyber Command (CYBERCOM)-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 and Network Operations and Security Centers (NOSCs) shall enable end-to-end visibility and the configuration of network components, as needed to respond to SA. All actions shall be coordinated with affected DoD Components before such actions are taken, if possible, consistent with the "Operational Tempo," and after such actions are taken.

f. Prevention of blocking of precedence 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. UC 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. UC networks shall be designed to assure that end-to-end voice, video, and data performance are clear, intelligible, and not distorted or degraded, using commercial standards performance metrics. The DoD UC networks shall be designed to meet voice, video, and data performance requirements end-to-end. Deployed UC networks can provide degraded performance consistent with meeting mission needs as compared to Fixed UC network performance.

k. Non-assured voice and video flows shall be policed or controlled to ensure they do not degrade the performance of assured voice and video flows that are using PBAS.

SECTION 4
UNIFIED CAPABILITIES MISSION REQUIREMENTS, E2E NETWORK DESCRIPTIONS, AND KEY CERTIFICATION PROCESSES

4.1 OVERVIEW

This section describes the UC Operational Framework, end-to-end UC network designs that illustrate how the UC products are employed to provide UC, 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 Approved Products List (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 OPERATIONAL FRAMEWORK

This framework is intended to guide and align DoD Component instantiation of respective implementation plans and solutions. It provides a common language and reference for DoD Components' implementation of UC technology, supports implementation of DoD Component solutions, and encourages adherence to common standards and specifications. All DoD Components shall develop and align respective Component implementation plans within this framework consistent with the constraints of DoD Component resources, mission needs, and business cases. The transition will begin in FY 2012. DoD Components implementation plans shall support individual mission requirements, business cases, and most cost effective implementation of enterprise UC.

Per DoDI 8100.04, all networks that support UC shall use certified products on the DoD UC APL, which may be found at http://disa.mil/ucco. Beginning in FY 2014, DoD Components shall be responsible for ensuring compliance with this operational framework.

4.2.1 Overview and Summary

The UC High Level Operational Framework illustrated in Figure 4.2.1, UC High Level Operational Framework, enables strategic, tactical, classified, and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks.

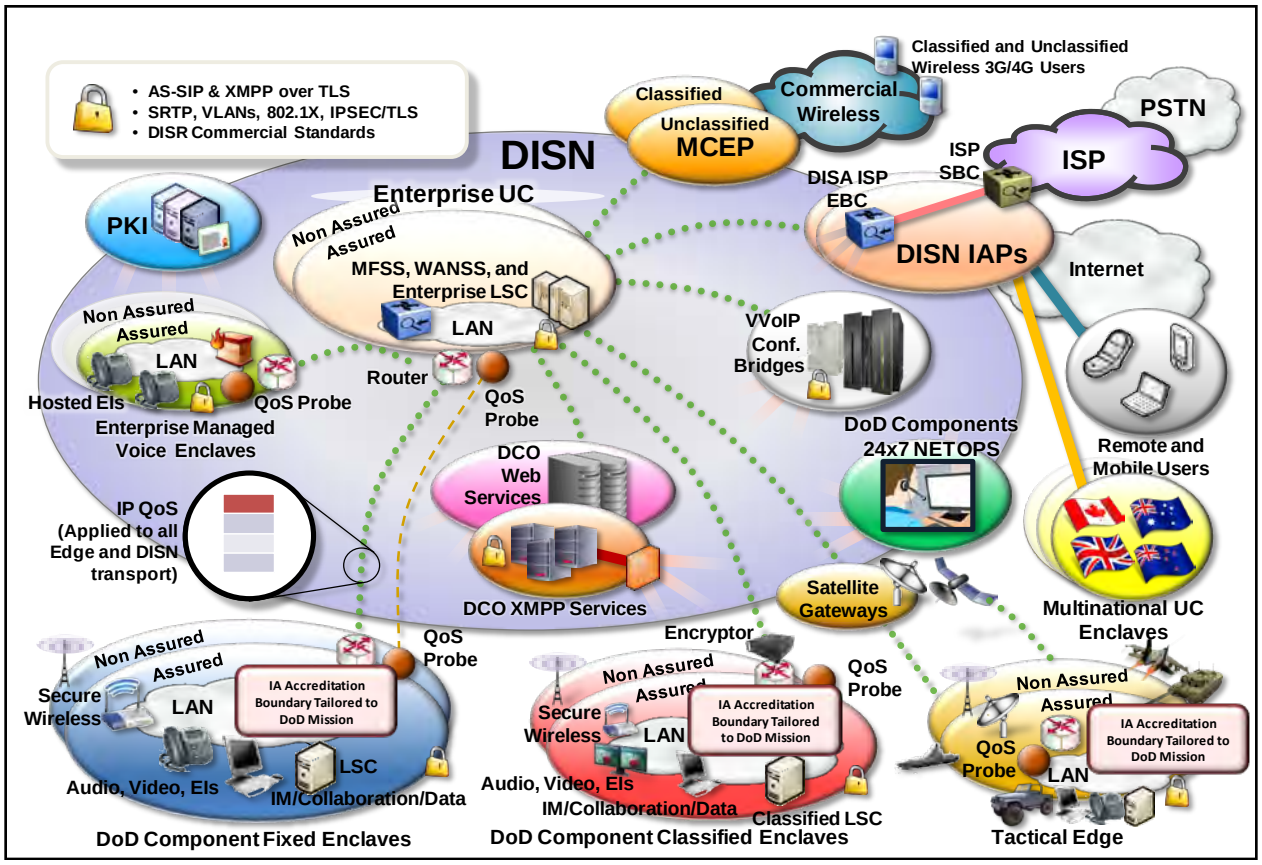


Figure 4.2.1 UC High Level Operational Framework

The operational framework is based on the extensive work already accomplished by DISA through laboratory and pilot testing using interoperable and secure products from the DoD UC APL, and deploying those products in the DISN backbone infrastructure. Because of the progress made to date, DoD has already begun deployment of approved IP-based products. This operational framework leverages IP technologies, and DoD aggregated buying power, to provide enterprise UC solutions by collaboration between DISA as the backbone and edge services provider, and the DoD Components as the edge infrastructure providers and users.

This operational framework is consistent with the Secretary of Defense Memorandum "DoD Efficiency Initiatives" goals and corresponding enterprise UC initiatives. By implementing enterprise multi-vendor UC investment in, and operating costs for, those services may be reduced using common and standard service models. Implementation of enterprise UC can provide a full range of related capabilities to all DoD users from central locations that leverage the DISN, and IP technologies. This approach minimizes potential duplication of costs that may occur for UC operations and maintenance, network operations, sustainment, and information assurance at DoD Component locations worldwide.

This operational framework leverages the requirements of the DoD UCR document, which has been coordinated with DoD Components and industry.

This operational framework shall continue to evolve as it is tested via multi-vendor test events, demonstrated via conduct of enterprise product solutions at DoD test laboratories, and implemented using planned UC pilot test and evaluation activities. The UCR shall be updated based on multi-vendor test events independently evaluated results.

4.2.2 Enterprise UC Vision

Figure 4.2.2, Enterprise UC Vision, describes the vision for unclassified and classified enterprise UC, enterprise and edge infrastructures, and secure access to various other networks. The key tenets of the Enterprise UC vision is the deployment of an Enterprise Local Session Controller (ELSC) in conjunction with the DoD Component edge infrastructure. The ELSC centrally provides the functionality essential for delivering enterprise non-assured and assured services securely across a QoS-enabled network using multiple vendor products. ELSCs may be deployed by individual DoD Components during the transition period to the UC operational framework.

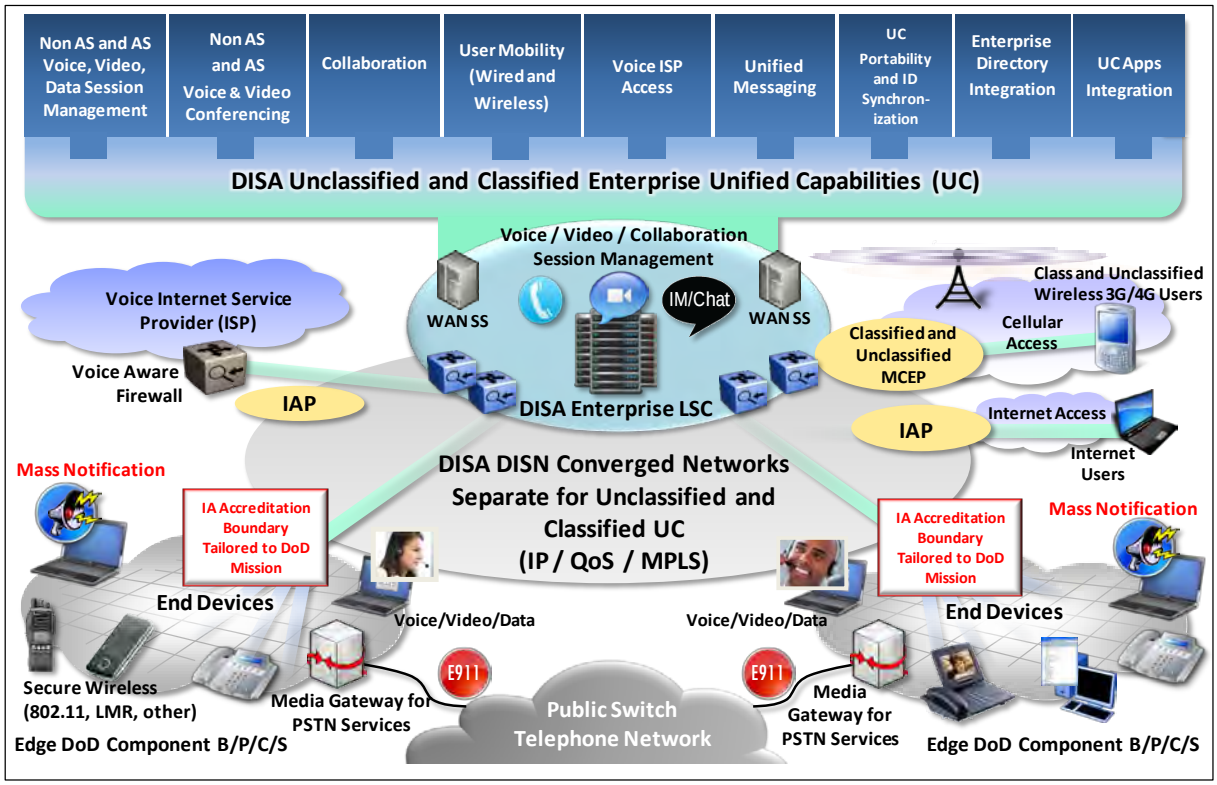


Figure 4.2.2. Enterprise UC Vision

The DoD Component edge infrastructure provides non-assured and assured enterprise services to the end user fixed or mobile devices. The edge infrastructures can consist of either a separate

security enclave or regional enclaves connected to the DISN core infrastructure. The edge includes non-assured and/or assured LANs (wired and wireless) tailored to meet mission needs that support converged UC consistent with DoD Component implementation plans. Consistent with DoD Component mission requirements and resources constraints, access to the Public Switched Telephone Network (PSTN) shall be via circuit switches until secure access to the voice Internet Service Provider (ISP) is accomplished centrally at the DISA Internet Access Point and ELSC, at which time the DoD Component may decide to migrate to an ISP offering, as appropriate.

When IP access to the ISP is implemented, all connections shall be managed by the ELSC to centrally protect the network. The handling of 911 calls may occur via the site local TDM connection, but other means of 911 calling could be utilized in the future as well. Calls to the PSTN could occur either via the local MG connection or the ISP connection in this case. The operational framework shall support local Enhanced 911 (E911), mass notification services, and critical emergency response capabilities. User requirements for non-assured and assured services shall be determined by the appropriate DoD Component.

The unclassified and classified enterprise UC, in priority order for implementation during the period of FY 2012 to FY 2016, include:

1. Non-Assured/Assured Voice, Video, and Data Session Management: Provides enterprise point-to-point UC, independent of the technology (circuit switched or IP). Capabilities include, but are not limited to, end device registration, session establishment and termination, and UC session features (e.g., Assured Services Admission Control, Call Hold, Call Transfer).

2. Non-Assured/Assured Voice and Video Conferencing: Provides the ability to conference multiple voice or video subscribers with a variety of room controls for displays of the participants. It also includes an optional component that allows subscribers to schedule conferences.

3. Collaboration: Provides IP-based solutions that allow subscribers to collaborate (e.g., instant messaging, chat, presence, and Web conferencing).

4. User Mobility (wired and wireless): Provides the ability to offer wireless and wired access, for UC supported by multifunction mobile devices. In addition, it provides access to enterprise UC globally using UC portability.

5. Voice Internet Service Provider (ISP) Access: provides unclassified and classified enterprise UC for access to commercial voice services over IP. This service provides both local and long distance dialing capability using commercial ISPs via secure interconnections.

6. Unified Messaging: Provides the integration of voicemail and e-mail. The integration of these two capabilities allows subscribers to access voicemail via e-mail or access e-mail via voicemail.

7. UC Portability and Identity Synchronization: Provides an enterprise UC systematic approach to portability functions (e.g., repository of user profiles and privileges, and subscriber identification and authentication). Uses DISA's existing Identification (ID) Synchronization service as the primary service for DoD ID Synchronization.

8. Enterprise Directory Integration: Integrates UC with repository of subscriber contact information accessible to all authorized and authenticated subscribers.

9. UC Applications Integration: Supports mission and business applications integration with the enterprise UC (e.g., integration of UC provided presence with DoD Component-owned business applications).

4.2.3 High Level Operational Concept

Figure 4.2.3, DISN Backbone Infrastructure, illustrates the DISN backbone infrastructure for up to 22 locations globally supporting a set of Geographic Regions (GeoRegions) based on DoD populations in Continental United States (CONUS) and Outside the Continental United States (OCONUS) as part of the DISN investments and the DISN Subscription Services (DSS). This backbone shall make available services to user end devices for DoD Component locations depending on individual DoD Component's mission requirements. Final decisions on the GeoRegions shall be made as part of the DoD Components collaborative UC Implementation Plan integration activities.

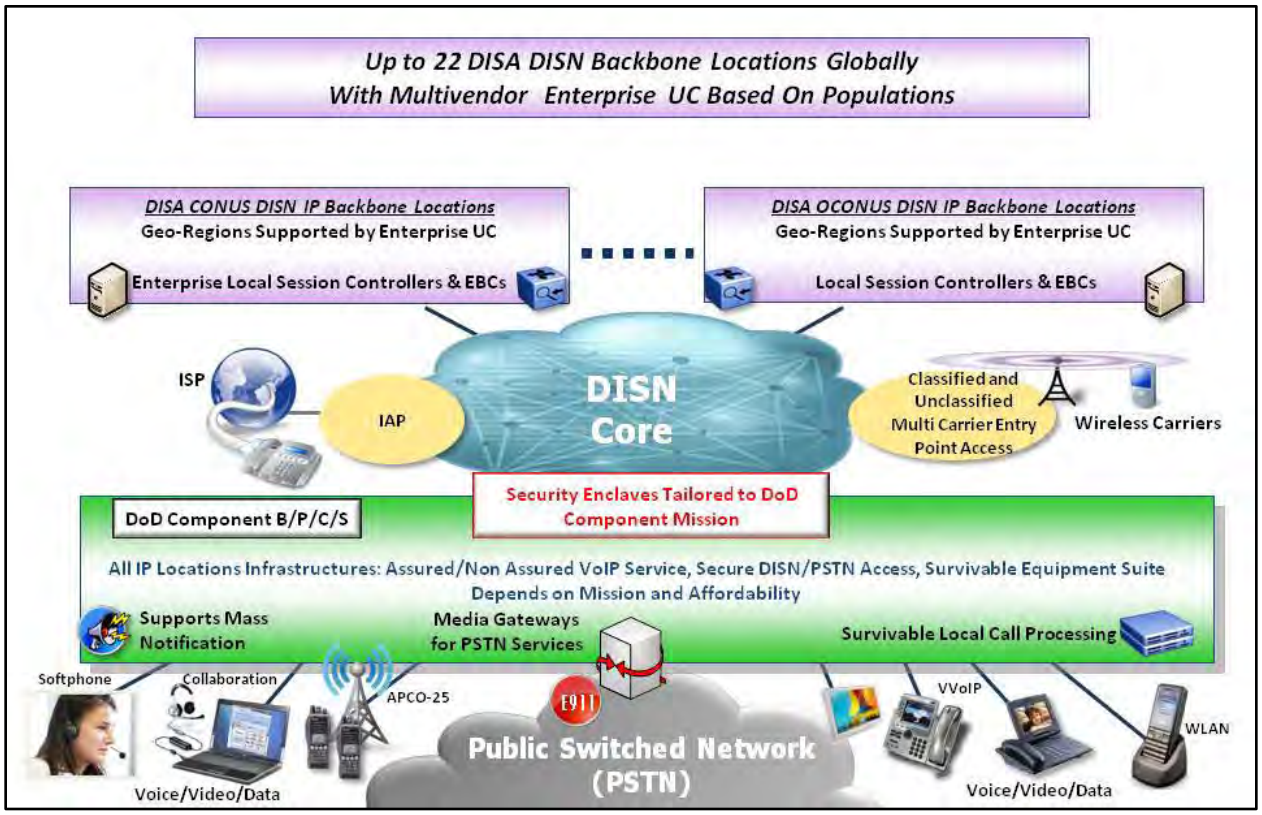


Figure 4.2.3. DISN Backbone Infrastructure

This operational concept has the potential to provide a single IP technology footprint, offer savings in operations and maintenance (O&M) and space requirements at the DoD Component level. At the enterprise level, this operational concept provides for integration of collaboration services, directory services, and conferencing capabilities as well as potentially enhancing NetOps situational awareness and improving end-to-end network performance.

4.2.4 Operational Construct for UC NetOps

Figure 4.2.4, Operational Construct for UC NetOps, defines the operational construct for UC NetOps based on the USCYBERCOM/USSTRATCOM approved DISN UC CONOPS.

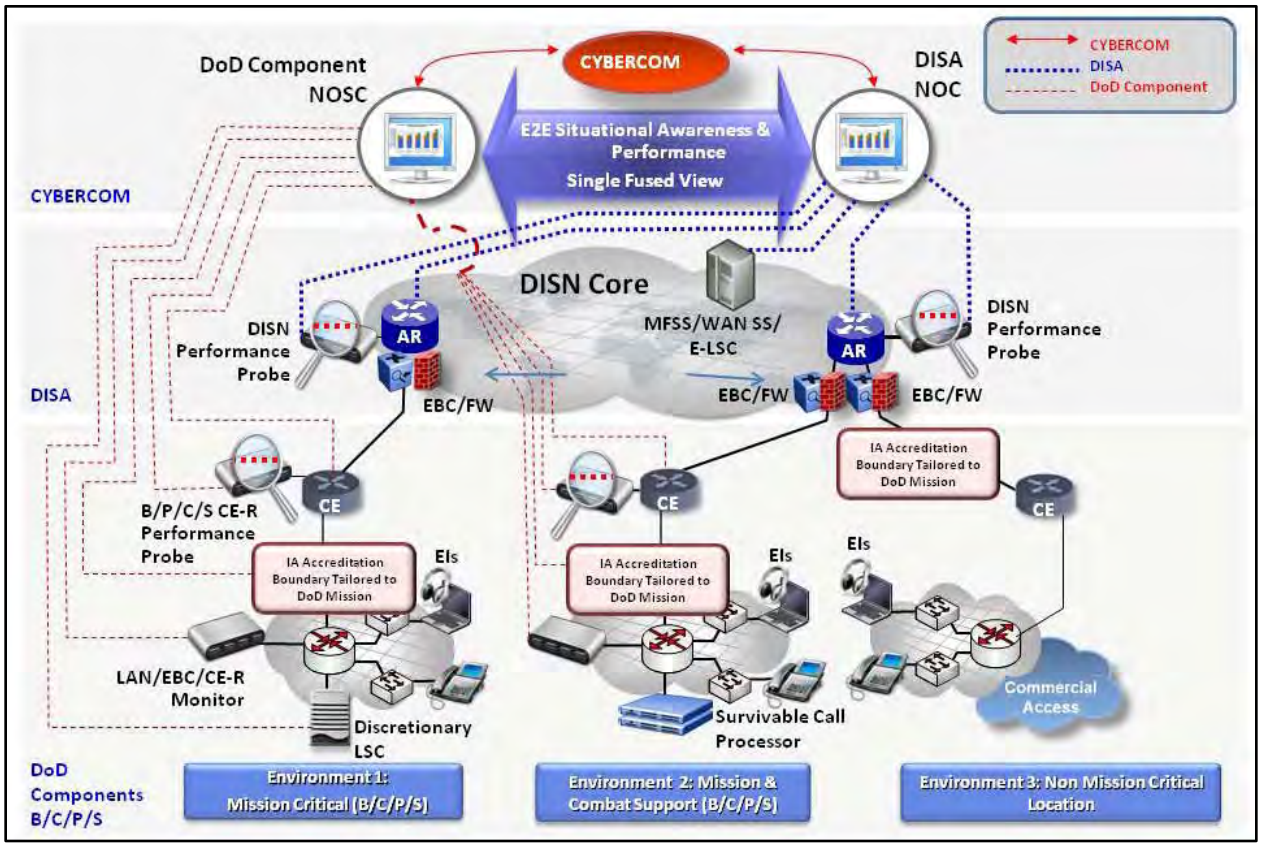


Figure 4.2.4. Operational Construct for UC NetOps

USCYBERCOM shall receive UC network situational awareness from DoD Component Network Operations and Security Centers (NOSCs) and the DISA Network Operation Center (NOC) infrastructure, and provide Operational Directive Messages to the DoD Components to meet mission needs. DISA and the other DoD Components shall be responsible for end-to-end UC network management, through the DISA NOC infrastructure and DoD Component NOSCs through exchange of information on end-to-end situational awareness and performance, to include quality of service, faults, configuration, administration, performance, and security.

The DISA NOC infrastructure shall oversee the DISN backbone infrastructure and DISA enterprise UC.

The DoD Component NOSCs (i.e., MILDEP and supported COCOM) shall oversee respective regional and B/P/C/S infrastructures supporting UC, delivered to the edge infrastructures and end devices. DoD Component B/P/C/S UC infrastructures may be tailored to meet respective mission needs for the three environments described in Section 4.2.6, System Interfaces.

4.2.5 Organizational Relationships/Responsibilities

Figure 4.2.5, Organizational Relationships, defines the organization relationships among the UC key stakeholders consisting of the DoD CIO, Joint Staff, DISA, and the other DoD Components over the life cycle of UC; from acquisition to operations; to sustainment until retirement. The DoD CIO is responsible for UC policy, requirements, and overarching planning documents. The notional governance structure for UC is established in DoDI 8100.04. Final governance structure for UC implementation shall be determined when Secretary of Defense reorganization efficiencies are complete. The Joint Staff is responsible for developing and issuing UC implementation instructions. DISA is responsible for UC enterprise funding, engineering, acquisitions, and operations associated with the DISN backbone and edge service provider (i.e., ELSC functionality for enterprise UC). Additionally, DISA shall provide a Blanket Purchase Agreement (BPA) for the DoD Components to use to acquire edge infrastructure UC APL products. The use of the DISA BPA is recommended for use by all DoD Components. DoD Components are responsible for edge infrastructure funding, engineering, acquisitions, and operations.

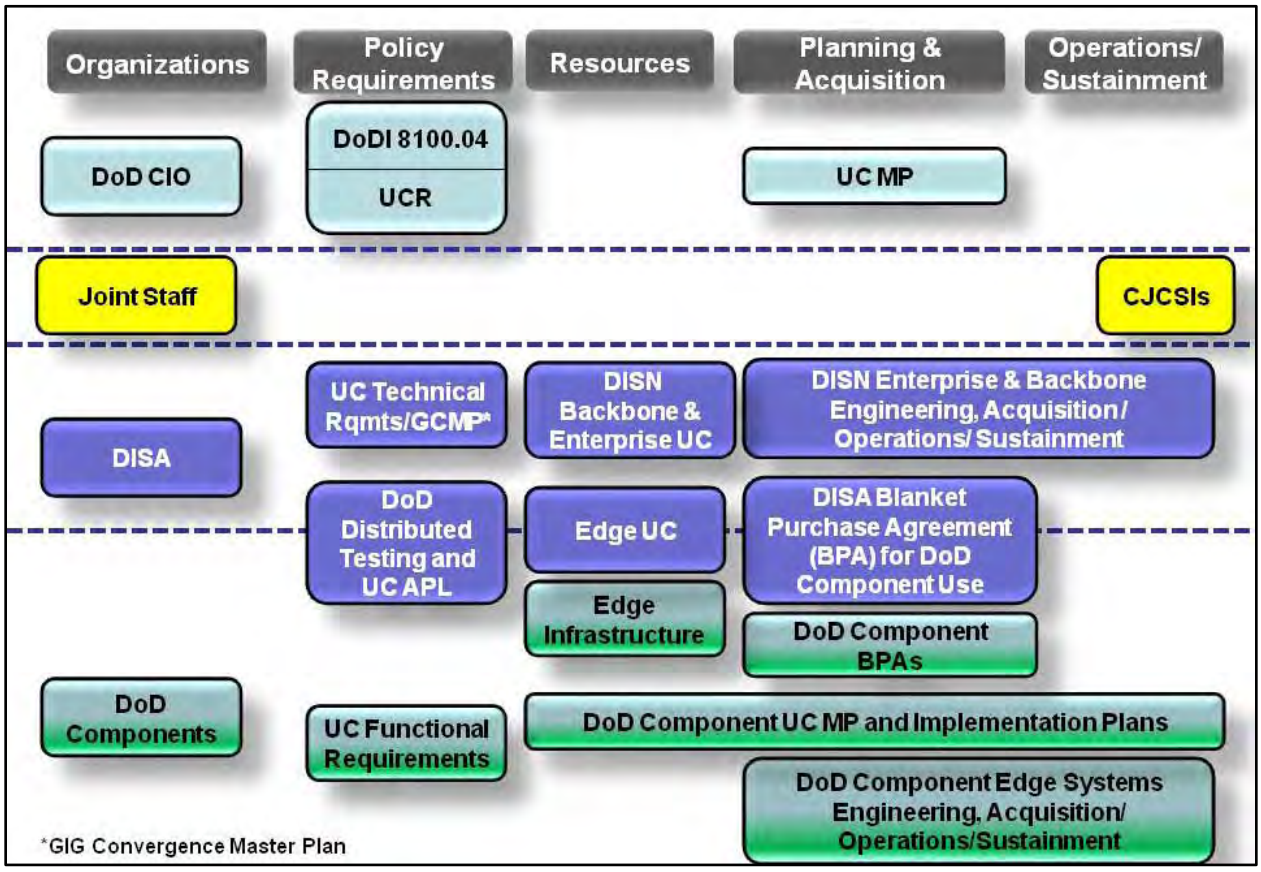


Figure 4.2.5. Organizational Relationships

4.2.6 System Interfaces

Figure 4.2.6, Systems Interfaces, depicts system interfaces between the DISN backbone and the DoD Components' edge infrastructures to deliver UC to end users. The functional requirements, performance objectives, and technical specifications needed for the initial deployment phase for assured, secure, and interoperable UC using multiple vendor products are contained in the DoD UCR. UC Transport will be primarily provided by the DISN Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) (for unclassified services) and by the DISN Secret Internet Protocol Router Network (SIPRNet) (for classified services). A key concept depicted in Figure 4.2.6 for tailoring UC implementations in DoD is based on three organizational mission environment types. A location's final recommended architecture will be based on the aggregate of tenant organizations' mission environments at a given location.
The three mission environments are:

- Environment 1: Mission Critical (B/P/C/S)

  (a) Organizations with mission sets that dictate, under normal conditions, access to all UC services, and, in the event the location is disconnected from the DISN, require all basic UC services, including intrabase precedence calling capability, external commercial services available to all users, and E911 service. Examples include a combat support unit or operational flying wing.

  (b) The same as Environment 1 (a), but in tactical deployed locations such as Afghanistan or Iraq with increased level of local management.

- Environment 2: Mission and Combat Support (B/P/C/S)

  Organizations with mission sets that dictate, under normal conditions, access to all UC services, and, in the event the location is disconnected from the DISN, require limited voice-only services, and limited external commercial services (E911 and external dial tone). Examples include a training unit, base airlift wing, logistic center, or an administrative center.

- Environment 3: Non Mission Critical Locations

  Organizations with mission sets that do not require significant voice services or external commercial services (E911, and external dial tone) in the event the location is disconnected from the DISN. An example would be a small administrative function (e.g., recruiting office). In this case, E911 and other services could be provided by other means (e.g., cellular, leased services).

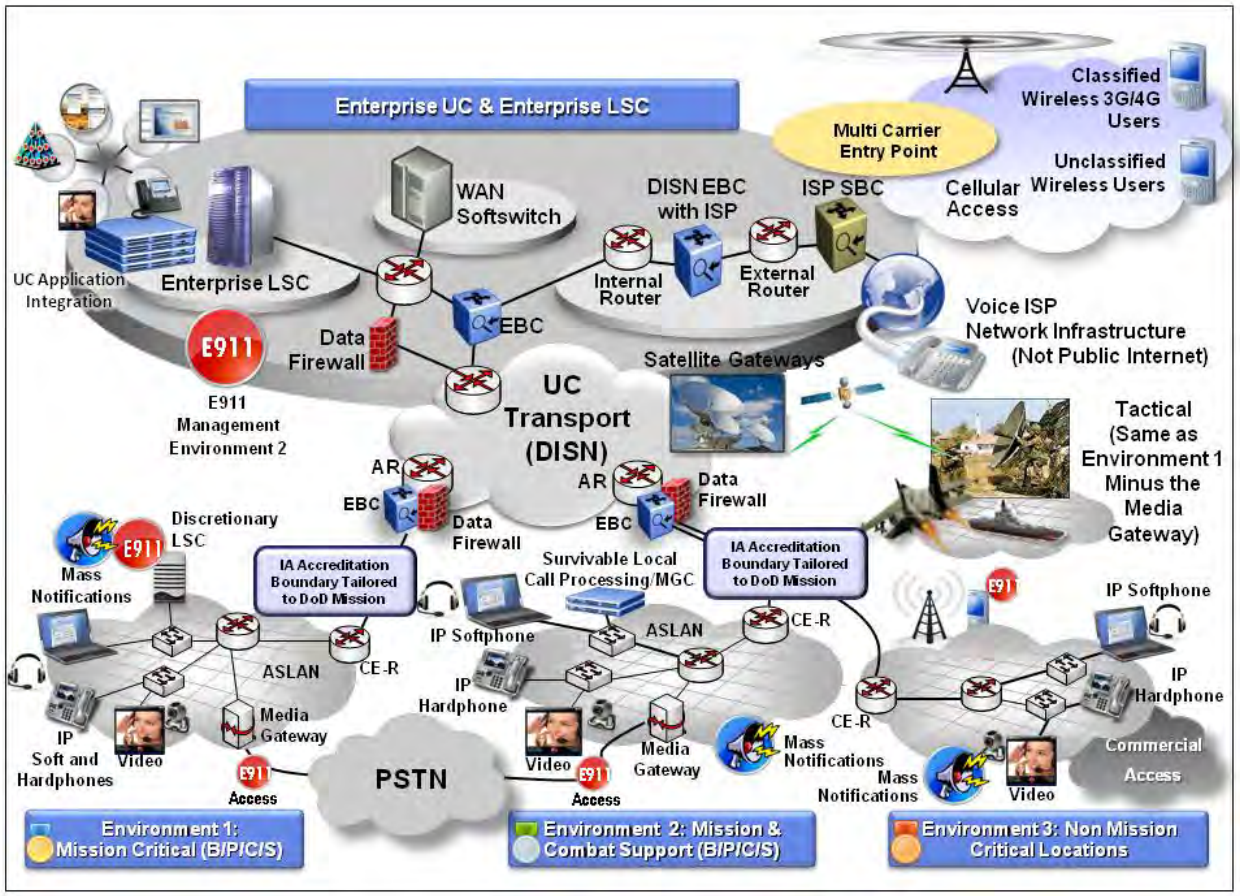


Figure 4.2.6. Systems Interfaces

4.2.7 Functional Requirements, Performance Objectives, Standards, and Technical Specifications

The standards for UC implementation are based on commercial standards mandated in the DoD IT Standards Registry (DISR) and the Data Services Environment, augmented as necessary, to meet DoD security requirements and to achieve multi-vendor interoperable solutions. Commercial standards will be employed for non-assured services, as appropriate. This UCR captures appropriate standards from the DISR and specifies the functional requirements, performance objectives, standards, and technical specifications for DoD networks that support UC.

The major drivers of mission needs for UC services are addressed in Section 3, Policy/ Requirements. UC services are driven by emerging IP and changing communications technologies, which recognize 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.

Voice, video, and data services that are addressed for integration in the UCR are as follows:

- Voice and Video Services Point-to-Point. Provides for two voice and/or video users to be connected EI-to-EI with services that can include capabilities such as voicemail, call forwarding, call transfer, call waiting, operator assistance, and local directory services

- Voice Conferencing. Provides for multiple voice users to conduct a collaboration session

- 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

- E-Mail/Calendaring. Provides for users to send messages to one or many recipients with features such as priority marking, reports on delivery status and delivery receipts, digital signatures, and encryption. Calendaring allows the scheduling of appointments with one or many desired attendees

- Unified Messaging. Provides access to voicemail via e-mail or access to e-mail via voicemail

- 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

- Unified Conferencing. Provides for multiple users to collaborate with voice, web, or videoconferencing integrated into a single, consolidated solution often as a collaboration application

- 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

  – 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

  – Chat provides the capability for two or more users operating on different computers to exchange text messages in real time. Chat is

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

– Presence/Awareness is a status indicator that conveys ability and willingness of a potential user to communicate

- 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

- 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 Smartphones. 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 needs to be provided by networks that meet end-to-end 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 NETWORK DESIGN FOR UNIFIED CAPABILITIES

This section provides a description of the end-to-end networks that use the UC products specified in Sections 5 and 6 that:

- Establish the requirements needed by industry to develop requirements-compliant UC solutions

- Provide the foundation for the development of UC Test Plans for interoperability and information assurance testing. These tests are used to make the certification decisions necessary to place products on the DoD UC APL

- Provide 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

- 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 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
- Video conferencing
- E-mail/calendaring
- Unified messaging
- Web conferencing and web collaboration
- Unified conferencing
- Instant messaging and chat
- Rich presence
- Mobility

This section provides a network-level overview of the end-to-end network designs and the products that provide UC services. The end-to-end IP network description is illustrated in Figure 4.3-1, End-to-End IP Network Description, which shows the major components of the design and the responsibilities. The edge is made up of the UC-approved products, which include telephones, video coders/decoders (codecs), Assured Services Local Area Network (ASLANs)/Non ASLANs, Local Session Controllers (LSCs), Enterprise LSCs, Edge Boundary Controllers (EBCs), and the Customer Edge (CE) Routers. The edge is connected to the DISN service delivery nodes (SDNs) and Transport via access circuits or via military department (MILDEP) Intranets.

Currently, the sensitive but unclassified (SBU) voice and integrated services digital network (ISDN) video services subset of UC are provided by the existing Time Division Multiplexing (TDM)-based Defense Switched Network (DSN) and its components with VoIP assured LAN services provided to the telephone on ASLANs. The TDM-based services on the network backbone will migrate over a long period to IP-based assured services systems end-to-end, over the MILDEP ASLANs, Intranets, and the DISN network infrastructure. During the migration timeframe, SBU UC will be provided by a hybrid arrangement of both TDM- and IP-based systems. The Defense Red Switch Network (DRSN) will remain based on circuit-switched technologies as the only technologies that can currently provide MLS. However, classified VVoIP will migrate from the current Voice over Secure Internet Protocol (VoSIP) using the same network design as the SBU VVoIP with a few feature differences. In addition, the current DISN Video Services (DVS) VTC services will be provided predominantly 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.

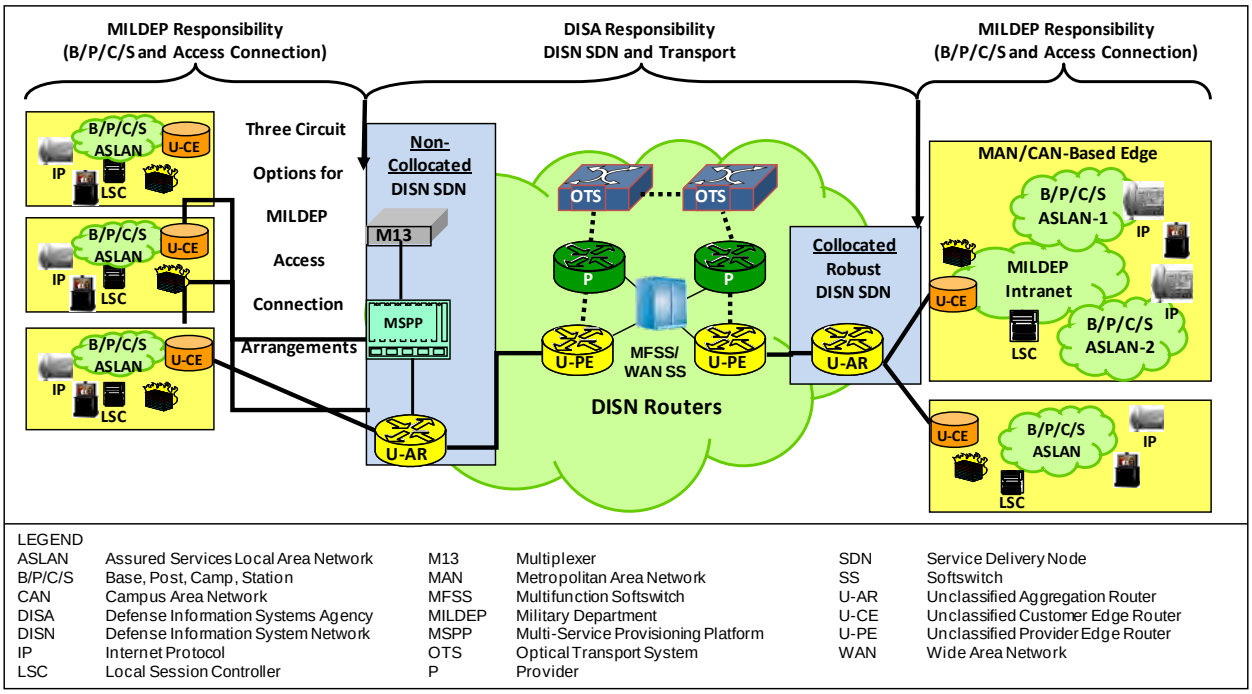


Figure 4.3-1. End-to-End IP Network Description

Figure 4.3-2, High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments, shows the three major end-to-end network segments: Customer Edge, Network Edge, and the Network Core (DISN SDNs and WAN Transport), which are all part of the UC end-to-end. 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.

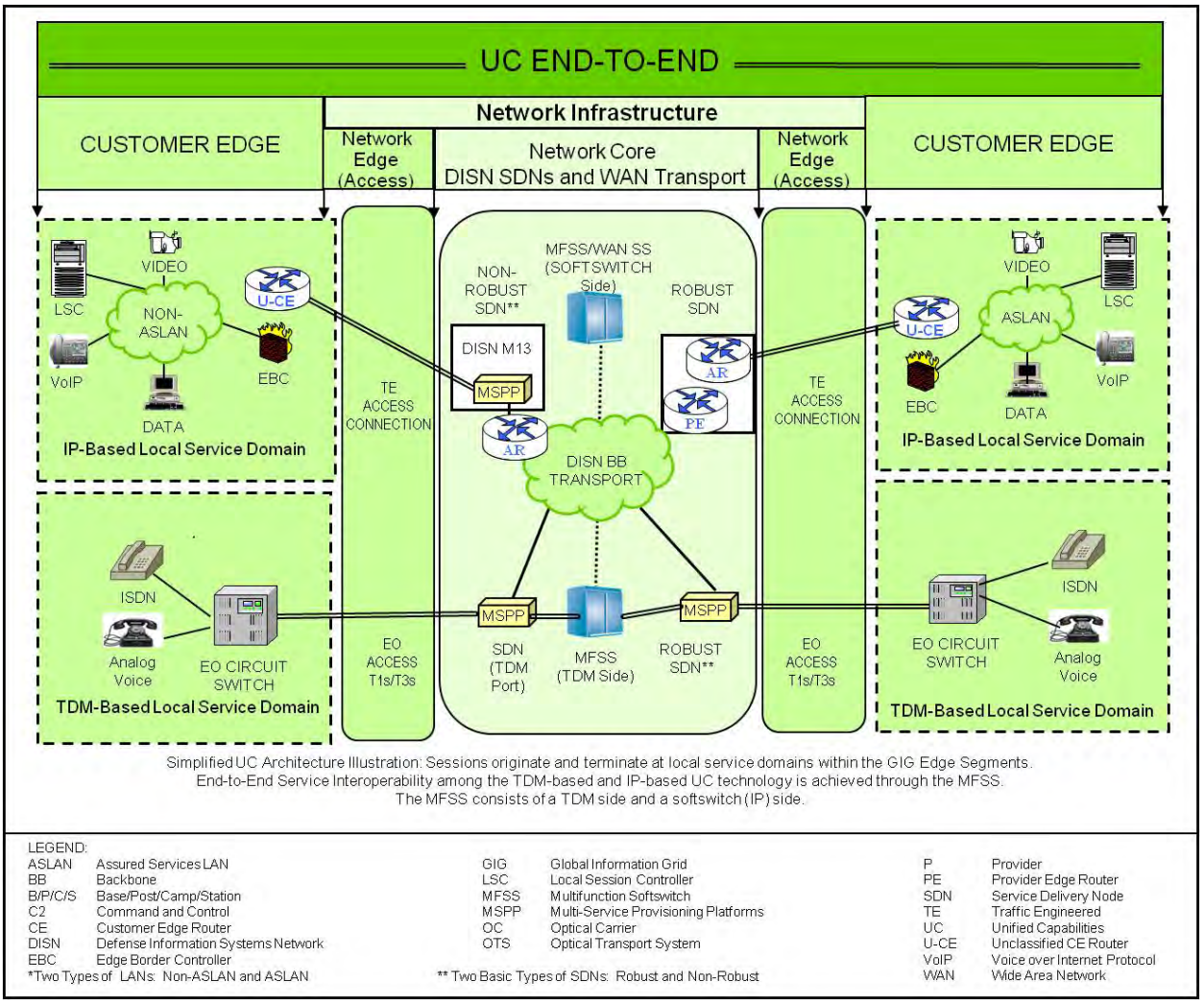


Figure 4.3-2. High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments

4.3.1 Overview of Network Design for UC

This section provides a high-level overview of the UC 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 4 traffic queues, plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, Network Management (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 4.3.1-1, Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site, 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.

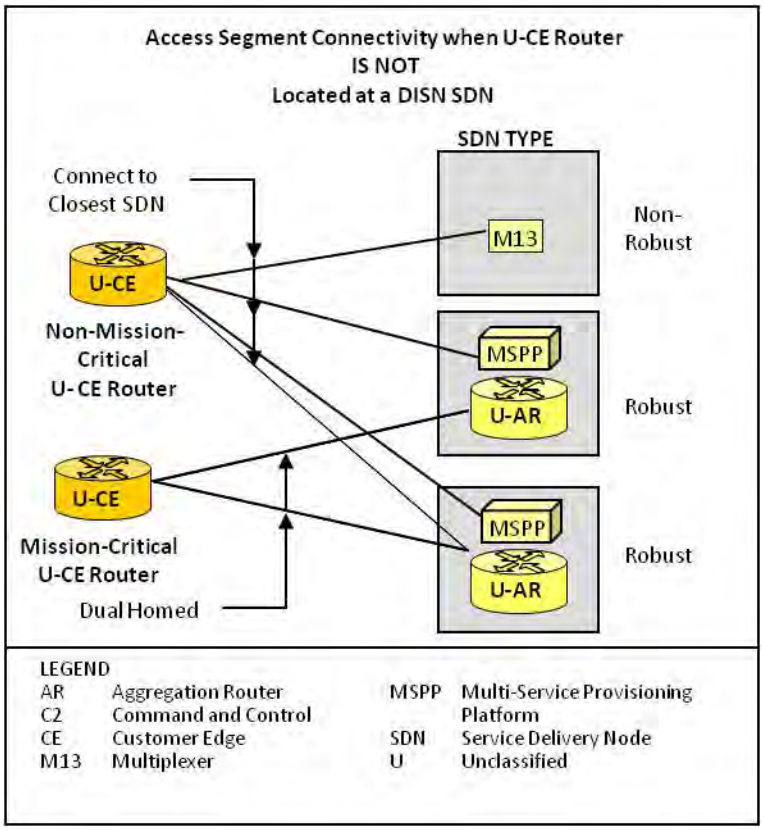


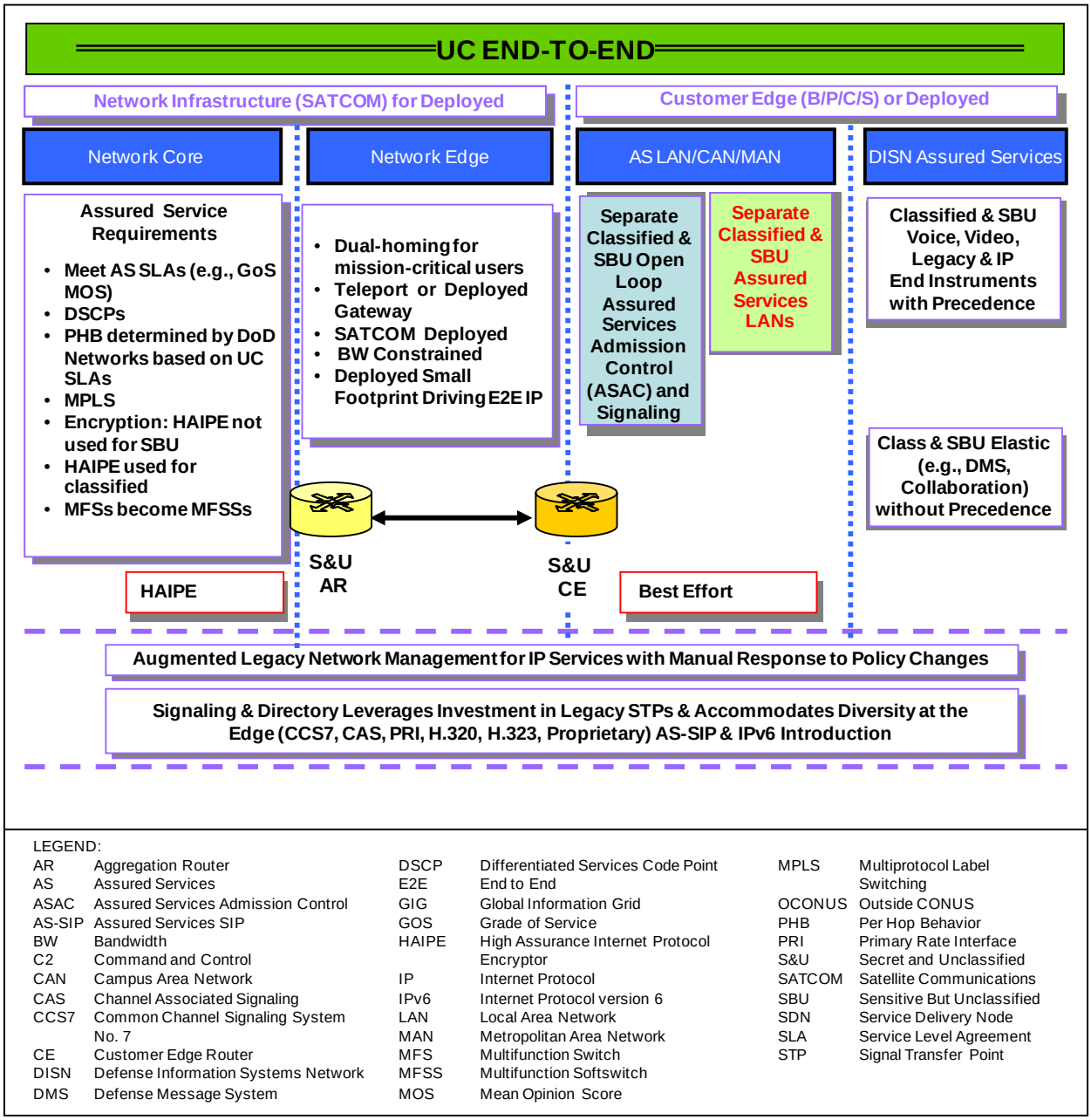
Figure 4.3.1-1. Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site

4.3.1.1 Overview of UC Network Design Attributes

The most important consideration for implementing the UC is not to degrade the capability to meet voice, video, and data services mission requirements. Preventing degradation begins with establishing a UC 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.

The logical location of the major UC network attributes within the UC E2E design is shown in Figure 4.3.1-2, Overview of UC 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. The functions contained in the boxes of Figure 4.3.1-2 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.



LEGEND:

AR	Aggregation Router	DSCP	Differentiated Services Code Point	MPLS	Multiprotocol Label Switching
AS	Assured Services	E2E	End to End		
ASAC	Assured Services Admission Control	GIG	Global Information Grid	OCONUS	Outside CONUS
AS-SIP	Assured Services SIP	GOS	Grade of Service	PHB	Per Hop Behavior
BW	Bandwidth	HAIPE	High Assurance Internet Protocol Encryptor	PRI	Primary Rate Interface
C2	Command and Control			S&U	Secret and Unclassified
CAN	Campus Area Network	IP	Internet Protocol	SATCOM	Satellite Communications
CAS	Channel Associated Signaling	IPv6	Internet Protocol version 6	SBU	Sensitive But Unclassified
CCS7	Common Channel Signaling System No. 7	LAN	Local Area Network	SDN	Service Delivery Node
		MAN	Metropolitan Area Network	SLA	Service Level Agreement
CE	Customer Edge Router	MFS	Multifunction Switch	STP	Signal Transfer Point
DISN	Defense Information Systems Network	MFSS	Multifunction Softswitch		
DMS	Defense Message System	MOS	Mean Opinion Score		

Figure 4.3.1-2. Overview of UC Network Attributes

4.3.1.1.1 Queuing Hierarchy for DISN IP Service Classes

Section 5.3.3, Network Infrastructure End-To-End 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 4.3.1-3 shows the queue structure, Differentiated Services Code Points (DSCPs), and associated rules for each granular service class.

Aggregate service class	Granular service class	Precedence	DSCP (Base 10)
Control	Network Control and Signaling	N/A	48
Inelastic/Real Time	User Signaling	N/A	40
	Short Message	FO	32
	Assured Voice	FO, F, I, P R	41, 43, 45, 47 49
	Assured Multimedia Conferencing	FO, F, I, P R	33, 35, 37, 39 51
	Broadcast Video	N/A	24
Preferred Elastic	Multimedia Streaming (Includes Non-Assured Video)	FO, F, I, P R	25, 27, 29, 31 26, 28, 30, 34, 36, 38
	Non-Assured Voice	N/A	46
	Low Latency Data: IM/Chat, Presence	FO, F, I, P R	17, 19, 21, 23 18, 20, 22
	High Throughput Data	FO, F, I, P R	9, 11, 13, 15 10, 12, 14
	OA&M	N/A	16
Elastic	Default (Best Effort)	N/A	0
	Low Priority Data	N/A	8

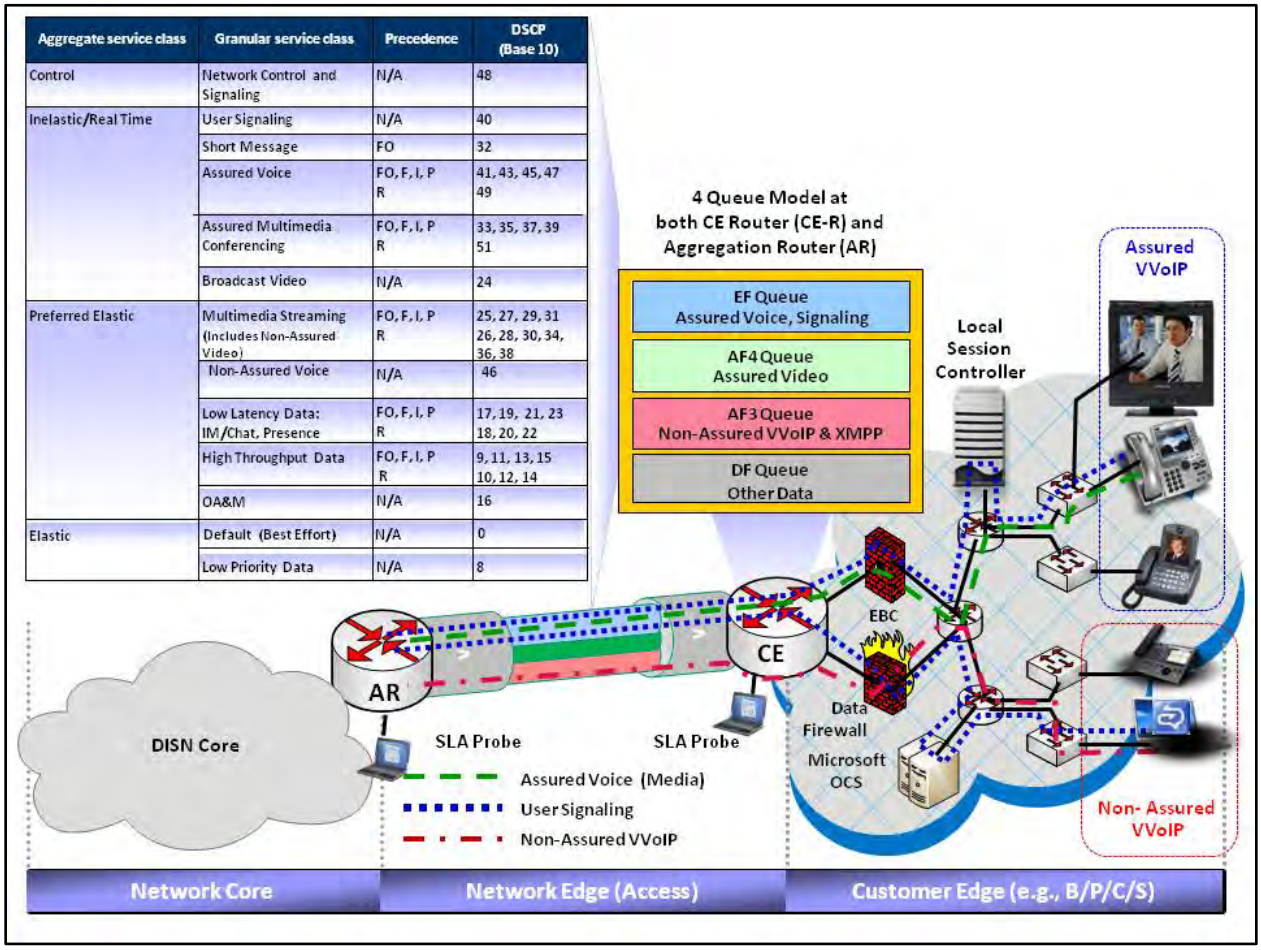


Figure 4.3.1-3. Queuing Design Overview

To ensure acceptable QoS in IP networks for assured VVoIP, it is necessary to assign the assured VVoIP traffic to different queues than non-assured VVoIP and data sessions on congested connections. Mixing assured VVoIP with non-assured VVoIP in the same aggregate service

class (and queue) will result in the uncontrolled non-assured VVoIP degrading the assured VVoIP sessions on congested networks. To delineate the assured VVoIP from the non-assured VVoIP (and other types of packets), IP packets are marked with unique DSCPs.

The following discussion explains the differences between assured and non-assured VVoIP, and why they are assigned to two different queues:

1. Assured VVoIP traffic is subject to Session Admission Control (SAC). SAC policies control the number of sessions that are offered to the network. Session admission control can be provided by LSCs or Gatekeepers (i.e., H.323 Gatekeepers) and is associated with establishing a budget for the number of simultaneous sessions and with ensuring that the number of active sessions is within that budget. Assured Services Admission Control (ASAC) extends SAC to allow sessions to be preempted when the SAC budget is at capacity and additional higher precedence sessions are offered. The ability to apply SAC to assured VVoIP ensures that assured VVoIP traffic is deterministic or predictable in nature. Since the offered load is predictable, it can be traffic-engineered, and the network (queue size) can be designed for the traffic-engineered load.

2. Non-assured VVoIP has many of the same characteristics as assured VVoIP with two critical differences. The first difference is that SAC is not applied to non-assured VVoIP. This is so because non-assured VVoIP typically is composed of peer-to-peer sessions that do not transit a centralized SAC appliance, (e.g., LSC); therefore, SAC cannot be applied. The second difference is that non-assured VVoIP sessions cannot be traffic-engineered to ensure QoS. This is so because, without SAC, the offered load is not predictable.

In addition to queuing, it is essential to apply traffic conditioning to the non-assured VVoIP packets since the packets are sent using the User Datagram Protocol (UDP) and are connectionless, meaning that the host will continue transmitting at the same rate independent of the network's ability to support that rate. Also, the UDP packets can quickly cause the preferred data sessions that are queued (in four-queue model) to terminate because of their use of Transmission Control Protocol (TCP), which responds to congestion by decreasing packet transmission rate. Enabling traffic conditioning on non-assured VVoIP packets will still cause unacceptable degradation on non-assured VVoIP sessions during periods of high usage, but will ensure that preferred data sessions continue to receive better than best effort performance IAW the UCR performance objectives.

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.

Non-assured VVoIP users can only interoperate with an assured services VVoIP user via an Assured Services Session Initiation Protocol (AS-SIP) gateway. All non-assured VVoIP users must be traffic engineered and controlled, and must meet information assurance requirements.

4.3.1.1.2 Customer Edge Segment Design

The Customer Edge Segment has the following attributes:

- LANs Configured to Meet Mission, Performance, and Affordability. At the Customer Edge, the design has an LAN that is designed with a mix of Assured Service and non-Assured Service LANs (ASLAN) based on availability, redundancy, and backup power tailored for organization's missions and affordability. Performance requirements with respect to QoS, security and network management are the same for ASLANs and Non ASLANs as described in Section 5.3.1, ASLAN Infrastructure.

- Session Admission Control. The LSCs use an 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.

- Session 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.

- 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.

- Multiprotocol Label Switching (MPLS) and MPLS Virtual Private Networks (VPNs). Can be implemented in the ASLAN but cannot be extended to the DISN.

4.3.1.1.2.1 B/P/C/S UC Design

The military B/P/C/S-level design is flexible, depending on whether or not the location uses Enterprise services. The design may consist 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 user and building mission requirements. Off-base connectivity to the long-haul DISN network infrastructure is provided through the edge boundary controller 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 to meet their organizational mission, performance and affordability requirements.

4.3.1.1.2.2 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 also found in the MFSS. 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 PSTN or to legacy B/P/C/S TDM systems, it must also support Primary Rate Interface (PRI), using its MG and Media Gateway Controller (MGC). All LSCs provide PBAS via AS-SIP/ASAC for IP and for TDM trunks (where equipped) via its Media Gateway using the T1.619a protocol.

Figure 4.3.1-4, 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. A single LSC per B/P/C/S or participation with a regional Enterprise LSC is the preferred affordable solution for fixed locations. Tactical deployments may be best served by treating the Tactical Theater as a region with multiple LSCs as shown in Case 3. 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 the other LSC. Should base connection to the DISN WAN or the MFSS be lost, then sessions from one base LSC to the other 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.

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

1. End instruments served by an MLSC are treated like EIs served by SLSCs.

2. The MLSC adjudicates the enclave budget between the SLSCs.

3. Either of the following two methods is acceptable:

    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 SLSC, for example:

        (1) If the ASAC budget is 30.

        (2) Each SLSC (3, total) allowed 10 voice sessions (3 budgets).

        (3) The Master LSC performs preemptions to ensure higher precedence sessions succeed.

        (4) The 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 SLSCs, for example:

        (1) If the ASAC budget is 30.

        (2) Each SLSC (3, total) with each allowed 10 sessions.

        (3) Does not use unfilled LSC budget to service above ROUTINE precedence sessions from another SLSC.

c. All LSCs directly connect to an element management system (EMS) to permit MILDEP support of the USCYBERCOM.

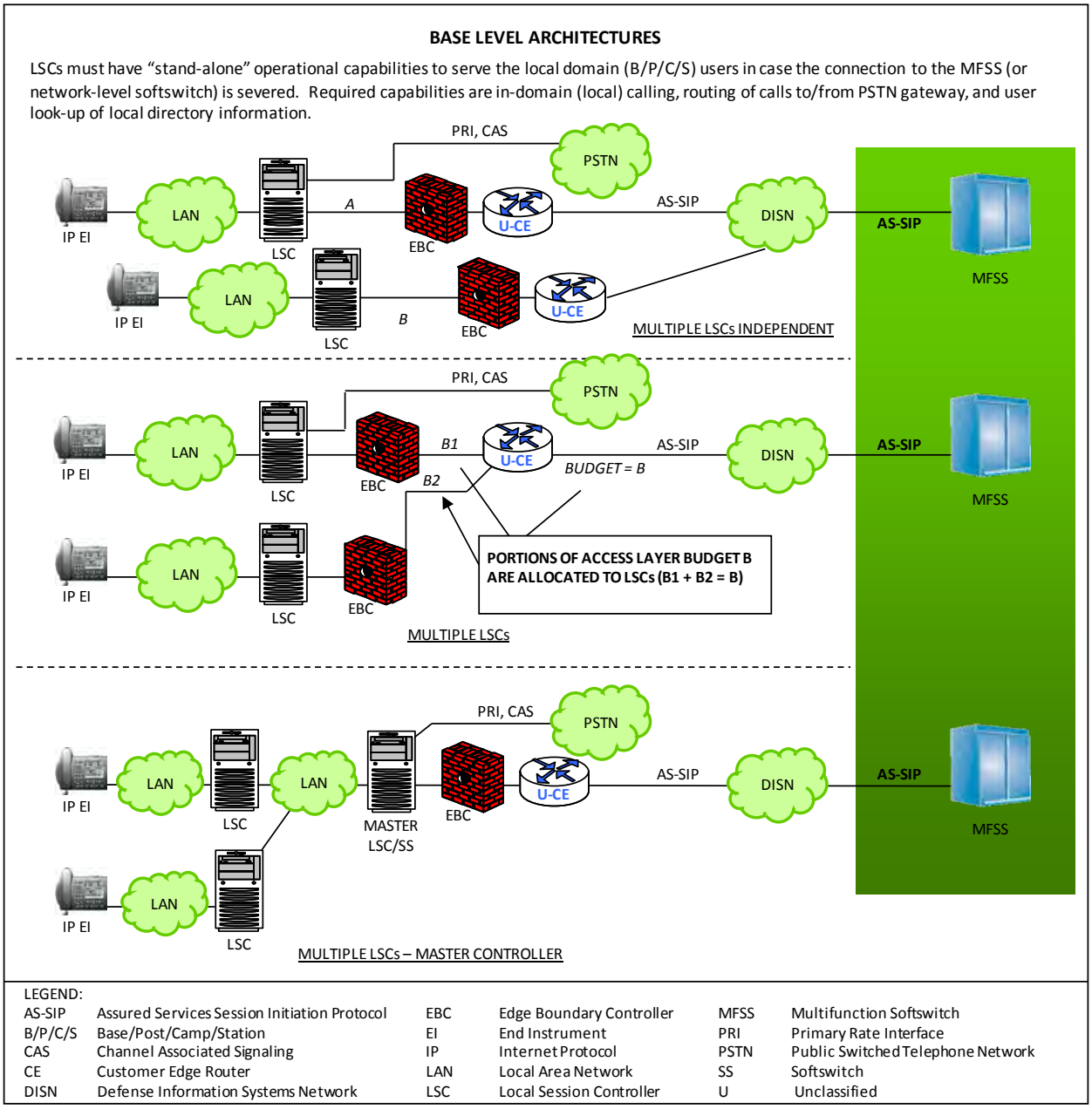


Figure 4.3.1-4. B/P/C/S-Level Voice over IP LSC Designs

d. The MLSC is not required to provide an aggregated NM view of the SLSCs.

e. Master LSCs and SLSCs communicate using AS-SIP and/or proprietary signaling protocols if LSCs are from the same vendor.

(1) All signaling destined external to the enclave passes through the MLSC.

(2) Allows multiple vendors within the enclave or a single vendor integrated solution.

f. Each LSC maintains two budget counts as follows:

(1) Intraenclave (based on local traffic engineering and not associated with the access link budget).

(2) Interenclave (ASAC controlled by each LSC).

g. It is desired that connections to the PSTN only be through the MLSC (simplifies location services).

h. When an SLSC directly connects to the PSTN (exception situation, not desired), then only EIs of the SLSC can originate and receive calls from that PSTN PRI/channel-associated signaling (CAS) trunk.

i. The MLSC 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.

4.3.1.1.2.3 LSC Designs – Video

Figure 4.3.1-5, 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 design 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 CAS using its MG and MGC. All LSCs provide PBAS via AS-SIP/ASAC for IP and for TDM trunks (where equipped).via its Media Gateway using the T1.619a protocol.

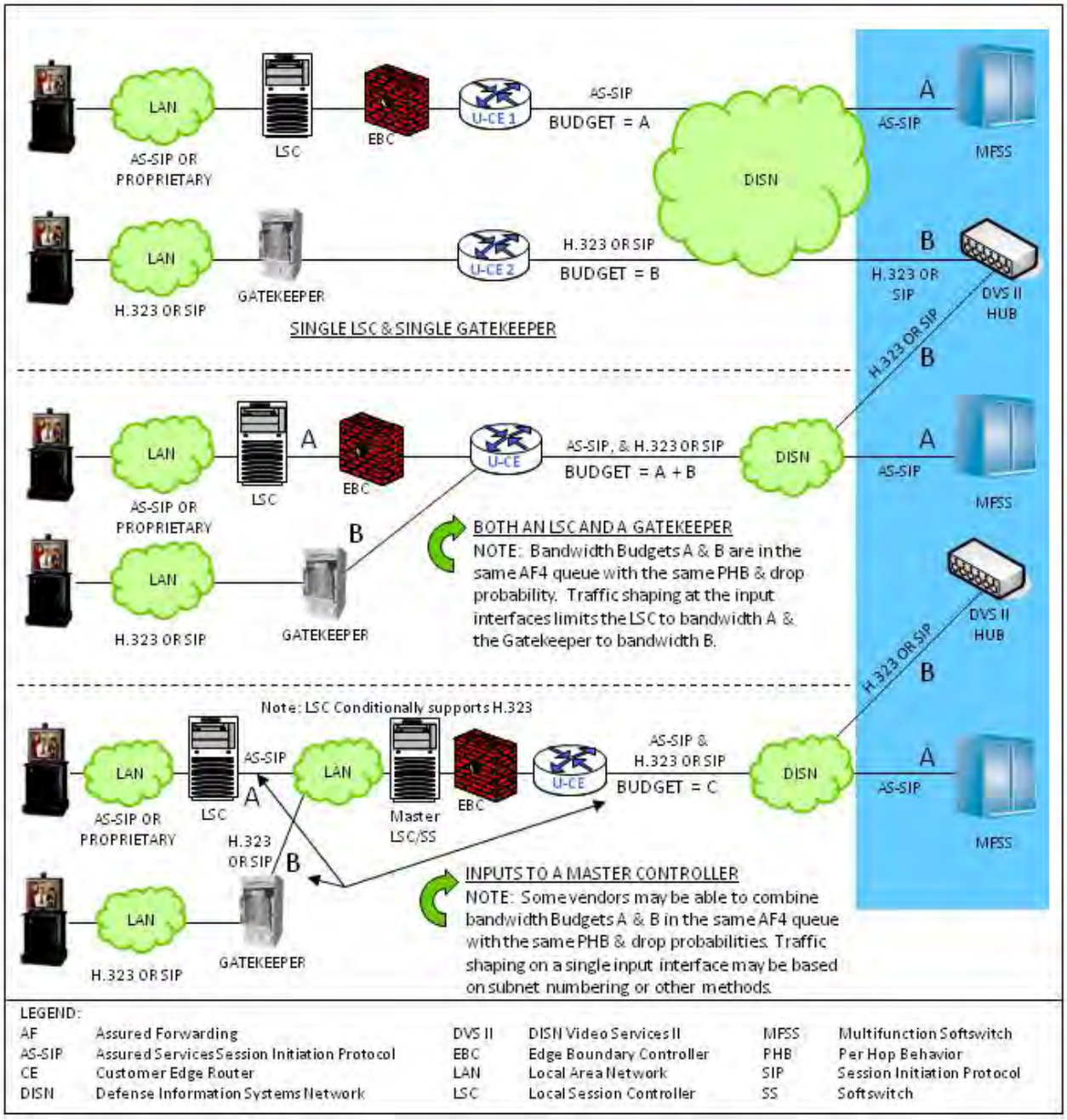


Figure 4.3.1-5. B/P/C/S Video over IP LSC Designs

Figure 4.3.1-5 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 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 the LSC and Gatekeeper (i.e., A+B). Although each router port processing video calls acts independently in the AF4 queue, both customer calls must be treated equally if and only if the H.323 traffic is traffic engineered and controlled. This assumes that the AF4 queue is sized to meet the aggregate demand of the AS-SIP VTC traffic and the H.323 Gateway-controlled traffic. If the H.323 traffic is not traffic engineered *and* controlled, then it goes into a different queue (i.e., the preferred data queue).

The third case requires the designation and implementation of an LSC cluster concept as described for the voice design in Section 4.3.1.1.2.2, LSC Designs–Voice.

With regard to the Gatekeeper interworking with the MLSC 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 MLSC 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 (unless a H.323/AS-SIP Gateway is used) because of different protocols used, the MLSC or SS will be able to process the calls into Budget C efficiently in the AF4 queue. All video calls leaving the MLSC or SS must be treated equally only if the H.323 traffic is traffic engineered and controlled. This assumes that the AF4 queue is sized to meet the aggregate demand of the AS-SIP VTC traffic and the H.323 Gateway-controlled traffic. If the H.323 traffic is not traffic engineered *and* controlled, then it goes into a different queue (i.e., the preferred data queue).

4.3.1.1.2.4 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 4.3.1-6.

Two types of LANs are ASLAN and non-ASLAN, depending on the type of missions and users served by a LAN. ASLANs provide enhanced availability and backup power as compared to Non-ASLANs. As a result, they are more robust and more costly. The two LAN types and three categories along with user classes are illustrated in Figure 4.3.1-7, Three Categories of LANs.

LAN
UCR/UCTP

REQUIREMENTS

- QOS
  - MEET VOICE, VIDEO & DATA PERFORMANCE
  - PACKET LOSS, JITTER, LATENCY MEASURED
- SUPPORT SERVICE CLASSES & PRECEDENCE MAPPED INTO DSCPs
- COMMERCIAL, MEDIUM, AND HIGH AVAILABILITY/ BACK UP POWER TAILORED TO USER MISSION
- VLAN FOR VOICE, VIDEO, DATA PERIPHERALS
- NETWORK MANAGEMENT OF LAN

LEGEND

DSCP	Differentiated Services Code Point
LAN	Local Area Network
QoS	Quality of Service
UCTP	Unified Capability Test Plan
VLAN	Virtual Local Area Network

Figure 4.3.1-6. LAN Requirements Summary

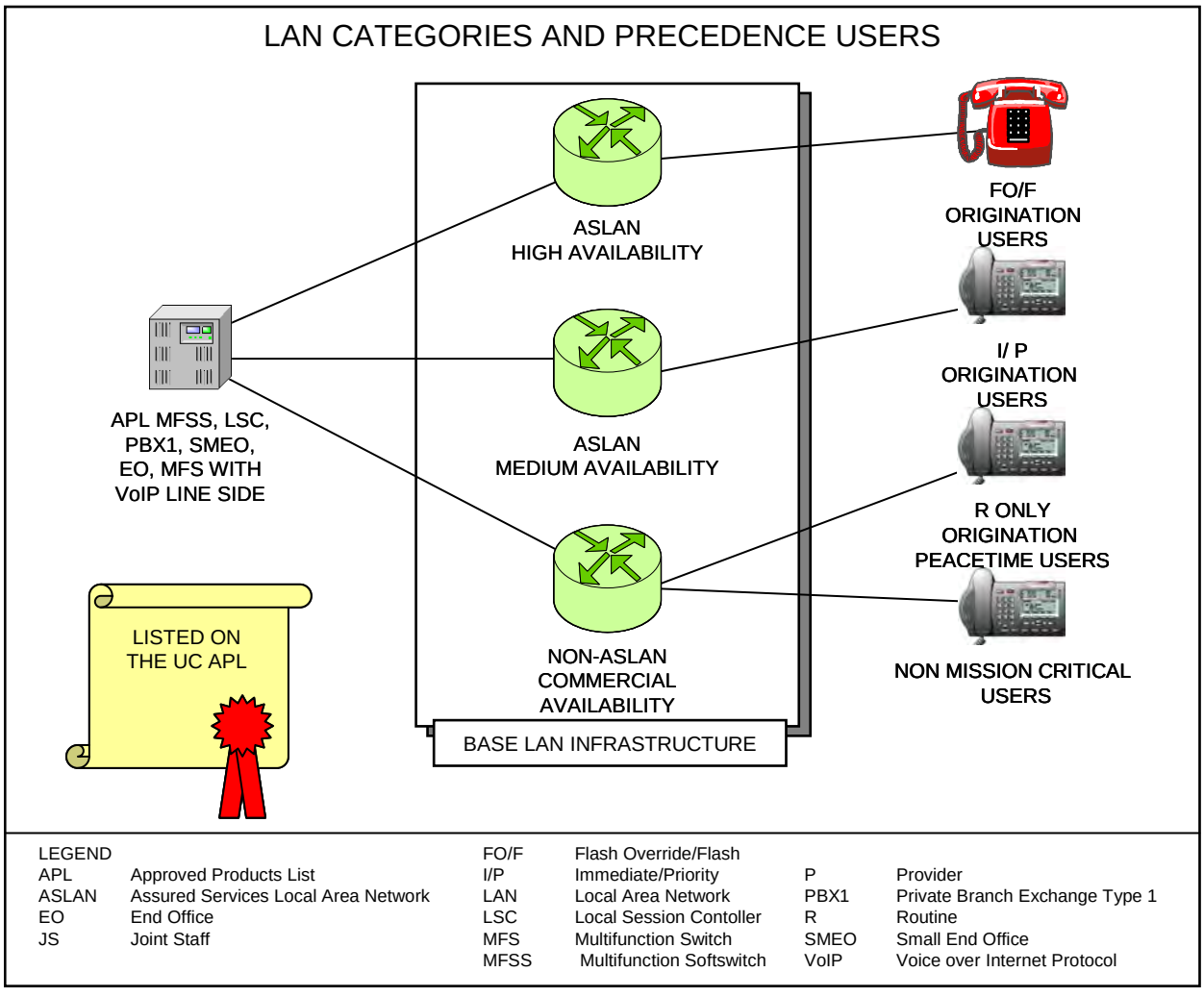


Figure 4.3.1-7. Three Categories of LANs Tailored to Mission Needs

Table 4.3.1-1, LAN Requirements Summary, shows the requirements needed based on subscriber mission category. Note that in addition to subscriber requirements, mission critical functions that do not originate or receive precedence traffic must also be supported since these functions must continue in time of crisis. *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).

Table 4.3.1-1. LAN Requirements Summary

LAN REQUIREMENT ITEM	USER PRECEDENCE ORIGINATION 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	NR
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

NOTE 1 GOS is discretionary and shall be determined by DoD Components.

LEGEND

ASF	Assured Services Features	I/P	IMMEDIATE/PRIORITY	P	Permitted
ASLAN	Assured Services LAN	LAN	Local Area Network	R	Required
FO/F	FLASH OVERRIDE/FLASH	NP	Not Permitted	R	ROUTINE
GOS	Grade of Service	NR	Not Required		

An ASLAN that supports users authorized IMMEDIATE/PRIORITY (I/P) is classified as a Medium Availability ASLAN. An ASLAN that supports users authorized FLASH OVERRIDE/FLASH (FO/F) is classified as a High Availability ASLAN.

Installing ASLAN in all buildings may result in a fiscally untenable cost. Therefore, 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 within the various buildings on the base.

ASLAN requirements for a Military installation can be determined by performing a site survey to identify the specific locations (buildings) that require a High, Medium, or non- ASLAN capabilities. Examples of buildings with mission critical functions include but are not limited to: Buildings with LAN core nodes, reachable nodes that extend services into, e.g., Theater, network operations and security centers, network control centers , command posts, battle staff, Core nodes including connectivity between the core nodes (i.e., the LAN backbone) must be high availability. If the backbone is not a high availability ASLAN, nothing else can be high availability.

Figure 4.3.1-8, An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users, is an example of a LAN with a mix of organizations with different Mission and Non-Mission-Critical Users that combines the LAN capabilities illustrated in Figure 4.3.1-7, Three Categories of LANs Tailored to Mission Needs. It shows a LAN at a location involving multiple buildings and types of mission users and how connectivity redundancy and the backup power time requirement of eight, two, or zero hours are met in a cost-effective manner.

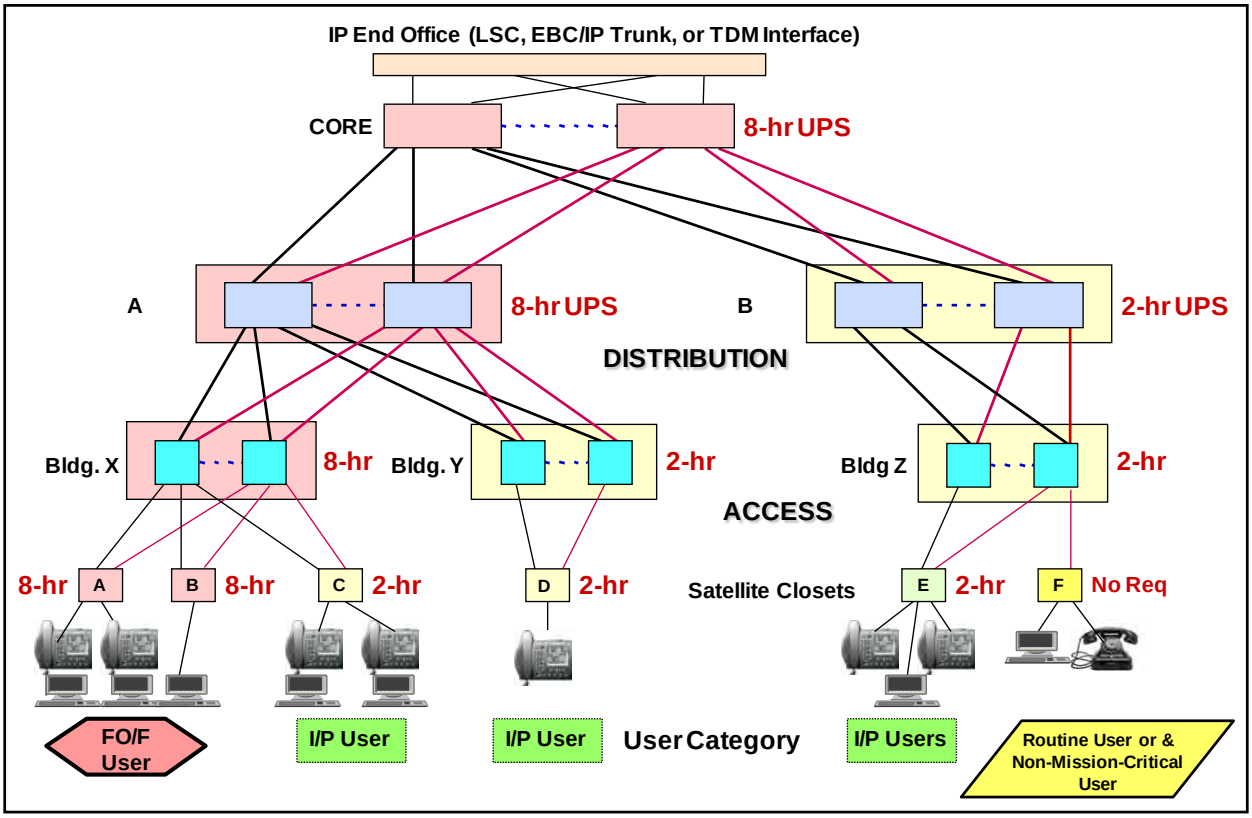


Figure 4.3.1-8. An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users

4.3.1.1.2.5 Regional ASLAN

Regional ASLAN designs are used where a local service enclave covers a large geographical area. Regional ASLANs typically consist of a single security enclave. Regional ASLANs use a centralized ELSC with redundancy and automatic failover of an EI to a "backup" LSC, high-speed links with MPLS at the LAN core layer, and remote MGs.

4.3.1.1.2.6 Required Ancillary Equipment

Operation of UC products requires support from server functions that normally are not part of an LSC or EBC product. These functions/severs are referred to as Required Ancillary Equipment (RAE) and must be made available at the site to support the LSC and EBC. The RAE support includes Authentication, Authorization, and Accounting (AAA) servers, access to a Domain Name System (DNS) server, SYSLOG server, Network Time Protocol (NTP) server, Dynamic Host Configuration Protocol (DHCP) server, and for PKI certificate verification, access to an Online Certificate Status Protocol (OCSP) responder.

4.3.1.1.3 Network Infrastructure End-To-End Performance (DoD Intranets and DISN SDNs)

Figure 4.3.1-9, Measurement Points for Network Segments, illustrates the components of the end-to-end network where measurements will be made to ascertain compliance with the service level agreements (SLAs).

To ensure end-to-end voice and video services' performance, an allocation of performance metrics 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 end-to-end network, that is not meeting the allocation have been developed. The specific end-to-end network performance requirements are described in Section 5.3.3, Network Infrastructure End-To-End Performance Requirements.

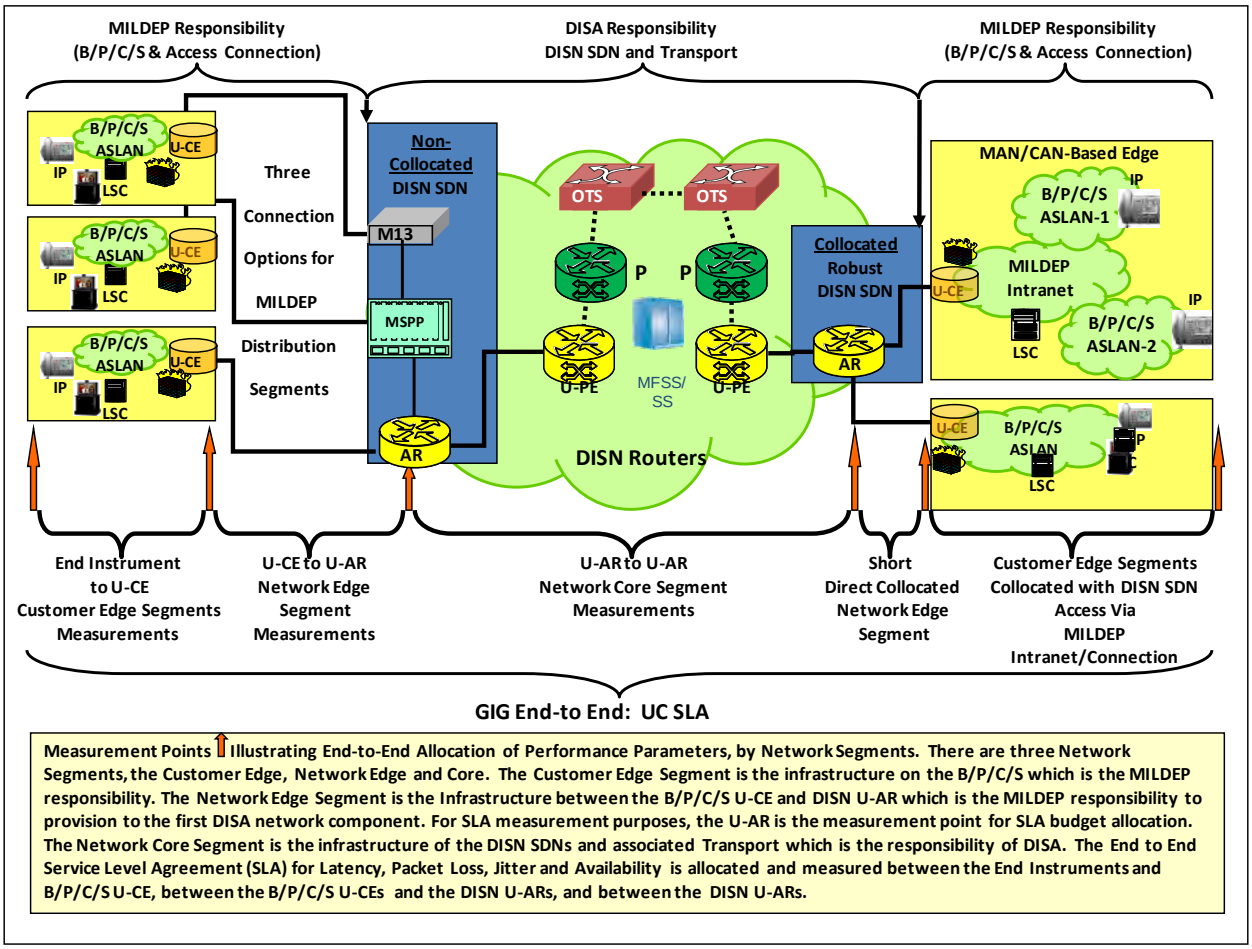


Figure 4.3.1-9. Measurement Points for Network Segments

The Services' Intranets, Intranets supporting COCOMs and the DISN SDNs serving SBU VVoIP traffic currently do not use HAIPEs. The DISN SDNs are assumed bandwidth rich and robust. Since the ASLAN is required to be implemented as nonblocking for voice and video traffic, it has no bandwidth limit either. The access circuit, which can include a SATCOM link from the Edge to the DISN Core SDN, is the only potential bandwidth-limited resource due to funding, crisis traffic surges, or damage. Therefore, the 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 MPLS Fast Failure Recovery (FFR) in the Core.

4.3.1.1.4 End-to-End Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions and protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes. The signaling plane is associated with the signaling and control protocols, such as AS-SIP and H.323.

Figure 4.3.1-10, Attributes of AS-SIP, illustrates the basic attributes of AS-SIP, which are critical to assured services, multivendor interoperability, and security.

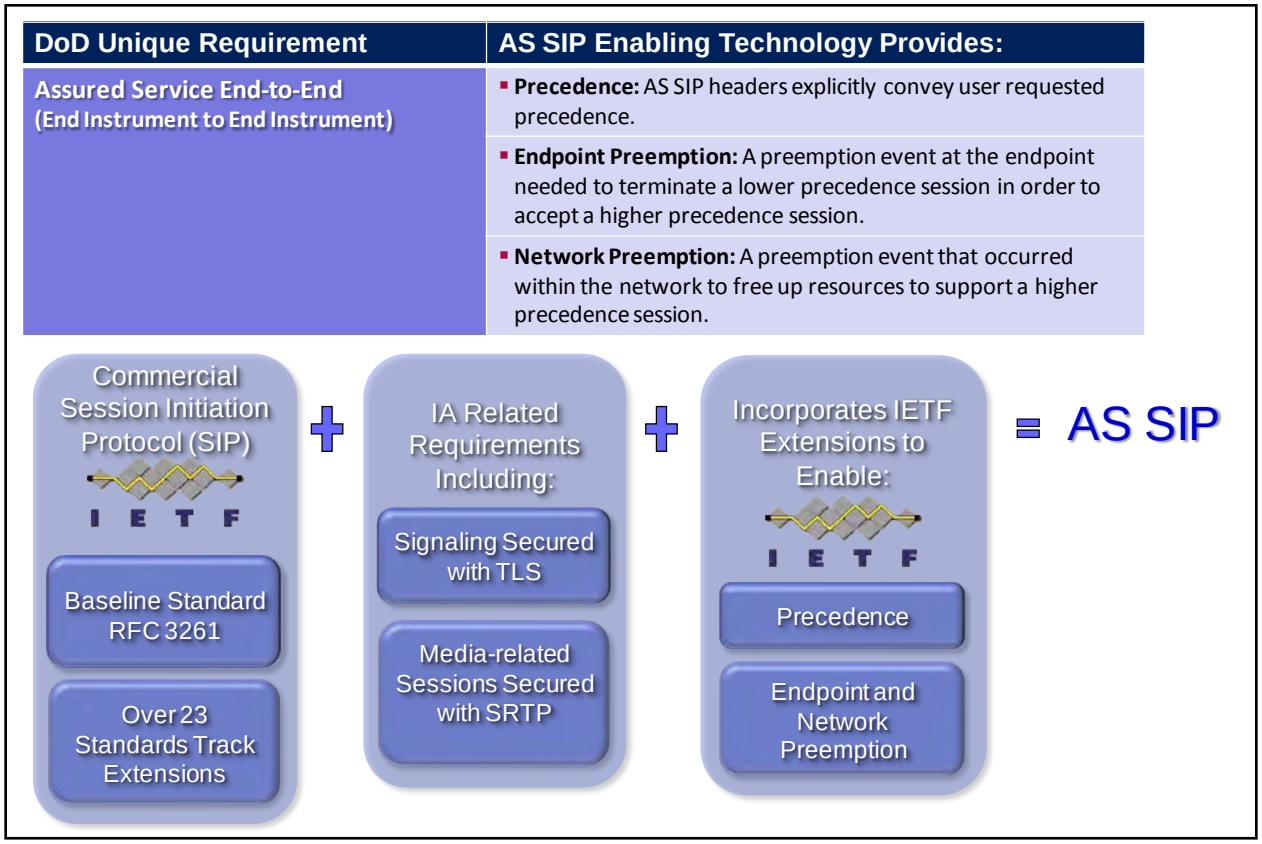


Figure 4.3.1-10. Attributes of AS-SIP

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).

4.3.1.1.5 ASAC Component

The ASAC technique is the key design component ensuring that end-to-end SLAs (grade of service (GOS), voice/video quality, assured service delivery, and session preemption to the EI) are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements (NEs) end-to-end as illustrated in Figure 4.3.1-11, Assured Services Functions. The ASAC functions identified for the LSC are also employed in the Enterprise LSC. Deployable VoIP products may connect via compressed

satellite circuits to the DISN backbone and operate in a similar manner to Fixed products on the LAN. 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.

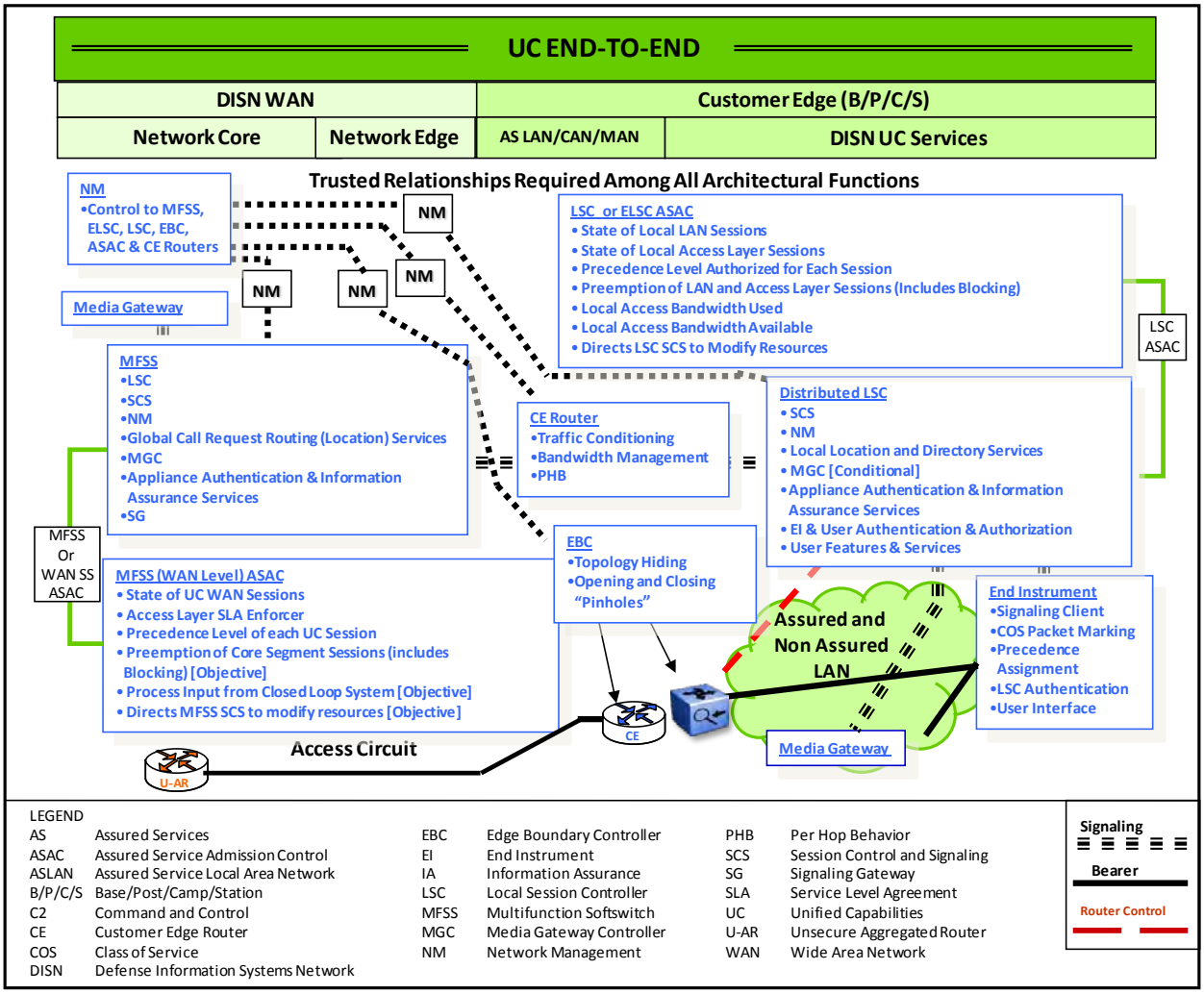


Figure 4.3.1-11. Assured Services Functions

In the access circuit and the ASLAN, AS-SIP signaling (see Section 5.3.4, AS-SIP Requirements) 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 Quality of Service/Differentiated Services Code Point (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/DSCP, traffic engineering, and MPLS. Traffic with no marking will be treated as Best Effort.

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 users will come under ASAC. Some H.323 video users on a base may choose to use a separate H.323 Gatekeeper and not come under ASAC. 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. Section 4.3.1.1.1 addressed the Queuing Hierarchy for DISN IP Service Classes.

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 Circuit Switched T1.619a/AS-SIP signaling conversion)), the MG (for EI IP signaling to Commercial PRI signaling), and as part of the AS-SIP signaling appliance part of the LSC and MFSS/WAN SS 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/WAN SS.

4.3.1.1.6 Voice and Video Signaling Design

The voice and video signaling design for SBU voice and video is shown in Figure 4.3.1-12, 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.

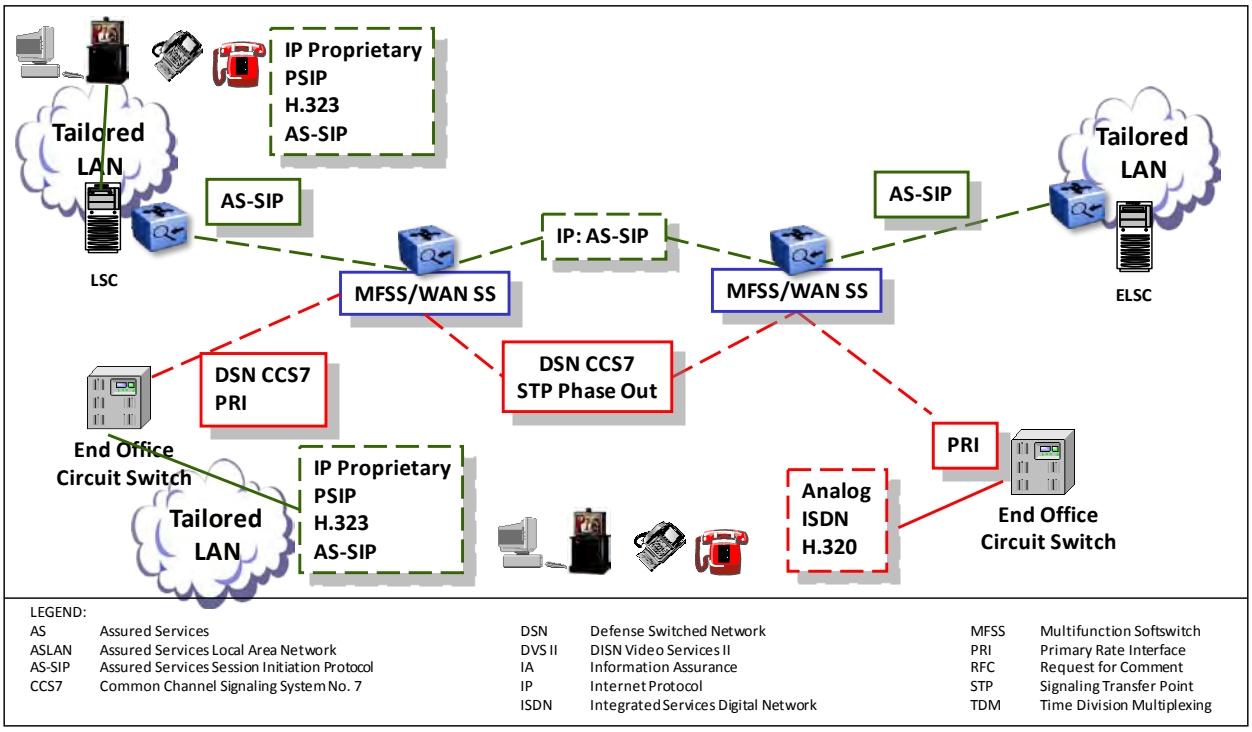


Figure 4.3.1-12. SBU Voice and Video Services Signaling Design

A stand-alone SS will support AS-SIP signaling in the classified 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 DSN CCS7 network is being phased out and replaced by PRI trunks. The TDM EOs signals via DSN CCS7 or PRI 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.

The MFSSs use DSN CCS7 or PRI to set up TDM-to-TDM EI sessions across the TDM trunking part of the DISN WAN. Both types of signaling (IP and TDM) 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.

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

- Two-level signaling hierarchy: LSC and MFSS (or WAN SS)
  - LSC A to MFSS A to MFSS B to LSC B when the LSCs have different primary MFSSs
  - LSC A to MFSS A to LSC B when they have the same primary MFSS

- The LSCs are assigned a primary and backup MFSS for signaling robustness
- Signaling from an IP EI to an LSC may be proprietary, or AS-SIP
- 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
- The LSC can set up:
  - On-base sessions when a connection to an MFSS is lost
  - Sessions to PSTN trunks independent of an MFSS
- Signaling
  - A TDM EO will signal via DSN CCS7 or PRI to MFSSs
  - The MFSSs will signal via PRI to the PSTN and to coalition gateways

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 Assured Services 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 PRI signaling.

The end-to-end, two-level SBU AS-SIP network signaling design is shown in Figure 4.3.1-13, End-To-End Two-Level SBU AS-SIP Network Signaling Design. This diagram illustrates operations with Distributed LSCs. Operations will be similar for ELSCs. For classified networks, the two-level signaling uses WAN SSs rather than MFSSs.

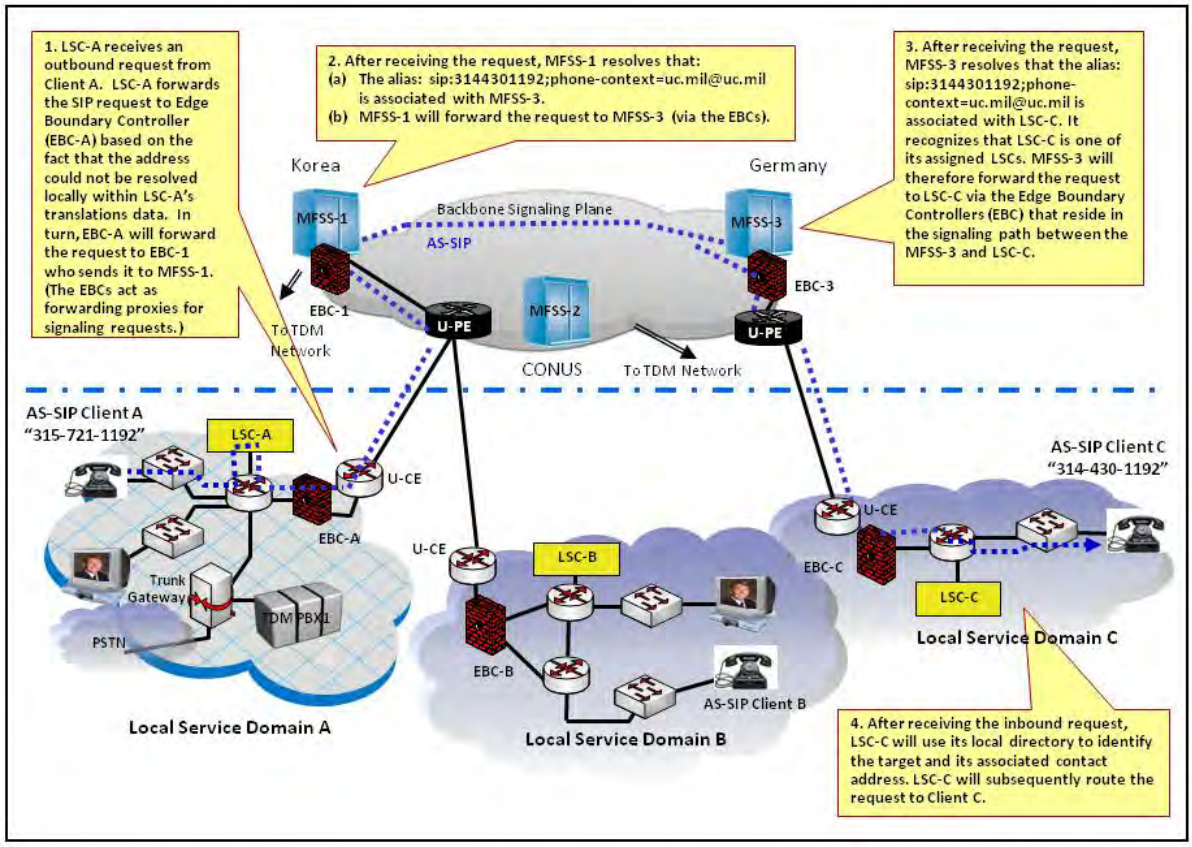


Figure 4.3.1-13. End-To-End Two-Level SBU AS-SIP Network Signaling Design

4.3.1.1.7 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 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/ELSCs and MFSS to external control devices, and the design of the ASLAN. The methods for securing the VVoIP protocols are illustrated in Figure 4.3.1-14, 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. In an Enterprise configuration, the sites can be in a single information assurance accreditation boundary in which the EBCs shown in the diagram will be associated with the ARs and will not be at the "local service enclaves."

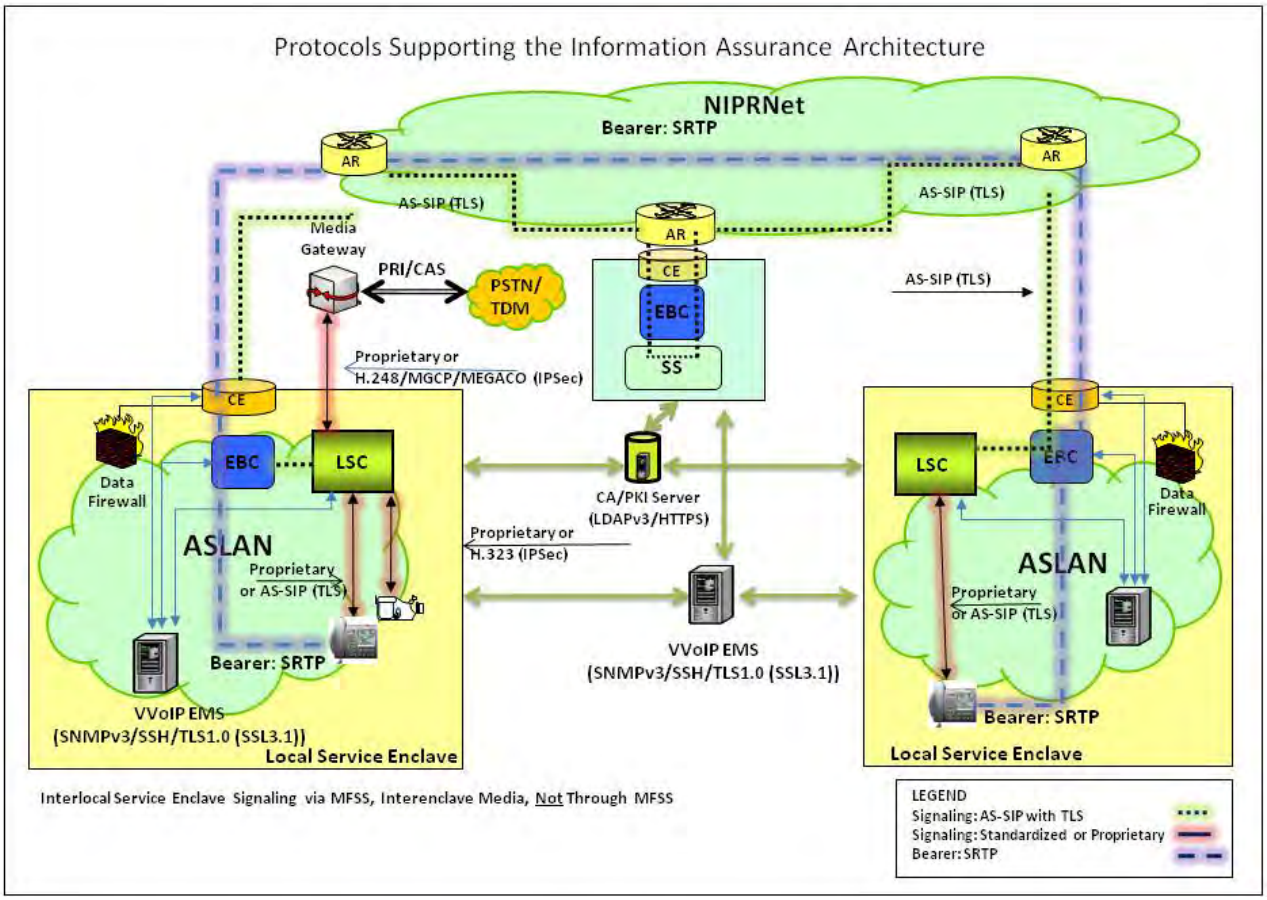


Figure 4.3.1-14. Information Assurance Protocols

Figure 4.3.1-15, VoIP Products External Ethernet Interfaces, illustrates the Information Assurance design for interfaces to external support systems (e.g., local and remote EMSs) and signaling and bearer virtual LANs (VLANs). This information assurance design uses access controls that may be configured to control traffic between interfaces.

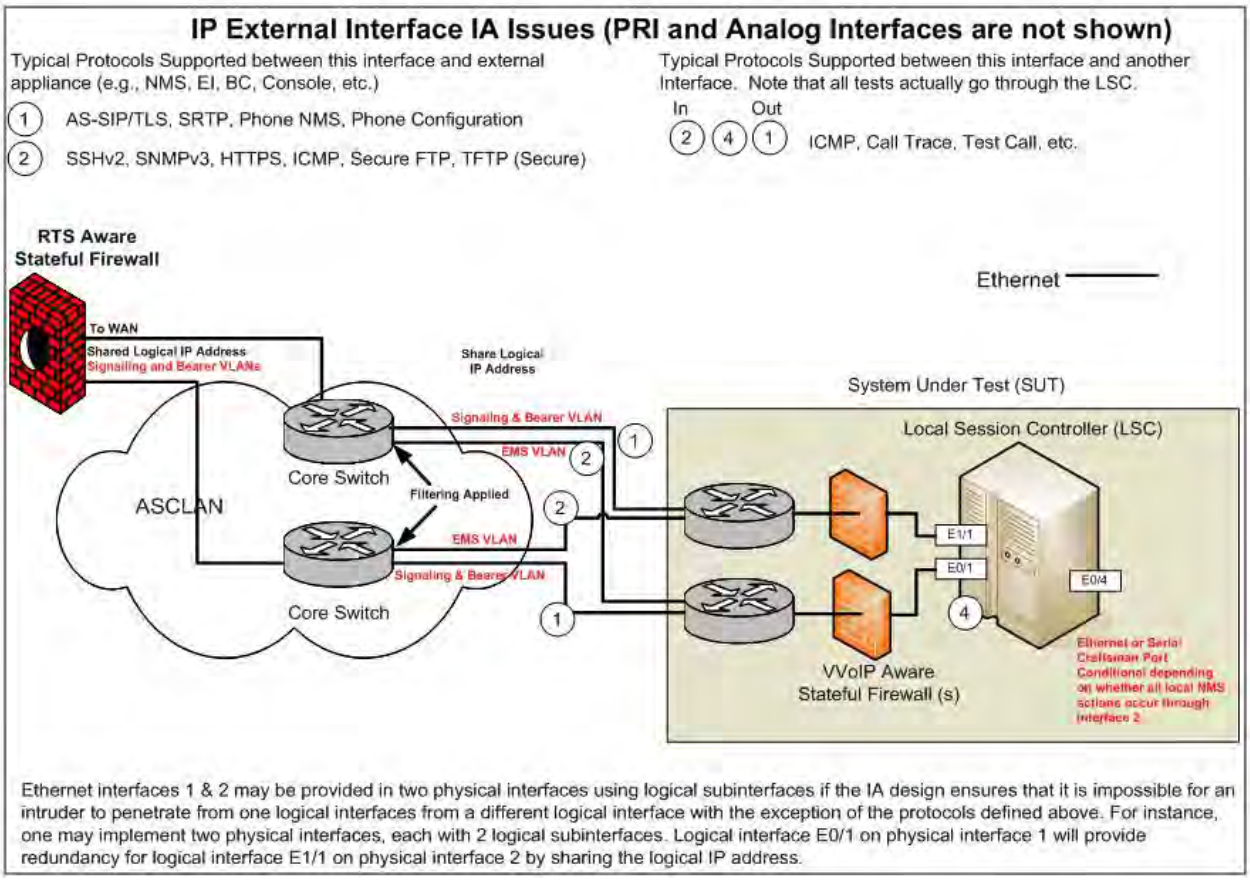


Figure 4.3.1-15. VVoIP Products External Ethernet Interfaces

Figure 4.3.1-16, ASLAN Enclave Boundary Security Diagram, depicts a diagram of the information assurance design needed as part of the ASLAN. The key feature of Figure 3.4.1-16 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 EBC consisting of the voice and/or video firewall/border controller, has been defined and specified in Section 5.3.2, Assured Services Requirements. In an Enterprise configuration, the site can be in a single information assurance accreditation boundary in which the EBCs shown in the diagram will be associated with the ARs and will not be within the Enclave Boundary shown on the diagram.

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.

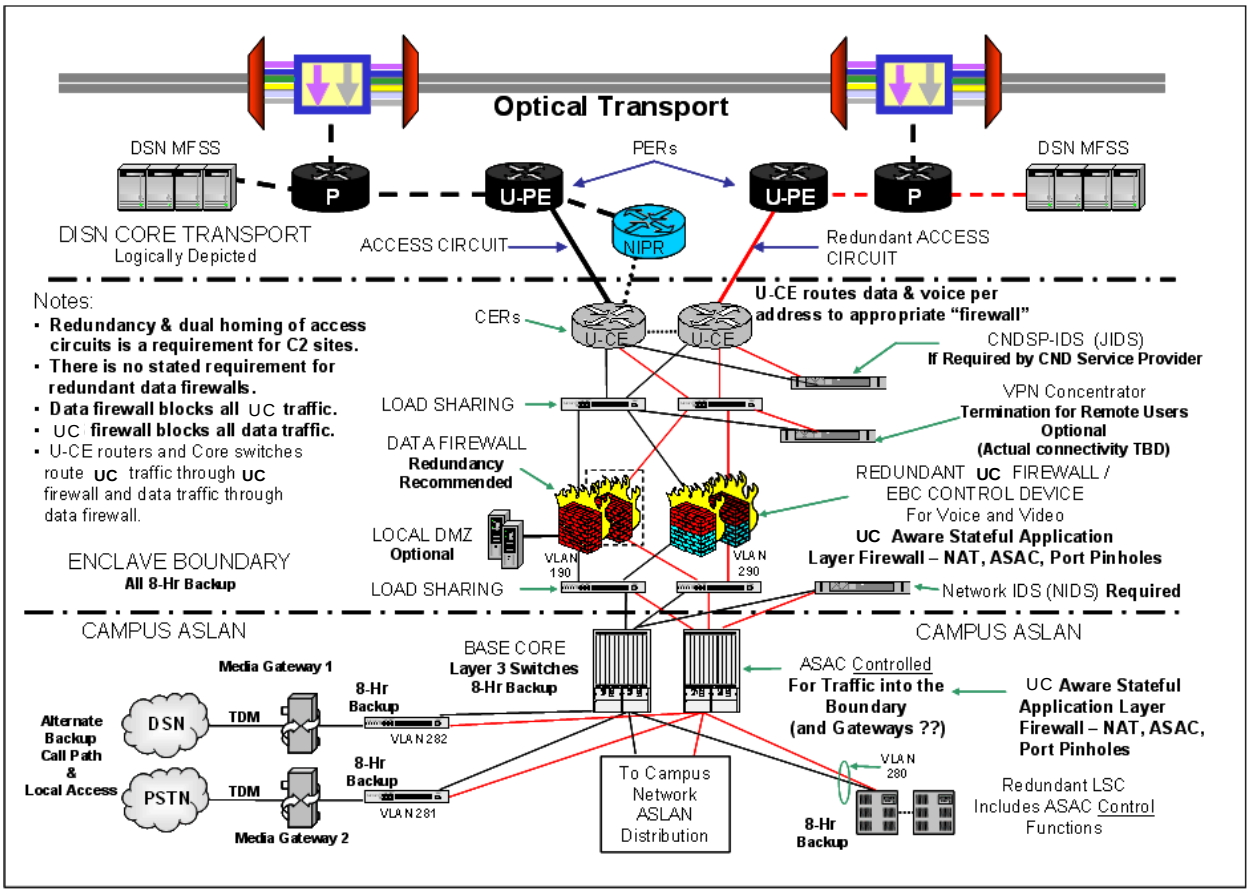


Figure 4.3.1-16. ASLAN Enclave Boundary Security Design

4.3.1.1.8 Network Management Design

Network management of the VVoIP services end-to-end is a critical component of NetOps. Since the VVoIP network will be a hybrid network for an extended period, the NMS must continue to provide an EMS that can command and monitor the voice and video services for both circuit-switched and IP technologies as part of the DISN Operational Support System (OSS). This hybrid operation within the DISN OSS is illustrated in Figure 4.3.1-17, Role of RTS EMS in DISN OSS, where the EMS is shown at the bottom of the DISN OSS hierarchy.

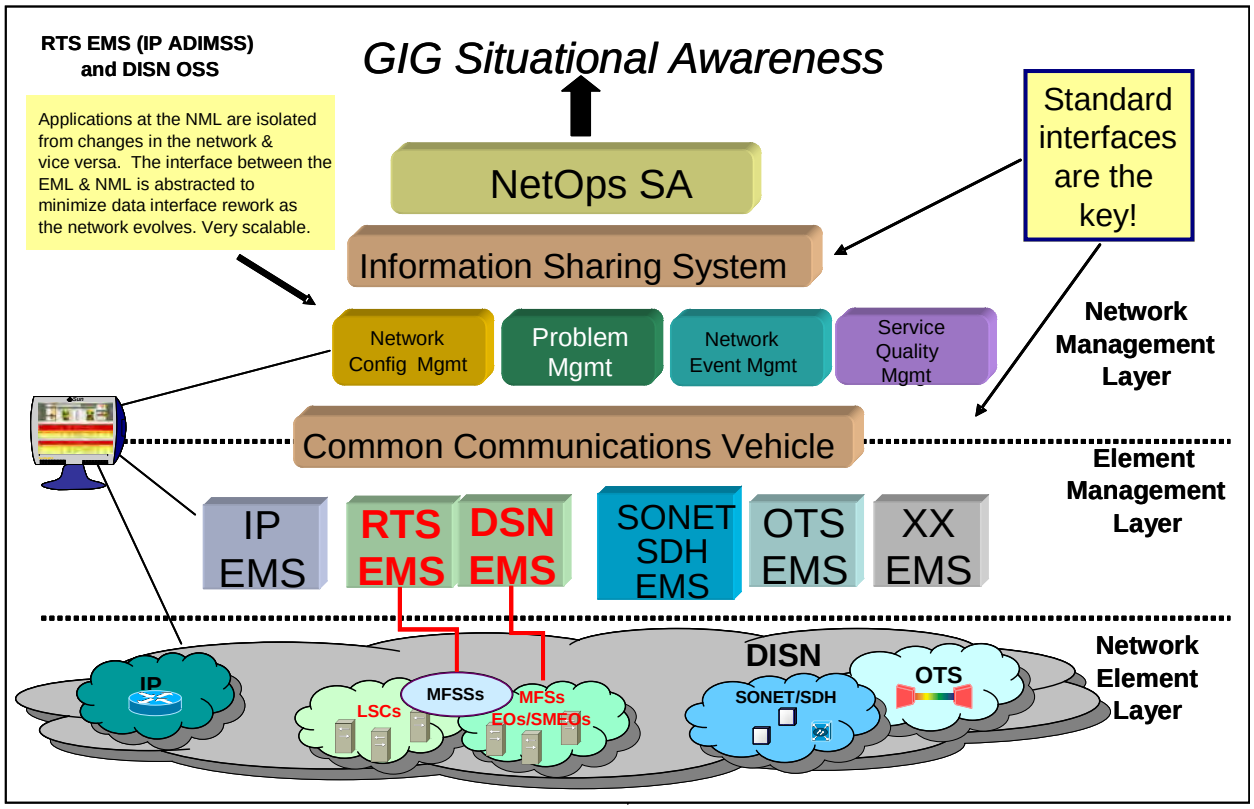


Figure 4.3.1-17. Role of RTS EMS in DISN OSS

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 real time services (RTS) EMS must provide new web services interfaces for "reading and writing" to the Services' NMS to support the CYBERCOM in both visibility and reconfiguration of the network, and in controlling the flow of sessions. The design for support of CYBERCOM is illustrated in Figure 4.3.1-18, RTS EMS Role in Providing End-to-End GEM. 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.

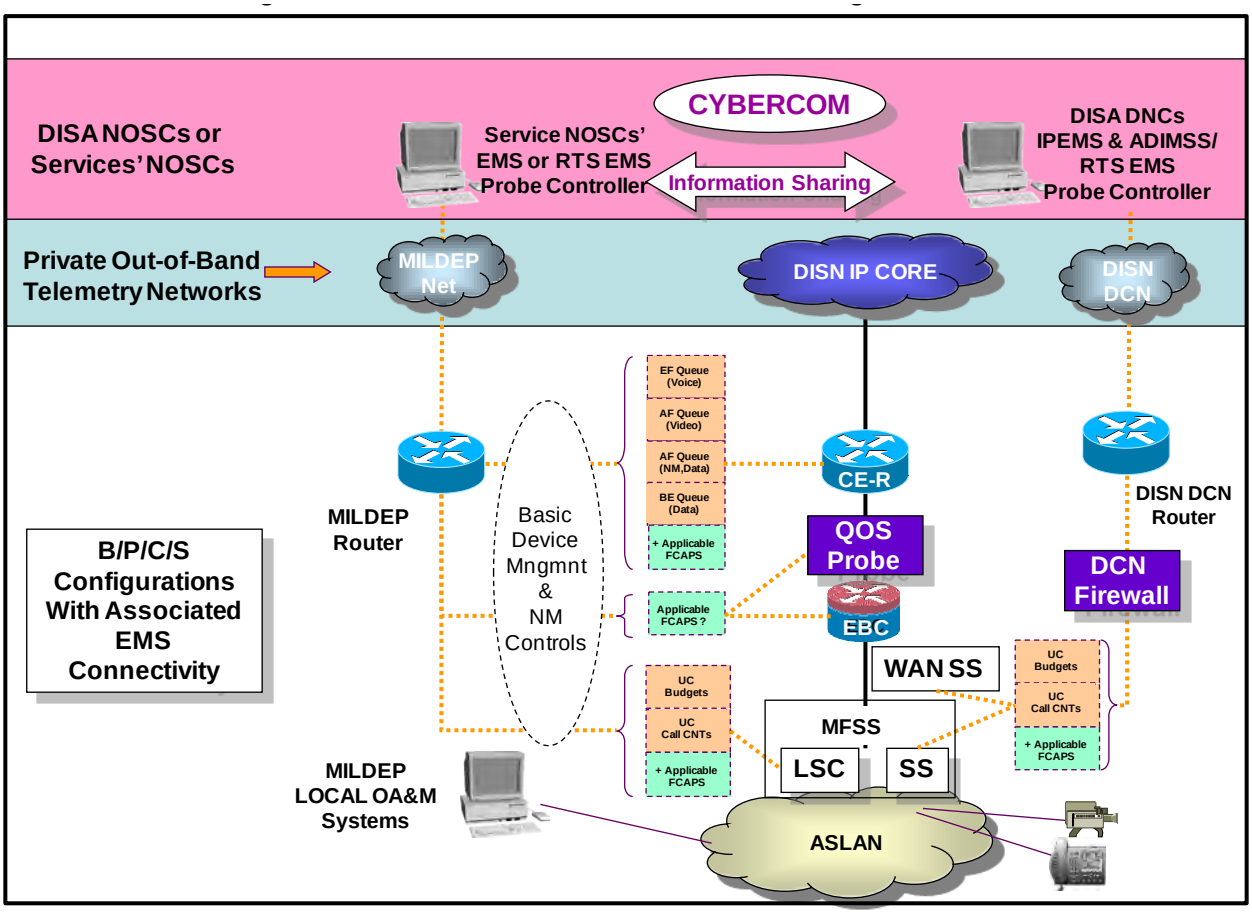


Figure 4.3.1-18. RTS EMS Role in Providing End-to-End GEM

4.3.1.1.9 Enterprise-wide Design

The enterprise-wide design as illustrated in Figure 4.3.1-19, Enterprise-wide Design, depicts system interfaces between the DISN backbone and the DoD Components' edge infrastructures to deliver UC to end users. A centralized EVoIP infrastructure with security features and access to commercial wired and wireless services is provided as part of the DISN by DISA. At the DoD Components' B/P/C/S sites, a common EVoIP infrastructure of Media Gateways and Survivable Call Processors at the DoD Component sites allows the DoD Components to employ the centralized EVoIP services via various end instruments and software licenses. The EVoIP network uses existing survivability inherent in the DISN and at mission critical DoD sites, and creates security enclaves to reduce equipment requirements consistent with best commercial practice. If a DoD Component chooses to enhance the survivability and security at a particular site, those costs are considered mission driven. This approach provides potential cost avoidance and equipment footprint reduction for voice, video, and data services, operations and maintenance, network operations, sustainment, and information assurance at DoD sites worldwide. UC Transport will be primarily provided by the DISN NIPRNet and SIPRNet. A key concept depicted in the diagram is for tailoring UC implementations in DoD based on three

organizational mission environment types. A location's final recommended architecture will be based on the aggregate of tenant organizations' mission environments at a given location. This design consists of an Enterprise Service node location from which a centrally located ELSC is capable of supporting a broad range of Enterprise Services to geographically separate regions. Information assurance accreditation boundaries will be tailored to local missions in order to centralize EBCs as much as practical. Access to the voice ISPs and commercial wireless services are provided centrally at the Enterprise level. However, PSTN TDM access is also available directly from each local service enclave via remote media gateways controlled by the ELSC. The centralized design can provide a tighter integration with DISN enterprise collaboration, directory services, and conferencing offerings.

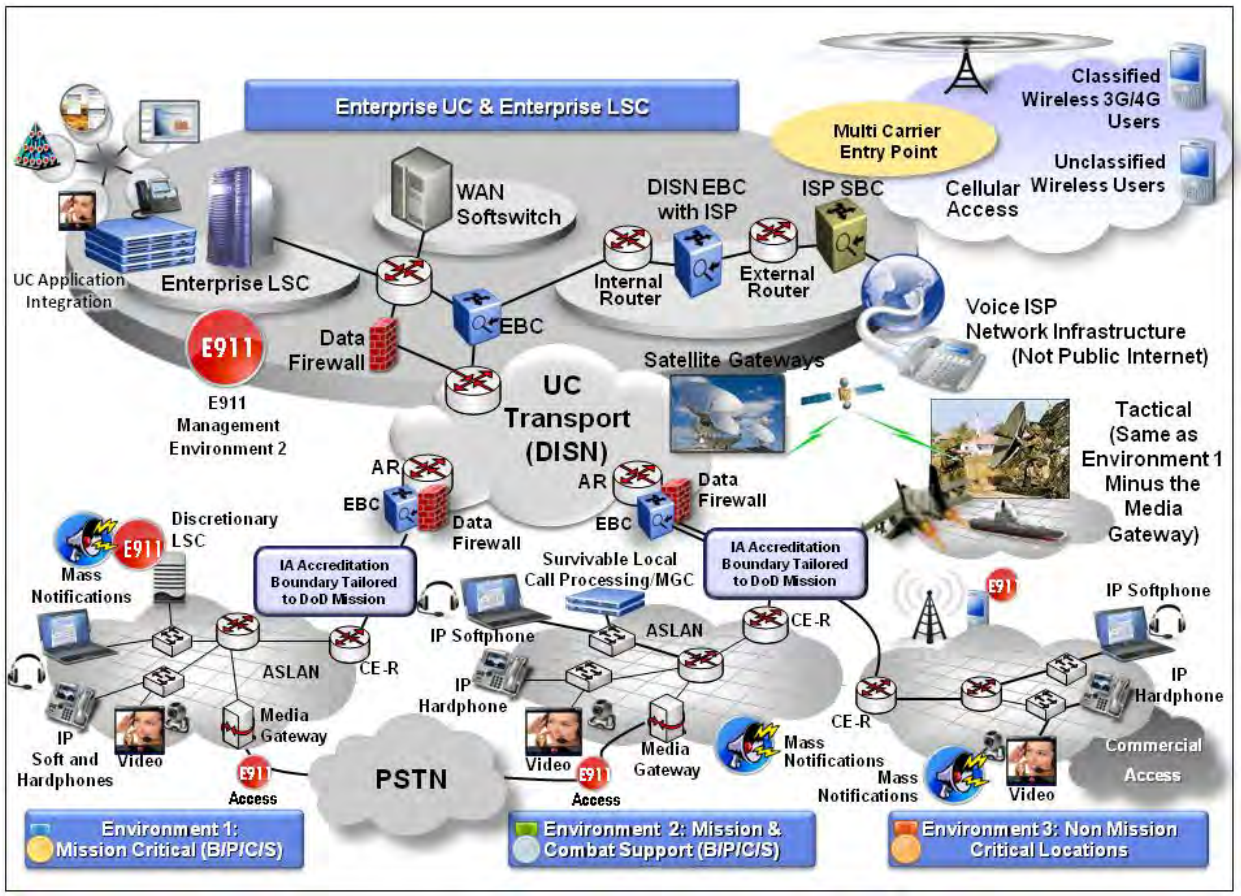


Figure 4.3.1-19. Enterprise-wide Design

The functional requirements, performance objectives, and technical specifications needed for the initial deployment phase for Enterprise assured, secure, and interoperable UC, using multiple vendor products, will be defined in this and future versions of the UCR. The major functional requirements for the ELSC are identified as follows:

1. The system shall provide an integrated enterprise voice and video capability.

2. The system shall provide an enterprise voicemail capability.

3. The system shall provide an AS-SIP voice and video conferencing capability.

4. The system shall offer hardware based voice, video, and videophone end instruments.

5. The system shall offer software based integrated voice, video, and text based data services (i.e., IM, presence, click-to-talk, chat).

6. The system shall have a migration path to federate text based data services (i.e., IM, presence, chat) with the Defense Connect On-line (DCO) XMPP server in accordance with section 5.7 of the UCR.

7. The system shall support an enterprise directory with a migration path to interoperate with the Joint Enterprise Directory Services (JEDS) directory populating the subscriber information in the directory.

8. The system shall support AS-SIP to the end instrument (AS-SIP end instruments are not required) although proprietary end instruments are allowed.

9. The system shall be capable of transitioning sessions to local attendants when appropriate to meet assured service requirements (i.e., defer precedence calls to MILDEP attendant instead of voicemail).

10. The system shall have a migration path to support the population of the RTS Routing Database as defined in Section 5.3.2 of the UCR.

11. The system shall support the LSC requirements defined in Section 5.3.2 of the UCR.

12. The system shall meet the end instrument (voice and video) requirements defined in Section 5.3.2 of the UCR.

13. The system shall interoperate with external enterprise solutions (i.e., one region to another region) using AS-SIP as defined in Section 5.3.4 of the UCR.

14. The system shall meet the information assurance requirements defined in Section 5.4 of the UCR.

15. The system shall meet the IPv6 requirements defined in Section 5.3.5 of the UCR.

16. The system shall have the capability to assign end instruments to different ASAC budgets consistent with their location.

17. The system shall support mobility by allowing the movement of the end instrument from one physical location (ASAC Budget A) to another (ASAC Budget B) within the enterprise region while making the transition transparent to the user.

18. The system shall support the DSCP markings defined in Section 5.3.3 of the UCR.

19. The system shall be capable of supporting up to 500 ASAC budgets within a region.

20. The system shall be capable of supporting up to 50,000 end instruments within a region and must have a migration plan to support up to one million end instruments within a region.

21. The system shall have an availability of at least 99.999%.

22. The system Call Connection Agent functionality must be able to be geographically distributed to support survivability (i.e., the LSC cannot be centralized at a single DECC/Base).

23. The ability of the end instruments to initiate and receive session invites shall not be impacted during a CCA failover although a session attempt in progress may be terminated requiring redial.

24. The system shall support billing, such as long distance charges, on a per ASAC budget basis.

25. The system shall be capable of providing local PRI PSTN access to avoid long distance charges for local MILDEP PSTN calls.

26. The system shall be capable of securely registering and controlling end instruments and media gateways across the enterprise information assurance boundaries using protocols that are approved by the Ports, Protocols, and Service Management (PPSM) Category Assurance List (CAL).

27. The system shall be capable of supporting announcements for the end instruments that are not impacted by enterprise information assurance (i.e., PPSM and firewalls) and WAN (e.g., delay, packet loss) boundaries.

28. The system shall be capable of operating across DoD firewalls where NAT/NAPT is performed.

29. The system shall be capable of providing OA&M across the enterprise to include the end instrument.

30. The system shall be capable of properly routing Public Safety Answering Point (PSAP) calls to the appropriate local level.

4.3.1.2 Classified VoIP Network Design

Figure 4.3.1.2-1, 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, described in Section 6.2, Unique Classified Unified Capabilities Requirements.

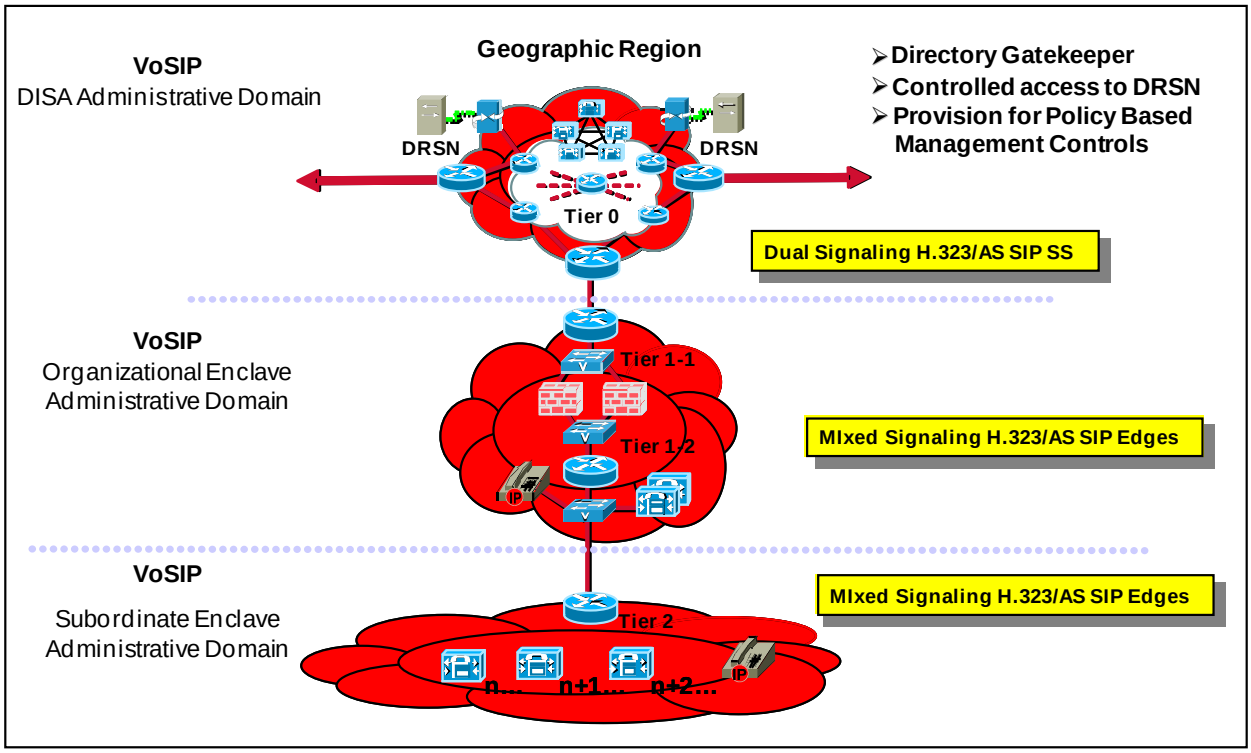


Figure 4.3.1.2-1. Classified VoIP Network Design Illustration

4.3.1.3 VTC Network Design

DISA provides VTC services as part of DISN Video Services (DVS). This service is available to the DoD, other Federal Government Departments and Agencies and their contractors for joint operations, and the MILDEPs have their own VTCs for their unique COIs.

Currently, IP Video Teleconferencing is allowed over the NIPRNet and the SIPRNet. The current DoD VTC architecture uses H.323 on IP routed networks and H.320 on the ISDN TDM DSN. The H.323 IP configurations are not specified to provide assured services. Due to DoD Components' budgetary constraints and because the VTC IP technology insertion must be determined by business cases, the current versions of DVS VTC and MILDEP VTC technologies will provide voice and video services over the DISN for the next several years as users transition to AS-SIP based VTC. Figure 4.3.1.3-1, Video Products Operations in a Hybrid Network, illustrates a high-level network design employing a variety of video products in a hybrid technology DISN network.

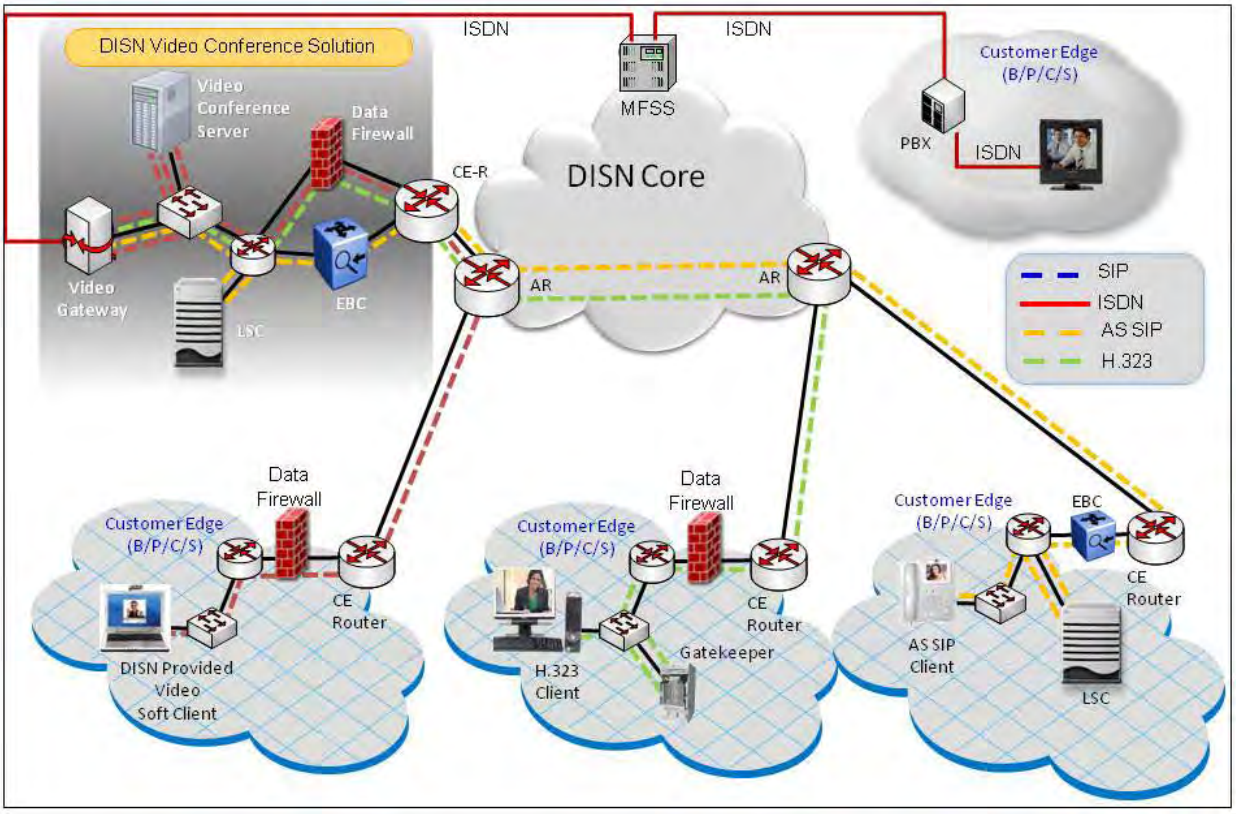


Figure 4.3.1.3-1. Video Products Operations in a Hybrid Network

H.320, H.323 and AS-SIP VTC within DoD networks and with users on public networks are addressed in the subsequent sections.

4.3.1.3.1 H.320 Video Teleconferencing

The goal is to phase out video ISDN TDM service and the H.320 protocol by Calendar Year 2013. During this transition, MILDEPs operating on video H.320 DSN networks, will have the option to migrate to an IP based H.323 or AS-SIP VTC solution. Once a full IP VTC solution has been implemented, remaining H.320 users will be supported via the use of a media

gateway with the capability to convert ISDN to an IP supported protocol. H.320 KIV-7 users will be migrated to H.323 or AS-SIP with the addition of an IP Type 1 encryption device that complies with the National Security Agency's High Assurance Internet Protocol Interoperability Specifications. Figure 4.3.1.3.2 illustrates the hybrid H.320/H.323 products and network design.

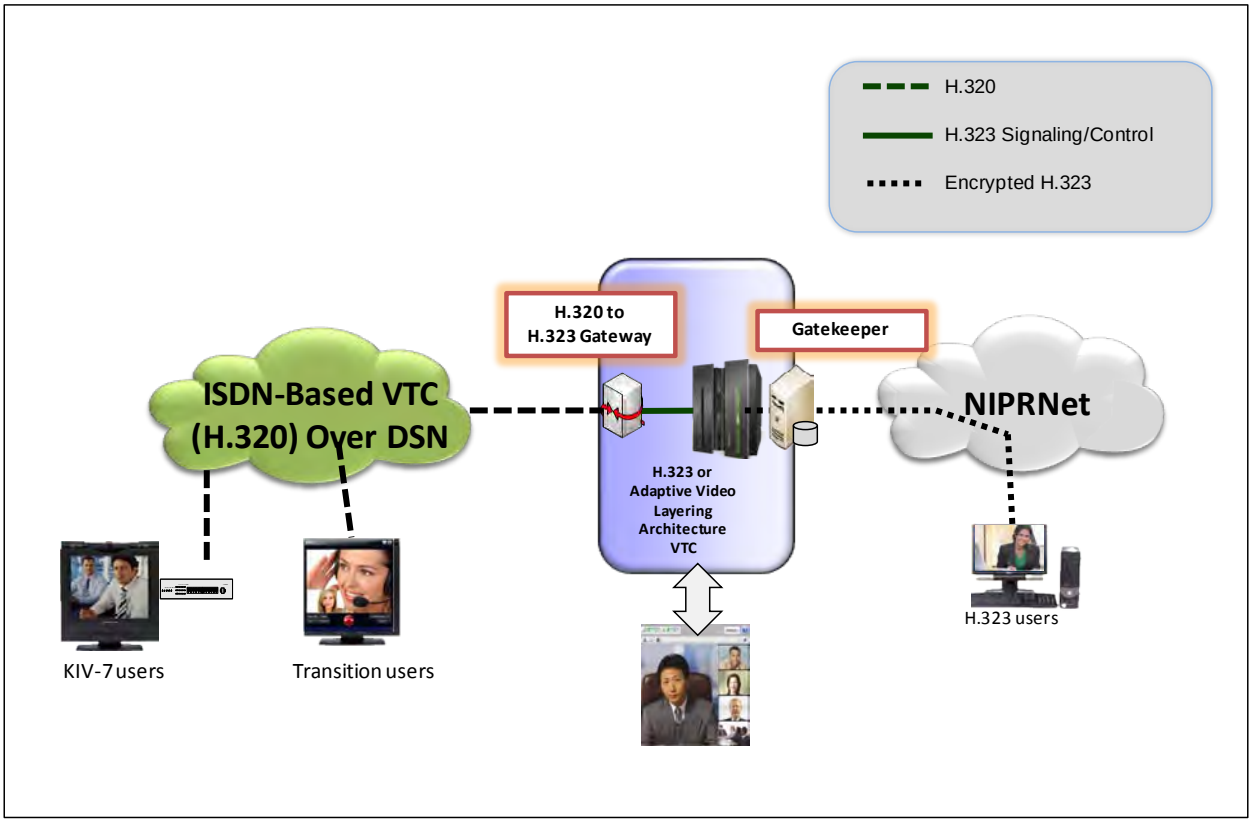


Figure 4.3.1.3-2. Hybrid H.320/H.323 Products and Network design

4.3.1.3.1 H.323 Video Teleconferencing

To meet Security Technical Implementation Guide (STIG) and PPSM Vulnerability Assessment (VA) requirements, H.323 video signaling and bearer streams have to be encrypted using a Virtual Private Network (VPN) or Application Layer encryption. In order to meet this information assurance requirement, static point-to-point or static multipoint VPNs would need to be configured at each enclave CE Router. As an alternative, a Dynamic Multipoint Virtual Private Network (DMVPN) solution can be used to scale the solution easily. Figure 4.3.1.3-3, H.323 VTC, depicts a VTC solution that leverages an H.323 Video Conferencing MCU using a statically configured multipoint VPN.

From a VTC equipment perspective, DoD Components will have the option to purchase a new H.323 VTC device or leverage a currently deployed H.323 VTC solution. KIV-7 users will need

to employ an H.320/H.323 Gateway for access to the H.323 VTC. Figure 4.3.1.3-3 illustrates H.323 VTC on the NIPRNet.

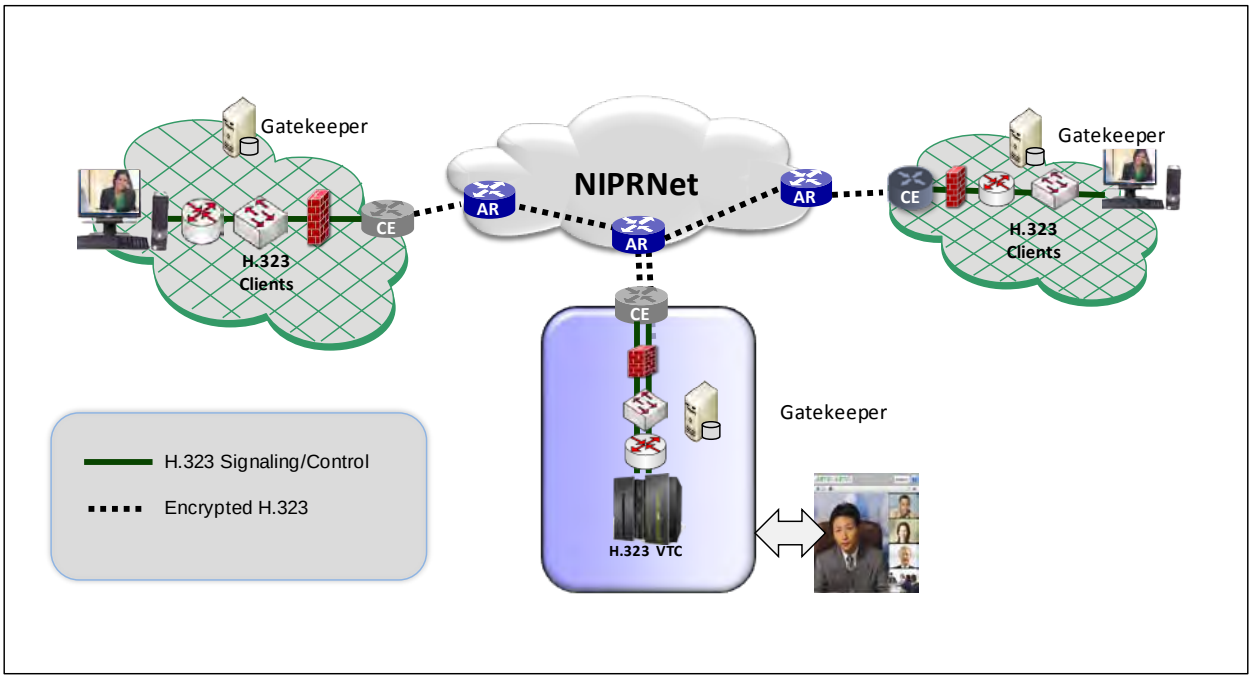


Figure 4.3.1.3-3. H.323 VTC

4.3.1.3.2 AS-SIP Video Teleconferencing With User Provided Codec

The second VTC network/product design leverages currently deployed AS-SIP architectures that support AS-SIP VTC with the customer providing the codec. In this scenario, DISA will front the video conferencing node with an AS-SIP/H.323 gateway to allow encrypted H.323 users to connect to the enclave. KIV-7 users will need to employ an H.320/H.323 Gateway for access to the VTC. This alternative is illustrated in Figure 4.3.1.3-4, H.323 VTC using AS-SIP VTC with AS-SIP/H.323 Gateway.

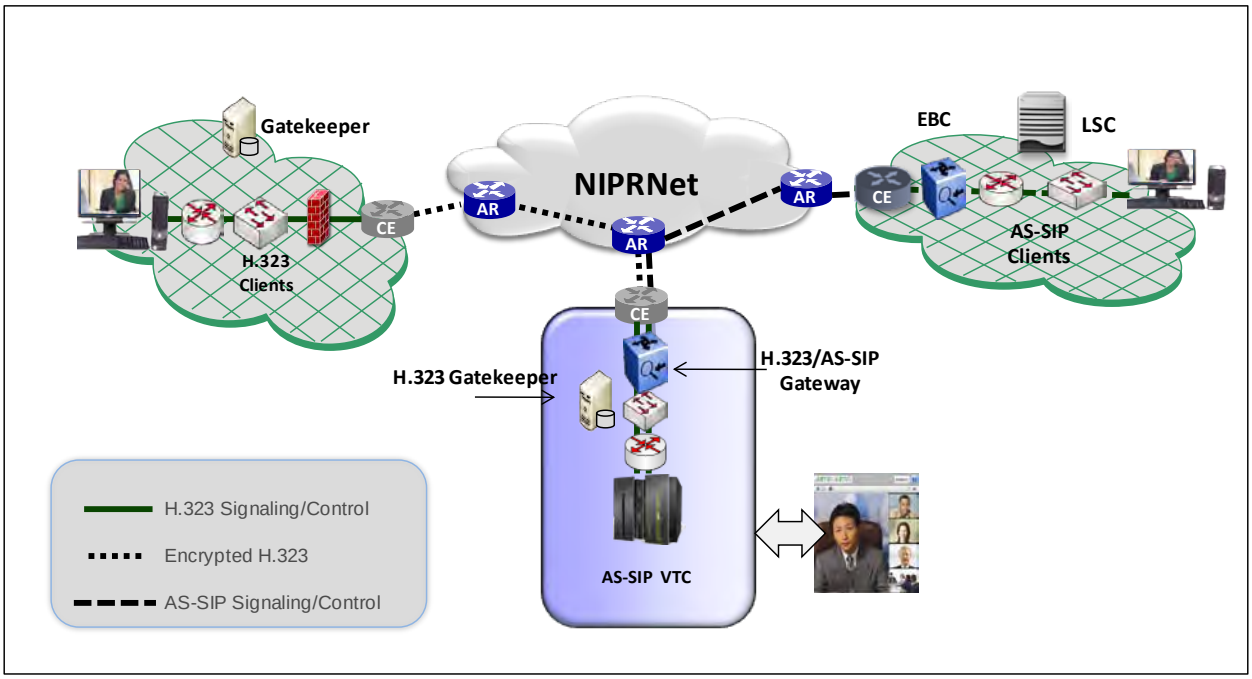


Figure 4.3.1.3-4. H.323 VTC using AS-SIP VTC with AS-SIP/H.323 Gateway

4.3.1.3.2 AS-SIP Video Teleconferencing With Software Downloaded Codec

The third VTC network/product design is based on a network design and product that uses AS-SIP and downloads the video codec to the user's personal computer (PC) and adjusts the rate to meet user video quality requirements. Figure 4.3.1.3-5, AS-SIP Video Teleconferencing with Software Downloaded Codec, illustrates AS-SIP Video Teleconferencing with a software-downloaded codec.

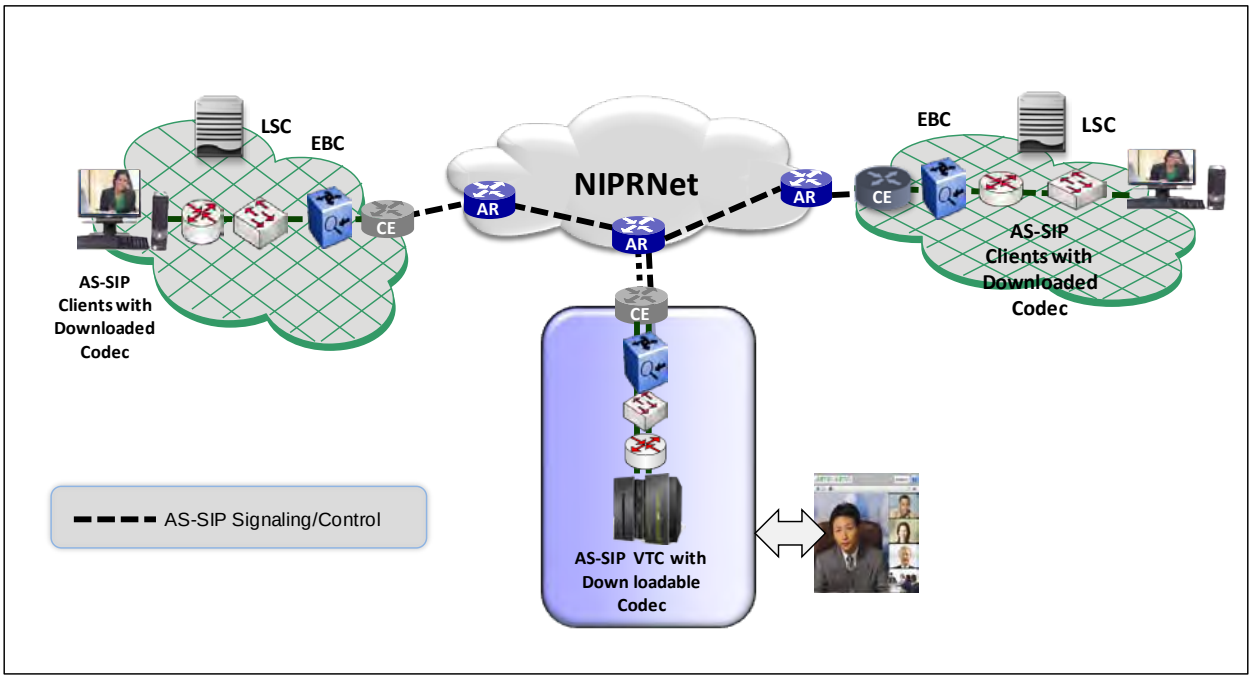


Figure 4.3.1.3-5. AS-SIP Video Teleconferencing with Software Downloaded Codec

4.3.1.3.2 Video Teleconferencing to the Internet

All commercial, Government, and coalition partner's video streams will be channeled through one of the major DoD Internet Access Points (IAPs). The IAP demilitarized zone (DMZ) will filter ingress video traffic between the internet and the DISN Core to ensure information assurance requirements are met. Video transcoding and protocol translation would occur at this point to support UCR approved video codecs and the solutions discussed in this section. Figure 4.3.1.3-6, VTC to the Internet, shows a high-level notional design for video conferencing to the internet.

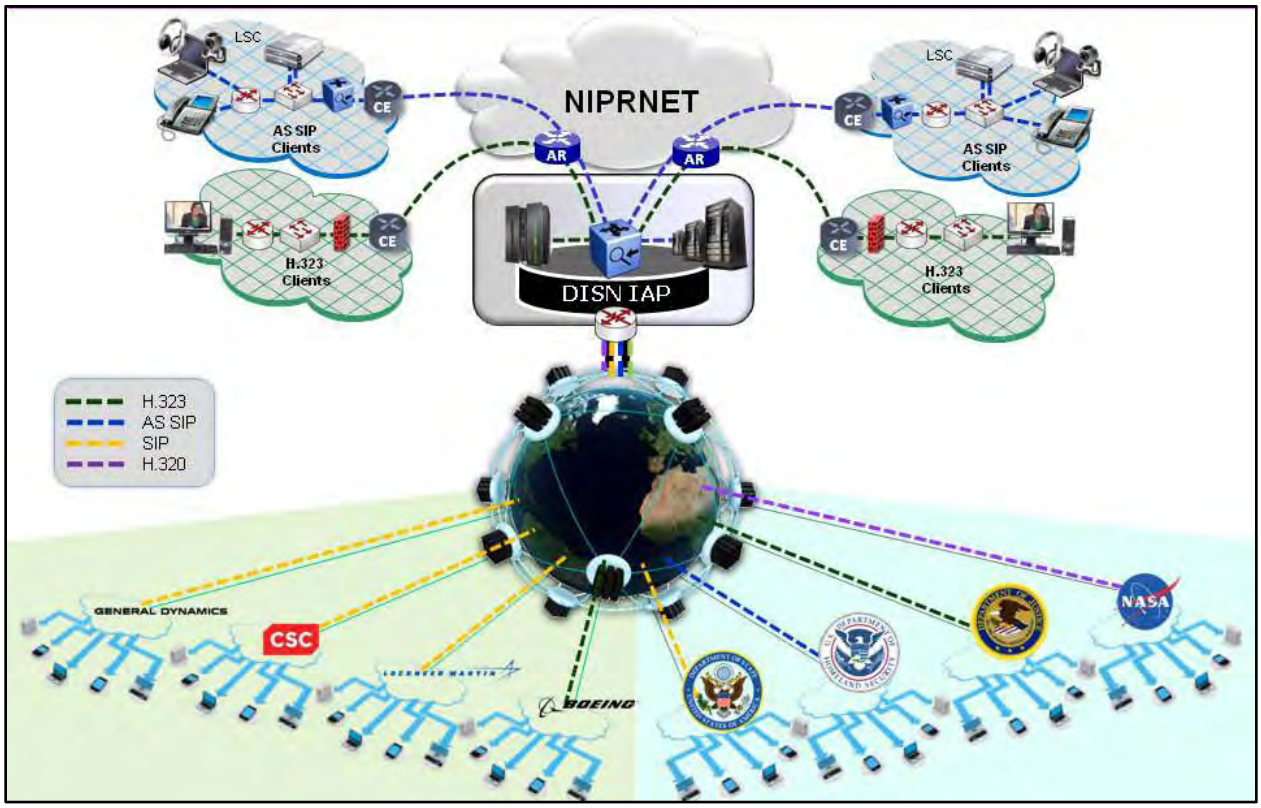


Figure 4.3.1.3-6. VTC to the Internet

4.3.1.4 Network Infrastructure Design and Products

This update to the UCR covers both the current DISN infrastructure and enhancements. The requirements are defined around functions. The products defined within this section can be deployed within the DISN or Base/Post/Camp/Station (B/P/C/S) infrastructure.

The UC products contained within this section are: Optical Transport System (OTS), Optical Digital Cross-Connect (ODXC), Multi-Service Provisioning Platform (MSPP), M13 Multiplexer (M13 Mux), Serial TDM Multiplexer (Serial TDM Mux), Timing and Synchronization Product (T&S Product), DISN Router, and Passive Optical Networks (PONs). Products within this section may be certified and APL listed for one product category (e.g., OTS) or a combined product category called a Network Infrastructure Product (NISP). Further descriptions of the products are as follows:

- OTS – OTS multiplexes optical signals from various sources (e.g., router, transport switch function, Channel Access Grooming) at the optical core layer. The OTS consists of the following components: Terminal, Reconfigurable Optical Add and Drop Multiplexer (ROADM), and an Optical Line Amplifier (OLA). An Optical Supervisory Channel (OSC) runs between these

components. The terminal is composed of two elements: the transponder and the muxponder

- Transport Switch Function (TSF) – Today, the TSF functionality is satisfied by the ODXC equipment within the DISN. The TSF is an Optical cross-connect device that is located primarily at Class 1 sites but it could also be deployed at select Class 2 sites. The lowest level that it will cross-connect is an STS-1

- Aggregation Grooming Function (AGF) – receives low-speed circuits on multiple ingress ports and multiplexes them together onto higher speed egress interfaces. The AGF multiplexing allows for multiple internal cross-connects between the low-speed ports and the high-speed ports. The AGF product can connect circuits from any port to any other port within the bandwidth limitations of the ports. The AGF product within the DISN is also known as an MSPP

- Network Infrastructure Product (NISP) – Section 5.5 of the UCR defines three products: an Optical Transport Switch (OTS) product, a TSF product, and an AGF product. The product category of NISP represents the combination of two or more network infrastructure products within the same platform. The SUT is certified to perform as a NISP product by performing the functions completely of any combination of the following products: OTS, TSF or AGF

- ODXC – ODXC input optical signals are converted into electronic signals after they are demultiplexed by demultiplexers. The electronic signals are then switched by an electronic switch module. Finally, the switched electronic signals are converted back into optical signals by using them to modulate lasers and then the resulting optical signals are multiplexed by optical multiplexers onto outlet optical fibers

- MSPP – MSPPs are close to the customer, they must interface with a variety of customer premises equipment and handle a range of physical interfaces. Most vendors support telephony interfaces (DS-1, DS-3), optical interfaces (OC-3, OC-12), and Ethernet interfaces (10/100Base-T). MSPPs enable service providers to offer customers new bundled services at the transport, switching, and routing layers of the network, and they dramatically decrease the time it takes to provision new services while improving the flexibility of adding, migrating or removing customer networks

- M13 Multiplexer (M13 MUX) – M13 multiplexer, or M13 MUX, integrates 28 T1 tributary channels into a single 45 Mbps data stream using bit-level

multiplexing and M13 bit-interleaving framing format. M13 terminal multiplexers also provide T1 channel grooming and offer direct connection to T3 networks or DS3 equipment over copper or fiber links

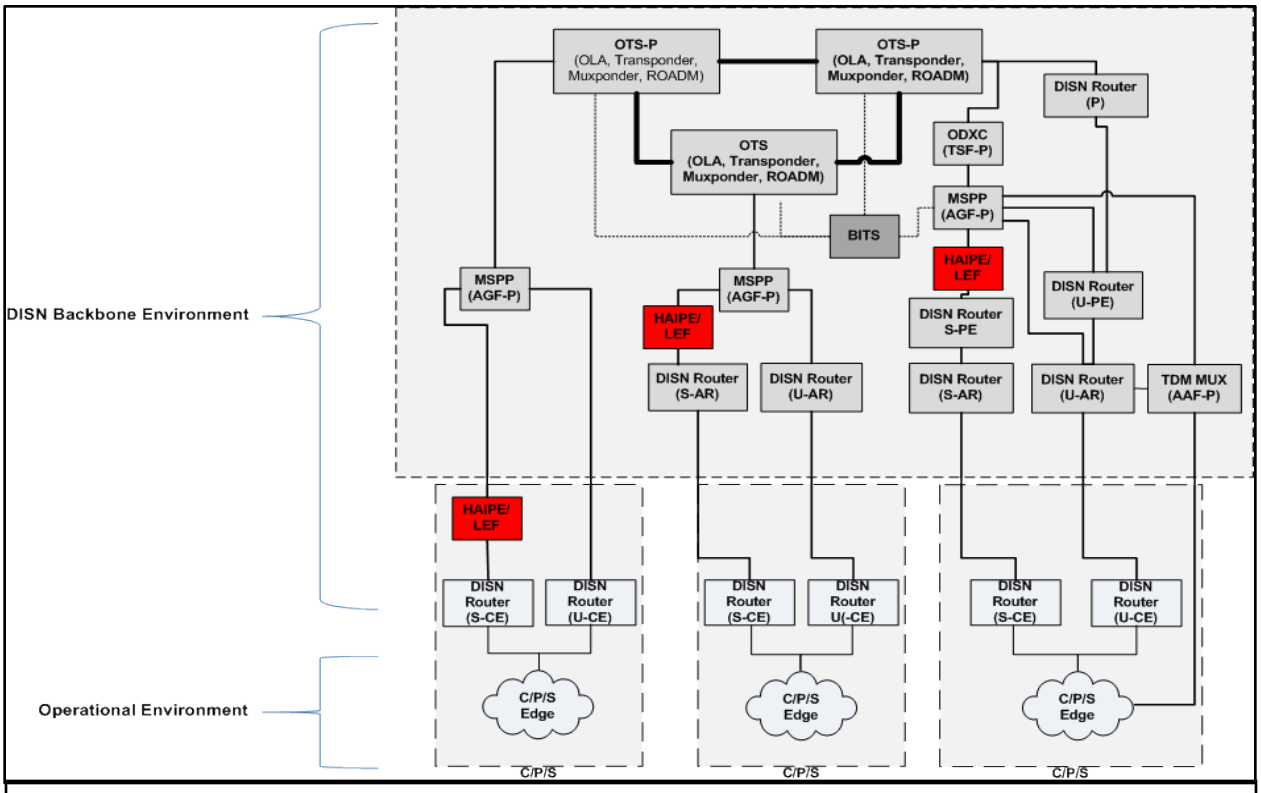
- Serial TDM Multiplexer (Serial TDM MUX) – supports TDM, asynchronous transfer mode (ATM), serial, and cell-based data types, and securely converts them for IP transport at gigabyte speeds. Serial TDM Multiplexers are required to ensure Mission critical legacy data can be smoothly transitioned to the GIG. Multiple timing recovery options, based on telecom standards should be enforced to ensure that the data that enters the IP cloud, exits in the proper order and precedence

- Timing And Synchronization (T&S) – The complexities of an analog and digital multi-standard, multi-format data transports require flexibility in customizing the synchronizing needs of the network. Signals from a master sync pulse generator (SPG) are critical in order to synchronize all of the equipment in a system

- DISN Routers – the routers required for the DISN fall into categories of small, medium, and large. Each of these routers may support a variety of interface types and numbers. The size of the routers is indicative of certain characteristics such as backplane capacity and packet forwarding capability, but the overall functionality of the router does more to place the router than any one attribute, and is determined by the sponsor

- PON – is a point-to-multipoint, fiber to the premises network architecture in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises, typically 16-128. A PON consists of an optical line terminal (OLT) at the service provider's central office and a number of optical network units (ONUs) near end users. A PON configuration reduces the amount of fiber and central office equipment required compared with point-to-point architectures. A passive optical network is a form of fiber-optic access network. Downstream signals are broadcast to all premises sharing a single fiber (encryption is used to prevent eavesdropping). Upstream signals are combined using a multiple access protocol, usually time division multiple access (TDMA)

The product placement of the equipment described above as members of the Network Infrastructure Design and Products class are depicted in Figure 4.3.1.4-1, Network Infrastructure Product.

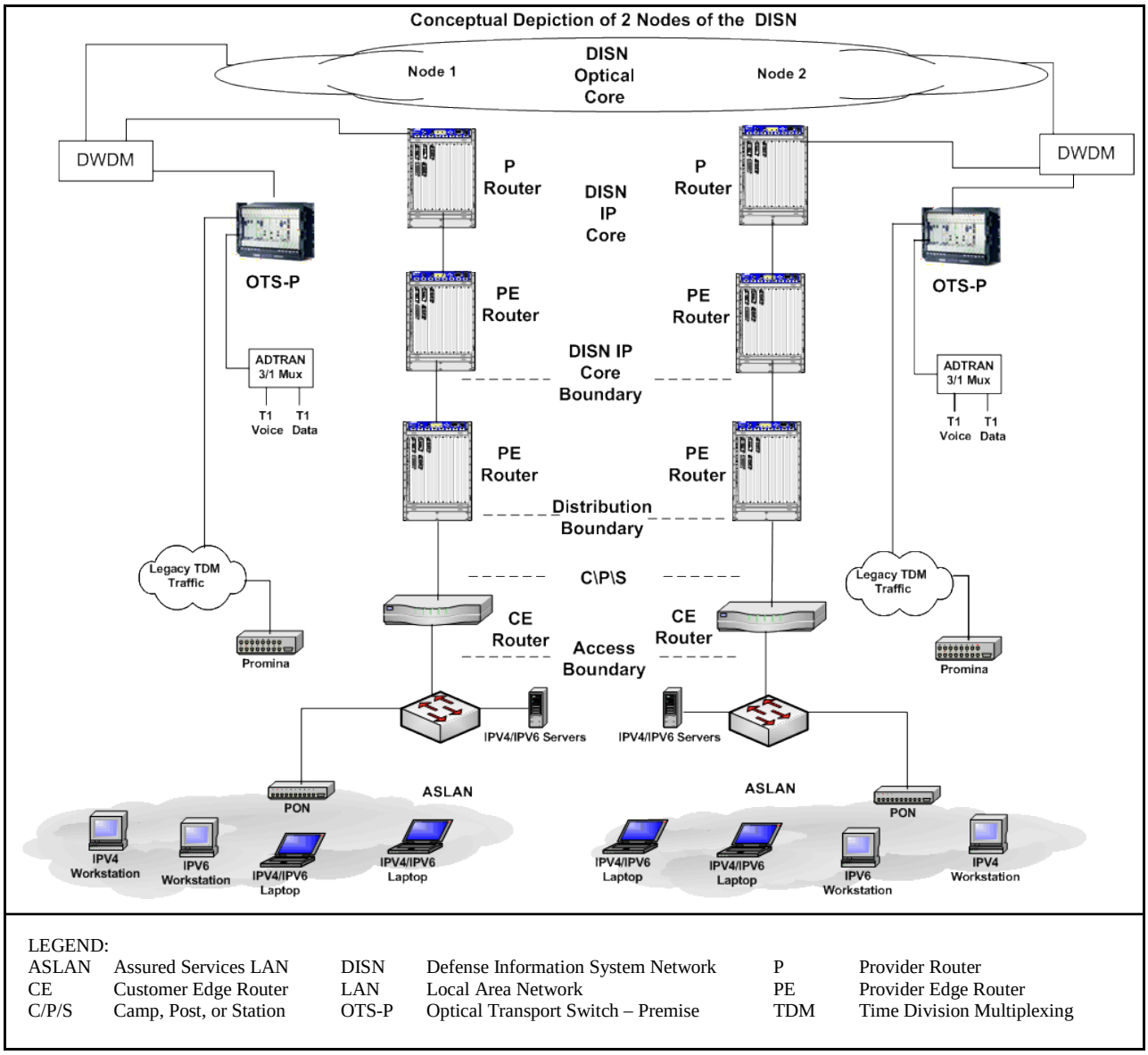


LEGEND:

AAF-P	Access Aggregation Function Product	OLA	Optical Line Amplifier
AGF-P	Access Grooming Function Product	OTS-P	Optical Transport System Product
AR	Aggregation Router	ROADM	Reconfigurable Optical Add and Drop Multiplexer
ATM	Asynchronous Transfer Mode	S-AR	Secret Aggregation Router
CE	Customer Edge Router	S-CE	Secret Customer Edge Router
C-PE	Classified Provider Edge Router	S-PE	Secret Provider Edge Router
C/P/S	Camp, Post, or Station	TDM	Time Division Multiplexing
DISN	Defense Information System Network	T-PE	Transport Provider Edge Router
HAIPE	High Assurance Internet Protocol Encryptor	TSF-P	Transport Switch Function Product
MSPP	Multi-Service Provisioning Platform	U-AR	Unclassified Aggregation Router
MUX	Multiplexer	U-CE	Unclassified Customer Edge Router
P	Provider Router	U-PE	Unclassified Provider Edge Router
ODXC	Optical Digital Cross Connect		

Figure 4.3.1.4-1. Network Infrastructure Product

Figure 4.3.1.4-2, Conceptual Depiction of 2 Nodes of the DISN illustrates the DISN router hierarchy from a Transport Boundary perspective. This will allow for a better understanding of NISP product placement relative to the DISN architecture (no circuit cross-connects shown). Predominantly, the products OTS, ODXC, MSPP, m13 MUX, Serial TDM MUX, Building Integrated Timing Supply (BITS), and DISN Routers are currently located above the DISN Distribution Layer Boundary, extending to the DISN IP Core; while PONs predominantly exist at the C/P/S Layer (Note - that the products defined within this section can be deployed within the DISN or Camp/Post/Station infrastructure).



LEGEND:

ASLAN	Assured Services LAN	DISN	Defense Information System Network	P	Provider Router
CE	Customer Edge Router	LAN	Local Area Network	PE	Provider Edge Router
C/P/S	Camp, Post, or Station	OTS-P	Optical Transport Switch – Premise	TDM	Time Division Multiplexing

Figure 4.3.1.4-2. Conceptual Depiction of 2 Nodes of the DISN

Figure 4.3.1.4-3, DISN Router Hierarchy, illustrates the current DISN router hierarchy 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, respectively.

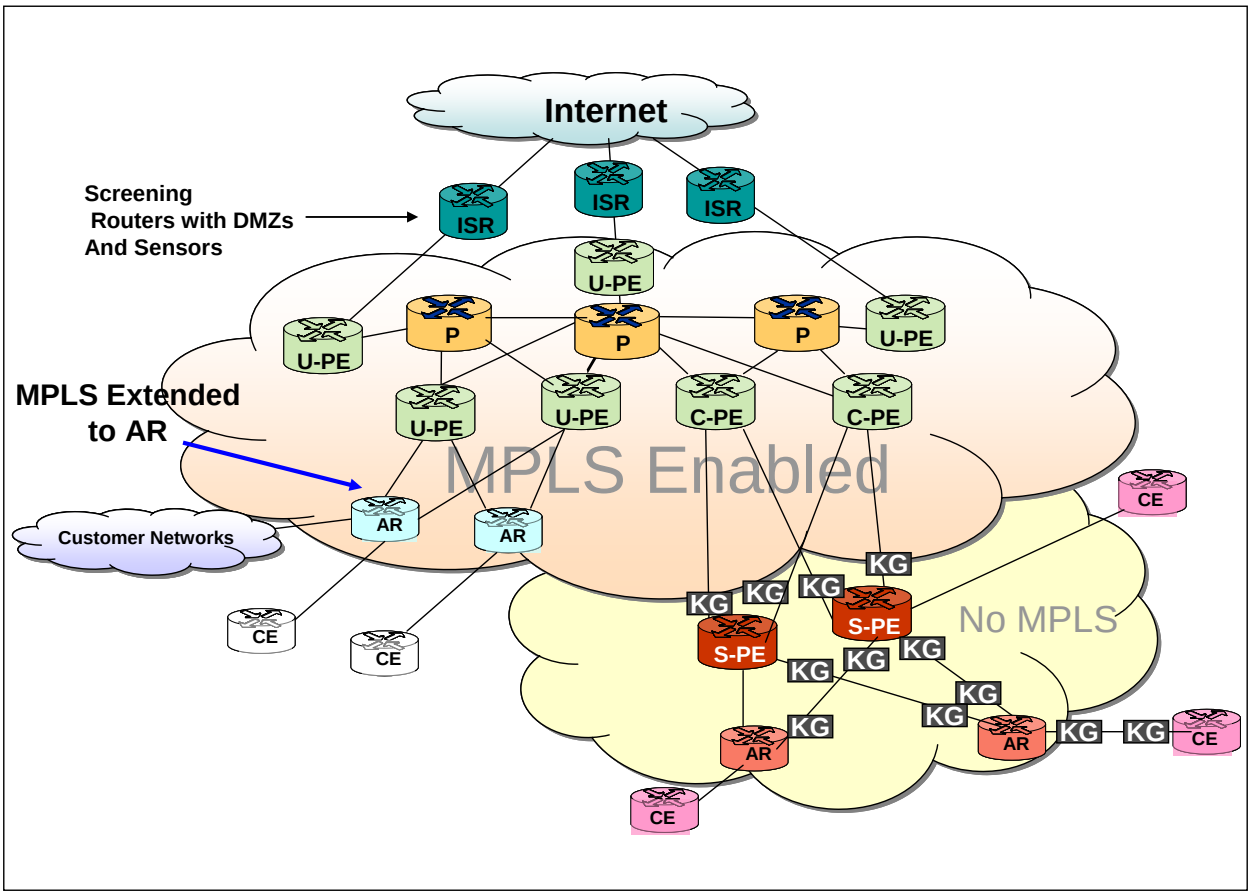


Figure 4.3.1.4-3. DISN Router Hierarchy

Near Term DISN Architecture – In addition to the DISN Core Transition, the DoD SATCOM networks will migrate from single channel per carrier (SCPC) type modems using serial trunks and dedicated point-to-point satellite circuits to IP modems over DAMA/BoD Time Division Multiple Access (TDMA) connections that allow for the more efficient utilization of scarce satellite resources. DISA leads the way in IP modem standards development that leverages COTS implementations in order to achieve interoperability in the meantime. Through its partnership with the Services, DISA also uses annual Joint User Interoperability Communications Exercise (JUICE) exercises to test various features and capabilities of IP modems. The effort will be in concert with other efforts such as WIN-T, Joint Tactical Radio System (JTRS), and Wideband Gapfiller System (WGS) and is called "incremental capability phase 2". In addition, the IP modems will also contain embedded Transmission Security (TRANSEC) and centralized management to ease the network management load on deployed warfighters.

2012 – Mid Term DISN Architecture – In 2012, the MSPPs and MPLS will provide Layer 1/ Layer 2 transport capabilities. Within DISN Class1A Sites, NIPRNet and SIPRNet will have disappeared as distinct entities. Legacy TDM (if any) will be supported on the MSPP. Edge

applications (DSN, DRSN, and DVS) will primarily us IP as a transport means. If funding and technology evolution permit, ATM and Promina/Integrated Digital Network Exchange (IDNX) could be removed from the DISN.

4.3.1.5 IPv6 Network Design

Figure 4.3.1.5-1, IPv6 Design for SBU and Classified VVoIP, depicts the 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.

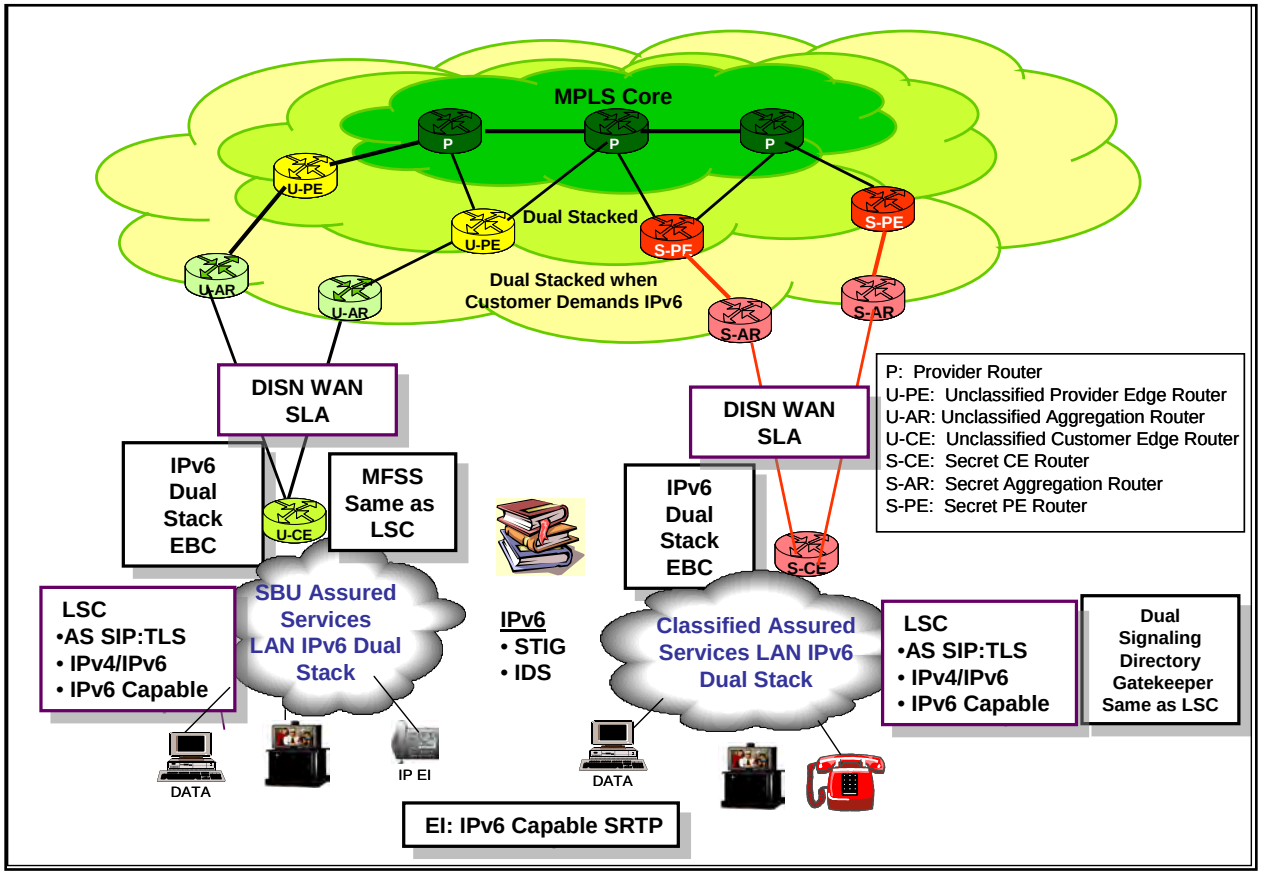


Figure 4.3.1.5-1. IPv6 Design for SBU and Classified VVoIP

4.3.2 Voice, Video, and Data Integrated Design for UC

UC services are 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.

4.3.2.1 Integration of Voice, Video, and Data (Web Conferencing, Web Collaboration, Instant Messaging and Chat, and Presence)

This section provides an overview of the initial system concepts for integration of UC services. The voice, video, and data services include multimedia or cross-media collaboration capabilities (including audio collaboration, video collaboration, text-based collaboration, and presence). The focus of the integration is to go beyond local, intra-enclave test events to implement and assess collaboration services and applications on an end-to-end, 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.

Leveraging the UCR capabilities, the key UC network-wide collaboration services objectives are listed in Figure 4.3.2.1-1, UC Network-Wide Collaboration Services Objectives.

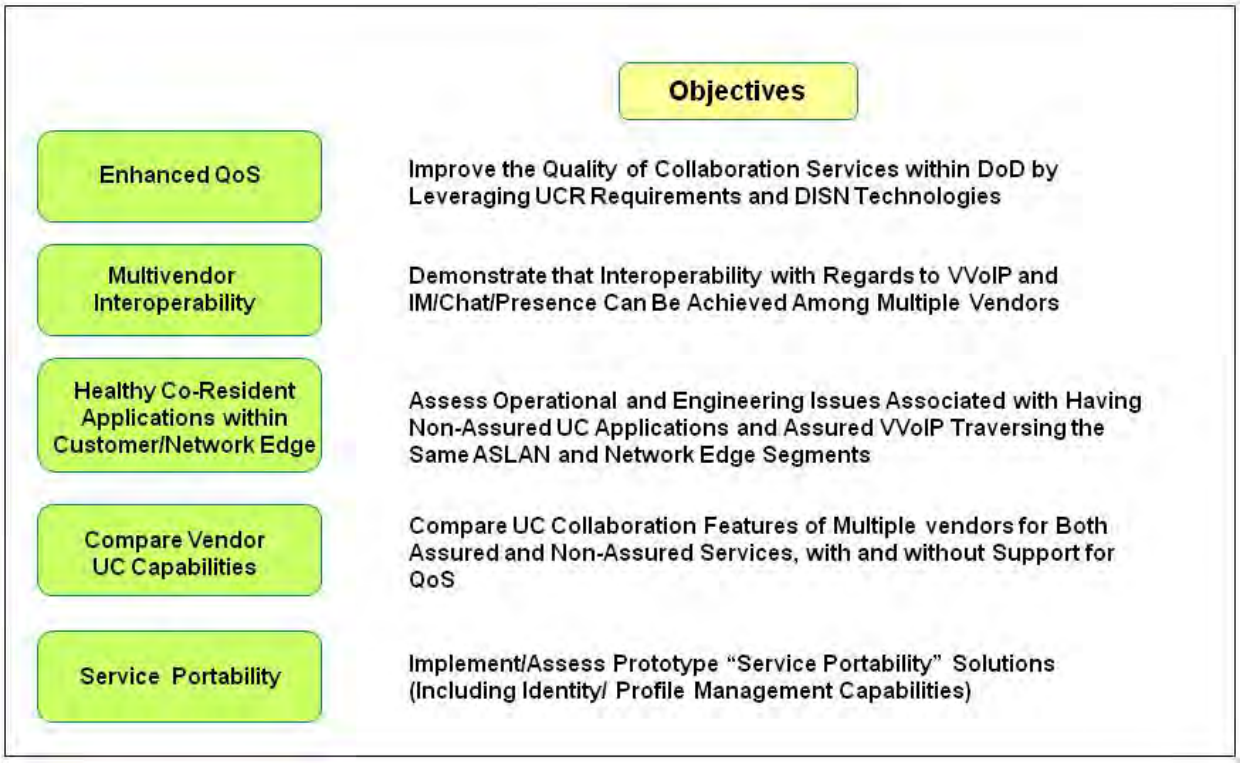


Figure 4.3.2.1-1. UC Network-Wide Collaboration Services Objectives

Figure 4.3.2.1-2, UC Collaboration Transitions, 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 Differentiated Services ("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.

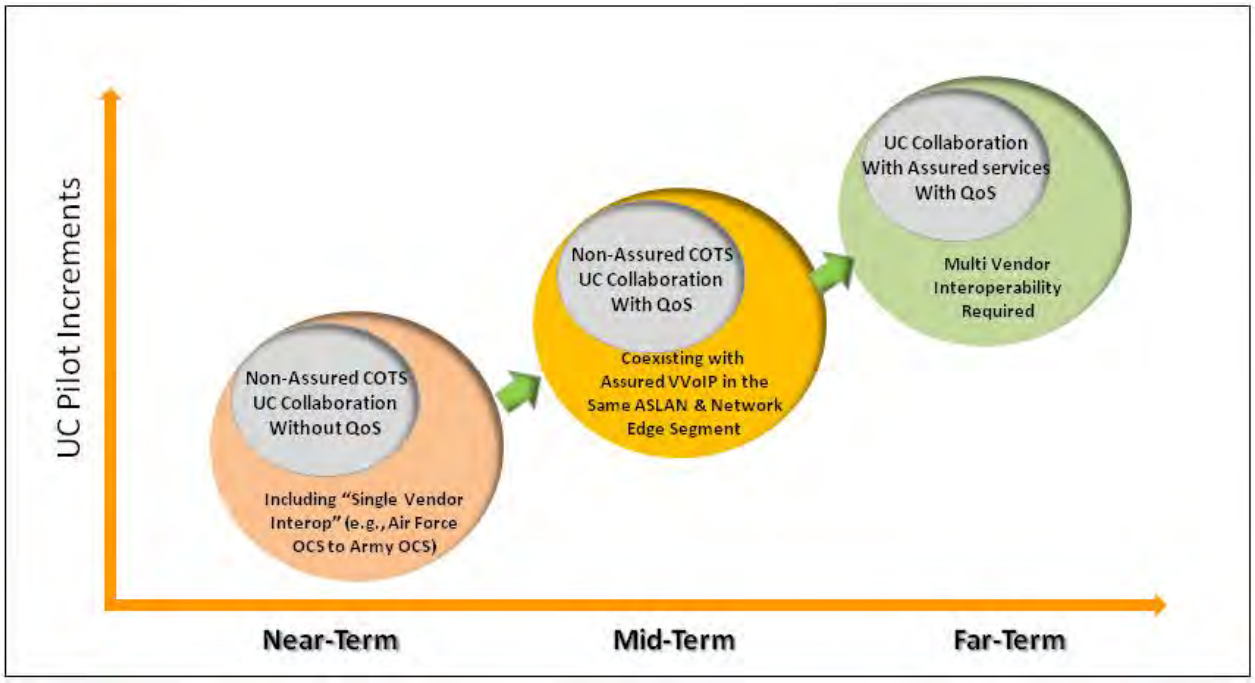


Figure 4.3.2.1-2. UC Collaboration Transitions

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 DISR requires the use of XMPP for IM, chat, and presence. Consistent with that requirement, the UCR requires XMPP for UC data. The UC framework for UC data is a federated architecture that leverages XMPP for interoperability. UC data clients can leverage other protocols such as SIMPLE, but must normalize to XMPP for interoperability. Federation allows multiple XMPP systems to interconnect in a flat topology. The enterprise LSC solution also provides an enterprise XMPP solution within a region and the Enterprise LSC will federate with the Enterprise Web Conferencing XMPP server (Defense Connect Online/Defense Collaboration Service [DCO/DCS]). Figure 4.3.2.1-3 illustrates Multivendor Interoperability Normalized on XMPP.

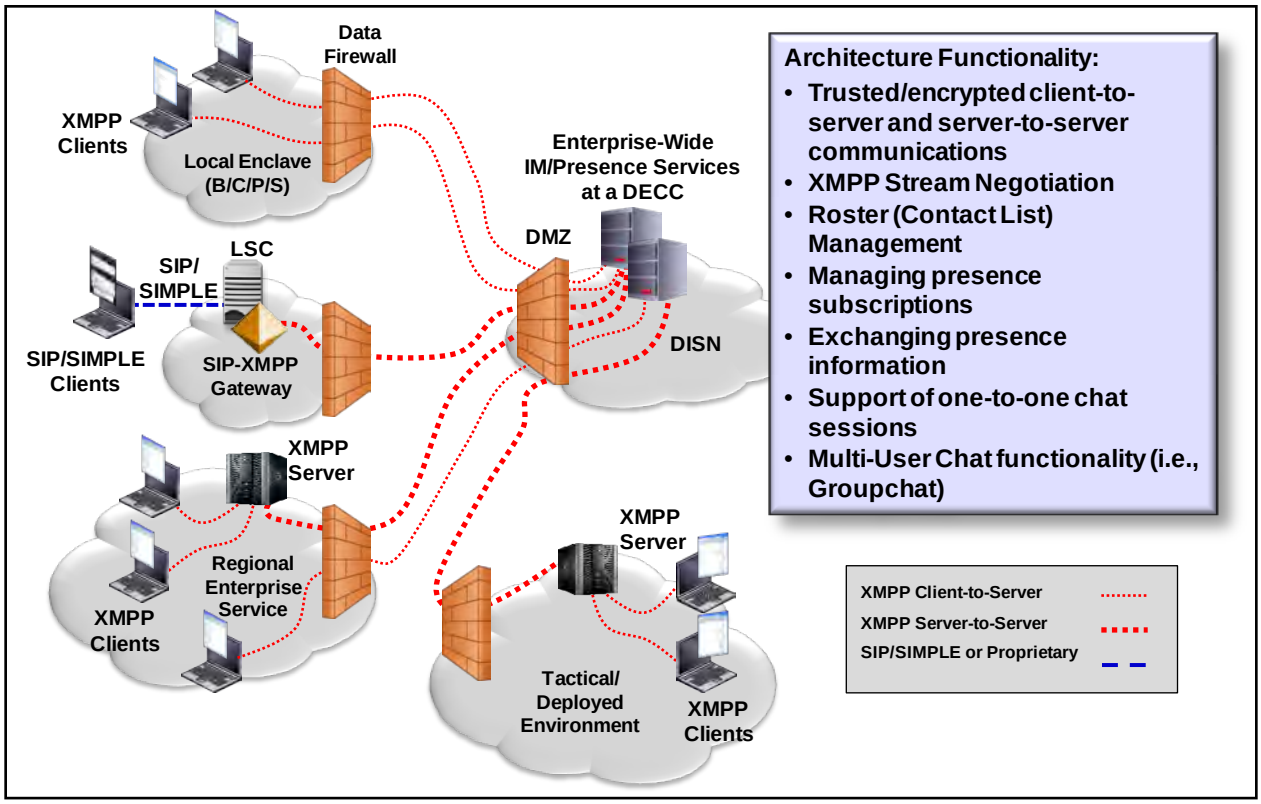


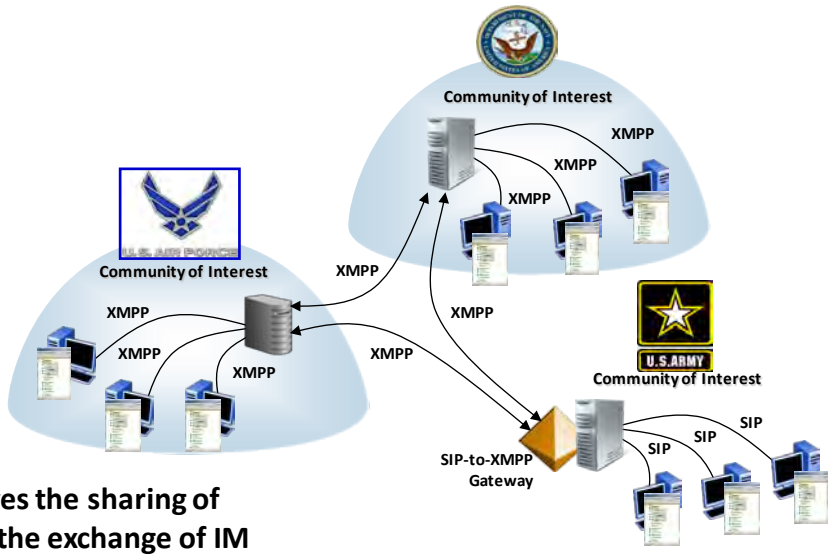
Figure 4.3.2.1-3. Multivendor Interoperability Normalized on XMPP

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 4.3.2.1-4, Interoperability/Federation of IM, Chat, and Presence, illustrates the following IM, Chat, and Presence demonstrations:

Demonstrate that the interoperability of IM/Chat & Presence can be achieved:

- **Within single vendor solutions.**
- **Within multivendor solutions.**
- **Using SIP-to-XMPP Gateways.**



- **Federation/Bridging involves the sharing of Presence information and the exchange of IM across multiple systems.**
- **Federation enables connectivity between otherwise isolated implementations allowing users who reside in different COIs to exchange IM/Chat/Presence using open, standards-based protocols and UCR 2008, Change 3, specifications.**

Figure 4.3.2.1-4. Interoperability/Federation of IM, Chat, and Presence

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

4.3.2.2 Integration of Voice, Video and Data Focused on Mobility

4.3.2.2.1 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 4.3.2.2-1, Mobile Warfighter's Communication Dilemma, shows the problem service portability is trying to solve.

Figure 4.3.2.2-1. Mobile Warfighter's Communication Dilemma

To achieve this objective, the UC framework 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. Figure 4.3.2.2-2, Single Number Portability, depicts an approach to single number portability, which supports subscriber mobility within a region.

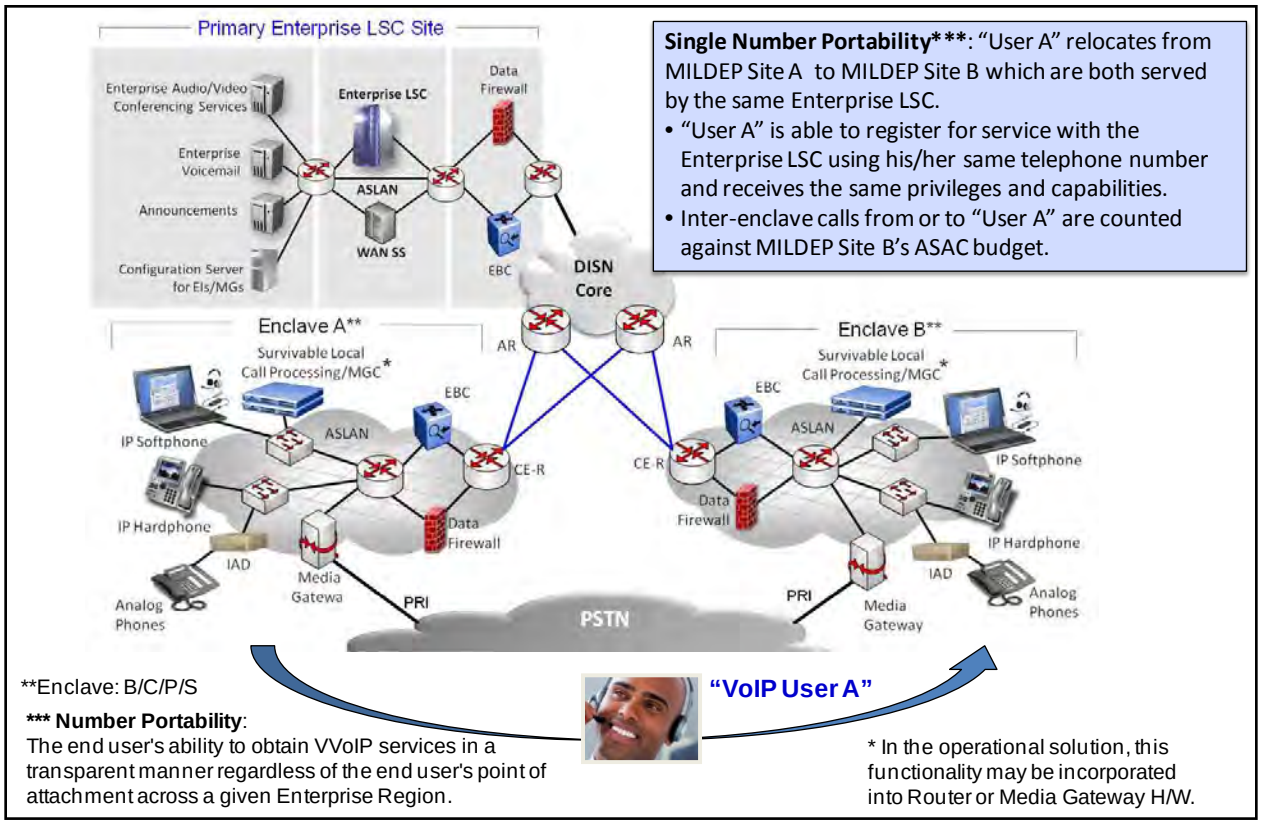


Figure 4.3.2.2-2. Single Number Portability

Figure 4.3.2.2-3, UC Mobility Between Regions, addresses the use of ELSCs to support UC Mobility. ELSCs intercommunicate via their co-located WAN SS. To support transparent user mobility between Regions, ELSCs would need to be able to exchange Subscriber Profile Data freely. Today, subscriber profile data is vendor specific. Therefore, the exchange of Subscriber Profile Data between ELSCs is not currently a viable option. Vendor End Instruments use proprietary protocols to interface between LSC and End Instrument. End Instrument movement would be limited to regions with the same vendor ELSC.

A near term approach would automate the process of populating specific user fields within a Subscriber's Profile using an add-on capability that permits the ELSC to import user attribute values from an external Enterprise Lightweight Directory Access Protocol (LDAP) directory into its embedded, local database and use AS-SIP end instruments when migrating between regions.

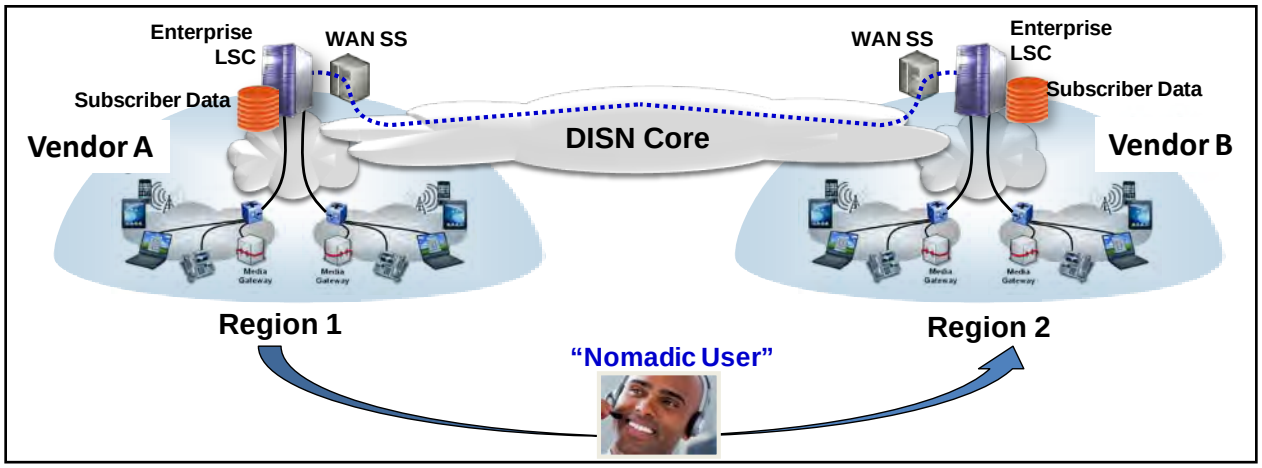


Figure 4.3.2.2-3. UC Mobility Between Regions

4.3.2.2.2 Multifunction Mobile Devices

Section 5.3.6 addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. A Multifunction Mobile Device (MMD) is defined as an advanced, yet highly portable computing platform that supports one or more compact input interfaces (e.g., touch screens, stylus, miniature keyboard) to facilitate user interaction. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. An MMD can assume any number of form factors including, but not limited to, a Smartphone, Personal Digital Assistant (PDA), or small form factor wireless tablet. The requirements for non-UC VVoIP-related functionality (such as e-mail or Web-browsing) provided by the MMDs are generally defined by DISA Field Security Office (FSO) STIGs.

The scenarios in which MMDs may be used for UNCLASSIFIED applications are currently grouped into two primary use cases. These are summarized in Table 4.3.2.2-1, Multifunction Mobile Device Use Cases. Additional UNCLASSIFIED use cases can also be defined (such as connectivity of MMDs to assured services UC VVoIP and collaboration systems), but these "sub use cases" will fall within one of these two primary use cases:

Table 4.3.2.2-1. Multifunction Mobile Device Use Cases

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	No Connectivity to DoD-Network and No Processing of Controlled Unclassified Information (CUI) data Use Case. No connectivity to DoD email	MMD that has no connectivity to a DoD network and processes only publicly available DoD "data" information ("Data" as defined in this context is clarified in the next section)

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#2	Full Connectivity to DoD network and Processing of sensitive UNCLASSIFIED Information Use Case	MMD that supports access to DoD networks either directly or via a secure tunnel established across public networks. Securely processes and stores DoD information at the CUI level

Mobile devices conforming to Use Case #2 are permitted to connect to DoD networks, transmit and receive sensitive information, and securely store the received information. The device may connect to the DoD network in a number of ways including direct access through a wired or wireless LAN connection, or indirect access by establishing a secure overlay across a carrier connection or via a DoD connected PC. To secure data in transit and store data at rest, use of National Institute of Standards and Technology Federal Information Processing Standard (NIST/ FIPS) approved cryptographic modules is required. In addition, all of the components that comprise this system are required to be fully STIG compliant from an Information Assurance standpoint.

Requirements for the Use Case #2 Multifunction Mobile Device platform itself are specified by the DISA FSO STIGs. Conformance of the multifunction mobile device platform to DISA FSO requirements is validated during testing by the appropriate DoD laboratory or in the field in accordance with the UCCO Process Guide and DoDI 8100.04. In addition, for more specialized applications, such as connectivity of the Multifunction Mobile Device to the DISN to directly obtain UC VVoIP and federated XMPP services, requirements to support this use case are specified in Section 5.3.6.

For Use Case #2, note that certain requirements are applicable to not only the MMD itself, but also the supporting infrastructure responsible for remote monitoring, remote management and provisioning of the device from a centralized enforcement point. The Mobile Device Backend Support System (MBSS) is a system which supports remote administration, monitoring, and secure enclave access for MMDs. For Use Case #1, the MBSS (if used) supports centralized management of MMDs via commercial networks and is not connected to DoD networks. For Use Case #2, the MBSS is located on the DoD network and plays a key role in ensuring DoD policy enforcement and providing secure DoD enclave access for MMD users. The MBSS also facilitates the use of only approved applications and services through the use of granular technical controls and centralized management consoles. The MBSS can take many forms and is highly vendor dependent; however, some of the common functions and features provided by the MBSS include remote data “wipe” functionality and remote patch remediation.

4.3.3 Hybrid Networks Design for UC

During the transition period, the hybrid network environment involving both the operational DSN and the evolving IP-based assured services network will require that voice and video services must be routed between the two different technology-based networks.

The following objectives for hybrid network operation have been defined:

- At the B/P/C/S level, full directory number (DN) portability is required as users transfer from a TDM-based EO to an IP-based edge solution within a local serving area.

- At the network (backbone) level, the quantity of end-to-end IP to TDM to IP conversion for calls shall be held to a minimum.

The rules defined here can be met by either using a network-level, 10-digit DN-based routing database (DB) (the RTS Routing DB described in Section 4.3.3.1, RTS Routing Database) or by a careful coordination of the DSN numbering plan assignments and the standard 6-digit DSN translation/routing tables.

The network-level, 10-digit DN routing DB will associate a 10-digit DN with the "technology type" of the called EI (e.g., IP or TDM instrument) and direct routing accordingly down to the specific switching system (EO or LSC) serving the individual EI.

4.3.3.1 RTS Routing Database

The RTS Routing DB is a DISA-owned and DISA-operated DB that contains records of the DSN numbers, commercial (PSTN) numbers, LSC identifiers, and WAN SS or MFSS identifiers for UC end users served by LSCs. This DB may also contain records of DSN numbers and commercial numbers for individual DSN end users served by DSN EOs and private branch exchanges (PBXs). The DB records may be populated automatically by LSCs, whenever end users' numbers are added to an LSC during activation of that end user on the LSC. The DB records also may be populated manually by a DISA craftsperson, using DSN and commercial number information from an LSC site or DSN EO or PBX site.

The WAN SSs and MFSSs that support the Hybrid Routing (HR) feature query the RTS Routing DB to determine whether there is an LSC identifier, a primary WAN SS or MFSS identifier, and a backup WAN SS or MFSS identifier stored there that matches the dialed DSN number on a UC call that enters the WAN SS or MFSS. Figure 4.3.3.1-1, Hybrid Routing Feature Operation in the Network, illustrates how the Hybrid Routing Feature operates in the network.

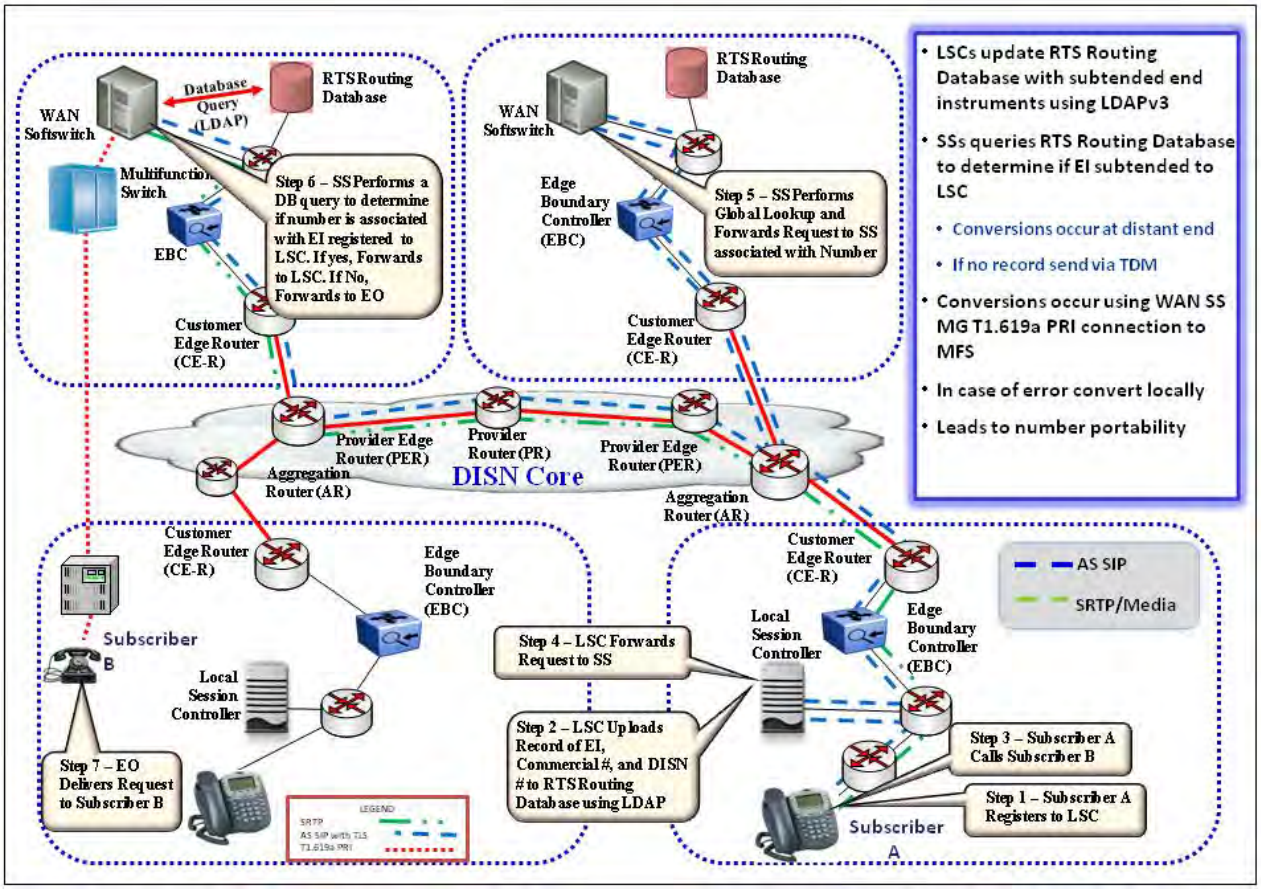


Figure 4.3.3.1-1. Hybrid Routing Feature Operation in the Network

The LSCs that support the Commercial Cost Avoidance feature query the RTS Routing DB to determine whether there is a DSN number stored there that matches the dialed commercial number on a commercial call from the LSC (e.g., a 9+9 call, or a 9+8 call). Figure 4.3.3.1-2, Commercial Cost Avoidance Feature Operation in the Network, depicts how the Commercial Cost Avoidance feature operates in the network.

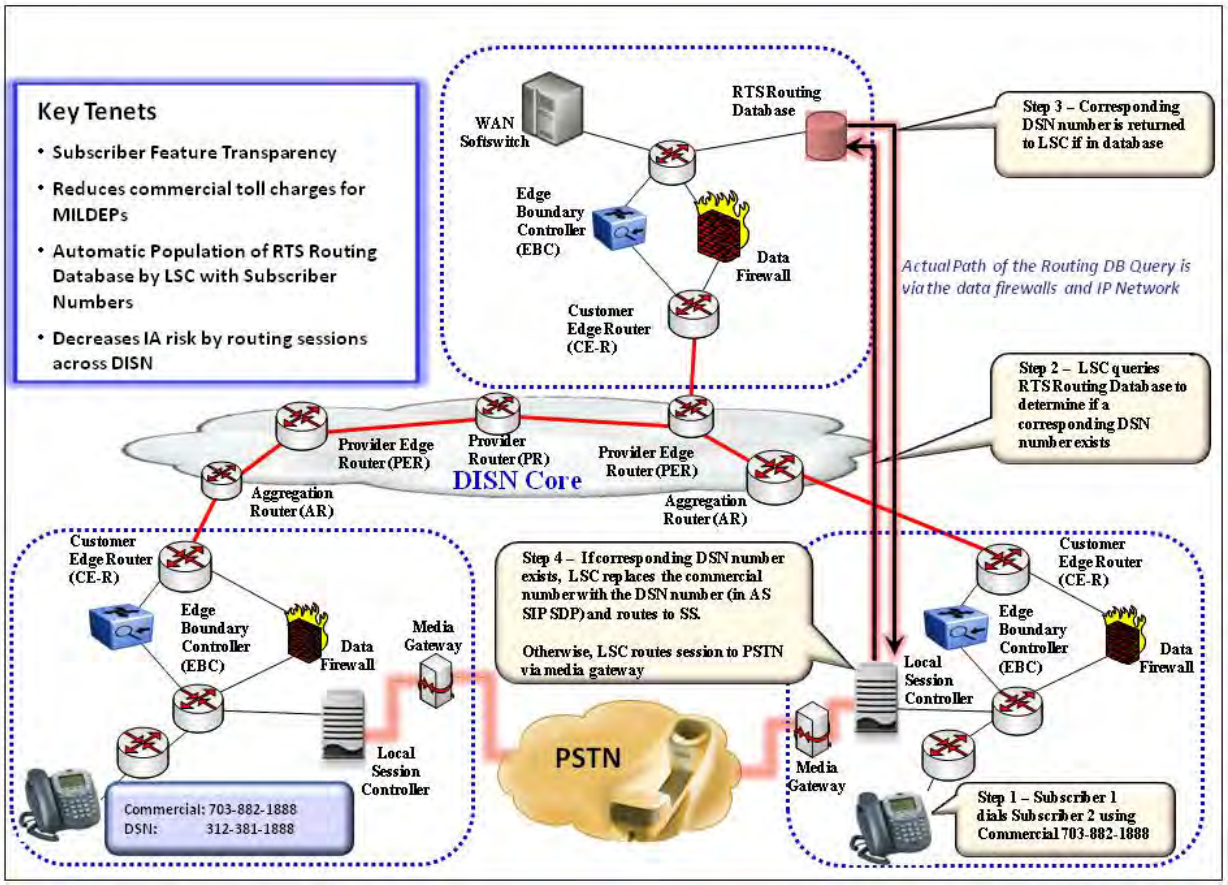


Figure 4.3.3.1-2. Commercial Cost Avoidance Feature Operation in the Network

The protocol that LSCs, MFSSs, and WAN SSs use to query and update the RTS Routing DB is LDAPv3, secured using Transport Layer Security (TLS), and signaled via IP over the DISN WAN.

4.3.4 Emergency Response Products

This section addresses two emergency response products that must be supported at DoD locations and must interface DoD UC products. These two systems are the E911 Management System and the Mass Notification Warning System.

Access to Enhanced 911 is available from LSC/Media Gateways using the dial plan. This interface is TDM due to information assurance requirements. E911 Management Systems interface with LSCs to provide reliable user locations to Public Safety Answering Points (PSAPs), including cases where DoD components host a PSAP for E911 services.

The Mass Notification Warning System will be used to meet DoD's requirements to provide Association of Public-Safety Communications Officials - International (APCO) Project 25

systems at DoD locations. The Mass Notification Warning System is a product that monitors event sources and if an event from an event source meets pre-defined emergency criteria then the default action is for the mass notification warning system (MNWS) to apprise system operators of the event. The operators qualify the event and when appropriate instructs the system to initiate alerts. The system then initiates alerts via interfaces to alert delivery systems.

Currently all local access to any public network such as PSTN service, E911 and Association of Public-Safety Communications Officials - International (APCO) Project 25 systems must be via TDM and cannot be transmitted over IP, because of information assurance requirements. The only connection to the PSTN is through a TDM interface using PRI or CAS signaling, so there is no interaction between the VVoIP system and commercial VVoIP IP networks. UCR Section 5.4.5.3 and Section 5.4.6.2 define this interface. Section 4.4.5, UC Gateways, includes future secure IP gateways to public non-DoD networks.

4.3.5 UC Gateways

As UC IP based products are deployed, a variety of gateways are necessary to interface non-DoD networks securely. These networks involve commercial public networks and Allied networks. Currently UC products will be employed in a variety of interfaces situations to non DoD networks as follows:

1. Centralized Secure Connection to Commercial Voice ISP, as illustrated in Figure 4.3.5-1.

2. Centralized Secure Connection to Wireless Carriers, as illustrated in Figure 4.3.5-2.

3. Allied Networks Interfaces, as illustrated in Figure 4.3.5-3.

4. Distributed “Authenticated/protected” UC Internet gateway to Trusted Voice/Video Networks (e.g., non-mission critical sites with no NIPR but with Internet Access to Centralized Connection to Commercial Voice Internet Service Providers Item 1 above.).

5. Access to Internet, unauthenticated, untrusted networks employing Analog as opposed to digital interfaces.

Figure 4.3.5-1, Centralized Secure Connection to Commercial Voice Internet Service Providers (ISP), depicts Centralized Secure Connection to Commercial Voice Internet Service Providers for allowing the user of an end instrument, in this case a softphone, to access the services provided by a Voice IP Service Provider (Voice ISP) from the MILDEP enclave. In this instance, session establishment and tear down signaling (the Assured Services Session Initiation Protocol) is transported through enclave EBCs to an enterprise LSC co-located with a WAN Softswitch.

The signaling is forwarded to the Voice ISP's network once the call is determined to be for a PSTN destination or a destination serviced exclusively by the Voice ISP's network. Media traffic is transmitted directly between EBCs across the DISN core. Within the IAP, the EBC fronting the Voice ISP's network converts the signaling and media traffic streams into a format supported by the Voice ISP's session border controller (SBC). It is anticipated that the interface between the commercial SBC and the EBC at the IAP will be a commercial variant of SIP and RTP.

The traffic between the SBC and the EBC in the IAP will be unencrypted, but authenticated, to allow monitoring and inspection by information assurance tools deployed at the IAP boundary.

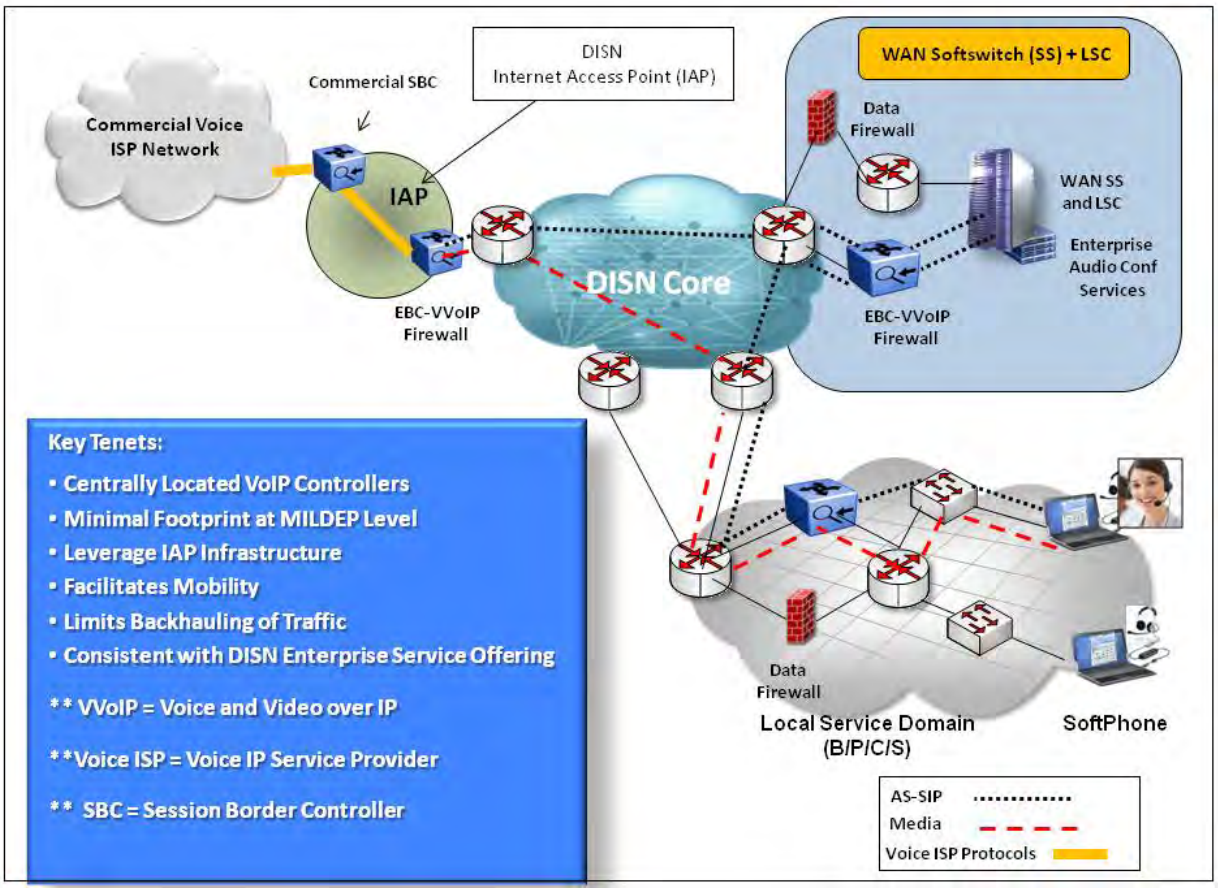


Figure 4.3.5-1. Centralized Secure Connection to Commercial Voice Internet Service Providers (ISPs)

Figure 4.3.5-2 illustrates "Centralized Secure Connection to Wireless Carriers". The multi-carrier entry point (MCEP) is a centralized access point for the wireless and cellular carriers to enter the DISN. DISA has several initiatives under way with the National Security Agency (NSA) and the carriers to increase support of mobility within the DoD by leveraging commercial wireless networks. The first effort is associated with the NSA Mobile Virtual Network Operator

(MVNO) "Fishbowl" effort, which is designed to replace the Secure Mobile Environment Portable Electronic Device (SME-PED) functionality as the SME-PED solution is phased out. The second effort is to allow MMD applications to be installed on commercial MMDs and to allow those devices (such as Smartphones) to be connected to the DISN in a secure approach that is endorsed by the STIGs and UCR. This aligns with Navy, Army, and Air Force initiatives to issue MMDs to warfighters as their primary end instrument. Finally, extension of the DISN to authorized commercial wireless and cellular end instruments, so they can transmit and receive DISN SBU voice sessions from their commercial wireless or cellular end instrument, is being assessed.

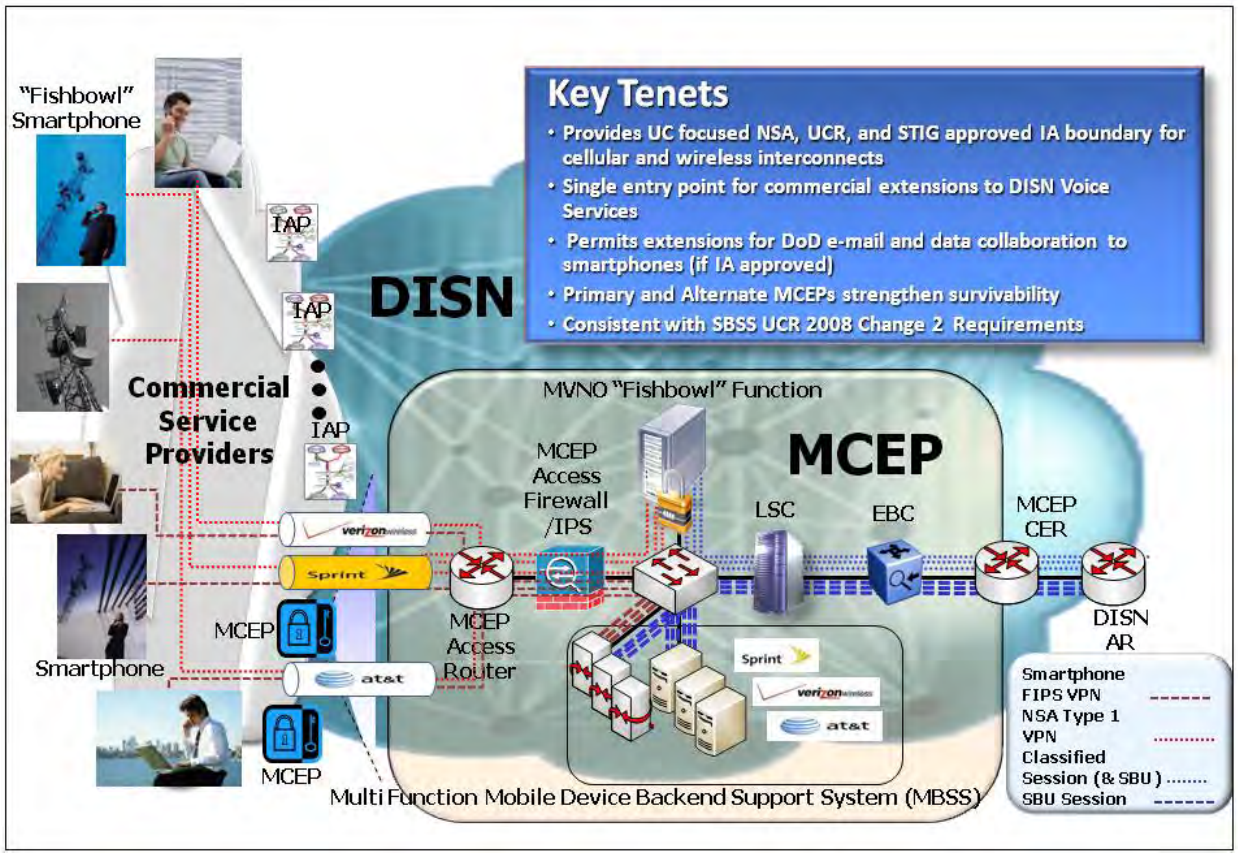


Figure 4.3.5-2. Centralized Secure Connection to Wireless Carriers

Figure 4.3.5-3, Allied Network Interfaces, provides a high-level illustration of an interface to Allied networks.

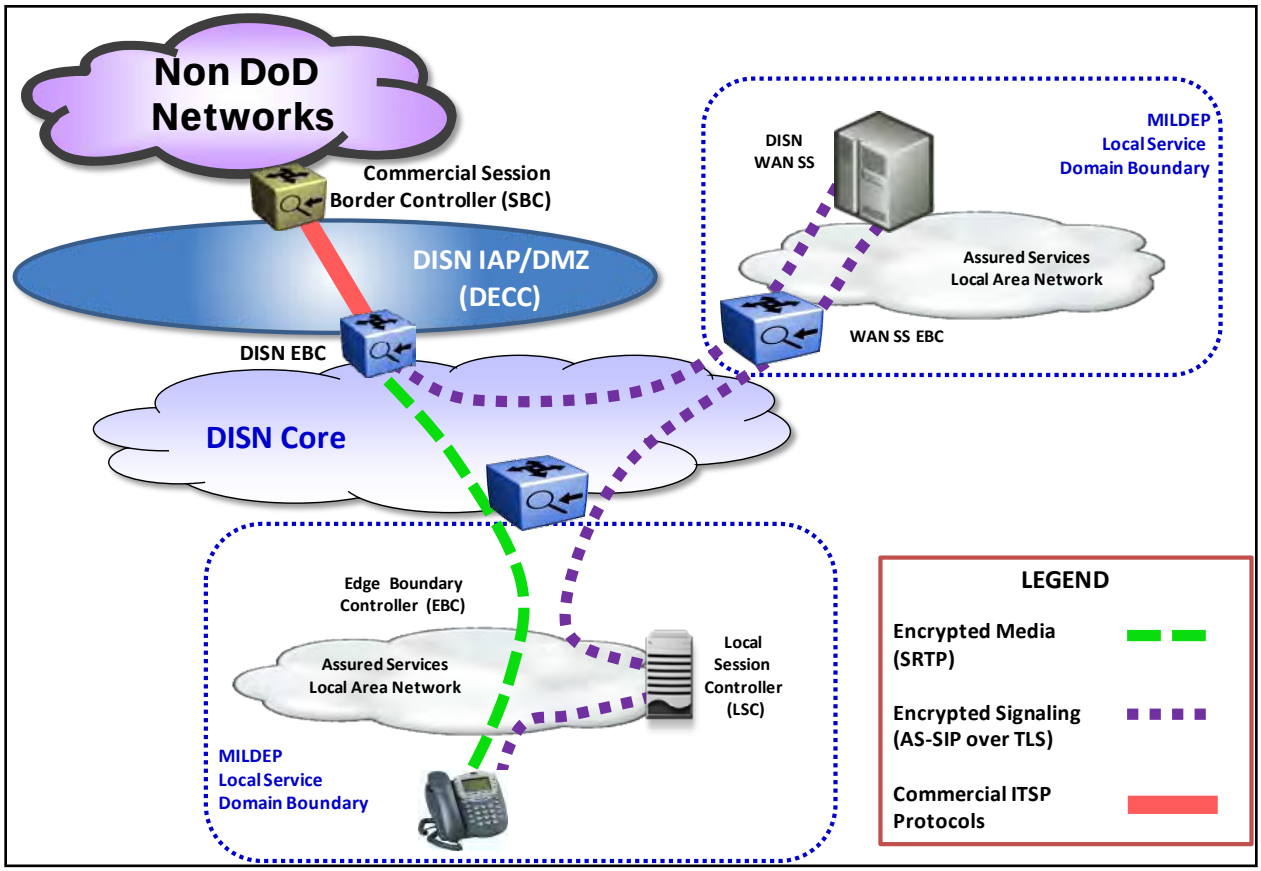


Figure 4.3.5-3. Allied Network Interfaces

4.4 UC APL PRODUCT TEST AND CERTIFICATION PROCESSES

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

4.4.1 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 (UC SG) advises the DoD CIO with respect to which product categories and products should appear in the UCR, and thus, on the APL. The APL products identified by the DoD CIO must be on the APL for DoD Components to acquire them. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless, and until, a waiver is approved. Products must also be granted a site Authority to

Operate (ATO) and be operated IAW appropriate STIGs to gain DISN Authority to Connect (ATC).

Figure 4.4.1-1, Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each UC product category would be found under their appropriate section of the UC APL. Many UC products would show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE Routers, EBCs, and ASLANs that can be used for both SBU and classified voice and video services.

The term appliance or appliance functions are used throughout the UCR as a generic term referring to a function or feature that may be part of a UC APL product.

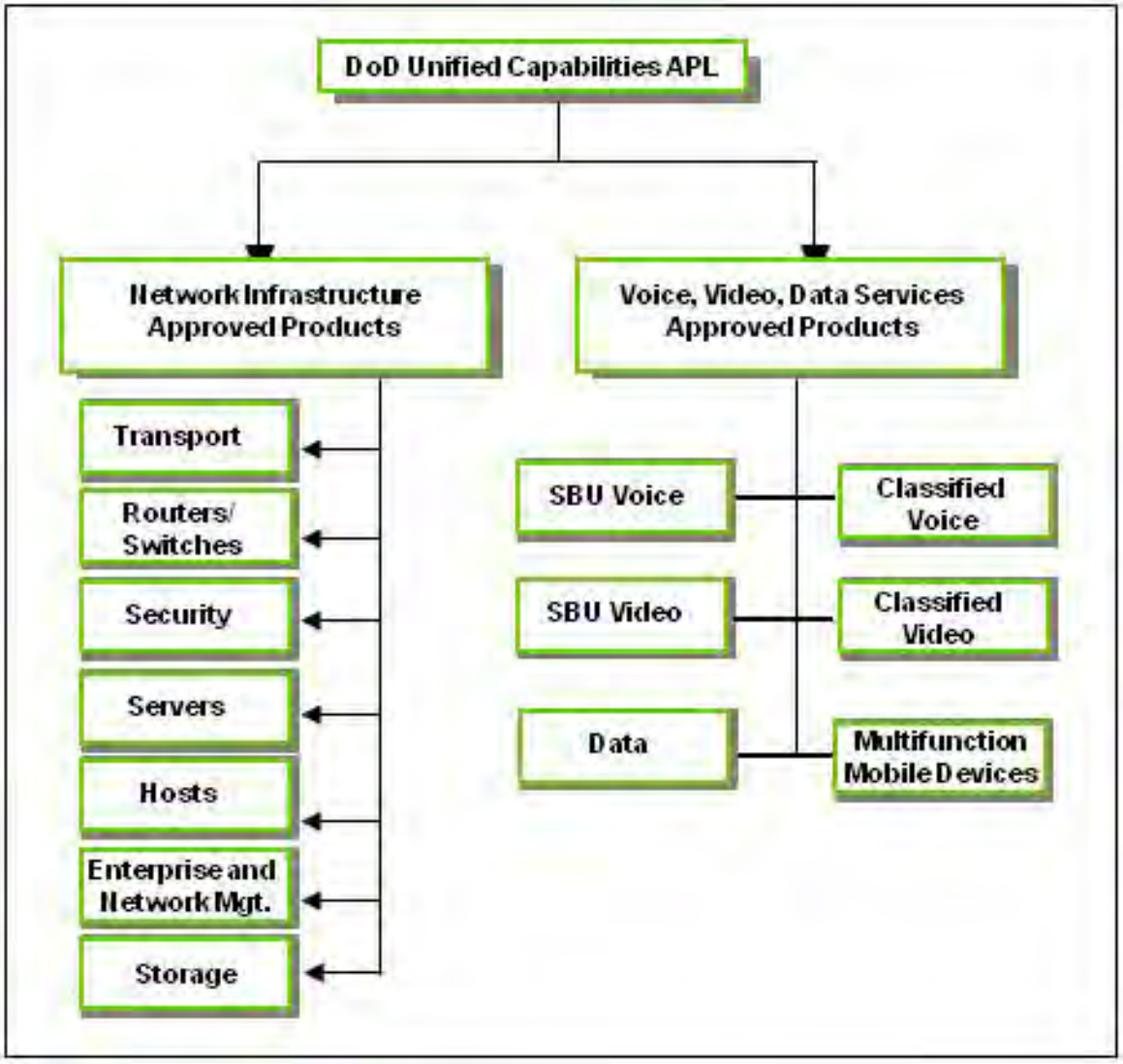


Figure 4.4.1-1. Overview of UC Product Categories within the DoD UC APL

4.4.1.1 Network Infrastructure Approved Products

Tables 4.4.1.1-1 through 4.4.1.1-5 within this section list the products for the following Network Infrastructure Approved Products categories:

- Transport
- Routers/Switches
- Security
- Enterprise and NM
- Storage
- Hosts*
- Servers*

*Currently, there are no UC products that the UC SG has approved for inclusion in the Host and Server categories.

Currently, Data-At-Rest products, Information Integrity (II)/Data Leakage, and High Assurance Internet Protocol Encryptor (HAIPE) discovery servers will not be included in this version of the UCR.

Table 4.4.1.1-1. Transport Appliances

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
MSPP	5.5 (Network Infrastructure Product Requirements)	Product that receives low-speed circuits on multiple ports and multiplexes them via TDM into a high-speed circuit, and transmits it to one of its high-speed ports
M13 Multiplexer	5.5 (Network Infrastructure Product Requirements)	Product that functionally multiplexes DS1s into a DS3
Serial TDM Multiplexer	5.5 (Network Infrastructure Product Requirements)	Product that multiplexes user serial synchronous and asynchronous data interfaces and 2-wire and 4-wire analog into one or more aggregated higher bandwidth network interface trunks
Timing and Synchronization	5.5 (Network Infrastructure Product Requirements)	Product consisting of modules that distribute precise timing and synchronization signals to network components
OTS	5.5 (Network Infrastructure Product Requirements)	Switching product providing high-speed optical transport in the DISN WAN

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
ODXC	5.5 (Network Infrastructure Product Requirements)	Product that is a cross-connect device located primarily at Class 1 sites but it could also be deployed at select Class 2 sites
Fixed NE	5.9 (Network Element Requirements)	Product that provides transport for bearer and signaling traffic in a Fixed network environment
Deployed NE	5.9 (Network Element Requirements)	Product that provides transport for bearer and signaling traffic in a deployed network environment

LEGEND

AGF	Access Grooming Functional	DS3	Digital Signal 3		
DISN	Defense Information System Network	NE	Network Element	TDM	Time Division Multiplexing
DS1	Digital Signal 1	OTS	Optical Transport System	WAN	Wide Area Network

Table 4.4.1.1-2. Router/Switches

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
DISN Router	5.5 (Network Infrastructure Product Requirements)	Product that provides IP routing within the DISN
OLT	5.3.1 (Assured Services Local Area Network Infrastructure)	Product that acts as a head-end device between a backbone network and the transport fiber in a PON deployment
ONT	5.3.1 (Assured Services Local Area Network Infrastructure)	Product that provides interface between end user devices and the transport fiber in a PON deployment
DSL Access Device	5.3.1 (Assured Services Local Area Network Infrastructure)	Product used to allow transport of high-bandwidth data, such as multimedia and video, between endpoints using existing twisted pair telephone lines
DSL Repeater	5.3.1 (Assured Services Local Area Network Infrastructure)	Product used to amplify DSL signals where required to drive the signal over a DSL transport link
DSLAM	5.3.1 (Assured Services Local Area Network Infrastructure)	Product that functions as a concentrator for multiple endpoints including Analog Voice and VoIP services to be transported over existing voice-grade copper links
Access IP Switch	5.3.1 (Assured Services Local Area Network Infrastructure)	Product used in a LAN to provide end-device access to the LAN
Distribution IP Switch	5.3.1 (Assured Services Local Area Network Infrastructure)	Product used in a LAN to provide an intermediate switching layer between LAN access and core layers
Core IP Switch	5.3.1 (Assured Services Local Area Network Infrastructure)	Product providing high-speed IP switching at the LAN core layer
Wireless LAN Equipment	5.3.1 (Assured Services Local Area Network Infrastructure)	Products used in wireless LANs: Wireless EI, Wireless LAN Access System, Wireless Access Bridges

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION

LEGEND

DISN	Defense Information System Agency	IP	Internet Protocol	PE	Provider Edge
DSL	Digital Subscriber Line	LAN	Local Area Network	WAN	Wide Area Network
EI	End Instrument				

Table 4.4.1.1-3. Security Devices

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
EBC	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	A product that provides firewall functions for voice traffic (also listed under voice products)
Data Firewall	5.8 (Security Devices Requirements)	A product that blocks unauthorized access while permitting authorized communications
VPN Concentrator	5.8 (Security Devices Requirements)	A product that sets up a secure link between an end user and an internal network
IPS	5.8 (Security Devices Requirements)	A product that detects unwanted attempts at accessing, manipulating, and/or disabling a computer system.
HAIPE	5.6 (Generic Encryption Device Requirements)	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 Encryptor	5.6 (Generic Encryption Device Requirements)	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
Integrated Security Solution	5.8 (Security Devices Requirements)	A product that provides the functionality of more than one information assurance device in one integrated device
Information Assurance Tools	5.8 (Security Devices Requirements)	Products that provide information assurance functions
Network Access Control	5.8 (Security Devices Requirements)	Products that provide information assurance functions

LEGEND

EBC	Edge Boundary Controller	IP	Internet Protocol	IPv6	Internet Protocol Version 6
HAIPE	High Assurance Internet Protocol Encryptor	IPS	Intrusion Protection System	NE	Network Element
		IPv4	Internet Protocol Version 4	NSA	National Security Agency
INFOSEC	Information Security			VPN	Virtual Private Network

Table 4.4.1.1-4. Enterprise and Network Management

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Element Management System	5.11 (Enterprise and Network Management Systems)	For monitoring FCAPS and command elements (products operating in a network)
Operational Support Systems	5.11 (Enterprise and Network Management Systems)	Manager of element managers for FCAPS and for information sharing
LEGEND FCAPS Fault, Configuration, Accounting, Performance, and Security		

Table 4.4.1.1-5. Storage

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Data Storage Controller	5.10 (Data Storage Controller)	Specialized multiprotocol computer system with an attached disk array that together serves in the role of a disk array controller and end-node in B/P/C/S networks
LEGEND B/P/C/S Base, Post, Camp, Station		

4.4.1.2 Voice, Video, and Data Services Approved Products

Table 4.4.1.2-1, SBU Voice, lists the products in the SBU UC Voice Product category.

Table 4.4.1.2-1. SBU Voice

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
LSC	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that provides many local telephony (UC) functions
MFSS	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Large, complex product that provides many local and WAN-related telephony functions
WAN SS	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	A product that acts as an AS-SIP B2BUA within the UC framework. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS
AEI		EI using AS-SIP signaling.

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
RTS Routing Database	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that provides commercial cost avoidance routing and hybrid call routing translations at the network level
EBC	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	A product that provides firewall functions for voice traffic (also listed in Table 4.4.1.1-3, Security Devices)
AS-SIP-to-TDM Gateway	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that provides interworking between AS-SIP, IP bearer, and TDM signaling and bearer
AS-SIP-to-IP Gateway	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that provides interworking between AS-SIP and proprietary UC appliance signaling
RSF	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that acts as a firewall protecting an LSC or SS
UC Conference Bridge	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that provides voice conferencing capabilities
Mass Notification Warning System	5.3.2.33	Product that provides dissemination of alert notifications to target authorized subscribers
E911 Management System		Product that interfaces with LSCs to provide reliable user locations to Public Safety Answering Points (PSAPs)

LEGEND

AEI	AS-SIP End Instrument	IA	Information Assurance	RSF	RTS Stateful Firewall
AS	Assured Services	IP	Internet Protocol	RTS	Real Time Services
AS-SIP	Assured Services Session Initiation Protocol	IPv6	Internet Protocol Version 6	SS	Softswitch
		LSC	Local Session Controller	TDM	Time Division Multiplexing
B2BUA	Back-to-Back User Agent	MFSS	Multifunction Softswitch	UC	Unified Capabilities
EBC	Edge Boundary Controller				

Table 4.4.1.2-2, Classified Voice, lists the products in the classified UC voice product category.

Table 4.4.1.2-2. Classified Voice

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
LSC	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements) 6.2 (Unique Classified Unified Capabilities Requirements)	Same product as in Table 4.4.1.2-1, SBU Voice
Dual Signaling SS	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements) 6.2 (Unique Classified Unified Capabilities Requirements)	Unique to Classified
AEI	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements) 6.2 (Unique Classified Unified Capabilities Requirements)	Unique to Classified

LEGEND

AEI	AS-SIP End Instrument	IPv6	Internet Protocol Version 6	SBU	Sensitive But Unclassified
AS	Assured Services	LSC	Local Session Controller	SS	Softswitch
AS-SIP	Assured Services Session Initiation Protocol				

Table 4.4.1.2-3, SBU Video, lists the products in the SBU UC video product category.

Table 4.4.1.2-3. SBU Video

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
LSC	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Same product as in Table 4.4.1.2-1, SBU Voice
MFSS	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Same product as in Table 4.4.1.2-1, SBU Voice

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
WAN SS	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Same product as in, Table 4.4.1.2-1, SBU Voice
AEI	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Unique to Video
AS-SIP to H.323 Video Conferencing Gateway	5.3.2 (Assured Services Requirements) 5.3.4 (AS-SIP Requirements) 5.3.5 (IPv6 Requirements) 5.4 (Information Assurance Requirements)	Product that allows interoperability between the DVS-G MCU and AS-SIP-based VTC
UC Conference Bridge	Same as above	Stand-Alone product with AS-SIP Required and H.323/H.320 Conditional
UC Conference Bridge Internal to LSC	Same as above	LSC product that includes internal conferencing capabilities; AS-SIP Required, H.323/H.320 Conditional

LEGEND

AEI	AS-SIP End Instrument	IPv6	Internet Protocol Version 6	SBU	Sensitive But Unclassified
AS	Assured Services	LSC	Local Session Controller	SS	Softswitch
AS-SIP	Assured Services Session Initiation Protocol	MCU	Multipoint Conferencing Unit	UC	Unified Capabilities
		MFSS	Multifunction Softswitch	VTC	Video Teleconferencing
DVS-G	DISN Video Services-Global			WAN	Wide Area Network

Table 4.4.1.2-4, Classified Voice, lists the products in Classified UC Video Product Category.

Table 4.4.1.2-4. Classified Video

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
LSC	6.2 (Unique Classified Unified Capabilities Requirements)	Same product as in Table 4.4.1.2-1, SBU Voice
Dual Signaling SS	6.2 (Unique Classified Unified Capabilities Requirements)	Unique to Classified
AEI	6.2 (Unique Classified Unified Capabilities Requirements)	Unique to Video and Classified
Multi-Signaling MCU	6.2 (Unique Classified Unified Capabilities Requirements)	Unique to Video

LEGEND

AEI	AS-SIP End Instrument	LSC	Local Session Controller	SBU	Sensitive But Unclassified
AS-SIP	Assured Services Session Initiation Protocol	MCU	Multipoint Conferencing Unit	SS	Softswitch

4.4.1.3 Data Category Approved Products

Data Category Products can include various combinations of the following data applications:

- E-mail/calendaring
- Unified messaging
- Web conferencing and web collaboration
- Unified conferencing
- IM and chat
- Rich presence

These data applications are features of UC Tool Suites and are considered to be data UC products. In addition, these data applications can be network aware to get enhanced QoS treatment on DoD networks. In these cases, the interface is specified for interoperability but the performance (e.g., response time, screen refresh rate) of the applications is not currently specified. These UC Tool Suites can be integrated with voice and video services to get assured services as well as QoS. Examples would be LSCs that include voice, video, and XMPP functionality as well as unified messaging. Table 4.4.1.3-1, Data Category Products, lists the data category products.

Table 4.4.1.3-1. Data Category Products

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
UC Tool Suite with specific features identified (XMPP Server, XMPP Client)	5.7 (Instant Messaging, Chat, and Presence/Awareness)	Integrated voice, video, and data services that operate at various security levels over a handheld device with wireless secure connectivity to the network or a desktop device with secure connectivity to the network
LEGEND UC Unified Capabilities XMPP Extensible Messaging and Presence Protocol		

4.4.1.4 Multifunction Mobile Devices Products

The UC APL now includes the “Multifunction Mobile Devices” High-Level product category. The types of products placed into this product category include not only the Multifunction Mobile Devices themselves (for example Smartphones, personal digital assistants, wireless

tablets, etc.) but also the supporting infrastructure that provides services such as remote management, authentication, and secure enclave network access.

The requirements for the non-UC VVoIP-related functionality (e.g., e-mail, Web browsing) provided by the Multifunction Mobile Devices category are defined within DISA FSO STIGs, STIG checklists, and security requirements matrices. The UC VVoIP-related requirements for Multifunction Mobile Devices that provide UC VVoIP-related functions, such as the ability to establish calls through an LSC or SS, are addressed in the UCR. Section 5.4, Information Assurance Requirements, defines the requirements for the "UC Multifunction Mobile Devices Applications," which provide UC VVoIP functionality.

Multifunction Mobile Devices that have access to DoD networks also require support from appliances and systems located at protected DoD installations, that provide application services, access control, and remote management. The implementation of these supporting services and infrastructures vary greatly from vendor to vendor, however, the UCR uses the generic term "Multifunction Mobile Devices Backend Support System" or "MBSS" to represent the appliances that allow Multifunction Mobile Devices connectivity and reachback to the enclave. As with Multifunction Mobile Devices themselves, non-UC-related functions of the MBSS (e.g., e-mail, web browsing) are defined by the appropriate DISA FSO STIGs. If the MBSS provides UC VVoIP functionality, this is addressed in Section 5.4, Information Assurance Requirements. During DoD Laboratory testing, the Multifunction Mobile Device and its associated MBSS are treated as a single system under test (SUT). Also, the LSC or SS/MFSS, at a minimum, will also be included in the SUT if the MBSS provides UC VVoIP capabilities.

Currently, only security requirements, rather than functional requirements, are specified for Multifunction Mobile Devices in this UCR. Table 4.4.1.4-1, Multifunction Mobile Devices, summarizes the Multifunction Mobile Devices category of the DoD UC APL.

Table 4.4.1.4-1. Multifunction Mobile Devices

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Multifunction Mobile Devices	5.4 (Information Assurance Requirements)	Advanced mobile computing platform that provides wireless connectivity, basic telephony functions, and portable computing capabilities. The device may also provide UC VVoIP-related services
Multifunction Mobile Devices Backend Support System (MBSS)	5.4 (Information Assurance Requirements)	An appliance or collection of appliances that allows remotely connected Multifunction Mobile Devices to access services within a DoD enclave, provides access control and remote management, while maintaining or enhancing the security posture of the network

4.4.1.5 Deployable UC Products

Table 4.4.1.5-1, Deployable UC Products and Paragraph References, delineates the deployable UC products. These products are based on configuring and installing UC products in a deployed, tactical environment. Table 4.4.1.5-1 does not list "legacy" deployable products that are found in UCR 2008.

Table 4.4.1.5-1. Deployable UC Products and Paragraph References

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	6.1.2 (Circuit-Based-Deployable Components)	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 (T-NE Requirements)	NEs used in deployed situations
Deployable LANs	5.3.1 (Assured Services Local Area Network Infrastructure) 6.1.5 (Deployed LANs)	LAN used in deployed situations
Deployed Tactical Radio	6.1.7 (Deployed Tactical Radio Requirements	Deployable radio systems used in deployed situations
DCVX	6.1.6 (DCVX System Requirements)	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
DCVX Deployed Cellular Voice Exchange
DVX-C Deployable Voice Exchange – COTS
LAN Local Area Network
NE Network Element

4.4.2 UC Distributed Testing

The objective of distributed testing is to leverage existing DoD Component test and evaluation capabilities and activities that already support DoD testing of products that support UC. Policy, roles and responsibilities, and procedures for the distributed test concept are contained in DoDI 8100.04.

DISA shall employ a distributed test capability that includes test and certification of voice, video, and/or data products to accommodate the expanded scope of the UCR, and to keep pace with emerging technology and the large demand from the DoD Components for interoperable and secure products. The precepts of the distributed test program are to "test once for many," create a single UC APL for use by the DoD Components in acquisitions and procurements, and more effectively integrate industry into the test and certification process. Additionally, distributed

testing will facilitate more timely delivery of emerging UC technologies to the warfighter. The CONOPS for distributed testing is illustrated in Figure 4.4.2-1, Distributed Testing CONOPS.

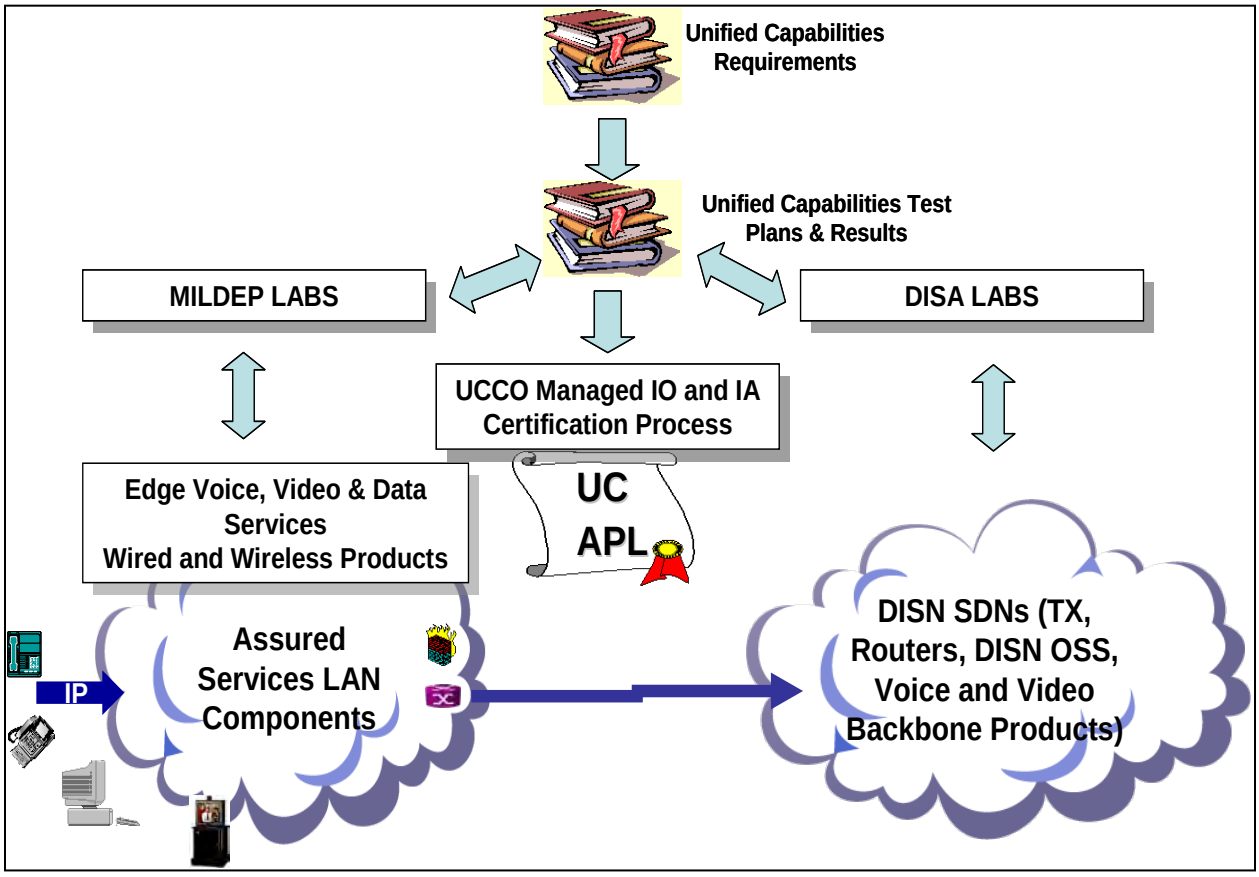


Figure 4.4.2-1. Distributed Testing CONOPS

Only product categories approved by the UC SG for inclusion in the UCR shall be tested and certified for inclusion on the UC APL. The level of testing required shall be guided by the requirements shown in Table 4.4.2-1, UC Test Requirements. The Director, DISA, in coordination with the DoD CIO shall resolve issues in interpretation and use of this table.

Table 4.4.2-1. UC Test Requirements

SERVICES COMPLEXITY	TECHNOLOGY MATURITY			
	PROTOTYPE	**PRE-PRODUCTION**	**APL READY**	**POST APL**
ASFs	• Full Test • Or incremental test and/or desktop review (DTR) if based on previously tested product	• Full Test • Or incremental test and/or DTR if based on previously tested product	• Full Test • Or incremental test and/or DTR if based on previously tested product	• Full Test for new software versions or significant Information Assurance-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product
Non ASFs Affecting ASFs	• 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 assured services features meeting brochure claims	• 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	• 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	• Partial test • Full test of interaction of features for new software versions or significant Information Assurance-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	• Random test of potential interactions	• Random test of potential interactions	• No test • Vendor LOC of vendor tests of features meeting brochure claims	• No test • Vendor LOC of vendor tests of features meeting brochure claims

LEGEND
AP Approved Products List ASF Assured Services Features DTR Desk-Top-Review LOC Letter of Compliance

4.4.3 Unified Capabilities Certification Office Processes

This section provides an overview of the UC approved products Unified Capabilities Connection Office (UCCO) processes.

This process is defined for mature products (APL and post-APL) and for technology insertion products (prototype and preproduction) that are evaluated via assessment testing in DoD test labs and validated for NetOps via Spirals that deploy capabilities. Table 4.4.2-1, UC Test Requirements, in Section 4.4.2, UC Distributed Testing, identifies three categories of Service Complexity and four categories of Technology Maturity for use in the determination of the type of UC APL process to be employed for a specific product. The matrix is used to determine which technologies need technology insertion assessment testing and DISN UC Spiral Deployment validations (i.e., Service Complexity: assured and affecting assured services; and technology maturity: prototype and preproduction) and which are ready for mature product approval testing (i.e., Service Complexity: assured or affecting assured services; and technology maturity: APL or post-APL). 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. The process for mature products is the UC APL process described in the subsequent section.

4.4.3.1 Standard Process for Gaining UC APL Status

The standard process for gaining APL status for all UC products is shown in Figure 4.4.3-1, Standard UC APL Product Certification Process. This process reflects that both interoperability and information assurance certifications are required for placement on the UC APL.

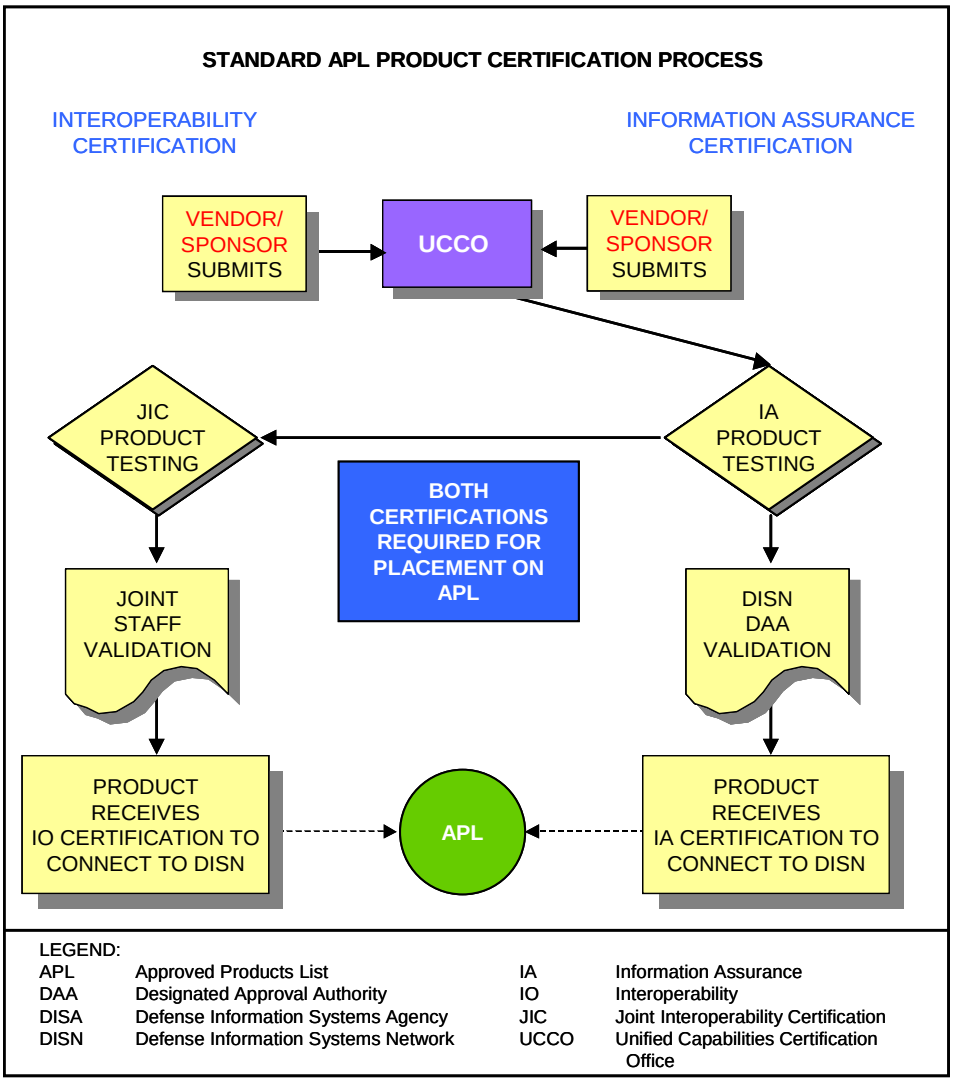


Figure 4.4.3-1. Standard UC APL Product Certification Process

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

- Circuit-switched/TDM products will no longer be tested for APL status. Once their existing 3-year APL status expires, they will be placed on the retired APL list. The products will continue to be allowed to operate in the network. Exceptions to this policy will be submitted through the appropriate channels for DoD CIO consideration. Circuit-switched/TDM product details are described in UCR 2008 for operational purposes only.

- A product enters the UC APL process by obtaining DoD Component sponsorship and providing both interoperability and information assurance information as shown in Figure 4.4.3-1.

- 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".

- 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 five dispositions will occur as follows:

- The vendors will have 18 months to develop the requirement if it is new and not previously available. Vendors may provide it earlier

- If the requirement has been lessened, vendor compliance is immediate

- If warning of the requirements has been given before approval, the requirement compliance may be immediate

- If the requirement addresses a Critical or Major information assurance risk, compliance is immediate

- If the requirement is necessary for multivendor interoperability, compliance is immediate

The 18-month period for development applies to a new feature or 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 4.4.3-1, New Features and Products in UCR 2008, Change 3, for which the 18-month rule applies.

Table 4.4.3-1. New Features and Products in UCR 2008, Change 3, for which the 18-Month Rule Applies

FEATURES	SECTION OF THE UCR
Smartphone	4.3.2.2.2
Commercial Cost Avoidance	5.3.2.23
MSMCU	4.4.1.4
XMPP servers	5.3.2.24
XMPP Client	5.7
Information Assurance Requirements Overlay for IM/Chat/Presence Awareness	5.3.5
LEGEND IM Instant Messaging MSMCU XMPP Extensible Messaging and Presence Protocol	

UCR Section 5.8, Security Devices, has been updated to add new information assurance products for Integrated Security Solutions and Information Assurance Tools. The 18-month rule does not apply to these products.

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

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 SG 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 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 SG

Three categories of FT products are as follows:

- Products within Current UCR Product Categories. Products that were tested by Joint Interoperability Test Command (JITC) before development of the product category or products that have existing requirements similar to those in the UCR that can be augmented with UCR requirements

- Operationally Validated. Products that are currently operating in DoD networks that have an Interim Authority to Operate (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)

- 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 SG

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/library/files/disn_cap_04272011.pdf

4.4.3.2 Waivers to DoD UCR Specifications Leading to Certification

1. The following applies to all DoD Components, sponsors, and/or fielding authorities seeking to place UC products on the DoD UC APL and field that product without meeting

all applicable technical requirements for respective product categories contained in the DoD UCR:

a. DoD Components shall comply with functional requirements, performance objectives, and technical specifications for DoD networks that support UC, as specified in the UCR.

b. Waivers may be granted to accommodate the introduction of new or emerging technology, pilot programs, or to accommodate critical operational requirements for specific limited fielding when validated by the DoD Component concerned, coordinated with, and recommended by the DISA (NS2), and approved by DoD CIO.

c. Only the DoD CIO, in coordination with DISA (NS) and DISA (JITC), may revise or waive requirements of the UCR.

d. Waivers to UC policy and the UCR shall not normally be granted for a period of more than 1 year. Only in exceptional circumstances, and with DoD CIO approval, shall extensions of waivers be granted. Vendors who do not implement corrective actions/mitigations to resolve waived requirements within the waived period (e.g., 1 year), are subject to having affected product removed from the APL. DISA shall maintain a database to track the status of granted waivers.

2. To certify and place products on the UC APL without meeting all applicable functional requirements, performance objectives, and technical specifications for respective product categories contained in the UCR, the following process shall be adhered to:

a. DISA (JITC) shall analyze interoperability test results with all parties concerned, and provide certification recommendations, as appropriate, for UC products seeking to attain DoD UC APL status, and provide the following to the DoD sponsoring agency/fielding authority, DISA (NS2), and DoD CIO:

(1) Results of Testing and Evaluation

(2) An assessment of the operational impact of UCR requirements not met for the respective product category.

b. If the DoD Component/sponsoring agency/fielding authority desires to field the UC product with the UCR deficiencies identified during Test and Evaluation (T&E), then the DoD Component/sponsoring agency/fielding authority shall submit a UCR Certification Waiver Request to DISA (NS2) and DoD CIO.

c. DISA (NS2) shall review the results of T&E, operational impact assessment, and DoD Component Waiver Request; and provide a recommendation on waiver of requirements contained in the UCR to DoD CIO.

d. DoD CIO shall review the DISA (JITC) assessment and DISA (NS2) recommendation, and make the final waiver/adjudication decisions leading to DISA (JITC) certification.

3. Final decision for certification and placement of the UC product on the UC APL shall be made by DoD CIO, in conjunction with DISA (NS2) and DISA (JITC).