Department of Defense

Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)

Final

December 2010

The Office of the Assistant Secretary of Defense

for

Networks and Information Integration / DoD Chief Information Officer

DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2008, CHANGE 2 (UCR 2008, CHANGE 2)

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.

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

DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2008 (UCR 2008)

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

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

DISTRIBUTION STATEMENT A:
Approved for public release; distribution is unlimited.

Approved by: _____

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

Dated: 1/22/09

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 1
PURPOSE

1.1 The "Department of Defense Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)" (hereinafter referred to as "UCR 2008, Change 2"), 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 1.

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 IA 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, 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 IA 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 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 UCR REQUIREMENT FRAMEWORK

This section provides a broad overview of requirements that establish the direction to be followed in the UCR. The overview is focused on requirements for DoD Components' planning, investment, development, acquisition, operations, and management of DoD networks that provide UC.

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

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.

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

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

- Dynamic formation of communities of interest (COIs) 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, Requirements Framework for UC Migration and Technology Insertions, illustrates the relationships among the documents that provide the requirements framework for UC migration and technology insertions.

There are three key Assistant Secretary of Defense for Networks & Information Integration/DoD Chief Information Officer ((ASD(NII)/DoD CIO) documents that drive UC implementation. The first is DoDI 8100.04, "DoD Unified Capabilities," which defines UC for the DoD, establishes policy, assigns responsibilities, and provides procedures for test; certification; acquisition, procurement, or lease; effective, efficient, and economical transport; connection and operation of DoD networks to provide UC; and establishment of the governing policy for UC products and services supported on DoD networks.

The second document is the "Department of Defense Unified Capabilities Requirements," which 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.

The third document is the "Unified Capabilities Master Plan," which will define the migration strategy to converged, net-centric, IP-based voice, video, and/or data services, and serve as a guideline to the DoD Components in the preparation of migration plans and acquisition plans for phasing in voice and video over IP services and other UC that will operate in converged voice, video, and/or data networks.

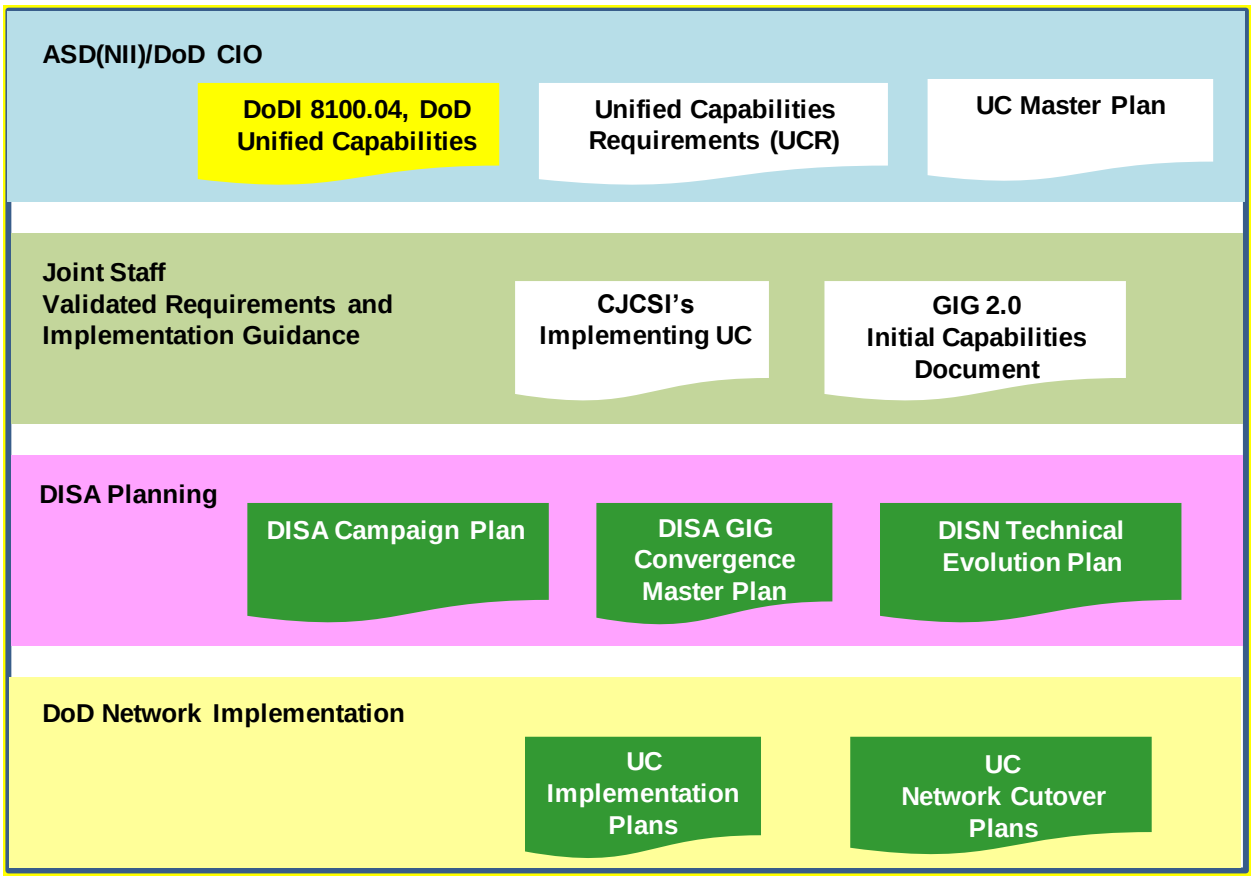


Figure 3-1. Requirements Framework for UC Migration and Technology Insertions

The Joint Staff will publish appropriate implementing instructions for UC. Global Information Grid 2.0 (GIG 2.0) has been initiated to meet warfighter requirements across the range of military operations. The GIG 2.0 transforms the current understanding of the GIG from a federated set of systems, processes, governance, and control to a unified and integrated net-centric environment. To support this transformation the "Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD)" (hereafter referred to as "GIG 2.0 ICD") (as approved in Joint Requirements Oversight Council Memorandum (JROCM) 095-09, dated 1 June 2009) is an overarching document identifying desired capabilities for the future of the GIG. The GIG 2.0 is envisioned to fulfill the global requirements of the Combatant Command/Service/Agency (CC/S/A) communities and serves as a platform to implement the DoD Information Enterprise (IE). The GIG 2.0 provides capabilities to all operating locations (bases, posts, camps, stations (B/P/C/Ss), facilities, mobile platforms, and deployed sites), and includes providing interfaces to coalition and mission partners, allies, and non-DoD users and systems. The GIG 2.0 will facilitate mission support emanating from joint bases in support of the warfighter. The GIG 2.0 also encompasses communications paths, such as MILSATCOM (Military Satellite Communication), commercial SATCOM, and terrestrial gateway. The five GIG 2.0 ICD critical characteristics that must be met by UC migration are Global Authentication, Access Control, and Directory Services; Information and Services "from the Edge;" Joint Infrastructure; Common

Policies and Standards; and Unity of Command. The five GIG 2.0 critical characteristics with the UC initiatives addressing them in parentheses are as follows:

- Global Authentication, Access Control, and Directory Services (UC Portable Assured Services in UC Pilots, UCR, and UC APL Products)

- Information and Services "from the Edge" (UC Assured Quality Services to Deployed Tactical Units based on the UCR and UC APL Products)

- Joint Infrastructure (Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to SA across a Diverse Spectrum of Operational Requirements)

- Common Policies and Standards (UCR and Test Programs for UC Spirals and for UC APL Products)

- Unity of Command (Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to SA across a Diverse Spectrum of Operational Requirements)

DISA has three major planning documents that are both driving and supporting the UC planning activities. The first is 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 that the UC migration must support. The three Lines of Operations with the UC initiatives addressing them in parentheses are as follows:

- Enterprise Infrastructure (UCR, Technology Insertions, and Test Programs for UC Spirals and UC APL Products)

- C2 and Information Sharing (UCR, Assured and Secure Products, Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to SA across a Diverse Spectrum of Operational Requirements)

- Operate and Assure (UCR, Assured and Secure Products, Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to SA across a Diverse Spectrum of Operational Requirements)

The second document is 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. These DISA programs and their migration directly affect UC implementation. The four categories, with the UC initiatives addressing them in parentheses, are as follows:

- Applications, Services, and Data (UC Collaboration Services Non-Assured Services with Quality of Service (QoS) and Assured Services with QoS)

- Communications and Networks (UC Assured Services via UCR and UC APL Products)

- Information Assurance (End-to-End IA UCR and Information Assurance Governance)

- NETOPS and Enterprise Management (NETOPS Concept of Operations (CONOPS)/Joint Tactics, Techniques, and Procedures (JTTPs), UC Element Management Systems (EMSs))

The third document is the "Defense Information Systems Network (DISN) Technical Evolution Plan (DTEP)." The DTEP addresses "how" and "when" for the DISN UC technical migration. The DTEP includes a section on DISN UC evolution and a section on DISN UC deployment, which addresses the technology migrations outlined in the "DoD Unified Capabilities Requirements (UCR)." The "UC Master Plan" (UC MP) will be consistent with these DISN documents, as well as DoD Components' UC technology implementation plans. The DTEP's four key capabilities, with the UC initiatives addressing them in parentheses, are as follows:

- Information Assurance (IA Technical Requirements in the UCR and IA Governance)

- Connectivity (Assured Services Requirements in the UCR)

- Network Management (NM) (NETOPS CONOPS/JTTPs, UC EMS)

- Interoperability (UCR and Test Programs for UC Spirals and UC APL Products)

There are two documents essential to synchronizing investments across DoD by DISA and other DoD Components. These documents are UC implementation plans and UC network cutover plans (NCPs). The UC implementation plans will synchronize the deployment of UC from a DoD network's perspective based on DoD Components' acquisition plans by quarter of fiscal year (FY). The UC NCPs will ensure the readiness of UC site installations, UC transport, and Network Operations and Security Centers (NOSCs) as they become operational.

The most demanding set of requirements in these documents are those associated with the following:

- Information Assurance consistent with the DoD IA Certification and Accreditation Process (DIACAP) and Security Technical Implementation Guides (STIGs) that must change constantly due to emerging vulnerabilities and threats

- Assured services across hybrid circuit-switched and IP networks

- End-to-end interoperability among multiple vendors

- End-to-end interoperability between fixed and multiple deployable programs

- NETOPS performance: sustaining high QoS for end-to-end voice, video, collaboration, and data performance over Internet Protocol (IP) networks

- NETOPS response to SA: collaboratively adapting DoD networks via the command hierarchy to meet mission needs

- Internet Protocol Version 6 (IPv6) end device-to-end device performance leveraging the capabilities of IPv6

- Fully leveraging COTS features associated with UC to enhance mission and combat support productivity

These requirements are the most demanding because IP-based technologies have inherent IA limitations that must be mitigated, and they were not designed originally for the voice and video subset of UC services; and therefore, require a variety of techniques to support UC services properly. Thus, IP-based technologies require GIG Enterprise Wide Systems Engineering (EWSE) by the Government, development by industry, and test and evaluation by the Government to satisfy the policies and meet the requirements. In addition, the challenges and military services' funding limitations force the installation of a common IP technology base to occur over a number of FYs. Thus, networks based on hybrid technologies including a mix of technologies (e.g., circuit-switched and/or IP) and converged or non-converged solutions, will be required for many years. The UC Deployment Spirals have been structured to resolve these challenges and to result in approved products for the DoD Components to purchase.

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

d. Precedence-based sessions placed to 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 SA to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock network operations centers (NOCs) that oversee voice, video, and data services. DISA shall oversee the DISN systems and shall have read-write access to DISN systems, which are shared with the military services for cost avoidance, such as the multifunction softswitch (MFSS) or WAN Softswitch (SS). All NOCs shall have EMSs that allow for read-write access for the systems for which they have direct responsibility. In addition, the 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 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. Unified Capabilities networks shall be designed with the capability to permit interconnection and interoperation with similar Services' Deployable programs, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable.

j. Unified Capabilities networks shall be designed to assure that 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 UC services, end-to-end UC network designs, the UC products that support those designs, and the core processes needed for a vendor to gain placement of its UC products on the DoD UC APL. Use of products from the DoD UC APL allows DoD Components to purchase and operate UC products over all DoD network infrastructures. This section applies to both fixed and deployable products that support UC services on DoD networks.

4.2 UNIFIED CAPABILITIES SERVICES DESCRIPTION

The major drivers of mission needs for UC services are addressed in Section 3, Policy/ Requirements. Unified Capabilities 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 MIGRATION TO UNIFIED CAPABILITIES

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

The purpose of the UC MP is to

- Define DoD's migration from the current legacy technologies to converged net-centric, IP-based voice, video, and data services.

- Serve as a guideline to the DoD Components in the preparation of migration and acquisition plans for phasing out circuit-switched voice and video services and initially phasing in Voice and Video over IP (VVoIP) services, and other UC services that will operate in converged voice, video, and data networks. The UC MP addresses synchronization of life-cycle activities, from acquisition to operations, for networks that provide UC services.

- Provide guidance for DoD Components' Program Objective Memorandum (POM) submissions.

The challenges of UC migration and DoD Component budgets prevent the ability to install a common IP technology base as a global "flash cut." Thus, networks based on hybrid technologies will be required for many years. The role of time division multiplexing (TDM) in future planning for UC is currently limited to the Defense Red Switch Network (DRSN) due to the need for Multilevel Security (MLS) for which IP is currently not well suited. The DISN Evolution Spirals as shown in Figure 4.3-1, DISN Evolution Spirals, have been structured to address these challenges.

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

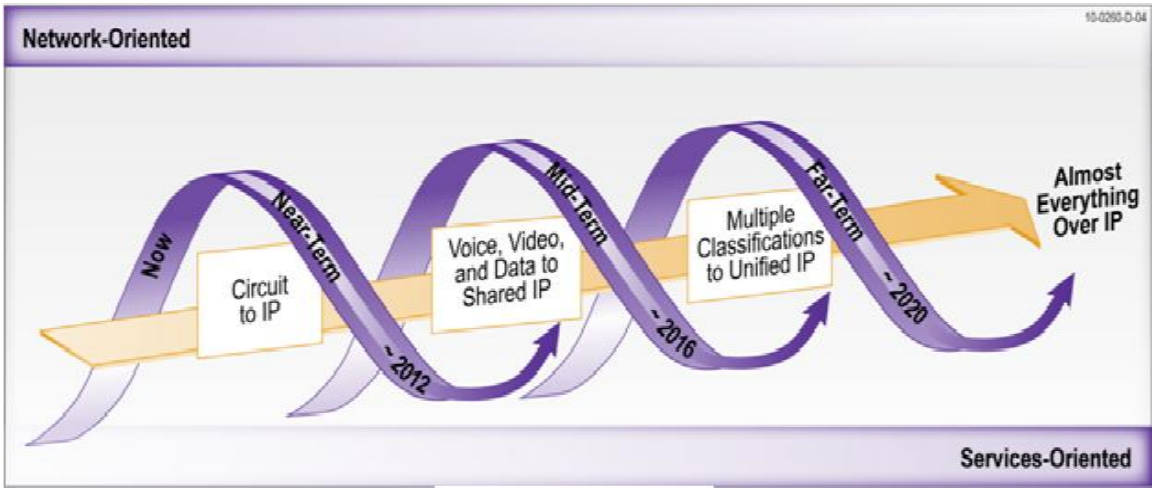


Figure 4.3-1. DISN Evolution Spirals

To support timely UC implementation, the migration strategy is structured to fully leverage DISN technical refreshment investments. The UC MP is based on the DISN Spiral timeframes to synchronize DISN and DoD Components investments. Figure 4.3-1 illustrates the Near-Term, Mid-Term, and Far-Term DISN Spirals that depict the evolution to the target capabilities and infrastructure. These three spirals are as follows:

- Near-Term (Current–FY 2012) – Circuit-Switched to IP Convergence
- Mid-Term (FY 2013–2016) – Voice, Video, and Data to Shared IP Convergence
- Far-Term (FY 2017–2020) – Multiple Classifications to Unified IP Convergence

At the completion of each spiral, UC services are implemented, both by the DoD Components and in the DISN infrastructure. As shown in Figure 4.3-1, network-oriented capabilities will evolve to enhanced service oriented capabilities.

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

Mid-Term Spiral. This spiral will focus on expanding converged voice, video, and data services by integrating service specific networks into a shared IP-based network using improved IP QoS, multicast, and session setup technologies. Ethernet-based transport services will support

different classification levels. Command and control applications will remain separate from the IP networks for mission assurance. High Assurance Internet Protocol Encryptor (HAIPE) deployments will be expanding. The phase-out of separate legacy circuit-based voice, video, and data networks in the DISN Mid-Term Spiral will expand as customers migrate to enhanced DISN IP data services. Assured services will provide availability, information protection, and optimized information delivery.

Far-Term Spiral. This spiral will focus on the DoD CIO's vision for net-centricity by establishing highly available, resilient, and secure IP-based networks, to include command and control applications. This DISN spiral will support user-encrypted, IP-based voice, video, and data services at all classification levels over a unified customer interface.

4.4 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 IA testing. These tests are used to make the certification decisions necessary to place products on the DoD UC APL.
- Provide IA requirements necessary for UC products to meet DoD IA policy to become approved products. Later, these IA 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.

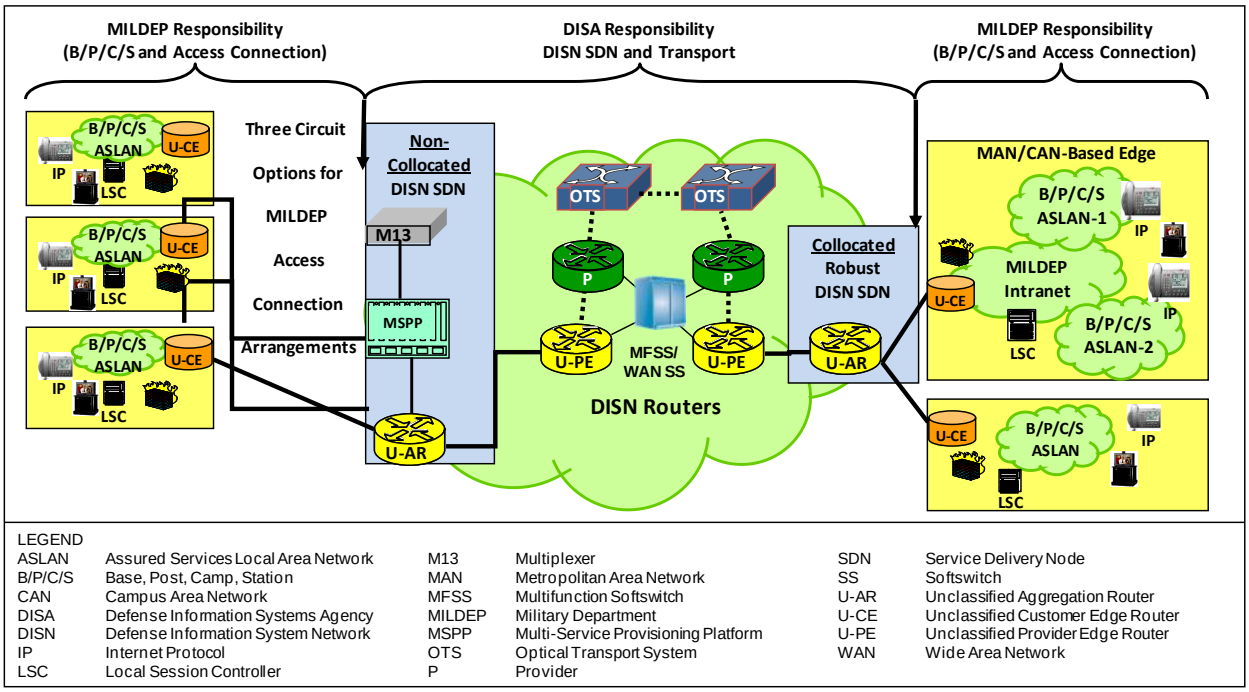
Specifically, this UCR specifies technical requirements for assured interoperability and IA of products that provide the following set of UC, which will be expanded in the future:

- 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 4.4-1, 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), Local Session Controllers (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 TDM-based Defense Switched Network (DSN) and its components with VoIP assured local area network (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 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. Since the circuit-switched TDM-based network is well established, the following subsections provide a UC network overview by first describing VVoIP subsystems followed by an overview of the TDM-based DSN design.



LEGEND

ASLAN	Assured Services Local Area Network	M13	Multiplexer	SDN	Service Delivery Node
B/P/C/S	Base, Post, Camp, Station	MAN	Metropolitan Area Network	SS	Softswitch
CAN	Campus Area Network	MFSS	Multifunction Softswitch	U-AR	Unclassified Aggregation Router
DISA	Defense Information Systems Agency	MILDEP	Military Department	U-CE	Unclassified Customer Edge Router
DISN	Defense Information System Network	MSPP	Multi-Service Provisioning Platform	U-PE	Unclassified Provider Edge Router
IP	Internet Protocol	OTS	Optical Transport System	WAN	Wide Area Network
LSC	Local Session Controller	P	Provider		

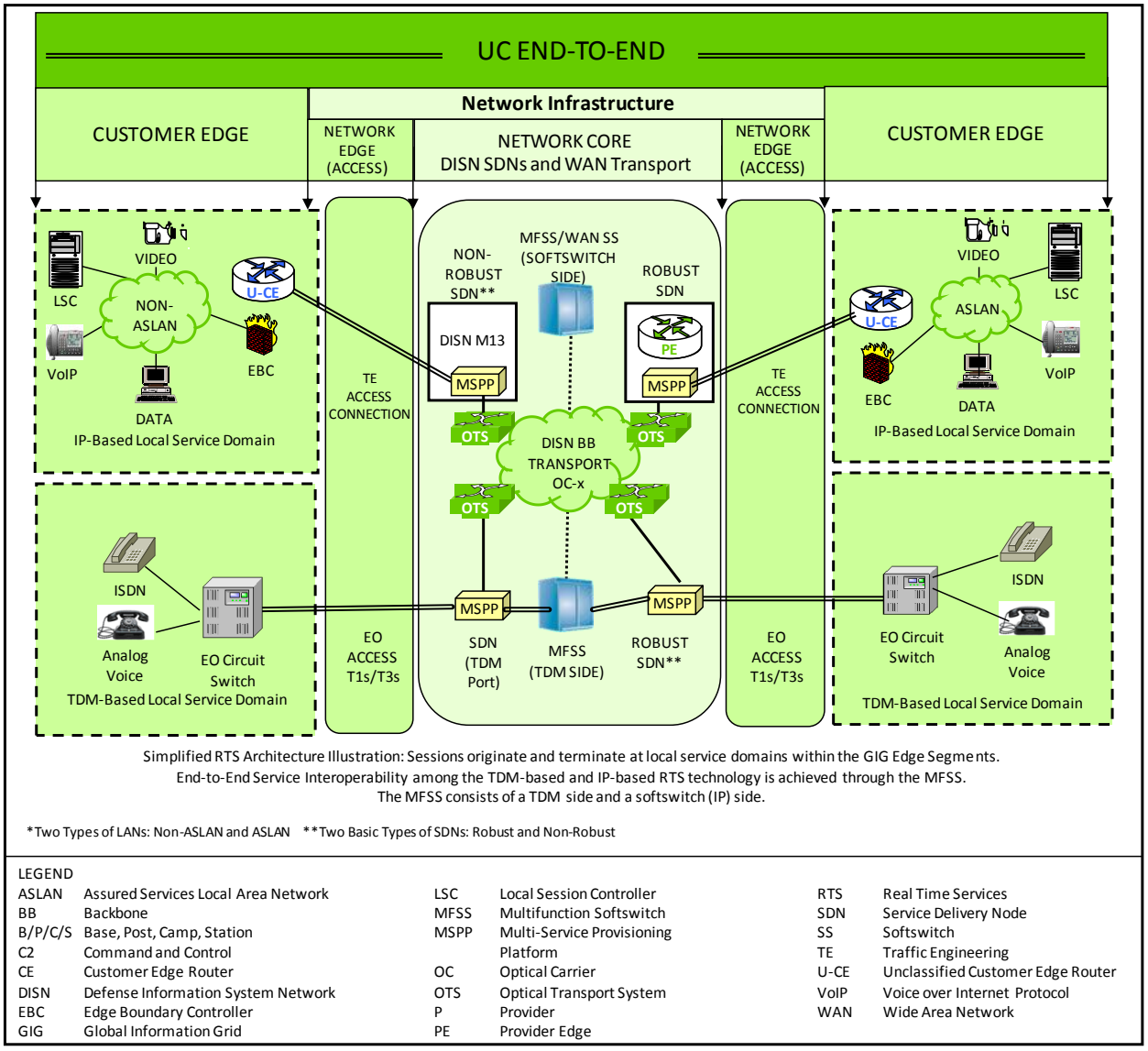
Figure 4.4-1. End-to-End IP Network Description

Figure 4.4-2, 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.

4.4.1 Overview of Network Design for VVoIP

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

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



Simplified RTS Architecture Illustration: Sessions originate and terminate at local service domains within the GIG Edge Segments.
End-to-End Service Interoperability among the TDM-based and IP-based RTS technology is achieved through the MFSS.
The MFSS consists of a TDM side and a softswitch (IP) side.

*Two Types of LANs: Non-ASLAN and ASLAN **Two Basic Types of SDNs: Robust and Non-Robust

LEGEND

ASLAN	Assured Services Local Area Network	LSC	Local Session Controller	RTS	Real Time Services
BB	Backbone	MFSS	Multifunction Softswitch	SDN	Service Delivery Node
B/P/C/S	Base, Post, Camp, Station	MSPP	Multi-Service Provisioning Platform	SS	Softswitch
C2	Command and Control			TE	Traffic Engineering
CE	Customer Edge Router	OC	Optical Carrier	U-CE	Unclassified Customer Edge Router
DISN	Defense Information System Network	OTS	Optical Transport System	VoIP	Voice over Internet Protocol
EBC	Edge Boundary Controller	P	Provider	WAN	Wide Area Network
GIG	Global Information Grid	PE	Provider Edge		

Figure 4.4-2. High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments

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

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

- Type of SDN
  - Non-Robust – M13 multiplexer
  - Robust –Multi-Service Provisioning Platform (MSPP) without Aggregation Router (AR) all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning)
  - Robust – MSPP with Unclassified Aggregation Router (U-AR)
- U-CE Router Location for the SDN
  - U-CE Router not at an SDN location
  - U-CE Router at a non-robust SDN location
  - U-CE Router at a robust SDN location
- Type of U-CE Router
  - Critical mission
  - Noncritical mission

As shown in Figure 4.4.1-1, 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.

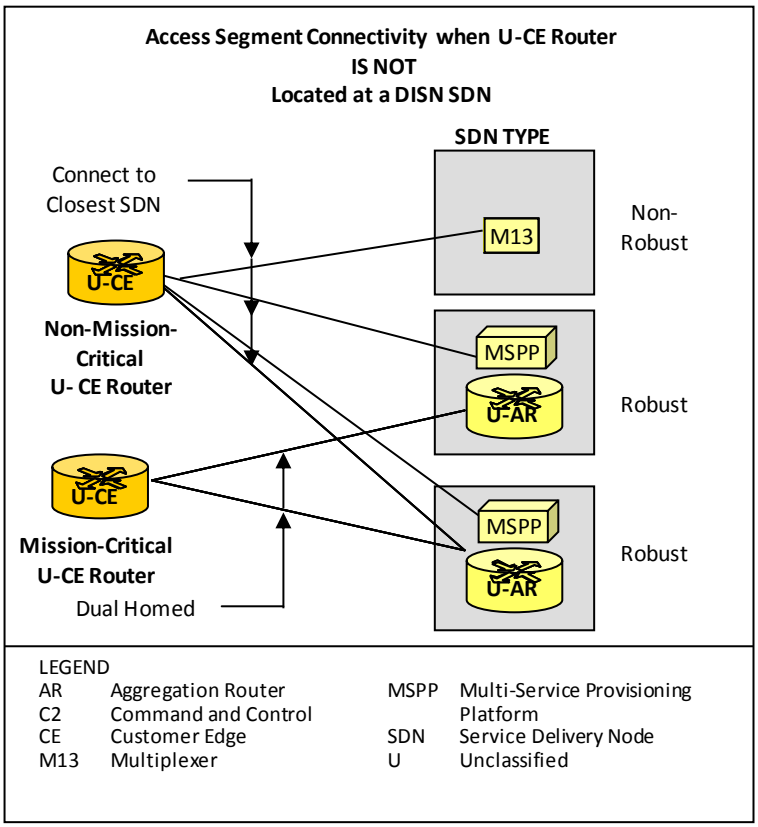


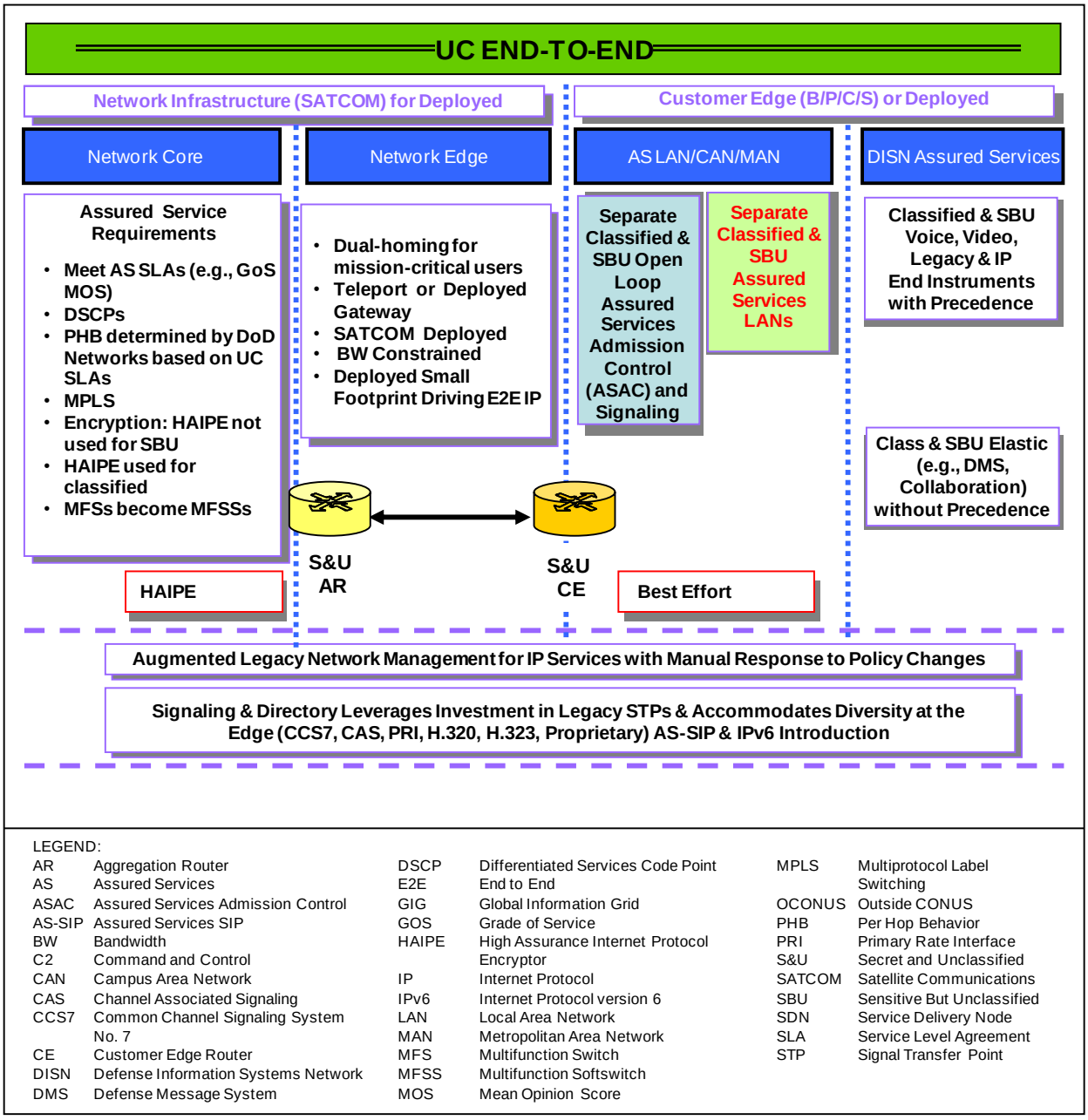
Figure 4.4.1-1. Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site

4.4.1.1 Overview of VVoIP Network Design Attributes

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

The logical location of the major VVoIP network attributes within the UC E2E design is shown in Figure 4.4.1-2, Overview of VVoIP network Attributes. The location of attributes in terms of the Customer Edge (B/P/C/S), the Network Edge (Access), and the Network Core is depicted, and the differentiation between assured service and non-assured service is shown between the top half of the diagram and the bottom half of the diagram, respectively.

The functions contained in the boxes located within the top half of Figure 4.4.1-2 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.



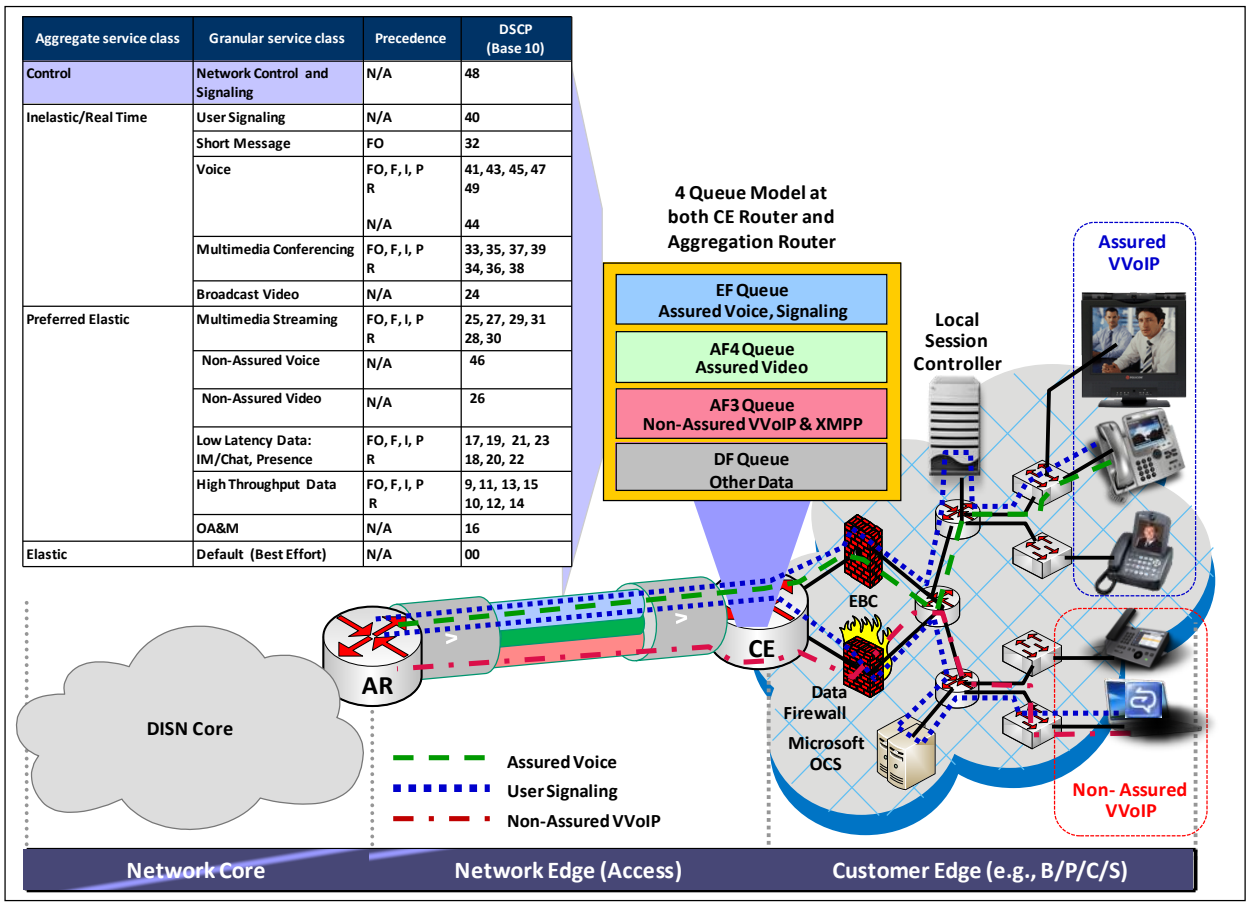
LEGEND:

AR	Aggregation Router	DSCP	Differentiated Services Code Point	MPLS	Multiprotocol Label Switching
AS	Assured Services	E2E	End to End	OCONUS	Outside CONUS
ASAC	Assured Services Admission Control	GIG	Global Information Grid	PHB	Per Hop Behavior
AS-SIP	Assured Services SIP	GOS	Grade of Service	PRI	Primary Rate Interface
BW	Bandwidth	HAIPE	High Assurance Internet Protocol Encryptor	S&U	Secret and Unclassified
C2	Command and Control	IP	Internet Protocol	SATCOM	Satellite Communications
CAN	Campus Area Network	IPv6	Internet Protocol version 6	SBU	Sensitive But Unclassified
CAS	Channel Associated Signaling	LAN	Local Area Network	SDN	Service Delivery Node
CCS7	Common Channel Signaling System No. 7	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 4.4.1-2. Overview of VVoIP Network Attributes

4.4.1.1.1 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 4.4.1-3 shows the queue structure and associated rules.



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
	Voice	FO, F, I, P R	41, 43, 45, 47 49
		N/A	44
	Multimedia Conferencing	FO, F, I, P R	33, 35, 37, 39 34, 36, 38
	Broadcast Video	N/A	24
Preferred Elastic	Multimedia Streaming	FO, F, I, P R	25, 27, 29, 31 28, 30
	Non-Assured Voice	N/A	46
	Non-Assured Video	N/A	26
	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	00

Figure 4.4.1-3. Queuing for the Bearer Design

There are two categories of VVoIP. The first category is assured VVoIP and this category has been discussed in depth in earlier sections. The second category is non-assured VVoIP. Non-assured VVoIP has many of the same characteristics as assured VVoIP with two critical

exceptions. The first exception is that session admission control (SAC) is not applied to non-assured VVoIP. Session admission control polices or controls the amount 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 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 second exception is that non-assured VVoIP sessions cannot be traffic-engineered to ensure QoS. The ability to apply SAC to assured VVoIP ensures that assured VVoIP is deterministic or predictable in nature. Since the offered load is predictable, it can be traffic-engineered and the network can be designed for the traffic-engineered load. Non-assured VVoIP does not have SAC, and therefore, cannot be traffic-engineered to ensure that acceptable QoS is achieved. The nature of non-assured VVoIP is that typically it is composed of peer-to-peer sessions that do not transit a centralized SAC appliance, and therefore, SAC cannot be applied.

Mixing assured VVoIP with non-assured VVoIP will result in the uncontrolled non-assured VVoIP degrading assured VVoIP on congested networks. To ensure acceptable QoS in IP networks for assured VVoIP, it is necessary to assign the assured VVoIP traffic to different queues than data sessions and non-assured VVoIP on congested connections. To delineate the assured VVoIP from the non-assured VVoIP (and other types of packets), it is necessary to mark the IP packets with unique Differentiated Services Code Points (DSCPs). Figure 4.4.1-3, Queuing for the Bearer Design, provides a table of the DSCP plan and the queuing approach that is extracted from Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, of this document. 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, the host will continue transmitting at the same rate independent of the ability of the network to support that rate. In addition, the UDP packets can quickly cause the preferred data sessions that they are queued with (in four-queue model) to terminate due to 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 cause unacceptable degradation on non-assured VVoIP sessions during periods of high usage, but will ensure that preferred data sessions continue to get 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 IA requirements.

4.4.1.1.2 Customer Edge Segment Design

The Customer Edge Segment has the following attributes:

- Nonblocking ASLAN. At the Customer Edge, the design has an ASLAN that is designed as nonblocking for voice and video traffic.

- Traffic Admission Control. The LSCs on a B/P/C/S use an Open Loop ASAC technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit consistent with maintaining a voice quality, as described in Section 5.3.3.15, Voice Service Quality.

- Call Preemption. Lower precedence sessions will be preempted on the access circuit to accept the LSC setup of a higher precedence level outgoing or incoming session establishment request.

- 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.

4.4.1.1.2.1 B/P/C/S VVoIP Design

The military B/P/C/S-level design consists of an LSC complex that may consist of a redundant LSC, or several LSCs in a cluster arrangement, in a LAN, campus area network (CAN), or metropolitan area network (MAN) structure. The LAN, CAN, or MAN design may be tailored to a single building or an entire base structure with varying degrees of robustness tailored to individual building mission requirements. Off-base connectivity to the long-haul DISN network infrastructure is provided through the 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.

4.4.1.1.2.2 LSC Designs – Voice

An LSC is a call stateful voice, video, and signaling server product at the B/P/C/S that directly serves IP and analog EIs. The LSCs are the cornerstone of all DoD VVoIP signaling functions.

The functions provided by the LSC are found in the MFSS also. The LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC uses AS-SIP signaling. If the LSC interfaces to the public switched telephone network (PSTN) or to legacy B/P/C/S TDM systems, it must support Primary Rate Interface (PRI) also, using its MG and Media Gateway Controller (MGC). All LSCs provide PBAS via AS-SIP/ASAC for IP and via T1.619a.

Figure 4.4.1-4, B/P/C/S-Level Voice over IP LSC Voice Designs, shows examples of three possible configurations for connecting multiple LSCs on a B/P/C/S to the DISN WAN and the MFSS. The U-CE Routers are dual homed and not shown for simplicity. At the top of the figure, the first case shown is where multiple LANs, each with its own LSC and U-CE Router, connect via separate access circuits to the DISN WAN. Each LSC would have its own traffic-engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from one LSC on the base to another LSC on the base must traverse the DISN WAN and use the MFSS to connect to another LSC. Should base connection to the DISN WAN or the MFSS be lost, then sessions from one base LSC to another on-base LSC could not be established. In addition, if one of the LSCs was not using all its traffic-engineered bandwidth (Budget A), a second LSC (Budget B) could not use the unused bandwidth of the other LSC (Budget A).

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

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

The third case requires the design and implementation of an LSC cluster concept where a master LSC, as shown in the figure, has a master directory of all users on the base. Under this arrangement, service order activity at one LSC will be reflected automatically at all LSCs in the cluster, including the master LSC. *Only the first case will be specified in detail in the UCR.* The other two cases will require custom engineering of the base design (including the use of the LSC portion of an MFSS where an MFSS is located on a base) to ensure interoperability and acceptable performance between the various on-base LSC arrangements and vendors.

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.

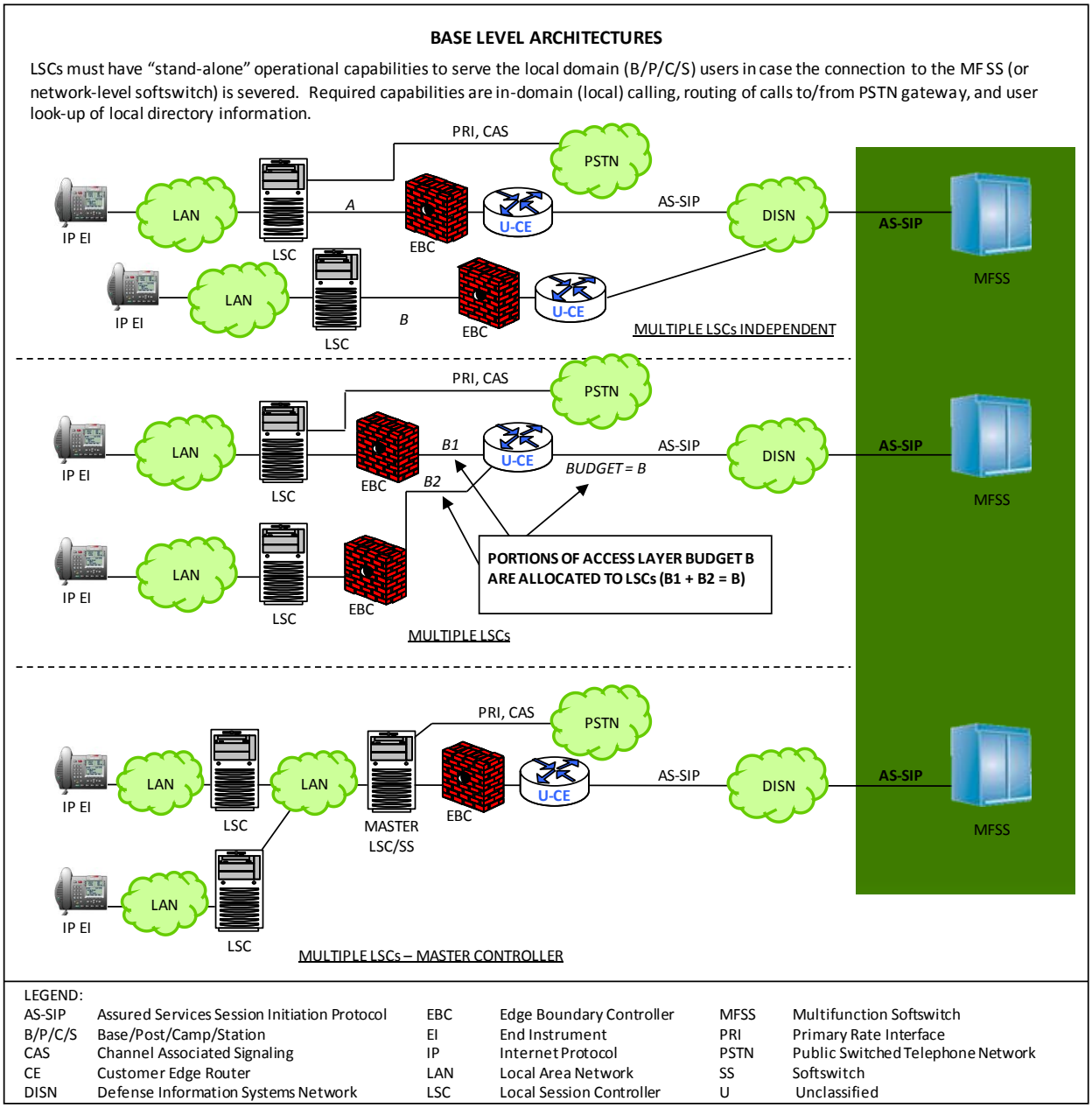


Figure 4.4.1-4. B/P/C/S-Level Voice over IP LSC Designs

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 (10 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 EMS that supports the USCYBERCOM.

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.

4.4.1.1.2.3 LSC Designs – Video

Figure 4.4.1-5, B/P/C/S Video over IP LSC Designs, illustrates the LSC designs for video services. An LSC is a call stateful AS-SIP signaling appliance at the B/P/C/S that directly serves IP video-capable EIs. The video LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC uses AS-SIP signaling. A Gatekeeper is an appliance that processes calls to the WAN using H.323 or Session Initiation Protocol (SIP) signaling. If the LSC or Gatekeeper interfaces to the PSTN or to legacy B/P/C/S TDM appliances, it must also support PRI and CAS using its MG and MGC. All LSCs provide PBAS via AS-SIP/ASAC for IP and via MLPP for the PRI.

Figure 4.4.1-5 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.

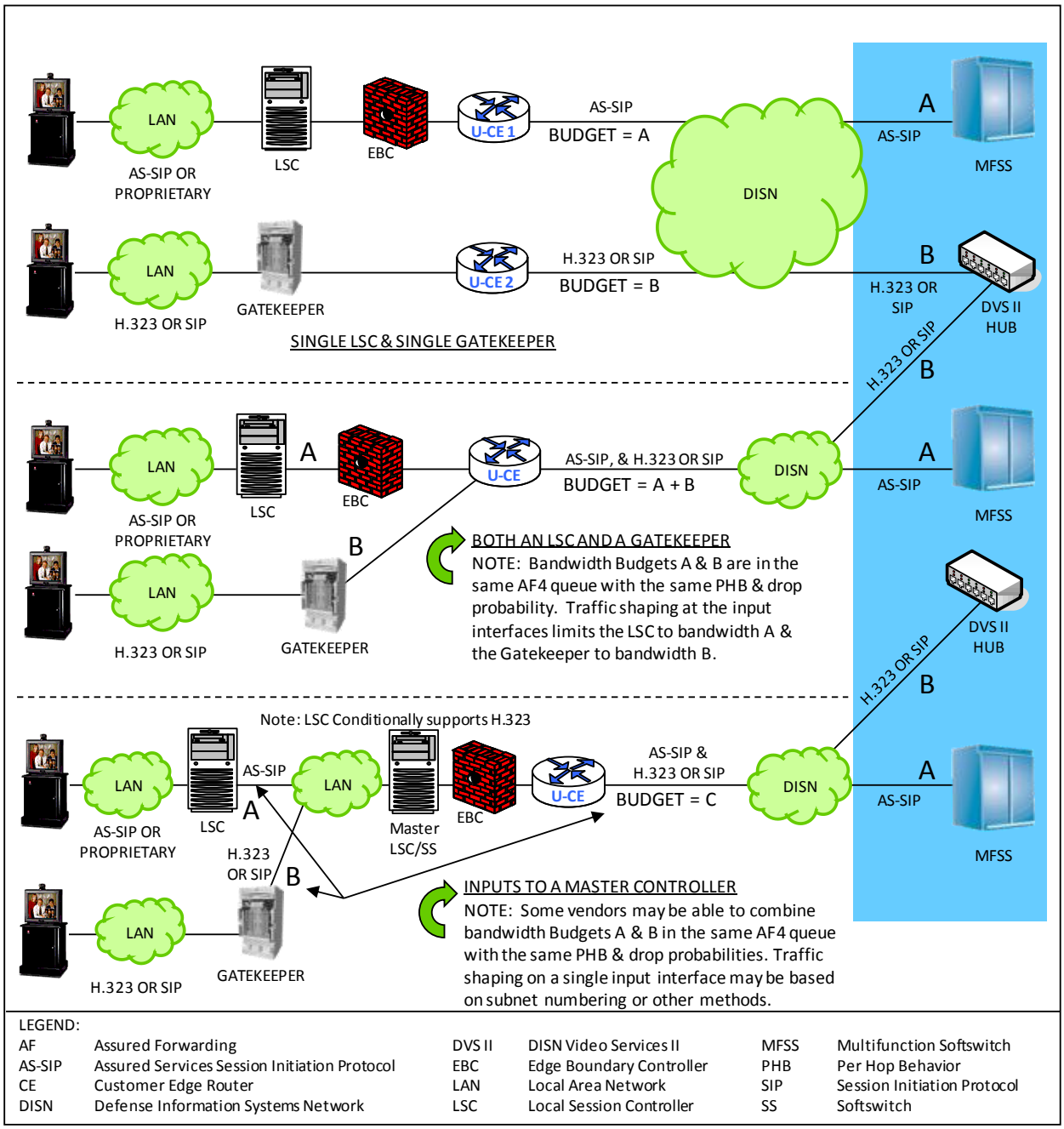


Figure 4.4.1-5. B/P/C/S Video over IP LSC Designs

The second case, shown in the middle of the figure, allows sessions to be established through the U-CE Router. In this case, both the LSC and the Gatekeeper will act independently as described in the first case, but both will connect to the same U-CE Router. However, the LSC video call and the Gatekeeper video call will connect to separate ports on the U-CE Router. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the

sum of the traffic-engineered bandwidth for each individual LSC (i.e., B1+B2). Although each router port processing video calls acts independently in the AF4 queue, both customer calls must be treated equally 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 4.4.1.1.2.2, 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).

4.4.1.1.2.4 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 4.4.1-6.

ASLAN
UCR/UCTP

REQUIREMENTS

- MEET VOICE, VIDEO & DATA PERFORMANCE
- SERVICE CLASSES & PRECEDENCE MAPPED INTO DSCPs
- QOS BY OVER-PROVISIONING/DSCPs
- PACKET LOSS, JITTER, LATENCY METRICS
- COMMERCIAL, MEDIUM, AND HIGH AVAILABILITY/POWER
- VLAN FOR VOICE, VIDEO, DATA PERIPHERALS
- NETWORK MANAGEMENT OF LAN

LEGEND

ASLAN	Assured Services Local Area Network	IATP	Information Assurance Test Plan
C2	Command and Control	LAN	Local Area Network
DISN	Defense Information Systems Network	MOS	Mean Opinion Score
DSCP	Differentiated Services Code Point	SLA	Service Level Agreement
GOS	Grade of Service	UCTP	Unified Capability Test Plan
GSR	Generic System Requirements	VLAN	Virtual Local Area Network

Figure 4.4.1-6. ASLAN Requirements Summary

Two types of LANs are ASLAN and non-ASLAN, depending on the type of missions and users served by a LAN. The two LAN types and three categories along with user classes are illustrated in Figure 4.4.1-7, Three Categories of LANs.

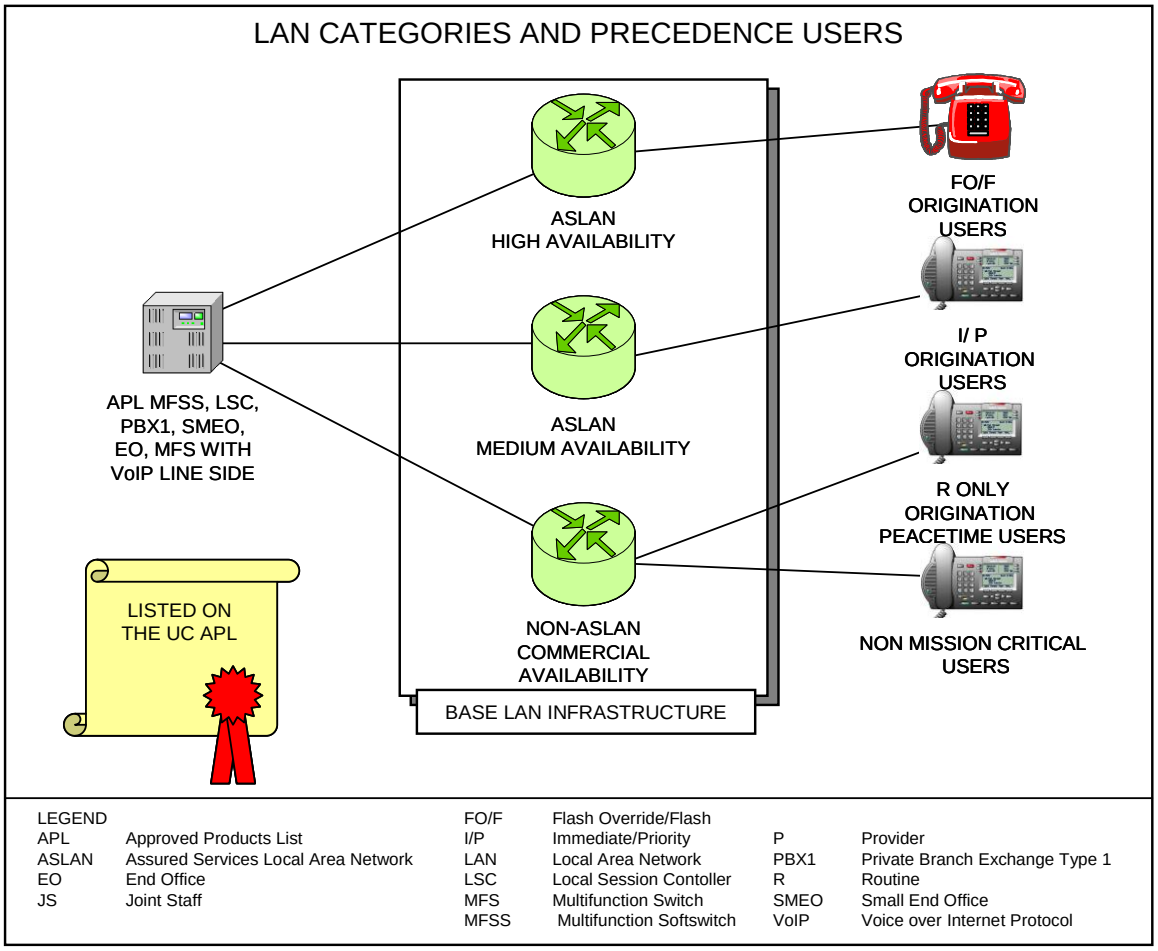


Figure 4.4.1-7. Three Categories of ASLANs

Table 4.4.1-1, LAN Requirements Summary, shows the requirements needed based on subscriber mission category. *Requirements* are defined, as necessary, for the user while *Permitted* allows other user types to be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence is required to be served on a High Availability ASLAN, and other users are permitted on the same LAN). *Not Permitted* means that the user must not be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence cannot be served by a Medium Availability ASLAN or non-ASLAN). *Not Required* are requirements that do not have to be met for some users (such as requirements for diversity, redundancy, and power backup that are not required for users that only have ROUTINE precedence).

Table 4.4.1-1. 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	N
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
GOS p=	0.0	0.0	0.0	Note 1
Availability	99.999	99.997	99.9	99.9

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.

The actual LAN implementation will vary from base to base depending on building or facility locations, installed cable plant, and the location and type of missions being performed on the base. Figure 4.4.1-8, An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users, is an example of one potential ASLAN implementation. It shows a CAN involving multiple buildings and types of mission users and how connectivity redundancy and backup power time requirement of 8, 2, or 0 hours are met in a cost-effective manner.

4.4.1.1.2.5 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, use a distributed LSC architecture 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.

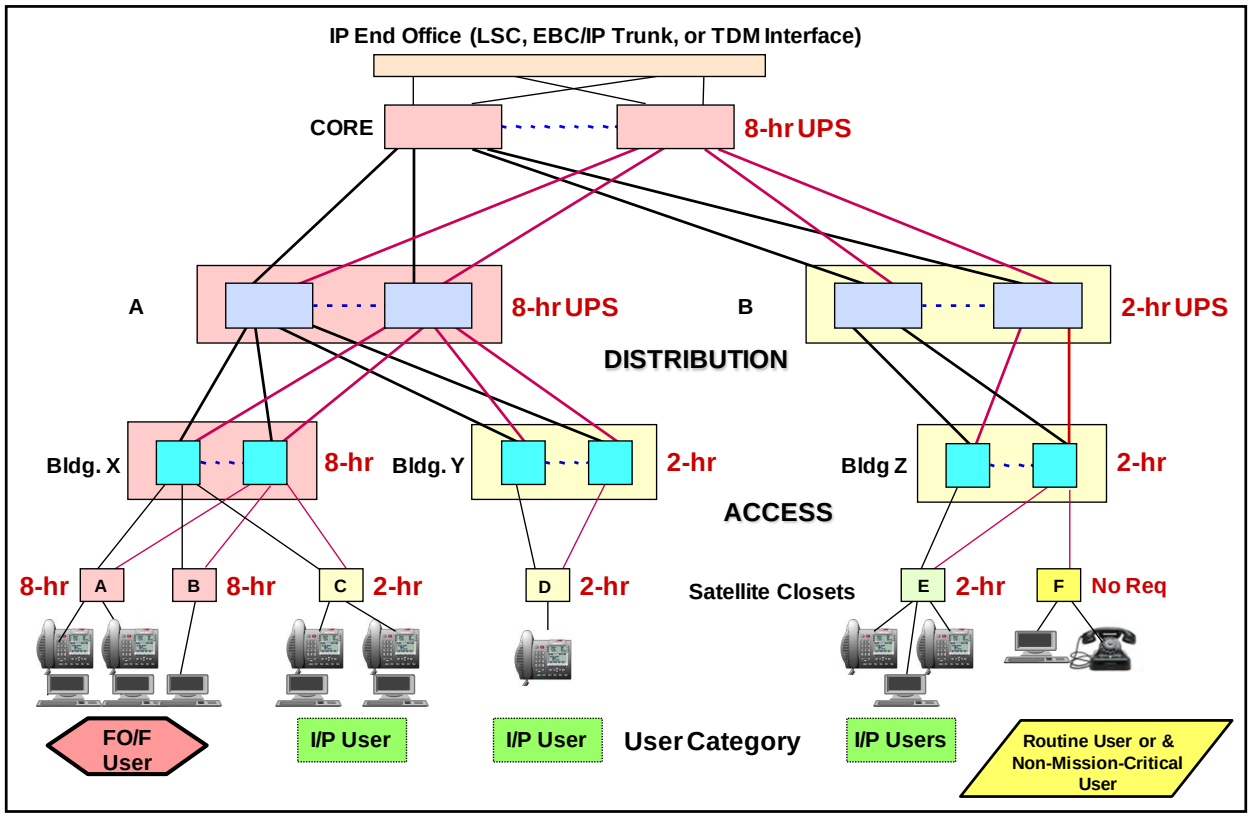


Figure 4.4.1-8. An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users

4.4.1.1.2.6 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 Control Protocol (DHCP) server, and for PKI certificate verification, access to an Online Certificate Status Protocol (OCSP) responder.

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

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 the MPLS Fast Failure Recovery (FFR) in the Core.

To ensure end-to-end voice and video services' performance, an allocation of performance must be established for the Services' Intranets and DISN SDNs, which are supporting IP-based voice, video, and data services. The performance requirements for voice and video is based on best commercial practices for latency, packet loss, jitter, and availability, which is allocated to the Services' ASLANs and their associated CE Router and EIs, to the Services' Intranets (called MANs and CANs) and to the DISN SDNs. Many techniques, such as MPLS, Multiprotocol Label Switching – Traffic Engineered (MPLS-TE), queuing, mesh routing, and redundancy, can be used by the networks to meet the performance allocations. Currently, only the voice and video performance metrics have been defined. Data application performance metrics will be addressed in the future. The performance metrics for voice (E-Model R-Factor) and video have been defined. Measurement techniques for validating that the performance allocations have been met and for isolating the portion of the end-to-end network, that is not meeting the allocations have been developed. Figure 4.4.1-9, 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). The specific end-to-end network performance requirements are described in Section 5.3.3, Network Infrastructure End-To-End Performance Requirements.

4.4.1.1.4 End-to-End Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions and protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes. The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and Resource Reservation Protocol (RSVP). The bearer plane is associated with the bearer traffic and protocols, such as Secure Real-Time Transport Protocol (SRTP) and Real Time Control Protocol (RTCP). The NM plane is associated with NM protocols and is used to transfer status and configuration information between 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).

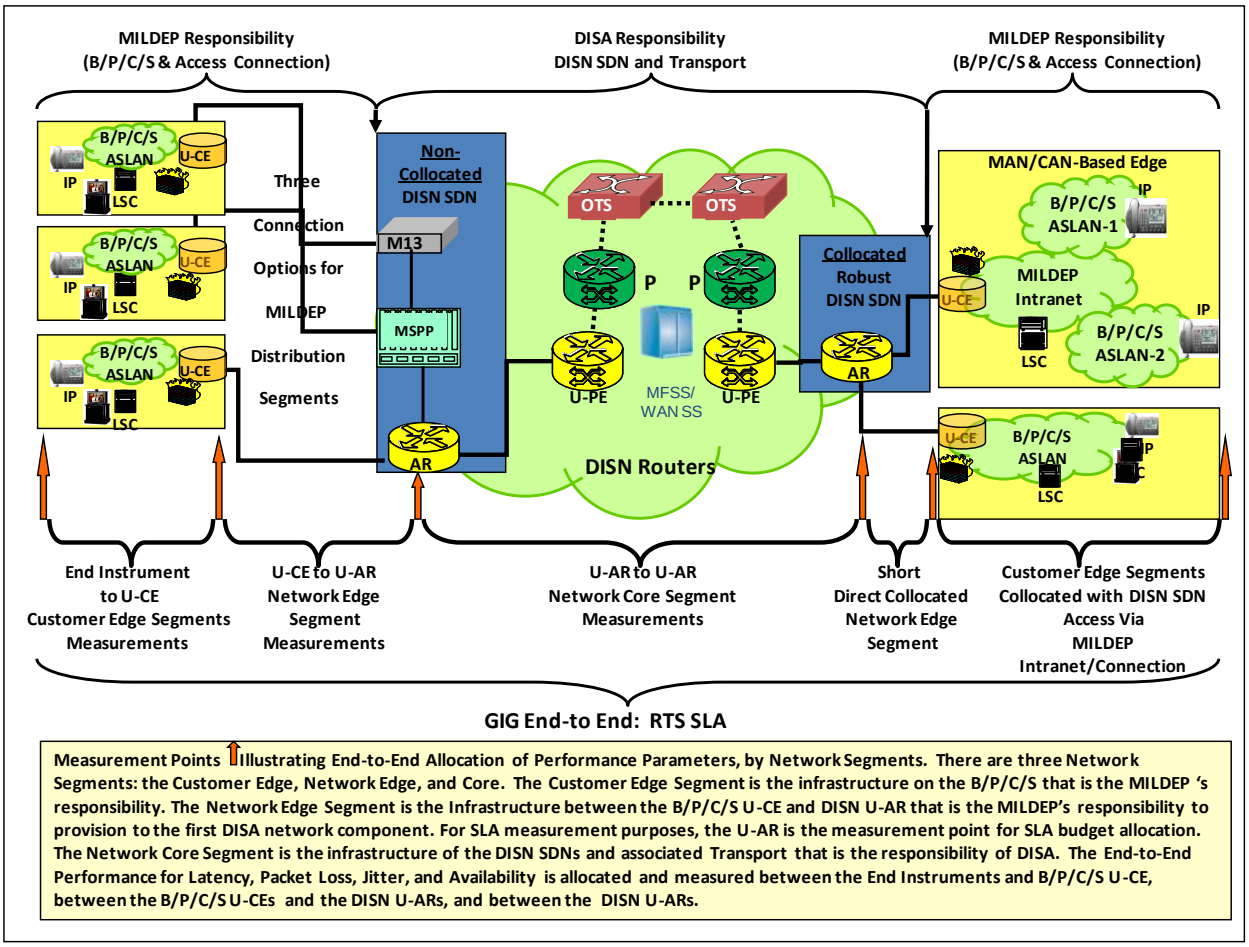


Figure 4.4.1-9. Measurement Points for Network Segments

4.4.1.1.5 ASAC Component

The ASAC technique is the key VVoIP design component ensuring that end-to-end SLAs (grade of service (GOS) voice quality, user assured service delivery, and call preemption to the EI) are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements (NEs) end-to-end.
Figure 4.4.1-10 represents the first step in specifying the DISN ASFs by depicting a more detailed functional breakdown of the components than that shown in Figure 4.4.1-2, Overview of VVoIP Network Attributes.

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.

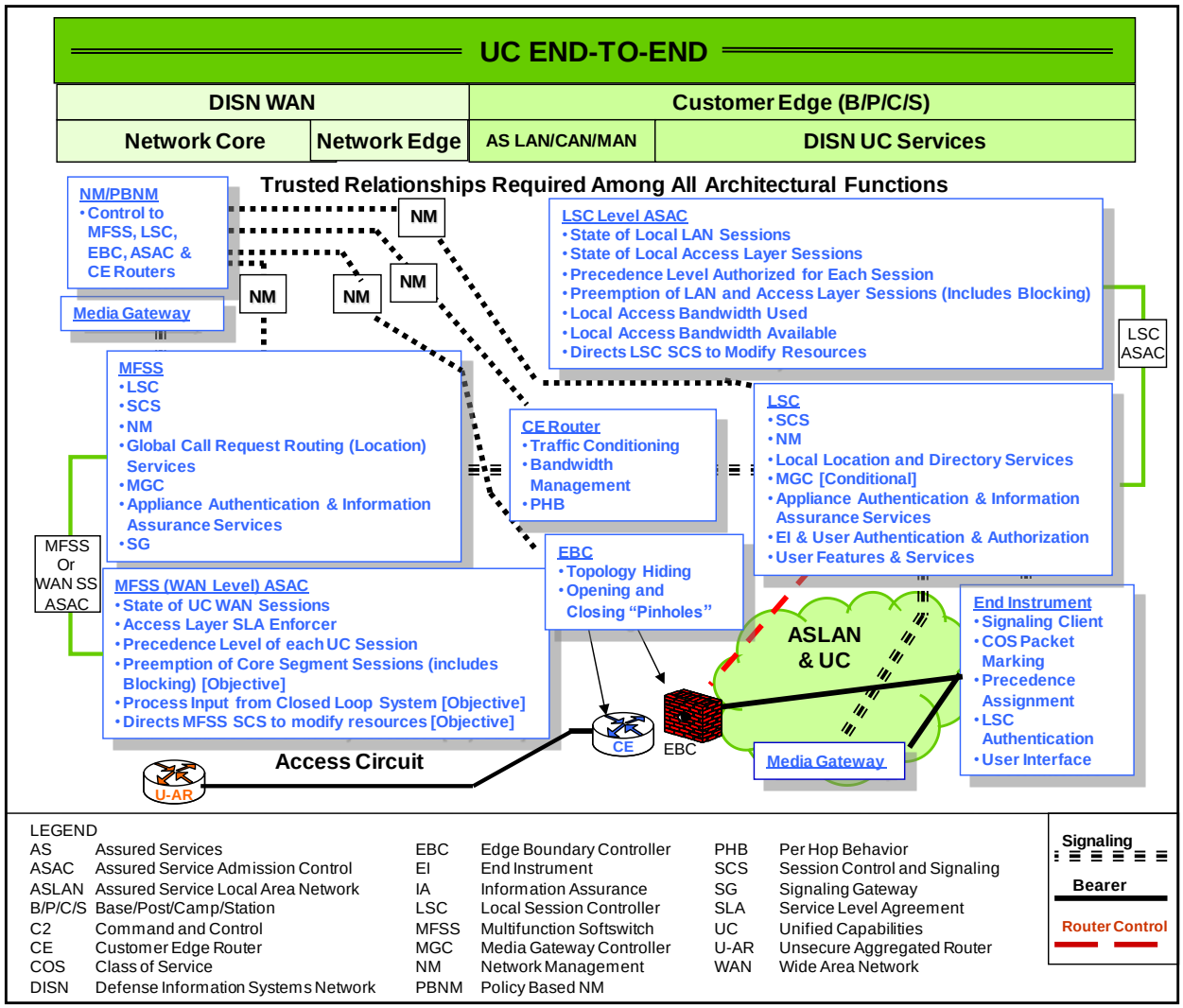


Figure 4.4.1-10. Assured Services Functions

The Open Loop ASAC design, depicted in Figure 4.4.1-11, Open Loop ASAC Network Design, is specified as the current method for achieving assured services end-to-end. The ASLAN connects via a local access circuit to a backbone network that consists of a Core MPLS-capable network.

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

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

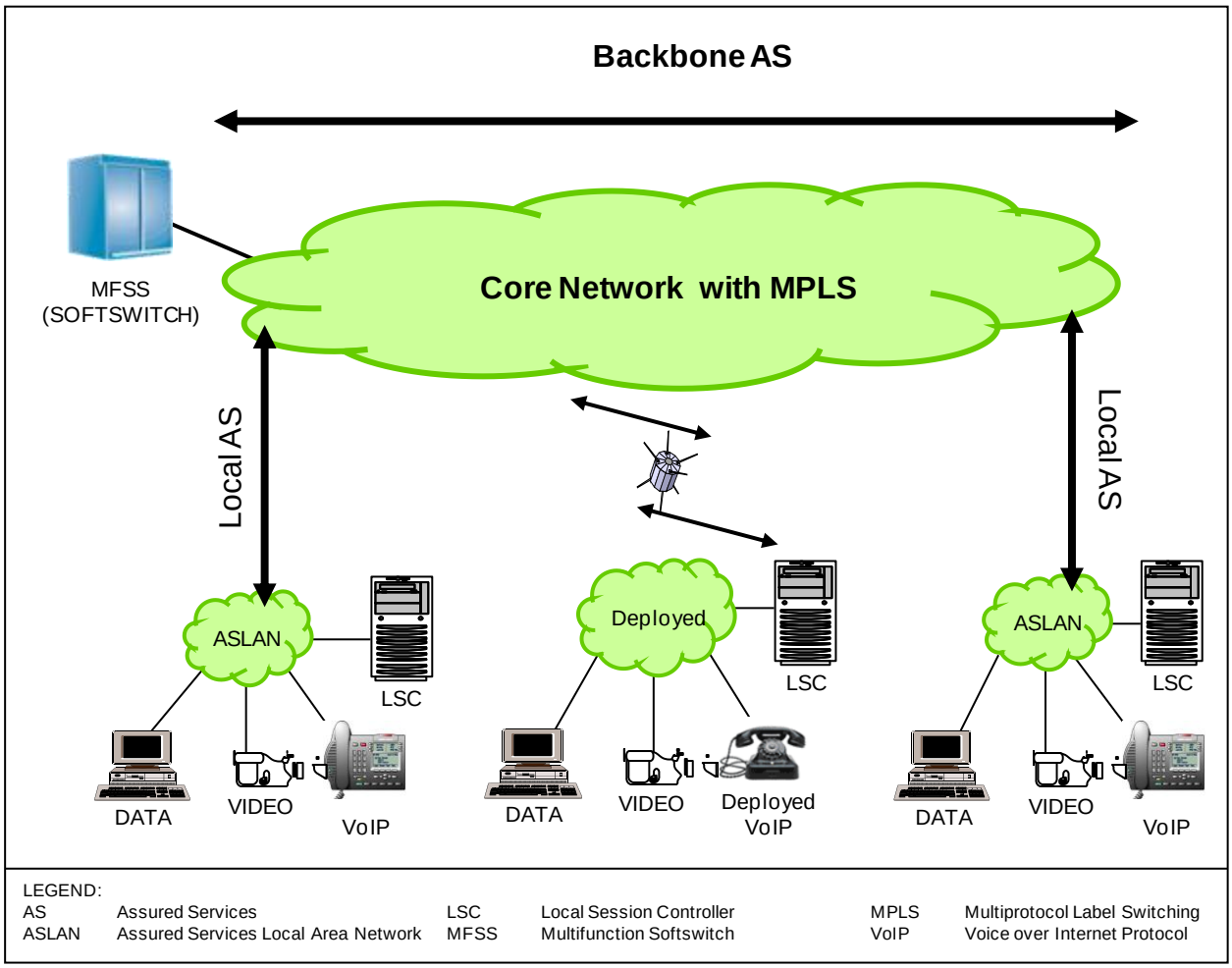


Figure 4.4.1-11. Open Loop ASAC Network Design

The components of the Open Loop ASAC method are shown in Figure 4.4.1-12, Open Loop ASAC for SBU Voice and Video. 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 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.

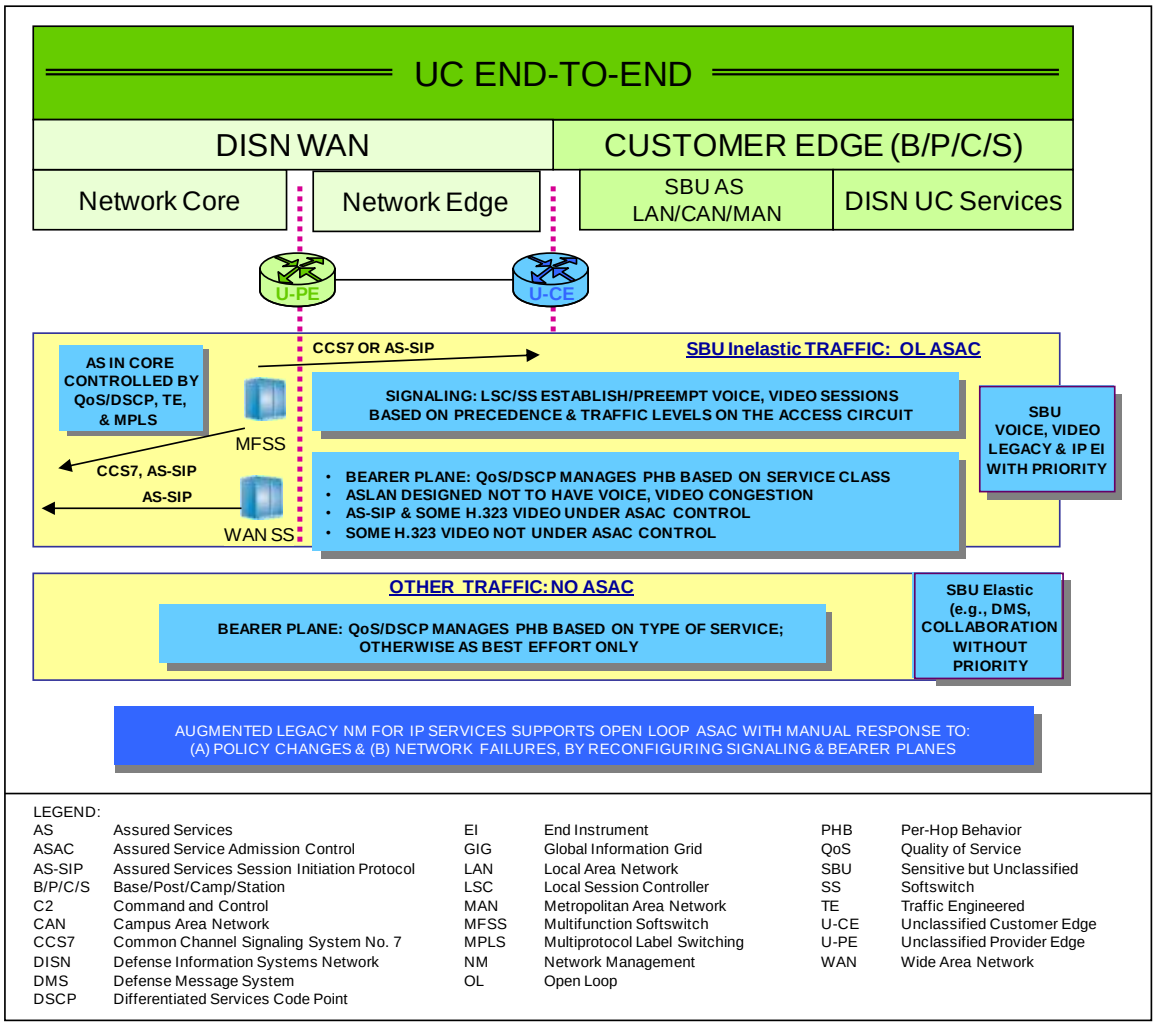
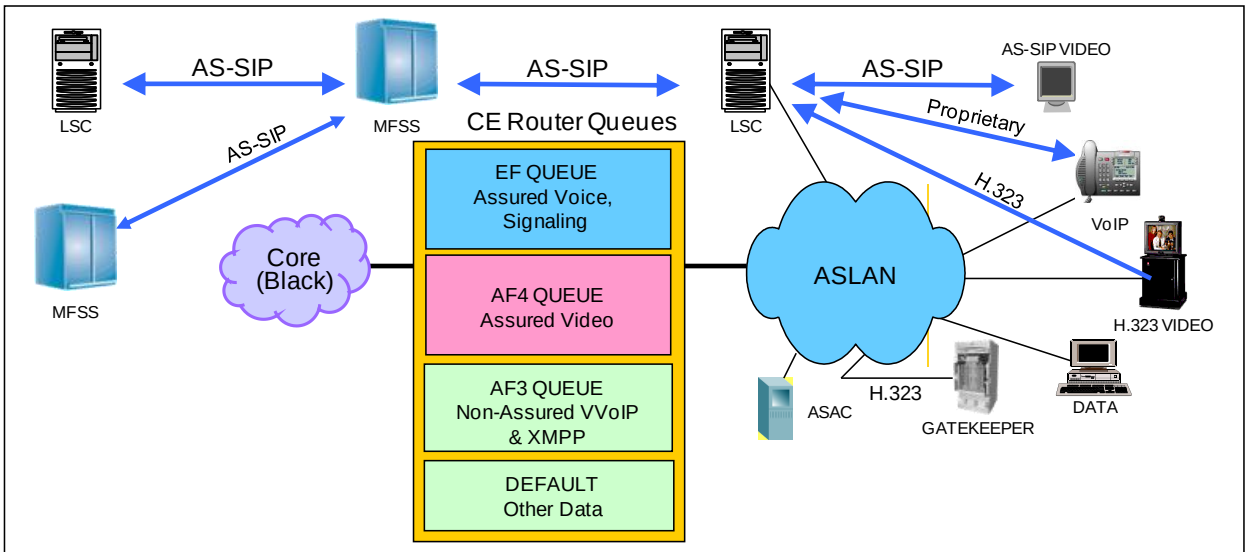


Figure 4.4.1-12. Open Loop ASAC for SBU Voice and Video

The LSC manages a budget for sessions determined by the voice and video traffic-engineered bandwidth of the associated access infrastructure. The Resource-Priority header portion of the AS-SIP signaling message conveys the precedence of the desired session establishment to the destination end LSC. Both the originating and destination LSCs independently manage their session budgets, so that sessions are permitted or established by precedence until the budget limit is reached. Then a new session can be allowed only if a lower precedence session is available to preempt. At the originating end after preemption has taken place, if necessary, the origination request is sent to the destination upon which, after preemption has taken place, if necessary, the request acceptance is returned to the originating LSC. If the originating LSC is at its budget limit and has no lower precedence session to preempt, then a blocked session indication, in the form of a Blocked Precedence Announcement (BPA), will be sent to the originating EI. If the terminating LSC is at its budget limit and has no lower precedence session to preempt, then a Session Request Denied message will be returned to the originating LSC, which, in turn, will

send a BPA to the EI. For ROUTINE precedence calls reaching the maximum budget limit, "fast busy" (120 impulses per minute (ipm)) will be sent to the originating EI. All AS-SIP voice users and some H.323 video users will come under Open Loop ASAC. Some H.323 video users on a base may choose to use a separate H.323 Gatekeeper and not come under LSC Open Loop ASAC.

NOTE: Data traffic (non-voice and video) does not have any ASAC and is handled as Best Effort or preferred data, if the data application implements DSCP packet marking. Figure 4.4.1-13, Converged VVoIP Design: Signaling, QoS, and Assured Service, shows the aspects of ASAC, signaling, and QoS (CE Router queues and PHB) in one diagram. All video calls leaving the MLSC or SS 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).



- Signaling: The local LSC manages ASAC on edge and on access link to the WAN, by preempting and/or blocking both incoming and outgoing sessions.
  - LSC forwards priority of connection request via AS-SIP.
- QoS complements signaling in support of assured services.
  - DSCP assignment as per QoS WG recommendation determines mapping to PHB.
  - The CE uses 4 queues that are bandwidth sized based on traffic engineered loads:
    - Voice, signaling, & routing in EF queue.
    - Video is placed in an AF queue with two drop probabilities.
    - Preferred data & NM in an AF queue with 2 drop probabilities.
    - Data in an AF queue as Best Effort.
- LSC/ASAC to EBC interface required to indicate which packet flows to allow into the WAN.

LEGEND

AF	Assured Forwarding	EF	Expedited Forwarding	PHB	Per Hop Behavior
ASAC	Assured Service Admission Control	EBC	Edge Boundary Controller	QoS	Quality of Service
ASLAN	Assured Services Local Area Network	IP	Internet Protocol	VoIP	Voice over Internet Protocol
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller	WAN	Wide Area Network
CER	Customer Edge Router	MFSS	Multifunction Softswitch	WG	Working Group
DSCP	Differentiated Services Code Point	NM	Network Management	XMPP	Extensible Messaging and Presence Protocol

Figure 4.4.1-13. Converged VVoIP Design: Signaling, QoS, and Assured Service

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 Common Channel Signaling System No. 7 (CCS7)), the MG (for CAS), or the AS-SIP signaling appliance part of the LSC and MFSS depending on requirements for a particular session. Local subscriber directories are stored in the LSCs and network-level worldwide routing tables and addressing and numbering plans are stored in the MFSS.

4.4.1.1.6 Voice and Video Signaling Design

The voice and video signaling design for SBU voice and video is shown in Figure 4.4.1-14, SBU Voice and Video Services Signaling Design. For classified voice and video, only the AS-SIP signaling is used since classified VVoIP does not have a TDM legacy infrastructure embedded in the design. During migration, both H.323 and AS-SIP signaling will be used in classified VVoIP. Classified VVoIP interfaces to the TDM DRSN via MGs and SGs.

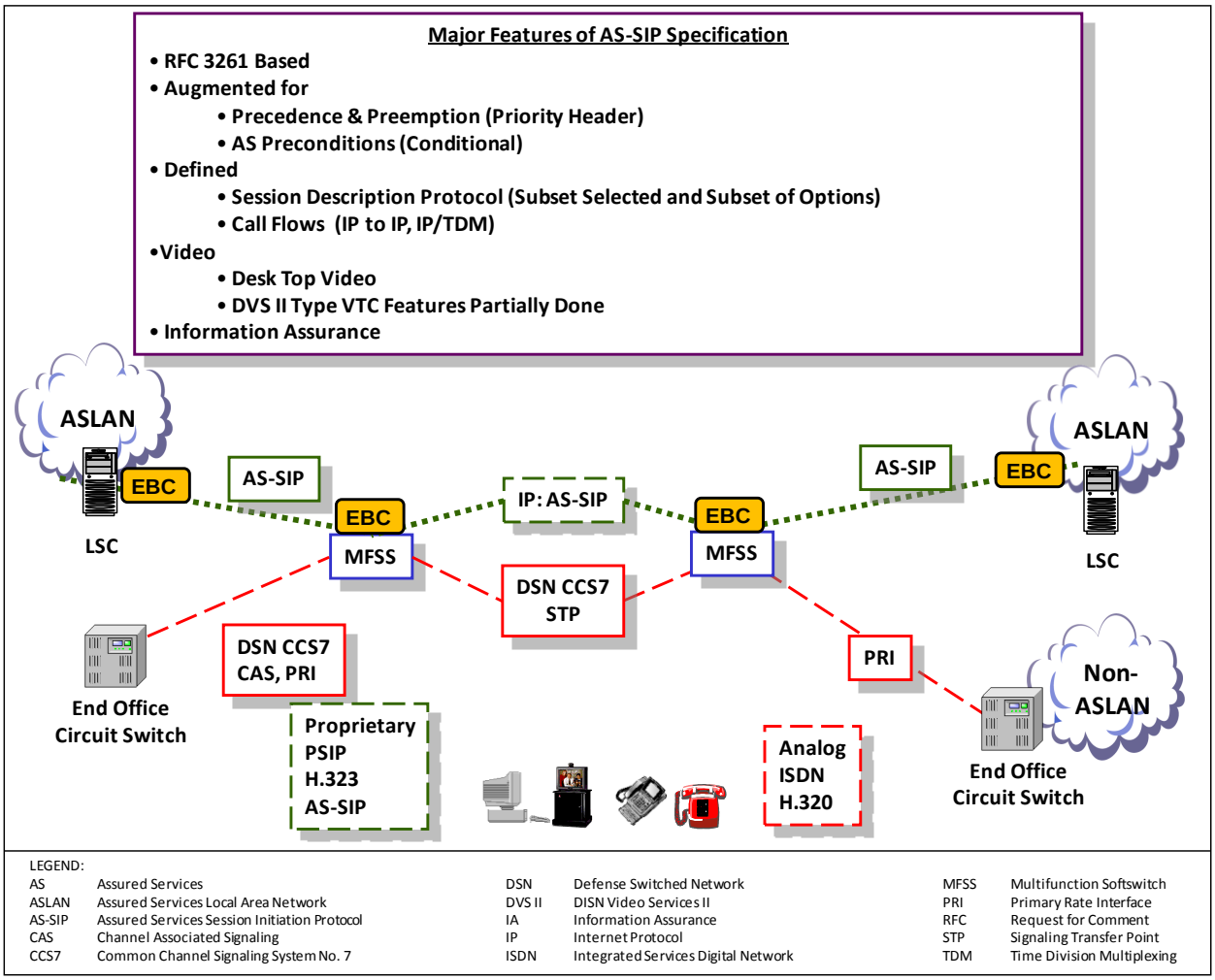


Figure 4.4.1-14. SBU Voice and Video Services Signaling Design

A stand-alone SS will support AS-SIP signaling in the classified VVoIP network. For SBU voice and video, on the edge of the DISN IP WAN cloud, an LSC on the B/P/C/S signals via AS-SIP to the network-level SS part of the MFSS. The TDM EOs signals via DSN CCS7 to the TDM switching part of the MFSS. The MFSSs use AS-SIP between themselves to set up IP-to-IP EI sessions across the DISN IP WAN.

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

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

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

- 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.
- The LSC and MFSS requirements.
- Signaling
  - A TDM EO will signal via DSN CCS7, PRI, or CAS to MFSSs.
  - The MFSSs will signal via CAS/PRI to the PSTN and to coalition gateways.

The LSC-to-LSC signaling without a network-level SS for other than deployed Joint Task Forces (JTFs) are under assessment. This assessment is necessary because this configuration has limitations with respect to managing traffic flows from the edge into the network for SA responses of the CYBERCOM NETOPS, and they have visibility limitations (except for cases involving intrabase where an LSC cluster with a master LSC is implemented or for some Services' Deployable Programs under Tailored Information Support Plans (TISPs)). Signaling from the LSC must pass through the network SS part of the MFSS or through a network-level SS so the MFSS/SS can implement Precedence-Based Network Management (PBNM) controls and police the proper use of access circuit bandwidth. For bases that have a collocated MFSS, base-level access to the local PSTN can be provided through the LSC portion of the MFSS. At the

network level, the MFSS will serve as the gateway to external networks, such as Services' Deployable Programs networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as CAS/PRI signaling.

The end-to-end, two-level SBU AS-SIP network signaling design is shown in Figure 4.4.1-15, End-To-End Two-Level SBU AS-SIP Network Signaling Design. For classified networks, the two-level signaling uses WAN SSs rather than MFSSs.

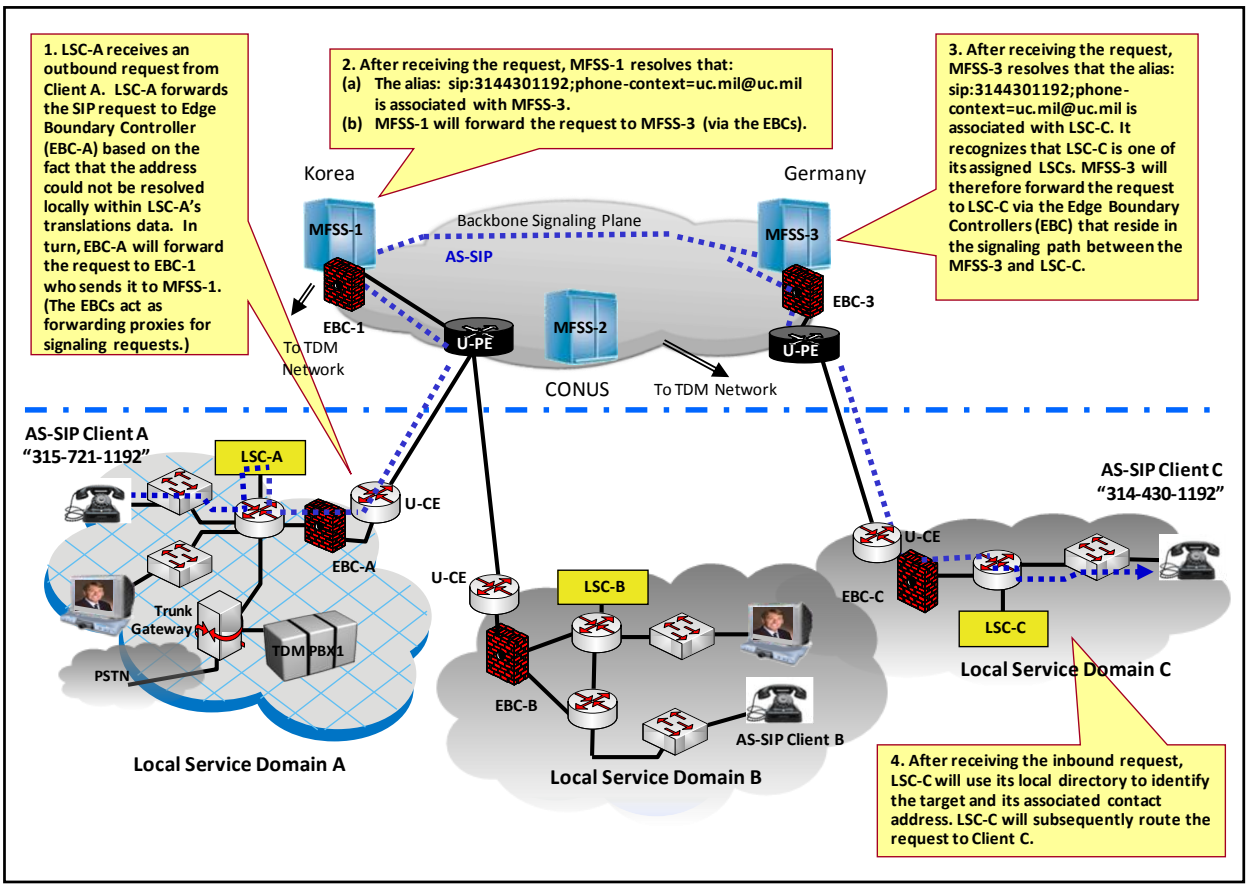


Figure 4.4.1-15. End-To-End Two-Level SBU AS-SIP Network Signaling Design

4.4.1.1.7 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 IA design is

necessary and is addressed in detail in Section 5.4, Information Assurance Requirements. The major components of the IA design include the protocols used, the interfaces of LSCs and MFSS to external control devices, and the design of the ASLAN. The methods for securing the VVoIP protocols are illustrated in Figure 4.4.1-16, Information Assurance Protocols. Key to the design is a hop-by-hop security model for trust between the signaling appliances using the DoD Public Key Infrastructure (PKI) for authentication.

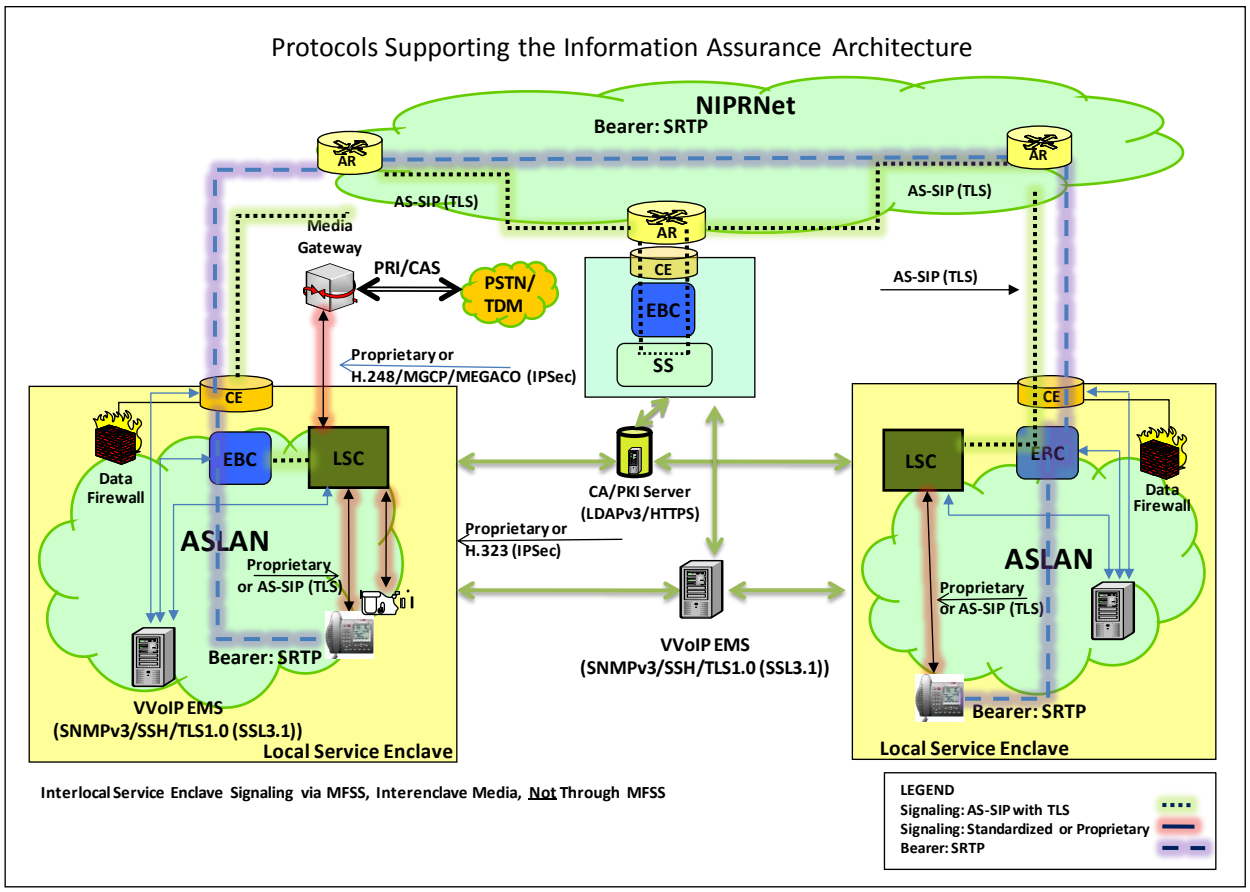


Figure 4.4.1-16. Information Assurance Protocols

Figure 4.4.1-17, 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 IA design uses access controls that may be configured to control traffic between interfaces.

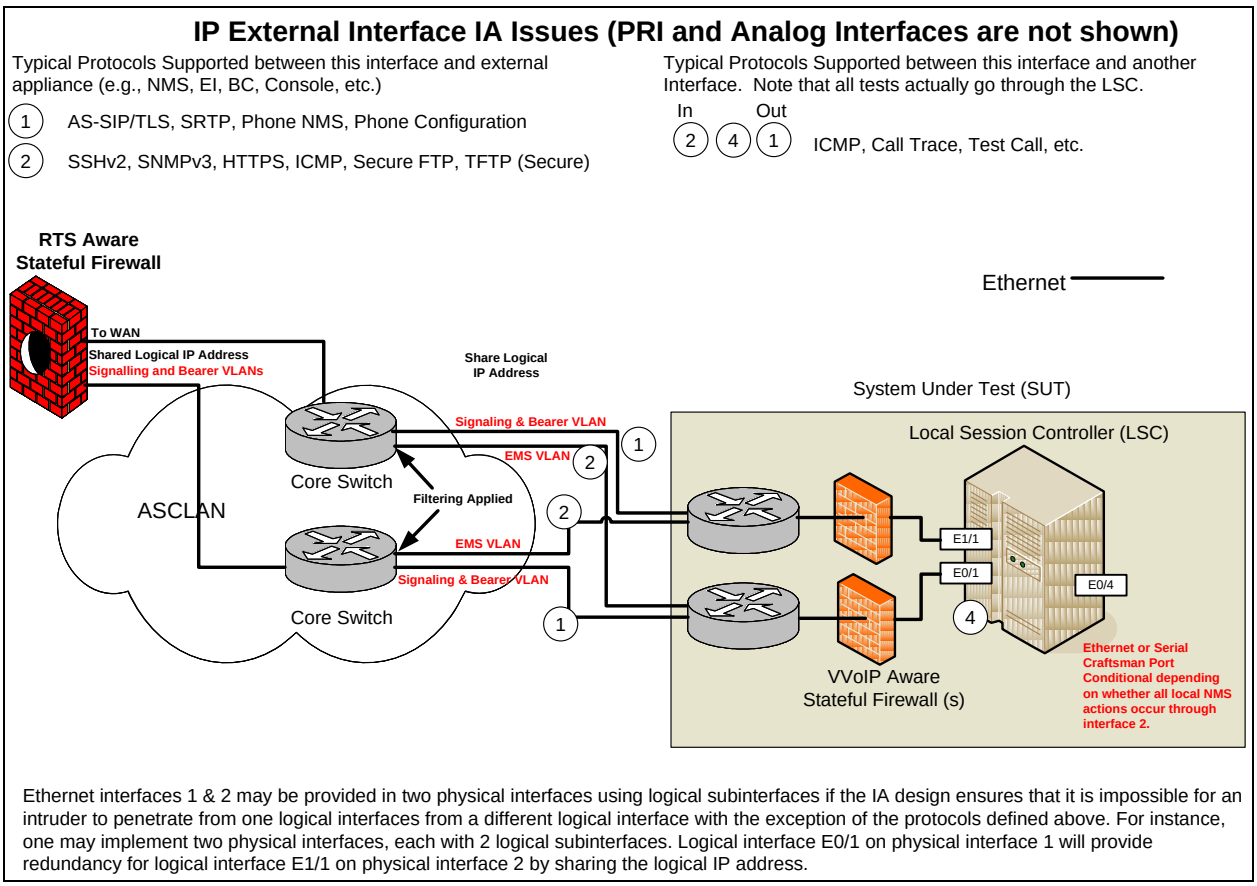


Figure 4.4.1-17. VVoIP Products External Ethernet Interfaces

Figure 4.4.1-18, ASLAN Enclave Boundary Security Diagram, depicts a diagram of the IA design needed as part of the ASLAN. The key feature of Figure 4.4.1-18 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice and/or video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice and/or video dynamic stateful AS-SIP aware application firewall, which provides Network Address Translation (NAT), MFSS failover, and port pinholes for individual voice and video sessions. A UC APL product called an EBC consisting of the voice and/or video firewall/border controller, has been defined and specified in Section 5.3.2, Assured Services Requirements.

The requirements for the IA 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.

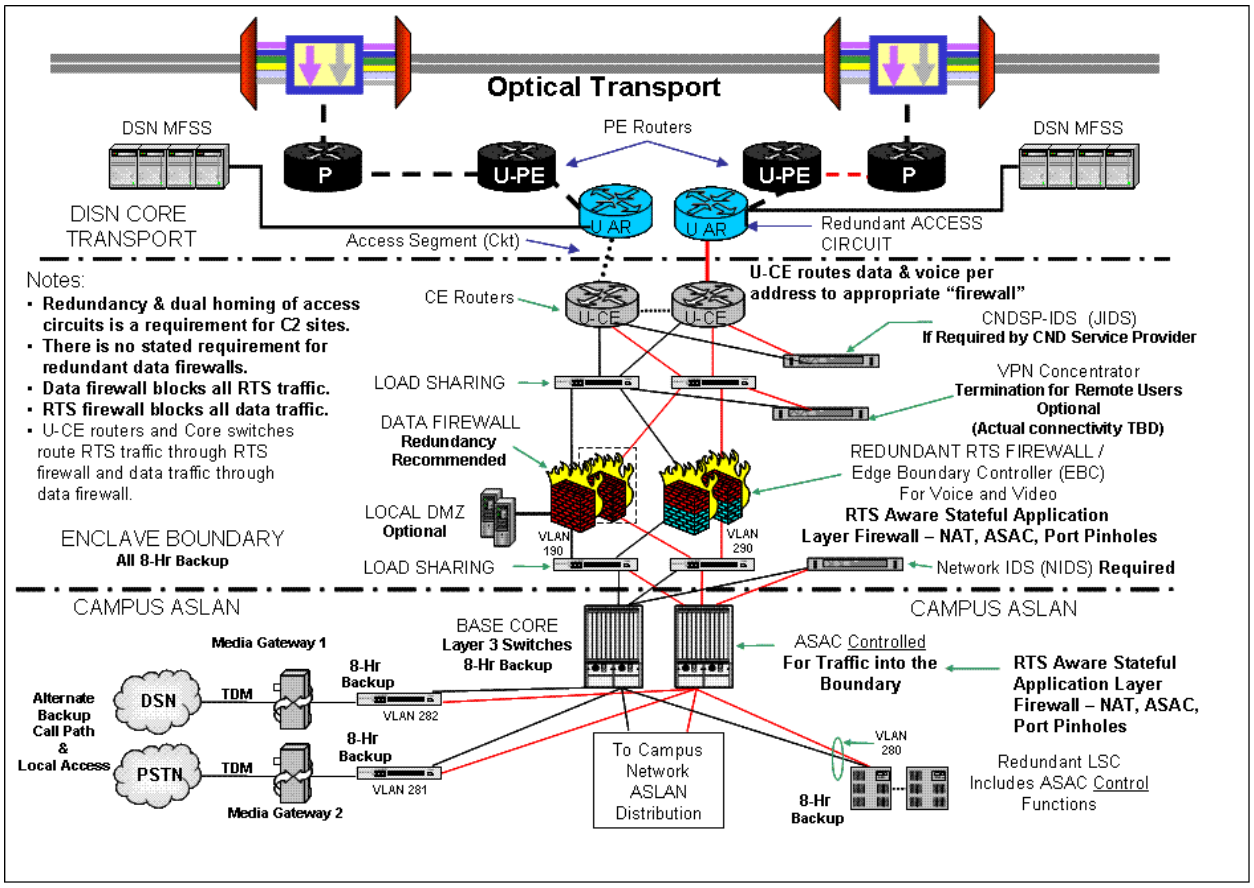


Figure 4.4.1-18. ASLAN Enclave Boundary Security Design

4.4.1.1.8 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 4.4.1-19, Role of RTS EMS in DISN OSS, where the EMS is shown at the bottom of the DISN OSS hierarchy.

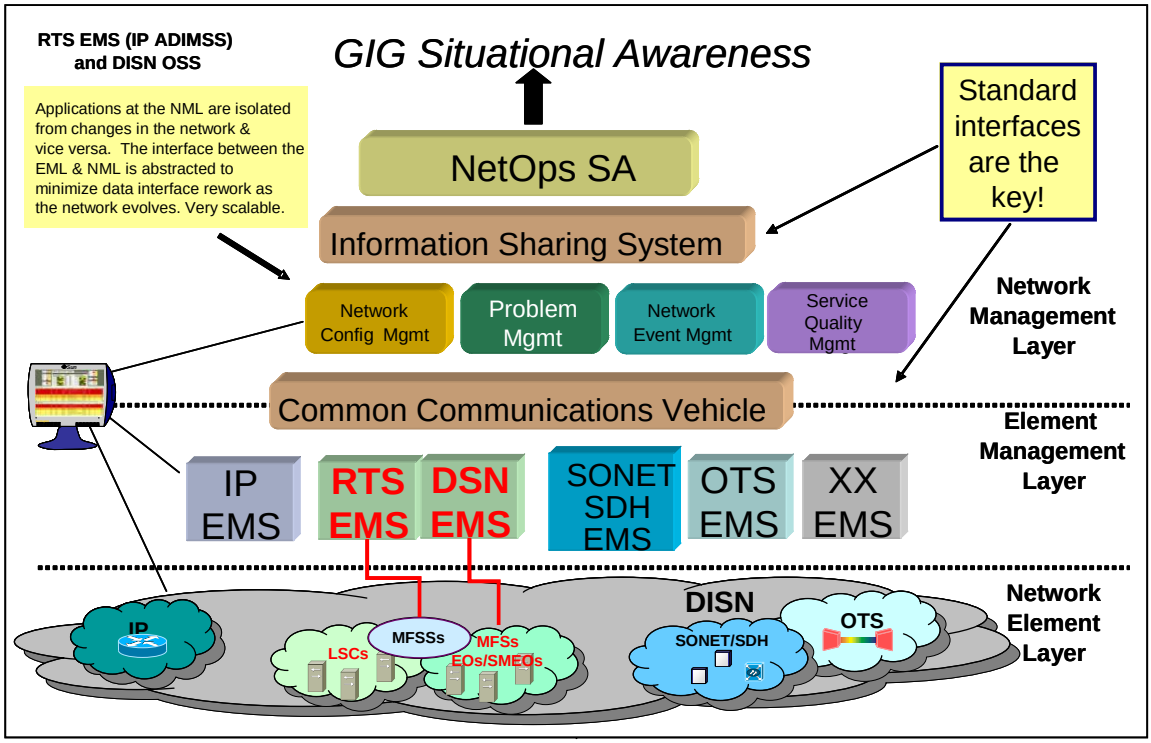


Figure 4.4.1-19. Role of RTS EMS in DISN OSS

In support of the Joint CONOPS for shared SA, and as an enabler of Net-Centric GIG Enterprise Management (GEM), the DoD Component EMS and RTS EMS must provide new 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 4.4.1-20, 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.

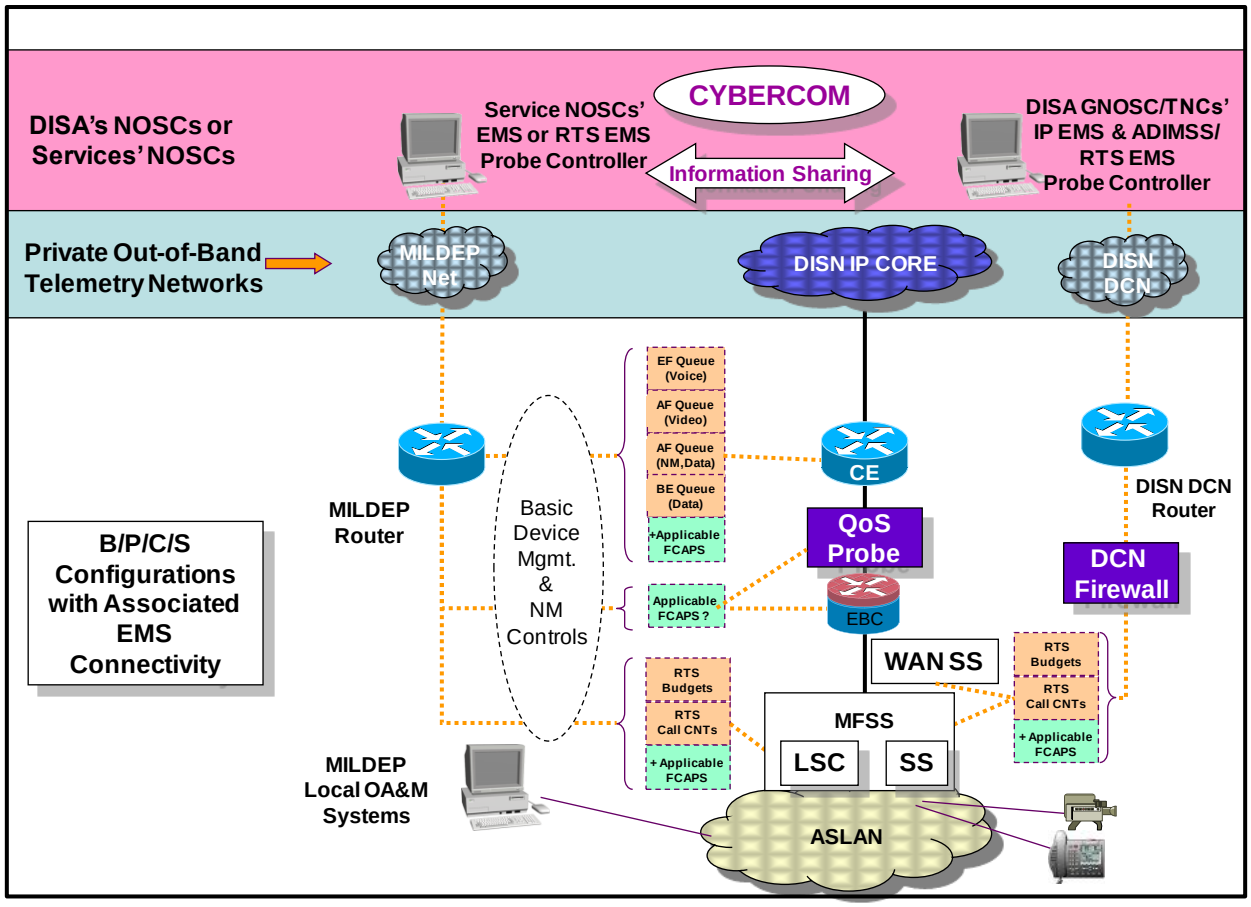


Figure 4.4.1-20. RTS EMS Role in Providing End-to-End GEM

4.4.1.1.9 Enterprise-wide Design

The enterprise-wide design is illustrated in Figure 4.4.1-21, DISN Enterprise UC Services Concept. This design consists of an Enterprise Service node location from which a centrally located LSC and Multipoint Conferencing Unit (MCU) provide UC service to several geographically separated local service enclaves. Note, the local service enclaves are separate security enclaves connected by the DISN Core. Access to the PSTN is provided directly from each local service enclave via remote media gateways controlled by the enterprise LSC. This design can provide a minimal footprint at the MILDEP level, offer savings in operations and maintenance (O&M) and space requirements, allow MILDEPS to invest in bandwidth and diversity in lieu of telecom equipment. The centralized design can provide a tighter integration with DISN enterprise collaboration, directory services, and conferencing offerings.

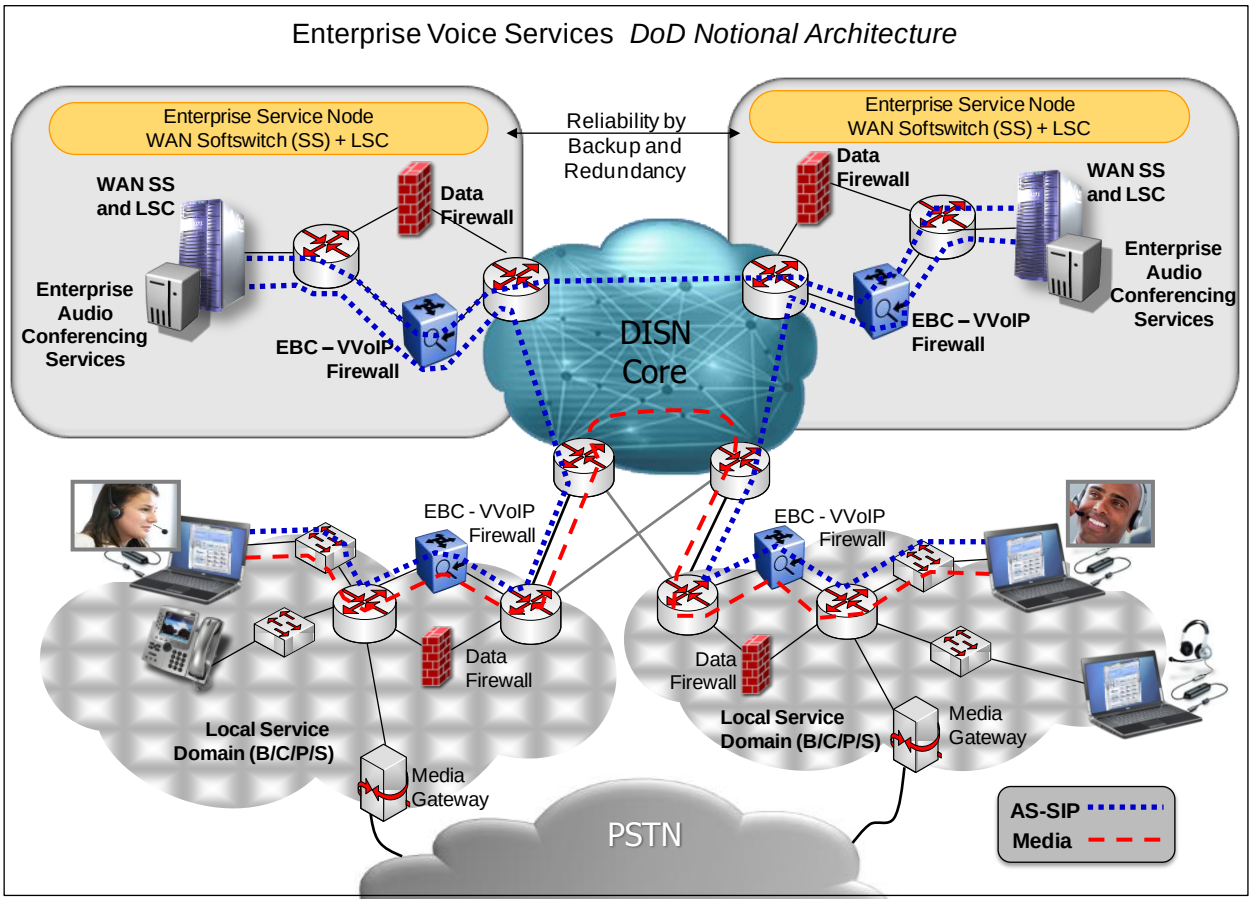


Figure 4.4.1-21. DISN Enterprise UC Services Concept

4.4.1.2 Classified VoIP Network Design

Figure 4.4.1.2-1, 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, which is described in Section 6.2, Unique Classified Unified Capabilities Requirements.

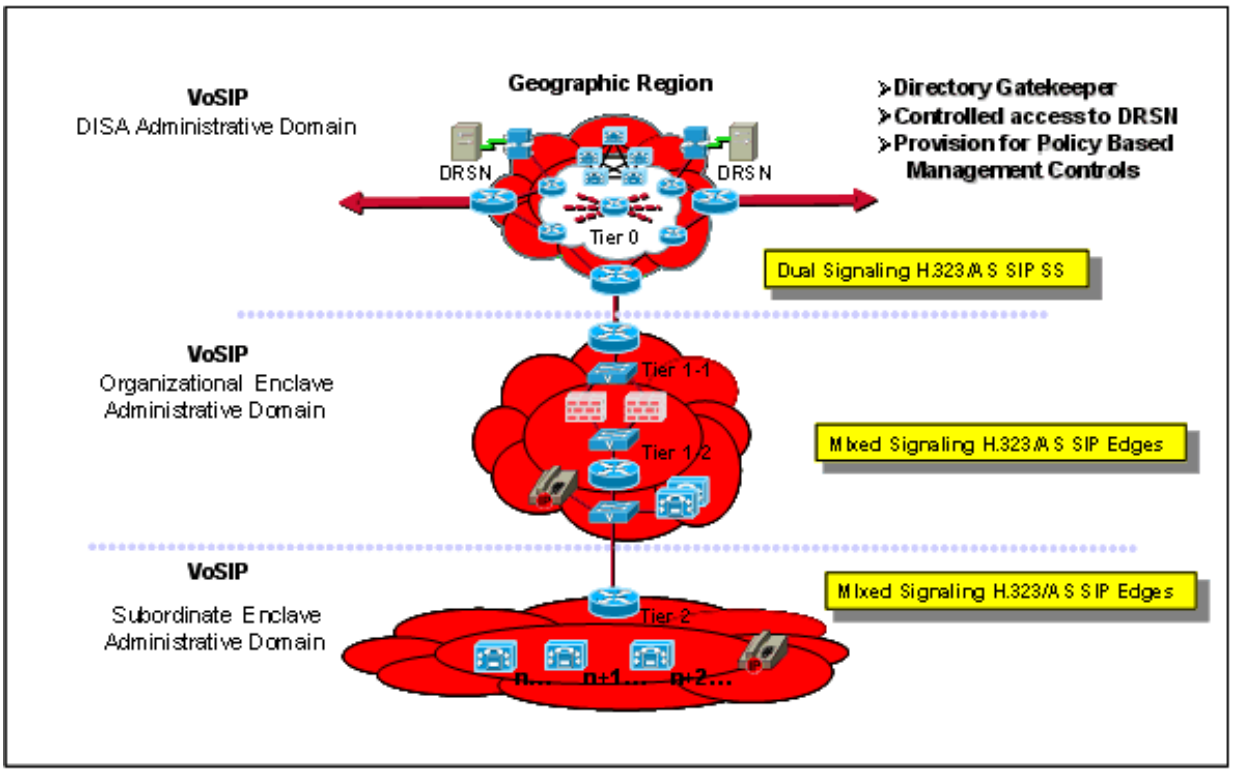


Figure 4.4.1.2-1. Classified VoIP Network Design Illustration

4.4.1.3 VTC Network Design

DISA provides VTC services as part of the DVS program for joint operations and the MILDEPs have their own VTCs for their unique COIs. The current Video Teleconferencing over IP (VTCoIP) end-to-end over both the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) does not provide assured services. The current DoD VTC services use an IP signaling protocol, called H.323 that does not provide assured services. They also support video using a TDM protocol, H.320. Due to DoD Components' budgetary constraints and because the VTCoIP technology insertion must be determined by site-by-site business cases, current versions of DVS VTC and MILDEP VTC technologies will provide voice and video services over the DISN for many years. Therefore, the current DVS and MILDEP VTCs, which use H.320 and H.323, will be supported during transition to AS-SIP. Three new conferencing solutions supporting a combination of AS-SIP, H.323 and H.320 will be introduced as shown in Figures 4.4.1.3-1, 4.4.1.3-2, and 4.4.1.3-3.

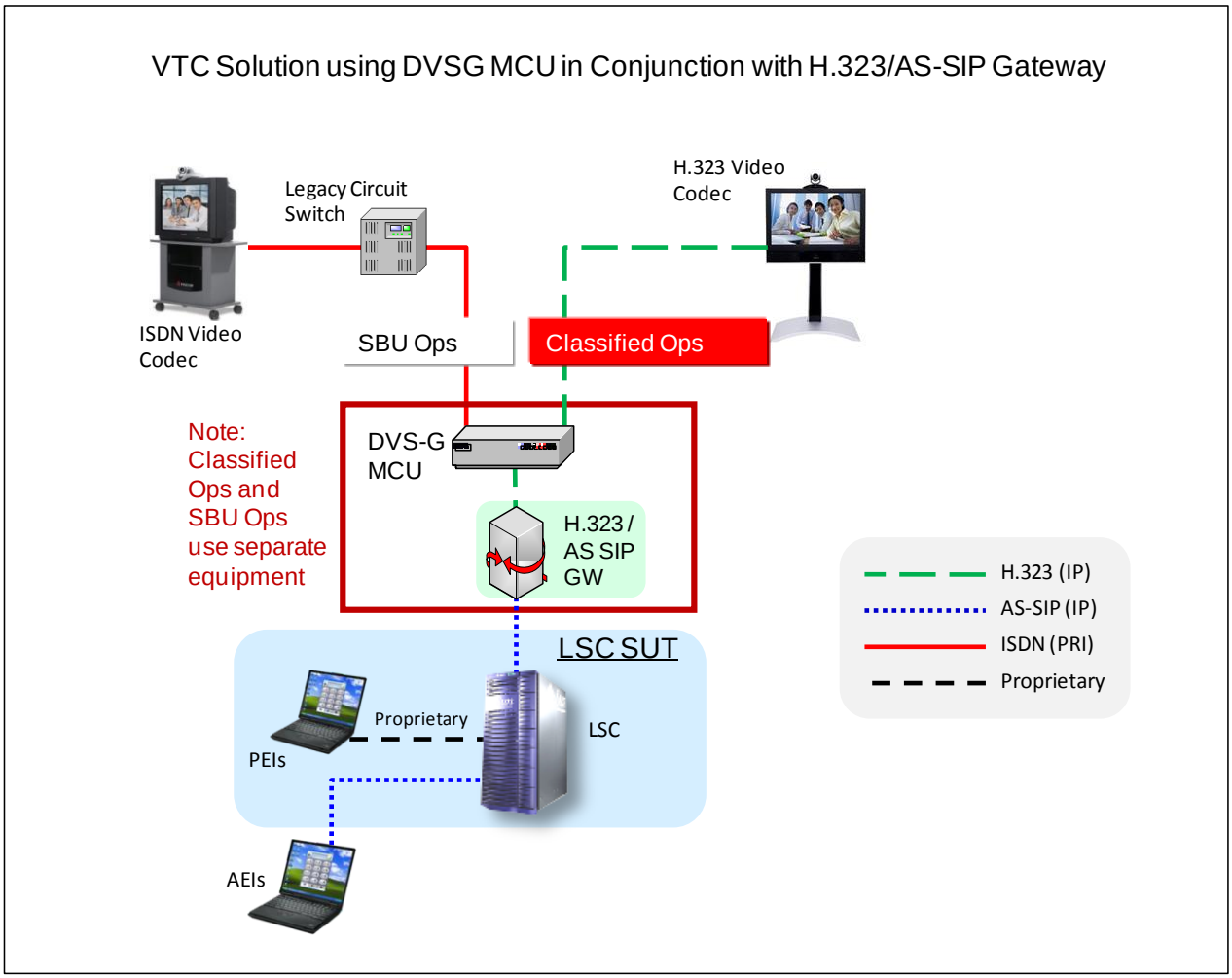


Figure 4.4.1.3-1. H.323/AS-SIP Gateway Conferencing Solution

The first solution, illustrated in Figure 4.4.1.3-1, uses a DISN Video Services – Global (DVS-G) MCU in conjunction with an H.323/AS-SIP Gateway. This solution can support all three protocols (AS-SIP/H.323/H.320). The LSC sends multiple AS-SIP sessions to the DVS-G MCU via the H.323/AS-SIP Gateway. For NIPRNet operation, the H.323 sessions have IA certification issues for transmissions across the WAN. The H.323/AS-SIP Gateway must be in the same security enclave as the DVS-G MCU. For SIPRNet operation, the H.323 sessions are IA certified.

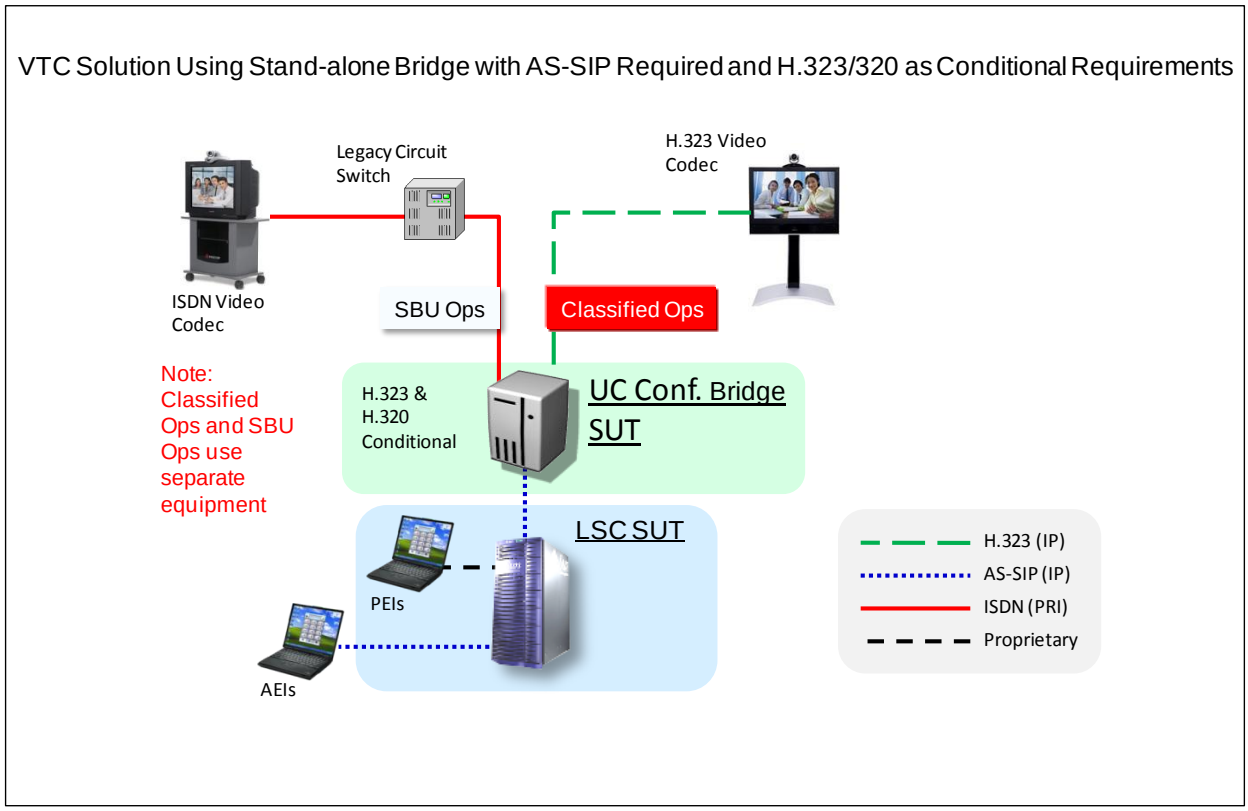


Figure 4.4.1.3-2. Conferencing Solution Using LSC and External Bridge with Conditional H.320/323 Support

The second VTC solution, illustrated in Figure 4.4.1.3-2, uses a standalone UC conference bridge. This conference bridge is required to support AS-SIP, and conditionally to support H.323 and H.320 endpoints. The signaling interface between the LSC and conference bridge is required to be AS-SIP. Market drivers will determine whether vendors choose to support conditional protocols.

The third VTC solution, illustrated in Figure 4.4.1.3-3, uses an LSC that contains a Conditional requirement for an internal conference bridge. In this solution, the interface between the conference bridge subsystem and the LSC may be proprietary or AS-SIP-based. The conference bridge function has a Conditional requirement to support H.323 and H.320 endpoints.

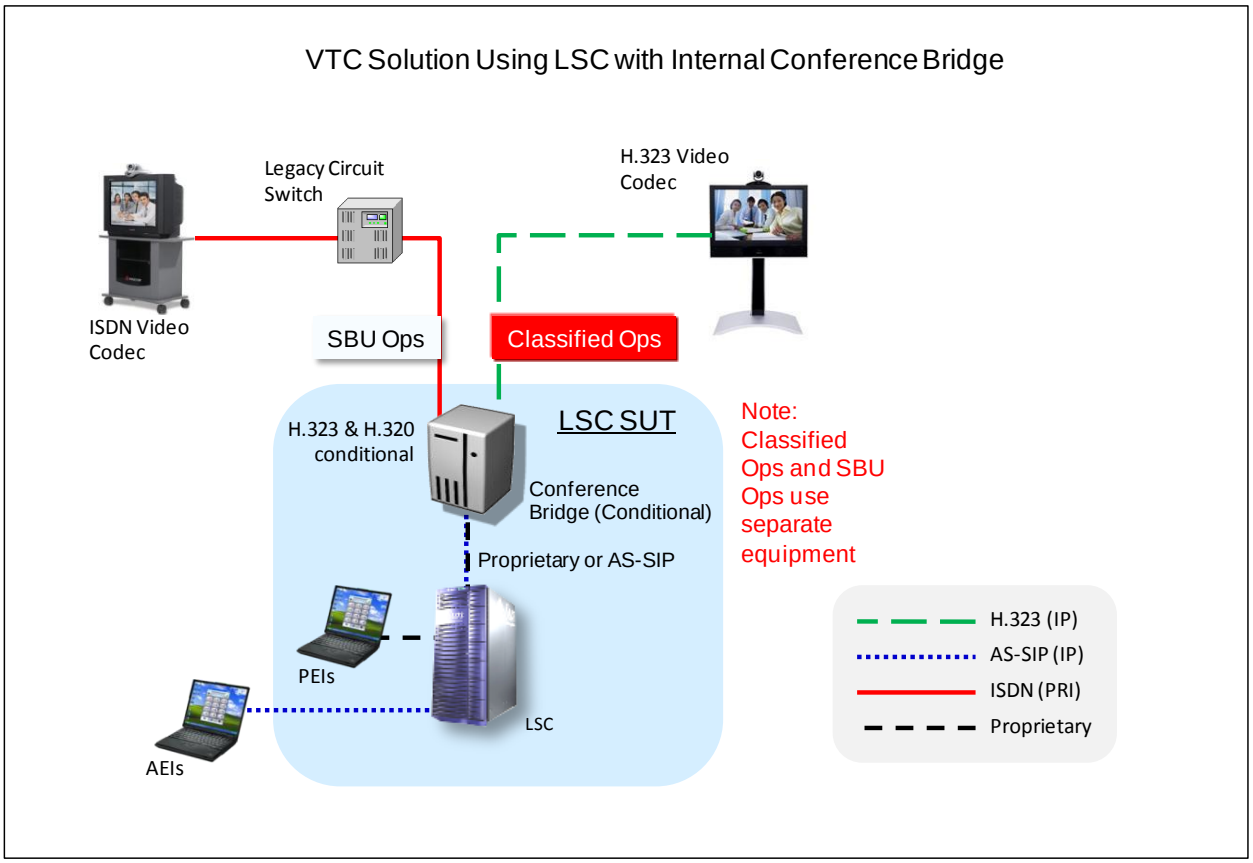


Figure 4.4.1.3-3. Conferencing Solution Using LSC with an Internal Bridge Function

4.4.1.4 DISN Router Hierarchy

Figure 4.4.1.4-1, DISN Router Hierarchy, illustrates the DISN router hierarchy for FY 2009 for both the unclassified network and the classified network. At this point, the NIPRNet and SIPRNet Routers have been transformed to be U-ARs and classified ARs connected to the unclassified Provider Edge (U-PE) Routers and classified Provider Edge (C-PE) Routers.

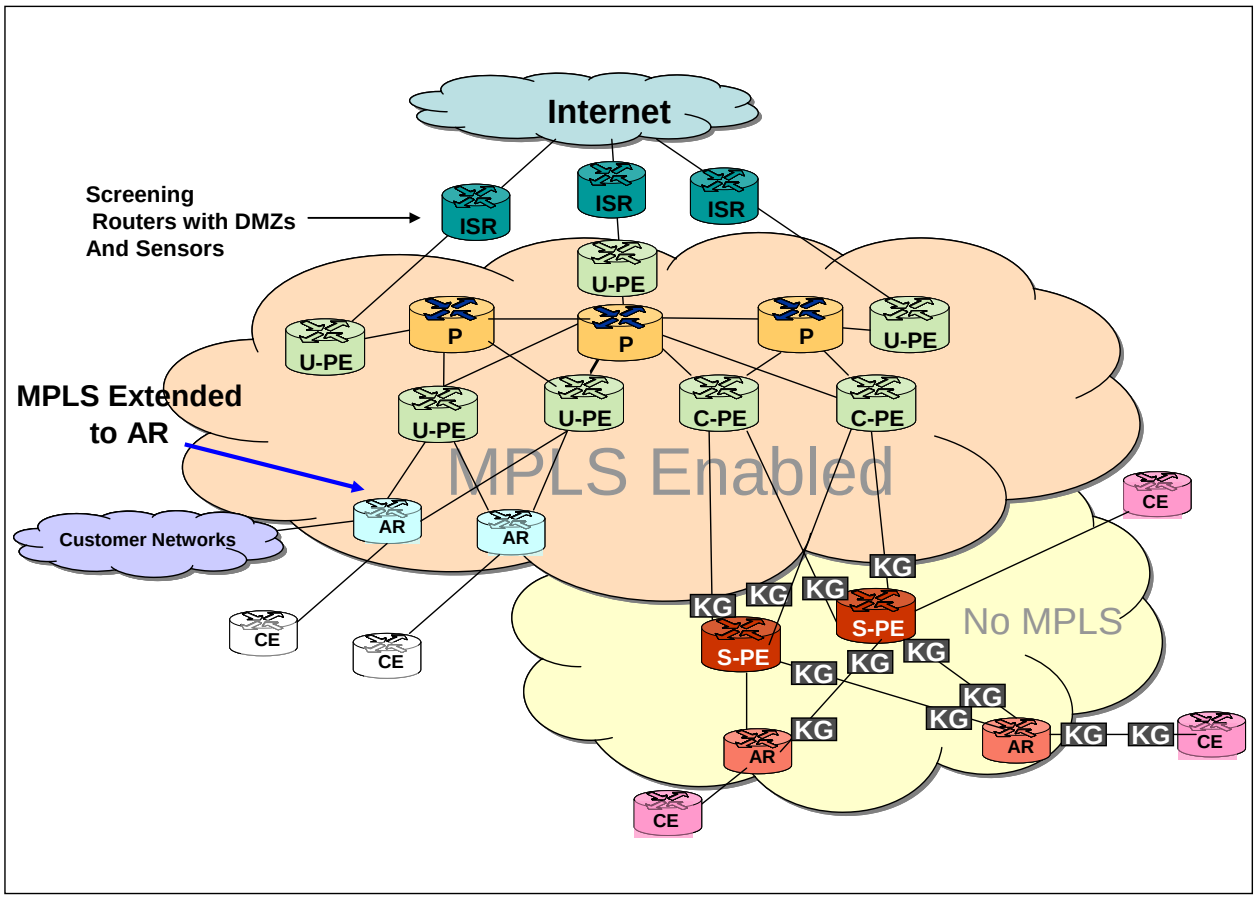


Figure 4.4.1.4-1. DISN Router Hierarchy

4.4.1.5 IPv6 Network Design

Figure 4.4.1.5-1, 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.

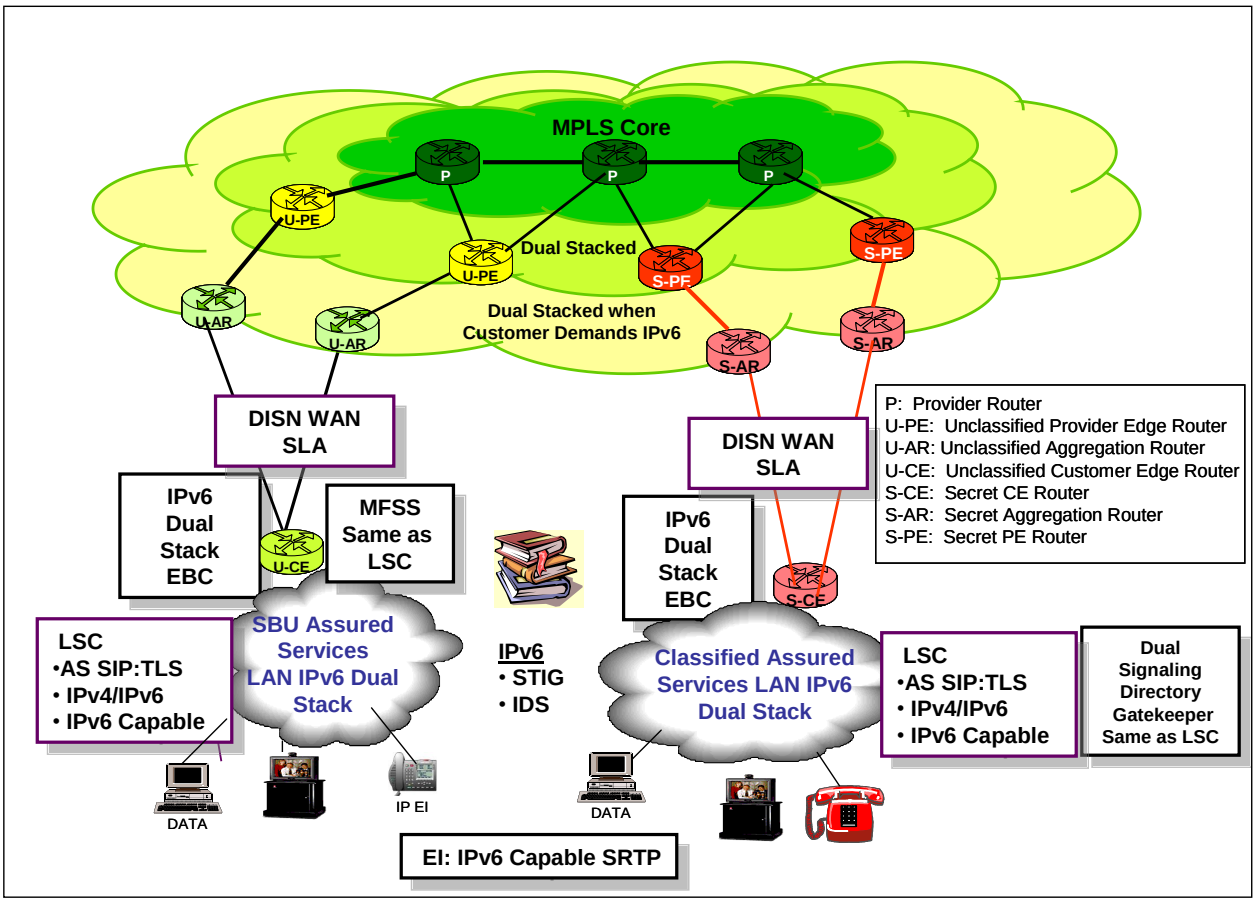


Figure 4.4.1.5-1. IPv6 Design for SBU and Classified VVoIP

4.4.2 Voice, Video, and Data Integrated Design for UC

Unified Capabilities 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.

4.4.2.1 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, intraenclave 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,

IA, 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 4.4.2.1-1, UC Network-Wide Collaboration Services Objectives.

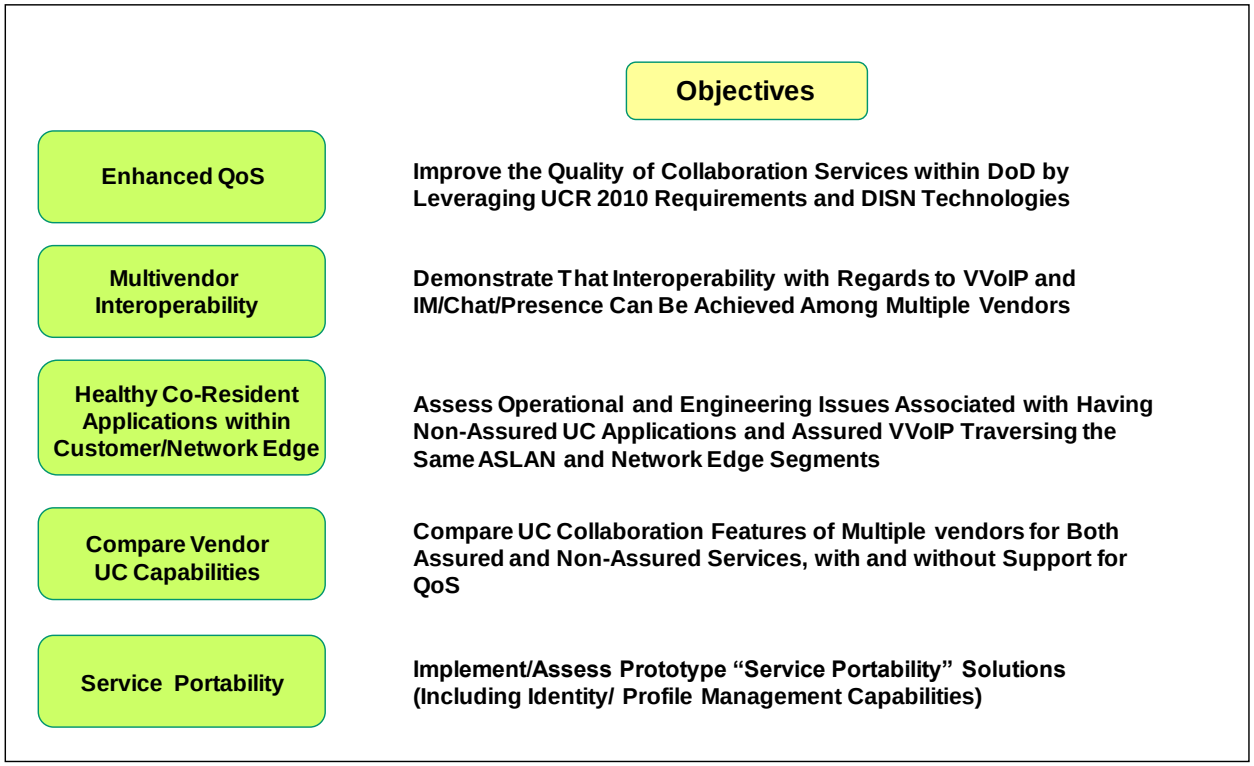


Figure 4.4.2.1-1. UC Network-Wide Collaboration Services Objectives

Figure 4.4.2.1-2, UC Pilot Increments, shows the near-term, mid-term, and long-term network-wide collaboration services capability increments. The initial increment moves forward with the testing of COTS UC solutions that are not capable of individually "class marking" IP packets consistent with the DSCP Plan shown in Section 5.3.3.3, General Network Requirements. Next, is the implementation and assessment of products that can mark individual flows (i.e., voice, video, IM/Chat) as belonging to a particular traffic class per 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.

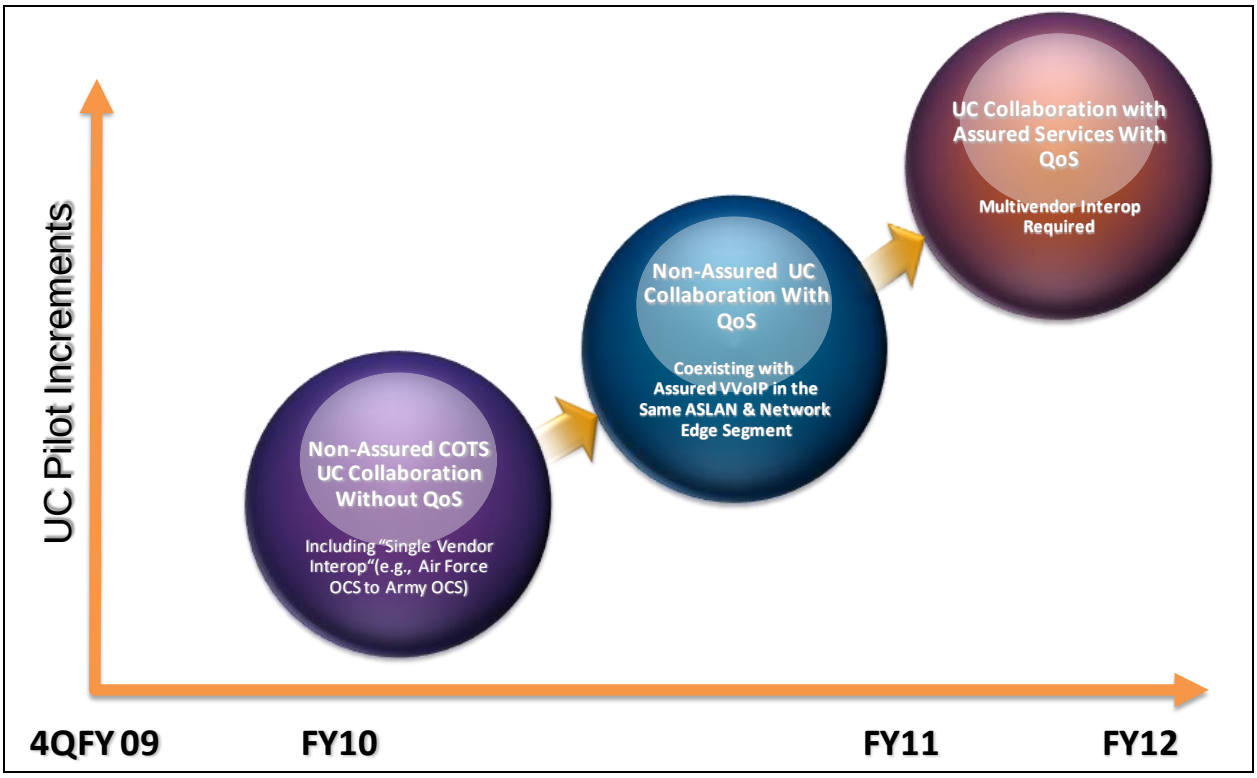


Figure 4.4.2.1-2. UC Pilot Increments

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

Figure 4.4.2.1-3, Interoperability/Federation of IM, Chat, and Presence, illustrates the following IM, Chat, and Presence demonstrations:

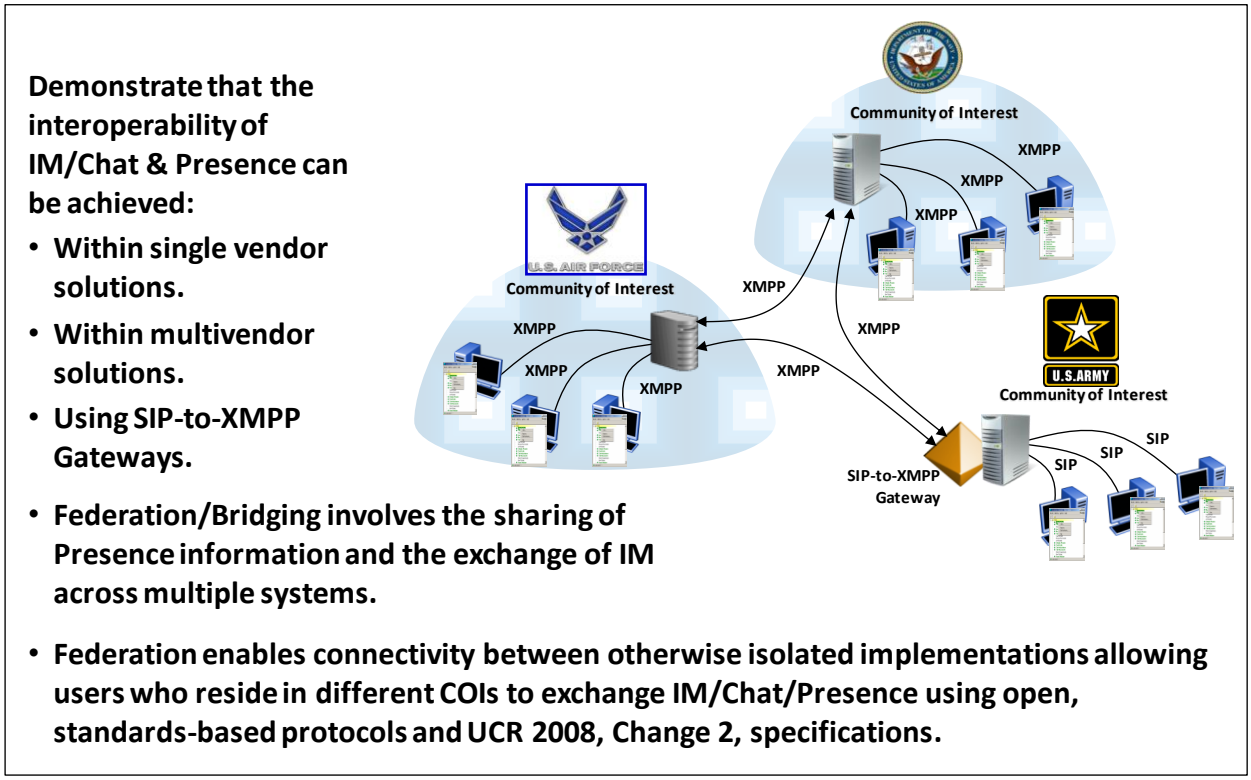


Figure 4.4.2.1-3. Interoperability/Federation of IM, Chat, and Presence

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

4.4.2.2 Integration of Voice, Video and Data Focused on Mobility

4.4.2.2.1 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 4.4.2.2-1, Mobile Warfighter's Communication Dilemma, shows the problem service portability is trying to solve.

Figure 4.4.2.2-1. Mobile Warfighter's Communication Dilemma

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

The near-term strategy is to deploy and assess prototype solutions in Spiral 1 and work with sponsoring MILDEPs to define test objectives, user requirements, and to resolve IA issues in order to complete an architecture. The lessons learned during Spiral 1 will be used to attain the mid-term strategy to incorporate the architecture and requirements into the UCR 2008, Change 2. Based on the vendors implementing the architecture and requirements within their products and systems, the long-term strategy is to test and field the products and systems within the Deployed and Fixed environments in the 2012–2013 timeframe.

4.4.2.2.2 Multifunction Mobile Devices

Multifunction Mobile Devices are a new top-level product category that will include product subcategories such as smartphones. This product category will primarily consist of COTS products with added IA requirements. See Section 4.5.1.4, Multifunction Mobile Devices Products, and Section 5.4, Information Assurance Requirements, for a more in-depth description of this product subcategory. The aspects of the smartphone, which are related to UC VVoIP functions, are generically defined as the "UC Smartphone Application." The requirements for non-UC VVoIP-related aspects of the smartphone (such as e-mail or Web-browsing) are generally defined by DISA Field Service Office (FSO) STIGs.

The UC Smartphone Application provides functionality that is similar to an EI or AS-SIP end instrument (AEI). However, unlike a traditional EI, the UC Smartphone Application operates within the confines of a STIG-compliant smartphone platform. The UC Smartphone Application uses the services of its homed LSC within the DoD enclave to establish VVoIP sessions; however, it establishes connectivity to the LSC via an intermediary called the Smartphone Backend Support System (SBSS). The SBSS provides security functions for the enclave such as access control, while simultaneously allowing the smartphone access to protected resources (like the LSC) within the DoD enclave. The SBSS may also support e-mail access and other functions, which are not defined in the UCR, but by DISA FSO STIGs as well. The SBSS's ability to support UC VVoIP services is a Conditional requirement.

Connectivity from the UC Smartphone Application to the SBSS is expected to occur in a secure manner. Two approaches are currently permissible for connecting back to the SBSS from the UC Smartphone Application. One approach is when the SBSS uses "back-to-back user agent" functionality to establish sessions on behalf of served UC Smartphone Applications. The other is when a VPN tunnel protects the VVoIP media and signal transmitted from the UC Smartphone Application. (Note that "VPN" does not necessarily denote Internet Protocol Security (IPSec) because a number of tunneling techniques at various levels of the Open Systems Interconnect (OSI) stack could be used depending on the operational environment.) These approaches were selected to allow the vendors maximum flexibility when designing solutions for specific wireless technologies or bandwidth/performance constraints. See Section 5.4, Information Assurance Requirements, for more detail on the interaction between the UC Smartphone Application and the SBSS.

4.4.3 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 three 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.

- At the network (backbone) level, calls originating as IP shall remain IP as far as possible toward the terminating end; calls originating as TDM shall remain TDM as far as possible toward the terminating end.

The three 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 4.4.3.1, 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.

4.4.3.1 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 RTS end users served by RTS 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 RTS LSCs, whenever an end user's 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 RTS LSC site or DSN EO or PBX site.

The RTS 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). 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 an RTS call that enters the WAN SS or MFSS.

The protocol that LSCs, MFSSs, and WAN SSs use to query and update the RTS Routing DB is Lightweight Directory Access Protocol Version 3 (LDAPv3), secured using Transport Layer Security (TLS), and signaled via IP over the DISN WAN. In general, the RTS Routing DB is located at a centralized DISA site that is physically separate from the LSC site, the MFSS site, or the WAN SS site.

4.5 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 get the products placed on the APL and processes needed to gain connection approvals for the products. More information is available at http://www.disa.mil/ucco/.

4.5.1 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 information technology (IT) products are required to be on the APL. The DoD UC Steering Group (UC SG) advises ASD(NII)/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 ASD(NII)/DoD CIO must be on the APL for DoD Components to acquire them. Products not listed on the UC APL cannot be acquired by DoD Components. 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 4.5.1-1, 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.

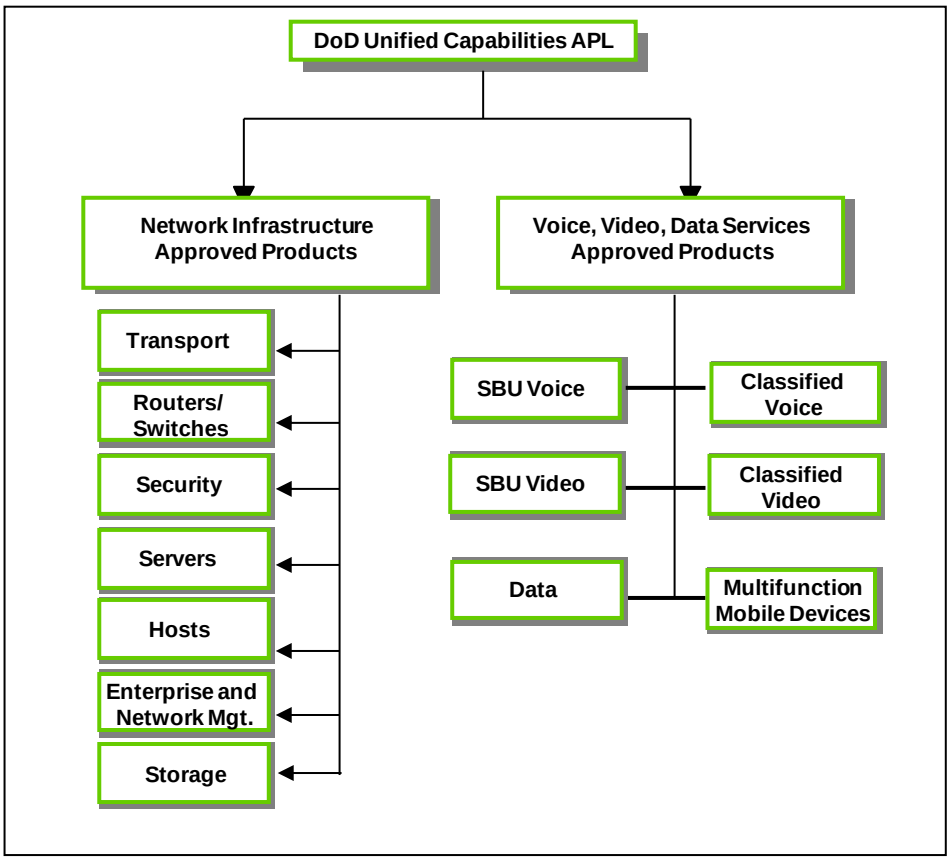


Figure 4.5.1-1. Overview of UC Product Categories within the DoD UC APL

4.5.1.1 Network Infrastructure Approved Products

Tables 4.5.1.1-1 through 4.5.1.1-5 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 HAIPE discovery servers will not be included in this version of the UCR.

Table 4.5.1.1-1. Transport Appliances

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
AGF Device	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
Access Aggregation Function M13 Device	5.5 (Network Infrastructure Product Requirements)	Product that functionally multiplexes DS1s into a DS3
OTS	5.5 (Network Infrastructure Product Requirements)	Switching product providing high-speed optical transport in the DISN WAN
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 4.5.1.1-2. Router/Switches

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Aggregation Router	5.5 (Network Infrastructure Product Requirements)	Product serving as a port expander for a PE Router
Provider Edge Router	5.5 (Network Infrastructure Product Requirements)	Product providing robust, high-capacity IP routing at the entry points to the DISN WAN
Provider Router	5.5 (Network Infrastructure Product Requirements)	Product providing robust, high-capacity IP routing in the DISN WAN
Customer Edge Router	5.3.2 (Assured Services Requirements)	Product providing IP routing toward the DISN WAN at a Customer Edge
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

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Distribution IP Switch	5.3.1 (Assured Services Local Area Network Infrastructure)	Product used in a LAN to provide an intermediate switching layer between a 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

LEGEND

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

Table 4.5.1.1-3. 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 IA 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.

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Integrated Security Solution	5.8 (Security Devices Requirements)	A product that provides the functionality of more than one IA device in one integrated device.
Information Assurance Tools	5.8 (Security Devices Requirements)	Products that provide IA functions.
Network Access Control	5.8 (Security Devices Requirements)	Products that provide IA functions.

LEGEND

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

Table 4.5.1.1-4. 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 4.5.1.1-5. 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

4.5.1.2 Voice, Video, and Data Services Approved Products

Table 4.5.1.2-1, SBU Voice, lists the products in the SBU UC Voice Product category.

Table 4.5.1.2-1. 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 architecture. 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.
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 4.5.1.1-3, 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.

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
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.

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 4.5.1.2-2, Classified Voice, lists the products in the classified UC voice product category.

Table 4.5.1.2-2. 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 4.5.1.2-1, 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

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
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 4.5.1.2-3, SBU Video, lists the products in the SBU UC video product category.

Table 4.5.1.2-3. 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 4.5.1.2-1, 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 4.5.1.2-1, SBU Voice
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 4.5.1.2-1, 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

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
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 4.5.1.2-4, Classified Voice, lists the products in Classified UC Video Product Category.

Table 4.5.1.2-4. Classified Video

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
LSC	6.2 (Unique Classified Unified Capabilities Requirements)	Same product as inTable 4.5.1.2-1, 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

4.5.1.3 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 those cases, the interface is specified for interoperability but the performance (e.g., response time, screen refresh rate) of the applications are not specified currently. 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 4.5.1.3-1, Data Category Products, lists the data category products.

Table 4.5.1.3-1. 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		

4.5.1.4 Multifunction Mobile Devices Products

The UC APL now includes the Multifunction Mobile Device High-Level Product category. The subcategories of products placed under Multifunction Mobile Device may include a wide range of advanced mobile computing platforms as this category evolves. Currently, this category contains only one subcategory called Smartphones. Even though smartphones are considered wireless, handheld computing devices that provide services beyond minimal telephony, in the context of the UCR, the term “smartphone” can also refer to devices that take a number of form factors and use different names. These form factors and names include “mobile phone,” “wireless tablets,” “personal digital assistants,” or other devices providing “smartphone-like” capabilities. The requirements for the non-UC VVoIP-related functionality (e.g., e-mail, web-browsing) provided by the Smartphone subcategory are defined within DISA FSO STIGs, STIG checklists, and security requirements matrices. Though these requirements are tested by the appropriate DoD Laboratory, a part of the Unified Capabilities Connection Office (UCCO) process, these requirements are not duplicated in the UCR. The requirements for smartphones 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 Smartphone Applications," which provide this type of functionality.

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

Security requirements, rather than functional requirements, are specified for these devices. Table 4.5.1.4-1, Multifunction Mobile Devices, lists the multifunction mobile devices.

Table 4.5.1.4-1. Multifunction Mobile Devices

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTION
Smartphone	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
Smartphone Backend Support System (SBSS)	5.4 (Information Assurance Requirements)	An appliance or collection of appliances that allows remotely connected smartphones to access services within a DoD enclave, provides access control and remote management, while maintaining or enhancing the security posture of the network

4.5.1.5 Deployable UC Products

Table 4.5.1.5-1, Deployable UC Products and Paragraph References, delineates the deployable UC products. These products are based on configuring and installing UC products in a deployed environment. Table 4.5.1.5-1 does not list "legacy" deployable products that are found in UCR 2008.

Table 4.5.1.5-1. Deployable UC Products and Paragraph References

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	6.1.3 (Deployed Voice Quality)	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
DVX-C Deployable Voice Exchange – COTS
NE Network Element
DCVX Deployed Cellular Voice Exchange
LAN Local Area Network

4.5.2 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 4.5.2-1, Distributed Testing CONOPS.

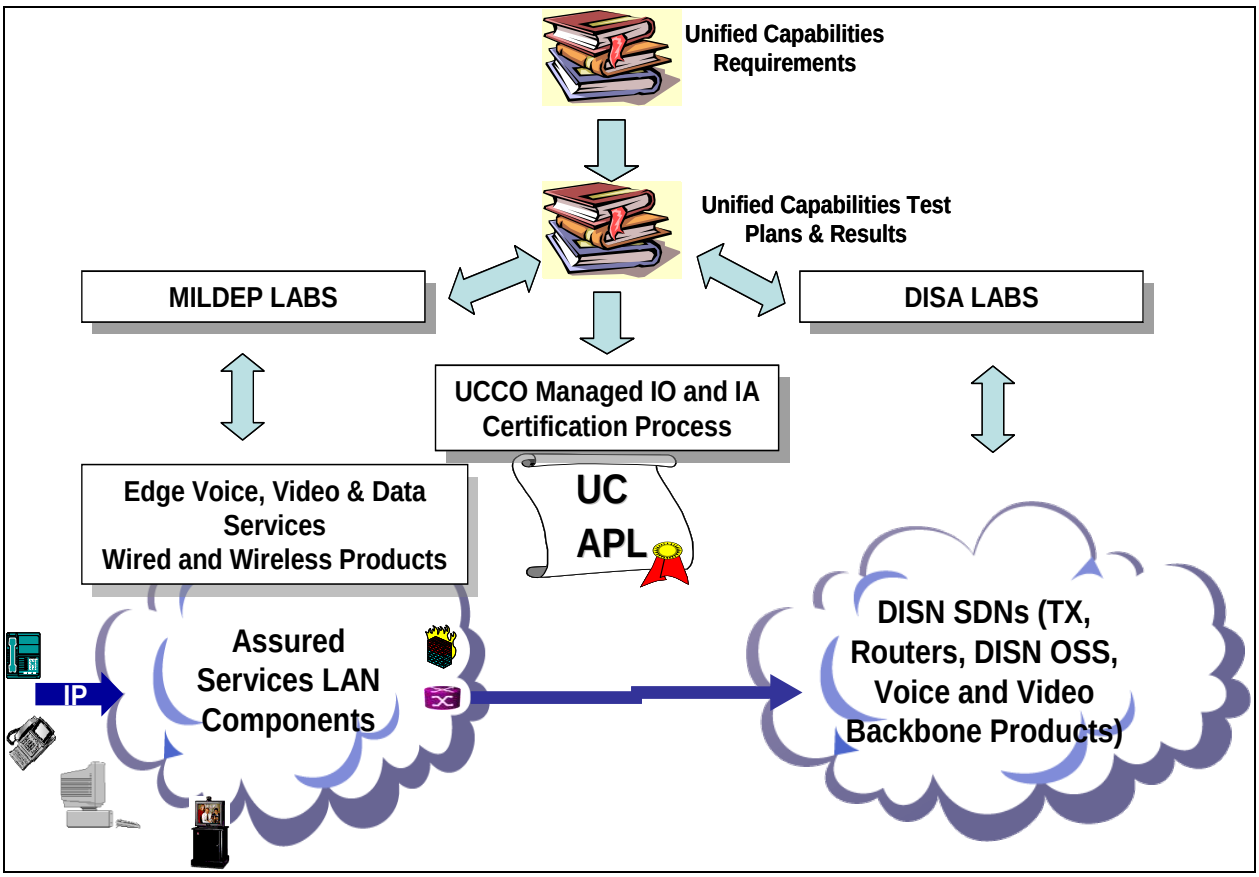


Figure 4.5.2-1. Distributed Testing CONOPS

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 4.5.2-1, UC Test Requirements. The Director, DISA, in coordination with the ASD(NII)/DoD CIO shall resolve issues in interpretation and use of this table.

Table 4.5.2-1. UC Test Requirements

SERVICES COMPLEXITY	TECHNOLOGY MATURITY			
	PROTOTYPE	PRE-PRODUCTION	APL READY	POST APL
ASFs	• Full Test • Or incremental test and/or desk-top 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 letter of compliance (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 letter of compliance (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 letter of compliance (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 letter of compliance (LOC) of vendor tests of non ASFs meeting brochure claims

SERVICES COMPLEXITY	TECHNOLOGY MATURITY			
	PROTOTYPE	PRE-PRODUCTION	APL READY	POST APL
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
APL Approved Products List
ASF Assured Services Features
DTR Desk-Top-Review
LOC Letter of Compliance

4.5.3 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) 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 4.5.2-1, UC Test Requirements, in Section 4.5.2, 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.

4.5.3.1 Standard Process for Gaining UC APL Status

The standard process for gaining APL status for all UC products is shown in Figure 4.5.3-1, Standard UC APL Product Certification Process. This process reflects that both interoperability and IA certifications are required for placement on the UC APL.

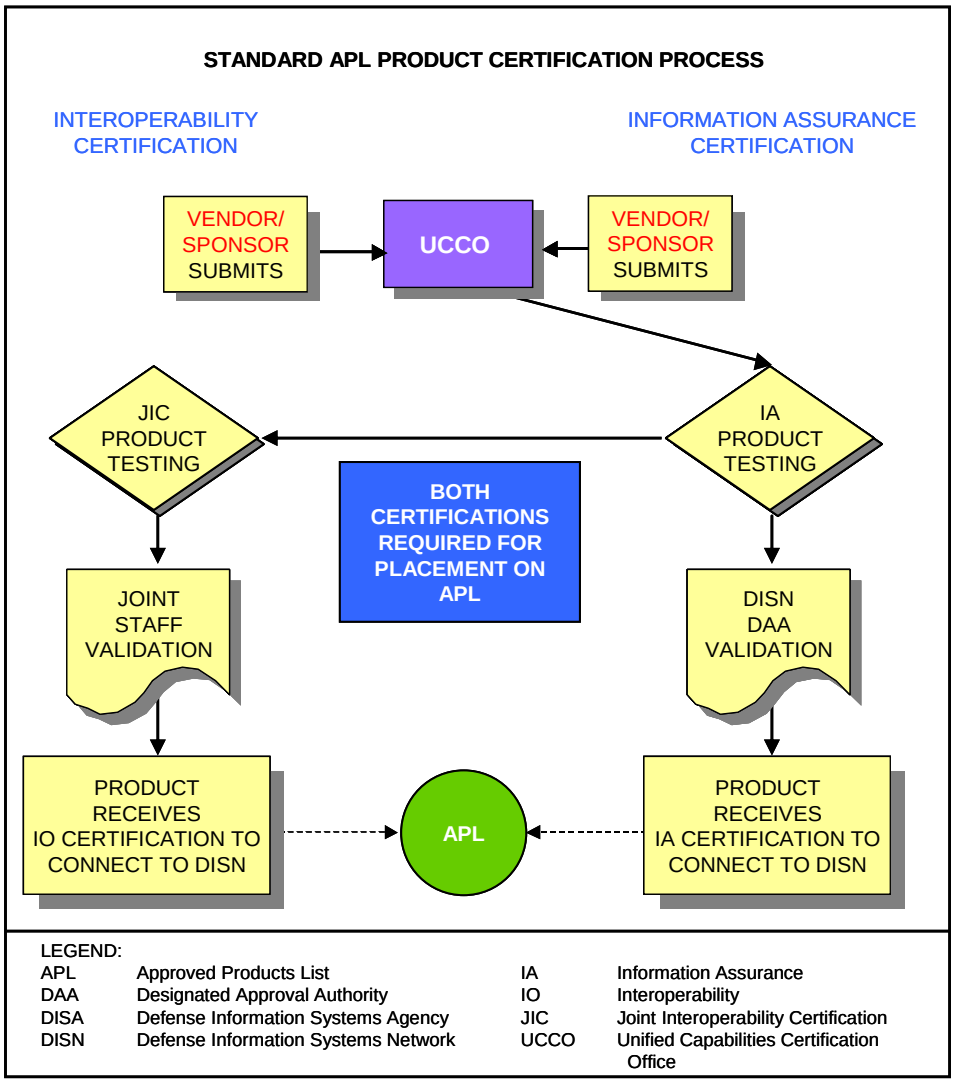


Figure 4.5.3-1. Standard UC APL Product Certification Process

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. They will continue to be allowed to operate in the network. Exceptions to this policy will be submitted through the appropriate channels for ASD(NII)/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 IA information as shown in Figure 4.5.3-1.

- If a product successfully passed both Interoperability and IA 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 IA risk, compliance is immediate.

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

The 18-month period for development would apply to a new feature or a product not previously required, and the vendors did not have long-range knowledge of the requirement. New features or products in this version of the UCR are included in Table 4.5.3-1, New Features and Products in UCR 2008, Change 2, for Which the 18-Month Rule Applies.

Table 4.5.3-1. New Features and Products in UCR 2008, Change 2 for Which the 18-Month Rule Applies

FEATURES	SECTION OF THE UCR
Smartphone	4.4.2.2.2
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 IA 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 which changes are subject to the 18-month rule and which ones are not.

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 that are currently fielded and successfully performing from both an interoperability and IA 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/overview/index.html.

4.5.3.2 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 that 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 T&E

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

b. If the DoD Component/sponsoring agency/fielding authority desires to field the UC product with the UCR deficiencies identified during T&E, then 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).