Department of Defense

Unified Capabilities Framework 2013
(UC Framework 2013)

January 2013

The Office of the DoD Chief Information Officer

DEPARTMENT OF DEFENSE

UNIFIED CAPABILITIES FRAMEWORK 2013 (UC FRAMEWORK 2013)

TABLE OF CONTENTS

LIST OF FIGURES

SECTION 1
INTRODUCTION AND UC DESIGN OVERVIEW

1.1   PURPOSE

The Department of Defense (DoD) Unified Capabilities Framework 2013 describes the technical framework for DoD networks that provide end-to-end (E2E) Unified Capabilities (UC).

The UC Framework is one of the documents that make up the UCR Family of documents as illustrated in Figure 1.1-1. The other UCR 2013 documents include the following:

- The UCR 2013 specifies the functional requirements, performance objectives, and technical specifications for products 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 (IA), and interface requirements among products that provide UC.

- The Assured Services Session Initiation Protocol (AS-SIP) 2013 contains requirements for the Internet protocol (IP)-based UC Signaling system.

- The UC Extensible Messaging and Presence Protocol (XMPP) 2013 contains requirements for multivendor interoperability as required to exploit the full potential of Instant Messaging (IM), Chat, and Presence across the DoD.

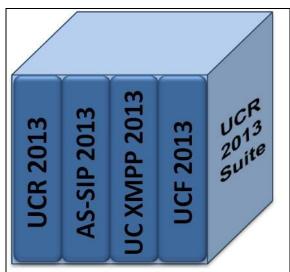- UC Framework 2013 – specifies the descriptive text and design associated with each of the UCR 2013 sections.

Figure 1.1-1. UCR Document Family

1.2 APPLICABILITY AND SCOPE

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

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

1.3 DOCUMENT OVERVIEW

The UC Framework consists of the following sections:

- Section 1, Introduction and UC Design Overview, describes the purpose, applicability, and scope for the UC Framework. A short synopsis of UC network infrastructure is also included.

- Section 2, Session Control Products, describes the UC network infrastructure in terms of network engineering attributes, and designs.

- Section 3, Auxiliary Services, describes miscellaneous features and interfaces to the UC network.

- Section 4, Information Assurance, provides an overview of IA requirements.

- Section 5, IPv6, summarizes requirements for IPv6 implementation.

- Section 6, Network Infrastructure End-to-End Performance, describes latency, jitter, and packet loss performance parameters required by the network segments to meet requirements for the Defense Information Systems Network (DISN) service classes.

- Section 7, Network Edge Infrastructure, describes designs for the Customer Edge network segment.

- Section 8, Multifunction Mobile Devices, describes arrangements for supporting mobile devices.

- Section 9, Video Distribution System, describes designs for H.320, H.323, and AS-SIP-based Video Teleconferencing (VTC) systems.

- Section 10, Network Infrastructure Products, describes current DISN Services and arrangement of products in the network infrastructure.

- Section 11, Network Elements, describe requirements and application of various network elements.

- Section 12, Generic Security Devices, provides a synopsis of encryption devices.

- Section 13, Security Devices, provides a synopsis of security devices.

- Section 14, Online Storage Controller, describes requirements for this product type.

- Section 15, Enterprise and Network Management Systems, describes element management systems and operational support systems used to manage the DISN.

- Appendix A, Unique Deployed (Tactical), provides a synopsis of tactical requirements.

- Appendix B, Unique Classified Unified Capability, provides a synopsis of the Classified network environment.

- Appendix C, Definitions, Abbreviations and Acronyms, and References.

1.4 NETWORK SUPPORT FOR UC SERVICES

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.

The networks that provide UC services must be designed to meet specific requirements to support the following voice, video, and data services:

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

- <u>Voice Conferencing</u>. Provides for multiple voice users to conduct a collaboration session.

- <u>Video Teleconferencing</u> (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.

- <u>Email/Calendaring</u>. 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.

- <u>Unified Messaging</u>. Provides access to voicemail via email or access to email via voicemail.

- <u>Web Conferencing and Web Collaboration</u>. Provides for multiple users to collaborate with voice, video, and data services simultaneously using web page type displays and features.

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

- <u>Instant Messaging (IM) and Chat</u>. 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.

- <u>Rich-Presence Services</u>. 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.

- <u>Mobility</u>. 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). Wireless includes communication between devices that are not physically connected, and it includes but is not necessarily limited to wireless broadband access (e.g., WiFi), cellular (e.g., LTE), satellite communications, line of sight ratio, push-to-talk broadcast radio services, telemetry services, telecommand services, and wireless machine-to-machine (M2M) services.

1.5 UC OPERATIONAL FRAMEWORK OVERVIEW AND SUMMARY

The UC High Level Operational Framework illustrated in Figure 1.5-1, UC High Level Operational Framework, enables strategic, tactical, classified, and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks.
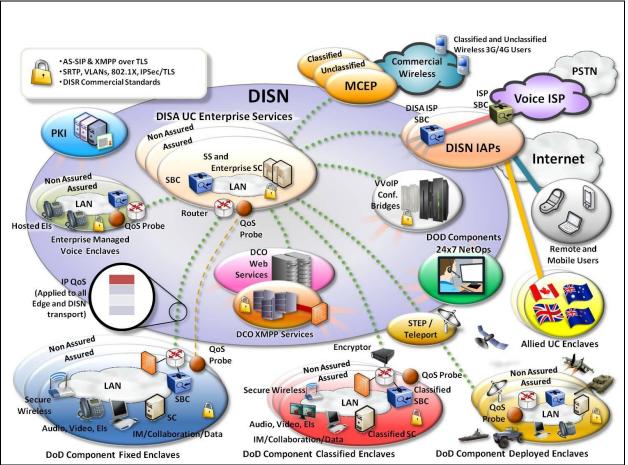
Figure 1.5-1. UC High Level Operational Framework

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

This operational framework is consistent with the Secretary of Defense Memorandum dated August 2012, "DoD Efficiency Initiatives" goals and corresponding Enterprise UC initiatives. By implementing enterprise multi-vendor UC investment in, and operating costs for, those services may be reduced using common and standard service models. Implementation of Enterprise UC can provide a full range of related capabilities to all DoD users from central locations that leverage the DISN and IP technologies. This approach minimizes potential duplication of costs that may occur for UC operations and maintenance, network operations, sustainment, and information assurance at DoD Component locations worldwide.

This operational framework leverages the requirements of the UCR 2013, which has been coordinated with DoD Components and industry.

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

1.6 HIGH LEVEL OPERATIONAL CONCEPT

Figure 1.6-1, DISN Backbone Infrastructure Global Locations, illustrates the DISN backbone infrastructure for up to 22 locations globally supporting a set of Geographic Regions (GeoRegions) based on DoD populations in the continental United States (CONUS) and outside CONUS (OCONUS) as part of the DISN investments and the DISN Subscription Services (DSS). This backbone shall make available services to user end devices for DoD Component locations depending on individual DoD Component's mission requirements. Final decisions on the GeoRegions shall be made as part of the DoD Components collaborative UC Implementation Plan integration activities.
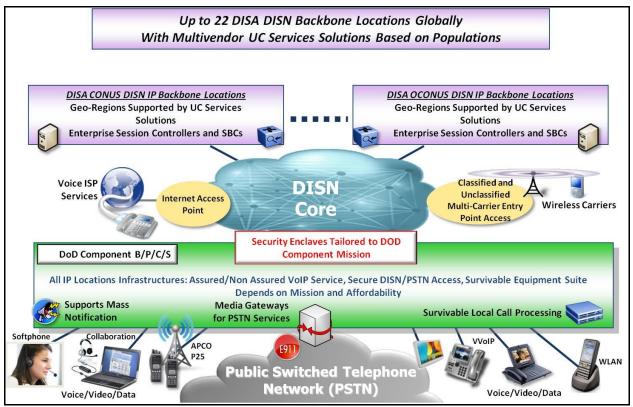

Figure 1.6-1. DISN Backbone Infrastructure

This operational concept has the potential to provide a single IP technology footprint, offer savings in operations and maintenance (O&M) and space requirements at the DoD Component level. At the enterprise level, this operational concept provides for integration of collaboration

services, directory services, and conferencing capabilities as well as potentially enhancing NetOps situational awareness and improving end-to-end network performance.

1.7   OPERATIONAL CONSTRUCT FOR UC NETOPS

Figure 1.7-1, Operational Construct for UC NetOps, defines the operational construct for UC Network Operations (NetOps) based on the U.S. Cyber Command (USCYBERCOM)/U.S. Strategic Command (USSTRATCOM) approved DISN UC Concept of Operations (CONOPS).
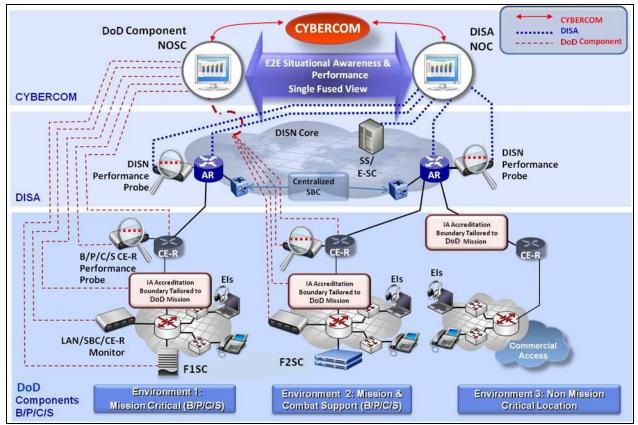

Figure 1.7-1. Operational Construct for UC NetOps

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

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

The DoD Component NOSCs (i.e., Military Department [MILDEP] and supported Combatant Command [COCOM]) shall oversee respective regional and Base/Post/Camp/Station (B/P/C/S) infrastructures supporting UC, delivered to the edge infrastructures and end devices. DoD Component B/P/C/S UC infrastructures may be tailored to meet respective mission needs for the three environments depicted in Figure 1.7-1. The environments are as follows:

Environment 1:   Mission critical - Organizations with mission sets that dictate, under normal conditions, access to all UC services, and in the event the location is disconnected from the DISN, require all basic UC services including intrabase precedence calling capability, external commercial services available to all users, and E911 service. Examples include a combat support unit or operational flying wing.

Environment 2:   Mission and Combat Support - Organizations with mission sets that dictate, under normal conditions, access to all UC services, and in the event the location is disconnected from the DISN, require limited voice-only services, and limited external commercial services (E911 and external dial tone). An example of this would be a training unit or an administrative center.

Environment 3:   Non-Mission Critical Location - Organizations with mission sets that do not require significant voice services or external commercial services (E911, and external dial tone) in the event the location is disconnected from the DISN. An example would be a small administrative function (e.g., recruiting office). In this case, E911 and other services could be provided by other means (e.g., cellular, leased services).

1.8   UC IMPLEMENTATION PRIORITY AND SCHEDULE

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

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

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

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

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

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

6. <u>Unified Messaging</u>. Provides the integration of voicemail and email. The integration of these two capabilities allows subscribers to access voicemail via email or access email via voicemail.

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

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

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

The specific DoD Component implementation schedules will be defined by their Implementation Plans.

1.9   ASSURED SERVICES DESIGN CRITERIA

The documents that define the UC network design requirements are referenced in the UC Master Plan. The most significant requirement is to provide Assured Services Features (ASFs) to mission-critical users as follows:

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) as described below

1. <u>Assured System and Network Availability</u>. This design requirement is achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, failover, diversity, and elimination of critical failure points. This ASF 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. <u>Assured Information Protection</u>. This design requirement 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:

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 DoD networks that provide UC services shall be configured to minimize and protect against attacks that could result in denial or disruption of service.

c. All hardware and software in the network must be information assurance-certified and accredited and operated in accordance with (IAW) the most current Security Technical Implementation Guidelines (STIGs).

3. <u>Assured Information Delivery</u>. This design requirement specifies 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:

a. Assured connectivity ensures the connectivity from user instrument-to-user instrument across all DoD UC networks, including U.S. Government-controlled UC network infrastructures, achieved under peacetime, crisis, and war situations.

b. The DoD UC networks are required to provide Precedence-Based Assured Services (PBAS) for delivery of UC services. Execution of PBAS is required on the sessions at the access and egress to the Wide Area Network (WAN) to meet mission needs. The WAN is expected to provide Quality of Service (QoS) to the sessions allowed by PBAS to access the WAN. The WAN need not be involved in precedence and preemption of the sessions, which will be determined at access and egress. Five precedence levels shall be provided. They are FLASH OVERRIDE (FO), FLASH (F), IMMEDIATE (I), PRIORITY (P), and ROUTINE (R). PBAS is required at WAN switches associated with WAN segments that have bandwidth restrictions and at the WAN to Tactical transitions at Gateways. Authorization for origination of sessions that use these precedence levels to support

mission-critical sessions shall be determined by the Joint Staff (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 EIs that are busy with lower precedence-based sessions shall be absolutely assured completion to a live person. This shall be accomplished by immediate disconnection of the lower precedence session and immediate completion of the higher precedence session.

e. Visibility and Rapid Reconfiguration. If blocking occurs to users' sessions caused by crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to situational awareness (SA) to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock 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 Softswitch (SS). All NOCs shall have Element Management Systems (EMSs) that allow for read-write access for the systems for which they have direct responsibility. In addition, the USCYBERCOM-sponsored NetOps Community of Interest (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 Chairman of the Joint Chiefs of Staff (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.

Note: Depending on the UC service of feature, a Non-assured service may be tested to ensure non-interference with an Assured service or to ensure interoperability with an Assured service or to verify the SLA of the Non-assured service.

1.10   UC NETWORK INFRASTRUCTURE OVERVIEW

The E2E UC network infrastructure consists of three network segments. The network segments are the Customer Edge (CE), Network Edge, and Core Segments. Figure 1.10-1, High Level UC Infrastructure Illustrating the Three Main Network Segment, illustrates a high-level overview of the three-segment network infrastructure. The CE Segment is connected to the Core Segment by the Network Edge Segment. The description of each segment is provided in the following paragraphs.
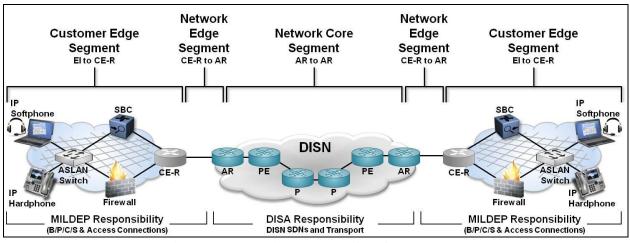

Figure 1.10-1. High-Level UC Infrastructure Illustrating the Three Main Network Segments

1.10.1   IP-Based CE Segment

The CE segment may consist of UC-approved products, which include EIs, ASLANs or Non ASLANs, or Metropolitan Area Networks (MANs), SCs, Enterprise SCs, SBCs, and the CE-Rs. The boundary device of the CE Segment is the CE-R. The Network Edge Segment connects the CE-R to the Aggregation Router (AR) via a DISN Service Delivery Node (SDN). The CE-R is owned and maintained by the B/P/C/S, unless the CE is used to delineate a standalone DISN

SDN. The CE Segment is considered robust and the LAN/Campus Area Network (CAN)/MAN characteristics include high bandwidth, diversity, and redundancy. The size of the LAN/CAN/MAN is dependent on its ability to meet the performance requirements defined in the UCR and the solution is internal to a Designated Approving Authority (DAA)-approved IA boundary. Design guidance and requirements for the LAN portion of the CE Segment are provided in Section 4, Customer Edge (ASLAN) Segment Design.

1.10.2 Network Edge Segment

The Network Edge Segment is measured from the WAN facing side of the CE-R to the MILDEP facing side of the AR. Depending on the specific class of DISN SDN (defined in Section 1.10.4) the Network Edge Segment may consist of several configurations. The simplest configuration, which has an extremely low packet delay, is encountered when the CE-R and AR are collocated. In this case, the Network Edge Segment is a direct, short Ethernet (i.e., 100Base-T or 1000Base-T) connection between the CE-R and an AR. Figure 1.10-2, High-Level Illustration of E2E Network Segments, illustrates short-delay and longer-delay Network Edge Segment configurations.
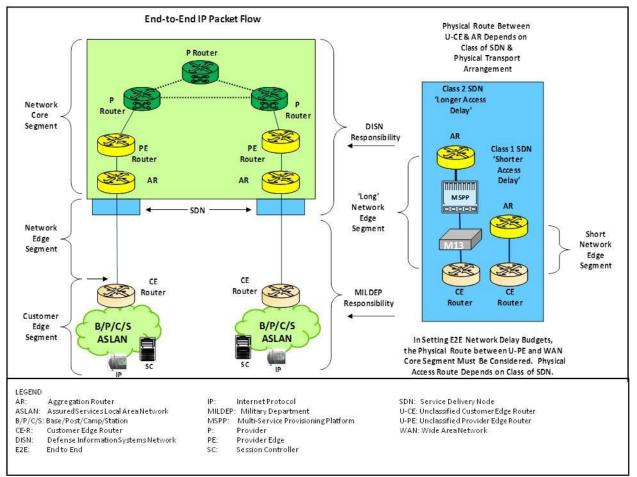

Figure 1.10-2. High-Level Illustration of E2E Network Segments

1.10.3 DISN Service Delivery Nodes

A DISN SDN is the start of DISA's layer of responsibility and it serves as the entry point for egress traffic exiting the CE Segment. From a physical perspective, the SDN is a computer room that houses all network equipment interfacing with the DISN. This location is most of the time found within the B/P/C/S. There are several classes of SDNs depending on whether the SDN has one or more of the following:

- M13, an APL product performing multiplexing and de-multiplexing functions of T1 and T3 carriers.

- Multi-Service Provisioning Platform (MSPP), a network device that may provide multiple network functions such as Routing, Switching, IDS, or Firewall.

- Provider (P) router.

- Provider Edge (PE) Router.

- AR.

In general, the CE-R connects either directly to the AR or through a series of equipment and connections to arrive at the AR. This is illustrated on the right hand side of Figure 1.10-2. This leads to two classes of SDNs:

1. Class 1 SDN. Type of SDN that has a short network segment, often categorized by the CE-R being collocated with the AR and has a shorter access and serialization delay.

2. Class 2 SDN. Type of SDN that has a longer network segment, often categorized by the CE-R not being collocated with the AR, has intervening network devices and connections, and has a longer access and serialization delay.

The customer is responsible for ensuring the aggregate access bandwidth on the Network Edge (Access) Segment is sized to meet the busy hour traffic demand for each service class and each of the 4 traffic queues, plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, Network Management (NM), and routing traffic.

Based on a site's DSS designation as a mission-critical site, the site's access to the DISN backbone 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: MSPP without AR all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning).
  - Robust: MSPP with Unclassified AR (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 1.10-3, 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.
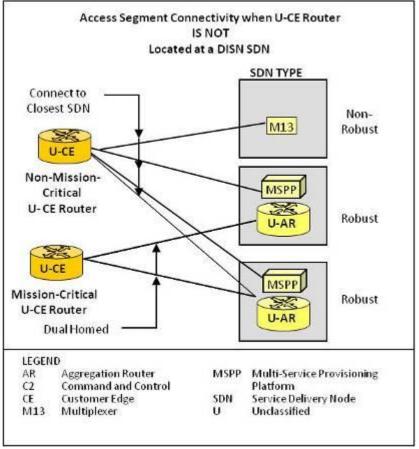

Figure 1.10-3. Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site

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.

1.10.4 Network Core Segment

The Network Core Segment provides IP-based transport services over a high-speed network infrastructure and consists of the SDNs and the DISN Transport elements between SDNs. The DISN Transport between SDNs typically consists of high-speed optical circuits that start and end at the PE router. The PE routers are connected by a series of Provider (P) routers to form a reliable and robust IP core network. Typically, the ARs are subtended off the PE Router via a high-speed Ethernet connection.

The network infrastructure is categorized according to its design state for performance measurement and analysis. Therefore, DISN networks are organized based on the infrastructure being a Deployed environment or a Fixed environment. Since the performance of the network infrastructure is affected by the type of deployment, the network infrastructure is categorized as the following:

- Fixed-to-Fixed (F-F). Deployments associated by terrestrial transport (wire line) connections serviced by the DISN.

- Fixed-to-Deployable (F-D). Deployments associated with a Fixed point of presence and a Deployable entry point as described below.

- Deployable-to-Deployable (D-D). Deployments associated with E2E military, on the field warfighter networks such as Standardized Tactical Entry Point (STEP)/Teleport, Joint Network Node (JNN) Regional Hub, the Naval Computer and Telecommunications Area Master Station (NCTAMS), or some other Teleport. D-D connections may or may not transit a Fixed point of presence.