

Office of the Army Chief Information Officer/G-6

U.S. Army

Unified Capabilities (UC) Reference Architecture (RA)

24 June 2015

Version 2.0



CIO/G-6
ENABLING SUCCESS For Today and Tomorrow



CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

U.S. Army Unified Capabilities Reference Architecture Executive Summary

The Army, Air Force, and Defense Information Systems Agency have been collaborating on a number of initiatives to accelerate the transition to the Joint Information Environment. This includes recent modernization of network transport and security architecture that will provide the foundation for enabling the transition toward Unified Capabilities (UC). The UC initiative involves a shift in focus from hardware-based voice over internet protocol to a Department of Defense (DoD) enterprise software-based solution that will quickly provide users integrated voice, video, and data (instant messaging/chat, presence, and screen sharing) on any approved user device. Underpinning this shift is the emergence and transition to enterprise cloud computing infrastructure that will provide standardized environments to host the UC capabilities as Software-as-a-Service solutions. Ultimately, the transition to software-based solutions will provide more user capability, improve mission effectiveness, and strengthen cybersecurity posture.

This UC Reference Architecture (RA) Version 2.0 document, as it supersedes UC RA Version 1.0, 11 October 2013, provides the Army with architectural guidance to enable the design, development, transition, and deployment of UC services. As a centralized reference to supporting architectural and associated efforts related to UC requirements, this RA describes architecture frameworks, principles, rules, technical positions, and implementation patterns to ensure integration, consistency, and standardization.

Army UC efforts are guided by the Army Network Campaign Plan– Implementation Guidance, Near-Term, Implementation Guidance, Mid-Term (Reference 1), and the Air Force and Army UC Implementation Plan, Version 1.0, October 2013 (Reference 2). In alignment with this guidance, the RA supports the focus on three lines of effort (UC Client, Internet Protocol Video Teleconferencing, and Assured voice over internet protocol) as priority enterprise service efforts.

This UC RA is aligned with the DoD Information Enterprise Architecture (Reference 3) and Joint Capability Areas (6.1.1, Information Transport , and 6.2.3, Core Enterprise Services) (Reference 4), and it guides key Army stakeholders and governs solutions integrators responsible for implementing UC initiatives to ensure compliance with business and architectural rules that improve interoperability within DoD and with Mission Partners.

GARY W. BLOHM

Director, Army Enterprise Architecture

Table of Contents

U.S. Army Unified Capabilities Reference Architecture Executive Summaryii

Table of Contentsiii

Chapter 1 Introduction..... 1

 1-1. Architecture Introduction 1

 1-2. Background..... 2

 1-3. Intended Audience 3

 1-4. Purpose 3

 1-5. Scope..... 4

 1-6. Problems, Issues, and Concerns 5

 1-7. Limitations, Assumptions, and Constraints 5

Chapter 2 Current and Objective State 7

 2-1. Current State 7

 2-2. Objective State..... 7

Chapter 3 Guiding Principles and Rules..... 13

 3-1. Principles and Rules 13

 3-2. Capability Gaps..... 19

 3-3. Traceability Alignment..... 22

 3-4. Considerations and Risks 29

 3-5. UCS Rules and Implementation States..... 32

Chapter 4 Patterns and Scenarios 40

 4-1. Patterns/Relationships 40

Chapter 5 Recommendations and Way Ahead 55

 5-1. Recommendations 55

 5-2. Way Ahead 55

Appendix A References 56

 A-1. Required References 56

 A-2. Related References 57

Appendix B Glossary of Acronyms 59

Appendix C Integrated Dictionary (AV-2) 65

Appendix D Technical Standards..... 86

Administrative Information Last Page

Table of Figures

Figure 1. Hierarchy and Context of the IEA Documents..... 1
Figure 2. Current Architecture 7
Figure 3. Objective Architecture 8
Figure 4. Vision (CV-1)..... 10
Figure 5. UC Operational Context 11
Figure 6. Capability Taxonomy (CV-2a): AEN Mapping of the DoD IEA Capabilities23
Figure 7. Capability Taxonomy (CV-2b): UC Mapping to AEN Domains 23
Figure 8. Implementation State Diagram..... 33
Figure 9. Services and Interfaces..... 41
Figure 10. Forecasted UC Transition 43
Figure 11. Activities Supporting Capabilities Phasing with Tactical Consideration.... 44
Figure 12. Legacy Environment (State 1a)..... 45
Figure 13. Early VoIP (State 1b) 46
Figure 14. Hardware Voice Light (State 1c) 47
Figure 15. UC Soft Client Solution Only (State 2) 48
Figure 16. Hardware Voice Only (State 3)..... 49
Figure 17. Hardware VTC Only (State 4) 50
Figure 18. UC Soft Client Solution + Hardware Voice (State 5) 51
Figure 19. UC Soft Client Solution + Hardware VTC (State 6) 52
Figure 20. Hardware Voice + Hardware VTC (State 7) 53
Figure 21. UC Soft Client Solution + Hardware Voice + Hardware VTC (State 8)..... 54

Table of Tables

Table 1. Capability Gaps 19
Table 2. Traceability Alignments 24
Table 3. Rules for Implementation States 34
Table 4. Service Descriptions..... 40
Table 5. Capability Taxonomy (CV-2) 41

Chapter 1 Introduction

1-1. Architecture Introduction

a. The Army Information Enterprise Architecture (IEA) is a high-level representation of the LandWarNet (LWN) architecture, as it supports the Army’s Enterprise Information Environment, Warfighting, Business, and Defense Intelligence Mission Areas. The IEA is sub-divided into the LWN 2020 and Beyond Enterprise Architecture (EA), and a set of Enterprise Reference Architectures (RAs), all of which the Chief Information Officer (CIO)/G-6 develops.

b. The hierarchy of the IEA, and the context in which it fits, is shown in Figure 1.

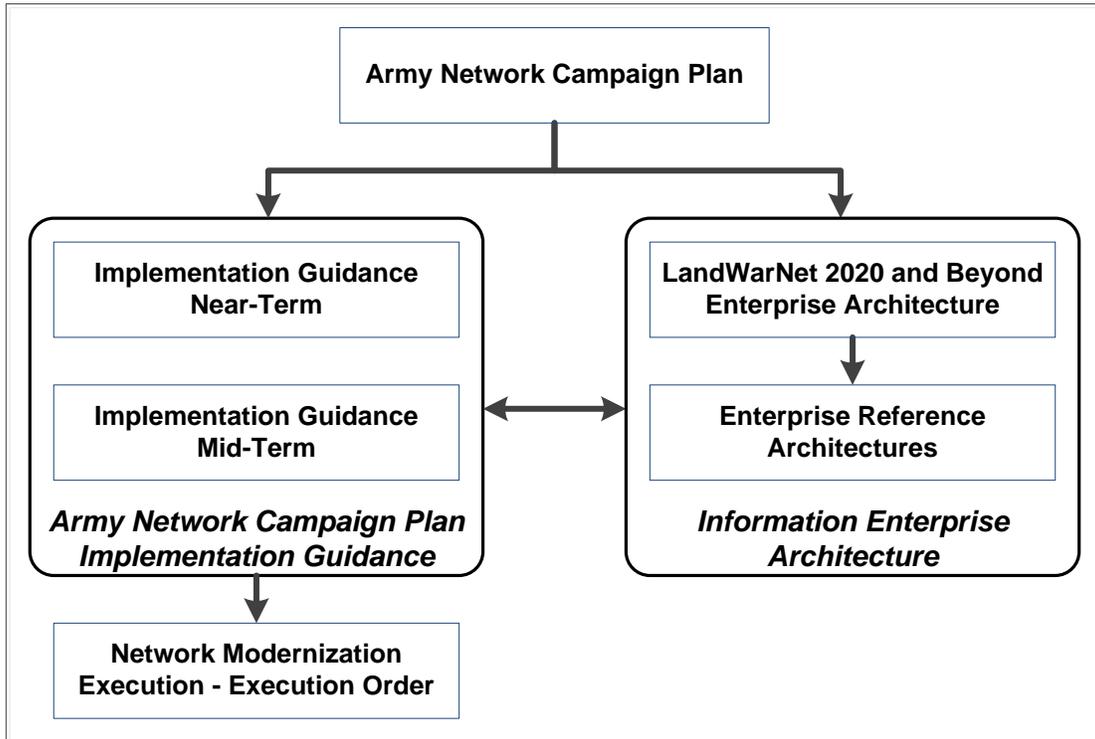


Figure 1. Hierarchy and Context of the IEA Documents

c. The overall objective of the documents shown in Figure 1 is to provide the architecture guidance and direction for LWN to achieve the vision in the Army Network Campaign Plan (ANCP) (Reference 1). This includes policy, principles and rules, constraints, technical guidance, standards and forecasts, implementation conventions, and criteria. Each of these documents has a unique role in the IEA by providing specific architecture-related information, as described below.

(1) LWN 2020 and Beyond EA (Reference 5) – Captures CIO/G-6 architecture guidance and direction at the level of detail needed to support the evaluation of potential Information Technology (IT) investments and architecture options for their alignment with the ANCP (Reference 1).

(2) Enterprise RAs – Aid in the resolution of specific recurring problems and explain context, goals, purpose, and the problems being solved.

d. The IEA documents can be found at <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>. Those with a Common Access Card (CAC) may also visit the Army Capability Architecture Development and Integration Environment (ArCADIE) site at https://cadie.tradoc.army.mil/CIO-G6_20Architecture/SitePages/Home.aspx.¹

1-2. Background

a. As provided by Department of Defense Instruction (DoDI) 8100.04, Department of Defense (DoD) Unified Capabilities (UC) (Reference 6, page 2):

“The DoD Components shall integrate current network technologies with future network technologies to provide UC (i.e., any single or combination of information media (voice, video, and data, whether converged or non-converged)) on DoD networks.”

b. During 2013, the Air Force, the Army, and the Defense Information Systems Agency (DISA) collaborated on a number of initiatives to accelerate the transition to the Joint Information Environment (JIE). Included in the initiative was a new approach to implementing UC based on the successful implementation of network transport and security architecture modernization. This new approach supports JIE objectives for enhanced mission effectiveness, improved cybersecurity posture, and increased efficiency. As guided by the Air Force and Army Unified Capabilities Implementation Plan (Reference 2), the collaborative team is moving toward the implementation of enterprise services within the DoD. This involves a shift from legacy end-user devices and circuit-switched, copper-based infrastructure to software-based solutions hosted in centrally managed, standardized, enterprise and regional data centers. Ultimately, the transition will reduce or eliminate legacy voice- and video-specific infrastructure investments identified under Joint Capability Areas (JCA) (Reference 4) Information Transport (JCA 6.1.1), and Core Enterprise Services (JCA 6.2.3).

c. This document, UC RA Version 2.0, supersedes UC RA Version 1.0, 11 October 2013. Version 1.0 was intended to describe a UC framework that “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 based on DISA described in DoD Unified Capabilities Requirements (UCR).” Version 2.0 focuses on supporting Air Force, Army, and DISA implementation involving a shift from hardware-based voice over internet protocol (VoIP) solutions to a DoD enterprise software-based solution. It will guide key Army stakeholders and govern solutions integrators responsible for implementing UC initiatives to ensure compliance with architectural rules that improve interoperability with DoD and Mission Partners.

¹ First time users may have to request access.

d. This UC RA Version 2.0 also shifts focus from alignment of higher-level architectures and principles to providing current architectural design guidance and governance specific to Army requirements. This guidance will enable implementation and integration activities; however, these activities will be controlled at the program and project management levels.

e. A part of the Army Enterprise Network's Enterprise Services Domain (ESD), UC will be directly enhanced by efforts made by the Network Capacity Domain (NCD) to upgrade transport capacity under the Multiprotocol Label Switching (MPLS), Area Distribution Node (ADN)/End-User Building (EUB) upgrades, and the Network Operations and Security Domain to simplify security architecture with Joint Regional Security Stacks (JRSS).

1-3. Intended Audience

The intended audience for this document includes Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT)), Program Executive Office Enterprise Information Systems (PEO EIS), U.S. Army Cyber Command (ARCYBER), Second Army and subordinate Signal Commands, and DISA. It also includes IT investment decision makers, architects, program managers, architecture developers, Army UC service providers, and UC mission support personnel associated with Enterprise Information Environment Mission Area (EIEMA), Warfighter Mission Area (WMA), Business Mission Area (BMA), Defense Intelligence Mission Area (DIMA), and Army Enterprise Network (AEN). Additionally, this document should be referenced when developing enterprise, operational, and solution architectures to ensure alignment with DoD guidance, architectures, strategies, and Joint initiatives. Lastly, this RA can be used to support IT investment review boards and portfolio review groups to validate procurement solutions supporting the EIEMA.

1-4. Purpose

a. The purpose of this RA is as follows:

(1) Provide architectural perspective of Army UC vision described in the ANCP (Reference 1).

(2) Establish foundational guidance derived from DoD IEA (Reference 3) and Army principles and rules to guide the delivery of UC capabilities and services.

(3) Provide guidance to support implementation efforts identified in ANCP - Implementation Guidance, Near-Term and ANCP - Implementation Guidance, Mid-Term (Reference 1).

b. This document provides guidance (principles, rules, technical positions, and implementation patterns) based on the Headquarters Department of the Army (HQDA) CIO/G-6 Rules-Based approach. Of particular note is the description of implementation states that can serve to support bridging strategy for installations during near-term and mid-term periods. Implementation states are characterized by a mix of legacy and software-based technology solutions. Due to the varying configuration differences of each installation, implementation states are to be used as general starting or intermediate points for any installation. Use of the most relevant and applicable

implementation state(s) will assist to identify the best course of action to successfully reach the To-Be state.

c. This document provides a reference to supporting architectural and associated efforts related to current and emerging UC requirements.

1-5. Scope

a. The focus of this RA is on UC and Collaboration (JCA 6.2.3.2), but the scope also includes applicable areas of Information Transport (JCA 6.1.1). Information Transport includes the capability areas of wired (local and long haul telecommunications), wireless transmission, and switching/routing as applicable to assured end-to-end connectivity services. Army Regulation (AR) 25-13, Telecommunications and Unified Capabilities (Reference 14), also provides the basis for coupling UC (collaboration) with telecommunications (areas closely tied to systems and services (e.g., telephone systems and video services)).

b. This RA also addresses other closely associated core enterprise capability areas. The principles and rules that apply to UC and collaboration also apply to the following JCAs (Reference 4) under Core Enterprise Services (JCA 6.2.3), which are also targeted ANCP Implementation Guidance, Mid-Term capabilities.

- | | |
|--|-------------|
| (1) Portal Services | JCA 6.2.3.1 |
| (2) Content Discovery | JCA 6.2.3.3 |
| (3) Content Delivery | JCA 6.2.3.4 |
| (4) Common Identity Assurance Services | JCA 6.2.3.5 |
| (5) Enterprise Messaging | JCA 6.2.3.6 |
| (6) Directory Services | JCA 6.2.3.7 |
| (7) Enterprise Application Software | JCA 6.2.3.8 |

c. The Air Force, Army, and DISA team is pursuing a DoD enterprise software-based UC solution that provides the user integrated voice, video, and data (instant messaging (IM)/chat, presence/awareness and screen sharing) on any approved device. For the near-term period, the ANCP (Reference 1) identifies three lines of effort (LOEs) to focus on. These LOEs, which also extend to the mid-term timeframe, include UC Client, Assured VoIP, and Internet Protocol (IP) video teleconferencing (VTC). Some of the key guidelines from the ANCP are summarized as follows:

- (1) Near-Term
 - (a) Begin UC Soft Client Solution Efforts
 - (b) Transition to VoIP
 - (c) Complete transitions to IP VTC
- (2) Mid-Term
 - (a) Start Joint assured voice
 - (b) Implementation of UC Soft Client Solution

(c) Begin integration of UC Soft Client Solution

d. There will be varying levels of installation modernization across both term periods. This RA supports both periods by accounting for initial installation capabilities being realized in the near-term and by identifying intermediate implementation states leading to To-Be states. These states are described in Paragraph 3-5 of this document.

e. There are also near-term targeted NCD priorities (Network Infrastructure Modernization and Path Diversity; Integrate Separate Networks; Improve Transport Capacity for Deployable Forces; and Divestiture Planning) that impact all areas in Information Transport (JCA 6.1.1). Modernization plans for the mid-term also include priorities associated network and computing infrastructure that will impact JCA 6.1.1.

f. The RA is intended for unclassified networks. Although this RA can generally be applied to classified and unique critical communication networks or circuits (e.g., Development Research and Engineering Network – in part, hosted by the Army Research Laboratory and the Engineer Research and Development Center), specific requirements and associated architectural guidance particular to these environments have not been identified at this time. In addition, this RA does mention some applicability to Continental United States (CONUS) and Outside CONUS (OCONUS) implementations. Refer to the ANCP (Reference 1), Air Force and Army Unified Capabilities Implementation Plan (Reference 2), and other applicable documents for further guidance.

g. Implementation and planning efforts for extending UC capabilities and services to the tactical environment occur during near-term and mid-term periods. Although the tactical environment is mentioned in this document, specific architecture guidance is not yet available for publication in this RA version.

1-6. Problems, Issues, and Concerns

The Army relies on a mix of local solutions and enterprise services for voice, video, and data capabilities to support collaboration and information sharing. Much of these services are non-standardized and primarily based on circuit-switched and copper-wire-based infrastructure that is inefficient and costly to maintain. In addition, the capabilities are not seamlessly integrated for ubiquitous delivery across a secure and highly available single protocol network infrastructure environment. The Army's near-term challenge is to begin addressing these problems by migrating to upgraded UC capabilities focusing on the three LOEs (UC Soft Client, IP VTC, and VoIP). The Army challenge also includes ensuring alignment with DoD JIE efforts to ensure the Army best leverages the common enterprise services.

1-7. Limitations, Assumptions, and Constraints

a. Limitations.

(1) The UC RA establishes a framework for developing UC in support of the Army Network Campaign Plan (Reference 1) and LWN 2020 EA (Reference 5). Updates to cover specific issues and areas shall be incorporated in future publications as required.

(2) The UC RA is focused on enterprise-level principles, rules, technical architectures, service and capability patterns, and implementation states.

(3) The UC RA does not address solution architecture or resourcing implementation; it is intended to inform, guide and constrain implementation efforts.

b. Assumptions.

(1) The Army will continue to support the fielding of infrastructure components (e.g., Joint Base Customer Edge Routers (JB CE-Rs), Edge Access Switches (EAS), and Area Core Switch (ACS)) in a regional approach based on the JIE implementation schedule.

(2) UC efforts depend on DoD JIE RAs used by the Army as sources of input to develop guidelines, policies, and rules. They include, but are not limited to, the following documents: DoD Enterprise-wide Access to Network and Collaboration Services (EANCS) (Reference 15), DoD Active Directory Optimization RA (ADORA) (Reference 16), DoD IEA Core Data Center (CDC) RA (Reference 17), DoD UC RA (Reference 7), and JIE EA (Reference 18).

(3) UC architecture is interdependent on the following U.S. Army-developed RAs: Identity and Access Management (IdAM) (Reference 8), Cloud Computing (CC) (Reference 9), Enterprise Service Management (ESM) (Reference 10), End-User Devices (EUD) (Reference 11), Network Operations (NetOps) (Reference 12), and Network Security (NS) (Reference 13); as well as on the applicable capabilities being in place to support UC capabilities.

(4) The network will have enhanced resilience and improved availability to support transitioning to UC enterprise-wide solutions.

(5) The network will provide Integrated Access Device (IAD) capability to connect digital and analog end instruments (e.g., laptops, hard phones, alarms) at required locations not supported by IP-based data networks.

c. Constraints.

(1) Network transport improvements are limited to MPLS, JB CE-R, ACS and EAS upgrades.

(2) Protection of UC implementations are limited to the JRSS architecture.

(3) Schedule constraints.

(a) Decommissioning of legacy systems following the deployment of UC Soft Client, HW voice upgrades (to VoIP phones), and HW video (to software-based devices).

(b) Delays in eliminating legacy and local service infrastructure would impact the effectiveness, security, and efficiency benefits gained from the transition to UC.

(4) Factors (e.g., error rates, bandwidth, throughput, transmission delay, availability) that influence quality of service (QoS) may require a trade space that may not result in achieving full and enhanced performance of UC services.

Chapter 2 Current and Objective State

2-1. Current State

The current architecture shown in Figure 2 is comprised of stove-piped infrastructure parts that separate data, voice and video into duplicative infrastructure and locally separate systems. Legacy infrastructure and capabilities, such as Time Division Multiplexing (TDM), Asynchronous Transport Mode (ATM), Integrated Services Digital Network (ISDN) and Primary Rate Interface (PRI), are provided at the local levels primarily via a physical copper infrastructure layer. Although efforts have already included some level of transition toward the To-Be architecture, the current architecture shown below essentially illustrates our technological starting point.

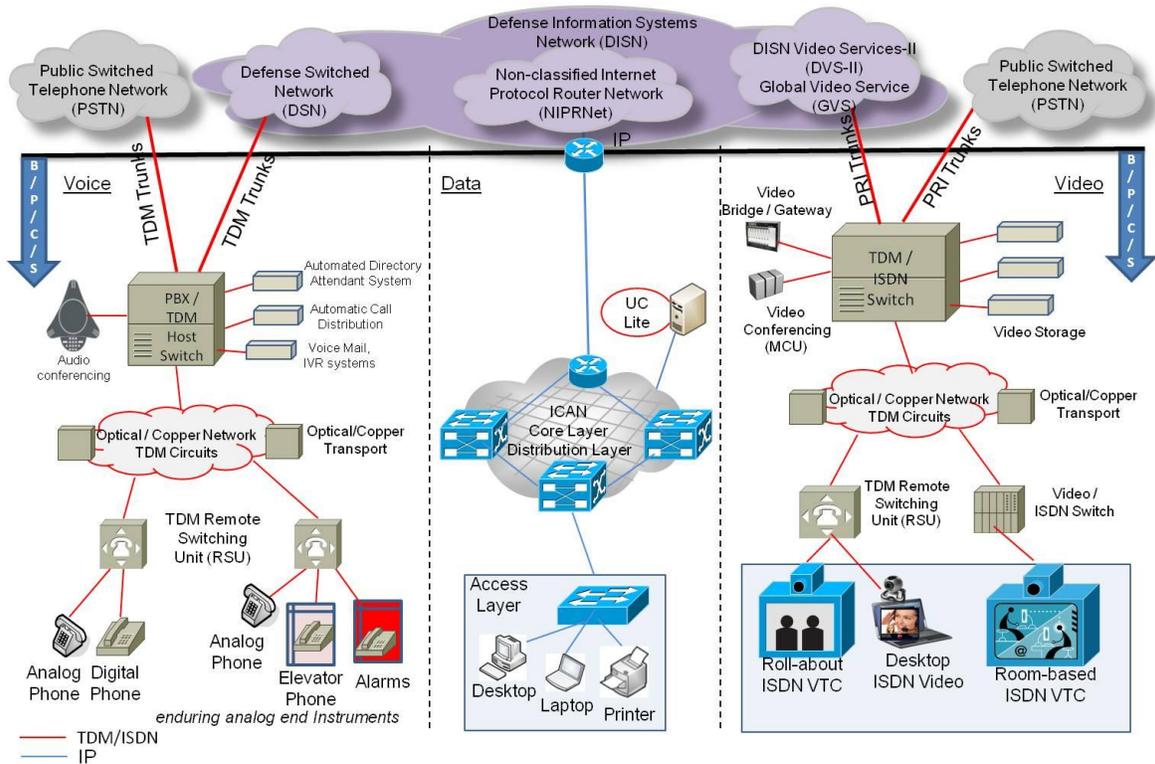


Figure 2. Current Architecture

2-2. Objective State

a. The objective state is described from three perspectives: Objective Architecture, Capability Vision, and Operational Context. All three perspectives provide a view of the To-Be environment depending on context.

b. Objective Architecture.

(1) This perspective shows the Army's transition to a nearly all-IP-based data network that will enable UC Soft Client Solution, hardware-based voice, and hardware-based video as shown in Figure 3.² Shown are the high-level components, connectivity, and interactions from the perspective of four major layers within the UC environment: Commercial, Defense Information Systems Network (DISN) Core, Installation Core, and Edge Access.

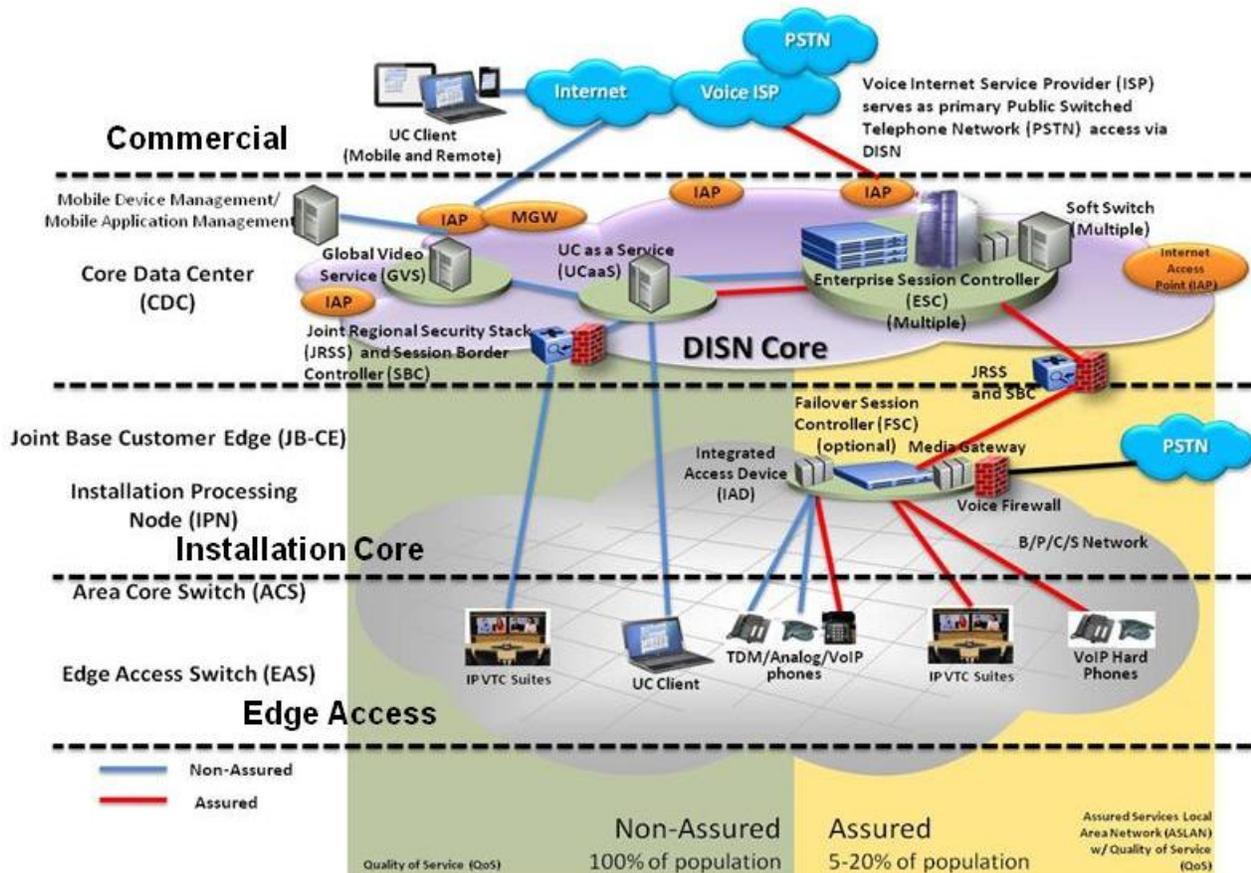


Figure 3. Objective Architecture

(2) The top is the Commercial layer which provides access and connectivity from the non-DoD environment to support UC end users (mobile and remote) for both assured and non-assured needs. DISA's voice Internet Service Provider (ISP) service, via the Internet, will serve as the primary Public Switched Telecommunications Network (PSTN) access point to provide commercial calling availability at the DISN level to reduce the connections to the PSTN at the Installation Core level.

(3) At the DISN Core layer, DISA provides Internet Access Point (IAP) Demilitarized Zones (DMZ) at several locations within CONUS. The core data center

² Source for the figure: Air Force and Army Unified Capabilities Implementation Plan, (Reference 2).

environment is contained in the DISN Core. This layer will provide the primary architecture to support enterprise level voice, video, IM/chat, presence, and screen sharing. These large network technologies will not be duplicated within the lower layers of the installation. The Army will use the JRSS and Session Border Controllers (SBC) within the DISN Core for all traffic that flows between the Installation Core and the DISN Core. The only exception will be placement of a voice firewall between the Installation Core voice technologies and the PSTN. DISA will provide the Defense Collaboration Service (DCS), and the Global Video Service (GVS), and Army leadership will leverage these services to the greatest extent possible. The Army will use all other enterprise services within the DISN Core layer.

(4) The Installation Core layer is the boundary of the Army base, post, camp, and stations (B/P/C/S). This layer will provide connectivity between DISN Core and the Edge Access and will be the only layer that connects the installation to the non-commercial PSTN. The Army is responsible for any architecture in this area and below. An important Army objective is to eliminate legacy technology within these layers. The Installation Core and Edge Access layers will provide a mixture of Non-Assured and Assured Services. Both will have the ability to provide QoS. The Installation Core layer will encompass the primary switches, routers (e.g., Customer Edge router (CE-R)), and ancillary technology to support the entirety of the installation. Not all installations will have all of the items depicted in this diagram. Those items that will be required are the ACS, JB CE-R, and Installation Processing Node (IPN). Items such as the Failover Session Controller (FSC), IAD, and Media Gateway (MG) may not be required in every installation. This layer will be based on enclaves depicted in the UC operational context graphic (see Figure 5).

(5) Finally, the Edge Access layer will encompass the end-user instruments/devices. A key Army objective in this layer is to implement an enterprise service for institutional voice, video, instant messaging/chat, presence, and screen sharing. This collaboration capability will be in the process of transitioning to a single asynchronous collaboration service to enhance Army-wide collaboration. A small amount of TDM/Digital/Analog/VoIP phones and IP VTC Suites will connect to the IAD at the Installation Core layer. These are hardware-based phones and video suites that are required in locations where UC Soft Client Solution is unavailable or does not meet availability requirements. All other End Instruments (EIs) will use the UC Soft Client Solution and connect directly into the DISN Core layer. The remaining supportability of legacy infrastructure and capabilities, such as TDM, will be moved into the Area of Responsibility (AOR) of CDCs within the DISN Core layer.

c. UC Vision.

(1) As described in the DoD Architecture Framework (DoDAF), the capability viewpoint (CV-1, Vision) addresses enterprise concerns associated with the overall vision for transformational endeavors and thus defines the strategic context for a group of capabilities.

(2) This perspective shows the context of capabilities to be offered by the UC architecture. These capabilities will provide a standardized enterprise infrastructure based on the integration of voice, video, and data (IM/chat, presence, and screen sharing services). Figure 4³ shows the UC vision for unclassified and classified enterprise UC, which contains the nine core capabilities (see Paragraph 4-1.c for descriptions). UC is envisioned to be a fully-enabled Software-as-a-Service (SaaS) capability implemented as an enterprise service delivered from DoD and commercial cloud computing environments and Army IPNs.

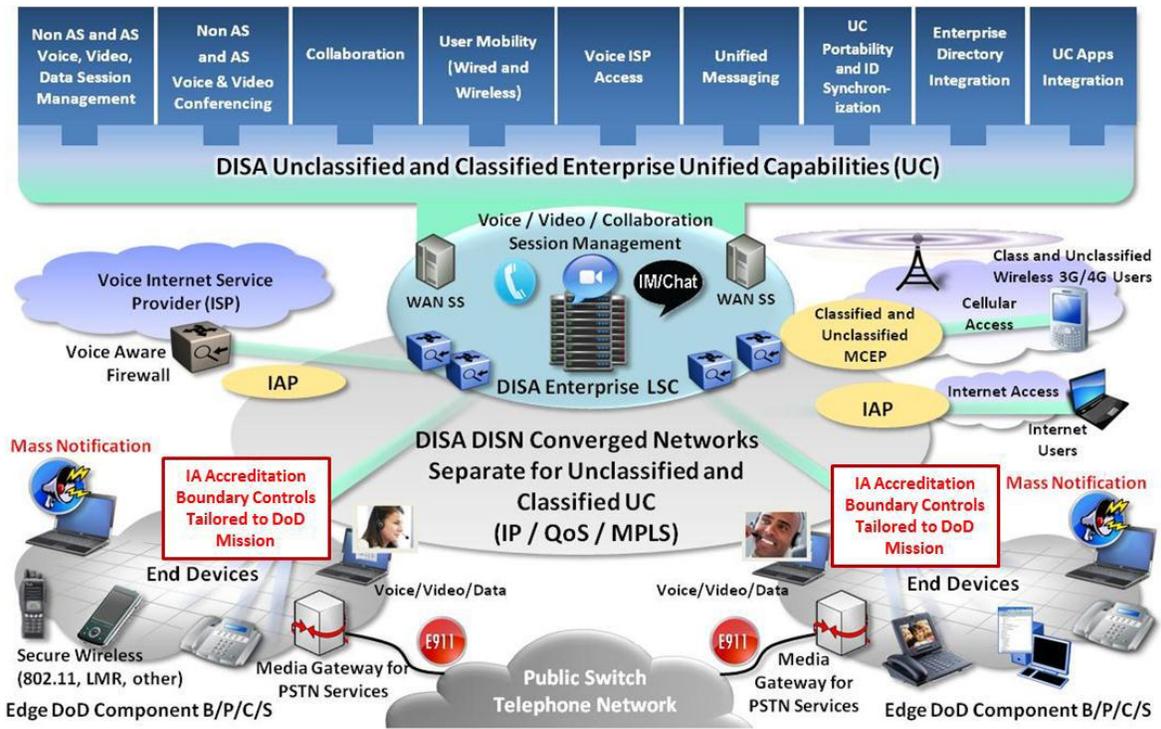


Figure 4. Vision (CV-1)

d. Operational Context.

(1) The Operational Context perspective, presented in Figure 5, illustrates the operational environment in the near-term to mid-term timeframes. The network is comprised of a number of systems that focus on the different elements of the network, including base infrastructure, the base security boundary, gateways to the DoD Information Network (DoDIN), core network services and the network management and monitoring capabilities necessary to operate and defend the network. Users of the

³ Source for the figure: DoD UC RA (Reference 7).

network are described within end point enclaves described below. These enclaves represent general communities of interests (COI), organizations, mission-focused units, and other applicable groupings. They are general in nature and may not necessarily define any particular group of users. In other words, a particular group of users may span over more than a single enclave.

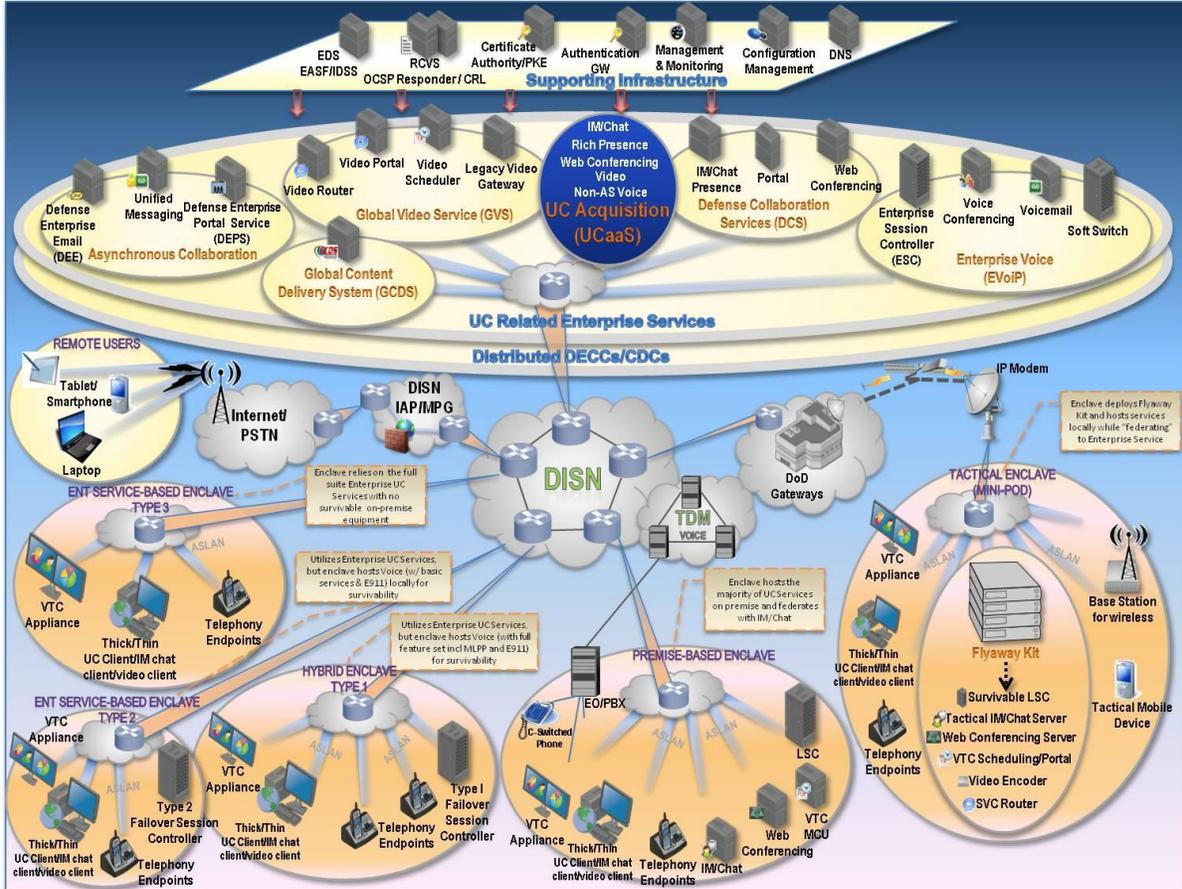


Figure 5. UC Operational Context

(a) *Hybrid Enclave Type 1: Mission Critical (B/P/C/S)*. Organizations with mission sets that dictate, under normal conditions, access to all UC services and, in the event the location is disconnected from the DISN, require all basic UC services including intra-base precedence calling capability, external commercial services available to all users, and emergency 911 (E911) service.

(b) *Enterprise Service-Based Enclave Type 2: Mission and Combat Support (B/P/C/S)*. Organizations with mission sets that dictate, under normal conditions, access to all UC services and, in the event the location is disconnected from the DISN, require limited voice-only services and limited external commercial services (E911 and external dial tone).

(c) *Enterprise Service-Based Enclave Type 3: Non-Mission-Critical Locations*. Organizations with mission sets that do not require significant voice services or external commercial services (e.g., E911, and external dial tone) in the event the

location is disconnected from the DISN. In this case, services such as E911 could be provided by other means (e.g., cellular, leased services).

(d) *Premise-Based Enclave*. This environment represents the As-Is or legacy enclave. Organizations that have partially transitioned to an IP end state will have items such as TDM, Local Session Controllers (LSC), private branch exchange (PBX) switches, Remote Switching Units (RSUs), VTC Multipoint Control Units (MCUs), circuit-switched technology, and analog supporting systems.

(e) *Remote Users*. Individuals who are not located at their primary installation are considered remote users. An example is an individual who is teleworking or on business travel. In this case, E911 and other services could be provided by other means (e.g., cellular, leased services).

(f) *Tactical Enclave (mini-pod)*. Organizations operating in the tactical environment will require a variety of end-user devices (e.g., VTC appliance, tactical mobile device) and flyaway kits capable of connecting to mini-pods. These mini-pods can host local services as well as provide access to enterprise services. Additional information on the tactical environment (e.g., tactical edge network, common operational environment, high level tactical UC architecture) can be found within DoD UC RA (Reference 7).

Chapter 3

Guiding Principles and Rules

a. Guiding principles represent the highest level of guidance and direction for IT planning and decision making. They are high-level statements that apply to specific business and warfighting requirements.

b. There are two sets of rules described in the following sections.

(1) Paragraph 3-1 includes higher level rules associated with guiding principles. These rules (e.g., UC R1.1) are at a general level that cross-cut or may have specific applicability to implementation.

(2) Paragraph 3-5 includes rules (e.g., UC Specific (UCS) R1.1.) that specifically apply to implementation states. These rules are more specific in nature and either support or enhance general rules in Paragraph 3-1. The table for UCS rules in Paragraph 3-5 addresses only two items, Rules and Desired Outcomes.

3-1. Principles and Rules

a. As shown in Subparagraphs b-g below, the general principles and rules are identified under six areas: Interoperability, Global Access, Service Level Agreement and Performance, Secure Sharing Collaborative Environment, Traffic Convergence, and Cross-Organization Information Sharing.

b. **Interoperability Guiding Principles and Rules. UC P1:** LWN will provide a secure, standards-based, and collaborative environment that supports UC systems and services for both classified and unclassified communications delivery. UC will interoperate with other areas and capabilities to provide the primary communication mechanism regardless of location or device.

(1) Compliance Category: Software Systems/Applications

(2) DoDAF Category: Operational

(3) UC R1.1: Minimize the use of legacy transport as applicable to locations/missions without access to IP network transport.

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(4) UC R1.2: Centralize/standardize synchronous collaboration solutions to simplify UC and reduce overlaps.

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(5) UC R1.3: Enable the LWN infrastructure with Core Enterprise Services that are available, discoverable and interoperable to share information for all mission requirements; ensure UC solutions leverage enterprise directory services.

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(6) UC R1.4: Maximize use of solutions that enable strong authentication (e.g., public key infrastructure (PKI)) and existing NetOps management tools.

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

For more information on identify and access management, refer to U.S. Army IdAM RA (Reference 8).

(7) UC R1.5: Leverage DoD-wide solutions for information sharing/secure exchange to minimize gaps and overlaps (e.g., collaboration services).

- (a) Compliance Category: Software Systems/Applications
- (b) DoDAF Category: Operational

(8) Desired Outcomes.

- (a) Minimal use of legacy technology that are duplicative or overlapping
- (b) Transport mechanisms in place to support Mission Partners
- (c) Simplified, standardized, and enhanced user experience with UC services
- (d) Improved cybersecurity posture
- (e) Enabled PKI authentication and decreased attack surface through reduced overlaps
- (f) Increased efficiency and interoperability
- (g) Decreased overlaps in information sharing
- (h) Increased user collaboration
- (i) Enabled synchronous global collaboration with all Unified Action Partners (UAPs) on any approved device

c. **Global Access Guiding Principle and Rule. UC P2:** The LWN shall enable connectivity to access Enterprise Services by all authorized users permitted by the Federal laws and Army policies as specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.

- (1) Compliance Category: Software Systems/Applications
- (2) DoDAF Category: Operational

(3) UC R2.1: Provide all authorized Army users (i.e., at Edge Access (see Figure 3)) access to Enterprise Services in order to communicate and share information through collaboration tools.

- (a) Compliance Category: Software Systems/Applications
- (b) DoDAF Category: Operational

(4) UC R2.2: Use common DoD-wide services and leverage DoD-wide solutions for collaborating/sharing with UAPs and across security domains to ensure access to (and only to) authorized information.

- (a) Compliance Category: Software Systems/Applications
- (b) DoDAF Category: Operational

(5) UC R2.3: Develop an end-to-end cybersecurity policy (i.e., authentication, authorization, encryption/integrity, and/or non-repudiation) for all UC applications and resources consumed by enterprise users (persons/non-persons); ensure the Army will use a single digital identity to uniquely identify an individual person and non-person entity.

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

(6) UC R2.4: Ensure that dial plans shall be implemented in accordance with DISA and Army guidance (e.g., 94=defense switched network (DSN), 99=outside, etc.).

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

For more information on identify and access management, refer to U.S. Army IdAM RA (Reference 8).

(7) UC R2.5: Maximize the use of strong authentication through PKI linking for global access with consistent user experience and satisfactory QoS to enterprise directories in accordance with the U.S. Army IdAM RA (Reference 8).

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

(8) Desired Outcomes.

- (a) Improved collaboration across the enterprise
- (b) Completed ability to access, share and disseminate information
- (c) Authorized users can access the applicable information
- (d) Reduced accessibility and interoperability issues caused by silo systems
- (e) Secured UC applications and resources

d. **Service Level Agreement and Performance Guiding Principle and Rule. UC P3:** The Army and the Service Provider(s) will have signed Service Level Agreements (SLA(s)) for delivering agreed upon services and ensuring service performance.

- (1) Compliance Category: Software Systems/Applications
- (2) DoDAF Category: Operational
- (3) UC R3.1: Develop detailed SLA/Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)/Contract Terms and Clauses for delivering

UC and overall service management plan for all the advertised services (e.g., QoS, reliability and availability).

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(4) UC R3.2: Define performance requirements/measures for Key Performance Parameters (KPPs) and/or Key System Attributes (KSAs) to ensure QoS.

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(5) Desired Outcomes.

(a) Service requirements specified in SLAs meet Army and Mission Partner goals for consistency and management control

(b) Compliant horizontal and vertical solutions able to meet the requirements of Federal, DoD, and Coalition partners

(c) Effective collaboration among authorized enterprise users

(d) Performance requirements and measures are specified and used to ensure policy compliance and mission effectiveness

e. *Secure Sharing Collaborative Environment Guiding Principle and Rule.* UC P4: The Army will provide a horizontal and vertical collaborative environment to share information with Federal, DoD, Coalition partners and non-governmental organizations to reach effectively and collaborate securely with UAPs.

(1) Compliance Category: Software Systems/Applications

(2) DoDAF Category: Operational

(3) UC R4.1: Ensure infrastructure transport (e.g., DISN Core, Installation Core (see Figure 3)) mechanisms support collaboration, information sharing and security up to the Edge Access layer (e.g., tactical environment).

(a) Compliance Category: Infrastructure

(b) DoDAF Category: Operational

(4) UC R4.2: Accelerate/improve delivery and reliability of enterprise content and enterprise services to facilitate information sharing globally.

(a) Compliance Category: Software Systems/Applications

(b) DoDAF Category: Operational

(5) UC R4.3: Ensure collaborative environment is secure in accordance with mission requirements (e.g., need-to-know).

(a) Compliance Category: Security

(b) DoDAF Category: Operational

(6) Desired Outcomes.

(a) Compliant and consistent horizontal and vertical solutions able to meet the collaboration, information sharing and security requirements of Federal, DoD, and Coalition partners as applicable

(b) Increased collaboration capability will enable a wide range of information sharing across many organizations

(c) Enhanced security in collaborative environments using CAC/PKI authentication

f. **Traffic Convergence Guiding Principle and Rule. UC P5:** The Army will develop an overarching LWN infrastructure strategy (HW, software (SW), etc.) to enforce a common computing infrastructure standard for hosting mandatory/shared enterprise services (e.g., integrated voice, video and collaboration tools).

(1) Compliance Category: Infrastructure

(2) DoDAF Category: Operational

(3) UC R5.1: Use IP-based infrastructure to support all UC services, except in specific cases where the capability may not be available (e.g., remote locations, natural disaster areas).

(a) Compliance Category: Infrastructure

(b) DoDAF Category: Operational

(4) UC R5.2: Limit the use of legacy solutions in order to mitigate localized power issues (e.g., ensure elevators are equipped with applicable operating emergency phone during power outages).

(a) Compliance Category: Infrastructure

(b) DoDAF Category: Operational

(5) UC R5.3: Limit voice services to only environments where the services must remain available for access to emergency service during power outages; ensure that at least one endpoint in each shared/group workspace must be able to place calls during power outages (e.g., health emergency, active shooter).

(a) Compliance Category: Infrastructure

(b) DoDAF Category: Operational

(6) Desired Outcomes.

(a) Improvements made to the Installation Campus Area Network (ICAN)/Wide Area Network (WAN)/LAN

(b) Integrated software-based voice, video, instant messaging/chat, presence, and screen sharing services are available from any Army approved end-user device

(c) Measurable transition progress will be made towards realizing the Joint Information Environment

(d) Simplified user training resulting from standardized enterprise solutions

g. Cross-Organization Information Sharing Guiding Principle and Rule. UC P6:

(1) UC P6a: Army will comply with DoDI 8500.01 (Reference 19) by revising Army security policies (i.e., AR 25-2 Information Management Information Assurance (Reference 20)).

- (a) Compliance Category: Monitoring & Management, and Security
- (b) DoDAF Category: Operational

(2) UC P6b: Army CIO/G6 will provide guidance on new required Risk Management Framework (RMF) and establish and enable cybersecurity policies and security controls validated through a standard security and engineering process. This will include updated guidance to the existing waiver policy.

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

(3) UC P6c: Global reach and global access items will have multiple security levels tied directly with UAP solutions as well as cybersecurity monitoring / management functions.

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

(4) UC R6.1: Develop/leverage information system-related security risk management based on the three-tiered security risk management approach published by National Institute of Standards and Technology (NIST); Guide for Applying the Risk Management Framework to Federal Information Systems (Reference 21).

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational

(5) UC R6.2: Publish and authorize information exchanges and connections for enterprise information systems (IS), cross-mission areas ISs, Mission Partner connections, cross domain connections, and foreign partner connections according to the specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.

- (a) Compliance Category: Infrastructure and Security
- (b) DoDAF Category: Operational

(6) UC R6.3: Ensure enterprise assets are managed through a cybersecurity/mission assurance capability (e.g., directory services, engineering/vulnerability assessments, supplier assurance).

- (a) Compliance Category: Monitoring and Management
- (b) DoDAF Category: Operational

(7) UC R6.4: Ensure security in the network (Premises/Access and IP/MPLS/Dense Wavelength Division Multiplexing (DWDM)/Generalized Multiprotocol

Label Switching (GMPLS)/Fiber Backbone; including virtual private network (VPN)/Virtual Local Area Network (VLAN) layer will work seamlessly with the higher layer security in view of a single digital identity to uniquely identify an individual.

- (a) Compliance Category: Security
- (b) DoDAF Category: Operational
- (8) Desired Outcomes.

(a) Authorized access for information sharing achieved through implementation of applicable cybersecurity policies and guidelines

(b) Management approach that ensures infrastructure assets are managed with minimal security risks

(c) Consistent source information and guidance to develop cost benefit analyses (CBA)

(d) Solution developers aligned and complied with Army CIO leadership priorities

(e) Army Enterprise Services transitioned away from localized solutions

3-2. Capability Gaps

Table 1. Capability Gaps

Applicable Rule(s)	Capability Gap
UC R1.1 – R1.5	JCA 6.1.1. Information Transport <ul style="list-style-type: none"> • Wired Transmission - Transport has duplicative deployments and component overlaps due to the use of legacy technology • Wireless Transmission - Transport is not always available for deployed Mission Partners in remote locations should they become disconnected
	JCA 6.2.3. Core Enterprise Services <ul style="list-style-type: none"> • User Access Portal - Duplicative protective voice and video boundary controllers at the edge, installation, and WAN environments reduce performance and degrade user experience (e.g., UC-specific voice and video security devices, management tools) • Collaboration - Duplicative services are not standardized or fully interoperable which limits the user ability to capture and share information • Directory services - Shortfalls exist for voice/video • Content Delivery - Legacy systems reliability (e.g., back-up) may not ensure mission support • Common Identity Assurance Services - Information sharing/secure info exchange (cross-domain, Mission Partner Gateway (MPGW), etc.) contain gaps/shortfalls which require overlaps in end-user services and collaboration with UAPs (secure/coalition/etc.)

Applicable Rule(s)	Capability Gap
UC R2.1 – R2.5	<p>JCA 6.2.3. Core Enterprise Services</p> <ul style="list-style-type: none"> • Collaboration - Outdated equipment (e.g., HW/SW) between end points are degraded, deprecated, or incorrectly deployed; inability to conduct communications and interaction across the enterprise • Content Delivery - Degraded or inaccessible connectivity (e.g., austere, isolated, non-connectable environment) does not ensure content and services delivery • Common Identity Assurance Services - Mobile information transport requires elevated levels of common identity assurance services for both data and networks; negatively impacted when there is a lack of consistent cross-domain solutions between Mission Partners • Directory Services - Inconsistent availability of a single global directory service or system; lack of synchronization with other directories and identity services
UC R3.1 – R3.2	<p>JCA 6.2.3. Core Enterprise Services</p> <ul style="list-style-type: none"> • Collaboration - The lack of a consistent information management policy, governance and controls across horizontal and vertical operating environments • Content Discovery - SLA agreements do not always include legal restrictions based upon interstate, country, regional, or interagency agreements for shared tenancy • Common Identity Assurance Services - Non-governmental organizations lack the security requirements to effectively collaborate with UAPs • Directory Services - Mission Partners, both vertically and horizontally, are negatively impacted when there is a lack of consistent Cross-Domain solutions

Applicable Rule(s)	Capability Gap
UC R4.1 – R4.3	<p>JCA 6.1.1. Information Transport</p> <ul style="list-style-type: none"> • Inconsistent cross-domain solutions; Federal, DoD, Mission Partners and non-government organizations, both vertically and horizontally, are negatively impacted • Outdated, degraded or deprecated equipment (e.g., HW/SW) between endpoints greatly affects deployed environments (mission effectiveness) • SLA agreements do not always include legal restrictions based upon interstate, country, regional, or interagency agreements for shared tenancy <p>JCA 6.2.3. Core Enterprise Services</p> <ul style="list-style-type: none"> • Collaboration - The lack of consistent information management policy, governance and controls across horizontal and vertical operating environments • Content Delivery - Non-governmental organizations lack the security requirements to effectively collaborate with UAPs
UC R5.1 – R5.3	<p>JCA 6.2.3. Core Enterprise Services</p> <ul style="list-style-type: none"> • Collaboration - Lack of common standards for the infrastructure to ensure communications and interaction across the enterprise involving converged voice, video and data • Content Delivery - Lack of capability to ensure adequate back-up power during power outages in the IP environment; inability to provide access to and delivery of information in emergency situations and to ensure voice and video collaboration solutions be hosted on the IP-based Internet
UC R6.1 – R6.4	<p>JCA 6.1.1. Information Transport</p> <ul style="list-style-type: none"> • Cybersecurity policies and security controls validated through a standard security and engineering process are not yet available <p>JCA 6.2.3. Core Enterprise Services</p> <ul style="list-style-type: none"> • User Access Portal - Cybersecurity policies and security controls validated through a standard security and engineering process are not yet available • Directory Services - Lack of standard process or approach to ensure global reach and global access assets (i.e., provided information and services) have multiple security levels tied directly with UAP solutions; lack of or inconsistent cybersecurity monitoring/management functions to ensure minimal security risks in events such as the mis-configuration of included assets/devices

3-3. Traceability Alignment

a. This section describes the alignment of UC with the DoD IEA and the AEN Portfolio Domains in terms of capabilities.

b. The JIE is envisioned as a secure environment comprised of shared information technology infrastructure, enterprise services and cybersecurity architecture to achieve full spectrum superiority, improved mission effectiveness, increased security and the realization of IT efficiencies. Operation and management of JIE is in accordance with the Unified Command Plan using enforceable standards, specifications, common tactics, techniques and procedures described in DoD IEA (Reference 3). The DoD JIE describes a vision of required information enterprise capabilities, which are as follows:

- (1) End-User Capabilities: Connect, Access, Share
- (2) Enable Capabilities: Operate, Defend
- (3) Users & Operations Requirement (Govern): Processes, Policy, Compliance

c. The Army's framework for managing network modernization is the Army AEN portfolio, which manages the Communications and Computers JCA (JCA 6) (Reference 4). The portfolio is comprised of three AEN Domains: Network Capacity, Enterprise Services and Network Operations and Security. Each domain is further divided into capabilities:

(1) Network Capacity Domain (NCD): The NCD portfolio includes the physical infrastructure necessary for all services and information based activities to traverse the network. The portfolio encompasses the foundational infrastructure upon which the Enterprise Services and Network Operations & Security solutions reside. Capabilities within this domain include: Information Transport and Computing Services.

(2) Enterprise Services Domain (ESD): This portfolio oversees delivery of an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly supports the Total Force while working with Unified Action Partners (UAPs). These services, both user-facing and enabling, provide the Total Force awareness of and access to information. Capabilities within this domain include: Core Enterprise Services and Position, Navigation and Timing.

(3) Network Operations & Security Domain (NSD): The NSD is responsible for providing a secure, seamless, and continuous network environment with protected critical data and information for the Total Force and UAPs. To meet this objective, NSD will provide capabilities that will improve the Army's ability to protect, detect, respond, restore, and manage information and systems. NSD will also pursue capabilities that support the management of underlying physical assets that provide end-user services for a continuous network environment. Capabilities within this domain include: Net Management and Cybersecurity.

d. The alignment between DoD IEA and AEN Domains is depicted in a Capability Viewpoint (CV-2a, Taxonomy) in Figure 6. This is a first-level mapping to identify the capabilities associated with UC. It is provided to support the crosswalk from delivered capabilities back to the DoD IEA capabilities.

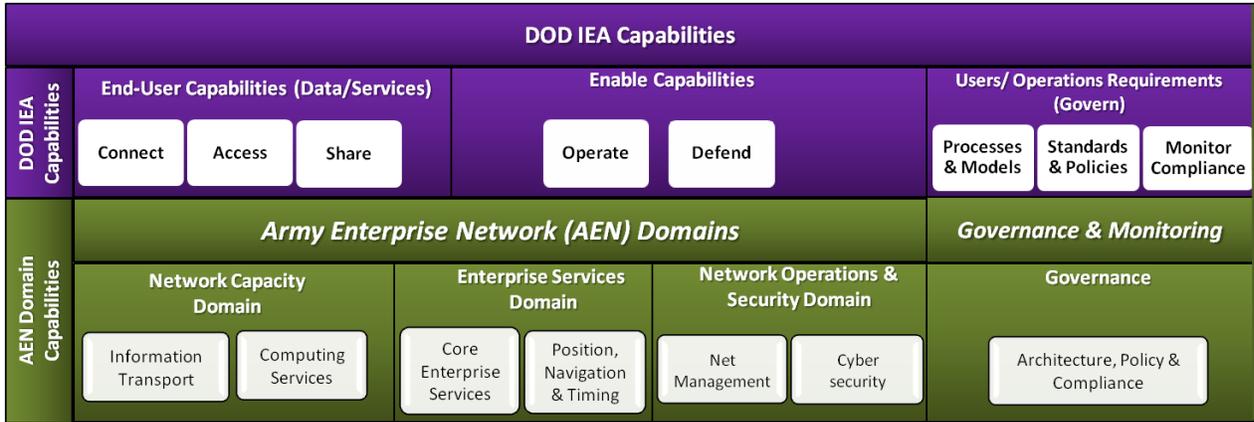


Figure 6. Capability Taxonomy (CV-2a): AEN Mapping of the DoD IEA Capabilities

e. The second level of mapping pertains to UC-specific capabilities. As described in Paragraph 4-1.c, there are nine Air Force/Army/DISA core capabilities. As depicted in a Capability Viewpoint (CV-2b, Taxonomy) in Figure 7, the nine capabilities are aligned to the AEN Domains.

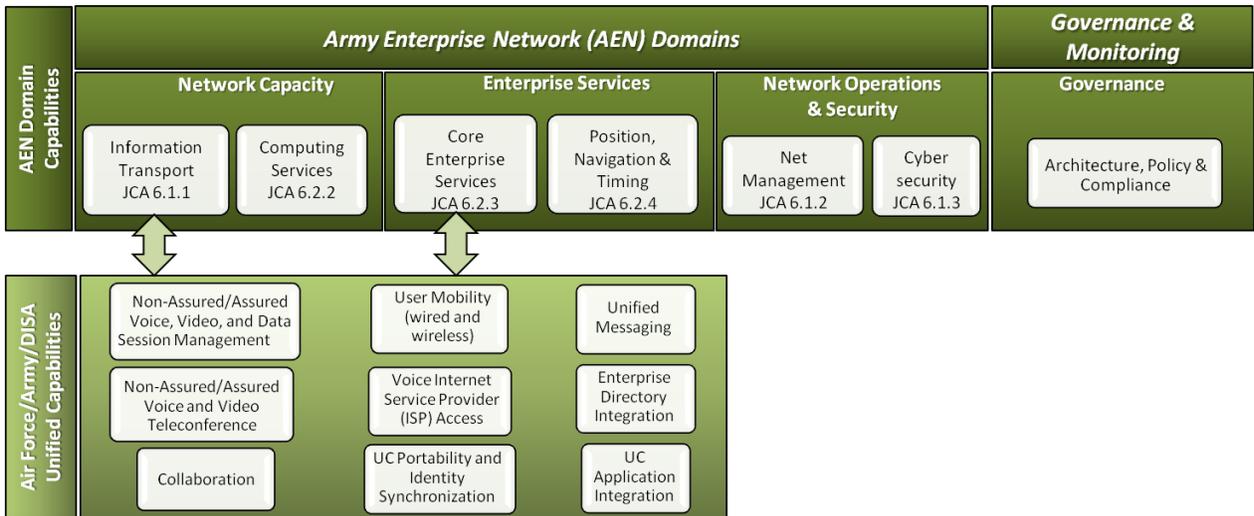


Figure 7. Capability Taxonomy (CV-2b): UC Mapping to AEN Domains

f. Table 2 describes the traceability alignments of the DoD IEA (Reference 3) and AEN Capabilities to the applicable UC principles and rules. As described in the DoD IEA, these principles and rules have been marked as Global Principles (GP), Computing Infrastructure Readiness Business Rules (CIRR), Communications Readiness Principles (CRP), Secured Availability Principles (SAP), and Secured Availability Business Rules (SAR).

Table 2. Traceability Alignments

Principle	Rule	Traceability Reference	Number	Name
UC P1	UC R1.1 – R1.5	DoD IEA Principle	GP 02	Interoperability of solutions across the Department is a strategic goal. All parts of the Global Information Grid (GIG) must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance. ⁴
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management
		AEN Capability	n/a	Enterprise Services Domain / Core Enterprise Services <ul style="list-style-type: none"> • Collaboration • Content Delivery • Directory Services • Enterprise Applications Software

⁴ Although usage of the term “Global Information Grid” has been replaced by “DoD Information Network (DoDIN),” the term will be used in the principles and rules cited in this RA because they are stated verbatim from DoD IEA (Reference 3).

UNCLASSIFIED

Principle	Rule	Traceability Reference	Number	Name
UC P2	UC R2.1 – R2.5	DoD IEA Principle	GP 06	The DoD Information Enterprise (IE) will include global access to common DoD-wide capabilities and services that enable access to people and information resources from any computer in the world. To the extent possible, services shall be developed for global use. The use of these globally accessible services will improve warfighting effectiveness, and interoperability, while reducing cost.
		DoD IEA Rule	SAR 07	All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access.
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Access <ul style="list-style-type: none"> • Identity Management • Attribute Services • Rules (Decisions/Enforcement) • PKI • Audit Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management
		AEN Capability	n/a	Enterprise Services Domain/Core Enterprise Services <ul style="list-style-type: none"> • Collaboration • Content Delivery • Common Identity Assurance Services • Directory Services
UC P3	UC R3.1 – R3.2	DoD IEA Principle	GP 04	DoD CIO services shall advertise SLAs that document their performance, and shall be operated to meet that agreement.

UNCLASSIFIED

Principle	Rule	Traceability Reference	Number	Name
		DoD IEA Rule	CIRR 04	Physical implementation of computing infrastructure shall include transparent interfaces to users to minimize, if not eliminate, degradation in performance and QoS.
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management
		AEN Capability	n/a	Enterprise Services Domain/Core Enterprise Services <ul style="list-style-type: none"> • User Access Portal • Collaboration • Content Discovery • Content Delivery • Enterprise Messaging • Directory Services • Enterprise Applications Software
UC P4	UC R4.1 – R4.3	DoD IEA Principle	GP 05	The GIG will provide a secure environment for collaborative sharing of information assets (information, services, and policies) with DoD’s external partners, including other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners.

UNCLASSIFIED

Principle	Rule	Traceability Reference	Number	Name
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management
		AEN Capability	n/a	Enterprise Services Domain / Core Enterprise Services <ul style="list-style-type: none"> • User Access Portal • Collaboration • Content Discovery • Content Delivery • Enterprise Messaging • Directory Services • Enterprise Applications Software
UC P5	UC R5.1 - R5.3	DoD IEA Principle	CRP 01	The GIG communications infrastructure shall support full IP convergence of traffic (voice, video, and data) on a single network.
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management

UNCLASSIFIED

Principle	Rule	Traceability Reference	Number	Name
		AEN Capability	n/a	Enterprise Services Domain / Core Enterprise Services <ul style="list-style-type: none"> • User Access (Portal) • Collaboration • Content Discovery • Content Delivery • Enterprise Messaging • Directory Services • Enterprise Application Software
UC P6a – 6c	UC R6.1 – R6.4	DoD IEA Principle	SAP 03	Global missions and globally dispersed users require global network reach. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable a seamless DoD Information Enterprise.
		DoD IEA Rule	SAR 06	All DoD services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational level (e.g., DoD Component), then at the service or application level.
		DoD IEA Capability	n/a	Connect <ul style="list-style-type: none"> • Assured End-to-End Communications • Unified Communications and Collaboration Share <ul style="list-style-type: none"> • Collaboration • Knowledge Sharing • Information Sharing with Mission Partners • Information Dissemination Management

Principle	Rule	Traceability Reference	Number	Name
		AEN Capability	n/a	Enterprise Services Domain/Core Enterprise Services <ul style="list-style-type: none"> • User Access Portal • Collaboration • Content Discovery • Content Delivery • Enterprise Messaging • Directory Services • Enterprise Applications Software

3-4. Considerations and Risks

a. Risks and Mitigation for UC P1.

(1) Risks

(a) Current infrastructure is reaching end of life and will not be supported by commercial industry

(b) Heterogeneous, ad-hoc, and incompatible operating systems remain in inventories; inability to quickly support equipment with acceptable level of interoperability

(c) Not all UC services currently have interoperability standards (e.g., screen sharing); inability to effectively collaborate

(d) Limited functionality with interoperability solutions; inability to effectively collaborate

(2) Mitigation

(a) Enable HW/SW, communication, and security infrastructure to protect information

(b) Provide survivable multi-path provisioning

(c) Enforce governance/compliance mechanism to improve interoperability

(d) Standardize solutions and configurations across users, devices, and operating systems

(e) Provide a common platform for a maximum number of population segments

(f) Support "special" missions and needs with targeted investment instead of comprehensive for all

(g) Leverage DoD/DISA-provided interfaces for phased legacy solution support

(h) Standardize protocols and interfaces where common solutions cannot be used

(i) Govern the use of non-standard/limited use tools and solutions

b. Risks and Mitigation for UC P2.

(1) Risks

(a) Incomplete collaboration and communication because non- CAC users will be unable to authenticate and access endpoint instruments (e.g., phones, video codec)

(b) For users authorized to possess only one CAC, there will be the inability to simultaneously use multiple end-user devices for full and effective collaboration

(2) Mitigation

(a) Develop end-to-end security policies

(b) Enforce guidance for two-factor authentication for non-CAC users

c. Risks and Mitigation for UC P3.

(1) Risks

(a) Consistent and continuous service monitoring may exceed allocated funding

(b) Access to emergency services may not be realized under multiple SLAs with various organizations

(c) Increased power requirements and costs for data networks performing service-level requirements for selected missions (e.g., emergency services)

(d) UC services are latency-sensitive, particularly in situations that demand end-to-end QoS

(e) Added management costs from maintaining multiple agreements (SLA/Operational Level Agreement (OLA)/MOU/MOA)

(2) Mitigation

(a) Establish service desk capabilities with required performance and cost objectives; ensure horizontal and vertical consistency across organizations

(b) Conduct a detailed analysis with recommendations to address emergency services support

(c) Define performance metrics for supported services

(d) Define end-to-end processes for QoS for UC services

(e) Integrate service desk support across Mission Partners for Joint/DoD services as applicable

(f) Use technology refresh or consolidation/standardization opportunities to address overlapping investments concerning missions/endpoints

d. Risks and Mitigation for UC P4.

(1) Risks

- (a) Evolving end-user devices are incompatible
- (b) Mission ineffectiveness from network bandwidth constraints
- (c) Inability of some DoD external partners (e.g., NGOs or academic researchers) to authenticate using CAC/PKI

(2) Mitigation

- (a) Standardize end-user devices; develop plan to ensure interoperability and compatibility of end-user devices
- (b) Implement MPLS upgrades to resolve bandwidth constraints; ensure reliable connectivity
- (c) For users without CAC/PKI capabilities, provide an alternate two factor authentication mechanism

e. Risks and Mitigation for UC P5.

(1) Risks

- (a) Power outages pose significant risk, especially in emergency situations, to the IP environment; high costs will result from providing failover continuity
- (b) Unable to maintain high QoS during network traffic operations; a performance factor needed in view of network transport and security architecture modernization (e.g., MPLS, JRSS)
- (c) Unable to reach cost-effective objectives when hardware-based voice and video over IP solutions will still be required at some locations
- (d) Interoperability issues with multi-vendor solutions for integrated soft client

- (e) Incompatible HW/SW solutions between end-user devices

(2) Mitigation

- (a) Ensure cost benefit analysis is performed
- (b) Provide detailed transition plans to ensure minimum impact on network traffic operations
- (c) Ensure standardization and interoperability of vendor solutions through pilot programs or other supportive activities

f. Risks and Mitigation for UC P6

(1) Risks

- (a) Guidance containing additional security control requirements may delay certification and accreditation (C&A) process
- (b) End users will experience delays in capability deployment

(2) Mitigation

(a) Develop transition plan defining a risk management process consistent with NIST SP 800-37 (Reference 21)

(b) Develop standard practices and credentials, security control assessors (formerly known as certifiers), vulnerability assessments, and mitigation recommendations to ensure results are reliable, repeatable, and accepted enterprise-wide

3-5. UCS Rules and Implementation States

a. As noted in the introduction of Chapter 3, UCS rules are specific rules directly applicable to implementation states.

b. General Description of Implementation States.

(1) It is recognized that every installation is currently configured to various levels of modernization. An installation can be considered to be in a certain implementation state at a given point in time.

(2) Implementation State – Defined as the particular condition (as characterized by technological capability) that an installation (or collection of installations) is in at a specific point in time.

(3) As an installation transitions from an As-Is state to a To-Be state, the installation can transition through various intermediate states. There are numerous implementation states. However, for the purpose of this document, only ten states are identified.

(4) Of the ten states, three are As-Is implementation states that represent “starting points” in the current architecture. The three implementation states can be regarded as general and characteristic of many installations. For those installations whose configurations are not clearly characterized by these three implementation states, the key point is that there are many As-Is states as well as several paths/variations along transitional states toward the As-Is environment.

(5) Figure 8 shows the available non-serial paths of transition from the three general As-Is states to transitional states and to the final To-Be architecture state.

(a) Title of a state (e.g., State 1b, Early VoIP) shows the predominant or characteristic feature of that state.

(b) States are not numerically sequential; from the As-Is, the path could go to states 2, 3, 4, 5 or 8 depending on schedule, resources and other applicable factors. From state 3, the path could lead to states 5 or 7.

(c) States show the overall structure and organization of systems and components (see Paragraph 4-1.d, for Detailed Description of Implementation States) with associated functions that provide UC services to users at a particular point in time.

(d) Paths from state to state are shown, but an actual implementation path could vary.

(e) The To-Be state includes features that correspond to the Installation Core and Edge Access layers described in the Objective Architecture (Figure 3).

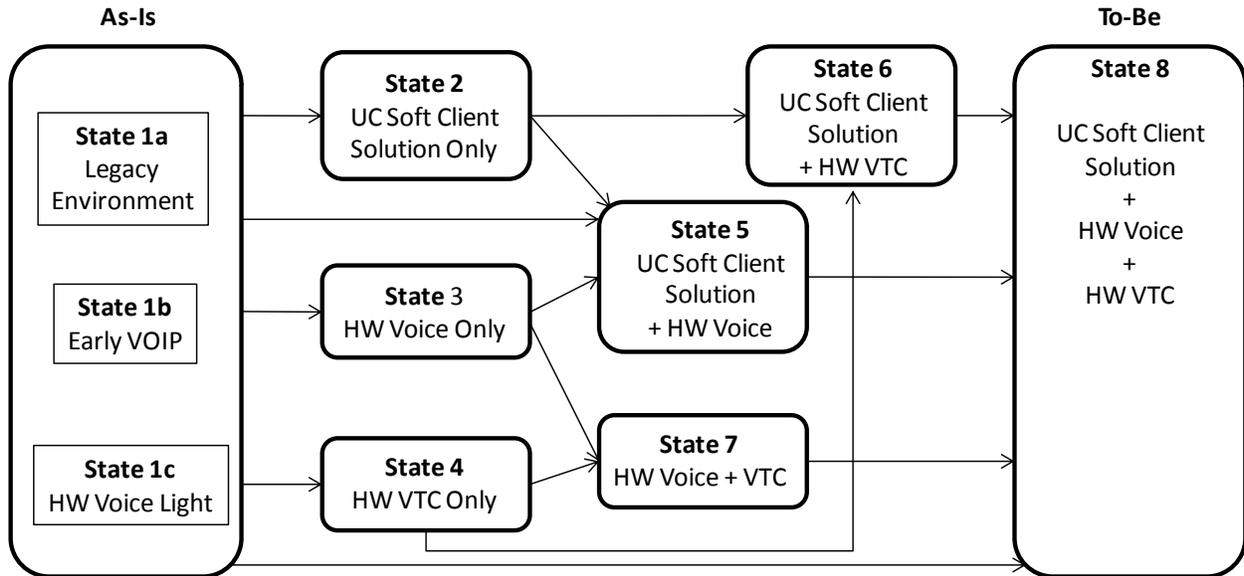


Figure 8. Implementation State Diagram

(6) Each implementation state is associated with applicable UC rules in general, but more specifically, each implementation state is associated with UCS rules. UCS rules are specific rules provided to ensure implementation consistency and standardization.

c. *UCS Rules for Implementation States.* Unlike the general UC rules, UCS rules shown in Table 3 below are associated with only two table items (Rules and Desired Outcomes) plus the affected states. The numbers indicate the specific implementation state for the rule. The second number accounts for the series of rules that apply to a specific state which is not an order or precedence.

Table 3. Rules for Implementation States

UCS #	UCS Rules	Desired Outcome	Affected States
R1.1	VTC elements must transition as soon as possible to the HW_VTC pattern (or UC Soft Client Solution when available) Note: DISA is reducing ISDN connectivity support under their transition from DISN Video Service Global (DVS-G) to GVS	<ul style="list-style-type: none"> Decreased overlaps Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	1a, 1b, 1c, 2, 4, 6
R1.2	Transition from As-Is Early VoIP to As-Is HW Voice Light as soon as possible to reduce ISDN WAN circuit costs; subtend the LSC to the TDM to include essential routing changes	<ul style="list-style-type: none"> Decreased overlaps Simplified, standardized, and enhanced user experience with UC services Reduced accessibility and interoperability issues caused by silo systems Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	1b, 1c
R1.3	Installation LSC will connect to DISA soft switch (SS) using Assured Services Session Initiation Protocol (AS-SIP) via a local SBC	<ul style="list-style-type: none"> Improved cybersecurity posture Availability specified in agreements is achieved as well as meets Army performance goals 	1c
R1.4	Use DISA Voice ISP Service in CONUS; use OCONUS Voice ISP connection or DoD/Army contract for PSTN connection Note: A business case analysis will be required to show increased cost deltas if DISA service is more than installation recommended solution	<ul style="list-style-type: none"> Increased efficiency and interoperability Increased user reach (ability of users to collaborate with many more users at distant locations) Guidance provided to develop a CBA Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	1c, 2, 3, 5, 6, 7, 8

UNCLASSIFIED

UCS #	UCS Rules	Desired Outcome	Affected States
R1.5	Conference rooms will transition to UC Soft Client Solution SW vs. HW codecs	<ul style="list-style-type: none"> • Improved cybersecurity posture • Increased efficiency and interoperability • Decreased overlaps • Enabled synchronous global collaboration with all UAPs on any approved device • Simplified, standardized, and enhanced user experience with UC services • Improvements to the ICAN and WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable • Software-based solution (integrated voice, video, instant messaging/chat, presence/awareness, and screen sharing) used from any Army approved end-user device • Simplified user training requirements based on standard enterprise solutions • Guidance provided to develop a CBA 	2, 4, 6, 7, 8
R1.6	Transition away from local SBCs and use capabilities provided by the DISA	<ul style="list-style-type: none"> • Improved cybersecurity posture 	2, 3, 4, 5, 6, 7, 8

UNCLASSIFIED

UCS #	UCS Rules	Desired Outcome	Affected States
R1.7	Use ancillary voice capabilities as provided by DISA (enterprise) or Army (regional)	<ul style="list-style-type: none"> • Solution developers aligned with Army CIO/G-6 leadership priorities • Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable • Army Enterprise Services are centrally governed and managed by the Army Enterprise Network Council (AENC) • Guidance provided to develop a CBA 	3, 4, 5, 6, 7, 8
R1.8	Limit hard phones to common areas, non-IP areas (e.g., elevators, ranges) or endpoints that must meet assured service/multilink protocol (MLPPP) requirements	<ul style="list-style-type: none"> • Decreased overlaps • Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	3, 5, 7, 8
R1.9	Endpoints will transition to IP-based capabilities; local ISDN VTC not allowed	<ul style="list-style-type: none"> • Decreased overlaps • Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	4, 6, 8
R1.10	Network Enterprise Technology Command (NETCOM) will neighbor with DISA GVS (NETCOM to provide applicable VTC services until such time when decommissioning is appropriate)	<ul style="list-style-type: none"> • Enhanced mission effectiveness • Increased efficiency and interoperability • Decreased overlaps • Increased user reach; users are able to collaborate and interoperate with each other 	4, 5, 6, 7, 8

UNCLASSIFIED

UCS #	UCS Rules	Desired Outcome	Affected States
R1.11	Software-based VTC will be used for all non-assured endpoints	<ul style="list-style-type: none"> • Decreased overlaps • Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	8
R2.1	Use ISDN-based secure voice (e.g., Secure Terminal Equipment (STE)) only where coalition or Defense Red Switch Network (DRSN)/Top Secret-level communications are required	<ul style="list-style-type: none"> • Enabled synchronous global collaboration with all UAPs on any approved device • Information accessed by authorized users • Secured UC; strong authentication (e.g., CAC/PKI) used at single entry point 	2, 3, 5, 6, 7, 8
R3.1	QoS/COI will be implemented on ICAN and WAN	<ul style="list-style-type: none"> • Enhanced mission effectiveness • Increased efficiency and interoperability • Ability to access, share and disseminate information • Availability specified in agreements is achieved as well as meets Army performance goals • Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	2, 5, 6, 8
R3.2	VTC service providers will neighbor with NETCOM virtual cluster switching (VCS) infrastructure to ensure WAN operator has visibility of traffic and can manage accordingly	<ul style="list-style-type: none"> • Enhanced mission effectiveness • Increased efficiency and interoperability • Decreased overlaps • Increased user reach; users are able to collaborate and interoperate with each other 	4, 5, 6, 7, 8

UNCLASSIFIED

UCS #	UCS Rules	Desired Outcome	Affected States
R3.3	ISDN PRI/Centralized Automated Message Accounting (CAMA) trunks will be limited to emergency failover capacity only (generally 5-10 percent of peak active)	<ul style="list-style-type: none"> • Improved cybersecurity posture • Enabled PKI authentication, and decreased attack surface through reduced overlaps • Increased efficiency and interoperability • Enabled, monitored and protected information and services without disruption (per SLAs) achieved via disaster recovery, backup and recovery/failover mechanisms 	1c
R3.4	Use legacy phones where services to support VoIP phones are not available or justified	<ul style="list-style-type: none"> • Enabled, monitored and protected information and services without disruption (per SLAs) achieved via disaster recovery, backup and recovery/failover mechanisms 	2
R3.5	Use ISDN-based unclassified voice only where IP network is unavailable (e.g., range, elevator)	<ul style="list-style-type: none"> • Enabled, monitored and protected information and services without disruption (per SLAs) achieved via disaster recovery, backup and recovery/failover mechanisms 	2, 3, 5, 6, 7, 8
R3.6	FSC will connect to the DISA enterprise session controller (ESC) via AS-SIP and will be sized only to support local missions with voice failover requirement; can also be used to support emergency call endpoints	<ul style="list-style-type: none"> • Solution developers aligned with Army CIO/G-6 leadership priorities • Enabled, monitored and protected information and services without disruption (per SLAs) achieved via disaster recovery, backup and recovery/failover mechanisms 	3
R3.7	FSCs will not be implemented or used if there is not an emergency voice failover requirement at the site; voice service will be drawn directly from the enterprise	<ul style="list-style-type: none"> • Enabled, monitored and protected information and services without disruption (per SLAs) achieved via disaster recovery, backup and recovery/failover mechanisms 	3, 4, 5, 6, 7, 8

UNCLASSIFIED

UCS #	UCS Rules	Desired Outcome	Affected States
R5.1	Sites with physical diversity to the WAN will not use FSCs	<ul style="list-style-type: none"> • Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable • Guidance provided to develop a CBA 	3, 4, 5, 6, 7, 8
R5.2	Transition away from WAN ISDN connections; IP connectivity will be used to connect to the DISA VCS Note: ISDN bridging will be provided by DISA GVS	<ul style="list-style-type: none"> • Decreased overlaps • Improvements to the ICAN, WAN/LAN; Army Enterprise Services transitioned away from local solutions to DoD-wide Enterprise Services where applicable 	4, 6, 8
R6b.1	VTC equipment will use specific VTC subnet for firewall traversal	<ul style="list-style-type: none"> • Improved cybersecurity posture • Enabled PKI authentication and decreased attack surface through reduced overlaps 	4, 6, 7

Chapter 4 Patterns and Scenarios

4-1. Patterns/Relationships

a. Implementation patterns are a collection of perspectives, descriptions and views that guide and support activities for transition and implementation. The paragraphs below include DoDAF viewpoints and a detailed description of the implementation states.

b. *Service Patterns. Service Context Descriptions (SvcV-1).* The capabilities described in Paragraph 4-1.c. are provided through a collection of services, where a service is defined as “a mechanism” to enable access to a set of one or more capabilities. UC services are driven by changing communications technologies, and those technologies support many capability changes (e.g., from point-to-point to multipoint, voice-only to rich-media, multiple devices to single device, wired to wireless and scheduled to ad hoc). These services are listed and defined via a Services Viewpoint (SvcV): the Services Context Description, SvcV-1.⁵ This is shown in Table 4 and depicted in Figure 9. The SvcV-1 describes the identification of service, service description, and their interconnections.

Table 4. Service Descriptions

Services	Description
Instant Messaging and Chat	The capability for users to exchange one-to-one ad hoc text messages over a network. Instant Messaging is not the same as, and must not be confused with, signaling or equipment messaging; 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. Chat is distinguished from IM by being focused on group chat or room-based chat. Typically, room persistence is a key.
Presence	Allows contact to be achieved with individuals based on their availability as displayed by presence information from multiple sources, including IM, telephone, and mobile devices.
Video Teleconference	Provides multiple video users with the ability to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.
Voice and Video (Point-to-Point)	Provides two voice and/or video users with the ability to be connected End-to-End with services that can include capabilities such as voicemail, call forwarding, call transfer, call waiting, operator assistance, and local directory services.
Voice Conference	Provides multiple voice users with the ability to conduct a collaboration session.

⁵ Source for the SvcV-1: DoD UC RA (Reference 7).

Services	Description
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.

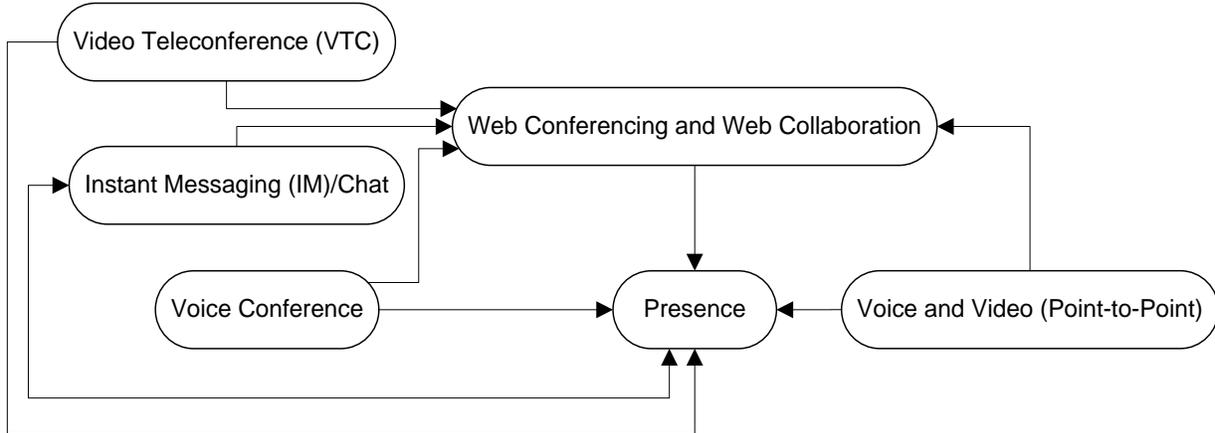


Figure 9. Services and Interfaces

c. Capability Patterns.

(1) *Capability Taxonomy (CV-2)*. As identified in the CV-1 (Figure 4), there are nine core capabilities. They support the overall UC vision to integrate current network technologies with future network technologies to provide UC (e.g., any single or combination of information media (voice, video, and/or data), whether converged or non-converged) on DoD networks. These capabilities are aligned with the DoD UC RA (Reference 7). These capabilities and their descriptions are also shown in the Capability Taxonomy below (Table 5). The Capability Taxonomy, CV-2, is a method to capture capability taxonomies and present a hierarchy of capabilities with descriptions.

Table 5. Capability Taxonomy (CV-2)

Capabilities	Description
1. Non-Assured/Assured Voice, Video, and Data Session Management	Provides enterprise point-to-point UC, independent of the technology (circuit switched or IP). Functionalities 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 Teleconference	Provides the ability to conference multiple voice or video subscribers with a variety of room controls for displays of the participants. It also includes an optional component that allows subscribers to schedule conferences.
3. Collaboration	Provides IP-based solutions that allow subscribers to collaborate (e.g., instant messaging, chat, presence, and web based conferencing).

Capabilities	Description
4. User Mobility (wired and wireless)	Provides the ability to offer wireless and wired access, for UC supported by multifunction mobile devices. In addition, it provides access to enterprise UC globally using UC portability.
5. Voice ISP Access	Provides unclassified and classified enterprise UC for access to commercial voice services over IP. This service provides both local and long distance dialing capability using commercial ISPs via secure interconnections.
6. Unified Messaging	Provides the integration of voicemail and e-mail. The integration of these two capabilities allows subscribers to access voicemail via e-mail or access e-mail via voicemail.
7. UC Portability and Identity Synchronization	Provides an enterprise UC systematic approach to portability functions (e.g., repository of user profiles and privileges, subscriber identification and authentication). Uses DISA's existing Identity (ID) synchronization service as the primary service for DoD ID Synchronization.
8. Enterprise Directory Integration	Integrates UC with repository of subscriber contact information accessible to all authorized and authenticated subscribers.
9. UC Application Integration	Supports mission and business applications integration with the enterprise UC (e.g., integration of UC provided presence with DoD Component-owned business applications).

(2) Unified Capabilities Transition.

(a) Details of the transition to UC are described in applicable implementation plans determined at the program and project levels. At those levels, the planning, time increment, and capability phasing, along with applicable gap analysis, are all part of the milestone activities. These activities, as coordinated through the Air Force and Army Unified Capabilities Implementation Plan (Reference 2), are guided by a UC transition approach.

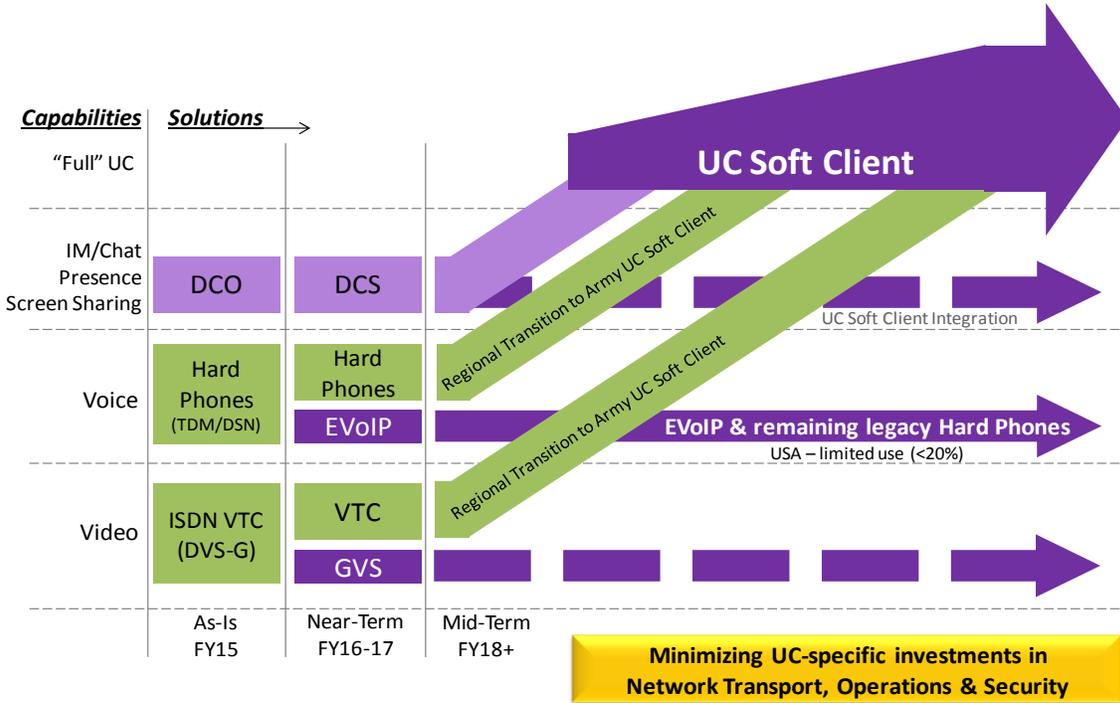


Figure 10. Forecasted UC Transition

(b) As shown in Figure 10, the focus is to shift from hardware-based VoIP solutions to a DoD enterprise software-based or “Soft” UC solution (e.g., UC Soft Client Solution) that provides users integrated voice, video, instant messaging/chat, presence/awareness and screen sharing on any approved device. When efforts have converged to an environment where this “Soft” UC solution exists, capabilities will reach a “Full” UC or To-Be architecture state. Note that although the objective is to achieve “Full” UC, the figure shows the future to include combined capabilities of “Full” UC and enterprise VoIP (EVoIP) hard phones and GVS. Until future capabilities beyond this To-Be architecture state are defined, this state represents the transition objective of current UC plans.

(c) As mentioned in Paragraph 2-2.d, Operational Context, the tactical enclave includes a mini-pod to support the tactical community. Although this RA does not address the details of the capability to support the tactical environment, activities supporting capabilities transition are being planned according to the Air Force and Army Unified Capabilities Implementation Plan (Reference 2). Those activities are summarized in Figure 11 below.

FY15-16	FY17-20
<ul style="list-style-type: none">• Transition institutional elements to enterprise UC Services• Address unclassified and secret networks, not TS networks• Extend UC client to communities supported by CAC/PKI solutions<ul style="list-style-type: none">• Plan for non-CAC population• Plan on extension of enterprise IdAM to tactical community (in conjunction with DoD Enterprise Email Program and DISA's Authentication Gateway Solution)• Identify future requirements and dependencies for extension of enterprise UC services to tactical environment	<ul style="list-style-type: none">• Focus on decommissioning of legacy equipment through voice and video lines of effort• Extend UC client service to tactical community (via mini-pod)<ul style="list-style-type: none">• Standardize UC Client• Integrate with existing tools and processes

Figure 11. Activities Supporting Capabilities Phasing with Tactical Consideration

d. *Detailed Description of Implementation States.* The ten implementation states described in Paragraph 3-5.b, are detailed below and shown in Figures 12 - 21.

(1) Legacy Environment (State 1a).

(a) The Legacy Environment, as depicted in Figure 12, is characterized by legacy solutions for voice, video, and data (IM/Chat, presence, and screen sharing) on separate networks based on legacy network transport (ATM, ISDN, and/or TDM).

- Voice networks may include End Office (EO), Small/Medium End Office (SMEO), and/or PBX. Sites may have a single instance or include sub-tended instances. These systems include voice-specific information transport (ISDN, Channel Banks, etc.), protection mechanisms (alarms and voice firewall), and end-user devices (phones).
- Video networks, based on MCUs, also may have multiple instances at a given site, although they are not often integrated. These systems rely on video-specific ISDN and end-user devices (codecs and peripherals).
- IM/Chat, presence, and screen sharing services are available from the enterprise (without directory integration) and/or locally (with local directory integration, but not integrated with the enterprise or generally, other instances). These services leverage the existing data network, data protection, and general purpose (computing) end-user devices.

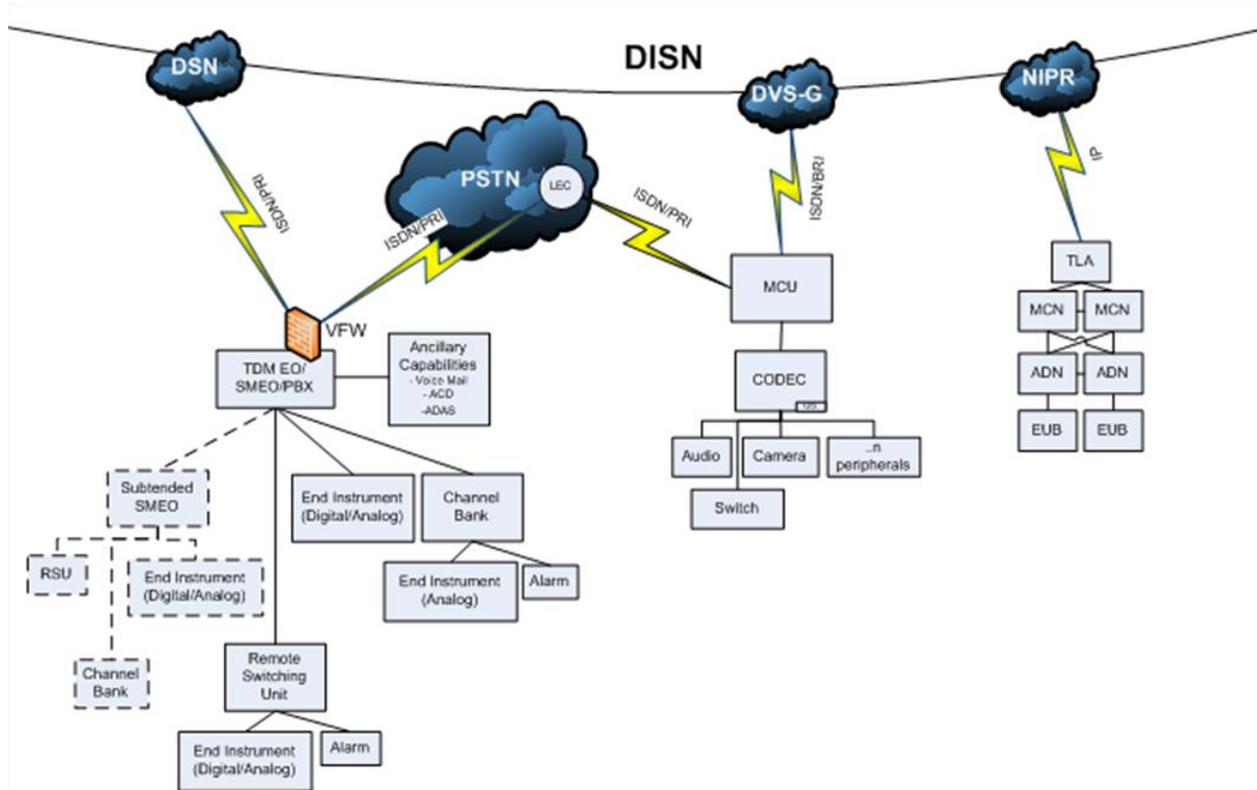


Figure 12. Legacy Environment (State 1a)

(2) Early VoIP (State 1b).

(a) The Early VoIP environment, as depicted in Figure 13, is characterized as follows:

- Voice services supported by the IP-based data network as well as dedicated networks based on legacy network transport (ATM, ISDN and/or TDM).
- All voice services rely on dedicated end-user devices (telephones).
- Video and data are delivered as described in the As-Is State 1a environment.

(b) This environment often results when a tenant unit installs its own IP-based voice service, which is subtended off the main post voice switch (EO/SMEO/PBX).

Note: Maintaining voice-specific legacy transport across the WAN does not fully support efficiencies that can be gained by transitioning away from dedicated WAN transport capability.

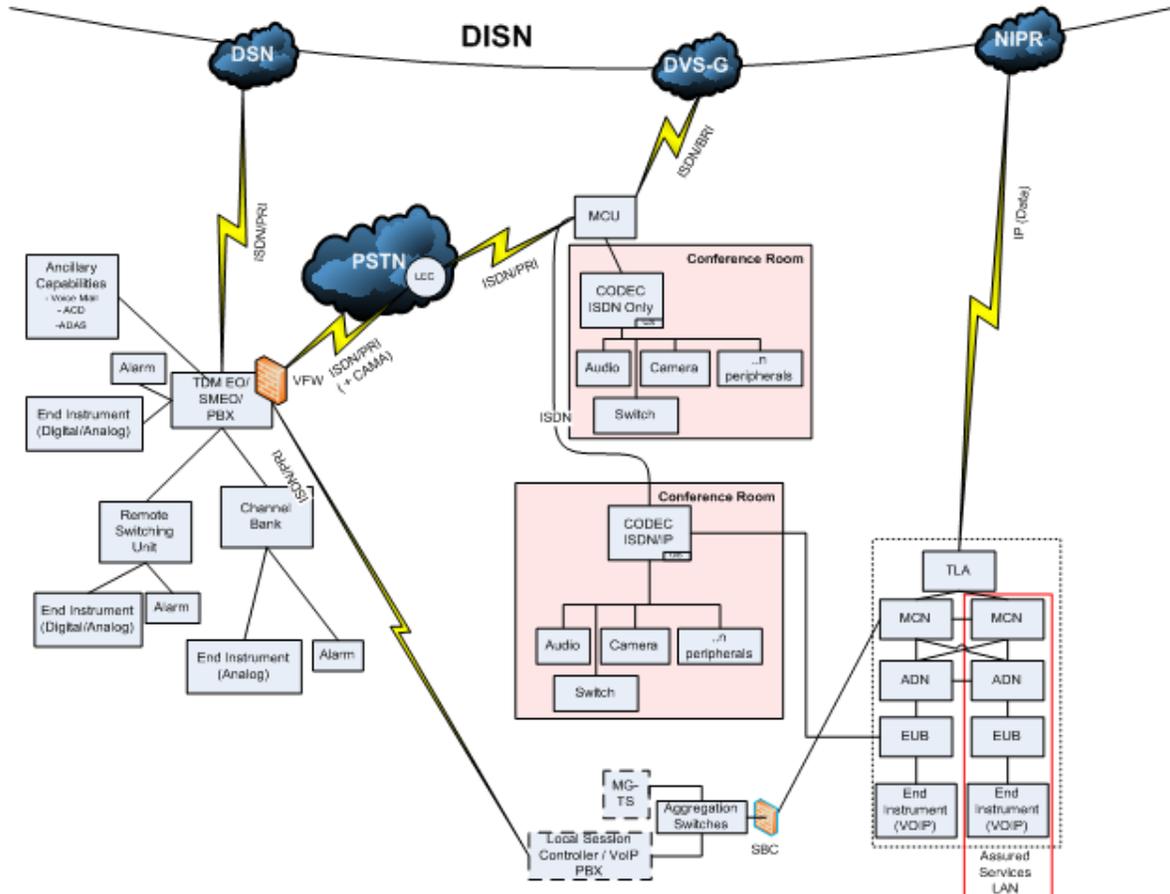


Figure 13. Early VoIP (State 1b)

(3) Hardware Voice Light (State 1c).

(a) The Hardware Voice Light environment, as depicted in Figure 14, generally results from an adjustment to the subtending arrangement described in State 1b, Early VoIP. This environment is characterized as follows:

- Voice-specific legacy transport on the WAN is reduced, but it is retained for emergency services and/or limited voice service when the data network is unavailable. This may be done without changing the end-user devices for legacy solution users.
- Video and data services are delivered as described in the As-Is State 1a environment.

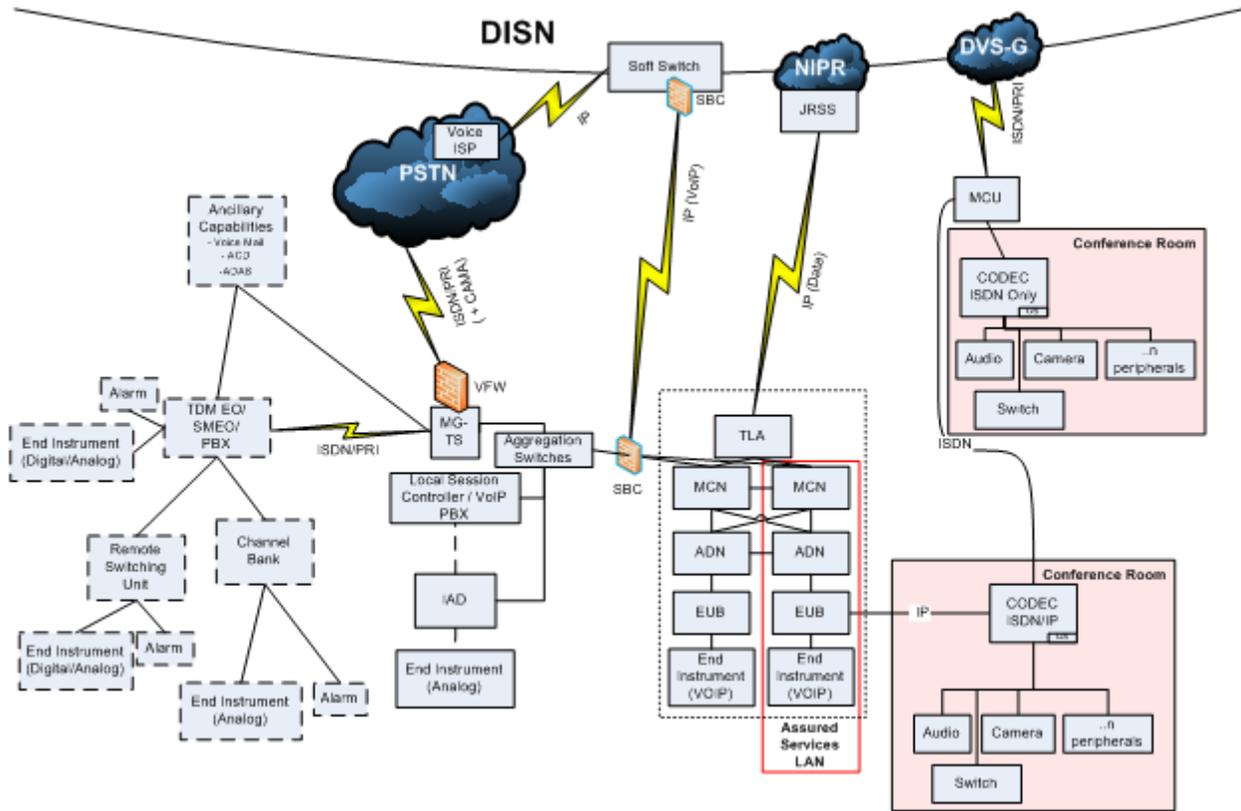


Figure 14. Hardware Voice Light (State 1c)

(4) UC Soft Client Solution only (State 2).

(a) The UC Soft Client Solution-Only environment, as depicted in Figure 15, is characterized as follows:

- UC services (voice, video, IM/chat, presence, screen sharing) are delivered to all users through general purpose computing end-user devices (desktop/laptop/mobile) over the data network (wired and wireless, including remote use).
- Voice service-specific end-user devices (telephones) are supported by dedicated legacy transport (TDM/ATM/ISDN) capabilities and protected with voice-specific solutions (voice firewall).
- Conference room video services are delivered through video-specific information transport (ISDN) and end-user devices (codecs and peripherals). Multiple instances may exist at a given site, although they are not often integrated.

Note: Legacy voice-specific solutions (supported by EO/SMEO/PBX) present increasing risk of voice service failure, and the continued use of legacy transport may increase costs as DISA begins to bill for these services in FY16.

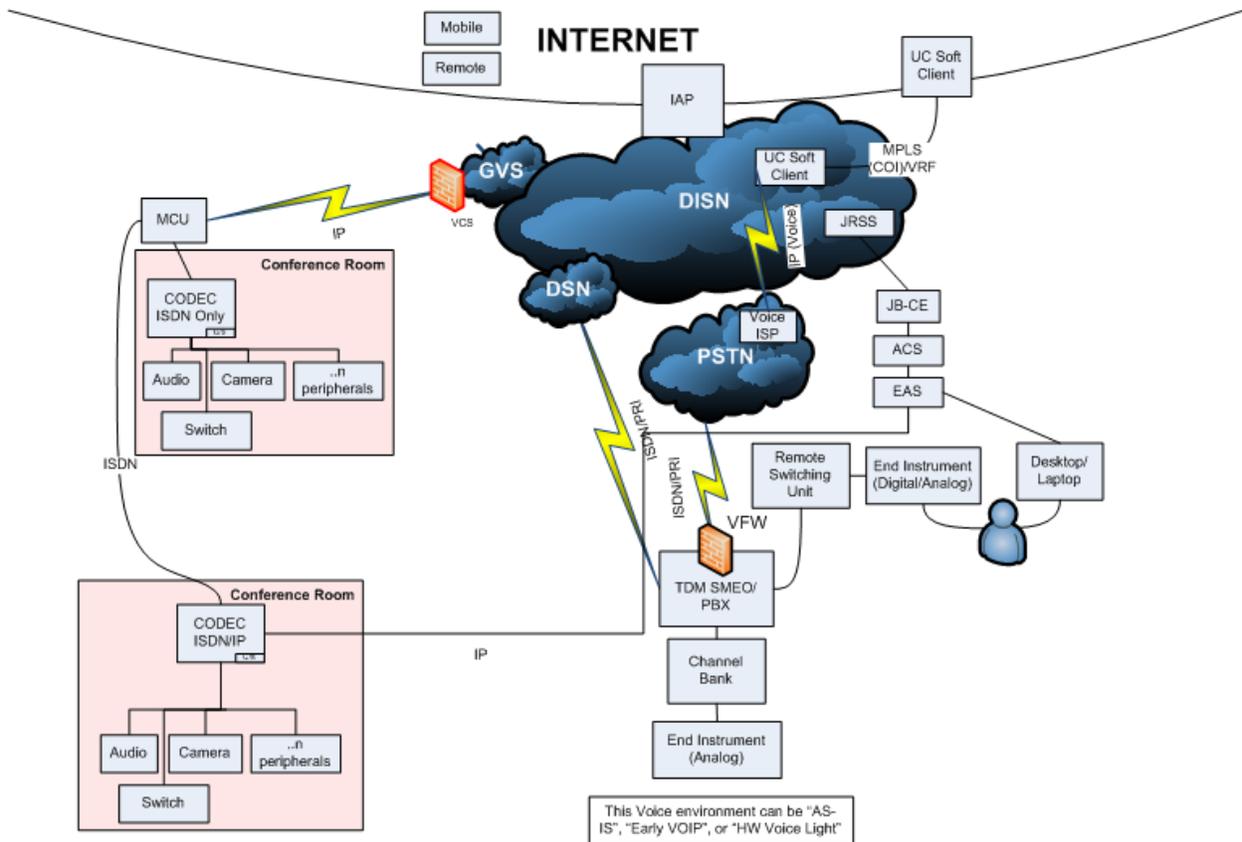


Figure 15. UC Soft Client Solution Only (State 2)

(5) Hardware Voice Only (State 3).

(a) The Hardware Voice Only environment, as depicted in Figure 16, is characterized as follows:

- Most legacy voice systems (TDM EO/SMEO/PBX) have been removed from the site. Legacy voice end-user devices (telephones) may still remain, although they will be integrated into the data network site. Voice services should be drawn over the WAN where diverse data network transport is available.
- Sites with assured services requirements will require a local voice system (e.g., FSC) to support emergency services and enable limited voice service when the data network is unavailable. Limited voice-specific transport (ISDN) is allowed on the WAN.

Note: This option may incur significant cost to replace or integrate legacy voice-specific end-user devices (phones) that will ultimately be replaced when UC Soft Client Solution is implemented.

- Conference room video services are delivered through video-specific information transport (ISDN) and end-user devices (codecs and peripherals). Multiple instances may exist at a given site, although they are not often integrated.

IM/Chat, presence, and screen sharing services are available from the enterprise (without directory integration) and/or locally (with local directory integration, but not integrated with the enterprise or generally, other instances). These services leverage the existing data network, data protection and general purpose (computing) end-user devices.

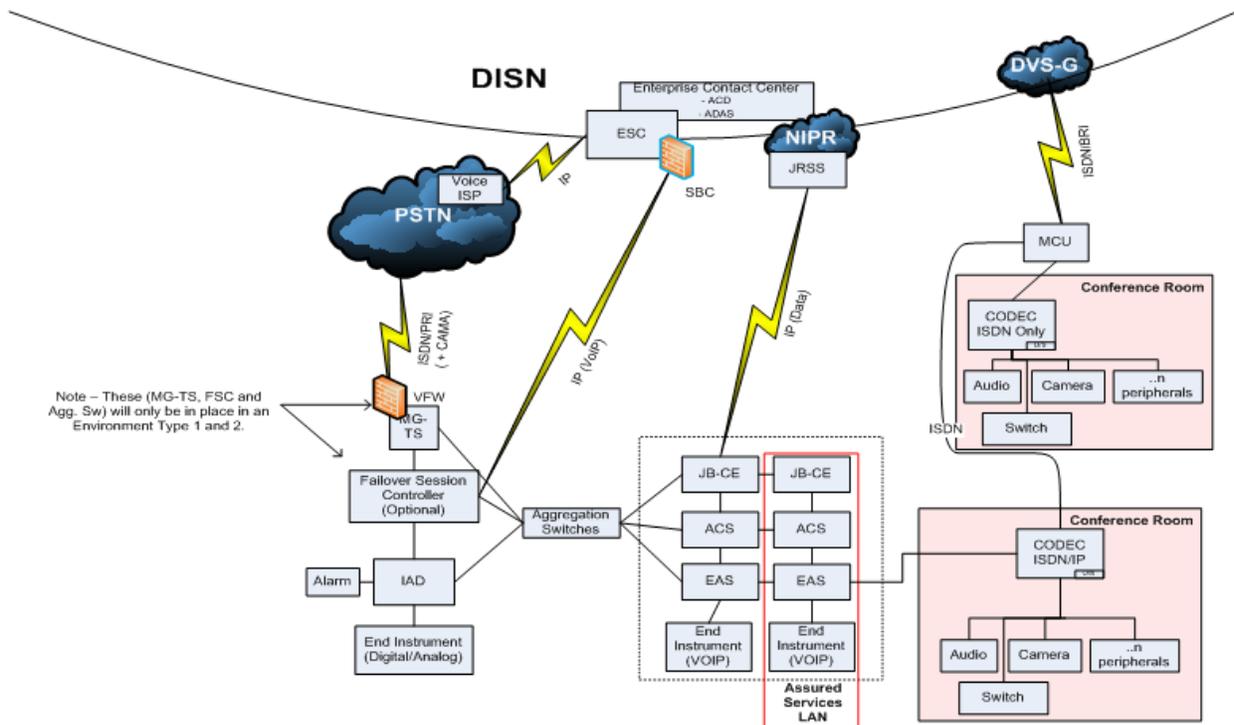


Figure 16. Hardware Voice Only (State 3)

(6) Hardware VTC Only (State 4).

(a) The Hardware VTC Only environment, as depicted in Figure 17, is characterized as follows:

- Video services have been modernized to leverage data network transport, delivered through video-specific end-user devices (codecs and peripherals). Video-specific data protection systems may be required (firewall traversal and/or session border control).
- Missions and locations with assurance requirements may operate their video services over an assured services network.
- Voice services are delivered through a dedicated end-user device (telephone) and voice-specific information transport (TDM/ATM/ISDN), and they are protected with voice-specific solutions (voice firewall).

Note: Legacy voice solutions (EO/SMEO/PBX) incur the risk of voice service failure; use of legacy transport may increase costs (DISA begins to bill for these services in FY16).

- IM/Chat, presence, and screen sharing services are available from the enterprise (without directory integration) and/or locally (with local directory integration, but not integrated with the enterprise or generally, other instances). These services leverage the existing data network, data protection and general purpose (computing) end-user devices.

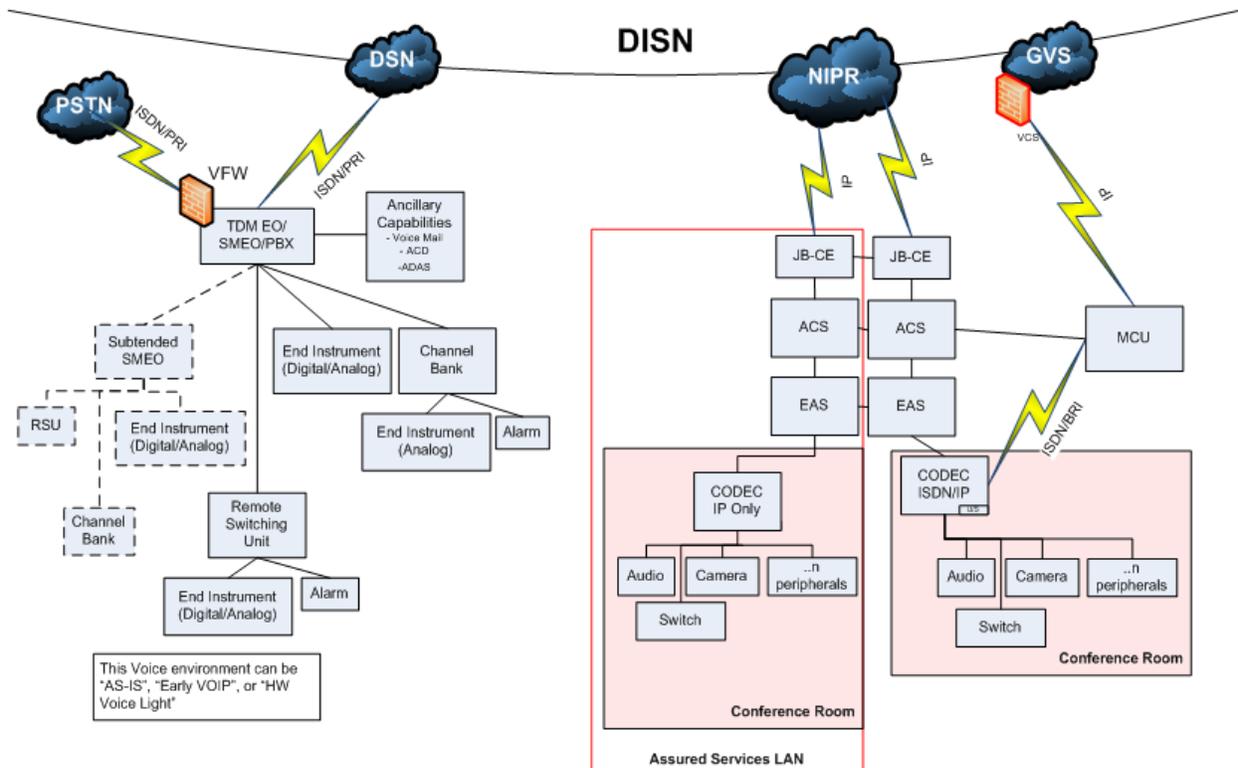


Figure 17. Hardware VTC Only (State 4)

(7) UC Soft Client Solution and Hardware Voice (State 5).

(a) The UC Soft Client Solution and Hardware Voice environment, as depicted in Figure 18, is characterized as follows:

- UC services (voice, video, IM/chat, presence, screen sharing) are delivered to all users through general purpose computing end-user devices (desktop/laptop/mobile) over the data network (wired and wireless, including remote use).
- A limited set of users also has voice-specific end-user devices (assured service VoIP phone over an assured services data network). Some legacy voice endpoints may also remain to provide service at locations without data network access (e.g., ranges) or for emergency use during power outages (e.g., elevators).
- Conference room video services are delivered through video-specific information transport (ISDN) and end-user devices (codecs and peripherals). Multiple instances may exist at a given site, although they are not often integrated.

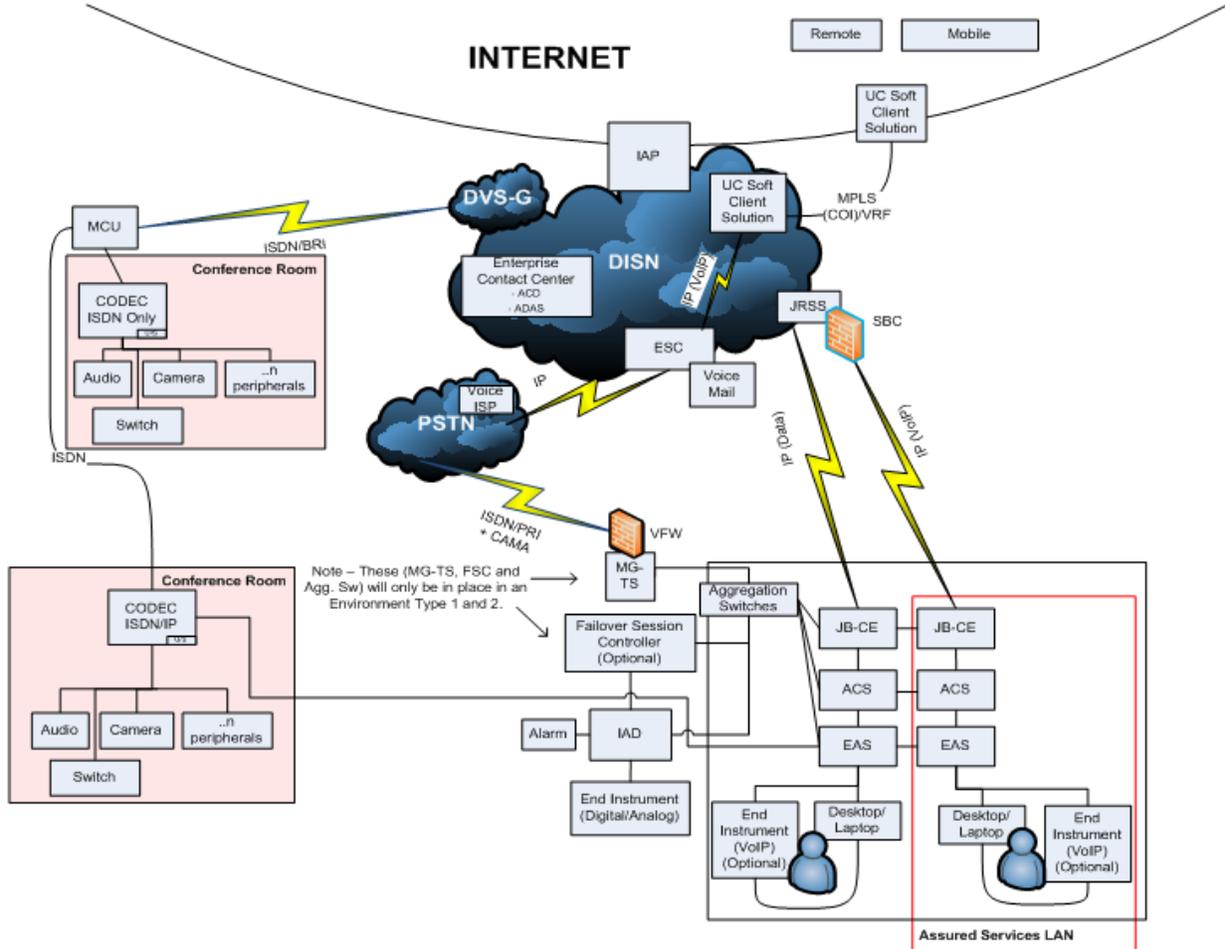


Figure 18. UC Soft Client Solution + Hardware Voice (State 5)

(8) UC Soft Client Solution and Hardware VTC (State 6).

(a) The UC Soft Client Solution and Hardware VTC environment, as depicted in Figure 19, is characterized as follows:

- Users have a legacy end-user device (telephone) and a software-based service (UC Soft Client Solution), providing integrated voice, video, instant messaging/chat, presence and screen sharing services.
- Conference room video services may be provided by either the software-based service (using general purpose computing end-user devices, likely with upgraded audio/visual hardware) or video-specific end-user devices (e.g., a VTC codec). The software-based service relies on the data network for transport and protection. The hardware-based service must use data network transport, although some sites may still have legacy transport within the site (this should be eliminated as soon as possible).
- This environment retains the risk of voice service failure in the legacy environment, although that is mitigated by the voice service available through the general purpose computing device (desktop/laptop).

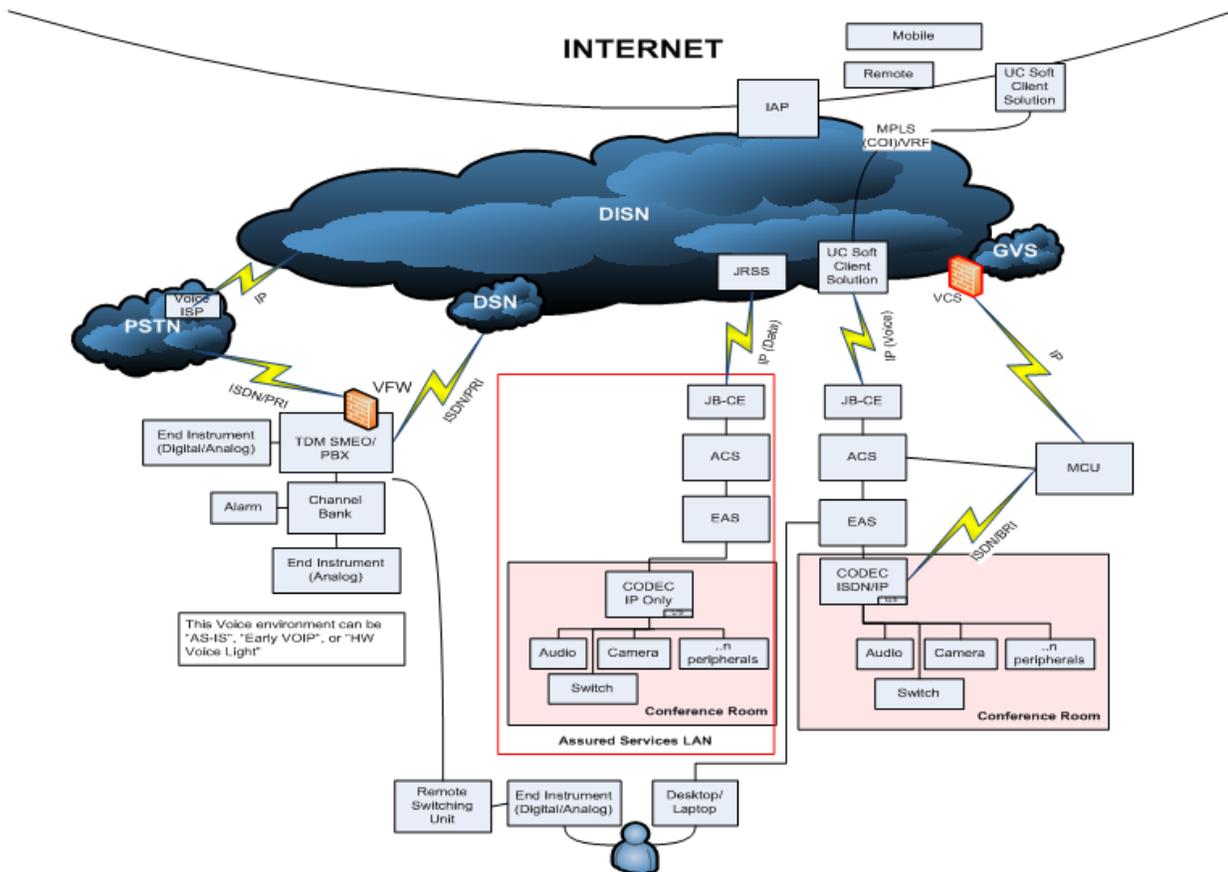


Figure 19. UC Soft Client Solution + Hardware VTC (State 6)

(9) Hardware Voice + Hardware VTC (State 7).

(a) The Hardware Voice and Hardware VTC environment, as depicted in Figure 20, is characterized as follows:

- Legacy voice and video services have essentially been tech refreshed to allow the use of the data network for information transport. Voice service, video service, IM/chat, and presence services are delivered separately and not integrated.
- Voice service is delivered through a dedicated end-user device (generally, VoIP telephone; legacy endpoints are strictly limited but also supported).
- Conference room video services are provided by video-specific end-user devices (e.g., a VTC codec) using data network transport, although some sites may still have legacy transport within the site (this should be eliminated as soon as possible).
- IM/chat and presence services are delivered through the general-purpose computing end-user device (desktop/laptop; typically not available on mobile devices).

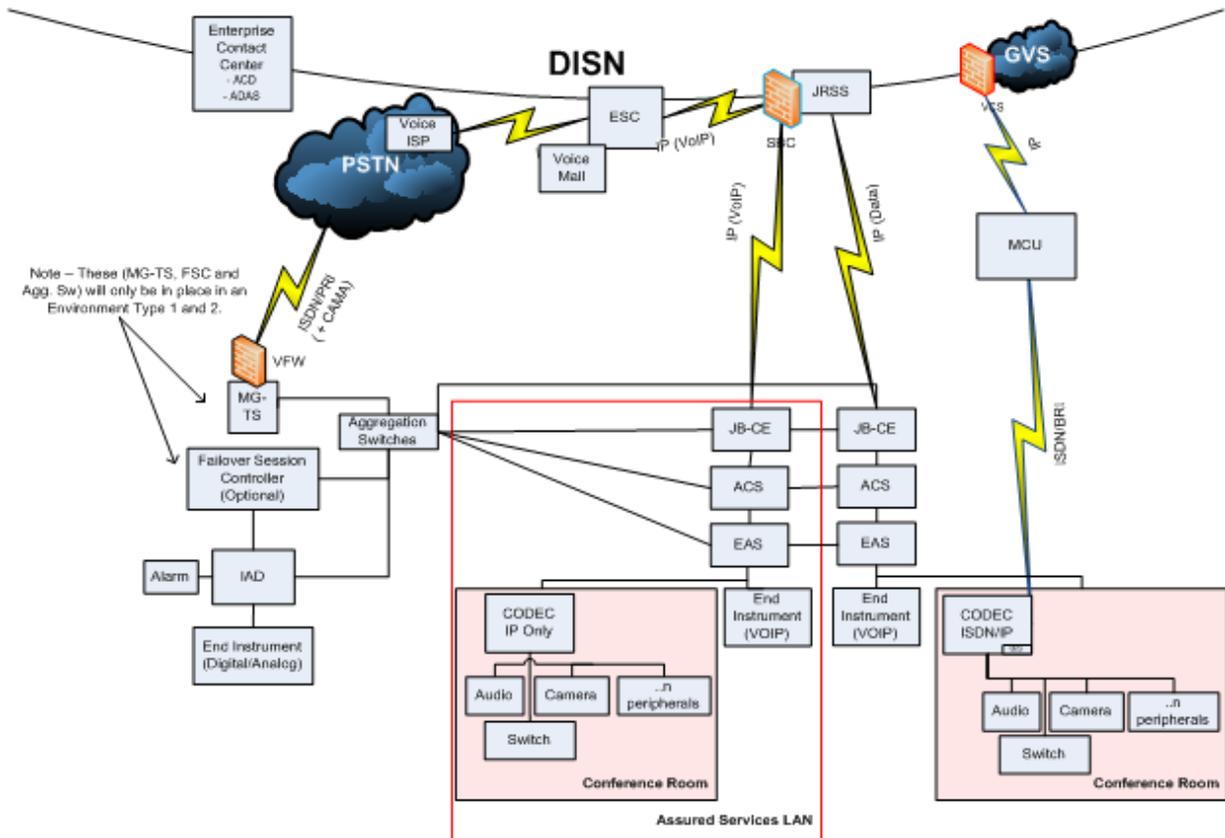


Figure 20. Hardware Voice + Hardware VTC (State 7)

(10) UC Soft Client Solution + Hardware Voice + Hardware VTC (State 8).

(a) The target To-Be institutional environment, as depicted in Figure 21, is characterized as follows:

- UC services are delivered to all users through general purpose computing end-user devices (desktop/laptop/mobile) over the data network (wired and wireless, including remote use).
- A limited set of users also has a voice-specific end-user device (assured service VoIP phone over an assured services data network).
- Conference room video services are provided by the software-based service using general purpose computing end-user devices, likely with upgraded audio/visual hardware.

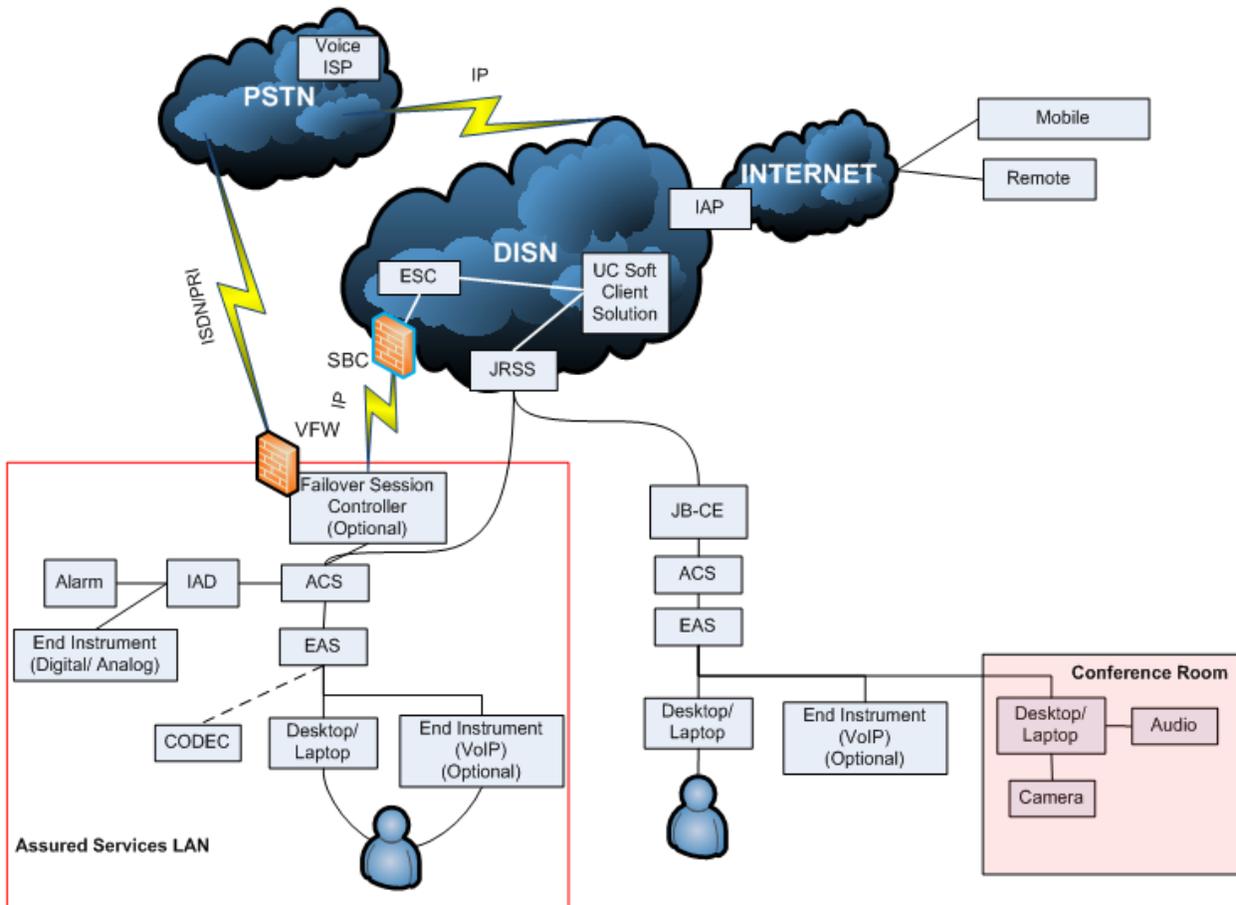


Figure 21. UC Soft Client Solution + Hardware Voice + Hardware VTC (State 8)

Chapter 5

Recommendations and Way Ahead

The Army is transitioning from costly legacy hardware-based solutions to a DoD enterprise software-based solution that will quickly provide users integrated voice, video, instant messaging/chat, presence and screen sharing on any approved end-user device. Ultimately, the transition to enterprise software-based UC services will reduce or eliminate legacy voice- and video-specific infrastructure costs. These UC capabilities will rely upon modernization efforts of network transport, security architecture, and emerging cloud-enabled infrastructure and services that will provide the foundation for enabling the transition toward UC.

5-1. Recommendations

It is recommended that Army UC efforts continue to ensure alignment with the ANCP (Reference 1). During planning and implementation, identify UC architecture issues and ensure coordination with HQDA CIO/G-6. Lastly, ensure the identification of requirements for decommissioning of legacy systems, tactical environment, special or unique networks, and classified networks, are available in a timely manner.

5-2. Way Ahead

CIO/G-6 Army Architecture Integration Center (AAIC) will continue to work and coordinate with stakeholders to complete, and is not limited to, the following:

- a. Participate in and support applicable UC Integrated Development Teams.
- b. Develop requirements for UC RA V3.0 in support of identified issues and concerns.
- c. Ensure future versions of the UC RA support Army UC development and implementation activities.

Appendix A References

Documents and links may have been updated since the release date of this Appendix; reviewers should refer to the applicable updated document or link for the latest information.

A-1. Required References

1. U.S. Army, HQDA, CIO/G-6; Army Network Campaign Plan 2020 and Beyond; ANCP-Implementation Guidance, Near-Term 2015 – 2016; ANCP-Implementation Guidance, Mid-Term 2017 – 2021 Version 1.2; February 2015; UNCLASSIFIED;
<http://ciog6.army.mil/AboutCIO/Mission/ANCP/tabid/237/Default.aspx>.
2. U.S. Air Force and U.S. Army; Air Force and Army Unified Capabilities Implementation Plan Version 1.0, September 2013; UNCLASSIFIED;
https://army.deps.mil/NETCOM/sites/7thSignal/7sctprojects/1to10/UCDataCall/Shared%20Documents/DISA%20Air%20Force%20Army%20UC%20Integrated%20Product%20Team/AF%20Army%20DISA%20UC%20Implementation%20Plan%20v1_1.docx. CAC required.
3. DoD CIO; DoD Information Enterprise Architecture Version 2.0; July 2012; UNCLASSIFIED;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf.
4. Joint Chiefs of Staff; Joint Capability Areas; 9 January 2015; UNCLASSIFIED;
https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas. CAC required.
5. U.S. Army, HQDA, CIO/G-6, AAIC; LandWarNet 2020 and Beyond Enterprise Architecture Version 2.0, 1 August 2014; UNCLASSIFIED;
http://ciog6.army.mil/Portals/1/Architecture/2014/20140801-LWN_2020_EA_V2-0.pdf.
6. DoD CIO; DoD Unified Capabilities (UC); 9 December 2010; DoDI 8100.04; UNCLASSIFIED; <http://dtic.mil/whs/directives/corres/pdf/810004p.pdf>.
7. DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED;
<http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf>.
8. U.S. Army, HQDA, CIO/G-6; U.S. Army Identity and Access Management Reference Architecture Version 4.0; 29 September 2014; UNCLASSIFIED;
http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US_Army_Identity_and_Access_Management_Reference_Architecture_V4-0.pdf.

9. U.S. Army, HQDA, CIO/G-6; U.S. Army Enterprise Cloud Computing Reference Architecture Version 1.0; 29 September 2014; UNCLASSIFIED;
<http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US Army Enterprise Cloud Computing Reference Architecture V1-0.pdf>.
10. U.S. Army, HQDA, CIO/G-6; U.S. Army Enterprise Service Management Reference Architecture Version 1.0; 20 May 2015; UNCLASSIFIED;
https://cadie.tradoc.army.mil/CIO-G6_20Architecture/Army%20EIEMA%20Architecture%20Documents/2%20-%20EIEMA%20Reference%20Architectures/20150520-US Army Enterprise Service Management Reference Architecture-V1-0.pdf.
11. U.S. Army, HQDA, CIO/G-6; U.S. Army End-User Devices Reference Architecture Version 1.0; 29 September 2014; UNCLASSIFIED;
<http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US Army End User Devices Reference Architecture and Annex V1-0.pdf>.
12. U.S. Army, HQDA, CIO/G-6; U.S. Army Network Operations Reference Architecture Version 1.0; 6 March 2014; UNCLASSIFIED;
<http://ciog6.army.mil/Portals/1/Architecture/2014/20140306-US Army NetOps Reference Architecture and Annex A-V1-0.pdf>.
13. U.S. Army, HQDA, CIO/G-6; U.S. Army Network Security Reference Architecture Version 2.0; 29 September 2014; UNCLASSIFIED;
<http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US Army Network Security Reference Architecture V2-0.pdf>.

A-2. Related References

14. U.S. Army, HQDA; Telecommunications and Unified Capabilities; 25 March 2013; Army Regulation (AR) 25-13; UNCLASSIFIED;
http://armypubs.army.mil/epubs/pdf/r25_13.pdf.
15. DoD CIO; DoD Enterprise-wide Access to Network and Collaboration Services (EANCS) Version 1.0; December 2009; UNCLASSIFIED;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/EANCS%20RA_Final_v1_20091221.pdf.
16. DoD CIO; DoD Active Directory Optimization Reference Architecture; 15 December 2010; UNCLASSIFIED;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/ADORA_Final_v1_20101215.pdf.
17. DoD CIO; DoD Information Enterprise Architecture Core Data Center Reference Architecture Version 1.0; 18 September 2012; UNCLASSIFIED;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/CDC%20RA%20v1_0_Final_Releaseable%20Version.pdf.
18. DoD CIO; DoD Joint Information Environment Enterprise Architecture (DoD JIE EA) Version 1.0; December 2012; UNCLASSIFIED;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/CDC%20RA%20v1_0_Final_Releaseable%20Version.pdf.

UNCLASSIFIED

19. DoD CIO; Cybersecurity; DoDI 8500.01; 14 March 2014; UNCLASSIFIED;
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.
20. U.S. Army, HQDA; Information Management Information Assurance; 23 March 2009; Army Regulation (AR) 25-2; UNCLASSIFIED;
http://armypubs.army.mil/epubs/pdf/r25_2.pdf.
21. National Institute of Standards and Technology (NIST); Guide for Applying the Risk Management Framework to Federal Information Systems; February 2010; NIST Special Publication 800-37; UNCLASSIFIED;
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

Appendix B Glossary of Acronyms

The following acronyms are applicable within this document.

Acronym	Description
AAIC	Army Architecture Integration Center
ACD	Automatic Call Distribution
ACS	Area Core Switch
ADAS	Automated Directory Assistance System
ADN	Area Distribution Node
ADORA	Active Directory Optimization Reference Architecture
AEN	Army Enterprise Network
AENC	Army Enterprise Network Council
AIA	Army Information Architecture
ANCP	Army Network Campaign Plan
AOR	Area of Responsibility
AR	Army Regulation
ArCADIE	Army Capability Architecture Development and Integration Environment
ARCYBER	U.S. Army Cyber Command
ASA(ALT)	Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Service – Session Initiation Protocol
ATM	Asynchronous Transfer Mode
BCA	Business Case Analysis
BMA	Business Mission Area
B/P/C/S	Base/Post/Camp/Station
BRI	Basic Rate Interface
CAC	Common Access Card
CAMA	Centralized Automated Message Accounting
CBA	Cost Benefit Analysis
CDC	Core Data Center
CE-R	Customer Edge Router
CIO	Chief Information Officer
CIRR	Computing Infrastructure Readiness Business Rules
COE	Common Operating Environment
COI	Community of Interest
CONUS	Continental United States

UNCLASSIFIED

Acronym	Description
CRL	Certificate Revocation List
CRP	Communications Readiness Principles
CTU	Conferencing Terminal Units
C&A	Certification & Accreditation
CV	Capability Viewpoint
DC	Data Center
DCS	Defense Collaboration Service
DECC	Defense Enterprise Computing Center
DEE	Defense Enterprise Email
DEPS	Defense Enterprise Portal Service
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
DMZ	Demilitarized Zones
DNS	Domain Name System
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVS	DISN Video Service
DVS - G	DISN Video Service - Global
DWDM	Dense Wavelength Division Multiplexing
EA	Enterprise Architecture
EANCS	Enterprise-wide Access to Network and Collaboration Services
EAS	Edge Access Switch
EASF	Enterprise Attribute Application Forest
EBC	Edge Border Controller
ECC	Enterprise Cloud Computing
EDS	Enterprise Directory Service
EI	End Instruments
EIEMA	Enterprise Information Environment Mission Area
EO	End Office
EOC	Enterprise Operations Center

UNCLASSIFIED

Acronym	Description
ES	Enterprise Services
ESC	Enterprise Session Controller
ESD	Enterprise Services Domain
ESM	Enterprise Service Management
EUB	End-User Building
EUD	End-User Devices
EVVoIP	Enterprise Voice over Internet Protocol
E911	Emergency 911
FSC	Failover Session Controller
FY	Fiscal Year
GIG	Global Information Grid
GP	Global Principle
GMPLS	Generalized Multiprotocol Label Switching
GTP	GIG Technical Profiles
GVS	Global Video Service
GW	Gateway
HQDA	Headquarters Department of the Army
HW	Hardware
IA	Information Assurance
IAD	Integrated Access Device
IAP	Internal Access Point
ICAN	Installation Campus Area Network
ID	Identity
IdAM	Identity and Access Management
IDSS	Identity Synchronization Service
IE	Information Enterprise
IEA	Information Enterprise Architecture
IM	Instant Messaging
IP	Internet Protocol
I/P	IMMEDIATE/PRIORITY
IPN	Installation Processing Node
IS	Information Systems
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IVR	Interactive Voice Response

UNCLASSIFIED

Acronym	Description
JB CE-R	Joint Base Customer Edge Router
JCA	Joint Capability Area
JIE	Joint Information Environment
JRSS	Joint Regional Security Stack
KPP	Key Performance Parameter
KSA	Key System Attribute
LAN	Local Area Network
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
LOE	Line of Effort
LSC	Local Session Controller
LWN	LandWarNet
MCEP	Multi-Carrier Entry Point
MCN	Multi-Channel Network
MCU	Multipoint Control Unit
MFSS	Multifunction Soft-Switch
MG (or MGW)	Media Gateway
MG-TS	Media Gateway Transport System
MILDEP	Military Department
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPG (or MPGW)	Mission Partner Gateway
MP (or MLPPP)	Multilink Protocol
MPLS	Multiprotocol Label Switching
NCD	Network Capacity Domain
NETCOM	Network Enterprise Technology Command
NetOps	Network Operations
NGOs	Non-Governmental Organizations
NIPR	Non-Classified Internet Protocol Router
NIST	National Institute of Standards and Technology
NMA	Network Management Area
NORA	Network Optimization Reference Architecture
NS	Network Security
NSD	Network Operations and Security Domain
OCONUS	Outside Continental United States

UNCLASSIFIED

Acronym	Description
OCSP	On-line Certificate Status Protocol
OLA	Operational Level Agreement
PBX	Private Branch Exchange
PEO	Program Executive Office
PEO EIS	Program Executive Office Enterprise Information Systems
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PM	Program Manager
PSTN	Public Switched Telecommunications Network
PRI	Primary Rate Interface
P&R	Policy & Resources
QoS	Quality of Service
RA	Reference Architecture
RCVS	Robust Certificate Validation System
RFC	Request for Comment
RMF	Risk Management Framework
RSU	Remote Switching Unit
SaaS	Software-as-a-Service
SAP	Secured Availability Principles
SAR	Secured Availability Business Rules
SBC	Session Border Controller (formerly known as Edge Border Controller)
SC	Session Controller
SCN	Switched Circuit Network
SG	Signaling Gateway
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SMEO	Small/Medium End Office
SOA	Service Oriented Architecture
SP	Special Publication
SS	Soft Switch
StdV	Standard Viewpoint
STE	Secure Terminal Equipment
SvcV	Services Viewpoint
SW	Software
Sw	Switch

UNCLASSIFIED

Acronym	Description
TDM	Time Division Multiplexing
TLA	Top Level Architecture
TRADOC	U.S. Army Training and Doctrine Command
UAP	Unified Action Partners
UC	Unified Capabilities
UCS	Unified Capabilities Specific
UC MP	Unified Capabilities Master Plan
UCR	Unified Capabilities Requirements
VCS	Virtual Cluster Switching
VFW	Virtual Firewall
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTC	Video Teleconferencing
WAN	Wide Area Network
WAN SS	Wide Area Network Soft Switch
WMA	Warfighter Mission Area
3G, 4G	Third Generation, Fourth Generation

**Appendix C
Integrated Dictionary (AV-2)**

Sources for many of the following vocabulary and terms below are specified. For items without a specified source, definitions were established based on government general usage (e.g., briefings, papers, etc.) and industry best practices.

Acronym	Term	Description	Reference
APL	Approved Products List	A list of products that have received Joint Interoperability Certification and Information Assurance Accreditation from the Defense Information System Network Designated Approval Authorities in accordance with the Department of Defense Instruction (DoDI) 8100.04. The list is published on the Joint Interoperability Test Command home page (https://aplits.disa.mil).	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
n/a	Assured Service	The ability of a system to optimize session completion rates for all IMMEDIATE/PRIORITY (I/P) users despite degradation because of network disruptions, natural disasters, or surges during crisis or war.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
AS-SIP	Assured Services Session Initiation Protocol	A session signaling protocol consisting of a defined set of Session Initiation Protocol signaling standards and incorporating Department of Defense Assured Service functionality.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Collaboration	The ability to conduct synchronous and asynchronous communications and interaction across the enterprise, including voice, data, video, and manipulated visual representation. JCA 6.2.3.2	Joint Chiefs of Staff; Joint Capability Areas; 9 January 2015; UNCLASSIFIED; https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas . CAC required.
CE-R	Customer Edge Router	A router located at the boundary between the Edge Segment and the Access Segment of the wide area network. The CE-R provides traffic conditioning, bandwidth management on a granular service class (i.e., voice, video) basis, and quality of service using per-hop behaviors. A B/P/C/S may have a single CE-R or multiple CE-Rs based on the local architecture. (Note: Edge Segment refers to the Edge Access layer (See Figure 3 of this UC RA) where EIs (e.g., laptops, hard phones, VTC suites) reside. Access Segment refers to that part of the Installation Core layer that connects to the DISN Core. The CE-R is a key Army B/P/C/S component connecting EIs to the network.)	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
CDC	Core Data Center	<p>A fixed DoD data center (DC) meeting DoD standards for facility and network infrastructure, security, technology, and operations and adhering to enterprise governance under a "franchise" model. Functions and services delivered by current DISA Defense Enterprise Computing Centers (DECCs), Component Enterprise DCs and Component Installation DCs will be consolidated to the greatest extent possible into CDCs totaling a few dozen at most. CDCs will be selected from existing Component data centers.</p>	<p>DoD CIO; DoD Information Enterprise Architecture Core Data Center Reference Architecture Version 1.0; 18 September 2012; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/CDC%20RA%20v1_0_Final_Releaseable%20Version.pdf.</p>
DISN	Defense Information Systems Network	<p>The DISN is an integrated network, centrally managed, and configured to provide long-haul information transfer services for all DoD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services.</p> <p>Also, the DISN is a worldwide-protected telecommunications network that enables the exchange of information in an interoperable and global space, partitioned by security demands, transmission requirements, and geographic needs of targeted end-user communities. The DISN offers a selection of integrated standards-based services to fulfill these connectivity needs.</p>	<p>http://www.disa.mil/network-services.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
DISN Core Layer	Defense Information Systems Network Core Layer	The DISN is a worldwide-protected telecommunications network that enables the exchange of information in an interoperable and global space, partitioned by security demands, transmission requirements, and geographic needs of targeted end-user communities. The DISN offers a selection of integrated standards-based services to fulfill these connectivity needs.	http://www.disa.mil/network-services .
DVS-G	Defense Information Systems Network Video Service-Global	The DVS-G is a service provided by the Defense Information Systems Agency. It is meant to provide a bridging service for DoD VTC users. It uses industry standards for interoperability and multipoint VTC requirements. The DVS-G has three operational areas - CONUS, Europe, and Pacific.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
DSC	Data Storage Controller	A DSC is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in B/P/C/S networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services LAN (ASLAN), but the DSC is not considered part of the ASLAN.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
ES	Enterprise Services	An enterprise service is any capability provided for broad use across the DoD that enables awareness of, access to, or delivers information across DoD networks. Enterprise services may be provided by any source within the DoD or any trusted partners. Enterprise services providing data or information must be authoritative and, therefore, trusted as being accurate, complete, and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source. Enterprise services include environments that are composed of multiple service layers such as the infrastructure, infrastructure services, platform services, common user services, enterprise service management, and mission assurance services.	DoD Instruction (DoDI) 8330.01, Interoperability of IT including National Security Systems, 21 May 2014; http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf .
ESC	Enterprise Session Controller	Centrally located Session Controller that provides UC services to multiple DoD Component sites.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
FSC	Failover Session Controller	<p>Session Controller located at a DoD Component Mission Environment Type 1 site that is part of an Enterprise Services Area. The DSC provides certain UC services to the site when access to the Enterprise Session Controller is interrupted.</p> <p>Call Processor located at a DoD Component Mission Environment Type 2 site that provides ROUTINE intra-site calling capability, and PSTN/DSN/E911 access via a local Media Gateway, when access to the Enterprise Session Controller is interrupted.</p>	<p>U.S. Air Force and U.S. Army; Air Force and Army Unified Capabilities Implementation Plan Version 1.0, September 2013; UNCLASSIFIED.</p> <p>DoD CIO; DoD Unified Capabilities Master Plan (UC MP); October 2011; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/Policies-and-Procedures.</p>
GP	Global Principles	<p>A designation of a type of principle as identified in Appendix B, DoD IEA Principles and Business Rules, of the source document.</p>	<p>DoD CIO; DoD Information Enterprise Architecture Version 2.0; July 2012; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf.</p>
n/a	Hard Phone	<p>A conventional telephone set, which is a single function terminal, hardwired to support voice communications. A hardphone is in sharp contrast to a softphone, which is a software-based telephone comprising a desktop, laptop, or tablet computer equipped with a microphone, a speaker, and software that allows it to emulate a hardphone.</p>	<p>http://www.yourdictionary.com/hardphone.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
IAP	Internet Access Point	A network exchange facility where Internet Service Providers (ISPs) connect with the DoD networks in a peering arrangement. The connections within IAPs determine traffic routing to DoD networks and the Internet.	Department of Defense (DoD) Unified Capabilities Master Plan (UC MP); October 2011; UNCLASSIFIED; http://www.disa.mil/network-services/UCCO/~media/Files/DISA/Services/UCCO/APL-Process/Unified_Capabilities_Master_Plan.pdf
IM and Chat	Instant Messaging and Chat	The capability for users to exchange one-to-one ad hoc text messages over a network in real time. IM is not the same as and must not be confused with signaling or equipment messaging; 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.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
JCA	Joint Capability Areas	Collections of like DoD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning.	Joint Chiefs of Staff; Joint Capability Areas; 9 January 2015; UNCLASSIFIED; https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas . CAC required.

UNCLASSIFIED

Acronym	Term	Description	Reference
LWN	LandWarNet	<p>(1) The Army's portion / contribution to the DoD Information Enterprise.</p> <p>(2) The IT environment that provides IT capabilities to Army users and Unified Action Partners. Its scope includes the Army's IT infrastructure plus all of the people, processes, and technologies required to provide those IT capabilities.</p> <p>Note: A related term, "Army network," is also used in the Army Network Campaign Plan 2020 and Beyond, Version 1.2, February 2015:</p> <p>The network of the future is a secure, integrated, standards-based environment that ensures uninterrupted global access and enables collaboration and decisive action through all operational phases across all environments. The network envisioned spans all Army operations, from administrative operations in garrison to the most forward-deployed Soldier at the tactical edge.</p>	<p>U.S. Army, HQDA, CIO/G-6, AAIC; LandWarNet 2020 and Beyond Enterprise Architecture Version 2.0, 1 August 2014; UNCLASSIFIED; http://ciog6.army.mil/Portals/1/Architecture/2014/20140801-LWN_2020_EA_V2-0.pdf.</p> <p>U.S. Army, HQDA, CIO/G-6; Army Network Campaign Plan 2020 and Beyond; ANCP-Implementation Guidance, Near-Term 2015 – 2016; ANCP-Implementation Guidance, Mid-Term 2017 – 2021 Version 1.2; February 2015; UNCLASSIFIED; http://ciog6.army.mil/About/CIO/Mission/ANCP/tabid/237/Default.aspx.</p>
LSC	Local Session Controller	<p>(1) LSC is an AS-SIP signaling device at a B/P/C/S that directly serves IP EIs.</p> <p>(2) A session controller that is located at the same DoD Component site as the End Instruments that it serves.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~/_media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
MG or MGW	Media Gateway	<p>A MG within the DoD environment is defined in accordance with the Internet Engineering Task Force Request for Comments 2805, "Media Gateway Control Protocol Architecture and Requirements," and provides the media mapping and/or transcoding functions between time division multiplexing and IP networks. The MG terminates switched circuit network (SCN) facilities (e.g., trunks, loops), packetizes the media stream, if it is not already packetized, and delivers packetized traffic to an IP network. It would perform these functions in the reverse order for media streams flowing from the IP network to the SCN.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf.</p>
MCU	Multipoint Control Unit	<p>An endpoint that enables intercommunication of three or more VTC endpoints in a conference call. It can be used with two VTC endpoints, for example, while beginning or ending a multipoint conference. The MCU may perform mixing or switching of audio, video, and data.</p> <p>A multipoint device, by means of which three or more conferencing terminal units (CTUs) may intercommunicate in a conference call. It can also be used with two CTUs; e.g., while beginning or ending a multipoint conference.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Non-Assured/Assured Voice, Video, and Data Session Management	Provides enterprise point-to-point UC, independent of the technology (circuit switched or IP). Functionalities 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, etc.).	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
Non-Assured/Assured Voice and VTC	Non-Assured/Assured Voice and Video Teleconferencing	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.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
Non-ASLAN	Non-Assured Service Local Area Network	The IP network infrastructure components used to provide services (i.e., voice, video, and data) to end users. Non-ASLANs are “commercial grade” and provide support to IMMEDIATE/PRIORITY (I/P) (ROUTINE only calls) (I/P(R)) or non-I/P voice subscribers.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
n/a	Non-Assured Service	A service (voice, video, or data) with none or any combination of the elements of assured service but not all of the elements of assured service (i.e., assured availability, assured protection, and assured delivery). For example, the service may establish audio or video sessions independent of any session admission control exercised by a session controller or H.323 Gatekeeper.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Presence/Awareness	A status indicator that conveys ability and willingness of a potential user to communicate.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
n/a	Physical Diversity	Route diversity is communications routing between two points over more than one geographic or physical path with no common points.	https://transition.fcc.gov/pshs/techtopics/techtopics14.html#fn2
n/a	Principles	Principles are high level statements that apply to the subject area and tie back to business/warfighting requirements. They incorporate values and organizational culture, and drive technical positions and patterns in defining how an organization fulfills its mission. The identification of assumptions and constraints can assist in gaining an understanding of the context of the RA, which can provide a helpful perspective on the guiding principles.	DoD CIO, Reference Architecture Description; June 2010; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
PKI	Public Key Infrastructure	An enterprise-wide service (i.e., data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption, and digital signature) that supports digital signatures and other public key-based security mechanisms for Department of Defense functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. A public key infrastructure provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable certification authority.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
QoS	Quality of Service	The capability to provide resource assurance and service differentiation in a network. Used with the local area network to provide different priority to traffic flows or sessions, or guarantee a certain level of performance to a traffic flow or session in accordance with requests from the application program. QoS is used in conjunction with traffic tagging to guarantee that prioritized traffic flows or sessions are given preferential treatment. Also, the collective effects of service performances that determine the degree of satisfaction of a user of the service.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
RA	Reference Architecture	<p>(1) Reference architecture guides and constrain the instantiations of solution architectures. It also provides a common language for various stakeholders, guidance and consistency of implementations of technology to solve problems, supports the validation of solutions, and encourages adherence to common standards, specification and patterns. Reference Architecture normalizes the institutional understanding of capabilities at the enterprise level, and provides a common set of principles/rules, process patterns, and technical positions for use within the DoD to guide development of Enterprise, Segment, or Solution architectures.</p> <p>(2) Reference Architecture is defined as an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. This definition is applicable to all of DoD.</p>	<p>DoD CIO, Reference Architecture Description; June 2010; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Router	<p>A router is an appliance that is a packet switch that operates at the network layer of the Open Systems Interconnection Protocol model. Routers within the IP Unified Capabilities architecture interconnect networks over local and wide areas, and provide traffic control and filtering functions when more than one pathway exists between two endpoints on the network. The primary function of routers is to direct IP packets along the most efficient or desired path in a meshed network that consists of redundant paths to a destination. Many routers in the DoD IP UC architecture include local area network switch functions and the distinction between the two types of appliances continues to blur.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf.</p>
SIPRNet	SECRET Internet Protocol Router Network	<p>SIPRNet is DoD's largest interoperable command and control data network supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. SIPRNet provides secure, seamless, interoperable, and common user packet switched data communications services to mission partners with access data rates ranging from 56 Kbps to 1.0 Gbps. Remote dial-up services are available up to 115 Kbps, and services to the Tactical community are available via Integrated Tactical-Strategic Data Network /Standard Tactical Entry Point (ITSDN/STEP) sites.</p>	<p>http://www.disa.mil/Network-Services/Data/Secret-IP</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
SBC	Session Border Controller	<p>An appliance that provides voice and video firewall functions. SBCs are typically located at the boundary between the edge segment and the access segment. The SBC exerts control over the signaling and media streams and is involved in setting up, conducting, and terminating sessions. Formerly known as the Edge Boundary Controller (EBC), the SBC acts as a firewall for voice and video traffic at the ASLAN enclave boundary.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework2013.pdf.</p>
SIP	Session Initiation Protocol	<p>The SIP is "...an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences."</p>	<p>Network Working Group; Request for Comments: 3261 SIP: Session Initiation Protocol; June 2002; UNCLASSIFIED; https://www.ietf.org/rfc/rfc3261.txt.</p>
SS	Soft Switch	<p>A stand-alone Approved Products List product that acts as an AS-SIP Back-to-Back User Agent within the UC architecture. It provides the equivalent functionality of a commercial soft switch, which is a central device in a telecommunications network which connects telephone calls from one phone line to another, across a telecommunication network or the public Internet, entirely by means of software running on a general-purpose computer system. The functionality of the session controllers is a conditional requirement and the support of a Signaling Gateway is not required.</p>	<p>DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework2013.pdf.</p>

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Soft Client	A PC or mobile software application providing UC or telephony over the network, replacing or supporting / enhancing a hardware device.	http://www.unify.com/us/support/industry-term-glossary.aspx .
n/a	Technical Positions and Patterns	Technical positions describe the technical guidance and standards established for UC. Defining technical positions forces an organization to identify relevant technical guidance and standards and justify their choices and tradeoffs. Technical guidance and standards, based on specified principles that need to be followed and implemented as part of the solution. Patterns provide how UC artifacts may be organized and related for repeated use. They are typically descriptions of structural, behavioral, or graphical model instantiations that focus on interaction of the artifacts. Patterns will undergo change as new pattern concepts are discovered and emerge from solution architectures.	DoD CIO, Reference Architecture Description; June 2010; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf
UAP	Unified Action Partners	Unified action partners are those military forces, governmental and nongovernmental organizations, and elements of the private sector with which Army forces plan, coordinate, synchronize, and integrate during the conduct of operations.	TRADOC; The U.S. Army Functional Concept for Engagement; 24 February 2014; TRADOC Pamphlet 525-8-5; UNCLASSIFIED; http://www.tradoc.army.mil/tpubs/pams/tp525-8-5.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
UCS Rules	Unified Capabilities Specific Rules	UCS rules represent relationships among the UC inputs, controls, outputs and mechanisms, and resources used. For example, a UCS rule can specify who can do what under specified conditions, the combination of inputs and controls needed, and the resulting outputs. UCS rules are based on best practices and provide design tenets and constrain the implementation of principles and relevant policies.	Used in this document.
UC Applications Integration	Unified Capabilities Applications Integration	Supports mission and business applications integration with the enterprise UC (e.g., integration of UC provided presence with DoD Component-owned business applications).	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
UC	Unified Capabilities	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.	U.S. Air Force and U.S. Army; Air Force and Army Unified Capabilities Implementation Plan Version 1.0, September 2013; UNCLASSIFIED; https://army.deps.mil/NETCOM/sites/7thSignal/7sctprojects/1to10/UCDataCall/Shared%20Documents/DISA%20Air%20Force%20Army%20UC%20Integrated%20Product%20Team/AF%20Army%20DISA%20UC%20Implementation%20Plan%20v1_1.docx .

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	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.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
n/a	Video	The technology of capturing, recording, processing, storing, transmitting, and reconstructing in electronic form, a sequence of still images representing scenes in motion.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
VTC	Video Teleconferencing	Two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communication. Meetings, seminars, and conferences are conducted as if all the participants are in the same room. Video teleconferencing provides the capability to exchange and distribute combinations of voice, video, imagery, messages, files, and streams. Also, VTC can be described from a Service perspective (from Table 4): Provides multiple video users with the ability to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
Voice ISP Access	Voice Internet Service Provider Access	Provides unclassified and classified enterprise UC for access to commercial voice services over IP. This service provides both local and long distance dialing capability using commercial ISPs via secure interconnections.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
VoIP System	Voice over Internet Protocol System	A set of components required to provide DSN IP voice services from EI to DSN trunk, or IP phone to IP phone. The VoIP system includes, but is not limited to, the IP telephony instrument, the local area network, the local session controller, and the IP gateway.	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .
VoSIP	Voice over Secure Internet Protocol	The instantiation of IP Telephony on a classified local area network or wide area network infrastructure that provides the routing of voice conversations using the Secret Internet Protocol Router Network (SIPRNet) as the transport medium. The use of the SIPRNet allows users in secure environments to communicate at the Secret level without the need for specialized phones or the use of key material (i.e., bidirectional interoperability).	DoD CIO; DoD Unified Capabilities Framework 2013; January 2013; UNCLASSIFIED; http://www.disa.mil/Network-Services/UCCO/~media/Files/DISA/Services/UCCO/UCR2013/01_Framework_2013.pdf .

UNCLASSIFIED

Acronym	Term	Description	Reference
n/a	Voice and Video (Point-to-Point)	Provides two voice and/or video users with the ability to be connected End-to-End with services that can include capabilities such as voicemail, call forwarding, call transfer, call waiting, operator assistance, and local directory services.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
n/a	Voice Conference	Provides multiple voice users with the ability to conduct a collaboration session.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .
n/a	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.	DoD CIO; DoD Unified Capabilities Reference Architecture Version 1.0; January 2013; UNCLASSIFIED; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Approved%20DoD%20UC%20Reference%20Architecture.pdf .

Appendix D Technical Standards

a. The Standards Profile (StdV-1), Standards Forecast (StdV-2), and Non-DISR Standards are not in this document due to their changing nature.

b. The standards can be found in an addendum on <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>.

Administrative Information

Approval Authority. HQDA CIO/G-6.

Distribution and Use Restrictions. This document is intended for use by US Government agencies and their Contractors doing business with the U.S. Army.

Document Custodian. The Custodian for this document is CIO/G-6, SAIS-AEA, usarmy.pentagon.hqda-cio-g-6.list.architecture@mail.mil.

-----Nothing follows-----