TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

APPENDIX A
UNIQUE DEPLOYED (TACTICAL)

This Section contains explanatory text related to Unified Capabilities Requirements (UCR) 2013, Appendix A, Unique Deployed (Tactical). This section's intent is to provide a framework to identify usable, common communications system operating standards (and associated information) to augment the efficient development, deployment, and establishment of communication networks for joint warfighting.

System interoperability is critical to effective joint warfighting operations. Therefore, communications system developers, planners, and operators are encouraged to leverage the information contained within this document to the fullest extent possible. A unified joint effort to use this information will contribute to greater network situational awareness and fewer configuration management challenges.

A.1 SCOPE

This document and the identified communications system operating standards are based on the OAN. This document encompasses aspects of tactical networked communications including multimedia networking, routing, switching, trunking, transmission, security, and interoperability of respective systems.

A.2 DEFINITIONS

Appendix C, Definitions, Abbreviations and Acronyms, and References, contains the definitions.

A.3 BACKGROUND

This section is the result of continued telecommunications interoperability challenges in the tactical warfighting environment. Lessons learned from past and current conflicts have demonstrated the need for a common approach to establishing and maintaining communication networks in the joint operational arena. Additionally, this section provides a framework to assist in identifying common communications system operating standards for establishing and employing joint tactical networks within a geographic identified theater and the GIG.

A.4 UNIFIED CAPABILITIES REFERENCE ARCHITECTURE

A.4.1 The UC Operational Framework

The UC Operational Framework is described in the UC Master Plan.

A.4.1.1 Tactical Edge Network

Tactical Operations Centers (TOCs) and other deployed enclaves operate under austere conditions; rely on a Deployed power supply or grid; and are restrictive in their size, weight, and packing allocations. The Deployed LAN and the backbone and transmission components operate from the same Deployed power source. It is extremely difficult to approach the availability and power backup requirements mandated on the fixed infrastructure with its commercial-grade power supply and fixed operating environment.

The Assured Services LAN (ASLAN) requirements defined in UCR Section 7, Network Edge Infrastructure, represent the optimal LAN design. Deployed users are encouraged to implement these requirements whenever possible. However, operational realities often preclude the deployment of highly redundant components and multiple backup power sources.

A.4.2 Operational Area Network (OAN)

The OAN is a template JTF network architecture that serves as a reference model for forces when deploying joint tactical networks. The OAN serves as a baseline for identifying the common communications system operating standards necessary for facilitating system interoperability and configuration management in the joint operating environment. The OAN is composed of tiers zero (0) through eight (8). Figure A.4-3, OAN Tier Structure, illustrates the OAN, and the tiers are described in the following text:

- Tier 0: includes DISN Video Services (DVS), Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Non-Classified Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), Defense Messaging, and DISN Transport*.
- Tier 1: includes the DISN Long-Haul systems*.
- Tier 2: includes DoD Gateways*.
- Tier 3: includes theater resources of the geographic combatant commands such as the theater headquarters and the Theater NetOps Control Center (TNCC).
- Tier 4: includes the force-level elements such JTFs, Joint Special Operation Task Forces (JSOTFs), and service component headquarters.
- Tier 5: includes unit levels such as Army Corps, Marine Expeditionary Forces (MEFs), numbered Air Forces, and Navy Carrier Battle Groups (CVBGs).
- Tier 6: includes unit levels such as divisions, wings, and task forces.
- Tier 7: includes unit levels such as brigades, regiments, groups, and task units.
- Tier 8: includes unit levels such as battalions, squadrons, and ships.

*Tiers 0–2 constitute the DISN core.

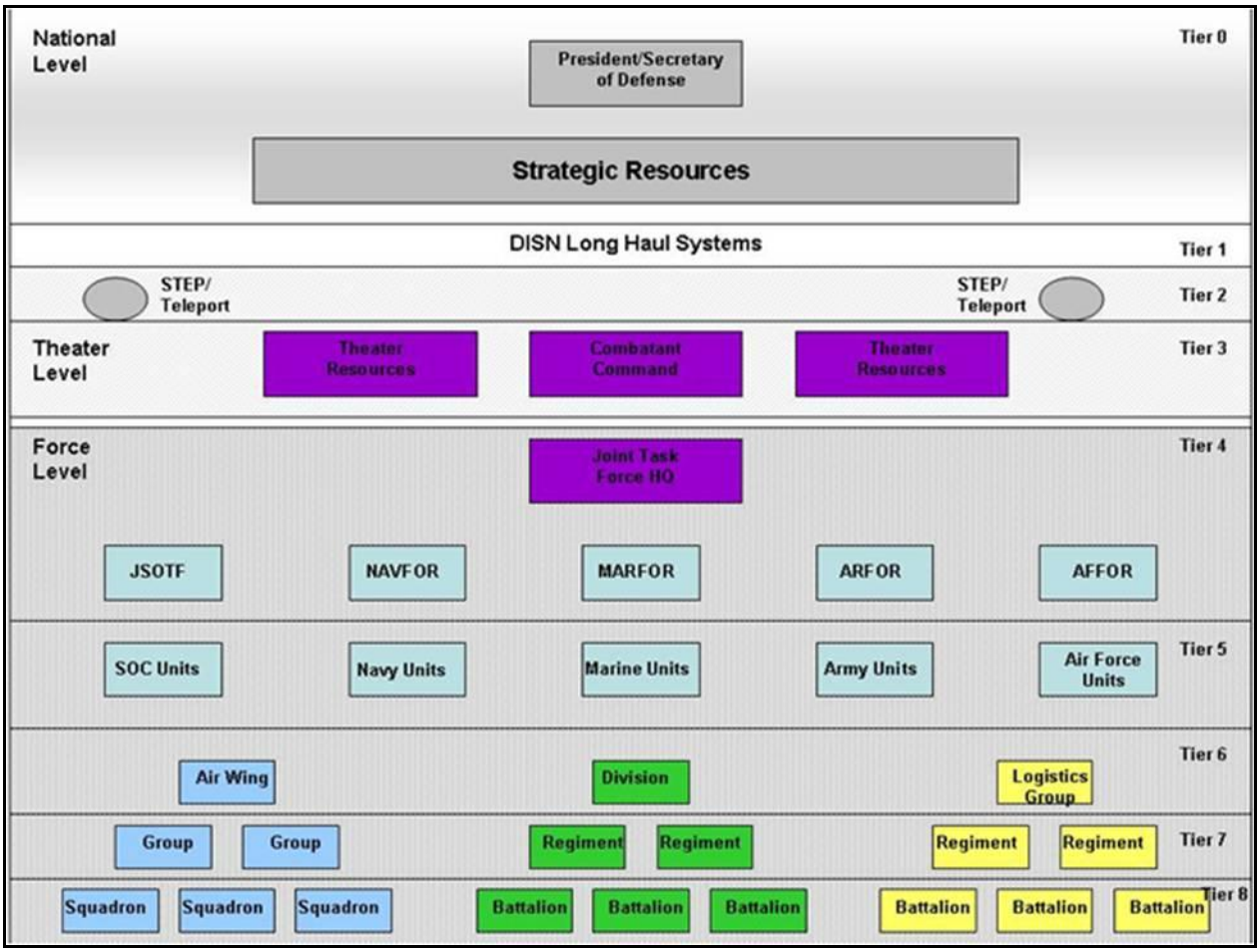

Figure A.4-3. OAN Tier Structure

A.5 ARMY COMMON OPERATING ENVIRONMENT (COE)

A.5.1 COE Overview

The Common Operating Environment is founded on these basic constructs:

1. Common Operating Environment (COE)– A Collection of six (6) Computing Environments
   I. Enterprise Server
   II. Tactical Server
   III. Mobile
   IV. Client
   V. Platform
   VI. Sensor

2. Computing Environment (CE) – A collection of Operating Environments, Computing Hardware / Infrastructure and User Specific Applications.
3. Operating Environment (OE) - Specifications of common configurations of Operating Systems, Security, Developer Kits and Standard Applications for systems utilized with a CE
4. Computing Environment Profile(CEC) – Pairing of a specific Operating Environment (OE) with specific Computing Hardware / Infrastructure to support a set of Standard Applications and User Specific Applications
5. Computing Hardware / Infrastructure – These are both computing and communications transport hardware configurations/devices that can be supported by one or more OEs
6. User Specific Applications - A set of approved specialized applications, providing unique operational functions, for use in CECs; one or more of which may be applied to any hardware configuration/device

A.5.2 COE Computing Environments

The following definitions are provided to establish the purpose, scope, and primary usage of the six (6) Computing Environments within the COE:

Enterprise Server - The Enterprise Server CE is a high-end computing environment capable of supporting enterprise scale applications and data processing. It can support both tactical and non-tactical operations, but it does not support the same applications as are in the Tactical Server CE.

Tactical Server -The Tactical Server CE provides specialized information services to users in the tactical community. Characterized by environmentally hardened server-class hardware, it resides in tactical tent or improved building environment. This allows command post mission environment users and systems to leverage the capabilities offered by both the tactical and enterprise environments.

Client - The Client CE provides information resource(s) access to users that can reside within the Public network, the DoD – NIPRNET, or a Classified network or enclave. It is comprised of end-user devices, typically running on a desktop, laptop or notebook computer connected at a non-DoD facility directly to the Public Internet, on a sustaining base (CONUS Army facility), or in a tactical environment (Post/Cam/Station/Forward Area) as a Battle Command Workstation on a Classified network.

Mobile - The Mobile CE provides information resource(s) access to users that require a standalone portable end-user computing and communications device. The technologies for this environment are based on lightweight handheld devices capable of supporting missions. These capabilities include digital signatures and encrypted e-mail, as well as being CAC-enabled for use on the public voice network or the Internet, or the DoD-NIPRNET. Tactical mobile devices such as handheld or “back pack” end-user devices (e.g., SINCGARS) (e.g., Portable Battle Command – Personal Digital Assistant (PDA)) is also within the Mobile CE.

Platform - The Platform CE is characterized by an air, sea or land-mounted device or vehicle that collects processes and disseminates data.

Sensor - The Sensor CE provides information services to systems that reside within a network or enclave, function as a standalone information "Data Collector". It is highly specialized and can be either a human-controlled or unattended computing environment. Sensors detect and report on conditions such as Biological/chemical threats, combatant movements, temperature and weather conditions, Radio Frequency RF) emissions, radioactivity levels, and munitions explosions/impact positions/strength). Sensors can also collect video, audio, topographical or terrain data, as well as detect multi spectrum light (infrared) instances.

A.5.3 COE Architecture

On 28 December 2009, the Vice Chief of Staff of the Army (VCSA) directed CIO/G-6 to develop _as is' and _end state' network architectures to guide network development, procurement and enhancement. The Army Network Architecture Strategy – Tactical version 1.1, dated 6 April 2010, was crafted in response to the VCSA's memorandum. Since then, CIO/G-6 has written the Guidance for 'End State' Army Enterprise Network Architecture version 2.0 to provide direction for the entire Army Enterprise Network. The Common Operating Environment (COE) Architecture is a key component of that guidance. The COE will be validated and republished twice each year at a minimum.

A.5.3.1 Background

The current Army approach to information technology implementation and management is cumbersome and inadequate to keep up with the pace of change. The acquisition process focuses on the development and fielding of systems by programs that were established to deliver capability for a specific combat or business function. Based on functional proponent requirements, program managers individually choose and field hardware platforms and software infrastructures. Meanwhile, to support ongoing conflicts, Army and combatant commanders independently procure commercially available solutions, often installing and customizing them in theater. As a result, deploying and deployed units frequently must plan and execute operations using multiple computer systems with different hardware, operating systems, databases, security configurations and end-user devices. The extraordinary scale and scope of this complex integration raise cost, decrease interoperability, increase network security risk, expand the deployment footprint and add a tremendous burden to managing configurations. Most importantly, the process carries significant operational impacts. The intent of the COE architecture is to normalize the computing environment and achieve a balance between unconstrained innovation and standardization. In the commercial sector, computing environments have become commodities and applications are developed and delivered on commoditized and inexpensive systems (for example, the Apple iPhone and Google Android mobile devices). With a COE, the Army can establish a framework similar to industry best practices. Communities of interest will be able to: produce high-quality applications quickly and

cheaply; improve security and the defense posture; reduce the complexities of configuration and support; and streamline and facilitate training. This is a wholesale shift from the Army's traditional procurement of systems with dedicated software and hardware. Instead, applications will be designed, developed and deployed on a common computing environment, allowing the end user to download what he needs when he needs it.

A.5.3.2 Approach

The Army Enterprise Network, illustrated in Figure A.5-1, is comprised of four networks: the Global Defense Network, the At Home/TDY Network, the At Post/Camp/Station Network and the Deployed Tactical Network. The Army Enterprise Network enables full-spectrum operations through all phases of deployment. The COE enables secure, uniform and interoperable access to warfighter capabilities across the Army enterprise.

Experience shows that conformance to standards leads to optimization. This document targets the FY13-17 Program Objective Memorandum period, providing standards for computing environments that execute within the Common Operating Environment framework. It applies to all organizations and agencies of the Army, U.S. Army Reserve and Army National Guard (to include standalone Reserve Centers located in the continental United States and U.S. territories and possessions).

The scope of the COE architecture is limited to programs that support the operating force across full-spectrum operations and through all phases of training and deployment. The COE architecture does not contain a comprehensive, rigid set of instructions for developing applications or systems. It also does not currently apply to embedded, real-time or safety-critical vetronics and avionics systems. Guidance for these systems will be provided in the next update of the COE Architecture.

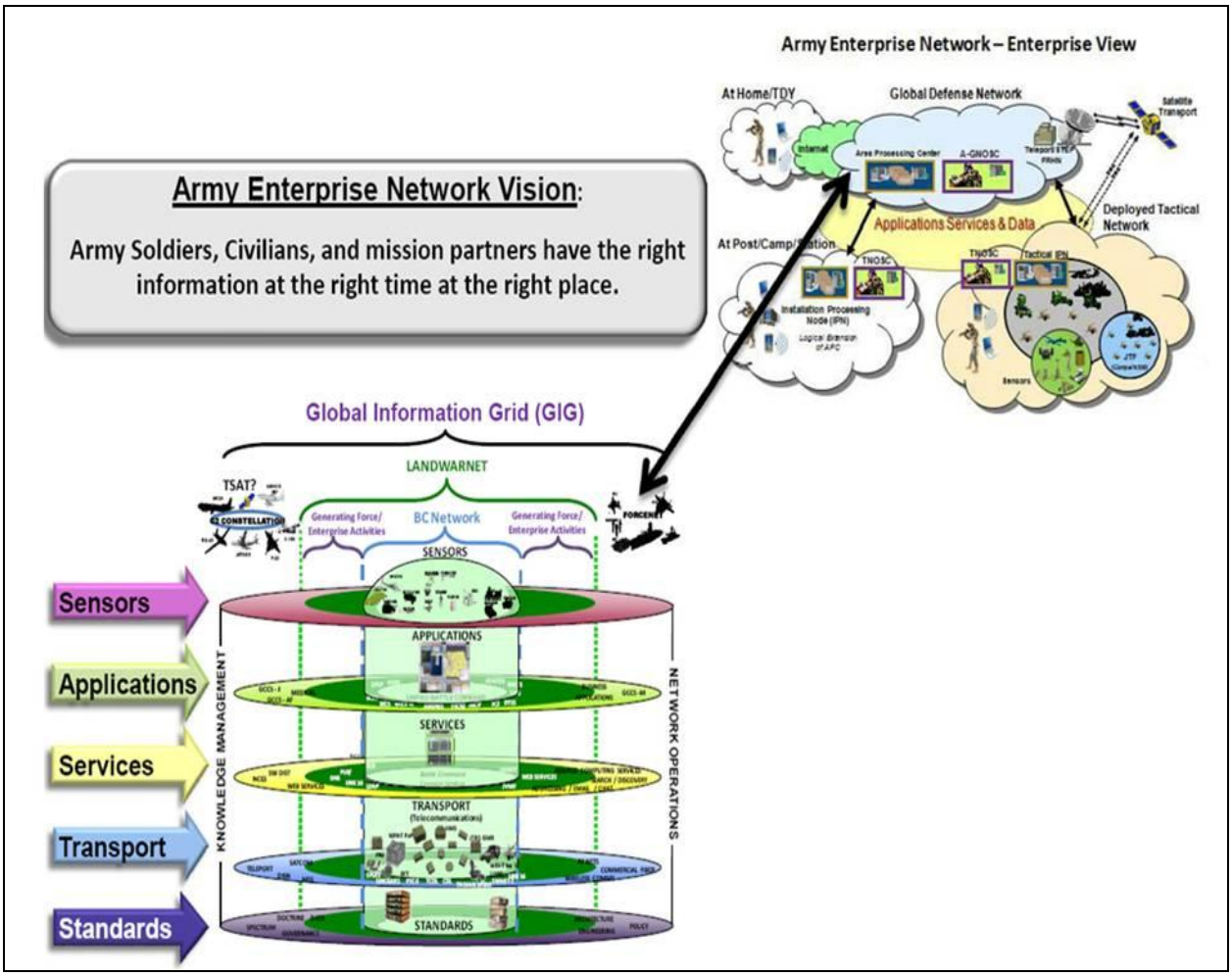

Figure A.5-1. Army Enterprise Network

A.6 DEPLOYED UNIFIED CAPABILITIES STANDARDS REFERENCES

The following section refers to common functional areas required for effective implementation of joint tactical networks. Each of the following topics highlights technical Tactical UC areas. Each topic is generally defined, along with amplifying or supporting information. When required, information is elaborated to ensure that all organizations referencing the UC Framework understand the information being presented.

A.6.1 Network Operations

Network Operations (NetOps) is the DoD-wide construct used to operate and defend the GIG. NetOps consists of three essential tasks—Enterprise Management, Network Defense, and Content Management; situational awareness; and command and control (C2)—and provides for integrated network visibility and end-to-end management of networks, global applications, and services across the GIG.

A.6.2 Information Assurance

Information Assurance refers to measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. For more information on Information Assurance (IA) requirements for Unified Capabilities (UC) products see UCR 2013, Section 4, Information Assurance.

A.6.3 Communications Security

Communications Security (COMSEC) is defined as measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto-security, transmission security, emission security, traffic-flow, and physical security of COMSEC material.

A.6.4 Quality of Service

This framework addresses Quality of Service (QoS) requirements for UC tactical networks. These requirements are distributed throughout the UCR, and generally fall into one of two categories:

1. Performance metrics, such as acceptable packet delay, jitter and loss, MOS scores, blocking probability.
2. Use of standardized mechanisms and best practices to ensure that performance requirements are supported for UC voice and video calls. If there is insufficient capacity to meet the performance requirements, a new call will be blocked unless there is a lower precedence call that can be pre-empted to provide that capacity.

Achievable performance metrics will differ significantly between tactical networks and strategic networks. Tactical networks tend to be connected to each other and the strategic backbone by satellite links, which have constrained and possibly variable capacity, are more prone to bit errors, and have longer propagation delays than links within and between strategic networks. This leads to higher delays, jitter and packet loss in tactical networks compared to strategic networks.

UC QoS is provided by the following mechanisms and best practices:

1. Use of DiffServ in routers, switches, IP modems to provide a method to mark and process packets as they move across a network so that the packets can get the packet delay, jitter and loss metrics required to meet end to end performance goals. DiffServ is applied to voice, video and data applications. The UCR incorporates the DoD standard for marking packets with DiffServ Code Points (DSCP) – see Reference (GTP-009)

2. Use of admission control to ensure that voice and video traffic sessions will not be initiated unless there is sufficient capacity along the path taken by the bearer traffic to provide the required performance. Admission control is administered by UC Session Controllers (SC). The SCs control access to constrained links along the path of a call. Any link not controlled by SCs must be provisioned so that no possible combinations of calls can create congestion along the link.
3. Application of a routing approach which ensures voice and video bearer traffic will follow the path that is admission controlled.
4. Use of traffic engineering and planning to ensure that the networks have sufficient capacity to provide the required performance for voice and video calls, and future data applications that will be provided with assured performance.

Not all tactical networks meet requirements 2 and 3. Some tactical networks sites are connected in a meshed fashion. Each site might have several satellite or RF links to other sites in the network. In such case, it might not possible to ensure that calls will follow a path where all constrained links are admission controlled. This creates a situation where UC gateways must be used at the edge sites that connect with other UC networks. The gateways will be used to connect UC compatible calls with non-UC calls in the network. It will be the MILDEP's responsibility to determine how to prevent congestion in that part of the tactical network that does not conform to the current UC admission control model.

A.6.4.1 Background

DoD has adapted Differentiated Services (DiffServ) as a major element to support QoS across multiple, heterogeneous IP networks. Unified Capabilities has incorporated the DiffServ concept described in Reference 1. The UCR provides requirements for assured service delivery of voice and video traffic and will be upgraded to include selected data traffic such as chat.

DiffServ provides the basis for establishing performance goals for aggregated IP packet flows across networks. DiffServ provides a standardized approach for establishing and coordinating router treatment of IP packet. With DiffServ, applications are associated with Service Classes. DiffServ-enabled routers and devices provide each Service Class with a guaranteed amount of outbound link capacity. In this way the capacity of the link is shared between the Service Classes. If the aggregate traffic rate in a Service Class remains within specified limits, packet performance will stay within specified packet loss, jitter and delay metrics, as described in Reference 1 and IETF RFCs (Reference 3). DiffServ does not guaranty performance for individual traffic flows within the Service Classes.

Voice and video services can be given QoS guarantees for each flow, provided that an admission control mechanism limits the total number of flows to ensure that sufficient network capacity is available for each call. The UCR defines a standard signaling approach for voice and video sessions called UC-SIP (Unified Capabilities-Session Initiation Protocol). UC-SIP supports a call counting approach for the admission control of ASLANs with constrained links. A "constrained

link" is one where the demand at times can exceed the capacity of the link. This is in distinction to an "overprovisioned link" where the expected demand never exceeds the capacity of the link.

The responsibility for admission control is vested in Session Controllers (SC) and Soft Switches (SS). The SCs and SSs have call budgets associated with all constrained links under their control. SCs will admit a call if the budget is not depleted. If the budget is depleted, the SC will determine if there is a lower precedence call that can be pre-empted. If so, the new call will be admitted and the other call pre-empted. If there is no lower precedence call, the new call will be blocked.

Assured services admission control (ASAC) is based on a fixed number of calls per constrained link. Each voice call is assumed to require 110 Kbps, whether it actually uses that much capacity or not. Video calls are set at multiples of 500 Kbps. These lead to conservative call admission policy where calls might be blocked even if there is capacity to support the call. This is satisfactory in strategic networks with well provisioned links, but could reduce the number of calls accepted in a tactical network below that which could be supported if a more finely tuned admission control method were used. Dynamic ASAC (DASAC) capability was added to the UCR to provide admission control based on the actual capacity required per call, compared to the available capacity on the constrained link. The SC determines if there is sufficient capacity in on each link in the path to support the new call. If so, the call is admitted. If not the call is either blocked or another lower precedence call is pre-empted.

Traffic engineering is a planning process that estimates the traffic demand in each UC Service Class and provisions the appropriate amount of link capacity to support the performance requirement for the Service Classes. Traffic engineering uses DiffServ to allocate a guaranteed minimum capacity for all Service Classes that share the same communication links. SCs support admission control which provides assured performance for individual UC voice and video streams. Traffic engineering for voice, video and data involves applies to all routers and IP modems in the networks carrying UC traffic.

"IP modems" are satellite modems that process IP packets and drive constrained RF links. In many cases these modems contain buffers and queues that provide a type of differentiated service similar to that provided by routers. However, there are some significant differences which will be addressed in this document.

In addition to traffic engineering and QoS mechanisms, QoS should be backed up by agreements between tactical network users and network providers such as DISA and the Teleport Program Office (TPO). These agreements are commonly called "Service Level Agreements" (SLA). These agreements define user and service provider obligations, performance guarantees, reporting requirements and measurement tools that will be used to determine performance levels (Reference on SLAs).

In summary end to end QoS depends on DiffServ, admission control, traffic engineering, and SLAs.

A.7 HIGH-LEVEL TACTICAL UC ARCHITECTURE

This section describes the architecture used to support UC assured services in the tactical world. The architecture is described at two levels. The network level architecture describes data flow between the ASLANs that comprise a tactical network. The LAN architecture describes functions and data flow at UC ASLANs.

Two network level architectures are discussed: the hierarchical architecture which can support UC services at each ASLAN; the meshed architecture used in some tactical networks, and which might not conform to the conditions necessary to support UC-based admission control.

A.7.1 Hierarchical Network Architecture

Figure A.7-1, Hierarchical Connectivity in UC, shows the connectivity model supported by the current UCR. The model, which was developed for the strategic world, has been modified to show a notional tactical environment. This model in Figure A.7-1 works because all calls move from one ASLAN to another over a single constrained link. There is no routing uncertainty. Each constrained link is under the control of a Session Controller (SC) so that with proper traffic engineering and configuration, no voice or video call will encounter congestion.

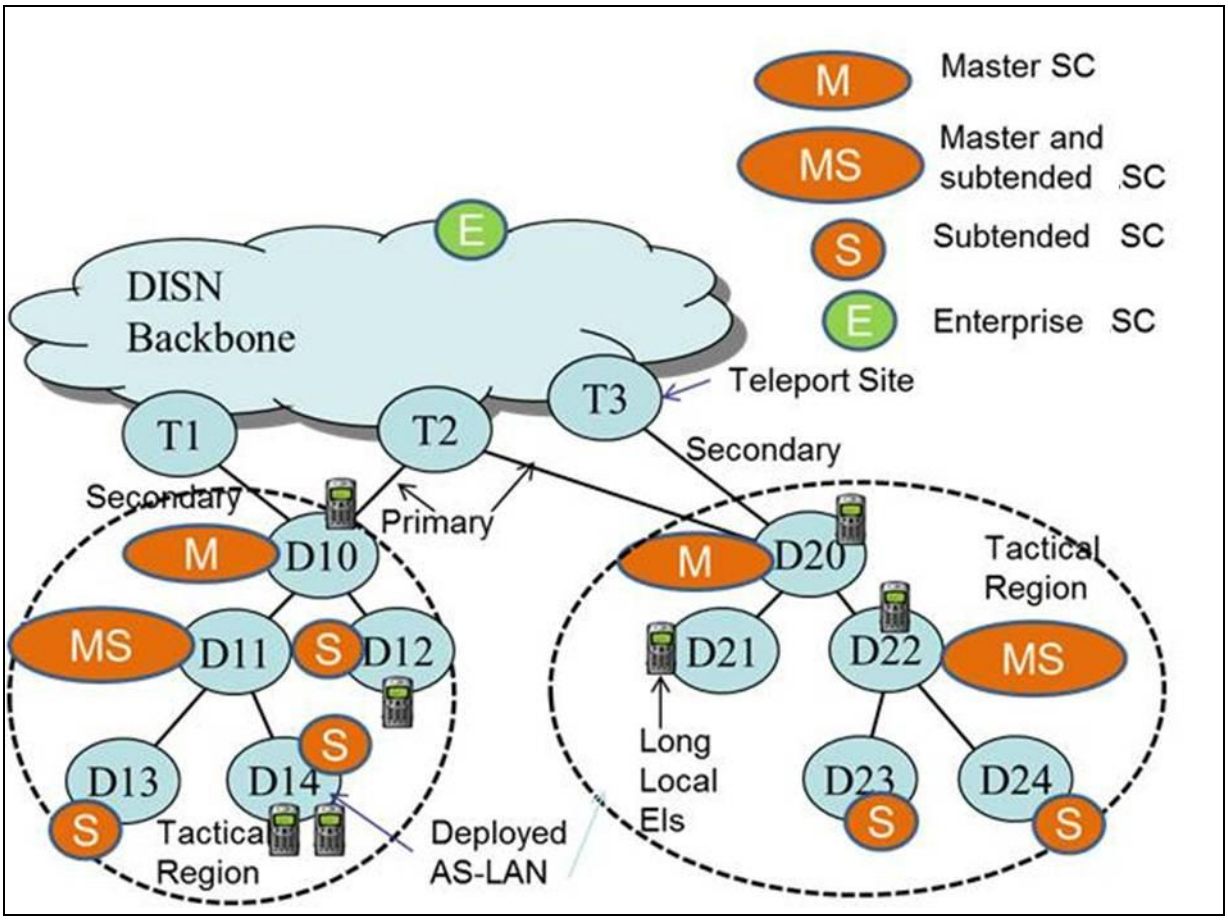

Figure A.7-1. Hierarchical Connectivity in UC

Figure A.7-1 depicts a strictly hierarchical flow of traffic between UC end instruments (EI) located at dispersed ASLANs. The ASLAN locations, represented by D1 etc., are overprovisioned and supported by a SC and possibly a Session Border Controller (SBC). The SC and SBCs are not shown in the Figure. UC voice and video traffic can flow only along links that are either overprovisioned or are strictly admission controlled by SCs. The locations marked as T1 etc. are DoD Teleports which provide a gateway between Tactical Regions and the DISN backbone.

There are a variety of SC types. Master SCs (marked as M in Figure 1) support and control Subtended SCs (marked as S). Some SCs are both Masters and Subtended and are marked as MS in Figure A.8-1. Enterprise SCs (marked as E) are located at sites that are well connected to the DISN backbone.

The ASLANs are connected by constrained links. Assured service is established because each call can transverse only one link between the ASLANs and that link is admission controlled by SCs at each end of the link. SCs employ UC-SIP signaling to coordinate the admission of a call. Each constrained connecting link is driven by a Customer Edge Router (CE-R) and possibly an IP Modem. These devices are provisioned to ensure that there is adequate capacity to support the maximum number of assured voice/video calls that will be admitted by the controlling SCs. There may be routers along the way that are not CE-Rs with links that are not under the purview of SCs, but in such case the links must be overprovisioned. This is typical of the routers in the DISN backbone.

The Backbone contains Softswitches (SS) and Enterprise Servers (ES). The SS supports AS-SIP signaling and discovery of End Instruments. The Enterprise servers can be used by the tactical community to support UC supplied enterprise services such as chat.

A.8 MESHED NETWORK ARCHITECTURE

Figure A.8-1 is a notional picture of the meshed connectivity that exists in many Tactical Regions. Some ASLANs are connected to multiple Teleports and to other ASLANs. There are lateral links within a Tactical Region and between Tactical Regions. The links could be satellite links, terrestrial wireless links, or cables. In some cases the link capacity could vary based on weather, jamming or movement of the receiving terminal.

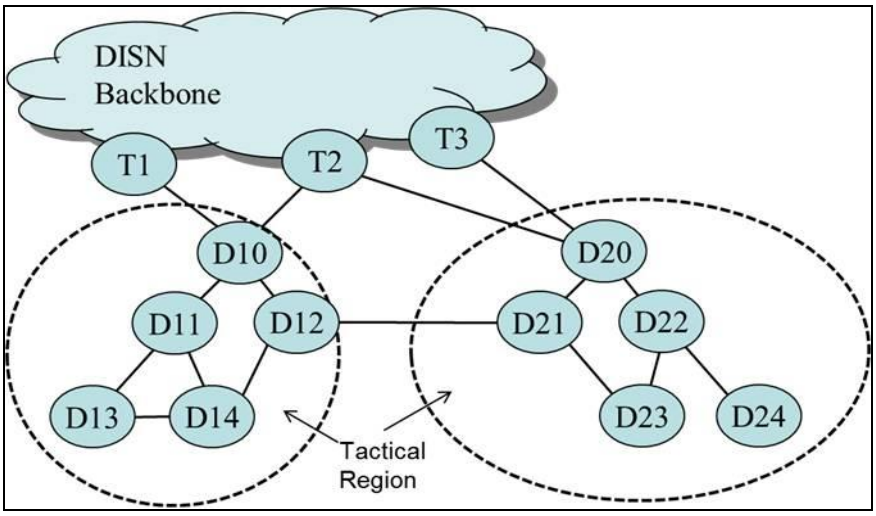

Figure A.8-1. Notional View of Tactical Region Mesh Connectivity

The connectivity in Figure A.8-1 creates a routing issue which negates the hierarchical assumption upon which UC assured service is currently based. For example, a bearer packet generated at D11 and destined for D23 could take one of 2 least-hop paths: D11/D10/D12/D21/D23; D11/D14/D12/D21/D23. Each path involves 4 hops, some of which could be over satellite. The SCs do not know which path the packets will take and therefore must manage their call budgets based on the following:

1. Uncertainty [1].
2. Not allowing any more calls than can be supported by the least capable link.
3. A policy whereby all voice traffic is sent out on one designated link, with the proviso that another link can be used in case of failure of the designated link.
4. Use of probes to determine if there is sufficient capacity on the path the routing protocols select for the call in question. This is sometimes called "measurements-based admission control" (MBAC).
5. Use of a local approach for admission control at all but the edge locations. Place SCs at the edge locations so that region to region calls can be admission controlled. Place voice and video over IP gateways at the edge locations so that calls from the proprietary portion of the network.

The first strategy could lead to congestion which would impair voice and video quality. The second and third strategy would be over-restrictive and not take advantage of all the capacity available on the connecting links. The MBAC approach would eliminate congestion, but would

[1] This uncertainty can be minimized if the outflow of traffic is, on average, heavily weighted towards data. In such case, voice and video traffic can be given priority treatment. If there are surges, the voice and video will be given priority over data for the period of the surges. This method becomes less viable if the expected voice and video traffic is greater than the expected data traffic. In such case it might possible to protect the voice traffic if it is less than the video traffic, but video QoS could suffer.

not enable the use of alternative paths, if the primary path is congested. MBAC could also introduce short periods of congestion, with resultant degradation of voice and video quality. The local approach will limit the deployment of UC congestion control methods to that portion of the tactical network which conforms to the hierarchical model.

The ultimate solution would be to create a standardized multipath call management (MPCM) mechanism that could both determine the optimum path over which to send a call and could guarantee that bearer traffic for the call would be routed over the optimum path. This is a subject for further discussion and beyond the scope of this framework document.

A.9 ASLAN ARCHITECTURE

Figure A.9-1 shows the basic traffic outbound flow for voice traffic in an ASLAN and across the access links from that LAN. This case illustrates voice flow, but is also representative of UC video traffic flow. It is a UC requirement that all bearer traffic traverse the Session Border Controller (SBC) prior to egress from the LAN. The SBC will send the traffic to Customer Edge Router (CER). The CER will queue the traffic for transmission to the IP Modem. In this case the IP Modem is a TDMA modem such as JIPM and provides TDMA/DAMA access to a satellite link. The IP Modem queues the traffic for transmission to another site, in this example a hub located at a DoD Teleport. Typically both the CER and the IP Modem have a high priority queue reserved for voice traffic. In DiffServ these are referred to as Expedited Forwarding (EF) queues. EF queues must be provisioned to handle the worst case traffic rates for traffic that enters the queue.

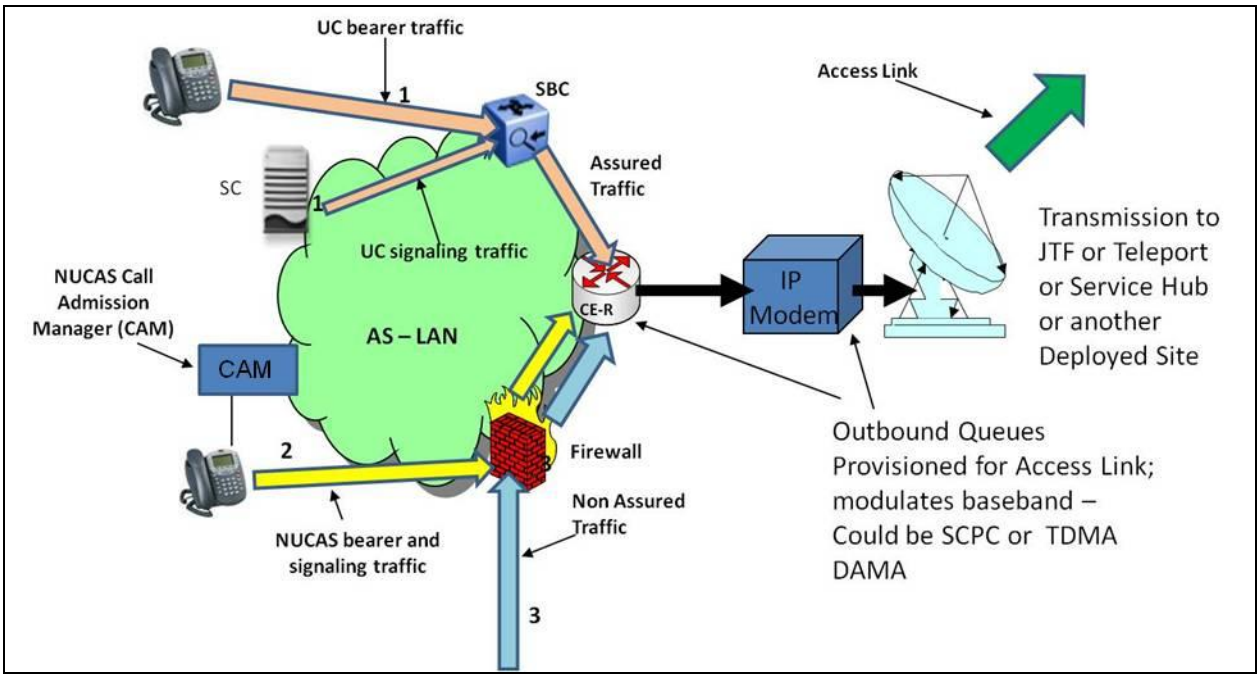

Figure A.9-1. Outbound Traffic Flow in Tactical ASLAN

From a traffic engineering point of view, it is relatively easy to calculate the number of calls that enter the queue based on the admission control parameter used by the UC Session Controller (SC) that provides admission control. For example if we wish to allow 10 simultaneous voice calls and each call takes 50 Kbps, the voice queue must be provisioned to support at least 500 Kbps. However, there are cases where non UC voice end instruments could generates traffic that must be supported in a voice queue. This traffic, known as "non UC assured services" (NUCAS) is admission controlled by a NUCAS admission Call Manager (CAM). There could be one or more such devices. Traffic from the EIs associated with the CAMs does not flow through the SBC but does egress via the CE-R. Proper traffic engineering for the CE-R requires that this flow must be added to the UC flows to determine the provisioning for the EF queue.

There are several types of IP modems. If the IP modem supports FDM or TDM traffic the link will be continuously available. In such case there is no queuing or need for QoS in the IP Modem. If however, the IP Modem supports a TDMA/DAMA link the capacity will only be available in bursts, with time gaps between the bursts. In such case the traffic sent from the CER must be queued in the IP Modem. Some IP modems have provision to transmit packets based on priority. Others will transmit in the order in which they were generated in the CE-R.

Figure A.9-1, Outbound Traffic Flow in Tactical ASLAN, shows the continuation of the traffic over the satellite link to a Teleport and from there to the DISN Backbone.

A.9.1 Precedence and Preemption

Precedence and preemption can only be implemented in a DoD network. This service has two parts: precedence and preemption. Precedence involves assigning a priority level to a call (wireless or wired). Preemption involves the seizing of a communications channel that is in use by a lower precedence level caller, in the absence of an idle channel. In the DCVX, the Precedence and Preemption capability is Conditional. Precedence and preemption may be provided by enacting enhanced multilevel precedence and preemption (eMLPP) or a vendor proprietary version that performs precedence and preemption in the DCVX between the terminal device and the cellular switch. The eMLPP is a cellular version of MLPP and Assured Service in TDM and IP networks respectively. In either version, precedence will be invoked by keying defined digits before dialing the destination number on cellular instruments that have been classmarked for this service. Precedence will function jointly in combination with WPS and will perform E2E as an adjunct to regular MLPP service on the wired DSN and Assured Service on the UC Network. However, in either of the provided versions, if available in the DCVX, eMLPP or vendor proprietary, the connection to the DSN will be MLPP PRI (T1.619a) or use the AS-SIP protocol for the UC Network.

Mobile systems, as currently designed, provide a maximum of seven priority levels. The two highest levels (A and B) are reserved for network internal use (e.g., for emergency calls or the network-related service configurations for specific voice broadcast or voice group call services). The second highest level (B) can be used for network internal use or optionally, depending on regional requirements, for subscription. These two levels (A and B) can only be used locally, that

is, in the domain of one DCVX. The other five priority levels are offered for subscription and can be applied globally if supported by all related switch elements, and for interworking with ISDN networks providing the MLPP service or Assured Service on UC Network. The seven eMLPP priority levels and their respective mapping to MLPP are defined as follows:

A	Highest, for network internal use	
B	For network internal use or, optionally, for subscription	
0	For subscription:	FLASH-OVERRIDE
1	For subscription:	FLASH
2	For subscription:	IMMEDIATE
3	For subscription:	PRIORITY
4	Lowes, for subscription:	ROUTINE

Levels A and B shall be mapped to level "0" for priority treatment outside of the DCVX area in which they are applied. The vendor-proprietary version will support the five precedence levels as specified for DSN MLPP or UC Assured Service.

A.9.2 Global Block Numbering Plan

The GBNP instituted by Joint Staff (JS) under the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5122.01C. The GBNP was developed for the purpose of supporting the Warfighter during "Real world missions", training exercises, and testing of TDM, IP and UCSIP voice telecommunication systems. The GBNP numbering system is a subset of the DISA strategic numbering system and is in compliance with the E.164 ITU numbering system supporting a worldwide numbering format. Its versatility allows for cross domain voice communication to and from the tactical, commercial and strategic communities of interest.

The GBNP is based on four pillars or categories that work in cohesion to effectively support the Warfighter, these categories are as follows:

1. Tutorial.

   This portion of the GBNP provides a "step by step" instruction to the Warfighter on the "how to" and helps to increase the users understanding of the GBNP and its deployment operational functions.

2. Assignment.

The portion of the GBNP, that captures the Routing, Numbering/IP addressing and CCAID information for all Combantant Commands, Services, and Agencies.

3. Database Management.

   The GBNP database defines all of the C/S/A CCAID assignments and requirements to support all Combantant Commands, Services, and Agencies.

4. Vetting Process (Dissemination and Feedback loop).

   This pillar is the methodology used to acquire, distribute, modify and upgrade or change portions of the GBNP that directly affect the Warfighter, these actions are usually conducted at Quarterly Working Group or electronically for critical issues.

A.9.3 Dynamic Unified Capabilities Admission Control (DASAC)

Dynamic ASAC (DASAC) enables an SC to admit, block, or preempt new voice and video sessions based on the bandwidth (bits/sec) required for the session and the link capacity available to support the session. Dynamic ASAC will augment the ASAC approach described earlier in UCR Section 2.5, ASAC, in which SCs admit sessions based on a fixed session budget, either 110 Kbps for voice, or a multiple of 500 Kbps for video. The DASAC will be applied independently to voice and video sessions.

The method for ASAC described earlier could unnecessarily limit the number of sessions on capacity-constrained communications links, such as are common in Deployable (Tactical) networks and in some Fixed (Strategic) networks. For example, the current approach provisions 110 Kbps for each voice session, but some Deployable (Tactical) sessions only need 30 Kbps for good quality. The 110 Kbps number is based on the assumption that a voice session will use a G.711 codec and will be encapsulated in an IP packet in an Ethernet frame. These are reasonable conservative assumptions in a Fixed (Strategic) environment, but are not appropriate for a Deployable (Tactical) environment or a constrained Strategic environment, where lower bit rate codecs are used and link capacity is limited.

Dynamic ASAC will provide a more realistic estimate of capacity needed for a voice or video session and admit, block, or preempt sessions based on this estimate. However, parameter determination for DASAC can be quite complex. Some session packets might be tunneled over a communications link, others might not be; others might have header compression and some packets might be aggregated in a voice multiplexer also called a ―voice mux.‖ Engineering analysis and traffic analysis are required to determine the overheads on the SC Path (the path between cooperating SCs and SSs).

The SC and SS analyze each session initiation and session modification request to determine which overheads are appropriate, and the codec rate and packets per second (PPS) negotiated between the EIs involved in the session. This rate could change during a session; an example being a mid-session codec change; a factor that must be monitored by these devices if the change information is conveyed in AS-SIP messages. This may not be the case for all types of sessions;

in some sessions the change information is conveyed in the bearer traffic. A bearer-based example would be a mid-session codec renegotiation via a modem protocol. In such cases, precautions during DASAC processing must be taken to ensure that there is sufficient capacity to accommodate the highest possible codec rate that could be renegotiated via the bearer mid-session. This could include using static, table driven parameters for session capacity, where these parameters represent the highest bits per second session capacity supported by the EI. Ideally, in lieu of the static table driven parameters, DASAC would process any bearer-based mid-session re-negotiation but such complexity is not currently required in the UCR.

For further information on DASAC see UCR Section 2.24, Dynamic ASAC.

A.9.4 Deployed Cellular Network Systems

Data Communications Network (DCN) systems provide wireless mobile communication services with military-unique features (MUFs) and draw their Strategic services by approved DoD authorized gateway switching systems only. DCN systems can be connected to a Deployed Voice Exchange – Commercial (DVX-C), connected directly to the DSN, and/or to the UC Services Network utilizing AS-Session Initiation Protocol (SIP) (AS-SIP) for Time Division Multiplexing (TDM) and IP switching systems, respectively. The DCN system also may be interconnected with other cellular telephone systems, excluding commercial systems, unless the commercial system is procured or leased for DoD usage and is operating in an isolated mode from other commercial provider cellular systems.

When placed in a Deployed environment, the DCN will have the capability to connect to DSN/UC Services and between other Deployed Cellular Voice Exchanges (DCVXs) and DVX-Cs using UCR-defined protocols such as Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI), Multilevel Precedence and Preemption (MLPP) PRI (T1.619a), and/or AS-SIP. A DCVX system may also be configured to interconnect at the network transmission level with other DCN systems to provide roaming capability outside the local home base cellular network for supported terminal devices. In support of this roaming capability, the DCN systems may interconnect based on the interconnection protocol requirements of the appropriate 2G, 3G, and/or 4G standards.

The DCN terminal devices often referred to as mobile subscriber cellular handsets, Personal Digital Assistants (PDAs), Smartphones, BlackBerrys®, and any other end user cellular devices, commercial or Government developed, may connect to commercial cellular systems when operating outside the transmission range of the DCN. Additionally, the cellular terminal devices may have the capability to interface with other wireless networks (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11 and IEEE 802.16). Actual employment of this additional cellular terminal device capability will be by command approval only in the Tactical OAN.

DCNs are composed of the following three major functional areas: Terminal devices(s), Access Network, and Core Network. Terminal devices can be mobile subscribers' cellular handsets, PDAs, Smartphones, BlackBerry, or any other end user cellular devices, commercial- or

Government-developed. With the evolution of cellular technology from 2G to 4G, the primary functional components that compose the DCN Access and Core Networks are evolving as well. For comparison of the primary functional Access and Core Network components that compose an operational DCVX across the evolutionary changes,

Figures A.9-2 through A.9-4, provide the primary cellular Access and Core Network components for 2G, 3G, and 4G systems, respectively.

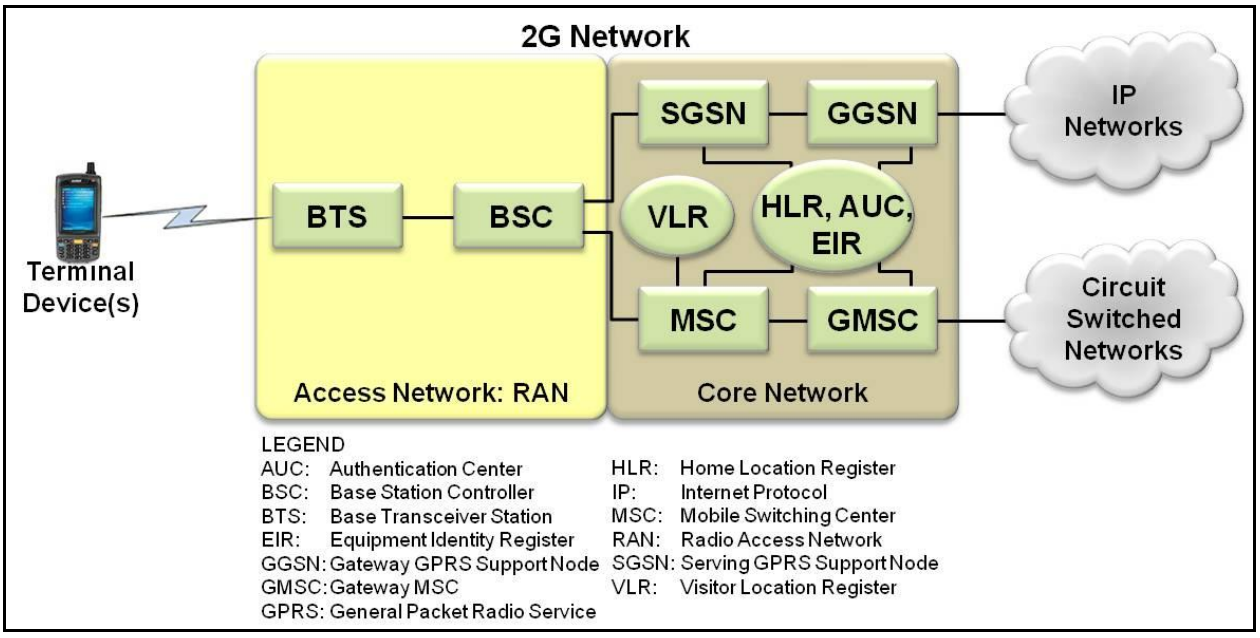

Figure A.9-2. 2G Cellular Primary Components

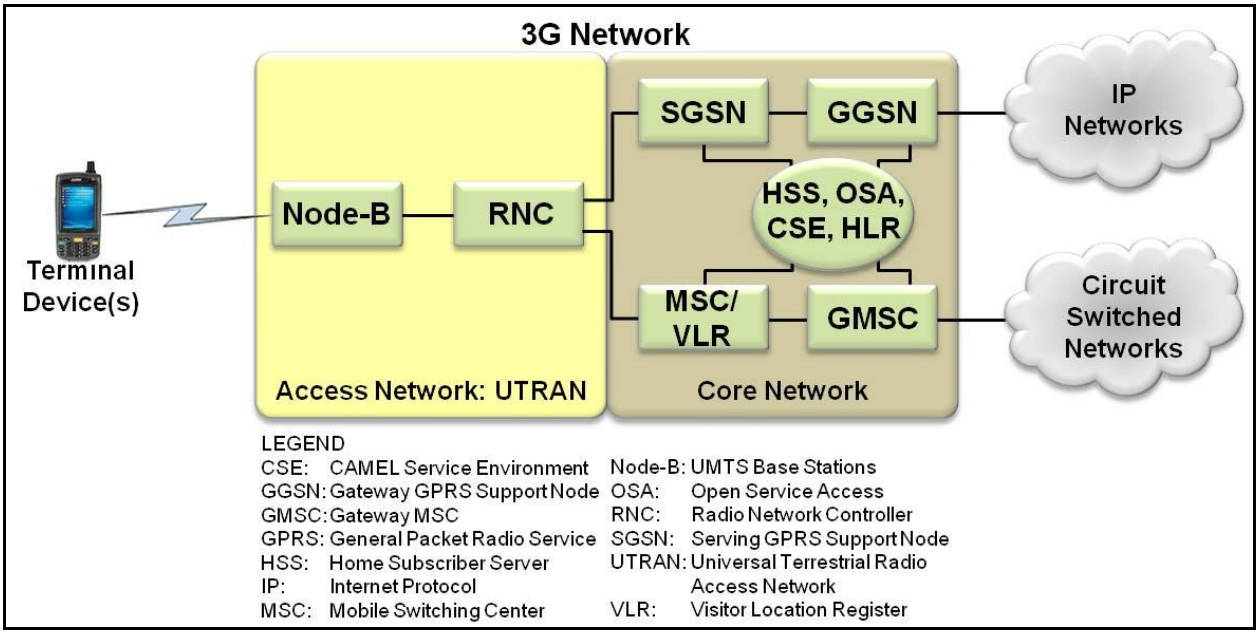

Figure A.9-3. 3G Cellular Primary Components

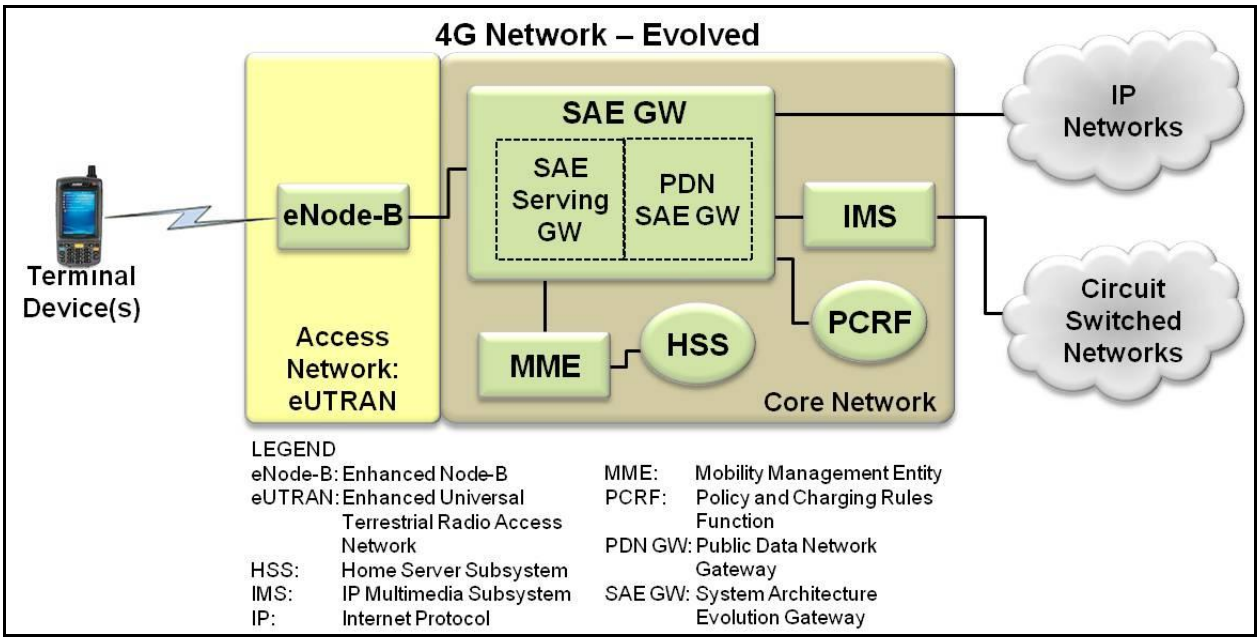

Figure A.9-4. 4G Cellular Primary Components

A.9.5 Deployed Voice Quality

The desired objective for Deployed voice quality is a mean opinion score (MOS) of 4.0 or greater, but it is realized that the network may operate under less than ideal conditions. The requirements provided in the following paragraphs are the minimally acceptable values under the conditions specified. The MOS calculation will assume the use of G.729 with 20 ms samples for the purpose of Service-Level Agreements (SLAs).

Using the International Telecommunications Union – Telecommunication (ITU-T) Recommendation P.862 testing standard, the baseline test environment shall be operated in an open air, clear of obstruction, line-of-sight environment, with the specific requirements. Based on the results, the estimated MOS performance range will be extrapolated and provided in the vendor Letter of Compliance (LOC) based on the Access Network operating at or near full power mode and, at a minimum, operating at a height of 80 feet. The values provided in the vendor LOC will be included in the APL report.

A.9.6 Deployed Tactical WAN Optimization

WOCs perform specific traffic conditioning processes to improve delivery time and bandwidth utilization across LAN/WAN infrastructures. Typically, these processes are combinations of techniques meant to improve the performance at several layers in the OSI model. These improvements are usually achieved by modifications in the TCP/IP model and or the OSI model. There are two distinct modifications in use:

Transport Protocol-optimizations operate primarily at layer 4 and tend to focus on streamlining Transmission Control Protocol (TCP) and other protocol chattiness to overcome latency issues.

Optimizations are achieved via Selective Acknowledgment (SACK), Space Communications Protocol Specification (SCPS), Window Sizing, Congestion Avoidance Modification, etc.

Application layer optimizations usually operate at several OSI layers simultaneously, typically layers 5–7, to achieve improved performance of application layer processes and user activities.

WOC optimizers are normally deployed in pairs. In tandem, they perform all of the functions required to optimize the prevailing circuit conditions for the IP traffic type that the WOC is transporting; this relationship is depicted in the DISN architecture. Figure A.9-5, UC Operational Framework.

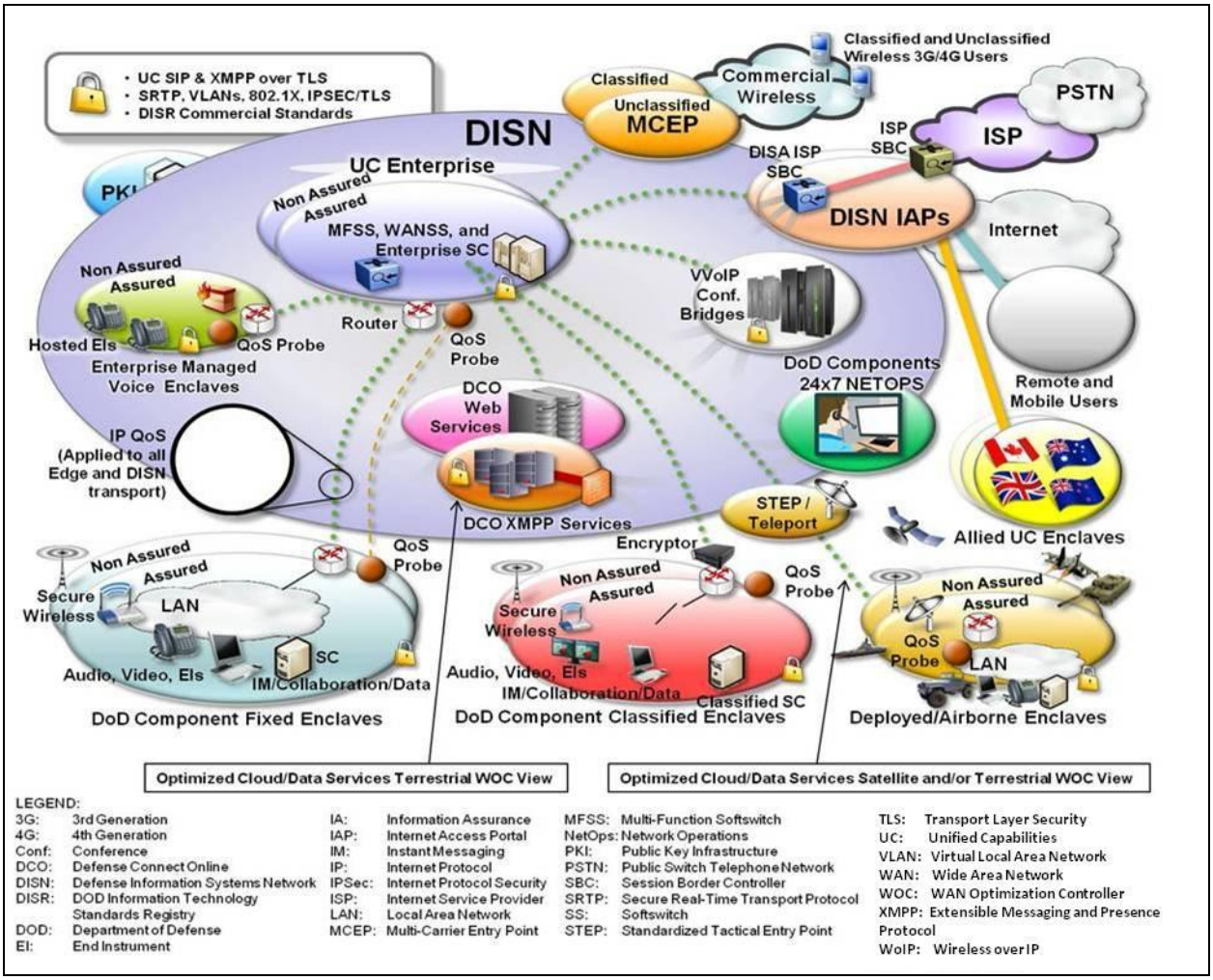

Figure A.9-5. UC Operational Framework

A.9.7 Spectrum Planning and Management

Spectrum Planning and Management is the effective control of the Electromagnetic Spectrum through proper planning of available resources by a central control. This includes frequency planning, requesting, allocation, and de-confliction to ensure maximum operational support while minimizing negative impacts to other spectrum users.

A.10 DEPLOYED UNIFIED CAPABILITIES STANDARDS REQUIREMENTS

A.10.1 Deployed Cellular Voice Exchange (DCVX)

The DCVX functions and provides mobile cellular services similar to standard commercial cellular systems with the addition of MUFs. It is based on a two-way cellular radio system that interconnects cell phones with other cell phones and landline stations. When used, the DCVX will provide full mobile cellular coverage in designated deployed environments; this includes training, exercise, and operational missions within COCOM areas of responsibility (AORs) or specific geographic areas. User voice, data, and related communications via terminal devices will be similar to landline wired DSN or commercial services. Except for the inherent characteristics of radio transmission, basic service features between the two systems will be similar and transparent to the users. After full mature architectural implementation, the DCVX will function as a wireless adjunct and extension of the joint OAN tier of the GIG.

A.10.1.1DCVX System Overview

The DCVX systems provide wireless mobile communication services with MUFs and draw their Strategic services by approved DoD authorized gateway switching systems only. The DCVX can be connected to a DVX-C or connected directly to the DSN and/or UC Services Network utilizing AS-SIP for TDM and IP switching systems, respectively. The DCVX systems also may be interconnected with other cellular telephone systems, excluding commercial systems, unless the commercial system is procured or leased for DoD usage and is operating in an isolated mode from other commercial provider cellular systems.

When placed in a Deployed environment, the DCVX will have the capability to connect to DSN/UC Services and between other DCVXs and DVX-Cs using UCR-defined protocols such as ISDN PRI, MLPP PRI (T1.619a), and/or AS-SIP. A DCVX system may also be configured to interconnect at the network transmission level with other DCVX systems to provide roaming capability outside the local home base cellular network for supported terminal devices. In support of this roaming capability, the DCVX cellular systems may interconnect based on the interconnection protocol requirements of the appropriate 2G, 3G, and/or 4G standards.

The DCVX terminal devices, often referred to as mobile subscriber cellular handsets, PDAs, Smartphones, BlackBerry®s, and any other end user cellular devices, commercial or Government developed, may connect to commercial cellular systems when operating outside the transmission range of the DCVX. Additionally, the cellular terminal devices may have the capability to interface with other wireless networks (e.g., IEEE 802.11 and IEEE 802.16). Actual employment of this additional cellular terminal device capability will be by command approval only in the Tactical OAN.

A.10.1.2DCVX Component

The DCVX is composed of the following three major functional areas: Terminal devices(s), Access Network, and Core Network. Terminal devices can be mobile subscribers' cellular handsets, PDAs, Smartphones, BlackBerry, or any other end user cellular devices, commercial- or Government-developed. With the evolution of cellular technology from 2G to 4G, the primary functional components that compose the DCVX Access and Core Networks are evolving as well. For comparison of the primary functional Access and Core Network components that compose an operational DCVX across the evolutionary changes.

A.10.1.3DCVX Operation

The DCVX functions and provides mobile cellular services similar to standard commercial cellular systems with the addition of MUFs. It is based on a two-way cellular radio system that interconnects cell phones with other cell phones and landline stations. When used, the DCVX will provide full mobile cellular coverage in designated deployed environments; this includes training, exercise, and operational missions within COCOM AORs or specific geographic areas. User voice, data, and related communications via terminal devices will be similar to landline wired DSN or commercial services. Except for the inherent characteristics of radio transmission, basic service features between the two systems will be similar and transparent to the users. After full mature architectural implementation, the DCVX will function as a wireless adjunct and extension of the joint OAN tier of the GIG. The following configurations, illustrated in Figure A.10-1, DCVX Connection Options, define the operational deployment options of a DCVX.

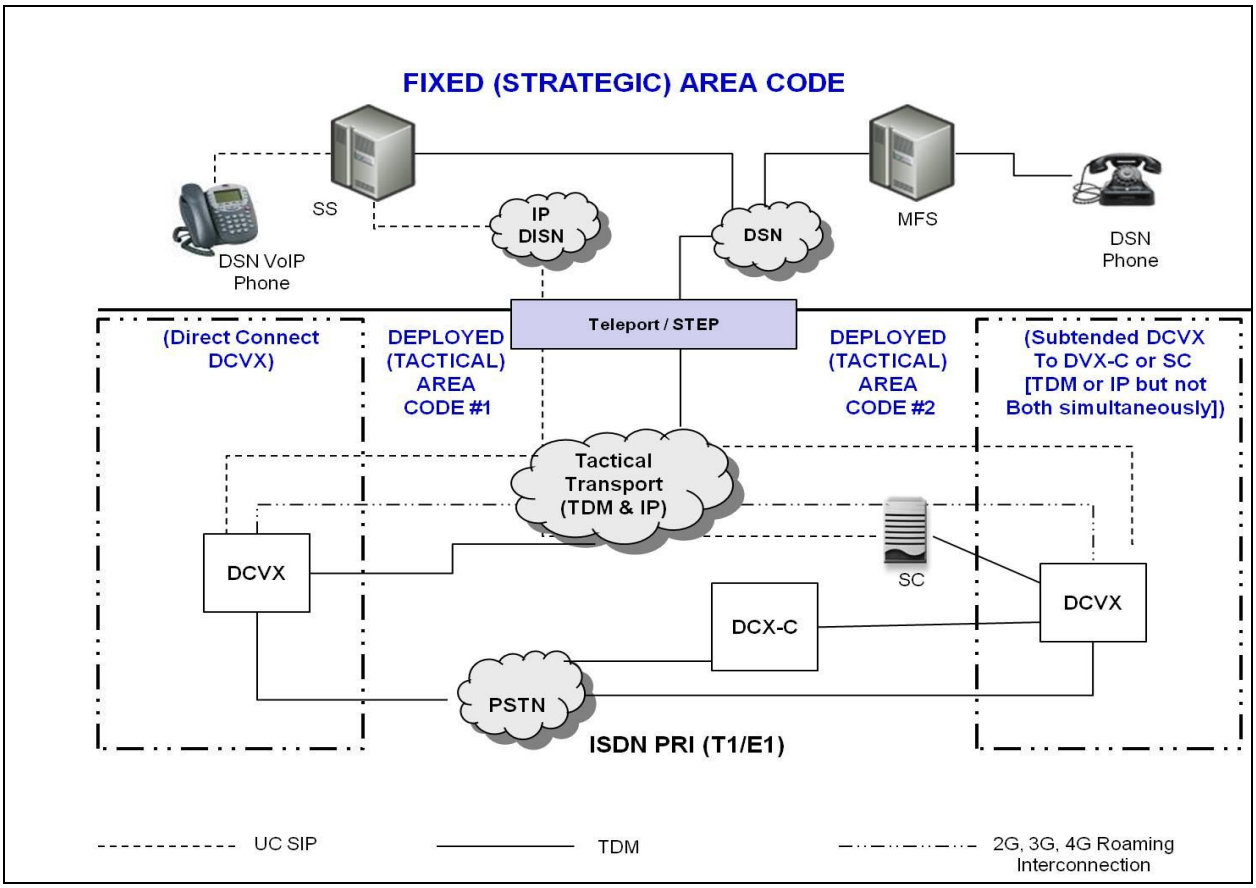

Figure A.10-1. DCVX Connection Options

A.10.1.4Subtended Deployment Connection

For a subtended deployed connection, the DCVX can reach DSN voice services or UC Services (VVoIP) using an existing authorized gateway switch; i.e., DVX-C or a Tactically deployed SC, respectively. To accomplish this, the DCVX can connect to the Tactical TDM and IP transport networks, with one or more of the following interfaces:

- ISDN PRI (T1/E1).
- MLPP ISDN PRI (T1/E1).
- IP AS-SIP (TLS signaling and associated SRTP bearer channel).
- IP Non-UC Services (non-Real Time Data, i.e., Best Effort Data).

If the DCVX supports AS-SIP in this subtended configuration, connected to a Tactical SC, then the DCVX operates in the Master-Subtended configuration to the Tactical SC. The DCVX can support simultaneous interface connections to the DSN and UC VVoIP/Data networks using TDM and IP, respectively, but not use TDM and AS-SIP protocol simultaneously in support of voice and/or video calls. Current connections to the PSTN and/or other non-Government networks will be limited to ISDN PRI (T1/E1) only. Future IP-based PSTN voice and video

service connections will be allowed once Information Assurance policy and STIGs are established.

A.10.1.5Direct DSN Deployment Connection

For a direct DSN or UC VVoIP connections for UC Services, as well as IP data connections, the DCVX will use the "direct connection" configuration to the Tactical, TDM, and IP transport networks with one or more of the following interfaces:

- ISDN PRI (T1/E1).
- MLPP ISDN PRI (T1/E1).
- IP AS-SIP (TLS signaling and associated SRTP bearer channel).
- IP Non-UC Services (non-Real Time Data, i.e., Best Effort Data).

The DCVX can support simultaneous interface connections to the DSN and UC VVoIP/Data networks using TDM and IP respectively, but not use TDM and AS-SIP protocol simultaneously in support of voice and/or video calls. Current connections to the PSTN and/or other non-Government networks will be limited to ISDN PRI (T1/E1) only. Future IP-based PSTN voice and video service connections will be allowed once Information Assurance policy and STIGs are established.

A.10.1.6Networked DCVX Deployment

When a DCVX is deployed in a networked DCVX configuration, a large deployed unit or multiple deployed units within the Tactical OAN may be interconnected with one or more HLR routing tables configured to support cellular terminal device roaming capabilities per the interconnections previously described.

For networked DCVXs within the Tactical OAN in support of a terminal device roaming capability, the DCVX configuration to the Deployed transport network will be with one or more of the following interfaces:

- ISDN PRI (T1/E1).
- MLPP ISDN PRI (T1/E1).
- IP AS-SIP (TLS signaling and associated SRTP bearer channel).
- SIGTRAN (CCS7 over IP).
- 2G, 3G, and/or 4G Standards interconnection protocols transported over DoD Networks.

The extent of terminal device roaming capability will depend on the number and type of interconnections made between the DCVXs within the Tactical OAN and switch lookup routing table updates in the DCVXs themselves.

Current connections to the PSTN and/or other non-Government networks will be limited to ISDN PRI (T1/E1) only. Future IP-based PSTN voice and video service connections will be allowed once Information Assurance policy and STIGs are established.

A.10.1.7Stand-Alone DCVX Deployment

When a DCVX is used in a stand-alone configuration, the only area served is a deployed unit establishing a JTF and its command, control, communications, and computers (C4) infrastructure. There is no DSN or PSTN access and no roaming beyond the deployed local network unit cell towers of its area of operation. The DCVX operates solely in an isolated mode.

A.10.2 Priority Access Service Wireless Access Service

Priority access service (PAS) provides the logical means for authorized mobile users to queue to the front and obtain priority access to the next available channel in a wireless call path. The goal of the wireless priority service (WPS) is to provide an E2E OAN-wide wireless priority communications capability to key military personnel during natural or manmade disasters. The WPS is an enhancement to basic cellular service. The full WPS capability can provide priority handling from mobile call origination, through the network, and all the way to the call destination.

The WPS is invoked by keying a special access number (*272) before the destination number on cellular instruments that have been classmarked for the WPS feature. A WPS user may be assigned one of five priority levels (i.e., 1, 2, 3, 4, or 5), with "1" being the highest priority level and "5" being the lowest. Each priority level has user-qualifying criteria that may be tracked for MLPP in DSN or in the UC Network via AS-SIP.

When a WPS call is queued for a radio traffic channel from a cellular user and no channel is available, the call is queued according to (1) the highest PAS priority first, and (2) queue entry time (i.e., earliest call first) within the same priority. If the queue for the call sector is full and the caller's priority is determined to be higher than the level of the lowest priority caller in the queue, then the most recent WPS entry shall be removed, with the new WPS call request queued IAW items (1) and (2).

A.10.2.1DoD Global System for Mobile Cellular Band

The current dedicated DoD Global System for Mobile (GSM) band is from 1755 MHz to 1835 MHz, which is a subset of the commercial DCS-1800 band. The remaining Government-owned frequency ranges are 1755 MHz to 1785 MHz for the uplink and 1805 MHz to 1850 MHz for the downlink. There are no non-DoD regulatory challenges associated with the use of the GSM band. The band has been approved for exclusive DoD use and is not authorized for use by any other entity. This band can be used for both voice and data applications to support unique DoD requirements. The Government-owned band may be adjusted in the future, and can be used appropriately at that time.

The band benefits are only effective in a CONUS environment; however, the DoD GSM may be used in OCONUS with specific host country/countries' authorization. The normal DoD frequency allocation process shall be followed to allow system operation within this band, and CC/S/A planners must ensure that an alternative solution is available before deployment as part of the planning process.

A.10.2.2Submission of Wireless Systems to UCCO for DSN Connection Request

The user shall submit a network design and engineering performance analysis with supporting calculations to meet minimum MOS performance with the request for DSN, PSTN, and/or UC Services Network connection. For certification procedures, the UCCO submittal shall include wireless security compliancy.

A.10.3 Radio Gateway

The UCR Radio Gateway Requirements product category is specific to the functionality of the RG. The functionality is available to support UC APL products and products that may not require UC APL certification. For example, DoD radio equipment, REIs and VNARs are not on the Unified Capability Approved Product List (APL) but are the critical communication asset that the RG MUST interface to. In addition to the radio assets, an IP End Instrument (EI) or its application may not be part of the UC APL. This is due to the new support capabilities of the RG's Stream Function. This function is capable of receiving and transmitting RTP voice traffic over multicast. While this category defines the RG's multicast requirements, the IP EI must also meet specific multicast requirements—similar to the requirements defined under the Stream Function.

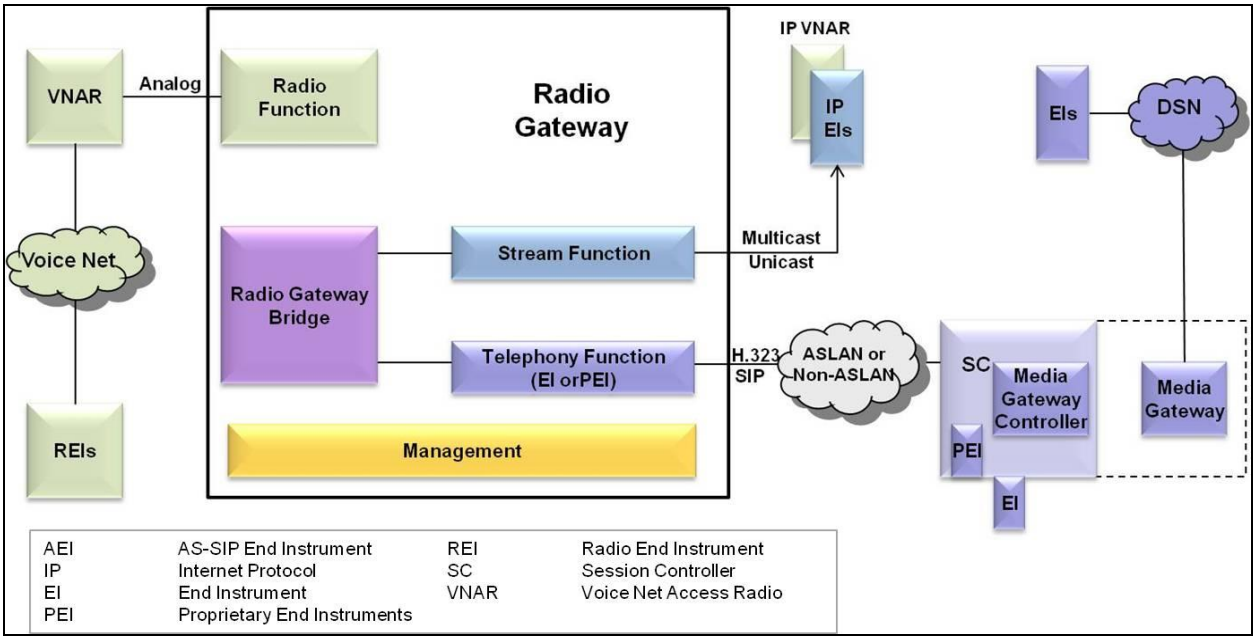

Figure A.10-2. Radio Gateway Components

RG Components are illustrated in Figure A.10-2 and are described as follows:

1. Radio Function. Provides the VNAR access to the RG through an analog interface. This is a 2 or 4 wire interface.
2. Telephony Function. Provides telephony access to the RG, using H.323, SIP, or proprietary protocols.
3. Stream Function. Provides a connectionless protocol interface to the RG. Data Terminals (DT)s or IP VNARs may stream Real-Time Protocol (RTP) audio through this interface.
4. RG Bridge. Performs the bridging of two or more RG interfaces (e.g. connect a VNAR's audio with a multicast group).
5. Management. Configuration front-end that allows an administrator to manipulate the RG's functions and bridge.

A.10.3.1Interfaces

The interfaces that the RG supports can be divided into three categories – Analog, Network, and Serial. These interfaces are illustrated in Figure A.10-3. Each of these performs a specific role to provide external access to various EIs.

1. Analog Interface. This interface is specific to a conventional VNAR connection. All received VNAR RF voice traffic is passed to the RG via this interface. As well, any voice traffic originating from an external EI, and bridged with the VNAR, will be transmitted from this interface towards the connected VNAR.
2. Network interface. The Network Interface connects to a Non-ASLAN or an ASLAN environment. The RG's Stream, Telephony, and Management Functions depend on this interface. It adheres to requirements that are set forth by Section 7, Network Edge Infrastructure, of the UCR.
3. Serial Interface. This interface traditionally gives a user direct access to the RG for configuration, troubleshooting, logging, and backup purposes. This MAY or MAY NOT be required for Management Functions.

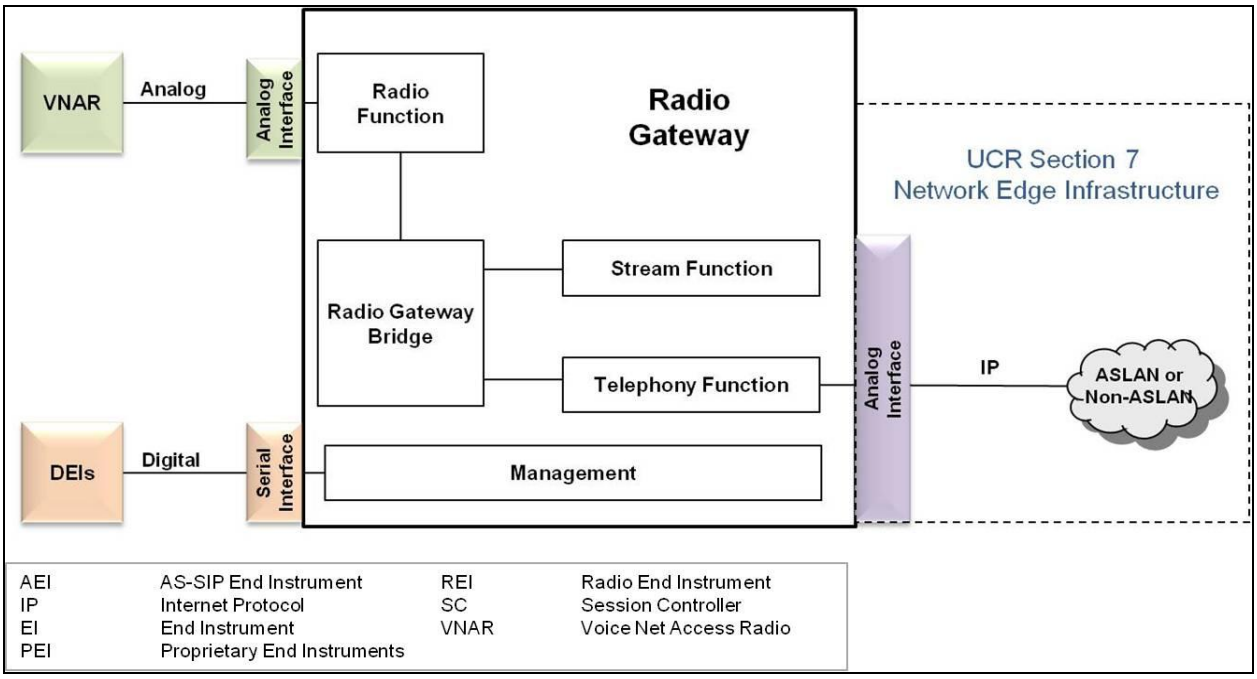

Figure A.10-3. Radio Gateway Interfaces

A.10.4 Code Division Multiple Access Mobile Systems

Mobile Code Division Multiple Access (CDMA) technology uses spread-spectrum telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. The latest technology today is based on third generation (3G) that allows high and fast bandwidth, generically called Evolution-Data Optimized (EVDO or EV-DO). This capability supports data usage of the terminal device to allow data connections to DoD networks and future possible use of a VoIP softphone on terminal devices when connected to commercial networks for extension of DSN single number presence.

A.10.5 GSM Communications Mobile Systems

Early technology for GSM allowed for the use Time Division Multiple Access (TDMA) technology. The TDMA allows several users to share the same frequency. It is the most popular standard for mobile phones in the world. The ubiquity of the GSM standard makes international roaming very common with "roaming agreements" between mobile phone operators. The latest GSM standard is based on an open standard that is developed by the Third Generation Partnership Project (3GPP).

A.10.6 4G IMT-Advanced System

Fourth generation (4G) refers to the fourth generation of cellular wireless standards. It is a successor to the 2G and 3G families of standards. The nomenclature of the generations generally refers to a change in the fundamental nature of the service, non-backwards-compatible

transmission technology, and new frequency bands. The term 4G refers to an all-IP packet-switched network, mobile ultra-broadband (gigabit speed) access, and multi-carrier transmission. 4G is based on the ITU-R standard IMT-Advanced (International Mobile Telecommunications Advanced). An IMT-Advanced cellular system must have target peak data rates of up to approximately 100 Mbps for high mobility such as mobile access and up to approximately 1 Gbps for low mobility such as nomadic/local wireless access, according to the ITU requirements. The 3GPP and Worldwide Interoperability for Microwave Access (WiMAX) standards that will meet the ITU IMT-Advanced standard, are the pending 4G-Advanced and 802.16m, respectively. In all suggestions for 4G, the CDMA spread spectrum radio technology used in 3G systems and IS-95, is abandoned and replaced by frequency-domain equalization schemes, for example multi-carrier transmission such as OFDMA. This is combined with Multiple In Multiple Out (MIMO) (i.e., multiple antennas), dynamic channel allocation and channel-dependent scheduling. In the meantime, pre-4G technologies such as first-release 4G Long Term Evolution (LTE) and Mobile WiMAX, have been available on the market since 2009 and 2006 respectively. However, 4G-LTE does not address the use of voice (a.k.a. VoIP) at this time. The GSM Association, via the Voice over LTE (VoLTE) initiative, is addressing this omission by selecting a subset of IP Multimedia Subsystem (IMS) standards to deliver E2E voice and SMS for LTE devices, including defining roaming and interconnect interfaces. In the meantime, most commercial cellular providers utilize Circuit-Switched Fallback (CSFB), which uses some initial signaling over the LTE Radio Access Network (RAN) and then "falls back" to the 2G/3G TDM RAN to establish the calls.

A.10.7 Secure Communications Interoperability Protocol

The SCIP is the NSA-approved secure voice and data encryption protocol used by DoD, U.S. Government agencies, and civilian authorities. The SCIP is used by NATO and coalition partners to provide secure voice interoperability between the United States and authorized foreign entities. Application of SCIP is described in detail in Section 13, Security Devices.

A.10.7.1Codecs

Bearer Traffic: In addition to acting as a PTT signaling and instruction interpreter, the RG MUST be able to receive and send audio traffic between the different endpoints (VNARs and EIs) using protocols and technologies that the RG and endpoints both support.

a. DSN approved Codecs: To communicate with the IP VNARs and EIs that traverses the DSN environment, the RG's Telephony function MUST be able to encode and decode the audio stream with at least one of the following codecs for each endpoint that MUST communicate with this function.

b. IP EI Stream Codecs. In addition to the DSN Approved Codecs, the IP EI may support additional codecs to make the RG more accessible to various EIs, reduce bandwidth requirements, and/or to improve voice quality.

c. Low-Bandwidth/Secure Audio. MELPe is a Department of Defense and NATO approved narrowband codec that is used for securing and encoding/decoding military communications over low-bandwidth links. If the RG will be interfacing to a MELPe compliant IP VNAR or IP EI, MELPe support is REQUIRED.

d. WAN Traversed Audio. If voice traffic must pass between IP enclaves (e.g. pass traffic from LAN A to LAN B through a WAN connection) G.729 MUST codec is used in order to support low-bandwidth WAN links, such as satellite links.

e. With the advent of the implementation of the Micro Light Software DefiThe UCR Radio Gateway Requirements product category is specific to the functionality of the RG. The functionality is available to support UC APL products and products that may not require UC APL certification. For example, DoD radio equipment, REIs and VNARs are not on the Unified Capability Approved Product List (APL) but are the critical communication asset that the RG MUST interface to.

In addition to the radio assets, an IP End Instrument (EI) or its application may not be part of the UC APL. This is due to the new support capabilities of the RG's Stream Function. This function is capable of receiving and transmitting RTP voice traffic over multicast. While this category defines the RG's multicast requirements, the IP EI must also meet specific multicast requirements – similar to the requirements defined under the Stream Function.

A.10.8 WAN Optimization Controller (WOC)

WOCs fall within the general class of Network Elements (NE). WOCs perform Traffic Conditioning Services, Bandwidth Management Services, and Per Hop Behavior (PHB) Management Services in order to achieve an improved level of performance in the transport efficiency of data. To achieve the desired level of traffic conditioning, various techniques are leveraged to manipulate processes at various layers within the Open Systems Interconnect (OSI) Model.

Optimization may be sought for a number of reasons; high latency links, bandwidth constrained links, or to overcome the effects of excessively "chatty" applications. Local Area Network (LAN)\WAN Optimizers can now be connected to the Defense Information System Network (DISN) in order to optimize Internet Protocol (IP) network capabilities. To take advantage of these advancements, this appendix defines the LAN\WAN Optimizer requirements that must be met in order to be placed on the Unified Capabilities (UC) Approved Products List (APL). The goal of optimization is to improve network efficiency and performance due to faster IP transport and improved bandwidth utilization.

A.10.8.1WOC Functional Description

WOCs perform specific traffic conditioning processes to improve delivery time and bandwidth utilization across LAN/WAN infrastructures. Typically, these processes are combinations of techniques meant to improve the performance at several layers in the OSI model. These

improvements are usually achieved by modifications in the TCP/IP model and or the OSI model. There are two distinct modifications in use:

Transport Protocol-optimizations operate primarily at layer 4 and tend to focus on streamlining Transmission Control Protocol (TCP) and other protocol chattiness to overcome latency issues. Optimizations are achieved via Selective Acknowledgment (SACK), Space Communications Protocol Specification (SCPS), Window Sizing, Congestion Avoidance Modification, etc.

Application layer optimizations usually operate at several OSI layers simultaneously, typically layers 5-7, to achieve improved performance of application layer processes and user activities.

WOC optimizers are normally deployed in pairs. In tandem, they perform all of the functions required to optimize the prevailing circuit conditions for the IP traffic type that the WOC is transporting;

A.10.8.2Applications and Configurations

WOCs address four distinct data transport configurations based on the physical characteristics of the WAN infrastructure, its primary function, or its method of implementation. The four configurations and transport characteristics are identified as follows:

- Transport:
  - Satellite Network (SN) – high latency due to long physical propagation time" bandwidth is limited.
  - Terrestrial Network (TN) – users often experience slow network responsiveness.
  - Configurations.
  - Disaster Recovery (DR) – requires speedy transport of high volume traffic.
  - Software Clients (SC) – software- based optimization capability. SCs can support individual remote or mobile users, or multiple users depending on application.