Department of Defense

Unified Capabilities Framework 2013
(UC Framework 2013)

January 2013

The Office of the DoD Chief Information Officer

DEPARTMENT OF DEFENSE

UNIFIED CAPABILITIES FRAMEWORK 2013 (UC FRAMEWORK 2013)

TABLE OF CONTENTS

SECTION **PAGE**

Section 1 Introduction and UC Design Overview 1-1
1.1 Purpose 1-1
1.2 Applicability and Scope 1-2
1.3 Document Overview 1-2
1.4 Network Support for UC Services 1-3
1.5 UC Operational Framework Overview and Summary 1-4
1.6 High Level Operational Concept 1-6
1.7 Operational Construct for UC NetOps 1-7
1.8 UC Implementation Priority and Schedule 1-8
1.9 Assured Services Design Criteria 1-9
1.10 UC Network Infrastructure Overview 1-12
1.10.1 IP-Based CE Segment 1-12
1.10.2 Network Edge Segment 1-13
1.10.3 DISN Service Delivery Nodes 1-14
1.10.4 Network Core Segment 1-16
Section 2 Session Control Products 2-1
2.1 Network Engineering Attributes 2-1
2.1.1 Quality of Service Features 2-2
2.1.2 Assured Services Features and Capabilities 2-4
2.1.2.1 Attributes Within the Edge Segment 2-5
2.1.2.2 Attributes Within the DISN WAN (Access/Distribution and Core) 2-5
2.1.2.3 E2E Protocol Planes 2-6
2.1.2.4 Assured Services Subsystem 2-6
2.1.3 Voice and Video Signaling Design 2-9
2.1.4 Distributed UC Services Model 2-11
2.1.5 Session Control Failover Feature 2-12
2.2 Enterprise UC Services Design 2-14
2.2.1 Enterprise UC Vision 2-14
2.2.2 Enterprise System Design 2-15
2.2.3 The Enterprise Continuity of Operations (COOP) Capabilities 2-16
2.2.3.1 Environment Type 1 2-16
2.2.3.2 Environment Type 2 2-17
2.2.3.3 Environment Type 3 2-18

2.2.4 Messaging (IM/Chat/Presence) Integration 2-19
2.2.5 Enterprise Directory Services (EDS) 2-20
2.3 Mobility and Service Portability 2-25
2.4 ASAC Operation Overview 2-26
2.4.1 ASAC Budgets and Counts 2-27
2.4.1.1 Voice Budgets and Counts 2-27
2.4.1.2 Video Budgets and Counts 2-27
2.4.2 ASAC Session Control Overview 2-28
2.4.2.1 Outbound (Originating-Outgoing) Voice Sessions 2-28
2.4.2.2 Inbound (Incoming-Terminating) Voice Sessions 2-28
2.4.2.3 Directionalization 2-29
2.4.2.4 Video Session Processing 2-29
2.5 Precedence-Based Assured Services 2-30
2.6 Voice Features and Capabilities 2-31
2.6.1 Call Forwarding 2-31
2.6.2 Precedence Call Waiting 2-32
2.6.3 Call Transfer 2-33
2.6.4 Call Hold 2-33
2.6.5 Three-Way Calling 2-34
2.6.6 Hotline Service 2-34
2.6.7 Calling Number Delivery 2-34
2.6.8 Call Pick-Up 2-35
2.6.9 Precedence Call Diversion 2-35
2.6.10 Public Safety Voice Features 2-36
2.6.10.1 Basic Emergency Service (911) 2-36
2.6.10.2 Tracing of Terminating Calls 2-36
2.6.10.3 Outgoing Call Tracing 2-36
2.6.10.4 Tracing of a Call in Progress 2-37
2.6.10.5 Tandem Call Trace 2-37
2.7 End Instruments 2-37
2.7.1 Voice over IP Sampling Standard 2-38
2.7.2 Operational Framework for AS-SIP EIs 2-39
2.7.2.1 AS-SIP Secure Voice EI Supplementary Services 2-40
2.7.3 V.150.1 Modem Relay Secure Phone 2-41
2.7.3.1 Architecture for Supporting SCIP/V.150.1 Modem Relay 2-41
2.7.3.2 SCIP/V.150.1 Gateway 2-44
2.7.3.3 SCIP/V.150.1 End Instrument 2-45
2.8 Session Controller 2-46

2.9 AS-SIP Gateways 2-49
2.9.1 AS-SIP TDM Gateway 2-49
2.9.1.1 Overview 2-49
2.9.1.2 AS-SIP TDM Gateway Functional Reference Model 2-50
2.9.2 AS-SIP IP Gateway 2-52
2.9.2.1 Overview 2-52
2.9.2.2 AS-SIP IP Gateway Functional Reference Model, Assumptions, Functions and Features 2-53
2.9.3 AS-SIP – H.323 Gateway 2-55
2.9.3.1 Overview 2-55
2.9.3.2 AS-SIP – H.323 Gateway Functional Reference Model 2-57
2.9.3.3 Summary of AS-SIP – H.323 Gateway Functions and Features 2-58
2.9.3.4 AS-SIP – H.323 Gateway CCA Function Overview 2-59
2.10 Network-Level Softswitch 2-60
2.10.1 SS Functional Reference Model, Assumptions and Signaling Interfaces 2-61
2.10.1.1 Assumptions – SS 2-61
2.10.1.2 Signaling Interfaces – SS 2-63
2.11 Call Connection Agent 2-64
2.11.1 Introduction 2-64
2.11.2 Functional Overview of the CCA 2-65
2.11.2.1 CCA IWF Component 2-67
2.11.2.2 CCA MGC Component 2-67
2.11.3 CCA Interaction With Network Appliances and Functions 2-67
2.11.3.1 CCA Interactions With Transport Interface Functions 2-67
2.11.3.2 2CCA Interactions With the SBC 2-68
2.11.3.3 CCA Support for Admission Control 2-69
2.11.3.4 CCA Support for User Features and Services 2-69
2.11.3.5 CCA Support for Information Assurance 2-70
2.11.3.6 CCA Interactions With Session Controller Location Service 2-70
2.11.3.7 CCA Interactions With Softswitch Location Service 2-71
2.11.3.8 CCA Interactions With End Instrument(s) 2-71
2.11.3.9 CCA Interactions With Service Control Functions 2-71
2.12 Media Gateway 2-72
2.12.1 Introduction 2-72
2.12.2 Overview of the MG and MGC Functions 2-74
2.12.2.1 Primary Trunk Functions and Interfaces 2-75

2.12.2.2 Primary Access Functions and Interfaces 2-75
2.12.2.3 MGC Functions 2-76
2.12.3 Role of the MG in Appliances 2-77
2.12.3.1 Role of the MG in the SC 2-77
2.12.3.2 Role of the MG in the SS 2-79
2.12.4 MG Interaction With NES and Functions 2-80
2.12.4.1 MG Support for ASAC 2-80
2.12.4.2 MG and Information Assurance Functions 2-81
2.12.4.3 MG Interaction With Service Control Functions 2-82
2.12.4.4 Interactions With IP Transport Interface Functions 2-82
2.12.4.5 MG-SBC Interaction 2-83
2.12.4.6 MG Support for Appliance Management Functions 2-84
2.12.4.7 Interactions With VoIP EIs 2-84
2.12.5 MG and Echo Cancellation 2-84
2.12.5.1 Echo Control Design 2-84
2.12.6 MG and Synchronization 2-86
2.12.7 MGC-MG CCA Functions 2-86
2.12.8 Remote Media Gateway Requirements 2-86
2.13 Session Border Controller 2-88
2.14 Worldwide Numbering and Dialing Plan 2-88
2.14.1 Domain Directory 2-92
2.15 Management of Network Appliances 2-94
2.15.1 Voice and Video Network Management Domain 2-95
2.15.2 General Management Approach 2-95
2.15.3 Traffic Flow Control Overview 2-97
2.15.3.1 Destination Code Controls 2-98
2.15.3.2 Call Budget Control 2-98
2.16 Dynamic ASAC 2-98
2.16.1.1 Dynamic ASAC Calculation Examples 2-103
Section 3 Auxiliary Services 3-1
3.1 Regional Hub Design for Required Ancillary Equipment (RAE) 3-1
3.2 Commercial Cost Avoidance and Hybrid Routing Feature 3-3
3.3 Interface to Emergency Response Systems 3-5
3.3.1 Enhanced 911 Interface 3-5
3.3.2 Mass Notification Warning System Interface 3-5
3.4 Other Auxiliary Services 3-6
Section 4 Information Assurance 4-1
Section 5 IPv6 5-1

5.1 Introduction 5-1
5.2 Definitions 5-1
5.3 DoD IPv6 Profile 5-3
5.3.1 Product Requirements 5-4
Section 6 Network Infrastructure End-to-End Performance 6-1
6.1 Network Segments and Measurement Points 6-1
6.2 UC Engineering Network Considerations 6-2
6.2.1 Voice Codec Compression 6-4
6.3 Assured UC Latency Design Considerations 6-4
6.3.1 Assured UC Router Serialization/Packet Switching Latency 6-4
6.3.2 Assured UC End-To-End Latency 6-4
6.3.3 Assured UC CE Segment Latency 6-5
6.3.4 Assured UC AR-to-AR Latency 6-7
6.3.5 Assured UC CE Router-to-CE Router Latency 6-8
6.4 Assured UC Jitter 6-9
6.4.1 Assured UC End-to-End Jitter 6-9
6.4.2 Assured UC AR-to-AR Jitter 6-10
6.4.3 Assured UC CE Router-to-CE Router Jitter 6-11
6.4.4 Assured UC CE Segment Jitter 6-12
6.5 Assured UC Packet Loss Design Considerations 6-12
6.5.1 Assured UC End-To-End Packet Loss 6-12
6.5.2 Assured UC AR-to-AR Packet Loss 6-13
6.5.3 Assured UC CE Router-to-CE Router Packet Loss 6-14
6.6 Non-Assured Voice 6-15
6.7 Data Applications 6-16
6.8 Service Level Specification 6-16
6.9 System-Level Quality Factors 6-17
6.9.1 Handset-to-Handset Availability 6-17
6.9.2 Network Segments Availability 6-18
6.9.3 Availability Design Considerations 6-19
6.9.4 Reliability and Failover Considerations 6-20
6.10 Bandwidth Provisioning Considerations 6-21
6.11 Voice Grade of Service 6-23
6.12 Traffic Conditioning Considerations 6-24
6.12.1 Queuing Trust Considerations 6-24
6.12.2 Queuing Policing, Scheduling & Markdown Considerations 6-24
6.13 UC Network Infrastructure Survivability 6-25
6.14 Voice Service Quality 6-25

Section 7 Network Edge Infrastructure 7-1
7.1 CE Segment Attributes 7-1
7.2 B/P/C/S UC Design 7-2
7.3 SC Designs – Voice 7-2
7.4 SC Designs – Video 7-5
7.5 LAN And ASLAN Design 7-7
7.5.1 Overview of LAN General Design and Requirements 7-8
7.5.2 LAN Types and Mission Support Summary 7-11
7.5.3 Wireless LANs 7-14
7.6 End-to-End LAN Performance Requirements 7-15
7.6.1 Voice Services 7-15
7.6.1.1 Latency 7-15
7.6.1.2 Jitter 7-15
7.6.1.3 Packet Loss 7-15
7.6.2 Video Services 7-15
7.6.2.1 Latency 7-15
7.6.2.2 Jitter 7-16
7.6.2.3 Packet Loss 7-16
7.6.3 Data Services 7-16
7.6.3.1 Latency 7-16
7.6.3.2 Jitter 7-16
7.6.3.3 Packet Loss 7-16
7.7 Infrastructure Network Management Requirements 7-17
7.7.1 Configuration Control 7-17
7.7.2 Operational Changes 7-17
7.7.3 Performance Monitoring 7-18
7.7.4 Alarms 7-18
7.7.5 Reporting 7-18
7.8 Engineering Requirements 7-18
7.8.1 Copper Media 7-18
7.8.2 Traffic Engineering 7-19
7.8.2.1 Voice Services 7-19
7.8.2.2 Video Services 7-22
7.8.2.3 Data Services 7-23
7.8.3 VLAN Design and Configuration 7-24
7.8.4 Power Backup 7-25
7.8.5 Availability 7-26
7.8.6 Maintainability 7-27

7.8.7 MPLS Background 7-28
7.8.8 MPLS Terminology 7-29
7.8.9 DoD LAN MPLS Operational Framework 7-30
7.8.10 Primary Application Support 7-30
7.8.11 DSL Overview 7-31
7.8.11.1 DSL Bonding 7-32
7.8.12 Ethernet in the First Mile Over Copper (EFMCu) 7-32
7.8.13 DSL-Based ASLAN Interconnection Operational Framework 7-33
7.8.13.1 Point-to-Point Interconnection of ASLANs 7-33
7.8.13.2 Point-to-Multipoint Interconnection of ASLANs 7-33
7.8.13.3 DSL Repeaters 7-34
7.8.13.4 DSL Support for Analog Voice and Voice over IP (VoIP) 7-35
7.8.14 References 7-37
7.9 Regional ASLAN 7-38
Section 8 Multifunction Mobile Devices 8-1
8.1 Use Cases for Multifunction Mobile Devices 8-2
8.1.1 Use Case #1: No DoD Network Access or CUI Processing (Non Enterprise Activated) 8-4
8.1.2 Use Case #2: Full DoD Network Connectivity Use Case – No Access to DoD UC Services 8-5
8.1.3 Use Case #3: Full DoD Network Connectivity Use Case with Access to DoD UC Services 8-5
8.2 Backend Support Systems Supporting Multifunction Mobile Devices 8-10
Section 9 Video Distribution System 9-1
9.1 Overview 9-1
9.2 General VDS System Recommendations 9-2
9.2.1 IP Recommendations for VDS Systems 9-2
9.2.2 VDS Signal Extenders Recommendations 9-2
9.2.3 VDS Peripheral Guidelines 9-2
9.2.4 VDS Peripheral Connectors Guidelines 9-3
9.2.5 VDS Peripheral Connector Conversion Devices 9-3
9.2.6 VDS Matrix Switch Guidelines 9-3
9.2.7 VDS IA Security Recommendations 9-3
9.2.8 VDS Availability Recommendations 9-3
9.2.9 VDS Capacity Recommendations 9-4
9.2.10 VDS Diagnostics Recommendations 9-4
9.3 Closed VDS System Design Guidelines 9-4
9.4 VDS over IP (VDS-IP) Design Guidelines 9-4

9.5 VDS Recording Guidelines 9-5
Section 10 Network Infrastructure Products 10-1
10.1 DISN Converged Access 10-7
Section 11 Network Elements 11-1
Section 12 Generic Security Devices 12-1
12.1 Introduction 12-1
12.2 Security Products Overview 12-1
12.2.1 HAIPE 12-1
12.2.1.1 HAIPE IS V1.3.5 Devices 12-4
12.2.1.2 HAIPE IS 1.3.X Devices 12-4
12.2.1.3 Suite B Devices 12-5
12.2.2 Link Encryptor Family 12-5
12.2.3 Secure Communications Interoperability Protocol (SCIP) 12-6
12.3 Device Evaluation 12-8
12.3.1 HAIPE 12-8
12.3.1.1 Throughput Test 12-8
12.3.1.2 Reliability Test 12-8
12.3.1.3 Configuration Changes 12-9
12.3.1.4 Field Tamper Recovery 12-9
12.3.1.5 Loss of Physical Medium 12-9
12.3.1.6 Line Impairment 12-9
12.3.1.7 Latency Test 12-9
12.3.1.8 Denial of Service Test 12-10
12.3.1.9 Vulnerability Test 12-10
12.3.1.10 Configuration and Management 12-10
12.3.1.11 Secure Tunnel Setup and Security Policy Database Management 12-10
12.3.1.12 Management of Remote Devices 12-10
12.3.1.13 Cryptographic Key Loading 12-10
12.3.1.14 Firefly Vector 12-10
12.3.1.15 Enhanced Firefly Vector Set 12-11
12.3.1.16 Pre-Placed Key 12-11
12.3.1.17 Algorithms Supported 12-11
12.3.1.18 Usability 12-11
12.3.1.19 Device Software Upgradeability 12-11
12.3.2 Interoperability 12-11
12.3.2.1 Reachability 12-12
12.4 LEF Test & Evaluation 12-12

12.4.1 Initialization/Functional 12-12
12.4.2 Personality/Cryptographic Algorithms 12-12
12.4.3 Interoperability 12-12
12.4.4 Asynchronous Modes 12-12
12.4.4.1 Synchronous Modes 12-13
12.4.4.2 Link Encryption Interoperability and Interchangeability 12-13
12.4.5 Reliability 12-13
12.4.6 Reboot Test 12-13
12.4.6.1 Key Loading 12-13
12.4.6.2 Over-the-Air-Distribution or Over-the-Air-Re-Key 12-14
12.4.6.3 Change Key/Local Update Operations 12-14
12.4.7 Network Management 12-14
12.4.8 Software Download 12-15
12.4.9 Degraded Network Capability and Robustness 12-15
12.4.10 Required Ancillaries Devices 12-15
12.4.11 Control Signal Requirements 12-15
12.4.12 Interface Requirements 12-16
12.5 SCIP Evaluation 12-17
12.5.1 General Description 12-17
12.5.1.1 Evaluation Methods 12-18
Section 13 Security Devices 13-1
13.1 Physical Security 13-1
13.2 Security Devices Security Design 13-1
13.3 Network Security Design 13-1
13.4 Requirements Development Concept 13-3
Section 14 Online Storage Controller 14-1
Section 15 Enterprise and Network Management Systems 15-1
15.1 DISN Operational Support System Complex 15-2
15.2 UC Voice and Video Services Backbone Management System 15-3
15.3 Information Sharing 15-4
Appendix A Unique Deployed (Tactical) A-1
A.1 Scope A-1
A.2 Definitions A-1
A.3 Background A-1
A.4 Unified Capabilities Reference Architecture A-1
A.4.1 The UC Operational Framework A-1
A.4.1.1 Tactical Edge Network A-2
A.4.2 Operational Area Network (OAN) A-2

A.5 Army Common Operating Environment (COE) A-3
A.5.1 COE Overview A-3
A.5.2 COE Computing Environments A-4
A.5.3 COE Architecture A-5
A.5.3.1 Background A-5
A.5.3.2 Approach A-6
A.6 Deployed Unified Capabilities Standards References A-7
A.6.1 Network Operations A-7
A.6.2 Information Assurance A-8
A.6.3 Communications Security A-8
A.6.4 Quality of Service A-8
A.6.4.1 Background A-9
A.7 High-Level Tactical UC Architecture A-11
A.7.1 Hierarchical Network Architecture A-11
A.8 Meshed Network Architecture A-12
A.9 ASLAN Architecture A-14
A.9.1 Precedence and Preemption A-15
A.9.2 Global Block Numbering Plan A-16
A.9.3 Dynamic Unified Capabilities Admission Control (DASAC) A-17
A.9.4 Deployed Cellular Network Systems A-18
A.9.5 Deployed Voice Quality A-20
A.9.6 Deployed Tactical WAN Optimization A-20
A.9.7 Spectrum Planning and Management A-21
A.10 Deployed Unified Capabilities Standards Requirements A-22
A.10.1 Deployed Cellular Voice Exchange (DCVX) A-22
A.10.1.1 DCVX System Overview A-22
A.10.1.2 DCVX Component A-23
A.10.1.3 DCVX Operation A-23
A.10.1.4 Subtended Deployment Connection A-24
A.10.1.5 Direct DSN Deployment Connection A-25
A.10.1.6 Networked DCVX Deployment A-25
A.10.1.7 Stand-Alone DCVX Deployment A-26
A.10.2 Priority Access Service Wireless Access Service A-26
A.10.2.1 DoD Global System for Mobile Cellular Band A-26
A.10.2.2 Submission of Wireless Systems to UCCO for DSN Connection Request A-27
A.10.3 Radio Gateway A-27
A.10.3.1 Interfaces A-28

A.10.4 Code Division Multiple Access Mobile Systems A-29
A.10.5 GSM Communications Mobile Systems A-29
A.10.6 4G IMT-Advanced System A-30
A.10.7 Secure Communications Interoperability Protocol A-30
A.10.7.1 Codecs A-30
A.10.8 WAN Optimization Controller (WOC) A-31
A.10.8.1 WOC Functional Description A-32
A.10.8.2 Applications and Configurations A-32
Appendix B Unique Classified Unified Capability B-1
B.1 Signaling Design B-1
B.2 Directory (White Pages) Services B-2
Appendix C Definitions, Abbreviations and Acronyms, and References B-1
C.1 Overview C-1
C.1.1 Numbers C-1
C.1.2 A C-1
C.1.3 B C-5
C.1.4 C C-6
C.1.5 D C-11
C.1.6 E C-15
C.1.7 F C-17
C.1.8 G C-19
C.1.9 H C-20
C.1.10 I C-20
C.1.11 J C-24
C.1.12 K C-24
C.1.13 L C-25
C.1.14 M C-27
C.1.15 N C-31
C.1.16 O C-34
C.1.17 P C-35
C.1.18 Q C-39
C.1.19 R C-39
C.1.20 S C-42
C.1.21 T C-48
C.1.22 U C-52
C.1.23 V C-53
C.1.24 W C-55
C.1.25 X C-56

C.2 Acronym List C-56
C.3 References C-69
C.3.1 American National Standards Institute Documentation C-69
C.3.2 Assistant Secretary of Defense for Networks & Information Integration/DoD Chief Information Office C-71
C.3.3 British Standards Institute Documentation C-71
C.3.4 Chairman of the Joint Chiefs of Staff Documentation C-71
C.3.5 Defense Information Systems Agency Documentation C-72
C.3.6 Department of Defense Documentation C-72
C.3.7 DoD Directives C-73
C.3.8 DoD Instructions C-73
C.3.9 Electronics Industries Alliance C-73
C.3.10 ETSI Documentation C-74
C.3.11 Federal Information Processing Standards Publications C-74
C.3.12 Institute of Electrical and Electronics Engineers, Inc. Documentation C-75
C.3.13 International Telecommunication Union Documentation C-78
C.3.14 Internet Engineering Task Force Requests for Comment C-85
C.3.15 Joint Requirements Oversight Council Documentation C-101
C.3.16 National Security Agency Documentation C-101
C.3.17 U. S. Secure Communication Interoperability Protocol C-102
C.3.18 Telcordia Technologies Documentation C-102
C.3.19 Telecommunications Industry Association C-104
C.3.20 United States Code C-104
C.3.21 Other Documentation C-104

LIST OF FIGURES

FIGURE		PAGE
Figure 1.1-1.	UCR Document Family	1-1
Figure 1.5-1.	UC High Level Operational Framework	1-5
Figure 1.6-1.	DISN Backbone Infrastructure	1-6
Figure 1.7-1.	Operational Construct for UC NetOps	1-7
Figure 1.10-1.	High-Level UC Infrastructure Illustrating the Three Main Network Segments	1-12
Figure 1.10-2.	High-Level Illustration of E2E Network Segments	1-13
Figure 1.10-3.	Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site	1-15
Figure 2.1-1.	Overview of UC Network Attributes	2-2
Figure 2.1-2.	Queuing Design Overview	2-3
Figure 2.1-3.	Attributes of AS-SIP	2-6
Figure 2.1-4.	Assured Services Subsystem Functional Diagram	2-7
Figure 2.1-5.	SBU Voice and Video Services Signaling Design	2-9
Figure 2.1-6.	End-to-End Two-Level SBU AS-SIP Network Signaling Design	2-11
Figure 2.1-7.	Distributed UC Services Model	2-12
Figure 2.2-1.	Enterprise UC Services Architecture	2-15
Figure 2.2-2.	Environment Type 1	2-17
Figure 2.2-3.	Environment Type 2	2-18
Figure 2.2-4.	Environment Type 3	2-19
Figure 2.2-5.	Multivendor Interoperability Normalized on XMPP	2-20
Figure 2.2-6.	Basic Architecture for Providing EDS in the Enterprise UC Network	2-23
Figure 2.3-1.	Mobile Warfighter's Communication Dilemma	2-25
Figure 2.6-1.	Call Forwarding Logic Diagram	2-32
Figure 2.6-2.	Call Hold Scenarios	2-33
Figure 2.7-1.	Framework for Proprietary and AS-SIP EIs	2-40
Figure 2.7-2.	Framework for SCIP Phones Using VoIP	2-43
Figure 2.7-3.	Framework for SCIP Phones Using Modem Relay	2-44
Figure 2.8-1.	Functional Reference Model – SC	2-47
Figure 2.9-1.	AS-SIP TDM Gateway Topologies	2-50
Figure 2.9-2.	Functional Reference Model – AS-SIP TDM Gateway	2-51
Figure 2.9-3.	AS-SIP IP Gateway Topology	2-53
Figure 2.9-4.	Functional Reference Model – AS-SIP IP Gateway	2-54
Figure 2.9-5.	AS-SIP – H.323 Gateway Topology	2-57
Figure 2.9-6.	Functional Reference Model – AS-SIP – H.323 Gateway	2-58

Figure 2.9-7. CCA Relationships 2-60
Figure 2.10-1. Functional Reference Model – SS 2-61
Figure 2.11-1. CCA Relationships With Functional Components 2-66
Figure 2.12-1. MGC – MG Layered Interface 2-74
Figure 2.12-2. MG Trunk Function 2-75
Figure 2.12-3. MG Primary Access Functions and Interfaces 2-76
Figure 2.12-4. Example IP Network Echo Control Design 2-85
Figure 2.12-5. Remote MG Architecture Diagram 2-87
Figure 2.15-1. Network Appliance Management Model 2-94
Figure 2.15-2. Relationship of UC Managements 2-95
Figure 2.16-1. AS-SIP Triggers for AVSC 2-101
Figure 2.16-2. Notional System Architecture for Examples 1, 2, and 4 2-103
Figure 2.16-3. Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel) 2-104
Figure 3.1-1. Regional RAE Hub Topology 3-2
Figure 3.2-1. Hybrid Routing Feature Operation in the Network 3-4
Figure 3.2-2. Commercial Cost Avoidance Feature Operation in the Network 3-5
Figure 4-1. Example of Information Assurance Protocol Usage in the DoD UC Architecture 4-2
Figure 4-2. ASLAN Enclave Boundary Security Design 4-3
Figure 5.2-1. IPv6 Design for SBU and Classified VVoIP 5-3
Figure 6.1-1. Measurement Points for Network Segments 6-1
Figure 6.3-1. F-F E2E Latency 6-5
Figure 6.3-2. CE Segment Outbound Latency 6-6
Figure 6.3-3. CE Segment Inbound Latency 6-7
Figure 6.3-4. F-F AR-to-AR Latency 6-8
Figure 6.3-5. F-F CE Router-to-CE Router Latency 6-9
Figure 6.4-1. E2E F-F Jitter 6-10
Figure 6.4-2. F-F AR-to-AR Jitter 6-11
Figure 6.4-3. F-F CE Router-to-CE Router Network Infrastructure Jitter 6-12
Figure 6.5-1. E2E F-F Packet Loss 6-13
Figure 6.5-2. F-F AR-to-AR One Way Packet Loss 6-14
Figure 6.5-3. F-F CE Router-to-CE Router Network Infrastructure Packet Loss 6-15
Figure 6.6-1. Latency Objectives for Non-Assured Voice 6-16
Figure 6.7-1. E2E Performance Measured from NIC to NIC 6-16
Figure 6.9-1. F-F Network Infrastructure Availability 6-19
Figure 7.3-1. B/P/C/S-Level Voice over IP SC Designs 7-3
Figure 7.4-1. B/P/C/S Video over IP SC Designs 7-6

Figure 7.5-1. B/P/C/S LAN Layers and Relationship to Customer Edge Network Segment 7-8
Figure 7.5-2. LAN Layers 7-9
Figure 7.5-3. Representative B/P/C/S Design and Terminology 7-10
Figure 7.5-4. LAN Requirements Summary 7-11
Figure 7.5-5. Three Categories of LANs Tailored to Mission Needs 7-12
Figure 7.5-6. An Example of a Potential CAN With a Mix of Mission and Non-Mission Critical Users 7-14
Figure 7.8-1. Voice over IP Packet Size 7-20
Figure 7.8-2. Port-Based VLANs 7-24
Figure 7.8-3. ASLAN UPS Power Requirements 7-26
Figure 7.8-4. MPLS Header 7-28
Figure 7.8-5. MPLS Header Stacking 7-29
Figure 7.8-6. MPLS OSI Layer 7-29
Figure 7.8-7. ASLAN MPLS Operational Framework 7-30
Figure 7.8-8. Point-to-Point LAN Interconnection 7-33
Figure 7.8-9. Point-to-Multipoint Interconnection Concentration 7-34
Figure 7.8-10. DSL Repeater Provides Extended Distance 7-35
Figure 7.8-11. Base Configuration Supporting Analog Voice and VoIP Using DSL Modems and a DSLAM 7-36
Figure 8.1-1. Illustration of Multifunction Mobile Device Use Cases 8-3
Figure 8.1-2. UC Multifunction Mobile Device Application Relationship to the Host Platform 8-6
Figure 8.1-3. Options (VPN and B2BUA) for Secure SC Connectivity From a UC Multifunction Mobile Device Application 8-8
Figure 8.1-4. UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection 8-9
Figure 9.4-1. VDS Over IP System 9-5
Figure 10-1. Current DISN Services and Networks Overview 10-1
Figure 10-2. Network Infrastructure Product Arrangements 10-4
Figure 10-3. Conceptual Depiction of 2 Nodes of the DISN 10-5
Figure 10-4. DISN Router Hierarchy 10-6
Figure 10-5. DCA Architecture 10-8
Figure 11-1. Network Element Diagram 11-3
Figure 12.2-1. Sample Network 12-2
Figure 12.2-2. Example HAIPE Application Diagram 12-3
Figure 12.2-3. LEF Application Example 12-6
Figure 12.2-4. SCIP Network Example 1 12-7
Figure 12.2.5. SCIP Network Example 2 12-8

Figure 13.3-1. Notional Example of Voice and Data ASLAN Segmentation 13-3
Figure 15-1. Definitions of End-to-End for Voice, Video, and Data Services 15-1
Figure 15.1-1. DISN OSS Functions 15-2
Figure 15.2-1. Spiral E2E EMS Monitoring of Voice/Video/Data Services 15-4
Figure 15.3-1. GIG E2E DISN UC Services Management Approach 15-5
Figure 15.3-2. DISN UC E2E Solution for UC Spirals 15-6
Figure A.4-3. OAN Tier Structure A-3
Figure A.5-1. Army Enterprise Network A-7
Figure A.7-1. Hierarchical Connectivity in UC A-11
Figure A.8-1. Notional View of Tactical Region Mesh Connectivity A-13
Figure A.9-1. Outbound Traffic Flow in Tactical ASLAN A-14
Figure A.9-2. 2G Cellular Primary Components A-19
Figure A.9-3. 3G Cellular Primary Components A-19
Figure A.9-4. 4G Cellular Primary Components A-20
Figure A.9-5. UC Operational Framework A-21
Figure A.10-1. DCVX Connection Options A-24
Figure A.10-2. Radio Gateway Components A-28
Figure A.10-3. Radio Gateway Interfaces A-29
Figure B-1. DISN CVVoIP Hybrid Signaling Design B-1
Figure C.1-1. Difference Between Outside Plant Loss and the Span Loss C-18
Figure C.1-2. Network Element Diagram C-32

LIST OF TABLES

TABLE **PAGE**

Table 2.8-1. Summary of SC Functions 2-48
Table 2.8-2. SC Support for VoIP and Video Signaling Interfaces 2-49
Table 2.9-1. AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces .. 2-51
Table 2.9-2. Summary of AS-SIP IP Gateway Functions 2-55
Table 2.9-3. Summary of AS-SIP – H.323 Gateway Functions 2-58
Table 2.10-1. SS Support for VoIP and Video Signaling Interfaces 2-63
Table 2.12-1. SC MG Support for VoIP Signaling Interfaces 2-78
Table 2.12-2. SS MG Support for VoIP Signaling Interfaces 2-79
Table 2.12-3. Protocol Stack 2-88
Table 2.14-1. DSN User Dialing Format 2-88

Table 2.14-2. Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers 2-90
Table 2.14-3. Mapping of DSN tel Numbers to SIP URIs 2-92
Table 2.14-4. White Pages Directory Data Elements 2-94
Table 2.16-1. EISC Estimation Parameters 2-99
Table 2.16-2. Example 1: Current Session Status (No HAIPE Case) 2-105
Table 2.16-3. Example 2: AVSC Calculation Assuming the G.711 Session Is New (HAIPE Case) 2-105
Table 2.16-4. Example 3: Use of Voice MUX With a HAIPE Tunnel 2-106
Table 2.16-5. Example 4: Use of Header Compression With a HAIPE Tunnel 2-107
Table 6.8-1. Service Level Class Specification 6-17
Table 6.10-1. DISN Four-Queue Bandwidth Provisioning Model 6-23
Table 6.10-2. DISN Six-Queue Bandwidth Provisioning Model 6-23
Table 7.5-1. OSI Layer Control Information Name 7-10
Table 7.5-2. LAN Requirements Summary 7-13
Table 7.8-1. Cable Grade Capabilities 7-19
Table 7.8-2. LAN VoIP Subscribers for IPv4 and IPv6 7-21
Table 7.8-3. Video Rates and IP Overhead 7-22
Table 7.8-4. Video over IP Bandwidth 7-23
Table 7.8-5. Methods of Expressing Availability 7-27
Table 7.8-6. ITU DSL Standards Overview 7-31
Table 7.8-7. DSL Bonding Standards 7-32
Table 8-1. Multifunction Mobile Devices 8-2
Table 8.1-1. Multifunction Mobile Device Use Cases 8-2
Table 12.4-1. Network Management Test Criteria 12-14
Table 12.4-2. Software Download Test Criteria 12-15
Table 12.4-3. Degrated Network Capability and Robustness Criteria 12-15
Table 12.4-4. Control Signal Requirements Matrix 12-16
Table 12.4-5. Interface Requirement Matrix 12-17
Table 14-1. DSC Data Storage and Service Types 14-1

SECTION 1
INTRODUCTION AND UC DESIGN OVERVIEW

1.1 PURPOSE

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

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

- The UCR 2013 specifies the functional requirements, performance objectives, and technical specifications for products that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may be used also for UC product assessments and/or operational tests for emerging UC technology. The Defense Information Systems Agency (DISA) translates DoD Component functional requirements into engineering specifications for inclusion into the UCR, which identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR also defines interoperability, Information Assurance (IA), and interface requirements among products that provide UC.
- The Assured Services Session Initiation Protocol (AS-SIP) 2013 contains requirements for the Internet protocol (IP)-based UC Signaling system.
- The UC Extensible Messaging and Presence Protocol (XMPP) 2013 contains requirements for multivendor interoperability as required to exploit the full potential of Instant Messaging (IM), Chat, and Presence across the DoD.
- UC Framework 2013 – specifies the descriptive text and design associated with each of the UCR 2013 sections.

Figure 1.1-1. UCR Document Family

1.2 APPLICABILITY AND SCOPE

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

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

1.3 DOCUMENT OVERVIEW

The UC Framework consists of the following sections:

- Section 1, Introduction and UC Design Overview, describes the purpose, applicability, and scope for the UC Framework. A short synopsis of UC network infrastructure is also included.
- Section 2, Session Control Products, describes the UC network infrastructure in terms of network engineering attributes, and designs.
- Section 3, Auxiliary Services, describes miscellaneous features and interfaces to the UC network.
- Section 4, Information Assurance, provides an overview of IA requirements.
- Section 5, IPv6, summarizes requirements for IPv6 implementation.
- Section 6, Network Infrastructure End-to-End Performance, describes latency, jitter, and packet loss performance parameters required by the network segments to meet requirements for the Defense Information Systems Network (DISN) service classes.
- Section 7, Network Edge Infrastructure, describes designs for the Customer Edge network segment.
- Section 8, Multifunction Mobile Devices, describes arrangements for supporting mobile devices.
- Section 9, Video Distribution System, describes designs for H.320, H.323, and AS-SIP-based Video Teleconferencing (VTC) systems.
- Section 10, Network Infrastructure Products, describes current DISN Services and arrangement of products in the network infrastructure.

- Section 11, Network Elements, describe requirements and application of various network elements.
- Section 12, Generic Security Devices, provides a synopsis of encryption devices.
- Section 13, Security Devices, provides a synopsis of security devices.
- Section 14, Online Storage Controller, describes requirements for this product type.
- Section 15, Enterprise and Network Management Systems, describes element management systems and operational support systems used to manage the DISN.
- Appendix A, Unique Deployed (Tactical), provides a synopsis of tactical requirements.
- Appendix B, Unique Classified Unified Capability, provides a synopsis of the Classified network environment.
- Appendix C, Definitions, Abbreviations and Acronyms, and References.

1.4 NETWORK SUPPORT FOR UC SERVICES

Unified Capabilities are the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities.

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

- Voice and Video Services Point-to-Point. Provides for two voice and/or video users to be connected End Instrument (EI)-to-EI with services that can include capabilities such as voicemail, call forwarding, call transfer, call waiting, operator assistance, and local directory services.
- Voice Conferencing. Provides for multiple voice users to conduct a collaboration session.
- Video Teleconferencing (VTC). Provides for multiple video users to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.
- Email/Calendaring. Provides for users to send messages to one or many recipients with features such as priority marking, reports on delivery status and delivery receipts, digital signatures, and encryption. Calendaring allows the scheduling of appointments with one or many desired attendees.
- Unified Messaging. Provides access to voicemail via email or access to email via voicemail.
- Web Conferencing and Web Collaboration. Provides for multiple users to collaborate with voice, video, and data services simultaneously using web page type displays and features.

- Unified Conferencing. Provides for multiple users to collaborate with voice, web, or videoconferencing integrated into a single, consolidated solution often as a collaboration application.
- Instant Messaging (IM) and Chat. Provides real-time interaction among two or more users who must collaborate to accomplish their responsibilities using messages to interact when they are jointly present on the network. For IM, presence is displayed:
  - Instant messaging provides the capability for users to exchange one-to-one ad hoc text message over a network in real time. This is different and not to be confused with signal or equipment messaging, in that IM is always user generated and user initiated.
  - Chat provides the capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from IM by being focused on group chat or room-based chat. Typically, room persistence is a key feature of multiuser chat, in contrast with typically ad hoc IM capabilities.
  - Presence/Awareness is a status indicator that conveys ability and willingness of a potential user to communicate.
- Rich-Presence Services. Allows contact to be achieved to individuals based on their availability as displayed by presence information from multiple sources, including IM, telephone, and mobile devices.
- Mobility. Provides the ability to offer wireless and wired access, and applies to voice, e mail, and many other communication applications. It includes devices such as personal digital assistants (PDAs) and Smartphones. In addition, it provides for users who move to gain access to enterprise services at multiple locations (e.g., your telephone number and desktop follow you). Wireless includes communication between devices that are not physically connected, and it includes but is not necessarily limited to wireless broadband access (e.g., WiFi), cellular (e.g., LTE), satellite communications, line of sight ratio, push-to-talk broadcast radio services, telemetry services, telecommand services, and wireless machine-to-machine (M2M) services.

1.5 UC OPERATIONAL FRAMEWORK OVERVIEW AND SUMMARY

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

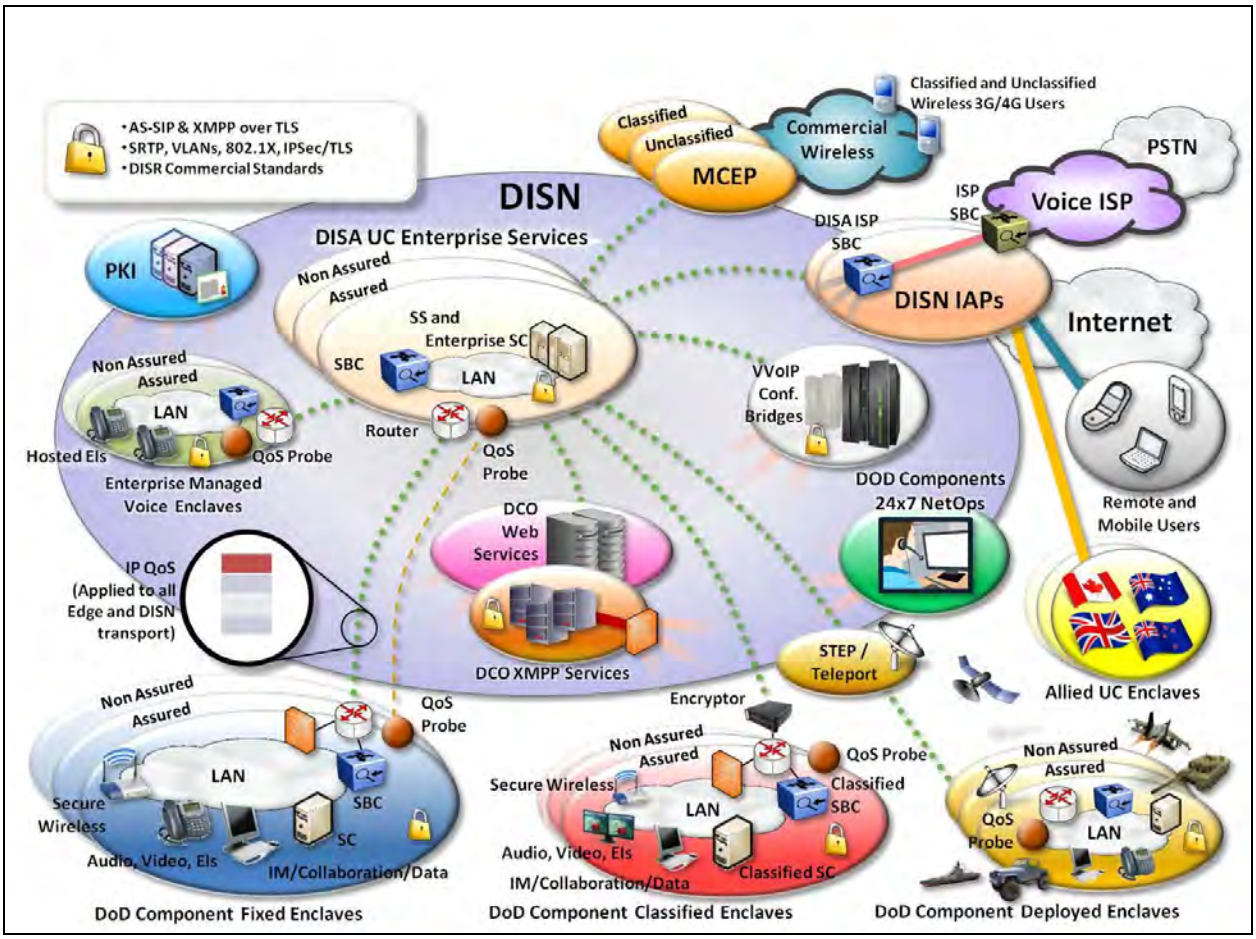

Figure 1.5-1. UC High Level Operational Framework

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

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

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

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

1.6 HIGH LEVEL OPERATIONAL CONCEPT

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

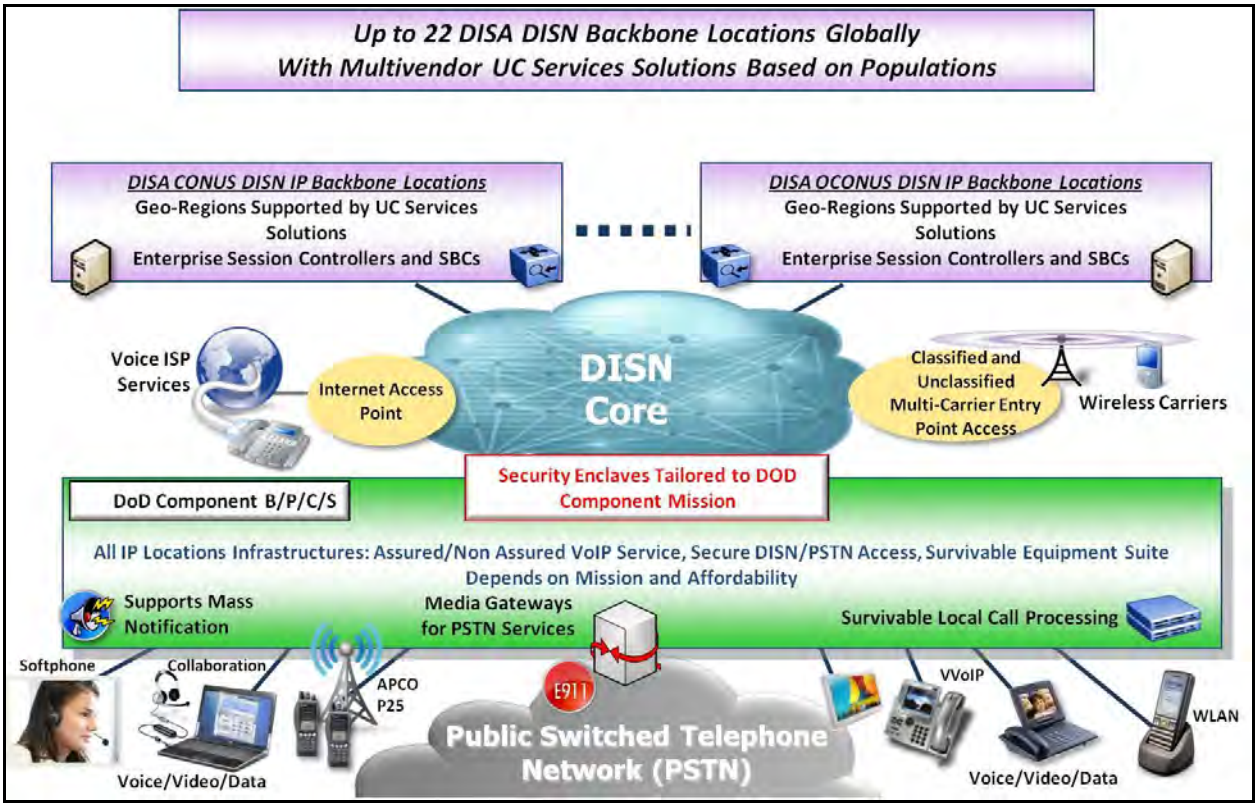

Figure 1.6-1. DISN Backbone Infrastructure

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

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

1.7 OPERATIONAL CONSTRUCT FOR UC NETOPS

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

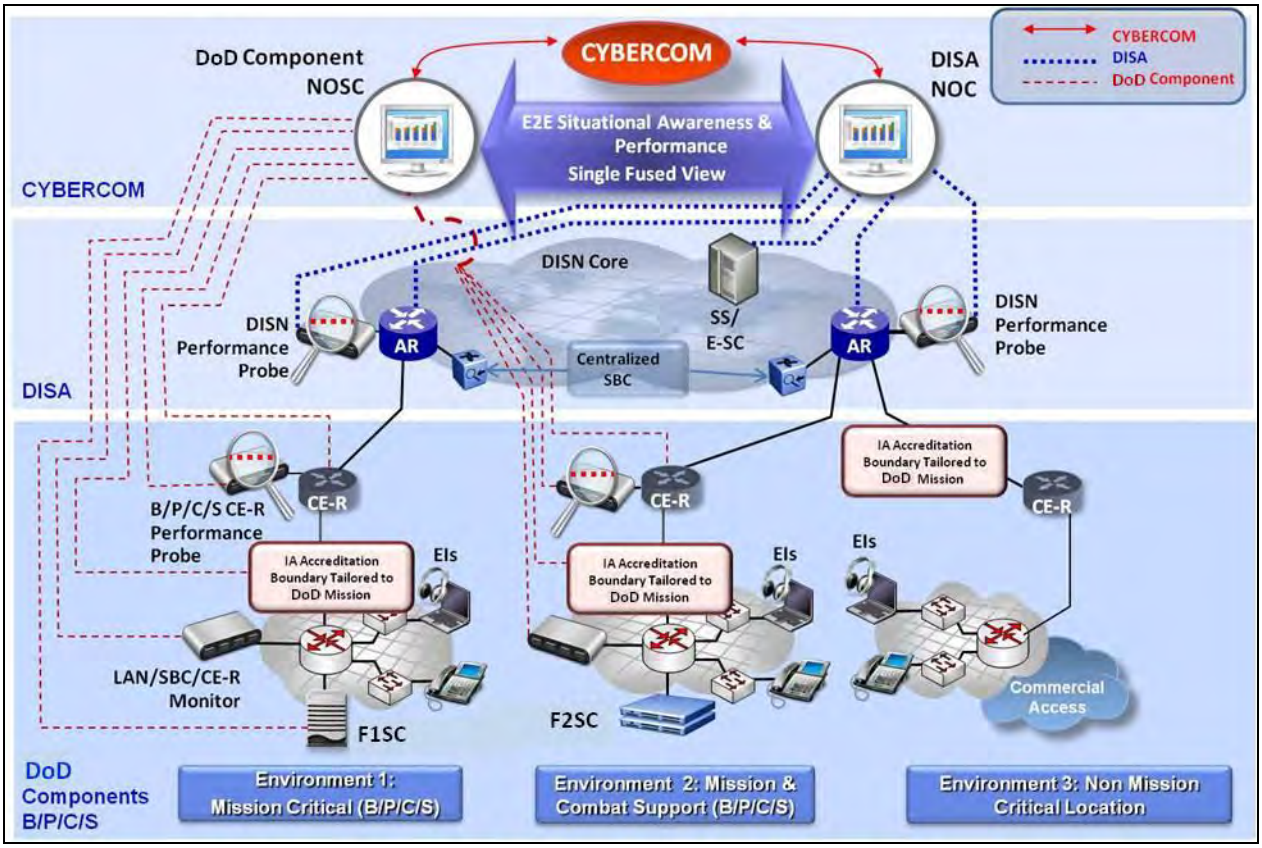

Figure 1.7-1. Operational Construct for UC NetOps

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

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

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

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

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

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

1.8 UC IMPLEMENTATION PRIORITY AND SCHEDULE

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

1. Non-Assured/Assured Voice, Video, and Data Session Management. Provides enterprise point-to-point UC, independent of the technology (circuit switched or IP). Capabilities include, but are not limited to, end device registration, session establishment and termination, and UC session features (e.g., Assured Services Admission Control, Call Hold, Call Transfer).
2. Non-Assured/Assured Voice and Video Conferencing. Provides the ability to conference multiple voice or video subscribers with a variety of room controls for displays of the participants. It also includes an optional component that allows subscribers to schedule conferences.
3. Collaboration. Provides IP-based solutions that allow subscribers to collaborate (e.g., IM, chat, presence, and Web conferencing).
4. User Mobility (wired and wireless). Provides the ability to offer wireless and wired access, for UC supported by multifunction mobile devices. In addition, it provides access to enterprise UC globally using UC portability.

5. Voice Internet Service Provider (ISP) Access. Provides unclassified and classified enterprise UC for access to commercial voice services over IP. This service provides both local and long distance dialing capability using commercial ISPs via secure interconnections.
6. Unified Messaging. Provides the integration of voicemail and email. The integration of these two capabilities allows subscribers to access voicemail via email or access email via voicemail.
7. UC Portability and Identity Synchronization. Provides an enterprise UC systematic approach to portability functions (e.g., repository of user profiles and privileges, and subscriber identification and authentication). Uses DISA's existing Identification (ID) Synchronization service as the primary service for DoD ID Synchronization.
8. Enterprise Directory Integration. Integrates UC with repository of subscriber contact information accessible to all authorized and authenticated subscribers.
9. UC Applications Integration. Supports mission and business applications integration with the enterprise UC (e.g., integration of UC provided presence with DoD Component-owned business applications).

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

1.9 ASSURED SERVICES DESIGN CRITERIA

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

ASFs must be provided by UC networks based on the mission of the users consistent with their roles in peacetime, crisis, and war. There are users who need the full range of assured services, those that only need limited assured services, and those that need non-assured services. Even if requirements for assured services do not apply to all users at a site, the Assured Information Protection features cannot be degraded.

In the operation of networks that provide UC services, the DoD Components shall comply with ASFs requirements, (i.e., Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery) as described below

1. Assured System and Network Availability. This design requirement is achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, failover, diversity, and elimination of critical failure points. This ASF supports mission-critical traffic during peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed. The following objectives contribute to the survivability of the UC:

a. No single point of vulnerability for the entire network, to include the NM facilities; no single point of vulnerability within a COCOM-defined geographic region of the COCOM's Theater.

b. No more than 15 percent of the B/P/C/S within a COCOM-defined geographic region of the COCOM's Theater can be affected by an outage in the network.

c. Networks robustness through maximum use of alternative routing, redundancy, and backup.

d. To the maximum extent possible, transport supporting major installations (i.e., B/P/C/S, leased or commercial sites or locations) will use physically diverse routes.

e. The National Military Command Center (NMCC) (and Alternate), COCOMs, or DoD Component headquarters will not be isolated longer than 30 minutes because of an outage in the backbone (long-haul or UC Transport) portion of the network.

2. Assured Information Protection. This design requirement applies to information in storage, at rest, and passing over networks, from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers:

   a. Secure End Instruments (SEIs) shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication.

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

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

3. Assured Information Delivery. This design requirement specifies that DoD networks providing UC services have the ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war:

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

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

mission-critical sessions shall be determined by the Joint Staff (JS) and COCOMs. All users shall be capable of receiving precedence UC services sessions, since locations of crises and wars cannot be determined in advance.

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

d. Precedence-based sessions placed to EIs that are busy with lower precedence-based sessions shall be absolutely assured completion to a live person. This shall be accomplished by immediate disconnection of the lower precedence session and immediate completion of the higher precedence session.

e. Visibility and Rapid Reconfiguration. If blocking occurs to users' sessions caused by crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to situational awareness (SA) to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock NOCs that oversee voice, video, and data services. DISA shall oversee the DISN systems and shall have read-write access to DISN systems, which are shared with the military services for cost avoidance, such as the Softswitch (SS). All NOCs shall have Element Management Systems (EMSs) that allow for read-write access for the systems for which they have direct responsibility. In addition, the USCYBERCOM-sponsored NetOps Community of Interest (COI) metadata standards and information sharing capabilities shall be used by all NOCs to share alarms, performance data, and trouble tickets. Information sharing and NOSCs shall enable end-to-end visibility and the configuration of network components, as needed to respond to SA. All actions shall be coordinated with affected DoD Components before such actions are taken, if possible, consistent with the "Operational Tempo," and after such actions are taken.

f. Prevention of blocking of precedence sessions that occur during short-term traffic surges shall be accomplished via PBAS.

g. During times of surge or crisis, the Chairman of the Joint Chiefs of Staff (CJCS) can direct implementation of session controls to allocate the use of resources in the network to meet mission needs.

h. The global and Theater networks must be able to support a regional crisis in one Theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another Theater.

i. Unified Capabilities networks shall be designed with the capability to permit interconnection and interoperation with similar Services' Deployable programs, U.S. Government, Allied, and commercial networks. All hardware and software in the network must be certified as interoperable.

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

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

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

1.10 UC NETWORK INFRASTRUCTURE OVERVIEW

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

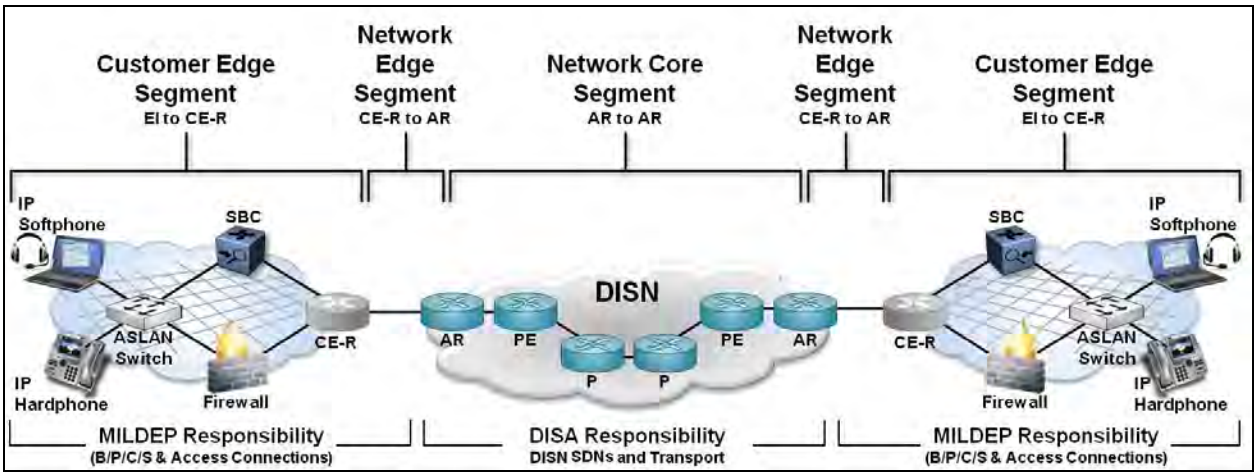

Figure 1.10-1. High-Level UC Infrastructure Illustrating the Three Main Network Segments

1.10.1 IP-Based CE Segment

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

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

1.10.2 Network Edge Segment

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

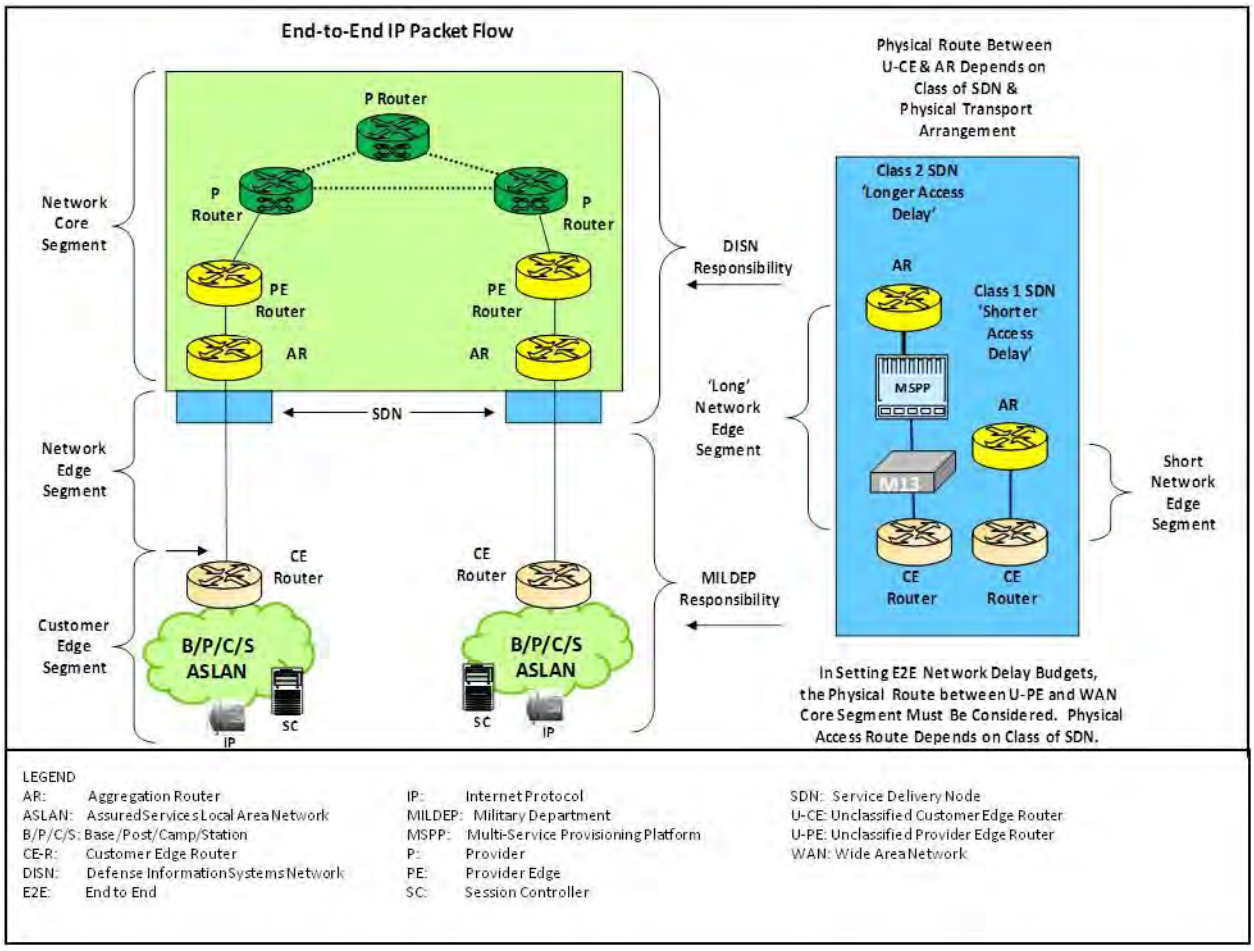

Figure 1.10-2. High-Level Illustration of E2E Network Segments

1.10.3 DISN Service Delivery Nodes

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

- M13, an APL product performing multiplexing and de-multiplexing functions of T1 and T3 carriers.
- Multi-Service Provisioning Platform (MSPP), a network device that may provide multiple network functions such as Routing, Switching, IDS, or Firewall.
- Provider (P) router.
- Provider Edge (PE) Router.
- AR.

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

1. Class 1 SDN. Type of SDN that has a short network segment, often categorized by the CE-R being collocated with the AR and has a shorter access and serialization delay.
2. Class 2 SDN. Type of SDN that has a longer network segment, often categorized by the CE-R not being collocated with the AR, has intervening network devices and connections, and has a longer access and serialization delay.

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

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

- Type of SDN:
  - Non-Robust: M13 multiplexer.
  - Robust: MSPP without AR all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning).
  - Robust: MSPP with Unclassified AR (U-AR).

- U-CE Router Location for the SDN:
  - U-CE Router not at an SDN location.
  - U-CE Router at a non-robust SDN location.
  - U-CE Router at a robust SDN location.
- Type of U-CE Router:
  - Critical mission.
  - Noncritical mission.

As shown in Figure 1.10-3, Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site, a noncritical mission U-CE Router may connect to the nearest SDN regardless of the type of SDN, while a critical mission U-CE Router must be dual homed to two separate robust types of SDNs.

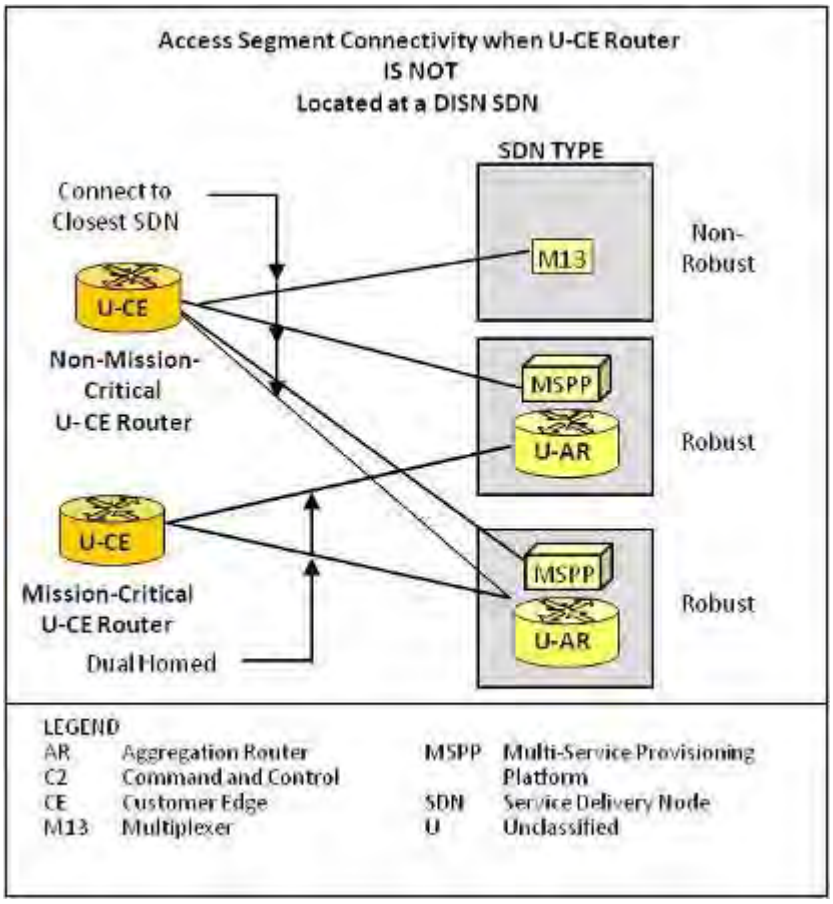

Figure 1.10-3. Network Edge Segment Connectivity When U-CE Router Is Not Located at SDN Site

If a critical mission U-CE Router is located on the same base as an SDN, it still requires a second connection to another robust SDN.

1.10.4 Network Core Segment

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

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

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

SECTION 2
SESSION CONTROL PRODUCTS

2.1 NETWORK ENGINEERING ATTRIBUTES

The logical location of the major Unified Capabilities (UC) network attributes within the UC End-to-End (E2E) design is shown in Figure 2.1-1, Overview of UC Network Attributes. The location of attributes in terms of the Customer Edge (Base/Post/Camp/Station [B/P/C/S]), the Network Edge (Access) and the Network Core are depicted.

The functions contained in the boxes of Figure 2.1-1 constitute the scope of the Assured Services functions while the placement of the boxes indicates where in the overall design (Wide Area Network [WAN] to Edge) the functions logically reside. Voice, video, and data sessions are converged in the Defense Information Systems Network (DISN) WAN and the Assured Services (AS) Local Area Network (LAN) (ASLAN), while currently only voice and video sessions are supported by Assured Services.

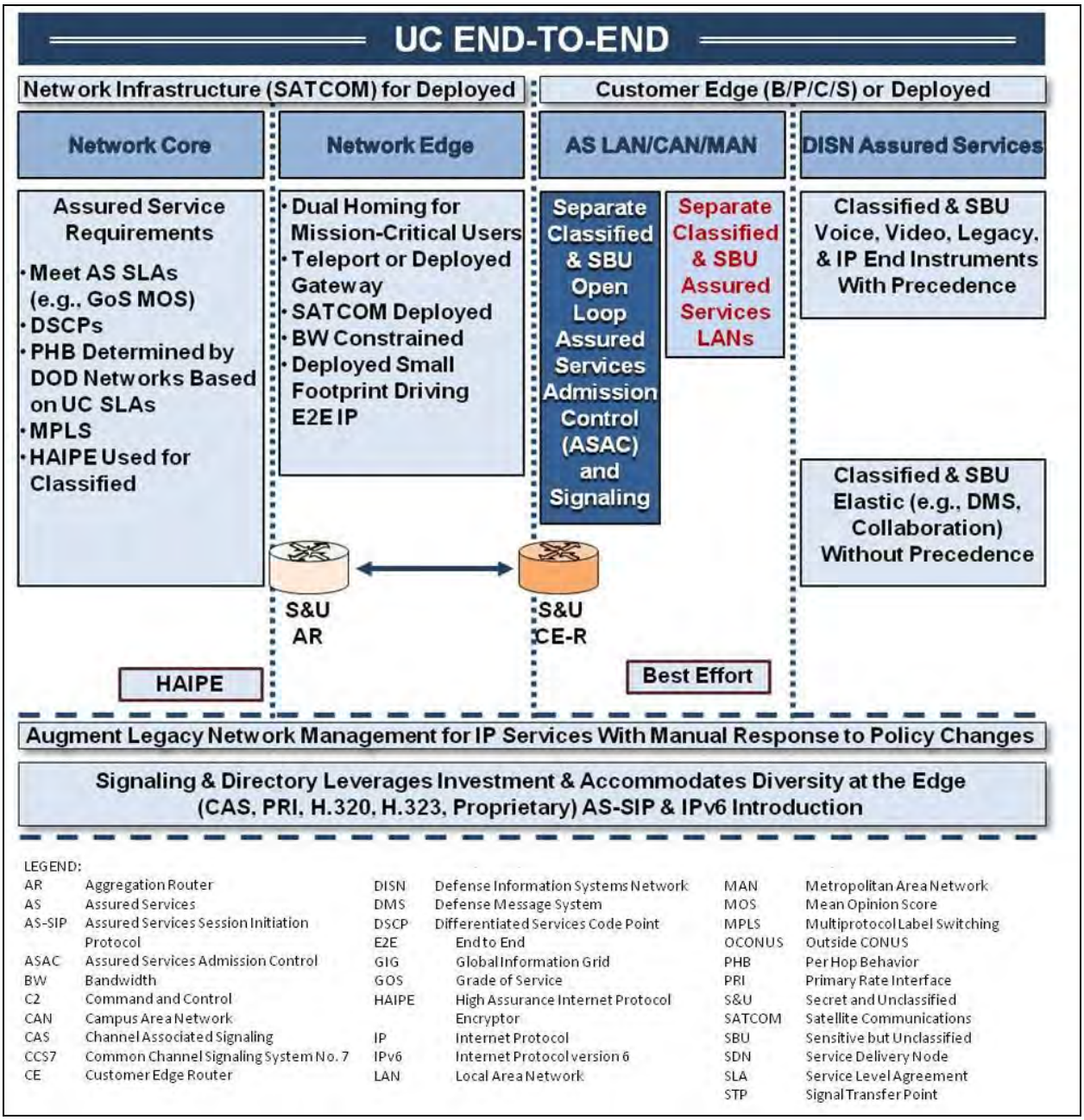

Figure 2.1-1. Overview of UC Network Attributes

2.1.1 Quality of Service Features

Quality of Service (QoS) features are implemented within the DISN to provide different priority to the DISN UC Service Classes. The various DISN UC Service classes have different network bandwidth needs and use different transmission protocols to send their data. When these different types of data converge, and are sent on a shared link, one transmission can overwhelm another, resulting in a negative effect. The required QoS for each UC Aggregate Service Class is

maintained by assigning Differentiated Services Code Points (DSCPs) to each DISN UC Service class and then assign the service classes into different queues.

There are four Aggregated Service Classes which in turn, are refined into 13 Granular Service Classes.

Each of the 13 Granular DISN UC Service Classes is mapped into a 6-queue structure or four-queue structure as described in Unified Capabilities Requirements (UCR) 2013, Section 6, Network Infrastructure End-to-End Performance. An example of the four-queue mapping is illustrated in Figure 2.1-2. Assured Voice, User Signaling, and Network Control Traffic are placed in the Expedited Forwarding (EF) queue. Assured Multimedia Conferencing (i.e., Video) traffic is placed in the Class 4 Assured Forwarding (AF4) queue. Preferred data, non-assured Voice and Video over Internet protocol (IP) (VVoIP); instant messaging (IM), Chat, and Presence; and Operations, Administration, and Maintenance (OA&M) traffic is placed in the Class 3 Assured Forwarding (AF3) queue. All other traffic (data and any other service) are placed in the Best Effort (Default) queue.

NOTE: User Signaling associated with non-assured Voice and Video over Internet Protocol (VVoIP) is placed in the EF queue. Figure 2.1-2 shows the queue structure, DSCPs, and associated rules for each granular service class.

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

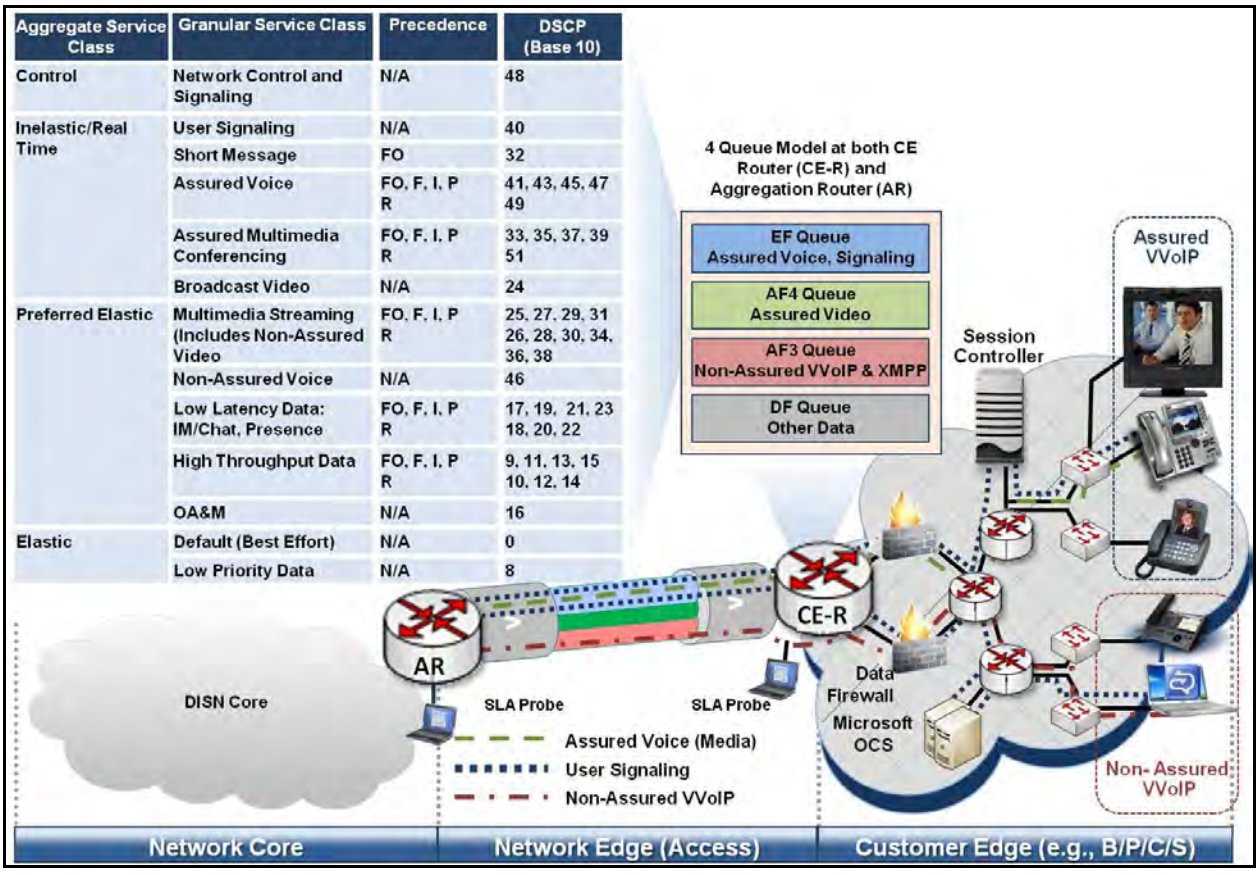

Figure 2.1-2. Queuing Design Overview

To ensure acceptable QoS in IP networks for assured VVoIP, it is necessary to assign the assured VVoIP traffic to different queues than non-assured VVoIP and data sessions on congested connections. Mixing assured VVoIP with non-assured VVoIP in the same aggregate service class (and queue) will result in the uncontrolled non-assured VVoIP degrading the assured VVoIP sessions on congested networks. To delineate the assured VVoIP from the non-assured VVoIP (and other types of packets), Internet protocol (IP) packets are marked with unique DSCPs.

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

Assured VVoIP traffic is subject to Session Admission Control (SAC). SAC policies control the number of sessions that are offered to the network. Session admission control can be provided by Session Controllers (SCs) or Gatekeepers (i.e., H.323 Gatekeepers) and is associated with establishing a budget for the number of simultaneous sessions and with ensuring that the number of active sessions is within that budget. Assured Services Admission Control (ASAC) extends SAC to allow sessions to be preempted when the SAC budget is at capacity and additional higher precedence sessions are offered.

SAC is not applied to non-assured VVoIP. Non-assured VVoIP typically is composed of peer-to-peer sessions that do not transit a centralized SAC appliance, (e.g., SC); therefore, SAC cannot be applied.

In addition to queuing, traffic conditioning is applied to the non-assured VVoIP packets. Enabling traffic conditioning on non-assured VVoIP packets may cause degradation on non-assured VVoIP sessions during periods of high usage, but will ensure that preferred data sessions continue to receive better than best effort performance in accordance with (IAW) the UCR performance objectives.

The bandwidth for each queue must be provided based on a sound traffic-engineering analysis, which includes the site budget settings, the site busy hour traffic load plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, Network Management (NM), and routing traffic.

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

2.1.2 Assured Services Features and Capabilities

A key component of the military robust VoIP and Video over IP design is the Assured Services subsystem. The Assured Services subsystem addresses Assured Services by replacing the current Time Division Multiplexing (TDM)-based Multilevel Precedence and Preemption (MLPP) functionality with IP-based ASLANs and ASAC. The Assured Services subsystem, in conjunction with the ASLAN subsystem, and the DISN WAN subsystem make up the total product that is required to initiate, supervise, and terminate voice and video, precedence and

preemption sessions on an End Instrument (EI)-to-EI basis, while functioning within a converged Department of Defense (DoD) UC network.

2.1.2.1 Attributes Within the Edge Segment

The attributes within the Edge Segment include the following:

1. Nonblocking ASLAN. At the Edge, the design has an ASLAN that is designed as nonblocking for voice and video traffic.
2. Traffic Admission Control. The SCs on a B/P/C/S use an Open Loop ASAC technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit, consistent with maintaining a voice quality of 4.0 as measured by the Mean Opinion Score (MOS) method.
3. Call Preemption. Lower precedence sessions will be preempted on the access circuit to accept the SC setup of higher precedence level outgoing or incoming session establishment requests.
4. Voice and Video Traffic Service Classification and Priority Queues. In terms of the Customer Edge (CE) Router (CE-R) queuing structure, voice and video traffic will be assigned to the higher priority queues by Aggregated Service Class as described in Section 2.1.1, Quality of Service Features.

2.1.2.2 Attributes Within the DISN WAN (Access/Distribution and Core)

Under the access part of the DISN WAN, dual homing is required between the CE-R and the Aggregation Router (AR) that serve an ASLAN having FLASH/FLASH OVERRIDE (F/FO) users, IMMEDIATE (I)/PRIORITY (P) users, and ROUTINE (R) users. Dual homing is optional for cases where only ROUTINE users (I/P [OUTINE] and non-I/P users) are supported. The DISN Core part of the DISN WAN (i.e., from AR to AR) is assumed to be bandwidth rich for whatever AR queue the voice and video traffic is placed in. That is, the core bandwidth for assured voice and video traffic will match or exceed the expected bandwidth required for the voice/video busy-hour traffic in each of the DISN worldwide geographic locations. Since the ASLAN is required to be implemented as non-blocking for voice and video traffic, the access circuit from the Customer Edge Segment to the DISN Core Service Delivery Node (SDN) is the only potential bandwidth-limited resource requiring the use of ASAC to prevent session overload from the Edge Segment. The DISN WAN provides high availability (99.96 percent or greater) using dual-homed access circuits and the Multiprotocol Label Switching (MPLS) fast reroute (FRR) in the Network Core. Naturally, users are provided a lower availability if they choose not to or cannot implement dual homing.

2.1.2.3 E2E Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions or protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes.

The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and RSVP. Figure 2.1-3, Attributes of AS-SIP, illustrates the basic attributes of AS-SIP, which are critical to assured services, multivendor interoperability, and security.

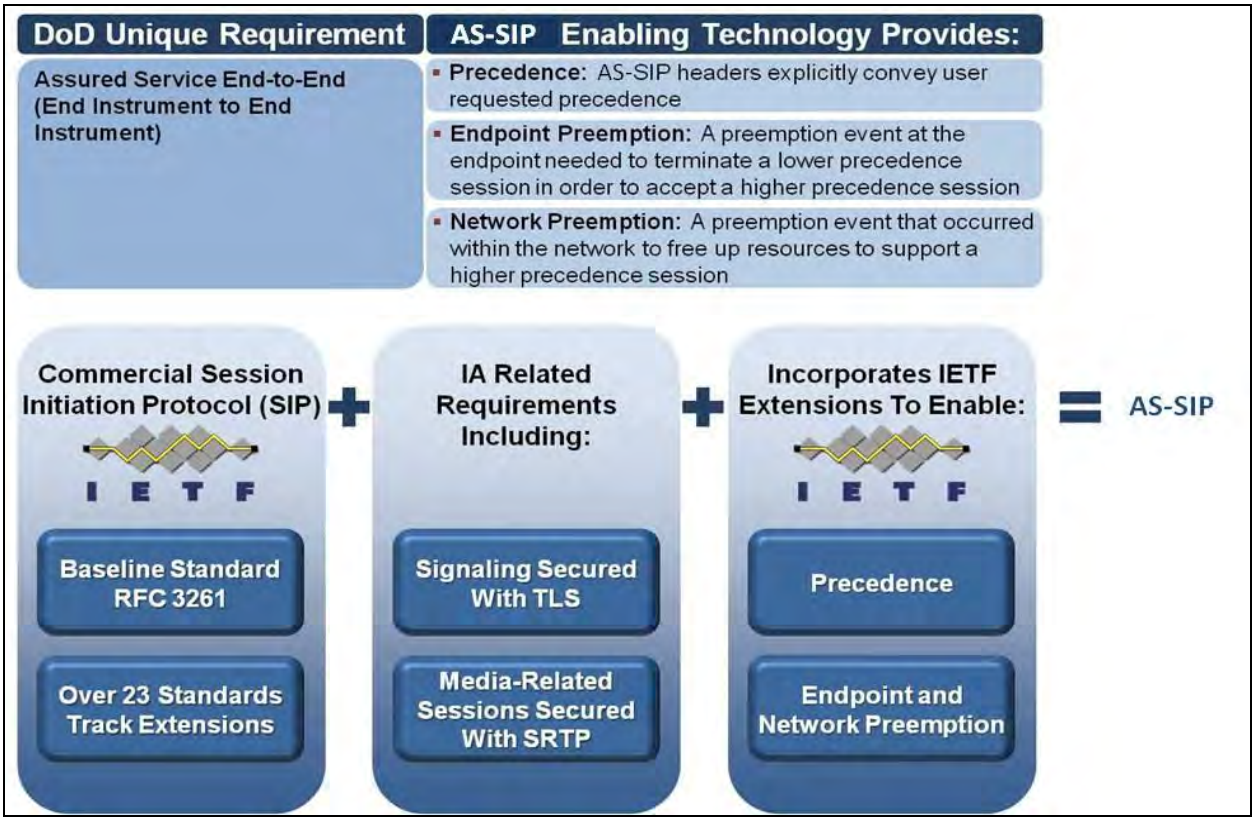

Figure 2.1-3. Attributes of AS-SIP

The transport plane is associated with the bearer traffic and protocols, such as Secure Real-Time Transport Protocol (SRTP) and Real-Time Transport Control Protocol (RTCP).

The NM plane is associated with NM protocols and is used to transfer status and configuration information between a Network Management System (NMS) and a network appliance. Network management protocols include Simple Network Management Protocol (SNMP), Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

2.1.2.4 Assured Services Subsystem

The Assured Services subsystem, shown in Figure 2.1-4, Assured Services Subsystem Functional Diagram, the DISN WAN, and the ASLAN make up the total system. These components are

required to initiate, supervise, and terminate voice and video, precedence and preemption sessions on an EI-to-EI basis, while functioning within a converged DoD network.

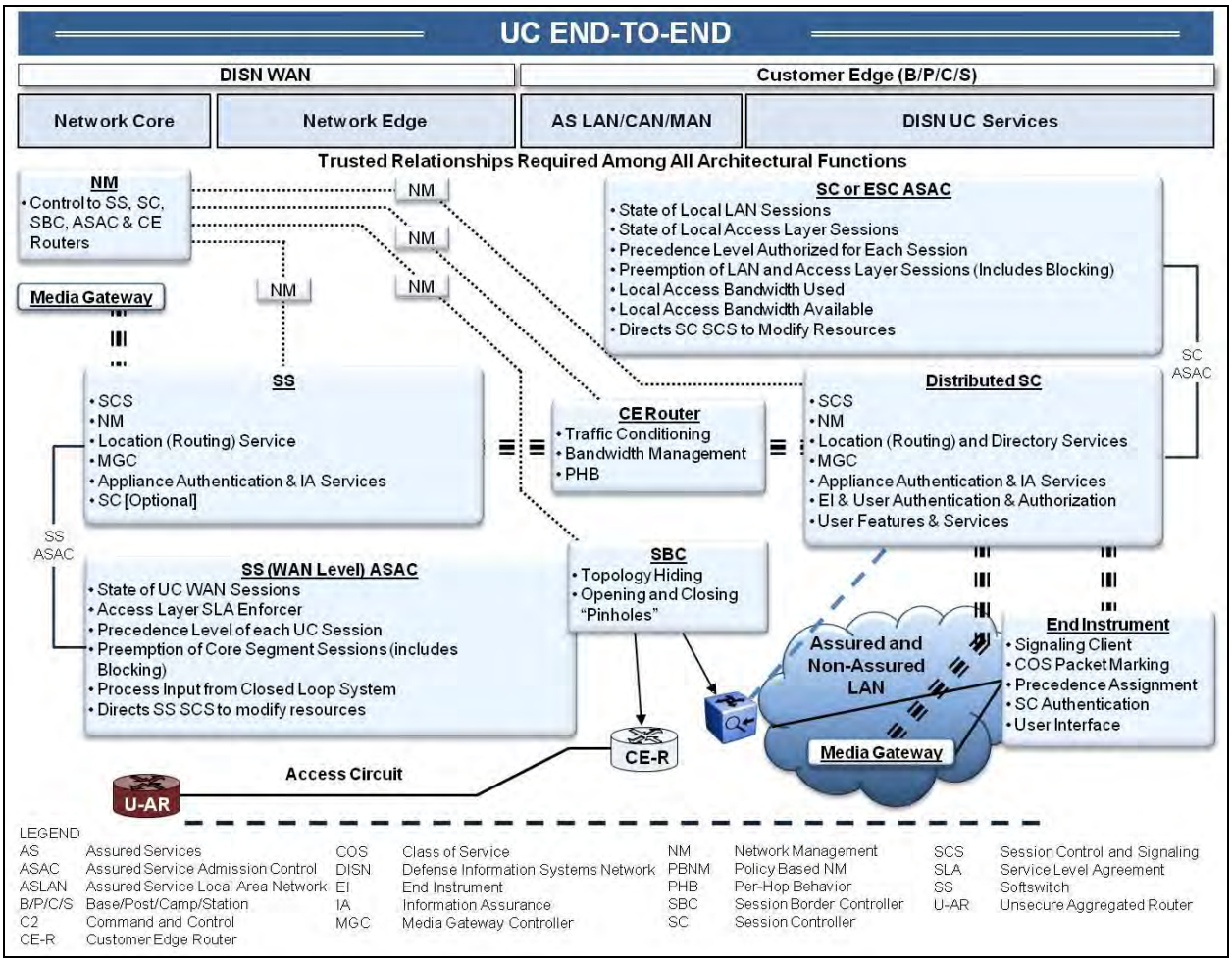

Figure 2.1-4. Assured Services Subsystem Functional Diagram

The functions contained in the Figure 2.1-4 boxes and the SBC router symbol constitute the scope of the Assured Services subsystem, while the placement of the boxes indicates where in the overall system (WAN to Edge) the functions logically reside.

Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while assured services are provided for voice and video sessions only.

The functional behavior and performance metrics for each of the assured services major functions defined by a box in Figure 2.1-4 and subordinate functions listed within each box are specified in this section. In addition, the interfaces between the major functional groupings (defined by a box) are specified in terms of electrical interfaces, protocols operating over these electrical interfaces, and their associated parameters. Best commercial practices and existing standards are specified to the maximum extent possible, and any deviations or enhancements to these are specified in detail within UCR 2013.

The ASAC technique is the key design component ensuring that E2E Service-Level Agreements (SLAs) (grade of service [GOS]), voice/video quality, assured service delivery, and session preemption to the EI] are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements (NEs) end-to-end as illustrated in Figure 2.1-4, Assured Services Subsystem Functional Diagram. The ASAC functions identified for the SC are also employed in the Enterprise SC. Deployable VoIP products may connect via compressed satellite circuits to the DISN backbone and operate in a similar manner to Fixed products on the LAN.

In the access circuit and the ASLAN, AS-SIP signaling is used by the SC and SS to establish or preempt voice and video sessions based on precedence and engineered traffic levels on the access circuits (both origination and destination ends). In the bearer plane, the QoS/DSCP manages router Per-Hop Behavior (PHB) based on the type of service class. Both the ASLAN and the backbone are assumed to be traffic engineered to be nonblocking for voice and video traffic. In the DISN Core, the DISN SLAs will support voice and video with assured services provided by QoS/DSCP, traffic engineering, and MPLS. Traffic with no marking will be treated as Best Effort.

The SC manages a budget for sessions determined by the voice and video traffic-engineered bandwidth of the associated access infrastructure. The Resource-Priority header portion of the AS-SIP signaling message conveys the precedence of the desired session establishment to the destination end SC. Both the originating and destination SCs independently manage their session budgets, so that sessions are permitted or established by precedence until the budget limit is reached. Then a new session can be allowed only if a lower precedence session is available to preempt. At the originating end after preemption has taken place, if necessary, the origination request is sent to the destination upon which, after preemption has taken place, if necessary, the request acceptance is returned to the originating SC. If the originating SC is at its budget limit and has no lower precedence session to preempt, then a blocked session indication, in the form of a Blocked Precedence Announcement (BPA), will be sent to the originating EI. If the terminating SC is at its budget limit and has no lower precedence session to preempt, then a Session Request Denied message will be returned to the originating SC, which, in turn, will send a BPA to the EI. For ROUTINE precedence calls reaching the maximum budget limit, “fast busy” (120 impulses per minute [ipm]) will be sent to the originating EI. All AS-SIP users will come under ASAC. Some H.323 video users on a base may choose to use a separate H.323 Gatekeeper and not come under ASAC. Data traffic (non-voice and video) does not have any ASAC and is handled as Best Effort or preferred data, if the data application implements DSCP packet marking.

Session control processing to establish, maintain, and terminate sessions is performed by the Call Connection Agent (CCA) part of the SC and SS. Signaling is performed by the Signaling Gateway (SG) (used for Circuit Switched T1.619a/AS-SIP signaling conversion), the Media Gateway (MG) (for EI IP signaling to Commercial Primary Rate Interface [PRI] signaling), and as part of the AS-SIP signaling appliance part of the SC and SS depending on requirements for a

particular session. Local subscriber directories are stored in the SCs and network-level worldwide routing tables and addressing and numbering plans are stored in the SS.

2.1.3 Voice and Video Signaling Design

The voice/video signaling design for SBU voice and video is shown in Figure 2.1-5, SBU Voice/Video Services Signaling Design. Currently, the classified voice and video services employ H.323, and will migrate to AS-SIP signaling in the future. Duration migration, both H.323 and AS-SIP signaling will be employed in classified VVoIP. Classified VVoIP interfaces to the TDM Defense RED Switch Network (DRSN) via a proprietary PRI. For SBU voice and video, on the edge of the DISN IP WAN cloud, an SC on the B/P/C/S signals via AS-SIP to the network-level softswitch part of SS. The Defense Switched Network (DSN) Common Channel Signaling 7 (CCS7) network is being phased out and replaced by PRI trunks. The TDM End Offices (EOs) use PRI for signaling to the TDM switching part of the SS. The SSs use AS-SIP between themselves to set up IP-to-IP EI sessions across the DISN IP WAN.

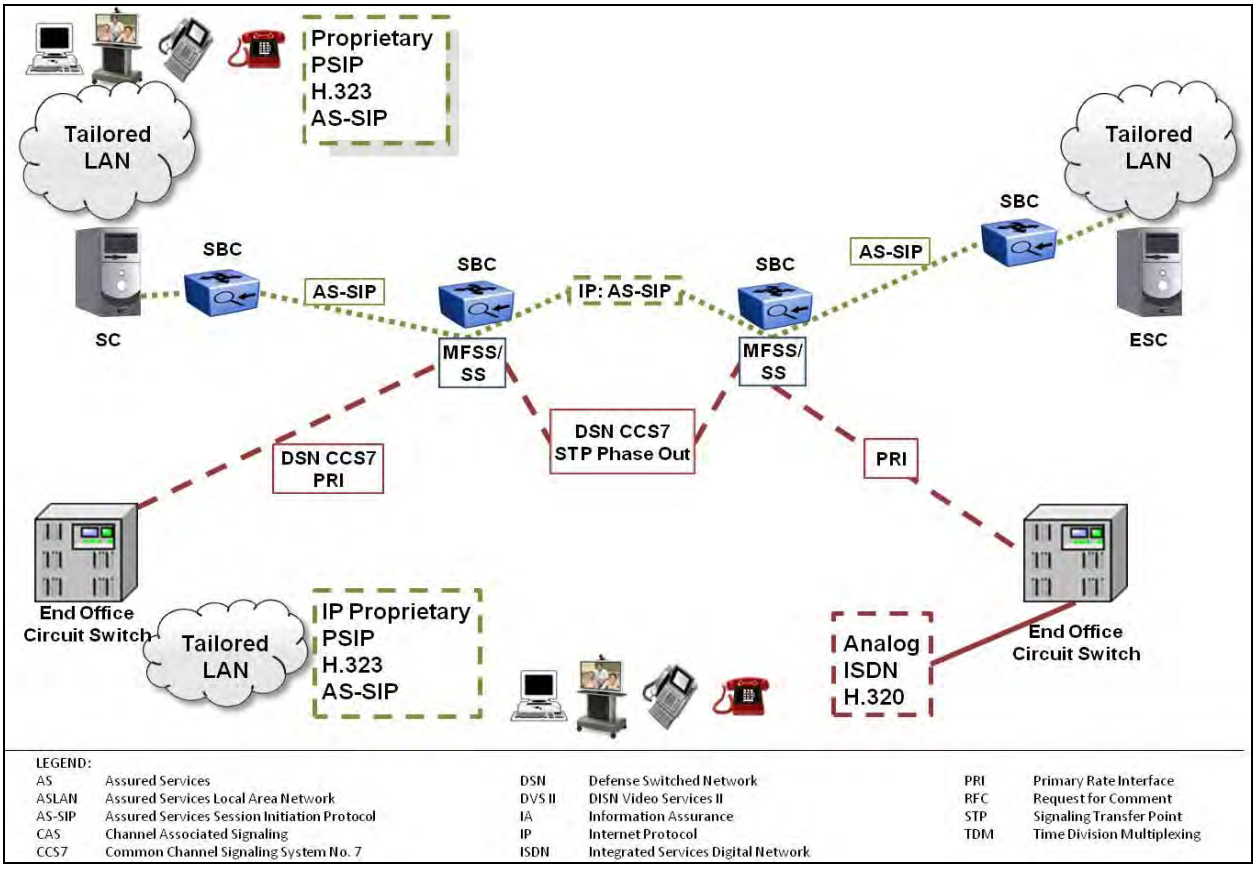

Figure 2.1-5. SBU Voice and Video Services Signaling Design

The SSs use PRI to set up TDM-to-TDM EI sessions across the TDM trunking part of the DISN WAN. Both types of signaling (IP or TDM) are required to support a hybrid TDM and IP EI environment as the DISN voice/video system migrates to an all IP EI environment in the post-2016 timeframe.

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

- Two-level signaling hierarchy—SC and SS:
  - SC A to SS A to SS B to SC B when the SCs have different primary SSs.
  - SC A to SS A to SC B when they have the same primary SS.
- The SCs are assigned a primary and backup SS for signaling robustness.
- Signaling from an IP EI to an SC may be proprietary, or AS-SIP.
- The SC-to-SC signaling is not permitted external to the security enclave except for use in cases involving Deployable products operating in a single area of operational responsibility network that is not the DISN.
- The SC can set up:
  - On-base sessions when a connection to an SS is lost.
  - Sessions to Public Switched Telephone Network (PSTN) trunks independent of an SS.
- Signaling:
  - A TDM EO will signal via DSN CCS7 or PRI to SSs.
  - The SSs will signal via PRI to the PSTN and to coalition gateways.

Signaling from the SC must pass through the network SS part of the SS or through a network-level SS so the SS can implement Precedence-Based Assured Services controls and police the proper use of access circuit bandwidth. For bases that have a collocated SS, base-level access to the local PSTN can be provided through the SC portion of the SS. At the network level, the SS will serve as the gateway to external networks, such as Services' Deployable Programs networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as PRI signaling.

The end-to-end, two-level SBU AS-SIP network signaling design is shown in Figure 2.1-6, End-to-End Two-Level SBU AS-SIP Network Signaling Design. This diagram illustrates operations with Local SCs (LSCs). Operations will be similar for Enterprise SCs (ESCs). For classified networks, the two-level signaling uses SSs.

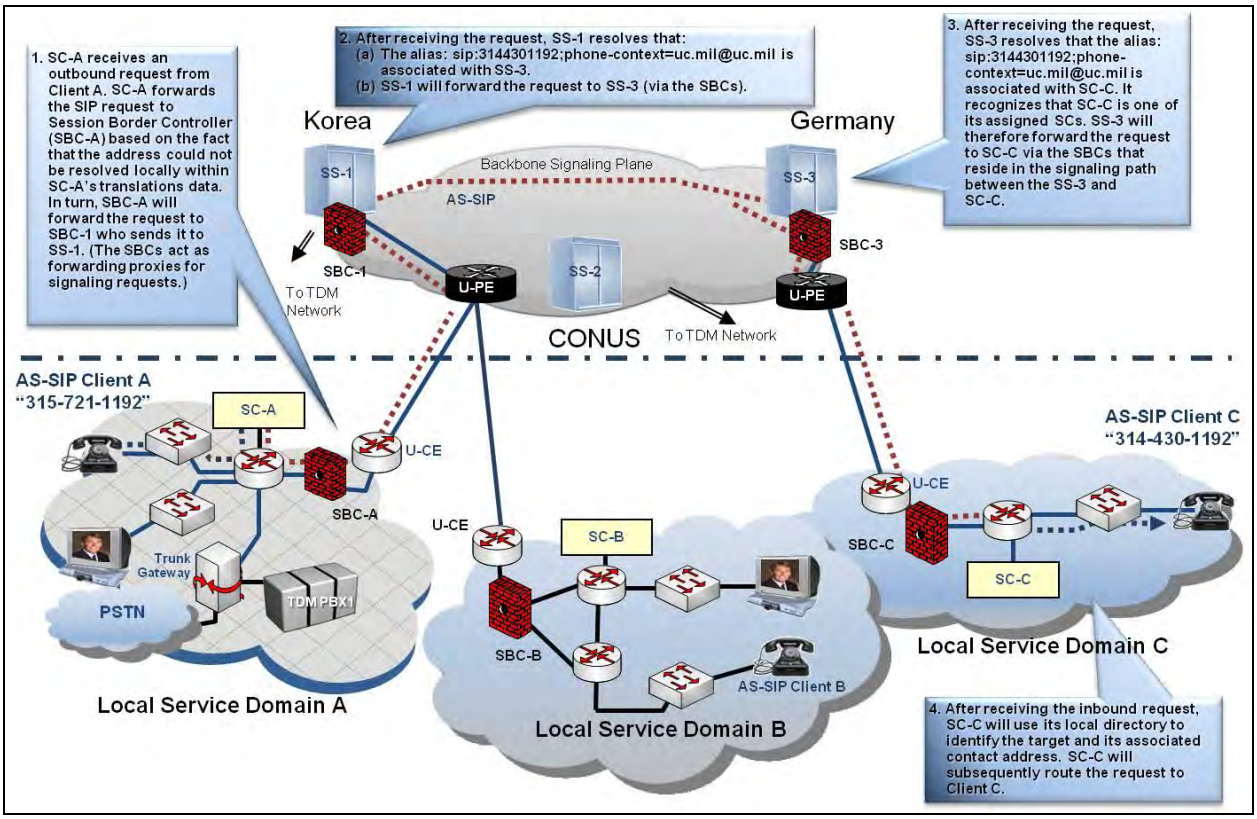

Figure 2.1-6. End-to-End Two-Level SBU AS-SIP Network Signaling Design

2.1.4 Distributed UC Services Model

The SC product can be deployed locally—physically located within the edge segment it serves—or as an enterprise services provider, with centrally located components interacting with components located at edge segments. Figure 2.1-7, Distributed UC Services Model, shows an arrangement of Local SCs and SSs in the DISN assured services voice and video network. See Section 2.2, Enterprise UC Services Design, for a description of the Enterprise UC Services model.

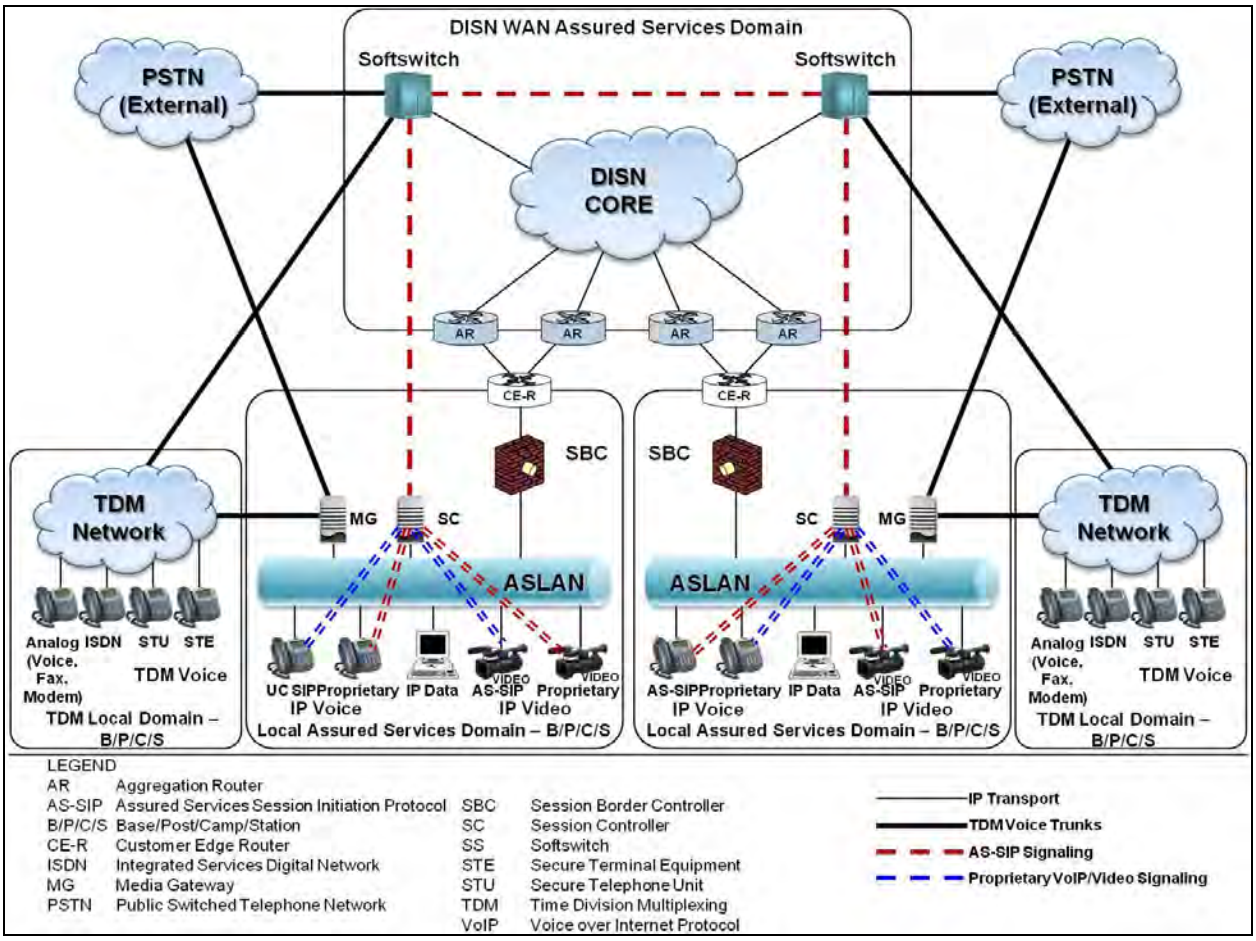

Figure 2.1-7. Distributed UC Services Model

The network is a hierarchical network supporting the following:

- Local services and features within an Edge Segment (base/post/camp/station [B/P/C/S]).
- Global services and features across the UC network.
- Services and features to Department of Defense (DoD) allied networks, DoD coalition networks, and the external Public Switched Telephone Network (PSTN).

2.1.5 Session Control Failover Feature

The session control failover feature involves deploying the SSs as active primary/secondary pairs, whereby one SS acts as the Primary SS for one set of SCs (set A) and acts as the Secondary SS for the SCs of its active paired SS (set B SCs). Similarly, its paired SS acts as the Primary SS for the set B SCs and acts as the Secondary SS for the set A SCs. The SCs shall be assigned to a primary and a secondary (i.e., backup) SS during network configuration.

Each SC is configured with the identity of its Primary SS and its Secondary SS. This is input by operations personnel during SC configuration.

Each SS in the network is configured with the identity of its secondary paired SS. This is input by operations personnel during SS configuration.

Each SS in the network is configured with the identity of every active primary/Secondary SS pair. This is input by operations personnel during SS configuration and is modified as new SSs are added to the network.

The SC and SS failover feature make use of SUBSCRIBE and NOTIFY requests associated with the failover event package defined in UCR 2013, Section 2.6, SC and SS Failover.

Each SC creates a subscription with its Primary SS and with its Secondary SS; the Primary SS and the Secondary SS each create subscriptions with every SC served by the Primary SS and served by the Secondary SS. The subscriptions are arranged based upon a failover event scenario. In addition, the Primary SS and the Secondary SS also create subscriptions with each other based on a failover event scenario. These subscriptions enable the SC and the SSs to send and receive the notification messages that trigger failover and failback.

Each SC sends periodic OPTIONS requests to its Primary SS to detect loss of SIP layer access to the Primary SS.

Each SS sends periodic OPTIONS requests to every one of the SCs for which the SS is operating as the Primary SS to detect loss of SIP layer access to an SC. Specifically, these OPTIONS requests are to enable the Primary SS to detect loss of the Transport Layer Security (TLS) path from the Primary SS SBC to the SC SBC. The TLS path from the SC SBC to the Primary SS MAY be operational in which case the SC cannot detect this outage by the periodic OPTIONS requests the SC sends to the Primary SS.

Each SS in the network sends periodic OPTIONS requests to every other SS in the network (with the exception of its paired SS) to detect loss of SIP layer accessibility to any other SS.

Whenever the SC sends a defined configurable number (default equals 2) of successive OPTIONS requests to its Primary SS that result in failure responses, then the SC concludes the Primary SS is inaccessible (this may be due to a transport failure or a failure of the Primary SS). The SC sends a ‘failover’ NOTIFY message to the Secondary SS informing the Secondary SS that the SC is failing over to the Secondary SS. Then the SC begins sending outbound AS-SIP messages intended for destinations outside the enclave to the Secondary SS.

Upon receipt of a ‘failover’ NOTIFY message, the Secondary SS sends OPTIONS request(s) to the Primary SS to determine whether the Primary SS is accessible at the SIP layer to the Secondary SS.

If the OPTIONS request is successful, then the Secondary SS sends a ‘failover’ NOTIFY message to the Primary SS. The Primary SS now sends all its inbound AS-SIP messages intended for the SC to the Secondary SS instead. The Secondary SS sends all new inbound INVITEs intended for the SC and all subsequent AS-SIP messages associated with the new inbound INVITEs to the SC.

2.2 ENTERPRISE UC SERVICES DESIGN

In accordance with the UC Master Plan, the Enterprise UC Services Architecture is a strategy for providing Enterprise UC Services from a centralized location to DoD Component enclaves within a select geographic region. To achieve the full potential of Enterprise UC Services, the architecture integrates UC voice, video, and IM/Chat/Presence capabilities with other DoD Enterprises Services such as Enterprise E-mail, Enterprise collaboration (e.g., Defense Connect Online), Enterprise Directory Services, and Enterprise Voice Internet Service Provider (ISP) services via a Defense Information Systems Agency (DISA) Internet Access Point (IAP).

2.2.1 Enterprise UC Vision

As depicted in Figure 2.2-1, the Enterprise UC Services Architecture consists of both Centralized Enterprise Infrastructure components and Edge Infrastructure components:

- The Centralized Enterprise Infrastructure is composed of the following:
  - ESC.
  - ESC-fronting SBC.
  - Enterprise Hosted UC Services.
  - Enterprise Required Ancillary Equipment (RAE).
- The Edge Infrastructure (at DoD Components' B/P/C/S locations) consist of the following:
  - End Instruments.
  - Media Gateways.
  - Enclave-fronting SBCs.
  - Survivable Call Processing capabilities (for Environments 1 and 2).
  - Local RAE.

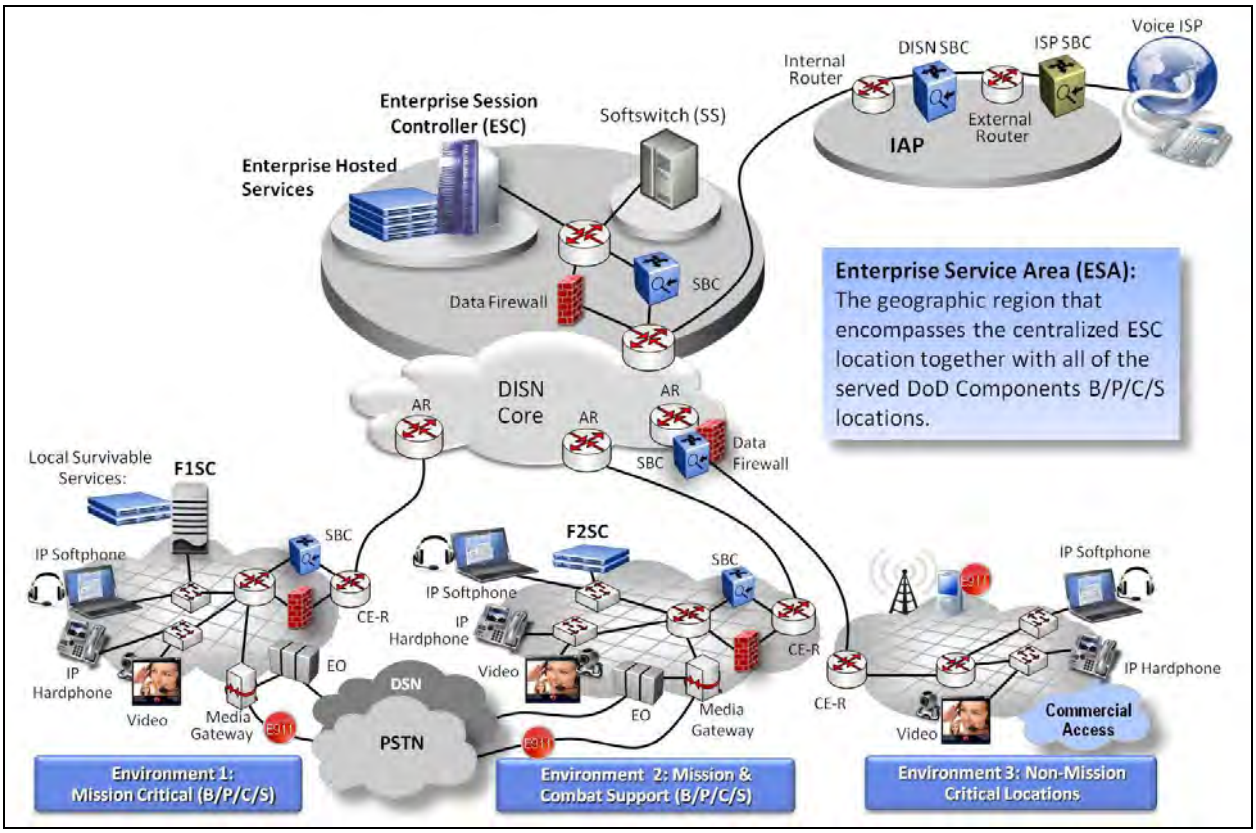

Figure 2.2-1. Enterprise UC Services Architecture

2.2.2 Enterprise System Design

The ESC provides centralized, integrated voice, video and data session management on behalf of served IP end instruments (EIs) that are located at different enclaves (i.e., B/P/C/S locations) within the served geographic region. A full suite of Enterprise Hosted UC Services are collocated with the ESC. The Hosted UC Services include the following:

- Centralized voice and video session management.
- Centralized voice and video conferencing.
- Unified messaging.
- Integrated E911 Call Management.
- Extensible Messaging and Presence Protocol (XMPP) IM/Chat/Presence federation.
- Service portability.
- Integrated Enterprise Directory Services.

The geographic region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations is referred to as the Enterprise Services Area (ESA). The ESC provides an integrated management framework that enables the centralized configuration, provisioning, administration, management, and monitoring of all Centralized

Enterprise Services Infrastructure components and all Edge Infrastructure components within the ESA. Reliable and redundant systems at all levels of the Enterprise UC Services architecture ensure the high availability needed to meet the requirements of the warfighter and operational user.

2.2.3 The Enterprise Continuity of Operations (COOP) Capabilities

The Enterprise UC Services Architecture includes a Continuity of Operations (COOP) strategy which provides for the survivability of essential UC services during a period of network disruption and/or a loss of access to the serving ESC. The survivable UC services (i.e., COOP) requirement of a given location is based upon the mission being performed at that location. The COOP requirements in turn dictate the technical solution components that must be deployed at each B/P/C/S location within the ESA. The UC Master Plan defines three mission environment types as defined in the following subsections.

2.2.3.1 Environment Type 1

Environment 1 is intended to support site user communities with only a limited degradation in UC service when the site is isolated from the ESC (see Figure 2.2-2). A Failover Type 1 Session Controller (F1SC), local service capabilities, enclave-fronting SBC and local media gateway resources are installed on the base. When access to the ESC is interrupted, an Environment 1 location shall have access to the following locally-provided UC services:

- Intra-base precedence calling capability.
- Audio conferencing (sized per customer requirements).
- Video point-to-point.
- Local IM/Chat/Presence capabilities.
- E911 services.
- PSTN/DSN access via local media gateway (sized per customer requirements).

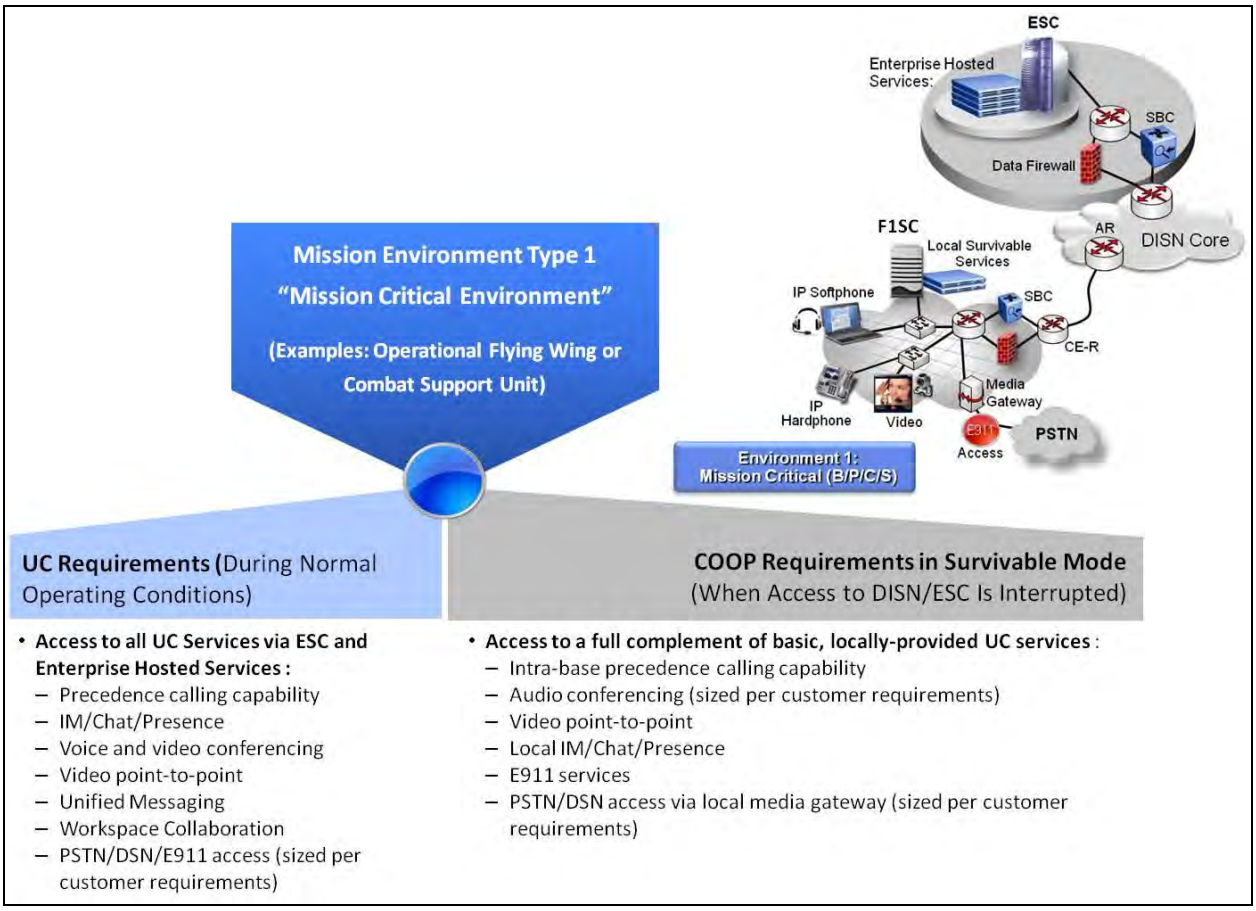

Figure 2.2-2. Environment Type 1

2.2.3.2 Environment Type 2

Environment 2 is intended to support user communities with routine voice only capability when the site is isolated from the ESC (see Figure 2.2-3). A Failover Type 2 Session Controller (F2SC), enclave-fronting SBC and local media gateway resources are installed on the base. When access to the ESC is interrupted, an Environment 2 location has access to the following voice services:

- Intra-base calling capability (ROUTINE service only).
- PSTN/DSN/E911 access via local media gateway (sized per customer requirements).

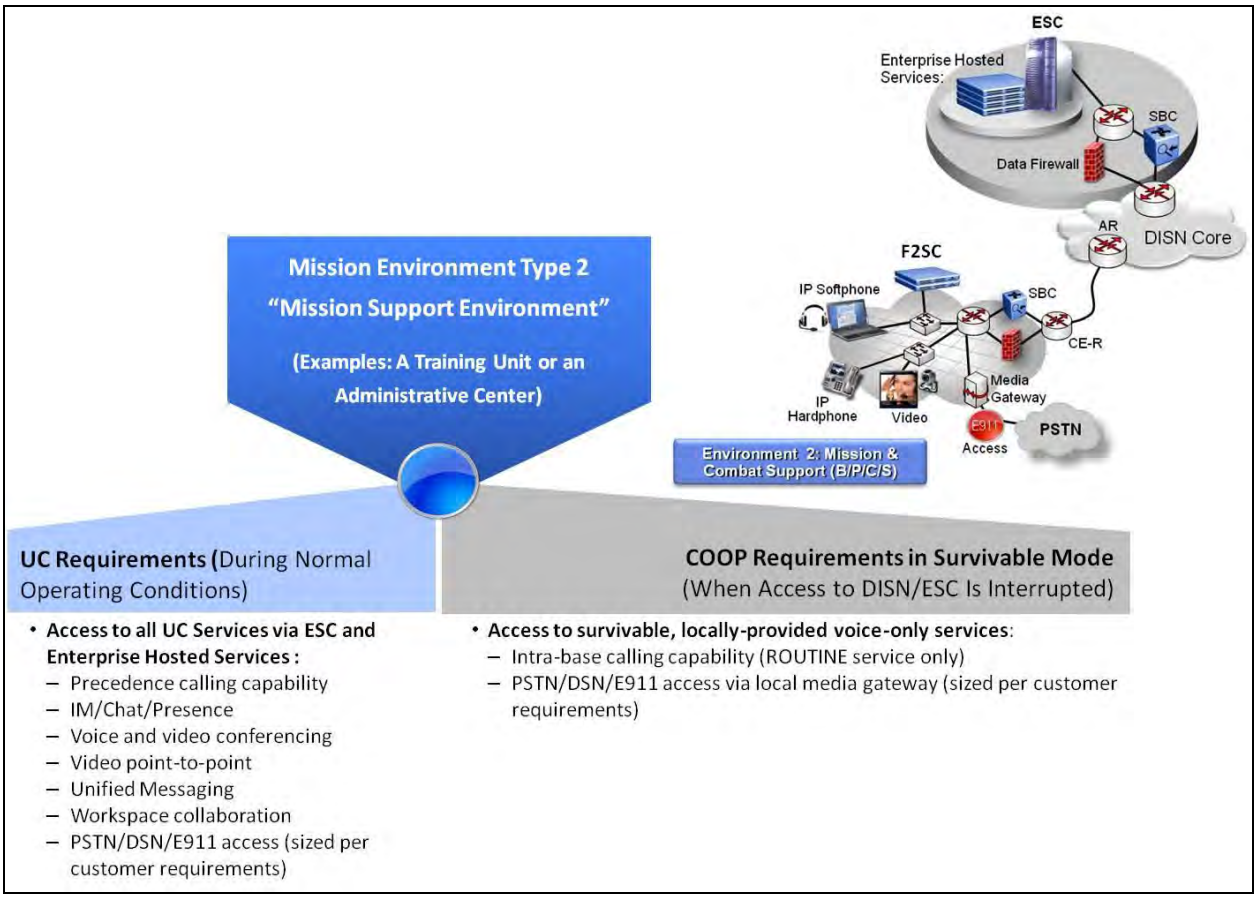

Figure 2.2-3. Environment Type 2

2.2.3.3 Environment Type 3

Environment 3 is intended to support user communities that do not require access to locally provided voice services when the site is isolated from the ESC (see Figure 2.2-4). When access to the ESC is interrupted, an Environment 3 location shall rely upon commercial services via a mobile device (e.g., a cell phone/smart phone).

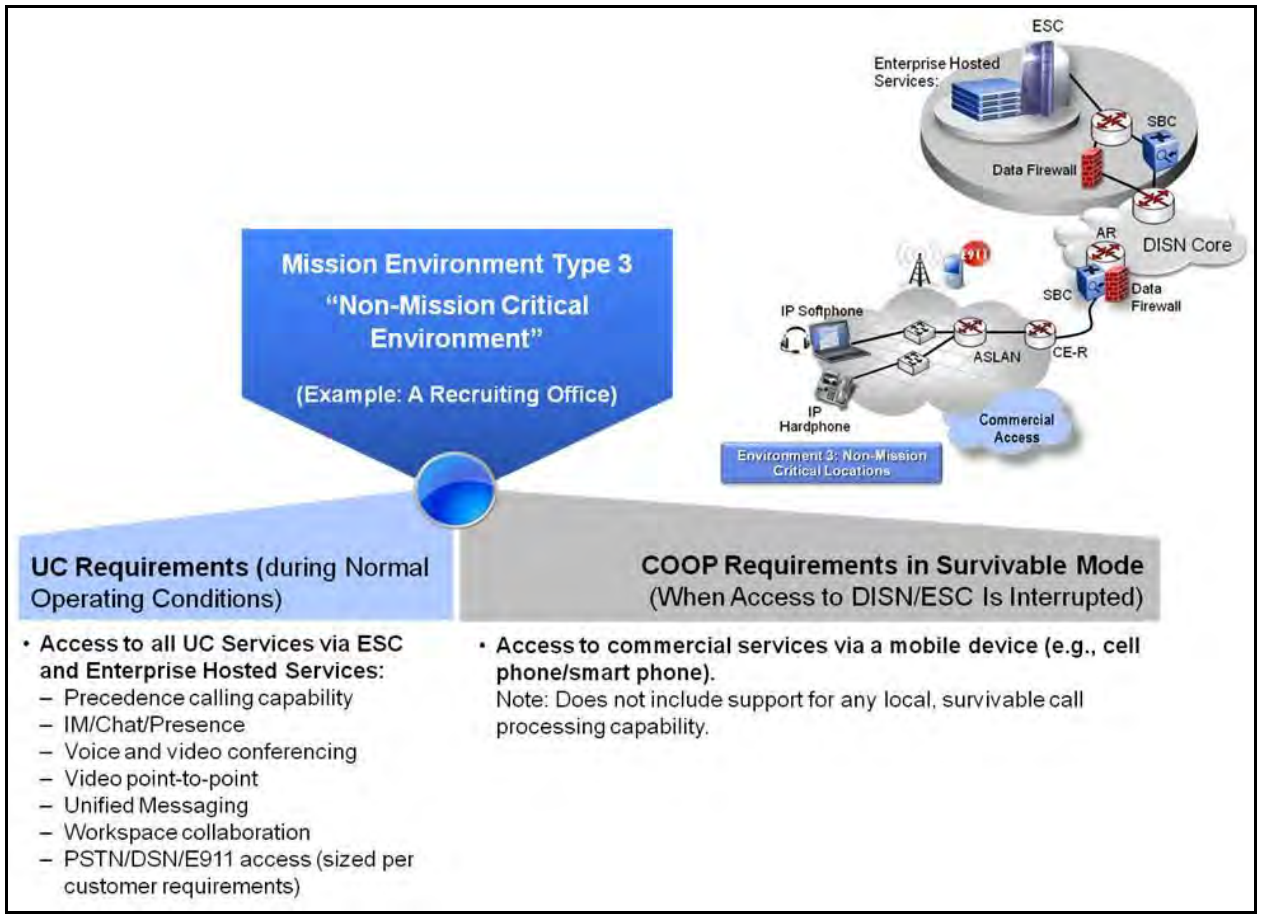

Figure 2.2-4. Environment Type 3

2.2.4 Messaging (IM/Chat/Presence) Integration

The principal focus of the UC Messaging (IM/Chat/Presence) Integration is to drive the certification and deployment of approved products that enable the near real-time exchange of text-based messages using the Extensible Messaging and Presence Protocol (XMPP). XMPP is an open, standards-based protocol specifically designed to enable the "near real-time" exchange of text-based communications in support of applications such as Instant Messaging (IM), Group Chat, and the exchange of presence information (a status indicator that conveys ability and willingness of another party to communicate). The XMPP protocol is a proven, mature technology that is highly scalable and secure with integrated support for channel encryption and strong authentication.

Another important aspect of the UC Messaging (IM/Chat/Presence) Integration is the support for XMPP-based server-to-server federation (i.e., server-to-server interoperability). As depicted in Figure 2.2.5, Multivendor Interoperability Normalized on XMPP, XMPP server-to-server federation permits users who are hosted on one vendor's messaging platform to seamlessly chat and exchange presence information with users who are hosted on another vendor's platform.

Without server-to-server federation, a user can only exchange messages and see the presence information of other users who are all hosted on the same system.

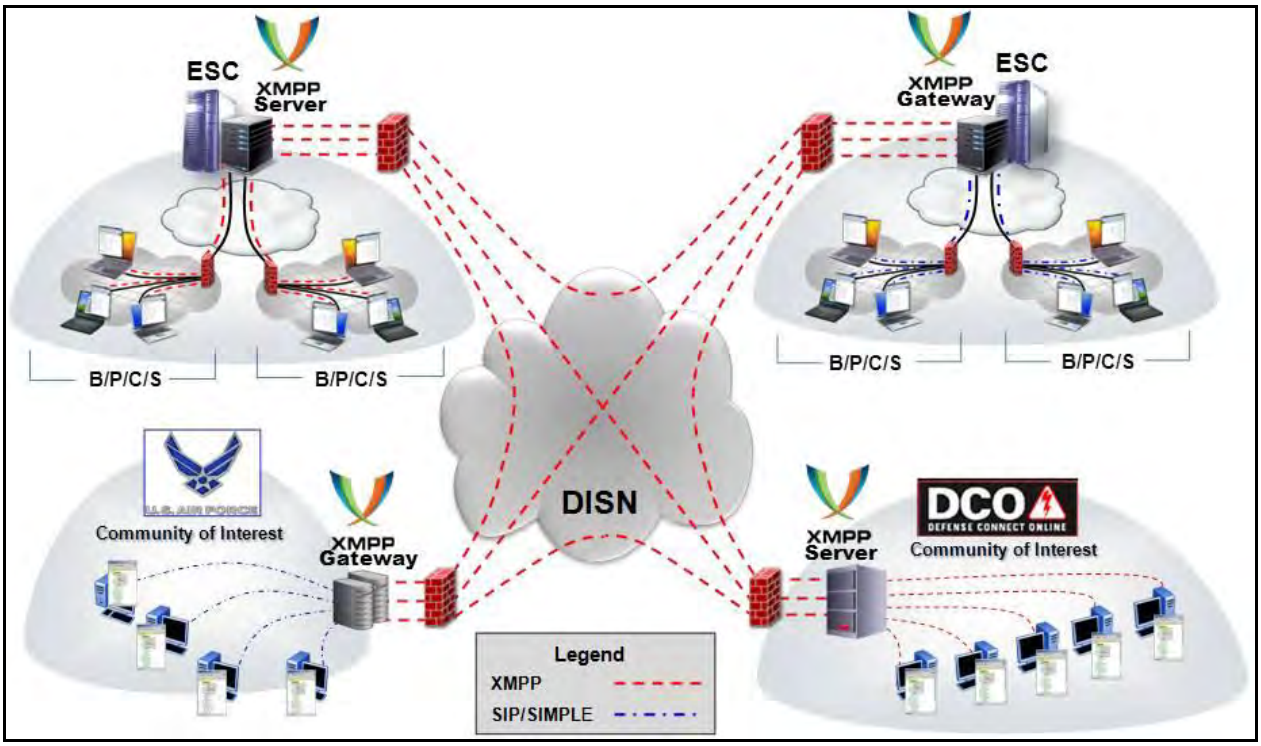

Figure 2.2-5. Multivendor Interoperability Normalized on XMPP

The concept of federating simply refers to a server-to-server link that permits the exchange of Presence information and IM between the two systems.

2.2.5 Enterprise Directory Services (EDS)

This section provides an overview of the initial system concepts for integration of UC services. The voice, video, and data services include multimedia or cross-media collaboration capabilities (including audio collaboration, video collaboration, text-based collaboration, and presence). The focus of the integration is to go beyond local, intra-enclave test events to implement and assess collaboration services and applications on an end-to-end, WAN-level basis. These UC network-wide collaboration services raise the need for new designs to address any potential performance, information assurance, or engineering/configuration issues associated with these different applications traversing the same ASLAN and Network Edge Segments.

This section describes the framework for Enterprise Directory Services (EDS), provided by ESCs and UC Video Conference Bridges for Enterprise UC end users.

The goal of EDS is to provide Enterprise UC end users with access to an Electronic Directory that contains Directory Data (user records) for various DoD end users (users in various DoD Components such as Combatant Commands [COCOMs], Services, and Agencies). The Directory typically contains one record for each end user, though in some cases the Directory may have

more than one record for an individual user. (This can occur in cases in which the user has more than one CAC card and each CAC card represents an individual role that the user performs within his or her DoD Component.) Each Directory record contains a set of attributes that contain information about that particular end user. Examples of attributes that can be found in an individual user's data record are as follows:

- First Name.
- Middle Initials.
- Last Name.
- Organization Name (e.g., Army [AR], Air Force [AF], Navy [NV], Marine Corps [MC], Department of Defense [DoD], Civilian [CIV]).
- Company Name (e.g., COCOM name, Major Command [MAJCOM] name).
- Department Name (e.g., Unit name).
- Display Name.
- E-mail address.
- Business phone number.
- Mobile phone number.
- Fax number.
- Office.
- Job Title.
- Rank.
- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

The number of DoD end users whose data is included in the EDS, and therefore the number of data records included in the EDS, is determined by DISA, which is both the EDS provider and the Enterprise UC provider.

An example of an EDS is the Global Address List (GAL) or Global Address Book (GAB) that is currently provided by the Microsoft Outlook (email client), Microsoft Exchange (email server), and Microsoft Active Directory (directory service) products. In an enterprise running these products, end users can look up information on other end users by sending a query to the directory service, and receive a response back from the service containing the records and attributes that match the criteria in the query. The directory queries and responses are performed using the MS Outlook client on the user's PC, the MS Exchange email server in the enterprise data network, and the MS Active Directory server in the enterprise data network.

DISA's current plan is to provide an EDS to Enterprise UC end users using the following:

- EDS client software on an end user's voice or video EI (i.e., a Voice or Video Hard-Phone that also contains an Enterprise Directory query-response capability);
- EDS client software on the end user's PC (i.e., a software application that contains an Enterprise Directory query-response capability); this application can be either integrated with or separate from the Voice Soft-Phone application or Video Soft-Phone application on that end user's PC.

- EDS gateway server software on the ESC serving the end user.
- EDS DoD Enterprise Email Global Address List (DEE GAL) servers in the Enterprise UC network.

The purpose of the EDS gateway server on the ESC is to provide a mediation point between 1) the various EDS clients on end users' EI and PCs served by the ESC and 2) the EDS DEE GAL servers themselves. The ESC concentrates EDS query traffic from the various EIs and PCs and presents a single EDS query/response interface to each EDS DEE GAL server.

The DEE GAL servers in the Enterprise UC network are also linked to IDSS DEE GAL servers in the DISN so that the directory data in the UC DEE GAL servers remains synchronized with the directory data in the IDSS DEE GAL servers. The data in the IDSS DEE GAL servers is considered an authoritative or "Master" version of the EDS data, and the data in the UC DEE GAL servers is a replica or copy of the Master version.

In addition, the EDS DEE GAL servers in the Enterprise UC Network are not UC APL Products. The EDS Framework in this section applies to EDS clients on Voice and Video EIs, EDS clients on Enterprise UC end users' PCs, and the EDS gateway server software on ESCs, but not to the EDS DEE GAL servers themselves.

Figure 2.2-6 shows the basic architecture used to provide EDS in the Enterprise UC network. Additional DISA and DoD Directory Servers upstream of the EDS DEE GAL servers (such as IDMI, EASF, IDSS, and DMDC) are shown for the sake of completeness. These additional servers are outside of the Enterprise UC network and not part of the framework for EDS.

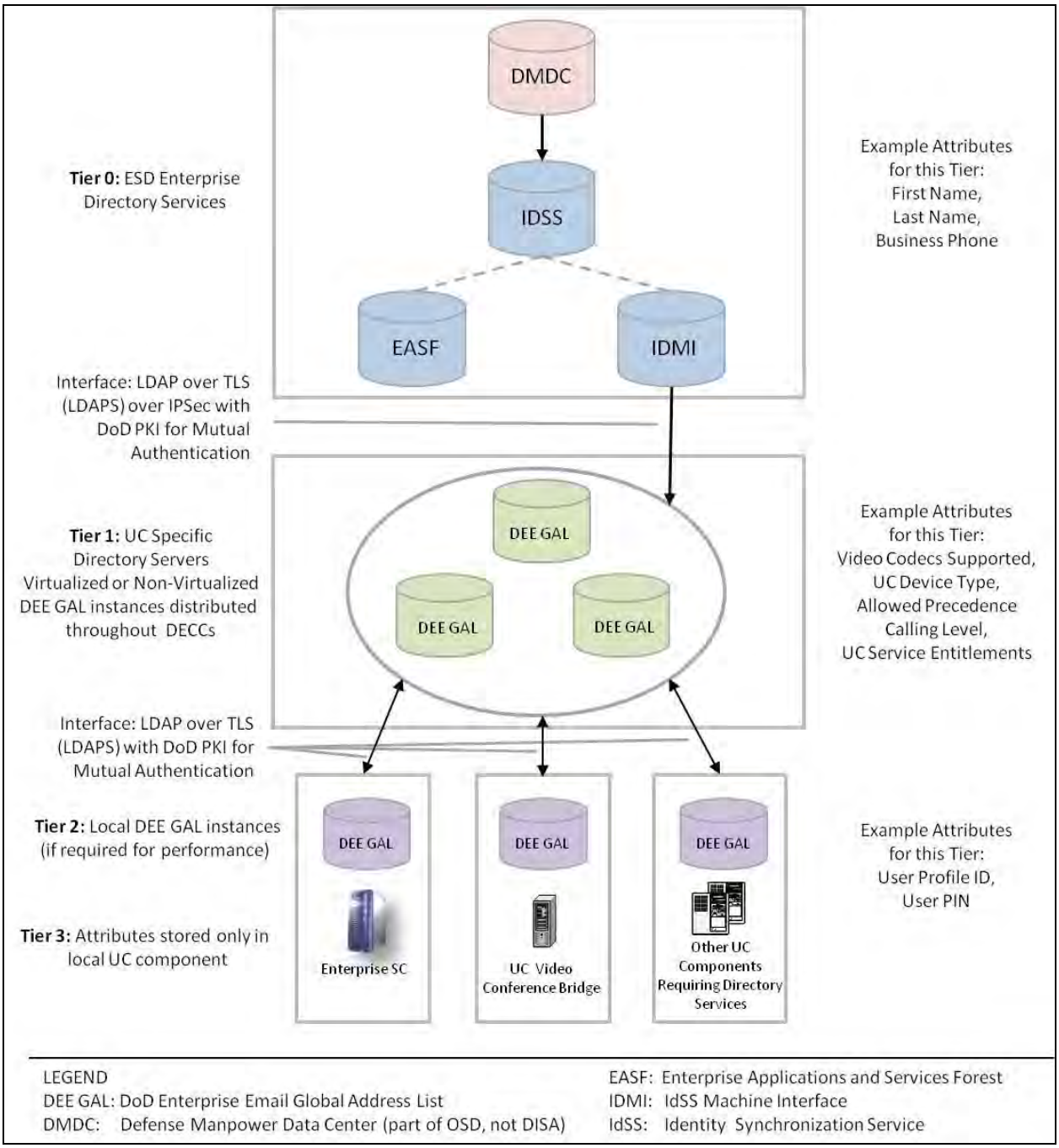

Figure 2.2-6. Basic Architecture for Providing EDS in the Enterprise UC Network

This framework uses an architecture that contains the following UC APL Products:

Voice EI with EDS Client, Video EI with EDS Client, ESC with EDS Gateway, and UC Video Conference Bridge with EDS Gateway. The definitions of these four APL Products are as follows:

Voice EI with EDS Client: A Voice EI (Proprietary EI or AS-SIP EI, Hard-phone or PC-based Soft-Phone, per UCR 2013, Sections 2.9.1 and 2.9.6) that contains an EDS Client Application that can be used to make EDS queries via the ESC EDS Gateway. This EDS Client Application also processes EDS query responses from the ESC EDS Gateway and allows the Voice EI user to place a UC VoIP call to another DoD end user by selecting that DoD end user's record from the query responses. The EDS Client Application may also allow the Voice EI user to select the called address (DSN number, commercial wireline number, commercial mobile number, or DoD SIP URI) from the DoD end user's record and use that address to place a VoIP call to the target DoD end user.

Video EI with EDS Client: A Video EI (Proprietary EI or AS-SIP EI, Hard-phone or PC-based Soft-Phone, per per UCR 2013, Sections 2.9.1 and 2.9.6) that contains an EDS Client Application that can be used to make EDS queries via the ESC EDS Gateway. This EDS Client Application also processes EDS query responses from the ESC EDS Gateway and allows the Video EI user to place a UC Video call to another DoD end user by selecting that DoD end user's record from the query responses. The selected DoD end user should also have UC Video capabilities in this case. The EDS Client Application may also allow the Video EI user to select the called address (DSN number or DoD SIP URI) from the DoD end user's record and use that address to place a Video call to the target DoD end user.

ESC with EDS Gateway: An ESC that contains an EDS Gateway that accepts directory queries from EDS Clients on Voice and Video EIs, converts them to LDAP queries, and then sends them on to the UC DEE GAL server that serves that ESC. When this UC DEE GAL server returns LDAP query responses to the ESC, the ESC converts these responses to a protocol (a format) that the EDS Clients can understand and returns these responses to these EDS Clients on the Voice and Video EIs. Note that the ESC and the UC DEE GAL exchange queries and responses using LDAP protocol, but the ESC EDS Gateways and the EDS Clients can exchange queries and responses using another protocol, such as HTTPS / XML / Simple Object Access Protocol (SOAP).

UC Video Conference Bridge with EDS Gateway: A UC Video Conference Bridge that contains an EDS Gateway. The role of the EDS Gateway in the UC Video Conference Bridge is identical to the role of the EDS Gateway in the ESC; that is, the Conference Bridge's EDS Gateway accepts directory queries from EDS Clients on Voice and Video EIs, converts them to LDAP queries, and sends these queries on to the UC DEE GAL server that serves the Conference Bridge. When this UC DEE GAL server returns LDAP query responses to the Bridge, the Bridge converts these responses to a protocol (a format) that the EDS Clients can understand and returns these responses to these EDS Clients on the Voice and Video EIs.

One difference between the ESC's EDS Gateway and the Video Conference Bridge's EDS Gateway is that the Bridge's EDS Gateway only supports EDS Clients on Voice and Video EIs

that are located behind the Video Conference Bridge in the Enterprise UC Architecture (EIs ⇔ Voice Conference Bridge ⇔ ESC.)

2.3 MOBILITY AND SERVICE PORTABILITY

Service portability is defined as the end user's ability to obtain subscribed services in a transparent manner regardless of the end user's point of attachment to the network. The key UC objective is to provide service continuity by ensuring mobile warfighters' telephone numbers, e mail addresses, and communication and collaboration tools remain constant as their mission and location change. Figure 2.3-1, Mobile Warfighter's Communication Dilemma, shows the problem service portability is trying to solve.

Figure 2.3-1. Mobile Warfighter's Communication Dilemma

To achieve this objective, DISA is working with ESC vendors to provide a UC Mobility feature that would allow Mobile Warfighters to move from one ESC to another and have their assigned phone numbers, IM addresses, and UC services "follow" them as they move. The long-term goal is to provide the same numbers, addresses, and UC services to the Warfighter, independent of the Warfighter's physical location, and independent of the ESC from which he or she is currently being served.

The different ESC vendors provide UC Mobility in their commercial solutions using different methods. The ESC vendors also provide UC services to end users using different EIs (that is, a Hard-Phone, Soft-Phone, or IM/Chat client that works on one vendor's ESC is not currently portable to another vendor's ESC). Because of these differences, DISA needs to work with the ESC vendors to determine the possibility of deploying a multi-vendor-interoperable version of UC Mobility in the worldwide UC network.

In the near term, DISA can use commercial enterprise solutions for User Mobility to serve the Mobile Warfighter. One approach is to use commercial Virtual Private Network (VPN) client software in the user's EI (where the EI is a VVoIP soft client and/or Presence/IM/Chat soft client), and a commercial VPN server in the UC network to provide a secure, encrypted connection ("VPN tunnel") between the user's current physical location and the physical location of the ESC that serves the user. In this approach, the user always obtains service from the same "home" ESC (e.g., the Garrison ESC in the above Figure).

This approach is consistent with the "teleworker" model in commercial enterprises today, where employees who travel or work from home use VPN tunnels over the public Internet to access their office location for corporate email, Web, IM/Chat, and even Voice and Video services. Mobile Warfighters also have the option of using VPN tunnels between their "visited location" and their "home location" in the near term to obtain consistent UC services from their home ESC location until a DISA version of the User Mobility feature is available from the various ESCs in the UC network.

2.4 ASAC OPERATION OVERVIEW

Call Admission Control (CAC) is defined as a process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service (QoS) requirements for the call.

CAC is also referred to as Session Admission Control (SAC), because in the network appliances a VoIP call is also a SIP voice session, and a video call is also a SIP video session. SAC is typically limited to managing the pre-populated session budgets for each Assured Service (voice and video).

Assured Services Admission Control (ASAC) includes CAC/SAC and its support for call counting, voice call budgets, and video call budgets. In addition, ASAC includes capabilities for handling calls differently based on their precedence level, and for having calls of a higher precedence level preempt calls of a lower precedence level. Two different levels of ASAC are employed: Session Controller (SC)-Level ASAC and WAN-Level ASAC Policing by the Softswitch (SS).

2.4.1 ASAC Budgets and Counts

2.4.1.1 Voice Budgets and Counts

The SC and its associated SS are configured with an IP Budget (IPB) value, the total budget of VoIP sessions, plus session attempts in the session setup phase, that are allowed on the CE-R to WAN IP access link between the SC and the SS. Optionally, separate budgets for inbound sessions (IPBi) and outbound sessions (IPBo) may also be set.

One voice session budget unit is equivalent to 110 kilobits per second (kbps) of access circuit bandwidth. This bandwidth equivalent is based on International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.711 encoding rate plus IPv6 packet overhead plus ASLAN Ethernet overhead. The G.711 encoding rate is used for the voice session budget unit even though other EI codecs, with lower bandwidth requirements, may be used in the network. Note that IPv6 overhead, not IPv4 overhead, is used in the determination of bandwidth equivalents here.

The terms “inbound” and “outbound” in the context of ASAC are always relative to an SC. An inbound session is one that has been initiated by an EI outside a given SC’s domain, whereas an outbound session is one that is initiated by an EI within a given SC’s domain. Performing ASAC separately on an inbound and outbound basis is called directionalization, and is optional.

The SC maintains the ASAC session state of each EI in its domain. That is, the SC knows whether the EI is in a busy state (including both the session setup phase and active session phase) and, if busy, the precedence level of the session.

The SC and its associated SS maintains the total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase. This value is the IP Count (IPC). Optionally, separate counts for inbound sessions (IPCi) and outbound sessions (IPCo) may also be maintained.

At the SC, a TDM Session Budget (TDMB) is configured and a TDM Session Count (TDMC) is maintained. The values for these items are in terms of digital signal level 0 (DS0s) on the TDM trunks between the SC and any local EO/Small EO (SMEO)/Private Branch Exchange (PBX) 1/PBX2.

2.4.1.2 Video Budgets and Counts

Since the bandwidth of a video session can vary, video sessions are budgeted in terms of Video Session Units (VSUs). One VSU equals 500 Kbps, and bandwidth for video sessions will be allocated in multiples of VSUs. For example, the bandwidth allocated to video sessions may be 500 Kbps, 1000 Kbps, 2500 Kbps, and 4000 Kbps. Thus, a video session that requires 2500 Kbps will be allocated five VSUs, and a video session that requires 4000 Kbps will be allocated eight VSUs.

Video budget and count values are in VSUs and are similar in concept to voice budgets and counts, except that no TDM-related items are maintained for video:

- VDB the configured video session budget (optional).
- VDBi the configured inbound video session budget (optional).
- VDBo the configured outbound video session budget (optional).
- VDC the count of video sessions, in VSUs.
- VDCi the count of inbound video sessions, in VSUs (optional).
- VDCo the count of outbound video sessions, in VSUs (optional).

2.4.2 ASAC Session Control Overview

2.4.2.1 Outbound (Originating-Outgoing) Voice Sessions

When an outbound session is initiated, the SC checks whether the VoIP count (IPC) is less than the VoIP budget (IPB). If so, the SC forwards the session request to its associated SS for further processing.

If IPC equals IPB, and all existing sessions traversing the SC-to-SS link are at a precedence level equal to or greater than the new session request, the new session is not placed. If the new session attempt is a precedence call (i.e., PRIORITY or higher), the calling party receives a BPA. If the new session attempt in this circumstance is a ROUTINE call, the caller receives an "all trunks busy" indication (also known as "fast busy').

If IPC equals IPB and at least one existing session is of lower precedence than the new session, the SC preempts one of the lowest precedence sessions and forwards the session INVITE (via the SS) to the sessioned SC for processing.

2.4.2.2 Inbound (Incoming-Terminating) Voice Sessions

When an inbound session INVITE is received by an SC, the SC checks whether the VoIP count (IPC) is less than the VoIP budget (IPB). If so, and the called party is not busy, the SC places the session.

If IPC is less than IPB and the called party is busy with a session that is at a lower precedence level than the one being placed, the SC preempts the existing session and places the new session.

If IPC is less than IPB and the called party is busy with a session that is of an equal or higher precedence level than the session being placed, the new session is not placed. If the new session attempt is a precedence call, the calling party receives a BPA. If the new session attempt is a ROUTINE call, the caller receives "fast busy".

If IPC equals IPB, and the called party is not busy, but all existing sessions traversing the SC-to-SS link are at a precedence level equal to or greater than the new session request, the new session is not placed. The caller receives a BPA, or if it is a ROUTINE call, the caller receives "fast busy".

If IPC equals IPB, and the called party is busy with a session that is of a lower precedence level than the new session, the SC preempts the existing session and forwards the session INVITE to the called party.

If IPC equals IPB, and the called party is busy with a session that is of equal or higher precedence level than the new session, the session is not placed. The caller receives a BPA, or if it is a ROUTINE call, the caller receives "fast busy".

The IPC must be incremented for each inbound and outbound session placed, and decremented for each such session taken down.

NOTE: Intra-enclave calls are subject to preemption rules but are not affected by session budgets or impact session counts.

2.4.2.3 Directionalization

If ASAC directionalization is implemented, directionalized session budgets (IPBo and IPBi) will be set and separate IPCo and IPCi counts will be maintained by the SC in order to ensure that these counts do not exceed their respective budgets. Outbound and inbound ASAC is carried out independently from each other, with each using the respective process described above.

2.4.2.4 Video Session Processing

ASAC processing of video sessions is similar to ASAC processing for VoIP sessions. However, some extensions to the VoIP rules are needed because video sessions consume varying VSU amounts (e.g., one video session could count as 1 VSU against the budget, but another video session could be consuming 8 VSUs):

1. Preempt sessions in the process of signaling setup (progress) before preempting active sessions.
2. Preempt the minimum number of sessions to accumulate the number of budgets needed to satisfy the video session request.
3. Accumulate the needed number of budgets by preempting all sessions of a lower precedence level (starting at the ROUTINE level) before proceeding to preempt from sessions of the next higher precedence level for the remaining required budgets.
4. When the number of sessions selected for preemption result is more budgets (excess) than are required to satisfy the video session request, return the excess budgets to the ASAC pool.

2.5 PRECEDENCE-BASED ASSURED SERVICES

DoD UC networks support Precedence-Based Assured Services (PBAS) for delivery of UC services. Connections and resources that belong to a call from a UC subscriber are marked with a precedence level and domain identifier and can only be preempted by calls of higher precedence from UC users in the same service domain. Precedence provides for preferred handling of PBAS service requests. PBAS involves assigning and validating priority levels to calls, and prioritized treatment of service requests.

There are five precedence levels; from lowest to highest they are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

The maximum precedence level of a subscriber is set at the subscription time by the UC network administrator based on the subscriber's validated need. When initiating a session, the subscriber may select a precedence level up to and including the maximum authorized precedence level for that subscriber, on a per call basis.

The network at the subscriber's originating interface ensures that the selected precedence level does not exceed the maximum level assigned to that telephone number. A call will default automatically to the ROUTINE precedence unless a higher precedence is dialed.

Preemption may take one of two forms. First, the called party may be busy with a lower precedence call that is preempted in favor of completing the higher precedence call from the calling party. Second, the network resources may be busy with calls; some of which are of lower precedence than the call requested by the calling party. One or more of these lower precedence calls are preempted in order to complete the higher precedence call.

Four characteristics of preemption follow:

1. Generally, any party whose connection is terminated, whether that resource is reused or not, receives a distinctive preemption notification.
2. Any called party of an active call that is being preempted by a higher precedence call must acknowledge the preemption by going "on-hook," before being connected to the new calling party.
3. When there are no idle resources, preemption of the lowest precedence resources occurs.
4. A call can be preempted any time after the precedence level of the call has been established and before call clearing has begun.

After attempting a precedence call, the calling party receives an audible ringback precedence call tone when the call is offered successfully to the called party.

If the attempted precedence call is not offered to the intended party – because of other calls of equal or higher precedence, or the called party belongs to a network that does not support preemption and there are insufficient resources on that network – the calling party receives a Blocked Precedence Announcement (BPA).

A Busy Not Equipped Announcement (BNEA) is played to the calling party of a precedence call when the called party is busy and classmarked as non-preemptable.

Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party are diverted to an attendant console.

2.6 VOICE FEATURES AND CAPABILITIES

This section describes the following Assured Services voice features and capabilities:

- Call Forwarding.
- Precedence Call Waiting.
- Call Transfer.
- Call Hold.
- Three-Way Calling.
- Hotline Service.
- Calling Number Delivery.
- Call Pick-Up.
- Precedence Call Diversion.

2.6.1 Call Forwarding

Four types of VVoIP Call Forwarding (CF) features are considered for UC:

- Call Forwarding Variable (CFV).
  - When the CFV feature is active for a given user's Directory Number (DN), calls intended for that DN are redirected to a user-specified DN (DSN Number or commercial). A user can activate and deactivate CFV for his DN, and specifies the desired terminating DN during each activation. Users cannot answer calls at a DN for which CFV is active, but can originate calls at that DN.
- Call Forwarding Busy Line (CFBL).
  - When Call Forwarding Busy Line (CFBL) is configured for a given DN, calls intended for that DN are redirected to a configured DN when the former DN is busy.
- Call Forwarding – Don't Answer – All Calls (CFDA).
  - Calls to DNs configured with CFDA that are not answered after a user -specified number of ringing cycles are redirected to a configured DN. NOTE: if the DN to which unanswered calls are forwarded is busy, the original DN continues to ring until the originator of the call abandons it or the call is answered.
- Selective Call Forwarding (SCF).

– SCF allows users to forward calls from selected, user-specified calling parties identified by DNs on a screening list.

Call forwarding interaction with PBAS is optional. Figure 2.6-1, Call Forwarding Logic Diagram, shows the VVoIP CF treatment logic.

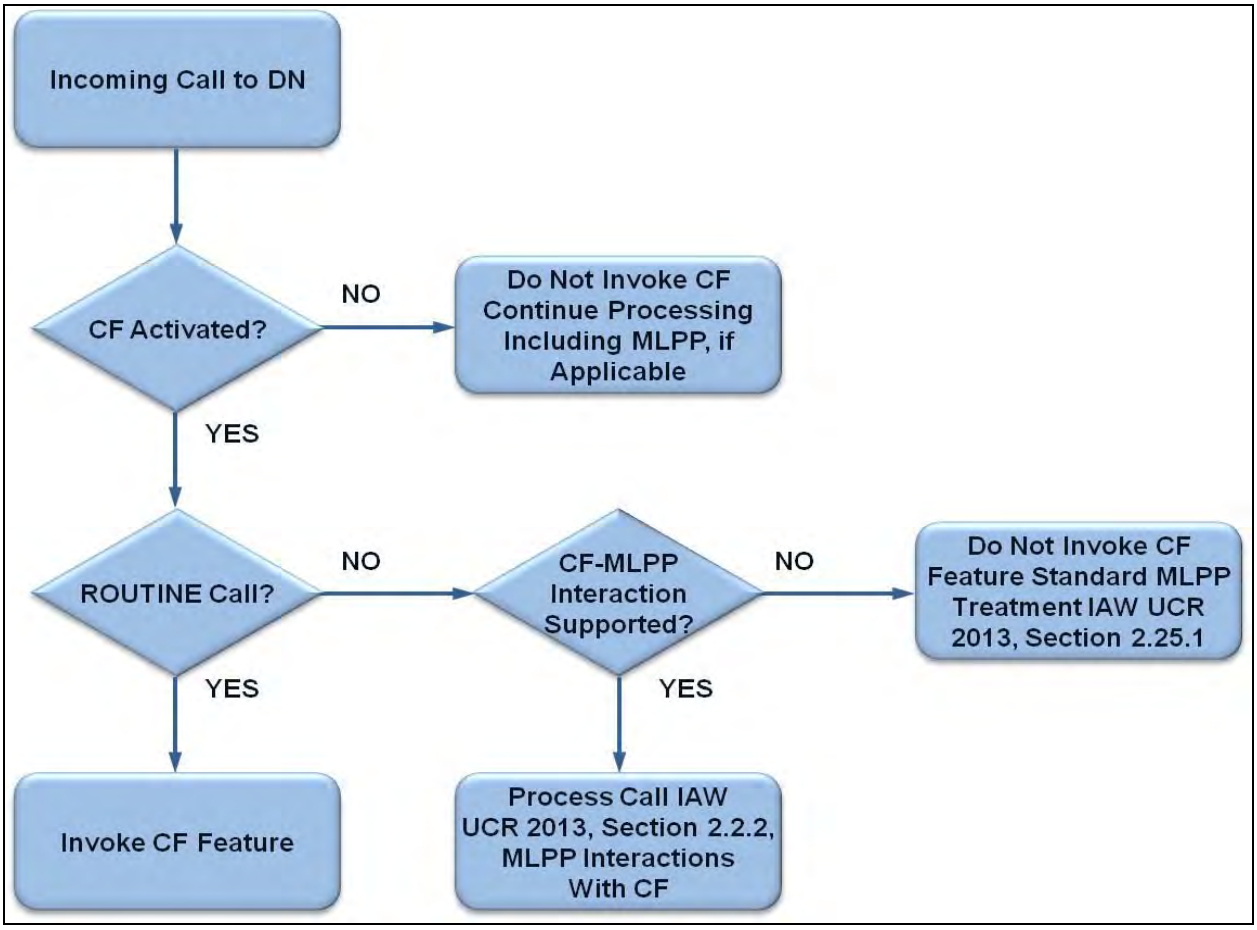

Figure 2.6-1. Call Forwarding Logic Diagram

2.6.2 Precedence Call Waiting

The UC Precedence Call Waiting feature is for single-call-appearance VoIP phones, Terminal Adapters (TAs), and Integrated Access Devices (IADs) only. It is not a feature for multiple-call-appearance VoIP phones.

When a DN is busy with a call at the same or lower precedence level as an incoming precedence call (i.e., PRIORITY or above), the called party receives the Precedence Call Waiting (CW) tone. The called party can place the current active call on hold, or disconnect the current active call, and answer the incoming precedence call. If the called party does not answer, the incoming precedence call is diverted to attendant (see Precedence Call Diversion).

2.6.3 Call Transfer

Two types of call transfer are supported:

- A normal call transfer takes place when a user transfers an incoming call to another party.
- An explicit call transfer happens when both calls are originated by the same subscriber.

When a call transfer is made at different precedence levels, the resulting connection is classmarked at the highest precedence level of the two segments of the transfer.

2.6.4 Call Hold

Call Hold is invoked by going "on-hook," then "off-hook." Calls on hold retain the precedence of the originating call. All DNs are subject to normal preemption procedures.

Figure 2.6-2, Call Hold Scenarios, illustrates three typical call hold scenarios. In each scenario, caller #3 is on hold with caller #1, and caller #1 is talking to caller #2.

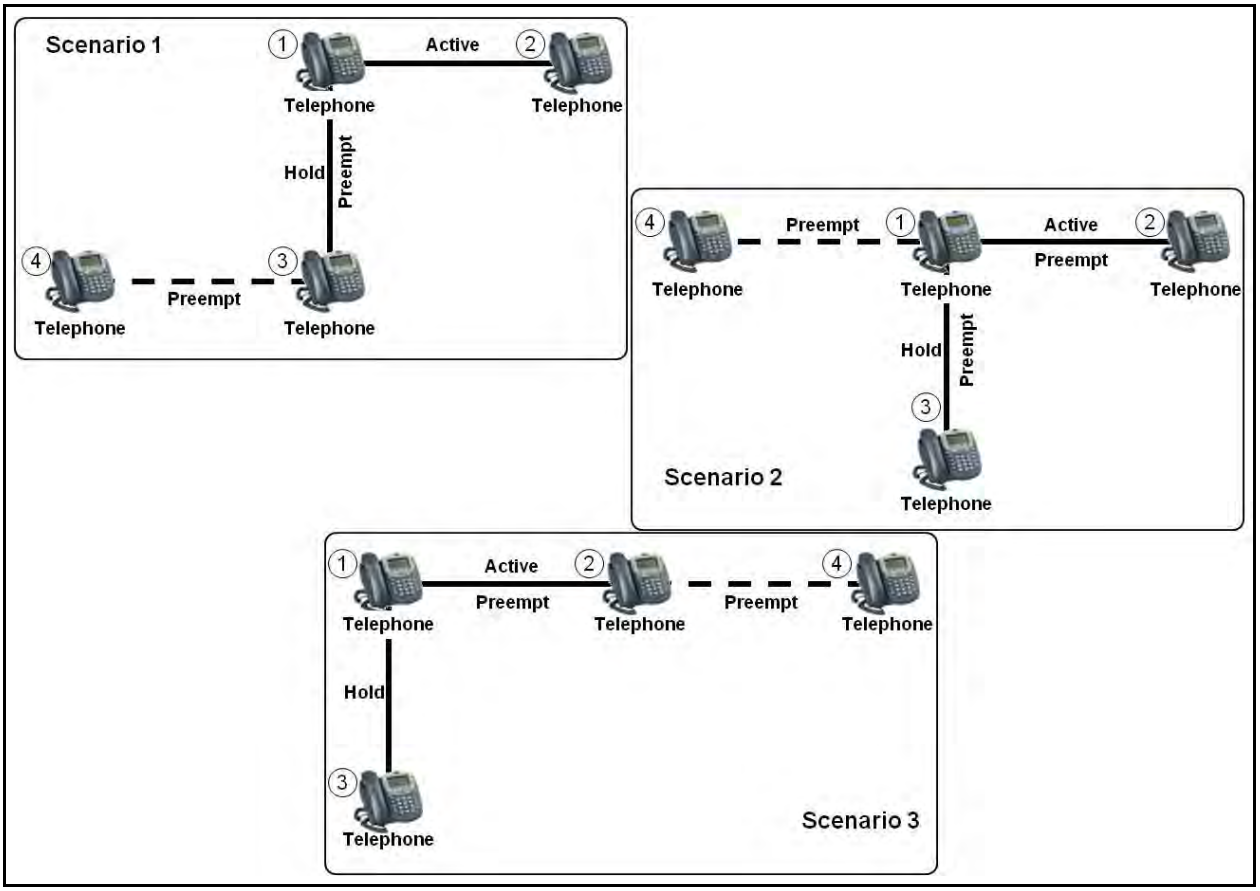

Figure 2.6-2. Call Hold Scenarios

In scenario 1, caller #3 receives an incoming, higher precedence call from caller #4. Caller #3 receives a preemption tone. After caller #3 acknowledges the preemption tone by going "on

hook," the call between caller #4 and caller #3 is established when caller #3 answers caller #4. Caller #1 will receive a preemption tone also only if caller #1 attempts to retrieve caller #3 while the preemption tone is being sent to caller #3.

(NOTE: The preemption tone shall not be sent to caller #1 while active with caller #2. This would give caller #1 the false indication that the active call with caller #2 is being preempted.)

Caller #2 remains connected to caller #1, and caller #1 does not receive any preemption notification.

In scenario 2, caller #1 receives an incoming, higher precedence call from caller #4. Caller #1, caller #2, and caller #3 receive a preemption tone (see Table 2.9-2, UC Information Signals). After caller #1 acknowledges the preemption and then goes "on hook," the higher precedence call from caller #4 is offered. Callers #2 and #3 are disconnected and the call between caller #4 and caller #1 is established.

In scenario 3, caller #2 receives an incoming, higher precedence call from caller #4. Caller #2 receives a preemption tone. Caller #1 receives a preemption tone. The tone indicates to caller #1 that caller #2 is being preempted. After caller #1 goes "on-hook," caller #1 receives a ringback from the call that is still on hold (caller #3).

2.6.5 Three-Way Calling

In Three-Way Calling (TWC), each call has its own precedence level. When a three-way conversation is established, each connection maintains its assigned precedence level. Each connection of a call resulting from a split operation maintains the precedence level that it was assigned upon being added to the three-way conversation. However, originator of the three-way call is classmarked at the highest precedence level of the two segments of the call. Incoming precedence calls to lines participating in TWC that have a higher precedence than the TWC originator invoke preemption (unless the call is marked non-preemptable).

2.6.6 Hotline Service

Hotline Service allows a user to initiate a voice or data call to a predetermined party automatically simply by "going off hook."

2.6.7 Calling Number Delivery

Called parties are provided with the number of the calling party, based on dialing plan used by the calling instrument:

- If the incoming call is from another DSN user, the calling number delivered is the 10-digit DSN number.

- If the incoming call is from a commercial user, the calling number delivered to the called party is in national or international calling number format.

The name, organization and location of the calling party may also be provided, when the called and calling parties are served by the same SC.

2.6.8 Call Pick-Up

Call Pick-Up is an optional feature that allows a user to answer calls directed to other users within a preset pick-up group.

Three types of Call Pick-Up features are considered for UC:

- Basic Call Pick-Up.
  - An EI may answer a call that has been offered to another EI in its common call pick up group in a business group. This is accomplished by dialing a pick-up access code while the called EI is being rung. If more than one EI in the group is being rung, the EI that has been ringing longer shall be picked up first.
- Directed Call Pick-Up.
  - Directed call pick-up permits a user to dial a code and destination number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up. If the other EI has answered, a TWC is established.
- Directed Call Pick-Up Without Barge-In.
  - This feature is identical to the Directed Call Pick-Up feature, except that if the destination number being picked up has already answered, the party dialing the pick-up code shall be routed to reorder rather than be permitted to barge in on the established connection to create a TWC.

If a Call Pick-Up feature is provided, it must support precedence and preemption. When a call pick-up group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pick-up attempt in that group retrieves the highest precedence call first. If multiple calls of equal precedence are ringing simultaneously, a call pick-up attempt in that group retrieves the longest ringing call. If a party in a call pick-up group is busy, and an incoming precedence call is placed to that number, normal PBAS rules apply.

2.6.9 Precedence Call Diversion

Unanswered precedence calls (i.e., PRIORITY and above) are diverted to a designated DN (e.g., attendant console), after a specified period. This diversion takes place before any forwarding to voice mail or Automatic Call Distribution (ACD) systems.

Incoming precedence calls to the attendant's listed DN, and incoming calls diverted to an attendant, signal the attendant by a distinctive visual signal indicating the precedence level, and

are placed in queue. Call distribution is used to reduce excessive waiting times. Each attendant position operates from a common queue or set of queues. Incoming calls are queued for attendant service by precedence and time of arrival. The highest precedence call with the longest holding time is answered first. A recorded message of explanation is played to the parties waiting in queue.

In some cases, the B/P/C/S where the SC or SS is located may not have a continuously manned Attendant Station (or set of Attendant Stations). In these cases, Precedence Call Diversion provides an announcement back to the calling party (the party whose call was diverted), providing them with a DSN number that gives them access to a continuously manned attendant.

- Support for Precedence Call Diversion from one UC EI to another UC EI on the same SC is required.
- Support for Precedence Call Diversion from an UC EI on one SC to an UC EI on another SC is required.
- Support for Precedence Call Diversion from an UC EI on an SC to a DSN EI (on an EO, SMEO, PBX1, or PBX 2) is not required.
- Support for Precedence Call Diversion from a DSN EI (on an EO, SMEO, PBX1, or PBX 2) to an UC EI on an SC is not required.

2.6.10 Public Safety Voice Features

2.6.10.1 Basic Emergency Service (911)

The Basic 911 Emergency Service feature provides a three-digit universal telephone number (e.g., 911) that gives direct access to an emergency service bureau. 911 calls may be routed either to a DoD emergency response center, or to a PSTN 911 PSAP. Calling 911 does not require the use of access codes such as 99. 911 calls are not subject to PBAS/MLPP preemption.

See Section 3.4.1 for a description of E911 Management Systems.

2.6.10.2 Tracing of Terminating Calls

The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice calls terminating to a specified DN. When this feature is activated, the originating DN, the terminating DN, and the time and date are recorded for each call to the specified line.

2.6.10.3 Outgoing Call Tracing

The Outgoing Call Tracing feature allows the tracing of nuisance calls to a specified DN suspected of originating from a given local office. The tracing is activated when the specified DN is entered. A record of the originating DN, and the time and date, are generated for every call to the specified DN.

2.6.10.4 Tracing of a Call in Progress

The Tracing of a Call in Progress feature identifies the originating DN for a call in progress. Authorized personnel entering a request that includes the specific terminating DN involved in the call activate the feature.

2.6.10.5 Tandem Call Trace

The Tandem Call Trace feature identifies the calling party of a call to a specified office DN for calls that involve a SS. A record of the calling party number and terminating DN, and the time and date, is generated for every call to the specified DN.

2.7 END INSTRUMENTS

The following End Instrument (EI) types are considered in UC:

- Proprietary IP voice EIs.
- Proprietary IP video EIs.
- ROUTINE-only EIs.
- AS-SIP voice EIs.
- AS-SIP video EIs.
- AS-SIP Secure voice EIs.
- Secure IP EI (using SCIP/V.150.1 protocol).
- Softphone.

Issues unique to classified EIs are described in Appendix B, Unique Classified Unified Capability.

An EI that uses vendor-proprietary signaling is indicated by PEI in this document and in UCR 2013. Both ITU H.323 and Internet Engineering Task Force (IETF) SIP (i.e., commercial SIP, not DISA-specified AS-SIP) also are considered vendor-proprietary EI to SC protocols. They are treated as vendor-proprietary protocols because one EI vendor's implementation of H.323 or SIP is not guaranteed to interoperate with another SC vendor's implementation of H.323 or SIP.

A ROUTINE-only EI (ROEI) is an EI that meets the PEI requirements in UCR 2013, Section 2, except that it is not required to support PBAS. Any SC that supports ROUTINE-only voice EIs must also support voice EIs that fully support PBAS. An SC is allowed to support ROUTINE-only video EIs without supporting fully PBAS-capable video EIs.

An AS-SIP voice EI is a UC voice phone (Hard-Phone or Soft-Phone) that uses AS-SIP signaling instead of vendor-proprietary signaling.

An AS-SIP video EI is a UC video phone (Hard-Phone or Soft-Phone) that uses AS-SIP signaling instead of vendor-proprietary signaling. A proprietary video EI is a video phone that uses vendor-proprietary signaling. The AS-SIP video EIs and proprietary video EIs are video phones (Hard-Phones or Soft-Phones), and are not MCUs. MCUs are more complex than video phones, and involve point-to-multipoint video conferences instead of point-to-point video calls.

An AS-SIP secure voice EI is a UC secure voice phone (hardphone only) that uses AS-SIP signaling instead of vendor-proprietary signaling. A proprietary secure voice EI is a secure phone that uses vendor-proprietary signaling. The AS-SIP secure voice EIs and proprietary secure voice EIs both use V.150.1 modem relay for secure voice media transfer, per the Government's SCIP-215 specification and ITU Recommendation V.150.1. The AS-SIP secure voice EIs also operate in the same manner as AS-SIP voice EIs, during nonsecure parts of the voice call where end-to-end voice communication is done "in the clear."

A softphone is an end user software application on an approved operating system that enables a general-purpose computer to function as either a PEI or AEI. The softphone is conceptually identical to a traditional IP "hard" telephone and is generally required to provide the voice features and functionality provided by a traditional IP hard telephone.

2.7.1 Voice over IP Sampling Standard

For Fixed-to-Fixed calls, EIs use 20 ms as the default voice sample length, and as the basis for the voice payload packet size. For other call types, e.g., Fixed-to-Deployable calls, the use of different voice sample lengths and voice payload packet sizes is negotiated during call setup via the Session Description Protocol (SDP).

As an example, for a Fixed-to-Fixed call using the G.711 codec, the 64-Kbps codec rate multiplied by the 20-ms sample length equals 1280 bits, or 160 bytes of voice payload packet size (where payload does not include SRTP, UDP, and IP packet header fields). This results in a packet-per-second rate (where "packet" means payload packet) of one packet every 20 ms equals 50 packets per second (PPS).

For a Deployable-to-Fixed call, the Navy may use the G.729 (8-Kbps) codec to minimize the bandwidth required on a ship-to-shore satellite link, and may use a 50-ms voice sample length. This results in an 8-Kbps codec rate multiplied by a 50-ms sample length equals 400 bits, or 50 bytes of voice packet payload size. This results in a PPS rate of one payload packet every 50 ms equals 20 PPS.

Using the 24-Kbps version of the G.722.1 codec with a 20-ms voice sample frame length, and two frames per packet, results in a packet-per-second rate of 25 PPS (one packet per every 40 ms). Each packet has 960 bits, or 120 bytes, of payload.

The 32-Kbps G.722.1, with a 20-ms frame length and two frames per packet, also has a 25 PPS rate, but each packet has 1280 bits, or 160 bytes, of payload.

The G.723.1 codec has two bit rates: 5.3- and 6.3-Kbps. Both use a frame size of 30 ms. At one frame per packet, the PPS rate is 33.3. The payload for the low bit rate version is 20 bytes and the payload for the high bit rate version is 24 bytes.

2.7.2 Operational Framework for AS-SIP EIs

This section describes a framework for how voice EIs, secure voice EIs, and video EIs (also known as video codecs) connect to, and interoperate with any VVoIP vendor's SC, using AS-SIP protocol instead of the various vendor-proprietary SC-to-EI protocols.
The basic change needed to support AS-SIP EIs is to add SC-to-AS-SIP-EI interfaces where proprietary SC-to-EI interfaces are currently supported:

- The SC CCA (called just the SC here).
- The Voice EI (for both the hardphone EI and the softphone EI).
- The Secure Voice EI (hardphone EI only).
- The Video EI (for both the hardphone EI and the softphone EI).

Secure video EIs (e.g., Video EIs that use SCIP to encrypt video media streams) are outside the scope of this section.

AS-SIP EI capabilities do not need to be supported in the following VVoIP NEs:

- The MG-Transport Switching (TS) and MG-MG-LAN Switch (LS).
- TAs.
- IADs.

The signaling interfaces between the SC CCA and the MG-TS, between the SC CCA and the MG-LS, between the SC CCA and the TA, and between the SC CCA and the IAD are vendor-proprietary.

Figure 2.7-1, Framework for Proprietary and Generic AS-SIP EIs, shows the support for AS-SIP EIs in a UC network (using multivendor-interoperable AS-SIP SC-EI signaling). The UC network still supports vendor-proprietary EIs using vendor-proprietary SC-EI signaling. As a result, both proprietary EIs using proprietary signaling and AS-SIP EIs using AS-SIP signaling are shown in Figure 2.7-1.

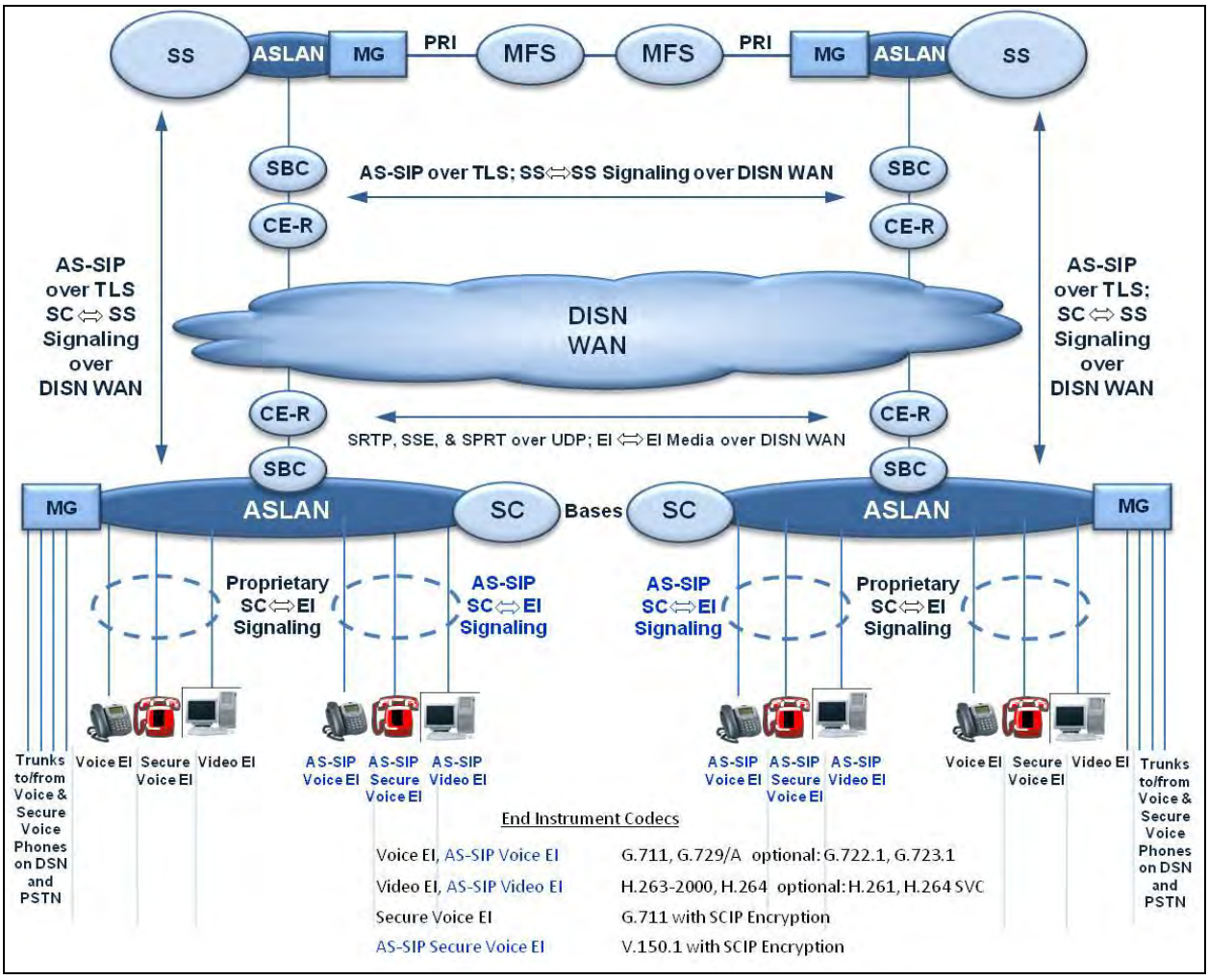

Figure 2.7-1. Framework for Proprietary and AS-SIP EIs

2.7.2.1 AS-SIP Secure Voice EI Supplementary Services

SCs support the following supplementary services for voice calls on AS-SIP secure voice EIs, consistent with Section 2.6, Assured Services Voice Features and Capabilities, using AS-SIP signaling:

- Precedence Call Waiting.
- Call Forwarding.
- Call Transfer.
- Call Hold.
- Three-Way Calling.
- Calling Number Delivery.
- Call Pickup.

SCs and SSs, which are in the session signaling path but not in the session media path, cannot make any distinctions between voice calls ("clear voice" calls) and secure voice calls at an AS-SIP secure voice EI. This limitation occurs because a secure voice call always starts off as a voice call first, and then later converts from a voice call to a secure voice call after an end-to-end exchange of V.150.1 SSE messages in the media path (and not in the signaling path). As a result, if an SC provides a supplementary service to an AS-SIP EI for voice calls, the SC also provides that supplementary service to the AS-SIP EI for secure voice calls (since the SC on its own cannot distinguish between a voice call at an AS-SIP EI and a secure voice call at that AS-SIP EI).

A AS-SIP Secure voice EI, however, can distinguish between a voice call (a call in "clear-voice" mode) and a secure voice call. So the AS-SIP secure voice EI can prevent the use of a supplementary service on secure voice calls (like Call Hold, Call Transfer, or TWC), where the use of that service can "break" the media path between the calling and called EIs (SCIP end points) and cause the secure voice call to fail. But the secure voice EI can also allow the use of a supplementary service on secure voice calls by requiring the end user to return the secure voice call to a voice call (a "clear-voice" call) so that the supplementary service can be used.

2.7.3 V.150.1 Modem Relay Secure Phone

This section describes the architecture for V.150.1 Modem Relay support by UC MGs of SCIP-based secure phones for all scenarios required by the National Security Agency (NSA).

V.150.1 Secure Phone Support relies on the following:

- SCIP-216 Modem Relay capabilities in UC MGs, TAs, and IADs.
- SCIP-215 Modem Relay capabilities in UC SEI.

V.150.1 is an ITU Recommendation that describes different methods for carrying Modem traffic over IP networks. SCIP-215 and SCIP-216 are the NSA's technical documents on "V.150.1 Minimum Essential Requirements (MER) for VoIP Gateways" and "V.150.1 MER for VoIP Secure Phones," respectively.

V.150.1 supports three different methods or modes for carrying modem traffic over IP networks:

- Audio.
- Voiceband Data (VBD).
- Modem Relay.

2.7.3.1 Architecture for Supporting SCIP/V.150.1 Modem Relay

Support for SCIP phones and V.150.1 is achieved by adding Modem Relay capabilities to the following UC NEs:

1. Media Gateway – Trunk Side (MG-TS). The portion of the MG that provides trunk-side connections to the DSN and the PSTN using Integrated Services Digital Network (ISDN) PRI and Channel Associated Signaling (CAS) Trunk Groups.
2. Media Gateway – Line Side (MG-LS). The portion of the MG that provides line-side connections to analog phones, analog secure phones, analog fax machines, and analog modems on the B/P/C/S, using analog line cards at the MG and the existing twisted-pair copper-wire plant at the B/P/C/S. Support for Modem Relay in the MG-LS is optional in the UCR.
3. Analog Terminal Adapter (ATA). A device on the UC end user's premise that supports interconnection between the ASLAN and the end user's analog phone, analog secure phone, analog fax machine, or analog modem. This device supports a single RJ-45 Ethernet interface on the ASLAN side and a single analog RJ-11 interface on the end user side. Support for modem relay in the ATA is optional in the UCR.
4. Integrated Access Device (IAD). A device on the end user's premise that supports interconnection between the ASLAN and multiple end user analog telephones, analog secure telephones, analog fax machines, and analog modems. This device supports a single Ethernet RJ-45 interface on the ASLAN side, and multiple analog RJ-11 interfaces on the end user side. Support for modem relay in the IAD is optional in the UCR.
5. AS-SIP Components of the SC and SS. The SC and SS CCAs must support new AS-SIP and SDP signaling for modem relay calls. Additional SDP lines for the modem relay media type are added to existing SDP lines for the audio media type in AS-SIP INVITE, UPDATE, 180 (Ringing), 183 (Session Progress), 200 (OK), and Acknowledgement (ACK messages).

Modem relay capabilities do not need to be added to the SBC. The SBCs only need to ensure the transparent passing of the V.150.1 Simple Packet Relay Transport (SPRT) and State Signaling Event (SSE) messages in modem relay media streams. This can be accomplished in UC by having the modem relay endpoints (MGs, TAs, IADs, and IP SCIP Phones) make secure SCIP calls using the same UDP port and protocol numbers for the nonsecure portion of the call (which uses Secure Real Time Protocol (RTP) for media transfer and Secure RTCP for media control) and the secure portion of the call (which uses SPRT and SSE for media transfer and does not use Secure RTCP for media control). Having the modem relay end points use the same UDP port and protocol numbers for the unsecure and secure portions of the call should make passing of modem relay SPRT and SSE messages transparent to SBCs.

When a nonsecure call is established between two IP media endpoints, a Secure RTP media stream is established using one UDP port number and a Secure RTCP media control stream is established using a second UDP port number. The SBC (when the media traverses an SBC) opens a UDP pinhole for the Secure RTP traffic and another UDP pinhole for the Secure RTCP traffic. When the call transitions from nonsecure (clear) voice using SRTP to secure voice using SPRT, the SPRT media stream reuses the UDP port number and SBC pinhole that were previously used by the SRTP media stream. The Secure Real-Time Transport Control Protocol (SRTCP) is turned off during this transition but the UDP port number used for the SRTCP media

control stream is maintained by the IP media endpoints and the UDP pinhole for the SRTCP media control stream is maintained by the SBC until the call is terminated. The port number and pinhole are maintained so that if the call transitions back to nonsecure voice, the RTCP port number and RTCP pinhole can be reused. In other words, if the call transitions from secure voice using SPRT back to nonsecure voice using SRTP, the new SRTP media stream reuses the UDP port number and SBC pinhole that were previously used by the original SRTP media stream. There also is a new SRTCP media control stream after this transition and the separate UDP port number for SRTCP is reused by the IP endpoints and the separate pinhole for SRTCP is reused by the SBC. One other architecture change is the addition of Secure IP Phones to the UC Network. Here, these Secure IP Phones are called IP SCIP Phones also.

Figure 2.7-2, Framework for SCIP Phones in Using VoIP, and Figure 2.7-3, Framework for SCIP Phones Using Modem Relay, show the frameworks for supporting analog and IP SCIP Phones in a VoIP network and a Modem Relay network, using modem relay media and either proprietary Phone-to-SC signaling or AS-SIP Phone-to-SC signaling. The Modem Relay network continues to support audio media in MGs, ATAs, IADs, SCs, and SBCs for backward compatibility with VoIP network operation.

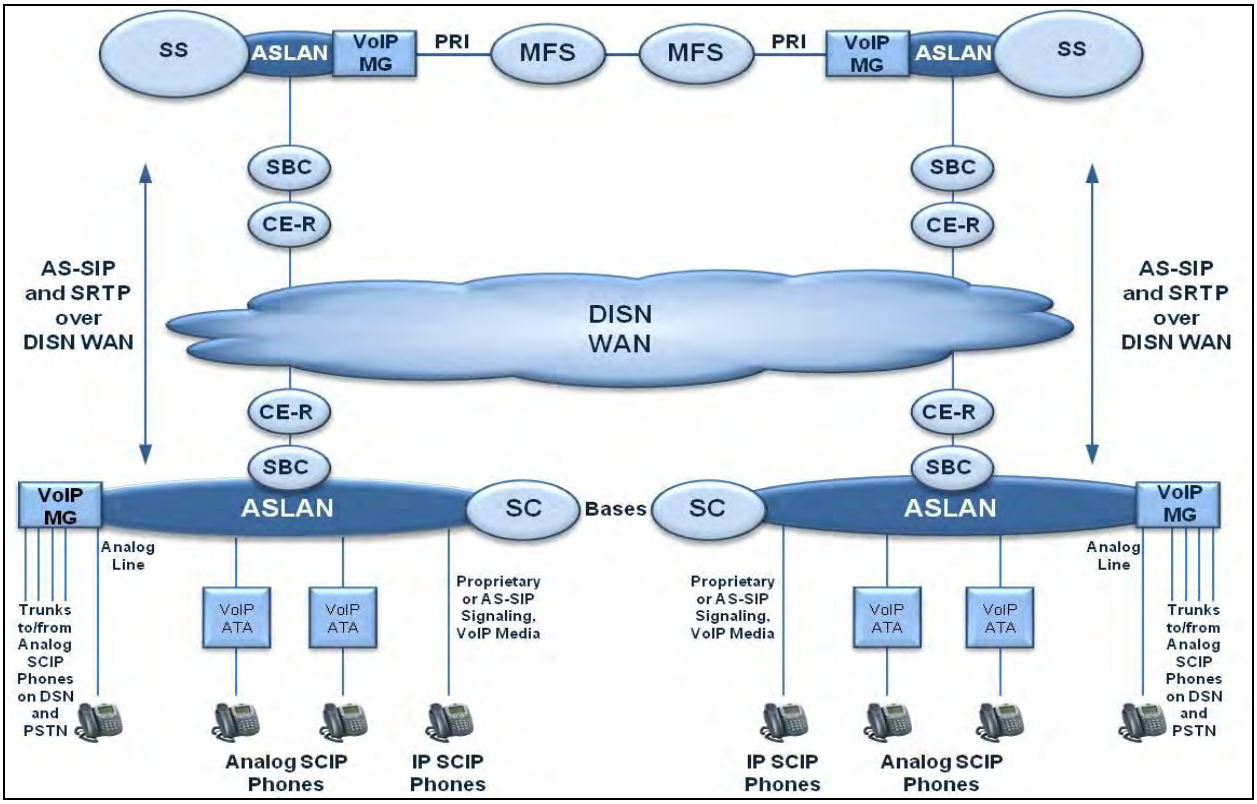

Figure 2.7-2. Framework for SCIP Phones Using VoIP

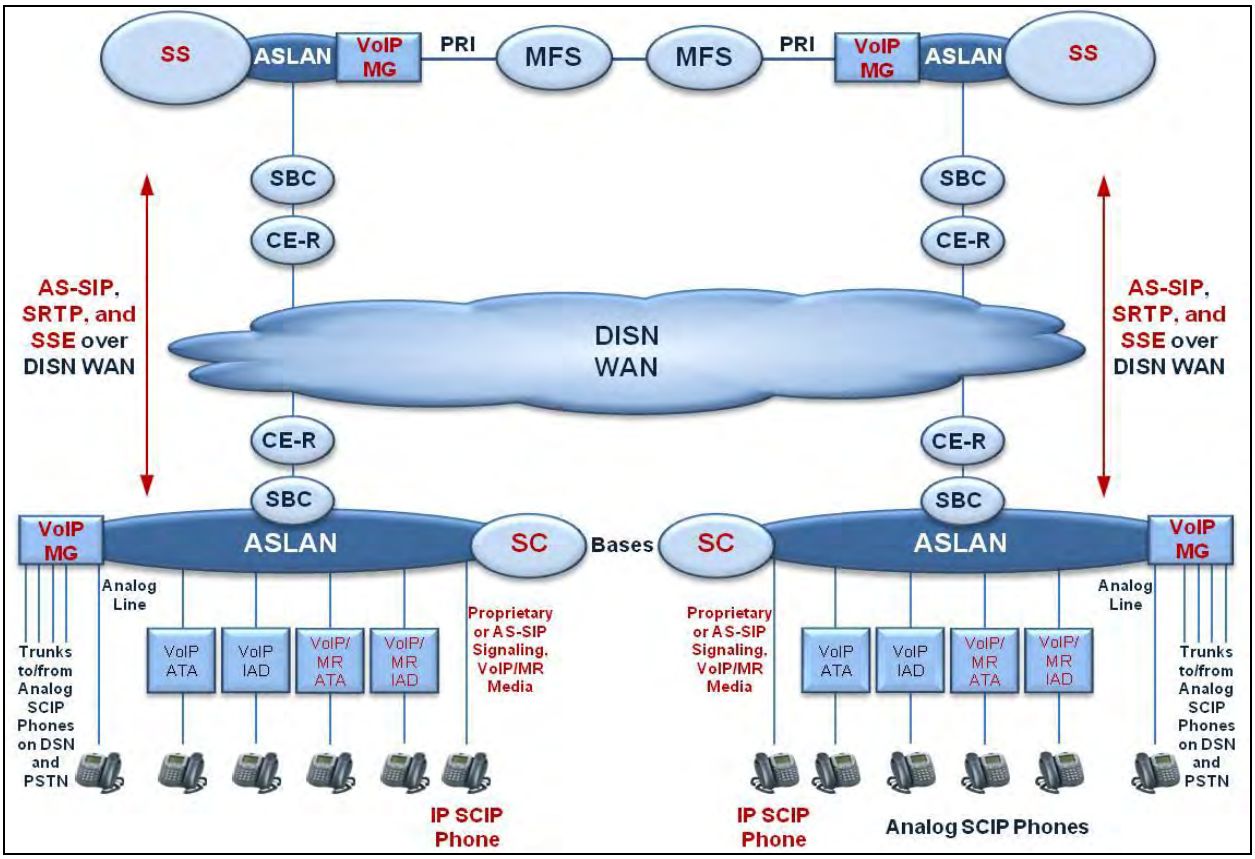

Figure 2.7-3. Framework for SCIP Phones Using Modem Relay

2.7.3.2 SCIP/V.150.1 Gateway

For UCR purposes, a "SCIP Gateway" is any VoIP Gateway that conforms to SCIP-216, Revision 2.1. SCIP Gateways may be used on the PSTN or on the DSN. An example of a SCIP Gateway is a VoIP Trunk Gateway that supports SCIP-216, is connected to a base IP LAN, and receives trunk-side service from a TDM switch on the Base.

For UCR purposes, a "SCIP/V.150.1 Gateway" is a VoIP Gateway that conforms to SCIP-216 and is served by an SC. Media Gateways, ATAs, and IADs that support SCIP-216 and are served by an SC are examples of SCIP/V.150.1 Gateways.

One key difference between the SCIP Gateway and the SCIP/V.150.1 Gateway is that the SCIP Gateway only supports trunk-side connections to the PSTN and the DSN. The SCIP/V.150.1 Gateway not only supports these trunk-side connections, but also supports line-side connections to analog phones, analog secure phones, analog fax machines, and analog modems.

SCIP/V.150.1 Gateways are expected to be deployed in both Strategic (Fixed) networks and Tactical (Deployable) networks.

2.7.3.3 SCIP/V.150.1 End Instrument

The UC SCIP/V.150.1 End Instrument (EI), is based on NSA document SCIP-215, Revision 2.1. All references to "SCIP-215" in the following paragraphs are references to SCIP-215, Revision 2.1.

In the UCR, a "SCIP EI" is any Secure IP Phone that conforms to SCIP-215. The SCIP EIs may be used on commercial VoIP networks or on the DSN. An example of a SCIP EI is a Secure IP Phone that supports SCIP-215, is connected to a base IP LAN, and receives line-side VoIP service from a TDM DSN switch on the base.

In the UCR, a "SCIP/V.150.1 EI" is a Secure IP Phone that conforms to SCIP-215 and is served by an SC.

A SCIP/V.150.1 EI communicates with the SC using either vendor-proprietary signaling and transport protocols or AS-SIP signaling over TLS.

A SCIP EI might communicate only with a TDM switch on the base (which provides DSN line-side VoIP) using vendor-proprietary signaling and transport protocols.

A SCIP/V.150.1 EI also exchanges media with other EIs, MGs, ATAs, and IADs using SRTP over UDP during the audio part of the call ("talking in the clear"), and using SSE and SPRT over UDP during the modem relay part of the call ("talking secure"). A SCIP EI on a commercial VoIP network or the DSN might instead exchange media with other SCIP end points using RTP over UDP during the audio part of the call, and using SSE and SPRT over UDP during the modem relay part of the call.

SCIP/V.150.1 EIs are expected to be deployed in both Strategic (Fixed) networks and Tactical (Deployable) networks.

It is also possible for two SCIP/V.150.1 EIs to communicate with one another over the UC VVoIP network using the SCIP-214.2 protocol, as defined in the NSA document SCIP 214.2, Secure Communication Interoperability Protocol (SCIP) over Real-Time Transport Protocol (RTP), Revision 1.0, January 2010.

Unlike SCIP-216 and SCIP-215, SCIP-214.2 does not use V.150.1 Modem Relay, SPRT, or SSE to exchange media over a VVoIP network. Instead, the SCIP media stream packets are sent from one EI to another over the VVoIP network, and do not traverse any SCIP/V.150.1 Gateways.

Before the call "goes secure," the media stream packets are exchanged between the two EIs using a VoIP codec (like G.711 or G.729) over Secure RTP. After the call goes secure, the media stream packets are exchanged between the two EIs using SCIP over Secure RTP, instead of using SCIP over SPRT. This means that the "clear voice to secure voice" transition only involves a change from a VoIP codec to the SCIP protocol; Secure RTP is used for media transport both before and after the transition.

In addition, this means that EI transitions from "clear voice" to "secure voice" and back again are transparent to SBCs, because SRTP is used to transport the media packets (and SRTCP is used to transport the media control packets) both in "clear voice" mode and in "secure voice" mode.

The SCIP-214.2 support is optional for SCIP/V.150.1 EIs in the UCR.

SCIP/V.150.1 EIs may use SCIP-214.2 to communicate in both Strategic (Fixed) networks and Tactical (Deployable) networks.

2.8 SESSION CONTROLLER

The Session Controller (SC) is a software-based call processing product that provides voice and video services to IP telephones and media processing devices within a service domain. Additionally, an SC extends signaling and session (call) control services to allow sessions to be established with users outside the local service domain. Connectivity to external networks outside a local service domain is provided via gateways to non-IP networks, or to an IP-based long-haul network.

SCs that provide Hosted UC voice and video services to end instruments (EIs) located at different enclaves (i.e., B/P/C/S locations) within a designated geographic region are called ESCs. The region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations is referred to as the Enterprise Services Area (ESA).

Local SCs are physically located at the B/P/C/S where the EIs they serve are located.

Multiple SCs may be deployed at a single serving area in a coordinated cluster with one SC acting as the Master SC (MSC) and the others – Subtended Session Controllers (SSCs) – subordinate to the MSC. MSC/SSC clusters may be used in both Strategic (Fixed) deployments and within tactical extensions of the DISN.

The SC software and functions may be distributed physically among several high-availability server platforms with redundant call management modules and subscriber tables to provide robustness.

Figure 2.8-1, Functional Reference Model – SC, illustrates the reference model for the Session Controller.

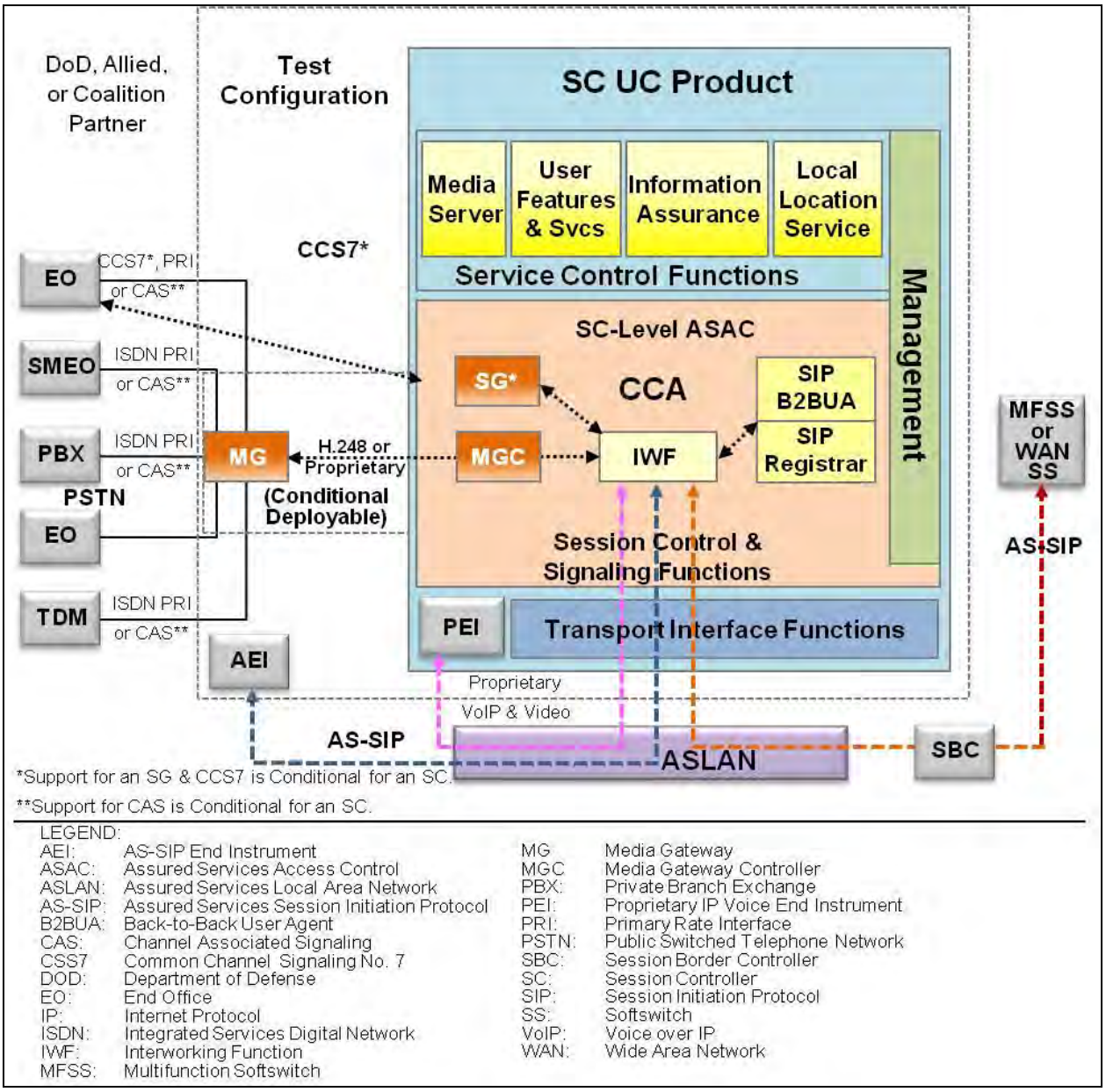

Figure 2.8-1. Functional Reference Model – SC

The SC provides voice functions and features similar to a DSN EO switching system. Line-Side (Local) Custom Calling features implemented at a vendor's discretion must not interfere with the functional requirements specified within Table 2.8-1, Summary of SC Functions, provides a summary of SC functions.

Table 2.8-1. Summary of SC Functions

FUNCTION	DESCRIPTION
Session Control and Signaling	Verifies call request is consistent with policy rules call management, CAC, AS-SIP signaling function serving PEIs and AEIs: B2BUA or Call Stateful Proxy Server (assumes that some EIs will not use AS-SIP; AS-SIP used on "trunk side"), intermediary in all inbound and outbound signaling messages to/from the PEI or AEI Requests network resources Signaling interworking [optional] H.323, H.248 PRI, MGCP
ASAC	Executes AS functions via control of the PEI and AEI. Determines and performs preemption where required. Maintains local active session state knowledge (session precedence level, CoS, local access bandwidth used and available).
Network Management	Provides traffic call information to, and responds to traffic flow control commands from, an EMS.
Local Domain Directory	Subscriber information, including telephone number, organization name, code address, and subscriber name.
MGC	Controls the MG when the MG in included in the SC.
PEI, AEI, and User Registration	Information Assurance; access control information for authentication and authorization; PEI and AEI registration: User identification, authentication, and authorization; numbering and addressing information; user profile; CoS; precedence level.
Dialing, numbering, and routing tables; UFS Administration	Dialing, numbering, and routing tables (location services for sending call requests) regarding local calling features, multiple line appearances, voice mail, and speed call.

LEGEND

AEI: AS-SIP Voice End Instrument	CoS: Class of Service	PEI: Proprietary IP Voice End Instrument
AS: Assured Services	EI: End Instrument	RTS: Real Time Services
ASAC: Assured Services Admission Control	EMS: Element Management System	SBC: Session Border Controller
AS-SIP: Assured Servies Session Initiation Protocol	IA: Information Assurance	SC: Session Controller
B2BUA: Back-to-Back User Agent	MG: Media Gateway	UFS: User Features and Services
CAC: Call Admission Control	MGC: Media Gateway Controller	
CE: Customer Edge	MGCP: Media Gateway Control Protocol	

Table 2.8-2, SC Support for VoIP and Video Signaling Interfaces, provides a complete list of the SC signaling interfaces.

Table 2.8-2. SC Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (SC)-to-CCA (SS)	AS-SIP over IP
CCA	CCA (SC)-to-PEI	Proprietary VoIP Signaling over IP
CCA	CCA (SC) to AEI	AS-SIP over IP
CCA/MGC and MG	CCA (MGC)-to-MG	ITU-T H.248 over IP (Optional - used with ISDN PRI, and CAS trunks)
CCA/MGC and MG	CCA (MGC)-to-MG	ISDN PRI over IP (Optional - North American National ISDN Version, used with ISDN PRI trunks only)
CCA/MGC and MG	CCA (MGC)-to-MG	Proprietary Supplier Protocols (used as an alternative to ITU-T Recommendation H.248 over IP and ISDN PRI over IP)

LEGEND

AEI: AS-SIP IP Voice End Instrument	ISDN: Integrated Services Digital Network	PEI: Proprietary IP Voice End Instrument
AS-SIP: Assured Services Session Initiation Protocol	ITU-T: International Telecommunications Union – Telecommunication	PRI: Primary Rate Interface
CAS: Channel Associated Signaling	MG: Media Gateway	SC: Session Controller
CCA: Call Connection Agent	MGC: Media Gateway Controller	SS: Softswitch
DoD: Department of Defense		VoIP: Voice over IP
IP: Internet Protocol		

The SC supports a Session Controller Location Server (SCLS) functionality that provides information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information maintained by the SCLS to route the following:

- Internal calls from one SC PEI or AEI to another PEI or AEI on the same SC.
- Outgoing calls from an SC PEI or AEI to another SC, an SS, or a TDM network.
- Incoming calls from another SC, an SS, or a TDM network to an SC PEI or AEI.

2.9 AS-SIP GATEWAYS

2.9.1 AS-SIP TDM Gateway

2.9.1.1 Overview

The AS-SIP TDM Gateway is a VVoIP appliance, and its purpose is to enable the interconnection and interoperation of a traditional TDM switch with the DISN UC system. The AS-SIP TDM Gateway performs interworking for voice and video sessions in both the signaling plane and the bearer plane. The AS-SIP TDM Gateway does not support interworking of IP-based signaling platforms and does not support or serve any TDM EIs or IP EIs.

Figure 2.9-1, AS-SIP TDM Gateway Topologies, depicts examples of the two basic topologies that use the AS-SIP TDM Gateway. The first example depicts a B/P/C/S having one Assured Services, precedence-capable TDM switch that interfaces with the AS-SIP TDM Gateway over ISDN MLPP PRI trunks. The second example depicts a B/P/C/S with multiple TDM switches that may include a PBX2 as well as MLPP-capable TDM switches. One Assured Services, precedence-capable TDM switch interfaces with the AS-SIP TDM Gateway over ISDN MLPP PRI trunks, and the other TDM switches interface with the TDM switch connected to the AS-SIP TDM Gateway. A PBX2 (or any other non-assured services TDM switch) is not permitted to directly interface with an AS-SIP TDM Gateway.

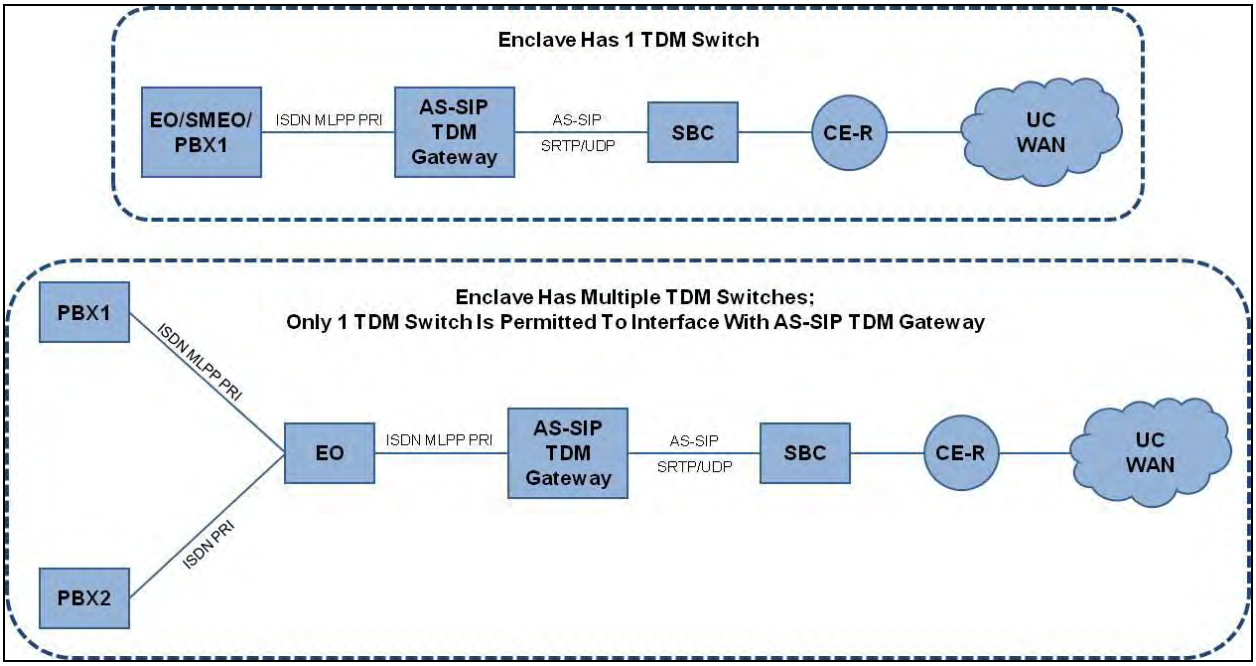

Figure 2.9-1. AS-SIP TDM Gateway Topologies

The AS-SIP TDM Gateway does not support ASAC and relies on the subtended TDM switch to perform that functionality. Appropriate traffic engineering must be performed with respect to the TDM trunks that interface to the AS-SIP TDM Gateway to ensure that the total number of DS0s available for serving calls via the AS-SIP TDM Gateway does not exceed the bandwidth constraints of the access link between the CE-R and the AR.

The SS that serves the AS-SIP TDM Gateway performs standard ASAC policing of the AS-SIP TDM Gateway.

2.9.1.2 AS-SIP TDM Gateway Functional Reference Model

Figure 2.9-2, Functional Reference Model – AS-SIP TDM Gateway, shows the reference model for the AS-SIP TDM Gateway. The AS-SIP TDM Gateway consists of several SCS functions performed by the CCA, Interworking Function (IWF), MGC, and MG. These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport

systems (via an ASLAN), and DISA's VVoIP NMS (Advanced DSN Integrated Management Support System [ADIMSS]) are provided by external interfaces.

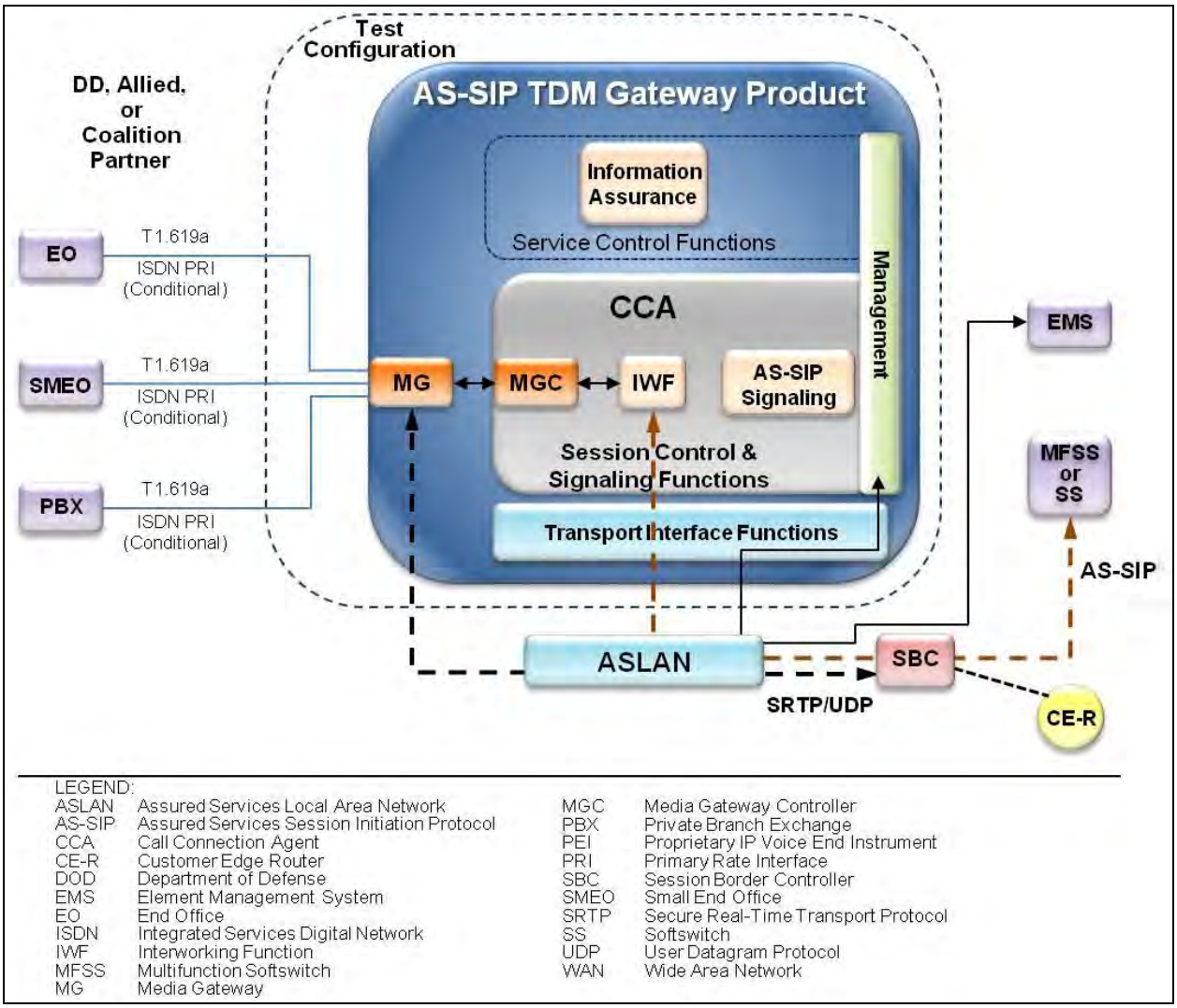

Figure 2.9-2. Functional Reference Model – AS-SIP TDM Gateway

The MGC and IWF are both components of the CCA. The MGC is responsible for controlling the MG in the AS-SIP TDM Gateway and the ISDN MLPP PRI TDM trunk groups that are connected to it. The IWF is responsible for supporting all the VoIP and TDM signaling protocols in the AS-SIP TDM Gateway, and for interworking the different protocols together (see Table 2.9-1).

Table 2.9-1. AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (AS-SIP TDM Gateway) – to – CCA (SS)	AS-SIP over IP

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA/MGC and MG	CCA (MGC) – to – MG	Internal interface to integrated MG functional component (used with ANSI T1.619a PRI trunks and optional non-ANSI T1.619a PRI trunks)

LEGEND

ANSI: American National Standards Institute	IP: Internet Protocol	PRI: Primary Rate Interface
AS-SIP: Assured Services Session Initiation Protocol	MG: Media Gateway MGC: Media Gateway Controller	SS: Softswitch TDM: Time Division Multiplexing
CCA: Call Connection Agent	MLPP: Multilevel Precedence and Preemption	

2.9.2 AS-SIP IP Gateway

2.9.2.1 Overview

The AS-SIP IP Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of proprietary IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support end-to-end voice and video sessions. The AS-SIP IP Gateway directly interfaces with only one IP-based UC signaling platform. It does not support interworking of TDM-based signaling platforms, and does not serve as a call manager for any TDM or IP EIs.

Unlike the AS-SIP TDM Gateway, the AS-SIP IP Gateway is not an Assured Services appliance.

The AS-SIP IP Gateway System Under Test (SUT) consists of the AS-SIP IP Gateway, the proprietary UC signaling platform, and the IP EIs served by the proprietary UC signaling platform.

The AS-SIP IP Gateway interfaces to an SBC in both the signaling plane and the bearer plane and is responsible for interworking AS-SIP voice and video signaling with the voice and video signaling of the proprietary UC signaling platform, and UCR-compliant voice and video media packets with the voice and video media packets supported by the proprietary UC signaling platform's IP EIs. Interoperability of UC features and services other than non-assured voice and video services is outside the scope of the required functionality for the AS-SIP IP Gateway.

Figure 2.9-3, AS-SIP IP Gateway Topology, depicts the AS-SIP IP Gateway in relation to the UC WAN where the logical interface is between the AS-SIP IP Gateway and the SBC. The internal signaling and media lines (in blue) represent notional internal connectivity options.

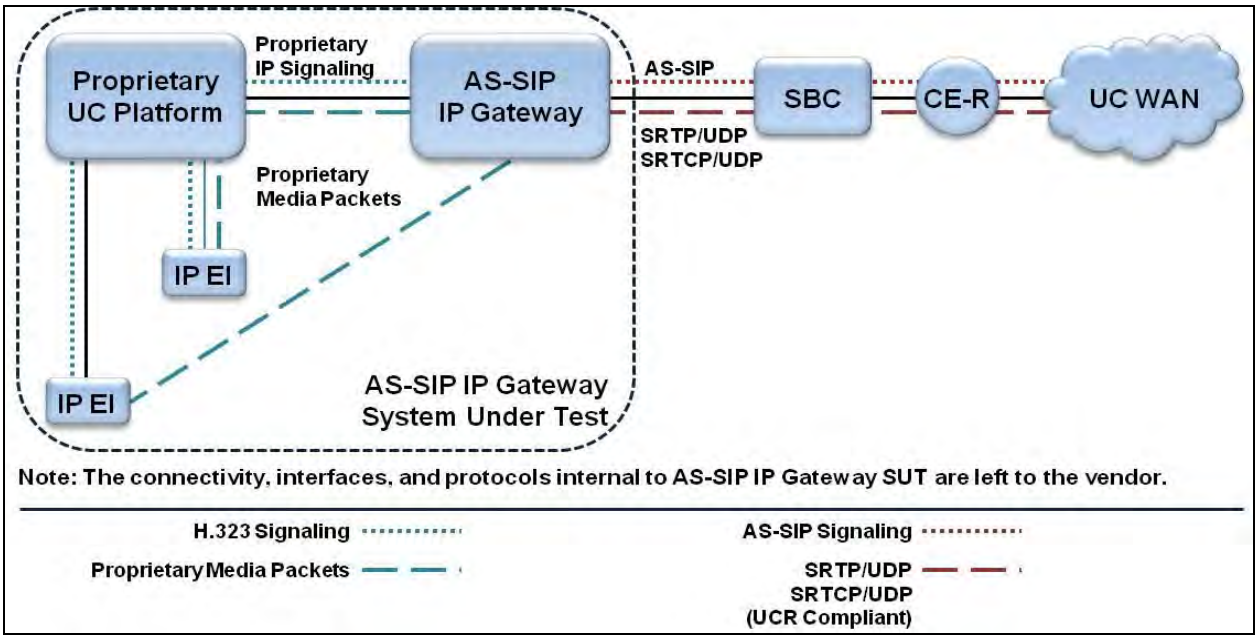

Figure 2.9-3. AS-SIP IP Gateway Topology

2.9.2.2 AS-SIP IP Gateway Functional Reference Model, Assumptions, Functions and Features

Figure 2.9-4 shows the reference model for the AS-SIP IP Gateway. The AS-SIP IP Gateway consists of several SCS functions performed by the CCA, IWF (for signaling), and IWF (for media). These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport systems (via an ASLAN), and DISA's VVoIP NMS (ADIMSS) are provided by external interfaces.

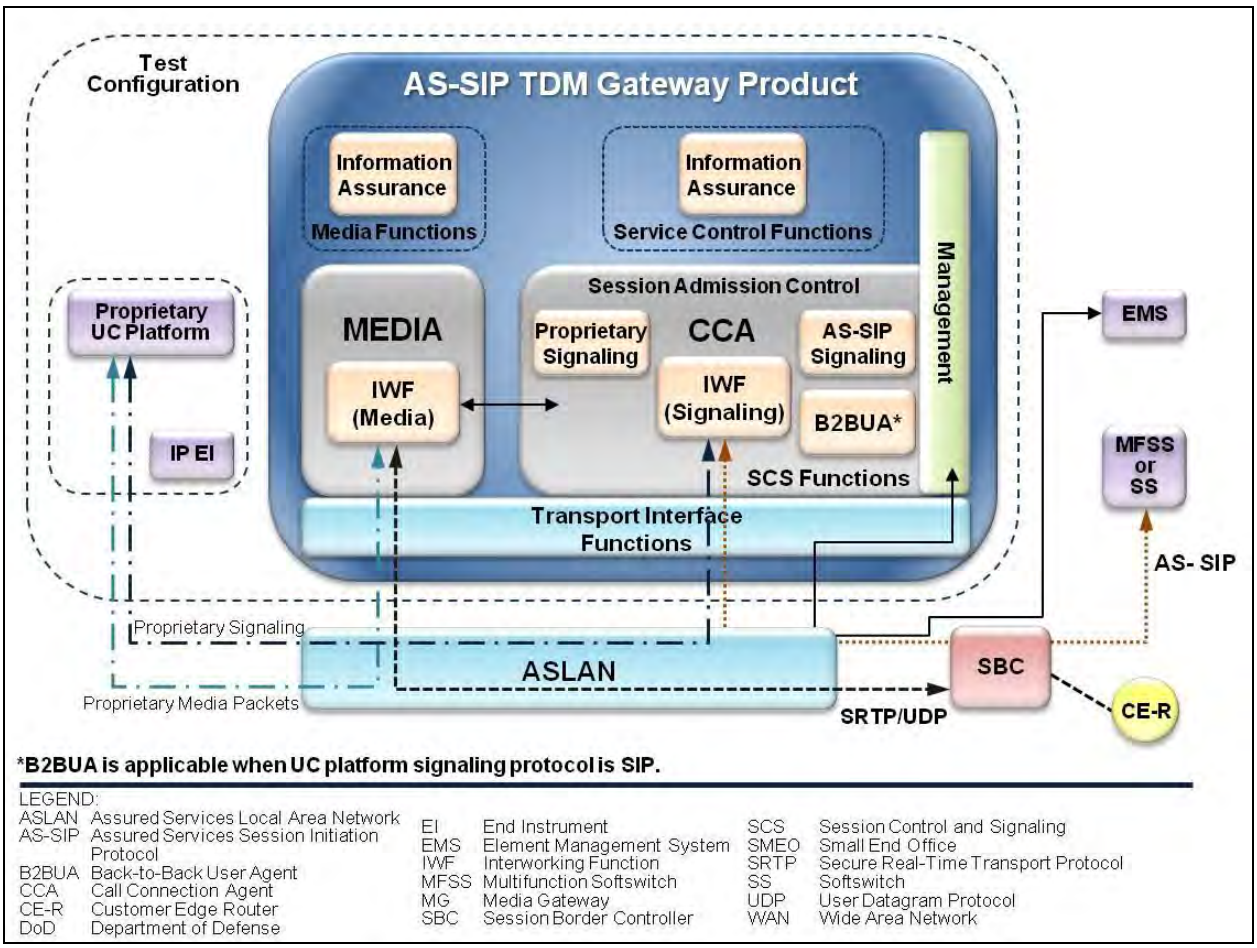

Figure 2.9-4. Functional Reference Model – AS-SIP IP Gateway

2.9.2.2.1 Assumptions

The following assumptions are made based on the AS-SIP IP Gateway reference model:

1. The AS-SIP IP Gateway interfaces with only one proprietary UC signaling platform.
2. The proprietary UC signaling platform has no other connectivity to the UC WAN aside from the AS-SIP IP Gateway.
3. Each functional component in the AS-SIP IP Gateway has associated management-related functions for Fault, Configuration, Accounting, Performance, and Security (FCAPS) management and audit logs.
4. The CCA interacts with the Service Control functions using internal interfaces and proprietary protocols that vary from one supplier's solution to another.
5. The AS-SIP IP Gateway interactions with its SBC are as follows:

a. The SBC controls signaling streams between the AS-SIP IP Gateway and a SS. The AS-SIP IP Gateway accesses the UC WAN via the SBC and an associated AR on the UC WAN.

b. The SBC controls media streams between the AS-SIP IP Gateway and other AS-SIP IP Gateways, or the EIs and MGs of SCs (whose separate ASLANs are connected to the DISN UC WAN).

2.9.2.2.2 Summary of AS-SIP IP Gateway Functions and Features

The AS-SIP IP Gateway provides interworking functions for the signaling and bearer planes (see Table 2.9-2, Summary of AS-SIP IP Gateway Functions).

Table 2.9-2. Summary of AS-SIP IP Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (proprietary to AS-SIP; AS-SIP to proprietary)
SAC	Maintains call thresholds Maintains active session state knowledge (local access bandwidth used and available, direction, session type: voice, video)
Media IWF	Converts proprietary media packets to UCR-compliant IP/UDP/SRTP packets Converts UCR compliant IP/UDP/SRTP packets to proprietary media packets
NM	Provides traffic call information to, and responds to traffic flow control commands from, an EMS

LEGEND	SAC: Session Admission Control
AS-SIP: Assured Services Session Initiation Protocol	SCS: Session Control and Signaling
EMS: Element Management System	SRTP : Secure Real-Time Transport Protocol
IP: Internet Protocol	UCR: Unified Capabilities Requirements
IWF: Interworking Function	UDP: User Datagram Protocol
NM: Network Management	

2.9.3 AS-SIP – H.323 Gateway

2.9.3.1 Overview

The AS-SIP – H.323 Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of H.323 IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support end-to-end voice and video sessions.

The Government has adopted Request for Change (RFC) 4123 – Session Initiation Protocol (SIP) – H.323 Interworking Requirements as the document which describes the requirements for the AS-SIP – H.323 Gateway.

NOTE: The AS-SIP – H.323 Gateway is not an Assured Services appliance because H.323 is not an Assured Services protocol, and its placement in this section is for requirements grouping

purposes and should not be interpreted as implying that the AS-SIP – H.323 Gateway is an Assured Services appliance.

The AS-SIP – H.323 Gateway is a standalone SUT for testing purposes.

The AS-SIP H.323 Gateway interfaces to the SBC in both the signaling plane and the bearer plane and is responsible for interworking AS-SIP voice and video signaling with the voice and video signaling of the H.323 UC signaling platform. The AS-SIP – H.323 Gateway is responsible for interworking UCR-compliant voice and video media packets with the voice and video media packets supported by the H.323 UC signaling platform's IP EIs. Interoperability of UC features and services other than non-assured voice and video services is outside the scope of the required functionality for the AS-SIP – H.323 Gateway and will not be a part of AS-SIP H.323 Gateway SUT interoperability testing.

From a signaling perspective, the AS-SIP – H.323 Gateway provides a AS-SIP-compliant signaling interface for end-to-end signaling interoperability between the AS-SIP – H.323 Gateway and the AS-SIP signaling appliances of the DISN UC WAN system.

From a media perspective, the AS-SIP – H.323 Gateway provides a UCR-compliant bearer interface for end-to-end interoperability of voice and video media packets between the AS-SIP – H.323 Gateway and SBCs, IP EIs of SCs, MGs, and AS-SIP EIs. The AS-SIP – H.323 Gateway interworks voice and video media packets generated by the IP EIs served by the IP-based UC signaling platform that are intended for a destination outside the H.323 system enclave, to UCR-compliant SRTP/UDP packets having the appropriate DSCP. Similarly, UCR-compliant SRTP/UDP voice and video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform are interworked by the AS-SIP – H.323 Gateway into the H.323 media packets supported by the IP EIs.

Figure 2.9-5, AS-SIP – H.323 Gateway Topology, depicts the AS-SIP – H.323 Gateway in relation to the UC WAN where the logical interface is between the AS-SIP – H.323 Gateway and the SBC. Signaling and media lines in blue represent notional internal connectivity options.

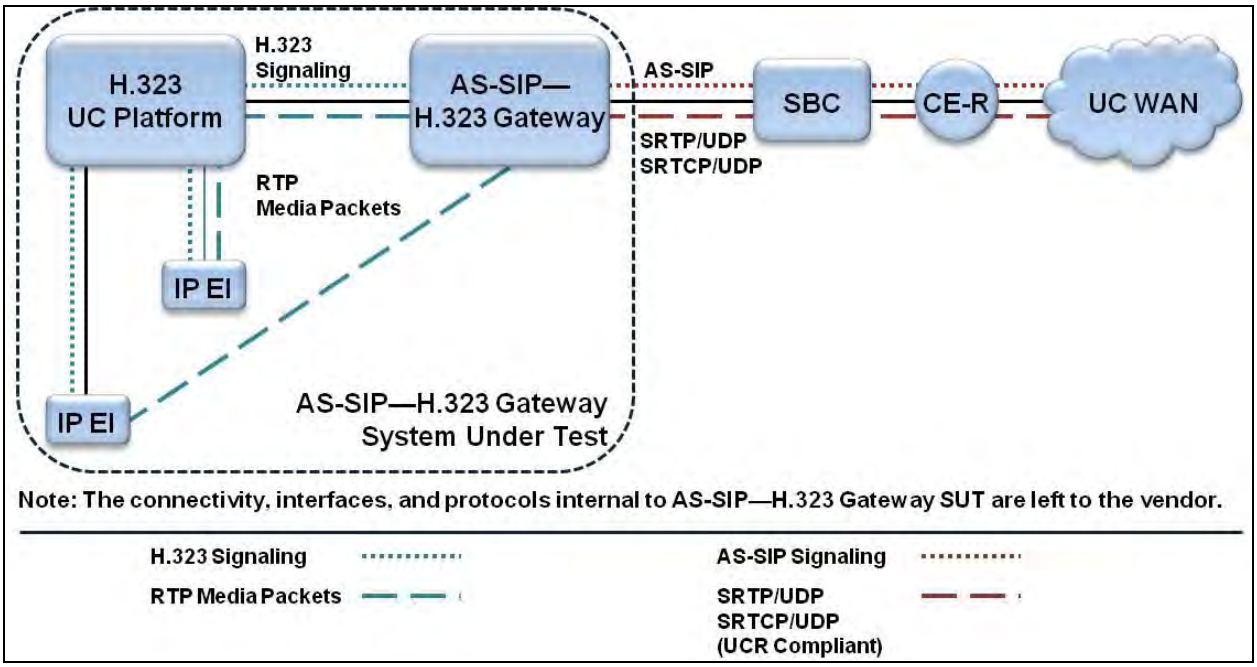

Figure 2.9-5. AS-SIP – H.323 Gateway Topology

The AS-SIP – H.323 Gateway maintains call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC).

2.9.3.2 AS-SIP – H.323 Gateway Functional Reference Model

Figure 2.9-6, Functional Reference Model – AS-SIP – H.323 Gateway, shows the reference model for the AS-SIP – H.323 Gateway. The AS-SIP – H.323 Gateway consists of several SCS functions performed by the CCA, IWF (for signaling), and IWF (for media). These are connected via H.323 internal interface functions. Connectivity to other networks, long-haul transport systems (via an ASLAN), and DISA's VVoIP NMS (ADIMSS) are provided by external interfaces.

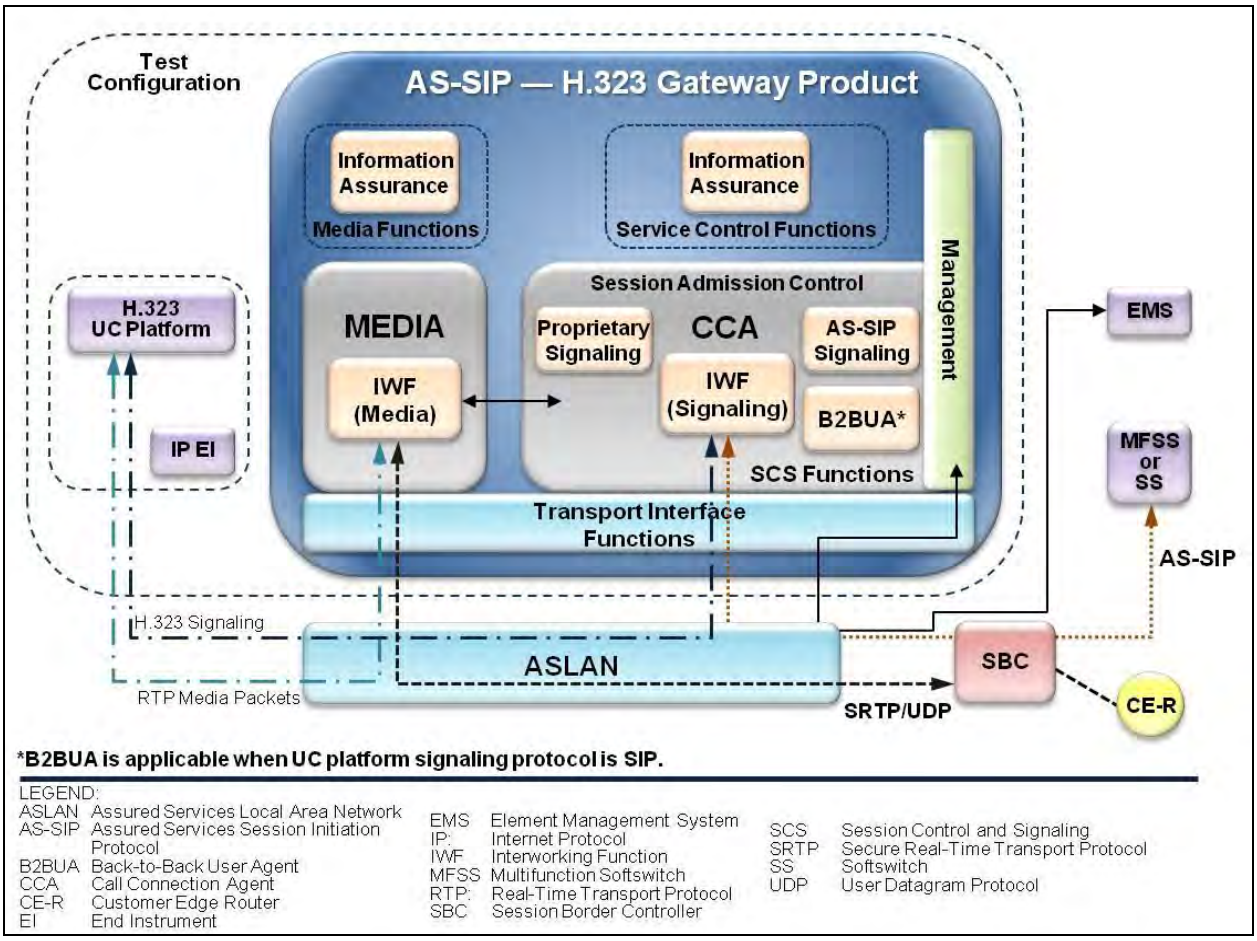

Figure 2.9-6. Functional Reference Model – AS-SIP – H.323 Gateway

2.9.3.3 Summary of AS-SIP – H.323 Gateway Functions and Features

The AS-SIP – H.323 Gateway provides interworking functions for the signaling and bearer planes (see Table 2.9-3, Summary of AS-SIP – H.323 Gateway Functions).

Table 2.9-3. Summary of AS-SIP – H.323 Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (H.323 to AS-SIP; AS-SIP to H.323)
SAC	Maintains call thresholds. Maintains active session state knowledge (local access bandwidth used and available, direction, session type: voice, video).
Media IWF	Converts H.323 media packets to UCR-compliant IP/UDP/SRTP packets. Converts UCR compliant IP/UDP/SRTP packets to H.323 media packets.
NM	Provides traffic call information to, and responds to traffic flow control commands from, an EMS.
LEGEND AS-SIP: Assured Services Session Initiation Protocol SAC: Session Admission Control	

FUNCTION	DESCRIPTION
EMS: Element Management System	SCS: Session Control and Signaling
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UCR: Unified Capabilities Requirements
NM: Network Management	UDP: User Datagram Protocol

2.9.3.4 AS-SIP – H.323 Gateway CCA Function Overview

The CCA is part of the SCS functions and includes the following:

- AS-SIP signaling protocol implementation for voice and video calls.
- H.323 signaling protocol implementation for voice and video calls (where signaling protocol implementation refers to the signaling being used by the H.323 UC signaling platform).
- Control of sessions within the AS-SIP – H.323 Gateway including the following:
  - H.323 sessions between the AS-SIP – H.323 Gateway and the H.323 UC signaling platform.
  - AS-SIP sessions between the AS-SIP – H.323 Gateway and the serving SS.
- Support for interactions with other network appliance functions including the following:
  - Admission control.
  - Information Assurance.
  - Media interworking.
  - Appliance Management functions.

Figure 2.9-7, CCA Relationships, illustrates the relationship between the CCA and other functional components.

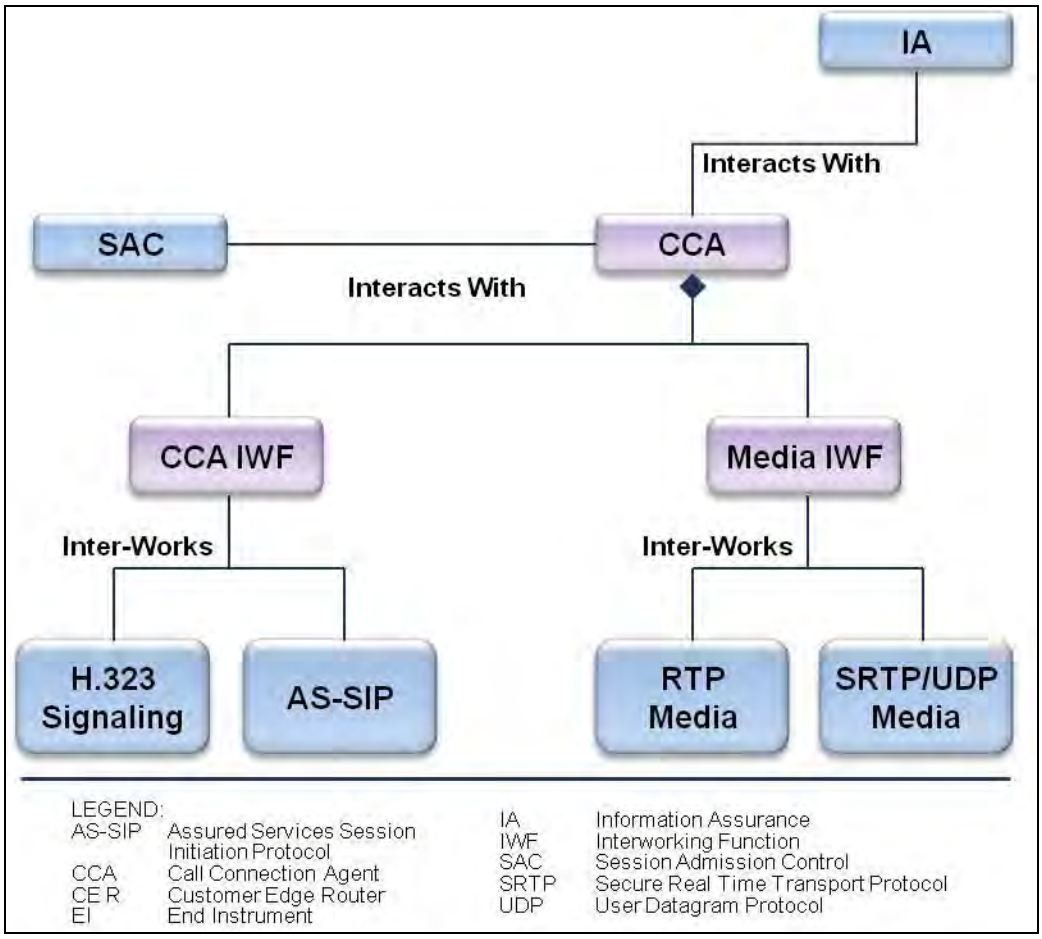

Figure 2.9-7. CCA Relationships

The role of the AS-SIP – H.323 Gateway CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by, or terminated in, the DISN UC network and are interworked by the AS-SIP – H.323 Gateway on behalf of the H.323 UC signaling platform. The signaling protocol used by the H.323 UC signaling platform is by definition an IP signaling protocol that is not compliant with the UCR AS-SIP requirements.

In addition, the CCA interacts with the Media Interworking function to convey the IP addresses/UDP ports of the RTP streams of sessions established by the signaling plane as well as the SRTP master keys exchanged in the SDP bodies to the Media interworking function. When the sessions are terminated the CCA notifies the media interworking function so that the Media Interworking function ceases to interwork the media packets for the terminated sessions.

2.10 NETWORK-LEVEL SOFTSWITCH

The network-level Softswitch (SS) is a backbone device that provides long-haul signaling between local service enclaves and acts as an AS-SIP B2BUA within the UC framework. It provides the equivalent functionality of a commercial SS.

A SS may serve EIs directly, if configured with an optional internal SC.

2.10.1 SS Functional Reference Model, Assumptions and Signaling Interfaces

Figure 2.10-1 shows the reference model for the SS:

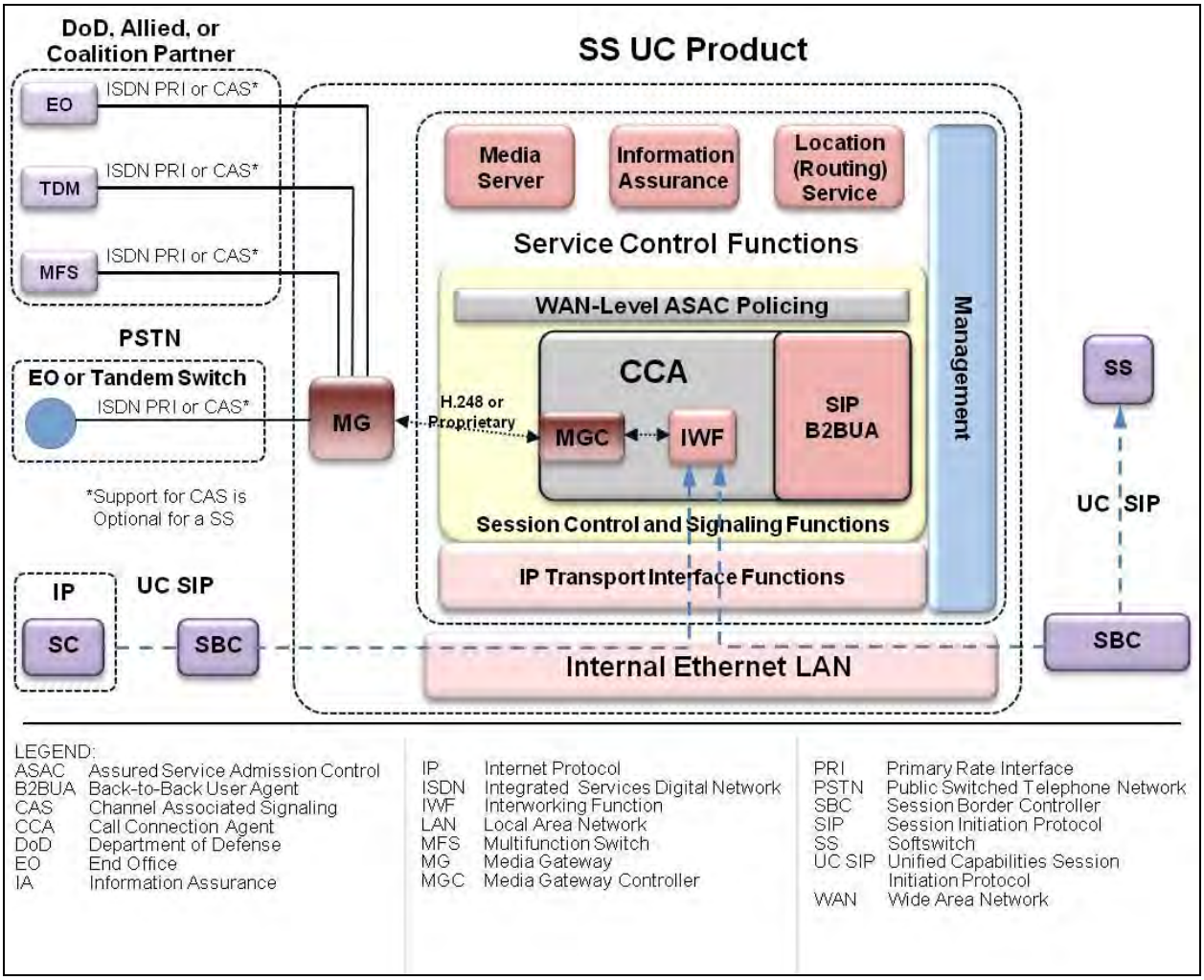

Figure 2.10-1. Functional Reference Model – SS

2.10.1.1 Assumptions – SS

The following assumptions are made based on the SS reference model:

1. External connections from an SS product are as follows:
   a. Connections to other IP-based products (e.g., SCs or other SSs) use AS-SIP signaling.
   b. Connections to TDM-based products (e.g., Multifunction Switch [MFS], EO, PBX, PSTN) use ISDN PRI or CAS.

2. The role of the CCA in the SS is identical to the role of the CCA in the SC (including the underlying assumptions, roles of the IWF and MGC, interactions with other SC components, and VoIP and Video signaling interfaces), with the following exceptions and extensions:

   a. The CCA in the SS interacts with both SC-Level ASAC and WAN-Level ASAC Policing. The SS supports SC-Level ASAC for admission control for calls to and from PEIs and AEIs that it directly serves (through its internal SC). The SS also supports WAN-Level ASAC Policing for admission control for calls to and from SCs that it directly serves.

   b. The CCA IWF in the SS is required to support interworking of the ISDN PRI protocol with AS-SIP.

3. The role of the MG in the SS is identical to the role of the MG in the SC (including the underlying assumptions, roles of the MG and MGC, interactions with other SC components, and VoIP signaling interfaces), with the following exceptions and extensions:

   a. The MG in the SS assists the SS CCA in providing call-denial treatments for CAC, and call-preemption treatments for SC-Level ASAC and WAN-Level ASAC Policing.

   b. The MG in the SS is required to support ISDN PRI trunks.

   c. Support for CAS trunks is optional for the MG in the SS.

4. Figure 2.10-1, Functional Reference Model – SS, shows the SS supporting a single MG on a single ASLAN. A single SS also can support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a Metropolitan Area Network (MAN) or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet the single-ASLAN performance requirements in Section 7, Network Edge Infrastructure. In this case, the SS supports sessions between an MG on one ASLAN and a PEI, AEI, MG, or SBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

   Another way of stating this is that a single SS is able to support MGs at multiple physical locations. In some voice deployments, an SS in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the SS supports MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in the UCR.

5. The SS Location Service (SSLS) functionality provides the CCA with information on call routing and called address translation for calls that are directed outside of the SS (where a called address is contained within the SIP URI in the form of a called number). For example, the CCA uses the routing information maintained by the SSLS to:

   a. Route outgoing calls from SS EIs, if any, to other SSs and SCs, and

   b. Route incoming calls from SCs and other SSs to other SCs and other SSs.

However, the SS still uses the routing information stored in its SCLS to route internal calls, if any, from one SS PEI or AEI to another; to route internal calls from an SS PEI or AEI to an SS MG (and vice versa); and to route incoming AS-SIP calls from another SS or SC to local SS PEIs or AEIs.

6. The SS interactions with its SBC are different from the SC interactions with its SBCs.
   a. In the SC case, the SBC controls signaling streams between an SC connected to an ASLAN and an SS where its separate ASLAN is connected to the DISN WAN. In this case, the SBC also controls media streams between SC PEIs/AEIs and MGs connected to the ASLAN, and PEIs/AEIs and MGs on other SCs where separate ASLANs are connected to the DISN WAN. The SC accesses the DISN WAN via the SC SBC and an associated Provider Edge (PE) Router on the DISN WAN. As a result, it is possible for an SC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an SBC to the DISN WAN, and through the DISN WAN to a remote PEI, AEI, or MG.
   b. In the SS case, the SBC controls signaling streams between the SS where the SBC is connected to the DISN WAN and the SCs that it serves, which are connected to the DISN WAN via their own SBCs and PE Routers. The SS SBC also controls signaling streams between the SS with its SBC connected to the DISN WAN and other SSs that it communicates with (with their own SBCs connected to the DISN WAN). As a result, the SS SBC is responsible for boundary control for both SS-SC signaling and SS-SS signaling.
   c. If supported, an SC within an SS will serve a set of (SS-internal) SC PEIs/AEIs and MGs. These SC EIs and MGs will exchange media streams with EIs and MGs on other SCs located elsewhere on the DISN WAN. In this case, the SS SBC also controls these media streams between the (SS-internal) SC EIs and MGs connected to the SS ASLAN, and EIs and MGs on other SCs where separate ASLANs are connected to the DISN WAN.

2.10.1.2 Signaling Interfaces – SS

The SS supports the VoIP and Video signaling interfaces shown in Table 2.10-1, SS Support for VoIP and Video Signaling Interfaces.

Table 2.10-1. SS Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (SS) – to – CCA (SC)	AS-SIP over IP
CCA	CCA (SS) – to – CCA (Other SS)	AS-SIP over IP
CCA	CCA (SS) – to – SS PEI	Proprietary VoIP over IP [Optional]
CCA	CCA (SS) – to – SS AEI	AS-SIP over IP [Optional]

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA/MGC and MG	SS CCA (MGC) – to – SS MG	ITU-T H.248 over IP (Optional - used with ISDN PRI and CAS trunks)
CCA/MGC and MG	SS CCA (MGC) – to – SS MG	ISDN PRI over IP (Optional - North American National ISDN Version, used with ISDN PRI trunks only)
CCA/MGC and MG	SS CCA (MGC)– to – SS MG	Proprietary Supplier Protocols (used with ISDN PRI and CAS trunks)

LEGEND

AEI: AS-SIP Voice End Instrument	ITU-T: International Telecommunications Union – Telecommunication	
AS-SIP: Assured Services Session Initiation Protocol		
CAS: Channel Associated Signaling	MG: Media Gateway	SC: Session Controller
CCA: Call Connection Agent	MGC: Media Gateway Controller	SS: Softswitch
DoD: Department of Defense		
IP: Internet Protocol	PEI: Proprietary End Instrument	TCAP: Transaction Capabilities
ISDN: Integrated Services Digital Network	PRI: Primary Rate Interface	Application Part
ISUP: ISDN User Part		VoIP: Voice over IP

2.11 CALL CONNECTION AGENT

2.11.1 Introduction

Session Controllers (SCs) and Softswitches (SSs) have a design that includes Session Control and Signaling (SCS) functions. These functions include both a Signaling Protocol IWF and a Media Gateway Controller function. The Call Connection Agent (CCA) described in this section is part of the SCS functions, and includes both the IWF and the MGC.

CCA responsibilities include the following:

1. Control of AS-SIP sessions within the network appliance, including:
   a. AS-SIP sessions from/to AEIs served by an SC or SS appliance.

   (NOTE: Proprietary protocol sessions from/to SC PEIs and SS PEIs are supported also.)

   b. AS-SIP sessions from/to SCs served by an SS appliance.
   c. AS-SIP sessions between SS appliances (where sessions span multiple SSs).
2. Support for the following PSTN and VoIP signaling protocols:
   a. AS-SIP.
   b. ISDN PRI (North American National ISDN version), including MLPP.
   c. PSTN CAS, for dual-tone multifrequency (DTMF) and multifrequency (MF) trunks (North American version).

3. Control of MGs that link the network appliance with TDM NEs through the CCA MGC in the following:
   a. DoD networks.
   b. Allied and coalition networks.
   c. PSTN in the continental United States (CONUS).
   d. PSTN Global (i.e., outside CONUS [OCONUS]).
4. CCA support for interactions with other network appliance functions, including:
   a. Admission control.
   b. The following Service Control functions:
      (1) Media servers.
      (2) UFS.
      (3) Information Assurance.
      (4) Session Controller Location Service (SCLS).
   c. Appliance Management functions.
   d. Softswitch Location Service (SSLS).
   e. SBCs.
5. CCA support for voice calls and video calls.
6. CCA support for Voice and Video services features and capabilities.

The CCA is also part of the SCS functions in AS-SIP Gateways. Please see Sections 2.9.1, 2.9.2 and 2.9.3 for the specific CCA responsibilities in those appliances.

2.11.2 Functional Overview of the CCA

Figure 2.11-1, CCA Relationships With Functional Components, illustrates the relationship between the CCA and other functional components. As indicated in the figure, the IWF and MGC are contained within a CCA.

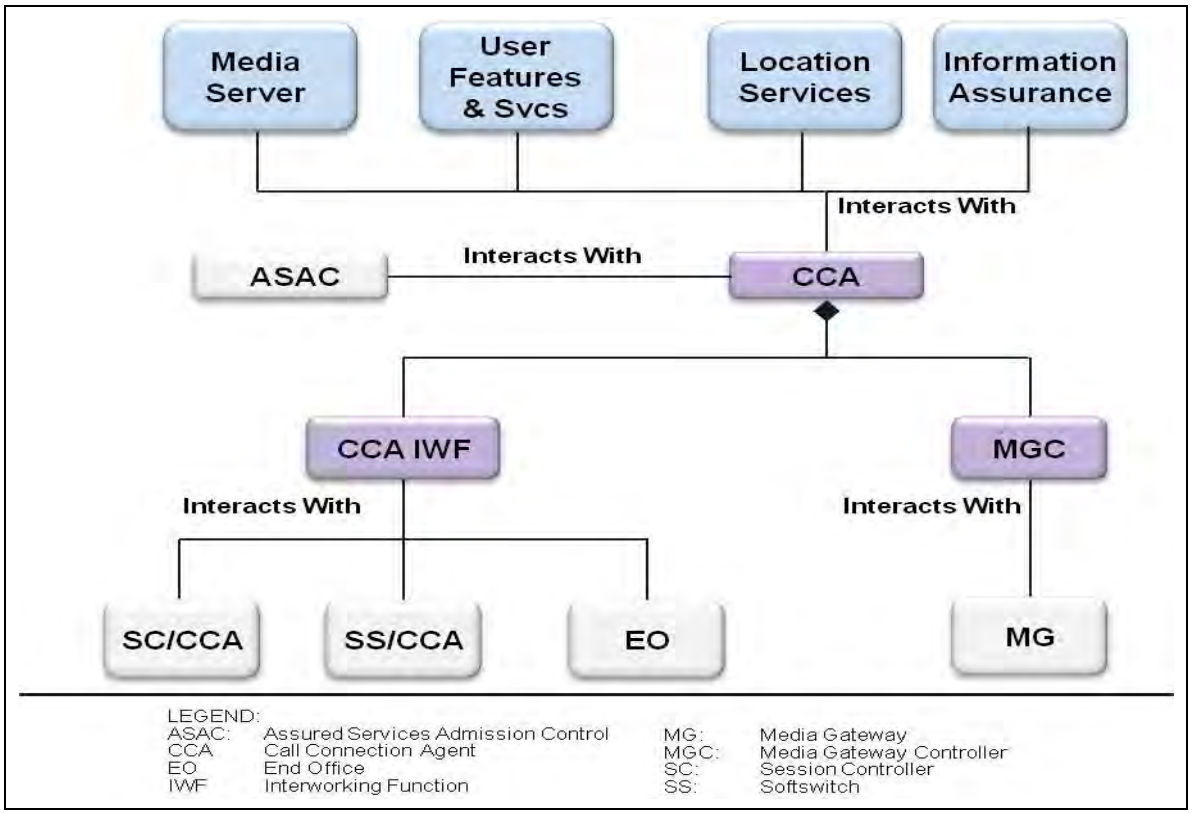

Figure 2.11-1. CCA Relationships With Functional Components

The role of a CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by, or terminated in, the voice network. These VoIP and Video sessions can be established using SIP, a Proprietary VoIP protocol, AS-SIP, or some combination of these (e.g., SIP and AS-SIP on an PEI-or-AEI/SC/SBC/SS session). The CCA takes on the role of the SIP B2BUA in the traditional SIP architecture.

In addition, the CCA takes on the role of a SIP Registrar for all PEIs, AEIs, MGs, and SBCs served by the SC, allowing PEIs, AEIs, MGs, and SBCs to register their SIP URIs (i.e., Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP-URI-to-IP-address "binding" for each PEI, AEI, MG, and SBC that is active on the SC at any moment in time.

In addition to acting as a SIP B2BUA, the CCA is responsible for providing call control and feature control for VoIP and Video over IP network-based calls and features. Most VoIP and Video over IP features that are provided to SC PEI and AEI end users, on either a per-call basis or an all-calls basis, are controlled by the CCA.

In the current design for an SC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (ISDN PRI trunks, and CAS trunks).

2.11.2.1 CCA IWF Component

The IWF has the following roles within the CCA:

- Support all the VoIP and TDM signaling protocols that the SC supports for EIs, MGs, and SBCs.
- Interwork all these various signaling protocols with one another.

2.11.2.2 CCA MGC Component

The MGC has the following roles within the CCA:

- Control all MGs within the SC or SS.
- Control all trunks (e.g., PRI, CAS) within each MG:
  - Support for DoD and PSTN ISDN trunks is required.
  - Support for CAS trunks is optional.
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.
- Within the SC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

  NOTE: The MGC and the MG that it controls are optional for deployable SCs.

2.11.3 CCA Interaction With Network Appliances and Functions

This section describes how the CCA interacts with network appliances and appliance functions, including the following:

- ASAC.
- Service Control functions.
- NM (FCAPS and audit logs).
- Transport Interface functions.
- SBC (not part of the SC, but part of the local Assured Services domain).

2.11.3.1 CCA Interactions With Transport Interface Functions

The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined in this section. The detailed implementation methods for these requirements are left up to each vendor. Examples of Transport Interface functions include:

- Network Layer functions: IP and IPSec.
- Transport Layer functions: TCP, UDP, Stream Control Transmission Protocol (SCTP), TLS.
- LAN protocols.

The CCA interacts with Transport Interface functions by using them to communicate with PEIs, AEIs, the SBC, the MGs, and the SG over the ASLAN. The following appliance elements are all IP end points on the ASLAN:

- Each PEI or AEI.
- Each MG and SG (even though the MG or SG may be connected physically to the CCA over an internal proprietary interface, instead of being logically connected to the CCA over the ASLAN).
- The CCA/IWF/MGC itself.
- The SBC (for SC, PEI, AEI, and MG communication with other SCs, SSs, PEIs, AEIs, and MGs over the DISN WAN).

As an example, the CCA interacts with the SC Transport Interface functions when it uses IP, TLS, TCP, and the native ASLAN protocols to exchange SIP signaling messages with PEIs or AEIs and the SBC over the ASLAN.

The MGs controlled by the CCA interact with the SC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from PEIs, AEIs, other SC MGs, and the SBC over the ASLAN.

2.11.3.2 2CCA Interactions With the SBC

The SBC provides Session Border Control and firewall capabilities for the ASLAN, the PEIs/AEIs, and the IP-based components of the SC, including the CCA/IWF/MGC and the MGs.

The CCA interacts with the SBC by directing AS-SIP signaling packets to it (for signaling messages destined for an SS) and by accepting AS-SIP signaling packets from it (for signaling messages directed to the SC from an SS).

The SC EIs and MGs, which are controlled by the CCA, interact with the SBC by directing SRTP media streams to it (for call media destined for EIs and MGs on other SCs), and by accepting SRTP media streams from it (for call media directed to the SC PEIs/AEIs and MGs from EIs and MGs on other SCs).

The AS-SIP signaling packets exchanged between the SC and an SS must pass through the SBC. The SRTP media streams exchanged between SC EIs /MGs and EIs/ MGs on other SCs must also pass through the SBC.

The CCA in the SS and SC needs to interact with AS-SIP functions in the SBC, which

- Mediates AS-SIP signaling between an SC and an SS, and between two SSs.

- Supports commercial SBC functions, such as NAT and Network Address and Port Translation (NAPT).
- Supports IP firewall functions.

2.11.3.3 CCA Support for Admission Control

The CCA interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls; managing separate call budgets for VoIP and Video over IP calls; and providing preemption.

Requirements for ASAC are handled in two categories: CAC and ASAC. Call Admission Control is defined as follows:

"A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service (QoS) requirements for the call."

Call Admission Control is also referred to as SAC, because in the network appliances a VoIP call is also a SIP Voice session, and a Video call is also a SIP Video session. Session Admission Control is limited as follows:

"SAC is typically limited to managing the pre-populated session budgets for each Assured Service (voice and video)."

Assured Services Admission Control includes CAC/SAC and its support for call counting, voice call budgets, and video call budgets. In addition, ASAC includes capabilities for handling calls differently based on their precedence level (e.g., DSN ROUTINE, PRIORITY, IMMEDIATE, FLASH, or FLASH OVERRIDE), and for having calls of a higher precedence level preempt calls of a lower precedence level.

Two different levels of ASAC are SC-Level ASAC (supported in the SC and the SS) and WAN-Level ASAC Policing (supported in the SS only). The SC and SS are responsible for maintaining the following:

- VoIP session budgets.
- VoIP session counts.
- VSU budgets.
- VSU counts.

2.11.3.4 CCA Support for User Features and Services

The User Features and Services (UFS) Server is responsible for providing features and services to VoIP and Video PEIs/AEIs on an SC or SS, where the CCA alone cannot provide the feature or service. In this section, no distinction is made between "features" and "services," and all

features and services, such as Call Hold, Call Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer, Hotline Service, and Calling Party and Called Party ID (number only), are called features. Examples of features that may require the use of a UFS Server are voice mail services; services that use TCAP queries and responses, such as toll-free 800/888 number services and calling name delivery services; and services that require screening of calling party numbers on incoming calls (e.g., block calls to this VoIP PEI/AEI from these numbers); and screening of called party numbers on outgoing calls (e.g., block calls from this VoIP PEI/AEI to these numbers).

The CCA interacts with UFS by relaying end-user requests for feature and service invocation to the UFS, and relaying UFS responses, such as text displays and message waiting indicators, back to PEIs/AEIs and end users. The CCA may relay feature information from the UFS to the EI/AEI and end user without a corresponding feature request from the PEI/AEI or the end user. Examples of this include the UFS text message that tells a PEI that a CW call is available, and the UFS indicator that tells a PEI that there is a message waiting for that PEI.

The interface and protocols used to interconnect the CCA with the UFS Server are internal to the network appliance and, therefore, are supplier-specific.

2.11.3.5 CCA Support for Information Assurance

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that use the appliance are all properly authenticated and authorized by the appliance. The Information Assurance function ensures that Voice and Video signaling streams that traverse the appliance and its ASLAN are properly encrypted.

The interface and protocols used to interconnect the CCA with the Information Assurance function are internal to the appliance and, therefore, are supplier specific.

2.11.3.6 CCA Interactions With Session Controller Location Service

The Session Controller Location Service (SCLS) provides information on called address translation in response to call routing queries from the CCA. The CCA sends call routing queries to the SCLS for both outgoing calls from appliance PEIs or AEIs and incoming calls to appliance PEIs or AEIs.

The CCA uses the information returned by the SCLS to route the following:

- Internal calls from one appliance PEI or AEI to another.
- Outgoing calls from an appliance PEI or AEI to another appliance (via an SBC), or to a TDM network (via an Appliance MG).
- Incoming calls from another appliance (via an SBC), or from a TDM network (via an Appliance MG), to an SC PEI or AEI.

The interface and protocols used to interconnect the CCA with the SCLS are internal to the appliance and, therefore, are supplier specific.

2.11.3.7 CCA Interactions With Softswitch Location Service

Like the SCLS, the Softswitch Location Service (SSLS) provides information on call routing in response to call-routing queries from the CCA. The CCA sends call-routing queries to the SSLS for calls where the CCA determines that the call's destination lies outside the SS.

The CCA may determine call routing based on an analysis of the called address. For example, it does this by finding that this address did not contain a PSTN escape code as a prefix, and by finding that the first six digits of this called address (i.e., the Numbering Plan Area [NPA]-NXX in the DoD dialing plan) pointed to a location in the DoD network outside the SS. The CCA may make this determination based on a previous call-routing response from the SS's SCLS that indicated, "This address is not assigned to any PEI, AEI, or MG on the SS."

As in the SCLS case, the query from the CCA to the SSLS identifies the called address for the call in question. It may be embedded within a SIP URI, e.g., sip: +17327582000@uc.mil; user=phone, or sip: 3144305353@uc.mil; user=phone. The response from the SSLS identifies either of the following:

- A remote IP address that points to the next appliance (i.e., an SC or an SS) that the call should be routed to.
- The local IP address of an SS MG trunk group that the call should be routed to. (This case applies when the MG TG connects to a TDM destination outside the SS that can be on the DoD TDM network, an allied or coalition partner TDM network, or on the PSTN (CONUS and Global)).

2.11.3.8 CCA Interactions With End Instrument(s)

The CCA in the SC, including an SC internal to an SS, needs to interact with VoIP PEIs and AEIs served by that SC. The VoIP interface between the PEI and the SC is left up to the network appliance supplier. The VoIP interface between the AEI and the SC is AS-SIP.

2.11.3.9 CCA Interactions With Service Control Functions

The interface and protocols used to interconnect the CCA with the media server are internal to the SC and SS and, therefore, supplier specific.

The Media Server function provides tones and announcements that the SC "plays out" to local and remote end users on VoIP and video calls. In addition, the media server may provide audio and video messages, or "clips," that the SC can "play" to local and remote users on video calls.

NOTE: It is possible that some tones and announcements may be generated locally by the end user's PEI or AEI, based on commands from the SC to the PEI or AEI that

mandate the "play" of the tones or announcements. (An example of this is the use of an SC command that instructs a PEI to "play" dial tone to a calling end user, and then to automatically halt "playing" dial tone upon receipt of the first keypad digit from that end user.) In these cases, the use of a separate media server to provide tones and announcements to end user PEIs or AEIs is up to the SC vendor.

The media server stores these tones, announcements, audio clips, and video clips locally, and "plays them out" to either local or remote end users in response to corresponding requests from the CCA. As part of this "play out" process, the media server may prompt the end users for information (e.g., entry of keypad digits, or vocal answers to media server questions). In this case, the media server collects that information and responds to the CCA indicating what the collected information was, or what action the CCA should take based on the collected information.

The CCA is responsible for asking the media server to "play out" tones, announcements, audio clips, and video clips, and for ensuring that the media from the media server is directed to the correct end user. In addition, the CCA is responsible for capturing collected information from the media server, such as the series of keypad digits entered by an end user in response to a media server prompt, and using that information appropriately for call processing or feature processing.

2.12 MEDIA GATEWAY

2.12.1 Introduction

This section describes the Media Gateway (MG) and Media Gateway Controller (MGC) functions in the SC and SS network appliances. These appliances have defined designs that include an MGC function and one or more MGs.

The scope of the MG requirements in UCR 2013 Section 2.18, Media Gateway, covers the following areas:

- Physical interfaces and protocols supported on the TDM side of the MG include the following:
  - ISDN PRI trunks: The TDM media (B channels) channels and the TDM signaling channels (D channels) both terminate on the MG.
  - CAS trunks: Both DTMF and MF; the TDM channel that carries both the media and the signaling terminates on the MG.
- VoIP interfaces and protocols supported on the IP side of the MG include the following:
  - Interface to the IP router network and the LAN (ASLAN, LANs internal to a UC product) that the network appliance is connected to.
  - VoIP protocol stacks supporting IP, IPSec, UDP, TCP, SCTP, and SRTP.

  - Secure VoIP media streams, packetized using IP, UDP, and SRTP, IAW Section 4, Information Assurance.
  - Secure VoIP signaling messages, packetized using IPSec, and UDP or TCP or SCTP, IAW, Section 4, Information Assurance:
    - H.248 signaling messages, for MGC control of ISDN PRI and CAS trunks, if the supplier supports ITU-T Recommendation H.248.
    - ISDN PRI signaling messages, for MGC control of ISDN PRI trunks.
- Support for the following VoIP codecs, at a minimum, on the IP side of the MG:
  - ITU-T Recommendation G.711 (uncompressed voice, both North American (μ-law and International A law)).
  - ITU-T Recommendation G.723.1.
  - ITU-T Recommendation G.729.
- Support for Fax over IP (FoIP) on the IP side of the MG.
- Support for Voiceband Modem over IP (MoIP) on the IP side of the MG. The following terms define "Modem over IP" traffic, as used in the UCR. The terms are listed here to clarify that SCIP over IP streams are a subset of all possible modem relay streams. In the UCR, the term SCIP over IP can be considered synonymous with the transmission of SCIP over V.150.1 Modem Relay. (These terms also appear in Appendix A, Definitions, Abbreviations and Acronyms, and References.)
  - Modem over IP. The transport of modem data across an IP network, via either modem relay or modem passthrough techniques.
  - Modem Relay. A subset of MoIP, in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network.
  - Voiceband Data (Modem Passthrough). A subset of MoIP in which modem signals are transmitted over a Voiceband Data channel in a packet network.
  - SCIP over IP. The transport of SCIP information over an IP network. The SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 Modem Relay.
- Support for SCIP over IP on the IP side of the MG. As noted previously, SCIP over IP streams are a subset of all possible modem relay streams. In the UCR, the term SCIP over IP is synonymous with the transmission of SCIP over V.150.1 Modem Relay. For SCIP over IP calls, the MG supports V.150.1 Modem Relay traffic IAW ITU Recommendation V.150.1 and NSA document SCIP 216 on the IP side of the MG.
- Support for 64-Kbps unrestricted digital information (clear channel) ISDN over IP on the IP side of the MG.

2.12.2 Overview of the MG and MGC Functions

Media Gateway is a generic term for a Trunk Gateway (TG) and for an Access Gateway (AG). Thus, MG requirements apply to TGs and to AGs.

Figure 2.12-1, MGC – MG Layered Interface, illustrates the relationship between the MGC, a component of the CCA, and a generic MG.

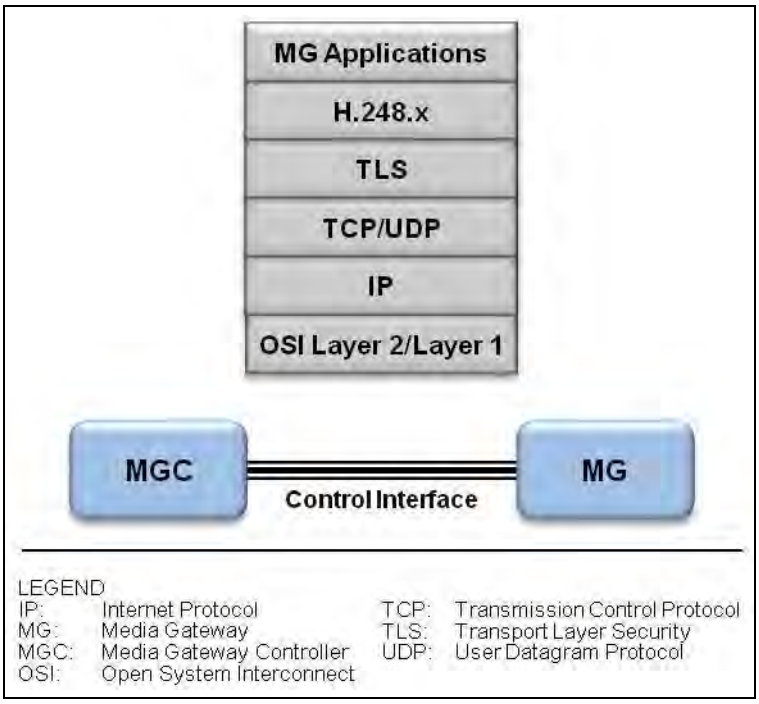

Figure 2.12-1. MGC – MG Layered Interface

Figure 2.12-2, MG Trunk Function, illustrates the MG trunk function.

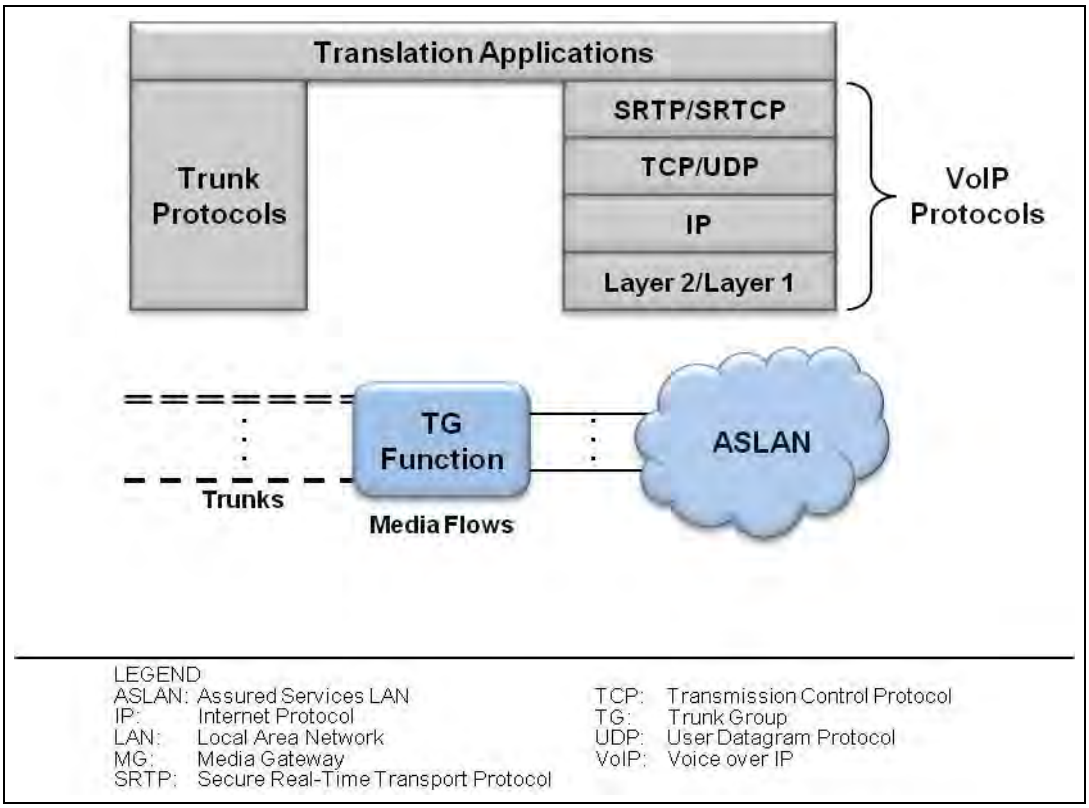

Figure 2.12-2. MG Trunk Function

2.12.2.1 Primary Trunk Functions and Interfaces

An MG may support a trunk-side interface to circuit-switched (CS) telephone networks. It terminates CS trunks in the CS networks and packet flows in the DISN Core network and, thus, provides functions such as media translation. The MG can set up and manage media flows through the Core network when instructed by the CCA. It is associated with a specific CCA that provides it with the necessary call control instructions.

2.12.2.2 Primary Access Functions and Interfaces

An MG may support line-side and trunk-side interfaces to the voice network end users. Traditional telephones and PBXs currently used in the PSTN, as well as ISDN Basic Rate Interface (BRI) telephones, ISDN BRI terminals, and ISDN-capable PBXs using PRIs, can access the DISN Core network through the MG. The MG provides functions, such as packetization and echo control, for its end users' information streams, and is associated with a specific CCA that provides the necessary call control and service control instructions. On receiving the appropriate commands from its CCA, the MG provides Call Control functions such as audible ringing and power ringing, as well as Service Control functions. The MG also is capable of setting up transport connections through the DISN Core network when instructed to do so by the CCA (see Figure 2.12-3, MG Primary Access Functions and Interfaces).

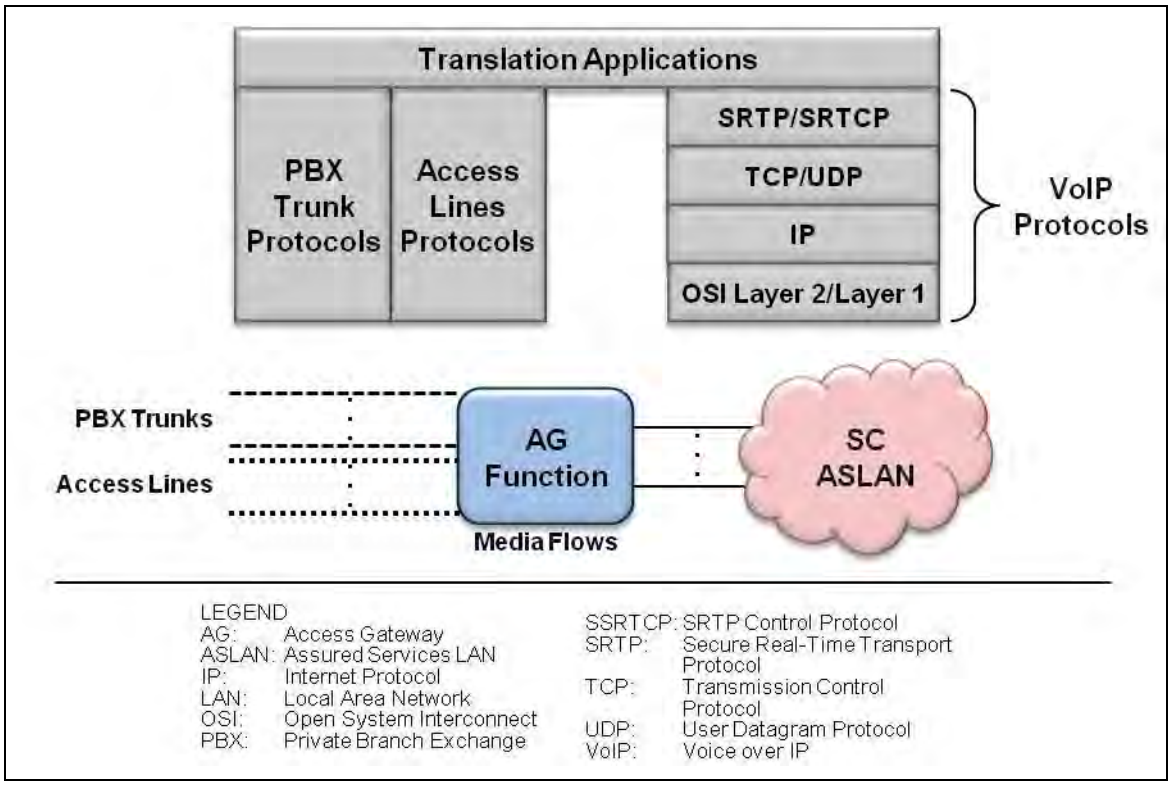

Figure 2.12-3. MG Primary Access Functions and Interfaces

2.12.2.3 MGC Functions

There are two options for the Gateway Control Protocol in the MGC and the MG:

1. An industry-standard Gateway Control Protocol, using an open interface between the MGC and the MG. This protocol assumes MG-to-MGC communication over IP and the LAN that the appliance is connected to. This LAN is the ASLAN for the SC and SS. (In some cases, this LAN may be the Internal LAN of the UC product, where the UC product also contains the SC or the SS. In these cases, the Internal LAN of the UC product is not an ASLAN.)

   The industry-standard Gateway Control Protocol used in these requirements is ITU-T Recommendation H.248.1.

2. A supplier-specific Gateway Control Protocol, using a closed (supplier-proprietary) interface between the MGC and the MG. This supplier-specific protocol may use MGC-to-MG communication over IP and the LAN that the appliance is connected to (ASLAN or Internal LAN for the UC product), or it may use separate physical, data link, and network layer interfaces that are also proprietary to the supplier.

   The MGC function is part of the CCA function in the SC and SS, which in turn is part of the SCS functions in these appliances. The MG function is a standalone appliance function in the SC and SS, and is not part of any other appliance function.

The role of the MGC within an SC and SS is to do the following:

- Control all MGs within the SC and SS.
- Control all trunks (e.g., PRI or CAS) within each MG.
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.

The MGC and the MG that it controls are optional for Deployable SCs.

2.12.3 Role of the MG in Appliances

The MG provides trunk termination for PRI and CAS trunks, and TDM/VoIP interworking. The MG is controlled by the MGC. The protocol that the MGC uses to control the MG can be ITU-T Recommendation H.248 (specifically, H.248.1) or a proprietary protocol chosen by the SC supplier.

2.12.3.1 Role of the MG in the SC

Figure 2.8-1, Functional Reference Model – SC, illustrates the reference model for the SC, including the VoIP MG and MGC.

The roles of the MG within the SC are as follows:

- The MG terminates all TDM trunks that interconnect the SC with TDM networks, including the following:
  - DoD TDM networks (e.g., DSN, including EO and Tandem switches within the DSN), both in the United States and worldwide.
  - PSTNs, both in the United States and worldwide.
  - Allied and U.S. coalition partner TDM networks.
- The MG terminates all TDM trunks that interconnect the SC with TDM PBXs within the same DoD B/P/C/S.

  Media gateway support for TDM trunk groups is expected to be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs.
- The MG is responsible for terminating the TDM media trunks and signaling links on the TDM side, and for terminating the VoIP/FoIP/MoIP media streams and signaling streams on the VoIP side.
- On calls that traverse the MG, the MG converts TDM media streams to VoIP, FoIP, or MoIP media streams, and converts VoIP, FoIP, or MoIP media streams to TDM media streams.
- The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following SC functions and end-user devices:

  - The SC media server, which provides tones and announcements for SC calls and SC features.
  - Proprietary VoIP, FoIP, and MoIP EIs on the SC (when these EIs are supported on the SC).
  - Proprietary SIP EIs on the SC (when these EIs are supported on the SC).
  - Proprietary H.323 EIs on the SC (when these EIs are supported on the SC).
  - AS-SIP VoIP, FoIP, and MoIP AEIs on the SC.
- On ISDN PRI calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams, and it converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will send and receive encapsulated PRI signaling to and from the CCA.
- On CAS trunk calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams, and it converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will translate between CAS signaling and H.248 protocol messages to and from the CCA.

  NOTE: The MG and the MGC that controls the MG are considered "Optional – Deployable" for the SC. Some SC suppliers may include an MGC and MG in their Deployable SC product, and other SC suppliers may not. Those suppliers who do are to follow the MG requirements defined in the UCR.

2.12.3.1.1 SC MG VoIP Signaling Interfaces

The SC MG supports the VoIP signaling interfaces shown in Table 2.12-1, SC MG Support for VoIP Signaling Interfaces.

Table 2.12-1. SC MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP SIGNALING INTERFACES	VOIP SIGNALING PROTOCOLS
MG and MGC (CCA)	MG – to – MGC (CCA)	ITU-T H.248 over IP (used with ISDN PRI and CAS trunks)
MG and MGC (CCA)	MG – to – MGC (CCA)	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC (CCA)	MG – to – MGC (CCA)	Proprietary Supplier Protocols (used as an alternative to ITU-T H.248 over IP and ISDN PRI over IP) (used with ISDN PRI and CAS trunks)
LEGEND		
CAS: Channel Associated Signaling		MG: Media Gateway
CCA: Call Connection Agent		MGC: Media Gateway Controller
DoD: Department of Defense		PRI: Primary Rate Interface

FUNCTIONAL COMPONENT	VOIP SIGNALING INTERFACES	VOIP SIGNALING PROTOCOLS
IP: Internet Protocol ISDN: Integrated Services Digital Network ITU-T: International Telecommunications Union – Telecommunication		VoIP: Voice over IP

2.12.3.2 Role of the MG in the SS

Figure 2.10-1, Functional Reference Model – SS, provides the functional reference model of the SS. The role of the MG in the SS is identical to the role of the MG in the SC (including the underlying assumptions, roles of the MG and MGC, interactions with other SC components, and VoIP signaling interfaces), with the following exceptions and extensions:

3. The MG in the SS assists the SS CCA in providing call denial treatments for CAC, and call preemption treatments for SC-Level ASAC and WAN-Level ASAC Policing. The SS supports SC-Level ASAC for admission control for calls to and from EIs that it serves directly. The SS also supports WAN-Level ASAC Policing for admission control for calls to and from SCs that it serves directly.
4. The MG in the SS supports ISDN PRI and, optionally, CAS trunks.

   NOTE: When an SC is included within a SS, it will serve a set of (SS-internal) SC EIs and MGs. These SC EIs and MGs will exchange media streams with EIs and MGs on other SCs located elsewhere on the DISN WAN. In addition, the SS SBC controls these media streams between the (SS-internal) SC EIs and MGs connected to the SS ASLAN, and EIs and MGs on other SCs, where separate ASLANs are connected to the DISN WAN.

2.12.3.2.1 SS MG VoIP Signaling Interfaces

The SS MG supports the VoIP signaling interfaces shown in Table 2.12-2, SS MG Support for VoIP Signaling Interfaces.

Table 2.12-2. SS MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
MG and MGC	SS MG – to – SS MGC	ITU-T H.248 over IP (used with ISDN PRI and CAS trunks)
MG and MGC	SS MG – to – SS MGC	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC	SS MG – to – SS MGC	Proprietary Supplier Protocols

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
LEGEND		
DoD: Department of Defense		MGC: MG Controller
IP: Internet Protocol		PRI: Primary Rate Interface
ISDN: Integrated Services Digital Network		SS: Softswitch
ITU-T: International Telecommunications Union – Telecommunication		
MG: Media Gateway		VoIP: Voice over IP

2.12.4 MG Interaction With NES and Functions

The MG is responsible for interacting with elements and functions of the SC and SS to support end-user calls, end-user features, and other operational capabilities needed by the DoD users. These other elements include the following:

- ASAC.
- Service Control functions (Information Assurance and media server).
- Management (FCAPS and audit logs).
- Transport Interface functions.
- SBC.

2.12.4.1 MG Support for ASAC

The MG interacts with the CCA, which in turn interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as providing denial treatments for calls that are denied admission to the SC and/or SS, and preemption treatments for calls that are preempted by PBAS/ASAC.

Requirements for ASAC are handled in two categories: CAC and ASAC. In addition, this section covers two different levels of ASAC: SC-Level ASAC, which is supported in the SC and the SS, and WAN-Level ASAC Policing, which is supported in the SS only.

The MG assists the CCA in performing CAC (i.e., call blocking based on budget restrictions) for outgoing TDM calls at MGs and for incoming TDM calls at MGs.

The MG assists the CCA in performing ASAC (i.e., call preemption based on per-call precedence levels) for outgoing TDM calls at MGs and for incoming TDM calls at MGs.

2.12.4.1.1 MG Call Denial Treatments To Support CAC

When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies (e.g., the VoIP session count equals the VoIP session limit for the type

of session being requested), the CCA will deny the session request and apply a Call Denial treatment (i.e., a busy signal or call denial announcement) to the calling party on that request. If the calling party is a TDM calling party whose call enters the appliance at an MG trunk group, the MG is responsible for applying that treatment.

2.12.4.1.2 MG Call Preemption Treatments To Support ASAC

When the CCA determines that an existing VoIP session or VoIP session request should be cleared because an Appliance ASAC preemption applies (e.g., a CAC limit applies and a call of a higher precedence level needs to complete within the appliance), the CCA will clear the existing session or session request and apply a Call Preemption treatment (i.e., a Call Preemption tone or announcement) to both the calling and called parties on that request. If the calling party is a TDM calling party whose call entered the appliance at an MG trunk group, or the called party is a TDM called party whose call left the appliance at an MG trunk group, the MG is responsible for applying the Call Preemption treatment.

2.12.4.2 MG and Information Assurance Functions

The MG interaction with Information Assurance function is consistent with the DoD Information Assurance requirements in UCR Section 4, Information Assurance.

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that interact with the appliance are all properly authenticated by the appliance. The Information Assurance function also ensures that VoIP signaling streams and media streams that traverse the appliance and its ASLAN are properly encrypted, using SIP/TLS and SRTP, respectively.

The MG performs the following authentication and encryption functions in conjunction with the CCA and Information Assurance:

1. When the MG registers with the MGC in the CCA, the MG exchanges authentication credentials with the CCA and, through the CCA, with Information Assurance.
2. The MG exchanges encryption keys with the CCA and, through the CCA, with Information Assurance, before exchanging H.248 messages and encapsulated PRI messages with the MGC in the CCA.
3. The MG uses the exchanged encryption keys to (1) encrypt H.248 messages and encapsulated PRI messages sent in the MG => CCA => Information Assurance direction, and (2) decrypt H.248 messages and encapsulated PRI messages sent in the Information Assurance => CCA => MG direction. The encryption and decryption are performed at the IP layer using IPSec packets, instead of being done at the message layer using H.248 messages or PRI messages.

4. The MG also performs the following encryption functions in conjunction with PEIs or AEIs, and the media server in the SC (NOTE: These functions may or may not use Information Assurance, depending on the internal design of the SC.):
   a. The MG exchanges encryption keys with local PEIs or AEIs and local MGs, remote PEIs or AEIs and remote MGs, and the media server, before exchanging encrypted VoIP media streams with these devices.
   b. The MG uses the exchanged encryption keys to (1) encrypt VoIP SRTP media streams sent in the MG => PEI/AEI/other MG/media server direction, and (2) decrypt VoIP SRTP media streams received in the PEI/AEI/other MG/media server => MG direction. The encryption and decryption are performed above the UDP Transport Layer using SRTP packets.

2.12.4.3 MG Interaction With Service Control Functions

The media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on video calls. In addition, the media server may provide "play announcement and collect digits" functionality to calling and called parties on VoIP and video calls when this functionality is required by certain features that the CCA supports. Depending on the complexity of those features, the media server may act as a full Interactive Voice Response (IVR) system for appliance PEIs/AEIs and other Assured Services end users, providing IVR-like features to local and remote VoIP callers, and providing video-enhanced IVR-like features to local and remote video callers.

The MG is responsible for routing individual VoIP, FoIP, and MoIP media streams to the media server when instructed to do so by the CCA/MGC. When instructed to do so by the CCA/MGC, the MG is responsible for removing individual VoIP, FoIP, and MoIP media streams from the media server, and for either disconnecting them entirely, or routing them on to other SC end users (e.g., VoIP or video EIs).

The interface and protocols used to interconnect the MG with the media server are internal to the appliance and are, therefore, supplier-specific.

2.12.4.4 Interactions With IP Transport Interface Functions

The Transport Interface functions in the SC provide interface and connectivity functions with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- Network Layer functions: IP, IPSec.
- Transport Layer functions: IP Transport Protocols (e.g., TCP, UDP), TLS.
- LAN protocols.

The MG interacts with Transport Interface functions by using them to communicate with PEIs or AEIs and the SBC (and through the SBC to remote PEIs or AEIs and MGs served by other SCs and SSs) over the ASLAN. The following elements are all IP endpoints on the ASLAN:

- Each PEI or AEI served by the SC.
- The MG itself.
- Any other MGs that are served by the SC (even though the other MGs may be connected physically to the CCA/MGC over an internal proprietary interface, instead of being logically connected to the CCA/MGC over the ASLAN).
- The CCA and its IWF and MGC.
- The SBC.

As an example, the MG interacts with the SC Transport Interface functions when it uses IPSec, UDP/TCP/SCTP, and the native ASLAN protocols to exchange H.248 and PRI signaling messages with the CCA/MGC over the ASLAN.

The MG interacts with the SC Transport Interface functions when it uses IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, other SC MGs, and the SBC over the ASLAN.

2.12.4.5 MG-SBC Interaction

The SBC provides Session Border Control and firewall capabilities for the ASLAN, the PEIs, AEIs, and the IP-based components of the SC, including the CCA, and its IWF and MGC, and the MGs.

The MG interacts with the SBC by sending SRTP media streams to it (for call media destined for a PEI, AEI, or MG that is served by another appliance outside the SC), or by accepting SRTP media streams from it (for call media arriving from a PEI, AEI, or MG that is served by another appliance outside the SC).

The SRTP media streams exchanged between the SC MG and a remote PEI, AEI, or MG must pass through the SBC. The SBC modifies these SRTP media streams by doing NAT/NAPT on them.

The VoIP MG in the SS or SC needs to interact with VoIP Media Transfer functions in the SBC. The SBC does the following:

- Transfers media streams between the PEIs or AEIs and MGs on the appliance, and PEIs or AEIs and MGs on remote appliances, located elsewhere on the DISN WAN.
- Supports commercial SBC functions, such as NAT and NAPT.
- Supports IP firewall functions.

2.12.4.6 MG Support for Appliance Management Functions

The Management function in the SBC, SC, and SS supports functions for SBC/SC/SS FCAPS management and audit logs.

The MG interacts with the Appliance Management function by doing the following:

- Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes.
- Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information.
- Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function so that the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

2.12.4.7 Interactions With VoIP EIs

The MG in the SS or SC needs to interact with VoIP EIs served by that SS or SC, and with VoIP EIs served by other SSs or SCs. The VoIP signaling interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP signaling interface between the AEI and the SS or SC is AS-SIP.

2.12.5 MG and Echo Cancellation

The MG supports Echo Cancellation, consistent with commercial VoIP network practices.

In any 2-wire or combination 2- and 4-wire telephone circuit, echo is caused by impedance mismatch. Echo Cancellers are voice-operated devices placed in the 4-wire portion of a circuit, which may be an individual circuit path or a path carrying a multiplexed signal, and are used for reducing the echo by subtracting an estimated echo from the circuit echo.

The ECs are assumed to be "half" ECs, i.e., those in which cancellation takes place only in the send path because of signals present in the receive path. In particular, echo cancellation should be enabled for all voice calls. The ITU-T requirements for echo cancellation are specified in ITU-T Recommendation G.168.

2.12.5.1 Echo Control Design

An example MG echo control design is illustrated in Figure 2.12-4, Example IP Network Echo Control Design.

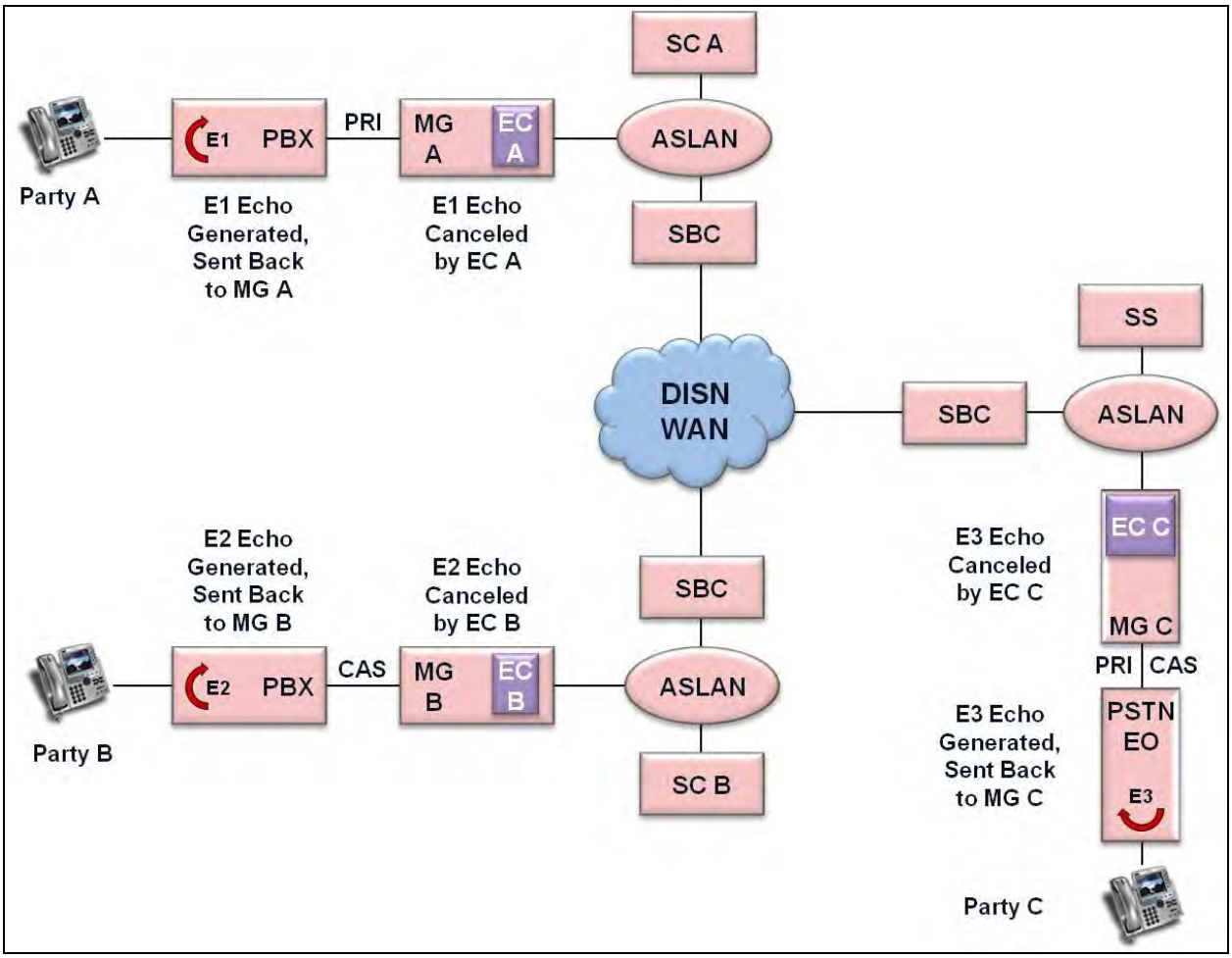

Figure 2.12-4. Example IP Network Echo Control Design

The EC function in MG A (controlled by SC A) is pointing toward the PRI interface to the PBX, canceling voice-frequency (VF) echo returning from the local PBX and the telephone end users behind that PBX. The EC function in MG B (controlled by SC B) is pointing toward the CAS interface to the other PBX, canceling VF echo returning from the local PBX and the telephone end users behind that PBX.

On a call between Party A and Party B, the EC function in MG A protects the "far-end party" (Party B) from excessive acoustical echo from the "near-end party" (Party A). Similarly, the EC function in MG B protects the "far-end party" (Party A) from excessive acoustical echo from the "near-end party" (Party B).

In addition, the EC function in MG C (controlled by the SS) is pointing toward the PRI or CAS interface to the PSTN EO, canceling VF echo returning from that EO and the telephone end users behind that EO. On a connection between Party A and Party C (a PSTN-served customer), the EC function in MG C is protecting the IP-network-served party (Party A) from excessive acoustical echo. Similarly, the EC function in MG A is controlling the VF echo returned toward the PSTN-served party (Party C).

The echo path capacity of an EC is the maximum echo path delay for which the device is designed to operate.

According to ITU Recommendation G.168, ECs may remain active for several types of non-voice calls as well; in particular, for G3 Fax calls and VBD modem calls.

2.12.6 MG and Synchronization

The use of digital switching systems and UC MGs directly interconnected with digital transmission facilities as an integral part of the DSN requires the use of techniques for synchronizing clock rates. The term synchronization refers to an arrangement for operating digital switching systems at a common (or uniform) clock rate where the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information. The DISN Timing and Synchronization (T&S) subsystem uses Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) transmissions from which a precise frequency is derived. This precise frequency timing signal is phase related (referenced) to Universal Time Coordinated (UTC). The T&S subsystem frequency multiplier accepts precise frequency signals from a primary source or, in case of failure, switches to an alternate source provided by atomic clocks, e.g., cesium beam or rubidium, if available. The Clock Distribution System disseminates timing through the equipment hierarchy. The DSN switches and UC MGs also may receive system timing via digital transmission facilities to locations having direct access to (synchronized to) the timing sources already described.

2.12.7 MGC-MG CCA Functions

Per Section 2.12.2.2, CCA MGC Component, the role of the MGC within the CCA is to

- Control all MGs within the SC or SS.
- Control all trunks (PRI, CAS) within each MG:
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.
- Within the SC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

2.12.8 Remote Media Gateway Requirements

A Remote Media Gateway (MG) appliance is a media gateway that is geographically separated from the SC/SS media gateway controller (MGC) that controls it. The Remote MG may be controlled by an SC or a SS. An SC/SS MGC may control several MGs with some local to the MGC and some remote to the MGC. The Remote MG connects to its MGC via an IP

CAN/MAN/WAN. Implementing a remote MG architecture allows more architectural richness in the implementation of UC solutions:

1. Replacing existing TDM trunks between a TDM EO and its serving SS with IP connectivity, thus extending IP closer to the end point.
2. In the case of a large geographical serving area, you can retain the current TDM-based switches and serve them with a remote MG via an IP CAN/MAN/WAN from a single SC. This may be the case in Europe; e.g., Mannheim-Heidelberg area where today we have several EOs with their own TDM interfaces transitioning to IP trunking by employing multiple remote MGs and single regional SC.
3. In the case of regional enterprise solutions, the SC would be centrally located with the MGs distributed at the Military Department (MILDEP) locations to allow for local PSTN access.

The architecture of a remote MG application is shown in Figure 2.12-5, Remote MG Architecture Diagram.

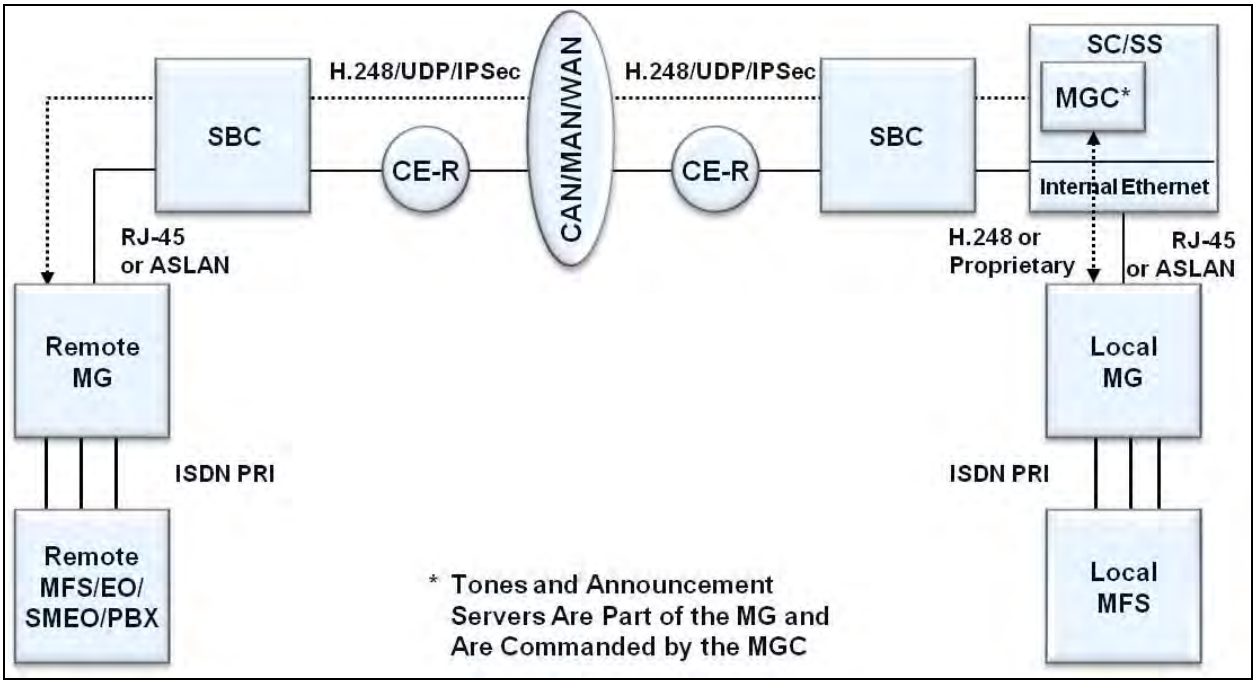

Figure 2.12-5. Remote MG Architecture Diagram

The protocol stack for Figure 2.12-5 is shown in Table 2.12-3.

Note that the H.248/UDP/IPSec signaling streams and the SRTP/IP media streams both flow through both SBCs (the SC SBC and the Remote MG SBC) in the above architecture.

Table 2.12-3. Protocol Stack

SIGNALING	MEDIA
H.248.1 with IPSec	Codec
UDP	SRTP
IP	IP
OSI Layer 2/Layer 1	OSI Layer 2/Layer 1
LEGEND	
IP: Internet Protocol	SRTP: Secure Real-Time Transport Protocol
IPSec: Internet Protocol Security	UDP: User Datagram Protocol
OSI: Open System Interconnect	

2.13 SESSION BORDER CONTROLLER

The Session Border Controller (SBC), formerly known as the Edge Boundary Controller (EBC), acts as a firewall for voice and video traffic at the ASLAN enclave boundary. All outgoing VVoIP media packets, that are marked for Assured Services and destined for points outside of the ASLAN, must be delivered to this SBC. All incoming VVoIP media packets on the WAN Access Circuit serving the ASLAN, that are marked for Assured Services and destined for points within the ASLAN, must be delivered to the SBC.

The SBC is a stateful, AS-SIP-aware application firewall that provides Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Network Address Translation (NAT), and port pinholes for individual voice and video sessions. The SBC acts as AS-SIP Back-to-Back User Agent (B2BUA).

2.14 WORLDWIDE NUMBERING AND DIALING PLAN

The DSN Worldwide Numbering and Dialing Plan is used as the addressing schema within the current DSN and its migration into the SIP environment.

The DSN user dialing format is illustrated in Table 2.14-1, DSN User Dialing Format. The digits shown in parentheses may not be dialed by the DSN user on all calls. Note that a softkey or other method may be used to indicate that a call is Routine or Precedence in lieu of explicitly dialing 94 or 9P (where P = 0, 1, 2, or 3), respectively.

Table 2.14-1. DSN User Dialing Format

ACCESS DIGIT	PRECEDENCE OR SERVICE DIGIT	ROUTE CODE	AREA CODE	SWITCH CODE	LINE NUMBER
(N)	(P OR S)	(1X)	(KXX)	KXX	XXXX
Where: • P is any precedence digit 0–4 and will be used on rotary-dial or 12-button DTMF keysets. • S is the service digit 5–9.					

ACCESS DIGIT	PRECEDENCE OR SERVICE DIGIT	ROUTE CODE	AREA CODE	SWITCH CODE	LINE NUMBER
(N)	(P OR S)	(1X)	(KXX)	KXX	XXXX
• N is any digit 2–9. • X is any digit 0–9. • K is any digit 2–8.					
NOTES: 1. Digits shown in parentheses are not dialed by the DSN user on all calls. 2. The Access Digit plus the Precedence or Service Digit constitute the Access Code.					

The following are highlights of the DSN Worldwide Numbering and Dialing Plan:

1. The current DSN numbering plan will be used in the near future by DISN Assured Services users as the means of specifying a called party address within the converged DISN. (Simply stated, an originating user will dial a DSN telephone number.) That means the subscriber's telephone number will be used as a basis for routing call requests within the AS-SIP-based converged network. The following attributes are associated with the DSN numbering plan:

   a. The internal DSN numbering plan is a private network plan (internally, a DSN number is not an E.164 number), which is modeled after the North American Numbering Plan (NPA-NNX-XXXX). Internally within the DSN, the DSN numbers are not part of the E.164-based global numbering plan; therefore, internally within the DSN, addressing will be based on a "SIP URI" using the "tel URI" with "phone context equals 'uc'" and not the Electronic Numbering (ENUM) schema. The tel URI method will provide the flexibility required when the DSN numbering plan is expanded to allow variable numbering schemes that will be used in support of coalition partner networks. The rationale is outlined as follows:

      (1) Most all DSN telephones can be direct dialed from the PSTN/PTT telephone, in addition to being direct dialed from internal DSN telephones. This is made possible because the PSTN/PTTs have assigned public telephone numbers to most DSN locations. The PSTN/PTT numbers are part of the global PSTN/PTT E.164 numbering plan. This is significant because, in the future, the PTTs can use the ENUM scheme within their own IP-based networks to address DSN numbers.

      (2) The DSN telephone number is the fundamental and globally unique address element of both the TDM- based real-time DSN and the VoIP- (e.g., SIP) based real-time UC network.

Examples of internal DSN telephone numbers and their corresponding numbers, which are used when dialing through the PSTN, are illustrated in Table 2.14-2, Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers.

Table 2.14-2. Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers

COUNTRY/ DSN LOCATION	CIVILIAN E.164 NUMBERS	DSN INTERNAL PRIVATE NUMBER
U.S./Scott AFB	+(1) 618-229-xxxx	(312) 779-xxxx
U.S./Wheeler AAF	+(1) 808-656-xxxx	(315) 456-xxxx
Germany/Patch Barracks	+(49) 711-68639-xxxx	(314) 430-xxxx
Bahrain/TCCC	+(973) 1785-xxxx	(318) 439-xxxx
Korea/Yongsan Main	+(822) 7913-xxxx	(315) 723-xxxx

2. Next, it is important to understand the relationship between basic SIP addressing, subscriber identification, and the existing DSN addressing plan and how it will be used as part of the SIP signaling messages.

   NOTE: The following examples use the SIP connotation.

   a. The simplest form of a SIP signaling message is as follows:

      sip:sgtbill@patch.eur.uc.mil

      This is sgtbill's sip identity. (Note the absence of a telephone number.)

   b. The sip identity is a type of URI called a SIP URI (RFC 3261, Section 19.1, SIP … Uniform Resource Indicators [URI]).

   c. The SIP URI has a form similar to an e-mail address, typically containing a username and a host name. In the above example, patch.eur.uc.mil is the domain of sgtbill's SIP service provider (e.g., the SC at Patch Barracks in the European Theater UC network within the .mil top-level domain).

3. The addressing system needs to correlate sgtbill's telephone number as part of the SIP URI (sip:sgtbill@patch.eur.uc.mil). This can be accomplished by analyzing the SIP URI format outlined as follows:

   a. The SIP URI general form is as follows:

      sip:user;password@host:port;uri-parameters?headers.

      (1) User: This is the identifier of a particular resource at the host being addressed.

      The userinfo part of a URI consists of the following:

      User field, Password field, and the @ sign following them.

   NOTE: The RFC does not recommend using the Password field.

      (2) The "Host" field represents the host (SC) providing the SIP resources. The Host field contains a Fully Qualified Domain Name (FQDN), an IPv4 address, or an IPv6 address. The RFC recommends using an FQDN for the Host field.

NOTE: Support for IETF FQDNs implies that UC also supports IETF Domain Name Service (DNS), which uses domain name servers and allows FQDNs to be resolved to IP addresses (and vice versa). The UC support for DNS is not a requirement in the UCR. Instead, UC support for DNS is conditional.

(3) Because we are addressing hosts that can process telephone numbers (e.g., an SC), we will use a "telephone-subscriber" field to populate the "user" field. [RFC 3966] This is accomplished by using the tel URI.

b. The tel URI specifies the telephone number as an identifier.

c. The termination point of the tel URI telephone number is not restricted. It can be in the public telephone network, a private telephone network, or the internet.

d. It can be fixed or wireless and address a fixed-wired, mobile, or nomadic terminal.

e. The terminal addressed can support any electronic communication service, including voice, data, and fax.

f. The tel URI specifies the telephone number as an identifier, which can be either globally unique, or only valid within a local context.

In summary, the tel URI allows us to bring a DSN telephone number into the internal DSN SIP addressing schema.

4. RFC 3966 defines the extent to which a telephone number is valid within a private network (e.g., a "local" number), or as a number part of the global public telephone system (e.g., a "global" number).

a. The DSN, being a private line network (although geographically it is a global network), with an internal standard numbering plan recognized by all DSN voice service locations, allows the definition of the entire DSN numbering plan as "local" telephone numbers at all SCs IAW RFC 3966.

b. Local telephone numbers must have a "phone context" parameter that identifies the scope of their validity. Standard 10-digit DSN numbers are valid throughout the DSN and the UC network, and thus, the phone context parameter in the UC network becomes phone-context=uc.mil.

Therefore, an example of a SIP URI containing a 10-digit DSN number becomes:

sip:3144301123;phone-context=uc.mil

Finally, there are two ways for SIP signaling to search for the called subscriber.

sip:sgtbill@patch.eur.uc.mil becomes:

sip:3144301123;phone-context=uc.mil@patch.eur.uc.mil;user=phone

5. There are two ways of using the SIP URI to direct the network-wide search for the SIP end point address, i.e., by NPA NNX or by a combination of a "username" (sgtbill) in conjunction with the FQDN assigned to an SC (patch.eur.uc.mil). In the near future, call requests will be forwarded (routed) based on the telephone number contained within the SIP request. Therefore, in the near future the 10 digit DSN number within the SIP URI will be used to route calls to their destination. The "phone-context=uc.mil" required by the SIP syntax is included strictly to indicate that the phone number is part of the UC network. In the long term future, the UC network may be enhanced to route calls based on FQDN within the SIP URI in addition to routing on the DSN number.

Table 2.14-3, Mapping of DSN tel Numbers to SIP URIs, provides examples of DSN numbers using SIP URIs that use the syntax defined in RFC 3966 and referenced in RFC 3261, Section 19.1.6.

Table 2.14-3. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (SC enclave) call	sip:4305335;phone-context=uc.mil@patch.eur.uc.mil;user=phone
7-digit interdomain (SC enclave) call within same area code	sip:4801235;phone-context=uc.mil@rsx.eur.uc.mil;user=phone
10-digit interdomain (SC enclave) call to another area code	sip:3157261135;phone-context=uc.mil@ysm.pac.uc.mil;user=phone

2.14.1 Domain Directory

Directories and directory services are not required or used for processing and routing of telephone call requests. Rather, the term directory services refers to the capability of using an IP telephone or other voice and/or video end points for looking up user information directly to obtain a user's telephone numbers (often referred to as "white pages" service). This eliminates the need for dialing an operator or using a hard-copy telephone book to obtain this information.

Traditionally, the subscriber assignment information contained within telephone switching systems consisted of just the subscriber telephone number, line equipment assignment, and subscriber attributes classmarks. Typically, data elements, such as the subscriber name, physical address, e mail address, or department code, were not part of the subscriber line assignment information. An internal table structure, rather than embedded databases, was used by the switching system to store this information.

Most new IP-based VoIP systems have the capability to store subscriber name, physical address, e-mail address, and/or department code in addition to the basic traditional assignment information as part of the subscriber information. Rather than using a table structure, the new systems store this information as embedded databases, often referred to as "directories" as part of the SC complex. An example of the embedded subscriber line database would be a Lightweight Directory Access Protocol (LDAP)-compliant format. This arrangement of a subscriber line

database represents a more "open standard" than a current TDM system's unique arrangement of using a table-based internal call processing structure.

The discussion of LDAP-based subscriber line databases here applies to Fixed appliances only, and not to Deployable appliances. Requirements for subscriber line databases for Deployable appliances are candidates for a future version of this document.

When the SC uses an LDAP (or other open standard)-based structure to store subscriber line data, this data can be imported easily from, or exported to, other external LDAP-based structures. The LDAP-based directories are extensible and multiple entries of "telephony" data can be added in batch mode, or additional attributes can be added to an existing LDAP directory using LDAP Interchange Format (LDIF) files. Consequently, when installing a new VoIP system, a subset of the subscriber line information can be extracted from an existing corporate directory (if it contains subscriber telephone number information) and automatically loaded into a new VoIP system. This represents a labor saving over having to build a portion of the subscriber information database manually.

Pure IP-based systems often have a built-in feature allowing importing and exporting of relevant telephone subscriber information between the VoIP system and an existing external "enterprise directory." Telephony-related data usually is stored in a single branch of the enterprise directory (referred to as the IP Telephony Network Branch). This enterprise directory is often a corporate e-mail directory. To facilitate data transfer, both the VoIP system subscriber database and the external corporate directory conform to a common standard.

Most VoIP systems provide instruments that can provide access to a "directory" function. These telephones have a display where alphanumeric information, such as telephone numbers and subscriber names, can be shown. A user can access the directory function via a dedicated button or soft keys. The VoIP system connects the telephone to the directory portion of the subscriber line database. Then the user can initiate a directory search from the telephone. This search is performed against subscriber data contained within the SC where the telephone is registered.

Additionally, VoIP systems have a feature allowing their instruments to access a Web browsing capability. Since a VoIP telephone is connected to a LAN to obtain voice services through the SC, a VoIP telephone also may be allowed to access an external directory server. This opens up possibilities: If the external directory server is accessible from the LAN, the IP telephone user may be allowed to browse to the corporate directory and perform a search of that directory, as well as the SC-contained directory.

It is anticipated that long-range functionality should be provided so that the "telephone part" of the SC directory can be imported to an external "corporate" (e-mail) directory. This function will require that the external directory is based on common standards, for example LDAP, and that the administrator in charge of the external directory extends the directory schema to add new object classes for storing the user telephony information. Likewise, the SC must have stored the subscriber directory information previously in an LDAP-based system as outlined in item 1f. Under these conditions, an LDIF file can be used to facilitate the upload of multiple entries in

batch mode, or add the telephony attributes to the existing external LDAP directory. The material here on exporting an SC directory to an external "corporate" directory (and storing subscriber directory information in an LDAP-based format) applies to Fixed (Strategic) appliances only, and not to Tactical (Deployable) appliances. Requirements for SC directory exports for Tactical (Deployable) appliances are candidates for a future version of this document.

Table 2.14-4, White Pages Directory Data Elements, shows essential elements in the white pages directory portion of the SC subscriber database.

Table 2.14-4. White Pages Directory Data Elements

DATA ITEM	EXAMPLE
USER 10-DIGIT DSN TELEPHONE NUMBER	315-454-1192
USER ORGANIZATION CODE	SCX
ORGANIZATION NAME	1st Comm Squadron
USER GEOGRAPHIC LOCATION	Langley AFB
USER NAME	Civ Bill Smith

2.15 MANAGEMENT OF NETWORK APPLIANCES

Figure 2.15-1, Network Appliance Management Model, is a logical view of a network appliance with an emphasis on its management functions. The internal implementations of the management functions are determined by the appliance supplier and may or may not align with Figure 2.15-1.

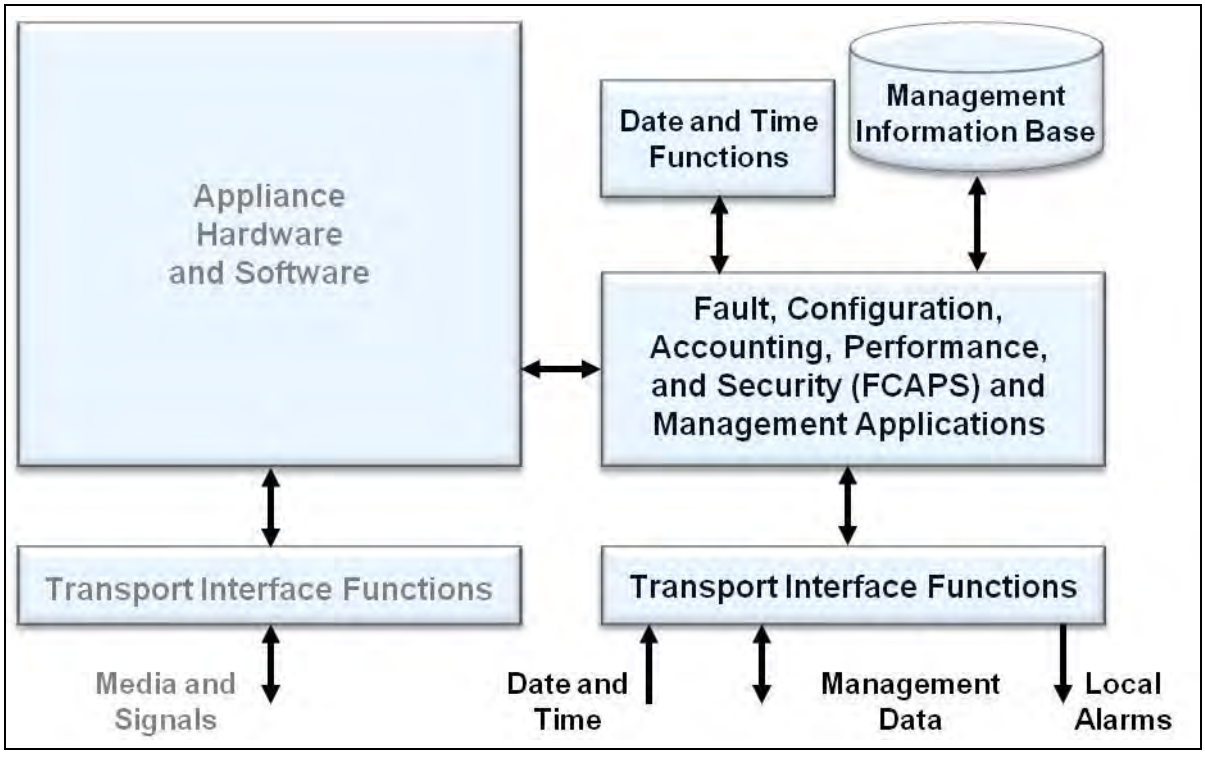

Figure 2.15-1. Network Appliance Management Model

2.15.1 Voice and Video Network Management Domain

Management of DoD's UC Voice and Video services requires each UC product have a minimum of two separate management domains. One domain provides local, on-site craft person type support, typically referred to as Operations, Administration, Maintenance, and Performance (OAM&P), while the other domain provides a remote, centralized management capability, typically referred to as NM. There is no attempt to delineate the responsibilities between these two functions in this section. The two domains must have simultaneous access to the UC products to effectively perform the DoD's end-to-end UC Management function. Where necessary, for clarification, the remote NM system will be referred to as the VVoIP Element Management System (EMS) and the local OAM&P system will be referred to as the Local EMS. See Figure 2.15-2, Relationship of UC Managements.

Figure 2.15-2. Relationship of UC Managements

2.15.2 General Management Approach

SCs and SSs must be capable of providing the following NM data to the VVoIP EMS:

- Alarm/log data.
- Performance data (e.g., traffic data).
- Accounting data (e.g., call detail recording).

SCs and SSs must allow the VVoIP EMS to have access to perform SC/SS datafill administration and network controls. Telcordia Technologies GR-740-CORE acts as guide for the interface between the network appliances (or components) and the external VVoIP EMS.

The preferred approach to managing the DoD VVoIP is using SNMP and MIBs. The two applicable IETF Standards are Standard 58 and 62. These two standards are composed of the following RFCs:

- Standard 58, Structure of Management Information Version 2 (SMIv2):
  - RFC 2578.
  - RFC 2579.
  - RFC 2580.
- Standard 62, Simple Network Management Protocol Version 3 (SNMPv3):
  - RFC 3411.
  - RFC 3412.

- RFC 3413.
- RFC 3414.
- RFC 3415.
- RFC 3416.
- RFC 3417.
- RFC 3418.

RFC 1213 is also referenced for Management Information Base II (MIB-II) definitions.

In addition to the direction provided by the documents noted above, FCAPS, the International Organization for Standardization (ISO) Telecommunications Management Network model and framework, guides how UC network management is performed. The FCAPS model organizes network management into five functional areas: fault, configuration, accounting, performance, and security.

Fault Management supports the detection, isolation, and correction of abnormal operating conditions in a telecommunications network and its environment. Fault Management provides the functions to manage service problems, to support customer interactions associated with service troubles, and to support business policies related to service problems.

Configuration Management (CM) exercises control over, identifies, collects data from, and provides data to NEs and the connections between NEs. Configuration Management is responsible for the planning and installation of NEs and their interconnection into a network. Configuration Management includes the establishment of customer services that use the network, all services and product planning, and business policy level functions related to service establishment.

Accounting Management enables the network service usage to be measured and the costs for such use to be determined. It provides facilities to collect accounting records and to set billing parameters for the usage of services and for access to the network.

Performance Management (PM) evaluates and reports the effectiveness with which the network and its NEs support assigned services. Performance Management provides mechanisms to measure service quality and provides the business policy functions for quality control.

Security management provides for prevention and detection of improper use or disruption of network resources and services, for the containment of and recovery from theft of services or other breaches of security, and for security administration. The VVoIP EMS uses the security services of access control, confidentiality, integrity, availability, and non-repudiation as specified in UCR Section 4, Information Assurance.

2.15.3 Traffic Flow Control Overview

Performance management evaluates alarm and performance data and, to minimize the effect on network traffic caused by a network anomaly, implements traffic flow controls.

Within an IP network, the SC handles only call signaling, while the IP network connecting the two communicating end instruments handles the bearer stream. The SC congestion resulting from an overload of SIP requests must be detected and controlled. Bearer stream congestion will affect non-real-time as well as real-time bearer traffic, making it an IP NM concern. While good traffic engineering and the presence of an MPLS router core mitigates much of the traffic congestion within LAN and WAN environments, congestion at the boundaries between these domains is of concern and needs specific detection and control actions to mitigate the congestion.

The SC congestion occurs when the volume of AS-SIP messages exceeds the SC's capacity to process them. A particular vendor's SC solution may threshold and alarm on congestion, but a simpler approach may be monitoring the Central Processing Unit (CPU) utilization on the SC host. Alarms generated from CPU utilization threshold violations could be the trigger events necessary for the VVoIP EMS to take the appropriate pre-emptive policy-based management action to execute PEI/AEI destination controls, limiting other SCs and their PEIs/AEIs from sending SIP (or proprietary protocol) messages to the overloaded SC. From the viewpoint of these other SCs, in effect, a code control would be executed on them.

Detection of network congestion at the edge of the LANs and WAN (DISN Core) resides with the performance management tools in place over those networks. These performance management tools must detect and report (via SNMP or syslog events) bandwidth utilization threshold violations in each of the CE-R, NIPRNet AR traffic queues. For the ARs, this must be by a southbound (CE connected) interface. From these events, each domain's policy-based management system must take the appropriate (precoordinated) control actions to mitigate the congestion.

Given no change in the physical resources (i.e., a larger bandwidth connection between the LAN and WAN), three basic actions can be taken to reduce congestion at the network edge:

1. Place a code control on other SCs to reduce the load of SIP messages sent through the overloaded edge (although this would have minimal effect on reducing the bearer traffic, unless done in conjunction with a call budget and bandwidth change).
2. Change the call budget on the SC, with a corresponding change in the VVoIP queue bandwidths on the CE and PE Routers.
3. Reallocate the queue bandwidth on the CE and PE Routers.

In summary, three control actions can help reduce congestion in the IP-based voice network: implementing EI destination controls, call budget changes, and router queue bandwidth

allocations. The first two controls are in the Session Control domain and are described further below.

2.15.3.1 Destination Code Controls

Destination Code Control functionality is applied at the SC or SS to prevent or limit the number of calls (session requests) to reach a specific destination. Destination code controls are applied to reduce calls to a specific area or location that has been temporarily designated as "difficult to reach" due to circumstances.

Within the DISN, call completion "difficulties" may include fixed or deployable situations for which a commander may want to minimize traffic to a given destination or set of destinations, such as a theater of operations. Given this, Minimize (currently a behavioral control to reduce traffic to a particular destination or region) initiated by a commander's order could be enforced using code controls, and set up to allow only FLASH and FLASH OVERRIDE traffic to be passed to the minimized destination.

2.15.3.2 Call Budget Control

Setting the call budgets on the SS and SC involves setting the maximum number of calls (voice and video) that may be in service at one time within, and/or to and from a local service area (i.e., military installation).

See Section 2.4, ASAC Operation Overview, for more information on call budgets.

2.16 DYNAMIC ASAC

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 Section 2.4, ASAC Operation Overview, 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.

The DASAC budget is based on metrics derived from the parameters shown in Table 2.16-1, EISC Estimation Parameters.

Table 2.16-1. EISC Estimation Parameters

#	PARAMETER	SOURCE	COMMENT
1	Codec Rate (bps)	Product extracts from SDP message; stored per codec class	Could change on a session-by-session basis per EI and within a session
2	Packet Rate (PPS)	Product extracts from information in SDP message	Could change on a session-by-session basis per EI and within a session. When the respective EIs support bearer-based mid-session renegotiation and if the product lacks the ability to process this bearer layer information, the PPS parameter needs to be set to the highest bits per second rate option available to the bearer-based mid-session renegotiation capability
3	Number of Sessions in Progress	Number of sessions in progress for this codec class. This includes sessions in both the setup and active states Running account kept by product	Initial value equals zero Incremented upon successful session connection Decremented upon successful session completion

#	PARAMETER	SOURCE	COMMENT
4	Tunnel Overhead Factor (bytes)	Pre-provisioned and entered into product	Indicates the number of overhead bytes that must be added to the IP packet size to account for encryption or other types of tunnels. If some sessions are tunneled and others are not, use the number of bytes associated with the largest overhead tunnel. Default is 100 bytes. Minimum 0 bytes. Maximum 512 bytes
5	IP Overhead (bytes)	Pre-provisioned and entered into product, includes IP, UDP, and RTP or SRTP overhead associated with packet flow over the target link	If IPv6, use 60 bytes If IPv4, use 40 bytes Default is 60 bytes
6	Layer 2 Overhead (bytes)	Pre-provisioned and entered into product	Sized according to layer 2 protocol used on target link—this parameter is the same for all packets in all codec classes. Default is 20 bytes
7	Safety Factor (%)	Pre-provisioned and entered into product	This parameter is used to provide a margin of error for the EISC calculation. Default is 10%
8	Voice Multiplexer (MUX) Overhead per Packet (bytes)	Pre-provisioned and entered into product	This parameter is used on a per packet basis if a voice MUX is used. There is no default value. Minimum 0 bytes. Maximum 512 bytes
9	Overhead per Voice MUX Sample (bytes)	Pre-provisioned and entered into product	This parameter is an overhead that is applied to each voice sample bundled in an output voice packet. There is no default value. Minimum 0 bytes. Maximum 512 bytes

Parameters 1 through 3 in Table 2.16-1, EISC Estimation Parameters, are dynamic and are calculated on a session-by-session basis. Parameters 4 through 9 are preloaded into the product based on traffic engineering analysis of the link.

The DASAC budget metrics are as follows:

- EI Session Capacity (EISC). The bandwidth required (in bps) for a session.
- Transmission Link Session Capacity (TSC). The capacity (bps) of the bottleneck link associated with the SC Path. The TSC is a pre-provisioned parameter entered for each SC Path link via NM commands. The TSC does not include an allocation for session signaling. Session signaling must be provisioned separately as part of traffic engineering for the bottleneck link on the path.
- Available Link Session Capacity (AVSC). The capacity (bps) currently available for sessions on the SC Path. The AVSC is calculated at each of the following events:
  - The session establishment AS-SIP dialog (specifically the AS-SIP message containing the SDP answer).
  - Mid-session re-INVITE dialog based on a mid-session codec change (specifically the AS-SIP message containing the new SDP answer to the new offer).
  - Session teardown (specifically based on SC detecting the AS-SIP 200 (OK) for the BYE).

The AVSC is calculated as follows:

AVSC = TSC—the sum of EISCs for all sessions in progress and in the process of being established on the SC Path

Figure 2.16-1, AS-SIP Triggers for AVSC, illustrates the AS-SIP triggers for the AVSC calculations. For reasons of simplification, it assumes the EIs are AS-SIP enabled. It is also assumes that only one session is preempted to enable a new session to be accepted. This is not meant to preclude the preemption of multiple lower precedence setup and/or active sessions collectively, with a higher than or equal to, bits per second bearer rate, to allow a new, higher precedence session with a lower than or equal to, bits per second bearer rate to be admitted.

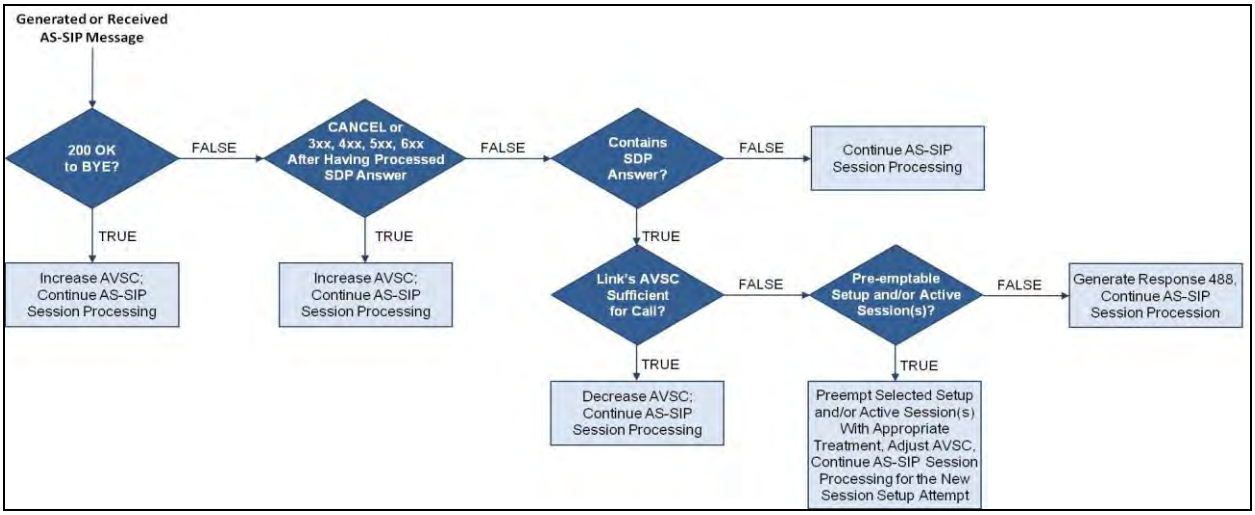

Figure 2.16-1. AS-SIP Triggers for AVSC

When a "200 OK" is received by the product, the bandwidth previously reserved for this session is released and thereby the AVSC is increased.

The "SDP Answer" message indicates the results of the codec negotiation between the EIs involved in the session request. The product processes the SDP Answer to determine whether there is sufficient capacity to support the new session. If so, the product will reserve bandwidth for the session and continue with AS-SIP session processing. If a Cancel or a 3xx, 4xx, 5xx, or 6xx message is received after the SDP Answer is processed but before the session setup is completed, the reserved capacity will be released and the AVSC increased accordingly.

If after receiving an SDP answer, the product determines if there is insufficient bandwidth for the new session. The product will review all sessions in progress, which includes those that are being set up ("setup sessions") and those that are active, to determine if any have lower precedence than the new session. If there are none, the new session will be blocked. If lower precedence sessions do exist, the product will use the algorithm specified below or its equivalent to determine if the new session must be blocked or alternately admitted after the preemption of one or more setup and/or active sessions:

1. The product will determine the precedence level (P) of the new session attempt, where P is an integer between 1 and 5, representing increasing levels of precedence. The lowest precedence is Routine, with P =1. The precedence level of the new session attempt is P = N.
   a. If N=1, the new session attempt is blocked because a new session can only preempt a lower precedence session. The product will exit this algorithm.
   b. If N is >1, the product will determine if EISC(N), the capacity of the new session, is =< AVSC (where AVSC is the available capacity):
      (1) If so, the product will accept the new session, set AVSC to = AVSC - EISC(N) and exit this algorithm.
      (2) If not, the product will set P = 1. The product will continue to the next step.
2. The product will determine if there is any combination of setup sessions at precedence level P that, if preempted along with all sessions at a lower precedence, would provide sufficient capacity to support the new session.
   a. If so, the "optimum" combination of setup sessions will be preempted and the new session will be accepted. The optimum combination is the one that provides the required capacity with the least number of preempted setup sessions. The product will set AVSC = AVSC plus the capacity of all preempted calls (including all sessions at lower precedence levels) minus EISC(N). The product will exit this algorithm.
   b. If not, the product will determine if there is some optimum combination of one or more active sessions at P which, if preempted along with all setup sessions at P and all current sessions at a lower precedence than P, will provide sufficient capacity for the new session. The optimum combination is the one that provides the required capacity with the least number of preempted active sessions at P. The combination of all preemptable sessions is called the "identified sessions".
      (1) If there is such an optimum combination, all identified sessions will be preempted and the new session will be accepted. The product will set the new AVSC to equal AVSC plus the capacity of the identified sessions minus EISC(N). The product will exit this algorithm.
      (2) If not, the product will continue processing as described in the next step.
3. The product will increment P by 1.
   a. If P = N, the setup attempt will be blocked. The product will exit this algorithm.
   b. If P < N, the product will re-execute step 2.

If one or more preemptions occur and the new session is established, the resulting AVSC may be larger or smaller than before the preemption(s). If the preempting session's bandwidth requirement is less than that of the preempted session or sessions, the AVSC increases. If the preempting session's bandwidth requirement is more than that of the preempted session or sessions, the AVSC decreases.

If one or more preemptions occur and the new session is established, the resulting AVSC may be larger or smaller than before the preemption(s). If the preempting session's bandwidth requirement is less than that of the preempted session or sessions, the AVSC increases. If the preempting session's bandwidth requirement is more than that of the preempted session or sessions, the AVSC decreases.

2.16.1.1 Dynamic ASAC Calculation Examples

Examples of notional EISC calculation for voice sessions are given in Tables 2.16-2 through 2.16-5. The environment for Examples 1, 2, and 4 is shown in Figure 2.16-2, Notional System Architecture for Examples 1, 2, and 4. The environment for Example 3 is shown in Figure 2.16-3, Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel). The example environments consist of 20 VoIP phones, each of which can support G.711, G.729, G.723, and 2400 bps Enhanced Mixed Excitation Linear Production (MELPe) codecs. The TSC for the controlled link is 256 Kbps full duplex. The examples differ in the number and types of communication devices that are used to support UC traffic flow. Point-to-Point Protocol (PPP) is used as the layer 2 protocol. It provides a 7-byte layer 2 overhead per packet.

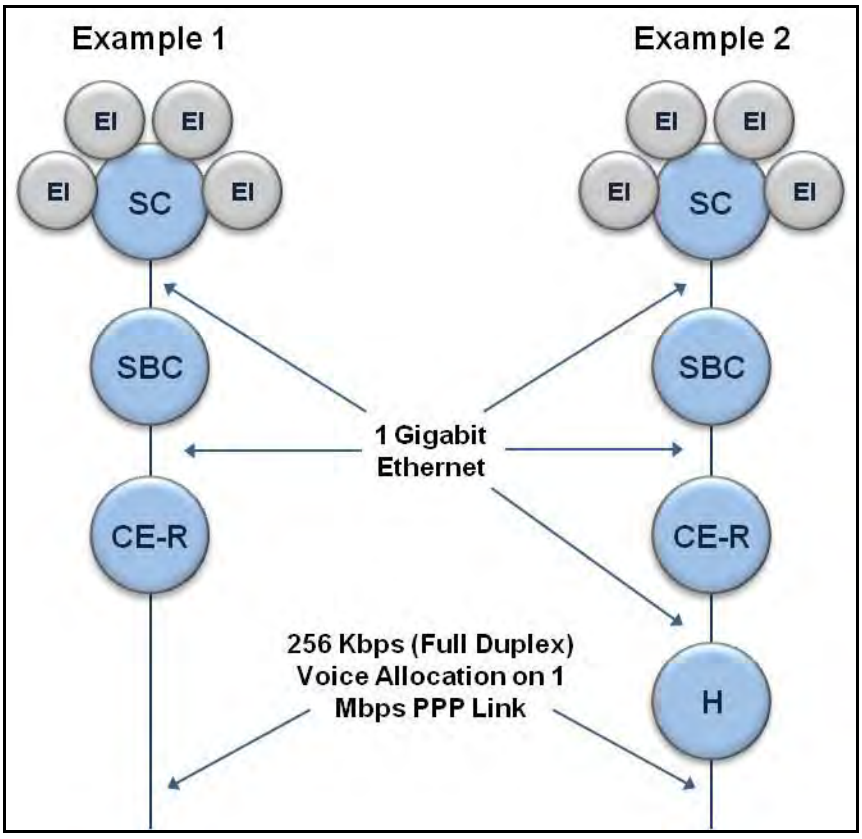

Figure 2.16-2. Notional System Architecture for Examples 1, 2, and 4

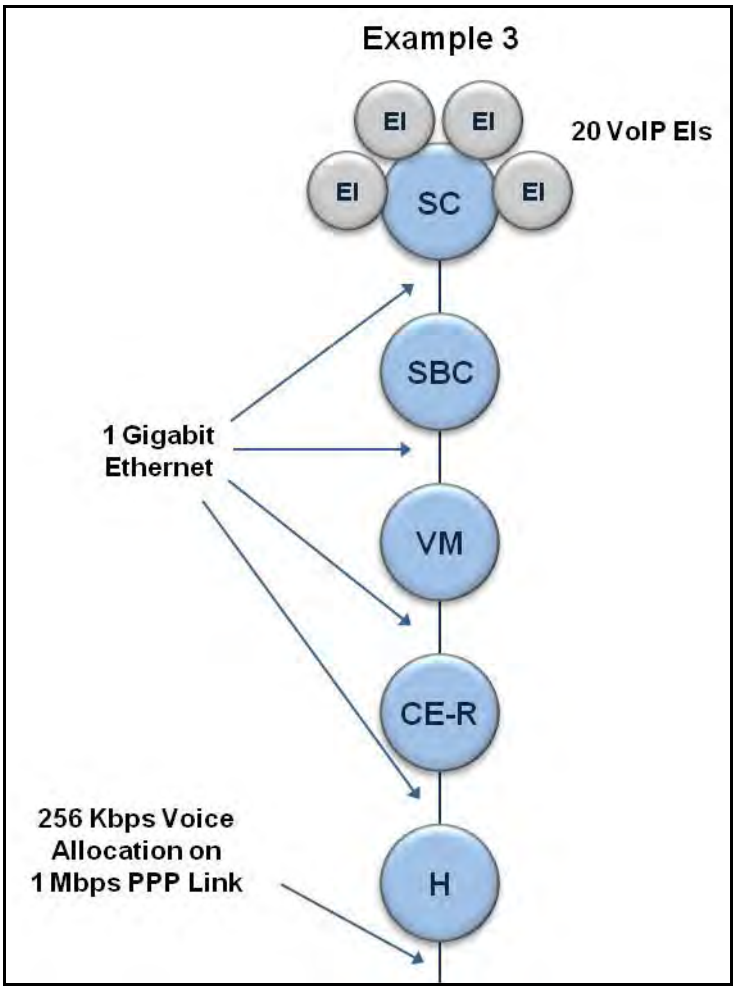

Figure 2.16-3. Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel)

In Tables 2.16-2 through 2.16-5, the bolded, non-italicized numbers represent parameters that have been pre-entered into the product via NM commands. The bolded, italicized numbers are calculated by the product based on inspection of signaling packets. The non-bolded numbers are the calculations made by the product as part of the AVSC determination.

Example 1 (Table 2.16-2, Example 1: Current Session Status (No HAIPE Case)) shows a case where there is no HAIPE or voice MUX. There are eight sessions in progress. Five of these are MELPe sessions with one session each for the other codecs. The total EISC for these sessions is 176.8 Kbps, as shown in Table 2.16-2. The AVSC is 79.2 Kbps, based on a TSC of 256 Kbps. In this case, the SC could admit a new session using any of the codec types except G.711. If the next session offers a G.711 codec, the SC must block the session unless there is a lower precedence session that can be preempted.

Example 2 (Table 2.16-3, Example 2: AVSC Calculation assuming the G.711 Session is new (HAIPE Case) shows a case where a HAIPE is used to encrypt packets traversing the bottleneck link. In this example, there are seven sessions in progress: five MELPe sessions, one session for

G.723.1, and one session for G.729. Also shown is one "potential" (new) G.711 session. The AVSC calculation takes place just after an INVITE request for a new G.711 session is generated. The SC calculates the AVSC for the G.711 session at negative 7.3 Kbps (see Table 2.16-3). The SC will reject the new session if it cannot preempt one of the existing sessions.

Table 2.16-2. Example 1: Current Session Status (No HAIPE Case)

	TLCC	IPV4 TLCC= 256 Kbps				
ID	Codec Type		MELPe	G723.1	G729	G711
1	Codec Rate	Kbps	***2.4***	***5.3***	***8***	***64***
2	Packet Rate	Packets per Second	***11.1***	***33.3***	***50.0***	***50.0***
3	Number of Voice Sessions in Progress		***5***	***1***	***1***	***1***
4	Tunnel Overhead	Bytes	**0**	**0**	**0**	**0**
5	IP Overhead	Bytes	**40**	**40**	**40**	**40**
6	Layer 2 Overhead	Bytes	***7***	***7***	***7***	***7***
7	Safety Factor	%	**10%**	**10%**	**10%**	**10%**
8	Payload Size	Bytes	28	20	20	160
9	Packet Size	Bytes	68	60	60	200
10	Packet Rate	Kbps	6.0	16.0	24.0	80.0
11	Layer 2 Overhead	Kbps	0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps	6.7	17.8	26.8	82.8
13	EISC (including Safety Factor) per call	Kbps	7.3	19.6	29.5	91.1
14	Total EISC for all calls in Codec Group	Kbps	36.7	19.6	29.5	91.1
15	Total EISC for all calls on link	Kbps	176.8			
	Grand Total Calls		8			
	AVSC	Kbps	79.2			

Table 2.16-3. Example 2: AVSC Calculation Assuming the G.711 Session Is New (HAIPE Case)

		HAIPE TUNNEL IPV4 TLCC= 256 Kbps				
ID	Codec Type		MELPe	G723	G729	G711
1	Codec Rate	Kbps	***2.4***	***5.3***	***8***	***64***
2	Packet Rate	Packets per Second	***11.1***	***33.3***	***50.0***	***50.0***
3	Number of Voice Sessions in Progress		***5***	***1***	***1***	***1***
4	Tunnel Overhead	Bytes	***52***	***52***	***52***	***52***
5	IP Overhead	Bytes	**40**	40	40	40
6	Layer 2 Overhead	Bytes	***7***	***7***	***7***	***7***
7	Safety Factor	%	**10%**	**10%**	**10%**	**10%**
8	Payload Size	Bytes	28	20	20	160
9	Packet Size	Bytes	120	112	112	252
10	Packet Rate	Kbps	10.7	29.8	44.8	100.8
11	Layer 2 Overhead Rate	Kbps	0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps	11.3	31.7	47.6	103.6
13	EISC (including Safety Factor) per call	Kbps	12.4	34.9	52.4	114.0
14	Total EISC for all calls in Codec Group	Kbps	62.1	34.9	52.4	114.0
15	Total EISC for all calls on link	Kbps	263.3			
	Grand Total Calls		8			
	AVSC	Kbps	-7.3			

Example 3 (Table 2.16-4, Example 3: Use of Voice MUX with a HAIPE Tunnel) shows the case where a voice MUX is used to reduce the EISC per voice session. The environment for this

example is given in Figure 2.16-3, Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel). The TSC is 256 Kbps (full duplex). The network also contains a HAIPE device. Eight sessions are active: five MELPe sessions and one session each based on G.723.1, G.729, and G.711 codecs.

Table 2.16-4. Example 3: Use of Voice MUX With a HAIPE Tunnel

	Voice Mux Calls	IPV4					
	Per Codec Type Calculations	TLCC=	256	Kbps			
ID	Codec Type		Packet	MELPe	G723	G729	G711
1	Codec Rate	Kbps		***2.4***	***6.4***	***8***	***64***
2	Packet Rate	PPS		***11.1***	***33.3***	***50.0***	***50.0***
3	Number of Voice Sessions in Progress			***5***	***1***	***1***	***1***
4	Overhead for voice mux sample	Bytes		***7***	7	7	7
5	Payload size	Bytes		28	24	20	160
6	Payload traffic rate	Kbps		2.49	6.40	8.00	64.00
7	Voice mux overhead traffic rate	Kbps		3.1	1.9	2.8	2.8
8	Voice mux and payload traffic rate	Kbps	91.5	5.6	8.3	10.8	66.8
	Per Packet Overhead Calculation						
9	Tunnel overhead	Bytes	52				
10	IP overhead	Bytes	**28**				
11	Voice mux overhead per packet	Bytes	**4**				
12	Layer 2 overhead	Bytes	**12**				
13	Safety Factor	%	**10%**		Packet rate is calculated		
14	Total per packet overhead rate	Kbps	42.24		as the maximum Packet		
15	Total EISC for all calls in progress	Kbps	133.7		Rate above (ID=2)		
	Grand Total Calls		8				
	AVSC	Kbps	122.3				

The calculation takes into account two types of overhead; one for each output packet generated by the voice MUX; the other for each voice sample in the output packet. The per-packet overhead consists of the IP, tunnel and voice MUX byte overheads for each output packet. This overhead is multiplied by the output packet rate to determine the overhead rate in Kbps. The output packet rate is set at the highest rate of the codecs supported by the EIs on the SC side of the SC Path. The voice sample overhead is the number of bytes that the voice mux appends to each voice sample encapsulated in the output packet. The number of bytes per sample is multiplied by the voice sample rate of the input packets, to determine the overhead rate in Kbps.

The EISC, for this example, is 133.7 Kbps. The AVSC is 122.3 Kbps, based on a TSC of 256 Kbps. In this case the SC could admit a new session from any of the codec types. Compared to Table 2.16-3, Example 2: AVSC Calculation Assuming the G.711 Session in New (HAIPE Case), the use of the voice mux reduces the bandwidth demand from 263.3 Kbps to 133.7 Kbps, based on the notional numbers used in the examples.

Example 4 (Table 2.16-5, Example 4: Use of Header Compression with a HAIPE Tunnel) shows the case where header compression and HAIPEs are used. This example is based on the environment used in Example 2 with one addition: the CE-R supports header compression on the bottleneck link. The IP overhead parameter has been modified to account for a header compression mechanism that, on average, transmits 95 percent of packets with a compressed

header of two bytes, and 5 percent of packets with a full IP, UDP, and RTP header of 40 bytes. This gives an average header size of 3.9 bytes, which has been rounded up to 5 bytes to provide a margin of safety. An approximate overhead factor of 4 percent has been added to account for MELPe overhead.

Table 2.16-5. Example 4: Use of Header Compression With a HAIPE Tunnel

		HAIPE TUNNEL				
		IPV4				
		TLCC=	**256** Kbps			
ID	Codec Type		MELPe	G723	G729	G711
1	Codec Rate	Kbps	***2.4***	***5.3***	***8***	***64***
2	Packet Rate	Packets per Second	***11.1***	***33.3***	***50.0***	***50.0***
3	Number of Voice Sessions in Progress		***5***	***1***	***1***	***1***
4	Tunnel Overhead	Bytes	**52**	**52**	**52**	**52**
5	IP Overhead	Bytes	***5***	5	5	5
6	Layer 2 Overhead	Bytes	***7***	***7***	***7***	***7***
7	Safety Factor	%	**10%**	**10%**	**10%**	**10%**
8	Payload Size	Bytes	28	20	20	160
9	Packet Size	Bytes	85	77	77	217
10	Packet Rate	Kbps	7.6	20.5	30.8	86.8
11	Layer 2 Overhead Rate	Kbps	0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps	8.2	22.4	33.6	89.6
13	EISC (including Safety Factor) per call	Kbps	9.0	24.6	37.0	98.6
14	Total EISC for all calls in Codec Group	Kbps	45.0	24.6	37.0	98.6
15	Total EISC for all calls on link	Kbps	205.1			
	Grand Total Calls		8		MELP overhead	
	AVSC	Kbps	50.9		factor =	**1.037**

The AVSC is 50.9 Kbps, which would enable the SC to accept any new session request without preemption or blocking, except for a session that requires a G.711 codec.

SECTION 3
AUXILIARY SERVICES

This Section contains explanatory text on some of the Auxiliary Services Requirements in Unified Capabilities Requirements (UCR) 2013, Section 3, Auxiliary Services. It also contains explanatory text on other Auxiliary Services in the Unified Capabilities (UC) Network, including Services provided by Required Ancillary Equipment, and Services provided by UC Gateways (such as Centralized Connections to Commercial Voice Internet Service Providers, Centralized Secure Connections to Wireless Providers, and Allied Network Interfaces).

3.1 REGIONAL HUB DESIGN FOR REQUIRED ANCILLARY EQUIPMENT (RAE)

Operation of UC products requires management/security support from server functions that normally are not part of a Softswitch (SS), Session Controller (SC), or Session Border Controller (SBC) product. These functions/severs are referred to as Required Ancillary Equipment (RAE) and must be made available at the site to support the SS, SC and SBC. The RAE support includes Authentication, Authorization, and Accounting (AAA) servers; access to a Domain Name Service (DNS) server; SYSLOG server; Network Time Protocol (NTP) server; Dynamic Host Configuration Protocol (DHCP) server; and Department of Defense (DoD) Public Key Infrastructure (PKI) certificate verification, including access to an Online Certificate Status Protocol (OCSP) responder.

As a companion project associated with relocating SSs from DoD Components to the Defense Information Systems Agency (DISA) network domain and security enclaves, DISA is in the process of procuring and installing RAE to support the SS nodes. To simplify management, minimize staffing and equipment cost centralized RAE hubs will be installed at Hickam, Scott, and Vaihingen. The three RAE hubs will provide support to the SSs within each theater. The RAE hub components will reside within the Defense Information Systems Network (DISN) network domain and DISA security enclaves. The operational concept for the regional RAE hub arrangement is illustrated in Figure 3.1-1.

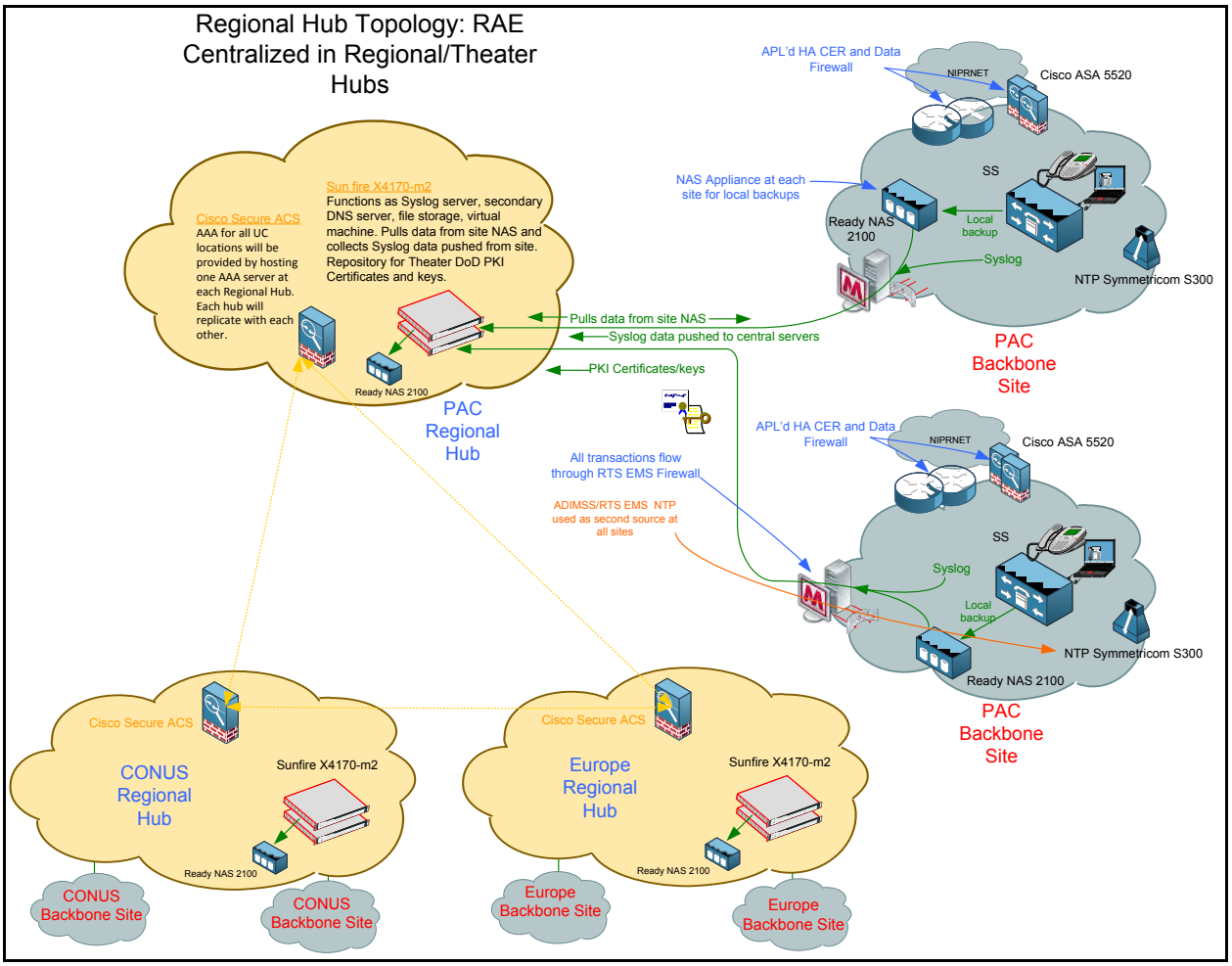

Figure 3.1-1. Regional RAE Hub Topology

1. Each SS in the network will have a 1 rack unit Network Attached Storage (NAS) appliance installed at the local site. The local on-site NAS provides a method to meet the local backup requirement without hosting a server. The on-site SS servers will push complete disk images to the local NAS and the central hub-based servers will pull the images from each NAS on a regular basis. The local file storage capability will be provided by a NETGEAR Ready NAS 2100 with 4 Terabytes (TB) of storage capacity.

2. The regional hubs will be equipped to provide off-site system backup storage, Authentication, Authorization, and Accounting (AAA) Services, SYSLOG, secondary DNS service, and storage of Internet Protocol (IP) Detail Records (IPDRs). The following equipment will be installed at each regional hub:

   a. AAA Services will be provided by one (1) Cisco 1121 Access Control System appliance with Cisco Secure Access Control System 5.2. The Cisco Access Control Server (ACS) will be configured to provide centralized AAA services to all other DISN UC Backbone locations/equipment (SS, SBCs, Firewalls [FWs], Customer Edge [CE] Routers [CE-Rs], Access Switches, etc.) within the theater by invoking either Remote Authentication Dial-

in User Server/Service (RADIUS) or Terminal Access Controller Access Control System (TACACS).

Additionally, the ACS servers will be configured to replicate with the other regional ACS servers located at the two other hub locations.

b. Centralized Services will be provided to support off-site system backup storage, SYSLOG, secondary DNS service, and storage of Internet Protocol Detail Record's (IPDR) will be provided centrally by a server located at each regional hub. The centralized services will be provided by two Oracle Sun Fire X4170-m2 servers, one active and one backup.

3.2 COMMERCIAL COST AVOIDANCE AND HYBRID ROUTING FEATURE

The Routing Database (DB) is a DISA-owned and DISA-operated DB that contains records of the Defense Switched Network (DSN) numbers, commercial (Public Switched Telephone Network [PSTN]) numbers, SC identifiers, and SS identifiers for UC end users served by SCs. This DB may also contain records of DSN numbers and commercial numbers for individual DSN end users served by DSN End Offices (EOs) and Private Branch Exchanges (PBXs). The DB records may be populated automatically by SCs, whenever end users' numbers are added to an SC during activation of that end user on the SC. The DB records also may be populated manually by a DISA craftsperson, using DSN and commercial number information from an SC site or DSN EO or PBX site.

The SSs that support the Hybrid Routing (HR) feature query the Routing DB to determine whether there is an SC identifier, a primary SS identifier, and a backup SS identifier stored there that matches the dialed DSN number on a UC call that enters the SS. Figure 3.2-1, Hybrid Routing Feature Operation in the Network, illustrates how the Hybrid Routing Feature operates in the network.

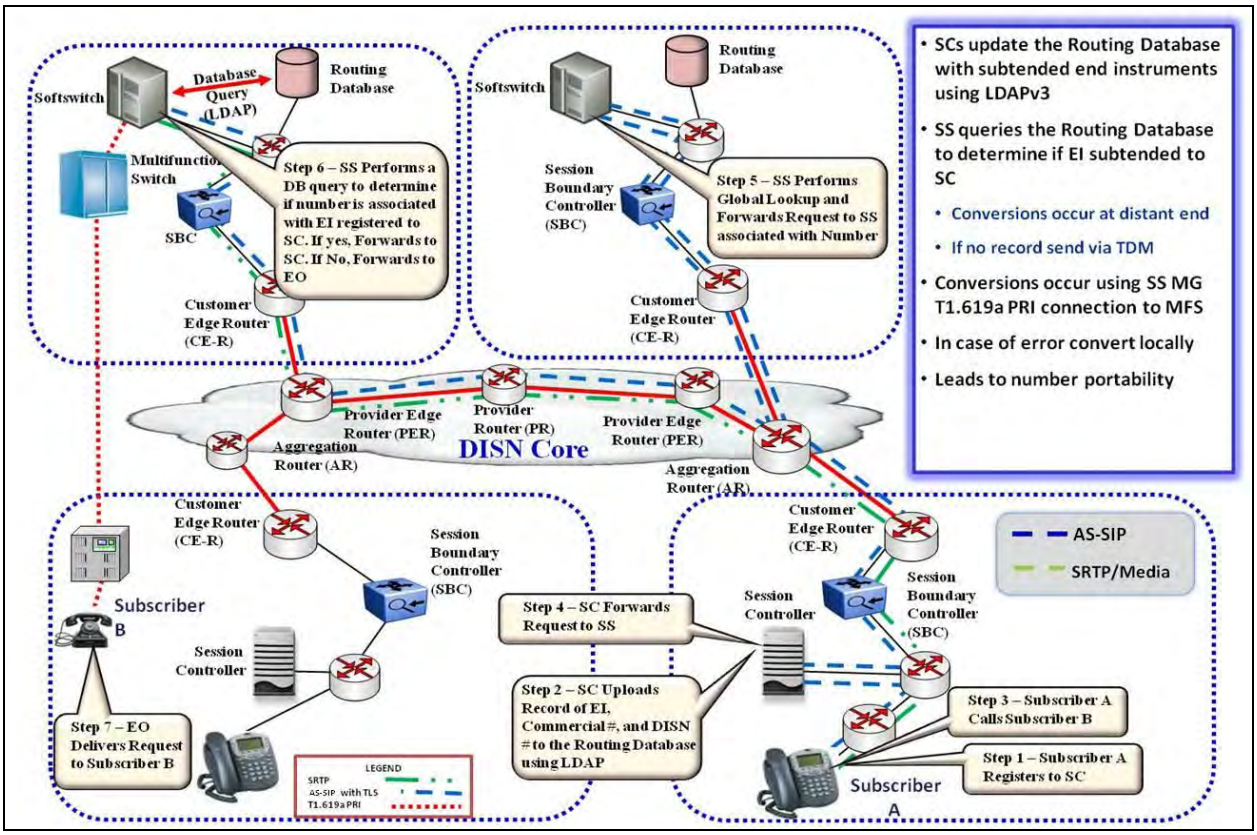

Figure 3.2-1. Hybrid Routing Feature Operation in the Network

The SCs that support the Commercial Cost Avoidance feature query the Routing DB to determine whether there is a DSN number stored there that matches the dialed commercial number on a commercial call from the SC (e.g., a 9+9 call, or a 9+8 call). Figure 3.2-2, Commercial Cost Avoidance Feature Operation in the Network, depicts how the Commercial Cost Avoidance feature operates in the network.

The protocol that SCs and SSs use to query and update the Routing DB is Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), secured using Transport Layer Security (TLS), and signaled via IP over the DISN Wide Area Network (WAN).

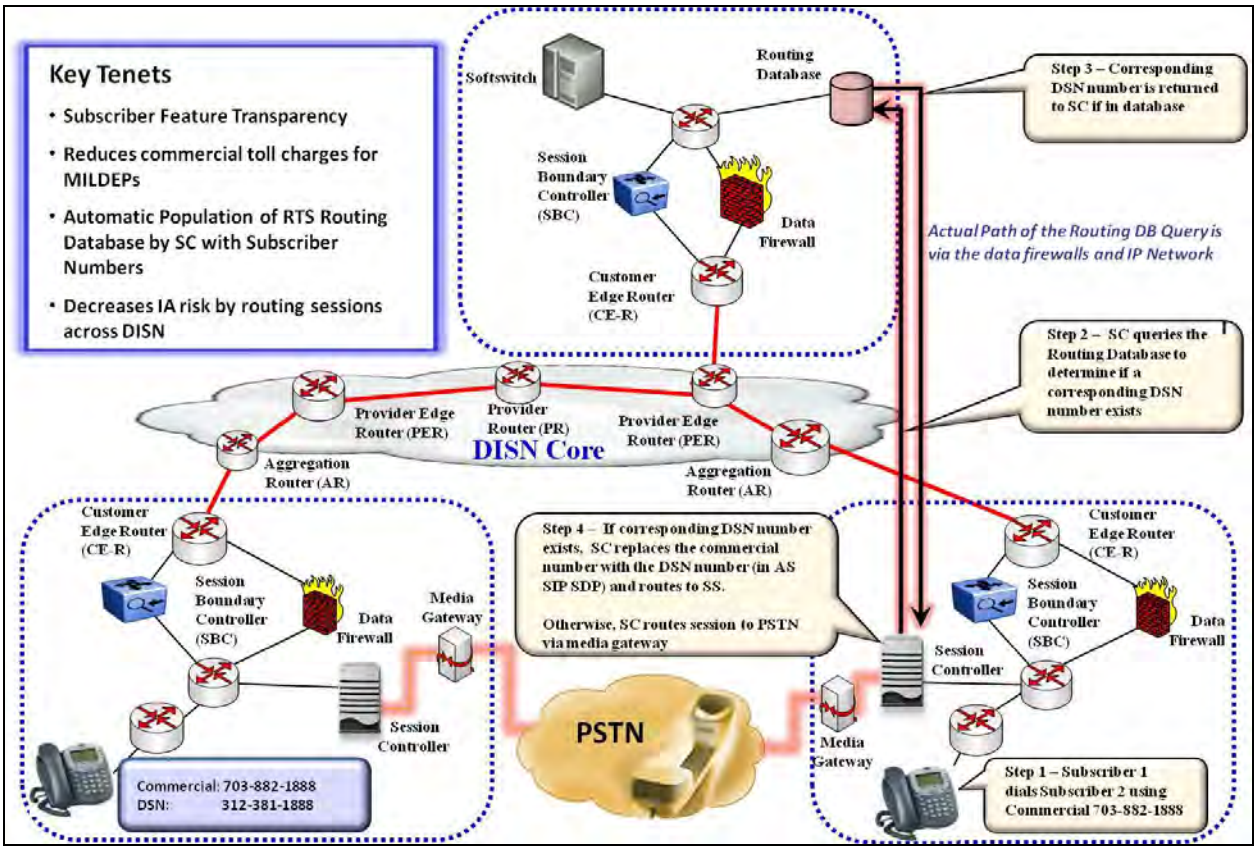

Figure 3.2-2. Commercial Cost Avoidance Feature Operation in the Network

3.3 INTERFACE TO EMERGENCY RESPONSE SYSTEMS

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

3.3.1 Enhanced 911 Interface

Access to Enhanced 911 is available from SC/Media Gateways using the dial plan. This interface is Time Division Multiplexing (TDM) because of Information Assurance requirements. E911 Management Systems interface with SCs to provide reliable user locations to Public Safety Answering Points (PSAPs), including cases where DoD components host a PSAP for E911 services.

3.3.2 Mass Notification Warning System Interface

The Mass Notification Warning System will be used to meet the DoD's requirements to provide Association of Public-Safety Communications Officials (APCO) – International, Project 25, systems at DoD locations. The Mass Notification Warning System is a product that monitors event sources and if an event from an event source meets pre-defined emergency criteria then the

default action is for the Mass Notification Warning System (MNWS) to inform system operators of the event. The operators qualify the event and when appropriate instructs the system to initiate alerts. The system then initiates alerts via interfaces to alert delivery systems.

Currently all local access to any public network such as PSTN service; E911; and APCO – International, Project 25, systems must be via TDM and cannot be transmitted over IP, because of Information Assurance requirements. The only connection to the PSTN is through a TDM interface using Primary Rate Interface (PRI) or Channel Associated Signaling (CAS), so there is no interaction between the Voice and Video over IP (VVoIP) system and commercial VVoIP IP networks.

3.4 OTHER AUXILIARY SERVICES

Other auxiliary services that are included in UCR 2013 are as follows:

- UC audio and video conferencing systems.
- Customer premises equipment.
- DoD secure communications devices.

SECTION 4
INFORMATION ASSURANCE

Information Assurance is a key aspect in the design of any Internet protocol (IP)-based network. Internet Protocol is inherently vulnerable to eavesdropping and a variety of denial of service (DoS) attacks. Voice and Video over IP (VVoIP) introduces avenues of attack because of its use of dynamically assigned User Datagram Protocol (UDP) sessions that cannot be addressed by traditional data firewalls. Therefore, VVoIP are applications that use IP for transport and inherit the threats associated with IP as well as adding vulnerabilities that are unique to the VVoIP technology. A tailored VVoIP information assurance design is necessary and is addressed in detail in Unified Capabilities Requirements (UCR) 2013 Section 4, Information Assurance DISA Field Security Office (FSO) Security Technical Implementation Guides (STIGs), and Security Requirements Guides (SRGs). With respect to the DoD UC architecture, the major components of the Information Assurance design include the protocols used, the interfaces of Session Controllers (SCs)/Enterprises SCs (ESCs) and Softswitch (SS) to external control devices, and the design of the Assured Services Local Area Network (LAN) (ASLAN). As an example, the methods for securing the VVoIP protocols are illustrated in Figure 4-1, Information Assurance Protocols. Key to the design is a hop-by-hop security model for trust between the signaling appliances using the Department of Defense (DoD) Public Key Infrastructure (PKI) for authentication. The diagrams illustrates an example of the UC distributed SC architecture however, the same protocols and concepts apply to the ESC architecture as well.

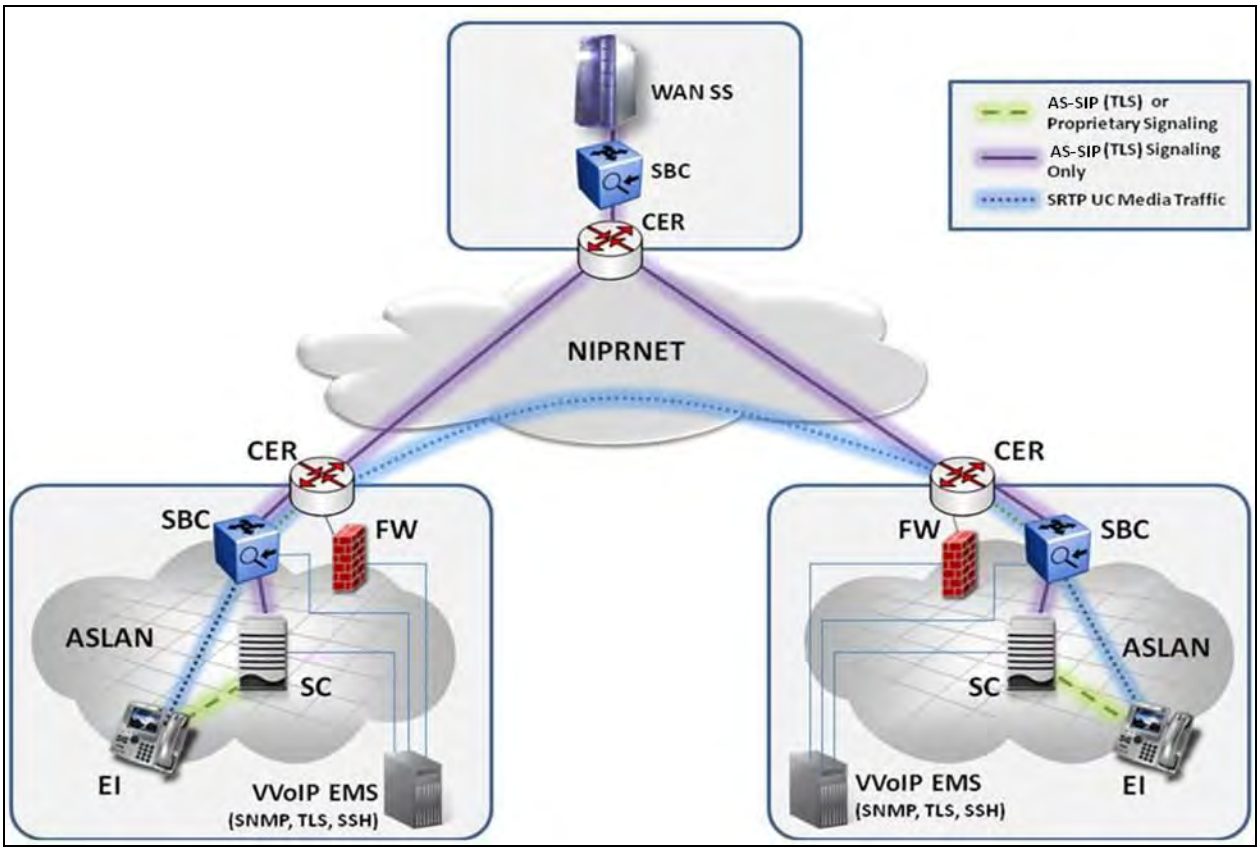

Figure 4-1. Example of Information Assurance Protocol Usage in the DoD UC Architecture

Figure 4-2, ASLAN Enclave Boundary Security Diagram, depicts a diagram of the Information Assurance design needed as part of the ASLAN. The key feature of Figure 4-2 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice and/or video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice and/or video dynamic stateful Assured Services (AS) Session Initiation Protocol (AS-SIP) aware application firewall, which provides Network Address Translation (NAT), SS failover, and port pinholes for individual voice and video sessions. A UC Approved Products List (APL) product called an SBC consisting of the voice and/or video firewall/border controller, has been defined and specified in UCR 2013, Section 7. In an Enterprise configuration, the site can be in a single Information Assurance accreditation boundary in which the SBCs shown in the diagram will be associated with the ARs and will not be within the Enclave Boundary shown on the diagram.

The requirements for the information assurance interoperability requirements are generally provided in UCR 2013, Section 4, Information Assurance. The result from testing against against these UCR requirements are adjudicated and placed in Interoperability (IO) Test Reports. The STIGs and SRGs provide the other basis for UC APL information assreance requirements and any findings against these requirements during testing are documented in IA Test Reports.

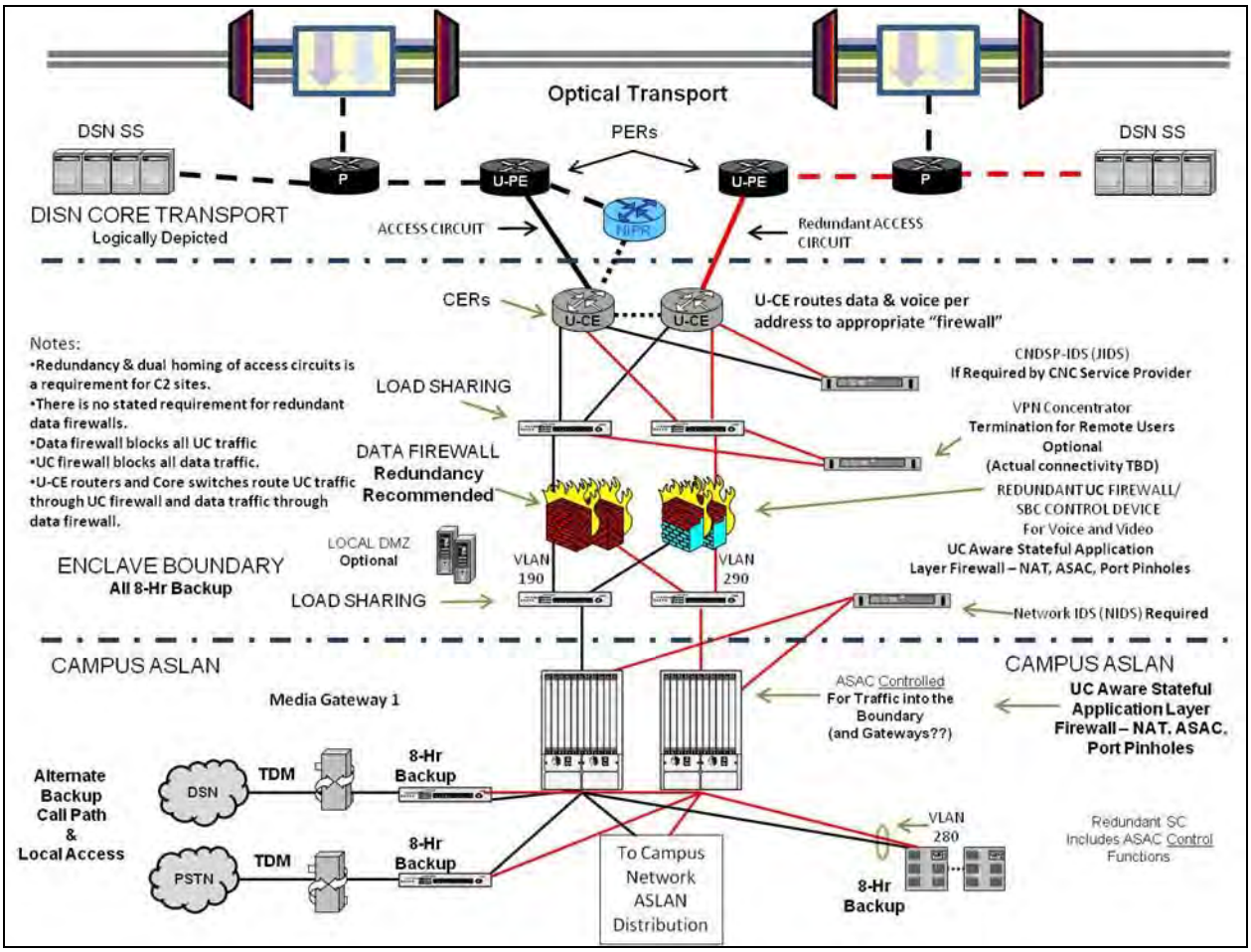

Figure 4-2. ASLAN Enclave Boundary Security Design

SECTION 5
IPV6

5.1 INTRODUCTION

The overarching guidance is that all Internet protocol (IP) interfaces have to be dual stacked and meet the IPv6 requirements. All features and functionality available on IPv4 networks will need to be supported on IPv6 networks as well. While there are requirements to manage IPv6 networks, the Network Management may be done using IPv4, at this time.

The Department of Defense (DoD) Information Technology (IT) Standards Registry (DISR) baseline is updated to ensure that DoD capabilities for building and buying products are based on a current and effective set of IT National Security Space (NSS) standards. DoD IPv6 Standard Profiles for IPv6-Capable Products, version 6.0, is approved for distribution via the DISR for IPv6 for DoD IT equipment and for providing a seamless integration of Unified Capabilities (UC) applications (e.g., voice, video, chat/presence, data).

The DoD has also published core IPv6 standards implementation guidance for Joint Capabilities Integration and Development System (JCIDS) Net-Ready Key Performance Parameter (NR-KPP) compliance in the IPv6 Global Information Grid (GIG) Technical Profiles.

The Defense Information Systems Agency (DISA) IPv6 Transition Office (DITO), in conjunction with the National Security Agency (NSA), has published the security requirements for all IPv6-capable devices, systems, services, and networks. The Milestone Objective 3 (MO3) outlines filtering, configuration, and transition related guidance for network nodes in the enclave boundary, demilitarized zone (DMZ), and interior networks. MO3 allows for the coexistence of IPv4 and IPv6, natively and in tunnels, to traverse inside and across the DoD network boundary. The MO3 describes security safeguards. It is imperative that products fielded in operational environments are configurable and support the outlined security mechanisms. These requirements are not only for Information Assurance devices, but also include configuration items for other non-Information Assurance devices that perform, implement, or manage a security-related function (e.g., host, router). At a future date, IPv6 Information Assurance guidance from MO3 will be incorporated into revisions of the appropriate Security Technical Implementation Guideline (STIG).

5.2 DEFINITIONS

These definitions are derived from DoD Deputy Chief Information Officer (CIO) Memorandum, DoD IPv6 Definitions:

1. IPv6-Capable Products. Products (whether developed by a commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. The IPv6-capable products shall be able to

interoperate with other IPv6-capable products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also do the following:

a. Conform to the requirements of the IPv6 profile in the Unified Capabilities Requirements (UCR).

b. Possess a migration path and/or letter of commitment to upgrade from the developer (signed by the company vice president or equivalent) as the IPv6 standard evolves.

c. Ensure that product developer IPv6 technical support is available.

d. Conform to NSA and/or Unified Cross Domain Management Office requirements for Information Assurance products.

2. System Under Test (SUT). The inclusive components required to test a UC product for Approved Products List (APL) certification. Examples of a System Under Test (SUT) include Voice over Internet Protocol (VoIP) system components (e.g., Session Controller [SC] and Gateway), Local Area Network (LAN) components (e.g., routers and Ethernet switches), and end instruments (EIs).

3. IPv6-Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6-capable network shall be ready to have IPv6 enabled for operational use when mission need or business case dictates. Specifically, an IPv6-capable network must do the following:

   a. Use IPv6-capable products.

   b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.

   c. Conform to DoD- and NSA-developed IPv6 network security implementation guidance.

   d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

4. IPv6-Enabled Network. An IP network that is supporting operational IPv6 traffic through the network, end-to-end.

Figure 5.2-1, IPv6 Design for SBU and Classified VVoIP, depicts the IPv6 network design for SBU and classified Voice and Video over IP (VVoIP), and includes the Defense Information Systems Network (DISN) Service Delivery Nodes (SDNs). All UC-approved products will be IPv6 capable, and the VVoIP network will be an IPv6-enabled network during Spiral 2 of its capabilities deployments.

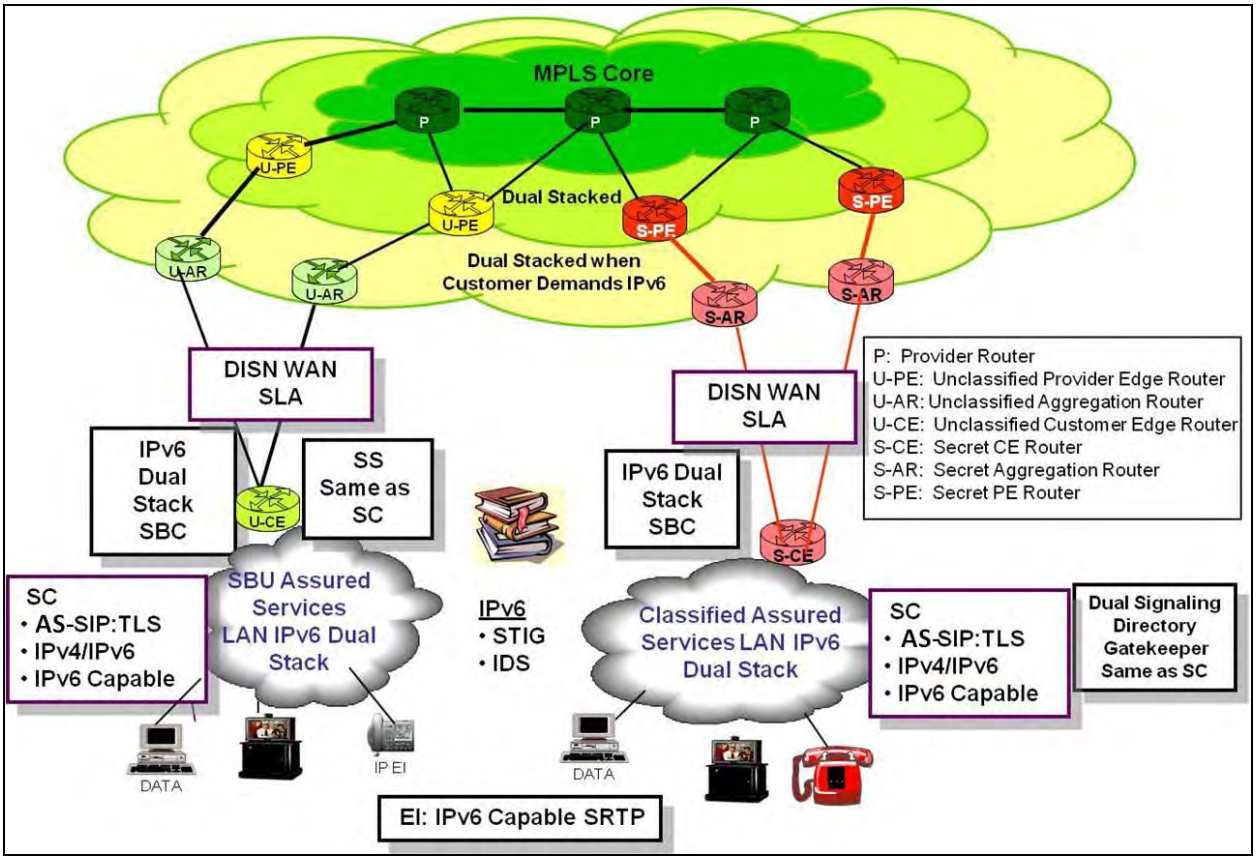

Figure 5.2-1. IPv6 Design for SBU and Classified VVoIP

5.3 DoD IPV6 PROFILE

DoD IPv6 Standard Profiles for IPv6 Capable Products, version 6.0, defines various LAN switches as follows:

1. Layer 2 Switch. A switch that forwards based on Layer 2 only (Media Access Control [MAC] address). Note that an unmanaged Layer 2 switch can be described as a "pure" Layer 2 switch; it operates at Layer 2 only and is transparent at the IP layer. As such, it has no IPv6-specific requirements and plays no active role as an IPv6-capable product. A Layer 2 switch may have some limited Layer 3 control plane functions but is primarily a data plane device. A managed Layer 2 switch product includes Simple Network Management Protocol (SNMP) management or other user access via an IPv6 interface, and it should be evaluated as a Simple Server.
2. Layer 3 Switch. A switch that incorporates Layer 3 information (IP addresses) into forwarding decisions. Forwarding may be manually configured, policy based, or based on routing protocols (Border Gateway Protocol [BGP], Routing Information Protocol [RIP], Open Shortest Path First version 3 [OSPFv3], or Intermediate System to Intermediate System [IS-IS]). Most Layer 3 switches require a router gateway to connect the LAN/Intranet to the

Internet. The most capable Layer 3 switches include a Wide Area Network (WAN) interface and an exterior routing protocol such as BGP.

3. Assured Services Switch. A switch that includes support for Quality of Service (QoS) features including the Differentiated Services Code Point (DSCP) queuing (Request for Comments [RFC] 2474). The DSCP queuing is an essential capability in the Unified Communications architecture to provide for Assured Services. Rather than being a separate product class, the requirements for Assured Services are specified as Conditional Requirements for compatibility with the UCR.

For the UCR, this third category of switch is called a LAN Access Switch, which is required to support RFC 2460/5095 and RFC 2464, and must be able to queue packets based on DSCPs in accordance with RFC 2474. If the application of the LAN Access Switch is a Layer 2 Switch, then it can be actively managed and supports queuing via DSCP, but not actually required to route. The complete set of RFCs for LAN switches is listed in UCR 2013, Section 5, Table 5.2-6, LAN Switch (LS). Part 1 is LAN Access Switch, Part 2 is LAN Distributed Switch, and Part 3 is LAN Core Switch.

5.3.1 Product Requirements

As mentioned in UCR 2013, Section 2, Session Control Products, the Unified Capabilities Requirements are the minimum set of requirements necessary for the system to be IPv6 capable for VVoIP.

As the evolution of IPv6 continues and industry-wide adoption of the same increases, the DoD community may consider other features and capabilities for IPv6 such as the following:

- Simple Mail Transfer Protocol (SMTP) IPv6 network management.
- Multicasting features to support IPv6 addressing and the service function of multicasting.
- Possible use of anycast addresses.
- Tactical, deployable, mobile IPv6.
- Ad hoc networks (such as Mobile Ad Hoc Network [MANET]).

Requirement for the use of such features will be defined in subsequent updates to the UCR 2013 based on the needs identified by the DoD community.

SECTION 6
NETWORK INFRASTRUCTURE END-TO-END PERFORMANCE

This section contains end-to-end (E2E) performance design guidelines for Unified Capabilities (UC) network infrastructures. The focus of this section is network-level design recommendations to attain optimal quality of service and service level objectives necessary for UC, while requirements for products used in the network infrastructure are defined in the Unified Capabilities Requirements (UCR) as follows:

1. The requirements for Local Area Network (LAN)/network edge products (i.e., LAN Core, Distribution, and Access switches; Customer Edge [CE] Routers [CE-Rs]) are provided in Section 7, Network Edge Infrastructure.
2. The requirements for the Network Infrastructure products (i.e., Defense Information Systems Network [DISN] Router, DISN Switch, and DISN Access Elements) are provided in Section 10, Network Infrastructure Products.
3. The Differentiated Services Code Point (DSCP) Plan, per-hop behavior (PHB), and traffic conditioning requirements for routers used in the UC network infrastructure are defined in UCR 2013, Section 6, Network Infrastructure End-to-End Performance.

6.1 NETWORK SEGMENTS AND MEASUREMENT POINTS

The E2E network infrastructure consists of three network segments: CE, Network Edge, and Core. These are illustrated in Figure 6.1-1, Measurement Points for Network Segments.

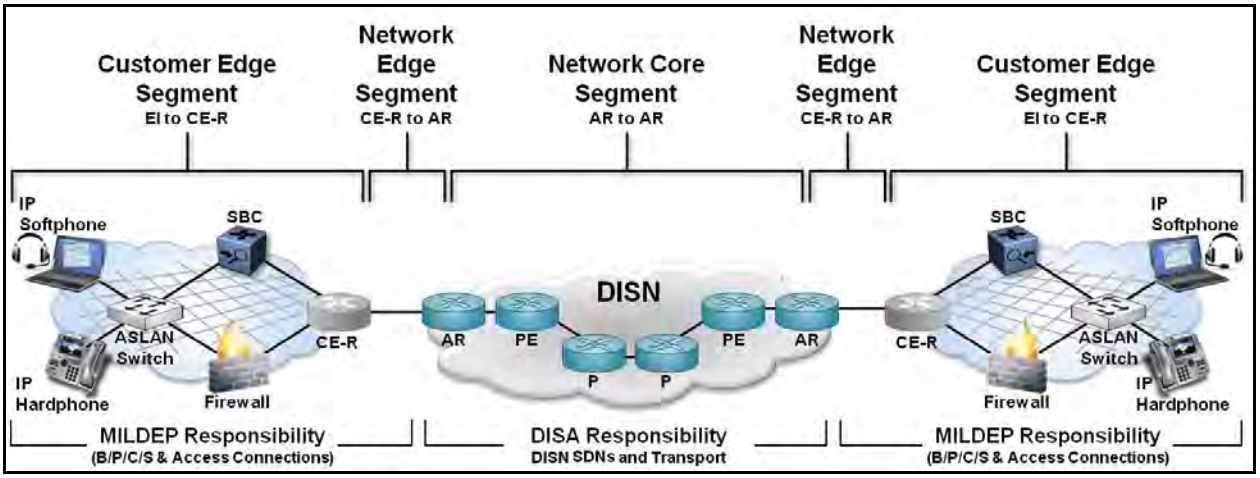

Figure 6.1-1. Measurement Points for Network Segments

This document does not intend to provide guidance on the many network deployment and implementation techniques, such as queuing strategies, traffic shaping, routing topology, or redundancy designs, that can be used freely by the network administrators to meet the required service objectives and their own internal needs. Its primary purpose is to provide a high-level design recommendation that, coupled with the performance metrics found in the UCR, can be

used to implement an optimal Internet protocol (IP)-based voice, video, and data architecture. These performance objectives are based on commercial best practices for latency, packet loss, jitter, and availability.

Figure 6.1-1, Measurement Points for Network Segments, illustrates the components of the E2E network where measurements should be made to ascertain compliance with the service level objectives.

For the purpose of this document, the DISN Service Delivery Nodes (SDNs) are assumed to be bandwidth rich and robust. In addition, since the Assured Services LANs (ASLANs) are required to be implemented as nonblocking network entities for voice and video traffic, it is assumed that there is no bandwidth limitation in those segments as well. The access circuit, which may include a satellite communications (SATCOM) link, is the only potential bandwidth bottleneck. Therefore, the network design includes the use of Assured Services Admission Control (ASAC) to prevent session overload and subsequent voice and video performance degradation egressing from the CE.

The DISN Core provides high availability (99.96 percent or greater) using dual-homed and multi-homed access circuits with Multiprotocol Label Switching (MPLS) Fast Failure Recovery (FFR).

6.2 UC ENGINEERING NETWORK CONSIDERATIONS

The primary performance driver for UC is voice. Voice quality is calculated E2E from handset to handset. For voice applications, the measurement model for the End Instrument (EI) is the E-Model as described in the Telecommunications Industry Association (TIA)/TSB-116 A, which is based on the International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation G.107. The E-Model uses an R-Factor rating, which correlates to the Mean Opinion Score (MOS) rating specified by ITU-T recommendation P.800. The detailed EI voice quality calculation recommendations are found in UCR 2013, Section 2.20, Accounting Management.

This section specifies network infrastructure-related performance recommendations and takes into account all elements of the network to ensure that handset-to-handset recommendations are achievable. The following assumptions were made in determining performance recommendations necessary to achieve acceptable service:

- IPv4 or IPv6.
- Wireline Fixed Network (A=0).
- G.711 codec with 20 ms samples (Ie=0).
- IPv4 Bearer packet size = 254 bytes, calculatd as the sum of the following:
  - Ethernet header – 22 bytes (Including optional VLAN Tag header)
  - IPv4 Packet header – 20 bytes

- UDP header – 8 bytes
- Real-Time Transport Protocol (RTP) header – 16 bytes (RFC 3550; section 5.1)
    - 2 bytes – Version, Padding, Extension, contributing source (CSRC) count, marker and payload type
    - 2 bytes – Sequence number
    - 4 bytes - Timestamp
    - 4 bytes - Synchronization source (SSRC) identifier
    - 4 bytes - Contributing source (CSRC) identifiers
- Secure Real-Time Transport Protocol (SRTP) authentication headers– 12 bytes (RFC 3711; section 3.1)
    - 4 bytes – Optional RTP Extension
    - 4 bytes – Optional Master Key Identifier (MKI)
    - 4 bytes – Recommended Authentication Tag
- G.711 - 160 bytes
    - 64000 bps (Bit Rate) * .020 seconds (Sampling Rate) = 1280 bits (160 bytes)
- Ethernet Frame Check Sequence – 4 bytes
- Ethernet Interframe Gap – 12 bytes

- IPv6 Bearer packet size = 274 bytes, Calculated as the sum of the following:
    - Ethernet header – 22 bytes (Including optional VLAN Tag header)
    - IPv6 Packet header – 40 bytes
    - UDP header – 8 bytes
    - Real-Time Transport Protocol (RTP) header – 16 bytes (RFC 3550; section 5.1)
        - 2 bytes – Version, Padding, Extension, contributing source (CSRC) count, marker and payload type
        - 2 bytes – Sequence number
        - 4 bytes - Timestamp
        - 4 bytes - Synchronization source (SSRC) identifier
        - 4 bytes - Contributing source (CSRC) identifiers
    - Secure Real-Time Transport Protocol (SRTP) authentication headers– 12 bytes (RFC 3711; section 3.1)
        - 4 bytes – Optional RTP Extension
        - 4 bytes – Optional Master Key Identifier (MKI)
        - 4 bytes – Recommended Authentication Tag

  - G.711 - 160 bytes
    - 64000 bps (Bit Rate) * .020 seconds (Sampling Rate) = 1280 bits (160 bytes)
  - Ethernet Frame Check Sequence – 4 bytes
  - Ethernet Interframe Gap – 12 bytes
- Weighted Terminal Coupling Loss (TCLw) = 52 dB (in accordance with [IAW] American National Standards Institute [ANSI]/ Telecommunications Industry Association [TIA]-810-B).
- Latency because of EI (voice to IP and IP to voice) is 50 ms:
  - Latency because of de-jitter buffer in an EI is 20 ms.
  - Includes Packet Loss Concealment delays.

6.2.1 Voice Codec Compression

The preferred codec used for E2E Fixed-to-Fixed (F-F) voice sessions is the G.711 Pulse-Code Modulation (PCM) (Uncompressed) with 20 ms samples. Other codecs are allowed, and a minimum list of codecs that must be supported by all EIs is found in Section 2, Session Control Products.

6.3 ASSURED UC LATENCY DESIGN CONSIDERATIONS

The one-way latency metric is reported as the arithmetic mean of several (specified) single measurements over a 5-minute period. Corrupt and lost packets are excluded from the calculation. The metric is reported to 1 ms accuracy, rounded up, with a minimum value of 1 ms.

6.3.1 Assured UC Router Serialization/Packet Switching Latency

UCR 2013, Section 6, Network Infrastructure End-to-End Performance, specifies that all routers must be capable of receiving, processing, and transmitting a voice packet within 2 ms or less in addition to the serialization delay for voice packets as measured from the input interface to output interface under congested conditions, to include all internal functions. For example, the serialization delay of a 100 Base-T interface is 0.017 ms, which would allow for voice latency from input to Ethernet output under congested conditions of 2.017 ms.

NOTE: Internal functions do not include Domain Name Service (DNS) lookups and other external actions or processes.

6.3.2 Assured UC End-To-End Latency

The E2E network infrastructure supporting UC must ensure that the one-way E2E latency (handset to handset) for F-F locations does not exceed 220 ms for UC sessions as averaged over any 5-minute period. Figure 6.3-1, F-F E2E Latency, illustrates the measurement points for calculating the F-F E2E latency.

NOTE 1: The 220 ms in this context is taken from the E-Model ITU-T G.107 Recommendation, that staes that a 220ms one-way delay is equal to a MOS of 4.0.

NOTE 2: The recommendation for 220 ms is due to the limits of talk over. This latency may not be feasible for all scenarios (i.e., Southwest Asia [SWA]), but the recommendation as stated is necessary to avoid talk over for the scenarios that are feasible.

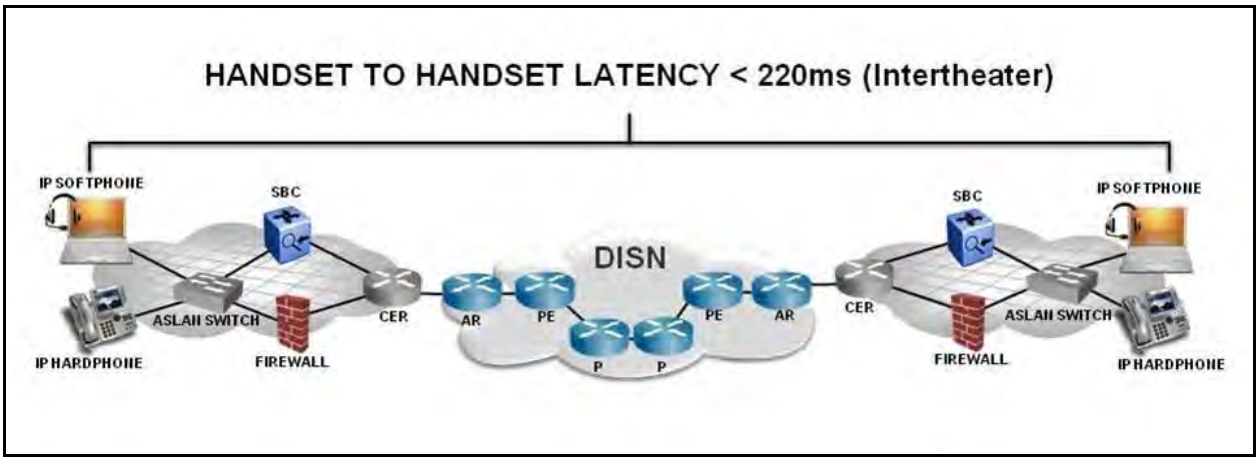

Figure 6.3-1. F-F E2E Latency

6.3.3 Assured UC CE Segment Latency

The CE Segment supporting UC must ensure that the one-way latency from the IP handset to the egress interface of the CE-R within the CE Segment is less than or equal to 35 ms (or less than or equal to 44 ms if the CE-R is collocated with an Aggregation Router [AR]) for UC sessions as averaged over any 5-minute period. Figure 6.3-2, CE Segment Outbound Latency, illustrates the delays associated with calculating the CE Segment outbound latency. The measurements must include the latency associated with the CE-R packet switching.

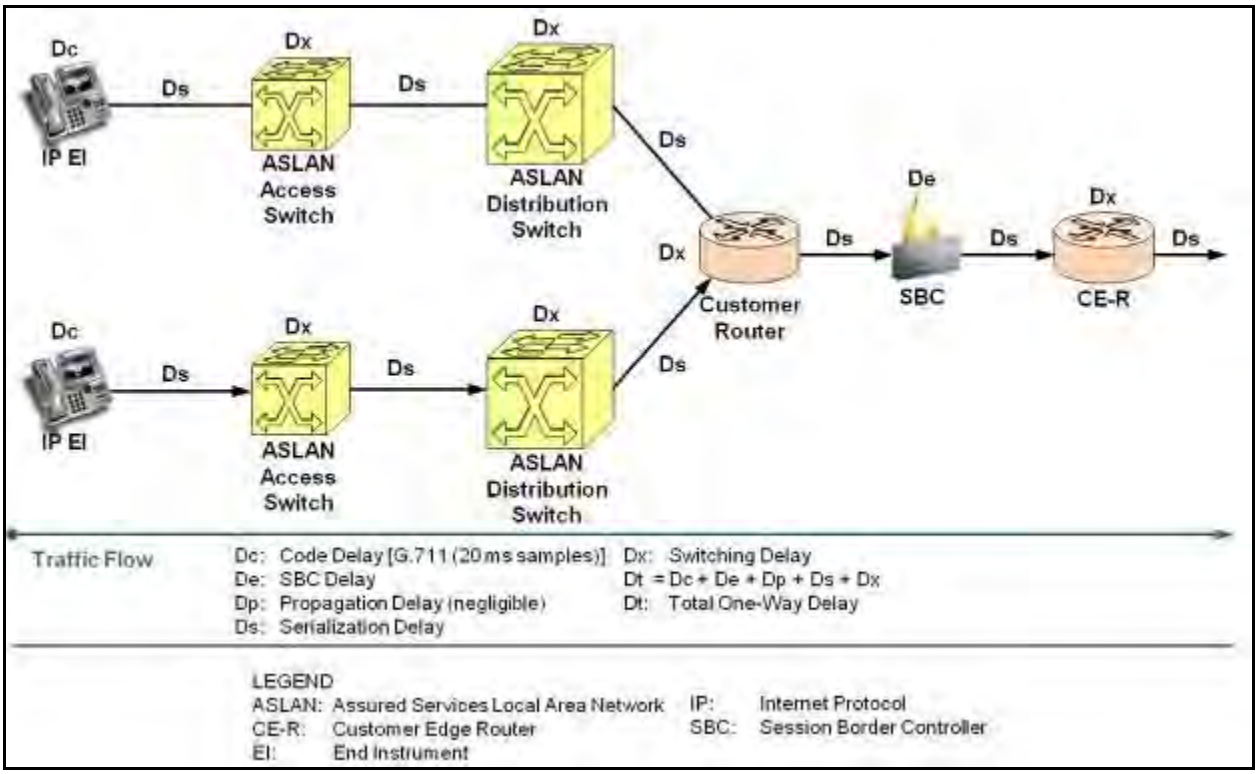

Figure 6.3-2. CE Segment Outbound Latency

The CE Segment supporting UC must ensure that the one-way latency from the ingress interface of the CE-R to the IP handset within the CE Segment is less than or equal to 35 ms (or less than or equal to 44 ms if the CE-R is collocated with an AR) for UC sessions as averaged over any 5-minute or period. Figure 6.3-3, CE Segment Inbound Latency, illustrates the delays associated with calculating the CE Segment inbound latency. The measurements must include the latency associated with the CE-R packet switching.

NOTE: This assumes that the latency associated with the de-jitter buffer is 20 ms.

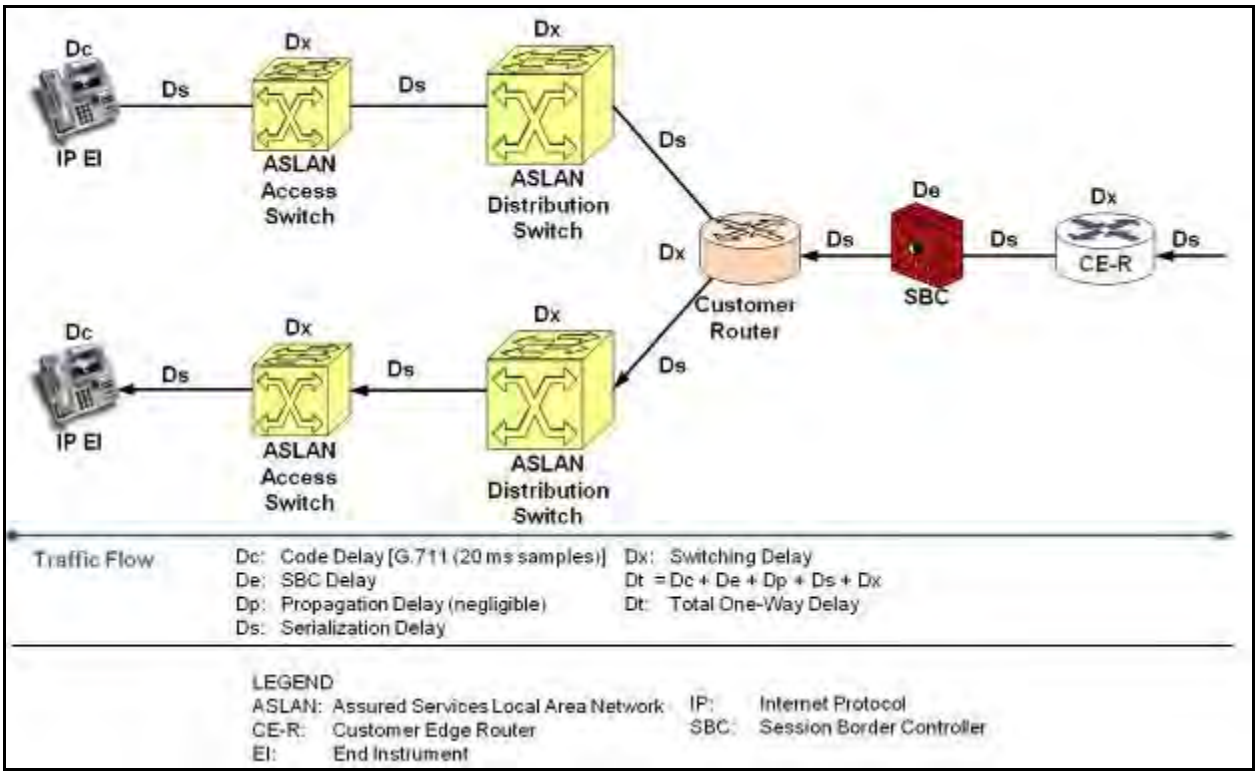

Figure 6.3-3. CE Segment Inbound Latency

6.3.4 Assured UC AR-to-AR Latency

The network infrastructure supporting UC must ensure that the one-way latency measured from the ingress interface of an AR to the egress interface of another AR across the DISN Wide Area Network (WAN) for F-F nodes does not exceed 130 ms latency for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces facing the CE-R to incorporate the packet switching delays through the network device. Figure 6.3-4, F-F AR-to-AR Latency, illustrates the measurement points for calculating the F-F AR-to-AR latency.

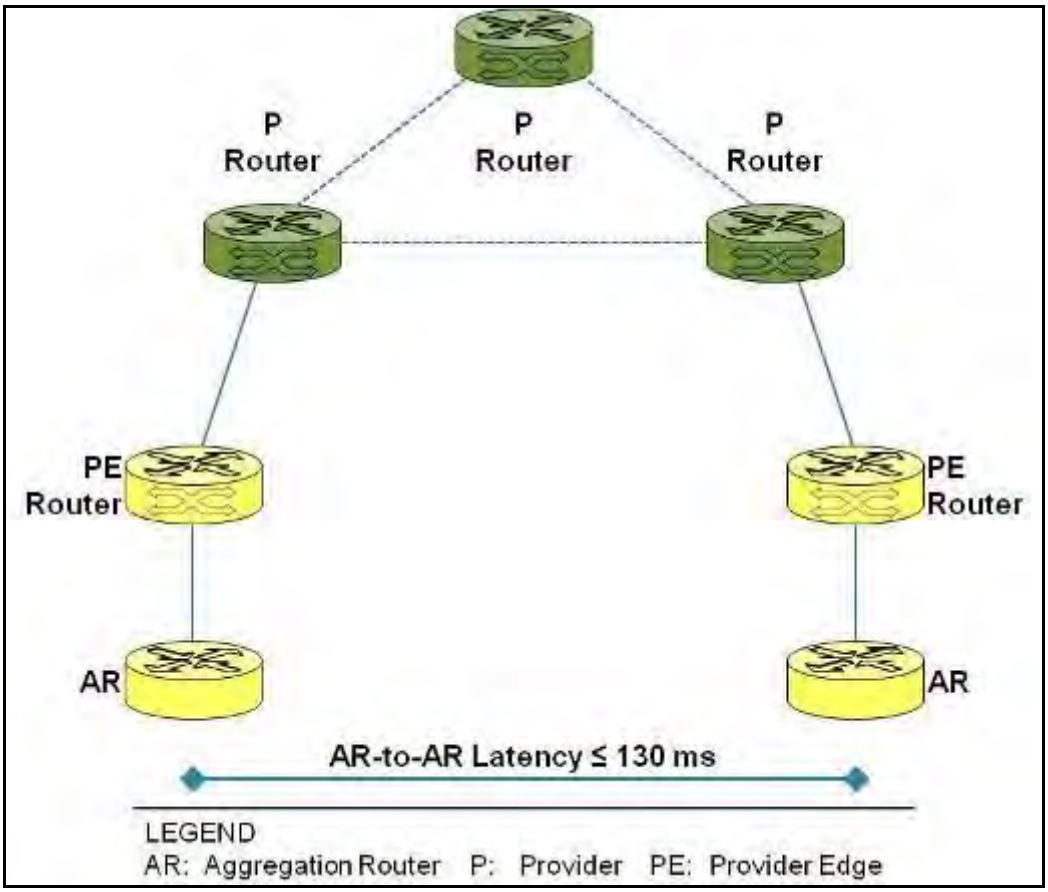

Figure 6.3-4. F-F AR-to-AR Latency

6.3.5 Assured UC CE Router-to-CE Router Latency

The DISN Network Infrastructure supporting UC must ensure that the one-way latency measured from the ingress interface of a CE-R to the egress interface of another CE-R across the DISN Network Infrastructure for F-F nodes does not exceed 150 ms (or 132 ms if the CE-R is collocated with an AR) for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces inclusive of the traffic flow through the CE-R to incorporate the packet switching delays through the network device. Figure 6.3-5, F-F CE Router-to-CE Router Latency, illustrates the measurement points for calculating the F-F CE Router-to-CE Router latency.

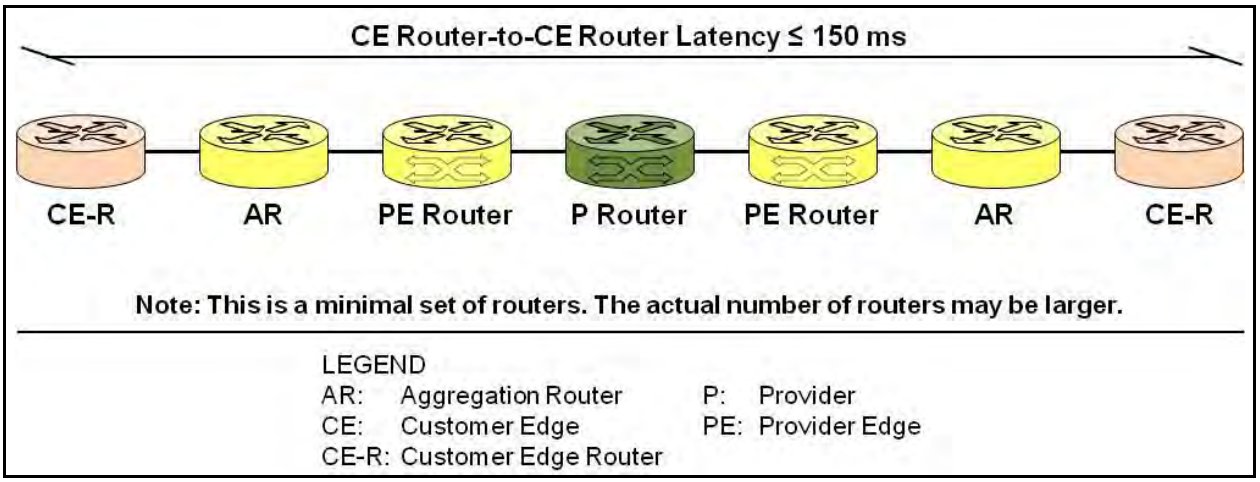

Figure 6.3-5. F-F CE Router-to-CE Router Latency

6.4 ASSURED UC JITTER

Jitter is defined in Appendix C, Definitions, Abbreviations and Acronyms, and References, and the term is used interchangeably with the term IP Packet Delay Variation (IPDV). The jitter numbers specified in this section are based on the minimum latency jitter model defined in ITU-T Recommendation Y.1540, November 2007. The one-way jitter is defined as the 99th percentile measurement of the distribution of singleton jitter (n) measurements over a 5-minute measurement interval.

6.4.1 Assured UC End-to-End Jitter

The E2E network infrastructure supporting UC must ensure that the E2E jitter (handset-to-handset) for F-F locations does not exceed 20 ms for UC sessions during any 5-minute period. Figure 6.4-1, E2E F-F Jitter, illustrates the measurement points for calculating the F-F E2E network jitter.

NOTE: Dynamic de-jitter buffers are allowed, but for these performance measurements are assumed to be 20 ms.

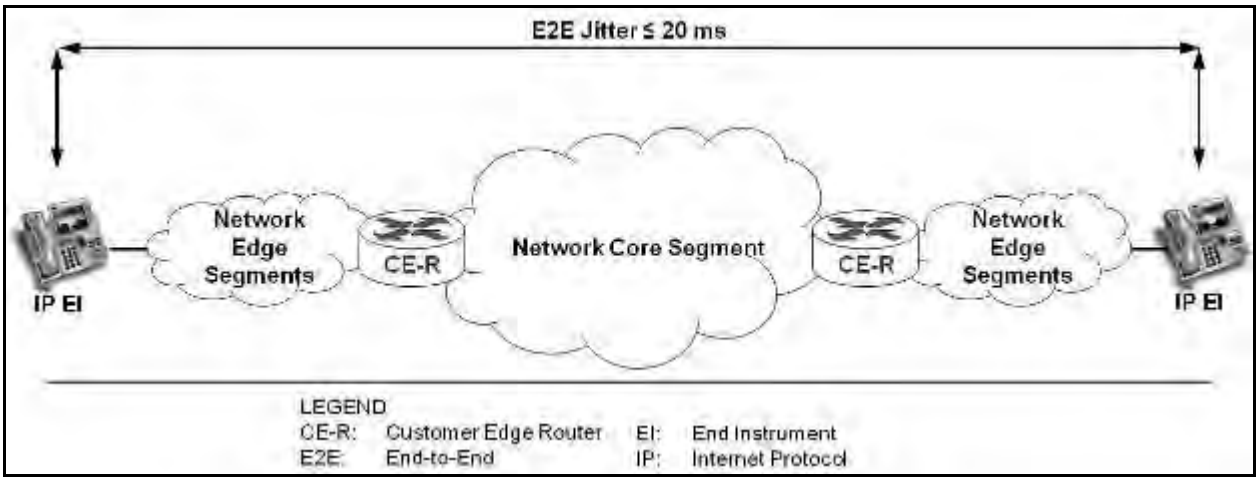

Figure 6.4-1. E2E F-F Jitter

6.4.2 Assured UC AR-to-AR Jitter

The network infrastructure supporting UC must ensure that the one-way jitter measured from the ingress interface of an AR to the egress interface of another AR across the DISN WAN for F-F nodes does not exceed 10 ms for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces facing the CE-R to incorporate packet jitter delays through the network device. Figure 6.4-2, F-F AR-to-AR Jitter, illustrates the measurement points for calculating the F-F AR-to-AR jitter.

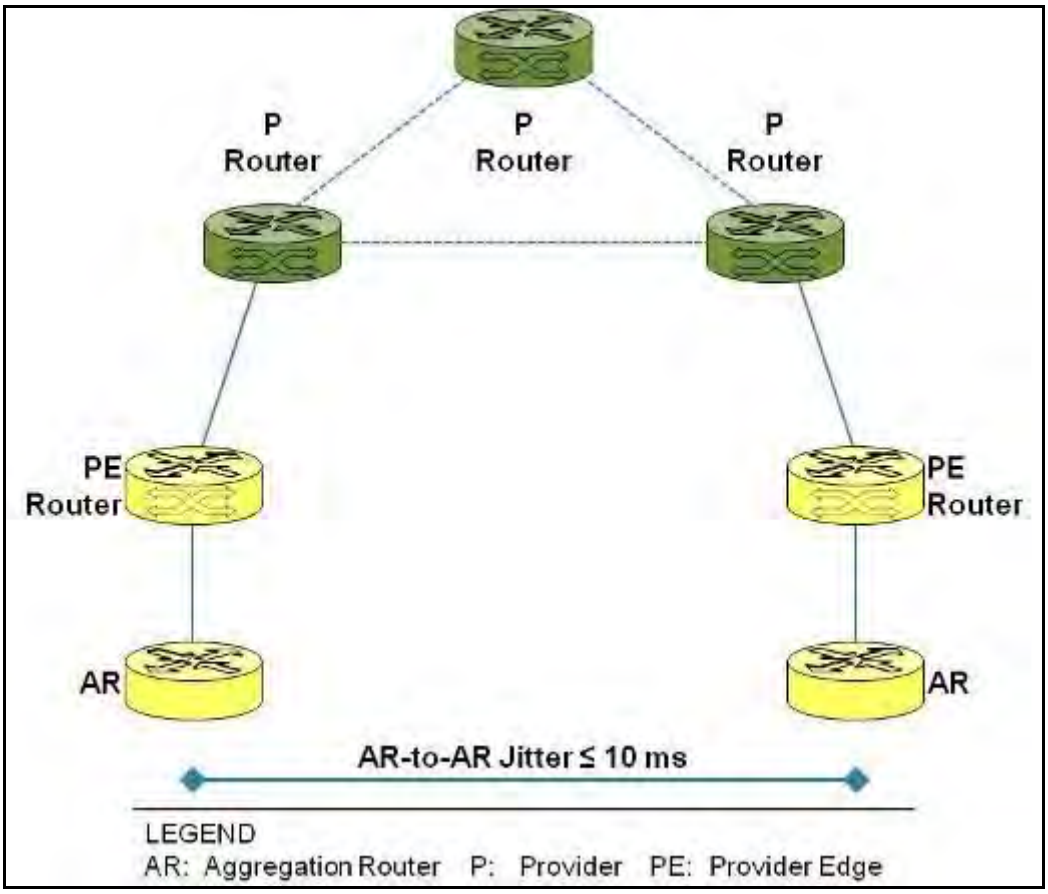

Figure 6.4-2. F-F AR-to-AR Jitter

6.4.3 Assured UC CE Router-to-CE Router Jitter

The DISN Network Infrastructure supporting UC must ensure that the one-way jitter measured from the ingress interface of a CE-R to the egress interface of another CE-R across the DISN Network Infrastructure for F-F nodes does not exceed 14 ms (or 10 ms if the CE-R is collocated with an AR) for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces inclusive of the traffic flow through the CE-R to incorporate packet jitter delays through the network device. Figure 6.4-3, F-F CE Router-to-CE Router Network Infrastructure Jitter, illustrates the measurement points for calculating the F-F CE Router-to-CE Router network infrastructure jitter.

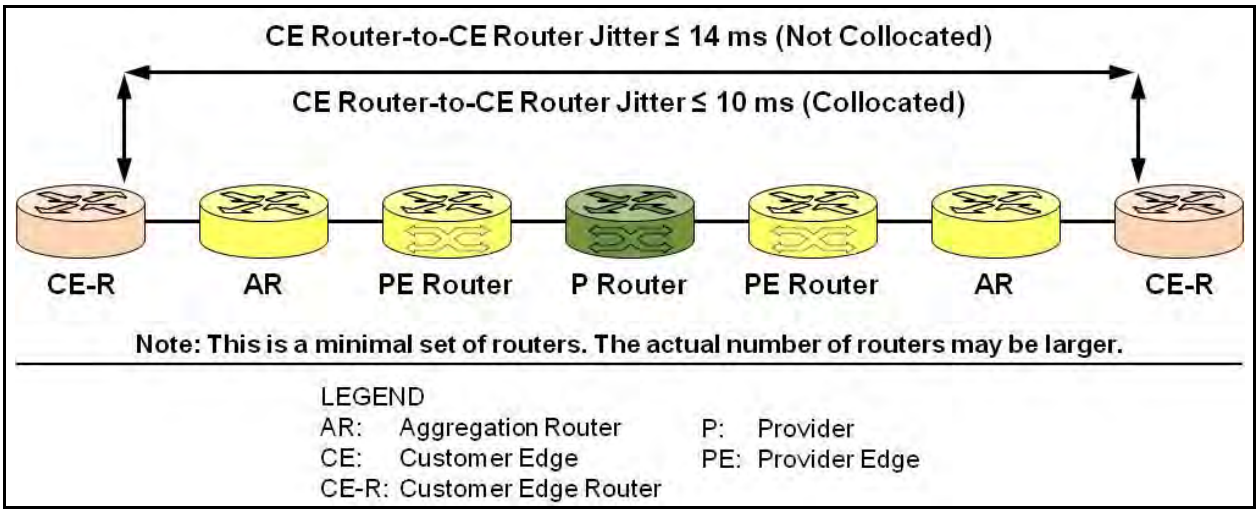

Figure 6.4-3. F-F CE Router-to-CE Router Network Infrastructure Jitter

6.4.4 Assured UC CE Segment Jitter

The CE Segment supporting UC must be configured not to exceed a one-way jitter of 3 ms (or 5 ms if the CE-R is collocated with an AR) measured between the handset and the egress interface of the CE-R for UC sessions during any 5-minute period.

6.5 ASSURED UC PACKET LOSS DESIGN CONSIDERATIONS

Packet loss is defined in Appendix C, Definitions, Abbreviations and Acronyms, and References, and the term is used interchangeably with the term IP Packet Loss Ratio (IPLR). A single instance of packet loss measurement is defined as a record of a packet sent by a sender reference point captured and compared at a destination reference point. The record is zero if the packet was received or one if the packet was not received. A packet is deemed to be lost if its one-way latency exceeds a time T_{max}, where T_{max} is equal to 3 seconds.

6.5.1 Assured UC End-To-End Packet Loss

The E2E network infrastructure supporting UC must ensure that the E2E one-way IP packet loss, as measured from handset to handset, for current F-F deployed locations does not exceed 1.0 percent for UC sessions averaged over any 5-minute period. Figure 6.5-1, E2E F-F Packet Loss, illustrates the measurement points for calculating the F-F E2E packet loss.

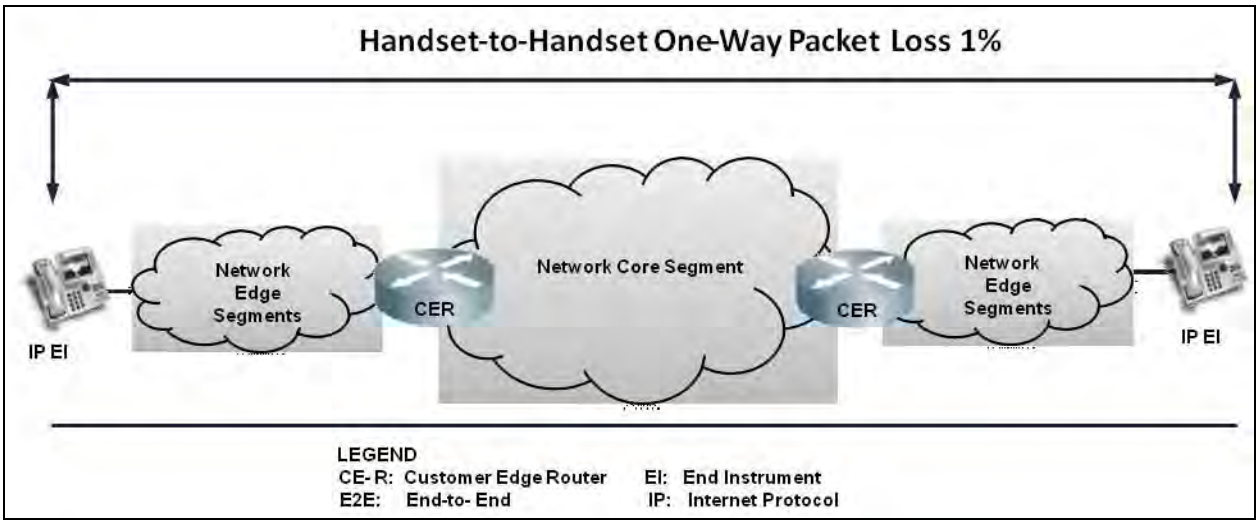

Figure 6.5-1. E2E F-F Packet Loss

On all new network deployments, the E2E network infrastructure supporting UC must be designed and engineered for a one-way E2E packet loss for F-F locations of 0 percent for UC sessions as averaged over any 5-minute period.

6.5.2 Assured UC AR-to-AR Packet Loss

The network infrastructure supporting UC must ensure that the one-way packet loss measured from the ingress interface of an AR to the egress interface of another AR across the DISN WAN for F-F nodes does not exceed 0.3 percent for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces facing the CE-R to incorporate packet loss through the network device. Figure 6.5-2, F-F AR-to-AR Packet Loss, illustrates the measurement points for calculating the F-F AR-to-AR packet loss.

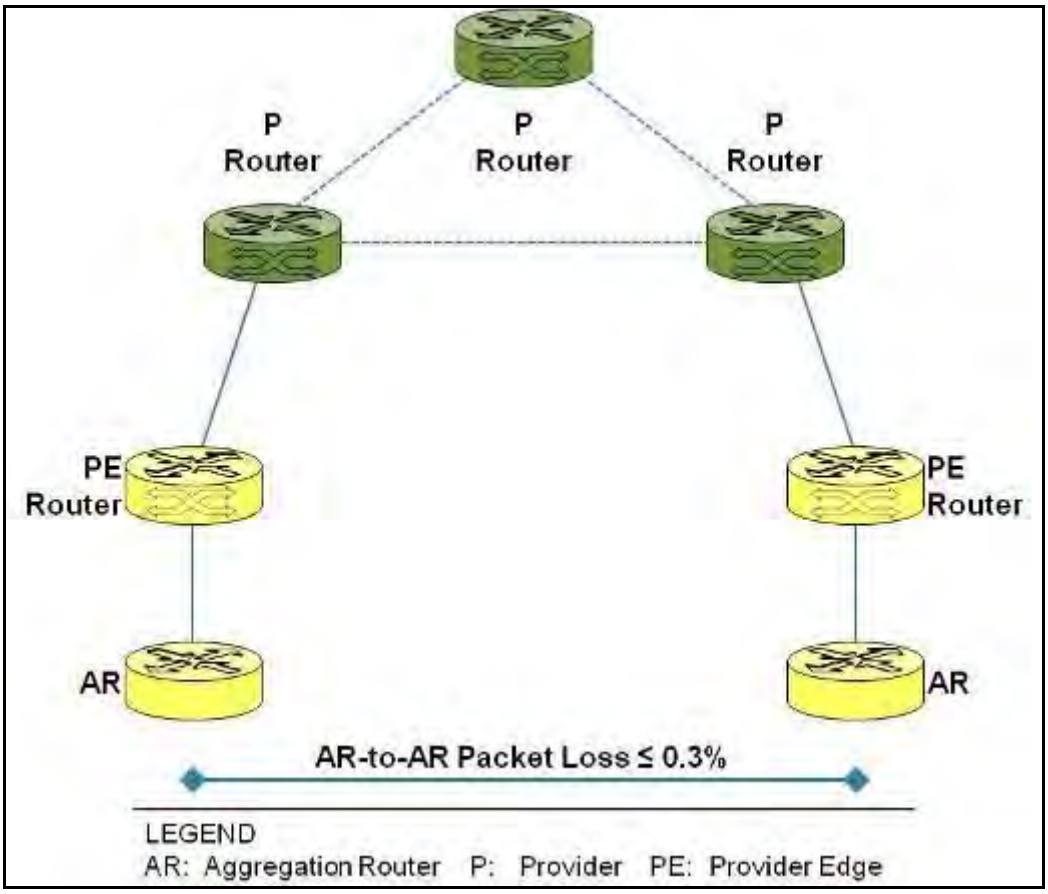

Figure 6.5-2. F-F AR-to-AR One Way Packet Loss

6.5.3 Assured UC CE Router-to-CE Router Packet Loss

The DISN Network Infrastructure supporting UC must ensure that one-way packet loss measured from the ingress interface of a CE-R to the egress interface of another CE-R across the DISN Network Infrastructure for F-F nodes does not exceed 0.8 percent (0.3 percent if the CE-R is collocated with an AR) for UC sessions averaged over any 5-minute period. The measurement must take place between interfaces inclusive of the traffic flow through the CE-R to incorporate packet loss through the network device.

Figure 6.5-3, F-F CE Router-to-CE Router Network Infrastructure Packet Loss, illustrates the measurement points for calculating the F-F CE Router-to-CE Router packet loss.

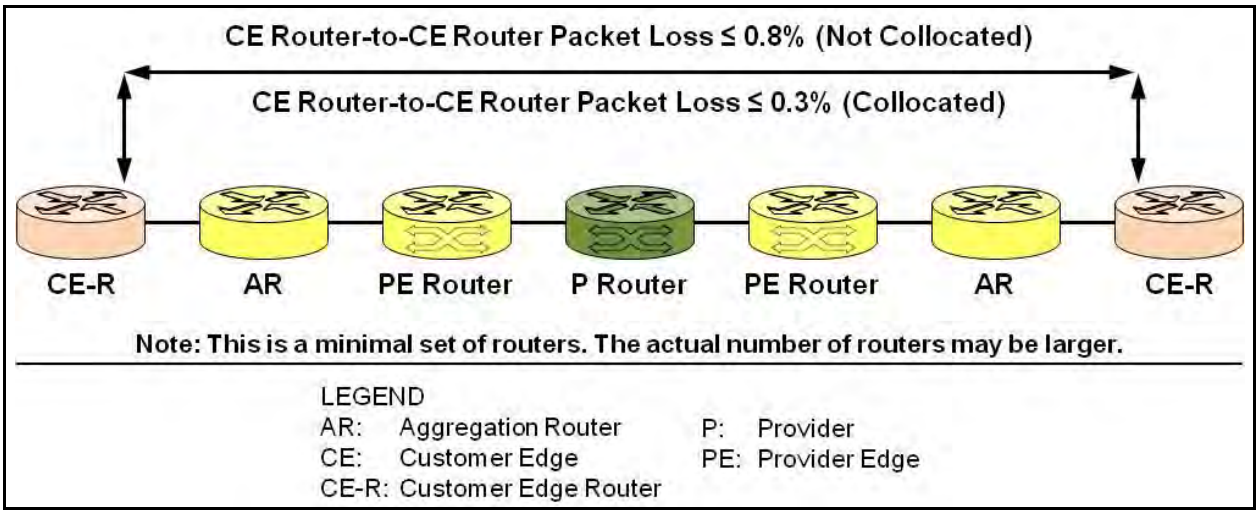

Figure 6.5-3. F-F CE Router-to-CE Router Network Infrastructure Packet Loss

NOTE: This assumes packet loss between a collocated CE-R and AR is 0.01 percent or less.

6.6 NON-ASSURED VOICE

The performance objectives for assured Voice and non-assured Voice are the same except with respect to E2E and AR-to-AR latency. Unlike assured Voice, non-assured Voice does not support Command and Control (C2) users and does not require as stringent performance objectives as assured Voice. As a result, non-assured VoIP is engineered for a MOS of 3.8, which is consistent with the performance of commercial wireless voice services. In accordance with the G.107 MOS model, a MOS of 3.8 can be achieved with a packet loss of 1 percent using the G.711 Codec when the latency is less than 250 ms. Therefore, E2E and AR-to-AR performance objectives for non-assured Voice latency are no longer the same E2E and AR-to-AR performance objectives for assured Voice latency. The performance objectives for non-assured VoIP are listed in Table 6.8-1, Granular Service Class Performance Objectives. Latency objectives for non-assured Voice are also illustrated in Figure 6.6-1, Latency Objectives for Non-Assured Voice.

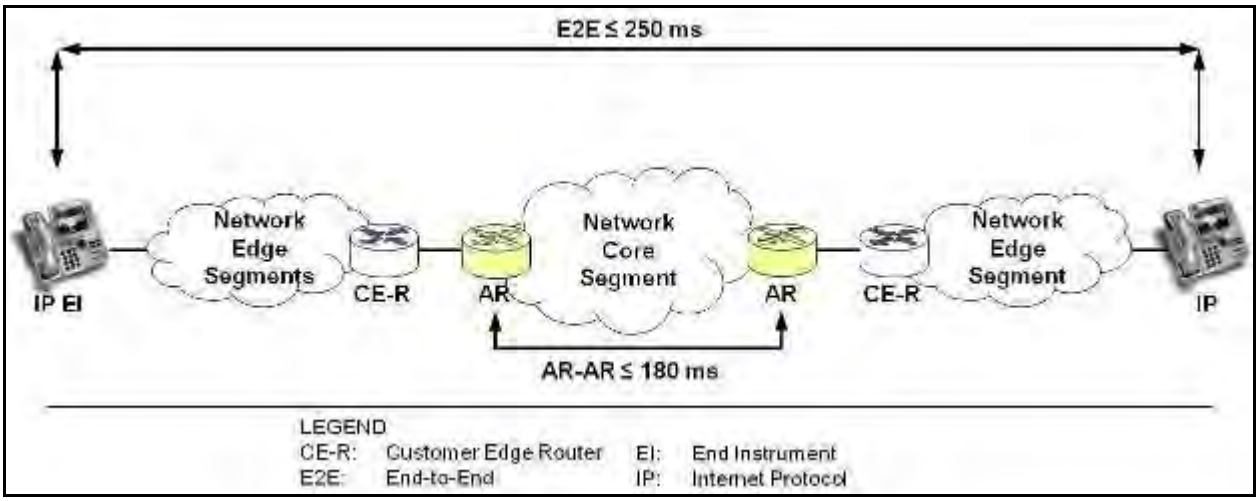

Figure 6.6-1. Latency Objectives for Non-Assured Voice

6.7 DATA APPLICATIONS

The performance of data applications will be measured at the same points as assured voice with the exception of E2E data performance, which will be measured from NIC to NIC (See Figure 6.7-1) instead of from IP Voice EI to IP Voice EI. The performance objectives for data applications are listed in Table 6.8-1, Summary of Granular Service Class Performance Objectives.

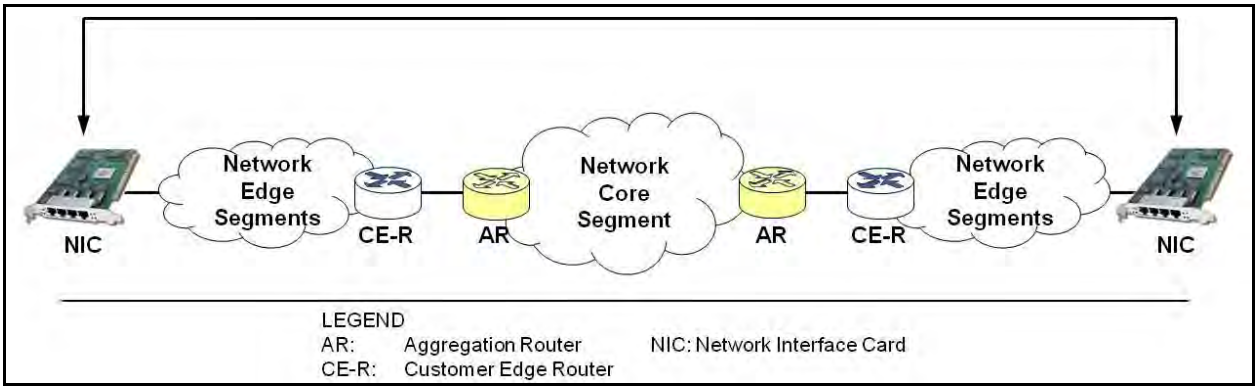

Figure 6.7-1. E2E Performance Measured from NIC to NIC

6.8 SERVICE LEVEL SPECIFICATION

Table 6.8-1 summarizes the Service Level Specification for each granular UC service class as defined in UCR 2013, Section 6, Network Infrastructure End-to-End Performance. This table defines one-way performance recommendations.

Table 6.8-1. Service Level Class Specification

GRANULAR SERVICE CLASS	E2E LATENCY (MS)	AR-AR LATENCY (MS)	EI-CE-R LATENCY (MS)	E2E PACKET LOSS (%)	AR-AR PACKET LOSS (%)	EI-CE-R PACKET LOSS (%)	E2E JITTER (MS)	AR-AR JITTER (MS)	EI-CE-R JITTER (MS)
Short Messaging	1000	900	50	0.5	0.4	0.05			
Assured Voice	220	150	35	1	0.8	0.05	20	14	3
Assured Multimedia Conferencing	220	150	35	1	0.8	0.05	20	14	3
Broadcast Video	1000	900	50	0.1	0.08	0.01			
Multimedia Streaming (includes Non-Assured Video)	250	180	35	1	0.8	0.05	20	14	3
Non-Assured Voice	250	180	35	1	0.8	0.05	20	14	3
Low Latency Data: IM/Chat, Presence	300	200	50	1	0.8	0.05			
High Throughput Data: Real-Time Data Backup, Web Hosting	300	200	50	1	0.8	0.05			
NOTE: Not All Aggregate Service Classes Have Performance Objectives (Best Effort, Signaling, Network Control, & Low Priority)									

6.9 SYSTEM-LEVEL QUALITY FACTORS

6.9.1 Handset-to-Handset Availability

The definition of availability, found in the Telcordia Technologies GR-512-CORE, Section 12, is the basis for the E2E UC network reliability. The following paragraphs outline the availability recommendations for the UC network.

1. Handset-to-Handset UC availability takes into account network resiliency and the availability of the devices that enable UC communications. The availability for the handset-to-handset network infrastructure between F-F locations serving UC users inclusive of scheduled maintenance must be as follows:
   a. ROUTINE (R) precedence of 99.55 percent or greater.
   b. IMMEDIATE/PRIORITY (I/P) precedence of 99.98 percent or greater.
   c. FLASH or FLASH OVERRIDE (F/FO) precedence of 99.98 percent or greater.

6.9.2 Network Segments Availability

1. The availability for the Network Core measured from AR to AR must be 99.999 percent or greater to include scheduled maintenance.
2. The availability for the network measured from CE-R to CE-R must be as follows:
   a. R precedence of 99.951 percent or greater.
   b. I/P, F, or F/O precedence of 99.987 percent or greater.
3. The availability for the CE Segment measured from EI to CE-R (ASLAN) must be as follows:
   a. R precedence of 99.8 percent or greater.
   b. I/P precedence of 99.997 percent or greater.
   c. F or F/O precedence of 99.999 percent or greater.
4. The availability for the UC CE Segment measured from EI to CE-R (to include ASLAN, Session Border Controller [SBC], Session Controller [SC], and CE-R) must be as follows:
   a. R precedence of 99.79 percent or greater.
   b. I/P precedence of 99.99 percent or greater.
   c. F or F/O precedence of 99.99 percent or greater.

   NOTE: Availability calculations are based on best practices because there appears to be no standardized model for calculating IP network availability.

Figure 6.9-1, F-F Network Infrastructure Availability, illustrates the measurement points for calculating the F-F network availability.

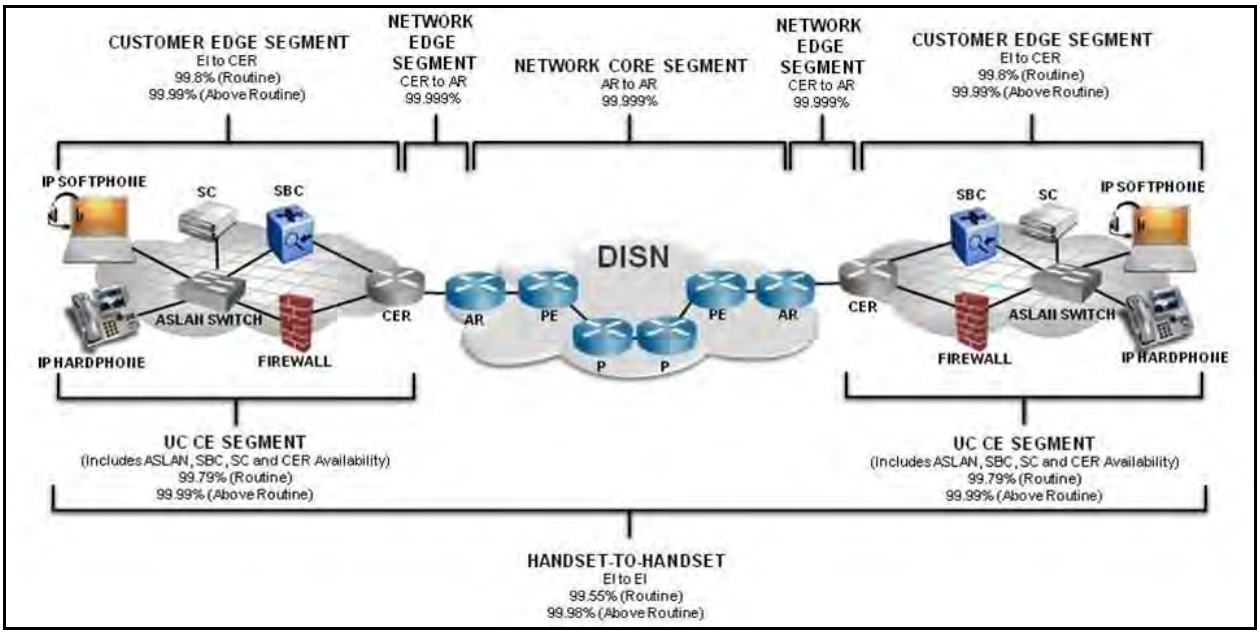

Figure 6.9-1. F-F Network Infrastructure Availability

6.9.3 Availability Design Considerations

1. The E2E network infrastructure supporting UC users with precedence above ROUTINE must have no single point of failure to include power sources and Network Management (NM).
2. If the network infrastructure supports users with precedence above ROUTINE, then the network infrastructure routers must provide five nines of availability (99.999 percent) to include scheduled maintenance.

   NOTE: Network infrastructure router availability recommendations may be met using dual homing and other routing techniques.

3. The National Military Command Center (and Alternate), Combatant Commands (COCOMs), or Component headquarters must not be isolated longer than 30 minutes because of an outage in the Core Segment of the network.
4. In the event of an E2E network infrastructure component failure in a network supporting UC users with precedence above ROUTINE, all sessions that are active must not be disrupted (i.e., loss of existing connection requiring redialing) and a path through the network must be restored within 5 seconds.
5. If the Edge Segment is dual-homed or multi-homed, then the UC traffic must be engineered to only use one access connection at a time to prevent asymmetric routing.

   NOTE: Data traffic should be engineered to use the alternate connection and serve as the UC traffic redundant link.

6. No segment of the E2E network infrastructure must use the same cost metric on dual-homed or multi-homed configurations forcing the same UC routing stream to be split into two distinct interfaces.

   NOTE: Cost metric redundancy routing is a technique used to provide survivability by sending packets associated with a session across multiple paths through the network infrastructure. This technique often introduces unacceptable and hard to troubleshoot latency and jitter on real time services and applications.

7. All network infrastructure products supporting UC users with precedence above ROUTINE must have 8 hours of backup power.

   NOTE: This recommendation does not address ASLAN backup power recommendations, which are addressed in Section 7, Network Edge Infrastructure.

8. If the Edge Segment supports users with precedence above ROUTINE, then the Edge Segment must be multi-homed, this means two separate access connections provisioned on physically diverse paths via two different ARs to two different service providers. Multi-homing is physically and logically diverse in accordance with the DISN subscription rates.
9. If the Edge Segment is dual-homed or multi-homed, and supports users with precedence above ROUTINE, then each connection must be traffic engineered to support 100 percent, which includes the 25 percent surge recommendation of the UC traffic load.
10. If the Edge Segment supports users with precedence above ROUTINE and the CE-R is collocated with an SDN containing a robust MSPP, then a separate access connection to another robust SDN must be used for redundancy.

6.9.4 Reliability and Failover Considerations

1. End-to-end network infrastructure products supporting UC users with precedence above ROUTINE must support a protocol that allows for dynamic rerouting of IP packets to eliminate any single points of failure in the network.
2. All network infrastructure products supporting UC users with precedence above ROUTINE used to meet the reliability recommendations must be capable of handling the entire session processing load in the event that its counterpart product fails.
3. All network infrastructure products supporting UC that implement MPLS must support a Fast Reroute (FRR) capability that restores routing paths following a local failure (i.e., a failure involving a single router or circuit) within 50 ms.
4. Network infrastructure routers must only enact switchovers based on a reduction in access network throughput or bandwidth with Network Management (NM) troubleshooting procedures, because the routers cannot determine where or what in the access IP connection is the cause of the reduction.

5. If the Edge Segment has at least two separate access connections and the CE-R detects an access connection failure, the CE-R must be configured to dynamically switch to the alternate or backup access connection.

   NOTE: A failure may be detected via a physical link alarm (level 2), or via a loss of a dynamic routing protocol HELLO status message (level 3).

6. If the CE-R has at least two separate access connections (i.e., dual-homed or multi-homed) and detects an access connection failure, the CE-R must switch to the alternate or backup access connection using an automatic process and must not require operator actions.

   NOTE: When the switchover occurs, UC sessions in progress may be lost, and new sessions may not be able to be established until the IP routing updates have taken place. This may take 10 seconds or more and is dependent on the routing protocol standard update interval.

7. If the Edge Segment has at least two access connections to provide redundancy, then the network administrators must implement a standard operating Procedure for switching UC traffic between access connections at least on a weekly basis to verify that the alternate circuit or path is working properly.

6.10 BANDWIDTH PROVISIONING CONSIDERATIONS

The recommended bandwidth per supported voice session on the Ethernet network infrastructure is 220 kbps (110 kbps each direction). This is based on the worst-case scenario assumption that uses a 274 bytes voice bearer packet as defined in Section 6.2.

In addition, the E2E network infrastructure supporting UC must assume the use of G.711 (20 ms) for calculating bandwidth budgets within F-F networks even if compressed codecs are used. For example, if G.729 is used for an F-D UC session, then the budget for the fixed portion of the network should allocate 110 kbps to that session even though the session uses less bandwidth.

1. Access connections supporting UC must be engineered to support one WAN (trunk) voice session (110 kbps of IP bandwidth in each direction) for every four EIs within the Edge Segment

   (NOTE: The 4:1 ratio does not include surge); or must be traffic engineered IAW the following approach:

   a. Determine the busy hour traffic load in Erlangs from current traffic pattern, matrix, or call volume using the following formula and use the Erlang B table to determine the number of connections/size of connection required to support the traffic load.

      Busy Hour Offered Load = Total Call Time for the Busy Hour in Seconds/10 (averaged over the 10 busiest hours of the year)

      Busy Hour Erlang = Busy Hour Offered Load in Seconds/3600

b. Calculate the Access Connection bandwidth recommendation based on the following assumptions:

Call Arrival Distribution	=	Poisson
Codec Type	=	G.711 (coding rate: 64000 bits/sec)
Frame Size	=	20 ms interval time (0.020 sec)
Samples/Packet	=	160 samples per packet
Frames/Packet	=	1
Frames/Second	=	50
Frame Size/Packet	=	160 bytes
Ethernet Interframe Gap	=	12 bytes
SRTP Authentication Tag	=	4 bytes
Frames/Erlang	=	50
Packets/Second/Erlang	=	50
Packet Size (for Ethernet)	=	274 bytes (assumes IPv6)
Access Bandwidth Formula	=	Busy Hour Erlang B * Packet Size * Packets/Second/Erlang B* 8 bits/byte

For example, if the Busy Hour Erlang B equals 25, then the access bandwidth should be 25*274*50*8 = 2,740,000 bits per second (bps) or 2.74 Mbps.

2. A Base/Post/Camp/Station (B/P/C/S) must not reduce the number of simultaneous Access Connection (trunk) subscriptions to the DISN when they migrate from Time Division Multiplexing (TDM) to IP unless traffic engineering is completed IAW the preceding recommendation.

   NOTE: For instance, if the existing B/P/C/S subscribed for 100 simultaneous DS0s to the DISN with their TDM infrastructure, but the engineered IP solution only requires 90 multiplied by 110 kbps of bandwidth, then the B/P/C/S design must support 100 multiplied by 110 kbps of bandwidth to meet this recommendation.

3. The E2E network infrastructure design must provide, at a minimum, a 25 percent increase in network capacity (i.e., throughput and number of sessions) above the current employed network capacity at all tandem switches, Multifunction Switches (MFSs), Softswitches (SSs), and critical dual-homed End Office (EO) switches and SCs.

4. The long-haul portion of the network infrastructure must be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.

5. All F-F network infrastructure network connections supporting UC must have at a minimum, T1 bandwidth of 1.544 Mbps or greater.

6. All CE-R and/or AR interfaces in the direction of the CE-R support bandwidth metering and provisioning in accordance with the Four and Six Queue Bandwidth Provisioning Models as defined in Tables 6.10-1 and 6.10-2.

   NOTE 1: The Provisioning Model described below depicts how the AR routers are configured in the DISN. It is optional, but highly recommended, for MILDEPs to follow this bandwidth provisioning approach when provisioning network queues in support of UC services.

   NOTE 2: Given the sensitivity and bandwidth constraints found in strategic and tactical environments, these types of B/P/C/S have the option to define their own provisioning model based on bandwidth availability and mission/operational recommendation needs.

Table 6.10-1. DISN Four-Queue Bandwidth Provisioning Model

AGGREGATE SERVICE CLASS	BANDWIDTH PROVISIONING
Network Control/Assured Real Time	25% Minimum Bandwidth
Assured Real-Time Video	15% Minimum Bandwidth
Preferred Elastic	40% Minimum Bandwidth
Best Effort	20% Minimum Bandwidth

Table 6.10-2. DISN Six-Queue Bandwidth Provisioning Model

AGGREGATE SERVICE CLASS	BANDWIDTH PROVISIONING
Network Control	5% Minimum Bandwidth
Assured Real Time	20% Minimum Bandwidth
Non-Assured Real Time	15% Minimum Bandwidth
Preferred Elastic	30% Minimum Bandwidth
Elastic	20% Minimum Bandwidth
Scavenger	10% Minimum Bandwidth

6.11 VOICE GRADE OF SERVICE

The Grade of Service (GOS) is defined in Appendix C, Definitions, Abbreviations and Acronyms, and References. In addition, the voice and video (UC only) GOS are calculated independently since the budgets associated with each are independent

1. The E2E network infrastructure must provide a GOS of P.00 (i.e., 0 sessions out of 100 will be “blocked” during the “busy hour”) for FLASH and FLASH OVERRIDE voice and video (UC only) sessions. This is also referred to as nonblocking service.
2. The E2E network infrastructure must provide a GOS of P.02 (i.e., 2 sessions out of 100 will be blocked during the busy hour) and P.01, respectively, during a 100 percent increase above

normal precedence usage for PRIORITY and IMMEDIATE voice and video (UC only) sessions at a minimum.

3. The E2E network infrastructure supporting UC must provide a peacetime theater GOS of P.07 (i.e., 7 voice sessions out of 100 will be blocked during the busy hour) or better, and an intertheater GOS of P.09 or better, as measured during normal business hours of the theaters for ROUTINE precedence voice and video (UC only) sessions traversing the network from an EO or SC EI and/or AS-SIP EI.
4. The CE Segment supporting UC must provide a GOS between the EO and any PBX users or between an SC and its subtended SC that do not exceed an additional blockage of P.02 for voice or video (UC video only) sessions.

6.12 TRAFFIC CONDITIONING CONSIDERATIONS

6.12.1 Queuing Trust Considerations

A trust boundary is the point within the network where DSCP markings begin to be accepted and packets are not dropped or overridden. The design objective is to enforce DSCP markings in accordance to the UCR as close to the endpoints as technically and administratively possible.

In order to achieve this objective, MILDEPs should adhere to the DSCP Plan as outlined in the UCR and described in section 6 of the UCR. MILDEP ASLAN infrastructure equipment should be configured to trust all UCR DSCP markings through every segment, or hop, of the network and must never attempt to markdown, reprioritize or drop UC DSCP markings. MILDEP ASLANs should not adopt COTS or vendor based QoS approaches, as these do not meet DoD requirements and guidance.

6.12.2 Queuing Policing, Scheduling & Markdown Considerations

DISA GNSC enforces Committed Information Rates (CIR) for DISA WAN aggregation routers. MILDEPs should configure their devices and adhere to the GNSC CIRs and must take into account how the GNSC handles any surges above the CIR, when capacity is available.

The UCR recommends industry best practices when implementing congestion avoidance mechanisms. Any rate limiting, markdown or drop policy should support Expedited Forwarding (EF) with a strict priority above all other traffic classes for all inelastic real-time queues. It should also support Assured Forwarding (AF) with a Class-Based Weighted Fair Queuing (CBWFQ) approach. This provides for a certain level of delivery guarantee as long as the traffic does not exceed the CIR. Traffic that exceeds the CIR should face a higher probability of being rate limited or dropped if congestion occurs based on the priority and precendence of the traffic within that specific traffic queue. When coupled with Random Early Detection Queuing (RED), CBWFQ can do the following:

1. Allow for lower level traffic flow fairness and prevents lower precedence queue bandwidth starvation by allowing for queue bandwidth reservation on converged networks
2. Lower precedence markings are only serviced when upper markings have been serviced
3. Aim to control the average queue size by indicating to the end hosts when they should slow down transmission of packets
4. Take advantage of the congestion control mechanism of TCP by randomly dropping packets
5. When the device begins to sense periods of high congestion, the source starts to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared
6. Cause TCP to slow down transmission of packets. TCP not only pauses, but it also restarts quickly and adapts its transmission rate to the rate that the network can support
7. Distribute losses in time and maintains normal low queue depth while absorbing spikes
8. Drop packets when congestion occurs at a rate selected during configuration, when enabled on an interface.

UCR DSCP markings should never be remarked to a lower priority marking within the strategic network and on tactical networks, packets may be remarked as long as the appropriate markings are restored prior to entering the strategic network. All traffic should be configured in accordance with the Traffic Conditioning Specification (TCS) specified in the UCR Section 6.3.2.

6.13 UC NETWORK INFRASTRUCTURE SURVIVABILITY

The following recommendations contribute to the survivability of the UC system:

No more than 15 percent of the B/P/C/Ss must be affected by any outage in the network. This includes issues such as overtaxing of processing capacity, link failure, and redundancy failover glitches.

6.14 VOICE SERVICE QUALITY

1. Because intelligibility of voice communications is critical to C2, the voice service quality rating, on at least 95 percent of the voice sessions, will have an MOS IAW the following scenarios:
   a. Fixed to Fixed Assured Voice – 4.0.
   b. Fixed to Fixed Non-Assured Voice – 3.8.
   c. Fixed to Deployable Assured Voice – 3.6.
   d. Deployable to Deployable Assured Voice – 3.2.

2. The method used for obtaining the MOS must be IAW the DoD Information Technology Standards Registry (DISR), which currently aligns with the use of the E-Model and TSB-116-A (03/2006) for F-F scenarios, and P.862 (02/2001) for Deployable scenarios.

SECTION 7
NETWORK EDGE INFRASTRUCTURE

7.1 CE SEGMENT ATTRIBUTES

The Customer Edge (CE) Segment may consist of a single Local Area Network (LAN) or a Campus Area Network (CAN), or it may be implemented as a Metropolitan Area Network (MAN) in certain locations. The boundary for the CE Segment is the CE Router (CE-R At Base/Post/Camp/Stations (B/P/C/S) that Support a Combatant Command (COCOM), all UC traffic associated with the COCOM will be routed through a COCOM-owned Tier 1 CE-R, directly to Defense Information systems Agency (DISA) Service Delivery Node (SDN) Provider Edge (PE) Tier 0 Routers. Other traffic on the B/P/C/S will be routed through the CE router owned by the B/P/C/S. The Customer Edge Segment is connected to the Network Core Segment by the Network Edge Segment, which is a traffic-engineered bandwidth (IP connection) that connects the CE-R to an SDN.

The CE Segment has the following attributes:

- LANs Configured to Meet Mission, Performance, and Affordability. At the CE, the design has a LAN that is designed with a mix of Assured Services and non-Assured Services LANs (ASLAN) based on availability, redundancy, and backup power tailored for an organization's missions and affordability. Performance requirements with respect to quality of service (QoS), security, and network management are the same for ASLANs and non ASLANs.
- Session Admission Control. The Session Controllers (SCs) use an Assured Services Admission Control (ASAC) technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit consistent with maintaining voice quality, so that on at least 95 percent of the voice sessions, the quality rating expressed as Mean Opinion Score (MOS) is as follows:
  - Fixed to Fixed Assured Voice 4.0.
  - Fixed to Fixed Non-Assured Voice 3.8.
  - Fixed to Deployed Assured Voice 3.6.
  - Deployable to Deployable Assured Voice 3.2.
- Session Preemption. Lower precedence sessions will be preempted on the access circuit to accept the SC setup of a higher precedence level outgoing or incoming session establishment request.
- Traffic Service Classification and Priority Queues. In terms of the CE-R queuing structure, traffic will be assigned to the higher priority queues by a UC defined service class as described in Section 3, Auxiliary Services.
- Multiprotocol Label Switching (MPLS) and MPLS Virtual Private Networks (VPNs). Can be implemented in the ASLAN but cannot be extended to the Defense Information Systems Network (DISN).

7.2 B/P/C/S UC DESIGN

The military B/P/C/S-level design is flexible, depending on whether or not the location uses Enterprise services. The design may consist of an SC complex that may consist of a redundant SC, or several SCs in an array or cluster arrangement, in a LAN, CAN, or MAN structure. The LAN, CAN, or MAN design may be tailored to a single building or an entire base structure with varying degrees of robustness tailored to individual user and building mission requirements. Off-base connectivity to the long-haul DISN network infrastructure is provided through the Session Border Controller function. Interface to the local commercial telephone network is provided through a Media Gateway (MG) function within an SC per local interface requirements. It is a Military Department (MILDEP) responsibility to design and fund the base infrastructure design to meet their organizational mission, performance and affordability requirements.

7.3 SC DESIGNS – VOICE

Figure 7.3-1, B/P/C/S-Level Voice over IP SC Voice Designs, shows examples of three possible configurations for connecting multiple SCs on a B/P/C/S to the DISN SS. A single SC per B/P/C/S or participation with a regional Enterprise SC is the preferred affordable solution for fixed locations. Tactical deployments may be best served by treating the Tactical Theater as a region with multiple SCs as shown in Case 3. The Unclassified CE (U-CE) Routers are dual homed (not illustrated in figure). At the top of the figure, the first case shown is when multiple LANs, each with its own SC and U-CE Router, connect via separate access circuits to the DISN WAN. Each SC would have its own traffic-engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from one SC on the base to another SC on the base must traverse the DISN SS to connect to the other SC. Should base connection to the DISN SS be lost, then sessions from one base SC to the other on-base SC could not be established. In addition, if one of the SCs was not using all its traffic-engineered bandwidth (Budget A), a second SC (Budget B), could not use the unused bandwidth of the other SC (Budget A).

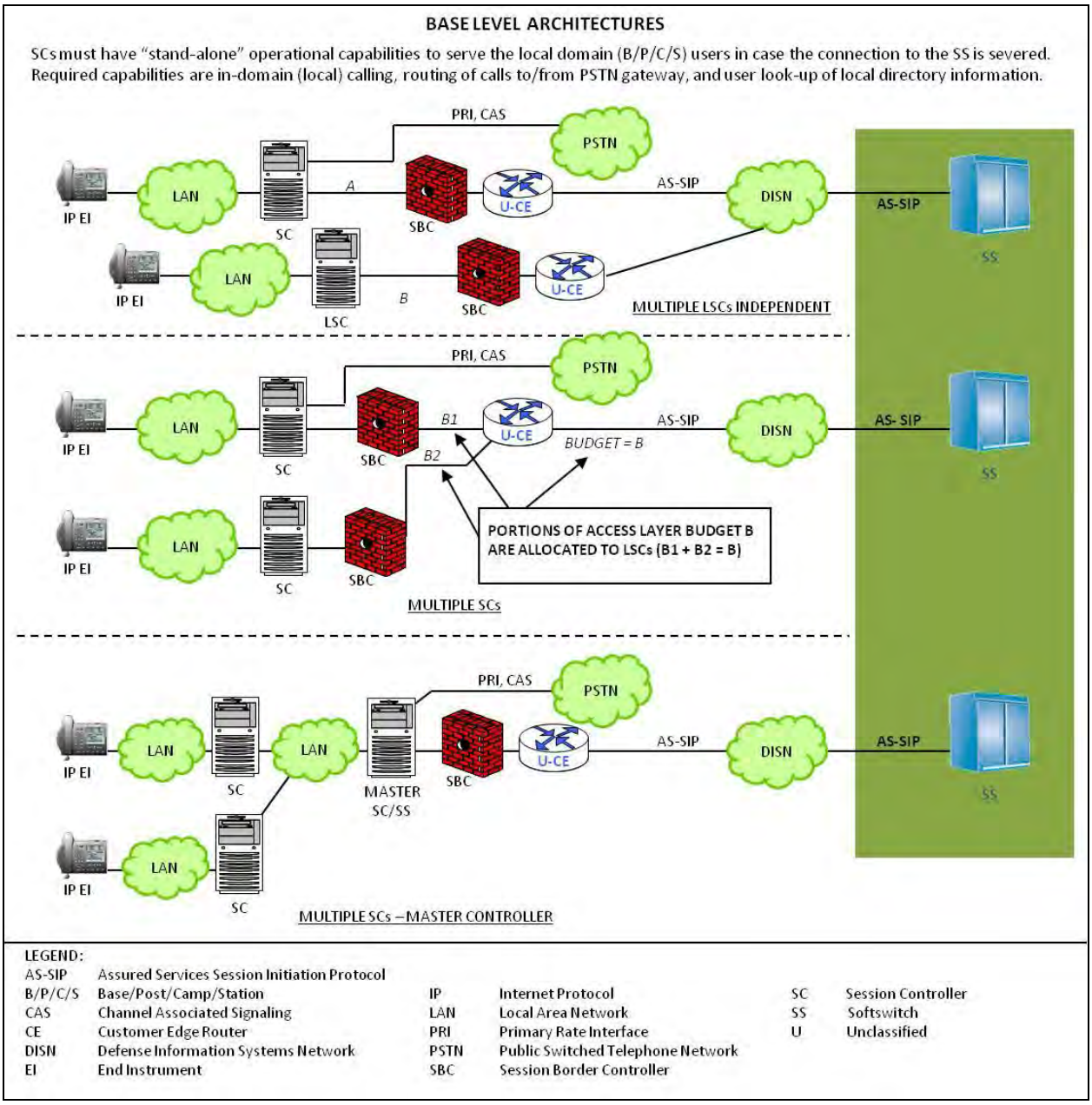

Figure 7.3-1. B/P/C/S-Level Voice over IP SC Designs

The second case, shown in the middle of the diagram, allows sessions to be established through the U-CE Router when connection to the DISN WAN is lost. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic-engineered bandwidth for each individual SC (i.e., B = B1+B2). Again, if one SC is not using all its budget/bandwidth, the other SC cannot use the unused budget/bandwidth. For one SC to establish a session to the other SC, without access to the SS, then each SC must contain the directory information of all SCs on the base.

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

The third case requires the design and implementation of an SC array or cluster concept where a master SC, as shown in the figure, has a master directory of all users on the base. Under this arrangement, service order activity at one SC will be reflected automatically at all SCs in the array or cluster, including the master SC. Only the first case will be specified in detail in the Unified Capabilities Requirements (UCR) 2013. The other two cases will require custom engineering of the base design to ensure interoperability and acceptable performance between the various on-base SC arrangements and vendors.

Some general rules to follow with respect to a Master SC (MSC) and Subtended SCs (SSCs) are as follows:

1. End instruments served by an MSC are treated like EIs served by SSCs.
2. The MSC adjudicates the enclave budget between the SSCs.
3. Either of the following two methods is acceptable:
    a. Method 1: the master always ensures the highest priority sessions are served (up to the budget limit of the access link) regardless of the originating SSC, for example:
        (1) If the ASAC budget is 30.
        (2) Each SSC (3, total) allowed 10 voice sessions (3 budgets).
        (3) The MSC performs preemptions to ensure higher precedence sessions succeed.
        (4) The MSC blocks ROUTINE precedence sessions from any SC after the access link budget is met.
    b. Method 2: the Master maintains a strict budget for SSCs, for example:
        (1) If the ASAC budget is 30.
        (2) Each SSC (3, total) with each allowed 10 sessions.
        (3) Does not use unfilled SC budget to service above ROUTINE precedence sessions from another SSC.
    c. All SCs directly connect to an E911 Management System (EMS) to permit MILDEP support of the U.S. Cyber Command (USCYBERCOM).
    d. The MSC is not required to provide an aggregated Network Management (NM) view of the SSCs.
    e. MSCs and SSCs communicate using AS-SIP and/or proprietary signaling protocols if SCs are from the same vendor:
        (1) All signaling destined external to the enclave passes through the MSC.

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

f. Each SC maintains two budget counts as follows:

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

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

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

h. When an SSC directly connects to the PSTN (exception situation, not desired), then only EIs of the SSC can originate and receive calls from that PSTN PRI/Channel Associated Signaling (CAS) trunk.

i. The MSC is the only connection to enclave TDM infrastructure (simplifies location services).

The choice of the B/P/C/S SC configurations is dependent on the size of the B/P/C/S. Very small bases will have only one SC so these configurations are not of concern. Larger B/P/C/Ss are most likely to have multiple circuit switches to replace, and might try to set up the SC connections like their circuit switches, which would lead to the undesirable configurations that do not use master SCs. Only the master configuration is recommended.

7.4 SC DESIGNS – VIDEO

Figure 7.4-1, B/P/C/S Video over IP SC Designs, illustrates the SC designs for video services. An SC is a call stateful AS-SIP signaling appliance at the B/P/C/S that directly serves IP video-capable EIs.

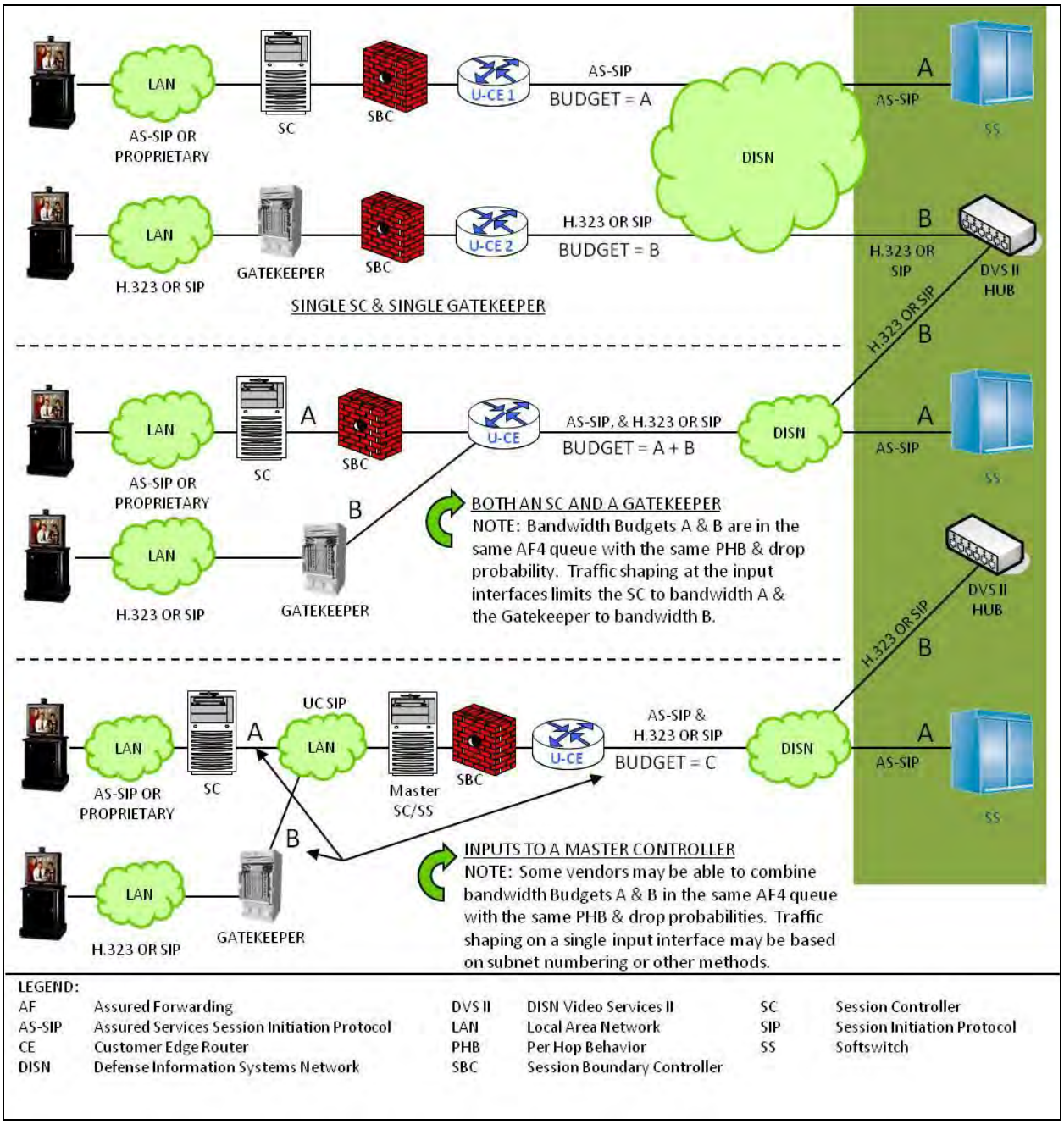

Figure 7.4-1. B/P/C/S Video over IP SC Designs

The design may consist of one or more physical platforms. On the trunk side to the WAN, the SC uses AS-SIP signaling. A Gatekeeper is an appliance that processes calls to the WAN using H.323 or SIP signaling. If the SC or Gatekeeper interfaces to the PSTN or to legacy B/P/C/S TDM appliances, it must also support PRI and CAS using its MG and MGC. All SCs provide PBAS via AS-SIP/ASAC for IP and for TDM trunks (where equipped).via its Media Gateway using the T1.619a protocol.

Figure 7.4-1 shows examples of three possible configurations for connecting multiple video-capable SCs and Gatekeepers on a B/P/C/S to the DISN SS.

The first case is, shown at the top of the figure, where multiple LANs, one with its own SC and U-CE Router, and another LAN with a Gatekeeper and U-CE Router that connect via separate access circuits to the DISN WAN. The SC and the Gatekeeper would each have its own traffic-engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from the SC or Gatekeeper on the base will not be able to communicate with each other because of the different signaling protocols in use by each. However, the SC and the Gatekeeper each will have separate bandwidths that act independently to each other.

The second case, shown in the middle of the figure, allows sessions to be established through the U-CE Router. In this case, both the SC and the Gatekeeper will act independently as described in the first case, but both will connect to the same U-CE Router. However, the SC video call and the Gatekeeper video call will connect to separate ports on the U-CE Router. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic-engineered bandwidth for the SC and Gatekeeper (i.e., A+B). Although each router port processing video calls acts independently in the AF4 queue, both customer calls must be treated equally if and only if the H.323 traffic is traffic engineered and controlled. This assumes that the AF4 queue is sized to meet the aggregate demand of the AS-SIP video teleconferencing (VTC) traffic and the H.323 Gateway-controlled traffic. If the H.323 traffic is not traffic engineered and controlled, then it goes into a different queue (i.e., the preferred data queue).

The third case requires the designation and implementation of an SC array or cluster concept as described for the voice design in Section 7.3, SC Designs–Voice.

With regard to the Gatekeeper interworking with the MSC or Softswitch (SS) in the third case, some vendors may be able to manage the SC-originated video call in addition to the Gatekeeper-originated call. In this case, the MSC or SS will manage Budgets A and B to make a more efficient use of Budget C. Although the SC video EI and the Gatekeeper EI will still not be able to communicate with each other (unless a H.323/AS-SIP Gateway is used) because of different protocols used, the MSC or SS will be able to process the calls into Budget C efficiently in the AF4 queue. All video calls leaving the MSC or SS must be treated equally only if the H.323 traffic is traffic engineered and controlled. This assumes that the AF4 queue is sized to meet the aggregate demand of the AS-SIP VTC traffic and the H.323 Gateway-controlled traffic. If the H.323 traffic is not traffic engineered and controlled, then it goes into a different queue (i.e., the preferred data queue).

7.5 LAN AND ASLAN DESIGN

The LAN consists of the Core, Distribution, and Access Layers, which all reside in the Customer Edge Segment of the E2E Global Information Grid (GIG) network reference. A high-level

illustration of the three LAN Layers is provided in Figure 7.5-1, B/P/C/S LAN Layers and Relationship to Customer Edge Segment. The figure depicts a traditional three tier LAN infrastructure. This is not to be interpreted that all LANs must be comprised of three tiers. The B/P/C/S LAN infrastructure may contain more or less tiers based on network engineering frameworks. The B/P/C/S LAN infrastructure must be composed from Approved Products List (APL) products. The number of tiers and composition (core, distribution, or access) is left to the discretion of the services.

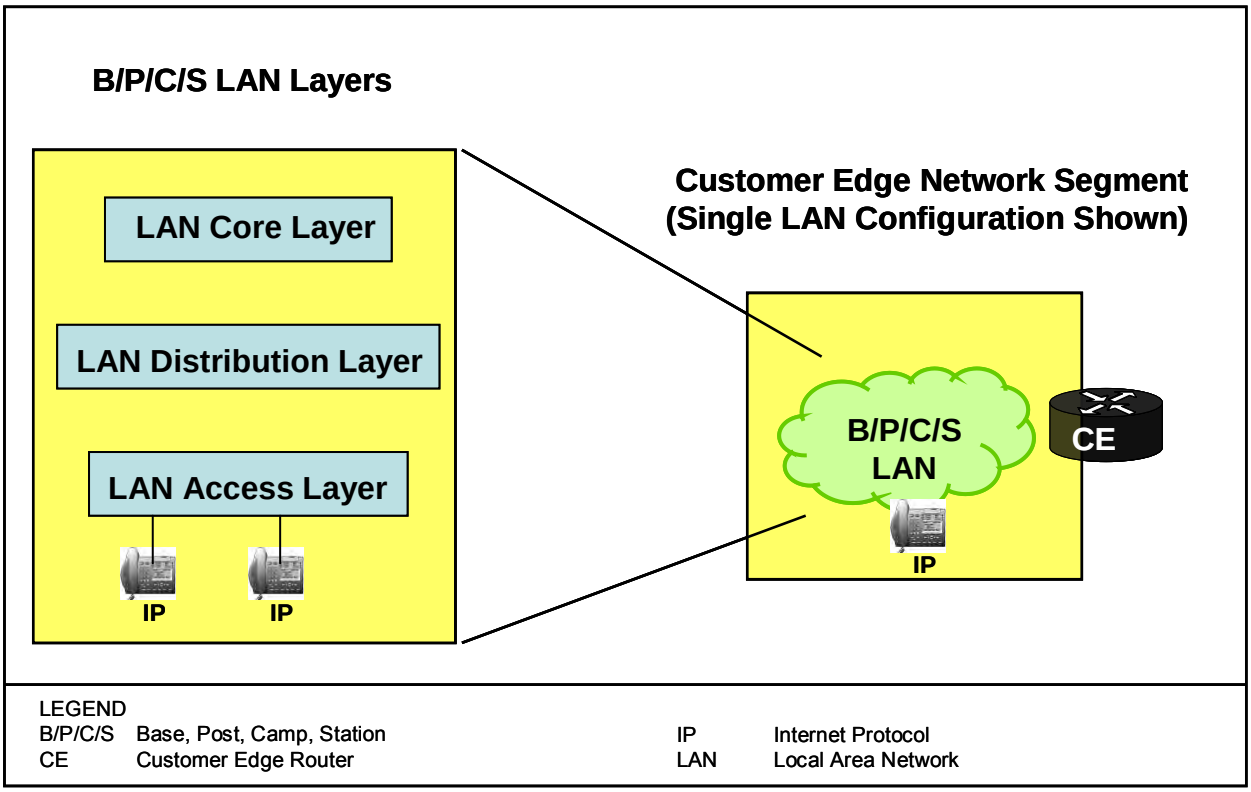

Figure 7.5-1. B/P/C/S LAN Layers and Relationship to Customer Edge Network Segment

7.5.1 Overview of LAN General Design and Requirements

To provide cost-effective LAN solutions that meet mission requirements for all users served by a LAN, two types of LANs are defined; they are ASLANs and non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs. The ASLANs and non-ASLANs may be designed to use any combination of the layers and functional capabilities, shown in Figure 7.5-2, LAN Layers. Multiple layers may be combined in a single switch or router (i.e., router acts as Distribution and Access Layers).

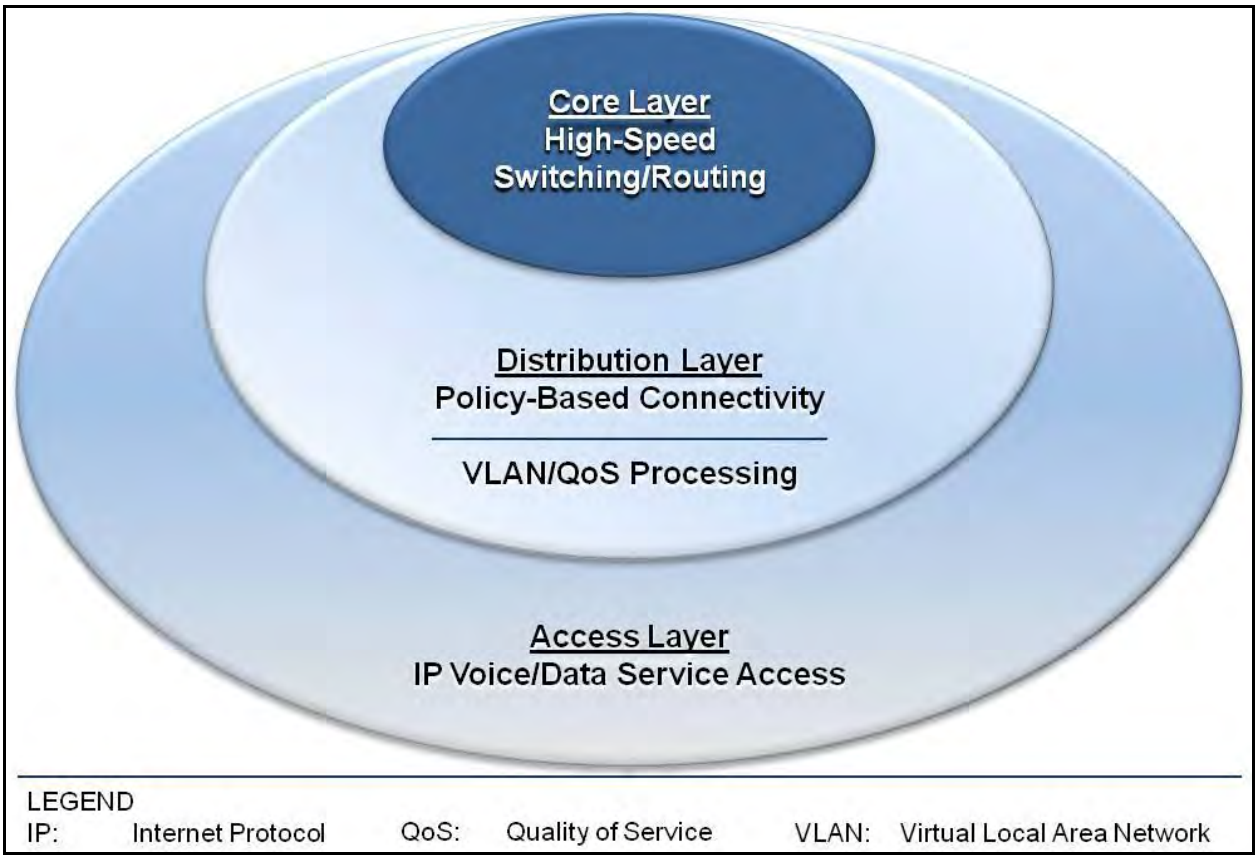

Figure 7.5-2. LAN Layers

The three LAN Layers are as follows:

1. Access Layer. The Access Layer is the point at which local end users are allowed into the network. This layer may use access lists or filters to optimize further the needs of a particular set of users.
2. Distribution Layer. The Distribution Layer of the network is the demarcation point between the Access and Core Layers and helps to define and differentiate the Core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.
3. Core Layer. The Core Layer is a high-speed switching backbone and is designed to switch packets as fast as possible.

Figure 7.5-3, Representative B/P/C/S Design and Terminology, illustrates a typical B/P/C/S LAN design. The LAN design and requirements refer to LAN products in terms of the Core, Distribution, and Access Layer products. These products are often known by other names such as Main Communication Node (MCN), Area Distribution Node (ADN), and End User Building (EUB) switch.

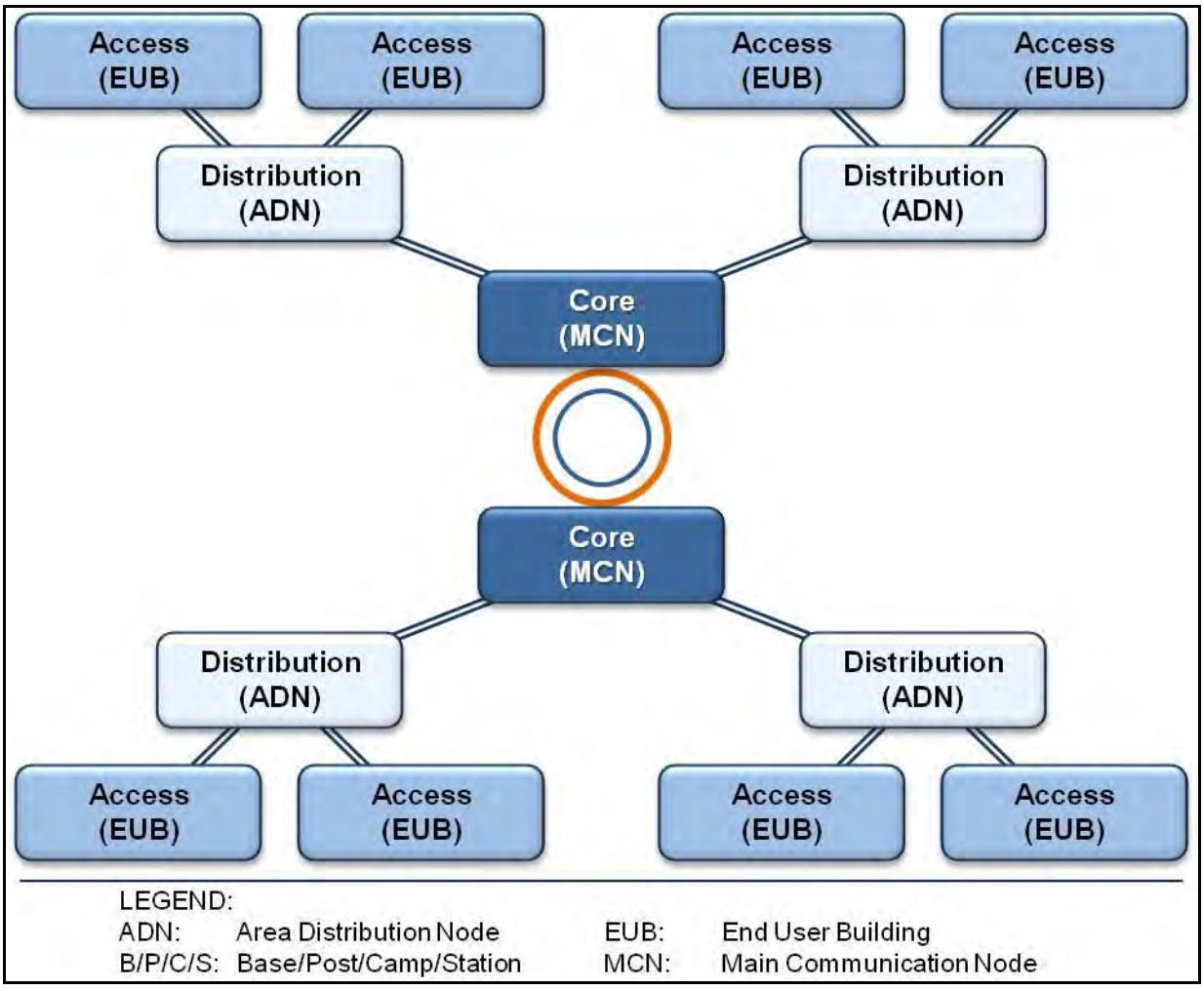

Figure 7.5-3. Representative B/P/C/S Design and Terminology

Within the LAN, the terminology used to reference traffic at each specific Open System Interconnect (OSI) layer is shown in Table 7.5-1, OSI Layer Control Information Name.

Table 7.5-1. OSI Layer Control Information Name

OSI LAYER	CONTROL INFORMATION NAME
Application Presentation Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit
LEGEND OSI: Open System Interconnect	

7.5.2 LAN Types and Mission Support Summary

The principal LAN requirements are summarized in Figure 7.5-4.

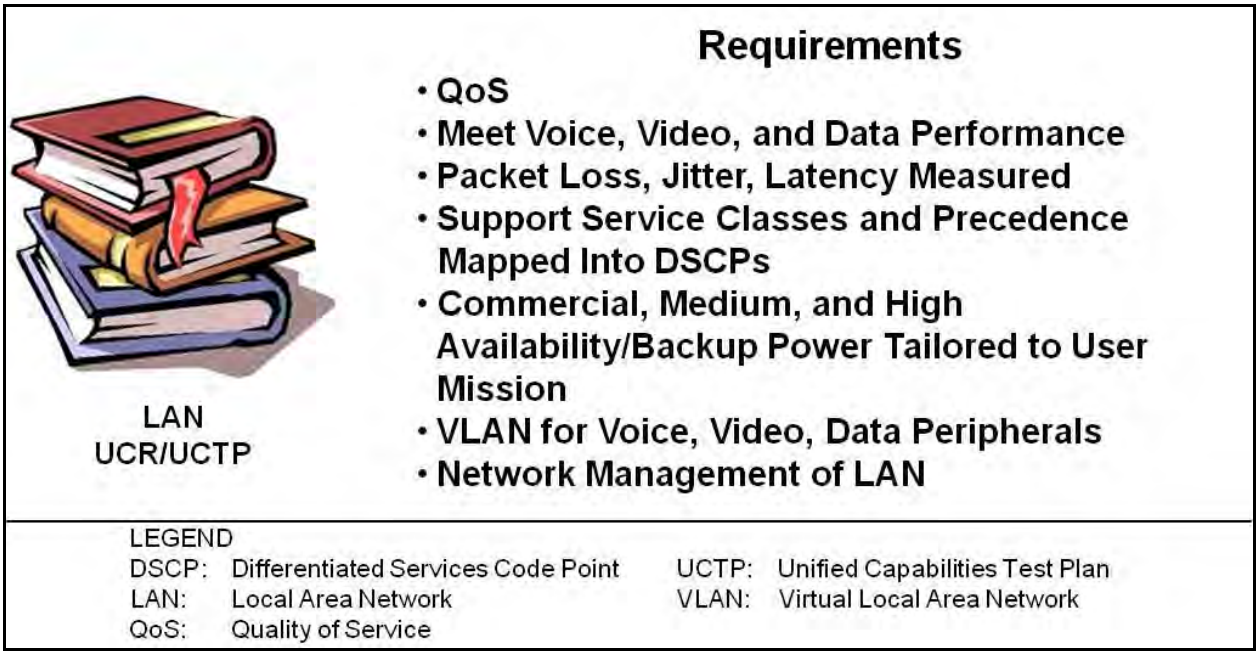

Figure 7.5-4. LAN Requirements Summary

Two types of LANs are ASLAN and non-ASLAN, depending on the type of missions and users served by a LAN. ASLANs support assured services while non-ASLAN need not meet assured services requirements. ASLANs provide enhanced availability and backup power as compared to Non-ASLANs. As a result, they are more robust and more costly. The two LAN types and three categories along with user classes are illustrated in Figure 7.5-5, Three Categories of LANs Tailored to Mission Needs.

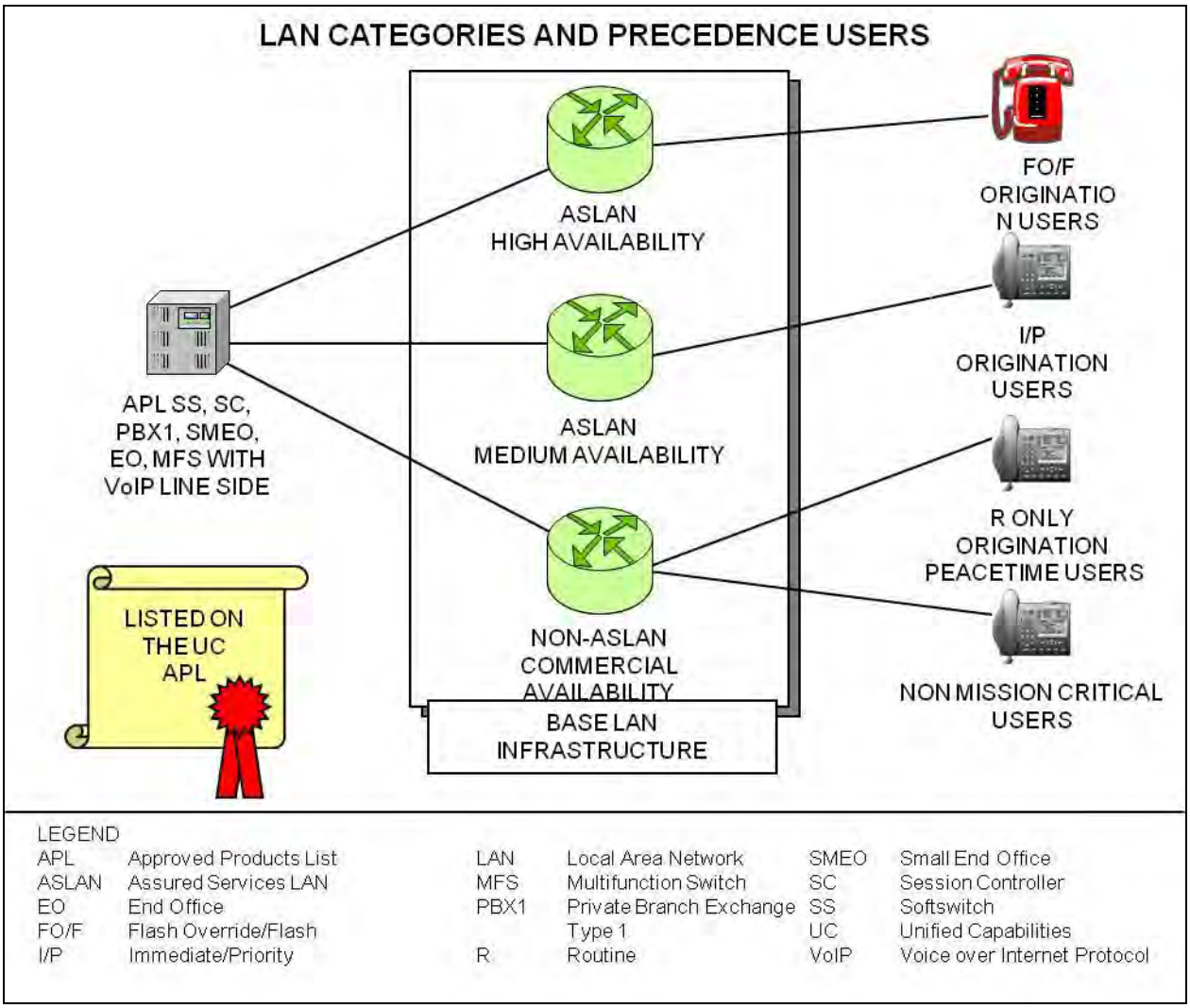

Figure 7.5-5. Three Categories of LANs Tailored to Mission Needs

Table 7.5-2, LAN Requirements Summary, shows the requirements needed based on subscriber mission category. Note that in addition to subscriber requirements, mission critical functions that do not originate or receive precedence traffic must also be supported since these functions must continue in time of crisis. Requirements are defined, as necessary, for the user, while Permitted allows other user types to be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence is required to be served on a High Availability ASLAN, and other users are permitted on the same LAN). Not Permitted means that the user must not be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence cannot be served by a Medium Availability ASLAN or non-ASLAN). Not required are requirements that do not have to be met for some users (such as requirements for diversity, redundancy, and power backup that are not required for users that only have ROUTINE precedence).

Table 7.5-2. LAN Requirements Summary

LAN REQUIREMENT ITEM	USER PRECEDENCE ORIGINATION AUTHORIZATION			
	F/FO	I/P	R	NOT MISSION CRITICAL
ASLAN High	R	P	P	P
ASLAN Medium	NP	R	P	P
Non-ASLAN	NP	NP	P	P
ASF	R	R	R	NR
Redundancy (with diversity)	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
GOS p=	0.0	0.0	0.0	Note 1
Availability	99.999	99.997	99.9	99.8
NOTE 1: GOS is discretionary and shall be determined by DoD Components.				
LEGEND				
ASF: Assured Services Features		I/P: IMMEDIATE/PRIORITY		P: Permitted
ASLAN: Assured Services LAN		LAN: Local Area Network		R: Required
F/FO: FLASH/FLASH OVERRIDE		NP: Not Permitted		R: ROUTINE
GOS: Grade of Service		NR: Not Required		

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

Installing ASLAN in all buildings may result in a fiscally untenable cost. Therefore, the actual LAN implementation will vary from base to base depending on building or facility locations, installed cable plant, and the location and type of missions being performed within the various buildings on the base.

ASLAN requirements for a Military installation can be determined by performing a site survey to identify the specific locations (buildings) that require a High, Medium, or non- ASLAN capabilities. Examples of buildings with mission critical functions include but are not limited to the following:

Buildings with LAN core nodes, reachable nodes that extend services into, e.g., Theater, network operations and security centers, network control centers , command posts, battle staff, Core nodes including connectivity between the core nodes (i.e., the LAN backbone) must be high availability. If the backbone is not a high availability ASLAN, nothing else can be high availability.

Figure 7.5-6, An Example of a Potential CAN With a Mix of Mission and Non-Mission-Critical Users, is an example of a LAN with a mix of organizations with different Mission and Non-Mission-Critical Users that combines the LAN capabilities illustrated in Figure 7.5-2, Three Categories of LANs Tailored to Mission Needs. It shows a LAN at a location involving multiple buildings and types of mission users and how connectivity redundancy and the backup power time requirement of eight, two, or zero hours are met in a cost-effective manner.

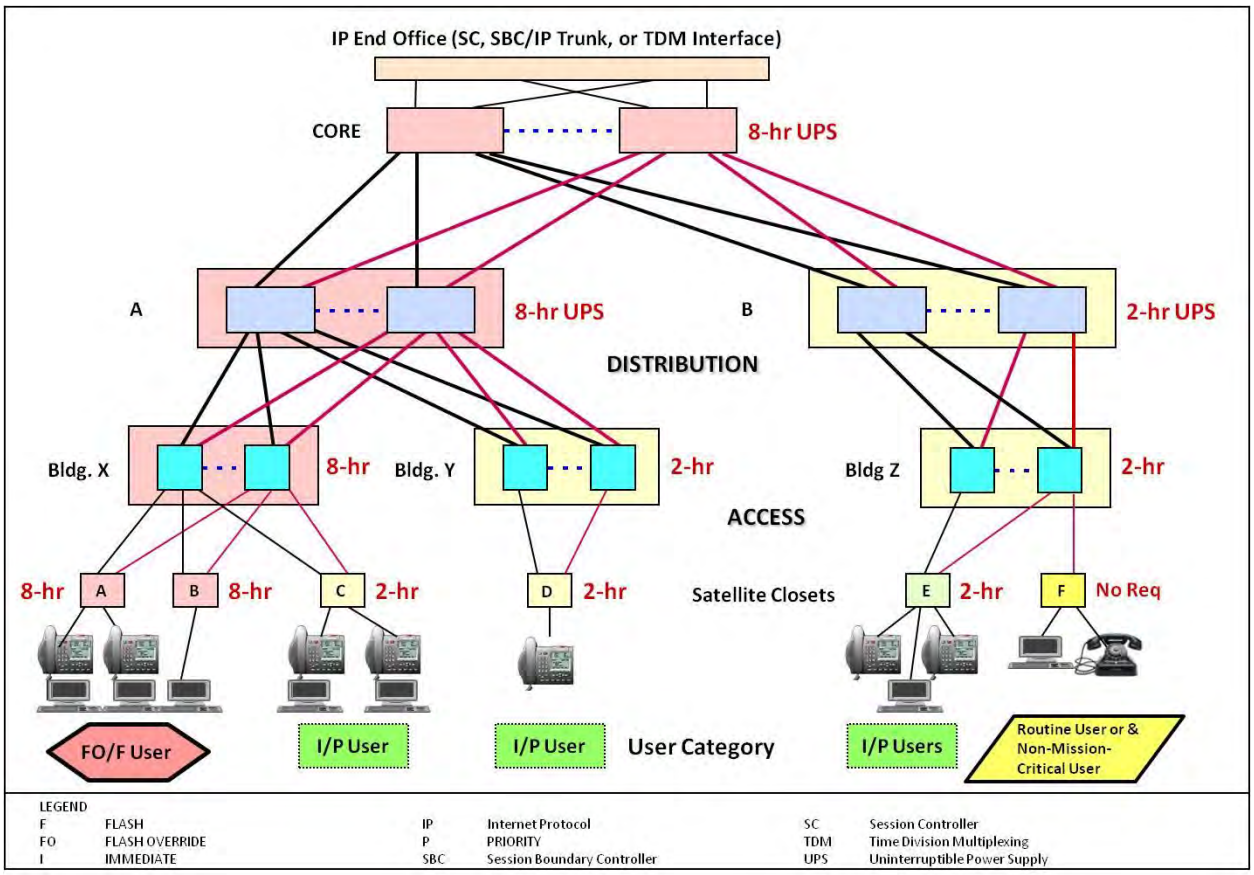

Figure 7.5-6. An Example of a Potential CAN With a Mix of Mission and Non-Mission Critical Users

7.5.3 Wireless LANs

Wireless networks may support IMMEDIATE/PRIORITY (I/P), ROUTINE (R), and non-mission critical users, but shall not be used to support F/FO users.

The use of wireless in the LAN as a bridging function shall not increase latency by more than 10 ms for each bridging pair. This is calculated based on the end-to-end requirements to support assured services users. Since the wireless bridge may be implemented within the ASLAN. It may process assured services voice. Thus the need to keep end-to-end latency below the prescribed 220 ms was considered. The use of wireless via an access point shall not increase LAN latency by more than 15 ms. Wireless access pints are not used to provide assured services voice. Therefore end-to-end latency for non-assures services voice is increased to 250 ms.

Given the possibility of having access points at either end, a budget of 15 ms for the access point was derived.

The WABs may support F/FO calls, I/P, and non-mission critical calls. All calls must meet other specified performance requirements for these users.

7.6 END-TO-END LAN PERFORMANCE REQUIREMENTS

End-to-end performance across a LAN is measured from the traffic ingress point (typically, the LAN Access product input port) to the traffic egress port (typically, the LAN Core product port connection to the CE Router). Metrics are based on best estimates for the DoD environment calculated through lab and operation testing.

7.6.1 Voice Services

7.6.1.1 Latency

The ASLAN shall have the capability to transport voice IP packets, media and signaling, with no more than 6 ms latency E2E across the network as measured under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering. The latency shall be achievable over any 5-minute measured period under congested conditions.

7.6.1.2 Jitter

The ASLAN shall have the capability to transport voice IP packets E2E across the network with no more than 3 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

7.6.1.3 Packet Loss

The ASLAN shall have the capability to transport voice IP packets E2E across the network with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the network shall not exceed 0.045 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

7.6.2 Video Services

7.6.2.1 Latency

The ASLAN shall have the capability to transport video IP packets with no more than 30 ms latency E2E across the network. Latency is increased over voice IP packets because of the

increased size of the packets (230 bytes for voice packets and up to 1518 bytes for video). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

7.6.2.2 Jitter

The ASLAN shall have the capability to transport video IP packets E2E with no more than 30 ms of jitter across the network. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering).

7.6.2.3 Packet Loss

The ASLAN shall have the capability to transport video IP packets E2E with packet loss not to exceed configured traffic engineered (queuing) parameters across the network. Actual measured packet loss across the network shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

7.6.3 Data Services

7.6.3.1 Latency

The ASLAN shall have the capability to transport prioritized data IP packets with no more than 45 ms latency E2E across the network. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for data). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

7.6.3.2 Jitter

There are no jitter requirements for preferred data IP packets.

7.6.3.3 Packet Loss

The ASLAN shall have the capability to transport prioritized data IP packets E2E with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the LAN shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute period measured under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering).

7.7 INFRASTRUCTURE NETWORK MANAGEMENT REQUIREMENTS

ASLAN Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. The infrastructure components shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/ reconfiguration of objects that have existing DoD GIG management capabilities. The infrastructure components must be able to be centrally managed by an overall Network Management System (NMS). In addition, both NMS (RMON2) and Management Information Base II (MIB II) shall be supported for Simple Network Management Protocol (SNMP). In addition, if other methods are used for interfacing between infrastructure products and the NMS they shall be implemented in a secure manner, such as with the following methods:

- Secure Shell 2 (SSH2). The SSH2 Protocol shall be used instead of Telnet because of its increased security. The LAN products shall support Request for Comments (RFC) 4251 through RFC 4254 inclusive.
- HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HyperText Transfer Protocol (HTTP) because of its increased security as described in RFC 2660. The infrastructure products shall support RFC 2818.

7.7.1 Configuration Control

The ASLAN Configuration Control identifies controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (DoD Chief Information Officer [CIO] Guidance IA6-8510 IA). Infrastructure components shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD GIG management capabilities. The NMS shall report configuration change events in near-real-time (NRT), whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. NRT is defined as receiving configuration control updates within 5 seconds of querying the status (polled) or within 5 seconds of changes being sent from the monitored device (pushed) Configuration change, excluding transport time.

7.7.2 Operational Changes

The ASLAN infrastructure components must provide metrics to the NMS to allow them to make decisions on managing the network. Network management systems shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). Near-real time is defined as receiving operational changes within 5 seconds of querying the status (polled) or within 5 seconds of receiving status changed (pushed), excluding transport time. Specific metrics are defined in NMS

Sections 2.17, Management of Network Appliances, and 2.18, Network Management Requirements of Appliance Functions.

7.7.3 Performance Monitoring

All ASLAN infrastructure components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. An NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) within 5 seconds of querying the status (polled) or within 5 seconds of receiving status changes (pushed) from the monitored device. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.

7.7.4 Alarms

All ASLAN infrastructure components shall be capable of providing SNMP alarm indications to an NMS. Network Management Systems will have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving. This capability allows network managers to monitor and maintain the situational awareness of the network's manageable products automatically, and to become aware of network problems as they occur based on the trouble tickets generated automatically by the affected object or network. Alarms will be correlated to eliminate those that are duplicate or false, initiate test, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. NRT is defined as receiving alarm changes within 5 seconds of querying the status (polled) or within 5 seconds of receiving alarm changes (pushed) from the monitored device.

7.7.5 Reporting

To accomplish GIG E2E situational awareness, an NMS will have the NM capability of automatically generating and providing an integrated/ correlated presentation of network and all associated networks.

7.8 ENGINEERING REQUIREMENTS

7.8.1 Copper Media

Cabling used for the ASLAN shall not be lower than a CAT-5 performance (see Table 7.8-1, Cable Grade Capabilities). The CAT-5 cable specification is rated up to 100 megahertz (MHz) and meets the requirement for high-speed LAN technologies, such as Fast Ethernet and Gigabit Ethernet. The Electronics Industry Association/Telecommunications Industry Association (EIA/TIA) formed this cable standard that describes performance the LAN manager can expect from a strand of twisted pair copper cable. Along with this specification, the committee formed

the EIA/TIA-568-B standard named the "Commercial Building Telecommunications Cabling Standard" to help network managers install a cabling system that would operate using common LAN types, like Fast Ethernet. The specification defines Near End Crosstalk (NEXT) and attenuation limits between connectors in a wall plate to the equipment in the closet. Wires used for interconnecting LANs using Digital Subscriber Line (DSL) Access Devices and DSL Concentrators should not be lower than a CAT3 performance (see Table 7.8-1, Cable Grade Capabilities). Actual implementations depend on existing wiring infrastructure.

Table 7.8-1. Cable Grade Capabilities

CABLE NAME	MAKEUP	FREQUENCY SUPPORT	DATA RATE	ASLAN COMPATIBILITY
CAT-3	1 twisted pair of copper wire– terminated by RJ11 connectors	16 MHz	Up to 10 Mbps	DSL (see Section 7.8, DSL Requirements)
CAT-4	2 twisted pairs of copper wire – terminated by RJ45 connectors	20 MHz	Up to 16 Mbps	DSL (see Section 7.8, DSL Requirements)
CAT-5	4 twisted pairs of copper wire – terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	1000Base-T, 100Base-TX, 10Base-T
CAT-5e	4 twisted pairs of copper wire – terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	10Base-T, 100Base-TX, 1000Base-T
CAT-6	4 twisted pairs of copper wire – terminated by RJ45 connectors	250 MHz	1000 Mbps	10Base-T, 100Base-TX, 1000Base-T
LEGEND				
ATM: Asynchronous Transfer Mode		Mbps: Megabits per second		T: Ethernet half-duplex
Base: Baseband		MHz: Megahertz		TX: Ethernet full-duplex
CAT: Category		RJ: Registered Jack		

7.8.2 Traffic Engineering

7.8.2.1 Voice Services

ASLAN bandwidth required per voice subscriber is calculated as 102 Kbps (each direction) for each IP call (for IPv4). This is based on G.711 (20 ms codec) with IP overhead as depicted in Figure 7.8-1, Voice over IP Packet Size, (97 Kbps for Ethernet IPv4) plus 5 Kbps for Secure Real-Time Transport Control Protocol (SRTCP).

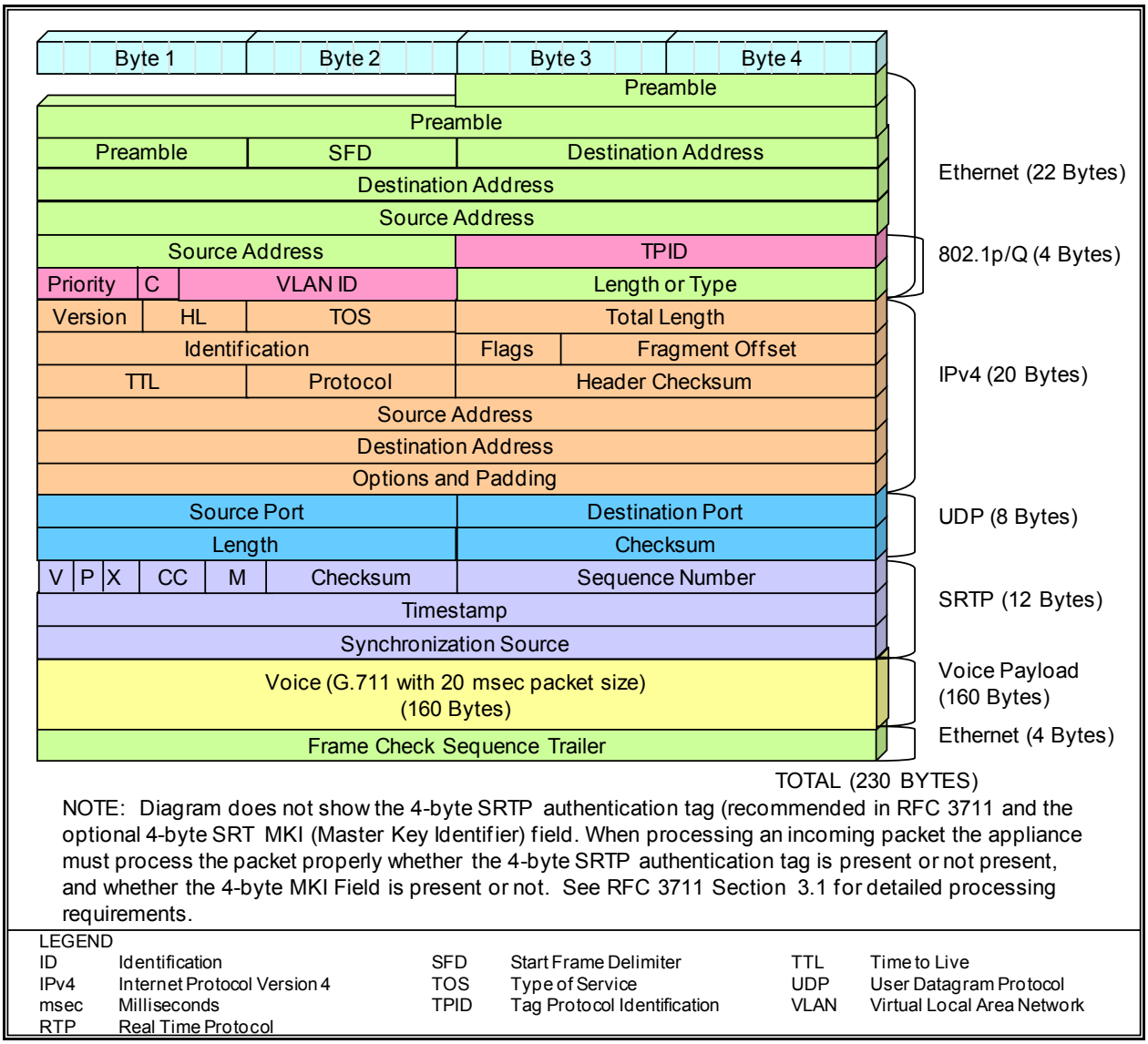

Figure 7.8-1. Voice over IP Packet Size

Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers. IPv6 adds an additional 20 bytes in the IP header (40 bytes instead of 20 bytes). The increase of 20 bytes to 250 bytes increases the IPv6 bandwidth to 110.0 Kbps. This calculation includes a 12-byte Ethernet Interframe gap and the SRTCP overhead.

Bandwidth in the LAN shall be engineered IAW Section 6.10 of the UC Framework

Table 7.8-2. LAN VoIP Subscribers for IPv4 and IPv6

PRODUCT	LINK TYPE	LINK SIZE	# MISSION CRITICAL VOIP SUBSCRIBERS (ASLAN)	# R AND NON-MISSION CRITICAL VOIP SUBSCRIBERS (NON-ASLAN)
Core	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000[3]	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	100 Mbps	250	500
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[4]	1
	IP Subscriber (converged)	100 Mbps	1[5]	1
Distribution	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	100 Mbps	250	500
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[4]	1
	IP Subscriber (converged)	100 Mbps	1[5]	1
Access	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	100 Mbps	250	500
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[4]	1
	IP Subscriber (converged)	100 Mbps	1[5]	1

NOTES:

1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements.
2. Link pairs may also include link aggregation. The link pair may use stand-by links or load balancing mechanisms. Regardless of method, the total number of subscribers per link pair (both links) is limited to the number of subscribers listed above.
3. For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization.
4. The minimum link for VoIP subscriber is 10 Mbps.
5. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps.

LEGEND

ASLAN: Assured Services LAN IP: Internet Protocol LAN: Local Area Network

PRODUCT	LINK TYPE	LINK SIZE	# MISSION CRITICAL VOIP SUBSCRIBERS (ASLAN)	# R AND NON-MISSION CRITICAL VOIP SUBSCRIBERS (NON-ASLAN)
C2: Command and Control	IPv4: IP Version 4		Mbps: Megabits per second	
Gbps: Gigabits per second	IPv6: IP Version 6		VoIP: Voice over IP	

1. No single point of failure within the ASLAN can cause a voice service outage to more than 96 users. It should be noted that a single point of failure for more than 96 subscribers may exist if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers). Based on the previous constraints, the recommended number of voice subscribers based on available link sizes is shown in Table 7.8-2.

7.8.2.2 Video Services

The amount of video bandwidth required over the ASLAN varies depending on the codec and other features that are negotiated at setup. Unlike voice, video over IP is not a constant rate. Video packets may range in size from hundreds of bytes up to 1500 bytes. Table 7.8-3, Video Rates and IP Overhead, lists the common video rates and associated IP overhead. Video bandwidth shall be engineered IAW bandwidth provisioning considerations provided in UCF Section 6.10, Bandwidth Provisioning Considerations.

Table 7.8-3. Video Rates and IP Overhead

VIDEO STREAM BANDWIDTH	IP OVERHEAD	TOTAL IP BANDWIDTH
128 kbps	32 kbps	160 kbps
256 kbps	64 kbps	320 kbps
384 kbps	96 kbps	480 kbps
768 kbps	192 kbps	960 kbps
2 Mbps	0.5 Mbps	2.5 Mbps
4.5 Mbps	1.125 Mbps	5.625 Mbps
6 Mbps	1.5 Mbps	7.5 Mbps
LEGEND		
IP: Internet Protocol	kbps: Kilobits per second	Mbps: Megabits per second

UCR 2013, Section 7, Table 7.3-2, Maximum Number of EIs Allowed per WLAS, lists the bandwidth available based on an engineered solution of 25 percent allocation of the bandwidth to video. Unlike voice, video does not have the single point of failure requirements. Thus, the capacity or available bandwidth on a link pair is based on the aggregate total, not one half used in the voice calculations. Table 7.8-4.

Table 7.8-4. Video over IP Bandwidth

ASLAN PRODUCT	LINK TYPE	LINK SIZE	# VIDEO OVER IP BW	# 384 KBPS SESSIONS
Core	IP Trunk Link	10 Gbps	2.5 Gbps	5000
	IP Trunk Link	1 Gbps	250 Mbps	500
	IP Trunk Link	100 Mbps	25 Mbps	50
	IP Trunk Link	10 Mbps	2.5 Mbps	5
	IP Subscriber (video only)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Distribution	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Access	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA

NOTES
1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements.
2. For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization.
3. The minimum link for VoIP subscriber is 10 Mbps.
4. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps.
5. Link pairs may use stand-by links or load balancing (e.g., link aggregation). Number of subscribers is calculated as not to exceed the link pair capacity listed above regardless of the method implemented.

LEGEND

ASLAN: Assured Services LAN	IP: Internet Protocol	Mbps: Megabits per second
BW: Bandwidth	kbps: kilobits per second	NA: Not Applicable
Gbps: Gigabits per second		

7.8.2.3 Data Services

The ASLAN will be traffic engineered to support data traffic IAW bandwidth provisioning considerations provided in Section 6.10.

7.8.3 VLAN Design and Configuration

The Virtual LANs (VLANs) offer the following features:

- Broadcast Control. Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.
- Security. The VLANs provide security in two ways:
  - High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside of that VLAN can communicate with them.
  - The VLANs are logical groups that behave like physically separate entities; inter-VLAN communication is achieved through a router. When inter-VLAN communication occurs through a router, all the security and filtering functionality that routers traditionally provide can be used because routers are able to look at Layer 3 information.

Two ways of defining a VLAN are as follows:

1. Port-Based. Port-based VLANs are VLANs that are dependent on the physical port that a product is connected to. All traffic that traverses the port is marked with the VLAN configured for that port. Each physical port on the switch can support only one VLAN. With port-based VLANs, no Layer 3 address recognition takes place. All traffic within the VLAN is switched, and traffic between VLANs is routed (by an external router or by a router within the switch). This type of VLAN is also known as a segment-based VLAN (see Figure 7.8-2, Port-Based VLANs).

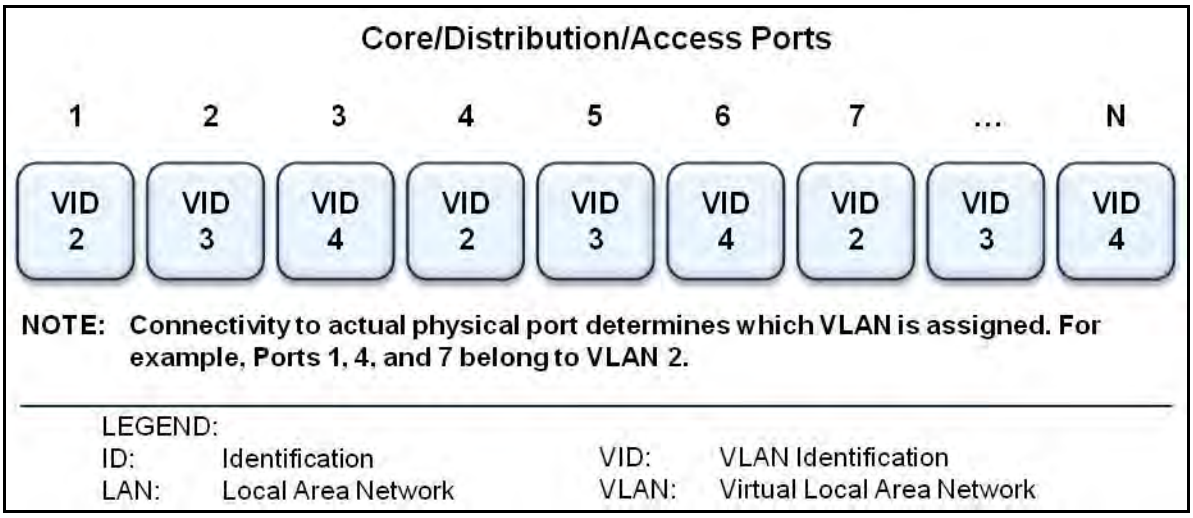

Figure 7.8-2. Port-Based VLANs

2. Institute of Electrical and Electronics Engineers (IEEE) 802.1Q. VLANs can be assigned by end products in accordance with (IAW) the IEEE 802.1Q VLAN ID tag.

7.8.4 Power Backup

To meet UC requirements for assured services, ASLAN equipment serving F/FO and I/P users must be provided with backup power. The ASLAN must meet the power requirements outlined. The following requirements for emergency power systems (EPSs) are bare minimum requirements. An EPS may be any combination of uninterruptible power source (e.g., batteries) or auxiliary power (e.g., generator) that it will provide near-instantaneous protection from input power interruptions. These requirements should be increased following the guidance in Telcordia Technologies GR-513-CORE to meet site operational requirements and extenuating characteristics of the application environment. Figure 7.8-3, ASLAN UPS Power Requirements, illustrates a typical arrangement of how the minimum power backup requirements can be met.

- F/FO. The ASLAN must provide an 8-hour backup capability in the event of primary power loss to F/FO user. Any ASLAN product, Core, Distribution, or Access, that supplies service to the F/FO user must have an 8-hour uninterruptible power supply (UPS).
- I/P. The ASLAN must provide 2-hour backup capability in the event of primary power loss to I/P users. Any ASLAN product, core, distribution, or access that supplies service to the I/P user must have a 2-hour UPS.
- R or Non-mission critical. R or non-mission critical users may lose telephony service in the event of a power failure. Commanders who are relying on voice communications to fulfill their responsibility for safety and force protection must take the above into account when implementing VoIP.

  NOTE: Backup Power (Environmental). Environmental systems (including but not limited to heating, ventilation and air conditioning) required to sustain continuous LAN equipment operation shall have backup power. Backup power may be provided by the same system used by the LAN or a separate backup system.

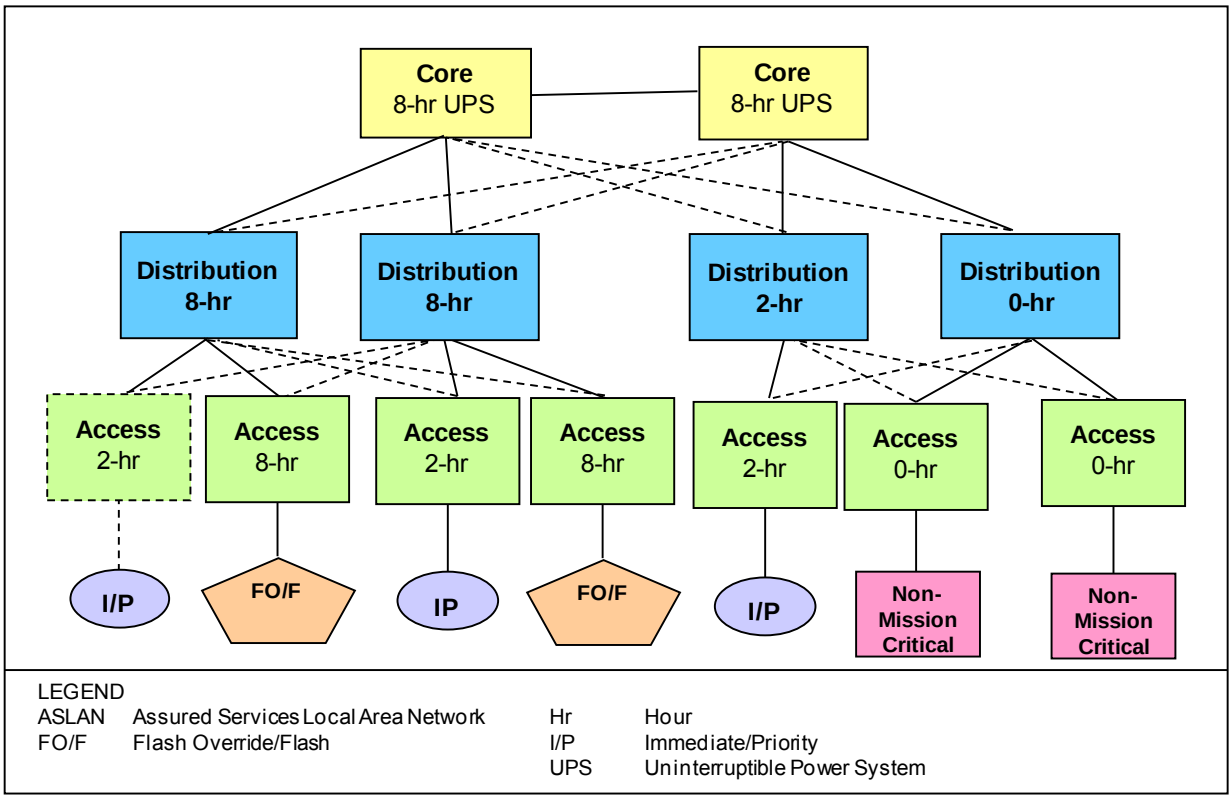

Figure 7.8-3. ASLAN UPS Power Requirements

7.8.5 Availability

The terms reliability, resiliency, and availability are sometimes used interchangeably. However, although all three terms are related to the concept of high availability, it is important to note the differences in terminology. Reliability is the probability that a system will not fail during a specified period of time. Resiliency is the ability of a system to recover to its normal operating form after a failure or an outage. Availability is the ratio of time that a service is available to total time.

Availability can be expressed as mean time between failure (MTBF) and mean time to repair (MTTR), and expressed in mathematical terms as:

Availability = MTBF/(MTBF+MTTR)

MTBF is tied to the reliability of the system, while MTTR and resiliency are closely related. Thus system availability increases as the reliability and/or resiliency of the system is increased. Availability is typically expressed in percentage of time the system is available or in downtime per year. The two methods of expressing availability are equivalent and related as shown in Table 7.8-5, Methods of Expressing Availability.

Table 7.8-5. Methods of Expressing Availability

NUMBER OF 9'S	AVAILABILITY	DOWNTIME PER YEAR
1	90.0%	36 days, 12 hrs
2	99.0%	87 hrs, 36 mins
2 (non-AS)	99.8%	17 hrs, 31 mins
3	99.9%	8 hrs, 46 mins
4	99.99%	52 mins, 33 secs
5	99.999%	5 mins, 15 secs
6	99.9999%	31.5 secs
LEGEND hrs: hours	mins: minutes	secs: seconds

The ASLAN has two configurations depending on whether it supports F/FO or I/P users. The ASLAN shall have a hardware availability designed to meet the needs of its subscribers:

- F/FO. An ASLAN that supports F/FO users is classified a High Availability ASLAN and must meet 99.999 percent availability to include scheduled maintenance.
- I/P. An ASLAN that supports I/P users is classified as a Medium Availability ASLAN and must have 99.997 percent availability to include scheduled maintenance.

The non-ASLAN shall provide an availability of 99.8 percent to include scheduled maintenance. R users who originate ROUTINE-only precedence calls but terminate any precedence level may be supported on a non-ASLAN, but the non-ASLAN must support Multilevel Precedence and Preemption (MLPP) for the R users. F/FO or I/P users shall not be supported on a non-ASLAN.

The methods for calculating reliability are found in Section 2, Session Control Products.

7.8.6 Maintainability

The following information is proved as an engineering guideline:

Maintainability is described in MIL-HDBK-470A as:

> "The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. In this context, it is a function of design."

Operational availability is similar to inherent availability but includes the effects of maintenance delays and other non-design factors.

The equation for operational availability, or Ao, is:

$$Ao = MTBM/(MTBM + MDT)$$

where MTBM is the mean time between maintenance and MDT is the mean downtime.

(NOTE: MTBM addresses all maintenance, corrective and preventive, whereas MTBF only accounts for failures. MDT includes MTTR and all other time involved with downtime, such as delays. Thus, Ao reflects the totality of the inherent design of the product, the availability of maintenance personnel and spares, maintenance policy and concepts, and other non-design factors, whereas availability reflects only the inherent design.)

When acquiring products for the ASLAN, maintainability of the products must be taken into consideration. Based on the need to meet operational availability for F/FO and I/P users, it is recommended that all ASLAN components have maintenance contracts in place that can replace key components in 24 hours or less.

7.8.7 MPLS Background

Traditional IP packet forwarding uses the IP destination address in the packet's header to make an independent forwarding decision at each router in the network. These hop-by-hop decisions are based on network layer routing protocols, such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP). These network layer routing protocols are designed to find an efficient path through the network, and do not consider other factors, such as latency or traffic congestion. Multiprotocol label switching creates a connection-based model overlaid onto the traditionally connectionless framework of IP routed networks. Multiprotocol label switching works by prefixing packets with an MPLS header, containing one or more "labels," as shown in Figure 7.8-4, MPLS Header, and Figure 7.8-5, MPLS Header Stacking. These short, fixed-length labels carry the information that tells each switching node how to process and forward the packets, from source to destination. Labels have significance only on a local node-to-node connection. As each node forwards the packet, it swaps the current label for the appropriate label to route the packet to the next node.

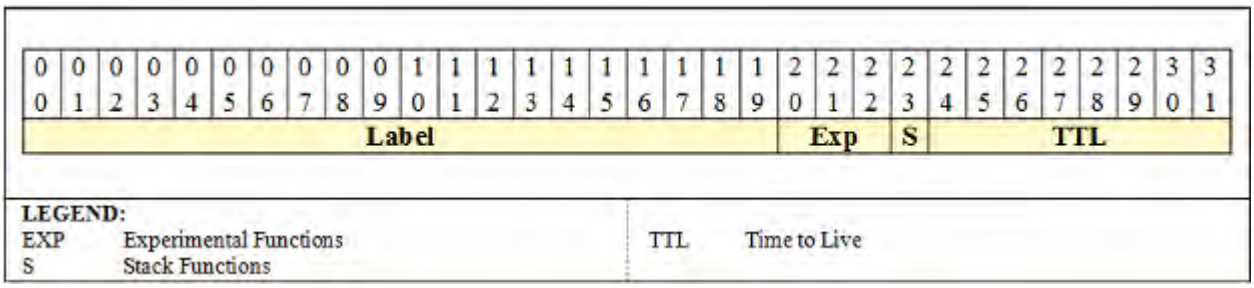

Figure 7.8-4. MPLS Header

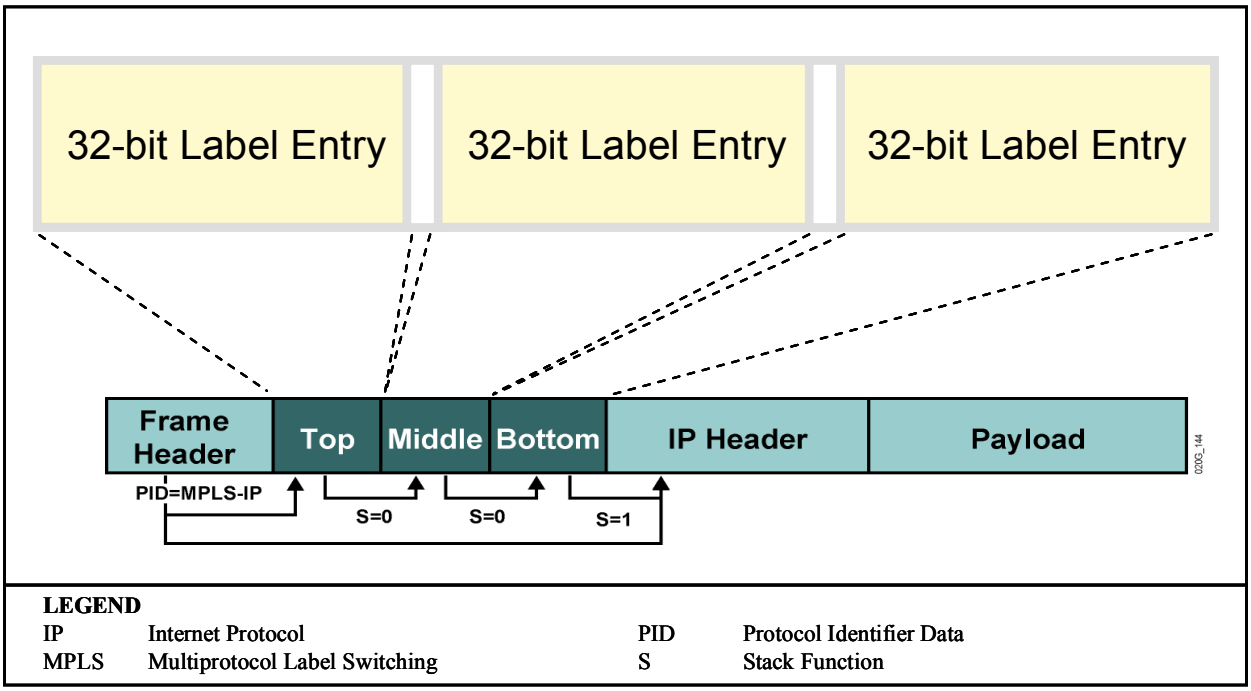

Figure 7.8-5. MPLS Header Stacking

Multiprotocol label switching relies on traditional IP routing protocols to advertise and establish the network topology. Multiprotocol label switching predetermines the path data takes across a network and encodes that information into a label that the network's routers understand. The MPLS operates at an OSI layer that is generally considered to lie between traditional definitions of Layer 2 (Data Link Layer) and Layer 3 (Network Layer). Figure 7.8-6, MPLS OSI Layer, illustrates the OSI Layer position of MPLS.

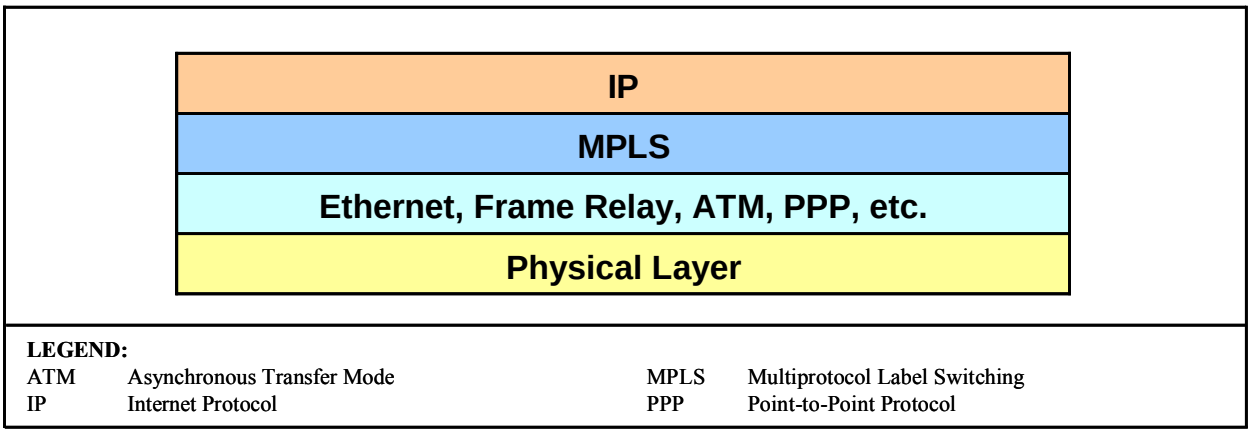

Figure 7.8-6. MPLS OSI Layer

7.8.8 MPLS Terminology

Definitions of terms can be found in Appendix C, Glossary and Terminology Description.

7.8.9 DoD LAN MPLS Operational Framework

The previous ASLAN sections detail requirements up to and including the Core LAN router devices. To interconnect Core or Distribution ASLAN routers on a B/C/P/S, transport technologies, such as MPLS, can be used. Figure 7.8-7, ASLAN MPLS Operational Framework, depicts DoD's ASLAN MPLS implementation. This section does not address WAN requirements for use of MPLS with the DISN backbone.

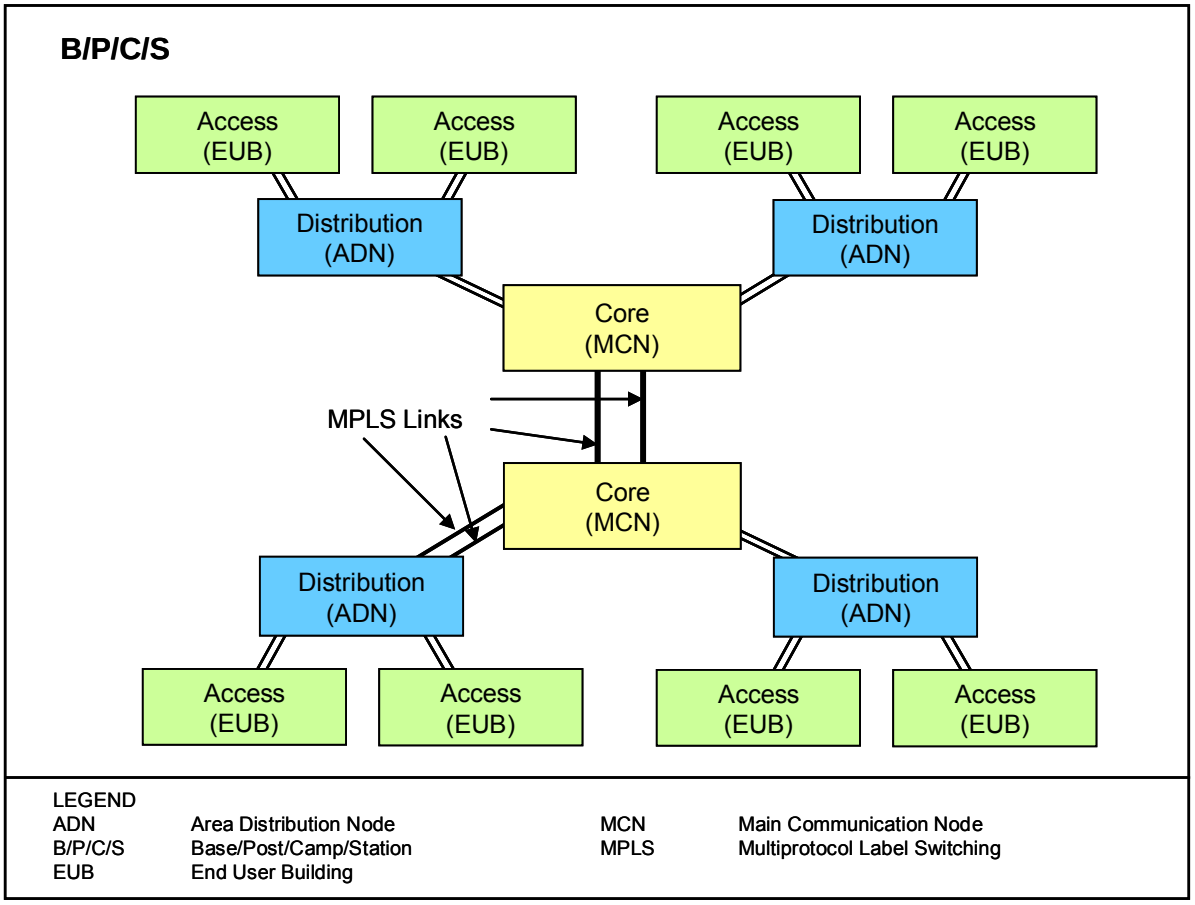

Figure 7.8-7. ASLAN MPLS Operational Framework

7.8.10 Primary Application Support

DSL is primarily used at military facilities to provide Local Area Network (LAN) interconnection. As such, the primary DSL functions that support this application are as follows:

- Symmetrical bandwidth (available with some DSL access technologies).
- Use of DSL repeaters to provide an extended range of operation.
- Point-to-Point configurations.
- Point-to-Multi-Point configurations.

7.8.11 DSL Overview

DSL uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, between endpoints. The term xDSL covers a number of DSL technologies. Those that are standards-based are shown in Table 7.8-6, ITU DSL Standards Overview.

Table 7.8-6. ITU DSL Standards Overview

VERSION	STANDARD	COMMON NAME	DOWNSTREAM RATE	UPSTREAM RATE	INITIALLY APPROVED IN
High Bit Rate DSL (HDSL)	ITU G.991.1	HDSL/2/4 (multi pair)	1.5-2.0 Mbps	1.5-2.0 Mbps	1998
ADSL	ITU G.992.1	ADSL (G.DMT)	6.144 Mbps	640 Kbps	1999
ADSL	ITU G.992.2	ADSL Lite (G.Lite)	1.5 Mbps	0.5 Mbps	1999
ADSL	ITU G.992.1 Annex A	ADSL over POTS	6.144 Mbps	640 Kbps	1999
Very High Speed DSL (VDSL)	ITU G.993.1	VDSL	52 Mbps	16 Mbps	2001
ADSL2	ITU G.992.3 Annex J	ADSL2	8 Mbps	800 Kbps	2002
ADSL2	ITU G.992.3	ADSL2	8 Mbps	800 Kbps	2002
ADSL2	ITU G.992.4	Splitterless ADSL2	1.5 Mbps	0.5 Mbps	2002
Single Pair High-Speed DSL (SHDSL)	ITU G.991.2	G.SHDSL (single pair)	2.3 Mbps	2.3 Mbps	2003
ADSL2+	ITU G.992.5	ADSL2+	24 Mbps	1.3 Mbps	2003
ADSL	ITU G.992.1 Annex B	ADSL over ISDN	12 Mbps	1.8 Mbps	2005
ADSL2	ITU G.992.3 Annex L	RE-ADSL2	5 Mbps	0.8 Mbps	2005
VDSL2	ITU G.993.2	VDSL2	100 Mbps[1]	100 Mbps[1]	2006
ADSL2+	ITU G.992.5 Annex M	ADSL2+M	24 Mbps	3.3 Mbps	2008

NOTE: VDSL2 supports transmission at a bidirectional net data rate (the sum of upstream and downstream rates) up to 200 Mbps.

Many of these DSL technologies support both analog voice services and high-bandwidth digital data services (which may include UC VoIP and Video over IP services). In this case, different frequency bands are used on each twisted-pair copper telephone line for the analog voice service and the digital data service.

7.8.11.1 DSL Bonding

Wire bonding solutions provide a method for combining multiple copper DSL connections (with the same or different bit rates) together into a single, aggregate connection. This technology is extremely valuable when support for high-speed services must be provided. Bonding can allow delivery of high-bandwidth services even when the bandwidth of individual DSL connections is relatively low.

Three DSL bonding standards are defined in Table 7.8-7, DSL Bonding Standards.

Table 7.8-7. DSL Bonding Standards

ITU-T STANDARD	DESCRIPTION
G.998.1	ATM-based multi-pair bonding: A method for bonding of multiple DSL lines to transport an ATM payload beyond the rate/reach capability of a single DSL loop. This protocol allows the bonding of 2 to 32 pairs and supports dynamic removal and restoration of pairs without human intervention.
G.998.2	Ethernet-based multi-pair bonding: Provides a method for bonding of multiple DSL lines for Ethernet transport. This recommendation builds on IEEE 802.3ah-2004 Ethernet in the First Mile (EFM) methods, and extends Ethernet transport over multiple xDSL technologies, including ADSL.
G.998.3	Multi-pair bonding using time-division inverse multiplexing: Details a method for bonding DSL lines using Time-Division Inverse Multiplexing (TDIM). This recommendation uses IEEE 802.3ah handshakes for pair discovery, parameter negotiation, and setup. It also allows the hitless addition and removal of pairs (i.e., without any service disruption) and the fast removal of a pair upon pair failure.

7.8.12 Ethernet in the First Mile Over Copper (EFMCu)

Ethernet in the first mile (EFM) is known as IEEE 802.3ah and defines Ethernet in the access network, i.e., first or last mile. EFMCu defines interfaces over voice-grade copper with optional multi-pair aggregation or bonding transmission.

EFMCu allows for deployment of resilient symmetrical Ethernet Access links over existing voice-grade copper infrastructure, providing an economical alternative to fiber and a solution where only voice-grade copper infrastructure exists.

There are two standardized EFMCu technologies:

- Long reach 2BASE-TL, delivering a minimum of 2 Mbps and a maximum of 5.69 Mbps over distances of at least 2700 m, using standard G.SHDSL.bis technology over a single copper pair.
- Short reach 10PASS-TS, delivering a minimum of 10 Mbps over distances of at least 750 m, using standard VDSL technology over a single copper pair.

7.8.13 DSL-Based ASLAN Interconnection Operational Framework

DSL or EFMCu connections are used to provide ASLAN interconnection in the Network Edge Segment. Either can be utilized in cases where voice-grade wiring is the only choice for linking ASLANs in different buildings within a military base. DSL or EFMCu utilization within a base is described in the following sections.

7.8.13.1 Point-to-Point Interconnection of ASLANs

Figure 7.8-8, Point-to-Point LAN Interconnection, illustrates the simplest scenario for DSL use on a military base is for basic point-to-point LAN interconnection. This can be used for connectivity within an ASLAN, or for connectivity between ASLANs on the same base. It makes use of Unshielded Twisted Pair (UTP) copper phone cables for connectivity.

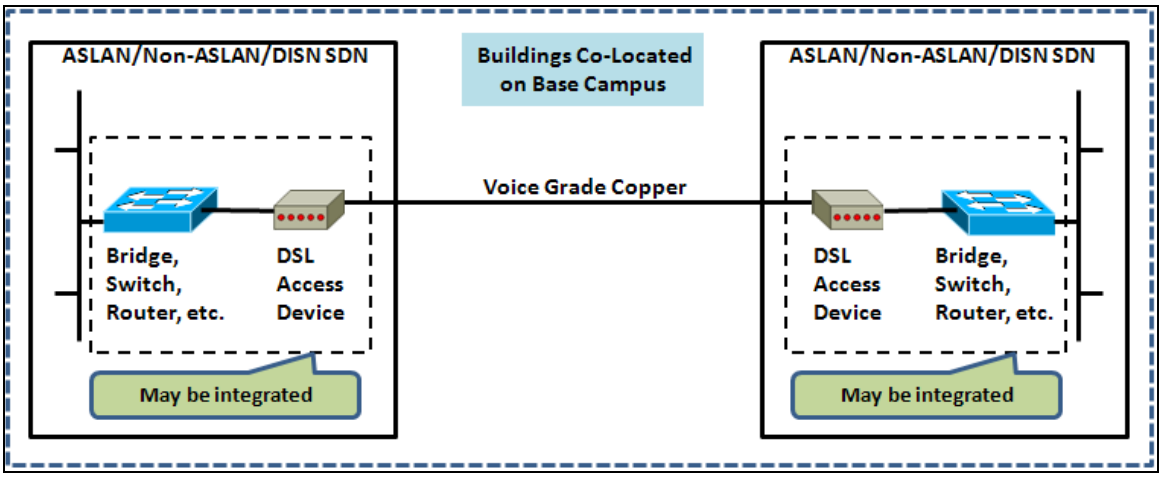

Figure 7.8-8. Point-to-Point LAN Interconnection

At each location is a DSL access device which contains a DSL line interface (on the voice-grade copper side) and typically an Ethernet physical interface (on the LAN side). At a minimum, the DSL access device supports data bridging between its two sides, but it may have additional functionality built in, such as LAN switching and IP routing.

7.8.13.2 Point-to-Multipoint Interconnection of ASLANs

As illustrated in Figure 7.8-9, Point-to-Multipoint Interconnection Concentration, a more complicated scenario for DSL use on a military base is for point-to-multipoint LAN interconnection. This can be used for aggregating connectivity of ASLANs to a single or multiple core locations within the same base. It also makes use of UTP copper phone cables for connectivity.

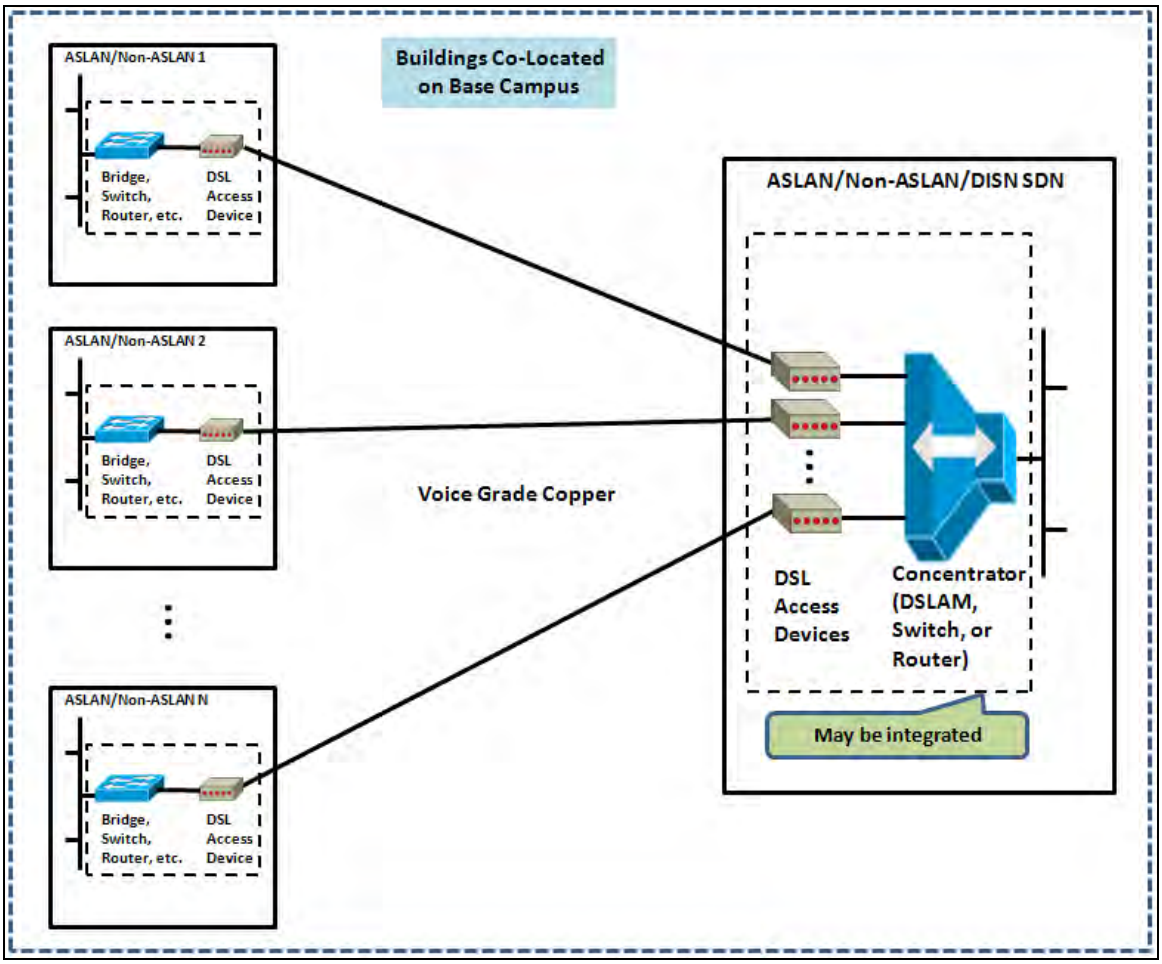

Figure 7.8-9. Point-to-Multipoint Interconnection Concentration

In this scenario, a Concentrator handles connectivity for multiple ASLAN locations and then aggregates traffic that is destined for remote destinations. Typically, the Concentrator is a DSL Access Manager (DSLAM), a Bridge, or a Router, all of which have advanced functionality to support switching or routing of IP packets between local ASLANs, and forwarding/routing of IP brackets between local DSLAMs and remote destinations.

DSLAMs can support a very large amount of interfaces (e.g., multiple 19 inch/23 inch racks of equipment that support hundreds of access interfaces), or they can be very small, mini-DSLAMs that support less than one hundred access interfaces.

7.8.13.3 DSL Repeaters

There may be situations where the distance between two ASLANs is too long to support a single DSL connection. In this scenario, a solution could be to use multiple DSL wire hops to bridge the link. While the total distance may be too great for a single DSL transmitter/receiver pair, cascading two separate DSL links may provide the solution. In this case, a DSL repeater could be used to amplify the DSL signal at a midpoint in the total link to provide enough amplification to

drive the signal over the total link length. The application of a DSL repeater to extend the signal distance is shown in Figure 7.8-10, DSL Repeater Provides Extended Distance.

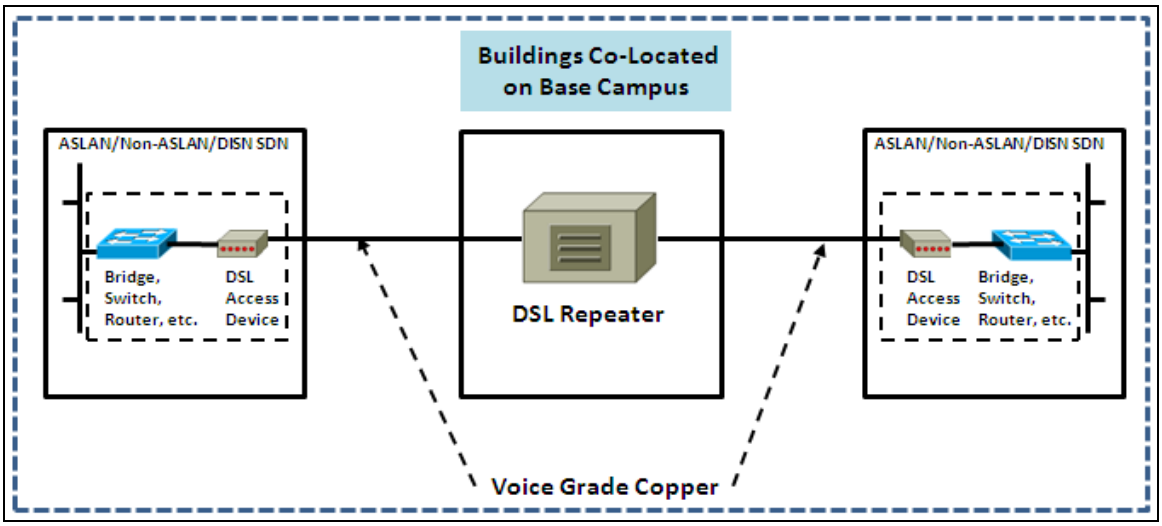

Figure 7.8-10. DSL Repeater Provides Extended Distance

Use of a DSL repeater provides extended distance/speed between DSL endpoints.

7.8.13.4 DSL Support for Analog Voice and Voice over IP (VoIP)

DSL Access Device, Concentrator, and Repeater products can also be used to carry both Analog Voice and VoIP services over existing voice-grade copper links. In this case, the Analog Voice is carried over the link using the pre-existing Analog Voice frequency band, and the VoIP is carried over the link using the separate frequency bands that the DSL products use for IP data service. A Base configuration supporting Analog Voice, IP Data, Voice over IP, and Video over IP with DSL Modems, a DSLAM, and a UC SC, is shown in Figure 7.8-11, Base Configuration Supporting Analog Voice and VoIP using DSL Modems and a DSLAM.

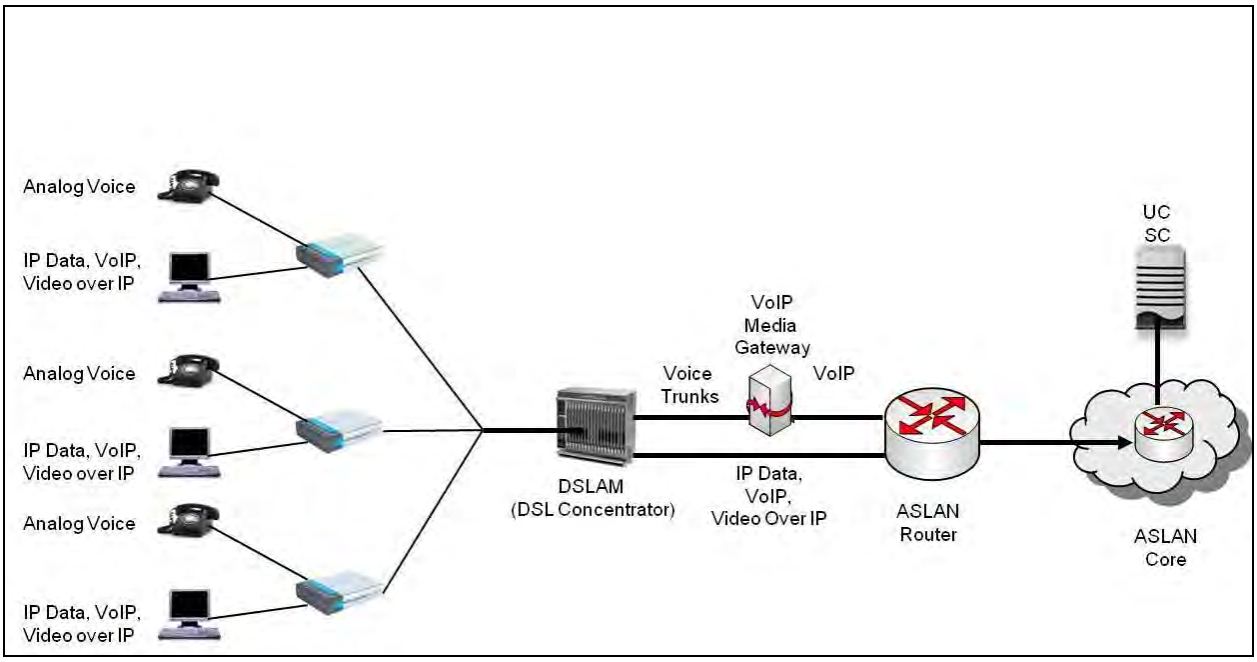

Figure 7.8-11. Base Configuration Supporting Analog Voice and VoIP Using DSL Modems and a DSLAM

In the above configuration, the Analog Voice, VoIP, and Video over IP Services are all provided by a UC SC and its associated VoIP Media Gateway on the Base. The Media Gateway provides conversion between Analog Voice service and UC VoIP service in this case. For VoIP and Video Over IP services, the DSLAM also needs to be interoperable with the ASLAN Router and the UC SC, based on the ASLAN Router requirements in this section and the SC requirements in Section 2.

On Bases that are not equipped with an SC and a Media Gateway, the Analog Voice service can be provided by an End Office or Private Branch Exchange (PBX) on the Base. When a UC SC and VoIP Media Gateway are located at the Base, the DSLAM and the MG can be interconnected using either individual analog lines (e.g., Unshielded Twisted Pairs) or by an Integrated Services Digital Network (ISDN) PRI, that multiplexes the analog lines onto one or more T1 facilities. In this case, the DSLAM also needs to be interoperable with the MG ISDN PRI requirements in Section 2, Session Control Products.

It is also possible for the DSLAM and the VoIP Media Gateway to be integrated into a single product. In this case, the DSLAM side of the product needs to meet the Concentrator requirements in this section, and the MG side of the product needs to meet the MG requirements in Section 2, Session Control Products. Support for integrated DSLAM/MG products is not required.

7.8.14 References

The following References were used in the DSL Requirements Section:

G.991.1 ITU-T Recommendation G.991.1, "High bit rate digital subscriber line (HDSL) transceivers," 1998.

G.991.2 ITU-T Recommendation G.991.2, "Single-pair high-speed digital subscriber line (SHDSL) transceivers," 1998.

G.992.1 ITU-T Recommendation G.992.1, "Asymmetric digital subscriber line (ADSL) transceivers," 1999.

G.992.2 ITU-T Recommendation G.992.2, "Splitterless asymmetric digital subscriber line (ADSL) transceivers," 1999.

G.992.3 ITU-T Recommendation G.992.3, "Asymmetric digital subscriber line transceivers 2 (ADSL2)," 2009.

G.992.4 ITU-T Recommendation G.992.4, "Splitterless asymmetric digital subscriber line transceivers 2 (splitterless ADSL2)," 2002.

G.992.5 ITU-T Recommendation G.992.5, "Asymmetric digital subscriber line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus)," 2009.

G.993.1 ITU-T Recommendation G.993.1, "Very high speed digital subscriber line transceivers (VDSL)," 2004.

G.993.2 ITU-T Recommendation G.993.2, "Very high speed digital subscriber line transceivers 2 (VDSL2)," 2006.

G.998.1 ITU-T Recommendation G.998.1, "ATM-based multi-pair bonding," 2005.

G.998.2 ITU-T Recommendation G.998.2, "Ethernet-based multi-pair bonding," 2005.

G.998.3 ITU-T Recommendation G.998.3, "Multi-pair bonding using time-division inverse multiplexing," 2005.

I.361 ITU-T Recommendation I.361, "B-ISDN ATM layer specification," 1999.

I.363.5 ITU-T Recommendation I.363.5, "B-ISDN ATM Adaptation Layer specification: Type 5 AAL," 1999.

RFC 1990 K. Sklower, B. Lloyd, et al, "The PPP Multilink Protocol (MP)," August 1996.

802.1D IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, June 2004.

802.1Q IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 2003.

802.3 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 26 December 2008.

802.3ab IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications: 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s), 1999.

802.3ah IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks, 2004.

802.3i IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbps (1.25 MB/s) over twisted pair, 1990.

802.3u IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbps (12.5 MB/s) w/auto-negotiation, 1995.

802.3z IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s), 1998.

7.9 REGIONAL ASLAN

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

SECTION 8
MULTIFUNCTION MOBILE DEVICES

The UCR section associated with UCF Sectoin 8 addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. A Multifunction Mobile Device (MMD) is an advanced, yet highly portable computing platform that supports one or more compact input interfaces (e.g., touch screens, stylus, miniature keyboard) to facilitate user interaction. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. An MMD can assume any number of form factors including, but not limited to, a Smartphone, Personal Digital Assistant (PDA), or small form factor wireless tablet. The requirements for unclassified non-Unified Capabilities (UC) Voice and Video over Internet Protocol (IP) (VVoIP)-related functionality (such as e-mail or Web browsing) provided by the MMDs are generally defined by the Defense Information Systems Agency (DISA) Field Security Office (FSO) Security Technical Implementation Guidelines (STIGs) and Security Requirements Guides (SRGs).

MMDs that have access to Department of Defense (DoD) networks also require support from appliances and systems located at protected DoD installations that provide application services, access control, and remote management. The implementation of these supporting services and infrastructures vary greatly from vendor to vendor; however, the Unified Capabilities Requirements (UCR) uses the generic term “Multifunction Mobile Devices Backend Support System,” or “MBSS,” to represent the appliances that allow MMDs connectivity and reachback to the enclave. As with MMDs themselves, non-UC-related functions of the MBSS (e.g., e-mail, Web browsing) are defined by the appropriate DISA FSO STIGs and SRGs. If the MBSS provides UC VVoIP functionality, this is addressed in UCR 2013, Section 8, Multifunction Mobile Devices. During DoD laboratory testing, the MMD and its associated MBSS are treated as a single System Under Test (SUT). Also, the Session Controller (SC) or Softswitch (SS), at a minimum, will also be included in the SUT if the MBSS provides UC VVoIP capabilities.

NOTE: Currently the UCR defines two primary multifunction mobile device-related product categories: the multifunction mobile device itself and the MMD backend supporting services. However, the UC Steering Group is reviewing proposals to add new product categories or refine these categories to include Mobile Device Manager (MDM), MMD Operational Support System (MOSS), Mobile Application Store (MAS), and other components related to MMDs. The outcome of this decision may result in changes to the current MMD section of this UCF.

Table 8-1, Multifunction Mobile Devices, summarizes the MMD category of the DoD UC Approved Products List (APL).

Table 8-1. Multifunction Mobile Devices

PRODUCT	ROLE AND FUNCTION
MMDs	Advanced mobile computing platform that provides wireless connectivity, basic telephony functions, and portable computing capabilities. The device may also provide UC VVoIP-related services
MBSS	An appliance or collection of appliances that allows remotely connected MMDs to access services within a DoD enclave and provides access control and remote management while maintaining or enhancing the network's security posture NOTE: See previous note concerning possible changes to this product category pending decision by the UC Steering Group.

8.1 USE CASES FOR MULTIFUNCTION MOBILE DEVICES

In the context of the UCR, the scenarios in which MMDs may be used for UNCLASSIFIED applications are currently grouped into three primary use cases, as shown in Table 8.1-1, Multifunction Mobile Device Use Cases.

Table 8.1-1. Multifunction Mobile Device Use Cases

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	No Connectivity to DoD Network and No Processing of CUI Data Use Case. No connectivity to DoD e-mail.	MMD that has no connectivity to a DoD network and processes only publicly available DoD data information (Data as defined in this context is clarified in the next section).
#2	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case. No Connectivity to DoD UC Services.	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks. Securely processes and stores DoD information at the CUI level. This MMD does not interace with any DoD UC Services.
#3	Full Connectivity to DoD Network and Processing fo Sensitive UNCLASSIFIED Information Use Case. Full Connectivity to DoD UC Services.	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks. Securely processes and stores DoD information at the CUI level. This MMD has full connectivity to DoD UC Services.

Figure 8.1-1, Illustration of Multifunction Mobile Device Use Cases, illustrates the relationship between the primary MMD use cases. The illustration for Use Case #1 shows an MMD with access to only a commercial network and publicly available information. For this scenario, external supporting infrastructure, as shown in the figure, may not, in all cases, be needed or used. The illustration for Use Case #2 depicts the connection of an MMD through a Defense Information Systems Network (DISN) Internet Access Point (IAP) or other DISN gateway to reach DISN services or a homed DoD Component Enclave. Also, the supporting infrastructure in Use Case #2 may, in some cases, be located at the entry point to the DISN instead of at the DoD Component Enclave. Use Case #3 resembles Use Case #2, but involves connectivity to DoD UC services in addition to connectivity to DoD enterprise networks. In Use Case #1, Use Case #2,

and Use Case #3, the MMDs are expected to be Government-furnished devices, whereby an authorized administrator issues and administers the devices on behalf of the user.

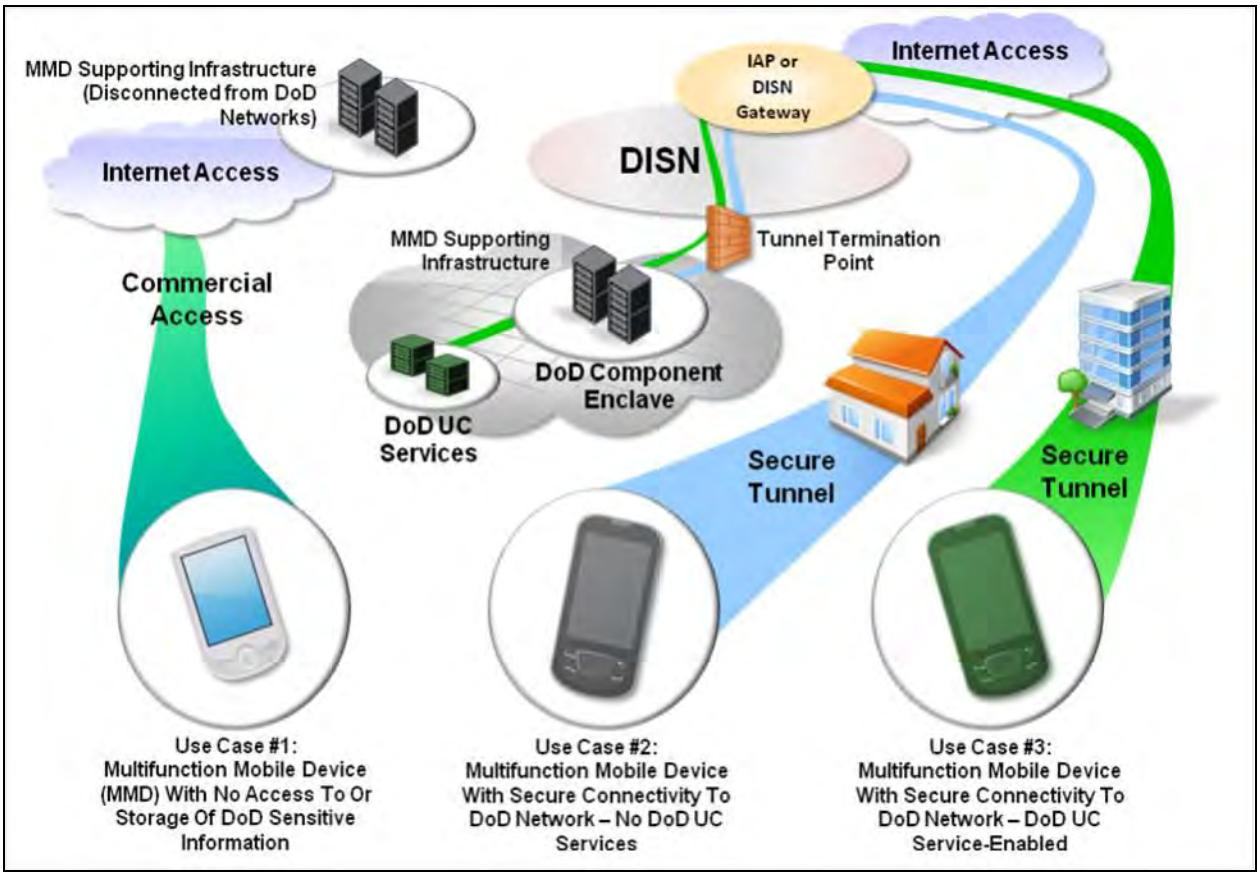

Figure 8.1-1. Illustration of Multifunction Mobile Device Use Cases

At the time of this document's writing, the devices provided for use in all three use cases are expected to be Government furnished. However, even though DoD policy does not currently permit the use of the "Bring Your Own Device" (BYOD) model, various DoD Components are actively examing the use of this approach in conjunction with virtualization, secure boot, and other device hardening techniques. Future developments in mobility dvice security and policy could eventually permit the use of the BYOD approach by DoD Components.

For maximum worldwide interoperability, it is recommended (not required) that these devices support Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS), at a minimum; generally, however, these devices will support connectivity to the Public Switched Telephone Network (PSTN) and data networks through a wide range of wireless technologies to include 2G, 3G, 4G, Wireless Local Area Network (WLAN), and personal area networking. The following sections describe the use cases in greater detail.

8.1.1 Use Case #1: No DoD Network Access or CUI Processing (Non Enterprise Activated)

While many DoD users of MMDs require the ability to connect to DoD networks and process Controlled Unclassified Information (CUI), pilot efforts within the DoD have determined that a number of scenarios exist in which access to sensitive DoD networks and information is not required. Though completely disconnected from sensitive DoD networks and data information, these MMDs still delivered critical capabilities that facilitated the fulfillment of a DoD component's mission. Examples of the capabilities provided by these types of devices might include the use of MMDs to distribute publicly releasable training materials, flight maps, briefings, or meteorological data.

MMDs supporting this use case can be used to conduct official DoD business; however, devices conforming to this use case are barred from processing, storing, transmitting, or receiving any persistent information (i.e., data or files that are stored or captured on the device) other than that which is publicly releasable and fully UNCLASSIFIED. In this context, persistent information would include, but would not be limited to, e-mail, files, calendar information, Short Message Service (SMS) messages (and similar), and Web-browsing traffic. Sensitive information of a real-time nature that is non-persistent, such as voice and video communications, would not be considered data in this context since such information is stored on the device only in a temporary manner. However, if Use Case #1 devices are used to support sensitive real-time communications, such use must be in accordance with DoD policy including DoD Directive (DoDD) 8100.02. Caution must be exercised when communicating with other DoD entities using devices meeting only the minimum set of requirements specific to Use Case #1 given that such communications would consist of information requiring protection from disclosure.

Use Case #1 devices cannot connect to DoD networks. Network access, if enabled, would generally occur through a commercial network service provider. Connectivity to DoD networks for this use case, even if indirectly through DoD network-connected PCs, is expressly prohibited. In addition, connectivity to and use of commercial voice networks must occur only in accordance with existing DoD policies.

As a result of these DoD network connectivity and processing restrictions, this type of MMD does not have to meet the same rigorous Information Assurance requirements levied on products that connect to DoD networks and process sensitive data information. However, use of these devices by DoD components will still be subject to approval by the DoD Component Designated Approving Authority (DAA).

The DoD Component DAA may also permit the installation of commercial applications on the device to support voice, video, Web browsing, Global Positioning System (GPS), Wi-Fi, and other services. However, DoD e-mail functionality is not permitted for use by MMDs conforming only to Use Case #1 applicable requirements. Technical controls are required to be enforced that allow DoD administrators to control the applications that are permitted for installation on the MMD. Also, if remote management servers are used for the purpose of remote

administration, these supporting infrastructure servers are not permitted to have connectivity to any operational DoD networks. Management of MMDs for this use case is further discussed in Section 8.2, Backend Support Systems Supporting Multifunction Mobile Devices.

8.1.2 Use Case #2: Full DoD Network Connectivity Use Case – No Access to DoD UC Services

Mobile devices conforming to Use Case #2 are permitted to connect to DoD networks, transmit and receive sensitive information, and securely store the received information. However, these devices do not have connectivity to DoD UC Services. The device may connect to the DoD network in a number of ways, including direct access through a wired or WLAN connection or indirect access by establishing a secure overlay across a carrier connection or via a DoD-connected PC. To secure data in transit and storage of data at rest, use of National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) approved cryptographic modules is required. In addition, all the components that compose this system are required to be fully complient from an Information Assureance standpoint based on the approved STIG(s) resulting from the FSO SRG-to-STIG vendor process using the appropriate Mobile SRG(s) and/or STIG(s) directly developed by the FSO.

Requirements for the Use Case #2 MMD platform itself are specified by the DISA FSO SRGs. Conformance of the MMD platform to DISA FSO requirements is validated during testing by the appropriate DoD laboratory or in the field in accordance with the UC Connection Office (UCCO) Process Guide and DoD Instruction (DoDI) 8100.04.

For this scenario, note that certain requirements are applicable to not only the MMD itself, but also the supporting infrastructure responsible for remote monitoring, remote management, and provisioning of the device from a centralized enforcement point. The next section discusses the role that the Backend Support System plays in supporting the MMD's secure reachback into the DoD Component enclave.

8.1.3 Use Case #3: Full DoD Network Connectivity Use Case with Access to DoD UC Services

Mobile devices conforming to Use Case #3 follow the same connectivity model defined for Use Case #2. These devices connect to DoD networks, transmit and receive sensitive information, and securely store the received information. However, in addition to conforming to all Use Case #2 requirements, these devices connect to DoD UC Services. For example, devices following into this use case may support a wide range of Internet Protocol (IP)-enabled applications including VVoIP or XMPP-enabled collaboration services. This UCR defines a "Unified Capabilities (UC) Multifunction Mobile Device Application" (UC Multifunction Mobile Device App) as an application, or series of applications, operating on an MMD that minimally provides VVoIP or XMPP-based collaboration functionality comparable to an End Instrument (EI) or Assured Services End Instrument (AEI) (or collaboration client). However, unlike a typical EI or

AEI, the UC MMD Application operates within the confines of a DISA FSO STIG-compliant MMD host platform.

This UCR specifies the functionality necessary for UC MMD Applications to connect securely to UC VVoIP and XMPP-based systems within DoD enclaves. Other applications may operate on the platform as well to support e-mail, calendar, Web browsing, SMS, and other services. However, the requirements for these additional services are defined in DISA FSO publications. Figure 8.1-2, UC Multifunction Mobile Device Application Relationship to the Host Platform, shows the relationships among a UC MMD Application, other non-UC VVoIP-related applications, and the MMD platform.

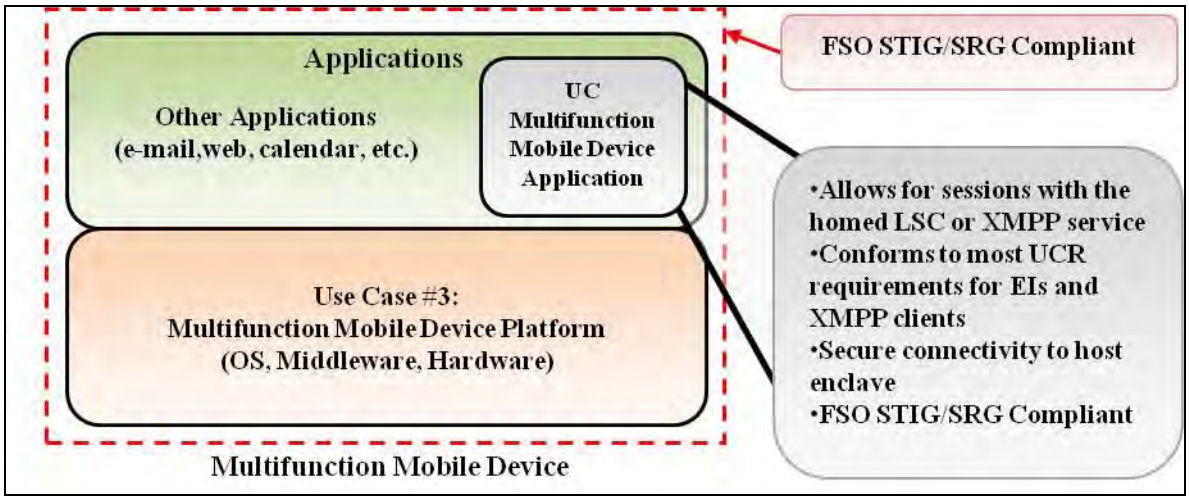

Figure 8.1-2. UC Multifunction Mobile Device Application Relationship to the Host Platform

Even though a UC MMD Application provides functionality similar to a standard EI or AEI, there are some important differences. Primarily, a UC MMD Application will typically leverage untrusted networks to reach its homed DoD enclave. For example, the MMD platform may connect to an untrusted commercial network at Open System Interconnect (OSI) Layers 2 and 3 but then use a secure mechanism at OSI Layer 3, Layer 4, or higher to reach its homed enclave in a secure manner. Also, because public networks in many cases do not provide Quality of Service (QoS) and availability guarantees, calls made using a UC MMD Application may not have availability comparable to calls originating and terminating within the Assured Service UC VVoIP network. Finally, other applications operating on the same platform as the UC MMD Application could provide any number of e-mail, GPS, Bluetooth, Web browsing, Instant Messaging (IM), SMS, and other applications and services. These additional services must not weaken the security posture of the UC MMD Application when it connects to UC services.

The addition of UC MMD Applications to the operating environment not only provides the opportunity for enhanced mobility and connectivity for UC VVoIP network services, but also requires the implementation of additional safeguards to maintain the network's security posture.

Unlike an EI or AEI, which has nearly direct network layer connectivity to its homed SC, a UC MMD Application is permitted to connect to only its homed SC in one of two ways:

1. Establish an encrypted VVoIP signaling and media traffic session with a Back-to-Back User Agent (B2BUA), providing functionality similar to a Session Border Controller (SBC), at the edge of the homed enclave. This B2BUA communicates on behalf of the UC MMD Application to the homed SC using the SC's native, vendor-defined, line-side protocol or UC Session Initiation Protocol (SIP). Secure connectivity with this B2BUA is generally expected to occur at OSI Layer 4 or above.
2. Establish a Virtual Private Network (VPN) tunnel to a VPN server located within the home enclave's Demilitarized Zone (DMZ). The VPN server extracts the VVoIP signaling from the VPN tunnel and transmits the information to the homed SC.

   NOTE: The VPN in this context does not necessarily denote IP Security (IPSec) since a wide range of tunneling mechanisms could be used at various OSI layers to support secure connectivity while maintaining optimal performance. If necessary, a translation step can occur at the VPN server if the information received or transmitted via the VPN tunnel is not already compatible with the SC's vendor-defined line-side protocol or UC SIP.

Regardless of whether a VPN or B2BUA (or both) is used to securely terminate connections from UC MMD Applications at the edge of the enclave, the MBSS is responsible for terminating the secure connection from the UC MMD Application and providing remote management functions.

Figure 8.1-3, Options for Secure SC Connectivity From a UC Multifunction Mobile Device Application, and Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, illustrate the possible connectivity options. For simplicity, required additional security elements such as firewalls and Intrusion Detection Systems (IDSs) are omitted from these figures.

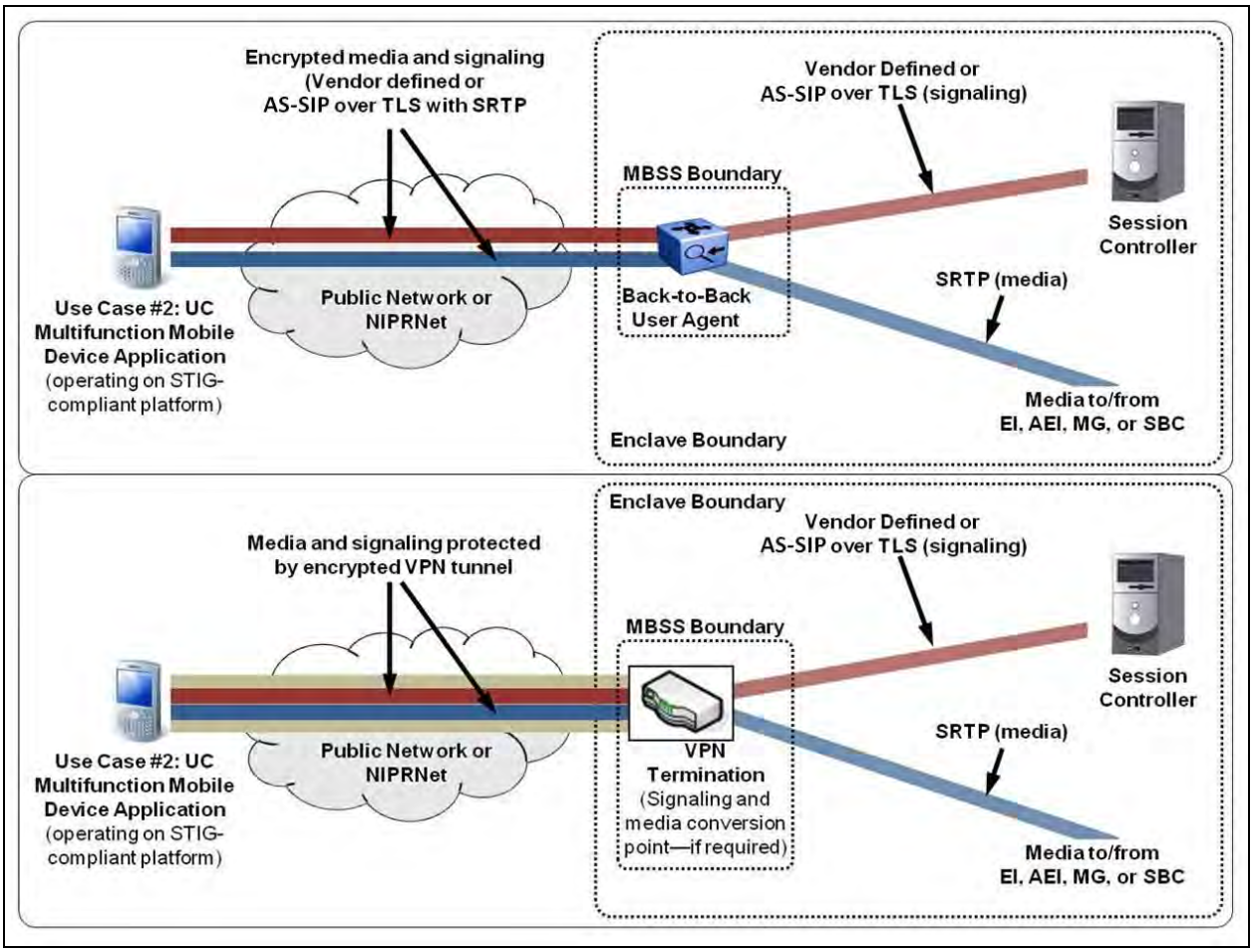

Figure 8.1-3. Options (VPN and B2BUA) for Secure SC Connectivity From a UC Multifunction Mobile Device Application

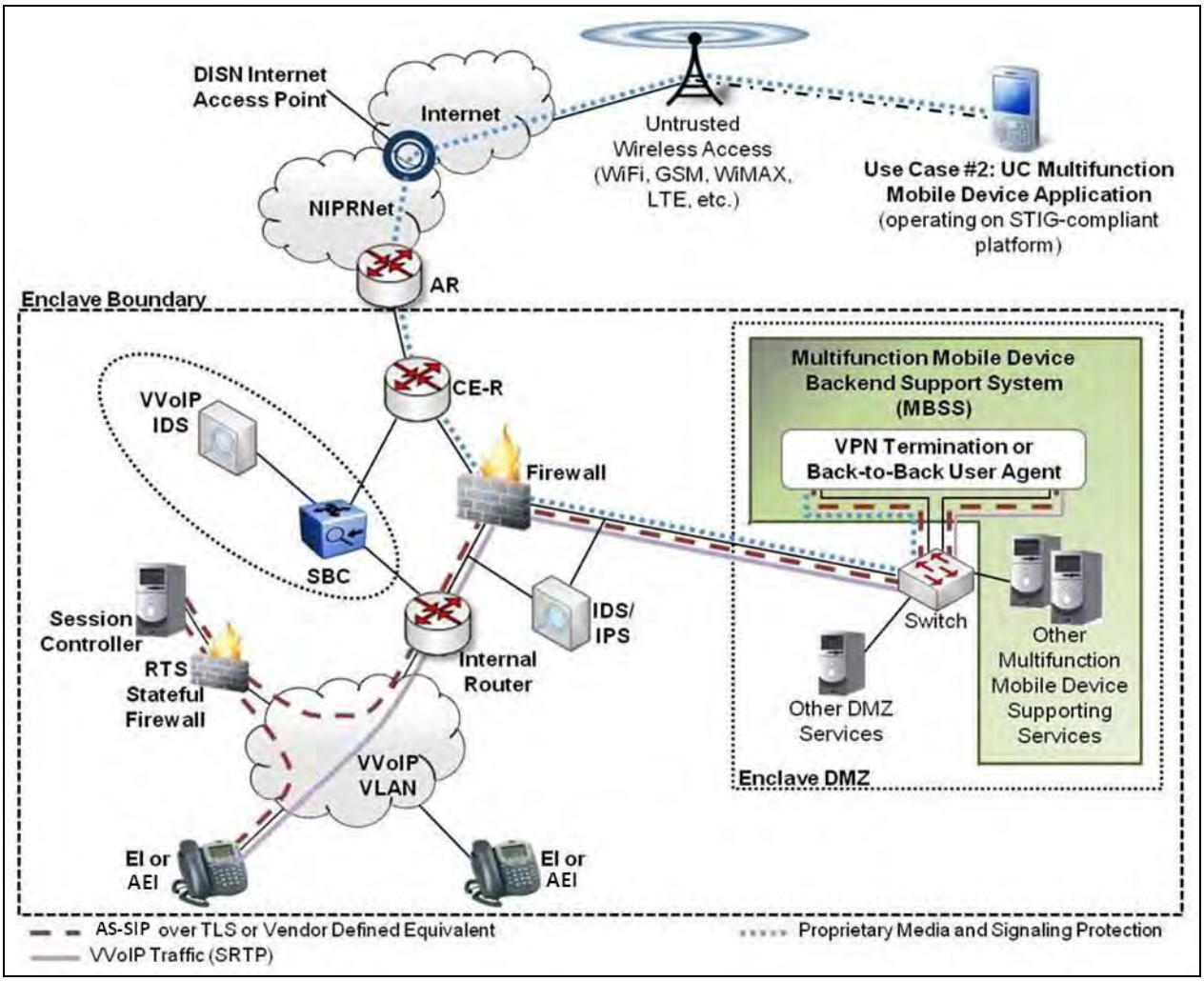

Figure 8.1-4. UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection

From an interoperability standpoint, it is anticipated that UC MMD Application vendors will not field directly compatible solutions. However, because the UC MMD Application relies on its homed SC for session establishment, the SC will serve as the basis for interoperability between other UC SIP devices on the UC network as well as other devices served by the line-side protocol of the SC. As a result, the UC MMD Application and the MBSS are considered to be a part of the SC during testing at an approved DoD laboratory. The UC MMD Application, the STIG/SRG-compliant platform, the MBSS, and the SC are tested together as a complete SUT.

Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, provides a more detailed view of how session establishment would occur between a UC MMD Application and a wired EI located within the enclave. Figure 8.1-4 shows a sample DMZ created using a triple-homed firewall; however, other DMZ designs exist using multiple firewalls and could just as easily be implemented to provide secure connectivity for the UC

MMD Application users. (Refer to the latest revision of the Network Infrastructure STIG for information on acceptable DMZ designs.)

Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, illustrates the placement of the MBSS within the enclave's DMZ. However, if the system provides B2BUA with dynamic port pinhole functionality similar to that of an SBC, sites may prefer to place the B2BUA in-line with the SBC and data firewall rather than behind the data firewall. For simplicity, this option is not shown in the figure and can be implemented only if done in accordance with (IAW) DISA FSO STIGs and accredited by the site DAA. In addition, the MBSS must provide a VVoIP IDS capability similar to that required of SBCs for VVoIP signaling and for media that traverses the enclave boundary. Existing IDSs can be reused, provided that VVoIP inspection functionality is supported and a dedicated MBSS IDS is not required.

Figure 8.1-4 also shows a call between a UC MMD Application and an EI or AEI. However, the call could just as easily have been routed between the UC MMD Application and an SBC or the Media Gateway (MG), depending on the call source and/or destination. Regardless, the traffic must be in a UC VVoIP-compliant format upon entry into the network. In other words, the VVoIP signaling and media must be protected IAW the requirements in UCR 2013, Section 4, Information Assurance as well as STIGs/SRGs, and the packets must have appropriate Differentiated Services Code Point (DSCP) markings consistent with the requirements in UCR 2013, Section 6, Network Infrastructure End-to-End Performance. Since the platform on which the UC MMD Application resides will likely support other applications besides voice, appropriate marking of the UC MMD Application packets becomes even more important.

The Other Multifunction Mobile Device Supporting Services symbol in the figure represents the services, including authentication of remote devices and checks related to the security posture of the device that must accompany these solutions. These services also may support other non-VVoIP related applications such as e-mail, Web browsing, and IM, as appropriate. In addition, even though the figures show the MBSS VVoIP functionality as being logically separate from the SC, some vendors may choose to implement certain functions within the SC rather than as a service provided by an external device (e.g., providing management for served UC MMD Applications and AEIs and EIs from a central location).

8.2 BACKEND SUPPORT SYSTEMS SUPPORTING MULTIFUNCTION MOBILE DEVICES

In the context of the UCR, the MBSS is a system that supports remote administration, monitoring, and secure enclave access for MMDs. For Use Case #1, the MBSS (if used) supports centralized management of MMDs via commercial networks and is not connected to DoD networks. For Use Cases #2 and #3, the MBSS is located on the DoD network and plays a key role in ensuring DoD policy enforcement and in providing secure DoD enclave access for users of MMDs. The MBSS also facilitates the use of only approved applications and services through the use of granular technical controls and centralized management consoles. The MBSS can take

many forms and is highly vendor dependent; however, some of the common functions and features provided by the MBSS include remote data wipe functionality and remote patch remediation.

SECTION 9
VIDEO DISTRIBUTION SYSTEM

9.1 OVERVIEW

The Unified Capabilities (UC) Framework document serves the purpose of design guide and is a complement to the Unified Capabilities Requirements (UCR), which states the specifications that need to be met in order for products to pass the Joint Interoperability Test Command's (JITC's) Approved Products List (APL) certification.

This section addresses Video Distribution System (VDS) specifications and design guidelines. VDS is a compliment of audio and video equipment designed for interfacing, switching/bridging, and distributing digital and/or analog audio, video and picture signals sourced from multiple devices and destined to multiple devices. Unlike a video teleconferencing (VTC) Multipoint Conferencing Unit (MCU), which performs solely many to one audio and video signal bridging, the VDS can perform many to one, one to many and many to many bridging of audio, video and pictures and can distribute signal feeds to geographically dispersed locations and may include Extended Display Identification Data, which is a data structure that provides additional information and intelligence about the feed (e.g., signal feed coordinates, Predator target, etc.).

VDS architectures are composed of subsystems that include the following:

1. VDS Distribution Devices (One to Many). Includes systems that receive signals sourced from one device which are then repeated to multiple destination devices or video displays.
2. VDS Switching Devices (Many to One). Includes systems that receive signals sourced from multiple devices which are then repeated to one destination device or video display. Sources are connected to a common central device that can actively select (switch) between any one of the sourced signals.
3. VDS Matrix Switching Devices (Many to Many). Includes systems that receive signals sourced from multiple devices which are then repeated to multiple destination devices or video displays. Sources are connected to a common central matrix device that can actively select (switch) from any source device(s) to one or multiple destination devices simultaneously without compromising signal quality.
4. VDS Peripherals. Normally devices that enable users to interact with the VDS system. They include the following:
    a. Source Devices. Computer Workstations, Laptop Computers, Video Playback Devices (DVD, BlueRay, Media-Players), Cable Television Tuners and Live Video Camera Feeds.
    b. Destination Devices. Desktop Monitors, Television Monitors, Video Projectors, Video Signal Processors, Video Recording Devices, and Video Wall Signal Processor Systems.

5. VDS Peripheral Connectors. These are modular standard components which provide different options for interfacing VDS peripheral devices; they include HD-SDI, DVI, VGA, HDMI, and Component HD.
6. VDS Peripheral Connector Conversion Devices. These are devices that convert between different types of peripheral connector standards (e.g., HDMI to VGA).
7. VDS Cabling. Includes common copper and optical cabling for passing the electrical signals that enable audio and video, from source devices to destination devices.
8. Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC). These are devices that convert a digital (usually binary) code to an analog signal (current, voltage, or electric charge) and vice versa.

9.2 GENERAL VDS SYSTEM RECOMMENDATIONS

General VDS configuration Recommendations apply to all VDS devices in both the Closed VDS system configuration as described in this section and VDS over Internet protocol (IP) configurations as described in Section 9.3.

9.2.1 IP Recommendations for VDS Systems

If the VDS system is inaccessible from Department of Defense (DoD) IP-routed networks, then the VDS system is considered a "Closed VDS System" and support of the IPv4 profile as defined in Section 7.2.1.5, and of the IPv6 profile as described in Section 5, is optional. Otherwise, if the VDS systems connect to IP-routed networks, then the VDS system is considered a "VDS over IP System" and must support the IPv4 profile as defined in Section 7.2.1.5 and the IPv6 profile as described in Section 5.

9.2.2 VDS Signal Extenders Recommendations

VDS source and destination devices may be physically separated by long geographical distances that exceed the maximum specifications of the original audio and video signal format. In these scenarios, VDS system can utilize signal extenders to convert or condition the original signal for transmission over longer cabling distances.

9.2.3 VDS Peripheral Guidelines

VDS Peripherals fall into one of two categories:

1. Source Devices. These are signal generators which output video, audio and other waveforms that are used in the communication, synchronization of VDS subcomponents. Examples include: Computer Workstations, Laptop Computers, Video Playback Devices (DVD, BlueRay, Media-Players), Cable Television Tuners, and Live Video Camera Feeds.

2. Destination Devices. These are signal receivers which input video, audio and other waveforms that are used in the communication, synchronization of VDS subcomponents and provide the necessary feedback that enables VDS. Examples include: Desktop Monitors, Television Monitors, Video Projectors, Video Signal Processors, Video Recording Devices, and Video Wall Signal Processor Systems.

9.2.4 VDS Peripheral Connectors Guidelines

VDS peripheral connectors are modular components which provide different options for interfacing audio and video interface formats and VDS subcomponents.

9.2.5 VDS Peripheral Connector Conversion Devices

VDS Peripheral Connector Conversion (VPCC) devices are system appliances that operate and provide gateway like capabilities and allow for different types of VDS subcomponents to interoperate by coupling unlike peripherals.

9.2.6 VDS Matrix Switch Guidelines

VDS systems connect via a VDS Matrix Switch, which is a device capable of accepting multiple inputs from source devices and selectively distributing any one of these inputs to one or many destination devices.

9.2.7 VDS IA Security Recommendations

VDS components must adhere to the appropriate STIGs, Ports, Protocols, and Services Management (PPSM) guidelines to achieve compliance for all information systems, applications, and services connected to the Global Information Grid (GIG). VDS systems must also meet all appropriate Information Assurance and Vulnerability Assessment (IAVA) and National Institute of Standards and Technology (NIST)/National Information Assurance Partnership (NIAP) standards.

9.2.8 VDS Availability Recommendations

Availability refers to the ability for the users to access the system, ensuring a prearranged level of operational performance, during a pre-determined contractual measurement period. Generally, the term downtime is used to refer to periods when a system is unavailable.

It is recommended for VDS equipment to operate 24x7 with the exception of scheduled maintenance.

9.2.9 VDS Capacity Recommendations

All VDS audio/visual (A/V) solutions must allow the user to add inputs independently of adding outputs. Similarly, the VDS solution must allow end users to add outputs independently of inputs.

NOTE: This flexibility provides system expansion to add additional sources (inputs) as mission Recommendations increase, without the addition of more outputs, thus reducing the cost of system expansion and providing a matrix which can support a system with more inputs than outputs or more outputs than inputs.

The VDS switch matrix should allow for a non-squared expansion capability on inputs and outputs by installing additional plug-in input cards, output cards, matrix cards, small form factor pluggable modules, and power supplies without disrupting existing signal paths. Best practices indicate that expansion in a non-squared (addition of sources/destination (X-Inputs/Y-Outputs)) affords the user the most economical approach to VDS switch matrix expansion thus lowering total life cycle costs.

9.2.10 VDS Diagnostics Recommendations

System diagnostics verify and validate proper system operation and system status information.

9.3 CLOSED VDS SYSTEM DESIGN GUIDELINES

By definition, Closed VDS systems do not interface with the DISN core. A Closed VDS System is considered to be a traditional VDS that enables video distribution over a Time Division Multiplexing (TDM)-based network and can from time to time support IP capabilities in a closed environment. Closed VDS systems leverages legacy standards and traditional TDM VDS. By definition, the UCR stipulates that Closed VDS systems are inaccessible from DoD IP routed networks.

A Closed VDS System is considered to be a traditional VDS that enables SMPTE signals to be transmitted over a digital infrastructure. In the context of the UCR and the UCF, a Closed VDS System enables video distribution over non IP-based networks, but can from time to time support IP capabilities in a closed environment. Closed VDS systems can leverage legacy standards and by definition, the UCR stipulates that Closed VDS Systems are inaccessible from DoD IP-routed networks. It is important to note however, that a Closed VDS system may use a peripheral device to extract video from an IP transport and covert it to a SMTP digital data stream, and passed through the VDS.

9.4 VDS OVER IP (VDS-IP) DESIGN GUIDELINES

By definition, VDS Over IP systems interface with the DISN core. Figure 9.4-1 depicts how a traditional VDS system becomes a VDS over IP (VDS-IP) system. A VDS-IP is an extension of

traditional VDS that enables added features such as enhanced compression procedures that allow for very low latency distribution over an IP transport. VDS-IP leverages standards based Moving Picture Compression Algorithm (MPCA) and/or Picture Compression Algorithm (PCA) to enable performance driven features and advantages over traditional TDM VDS. This approach allows for VDS-IP systems to extend and reach across networking infrastructures where TDM based and Closed VDS systems have physical and architectural limitations. By definition, the UCR stipulates that VDS-IP systems are accessible from and interface with DoD IP routed networks.

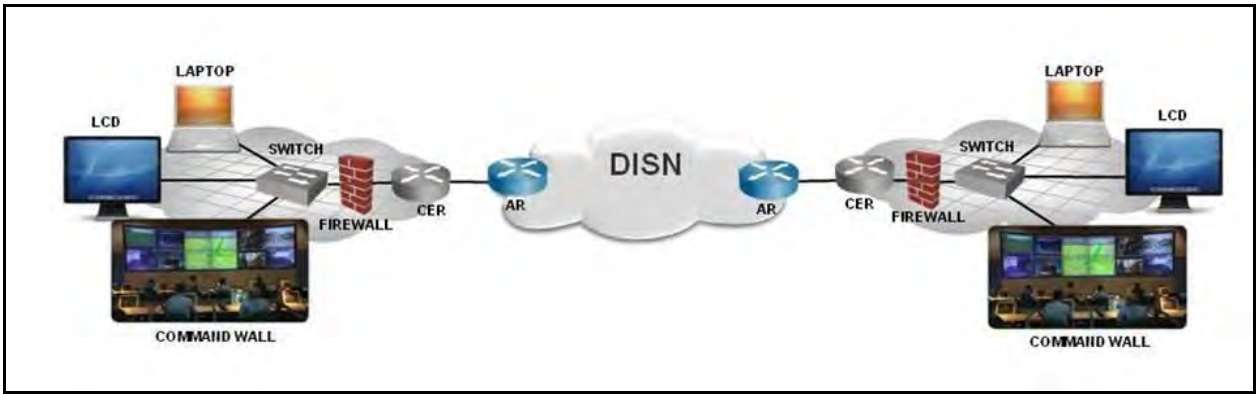

Figure 9.4-1. VDS Over IP System

9.5 VDS RECORDING GUIDELINES

VDS recording relates to the capturing and archiving of video and audio, analog or digital signals that are stored for later retrieval in optical disc recording technologies (e.g., DVD, CDs) Magnetic Storage (e.g., Hard drives), Flash Memory (e.g., Memory Cards, USB Flash Drives, Solid State Drives) or Magnetic tape (e.g., Video Tape, Compact Cassette).

VDS Recording Devices fall into one of two categories:

- Video Tape Recording (VTR). Is a device that captures and archives video and/or audio material on a magnetic tape (e.g., Video Tape, Compact Cassette).
- Digital Video Recorder (DVR). Is a device or application software that captures and archives video and/or audio in a digital format to a disk drive, USB flash drive, SD memory card, or other local or networked mass storage device.

SECTION 10
NETWORK INFRASTRUCTURE PRODUCTS

This section provides an overview of current Defense Information Systems Network (DISN) Services, networks, and products used in the network infrastructure. DISN services include transport, data, voice, video, messaging, and other Unified Capabilities (UC) along with ancillary enterprise services, such as directories. The DISN services also provides less apparent but critical support services, such as timing and synchronization (T&S), Source Address (SA) of the network, address assignment services, and domain name services.

Currently, DISN uses a composite of separate networks to provide customers with transport, data, voice, and video services as well as the means to satisfy their classified and Sensitive but Unclassified (SBU) requirements. These networks and their relationship to each other and to the DISN service are shown in Figure 10-1, Current DISN Services and Networks Overview.

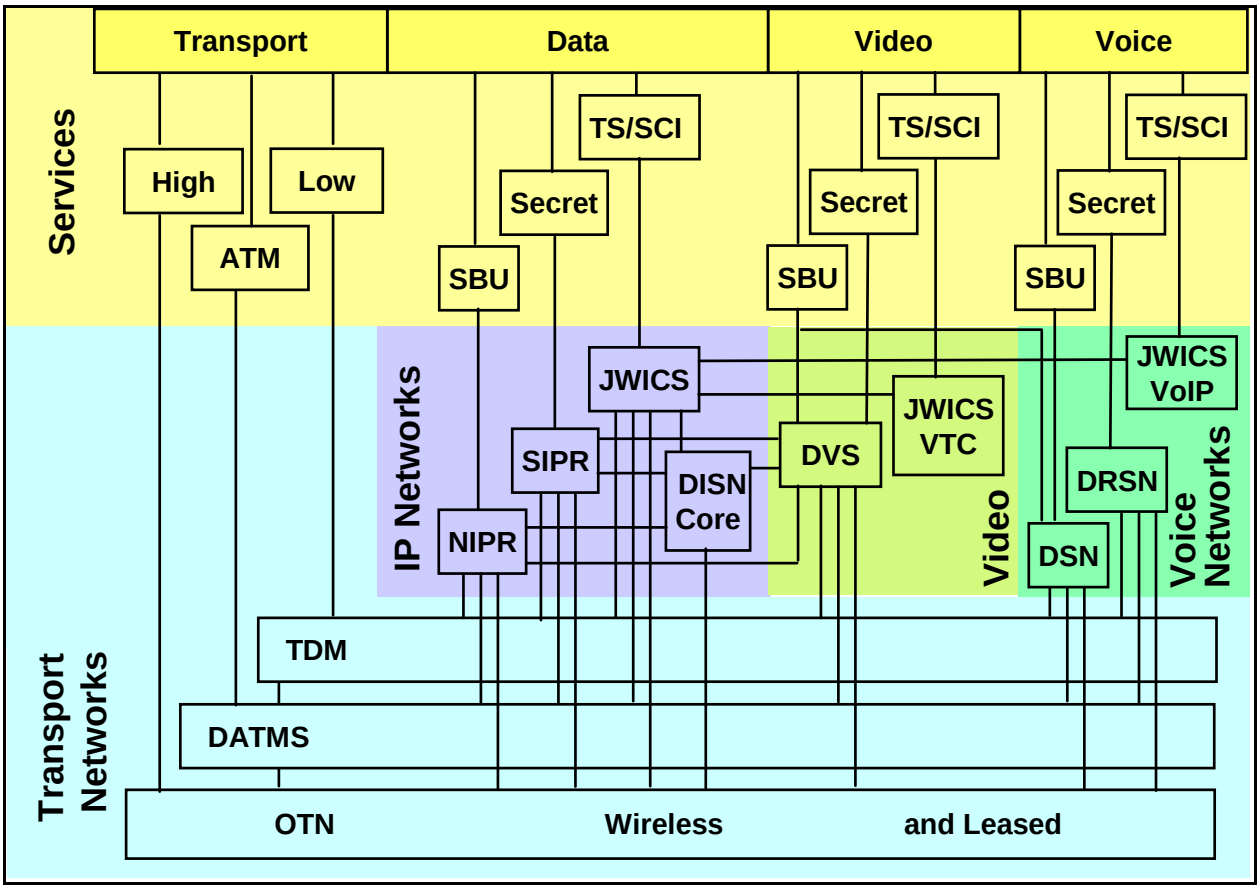

Figure 10-1. Current DISN Services and Networks Overview

Products employed within the network infrastructure include Optical Transport System (OTS), Optical Digital Cross-Connect (ODXC), Multi-Service Provisioning Platform (MSPP), M13 Multiplexer (M13 MUX), Serial Time Division Multiplexing (TDM) Multiplexer (Serial TDM MUX), T&S Product, DISN Router, and Passive Optical Networks (PONs). Products within this

section may be certified and Approved Products List (APL) listed for one product category (e.g., OTS) or a combined product category called a Network Infrastructure Product (NISP):

- OTS. Multiplexes optical signals from various sources (e.g., router, transport switch function, Channel Access Grooming) at the optical core layer. The OTS consists of the following components: Terminal, Reconfigurable Optical Add and Drop Multiplexer (ROADM), and an Optical Line Amplifier (OLA). An Optical Supervisory Channel (OSC) runs between these components.
- Transport Switch Function (TSF). Today, the TSF functionality is satisfied by the ODXC equipment within the DISN. The TSF is an Optical cross-connect device that is located primarily at Class 1 sites but it could also be deployed at select Class 2 sites. The lowest level that it will cross-connect is an STS-1.
- Aggregation Grooming Function (AGF). Receives low-speed circuits on multiple ingress ports and multiplexes them together onto higher speed egress interfaces. The AGF multiplexing allows for multiple internal cross-connects between the low-speed ports and the high-speed ports. The AGF product can connect circuits from any port to any other port within the bandwidth limitations of the ports. The AGF product within the DISN is also known as an MSPP.
- Network Infrastructure Product (NISP). UCR 2013, Section 10, defines three products: an OTS product, a TSF product, and an AGF product. The product category of NISP represents the combination of two or more network infrastructure products within the same platform. The System Under Test (SUT) is certified to perform as a NISP product by performing the functions completely of any combination of the following products: OTS, TSF or AGF.
- ODXC. Input optical signals are converted into electronic signals after they are demultiplexed by demultiplexers. The electronic signals are then switched by an electronic switch module. Finally, the switched electronic signals are converted back into optical signals by using them to modulate lasers and then the resulting optical signals are multiplexed by optical multiplexers onto outlet optical fibers.
- MSPP. Close to the customer, must interface with a variety of customer premises equipment and handle a range of physical interfaces. Most vendors support telephony interfaces (DS-1, DS-3, E1, E3), optical interfaces (OC-3, OC-12, OC-48, STM-1, STM-3, STM12), and Ethernet interfaces (10/100Mb). MSPPs enable service providers to offer customers new bundled services at the transport, switching, and routing layers of the network, and they dramatically decrease the time it takes to provision new services while improving the flexibility of adding, migrating or removing customer networks.
- M13 Multiplexer (M13 MUX). Integrates 28 T1 tributary channels into a single 45 Mbps data stream using bit-level multiplexing and M13 bit-interleaving framing format. M13 terminal multiplexers also provide T1 channel grooming and offer direct connection to T3 networks or DS3 equipment over copper or fiber links.

- Serial TDM Multiplexer (Serial TDM MUX). Supports TDM, asynchronous transfer mode (ATM), serial, and cell-based data types, and securely converts them for Internet protocol (IP) transport at gigabyte speeds. Serial TDM Multiplexers are required to ensure Mission critical legacy data can be smoothly transitioned to the GIG. Multiple timing recovery options, based on telecom standards should be enforced to ensure that the data that enters the IP cloud, exits in the proper order and precedence.
- Timing and Synchronization (T&S). The complexities of an analog and digital multi-standard, multi-format data transports require flexibility in customizing the synchronizing needs of the network. Signals from a master sync pulse generator (SPG) are critical in order to synchronize all of the equipment in a system.
- DISN Routers. Routers required for the DISN fall into categories of small, medium, and large. Each of these routers may support a variety of interface types and numbers. The size of the routers is indicative of certain characteristics such as backplane capacity and packet forwarding capability, but the overall functionality of the router does more to place the router than any one attribute, and is determined by the sponsor.
- PON. Point-to-multipoint, fiber to the premises network architecture in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises, typically 16-128. A PON consists of an optical line terminal (OLT) at the service provider's central office and a number of optical network units (ONUs) near end users. A PON configuration reduces the amount of fiber and central office equipment required compared with point-to-point architectures. A passive optical network is a form of fiber-optic access network. Downstream signals are broadcast to all premises sharing a single fiber (encryption is used to prevent eavesdropping). Upstream signals are combined using a multiple access protocol, usually time division multiple access (TDMA).

The product placement of the equipment described above as members of the Network Infrastructure Design and Products class are depicted in Figure 10-2, Network Infrastructure Product Arrangements.

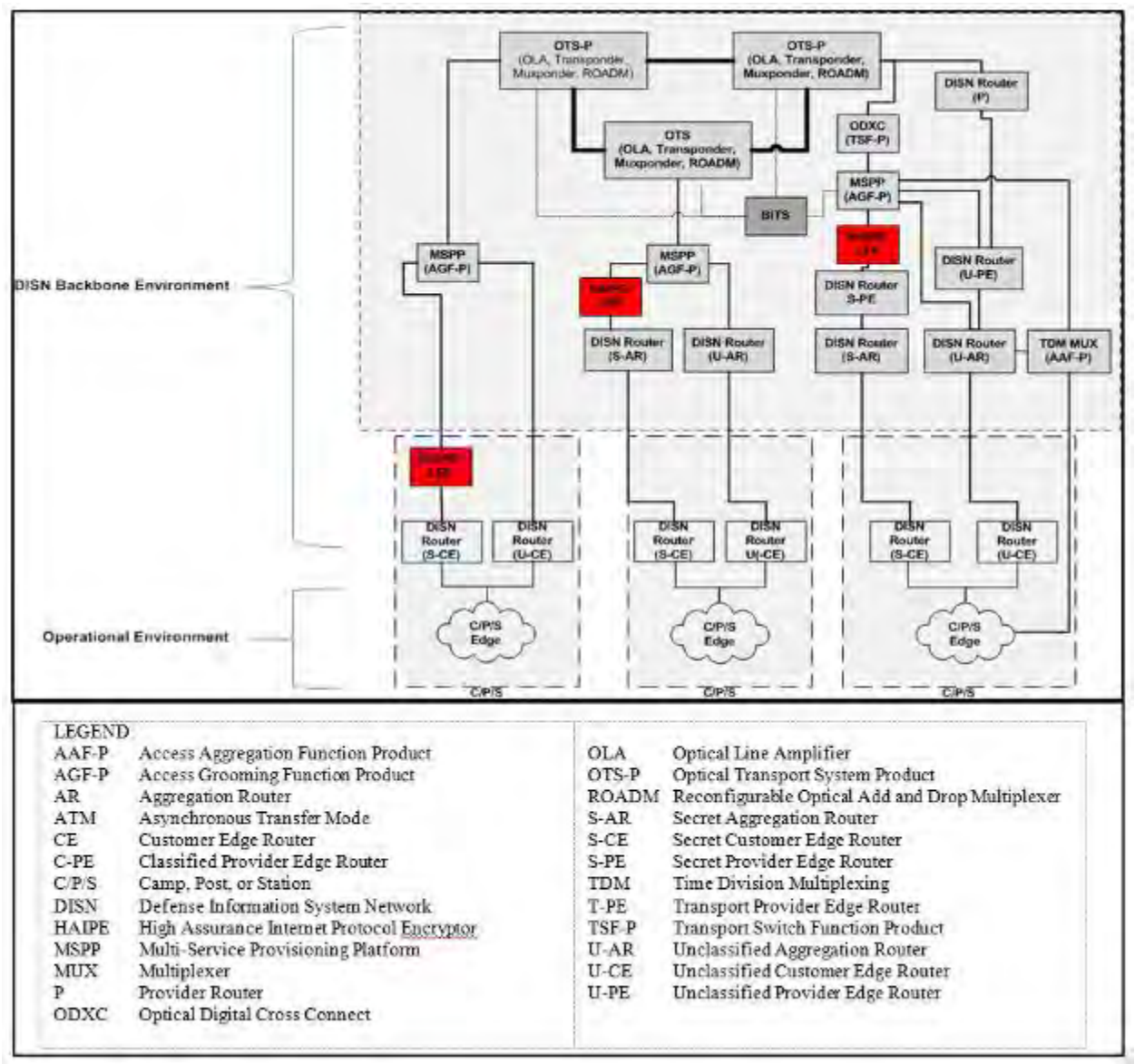

Figure 10-2. Network Infrastructure Product Arrangements

Figure 10-3, Conceptual Depiction of 2 Nodes of the DISN illustrates the DISN router hierarchy from a Transport Boundary perspective. This will allow for a better understanding of NISP product placement relative to the DISN architecture (no circuit cross-connects shown). Predominantly, the products OTS, ODXC, MSPP, m13 MUX, Serial TDM MUX, Building Integrated Timing Supply (BITS), and DISN Routers are currently located above the DISN Distribution Layer Boundary, extending to the DISN IP Core; while PONs predominantly exist at the Base/Camp/Post/Station (B/C/P/S) Layer (Note that the products defined within this section can be deployed within the DISN or B/C/P/S infrastructure).

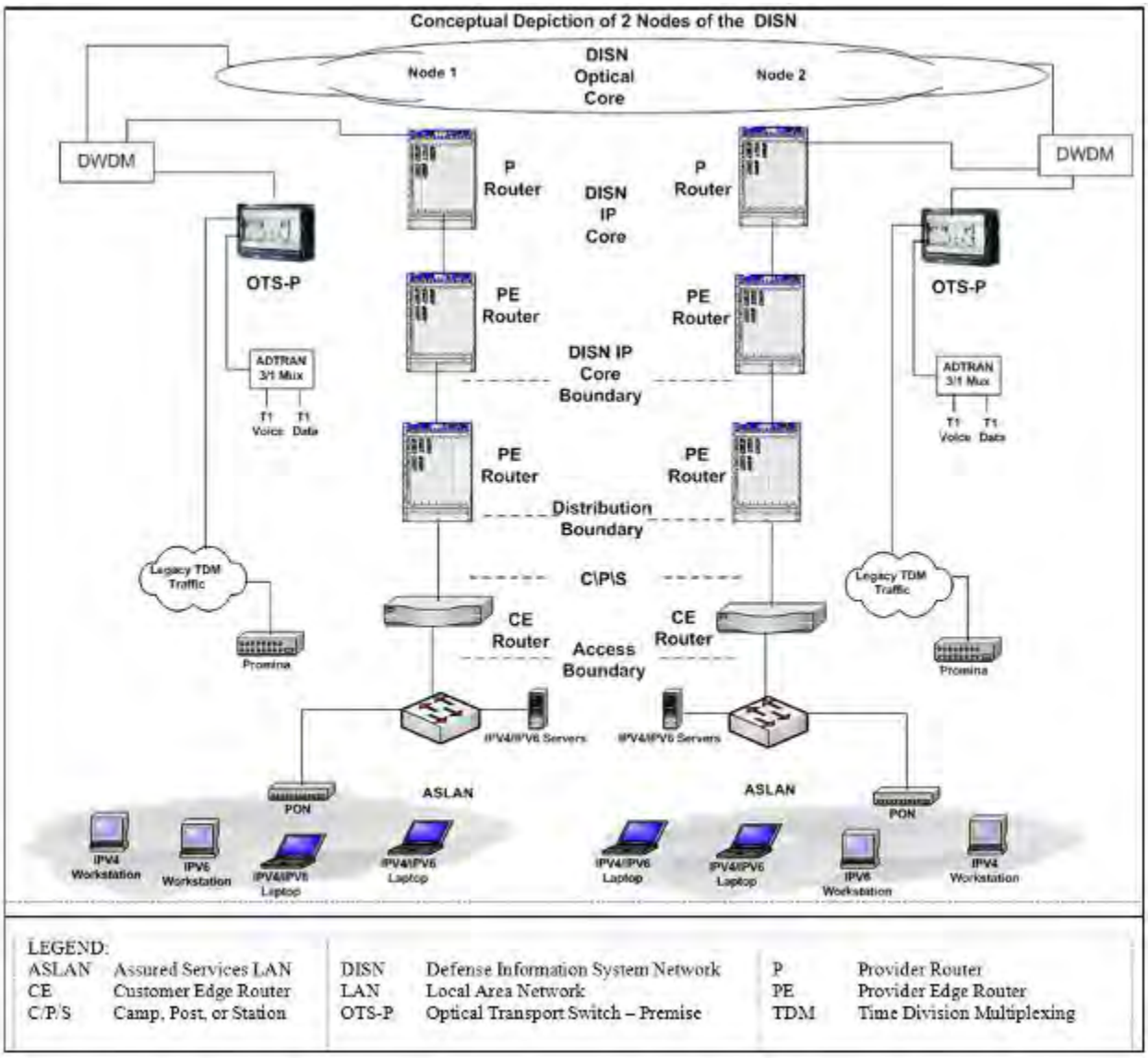

Figure 10-3. Conceptual Depiction of 2 Nodes of the DISN

Figure 10-4, DISN Router Hierarchy, illustrates the current DISN router hierarchy for both the unclassified network and the classified network. At this point, the NIPRNet and SIPRNet Routers have been transformed to be Unclassified Aggregation Routers (ARs) (U-ARs) and classified ARs connected to the unclassified Provider Edge (U-PE) Routers and classified Provider Edge (C-PE) Routers, respectively.

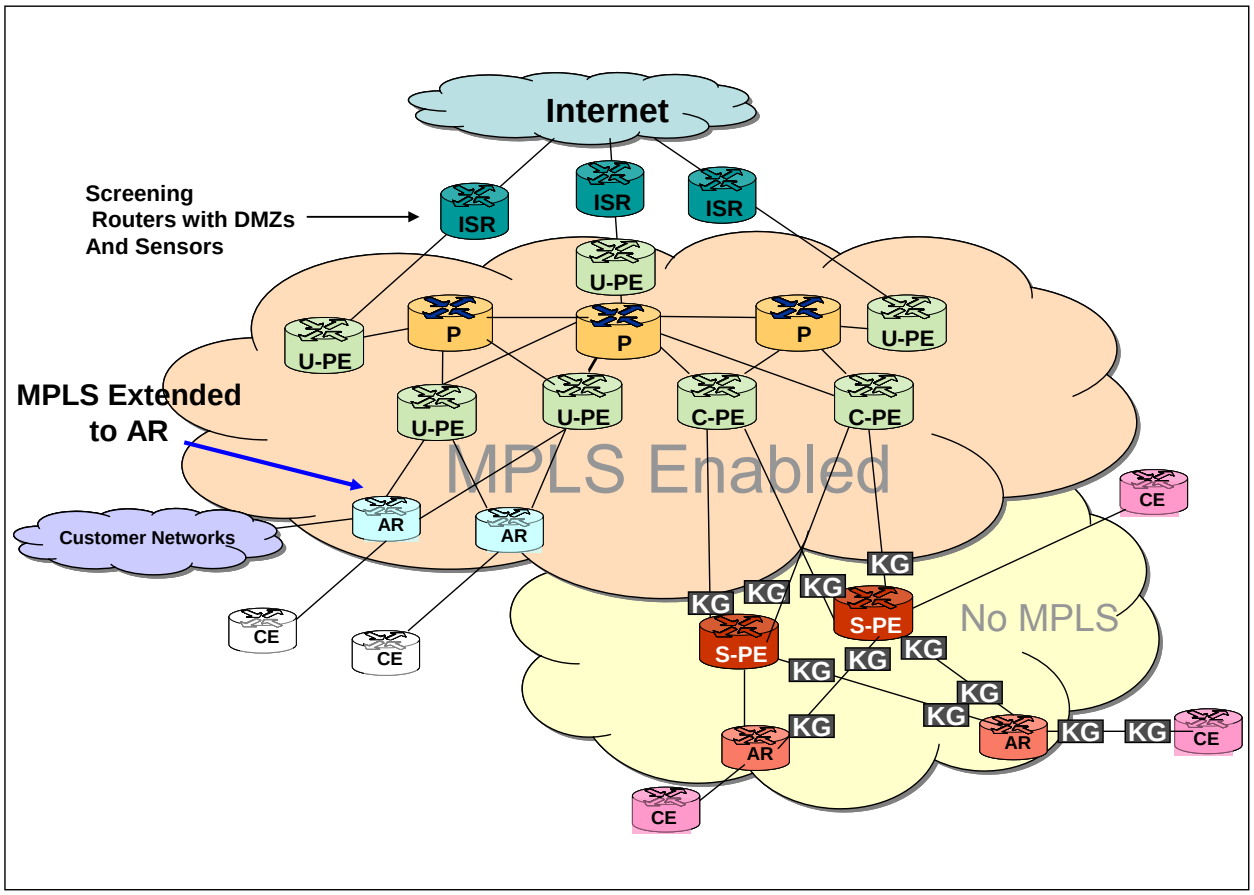

Figure 10-4. DISN Router Hierarchy

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

2013 – Mid Term DISN Architecture. In 2013, the MSPPs and Multiprotocol Label Switching (MPLS) will provide Layer 1/Layer 2 transport capabilities. Within DISN Class1A Sites, NIPRNet and SIPRNet will have disappeared as distinct entities. Legacy TDM (if any) will be supported on the MSPP. Edge applications (Defense Switched Network [DSN], Defense RED

Switch Network [DRSN], and DISN Video Services [DVS]) will primarily use IP as a transport means. The DISN Converged Access (DCA) architecture with the added use of Serial to IP (STI) devices will permit ATM and Promina/Integrated Digital Network Exchange (IDNX) to be removed from the DISN.

10.1 DISN CONVERGED ACCESS

This new transport access architecture is called the DISN Converged Access (DCA). The DCA architecture uses IP/MPLS with CoS (traffic shaping, policing and prioritization) to provide deterministic transport of customer requirements. RSVP-TE will be used to create label-switched paths (LSPs) and MPLS fast re-route will be used to quickly switch traffic to a back-up path in the event of a network failure. DCA equipment will support a single data stream that contains a variety of cypher text and unencrypted unclassified traffic. The DCA architecture goal is to replace native ATM at the edge, and accept circuit emulation traffic containing TDM and serial traffic. It will support ATM elimination for multiple traffic types, including native ATM cell traffic, IP traffic including NIPRNET, SIPRNet and Private IP traffic and layer 1 circuit traffic. For unencrypted IP traffic, DCA equipment shall support interworking of customer interfaces from ATM, T1/E1, DS3/E3 and Packet over SONET, to Ethernet in support of an Ethernet-based DISN infrastructure.

Transport for layer 2 traffic (ATM and Ethernet) as well as unencrypted IP traffic will be provided by L2 pseudowires (PW). In the case of layer 2 traffic, the layer 2 datagram (Ethernet frame or ATM cell) will be encapsulated in MPLS for transport at the ingress and will be delivered to the customer in the format received. When the destination interface is ATM, DCA will support aggregation of customer traffic using ATM VPI/VCIs. In the case of unencrypted IP traffic, the IP datagram will be encapsulated for transport. When the destination interface is Ethernet, DCA will provide aggregation of customer traffic using 802.1Q VLAN tags. DCA will have port density to support new services required, achieved via IEEE 802.1Q L2 VLAN aggregation of Ethernet interfaces to within the core infrastructure. This will enable use of only one port for multiple VLANs with ATM, Ethernet cards.

DCA equipment will use L1 circuit emulation when the DCA devices cannot detect IP packets in the bit stream, either because the interface is inherently not IP (Low-Speed Time Division Multiplexing [LSTDM], PBX to MFSS legacy voice circuit) or when the bit stream is encrypted.

DCA will be configurable to either recognize the Differentiated Services Code Point (DSCP) and prioritize traffic in accordance with the UCR, or ignore customer DSCPs. Layer 1circuit emulation traffic will be treated as Expedited Forwarding (EF) traffic to minimize delay.

Layer 2 (L2) PWs are an MPLS transport capability (RFC 3985, 5462) that encapsulates ATM, Ethernet (C2, SIPR, and NIPR traffic), but does no L3 routing or VPN. Layer 2 VPN support is needed to support the evolution of DISN access from point-to-point access circuits to multipoint access LANs, potentially improving reliability of IP services and utilization of access infrastructure.

Traffic policing and marking will be used for layer-2 PWs at the customer interface. Traffic that is within the requested bandwidth will be queued differently than traffic that exceeds the requested bandwidth. This excess traffic can either be dropped at ingress (at the customer interface) or marked as 'drop eligible' so that it will be dropped before other traffic that does comply to agreements. The architecture for DCA access networks will be engineered to support "in contract" traffic under certain failure conditions. Edge switches are often dual homed to larger switches at the edge or at the core sites.

Customers may encrypt their traffic before handing to DCA (this is transparent to the DCA, which emulates a L2 switch) using CoS with proper queuing and interface policing, DCA can allow customer IP traffic to burst into otherwise unused bandwidth.

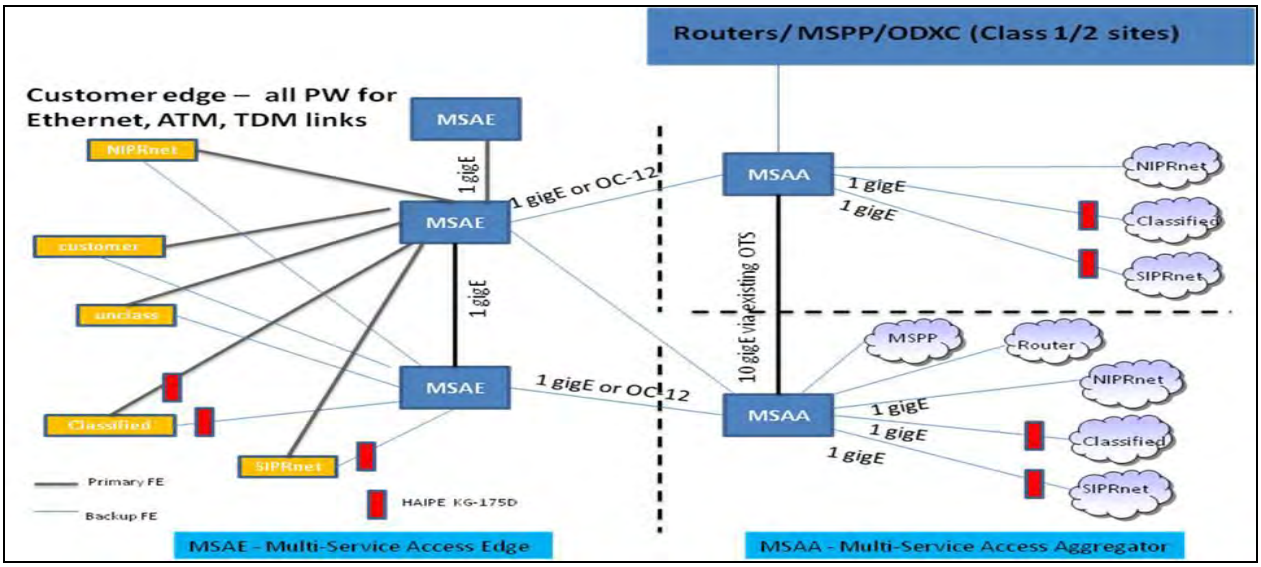

Figure 10-5. DCA Architecture

MSAA devices will be at the CORE Class 1 and 2 locations and they will have a larger node requirement that could support up to 10Gig of bandwidth for aggregation to DISN service nodes and inter DCA connectivity for redundancy purposes. MSAA can also connect to ODXC via SONET. DCA physical interfaces will comply with UCR 2013 section 10.6.1.1 through 10.6.1.3. The equipment redundancy requirements for DCA are compliant with 10.6.14.

SECTION 11
NETWORK ELEMENTS

A Network Element (NE) is any component of a network through which the Defense Switched Network (DSN) bearer and signaling traffic transits. This may include either Time Division Multiplexing (TDM) or Internet protocol (IP) bearer and signaling traffic or both. The transport between NEs may be TDM, IP, or Direct Line of Sight (DLoS). For IP transport, the IP connection may transit a Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), or Wide Area Network (WAN) dependent on its deployment. It can interconnect Session Controller (SC), Multifunction Softswitch (MFSS), and Softswitch (SS) Voice and Video over IP (VVoIP) bearer and signaling traffic as well as transport all other IP traffic.

NEs using DLoS transport have no intervening bridge, relay, or switch device between the actual transport devices. An NE using DLoS transport may be comprised of a single transmitter or receiver device, or operate with a separate receiver and transmitter elements, but still operate on the whole as a single NE. Additionally, the NE using DLoS transport may have redundant transmitters or receivers to increase reliability and to meet other stated requirements. The NEs may include multiplexers, routers, Channel Servicing Unit/Data Servicing Units (CSU/DSUs), compression devices, circuit emulation, channel banks, and/or any network device that could have an effect on the performance of the associated network traffic. For DLoS transport, this would include technologies such as Free Space Optics, millimeter wave, or other radio frequency (RF) formats, proprietary or standards-based, such as IP-based protocols (e.g., the 802.11 and 802.16 series). However, an NE having an IP interface and using a DLoS transport composed of 802.11 and/or 802.16 series standards shall instead meet the requirements for a Wireless Access Bridge in Unified Capabilities Requirements (UCR) 2013, Section 7, Network Edge Infrastructure.

In terms of network arrangements, the DLoS can be used for direct Point-to-Point (P2P) Link, Point-to-MultiPoint (P2MP) Link, and/or Mesh/Semi-Mesh (M/SM) Link arrangement. A P2P Link consists of two connection endpoints with no intervening connection endpoints in between. A P2MP Link is a specific type of multipoint link providing network traffic multiple paths from a single location to multiple locations. Such a link consists of a central connection endpoint that is connected to multiple peripheral connection endpoints. Any transmission of data that originates from the central connection endpoint can be received by all of the peripheral connection endpoints, also known as multicast like, while any transmission of data that originates from any of the peripheral connection endpoints is received only by the central connection endpoint. An M/SM network arrangement implies a peer-to-peer type relationship between two or more multiple connection endpoints.

Given the three link architectures defined previously, the NEs may operate in three defined architectural configurations: P2P, P2MP, and M/SM. In P2P architecture, the two NEs have a single connection and traffic flow association; thus, the two NEs operate as a matched set only. The ingress traffic to the NE is the egress traffic of the other, and vice versa.

The P2MP and M/SM architectures behave somewhat the same; thus, they can be referred to as Point-to-Network (P2N) for NEs. In a P2N configuration, this is not the case. The P2N architecture defines all the physical route connections between the various NEs composing the P2N. The P2N Association Path (AP) defines what ingress traffic types and bandwidth amount are routed via a specific NE's route path within that P2N architecture. The ingress traffic to one of the NEs in the P2N AP may fully or partially egress one or more of the other NEs. However, the aggregate egress from all NEs in the P2N architecture must be identical to the aggregate ingress of all of the NEs in the same P2N architecture. However, if operating in a P2MP mode that is applying multicast from a central NE to the peripheral NEs, then the aggregate of the additional multicast traffic must be accounted for in the egress sum total.

A P2N architecture can be a star, full-mesh, semi-mesh, or other architecture configuration. Since P2N architectures can result in multiple serial NE hops from where the associated ingress and egress traffic enters and exits the P2N architecture, the Special Interoperability Test Certification Report will state the maximum latency for a P2N AP. This maximum AP latency will be the limiting design criteria for establishing the P2N deployment architecture.

Figure 11-1, Network Element Diagram, shows the typical P2P architecture where an NE can operate as a standalone device or integrated into the transmission interfaces of switches or other network devices. The same stand-alone or integrated capability also applies to NEs in a P2N architecture approach wherein the only difference in Figure 11-1 is that there are three or more NEs connected to the "Transport Bandwidth" interoperating. Network Elements could be anything and everything in the route or path that connects DSN switches, non-DSN switches, and/or IP devices not categorized elsewhere in this document (e.g., multiplexers, routers, CSU/DSUs, D-channel compression devices, and/or trunk encryption). The use of NEs shall not provide the means to bypass the DSN as the first choice for all switched voice and dial-up video telecommunications between Department of Defense (DoD) user locations.

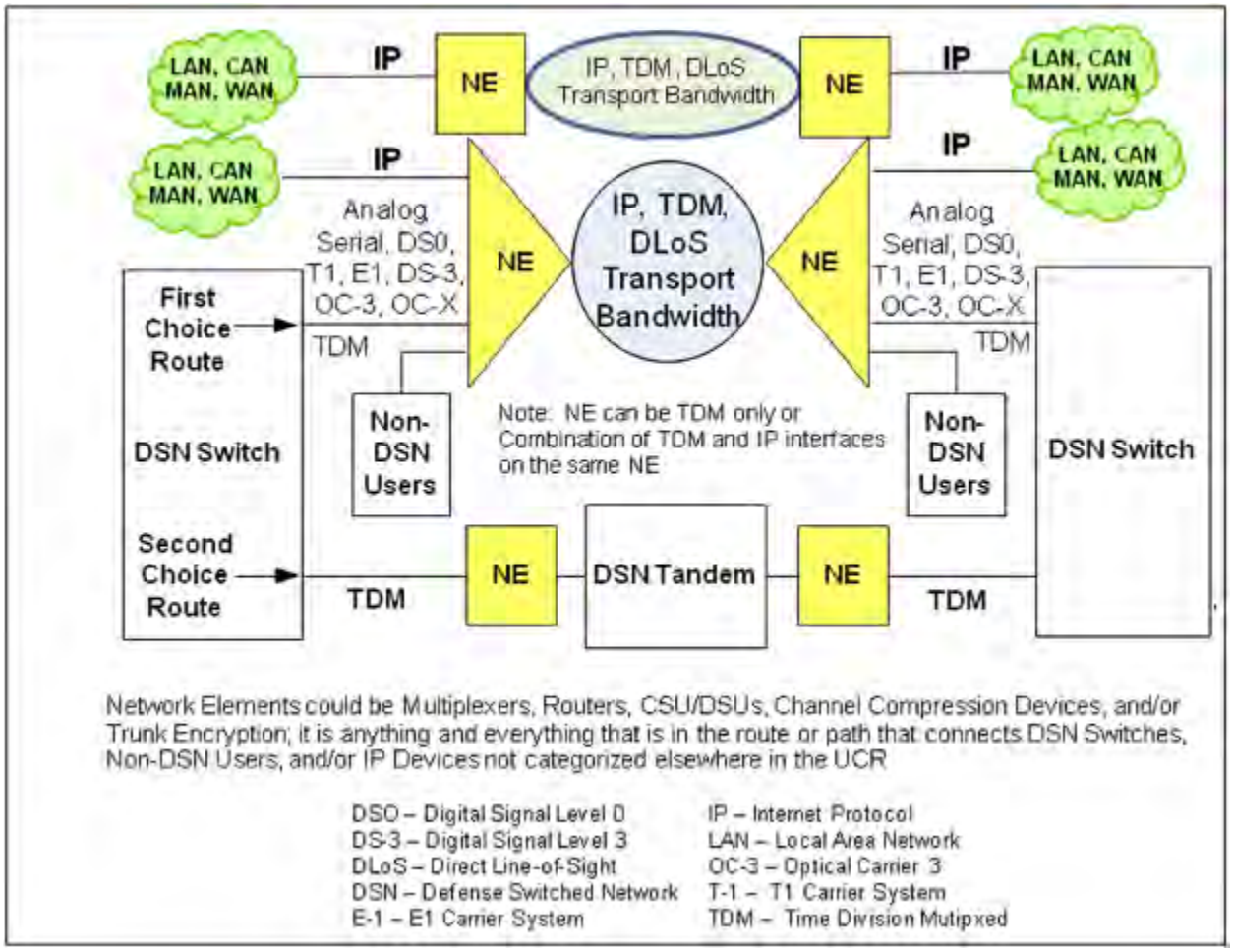

Figure 11-1. Network Element Diagram

SECTION 12
GENERIC SECURITY DEVICES

12.1 INTRODUCTION

Interoperability and supportability needs are addressed in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). CJCSI 6212.01E establishes policies and procedures for developing, coordinating, reviewing, and approving interoperability and supportability needs, as well as certifying that those needs have been met. This section of the Unified Capabilities (UC) Framework provides a product overview of End Cryptographic Units (ECUs) encryption products (e.g., High Assurance Internet Protocol Encryptor [HAIPE], Secure Communications Interoperability Protocol [SCIP] Device, and Link Encryptor Family [LEF]) and a framework of the interoperability testing of these products.

12.2 SECURITY PRODUCTS OVERVIEW

12.2.1 HAIPE

ECUs are components of information systems that provide security services, which may include confidentiality, identification and authentication, integrity, and non-repudiation, to the overall system. Typically, the ECU is integrated with other components to provide the overall security required for the system. As such, neither the ECU nor the encryption function provided is a standalone system. Figure 12.2-1, Sample Network, illustrates the use of the ECU in a system.

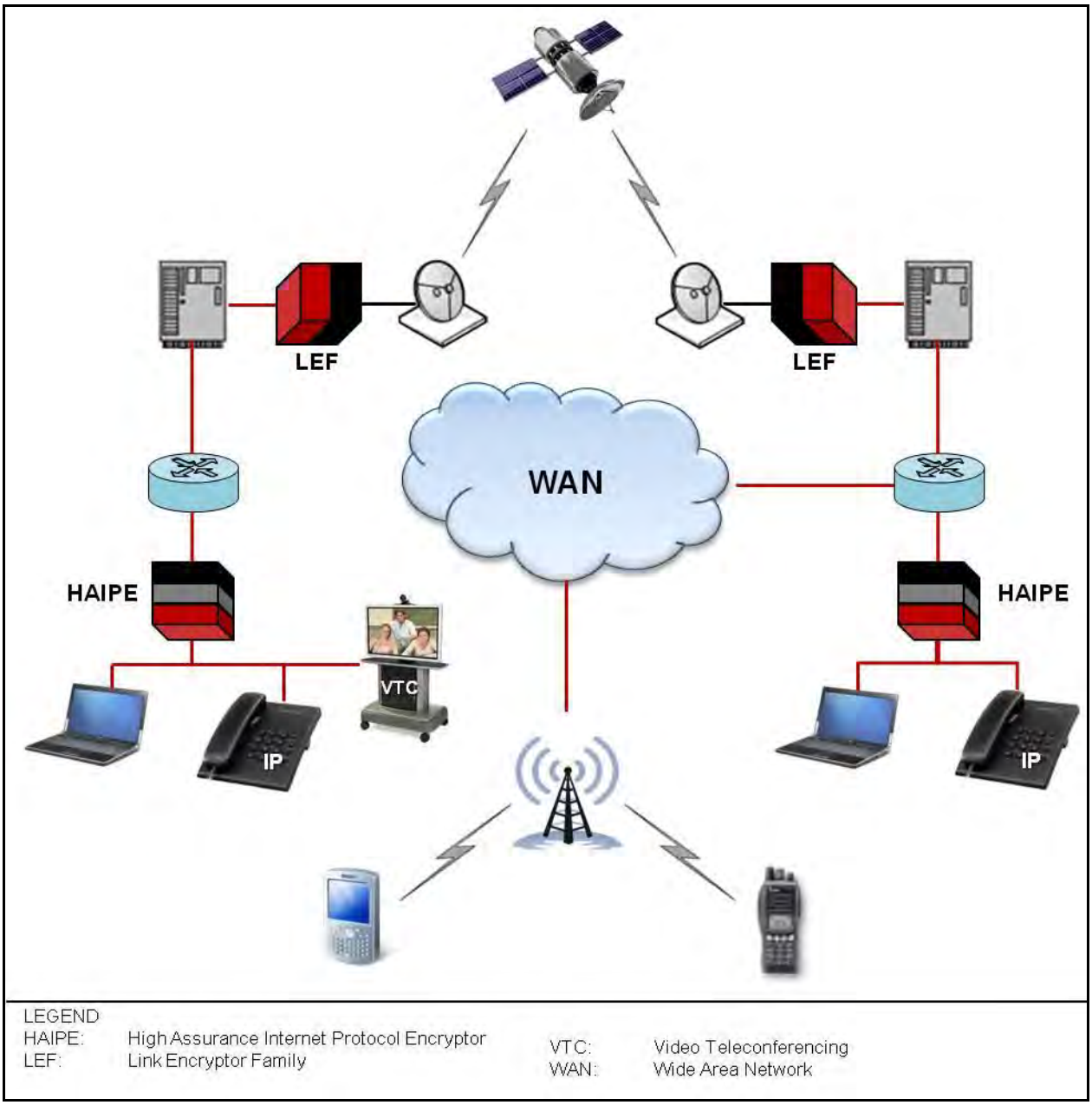

Figure 12.2-1. Sample Network

A HAIPE is a programmable Internet Protocol (IP) Information Security (INFOSEC) device with traffic protection, networking, and management features that provide Information Assurance services for IPv4 and IPv6 networks. The HAIPE(s) that are version 3.x or higher compliant meet the DoD mandate for IPv6 compatibility and the goals of the Cryptographic Modernization Initiative (CMI), and are a key component of the Global Information Grid (GIG) Vision. The HAIPE device is designed to provide confidentiality, integrity, and authentication services for IP traffic for Deployable and Fixed network applications. The HAIPE enables secure transmission across wide area networks (WANs) via IP packet encryption to compatible destination network

security devices where decryption takes place. Figure 12.2-2, Example HAIPE Application Diagram, provides an example of HAIPE implementation within a WAN.

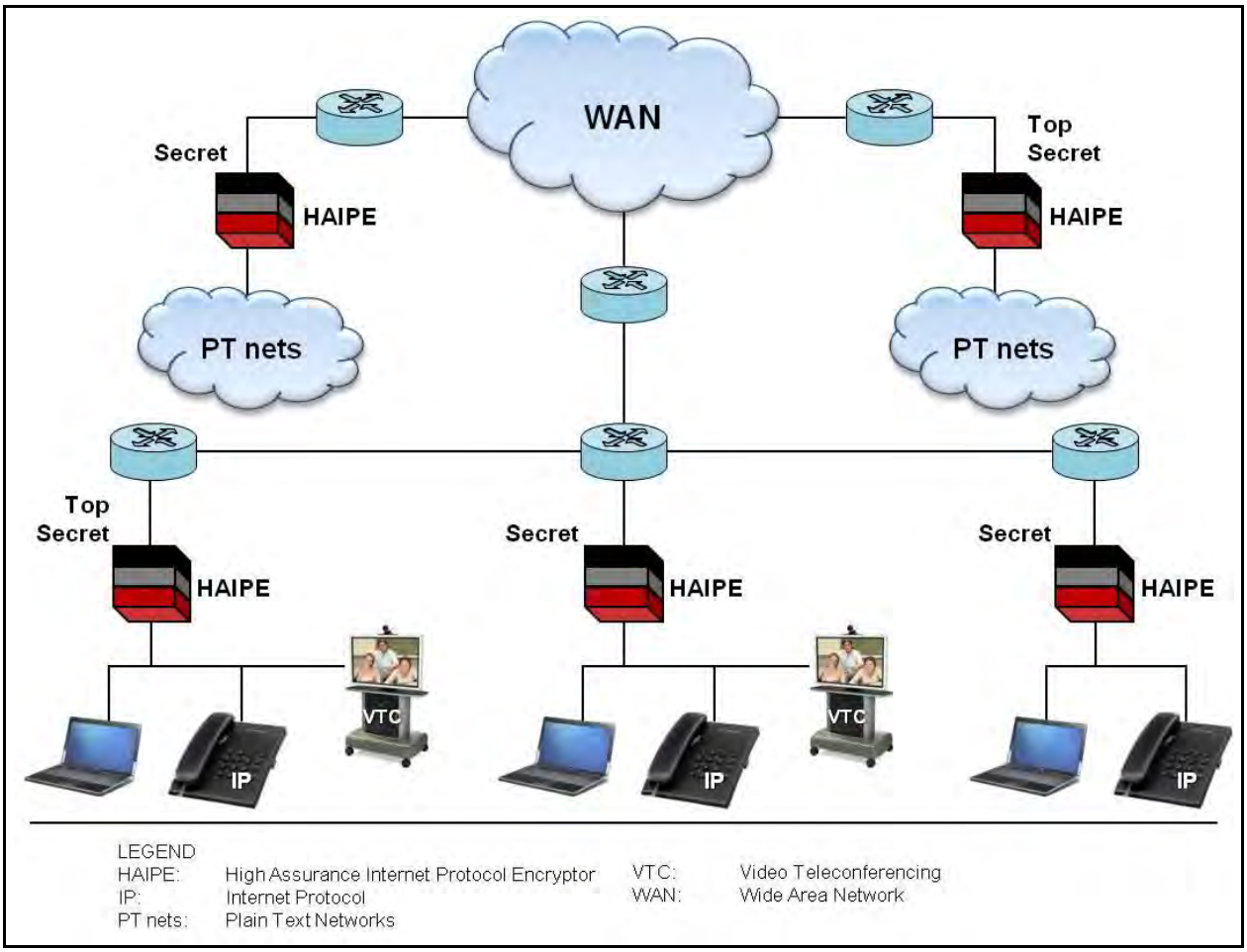

Figure 12.2-2. Example HAIPE Application Diagram

Design requirements are captured and promulgated in the HAIPE Interoperability Specification (IS). The HAIPE IS provides interoperability requirements for the following interconnections:

- HAIPE Device to HAIPE Device.
- HAIPE Device to Key Management Infrastructure (KMI).
- HAIPE Device to Security Management Infrastructure (SMI).
- HAIPE Device to Network Component Infrastructure (NCI).

A HAIPE compliancy, (that is, "HAIPE Interoperability Certification") is granted by the National Security Agency (NSA) for a communications security (COMSEC) device that complies with HAIPE IS. Whereas Joint Interoperability Test Command (JITC) interoperability Certification deals with interoperability as defined by CJCSI 6212.01E, JITC certification will not be granted until the device is certified by the NSA. The HAIPE compliance is met by meeting the requirements in the Networking Core and Traffic Protection Core Specifications,

plus the three Classified cryptography specifications (Suite A, Suite B, and Legacy), and any Extension Specifications. In HAIPE IS 3.1.x, the Networking Core and Traffic Protection Core Specifications have been combined into a single Core specification.

12.2.1.1 HAIPE IS V1.3.5 Devices

The devices listed below should be tested using Legacy (HAIPE IS v1.3.5) algorithms/transforms for both PPK (Baton-48) and Firefly (Medley-8):

- General Dynamics TACLANE KG-175 Classic. The KG-175 Classic is limited to 10-Half Duplex Speeds.
- General Dynamics TACLANE KG-175 E100. The KG-175 E100 is capable of 10/100-Full Duplex Speeds.
- General Dynamics TACLANE KG-175A (GigE). The KG-175A is capable of 10/100/1000-Full Duplex Speeds.
- General Dynamics TACLANE KG-175B (Mini). The KG-175B is capable of 10/100-Full Duplex Speeds.
- General Dynamics Sectera KG-235. The KG-235 is capable of 10-Half Duplex Speeds.
- Altasec KG-255. The KG-255 is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KOV-26 (Talon). The KOV-26 (Talon) is capable of approximately 10-Full Duplex Speeds.
- Harris KIV-54 (SecNet 54). The KIV-54 is capable of 10/100-Full Duplex Speeds.
- Safenet KIV-7MIP. The KIV-7MIP is capable of 10/100-Full Duplex Speeds.

12.2.1.2 HAIPE IS 1.3.X Devices

Devices listed below should be tested using Modern (HAIPE IS 3.x) algorithms/transforms for both PPK and Firefly (Medley-4).

- General Dynamics TACLANE KG-175D (Micro). The KG-175D is capable of 10/100-Full Duplex Speeds
- L-3 Communications KG-245A. The KG-245A is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KG-240A. The KG-240A is capable of 10/100-Full Duplex Speeds.
- L-3 Communications KG-245X. The KG-245X is capable of 10 Gigabit-Full Duplex Speeds.
- Altasec KG-250. The KG-250 is capable of 10/100-Full Duplex Speeds
- Altasec KG-250X. The KG-250X is capable of 10/100-Full Duplex Speeds.

12.2.1.3 Suite B Devices

Suite B devices include the HAIPE 3.x devices interoperating in Suite B mode, as well as standalone Suite B only devices known as Controlled High Value Products (CHVP). All of the following devices are Suite B devices and should be tested using Suite B algorithms/transforms for both PPK and Firefly (AES-4).

- General Dynamics TACLANE KG-175D (Micro). The KG-175D is capable of 10/100-Full Duplex Speeds.
- L-3 Communications KG-245A. The KG-245A is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KG-240A. The KG-240A is capable of 10/100-Full Duplex Speeds.
- Altasec KG-250. The KG-250 is capable of 10/100-Full Duplex Speeds.
- Altasec KG-250X. The KG-250X is capable of 10/100-Full Duplex Speeds.
- Altasec IPS-250. This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.
- General Dynamics C-100. This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.

12.2.2 Link Encryptor Family

LEF ECUs provide data security for the U.S. Military, U.S. Government, Allied forces, and coalition security environments. Current LEF devices include link and bulk encryptors. The LEF's primary mission is to protect Classified and sensitive digital data in a multitude of network environments: point-to-point, netted, broadcast, or high-speed trunk. The LEF ECU provides the means for encryption and decryption using Suite A and Suite B data security while providing advanced key management features that support the current key distribution system and the KMI initiatives.

The LEF ECUs are backward compatible with their legacy family members of equipment (HAIPE IS v1.35) to the degree necessary to support continuous operations. Although LEF requirements will vary based on implementation, JITC interoperability testing is still required. Additional testing may be required based on individual Services requirements.

The LEF Specification establishes the detailed cryptographic requirements and basic functional, performance, and security requirements of the Cryptographic Modernization (CM) version of the LEF link/bulk ECUs. This section incorporates the appropriate LEF Specification requirements to provide a sufficiently detailed baseline set of requirements while allowing vendors design flexibility as to the form, fit, and additional functionality of the resulting ECUs. Figure 12.2-3, Example LEF Application Diagram, illustrates the use of the LEF in a system.

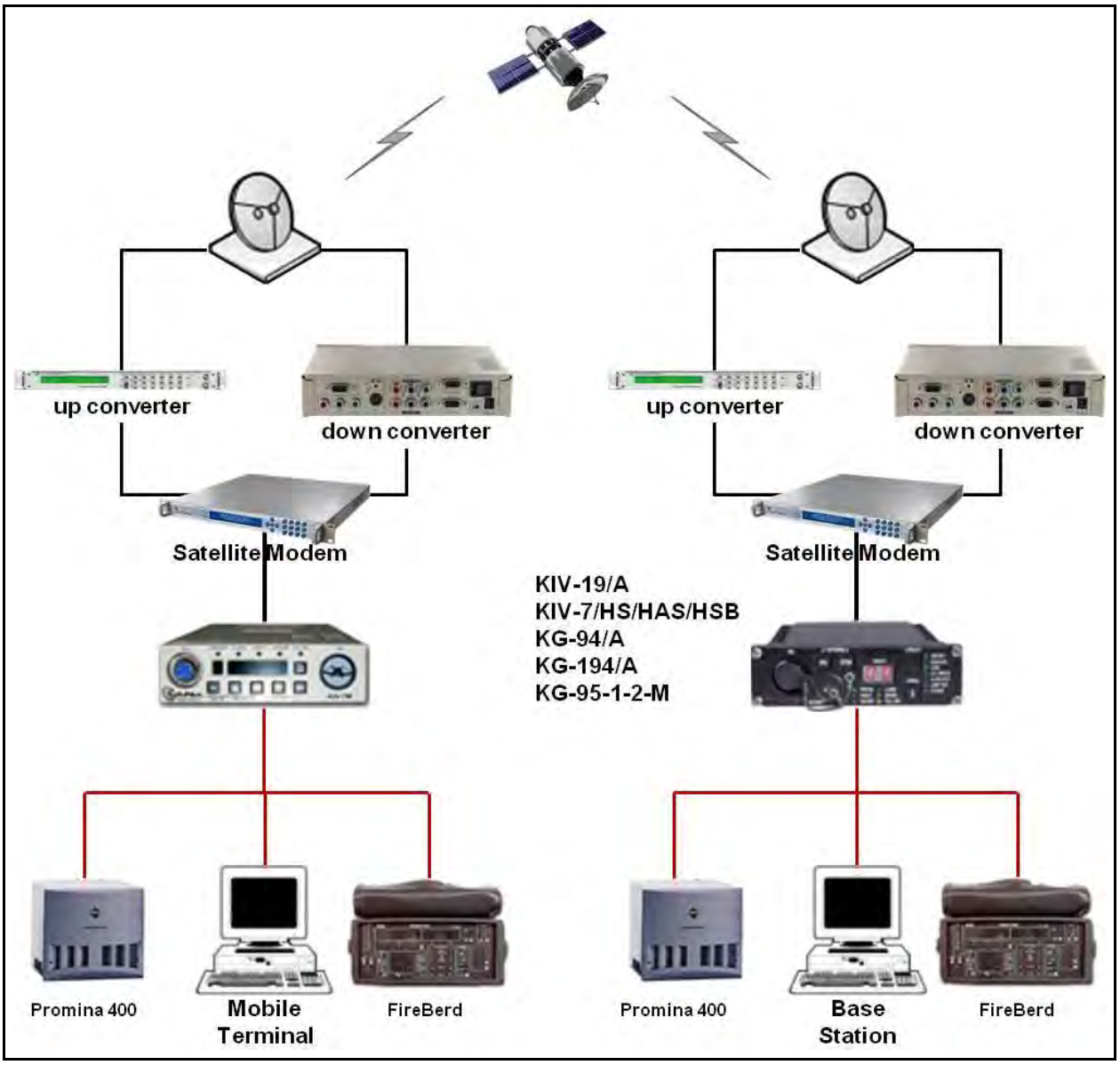

Figure 12.2-3. LEF Application Example

12.2.3 Secure Communications Interoperability Protocol (SCIP)

SCIP is a multinational standard for secure voice and data communication. SCIP derived from the U.S. Government Future Narrowband Digital Terminal (FNBDT) project after the United States offered to share details of FNBDT with a number of other nations in 2003. SCIP provides voice and data security for the U.S. Military, U.S. Government, Allied forces, and coalition security environments. SCIP supports a number of different modes, including national and multinational modes, which employ different cryptography. Many nations and industries are actively developing SCIP devices to support the multinational and national modes of SCIP.

SCIP has to operate over the wide variety of communications systems, including commercial landline telephone, military radios, communication satellites, Voice over IP (VoIP), and the different cellular telephone standards. It was designed to make no assumptions about the underlying channel other than a minimum bandwidth of 2400 Hz. It is similar to a dial-up modem in that, once a connection is made, two SCIP phones first negotiate the parameters they need and then communicate in the best way possible. Figures 12.2-4 and 12.2-5 illustrate SCIP network examples.

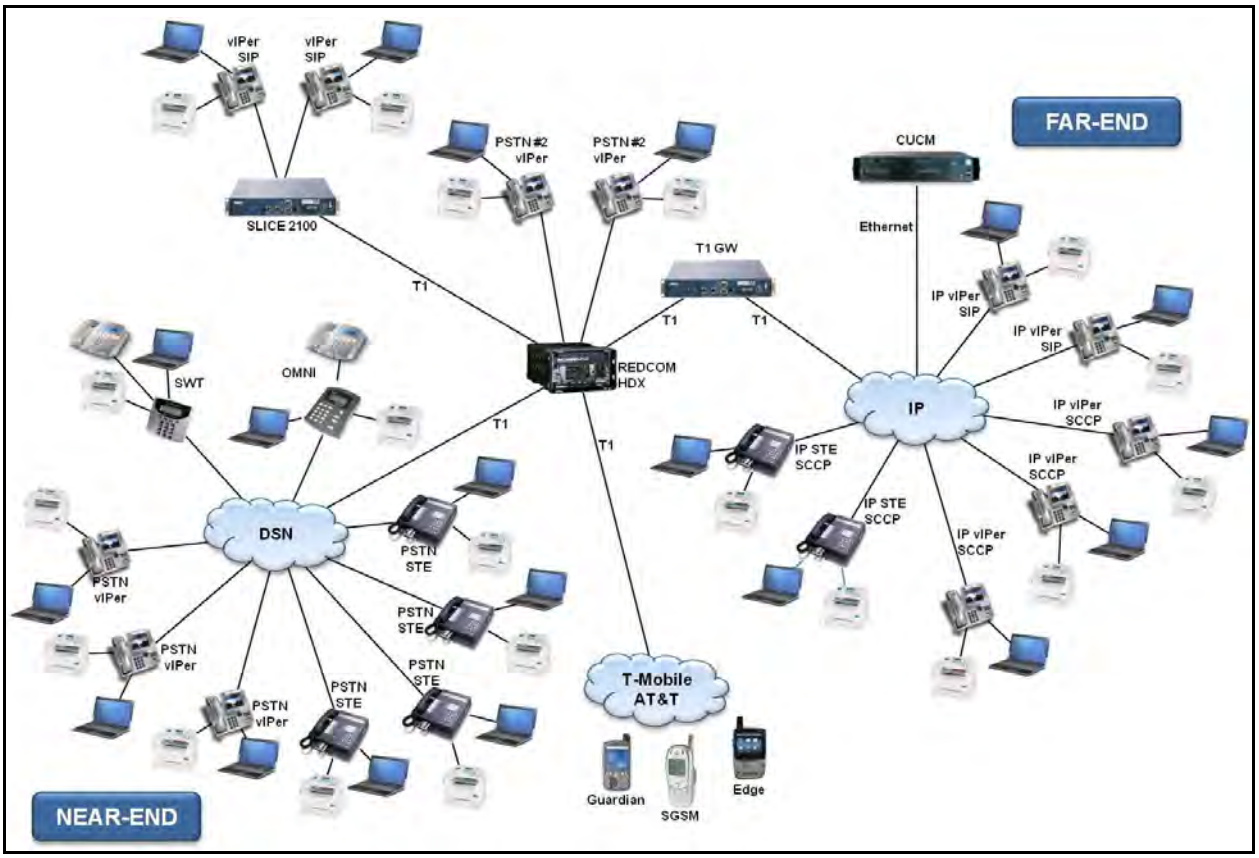

Figure 12.2-4. SCIP Network Example 1

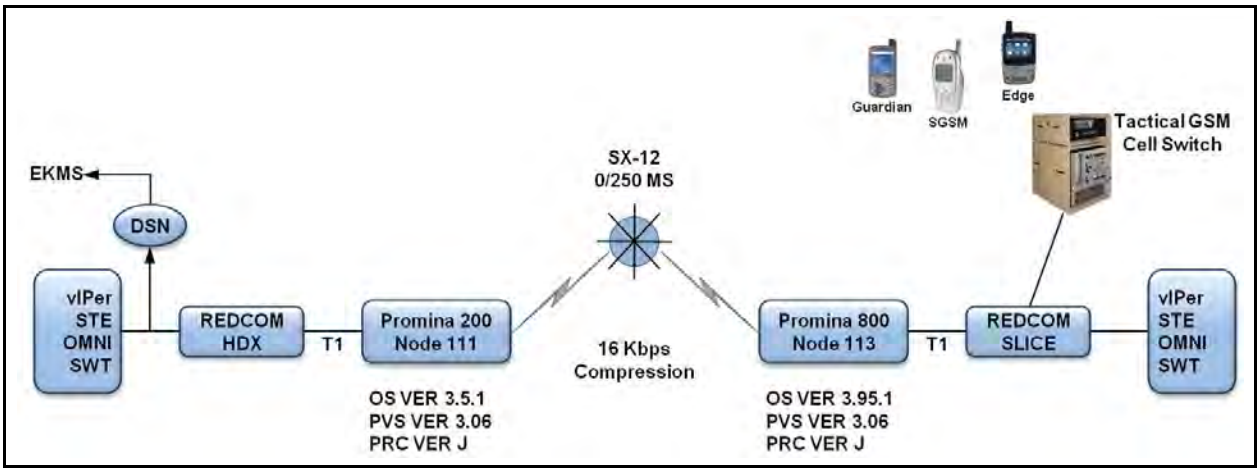

Figure 12.2.5. SCIP Network Example 2

12.3 DEVICE EVALUATION

This section provides information on HAIPE, LEF, and SCIP devices' performance and interoperability evaluation.

12.3.1 HAIPE

12.3.1.1 Throughput Test

Throughput testing should be conducted with a packet loss acceptance of 0 percent as per Request for Comments (RFC) 2544. Tests should run on both copper and fiber interfaces (if available) using both IPv4 and IPv6 addresses. The following key areas are evaluated in these tests:

- Maximum throughput in bidirectional scenarios with varied frame sizes (64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, and 1400 bytes).
- Effects of changing Encapsulating Security Payload (ESP) settings (Tunnel vs. Transport).
- Effects of changing Crypto Block settings (4 bytes, 8 bytes, 48 bytes).
- Effects of changing IP version (IPv4 vs. IPv6).
- Effects of changing Fixed Packet Length (FPL) settings.
- Effects of changing physical medium (Ethernet vs. Fiber).

12.3.1.2 Reliability Test

Reliability should be measured throughout the technical performance tests. A failure is defined as the inability to reboot, initialize, pass traffic as specified, and/or report status.

12.3.1.3 Configuration Changes

Configuration changes in the unit under test (UUT) may require a reboot or a loss in communications. These evaluations are performed to determine which configuration settings require the device to be rebooted, or cause a temporary loss of communications.

Configuration-change downtime is rated as follows:

Poor 1:	All configuration changes require downtime.
Fair 2:	≥ 50 % configuration changes require downtime.
Good 3:	< 50 % configuration changes require down time.
Excellent 4:	No configuration changes causes downtime.

12.3.1.4 Field Tamper Recovery

Tamper recovery requirements are derived from CES-CDD, Section 14.6.4 “Support Equipment,” and KSA, Section 6 b(7), “Tamper Detection.”

12.3.1.5 Loss of Physical Medium

Tests should be done to determine device responses and device recovery time from power outages. Results can be classified as:

Poor 1:		Recovery time	≥	2 minutes.
Fair 2:	1 minute ≤	Recovery time	<	2 minutes.
Good 3:	30 seconds ≤	Recovery time	<	1 minute.
Excellent 4:		Recovery time	<	30 seconds.

12.3.1.6 Line Impairment

The Line Impairment test should be conducted to verify that the device recovers secure communications after or during the interruptions.

12.3.1.7 Latency Test

Latency testing should be conducted with a packet loss acceptance of 0 percent as per RFC 2544. Network tools such as ping tests and trace route measure latency by determining the time it takes a given network packet to travel from source to destination and back on both copper and fiber interfaces (if available) using both IPv4 and IPv6 addresses.

12.3.1.8 Denial of Service Test

The INE should be tested for its ability to protect itself against denial of service (DOS) attempts. This test should be done on both the RED and BLACK side interfaces.

12.3.1.9 Vulnerability Test

The INE should protect against intentional and non-intentional malicious activity within the network. Fuzzing, enumeration, and spoofing are among the suite of attacks that should be run against the device. The device should not react at all to the malicious activities.

12.3.1.10 Configuration and Management

Configuration Management tests should be conducted to satisfy CES-CDD KSA, Section 6b(2), "Multiple Algorithms, Modes, Keys"; KSA, Section 6 b(5), "Configuration Management"; AA, Section 6c(1), "Operational Information"; KSA, Section 6b(4), "Management and Control"; KSA, Section 6b(6), "Cryptographic Product Distribution"; and KSA, Section 6b(8), "Form, Fit, Operational Function Replacement."

The Configuration Management is a software application that enables an administrator to locally or remotely configure or monitor an INE..

12.3.1.11 Secure Tunnel Setup and Security Policy Database Management

A Configuration Manager must be capable of configuring the Security Policy Database (SPD) entries in the two communicating INE UUTs. These evaluations should be conducted to determine ease or complexity for an administrator to set up the SPD.

12.3.1.12 Management of Remote Devices

Management of remote INE UUTs is essential to the Warfighter. The ability to manage these devices with ease is critical. Tests should be done to evaluate how easily a remote UUT can be configured, keyed, and monitored.

12.3.1.13 Cryptographic Key Loading

Cryptographic Key Loading evaluations should be performed with all available key loading devices. These include the Data Transfer Device (DTD) (AN-CYZ 10), Simple Key Loader (SKL), and Secure DTD2000 System (SDS).

12.3.1.14 Firefly Vector

Tests should be conducted to determine the complexity of loading Firefly Vector (FFV) sets into the UUT, using all available key loading devices.

12.3.1.15 Enhanced Firefly Vector Set

Tests should be conducted to determine the complexity of loading the Enhanced FFV (EFFV) into the UUT, using all available key loading devices.

12.3.1.16 Pre-Placed Key

Tests should be done to determine the complexity of loading the pre-placed key (PPK) into the UUT, using all available key loading devices.

12.3.1.17 Algorithms Supported

Tests should be conducted to determine which specific algorithms are supported by the UUT (Suite A, Suite B).

12.3.1.18 Usability

Usability evaluation should be conducted in accordance with the Functional requirements for the UUT covered in the CES-CDD KPP Section 6 a(2) "Programmability."

12.3.1.19 Device Software Upgradeability

The following key areas should be evaluated for software upgradeability:

1. Software (SW) Version display.
2. Ease for an administrator to install a software update.
3. Determination that, during or after SW update, UUT network connections are maintained.
4. Remote SW update.
5. SW update roll-back.
6. Remote SW update done via RED network.
7. Upgrade of SW while the device is actively in service.
8. UUT accomplished with restart or other downtime.

12.3.2 Interoperability

There are three different types of devices:

- HAIPE IS v1.3.5 devices.
- HAIPE IS 3.x devices.
- Suite B (a subset of HAIPE IS 3.x devices using Suite B encryption).

12.3.2.1 Reachability

The HAIPE IS 3.0.2 introduces two functionalities:

1. Peer HAIPE Reachability Detection (PHRD).
2. Peer Destination Unreachable Notification (PDUN).

PHRD performs a keep-alive function between two HAIPEs to determine if a Security Association (SA) endpoint is reachable. PDUN is a notification message sent by a HAIPE, if the destination address of the de-capsulated packet is no longer available on that HAIPE's local PT network.

PDUN should be tested to ensure that, when a destination network is removed, the source network's Peer Enclave Prefix Table updates accordingly. The PHRD option is tested to ensure that, when one UUT is removed from the network, the accompanying SA from the source network shows that the removed network is now "Unreachable."

12.4 LEF TEST & EVALUATION

12.4.1 Initialization/Functional

These tests confirm power-up, self test, operating, and general use from one day to the next without reset; loading of cryptographic keys; unit tests; and loading of personalities. The LEF device must perform by operating at a minimum of 24 consecutive hours without any errors. The LEF device should also be tested in various timed intervals after a stress test of operations. These intervals should be at least 10–15 executions of the feature under-test.

12.4.2 Personality/Cryptographic Algorithms

Tests should be conducted to verify that the LEF encryptor's initialization procedure matches its personality. The KIV-194 personality is verified to function as a KG-194/KIV-19A, and the KG-84 (KIV-7) personality is verified to function as a KG-84/KIV-7.

12.4.3 Interoperability

Interoperability tests should be performed to verify all known configurations in use.

12.4.4 Asynchronous Modes

Asynchronous data communication is used throughout many older Army systems. It is a vital part of the KG-84A/C operation. The UUT must operate in the Suite A and Suite B personalities, using the equivalent asynchronous options.

12.4.4.1 Synchronous Modes

The LEF has different synchronous modes available for use. Each mode is designed for use in different environments ranging from reduced synchronization overhead to high- and low-bit error rates.

The LEF encryptor UUT should be tested against all supported modes. In each mode, data rates from 50 bps to the maximum data rate supported by that algorithm are tested.

12.4.4.2 Link Encryption Interoperability and Interchangeability

UUT must be interoperable with modern link encryptors.

To test interoperability, the UUT should be tested with KIV-7M and KIV-19M to determine any deficiencies in modern encryptors so that users are made aware of the issue. Each mode and interface are tested from a minimum data rate of 50 bps to a maximum data rate of 50 Mps with 25 randomly picked frequencies.

12.4.5 Reliability

Reliability tests/assessment should be conducted to document defects and to determine Mean Time between Failures (MTBF).

A software defect which causes a lockup that can be cleared with a reboot is noted as a Severity 3. If the incident can be reproduced and/or happens more than three times during test conduct, it is noted as a Severity 2 defect. If the software failure cannot be cleared with a reboot or power cycle and requires the reloading of the software image, or COMSEC keying material, it is considered a catastrophic defect (Severity 1; refer to Section 5). All software failures (e.g., lockups and hangs) are noted in the evaluation report. Repeated sequential software defects are considered a failure. Any operational problems (except an intentional zeroize) that causes reproducible lockup of the unit is considered a major software failure (i.e., Severity 1 defect).

12.4.6 Reboot Test

The UUT is tested to ensure that, if power is removed and replaced, an operational circuit will retain key and previous strap settings so as to resume operational status without the unit going into alarm. This test is performed at least 500 times with an expected failure rate of less than 1 percent.

12.4.6.1 Key Loading

The UUT should be tested for its ability to accept keys through the fill port. Keys are loaded using DS-101, DS-102, and RS-232 protocols. The UUT must operate with the AN/CYZ-10 (DTD) or simple key loader (SKL). Proper operation consists of the Key Management Interface being able to recognize the proper and improper key for the respective personalities. The UUT

would be categorized as a failure if the UUT does not recognize improper key or goes into a hard fault error state.

12.4.6.2 Over-the-Air-Distribution or Over-the-Air-Re-Key

The UUT must properly perform the Over-the-Air Distribution (OTAD) and Over-the-Air-Re-Key (OTAR) operations with the supported algorithms. Operations will consist of being the receiving and transmitting side of the link. An OTAR/OTAD operation is considered a FAILURE if the key is improperly transferred or cannot be performed. A limited PASS will be given if a workaround (i.e., disabling "UpdateU") has to be performed for the operation to be successful.

12.4.6.3 Change Key/Local Update Operations

The UUT must properly perform the change key operation using both PPK and EFF. Change key operations will be performed during testing at a minimum of 10 times initiated from each side and be performed in 1/2/3 consecutive sequences at random. The operation will consist of performing a change key and then awaiting for the link to be reestablished. No other user operation should be performed if the link has resynchronized enabled.

The UUT must properly perform a local update when using PPK. Change key operation is conducted to set the count at a random number. If the link does not re-establish, the UUT should be categorized as FAIL.

12.4.7 Network Management

The UUT must be manageable via Ethernet port by a remote system. The UUT should be tested using human manual interaction and computer automated HyperText Transfer Protocol, Secure (HTTPS) requests/posts to verify the robustness and viability of the UUT. The UUT should not enter an alarm state. Table 12.4-1 lists the test criteria.

Table 12.4-1. Network Management Test Criteria

RANK	GRADE	CRITERIA
Failure	0	No Ethernet port
Poor	1	Poor configuration of HCI
Fair	2	Clear configuration of HCI, able to process all requests
Good	3	Clear configuration of HCI, able to manage multiple units
Excellent	4	Robust user interface, manage multiple units, capable to save and reload different configurations

12.4.8 Software Download

Assessments should be done to determine the level of effort required to load and upgrade software for the device. This should include validating the instructions in the documentation provided by the OEM. Evaluating the UUT for mass updating capabilities and isngle-button operation updates should be considered. Table 12.4-2 lists some criteria for assessment.

Table 12.4-2. Software Download Test Criteria

RANK	GRADE	CRITERIA
Failure	0	No Management port
Poor	1	No Instruction
Fair	2	Minimal instruction, requires highly skilled user
Good	3	Step-by-step instruction provided
Excellent	4	Step-by-step instruction with images for clarification

12.4.9 Degraded Network Capability and Robustness

LEF devices should be tested for its capabilities to function in a degraded network environment. LEF devices should be able to accept a wide variety of network timing and variable speeds. Standard LEF test speeds range from 50 bps to 50 Mbps. Table 12.4-3 lists the test criteria.

Table 12.4-3. Degrated Network Capability and Robustness Criteria

RANK	GRADE	CRITERIA
Failure	0	Device works only in ideal condition – No delay or error
Poor	1	Device works with minimal delay and error (10^-7)
Fair	2	Device passes test with intermediate delay and error (<10^5)
Good	3	Device passes test with intermediate delay and error (<10<3)
Excellent	4	Device passes test with extreme delay and error (>=10^3)

12.4.10 Required Ancillaries Devices

Interface connections should be verified for each device. There are more than 24 variants of rack-mounted adapters for different KIV-7, KIV-19, KG-84, KG-94, and KG-194 applications. Each of these rack mounts have different connectors and use different pin-outs.

12.4.11 Control Signal Requirements

Control signal options should be tested to ensure that they operate as used in the field and specified in the manual.

Table 12.4-4 lists the types of signals supported for each device. The UUT should be tested for its supported control signals. Any signals not supported should be considered as deficiencies.

Table 12.4-4. Control Signal Requirements Matrix

ALGORITHM	KIV-7M A	KIV-7M B	KIV-7M W	KIV-7M S	KIV-19M A	KIV-19M B	KIV-19M W	KIV-19M S	KIV-7 S	KIV-7HSA S	KIV-7HSB S	KIV-7HS S	KG-84A S	KG-84C S	KIV-19 W	KIV-19A W	KG-194 W	KG-194A W	KG-94 W	KG-94A W
RED Request to Send	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X						
RED terminal Ready	M	M	X/L	X/L	M	M	X/L	X/L												
RED Clear to Send	M	M	X/L	X/L	M	M	X/L	X/L												
RED DCE Ready	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Clear to Send	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X						
BLACK Ready to Receive	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK DTE Ready	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Ready to Send	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Terminal Ready	M	M	X/L	X/L	M	M	X/L	X/L												
Contact Closure Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Differential Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Single-Ended Positive Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Single-Ended Negative Resyn.	M	M	X/L	X/L	M	M	X/L	X/L						X	X	X	X	X	X	X
Single-Ended Balanced Resyn.	M	M	X/L	X/L	M	M	X/L	X/L						X	X	X	X	X	X	X

Legend:
L: Denotes the requirement for legacy transitioning testing.
M: Denotes the requirement for modern testing.
X: Denotes the requirement for legacy testing.

12.4.12 Interface Requirements

The LEF devices should be tested against various combinations of interface specifications: RS-232, EIA-530, and EIA-644. Table 12.4-5 lists which combination of interfaces will be required for test conduct.

Table 12.4-5. Interface Requirement Matrix

	KIV-7M	KIV-7M	KIV-7M	KIV-7M	KIV-19M	KIV-19M	KIV-19M	KIV-19M	KIV-7	KIV-7HSA	KIV-7HSB	KIV-7HS	KG-84A	KG-84C	KIV-19	KIV-19A	KG-194	KG-194A	KG-94	KG-94A
ALGORITHM	**A**	**B**	**W**	**S**	**A**	**B**	**W**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**W**	**W**	**W**	**W**	**W**	**W**
RED RS-232 BLACK RS-232									X	X	X	X	X	X						
RED RS-232 BLACK EIA-530									X	X	X	X	X	X						
RED RS-232 BLACK EIA-644																				
RED EIA-530 BLACK RS-232									X	X	X	X	X	X						
RED EIA-530 BLACK EIA-530					M	M			X	X	X	X	X	X	X	X	X	X	X	X
RED EIA-530 BLACK EIA-644																				
RED EIA-644 BLACK RS-232																				
RED EIA-644 BLACK EIA-530																				
RED EIA-644 BLACK EIA-644					M	M														

Legend:
M: Denotes the requirement for modern testing.
X: Denotes the requirement for legacy testing.

12.5 SCIP EVALUATION

12.5.1 General Description

The SCIP requirements are used to certify DoD Secure Communications Devices (DSCDs) when directly connected to or otherwise traversing the Defense Switched Network (DSN), the Public Switched Telephone Network (PSTN), or the Defense RED Switch Network (DRSN) Gateway to or from the DSN.

This section applies to the evaluation of secure mode operation of any DSCD that either directly connects to the DSN, the PSTN, or the DRSN Gateway or traverses these networks in the course of conducting a secure communications session, regardless of where the telephone call originates

or terminates. The certification test environment for DSCDs shall include configurations that realistically simulate fixed networks (i.e., DSN, DRSN via the DSN Gateway, PSTN) and deployed networks, as illustrated in Figures 12.2-4 and 12.2-5.

12.5.1.1 Evaluation Methods

The secure voice equipment will be evaluated to include features and capabilities of a DSCD device to include voice, data, and facsimile transmission.

1. SCIP Protocol.

   The enabled DSCD shall be only those that are Type Approved by NSA and are listed on the NSA Secure Product web site. Each DSCD must support at least one NSA-approved secure protocol. If the DSCD supports more than one secure protocol, it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD.

2. Interface.

   The DSCD devices that use a two-wire analog or basic rate interface (BRI) shall meet the End Instrument (EI) requirements as specified in Section 3.7, Customer Premises Equipment. The DSCD devices that use an IP interface shall meet the EI requirements as specified in Section 2, Session Control Products. DSCD devices that support DSN trunk interfaces (Primary Rate Interface [PRI] or IP [UC Session Initiation Protocol (SIP)]) shall meet the interface requirements defined in AS-SIP 2013, Section 2.14.10, MG Support for ISDN PRI Trunks, for PRI, and Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, for the AS- SIP.

3. Call Completion Rate.

   A DSCD device that supports one of the required signaling modes should interoperate with and establish secure sessions with other compatible devices.

4. Multiple SCIP Modes.

   The DSCD should be capable of using the protocol(s) provided to establish a secure session and should maintain secure communications for the duration of the secure portion of the call.

5. Minimum Essential Requirements.

   If the DSCDs that establish secure sessions on IP networks use SCIP, then it shall satisfy all the end point requirements described in SCIP-215 and SCIP-216.

SECTION 13
SECURITY DEVICES

The UCR Security Devices Section 13 describes the requirements for security devices that will be on the Approved Products List (APL). This includes requirements for firewalls (FWs), Intrusion Prevention Systems (IPSs), Network Access Control, Wireless Internet protocols (IPs), and Virtual Private Network (VPN) devices.

13.1 PHYSICAL SECURITY

Physical security is the responsibility of the installing Base/Camp/Post/Station (B/P/C/S). Essentially, two sets of requirements are associated with a complete Unified Capabilities (UC) system. The end points (i.e., PCs, End Instruments [EIs], Classified Provider Edge [C-PE]) have one set of physical security requirements while the network (i.e., Local Area Network [LAN] switches, security devices, and routers) and signaling products (i.e., Session Controller [SC], Softswitch [SS], and Media Gateway [MG]) require another set of requirements. A full definition of physical security requirements is beyond the scope of this section.

13.2 SECURITY DEVICES SECURITY DESIGN

Security devices use a defense in-depth approach based on best commercial practices. The product security defenses are categorized as follows and are discussed in Section 4, Information Assurance:

- User Roles.
- Hardened operating systems.
- Auditing.
- Application security.
- Redundant systems.

Additional defenses may be added dependent on the specific threats associated with a product.

The requirements in UCR Section 13 describe the requirements necessary to ensure that the separation of information is maintained and that the network managers are able to be aware of attacks against the network, configure the devices to protect against those attacks, and provide data to perform forensic activity on security-related incidents.

13.3 NETWORK SECURITY DESIGN

One of the principal tenets of any Information Assurance design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics. A converged network requires the opposite, in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions

between the various component segments must be controlled to ensure that an attacker that gains access to one segment cannot gain access to nor affect the other segments. In addition, interaction control between various segments is used to prevent configuration or user errors in one segment from affecting other segments. The actions of normal users of converged network services must not affect the other services, specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are Virtual LANs (VLANs), segmented IP address space or subnets, and VPNs, and are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls (Voice and Video over IP [VVoIP] stateful firewalls) to control the flow of traffic between the VLANs and VPNs.

The UCR ensures that the equipment can set up VLANs or VPNs as appropriate. It does not dictate the way that they should be implemented, but the STIGs do provide that guidance.Figure 13.3-1, Notional Example of Voice and Data ASLAN Segmentation, provides one example and presents the simplest type of converged LAN with only voice and data applications. Separate VLANs are established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the Customer Edge (CE) Router (CE-R), separate VPNs may be established, if necessary, to segment the voice traffic from the data traffic as the packets transit the Defense Information Systems Network (DISN) Wide Area Network (WAN). In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE-R to the Provider Edge (PE) Router along the same path as the non-VVoIP traffic. The only connection to the Public Switched Telephone Network (PSTN) is through a Time Division Multiplexing (TDM) interface using Primary Rate Interface (PRI) or Channel Associated Signaling (CAS) so that there is no interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the SC has two separate interfaces: one for local Network Management (NM) and a second for the Voice over IP (VoIP) end-to-end (E2E) NM traffic.

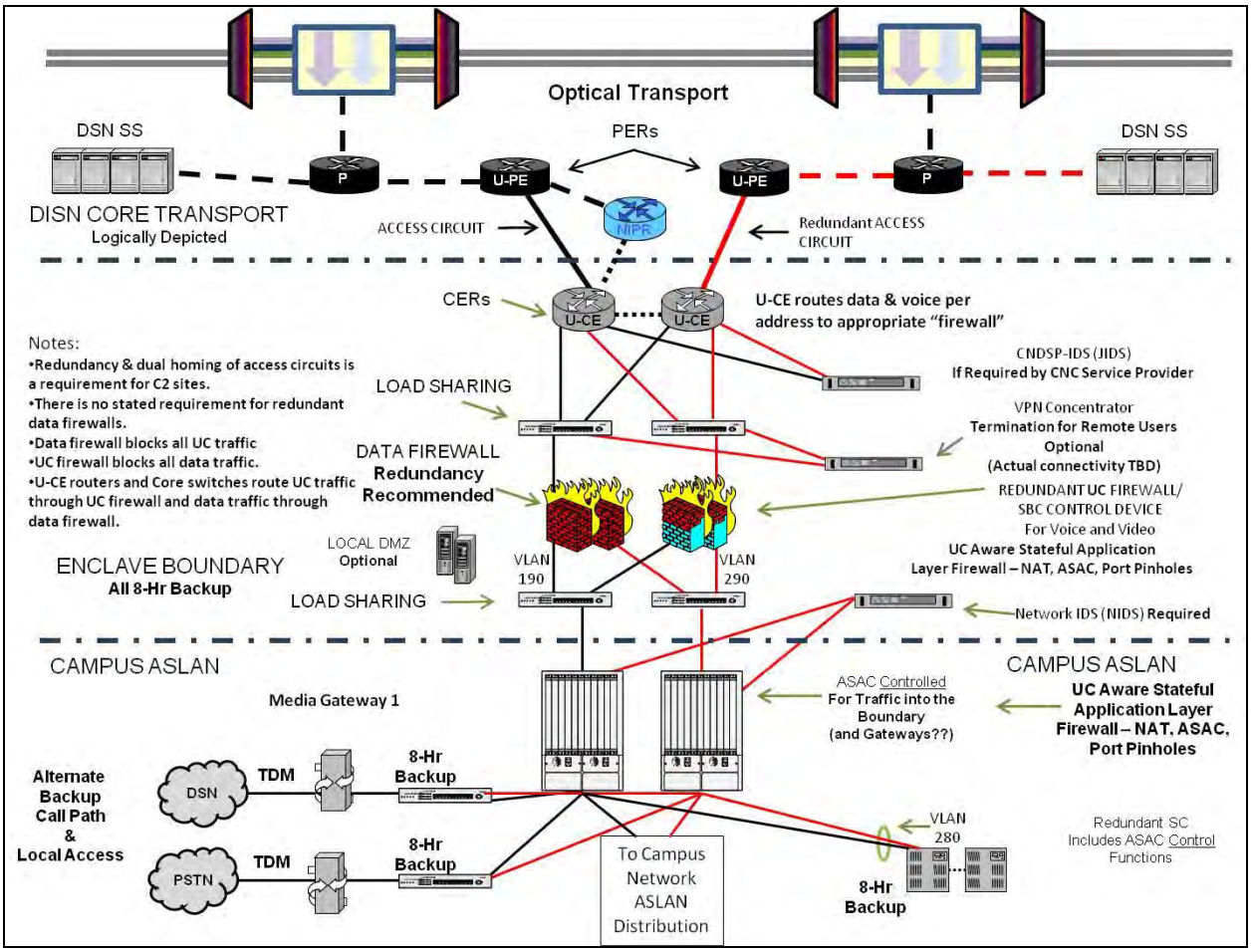

Figure 13.3-1. Notional Example of Voice and Data ASLAN Segmentation

13.4 REQUIREMENTS DEVELOPMENT CONCEPT

Based on the UC Information Assurance design, threats, and countermeasures, a set of derived requirements were developed for security devices. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of the Unified Capabilities Requirements (UCR), the requirements are levied on the individual security devices, as applicable, to secure the entire product. It is understood that the Information Assurance design provides a high-level description of how the security devices interact in a secure manner. In addition, the appropriate Security Technical Implementation Guidelines (STIGs) will further clarify how the Information Assurance design and requirements are implemented on the appliance. This section is intended to provide a level of security requirements consistent with the level of security requirements defined for the UC, but adapted for the unique Department of Defense (DoD) UC environment consistent with the requirements in the UCR.

SECTION 14
ONLINE STORAGE CONTROLLER

A Data Storage Controller (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 Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (LAN) (ASLAN), but the DSC is not considered part of the ASLAN. A DSC provides data storage and services as depicted in Table 14-1, DSC Data Storage and Service Types.

Table 14-1. DSC Data Storage and Service Types

STORAGE TYPE	NETWORK INFRASTRUCTURE
Network Attached Storage (NAS)	Ethernet Multiprotocol: NFS, CIFS, iSCSI, HTTP, FTP
Storage Area Network (SAN)	Fibre Channel (FC) Fibre Channel Protocol (FCP)
Converged Network	Ethernet Multiprotocol: NFS, CIFS, iSCSI, HTTP, FTP Fibre Channel over Ethernet (FCoE) Data Center Bridging (DCB)

LEGEND

CIFS: Common Internet File System	FCP: Fibre Channel Protocol	NAS: Network Attached Storage
DCB: Data Center Bridging	FTP: File Transfer Protocol	NFS: Network File System
FC: Fibre Channel	HTTP: HyperText Transfer Protocol	SAN: Storage Area Network
FCoE: Fibre Channel over Ethernet	iSCSI: Internet Small Computer System Interface	

The DSC features and capabilities listed in UCR 2013, Section 14, Online Storage Controller, may be offered as part of a unified capability offering associated with other products on the Approved Products List (APL). The definitions for DSC are found in Appendix C, Definitions, Abbreviations and Acronyms, and References.

SECTION 15
ENTERPRISE AND NETWORK MANAGEMENT SYSTEMS

The migration to Unified Capabilities (UC) services in which voice, video, and data services are being converged onto an Internet protocol (IP) infrastructure requires enhancement to the existing methods and procedures used to perform network management of the hybrid Time Division Multiplexing (TDM)/IP based voice, video, and data service environment. The enhancement to current methods and procedures is also required to support the new Network Operations (NetOps) environment defined by Department of Defense (DoD) Instruction (DoDI) 8410.02.

The end-to-end (E2E) management functions and metrics that must be collected and the measurements taken for voice and video services are different from those required to manage data services. Voice and video quality is sensitive to E2E delay, while data services are not delay sensitive, but sensitive to packet loss. E2E performance management of voice and video services must therefore extend to End Instruments (EIs) to obtain true voice performance assessment. Another important consideration is that the converged network infrastructure being used E2E for voice and video sessions consists of Military Department (MILDEP)-managed local infrastructures and intranets and the Defense Information Systems Agency (DISA)-managed backbone infrastructure. This is reflected in the definition of "E2E" for voice, video, and data services shown in Figure 15-1.

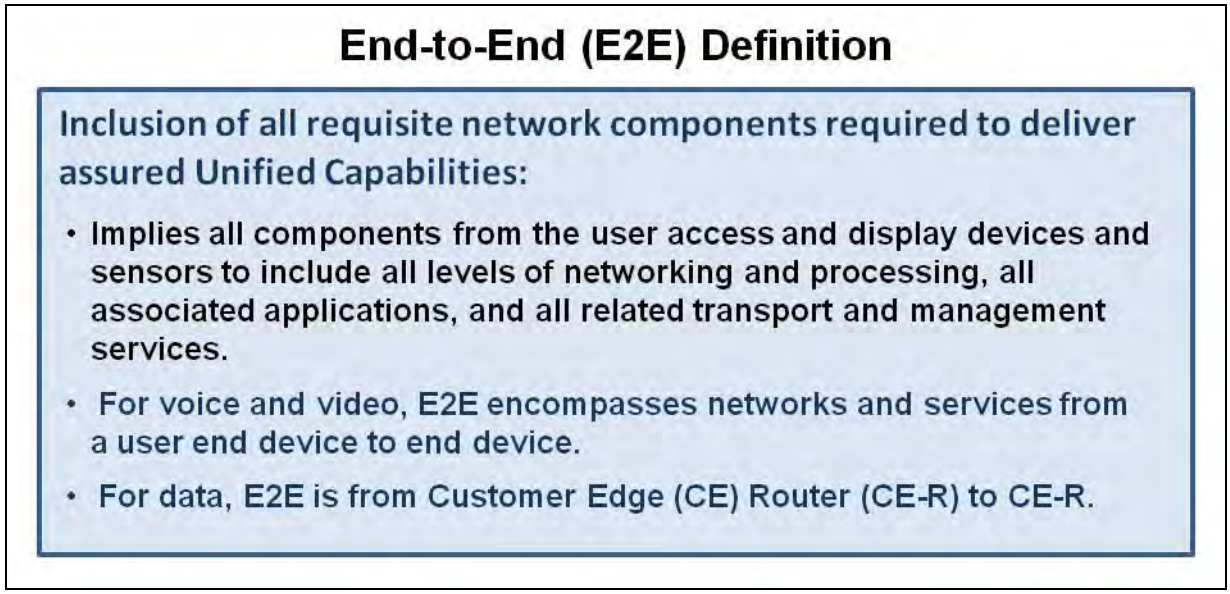

Figure 15-1. Definitions of End-to-End for Voice, Video, and Data Services

To satisfy the E2E management responsibilities for the Global Information Grid (GIG), it is critical that NetOps systems are implemented that support the information sharing concept (as directed by policy). The concept is the enabler that provides E2E visibility and situational awareness to U.S. Cyber Command (USCYBERCOM). The following sections describe the

NetOps support systems and their application in providing E2E system performance monitoring and situational awareness to USCYBERCOM.

15.1 DISN OPERATIONAL SUPPORT SYSTEM COMPLEX

The Defense Information Systems Network (DISN) Operational Support System (OSS) complex used by DISA consists of "all the systems" that automate Operations, Administration, Maintenance, and Performance (OAM&P) management functions. Figure 15.1-1, DISN OSS Functions, illustrates the OSS hierarchy. At the bottom of the hierarchy is the Network Element (NE) layer. The NEs are monitored and controlled by a series of Element Management Systems (EMSs). The EMSs communicate with the Network Management (NM) layer using a common communications vehicle. At the NM layer, alerts from the monitored NEs are consolidated into situational awareness data. This data is made available to MILDEP Network Operations and Security Centers (NOSCs) or USCYBERCOM for a top-level E2E view of the DISN backbone. The situational awareness data is provided through the DISN Information Sharing Service (ISS) on Secure IP Router Network (SIPRNet).

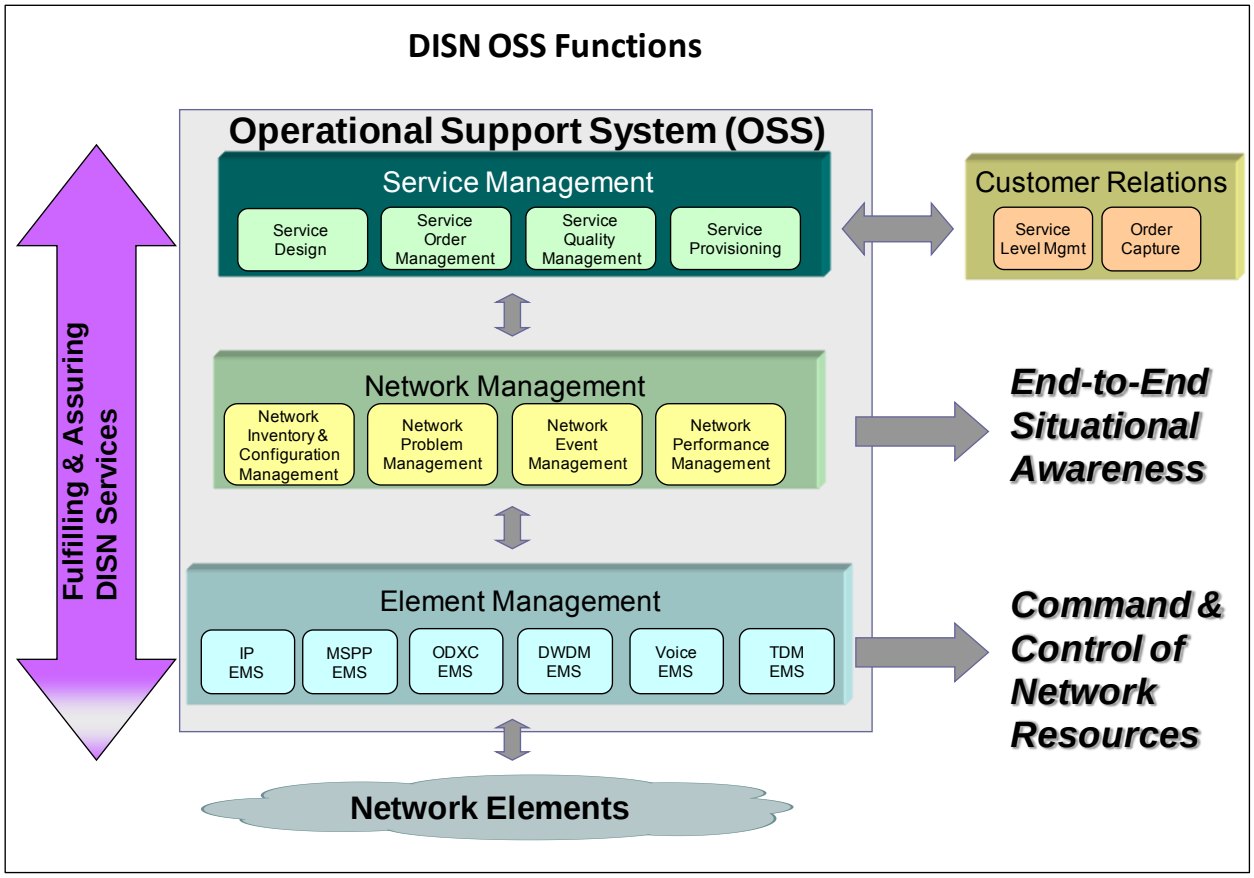

Figure 15.1-1. DISN OSS Functions

15.2 UC VOICE AND VIDEO SERVICES BACKBONE MANAGEMENT SYSTEM

Performance monitoring and management of the UC voice and video services backbone is presently managed by DISA using EMS (as the Voice EMS depicted in Figure 15.1-1). This includes point-to-point (P2P) video systems services with Assured Services Session Initiation Protocol (AS-SIP) signaling. The EMS collects performance data from all voice/video backbone switches including TDM-based Multifunction Switches (MFSs) and IP-based softswitches (SSs). The EMS connects to the switch monitoring ports with a closed telemetry network using secure protocols including Secure Shell Version 2 (SSHv2) and Transport Layer Security (TLS). Data is transferred using either command line syntax or Simple Network Management Protocol Version 2 (SNMPv2) (with IP Security [IPSec]) or SNMPv3, depending on the particular switch vendor management port interface capabilities. The EMS also sends NM controls to the switching systems using each vendor's unique command syntax. The EMS forwards data to the DISN OSS NM layer with a one-way data feed.

DISA's voice and video performance monitoring capabilities are being augmented by the installation of Telchemy probes connected to the Customer Edge (CE) Routers (CE-Rs) at each SS location. Combined, the EMS and Telchemy probes will provide performance monitoring and measuring capability for the voice and video services within the converged DISN IP backbone.

Figure 15.2-1, Spiral E2E EMS Monitoring of Voice/Video/Data Services, provides a high-level illustration of how the EMS solution monitors performance of the TDM and IP-based voice/video network elements E2E.

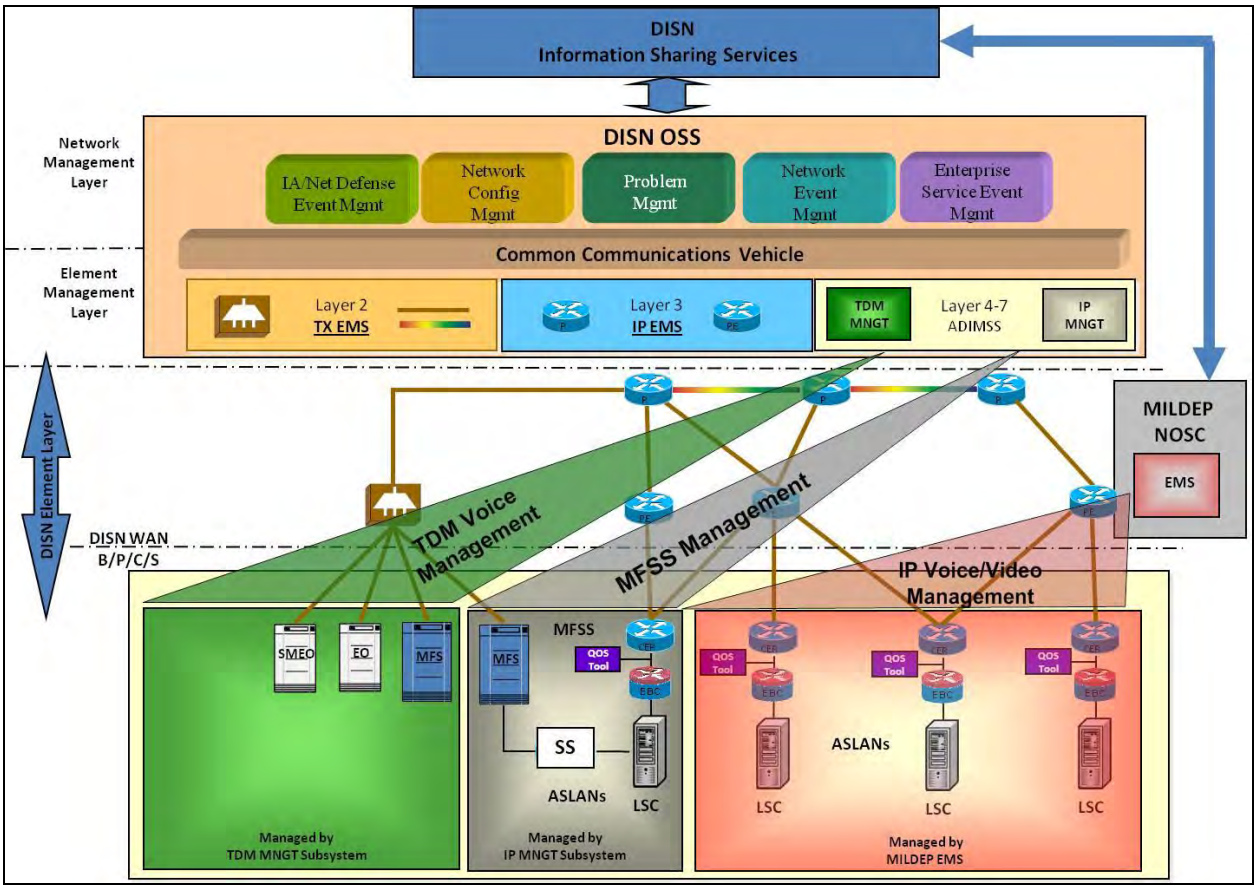

Figure 15.2-1. Spiral E2E EMS Monitoring of Voice/Video/Data Services

15.3 INFORMATION SHARING

Information sharing between DISA backbone monitoring systems and MILDEP Edge monitoring systems is a critical component of the NetOps requirements for GIG Enterprise Management (GEM) and GIG Network Assurance (GNA). The envisioned DoD ISS provides both Machine-to-Machine (M2M) and Human-to-Machine (H2M) methods of sharing DISN OSS data and MILDEP Edge data. The ISS is an enabler of the following:

- The Joint Concept of Operations (JCONOPS) for NetOps.
- DoD Chief Information Officer (CIO) NetOps Strategic Vision.
- GEM (DoDI 8410.02).

Information Sharing is the solution being adopted for the UC Spirals. DISA/NS8, Operational Support System (OSS) Division, has developed an information sharing solution based on net-centric, service-oriented principles and technologies for sharing NetOps information across boundaries. Figure 15.3-1, GIG E2E DISN UC Services Management Approach, depicts the high-level approach to information sharing.

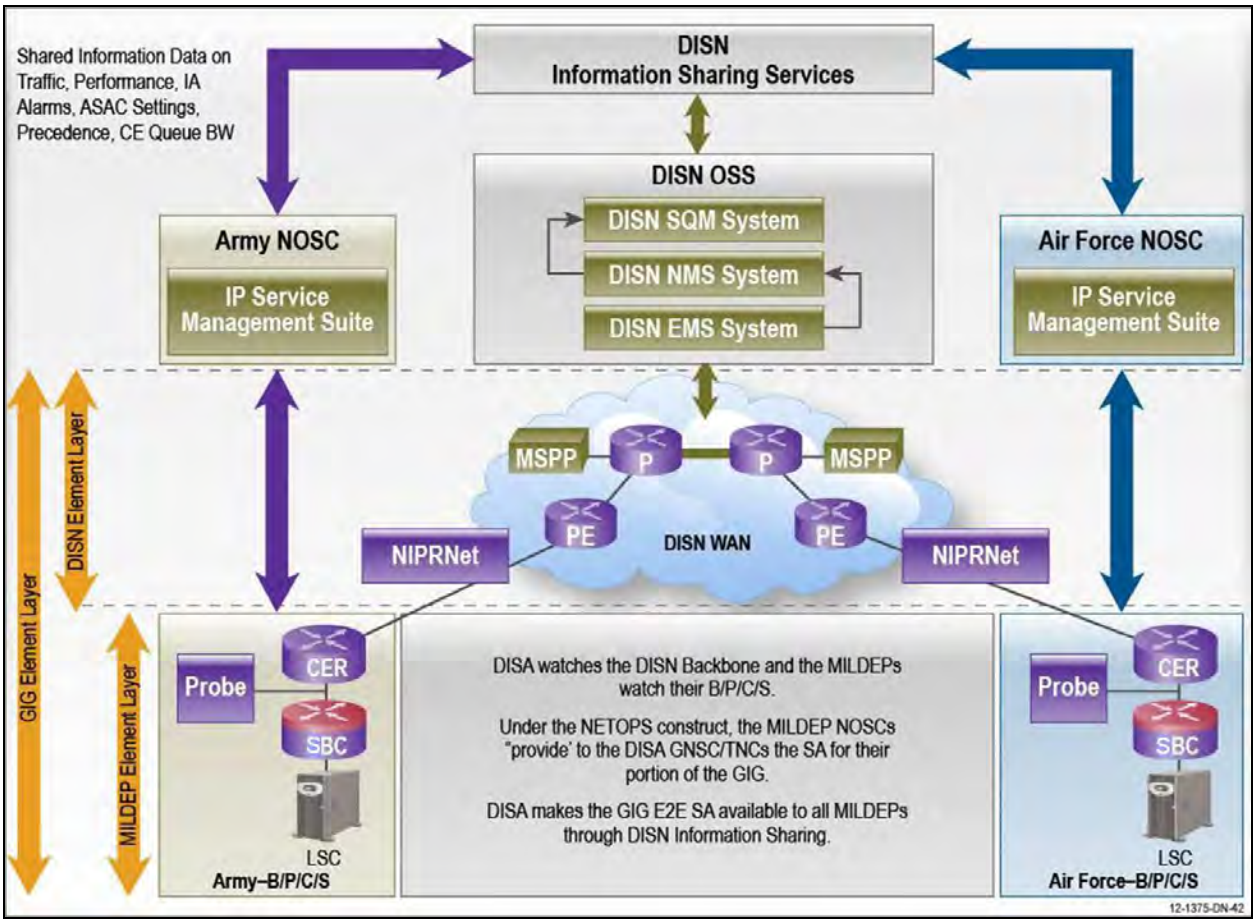

Figure 15.3-1. GIG E2E DISN UC Services Management Approach

Figure 15.3-1 depicts the information sharing solution that requires DISA and the MILDEPs to be both producers and subscribers of information services over the SIPRNet to establish E2E situational awareness about the GIG UC environment. For DISA, the DISN OSS will provide alarm, performance, trouble tickets, and inventory data using web services technologies for authorized users to analyze.

Figure 15.3-1 also depicts that the MILDEPs will provide alarm, traffic, performance, trouble tickets, Assured Services Admission Control (ASAC) settings, and inventory data about their enclaves also using web services technology for authorized users to analyze. Both DISA and the MILDEPs will use the data they consume to aggregate, correlate, and present an E2E operational view of the infrastructure.

Figure 15.3-2 depicts information sharing from a slightly different perspective. It shows the DISA Network Operations Centers (NOCs) displaying information pulled from the SSs by the EMS and DISN OSS Data Communications Network (DCN), and Information Sharing data published by the MILDEP edge sites via a MILDEP network (either out-of-band or in-band). Further, the figure shows MILDEP NOSCs displaying information provided from their MILDEP

edge sites via their MILDEP networks and combining it with DISA network and network component information pulled from DISA's Information Sharing solution.

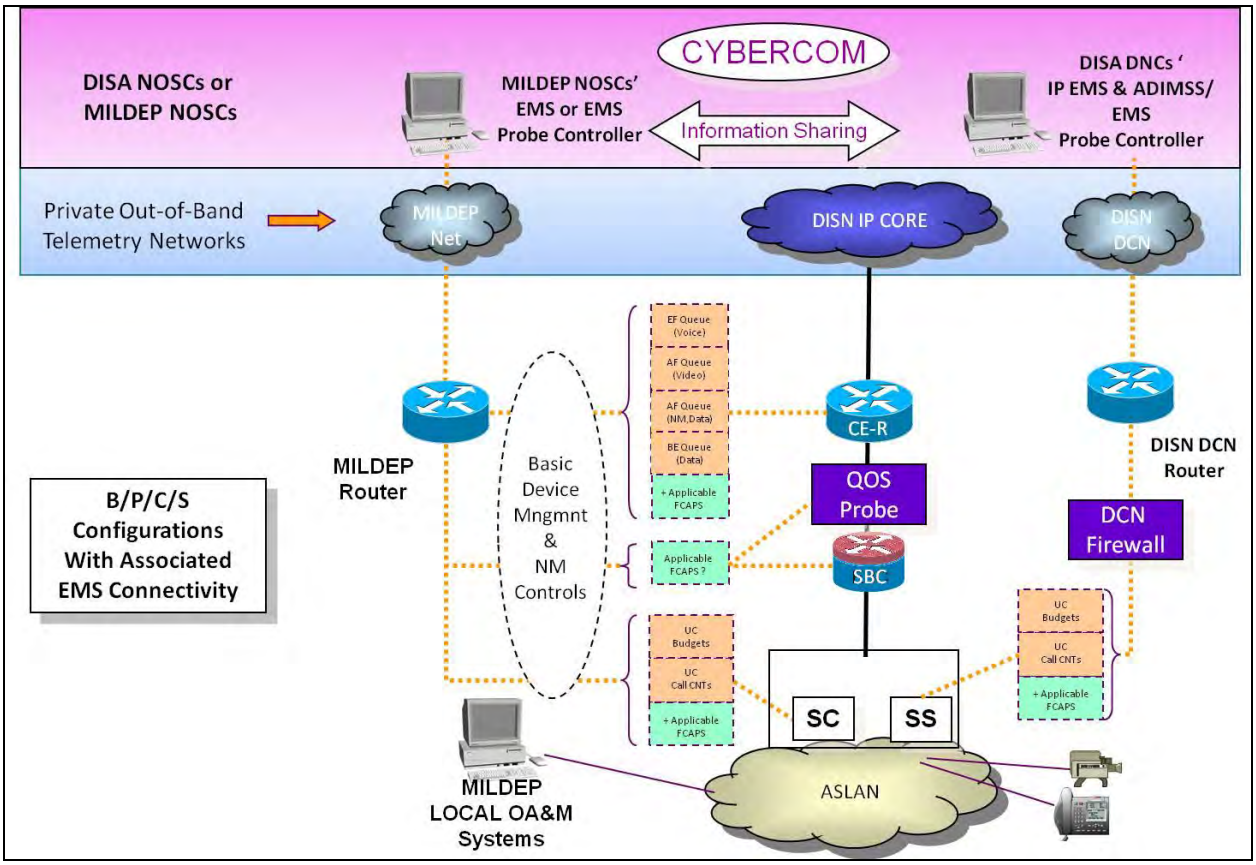

Figure 15.3-2. DISN UC E2E Solution for UC Spirals

Using the composite information shared by the DISA solution, both DISA NOCs and the MILDEP NOSCs can obtain an E2E view of the network including its various network segments and components to determine where degraded service is being experienced.

As outlined in the Joint Concept of Operations (JCONOPS) for NetOps, the NetOps Center for each network must cooperate with the other centers to consolidate and integrate information regarding the operational health and status of their networks and systems. The fusion of the information from the NetOps Centers in the theater of operations and up to USCYBERCOM will provide E2E situational awareness of the GIG to improve decision-making for the Commander, U.S. Strategic Command (CDRUSSTRATCOM) and, ultimately, for all Warfighters.

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.

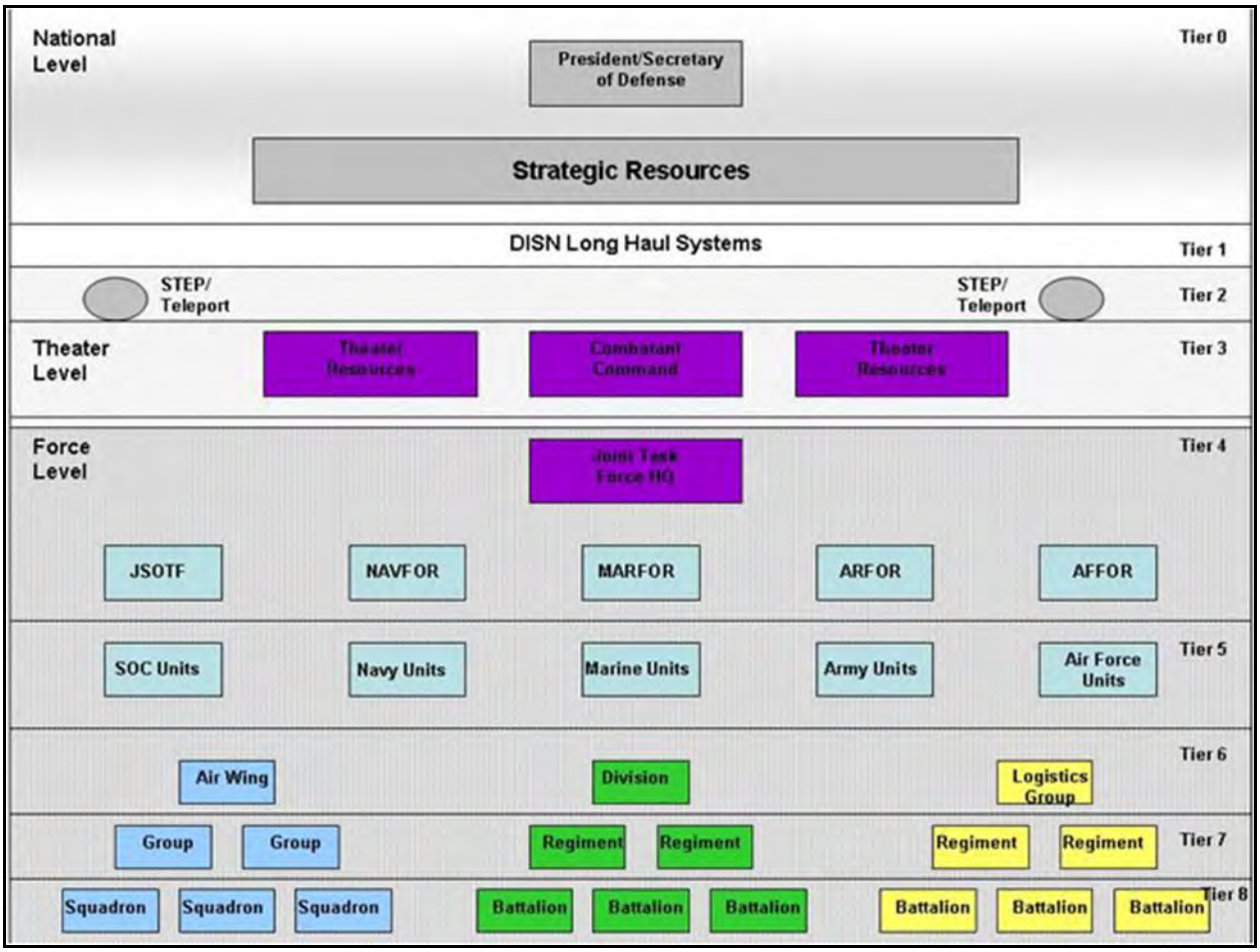

Figure A.4-3. OAN Tier Structure

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
   a. Enterprise Server
   b. Tactical Server
   c. Mobile
   d. Client
   e. Platform
   f. 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.

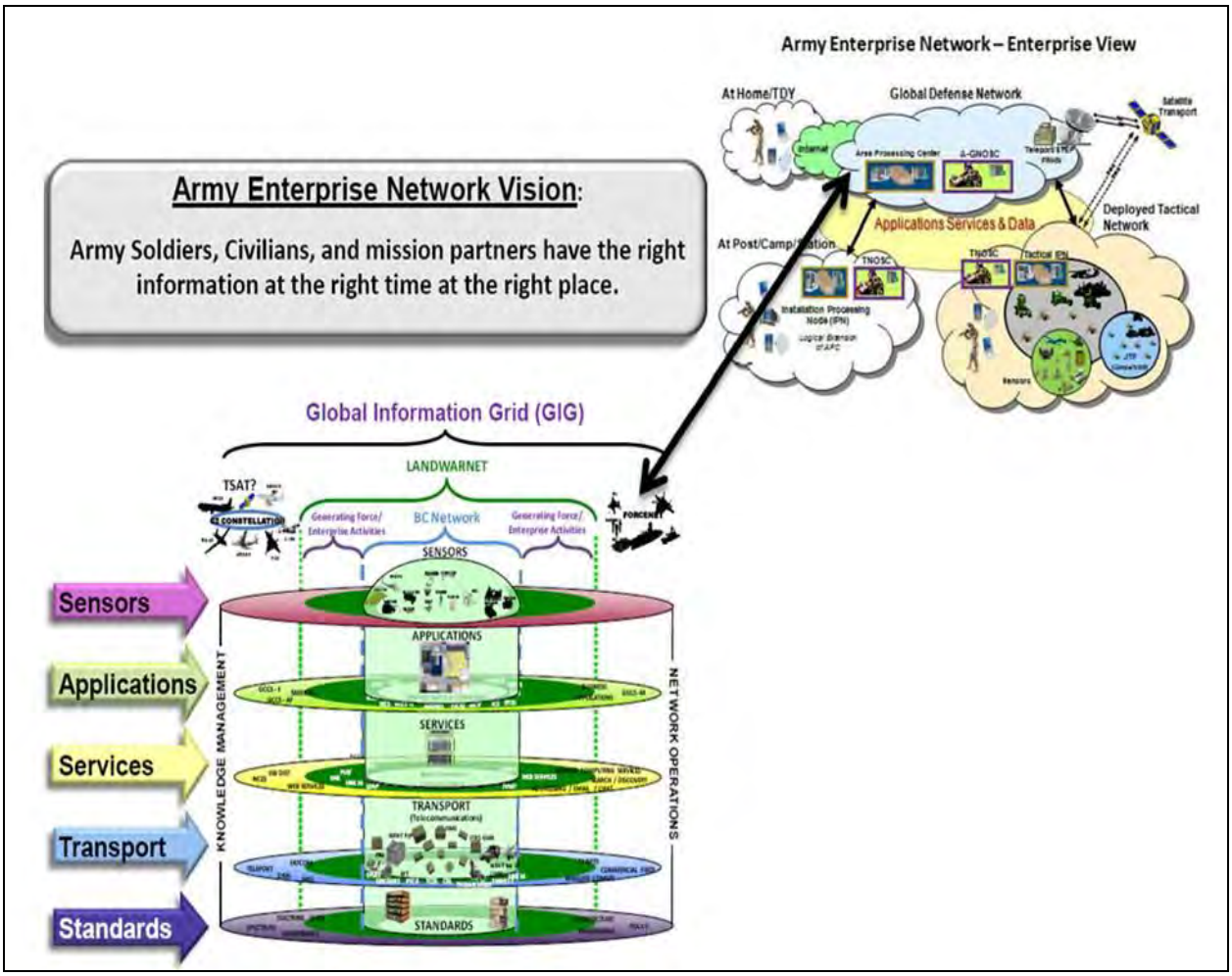

Figure A.5-1. Army Enterprise Network

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.

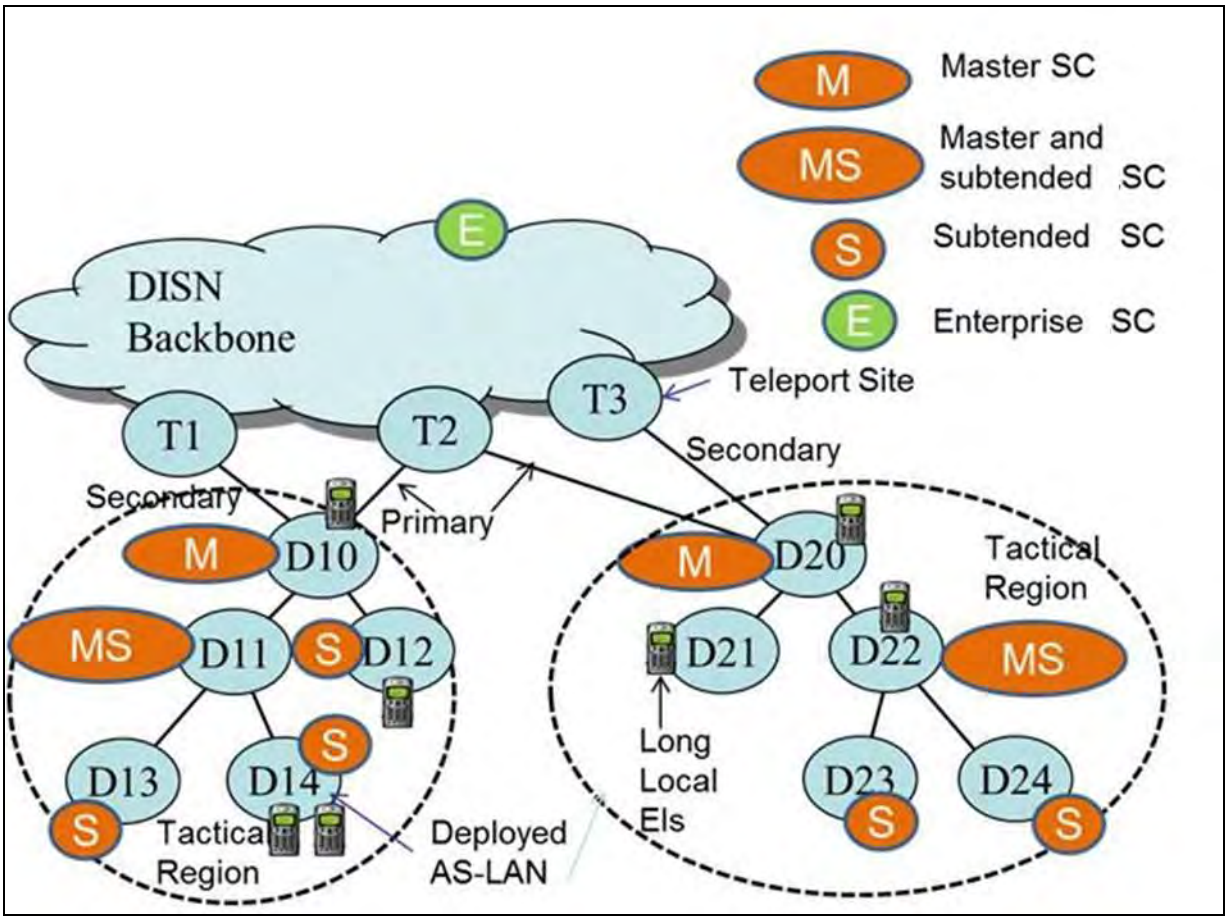

Figure A.7-1. Hierarchical Connectivity in UC

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.

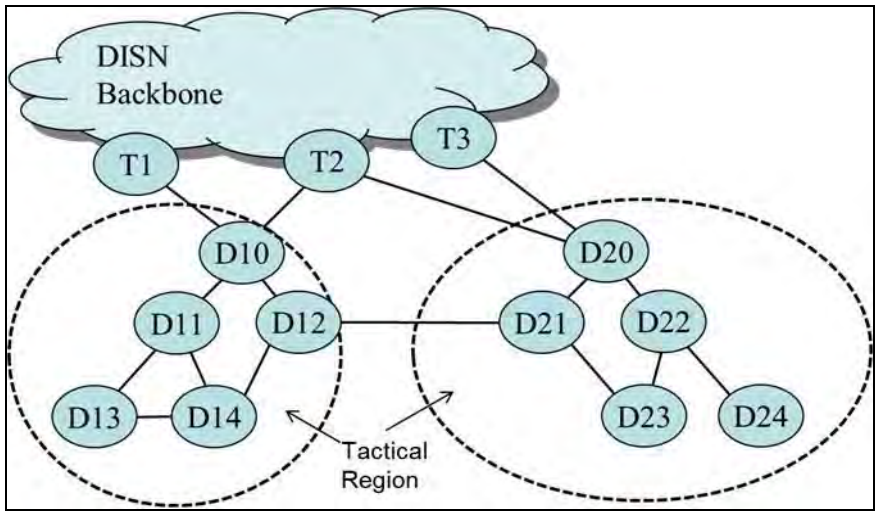

Figure A.8-1. Notional View of Tactical Region Mesh Connectivity

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.

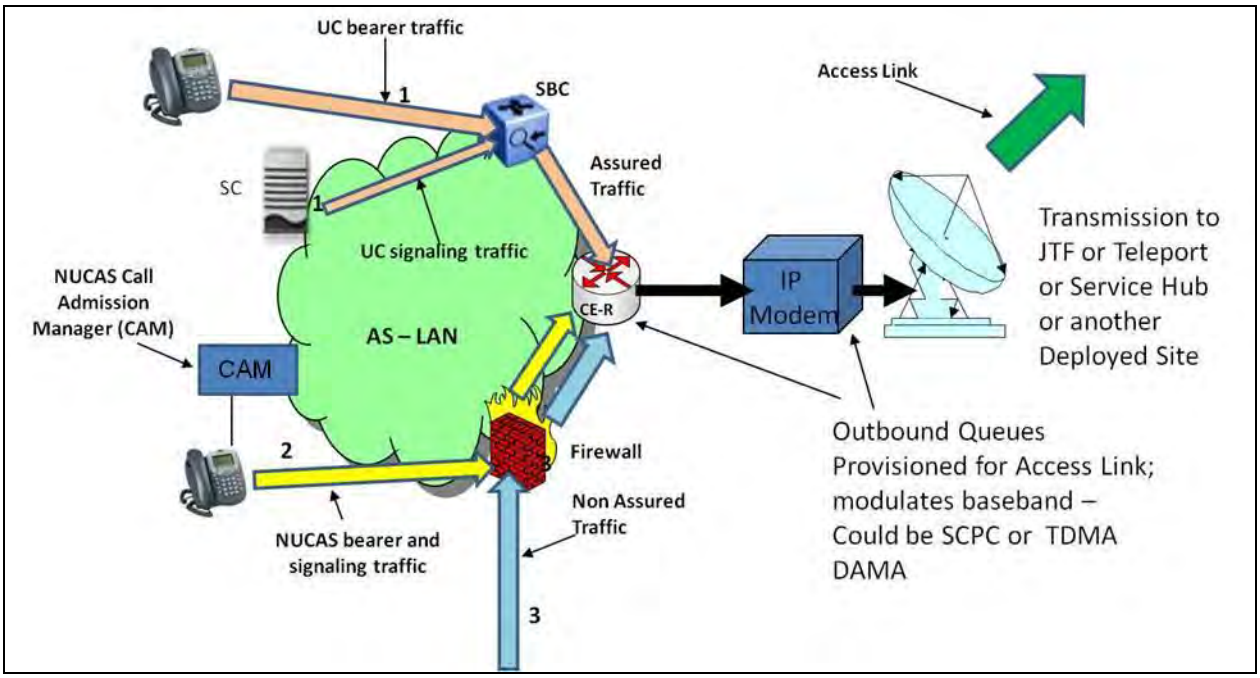

Figure A.9-1. Outbound Traffic Flow in Tactical ASLAN

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.

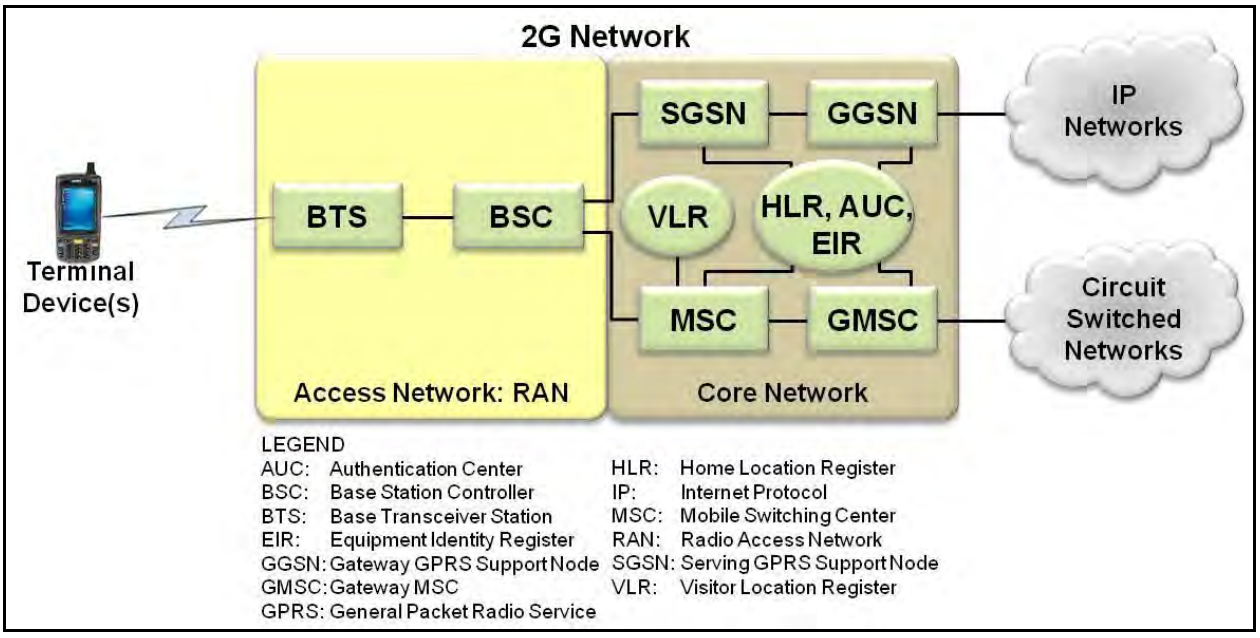

Figure A.9-2. 2G Cellular Primary Components

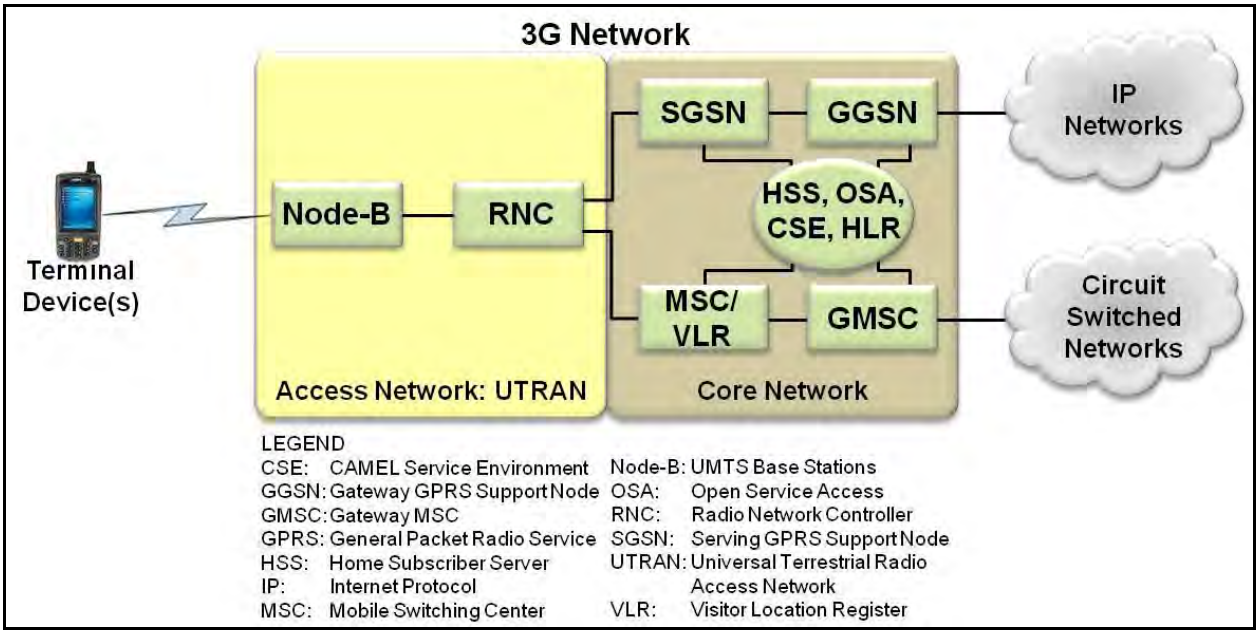

Figure A.9-3. 3G Cellular Primary Components

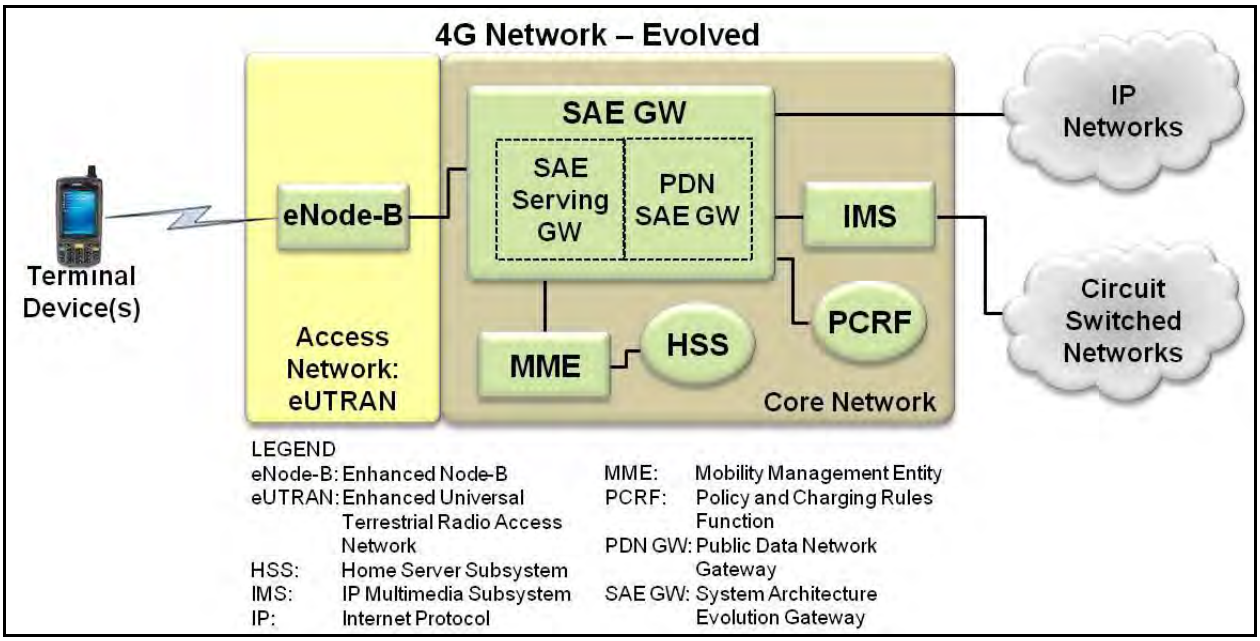

Figure A.9-4. 4G Cellular Primary Components

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.

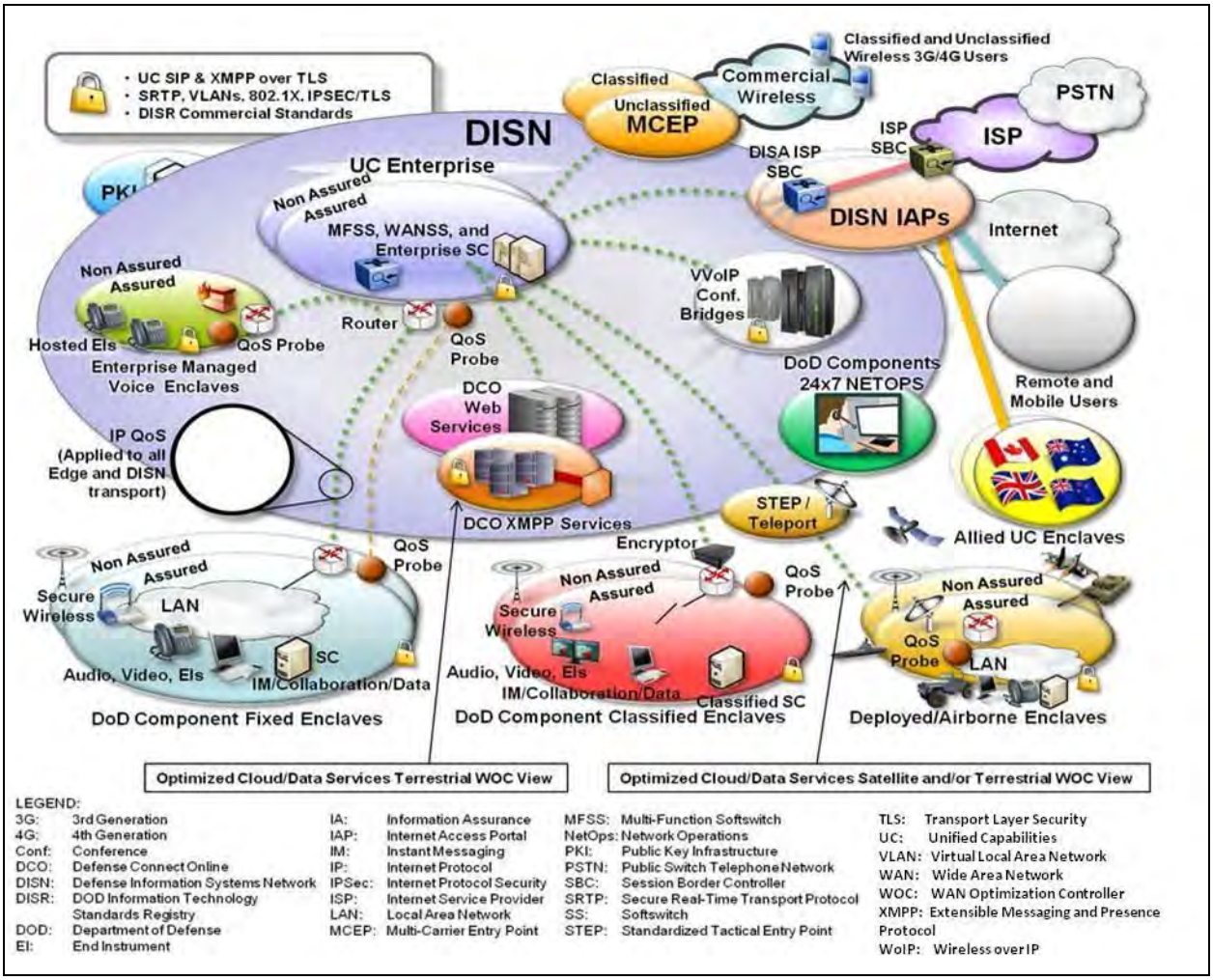

Figure A.9-5. UC Operational Framework

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.10.1.1 DCVX 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.10.1.2 DCVX 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.10.1.3 DCVX 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.

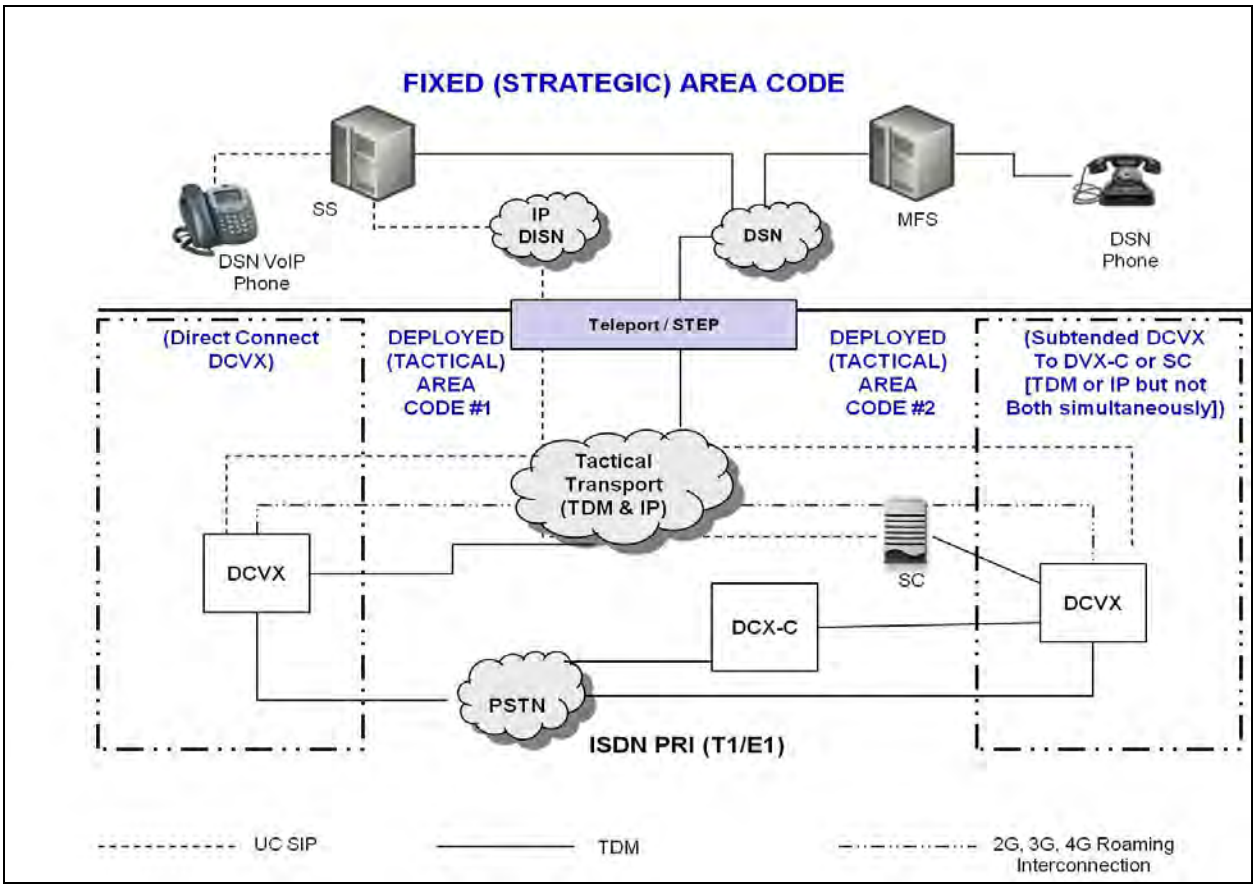

Figure A.10-1. DCVX Connection Options

A.10.1.4 Subtended 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.10.1.5 Direct 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.10.1.6 Networked 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.10.1.7 Stand-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.10.2.1 DoD 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.10.2.2 Submission 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.

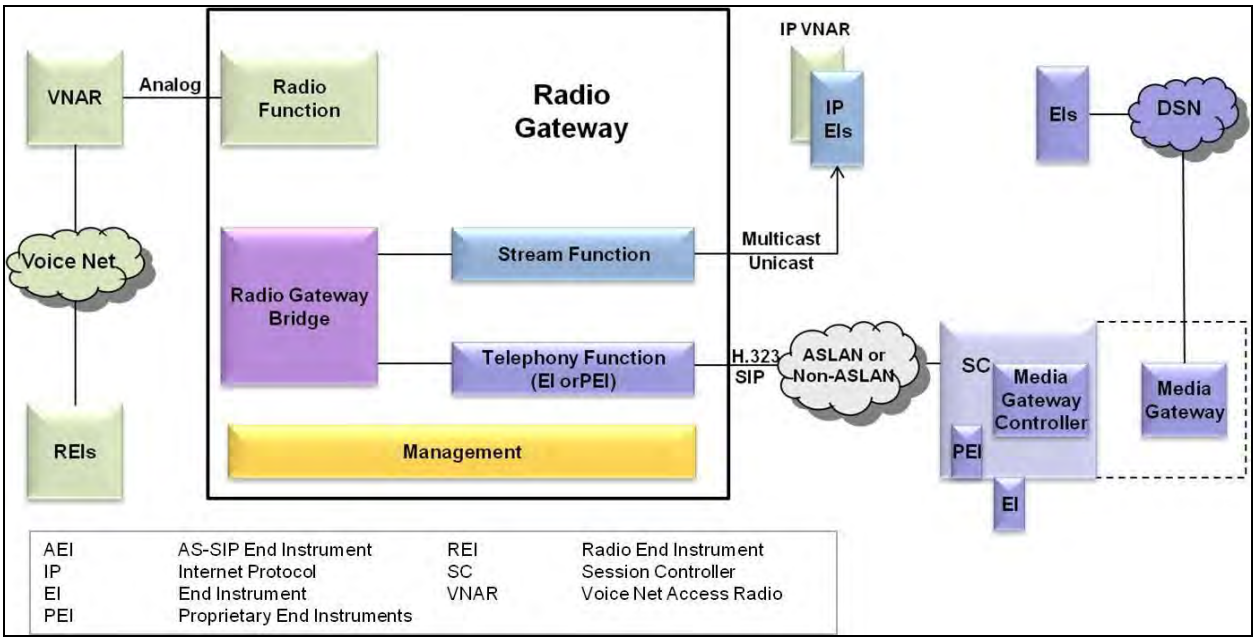

Figure A.10-2. Radio Gateway Components

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.10.3.1 Interfaces

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.

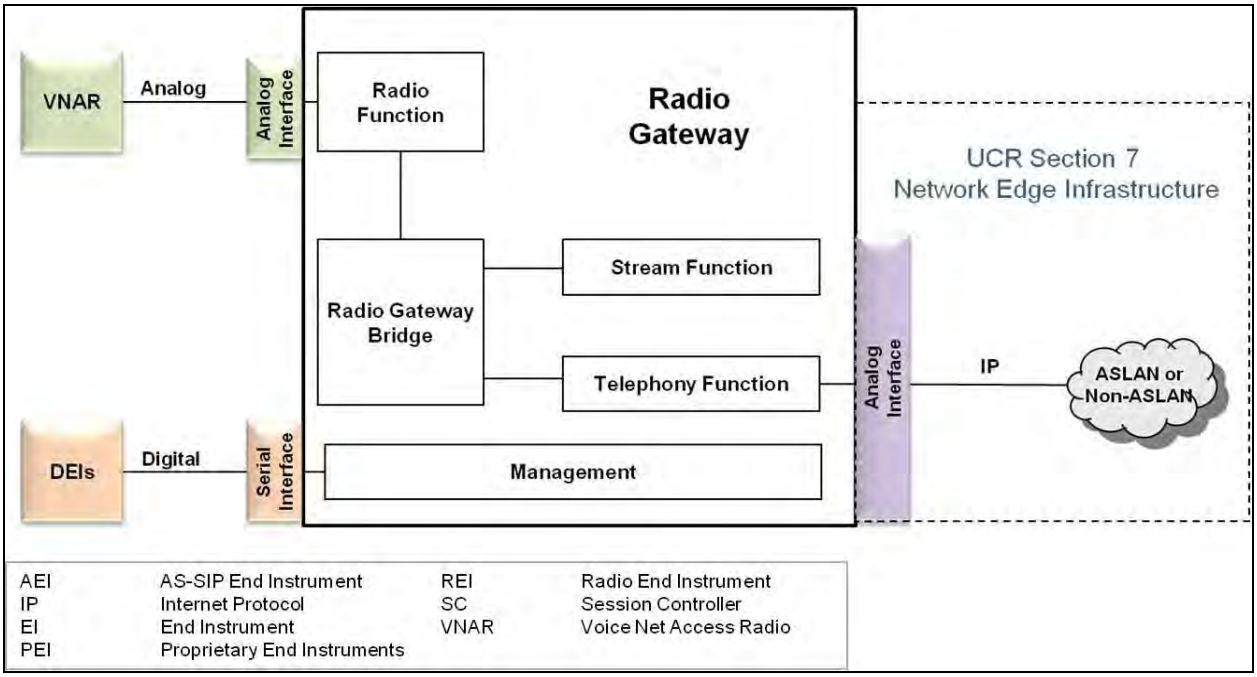

Figure A.10-3. Radio Gateway Interfaces

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.10.7.1 Codecs

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.10.8.1 WOC 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.10.8.2 Applications 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.

APPENDIX B
UNIQUE CLASSIFIED UNIFIED CAPABILITY

Figure B-1, Classified VoIP Network Design Illustration, illustrates the classified Voice over Internet Protocol (IP) (VoIP) design. The approved product types are the same as the Sensitive but Unclassified (SBU) approved product types with the exception of the Softswitch (SS), which is not needed for classified VoIP and is replaced with a dual-signaling Wide Area Network (WAN) SS capable of both H.323 and Assured Services (AS) Session Initiation Protocol (SIP) (AS-SIP) signaling, described in Unified Capabilities Requirements (UCR) 2013, Appendix B, Unique Classified Unified Capability.

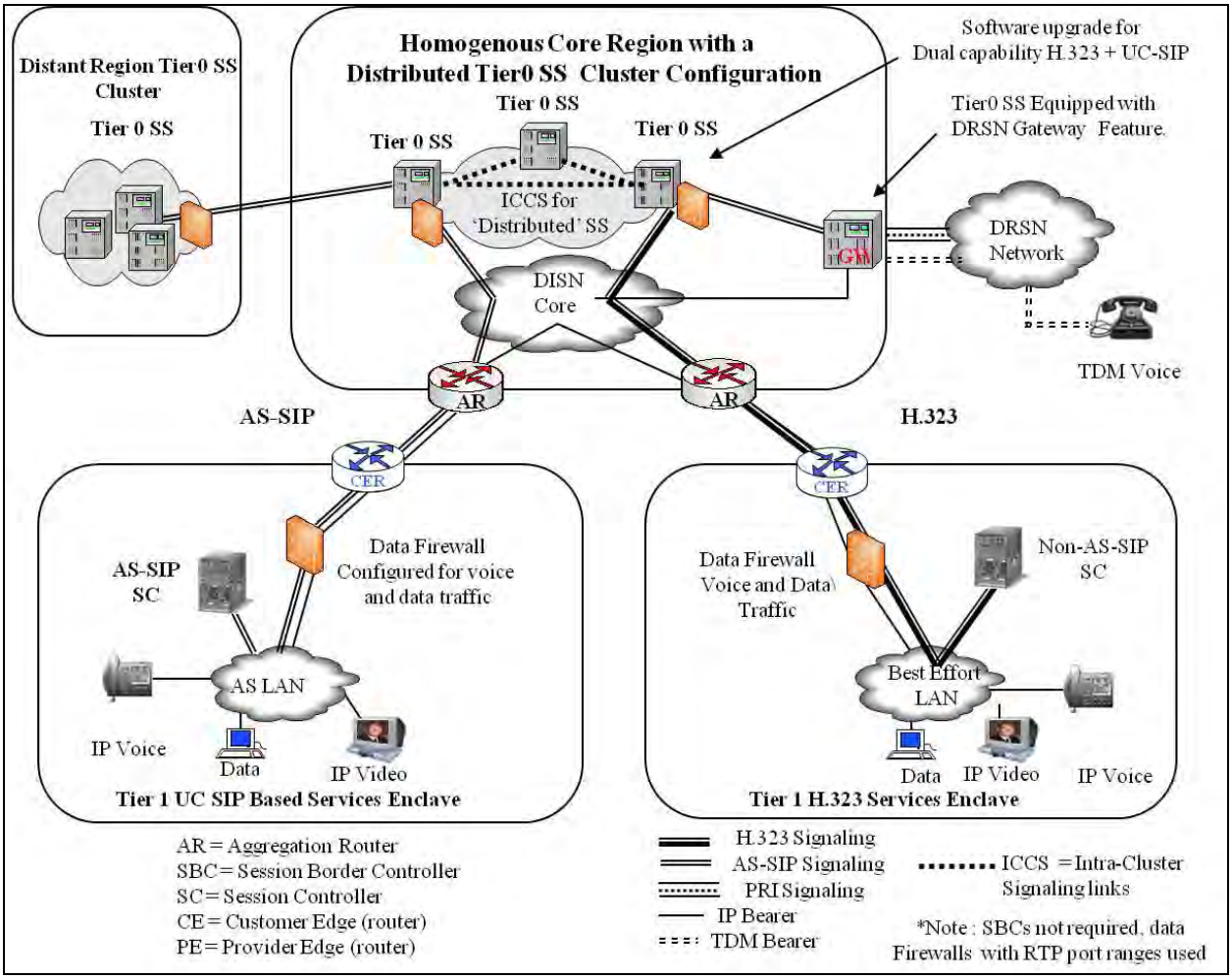

Figure B-1. DISN CVVoIP Hybrid Signaling Design

B.1 SIGNALING DESIGN

The signaling design has to provide both backward and forward technology capabilities. Thus, Channel Associated Signaling (CAS) and Primary Rate Interface (PRI) in the Defense RED Switch Network (DRSN) have to interoperate with H.323 signaling in the current Classified

Voice and Video over IP (CVVoIP) network to be followed by H.323 and AS-SIP interoperating in CVVoIP until all IP services are via AS-SIP. Once that is achieved, the DRSN interoperability must be maintained until its features can be replicated with IP technologies.

The hybrid CVVoIP signaling design is depicted in Figure B-1, DISN CVVoIP Hybrid Signaling Design.

The hybrid signaling design is constructed as a two-tier hierarchy consisting of a "local" level and a "backbone" level. At the local level, Session Controllers (SCs) are located in secure enclaves and represent the level of the signaling hierarchy closest to the End Instruments (EIs). The local level is based on a multivendor assortment of SCs. The backbone, or Tier0 signaling, level is a robust, homogeneous design based on current vendor-unique geographic cluster arrangements of Tier0 SS. The CVVoIP assured services signaling backbone will be based on the Tier0 SS cluster concept, with AS-SIP as the CVVoIP signaling method, but, during the transition period to AS-SIP-based CVVoIP, there will be segments using H.323 signaling also. Signaling interoperability between H.323 and AS-SIP will be achieved by an Approved Products List (APL) product called a Dual-Signaling Softswitch (DSSS).

The backbone Tier0 SSs represent the upper level of the signaling hierarchy and provide inter-enclave as well as inter-geographical area signaling forwarding. Some of the SCs as well as a select few Tier0 SSs provide "Managed Services" to a limited set of EIs; therefore, a Tier0 SS may have an SC function associated with it as well.

Every SC is assigned to a primary Tier0 SS and to at least one secondary Tier0 SS for automatic failover.

A Tier0 geographic cluster typically consists of at least three Tier0 SSs. The clustered SSs are connected by Intra-Cluster Communication Signaling (ICCS) links, and they automatically update each other's databases, as required, in response to configuration changes within the geographic region controlled by the cluster and, as such, can be viewed as a distributed SS. This feature provides an extremely robust Tier0 signaling design enabling automatic non-service interrupting failover in case a Tier0 SS goes down. The distance between the clustered SSs must be planned so that the maximum round-trip time (RTT) between the clustered SSs does not exceed 40 ms. Based on a propagation delay of 6 microseconds per kilometer without any other network delays being considered, this translates to a maximum theoretical transmission distance of approximately 1860 miles.

B.2 DIRECTORY (WHITE PAGES) SERVICES

The CVVoIP will have a directory services capability for searching "white pages" that allows subscribers to look up specific and applicable user information assigned to other CVVoIP subscribers. Requirements for CVVoIP Directory Services are found in Section 3.2, Directory Services ("White Pages"), for consideration by SC/SS product development teams. Systems providing CVVoIP Directory Services must be dedicated to CVVoIP and cannot also provide SBU Directory Services.

APPENDIX C
DEFINITIONS, ABBREVIATIONS AND ACRONYMS, AND REFERENCES

C.1 OVERVIEW

This glossary defines terms as they apply to the UCR 2013. It is understood that other documents or organizations may define the terms differently. These terminology definitions are not requirements and are defined to provide context for a requirement in the UCR 2013.

C.1.1 Numbers

4 Common Intermediate Format (4CIF). A video format defined in ITU-T Recommendation H.263 that is characterized by 704 luminance pixels on each of 576 lines, with half as many chrominance pixels in each direction. Four times the resolution of CIF, respectively.

16 Common Intermediate Format (16CIF). A video format defined in ITU-T Recommendation H.263 that is characterized by 1408 luminance pixels on each of 1152 lines, with half as many chrominance pixels in each direction. Sixteen times the resolution of CIF, respectively.

C.1.2 A

A-Law. A companding (compressing and expanding) method for encoding and decoding audio waveforms into/from digital data in a pulse code modulated system. A-Law is the primary companding method for E1 transmissions.

Add-On Transfer and Conference Calling. A feature set that provides the user with the capabilities to handle more than one call at a time on a given line.

Admission Control. The process by which flows are allowed to enter a network based on their level of quality of service.

Aggregate Service Class. An aggregation of service classes based on a selected set of quality of service criteria.

Annotation. Text, graphics, or free hand markings used to highlight or provide explanation to areas of interest on an image or whiteboard.

Appliance. A hardware platform with its supporting software that performs a single function or multiple functions.

Application Layer Control Protocol. See Call Control.

Approved Products List (APL). 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 8100.04. The list is published on the Joint Interoperability Test Command home page (https://aplits.disa.mil).

Approved Products List System Under Test (SUT). The set of appliances required to meet a Defense Switched Network switch certification (i.e., Multifunction Switch, End Office). Examples of a SUT include Time Division Multiplexing or circuit switch components, Voice over Internet Protocol system components (e.g., Session Controller and gateway), local area network components (e.g., routers and Ethernet switches), and End Instruments.

Assured Availability. The uninterrupted availability and protection of system and network resources by technology solutions that provide self-healing failover, diversity and elimination of critical failure points.

Assured Delivery. The ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war. Features of assured delivery include Forward Error Correction (FEC), compression, Quality of Service, Priority Based Admission Control (PBAS), Session Admission Control (SAC) or Assured Services Admission Control (ASAC).

Assured Forwarding (AF). Provides delivery of Internet Protocol (IP) packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested Differentiated Services (DS) node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value. A DS node must allocate forwarding resources (i.e., buffer space and bandwidth) to AF classes so that, under reasonable operating conditions and traffic loads, packets of an AF class x do not have a higher probability of timely forwarding than packets of an AF class y if x is less than y. [RFC 2597]

Assured Protection. Protection based on a detailed analysis of the threats and generic countermeasures (CMs), which results in the implementation of security controls addressing Access Control, Authentication, Non-Repudiation, Data Confidentiality, Data Integrity, Survivablility/Availability to protect information at rest and in transit.

Assured Service. A service (voice, video, or data) that provides assured availability, protection, and delivery. Examples of features of assured service include QoS, security, Session Admission Control (SAC), and Assured Session Admission Control (ASAC).

Assured Services Admission Control (ASAC). A process by which the quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services.

Assured Services Local Area Network (ASLAN). The Internet Protocol (IP) network infrastructure components used to provide command and control voice services to end users. It applies to switch certifications for Multifunction Switches, End Office Switches, Small End Office Switches, and Private Branch Exchange 1, and to certifications for Session Controllers, Multifunction Softswitches, and Softswitches. A local area network that supports IMMEDIATE/PRIORITY (I/P) users is considered an ASLAN. The ASLAN has two configurations depending on whether it supports I/P users or FLASH/FLASH OVERRIDE (F/FO) users. An ASLAN that supports I/P users is classified a Medium Availability ASLAN and the primary requirements that differentiate it from a non-ASLAN are that it requires a 2-hour power backup capability for all ASLAN components in addition to providing 0.99997 reliability. An ASLAN that supports F/FO users is classified a High Availability ASLAN and the primary requirements that differentiate it from a Medium Availability ASLAN are that it requires an 8-hour power backup capability for all ASLAN components in addition to providing 0.99999 reliability.

Assured Services Session Initiation Protocol (AS-SIP). A session signaling protocol consisting of a defined set of Session Initiation Protocol signaling standards and incorporating Department of Defense Assured Service functionality.

Assured Services Session Initiation Protocol (AS-SIP) End Instrument (AEI). A user appliance that interacts with an associated serving appliance using AS-SIP to originate, accept, and/or terminate a voice, video, and/or data session(s).

Assured Services Session Initiation Protocol (AS-SIP) Signaling Appliance. Any Department of Defense signaling appliance (exclusive of End Instruments) that supports the receipt, processing, or forwarding of AS-SIP messages. These appliances MAY support the receipt and forwarding of encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) Multipurpose Internet Mail Extension (MIME) objects.

Asymmetric DSL (ADSL). A technology for transmitting digital information on a metallic twisted pair that allows high-speed data transmission between the network operator end and the customer end. Systems allow approximately 6 Mbps downstream and approximately 640 Kbps upstream data rates, depending on line distance – up to 12,000 feet (about 2.3 miles) from the central office.

Asymmetric DSL 2 (ADSL2). Extends the capability of basic ADSL in data rates that range up to a minimum of 8 Mbps downstream and 800 Kbps upstream. Support of net data rates above 8 Mbps downstream and support of net data rates above 800 Kbps upstream are optional. ADSL2 utilizes the same bandwidth as ADSL but achieves higher throughput via data compression techniques.

Audio. The voice or sound portion of a teleconference.

Audio Add-On. A feature that allows a participant to join a videoconference via audio (telephone) only.

Audio Mixing. The process of combining two or more audio signals to produce a single composite audio signal. This allows each participant in a conference to hear all other participants simultaneously.

Audio Switching. The process of switching the audio portion of the video teleconferencing (VTC) system to be heard by all participants so that the input signal comes from the designated speaker. No other participants can be heard until they are selected as the audio source.

Automated Receiving Devices (ARD). A family of automated devices, which are customer premises equipment or network elements that attaches to the receiving end of a telephone call. Typical ARDs will have an automatic call distribution front-end, which could be as simple as a queue that handles incoming calls on a first come first serve basis. More complex ARDs can be full function Automatic Call Distributors that also include predetermined schemes and route calls based on routing criteria and, quite often, database handling instructions. Once in queue, if the call is not answered in a specified amount of time and the caller had not terminated the call, ARD can terminate the call or send the call to another location. Usually the ARD invokes a network carrier-based “take back and transfer” to the alternative location. Automated Receiving Devices do not originate calls to the network.

Availability. The fraction of the time the system is available to a service user’s requests. The time during which the system is unavailable is called downtime; the time during which the system is available is called uptime. In Internet Protocol terms, it is the percentage of time that the packet loss is less than the threshold.

C.1.3 B

Back-to-Back User Agent (B2BUA). "A back-to-back user agent (B2BUA) is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior." [RFC 3261]

Basic Rate Interface (BRI). The basic Integrated Services Digital Network (ISDN) service, consisting of two 64 kbps B-channels (bearer channels) that carry data and voice in both directions, and one 16 kbps D-channel (data channel) that carries call-control information.

Bit-Rate Allocation Signal (BAS). An 8-bit word within the frame structure of ITU-T Recommendation H.221 that is used to transmit commands, control and indication signals, and capabilities.

Bitmap. A two-dimensional array of pixels representing an image.

Blocking. The process by which a message is denied entry to a network that is caused by a lack of resources in the network.

Broadband ISDN (B-ISDN). An Integrated Services Digital Network (ISDN) offering broadband capabilities. A B-ISDN is a proposed service that may (1) include interfaces operating at data rates from 150 to 600 Mbps, (2) use asynchronous transfer mode (ATM) to carry all services over a single, integrated, high-speed packet-switched network, (3) have local area network (LAN) interconnection capability, (4) provide access to a remote, shared disk server, (5) provide voice, video, or data teleconferencing, (6) provide transport for programming services, such as cable television, (7) provide single-user controlled access to remote video sources, (8) handle voice/video telephone calls, and (9) access shop-at-home and other information services.

Broadband Streaming. For the purposes of this document, Broadband Streaming refers to the transfer of data in a continuous audio and/or video stream over a network using bandwidth from 2 to 15 Mbps.

Broadcasting. The transmission of data or information that may be simultaneously received by stations that usually make no acknowledgement.

C.1.4 C

Call. A message that is subject to Call Admission Control or Session Admission Control. A Voice over Internet Protocol (IP) or Video over IP call that is placed or answered by a Proprietary End Instrument or Assured Services Session Initiation Protocol (AS-SIP) End Instrument end user.

Call Admission Control (CAC). A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service requirements for the call.

Call Connection Agent (CCA). The CCA is part of the Session Control and Signaling functions and includes both the Interworking Function (IWF) and the Media Gateway Controller. As a result, the scope of the CCA includes the following areas:

1. Control of Assured Services Session Initiation Protocol (AS-SIP) sessions within the network appliance.
2. Support for public switched telephone network (PSTN) and Voice over IP (VoIP) signaling protocols.
3. Protocol interworking of signaling protocols (e.g., AS-SIP⟺DoD Common Channel Signaling System No. 7 interworking) through the CCA IWF control of Media Gateways that link the network appliance with Time Division Multiplexing network elements.
4. Support for interactions with other network appliance functions.
5. Support for assured services voice and video calls.
6. Support for assured services user features and services.

Call Control. Establishes, modifies, and terminates sessions (e.g., multimedia conferences). It can invite participants to existing sessions, such as multicast conferences. (Referred to as Application Layer Control Protocol in RFC 3261.)

Call Forwarding Variable (CFV). This feature allows ROUTINE precedence calls attempting to terminate to a line to be redirected to another customer-specified line served by the same office or by another office for Defense Switched Network and/or commercial.

Call Hold. A feature that provides the capability for the user to hold a call for an extended period, and then return to the call, with or without making another call.

Call Stateful. A proxy is call stateful if it retains state for a dialog from the initiating INVITE to the terminating BYE request. A call stateful proxy is always transaction stateful, but the converse is not necessarily true. [RFC 3261]

Call Waiting. A feature whereby a line in the talking state is alerted by a call waiting tone when another call is attempting to complete to that line. The call waiting tone is only audible to the line with the Call Waiting feature activated. Audible ringing is returned to the originating line.

Camera. In television, an electronic device using an optical system and a light-sensitive pickup tube or chip to convert visual signals into electrical impulses.

Cancel Call Waiting. A feature that allows the customer with Call Waiting service to inhibit the operation of call waiting for one call.

Cascading. The process of providing a video teleconferencing (VTC) conference involving more than one Multipoint Control Unit (MCU), so that information must pass not only between Conferencing Terminal Unit (CTU) and MCU, but also from one MCU to another. The ability of an MCU to participate in a conference involving more than one MCU is optional and is called cascading.

Certificate Path. A sequence of certificates that connect the target certificate to one of the relying party's trust points. Construction of the path is known as path development and verification of that path providing a chain of trust and is known as path processing. A target certificate belongs to an end-entity that either sent a signed message to the relying party or to which the relying party desires to send an encrypted message. This is also called a certificate chain.

Certificate Trust List (CTL). A predefined list of items that have been signed by a trusted entity. All items in the list are authenticated and approved for use by the signing entity.

Chair Control. A method of providing the capability for one of the conferencing terminal units (CTUs) involved in a conference to exercise some measure of authority over the conference, particularly in making the decision of which video will be broadcast to the other CTUs.

Chair-Control Conferencing Terminal Unit (CTU). An enhanced CTU possessing the capability to exert a certain measure of authority over the operation of the multipoint conference. The chair-control assignment may be prearranged, assigned by an operator or by protocol during the call. The person controlling need not be the actual chairperson of the meeting.

Chat. The capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from instant messaging (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.

Chrominance. The color component of a pixel. The Cb and Cr components in YCbCr. The A and B components in CIElab.

Circuit Emulation Service (CES) Over Internet Protocol (IP). Trunking of time division multiplexing (TDM) data between IP points. Circuit Emulation Service over IP provides a method to transport T1/E1 or T3/E3 streams over an IP network. The service is similar to CES over asynchronous transfer mode (ATM) that has been in the industry for some time but the transport layer is IP. The circuit may include compression, which may include silence suppression, and echo cancellation. The CES over IP is also known as Circuit Emulation Service over Packet.

Classified. Any information that has been determined to require protection against unauthorized disclosure to avoid harm to U.S. national security. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information, referred to as "classified information."

Classifier. An entity that selects packets based on the content of packet headers according to defined rules. [RFC 2475]

Client Management Entity (CME). A data link client that uses Client ID 0x00 to send a complete list of locally registered clients and their optional extra capabilities.

CODEC. Acronym for Coder/Decoder. In video teleconferencing, an electronic device that converts analog signals, typically video or voice, into digital form and compresses them into a fraction of their original size to save frequency bandwidth on a transmission path. It also performs the inverse operation; decompressing received signals and converting them back to analog.

Common Channel Signaling System No. 7 (i.e., SS7 or CCS7). A global standard for telecommunications defined by the International Telecommunications Union (ITU) Telecommunication Standardization Sector (ITU-T). The standard defines the procedures and protocol by which network elements in the public switch telephone network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wire line call setup, routing, and control. The ITU definition of SS7 allows for national variants, such as the American National Standards Institute and Telcordia Technologies standards used in North America, and the European Telecommunications Standards Institute standard used in Europe.

Common Intermediate Format (CIF). See Full Common Interface Format Component in CIElab.

Compression. See Data Compression.

Conditional Requirement [Conditional]. A requirement that addresses features and capabilities that are not considered critical for DoD mission support based on DoD policies. However, it is recognized that such features and capabilities do have utility for some users or for specific operations. To ensure interoperability and consistency of these features and capabilities across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the appliance shall perform and meet the specifications as identified in the appropriate section of UCR 2013.

Conditional – Deployable. A variation of the "Conditional" case, where the requirement is Required for Fixed appliances, such as Session Controllers (SCs) in Fixed DoD networks, but is Conditional for Deployable appliances, such as SCs in Deployable DoD networks. In other words, "Conditional – Deployable" means "Required for Fixed appliances, but Conditional for Deployable appliances."

Conference Call. A telephone meeting that involves three or more telephone lines connected via an audio conference bridge. Also known as audio teleconferencing.

Conference Calling. A feature that allows the user to establish a call involving up to six conferees (including the user).

Conferencing. Programs and meetings for purposes such as presenting and exchanging information, comparing views, learning, planning, or decision making. Conferences can be held in one location or conducted simultaneously at multiple locations and linked together by telecommunications systems contains images, annotations, or pointers.

Conferencing Terminal Unit (CTU). Video teleconferencing equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It does not include input/output devices, embedded and non-embedded cryptographic devices, network interface equipment, end-to-network signaling, network connections, or the network itself.

NOTE: The scope of this profile is broader than the scope of the CTU because the scope of the profile includes cryptographic devices and other items that the CTU does not include.

Congested Condition. One hundred percent utilization of bandwidth on the link, or links, under test. Link traffic may be any combination of real time services traffic and data, up to and including specified traffic engineering (i.e., 25 percent voice, 25 percent video, and up to 100 percent data.

Content. Data that is transmitted recorded and/or stored as "audio," "video," "images," "high-resolution graphics," and "slides."

Content Delivery. The act of being able to route requests for video on-demand (VoD) to the clients nearest a VoD server or cache. Also being able to distribute content to remote VoD or cache servers on-demand or on a scheduled basis.

Continuous Presence. Enables each site to see multiple sites simultaneously. The participants' video window is divided into two, four, six, nine, or more sections that display preselected sites.

Control Plane. Quality of service mechanism to provide the ability to route data correctly and perform actions during session establishment and operation to allow a network to meet quality of service needs in the data plane. This plane defines the configuration, start-up conditions, and instability conditions of the control protocols, which may include routing protocols, multicast protocols, link management, and Multiprotocol Label Switching protocols.

Converged. All types of services, defined by the GIG Enterprise Service Profile Document (GESP), exist simultaneously on the same Internet Protocol (IP) network.

Converged Local Area Network (CLAN). A local area network (LAN) is an Internet Protocol (IP) network, composed of routers and LAN switches, that is used to connect nodes that are geographically close, usually within the same building. In a wider view of a LAN, multiple LANs are interconnected in a geographically compact area, usually by attaching the LANs to a higher speed local backbone called a campus area network (CAN). A CAN is larger than a LAN but smaller than a metropolitan area network (MAN) or wide area network (WAN). A CLAN is a LAN that supports multiple types of IP services. In the DoD, the CLAN supports voice, video, and data services as a minimum. The CLAN is not intended to support IMMEDIATE/ PRIORITY (I/P) users and the requirements associated with a CLAN are those that are typical for commercial voice and video CLANs to include commercial grade power and availability requirements.

Converged Network. An Internet Protocol (IP) network used to transmit a combination of voice, video, and/or data services.

Converged Network Adapter (CNA). Converged network adapters consolidate the Ethernet data networking capabilities of a 10 Gigabit Ethernet (GbE) network interface card (NIC) with the storage networking capabilities of a Fibre Channel (FC) Host Bus Adapter (HBA) onto a single 10GbE Ethernet adapter. The CNAs provide traditional data networking for network file system (NFS), Common Internet File System (CIFS) and Internet Small Computer System Interface (iSCSI) storage protocols concurrently with Fibre Channel over Ethernet (FCoE) storage networking. The CNAs provide significant data center cost savings while preserving an existing investment in FC storage. The CNAs are also used in Data Center Bridging (DCB) network infrastructures.

Cryptographic Boundary. An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic Module. The set of hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation, and are contained within the cryptographic boundary.

Cryptographic Resynchronization. The process by which the conferencing terminal unit has the capability to automatically send a signal for resynchronization to the cryptographic device whenever resynchronization is needed.

Customer Edge Router (CE Router). A router located at the boundary between the Edge Segment and the Access Segment of the wide area network. The CE Router provides traffic conditioning, bandwidth management on a granular service class (i.e., voice, video) basis, and quality of service using per-hop behaviors. A base/post/camp/station may have a single CE Router or multiple CE Routers based on the local architecture.

C.1.5 D

Data Communications Port. A port used to transfer information between functional units by means of data transmission, according to a protocol.

Data Compression. Increasing the amount of data that can be stored in a given domain, such as space, time, or frequency, or contained in a given message length. [FED-STD-1037C]

Data Plane. Quality of service mechanism to provide the ability to manage and forward data packets, including one or more of the following: packet marking and re-marking, implementing scheduling and packet drop priorities, metering the traffic and performing congestion control, and policing and shaping the traffic. This plane defines the configuration, start-up conditions, and instability conditions of the data traffic including the traffic, collection of network elements, links between network elements, and interface profile.

Data Port. See Data Communications Port.

Data Rate. In digital data communications, the rate at which data (bits in this case) is transmitted, usually expressed in bits per second.

Default Best Effort (BE). This is the common, best-effort forwarding behavior available in existing routers. When no other agreements are in place, it is assumed that the packets belong to this aggregate. Such packets may be sent into a network without adhering to any particular rules, and the network will deliver as many of these packets as possible and as soon as possible, subject to other resource policy constraints. This forwarding behavior is not to be used for VoIP.

Defense Switched Network (DSN). An interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voiceband data, and dial-up video teleconference for end-to-end command use and DoD authorized IMMEDIATE/PRIORITY (I/P) and non-I/P users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal service.

Denied Originating Service. A system feature that provides the capability to deny call originations selectively to individual lines.

Deployable Network Element (D-NE). Any network element used in the Deployable network. A D-NE can be used for long local, encapsulated time division multiplexing, and proprietary Internet Protocol trunks.

Deployable Private Branch Exchange (PBX). A PBX that is allowed to connect to the Defense Switched Network via a Standard Tactical Entry Point/Teleport. Deployed PBX Type 1s do not support tandem calls and they are not approved to support FLASH and FLASH OVERRIDE users as their only means of communication. FLASH and FLASH OVERRIDE users shall be supported by other means such as a long local.

Deployable Voice Exchange (DVX). A Deployable switch with military-unique features capabilities to support the assured service requirements used for rapid deployment situations and contingencies in the deployable environment. The DVXs can be either DVX Commercial Off-the-Shelf (COTS) (DVX-C), or DVX legacy (DVX-L) Tactical (TRI-TAC) systems. Normally, a DVX is connected to the Defense Switched Network (DSN) using gateway trunks routed through a Standard Tactical Entry Point/Teleport location. It can be connected directly to the DSN (Tandem Switch/ Multifunction Switch/End Office/Small End Office), if it is to be used as a temporary solution for either of the following:

- An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.
- A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

Deployable Voice Exchange – Commercial Off-the-Shelf (DVX-C). A Government-deployable commercial switch that may have been modified for use within deployable environments to provide military-unique features.

Deployable Voice Exchange – Legacy (DVX-L). A Government-deployable legacy voice switching system, such as the Common Baseline Circuit Switch and Unit Level Circuit Switch.

Differential Treatment. A mechanism that allows differential handling of packets in the Edge and Core nodes. It also includes providing differential treatment at the time of resource reservation and provisioning requests.

Differentiated Services (DS). A quality of service delivery model, in which the flows are classified, policed, marked, and shaped at the edges of a DS domain. The nodes in the core of the network handle packets according to the per-hop behavior that is selected based on the contents of the DS field (Differentiated Services Code Point) in the packet header.

Differentiated Services Architecture. Contains two main components. One is the fairly well understood behavior in the forwarding path and the other is the more complex and still emerging background policy and allocation component that configures parameters used in the forwarding path. The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single Differentiated Services Code Point (DSCP). Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DSCP. [RFC 2475]

Differentiated Services (DS) Field (DS Field). The six most significant bits of the Internet Protocol, version 4, Type of Service octet or the Internet Protocol, version 6, traffic class octet.

Differentiated Services Code Point (DSCP). A value that is encoded in the Differentiated Services (DS) field and that each DS node must use to select the per-hop behavior that is to be experienced by each packet it forwards.

Directed Call Pickup. A feature that permits a user to dial a code and station number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up.

Directed Inward Dial (DID). A feature that allows an incoming call to reach a specific Private Branch Exchange (PBX) station line without attendant assistance. With DID, the switch seizes a DID trunk and outpulses the station line number to the PBX. If the called station's line is idle and not restricted from receiving terminating calls, the PBX alerts the called station and returns audible ringing on the incoming connection. If the called station's line is busy, the PBX returns a busy tone. If the called station is restricted from receiving terminating calls, the PBX routes the incoming call to an announcement, reorder tone, or to the attendant.

Directly Connected Conferencing Terminal Unit (CTU). A CTU that is directly connected to the multipoint control unit (MCU) in question, rather than through another MCU. It may or may not be collocated with the MCU.

DISN Video Services, Global (DVS-G). The DVS-G is a service provided by the Defense Information Systems Agency. It is meant to provide a bridging service for Department of Defense video teleconferencing (VTC) users. It uses industry standards for interoperability and multipoint VTC requirements. The DVS-G has three operational areas—the continental United States, Europe, and Pacific.

DISN Video Services II (DVS-II). The DVS-II is a service provided by the Defense Information Systems Agency. It provides an Internet Protocol and Integrated Services Digital Network (ISDN) bridging service. It uses industry standards for interoperability and multipoint video teleconferencing (VTC) services. It will deliver enhanced services that are video centric in nature to facilitate the use of VTC communications for Department of Defense VTC users. The DVS-II has three operational areas—the continental United States, Europe, and Pacific.

Disruptive. A disruptive action is one that prevents a given quantity of end instruments from placing or receiving a session for more than 5 minutes.

DoD Directives. Broad DoD policy documents containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities.

DoD Secure Communications Devices (DSCDs). Hardware devices that, when placed in the secure mode, protects the transmission of classified voice, data, or facsimile over the Defense Switched Network or other connected networks to another compatible DSCD.

Downspeed. For Integrated Services Digital Network (ISDN) conferences, the ability of a coder/decoder (codec) to carry on a conference, uninterrupted, at a lower ISDN rate, should one ISDN line or channel suddenly fail during a call.

C.1.6 E

E-911 Management System. A UC appliance that interfaces with Session Controllers (SCs) to enable reliable user locations to be provided to emergency response dispatch centers when a 911 call is made from a UC end instrument (EI).

Edge Label Switch Router (eLSR). The eLSR provides the edge function of multiprotocol label switching (MPLS). The eLSR is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The eLSR functions as an MPLS provider edge (PE) node in an MPLS network. The eLSR is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The eLSR uses Internet Protocol routing toward the customer interface and "label swapping" toward the MPLS core. The term, label edge router, is used interchangeably with eLSR.

EIA-449 (formerly RS-449). The EIA-449 serial mechanical interface standard was for transmission of balanced and unbalanced signals between a variety of computer, media, and multimedia peripherals. The EIA-449 allows a maximum data rate of 10 megabits per second and uses a 37- or 9-pin connector.

(NOTE: EIA-449 has been replaced by TIA/EIA-530; however, equipment that implements this interface is still in use.)

Elastic Service. A service that has high tolerance for packet loss, delay, and jitter (i.e., delay variation) at packet and overall message level. This service can tolerate a wide variation in the throughput.

Electronic Industries Alliance (EIA). A U.S. commercial standards organization. The abbreviation Telecommunications Industries Association (TIA)/EIA (which replaces the obsolete designation "RS") precedes a technical recommendation's numerical designation. An example is TIA/EIA-232-F, indicating its acceptance by both those bodies, replacing RS-232.

Embedded Encryption. Encryption integrated into the conferencing terminal unit (CTU).

Emergency Service. A feature that provides a 3-digit universal telephone number (911) that gives the caller access to help and support from an emergency service bureau.

Encapsulated Time Division Multiplexing (TDM). T1/E1 or Fractional T1/E1 encapsulated within an alternate transport mechanism that provides assured bandwidth for both signaling and bearer channels.

Encoder. A device that converts plain text to equivalent cipher text by means of a code.

Encryption. The process of converting plain text into unintelligible form by means of a crypto system.

End Instrument (EI). A user appliance that initiates, accepts, and/or terminates a voice or video session. End instruments may be standalone applications or may be used in conjunction with other applications (e.g., softphone). They may provide a single service (e.g., voice or video) or multiple services (e.g., videophone). In addition, EIs may signal the Session Controller (SC) with standardized protocols or proprietary protocols.

The EI is the primary user interface to customers for voice or video and is the originating or terminating endpoint for all voice or video sessions. It is the appliance at which the user assigns the precedence to the voice or video session, and the EI is responsible for collecting and disseminating the user authentication information to the SC. Finally, the EI is the point at which the network level Class of Service markings are set based on instructions from the SC.

End Office (EO). A legacy central office at which user lines and trunks are interconnected, providing long-distance service by interconnecting with Defense Switched Network (DSN) nodal switches. End Office switches provide users with switched call connections and all DSN service features, including Multilevel Precedence and Preemption.

A switch that is integral to the DSN and serves as a primary switch for long-distance services for either an installation or group of installations in a geographic area by interconnecting users to the DSN nodal switches.

End Terminal (ET). Optical terminal capable of terminating up to 80 channels in one direction.

Enterprise Services Area (ESA). The geographic region that encompasses a centralized Enterprise Session Controller together with all of the DoD Component sites that Enterprise Session Controller serves.

Enterprise Session Controller (ESC). Centrally located Session Controller that provides UC services to multiple DoD Component sites.

Ethernet. Popular network hardware standard that uses data transfer rates of either 10 megabits per second (Mbps) or 100 Mbps.

Expedited Forwarding (EF). The forwarding treatment for a particular Differentiated Services (DS) aggregate where the departure rate of the aggregate's packets from any DS node must equal or exceed a configurable rate. The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. If the EF per-hop behavior is implemented by a mechanism that allows unlimited preemption of other traffic (e.g., a priority queue), the implementation shall include some means to limit the damage EF traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit shall be discarded. [RFC 3246]

Explicit Routing. In explicit routing, the entire list of nodes traversed by the label switched path is specified in advance. The path specified could be optimal or not, but is based on the overall view of the network topology and, potentially, on additional constraints. This is called constraint-based routing. Along the path, resources may be reserved to ensure quality of service. This permits traffic engineering to be deployed in the network to optimize use of bandwidth.

C.1.7 F

Failover Type 1 Session Controller (F1SC). 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.

Failover Type 2 Session Controller (F2SC). 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.

Fast Ethernet. A high-speed Ethernet network that uses data transfer rates of 100 megabits per second.

Fiber Maintenance Margin. The additional margin allocated to the fiber network to warrantee the continuous operation to the end of life of the Dense Wave Division Multiplex (DWDM) system. This Fiber Maintenance Margin does not include any margins for DWDM seller's equipment.

Fiber Span. The span loss is the attenuation between Dense Wave Division Multiplex (DWDM) equipment at adjacent DWDM locations (i.e., Optical Line Amplifier (OLA), Reconfigurable Optical Add Drop Multiplexer (ROADM), and End Terminal). The span loss consists of the outside plant (OSP) loss, the intraoffice loss, and the fiber maintenance margin. The OSP loss is the loss from the Fiber Service Delivery Point (FSDP) to FSDP. The intraoffice is from FSDP to DWDM equipment as illustrated in Figure C.1.1. The entrance/exist points of the DWDM equipment are the reference points MPI-S/R according to ITU-T Recommendation G.692.

Fixed Wireless End Instrument (WEI). Those WEIs that access a single wireless local area network (WLAN) access system (WLAS) for the duration of the session and are not expected to traverse between WLASs so that handoffs are required.

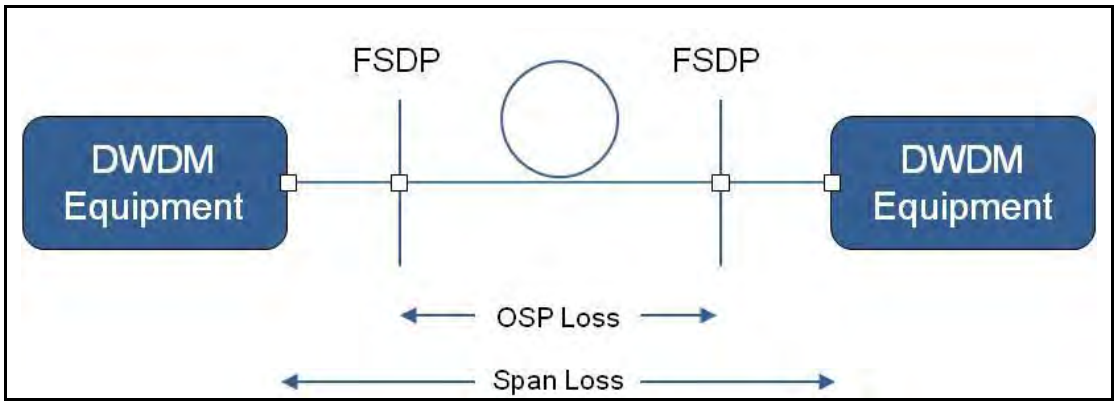

Figure C.1-1. Difference Between Outside Plant Loss and the Span Loss

FLASH and FLASH OVERRIDE Users. A special class of users who have access to the Defense Switched Network for "essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness." This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders.

Flow. A group of packets with similar attributes as defined by a subset of the parameters in the Internet Protocol (IP) header of each packet.

Forward Equivalence Class (FEC). Each multiprotocol label-switching router independently selects the next hop for a given FEC. An FEC describes a group of packets of the same type; all packets assigned to an FEC receive the same routing treatment. An FEC can be based on an IP address route or the service requirements for a packet, such as low latency.

Frame. (1) When referring to an image, the set of all the picture elements in an image. (2) When referring to ITU-T Recommendation H.221, a frame consists of 80 octets (bytes) of multiplexed signals. This is opposed to the term field referring to interlaced television pictures where 60 fields per seconds considered full motion compared to 30 frames per second for our case of computer displays.

Frame Alignment. In the profile, frame alignment refers to the ITU-T Recommendation H.221 frame, not the image frame.

Frame Alignment Signal (FAS). In the transmission of data frames, a distinctive sequence of bits used to accomplish frame alignment. In ITU-T Recommendation H.221, this signal also contains additional bits for status, control, and error detection.

Freeze-Frame Image. A frame of visual information selected from a video signal and processed through the video codec, usually for transmission to remote sites.

Full Common Intermediate Format (FCIF). A video format defined in ITU-T Recommendation H.261 that is characterized by 352 luminance pixels on each of 288 lines, with half as many chrominance pixels in each direction.

Future Narrowband Digital Terminal/Secure Communications Interoperability Protocol (FNBDT/SCIP). A protocol used to conduct a secure session with another FNBDT/SCIP capable device. SCIP and FNBDT are synonymous terms and refer to the protocols currently documented in the SCIP series of documents (e.g., SCIP-215, 216). The current preference is to use SCIP because it more accurately reflects a protocol (layer 7) as opposed to the use of FNBDT, which implies a terminal type.

C.1.8 G

Gatekeeper. An H.323 entity that provides management functions, such as address translation and control access for terminals and other endpoints.

Gateway. An H.323 entity that provides real-time communication between H.323 terminals and terminals on other networks, such as Integrated Services Digital Network or Public Switched Telephone Network.

a. The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction, (e.g., P.09 means nine calls out of 100 will be blocked). Grade of Service (GOS) may be viewed independently from the perspective of incoming versus outgoing calls and is not necessarily equal in each direction. GOS may be applied to the busy hour or to some other specified period or set of traffic conditions.

b. In telephony, the QoS for which a circuit is designed or conditioned to provide; e.g., voice grade or program grade. Criteria for different grades of service may include equalization for amplitude over a specified band of frequencies, or in the case of digital data transported via analog circuits, equalization for phase.

Granular Service Class. Represents the atomic identification of a service class. A set of granular service classes sharing similar traffic characteristics forms an aggregate service class.

Guaranteed Service. The use of signaling to reserve network resources end-to-end to meet preset performance objectives.

C.1.9 H

H.323 to H.320 Gateway. A videoconferencing endpoint that converts between H.323 IP endpoint protocols and services and H.320 endpoint protocols and services for transport of videoconferencing data between IP and serial or integrated services digital network (ISDN) sessions.

High Assurance Internet Protocol Encryptor (HAIPE). A Type I encryptor device used to encrypt data used on an IP network.

High Bit Rate DSL (HDSL). A bidirectional and symmetrical transmission system that allows the transport of signals with a bit rate of 1544 Kbps or 2048 Kbps on the copper twisted pairs of an access network at a distance of up to 12,000 feet.

High-Resolution Graphics. Graphics captured and displayed at a higher resolution than the National Television System Committee standard (EIA-170-A).

Hub 1. A distribution point in a network. 2. A device that accepts a signal from one point and redistributes it to one or more points.

C.1.10 I

IMMEDIATE/PRIORITY (I/P) Users. Any person (regardless of the position in the chain of command) who issues or receives guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime.

In-Band. Term used when network management system connects to the network device using the same Ethernet port communication channel used for user traffic.

Individual Line. A line arranged to serve only one main station, although additional stations may be connected to the line as extensions of the main station.

Inelastic Service. A voice and video service that typically requires strict bounds on packet loss, delay, and jitter.

Information Assurance Enabled Product. A system whose primary function is not Information Assurance, but does have some Information Assurance functions.

Information Assurance Product. A system that provides Information Assurance functions consistent with the Information Assurance services and categories (i.e. authentication, confidentiality). An Information Assurance product's primary purpose is to provide Information Assurance functions.

Information Technology (IT) Products. Systems that receive, process, store, display, or transmit Department of Defense voice and video services.

Instant Messaging (IM). The capability for users to exchange one-to-one ad hoc text messages over a network in real time. 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.

Integrated Services Digital Network (ISDN). See FED-STD-1037C, Integrated Services Digital Network.

NOTE: Access channels include a basic rate (two 64-kilobits per second (kbps) B-channels plus one 16-kbps D-channel) and a primary rate (twenty-three 64-kbps B channels and one 64-kbps D-channel). Also known as Narrowband-ISDN or N-ISDN.

Integrated Services Digital Network (ISDN) Device. An ISDN specifies a number of reference points that define logical interfaces between functional ISDN devices such as terminals, terminal adapters, network termination devices, and line termination equipment. An ISDN specifies a number of reference points that define the interconnection of these devices.

Integrated Services Digital Network devices are defined as:

TE1 Terminals with built-in ISDN connection capability (also referred to as TE).

TE2 An existing terminal device, designed for existing protocols. It is not capable of directly interoperating with ISDN.

TA An adaptive device designed to permit TE2s to interoperate with ISDN.

Integrated Services Digital Network (ISDN) Integrated Access Interface. An ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D channel.

Integrated Services Digital Network (ISDN) NT 1. A single (physical) layer device that contains all the necessary interface elements to communicate with the network. It terminates the local loop and provides the user interface to the network while isolating this user from the operation of the network.

Integrated Services Digital Network (ISDN) R. The reference point representing a standardized non-ISDN interface, such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a Terminal Adapter and Terminal Equipment Type 2 is equivalent to a Terminal Equipment Type 1.

Integrated Services Digital Network (ISDN) Reference Points. The reference points applicable for Defense Switched Network customer premises equipment are as follows:

U The reference point for a basic rate interface (BRI) connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

S The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 (TE1) or Terminal Adapter (TA)) and the network termination equipment. This is a 4-wire interface that supports the BRI 2B+D protocol.

R The reference point representing a standardized non-ISDN interface such as Electronics Industries Alliance (EIA)-232, EIA-422, V.24, V.35, and others. The combination of a TA and Terminal Equipment Type 2 (TE2) is equivalent to a TE1.

Integrated Services Digital Network (ISDN) S. The reference point between ISDN user terminal equipment (i.e., Terminal Equipment Type 1 or Terminal Adapter) and the network termination equipment (NT1). This is a 4 wire interface that supports the Basic Rate Interface 2B+D protocol.

Integrated Services Digital Network (ISDN) Terminal Adapter. An adaptive device designed to permit Terminal Equipment Type 2 to interoperate with ISDN.

Integrated Services Digital Network (ISDN) Terminal Equipment (TE) 1. Terminals with built-in ISDN connection capability (also referred to as TE).

Integrated Services Digital Network (ISDN) Terminal Equipment (TE) 2. An existing terminal device designed for existing protocols. It is not capable of directly interoperating with ISDN.

Integrated Services Digital Network (ISDN) U. The reference point for a Basic Rate Interface connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

Internet Protocol (IP) Centric. Architectures that are designed around an IP core packet switching system. These solutions have distributed IP devices that function together to provide voice and video over IP services.

Internet Protocol (IP) Data Subscriber. A user connected to an IP network to receive Department of Defense IP services, such as data and IP video. Defense Switched Network IP telephony is not included.

Internet Protocol Packet Delay Variation (IPDV). The one-way IPDV(n) is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU T Recommendation Y.1540, IETF RFC 3393]. In the case of voice and video services, the measurements are typically taken at the end instruments. This is also referred to as jitter.

Internet Protocol Packet Loss Ratio (IPLR). A metric measured for packets traversing the network segment between the source reference point and destination reference point. The IPLR metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Recommendation Y.1540, IETF RFC 2680]. This is also referred to as packet loss.

Internet Protocol Packet Transfer Delay (IPTD). The single instance of the one-way IPTD measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time starting from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Recommendation Y.1540, IETF RFC 2679] In the case of voice and video services, the measurement points are the end instruments. This is also referred to as latency.

Internet Protocol Signaling Gateway (IPSG) Function. A signaling appliance that relays, translates, or terminates IP messages between various IP signaling protocols such as Unified Capabilities Session Initiation Protocol, H.323, H.248, and IP proprietary signaling protocols.

Internet Protocol (IP) Telephony Subscriber. A Defense Switched Network IMMEDIATE/PRIORITY (I/P) or non-I/P user that receives voice service via an IP telephone instrument (also known as an End Instrument.

Internet Protocol (IP) Transport. The aggregation of various types of IP traffic, such as voice, video, and data that is transmitted over IP link.

Internet Protocol Version 6 (IPv6) Capable. A system or product capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IP version 4.

Internet Protocol Version 6 (IPv6) Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only Internet Protocol version 4 (IPv4), only IPv6, or both IPv4 and IPv6.

Internet Protocol Version 6 (IPv6) Capable Products. Products (whether developed by commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed Internet Protocol version 4/IPv6 environments.

Internet Protocol Version 6 (IPv6) Enabled Network. An IP network that is supporting operational IPv6 traffic through the network end-to-end.

Internet Protocol (IP) Video. Transfer of video information (moving pictures and the associated audio, with the corresponding clock interval) in an IP packet data format.

Internet Protocol (IP) Video Subscriber. A Defense Switched Network non-IMMEDIATE/ PRIORITY user that receives video service via an IP video system.

Inverse Multiplexer (IMUX). A device used to create a single, higher speed network data channel by combining, separating, and synchronizing multiple, independent 56- or 64 kilobits per second network data channels. Also known as an aggregator.

C.1.11 J

Jitter. The one-way jitter is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: IPDV(n) = IPTD(n) – IPTD(0). [ITU-T Recommendation Y.1540, IETF RFC 3393]. In the case of voice and video services, the measurements are taken at the end instruments. This is also referred to as the IP Packet Delay Variation (IPDV). The difference in arrival time of packets sent over a network at the receiving end compared to the difference in packet spacing at the sending end.

C.1.12 K

kbps. An abbreviation for kilobits per second, a measure of bandwidth. A measurement of digital information transmission speed of data measured in 1,024 bits per second.

KG-194/194A (National Security Agency cryptographic device nomenclature). A Federally certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second up to 13 megabits per second over synchronous serial links, typically on dedicated circuit networks.

KIV-7/KIV-7HS (National Security Agency cryptographic device nomenclature). A Federally certified cryptographic device used to provide data encryption at data rates up to 2.048 megabits per second on dial-up and other nondedicated networks.

KIV-19/19A (National Security Agency cryptographic device nomenclature). A Federally certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second up to 13 megabits per second over synchronous serial links on dedicated circuit or dial-up network paths. The KIV-19/19A is interoperable with the KG 194/194A.

C.1.13 L

Label. A header created by an Edge Label Switch Router and used by Label Switch Routers to forward packets. The header format various based on the network media type. In the Assured Services Local Area Network environment, the header is a "shim" located between the Layer 2 and Layer 3 headers.

Label Distribution Protocol (LDP). This protocol defines a set of procedures used by multiprotocol label switching (MPLS) routers to exchange label and stream mapping information. It is used to establish label switched paths, mapping routing information directly to Layer 2 switched paths. It is also commonly used to signal at the edge of the MPLS network the critical point where non-MPLS traffic enters. For example, such signaling is required when establishing MPLS virtual private networks.

Label Edge Router (LER). The LER provides the edge function of multiprotocol label switching (MPLS). The LER is where the label is first applied when traffic is directed toward the core of the MPLS network or last referenced when traffic is directed toward the customer. The LER functions as an MPLS provider edge (PE) node in an MPLS network. The LER is a functional PE that sends traffic to provider nodes to traverse the MPLS core, and it sends traffic to the customer interface known in MPLS terminology as the customer edge. The LER uses IP routing toward the customer interface and "label swapping" toward the MPLS core. The term Edge Label Switch Router is used interchangeably with LER.

Label Information Base (LIB). As the network is established and signaled, each multiprotocol label switching router builds a LIB, a table that specifies how to forward a packet. This table associates each label with its corresponding Forward Equivalence Class and the outbound port to forward the packet to. Typically, the LIB is established in addition to the routing table that traditional routers maintain.

Label Swapping. A forwarding decision process set that allows streamlined forwarding of data by using labels to identify classes of data packets, which are treated indistinguishably when forwarding.

Label Switch Router (LSR) or Label-Switching Router (LSR). The LSR provides the core function of multiprotocol label switching (MPLS). The LSR is equipped with both Layer 3 routing and Layer 2 switching characteristics. The LSR functions as a provider node in an MPLS network.

Label Switched Path (LSP). Multiprotocol label switching networks establish LSPs for data crossing the network. An LSP is defined by a sequence of labels assigned to nodes on the packet's path from source to destination. An LSP directs packets in one of two ways: hop-by-hop routing or explicit routing. The path goes through one or more Label Switch Routers at one level of the hierarchy followed by a packet in a particular Forward Equivalence Class.

Latching. The ability of the reconfigurable optical add drop multiplexer to maintain its current state in the event of power failure.

Latency. The single instance of the one-way latency measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Recommendation Y.1540 and IETF RFC 2679] In the case of voice and video services, the measurement points are the end instruments. This is also referred to as IP packet transfer delay (IPTD.

Link. The communications facilities between adjacent nodes of a network. For voice over IP systems, a link is an Ethernet connection used for IP transport as opposed to trunks used for time division multiplexing transport.

Link Pair. To ensure no single point of failure to more than 64 Internet Protocol (IP) telephony subscribers, IP network links shall have a second link (standby or load sharing). The combination of the two links is called a link pair.

Local Area Network (LAN) Access or Edge Layer. The point at which local end users are allowed into the LAN. In addition, these layers may use access lists or filters to optimize further the needs of a particular set of users. This term should not be confused with the wide area network (WAN) Edge or WAN Access Layer.

Local Area Network (LAN) Core Layer. A high-speed switching backbone that is designed to switch packets as fast as possible within the LAN. This term should not be confused with the wide area network Core Layer.

Local Area Network (LAN) Distribution or Building Layer. The distribution or building layer of the LAN is the demarcation point between the Access and Core Layers, and it helps to define and differentiate the core. This layer provides boundary definition, and it is where packet manipulation can take place.

Local Area Network (LAN) Network Links. Internal Internet Protocol (IP)/Ethernet links that interconnect LAN components.

Local Area Network (LAN) Switch. A LAN switch is an appliance that reduces contention on LANs by reducing the number of nodes on a segment using microsegmentation techniques. On a microsegmented network, a LAN segment may have many nodes or a single node. The LAN switch handles all the connections between nodes on different LAN segments when they need to communicate through an internal matrix switch that processes the packets at the Media Access Control (MAC) layer. When a packet arrives at the switch, its destination MAC address is quickly noted and a connection is set up to the appropriate end segment. Subsequent packets are relayed through the switch without the need to store and forward packets, as is necessary with bridges. Many LAN switches in the DoD Internet Protocol Unified Capabilities architecture include router functions.

Location Server. The location server provides information on call routing and called address translation (where a called address is contained within the called Session Initiation Protocol Secure Uniform Resource Identifier in the form of the called number). The service provided by the server typically is referred to as location services. The Call Connection Agent uses the routing information stored in the location server:

- To route internal calls from one Session Controller (SC) end instrument (EI) to another EI on the same SC.
- To route outgoing calls from an SC EI to another SC or a time division multiplexing (TDM) network.
- To route incoming calls from another SC or a TDM network to an SC EI or SS.

Local Session Controller (LSC). A Session Controller that is located at the same DoD Component site as the End Instruments that it serves.

Long Local. A long-local telephone is connected remotely through an assured transmission means, time division multiplexing or Internet Protocol, to a distant site. This interface is handled as a local loop to the host Defense Switched Network switch.

Luminance. The intensity component of a pixel. The Y component in YCbCr. The L component in CIElab.

C.1.14 M

Management Plane. A quality of service mechanism to access network elements for network management purposes, such as provisioning and policy setting. This plane is used to define the configuration, startup conditions, and instability conditions of the management protocols and features including Simple Network Management Protocol, Logging/Debug, statistics collection, and management configuration sessions such as telnet, Secure Shell, and serial console.

Master Session Controller (MSC). Session Controller that coordinates session processing of all Session Controllers deployed in a Master-Subtended cluster at a DoD Component site or within a Deployable Extension of the DISN.

Maximum Segment Size (MSS). The largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. The MSS is an important consideration in Internet Protocol (IP)-based networks. As data is routed over an IP network, it must pass through multiple gateway routers. Ideally, each TCP segment can pass through every router without being fragmented. If the data segment size is too large for any of the routers through which the data passes, the oversized segments are fragmented. This fragmentation slows down the connection speed seen by the computer user, in some cases dramatically. The likelihood of such fragmentation can be minimized by keeping the MSS as small as reasonably possible. For most computer users, the MSS is set automatically by the operating system.

Maximum Transition Unit (MTU). A term for the size (in bytes) of the largest datagram that can be passed by a layer of a communications protocol.

Mbps (Megabits Per Second). A measure of bandwidth. A measurement of the transmission speed of data measured in 1,048,576 bits per second. A unit of how much digital information is transferred over time.

Mean Time Between Failures (MTBF). For a particular interval, the total functional life of a population of an item divided by the total number of failures (requiring corrective maintenance actions) within the population.

Mean Time To Repair (MTTR). The total amount of time spent performing all corrective maintenance repairs divided by the total number of those repairs.

Measurement-Based Admission Control. An approach that bases a call control decision on the monitoring of network capacity. Admits, rejects, or redirects calls based on current network congestion.

Media Gateway (MG). An 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 Internet Protocol (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.

Media Gateway Controller (MGC). The function in a signaling appliance that controls a media gateway.

Media Server. A platform in an Internet Protocol telephony network that transmits dial tones, busy signals, and announcements.

Meet-Me Conferencing. A conference that is established when each conferee dials into the conference bridge at a scheduled time as directed by a conference attendant.

Message. A unit of data transfer from an application in one host to an application in another host.

Message Discrimination and Distribution Function. A function that examines the Destination Point Code of a received signaling message to determine whether it is destined to the receiving signaling point.

Metering. The process of measuring the temporal properties (e.g., rate) of a traffic stream selected by a classifier. The instantaneous state of this process may be used to affect the operation of a marker, shaper, or dropper, and/or may be used for accounting and measurement purposes. [RFC 2475]

Metric. A quality of service delivery parameter such as delay, packet loss, data rates, and availability.

Microflow. A single instance of an application-to- application flow of packets that is identified by source address, source port, destination address, destination port, and protocol identification. [RFC 2475]

Minimum Requirements. Features and capabilities considered necessary for a particular switch type to support warfighter missions in the DoD. These features and capabilities will require certification before introduction into the Defense Switched Network.

Mobile Code. Software modules obtained from or provided by remote systems, transferred or downloaded across a network, and then executed on local systems without explicit installation or execution by the recipient.

Modem over IP (MoIP). The transport of modem data across an Internet Protocol network, via either modem relay or voiceband data (modem pass-through) techniques.

Modem Relay. A subset of Modem over IP in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network.

MPEG (Moving Picture Experts Group). A standard for a digital video and audio compression.

MTU. See Maximum Transition Unit.

μ-Law. The pulse code modulation coding and companding (compressing and expanding) standard used for non-linear compression in the analog-to-digital conversion process that is used primarily in Japan and North America.

Multicasting. The ability of the reconfigurable optical add drop multiplexer to allow one input wavelength to be duplicated on multiple output tributary and line ports. Also, the process of transmitting data/information from one source to many destinations in a single transfer.

Multifunction Switch (MFS). "A switch that combines the tandem function of the SA [Standalone] switch with the EO [End Office] function of connecting the user's lines to the backbone trunks. Logically the SA and EO are separate, but within the same physical configuration."

Multilevel Precedence and Preemption (MLPP). In circuit-switched systems, a priority scheme:

- For assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and timeframe.
- For gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages.
- That is recognized only within a predefined domain.
- In which the precedence level of a call outside the predefined domain is usually not recognized.

Multilevel Precedence and Preemption (MLPP) Call. A call that has a precedence level established and is either being set up or is set up. In Digital Subscriber Signaling System No. 1 (DSS1: ISDN Q.931 signaling), an MLPP call is a call from an MLPP subscriber for which a setup has been sent but no DISCONNECT has been sent or received.

Multilevel Precedence and Preemption (MLPP) Service Domain. A set of MLPP subscribers (MLPP users) and the network and access resources that are in use by that set of MLPP subscribers at any given time. Connections and resources that are in use by MLPP subscribers may be preempted only by higher precedence calls from MLPP subscribers within the same domain. The service domain consists of a 3-octet field ranging from 00 00 00 to FF FF FF in hexadecimal. The Defense Switched Network service domain is zero (0).

Multipoint. A telecommunications system that permits three or more locations to intercommunicate in a conference call.

Multipoint Control Unit (MCU). (1) An endpoint that enables intercommunication of three or more video teleconferencing (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. (2) A multiport 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.

Multipoint Controller (MC). The MC is an H.323 entity on the network that provides for the control of three or more terminals participating in a multipoint conference. It may also connect two terminals in a point-to-point conference, which may later develop into a multipoint conference. The MC provides for capability negotiation with all terminals to achieve common levels of communications. It may also control conference resources such as who is multicasting video. The MC does not perform mixing or switching of audio, video, and data.

Multipoint Processor (MP). The MP is an H.323 entity on the network that provides for the centralized processing of audio, video, or data streams in a multipoint conference. The MP provides for the mixing, switching, or other processing of media streams under the control of the Multipoint Controller. The MP may process a single media stream or multiple media streams depending on the type of conference supported.

C.1.15 N

Nailed Up Connections. A special use permanently established path through a switch for either a network circuit (trunk) or a special service facility.

Narrowband Streaming. For the purposes of this document, Narrowband Streaming refers to the transfer of data in a continuous audio and/or video stream over a network using bandwidth from 28.8 kilobits per second to 1.5 megabits per second.

National Institute of Standards and Technology (NIST). Special Publication 800-72-3, "Cryptographic algorithm and Key Sizes for Personal Identify Verification", W. Timothy Polk, Donna F. Dodson, William Burr, Hildegard Ferraiolo, and David Cooper, December 2010.

Network 1. All telecommunications equipment that has any part in processing a call or a supplementary service for the user referred to. It may include local exchanges, transit exchanges, and Network Termination 2 but does not include the integrated services digital network (ISDN) terminal and is not limited to the “public” network or any other particular set of equipment. 2. Refers to the system of cables, microwave links, and switching centers that allow the transmission of data, as opposed to the terminal equipment (such as CODECs and input/output devices) connected to the cables. [FED-STD-1037C]

Network Domain. A contiguous set of network elements that belongs to the same administrative authority.

Network Element (NE). A component of a network through which the Defense Switched Network (DSN) bearer and/or signaling traffic transits. For Internet Protocol (IP) transport, the IP connection may transit a Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), or Wide Area Network (WAN) dependent on its deployment. Network elements may include multiplexers, routers, Channel Service Units/Digital Service Units (CSU/DSUs), compression devices, circuit emulation, channel banks, and/or any network device that could have an effect on the performance of the associated network traffic. The network diagram, shown in Figure A-2, Network Element Diagram, shows the typical NE as a standalone device or integrated into the transmission interfaces of switches or other network devices. The use of NEs shall not provide the means to bypass the DSN as the first choice for all switched voice and dial-up video telecommunications between DoD user locations.

Network Interface Equipment. The equipment connected between the network and the conferencing terminal unit (CTU). Such examples of this equipment include (a) the channel service unit (CSU), (b) the data service unit (DSU), and the (c) terminal adapters.

Network Signaling Based Admission Control. Determines based on requests indicated through a signaling protocol whether a node or network has sufficient available resources to meet the requested quality of service. [RFC 2205]

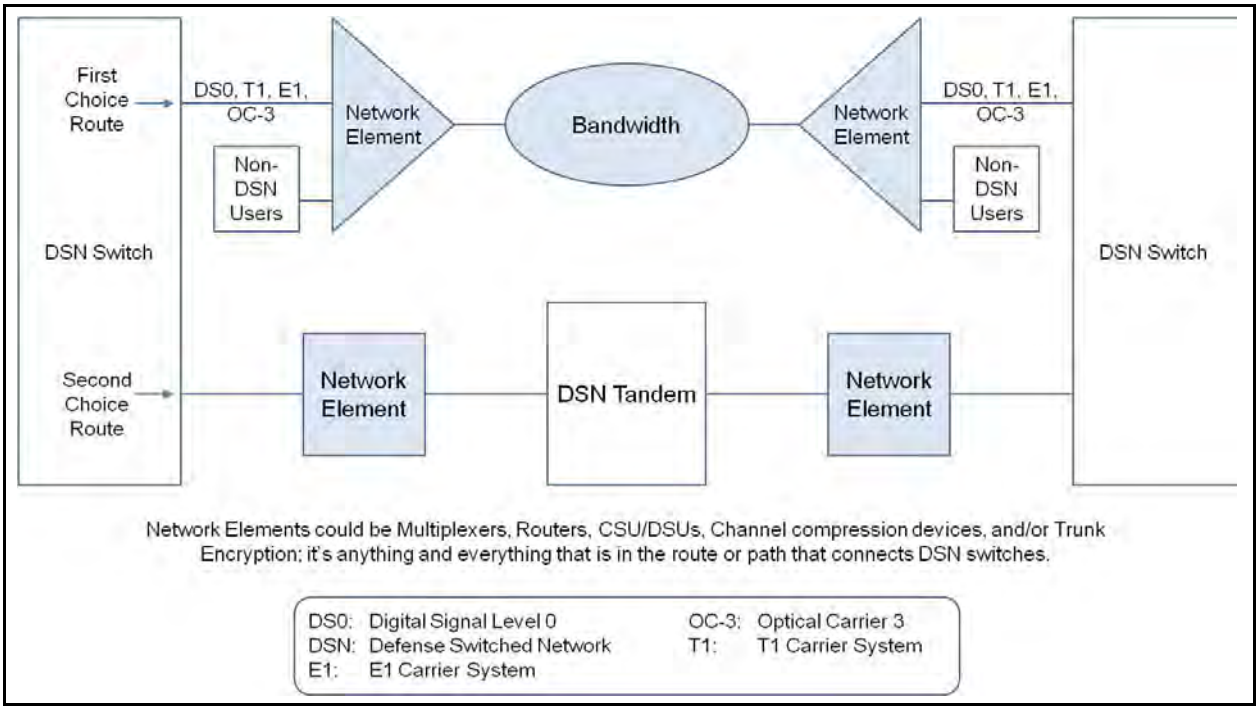

Figure C.1-2. Network Element Diagram

Network Terminator Type 1 (NT-1). A device that converts a 2-wire U-interface to a 4-wire S/T interface, allowing multiple conferencing terminal unit connections.

New Call. The event that precipitates a trunk seizure or when preemption for reuse of a trunk is used to support multilevel precedence and preemption calls in the Defense Switched Network.

Nomadic Wireless End Instrument (WEI). Those WEIs that are mobile and may traverse different wireless local area network access systems during a single session.

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.

Non-Assured Service Local Area Network (Non-ASLAN). The Internet Protocol (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.

Non-Converged Network. A network that is used solely to provide Defense Switched Network Voice over Internet Protocol (IP) services. A separate IP network will be used to provide IP data services.

Non-IMMEDIATE/PRIORITY (I/P) Users. Those users, DoD, non-DoD, non-U.S. Government and foreign government users that have no missions or communications (equipment) requirements to originate or receive I/P communications under the existing military scenarios. These users are provided access to the Defense Switched Network (DSN) for economic benefit of the DoD. During a crisis or contingency, these users may be denied access to the DSN. It is the primary means of secure communications for non-Deployable I/P users. The DSN must be the user's first choice; however, if the DSN is not immediately available, or if the called party does not have access to DSN service, other long-distance calling methods may be used.

Nonblocking Local Area Network (LAN). A LAN that is provisioned so all Internet Protocol telephone instruments can be off hook simultaneously and successfully engaged in a full duplex voice call.

Nonpreemptive Service. A Global Information Grid service that offers a committed information rate between two or more Edge networks, where the bandwidth cannot be preempted for the use of any other party than the one contracting for the service.

Nonsignaled Flow. A flow that does not require signaling to enter a network.

C.1.16 O

Objective Requirement [Objective]. A requirement that does not have to be met in the initial operational capability (IOC), but must be met in the final operational capability (FOC). The timeframe associated with the IOC is fiscal year (FY) 2008 and the timeframe associated with the FOC is FY 2012 unless specifically stated.

Offered Load Control. A mechanism that allows control of packet transfer loads to keep them within specified bounds (possibly described in service level agreements) so that network domains can deliver the promised quality of service.

Operations, Administration, and Maintenance (OA&M). A set of network management functions, providing network fault indication, performance information, and data and diagnosis functions.

Optical Line Amplifier (OLA). Provides optical signal reamplification without converting to electrical signal along the spans between optical terminal equipment.

Originating Gateway. An Assured Service Session Initiation Protocol for Telephones signaling appliance performing the originating Internet Protocol/Time Division Multiplexing Signaling Gateway function.

Originating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function. The function related to receiving an Initial Address Message (IAM) from the Common Channel Signaling System No. 7 network and generating an Assured Service Session Initiation Protocol INVITE with the encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM that is sent over the IP network—identical to Outgoing Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part."

Out-of-Band. A term used to describe network management systems that connect to the network device using a physically separated network from the network used for user traffic. This requires an additional network infrastructure to support management traffic.

Outgoing Call Trace. A feature that allows the tracing of nuisance calls to a specified directory number suspected of originating from a given local office. The tracing is activated when the specified directory number is entered. A printout of the originating directory number, outgoing trunk number, or terminating number, and the time and date is generated for every call to the specified directory number.

Outside Plant (OSP) Loss. The OSP loss is measured from the fiber connector in the Fiber Service Delivery Point (FSDP) of a Dense Wave Division Multiplex (DWDM) equipment location to the fiber connector (at the other end of the fiber) in the FSDP of the next DWDM equipment location. The OSP loss is the combined loss of the fiber attenuation itself and the attenuation due to splices and connectors across the span.

Overflow Process. A process that allows calls of a lower precedence level and narrower calling area to utilize unused calling capacity of a higher precedence level and equal and wider calling area, and equal precedence level and wider calling area call types without blocking calls of a higher precedence level and wider calling area.

C.1.17 P

p. An integer that can range from 1 to 30 and is limited to the values of 1, 2, 3, 4, 5, 6, 12, 18, 23, 24, and 30 for conferencing terminal unit (CTU) operation over digital-switched networks. It relates to CTUs that operate at nominal bit rates of integer "p" multiples of 64,000 bits per second (bps). For unrestricted channels, such as provided by integrated services digital network, each increment of data rate may actually be 64,000 bps, but in restricted channels, each increment may be only 56,000 bps.

Packet Loss. A metric measured for packets traversing the network segment between the source reference point and destination reference point. The Packet Loss metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as Internet Protocol packet loss ratio.

Packet Marking. Marking in packets following their classification for a given service delivery, which includes Differentiated Services Code Point, Flow Label, or Security Parameter Index bit fields.

Path. Communications link between two network components. A path may include a number of communications links.

PC (Personal Computer). A computer specifically designed for use by one person at a time, equipped with its own CPU, memory, operating system, keyboard and display, hard/floppy disks, as well as other peripherals when needed.

Per-Domain Behavior (PDB). An externally observable edge-to-edge functional and performance quality of service behavior on a per-domain basis.

Per-Hop Behavior (PHB). An externally observable forwarding behavior applied at a Differentiated Services (DS)-compliant node to a DS behavior aggregate based on the Differentiated Services Code Point marking in the packet. [RFC 2475]

Pixel (Picture Element). Converts the input light image to an electronic signal. The smallest discrete picture element that can be transmitted using the video or still image coding algorithms. A pixel is similar to grains in a photograph or dots in a halftone. Each pixel can represent a number of different shades or colors, depending on how many bits are allocated for it.

Point-to-Point Video Teleconferencing (VTC). A two-party video teleconference.

Policing. The process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile. [RFC 2475]

Port. A point of access where signals may be inserted or extracted into or out of a device, such as a conferencing terminal unit or multipoint control unit.

Precedence. The designation assigned to a message by the originator to indicate its relative level of importance of the message up to the originator's maximum authorization level as defined by DoD requirements documents.

Precedence-Based Assured Service (PBAS). This service implies that, in general, quality of service requirements of a higher precedence class will be met at the expense of a lower precedence class if the network conditions do not allow meeting quality of service requirements of all service classes.

Precedence-Based Treatment. The process of allocating network resources to the higher precedence messages more favorably while restricting lower precedence traffic during periods of resource shortage.

Precedence Inversion. The phenomenon that occurs when a higher precedence flow or flow aggregate does not receive its quality of service commitments, while a lower precedence flow or flow aggregate competing for the same communications source does receive its quality of service commitments.

Precondition. "A precondition is a set of constraints about the session that are introduced in the offer. The recipient of the offer generates an answer, but does not alert the user or otherwise proceed with session establishment. That only occurs when the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new offer sent by the caller." [RFC 3312]

Preemptable Circuit. A circuit that is active with or reserved for a multilevel precedence and preemption call: (a) within the same domain as the preempting call and (b) with a lower precedence than the preempting call. A busy or reserved circuit for which a precedence level has not been specified is not a preemptable circuit.

Preemption Initiating Exchange. An exchange that is congested (i.e., no idle circuits) and has received a preempting call setup.

Preferred Elastic. A specially created service class category to meet unique DoD application requirements; it has varying degrees of service class categories. Examples include short, interactive transactions and delay-sensitive file transfers.

Presence/Awareness. A status indicator that conveys ability and willingness of a potential user to communicate. A user's client provides presence information (presence state) via network connection to a presence service, which is stored in what constitutes the user's personal availability record (called a presentity) and can be made available for distribution to other users (called watchers) to convey the user's availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging (IM) or recent implementations of voice over IP clients.

A user client may publish a presence state to indicate its current communication status. This published state informs others that wish to contact the user of the user's availability and willingness to communicate. The most common use of presence is to display a status indicator icon on IM clients, and a list of corresponding text descriptions of each of the states. Even when technically not the same, the "on-hook" or "off-hook" state of a called telephone is an analogy; the caller receives a distinctive tone indicating unavailability ("line busy") or availability ("ring-back tone" followed by voice mail).

Primary Rate Interface (PRI). A high-speed ISDN service, consisting of 23 B-channels (30 in Europe) and one D-channel.

Private Branch Exchange (PBX) Line. A line appearance at the local switching system that permits connection to a customer premise switching system. The connecting facility may be 1- or 2-way, and it may be loop start or ground start. A PBX line is like an individual line except for ringback, power cross test, and permanent signal treatment.

Private Branch Exchange (PBX) Type 1 (PBX1). A PBX with multilevel precedence and preemption capabilities. Based on mission requirements, this switch may serve those non-IMMEDIATE/PRIORITY (I/P) users defined as DoD users having a military mission that might receive I/P calls for orders or direction at precedence levels above a ROUTINE precedence, even though they do not have a I/P mission for issuing guidance or orders. FLASH and FLASH OVERRIDE users are unauthorized to be served by a PBX1 and must connect to an End Office Switch or a Small End Office Switch.

Private Branch Exchange (PBX) Type 2 (PBX2). A PBX with no multilevel precedence and preemption capabilities. This switch can serve only DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive IMMEDIATE/PRIORITY (I/P) communications under existing military scenarios. These users are provided access to the Defense Switched Network (DSN) for the economic or policy benefits of the DoD, when it is not in conflict with local Public Telephone and Telegraph ordinances. During a crisis or contingency, they may be denied access to the DSN. The I/P, FLASH, and FLASH OVERRIDE users are unauthorized to be served by a PBX2.

Propagation Delay. Travel time of an electromagnetic signal from one measurement point to another.

Proprietary End Instrument (PEI). A user appliance that interacts with the serving appliance (i.e., local session controller, Multifunction Softswitch, or Wide Area Network Softswitch), using a proprietary protocol to originate, accept, and/or terminate a voice, video, or data session(s).

Proprietary IP Trunk (PIPT). A virtual network element that provides a virtual IP trunk connection between a pair of certified switches (e.g., Deployable Voice Exchange (DVX) to DVX, DVX to Private Branch Exchange (PBX) Type 1, DVX to PBX Type 2). The PIPT may use proprietary signaling but must support the equivalent features and functions of a Primary Rate Interface, multilevel precedence and preemption (MLPP) (T1.619a), or non-MLPP (NI 1/2), as appropriate.

Protection. A preplanned alternate path for the service.

Proxy Server. "An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it." [RFC 3261]

px64. In video teleconferencing, pertaining to a family of ITU-T Recommendations, where p is a non-zero positive integer indicating the number of 64 kilobits per second channels. These recommendations form the basis for video telecommunications interoperability.

(NOTE: The p × 64 family includes ITU-T Recommendations H.261, H.221, H.242, H.230, and H.320.)

C.1.18 Q

Quality of Service (QoS). 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. Quality of service 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.

Quality of Service Domain. An administrative network domain that is designed based on a single quality of service architecture and operated under the same set of quality of service policies.

Quality of Service Network. A quality of service aware or enabled network; it consists of one or more interconnected quality of service domains.

Quarter Common Intermediate Format (QCIF). A video format defined in ITU-T Recommendation H.261 that is characterized by 176 luminance pixels on each of 144 lines, with half as many chrominance pixels in the horizontal and vertical directions. QCIF has one fourth as many pixels as Full Common Intermediate Format (q.v.).

Queuing Delay. Waiting time of a packet for its turn to be serviced at the interface of a network device, such as a router.

C.1.19 R

Real Time. At the same time, simultaneously. An event where two or more people communicate simultaneously, similar to the way people speak on a telephone at the same time. Any event that occurs in real time indicates that the event is happening, as we would see it, in actual time. Recording video in real time would require at least 30 frames per second. If the user defines or initiates an event and the event occurs instantaneously, the computer is said to be operating in real time. Real-time support is especially important for multimedia applications.

Real Time Control Protocol (RTCP). As defined in IETF RFC 1889, the Real Time Transport Control Protocol (RTP control protocol or RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets.

Real Time Protocol (RTP). As defined in IETF RFC 1889, a transport protocol for real-time applications. Real Time Protocol is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. Real Time Protocol provides services such as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications. Real Time Protocol is used by all the Voice over Internet Protocol and H.323 signaling protocols.

Real Time Streaming Protocol (RTSP). An open, standards-based protocol for multimedia streaming. The Real Time Streaming Protocol enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, live audio and video, and stored content. The Real Time Streaming Protocol is designed to work with established protocols, such as Real Time Protocol (RTP) and HyperText Transfer Protocol. The Real Time Streaming Protocol provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. The Real Time Streaming Protocol is intended to control multiple data delivery sessions, provide a means for choosing delivery channels such as User Datagram Protocol (UDP), multicast UDP, and Transmission Control Protocol (TCP), and provide a means for choosing delivery mechanisms based on RTP.

Reconfigurable Optical Add Drop Multiplexer (ROADM). Optical terminal equipment capable of terminating up to 80 channels in both directions. It performs wavelength add and drop functions, as well as allowing wavelengths to pass through.

Release to Pivot (RTP). A network routing capability that consists of a collection of call setup procedures that provides flexibility to a Tandem Switch/Multifunction Switch/End Office-type switch to determine conditions for either forwarding a call or releasing it back to a previous switch in the call path. The RTP is a network capability that is invoked in support of service or business needs, and not invoked directly by an end user. After an operator services switch has determined a new destination for the call, the RTP network capability permits an operator services switch to have the connection established from the originating switch. The basic capability allows any switch to indicate to switches farther forward in the call path that it has the ability to pivot the call. Then an application that determines the new destination for the call (in this case, the operator services switch) can release the call with a Redirection Number parameter containing the address of the new destination. The Pivot switch (in this case, the originating switch) will not terminate the call on receipt of the Release message, but will pass the call forward toward the new destination. The result is that the Release switch, which determined the new destination, saves an incoming and an outgoing trunk relative to the case where the call is forwarded to the new destination.

Reliability. The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system.

Required Requirement [Required]. A requirement is required if it must be met in the initial operational capability (IOC). The IOC is associated with the fiscal year 2008 timeframe. An IOC requirement is often labeled a Threshold requirement to differentiate the requirement from an Objective requirement.

Reservationless. A conferencing service that allows you to initiate a conference 24 hours a day, 7 days a week, without the need to make a reservation or rely on an operator. A Meet-Me conference that does not require advance reservations.

Resolution. A measurement of the number of pixels in the horizontal and vertical directions. For example, the resolution of Full Common Intermediate Format is 352 X 288 meaning that it contains 352 pixels in each horizontal row and 288 rows of pixels in the vertical direction for a total of 101,376 pixels.

Resource Reservation Protocol (RSVP). A protocol developed by the Internet Engineering Task Force for hosts (applications) and routers to communicate service requirements to the network and to enable the routers in the network to set up the reservations.

Response Time. Round-trip delay from a network application source through destination, back to the application source.

Restoration. The switching of the service to an alternate path after a failure.

Round Trip Time (RTT). The RTT is the time required to send a signal from point A to point B and back to point A over a particular end-to-end communication path. Networks with both high bandwidth and a high RTT can have a very large amount of unacknowledged data "in flight" at any given time, known as the bandwidth-delay product. Such networks require special protocol design considerations, such as larger packet receive buffers for high input/output streaming protocol sessions.

Route Code. A special purpose Defense Switched Network code that permits the customer to inform the switch of special routing or termination requirements. Presently, the route code is used to determine whether a call will use circuit-switched data or voice-grade trunking. The route code may be used to disable echo suppressers and cancellers, and override satellite link control.

Router. 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 Internet Protocol (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 Unified Capabilities architecture include local area network switch functions and the distinction between the two types of appliances continues to blur.

C.1.20 S

Scalability. The degree to which the H.323 standard and products based on that standard can support IP-based conferences containing both small and large numbers of participants. Typically, for large numbers of participants, most would be in a receive-only mode, listening to one or a small group (panel) of talkers.

Secure Communications Interoperability Protocol (SCIP) over Internet Protocol (IP). The transport of SCIP information over an IP network. The SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 Modem Relay.

Secure Cryptographic Processes. Constitute the basic requirement for effective data security and effective data protection in the use of information technology. The basic requirements include digital signatures, authentication and access control, and encryption.

Secure End Instrument (SEI). An end instrument that is able to operate in the normal real time services (RTS) mode and in a secure (typically type 1 encryption) mode.

Secure Telephone Equipment (STE). Refers to both a DoD Secure Communications Device (DSCD) and a mode of operation. It is a DSCD that uses any one of the multiple supported protocols to conduct a secure session with another compatible protocol device.

Secure Voice over IP (SVoIP). Provides Type 1 encrypted communications end to end. Security (encryption for confidentiality) is provided at the Application layer using Secure Communication Interoperability Protocol (SCIP) (formerly known as Future Narrow Band Digital Terminal (FNBDT)) devices. The encryption is typically Type 1; however, SCIP/FNBDT devices can use other crypto methods and libraries, such as Advanced Encryption Standard. Secure VoIP provides talker-to-listener security and session-unique security levels. It is capable of transitioning through BLACK Public Switch Telephone Network and provides interoperability with legacy service voice systems (Secure Telephone Unit and Secure Telephone Equipment).

Secure Voice over Secure IP (SVoSIP). The use of SVoIP devices on a Voice over Secure Internet Protocol (VoSIP) network that provides the following features:

- Security (confidentiality) is provided at both the application and network layers.
- Using Secure High Assurance Internet Protocol Encryptor (HAIPE) + Future Narrow Band Digital Terminal (FNBDT).
- Confidentiality within HAIPE's domain (end-to-end on top of system high).
- Independent negotiations can permit interoperability with FNBDT only.
- HAIPE-only systems.

Selective Call Forwarding. A feature that allows customers to have only calls from selected calling parties forwarded.

Service Class. A set of traffic that requires specific delay, loss, and jitter characteristics from the network for which a consistent and defined per-hop behavior applies.

Service Assurance. Proactive monitoring and support activities to ensure that services provided to customers are continuously available and to SLA or QoS performance levels.

Service Definition. A standards document that defines the scope of the standardization effort of commercial standards. Service definitions for video teleconferencing have been written by the ANSI T1A1.5 committee, and by ITU-T Study Group 1.

Service Level Agreement (SLA). Binding contractual agreement between two parties, Global Information Grid (GIG) networks service provider and GIG users, listing offered services and service-level specifications about the technical parameters of the service requested. An SLA may include traffic conditioning rules. An SLA is often the result of the mission planning process.

Service Level Objective (SLO). A numerical performance value that specifies a commitment made by the provider to the user, in the service level specifications of the service level agreement.

Service Level Specification (SLS). A set of quantitative performance metrics that together define the service offered to a traffic stream by a differentiated services domain related to a specific service level agreement.

Service Provisioning Policy. A policy that defines how traffic conditioners are configured on differentiated services (DS) boundary nodes and how traffic streams are mapped to DS behavior aggregates to achieve a range of services. [RFC 2475]

Session. The underlying AS-SIP or Proprietary Voice over Internet Protocol (VoIP) session that is processed by the proprietary end instrument/AS-SIP end instrument and the session controller. The VoIP signaling and media streams in the appliance that support an individual end user's call.

Session Controller (SC). A call stateful AS-SIP signaling appliance at a base/post/camp/station that directly serves Internet Protocol (IP) end instruments (EIs). The SC may consist of one or more physical platforms. On the trunk side, the SC uses AS-SIP signaling. On the line side, the SC may serve any combination of Session Initiation Protocol EIs, H.323 EIs, and proprietary EIs. The SC must be an intermediary for every inbound and outbound call signaling message received and transmitted by each IP EI served by the given SC.

Session Controller (SC) Level Assured Services Admission Control (L-ASAC). The processes on an SC that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services. Typically, the processes are associated with the preemption of lower precedence sessions to an end instrument to ensure that higher precedence sessions can be completed.

Session Initiation Protocol (SIP). "…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." [RFC 3261]

Session Initiation Protocol (SIP) Proxy Server. Equivalent to time division multiplexing call processing software that detects call for service ("off-hook"), analyzes address digits received, and based on data contained in translation tables/local subscriber line tables obtains the called telephone addressing information. Then it forwards the session invitation directly to the called telephone if it is located in the same domain, or to another proxy server if the call telephone resides in another domain.

Session Initiation Protocol (SIP) Redirect Server. Equivalent to time division multiplexing routing tables that allow SIP proxy servers to direct SIP session invitations to external domains. The SIP redirect servers may reside in the same hardware as SIP registrar and Internet service provider proxy servers.

Session Initiation Protocol (SIP) Registrar Server. Equivalent to time division multiplexing subscriber line database tables and classmarks for all telephones served directly off or by the local session controller controlling a domain. In SIP messaging, these servers retrieve and send participant's IP addresses and other pertinent information to the SIP proxy server.

Session Initiation Protocol (SIP) User Agents. Intelligent Internet Protocol (IP) telephones with SIP software that create and manage a SIP session.

SETUP Message. The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. Defense Switched Network (DSN) calls shall use the SETUP message specified in American National Standards Institute T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory information elements (IEs). For a multilevel precedence and preemption (MLPP) call (invoking MLPP feature) on the DSN user-to-network interface, the SETUP message shall include the Precedence Level IE. It shall contain other IEs, such as the Business Group IE for the Community of Interest feature, when such unique DSN features are required and the call identity IE (as defined in International Telecommunication Union (ITU) Recommendation Q.931) for the MLPP feature. The precedence level and MLPP service domain (both contained in the Precedence Level IE), and the Calling Party Number (contained in the Calling Party Number IE) shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as "reserved" for reuse by the preempting call when the Look-Ahead for Busy option is exercised on the DSN user-to-network interface.

Seven-Digit Dialing. The ability to dial using the seven digits of the switch code and line number to establish either interswitch or intraswitch calls within the same numbering plan area.

Shaping. The process of delaying packets within a traffic stream to cause it to conform to some defined traffic profile. [RFC 2475]

Signaled Flow. A flow that requires signaling to determine whether there are sufficient resources to support its quality of service requirements. If the resources do not exist or they cannot be preempted, the flow is blocked from entering the network.

Signaling. The process of exchanging information between two or more parties to initiate or terminate a communication session, and for the management and maintenance of the session.

Signaling Appliance. See Unified Capabilities Session Initiation Protocol Signaling Appliance.

Signaling Gateway (SG) Function. Receives or sends switched circuit network native signaling at the edge of a data network. For example, the SG function MAY relay, translate, or terminate Signaling System No. 7 (SS7) signaling in an SS7-Internet Gateway. The SG function MAY also be co-resident with the Media Gateway (MG) function to process switched circuit network signaling associated with line or trunk terminations controlled by the MG, such as the D-channel of an Integrated Services Digital Network (ISDN) Primary Rate Interface trunk. The use of the SG function within the Assured Real Time Services Generic System Requirements refers only to SS7 signaling. The use of the SG within the Unified Capabilities Session Initiation Protocol Generic System Specification allows the SG to be co-resident with the MG. [RFC 2805]

Single-Pair High-Speed DSL (SHDSL). SHDSL is a symmetric DSL designed primarily for duplex operation over mixed gauge two-wire twisted metallic pairs. Optional multi-pair operation is supported for extended reach applications. Optional signal regenerators are supported for both single-pair and multi-pair operation SHDSL transceivers are capable of supporting selected symmetric user data rates in the range of 192 Kbps to 2312 Kbps. Optional extensions allow user data rates up to 5696 Kbps. Loop distances can be from 2.4 to 4 miles.

Small End Office (SMEO). "A switch that serves as the primary switch, functions as an EO [End Office], but at smaller DoD [Department of Defense] installations. A SMEO does not have full DSN [Defense Switched Network] Network Traffic Management capabilities. It offers limited performance reporting and may not support SS7 [Signaling System No. 7] signaling. Therefore, SMEOs will not serve installations that are critical to combatant command missions where NM [network management] control and network visibility for situational awareness is required." [CJCSI 6215.01C]

Softphone. An end-user software application on an approved operating system that enables a general-purpose computer to function as a telephony end instrument. It will be tested on an approved operating system as part of the system under test. The softphone application is considered an IP end instrument and is associated with the IP telephone switch.

Softswitch. A stand-alone Approved Products List product that acts as a AS-SIP Back-to-Back User Agent within the Unified Capabilities (UC) architecture. It provides the equivalent functionality of a commercial softswitch. The functionality of the Session Controller (SC) is a conditional requirement and the support of a Signaling Gateway is not required. The softswitch does the following:

- Controls connection services for a media gateway and/or native IP endpoints.
- Selects processes and services that can be applied to a call.
- Provides routing for call control within the network based on signaling and customer database information.

- Transfers control of the call to another network element.
- Interfaces to and supports management functions such as provisioning, fault, and billing.
- Ability to control the access of sessions within and external to its domain. [International Softswitch Consortium]

STEP. An acronym for Standardized Tactical Entry Point.

Still Image. Non-moving visual information such as graphs, drawings, pictures, or video frames not processed by the video codec portion of the conferencing terminal unit.

Strong Authentication. The process of authenticating a user based on at least two of three factors: something you know (i.e., username and password), something you have (i.e., token device), and something you are (i.e., fingerprints).

Sub Quarter Common Intermediate Format (SQCIF). A video format defined in ITU-T Recommendation H.263 that is characterized by 128 luminance pixels on each of 96 lines, with half as many chrominance pixels in each direction. SQCIF has half as many pixels as Quarter Common Intermediate Format.

Subscriber. The owner of a public key contained in a Public Key Infrastructure certificate. A subscriber may be an appliance or a person.

Subtended Session Controller (SSC). Session Controller that is subordinate to a MSC as part of a cluster of coordinated Session Controllers located at a DoD Component site or within a Deployable Extension of the DISN.

Survivability. The capability of a system to survive in a specified threat environment and accomplish its designated mission.

Synchronization. An arrangement for operating digital switching systems at a common (or uniform) clock rate whereby the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information.

System. An appliance or group of appliances. The systems described in this document include Multifunction Softswitches, Softswitches, local session controllers, Media Gateways, border controllers, end instruments, local area network switches, and routers.

System Under Test (SUT). The inclusive components required to test a Unified Capabilities product for Approved Products List certification. Examples of a SUT include time division multiplexing or circuit-switch components, Voice over Internet Protocol system components (e.g., local session controller and gateway), local area network components (e.g., routers and Ethernet switches), and end instruments.

C.1.21 T

Tandem Call Trace. A feature that identifies the incoming trunk of a tandem call to a specified office directory number. The feature is activated by entering the specified distant office directory number for a tandem call trace. A printout of the incoming trunk number and terminating directory number, and the time and date is generated for every call to the specified directory number.

Telebroadcast. Transmitted video or audio data that is viewed (or listened to) in real time; i.e., as the information is received. Streaming media may be user-controlled (as in on-demand, pay-per-view content) or server-controlled (as in webcasting).

Telecom Switch/Device. Hardware or software designed to send and receive voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the Defense Switched Network or public switch telecommunications network.

Teleconferencing. A conference among people remote from one another who are linked by one or more telecommunications devices.

Teleconferencing System. A collection of equipment and integral components (customer premises equipment and facilities) required to process teleconferencing programs and control data, less network interface devices.

TEMPEST-Approved. See TEMPEST in FED-STD-1037C. A device endorsed by the National Security Agency as meeting stringent signal radiation requirements. The electromagnetic waves it emits have been reduced through shielding or other techniques to a point where it would be extremely difficult for a hostile force to gather information from the electromagnetic waves and disclose the classified information being transmitted.

Ten-Digit Dialing. The ability to use ten digits comprising the area code, switch code, and line number to establish interswitch calls where the number plan area of the calling party is different from the number plan area of the called party.

Terminal Equipment. A device or devices connected to a network or other communications system used to receive or transmit data. It usually includes some type of input/output device.

Terminal ID. A form of identification that allows a conferencing terminal unit to be assigned an alphanumeric string such as a name or location rather than just an arbitrary terminal number.

Terminal Number. A number assigned by an multipoint control unit to a conferencing terminal unit (CTU) for identifying CTUs in a conference. Terminal numbering is necessary for call association, chair control, and video select capabilities.

Terminating Gateway. Assured Services Session Initiation Protocol (AS-SIP) for Telephones signaling appliance performing the terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway function in the case of TDM bridging call flows and IP-to-TDM call flows, and either directly serving the destination IP end instruments (EIs) or the AS-SIP signaling appliances representing the destination IP EIs in the case of TDM-to-IP call flows.

Terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function. The function related to receiving an Assured Services Session Initiation Protocol (AS-SIP) INVITE from the IP network and sending an Initial Address Message (IAM) onto the Signaling System No. 7 network. If the AS-SIP INVITE included an encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM, then it is decapsulated—identical to Incoming Interworking Unit in International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation Q.1912.5, Interworking between Session Initiation Protocol and Bearer Independent Call Control Protocol or ISUP.

Three-Way Calling. A feature that allows a station in the talking state to add a third party to the call without operator assistance.

Throughput. The number of octets is transmitted successfully (Internet Protocol) during the measurement interval (typically seconds). Assumes the packets sent do not exceed the capacity of the link. [GESP]

TIA (Telecommunications Industry Association) (http://www.tiaonline.org). A U.S. commercial standards organization aligned with the Electronic Industries Alliance (EIA). The acronym TIA/EIA precedes a numerical designation, such as TIA/EIA-232-F, that replaces the now obsolete RS (Recommended Standard) designation, for example, RS-232.

TIA/EIA-232-F (formerly RS-232). A serial interface standard for transmission of unbalanced signals between a variety of computer, media, and multimedia peripherals. TIA/EIA-232-F transmits at a maximum of 19.2 kilobits per second for up to a distance of about 50 feet and uses a type D-subminiature 25-pin (DB-25) connector, though other connectors have been used.

TIA/EIA-422 (formerly RS-422). A serial electrical interface standard for transmission of balanced and unbalanced signals between a variety of higher end computer, media, and multimedia peripherals. TIA/EIA-422 allows a maximum data rate of 10 megabits per second at a distance of 40 feet.

TIA/EIA-423 (formerly RS-423). A serial electrical interface standard for transmission of unbalanced signals between a variety of higher end computer, media, and multimedia peripherals. TIA/EIA-423 allows a maximum data rate of 100 kilobits per second at a distance of 30 feet.

TIA/EIA-530. A replacement for EIA-449 that uses a DB-25 connector instead of a 37-pin connector, while keeping the critical EIA-449 signals intact. TIA/EIA-530 is to be used in conjunction with TIA/EIA-422-B.

Trace Call in Progress. A feature that identifies the originating directory number or incoming trunk for a call in progress. The feature is activated by authorized personnel entering a request that includes the specific terminating directory number or trunk involved in the call.

Tracing of Terminating Calls. A feature that identifies the calling number on intraoffice calls or the incoming trunk on incoming calls for calls terminating to a specified directory number. When this feature is activated, a printout of the originating directory number or incoming trunk number, terminating directory number, and the time and date is generated for every call to the specified line.

Traffic Classification. A mechanism that allows the networks to distinguish among different categories of traffic, connection requests, and provisioning requests. The classification may be performed at the Edge and Core nodes during packet transport, as well as through indications in the control and management planes for setting up connections and provisioning. Classification can be based on fields in the packets and/or indications in control and management messages.

Traffic Conditioner. An entity that performs traffic conditioning functions and may contain meters, markers, droppers, and shapers. Typically, traffic conditioners are deployed in differentiated services boundary nodes only. A traffic conditioner may re-mark a traffic stream or may discard or shape packets to alter the temporal characteristics of the stream and bring it into compliance with a traffic profile. [RFC 2475]

Traffic Conditioning. Control functions performed to enforce traffic classification rules and may include traffic metering, marking, shaping, and policing. Traffic conditioning, when used, will be tied to the parameters chosen for the offered load control.

Traffic Conditioning Agreement (TCA). An agreement specifying classifier rules and any corresponding traffic profiles and metering, marking, discarding, and/or shaping rules that are to apply to the traffic streams selected by the classifier. A TCA encompasses all traffic conditioning rules explicitly specified within a service level agreement along with all the rules implicit from the relevant service requirements and/or from a differentiated services domain's service provisioning policy. [RFC 2475]

Traffic Engineering. An operator or automaton with the express purpose of minimizing congestion in a network. It encompasses the application of technology and scientific principles to the measurement, modeling, characterization, and control of Internet traffic, and the application of such knowledge and techniques to achieve specific performance objectives. [RFC 2702]

Transcoding. Provides the ability of converting a media stream from one format to another. Transcoding is often used to convert video/audio formats (i.e., H.261 to H.263, G.711 to G.722) to allow conference participants to communicate with each other even though their video endpoints are equipped with different encoding/decoding capabilities.

Trunks. Time division multiplexing links used by a circuit switch system to connect to or interconnect Defense Switched Network switches.

Trust Point. Public keys (or certificates containing them) that the relying party designates as reliable and trustworthy. The relying party should obtain the public keys (or certificates) through a reliable out-of-band method. Trust points are usually Root Certificates. Under certain circumstances, a relying party may decide to trust an intermediate Certificate Authority (CA) or even an end entity. Trust is transitive. If the relying party trusts a CA, it also trusts other CAs to which the CA delegates its CA responsibilities. This is also known as a trust anchor.

Turnkey. Pertaining to a procurement process that (1) includes contractual actions at least through the system, subsystem, or equipment installation phase, and (2) may include follow-on contractual actions, such as testing, training, logistical, and operational support. (188)

NOTE: Precise definition of the types of allowable contractual features are contained in the Federal Acquisition Regulations (FAR).

Type 1 A classified or controlled cryptographic equipment, assembly, component, or item endorsed by the National Security Agency for securing telecommunications and automated information systems for the protection of classified or sensitive U.S. Government information exempted by the Warner Amendment for use by the U.S. Government and its contractors, and subject to restrictions in accordance with the International Traffic in Arms Regulation.

Type 2 An unclassified cryptographic equipment, assembly, component, or item endorsed by the National Security Agency for use in telecommunications and automated information systems for the protection of unclassified but sensitive information. Type 2 equipment is exempted by the Warner Amendment. Type 2 is available to U.S. Government departments, agencies, sponsored elements of state and local government, sponsored U.S. Government contractors, and sponsored private sector entities. It is subject to restrictions in accordance with the International Traffic in Arms Regulation.

Type 3 An unclassified cryptographic equipment, assembly, component, or item that implements an unclassified algorithm registered with the National Institute of Standards and Technology as a Federal Information Processing Standard for use in protecting unclassified sensitive, or commercial, information. This definition does not include Warner-Amendment-exempt equipment.

C.1.22 U

Unclassified. Information or material that does not require protection in the interests of national security and that is not classified for such purposes by appropriate classifying authority in accordance with the provisions of Executive Order 12356, "National Security information," of April 2, 1982.

Unclassified Sensitive. A designation for information that is not classified, but needs to be protected from unauthorized disclosure. Examples of types of information that fall under this category are For Official Use Only (FOUO), proprietary, contractor sensitive, limited distribution, and personal in nature.

Unicasting. The process of transmitting data/information from one source to many destinations using multiple point-to-point transmissions.

Unified Capabilities (UC). The seamless integration of voice, video, and data services delivered ubiquitously across a secure and highly available network independent of technology infrastructure to provide increased mission effectiveness to the warfighter and business communities. Unified capabilities integrate standards-based communication and collaboration services including, but not limited to, the following:

- Messaging.
- Voice, video, and web conferencing.
- Unified communication and collaboration applications or clients.

These standards-based UC services are integrated with available enterprise applications, both business and warfighting.

User Agent Client (UAC). "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction." [RFC 3261]

User Agent Server (UAS). "A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction." [RFC 3261]

C.1.23 V

Very High Speed DSL (VDSL). VDSL is a DSL technology that permits the transmission of asymmetric and symmetric aggregate data rates up to tens of Mbps on twisted pairs. The maximum downstream rate is about 52 Mbps over lines up to 1,000 feet (300 meters) in length. The maximum upstream rate is 16 Mbps for lines up to 1,000 feet in length.

Very High Speed DSL 2 (VDSL2). VDSL2 is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for POTS services. It can be deployed from central offices, from fiber-fed cabinets located near the customer premises, or within buildings. VDSL2 is an enhancement to VDSL that supports asymmetric and symmetric transmission at a bidirectional net data rate up to 200 Mbps on twisted pair wiring. Loop distances can be up to 8,200 feet.

Video. The technology of capturing, recording, processing, storing, transmitting, and reconstructing in electronic form, a sequence of still images representing scenes in motion.

Video CODEC. See CODEC.

Video Mixing. The process of combining two or more video signals to produce a single composite frame (video image). This allows each participant in a conference to view more than one of the other participants in the conference simultaneously. For example, the composite video image may be a two-by-two array in which the video from four participants appears in four blocks within the array [i.e., Hollywood Squares (See continuous presence)]. This is contrasted with the method of mixing signals in the analog domain using a video quad splitter. This is also contrasted with windowing that uses multiple frames to display images from different sources, such as data, motion video, or graphics.

Video Server. A server that distributes video images on demand.

Video Switching. The process of switching the video signal that a participant sees to one of the other participants. The participant that is seen can be determined by the chairperson, the participants, or as a function of the audio signal.

Video Teleconferencing (VTC). 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.

Video Teleconferencing Unit (VTU). Video teleconferencing endpoint equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It may include input/output functions, embedded cryptographic functions, network interface functions, end-to-network signaling, and connections to networks.

Video Telephony. Relating to videophones and video teleconferencing.

Videoconferencing. See Video Teleconferencing.

Virtual Network Element (VT-NE). A VT-NE is any network element integrated into a certified Defense Switched Network switch. A VT-NE can be used for long local, encapsulated time division multiplexing, and proprietary Internet Protocol trunks.

Voice Activated Switching. The function of a multipoint control unit that determines which video signal is seen by the participants in a conference based on the audio signal. Typically, the loudest speaker will be seen by all the participants.

Voice over IP (VoIP) System. A set of components required to provide Defense Switched Network (DSN) Internet Protocol (IP) voice services from end instrument 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.

Voice over Secure Internet Protocol (VoSIP). The instantiation of Internet Protocol (IP) Telephony on a classified local area network or wide area network infrastructure that provides the routing of voice conversations using the Secure 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. Bidirectional interoperability with the Defense Red Switch Network is provided through the Defense Information Systems Agency-managed IP-to-Time Division Multiplexing interfaces.

Voiceband Data (VBD) (Modem Pass-Through). A subset of Modem over Internet Protocol in which modem signals are transmitted over the voice channel of a packet network.

C.1.24 W

Warner Amendment Title 10, United States Code, Section 2315. "Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes." Enacted as Public Law 97-86, 1 December 1981. The Warner Amendment amends Section 111 of the Federal Property and Administrative Services Act of automatic data processing equipment (currently defined to include telecommunications services and equipment) if the function, operation, or use of the equipment or services:

- Involves intelligence activities.
- Involves cryptologic activities related to national security.
- Involves the command and control of military forces.
- Involves equipment that is an integral part of a weapon or weapons system.
- Subject to (6) is critical to the direct fulfillment of military or intelligence missions.

Subpart (5) does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications.

Warner-Exempt. A telecommunications requirement that meets the stipulations as stated in the Warner Amendment.

Web-Scheduled Conferences. These conferences have a guaranteed time slot on a conference bridge for the number of participants, date, and time that you select. You reserve this time slot in advance by using an online scheduling interface.

Wide Area Network (WAN) Level Assured Services Admission Control (W-ASAC). The processes on a Softswitch that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the WAN conditions do not allow meeting quality of service requirements of all services. The processes are associated typically with the preemption of lower precedence sessions within the WAN to ensure that higher precedence sessions can be completed. In addition, the W-ASAC ensures that its subtended local session controllers remain within their traffic-engineered real time service allocations.

Wide Area Network Softswitch (WAN SS). An earlier term used for what is now defined as a Softswitch (SS).

Wideband Audio. In audio transmission, an audio signal of a wider bandwidth than 3 kilohertz (KHz) (nominal), or a carrier channel or system supporting that signal.

(NOTE: G.722 specifies a bandwidth of 7 KHz.)

Wireless. Can refer to either 802.x devices or cellular telephones.

Wireless Access Bridge (WAB). A device that connects two local area network segments together via wireless transmission.

Wireless Device. An 802.x device or cellular phone.

Wireless End Instrument (WEI). A Defense Switched Network IMMEDIATE/PRIORITY (I/P) or non-I/P user device that receives voice service via an IP telephone instrument using wireless technologies, such as 802.11 or 802.16. Also known as a wireless telephony subscriber.

Wireless Local Area Network (LAN) (WLAN). Generic term used to describe the use of wireless technologies in the LAN. The WLAN includes all the wireless terminology (i.e., wireless access bridge, wireless end instrument, and wireless LAN access system).

Wireless Local Area Network (LAN) Access System (WLAS). An implementation of wireless technologies considered to be the replacement of the physical layer of the wired Access Layer of a LAN.

C.1.25 X

XMPP Server. An XMPP server manages XMPP streams with locally hosted clients and delivers XML stanzas to those clients over the negotiated streams. The server also manages XML streams with peer servers and toutes XML stanzas to those servers over the negotiated streams. A server is responsible for the enforcement of security policies (e.g., user authentication and channel encryption), storing a user's roster, and maintaining presence information for all of its hosted users. A server may also host local services that use XMPP communitcation primatives (e.g., multiuser chat service). [Section2.2, RFC 6120]

XMPP Gateway: The XMPP gateway implementations provide a protocol translation function between XMPP and non-XMPP protocol (e.g., SIP/SIMPLE) in support of IM, Chat, and Presence services.

C.2 ACRONYM LIST

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ACD	Automatic Call Distribution
ACL	Access Control List
ACS	Access Control Server

ACRONYM	DEFINITION
ADC	Analog-to-Digital Converter
ADN	Area Distribution Node
ADSL	Asymmetric Digital Subscriber Line
ADSL2	Asymmetric Digital Subscriber Line Transceivers 2
AEI	Assured Services End Instrument
AEI	Assured Services Session Initiation Protocol Video End Instruments
AEI	Assured Services Session Initiation Protocol Voice End Instruments
AF3	Class 3 Assured Forwarding
AF4	Class 4 Assured Forwarding
AG	Access Gateway
AGF	Aggregation Grooming Function
AOR	Area of Responsibility
AP	Association Path
APCO	Association of Public Safety Communications Officials
APL	Approved Products List
AR	Aggregation Router
ASAC	Assured Services Admission Control
ASF	Assured Services Features
ASLAN	Assured Services Local Area Network
ATA	Analog Terminal Adapter
ATM	Asynchronous Transfer Mode
AVSC	Available Link Session Capacity
B2BUA	Back-to-Back User Agent
BGP	Border Gateway Protocol
BITS	Building Integrated Timing Supply
BNEA	Busy Not Equipped Announcement
BoD	Bandwidth on Demand
BPA	Blocked Precedence Announcement
BRI	Basic Rate Interface
BW	Bandwidth
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
CAC	Call Admission Control
CAN	Campus Area Network
CAS	Channel Associated Signaling
CC	Combatant Command

ACRONYM	DEFINITION
CCA	Call Connection Agent
CCS7	Common Channeling Signaling 7
CD	Collision Detection
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CE	Customer Edge
CE-R	Customer Edge Router
CERDEC	Communications, Electronics, Research, Development, and Engineering Center
CES	Common Enterprises Services
CF	Call Forwarding
CFBL	Call Forwarding Busy Line
CFDA	Call Forwarding Don t Answer
CFV	Call Forwarding Variable
CHVP	Controlled High-Value Products
CIFS	Common Internet File System
CIO	Chief Information Officer
CIK	Crypto Ignition Key
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	Configuration Management
CMI	Cryptographic Modernization Initiative
COIN	Community of Interest Network
COMSEC	Communications Security
CONUS	Continental United States
COOP	Continuity of Operations
COPS	Common Open Policy Service
COTS	Commercial off-the-Shelf
C-PE	Classified Provider Edge
CPU	Central Processing Unit
CS	Circuit Switched
CSMA	Carrier Sense Multiple Access
CSU	Channel Servicing Unit
CUI	Controlled Unclassified Information
CVBG	Carrier Battle Groups
CW	Call Waiting
DAA	Designated Approval Authority
DAC	Digital-to-Analog Converter
DAMA	Demand Assigned Multiple Access

ACRONYM	DEFINITION
DASAC	Dynamic Assured Services Admission Control
DCB	Data Center Bridging
DCN	Data Communications Network
DCO	Defense Connect Online
DCS	Defense Collaboration Service
DCVX	Deployed Cellular Voice Exchange
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
DITO	DISA IPv6 Transition Office
DLoS	Direct Line of Sight
DMZ	Demilitarized Zone
DN	Directory Number
DNS	Domain Name Service
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
DRSN	Defense RED Switch Network
DS0	Digital Signal Level 0
DSCD	Department of Defense Secure Communications Devices
DSCP	Differentiated Services Code Points
DSLAM	Digital Subscriber Line Access Manager
DSN	Defense Switched Network
DSS	Defense Information Systems Network Subscription Services
DSSS	Dual-Signaling Softswitch
DSU	Data Servicing Unit
DTD	Data Transfer Device
DTMF	Dual Tone Multifrequency
DVR	Digital Video Recorder
DVS	Defense Information Systems Network Video Services
DVX-C	Deployed Voice Exchange – Commercial
E2E	End-to-End
ECU	End Cryptographic Unit
EF	Expedited Forwarding

ACRONYM	DEFINITION
EFFV	Enhanced Firefly Vector
EFM	Ethernet in the First Mile
EFMCu	Ethernet in the First Mile Over Copper
EI	End Instrument
EIA	Electronics Industry Association
EISC	End Instrument Session Capacity
eMLPP	Enhanced Multilevel Precedence and Preemption
EMS	Element Management System
ENUM	Electronic Numbering
EO	End Office
EPS	Emergency Power System
ESA	Enterprise Services Area
ESC	Enterprise Session Controller
ESP	Encapsulating Security Payload
EUB	End User Building
F	FLASH
F1SC	Failover Type 1 Session Controller
F2SC	Failover Type 2 Sessoin Controller
FC	Fibre Channel
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCoE	Fibre Channel Over Ethernet
FCP	Fibre Channel Protocol
F-D	Fixed-to-Deployable
F-F	Fixed-to-Fixed
FFR	Fast Failure Recovery
FFV	Firefly Vector
FIPS	Federal Information Processing Standard
FNBDT	Future Narrowband Digital Terminal
FO	FLASH OVERRIDE
FO/F	FLASH/OVERRIDE FLASH
FoIP	Fax over Internet Protocol
FPL	Fixed Packet Length
FQDN	Fully Qualified Domain Name
FRR	Fast Reroute
FSO	Field Security Office
FTP	File Transfer Protocol

ACRONYM	DEFINITION
FW	Firewall
FY	Fiscal Year
GEM	Global Information Grid Enterprise Management
GIG	Global Information Grid
GigE	Gigabit Ethernet
GNA	Global Information Grid Network Assurance
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSTP	Generic Switch Test Plan
H2M	Human-to-Machine
HAIPE	High Assurance Internet Protocol Encryptor
HCI	Human Computer Interface
HDSL	High Bit Rate Digital Subscriber Line
HR	Hybrid Routing
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol, Secure
I	IMMEDIATE
I/P	IMMEDIATE/PRIORITY
IAD	Integrated Access Device
IAP	Internet Access Point
IAVA	Information Assurance and Vulnerability Assessment
IAW	In Accordance With
IC	Intelligence Community
ICCS	Intra Cluster Communication Signaling
ID	Identification
IDNX	Integrated Digital Network Exchange
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IM	Instant Messaging
INE	In-Line Network Encryptor
INFOSEC	Information Security
IP	Internet Protocol
IPB	Internet Protocol Budget
IPC	Internet Protocol Count
IPDR	Internet Protocol Detail Record s

ACRONYM	DEFINITION
IPDV	Internet Protocol Packet Delay Variation
IPLR	Internet Protocol Packet Loss Ratio
ipm	Impulse per Minute
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IS	Interoperability Specification
iSCSI	Internet Small Computer System Interface
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISS	Information Sharing Service
IT	Information Technology
ITU-T	International Telecommunications Union – Telecommunication
IVR	Interactive Voice Response
IWF	Interworking Function
JCIDS	Joint Capabilities Integration and Development System
JCONOPS	Joint Concept of Operations
JITC	Joint Interoperability Test Command
JNN	Joint Network Node
JSOTF	Joint Special Operation Task Force
JTRS	Joint Tactical Radio System
JUICE	Joint User Interoperability Communications Exercise
JWICS	Joint Worldwide Intelligence Communications System
KMI	Key Management Infrastructure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	Lightweight Directory Access Protocol Interchange Format
LEF	Link Encryptor Family
LOC	Letter of Compliance
LS	Local Area Network Switch
M/SM	Mesh/Semi Mesh
M2M	Machine-to-Machine
MAC	Media Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad Hoc Network
Mbps	megabits per second

ACRONYM	DEFINITION
MBSS	Multifunction Mobile Device Backend Support System
MCEP	Multi Carrier Entry Point
MCN	Main Communication Node
MCU	Multipoint Conferencing Unit
MDM	Mobile Device Management
MDT	Mean Downtime
MEF	Marine Expeditionary Force
MER	Minimum Essential Requirement
MF	Multifrequency
MFS	Multifunction Switch
MG	Media Gateway
MGC	Media Gateway Controller
MG-LS	Media Gateway – Line Side
MG-TS	Media Gateway – Trunk Side
MHz	megahertz
MIB	Management Information Base
MILDEP	Military Department
MLPP	Multilevel Precedence and Preemption
MMD	Multifunction Mobile Device
MNWS	Mass Notification Warning System
MO	Milestone Objective
MoIP	Modem over Internet Protocol
MOS	Mean Opinion Score
MP	Multilink Protocol
MPCA	Moving Picture Compression Algorithm
MPLS	Multiprotocol Label Switching
MSC	Master Session Controller
MSPP	Multi-Service Provisioning Platform
MTBF	Mean Time Between Failure
MTBM	Mean Time Between Maintenance
MTTR	Mean Time To Repair
MUF	Military Unique Feature
MUX	Multiplexer
MVNO	Mobile Virtual Network Operator
N	NUMBER
NAPT	Network Address and Port Translation

ACRONYM	DEFINITION
NAS	Network Attached Storage
NAT	Network Address Translation
NAVSTAR	Navigation Satellite Timing and Ranging
NCES	Net-Centric Enterprise Services
NCI	Network Component Infrastructure
NCTAMS	Naval Computer and Telecommunications Area Master Station
NES	Network Encryption System
NetOps	Network Operations
NEXT	Near End Crosstalk
NFS	Network File System
NIAP	National Information Assurance Partnership
NISP	Network Infrastructure Product
NIST	National Institute of Standards and Technology
NM	Network Management
NMCC	National Military Command Center
NOC	Network Operations Center
NOSC	Network Operations and Security Center
NPA	Numbering Plan Area
NR-KPP	Net Ready Key Performance Parameter
NRT	Near-Real Time
NSA	National Security Agency
NSS	National Security Space
NTP	Network Time Protocol
O&M	Operations and Maintenance
OA&M	Operations, Administration, and Maintenance
OAM&P	Operations, Administration, Maintenance, and Performance
OAN	Operational Area Network
OCONUS	Outside the Continental United States
OCSP	Online Certificate Status Protocol
ODXC	Optical Digital Cross-Connect
OEM	Original Equipment Manufacturer
OLA	Optical Line Amplifier
OLT	Optical Line Terminal
ONU	Optical Network Unit
OSC	Optical Supervisory Channel
OSI	Open System Interconnect

ACRONYM	DEFINITION
OSPF	Open Shortest Path First
OSS	Operational Support System
OTAD	Over-the-Air Distribution
OTAR	Over-the-Air Rekey
OTS	Optical Transport System
P	PRIORITY
P2MP	Point-to-Multipoint
P2N	Point-to-Network
P2P	Point-to-Point
PBAS	Precedence-Based Assured Services
PBX	Private Branch Exchange
PCA	Picture Compression Algorithm
PDA	Personal Digital Assistant
PDUN	Peer Destination Unreachable Notification
PE	Provider Edge
PED	Portable Electronic Device
PEI	Proprietary Internet Protocol Voice End Instrument
PHB	Per-Hop Behavior
PHRD	Peer High Assurance Internet Protocol Encryptor Reachability Detection
PKI	Public Key Infrastructure
PM	Performance Management
PON	Passive Optical Network
PPK	Pre-Placed Key
PPP	Point-To Point Protocol
PPS	Packets per Second
PPSM	Ports, Protocols, and Services Management
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R	ROUTINE
RADIUS	Remote Authentication Dial-in User Server/Service
RAE	Required Ancillary Equipment
RF	Radio Frequency
RFC	Request for Comment
RIP	Router Information Protocol

ACRONYM	DEFINITION
ROADM	Reconfigurable Optical Add-Drop Multiplexer
ROEI	ROUTINE Only End Instrument
RTP	Real-Time Transport Protocol
RTS	Real-Time Services
RTT	Round-Trip Time
SA	Situational Awareness
SAC	Session Admission Control
SAN	Storage Area Network
SBC	Session Border Controller
SC	Session Controller
SCF	Selective Call Forwarding
SCIP	Secure Communication Interoperability Protocol
SCLS	Session Controller Location Server
SCPC	Single Channel per Carrier
SCS	Session Control and Signaling
SCTP	Stream Control Transmission Protocol
SDN	Service Delivery Node
SDP	Session Description Protocol
SDS	Secure DTD2000 System
SEI	Secure End Instrument
SG	Signaling Gateway
SHDSL	Single Pair High-Speed Digital Subscriber Line
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extension
SIP	Session Initiation Protocol
SIPRNet	Secure Internet Protocol Router Network
SIPS	Session Initiation Protocol Secure
SKL	Simple Key Loader
SME	Secure Mobile Environment
SMEO	Small End Office
SMI	Security Management Infrastructure
SMIv2	Structure of Management Information Version 2
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMPv3	Simple Network Management Protocol Version 3
SPD	Security Policy Database
SPG	Sync Pulse Generator

ACRONYM	DEFINITION
SPRT	Simple Packet Relay Transport
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SS	Softswitch
SSC	Subtended Session Controller
SSE	State Signaling Event
SSHv2	Secure Shell Version 2
SSLS	Softswitch Location Service
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guideline
SUT	System Under Test
SW	Software
T&S	Timing and Synchronization
TA	Terminal Adapter
TACACS	Terminal Access Controller Access Control System
TACLANE	Tactical Local Area Network Encryptor
TB	Terabyte
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDIM	Time Division Inverse Multiplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDMB	Time Division Multiplexing Session Budget
TDMC	Time Division Multiplexing Session Count
TG	Trunk Gateway
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TNCC	Theater Network Operations Control Center
TOC	Tactical Operations Center
TRANSEC	Transmission Security
TRN	Tactical Radio Network (Gateway)
TS	Transport Switching
TSC	Transmission Link Session Capacity
TSF	Transport Switch Function
TWC	Three-Way Calling
U-AR	Unclassified Aggregation Router

ACRONYM	DEFINITION
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
UCR	Unified Capabilities Requirements
UDP	User Datagram Protocol
UFS	User Features and Services
U-PE	Unclassified Provider Edge
URI	Uniform Resource Indicator
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command
UTC	Universal Time Coordinated
UTP	Unshielded Twisted Pair
UUT	Unit Under Test
VBD	Voiceband Data
VDS	Video Distribution System
VDS-IP	Video Distribution System Over Internet Protocol
VDSL	Very High Speed Digital Subscriber Line
VF	Voice Frequency
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPCC	Video Distribution System Peripheral Connector Conversion
VPN	Virtual Private Network
VSU	Video Session Unit
VTC	Video Teleconferencing
VTR	Video Tape Recording
VVoIP	Video and Voice Over IP
WAN	Wide Area Network
WGS	Wideband Gapfiller System
WLAN	Wireless Local Area Network
WOC	Wide Area Network Optimization Controller
WPS	Wireless Priority Service
XMPP	Extensible Messaging and Presence Protocol

C.3 REFERENCES

C.3.1 American National Standards Institute Documentation

PUBLICATION NUMBER	TITLE	DATE
T1M1.5/2003-007R4	American National Standard Institute (ANSI), "Operations, Administration, Maintenance, and Provisioning Security Requirements for Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane"	Draft Proposed April 1, 2003
T1.101-1987	*Synchronization Interface Standards for Digital Networks*	1987
T1.102-1993	*Digital Hierarchy – Electrical Interfaces*, December	1993
T1.102-1999	*Digital Hierarchy – Electrical Interfaces*	1999
T1.105-2001	*Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*	May 2001
T1.105.1-2000	*Synchronous Optical Network (SONET) – Automatic Protection*	Revised 2005
T1.105.03-1994	*Synchronous Optical Network (SONET) – Jitter Network Interfaces*	Revised 2008
T1.105.03-2003	*Synchronous Optical Network (SONET) – Jitter Network Interfaces*	Revised 2008
T1.105.06-2002	*Synchronous Optical Network (SONET) – Physical Layer Specifications*	Revised 2007
T1.107-2002	*Digital Hierarchy – Formats Specifications*	Revised 2006
T1.110	*Signaling System Number 7 (SS7) –General Information*	2006
T1.111	*Signaling System Number 7 (SS7) – Message Transfer Part (MTP)*	2001
T1.112	*Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP)*	2001
T1.113	*Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*	1995
T1.113-2000	*Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*. (Revision of T1.113-1995; includes two Supplements: T1.113a-2000 and T1.113b-2001)	
T1.114-2000	*Signaling System Number 7 (SS7) – Transaction Capabilities and Application Part (TCAP)*	2000
T1.116	*Signaling System Number 7 (SS7) – Operations, Maintenance, and Administration Part (OMAP)*	2000
T1.231-1993	*Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*	1993
T1.231.01-2003	*Digital Subscriber Line (DSL) – Layer 1 In-Service Digital Transmission Performance Monitoring*	Revised 2007
T1.264	*Operations, Administration, Maintenance, and Provisioning (OAM&P) – Model for Alarm Synchronization, for Telecommunications*	1999
T1.401	*Network to Customer Installation Interfaces – Analog Voice Grade Switched Access Lines Using Loop-Start and Ground Start Signaling*	1993
T1.403-1999	*Network to Customer Installation Interfaces – DS1 Electrical Interface*	Revised 2007

PUBLICATION NUMBER	TITLE	DATE
T1.404-2002	*Network and Customer Installation Interfaces – DS3 Metallic Interface Specification* (Revision and Consolidation of T1.404-1994 and T1.404a-1996)	Revised 2006
T1.408	*Integrated Services Digital Network (ISDN) Primary Rate – Customer Installation Metallic Interfaces Layer 1 Specification*	1990
T1.523-2000	*Telecom Glossary*	2000
T1.601-1999	*ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification*	
T1.602	*Data Link Layer Signalling Specification for Application at the User-Network Interface*	February 2000
T1.605-1991	*ISDN Basic Access Interface for S and T Reference Points and Layer 1* (1999) *Specification*	
T1.607-1998	*ISDN Layer 3 Signaling Specifications for Circuit Switched Bearer Service for Digital Subscriber Signaling System No. 1 (DSS1)*	
T1.613-1992	*ISDN Call Waiting Supplementary Service*	
T1.615-1992	*Digital Subscriber Signalling System No. 1 (DSS1)-Layer 3 Overview*	(R1999)
T1.616-1992	*ISDN Call Hold Supplementary Service*	
T1.619-1992	*Integrated Services Digital Network (ISDN) – Multi-Level Precedence*	
(R2005)	*and Preemption (MLPP) Service Capability*	February 1992 Reaffirmed 2005
T1.619a-1994 (R1999)	*Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability (MLPP Service Domain and Cause Changes)*	July 1994 Reaffirmed 1999
T1.621-1992	*ISDN User-to-User Signaling Supplementary Service*	
T1.632-1993	*ISDN Normal Call Transfer Supplementary Service*	
T1.642-1993	*ISDN Call Deflection Supplementary Service*	
T1.643-1995	*ISDN Explicit Call Transfer Supplementary Service*	
T1.647-1995	*ISDN Conference Calling Supplementary Service*	
ANSI/TIA-1057	*Link Layer Discovery Protocol for Media Endpoint Device*s	April 2006
T1X1.3/94-001R5	*Jitter Measurement Methodology*	
T11 FC-BB-5	*Fibre Channel – Fibre Channel Backbone – 5 (FC-BB-5)*, Revision 2.00	4 June 2009
X3.230	See ANSI INCITS 230-1994	
X3.296	*Information Technology – Single-Byte Command Code Sets Connection (SBCON) Architecture*, Replaces ANSI X3.296-1997	
X3.297	*Fibre Channel Physical and Signalling Interface – 2 (FC-PH-2)*	1997
X3.303	*Fibre Channel Physical and Signalling interface - 3 (FC-PH-3)*	1997
INCITS 230-1994	*Information Technology - Fibre Channel - Physical and Signaling Interface (FC-PH) - Amendment 2* (supplement to ANSI X3.230-1994) (formerly ANSI X3.230-1994/AM 2-1999)	

PUBLICATION NUMBER	TITLE	DATE
INCITS 374-2003	*Information Technology – Fibre Channel – Single-Byte Command Code Sets Mapping Protocol – 3 (FC-SB-3)*	2003
ANSI/TIA-810-B	*Telecommunications – Telephone Terminal Equipment – Transmission Requirements for Narrowband Voice over IP and Voice over PCM Digital Wireline Telephones*, SP-3-4352-RV2 (to become ANSI/TIA-810-B)	

C.3.2 Assistant Secretary of Defense for Networks & Information Integration/DoD Chief Information Office

AGENCY	TITLE	DATE
ASD(NII)/DoD CIO Memorandum	"Department of Defense Unified Capabilities Requirements"	current edition
ASD(NII)/DoD CIO	"Global Information Grid (GIG) Architectural Vision"	
ASD(NII)/DoD CIO	"DoD Unified Capabilities 2008 (UCR 2008)"	January 2009
ASD(NII)/DoD CIO	"DoD Unified Capabilities 2008 (UCR 2008) Change 1"	January 2010
ASD(NII)/DoD CIO	"DoD Unified Capabilities 2008 (UCR 2008) Change 2"	December 2010
ASD (NII)/DoD CIO	"DoD Unified Capabilities 2008 (UCR 2008) Change 3"	September 2011

C.3.3 British Standards Institute Documentation

PUBLICATION NUMBER	TITLE	DATE
BS EN 60950-1:2006	"Information Technology Equipment. Safety. General Requirements"	August 6, 2006

C.3.4 Chairman of the Joint Chiefs of Staff Documentation

PUBLICATION NUMBER	TITLE	DATE
	CJCS Standing Execute Order for Computer Network Attack and Computer Network Defense	January 20, 2004
CJCSI 6211.02D	"Defense Information Systems Network (DISN) Responsibilities," http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf.	January 24, 2012
CJCSI 6212.01E	"Interoperability and Supportability of Information Technology and National Security Systems," http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf.	December 15, 2008
CJCSM 3170.01C	"Operation of the Joint Capabilities Integration and Development System," www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf	May 1, 2007

C.3.5 Defense Information Systems Agency Documentation

TITLE	DATE
Defense Information Systems Agency, DISA Circular 310-55-1.	
Defense Information Systems Agency, DISA Circular 310-255-1, "DSN User Services Guide,".	April 21, 1998
DISA Field Security Operations, "Instant Messaging Checklist," Version 1, Release 1.3,.	February 15, 2008
"Initial Capabilities Document for Global Information Grid 2.0 (GIG 2.0),".	May 29, 2009
DISA Security Technical Implementation Guides (STIGs) are listed on the http://iase.disa.mil/stigs/index.html website.	
Global Information Grid Enterprise Services, DISA Web page.	

C.3.6 Department of Defense Documentation

TITLE	DATE
Center for DISN Services, "DISN Service Level Agreement for the Defense Information Systems Agency and its customers"	
Common Criteria Evaluation and Validation Scheme	August 6, 2004
Department of Defense 8910.1-M, "DoD Procedures for Management of Information Requirements"	June 30, 1998
"Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements," Version 1.0	July 13, 2000
Department of Defense Collaboration Interoperability Standards, J.P. Stenbit, Memorandum	November 1, 2002
Department of Defense, "GIG Architecture Master Plan," Final Draft	November 29, 2002
Department of Defense, "GIG Architecture Project Management Plan"	August 14, 2002
"Department of Defense Joint Technical Architecture (JTA)," Version 6, Volumes I and II	October 3, 2003
Deputy Secretary of Defense, "Smart Card Adoption and Implementation"	November 10, 1999
Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartmented Information within Information Systems"	June 5, 1999
"DoD Architecture Framework Version 1.0"	February 8, 2004
DoD CIO, "Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise," Version 1	June 2007
DoD CIO Guidance IA6-8510 IA	
DoD Information Technology Standards Registry (DISR) IPv6 Standards Technical Working Group (TWG), "DoD IPv6 Standard Profiles for IPv6 Capable Products," Version 1.0	June 1, 2006
"DoD PKI Functional Interface Specification," Version 3.0	September 2010
DoD PKI PMO, "DoD PKE Application Requirements Specification"	latest version
Department of Defense, "X.509 Certificate Policy," Version 10.4, http://iase.disa.mil/pki-pke/downloads/unclass-dod_cp_v10-4.pdf	June 21, 2012
"DoD Policy for Enterprise-wide Deployment of IPv6"	June 9, 2003
DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6) Interim Transition Guidance"	September 29, 2003

TITLE	DATE
DoD CIO Memorandum, "Internet Protocol Version 6 (IPv6)"	June 9, 2003
DoD CIO Memorandum "DoD IPv6 Definitions"	June 26, 2008
DoD Unified Facilities Criteria (UFC), "Design and O&M: Mass Notification Systems," Change 1	January 2010
DSN Systems Design, Implementation, and Transition Branch, "Defense Switched Network (DSN) IPv6 Transition Plan," Version 1.1	June 28, 2006
Office of DoD CIO, "DoD Internet Protocol Version 6 (IPv6) Transition Plan," Version 1.0	November 2003
"The Global Information Grid (GIG) Enterprise Service Profile"	
United States Strategic Command (STRATCOM), "Joint Concept of Operations for Global Information Grid Network Operations (NetOps)"	April 20, 2004

C.3.7 DoD Directives

PUBLICATION NUMBER	TITLE	DATE
DoDD 5000.01	"The Defense Acquisition System," 12 May 2003	certified current as of November 20, 2007
DoDD 5200.28	"Security Requirements for Automated Information Systems (AISs)"	March 21, 1988
DoDD 8500.01E	"Information Assurance (IA)," October 24, 2002http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.	certified current as of April 23, 2007

C.3.8 DoD Instructions

PUBLICATION NUMBER	TITLE	DATE
DoDI 5000.02	"Operation of the Defense Acquisition System"	December 8, 2008
DoDI 8100.04	"DoD Unified Capabilities"	December 2010
DoDI 8410.02	"NetOps for the Global Information Grid (GIG)"	December 19, 2008
DoDI 8510.01	"DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)"	November 28, 2007

C.3.9 Electronics Industries Alliance

PUBLICATION NUMBER	TITLE	DATE
EIA-366-A	"Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication"	March 1979
EIA-422-B	"Electrical Characteristics of Balanced Voltage Digital Interface Circuits"	1994
EIA-449-1	"General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange"	January 2000

PUBLICATION NUMBER	TITLE	DATE
EIA-530	"Interconnection of DTE and DCE Employing Serial Binary Data Interchange with Control Information Exchanged on Separate Control Circuits."	
TIA-530-A	"High Speed 25 Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector"	December 2003

C.3.10 ETSI Documentation

PUBLICATION NUMBER	TITLE	DATE
EN 50022	"Specification for low voltage switchgear and controlgear for industrial gear"	1977
EN 50082 ETS-FN-50022	"Electromagnetic compatibility. Generic immunity standard. Residential, commercial and light industry"	January 1998
ETS 300 019	"Equipment Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment"	1994
EN 300 386	"Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements," Version 1.5.1	May 2010
TS 102 165-1	"Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) – Methods and protocols; Part 1: Method and Proforma for Threat, Risk, Vulnerability Analysis," Version 4.2.1	December 2006
TS 102 165-2	"Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols;; Part 2: Protocol Framework Definition; Security Counter Measures," Version 4.2.1	February 2007
TS 183 029	Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification, Version 2.6.0	June 2008

C.3.11 Federal Information Processing Standards Publications

PUBLICATION NUMBER	TITLE	DATE
FIPS PUB 140-2	U.S. Department of Commerce/National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules"	May 25, 2001

C.3.12 Institute of Electrical and Electronics Engineers, Inc. Documentation

PUBLICATION NUMBER	TITLE	DATE
455-1985	IEEE Standard for Standard Test Procedure for Measuring Longitudinal Balance of Telephone Equipment Operating in the Voice Band	January 1, 2001
802.1p	IEEE Standard for Traffic Class Expediting and Dynamic Multicast Filtering (published in 802.1D-1998)	
802.1AB-2009	IEEE Standard for Station and Media Access Control Connectivity Discovery	September 11, 2009
802.1AX-2008	IEEE Standard for IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation	2008
802.1D™-2004	IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges	June 2004
802.1Q™-1998	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	January 1, 1998
802.1Q™-2003	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	2003
802.1Qau	IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: 10: Congestion Notification	September 15, 2006
802.1Qaz	IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: Enhanced Transmission Selection	March 27, 2008
802.1Qbb	IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks – Amendment: Priority-based Flow Control	March 27, 2008
802.1s	IEEE Standard for Local and Metropolitan Area Networks: Multiple Spanning Trees (Merged into 802.1Q-2003).	2003
802.1w	IEEE Standard for Local and Metropolitan Area Networks: Rapid Reconfiguration of Spanning Tree (Merged into 802.1D-2004).	2003
802.1X™-2001	IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control	2001
802.1X™-2004	IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control	2004
802.3™-1993	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications	1993
802.3™-2008	IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications	December 26, 2008

PUBLICATION NUMBER	TITLE	DATE
802.3i	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair	1990
802.3u-1995	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/autonegotiation	1995
802.3x-1997	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Full Duplex and flow control	1997
802.3z-1998	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s)	1998
802.3ab-1999	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: http://en.wikipedia.org/wiki/802.3ab1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s)	1999
802.3ad-2000	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Link aggregation for parallel links	2000
802.3ae-2003	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10 Gbit/s (1,250 MB/s) Ether over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW	2003
802.3ah-2004	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Media Access Control Parameters, Physical layers, and Management Parameters for Subscriber Access Networks	2004

PUBLICATION NUMBER	TITLE	DATE
802.3at-2009	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements	2009
802.3av-2009	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications- Amendment 1: Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks	2009
802.3ba-2010	IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Amendment 4: Media Access Control Parameters, Physical Layers and Management Parameters for 40 Gb/s and 100 Gb/s Operation	2010
802.11™-2007	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	June 2007
802.11a	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band	June 2003
802.11b	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band	June 2003
802.11e	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless LAN for Quality of Service	June 2003
802.11e-2005	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8, Medium Access Control (MAC) Quality of Service Enhancements	February 9, 2006

PUBLICATION NUMBER	TITLE	DATE
802.11h	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 5	December 29, 2003
802.11i	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6, Medium Access Control (MAC)	February 14, 2005
802.11g	Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band	June 2003
802.11n	IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements –Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput	
802.16™-2004	IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems	October 1, 2004
802.16d™	Standard for Amendment to IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Detailed System Profiles for 2-11 GHz	December 11, 2002
802.16e™	IEEE Standard for Local and metropolitan area networks— Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands *and* Corrigendum 1	February 28, 2006
802.17-2004	IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications	September 24, 2006

C.3.13 International Telecommunication Union Documentation

PUBLICATION NUMBER	TITLE	DATE
E.164	ITU-T Recommendation E.164, "The International Public Telecommunication Numbering Plan," Geneva, Switzerland	2005
G.107	ITU-T Recommendation G.107, "The E-model: a computational model for use in transmission planning," Geneva, Switzerland	April 2009
G.165	ITU-T Recommendation G.165, "Echo cancellers," Geneva, Switzerland	November 1988

PUBLICATION NUMBER	TITLE	DATE
G.168	ITU-T Recommendation G.168, "Digital network echo cancellers," Geneva, Switzerland	January 2007
G.651	ITU-T Recommendation G.651, "Characteristics of a 50/125 µm multimode graded index optical fibre cable"	February 1998
G.651.1	ITU-T Recommendation G.651.1, "Characteristics of a 50/125 µm multimode graded index optical fibre cable for the optical access network," Geneva, Switzerland	July 2007
G.652	ITU-T Recommendation G.652, "Characteristics of a single-mode optical fibre and cable," Geneva, Switzerland	June 2005
G.655	ITU-T Recommendation G.655, "Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable," Geneva, Switzerland	March 2006
G.664	ITU-T Recommendation G.664, "Optical safety procedures and requirements for optical transport systems"	August 2012
G.671	ITU-T Recommendation G.671, "Transmission characteristics of optical components and subsystems"	February 2012
G.691	ITU-T Recommendation G.691, "Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers," Geneva, Switzerland	March 2006
G.693	ITU-T Recommendation G.693, "Optical interfaces for intra-office systems," Geneva, Switzerland	May 2006
G.694.1	ITU-T Recommendation G.694.1, "Spectral grids for WDM applications: DWDM frequency grid," Geneva, Switzerland	2002
G.703	ITU-T Recommendation G.703, "Physical/Electrical Characteristics of Hierarchical Digital Interfaces at 1544, 2048, 8448, and 44736 kbit/s Hierarchical Levels"	2001
G.704	ITU-T Recommendation G.704, "Series G: Transmission Systems and Media, Digital Systems and Networks—Digital transmission systems – Terminal equipments – General Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels"	October 1998
G.707/Y.1322	ITU-T Recommendation G.707/Y.1322, "Network node interface for the synchronous digital hierarchy (SDH)," Geneva, Switzerland	January 2007
G.709/Y.1331	ITU-T Recommendation G.709/Y.1331, "Network node interface for the optical transport network (OTN)," Geneva, Switzerland	March 2003
G.711	ITU-T Recommendation G.711, "General Aspects of Digital Transmission Systems, Terminal Equipments, Pulse code modulation (PCM) of voice frequencies," Geneva, Switzerland	November 1988
	Appendix I, "A high quality low complexity algorithm for packet loss concealment with G.711," Geneva, Switzerland	September 1999
	Appendix II, "A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems," Geneva, Switzerland	February 2000
G.722	ITU-T Recommendation G.722, "7 kHz audio-coding within 64 kbit/s," Geneva, Switzerland	November 1988

PUBLICATION NUMBER	TITLE	DATE
G.723.1	ITU-T Recommendation G.723.1, "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s," Geneva, Switzerland,.	May 2006
G.726	ITU-T Recommendation G.726, "32 kbps Adaptive Differential Pulse Code Modulation (ADPCM)," Geneva, Switzerland,.	December 1990
G.728	ITU-T Recommendation G.728, "Coding of speech at 16 kbit/s using low-delay code excited linear prediction," Geneva, Switzerland,.	September 1992
G.729	ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)," Geneva, Switzerland, March 1996, plus Erratum 1, April 2006, and Annexes A through J, and Appendices I, II, and III	March 1996 April 2006
G.729.1	ITU Recommendation G.729.1 (2006) Amendment 1, "New Annex A on G.729.1 usage in H.245, plus corrections to the main body and updated test vectors," Geneva, Switzerland	January 2007
	This corrigendum was never published, its content having been included in the published ITU-T Recommendation G.729.1 (2006)	
G.729.1	ITU Recommendation G.729.1 (2006), "G.729 based Embedded Variable bit-rate codor: An 8-32 kbit/s scalable wideband coder bit stream interoperable with G.729," Geneva, Switzerland	May 2006
	This edition includes the modifications introduced by G.729.1 (2006) Amd. 1 approved on 13 January 2007, and G.729.1 (2006) Amd. 2 approved on 13 February 2007	
G.732	ITU-T Recommendation G.732, "Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s," Geneva, Switzerland,.	November 1988
G.772	ITU-T Recommendation G.772, "Protected monitoring points provided on digital transmission systems"	March 1993
G.775	ITU-T Recommendation, G.775, "Loss of Signal (LOS), Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) defect detection and clearance criteria for PDH signals"	October 1998
G.783	ITU-T Recommendation G.783, "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks," Geneva, Switzerland	March 2006
G.798	ITU-T Recommendation G.798, "Characteristics of optical transport network hierarchy equipment functional blocks"	October 2011
G.806	ITU-T Recommendation G.806, "Characteristics of transport equipment – Description methodology and generic functionality"	February 2012
G.808.1	ITU-T Recommendation G.808.1, "Generic protection switching – Linear trail and subnetwork protection"	February 2010
G.811	ITU-T Recommendation G.811, "Timing characteristics of primary reference clocks"	1997
G.823	ITU-T Recommendation G.823, "The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy"	March 2000

PUBLICATION NUMBER	TITLE	DATE
G.825	ITU-T Recommendation G.825, "The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)," Geneva, Switzerland	March 2003
G.826	ITU-T Recommendation G.826, "End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections," Geneva, Switzerland	December 2002
G.829	ITU-T Recommendation G.829, "Error performance events for SDH multiplex and regenerator sections," Geneva, Switzerland	December 2002
G.831	ITU-T Recommendation G.831, "Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)," Geneva, Switzerland	March 2000
G.841	ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures," Geneva, Switzerland	October 1998
G.842	ITU-T Recommendation G.842, "Interworking of SDH network protection architectures," Geneva, Switzerland	April 1997
G.871/	ITU-T Recommendation G.871/Y.1301, "Framework of Optical Transport	
Y.1301	Network Recommendations," Geneva, Switzerland, Geneva, Switzerland	October 2000
G.872	ITU-T Recommendation G.872, "Architecture of optical transport networks," Geneva, Switzerland	November 2001
G.874	ITU-T Recommendation G.874, "Management aspects of optical transport network elements," Geneva Switzerland	July 2010
G.957	ITU-T Recommendation G.957, "Optical interfaces for equipments and systems relating to the synchronous digital hierarchy," Geneva, Switzerland	March 2006
G.958	ITU-T Recommendation G.958, "Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables" [Withdrawn]	
G.991.1	ITU-T Recommendation G.991.1, "High bit rate digital subscriber line (HDSL) transceivers"	1998
G.991.2	ITU-T Recommendation G.991.2, "Single-pair high-speed digital subscriber line (SHDSL) transceivers"	1998
G.992.1	ITU-T Recommendation G.992.1, "Asymmetric digital subscriber line (ADSL) transceivers"	1999
G.992.2	ITU-T Recommendation G.992.2, "Splitterless asymmetric digital subscriber line (ADSL) transceivers"	1999
G.992.3	ITU-T Recommendation G.992.2, "Asymmetric digital subscriber line transceivers 2 (ADSL2)"	2009
G.992.4	ITU-T Recommendation G.992.4, "Splitterless asymmetric digital subscriber line transceivers 2 (splitterless ADSL2)"	2002
G.992.5	ITU-T Recommendation G.992.5, "Asymmetric digital subscriber line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus)"	2009

PUBLICATION NUMBER	TITLE	DATE
G.993.1	ITU-T Recommendation G.993.1, "Very high speed digital subscriber line transceivers (VDSL)"	2004
G.993.2	ITU-T Recommendation G.993.2, "Very high speed digital subscriber line transceivers 2 (VDSL2)"	2006
G.998.1	ITU-T Recommendation G.993.2, "ATM-based multi-pair bonding"	2005
G.998.2	ITU-T Recommendation G.993.2, "Ethernet-based multi-pair bonding"	2005
G.998.3	ITU-T Recommendation G.993.2, "Multi-pair bonding using time-division inverse multiplexing"	2005
G.7041/Y.1303	ITU-T Recommendation G.7041/Y.1303, "Generic framing procedure (GFP)," Geneva, Switzerland, Geneva, Switzerland	October 2008
G.7042/Y.1305	ITU-T Recommendation G.7042/Y.1305, "Link capacity adjustment scheme (LCAS) for virtual concatenated signals," Geneva, Switzerland	March 2006
G.7043 Y.1343	ITU-T Recommendation G.7043/Y.1343, "Virtual concatenation of plesiochronous digital hierarchy (PDH) signals," Geneva, Switzerland	July 2004
G.7710 Y.1710	ITU-T Recommendation G.7710/Y.1710, "Common equipment management function requirements," Geneva, Switzerland	February 2012
G.8251	ITU-T Recommendation G.8251(G.otnjit), "The control of jitter and wander within the optical transport network (OTN)," Geneva, Switzerland	November 2001
H.221	ITU-T Recommendation H.221, "Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices," Geneva Switzerland	March 2009
H.224	ITU-T Recommendation H.224, "A real time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels," Geneva, Switzerland	January 2005
H.230	ITU-T Recommendation H.230, "Frame-synchronous control and indication signals for audiovisual systems"	March 2004
H.235	ITU-T Recommendation H.235, "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals"	August 2003
H.239	ITU-T Recommendation H.239, "Role management and additional media channels for H.300-series terminals"	July 2003
H.242	ITU-T Recommendation H.242, "System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/S"	March 2004
H.248.1	ITU-T Recommendation H.248.1, "Gateway control protocol: Version 3," Geneva Switzerland	September 2005
H.248.24	ITU-T Recommendation H.248.24, "Gateway control protocol: Multi-frequency tone generation and detection packages," Geneva, Switzerland	July 2003
H.248.25	ITU-T Recommendation H.248.24, "Gateway control protocol: Basic CAS packages," Geneva, Switzerland	January 2007
H.248.28	ITU-T Recommendation H.248.28, "Gateway control protocol: International CAS packages," Geneva, Switzerland	January 2007

PUBLICATION NUMBER	TITLE	DATE
H.261	ITU-T Recommendation H.261, "Video codec for audiovisual services at p x 64 kbit/s," Recommendation H.261, Geneva, Switzerland	March 1993
H.263	ITU-T Recommendation H.263, "Video coding for low bit rate communication," Geneva, Switzerland (H.263a, H.323+, H.263 (1999)).	January 2005
H.264	ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services," Geneva, Switzerland (Also known as H.264/AVC)	March 2005
H.281	ITU-T Recommendation H.281, "A far end camera control protocol for videoconferences using H.224," Geneva, Switzerland	November 1994
H.320	ITU-T Recommendation H.320, "Narrow-band visual telephone systems and terminal equipment," Geneva, Switzerland	March 2004
H.323	ITU-T Recommendation H.323, "Packet-based multimedia communications systems," Geneva, Switzerland	June 2006
I.320	ITU-T Recommendation I.320, "ISDN Protocol Reference Model"	1993
I.361	ITU-T Recommendation I.361, "B-ISDN ATM layer specification"	1999
I.430	ITU-T Recommendation I.430, "Basic User-Network Interface - Layer 1 Specification"	1995
I.431	ITU-T Recommendation I.431, "Primary Rate User-Network Interface - Layer 1 Specification"	1993
H.363.5	ITU-T Recommendation H.363.5, "B-ISDN ATM Adaptation Layer specification : Type 5 AAL"	1999
M.2101	ITU-T Recommendation M.2101, "Performance limits for bringing-into-service and maintenance of international multi-operator SDH paths and multiplex sections," Geneva, Switzerland	June 2003
M.3100	ITU-T Recommendation M.3100, "Generic network information model," Geneva, Switzerland	April 2005
P.800	ITU-T Recommendation P.800, "Methods for subjective determination of transmission quality," Geneva, Switzerland (Formerly ITU-T Recommendation P. 80)	1996
P.800.1	ITU-T Recommendation P.800.1, "Methods for Subjective Determination of Transmission Quality - Series P: Telephone Transmission Quality; Methods for Objective and Subjective Assessment of Quality," Geneva, Switzerland	August 1996
P.862	ITU-T Recommendation P.862, "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs," Geneva, Switzerland	February 2001
Q.735.3	ITU-T Recommendation Q.735.3, "Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption," Geneva, Switzerland	March 1993
Q.850	ITU-T Recommendation Q.850, "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part," Geneva, Switzerland	May 1998

PUBLICATION NUMBER	TITLE	DATE
Q.822	ITU-T Recommendation Q.822, "Stage 1, stage 2 and stage 3 description for the Q3 interface – Performance management," Geneva Switzerland	April 1994
Q.920	ITU-T Recommendation Q.920, "ISDN user-network interface data link layer – General aspects," Geneva, Switzerland	March 1993
Q.921	ITU-T Recommendation Q.921, "ISDN user-network interface – Data link layer specification," Geneva, Switzerland	September 1997
	NOTE: This Recommendation is published with the double number Q.921 and I.441	
Q.931	ITU-T Recommendation Q.931, "ISDN user-network interface layer 3 specification for basic call control," Geneva, Switzerland	May 1998
	NOTE: This Recommendation is also included but not published in I series under alias number I.451	
Q.955.3	ITU-T Recommendation Q.955.3, "Stage 3 description for community of interest supplementary services using DSS 1 – Multi-level precedence and preemption (MLPP)," Geneva, Switzerland	March 1993
Q.1912.5	ITU-T Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part," Geneva, Switzerland	March 2004
T.4	ITU-T Recommendation T.4, "Standardization of Group 3 facsimile terminals for document transmission," Geneva, Switzerland	July 2003
T.38	ITU-T Recommendation T.38, "Procedures for real-time Group 3 facsimile communication over IP networks," Geneva, Switzerland	April 2007
V.14	ITU-T Recommendation V.14, "Transmission of start-stop characters over synchronous bearer channels," Geneva, Switzerland	March 1993
V.24	ITU-T Recommendation V.24, "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)," Geneva, Switzerland	February 2000
V.32	ITU-T Recommendation V.32, "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits," Geneva, Switzerland	March 1993
V.34	ITU-T Recommendation V.34, "A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits," Geneva, Switzerland	February 1998
V.35	ITU-T Recommendation V.35, "Data transmission at 48 kilobits per second using 60-108 kHz group band circuits," Geneva, Switzerland	October 1984
V.42bis	ITU-T Recommendation V.42bis, "Data compression procedures for DCEs using error correction procedures"	January 1990
V.54	ITU-T Recommendation V.54, "Loop test devices for modems," Geneva, Switzerland	November 1988

PUBLICATION NUMBER	TITLE	DATE
V.90	ITU-T Recommendation V.90, "A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream," Geneva, Switzerland	September 1998
V.92	ITU-T Recommendation V.92, "Enhancements to Recommendation V.90"	November 2000
V.150.1	ITU-T Recommendation V.150.1, "Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs," Geneva, Switzerland	January 2003
	ITU-T Recommendation V.150.1, Amendment 1, Geneva, Switzerland	January 2005
X.721	ITU-T Recommendation X.721, "Information technology – Open systems Interconnection – Structure of management information: Definition of management information"	February 1992
X.744	ITU-T Recommendation X.744, "Information technology Interconnection – Systems Management: Software management function	October 1996
Y.1540	ITU-T Recommendation Y.1540, "Internet protocol data communication service - IP packet transfer and availability performance parameters"	November 2007

C.3.14 Internet Engineering Task Force Requests for Comment

PUBLICATION NUMBER	TITLE	DATE
RFC 125	J. McConnell, "Proposal for Network Standard Format for a Graphic Data Stream"	April 1971
RFC 233	A. Bhushan and B. Metcalfe, "Standardization of Host Call Letters"	September 1971
RFC 768	Postel, J., "User Datagram Protocol"	August 1980
RFC 791	Information Services Institute, "Internet Protocol"	September 1981
RFC 793	Information Services Institute, "Transmission Control Protocol"	September 1981
RFC 1046	Prue, W. and J. Postel, "A Queuing Algorithm to Provide Type-of-Service for IP Links"	February 1988
RFC 1142	Oran, D., Ed., "OSI IS-IS Intra-domain Routing Protocol"	February 1990
RFC 1157	Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)"	May 1990
RFC 1195	R. Callon, "A Use of OSI IS-IS for Routing in TCP/IP and Dual Environments"	December 1990
RFC 1215	Rose, M., Ed., "A Convention for Defining Traps for use with SNMP"	March 1991
RFC 1256	Deering, S., Ed., "ICMP Router Discovery Messages"	September 1991
RFC 1305	Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis"	March 1992
RFC 1332	McGregor, G., "The PPP Internet Protocol Control Protocol"	May 1992

PUBLICATION NUMBER	TITLE	DATE
RFC 1471	Kastenholz, F., "The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol"	June 1993
RFC 1472	Kastenholz, F., "The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol"	June 1993
RFC 1473	Kastenholz, F., "The Definitions of Managed Objects for IP Network Control Protocol of the Point-to-Point Protocol"	June 1993
RFC 1519	Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy"	September 1993
RFC 1570	Simpson, W., Ed., "PPP LCP Extensions"	January 1994
RFC 1657	Willis, S., Burruss, J., and J. Chu, "Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2"	July 1994
RFC 1662	Simpson, W., Ed., "PPP in HDLC-like Framing"	July 1994
RFC 1772	Rekhter, Y., P. Gross, "Application of the Border Gateway Protocol in the Internet"	March 1995
RFC 1812	Baker, F., Ed., "Requirements for IP Version 4 Routers,".	June 1995
RFC 1918	Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. De Groot, and E. Lear, "Address Allocation for Private Internets"	February 1996
RFC 1981	McCann, J., S. Deering, and J. Mogul, "Path MTU Discovery for IP Version 6"	August 1996
RFC 1989	Simpson, W., "PPP Link Quality Monitoring"	August 1996
RFC 1990	K. Sklower, B. Loyd, et al, "The PPP Multilink Protocol (MP)"	August 1996
RFC 1994	Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)"	August 1996
RFC 1997	Chandra, R., P. Traina, and T. Li, "BGP Communities Attribute"	August 1996
RFC 2006	Dong, D., Hamlen, M., and C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2"	October 1996
RFC 2119	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels"	March 1997
RFC 2126	Pouffary, Y. and A. Young, "ISO Transport Service on top of TCP (ITOT)"	March 1997
RFC 2131	Droms, R., "Dynamic Host Configuration Protocol"	March 1997
RFC 2132	Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions"	March 1997
RFC 2198	Perkins, C, I. Kouvelas, O. Hodson, V. Hardman, M. Handley, J.C. Bolot, A. Vega-Garcia, and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data"	September 1997
RFC 2202	Chen, F. and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1"	September 1997
RFC 2205	Braden, R., Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin, "ReSerVation Protocol (RSVP)–Version 1 Functional Specification"	September 1997

PUBLICATION NUMBER	TITLE	DATE
RFC 2206	Baker, F., J. Krawczyk, and A. Sastry, "RSVP Management Information Base using SMIv2"	September 1997
RFC 2207	Berger, L. and T. O'Malley, "RSVP Extensions for IPSEC Data Flows"	September 1997
RFC 2210	Wroclawski, J., "The Use of RSVP with IETF Integrated Services"	September 1997
RFC 2211	Wroclawski, J., "Specification of the Controlled-Load Network Element Service"	September 1997
RFC 2212	Shenker, S., C. Partridge, and R. Guerin, "Specification of Guaranteed Quality of Service"	September 1997
RFC 2215	Shenker, S. and J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements"	September 1997
RFC 2251	Lightweight Directory Access Protocol (V3)	
RFC 2252	Lightweight Directory Access Protocol (V3): Attribute Syntax Definitions	
RFC 2253	Lightweight Directory Access Protocol (V3): UTF-8 String Representation of Distinguished Names	
RFC 2254	The String Representation of LDAP Search Filters	
RFC 2255	The LDAP URL Format	
RFC 2256	A Summary of the X.500(96) User Schema for use with LDAPv3	
RFC 2328	Moy, J., "OSPF Version 2"	April 1998
RFC 2330	Paxson, V., G. Almes, J. Mahdavi, and M. Mathis, "Framework for IP Performance Metrics"	May 1998
RFC 2332	Luciani, J., Katz, D., Piscitello, D., Cole, B., and N. Doraswamy, "NBMA Next Hop Resolution Protocol (NHRP)"	April 1998
RFC 2362	Estrin, D., D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification"	June 1998
RFC 2365	Meyer, D., "Administratively Scoped IP Multicast"	July 1998
RFC 2385	Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option"	August 1998
RFC 2404	Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH"	November 1998
RFC 2407	Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP"	November 1998
RFC 2408	Maughan, D., M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)"	November 1998
RFC 2409	Harkins, J. and D. Carrel, "The Internet Key Exchange (IKE)"	November 1998
RFC 2427	Brown, C. and A. Malis, "Multiprotocol Interconnect over Frame Relay"	September 1998
RFC 2439	Villamizar, C., R. Chandra, and R. Govindan, "BGP Route Flap Damping"	November 1998

PUBLICATION NUMBER	TITLE	DATE
RFC 2460	Deering S. and R. Hinden, "Internet Protocol Version 6 (IPv6) Specification"	December 1998
RFC 2462	Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration"	December 1998
RFC 2464	Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks"	December 1998
RFC 2473	Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification"	December 1998
RFC 2474	Nichols, K., S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"	December 1998
RFC 2475	Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services"	December 1998
RFC 2507	Degermark, M., Nordgren, B., and S. Pink, "IP Header Compression"	February 1999
RFC 2508	Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links"	February 1999
RFC 2543	Handley, M., H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol"	March 1999
RFC 2544	Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices"	March 1999
RFC 2545	Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing"	March 1999
RFC 2547	Rosen, E. and Y. Rekhter, "BGP/MPLS VPNs"	March 1999
RFC 2560	Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"	June 1999
RFC 2578	McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)"	April 1999
RFC 2579	McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Textual Conventions for SMIv2"	April 1999
RFC 2580	McCloghrie, K., D. Perkins, and J. Schoenwaelder, "Conformance Statements for SMIv2"	April 1999
RFC 2581	Allman, M., Paxson, V. and W. Stevens, "TCP Congestion Control"	April 1999
RFC 2597	Heinanen, J., F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group"	June 1999
RFC 2615	Malis, A. and W. Simpson, "PPP over SONET/SDH"	June 1999
RFC 2660	Rescorla, E., and A. Schiffman, "The Secure HyperText Transfer Protocol"	August 1999
RFC 2679	Almes, G., S. Kalidindi, and M. Zekauskas, "A One-way Delay Metric for IPPM"	September 1999
RFC 2680	Almes, G., S. Kalidindi, and M. Zekauskas, "A One-way Packet Loss Metric for IPPM"	September 1999
RFC 2684	Grossman, D, and J. Heinanem, "Multiprotocol Encapsulation over ATM Adaptation Layer 5"	September 1999

PUBLICATION NUMBER	TITLE	DATE
RFC 2685	Fox, B., B. Gleeson, "Virtual Private Networks Identifier"	September 1999
RFC 2702	Awduche, D., J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS"	September 1999
RFC 2710	Deering S., W. Feener, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6"	October 1999
RFC 2711	Partridge, C. and A. Jackson, "IPv6 Router Alert Option"	October 1999
RFC 2719	L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdredge, C. Sharp, "Architectural Framework for Signaling Transport"	October 1999
RFC 2737	McCloghrie, K. and A. Bierman, "Entity MIB (Version 2)"	December 1999
RFC 2740	Coltun, R., D. Ferguson, and J. Moy, "OSPF for IPv6"	December 1999
RFC 2747	Baker, F., Lindell, B., Talwar, M., "RSVP Cryptographic Authentication"	January 2000
RFC 2778	Day, M., Rosenberg, J., "A Model for Presence and Instant Messaging"	February 2000
RFC 2782	Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for Specifying the Location of Services (DNS SRV)"	February 2000
RFC 2784	Farinacci, D., T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)"	March 2000
RFC 2787	Jewell, B., "Definitions of Managed Objects for the Virtual Router Redundancy Protocol"	March 2000
RFC 2788	Freed, N., and S. Kille, "Network Services Monitoring MIB"	March 2000
RFC 2796	Bates, T., Chandra, R., and E. Chen, "BGP Route Reflection – An Alternative to Full Mesh IBGP"	April 2000
RFC 2805	Greene, N., M. Ramalho, and B. Rosen, "Media Gateway Control Protocol Architecture and Requirements"RFC 2805,	April 2000
RFC 2818	Rescorla, E., "HTTP over TLS,	May 2000
RFC 2819	Waldbusser, S., "Remote Network Monitoring Management Information Base"	May 2000
RFC 2829	Authentication Methods for LDAP	
RFC 2830	Lightweight Directory Access Protocol (V3) Extension for Transport Layer Security (TLS)	
RFC 2833	Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"	May 2000
RFC 2863	McCloghrie, K. and F. Kastenholz, "The Interface Group MIB"	June 2000
RFC 2865	Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)"	June 2000
RFC 2866	Rigney, C., "RADIUS Accounting"	June 2000
RFC 2917	Muthukrishnan, K. and A. Malis, "A Core MPLS IP VPN Architecture"	September 2000
RFC 2918	Chen, E., "Route Refresh Capability for BGP-4"	September 2000

PUBLICATION NUMBER	TITLE	DATE
RFC 2961	Berge, L., Gan, D., Swallow, G., Pan, P., Tommasi, F., Molendini, S., "RSVP Refresh Overhead Reduction Extensions"	April 2001
RFC 2973	Balay, R., Katz, D., Parker, J., "IS-IS Mesh Groups"	October 2000
RFC 3031	Rosen, E., A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture"	January 2001
RFC 3032	Rosen, E., D. Tappan, G. Fedorkow, Y. Rekter, D. Farinacci, T. Li, and A. Conta, "MPLS Label Stack Encoding"	January 2001
RFC 3037	Thomas, B. and E. Gray, "LDP Applicability"	January 2001
RFC 3053	Durand, A., P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker"	January 2001
RFC 3060	Moore, B., Ellesson, E., Strassner, J., and A. Westerinen, "Policy Core Information Model – Version 1 Specification"	February 2001
RFC 3097	Braden, R. and L. Zhang, "RSVP Cryptographic Authentication – Updated Message Type Value"	April 2001
RFC 3107	Rekhter, Y. and E. Rosen, "Carrying Label Information in BGP-4"	May 2001
RFC 3140	Black, D., S. Brim, B. Carpenter, and F. Le Faucheur, "Per Hop Behavior Identification Codes"	June 2001
RFC 3162	Aboba, B., G. Zorn, and D. Mitton, "RADIUS and IPv6"	August 2001
RFC 3164	Lonvick, C., "The BSD syslog Protocol"	August 2001
RFC 3168	Ramakrishnan, K., Floyd, S., and D. Black, "RADIUS and IPv6"	September 2001
RFC 3173	Shacham, A., Monsour, B., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)"	September 2001
RFC 3181	Herzog, S., "Signaled Preemption Priority Policy Element"	October 2001
RFC 3195	New, D. and M. Rose, "Reliable Delivery for syslog"	November 2001
RFC 3209	Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels"	December 2001
RFC 3210	Awduche, D., A. Hannan, and X. Xiao, "Applicability Statement for Extensions to RSVP for LSP-Tunnels"	December 2001
RFC 3246	Davie, B., A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)"	March 2002
RFC 3260	Grossman, D., "New Terminology and Clarification for Diffserv"	April 2002
RFC 3261	Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and R. Schooler, "SIP: Session Initiation Protocol"	June 2002
RFC 3262	Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)"	June 2002
RFC 3264	Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)"	June 2002
RFC 3265	Roach, A. B., "Session Initiation Protocol (SIP)-Specific Event Notification"	June 2002

PUBLICATION NUMBER	TITLE	DATE
RFC 3270	Le Faucheur, F., L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services"	May 2002
RFC 3273	Waldbusser, S., "Remote Network Monitoring Management Information Base for High Capacity Networks"	July 2002
RFC 3310	Niemi, A., J. Arkko, and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"	September 2002
RFC 3311	Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method"	September 2002
RFC 3312	Camarillo, G., W. Marshall, and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)"	October 2002
RFC 3315	Droms, E., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"	July 2003
RFC 3323	Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)"	November 2002
RFC 3325	Jennings, C., J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"	November 2002
RFC 3326	Schulzrinne, H., D. Oran, and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)"	December 2002
RFC 3329	Arkko, J., V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)"	January 2003
RFC 3344	Perkins, C., "IP Mobility Support for IPv4"	August 2002
RFC 3345	McPherson, D., Gill, V, Walton, D., and A. Retana, "Border Gateway Protocol (MGP) Persistent Route Oscillation Condition"	August 2002
RFC 3359	Przygienda, T., "Reserved Type, Length and Value (TLV) codepoints in Intermediate System to Intermediate System"	August 2002
RFC 3366	Fairhurst, G., and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)"	August 2002
RFC 3376	Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3"	October 2002
RFC 3392	Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4"	November 2002
RFC 3393	Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)"	November 2002
RFC 3398	Camarillo, G., A. B. Roach, J. Peterson, and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping"	December 2002
RFC 3407	Andreasen, F., "Session Description Protocol (SDP) Simple Capability Declaration"	October 2002

PUBLICATION NUMBER	TITLE	DATE
RFC 3410	Case, J., R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet Standard Management Framework"	December 2002
RFC 3411	Harrington, D., R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks"	December 2002
RFC 3412	Case, J., D. Harrington, R. Presuhn, and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)"	December 2002
RFC 3413	Levi, D., P. Meyer, and B. Stewart, "Simple Network Management Protocol (SNMP) Applications"	December 2002
RFC 3414	Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)"	December 2002
RFC 3415	Wijnen, B., R. Presuhn, and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)"	December 2002
RFC 3416	Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)"	December 2002
RFC 3417	Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Transport Mappings for the Simple Network Management Protocol (SNMP)"	December 2002
RFC 3418	Presuhn, R., Ed., J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)"	December 2002
RFC 3443	Agarwal, P. and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks"	January 2003
RFC 3446	Kim, D., Meyer, D., Kilmer, H., and D. Farinacci, "Anycast Rendevous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)"	January 2003
RFC 3455	Garcia-Martin, M., E. Henrikson, and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)"	January 2003
RFC 3471	Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description"	January 2003
RFC 3473	Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions"	January 2003
RFC 3478	Leelanivas, M., Y. Rekhter, and R. Aggarwal, "Graceful Restart Mechanism for Label Distribution Protocol"	February 2003
RFC 3479	Farrel, A., Ed., "Fault Tolerance for the Label Distribution Protocol (LDP)"	February 2003
RFC 3484	Draves, R., "Default Address Selection for Internet Protocol Version 6 (IPv6)"	February 2003

PUBLICATION NUMBER	TITLE	DATE
RFC 3486	Camarillo, G., "Compressing the Session Initiation Protocol (SIP)"	February 2003
RFC 3515	Sparks, R., "The Session Initiation Protocol (SIP) Refer Method"	April 2003
RFC 3539	Aboda, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile"	June 2003
RFC 3544	Koren, T., Casner, S., and C. Bormann, "IP Header Compression over PPP"	July 2003
RFC 3550	Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications"	July 2003
RFC 3564	Le Faucheur, F. and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering"	July 2003
RFC 3579	Aboda, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)"	September 2003
RFC 3581	Rosenberg, J. and H. Schulzrinne, "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"	August 2003
RFC 3584	Frye, R., D. Levi, S. Routhier, and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework"	August 2003
RFC 3588	Calhoun, P., Loughney, J. Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol"	September 2003
RFC 3596	Thomson, S., C. Huitema, V. Ksinant, and M. Souissi, "DNS Extensions to Support IPv6"	October 2003
RFC 3603	Marshall, W. and F. Andreasen, "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture"	October 2003
RFC 3618	Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)"	October 2003
RFC 3618	Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)"	October 2003
RFC 3623	Moy, J., Pillay-Esnault, F., and A. Lindem, "Graceful OSPF Restart"	November 2003
RFC 3644	Snir, Y., Ramberg, Y. Strassner, J. Cohen, R., and B. Moore, "Policy quality of Service (Qos) Information Model"	November 2003
RFC 3662	Bless, R., K. Nichols, and K. Wehrle, "A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services"	December 2003
RFC 3670	Moore, B., D. Durham, J. Strassner, A. Westerinen, and W. Weiss, "Information Model for Describing Network Device QoS Datapath Mechanism"	January 2004
RFC 3711	Baugher, M., D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)"	March 2004
RFC 3725	Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session initiation Protocol (SIP)"	March 2004
RFC 3748	Aboba, B., Blunk, L, Vollbrecht, J. Carlson, J. and H. Levkowetz, Ed., "Extensible Authentication Protocol IEAP)"	June 2004

PUBLICATION NUMBER	TITLE	DATE
RFC 3754	Bless, R., and K. Wehrle, "IP Multicast in Differentiated Services (DS) Networks"	April 2004
RFC 3764	Person, J., "enumservice registration for Session initiation Protocol (SIP) Addresses-of-Record)"	April 2004
RFC 3810	Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6"	June 2004
RFC 3826	Blumenthal, U., F. Maino, and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model"	June 2004
RFC 3840	Rosenberg, J., H. Schulzrinne, and P. Kyzivat, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"	August 2004
RFC 3842	Mahy, R., "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"	August 2004
RFC 3879	Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses"	September 2004
RFC 3890	Westerlund, M., "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)"	September 2004
RFC 3891	Mahy, R., B. Biggs, and R. Dean, "The Session Initiation Protocol (SIP) "Replaces"Header"	September 2004
RFC 3892	Sparks, R., "The Session Initiation Protocol (SIP) Referred By Mechanism"	September 2004
RFC 3893	Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format"	September 2004
RFC 3913	Thaler, D., "Border Gateway Multicast Protocol (BGMP)"	September 2004
RFC 3936	Kompella, K. and J. Lang, "Procedures for Modifying the Resource reSerVation Protocol (RSVP)"	October 2004
RFC 3948	Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets"	January 2005
RFC 3966	Schulzrinne, H., "The tel URI for Telephone Numbers"	December 2004
RFC 3968	Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)"	December 2004
RFC 3986	Berners-Lee, T., R. Fielding, and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax"	January 2005
RFC 4003	Berger, L., "GMPLS Signaling Procedure for Egress Control"	February 2005
RFC 4007	Deering, S., B. Haberman, T. Jinmei, E. Nordmark, and B. Zill, "IPv6 Scoped Address Architecture"	March 2005
RFC 4022	Raghunarayan, R., "Management Information Base for the Transmission Control Protocol (TCP)"	March 2005
RFC 4028	Donovan, B., and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)"	April 2005
RFC 4040	Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call"	April 2005
RFC 4044	McGloghrie, K., "Fibre Channel Management MIB"	May 2005

PUBLICATION NUMBER	TITLE	DATE
RFC 4072	Eronen, P., Ed., T. Hiller, and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application"	August 2005
RFC 4087	Thaler, D., "IP Tunnel MIB"	June 2005
RFC 4090	Pan, P., Ed., G. Swallow, Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels"	May 2005
RFC 4091	Camarillo, G. and J. Rosenburg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework"	June 2005
RFC 4092	Camarillo, G. and J. Rosenburg, "Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)"	June 2005
RFC 4109	Hoffman, P., "Algorithms for Internet Key Exchange Version 1 (IKEv1)"	May 2005
RFC 4113	Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)"	June 2005
RFC 4120	Neuman, C., T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)"	July 2005
RFC 4122	Leach, P., Mealling, M. and R. Salz, "A Universally Unique Identifier (UUID) URN Namespace, "	July 2005
RFC 4123	Schulzrinne, H., "Session Initiation Protocol (SIP)-H.323 Internetworking Requriements"	July 2005
RFC 4124	Faucheur, F., "Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering"	June 2005
RFC 4171	Tseng, J., K. Gibbons, F. Travostino, C. Du Laney, and J. Souza, "Internet Storage Name Service (iSNS)"	September 2005
RFC 4182	Rosen, E., "Removing a Restriction on the use of MPLS Explicit NULL"	September 2005
RFC 4193	Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses"	October 2005
RFC 4201	Kompella, K., Y. Rekhter, and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)"	October 2005
RFC 4204	Lang, J., "Link Management Protocol (LMP)"	October 2005
RFC 4206	Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)"	October 2005
RFC 4213	Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers"	October 2005
RFC 4233	Morneault, K., S. Rengasami, M. Kalla, and G. Sidebottom, "Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer"	January 2006
RFC 4244	Barnes, M., Ed., "An Extension to the Session Initiation Protocol (SIP) for Request History Information,	November 2005
RFC 4251	Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture"	January 2006

PUBLICATION NUMBER	TITLE	DATE
RFC 4252	Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol"	January 2006
RFC 4253	Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol"	January 2006
RFC 4254	Ylonen, T., and C. Lonvick, Ed., "The Secure Shell (SSH) Connection Protocol"	January 2006
RFC 4271	Rekhter, Y., T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)"	January 2006
RFC 4282	Aboba, B., M. Beadles, J. Arkk and P. Eronen, "The Network Access Identifier"	December 2005
RFC 4291	Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture"	February 2006
RFC 4292	Haberman, B., "IP Forwarding Table MIB"	April 2006
RFC 4293	Routhier, S., "Management Information Base for the Internet Protocol (IP)"	April 2006
RFC 4301	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol"	December 2005
RFC 4302	Kent, S., "IP Authentication Header"	December 2005
RFC 4303	Kent, S., "IP Encapsulating Security Payload (ESP)"	December 2005
RFC 4306	Kaufman, E., "Internet Key Exchange (IKEv2) Protocol"	December 2005
RFC 4328	Papadimitriou, D., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control"	January 2006
RFC 4338	DeSanti, C., Carlson, C., and R. Nixon., "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel"	January 2006
RFC 4344	Bellare, M., Kohno, T., and C. Namprempre., "The Secure Shell (SSH) Transport Layer Encryption Modes"	January 2006
RFC 4353	Rosenberg, J., "A Framework for Conferencing with the Session Initiation Protocol (SIP)"	January 2006
RFC 4360	Sangli, S., Tappan, D., and Y. Rekhter, "BGP/Extended Communities Attribute"	February 2006
RFC 4362	Jonsson, L-E, Pelletier, G., and K. Sandlund, "RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP" (Replaces RFC 2547)	February 2006
RFC 4364	Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)" (Replaces RFC 2547)	February 2006
RFC 4379	Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures"	February 2006
RFC 4382	Nadeau, T., Ed., and H. van der Linde, Ed., "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base"	February 2006
RFC 4411	Polk, J., "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events, "	February 2006
RFC 4412	Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)"	February 2006

PUBLICATION NUMBER	TITLE	DATE
RFC 4443	Conta, A., S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification"	March 2006
RFC 4447	Martini, L., Ed., E. Rosen, N. El-Aawar, T. Smith, and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)"	April 2006
RFC 4448	Martini, L., Ed., E. Rosen, N. El-Aawar, and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks"	April 2006
RFC 4456	Bates, T., Chen, E., "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)"	April 2006
RFC 4502	Waldbusser, S., "Remote Network Monitoring Management Information Base Version 2"	May 2006
RFC 4510	Zeilenga, E., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map"	June 2006
RFC 4511	Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol"	June 2006
RFC 4552	Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFV3"	June 2006
RFC 4566	Handley, M., V. Jacobson, and C. Perkins, "SDP: Session Description Protocol"	July 2006
RFC 4568	Andreasen, F., M. Baugher, and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams"	July 2006
RFC 4573	Even, R., and A. Lochbaum, "MIME Type Registration for RTP Payload Format for H.224"	July 2006
RFP 4574	Levin, O., and G. Camarillo, "Session Description Protocol (SDP) Label Attribute"	August 2006
RFC 4575	Rosenberg, J., Schulzrinne, H., and O. Levin, "A Session Initiation Protocol (SIP) Event Package for Conference State"	August 2006
RFC 4577	Rosen, E., Psenak, P., and P. Pillay-Esnault, "OSPF as the Provided/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)"	June 2006
RFC 4579	Johnston, A. and O. Levin, "Session Initiation Protocol (SIP) Call Control – Conferencing for User Agents"	August 2006
RFC 4583	Camarillo, G., "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams"	November 2006
RFC 4585	Ott, J., S. Wenger, N. Sato, C. Burmeister, and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF),	July 2006
RFC 4601	Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)"	August 2006
RFC 4604	Holbrook, H., Haberman, B. and B. Cain, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery protocol Version 2 (MLDv2) for Source-Specific Multicast"	August 2006

PUBLICATION NUMBER	TITLE	DATE
RFC 4607	Holbrook, H. and B. Cain, "Source-Specific Multicast for IP"	August 2006
RFC 4616	Zeilenga, K., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism"	August 2006
RFC 4659	De Clercq, J., D. Ooms, M. Carugi, and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN"	September 2006
RFC 4666	Morneault, K., Ed., and J. Pastor-Balbas, Ed., "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)"	September 2006
RFC 4684	Marques, P., R. Bonica, L. Fang, L. Martini, R. Raszuk, K. Patel, and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)"	November 2006
RFC 4724	Sangli, S., Chen, E., Fernando, R., Scudder, J., Rekhter, Y., "Graceful Restart Mechanism for BGP"	January 2007
RFC 4730	Burger, E. and M. Dolly, "A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)"	November 2006
RFC 4733	Schulzrinne, H. and T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"	December 2006
RFC 4750	Joyal, D., Galecki, P., and S. Giacalone, "OSPF Version 2 Management Information Base"	December 2006
RFC 4760	Bates, T., R. Chandra, D. Katz and Y. Rekhter, "Multiprotocol Extensions for BGP-4"	January 2007
RFC 4761	Kompella, K., Ed. and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" (Updated by RFC 5462).	January 2007
RFC 4762	Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling"	January 2007
RFC 4783	Berger, L., Ed., "GMPLS – Communication of Alarm Information"	December 2006
RFC 4796	Hautakorpi, J. and G. Camarillo, "The Session Description Protocol (SDP) Content Attribute"	February 2007
RFC 4807	Baer, M., R. Charlet, W. Hardaker and R. Story, "IPSec Security Policy Dtabase Configuration MIB"	March 2007
RFC 4835	Manral, V, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)"	April 2007
RFC 4835	Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Secruity Payload (ESP) and Authentication Header (AH)"	April 2007
RFC 4861	Narten, T., E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)"	September 2007
RFC 4862	Thomson, S., T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration"	September 2007

PUBLICATION NUMBER	TITLE	DATE
RFC 4864	Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6"	May 2007
RFC 4872	Lang, J.P., Ed., Y. Rekhter, Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery"	May 2007
RFC 4873	Berger, L., I. Bryskin, D. Papadimitriou, and A. Farrel, "GMPLS Segment Recovery"	May 2007
RFC 4874	Lee, C.Y., A. Farrel, and S. De Cnodder, "Exclude Routes – Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)"	April 2007
RFC 4904	Gurbani, V. and C. Jennings, "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)"	June 2007
RFC 4918	Dusseault, L., Ed., "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)"	June 2007
RFC 4941	Narten, T., R. Draves, and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6"	September 2007
RFC 4960	Stewart, E., "Stream Control Transmission Protocol"	September 2007
RFC 4974	Papadimitriou, D. and A. Farrel, "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls"	August 2007
RFC 5036	Andersson, L, Minei, I., and R. Thomas, "LDP Specification"	October 2007
RFC 5059	Bhaskar, N., Gall, A., Lingard, J., and S. Venaas, "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)"	January 2008
RFC 5063	Satyanarayana, A., Ed. and R. Rahman, Ed., "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart"	October 2007
RFC 5065	Traina, P., McPherson, D. and J. Scudder, "Antonomous System Confederations for BGP"	August 2007
RFC 5072	Varada, S., "IP Version 6 over PPP"	September 2007
RFC 5095	Abley, J., P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6"	December 2007
RFC 5104	Wenger, S., U. Chandra, M. Westerlund, and B. Burman, "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)"	February 2008
RFC 5129	Davie, B., B. Briscoe, and J. Tay, "Explicit Congestion Marking in MPLS"	January 2008
RFC 5136	Chimento, P., and J. Ishac, "Defining Network Capacity"	February 2008
RFC 5151	Farrel, A., Ed., A. Ayyangar, and J.P. Vasseur, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions"	February 2008
RFC 5187	Pillay-Esnault, P., and A. Lindem, "OSPFv3 Graceful Restart"	June 2008
RFC 5246	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2"	August 2008
RFC 5301	McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS"	October 2008

PUBLICATION NUMBER	TITLE	DATE
RFC 5303	Katz, D., Saluja, R. and D. Eastlake, "Three-Way Handshake for IS-IS Point-to-Point Adjacencies"	October 2008
RFC 5304	Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication"	October 2008
RFC 5305	Li, T., Redback Networks, Inc., H. Smit, "IS-IS Extensions for Traffic Engineering"October 2008.	
RFC 5306	Shand, M., and L. Ginsberg, "Restart Signaling for IS-IS"	October 2008
RFC 5307	Kompella, K. and Y. Rekhter, "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)"	October 2008
RFC 5308	Hopps, C., "Routing IPv6 with IS-IS"	October 2008
RFC 5309	Shen, N. and A. Zinin, "Point-to-Point Operation over LAN in Link State Routing Protocols"	October 2008
RFC 5310	Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R. and M. Fanto., "IS-IS Generic Cryptographic Authentication"	February 2009
RFC 5331	Aggarwal, R., Y. Rekhter, and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space"	August 2008
RFC 5332	Eckert, T., E. Rosen, Ed., R. Aggarwal, and Y. Rekhter, "MPLS Multicast Encapsulations"	August 2008
RFC 5340	Coltun, R., Ferguson, D., Moy, J. and E. Lindem, "OSPF for IPv6"	July 2008
RFC 5359	Johnston, A., Sparks, R., Cunningham, C., Donovan, S. and K. Summers, "Session Initiation Protocol Service Examples"	October 2008
RFC 5415	Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification"	March 2009
RFC 5416	Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Finding for IEEE 802.11"	March 2009
RFC 5420	Farrel, A., Ed., D. Papadimitriou, J.P. Vasseur, and A. Ayyangarps, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)"	February 2009
RFC 5462	Andersson L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP"Field Renamed to "Traffic Class"Field"	February 2009
RFC 5492	Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4"	February 2009
RFC 5501	Kamite, y., Ed., Y. Wada, Y. Serbest, T. Morin, and L. Fang, "Requirements for Multicast Support in Virtual Private LAN Services"	March 2009
RFC 5626	Jennings, C., Mahy, R., and F. Audet, "Managing client-Initiated Connections in the Session initiation Protocol (SIP)"	October 2009
RFC 5746	Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension"	February 2010
RFC 5798	Nadas, S., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6"	March 2010
RFC 5806	Levy, S. and M. Mohali, "Diversion Indication in SIP"	March 2010

PUBLICATION NUMBER	TITLE	DATE
RFC 5922	Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)"	June 2010
RFC 5923	Gurbani, V., Mahy, R., and B. Tate, "Connection Reuse in the Session initiation Protocol"	June 2010
RFC 5925	Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option"	June 2010
RFC 5954	Gurbani, V., Carpenter, B., and B. Tate, "Essential Correction for IPv6 ABNF and URI Comparison for RFC 3261"	August 2010
RFC 6119	Harrison, J., Berger, J., and M. Bartlett, "IPv6 Traffic Engineering in IS-IS"	February 2011
RFC 6120	Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core"	March 2011
RFC 6121	Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence"	March 2011
RFC 6122	Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Address Format"	March 2011
RFC 6184	Wang, Y., Even, R., Kristensen, T., and R. Jesup, "RTP Payload Format for H.264 Video,	May 2011
draft-ietf-bfcpbis-rfc4582bis-05	Camarillo, G., K. Drage, T. Kristensen, J. Ott and C. Eckel, "The Binary Floor Control Protocol (BFCP) draft-ietf-bfcpbis-rfc4582bis-05"	August 2012

C.3.15 Joint Requirements Oversight Council Documentation

PUBLICATION NUMBER	TITLE	DATE
JROCM 048-96	Memorandum for the Under Secretary of Defense for Acquisition and Technology, Subject: Validation of Defense Information Systems Network (DISN) Capstone Requirements Document (CRD)	April 15, 1996
JROCM 134-01	"Global Information Grid (GIG) Capabilities Requirement Document (CRD)"	August 30, 2001
JROCM 202-02	"Global Information Grid (GIG), Mission Area Initial Capabilities Document (MA ICD)"	November 22, 2002

C.3.16 National Security Agency Documentation

TITLE	DATE
National Security Agency, "Commercial COMSEC Endorsement Program Procedures"	August 31, 1987
National Security Agency, "Common Criteria for Protection Profile for Switches and Routers (CCPPSR)," Version 3.,1 Revision 3 unless superseded by later version that then takes precedence per http://www.niap-ccevs.org/pp/	July 2009
National Security Agency, "DoD Class 3 Public Key Infrastructure Interface Specification,"	August 10, 2000

TITLE	DATE
Version 1.2	
National Security Agency, "INFOSEC System Security Products and Services Catalog"	October 1990

C.3.17 U. S. Secure Communication Interoperability Protocol

PUBLICATION NUMBER	TITLE	DATE
SCIP-215	U.S. Secure Communication Interoperability Protocol (SCIP) over IP Implementation Standard and Minimum Essential Requirements (MER) Publication, Revision 2.1	December 10, 2009
SCIP-216	Minimum Essential Requirements (MER) for V.150.1 Gateways Publication, Revision 2.1	December 10, 2009

C.3.18 Telcordia Technologies Documentation

PUBLICATION NUMBER	TITLE
Feature Service Description (FSD) 30-33-0000	*Release to Pivot Network Capability*.
FR-796	Reliability and Quality Generic Requirements (RQGR), Issue 1, October 1995; Issue 2; Issue 3, March 2006; Issue 5, April 2008.
GR-31-CORE	*G LSSGR: CLASSSM Feature: Calling Number Delivery (FSD 01-02-1051),* Issue 1, June 2000.
GR-63-CORE	*NEBS™ Requirements: Physical Protection*, Issue 1, October 1995, Issue 2, April 2002, Issue 3, March 2006.
GR-181-CORE	*Dual-Tone Multifrequency Receiver Generic Requirements for End-to-End Singaling Over Tandem-Switched Voice Links*, Issue 1, July 2003.
GR-205-CORE	*Generic Requirements for ISDN Electronic Key Telephone Service,* Issue 1 with Revision 1, September 1997.
GR-217-CORE	*LSSGR: CLASS^{SM} Feature: Selective Call Forwarding (FSD-01-02-1410),* Issue 1, June 2000; Issue 2, April 2002.
GR-253-CORE	*Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, December 2005.
GR-282-CORE	*Software Reliability and Quality Acceptance Criteria (SRQAC)*, Issue 4, July 2006.
GR-303-CORE	*Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface*, Issue 4, December 2000.
GR-317-CORE	*Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.
GR-383-CORE	*COMMON LANGUAGE® Equipment Codes (CLEI™ Codes) – Generic Requirements for Product Labels*, Issue 3, February 2006.
GR-394-CORE	*Switching System Generic Requirements for Interexchange Carrier Interconnection (ICI) Using the Integrated Services Digital Network User Part (ISDNUP)*, November 2007.

PUBLICATION NUMBER	TITLE
GR-436-CORE	*Digital Network Synchronization Plan*, Issue 1 with Revision 1, June 1996.
GR-472-CORE	*Network Element Configuration Management*, Revision 2, February 1999.
GR-477-CORE	*Network Traffic Management*, February 2000.
GR-496-CORE	*SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria*, Issue 2, August 2007.
GR-499-CORE	*Transport Systems Generic Requirements (TSGR): Common Requirements*, Issue 3, September 2004.
GR-506-CORE	*LSSGR: Signaling for Analog Interfaces*, December 2006.
GR-512-CORE	*LSSGR: Reliability*, Section 12, January 1998.
GR-513-CORE	*Module of the LSSGR, FR-64*, Issue 1, September 1995.
GR-518-CORE	*LSSGR: Synchronization Section 18,* Issue 1, May 1994.
GR-529-CORE	*LSSGR: Public Safety*, Issue 1, FSDs 15-01-0000, 15-03-0000, and 15-07-0000, June 2000.
GR-569-CORE	*LSSGR: Multiline Hunt Service (FSD 01-02-0802)*, Issue 1, June 2000.
GR-571-CORE	*LSSGR: Call Waiting, FSD 01-02-1201*, June 2000.
GR-572-CORE	*LSSGR: Cancel Call Waiting, FSD 01-02-1204*, June 2000.
GR-580-CORE	*LSSGR: Call Forwarding Variable, FSD 01-02-1401*, June 2000.
GR-586-CORE	*LSSGR: Call Forwarding Subfeatures, FSD 01-02-1450*, April 2002.
GR-590-CORE	*LSSGR: Call Pickup Features,* Issue 1, June 2000.
GR-740-CORE	*Stored Program Control System/Operations System (SPCS/OS) - Network Data Collection Operations System (NDC OS) Interface*, March 200).
GR-815-CORE	*Generic Requirements for Network Element/Network System (NE/NS) Security: A Module of LSSGR*, Component of FR-64, Issue 2, March 2002.
GR-820-CORE	*OTGR Section 5.1: Generic Digital Transmission Surveillance*, Issue 2, December 1997.
GR-1089-CORE	*Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*, Issue 05, August 2009.
GR-1230-CORE	*SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria*, Issue 4, December 1998.
GR-1244-CORE	*Clocks for the Synchronized Network: Common Generic Criteria*, Issue 1, May 2005.
GR-1400-CORE	*SONET Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria*, Issue 3, July 2006.
GR-2865-CORE	*Generic Requirements for ISDN PRI Two B-Channel Transfer*, Issue 3, March 2000.
GR-2911-CORE	*Software Inventory for Network Element Software Management*, Issue 1, June 1995.
GR-2996-CORE	*Generic Criteria for SONET Digital Cross-Connect Systems*, Issue 1, January 1999.
GR-3051-CORE	*Voice Over Packet: NGN Call Connection Agent Generic Requirements*, Issue 2, January 2001.
GR-3055-CORE	*Voice Over Packet: NGN Access Gateway Generic Requirements*, Issue 1, March 2000.
SR-2275	*Telcordia Notes on the Networks*, Issue 4, October 2000.
SR-3580	*NEBS Criteria Levels*, Issue 3, June 2007.
SR-4994	*2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment*

PUBLICATION NUMBER	TITLE
	Generic Guidelines, Issue 1, December 1999.
SR-NWT-002120	*National ISDN-2*, Issue 1, May 1992 with revision 1, June 1993.
SR-NWT-002343	*ISDN Primary Rate Interface Generic Guidelines for Customer Premises Equipment*, Issue 1, June 1993.
SR-NWT-002419	*Software Architecture Review Checklists*, Issue 01, December 1992.
TR-917	*SONET Regenerator (SONET RGTR) Equipment Generic Criteria*, December 1990.
TR-NWT-000057	*Functional Criteria for Digital Loop Carrier Systems*, Issue 2, January 1993.
TR-NWT-000170	*Digital Cross-Connect System Generic Requirements and Objectives*, January 1993.
TR-NWT-000179	*Software Quality Program Generic Requirements*, June 1993.
TR-NWT-000295	*Isolated Ground Planes: Definition and Application to Telephone Central Offices*, Issue 2, July 1992.
TR-NWT-000418	*Generic Reliability Assurance for Fiber Optic Transport Systems*, Issue 2, December 1992.
TR-NWT-001244	*Clocks for the Synchronized Network: Common Generic Criteria,* Issue 1, June 1993.
TR-NWT-001268	*ISDN Primary Rate Interface Call Control Switching and Signaling Generic Requirements for Class II Equipment*, Issue 1, December 1991.

C.3.19 Telecommunications Industry Association

TITLE	DATE
EIA/TIA-530-A, "High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector," ANSI/TIA/EIA-530-A-92) (R98) (R2003)	June 1992
TIA/EIA-232-F, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange"	October 1997
TIA-422-B, "Electrical Characteristics of Balanced Voltage Digital Interface Circuits," (ANSI/TIA/EIA-422-B-1994) (R2000) (R2005)	April 13, 2004
TIA-810-B	November 3, 2006
TIA TSB-116-A, "Telecommunications System Bulletin – Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony"	March 2006

C.3.20 United States Code

TITLE	DATE
Title 10	Section 2224, "Defense Information Assurance Program"

C.3.21 Other Documentation

TITLE	DATE
3G TS 24.067 V3.0.0 (1999-05), 3rd Generation Partnership Project; Technical Specification Group Core Network; enhanced MLPP (eMLPP) – Stage 3.	

TITLE	DATE
Alberts, Garstka, and Stein, "Network Centric Warfare," 2nd Edition Revised	February 2000
American National Standards Institute (ANSI)/Electronic Industries Association (EIA) Standard, ANSI/EIA-310-D-92, *Cabinets, Racks, Panels and Associated Equipment*	September 1992
AT&T TR62411.	
Defense Intelligence Agency, Defense Intelligence Agency Manual (DIAM) 50-3, "Physical Security Standards for Construction of Sensitive Compartmented Information Facilities"	
Director of Central Intelligence Directive 6/3, DCID 6/3, Series, "Protecting Sensitive Compartmented Information within Information Systems"	1999
FED-STD-1037, "Telecommunications: Glossary of Telecommunication Terms," http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm.	August 7, 1996
Federal Telecommunications Recommendation 1080B-2002, *"Video Teleconferencing Services"*	August 15, 2002
"Generic Cryptographic Interoperability Requirements Document (GCIRD)," Version 1.3	January 7, 2008
Global Information Grid NetOps Guidance and Policy Memorandum No. 10-8460, "Network Operations"	August 24, 2000
Horizontal Fusion Standards and Specifications	November 3, 2004
House Report 107-436, "Bob Stump National Defense Authorization Act for Fiscal Year 2003": Report of the Committee on Armed Services, House of Representatives on H.R. 4546	May 3, 2002
International Electrotechnical Commission (IEC), 60950-1, "Information technology equipment – Safety – Part 1: General requirements," Second Edition, 2005-12.	
International Standardization Organization, ISO 13871, "Digital Channel Aggregation," June 2001.	June 2001
Joint Interoperability Test Center, "Internet Protocol Version 6 Generic Test Plan," Version 2	June 2006
Joint Staff, Command, Control, Communications, and Computer Systems Directorate (J-6), "Joint Net-Centric Operations Campaign Plan"	October 2006
Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Concept of Operations (CONOPS)"	
Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Initial Capability Document (ICD)"	
Joint Staff, "Global Information Grid 2.0 (GIG 2.0) Implementation Plan"	
National Communications System, NCS Directive 3-10, "Telecommunications Operations, Government Emergency Telecommunications Service (GETS)"	2000
National Fire Protection Association (NFPA) 72, "National Fire Alarm and Signaling Code"	2010
National Institute of Standards and Technology (NIST) Special Publication 800-88, "Guidelines for Media Sanitization, Computer Security, Richard Kissel, Matthew Scholl, Steven Skolochenko, and Xing Li	September 2006
National Institute of Standards and Technology (NIST) Special Publication 800-57, "Recommendation for Key Management-Part 1: General (Revised)", Elaine Barker, Williams Barker, William Burr, William Polk, and Miles Smid, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf	March 2007
National Institute of Standards and Technology (NIST) Special Publication 800-57, "Recommendation for Key Management-Part 2: Best Practices for Key Management Organization", Elaine Barker, Williams Barker, William Burr, William Polk, and Miles Smid, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf	March 2007

TITLE	DATE
National Institute of Standards and Technology (NIST) Special Publication 800-57, "Recommendation for Key Management-Part 3: Application-Specific Key Management Guidance", Elaine Barker, William Burr, Alicia Jones, Timothy Polk, Scott Rose, Miles Smid and Quynh Dang, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf	December 2009
National Institute of Standards and Technology (NIST) Special Publication 800-72-3, "Cryptographic algorithm and Key Sizes for Personal Identify Verification", W. Timothy Polk, Donna F. Dodson, William Burr, Hildegard Ferraiolo, and David Cooper,	December 2010
National Institute of Standards and Technology (NIST) Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", Elaine Barker and Allen Roginsky, http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf	January 2011
North American Treaty Organization (NATO), Standard NATO Agreement (STANAG 4214), "International Rating and Directory for Tactical Communications Systems," Edition 3, Version T	January 7, 2005
OASIS Standard Common Alerting Protocol (CAP), v1.1	October 2005
Office of Management and Budget (OMB) Circular A-130, Appendix III	
RS-232, Recommended Standard 232 for Serial Binary Data Signals Connecting Between a DTE and a DCE	
Underwriters Laboratories, Inc., UL-1950, Standard for Safety, Information Technology Equipment Including Electrical Business Equipment," First Edition	1999
"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for CDMA-Based Systems – Home Location Register (HLR)," Issue 1	June 4, 2004
"Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for GSM-Based Systems," Issue 2	January 2004