

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 7 Network Edge Infrastructure.....	7-1
7.1 Introduction.....	7-1
7.1.1 LAN Infrastructure Requirements by End User and Mission Environments ...	7-1
7.1.2 LAN Types and Nomenclature	7-2
7.2 LAN Switch and Router Product	7-4
7.2.1 General LAN Switch and Router Product	7-4
7.2.1.1 Port Interface Rates.....	7-5
7.2.1.2 Port Parameter.....	7-7
7.2.1.3 Class of Service Markings	7-7
7.2.1.4 Virtual LAN Capabilities.....	7-9
7.2.1.5 Protocols	7-12
7.2.1.6 Quality of Service Features.....	7-15
7.2.1.7 Network Monitoring	7-19
7.2.1.8 Security	7-19
7.2.2 LAN Switch and Router Redundancy.....	7-20
7.2.2.1 Single Product Redundancy	7-20
7.2.2.2 Dual Product Redundancy	7-21
7.2.3 LAN Product Requirements Summary	7-21
7.2.4 Multiprotocol Label Switching in ASLANs	7-23
7.2.4.1 MPLS	7-23
7.2.4.2 MPLS ASLAN.....	7-23
7.2.4.3 MPLS VPN Augmentation to VLANs	7-27
7.3 Wireless LAN	7-28
7.3.1 General Wireless Product	7-29
7.3.2 Wireless Interface	7-31
7.3.3 Wireless End Instruments	7-32
7.3.4 Wireless LAN Access System	7-33
7.3.5 Wireless Access Bridge	7-35
7.3.6 Survivability.....	7-38
7.4 Digital Subscriber Line (DSL).....	7-39
7.4.1 Introduction.....	7-39
7.4.2 DSL Product.....	7-39
7.4.3 Physical Layer.....	7-39
7.4.4 Data Link Layer	7-40

7.4.5	Network Layer	7-40
7.4.6	Information Assurance.....	7-41
7.4.7	DSL Support for Analog Voice Services.....	7-41
7.4.8	Device Management	7-42
7.5	Passive Optical Network (PON) Technology	7-42
7.5.1	Definition of PON.....	7-42
7.5.2	Interfaces.....	7-46
7.5.2.1	NNI Interface	7-46
7.5.2.2	OLT to ONT PON Interface	7-47
7.5.2.3	Network Management Interface	7-48
7.5.2.4	UNI Interface	7-49
7.5.3	Class of Service Markings	7-49
7.5.4	Virtual LAN Capabilities.....	7-50
7.5.5	Protocols	7-50
7.5.6	Quality of Service Features.....	7-50
7.5.7	Voice Services	7-50
7.5.7.1	Latency.....	7-50
7.5.7.2	Jitter.....	7-50
7.5.7.3	Packet Loss	7-50
7.5.8	Video Services	7-51
7.5.8.1	Latency.....	7-51
7.5.8.2	Jitter.....	7-51
7.5.8.3	Packet Loss	7-51
7.5.9	Data Services	7-51
7.5.9.1	Latency.....	7-51
7.5.9.2	Jitter.....	7-52
7.5.9.3	Packet Loss	7-52
7.5.10	Information Assurance.....	7-52
7.5.11	PON Network Management.....	7-52
7.5.11.1	Secure Shell Version 2.....	7-52
7.5.11.2	Telnet	7-53
7.5.11.3	HTTPS	7-53
7.5.11.4	LAN Products	7-53
7.5.11.5	Other Methods for Interfacing	7-53
7.5.12	Configuration Control.....	7-53
7.5.13	Operational Changes.....	7-53
7.5.14	Performance Monitoring.....	7-53
7.5.15	Alarms.....	7-53

7.5.16	Reporting.....	7-54
7.5.17	Fiber Media.....	7-54
7.5.18	RF-over-Glass (RFoG) Video.....	7-54
7.5.19	Traffic Engineering.....	7-54
7.5.20	VLAN Design and Configuration.....	7-54
7.5.21	Power Backup.....	7-54
7.5.22	Availability.....	7-55
7.5.23	Redundancy.....	7-55
7.5.23.1	Single Product Redundancy.....	7-55
7.5.23.2	Dual Product Redundancy.....	7-56
7.5.24	Survivability.....	7-56
7.5.25	Summary of PON Requirements by Subscriber Mission.....	7-56
7.6	Customer Edge Router.....	7-56
7.6.1	Traffic Conditioning.....	7-56
7.6.2	Differentiated Services Support.....	7-57
7.6.3	Per-Hop Behavior Support.....	7-57
7.6.4	Interface to the SC/SS for Traffic Conditioning.....	7-57
7.6.5	Interface to the SC/SS for Bandwidth Allocation.....	7-57
7.6.6	Network Management.....	7-57
7.6.7	Availability.....	7-58
7.6.8	Packet Transit Time.....	7-58
7.6.9	Customer Edge Router Interfaces and Throughput Support.....	7-59
7.6.10	Deployable (Tactical) Customer Edge Router.....	7-61

LIST OF FIGURES

<u>FIGURE</u>	<u>PAGE</u>
Figure 7.1-1. LAN Layers.....	7-2
Figure 7.1-2. Representative B/P/C/S Design and Terminology.....	7-3
Figure 7.2-1. IEEE 802.1Q Tagged Frame for Ethernet.....	7-8
Figure 7.2-2. TCI Field Description	7-9
Figure 7.2-3. Port-Based VLANs	7-10
Figure 7.2-4. IEEE 802.1Q-Based VLANs	7-11
Figure 7.2-5. User-Defined VLANs	7-12
Figure 7.2-6. Four-Queue Design	7-15
Figure 7.3-1. Access Methods for the Wireless Access Layer End Item Product Telephones	7-33
Figure 7.3-2. Example of Combined WLAS/WAB and Second Layer WAB.....	7-36
Figure 7.5-1. Typical PON Network Connectivity.....	7-43
Figure 7.5-2. PON Connectivity in the DOD Operational Framework	7-45
Figure 7.5-3. PON Connectivity in a Collapsed DOD Backbone Operational Framework	7-46

LIST OF TABLES

<u>TABLE</u>	<u>PAGE</u>
Table 7.1-1. Summary of LAN Requirements by End User Mission Category.....	7-1
Table 7.2-1. 802.1Q Default Values.....	7-8
Table 7.2-2. ASLAN Infrastructure RFC Requirements.....	7-13
Table 7.2-3. DSCP Assignments	7-18
Table 7.2-4. Core, Distribution, and Access Product Requirements Summary	7-21
Table 7.2-5. ASLAN Product MPLS Requirements	7-23
Table 7.3-1. 802.16 Service Scheduling.....	7-30
Table 7.3-2. Maximum Number of EIs Allowed per WLAS	7-34
Table 7.5-1. OLT to ONT Signaling Standards	7-48

SECTION 7 NETWORK EDGE INFRASTRUCTURE

7.1 INTRODUCTION

This section defines the following:

- Technical requirements for the products used in configuring the network edge infrastructure.
- Technical requirements for Customer Edge (CE) Routers (CE-Rs).
- Design requirements for Assured Services (AS) Local Area Networks (LANs) (ASLANs).

The network edge infrastructure consists of LAN products, local Digital Subscriber Line (DSL) and Passive Optical Network (PON) transport products, and the CE-R. The design requirements, based on commercial standards, were developed to support assured services for mission-critical users.

7.1.1 LAN Infrastructure Requirements by End User and Mission Environments

In order to provide cost-effective LAN solutions that meet mission requirements for all users served by a LAN, two types of LANs are defined: ASLANs and non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs.

[Table 7.1-1](#) summarizes selected LAN requirements in terms of LAN types and end user mission category.

Table 7.1-1. Summary of LAN Requirements by End User Mission Category

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	F/FO	I/P	R	NON-MISSION CRITICAL
ASLAN High	R	P	P	P
ASLAN Medium	NP	P	P	P
Non-ASLAN	NP	NP	N	P
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
Availability	99.999	99.997	99.9	99.8
LEGEND				
ASLAN: Assured Services LAN LAN: Local Area Network p: Probability of Blocking				

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	F/FO	I/P	R	NON-MISSION CRITICAL
F/FO: FLASH/FLASH OVERRIDE	MLPP: Multilevel Precedence and Preemption			
I/P: IMMEDIATE/PRIORITY	NP: Not Permitted		P: Permitted	
GOS: Grade of Service	NR: Not Required		R: Required	

7.1.2 LAN Types and Nomenclature

The ASLANs and non-ASLANs may be designed to use any combination of the layers and functional capabilities, shown in [Figure 7.1-1](#), LAN Layers. Multiple layers may be combined in a single switch or router (i.e., router acts as Distribution and Access Layers).

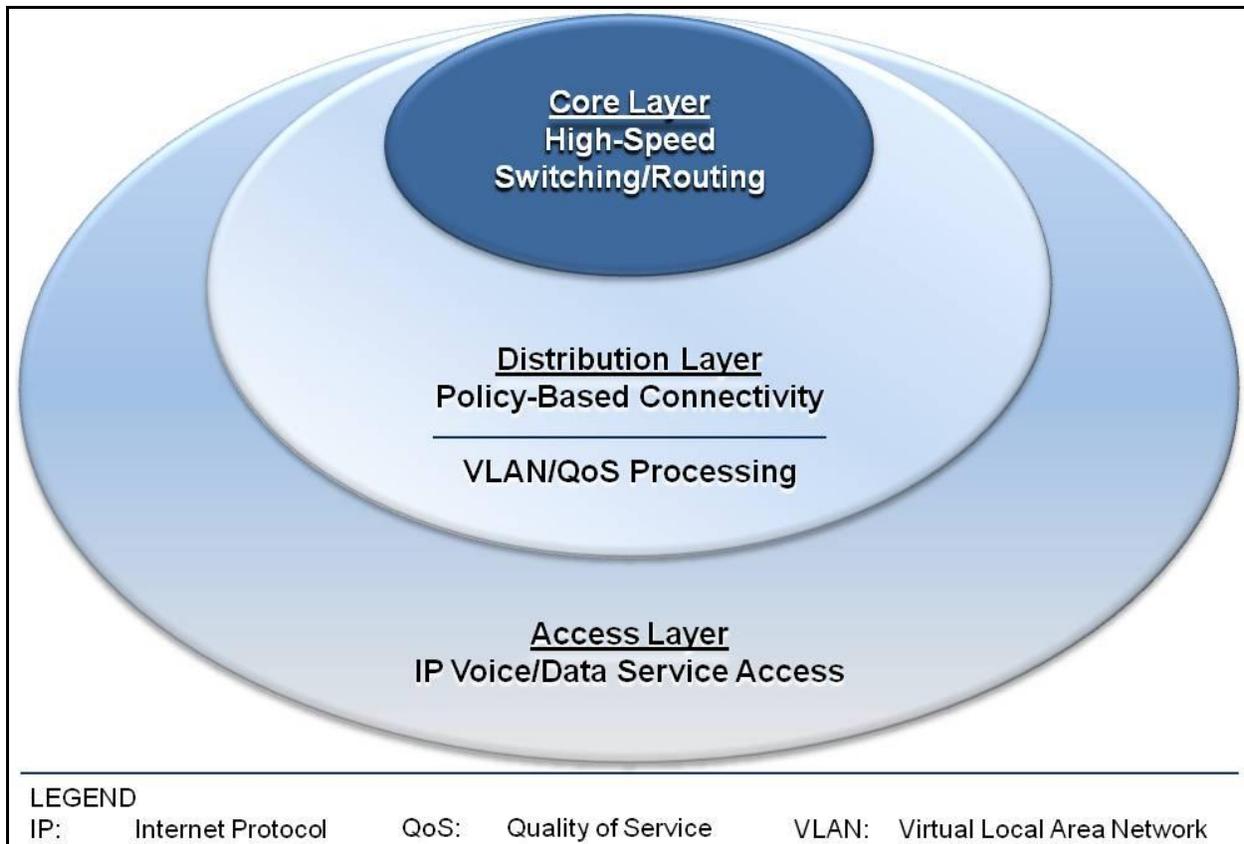


Figure 7.1-1. LAN Layers

The three LAN Layers are as follows:

1. Access Layer. 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 demarcation point between the Access and Core Layers. Helps to define and differentiate the Core. Provides boundary definition and is the place at which packet manipulation can take place.
3. Core Layer. A high-speed switching backbone designed to switch packets as quickly as possible.

[Figure 7.1-2](#), Representative B/P/C/S Design and Terminology, illustrates a typical Base/Post/Camp/Station (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.

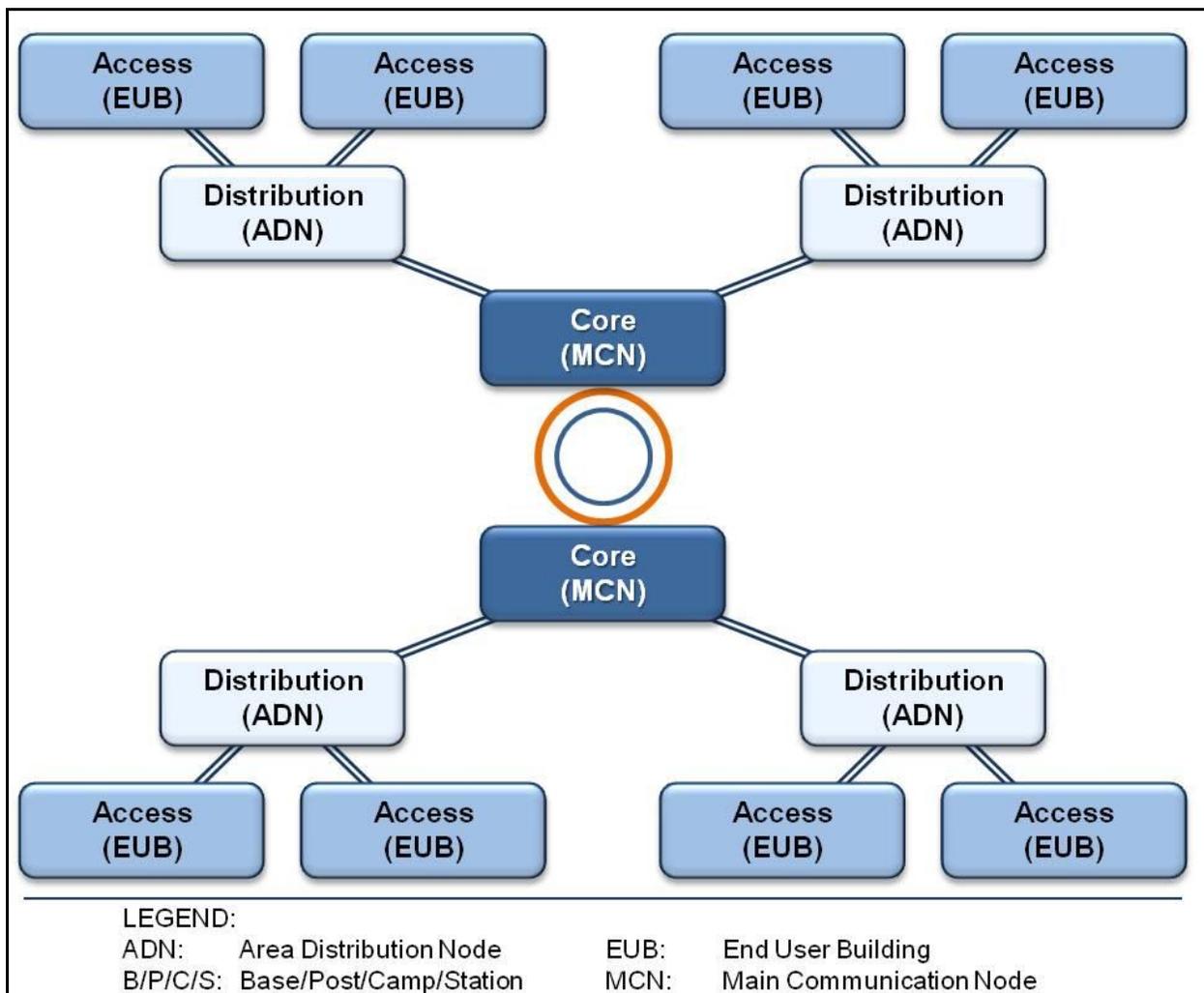


Figure 7.1-2. Representative B/P/C/S Design and Terminology

The LAN infrastructure may use DSL and PON products to extend voice, video, and data services at the access layer of the LAN hierarchy.

7.2 LAN SWITCH AND ROUTER PRODUCT

7.2.1 General LAN Switch and Router Product

EDG-000010 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of meeting the following parameters:

- a. Non-blocking. All Core, Distribution, and Access products shall be non-blocking for their ports based on the following traffic engineering. Non-blocking is defined as the capability to send and receive a mixture of 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports without losing any packets. Blocking factor is defined as the ratio of all traffic to non-blocked traffic (i.e., a blocking factor of 8 to 1 means that 12.5 percent of the traffic must be non-blocking). Each Core, Distribution, and Access product has up to three levels of performance: Minimum, Medium, and Maximum. For certification purposes, products need only meet minimum performance levels.

NOTE: These definitions/requirements are not applicable for wireless products; wireless products are half-duplex in accordance with (IAW) radio limitations.

- (1) Access Products. Access products shall not have a blocking factor that exceeds 8 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level Access products shall not have a blocking factor that exceeds 2 to 1. This blocking factor includes all hardware and software components. Maximum performance level Access products shall be non-blocking. This blocking factor includes all hardware and software components.
 - (2) Distribution and Core Products. These products shall not have a blocking factor that exceeds 2 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level products shall not have a blocking factor that exceeds 1.5 to 1. This blocking factor includes all hardware and software components. Maximum performance level products shall be non-blocking. This blocking factor includes all hardware and software components.
- b. Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The latency shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization.
 - (1) Voice/Signaling packets. No more than 2 milliseconds (ms) latency.
 - (2) Video Packets. No more than 10 ms latency.
 - (3) Preferred Data Packets. N/A.
 - (4) Best Effort Data. N/A.

-
- c. Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization.
- (1) Voice Packets. No more than 1 ms jitter.
 - (2) Video Packets. No more than 10 ms jitter.
 - (3) Preferred Data Packets. N/A.
 - (4) Best Effort Data. N/A.
- d. Packet Loss. All Core, Distribution and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The packet loss shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization.
- (1) Voice Packets. Allowed packet loss is dependent upon the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.015 percent for Access, Distribution, and Core products.
 - (2) Video Packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products.
 - (3) Preferred Data packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products.

7.2.1.1 Port Interface Rates

EDG-000020 [Required: Core and Distribution Products] Minimally, Core and Distribution products shall support the following interface rates [other rates and Institute of Electronics and Electrical Engineers (IEEE) standards may be provided as optional interfaces]. Rates specified are the theoretical maximum data bit rate specified for Ethernet; link capacity and effective throughput is influenced by many factors. For calculation purposes, link capacities are to be calculated IAW Request for Change (RFC) 2330 and RFC 5136. Network Management (NM) interfaces are defined in Section 2.19.

- a. Wide Area Network (WAN)-Side Interface. The product must minimally support the following:
 - (1) 100 megabits per second (Mbps) in accordance with (IAW) IEEE 802.3u.

(2) 1000 Mbps IAW IEEE 802.3z.

b. LAN-Side Interface. The product must minimally support the following:

(1) 100 megabits per second (Mbps) in accordance with (IAW) IEEE 802.3u.

(2) 1000 Mbps IAW IEEE 802.3z.

EDG-000030 [Required: Access Products] Minimally, Access products shall provide one of the following user-side interface rates (other rates and IEEE standards may be provided as optional interfaces):

a. 10 Mbps IAW IEEE 802.3i.

b. 10 Mbps IAW IEEE 802.3j.

c. 100 Mbps IAW IEEE 802.3u.

d. 1000 Mbps IAW IEEE 802.3z.

e. 1000 Mbps IAW IEEE 802.3ab.

EDG-000040 [Required: Access Products] Minimally, Access products shall provide one of the following trunk-side interface rates (other rates and IEEE standards may be provided as optional interfaces):

a. 100 Mbps IAW IEEE 802.3u.

b. 1000 Mbps IAW IEEE 802.3z.

EDG-000050 [Optional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide a fibre channel interface IAW American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) T11.2 and T11.3 (previously known as X3T9.3). If provided, the interface must meet the following:

a. RFC 4338, Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel.

b. RFC 4044, Fibre Channel Management.

EDG-000060 [Optional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide the following wireless LAN interface rates:

a. 54 Mbps IAW IEEE 802.11a.

b. 11 Mbps IAW IEEE 802.11b.

c. 54 Mbps IAW IEEE 802.11g.

d. 300–600 Mbps IAW IEEE 802.11n.

e. IEEE 802.16 – Broadband wireless communications standards for MANs.

EDG-000070 [Optional] If any of the above wireless interfaces are provided, then the interfaces must support the requirements of [Section 7.3](#), Wireless LAN.

7.2.1.2 Port Parameter

EDG-000080 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall provide the following parameters on a per port basis as specified:

- a. Auto-negotiation IAW IEEE 802.3.
- b. Force mode IAW IEEE 802.3.
- c. Flow control IAW IEEE 802.3x (Optional: Core).
- d. Filtering IAW RFC 1812.
- e. Link Aggregation IAW IEEE 802.1AX (applies to output/egress trunk-side ports only).
- f. Spanning Tree Protocol IAW IEEE 802.1D (Optional: Core).
- g. Multiple Spanning Tree IAW IEEE 802.1s (Optional: Core).
- h. Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w (Optional: Core).
- i. Port-Based Access Control IAW IEEE 802.1x (Optional: Core).
- j. Link Layer Discovery Protocol (LLDP) IAW IEEE 802.1AB (Optional Core and Distribution).
- k. Link Layer Discovery – Media Endpoint Discovery IAW ANSI/ Telecommunications Industry Association (TIA)-1057 (Optional Core and Distribution).
- l. Power over Ethernet (PoE) IAW either 802.3af-2003 or 802.3at-2009. (Required only for VVoIP solutions; for data applications or non-Assured Services (AS) solutions, PoE is optionally required.)

7.2.1.3 Class of Service Markings

EDG-000090 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall support Differentiated Services Code Points (DSCPs) IAW RFC 2474 for both Internet protocol (IP) IPv4 and IPv6 Packets, as follows:

- a. The Core, Distribution, and Access products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and assign that packet to a Quality of Service (QoS) behavior listed in [Section 7.2.1.6](#), Quality of Service Features.
- b. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Current DSCP values are provided in Section 6.2.2, Differentiated Service Code Point. (Optional: Access products)
- c. The Core, Distribution, and Access products must be able to support the prioritization of aggregate service classes with queuing according to [Section 7.2.1.6](#), Quality of Service Features.

EDG-000100 [Optional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see [Figure 7.2-1](#), IEEE 802.1Q Tagged Frame for Ethernet, and [Figure 7.2-2](#), TCI Field Description). Default values are provided in [Table 7.2-1](#), 802.1Q Default Values. If provided, the following Class of Service (CoS) requirements apply:

- a. The Core, Distribution, and Access products shall be capable of accepting any frame tagged with a user priority value (0–7) on an ingress port and assign that frame to a QoS behavior listed in [Section 7.2.1.6](#), Quality of Service Features.
- b. The Core and Distribution products shall be capable of accepting any frame tagged with a user priority value (0-7) on an ingress port and reassign that frame to any new user priority value (0-7) (Optional: Distribution and Access).

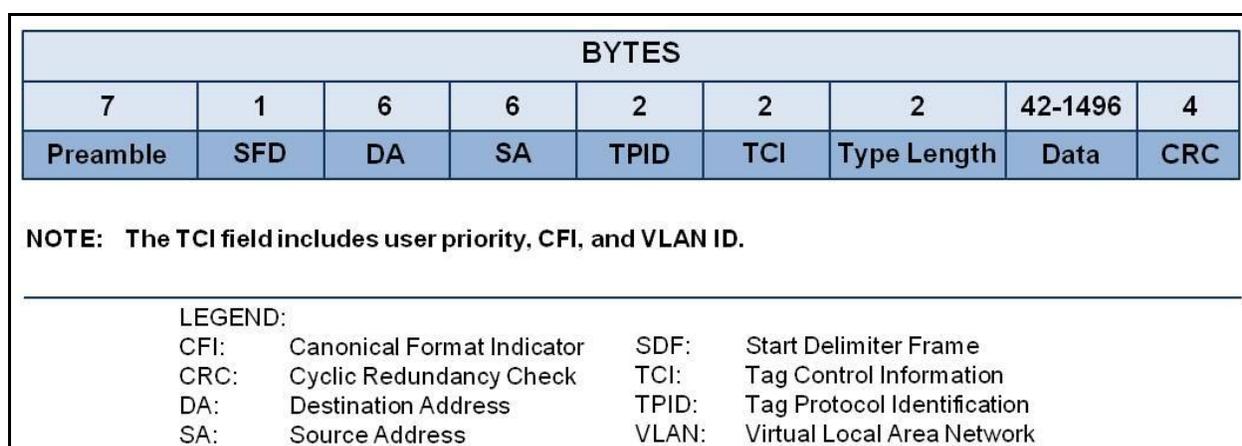


Figure 7.2-1. IEEE 802.1Q Tagged Frame for Ethernet

Table 7.2-1. 802.1Q Default Values

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT 802.1Q COS TAG	
		BASE 2	BASE 10
Control	Network Control	111	7
Inelastic/ Real-Time	User Signaling1	110	6
	Circuit Emulation1	110	6
	Short messages1	110	6
	Voice2	101	5
	Video/VTC	100	4
	Streaming	011	3
Preferred Elastic	Interactive Transactions OA&M – SNMP	010	2
	File Transfers OA&M – Trap/SysLog	001	1
Elastic	Default	000	0

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT 802.1Q COS TAG	
		BASE 2	BASE 10
NOTES:			
<ol style="list-style-type: none"> All user signaling (voice and video) may be grouped into this granular service class. User signaling, circuit emulation, and short messages may use the same TCI tag. Voice traffic must be differentiated with a different TCI tag from user signaling, circuit emulation, and short messages. 			
LEGEND			
802.1Q: IEEE VLAN/User Priority Specification		SysLog: System Log	
CoS: Class of Service		TCI: Tag Control Information	
OA&M : Operations, Administration, and Maintenance		VLAN: Virtual Local Area Network	
SNMP: Simple Network Management Protocol		VTC: Video Teleconferencing	

7.2.1.4 Virtual LAN Capabilities

EDG-000110 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of the following:

- Accepting Virtual Local Area Network (VLAN) tagged frames according to IEEE 802.1Q (see [Figure 7.2-1](#), IEEE 802.1Q Tagged Frame for Ethernet, and [Figure 7.2-2](#), TCI Field Description).

BITS		
3	1	12
User Priority	CFI	VID

NOTES:

- User Priority.** Defines eight (23) user priority levels. Access devices must be capable of recognizing the user priorities (0–7) and assign them to the QoS mechanisms listed below.
- CFI.** Always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- VID.** Has 12 bits and allows the identification of 4096 (2¹²) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.

LEGEND:

CFI:	Canonical Format Indicator	VID:	VLAN Identification
QoS:	Quality of Service	VLAN:	Virtual Local Area Network

Figure 7.2-2. TCI Field Description

- Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095).
- Supporting VLANs types IAW IEEE 802.1Q.

The VLANs offer the following features:

- **Broadcast Control.** Just as switches isolate collision domains for attached hosts and forward only 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.

Three ways of defining a VLAN are as follows:

- **Port-Based.** Port-based VLANs are VLANs that are dependent on the physical port 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 7.2-3](#), Port-Based VLANs).

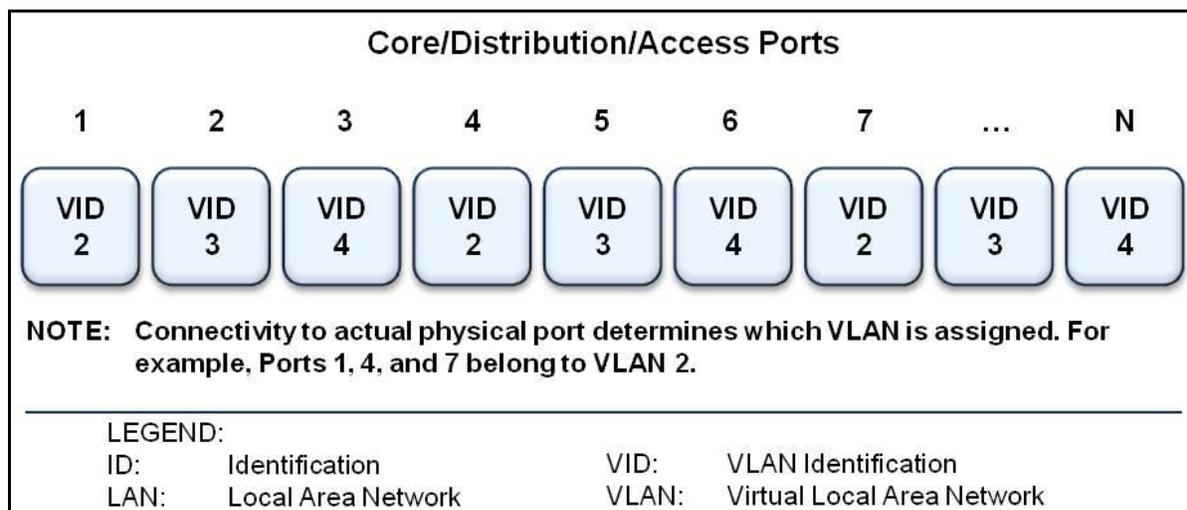


Figure 7.2-3. Port-Based VLANs

- **IEEE 802.1Q.** VLANs can be assigned by end products IAW the IEEE 802.1Q VLAN ID tag.

EDG-000120 [Required: Core, Distribution, and Access Products] The Unified Capabilities (UC) products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see [Figure 7.2-4](#), IEEE 802.1Q-Based VLANs).

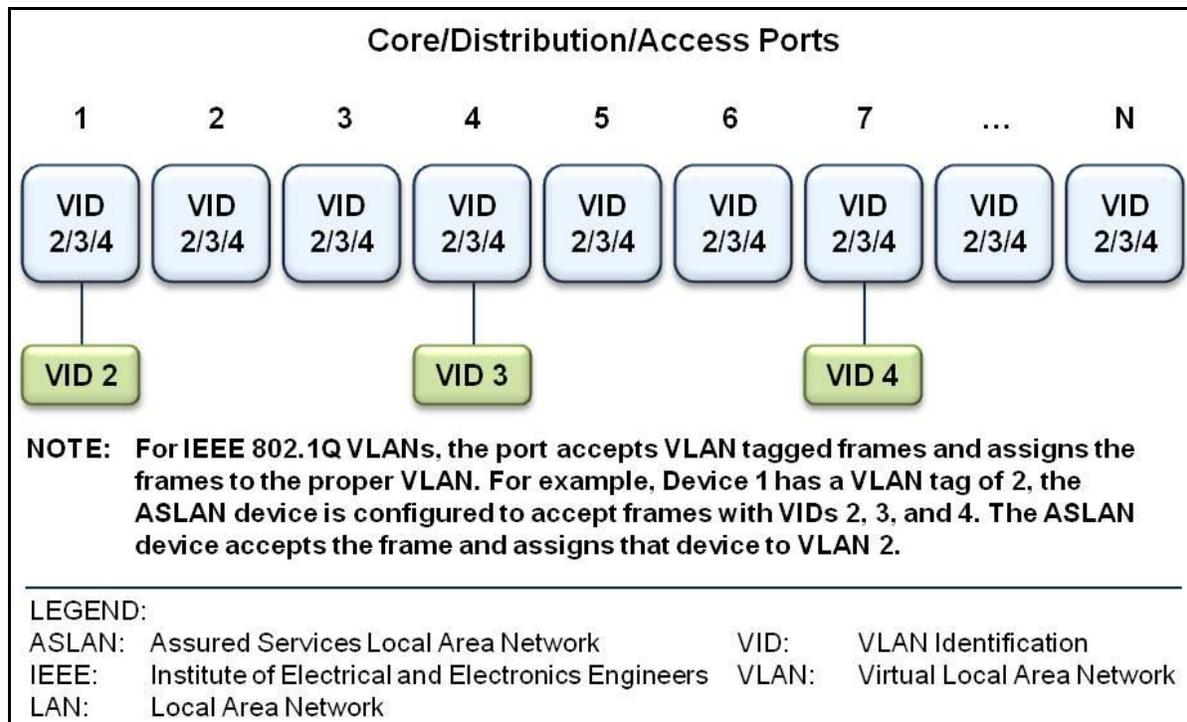


Figure 7.2-4. IEEE 802.1Q-Based VLANs

- **User-Defined Value.** This type of VLAN is typically the most flexible, allowing VLANs to be defined based on the value of any field in a packet or frame. For example, VLANs could be defined on a protocol basis or could be dependent on a particular address (Layer 2 or Layer 3). The simplest form of this type of VLAN is to group users according to their Media Access Control (MAC) addresses (see [Figure 7.2-5](#), User-Defined VLANs). The LAN shall be designed so that Real-Time Services (RTS) and data reside in separate VLANs. Whether a product is performing converged services or a single service will decide how VLANs are designed.

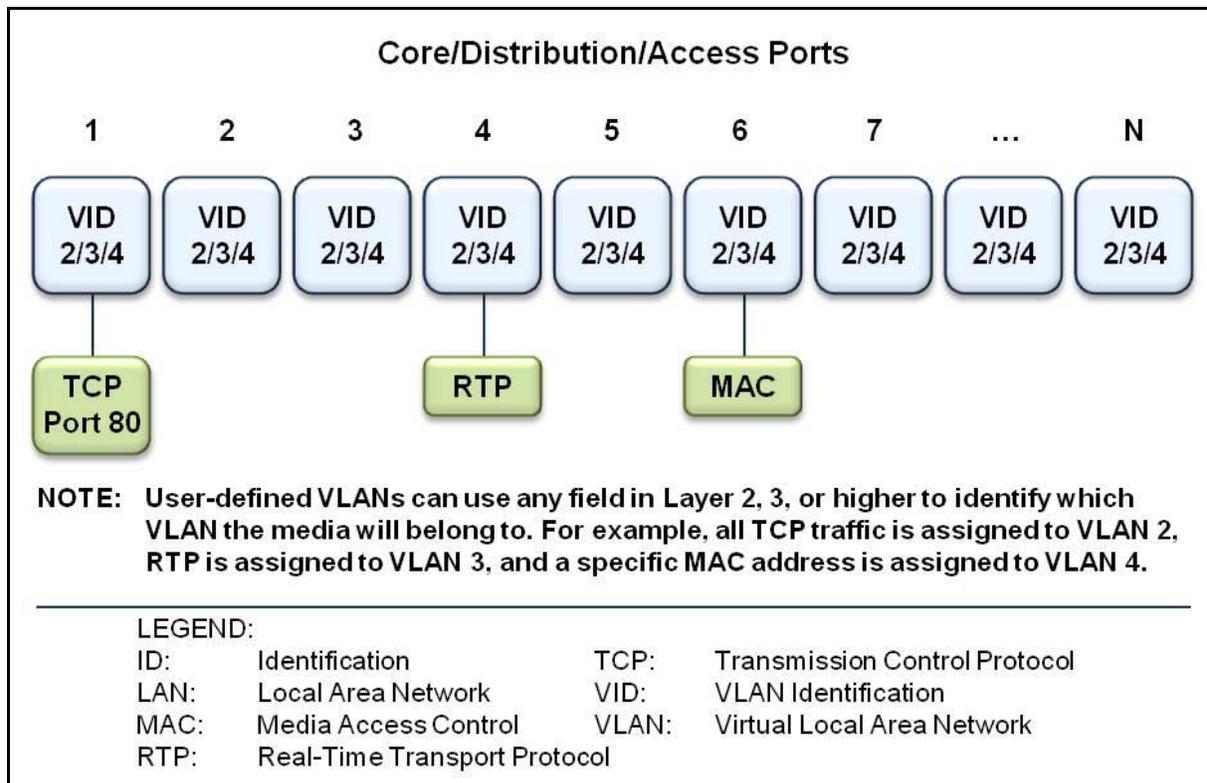


Figure 7.2-5. User-Defined VLANs

The required VLAN types are port-based and IEEE 802.1Q tagged frames. For VoIP, video, and data end products, any end system that supports convergence (i.e., more than one media) requires that the end-system pre-assign the VLAN using IEEE 802.1Q tags before the frames entering the ASLAN. For end-systems that support just one media (i.e., voice or video or data), the LAN can assign the VLAN based on port-based VLAN assignment.

Real-time services and data must be placed in separate VLANs for security purpose. The LAN may be designed with more than one VLAN per media type. Signaling for voice and video can be placed in the same VLAN as the respective media, or placed in an entirely different signaling VLAN.

7.2.1.5 Protocols

EDG-000130 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet protocol requirements for IPv4 and IPv6. RFC requirements are listed in [Table 7.2-2](#), ASLAN Infrastructure RFC Requirements. Additional IPv6 requirements by product profile are listed in Section 5, IPv6. These RFCs are not meant to conflict with Department of Defense (DOD) Information Assurance (IA) policy [e.g., Security Technical Implementation Guidelines (STIGs)]. Whenever a conflict occurs, DOD IA policy takes precedence. If there are conflicts with Section 5, RFCs applicable to IPv6 in Section 5 take precedence.

Table 7.2-2. ASLAN Infrastructure RFC Requirements

TITLE	RFC	C	D	A	WIRELESS
Open System Interconnect (OSI) Intermediate System to Intermediate System (IS-IS) for routing in Transmission Control Protocol (TCP)/IP and dual environments	RFC 1195	C	C	C	NA
Internet Control Message Protocol (ICMP) (PING)	RFC 1256	R	R	R	R
Network Time Protocol (NTP) (v3)	RFC 1305	R	R	R	R
Point-to-Point Protocol (PPP) Internet Protocol Control Protocol (IPCP)	RFC 1332	C	C	C	C
Management Information Base (MIB) (Definitions of Managed Objects)	RFC 1471	C	C	C	C
MIB (Definitions of Managed Objects for the Security Protocols)	RFC 1472	C	C	C	C
MIB (Definitions of Managed Objects for the IP Network Control Protocol)	RFC 1473	C	C	C	C
CIDR MIB (Classless Inter-Domain Routing)	RFC 1519	R	R	C	C
PPP Extensions	RFC 1570	C	C	C	C
MIB (Definitions for 4th version of BGP-4)	RFC 1657	R	C	C	C
Border Gateway Protocol (BGP 4)	RFC 1772	R	C	C	C
Requirements for IP version 4 Routers	RFC 1812	R	R	R	R
PPP Link Quality	RFC 1989	C	C	C	C
PPP Multi-Link	RFC 1990	C	C	C	C
PPP Handshake	RFC 1994	C	C	C	C
BGP Communities	RFC 1997	R	C	C	C
MIBs (IP mobility)	RFC 2006	C	C	C	C
International Organization for Standardization (ISO) Transport	RFC 2126	C	C	C	C
Dynamic Host Configuration Protocol (DHCP)	RFC 2131	C	C	C	C
DHCP and Bootstrap Protocol (BOOTP)	RFC 2132	C	C	C	C
Resource Reservation Protocol (RSVP)	RFC 2205	C	C	C	C
RSVP extensions	RFC 2207	C	C	C	C
RSVP with IntServ	RFC 2210	C	C	C	C
IntServ	RFC 2215	C	C	C	C
Open Shortest Path First version 2 (OSPFv2)	RFC 2328	R	R	C	C
Non-Broadcast Multi-Access (NBMA)	RFC 2332	C	C	C	C
BGP Protection	RFC 2385	R	C	C	C
BGP Route Flap	RFC 2439	R	C	C	C
Definition of the DS Field in the IPv4 and IPv6 Headers	RFC 2474	R	R	R	R
IP Header Compression	RFC 2507	C	C	C	C
Compressing IP/UDP/RTP	RFC 2508	C	C	C	C

TITLE	RFC	C	D	A	WIRELESS
X.509 Internet Public Key Infrastructure (PKI) OCSP	RFC 2560	R1	R1	R1	R1
TCP Congestion Control	RFC 2581	R	R	R	R
AF Per-Hop Behavior (PHB) Group	RFC 2597	R	R	R	R
MIB (Entity)	RFC 2737	R	R	R	R
OSPF for IPv6	RFC 2740	R	R	C	C
MIB (Network Services)	RFC 2788	C	C	C	C
BGP-4 Route Reflection	RFC 2796	R	C	C	C
MIB (Interfaces Group)	RFC 2863	R	R	R	R
BGP-4 Route Refresh	RFC 2918	R	C	C	C
Policy Core Information	RFC 3060	C	C	C	C
PHB ID Codes	RFC 3140	R	R	R	R
ECN	RFC 3168	C	C	C	C
IP Payload Compression	RFC 3173	C	C	C	C
Expedited PHB	RFC 3246	R	R	R	R
Remote NM	RFC 3273	R	R	R	R
Mobility for IPv4	RFC 3344	C	C	C	C
IGMP	RFC 3376	R	R	C	C
Capabilities Advertisement	RFC 3392	R	C	C	C
Architecture for SNMP Management Frameworks	RFC 3411	R	R	R	R
Message Processing and Dispatching	RFC 3412	R	R	R	R
SNMP Applications	RFC 3413	R	R	R	R
User-based Security Model	RFC 3414	R	R	R	R
View-based Access Control Model	RFC 3415	R	R	R	R
V2 of SNMP Protocol Operations	RFC 3416	R	R	R	R
Transport Mappings	RFC 3417	R	R	R	R
IP Header Compression over PPP	RFC 3544	C	C	C	C
OSPFv2 Graceful Restart	RFC 3623	R2	R2	C	C
Policy QoS	RFC 3644	R	R	R	R
BGP-4	RFC 4271	R	C	C	C
BGP-4 Extended Communities Attribute	RFC 4360	R	C	C	C
Robust Header Compression	RFC 4362	C	C	C	R
Remote Monitoring (RMON) MIB	RFC 4502	R	R	R	R
Authentication/Confidentiality for OSPFv3	RFC 4552	R	R	C	NA
PIM-SM	RFC 4601	R	R	C	NA

TITLE	RFC	C	D	A	WIRELESS
Graceful Restart for BGP	RFC 4724	R2	R2	C	C
MIB (OSPF V2)	RFC 4750	R	R	C	NA
OSPFv3 Graceful Restart	RFC 5187	R2	R2	C	C
RFC 5556 "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement"	RFC 5556	C	C	C	C
NOTE 1: If there are any conflicts between the RFC and the implementation of DOD PKI requirements, then DOD PKI requirements take higher priority.					
NOTE 2: The 18-month rule applies.					

7.2.1.6 Quality of Service Features

EDG-000140 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of the following QoS features:

- a. Providing a minimum of four queues (see [Figure 7.2-6](#), Four-Queue Design).

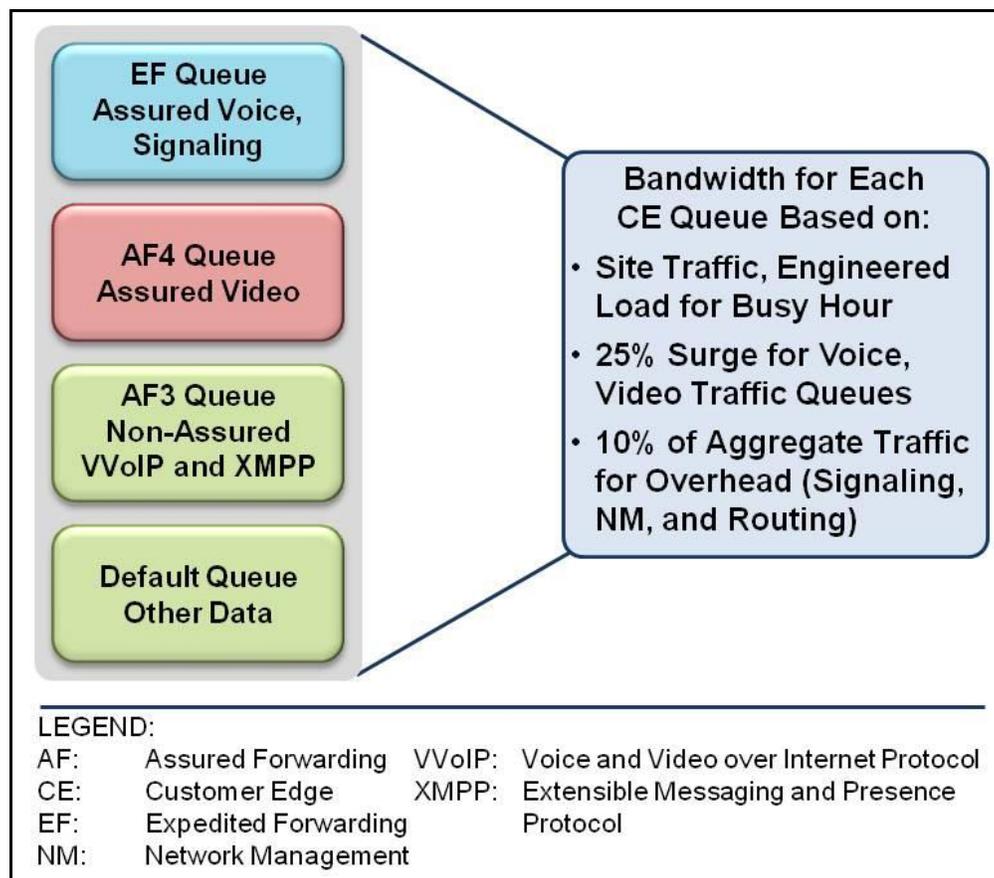


Figure 7.2-6. Four-Queue Design

- b. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface.

-
- c. Supporting Differentiated Services (DS), Per-Hop Behaviors (PHBs), and traffic conditioning IAW RFCs 2474, 2597, 3140, and 3246:
 - (1) Expedited Forwarding (EF).
 - (2) Assured Forwarding (AF).
 - (3) Best Effort (BE).
 - (4) Class Selector (CS).
 - (5) PHB Identification Codes.
 - d. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic.
 - e. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows:
 - (1) The product shall calculate the bandwidth associated with traffic conditioning in accordance with RFC 3246, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers [i.e., Point-to-Point Protocol (PPP), MAC, and so on] within a margin of error of 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.
 - (2) Core and Distribution products have been engineered for a blocking factor not to exceed 2:1. The aggregation of the Assured Forwarding and Expedition Forwarding queues should be configured to guarantee prioritization correctly, given the blocking factor. Priority queues (EF, AF4, and AF3) shall be configured so as not to exceed 50 percent of the egress link capacity.
 - (3) Access devices have been engineered for a blocking factor of 8:1 or less. Traffic prioritization is accomplished primarily to minimize latency. VoIP traffic is estimated at 2 (for dual appearances) bidirectional calls at 100 Kbps each or 400 Kbps (0 percent of 100 Mbps), video traffic is estimated at 500 Kbps bidirectional or 1 Mbps total (1.0 percent). With estimated blocking factor (8:1), 12.5 percent of the traffic is non-blocking. Based on traffic engineering outlined, the three priority queues should be set up not to exceed 12 percent of the egress link capacity.

NOTE: Bandwidth calculation assumes highest bandwidth use codec of G.711.

EDG-000150 [Required: 18-Month Rule] Provide a minimum of six queues (see Six-Queue Design).

-
- a. Assigning any incoming access/user-side “tagged” session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface.
 - b. Supporting DS, PHBs, and traffic conditioning IAW RFCs 2474, 2597, 3140, and 3246:
 - (1) Expedited Forwarding (EF).
 - (2) Assured Forwarding (AF).
 - (3) Best Effort (BE).
 - (4) Class Selector (CS).
 - (5) PHB Identification Codes.
 - c. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic.
 - d. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows:
 - (1) The product shall calculate the bandwidth associated with traffic conditioning in accordance with RFC 3246, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers (i.e., PPP, MAC, etc.) within a margin of error of 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.
 - (2) Core and Distribution products have been engineered for a blocking factor not to exceed 2:1. The aggregation of the Assured Forwarding and Expedition Forwarding queues should be configured to guarantee prioritization correctly, given the blocking factor. Priority queues (EF, AF4, and AF3) shall be configured as not to exceed 50 percent of the egress link capacity.
 - (3) Access devices have been engineered for a blocking factor of 8:1 or less. Traffic prioritization is accomplished primarily to minimize latency. VoIP traffic is estimated at 2 (for dual appearances) bidirectional calls at 100 Kbps each or 400 Kbps (0 percent of 100 Mbps), video traffic is estimated at 500 Kbps bidirectional or 1 Mbps total (1.0 percent). With estimated blocking factor (8:1), 12.5 percent of the traffic is non-blocking. Based on traffic engineering outlined, the three priority queues should be set up not to exceed 12 percent of the egress link capacity.

NOTE: Bandwidth calculation assumes highest bandwidth use codec of G.711.

EDG-000160 [Required] The product shall support the Differentiated Services Code Point (DSCP) plan, as shown in [Table 7.2-3](#), DSCP Assignments. DS assignments shall be software configurable for the full range of six bit values (0-63 Base10) for backwards compatibility with

IP precedence environments that may be configured to use the Type of Service (TOS) field in the IP header but do not support DSCP.

Table 7.2-3. DSCP Assignments

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8	
Network Control	Network Signaling (OSPF, BGP, etc.)	N/A	48	110 000	60	
Inelastic Real-Time	User Signaling (UC SIP, H.323, etc.)	N/A	40	101 000	50	
	Short Message	FO	32	100 000	40	
	Assured Voice (Includes SRTCP)		FO	41	101 001	51
			F	43	101 011	53
			I	45	101 101	55
			P	47	101 111	57
			R	49	110 001	61
	Non-Assured Voice*	N/A	46	101 110	56	
	Assured Multimedia Conferencing (voice, video, and data) (code points 34, 36, and 38 are for Non-Assured Multimedia Conferencing)		FO	33	100 001	41
			F	35	100 011	43
			I	37	100 101	45
			P	39	100 111	47
			R	51 [34,36,38]**	110 011	63
	Broadcast Video	N/A	24	011 000	30	
Preferred Elastic	Multimedia Streaming	FO	25	011 001	31	
		F	27	011 011	33	
		I	29	011 101	35	
		P	31	011 111	37	
		R	26 [28,30]**	011 010	32	
	Low-Latency Data: (IM, Chat, Presence)		FO	17	010 001	21
			F	19	010 011	23
			I	21	010 101	25
			P	23	010 111	27
			R	18 [20,22]**	010 010	22
	High Throughput Data		FO	9	001 001	11
			F	11	001 011	13
			I	13	001 101	15

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
		P	15	001 111	17
		R	10 [12,14]**	001 010	12
	OA&M	N/A	16	010 000	20
Elastic	Best Effort	N/A	0	000 000	00
	Low Priority Data	N/A	8	001 000	10
<p>LEGEND:</p> <p>BGP: Border Gateway Protocol DSCP: Differentiated Services Code Point F: FLASH FO: FLASH OVERRIDE I: INTERMEDIATE IM: Instant Messaging N/A: Not Applicable</p> <p>OA&M: Operations, Administration, and Maintenance OSPF: Open Shortest Path First P: PRIORITY R: ROUTINE SRTCP: Secure Real-Time Transport Control Protocol UC SIP: Unified Capabilities Session Initiation Protocol</p> <p>* For a definition see Appendix A, Section A2, Glossary and Terminology Description. ** Code points in brackets are reserved for nonconformance marking.</p>					

7.2.1.7 Network Monitoring

EDG-000170 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall support the following network monitoring features:

- a. Simple Network Management Protocol Version 3 (SNMPv3) IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416, and 3417.
- b. Remote Monitoring (RMON) IAW RFC 2819.
- c. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584.
- d. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826.

7.2.1.8 Security

EDG-000180 [Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet the security protocol requirements listed in Section 4, Information Assurance, as follows: Core and Distribution products shall meet all requirements annotated as Router (R) and LAN Switch (LS). Access switches shall meet the IA requirements annotated for LS. In addition to wireless IA requirements previously specified, Wireless Local Area Network Access Systems (WLASs) and Wireless Access Bridges (WABs) shall meet all IA

requirements for LSs. Wireless End Instruments (WEIs) shall meet all IA requirements annotated for End Instruments (EIs). When conflicts exist between the Unified Capabilities Requirements (UCR) and STIG requirements, the STIG requirements will take precedence.

7.2.2 LAN Switch and Router Redundancy

The following paragraphs outline the redundancy requirements for the LAN products.

EDG-000190 [Required: Core, Distribution, and Access Products] The ASLAN (High and Medium) shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. A single point of failure up to and including 96 subscribers is acceptable; however, to support mission-critical needs, FLASH/FLASH OVERRIDE (F/FO) subscribers should be engineered for maximum availability. To meet the availability requirements, all switching/routing platforms that offer service to more than 96 telephony subscribers shall provide redundancy in either of two ways:

- a. The product itself (Core, Distribution, or Access) provides redundancy internally.
- b. A secondary product is added to the ASLAN to provide redundancy to the primary product (redundant connectivity required).

7.2.2.1 Single Product Redundancy

EDG-000200 [Optional: Core, Distribution, and Access Products] If a single product is used to meet the redundancy requirements, then the following requirements are applicable to the product:

- a. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis.
- b. Dual Processors (Control Supervisors). The chassis shall support dual-control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls). Failure of the primary processor to secondary must meet 5-second failover without loss of active calls.
- c. Termination Sparing. The chassis shall support a (N + 1) sparing capability for available 10/100 Base-T modules used to terminate to an IP subscriber.
- d. Redundancy Protocol. Routing equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the ASLAN that could cause an outage to more than 96 IP subscribers. Redundancy protocols will be standards based as specified in this document.
- e. No Single Failure Point. No single point shall exist in the LAN that would cause loss of voice service to more than 96 IP telephony instruments.

- f. Switch Fabric or Backplane Redundancy. Switching platforms within the ASLAN shall support a redundant (1 + 1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the switch.

NOTE: In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds.

7.2.2.2 Dual Product Redundancy

EDG-000210 [Optional: Core, Distribution, and Access Products] If the System Under Test (SUT) provides redundancy through dual products, then the following requirements are applicable:

- a. The failover over to the secondary product must not result in any lost calls. The secondary product may be in "standby mode" or "active mode," regardless of the mode of operation the traffic engineering of the links between primary and secondary must meet the requirements provided in [Section 7.5.19](#), Traffic Engineering.

NOTE: In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds.

7.2.3 LAN Product Requirements Summary

[Table 7.2-4](#), Core, Distribution, and Access Product Requirements Summary, summarizes product requirements.

Table 7.2-4. Core, Distribution, and Access Product Requirements Summary

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
Physical Ports	Serial Port	EIA/TIA	C	C	C
	10Base-TX	IEEE 802.3i	C	C	R1
	10Base-FX	IEEE802.3j	C	C	R1
	100Base-TX	IEEE 802.3u	R1	R1	R1
	100Base-FX	IEEE 802.3u	R1	R1	R1
	1000Base-TX	IEEE 802.3ab	C	C	R1
	1000Base-X	IEEE 802.3z	R	R	R1
	10GBase-X	IEEE 802.3ae, 802.3ak, 802.3an, 802.3aq, 802.3av	C	C	C
40GBase-X	IEEE 802.3ba	C	C	C	

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
	100GBase-X	IEEE 802.3ba	C	C	C
Port Parameters	Auto-negotiation	IEEE 802.3	R	R	R
	Force Mode	IEEE 802.3	R	R	R
	Flow Control	IEEE 802.3x	C	R	R
	Filtering	RFC 1812	R	R	R
Port Parameters (cont.)	Link Aggregation	IEEE 802.3ad	R	R	R
	Rapid Spanning Tree Protocol	IEEE 802.1D	C	R	R
	Multiple Spanning Tree Protocol	IEEE 802.1Q	C	R	R
	Port Based Access Control	IEEE 802.1x 2	C	R	R
Traffic Prioritization	CoS Traffic Classes (PCP Field)	IEEE 802.1Q	C	C	C
	DSCP	RFC 2474	R	R	R
VLANs	Port Based	IEEE 802.1Q	R	R	R
IPv4 Protocols	IPv4 features	Section 7.2.1.5 , Protocols	R	R	R
IPv6 Protocols	IPv6 features	Section 5	R	R	R
QoS	DS PHBs	RFCs 3246, 2597	R	R	R
	Minimum 4 hardware queues	DOD CoS/QoS WG	R	R	R
	FIFO	RFC 3670	C	C	C
	WFQ	RFC 3662	C3	C3	C3
	CQ	RFC 3670	C3	C3	C3
	PQ	RFC 1046	C3	C3	C3
	CB-WFQ	RFC 3366	C3	C3	C3
Security	Security requirements are contained in the IA portion of the document		R	R	R

NOTE 1. Product need only provide one of the specified interfaces.

NOTE 2. Only between end-user and product, not trunks.

NOTE 3. One of these queuing mechanisms is required to implement EF PHB.

LEGEND

C: Optional

FIFO: First-in First-out

RFC: Request for Change

CB-WFQ: Class-Based Weighted Fair Queuing

IEEE: Institute of Electrical and Electronic Engineers

RMON: Remote Monitoring

CoS: Class of Service

IPv4: IP Version 4

RTS: Real-Time Services

CQ: Custom Queuing

IPv6: IP Version 6

TIA: Telecommunications Industry Association

DISR: DOD Information Technology Standards Registry

MAC: Media Access Control

UTP: Unshielded Twisted Pair

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
DS: Differentiated Services	PHB: Per Hop Behavior	VLAN: Virtual LAN			
EF: Expedited Forwarding	PQ: Priority Queuing	WFQ: Weighted Fair Queuing			
EIA: Electronics Industries Alliance	R: Required				

7.2.4 Multiprotocol Label Switching in ASLANs

The implementation of ASLANs sometimes may cover a large geographical area. For large ASLANs, a data transport technique referred to as Multiprotocol Label Switching (MPLS) may be used to improve the performance of the ASLAN core layer. The following paragraphs define the requirements for MPLS when used within the ASLAN.

7.2.4.1 MPLS

7.2.4.2 MPLS ASLAN

EDG-000220 [Optional: Core and Distribution Products] An ASLAN product that implements MPLS must still meet all the ASLAN requirements for jitter, latency, and packet loss. The addition of the MPLS protocol must not add to the overall measured performance characteristics with the following caveats:

- a. The MPLS device shall reroute data traffic to a secondary pre-sigaled Label Switched Path (LSP) in less than 1 second upon indication of the primary LSP failure.

EDG-000230 [Optional: Core and Distribution Products] Assured Services LAN Core and Distribution products are not required to support MPLS. Services and Agencies may choose to implement MPLS in the ASLAN to take advantage of the inherent technological advantages of MPLS. The ASLAN Core and Distribution products that will be used to provide MPLS services must support the RFCs contained in [Table 7.2-5](#), ASLAN Product MPLS Requirements. RFCs are listed as being REQUIRED (R), OPTIONAL (O), or CONDITIONAL (C). Optionally required RFCs are based on implementation of a particular feature, such as Virtual Private Networks (VPNs).

Table 7.2-5. ASLAN Product MPLS Requirements

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 5462, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field"	C	MPLS	
RFC 5420, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)"	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5332, "MPLS Multicast Encapsulations"	O	MPLS	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 5331, "MPLS Upstream Label Assignment and Context-Specific Label Space"	O	MPLS	
RFC 5151, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions"	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5129, "Explicit Congestion Marking in MPLS"	O	MPLS	
RFC 5063, "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart"	C	GMPLS	Required if GMPLS RSVP implemented
RFC 4974, "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls"	C	RSVP-TE/ GMPLS	Required if GMPLS RSVP-TE implemented
RFC 4874, "Exclude Routes – Extension to Resource Reservation Protocol-Traffic Engineering (RSVP-TE)"	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 4873, "GMPLS Segment Recovery"	C	GMPLS	Required if GMPLS implemented
RFC 4872, "RSVP-TE Extensions in Support of End-to-End (E2E) Generalized Multi-Protocol Label Switching (GMPLS) Recovery"	C	RSVP-TE/ GMPLS	Required if RSVP-TE implemented
RFC 4783, "GMPLS – Communication of Alarm Information"	C	GMPLS	Required if GMPLS implemented
RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling"	R	VPLS	
RFC 4761, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" (Updated by RFC 5462)	O	VPLS	Required if L2VPN implemented via BGP
RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/Multiprotocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)"	C	BGP/MPLS VPNs	Required if L3VPN implemented
RFC 4448, "Encapsulation Methods for Transport of Ethernet over MPLS Networks"	R	VPLS	
RFC 4447, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)"	C	VPLS	Required if LDP implemented
RFC 4420, "Encoding of Attributes for Multiprotocol Label Switching (MPLS) Label Switched Path (LSP) Establishment Using Resource Reservation Protocol-Traffic Engineering (RSVP-TE)"	C	RSVP-TE/MPLS	Required if RSVP-TE implemented

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 4379, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures"	C	MPLS; BGP/MPLS VPNs	Required if L3VPN implemented
RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)" (replaces RFC 2547)	C	MPLS VPNs	Required if L3VPN implemented
RFC 4328, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control"	C	GMPLS	Required if SONET optical interface implemented
RFC 4201, "Link Bundling in MPLS Traffic Engineering (TE)"	R	MPLS	
RFC 4182, "Removing a Restriction on the use of MPLS Explicit NULL"	R	MPLS	
RFC 4090, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels" The device shall be able to locally repair an RSVP-TE LSP by rerouting the LSP traffic around the failure using both the one-to-one backup and the facility backup methods as specified in Internet Engineering Task Force (IETF) RFC 4090.	C	MPLS	Required if RSVP-TE implemented
RFC 4003, "GMPLS Signaling Procedures for Egress Control"	C	GMPLS	Required if GMPLS implemented
RFC 3936, "Procedures for Modifying the Resource Reservation Protocol (RSVP)"	C	MPLS/RSVP	Required if RSVP implemented
RFC 3564, "Requirements for support of Differentiated Services-aware MPLS Traffic Engineering"	O	MPLS	
RFC 3479, "Fault Tolerance for the Label Distribution Protocol (LDP)"	C	MPLS	Required if LDP implemented
RFC 3478, "Graceful Restart Mechanism for Label Distribution Protocol"	C	MPLS	Required if LDP implemented
RFC 3473, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions" (Updated by RFCs 4003, 4201, 4420, 4783, 4874, 4873, 4974, 5063, 5151, and 5420)	C	MPLS	Required if RSVP-TE implemented
RFC 3471, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description" (Updated by RFCs 4201, 4328, and 4872)	R	MPLS	
RFC 3443, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks"	R	MPLS	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 3392, "Capabilities Advertisement with BGP-4"	C	BGP; BGP/MPLS VPNs	Required if BGP implemented
RFC 3270, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services" (Updated by RFC 5462)	R	MPLS	
RFC 3210, "Applicability Statement for Extensions to RSVP for LSP-Tunnels"	O	MPLS VPNs	
RFC 3209, "RSVP-TE: Extensions to RSVP for LSP Tunnels" (Updated by RFCs 3936, 4420, 4874, 5151, and 5420)	C	MPLS VPNs	Required if RSVP-TE implemented
RFC 3140, "Per Hop Behavior Identification Codes"	R	MPLS	
RFC 3107, "Carrying Label Information in BGP-4"	C	BGP/MPLS VPNs	Required if BGP implemented
RFC 3037, "LDP Applicability"	O	MPLS	
RFC 3036, "LDP Specification"	C	MPLS, VPLS	Required if LDP implemented
RFC 3032, "MPLS Label Stack Encoding" (Updated by RFCs 3270, 3443, 4182, 5129, 5332, and 5462)	R	MPLS	
RFC 3031, "Multi-Protocol Label Switching Architecture"	R	MPLS	
RFC 2961, "RSVP Refresh Overhead Reduction Extensions"	C	RSVP	Required if RSVP implemented
RFC 2917, "A Core MPLS IP Architecture"	O	MPLS	
RFC 2747, "RSVP Cryptographic Authentication" and RFC 3097, RSVP Cryptographic Authentication (Updated Message Type Value)	C	RSVP	Required if RSVP implemented
RFC 2702, "Requirements for Traffic Engineering Over MPLS"	R	MPLS	
RFC 2685, "Virtual Private Networks Identifier"	R	MPLS	
LEGEND:			
ASLAN: Assured Services Local Area Network	L2VPN: Layer 2 Virtual Private Network	RFC: Request for Change	
BGP: Border Gateway Protocol	L3VPN: Layer 3 Virtual Private Network	RSVP: Resource Reservation Protocol	
C: Optional	LAN: Local Area Network	RSVP-TE: Resource Reservation Protocol-Traffic Engineering	
EXP: Experimental	LDP: Label Distribution Protocol	SONET: Synchronous Optical Network	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
GMPLS: Generalized Multiprotocol Label Switching	LSP: Label Switched Path	TE: Traffic Engineering	
G.709: ITU-T Recommendation G.709, "Interfaces for the optical transport network (OTN)"	MPLS: Multiprotocol Label Switching	TTL: Time To Live	
IP: Internet Protocol	R: Required	VPLS: Virtual Private LAN Service	
ITU-T: International Telecommunication Union – Telecommunication Standardization Sector		VPN: Virtual Private Network	

7.2.4.3 MPLS VPN Augmentation to VLANs

The MPLS supports both Layer 2 and Layer 3 VPNs. A Layer 2 MPLS VPN, also known as L2VPN, is a point-to-point pseudo-wire service. An L2VPN can be used to replace existing physical links. The primary advantage of this MPLS VPN type is that it can replace an existing dedicated facility transparently without reconfiguration, and that it is completely agnostic to upper-layer protocols. A Layer 3 MPLS VPN, also known as L3VPN, combines enhanced routing signaling, MPLS traffic isolation, and router support for Virtual Routing/Forwarding (VRF) to create an IP-based VPN.

7.2.4.3.1 MPLS Layer 2 VPNs

EDG-000240 [Required: Core and Distribution Products Supporting MPLS] The ASLAN Core or Distribution products will provide Layer 2 MPLS VPNs by minimally supporting the following:

- a. RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling."

The product may additionally support the following:

- b. RFC 4761, "Virtual Private LAN Services (VPLS) Using BGP for Auto-Discovery and Signaling."

These methods are commonly referred to as "VPLS" even though they are distinct and incompatible with one another.

EDG-000250 [Optional: Core and Distribution Products] The ASLAN products used to support L2VPNs, RFC 4761, or RFC 4762 may support RFC 5501, "Requirements for Multicast Support in Virtual Private LAN Services."

7.2.4.3.2 MPLS Layer 3 VPNs

EDG-000260 [Required: Core and Distribution Products Supporting MPLS] The ASLAN Core or Distribution products will provide Layer 3 MPLS VPNs by supporting RFC 4364, “BGP/MPLS IP Virtual Private Networks (VPNs).”

EDG-000270 [Required: Core and Distribution Products Supporting MPLS] The ASLAN products used to support L3VPNs by RFC 4364 shall support the following RFCs:

- a. RFC 4382, “MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base.”
- b. RFC 4577, “OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs).”
- c. RFC 4659, “BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN.”
- d. RFC 4684, “Constrained Route Distribution for Border Gateway Protocol/Multiprotocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs).”

7.2.4.3.3 MPLS QoS

EDG-000280 [Required: Core and Distribution Products Supporting MPLS] The MPLS device must support QoS in order to provide for assured services. The product must support one of the following QoS mechanisms:

- a. DSCP mapping to 3 bit EXP field (E-LSP).
- b. Label description of PHB (L-LSP).

7.3 WIRELESS LAN

Wireless LAN implementations are considered as extensions of the physical layer. This section outlines the requirements when using wireless Ethernet technologies in a LAN to provide VoIP service to subscribers. In particular, this section defines four wireless areas that may apply to VoIP subscribers: Wireless End Instruments (WEIs), Wireless LAN Access System (WLAS), Wireless Access Bridges (WABs), and general requirements for wireless LANs (WLANs). For LANs supporting VoIP subscribers, wireless transport may only be used:

- Between WEIs and a WLAN to provide Access Layer functionality (i.e., wired Distribution and Core Layers).
- Between two or more LANs as a “bridge” technology.

The components of a wireless network are certified along with an ASLAN, while wireless VoIP devices are certified with the VoIP solution.

The requirements for each of the wireless technologies (i.e., WEIs, WLAS, and WABs) are contained in the following sections.

7.3.1 General Wireless Product

EDG-000290 [Required: Wireless Products] The following general wireless requirements must be ASLAN wireless components:

- a. If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DOD Profile for IPv6.
- b. 802.11 wireless products must be WiFi Alliance Certified and shall be certified at the Enterprise level for WiFi Protected Access 2 (WPA2). The products will also be WiFi multimedia (WMM) certified.
- c. 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.
- d. For wireless products that provide transport to more than 96 (I/P) telephony users, the wireless products shall provide redundancy, and WLAS and/or associated controller/ switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through one of the following:
 - (1) Single Product Redundancy. Shall have the following as a minimum: Dual power supplies/processors/radio systems/Ethernet ports, and no single point of failure for more than 96 subscribers. It should be noted that single point of failure may exist for more than 96 subscribers if 96 or fewer are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers).
 - (2) Dual Product Redundancy. Shall be collocated or co-adjacent and shall have the following as a minimum: Traffic engineering to support all users on a single product upon failure of the other product. Secondary product may be on full standby or traffic sharing, supporting 50 percent of the traffic before failure rollover. Products must support a redundancy protocol.
- e. All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as follows:
 - (1) FIPS 140-2, Level 1. Wireless components must be operated from within a “limited access, secure room” and be under user positive control at all times. However, if the wireless end item is designed to be left unattended or is designed as an item that can be left behind, such as a wireless free-standing desk telephone, then that wireless end item must be Level 2 compliant.
 - (2) FIPS 140-2, Level 2. Wireless components can be operated in an open public area such as an “open hallway,” but the use of a “limited access, secure room” if available and/or operationally feasible is recommended.

- f. The use of wireless in the LAN as a bridging function shall not increase latency by more than 10 ms for each bridging pair. The use of wireless via an access point shall not increase LAN latency by more than 10 ms.
- g. The wireless products shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type:
- (1) **802.11 Interfaces.** Wireless products using 802.11 shall use the settable Service Class tagging/QoS parameters within 802.11e to implement, as a minimum, DSCP. The product shall support WMM. Wireless mobile devices shall also support WMM Power Save.
 - (2) **802.16 Interfaces.** Wireless products using 802.16d and/or 802.16e, QoS/Service Class tagging shall meet the following requirements:
 - (a) The WLAN products may use 802.16 services to provide QoS over the wireless portion of the transport.
 - (b) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPs (see [Table 7.3-1](#), 802.16 Service Scheduling).

Table 7.3-1. 802.16 Service Scheduling

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	802.16 SERVICE	RADIO SERVICE TRAFFIC PRIORITY	WIRED LANS DEFAULT DSCPS	
				BASE 2	BASE 10
Control	Network Control	N/A	N/A	110 000-110 111	48-56
Inelastic/Real-Time	User Signaling	UGS	7	101 000-101 111	40-47
	Circuit Emulation	UGS	6		
	Voice	UGS	6		
	Short messages	ertPS	5		
	Video/VTC	ertPS	4	100 000-100 111	32-39
	Streaming	rtPS	3	011 000-011 111	24-31
Preferred Elastic	Interactive Transactions and OA&M	nrtPS	2	010 000-010 111	16-23
	File Transfers and OA&M	nrtPS	1	001 000-001 111	8-15
Elastic	Default	BE	0	000 000-000 111	0-7

LEGEND

BE: Best Effort

NA: Not Applicable

rtPS: Real-Time Polling Service

DSCP: Differentiated Services Code Point

nrtPS: Non Real-Time Polling Service

UGS: Unsolicited Grant Service

ertPS: Extended Real-Time Polling Service

OA&M: Operations, Administration, and Management

VTC: Video Conferencing

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	802.16 SERVICE	RADIO SERVICE TRAFFIC PRIORITY	WIRED LANS DEFAULT DSCPS	
				BASE 2	BASE 10
LAN: Local Area Network		N/A: Not Applicable			

- h. Wireless products shall meet the security requirements as stipulated in the Wireless Security Technical Implementation Guide (STIG) and the following specified requirements:
- (1) All 802.11 wireless components shall do the following:
 - (a) Use the AES-Counter with Cipher Block Chaining-Message Authentication Code Protocol (CCMP) (AES-CCMP). It will be implemented in 802.11i system encryption modules.
 - (b) Implement the Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi Protected Access (WPA2).
 - i. Wireless access systems shall meet previously stated requirements for access products.
 - j. Wireless systems shall use the Control and Provisioning of Wireless Access Points (CAPWAP) Protocol IAW RFC 5415 and RFC 5416.

7.3.2 Wireless Interface

EDG-000300 [Required: WEI and WLAS] If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces:

- a. 802.11a IAW 802.11-2007 – 5 GHz.
- b. 802.11b IAW 802.11-2007 – 2.4GHz.
- c. 802.11g IAW 802.11-2007 – 2.4 GHz.
- d. 802.11n-2009 – 2.4 GHz and 5 Ghz.
- e. 802.16-2009.

EDG-000310 [Required: WEI and WLAS] For any of the 802.11 interfaces, the wireless product must minimally support the following two 802.11 standards:

- a. 802.11e – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. See, for priority bit assignment.
- b. 802.11i – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 6: Medium Access Control (MAC) Security Enhancements.

EDG-000320 [Required: WEI and WLAS] For the 802.11a interface, the wireless product must support the standard 802.11h – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe.

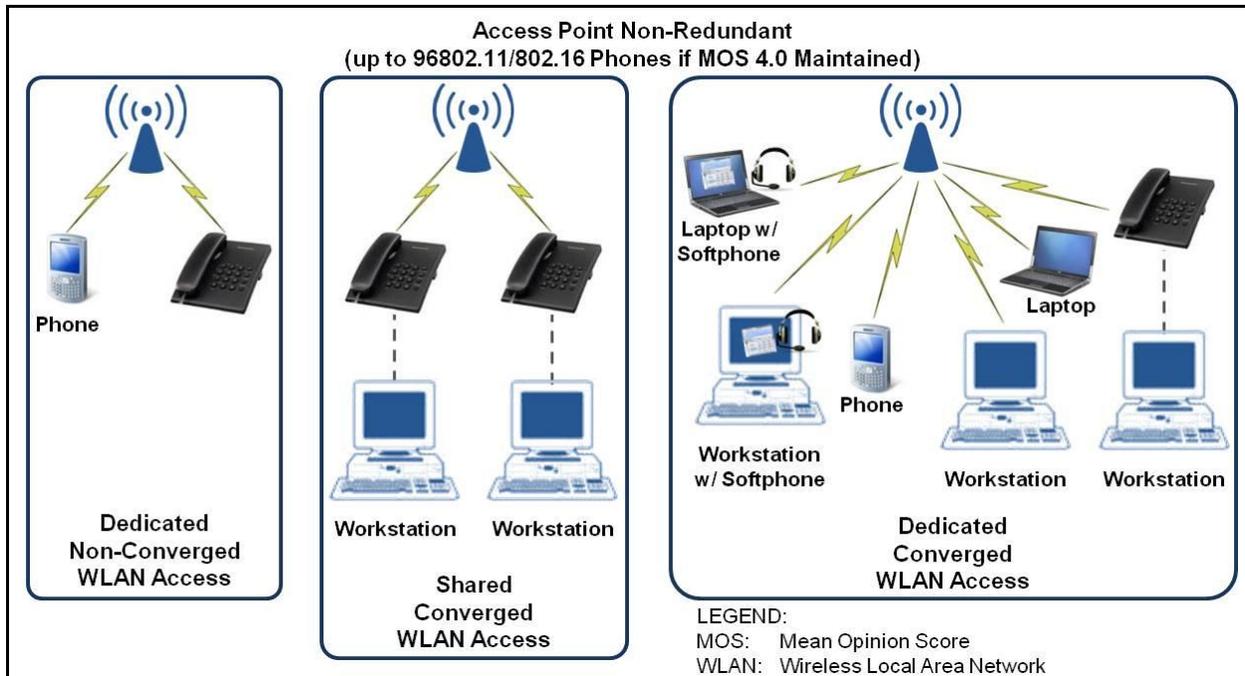
EDG-000330 [Required: WEI and WLAS] For any of the 802.16 interfaces, the wireless product must support the following 802.16 standards dependent on whether the end item attached to the WLAS is “fixed” or “nomadic.”

- a. Fixed WEIs are those WEIs that access a single WLAS during the session and are not expected to traverse between WLASs so that handoffs are not required. Fixed WEIs may support either 802.16-2009 – Part 16: Air Interface for Fixed Broadband Wireless Access Systems or 802.16-2009 – 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.
- b. Nomadic WEIs are those WEIs that are mobile and may traverse different WLASs during a single session (i.e., handoffs are seamless from the user perspective). Nomadic WEIs must support 802.16-2009 – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, and Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.

7.3.3 Wireless End Instruments

EDG-000340 [Required: WEIs] The following requirements apply.

- a. Wireless VoIP EIs are certified as part of the VoIP solution [i.e., Session Controller (SC)] unless they are wireless Audio End Instruments (AEIs) (Wireless AEIs shall meet all AEI requirements as well as meeting the wireless interface requirements listed in this section).
- b. Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service (see [Figure 7.3-1](#), Access Methods for the Wireless Access Layer End Item Product Telephones). The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or Personal Electronic Device (PED) to connect to the wireless WLAS.



**Figure 7.3-1. Access Methods for the Wireless Access Layer
End Item Product Telephones**

- c. WEIs may use either method separately or a combination to provide wireless access (see [Figure 7.3-1](#), Access Methods for the Wireless Access Layer End Item Product Telephones).
- d. WEIs or soft clients on workstations acting as WEIs shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements.
- e. The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated.
- f. Minimally, all WEIs shall be FIPS 140-2 Level 1 certified.
- g. If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0–60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument.

7.3.4 Wireless LAN Access System

A WLAS implementation is considered to be the replacement of the physical layer of the wired Access Layer of a LAN. A WLAS that is used may range in size from 96 voice IP subscriber services for non-redundant WLAS(s) to more than 96 voice IP subscriber services for a

redundant WLAS(s). Wireless products that support 96 or less voice users are not required to be redundant.

EDG-000350 [Required: WLAS] If a WLAS is used as part of the LAN design supporting VoIP subscribers, the following requirements must be met:

- a. Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary to alternate system. However, it may allow a single momentary 5-second delay in voice bearer traffic in both directions of the wireless link as wireless VoIP telephone clients are re-authenticated to the standby system. The 5-second voice delay will not be factored into the overall Mean Opinion Score (MOS).
- b. The WLAS shall support the following maximum number of EIs per [Table 7.3-2](#), Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., Strategic MOS 4.0, Strategic-to-Tactical MOS 3.6, Tactical-to-Tactical MOS 3.2).

Table 7.3-2. Maximum Number of EIs Allowed per WLAS

WLAN CONVERGENCE TYPE	ACCESS TYPE	WLAS REDUNDANCY	L2/L3 SWITCH LINK(S)	L2/L3 CONNECTION LINK ETHERNET SPEED	MAXIMUM # WIRELESS PHONE SUBSCRIBERS
Non-Converged	Non-Sharing	Non-Redundant	Single	10 Mbps	96
		Redundant	Link Pair	10 Mbps	100
				100 Mbps	1,000
				1 Gbps	10,000
10 Gbps	100,000				
Converged	Shared and/or Dedicated	Non-Redundant	Single	100 Mbps	96
		Redundant	Link Pair	100 Mbps	250
				1 Gbps	2,500
				10 Gbps	25,000
NOTE: This table defines the maximum number of telephones allowed. This number greatly exceeds the expected WLAS capability for maintaining appropriate MOS (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) when all telephones are off-hook simultaneously.					
LEGEND:					
Gbps: Gigabits per second			MOS: Mean Opinion Score		
L2: OSI Layer 2			OSI: Open System Interconnect		
L3: OSI Layer 3			WLAN: Wireless Local Area Network		
Mbps: Megabits per second			WLAS: Wireless LAN Access System		

- c. At the point when voice quality degradation occurs, defined as a MOS score below appropriate levels (i.e., Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2), when all telephones are off-hook simultaneously, this becomes the maximum number of telephones and/or other wireless non-voice end item products that the WLAS can support for the WLAS transmitter coverage distance.
- d. The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone. The source and destination WLAS transmitters involved in the roaming are connected to the same WLAS controller or are otherwise part of the same WLAS.
- e. Minimally, WLAS products shall provide one of the following trunk-side interface (ASLAN network side) rates (other rates and IEEE standards may be provided as optional interfaces):
 - 10 Mbps IAW IEEE 802.3i.
 - 10 Mbps IAW IEEE 802.3j.
 - 100 Mbps IAW IEEE 802.3u.
 - 1000 Mbps IAW IEEE 802.3z.
 - 1000 Mbps IAW IEEE 802.3ab.

7.3.5 Wireless Access Bridge

Wireless access bridges can be used to replace the physical layer of the wired Open System Interconnect (OSI) Layer 2/3 (L2/L3) Access Layer of the ASLAN or non-ASLAN with wireless technology. IEEE 802.11 and/or 802.16 systems can be used to provide a wireless communications link (or bridge) between two or more wired LANs, typically located in adjacent buildings. The WAB functions within the LAN primarily as a wireless NE. The hardware used in a wireless LAN bridge is similar to a WLAS, but instead of connecting only wireless clients to the wired network, bridges are used primarily to connect other wireless LAN bridges to the network. Simultaneously, the WAB may provide connection services to wireless end item products too (i.e., act simultaneously as a WLAS). An example of a combination WLAS/WAB and WAB is provided in [Figure 7.3-2](#), Example of Combined WLAS/WAB and Second Layer WAB [a combination protocol WLAN/WAB (802.11 WLAS with 802.16)].

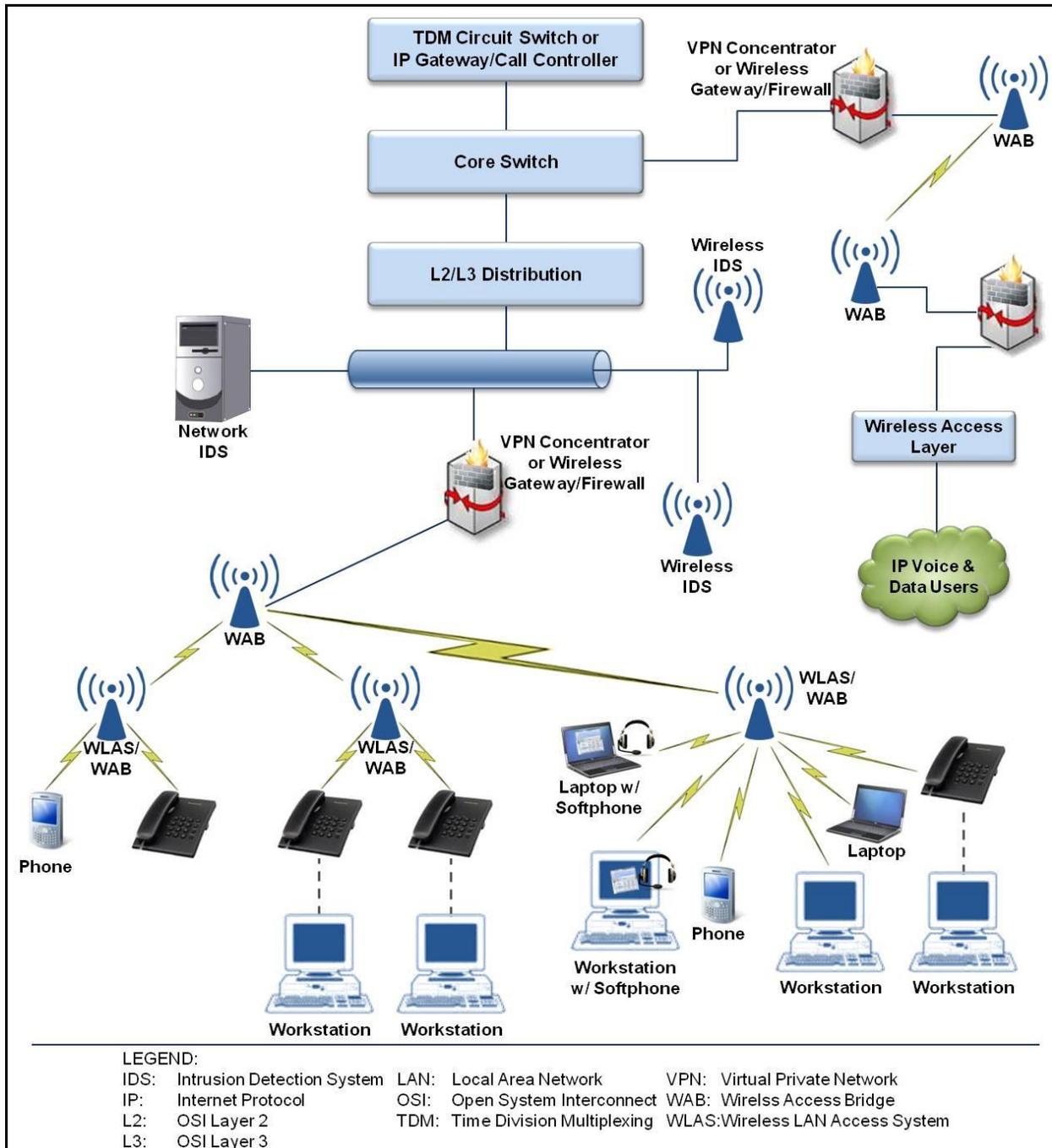


Figure 7.3-2. Example of Combined WLAS/WAB and Second Layer WAB

EDG-000360 [Required: WAB] the WAB will be required to meet all the following requirements for each individual type interface.

- a. The WAB shall minimally provide one wireless interface that serves as the communication path between WAB components. The WAB shall also provide a wired interface to connect to the ASLAN components. Minimally, WAB products shall provide

one of the following wired trunk-side (ASLAN network side) interface rates (other rates and IEEE standards may be provided as optional interfaces):

- 10 Mbps IAW IEEE 802.3i.
- 10 Mbps IAW IEEE 802.3j.
- 100 Mbps IAW IEEE 802.3u.
- 1000 Mbps IAW IEEE 802.3z.
- 1000 Mbps IAW IEEE 802.3ab.

In addition, the WAB must provide one of the following wireless interfaces:

- (1) 802.16 interfaces. If supported, the WAB must support either 802.16d - Part 16: Air Interface for Fixed Broadband Wireless Access Systems, or 802.16e - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, and Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1. The product must support 802.16 QoS specified in [Section 7.3.1](#), General Wireless Product.
 - (2) 802.11 interfaces, the WAB must meet a minimum of one of 802.11 standards (802.11a, b, g, or n). The product must support 802.11 QoS specified in [Section 7.3.1](#).
 - (3) For the wireless interface, vendors may support a pair-wise proprietary wireless technology. The interface must support a QoS mechanism (e.g., DSCP or 802.1 L2 tag (aka 802.1p)) to support assured services transport of prioritized traffic (if congestion or over subscription is possible). The interface must transport and not modify the existing layer 3 DSCP value.
- b. The maximum number of voice calls transported across the WAB shall be in accordance with [Section 7.15.19](#), Traffic Engineering. Maximum voice users will be determined by the smallest link size (i.e., Ethernet connection to the WAB or the WAB wireless link speed of the WAB itself).
 - c. The introduction of WAB(s) shall not cause the End-to-End (E2E) average MOS to fall below appropriate levels (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) as measured over any 5-minute time interval.
 - d. The introduction of WAB(s) shall not exceed the E2E digital Basic Encoding Rule (BER) requirement of less than 1 error in 1×10^{-8} (averaged over a 9-hour period).
 - e. The introduction of WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, 22 January 2009, Section 3.8, DOD Secure Communications Devices (DSCDs).
 - f. The WAB shall transport all call control signals transparently on an E2E basis.

- g. The addition of WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.
- h. The addition of WAB(s) shall not increase the LAN jitter requirements previously specified in this section.

A WAB may simultaneously act as a WLAS.

EDG-000370 [Required: WLAS/WAB] The WLAS/WAB combination must meet all the requirements for access (WLAS) and bridging (WAB).

- a. The WAB(s) and/or WLAS/WAB shall support Service Class tagging/QoS as previously specified in this section.
- b. 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.

7.3.6 Survivability

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures quickly and maintaining the required QoS for existing services.

For the ASLAN, survivability needs to be inherent in the design. The following guidelines are provided for the ASLAN:

- Layer 3 Dynamic Rerouting. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DOD Information Technology (IT) Standards Registry (DISR) to provide survivability. The minimum routing protocols that must be supported are as follows:
 - Border Gateway Protocol (BGP) for inter-domain routing (Required: Core products).
 - Open Shortest Path First (OSPF), Version 2, for IPv4 and OSPF Version 3 for IPv6, July 2008, IAW RFC 5340 (Required: Core and Distribution products).
 - OSPFv2 Graceful restart (RFC 3623) and OSPFv3 Graceful Restart (RFC 5187) are required (18-month rule) for Core and Distribution products. It is not applicable to access devices unless routing (OSPF) provided.
 - Graceful Restart for BGP (RFC 4724) is required (18-month rule) for core and distribution infrastructure products.
- Layer 2 Dynamic Rerouting:
 - Virtual Router Redundancy Protocol (VRRP) – RFCs 2787 and RFC 5798. VRRP is able to provide redundancy to Layer 2 switches that lose connectivity to a Layer 3 router. The Distribution product shall employ VRRP to provide survivability to any product running Layer 2 (normally the Access Layer).

7.4 DIGITAL SUBSCRIBER LINE (DSL)

7.4.1 Introduction

This section includes requirements for using DSL access technologies to link buildings within DOD Bases at UC locations worldwide. This section also describes how newer Ethernet in the First Mile over Copper (EFMCu) access technologies, could be used to link buildings within Bases at these UC locations.

7.4.2 DSL Product

The requirements that follow are specified for the DSL products that implement the DSL operational framework utilized by DISA. The DSL products are categorized into the following types:

- Access Devices.
- Concentrators.
- Repeaters.

7.4.3 Physical Layer

EDG-000380 [Required: Access Devices, Concentrators, Repeaters] DSL products shall provide at least one of the following DSL interface types:

- | | |
|-----------|-----------------------|
| a. ADSL | ITU G.992.1 (G.DMT). |
| b. ADSL | ITU G.992.2 (G.Lite). |
| c. ADSL2 | ITU G.992.3. |
| d. ADSL2+ | ITU G.992.5. |

EDG-000390 [Optional: Access Devices, Concentrators, Repeaters] Access Devices, Concentrators, and Repeaters shall provide the following DSL interface types:

- | | |
|--------------------------|-------------------|
| a. SHDSL | ITU G.991.2. |
| b. VDSL | ITU G.993.1. |
| c. HDSL | ITU G.991.1. |
| d. VDSL2 | ITU G.993.2. |
| e. Long reach 2BASE-TL | IEEE Std 802.3ah. |
| f. Short reach 10PASS-TS | IEEE Std 802.3ah. |

EDG-000400 [Required: Access Devices, Concentrators] DSL products shall provide at least one of the following Ethernet interface types (other types may be provided as optional interfaces):

- a. 10 Mbps IEEE Std 802.3i (10-BaseT Ethernet).
- b. 100 Mbps IEEE Std 802.3u (100-BaseT Fast Ethernet).

EDG-000410 [Optional: Access Devices, Concentrators] DSL products shall also provide at least one of the following Ethernet interface types:

- a. 1000 Mbps IEEE Std 802.3z (1000-Base X Gigabit Ethernet over Fiber-Optic).
- b. 1000 Mbps IEEE Std 802.3ab (1000-Base T Gigabit Ethernet over Twisted Pair).

7.4.4 Data Link Layer

EDG-000420 [Optional: Access Devices, Concentrators] DSL products shall meet at least one of the following DSL bonding capabilities:

- a. Asynchronous Transfer Mode (ATM)-based multi-pair bonding ITU G.998.1.
- b. Ethernet-based multi-pair bonding ITU G.998.2.
- c. Multi-pair bonding using time-division inverse multiplexing ITU G.998.3.
- d. Multilink Point-to-Point Protocol bonding RFC 1990.

EDG-000430 [Required: Access Devices, Concentrators] DSL products shall meet the Ethernet Media Access Control (MAC) capabilities defined in IEEE Std 802.3-2002.

EDG-000440 [Required: Access Devices, Concentrators] DSL products shall meet the Ethernet MAC bridging capabilities defined in IEEE Std 802.1D-2004.

EDG-000450 [Required: Access Devices, Concentrators] DSL products shall meet the Ethernet Virtual Local Area Network (VLAN) capabilities defined in IEEE Std. 802.1Q.

EDG-000460 [Optional: Access Devices, Concentrators] DSL products shall meet the Ethernet in the First Mile bonding requirements specified in IEEE Std 802.3ah.

EDG-000470 [Optional: Access Devices, Concentrators] DSL products shall meet the ATM capabilities defined in International Telecommunications Union (ITU) I.361.

EDG-000480 [Optional: Access Devices, Concentrators] DSL products shall meet the ATM Adaptation Layer 5 (AAL5) capabilities defined in ITU I.363.5.

7.4.5 Network Layer

EDG-000490 [Required: Access Devices, Concentrators] DSL products shall meet all of the IPV4 protocol requirements for UC Access products as listed in [Table 7.2-4](#), Core, Distribution, and Access Product Requirements Summary.

EDG-000500 [Required: Access Devices] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.2-3, UC End Instruments (EI), of Section 5, IPV6.

EDG-000510 [Required: Concentrators] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.2-6, LAN Switch (LS), of Section 5, IPV6.

7.4.6 Information Assurance

EDG-000520 [Required: Access Devices, Concentrators, Repeaters] The Information Assurance requirements are contained in Section 4, Information Assurance.

7.4.7 DSL Support for Analog Voice Services

The following Access Device and Concentrator requirements are based on the Base Configuration Supporting Analog Voice and VoIP using DSL Modems and a Digital Subscriber Line Access Multiplexer (DSLAM). These requirements apply to Analog Voice services, and do not apply to VoIP or Video over IP Services.

EDG-000530 [Optional: Concentrators] If the Concentrator (DSLAM) routes analog voice traffic (or analog voice traffic multiplexed onto a T1) to/from a VoIP Media Gateway and UC SC for voice call completion, the Concentrator's interface to the VoIP Media Gateway shall match the Media Gateway interface requirements in Section 2.14, Media Gateway.

When the Concentrator is a DSLAM that supports analog voice traffic, analog phones can also be supported at the DSL Access Devices (the DSL Modems). In this scenario, the analog voice signal is transmitted together with the digital DSL signal over the DSL copper lines.

EDG-000540 [Optional: Concentrators] If the Concentrator (DSLAM) supports analog voice traffic, the side of the DSLAM that terminates the Voice Grade Copper lines shall use a splitter to separate the analog phone traffic from the digital DSL traffic at each of the lines. In this case, the DSLAM shall also route the analog phone traffic to the point of analog voice distribution [the local VoIP Media Gateway, End Office, or Private Branch Exchange (PBX)] and route the digital DSL traffic to the DSL components within the DSLAM. This DSLAM-based splitter shall also act as a filter to prevent interference between the analog phone service and the DSL IP data service (including VoIP and Video over IP services when they are used).

EDG-000550 [Optional: Access Devices] If the Access Device (DSL Modem) supports an analog phone connection, then the Access Device shall contain a low pass filter that is located between the analog phone line (DSL modem user side) and the DSL line (DSL modem network side). This low pass filter shall prevent interference between the analog phone service and the DSL IP data service (including VoIP and Video over IP services when they are used).

7.4.8 Device Management

EDG-000560 [Required: Access Devices, Concentrators, Repeaters] DSL products shall meet the device management requirements for Management Options, Fault Management, Loopback Capability, and Operational Configuration Restoral, as specified in [Section 7.4.8](#), Device Management.

EDG-000570 [Required: Access Devices, Concentrators, Repeaters] DSL products shall meet the device management requirements that allow network managers to monitor, configure, and control all aspects of the network and observe changes in network status.

EDG-000580 [Required: Access Devices, Concentrators, Repeaters] DSL products shall support the following device management functions that secure access to these devices:

- a. Password-protected user accounts that are either defined for each individual device, or centrally controlled for multiple devices using a Radius server.
- b. Secure Shell (SSH) interfaces that provide encryption, authentication and data integrity.
- c. Graphical User Interface (GUI) applications that can be used for local and remote management of all DSL elements served by the management function.

EDG-000590 [Required: Access Devices, Concentrators, Repeaters] DSL products shall support the Simple Network Management Protocol (SNMP) Version 3 network management protocol and have the ability to send SNMP traps to up to four defined trap destinations. The DSL products shall allow the SNMP agent parameters and trap destinations to be defined on an individual element basis (per Access Device, Concentrator, and Repeater) and on a group-of-elements basis.

7.5 PASSIVE OPTICAL NETWORK (PON) TECHNOLOGY

This section establishes the requirements for the products used in PON technology within ASLAN, Non-ASLAN, and WAN environments.

7.5.1 Definition of PON

Passive Optical Network (PON) is a technology composed of an Optical Line Terminal (OLT), a varying number of Optical Network Units/Terminals (ONUs/ONTs) with fiber optic cable and splitters connecting them. Interface from the backbone network [Network-to-Network Interface (NNI) or Ingress] is provided by the OLT while the user interface [User Network Interface (UNI) or Egress] is provided by the ONT. Typical PON network connectivity is illustrated in [Figure 7.5-1](#), Typical PON Network Connectivity. A PON is a converged transport schema that is designed to carry multiple services such as VoIP, Data, IP Video, and Radio Frequency (RF) Video. Organizations that plan to deploy PON with ONTs on the desktop should be aware that power to the ONT is not provided via the fiber network. Power would be needed provided via

copper (which could be included with fiber in the network cable). Backup power to the desktop could also be provided via other mechanisms.

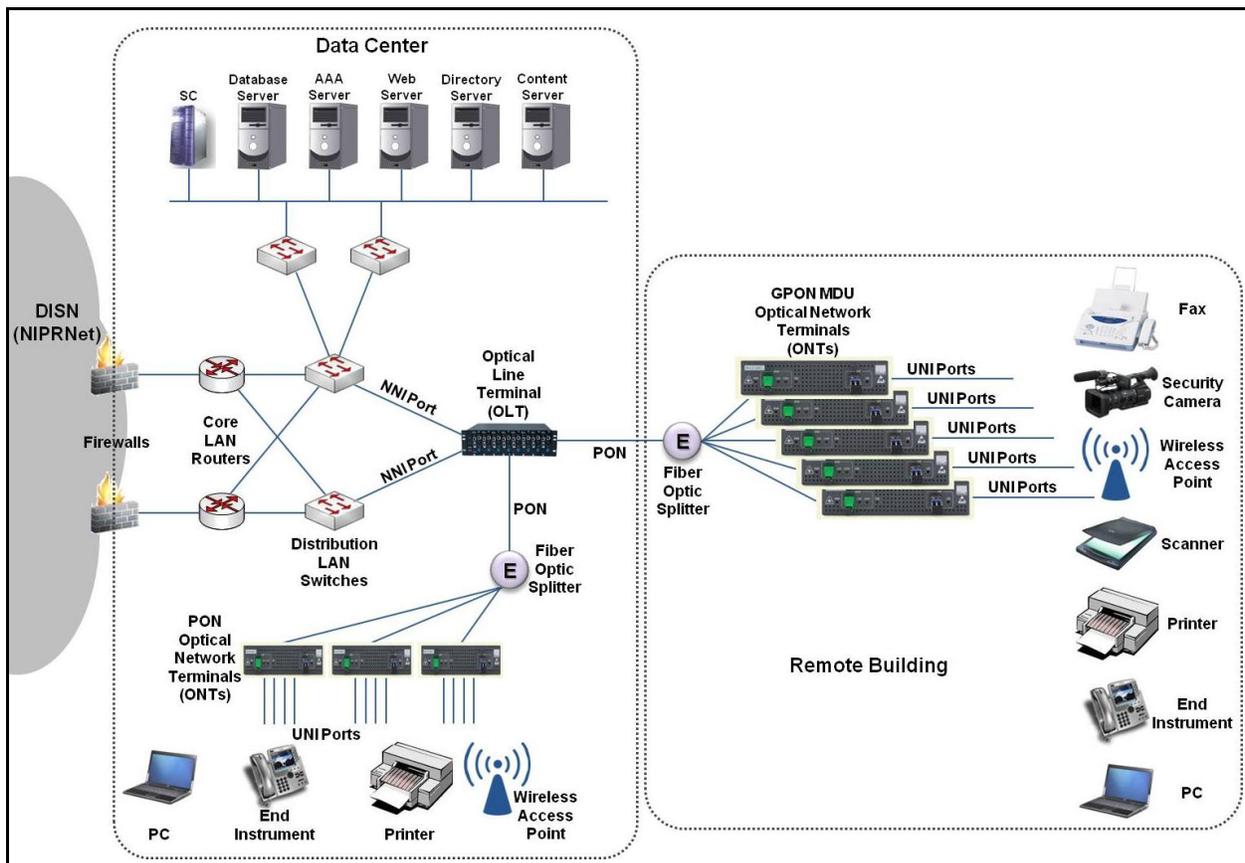


Figure 7.5-1. Typical PON Network Connectivity

The common PON operational framework technologies in use are Ethernet PON (EPON), Broadband PON (BPON) and Gigabit PON (GPON). The first PON technology introduced was BPON. The most current versions are EPON and the newer standard of GPON, which are rapidly replacing the older BPON networks.

BPON conforms to the ITU T G983.1 specification, which includes 622 Mbps download speed with 155 Mbps upload speed per PON port on the OLT. GPON conforms to the ITU T G984.1 and provides bit rates above 1 Gbps. The GPON specification includes 2.4 Gbps download speed with 1.2 Gbps upload speed per PON port. EPON conforms to the IEEE 802.3ah with options for 1/1 Gbps 10/1 Gbps and 10/10 Gbps.

In a PON configuration, downstream signals are broadcast to each end user sharing a fiber. Upstream signals are combined using a multiple access protocol. This allows for two-way traffic on a single fiber optic cable. Bandwidth allocated to each end user from this aggregate bandwidth can be assigned statically or dynamically in order to support voice, data and video applications. It should also be noted that PON technologies may not provide the same data rate in both directions. For example, a typical deployment is to install an ONT in an End User Building

(EUB) attached to a Layer 2 (L2) switch. The ONT will typically be configured to provide 100 Mbps in one direction and 50 Mbps in the other direction and traffic engineering for UC services should utilize the lower number for synchronous services (i.e., VVoIP).

At a high level, a PON consists of a head-end device called an OLT. The OLT may be deployed at the Distribution (e.g., Main Communication Node or Area Distribution Node), and Access (e.g., End User Building) Layers. End user endpoints are equipped with ONTs that provide Ethernet, analog Plain Old Telephone Service (POTS), and even RF video. As many as 64 (and in some cases more) ONTs connect to a PON port via a single, single mode fiber whose optical signals are combined at a passive splitter. A PON utilizes Wavelength Division Multiplexing (WDM), using one wavelength for downstream traffic and another for upstream traffic across one single, single-mode fiber optic cable. The PON specifications provide downstream traffic to be transmitted over a single fiber on the 1490 nanometer (nm) wavelength and upstream traffic to be transmitted at 1310 nm. A third 1550 nm band is allocated for overlay services, in this case, RF (analog) video.

The following figures display two different connectivity solutions utilizing the GPON network operational framework. [Figure 7.5-2](#), PON Connectivity in the DOD operational framework, shows a typical installation utilizing the OLT in the Distribution (ADN) and Access (EUB) Layers of the DOD UC model. [Figure 7.5-3](#), PON Connectivity in a Collapsed DOD Backbone Operational Framework, shows a collapsed backbone where fibre splitters are the only equipment required at the ADN.

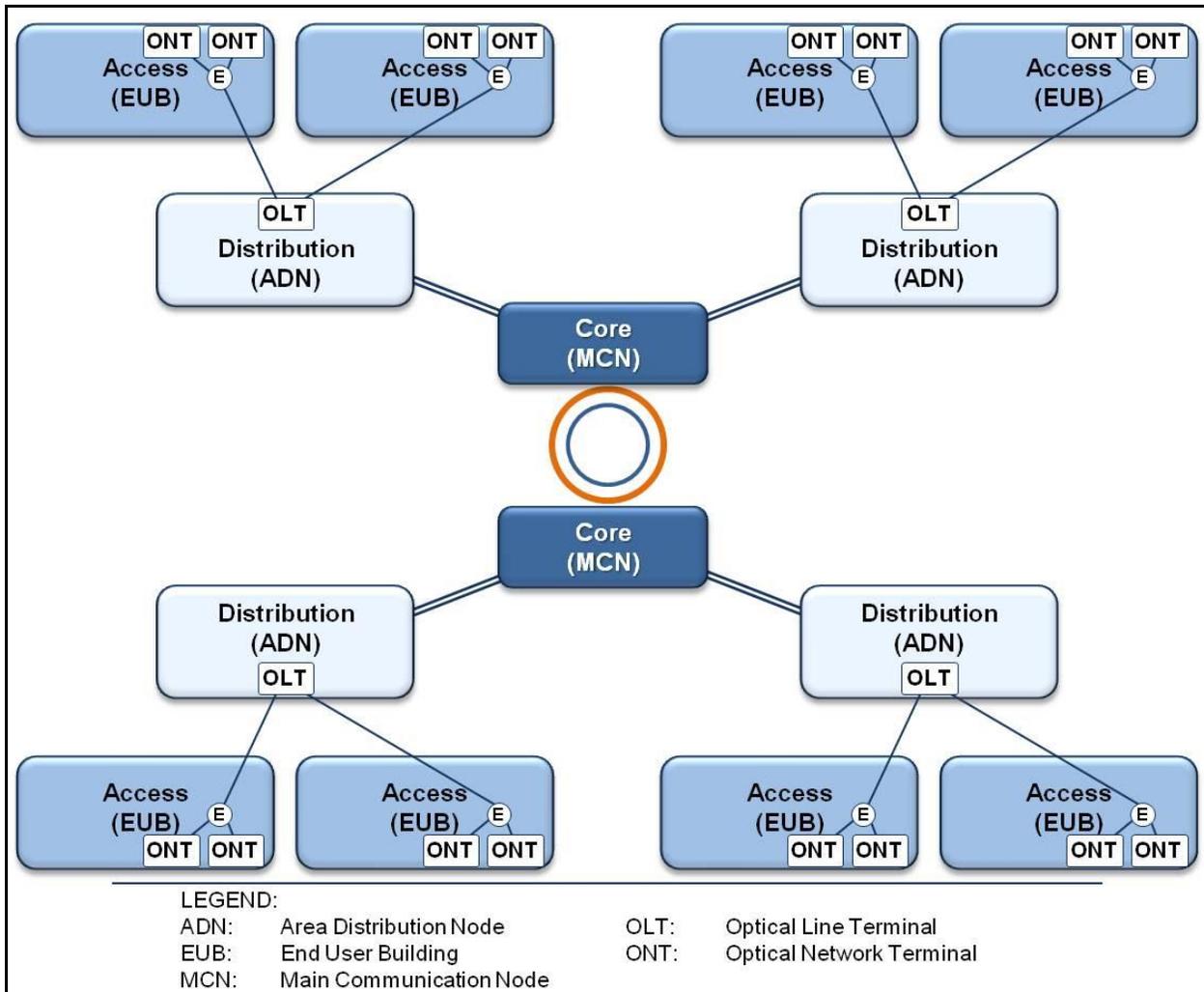


Figure 7.5-2. PON Connectivity in the DOD Operational Framework

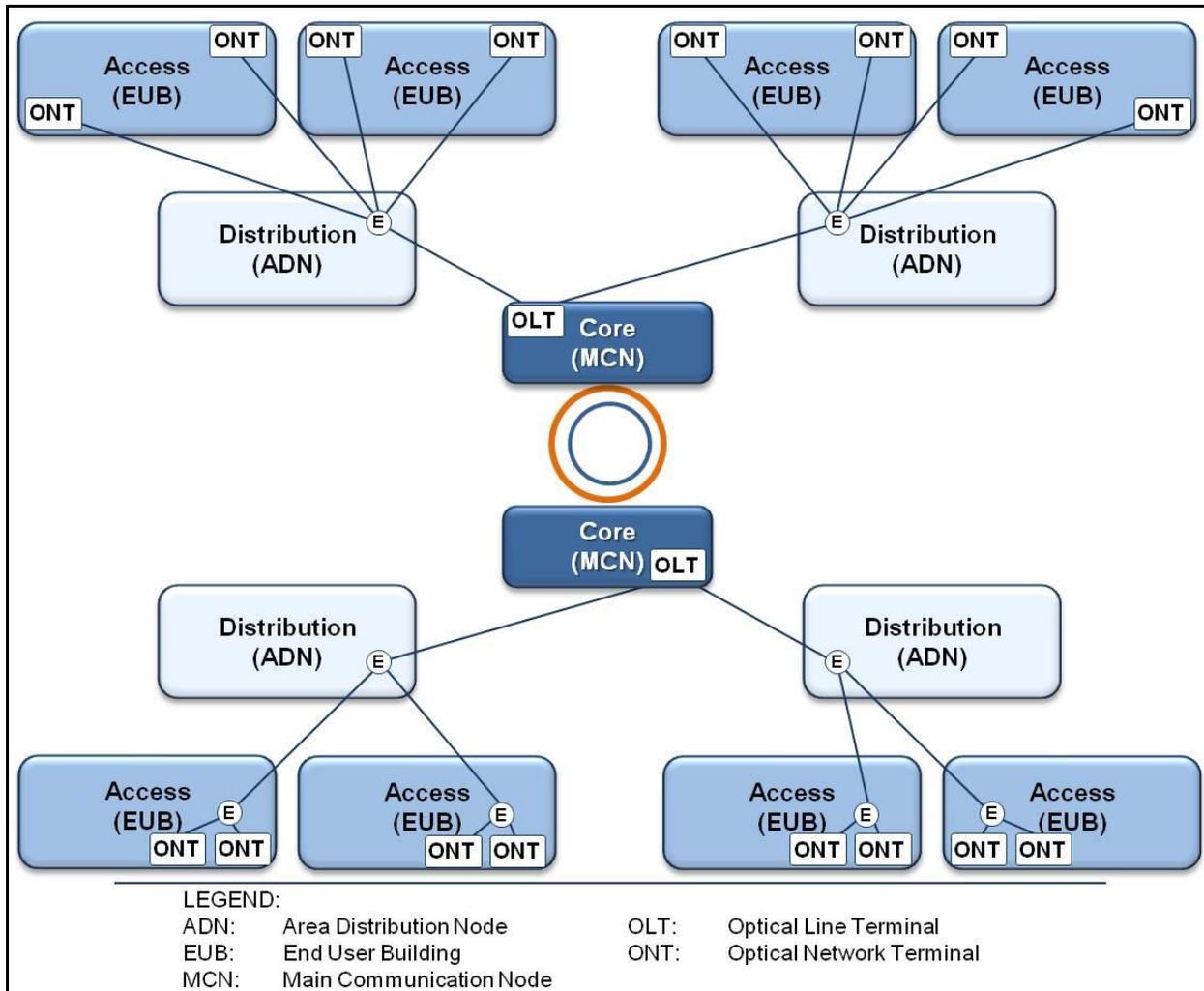


Figure 7.5-3. PON Connectivity in a Collapsed DOD Backbone Operational Framework

7.5.2 Interfaces

PONs can be composed of BPON, EPON, and GPON, and the requirements do not delineate between the different types. The UCR defines four types of interfaces in a typical PON: NNI: Ingress, OLT to ONT (PON), Network Management, and UNI.

7.5.2.1 NNI Interface

EDG-000600 [Required: PON] The NNI interface is composed of the uplink between the OLT and the Core network (LAN or WAN). This interface shall minimally be an IEEE 802.3 interfaces; the SUT may provide a Fibre channel interface IAW ANSI INCITS T11.2 and T11.3 (previously known as X3T9.3).

- a. Minimally, the NNI shall be one of the following interface rates (other rates and IEEE standards may be provided as Optional interfaces):

-
- (1) 100 Mbps IAW IEEE 802.3u.
 - (2) 1000 Mbps IAW IEEE 802.3z.
 - b. The NNI ports shall provide the following parameters on a per port basis as specified:
 - (1) Auto-negotiation IAW IEEE 802.3.
 - (2) Force mode IAW IEEE 802.3.
 - (3) Flow control IAW IEEE 802.3x.
 - (4) Filtering IAW RFC 1812.
 - (5) Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad).
 - (6) Spanning Tree Protocol IAW IEEE 802.1D.
 - (7) Multiple Spanning Tree IAW IEEE 802.1s.
 - (8) Rapid Configuration of Spanning Tree IAW IEEE 802.1w.
 - c. If the Fibre Channel Interface is provided the interface must meet:
 - (1) RFC 4338 Transmission of IPv6, Ipv4 and Address Resolution Protocol (ARP) Packets over Fibre channel.
 - (2) RFC 4044 Fibre Channel Management.

7.5.2.2 OLT to ONT PON Interface

EDG-000610 [Required: PON] The GPON OLT to ONT interface is defined by the ONT Management Control Interface (OMCI) protocol and was standardized and defined by the ITU standard G.984.4. This interface is composed of the PON port on the OLT and the Fiber port on the ONT. Between these ports is a single strand of Single Mode Fiber and one or more optical splitters. Bi directional transmission is accomplished by use of separate wavelengths (1310 nm and 1490 nm) for transmission. The number of splitters is driven by local requirements, and does not exceed the ITU T G.984 specification for fiber loss per PON port between the OLT and ONT. There may be one to 64 (some vendors support more) ONTs on a single PON port. The number of ONTs is driven by the required bandwidth for each user and in accordance with the traffic engineering guidelines in [Section 7.5.19](#), Traffic Engineering. The OLT to ONT interface will support the Telcordia Standards shown in [Table 7.5-1](#), OLT to ONT Signaling Standards.

Table 7.5-1. OLT to ONT Signaling Standards

TELCORDIA STANDARDS:	GR-63-CORE	NEBS Generic Equipment Requirements
	GR-078-CORE	Physical Design and Manufacture Generic Requirements
	GR-199-CORE	Memory Administration Messages
	GR-418-CORE	Generic Reliability Requirements
	GR-472-CORE	Network Element Configuration Management
	GR-474-CORE	Alarm and Control for Network Elements
	GR-499-CORE	Transport System Generic Requirements
	GR-815-CORE	Generic Requirements for NE/NS Security
	GR-831-CORE	Language for Operations Application Messages
	GR-833-CORE	NE and Transport Surveillance Messages
	GR-1093-CORE	Generic State Requirements for Network Elements
	GR-1250-CORE	Generic Requirements for SONET File Transfer
	SR-1665	NMA Operations System Generic Transport NE Interface Support
	TR-NWT-000835	NE and Network System Security Administration Messages
	TR-TSY-000480	User System Interface – Directory for TR-TSY-000824 & 000825
ETSI STANDARDS:	ETSI-300-119-2, ETSI-300-119-3, ETSI-300-119-4	
ANSI STANDARDS:	T1.231, T1.264	
ITU-T STANDARDS:	G.664, G.671, G.681, G.692, G.703, G.704, G.707, G.709, G.775, G.783, G.798, G.806, G.808.1, G.823, G.825, G.831, G.841, G.842, G.871, G.872, G.873, G.874, G.875, G.957, G.958, G.959, G.7710, G.8251, X.721, X.744, M.3100, Q.822	

7.5.2.3 Network Management Interface

EDG-000620 [Required: PON] The GPON products shall support the following network monitoring features:

- a. Simple Network Management Protocol (SNMP) IAW RFCs 1157, 3410, 3411, 3412, 3413, and 3414.
- b. SNMP Traps IAW RFC 1215.
- c. RMON IAW RFC 2819.
- d. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584.
- e. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826.

7.5.2.4 UNI Interface

EDG-000630 [Required: PON] PON products shall provide at least one of the following interface rates:

- a. 10 Mbps IAW IEEE 802.3i.
- b. 100 Mbps IAW IEEE 802.3u.
- c. 1000 Mbps IAW IEEE 802.3z.
- d. 1000 Mbps IAW IEEE 802.3ab.

In addition, PON must support traffic conditioning, which will ensure that the required bandwidth is available for all prioritized traffic.

7.5.2.4.1 UNI Ports

EDG-000640 [Required: PON] The UNI interface shall provide the following parameters on a per port basis as specified:

- a. Auto-negotiation IAW IEEE 802.3.
- b. Force mode IAW IEEE 802.3.
- c. Flow control IAW IEEE 802.3x.
- d. Filtering IAW RFC 1812.
- e. Port-Base Access Control IAW 802.1x.
- f. Link Layer Discover – Media Endpoint Discovery IAW ANSI TIA 1057.

EDG-000650 [Optional: PON] Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad).

EDG-000660 [Optional: PON] The UNI ports may provide the following features parameters on a per port basis as specified:

- a. Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) PoE for Optional Interfaces IEEE 802.3af.
- b. PoE Plus or Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) for Optional Interfaces IEEE 802.3at.

7.5.3 Class of Service Markings

EDG-000670 [Required: PON] The PON network shall comply with access product requirements, [Section 7.2.1.3](#), Class of Service Markings, Class of Service Markings, paragraph 1 (a, b, and c).

7.5.4 Virtual LAN Capabilities

EDG-000680 [Required: PON] The NNI and UNI PON ports shall comply with [Section 7.2.1.4](#), Virtual LAN Capabilities.

7.5.5 Protocols

EDG-000690 [Optional: PON] The PON network shall support bridging at Layer 2 of the OSI model. Bridging will provide for higher survivability as well as reducing traffic congestion on the uplinks to the Distribution or Core Layers of the network. Bridging at Layer 2 will be supported for packets that do not require Layer 3 handling.

7.5.6 Quality of Service Features

EDG-000700 [Required: PON] The PON shall comply with the Access product requirements listed in [Section 7.2.1.6](#), Quality of Service Features. PON products targeted for non-assured services are not subject to the Layer 3 queuing requirements in this section and the conditions of fielding will state whether the PON can support Assured Services or not.

7.5.7 Voice Services

7.5.7.1 Latency

EDG-000710 [Required: PON] The PON shall have the capability to transport prioritized voice IP packets, media, and signaling, with no more than 6 ms latency end-to-end (E2E) across the PON System Under Test (SUT) as measured under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering 25 percent voice/signaling, 25 percent IP video, 25 percent preferred data, and 25 percent best effort traffic). The latency shall be achievable over any 5 minute measured period under congested conditions.

7.5.7.2 Jitter

EDG-000720 [Required: PON] The PON shall have the capability to transport prioritized voice IP packets across the PON SUT with no more than 3 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent IP video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.7.3 Packet Loss

EDG-000730 [Required: PON] The PON shall have the capability to transport prioritized IP packets across the PON SUT with packet loss not to exceed configured traffic engineered

(queuing) parameters. Actual measured packet loss across the PON 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 conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.8 Video Services

7.5.8.1 Latency

EDG-000740 [Required: PON] The PON shall have the capability to transport prioritized video IP packets with no more than 30 ms latency across the PON SUT. Latency is increased over prioritized 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 conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.8.2 Jitter

EDG-000750 [Required: PON] The LAN shall have the capability to transport prioritized video IP packets across the PON SUT with no more than 30 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.8.3 Packet Loss

EDG-000760 [Required: PON] The PON shall have the capability to transport prioritized video IP packets across the PON SUT with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the PON 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 conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.9 Data Services

7.5.9.1 Latency

EDG-000770 [Required: PON] The PON shall have the capability to transport prioritized data IP packets with no more than 45 ms latency across the PON SUT. 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 conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.9.2 Jitter

There are no jitter requirements for preferred data IP packets.

7.5.9.3 Packet Loss

EDG-000780 [Required: PON] The PON shall have the capability to transport prioritized data IP packets across the PON SUT 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 conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic)).

7.5.10 Information Assurance

EDG-000790 [Required: PON] All systems must comply with the applicable Security Technical Implementation Guides (STIGs).

7.5.11 PON Network Management

EDG-000800 [Required: PON] Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. The PON infrastructure components shall have a Network Management (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 Global Information Grid (GIG) management capabilities. The PON infrastructure components must be able to be centrally managed by an overall Network Management System (NMS). In addition, Management Information Base (MIB) II shall be supported for SNMP. In addition, if other methods are used for interfacing between PON products and the NMS, they shall be implemented in a secure manner, such as with the following methods.

7.5.11.1 Secure Shell Version 2

EDG-000810 [Required: PON] Secure Shell version 2 (SSHv2). The PON products shall support RFC 4251 through RFC 4254 inclusive.

7.5.11.2 Telnet

EDG-000820 [Required: PON] The PON product shall be configured by default not to accept Telnet.

7.5.11.3 HTTPS

EDG-000830 [Optional: PON] 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.

7.5.11.4 LAN Products

EDG-000840 [Optional: PON] The LAN products shall support RFC 3414 for SNMP.

7.5.11.5 Other Methods for Interfacing

EDG-000850 [Optional: PON] If other methods are used for interfacing between LAN products and the NMS, they shall be implemented in a secure manner.

7.5.12 Configuration Control

EDG-000860 [Required: PON] 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]. Local area networks 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 within 5 seconds of detecting the event, excluding transport time.

7.5.13 Operational Changes

EDG-000870 [Required: PON] The PON shall meet the requirements in this section.

7.5.14 Performance Monitoring

EDG-000880 [Required: PON] The PON shall meet the requirements in this section.

7.5.15 Alarms

EDG-000890 [Required: PON] The PON shall meet the requirements in this section. In addition to the alarms defined in this section, the OLT shall support the alarms as defined by ITU G994.4.

7.5.16 Reporting

EDG-000900 [Required: PON] The PON shall meet the requirements in this section. In addition, the PON system must also report optical errors to include degraded optical conditions.

7.5.17 Fiber Media

EDG-000910 [Required: PON] Fiber Optic Cable used for the PON shall be Single Mode Fiber. The single mode fiber shall be in compliance with ITU G.652/TIA OS1/International Electrotechnical Commission (IEC) B1.1.

7.5.18 RF-over-Glass (RFoG) Video

EDG-000920 [Optional: PON] The PON network shall support RFoG via PON and its RF overlay framework. ITU-T G.984.5 defines this band as an Enhancement band for video distribution services. This ITU forum also specifies a wavelength of 1150 nm to 1560 nm. This video capacity is in addition to the 2.4Gbps downstream and 1.2 upstream capacity of GPON. It is the responsibility of the ONT to either block or separate the RFoG from the downstream GPON signal of 1480 to 1500 nm.

The spectrum is allocated as follows:

- 40 Analog channels at 54 to 550 Mhz.
- 63 Digital 256 Quadrature Amplitude Modulation (QAM) channels at 225 to 870 Mhz.
- One Quadrature Phase-Shift Keying (QPSK) Out of Band (OOB) channel at 71 to 125 MHz.

7.5.19 Traffic Engineering

EDG-000930 [Required: PON] Bandwidth required per subscriber must be in compliance with the requirements in this section and additional DOD regulations as applicable.

7.5.20 VLAN Design and Configuration

EDG-000940 [Required: PON] VLAN Design and Configuration for all PON networks must be in compliance with Distribution and Access Layer Network Elements as defined in this section.

7.5.21 Power Backup

EDG-000950 [Required: ASLAN Network PON – Optional: Non-ASLAN Network PON] To meet Chairman of the Joint Chiefs of Staff (CJCS) requirements, the PON network must be in compliance with the requirements in this section. Required or Optional adherence shall be based on whether the PON Network Element is being placed into an ASLAN or a Non-ASLAN.

7.5.22 Availability

Availability of a PON network will be determined the same as for active Ethernet networks as defined in this section. PON Network Elements that are utilized in ASLANs and Non-ASLANs must meet the availability requirements for the appropriate LAN.

EDG-000960 [Optional: PON] The PON platform shall support Type B PON Protection as defined in ITU-T G.984.1 3/2008 to provide increased reliability for all services carried on the PON, including data.

7.5.23 Redundancy

The following paragraphs outline the redundancy requirements for the PON Network.

EDG-000970 [Required: PON in ASLAN – Optional: PON in Non-ASLAN] The PON product shall have no single point of failure that can cause an outage of more than 96 IP telephone subscribers. It should be noted that a PON may be used with a single point of failure for more than 96 subscribers if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers).

7.5.23.1 Single Product Redundancy

EDG-000980 [Optional: PON] If redundancy is met through single product, the following requirements are applicable:

- a. Dual Power Supplies. The platform shall provide a minimum of two power inputs each with the power capacity to support the entire chassis. Loss of a single power input shall not cause any loss of ongoing functions within the chassis.
- b. Dual Processors (Control Supervisors). The chassis shall support dual control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls). Failure of the primary processor to secondary must meet 5-second failover without loss of active calls.
- c. Redundancy Protocol. PON equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the PON that could cause an outage to more than 96 IP subscribers. It should be noted that a PON may be used with a single point of failure for more than 96 subscribers if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers). Redundancy protocols will be standards based as specified in this document.
- d. Backplane/Bridging Redundancy. Bridging platforms within the PON shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the OLT.

NOTE: In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds.

7.5.23.2 Dual Product Redundancy

EDG-000990 [Optional: PON] In the case where a secondary product has been added to provide redundancy to a primary product, the failover over to the secondary product must not result in any lost calls. The secondary product may be in “standby mode” or “active mode,” regardless of the mode of operation the traffic engineering of the links between primary and secondary links must meet the requirements provided in [Section 7.5.19](#), Traffic Engineering.

NOTE: In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds.

7.5.24 Survivability

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures and maintaining the required QoS for existing services.

EDG-001000 [Required: PON] For PON Survivability, the PON shall support a Layer 2 Dynamic Rerouting protocol. Failover shall occur in no more than 1 second.

7.5.25 Summary of PON Requirements by Subscriber Mission

EDG-001010 [Required: PON] The PON Network Elements shall meet the same requirements as specified in [Table 7.1-1](#), Summary of LAN Requirements by Subscriber Mission, as applicable for the LAN the Network Element will be included within to include meeting the IPv6 requirements as defined in Section 5, IPv6. The PON shall meet all IPv6 requirements applicable as defined for a LAN access switch (Table 5.2-6, LAN Switch).

7.6 CUSTOMER EDGE ROUTER

7.6.1 Traffic Conditioning

EDG-001020 [Required: CE Router] The product shall be capable of performing traffic conditioning (policing and shaping) on inbound and outbound traffic. This may involve the dropping of excess packets or the delaying of traffic to ensure conformance with SLAs. The product shall meet the requirements for “core” products defined within [Section 7.5.6](#), Quality of Service Features.

EDG-001030 [Required: CE Router] The product shall be capable of traffic conditioning the bandwidth associated with a service class.

7.6.2 Differentiated Services Support

EDG-001040 [Required: CE Router] The product shall be capable of supporting DS IAW RFCs 2475 and 2474 as specified in [Section 7.5.3](#), Class of Service Markings.

7.6.3 Per-Hop Behavior Support

EDG-001050 [Required: CE Router] The product shall be capable of supporting the PHBs. The CE-R shall meet “core” behavior requirements are defined in [Section 7.5.6](#), Quality of Service Features.

NOTE: The product shall be capable of supporting EF PHBs IAW RFC 3246.

EDG-001060 [Required: CE Router] The product shall be capable of supporting the AF PHB IAW RFC 2597.

7.6.4 Interface to the SC/SS for Traffic Conditioning

EDG-001070 [Optional: CE Router] The CE-R shall be capable of interfacing to the SC/SS in real time to adjust traffic conditioning parameters based on the updated SC/SS budgets.

NOTE: For example, if the SC budget decreases from ten Voice sessions to five Voice sessions, then the traffic conditioning parameters should change from 10 x 110 equals 1100 kbps to 5 x 110 equals 550 kbps in both directions. Initially, the process will be a manual process to configure the PHB allocations statically. This assumes that traffic conditioning occurs before applying the PHBs.

7.6.5 Interface to the SC/SS for Bandwidth Allocation

EDG-001080 [Optional: CE Router] The product shall be capable of interfacing to the SC/SS in real time to adjust the PHB bandwidth allocations based on the updated SC/SS budgets.

NOTE: For example, if the SC budget decreases from ten Voice sessions to five Voice sessions, then the EF queue bandwidth allocation should change from 10 x 110 equals 1100 kbps to 5 x 110 equals 550 kbps in both directions. Initially, the process will be a manual process to configure the PHB allocations statically. This assumes that traffic conditioning occurs before applying the PHBs.

7.6.6 Network Management

EDG-001090 [Required: CE Router] The product shall support Fault, Configuration, Accounting, Performance, and Security (FCAPS) Network Management functions as defined in the Section 2.17, Management of Network Appliances, in this document.

7.6.7 Availability

The four types of CE-Rs are High Availability, Medium Availability without System Quality Factors (SQFs), Medium Availability with SQF, and Low Availability. Defining four types of CE-Rs is driven by cost factors, and the availability that can be provided by commercial off-the-shelf (COTS) products.

Locations serving F/FO users and I/P users and R users with PRIORITY and above precedence service should install High Availability CE-Rs. The Medium Availability (two types) and Low Availability CE-R provide a cost-effective solution for locations that serve R users.

EDG-001100 [Required: High Availability CE Router] The product shall have an availability of 99.999 percent, including scheduled hardware and software maintenance (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors, in this document.

EDG-001110 [Required: Medium Availability CE Router Without SQF] The product shall have an availability of 99.99 percent, including scheduled hardware and software maintenance (non-availability of no more than 52.5 minutes per year). The product does not need to meet the requirements specified in Section 2.8.2, Product Quality Factors.

EDG-001120 [Optional: Medium Availability CE Router With SQF] The product shall have an availability of 99.99 percent, including scheduled hardware and software maintenance (non-availability of no more than 52.5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors.

EDG-001130 [Optional: Low Availability CE Router] The product shall have an availability of 99.9 percent, including scheduled hardware and software maintenance (non-availability of no more than 8.76 hours per year). The product does not need to meet the requirements specified in Section 2.8.2, Product Quality Factors.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

7.6.8 Packet Transit Time

EDG-001140 [Required: CE Router] The CE-R shall meet the following requirements:

- a. The CE-R shall be non-blocking (see [Section 7.2.1](#), General LAN Switch and Router Product, for definitions and conditions.)
- b. The CE-R shall meet the latency requirements for “core” products specified in [Section 7.2.1](#).
- c. The CE-R shall meet the Jitter requirements specified for “core” products in [Section 7.2.1](#).

- d. The CE-R shall meet the packet loss requirements specified for “core” products in [Section 7.2.1](#).

This transit time shall be in addition to the serialization delay for voice packets as measured from the input interface to output interface under congested conditions (as described in [Section 7.5.7.1](#), Latency) to include all internal functions. For example, the serialization delay of a 100BT Interface is 0.017 ms, which would allow for a voice packet 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.

7.6.9 Customer Edge Router Interfaces and Throughput Support

The CE-R supports an ASLAN-side connection to the Session Border Controller (SBC) and a WAN-side connection to the Defense Information Systems Network (DISN) WAN.

EDG-001150 [Required: CE Router] The ASLAN-side interface shall be an Ethernet interface (10 BT, 100 BT, [Optional] 1 Gigabit Ethernet, or [Optional] 10GbE) full duplex, and at least one of the WAN-side interfaces shall be an Ethernet interface (10 BT, 100BT, [Optional] 1 Gigabit Ethernet, or [Optional] 10GbE) full duplex.

EDG-001160 [Optional: CE Router] The WAN-side access connection interface can also be Time Division Multiplexing (TDM) based (i.e., DS1, DS3, or E1). These are all full-duplex interfaces, and support two-way simultaneous information exchange at the “line rate” for the interface (i.e., 1.5 Mbps for DS1, 45 Mbps for DS3, 2.0 Mbps for E1).

EDG-001170 [Optional: CE Router] The WAN-side access connection interface can also be Synchronous Optical Network (SONET) based (i.e., OC-x; e.g., OC3, OC12, OC48 or OC192). These are all full-duplex interfaces, and support two-way simultaneous information exchange at the “line rate” for the interface.

The CE-R needs to support information “throughput” in two directions: from the ASLAN side to the WAN side, and from the WAN side to the ASLAN side. The CE-R also needs to support this throughput in full-duplex mode, which means that the CE-R needs to support the maximum possible throughput on the WAN-side interface for packets sent in the ASLAN-to-WAN direction. At the same time, the CE-R needs to support the maximum possible throughput on the WAN-side interface for packets sent in the WAN-to-ASLAN direction. The maximum possible throughput for an interface is the maximum line rate for that interface, as provisioned on the CE-R.

A CE-R may support multiple interfaces on the ASLAN side, such as two 100 BTs to an SBC and a data firewall, and on the WAN side, such as two DS1s to two different DISN SDNs. These requirements assume that the CE-R only has one WAN-side interface active. They also assume that the line rate for the WAN-side interface is less than or equal to the sum of the line rates for the ASLAN-side interfaces.

EDG-001180 [Required: CE Router] The CE-R shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the ASLAN-to-WAN direction.

EDG-001190 [Required: CE Router] The CE-R shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the WAN-to-ASLAN direction.

EDG-001200 [Required: CE Router] The CE-R shall support the maximum possible throughput on the WAN side interface in a full-duplex mode, for a full traffic load of UC packets sent simultaneously in both the ASLAN-to-WAN and WAN-to-ASLAN directions.

EDG-001210 [Required: CE Router] The Maximum Possible Throughput (MPT) on the WAN-side interface shall be the maximum line rate that the WAN-side interface is provisioned for on the CE-R. The following MPTs shall apply for the different WAN-side interfaces:

- a. 10 BT: 10 Mbps.
- b. 100 BT: 100 Mbps.
- c. 1 Gigabit Ethernet: 1 Gbps [Optional].
- d. 10 Gigabit Ethernet: 10 Gbps [Optional].
- e. DS1: 1.5 Mbps [Optional].
- f. DS3: 45 Mbps [Optional].
- g. E1: 2.0 Mbps [Optional].
- h. OC3: 155 Mbps [Optional].
- i. OC12: 622 Mbps [Optional].
- j. OC48: 2.5 Gbps [Optional].
- k. OC192: 9.6 Gbps [Optional].

These MPTs may not be attainable on some interfaces on some products. If a vendor cannot meet one of the MPTs listed, they should identify the actual MPT that their product supports. If this actual MPT depends on frame size, the vendor should document how the frame size should be used to calculate the actual MPT.

EDG-001220 [Required] The CE-R must minimally support the following routing protocols:

- a. LAN-side interfaces must support OSPF IAW RFCs 2328, 2740, 3623, 5187, and 5340.
- b. WAN-side interfaces shall support BGP IAW RFCs 1772, 2439, 4271, and 4760. The CE-R shall support both external BGP (eBGP) and internal BGP (IBGP). The CE router shall support route reflectors (RFC 4456) and confederations (RFC 5065).

EDG-001230 [Required] The CE-R must meet the IA requirements specified for Router “R.”

EDG-001240 [Required] The CE-R must meet the IPv6 Requirements in Section 5 specified for Router “R.”

7.6.10 Deployable (Tactical) Customer Edge Router

The requirements in this section apply to both a Deployable (Tactical) CE-R and a fixed (strategic) CE-R.

EDG-001250 [Required: Deployable (Tactical) CE Router, Fixed (Strategic) CE Router]

Within an ASLAN, Deployable (Tactical) or Fixed (Strategic), all inbound packets that enter the CE-R from outside of the LAN, and that are marked with the DSCP Assured Service values associated with the Granular Service Classes of Assured Voice and Assured Multimedia Conferencing per Tables 6.3-2, Traffic Conditioning Specification, and 6.3-3, Four-Queue PHB Approach, must be routed to the SBC.