Changes to UCR 2008, Change 2, made by UCR 2008, Change 3 for Section 5.3.1, ASLAN Requirements

SECTION	CORRECTION OR NEW REQUIREMENTS	EFFECTIVE DATE
5.3.1.3 (para 1)	Clarified blocking factor definition	Immediate
5.3.1.3 (para 2.c)	Deleted preferred data latency metric.	Immediate
5.3.1.3.1	Changed 802.11n data rate from 600 Mbps to 300-600 Mbps	Immediate
5.3.1.3.2	Added Power over Ethernet Requirements	18-months
5.3.1.3.3	Clarified Class of service markings	Immediate
5.3.1.3.5	Clarified RFC requirements in Table 5.3.1-4	Immediate
5.3.1.3.6	Clarified use of queuing to support blocking factors	Immediate
5.3.1.3.7	Updated to reflect SNMPv3	18 Months
5.3.1.3.9	Updated Spanning Tree to Rapid Spanning Tree	Immediate
5.3.1.3.9	Updated Table 5.3.1-5 terminology	Immediate
5.3.1.4.1	Updated parameters for queuing (reduced)	Immediate
5.3.1.4.2	Updated parameters for queuing (reduced)	Immediate
5.3.1.4.3	Updated parameters for queuing (reduced)	Immediate
5.3.1.5	Changed terminology	Immediate
5.3.1.6	Changed terminology	Immediate
5.3.1.7.2	Added Wi-Fi Multimedia (WMM) certification	18 Months
5.3.1.7.5	Clarified use of emergency power system as opposed to uninterruptible power system.	Immediate
5.3.1.7.9	Survivability – routing protocol changed to minimally support OSPF	Immediate
5.3.1.8.4.2.3	Added MPLS QoS	Immediate
5.3.1.9	New Requirements: Digital Subscriber Line	Immediate
5.3.1.10	New Requirements: Passive Optical Network	Immediate

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

5.3 IP-BASED CAPABILITIES AND FEATURES

This section and its subsections describe requirements for IP-based UC products to be certified for use in the DISN in support of UC. Requirements for IP-based products are spread across several subsections of this document. As an example illustrated by Table 5.3-1, Illustration of how EBC Requirements are defined Across Multiple UCR Sections, requirements for an EBC are specified in Sections 5.3.2, Assured Services Requirements; 5.3.4, AS-SIP Requirements; 5.3.5, IPv6 Requirements; and 5.4, Information Assurance Requirements.

Table 5.3-1. Illustration of how EBC Requirements are defined across Multiple UCR Sections

APL PRODUCT: EBC	
Requirement Category	**UCR Section**
Assured Services	5.3.2
AS-SIP	5.3.4
IPv6	5.3.5
Information Assurance	5.4

Section 5.3.1, Assured Services Local Area Network Infrastructure, defines basic requirements for LAN products and design guidance for an ASLAN, while Information Assurance requirements applicable to LAN products are found in Section 5.4, Information Assurance Requirements; Internet Protocol version 6 (IPv6) requirements for each ASLAN product type are found in Section 5.3.5, IPv6 Requirements.

Section 5.3.2, Assured Services Requirements, defines requirements for assured services. Assured services are provided by replacing the current TDM-based MLPP functionality with IP-based ASLANs, ASAC, and AS-SIP signaling. The assured services requirements, which must be met by the LSC, MFSS, EBC, CE Router, together with ASLAN and the E2E network infrastructure, make up the total system required to initiate, supervise, and terminate voice and video sessions with precedence and preemption on an EI-to-EI basis, while functioning within a converged total DoD GIG network.

Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, defines E2E performance requirements for the GIG network infrastructure. The GIG E2E is defined in terms of three network segments referred to as Customer Edge, Network Edge, and Network Core Segments. The Core Segment DISN WAN consists of hundreds of worldwide service delivery nodes (SDNs) interconnected by a highly robust, bandwidth-rich, optical fiber, cross-connected core with gigabit routers (i.e., DISN Core).

Section 5.3.4, AS-SIP Requirements, defines requirements for the AS-SIP. The AS-SIP is critical to provide assured services from EI to EI across the IP-based infrastructure.

The following sections use terms such as "appliance functions" and UC products to be tested for APL certification. The term "appliance function" is introduced because IP-based APL products will often consist of software functions and features (e.g., appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a TDM-based APL product, such as an EO, consists of a single unit containing all required functions. Appliances operate at the signaling, bearer, and NM planes. Appliance functions are described or referred to throughout this document, but are not considered products for APL certification, rather as functions and features that form parts of the UC APL products requirements defined in this document.

The concept of appliance functions and APL products categories are illustrated in Table 5.3-2, Partial Listing of Appliances and UC APL Products, which provides a partial listing of appliance functions and UC APL Products.

Table 5.3-2. Partial Listing of Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
End Instrument	Appliance	Appliance part of LSC
AS-SIP End Instrument	APL Product	System consisting of a single appliance
Media Gateway	Appliance	Appliance function performing media conversion as part of the LSC , WAN SS, and MFSS, and in-band signaling conversion
Signaling Gateway	Appliance	Appliance function performing signaling conversion between CCS7 and AS-SIP as part of the LSC, WAN SS, and MFSS
AS-SIP Signaling Appliance	Appliance	Appliance function within an LSC, WAN SS, and MFSS that provides AS-SIP signaling capabilities
Call Connection Agent	Appliance	Appliance function within an LSC, WAN SS, and MFSS that performs parts of session control and signaling functions
Registrar	Appliance	Appliance function that stores the location of a registrant and its profile
Registrant	Appliance	An appliance that is used to register with the network to seek and gain authority to invoke services or resources from the network
Secure End Instrument	APL Product	An APL product providing secure UC bearer service
Local Session Controller	APL Product	An APL product providing many local voice and video session control functions and features
Multifunction Softswitch	APL Product	Large, complex APL product providing many local and WAN-related session controls and signaling functions

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
WAN Softswitch	APL Product	An APL product that acts an AS-SIP B2BUA within the UC Operational Framework
Edge Boundary Controller	APL Product	An APL product providing firewall functions
Customer Edge Router	APL Product	An APL product providing routing functions at the customer enclave boundary
DISN WAN Access Device M13 Multiplexer	APL Product	An APL product performing multiplexing of T1 carriers to T3 carriers
DISN WAN Access Device Multi-Service Provisioning Platform	APL Product	An APL product providing the interface point to the DISN WAN for all customer legacy point-to-point services
DISN WAN Router (Aggregation, Provider, Provider Edge Router)	APL Product	An APL Products performing routing of IP packets in the DISN WAN
DISN Optical Switch	APL Product	An APL product serving as an optical transport node
Access IP Product	APL Product	ASLAN Infrastructure Product
Distribution IP Product	APL Product	ASLAN Infrastructure Product
Core IP Product	APL Product	ASLAN Infrastructure Product
Wireless Access System (WLAS)	APL Product	A LAN product that provides wireless access
Wireless Access Bridge (WAB)	APL Product	A LAN product that provides wireless transport
Wireless End Instrument (WEI)	Appliance/APL Product	Certified in conjunction with MFSS or LSC
DSL	APL Product	ASLAN Infrastructure Product
PON	APL Product	ASLAN Infrastructure Product

LEGEND

APL	Approved Products List	GEI	Generic End Instrument
ASLAN	Assured Services Local Area Network	LAN	Local Area Network
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller
B2BUA	Back-to-Back User Agent	MFSS	Multifunction Softswitch
CCS7	Common Channel Signaling No. 7	WAN	Wide Area Network
DISN	Defense Information System Network		

THIS PAGE INTENTIONALLY LEFT BLANK

5.3.1 Assured Services Local Area Network Infrastructure

5.3.1.1 Introduction

This section establishes the requirements for the products used in Local Area Networks (LANs), both for Assured Services (AS) and non-AS, to support FO/F, I/P, R and non-mission critical IP-based communication services. The requirements, which are based on commercial standards, were developed to ensure availability of assured services capabilities to users.

This section has two main purposes:

1. Define Product Requirements. Specifies the required and optional capabilities for network products that can be used in a LAN. This section is intended to support equipment certification.

2. Design Guidance. Provides design guidance for an ASLAN to meet its mission needs; provides introductory guidance on issues, such as traffic engineering for performance (to ensure that an ASLAN can support the planned traffic and surges), availability (i.e., through high-reliability components and redundant components with automatic component failover), E2E performance requirements, and system administration and management.

5.3.1.1.1 IP Network Segments and LAN Nomenclature

Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, describes the E2E network infrastructure as consisting of three network segments. The network segments are the Customer Edge, Network Edge, and Network Core. Figure 5.3.1-1, GIG End-to-End IP Network Infrastructure Segments, provides a high-level overview of the three-segment network infrastructure.

The Customer Edge Segment may consist of a single LAN or a Campus Area Network (CAN), or it may be implemented as a Metropolitan Area Network (MAN) in certain locations. "The boundary for the Customer Edge Segment is the CE Router. At Base/Post/Camp/Station (B/P/C/S) that support a Combatant Command (CC), VVoIP traffic associated with the CC will be routed through a CC owned Tier 1 CE router, directly to DISA SDN PE routers. Other traffic on the B/P/C/S will be routed through the CE router owned by the B/P/C/S. The Customer Edge Segment is connected to the Network Core Segment by the Network Edge Segment, which is a traffic-engineered bandwidth (IP connection) that connects the CE Router to an SDN. Detailed descriptions of the network segments and connection arrangements at an SDN are provided in Section 5.3.3.1, End-to-End Network Infrastructure Description.

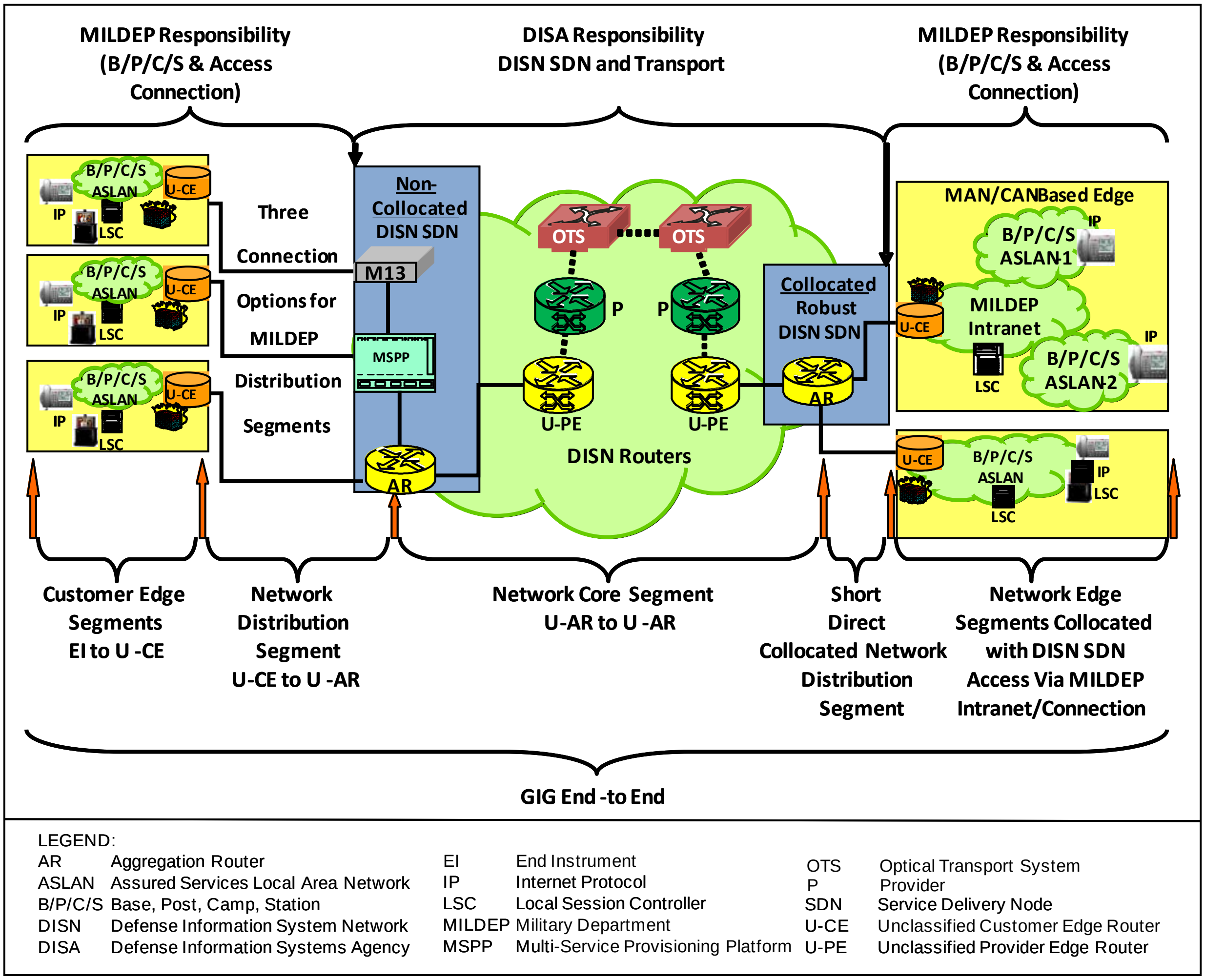


Figure 5.3.1-1. GIG End-to-End IP Network Infrastructure Segments

The LAN consists of the Core, Distribution, and Access Layers, which all reside in the Customer Edge Segment of the E2E GIG network reference. A high-level illustration of the three LAN Layers is provided in Figure 5.3.1-2, B/P/C/S LAN Layers and Relationship to Customer Edge Segment. The figure depicts a traditional three tier LAN infrastructure. This is not to be interpreted that all LANs must be comprised of three tiers. The C/P/S LAN infrastructure may contain more or less tiers based on network engineering frameworks. The C/P/S LAN infrastructure must be composed from approved APL products. The number of tiers and composition (core, distribution, or access) is left to the discretion of the services.

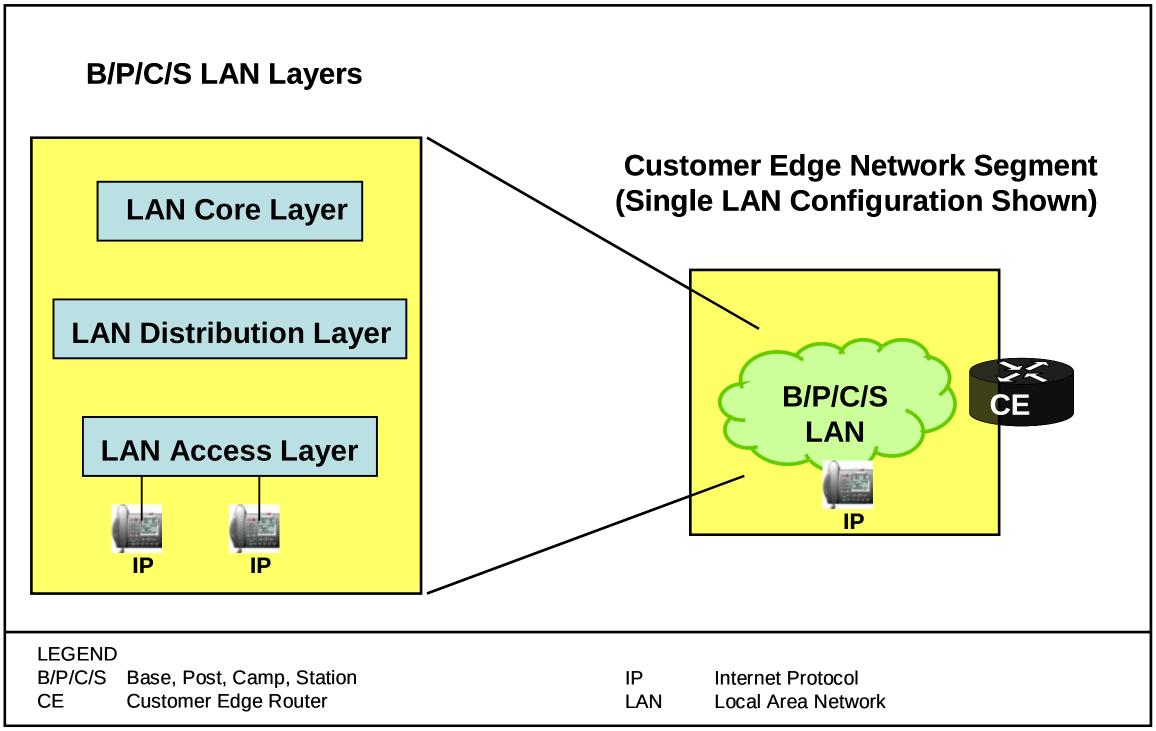


Figure 5.3.1-2. B/P/C/S LAN Layers and Relationship to Customer Edge Network Segment

5.3.1.2 Overview of LAN General Design and Requirements

To provide cost-effective LAN solutions that meet mission requirements for all users served by a LAN, two types of LANs are defined; they are ASLANs and non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs. The ASLANs and non-ASLANs may be designed to use any combination of the layers and functional capabilities, shown in Figure 5.3.1-3, LAN Layers. Multiple layers may be combined in a single switch or router (i.e., router acts as Distribution and Access Layers).

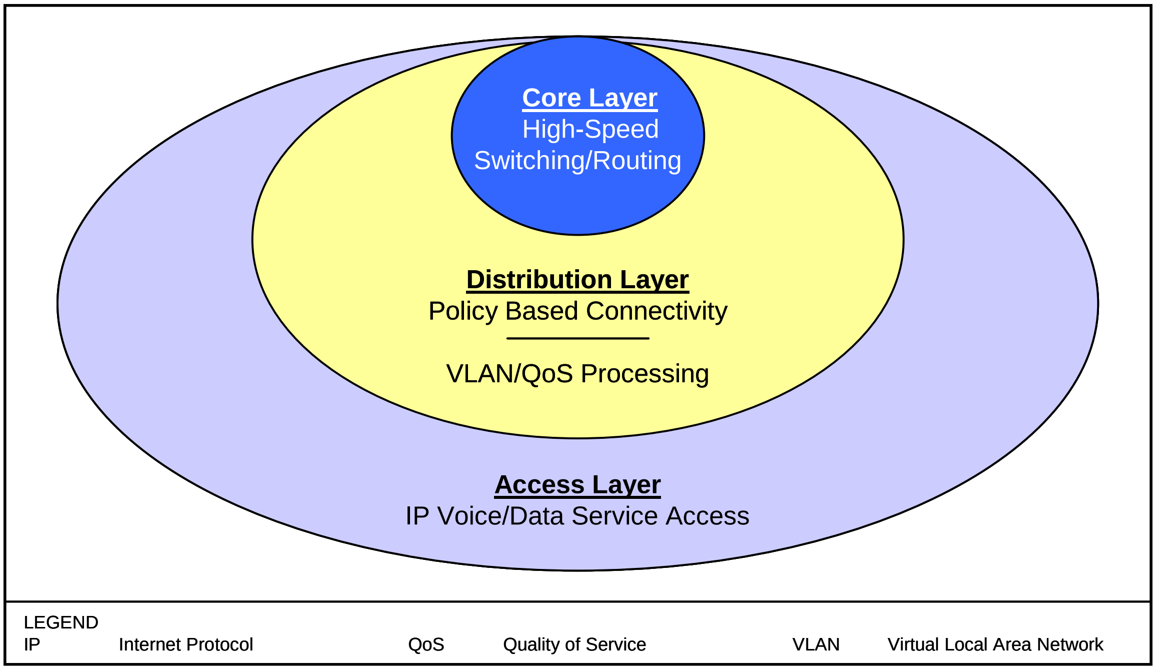


Figure 5.3.1-3. LAN Layers

The three LAN Layers are as follows:

1. Access Layer. The Access Layer is the point at which local end users are allowed into the network. This layer may use access lists or filters to optimize further the needs of a particular set of users.

2. Distribution Layer. The Distribution Layer of the network is the demarcation point between the Access and Core Layers and helps to define and differentiate the Core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.

3. Core Layer. The Core Layer is a high-speed switching backbone and is designed to switch packets as fast as possible.

Figure 5.3.1.4, Representative B/P/C/S Design and Terminology, illustrates a typical B/P/C/S LAN design. The LAN design and requirements refer to LAN products in terms of the Core, Distribution, and Access Layer products. These products are often known by other names such as Main Communication Node (MCN), Area Distribution Node (ADN), and End User Building (EUB) switch.

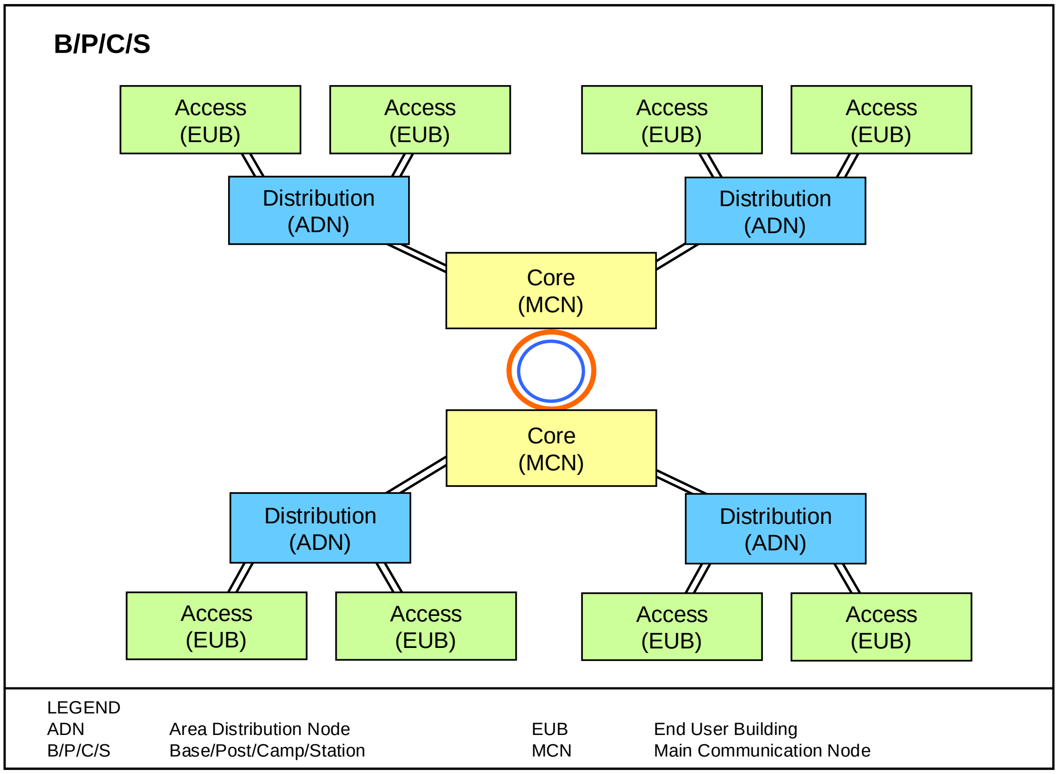


Figure 5.3.1-4. Representative B/P/C/S Design and Terminology

Within the LAN, the terminology used to reference traffic at each specific Open Systems Interconnect (OSI) layer is shown in Table 5.3.1-1, OSI Layer Control Information Name.

Table 5.3.1-1. OSI Layer Control Information Name

OSI LAYER	CONTROL INFORMATION NAME
Application Presentation Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit
LEGEND OSI Open Systems Interconnect	

5.3.1.2.1 LAN Types and Mission Support Summary

The LAN requirements are driven primarily by the types of users they support. To provide cost-effective LAN solutions that meet mission requirements, two types of LANs have been defined: the ASLAN and the non-ASLAN. Within the ASLAN type, there are two categories: high availability ASLANs and medium availability ASLANs. Table 5.3.1-2, Summary of LAN Types by Subscriber Mission, outlines the types of LANs that may support voice and video traffic by subscriber mission categories. ASLAN requirements can be met by using wireless systems in concert with wired service. The combined infrastructure, wired and wireless, must meet the appropriate level of redundancy for ASLAN High, Medium, and Low.

Table 5.3.1-2. Summary of LAN Types by Subscriber Mission

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	FO/F ORIGINATION	I/P ORIGINATION	R ONLY	NON-MISSION CRITICAL
ASLAN High	R	P	P	P
ASLAN Medium	NP	P	P	P
Non-ASLAN	NP	NP	P	P
MLPP	R	R	R	NR
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Power Backup	8 hours	2 hours	NR	NR
Single Point of Failure user > 96 allowed	No	No	Yes	Yes
LAN GOS p=	0.0	0.0	0.0	N/A
Availability	99.999	99.997	99.9	99.9

LEGEND

ASLAN	Assured Services LAN	N/A	Not Applicable
FO/F	Flash Override/Flash	NP	Not Permitted
I/P	Immediate/Priority	NR	Not Required
GOS	Grade of Service	p	Probability of Blocking
LAN	Local Area Network	P	Permitted
MLPP	Multilevel Precedence and Preemption	R	Required

5.3.1.3 General Performance Parameters

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

1. Non-blocking. All Core, Distribution, and Access products shall be non-blocking for its 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 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).

_____NOTE: These definitions/requirements are not applicable for wireless products; wireless products are half-duplex IAW radio limitations. Access requirements for Wireless products are contained within Section 5.3.1.7, Engineering Requirements.

   a. Access Products. Access products shall not have a blocking factor that exceeds 8 to 1. This blocking factor includes all hardware and software components.

b. Distribution and Core Products. These products shall not have a blocking factor that exceeds 2 to 1. This blocking factor includes all hardware and software components.

2. 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.

   a. Voice/Signaling packets. No more than 2 milliseconds (ms) latency.
   b. Video Packets. No more than 10 ms latency.
   c. Preferred Data Packets. NA.
   d. Best Effort Data. NA.

3. 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.

   a. Voice Packets. No more than 1 ms jitter.
   b. Video Packets. No more than 10 ms jitter.
   c. Preferred Data Packets. NA.
   d. Best Effort Data. NA.

4. 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.

   a. 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.

   b. Video 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 0.05 percent for Access, Distribution, and Core products.

   c. Preferred Data 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 0.05 percent for Access, Distribution, and Core products.

5.3.1.3.1 Port Interface Rates

[Required: Core and Distribution Products] Minimally, Core and Distribution products shall support the following interface rates (other rates and IEEE standards may be provided as conditional 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 RFC 2330 and RFC 5136.

- 100 megabits per second (Mbps) in accordance with (IAW) IEEE 802.3u
- 1000 Mbps IAW IEEE 802.3z

[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 conditional 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

[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 conditional interfaces):

- 100 Mbps IAW IEEE 802.3u
- 1000 Mbps IAW IEEE 802.3z

[Conditional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide a fiber channel interface IAW ANSI International Committee for Information Technology Standards (INCITS) T11.2 and T11.3 (previously known as X3T9.3). If provided the interface must meet:

- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fiber Channel; and

- RFC 4044 Fiber Channel Management

[Conditional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide the following wireless LAN interface rates:

- 54 Mbps IAW IEEE 802.11a

- 11 Mbps IAW IEEE 802.11b
- 54 Mbps IAW IEEE 802.11g
- 300–600 Mbps IAW IEEE 802.11n
- IEEE 802.16 – Broadband wireless communications standards for MANs

[Conditional] If any of the above wireless interfaces are provided, the interfaces must support the requirements of Section 5.3.1.7.2, Wireless.

5.3.1.3.2 Port Parameter Requirements

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

- Auto-negotiation IAW IEEE 802.3
- Force mode IAW IEEE 802.3
- Flow control IAW IEEE 802.3x (Conditional: Core)
- Filtering IAW RFC 1812
- Link Aggregation IAW IEEE 802.1AX (applies to output/egress trunk-side ports only)
- Spanning Tree Protocol IAW IEEE 802.1D (Conditional: Core)
- Multiple Spanning Tree IAW IEEE 802.1s (Conditional: Core)
- Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w (Conditional: Core)
- Port-Based Access Control IAW IEEE 802.1x (Conditional: Core)
- Link Layer Discovery Protocol (LLDP) IAW IEEE 802.1AB (Conditional Core and Distribution)
- Link Layer Discovery- Media Endpoint Discovery IAW ANSI/TIA-1057 (Conditional Core and Distribution)
- Power over Ethernet IAW either 802.3af-2003 or 802.3at-2009

5.3.1.3.3 Class of Service Markings

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

1. 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 5.3.1.3.6, Quality of Service Features.

2. 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 5.3.3.3.2, Differentiated Service Code Point. (Conditional: Access products)

3. The Core, Distribution, and Access products must be able to support the prioritization of aggregate service classes with queuing according to Section 5.3.1.3.6, Quality of Service Features.

[Conditional: 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 5.3.1-5, IEEE 802.1Q Tagged Frame for Ethernet, and Table 5.3.1-6, TCI Field Description). Default values are provided in Table 5.3.1-3, 802.1Q Default Values. If provided, the following Class of Service (CoS) requirements apply:

1. 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 5.3.1.3.6, Quality of Service Features.

2. 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) (Conditional: Distribution and Access).

Table 5.3.1-3. 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 Signaling[1]	110	6
	Circuit Emulation[1]	110	6
	Short messages[1]	110	6
	Voice[2]	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

NOTES
1. 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.
2. 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
CoS Class of Service
OA&M Operations, Administration, and Maintenance
SNMP Simple Network Management Protocol
SysLog System Log
TCI Tag Control Information
VTC Video Teleconferencing

5.3.1.3.4 Virtual LAN Capabilities

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

1. Accepting VLAN tagged frames according to IEEE 802.1Q (see Figure 5.3.1-5, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 5.3.1-6, TCI Field Description).

2. Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095).

3. Supporting VLANs types IAW IEEE 802.1Q.

5.3.1.3.5 Protocols

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet protocol requirements for IPv4 and IPv6. Request for Comment (RFC) requirements are listed below in Table 5.3.1-4, ASLAN Infrastructure RFC Requirements. Additional IPv6 requirements by product profile are listed in Section 5.3.5. These RFCs are not meant to conflict with DoD IA policy (e.g., STIGs). Wherever a conflict occurs, DoD IA policy takes precedence. If there are conflicts between 5.3.5, RFCs applicable to IPv6, Section 5.3.5 takes precedence.

Table 5.3.1-4. ASLAN Infrastructure RFC Requirements

Title	RFC	C	D	A	Wireless
OSI IS-IS for routing in TCP/IP and dual environments	RFC 1195	C	C	C	NA
ICMP (PING)	RFC 1256	R	R	R	R
NTP (v3)	RFC 1305	R	R	R	R
PPP Internet Protocol Control Protocol (IPCP)	RFC 1332	C	C	C	C
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 (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
ISO Transport	RFC 2126	C	C	C	C
DHCP	RFC 2131	C	C	C	C
DHCP and BOOTP	RFC 2132	C	C	C	C
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
OSPFv2	RFC 2328	R	R	C	C
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
X.509 Internet PKI OCSP	RFC 2560	R[1]	R[1]	R[1]	R[1]
TCP Congestion Control	RFC 2581	R	R	R	R
AF 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

Title	RFC	C	D	A	Wireless
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	C	C	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
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
Graceful Restart for BGP	RFC 4724	C	C	C	C
MIB (OSPF V2)	RFC 4750	R	R	C	NA
OSPFv3 Graceful Restart	RFC 5187	C	C	C	C
RFC 5556 "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement"	RFC 5556	C	C	C	C
NOTES: 1. If there are any conflicts between the RFC and the implementation of DoD PKI requirements, DoD PKI requirements take higher priority.					

BYTES								
7	**1**	**6**	**6**	**2**	**2**	**2**	**42-1496**	**4**
Preamble	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

NOTE: The TCI field includes user priority, CFI, and VLAN ID.

LEGEND

CFI	Canonical Format Indicator	SFD	Start Delimiter Frame
CRC	Cyclic Redundancy Check	TCI	Tag Control Information
DA	Destination Address	TPID	Tag Protocol Identification
SA	Source Address	VLAN	Virtual Local Area Network

Figure 5.3.1-5. IEEE 802.1Q Tagged Frame for Ethernet

BITS		
3	**1**	**12**
User Priority	CFI	VID

NOTES
1. **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.
2. **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.
3. **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	Virtual Identification
QoS	Quality of Service	VLAN	Virtual Local Area Network

Figure 5.3.1-6. TCI Field Description

5.3.1.3.6 Quality of Service Features

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

1. Providing a minimum of four queues (see Figure 5.3.1-7, Four-Queue Design).

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

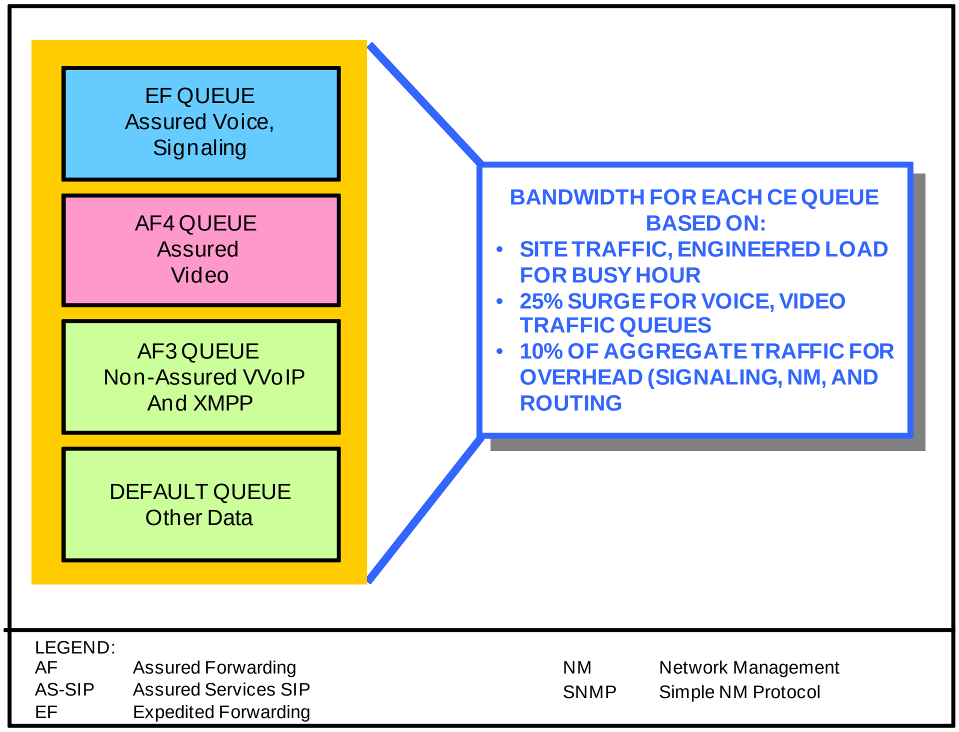


Figure 5.3.1-7. Four-Queue Design

3. Supporting Differentiated Services (DiffServ) per hop behaviors (PHBs) and traffic conditioning IAW RFCs 2474, 2597, 3140, and 3246.

   a. Expedited Forwarding (EF)
   b. Assured Forwarding (AF)
   c. Best Effort (BE)
   d. Class Selector (CS)
   e. PHB Identification Codes

4. 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.

5. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 5.3.3.3.4 as follows:

   a. 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.

b. 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.

c. Access devices have been engineered for a blocking factor of 8:1 or less. Prioritization of traffic 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 100Mbps), 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 3 priority queues should be set up not to exceed 12.5 percent of the egress link capacity.

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

5.3.1.3.7 Network Monitoring

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

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

5.3.1.3.8 Security

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet the security protocol requirements listed in Section 5.4, Information Assurance Requirements 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, WLASs and WABs shall meet all IA requirements for LAN switches (LS). Wireless End Instruments (WEIs) shall meet all IA requirements annotated for EI. Where conflicts exist between the UCR and STIG requirements, the STIG requirements will take precedence.

5.3.1.3.9 Product Requirements Summary

Table 5.3.1-5, Core, Distribution, and Access Product Requirements Summary, summarizes product requirements.

Table 5.3.1-5. 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	R[1]
	10Base-FX	IEEE802.3j	C	C	R[1]
	100Base-TX	IEEE 802.3u	R[1]	R[1]	R[1]
	100Base-FX	IEEE 802.3u	R[1]	R[1]	R[1]
	1000Base-TX	IEEE 802.3ab	C	C	R[1]
	1000Base-X	IEEE 802.3z	R	R	R[1]
	10GBase-X	IEEE 802.3ae, 802.3ak, 802.3an, 802.3aq, 802.3av	C	C	C
	40GBase-X	IEEE 802.3ba	C	C	C
	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
	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

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
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 5.3.1.3.5	R	R	R
IPv6 Protocols	IPv6 features	Section 5.3.5	R	R	R
QoS	DiffServ 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	C[3]	C[3]	C[3]
	CQ	RFC 3670	C[3]	C[3]	C[3]
	PQ	RFC 1046	C[3]	C[3]	C[3]
	CB-WFQ	RFC 3366	C[3]	C[3]	C[3]
Security	Security requirements are contained in the IA portion of the document.		R	R	R

NOTES
1. Product need only provide one of the specified interfaces.
2. Only between end-user and product, not trunks.
3. One of these queuing mechanisms is required to implement EF PHB.

LEGEND

C	Conditional	MAC	Media Access Control
CB-WFQ	Class-Based Weighted Fair Queuing	PHB	Per Hop Behavior
CoS	Class of Service	PQ	Priority Queuing
CQ	Custom Queuing	R	Required
DiffServ	Differentiated Services	RFC	Request for Comment
DISR	DoD Information Technology Standards Registry	RMON	Remote Monitoring
EF	Expedited Forwarding	RTS	Real Time Services
EIA	Electronics Industries Alliance	TIA	Telecommunications Industry Association
FIFO	First-in First-out	UTP	Unshielded Twisted Pair
IEEE	Institute of Electrical and Electronic Engineers Inc.	VLAN	Virtual LAN
IPv4	IP Version 4	WFQ	Weighted Fair Queuing
IPv6	IP Version 6		

5.3.1.4 End-to-End Performance Requirements

End-to-end performance across a LAN is measured from the traffic ingress point (typically, the LAN Access product input port) to the traffic egress port (typically, the LAN Core product port connection to the CE Router).

5.3.1.4.1 Voice Services

5.3.1.4.1.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets, media and signaling, with no more than 6 ms latency E2E across the network as measured under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering. The latency shall be achievable over any 5-minute measured period under congested conditions.

5.3.1.4.1.2 Jitter

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets E2E across the network with no more than 3 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

5.3.1.4.1.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets E2E across the network with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the network shall not exceed 0.045 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

5.3.1.4.2 Video Services

5.3.1.4.2.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets with no more than 30 ms latency E2E across the network. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for video). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

5.3.1.4.2.2 Jitter

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets E2E with no more than 30 ms of jitter across the network. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

5.3.1.4.2.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets E2E with packet loss not to exceed configured traffic engineered (queuing) parameters across the network. Actual measured packet loss across the network shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.3 Data Services

5.3.1.4.3.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets with no more than 45 ms latency E2E across the network. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for data). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.3.2 Jitter

There are no jitter requirements for preferred data IP packets.

5.3.1.4.3.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets E2E with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the LAN shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute period measured under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering.

5.3.1.5 Information Assurance Requirements

[Required: ASLAN and Non-ASLAN] All infrastructure components must be IA certified to be placed on the APL. The IA requirements are contained in Section 5.4, Information Assurance Requirements.

5.3.1.6 Infrastructure Network Management Requirements

[Required: ASLAN and Non-ASLAN] Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. The infrastructure components shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/ reconfiguration of objects that have existing DoD GIG management capabilities. The infrastructure components must be able to be centrally managed by an overall network management system (NMS). In addition, both NMS (RMON2) and (MIB II) shall be supported for SNMP. In addition, if other methods are used for interfacing between infrastructure products and the NMS they shall be implemented in a secure manner, such as with the following methods:

1. Secure Shell 2 (SSH2). The SSH2 Protocol shall be used instead of Telnet due to its increased security. The LAN products shall support RFC 4251 through RFC 4254 inclusive.

2. HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HTTP due to its increased security as described in RFC 2660. The infrastructure products shall support RFC 2818.

5.3.1.6.1 Configuration Control

[Required: ASLAN and Non-ASLAN] Configuration Control identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (DoD CIO Guidance IA6-8510 IA). Infrastructure components shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD GIG management capabilities. The NMS shall report configuration change events in near-real-time (NRT), whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. Near real time is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.1.6.2 Operational Changes

[Required: ASLAN and Non-ASLAN] Infrastructure components must provide metrics to the NMS to allow them to make decisions on managing the network. Network management systems shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). Near real time is defined as within 5 seconds of detecting the event, excluding transport time. Specific metrics are defined in NMS Sections 5.3.2.17, Management of Network Appliances, and 5.3.2.18, Network Management Requirements of Appliance Functions.

5.3.1.6.3 Performance Monitoring

[Required: ASLAN and Non-ASLAN] All infrastructure components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. An NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) within 5 seconds of detecting the event, excluding transport. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.

5.3.1.6.4 Alarms

[Required: ASLAN and Non-ASLAN] All infrastructure components shall be capable of providing SNMP alarm indications to an NMS. Network Management Systems will have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving. This capability allows network managers to monitor and maintain the situational awareness of the network's manageable products automatically, and to become aware of network problems as they occur based on the trouble tickets generated automatically by the affected object or network. Alarms will be correlated to eliminate those that are duplicate or false, initiate test, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. Near real time is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.1.6.5 Reporting

[Required: ASLAN and Non-ASLAN] To accomplish GIG E2E situational awareness, an NMS will have the NM capability of automatically generating and providing an integrated/ correlated presentation of network and all associated networks.

5.3.1.7 Engineering Requirements

5.3.1.7.1 Copper Media

[Required: ASLAN and Non-ASLAN] Cabling used for the LAN shall not be lower than a CAT-5 performance (see Table 5.3.1-6, Cable Grade Capabilities). The CAT-5 cable specification is rated up to 100 megahertz (MHz) and meets the requirement for high-speed LAN technologies, such as Fast Ethernet and Gigabit Ethernet. The Electronics Industry Association/Telecommunications Industry Association (EIA/TIA) formed this cable standard that describes performance the LAN manager can expect from a strand of twisted pair copper cable. Along with this specification, the committee formed the EIA/TIA-568-B standard named the "Commercial Building Telecommunications Cabling Standard" to help network managers install a cabling system that would operate using common LAN types, like Fast Ethernet. The specification defines Near End Crosstalk (NEXT) and attenuation limits between connectors in a wall plate to the equipment in the closet. Wires used for interconnecting LANs using DSL Access Devices and DSL Concentrators (see Section 5.3.1.9, DSL Requirements) should not be lower than a CAT3 performance (also see Table 5.3.1.6, Cable Grade Capabilities). Actual implementations depend upon existing wiring infrastructure.

Table 5.3.1-6. Cable Grade Capabilities

CABLE NAME	MAKEUP	FREQUENCY SUPPORT	DATA RATE	ASLAN COMPATIBILITY
CAT-3	1 twisted pair of copper wire–terminated by RJ11 connectors	16 MHz	Up to 10 Mbps	DSL (see Section 5.3.1.9, DSL Requirements),
CAT-4	2 twisted pairs of copper wire –terminated by RJ45 connectors	20 MHz	Up to 16 Mbps	DSL (see Section 5.3.1.9, DSL Requirements),
CAT-5	4 twisted pairs of copper wire –terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	1000Base-T, 100Base-TX, 10Base-T
CAT-5e	4 twisted pairs of copper wire –terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	10Base-T, 100Base-TX, 1000Base-T
CAT-6	4 twisted pairs of copper wire –terminated by RJ45 connectors	250 MHz	1000 Mbps	10Base-T, 100Base-TX, 1000Base-T

LEGEND

ATM	Asynchronous Transfer Mode	Mbps	Megabits per second	T	Ethernet half-duplex
Base	Baseband	MHz	Megahertz	TX	Ethernet full-duplex
CAT	Category	RJ	Registered Jack		

5.3.1.7.2 Wireless

[Conditional: ASLANs or Non-ASLANs] 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.

5.3.1.7.2.1 General Wireless Product Requirements

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

1. 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.

2. 802.11 wireless products must be WiFi Alliance Certified and shall be certified at the Enterprise level for WPA2. The products will also be Wi-Fi multimedia (WMM) certified.

3. Wireless networks may support I/P, R, and non-mission critical users, but shall not be used to support FO/F users.

4. 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 either:

    a. 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 less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers).

    b. 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.

5. 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:

a. 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.

b. FIPS 140-2, Level 2. Wireless components can be operated in an open public area such as an "open hallway," but recommend the use of a "limited access, secure room" if available and/or operationally feasible.

6. 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.

7. The wireless products shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type:

a. 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.

b. 802.16 Interfaces. Wireless products using 802.16d and/or 802.16e, QoS/Service Class tagging shall meet the following requirements:

(1) The WLAN products may use 802.16 services to provide QoS over the wireless portion of the transport. Services associated with the granular service class are listed in Table 5.3.1-6, Cable Grade Capabilities.

(2) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPs (see Table 5.3.1-7, 802.16 Service Scheduling).

Table 5.3.1-7. 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	NA	NA	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	OA&M	Operations, Administration and Management
DSCP	Differentiated Services Code Point	NA	Not Applicable
ertPS	Extended Real-Time Polling Service	rtPS	Real-Time Polling Service
LAN	Local Area Network	UGS	Unsolicited Grant Service
NA	Not Applicable	VTC	Video Teleconferencing
nrtPS	Non-Real Time Polling Service		

8. Wireless products shall meet the security requirements as stipulated in the Wireless Security Technical Implementation Guide (STIG) and the following specified requirements:

   a. All 802.11 wireless components shall:

      (1) Use the Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP). It will be implemented in 802.11i system encryption modules.

      (2) Implement the Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi Protected Access (WPA2).

9. Wireless access systems shall meet previously stated requirements for access products.

10. Wireless systems shall use the Control and Provisioning of Wireless Access Points (CAPWAP) Protocol IAW RFC 5415 and RFC 5416.

5.3.1.7.2.2 Reserved

5.3.1.7.2.3 Wireless Interface Requirements

[Required: WEI and WLAS]

1. 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

2. 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.

3. 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.

4. 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.

5.3.1.7.2.4 Wireless End Instruments

[Required: WEIs] If WEIs are used, the following requirements will apply.

1. Wireless VoIP EIs are certified as part of the VoIP solution.

2. 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 5.3.1-8, 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 Equipment Product (PED) to connect to the wireless WLAS.

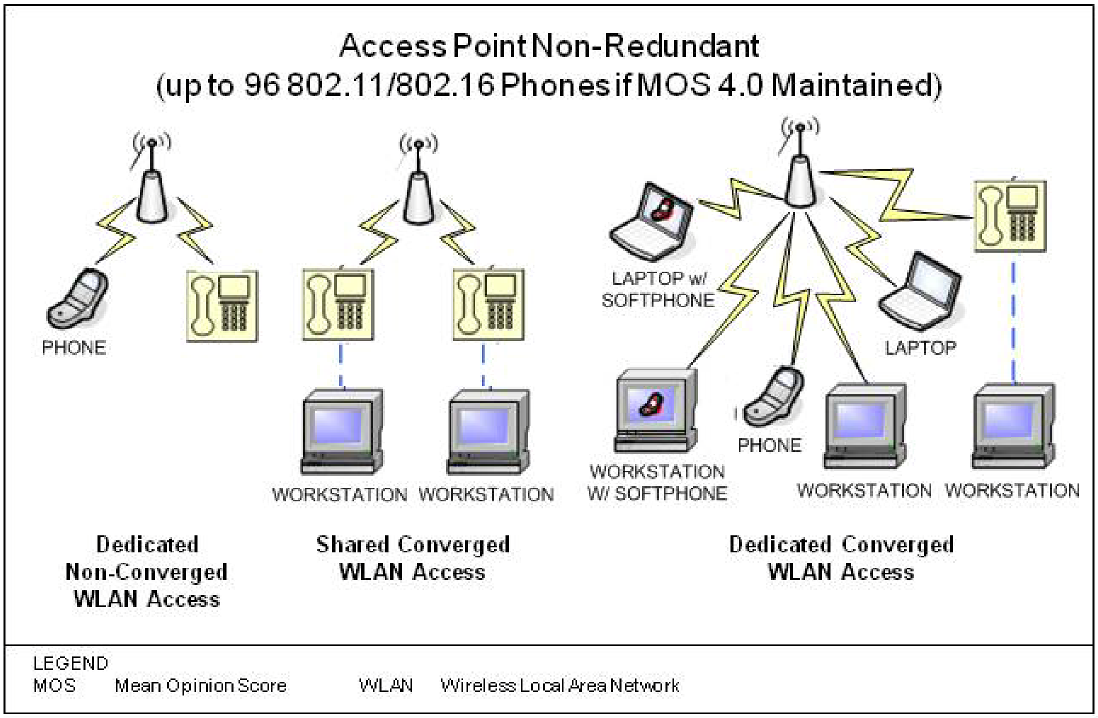


Figure 5.3.1-8. Access Methods for the Wireless Access Layer End Item Product Telephones

3. WEIs may use either method separately or a combination to provide wireless access (see Figure 5.3.1-8, Access Methods for the Wireless Access Layer End Item Product Telephones).

4. 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.

5. 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.

6. Minimally, all WEIs shall be FIPS 140-2 Level 1 certified.

7. 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.

5.3.1.7.2.5 Wireless LAN Access System Requirements

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.

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

1. 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 MOS score.

2. The WLAS shall support the following maximum number of EIs per Table 5.3.1-8, 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).

3. 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.

4. 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.

5. 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 conditional 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

Table 5.3.1-8. 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

5.3.1.7.2.6 Wireless Access Bridge

Wireless access bridges can be used to replace the physical layer of the wired 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 5.3.1-9, Example of Combined WLAS/WAB and Second Layer WAB (a combination protocol WLAN/WAB (802.11 WLAS with 802.16)).

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

1. 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 conditional 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:

a. 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 sub-paragraph 7.b of Section 5.3.1.7.2.1.

b. 802.11 interfaces, the WAB must meet a minimum of one of 802.11standards (802.11a, b, g, or n). The product must support 802.11 QoS specified in sub-paragraph 7.a of Section 5.3.1.7.2.1.

c. 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.

2. The maximum number of voice calls transported across the WAB shall be in accordance with Section 5.3.1.7.3, 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).

3. The introduction of a WAB(s) shall not cause the 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.

4. The introduction of a WAB(s) shall not exceed the E2E digital BER requirement of less than 1 error in $1x10^{-8}$ (averaged over a 9-hour period).

5. The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, 22 January 2009, Section 5.2.12.6, DoD Secure Communications Devices (DSCDs).

6. The WAB shall transport all call control signals transparently on an E2E basis.

7. The addition of a 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.

8. The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section.

A WAB may simultaneously act as a WLAS.

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

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

2. The WABs may support FO/F calls, I/PR, and non-mission critical calls. All calls must meet other specified performance requirements for these users.

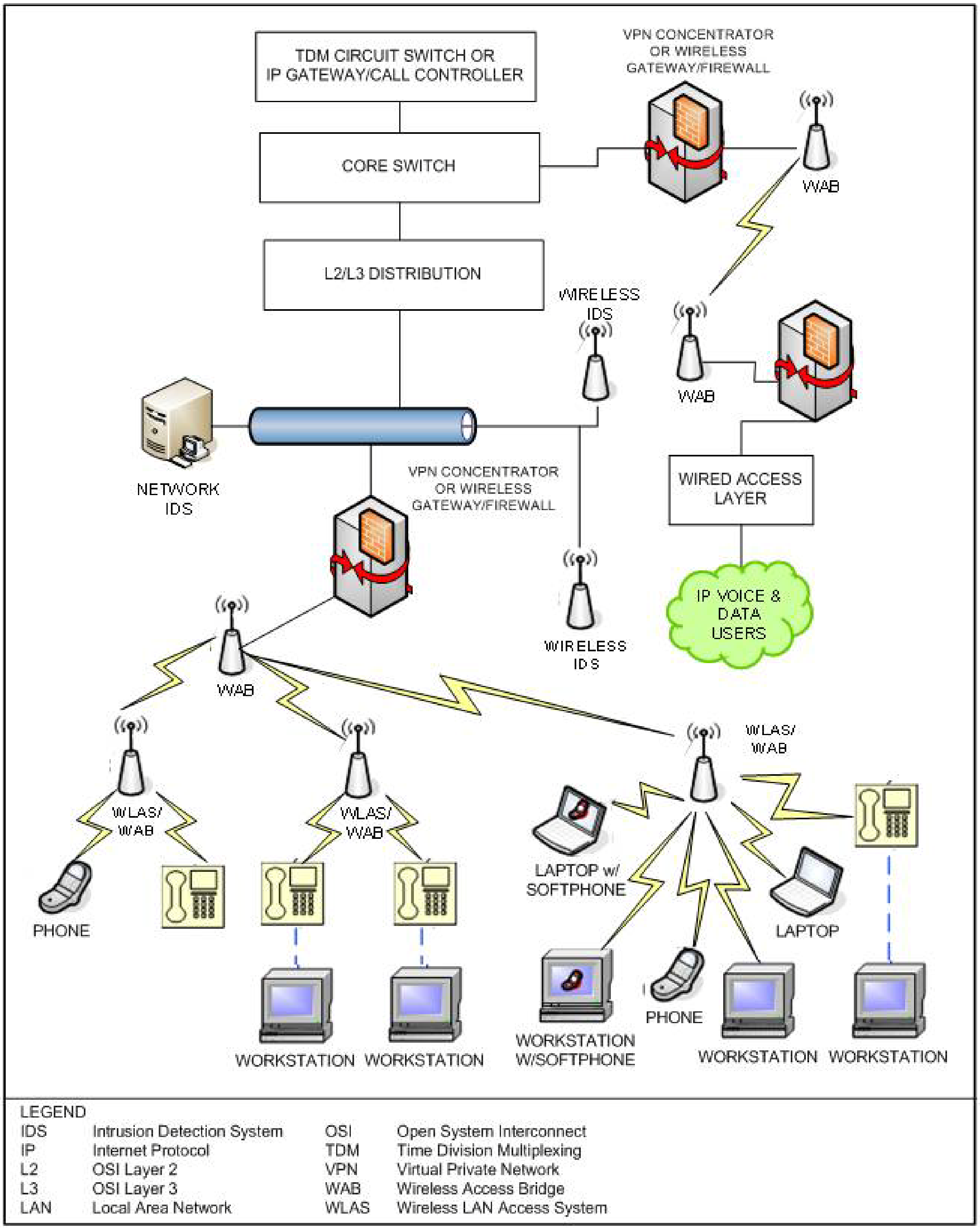
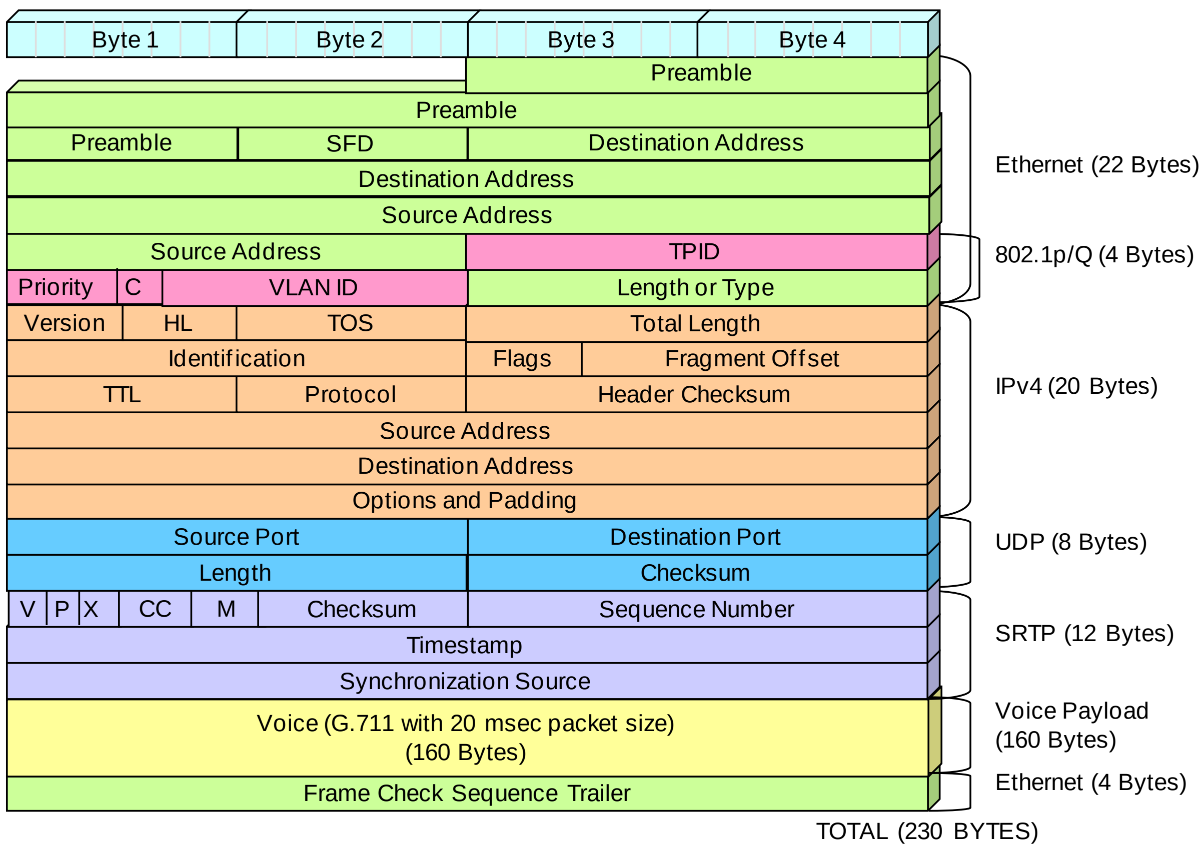


Figure 5.3.1-9. Example of Combined WLAS/WAB and Second Layer WAB

5.3.1.7.3 Traffic Engineering

5.3.1.7.3.1 Voice Services

[Required: ASLAN and Non-ASLAN] Bandwidth required per voice subscriber is calculated as 102 kbps (each direction) for each IP call (for IPv4). This is based on G.711 (20 ms codec) with IP overhead as depicted in Figure 5.3.1-10, Voice over IP Packet Size, (97 kbps for Ethernet IPv4) plus 5 kbps for SRTCP.



NOTE: Diagram does not show the 4-byte SRTP authentication tag (recommended in RFC 3711 and the optional 4-byte SRT MKI (Master Key Identifier) field. When processing an incoming packet the appliance must process the packet properly whether the 4-byte SRTP authentication tag is present or not present, and whether the 4-byte MKI Field is present or not. See RFC 3711 Section 3.1 for detailed processing requirements.

LEGEND

ID	Identification	SFD	Start Frame Delimiter	TTL	Time to Live
IPv4	Internet Protocol Version 4	TOS	Type of Service	UDP	User Datagram Protocol
msec	Milliseconds	TPID	Tag Protocol Identification	VLAN	Virtual Local Area Network
RTP	Real Time Protocol				

Figure 5.3.1-10. Voice over IP Packet Size

Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers. IPv6 adds an additional 20 bytes in the IP header (40 bytes instead of 20 bytes). The increase of 20 bytes to 250 bytes increases the IPv6 bandwidth to 110.0 kbps. This calculation includes a 12-byte Ethernet Interframe gap and the SRTCP overhead.

Bandwidth in the LAN shall be engineered so the following stipulations are met:

1. Voice IP subscribers do not exceed more than 25 percent of available egress trunk bandwidth (see examples of number of users based on common link sizes in Table 5.3.1-9, LAN VoIP Subscribers for IPv4 and IPv6. VoIP traffic on egress links may be less than 25 percent based on aggregation of links (e.g., 25 percent VoIP traffic on 10 ingress 100 Mbps links equates to 25 percent VoIP traffic on an egress trunk; 25 percent VoIP traffic on 5 100 Mbps ingress links need only have 12.5 percent VoIP on egress link. VoIP traffic aggregation may less than 25 percent but not more than 25 percent unless specifically requested by the service to the DSN Program Office with justification supporting operational requirement).

2. No single point of failure within the ASLAN can cause a voice service outage to more than 96 users. It should be noted that a single point of failure for more than 96 subscribers may exist if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers). Based on the previous constraints, the recommended number of voice subscribers based on available link sizes is shown in Table 5.3.1-9.

Table 5.3.1-9. LAN VoIP Subscribers for IPv4 and IPv6

PRODUCT	LINK TYPE	LINK SIZE	# MISSION CRITICAL VoIP SUBSCRIBERS (ASLAN)	# R AND NON-MISSION CRITICAL VoIP SUBSCRIBERS (NON-ASLAN)
Core	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000[2]	50000
	IP Trunk Link Pair	**1 Gbps**	**2500**	**5000**
	IP Trunk Link Pair	100 Mbps	250	500
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1
	IP Subscriber (converged)	100 Mbps	1[4]	1
Distribution	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	**100 Mbps**	**250**	**500**
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1

PRODUCT	LINK TYPE	LINK SIZE	# MISSION CRITICAL VoIP SUBSCRIBERS (ASLAN)	# R AND NON-MISSION CRITICAL VoIP SUBSCRIBERS (NON-ASLAN)
	IP Subscriber (converged)	100 Mbps	1[4]	1
Access	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	**100 Mbps**	**250**	**500**
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1
	IP Subscriber (converged)	100 Mbps	1[4]	1

NOTES
1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements.
2. For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization.
3. The minimum link for VoIP subscriber is 10 Mbps.
4. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps.
5. Numbers in bold represent the minimum recommended trunk sizes.
6. Link pairs may also include link aggregation. The link pair may use stand-by links or load balancing mechanisms. Regardless of method, the total number of subscribers per link pair (both links) is limited to the number of subscribers listed above.

LEGEND:
ASLAN Assured Services LAN; IP Internet Protocol; LAN Local Area Network
C2 Command and Control; IPv4 IP Version 4; Mbps Megabits per second
Gbps Gigabits per second; IPv6 IP Version 6; VoIP Voice over IP

5.3.1.7.3.2 Video Services

The amount of video bandwidth required over the ASLAN varies depending on the codec and other features that are negotiated at setup. Unlike voice, video over IP is not a constant rate. Video packets may range in size from hundreds of bytes up to 1500 bytes. Table 5.3.1-10, Video Rates and IP Overhead, lists the common video rates and associated IP overhead.

Table 5.3.1-10. Video Rates and IP Overhead

VIDEO STREAM BANDWIDTH	IP OVERHEAD	TOTAL IP BANDWIDTH
128 kbps	32 kbps	160 kbps
256 kbps	64 kbps	320 kbps
384 kbps	96 kbps	480 kbps
768 kbps	192 kbps	960 kbps
2 Mbps	0.5 Mbps	2.5 Mbps
4.5 Mbps	1.125 Mbps	5.625 Mbps
6 Mbps	1.5 Mbps	7.5 Mbps

LEGEND: IP Internet Protocol; kbps Kilobits per second; Mbps Megabits per second

Table 5.3.1-8, Maximum Number of EIs Allowed per WLAS, lists the bandwidth available based on an engineered solution of 25 percent allocation of the bandwidth to video. Unlike voice, video does not have the single point of failure requirements. Thus, the capacity or available bandwidth on a link pair is based on the aggregate total, not one half used in the voice calculations. Table 5.3.1-11, Video over IP Bandwidth, lists available video BW based on 25 percent traffic engineering and how many sessions are possible at a video rate of 384 kbps (480 kbps with IP overhead).

Video traffic on egress links may be less than 25 percent based on aggregation of links (e.g., 25 percent Video traffic on 10 ingress 100 Mbps links equates to 25 percent video traffic on an egress trunk; 25 percent video traffic on 5 ingress 100 Mbps ingress links need only have 12.5 percent Video on egress link. Video traffic aggregation may less than 25 percent but not more than 25 percent unless specifically requested by the service to the DSN Program Office with justification supporting operational requirement).

Table 5.3.1-11. Video over IP Bandwidth

ASLAN PRODUCT	LINK TYPE	LINK SIZE	# VIDEO OVER IP BW	# 384 kbps SESSIONS
Core	IP Trunk Link	10 Gbps	2.5 Gbps	5000
	IP Trunk Link	1 Gbps	250 Mbps	500
	IP Trunk Link	100 Mbps	25 Mbps	50
	IP Trunk Link	10 Mbps	2.5 Mbps	5
	IP Subscriber (video only)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Distribution	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Access	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA

ASLAN PRODUCT	LINK TYPE	LINK SIZE	# VIDEO OVER IP BW	# 384 kbps SESSIONS

NOTES
1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements.
2. For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization.
3. The minimum link for VoIP subscriber is 10 Mbps.
4. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps.
5. Numbers in bold represent the minimum recommended trunk sizes.
6. Link pairs may use stand-by links or load balancing (e.g., link aggregation). Number of subscribers is calculated as not to exceed the link pair capacity listed above regardless of the method implemented.

LEGEND

ASLAN	Assured Services LAN	kbps	kilobits per second
BW	Bandwidth	Mbps	Megabits per second
Gbps	Gigabits per second	NA	Not Applicable
IP	Internet Protocol		

5.3.1.7.3.3 Data Services

[Required: ASLAN and Non-ASLAN]. The LAN will be traffic engineered to support data traffic based on utilization of voice and video traffic engineering (0–25 percent voice/signaling, 0–25 percent video, 0–25 percent preferred data. Best Effort data traffic can burst up to the full link capacity if voice and video are not present.

5.3.1.7.4 VLAN Design and Configuration

The VLANs offer the following features:

1. <u>Broadcast Control</u>. Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.

2. <u>Security</u>. The VLANs provide security in two ways:

   a. 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.

   b. 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:

1. Port-Based. Port-based VLANs are VLANs that are dependent on the physical port that a product is connected to. All traffic that traverses the port is marked with the VLAN configured for that port. Each physical port on the switch can support only one VLAN. With port-based VLANs, no Layer 3 address recognition takes place. All traffic within the VLAN is switched, and traffic between VLANs is routed (by an external router or by a router within the switch). This type of VLAN is also known as a segment-based VLAN (see Figure 5.3.1-11, Port-Based VLANs).

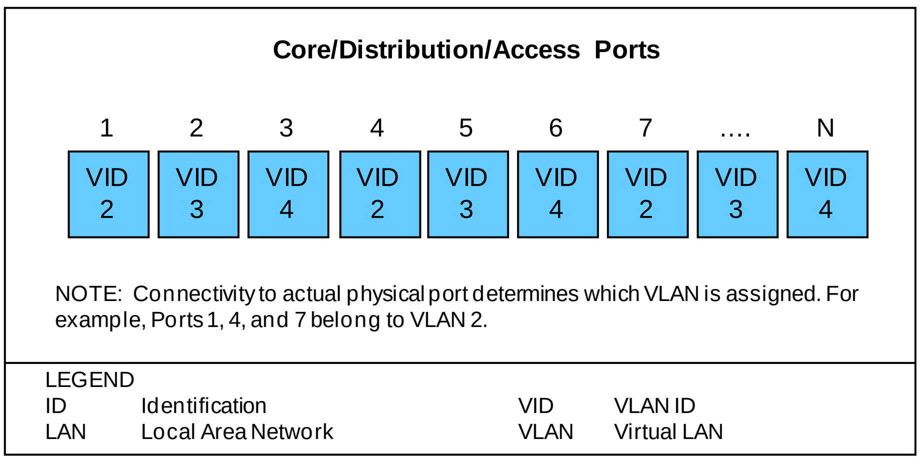


Figure 5.3.1-11. Port-Based VLANs

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

   [Required: Core, Distribution, and Access Products] The ASLAN products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see Figure 5.3.1-12, IEEE 802.1Q-Based VLANs).

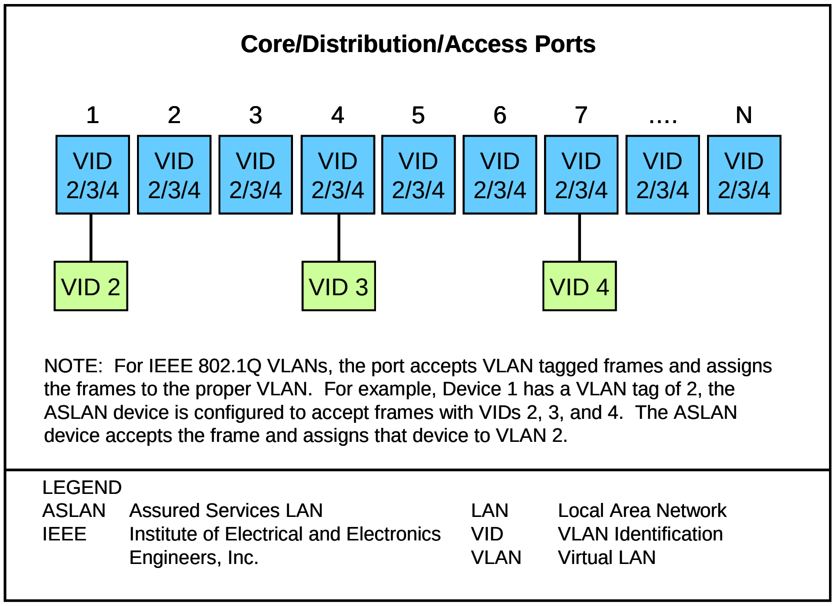


Figure 5.3.1-12. IEEE 802.1Q-Based VLANs

3. <u>By a User-Defined Value</u>. 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 MAC addresses (see Figure 5.3.1-13, User-Defined VLANs). The LAN shall be designed so RTS and data reside in separate VLANs. Whether a product is performing converged services or a single service will decide how VLANs are designed.

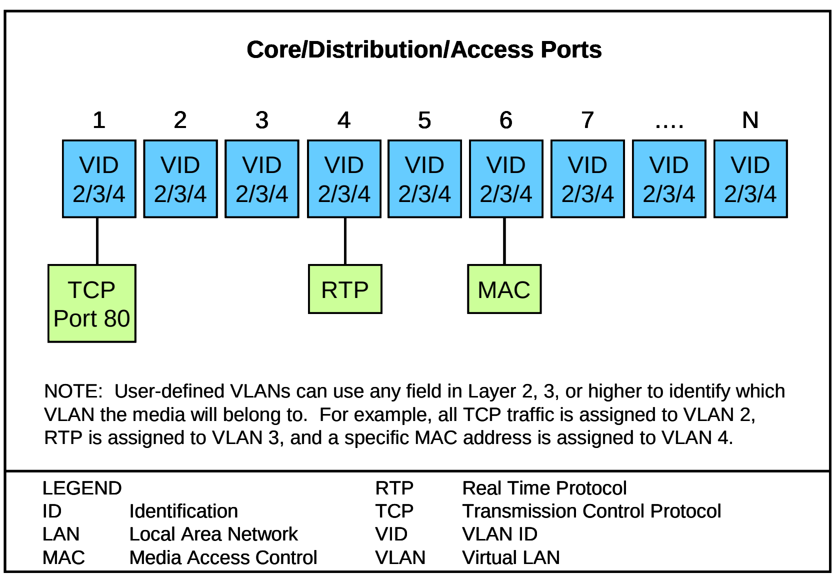


Figure 5.3.1-13. User-Defined VLANs

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) the end-system must 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.

5.3.1.7.5 Power Backup

[Required: ASLAN – Conditional: Non-ASLAN] To meet CJCS requirements for assured services, equipment serving FO/F and I/P users must be provided with backup power. The ASLAN must meet the power requirements outlined. The following requirements for emergency power systems (EPSs) are bare minimum requirements. An EPS may be any combination of uninterruptible power source (e.g., batteries) or auxiliary power (e.g., generator) that it will provide near-instantaneous protection from input power interruptions. These requirements should be increased following the guidance in Telcordia Technologies GR-513-CORE to meet site operational requirements and extenuating characteristics of the application environment. Figure 5.3.1-14, ASLAN UPS Power Requirements, illustrates a typical arrangement of how the minimum power backup requirements can be met.

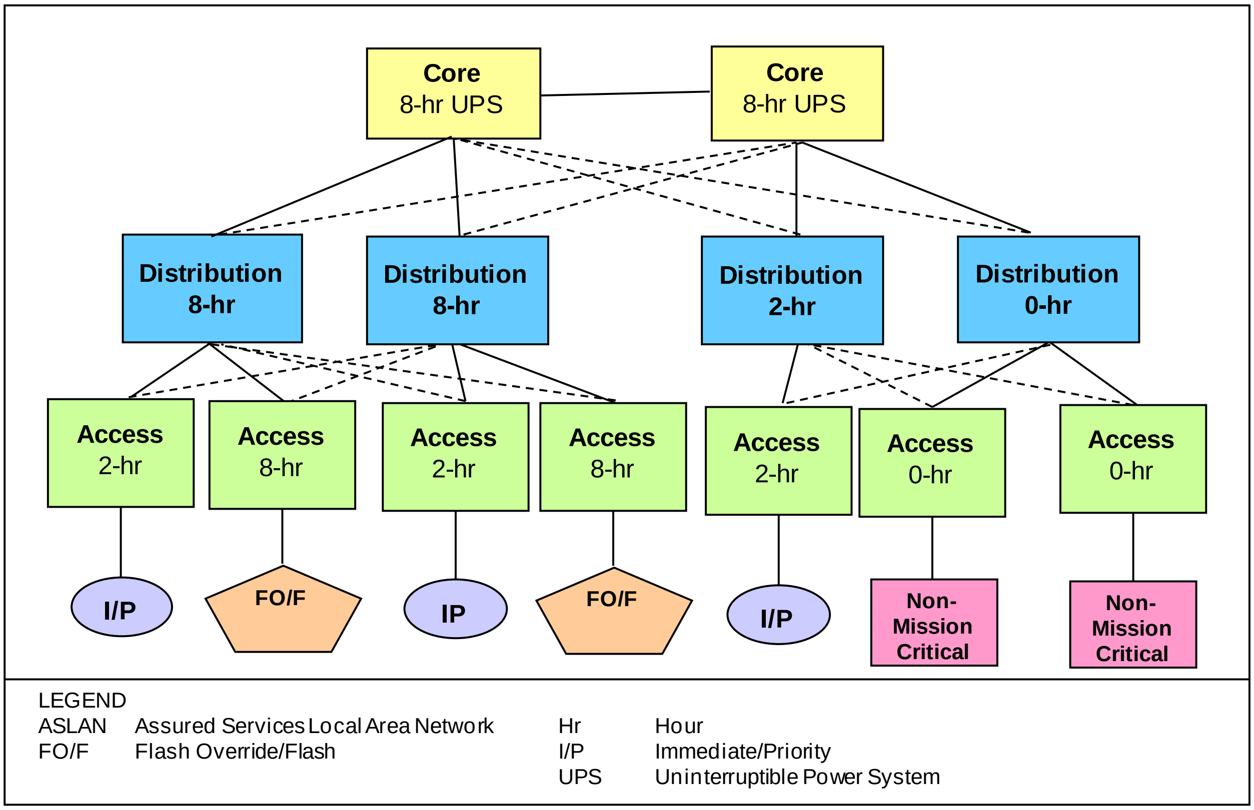


Figure 5.3.1-14. ASLAN UPS Power Requirements

1. FO/F. The ASLAN must provide an 8-hour backup capability in the event of primary power loss to FO/F users. Any ASLAN product, Core, Distribution, or Access, that supplies service to the FO/F user must have an 8-hour UPS.

2. I/P. The ASLAN must provide 2-hour backup capability in the event of primary power loss to I/P users. Any ASLAN product, core, distribution, or access that supplies service to the I/P user must have a 2-hour UPS.

3. R or Non-mission critical. R or non-mission critical users may lose telephony service in the event of a power failure. Commanders who are relying on voice communications to fulfill their responsibility for safety and force protection must take the above into account when implementing VoIP.

   NOTE: Backup Power (Environmental). Backup Power (Environmental). Environmental systems (including but not limited to heating, ventilation and air conditioning) required to sustain continuous LAN equipment operation shall have backup power. Backup power may be provided by the same system used by the LAN or a separate backup system.

5.3.1.7.6 Availability

The terms reliability, resiliency, and availability are sometimes used interchangeably. However, although all three terms are related to the concept of high availability, it is important to note the differences in terminology. Reliability is the probability that a system will not fail during a specified period of time. Resiliency is the ability of a system to recover to its normal operating form after a failure or an outage. Availability is the ratio of time that a service is available to total time.

Availability can be expressed as mean time between failure (MTBF) and mean time to repair (MTTR), and expressed in mathematical terms as:

$$\text{Availability} = \text{MTBF}/(\text{MTBF}+\text{MTTR})$$

MTBF is tied to the reliability of the system, while MTTR and resiliency are closely related. Thus system availability increases as the reliability and/or resiliency of the system is increased. Availability is typically expressed in percentage of time the system is available or in downtime per year. The two methods of expressing availability are equivalent and related as shown in Table 5.3.1-12, Methods of Expressing Availability.

Table 5.3.1-12. Methods of Expressing Availability

NUMBER OF 9'S	AVAILABILITY	DOWNTIME PER YEAR
1	90.0%	36 days, 12 hrs
2	99.0%	87 hrs, 36 mins
3	99.9%	8 hrs, 46 mins
4	99.99%	52 mins, 33 secs
5	99.999%	5 mins, 15 secs
6	99.9999%	31.5 secs
LEGEND: hrs hours	mins minutes	secs seconds

[Required: ASLAN – Conditional: Non-ASLAN] The ASLAN has two configurations depending on whether it supports FO/F or I/P users. The ASLAN shall have a hardware availability designed to meet the needs of its subscribers:

1. FO/F. An ASLAN that supports FO/F users is classified a High Availability ASLAN and must meet 99.999 percent availability to include scheduled maintenance.

2. I/P. An ASLAN that supports I/P users is classified as a Medium Availability ASLAN and must have 99.997 percent availability to include scheduled maintenance.

[Required: Non-ASLAN] The non-ASLAN shall provide an availability of 99.9 percent to include scheduled maintenance. R users who originate ROUTINE-only precedence calls but terminate any precedence level may be supported on a non-ASLAN, but the non-ASLAN must support MLPP for the R users. FO/F or I/P users shall not be supported on a non-ASLAN.

The methods for calculating reliability are found in Section 5.3.2, Assured Services Requirements.

5.3.1.7.7 Redundancy

The following paragraphs outline the redundancy requirements for the LAN.

[Required: ASLAN – Conditional: Non-ASLAN] 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 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:

1. The product itself (Core, Distribution, or Access) provides redundancy internally.

2. A secondary product is added to the ASLAN to provide redundancy to the primary product (redundant connectivity required).

5.3.1.7.7.1 Single Product Redundancy

[Conditional: ASLAN – Conditional: non-ASLAN] Single product redundancy may be met with a modular chassis that at a minimum provides the following:

1. <u>Dual Power Supplies</u>. 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.

2. <u>Dual Processors (Control Supervisors)</u>. 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.

3. <u>Termination Sparing</u>. The chassis shall support a (N + 1) sparing capability for available 10/100Base-T modules used to terminate to an IP subscriber.

4. 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.

5. 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.

6. 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.

5.3.1.7.7.2 Dual Product Redundancy

[Conditional: ASLAN – Conditional: Non-ASLAN] 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 must meet the requirements provided in Section 5.3.1.7.3, 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.

5.3.1.7.8 Maintainability

The following information is proved as an engineering guideline:

Maintainability is described in MIL-HDBK-470A as:

> "The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. In this context, it is a function of design."

Operational availability is similar to inherent availability but includes the effects of maintenance delays and other non-design factors.

The equation for operational availability, or Ao, is:

$$Ao = MTBM/(MTBM + MDT)$$

where MTBM is the mean time between maintenance and MDT is the mean downtime. (NOTE: MTBM addresses all maintenance, corrective and preventive, whereas MTBF only accounts for failures. MDT includes MTTR and all other time involved with downtime, such as delays. Thus, Ao reflects the totality of the inherent design of the product, the availability of maintenance personnel and spares, maintenance policy and concepts, and other non-design factors, whereas availability reflects only the inherent design.

When acquiring products for the ASLAN, maintainability of the products must be taken into consideration. Based on the need to meet operational availability for FO/F and I/P users, it is recommended that all ASLAN components have maintenance contracts in place that can replace key components in 24 hours or less.

5.3.1.7.9 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:

1. <u>Layer 3 Dynamic Rerouting</u>. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DISR to provide survivability. The minimum routing protocols that must be supported are:

    a. Border Gateway Protocol (BGP) for inter-domain routing (Required: Core products)

    b. 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).

    c. OSPFv2 Graceful restart (RFC 3623) and OSPFv3 Graceful Restart (RFC 5187) are conditional for Core and Distribution products. It is not applicable to access devices unless routing (OSPF) provided.

    d. Graceful Restart for BGP (RFC 4724) is conditional for infrastructure products.

2. Layer 2 Dynamic Rerouting.

   a. 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 ASLAN shall employ VRRP to provide survivability to any product running Layer 2 (normally the Access Layer).

5.3.1.7.10 Summary of LAN Requirements by Subscriber Mission

Table 5.3.1-13, Summary of LAN Requirements by Subscriber Mission, summarizes selected LAN requirements in terms of LAN types and subscriber missions.

Table 5.3.1-13. Summary of LAN Requirements by Subscriber Mission

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	FO/F	**I/P**	**R**	**NON-MISSION CRITICAL**
ASLAN High	R	P	P	P
ASLAN Medium	NP	P	P	P
Non-ASLAN	NP	NP	P	P
MLPP	R	R	R	N
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
LAN GOS p=	0.0	0.0	0.0	N/A
Availability	99.999	99.997	99.9	99.9

LEGEND

ASLAN	Assured Services LAN	NP	Not Permitted
FO/F	Flash Override/Flash	NR	Not Required
I/P	Immediate/Priority	p	Probability of Blocking
GOS	Grade of Service	P	Permitted
LAN	Local Area Network	R	Required
MLPP	Multilevel Precedence and Preemption		

5.3.1.8 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.

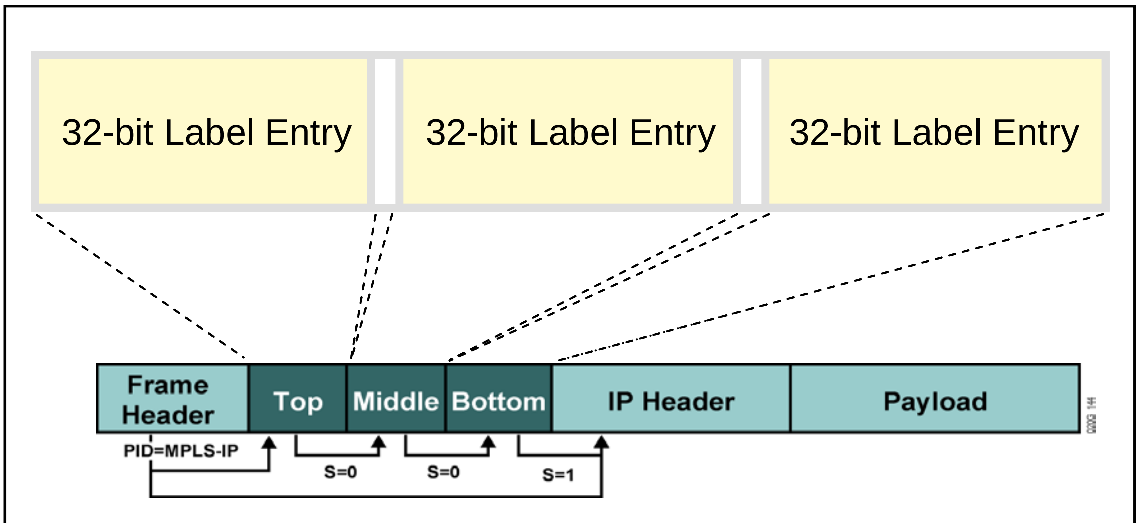
5.3.1.8.1 MPLS Background

Traditional IP packet forwarding uses the IP destination address in the packet's header to make an independent forwarding decision at each router in the network. These hop-by-hop decisions are based on network layer routing protocols, such as OSPF or BGP. These network layer routing protocols are designed to find an efficient path through the network, and do not consider other factors, such as latency or traffic congestion. Multiprotocol label switching creates a connection-based model overlaid onto the traditionally connectionless framework of IP routed networks. Multiprotocol label switching works by prefixing packets with an MPLS header, containing one or more "labels," as shown in Figure 5.3.1-15, MPLS Header, and Figure 5.3.1-16, MPLS Header Stacking. These short, fixed-length labels carry the information that tells each switching node how to process and forward the packets, from source to destination. Labels have significance only on a local node-to-node connection. As each node forwards the packet, it swaps the current label for the appropriate label to route the packet to the next node.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Label																				**Exp**			**S**	**TTL**							

LEGEND:
EXP Experimental Functions
S Stack Functions
TTL Time to Live

Figure 5.3.1-15. MPLS Header



LEGEND
IP Internet Protocol
MPLS Multiprotocol Label Switching
PID Protocol Identifier Data
S Stack Function

Figure 5.3.1-16. MPLS Header Stacking

Multiprotocol label switching relies on traditional IP routing protocols to advertise and establish the network topology. Multiprotocol label switching predetermines the path data takes across a network and encodes that information into a label that the network's routers understand. The MPLS operates at an OSI layer that is generally considered to lie between traditional definitions of Layer 2 (Data Link Layer) and Layer 3 (Network Layer). Figure 5.3.1-17, MPLS OSI Layer, illustrates the OSI Layer position of MPLS.

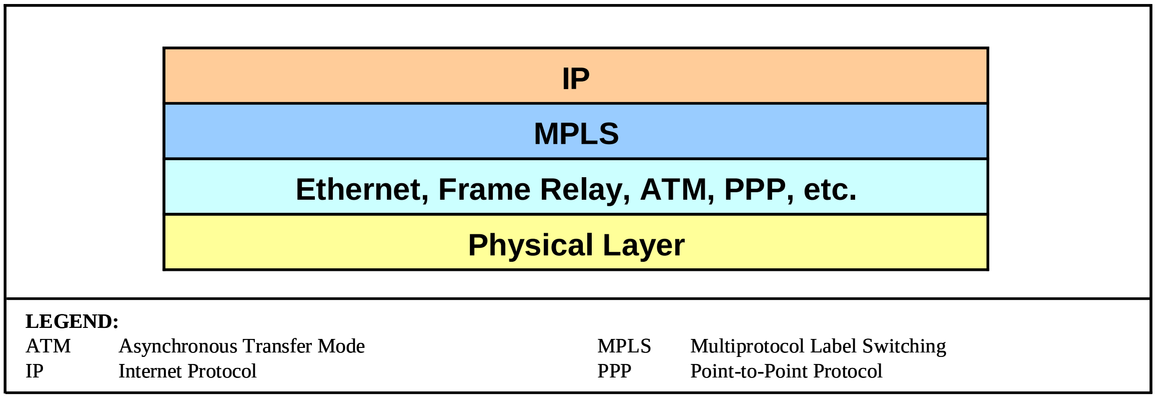


Figure 5.3.1-17. MPLS OSI Layer

5.3.1.8.2 MPLS Terminology

Definitions of terms can be found in Appendix A, Section A2, Glossary and Terminology Description.

5.3.1.8.3 DoD LAN MPLS Operational Framework

The previous ASLAN sections detail requirements up to and including the Core LAN router devices. To interconnect Core or Distribution ASLAN routers on a C/P/S, transport technologies, such as MPLS, can be used. Figure 5.3.1-18, ASLAN MPLS Operational Framework, depicts DoD's ASLAN MPLS implementation. This section does not address WAN requirements for use of MPLS with the DISN backbone.

5.3.1.8.4 MPLS Requirements

5.3.1.8.4.1 MPLS ASLAN Requirements

[Conditionally Required: 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:

- The MPLS device shall reroute data traffic to a secondary pre-signaled LSP in less than 50 ms upon indication of the primary LSP failure.

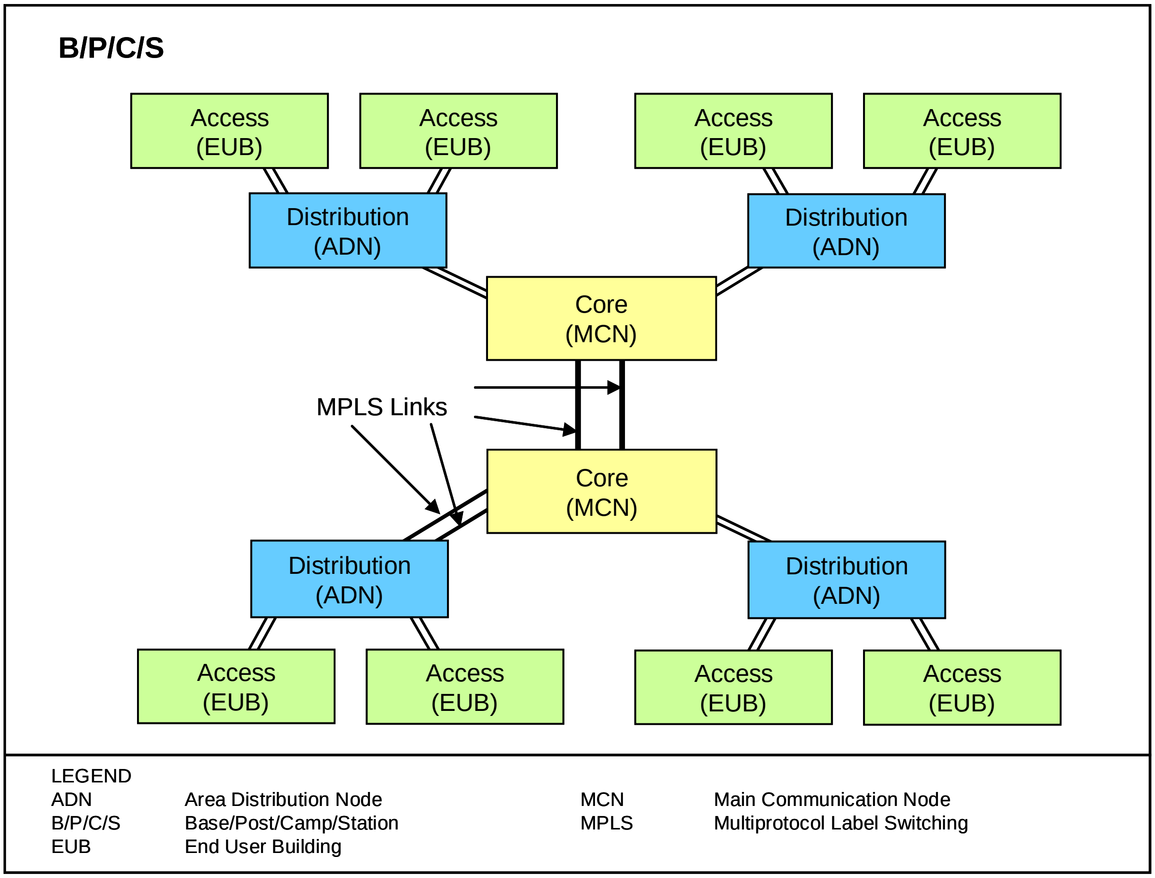


Figure 5.3.1-18. ASLAN MPLS Operational Framework

[Conditional: 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 5.3.1-14. Requests for Comment are listed as being required (R), conditional (C), or conditionally required (CR). Conditionally required RFCs are based on implementation of a particular feature, such as VPNs.

Table 5.3.1-14. 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"	CR	MPLS	
RFC 5420, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)"	CR	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5332, "MPLS Multicast Encapsulations"	C	MPLS	
RFC 5331, "MPLS Upstream Label Assignment and Context-Specific Label Space"	C	MPLS	
RFC 5151, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions"	CR	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5129, "Explicit Congestion Marking in MPLS"	C	MPLS	
RFC 5063, "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart"	CR	GMPLS	Required if GMPLS RSVP implemented
RFC 4974, "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls	CR	RSVP-TE/ GMPLS	Required if GMPLS RSVP-TE implemented
RFC 4874, "Exclude Routes – Extension to Resource Reservation Protocol-Traffic Engineering (RSVP-TE)	CR	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 4873, "GMPLS Segment Recovery"	CR	GMPLS	Required if GMPLS implemented
RFC 4872, "RSVP-TE Extensions in Support of E2E Generalized Multi-Protocol Label Switching (GMPLS) Recovery	CR	RSVP-TE/ GMPLS	Required if RSVP-TE implemented
RFC 4783, "GMPLS – Communication of Alarm Information"	CR	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)	C	VPLS	Required if L2VPN implemented via BGP

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)	CR	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)"	CR	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)"	CR	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 4379, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures"	CR	MPLS; BGP/MPLS VPNs	Required if L3VPN implemented
RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)" (replaces RFC 2547)	CR	MPLS VPNs	Required if L3VPN implemented
RFC 4328, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control"	CR	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 IETF RFC 4090.	CR	MPLS	Required if RSVP-TE implemented
RFC 4003, "GMPLS Signaling Procedures for Egress Control"	CR	GMPLS	Required if GMPLS implemented
RFC 3936, "Procedures for Modifying the Resource Reservation Protocol (RSVP)"	CR	MPLS/RSVP	Required if RSVP implemented
RFC 3564, "Requirements for support of Differentiated Services-aware MPLS Traffic Engineering"	C	MPLS	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 3479, "Fault Tolerance for the Label Distribution Protocol (LDP)"	CR	MPLS	Required if LDP implemented
RFC 3478, "Graceful Restart Mechanism for Label Distribution Protocol"	CR	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)	CR	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	
RFC 3392, "Capabilities Advertisement with BGP-4"	CR	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"	C	MPLS VPNs	
RFC 3209, "RSVP-TE: Extensions to RSVP for LSP Tunnels" (Updated by RFCs 3936, 4420, 4874, 5151, and 5420)	CR	MPLS VPNs	Required if RSVP-TE implemented
RFC 3140, "Per Hop Behavior Identification Codes"	R	MPLS	
RFC 3107, "Carrying Label Information in BGP-4"	CR	BGP/MPLS VPNs	Required if BGP implemented
RFC 3037, "LDP Applicability"	C	MPLS	
RFC 3036, "LDP Specification"	CR	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"	CR	RSVP	Required if RSVP implemented
RFC 2917, "A Core MPLS IP Architecture"	C	MPLS	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 2747, "RSVP Cryptographic Authentication" and RFC 3097, RSVP Cryptographic Authentication (Updated Message Type Value)	CR	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	LDP	Label Distribution Protocol
BGP	Border Gateway Protocol	LSP	Label Switched Path
CR	Conditionally Required	MPLS	Multiprotocol Label Switching
EXP	Experimental	R	Required
GMPLS	Generalized Multiprotocol Label Switching	RFC	Request for Comments
G.709	ITU-T Recommendation G.709, "Interfaces for the optical transport network (OTN)"	RSVP	Resource Reservation Protocol
		RSVP-TE	Resource Reservation Protocol-Traffic Engineering
IP	Internet Protocol	SONET	Synchronous Optical Network
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector	TE	Traffic Engineering
		TTL	Time To Live
L2VPN	Layer 2 Virtual Private Network	VPLS	Virtual Private LAN Service
L3VPN	Layer 3 Virtual Private Network	VPN	Virtual Private Network
LAN	Local Area Network		

5.3.1.8.4.2 MPLS ASLAN Requirements MPLS VPN Augmentation to VLANs

The MPLS supports both Layer 2 VPNs 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 (VRFs) to create an IP-based VPN.

5.3.1.8.4.2.1 MPLS Layer 2 VPNs

[Required: Core and Distribution Products supporting MPLS]

The ASLAN Core or Distribution products will provide Layer 2 MPLS VPNs by minimally supporting :

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

The product may additionally support:

- 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.

[Conditional: 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."

5.3.1.8.4.2.2 MPLS Layer 3 VPNs

[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)."

[Required: Core and Distribution Products supporting MPLS]

The ASLAN products used to support L3VPNs by RFC 4364 shall support the following RFCs:

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

5.3.1.8.4.2.3 MPLS QoS

[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:

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

5.3.1.9 Digital Subscriber Line (DSL) Requirements

5.3.1.9.1 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.

5.3.1.9.2 Primary Application Support

DSL is primarily used at military facilities to provide Local Area Network (LAN) interconnection. As such, the primary DSL functions that support this application are:

- Symmetrical bandwidth (available with some DSL access technologies)
- Use of DSL repeaters to provide an extended range of operation
- Point-to-Point configurations
- Point-to-Multi-Point configurations

5.3.1.9.3 DSL Overview

DSL uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, between endpoints. The term xDSL covers a number of DSL technologies. Those that are standards-based are shown in Table 5.3.1-15, ITU DSL Standards Overview.

Many of these DSL technologies support both analog voice services and high-bandwidth digital data services (which may include UC VoIP and Video over IP services). In this case, different frequency bands are used on each twisted-pair copper telephone line for the analog voice service and the digital data service.

Table 5.3.1-15. ITU DSL Standards Overview

VERSION	STANDARD	COMMON NAME	DOWNSTREAM RATE	UPSTREAM RATE	INITIALLY APPROVED IN
High Bit Rate DSL (HDSL)	ITU G.991.1	HDSL/2/4 (multi pair)	1.5-2.0 Mbps	1.5-2.0 Mbps	1998
ADSL	ITU G.992.1	ADSL (G.DMT)	6.144 Mbps	640 Kbps	1999
ADSL	ITU G.992.2	ADSL Lite (G.Lite)	1.5 Mbps	0.5 Mbps	1999
ADSL	ITU G.992.1 Annex A	ADSL over POTS	6.144 Mbps	640 Kbps	1999
Very High Speed DSL (VDSL)	ITU G.993.1	VDSL	52 Mbps	16 Mbps	2001
ADSL2	ITU G.992.3 Annex J	ADSL2	8 Mbps	800 Kbps	2002
ADSL2	ITU G.992.3	ADSL2	8 Mbps	800 Kbps	2002
ADSL2	ITU G.992.4	Splitterless ADSL2	1.5 Mbps	0.5 Mbps	2002
Single Pair High-Speed DSL (SHDSL)	ITU G.991.2	G.SHDSL (single pair)	2.3 Mbps	2.3 Mbps	2003
ADSL2+	ITU G.992.5	ADSL2+	24 Mbps	1.3 Mbps	2003
ADSL	ITU G.992.1 Annex B	ADSL over ISDN	12 Mbps	1.8 Mbps	2005
ADSL2	ITU G.992.3 Annex L	RE-ADSL2	5 Mbps	0.8 Mbps	2005
VDSL2	ITU G.993.2	VDSL2	100 Mbps[1]	100 Mbps[1]	2006
ADSL2+	ITU G.992.5 Annex M	ADSL2+M	24 Mbps	3.3 Mbps	2008

NOTES :
1. VDSL2 supports transmission at a bidirectional net data rate (the sum of upstream and downstream rates) up to 200 Mbps.

5.3.1.9.3.1 DSL Bonding

Wire bonding solutions provide a method for combining multiple copper DSL connections (with the same or different bit rates) together into a single, aggregate connection. This technology is extremely valuable when support for high-speed services must be provided. Bonding can allow delivery of high-bandwidth services even when the bandwidth of individual DSL connections is relatively low.

Three DSL bonding standards are defined in Table 5.3.1-16, DSL Bonding Standards.

Table 5.3.1-16. DSL Bonding Standards

ITU-T STANDARD	DESCRIPTION
G.998.1	**ATM-based multi-pair bonding:** A method for bonding of multiple DSL lines to transport an ATM payload beyond the rate/reach capability of a single DSL loop. This protocol allows the bonding of 2 to 32 pairs and supports dynamic removal and restoration of pairs without human intervention.
G.998.2	**Ethernet-based multi-pair bonding:** Provides a method for bonding of multiple DSL lines for Ethernet transport. This recommendation builds on IEEE 802.3ah-2004 Ethernet in the First Mile (EFM) methods, and extends Ethernet transport over multiple xDSL technologies, including ADSL.
G.998.3	**Multi-pair bonding using time-division inverse multiplexing:** Details a method for bonding DSL lines using Time-Division Inverse Multiplexing (TDIM). This recommendation uses IEEE 802.3ah handshakes for pair discovery, parameter negotiation, and setup. It also allows the hitless addition and removal of pairs (i.e., without any service disruption) and the fast removal of a pair upon pair failure.

Each of these bonding methods is designed to be efficient in a DSL environment and independent of the particular physical layer being used. A primary goal of each method is to provide the capability to bond lines that are running at different data rates in order to maximize the bit rate available over the bonded connection.

Bonding of multiple logical links, which is done independent of physical layer technology, can also be provided using the Multilink Point-to-Point Protocol (MLPPP), as specified in IETF Request for Comment (RFC) 1990, *The PPP Multilink Protocol (MP)*. This type of bonding can be used with any xDSL technology. MLPPP defines a method for splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP is currently used in some ADSL products to provide link bonding.

5.3.1.9.4 Ethernet in the First Mile over Copper (EFMCu)

Ethernet in the first mile (EFM) is known as IEEE 802.3ah and defines Ethernet in the access network, i.e., first or last mile. EFMCu defines interfaces over voice-grade copper with optional multi-pair aggregation or bonding transmission.

EFMCu allows for deployment of resilient symmetrical Ethernet Access links over existing voice-grade copper infrastructure, providing an economical alternative to fiber and a solution where only voice-grade copper infrastructure exists.

There are two standardized EFMCu technologies:

- Long reach 2BASE-TL, delivering a minimum of 2 Mbps and a maximum of 5.69 Mbps over distances of at least 2700 m, using standard G.SHDSL.bis technology over a single copper pair.

- Short reach 10PASS-TS, delivering a minimum of 10 Mbps over distances of at least 750 m, using standard VDSL technology over a single copper pair.

5.3.1.9.5 DSL-Based ASLAN Interconnection Operational Framework

DSL or EFMCu connections are used to provide ASLAN interconnection in the Network Edge Segment. Either can be utilized in cases where voice-grade wiring is the only choice for linking ASLANs in different buildings within a military base. DSL or EFMCu utilization within a base is described in the following sections.

5.3.1.9.5.1 Point-to-Point Interconnection of ASLANs

Figure 5.3.1-19, Point-to-Point LAN Interconnection, illustrates the simplest scenario for DSL use on a military base is for basic point-to-point LAN interconnection. This can be used for connectivity within an ASLAN, or for connectivity between ASLANs on the same base. It makes use of Unshielded Twisted Pair (UTP) copper phone cables for connectivity.

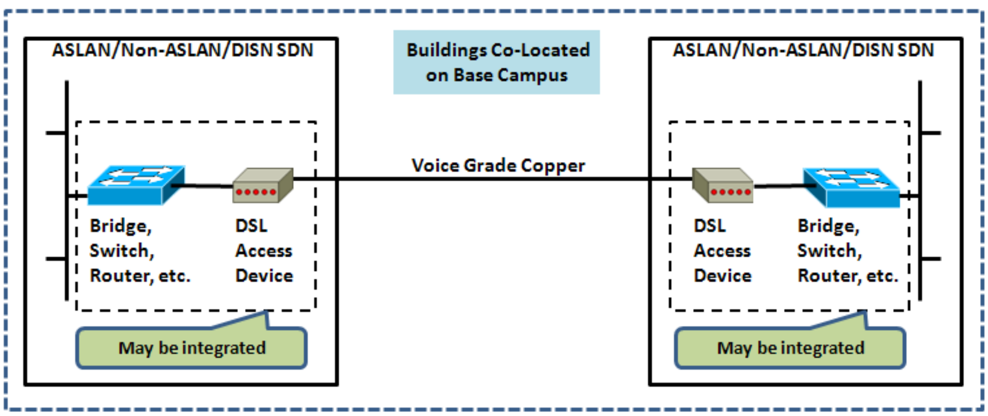


Figure 5.3.1-19. Point-to-Point LAN Interconnection

At each location is a DSL access device which contains a DSL line interface (on the voice-grade copper side) and typically an Ethernet physical interface (on the LAN side). At a minimum, the DSL access device supports data bridging between its two sides, but it may have additional functionality built in, such as LAN switching and IP routing.

5.3.1.9.5.2 Point-to-Multipoint Interconnection of ASLANs

As illustrated in Figure 5.3.1-20, Point-to-Multipoint Interconnection Concentration, a more complicated scenario for DSL use on a military base is for point-to-multipoint LAN interconnection. This can be used for aggregating connectivity of ASLANs to a single or multiple core locations within the same base. It also makes use of UTP copper phone cables for connectivity.

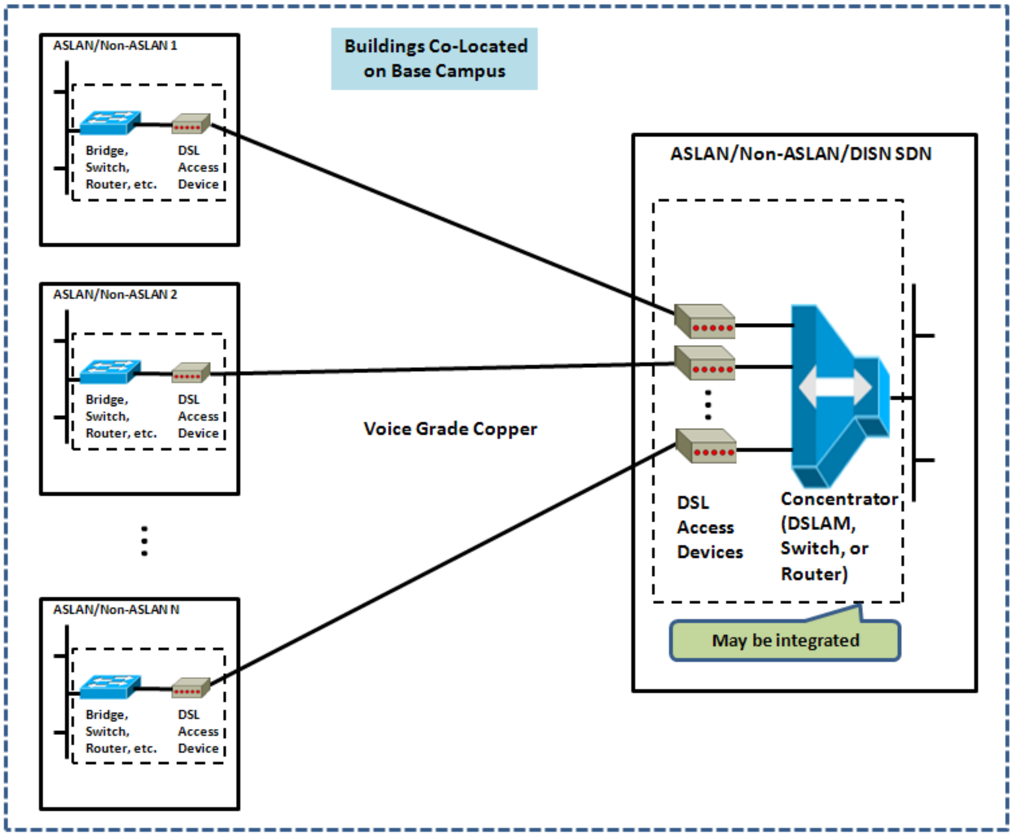


Figure 5.3.1-20. Point-to-Multipoint Interconnection Concentration

In this scenario, a Concentrator handles connectivity for multiple ASLAN locations and then aggregates traffic that is destined for remote destinations. Typically, the Concentrator is a DSL Access Manager (DSLAM), a Bridge, or a Router, all of which have advanced functionality to support switching or routing of IP packets between local ASLANs, and forwarding/routing of IP brackets between local DSLAMs and remote destinations.

DSLAMs can support a very large amount of interfaces (e.g., multiple 19 inch/23 inch racks of equipment that support hundreds of access interfaces), or they can be very small, mini-DSLAMs that support less than one hundred access interfaces.

5.3.1.9.5.3 DSL Repeaters

There may be situations where the distance between two ASLANs is too long to support a single DSL connection. In this scenario, a solution could be to use multiple DSL wire hops to bridge the link. While the total distance may be too great for a single DSL transmitter/receiver pair, cascading two separate DSL links may provide the solution. In this case, a DSL repeater could be used to amplify the DSL signal at a midpoint in the total link to provide enough amplification to drive the signal over the total link length.

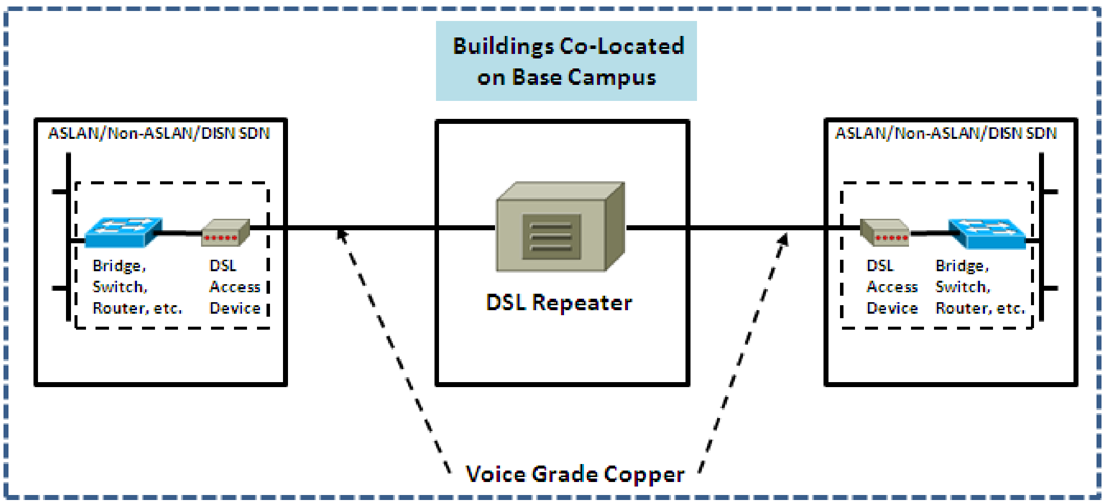


Figure 5.3.1-21. DSL Repeater Provides Extended Distance

Use of a DSL repeater provides extended distance/speed between DSL endpoints.

5.3.1.9.5.4 DSL Support for Analog Voice and Voice over IP (VoIP)

DSL Access Device, Concentrator, and Repeater products can also be used to carry both Analog Voice and VoIP services over existing voice-grade copper links. In this case, the Analog Voice is carried over the link using the pre-existing Analog Voice frequency band, and the VoIP is carried over the link using the separate frequency bands that the DSL products use for IP data service. A Base configuration supporting Analog Voice, IP Data, Voice over IP, and Video over IP with DSL Modems, a DSLAM, and a UC LSC, is shown in Figure 5.3.1-22, Base Configuration Supporting Analog Voice and VoIP using DSL Modems and a DSLAM.

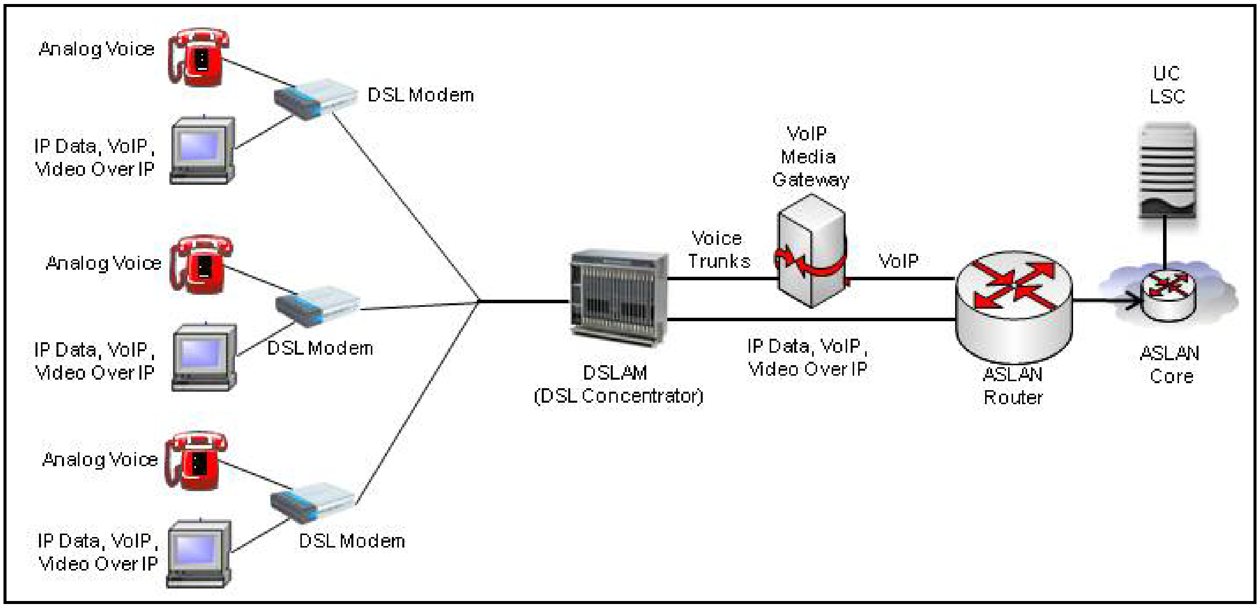


Figure 5.3.1-22. Base Configuration Supporting Analog Voice and VoIP using DSL Modems and a DSLAM

In the above configuration, the Analog Voice, VoIP, and Video over IP Services are all provided by a UC LSC and its associated VoIP Media Gateway on the Base. The Media Gateway provides conversion between Analog Voice service and UC VoIP service in this case. For VoIP and Video Over IP services, the DSLAM also needs to be interoperable with the ASLAN Router and the UC LSC, based on the ASLAN Router requirements in Section 5.3.1 and the LSC requirements in Section 5.3.2.

On Bases that are not equipped with an LSC and a Media Gateway, the Analog Voice service can be provided by an End Office or PBX on the Base. When a UC LSC and VoIP Media Gateway are located at the Base, the DSLAM and the MG can be interconnected using either individual analog lines (e.g., Unshielded Twisted Pairs) or by an ISDN PRI, that multiplexes the analog lines onto one or more T1 facilities. In this case, the DSLAM also needs to be interoperable with the MG ISDN PRI requirements in Section 5.3.2.

It is also possible for the DSLAM and the VoIP Media Gateway to be integrated into a single product. In this case, the DSLAM side of the product needs to meet the Concentrator requirements in this section, and the MG side of the product needs to meet the MG requirements in Section 5.3.2. Support for integrated DSLAM/MG products is not required.

5.3.1.9.6 DSL Requirements

The following requirements 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

5.3.1.9.6.1 Physical Layer

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

- ADSL ITU G.992.1 (G.DMT)
- ADSL ITU G.992.2 (G.Lite)
- ADSL2 ITU G.992.3
- ADSL2+ ITU G.992.5

[Conditional: Access Devices, Concentrators, Repeaters] Access Devices, Concentrators, and Repeaters shall provide the following DSL interface types:

- SHDSL ITU G.991.2
- VDSL ITU G.993.1
- HDSL ITU G.991.1
- VDSL2 ITU G.993.2
- Long reach 2BASE-TL IEEE Std 802.3ah
- Short reach 10PASS-TS IEEE Std 802.3ah

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

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

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

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

5.3.1.9.6.2 Data Link Layer

[Conditional: Access Devices, Concentrators] DSL products shall meet at least one of the following DSL bonding capabilities:

• ATM-based multi-pair bonding	ITU G.998.1
• Ethernet-based multi-pair bonding	ITU G.998.2
• Multi-pair bonding using time-division inverse multiplexing	ITU G.998.3
• Multilink Point-to-Point Protocol bonding	RFC 1990

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

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

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

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

[Conditional: Access Devices, Concentrators] DSL products shall meet the Asynchronous Transfer Mode (ATM) capabilities defined in ITU I.361.

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

5.3.1.9.6.3 Network Layer

[Required: Access Devices, Concentrators] DSL products shall meet all of the IPV4 protocol requirements for UC Access products as listed in Table 5.3.1-5, Core, Distribution, and Access Product Requirements Summary.

[Required: Access Devices] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.3.5-3, UC End Instruments (EI), of Section 5.3.5, IPv6 Requirements.

[Required: Concentrators] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.3.5-6, LAN Switch (LS), of Section 5.3.5, IPv6 Requirements.

5.3.1.9.6.4 Information Assurance

[Required: Access Devices, Concentrators, Repeaters] The Information Assurance requirements are contained in Section 5.4, Information Assurance Requirements.

5.3.1.9.6.5 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 DSLAM shown in Figure 5.3.1-22. These requirements apply to Analog Voice services, and do not apply to VoIP or Video over IP Services.

[Conditional: 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 LSC for voice call completion, the Concentrator's interface to the VoIP Media Gateway shall match the Media Gateway interface requirements in Section 5.3.2.12, Media Gateway Requirements.

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.

[Conditional: 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 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).

[Conditional: 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).

5.3.1.9.6.6 Device Management

[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 5.9.2.4, Device Management.

[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, as specified in Section 5.3.1.6, Infrastructure Network Management Requirements.

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

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

[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.

5.3.1.9.7 References

The following References were used in the DSL Requirements Section:

G.991.1	ITU-T Recommendation G.991.1, “High bit rate digital subscriber line (HDSL) transceivers,” 1998.
G.991.2	ITU-T Recommendation G.991.2, “Single-pair high-speed digital subscriber line (SHDSL) transceivers,” 1998.
G.992.1	ITU-T Recommendation G.992.1, “Asymmetric digital subscriber line (ADSL) transceivers,” 1999.
G.992.2	ITU-T Recommendation G.992.2, “Splitterless asymmetric digital subscriber line (ADSL) transceivers,” 1999.
G.992.3	ITU-T Recommendation G.992.3, “Asymmetric digital subscriber line transceivers 2 (ADSL2),” 2009.
G.992.4	ITU-T Recommendation G.992.4, “Splitterless asymmetric digital subscriber line transceivers 2 (splitterless ADSL2),” 2002.
G.992.5	ITU-T Recommendation G.992.5, “Asymmetric digital subscriber line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2plus),” 2009.
G.993.1	ITU-T Recommendation G.993.1, “Very high speed digital subscriber line transceivers (VDSL),” 2004.
G.993.2	ITU-T Recommendation G.993.2, “Very high speed digital subscriber line transceivers 2 (VDSL2),” 2006.
G.998.1	ITU-T Recommendation G.998.1, “ATM-based multi-pair bonding,” 2005.
G.998.2	ITU-T Recommendation G.998.2, “Ethernet-based multi-pair bonding,” 2005.
G.998.3	ITU-T Recommendation G.998.3, “Multi-pair bonding using time-division inverse multiplexing,” 2005.

I.361	ITU-T Recommendation I.361, "B-ISDN ATM layer specification," 1999.
I.363.5	ITU-T Recommendation I.363.5, "B-ISDN ATM Adaptation Layer specification : Type 5 AAL," 1999.
RFC 1990	K. Sklower, B. Lloyd, et al, "The PPP Multilink Protocol (MP)," August 1996.
802.1D	IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, June 2004.
802.1Q	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 2003.
802.3	IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 26 December 2008.
802.3ab	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s), 1999.
802.3ah	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks, 2004.
802.3i	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbps (1.25 MB/s) over twisted pair, 1990.
802.3u	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbps (12.5 MB/s) w/auto-negotiation, 1995.
802.3z	IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s), 1998.

5.3.1.10 Passive Optical Network (PON) Technology

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

5.3.1.10.1 Definition of PON

Passive Optical Network (PON) is a technology that is composed of an Optical Line Termination (OLT), a varying number of Optical Network Units/Terminals (ONU/ONT) with fiber optic cable and splitters connecting them. Interface from the backbone network (NNI or Ingress) is provided by the OLT while the user interface (UNI or Egress) is provided by the ONT. Typical PON network connectivity is illustrated in Figure 5.3.1-23, 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 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.

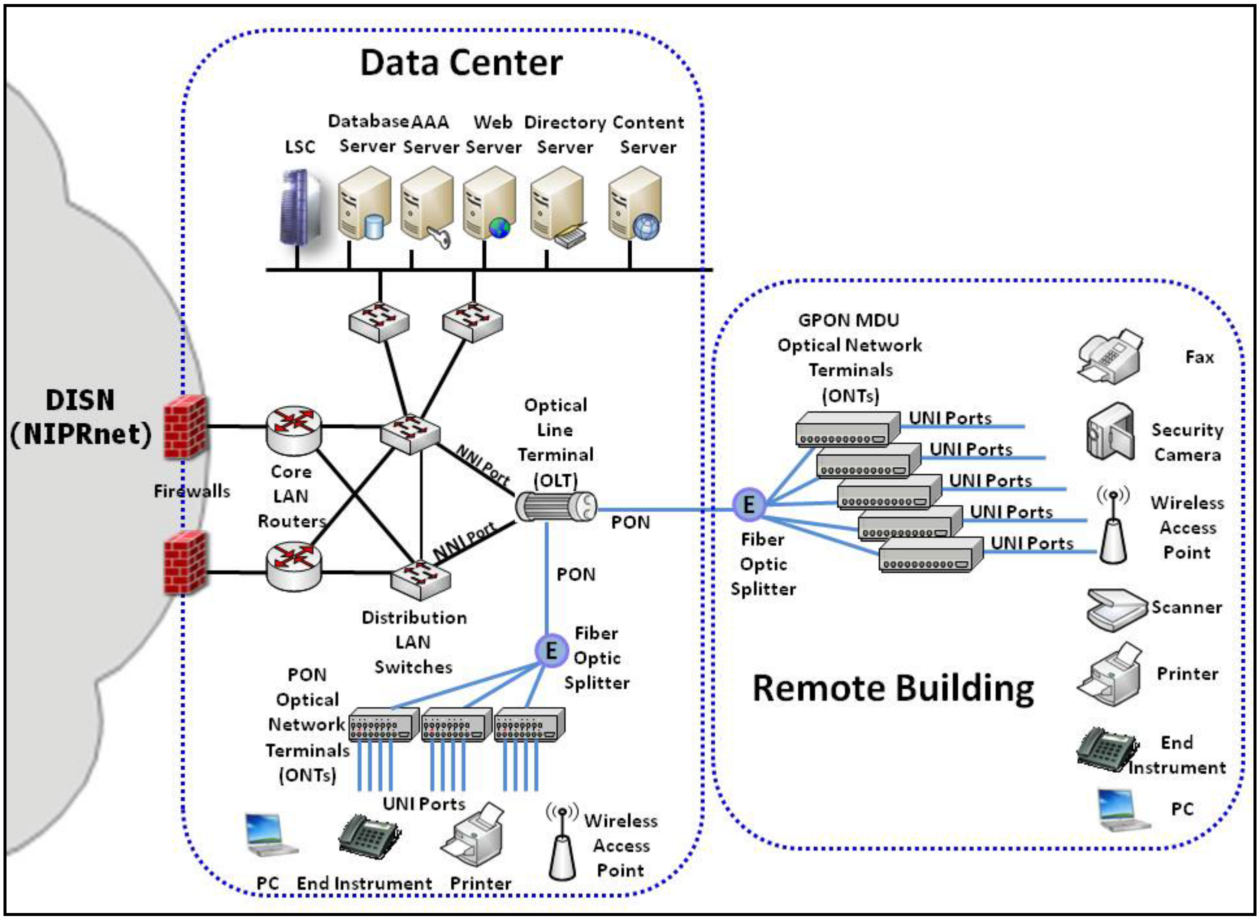


Figure 5.3.1-23. Typical PON Network Connectivity

The common PON operational framework 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 Gbit/s 10/1 Gbit/s and 10/10 Gbit/s.

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 Optical Line Terminal (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 Optical Network Terminals (ONT) which provide Ethernet, analog 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 figures below display two different connectivity solutions utilizing the GPON network operational framework. Figure 5.3.1-24, 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 5.3.1-25, PON Connectivity in a Collapsed DoD Backbone Operational Framework, shows a collapsed backbone where fiber splitters are the only equipment required at the ADN.

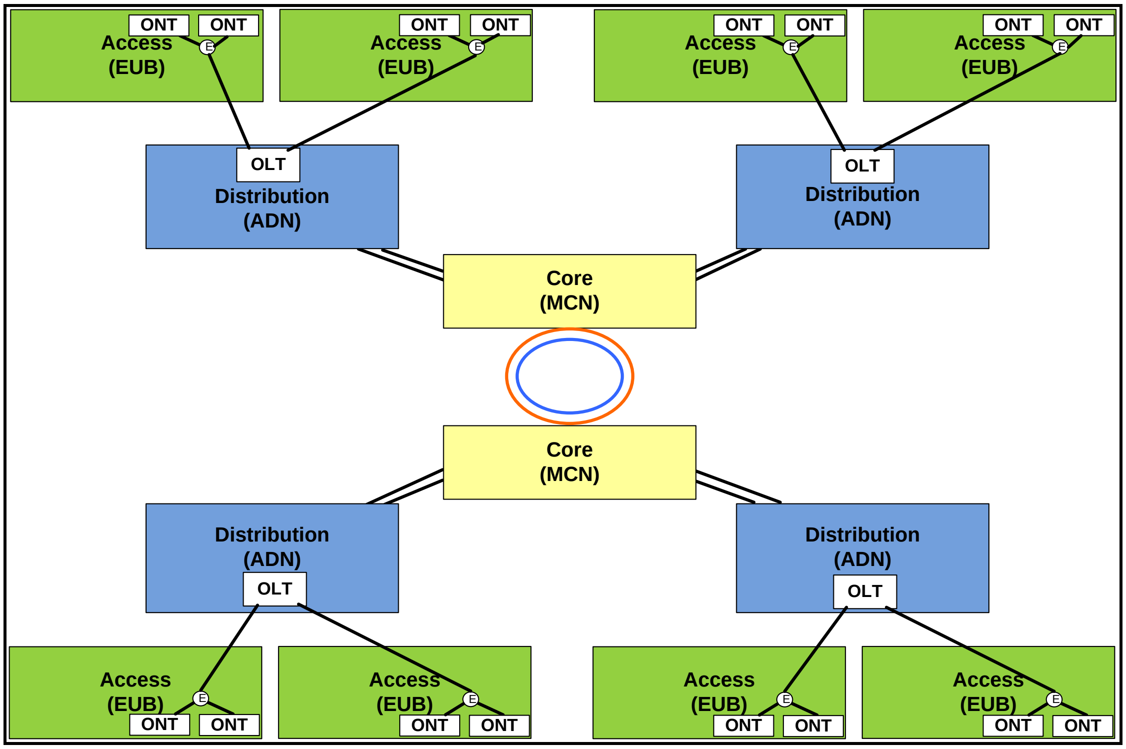


Figure 5.3.1-24. PON Connectivity in the DoD Operational Framework

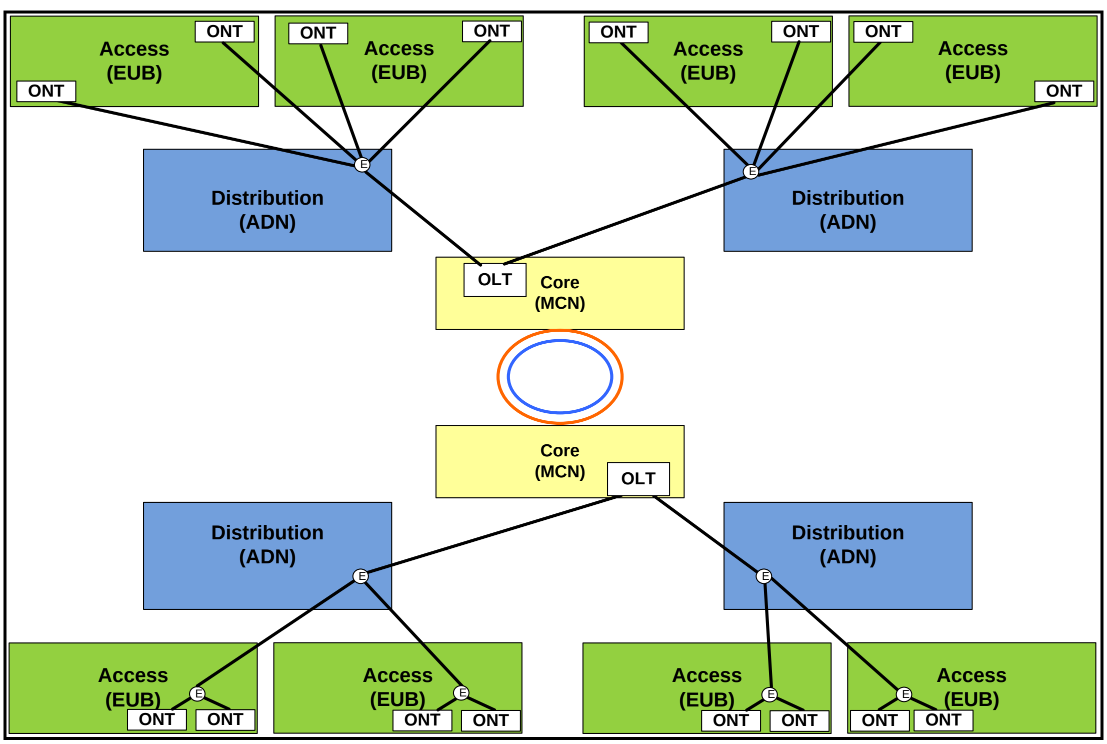


Figure 5.3.1-25. PON Connectivity in a Collapsed DoD Backbone Operational Framework

5.3.1.10.2 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. The NNI: the Ingress interface, OLT to ONT interface (PON), Network Management interface, and the UNI interface.

5.3.1.10.2.1 NNI-NNI Interface

[Required: PON] The NNI-NNI interface is composed of the uplink between the OLT and the Core network. This interface is composed of IEEE 802.3 interfaces and may provide a Fibre channel interface IAW ANSI International Committee for Information Technology Standards (INICITS) T11.2 and T11.3 (previously known as X3T9.3). At this time, no minimum rate or type of IEEE 802.3 interface is specified and COTS interfaces are accepted. If the Fibre Channel Interface is provided the interface must meet:

- RFC 4338 Transmission of IPv6, Ipv4 and Address Resolution Protocol (ARP) Packets over Fibre channel: and

- RFC 4044 Fibre Channel Management

[Required: PON] The OLT NNI-NNI port shall support at least one of the following interface rates (other rates and IEEE standards may be provided as conditional interfaces)):

- 100 Megabits per second (Mbps) IAW IEEE 802.3u
- 1 Gigabit per second (Gbps) IAW IEEE 802.3z
- 10 Gigabit per second (Gbps) IAW IEEE 802.3ae

The NNI ports shall provide the following parameters on a per port basis as specified:

- Auto-negotiation IAW IEEE 802.3
- Force mode IAW IEEE 802.3
- Flow control IAW IEEE 802.3x
- Filtering IAW RFC 1812
- Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad)
- Spanning Tree Protocol IAW IEEE 802.1D
- Multiple Spanning Tree IAW IEEE 802.1s
- Rapid Configuration of Spanning Tree IAW IEEE 802.1w

5.3.1.10.2.2 OLT to ONT PON Interface

[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 1490nm) 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 5.3.1.7.3 ,Traffic Engineering. The OLT to ONT interface will support the Telcordia Standards shown in Table 5.3.1-17, OLT to ONT Signaling Standards.

Table 5.3.1-17. 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	

5.3.1.10.2.3 Network Monitoring

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

- Simple Network Management Protocol (SNMP) IAW RFCs 1157, 3410, 3411, 3412, 3413, and 3414

- SNMP Traps IAW RFC 1215

- Remote Monitoring (RMON) IAW RFC 2819

- Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584

- The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826

5.3.1.10.2.4 UNI Interface

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

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

In addition, PON must support traffic conditioning, which will insure that the required bandwidth is available for all network users.

5.3.1.10.2.4.1 UNI Ports

[Required: PON] The UNI ports shall provide the following parameters on a per port basis as specified:

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

[Conditional: PON] Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad)

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

- Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) PoE for Conditional Interfaces IEEE 802.3af

- PoE Plus or Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) for Conditional Interfaces IEEE 802.3at

5.3.1.10.3 Class of Service Markings

[Required: PON] The PON network shall comply with access product requirements, Section 5.3.1.3.3, #1 and #3.

5.3.1.10.4 Virtual LAN Capabilities

[Required: PON] The NNI and UNI PON ports shall comply with Section 5.3.1.3.4, Virtual LAN Capabilities.

5.3.1.10.5 Protocols

[Conditional: 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.

5.3.1.10.6 Quality of Service Features

[Required: PON] The PON shall comply with the Access product requirements listed in Section 5.3.1.3.6, 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.

5.3.1.10.7 Network Monitoring

[Required: PON] The PON shall comply with the product requirements listed in Section 5.3.1.3.7, Network Monitoring.

5.3.1.10.8 Voice Services

5.3.1.10.8.1 Latency

[Required: PON] The PON shall have the capability to transport voice IP packets, media, and signing, 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.

5.3.1.10.8.2 Jitter

[Required: PON] The PON shall have the capability to transport 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 25 percent voice/signaling, 25 percent IP video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.8.3 Packet Loss

[Required: PON] The PON shall have the capability to transport voice 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.9 Video Services

5.3.1.10.9.1 Latency

[Required: PON] The PON shall have the capability to transport video IP packets with no more than 30 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 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.9.2 Jitter

[Required: PON] The LAN shall have the capability to transport 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.9.3 Packet Loss

[Required: PON] The PON shall have the capability to transport 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.10 Data Services

5.3.1.10.10.1 Latency

[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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.10.2 Jitter

There are no jitter requirements for preferred data IP packets.

5.3.1.10.10.3 Packet Loss

[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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.10.11 Information Assurance Requirements

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

5.3.1.10.12 PON Network Management Requirements

[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 GIG management capabilities. The PON infrastructure components must be able to be centrally managed by an overall network management system (NMS). In addition, 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:

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

5.3.1.10.12.2 **[Required: PON]** The PON product shall be configured by default, not to accept Telnet.

5.3.1.10.12.3 **[Conditional: PON]** HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HTTP due to its increased security as described in RFC 2660.

5.3.1.10.12.4 **[Conditional: PON]** The LAN products shall support RFC 3414 for SNMP.

5.3.1.10.12.5 **[Conditional: PON]** If other methods are used for interfacing between LAN products and the NMS, they shall be implemented in a secure manner.

5.3.1.10.13 Configuration Control

[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 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.

5.3.1.10.14 Operational Changes

[Required: PON] The PON shall meet the requirements in Section 5.3.1.6.2, Operational Changes.

5.3.1.10.15 Performance Monitoring

[Required: PON] The PON shall meet the requirements in Section 5.3.1.6.3, Performance Monitoring.

5.3.1.10.16 Alarms

[Required: PON] The PON shall meet the requirements in Section 5.3.1.6.4, Alarms. In addition to the alarms defined in this section, the OLT shall support the alarms as defined by ITU G994.4.

5.3.1.10.17 Reporting

[Required: PON] The PON shall meet the requirements in Section 5.3.1.6.5, Reporting. In addition, the PON system must also report optical errors to include degraded optical conditions.

5.3.1.10.18 Fiber Media

[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/IEC B1.1.

5.3.1.10.19 RF-over-Glass (RFoG) Video

[Conditional: 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 1150nm to 1560nm. 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 1500nm.

The spectrum is allocated as follows:

- 40 Analog channels at 54 to 550 Mhz
- 63 Digital 256 QAM channels at 225 to 870 Mhz
- One QPSK OOB channel at 71 to 125 Mhz

5.3.1.10.20 Traffic Engineering

[Required: PON] Bandwidth required per subscriber must be in compliance with Section 5.3.1.7.3, Traffic Engineering, and additional DoD regulations as applicable.

5.3.1.10.21 VLAN Design and Configuration

[Required: PON] VLAN Design and Configuration for all PON networks must be in compliance with Distribution and Access Layer Network Elements as defined in Section 5.3.1.7.4, VLAN Design and Configuration.

5.3.1.10.22 Power Backup

[Required: ASLAN Network PON – Conditional: Non-ASLAN Network PON] To meet CJCS requirements the PON network must be in compliance with Section 5.3.1.7.5, Power Backup, and Figure 5.3.1-14, ASLAN UPS Power Requirements. Required or Conditional adherence shall be based on whether the PON Network Element is being placed into an ASLAN or a Non-ASLAN.

5.3.1.10.23 Availability

Availability of a PON network will be determined the same as for active Ethernet networks as defined in Section 5.3.1.7.6, Availability, and Table 5.3.1-12, Methods of Expressing Availability. PON Network Elements that are utilized in ASLANs and Non-ASLANs must meet the availability requirements for the appropriate LAN.

[**Conditional: 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.

5.3.1.10.24 Redundancy

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

[Required: PON in ASLAN – Conditional: PON in Non-ASLAN] The PON network 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).

5.3.1.10.24.1 Single Product Redundancy

[Conditional: PON] Single product redundancy may be met with a modular chassis that at a minimum provides the following:

1. 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.

2. 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.

3. 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.

4. 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.

5.3.1.10.24.2 Dual Product Redundancy

[Conditional: 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 5.3.1.7.3, 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.

5.3.1.10.25 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.

[Required: PON] For PON Survivability, the PON shall support a Layer 2 Dynamic Rerouting protocol. Failover shall occur in no more than 50 ms.

5.3.1.10.26 Summary of LAN Requirements by Subscriber Mission

[Required: PON]

The PON Network Elements shall meet the same requirements as specified in Table 5.3.1-14, 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 5.3.5, IPv6 Requirements. The PON shall meet all IPv6 requirements applicable as defined for a LAN access switch (Table 5.3.5-6, LAN Switch).