Changes to UCR 2008, Change 1, Section 5.3.1, ASLAN Requirements

SECTION	CORRECTION	EFFECTIVE DATE
5.3.1.3	Change video latency and jitter to match E2E of 30 ms. Change access from 1 ms to 2 ms because of added L3.	Immediately
5.3.1.8	Added new section to address MPLS requirements	18-Month Rule

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

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 DISN in support of UC. As illustrated in Figure 5.3-1, Illustration of How Requirements for IP-Based APL Products are Defined Across Multiple UCR 2008 Sections, requirements for IP-based products are spread across several subsections of this document. As an example, requirements for an LSC 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.

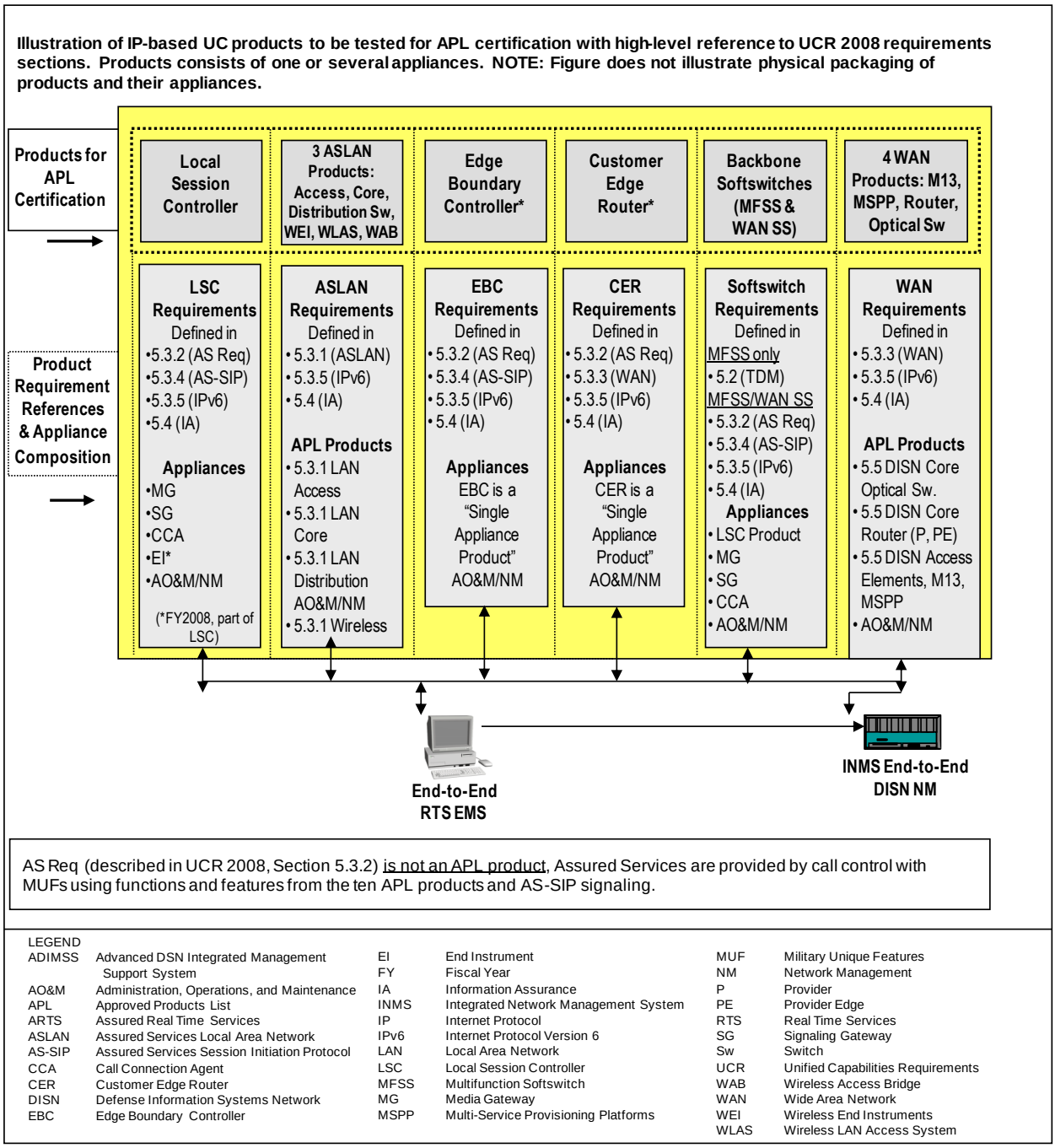
Section 5.3.1, Assured Services Local Area Network Infrastructure, defines basic requirements for LAN products and design guidance for an ASLAN; while IA requirements applicable to LAN products are found in Section 5.4, Information Assurance Requirements.

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.



LEGEND

ADIMSS	Advanced DSN Integrated Management Support System	EI	End Instrument	MUF	Military Unique Features
AO&M	Administration, Operations, and Maintenance	FY	Fiscal Year	NM	Network Management
APL	Approved Products List	IA	Information Assurance	P	Provider
ARTS	Assured Real Time Services	INMS	Integrated Network Management System	PE	Provider Edge
ASLAN	Assured Services Local Area Network	IP	Internet Protocol	RTS	Real Time Services
AS-SIP	Assured Services Session Initiation Protocol	IPv6	Internet Protocol Version 6	SG	Signaling Gateway
CCA	Call Connection Agent	LAN	Local Area Network	Sw	Switch
CER	Customer Edge Router	LSC	Local Session Controller	UCR	Unified Capabilities Requirements
DISN	Defense Information Systems Network	MFSS	Multifunction Softswitch	WAB	Wireless Access Bridge
EBC	Edge Boundary Controller	MG	Media Gateway	WAN	Wide Area Network
		MSPP	Multi-Service Provisioning Platforms	WEI	Wireless End Instruments
				WLAS	Wireless LAN Access System

Figure 5.3-1. Illustration of How Requirements for IP-Based APL Products are Defined Across Multiple UCR 2008 Sections

Table 5.3-1 provides a partial listing of appliance functions and UC APL Products.

Table 5.3-1. 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 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 and MFSS
AS-SIP Signaling Appliance	Appliance	Appliance function within an LSC and MFSS that provides AS-SIP signaling capabilities
Call Connection Agent	Appliance	Appliance function within an LSC 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
LAN Switch/Routers: Access, Distribution, and Core Devices	APL Products	Three APL products used in ASLANs
Secure End Instrument	APL Product	An APL product providing secure RTS 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
WAN Softswitch	APL Product	An APL product that acts an AS-SIP B2BUA within the UC architecture
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

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
DISN Optical Switch	APL Product	An APL product serving as an optical transport node.
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	Appliance part of LSC

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	RTS	Real Time Services
DISN	Defense Information System Network	WAN	Wide Area Network

5.3.1 Assured Services Local Area Network Infrastructure

5.3.1.1 Introduction

This section establishes the requirements for the products used in LANs 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:

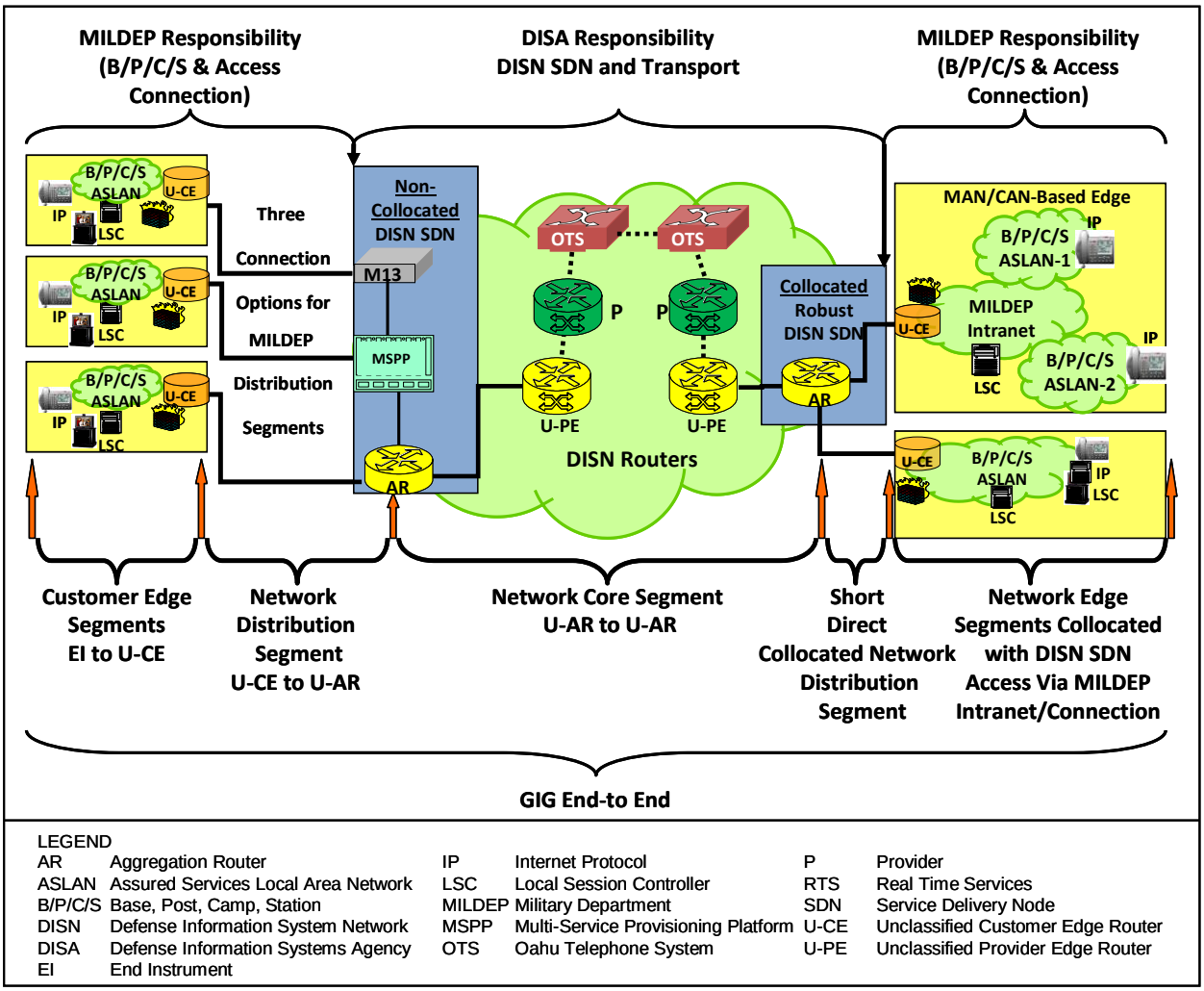
1. Define Product Requirements. Specifies the required and optional capabilities for network products that can be used in a LAN. This section is intended to support equipment certification.

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, which is owned and maintained 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.



LEGEND

AR	Aggregation Router	IP	Internet Protocol	P	Provider
ASLAN	Assured Services Local Area Network	LSC	Local Session Controller	RTS	Real Time Services
B/P/C/S	Base, Post, Camp, Station	MILDEP	Military Department	SDN	Service Delivery Node
DISN	Defense Information System Network	MSPP	Multi-Service Provisioning Platform	U-CE	Unclassified Customer Edge Router
DISA	Defense Information Systems Agency	OTS	Oahu Telephone System	U-PE	Unclassified Provider Edge Router
EI	End Instrument				

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.

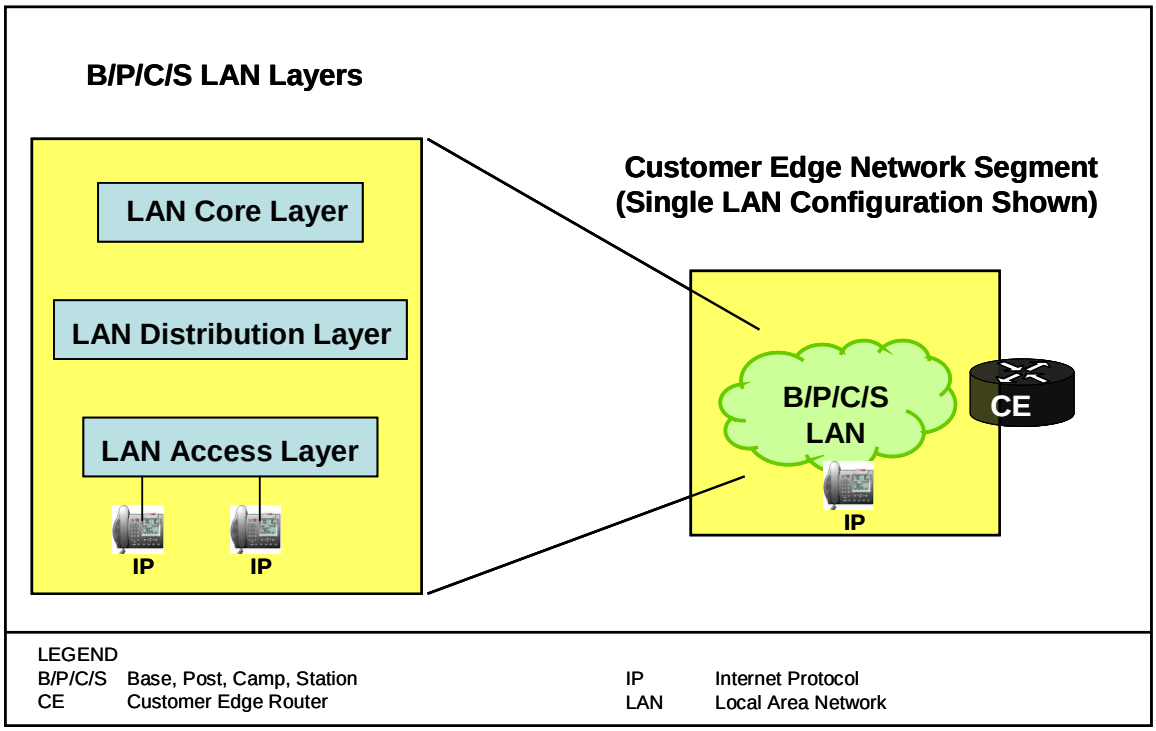


Figure 5.3.1-2. B/P/C/S LAN Layers and Relationship to Customer Edge Network Segment

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).

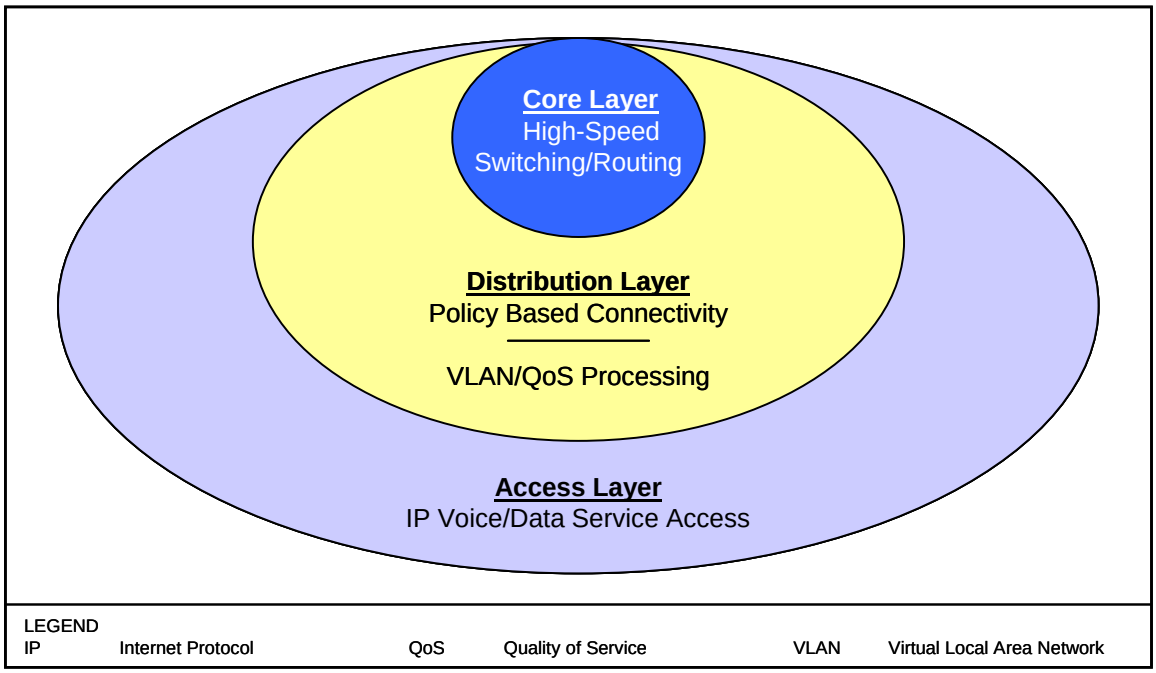


Figure 5.3.1-3. LAN Layers

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.

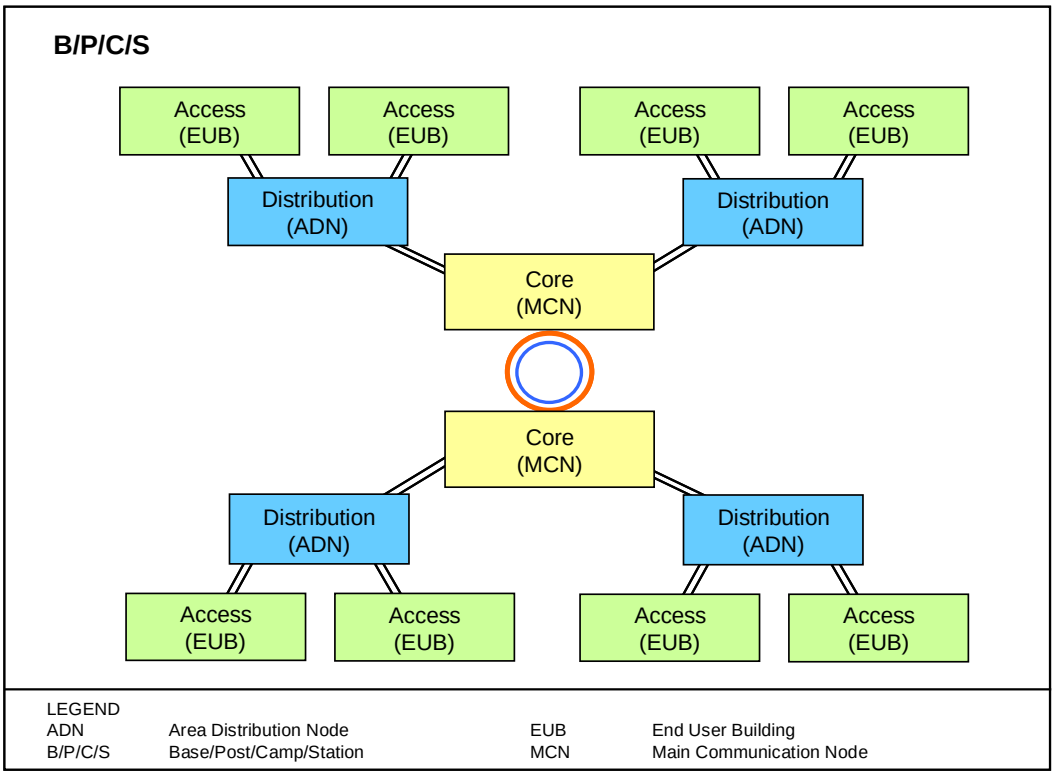


Figure 5.3.1-4. Representative B/P/C/S Design and Terminology

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.

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
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	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 a minimum of 50 percent (maximum voice and video traffic) of its maximum rated output capacity for egress ports that interconnect (trunk) the product to other products. Non-blocking is defined as the capability to send and receive 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports without losing any packets.

2. Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized voice packets (media and signaling), with no more than 2 milliseconds (ms) latency for Core, Distribution, and Access products. All Core, Distribution, and Access products shall have the capability to transport prioritized video packets (media and signaling), with no more than 10 ms latency for Core, Distribution, and Access products. The latency shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

3. Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized voice packets (media and signaling) with no more than 1 ms jitter across Core, Distribution, and Access products. All Core, Distribution, and Access products shall have the capability to transport prioritized video packets (media and signaling) with no more than 10 ms jitter across Core, Distribution, and Access products. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

4. Packet Loss. All Core and Distribution products shall have the capability to transport prioritized voice and video packets (media and signaling) with no more than 0.02 percent packet loss. Access products shall have the capability to transport prioritized voice and video packets with no more than 0.01 percent packet loss. The packet loss shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

5. Bit Error Rate (BER). All Core, Distribution, and Access products shall have the capability to transport prioritized voice and video packets (media and signaling) with a BER of no more than 1 bit error in 10^6 bits. The BER shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

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 may be provided as conditional interfaces):

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

[Required: Access Products] Minimally, Access products shall provide the following interface rates (other rates may be provided as conditional interfaces):

- 10 Mbps IAW IEEE 802.3i
- 100 Mbps IAW IEEE 802.3u

[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
- 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:

- 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 802.3ad (output/egress ports only)
- Spanning Tree Protocol IAW IEEE 802.1D
- Multiple Spanning Tree IAW IEEE 802.1s
- Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w
- Port-Based Access Control IAW IEEE 802.1x

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 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, Distribution, and Access 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.

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 5.3.1-7, TCI Field Description). Default values are provided in Table 5.3.1-4, 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, Distribution, and Access 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).

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:

Table 5.3.1-4. 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	SysLog	System Log
CoS	Class of Service	TCI	Tag Control Information
OA&M	Operations, Administration, and Maintenance	VTC	Video Teleconferencing
SNMP	Simple Network Management Protocol		

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 port-based VLANs, Media Access Control (MAC) address-based VLANs, and protocol-based VLANs.

5.3.1.3.5 Protocols

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet the DISR protocol requirements for IPv4 and IPv6.

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 "tagged" session to any of the queues.

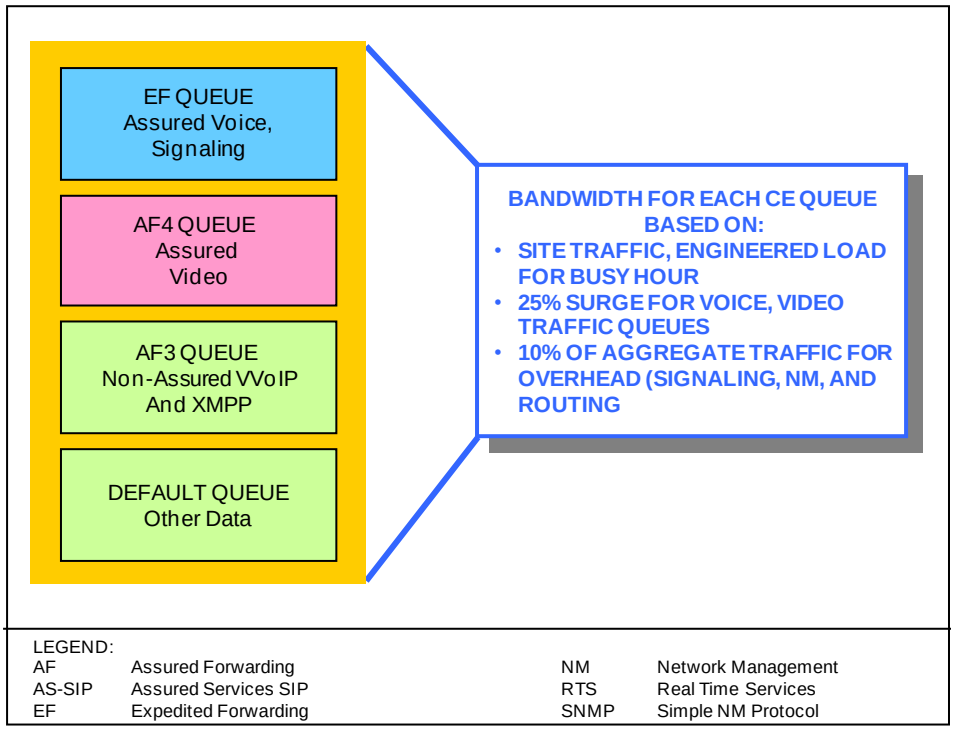


Figure 5.3.1-7. Four-Queue Design

3. Supporting Differentiated Services (DiffServ) per hop behaviors (PHBs) per RFCs 2474, 2494, 2597, 2598, and 3246.

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

4. Supporting a minimum of one of the following:

    a. Weighted Fair Queuing (WFQ) IAW RFC 3662

b. Priority Queuing (PQ) IAW RFC 1046
c. Class-Based WFQ IAW RFC 3366

5. 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).

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 (SNMP) IAW RFCs 1157, 2206, 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

5.3.1.3.8 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.

5.3.1.3.9 Product Requirements Summary

Table 5.3.1-6, 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	R	R	R
	10BaseT UTP	IEEE 802.3i	C	C	R
	100BaseT UTP	IEEE 802.3u	R	R	R
	100Base-FX	IEEE 802.3u	R	R	R
	1000Base-T UTP	IEEE 802.3ab	C	C	C
	1000Base-X Fiber	IEEE 802.3z	R	R	C
	10GBase-X	IEEE 802.3ae	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	R	R	R
	Filtering	RFC 1812	R	R	R
	Link Aggregation	IEEE 802.3ad	R	R	R
	Spanning Tree Protocol	IEEE 802.1D	R	R	R
	Multiple Spanning Tree Protocol	IEEE 802.1s	R	R	R
	Rapid Reconfiguration of Spanning Tree	IEEE 802.1w	R	R	R
	Port Based Access Control	IEEE 802.1x [1]	R	R	R
Traffic Prioritization	CoS Traffic Classes	IEEE 802.1D/Q	C	C	C
	DSCP	RFC 2474	R	R	R
VLANs	Port based	IEEE 802.1Q	R	R	R
	MAC based	IEEE 802.1Q	R	R	R
	Protocol based	IEEE 802.1Q	R	R	R
IPv4 Protocols	IPv4 requirements are contained within the DISR on-line RTS profiles for Core, Distribution, and Access products.	DISR	R	R	R
IPv6 Protocols	See IPv6 profiles contained in the DISR	DISR	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[2]	C[2]	C[2]
	CQ	RFC 3670	C[2]	C[2]	C[2]
	PQ	RFC 1046	C[2]	C[2]	C[2]
	CB-WFQ	RFC 3366	C[2]	C[2]	C[2]
Security	Security requirements are contained in the IA portion of the document.		R	R	R

NOTES
1 Only between end-user and product; not trunks.
2. One of these queuing mechanisms is required to implement EF PHB.

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A

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 ASLAN as measured under congested conditions. Congested condition is defined as 100 percent of link capacities (as defined by baseline traffic engineering (25percent voice/signaling, 25percent video, 25percent preferred data, and 25 percent best effort traffic). The latency shall be achievable over any 5-minute measured period under congested conditions.

5.3.1.4.1.2 Jitter

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets E2E 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 (25percent voice/signaling, 25percent video, 25percent preferred data, and 25 percent best effort traffic).

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 with packet loss not to exceed configured traffic engineered (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 (25percent voice/signaling, 25percent video, 25percent preferred data, and 25 percent best effort traffic).

5.3.1.4.1.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets E2E with a BER of no more than 3 bit errors in 10^6 bits. The BER 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 (25percent voice/signaling, 25percent video, 25percent preferred data, and 25 percent best effort traffic).

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

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

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

5.3.1.4.2.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets E2E with a BER of no more than 3 bit errors in 10^6 bits. The error rate 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

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 50 ms latency E2E across the ASLAN. 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 (as defined by baseline traffic engineering (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.4.3.2 Jitter

There are no jitter requirements for 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. 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 (25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

5.3.1.4.3.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets E2E with a BER of no more than 3 bit error in 10^6 bits.

5.3.1.5 Information Assurance Requirements

[Required: ASLAN and Non-ASLAN] All LAN 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 LAN 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 LAN 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 LAN 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 LAN 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 LAN 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). 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. 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] Local area network 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 LAN 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 LAN 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 Physical Media

[Required: ASLAN and Non-ASLAN] Wires used for the LAN shall not be lower than a CAT-5 performance (see Table 5.3.1-7, 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.

Table 5.3.1-6. Cable Grade Capabilities

CABLE NAME	MAKEUP	FREQUENCY SUPPORT	DATA RATE	NETWORK COMPATIBILITY
CAT-5	4 twisted pairs of copper wire -- terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	ATM, Token Ring, 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	MHz	Megahertz
Base	Baseband	RJ	Registered Jack
CAT	Category	T	Ethernet half-duplex
Mbps	Megabits per second	TX	Ethernet full-duplex

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 EIs 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, WABs, and WLANs) are contained in the following sections.

5.3.1.7.2.1 General Wireless Product Requirements

[Required: WLANs] The following general wireless requirements must be met by WLANs and WLAN 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.

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 mission critical telephony users, the wireless products shall provide redundancy and WLAS and/or associated WLAN 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; redundancy protocol; and no single point of failure for more than 96 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.

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, 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 shall not increase latency by more than 10 ms above the specified maximum latency for a wired LAN.

7. The WLAN 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.

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 5.3.1-7, 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		

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	802.16 SERVICE	RADIO SERVICE TRAFFIC PRIORITY	WIRED LANs DEFAULT DSCPs	
				BASE 2	BASE 10
	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 WLAN 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). This requirement does not apply to connections between 802.11 WABs.

5.3.1.7.2.2 WLAS, WAB Wireless Intrusion Detection System

[Required: WLAS, WAB] The WLAS and/or WAB wireless network shall be monitored by a Wireless Intrusion Detection System (WIDS). The system will have the following capabilities:

1. Continuous scanning: The WIDS will scan continuously around-the-clock to detect authorized and unauthorized activity.

2. Location-sensing WIDS: The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless products.

3. Deployed systems shall be properly engineered so that the WLAN and wireless products achieve the required performance requirements in their specific structural environment. Users shall submit their network design with their request for DSN connection. The Unified Capabilities Connection Office (UCCO) submittal shall include wireless security compliancy FIPS 140 and proposed accessibility as well as WIDS National Information Assurance Partnership (NIAP) Common Criteria validation for basic robustness. Medium robustness will be applied, as determined by the Designated Approving Authority (DAA), when the NIAP Common Criteria for that level is approved.

5.3.1.7.2.3 Wireless Interface Requirements

[Required: WEI, WLAS, and WAB]

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 (WEI, WLAS, WAB)
   b. 802.11b (WEI ,WLAS)
   c. 802.11g (WEI, WLAS, WAB)
   d. 802.16 (WEI, WLAS, WAB)

2. For any of the 802.11 interfaces, the wireless product must 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 Table 5.3.1-6, Cable Grade Capabilities, 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 802.16d – 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, & 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. Nomadic WEIs must support 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.

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.

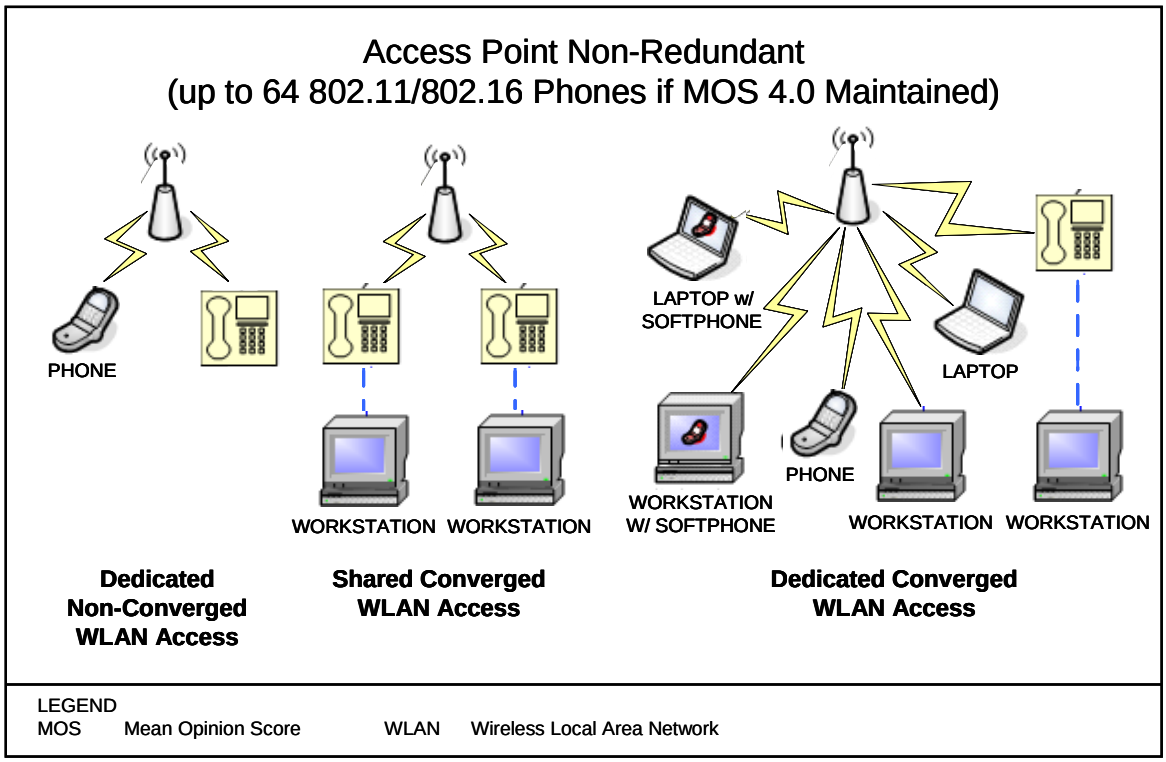


Figure 5.3.1-8. Access Methods for the Wireless Access Layer End Item Product Telephones

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.

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] If provided, the WAB will be required to meet all the requirements for each individual type interface.

1. For any of the 802.16 interfaces, the WAB must support any of the following 802.16 standards:

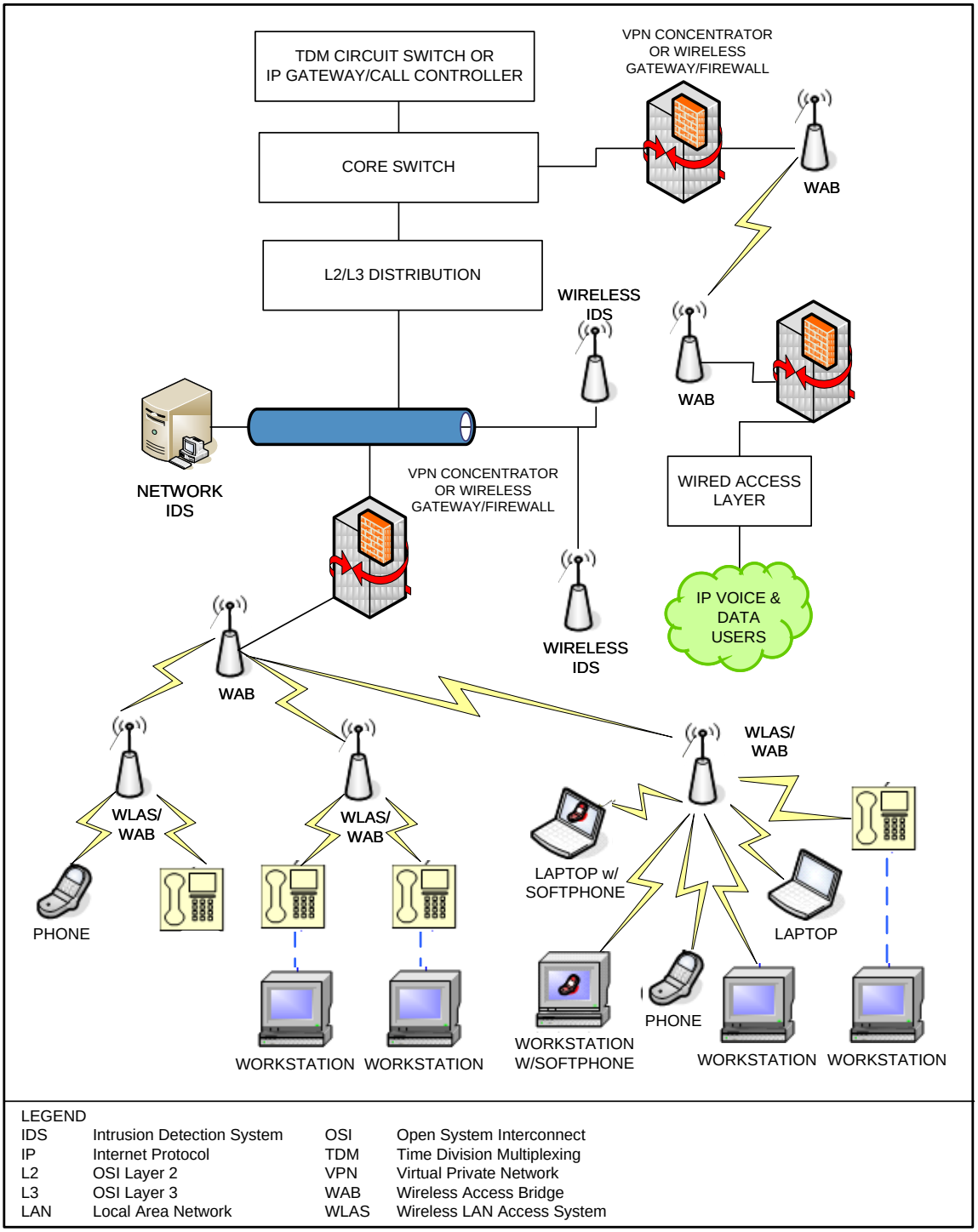


Figure 5.3.1-9. Example of Combined WLAS/WAB and Second Layer WAB

a. 802.16d – Part 16: Air Interface for Fixed Broadband Wireless Access Systems, or

b. 802.16e – 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.

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 Section 5.2.6, 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.

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.

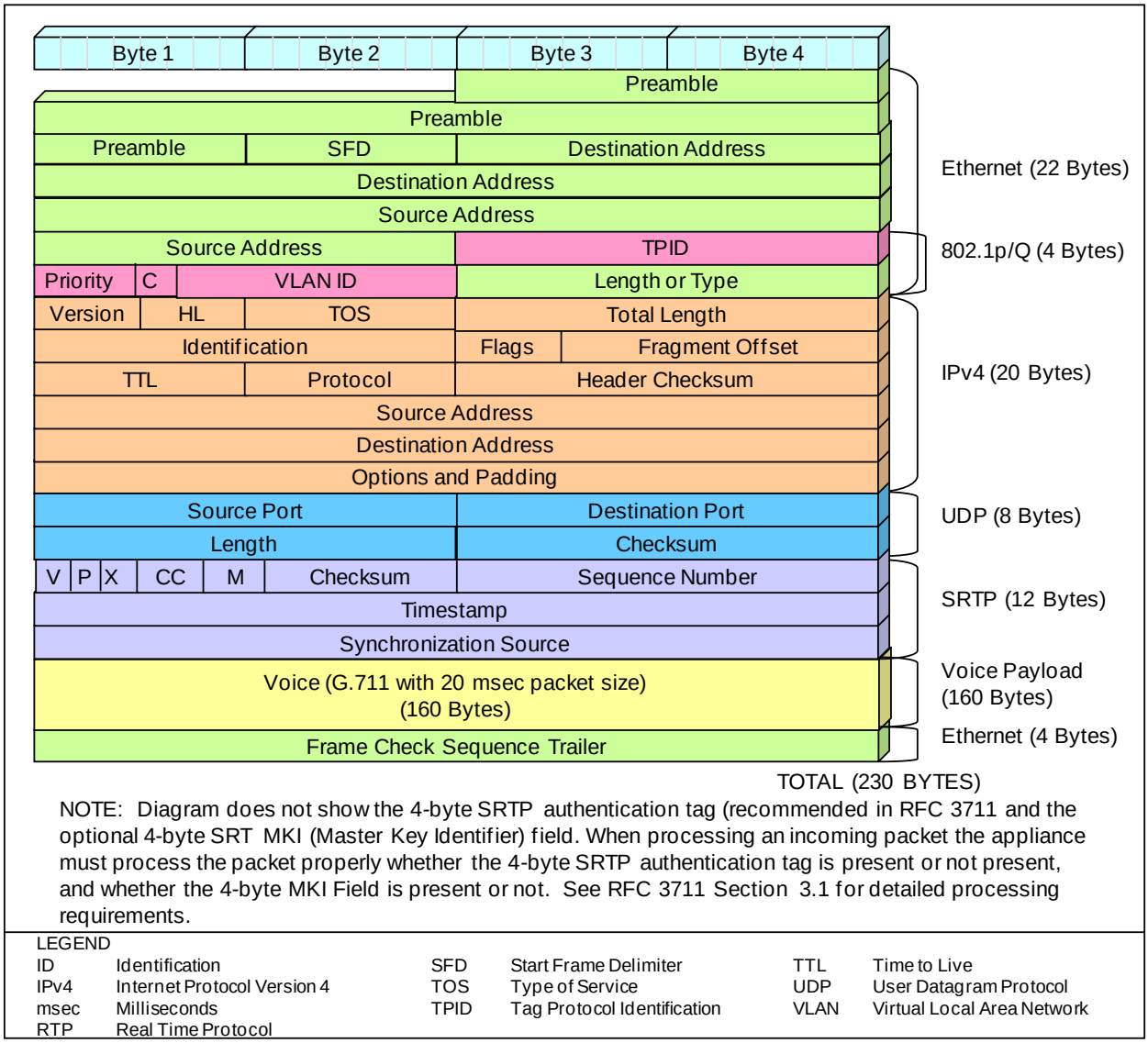


Figure 5.3.1-10. Voice over IP Packet Size

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. 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
	IP Subscriber (converged)	100 Mbps	1[4]	1

PRODUCT	LINK TYPE	LINK SIZE	# MISSION CRITICAL VoIP SUBSCRIBERS (ASLAN)	# R AND NON-MISSION CRITICAL VoIP SUBSCRIBERS (NON-ASLAN)
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.

- Numbers in bold represent the minimum recommended trunk sizes.
- Link pairs may use stand-by link or load balancing. Number of subscribers is calculated at one half the total link pair capacity.

LEGEND:

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

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

VIDEO STREAM BANDWIDTH	IP OVERHEAD	TOTAL IP BANDWIDTH
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 link or load balancing. Number of subscribers is calculated at one half the total link pair capacity.				
LEGEND ASLAN Assured Services LAN BW Bandwidth Gbps Gigabits per second IP Internet Protocol			kbps kilobits per second Mbps Megabits per second NA Not Applicable	

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

2. Security. 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).

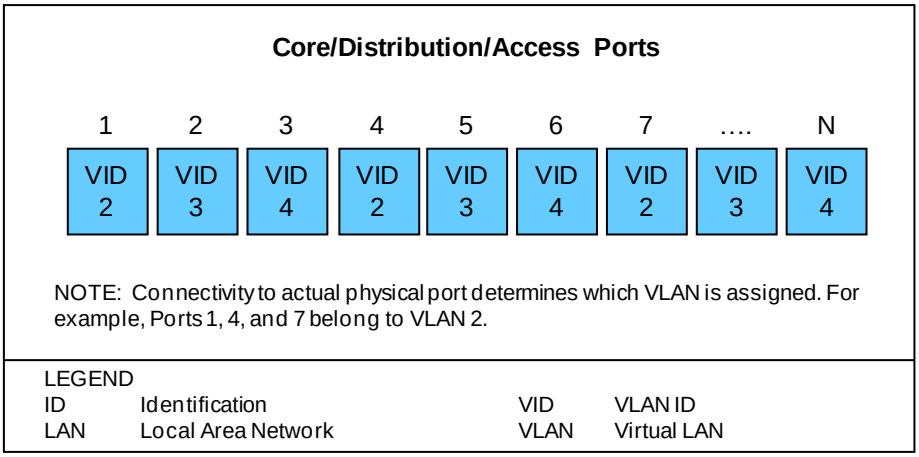


Figure 5.3.1-11. Port-Based VLANs

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

   [Required: ASLAN] 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).

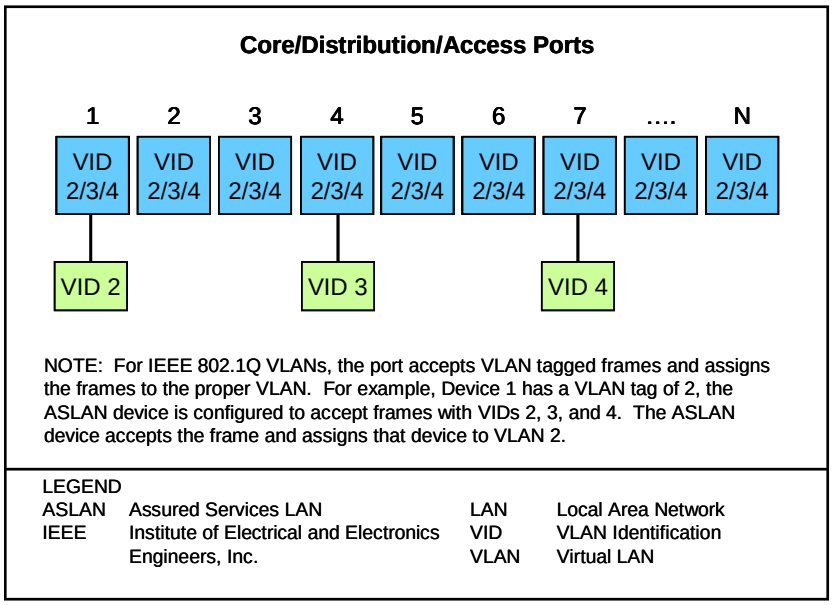


Figure 5.3.1-12. IEEE 802.1Q-Based VLANs

3. By a User-Defined Value. This type of VLAN is typically the most flexible, allowing VLANs to be defined based on the value of any field in a packet or frame. For example, VLANs could be defined on a protocol basis or could be dependent on a particular address (Layer 2 or Layer 3). The simplest form of this type of VLAN is to group users according to their 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.

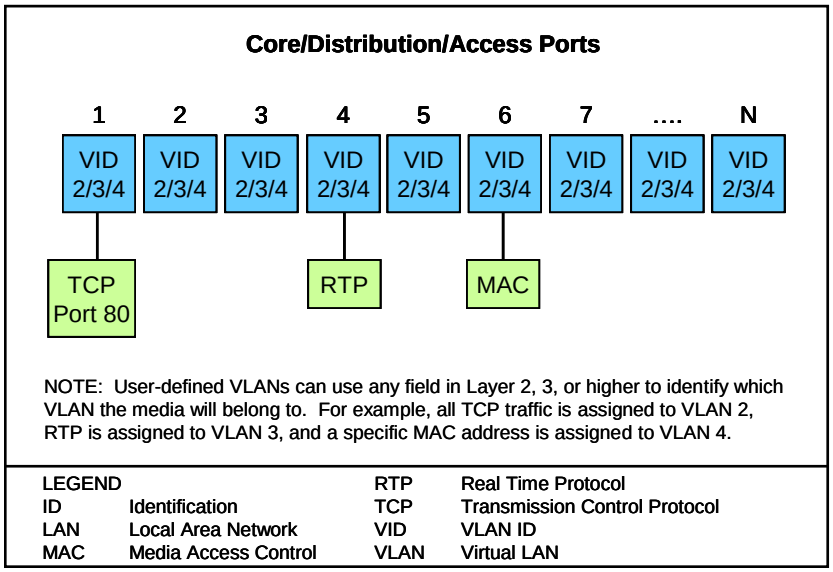


Figure 5.3.1-13. User-Defined VLANs

The recommended 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 uninterruptible power systems (UPSs) are bare minimum requirements. 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.

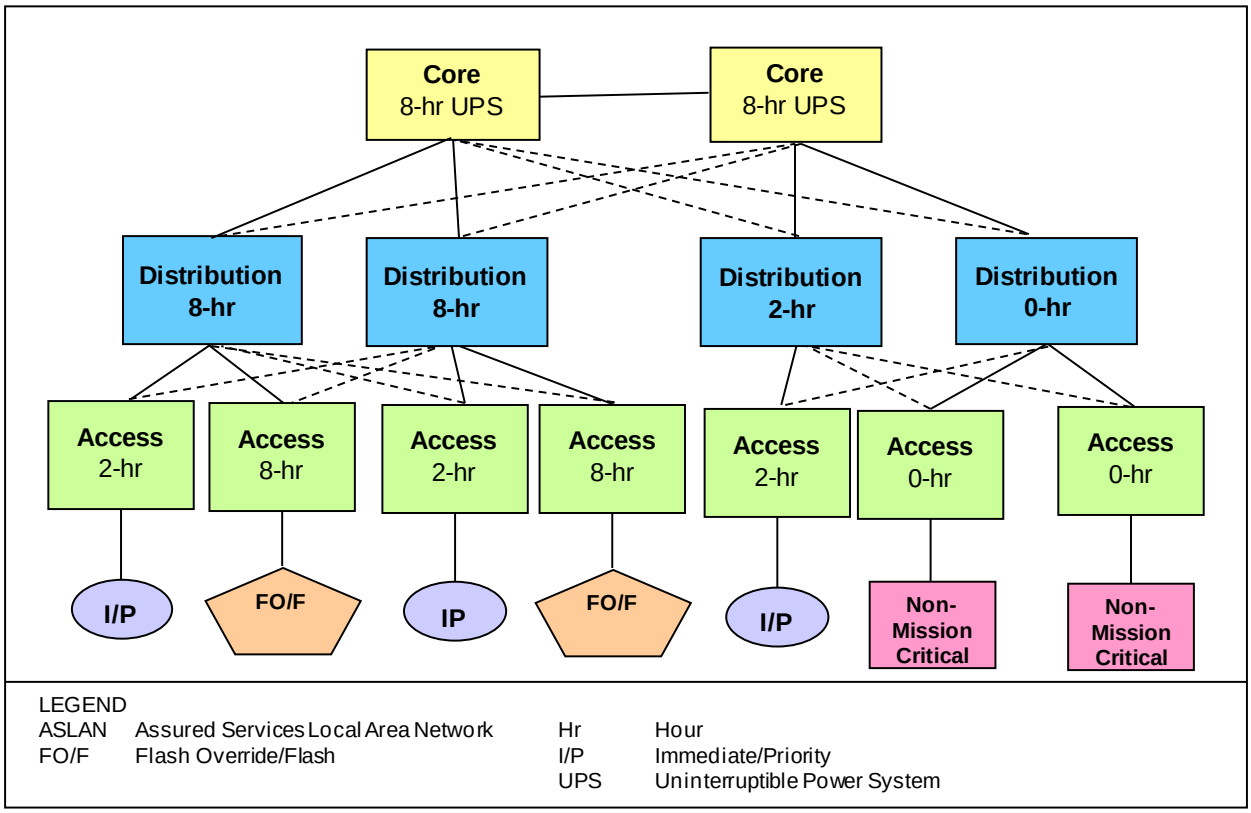


Figure 5.3.1-14. ASLAN UPS Power Requirements

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.

   NOTE: Backup Power (Environmental). Environmental systems needed 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	99.997%	15 mins, 46 secs
6	99.999%	5 mins, 15 secs
7	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 shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. 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.

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. Dual Power Supplies. The platform shall provide a minimum of two power supplies each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis.

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).

3. Termination Sparing. 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.

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 nondesign 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. Layer 3 Dynamic Rerouting. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DISR to provide survivability. The routing protocols of choice per the DISR are:

    a. Border Gateway Protocol (BGP) for interdomain routing

    b. Open Shortest Path First (OSPF), Version 2, for IPv4 and (OSPF), Version 3, for IPv6 or Intermediate System-Intermediate System (IS-IS) (IAW RFC 1629) for intradomain routing

2. Layer 2 Dynamic Rerouting.

    a. Virtual Router Redundancy Protocol (VRRP) – RFCs 2787 and 3768. 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 Figures 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.

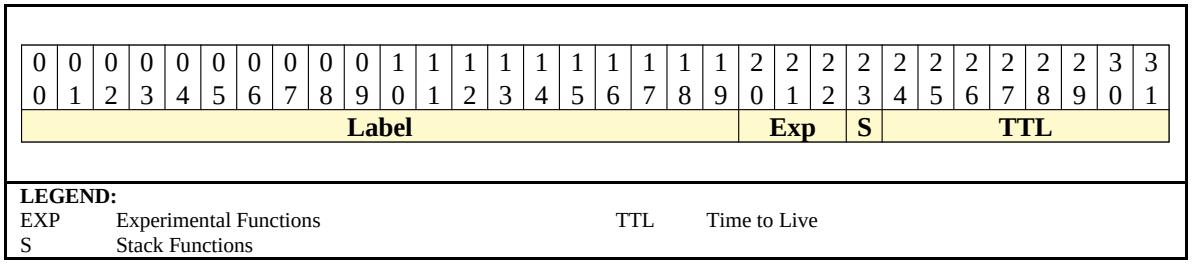


Figure 5.3.1-15. MPLS Header

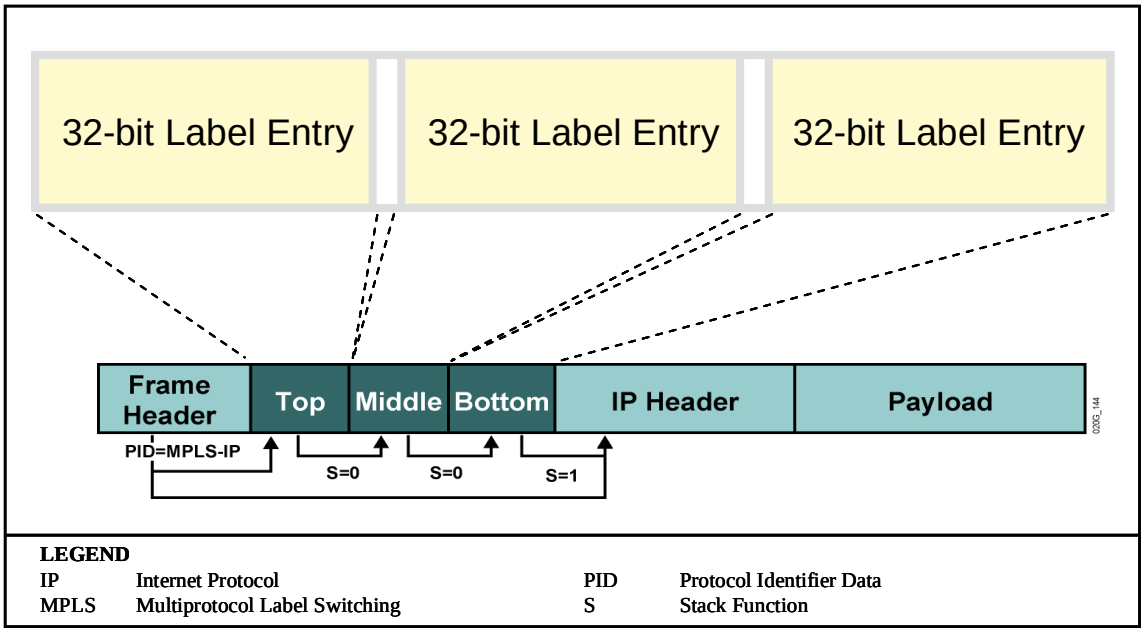


Figure 5.3.1-16. MPLS Header Stacking

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.

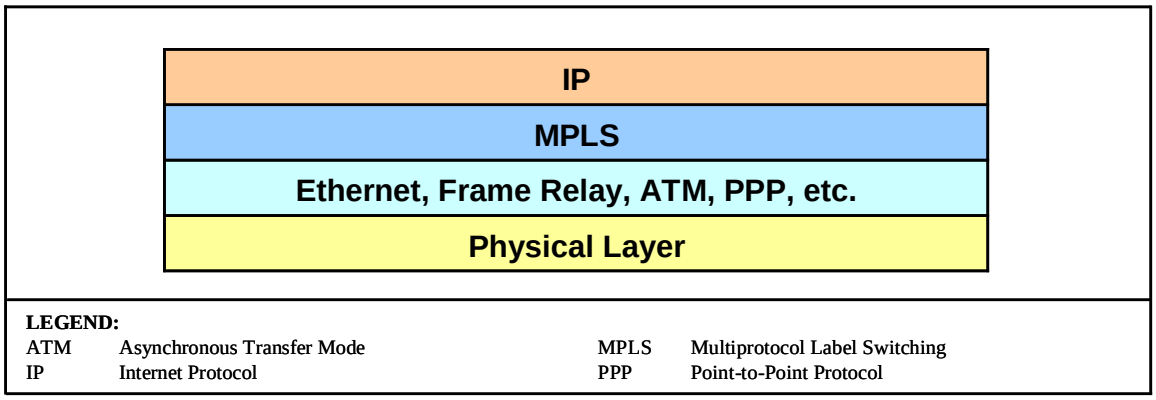


Figure 5.3.1-17. MPLS OSI Layer

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 Architecture

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 Architecture, depicts DoD's ASLAN MPLS architecture. 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 20 ms upon indication of the primary LSP failure.

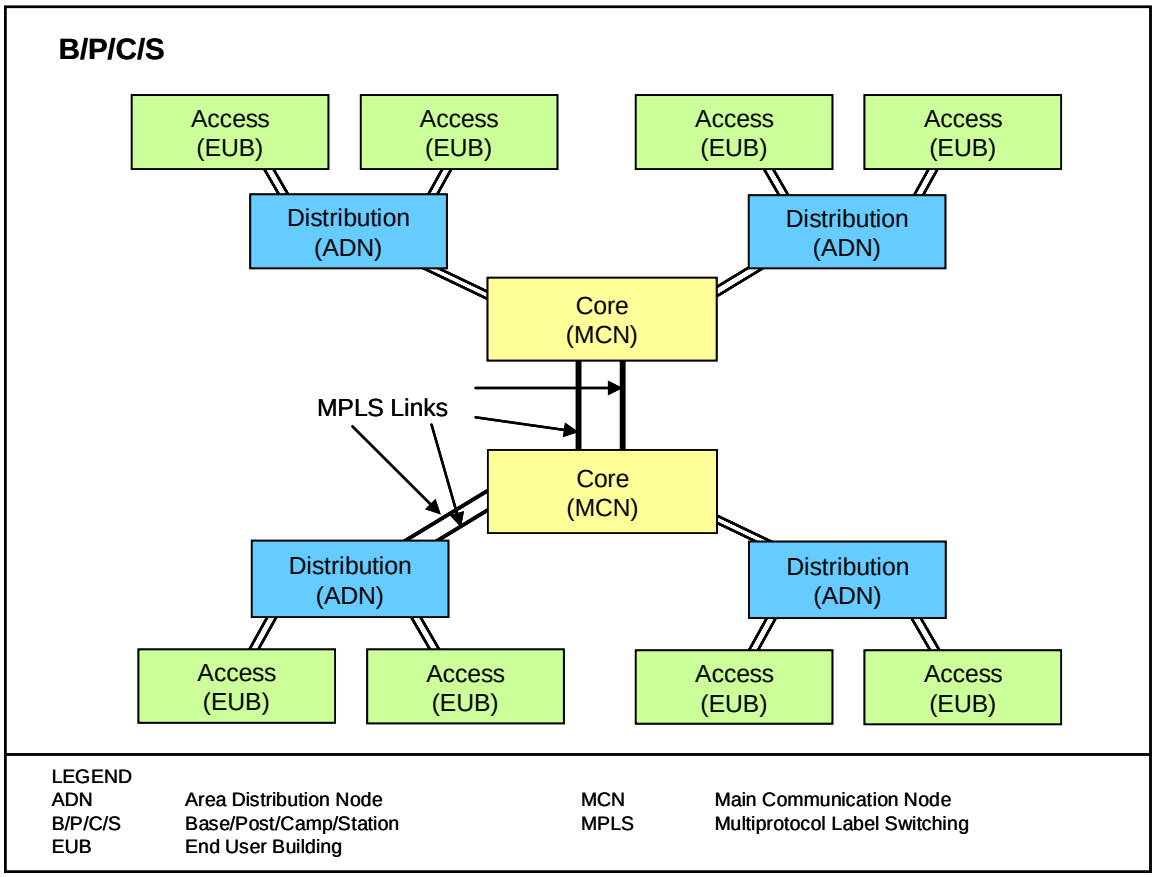


Figure 5.3.1-18. ASLAN MPLS Architecture

[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	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
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"	CR	VPLS	Required if L2VPN implemented via LDP
RFC 4761, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" (Updated by RFC 5462)	CR	VPLS	Required if L2VPN implemented via BGP
RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)	CR	BGP/MPLS VPNs	Required if L3VPN implemented

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
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	
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

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
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	
RFC 2747, "RSVP Cryptographic Authentication" and RFC 3097, RSVP Cryptographic Authentication (Updated Message Type Value).	CR	RSVP	Required if RSVP implemented

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
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]

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

- RFC 4761, "Virtual Private LAN Services (VPLS) Using BGP for Auto-Discovery and Signaling"; or
- RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) 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]

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]

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)"

THIS PAGE INTENTIONALLY LEFT BLANK