CHAPTER 22

Network-Based Protocol Suite

LIST OF FIGURES

LIST OF TABLES

CHAPTER 22

Network-Based Protocol Suite

22.1 General

The *Telemetry Network Standards* (TmNS) leverages existing standardized Internet protocols to serve as the core set of communication protocols used by *NetworkNodes* within a *TmNS Network*. The TmNS's network-based protocol suite incorporates a large portion of the TCP/IP Protocol Suite (also known as the Internet Protocol Suite) along with other supporting technologies (e.g., underlying data link and physical layer technologies). Figure 0-1 illustrates the Open Systems Interconnection (OSI) Model, the corresponding TCP/IP Model, and the major components of the TCP/IP Protocol Suite.

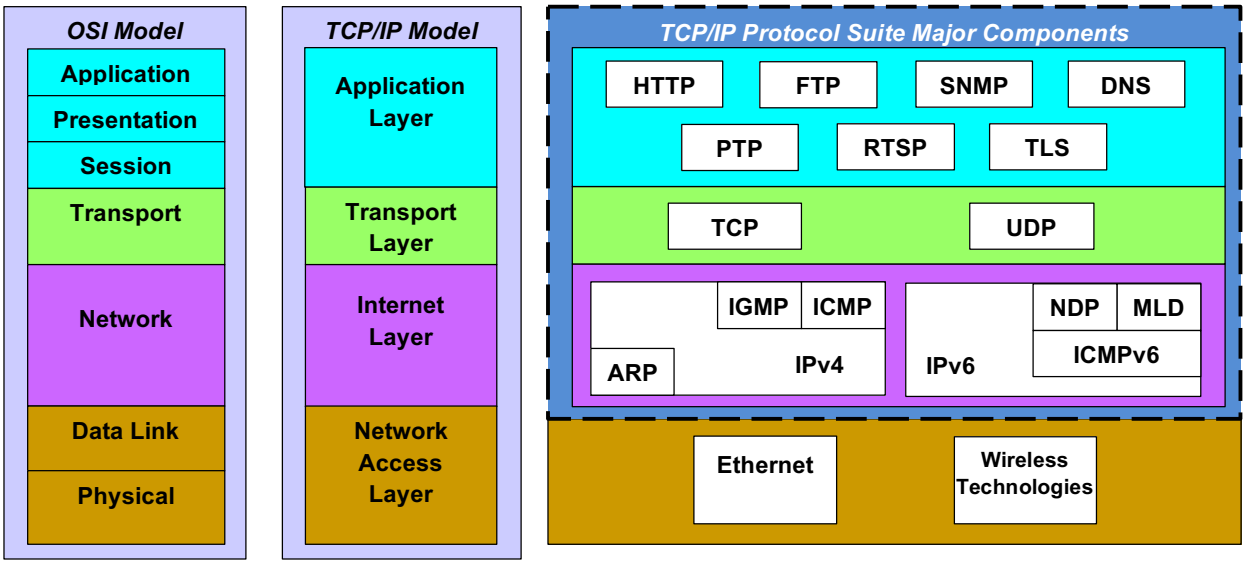


Figure 0-1. OSI and TCP/IP Model with TCP/IP Protocol Suite

This document follows the TCP/IP Model layering convention and consists of the following major sections:

- **Network Access Layer**: Consists of the Physical and Data Link layers that define the underlying hardware networking technology. The networking scope of this layer is limited to the local network connection.

- **Internet Layer Protocols**: Responsible for sending datagrams across potentially multiple networks. Internetworking (i.e., routing) requires sending data from the source network to the destination network.

- **Transport Layer Protocols**: Establishes a basic data channel that an application uses to exchange data.

- **Application Layer Protocols**: Includes protocols used by applications for exchanging application data over the network connections established by the lower level protocol. Basic network support services are also included (e.g., routing and host configuration protocols).

The bit numbering, bit ordering, and byte ordering conventions used in this chapter are described in Appendix 21B.

22.1.1 General *NetworkNode* Requirements

NetworkNodes with host functionality shall conform to the following standards that specify host functionality requirements:

- RFC 1122: Requirements for Internet Hosts – Communication Layers
- RFC 1123: Requirements for Internet Hosts – Application and Support

22.1.2 General *NetworkDevice* Requirements

NetworkDevices that support IPv4 routing shall conform to the following standard that specifies routing functionality requirements:

- RFC 1812: Requirements for IP Version 4 Routers

22.2 Network Access Layer

22.2.1 Physical Layer

Connectors and cable media should meet the electrical or optical properties required by the applicable standards referenced herein. However, applicability to the selected operational environment will place additional constraints on the selection of the connectors and cable media.

22.2.1.1 Wired Ethernet

NetworkNodes shall support one or more of the bit rate and physical protocol standards specified below.

22.2.1.1.1 100 Mbps Ethernet

22.2.1.1.1.1 100BASE-TX

Copper media connections using 100BASE-TX Ethernet shall comply with:

- IEEE 802.3-2012, Section 2, Clause 25

22.2.1.1.1.2 100BASE-FX

Multi-mode fiber media connections using 100BASE-FX Ethernet shall comply with:

- IEEE 802.3-2012, Section 2, Clause 26

22.2.1.1.2 Gigabit Ethernet

22.2.1.1.2.1 1000BASE-T

Copper media connections using 1000BASE-T Ethernet shall comply with:

- IEEE 802.3-2012, Section 3, Clause 40

22.2.1.1.2.2 1000BASE-SX

Multi-mode fiber media connections using 1000BASE-SX Ethernet shall comply with:

- IEEE 802.3-2012, Section 3, Clause 38

22.2.1.1.2.3 1000BASE-LX

Multi-mode or single-mode fiber media connections using 1000BASE-LX Ethernet shall comply with:

- IEEE 802.3-2012, Section 3, Clause 38

22.2.1.1.3 10 Gigabit Ethernet

22.2.1.1.3.1 10GBASE-T

Copper media connections using 10 Gigabit Ethernet shall comply with:

- IEEE 802.3-2012, Section 5, Clause 55

22.2.1.1.3.2 10GBASE-SR, 10GBASE-LR, 10GBASE-ER

Fiber media connections using 10 Gigabit Ethernet shall comply with:

- IEEE 802.3-2012, Section 5, Clause 52

22.2.1.1.4 Auto-Negotiation

22.2.1.1.4.1 Copper Auto-Negotiation

Copper media connections, as described in the preceding sections, shall support auto-negotiation of speed, duplex, and flow control in the manner specified in:

- IEEE 802.3-2012, Section 2, Clause 28

22.2.1.1.4.2 Fiber Auto-Negotiation

Gigabit and 10 Gigabit fiber media connections, as described in the preceding sections, should support auto-negotiation of speed, duplex, and flow control in the manner specified in:

- IEEE 802.3-2012, Section 3, Clause 37

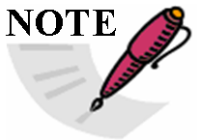
22.2.1.2 Wireless Technologies

22.2.1.2.1 Radio Frequency Waveform

Radio Access Network radios shall comply with the RCC-TG variant of the Shaped Offset Quadrature Phase Shift Keying (SOQPSK-TG) ternary constant phase modulation as defined in:

- IRIG 106 Part 1, Chapter 2, Section 2.4.3.2

Chapter 27, RF Network Access Layer, provides more details regarding the characteristics of the SOQPSK-TG single-carrier waveform.

NOTE 	Future revisions of this standard may include 802.11 technologies (wireless Ethernet).

22.2.2 Data Link Layer Protocols

NetworkNodes shall support the Ethernet data link protocols as specified in:

- IEEE 802.3-2012

22.2.2.1 Frame Structure

NetworkNodes shall support the frame structure, field definitions, and MAC conventions specified in:

- IEEE 802.3-2012, Section 1, Clauses 2, 3, and 4

Data link frames shall support 48-bit locally and universally administered addresses in a manner consistent with:

- IEEE 802.3-2012, Section 1, Clause 3, Paragraph 3.2.3, and Clause 4, Paragraph 4.2

Data link frame structures shall support type-encapsulated and length-encapsulated frames as specified in:

- IEEE 802.3-2012, Section 1, Clause 3, Paragraph 3.2.6

22.2.2.2 Media Access Control (MAC)

NetworkNodes shall support the MAC protocols specified in:

- IEEE 802.3-2012, Section 1, Clauses 2, 3, and 4

The MAC protocols shall convey type and length-encapsulated frames to support IP network layer protocols.

22.2.2.3 Logical Link Control (LLC)

NetworkNodes shall support the LLC protocols as specified in:

- IEEE 802.2-1998 to the extent necessary to support IP network layer protocols

22.2.2.4 Link Layer Switching

NetworkDevices that perform link layer switching shall conform to the requirements set forth in:

- IEEE 802.1D-2004 for *Rapid Spanning Tree Protocol* (RSTP) functionality

22.2.2.5 Link Layer Bridging

NetworkDevices that perform link layer bridging shall conform to the requirements set forth in:

- IEEE 802.1D-2004 for transparent bridging

22.2.2.6 Link Layer Flow Control

NetworkNodes that support full-duplex Ethernet shall support flow control “PAUSE” frames as specified in:

- IEEE 802.3-2012, Section 3, Clause 31

22.2.2.7 Address Resolution

22.2.2.7.1 Address Resolution Protocol (ARP) for IPv4

NetworkNodes that support IPv4 shall conform to the following core address resolution standard:

- RFC 826: Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48-bit Ethernet Address for Transmission on Ethernet Hardware

22.2.2.7.2 Neighbor Discovery Protocol (NDP) for IPv6

NetworkNodes that support IPv6 shall conform to the following core link-layer address resolution standards:

- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration

22.3 Internet Layer Protocols

22.3.1 Internet Protocol version 4 (IPv4)

NetworkNodes shall conform to the following IPv4 core standards:

- RFC 791: Internet Protocol
- RFC 919: Broadcasting Internet Datagrams
- RFC 922: Broadcasting Internet Datagrams in the Presence of Subnets

22.3.1.1 Internet Control Message Protocol (ICMP)

NetworkNodes shall conform to the following core ICMP standard:

- RFC 792: Internet Control Message Protocol

NetworkNodes shall include support for ICMP broadcast pings.

22.3.1.2 Internet Group Management Protocol (IGMP)

NetworkNodes that consume or forward dynamically configured IPv4 multicast datagrams shall conform to the following core IGMP standard:

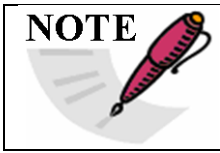
- RFC 3376: Internet Group Management Protocol, Version 3

22.3.1.2.1 IGMP Snooping

Switching *NetworkDevices* should use IGMP "snooping" as presented in:

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

Switching *NetworkDevices* that implement IGMP Snooping shall use at least one of the methods B or C in Section 2.1.1.1 of RFC 4541.

NOTE 	IGMP Snooping is recommended for performance considerations in a dynamically configured IPv4 multicast environment.

22.3.2 Internet Protocol version 6 (IPv6)

NetworkNodes that support IPv6 shall conform to the following IPv6 core standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification

22.3.2.1 Internet Control Message Protocol Version 6 (ICMPv6)

NetworkNodes that support IPv6 shall conform to the following core ICMPv6 standard:

- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

22.3.2.2 Multicast Listener Discovery (MLD) for IPv6

NetworkDevices that support IPv6 should conform to the following Multicast Listener Discovery standards:

- RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast

22.3.3 IP Datagram Transmission

NetworkNodes shall conform to the following core standards for the transmission of IP datagrams:

- RFC 894: A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC 1042: A Standard for the Transmission of IP Datagrams over IEEE 802 Networks

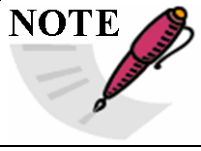
22.3.4 Protocol Independent Multicast (PIM)

NetworkDevices that perform routing functions shall conform to the following core Protocol Independent Multicast standard:

- RFC 4601: Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification (Revised)

22.3.5 Network Routing

NetworkNodes (which includes *NetworkDevices*) shall be capable of being configured to use static routes as defined in Section 7.4 *Static Routing* of RFC 1812: Requirements for IP Version 4 Routers.

NOTE 	It is expected that this capability is a default capability provided by the host operating system (e.g. the linux *route* command).

NetworkDevices that provide network-layer services shall be capable of being configured to use static routes for unicast and multicast traffic.

NetworkDevices that provide IPv4 routing functionality should be capable of running the following interior routing protocol: RFC 2328: OSPF Version 2.

NetworkDevices that provide IPv6 routing functionality should be capable of running the following interior routing protocol: RFC 5340: OSPF Version 3.

22.4 Transport Layer Protocols

22.4.1 Transmission Control Protocol (TCP)

NetworkNodes that implement TCP shall conform to the following core TCP standard:

- RFC 793: Transmission Control Protocol

NetworkNodes using TCP shall conform to the following standard for TCP congestion control:

- RFC 5681: TCP Congestion Control

22.4.2 User Datagram Protocol (UDP)

NetworkNodes that implement UDP shall conform to the following core UDP standard:

- RFC 768: User Datagram Protocol

22.4.3 Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

NetworkNodes that implement TLS and/or SSL shall conform to the following standards for cryptographic protocols:

- RFC 6101: The Secure Sockets Layer (SSL) Protocol Version 3.0
- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

NOTE	It is anticipated that the TmNS will upgrade and follow the latest government guidance for selection of the exact SSL and TLS versions to use.

Certificate generation and exchanges shall be in accordance with the profile identified in the following standard:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

22.5 Application Layer Protocols

22.5.1 Core *NetworkNode* Protocols

22.5.1.1 Host/Address Configuration

NetworkNodes requiring IPv4 addressing should conform to the following addressing standard:

- RFC 4632: Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan

NetworkNodes requiring IPv6 addressing should conform to the following addressing standard:

- RFC 4291: IP Version 6 Addressing Architecture

22.5.1.1.1 Static Configuration

NetworkNodes requiring IPv4 address configuration shall support static IP address assignment, conforming to the following core addressing standard:

- RFC 950: Internet Standard Subnetting Procedure

NetworkNodes requiring IPv6 address configuration shall support static IP address assignment.

22.5.1.1.2 Dynamic Configuration

A *TmNS Network* incorporating IPv4 shall support dynamic IP address assignment, conforming to the following standard for automatic host configuration:

- RFC 2131: Dynamic Host Configuration Protocol

A *TmNS Network* incorporating IPv6 shall support IPv6 Stateless Address Autoconfiguration (SLAAC) as specified in Section 22.2.2.7.2.

A *TmNS Network* incorporating IPv6 that requires dynamic IP address assignment shall conform to the following standard for automatic host configuration:

- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

22.5.1.2 Domain Name Services

NetworkNodes that use domain name labels shall conform to the following core name service standards:

- RFC 1034: Domain names – concepts and facilities
- RFC 1035: Domain names – implementation and specification

22.5.1.3 Time Synchronization

NetworkNodes requiring network time synchronization shall support network time synchronization as specified in:

- IEEE 1588-2008: Precision Time Protocol (PTP) Version 2

22.5.1.3.1 IEEE 1588 Master Clock

NetworkNodes performing as IEEE 1588 masters shall support the master clock interface as specified in:

- IEEE 1588-2008: Precision Time Protocol (PTP) Version 2

IEEE 1588-2008 master clocks:

- shall be able to synchronize with an external source.

- should synchronize with the Global Positioning System external time reference (see Section 22.5.1.3.5).
- shall use the PTP epoch when performing as the IEEE 1588 grandmaster clock.
- shall use an internal reference clock that tracks a best estimate of Global Positioning System time in the absence of an external time synchronization reference.

22.5.1.3.2 IEEE 1588 Slave Clock

NetworkNodes requiring time synchronization to an IEEE 1588-2008 master clock shall support the slave clock interface as specified in:

- IEEE 1588-2008: Precision Time Protocol (PTP) Version 2

Slave clocks shall continue to run freely using the last known time in the absence of a grandmaster clock on the network.

22.5.1.3.3 IEEE 1588 Boundary Clock

NetworkDevices that transport time synchronization data to devices requiring a high degree of synchronization shall support boundary clock techniques or approaches that are interoperable with boundary clocks (e.g., transparent clock implementations) as specified in:

- IEEE 1588-2008: Precision Time Protocol (PTP) Version 2

22.5.1.3.4 One Pulse-Per-Second (1 PPS) Outputs on IEEE 1588 Devices

NetworkNodes with IEEE 1588-2008 master or slave clocks should support external 1 PPS outputs to allow verification of time signal lock between distributed clocks within one microsecond.

- 1 PPS outputs should be compatible with standard 0-to-5VDC transistor-transistor logic (TTL) levels.
- The rising edge of the pulse shall define the beginning of a second.
- The duty cycle of the 1 PPS signal shall be between 5% and 95%.
- The pulse rise time between the 10% and 90% amplitude points shall be less than or equal to one microsecond.

22.5.1.3.5 Global Positioning System (GPS)

The GPS external time reference interface shall implement the GPS Space Segment (SS) RF waveform interface and the GPS Navigation User Segment (US) interface as specified in:

- IS-GPS-200H, NAVSTAR Global Positioning System (GPS) Interface Specification

22.5.1.3.6 TmNS Time Format

The TmNS-specific Time Format describes a time format for encoding timestamps in a textual representation.

```
TmNStimestamp = TmNSdate "T" TmNStime
TmNSdate      = 8DIGIT ; < YYYYMMDD >
TmNStime      = 6DIGIT [ "." 1*9DIGIT ] ; < hhmmss.fraction >
   where:
      YYYY is the four-digit year
      MM is month (01-12)
      DD is day of the month (01-31)
```

```
hh is hours on a 24-hour clock (00-23)
mm is minutes (00-59)
ss is seconds (00-59)
fraction is the fractional portion of the seconds
```

22.5.1.4 Information Assurance and Encryption

22.5.1.4.1 High Assurance Internet Protocol Encryptor (HAIPE)

NetworkNodes that provide Information Assurance services shall comply with the following:

- High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification (IS)

22.5.1.4.2 Advanced Encryption Standard (AES)

NetworkNodes that support AES data encryption shall comply with the following:

- NIST FIPS PUB 197: Advanced Encryption Standard (AES)

NOTE	AES will be revisited in future editions of this standard.

22.5.2 Core *TmNSApp* Protocols

22.5.2.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol version 3 (SNMPv3) shall be supported. Simple Network Management Protocol version 2c (SNMPv2c) may be supported.

TMAs shall conform to the following management protocol standards:

- RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3413: Simple Network Management Protocol (SNMP) Applications
- RFC 2579: Textual Conventions for SMIv2

SNMPv3-capable *TMAs* shall support:

- RFC 3410: Introduction and Applicability Statements for Internet Standard Management Framework
- RFC 3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)
- RFC 3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3417: Transport Mappings for the Simple Network Management Protocol (SNMP)

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

SNMPv2c-capable *TMAs* shall support:

- RFC 1901: Introduction to Community-based SNMPv2
- RFC 2578: Structure of Management Information Version 2 (SMIv2)
- RFC 3416: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

Chapter 25, Management Resources, defines the specific SNMP-based resources.

22.5.2.1.1 Error Values

Error handling is detailed by the SNMP RFCs referenced in this document. Some key SNMP protocol error cases are emphasized here for clarity:

- The SNMP exception value of noSuchObject(0) shall be returned for each variable not implemented, as stated in RFC 3416.
- Unsupported enumerations or value ranges shall return an SNMP error-status of inconsistentValue(12), as stated in RFC 3416.

22.5.2.2 Hypertext Transfer Protocol (HTTP)

TmNSApps that support HTTP shall conform to the following protocol standards:

- RFC 7230: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
- RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
- RFC 7232: Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests
- RFC 7233: Hypertext Transfer Protocol (HTTP/1.1): Range Requests
- RFC 7234: Hypertext Transfer Protocol (HTTP/1.1): Caching
- RFC 7235: Hypertext Transfer Protocol (HTTP/1.1): Authentication

22.5.2.3 Real Time Streaming Protocol (RTSP)

TmNSApps that support *TmNS* Data Delivery using a *DataDeliveryControlChannel* shall exchange control commands and parameters using Real Time Streaming Protocol (RTSP), as specified in:

- RFC 2326: Real Time Streaming Protocol (RTSP)

Chapter 26, TmNSDataMessage Transfer Protocol, defines the *DataDeliveryControlChannel*, which is an augmentation of the RTSP specification.

22.5.2.4 File Transfer

TmNSApps that support file transfer services shall support the following protocol:

- RFC 959: File Transfer Protocol (FTP)

22.5.2.5 Voice Over IP

TmNSApps that provide voice services shall comply with one or more of the following Voice over IP (VoIP) standards:

- International Telecommunication Union (ITU) H.323 Packet Based Multimedia Communication
- RFC 3261: SIP: Session Initiation Protocol and RFC 3550: RTP: A Transport Protocol for Real-Time Applications

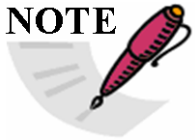
TmNSApps that provide voice services shall comply with one or more of the following CODEC standards:

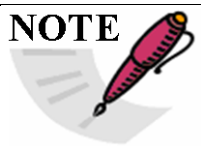
- ITU-T G.711 – Pulse Code Modulation (PCM)
- ITU-T G.726 – Adaptive Differential Pulse Code Modulation (ADPCM)

22.5.2.6 Secure Communications

TmNSApps requiring secure, reliable network communication shall conform to the following standard:

- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

	Specific implementation may require additional security.

	SNMP incorporates a security model that does not use TLS.

22.5.2.6.1 Secure FTP (FTPS)

TmNSApps that support secure file transfer services shall support the following protocols:

- RFC 2228: FTP Security Extensions
- RFC 4217: Securing FTP with TLS

22.5.2.6.2 Secure HTTP (HTTPS)

TmNSApps that support secure HTTP services should follow the recommendations in:

- RFC 2818: HTTP Over TLS

22.5.2.7 Uniform Resource Identifier (URI)/Uniform Resource Name (URN)

TmNSApps shall conform to the following standards governing URI/URN syntax:

- RFC 3986: Uniform Resource Identifier (URI): Generic Syntax
- RFC 3406: Uniform Resource Names (URN) Namespace Definition Mechanisms

The TmNS URN is registered as TBD.

22.5.3 Quality of Service (QoS)

22.5.3.1 Differentiated Services (DiffServ)

NetworkNodes shall support the Differentiated Services standards as specified in:

- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2475: An Architecture for Differentiated Services
- RFC 2597: Assured Forwarding PHB Group
- RFC 3140: Per Hop Behavior Identification Codes
- RFC 3246: An Expedited Forwarding PHB (Per-Hop Behavior)
- RFC 4594: Configuration Guidelines for DiffServ Service Classes

22.5.3.2 DiffServ Code Point (DSCP) Assignments

NetworkNodes shall mark IP packets with DSCP markings as specified through configuration via an MDL file.

NetworkNodes shall not mark traffic with the DSCP assignments identified in Table 0-1.

Table 0-1. Restricted DSCP Assignments

DSCP Class	IP Precedence	DSCP Range	Comment
6	Internetwork Control	6'b110000 (6'd48) – 6'b110111 (6'd55)	Used for IP routing protocols
7	Network Control	6'b111000 (6'd56) – 6'b111111 (6'd63)	Link layer and routing protocol keep alive

NetworkDevices forwarding IP packets with unrecognized DSCP values shall forward the packets with the DSCP value unchanged but queue the packets using the PHB of 6'b000000.

NOTE	DSCP assignments are implementation specific; the *TmNS* Engineer's Handbook contains example DSCP assignments.

22.5.4 EXtensible Markup Language (XML)

Portions of the TmNS interchanges are described with XML. A detailed explanation of the fundamentals of an XML Schema standard is outside the scope of this document, but an explanation can be found at the W3C reference in Section 2.2.2.

APPENDIX 22A Default DSCP Traffic Classification for TmNS

DSCP markings to be assigned to network traffic in a TmNS system is described in the MDL configuration file for the test. The default DSCP markings to be associated with different types of traffic in a TmNS system is according to Table 22A-1.

Table 22A-1. DSCP Traffic Classifications for TmNS

IEEE 802.1Q PCP – IEEE P802.1p	DSCP Category Description	Expected TmNS Use
0 – Best Effort	Best Effort	DSCP 0: General Network Traffic (e.g. FTP)
1 – Background	Class 1	DSCP 8: RC Delivery at Normal Priority & System Management Status
2 – Excellent Effort	Class 2	DSCP 16: LTC Delivery
3 – Critical Applications	Class 3	DSCP 24: RC Delivery at High Priority
4 – "Video," < 100 ms latency & jitter	Class 4	DSCP 32: System Management Control & Video
5 – "Voice," < 10 ms latency and jitter	Expedited Forwarding (EF)	DSCP 40: Voice
6 – Internetwork Control	Control (used for IP routing protocols)	DSCP 48: RF Network Messages
7 – Network Control	Control (link layer and routing protocol keep alive)	DSCP 56: RF Network Messages