# CHAPTER 22
# Network-Based Protocol Suite



## List of Figures



## List of Tables

This page intentionally left blank.

# Acronyms

| NOTE | Acronyms in the following list that are marked with an asterisk appear in this document only in titles of referenced materials. Some of the marked acronyms appear only once in the document. |
|---|---|

| | |
|---|---|
| *ADPCM | Adaptive Differential Pulse Code Modulation |
| AES | Advanced Encryption Standard |
| *CIDR | Classless Inter-Domain Router |
| *CRL | Certificate Revocation List |
| *DHCP | Dynamic Host Configuration Protocol |
| *DiffServ | Differentiated Services |
| DSCP | Differentiated Services Code Point |
| FTP | File Transfer Protocol |
| GPS | Global Positioning System |
| *HAIPE | High Assurance Internet Protocol Encryptor |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| ITU | International Telecommunication Union |
| LLC | logical link control |
| MAC | media access control |
| MLD | Multicast Listener Discovery |
| OSI | Open Systems Interconnection |
| *PCM | Pulse Code Modulation |
| *PIM-SM | Protocol-Independent Multicast-Sparse Mode |
| PPS | pulse per second |
| PTP | Precision Time Protocol |
| RCC | Range Commanders Council |
| RF | radio frequency |
| RFC | Request for Comment |
| RTSP | Real-Time Streaming Protocol |
| SNMP | Simple Network Management Protocol |
| SOQPSK | shaped offset quadrature phase shift keying |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TMA | TmNS manageable application |
| TmNS | Telemetry Network Standard |
| UDP | User Datagram Protocol |
| URI | Uniform Resource Identifier |
| URN | Uniform Resource Name |
| *USM | User-based Security Model |

| | |
|---|---|
| *VACM | View-based Access Control Model |

# CHAPTER 22

# Network-Based Protocol Suite

## 22.1 General

The Telemetry Network Standard (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 Transmission Control Protocol (TCP)/Internet Protocol (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 22-1 illustrates the Open Systems Interconnection (OSI) Model, the corresponding TCP/IP Model, and the major components of the TCP/IP Protocol Suite.

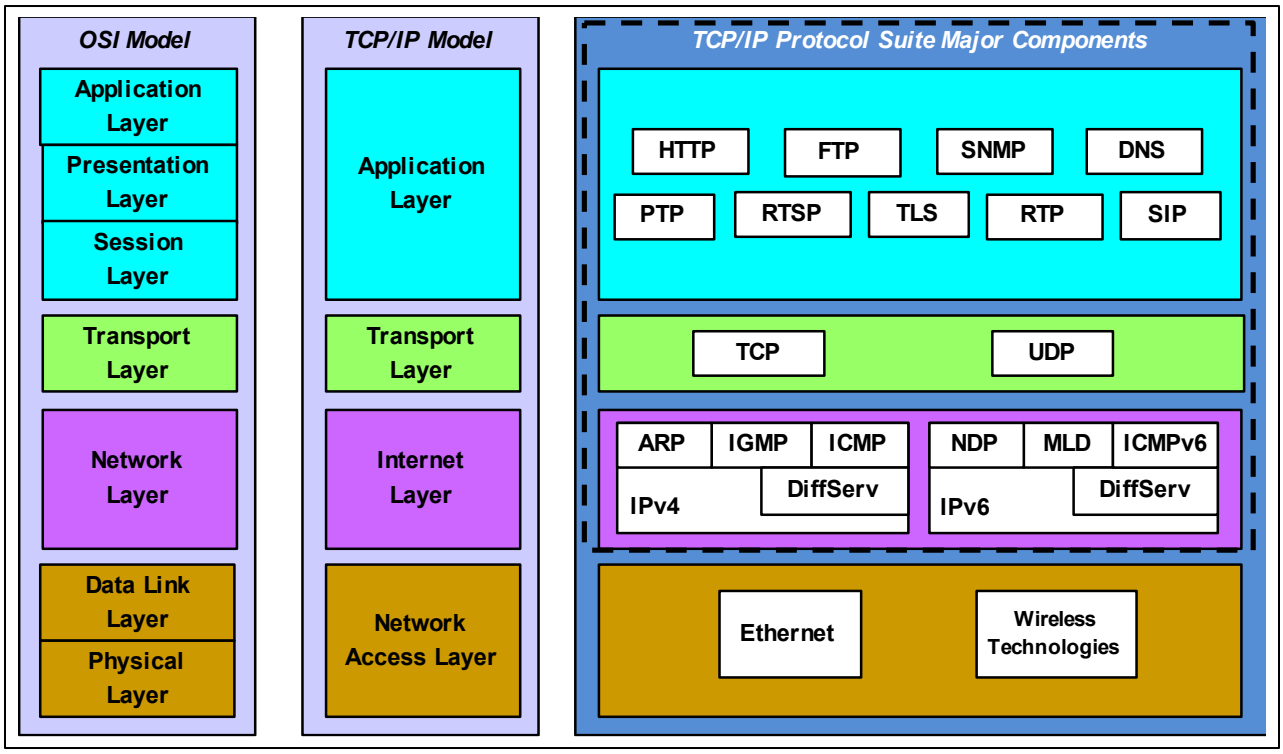



Figure 22-1. OSI and TCP/IP Model with TCP/IP Protocol Suite

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 Chapter 21 Appendix 21-B.

### 22.1.1 General *NetworkNode* Requirements

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

- Request for Comment (RFC) 1122: Requirements for Internet Hosts – Communication Layers[1]
- RFC 1123: Requirements for Internet Hosts – Application and Support[2]

### 22.1.2 General *NetworkDevice* Requirements

*NetworkDevices* that support IP version 4 (IPv4) routing shall conform to RFC 1812: Requirements for IP Version 4 Routers[3], which specifies routing functionality requirements.

## 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.

[1] Internet Engineering Task Force. "Requirements for Internet Hosts – Communication Layers." RFC 1122. October 1989. Updated by RFC 8029, RFC 6864, RFC 6093, RFC 5884, RFC 1349, RFC 6298, RFC 6633, and RFC 4379. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1122/.
[2] Internet Engineering Task Force. "Requirements for Internet Hosts – Application and Support." RFC 1123. October 1989. Updated by RFC 5966, RFC 2181, RFC 5321, RFC 7766, and RFC 1349. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1123/.
[3] Internet Engineering Task Force. "Requirements for IP Version 4 Routers." RFC 1812. June 1995. Updated by RFC 2644 and RFC 6633. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1812/.

*22.2.1.1.1 100 megabits per second Ethernet*

22.2.1.1.1.1 100BASE-TX

Copper media connections using 100BASE-TX Ethernet shall comply with IEEE 802.3-2012[4], 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.

[4] Institute of Electrical and Electronics Engineers. *IEEE standard for ethernet*. IEEE Std 802.3-2012. New York: Institute of Electrical and Electronics Engineers, 2012.

#### 22.2.1.2 Wireless Technologies

The radio frequency waveform of the Radio Access Network radios shall comply with the Range Commanders Council (RCC)-Telemetry Group variant of the shaped offset quadrature phase shift keying (SOQPSK-TG) ternary constant phase modulation as defined in Chapter 2 Subsection 2.4.3.2.

Chapter 27 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 media access control (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

*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[5] to the extent necessary to support IP network layer protocols.

[5] Institute of Electrical and Electronics Engineers. *Information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 2: logical link control*. IEEE 802.2-1998. New York: Institute of Electrical and Electronics Engineers, 1998.

#### 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[6] for Rapid Spanning Tree Protocol 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 for IPv4*

*NetworkNodes* that support IPv4 shall conform to RFC 826: Ethernet Address Resolution Protocol.[7]

##### *22.2.2.7.2 Neighbor Discovery Protocol 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)[8]
- RFC 4862: IPv6 Stateless Address Autoconfiguration[9]

## 22.3 Internet Layer Protocols

### 22.3.1 Internet Protocol version 4

*NetworkNodes* shall conform to the following IPv4 core standards.

- RFC 791: Internet Protocol[10]
- RFC 919: Broadcasting Internet Datagrams[11]

---

[6] Institute of Electrical and Electronics Engineers. *IEEE standard for local and metropolitan area networks: media access control (MAC) bridges*. IEEE 802.1-D-2004. New York: Institute of Electrical and Electronics Engineers, 2004.

[7] Internet Engineering Task Force. "An Ethernet Address Resolution Protocol." RFC 826. November 1982. Updated by RFC 5227 and RFC 5494. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc826/.

[8] Internet Engineering Task Force. "Neighbor Discovery for IP version 6 (IPv6)." RFC 4861. Updated by RFC 7559, RFC 5942, RFC 6980, RFC 8028, RFC 7527, RFC 8425, RFC 8319, and RFC 7048. September 2007. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4861/.

[9] Internet Engineering Task Force. "IPv6 Stateless Address Autoconfiguration." RFC 4862. Updated by RFC 7527. September 2007. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4862/.

[10] Internet Engineering Task Force. "Internet Protocol." RFC 791. Updated by RFC 2474, RFC 6864, and RFC 1349. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc791/.

[11] Internet Engineering Task Force. "Broadcasting Internet Datagrams." RFC 919. May be superseded or amended by update. October 1984. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc919/.

- RFC 922: Broadcasting Internet Datagrams in the Presence of Subnets[12]

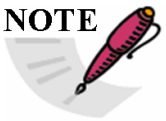
#### 22.3.1.1 Internet Control Message Protocol (ICMP)

*NetworkNodes* shall conform to RFC 792: Internet Control Message Protocol[13] and 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 RFC 3376, Internet Group Management Protocol, Version 3.[14]

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.[15] Such switching *NetworkDevices* shall use at least one of the methods B or C in Subsection 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 RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.[16]

#### 22.3.2.1 Internet Control Message Protocol Version 6 (ICMPv6)

*NetworkNodes* that support IPv6 shall conform to RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.[17]

#### 22.3.2.2 Multicast Listener Discovery for IPv6

*NetworkDevices* that support IPv6 should conform to the following MLD standards.

---

[12] Internet Engineering Task Force. "Broadcasting Internet Datagrams in the Presence of Subnets." RFC 922. May be superseded or amended by update. October 1984. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc922/.
[13] Internet Engineering Task Force. "Internet Control Message Protocol." RFC 792. Updated by RFC 950, RFC 4884, RFC 6633, and RFC 6918. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc792/.
[14] Internet Engineering Task Force. "Internet Group Management Protocol, Version 3." RFC 3376. Updated by RFC 4604. October 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3376/.
[15] Internet Engineering Task Force. "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches." RFC 4541. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4541/.
[16] Internet Engineering Task Force. "Internet Protocol, Version 6 (IPv6) Specification." RFC 2460. Obsoleted by RFC 8200. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2460/.
[17] Internet Engineering Task Force. "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification." Updated by RFC 4884. March 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4443/.

- RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6[18]
- RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast[19]

### 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[20]
- RFC 1042: A Standard for the Transmission of IP Datagrams over IEEE 802 Networks[21]

### 22.3.4 Protocol Independent Multicast

*NetworkDevices* that perform routing functions shall conform to RFC 4601: Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification (Revised).[22]

### 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 of RFC 1812.

| | |
|---|---|
| **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 interior routing protocol found in RFC 2328: OSPF Version 2.[23]

---

[18] Internet Engineering Task Force. "Multicast Listener Discover Version 2 (MLDv2) for IPv6." RFC 3810. Updated by RFC 4604. June 2004. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3810/.
[19] Internet Engineering Task Force. "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast." RFC 4604. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4604/.
[20] Internet Engineering Task Force. "A Standard for the Transmission of IP Datagrams over Ethernet Networks." RFC 894. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc894/.
[21] Internet Engineering Task Force. "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks." RFC 1042. February 1988. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1042/.
[22] Internet Engineering Task Force. "Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification." RFC 4601. Obsoleted by RFC 7761. August 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4601/.
[23] Internet Engineering Task Force. "OSPF Version 2." RFC 2328. Updated by RFC 6845, RFC 5709, RFC 8042, RFC 7474, RFC 6549, and RFC 6860. April 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2328/.

*NetworkDevices* that provide IPv6 routing functionality should be capable of running the following interior routing protocol: RFC 5340: OSPF for IPv6.[24]

## 22.4 Transport Layer Protocols

### 22.4.1 Transmission Control Protocol

*NetworkNodes* that implement TCP shall conform to RFC 793: Transmission Control Protocol.[25]

*NetworkNodes* using TCP shall conform to RFC 5681: TCP Congestion Control.[26]

### 22.4.2 User Datagram Protocol (UDP)

*NetworkNodes* that implement UDP shall conform to RFC 768: User Datagram Protocol.[27]

### 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[28]
- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2[29]

| | |
|---|---|
| **NOTE**  | It is anticipated that the TmNS will update 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 RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.[30]

---

[24] Internet Engineering Task Force. "OSPF for IPv6." RFC 5340. Updated by RFC 7503, RFC 6845, RFC 8362, and RFC 6860. July 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5340/.
[25] Internet Engineering Task Force. "Transmission Control Protocol." RFC 793. Updated by RFC 6093, RFC 3168, RFC 1122, and RFC 6528. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc793/.
[26] Internet Engineering Task Force. "TCP Congestion Control." RFC 5681. September 2009. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5681/.
[27] Internet Engineering Task Force. "User Datagram Protocol." RFC 768. 28 August 1980. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc768/.
[28] Internet Engineering Task Force. "The Secure Sockets Layer (SSL) Protocol Version 3.0." RFC 6101. August 2011. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc6101/.
[29] Internet Engineering Task Force. "The Transport Layer Security (TLS) Protocol Version 1.2." RFC 5246. Obsoleted by RFC 8446. August 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5246/.
[30] Internet Engineering Task Force. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280. Updated by RFC 6818, RFC 8398, and RFC 8399. May 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5280/.

## 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 RFC 4632: Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.[31]

*NetworkNodes* requiring IPv6 addressing should conform to RFC 4291: IP Version 6 Addressing Architecture.[32]

##### *22.5.1.1.1 Static Configuration*

*NetworkNodes* requiring IPv4 address configuration shall support static IP address assignment, conforming to RFC 950: Internet Standard Subnetting Procedure.[33]

*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 RFC 2131: Dynamic Host Configuration Protocol.[34]

A *TmNS Network* incorporating IPv6 shall support IPv6 Stateless Address Autoconfiguration as specified in Subsection 22.2.2.7.2.

A *TmNS Network* incorporating IPv6 that requires dynamic IP address assignment shall conform to RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6).[35]

#### 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[36]

[31] Internet Engineering Task Force. "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan." RFC 4632. August 2006. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4632/.
[32] Internet Engineering Task Force. "IP Version 6 Addressing Architecture." RFC 4291. Updated by RFC 7371, RFC 7136, RFC 5952. RFC 8064, RFC 7346, and RFC 6052. February 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4291/.
[33] Internet Engineering Task Force. "Internet Standard Subnetting Procedure." RFC 950. Updated by RFC 6918. August 1985. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc950/.
[34] Internet Engineering Task Force. "Dynamic Host Configuration Protocol." RFC 2131. Updated by RFC 6842, RFC 4361, RFC 5494, and RFC 3396. March 1997. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2131/.
[35] Internet Engineering Task Force. "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)." RFC 3315. Obsoleted by RFC 8415. July 2003. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3315/.
[36] Internet Engineering Task Force. "Domain Names – Concepts and Facilities." RFC 1034. Updated by many. November 1987. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1034/.

- RFC 1035: Domain names – implementation and specification[37]

#### 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.[38]

##### *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.

Master clocks compliant with IEEE 1588-2008:

- shall be able to synchronize with an external source;
- should synchronize with the Global Positioning System (GPS) external time reference (see Subsection 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 GPS 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.

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.

##### *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-5-volts direct current transistor-transistor logic 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%.

---

[37] Internet Engineering Task Force. "Domain Names – Implementation and Specification." RFC 1035. Updated by many. November 1987. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1035/.
[38] Institute of Electrical and Electronics Engineers. *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. IEEE 1588-2008. Geneva: International Electrotechnical Commission, 2008.

- 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*

The GPS external time reference interface shall implement the GPS Space Segment RF waveform interface and the GPS Navigation User Segment interface as specified in IS-GPS-200J, NAVSTAR Global Positioning System (GPS) Interface Specification.[39]

#### *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*

*NetworkNodes* that provide Information Assurance services shall comply with 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 NIST FIPS PUB 197: Advanced Encryption Standard (AES).[40]

## 22.5.2 Core *TmNSApp* Protocols

### 22.5.2.1 Simple Network Management Protocol (SNMP)

All *TmNS manageable applications* (*TMAs*) shall conform to the following management protocol standards.

---

[39] Global Positioning Systems Directorate. "Navstar GPS Space Segment/Navigation User Interfaces." IS-GPS-200J. 25 April 2018. Superseded by IS-GPS-200L. Retrieved 23 June 2023. Available at https://www.gps.gov/technical/icwg/.

[40] National Institute of Standards and Technology. "Specification for the Advanced Encryption Standard (AES)." FIPS PUB 197. 26 November 2001. Superseded by NIST FIPS 197-upd1. Retrieved 23 June 2023. Superseding document available at https://safe.menlosecurity.com/https://doi.org/10.6028/NIST.FIPS.197-upd1.

- RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks[41]
- RFC 3413: Simple Network Management Protocol (SNMP) Applications[42]
- RFC 2579: Textual Conventions for SMIv2[43]

Chapter 25 defines the specific SNMP-based resources.

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[44];
- Unsupported enumerations or value ranges shall return an SNMP error-status of inconsistentValue(12), as stated in RFC 3416.

#### *22.5.2.1.1 SNMP Version 3*

The *TMAs* that implement SNMPv3 shall support the following RFCs.

- RFC 3410: Introduction and Applicability Statements for Internet Standard Management Framework[45]
- RFC 3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)[46]
- RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)[47]
- RFC 3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)[48]

---

[41] Internet Engineering Task Force. "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks." RFC 3411. Updated by RFC 5343 and RFC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3411/.
[42] Internet Engineering Task force. "Simple Network Management Protocol (SNMP) Applications." RFC 3413. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3413/.
[43] Internet Engineering Task Force. "Textual Conventions for SMIv2." RFC 2579. April 1999. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2579/.
[44] Internet Engineering Task Force. "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)." RFC 3416. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3416/.
[45] Internet Engineering Task Force. "Introduction and Applicability Statements for Internet Standard Management Framework." RFC 3410. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3410/.
[46] Internet Engineering Task Force. "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)." RFC 3412. Updated by RFC 5590. December 2002. 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3412/.
[47] Internet Engineering Task Force. "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)." RFC 3414. Updated by RFC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3414/.
[48] Internet Engineering Task Force. "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)." RFC 3415. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3415/.

- RFC 3417: Transport Mappings for the Simple Network Management Protocol (SNMP)[49]
- RFC 3826: The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model[50]

#### *22.5.2.1.2 SNMP Version 2c*

The *TMAs* that implement SNMPv2c shall support the following RFCs.

- RFC 1901: Introduction to Community-based SNMPv2[51]
- RFC 2578: Structure of Management Information Version 2 (SMIv2)[52]
- RFC 3416

### 22.5.2.2 Hypertext Transfer Protocol (HTTP)

The *TmNSApps* that support HTTP shall conform to the following protocol standards.

- RFC 7230: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing[53]
- RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content[54]
- RFC 7232: Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests[55]
- RFC 7233: Hypertext Transfer Protocol (HTTP/1.1): Range Requests[56]
- RFC 7234: Hypertext Transfer Protocol (HTTP/1.1): Caching[57]
- RFC 7235: Hypertext Transfer Protocol (HTTP/1.1): Authentication[58]

---

[49] Internet Engineering Task Force. "Transport Mappings for the Simple Network Management Protocol (SNMP)." RFC 3417. Updated by RFC 4789 and R FC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3417/.
[50] Internet Engineering Task Force. "Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model." RFC 3826. June 2004. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3826/.
[51] Internet Engineering Task Force. "Introduction to Community-based SNMPv2." RFC 1901. January 1996. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1901/.
[52] Internet Engineering Task Force. "Structure of Management Information Version 2 (SMIv2)." RFC 2578. April 1999. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2578/.
[53] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing." RFC 7230. June 2014. Updated by RFC 8213. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7230/.
[54] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content." RFC 7231. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7231/.
[55] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests." RFC 7232. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7232/.
[56] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Range Requests." RFC 7233. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7233/.
[57] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Caching." RFC 7234. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7234/.
[58] Internet Engineering Task Force. "Hypertext Transfer Protocol (HTTP/1.1): Authentication." RFC 7235. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7235/.

#### 22.5.2.3 Real Time Streaming Protocol (RTSP)

The *TmNSApps* that support TmNS Data Delivery using a *DataDeliveryControlChannel* shall exchange control commands and parameters using RTSP, as specified in RFC 2326: Real Time Streaming Protocol (RTSP).[59]

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

#### 22.5.2.4 File Transfer

The *TmNSApps* that support file transfer services shall support RFC 959: File Transfer Protocol (FTP).[60]

#### 22.5.2.5 Voice Over IP

The *TmNSApps* that provide voice services shall comply with one or more of the following Voice over IP standards.

- International Telecommunication Union (ITU) H.323 Packet Based Multimedia Communication[61]
- RFC 3261: SIP: Session Initiation Protocol[62]
- RFC 3550: RTP: A Transport Protocol for Real-Time Applications[63]

The *TmNSApps* that provide voice services shall comply with one or more of the following coder-decoder standards.

- ITU-T G.711 – Pulse Code Modulation (PCM)[64]
- ITU-T G.726 – Adaptive Differential Pulse Code Modulation (ADPCM)[65]

---

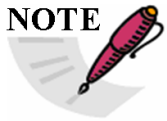
[59] Internet Engineering Task Force. "Real Time Streaming Protocol (RTSP)." RFC 2326. Obsoleted by RFC 7826. April 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2326/.
[60] Internet Engineering Task Force. "File Transfer Protocol (FTP)." RFC 959. Updated by RFC 3659, RFC 7151, RFC 2640, RFC 2773, RFC 2228, and RFC 5797. October 1985. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc959/.
[61] International Telecommunication Union. "Packet-based multimedia communications systems." ITU-T H.323. March 2022. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-H.323/en.
[62] Internet Engineering Task Force. "SIP: Session Initiation Protocol." RFC 3261. Updated by many. June 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3261/.
[63] Internet Engineering Task Force. "RTP: A Transport Protocol for Real-Time Applications." RFC 3550. Updated by RFC 7022, RFC 5761, RFC 8108, RFC 8083, RFC 6222, RFC 6051, RFC 5506, RFC 7160, and RFC 7164. July 2003. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3550/.
[64] International Telecommunication Union. "Pulse Code Modulation (PCM) of Voice Frequencies." ITU-T G.711. 25 November 1988. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-G.711/en.
[65] International Telecommunication Union. "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)." ITU-T G.726. 14 December 1990. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-G.726/en.

#### 22.5.2.6 Secure Communications

The *TmNSApps* requiring secure, reliable network communication over connection-oriented transports shall conform to RFC 5246.

The *TmNSApps* requiring secure network communication over SNMP shall conform to RFC 5953: Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP).[66]

| | |
|---|---|
|  | Specific implementation may require additional security. |

| | |
|---|---|
|  | The SNMP incorporates a security model that utilizes TLS. The open-source Net-SNMP implementation has supported both TLS and Datagram TLS (DTLS) since version 5.6. |

##### *22.5.2.6.1 Secure FTP*

The *TmNSApps* that support secure file transfer services shall support the following protocols.

- RFC 2228: FTP Security Extensions[67]
- RFC 4217: Securing FTP with TLS[68]

##### *22.5.2.6.2 Secure HTTP*

The *TmNSApps* that support secure HTTP services should follow the recommendations in RFC 2818: HTTP Over TLS.[69]

#### 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[70]

---

[66] Internet Engineering Task Force. "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)." RFC 5953. Obsoleted by RFC 6353. August 2010. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5953/.
[67] Internet Engineering Task Force. "FTP Security Extensions." RFC 2228. October 1997. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2228/.
[68] Internet Engineering Task Force. "Securing FTP with TLS." RFC 4217. October 2005. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4217/.
[69] Internet Engineering Task Force. "HTTP Over TLS." RFC 2818. Updated by RFC 5785 and RFC 7230. May 2000. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2818/.
[70] Internet Engineering Task Force. "Uniform Resource Identifier (URI): Generic Syntax." RFC 3986. Updated by RFC 8820, RFC 7320, and RFC 6874. January 2005. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3986/.

- RFC 3406: Uniform Resource Names (URN) Namespace Definition Mechanisms[71]

| NOTE | The TmNS-specific URN is not registered. It is anticipated that the RCC may register it in the future. |
|---|---|

### 22.5.3 Quality of Service

#### 22.5.3.1 Differentiated Services (DiffServ)

*NetworkNodes* shall support the DiffServ standards as specified in:

- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers[72];
- RFC 2475: An Architecture for Differentiated Services[73];
- RFC 2597: Assured Forwarding PHB Group[74];
- RFC 3140: Per Hop Behavior Identification Codes;[75]
- RFC 3246: An Expedited Forwarding PHB (Per-Hop Behavior);[76]
- RFC 4594: Configuration Guidelines for DiffServ Service Classes.[77]

#### 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.

The DSCP assignments identified in Table 22-1 have restricted usage and shall only be assigned to network traffic that is directly related to network and internetwork control, such as RF network messages that are exchanged between RF link management and radios. *NetworkNodes* shall not mark traffic with the restricted DSCP assignments if the traffic is not directly related to network and internetwork control.

---

[71] Internet Engineering Task Force. "Uniform Resource Names (URN) Namespace Definition Mechanisms." RFC 3406. October 2002. Obsoleted by RFC 8141. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3406/.

[72] Internet Engineering Task Force. "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers." RFC 2474. Updated by RFC 3260, RFC 3168, and RFC 8436. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2474/.

[73] Internet Engineering Task Force. "An Architecture for Differentiated Services." RFC 2475. Updated by RFC 3260. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2475/.

[74] Internet Engineering Task Force. "Assured Forwarding PHB Group." RFC 2597. Updated by RFC 3260. June 1999. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2597/.

[75] Internet Engineering Task Force. "Per Hop Behavior Identification Codes." RFC 3140. June 2001. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3140/.

[76] Internet Engineering Task Force. "An Expedited Forwarding PHB (Per Hop Behavior)." RFC 3246. March 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3246/.

[77] Internet Engineering Task Force. "Configuration Guidelines for DiffServ Service Classes." RFC 4594. Updated by RFC 5865 and RFC 8622. August 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4594/.

**Table 22-1. 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.

This page intentionally left blank.

# APPENDIX 22-A

## Default DSCP Traffic Classification for TmNS-based Systems

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

Table **A-1**. DSCP Traffic Classifications for TmNS-based Systems

| **IEEE 802.1Q PCP – IEEE P802.1p** | DSCP Category Description | Expected Use Within TmNS-based System |
|---|---|---|
| **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 |

This page intentionally left blank.

# APPENDIX 22-B

## Citations

Global Positioning Systems Directorate. "Navstar GPS Space Segment/Navigation User Interfaces." IS-GPS-200J. 25 April 2018. Superseded by IS-GPS-200N. Retrieved 23 June 2023. Available at https://www.gps.gov/technical/icwg/.

Institute of Electrical and Electronics Engineers. *IEEE standard for Ethernet*. IEEE Std 802.3-2012. New York: Institute of Electrical and Electronics Engineers, 2012.

———. *IEEE standard for local and metropolitan area networks: media access control (MAC) bridges*. IEEE 802.1-D-2004. New York: Institute of Electrical and Electronics Engineers, 2004.

———. *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. IEEE 1588-2008. Geneva: International Electrotechnical Commission, 2008.

———. *Information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 2: logical link control*. IEEE 802.2-1998. New York: Institute of Electrical and Electronics Engineers, 1998.

International Telecommunications Union. "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)." ITU-T G.726. 14 December 1990. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-G.726/en.

———. "Packet-based multimedia communications systems." ITU-T H.323. March 2022. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-H.323/en.

———. "Pulse Code Modulation (PCM) of Voice Frequencies." ITU-T G.711. 25 November 1988. May be superseded by update. Retrieved 23 June 2023. Available at https://www.itu.int/rec/T-REC-G.711/en.

Internet Engineering Task Force. "A Standard for the Transmission of IP Datagrams over Ethernet Networks." RFC 894. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc894/.

———. "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks." RFC 1042. February 1988. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1042/.

———. "Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model." RFC 3826. June 2004. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3826/.

———. “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.” RFC 3411. Updated by RFC 5343 and RFC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3411/.

———. “An Architecture for Differentiated Services.” RFC 2475. Updated by RFC 3260. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2475/.

———. “An Ethernet Address Resolution Protocol.” RFC 826. November 1982. Updated by RFC 5227 and RFC 5494. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc826/.

———. “An Expedited Forwarding PHB (Per Hop Behavior).” RFC 3246. March 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3246/.

———. “Assured Forwarding PHB Group.” RFC 2597. Updated by RFC 3260. June 1999. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2597/.

———. “Broadcasting Internet Datagrams.” RFC 919. May be superseded or amended by update. October 1984. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc919/.

———. “Broadcasting Internet Datagrams in the Presence of Subnets.” RFC 922. May be superseded or amended by update. October 1984. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc922/.

———. “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.” RFC 4632. August 2006. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4632/.

———. “Configuration Guidelines for DiffServ Service Classes.” RFC 4594. Updated by RFC 5865 and RFC 8622. August 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4594/.

———. “Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.” RFC 4541. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4541/.

———. “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.” RFC 2474. Updated by RFC 3260, RFC 3168, and RFC 8436. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2474/.

———. “Domain Names – Concepts and Facilities.” RFC 1034. Updated by many. November 1987. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1034/.

———. “Domain Names – Implementation and Specification.” RFC 1035. Updated by many. November 1987. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1035/.

———. “Dynamic Host Configuration Protocol.” RFC 2131. Updated by RFC 6842, RFC 4361, RFC 5494, and RFC 3396. March 1997. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2131/.

———. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6).” RFC 3315. Obsoleted by RFC 8415. July 2003. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3315/.

———. “File Transfer Protocol (FTP).” RFC 959. Updated by RFC 3659, RFC 7151, RFC 2640, RFC 2773, RFC 2228, and RFC 5797. October 1985. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc959/.

———. “FTP Security Extensions.” RFC 2228. October 1997. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2228/.

———. “HTTP Over TLS.” RFC 2818. Updated by RFC 5785 and RFC 7230. May 2000. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2818/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Authentication.” RFC 7235. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7235/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Caching.” RFC 7234. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7234/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests.” RFC 7232. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7232/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.” RFC 7230. June 2014. Updated by RFC 8213. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7230/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Range Requests.” RFC 7233. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7233/.

———. “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.” RFC 7231. June 2014. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc7231/.

———. “Internet Control Message Protocol.” RFC 792. Updated by RFC 950, RFC 4884, RFC 6633, and RFC 6918. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc792/.

———. “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.” RFC 4443. Updated by RFC 4884. March 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4443/.

———. “Internet Group Management Protocol, Version 3.” RFC 3376. Updated by RFC 4604. October 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3376/.

———. “Internet Protocol.” RFC 791. Updated by RFC 2474, RFC 6864, and RFC 1349. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc791/.

———. “Internet Protocol, Version 6 (IPv6) Specification.” RFC 2460. Obsoleted by RFC 8200. December 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2460/.

———. “Internet Standard Subnetting Procedure.” RFC 950. Updated by RFC 6918. August 1985. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc950/.

———. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.” RFC 5280. Updated by RFC 6818, RFC 8398, and RFC 8399. May 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5280/.

———. “Introduction and Applicability Statements for Internet Standard Management Framework.” RFC 3410. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3410/.

———. “Introduction to Community-based SNMPv2.” RFC 1901. January 1996. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1901/.

———. “IP Version 6 Addressing Architecture.” RFC 4291. Updated by RFC 7371, RFC 7136, RFC 5952. RFC 8064, RFC 7346, and RFC 6052. February 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4291/.

———. “IPv6 Stateless Address Autoconfiguration.” RFC 4862. Updated by RFC 7527. September 2007. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4862/.

———. “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).” RFC 3412. Updated by RFC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3412/.

———. “Multicast Listener Discover Version 2 (MLDv2) for IPv6.” RFC 3810. Updated by RFC 4604. June 2004. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3810/.

———. “Neighbor Discovery for IP version 6 (IPv6).” RFC 4861. Updated by RFC 7559, RFC 5942, RFC 6980, RFC 8028, RFC 7527, RFC 8425, RFC 8319, and RFC 7048. September 2007. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4861/.

———. “OSPF for IPv6.” RFC 5340. Updated by RFC 7503, RFC 6845, RFC 8362, and RFC 6860. July 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5340/.

———. “OSPF Version 2.” RFC 2328. Updated by RFC 6845, RFC 5709, RFC 8042, RFC 7474, RFC 6549, and RFC 6860. April 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2328/.

———. “Per Hop Behavior Identification Codes.” RFC 3140. June 2001. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3140/.

———. “Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification.” RFC 4601. Updated by RFC 5796, RFC 6226, and RFC 5059. August 2006. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4601/.

———. “Real Time Streaming Protocol (RTSP).” RFC 2326. Obsoleted by RFC 7826. April 1998. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2326/.

———. “Requirements for Internet Hosts – Application and Support.” RFC 1123. October 1989. Updated by RFC 5966, RFC 2181, RFC 5321, RFC 7766, and RFC 1349. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1123/.

———. “Requirements for Internet Hosts – Communication Layers.” RFC 1122. October 1989. Updated by RFC 8029, RFC 6864, RFC 6093, RFC 5884, RFC 1349, RFC 6298, RFC 6633, and RFC 4379. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1122/.

———. “Requirements for IP Version 4 Routers.” RFC 1812. June 1995. Updated by RFC 2644 and RFC 6633. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc1812/.

———. “RTP: A Transport Protocol for Real-Time Applications.” RFC 3550. Updated by RFC 7022, RFC 5761, RFC 8108, RFC 8083, RFC 6222, RFC 6051, RFC 5506, RFC 7160, and RFC 7164. July 2003. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3550/.

———. “Securing FTP with TLS.” RFC 4217. October 2005. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4217/.

———. “Simple Network Management Protocol (SNMP) Applications.” RFC 3413. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3413/.

———. “SIP: Session Initiation Protocol.” RFC 3261. Updated by many. June 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3261/.

———. “Structure of Management Information Version 2 (SMIv2).” RFC 2578. April 1999. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2578/.

———. “The Secure Sockets Layer (SSL) Protocol Version 3.0.” RFC 6101. August 2011. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc6101/.

———. “TCP Congestion Control.” RFC 5681. September 2009. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5681/.

———. “Textual Conventions for SMIv2.” RFC 2579. April 1999. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc2579/.

———. “Transmission Control Protocol.” RFC 793. Updated by RFC 6093, RFC 3168, RFC 1122, and RFC 6528. September 1981. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc793/.

———. “The Transport Layer Security (TLS) Protocol Version 1.2.” RFC 5246. Obsoleted by RFC 8446. August 2008. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5246/.

———. “Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP).” RFC 5953. Obsoleted by RFC 6353. August 2010. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc5953/.

———. “Transport Mappings for the Simple Network Management Protocol (SNMP).” RFC 3417. Updated by RFC 4789 and R FC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3417/.

———. “Uniform Resource Identifier (URI): Generic Syntax.” RFC 3986. Updated by RFC 8820, RFC 7320, and RFC 6874. January 2005. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3986/.

———. “Uniform Resource Names (URN) Namespace Definition Mechanisms.” RFC 3406. October 2002. Obsoleted by RFC 8141. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3406/.

———. “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).” RFC 3414. Updated by RFC 5590. December 2002. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3414/.

———. “User Datagram Protocol.” RFC 768. 28 August 1980. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc768/.

———. “Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.” RFC 4604. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc4604/.

———. “Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).” RFC 3416. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3416/.

———. “View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).” RFC 3415. December 2002. May be superseded or amended by update. Retrieved 23 June 2023. Available at https://datatracker.ietf.org/doc/rfc3415/.

National Institute of Standards and Technology. “Specification for the Advanced Encryption Standard (AES).” FIPS PUB 197. 26 November, 2001. Superseded by NIST FIPS 197-upd1. Retrieved 23 June 2023. Superseding document available at https://safe.menlosecurity.com/https://doi.org/10.6028/NIST.FIPS.197-upd1.

****** END OF CHAPTER 22 ******