FAA-STD-039C
August 14, 2003

Department of Transportation
Federal Aviation Administration

Standard Practice

NATIONAL AIRSPACE SYSTEM (NAS) OPEN SYSTEM ARCHITECTURE AND PROTOCOLS

A. Approved for public release; distribution is unlimited

FOREWORD

This standard establishes the open systems data communications architecture and authorized protocol standards for the National Airspace System (NAS). The NAS will consist of various types of processors and communications networks procured from a variety of vendors. Well-defined data communications architecture is required to ensure interoperability among NAS open end-systems, and with external systems.

This document was prepared in accordance with FAA-STD-005e.

TABLE of CONTENTS

Table of Figures

1 SCOPE

This standard establishes the protocols, features, standards, and services that should be supported in the Federal Aviation Administration (FAA) National Airspace System (NAS) data communications infrastructure, including end systems, LANs, and WANs.

This standard specifies the available protocols and services, from which a minimum subset must be implemented by mutual agreement between NAS system programs to insure system interoperability. The minimum set defined herein may exceed the minimum requirements for a particular program or project. For example, additional requirements are herein levied to accommodate ATN connectivity as per ICAO Doc. 9705 Ed. 3 and ICAO Doc. 9739.

1.1 PURPOSE

The purpose of this document is to provide a standardized set of protocols for implementation in the NAS data communications infrastructure, in accordance with specified Request for Comments (RFCs) and standards. The implementation of the specified protocols and services will enable current and future FAA systems to be compatible with domestic and international Air Traffic Management systems.

2 APPLICABLE DOCUMENTS

2.1 GOVERNMENT DOCUMENTS

The following government documents form a part of this standard to the extent specified herein. In the event of conflict between the documents referenced herein and the content of this standard, the content of this standard shall be considered the superseding document.

Standards

FAA-STD-005e	Preparation of Specifications, Standards and Handbooks, 1996
FAA-STD-045	Security Architecture Protocols and Mechanisms, 2003

Other Government Publications

FAA-HDBK-002	Systems Management, 1997

2.2 NON-GOVERNMENT DOCUMENTS

The following non-government documents form a part of this standard to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this standard, the contents of this standard shall be considered the superseding document.

Institute of Electrical and Electronic Engineers (IEEE) Standards

IEEE 802.3	Information Technology – Telecommunication & Information Exchange between Systems – LAN/MAN – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 2002

Internet Standards

RFC-768	User Datagram Protocol, August 1980
RFC-791	Internet Protocol, September 1981
RFC-792	Internet Control Message Protocol (ICMP), September 1981
RFC-793	Transmission Control Protocol, September 1981
RFC-796	Address Mappings, September 1981
RFC-822	Standard for the Format of ARPA Internet Text Messages, August 1982

RFC-826	An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware, November 1982
RFC-894	Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
RFC-903	Reverse Address Resolution Protocol, June 1984
RFC-950	Internet Standard Subnetting Procedure, August 1985
RFC-959	File transfer Protocol, October 1985
RFC-1042	Standard for the Transmission of IP Datagrams over 802 Networks, February 1988
RFC-1055	A Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP, June 1988
RFC-1058	Routing Information Protocol, June 1988
RFC-1108	U.S. Department of Defense Security Options for the Internet Protocol, November 1991
RFC-1112	Host Extensions for IP Multicasting, August 1989
RFC-1122	Requirements for Internet Hosts-Communications Layers, October 1989
RFC-1123	Requirements for Internet Hosts-Application and Support, October 1989
RFC-1142	OSI IS-IS Intra-domain Routing Protocol, February 1990
RFC-1191	Path MTU Discovery, November 1990
RFC-1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments, December 1990
RFC-1332	The PPP Internet Protocol Control Protocol (IPCP), May 1992
RFC-1350	The TFTP Protocol (Revision 2), July 1992
RFC-1356	Multiprotocol Interconnect and X.25 and ISDN in the Packet Mode, August 1992

RFC-1390	Transmission of IP and ARP over FDDI Networks, January 1993
RFC-1661	The Point-to-Point Protocol (PPP), July 1994
RFC-1706	DNS NSAP Resource Records, October 1994
RFC-1771	A Border Gateway Protocol 4 (BGP-4), March 1995
RFC-1825	Security Architecture for the Internet Protocol, August 1995
RFC-2080	RIPng for IPv6, January 1997
RFC-2153	PPP Vendor Extensions, May 1997
RFC-2156	MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME, January 1998
RFC 2225	Classical IP and ARP over Asynchronous Transfer Mode (ATM), April 1998
RFC 2331	ATM Signaling Support for IP over ATM – UNI Signaling 4.0 Update, April 1998
RFC-2328	OSPF Version 2, J. Moy, April 1998
RFC-2347	TFTP Option Extension, May 1998
RFC-2348	TFTP Blocksize Option, May 1998
RFC-2349	TFTP Timeout Interval and Transfer Size Options, May 1998
RFC-2373	IP Version 6 Addressing Architecture
RFC-2401	Security Architecture for the Internet Protocol, November 1998
RFC-2427	Multiprotocol Interconnect over Frame Relay (FR), September 1998
RFC-2453	RIP Version 2-Carring Additional Information, November 1998
RFC-2460	Internet Protocol, Version 6 (IPv6) Specification, December 1998
RFC-2461	Neighbor Discovery for IPv6, December 1998

RFC-2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, December 1998
RFC-2464	Transmission of IPv6 Packets over Ethernet Networks, December 1998
RFC-2467	Transmission of IPv6 Packets over FDDI Networks, December 1998
RFC-2472	IP Version 6 over PPP, December 1998
RFC-2473	Generic Packet Tunneling in IPv6 Specification, December 1998
RFC-2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
RFC-2492	IPv6 over ATM Networks, January 1999
RFC-2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, March 1999
RFC-2590	Transmission of IPv6 Packets over Frame Relay Networks Specification, May 1999
RFC-2640	Internationalization of the File Transfer Protocol, July 1999
RFC-2740	OSPF for IPv6, December 1999
RFC-2784	Generic Routing Encapsulation (GRE), March 2000
RFC-2821	Simple Mail Transfer Protocol, April 2001
RFC-2858	Multiprotocol Extensions for BGP-4, June 2000
RFC-2893	Transition Mechanisms for IPv6 Hosts and Routers, August 2000
RFC-3168	The Addition of Explicit Congestion Notification (ECN) to IP, September 2001
RFC-3260	New Terminology and Clarifications for Diffserv, April 2002
RFC-3376	Internet Group Management Protocol, Version 3, October 2002
STD 8 (RFC 854)	Telnet Protocol Specification, May 1983

International Organization for Standardization (ISO)

ISO 9542	Information processing systems -- Telecommunications and information exchange between systems -- End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473) End System to Intermediate System (ES-IS) Protocol, 1988
ISO 10589	Information technology -- Telecommunications and information exchange between systems -- Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473), 2002
ISO 10747	Information technology -- Telecommunications and information exchange between systems -- Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO 8473. 1994

American National Standards Institute (ANSI) and Electrical Industries Association (EIA)

ANSI X3T12	Fiber Distribution Data Interface (FDDI), 1995
ANSI T1.102 (R1999)	Telecommunications –Digital Hierarchy – Electrical Interfaces, 1993
ANSI T1.403	Telecommunications – Network and Customer Installation Interfaces – DS1 Electrical Interface, 1999
ANSI T1.404	DS3 Metallic Interface Specification, 2002
ANSI T1.410	Carrier to Customer Metallic Interface - Digital Data at 64 kbit/s and Subrates, 2001
ANSI T1.618 (R2003)	DSS1 – Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service, 1991
ANSI T1.634 (R2001)	Frame Relay Service Specific Convergence Sublayer, 1993
TIA/EIA-232-E/F	Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, 1997

TIA/EIA-530-A	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector, 1998

International Telecommunications Union – Telecommunications (ITU-T)

ITU-T V.35	Data Transmission at 56 Kilobits per Second using 60-108 Khz Group Band Circuits, 1985

2.3 OTHER PUBLICATIONS

ICAO ATN Doc. 9705 Edition 3 Profile Requirement List ISO-8571-5: File Transfer, Access, and Management – Part: Protocol Implementation Conformance Statement (PICS) Proforma

ICAO Doc. 9739 Comprehensive Aeronautical Telecommunication Network (ATN) Manual

2.4 DOCUMENT SOURCES

Obtain copies of the applicable documents or standards by contacting the appropriate organizations.

FAA documents
Copies of FAA specifications, standards, and publications may be obtained from the Contracting Officer, Federal Aviation Administration, 800 Independence Avenue, S.W., Washington, D.C., 20591. Request should clearly identify the desired material by number and date, and state the intended use of the material.

Federal or military documents
Copies of federal or military documents are available from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094

Request for comments
Copies of Request for Comments (RFC) may be obtained from DS.INTERNIC.NET via File Transfer Protocol (FTP), Wide Area Information Service (WAIS), and electronic mail.

If FTP is used, RFCs are stored as rfc/rfcnnnn.txt or rfc/rfcnnnn.ps where "nnnn" is the RFC number. Login as "anonymous" and provide your E-Mail address as the password. If WAIS is used, the local WAIS client or Telnet to DS.INTERNIC.NET can be used. Login as "wais" (no password is required) to access a WAIS client; help information and a tutorial for using WAIS are available online. Search the "rfcs" database to locate the desired rfc.

If electronic mail is used, send a mail message to mailserv@ds.internic.net and include any of the following commands in the message body:

document-by-name rfcnnnn	where "nnnn" is the RFC number; the text version is sent
file/ftp/rfc/rfcnnnn.yyy	where "nnnn" is the RFC number and "yyy" is "txt" or "ps"

3 Definitions and Acronyms

3.1 ACRONYMS

The acronyms used in this standard are defined as follows:

AP	Application Process
API	Application Programming Interface
ATN	Aeronautical Telecommunication Network
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CL	Connection-less
CLNP	Connection-less Network Protocol
CO	Connection-oriented
DGRAM	Datagram
DNS	Domain Name System
DOD	Department of Defense
EGP	Exterior Gateway Protocol
ES-IS	End System to Intermediate System
FAA	Federal Aviation Administration
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards Publication
FTP	File Transfer Protocol
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
ICMP	Internet Control Message Protocol

IDRP	Inter-Domain Routing Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IS-IS	Intermediate System to Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
LAN	Local Area Network
MTU	Maximum Transmission Unit
NAS	National Airspace System
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PPP	Point-to-Point Protocol
RARP	Reverse Address Resolution Protocol
RFC	Request for Comments
RIP	Routing Information Protocol
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAIS	Wide Area Information Service
WAN	Wide Area Network

3.2 DEFINITIONS

AP A set of resources, including processing resources, within a real open system, which may be used to perform a particular information processing activity.

Internet A NAS computer communications network that interconnects various networks (e.g., WANs, LANs, and MANs) and users.

ISDN Integrated Service Digital Network, ITUT adopted protocol reference model intended for providing a ubiquitous, end-to-end, interactive, digital services for data, audio and video. ISDN is available as BRI, PRI and B-ISDN.

LAN A system that links together electronic office equipment, such as computers and printers network within an office or building that allows users to communicate and share resources.

Network System of mutually-communicating devices (e.g., computers, terminals, peripheral devices, process controls) connected by one or more transmission facilities.

Profile A list of protocols that support the implementation of a service or function in a network.

Protocol A set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and transmission, error detection, and correction of the bit stream. High-level protocols deal with data formatting, including the syntax of messages, the terminal-to-computer dialogue, character sets, sequencing of messages, etc. Many protocols are defined by RFCs or by International Organization for Standardization (ISO) standards.

Service Element	A set of procedures that provide service between two layers in the IPS protocol stack.
Subnetwork	1) A collection of end systems and intermediate systems under the control of a single administrative domain, which uses a single network access protocol. 2) An actual implementation of data network that employs a homogeneous protocol and addressing plan and is under control of a single authority.
Sub-profile	A subset of a profile that supports a specific protocol layer in a network application.
WAN	A communications network that uses such devices as telephone lines, satellite dishes, or radio waves to span a larger geographic area than can be covered by a LAN.
World Wide Web	An Internet client-server distributed information retrieval system which originated in the CERN High-Energy Physics laboratories in Geneva, Switzerland.
X.25	ITUT – Standardized – public (data) packet – switching network layer protocols.

4 Requirements

This section specifies general requirements for implementing the communications protocols within a network. The communications protocols allow computers from different vendors, using different operating systems, to exchange data. This data transfer is accomplished over data networks using various protocols. The complete set of protocols necessary for such communication is referred to as a protocol suite. Depicted in Figure 1 are examples of two NAS protocol suites[1] that will accommodate various applications.

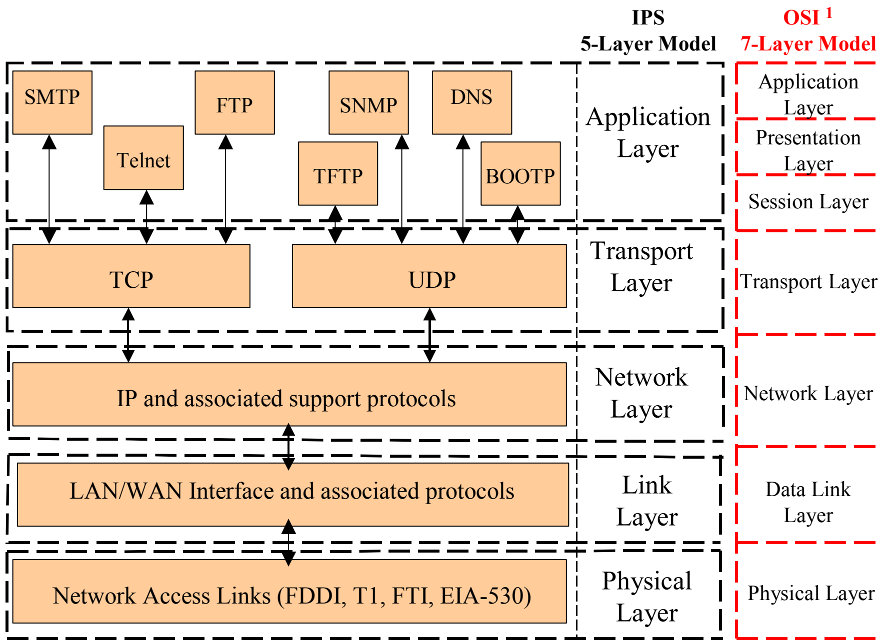


Figure 1 NAS End System Communication Protocol Suites

Each layer of the protocol suite supports the implementation of a different function within a communication network. Typically, any given layer provides services to the layer above. In order to accommodate multiple configurations, a layer may support more than one protocol. The grouping of protocols that support the functional requirements of a protocol layer is referred to as a sub-profile. Note that the three lowest layers will interface with the FAA Telecommunications Infrastructure (FTI).

A more detailed explanation of the IPS sub-profile layers is contained in the following paragraphs.

---

[1] For more information on OSI model go to http://www.microsoft.com/ntserver/techresources/commnet/TCPIP/TCPIntrowp.asp

4.1 PHYSICAL LAYER SUB-PROFILE

The physical layer handles the hardware details or the physical interfacing to the transmission medium (e.g., cable, radio link). It provides the mechanical, electrical, functional, and procedural methods necessary to activate, maintain, and deactivate physical connections for data links.

General requirements for implementing this layer are included in this standard; additional functions may be included in particular implementations of the physical layer in accordance with applicable project or program requirements. Detailed requirements for physical layer interfaces are contained in Section 5.1 of this document.

4.2 LINK LAYER SUB-PROFILE

The link layer provides the procedural and functional means to establish, maintain, and release data link connections between hosts and nodes (e.g., network entities). It is the layer for transferring data frames, and detecting – and optionally correcting – errors incurred in the physical layer. The Media Access Control (MAC) portion of the link layer, is network-specific, and normally includes the device drivers for the operating system and the corresponding network interface card installed in the computer. The Logical Link Control (LLC) portion of the link layer is generic, and independent of the particular network medium.

General requirements for implementing this layer are included in this standard; additional functions may be included in particular implementations of the link layer in accordance with applicable project or program requirements. Detailed requirements for link layer interfaces are contained in Section 5.2 of this document.

4.3 NETWORK LAYER SUB-PROFILE

The network layer is responsible for connectivity and path selection between two end systems. This layer can integrate virtual networks independent of lower layer configurations. There is no guarantee of correct data delivery, since the network layer does not provide error correction. The devices active on this layer are called routers, and the data units are referred to as packets.

Detailed requirements for the network layer are contained in Section 5.3 of this document.

4.4 TRANSPORT LAYER SUB-PROFILE

The transport layer provides a flow of data between two end systems for the application layer above it. There are two protocols available at this layer. The Transport Control Protocol (TCP) guarantees end-to-end delivery, while the User Datagram Protocol (UDP) is used for applications not requiring reliable delivery [e.g., Trivial File Transfer Protocol

(TFTP), simple network management (SNMP)]. Detailed requirements for the transport layer are contained in Section 5.4 of this document.

4.5 APPLICATION LAYER SUB-PROFILE

The application layer contains the user-specific information for applications distributed across the enterprise (i.e., NAS). This is the layer at which communication partners and their relationship mechanisms are identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is *not* the application program itself, although some applications may perform application layer functions). Active devices for internetworking are called application gateways.

Detailed requirements for the application layer are contained in Section 5.5 of this document.

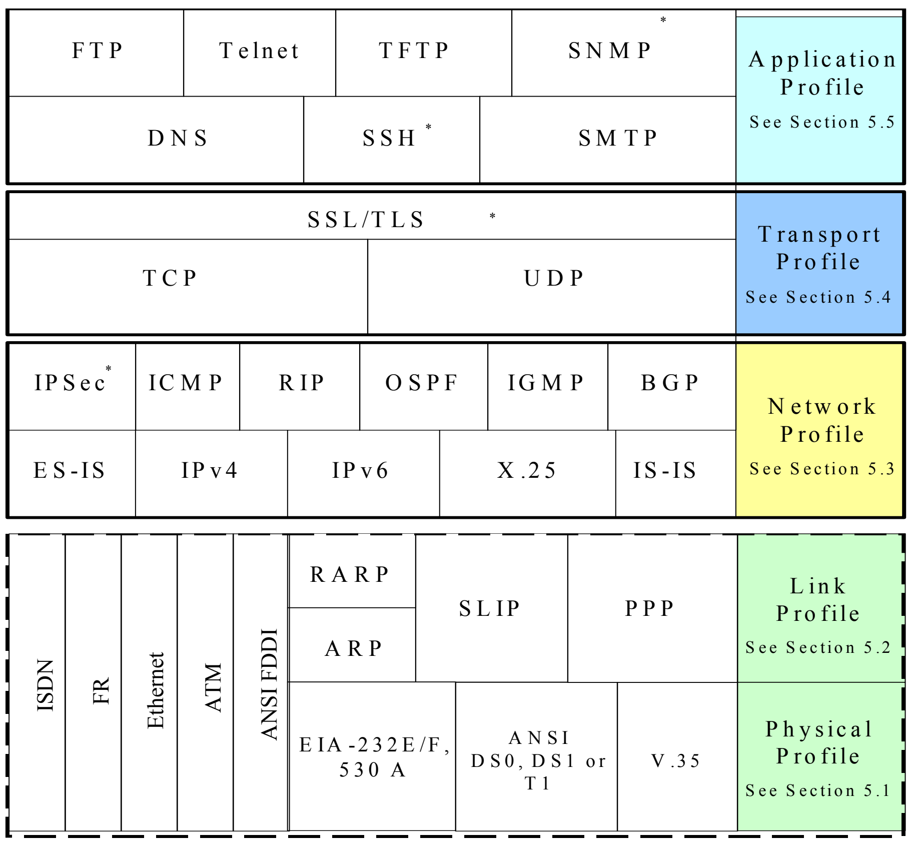
4.6 APPLICATION PROCESSES

Many applications often require special interfaces to the Application Layer (e.g., operating system). These are called Application Program Interfaces (API). This is out of the scope of this standard. Detailed requirements for the application processes can be found in the applicable interface control document (ICD).

5 DETAILED REQUIREMENTS

This section specifies the communication protocols and services which are to be implemented within the NAS data communications infrastructure. Contained in the following sections are the profile recommendations that will provide a consistent and uniform data transmission environment across FAA networks. Compliance with these recommendations will allow the same services and features to be supported in all similar networks, enable network-to-network compatibility, standardize maintenance and troubleshooting, and decrease implementation costs.

The protocols are implemented at different layers of the protocol hierarchy and perform different communication services as shown in Figure 2.



* Refer to FAA-HDBK-002 or latest version of FAA-STD-045

Figure 2 NAS Communication Stack Layer Profiles

5.1 PHYSICAL SUB-PROFILE

The physical layer is specified in this standard for the following characteristics:

- Mechanical – Physical attributes of cables and connectors
- Electrical – Signal characteristics
- Functional – Synchronization and Control of media

Users may be directly connected to a NAS access LAN or backbone Wide Area Network (WAN). Access LAN end-systems typically adhere to the available access LAN sub-profiles, which are based on Ethernet, Token Ring, or serial interface protocols. Backbone WAN end-systems adhere to the backbone WAN sub-profile, which are typically based on Frame Relay, X.25 LAPB, ATM, or any desired wide area networking technology. Access LAN end-systems are connected to backbone WAN and remote LAN end systems via a NAS multiprotocol router.

NAS communication elements should implement at least one of the following standards. However, these standards do not preclude the use of other physical interfaces that are in accordance with project Interface Control Documents (ICDs).

5.1.1 Physical Interfaces

The following standards are allowable physical interface implementations in the NAS are described in the following paragraphs.

5.1.1.1 TIA/EIA-232-E/F

The TIA/EIA-232-E/F should be implemented according to TIA/EIA-232-E/F documents or project ICDs.

5.1.1.2 TIA/EIA-530-A

The TIA/EIA-530-A should be implemented according to TIA/EIA-530-A document.

5.1.1.3 V.35

The V.35 should be implemented according to ITU-T V.35 document.

5.1.1.4 DS0, DS1, and T1

The ANSI D0, D1 and T1 should be implemented according to relevant ANSI documents or project ICDs.

5.1.1.5 Ethernet

Transmission of IPv4 datagrams over Ethernet networks should be in accordance with RFC 894. IPv6 based networks should conform to RFC-2464.

5.1.1.6 FDDI

Transmission of IPv4 datagrams over FDDI networks should be in accordance with RFC-1390. Transmission of IPv6 datagrams over FDDI networks should be in accordance with RFC-2467.

5.1.1.7 Frame Relay (FR)

Transmission of IPv4 datagrams over Frame Relay should be done in accordance with RFC-2427.

Transmission of IPv6 datagrams over Frame Relay should be done in accordance with RFC-2590.

5.1.1.8 Asynchronous Transfer Mode (ATM)

Transmission of IPv4 datagrams over ATM networks should be done in accordance with RFC-2225 and RFC-2331.

Transmission of IPv6 datagrams over ATM networks should be done in accordance with RFC 2492.

5.1.1.9 ISDN

The ISDN should be implemented according to RFC-1356.

5.2 LINK SUB-PROFILE

The link sub-profile specifies the link layer protocols. The link sub-profile protocols should be implemented on top of compatible physical interface.

NAS communication elements should implement at least one of the following standards. However, these standards do not preclude the use of other link protocols that are in accordance with project Interface Control Documents (ICDs).

5.2.1 Link protocols

The following standards are allowable link layer implementations in the NAS are described in the following paragraphs.

5.2.1.1 Ethernet

Transmission of IPv4 datagrams over Ethernet networks should be in accordance with RFC 894. IPv6 based networks should conform to RFC-2464. Transmission of IP datagrams over IEEE 802.3 networks should be in accordance with RFC-1042.

5.2.1.2 FDDI

Transmission of IPv4 datagrams over FDDI networks should be in accordance with RFC-1390. Transmission of IPv6 datagrams over FDDI networks should be in accordance with RFC-2467.

5.2.1.3 Frame Relay (FR)

Transmission of IPv4 datagrams over Frame Relay should be done in accordance with RFC-2427.

Transmission of IPv6 datagrams over Frame Relay should be done in accordance with RFC-2590.

5.2.1.4 Asynchronous Transfer Mode (ATM)

Transmission of IPv4 datagrams over ATM networks should be done in accordance with RFC-2225 and RFC-2331.

Transmission of IPv6 datagrams over ATM networks should be done in accordance with RFC 2492.

5.2.1.5 Point-to-Point Protocol (PPP)

The PPP should be in accordance with RFC-1661 and RFC-2153.

Transmission of IPv4 datagrams over PPP should be in accordance with RFC-1332.

Transmission of IPv6 datagrams over PPP should be done in accordance with RFC-2472.

5.2.1.6 SLIP

The SLIP should be implemented according to RFC-1055.

5.2.1.7 ISDN

The ISDN should be implemented according to RFC-1356.

5.2.1.8 ARP

The ARP protocol should be implemented according to RFC-826.

5.2.1.9 RARP

The RARP protocol should be implemented according to RFC-903.

5.3 NETWORK SUB-PROFILE

The network sub-profile specifies the protocols that provide services corresponding to the network layer. The protocol used in this layer for the NAS shall be Internet Protocol (IP). IP is designed for use in interconnected packet-switched computer communication networks and provides addressing and fragmentation services.

Note: In general, IP is not an inherently reliable communication facility. If a higher quality of service is desired, those features should be implemented by a higher layer protocol.

5.3.1 Internet Protocol (IP)

Two versions of this protocol shall be allowable for the NAS – the commonly available IPv4, and the upcoming IPv6 (see Section 6 for a discussion and comparison of these protocols).

IPv4 implementations shall be in accordance with RFC-791.

IPv6 implementations shall be in accordance with RFC-2460.

In addition, both IPv4 and IPv6 implementations shall include the capabilities of RFC-2474, RFC-3168, and RFC-3260.

5.3.1.1 Network addressing

Network addressing should be in accordance with RFC-796 for IPv4 implementations in NAS networks. IPv6 implementations in the NAS should be in accordance with RFC-2373.

5.3.1.2 Subnet extensions

Subnet extensions to the addressing architecture for IPv4 networks in the NAS should be in accordance with RFC-950.

Note: This capability is not required for IPv6.

5.3.1.3 IP multicasting

Multicasting implementations in the NAS should be in accordance with RFC-1112 and RFC-3376.

5.3.1.4 Neighbor Discovery IPv6

Neighbor discovery for IPv6 should be done in accordance with RFC-2461.

Note: This capability is not applicable for IPv4.

5.3.1.5 Tunneling over IPv4

Tunneling of datagrams (e.g., CLNP, ES-IS) over IPv4 should be done in accordance with RFC-2784.

5.3.1.6 Tunneling over IPv6

Tunneling of datagrams (e.g., CLNP, ES-IS) over IPv6 should be done in accordance with RFC-2473.

5.3.1.7 Interfacing Between IPv6 Systems and IPv4 Networks

Establishment of compatibility between IPv6 systems (e.g., hosts and routers) with IPv4 networks should be done in accordance with mechanisms described in RFC-2893.

5.3.2 Routing

Routing is a network management function responsible for forwarding packets from their source to their ultimate destination. Disparately managed networks are referred to as autonomous systems. Routers used for information exchange within autonomous systems are called interior routers, and they exchange network connectivity parameters in accordance with a particular Interior Gateway Protocol (IGP). Routers that move information between autonomous systems are exterior routers, and they exchange limited network connectivity information in accordance with a mutually agreeable Exterior Gateway Protocol (EGP).

5.3.2.1 Interior Gateway Protocols (IGP)

NAS IPv4 interior routers should support at least one of the following IGPs:

- Routing Information Protocol (RIP), in accordance with RFC-1058 and RFC-2453
- Open Shortest Path First (OSPF), in accordance with RFC-2328
- IS-IS, in accordance with ISO 10589, or RFC-1195, along with RFC-2474, and RFC-3260 when implementing Differentiated services enhancements to the Internet protocol, and RFC-3168 when incorporating Explicit Congestion Notification) to TCP and IP.

Implementation of the ISO Standard 9542 End System to Intermediate System (ES-IS) protocol in the NAS IP environment should be done with the mechanism prescribed in RFC 2473.

NAS IPv6 interior routers should support at least one of the following IGPs:

- RIPng, in accordance with RFC 2080
- OSPFv3, in accordance with RFC 2740
- IS-IS, in accordance with ISO 10589, or RFC 1142, along with RFC-2474, and RFC-3260 when implementing Differentiated services enhancements to the Internet protocol, and RFC-3168 when incorporating Explicit Congestion Notification) to TCP and IP.

5.3.2.2 5.2.2.2 Exterior Gateway Protocols (EGP)

NAS IPv4 exterior routers should support at least one of the following EGPs:

- Routing Border Gateway Protocol 4 (BGP 4) for inter autonomous system, in accordance with RFC 1771
- IDRP, in accordance with ISO 10747 for international application see note below

Note: ATN routing implementation should be done in accordance with ICAO Document 9705 and ICAO Document 9739.

NAS IPv6 exterior routers should support at least one of the following:

- RFC 2545 for conveying IPv6 routing information among routers compliant with this RFC
- RFC 2858 for mixed environments where not all routers are compliant, or where non-IPv6 protocols are also involved

5.3.3 Error detection and reporting

Error detection and reporting in IPv4 environments should be in accordance with RFC-792 and RFC-950.

Error detection and reporting in IPv6 environments should be in accordance with RFC-2463.

5.3.4 IP over X.25 and Packet-Mode ISDN

Implementations of IP (or other network protocols) over an X.25 or packet-mode ISDN infrastructure should be in accordance with RFC-1356.

5.3.5 Maximum Transmission Unit (MTU)

Sizes of MTUs for network segments and their dynamic discovery should be in accordance with RFC-1191.

5.3.6 Network Layer Security (IPSec)

Refer to latest revision of FAA-STD-045 for detailed network layer security requirements.

5.3.7 Internet Group Management Protocol (IGMP)

Implementation of Internet Group Management Protocol (IGMP) should be done in accordance with RFC-3376.

5.4 TRANSPORT SUB-PROFILE

The transport sub-profile specifies the protocols that provide services for the transport layer of the communication stack. Transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis.

The transport layer will support two sub-profiles - Connection-Oriented (CO) and Connection-Less (CL).

CO service is provided using the Transport Control Protocol (TCP), which provides reliable, in-sequence delivery of a full-duplex data stream (e.g., SMTP, File Transfer Protocol (FTP), and Telnet).

CL service is provided using the User Datagram Protocol (UDP), which offers minimal transport service and does not provide guaranteed delivery. This protocol gives applications direct access to the datagram service of the IP layer. The only services this protocol provides over IP are check summing of the data and multiplexing by port number. Therefore, applications running over UDP should deal directly with end-to-end communication problems that a CO protocol would have handled (i.e., transmission for reliable delivery, packetization and reassembly, flow control, etc.). UDP is used by applications that do not require the level of service that TCP provides, or if communications services that TCP does not provide (i.e., broadcast, multicast) are to be used.

ATN transport layer service implementation support should be done in accordance with ICAO 9705 and ICAO 9739.

5.4.1 Transmission Control Protocol (TCP)

Implementations of TCP in the NAS shall be in accordance with RFC-793 and RFC-3168.

5.4.2 User Datagram protocol (UDP)

Implementations of UDP in the NAS shall be in accordance with RFC-768.

5.4.3 Transport Layer Security (TLS) Protocol

Refer to the latest revision of FAA-STD-045 for detailed transport layer security requirements.

5.4.4 Secure Sockets Layer (SSL)

Refer to the latest revision of FAA-STD-045 for detailed transport layer security requirements.

5.5 APPLICATION SUB-PROFILE

The application sub-profile provides services corresponding to the application layer. The Application Layer enables common functions and services required by particular user-designed application processes.

Application layer services include, but are not exclusive to:

- Remote Login
- File Transfer
- Electronic Mail
- Network Management

- Support Services

The general implementation of these services should be in accordance with RFC-1123.

ATN application implementation should be done in accordance with ICAO 9705 Ed. 3 and ICAO 9739.

5.5.1 Remote login

Implementations of remote login should be in accordance with STD 8 for Telnet.

5.5.2 File transfer

The application sub-profile for NAS networks should support two file transfer protocols, as described below.

5.5.2.1 File Transport Protocol (FTP)

Implementation of the FTP over TCP should be in accordance with RFC-959 and RFC-2640.

5.5.2.2 Trivial File Transfer Protocol (TFTP)

Implementation of the file transfer protocol for UDP should be in accordance with RFC-1350, RFC-2347, RFC-2348, and RFC-2349.

5.5.3 Electronic Mail

Implementation of electronic mail for TCP should be in accordance with RFC-2821, RFC-2156, and RFC-822.

5.5.4 Support services

The following sections cover the protocols necessary to supply support services. The standard support services are domain name system, host initialization, and network management. Implementation of these services should be in accordance with RFC-1123.

5.5.4.1 Network management

Refer to FAA-HDBK-002 for detailed network management requirements.

5.5.4.2 Application Layer Security

Refer to latest revision of FAA-STD-045 for detailed application layer security requirements.

5.5.5 Domain Name Server (DNS)

Implementation of Domain Name Server (DNS) should be done in accordance with RFC-1706.

5.6 INTEROPERABILITY AND CONFORMANCE TESTING

This information is not covered in this document. System, network interoperability, and conformance testing should be done in accordance with the applicable documents for your project or program.

5.7 NAMING AND ADDRESSING

This information is not covered in this document. Refer to the applicable ICD for requirements for naming and addressing.

6 NOTES

Both IPv4 and IPv6 support connectionless services. They are functionally similar - major differences include addressing structure, native security, Quality of Service (QoS), parameters and packet formats. As a result, enhancements were provided in a series of RFC documents. The following is a tabular comparison between IPv4, IPv6, ICMPv4 and ICMPv6.

6.1 COMPARISON OF IPV4 AND IPV6 FEATURES

Services	IPv4	IPv6	Comments
Addressing Size	4 bytes	16 bytes	RFC 1888 describes an experimental method to map IPv6 addressing space to CLNP
Addressing Class Structure	4 classes or Classless Inter-Domain Routing (CIDR)	None	CLNP and IPv6 offer more efficient routing due to no class structure
Special Addressing	Multicast/ Broadcast	Multicast/ Anycast	IPv6 offers anycast addressing, to send a packet to any one of a group of nodes
Embedded Hierarchical Addresses	Not available due to IP addressing size	Not available due to IP addressing size	NSAP addressing structure supports embedded hierarchical addressing for end-to-end services.
Security	Optional support for conveyance of security level, restriction codes, and user group parameters (RFC 1108 and 1825)	Supports IPSec with RFC 2401	IPv6 supports authentication, data integrity and confidentiality, encryption, PPP, VPN under IPSec.

Services	IPv4	IPv6	Comments
Quality of Services (QoS)	Limited to ToS (See RFC 791)	QoS supported with Traffic Class and Flow Label (see RFC 2460)	QoS in CLNP and IPv6 provides more robust quality-ensuring services than IPv4
Support for Mobility	Public domain software is available that supports this functionality using RFCs 2002, 2290, and 2794.	In accordance with RFC 2026 (may be modified by Internet Draft “Mobility Support in IPv6”, July 2, 2001)	RFC not yet approved for Mobile IPv6
Header Length	4 bits, in units of 32-bit words	Removed	IPv6 does not include an Internet Header Length field
Version Identification	4 bits	4 bits	--
Segment/fragment offset	13 bits, in units of octets (Fragment)	Not present; See comment	No fragmentation allowed in basic IPv6; see Figure 4 for IPv6 extension that allows fragmentation for packets larger than Maximum Transmission Unit (MTU)
Protocol Identifier	1 Octet	1 Octet	IPv6 Next Header field is equivalent to IPv4 Protocol field

Services	IPv4	IPv6	Comments
Total length	16 bits, in units of octet	Similar to IPv4 Total Length, with exception – see Comment	IPv4 Total Length measures header and data; IPv6 Payload Length only measures data
Packet Longevity	1 Octet, in units of seconds (Time to Live)	1 Octet (Hop Limit)	CLNP and IPv4 measure packet longevity in time; IPv6 limits number of hops for each packet
Packet Header size	20-40 octet	40 Octet	IPv6 header is 40 octets. As option Extension Header can be add (see RFC 2406)
Header Checksum	2 Octet	Removed	In IPv6 error detection for packet is performed by the link layer
Flags	Don't fragment; More fragments	Removed	Fragmentation for IPv6 contained on extension header
Options	Precedence bits in ToS Strict source route Loose source route Record route Padding Timestamp N/A	Removed	IPv4 options are replaced by IPv6 extension header (see RFCs 2460, 2402, and 2406)

6.2 ERROR REPORTING

The following is a comparison of the features and services of ICMPv4 and ICMPv6.

Category	IPv4 ICMP Message	IPv6 ICMP Message	Comments
General	Parameter problem -Type 12, code 0 (see RFC 792)	Parameter problem	See note below
	Source quench - Type 4, code 0 (see RFC 792)	N/A	See note below
	Parameter problem –Type 12 , code 0 (see RFC 792)	Parameter problem	See note below
	Destination Unreachable - Fragmentation needed, but Don't Fragment flag is set -Type 3, code 4 (see RFC 792)	Packet Too Big -Type 2, code 0 (see RFC 2463)	--
Addressing-related	Destination unreachable- host unknown - Type 3, code 1 (see RFC 792)	Destination unreachable – Address unreachable -Type 1, code 3 (see RFC 2463)	Type/Code values are different between IPv4 and IPv6

Category	IPv4 ICMP Message	IPv6 ICMP Message	Comments
	Destination unreachable- Network unreachable - Type 3, code 1 (see RFCs 792 & 1122)	Destination unreachable- No routing to destination -Type 1, code 0 (see RFC 2463)	Type/Code values are different between IPv4 and IPv6
Source routing	Destination unreachable – Type 3, Code 5 (see RFCs 792)	Not supported	--
	Parameter problem – Type 12, Code 0 (see RFC 792)	Not Supported	Type/Code values are different between IPv4 and IPv6
	Destination unreachable – Type 3, Code 5 (see RFCs 792 & 1122)	Not Supported	--
Lifetime	Time Exceeded - Time to live exceeded in transit -Type 11, code 0 (see RFC 792)	Time Exceeded – hop limit exceeded in transit -Type 3, code 0 (see RFC 2463)	Type/Code values are different between IPv4 and IPv6
	Time Exceeded - fragment reassembly time exceeded -Type 11, code 1 (see RFC 792)	Time exceeded - fragment reassembly time exceeded -Type 3, code 1 (see RFC 2463)	Type/Code values are different between IPv4 and IPv6

Category	IPv4 ICMP Message	IPv6 ICMP Message	Comments
Reassembly	Time Exceeded - fragment reassembly time exceeded -Type 11, code 1 (see RFC 792)	Time exceeded - fragment reassembly time exceeded -Type 3, code 1 (see RFC 2463)	Type/Code values are different between IPv4 and IPv6
PDU discarded	Parameter problem -Type 12, code 0 (see RFC 792)	Parameter problem – Type 4, Code 2 (see RFC 2463)	See note below

Note:
An ICMPv6 Parameters Problem message is either sent by a router or by the destination. This occurs when an error is detected in either the IPv6 header or in an extension header - see RFC 2463.