MIL-STD-187-700
1 JUNE 1992

MILITARY STANDARD

INTEROPERABILITY AND PERFORMANCE STANDARDS FOR THE DEFENSE INFORMATION SYSTEM

AMSC N/A

AREA SLHC/TCTS/DCPS

FOREWORD

1. This military standard (MIL-STD) is approved for use by all departments and agencies of the Department of Defense (DoD).

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this document should be addressed to:

Defense Information Systems Agency
Joint Interoperability and Engineering Organization
ATTN: TBBB
Fort Monmouth, New Jersey 07703-5613

by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter. For immediate concerns, questions can be resolved by calling (908) 532-7720, DSN 992-7720, or by fax (908) 389-8333.

3. MIL-STD-188-100, -200, and -300 series documents contain performance standards for existing DoD long-haul and tactical communications systems. These standards apply to current analog and digital network elements used to form a connection of loosely coupled subsystems, each designed to provide a unique service. MIL-STD-187 series documents are planning standards for systems and system parameters that have not been tested. It is intended that all or part of this document will transition to a MIL-STD-188 series document as the parameters defined in this document are validated through testing.

4. We are approaching an era in which digital communications and computer networks will be combined into an information system. The Defense Information Systems Agency (DISA) and the services recognize the need to move beyond the traditional approach reflected in the MIL-STD-188 series. The purpose of this -187 series document is to provide the framework for a forward-looking standards base required to plan and design the Defense Information System (DIS). It should be understood that there are some areas in which standards direction is not yet clear. These areas are discussed in this document and they are subject to further definition.

5. This document contains the technical standards and design objectives necessary to provide a DIS that will allow strategic and tactical users to exchange all forms of information digitally. The standards contained herein are common to both tactical and strategic systems, unless otherwise specified. This document addresses all interoperability elements specified in the DIS framework, except data-processing standards such as standard programming languages and data elements.

6. The standards in this document are based on, or make reference to, corresponding parameters in other MIL-STDs, as well as American National Standards Institute (ANSI) standards, International Telegraph and Telephone Consultative Committee (CCITT) recommendations, International Organization for Standardization (ISO) standards, and NATO standardization agreements (STANAGs), wherever applicable.

(This page intentionally left blank.)

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

1. SCOPE

1.1 Purpose. The purpose of this document is to provide a baseline for planning and designing the evolving Defense Information System (DIS) defined in 1.6.

1.2 Applicability. This document is to be used in planning, designing, and developing new DIS communications systems, and in making major changes to existing systems. This document does not necessarily apply to leased commercial facilities, but such facilities should be selected to be compatible with its requirements. This document applies to digital communications systems only. Military Standard (MIL-STD)-188-100 will continue to provide the standards for analog communications systems.

1.3 Objectives. This document has five objectives:

a. To achieve interoperability between strategic and tactical digital networks for voice, data, facsimile, record traffic, and video services.

b. To provide performance standards for strategic and tactical system users.

c. To adopt specific subsets of commercial standards, where feasible, to achieve cost-effective interoperability, performance, and interfaces.

d. To provide a framework to change existing standards and prepare new standards.

e. To establish a reference source for use by all organizations involved in developing the DIS and procuring DIS-compatible hardware and software.

1.4 System standards and design objectives. When procurement, engineering, or design activities elect to incorporate this planning standard in their acquisition documents, the parameters and requirements specified in this document shall be treated as mandatory system standards if the word *shall* is used. Nonmandatory parameters, requirements, and design objectives are indicated by the word *should* (design objectives, rather than standards, are used when there is a lack of measured and verified data or no consensus on the interpretation of the data). *Will* is used to express a declaration of purpose or intent. For a definition of *system standards* and *design objectives*, see FED-STD-1037.

1.5 Standards action areas. This document addresses the interoperability, performance, and interface standards that should be met by future Department of Defense (DoD) information systems to provide a wide variety of end-to-end digital subscriber services in a single integrated network. These services include voice telephony, data transmission, facsimile, record traffic, and video. This document addresses standardization in the following major areas:

a. Subscriber services

b. Interfaces, including protocols and voice algorithms

c. Circuit and packet switching

d. Transmission

e. Signaling

f. Information security

g. Network management and system control

h. End-to-end performance requirements

Wherever possible, the standards are based on American National Standards Institute (ANSI) standards, International Telegraph and Telephone Consultative Committee (CCITT) recommendations for the Integrated Services Digital Network (ISDN), the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) reference model, and existing MIL-STD-188 series standards. This document references other existing standards (military, federal, commercial, and international). This approach avoids duplication of existing standards, ensures backward interoperability, and provides for orderly transition to forward-looking standards for new systems.

1.6 DIS framework. The standards provided in this document are based on the DIS framework (see figure 4-1) described below:

a. The DIS concept provides for an evolutionary integration of existing and future defense computer and telephone communications systems. The services and agencies adopted the DIS framework as a guide for the development of this document. The DIS framework provides efficient end-to-end integrated service for information sources, sinks, and processors. Integrated service provides for voice, message, data, graphics, and imagery information transfer across a single network interface. By definition, the DIS framework includes all

components necessary to achieve interoperability between DoD users.

b. The DIS framework consists of three major sections demarcated by reference points A and B. Users may access the DIS through subscriber network elements, such as source, sink, or processor terminal equipment. These terminal equipment include telephones, facsimile machines, and other data terminal equipment (DTE). For the information source, sink, or processor elements to be interoperable, all seven layers of the ISO OSI reference model must be interoperable.

c. DTEs exchange information through information transfer utilities. Information transfer utilities are comprised of local-network elements, wide-network elements, and their respective interoperability reference points. The military services provide fixed-plant, local-network elements to support strategic users and base operations. They also provide tactical local-network elements to support garrison operations and access to wide-network elements, as well as tactical local-network elements to support deployed combat forces. DISA provides wide-network elements to interconnect geographically separated local networks. The wide network includes the Defense Communications System (DCS) and public switched telephone networks (PSTN). Since the local- and wide-network elements and interoperability reference points in the information transfer utilities represent the telecommunications portion of DIS, their functionality is limited to the lower three layers of the OSI reference model.

d. Advances in computer and telephone communications technology allow multiple services to be provided by a single network, as in ISDN. Wherever applicable, the DIS framework allows the adoption of ANSI standards for ISDN. Within the DIS framework, circuit-switched voice and data services are based on military standards for tactical systems and ISDN commercial standards for strategic systems.

(This page intentionally left blank.)

2. APPLICABLE DOCUMENTS*

2.1 Government documents

2.1.1 Standards. The following standards form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the current issue of the Department of Defense Index of Specifications and Standards (DoDISS) and supplements thereto.

FEDERAL

FED-STD-1002	Time and Frequency Reference Information in Telecommunications Systems
FED-STD-1016	Telecommunications: Analog-to-Digital Conversion of Radio Voice by 4,800 Bit/Second Code Excited Linear Prediction (CELP)
FED-STD-1037	Glossary of Telecommunication Terms
FED-STD-1045	Telecommunications: HF Radio Automatic Link Establishment
FED-STD-1046	Telecommunications: HF Radio Automatic Networking (Draft)
FED-STD-1047	Telecommunications: HF Radio Automatic Message Exchange (Draft)
FED-STD-1048	Telecommunications: HF Radio Automatic Networking to Multimedia (Draft)
FED-STD-1049	HF Radio Automatic Operation in Stressed Environment (Draft)
FIPS 146	U.S. Government Open Systems Interconnection Profile
FIPS XXX	Government Network Management Profile (GNMP) (Draft)

*** NOTE: Only applicable sections of the referenced documents are intended to be used.**

MILITARY

MIL-STD-187-721	Draft military standard in preparation: Planning and Guidance Standard for Automated Control Applique for HF Radio
MIL-STD-188-110	Equipment Technical Design Standards for Common Long Haul/Tactical Data Modems
MIL-STD-188-111	Interoperability and Performance Standards for Fiber Optic Communications Systems
MIL-STD-188-112	Subsystem Design and Engineering Standards for Common Long Haul/Tactical Cable and Wire Communications
MIL-STD-188-113	Interoperability and Performance Standards for Analog-to-Digital Conversion Techniques
MIL-STD-188-114	Electrical Characteristics of Digital Interface Circuits
MIL-STD-188-115	Interoperability and Performance Standards for Communications Timing and Synchronization Subsystems
MIL-STD-188-124	Grounding, Bonding and Shielding for Common Long Haul/Tactical Communication Systems Including Ground Based Communications-Electronics Facilities and Equipments
MIL-STD-188-131	Draft military standard: Interoperability and Performance Standard for Video Teleconferencing
MIL-STD-188-132	Audiographics Conferencing (Draft)
MIL-STD-188-140	Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the Low Frequency Band and Lower Frequency Bands

MIL-STD-188-141	Interoperability and Performance Standards for Medium and High Frequency Radio Equipment
MIL-STD-188-145	Interoperability and Performance Standards for Digital LOS Microwave Radio Equipment
MIL-STD-188-146	Interoperability and Performance Standards for Satellite Communications
MIL-STD-188-148	Interoperability Standard for AJ Communications in the High Frequency (2-30 MHz) Band (U), SECRET
MIL-STD-188-161	Interoperability and Performance Standards for Digital Facsimile Equipment
MIL-STD-188-190	Methods for Communications Systems Measurements
MIL-STD-188-194	Integrated Services Digital Network Profile (ISDNP) (Draft)
MIL-STD-188-200	System Design and Engineering Standards for Tactical Communications
MIL-STD-188-202	Interoperability and Performance Standards for Tactical Digital Transmission Groups (Coaxial Cable)
MIL-STD-188-203-1	Subsystem Design and Engineering Standards for Tactical Digital Information Link (TADIL) A
MIL-STD-188-203-2	Subsystem Design and Engineering Standards for Tactical Digital Information Link (TADIL) B
MIL-STD-188-203-3	Subsystem Design and Engineering Standards for Tactical Digital Information Link (TADIL) C
MIL-STD-188-216	Interoperability Standards for Data Adapter Control Mode

MIL-STD-188-242	Interoperability and Performance Standards for Tactical Single Channel Very High Frequency (VHF) Radio Equipment
MIL-STD-188-243	Interoperability and Performance Standards for Tactical Single Channel Ultra High Frequency (UHF) Radio Communications
MIL-STD-188-260	Design and Engineering Standards for Tactical Terminal Subsystems
MIL-STD-188-313	Subsystem Design and Engineering Standards and Equipment Technical Design Standards for Long Haul Communications Transversing Microwave (LOS) Radio and Tropospheric Scatter Radio
MIL-STD-188-347	Standards for Long Haul Communications Equipment Technical Design Standards for Digital End Instruments and Ancillary Devices
MIL-STD-210	Climatic Information to Determine Design and Test Requirements for Military Systems and Equipment
MIL-STD-449	Radio Frequency Spectrum Characteristics, Measurement of
MIL-STD-461	Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference
MIL-STD-462	Electromagnetic Interference Characteristics, Measurement of
MIL-STD-470	Maintainability Program for Systems and Equipment
MIL-STD-471	Maintainability Verification/ Demonstration/Evaluation
MIL-STD-781	Reliability Testing for Engineering Development, Qualification, and Production

MIL-STD-785	Reliability Program for Systems and Equipment Development and Production
MIL-STD-810	Environmental Test Methods and Engineering Guidelines
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1777	Internet Protocol
MIL-STD-1778	Transmission Control Protocol
MIL-STD-1782	Telnet Protocol
MIL-STD-2045-38000	Network Management for DoD Communications (Draft)

2.1.2 Military specifications

MIL-H-46855	Human Engineering Requirements for Military Systems, Equipment and Facilities

2.1.3 Military handbooks

MIL-HDBK-232	RED/BLACK Engineering Installation Guidelines
MIL-HDBK-235	Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment, Subsystems and Systems
MIL-HDBK-237	Electromagnetic Compatibility Management Guide for Platforms, Systems and Equipment
MIL-HDBK-241	Design Guide for Electromagnetic Interference (EMI) Reduction in Power Supplies
MIL-HDBK-253	Guidance for the Design and Test of Systems Protected Against the Effects of Electromagnetic Energy
MIL-HDBK-419	Grounding, Bonding and Shielding

2.1.4 Other DoD publications

DCAC 370-175-13	Defense Switched Network (DSN) System Interface Criteria
DoD 5200.28-STD	Department of Defense Trusted Computer System Evaluation Criterion
Joint Pub 6-01.1	Tactical Digital Information Link (TADIL) Message Standards
Joint Pub 6-05	Manual for Employing Joint Tactical Communications Systems
JTC3A Specification 9001	Joint Technical Interface Specification for VHF SINCGARS Waveform
JTC3A Specification 9109	Technical Interface Specification; Joint Interoperability via Fiber Optic Cable
NACSEM 5201	TEMPEST Guidelines for Equipment/ System Design (U)
NSTISSAM TEMPEST/ 1-91	Compromising Emanations Laboratory Test Requirements, Electromagnetics (U)
SR-RG-83-9-B	Technical Interface Design Plan for ATDL-1
TT-A3-9012-0046	Digital Loop Signaling/Supervision Plan
TT-A3-9016-0056	Digital Common Channel Signaling/Supervision Plan

2.1.5 Standardization Agreements (STANAG)

STANAG 4175	Technical Characteristics of the Multi-Functional Information Distribution System (MIDS)
STANAG 4206	The NATO Multi-Channel Tactical Digital Gateway System Standards

STANAG 4207	The NATO Multi-Channel Tactical Digital Gateway Multiplex Group Framing Standards
STANAG 4208	The NATO Multi-Channel Tactical Digital Gateway Signalling Standards
STANAG 4209	The NATO Multi-Channel Tactical Digital Gateway Standards for Analogue-to-Digital Conversion of Speech Signals
STANAG 4210	The NATO Multi-Channel Tactical Digital Gateway Cable Link Standards
STANAG 4211	The NATO Multi-Channel Tactical Digital Gateway System Control Standards
STANAG 4212	The NATO Multi-Channel Tactical Digital Gateway Radio Relay Link Standards
STANAG 4214	International Routing and Directory for Tactical Communications Systems
STANAG 4249	The NATO Multi-Channel Tactical Digital Gateway -- Data Transmission Standards (Packet Switching Service)
STANAG 4251	NATO Reference Model for Open Systems Interconnection Layer 1 (Physical Layer) Service Definition
STANAG 4252	NATO Reference Model for Open Systems Interconnection Layer 2 (Data Link Layer) Service Definition
STANAG 4253	NATO Reference Model for Open Systems Interconnection Layer 3 (Network Layer) Service Definition
STANAG 4254	NATO Reference Model for Open Systems Interconnection -- Layer 4 (Transport Layer) Service Definition (Draft)

STANAG 4255	NATO Reference Model for Open Systems Interconnection -- Layer 5 (Session Layer) Service Definition (Draft)
STANAG 4256	NATO Reference Model for Open Systems Interconnection -- Layer 6 (Presentation Layer) Service Definition (Draft)
STANAG 4259	NATO Reference Model for Open Systems Interconnection Encoding Rules for ASN.1
STANAG 4261	NATO Reference Model for Open Systems Interconnection Layer 1 (Physical Layer) Protocol Specification
STANAG 4262	NATO Reference Model for Open Systems Interconnection Layer 2 (Data Link Layer) Protocol Specification; Annex D, Data Link Access Procedure Balanced (LAPB)
STANAG 4263	NATO Reference Model for Open Systems Interconnection Layer 3 (Network Layer) Protocol Specification, Annex D, X.75 Packet Level Protocol (STE-STE)
STANAG 4264	NATO Reference Model for Open Systems Interconnection -- Layer 4 (Transport Layer) Protocol Specification (Draft)
STANAG 4265	NATO Reference Model for Open Systems Interconnection -- Layer 5 (Session Layer) Protocol Specification (Draft)
STANAG 4266	NATO Reference Model for Open Systems Interconnection -- Layer 6 (Presentation Layer) Protocol Specification (Draft)
STANAG 4290	The NATO Multi-Channel Tactical Digital Gateway Cable Link (Optical) Standards

STANAG 4372	Second-generation Anti-jam Tactical UHF Radio for NATO (SATURN)
STANAG 4406	Military Message Handling System
STANAG 5516	Tactical Data Exchange Link-16

2.1.6 NIST publications

NIST IR90-4250	Network Transport and Message Security Protocols
NIST Special Publication 500-183	National Institute of Standards and Technology (NIST) Special Publication 500-183, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 4, Edition 1

[Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Commanding Officer, Naval Publications and Forms Center (ATTN: NPODS), 5901 Tabor Avenue, Philadelphia, PA 19120-5099.]

[Copies of Federal Information Processing Standards (FIPS) are available to Department of Defense activities from the Commanding Officer, Naval Publications and Forms Center, 5901 Tabor Avenue, Philadelphia, PA 19120-5099. Others must request copies of FIPS from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161-2171.]

[To obtain other DoD publications (see 2.1.4) not found in the DoDISS, contact the Defense Information Systems Agency, Center for Standards, ATTN: TBBF (C3A-STC) Fort Monmouth, NJ 07703-5613.]

(STANAGs. Copies of STANAGs, required by contractors in connection with specific acquisition functions, should be obtained from the contracting activity or as directed by the contracting officer.)

[NIST documents can be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161-2171 or by calling 1-800-553-6847.]

(Requests for NACSEM 5201 and NSTISSAM TEMPEST/1-91 should be submitted to the National TEMPEST Information Center, Attention C941, National Security Agency, Fort George Meade, MD 20899.)

2.2 Nongovernment documents

2.2.1 CCITT recommendations. The CCITT is part of the United Nations, a treaty organization. The United States Government participates in it through the Department of State, and although industry representatives may work on its committees, approval of standards (called recommendations) is by governments.

CCITT E.163	Numbering Plan for the International Telephone Service
CCITT E.164	Numbering Plan for the ISDN Era
CCITT F.69	Plan for Telex Destination Codes
CCITT G.703	Physical/Electrical Characteristics of Hierarchical Digital Interfaces
CCITT G.704	Synchronous Frame Structures Used at Primary and Secondary Hierarchical Levels
CCITT G.707	Synchronous Digital Hierarchy Bit Rates
CCITT G.708	Network Node Interface for the Synchronous Digital Hierarchy
CCITT G.709	Synchronous Multiplexing Structure
CCITT G.721	32 kbps Adaptive Pulse Code Modulation
CCITT G.811	Timing Requirements at the Outputs of Primary Reference Clocks Suitable for Plesiochronous Operation of International Digital Links
CCITT H.320	Narrowband Visual Telephone Systems and Terminal Equipment
CCITT I.121	Broadband Aspects of ISDN
CCITT I.150	Broadband Integrated Services Digital Network (B-ISDN) ATM Functional Characteristics (Draft)

CCITT I.211	Broadband Integrated Services Digital Network (B-ISDN) Service Aspects (Draft)
CCITT I.311	Broadband Integrated Services Digital Network (B-ISDN) General Network Aspects (Draft)
CCITT I.321	Broadband Integrated Services Digital Network (B-ISDN) Protocol Reference Model and its Application (Draft)
CCITT I.327	Broadband Integrated Services Digital Network (B-ISDN) Functional Architecture (Draft)
CCITT I.361	Layer Specification (Draft)
CCITT I.363	B-ISDN ATM Adaptation Layer (AAL) Specification (Draft)
CCITT I.432	B-ISDN User-Network Interface Physical Layer Specification (Draft)
CCITT I.460	Multiplexing, Rate Adaptation and Support of Existing Interfaces
CCITT M.20	Maintenance Philosophy for Telecommunications Networks
CCITT M.30	Principles for a Telecommunications Management Network
CCITT M.36	Principles for the Maintenance of ISDNs
CCITT Q.704	Signalling Network Functions and Messages
CCITT Q.774	Transaction Capabilities Procedure
CCITT Q.920	ISDN User-Network Interface Data Link Layer -- General Aspects
CCITT Q.921	ISDN User-Network Interface -- Data Link Layer Specification

CCITT Q.922	ISDN-Data Link Layer Specification for Frame Mode Bearer Service
CCITT Q.931	ISDN User-Network Interface Layer 3 Specification for Basic Call Control
CCITT V.35	Data Transmission at 48 Kilobits Per Second Using 60-108 kHz Group Band Circuits
CCITT V.110	Support of Data Terminal Equipments (DTEs) with V-Series Type Interfaces by an Integrated Services Digital Network (ISDN)
CCITT X.25	Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit
CCITT X.31	Support of Packet Mode Terminal Equipment by an ISDN
CCITT X.75	Packet-Switched Signalling System Between Public Networks Providing Data Transmission Services
CCITT X.121	International Numbering Plan for Public Data Networks
CCITT X.224	Transport Protocol Specification for Open Systems Interconnection for CCITT Applications
CCITT X.290	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications
CCITT X.400	Message Handling System and Service Overview
CCITT X.410	Message Handling System: Remote Operations and Reliable Transfer Service (Red Book)

CCITT X.435	Electronic Data Interchange (EDI) (Draft)
CCITT X.500	The Directory -- Overview of Concepts, Models and Services

2.2.2 ANSI standards

ANSI T1.101	Synchronization Interface Standards for Digital Service
ANSI T1.105	Digital Hierarchy -- Optical Interface Rates and Formats Specifications
ANSI T1.106	Digital Hierarchy -- Optical Interface Specifications (Single Mode)
ANSI T1.111	Signalling System Number 7 (SS7) -- Message Transfer Part (MTP)
ANSI T1.112	Signalling System Number 7 (SS7) -- Signalling Connection Control Part (SCCP)
ANSI T1.113	Signalling System Number 7 (SS7) -- Integrated Services Digital Network (ISDN) User Part
ANSI T1.114	Signalling System Number 7 (SS7) -- Transaction Capability Application Part (TCAP)
ANSI T1.408	ISDN Primary Rate -- Customer Installation Metallic Interfaces, Layer 1 Specification
ANSI T1.601	Integrated Services Digital Network (ISDN) -- Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification)
ANSI T1.602	Integrated Services Digital Network (ISDN) -- Data-Link Layer Signalling Specification for Application at the User-Network Interface

ANSI T1.605	Integrated Services Digital Network (ISDN) -- Basic Access Interface for S and T Reference Points (Layer 1 Specification)
ANSI T1.606	Integrated Services Digital Network (ISDN) -- Architectural Framework and Service Description for Frame-Relaying Bearer Service
ANSI T1.607	Digital Subscriber Signalling System No. 1 -- Layer 3 Signalling Specification for Circuit Switched Bearer Service
ANSI T1.608	Digital Subscriber Signalling System No. 1 (DSS1) -- Signalling Specification for X.25 Packet Switched Bearer Service
ANSI T1.609	Interworking Between the ISDN User -- Network Interface Protocol and the Signalling System Number 7 ISDN User Part
ANSI T1.610	Digital Subscriber Signalling System No. 1 (DSS1) -- Generic Procedures for the Control of ISDN Supplementary Services
ANSI T1.617	Integrated Services Digital Network (ISDN) -- Digital Subscriber Signaling System No. 1 (DSS1) -- Signaling Specification for Frame Relay Bearer Service
ANSI T1.618	Integrated Services Digital Network (ISDN) -- Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service

2.2.3 ISO/IEC documents

TR 10000	Information Technology -- Framework and Taxonomy of International Standardized Profiles -- Part 1: Framework and Part 2: Taxonomy of Profiles

ISO 3166	Codes for the Representation of Names of Countries
ISO 3309	Information Processing Systems -- Data Communication - High-Level Data Link Control Procedures -- Frame Structure
ISO 4335	Information Processing Systems -- Data Communication -- High-Level Data Link Control Elements of Procedures
ISO 6523	Data Interchange -- Structure for the Identification of Organizations
ISO 7498	Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- X-ref: CCITT X.200
ISO 7809	Information Processing Systems -- Data Communication -- High-Level Data Link Control Procedures -- Consolidation of Classes of Procedures
ISO 8072	Information Processing Systems -- Open Systems Interconnection -- Transport Service Definition -- X-ref: CCITT X.214
ISO 8073	Information Processing Systems -- Open Systems Interconnection -- Connection Oriented Transport Protocol Specification -- X-ref: CCITT X.224
ISO 8208	Information Processing Systems -- Data Communications -- X.25 Packet Level Protocol for Data Terminal Equipment -- X-ref: CCITT X.25
ISO 8326	Information Processing Systems -- Open Systems Interconnection -- Basic Connection Oriented Session Service Definition -- See: CCITT X.215

ISO 8327	Information Processing Systems -- Open Systems Interconnection -- Basic Connection Oriented Session Protocol Specification -- See: CCITT X.225
ISO 8348	Information Processing Systems -- Data Communications -- Network Service Definition -- X-ref: CCITT X.213
ISO 8471	Data Communication -- High-Level Data Link Control Balanced Classes of Procedures -- Data-Link Layer Address Resolution/Negotiation in Switched Environments
ISO 8473	Information Processing Systems -- Data Communications, Protocol for Providing the Connectionless -- Mode Network Service
ISO 8571-1	Information Processing Systems -- Open Systems Interconnection -- File Transfer, Access and Management -- Part 1: General Introduction
ISO 8571-2	Information Processing Systems -- Open Systems Interconnection -- File Transfer, Access and Management -- Part 2: Virtual Filestore Definition
ISO 8571-3	Information Processing System -- Open Systems Interconnection -- File Transfer, Access and Management -- Part 3: File Service Definition
ISO 8571-4	Information Processing System -- Open Systems Interconnection -- File Transfer, Access and Management -- Part 4: File Protocol Specification

ISO 8613 (Parts 1, 2, and 4-8)	Information Processing -- Text and Office Systems -- Office Document Architecture (ODA) and Interchange Format -- Part 1: Introduction and General Principles -- X-ref: CCITT T.411
ISO 8649	Information Processing Systems -- Open Systems Interconnection -- Service Definition for the Association Control Service Element -- See: CCITT X.217
ISO 8650	Information Processing Systems -- Open Systems Interconnection -- Protocol Specification for the Association Control Service Element -- See: CCITT X.227
ISO 8802-2	Information Processing Systems -- Local Area Networks -- Part 2: Logical Link Control
ISO 8802-3	CSMA/CD Media Access Control
ISO 8802-4	Token Bus Media Access Control
ISO 8802-5	Token Ring Media Access Control
ISO 8822	Information Processing Systems -- Open Systems Interconnection -- Connection Oriented Presentation Service Definition -- See: CCITT X.216
ISO 8823	Information Processing Systems -- Open Systems Interconnection -- Connection Oriented Presentation Protocol Specification -- See: CCITT X.226
ISO 8824	Information Processing Systems -- Open Systems Interconnection -- Specification of Abstract Syntax Notation One (ASN.1) -- See: CCITT X.208

ISO 8825	Information Processing Systems -- Open Systems Interconnection -- Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) -- See: CCITT X.209
ISO 8878	Information Processing Systems -- Data Communication -- Use of X.25 to Provide the OSI Connection Mode Network Service (CONS)
ISO 8880	Information Processing System -- Open Systems Interconnection -- Protocol Combinations to Provide and Support the OSI Network Service
ISO 8885	Information Processing Systems -- Data Communication High Level Data Link Control (HDLC) Procedures -- General Purpose XID Frame Information Field Content and Format
ISO 8886	Information Processing Systems -- Data Communication -- Data Link Service Definition for Open Systems Interconnection -- See: CCITT X.212
ISO 9040	Information Processing Systems -- Open Systems Interconnection -- Virtual Terminal Service
ISO 9314	Fibre Distributed Data Interface (FDDI)
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 DIS 9595	Open Systems Interconnection -- Management Information Service Specification Overview and Definition

ISO DIS 9596	Open Systems Interconnection -- Management Information Protocol Specification Overview and Definition
ISO 9646	Open Systems Interconnection -- Conformance Testing Methodology and Framework
ISO DIS 10165-1	Information Technology -- Open Systems Interconnection -- Management Information Services Part 1: Structure of Management Information
ISO DIS 10165-2	Information Technology -- Open Systems Interconnection -- Management Information Services Part 2: Definition of Management Information
ISO DIS 10165-4	Information Technology -- Open Systems Interconnection -- Management Information Services Part 4: Guidelines for the Definition of Managed Objects
ISO DIS 10589	Information Processing System -- Intermediate System to Intermediate System Routing Protocols
ISO XXXX	Remote Operations Service Element (ROSE) (Draft)
ISP 10607 (6 Parts)	Information Technology -- International Standardized Profile AFTnn -- File Transfer, Access, and Management (Draft)
ISP 10608 (Parts 1, 2, and 5)	Information Technology -- International Standardized Profile TAnnnn -- Connection-Mode Transport Service Over Connectionless-Mode Network Service (Draft)

ISP 10609 (9 Parts)	Information Technology -- International Standardized Profile TB, TC, TD and TE -- Connection -- Mode Transport Service Over Connection Mode Network Service (Draft)

2.2.4 IEEE standards

IEEE 802.1D	MAC Bridges
IEEE P802.1 G/1D	Remote MAC Bridge
IEEE 802.6	Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN)

(NOTE: IEEE 802.3, 802.4, and 802.5 are referenced as ISO 8802-3, 8802-4, and 8802-5.)

2.2.5 Request for comments

RFC 1006	ISO Transport Service on Top of the TCP; Version: 3
RFC 1086	ISO -- TP0 Bridge Between TCP and X.25

2.2.6 Electronic Industries Association

EIA 232	Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
EIA 422	Electrical Characteristics of Balanced Voltage Digital Interface Circuits
EIA 423	Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits

[American National Standards Institute (ANSI). Copies of ANSI standards may be obtained from: American National Standards Institute, 1430 Broadway, New York, NY 10018.]

[International Telegraph and Telephone Consultative Committee (CCITT). Copies of CCITT standards may be obtained from: National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.]

(Copies of ISO standards may be obtained from: American National Standards Institute, 1430 Broadway, New York, NY 10018.)

(Copies of IEEE standards may be obtained from: Secretary, IEEE Standards Board, Institute of Electrical and Electronics Engineers, Inc., P.O. Box 1331, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA.)

(RFCs may be obtained from: SRI International, Room EJ291, Network Information Systems Center, 333 Ravenswood Avenue, Menlo Park, CA 94025, USA.)

(Copies of EIA standards may be obtained from ANSI or EIA, Electronic Industries Association, Engineering Department, 2001 Eye Street, Northwest Washington, D.C. 20006.)

2.3 Order of precedence. In the event of a conflict between this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

(This page intentionally left blank.)

3. DEFINITIONS

3.1 Definitions of terms. Definitions of terms used in this document shall be as specified in Federal Standard (FED-STD)-1037. Those definitions unique to information systems, and not defined in FED-STD-1037, are provided in this section.

Functional profiles: DoD functional profiles are defined using Government Open Systems Interconnection Profile (GOSIP) protocols and ISO/IEC TR 10000. A functional profile is defined by a combination of base standards necessary to support a specific information transfer function. A functional profile once defined standardizes all options and other variations allowed by the base standards. It also provides for the development of uniform, internationally recognized tests. Further, it ensures interoperability between different network elements and terminal equipment that implement a specific profile.

Generic flow control: Bit sequence contained in the Asynchronous Transfer Mode (ATM) cell header to assist the user facility in controlling the flow of traffic into the network in order to support different quality of service (QOS).

Local-network elements: Local-network elements are the elements that make up a base information transfer utility for strategic users or a tactical information transfer utility for tactical users. They include such elements as circuit and packet switches and transmission equipment.

Reference point A: The interface between the subscriber-network elements and the local-network elements.

Reference point B: The interface between the local-network elements and the wide-network elements.

Reference point B (NATO): The interface between U.S. network elements and NATO network elements.

Strategic user: A person, organization, or other entity (including a computer or computer system) not assigned to a combat unit that employs the services provided by a telecommunications system, or by an information processing system, for transfer of information to others.

Subscriber-network elements: Elements such as terminal equipment, end systems, intermediate systems, local-area networks, metropolitan-area networks, and radio networks.

Tactical user: A person, organization, or other entity (including a computer or computer system) assigned to a combat unit that employs the services provided by a telecommunications system, or by an information processing system, for transfer of information to others.

Virtual Channel Indicator (VCI): Defines the explicit cell channel identification at the user-to-network interface (UNI) and network-to-node interface (NNI).

Virtual Path Indicator (VPI): Defines the explicit cell path identification at the UNI and NNI.

Wide-network elements: Elements, such as circuit switches, packet switches, and transmission equipment, that form the Defense Communications System (DCS) and PSTNs.

3.2 Acronyms and abbreviations used in this standard

AAL	ATM adaptation layer
ACSE	associated control service elements
A-D	analog-to-digital
ADPCM	adaptive differential pulse-code modulation
AFI	authority and format identifier
AJ	anti-jam
ALE	automated link establishment
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
ASN.1	abstract syntax notation 1
ATM	asynchronous transfer mode
AUI	attachment unit interface
B	bearer channel
BER	bit error ratio
B-ISDN	broadband ISDN

BITE	built-in test equipment
BNZS	bipolar with N-zero substitution
B8ZS	bipolar with 8-zero substitution
bps	bit(s) per second
BRI	basic rate interface
CATV	cable television
CBR	constant bit rate
CC	country code
CCIR	International Radio Consultation Committee
CCITT	International Telegraph and Telephone Consultative Committee
CELP	code excited linear prediction
CL	connectionless
CLNS	connectionless network service
CLP	cell loss priority
CLSF	connectionless service function
CLTS	connectionless transport service
CNR	combat net radio
COMPUSEC	computer security
COMSEC	communications security
CONS	connection-oriented network service
CONUS	Continental United States
COTS	connection-oriented transport service
CRC	cyclic redundancy check
CSMA/CD	carrier sense multiple access/collision detection

CSN	circuit-switched network
CTIA	Cellular Telecommunications Industry Association
CVSD	continuously variable slope delta
D	D-channel
DACS	Digital Access and Cross-Connect System
dc	direct current
DCA	Defense Communications Agency
DCAC	DCA circular
DCC	data country code
DCE	data circuit-terminating equipment
DCEC	Defense Communications Engineering Center
DCN	Data Communications Network
DCS	Defense Communications System
DDN	Defense Data Network
DIS	Defense Information System; Draft International Standard
DISA	Defense Information Systems Agency
DISP	Draft International Standardized Profile
DL	data link
DLSAP	data-link service access point
DoD	Department of Defense
DoDISS	Department of Defense Index of Specifications and Standards
DQDB	distributed queue dual-bus directory service
DSN	Defense Switched Network
DSP	domain specific part

DSS1	Digital Subscriber Signaling System Number 1
DTE	data terminal equipment
DTH	down-the-hill
DTMF	dual-tone multifrequency
DU	data unit
ECCM	electronic counter-countermeasures
EDI	Electronic Data Interchange
EFS	error-free second
EHF	extremely high frequency
EIA	Electronic Industries Association
ELF	extremely low frequency
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMSEC	emission security
ES	end system
ETSI	European Telecommunications Standards Institute
EW	electronic warfare
FADU	file access data unit
FAS	frame alignment signal
F-bit	frame bit
FDDI	Fiber Distributed Data Interface
FEC	forward error correction
FED-STD	federal standard
FIPS	Federal Information Processing Standard
FRM	frame relay mode

FSK	frequency-shift keying
FTAM	file transfer, access, and management
GFC	generic flow control
GHz	gigahertz
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GSA	General Services Administration
GSM	Special Mobile Group
H	high-rate channel
H_0	384 kbps
H_{10}	1472 kbps
HDB3	High density bipolar with a maximum of 3 consecutive zeros
HDLC	High-level Data Link Control
HDTV	High density television
HEC	header error check
HF	high frequency
HRC	hypothetical reference circuit
HRX	hypothetical reference connection
Hz	hertz
IAP	international access prefix
ICD	international code designator
IDI	initial domain identifier
IDP	initial domain part
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IP	internet protocol
IPMS	interpersonal message service
IRAC	Interdepartment Radio Advisory Committee
IS	intermediate system
ISB	independent sideband
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	International Standardized Profile
ITU	International Telecommunications Union
IWG	interim working group
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability and Engineering Organization
JTC3A	Joint Tactical Command, Control and Communications Agency
JTIDS	Joint Tactical Information Distribution System
K	kilo
kbps	kilobit(s) per second
kHz	kilohertz
km	kilometer(s)
LAN	local area network
LAP	link access procedure
LAPB	LAP balanced
LAPD	LAP on the D channel

LF	low frequency
LLC	logical link control
LPC	linear predictive coding
LOS	line-of-sight
LSDU	link service data unit
MAC	media access control
MAN	metropolitan area network
MAU	medium attachment unit
Mbps	megabit(s) per second
MCEB	Military Communications-Electronics Board
MF	medium frequency
MHS	message-handling service
MHz	megahertz
MIB	management information base
MILDEP	military department
MIL-HDBK	military handbook
MIL-STD	military standard
MLPP	multi-level precedence and preemption
MMHS	Military Message Handling System
MMS	Military Messaging System
MSP	maintenance service provider
MTBF	mean time between failures
MTBPM	mean time between preventive maintenance
MTP	message transfer part
MTTR	mean time to repair

mW	milliwatt(s)
n	integer
NACSEM	National COMSEC Engineering Memorandum
NACSIM	National COMSEC Information Memorandum
NATO	North Atlantic Treaty Organization
NCC	network control center
NDI	nondevelopmental item
NE	network element
NI	nationality identifier
NIST	National Institute of Standards and Technology
NNI	network-node-interface
NRI	net radio interface
NSA	National Security Agency
NSAP	network service access point
NT	network terminal
NTIS	National Technical Information Service
OC	optical carrier level
ODA	Office Document Architecture
ODIF	Office Document Interchange Format
OS	operating system
OSI	Open Systems Interconnection
PBX	private branch exchange
PCM	pulse-code modulation
PDN	public data network
PDU	protocol data unit

PLP	packet layer protocol
PLRS	Position Location Reporting System
PLS	physical layer signaling
PMA	physical medium attachment
PSAP	presentation service access point
PSN	packet-switched network
PSTN	public switched telephone network
PT	payload type
PTS	personal telecommunications service
QOS	quality-of-service
R	radio
RES	reserved
rf	radio frequency
RFC	request for comment
RM	reference model
ROSE	remote operations service element
SATCOM	satellite communications
SCCP	signaling connection control part
SDH	synchronous digital hierarchy
SDNS	secure data network system
SDU	service data unit
SG	study group
SHF	super high frequency
SINCGARS	Single-Channel Ground and Airborne Radio System
SMAF	Specific Management Application Function

SMDS	switched multi-megabit data service
SNE	subscriber network element
SOH	synchronous optical hierarchy
SONET	synchronous optical network
SP	security protocol
SSAP	session service access point
SSB	single sideband
SS7	Signaling System Number 7
STANAG	standardization agreement
STE-STE	signaling terminal-to-signaling terminal
STM	synchronous transport module
STS	synchronous transport signal
TADIL	tactical digital information link
TBD	to be determined
TC	transport connect
TCAP	transaction capabilities application part
TCP	transmission control protocol
TDMA	time-division multiple access
TE	terminal equipment
TELNET	telecommunications network
TEMPEST	compromising emanations
TIA	Telecommunications Industry Association
TMN	Telecommunications Management Network
TP	transport protocol
TP0	Transport Protocol class 0

TP1	Transport Protocol class 1
TP2	Transport Protocol class 2
TP3	Transport Protocol class 3
TP4	Transport Protocol class 4
TPDU	transport protocol data unit
TR	technical report
TRANSEC	transmission security
TRI-TAC	Tri-Service Tactical Communications
TSAP	transport service access point
TTY	teletypewriter
UHF	ultra high frequency
ULF	ultra low frequency
UMTS	universal mobile telecommunications system
UNI	user-to-network interface
UPT	universal personal telecommunications
USAT	Ultra Small Aperture Terminal
UTC	coordinated universal time
VBR	variable bit rate
VCC	virtual channel connection
VCI	virtual channel indicator
VPC	virtual path connection
VPI	virtual path indicator
VF	voice frequency
VHF	very high frequency
VLF	very low frequency

VOX	voice-operated transmit
VT	virtual terminal
WARC	World Administrative Radio Conference
WG	working group
2B1Q	Two binary, one quaternary

(This page intentionally left blank.)

4. GENERAL REQUIREMENTS

4.1 System requirements. The following general system requirements affect the design of the terminal equipment (information sources and sinks), local-network elements, and wide-network elements as described in the DIS framework (see 1.6) and figure 4.1. New strategic switching systems that provide ISDN features shall comply with MIL-STD-188-194.

4.1.1 End-to-end digital service. All signals entering the local- and wide-network elements shall be digital and shall remain in a digital form until the signals exit the local network at reference point A. Analog-to-digital and digital-to-analog conversion, when required, shall be accomplished in the terminal equipment or in a terminal adapter. The network elements shall preserve bit-count integrity through the aggregate of network elements for data service.

4.1.2 Signaling. This DIS shall provide for intranetwork, user-to-network, and user-to-user signaling as described in 4.1.2.1 to 4.1.2.3.

4.1.2.1 Intranetwork. Common-channel signaling shall be employed in local networks and wide networks. For tactical information transfer systems, interswitch common-channel-signaling messages shall comply with TT-A3-9016-0056. For base information transfer systems and wide networks, interswitch common-channel-signaling messages shall comply with ANSI Standards for Signaling System Number 7 (SS7) T1.111, ANSI T1.112, and ANSI T1.113, as modified to provide the military enhancements described in mandatory Appendix D.

4.1.2.2 User-to-network signaling

a. Common-channel signaling shall be employed at the user-to-network interface in base information transfer systems. User-to-network signaling messages shall comply with the following ANSI standards as described in mandatory Appendix D:

(1) ANSI T1.602

(2) ANSI T1.607

(3) ANSI T1.608

(4) ANSI T1.610

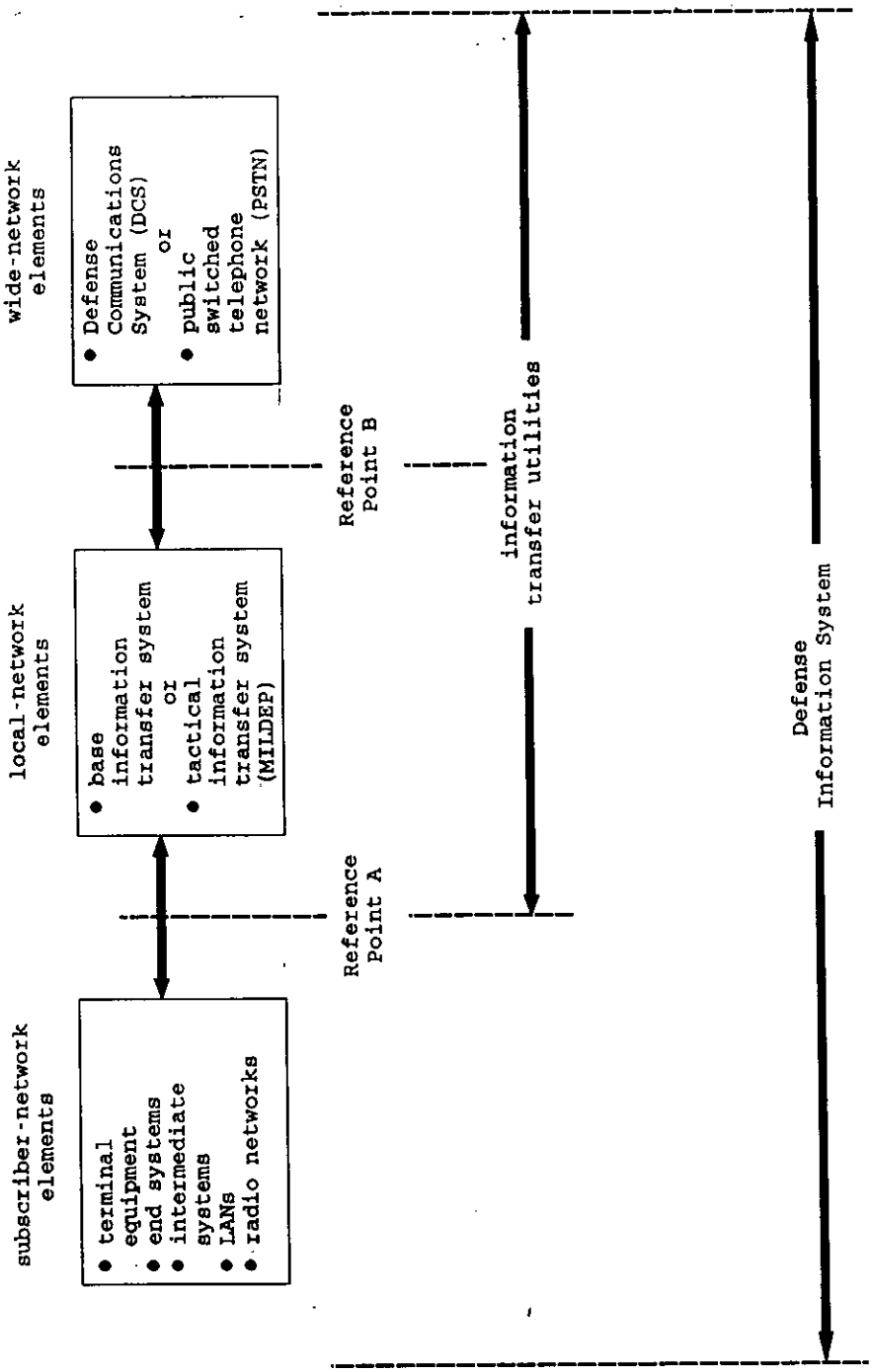


FIGURE 4.1. DIS framework.

b. In-band signaling shall be employed at the user-to-network interface in tactical information transfer systems. User-to-network signaling messages shall comply with TT-A3-9012-0046.

4.1.2.3 User-to-user signaling. User-to-user signaling is the control information exchanged between users' terminal equipment. This information shall be transmitted in the signaling and the information bearer channels, but shall be transparent to network elements.

4.1.3 Internetwork and gateway functions. Reference point B shall include a wide-network gateway function to achieve interoperability between switched subscribers in tactical information transfer systems and base information transfer systems. The gateway function requires standards for layers 1 to 3 for tactical systems using 16-kbps channels and strategic systems using 32- and 64-kbps channels. The gateway function shall include the capability to convert voice algorithms used in tactical information transfer systems to 32-kbps adaptive differential pulse-code modulation (ADPCM) and 64-kbps pulse-code modulation (PCM) used in base information transfer systems. The gateway function shall have the capability to accommodate additional conversion algorithms if needed in the future. The gateway function shall also include the signaling-message converter necessary to allow tactical switched systems to internetwork with strategic-switched systems. The signaling messages shall be examined by the gateway function. If it is determined that a secure voice or data call is being established, the gateway function shall use rate adaptation at the interface in accordance with 4.1.7. Gateways are a necessary solution for the interoperability of near-term tactical and strategic networks. Since end-to-end encryption is a long-term objective of this standard, the use of gateways that require re-encryption should be minimized.

4.1.4 Subscriber services. Local-network elements shall provide telecommunications subscriber services for circuit-switched voice, circuit-switched data, and packet-switched data. Services supported include voice telephony, data transmission, facsimile, record traffic, and video.

4.1.5 Voice digitization. The following voice digitization algorithms shall be used:

a. Base information transfer systems shall use 64-kbps PCM (mu-law companding) as defined in MIL-STD-188-113, the section titled *Eight-bit pulse-code modulation (PCM)*.

b. Tactical information transfer systems shall have the capability to interface either directly or via a switch, using 16-kbps continuously variable slope delta (CVSD) modulation as defined in MIL-STD-188-113, the section titled *CVSD modulation*. Tactical systems employing 32-kbps digital loops shall double sample 16-kbps CVSD signals to achieve joint interoperability.

c. Narrowband voice subscribers connected to the local network through high frequency (HF) radio, special electronic counter-countermeasures (ECCM) radios, or other narrow-bandwidth facilities shall use 2.4-kbps linear predictive coding (LPC) as defined in MIL-STD-188-113, the section titled *LPC*; or 4.8-kbps code excited linear prediction (CELP) as defined in FED-STD-1016.

d. Digital voice encoders employing ADPCM shall conform to CCITT G.721.

4.1.6 End-to-end secure voice service. The aggregate of tactical-network elements, wide-network elements, and base-level network elements shall provide the capability for end-to-end secure voice calls between subscribers at a base and subscribers in a tactical system. Secure voice calls shall be treated as a data service. Bit count integrity shall be preserved to maintain cryptographic synchronization between the calling and called secure voice terminals. End-to-end secure voice calls between base-level and tactical subscribers may occur at any standard bit rate up to and including 16 kbps. The network elements shall allow the control for switching from data-to-voice and voice-to-data to occur at the terminals.

4.1.7 Rate adaptation

a. Information sources, linked to a strategic-local network, that operate at rates of 600, 1200, 2400, 4800, 9600, 16000, 19200, or 32000 bps, shall be rate-adapted to a 64-kbps channel. The rate adaptation of bit rates up to 32 kbps shall use the multi-stage approach defined in CCITT Recommendation V.110, the section titled *Adaptation of V-series data signaling rates to the intermediate rates*, in which user rates of 4.8 kbps and below are mapped to 8 kbps, 9.6 kbps is mapped to 16 kbps, and 19.2 kbps is mapped to 32 kbps. Rate adaptation of 8-, 16-, and 32-kbps signals shall be rate-adapted in accordance with the following procedure as documented in CCITT Recommendation I.460, the section titled *Rate adaptation of 8-, 16-, and 32-kbps streams*:

(1) The 8-kbps stream occupies bit position 1.

(2) The 16-kbps stream occupies bit positions 1 and 2.

(3) The 32-kbps stream occupies bit positions 1, 2, 3, and 4.

(4) All unused bit positions shall be set to "1."

(5) The order of bit transmission of the subrate stream shall be identical before and after rate adaptation.

b. Information sources, linked to a tactical network, that operate at rates of 75, 600, 1200, 2400, 4800, or 9600 bps shall be rate-adapted to a 16-kbps channel as described in MIL-STD-188-216, the section titled Multisampling.

4.1.8 Dedicated circuits. The DIS shall be capable of providing dedicated circuits at 64-kbps, 384-kbps, and 1.544-Mbps rates. These circuits shall be provided by commercially leased lines or by multiplexing existing channels into dedicated through groups. The layer 1 interface shall conform to applicable portions of 5.1.1.1 for the 64-kbps rate and 5.2.1.1 for both the 384-kbps and 1.544-Mbps rates.

4.2 Information-transfer utility system parameters. The following system parameters listed in 4.2.1 through 4.2.4, shall apply to the information transfer utilities portion of the DIS framework. These parameters are summarized here because of their impact on the design of information sources, sinks, and processors that exchange information through information transfer utilities.

4.2.1 Information bearer channels. Base information transfer systems shall be capable of exchanging multiple bearer channels over a single connection at reference point A. Below are four interface options:

a. Basic rate interface. The basic rate interface provides two 64-kbps bearer (B-) channels and a 16-kbps signaling data (D-) channel. B-channels can be used for voice or data. The D-channel is used for call control and low-speed packet data. The required method for multiplexing the 2B+D channels into a form suitable for transmission over a single twisted wire pair is provided in 5.1.1.1.

b. Primary rate interface. The primary rate interface provides a combination of 23 B- (or 30 B-) channels and one 64-kbps D-channel. The 23 B+D (or 30 B+D) channels will be used primarily to connect PBXs to central offices at reference point A. The primary rate interface will also be used at reference point B to interconnect local network elements to wide network elements. A D-channel may not be required for every primary rate

interface, in this case, all 24 or 31 channels shall be available for use as B-channels. Multiplexing requirements applicable to primary rate signals are provided in 5.2, 5.3, figure 5.1, and figure 5.4.

c. High-rate channels. It shall be possible to treat multiple 64-kbps channels as a single high-rate (H) channel. Six B-channels can be treated as a single 384-kbps (H0) channel. Twenty-three B-channels can be treated as a single 1472 kbps (H10) channel. H0 channels can be used in combination with B-channels on the same primary rate interface. Rules for time-slot assignments for high-rate signals are provided in 5.2.1.1j and 5.3.1.1j.

d. Broadband services interface. A discussion of broadband services is provided in 5.6.

4.2.2 Timing and synchronization

4.2.2.1 Reference point A. In general, information source bit timing shall be slaved to the local network, as described in the discussion of master-slave operation in MIL-STD-188-115. Terminal equipment connected to network elements in the base information transfer system shall comply with ANSI T1.601, the section titled *Baud Rate, Timing, and Synchronization*. Terminal equipment connected to network elements in the tactical information transfer system shall comply with MIL-STD-188-115.

4.2.2.2 Reference point B. Local-network and wide-network elements that provide the reference point B interface shall provide stratum 1 clock accuracy, as defined in ANSI T1.101 and CCITT G.811, and buffering sufficient to maintain bit count integrity for a minimum of 24 hours. Frame synchronization, as required to demultiplex time-division-multiplexed signals, shall be provided by inserting a known frame pattern in predefined time slots in the transmitted data stream, as described in ANSI T1.408 and MIL-STD-188-202.

4.2.2.3 Coordinated Universal Time. Systems that require time and frequency reference information based on Coordinated Universal Time (UTC) shall comply with FED-STD-1002.

4.2.3 System performance. System performance standards for base information transfer systems and wide networks shall be based on the standards for 64-kbps channels given in 5.8. System performance standards for tactical information transfer systems shall be based on 5.8.

4.2.4 Network management. The objective of DIS network management is to conform to the Government Network Management

Profile (GNMP) (FIPS-XXX), and to support the establishment, reconfiguration, and maintenance of a stable signaling and user network environment. To achieve this objective, network management entities within each segment of the DIS shall be based on an integrated management architecture and shall employ a set of common management protocols, as defined in MIL-STD-2045-38000. DIS network management shall provide support for the following set of common management application functions:

a. Performance management

b. Fault management

c. Configuration

d. Security management

e. Account management

Maximum use shall be made of automated management aids to ensure effective and responsive DIS network management. Section 5.7 defines specific DIS network management requirements.

4.3 Common requirements. DIS equipment will be used in a variety of applications and environments. Acquisition specifications should contain design requirements tailored to the expected application and environment; however, the nature of military operations also dictates some degree of flexibility. Extreme care must be taken to ensure design requirements selected from applicable DoD documents are tailored to provide the necessary flexibility. The use of commercial off-the-shelf equipment is encouraged when the acquisition authority determines that some or all of the common requirements listed in 4.3.1 to 4.3.13 are not applicable.

4.3.1 Information security. The design of information systems shall allow the incorporation of communications security (COMSEC) and computer security (COMPUSEC) to protect information against unauthorized disclosure, transfer, modification, or destruction.

4.3.1.1 Communications security. Provisions for COMSEC shall include cryptosecurity, transmission security (TRANSEC), emission security (EMSEC), and physical security.

4.3.1.1.1 Cryptosecurity. Information systems shall provide internal or external cryptoequipment. Digital interfaces to external cryptoequipment shall be in accordance with MIL-STD-188-114.

4.3.1.1.2 Transmission security. HF radio anti-jam systems shall comply with the TRANSEC algorithm provisions in MIL-STD-188-148. Very high frequency (VHF) radios shall comply with JTC3A Specification 9001. Ultra high frequency (UHF) radios shall comply with STANAG 4372. Standards for satellite communications (SATCOM) anti-jam systems shall be based on existing UHF, super high frequency (SHF), and extremely high frequency (EHF) common-user DoD satellite systems.

4.3.1.1.3 Emission security. Compromising emanations shall be controlled within applicable TEMPEST criteria in the current edition of NSTISSAM TEMPEST/1-91.

NOTE: NACSEM 5201 provides design guidance and MIL-HDBK-232 provides installation guidelines for compromising emanations.

4.3.1.1.4 Physical security. Systems shall have appropriate tamper-resistant design features and tamper-detection mechanisms.

4.3.1.2 Computer security. Computer systems shall comply with applicable provisions of DoD 5200.28-STD.

4.3.2 Electromagnetic compatibility. Systems and associated subsystems shall be designed to achieve intrasystem and intersystem electromagnetic compatibility (EMC). There shall be no emissions by any item of the subsystem or system beyond the tolerances established in MIL-STD-461. Techniques used to measure and determine EMC characteristics shall comply with the applicable requirements of MIL-STD-462. Equipment and subsystems should be designed in accordance with applicable EMC guidance in MIL-HDBK-235, MIL-HDBK-237, MIL-HDBK-241, and MIL-HDBK-253. The EMC program must address both emissions and susceptibilities, not just emissions. Future specific electromagnetic emission requirements will require tailoring of MIL-STD-461 requirements to ensure compatibility.

NOTE: MIL-HDBK-237 provides guidance for implementing an EMC program, and MIL-HDBK-241 provides guidance for EMC enhancement (electromagnetic interference reduction) of equipment power supplies.

4.3.3 Electronic warfare vulnerability and electronic counter-countermeasures capabilities. Electronic warfare (EW) vulnerability analyses should be performed on all radio subsystems, beginning with the concept formulation stage. Appropriate ECCM capabilities should be developed to protect these systems from the applicable EW threat.

4.3.3.1 Determining the electronic warfare technical threat. Appropriate EW intelligence sources should be used to provide an

EW technical threat model during the concept formulation stage of system development.

4.3.3.2 Analyzing electronic warfare vulnerability. Simulation techniques should be used to assess the effects of EW on radio links. Preliminary analysis of EW effects on candidate systems should be made to help eliminate unacceptable approaches. Subsequent analysis of emerging candidate techniques and equipment should be made at several stages of development. EW vulnerability analyses should be performed in accordance with applicable department or agency directives.

4.3.3.3 Developing electronic counter-countermeasures techniques. During each phase of system development and production, available ECCM technology should be reviewed for applicability to EW vulnerability. Where necessary, ECCM capability should be made integral to the system design. It should not be assumed that ECCM remedies can be applied at later stages of system development. EW/ECCM test requirements shall be stated in applicable system specifications. HF radio anti-jam systems shall comply with applicable provisions of MIL-STD-188-148. Very high frequency (VHF) radios shall comply with JTC3A Specification 9001. Ultra high frequency (UHF) radios shall comply with STANAG 4372. Standards for SATCOM anti-jam systems shall be based on existing UHF, SHF, and EHF common-user DoD satellite systems.

4.3.4 Human engineering design. All information systems, subsystems, and facilities shall be designed in accordance with the applicable requirements in MIL-STD-1472 and MIL-H-46855.

4.3.5 Reliability. All systems and subsystems shall be designed to meet quantitative reliability requirements. The reliability program shall be established in accordance with the applicable requirements of MIL-STD-785. Reliability acceptance tests shall be performed in accordance with the applicable requirements of MIL-STD-781.

4.3.6 Maintainability. All equipment, subsystems, and systems shall be designed to meet quantitative maintainability requirements. The maintainability program shall be established in accordance with the applicable requirements of MIL-STD-470. Maintainability acceptance tests shall be performed in accordance with the applicable requirements of MIL-STD-471.

4.3.7 Survivability. Survivability is the characteristic of equipment, subsystems, and systems to withstand or avoid such damage mechanisms as blast fragments, bullets, and explosive and incendiary devices, as well as the effects of such natural phenomena as lightning, without causing a malfunction.

Survivability can be enhanced by such measures as adding armor plating, duplicating and separating critical components, and simplifying the design to reduce the number of critical components. The survivability of all systems and subsystems should be assessed by performing vulnerability reduction studies in accordance with applicable department or agency directives, regulations, and instructions.

4.3.8 Climatic conditions. All equipment shall be designed to meet the applicable climatic conditions specified in MIL-STD-210. The climatic condition and induced stress requirements for an equipment or an assemblage shall be consistent with the degree of exposure anticipated for intended field applications.

4.3.9 Environmental test methods. All systems and subsystems shall be designed to comply with the applicable environmental test methods specified in MIL-STD-810.

4.3.10 Electrical measurement and test methods. Electrical measurement and test methods for communications systems shall comply with MIL-STD-188-190

4.3.11 Grounding, bonding, and shielding. Methods and practices for grounding, bonding, and shielding of ground-based telecommunications equipment and facilities, including buildings and structures supporting tactical and long-haul communications, shall comply with the applicable requirements of MIL-STD-188-124. MIL-HDBK-419 provides practical considerations for grounding, bonding, and shielding systems.

4.3.12 Radio regulations. The use of the frequency spectrum is regulated by international agreements embodied in radio regulations published by the General Secretariat of the International Telecommunications Union (ITU), Geneva, Switzerland, and modified periodically by a World Administrative Radio Conference (WARC). These radio regulations are further qualified at the national level through such Federal Government agencies as the Interdepartment Radio Advisory Committee (IRAC), and through such military agencies as the Joint Chiefs of Staff (JCS) and the Military Communications-Electronics Board (MCEB). Military frequency planning, including joint functional frequency allocation tables, is established as a joint action area under the MCEB. For subsystems and equipment design, the choice and performance of the equipment, as well as frequencies and emissions of any radio subsystem, shall satisfy the provisions of those radio regulations. Therefore, radio subsystem designers and users are required to have adequate familiarity with these regulations. Final approval of frequency bands, operating modes, and equipment characteristics within DoD rests with the MCEB.

4.3.13 Radio frequency spectrum characteristics. The spectral characteristics of all radio frequency (rf) transmitters, receivers, and antennas shall be measured in accordance with the applicable requirements of MIL-STD-449.

4.3.14 Conformance testing. ISO 9646 and CCITT X.290 shall be used for the conformance testing methodology and framework to ensure that conformance testing produces correct and consistent results. Acquisition agencies are cautioned that successful conformance testing of an equipment will not guarantee interoperability with all other equipment that also passed conformance testing. Conformance testing is not a substitute for interoperability testing.

4.3.15 Interoperability testing. Testing shall be performed to successfully demonstrate that systems successfully interoperate.

4.4 Subsystem design considerations

4.4.1 Terminal subsystems. Digital interfaces between terminal subsystem equipment shall comply with MIL-STD-188-114 unless other standards apply.

4.4.1.1 Tactical terminal subsystems. Tactical terminal subsystems shall comply with the applicable requirements of MIL-STD-188-260 and MIL-STD-188-216.

4.4.1.2 Long-haul digital terminal subsystems. Long-haul digital terminal subsystems shall comply with the applicable requirements of MIL-STD-188-347.

4.4.1.3 Facsimile subsystems. Tactical and long-haul facsimile subsystems shall comply with the applicable requirements of MIL-STD-188-161.

4.4.1.4 Tactical digital information links. Message formats and related information for tactical digital information links (TADIL) A, B, and C are published in Joint Pub 6-01.1. Technical characteristics for all TADILs are being published in the MIL-STD-188-203 series.

4.4.1.4.1 TADIL A subsystems. Technical characteristics of TADIL A subsystems shall comply with applicable requirements of MIL-STD-188-203-1.

4.4.1.4.2 TADIL B subsystems. Technical characteristics of TADIL B subsystems shall comply with applicable requirements of MIL-STD-188-203-2.

4.4.1.4.3 TADIL C subsystems. Technical characteristics of TADIL C subsystems shall comply with applicable requirements of MIL-STD-188-203-3.

4.4.1.4.4 TADIL J subsystems. Technical characteristics of TADIL J shall comply with STANAGs 4175 and 5516.

4.4.1.4.5 ATDL-1 subsystem. Technical characteristics of Army Tactical Data Link 1 (ATDL-1) shall comply with SR-RG-83-9-B.

4.4.2 Transmission subsystems. Transmission subsystems include fiber optic cables, metallic lines, and satellite and terrestrial radios.

4.4.2.1 Long-haul transmission subsystems. Long-haul transmission subsystems shall comply with the performance requirements given in 5.8.

4.4.2.2 Tactical transmission subsystems. Tactical transmission subsystems shall comply with the applicable requirements of MIL-STD-188-202.

4.4.2.3 Fiber optic communications subsystems. Long-haul fiber optic subsystems shall comply with the applicable requirements of MIL-STD-188-111. Tactical fiber optic subsystems shall comply with applicable requirements of MIL-STD-188-111 and JTC3A Specification 9109.

4.4.2.4 Metallic lines transmission subsystems. Wire and cable transmission subsystems shall comply with the applicable requirements of MIL-STD-188-112.

4.4.2.5 Radio relay subsystems. The term *radio relay* is generally applied to radio subsystems that operate in rf bands in which transmission, while varying continually within a restricted range, is relatively stable. The bands of the radio spectrum classified as VHF, UHF, and SHF are used by various types of radio relay subsystems.

4.4.2.5.1 Long-haul line-of-sight transmission subsystems. Long-haul LOS transmission subsystems shall comply with the applicable requirements of MIL-STD-188-313.

4.4.2.5.2 Satellite transmission subsystems. Satellite transmission subsystems shall comply with the applicable requirements of MIL-STD-188-146.

4.4.2.6 Radio subsystems operating in medium frequency and lower bands. Radio subsystems operating in the MF band shall comply with the applicable requirements of MIL-STD-188-141. Radio

subsystems operating in the LF and lower bands shall comply with the applicable requirements of MIL-STD-188-140.

4.4.2.7 High frequency radio subsystems. Radio subsystems using frequencies between 3 and 30 MHz shall comply with the applicable requirements of MIL-STD-188-141. Anti-jam transmission systems operating in the HF band shall comply with the applicable requirements of MIL-STD-188-148 and MIL-STD-188-110. HF digital voice shall use LPC at 2.4 kbps in accordance with MIL-STD-188-113. Automatic link establishment (ALE) of HF radio links shall be accomplished using the waveforms and procedures specified in Appendix A of MIL-STD-188-141 or FED-STD-1045.

4.4.2.8 Very high frequency radio subsystems. Radio subsystems using frequencies between 30 and 300 MHz shall comply with the applicable requirements of MIL-STD-188-242.

4.4.2.9 Ultra high frequency radio subsystems. Radio subsystems using frequencies between 300 and 3000 MHz shall comply with the applicable requirements of MIL-STD-188-243.

4.4.2.10 Super high frequency radio subsystems. Radio subsystems using frequencies between 3 and 30 GHz shall comply with the applicable requirements of MIL-STD-188-145.

4.4.2.11 Extremely high frequency radio subsystems. Technical characteristics of extremely high frequency (EHF) radio subsystems are under consideration.

4.4.2.12 Single-channel-radio to switched-system interfaces. See 5.1.3.

4.5 Functional interface requirements. This section defines the scenario, network elements, and applications supported by this document. This scenario and these applications determine which standards, options, and parameters are incorporated in this document.

4.5.1 Scenario. The development of new systems is driven by the availability of new technology and funding for implementation. DoD procures nondevelopmental items to meet military requirements at reduced costs. DoD will take advantage of rapid advances in commercial computer and communications technology and emerging open standards to meet future C3I requirements. Military-unique features must be introduced early in the commercial standards development cycle. Higher performance processing systems and the provision of intelligent networks are new trends that will impact DIS. These changes will accompany the introduction of ISDN for base and long-haul requirements, whereas the tactical system has evolved to an all-digital system based on Tri-Service Tactical

Communications (TRI-TAC) specifications. The tactical environment is expected to further evolve toward a hybrid TRI-TAC/commercial standard as the services upgrade their deployable systems. In the future, broadband ISDN (B-ISDN) services will be introduced to the DIS to provide switched broadband video service, multi-megabit data service, flexible multi-party conference service, and bidirectional distribution service with subscriber control. Tactical assets may have limited capability for broadband services due to spectrum limitations. In the long term, the tactical architecture shall depend on the asynchronous transfer mode, thus moving away from channel limitations caused by the present synchronous transfer mode. Also, the radio-based architecture shall move to a channel rate of 4.8-kbps to conform to the standardization being pursued by the commercial world.

4.5.2 Network elements. This document identifies the standards necessary for information exchange between subscribers of common-user switched systems. Subscribers may be connected to the same network, or they may be connected to different but interconnected networks. Each network may consist of different network elements, as illustrated in figure 4.2 and described in 4.5.2.1 to 4.5.2.4.

4.5.2.1 Subscriber network elements. Two types of subscriber network elements exist: subscriber terminal equipment and subscriber networks. Subscriber terminal equipment, which can be manned or unmanned, includes telephones, teleprinters, facsimile machines, data terminals (such as host computers, work stations, personal computers, digital message entry devices, sensors, and weapons systems), video terminals, or other information sources and sinks. Subscriber networks, through a common media, provide connectivity between a limited set of subscribers. These networks can provide selective addressing, but they do not switch or route traffic. Subscriber networks may be local area networks (LAN), as defined in ISO 8802-3, 8802-4, and 8802-5; or radio networks such as combat radio networks. This document does not apply to closed networks that do not interface with remote users via common-user systems. Subscriber terminal equipment and subscriber networks are illustrated in figure 4.2. Terminal equipment (TE) is used to designate terminals in which information to be exchanged is voice or non-voice. End system (ES) and intermediate system (IS) are used to designate data communications elements that comply with ISO and CCITT data communications standards. ES represents a host for information transfer applications. IS represents a relay or bridge used to transfer data between one subnetwork and another. The letter "R" represents a radio terminal in a network of similar radios, for example, the Position Location Reporting System (PLRS), the Joint Tactical Information Distribution System (JTIDS), or combat net radio (CNR).

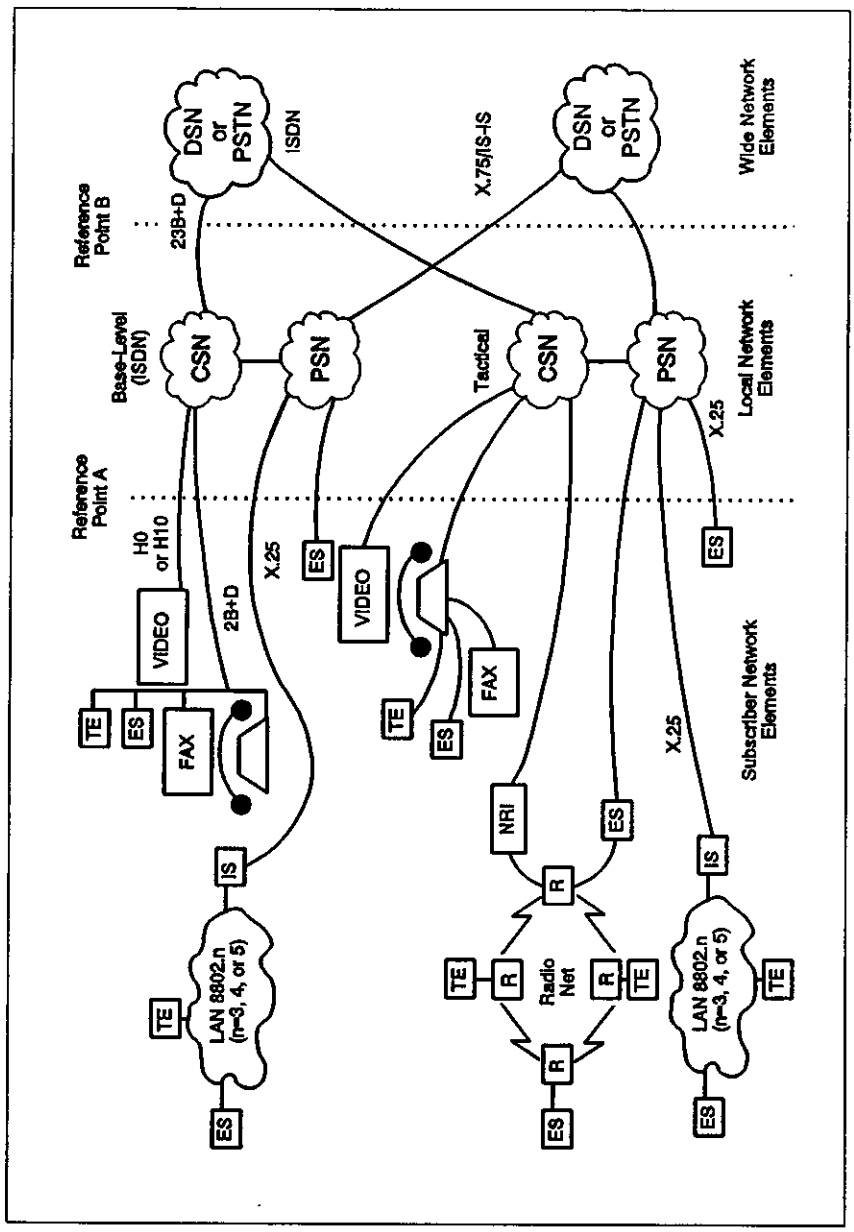


Figure 4.2. Typical DIS network elements (ATM not Shown).

4.5.2.2 Local-network elements. Local-network elements are the circuit switches, packet switches, and transmission equipment that constitute the common-user systems provided by the military services. They provide switched service for base-level and tactical subscribers. Local network elements are illustrated in figure 4.2. The base-level circuit-switched networks (CSN) and packet-switched networks (PSN) are based on commercial standards for ISDN. Tactical CSNs and PSNs currently interface with TRI-TAC equipment. Future upgrades to tactical systems should be based on commercial standards. Compatible terminal equipment shall be capable of exchanging information via switched networks comprised of local-network elements. The interface between subscriber-network elements and local-network elements shall comply with the standards described in 5.1. Tactical CSNs and PSNs within a theater of operations may be interconnected without going through the DSN or DDN.

4.5.2.3 Wide-network elements. Wide-network elements are the circuit switches, packet switches, and transmission equipment provided by the DCS and public switched networks. Wide-network elements are used to transfer information between remote local-network elements. The interface between local-network elements and wide-network elements shall comply with the standards described in 5.2.

4.5.2.4 NATO-network elements. North Atlantic Treaty Organization (NATO) network elements are the circuit switches, packet switches, and transmission equipment provided by NATO nations or those portions of the DCS that adhere to the technical standards of the host nation. Subscribers to U.S. common-user systems shall be capable of exchanging information with subscribers of other nations through reference point B (NATO), as illustrated in figure 4.3. The interface between U.S. network elements and NATO network elements shall comply with the standardization agreements (STANAG) and CCITT standards described in 5.3.

4.5.3 Military enhancements to commercial data communications protocols and standards. This standard adopts commercial standards for military use. These adopted commercial standards are acceptable; however, in some cases they require enhancement to satisfy the complete military requirement for a specific function or capability. Eight military features have been identified in the data communications protocol area that are not adequately addressed by existing commercial data communications standards. These features are described in 4.5.3.1 through 4.5.3.8. Acquisition authorities should review the standards to ensure that these features are satisfactorily addressed and supplement their procurement documentation as necessary.

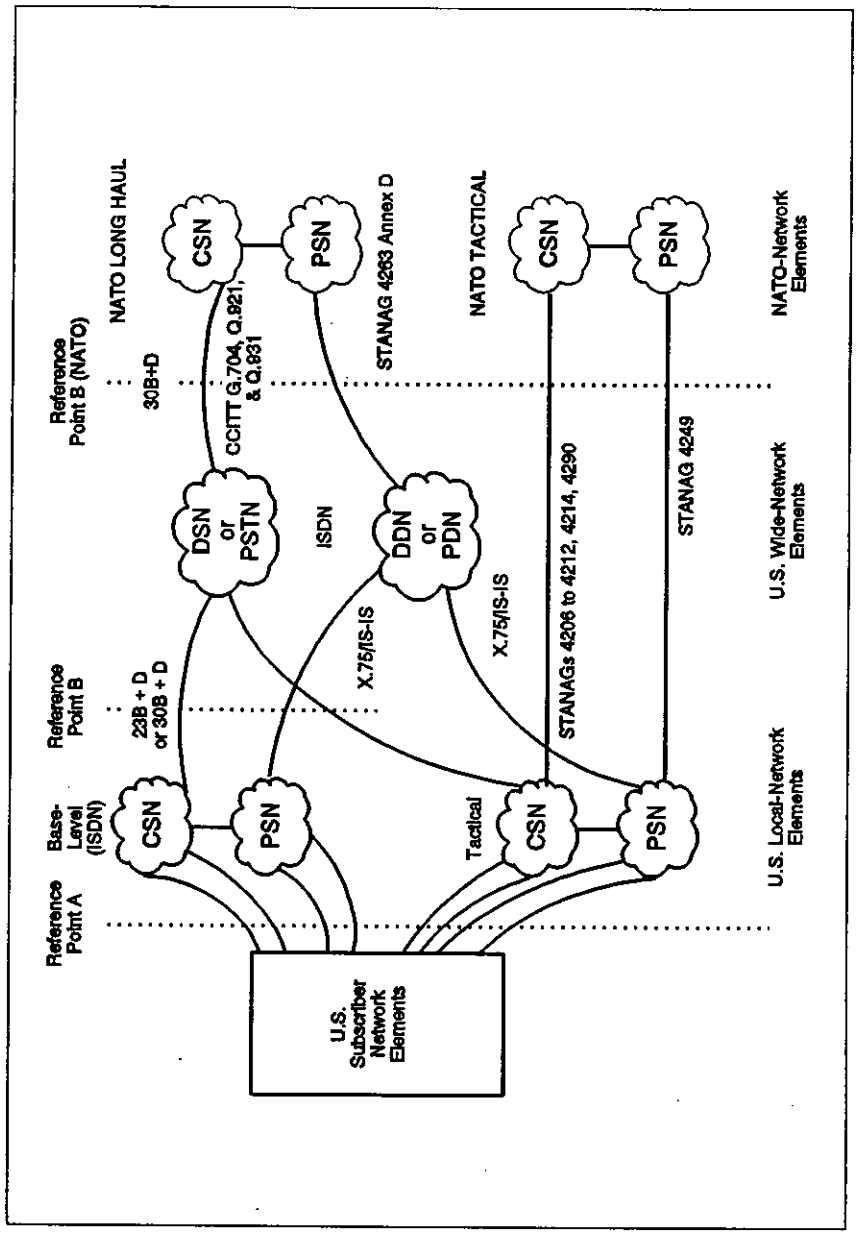


FIGURE 4.3. Typical DIS interface with NATO network elements.

4.5.3.1 Multihomed and mobile host systems. Multihoming is a mechanism for attaching an end system to two or more network access points so that a system setting up a call to the end system is not aware of the extra connectivity. In addition to enhancing survivability, this mechanism may be extended to "mobile hosts" such as aircraft, ships, and land vehicles during the move from one node to another.

4.5.3.2 Multi-endpoint connections (multi-addressing). To transmit data to a number of recipients (a common occurrence in signal handling), a user must establish a connection for each recipient and send a separate copy of the data across each connection. More efficient use is made of the communications resources (in particular, improved performance in terms of minimizing delay and conservation of bandwidth) if the sender has to transmit only one copy of the data. The network then takes care of routing, controlling, and distributing the data.

4.5.3.3 Internetworking. Mechanisms are required to facilitate the interconnection of various systems at the boundary point between subnetworks.

4.5.3.4 Network and system management. Management functions are required that may be more sophisticated than those considered satisfactory for civilian networks: management of broken networks in which layers of protocols are inoperable; fast responses to changes in network topology essential to maintain important connections; and counterattack management, to recognize and counter the effects of intelligent attack on and physical damage to the network.

4.5.3.5 Security. Protection measures are required (a) to prevent unauthorized access to the system and ensure the confidentiality of the information it carries, and (b) to preserve the integrity of the data and mitigate against denial of service.

4.5.3.6 Quality-of-service. The range of quality-of-service parameters required for military systems exceeds those currently permitted within civilian networks. The particular aim, to maximize network survivability, is to maintain an adequate quality-of-service to the users (or at least to users operating above a given priority level) in the face of a severely damaged or partitioned network. There is a military requirement for an ultimate delivery capability, whereby important communications are sustained, even at very low data rates.

4.5.3.7 Precedence and preemption. To minimize congestion, particularly in a damaged network where resources are at a premium, it is desirable to be able to allocate resources on the basis of priority levels assigned to the messages being routed through the congested area. A facility is therefore required to associate a priority level with a message. This requirement is needed for both connection-oriented and connectionless communications.

4.5.3.8 Real-time and tactical communications. Certain applications (often tactical in nature) require communications with specified time outs, which can be in the range of milliseconds to seconds. Accurate sequencing is essential. Real time may also include high demands on sequencing accuracy.

4.5.4 Functional profiles. To promote open digital systems, the commercial world has developed the 7-layer OSI Reference Model (RM), ISO 7498, with corresponding ISO and CCITT standards. ANSI standards address the differences between the North American and European implementations. NIST developed the Government Open Systems Interconnection Profile (GOSIP), FIPS 146, which specifies a subset of existing standards approved for Government use. (FIPS-146-1 was used to develop this document.) To define the end-system interface for data communications, the 7-layer OSI RM is divided into two profiles. The top 3 layers are designated the application profile, and the remaining lower 4 layers are designated the transport profile. The application and transport profiles are described in 5.4. The relay profile represents the interface between two different systems and consists of the lower 3 layers with a relay function that maps one system's network layer into the other system's network layer. Relay profiles occur at Reference points A and B and are described in 5.1 and 5.2, respectively.

(This page intentionally left blank.)

5. DETAILED REQUIREMENTS

5.1 Standards for reference point A. This section defines the standards applicable at the interface between the subscriber terminal equipment (or the subscriber's network equipment) and the local-network element (reference point A).

5.1.1 ISDN-terminal to base information transfer system. The terminal equipment interfacing with the base information transfer system shall comply with the existing ANSI standards and CCITT recommendations cited in 5.1.1.1 to 5.1.1.3.3, and shall conform to FIPS 146 for ISDN basic rate access at the user-to-network interface. This interface is applicable to both circuit-switched and packet-switched service.

5.1.1.1 Layer 1 (the physical layer). Layer 1 provides the mechanical, electrical, functional, and procedural characteristics to activate, maintain, and deactivate a physical circuit. Layer 1 allows for the transparent transmission of bits between the terminal equipment and local-network elements. The interface between the terminal equipment and local-network elements shall comply with ANSI T1.601. This interface shall support up to two full-duplex, 64-kbps information bearer channels; one full-duplex, 16-kbps signaling channel; and one full-duplex, 16-kbps overhead channel over a single twisted pair of telephone wires.

5.1.1.1.1 Physical characteristics. The wiring polarity and connector shall comply with ANSI T1.601, the section titled *Physical Characteristics*.

5.1.1.1.2 Transmission method. The line code used on the twisted pair of telephone wires shall be 2B1Q (2 binary, 1 quaternary) as defined in ANSI T1.601, the section titled *Transmission Method*.

5.1.1.1.3 Functional characteristics. The modulation rate of the 2B1Q signal shall be 80 kilobaud. The timing signal for the subscriber's terminal equipment shall be slaved to the signal received from the local-network element. The two 64-kbps bearer channels, the 16-kbps signaling channel, and the 16-kbps overhead channel shall be multiplexed in accordance with the frame structure defined in ANSI T1.601, the section titled *Functional Characteristics*.

5.1.1.1.4 Electrical characteristics. The subscriber's terminal equipment shall comply with the impedance and return loss, longitudinal output voltage, longitudinal balance, jitter, and dc

characteristics defined in ANSI T1.601, the section titled *Electrical Characteristics*.

5.1.1.2 Layer 2 (the data link layer). Layer 2 defines the procedures required to establish, maintain, and disconnect the data link between the subscriber's terminal equipment and the network.

5.1.1.2.1 Signaling channel (the D-channel). The link access procedure on the D-channel shall comply with ANSI T1.602. T1.602 contains the complete text of CCITT Recommendations Q.920 and Q.921, which specify the frame structure, the procedure elements, the field formats, and the link access procedures (LAP) for the D-channel (LAPD). Out-of-band signaling procedures (D-channel) shall be used to negotiate a packet-switched or circuit-switched connection for each information bearer channel.

5.1.1.2.2 Signaling in the bearer channel. Packet-switched calls shall be connected to the local packet handler. Remaining signaling information, including the called user address, shall be provided in the bearer channel and shall comply with the link access procedures balanced (LAPB), as defined in sections 2.2, 2.3, and 2.4 of CCITT Recommendation X.25 for basic (modulo 8) operation. Connections for circuit-switched calls shall be completed based on D-channel signaling only. At the user-to-network interface, layer 2 does not apply to information bearer channels, for circuit-switched calls.

5.1.1.3 Layer 3 (the network layer). Layer 3 protocols provide the information required to route calls through the local- and wide-network elements to the destination-terminal equipment. Three types of signaling messages shall be used to control circuit-switched and packet-switched connections: call establishment, call clearing, and miscellaneous messages. A list of the messages in each category is provided in tables I and II.

5.1.1.3.1 Circuit-switched connections. The definition, message format, and information element coding for messages used to control circuit-switched connections shall be as defined in ANSI T1.607 and 5.1.1.3.2. ANSI T1.607 is aligned with CCITT Recommendation Q.931. It specifies the messages and procedures used for control of circuit-switched connections at user-to-network interfaces. The messages are exchanged over the D-channel and are applicable to both basic-rate and primary-rate interfaces.

TABLE I. Messages for circuit-switched connection control.

CALL ESTABLISHMENT	CALL CLEARING	MISCELLANEOUS
Alerting	Disconnect	Information
Call Proceeding	Release	Notify
Connect	Release Complete	Status
Connect Acknowledge	Restart	Status Inquiry
Progress	Restart Acknowledge	
Set-up		
Set-up Acknowledge		

TABLE II. Messages for packet-switched connection control.

CALL ESTABLISHMENT	CALL CLEARING	MISCELLANEOUS
Alerting	Disconnect	Status
Call Proceeding	Release	Status Inquiry
Connect	Release Complete	
Connect Acknowledge	Restart	
Progress	Restart Acknowledge	
Set-up		

5.1.1.3.2 DSN features. The circuit-switched call control procedures described in ANSI T1.607 shall be used in the control of supplementary procedures as specified in ANSI T1.610, except where modified to provide for DSN features. The following DSN features shall be implemented in accordance with mandatory Appendix D:

a. Multi-level precedence and preemption (MLPP)

b. Off-hook (or hot-line) service

c. Preset conference calling

d. Community-of-interest service

5.1.1.3.3 Packet-switched connections. The definition, message format, and information element coding for messages used to control packet-switched connections are defined in ANSI T1.608. ANSI T1.608 specifies the messages and procedures used for control of packet-switched connections at user-to-network interfaces. The procedures in T1.608 shall be used for the following two cases:

Case A: Circuit-switched access to packet-switched public data network. Layer 3 signaling between the subscriber's terminal equipment and the public data network (PDN) shall comply with the packet layer protocol defined in section 3 of CCITT Recommendation X.25. Only the B-channel is used after the circuit-switched connection to the PDN is completed. Signaling for the circuit-switched portion of the call shall be accomplished using the D-channel.

Case B: Packet-switched access to an ISDN virtual circuit service (B- and D-channels). Layer 3 signaling between the subscriber and the ISDN packet handler shall comply with the packet layer protocol defined in section 3 of CCITT Recommendation X.25. The connection between the subscriber's terminal equipment and the packet handler may be a full period connection or may be obtained using D-channel signaling as defined in ANSI T1.608. In this case, the information bearer channel may be either a B- or D-channel.

A list of the ANSI T1.608 messages applicable to D-channel signaling is provided in table I for Case A and table II for Case B.

5.1.2 Terminal-equipment to tactical-network interface. The terminal equipment interface for tactical subscribers shall comply with the existing MIL-STD-188 series standards and CCITT Recommendations cited in 5.1.2.1 and 5.1.2.2.

5.1.2.1 Tactical circuit-switched connections. The terminal equipment interface for tactical circuit-switched subscribers shall comply with 5.1.2.1.1 to 5.1.2.1.3.

5.1.2.1.1 Layer 1 (the physical layer). Loops between tactical terminal equipment and tactical local-network elements shall operate on a full-duplex, 4-wire basis with a transmit pair and a receive pair. Common battery may be provided between the pairs by a local-network element. The loop shall operate at a 16-kbps information rate in each direction, using conditioned diphase, as

defined in MIL-STD-188-200. The signal amplitude shall be 3 volts, plus or minus 10 percent, with a source impedance of 125 ohms, resistive.

5.1.2.1.2 Layer 2 (the data link layer). Tactical loop signaling shall be in-band, using 8-bit cyclically permutable codewords. The codewords shall be repeated continuously until acknowledged or timed-out in accordance with TT-A3-9012-0046, the sections titled *Signaling codewords and Signaling timeout*. The idle state, for the signaling channel, shall consist of alternating ones and zeros.

5.1.2.1.3 Layer 3 (the network layer). Tactical loop signaling shall be in accordance with TT-A3-9012-0046, the section titled *Signaling and cryptophases*. Certain codewords shall be used to represent more than one signaling statement. The ambiguity shall be resolved by considering the context of the signaling sequence involving use of the codewords.

5.1.2.2 Tactical packet-switched connections. As illustrated in figure 4.2, a host computer or ES may be connected to a tactical packet switch in three ways:

a. By direct cable connection to a packet switch.

b. By connection to a LAN through an IS to a packet switch (the IS may be located with the LAN or with the packet switch).

c. By connection to a telephone through a circuit switch to a packet switch (in this case, the subscriber must first call up the local-packet switch).

5.1.2.2.1 Layer 1. The interface, at reference point A, shall comply with MIL-STD-188-114 for 5.1.2.2 a and b. It shall comply with 5.1.2.1.1 for 5.1.2.2c.

5.1.2.2.2 Layer 2. The protocol used to access the packet switch shall comply with LAPB basic (modulo 8) operation, as defined in sections 2.2, 2.3, and 2.4 of CCITT Recommendation X.25.

5.1.2.2.3 Layer 3. Network signaling to the packet switch shall comply with the packet layer protocols as defined in section 3 of CCITT Recommendation X.25.

5.1.3 Net-radio-terminal to tactical-network interface. Tactical network elements shall provide circuit-switched and packet-switched service to and from radio networks. Interoperability between the radio network and local-network

elements shall be achieved by providing a net radio interface (NRI) for circuit-switched voice and data calls, or an IS function for packet-switched data communications.

5.1.3.1 Circuit-switched connections. Tactical circuit-switched network interfaces to net radio terminals shall use the same loop signaling protocols as described in 5.1.2.1, with the addition of a means to control the NRI gateway's push-to-talk function. These means may be manual (whereby a local operator monitors both sides of the interface), or automatic. Automatic operation may be achieved by voice-operated transmit (VOX), digitized push-to-talk control tone bursts (1231 Hz, transmit on; 1455 Hz, transmit off), dual-tone multifrequency (DTMF) digits (1 transmit on, 3 transmit off), or digital start-of-transmission/end-of-transmission codewords.

5.1.3.2 Packet-switched data. Tactical packet-switched network interfaces to and from net radio terminals shall use the same protocols described in 5.1.2.2. The IS function may be an integral part of the radio terminal located at the network gateway.

5.2 Standards for reference point B. This section defines the standards applicable at the interface between local-network elements and wide-network elements.

5.2.1 ISDN base-level interface to reference point B. Base information transfer systems shall comply with 5.2.1.1 to 5.2.1.3 at reference point B.

5.2.1.1 Layer 1. The signal at the wide-network interface shall comply with the following parameters as specified in ANSI T1.408:

a.	Line code	Bipolar with 8-zero substitution (B8ZS) and 50% duty cycle.
b.	B8ZS	Eight consecutive zeros shall be replaced with 000+-0-+ if the preceding pulse was positive and with 000-+0+- if the preceding pulse was negative.
c.	Bit rate	1.544 Mbps.

d.	Number of channels	24 (Normally 23 channels are used as information-bearer channels and 1 channel is reserved for common-channel signaling.)
e.	Frame format	193-bit frame (see figure 5.1).
f.	Frame repetition rate	8000 frames per second.
g.	F-bit signal bit rate and allocation	2000 bps of the 8000-bps F-bit signal shall be used for the frame alignment signal (FAS). To convey fault status and maintenance information, 4000 bps shall be available for use as a data link (data orderwire). Using the CRC-6 cyclic redundancy check as defined in ANSI T1.408, 2000 bps shall be available for performance monitoring.
h.	F-bit signal format	See table III.
i.	High rate signals	H_0=384 kbps; H_{10}=1472 kbps; H_{11}=1536 kbps. (H_{10} and H_{11} are optional services.)
j.	Time-slot assignment	Time slot 24 shall be used to transfer common-channel signaling information (D-channel), when it is present. A channel shall occupy an integer number of time slots and the same time-slot positions in every frame. A B-channel may be assigned any time slot in the frame; an H_0-channel shall be assigned any six slots in the frame, in numerical order (not necessarily consecutive); and an H_{10} channel shall be assigned time slots 1 to 23. The assignment may vary on a call-by-call basis.

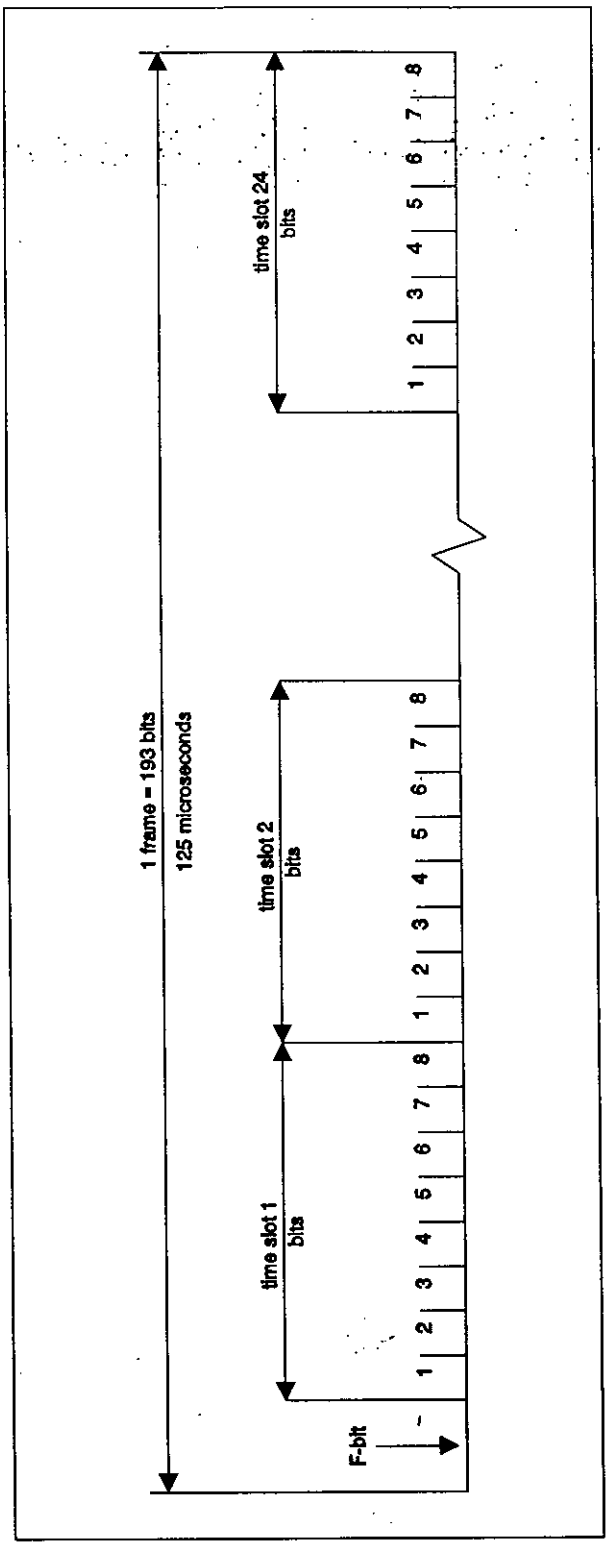


FIGURE 5.1. Frame format for a 1.544-Mbps signal.

TABLE III. F-bit signal format.

FRAME NUMBER	F-BITS			
	BIT NUMBER	FAS	DL	CRC
1	1		m	
2	194			C1
3	387		m	
4	580	0		
5	773		m	
6	966			C2
7	1159		m	
8	1352	0		
9	1545		m	
10	1738			C3
11	1931		m	
12	2124	1		
13	2317		m	
14	2510			C4
15	2703		m	
16	2896	0		
17	3089		m	
18	3282			C5
19	3475		m	
20	3668	1		
21	3861		m	
22	4054			C6
23	4247		m	
24	4440	1		

FAS = framing alignment signal
DL = 4-kbps data link
CRC = CRC-6 cyclic redundancy check
m = data bit in maintenance channel

k. Signaling data link	The signaling data link bit rate shall be 56 kbps, evolving to 64 kbps. Fifty-six kbps signals shall occupy bit positions 1, 2, 3, ..., 7 of the 64-kbps D-channel. The unused bit position shall be set to "1." The signaling data link shall be a bidirectional transmission path for common-channel signaling, comprising two "data channels" operating together in opposite directions at the same data rate. The signaling data link constitutes the lowest functional level (layer 1) in the SS7 functional hierarchy. SS7 shall be capable of operating over both terrestrial and satellite transmission links. The operational signaling data link shall be exclusively dedicated to the use of a SS7 signaling link between two signaling points in SS7.

5.2.1.2 Layer 2. The data link layer shall provide for reliable transfer of common-channel signaling information across the physical channel. This shall include error control, message sequencing, and message delimitation. Data link signaling functions and procedures shall comply with ANSI T1.111, the section titled *Signaling data link*. The data link layer shall also be responsible for initializing the link and logically disconnecting secondary stations.

5.2.1.3 Layer 3. The network layer shall comply with the following requirements:

a. Layer 3 protocols shall comply with ANSI standards T1.111 (sections 4 and 5), T1.112, T1.113, and T1.114.

b. The interworking relationship between the D-channel signal at the user-to-network interface and the ISDN-User Part, as defined in ANSI T1.113, shall comply with ANSI T1.609.

5.2.2 Tactical network interface to reference point B. Tactical local network elements are likely to change in the long-range future to reflect commercial 64-kbps ISDN architectures for fixed applications and 4.8-kbps architectures for mobile applications. Future tactical interfaces are likely to reflect these commercial standards when they are in place. The near-term standards for tactical local-network elements shall comply with 5.2.2.1 to 5.2.2.3 at reference point B.

5.2.2.1 Layer 1. Tactical common-channel signaling shall take place over an 8-kbps, full-duplex subchannel of the 16-kbps overhead channel. It shall be multiplexed in a digital transmission group, in accordance with MIL-STD-188-202.

5.2.2.2 Layer 2. Digital common-channel signaling messages shall be composed of 8-bit characters. The eighth bit of each message character shall be set to produce odd parity. These 8-bit characters shall be encoded into 16-bit blocks by employing the error detection and correction encoding described in TT-A3-9016-0056, the section titled *Trunk signaling message processing*.

5.2.2.3 Layer 3. Tactical common-channel signaling messages shall consist of a fixed number of fields, each comprised of one or more 8-bit characters. Each 8-bit character shall have 6 bits to carry trunk-signaling information. The other 2 bits shall be reserved for control and parity. Each message shall contain, as a minimum, a start-of-message field, a message-type field, a message-number field, an end-of-message field, and a message-parity field. Most messages have additional fields between the message-type field and the end-of-message field. The messages shall be composed in accordance with TT-A3-9016-0056, the section titled *Common channel signaling messages*.

5.2.3 Wide-network interface to reference point B. Same as ISDN base-level interface (see 5.2.1).

5.2.4 Gateway functions. The tactical, ISDN base level, and wide networks shall provide end-user to end-user service. The gateway function at reference point B shall provide signal conversion, as described in 5.2.4.1 to 5.2.4.4, to obtain interoperability between strategic and tactical subscribers.

5.2.4.1 Circuit-switch-signaling message conversion. Interoperability between tactical circuit switches and ISDN circuit switches shall be accomplished through appropriate transformation of signaling messages at the gateway function located at reference point B. The gateway function shall translate out-of-band signaling messages between the tactical circuit-switched network and ISDN switched networks for calls

initiated in either direction. Messages to and from the tactical circuit-switched network side of the gateway function shall comply with the digital common-channel signaling and supervision paragraphs of TT-A3-9016-0056. Messages to and from the ISDN side of the gateway function shall comply with ANSI T1.111, T1.112, and T1.113, as described in mandatory Appendix D. Messages shall be converted or translated by mapping information in appropriate fields, as necessary, to support orderly call initiation, connection, and release phases. Applicable messages shall be returned and translated, as needed, because of busy conditions, nonavailability of the called party, incompatible terminals, security restrictions, or preemption. A typical call initiation, connection, and release gateway signaling conversion is shown in figures 5.2 and 5.3.

5.2.4.1.1 Call initiation phase. For calls originated in the tactical circuit-switched network, tactical call-initiate messages shall be forwarded to ISDN as initial address messages; ISDN address-complete message replies shall be returned to the tactical network as call-complete messages. For calls originated in the ISDN, initial address messages shall be forwarded as tactical call-initiate messages; tactical call-complete message replies shall be returned as ISDN address-complete messages.

5.2.4.1.2 Call connection phase. For calls initiated in the tactical network, ringback shall be returned to the originating tactical network in the traffic channel, after the call complete message has been returned in the signaling channel. Ringback shall continue until the answer message is received from ISDN. When the answer message is received, the traffic channel connects through as a 64-kbps-ISDN-PCM to 16-kbps-tactical-CVSD channel for nonsecure voice calls. For calls originated in ISDN, ringback shall not be supplied by the gateway. The gateway function shall monitor ringback in the traffic channel from the tactical network; when ringback ceases, the gateway shall send an answer message, in the signaling channel, to ISDN and shall connect through the traffic channel as a 64-kbps-ISDN-PCM to 16-kbps-tactical-CVSD channel for nonsecure voice calls. For secure voice or data calls, the traffic channel shall be connected through as a rate-adapted, 64-kbps-ISDN to 16-kbps-tactical channel.

5.2.4.1.3 Call release phase. For call disconnects originated in the tactical circuit-switched network, tactical release messages shall be forwarded as ISDN release messages; the ISDN release-complete message shall be returned as a tactical release-acknowledge message. For call disconnects originated in the ISDN network, the ISDN release message shall be forwarded as a tactical release message; the ISDN release-complete message shall be returned as a tactical release-acknowledgment message.

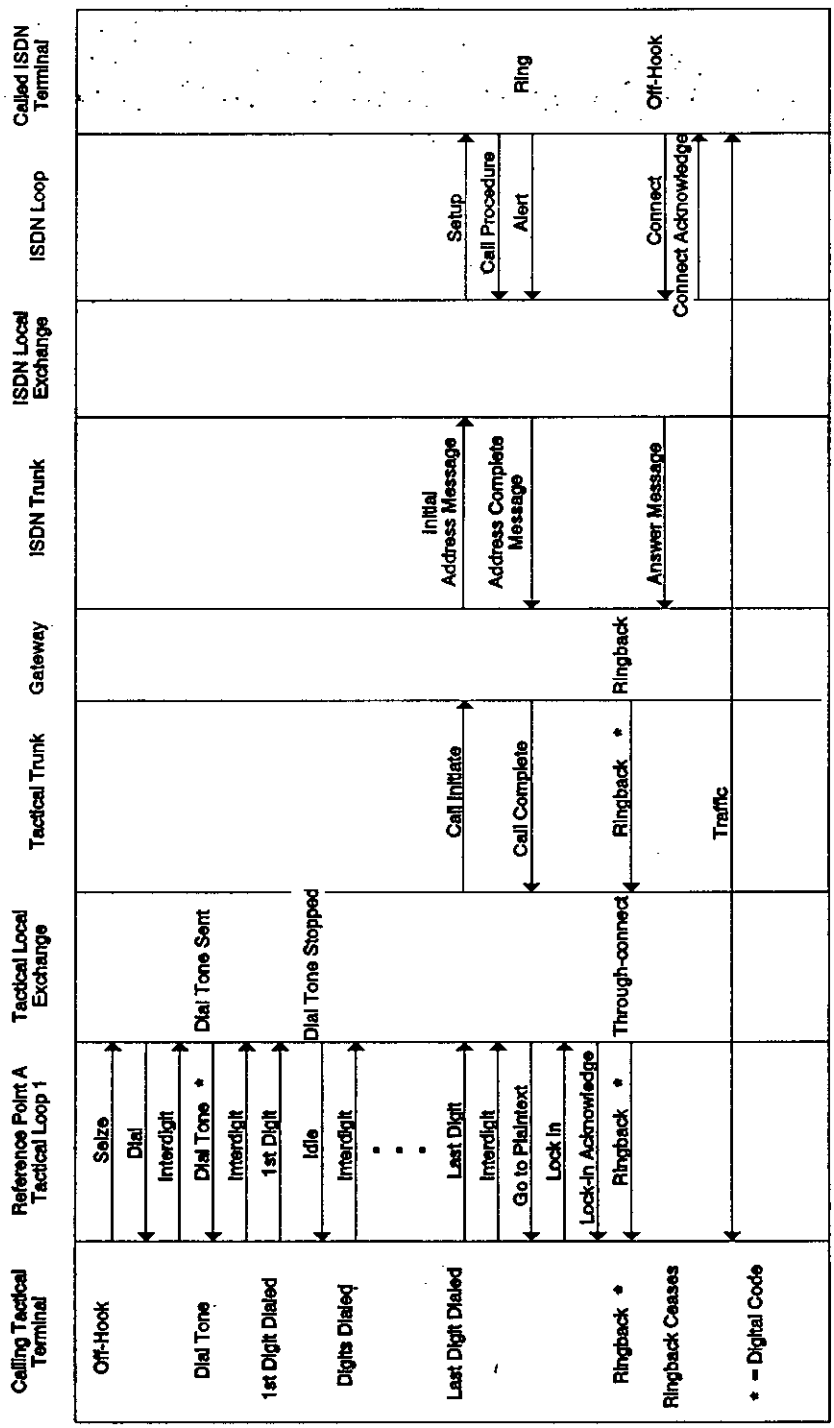


FIGURE 5.2. Call initiate and connection phase signalling.

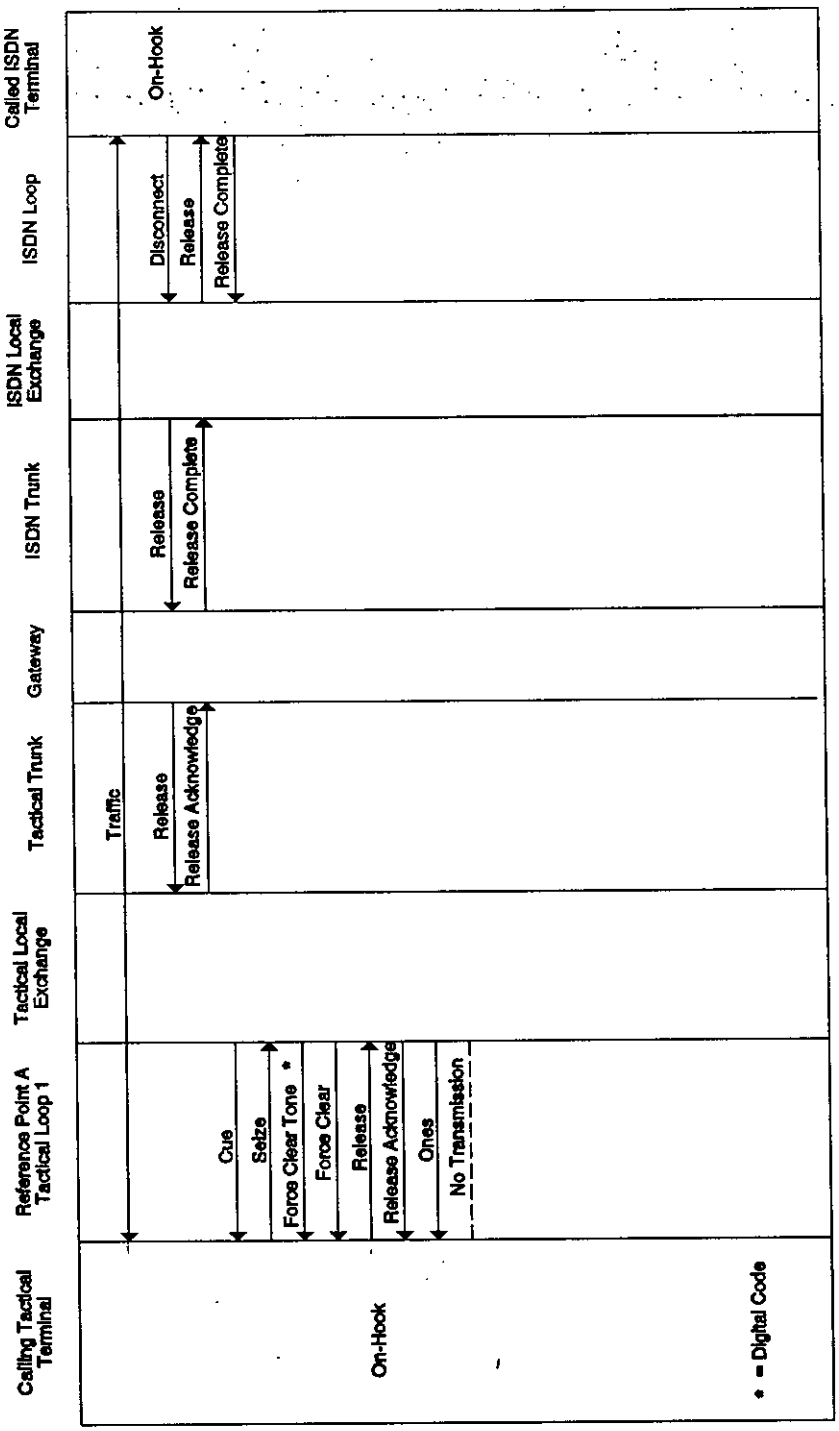


FIGURE 5.3. Call Release Phase Signalling.

5.2.4.2 Packet switching. Tactical packet switches and ISDN packet switches shall comply with CCITT X.75 for connection mode service. They shall provide interoperability between host computers connected to tactical packet-switched networks and host computers connected to ISDN packet-switched networks. All switches requiring connectionless mode of service will comply with ISO DIS 10589 for IS-IS routing information exchange protocols.

5.2.4.3 Voice telephony. Tactical telephone subscribers shall be interoperable with ISDN telephone subscribers. Normally, this shall be accomplished by conversion between the tactical voice algorithm and the ISDN voice algorithm. See 4.1.5 for a description of ISDN and tactical voice algorithms. The gateway function shall provide the capability to achieve end-to-end secure voice calls by providing a transparent, bit-rate-adapted connection between compatible digital voice terminals as described in 4.1.6 and 4.1.7.

5.2.4.4 Circuit-switched data. The gateway function shall provide for the transfer of circuit-switched data between tactical subscribers and ISDN subscribers. The gateway function shall provide bit-rate adaption for ISDN B-channels in the manner described in 4.1.7, for standard bit rates up to 16 kbps.

5.3 Standards for reference point B (NATO). This standard defines the standards applicable to the interface between U. S. network elements and NATO network elements.

5.3.1 U.S.-wide-network to NATO interface. The interface between U.S. strategic and NATO strategic circuit-switched networks shall comply with 5.3.1.1 to 5.3.1.3. The interface between U.S. strategic and NATO strategic packet-switched networks shall comply with STANAG 4263, Annex D (for layer 3), and STANAG 4262, Annex D (for layer 2).

5.3.1.1 Layer 1. The signal at reference point B (NATO) shall comply with the following parameters, as specified in CCITT Recommendation G.704.

a.	Line code	HDB3.
b.	BNZS	B4ZS in accordance with CCITT Recommendation G.703, the Annex titled *Definition of Codes*.
c.	Bit rate	2.048 Mbps.

d.	Number of channels	32, numbered from 0 to 31. (Normally, 30 channels are used as information-bearer channels, 1 channel is reserved for frame alignment, and 1 channel is reserved for common-channel signaling.)
e.	Frame length	256 bits, numbered 1 to 256.
f.	Frame repetition rate	8000 frames per second.
g.	Frame alignment signal	0011011. The frame alignment signal shall occupy positions 2 to 8 in time slot 0 of every other frame. Bit 2 of time slot 0, in frames not containing the frame alignment signal, shall be fixed at logical one. (See figure 5.4.)
h.	Frame alignment signal format	See table IV.
i.	High-rate signals	H_0=384 kbps.
j.	Time-slot assignment	Time slot 16 shall be used to transfer common-channel signaling information (D-channel), when it is present. Time slots 1 to 15 and 17 to 31 are available for allocation to other channels (B or H_0). An H_0-channel may be assigned any six time slots in the frame, in numerical order (not necessarily consecutive).

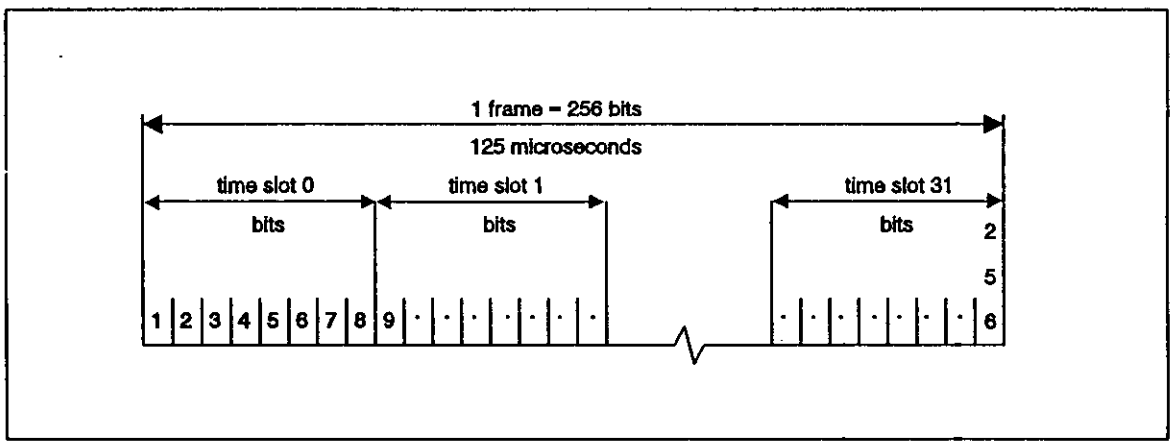


FIGURE 5.4. Frame format for a 2.048-Mbps signal.

TABLE IV. Allocation of frame bits 1 to 8.

Bit number / Alternate frames	1	2	3	4	5	6	7	8
Frame containing the frame alignment signal	Si	0	0	1	1	0	1	1
	Note 1	Frame alignment signal						
Frame not containing the frame alignment signal	Si	1	A	Sa4	Sa5	Sa6	Sa7	Sa8
	Note 1	Note 2	Note 3	Note 4				

Note 1 -- Si is the bit reserved for international use. If not used, this bit should be fixed at 1 on digital paths crossing an international border.

Note 2 -- This bit is fixed at 1 to assist in avoiding simulation of the frame alignment signal.

Note 3 -- A is the remote alarm indication. In undisturbed operation, it is set to 0; in alarm condition, it is set to 1.

Note 4 -- Sa4 to Sa8 are spare bits.

k.	Signaling data link	The signaling data link bit rate shall be 56 kbps, evolving to 64 kbps. Fifty-six kbps signals shall occupy bit positions 1, 2, 3, . . ., 7 of the 64-kbps D-channel. The unused bit position shall be set to "1." The signaling data link shall be a bidirectional transmission path for common-channel signaling, comprising two "data channels" operating together in opposite directions at the same data rate. The signaling data link constitutes the lowest functional level (layer 1) in the SS7 functional hierarchy. SS7 shall be capable of operating over both terrestrial and satellite transmission links. The operational signaling data link shall be exclusively dedicated to the use of a SS7 signaling link between two signaling points in SS7.

5.3.1.2 Layer 2. Layer 2 is the same as 5.2.1.2, except for the signaling message structure. The standard routing label for international signaling shall comply with CCITT Q.704, the section titled *Routing label*. The routing label for international calls shall consist of 14 bits for the destination point code, 14 bits for the originating point code, and 4 bits for the link selection code.

5.3.1.3 Layer 3. Layer 3 is the same as 5.2.1.3, except for section 4 of ANSI T1.114. The ANSI standards in section 4 of T1.114 include some minor variations from the international standards. CCITT Recommendation Q.774 shall take precedence over the national standard when signaling messages are exchanged over international gateways.

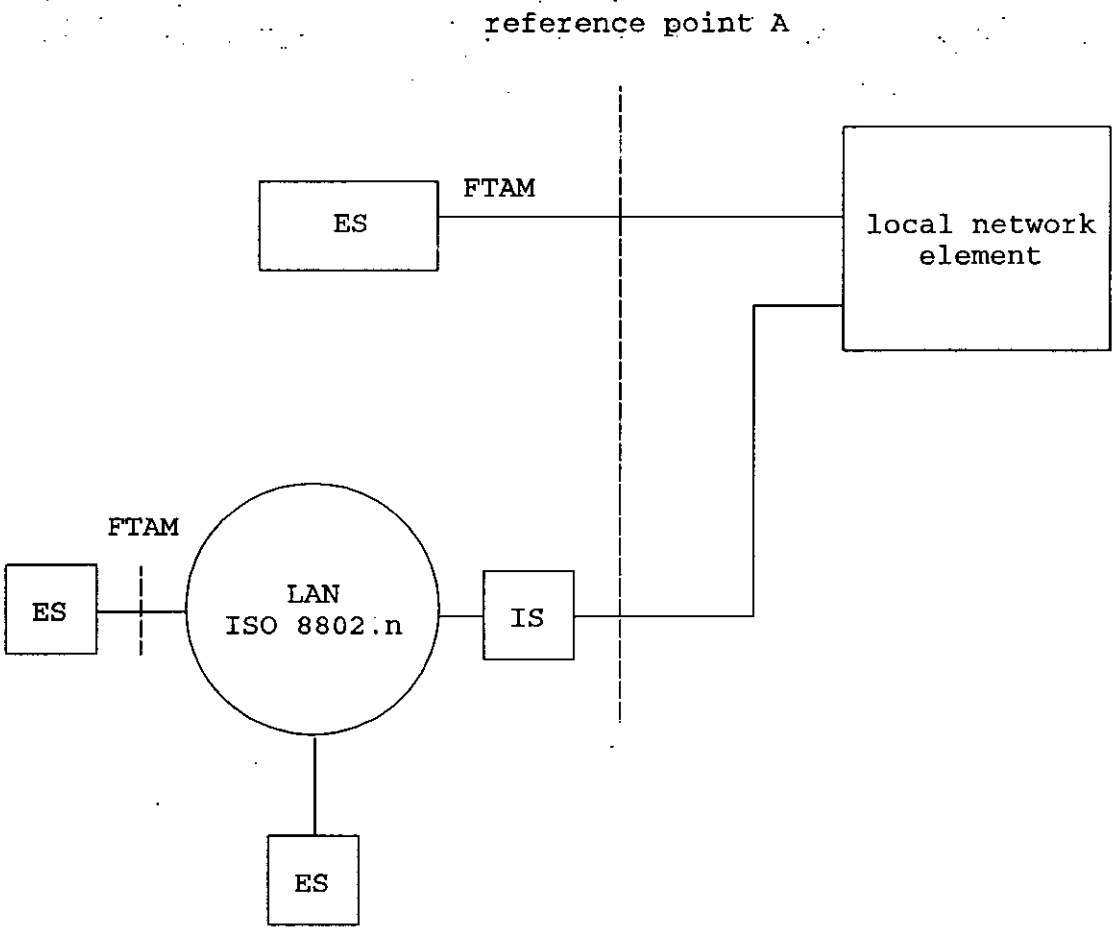
5.3.2 U.S.-tactical to NATO-tactical interface. The interface between U.S.-tactical and NATO-tactical circuit-switched networks shall comply with STANAGs 4206 to 4212, 4214, and 4290. The interface between U.S.-tactical and NATO-tactical packet-switched networks shall comply with STANAG 4249.

5.3.3 TCP/ISO gateway. It is anticipated that U.S. end systems and networks will use data communications protocols based on MIL-STD-1777 and MIL-STD-1778 for a period of time after the ISO transport protocol is implemented in NATO. For this reason, a TCP-to-ISO protocol conversion capability shall be included at reference point B (NATO). This will allow the U.S. to comply with STANAG 4264 during the transition period where both TCP and ISO transport protocols must be accommodated. This approach has been described and published, and is provided in mandatory Appendix A. The TCP/ISO gateway approach shall be an interim measure until ESs achieve ISO compatibility as described in 5.4.2.

5.4 Functional profiles. The functional profiles described in 5.4.1 and 5.4.2 apply to host computers (end systems) that may be connected directly to a local-network element (reference point A) or to a gateway (intermediate system), which is then connected to a common-user network via reference point A (see figure 5.5). Data communications between end systems may cross-reference points A, B, and B (NATO). Data communications, which cross reference point B (NATO), between a U.S. end system and an end system of a NATO nation shall comply with all STANAGs applicable to layers 4-7 of the OSI reference model. The STANAG numbers are given in 5.4.1 and 5.4.2. The corresponding International Standardized Profile (ISP) classifications are provided. The document governing the preparation of ISPs is ISO/IEC TR 10000.

5.4.1 Application profiles. DoD application profiles use protocol standards from the ISO RM layers 5 through 7 to provide end-to-end information transfer. Sections 5.4.1.1 through 5.4.1.4 provide the application profiles for file transfer, access, and management (FTAM); for the message handling system (MHS); for directory service (DS); and for virtual terminals (VT). These functional profiles are used to ensure interoperability between DoD computers. Part 5 of NIST Special Publication 500-183 provides stable implementation agreements for protocols associated with the upper layers (4-7).

5.4.1.1 File transfer, access, and management. The FTAM application shall provide the capability to address, access, and manage the movement of information files among users. *File transfer* is the movement of a complete file between end systems. *File access* is the reading, writing, or deleting of selected parts of a file residing on one end system by a user located at a remote end system. *File management* is the remote reading and altering of attributes that define a file. The ISPs for FTAM will be found in ISO ISP 10607 (6 parts). Two categories are defined: limited-purpose and full-purpose systems.



LEGEND:

ES = end system
IS = intermediate system
n = 3, 4, or 5
FTAM =file transfer, access, and management
LAN = local area network

FIGURE 5.5. Functional profiles.

5.4.1.1.1 Limited-purpose system. A limited-purpose system shall implement, as a minimum, the following profiles:

ISP	DESCRIPTION
AFT 11	Simple File Transfer -- This profile shall enable users to read or write a complete file with unstructured text or a binary set.
AFT 3	Management -- This profile shall enable end-system users to manage files within the Virtual Filestore residing remotely.

5.4.1.1.2 Full-purpose system. A full-purpose system shall implement, as a minimum, the following profiles:

ISP	DESCRIPTION
AFT 12	Positional File Transfer -- This profile shall enable users to read or write a single file access data unit or a complete file with sequential text, in addition to the capability provided by the AFT 11 profile. This profile shall be compatible with the Simple File Transfer (AFT11) for transfer of unstructured files.
AFT 21	Simple File Access -- This profile shall enable users to access files with unstructured text, sequential text, and an unstructured binary set.
AFT 3	Management -- This profile shall enable end-system users to manage files within the Virtual Filestore residing remotely.

5.4.1.1.3 Virtual filestore. FTAM protocol and service definitions shall allow users on different end systems to modify and transfer files without requiring that one user know the detailed file characteristics of the other user. This shall be accomplished by defining Virtual Filestore, which is used for communications between end systems and is mapped to corresponding elements of the local file system residing in an end system. The mapping between the real file and the virtual file, with its file

access structure, is performed by the local FTAM agent. Virtual Filestore is defined in ISO 8571-2. Virtual Filestore shall be defined by the attributes defined in 5.4.1.1.3.1 and 5.4.1.1.3.2.

5.4.1.1.3.1 File attributes. The file attributes represent a file as it is actually stored and shall consist of the following:

- File name
- Storage account
- Encryption name
- Legal qualification
- Permitted actions
- File availability
- File size
- Private use
- Access control
- Contents type
- Future file size

Date and time of:

- Creation
- Last modification
- Last read access
- Last attribute modification

Identity of:

- Creator
- Last modifier
- Last reader
- Last attribute modifier

5.4.1.1.3.2 Activity attributes. The activity attributes shall occur only while an FTAM dialog is in progress. They are of no relevance to an end system and its real file outside of such a dialog. The activity attributes shall consist of the following:

a. Current access request

b. Current initiator identity

c. Current access passwords

d. Current calling application entity title

e. Current account

f. Current responding application entity title

g. Current access context

h. Current concurrency control

i. Current location

j. Current processing mode

5.4.1.1.4 Application layer. The FTAM functional profiles shall be supported at the application layer by the following base standards:

ISO 8613 Office Document Architecture (ODA)

ISO 8571 FTAM

ISO 8650 Association Control Service Elements (ACSE)

5.4.1.1.4.1 Office document architecture. ISO 8613 (Parts 1, 2, and 4 to 8) specifies rules for describing the logical and layout structures of documents. It also specifies the rules for character, raster, and geometric content of documents so that complex documents can be interchanged. Since the functional profiles addressed are limited to files with unstructured text, sequential text, and an unstructured binary set, no further discussion is provided for ODA at this time.

5.4.1.1.4.2. FTAM service elements. The services offered are defined in ISO 8571-3. The part of a protocol concerned with the realization of a particular service is a service element. FTAM offers a file service provided by a considerable number of service elements. Association between peer FTAM processes shall be achieved by the use of ACSE (see 5.4.1.1.4.3). Once an FTAM association has been established, the function determines the FTAM operational environment that is to exist over the association. Table V provides the relationship between FTAM functions, profiles, services, and associated service elements. These protocol specifications shall define the formats and parameters of the control messages, and the actions to be taken by the peer entity on receiving a control message or a user's service request. The protocol specification offered can be found in ISO 8571-4. Parts 9 and 10 of NIST Special Publication 500-183 provides stable implementation agreements for FTAM protocols. The FTAM service elements are grouped into functional units that support FTAM.

5.4.1.1.4.3 Association control service elements. The FTAM shall use ACSEs that are required by all application standards but that do not depend on the specific nature of the application that is standardized. ISOs 8649 and 8650 define these service elements and protocol standards. The services in the association category shall include the following: application association establish, application association release (orderly release), and application association abort (disorderly release).

TABLE V. Relationship between FTAM functions and service classes.

FUNCTION	PROFILE				SERVICE	SERVICE ELEMENT
	AFT11	AFT12	AFT21	AFT3		
Kernel	M	M	M	M	• Establish regime • Release orderly regime • Release disorderly regime • Select file • Deselect file	• F-INITIALIZE • F-TERMINATE • F-ABORT • F-SELECT • F-DESELECT
Read	M	M	M	--	• Read bulk data • Transfer data unit • End data transfer • End transfer • Cancel data transfer • Open file • Close file	• F-READ • F-DATA • F-DATA-END • F-TRANSFER-END • F-CANCEL • F-OPEN • F-CLOSE
Write	M	M	M	--	• Write bulk data • Transfer data unit • End data transfer • End transfer • Cancel data transfer • Open file • Close file	• F-WRITE • F-DATA • F-DATA-END • F-TRANSFER-END • F-CANCEL • F-OPEN • F-CLOSE
File Access	--	--	M	--	• Locate • Erase	• F-LOCATE • F-ERASE
File Management	--	--	--	M	• Create file • Delete file • Read attributes • Change attributes	• F-CREATE • F-DELETE • F-READ-ATTRIB • F-CHANGE-ATTRIB
Recovery	O	O	O	--	• Recover regime • Insert check point • Cancel data transfer	• F-RECOVERY • F-CHECK • F-CANCEL
Restart Data Transfer	O	O	O	--	• Restart data transfer • Insert check point • Cancel data transfer	• F-RESTART • F-CHECK • F-CANCEL

NOTES:

M = mandatory; O = optional; -- = not available.

5.4.1.1.5 Presentation layer. This layer is associated with presentation issues over a session connection and is defined in ISO 8823. STANAG 4256 contains a provision to satisfy NATO military requirements for OSI RM presentation layer service, and STANAG 4266 discusses the provision for the basic NATO military features for the presentation layer protocol. With the interconnection of heterogeneous systems, it is assumed that the service coding is not necessarily the same at both systems.

5.4.1.1.5.1 Abstract syntax. The FTAM presentation entities shall exchange abstract syntax in a precise representational form understood by peer entities for the following abstract syntaxes:

a. ISO FTAM unstructured text (FTAM-1)

b. ISO FTAM sequential text (FTAM-2)

c. ISO FTAM unstructured binary set (FTAM-3)

The abstract syntax is formally defined in ISO 8824, Abstract Syntax Notation 1 (ASN.1), without reference to the use of any encoding technique. The transfer syntax defines the order in which the bytes shall be physically transmitted to include information encryption requirements, compression of recurrent information, or both. Transfer syntax is derived by applying the basic encoding rules for ASN.1 to the abstract syntax defined in ISO 8825 and STANAG 4259. A pairing of abstract and transfer syntax, known as presentation context, shall be successfully negotiated between peer presentation entities. The list of negotiated presentation contexts is known as the defined context set.

5.4.1.1.5.2 Presentation services. The presentation services shall comply with ISO 8822 and shall be limited to the kernel portion, which is related to connection establishment and release, and to application information transfer services. STANAG 4266 contains provisions to satisfy NATO's military requirement for the OSI RM presentation layer.

5.4.1.1.6 Session layer. The session layer protocol defined in ISO 8327 and service elements are defined in ISO 8326. STANAG 4255 contains a provision to satisfy NATO military requirements for OSI RM session layer service, and STANAG 4265 discusses the provision for the basic NATO military features for the session layer protocols. This layer, defined in ISO 8327, is associated with data transfer, control, and management services over a session connection. The intelligence behind the control of session services lies with the peer application processes. They shall access the session services by use of mirrored services

provided through the presentation layer. For the FTAM to function over a session connection, the following functional units shall be available at this layer: kernel, resynchronization, and minor synchronization.

5.4.1.1.6.1 Kernel. The kernel functional unit supports the basic session services of connection establishment, normal data transfer, and connection release.

5.4.1.1.6.2 Resynchronization. The resynchronization function shall be used when a session user determines the information exchange is unreliable and requests that information transfer restarts at a mutually agreed point: synchronization point serial number. This service originated at the application layer (F-CANCEL) and mirrored through the presentation layer (P-RESYNCHRONIZE). On issuing this request, the application processor shall not invoke any further session service, other than a disorderly termination (F-ABORT), until such time as the confirmation has been received.

5.4.1.1.6.3 Minor synchronization. Minor synchronization points are used to establish commonly understood points in the information exchange within a dialog unit. The FTAM check point service shall be used to provide either the recovery or restart function. The F-CHECK service element shall provide a facility for FTAM to insert check points into the flow of data. The presentation layer mirrors this service element (P-MINOR-SYNC) and becomes S-MINOR-SYNC at the session layer.

5.4.1.2 Military Message-Handling System (MMHS). The MMHS application profile addresses store and forward electronic messaging between network users. The MMHS is defined in STANAG 4406 and is based on the CCITT Recommendation X.400.

5.4.1.2.1 Military Messaging Service (MMS). The MMS is similar to the Interpersonal Message Service (IPMS) defined in civilian standards, but includes extensions for services required in the military environment. The vendor shall provide an MMS in accordance with STANAG 4406. The content-type used for the MMS is P772 (IPMS uses P22).

5.4.1.2.2 Electronic Data Interchange (EDI) service. The vendor shall provide EDI service in accordance with CCITT Recommendation X.435 and applicable portions of NIST Special Publication 500-183 (Stable Implementation Agreements).

5.4.1.3 Directory services. DS is specified in CCITT Recommendation X.500 (Blue Book, 1988). FIPS 146 Version 3 is expected to address X.500. Part 11 of NIST Special Publication 500-183 provides stable implementation agreements for DS

protocols. The ISP for DS will comply with the profile classification ADIn, as indicated below:

ADIn	APPLICABLE STANDARDS
Layer 7	CCITT X.500 ISO 8650 Association Control Service Element (5.4.1.1.4.3)
Layer 6	ISO 8823 Connection-oriented Presentation Protocol (5.4.1.1.5)
Layer 5	ISO 8327 Connection-oriented Session Protocol (5.4.1.1.6)

5.4.1.4 Virtual terminal. VT application profiles allow terminals and hosts on different networks to communicate without the hosts having knowledge of specific terminal characteristics. Part 14 of NIST Special Publication 500-183 provides stable implementation agreements of VT protocols. Two categories are defined:

a. Simple System -- A teletype (TTY)-compatible device that uses a simple line or character at a time and controls characters from the American Standard Code for Information Interchange (ASCII) character set. A simple system supporting the TELNET profile requires the asynchronous mode (A-mode) of operation, as indicated below:

ISP	DESCRIPTION	
AVT12	Mode A; TELNET	MIL-STD-1782
AVT13	Mode A; Line Scroll	FIPS 146 Version 3
AVT14	Mode A; Paged	FIPS 146 Version 3

b. Forms Capable System -- Supports forms-based applications with local entry and validation of data by the terminal system. Some of the functions supported are cursor movement, erase screen, and field protection. The forms profile requires the synchronous mode (S-mode) of operation and specifies simple delivery control. A forms-capable system shall support both the forms profile specified in section 14.8.3 of the Workshop Agreements and the TELNET profile defined in MIL-STD-1782. The corresponding Workshop Agreements with FIPS 146, Version 2, limits the forms-capable system to the A-mode. The S-

mode should be addressed when the FIPS 146, Version 3, is released. The applicable standards are shown below:

AVT2n	APPLICABLE STANDARDS
Layer 7	ISO 9040 VT ISO 8650 Association Control Service Element (5.4.1.1.4.3) ISO XXXX Remote Operations Service Element (ROSE)
Layer 6	ISO 8823 Connection-oriented Presentation Protocol (5.4.1.1.5)
Layer 5	ISO 8327 Connection-oriented Session Protocol (5.4.1.1.6)

5.4.2 Transport profiles. Transport profiles identify the use of base standards for OSI RM layers 1 through 4 to provide information transfer between transport entities. The transport profiles are limited to providing connection-oriented transport service (COTS) (see 5.4.2.1). COTS may be supported by either a connectionless network, (see 5.4.2.2.2) or a connection-oriented network (see 5.4.2.2.3). To meet the evolutionary requirement for existing DoD network protocols, ESs shall emulate the transport service described in 5.4.2.1.1, using the end-to-end service of the internet protocol suite. The approach taken shall be based on the RFC 1006 method (see mandatory Appendix B) to treat the transmission control protocol (TCP), which is a connection-oriented, stream-based, transport protocol, as though it were actually offering a connection-oriented network service. RFC 1086 supplements RFC 1006 and is contained in Appendix C. This approach shall be used only on an interim basis until GOSIP is fully implemented.

5.4.2.1 Connection-oriented transport service. COTS implies that although the internal operation of a network is based on packets, to the end user the network is indistinguishable from a full-period, end-to-end system. The packetized operation must be essentially invisible to the user, with data coming out of the network in exactly the same sequence it went into the network.

5.4.2.1.1 Transport service. The transport service, as defined in ISO 8072, shall move data reliably from one end system to another. STANAG 4254 contains provisions to satisfy NATO military requirements for transport layer service. The transport service is in one of three phases at any one time: transport connect (TC) establishment, data transfer, and transport connection release.

5.4.2.1.2 Transport protocols. Based on the available network service, five different COTS protocols exist. These are termed Transport Protocol (TP) Classes 0 through 4 (TP0-TP4). For GOSIP end-systems, COTS, as provided by TP4, is mandatory, except when the end system is also connected to public messaging domains conforming to CCITT Recommendation X.410 (Red Book). Then it must be capable of using TP0 when acting as a messaging relay between the two domains. A detailed description of the structure and encoding of these transport protocol data units (TPDU) can be found in CCITT Recommendation X.224, the section titled *Structure and Encoding of TPDUs*, or ISO 8073. STANAG 4264 discusses the provision for the basic NATO military features for the transport layer protocol. Part 4 of NIST Special Publication 500-183 provides stable implementation agreements for TPDUs. All unknown parameters in a TPDU shall be ignored. Known parameters with valid lengths but with invalid values shall be handled as follows:

a. Parameter	Action
• transport service	
• access point (TSAP) identifier	• Send T-DISCONNECT
• TPDU size	• ignore parameter; use default
• version	• ignore parameter; use default
• checksum	• discard
b. Alternate Protocol	
• Class	• Protocol error

5.4.2.1.3 Security protocol. The end-to-end security protocol shall be as defined by NIST IR 90-4250. The NIST IR 90-4250 submitted to ANSI for adoption shall be used to define the end-to-end security protocol at the transport layer. This security protocol encapsulates the TPDU, but first, it adds an integrity code if integrity is required, encrypts the entire TPDU if confidentiality is required, and then puts the result in a secure encapsulation of the TPDU. A receiver that has the correct cryptographic key shall be able to decrypt the secure encapsulation of the TPDU, to verify its integrity and then process the resulting TPDU.

5.4.2.2 Supporting networks. COTS shall be supported by either a connectionless network that provides Connectionless Network Service (CLNS) or a connection-oriented network (see 5.4.2.2.3) that provides Connection-Oriented Network Service (CONS) and shall have a common network addressing structure (see 5.4.2.2.1).

5.4.2.2.1 Network addressing. The second addendum to the network service, ISO 8348, defines network layer addressing. To maintain the transparent goals of the OSI RM, a network address makes no implications about the physical location of a node; nor does a network address contain explicit routing information. The OSI strategy is to use a hierarchically structured address. At the top level, an address shall be divided into two parts: an initial domain part (IDP) assigned by the ISO/IEC, and a domain specific part (DSP). The IDP is further subdivided into two parts: the authority and format identifier (AFI) and the initial domain identifier (IDI). Table VI provides the AFI values assigned by ISO/IEC as a function of the IDI format. The AFI values are a function of the DSP syntax indicating either decimal or binary. The maximum IDP length in digits is also provided.

TABLE VI. AFI values.

IDI FORMAT	AFI VALUE DSP SYNTAX		IDP MAXIMUM LENGTH
	DECIMAL	BINARY	
CCITT X.121	36, 52	37, 53	16
ISO 3166 DCC	38	39	5
CCITT F.69	40, 54	41, 55	10
CCITT E.163	42, 56	43, 57	14
CCITT E.164	44, 58	45, 59	17
ISO 6523 ICD	46	47	6
NON-ALIGNED	48	49	2

The ISO/IEC assigned the international code designator (ICD) to NIST and the data country code (DCC) to ANSI. The System and Network Architecture Division at NIST determines how Government agency-specific identifications are assigned and registered at the national level. NIST has delegated the management responsibility to the Telecommunications Customer Service

Division within the General Service Administration (GSA). Presently, the GSA is defining the registration procedures as well as usage guidelines. The AFI value of decimal 47 specifies that the IDI part is interpreted as a four-decimal-digit ICD and that the DSP has a binary abstract syntax. The IDI, set to 5 for the entire Federal Government's use, including DoD and the DSP address structure, is defined in FIPS 146-1, section 5.1.1. NIST applied for and obtained an ICD equal to 6 for DoD use. The DSP is presently undefined.

5.4.2.2.2 Connectionless network. A connectionless network is one in which a service can be requested at any time there is no requirement for a direct connection between users. Since no connection exists between users, the network address shall be included explicitly with every transfer request. Wide-area networks, such as the Defense Data Network (DDN), use internetwork protocols (see 5.4.2) to provide connectionless network service. Most of the commercially available connectionless networks are configured within a localized geographical area known as a LAN. These LANs are often capable of transmitting data at very high rates, up to 10 Mbps. This is made possible by the fact that the physical medium is installed between systems located in close proximity. The ISPs for COTS over CLNS will be found in ISO ISP 10608 (Parts 1, 2, and 5). GOSIP, Version 2, mandates that connectionless network service be provided to Government users.

5.4.2.2.2.1 Network service. Connectionless network services are defined in addendum 1 to the Network Service Definition Standard, ISO 8348.

5.4.2.2.2.2 Network protocols. Protocol combinations to provide connectionless network service are defined in ISO 8880, Appendix 3. To offer connectionless network service, ISO 8880, Appendix 3, identifies the protocols used to implement the connectionless network protocols found in ISO 8473. ISO 8473, Addendum 3, specifies the provisions of the underlying service over a subnetwork that provides the OSI data link service. Part 3 of NIST Special Publication 500-183 provides stable implementation agreements for network protocols. When an end system is connected to a local-area or point-to-point subnetwork, the end system to intermediate system dynamic routing protocol, as defined in ISO 9542, shall be used. This protocol is limited to addressing the routing between end systems and intermediate systems on the same or directly connected subnetworks. (Intermediate system to intermediate system dynamic routing protocols shall comply with ISO DIS 10589 after approval. Implementation of the security option shall require the assignment of new parameter values to the Reason for Discard parameter in the error reporting, as defined in FIPS 146-1. The

NIST IR 90-4250 SP3 (submitted to ANSI for adoption) shall be used to define the security option at the network layer. This standard shall be implemented in intermediate gateway systems, as well as end systems. The security protocol encapsulates the TPDU, but first adds network addresses to the protocol header for network routing, adds an integrated code if integrity is required, encrypts the entire TPDU if required, and then puts the result in a secure encapsulation of the TPDU.

5.4.2.2.2.3 Link service. The link service provided over a LAN shall be a Type-1 connectionless network service. The link layer of the OSI RM shall be divided into two sublayers. The logical link control (LLC) shall establish, maintain, and terminate the logical link between devices, and the media access control (MAC) shall regulate access to the medium. Part 2 of NIST Special Publication 500-183 provides stable implementation agreements for protocols related to subnetworks.

5.4.2.2.2.3.1 Logical link control. For LANs, the LLC shall comply with ISO 8802-2 to provide a connectionless subnetwork service to support connectionless network protocols. The LLC shall be used to maintain the logical link between devices. The LLC generates command packets (or frames) called protocol data units, and interprets them. The unacknowledged connectionless service shall allow the network entities to exchange link service data units without a data-link level connection. The data transfer can be point-to-point, multicast, or broadcast.

5.4.2.2.2.3.2 Media access control. The MAC in LANs deals with the methods for allowing a particular node to transmit on the data transmission channel available to it. A LAN can be configured as either a bus or a ring topology. Furthermore, two primary methods are used to control access: carrier sense multiple access/collision detection (CSMA/CD) and token passing. The IEEE 802 Committee on LAN and the ISO community have followed with corresponding ISO 8802 series standards that address media control and physical layers. The ISO 8802-3 standard addresses CSMA/CD, ISO 8802-4 addresses token-passing buses, ISO 8802-5 addresses token-passing ring buses, and ISO 9314 addresses FDDI.

5.4.2.2.2 Connection-oriented network. A connection-oriented network is based on the ability to reserve a path through a network for the duration of the network connection. Based on FIPS 146-1, an end-system shall be directly connected to a connection-oriented network only when the network is an CCITT X.25 wide-area network or an ISDN wide-area network. The ISPs for COTS over CONS will be found in ISO ISP 10609 (9 parts).

5.4.2.2.3.1 Network service. The network service for a connection network is defined in ISO 8348. STANAG 4253 contains provisions to satisfy NATO's military requirements for OSI RM network layer service. The network service is in one of three phases at any one time: connection establishment, data transfer, and connection release.

5.4.2.2.3.2 Network protocols. Protocol combinations to provide connection network service shall be defined in ISO 8880, Appendix 2. To offer the connection network service, ISO 8880, Appendix 2, identifies the protocols used to realize the CCITT X.25 packet-layer protocol (PLP) over the subnetwork. ISO 8878 defines the use of CCITT X.25 PLP to provide the OSI connection network service. ISO 8208 defines the packet format and control procedures for the exchange of packets that contain control information and user data at data terminal equipment. ISO 8208, Addendum 2, defines the dial-up access to a packet-switched public data network through a public switched telephone network (PSTN), an integrated-services digital network, or a circuit-switched public data network. CCITT Q.931 defines additional signaling requirements during set-up of an incoming call when D-channel access is required on the ISDN. Part 3 of NIST Special Publication 500-183 provides stable implementation agreements for network protocols. STANAG 4263 contains the military features required for NATO's network layer protocols.

5.4.2.2.3.3 Data link service. Data link service for a connection network is defined in ISO 8886. STANAG 4252 contains provisions to satisfy NATO's military requirements for OSI RM data-link layer service. The data link service is in one of three phases at any one time: connection establishment, data transfer, and connection release.

5.4.2.2.3.4 Data link protocols. End systems that are directly connected or use dial-up access to the packet-switched public network shall use the LAPB protocol, except for connection to the ISDN D-channel. For access via the ISDN D-channel, the LAPD protocol shall be used as defined in CCITT Q.921. The LAPD protocol is a fully standard implementation of the ISO High-level Data Link Control (HDLC) protocol and can be found in the following documents: ISO 7809, ISO 4335, ISO 3309, ISO 8471, and ISO 8885. Part 2 of NIST Special Publication 500-183 provides stable implementation for protocols related to subnetworks. STANAG 4262 contains the military features required for NATO's data-link layer protocols.

5.4.2.2.3.5 Physical layer. FIPS 146-1 does not mandate any specific physical interface except for ISDN. For non-ISDN application, or for the R interface of ISDN applications using terminal adapters, MIL-STD-188-114 shall be used for the physical

layer interface. MIL-STD-188-114 is based on EIA 422 and 423 and is interoperable with EIA 232 (formerly RS-232), and the CCITT V.35 digital interface referenced in GOSIP FIPS 146. For ISDN, FIPS 146, Version 2, mandates that for the basic rate interface (BRI) at the S and T reference points, ANSI T1-605-1988 shall be used. STANAG 4251 contains provisions to satisfy NATO's military requirements for OSI RM physical layer service, and STANAG 4261 contains the military features for NATO's physical layer protocols.

5.5 Subscriber network elements. General requirements for subscriber network elements are listed in 4.5.2.1. The implementation of narrowband ISDN and in the future broadband ISDN requires a substantial investment in the upgrade of DIS. To take advantage of DIS features requires direct digital capabilities be provided to all subscriber network elements. These subscriber elements are discussed on the basis of their access requirements: direct, mobile, universal, and indirect.

5.5.1 Direct access. Direct access can be provided by copper wire, coaxial cable, or fiber optical cable. The access method depends on the bandwidth that must be supported. This entails developing all-digital subscriber-terminal equipment with direct access that can provide voice, high-speed communications of data; facsimile (text and graphics); still and motion video communications; as well as broadcast of high-resolution television.

5.5.1.1 Voice. All voice end terminals shall provide voice digitization. Strategic subscriber terminals shall use 64-kbps PCM or 32-kbps ADPCM. Tactical subscriber terminals shall have the capability to interface, either directly or via a switch, using 16-kbps CVSD analog-to-digital (A-D) conversion as defined in MIL-STD-188-113. Voice terminals employing CELP shall be capable of providing 4.8-kbps CELP A-D conversion as defined in FED-STD 1016. The voice digitization algorithm shall be negotiated during call set-up and the 4.8-kbps CELP shall be the preferred mode. Military satellite (in the anti-jam mode) and HF radio applications shall use 2.4-kbps LPC.

5.5.1.2 Data. All end terminals that provide data communications shall be capable of supporting all application profiles, as defined in 5.4.1.

5.5.1.3 Facsimile. All end terminals that provide text and graphics in the form of facsimile shall conform to MIL-STD-188-161.

5.5.1.4 Video. All end terminals that provide motion video conferencing shall conform to MIL-STD-188-131, which is being

written to comply with the P times 64 standard described in CCITT H.320. All end terminals that provide still graphics video conferencing shall conform to MIL-STD-188-132, which is being developed to conform to the commercial standard being sponsored by DoD in the EIA TR29 Facsimile Committee.

5.5.1.5 High-definition television. High-definition television (HDTV) standards are under development for end terminals that provide the HDTV function.

5.5.2 Mobile access. Due to rapid advances in signal processing and integrated circuit technology, digital radio has become viable technology for implementing wireless subscriber loop service in remote rural areas; for providing wireless private branch exchange (PBX) service; for cellular digital mobile radio service; for digital mobile satellite service; and for tactical digital radio network service. All subscriber network elements requiring mobile access shall have a default voice algorithm of 4.8-kbps CELP, and the gateway function at reference point A shall allow for data traffic with bit count integrity to support both secure voice and data. Standards for mobile access are under development. NSA has been leading the Government effort to create standards within industry that support interoperable data communications via mobile subscriber interface and control, and network interface and control.

5.5.2.1 Wireless subscriber loop service. Standards for remote wireless subscriber loop service are under development.

5.5.2.2 Wireless PBX service. New low-power, short-range digital radio (average transmitter power in the order of 10 mW) technologies are being developed. The use of digital multiplexing with demand assignment access of digital radio links could service multiple user terminals. Time-division multiple access (TDMA) standards for cellular digital mobile radio service (see 5.5.2.3) may also be viable for multiple user indoor application.

5.5.2.3 Cellular digital mobile radio service. Standards are being developed for next-generation digital cellular mobile radio systems. [The Special Mobile Group (GSM) of the European Telecommunications Standards Institute (ETSI) is standardizing a pan-European TDMA mobile radio technology. The Telecommunications Industry Association (TIA) and Cellular TIA (CTIA) are standardizing an entirely different TDMA technology for North America. It is expected that these two efforts will converge to enhance interoperability.]

5.5.2.4 Digital mobile satellite service. Digital mobile satellite service will be based on Ultra Small Aperture Terminal

(USAT) technology with a 10 to 12-inch antenna diameter. USAT requires very complex hybrid spread-spectrum modulation and access techniques to limit interference. The information rate is limited to 2.4 kbps, ruling out the use of the default 4.8-kbps CELP voice algorithm for this service. Standards will be developed for end terminals requiring service over digital mobile satellite links.

5.5.2.5 Tactical digital radio network service. Standards for HF radio subsystems are listed in 4.4.2.7. Standards for HF radio subscriber networks are under development. Planning standards for HF will be contained in MIL-STD-187-721. HF radio automatic link establishment (ALE) shall comply with FED-STD-1045. Standards for automatic HF radio networking will be contained in FED-STD-1046. Standards for HF store-and-forward service will be contained in FED-STD-1047. Standards for automatic HF networking to multiple transmission media will be contained in FED-STD-1048. Standards for HF radio automatic operation in stressed environments will be contained in FED-STD-1049.

5.5.3 Universal access. Universal access will allow subscribers to initiate and receive calls through the DIS irrespective of their geographical location. Two basic concepts related to universal access are emerging: the mobile communication facility offered by the Universal Mobile Telecommunications System (UMTS), and the personal communication facility offered by the Personal Telecommunications Service (PTS). Standards for universal access are under development.

5.5.3.1 Universal mobile telecommunications system. The UMTS shall provide mobile communications, not only by keeping track of the location of the mobile subscriber (by storing information about their current location), but also by maintaining ongoing calls and connection, despite their movement.

5.5.3.2 Personal telecommunications service. The PTS shall be provided across multiple networks and allows network-independent user identification. From a network point of view, the PTS may be based on either wired or wireless interface.

5.5.4 Indirect access. End terminals can be configured on a LAN or a group of LANs that are joined by bridges to form an extended LAN.

5.5.4.1 Local area network. End terminals configured to a LAN at the network layer shall use connectionless network protocols, as defined in ISO 8473, and at the link layer shall use logical link control type-1, as defined in ISO 8802-2. End terminals at the MAC level that require: carrier sense multiple access shall

conform to ISO 8802-3. End terminals at the MAC level that require token passing bus access shall conform to ISO 8802-4. End terminals at the MAC level that require token-passing ring-bus access shall conform to ISO 8802-5. End terminals at the MAC level that require FDDI shall conform to ISO 9314. The IEEE has developed an IEEE Standard 802.6, *Distributed Queue Dual Bus (DQDB) Subnet of a Metropolitan Area Network (MAN)*, which will eventually be adapted as an ISO 8802-6 standard. End terminals at the MAC level that require broadband service (see 5.6) via MAN shall conform to ISO 8802-6. Wireless LANs are a subject for further study.

5.5.4.2 Bridges. A bridge connects data links for the purpose of forwarding packets between local networks. A bridge operates at the logical link or MAC layer (level 2 of the ISO RM), independent of higher-level protocols. A bridge architecture can be based on either a transparent spanning tree or on source routing.

5.5.4.2.1 Transparent-spanning-tree bridge. A transparent-spanning-tree bridge shall modify its address table dynamically for each packet it receives. If a station address is unknown, the bridge shall flood all links other than the link over which the packet was received. A transparent-spanning-tree bridge can function as either a local or remote MAC bridge. A local bridge is directly connected to LANs and shall conform to IEEE 802.1D. A remote bridge is directly attached to one or more LANs, and also on unspecified interconnection medium and will conform to draft standard IEEE P802.1G/1D. The MAC frame is encapsulated within the appropriate interconnecting medium for transmission across the network to a peer remote bridge.

5.5.4.2.2 Source routing bridge. In a source routing bridge the route shall be determined by the source station for each frame sent through one or more bridges to the destination station. The routing information is contained within each frame and used by each bridge it transitions over. Source routing information shall be acquired by the originating station by broadcasting a request that is updated by each bridge it transitions over. Multiple copies that are received by the destination station are sent back to the originating station, and the information is used to select the preferred path. A source routing bridge shall conform to ISO 8802-5.

5.6 Broadband service support. Broadband service support within the DIS shall pertain to network interface transport rates, formats, and architectures associated with digital hierarchies defined in ANSI T1.105, CCITT Recommendations G.707 and I.121, and IEEE 802.6.

5.6.1 The transport digital hierarchy. In support of broadband services, two primary digital hierarchy standards are applicable: ANSI T1.105 and CCITT Recommendation G.707. Within CONUS, the ANSI T1.105 Digital Hierarchy Optical Interface Rates and Formats Specification, commonly referred to as SONET, defines the layer 1 Synchronous Optical Hierarchy (SOH). CCITT Recommendations G.707 through G.709 define the layer 1 Synchronous Digital Hierarchy (SDH) for international use. Where common rates and formats exist, the SONET standard is functionally and structurally equivalent to CCITT Recommendation G.707.

5.6.1.1 Synchronous Optical Network. The primary objective of SONET is the definition of a SOH with sufficient flexibility to support transmission rates and formatted signals. Any signal transmitted using ANSI T1.105 shall employ ANSI T1.106 to provide opto-electrical conversion.

5.6.1.1.1 Rates. Where necessary, support of various low transmission rates across a high-rate connection shall be accomplished through the employment of synchronous multiplexing. Multiplexing results in a family of standard rates and formats, which are multiples of the basic 51.84-Mbps Synchronous Transport Signal 1 (STS-1) rate. To support broadband services, basic rate signals shall be time-division multiplexed to build higher transmission rates. SONET shall support sub-STS-1 rate signals by multiplexing these lower rate signals in accordance with ANSI T1.105. The SONET rates applicable to the DIS are listed in table VII.

TABLE VII. SONET rates (Mbps).

STS-1	51.840
STS-3	155.520
STS-12	622.080
STS-24	1244.160
STS-48	2488.320

NOTE:

STS-M = Synchronous Transport Signal M.
Optical Carrier Level-M (OC-M) is the optical equivalent to STS-M.

5.6.1.1.2 Frame format. Figure 5.6 depicts the STS-M frame structure. For M=3, each of nine rows of the STS-1 frame consists of 9 octets of overhead and 261 octets of user traffic payload.

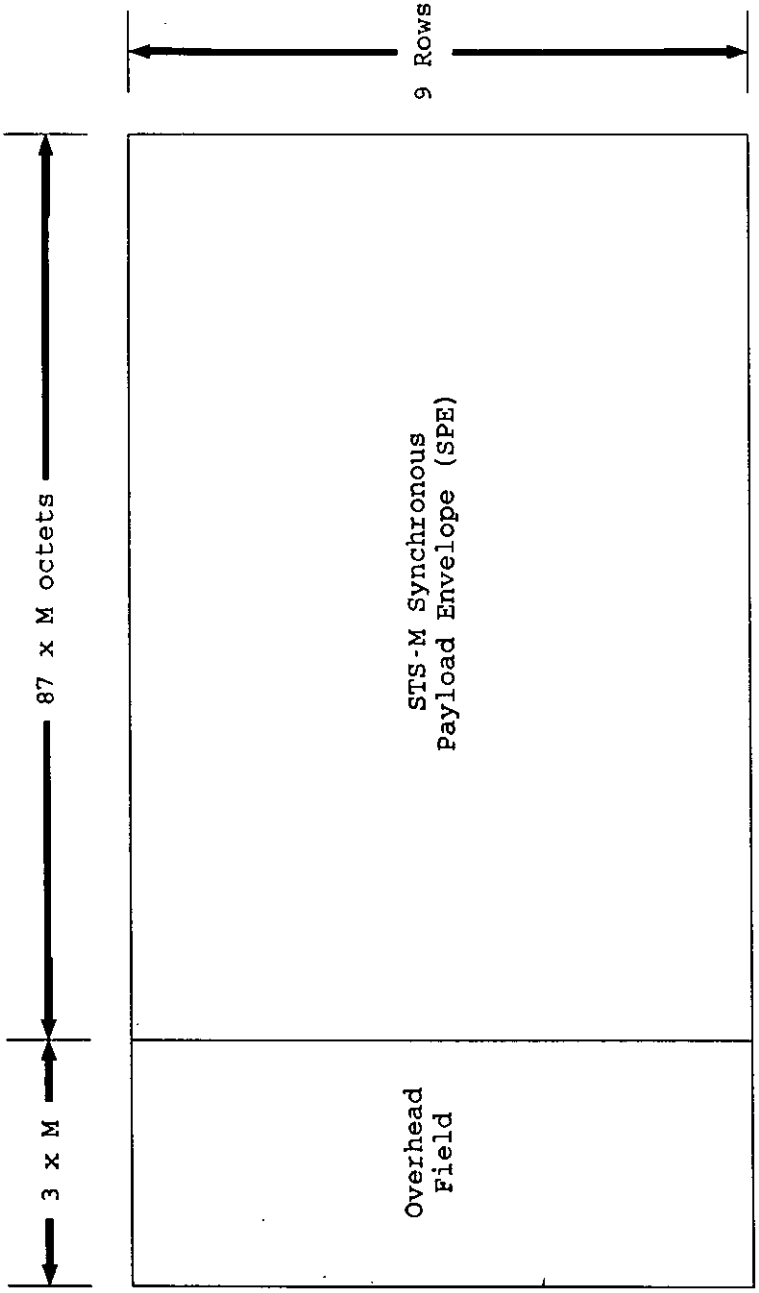


FIGURE 5.6. SONET STS-M frame format.

5.6.1.1.3 Services. The SONET standard is capable of supporting a variety of connection-oriented and connectionless transport data services. (The services that SONET supports include DS3 telecommunications signals, video, or low-rate telephone services such as DS1, DS1C, or DS2 signals). The following SONET concatenated rates shall be supported: STS-3C, STS-12C, and STS-24C.

5.6.1.1.3.1 Management. The SONET standard incorporates embedded operations channels within its overhead field. These embedded operations channels shall be used to provide communications capacity to support DIS integrated network management. To facilitate the reliable transport of user traffic, the overhead operations channel shall be multiplexed into the STS-M frame to support link integrity.

5.6.1.1.4 Interworking support. SONET shall provide a layer 1 transport service for interworking between DIS network elements.

5.6.1.2 The Synchronous Digital Hierarchy

5.6.1.2.1 Rates. The SDH supports broadband services as a layer 1 capability. Table VIII shows the applicable SDH rates. The basic SDH rate of 155.520 Mbps is designated STM-1. Other rates are derived by multiplexing the basic rate in accordance with CCITT Recommendations G.708 and G.709.

TABLE VIII. CCITT Recommendation G.707 rates (Mbps).

STM-1	155.520
STM-4	622.080
STM-8	1244.160 (*)
STM-16	2488.320 (*)

NOTE:

(*) indicates rate under study by the CCITT.
STM-N = Synchronous Transport Module-Level N

In accordance with CCITT Recommendation G.709, provisions shall be made to support sub-STM-1 rates.

5.6.1.2.2 Frame format. Figure 5.7 illustrates the STM-N frame format. For N=1, the STM-1 frame shall consist of 93 octets of overhead and 2337 octets of payload. An STM-N (where N>1) consists of 81 x N octets of overhead and 2349 x N octets of payload.

5.6.1.2.3 Services. The SDH shall support all services defined in 5.6.1.1.3.

5.6.1.2.4 Management. Network management services shall be supported via an embedded service channel within the SDH overhead structure. The SDH service channels shall support DIS network management objectives as specified in 5.7.

5.6.2 Metropolitan area networks. The DIS shall support the IEEE 802.6 DQDB. To support broadband services across large areas, multiple DQDB subnetworks may be interconnected to form MANs. MANs may be suitably interconnected to form wide area networks (WANs). By definition, MANs are subscriber-network elements within the DIS framework.

The primary objective of MANs shall be the establishment of a transparent and reliable (low delay and no loss of user throughput capacity) mechanism for interconnecting LANs. A transparent MAN environment is one in which two or more interconnected LANs appear as a single logical LAN to their respective users. The IEEE 802.6 standard has not been adopted as an international standard.

5.6.2.1 Services. The DQDB subnetwork is a distributed multi-access network that supports integrated communications services. Specifically, the DQDB supports connectionless data transfer, connection-oriented data transfer, and isochronous communications (e.g., voice). In support of connectionless services, annex B of IEEE 802.6 provides information on a mechanism for controlling bus communications between nodes. Currently DQDB/MAN related services are planned as a public offering within the contintental United States (CONUS). Outside CONUS, the DQDB/MAN architecture and its services must be supported as a private subscriber network element.

Connectionless packet service shall support variable-length packet service. The connection-oriented data service shall support a virtual channel between any pair of data service users. [A form of connection-oriented data service called Switched Multi-megabit Data Service (SMDS) shall be supported via the IEEE 802.6 compliant open bus when they are aligned at the connectionless MAC service via remote bridge.] The MAN reference model used to support these services is depicted in figure 5.8.

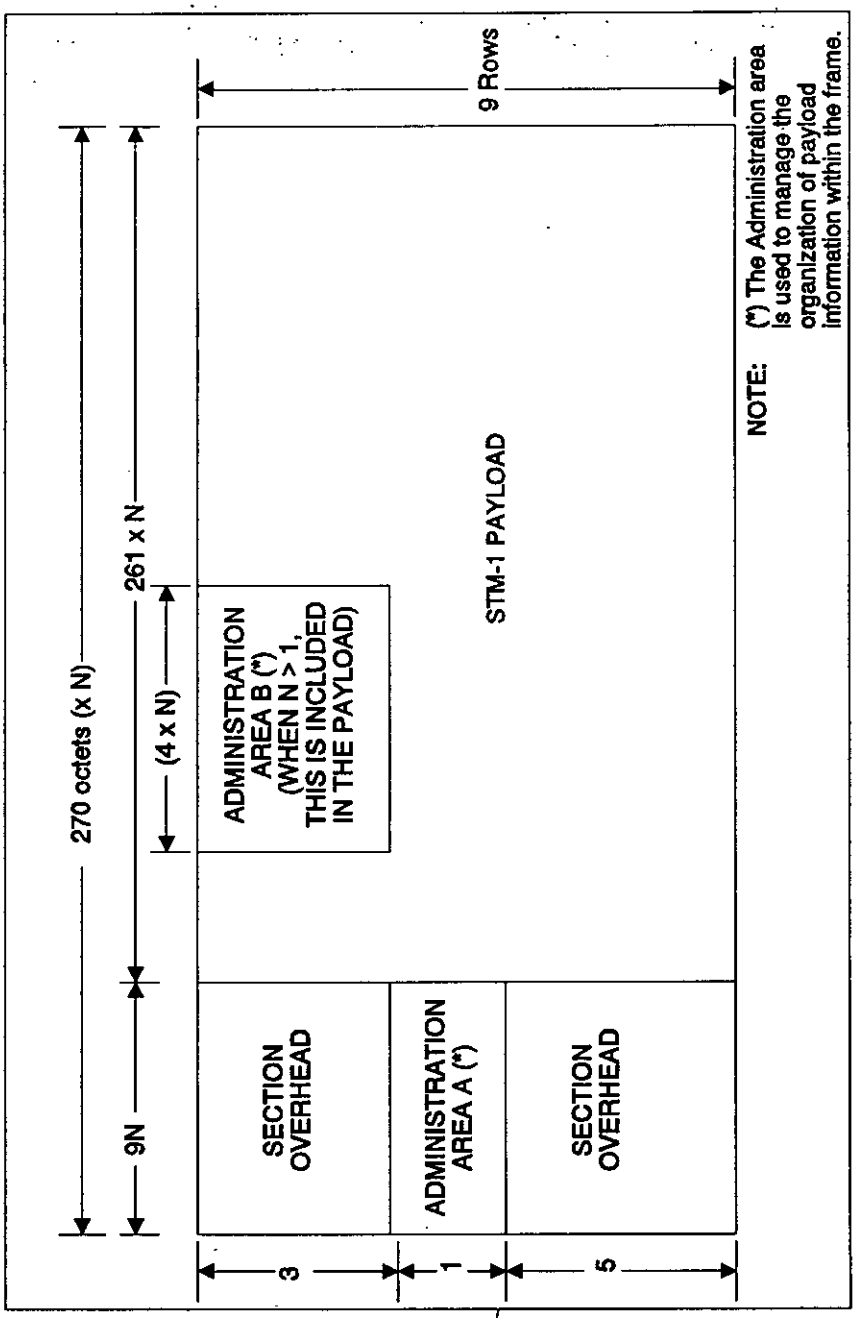


FIGURE 5.7. CCITT STM-N frame format.

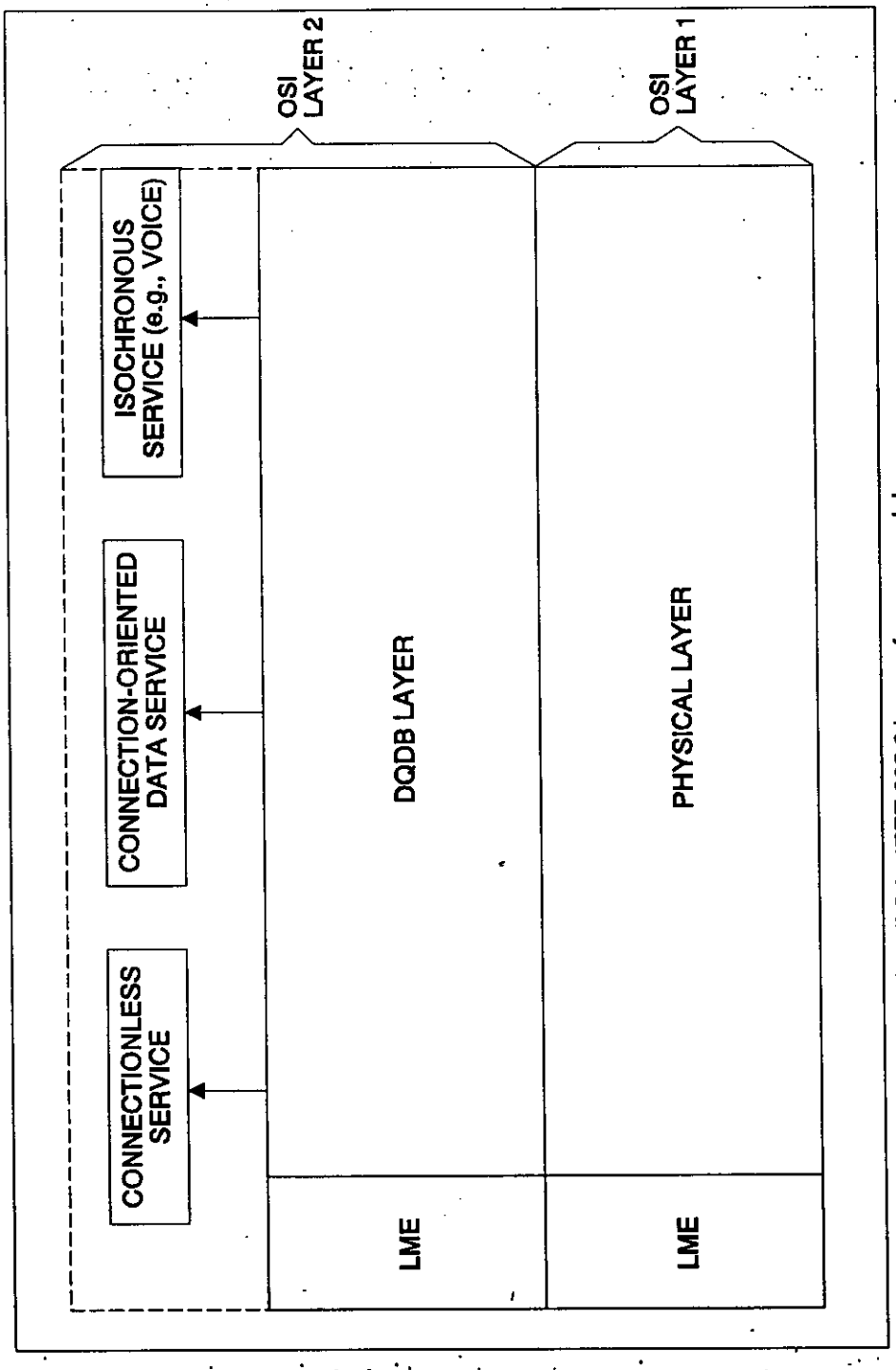


FIGURE 5.8. IEEE 802.6 layer reference model.

5.6.2.2 Rates. The IEEE 802.6 DQDB/MAN standard supports high-speed transport of information across interconnected subnetworks within the DIS. Transport of information is achieved through the use of a 53-octet fixed-cell-based format. [The cell length is equivalent to that of an ATM cell. However, the ATM cell payload is between 44 and 48 octets, depending on whether the ATM Adaptation layer (AAL) uses a portion of the payload capacity for its purposes as defined in 5.6.3.] A DQDB/MAN located outside CONUS shall be interconnected via a SONET/CCITT Recommendation G.707 rate interface.

The rates supported are as defined in CCITT Recommendation G.703 (at 34.368 Mbps and 139.264 Mbps) and CCITT G.707 (at 155.520 Mbps). Lower-rate interfaces shall be supported via multiplexing in accordance with CCITT Recommendation G.709.

5.6.2.3 Architecture. Multiple DQDB subnetworks may be interconnected to form MANs via mediation devices (bridge, router, or gateway). MANs may be viewed as a public or private (e.g., DoD) backbone network. Figure 5.9 shows a notional interconnection of public and private MAN networks.

5.6.2.3.1 DQDB subnetwork architecture. A DQDB subnetwork uses a pair of unidirectional buses (a dual bus pair), referred to as Bus A and Bus B. Bus A and Bus B are independent from the point-of-view of data flow. That is, information on the buses flows independently in opposite directions.

A DQDB subnetwork shall support either an open dual bus or a looped dual bus; in the open dual bus topology, the head of Bus A (i.e., the information source node for Bus A) and the head of Bus B are logically separate and distinct. In the looped bus topology, the head of Bus A and Bus B are collocated.

Within the DQDB subnetwork, nodes shall be physically interconnected by a separate transmission link. A full-duplex transmission link shall carry both Bus A and Bus B management and user traffic between adjacent nodes. Eight levels of priority are supported by the DQDB standard. These levels of priority must be shared between network and user traffic.

5.6.2.4 DQDB/MAN interworking. In support of broadband interworking within the DIS, the IEEE 802.6 DQDB/MAN architecture and protocols shall be used to support any combination of LAN and ISDN connectivity (e.g., LAN-LAN, LAN-ISDN-LAN).

To simplify LAN/MAN interworking, the IEEE 802.6 MAN has been designed to be compatible with other LANs at OSI layer 2. Figure 5.9 depicts a typical scenario in which DQDB/MANs are

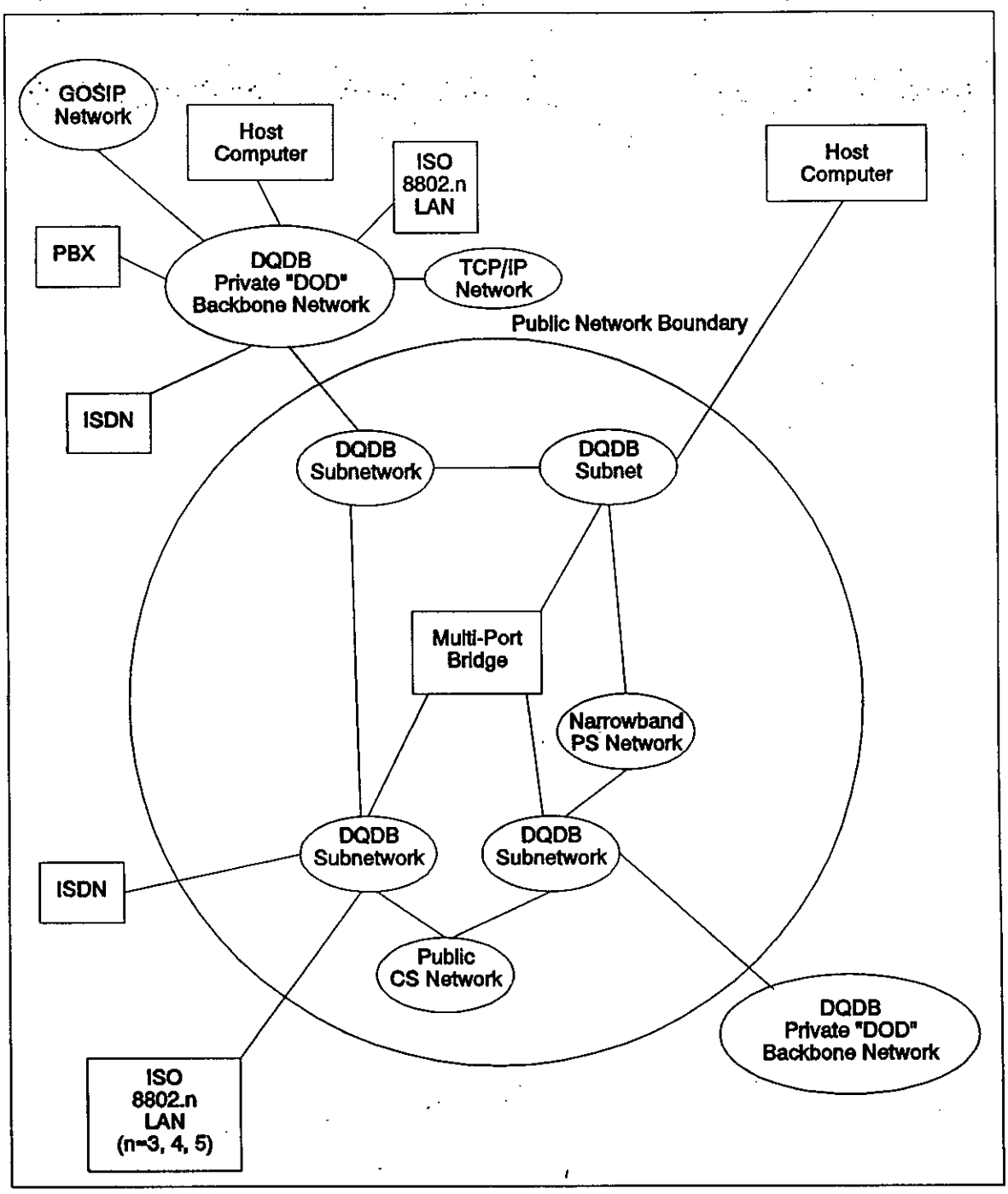


FIGURE 5.9. Notional IEEE 802.6 interworking network architecture.

interworking with a variety of other LANs, MANs, and end-systems (hosts and terminal equipments).

5.6.2.5 Protocol. The DQDB shall employ management, signaling, and traffic protocols to control and monitor access and use of its resources.

5.6.2.5.1 Signaling. Signaling associated with IEEE 802.6 services is not specified within the standard. Wherever possible, existing signaling protocols (e.g., CCITT Q.931) shall be employed. The signaling shall provide for interworking across public networks that use SS7.

5.6.2.5.2 Management. To support integrated DIS network management, the DQDB/MAN shall provide for local and remote management and control of its resources.

5.6.2.5.2.1 Local node management. Local management is not subject to the OSI management definition since all information flow is local to the node's management process. However, when MANs are interconnected via a DIS local- or wide-area network element, the local management shall conform to the management concept defined in 5.7.

5.6.2.5.2.2 Remote management via network/system management. A node's physical and data-link layer objects are monitored, controlled, and coordinated via DIS network management through the DQDB layer management interface. System management application functions shall provide for monitoring, control, and coordination of managed objects through interaction with the DQDB layer management interface.

5.6.2.5.2.3 Remote management via DQDB layer management. Remote management shall provide for remote monitoring, control, and coordination of managed objects within a local node.

5.6.3 The asynchronous transfer mode. The ATM shall be used to provide broadband services. The ATM shall be a transport connection-oriented packet service. The ATM shall provide trunking between the DIS local-network element and the wide-network element at DIS reference point B. The ATM shall comply with draft CCITT Recommendations I.150 and I.361 after approval.

5.6.3.1 The ATM services. The ATM shall support two primary services: interactive and distribution. Interactive services shall correspond to conversational, messaging, and retrieval service. Distribution services shall provide for user control/noncontrol of presentation services. Service parameters shall be negotiable on a cell-by-cell basis, subject to network

management constraints and limitations on parameter ranges. The ATM shall support CONS and CLNS.

5.6.3.1.1 Multimedia service support. Independent network access and connection control functions shall not restrict concurrent support of mixed services (e.g., audio and video) on a single connection. Further, there shall be no inherent impediments to the establishment of multiple connections associating a specific information type. Addition and deletion of optional information types (such as voice, data, facsimile, video) during an active network access shall not be inhibited.

5.6.3.2 The ATM cell attributes. The ATM cell format and cell transfer rate shall comply with 5.6.3.2.1 and 5.6.3.2.2.

5.6.3.2.1 Cell format. The ATM shall be based on the cell structure shown in figure 5-10. The multiplexed information shall be organized as fixed-sized frames called cells. The ATM cell structure shall provide the transport mechanism for information delivered to the User Network Interface (UNI). The UNI shall logically correspond to the DIS at reference point B. The ATM cell presented to the UNI shall be identical to the cell at the network-node interface (NNI), except the NNI cell shall not provide for cell flow control. The UNI shall not flow control incoming network cells.

The ATM cell structure shall be functionally divided into three fields: the cell header field, the AAL field, and the user information part. The AAL field shall correspond to the first four octets of the user information part (information payload) of a cell.

5.6.3.2.2 Cell transfer rate. The ATM supports constant bit rate (CBR) and variable bit rate (VBR) end-to-end bearer service connections. ATM UNI operational rates shall be 155.52 Mbps (SONET STS-3 and CCITT STM-1) and 622.08 Mbps (SONET STS-12 and CCITT STM-4). The ATM shall not inhibit operation across lower-rate digital hierarchies.

5.6.3.3 The ATM reference model. Figure 5-11 depicts the ATM layered protocol reference model. The layered ATM reference model (ATM-RM) shall be functionally aligned with the ISO OSI RM. The ATM-RM shall consists of a physical layer 1, a data link layer 2 (to include the ATM sublayer and AAL functionality) (see 5.6.3.3.2.), and higher layers corresponding to the ISO OSI RM layers 3 through 7. The ATM reference model shall comply with draft CCITT Recommendations I.321 and I.327, after approval.

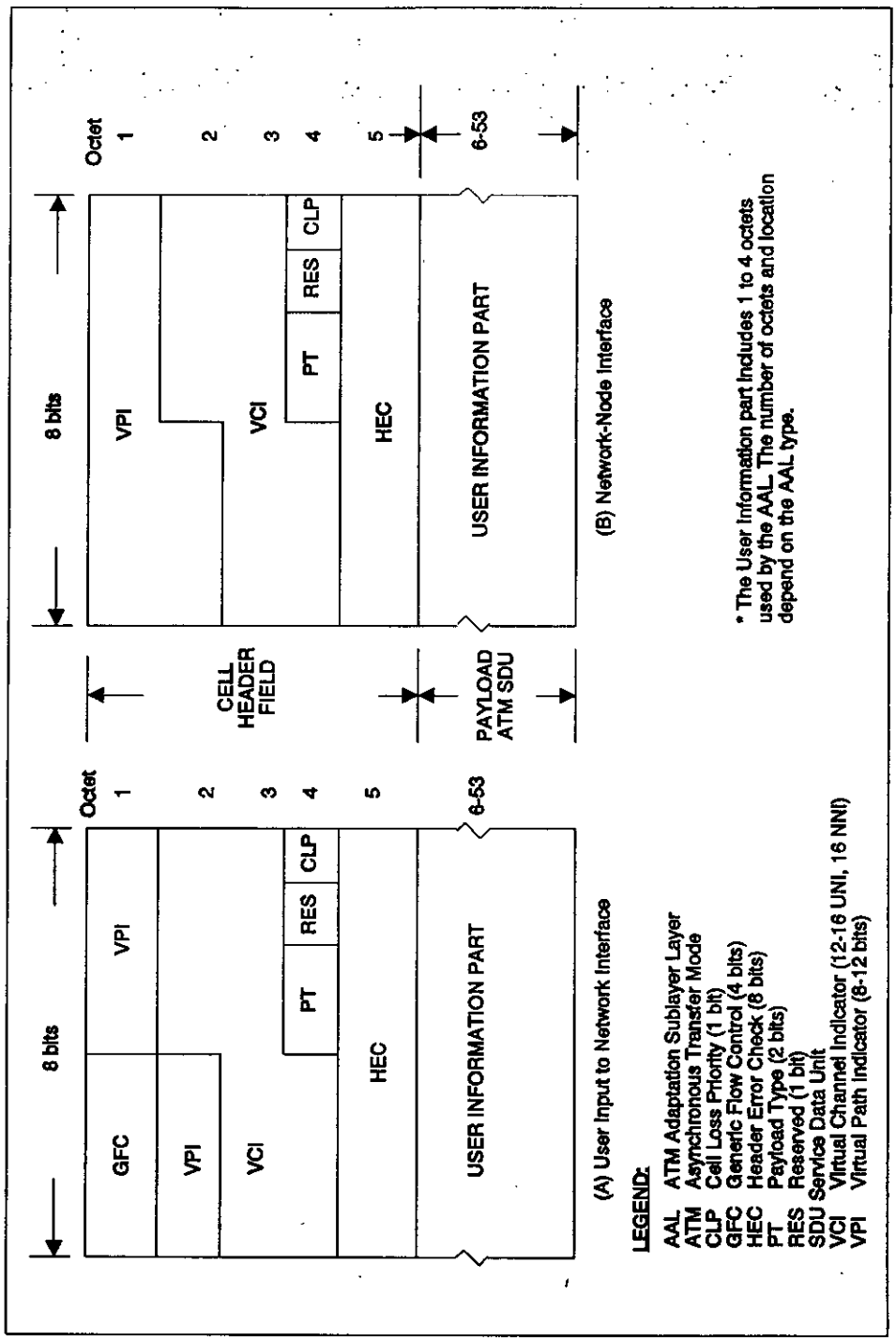


FIGURE 5-10. ATM cell structure.

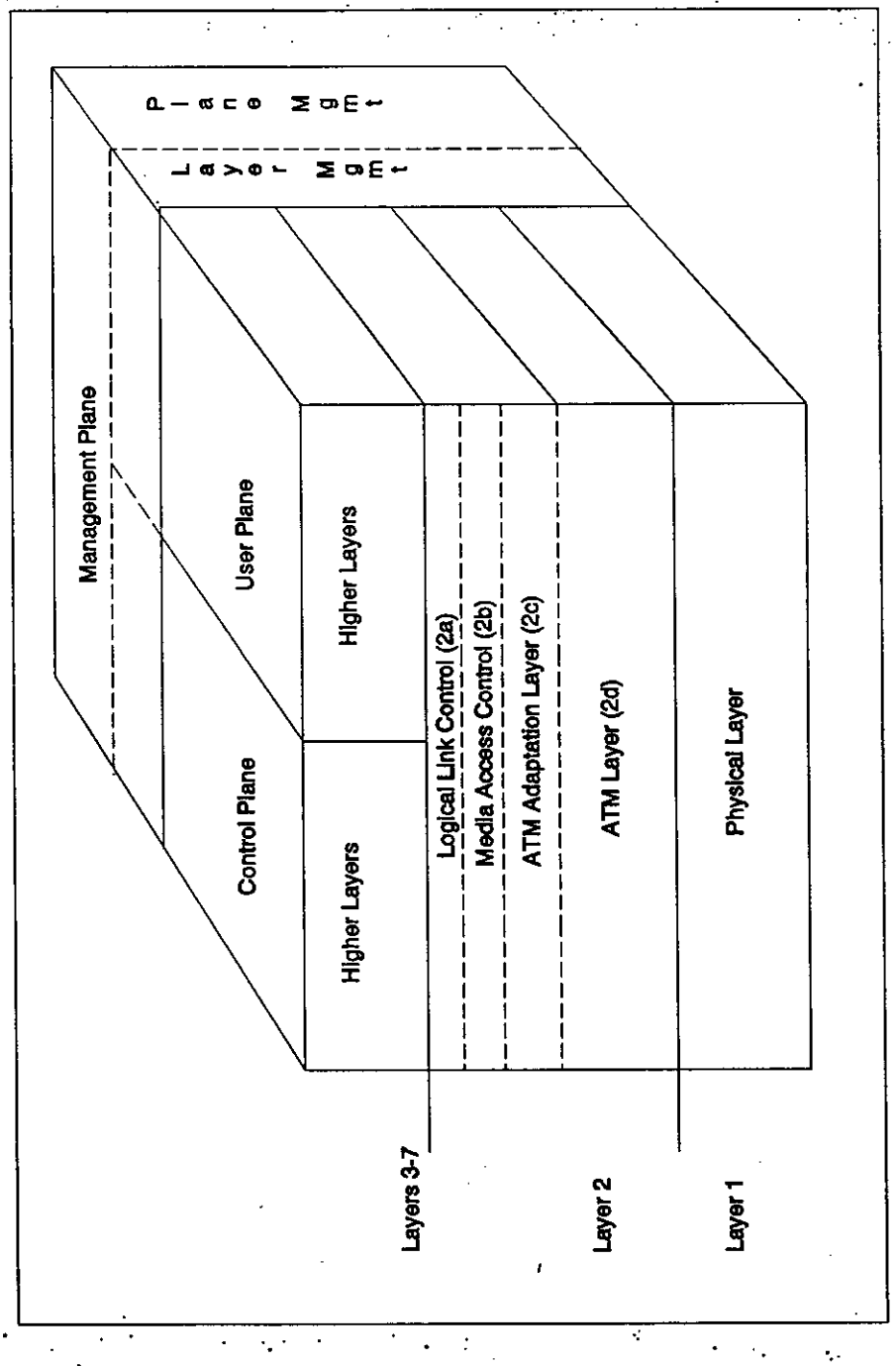


FIGURE 5-11. The ATM protocol reference model.

5.6.3.3.1 Preferred ATM physical layer (layer 1). The preferred ATM physical layer shall be based on the ANSI TI.105-1988 SONET. The ATM sublayer shall be functionally independent of the layer 1 digital hierarchy. The ATM shall support asymmetric interface connections. Asymmetric interfaces shall be those interfaces in which the transmission rate across the interface is not the same in both directions. The ATM physical layer shall comply with draft CCITT Recommendation I.432, and ISO DIS 9314-3, after approval.

5.6.3.3.2 The data link layer (layer 2). The ATM protocol shall reside at the data link layer. The data link layer in support of the ATM shall be functionally separated into an AAL and an ATM layer. The AAL shall perform functions required by the Application profiles, and control and management planes. In addition, it shall support the mapping between the ATM sublayer and the OSI RM layer 3 function. The AAL shall comply with draft CCITT Recommendation I.363 after approval. The ATM sublayer shall ensure delivery of cells.

The AAL shall provide CBR and VBR service support to ISO layers 3 to 7 through the definition of four types of AAL service functions. The AAL type 1 functions shall support CBR service. The AAL type 2 functions shall support CBR service. The AAL type 2 functions shall support VBR service. The AAL type 3 functions shall provide message and streaming services. The Type 3 function shall transport end-to-end one or more (optional) AAL convergence sublayer protocol data units (PDU) in the message mode. Streaming mode service shall provide end-to-end transport of one or more fixed-size service data units (SDUs) within a single AAL convergence sublayer PDU. Delivery of AAL PDU(s) may be tagged as guaranteed or not-guaranteed. The AAL type 4 functions shall provide connection-oriented and connectionless point-to-multipoint VBR message and streaming mode service through the ATM network. The message and streaming mode services shall be functionally identical to the AAL type 3 function.

The ATM sublayer shall provide a common transfer capability to all services, including connectionless services. The ATM sublayer shall support user end-system control of traffic from multiple CBR regular and VBR ATM connections that have various QOS classmarks.

5.6.3.4 ATM interworking. The ATM connections shall support basic ISDN user and signaling services. The ATM shall not inhibit interworking between itself and the basic (nB+D) ISDN network. Interworking with non-ISDN networks shall be accomplished via a network adapter. The network adapter shall provide the necessary translation functions required to ensure that ATM cell information content is delivered to its

destination. The adaptor shall be implemented within the ATM terminal equipment or via an external ATM terminal adapter. The AAL shall support connections between ATM and non-ATM interfaces.

5.6.3.4.1 ATM cell interworking. When interworking between ATM and non-ATM networks within the DIS is required, cell translation shall be performed at the UNI. Cell translation applies to a manipulation of the ATM cell header information to support the routing required by the non-ATM network. No additional information shall be required of the ATM cell to support the interworking function.

5.6.3.5 ATM signaling. (It is envisioned that SS7 will eventually support the ATM). The ATM shall provide a flexible transport service common to connection and connectionless network and bearer services. The preferred method of signaling shall be through the use of separate channel identifiers. Out-of-band (and for interworking in-band) signaling shall be supported. ATM signaling shall comply with draft CCITT Recommendation I.311, after approval.

The ATM signaling function shall support control of ATM virtual channel connections (VCCs) and virtual path connections (VPCs) for information transfer. The signaling function shall support simple multipoint and multiconnection network accesses.

The ATM shall allow for multiple types of services and for the logical separation of signaling from the user information stream. The ATM signaling mechanism shall not prevent a user from supporting multiple signaling entities connected to the network call-control management function via separate ATM VCCs.

5.6.3.5.1 Signaling configurations. The ATM shall support three signaling configurations designated Case A, Case B, and Case C. The Case A configuration shall provide for the establishment of virtual channel (i.e., connectionless) connections through the DIS. Case B shall provide for the establishment of virtual paths (i.e., connection-oriented) connections through the DIS. Case C shall provide for both connectionless and connection-oriented connections through the DIS.

5.6.3.5.2 ATM connectionless service support. The ATM shall support B-ISDN connectionless data service between functional groups able to handle connectionless messages. The ATM shall provide direct and indirect support of connectionless services. The ATM connectionless service support shall comply with draft CCITT Recommendation I.327, Annex A, after approval.

5.6.3.5.2.1 ATM direct support of CLNS. In order to access connectionless data services, a connection shall be established

between the local network element and the ATM network's connectionless service function (CLSF). The CLSF shall reside within the DIS local and wide area networks. The CLSF shall terminate connectionless protocols and reroute cells to the destination end user, based on cell routing information. Direct support of connectionless service is defined to be Case A. The ATM direct support of CLNS shall comply with draft CCITT Recommendation I.211, after approval.

5.6.3.5.2.2 ATM indirect support of CLNS. The connectionless protocol shall be invisible to and independent of the ATM switching function located within the local and wide area networks. ATM indirect support of connectionless services shall be via the connection-oriented service. A transparent connection of the ATM layer, either permanent, reserved, or on-demand, shall be used between B-ISDN. To ensure that no impediments exist to the adoption of a CL protocol, the CL and AAL functions shall be implemented outside ISDN. ATM Case A shall provide indirect support of connectionless services. The ATM indirect support of CLNS shall comply with draft CCITT Recommendation I.211, after approval.

5.6.4 Frame relay mode. The DIS shall support the frame relay mode (FRM). Support of FRM within the DIS shall conform to the ISDN FRM bearer service definition and architectural framework defined in ANSI T1.606. The ANSI FRM definition is closely aligned with CCITT Recommendation Q.922.

5.6.4.1 Services. Although the ANSI FRM is, by definition, an ISDN packet mode bearer service, the FRM service definition does not inhibit its use with any suitable low-bit-error-rate service.

The FRM shall be capable of supporting a variety of connection-oriented and connectionless transport data services. These services shall support the following DIS service access definitions:

a. Circuit-switched access to the DIS network element's remote frame handler (FRM-Case A). The B- and H-channels shall be used to support this access method.

b. Virtual access via the DIS network element's local ISDN connection (FRM-Case B). The B-, H-, and D-channels shall be used to support this access method.

It shall be possible to establish access connections on a demand and permanent basis in accordance with ANSI T1.617. Multiplexing of multiple subscriber data streams onto a single connection, unlike CCITT X.25, shall be performed at the link layer.

5.6.4.2 Rates. The FRM shall have the capability of using the strategic-local network B-, H-, and D-channels and tactical-local network bit rates from 16 kbps to 2.048 Mbps. When using the basic rate ISDN interface, the FRM shall operate at the 64-kbps rate. The FRM use of the D-channel shall be at either the basic (16-kbps) or the primary (64-kbps) rates. The D-channel rates are only applicable for the FRM-Case B.

5.6.4.3 Format. The FRM frame format shall be as depicted in figure 5.12 and defined in ANSI T1.618. The fields identified in the figure are described as follows:

Flag:	Each frame contains a beginning and closing HDLC flag. The flags are used to indicate the beginning and end of a negotiated packet of user information.
Address:	The address field is used to support routing and network status (e.g., congestion) control information.
Control:	The FRM does not employ the HDLC control field.
Information:	The information field shall support the transport of a defined amount of user information. The default information field size is 262 octets (chosen to be compatible with LAPD on the D-channel). The minimum frame relay information field size is one octet. The support by networks of a negotiated maximum value of at least 1600 octets is recommended for applications such as LAN interconnect, to minimize the need for segmentation and reassembly by the user equipment.
Frame check sequence:	The frame check sequence (FCS) is used to provide error-checking. The FCS is defined to be a 16-bit sequence.

5.6.4.4 Management. The FRM provides no intrinsic network management capability. Thus, the FRM shall be managed as a layer 1 and layer 2 service in accordance with relevant portions of 5.7.

5.6.4.5 Interworking. The FRM shall support interworking between tactical-local network and strategic-local networks. Interworking via the FRM shall support LAN-to-LAN, and terminal-to-terminal interconnections. (Where feasible, the FRM may also

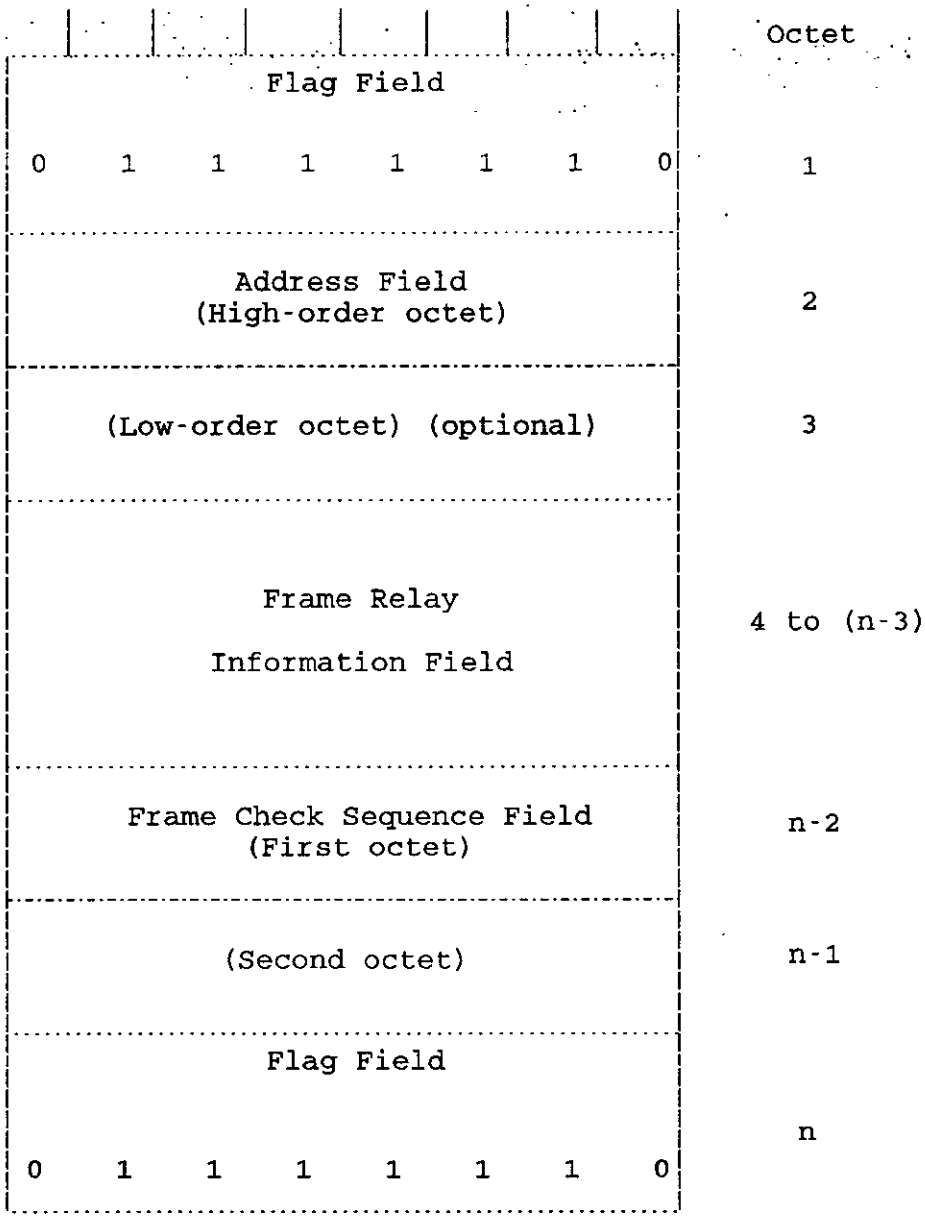


FIGURE 5.12. Frame format for frame relay mode.

take advantage of broadband transport services to traverse non-FRM network segments.)

5.7 Network management. To maintain a coherent and stable network, each segment of the DIS shall support a local network management function as indicated in figure 5.13. The Telecommunications Management Network (TMN) architecture, as defined in CCITT M.30, shall be used as the basis for a common network management framework within the DIS. The TMN shall provide a framework for management of both signaling and user network resources. The TMN framework shall support management information exchanges between peer and subordinate network management entities. Within individual TMN elements (e.g., NEs), the OSI system management framework shall be used. Part 18 of NIST Special Publication 500-183 provides stable implementation agreement to enable independent vendors to supply customers with a diverse set of networking products that can be managed as part of an integrated environment.

5.7.1 Network management objective. Network management entities (DIS systems supporting network management) shall make maximum use of integrated and automatic management aids to facilitate effective and responsive support of the Specific Management Applications Functions (SMAFs). Network management as defined in this standard does not attempt to establish bounds on or restrict implementation of any aspect of DIS network management, but rather to define its minimum required degree of interoperability. When applicable, MIL-STD-2045-38000 shall define the DIS network management within a DoD facility.

5.7.2 Network management infrastructure. The network management infrastructure shall consist of the network management architecture, network administration, and management communications.

5.7.2.1 Architecture. The TMN shall support the establishment of a common and coherent framework for network management. Network management as exercised via the TMN architecture shall not inhibit the establishment of a centralized, distributed-hierarchical or distributed-peer management (sub)architecture or any combination thereof within a DIS element. To support either a centralized or distributed DIS management objective, a virtual network management strategy shall be adopted. Virtual network management shall imply the use of a common framework (architecture and services) for the management of all resources within all elements of the DIS. The virtual network management approach shall in no way restrict achievement of the overall DIS network management objective stated in 5.7.1. The DIS TMN architecture shall support network management within a DoD facility as defined in MIL-STD-2045-38000 and shown in figure 5.14.

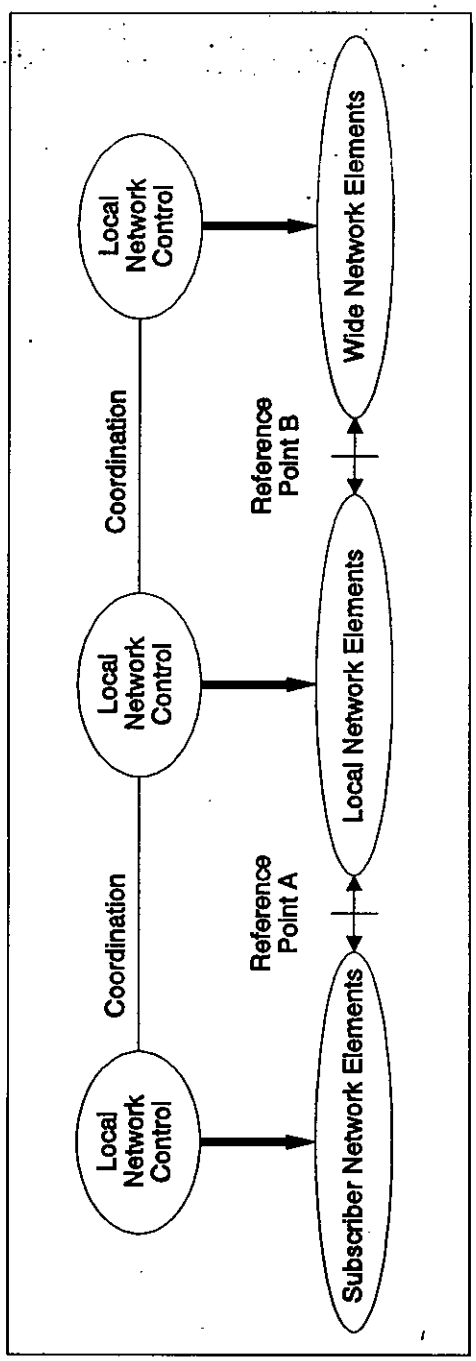


FIGURE 5.13. Overview of the DIS network management scenario.

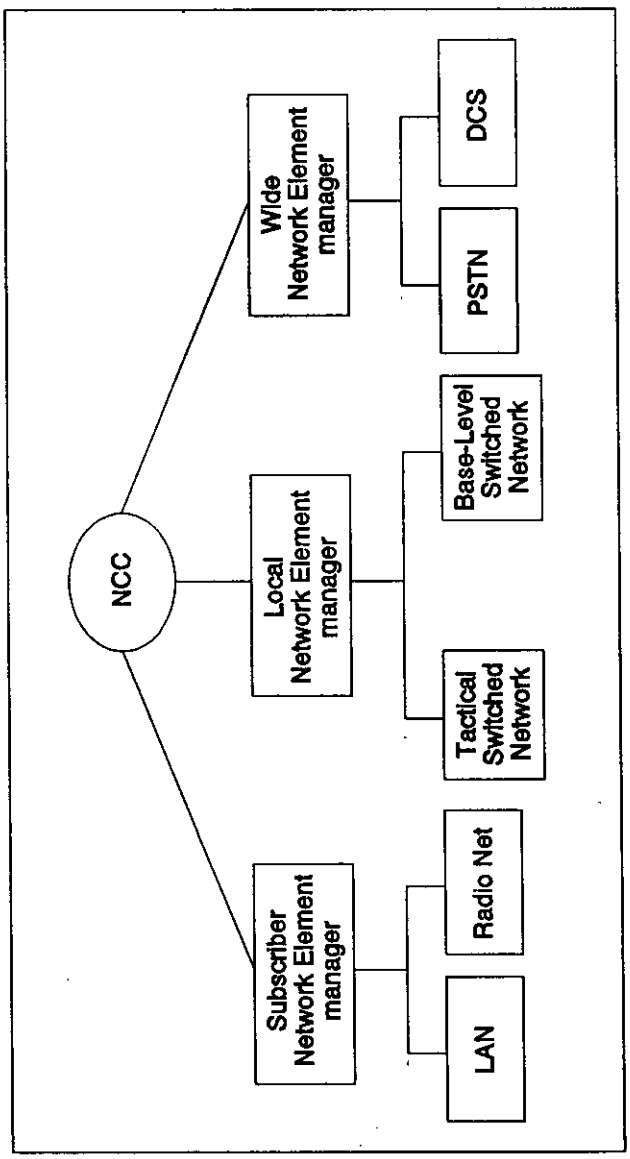


FIGURE 5.14. Typical intrabase distributed-hierarchial network management architecture.

TMNs shall support internetworking across the DIS to provide end-to-end network (and path) management. A TMN associated with a specific DIS element may employ a subset of the typical TMN architecture. (That is, differences may exist between TMN network topologies. This difference may translate into a variance in the type and number of equipment used in TMN. Employment of a TMN subarchitecture shall not imply a reduction in the degree of management functional control.)

A TMN shall have an Operating System (OS) function to exercise control of manageable resources within its domain. A TMN's domain may extend across an entire DIS network or some portion thereof. The OS shall also support an external management interface for authorized remote access and control. The OS shall interface to the backbone (or subnetwork) Data Communications Network (DCN) for the exchange of management information between other peer or subordinate TMNs. A workstation function shall provide a local administration interface to the TMN. A notional TMN is shown in figure 5.15. Local management within TMN elements shall be in accordance with MIL-STD-2045-38000.

5.7.2.2 Administration. The administration architecture (i.e., operational control) within the DIS, in accordance with DoD policy, shall conform to the distributed-hierarchical management structure. Subadministrations shall be designated by the DIS administrator to support network operations at lower echelons. All primary network element (NE) nodes (e.g., switch) designated by the DIS administrator shall have a network administration function. The subadministrator shall be responsible for executing network management functions within a management domain. All administrators shall perform their management functions through the employment of the common network management infrastructure and a set of uniform management services.

5.7.2.3 Communications. Although the TMN is logically a separate network from the user and signaling traffic networks, which its manages, it shall be capable of using these networks to support its communications requirements. Provisions shall be made to support management communications between two or more principal (sub)networks of a DIS element. A principal (sub)network shall contain a network management entity. A point-to-point circuit shall be available to link a DIS segment consisting of two (sub)networks. An omnibus circuit shall be available to link tandem (sub)networks. The management circuits shall provide an ability for network administration and/or manager processes to exchange management information in accordance with ISO DIS 9595 and ISO DIS 9596.

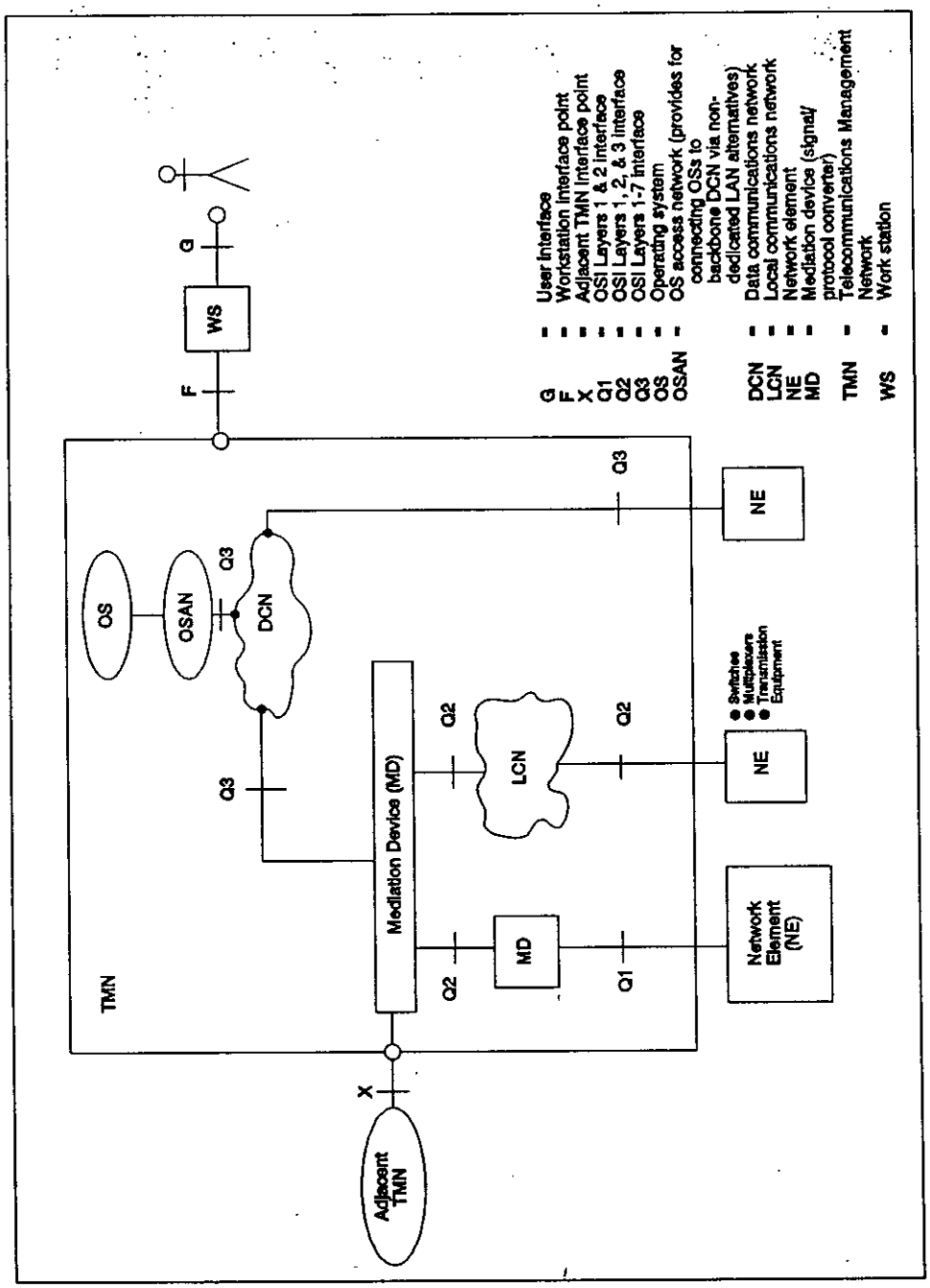


FIGURE 5-15. Notional TMN architecture.

5.7.3 Network management requirements. The following network management requirements as defined in ISO DIS 10165-2 shall support the establishment, (re)configuration, and maintenance of a stable signaling and user network environment. The network management entities shall be supported by SMAFs, which are defined in 5.7.3.1 through 5.7.3.5.

5.7.3.1 Fault management. Fault management, in accordance with CCITT M.20, M.30, and M.36, shall allow for detection, isolation, and correction of abnormal (i.e., unplanned) operation of the telecommunications network. A TMN elements maintenance service provider (MSP) shall not disturb any other domain when attempting to localize a fault. To accomplish the fault management objective, the following functions shall be supported:

a. Alarm surveillance

- A TMN shall provide the capability to monitor NE failures in near-real-time.
- Spontaneous error reporting.
- Error threshold alarm reporting.
- Continuous monitoring.

b. Fault localization

- Trouble isolation.
- Fault tracing.
- Supplementary fault isolation shall be provided when initial failure information is insufficient for fault localization. Internal and/or external test assets shall be controllable by a TMN. Remote control via local management process shall be sufficient.

c. Testing (requested, on-demand, routine scheduled)

- Diagnostic testing.
- Confidence testing.

d. Resource management

- Maintenance functions (corrects isolated faults and maintains operating conditions)

- Resource (re)initialization
- Resource identification.

An appropriate set of fault management procedures and objects shall be defined to enable effective and responsive fault management. Where necessary, the fault management function shall interact with other SMAFs to accomplish its management function.

5.7.3.2 Configuration management. Configuration management shall support functions necessary for exercising control over, identifying, collecting data from, and providing data to NEs. To accomplish these objectives, configuration management shall provide the following:

a. Provisioning function:

- The provisioning function shall provide for the ability to control/activate equipment into service (not including installation). The TMN administration shall initiate the service status of equipment (in service, out-of-service, stand-by, reserved) and selected parameters.

b. Status and control functions:

- The TMN administration shall have the ability to monitor and control certain NE attributes on demand (i.e., checking/changing service state; initiating/terminating diagnostics; and rearranging equipment or rerouting traffic in response to faulty NE equipment). Ability to assess impact of a potential NE's configuration prior to activating that configuration.

c. Installation function:

- The TMN shall support installation of equipment and/or channels into an active network.

An appropriate set of configuration management procedures and objects shall be defined to enable effective and responsive configuration management. Where necessary, the configuration management function shall interact with other SMAFs to accomplish its management function.

5.7.3.3 Performance management. To execute performance management as defined in CCITT M.20 and M.30, functions shall be provided to evaluate and report on the behavior of network elements and their effectiveness in meeting desired performance

objectives. Performance management shall pertain to the following functions:

a. Performance Monitoring:

- Collecting and reporting of traffic data trends in traffic load, bandwidth utilization, and response time.
- Reporting end-to-end circuit trends
- Detection of:
  - -- Loss of frame sync
  - -- Loss of signal
  - -- Alarm indication signal
  - -- Alarm information to the remote end
  - -- Slips
  - -- Restoration indication signal
- Bit error indicators:
  - -- Code violations
  - -- FCRC errors
  - -- Frame alignment signal errors
  - -- Block parity errors
  - -- Errored seconds
  - -- Severely errored seconds
  - -- Degraded minutes
- Loss of signal energy
- Applying controls:
  - -- Congestion
  - -- Exceeding Allocation

b. Traffic management functions:

- A TMN collects traffic statistics data from NEs to reconfigure the telecommunications network or modify operations in response to extraordinary traffic conditions.
- The TMN receives traffic reports (periodically, on demand, or as a result of the NEs exceeding its threshold). The TMN may reset an NE's threshold for generating reports.
- Raw data or summary reports shall be available from an NE upon the TMN administrator's request.

c. Quality-of-service:

- (Same basic items identified for traffic management above.)
- The QOS function shall monitor and record the following parameters:
  - -- Connection establishment (e.g., call setup delays, successful and failed call requests).
  - -- Connection retention.
  - -- Connection quality.
    - --- Historical system state
    - --- Cooperation with fault (or maintenance) management to establish cause of possible failure of resources
    - --- Cooperation with configuration management to adopt routing and load control parameters and limits
    - --- Initiation of test calls to monitor QOS parameters.

An appropriate set of performance management procedures and objects shall be defined to enable effective and responsive performance management. Where necessary, the performance management function shall interact with other SMAFs to accomplish its management function.

5.7.3.4 Security management. Security management shall pertain to the monitoring and control of access to network resources and services. To meet this objective, the following shall apply:

a. Peer entity authentication exchange

b. Access control

c. Connection confidentiality

d. Connectionless confidentiality

e. Selective field confidentiality

f. Traffic flow confidentiality:

- Signaling message protection
- Traffic padding
- Stable routing tables

g. Connection integrity (with or without recovery)

h. Selective field connection integrity

i. Connectionless integrity

j. Selective field connectionless integrity

k. Nonrepudiation (origin or delivery):

- Digital signature
- Data origin authentication
- Notorization

l. Data integrity

An appropriate set of security management procedures and objects shall be defined to enable effective and responsive security management. Where necessary, the security management function shall interact with other SMAFs to accomplish its management function.

5.7.3.5 Account management. Account management shall pertain to resource utilization and audit tracing. The network management process shall be capable of performing all functions necessary to

meet these account management objectives. To meet the objective, the management process shall provide as a minimum the following:

a. Traffic summary

b. Resource utilization statistics

c. Circuit status

d. Billing

An appropriate set of account management procedures and objects shall be defined to enable effective and responsive account management. Where necessary, the account management function shall interact with other SMAFs to accomplish its management function.

5.7.4 Managed objects. All system management entities within a DIS network element's TMN domain shall maintain a set of manageable objects. An object is an abstract means of referencing controllable (manual or automatic) physical and logical equipment and their related signaling, management, and user services within the DIS. Resources within a management domain having control, status, and test points and services shall organize their subordinate objects in a containment hierarchy. The object's containment hierarchy shall define the internal relationship of objects within the management information base (MIB). Managed objects shall have a defined association within and between SMAFs (see 5.7.3).

5.7.4.1 Management information base. The MIB shall contain common standard definitions of all manageable objects within a control domain. Where appropriate, the MIB shall contain locally and globally (intermediate gateways and other DIS elements) significant object definitions. Provisions shall be made to allow specific DIS element specific extensions to the common MIB.

5.7.4.2 Object definition. All objects defined within the MIB shall be defined using the techniques and templates specified in the FIPS XXX, the section titled *Guidelines for the Definition of Management Objectives* and further constrained by NIST Special Publication 500-183 (Part 18, clause 7). All managed objects must have registered object identifiers. In accordance with ISO DIS 10165-1/2/4, the structural definition of an object shall include:

a. Object Name Identifier (in terms of the ASN.1 notional language)

b. Syntax (i.e., type of object: numeric, global, threshold)

c. Access (i.e., read-only, read-write, write-only, not accessible)

d. Status (i.e., mandatory, optional, obsolete)

e. Description (textual description of the object)

f. State (service availability to which object refers)

g. Schedule (time-driven actions)

A DIS element may also require locally unique intraelement objects. These objects shall be defined in a partitioned extension of the MIB. Due to the potential, unique characteristics of a particular DIS element, the defined set of objects associated with a DIS element shall be called "native" elements.

5.7.4.3 Interworking objects. The DIS stipulates that interworking is a requirement. Thus, where necessary, a set of objects shall be defined for the management and control of internetworking across heterogeneous DIS elements. A class of manageable objects shall be reserved for coordinating between TMNs. Internetworking shall have minimal impact on signaling traffic, user traffic, and their services.

5.7.5 Security considerations. Network management via security features associated with the SMAFs shall provide the necessary level of security for all DIS network management objects.

5.7.5.1 SMAF execution. Strict security provisions shall be defined and designed into the network infrastructure at the administrator, manager, agent, and object levels to control unauthorized access to and operation of SMAFs associated with each DIS TMN. Security consideration of the user information flow shall be taken into consideration when gaining or allowing access to manageable user traffic objects.

5.7.5.2 Access to managed objects. The network management function shall gain access to a managed object via its management protocol. The management protocol shall interrogate the object's agent to provide physical access to the object. Examination of an object shall be consistent with the level of control and security possessed by the requesting administration's management function. Where authorization exists, the object's descriptive attributes may be modified by the network management function.

Attempts to access to undefined objects shall not create an unpredictable response from a network agent.

5.8 Performance standards. Terminal-to-terminal performance standards, applied to hypothetical reference circuits (HRC), are included in this standard to provide system designers and planners with a consistent basis for establishing system parameters.

5.8.1 Hypothetical reference circuits. An HRC has a specified configuration and length. It is based on such factors as communications requirements, user satisfaction, equipment performance, installation and operation procedures, and experience. Reference circuit configurations, such as the number of links, trunks, and nodes in tandem with associated transmission equipment, are chosen so that each configuration can be considered representative of a typical network or subsystem operational circuit. The nominal length of a reference circuit normally represents the probable maximum distance over which communications are required in the network or subsystem under consideration.

An HRC is used (a) as a reference for the performance of planned or operational circuits; (b) as guidance for planning and engineering circuits and networks; (c) as a means of prorating and allocating transmission parameters to different portions of a circuit and associated equipment; and (d) as a basis to derive interface, subsystem, and equipment standards.

Normally, in an operational communications system, various circuits with different lengths and parameters from the HRCs must be employed. It is not practical to standardize the performance of every link or circuit that may have to be engineered and installed. The purpose of standardizing performance on an end-to-end basis (and defining HRCs) is to ensure that actual links, trunks, and circuits will perform satisfactorily as parts of an overall subsystem or system.

Designers and circuit engineers are expected to make their own assumptions and decide on such factors as length of radio links; channel perturbations, such as noise and jitter; number of PCM, ADPCM, and CVSD tandem links; number of A/D conversions; and delay characteristics to optimize circuit performance.

5.8.2 Hypothetical reference connections. The HRCs described in 5.8.2.1 and 5.8.2.2 can also be viewed as hypothetical reference connections (HRX) for circuit-switched calls or packet-switched calls. End-to-end performance parameters given in 5.8.2.2 and 5.8.3 apply only to circuit-switched calls. End-to-end

performance parameters for packet-switched calls are a subject for further study.

5.8.2.1 Wide-network segments. The segments that constitute each HRC are summarized in table IX.

TABLE IX. Reference segments for wide-network segments.

REFERENCE SEGMENT	DESCRIPTION
Tail	Same as 320-km terrestrial segment.
320-km terrestrial segment	Eight line-of-sight (LOS) radio repeater links.
Satellite or transoceanic submarine cable	One satellite link with a 40-km LOS radio link at one end, and a metallic or fiber optic cable connection at the other end.

5.8.2.2 Error-free-second ratio allocation. The error-free-second (EFS) ratio allocation for each segment and the resulting performance for each HRC is provided in table X.

5.8.3 Wide networks. Three HRCs for wide networks exist. They are illustrated in figure 5.16. The parameter selected to characterize error performance in wide networks shall be the EFS ratio for a 64-kbps channel. The terminal-equipment to terminal-equipment performance requirement for the EFS ratio is 0.99 for a circuit traversing each HRC, as shown in figure 5.16.

TABLE X. Error-free-second ratio allocation.

SEGMENT	PER SEGMENT	HRC		
		GLOBAL	OVERSEAS	INTRA-CONTINENTAL
Tail	0.9996	---	---	---
320-km terrestrial segment	0.9995	---	---	---
Satellite or transoceanic cable	0.9997	0.9936 ---	N/A ---	0.9968 ---
HRC	---	0.9916	0.9936	0.9949

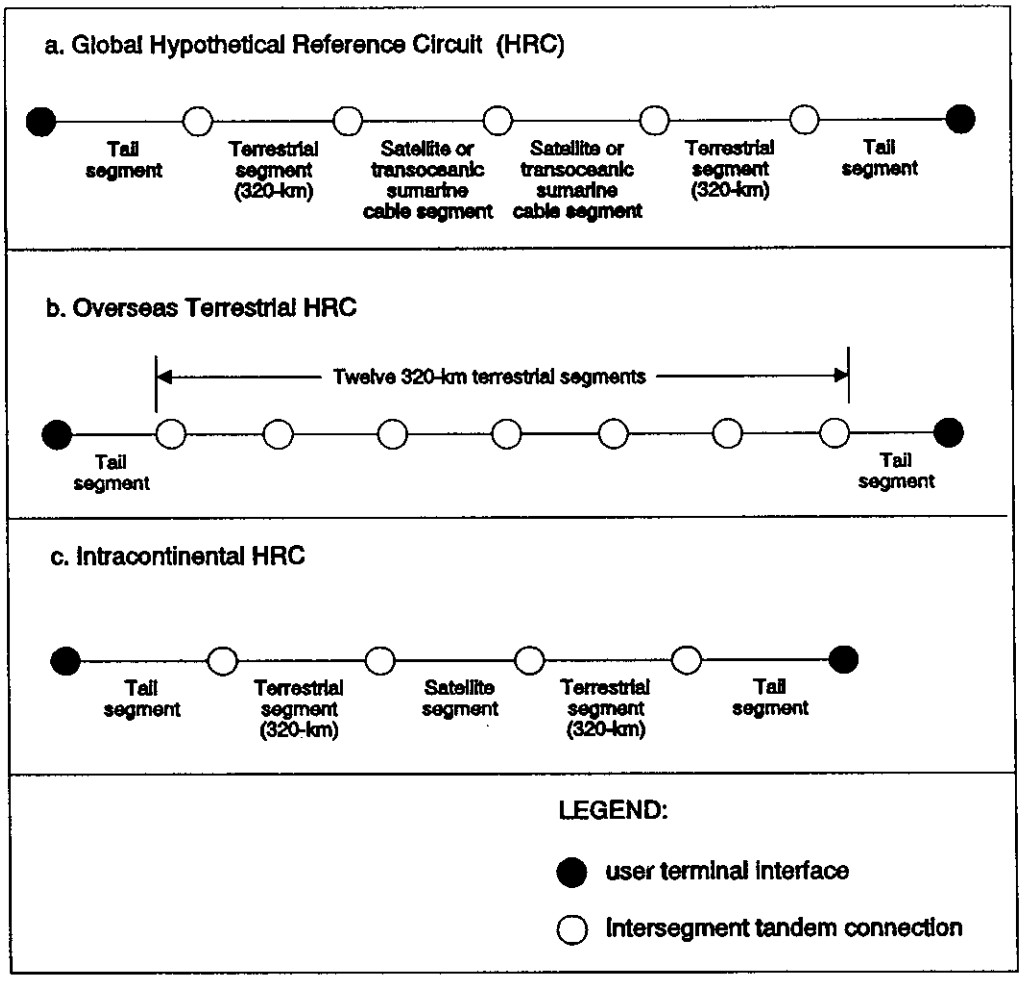


FIGURE 5.16. HRCs for wide networks.

5.8.4 Tactical networks. Three HRCs exist for U.S. tactical circuits:

a. The first HRC, shown in figure 5.17, consists of six internodal line-of-sight (LOS) radio links in tandem. Each internodal LOS radio has a nominal distance of 50 km with an 8-km down-the-hill (DTH) millimeter wave or cable link on each end.

b. The second HRC, shown in figure 5.18, consists of one internodal troposcatter link covering a transmission distance of 200 km in tandem with two internodal LOS radio links of 50 km each. Each troposcatter and LOS radio link has an 8-km DTH millimeter wave radio or cable link on each end.

c. The third HRC, shown in figure 5.19, consists of two tactical subnetworks interconnected by wide network elements, as provided by the DCS or public switched telephone networks (PSTN). In this case the information transmits up to 12 LOS radio links and 24 DTH links.

The contribution to the overall circuit error ratio allocated to tactical network elements is provided in table XI.

TABLE XI. Operational bit error ratios for HRCs that use tactical network elements.

TYPE OF SECTION	CONTRIBUTION PER CIRCUIT	
	BIT ERROR RATIO (BER)	% OF ANY MINUTE
LOS radio	1×10^{-4}	99.0
Tropo radio	4×10^{-4}	99.0
DTH radio	1×10^{-5}	99.0
DTH coaxial cable	1×10^{-6}	99.9
DTH fiber optic cable	1×10^{-8}	99.9

NOTE: The operational error rates are transmission errors and do not include effects of error correction or encryption devices.

5.8.5 Subscriber networks. Subscriber terminal equipment is connected to the local base-level or tactical network via subscriber network elements. Four HRCs applicable to subscriber networks exist. The first two are applicable to both strategic and tactical subscribers. The third and fourth are applicable to tactical subscribers only.

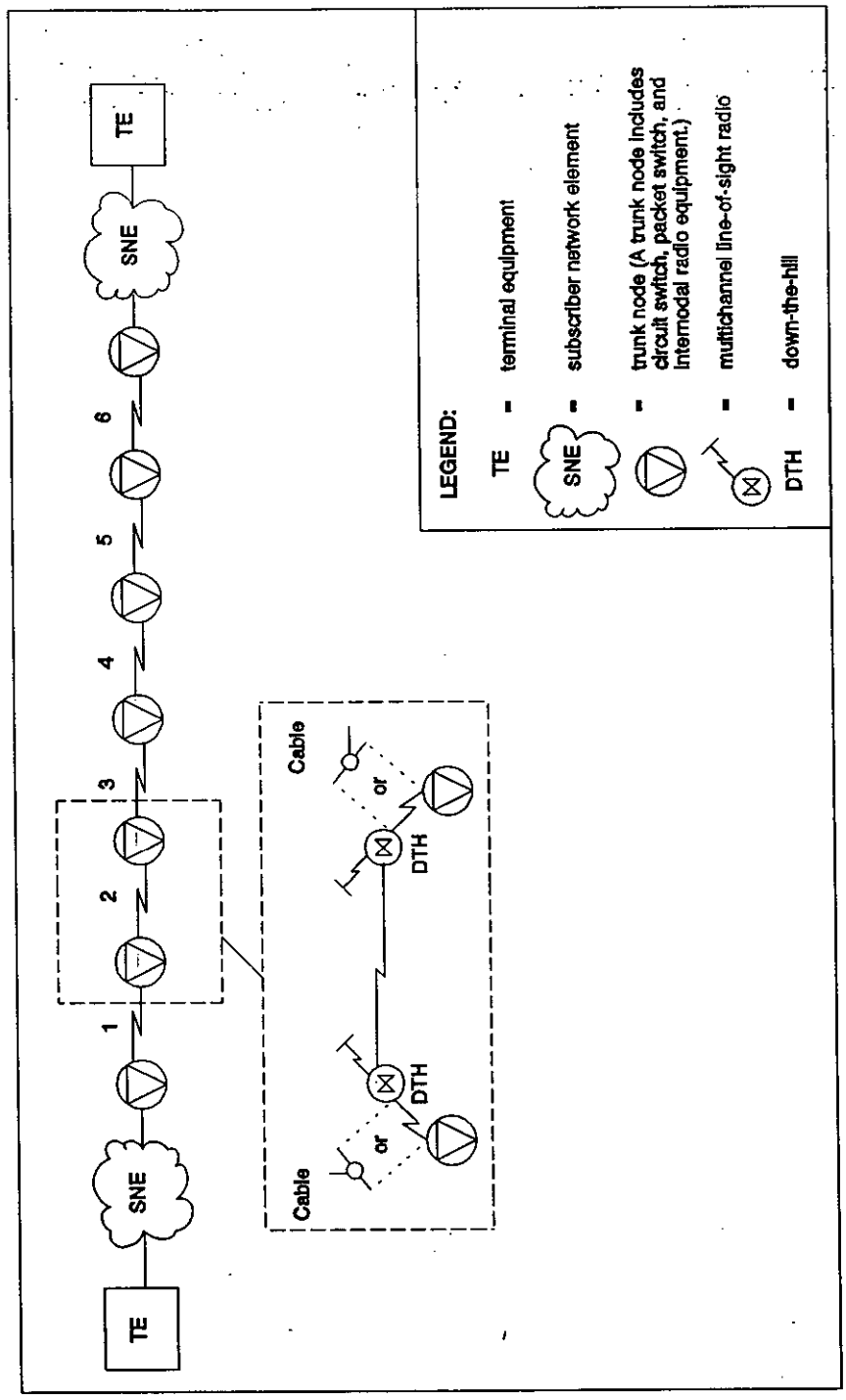


FIGURE 5.17. HRC for tactical networks based on LOS and tropo radio links.

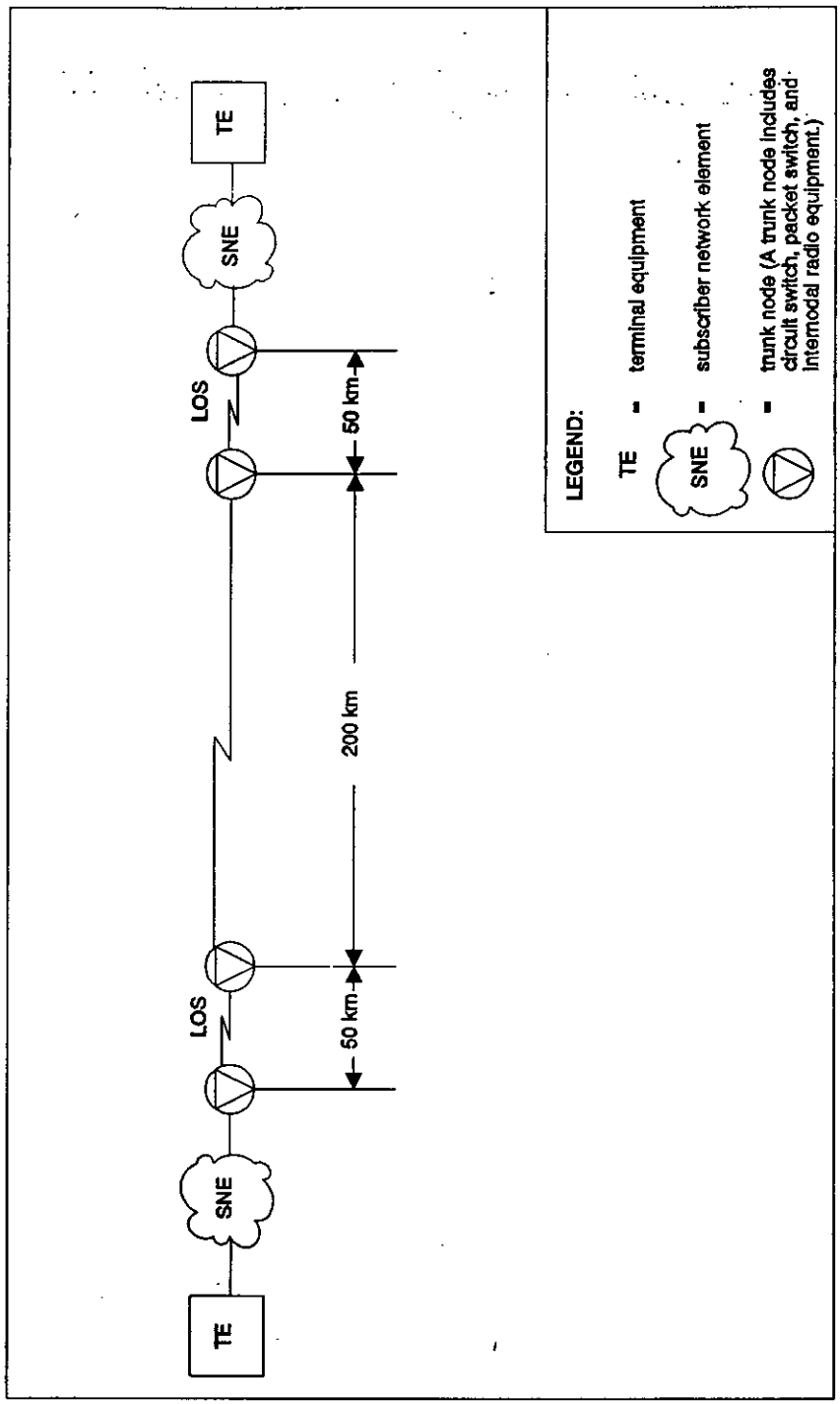


FIGURE 5.18. HRC for tactical networks based on LOS radio links.

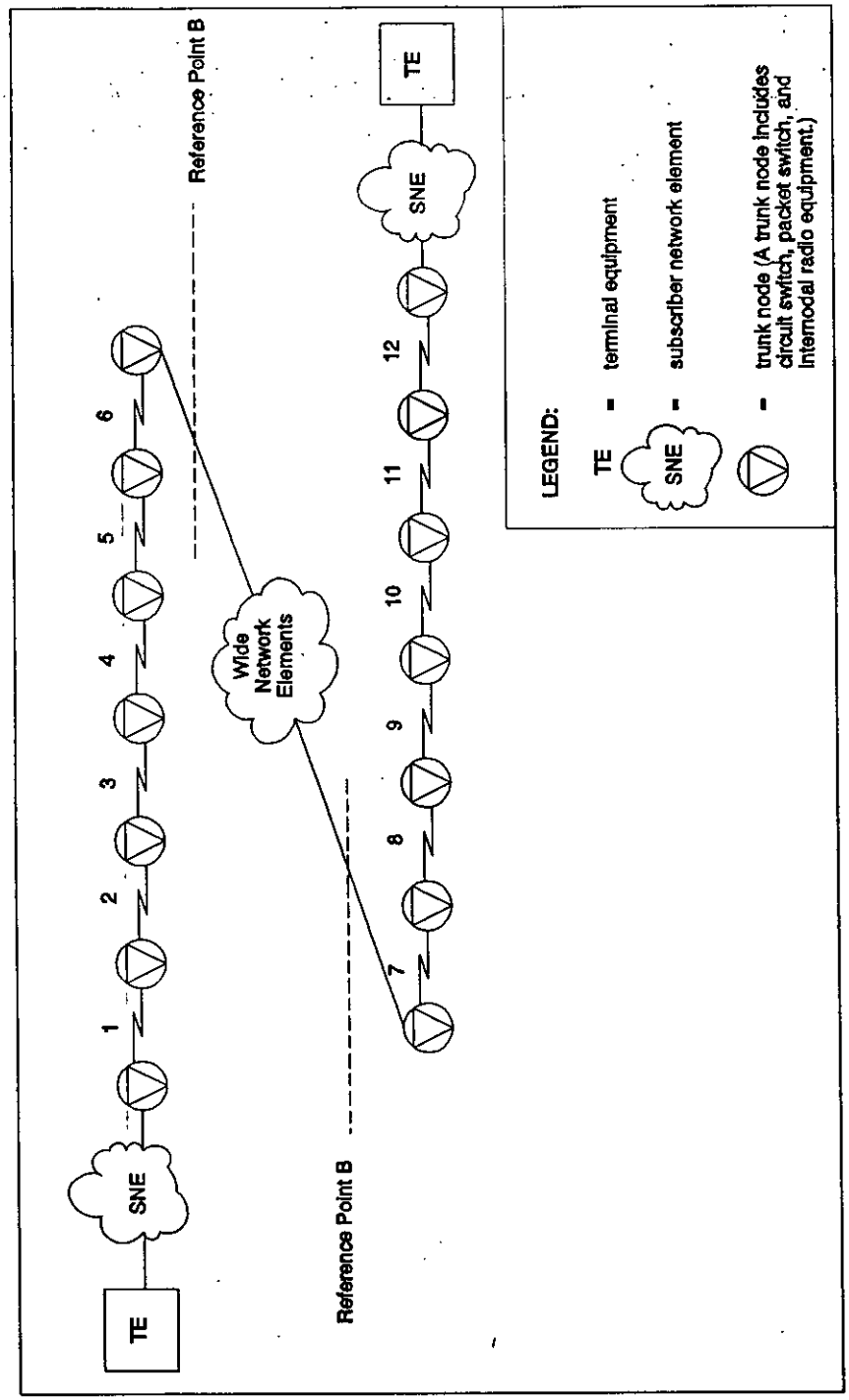


FIGURE 5.19. HRC for tactical networks interconnected by wide-network elements.

a. A direct metallic cable connection between the subscriber's terminal equipment and the local circuit or packet switch. The cable may be up to 4 km long.

b. A LAN complying with LAN standards ISO 8802.3, 8802:4, or 8802.5.

c. A radio network made of combat net radios.

d. A mobile subscriber radio terminal.

The contributions to the overall circuit bit error ratio (BER) allocated to subscriber network elements is provided in table XII.

TABLE XII. Operational error rates for HRCs that use subscriber network elements.

TYPE OF SECTION	CONTRIBUTION PER CIRCUIT	
	BIT ERROR RATIO (BER)	% OF ANY MINUTE
Metallic cable connection	1×10^{-6}	99.9
Local area network	TBD	TBD
Radio network	4×10^{-3}	95.0
Mobile subscriber radio terminal	TBD	TBD
DTH fiber optic cable	1×10^{-8}	99.9

5.9 Numbering plans. A standard numbering plan format shall be employed on all trunks that cross-reference point B. This includes all joint and international circuit- and packet-switched trunks.

5.9.1 Circuit-switched trunks. Telephone numbers, as they appear on joint circuit-switched trunk interfaces, shall consist of a three-digit area code and a seven-digit subscriber number unique to each area code. Telephone numbers for international calls shall consist of an international access prefix (IAP), in addition to the area code and the subscriber number.

5.9.1.1 International access prefix. The IAP for calls between U.S.-tactical subscribers and NATO-tactical subscribers, reference point B (NATO), shall comply with STANAG 4214 and its description of the nationality identifier (NI). The NI is of the form 9CC, where CC is a two-digit country code. The IAP for

calls between U. S.-strategic subscribers and strategic subscribers of other nations shall comply with CCITT Recommendations E.163 and E.164.

5.9.1.2 Area codes. The area codes for calls between U.S.-tactical subscribers and NATO-tactical subscribers shall comply with STANAG 4214 and shall be of the form NCC, where N=0, 1, ..., 8 and CC is the two-digit country code. Area codes for calls between U.S.-joint tactical networks shall comply with the Joint Pub 6-05 chapter titled *New Integrated Tactical Numbering Plan*. Area codes for base-level and wide-network elements shall comply with DCAC 370-175-13, the section titled *DSN Worldwide Numbering and Dialing Plan*.

5.9.1.3 Subscriber telephone numbers. The standard telephone number, as it appears at joint and combined trunk interfaces, shall have seven digits. The seven digits may consist of two subcomponents: a unique switch code for each area code, and a unique subscriber number for each switch code. Systems, which employ deducible directories, automatic subscriber affiliation, and flood-search routing shall use all seven digits as the unique subscriber number.

5.9.2 Packet-switched trunks. The address of the called terminal shall be provided in the call request packet in accordance with CCITT Recommendation X.31. As an objective, DoD will evolve toward an integrated addressing plan applicable to both circuit-switched and packet-switched trunking. In the interim, packet-switched network elements shall comply with standards adopted for use by DDN.

5.9.3 Digit capacity for international systems. The number length for international calls may be increased to accommodate future network requirements (see CCITT Recommendations E.163, the section titled *Digit capacity of international registers*, and E.164, the section titled *Number length*). The digit capacity of registers required to process international calls should provide a minimum capacity of 15 digits. This digit capacity does not include all digits dialed by telephone subscribers, such as access and priority digits.

5.9.4 Subaddressing (network address extension). The seven-digit subscriber number shall identify connections at reference point A. Additional subaddressing required to identify subscriber-to-network terminations or service access points shall be transparent to the local- and wide-network elements. For base-level subscribers, up to 40 digits may follow the subscriber number, as illustrated in CCITT Recommendation E.164, the section titled *Address information*. Subaddressing for tactical subscribers is a subject for further study.

MANDATORY APPENDIX A

CONVERSION BETWEEN THE TCP AND ISO TRANSPORT PROTOCOLS AS A METHOD OF ACHIEVING INTEROPERABILITY BETWEEN DATA COMMUNICATIONS SYSTEMS

(Reprinted, with permission, from *IEEE Journal on Selected Areas in Communications*, Vol. SAC-4, No. 2, pages 288-296, March 1986.)

Scope. This appendix describes the TCP-to-ISO protocol conversion capability that is needed at reference point B (NATO). This capability is needed because the U.S. end systems and networks will use data communications protocols based on TCP/IP for a period of time after the ISO transport protocol is implemented in NATO.

Conversion Between the TCP and ISO Transport Protocols as a Method of Achieving Interoperability Between Data Communications Systems

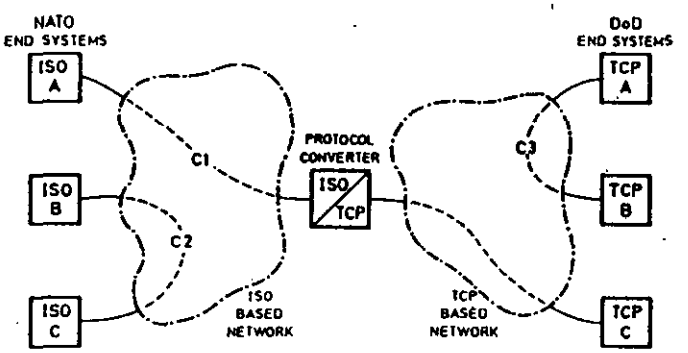
INGE GROENBAEK

Abstract—A solution to the lack of interoperability between the U.S. Department of Defense (DoD) data communications standards and the NATO standards based on the International Organization for Standardization concept for open systems interconnection is presented. The solution is based on conversion between a common subset of the US DoD Transmission Control Protocol and the ISO Class 4 Transport Protocol at the Transport layer, which is the first layer offering any end-to-end service.

I. Introduction

In December 1978, the U.S. Department of Defense (DoD) recognized the Transmission Control Protocol (TCP) [1] and the Internet Protocol (IP) [2] as official DoD standards satisfying the requirements of the U.S. military in respect to security, survivability, and reliability. These factors were considered to be so pressing that they justified the adoption of the TCP and IP until such time as comparable commercial standards would be available. However, the main substance of the TCP and the IP has not changed since their adoption in 1978, and they have now been in use in military and civilian applications (DoD and ARPANET) for several years.

The TCP standard corresponds roughly to the ISO Class 4 Transport Protocol, and the ISO Transport Protocol Specification [3] was accepted as a Draft International Standard in 1984. In the years to come, the ISO Class 4 Transport Protocol is expected to become the most popular Layer-4 protocol both for military and civilian systems, and so the need for the growing ISO community to interoperate with the existing TCP community will steadily increase. This applies to the need for interoperability between the U.S. and the rest of NATO, as well as to the general problem of interoperability between existing TCP systems and emerging ISO protocol systems. The availability of a conversion facility between TCP and the ISO Class 4 Transport Protocol would allow such interoperation, and would let the traditional TCP community transit to the ISO protocols in future systems without losing the possibility of interoperating with existing TCP-based systems.



C1: The ISO A and TCP C end-systems interoperate through a restricted common service with protocol conversion.

C2: The ISO B and ISO C end-systems interoperate through the full or restricted ISO service.

C3: The TCP A and TCP B end-systems interoperate through the full or restricted TCP service

Fig. 1. Modes of interworking.

This paper compares the service provided by TCP to the service provided by the ISO protocols, and sketches a conversion procedure which retains the end-to-end significance of the protocols. The similarity of the two transport protocols makes it possible to achieve this with only minor restrictions to the service supported. The common service subset, which can be supported by both ends through conversion was derived in [4], and the conversion algorithm is specified in [5].

The common subset for which conversion takes place includes the ISO Session Orderly Release, and appears sufficiently powerful for all military and civilian applications. Fig. 1 illustrates the three modes of interworking, while Fig. 2 models the converter in the context of the OSI basic reference model [6].

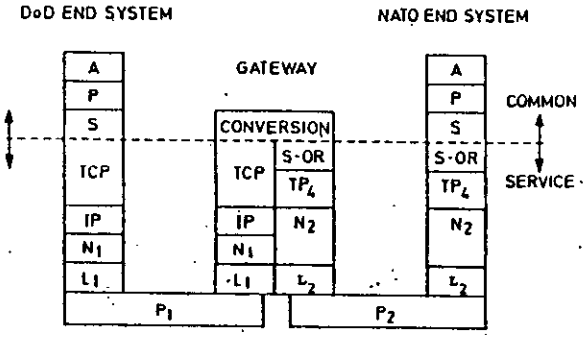
Use of the restricted common service subset for intranetwork communication (see Fig. 1, connections C2 and C3) would simplify internetwork communication, since the identical service would be applied for both purposes.

Manuscript received August 6, 1984; revised March 1, 1985. This work was supported by NATO and performed at SHAPE Technical Centre, 2501 CD The Hague, The Netherlands.

The author is with Siemens, Oslo 5, Norway.

IEEE Log Number 8406020.

0733-8716/86/0300-0288$01.00



A: Application layer protocols (common to all communicating end systems)

P: Presentation layer protocol (common to all communicating end systems)

S: ISO Session sub-layer protocol excluding Orderly Release (common to all communicating end-systems)

S-OR: ISO Session Orderly Release sub-layer

TP4: ISO Class 4 Transport Protocol

TCP: DoD Transmission Control Protocol

IP: DoD Internet Protocol

N_1: DoD subnetwork protocol

N_2: ISO Network layer (possibly including the Internet sub-layer)

L1: DoD Link layer (In many configurations there is no need for a Link layer protocol)

L2: ISO Link layer

P1: DoD Physical layer

P2: ISO Physical layer

Fig. 2. Interoperation model.

Interoperability over the subnetwork boundaries is not required in Layers 1–3 (inclusive) of the OSI model. This is because these layers mainly deal with node-to-node and intranetwork functions. The main exception to this is the global addressing which functionally belongs to the Internet sublayer of the Network layer.

The implementation of the Internet sublayer is not generally mandatory (although it is a requirement in the U.S. DoD environment), but an Internet address has to be carried across the different subnetworks, either by the Network layer or by the Transport layer. The flexibility that this affords each individual subnetwork in regard to choice of protocol for Layers 1, 2, and 3 opens the way to interoperation in an environment of heterogeneous subnetworks. This will allow technological evolution towards subnetworking optimized for specific applications, and for interconnection of existing diverse networks.

II. Interoperability Strategy

Any solution to the interoperability problem has to allow for easy migration towards deployment of ISO standards for all future communication systems. At the same time it has to comply with military standards, which means that it must involve no more than minimum additions to existing DoD systems.

To achieve host-level interoperability, it is necessary to have the same protocol functionality whether it is implemented with the ISO or any other protocols, from the application level down to the level where a conversion or gateway occurs. In the DoD system this level is below the Internet Protocol, and the Internet Protocol provides the common gateway function. For two DoD hosts to communicate, therefore, it is necessary for them to provide compatible protocol functionality from the Internet layer through the Application layer.

Initially it may be impossible, for practical reasons which will be explained, to have the same protocols in all layers above the Network level for every host in a system. The optimum short-term solution to the lack of interoperability imposed by this may seem to be conversion of all of the protocol layers. This would facilitate interoperation through a converter (possibly in a gateway). However the higher protocol layers (i.e., those above the Transport layer) are so diverse that an all-embracing protocol conversion which retains the defined end-to-end conditions for every layer is not feasible. For example, it does not seem possible to convert between the DoD File Transfer Protocol and the ISO File Transfer and Manipulation Protocol.

A store-and-forward unit, which acts as an intermediate end-system for the Transport, Session, and the Presentation layers, might be able to process all layers, but it would violate the defined end-to-end operating characteristics of the Transport and higher layers. This implies that the store-and-forward unit would have to be given the responsibility for delivery of data to the real end systems. Such an arrangement would not be suitable for certain applications where survivability and delay are critical.

Therefore, we have to revert to a conversion which retains the real end-to-end operation without our intermediate thrusted relay, and this should take place at a layer for which it is possible to establish the defined end-to-end conditions for all subsequent lower layers. The closer the level of conversion can be located to the Application layer, the less the required additions to existing DoD systems will be.

It was previously assumed not possible to implement such a conversion above the Network layer, but the author has developed an algorithm which, through conversion at the Transport layer, maintains end-to-end conditions for a common subset of the services provided by the TCP and the ISO protocols. Common protocols should be used at all layers above the Transport layer for a TCP host in communication with an ISO Transport-based host through the suggested conversion system. Why not then simply use a common Transport layer? The answer is that it is not practical. Many TCP/IP implementations are performed inside the operating system for efficiency. When the ISO Transport protocol becomes widely implemented, it too can be expected to be implemented inside the operating system, or if external, tailored to the specific host involved. On the other hand, most of the implementations of higher level protocols have tended to be performed as application processes. Therefore, if two hosts wish to communicate, it

is relatively easy to implement common protocols above the Transport level and relatively difficult to implement additional Transport protocols beyond those that are in the system already. Therefore, implementing a conversion at the Transport level is eminently practical.

If two or more applications are to be interoperable via a compatible (i.e., identical or translatable) Transport protocol, then their respective set of application-specific functions must be equivalent. It is not essential that the implementations of these functions be based on any specific layering principles or protocols. However, clearly the normal benefits of a layered structure are still relevant, and common higher level protocols would permit the benefits of common design and development and ensure compatibility is maintained in any subsequent updates.

III. Comparison Between the TCP and ISO Transport Service

This comparison is based on a Shape Technical Centre study [4], which employed the OSI basic reference model in a description of the service supported by the TCP. The ISO Transport service is defined in [7]. The comparison is functional and qualitative. Table I gives an overview of the comparison, and the following text discusses the major differences in the services.

A. Connection Establishment

1) Function: The transport service (TS) establishment primitives can be used to set up a transport connection (TC), provided the TS users exist and are known to the TS provider.

a) ISO: Simultaneous T-CONNECT requests (connect collision) at the two transport service access points (TSAP's) are handled independently by the TS provider. Simultaneous T-CONNECT requests typically result in a corresponding number of TC's.

b) TCP: Simultaneous T-CONNECT requests at the two TSAP's result in establishment of one TC. In a TCP TC establishment the initiator of the establishment fully specifies the global identity of the TC wanted (the pair of sockets), while in the ISO TC establishment only the two TSAP's through which the connection is wanted need to be specified. It is up to the correspondent TS users or the correspondent entities to provide for an identification of the connection within the Service Access Points.

2) Called Address: The called address parameter conveys the address of the TSAP to which the TC is to be established. For TCP the internet address plus the port identifier (the remote socket) has to be used.

The TCP port identifier is, in the ISO context, composed of a T-suffix and a TC reference, where the T-suffix identifies the TSAP, and the TC reference identifies the TC within the TSAP.

3) Expedited Data Option

a) ISO: The Expedited Data option parameter indicates whether the Expedited Data option is to be available on the TC.

TABLE I
TCP/ISO Transport Service Comparison

Function/event	ISO	TCP
A. Transport connection (TC) establishment phase		
Connect collision	Two TCs established (one each way)	One TC established for a given pair of sockets*
Addressing	Undefined, but any structure possible	Statically defined address length
Expedited Data Option	Negotiable, according to user needs	Not available (Urgent signal available)
Quality of Service	Loosely defined, multi-functional (implementation-dependent)	Well-defined subset of ISO
TS User-Data	Limited length, conveyed in Connect TPDUs	Not available (when possible, buffered until the TC is established)
B. Data transfer phase		
TS User-Data	TSDU of an integral number of octets (a TSDU itself may be thought of as being an octet stream)	Octet stream which may be divided into TSDUs by the use of the Push function
Urgent Signal	Not available	Out of data-band signal
Expedited Data	Takes precedence over normal data	Not available
Flow control**	Explicit or implicit	Explicit
C. Transport connection release phase		
Orderly Release	Not available in Layer 4***	Available without any User-Data
Abrupt Release	Available with limited amount of User-Data (which could be lost) and Reason indication	Available, possibly with Reason indication

* A socket is an Internet address plus a TCP port identifier.
** Explicit flow control is the flow control performed by the TP; implicit flow control is when the TP relies only on back pressure from the lower layers. (Class 4 provides explicit flow control only)
*** ISO supplies the Orderly Release in the Session layer (Layer 5).
TS Transport Service
TPDU Transport Protocol Data Unit
TSDU Transport Service Data Unit

b) TCP: No Expedited Data option. However, Urgent data can be signaled by the use of the inherent TCP Urgent function.

4) TS User Data

a) ISO: May not exceed 32 octets.

b) TCP: User data are permitted, and the TCP PUSH function could be used to separate TSDU's from each other. Data transferred in the T-CONNECT request are not delivered to the service user before the TCP three-way handshake is regarded as completed by the provider receiving the T-CONNECT request.

B. Data Transfer

1) Normal Data Transfer Service: The TS provider allows for an exchange of transport service data units (TSDU's). (The TCP PUSH function may be used to delimit the character stream into TSDU's.)

2) Expedited Data Transfer Service: The service is full duplex.

a) ISO: The transfer of expedited TSDU's is subject to a different quality of service and separate flow control from those applying to the standard data transfer service.

Expedited data will be delivered when the receiving TS user is not accepting normal data.

b) TCP: No expedited data. However, the data primitive with the Urgent flag set is equivalent to a signal indicating that TCP urgent data has arrived. It is up to the receiving service user to take action to receive the indicated Urgent information. It is not possible for Urgent data to bypass normal data.

C. Connection Release

1) Orderly Release: ISO regards this as being a function belonging to the Session layer, details are contained in the Session service definition, [8]. This service is thus only available in TCP, as the TCP Close service. Release occurs without the loss of data after all in-transit data has been delivered and accepted. The service can be initiated by a service user at any time, regardless of the current TC phase.

2) Abrupt Release: The TC release (TCP Abort/RST) TS primitives are used to release a TC. Release is permitted at any time, regardless of the current TC phase. A request for release cannot be rejected. The Transport Service does not guarantee delivery of any TS user data once the release phase is entered.

The release may be performed:

a) by either or both of the TS users, to release an established TC;

b) by the TS provider, to release an established TC;

c) by either or both of the TS users, to abandon TC establishment;

d) by the TS provider, to indicate its inability to establish a requested TC.

The ISO user-data parameter is employed only when the disconnect is user-initiated. It is not guaranteed that user-data issued in the T-DISCONNECT request by one service user will reach the remote service user.

D. Assessment

1) Connection Establishment Phase: The ISO service is functionally more powerful than the TCP service, since user data are available in the ISO service, and the ISO service can more easily be adapted to meet future needs.

2) Data Transfer Phase: The ISO service is judged to be better than the TCP service because of the availability of expedited data. (The TCP URGENT function cannot itself carry any data.)

3) Connection Release Phase: The two services are judged to be functionally equivalent. This is based on the assumption that the ISO session-level Orderly Release is made available through a sublayer.

IV. Largest Common Service Subset

The Transport Service primitives given in Table II are compatible with TCP although some restrictions exist with respect to the parameters that are conveyed.

TABLE II
COMPATIBLE TRANSPORT SERVICE PRIMITIVES

Phase	Service	Primitive	Parameters
TC establishment	TC establishment	T-CONNECT request	(Called Address, Calling Address,* Quality of Service)**
		T-CONNECT indication	(Called Address, Calling Address, Quality of Service)
		T-CONNECT response	(Quality of Service, Responding Address)
		T-CONNECT confirm	(Quality of Service, Responding Address)
Data transfer	Normal data transfer	T-DATA request	(TS User-Data)***
		T-DATA indication	(TS User-Data)
TC release	Abrupt release	T-DISCONNECT request****	
		T-DISCONNECT indication	(Disconnect Reason)

*: Addresses are limited to fit within the TCP constraints on format and structure. (A mapping could be defined to hide this from the service user.)

**: The number of effective choices for the quality of service is limited to what is available for TCP. (A mapping between TCP and ISO is required).

***: The TCP Push function may be used for Service Data Unit (SDU) separation when more than one SDU is to be transmitted for the duration of the connection.

****: No Reason parameter can be supported by TCP for the request primitive.

To ease rehosting of applications, it is proposed that the ISO Session Orderly Release be included in the common subset, relying on the TCP Orderly Release to enhance the functionality of the subset to a level that appears acceptable for all military and civilian applications, and to allow any special applications, for which it is impracticable to employ the Session and Presentation Services, to obtain access to a much more useful service. (This is especially important during the transition to ISO-defined protocols, because the higher layer becomes available later than the Transport layer.)

The introduction of the Orderly Release in the Transport service constitutes a violation of the ISO TS definition, and in practice would imply duplication of the Orderly Release service, which would have to be implemented in both the Session layer and the Transport layer. Another solution would be to define the level of interoperation between the ISO protocol and the TCP as the level resulting from the addition of the Session Orderly Release service defined in [8] with the protocol given in [9] as a sublayer on top of the Transport layer. Interoperation through this sublayer would obviate the need for duplication of functions. Fig. 2 illustrates the resulting level of interoperation. The Session component of the common service subset (the Orderly Release) is given in Table III. The Orderly Release sublayer may be regarded a component of the Session layer or of the Transport layer. The U.S. National Bureau of Standards (NBS) has chosen to include the Orderly Release in the Transport protocol, which is the preferred solution, considering the complexity involved. It is hoped that ISO can also adopt this solution, and formally define the Orderly Release to belong to the Transport layer. The NBS version

TABLE III
COMPATIBLE SESSION SERVICE PRIMITIVES

Phase	Service	TCP	ISO (Session Service)
Release	Orderly Release	T-CLOSE request	S-RELEASE request
		T-CLOSE indication	S-RELEASE indication
		T-CLOSE response	S-RELEASE response
		T-CLOSE confirm	S-RELEASE confirm

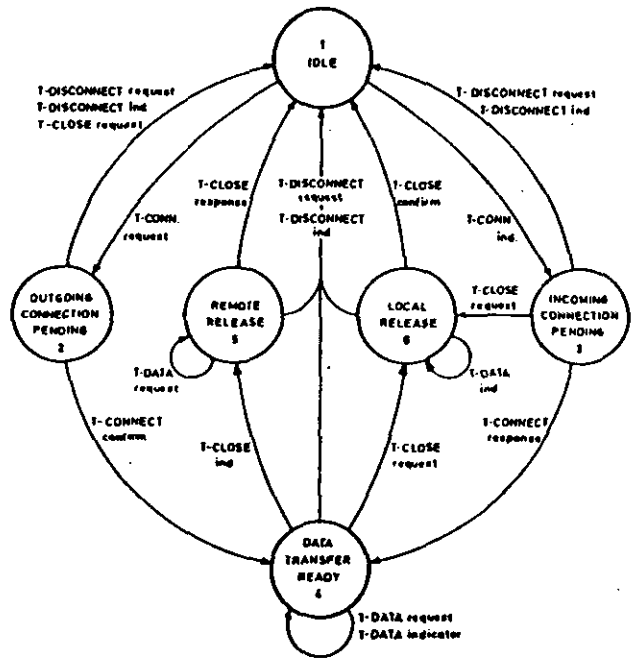
Notes to Table 3

(a) No parameter can be supported by the TCP CLOSE primitives. The Result and User Data parameters of the S-RELEASE primitives are therefore not part of the common subset.

(b) The permissible sequences for activation of the service primitives are described by the state diagram in Figure 3. The diagram specifies the order in which TS primitives shall occur, but does not fully specify the time at which they may occur. Constraints, such as flow control of data, will affect the ability of a TS user or TS provider to issue a TS primitive at any particular time.

of the Class 4 Transport protocol is now a proposed Federal Information Processing Standard (FIPS), and is specified in [10].

The permissible sequences of service primitives are shown in Fig. 3.



a) The Idle state (State 1) reflects the absence of a TC.

b) The Abrupt Release service can be invoked at any point during the TC establishment or data transfer phase.

c) ISO: procedures other than the TC release procedure cannot be initiated within the establishment phase (States 2 and 3).

TCP: in some implementations it is possible to queue invocations of the data transfer service during the establishment phase.

d) Implementation of sequencing procedures and reactions to illegal sequences are not described.

e) Transitions (arrows) labelled by request or response primitives are initiated by the local service user, while indication and confirmation primitives are initiated by the remote service user (the correspondent user).

f) The ISO term T-DISCONNECT is equivalent to the TCP term ABORT.

g) The T-CLOSE is available in TCP and in the ISO Session protocol.

Fig. 3. Permissible sequences of service primitives.

V. THE FUNCTIONALITY OF THE COMMON SERVICE

The following major restrictions apply:

1) No user data can be conveyed during TC establishment;

2) no Expedited data transfer;

(The difficulty in defining a mapping between Expedited and Urgent data is due to the lack in TCP of a mechanism for identification of the Urgent part of the data stream. A simple mapping can be devised under the assumption that the Urgent data extends from the beginning of the TCP segment carrying the Urgent flag (URG). However, the author is not proposing such mapping in this paper, as he has not investigated the validity and implications of the assumption.)

3) no Urgent signal (TCP);

4) no user data can be conveyed during TC Orderly Release;

5) the TCP PUSH function (or a new protocol mechanism) has to be used for TSDU separation.

The implications of these restrictions are as follows.

Restrictions (1) and (4): These have no implications for TCP users, and ISO users may send this data during the ordinary data transfer phase (after TC establishment, before TC release).

Restriction (2): This does not affect TCP users, and neither does it affect ISO users, since the only guarantee given for the ISO Expedited service is that it is no slower than the ordinary data transfer service.

Restriction (3): This is a restriction that may influence some TCP interactive applications. The Urgent function is, for example, used by the TELNET virtual-terminal protocol (DoD/ARPA). There are at least two solutions to this problem. The preferred solution is to substitute the ISO virtual terminal protocol for TELNET as soon as the ISO protocol becomes available. This is a practical solution since the Application layer and higher level protocols are relatively simple to implement in existing systems. The other alternative is to implement the PUSH function explicitly in existing protocols and applications which currently make use of the TCP PUSH function.

Restriction (5): Some of the implementers of TCP have chosen to hide the PUSH parameters from the TCP service user. (Reference [1] recommends user control of the PUSH function.) This means that all implementations with implicit setting of the PUSH flag would have to be modified to comply with the TCP specification before interoperability

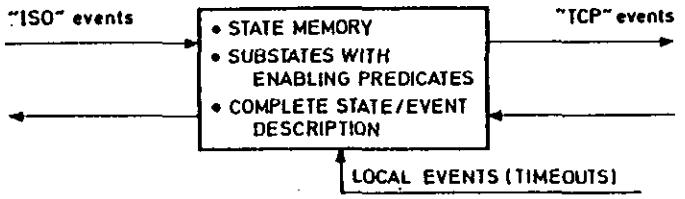


Fig. 4. Specification model.

for the proposed service subset through a protocol converter is possible. A TSDU may be transmitted as a sequence of one or more TCP segment(s), with the PUSH flag (indicating the invocation of the PUSH function and the end of the TSDU) set to zero in all but the last segment. No TCP segment may carry data for multiple TSDU's. (If it turns out to be difficult to get all TCP implementations to comply with this, then it may be necessary to consider introducing a header field in the TCP user data for conveyance of the TSDU delimiter.)

VI. Protocol Conversion

The specification of the conversion algorithm [5] is in the form of an extended finite-state machine (EFSM) with descriptions of transitions and actions for every state/event combination. This includes legal combinations, illegal combinations, and inconsistent combinations. The inconsistent combinations signify errors in the converter hardware or software, while illegal combinations signify protocol errors at the end system(s), or errors in the lower layers. The specification contains a description of 654 state/event combinations, of which approximately 300 are unique. The EFSM description technique that is applied is similar to the technique used in the ISO Transport Protocol specification [2], and is illustrated in Fig. 4.

It was unfortunate that a formal description technique like the ISO ESTELLE [11] was not available, because such a tool with the proper computer-based support systems for validation, implementation, and testing would possibly have been of great help, particularly in the last of the three phases into which the development of the specification was divided:

1) creation of signal-sequence diagrams;

2) generalization of the signal sequences into state diagrams for legal state/event combinations;

3) definition of state/event tables with transitions and actions for all state/event combinations.

The formal method would have been used for Phase 3, or for an additional Phase 4 which would restate and refine the outcome of Phase 3 in a formalized way. This could be the preferred way of working, at least until sufficient experience is gained in the use of formal methods and tools. Reference [12] describes an early protocol development system suitable for such an application.

The following description of the conversion algorithm is based on the definition of the attributes of the EFSM. Table IV defines all incoming events including local events. (The outgoing events are equivalent to the incoming events except those for the network service.) The decision matrix in Table V specifies the algorithm for identification of TCP events and for individual ordering of these events within the segment. Each TCP segment can convey more than one basic event, and the identification of a basic TCP event is state-dependent.

TABLE IV
Incoming Events

Abbreviated name	Category	Name and description
NDISind	NS-provider	N-DISCONNECT indication primitive
NCONind	NS-provider	N-DISCONNECT indication primitive
NCONconf	NS-provider	N-CONNECT confirm primitive
NRSTind	NS-provider	N-RESET indication primitive
CR	TPDU	ISO Connect Request TPDU
CC	TPDU	ISO Connect Confirm TPDU
DR	TPDU	ISO Disconnect Request TPDU
DC	TPDU	ISO Disconnect Confirm TPDU
AK	TPDU	ISO Data Acknowledgment TPDU
EA	TPDU	ISO Expedited Data Acknowledgement TPDU
DT	TPDU	ISO Data TPDU conveying a Session DT SPDU
ED	TPDU	ISO Expedited Data TPDU conveying an expedited SPDU
ER	TPDU	ISO Error TPDU
SYNR	TPDU	TCP SYN Request TPDU
SYNC	TPDU	TCP SYN,ACK
SYNCC	TPDU	TCP SYN, ACK Confirmation
FINR	TPDU	TCP Orderly Release Request
FINC	TPDU	TCP Orderly Release Confirm (ACK)
ACK	TPDU	TCP Data Acknowledgement TPDU
DATA	TPDU	TCP Data TPDU
RST	TPDU	TCP Reset TPDU
FN	SPDU	ISO Release Request (FINISH) embedded in a DT TPDU
DN	SPDU	ISO Release affirmative confirmation (DISCONNECT) embedded in a DT TPDU
I-T	Local	ISO inactivity timer (I) expired (no traffic received from the remote entity)
TS1-T	Local	No response is received to issued CRs (N CRs transmitted)
TS2-T	Local	General timer event used to initiate release of network connections
PROGRESS-T	Local	Timer used to prevent a connection from remaining in a given state indefinitely

TABLE V
Identification of TCP Events

Notation: Y = YES; N = NO; (n) = Note No.

The absence of an entry (-) indicates that the decision is independent of that particular condition.

	RST	SYNR	SYNC	SYNCC	FINR	FINC	ACK	DATA
RST	Y	N	N	N	N	N	N	N
ACK	-	N	Y	Y	Y	Y	Y	Y
SYN	-	Y	Y	N	N	N	N	N
FIN	-	N	N	N	Y	(3)	N	N
User Data	-	(1)	(1)	(1)	(2)	(2)	N	Y
STATE = WFSYNCC	-	-	-	Y	-	N	-	-
Acknowledges SYNC	-	-	-	Y	-	N	N	N
Acknowledges FINR	-	-	-	N	-	Y	N	N
Acknowledges SYNR	-	-	-	N	-	N	N	N
STATE = WFFINC3 or WFFINCDN2 or WFFINC4 or WFFINC1 or WFFINCDN1	-	-	-	N	-	Y	-	-

Notes to Table 5:

1: Any User-Data shall be assumed to arrive in a DATA event immediately following this event.

2: Any User-Data shall be assumed to have arrived in a DATA event immediately preceding this event.

3: This event shall be treated as being composed of a FINC followed by a FINR when FIN is set.

TABLE VI
MAIN STATES

Abbreviated name	Name and description
CLOSED	Transport connection is closed
NESTABLISH/TCP	TCP initiated connection in progress
NESTABLISH/ISO	ISO initiated connection in progress
WFNCONconf/ISO	ISO NCONconf pending
WFSYNR	TCP SYN request pending
WFNCONconf/TCP	TCP NCONconf pending
WFCR	ISO Connect Request pending
WFCC	ISO Connect Confirmation pending
WFSYNC	TCP SYN Confirmation (SYN,ACK) pending
WFSYNCC	TCP SYN Confirmation ACK pending
AKWAIT	ISO AK pending
OPEN	Transport connection is open
WBCL	Wait before releasing (wait for CC before sending the DR TPDU)
WFDN1	ISO S-Disconnect (DN) pending
WFFINC3	TCP FIN confirmation pending
WFFINCDN1	ISO/TCP finished confirmations pending
WFFINCDN2	ISO/TCP finished confirmations pending
WFFINR	TCP FIN request pending
WFFINC1	TCP FIN confirmation pending
WFDN3	ISO S-Disconnect pending
WFFINC2	TCP FIN confirmation pending
WFDN2	ISO S-Disconnect pending
WFFINC4	TCP FIN confirmation pending
WFDN4	ISO S-Disconnect pending
TIMEWAIT	Wait before re-use of TCP connection
CLOSING	ISO Abrupt Release in progress

TABLE VII
SUBSTATES

Abbreviated name	Description	Main States for which the substate applies
WFEA	Wait for EA TPDU	OPEN
FINR-SENT	All data on the connection queued for the TCP party and FINR are sent	WFFINC2, WFFINCDN1, WFFINC1, WFFINC4, WFINCDN2, WFFINC3
FN-SENT	All data on the connection queued for the ISO party and FN are sent	WFDN1, WFFINCDN1, WFDN2, WFFINCDN2, WFDN3, WFDN4
WFDR	The ISO TC is still established after a successful Orderly Release	CLOSED, TIMEWAIT
DR-SENT	A DR is issued	CLOSED, TIMEWAIT
REFUSE	The TC shall not be established due to lack of a Network connection from the converter to the "remote" end system	NESTABLISH/ISO NESTABLISH/TCP

The 26 main states for the EFSM are defined in Table VI. Substates and enabling predicates are used to avoid an excessive number of state/event combinations. The six substates which may be active within several of the main states, are defined in Table VII. The transition-enabling predicates used in the state/event tables of [5] are formed as predicates over the attributes of protocol data units (events) and substates.

Some precautions have to be taken to prevent call collisions on the TCP side of the converter. Such collisions might lead to misconnection of calls and have to be avoided.

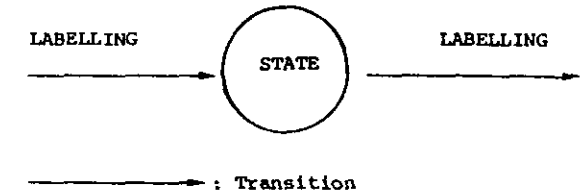
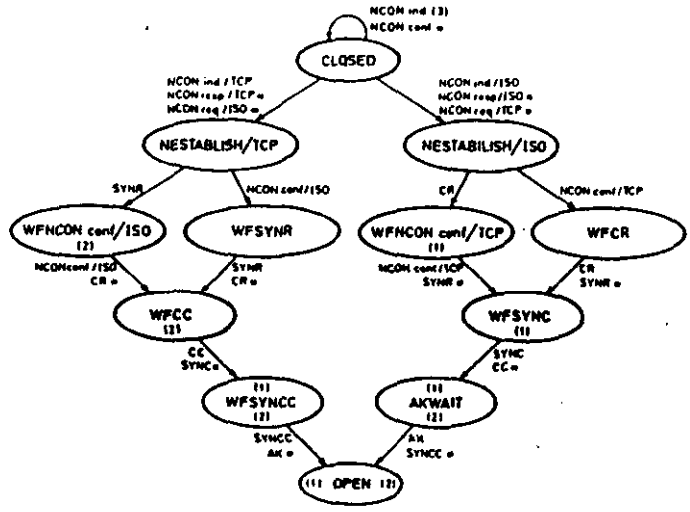


Fig. 5. Notation for state diagrams. Labeling: List of events involved in the transition. The triggering event is unmarked, while resulting events are marked with an asterisk.



1) Data can be present in the TCP output queue

2) Data can be present in the ISO output queue

3) Transition taken when the N-layer is not conveying the end-system address.

Fig. 6. Normal sequence for connection establishment. The assumption that there are no network connections readily available applies. (Data transfer takes place within the OPEN state.)

The simplest solution (proposed in [5]) is to restrict incoming calls to the converter, on the TCP side, to be destined for even-valued ports. The converter would have to use only odd-valued source ports for outgoing TCP calls. This solution burdens the service user with choosing even-valued port numbers for all calls through a converter, and through this, forces the service user to be aware of the existence of the converter.

An alternative, and possibly superior, solution is to have the converter reissue an outgoing call from a different source port every time a call collision is detected (i.e., when a SYNR arrives in the WFSYNC state).

The state diagrams of Figs. 6 and 7 give an overview of the protocol conversion procedure (the operation of the EFSM). The use of multiple network connections (splitting), substate-dependent actions and error handling are not described in the diagrams, but are dealt with in the state/event tables in [5]. The notation is defined by Fig. 5.

In a system where the converter is implemented between a TCP-based subnetwork and an ISO-based subnetwork, it is necessary to transfer the end-user network address through the converter. This is taken care of by the IP protocol when IP is in use on both sides of the converter.

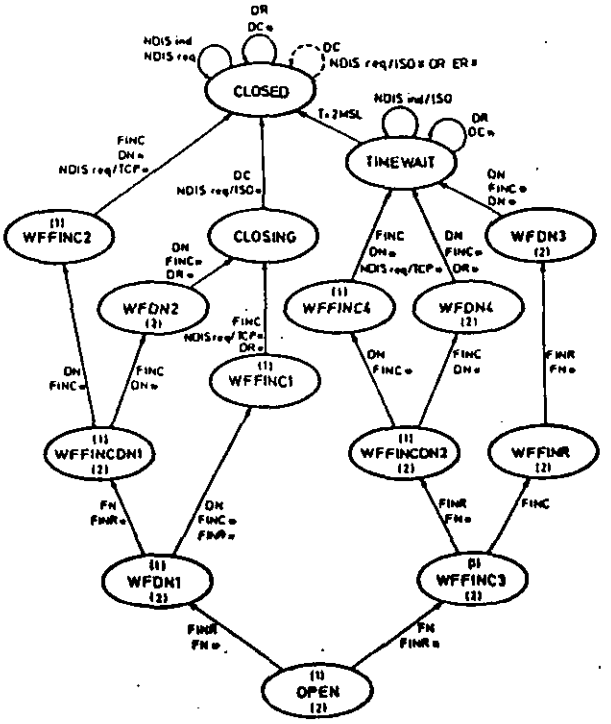


Fig. 7. Normal sequences for orderly release. Disconnection of the network connections is based on the assumption that no other T connections are multiplexed on the used N connections.

In other cases, where one or both of the subnetworks connected to the converter does not support IP, there is a need for a Level 3 or Level 4 mechanism (for transfer of the end-user network address). It is quite clear that such a function belongs to the IP sublayer of the Network layer, but the following alternatives exist (with the preferred solution listed first).

1) Include the IP layer in all subnetworks,

2) utilize the user-data field of the N-CONNECT request and indication primitives to convey the address,

3) include the end-user network address in the called TSAP-ID of the T-CONNECT request and indication primitives,

4) utilize the user-data field of the T-CONNECT request and indication primitives to convey the address.

The DT TPDU shall always convey a session protocol data unit (SPDU). The three different SPDU's that shall be embedded in this way are:

1) the DT SPDU,

2) the FN SPDU, and

3) the DN SPDU.

None of these SPDU's shall be embedded in an ED TPDU.

A connection-oriented network service is assumed in [5] for descriptive purposes, but a datagram-type service, which is simpler than a connection-type service, can be accessed through the same service primitives defined for the connection-oriented service. Basing the specification on a connection oriented service is, thus, merely a way of extending its generality.

The general approach to protocol conversion and its formal background are explained well in [13].

An implementation of the converter, based on [5], is currently undertaken as a joint effort between the SHAPE Technical Centre and the U.S. DoD. Follow-up international experiments are in the initial planning phase.

VII. Conclusions

The great similarity of the ISO and TCP protocols, the power of common service subset, and the fact that the conversion algorithm presented is no more complex than the more complicated of the two protocols, supports the conclusion that the proposed conversion strategy is a practical short-term approach to providing a solution to the interoperability problem.

It is NATO's intention to introduce ISO protocols as far as possible in all new systems, as the means of ensuring cost-effective interoperation.

In order to serve a wider user group, ISO may have to make the Orderly Release accessible as a Transport Service extension, either by introduction of a Session sublayer containing the Orderly Release function or, as a simpler solution, by moving the Orderly Release from the Session layer to the Transport layer (as is done in the NBS version of the Class 4 Transport protocol).

Summary

In 1978, the U.S. Department of Defense (DoD) accepted the Transmission Control Protocol (TCP) and the Internet Protocol (IP) as standards for data communications purposes. However, since then ISO has introduced standards based on the OSI model and this has given rise to an urgent need for interoperation between existing TCP/IP-based systems and evolving systems.

The ideal solution to the interoperability problem is to use common protocols for all layers above the network level. This is not always possible in the short term. For this reason, it may seem that the optimum solution to the interoperability problem is to convert all of the protocol layers. This would make full interoperation through a converter possible. However, the higher protocol layers (above the Transport layer) are so diverse that an all-embracing protocol layer conversion which retains the defined end-to-end conditions of every layer is not feasible.

A store-and-forward unit might be able to process all layers, but would violate the defined end-to-end operating characteristics of the Transport and higher layers.

Therefore, we have to revert to conversion, and this should take place at a layer at which it is possible to establish the defined end-to-end conditions for all subsequent layers.

The specific application functionality (above the Transport layer), whether it is implemented with ISO protocols or any other protocols, must be fully compatible in each and every end-system involved.

The author has developed an algorithm which, through conversion at the Transport layer, maintains end-to-end conditions for a common subset of the services provided by the TCP and the ISO protocols. This subset includes the ISO Session Orderly Release, and appears sufficiently powerful for all military and civilian applications.

The specification of the conversion algorithm is based on an extended finite-state machine description. Enabling predicates and substates are used to prevent an excess in the number of state/event combinations.

The required actions and state transitions are described for every state/event combination. This includes legal combinations, illegal combinations, and inconsistent combinations.

The great similarity of the TCP and the ISO Transport protocol, and the fact that the conversion algorithm is no more complex than the more complicated of the two, supports the conclusion that the proposed protocol conversion strategy is a practical short-term approach to solving the interoperability problem.

It is NATO's intention to introduce ISO protocols as far as possible in all new systems as the means of ensuring cost-effective interoperation. The set of requirements which have been identified as permitting ISO to interoperate with TCP/IP appears to encompass those which ISO may have to include in any case, in order to serve a wider user group.

Acknowledgment

The author is grateful to Dr. R. Benjamin and E. Wells for their ideas and suggestions on improvements, and to Dr. P. Spilling and H. T. Alvestrand at the Norwegian Telecommunications Research Establishment who provided good comments and valuable information on existing TCP implementations. In addition, the author appreciated the reviewer's comments and thanks R. Cameron and J. McWhirter for their help with preparing the manuscript.

References

[1] "U.S. DoD transmission control protocol," Military Standard, M1778, Aug. 12, 1983.
[2] "U.S. DoD Internet protocol," Military Standard, M1777.
[3] "Information processing systems—Open systems interconnection —Transport protocol specification," ISO DIS 8073 Rev., Sept. 1984.
[4] I. Groenbaek, "The TCP and ISO transport service—A brief description and comparison," SHAPE Technical Centre, Tech. Memo. TM-726 (NATO Unclassified Report), Feb. 1984.
[5] ———, "Specification of protocol conversion between the TCP and the ISO class 4 transport protocol," SHAPE Technical Centre, Tech. Memo. TM-733 (NATO Unclassified Report), Dec. 1984.
[6] "Information processing systems—Open systems interconnection —Basic reference model," ISO 7498, 1984.
[7] "Information processing systems—Open systems interconnection —Transport service definition," ISO DIS 8072, 1983.
[8] "Information processing systems—Open systems interconnection —Basic connection-oriented session service definition," ISO DIS 8326, 1984.
[9] "Information processing systems—Open Systems Interconnection —Basic connection-oriented session protocol specification," ISO DIS 8327, 1984.
[10] *Specification of the Transport Protocol Vol. 3: Extended Class Protocol ICST/HLNP-83-1*, National Bureau of Standards, Gaithersburg, MD, Jan. 1983.
[11] "A formal description technique based on an extended state transition model," ISO/TC 97/SC 21 N1777, Oct. 1984.
[12] D. P. Sidhu and T. P. Blumer, "An automated protocol development system," in *Proc. Symp. Application and Assessment of Automated Tools for Software Development*, Nov. 1–3, 1983, San Francisco, CA; Silver Spring, MD: IEEE Comput. Soc. Press.
[13] P. E. Green, Jr., "Protocol conversion," to be published.

Inge Groenbaek received the M.S. degree in computer science from the Technical University, Trondheim, Norway, in 1977.

He has since been involved in protocol design and implementation for systems involving circuit switching, packet switching, and message handling. From late 1982 to September 1985, he was seconded from Siemens Norway A/S to NATO at SHAPE Technical Centre (STC) in The Hague, Holland, where he was working in the areas of protocol standardization and transmission media management. He was, for a period, the STC representative on the working group for the application of the ISO model (particularly levels 1–4) to NATO needs and systems. He is currently back with Siemens, where he will work on systems oriented in the area of ISO OSI and CCITT ISDN.

(This page intentionally left blank.)

MANDATORY APPENDIX B

REQUEST FOR COMMENTS: RFC 1006

ISO TRANSPORT SERVICE ON TOP OF THE TCP

VERSION: 3

Scope. This appendix describes the method to be used by DoD ESs to transition from TCP/IP protocols to GOSIP.

Network Working Group
Request for Comments: RFC 1006

Marshall T. Rose, Dwight E. Cass
Northrop Research and Technology Center
May 1987

ISO Transport Service on top of the TCP
Version: 3

Status of this Memo

This memo specifies a standard for the Internet community. Hosts on the Internet that choose to implement ISO transport services on top of the TCP are expected to adopt and implement this standard. TCP port 102 is reserved for hosts which implement this standard. Distribution of this memo is unlimited.

This memo specifies version 3 of the protocol and supersedes [RFC983]. Changes between the protocol as described in Request for Comments 983 and this memo are minor, but are unfortunately incompatible.

1. Introduction and Philosophy

The Internet community has a well-developed, mature set of transport and internetwork protocols (TCP/IP), which are quite successful in offering network and transport services to end-users. The CCITT and the ISO have defined various session, presentation, and application recommendations which have been adopted by the international community and numerous vendors. To the largest extent possible, it is desirable to offer these higher level directly in the ARPA Internet, without disrupting existing facilities. This permits users to develop expertise with ISO and CITT applications which previously were not available in the ARPA Internet. It also permits a more graceful convergence and transition strategy from TCP/IP-based networks to ISO-based networks in the medium-and long-term.

There are two basic approaches which can be taken when "porting" an ISO or CCITT application to a TCP/IP environment. One approach is to port each individual application separately, developing local protocols on top of the TCP. Although this is useful in the short-term (since special-purpose interfaces to the TCP can be developed quickly), it lacks generality.

A second approach is based on the observation that both the ARPA Internet protocol suite and the ISO protocol suite are both layered systems (though the former uses layering from a more pragmatic perspective). A key aspect of the layering principle is that of layer-independence. Although this section is redundant for most readers, a slight bit of background material is necessary to introduce this concept.

Externally, a layer is defined by two definitions:

> a service-offered definition, which describes the services provided by the layer and the interfaces it provides to access those services; and,
>
> a service-required definitions, which describes the services used by the layer and the interfaces it uses to access those services.

Collectively, all of the entities in the network which co-operate to provide the service are known as the service-provider. Individually, each of these entities is known as a service-peer.

Interally, a layer is defined by one definition:

> a protocol definition, which describes the rules which each service-peer uses when communicating with other service-peers.

Putting all this together, the service-provider uses the protocol and services from the layer below to offer the its service to the layer above. Protocol verification, for instance, deals with proving that this in fact happens (and is also a fertile field for many Ph.D. dissertations in computer science).

The concept of layer-independence quite simply is:

> IF one preserves the services offered by the service-provider
>
> THEN the service-user is completely naive with respect to the protocol which the service-peers use

For the purposes of this memo, we will use the layer-independence to define a Transport Service Access Point (TSAP) which appears to be identical to the services and interfaces offered by the ISO/CCITT TSAP (as defined in [ISO8072]), but we will in fact implement theISO TP0 protocol on top of TCP/IP (as defined in [RFC793,RFC791]), not on top of the the ISO/CCITT network protocol. Since the transport class 0 protocol is used over the TCP/IP connection, it achieves identical functionality as transport class 4. Hence, ISO/CCITT higher level layers (all session, presentation, and application entities) can operate fully without knowledge of the fact that they are running on a TCP/IP internetwork.

2. Motivation

In migrating from the use of TCP/IP to the ISO protocols, there are several strategies that one might undertake. This memo was written with one particular strategy in mind.

The particular migration strategy which this memo uses is based on the notion of gatewaying between the TCP/IP and ISO ptotocol suites at the transport layer. There are two strong arguments for this approach:

1. Experience teaches us that it takes just as long to get good implementations of the lower level protocols as it takes to get implementations of the higher level ones. In particular, it has been observed that there is still a lot of work being done at the ISO network and transport layers. As a result, implementations of protocols above these layers are not being aggressively pursued. Thus, something must be done "now" to provide a medium in which the higher level protocols can be developed. Since TCP/IP is mature, and essentially provides identical functionality, it is an ideal medium to support this development.

2. Implementation of gateways at the IP and ISO IP layers are probably not of general use in the long term. In effect, this would require each Internet host to support both TP4 and TCP. As such, a better strategy is to implement a graceful migration path from TCP/IP to ISO protocols for the ARPA Internet when the ISO protocols have matured sufficiently.

Both of these arguments indicate that gatewaying should occur at or above the transport layer service access point. Further, the first argument suggests that the best approach is to perform the gatewaying exactly AT the transport service access point to maximize the number of ISO layers which can be developed.

NOTE: This memo does not intend to act as a migration or intercept document. It is intended ONLY to meet the needs discussed above. However, it would not be unexpected that the protocol described in this memo might form part of an overall transition plan. The description of such a plan however is COMPLETELY beyond the scope of this memo.

Finally, in general, building gateways between other layers in the TCP/IP and ISO protocol suites is problematic, at best.

To summarize: the primary motivation for the standard described in this memo is to facilitate the process of gaining experience with higher-level ISO protocols (session, presentation, and application). The stability and maturity of TCP/IP are ideal for

providing solid transport services independent of actual implementation.

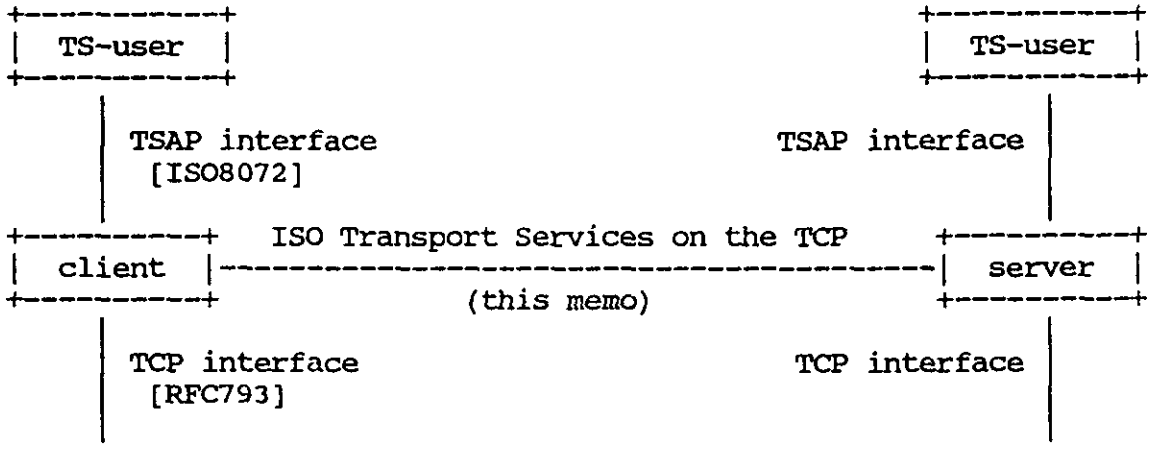
3. The Model

The [ISO8072] standard describes the ISO transport service definition, henceforth called TP.

ASIDE: This memo references the ISO specifications rather than the CCITT recommendations. The differences between these parallel standards are quite small, and can be ignored, with respect to this memo, without loss of generality. To provide the reader with the relationships:

Transport service	[ISO8072]	[X.214]
Transport protocol	[ISO8073]	[X.224]
Session protocol	[ISO8327]	[X.225]

The ISO transport service definition describes the services offered by the TS-provider (transport service) and the interfaces used to access those services. This memo focuses on how the ARPA Transmission Control Protocol (TCP) [RFC793] can be used to offer the services and provide the interfaces.



For expository purposes, the following abbreviations are used:

TS-peer — a process which implements the protocol described by this memo

TS-user — a process talking using the services of a TS-peer

TS-provider the black-box entity implementing the protocol described by this memo

For the purposes of this memo, which describes version 2 of the TSAP protocol, all aspects of [ISO8072] are supported with one exception:

Quality of Service parameters

In the spirit of CCITT, this is left "for further study". A future version of the protocol will most likely support the QOS parameters for TP by mapping these onto various TCP parameters.

The ISO standards do not specify the format of a session port (termed a TSAP ID). This memo mandates the use of the GOSIP specification [GOSIP86] for the interpretation of this field. (Please refer to Section 5.2, entitled "UPPER LAYERS ADDRESSING".)

Finally, the ISO TSAP is fundamentally symmetric in behavior. There is no underlying client/server model. Instead of a server listening on a well-known port, when a connection is established, the TS-provider generates an INDICATION event which, presumably the TS-user catches and acts upon. Although this might be implemented by having a server "listen" by hanging on the INDICATION event, from the perspective of the ISO TSAP, all TS-users just sit around in the IDLE state until they either generate a REQUEST or accept an INDICATION.

4. The Primitives

The protocol assumes that the TCP[RFC793] offers the following service primitives:

Events

connected	- open succeeded (either ACTIVE or PASSIVE)
connect fails	- ACTIVE open failed
data ready	- data can be read from the connection
errored	- the connection has errored and is now closed
closed	- an orderly disconnection has started

Actions

listen on port	- PASSIVE open on the given port
open port	- ACTIVE open to the given port
read data	- data is read from the connection
send data	- data is sent on the connection
close	- the connection is closed (pending data is sent)

This memo describes how to use these services to emulate the following service primitives, which are required by [ISO8073]:

Events

N-CONNECT.INDICATION
- An NS-user (responder) is notified that connection establishment is in progress

N-CONNECT.CONFIRMATION
- An NS-user (responder) is notified that the connection has been established

N-DATA.INDICATION
- An NS-user is notified that data can be read from the connection

N-DISCONNECT.INDICATION
- An NS-user is notified that the connection is closed

Actions

N-CONNECT.REQUEST
- An NS-user (initiator) indicates that it wants to establish a connection

N-CONNECT.RESPONSE
- An NS-user (responder) indicates that it will honor the request

N-DATA.REQUEST - An NS-user sends data

N-DISCONNECT.REQUEST
- An NS-user indicates that the connection is to be closed

The protocol offers the following service primitives, as defined in [ISO8072], to the TS-user:

Events

T-CONNECT.INDICATION
- a TS-user (responder) is notified that connection establishment is in progress

T-CONNECT.CONFIRMATION
- a TS-user (initiator) is notified that the connection has been established

T-DATA.INDICATION
- a TS-user is notified that data can be read from the connection

T-EXPEDITED DATA.INDICATION
- a TS-user is notified that "expedited" data can be read from the connection

T-DISCONNECT.INDICATION
- a TS-user is notified that the connection is closed

Actions

T-CONNECT.REQUEST
- a TS-user (initiator) indicates that it wants to establish a connection

T-CONNECT.RESPONSE
- a TS-user (responder) indicates that it will honor the request

T-DATA.REQUEST - a TS-user sends data

T-EXPEDITED DATA.REQUEST
- a TS-user sends "expedited" data

T-DISCONNECT.REQUEST
- a TS-user indicates that the connection is to be closed

5. The Protocol

The protocol specified by this memo is identical to the protocol for ISO transport class 0, with the following exceptions:

- for testing purposes, initial data may be exchanged during connection establishment
- for testing purposes, an expedited data service is supported
- for performance reasons, a much larger TSDU size is supported
- the network service used by the protocol is provided by the TCP

The ISO transport protocol exchanges information between peers in discrete units of information called transport protocol data units (TPDUs). The protocol defined in this memo encapsulates these TPDUs in discrete units called TPKTs. The structure of these TPKTs and their relationship to TPDUs are discussed in the next section.

PRIMITIVES

The mapping between the TCP service primitives and the service primitives expected by transport class 0 are quite straightforward:

network service	TCP
CONNECTION ESTABLISHMENT	
N-CONNECT.REQUEST	open completes
N-CONNECT.INDICATION	listen (PASSIVE open) finishes
N-CONNECT.RESPONSE	listen completes
N-CONNECT.CONFIRMATION	open (ACTIVE open) finishes
DATA TRANSFER	
N-DATA.REQUEST	send data
N-DATA.INDICATION	data ready followed by

	read data
CONNECTION RELEASE	
N-DISCONNECT.REQUEST	close
N-DISCONNECT.INDICATION	connection closes or errors

Mapping parameters is also straight-forward:

network service	TCP
CONNECTION RELEASE	
Called address	server's IP address (4 octets)
Calling address	client's IP address (4 octets)
all others	ignored
DATA TRANSFER	
NS-user data (NSDU)	data
CONNECTION RELEASE	
all parameters	ignored

CONNECTION ESTABLISHMENT

The elements of procedure used during connection establishment are identical to those presented in [ISO8073], with three exceptions.

In order to facilitate testing, the connection request and connection confirmation TPDUs may exchange initial user data, using the user data fields of these TPDUs.

In order to experiment with expedited data services, the connection request and connection confirmation TPDUs may negotiate the use of expedited data transfer using the negotiation mechanism specified in [ISO8073] is used (e.g., setting the "use of transport expedited data transfer service" bit in the "Additional Option Selection" variable part). The default is not to use the transport expedited data transfer service.

In order to achieve good performance, the default TPDU size is 65531 octets, instead of 128 octets. In order to negotiate a smaller (standard) TPDU size, the negotiation mechanism specified in [ISO8073] is used (e.g., setting the desired bit in the "TPDU Size" variable part).

To perform an N-CONNECT.REQUEST action, the TS-peer performs an active open to the desired IP address using TCP port 102. When the TCP signals either success or failure, this results in an N-CONNECT.INDICATION action.

To await an N-CONNECT.INDICATION event, a server listens on TCP port 102. When a client successfully connects to this port, the event occurs, and an implicit N-CONNECT.RESPONSE action is performed.

NOTE: In most implementations, a single server will perpetually LISTEN on port 102, handing off connections as they are made

DATA TRANSFER

The elements of procedure used during data transfer are identical to those presented in [ISO8073], with one exception: expedited data may be supported (if so negotiated during connection establishment) by sending a modified ED TPDU (described below). The TPDU is sent on the same TCP connection as all of the other TPDUs. This method, while not faithful to the spirit of [ISO8072], is true to the letter of the specification.

To perform an N-DATA.REQUEST action, the TS-peer constructs the desired TPKT and uses the TCP send data primitive.

To trigger an N-DATA.INDICATION action, the TCP indicates that data is ready and a TPKT is read using the TCP read data primitive.

CONNECTION RELEASE

To perform an N-DISCONNECT.REQUEST action, the TS-peer simply closes the TCP connection.

If the TCP informs the TS-peer that the connection has been closed or has errored, this indicates an N-DISCONNECT.INDICATION event.

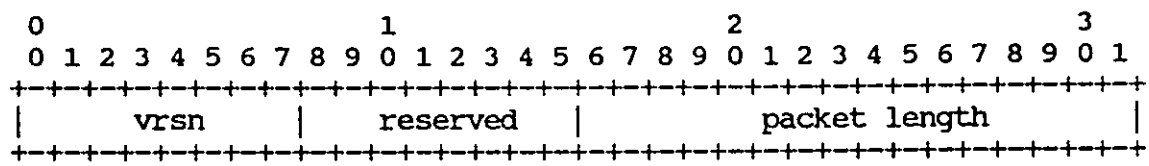
6. Packet Format

A fundamental difference between the TCP and the network service expected by TP0 is that the TCP manages a continuous stream of octets, with no explicit boundaries. The TP0 expects information to be sent and delivered in discrete objects termed network service data units (NSDUs). Although other classes of transport may combine more than one TPDU inside a single NSDU, transport class 0 does not use this facility. Hence, an NSDU is identical to a TPDU for the purposes of our discussion.

The protocol described by this memo uses a simple packetization scheme in order to delimit TPDUs. Each packet, termed a TPKT, is viewed as an object composed of an integral number of octets, of variable length.

NOTE: For the purposes of presentation, these objects are shown as being 4 octets (32 bits wide). This representation is an artifact of the style of this memo and should nto be interpreted as requiring that a TPKT be a multiple of 4 octets in length.

A TPKT consists of two parts: a packet-header and a TPDU. The format of the header is constant regardless of the type of packet. The format of the packet-header is as follows:



where:

vrsn 8 bits

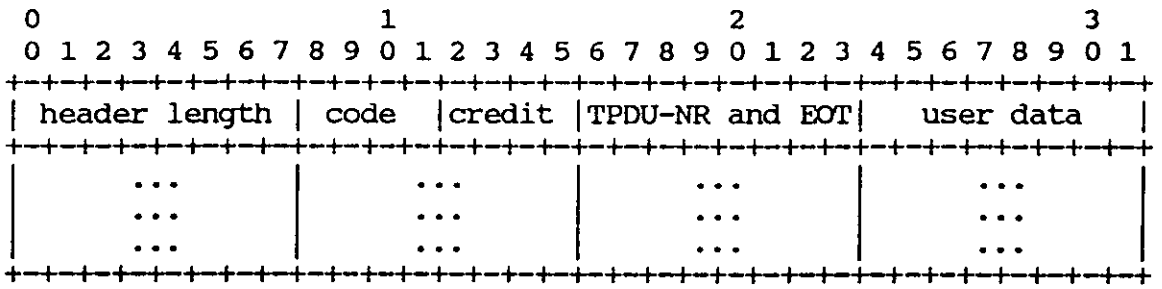
This field is always 3 for the version of the protocol described in this memo.

packet length 16 bits (min=7, max=65535)

This field contains the length of entire packet in octets, including packet-header. This permits a maximum TPDU size of 65531 octets. Based on the size of the data transfer (DT) TPDU, this permits a maximum TSDU size of 65524 octets.

The format of the TPDU is defined in [ISO8073]. Note that only TPDUs formatted for transport class 0 are exchanged (different transport classes may use slightly different formats).

To support expedited data, a non-standard TPDU, for expedited data is permitted. The format used for the ED TPDU is nearly identical to the format for the normal data, DT, TPDU. The only difference is that the value used for the TPDU's code is ED, not DT:



After the credit field (which is always ZERO on output and ignored on input), there is one additional field prior to the user data.

TPDU-NR and EOT 8 bits

Bit 7 (the high-order bit, bit mask 1000 0000) indicates the end of a XSDU (expedited TSDU). All other bits should be ZERO on output and ignored on input.

Note that the TP specification limits the size of an expedited transport service data unit (XSDU) to 16 octets.

7. Comments

Since the release of RFC983 in April of 1986, we have gained much experience in using ISO transport services on top of the TCP. In September of 1986, we introduced the use of version 2 of the protocol, based mostly on comments from the community.

In January of 1987, we observed that the differences between version 2 of the protocol and the actual transport class 0 definition were actually quite small. In retrospect, this realization took much longerr than it should have: TP0 is is meant to run over a reliable network service, e.g., X.25. The TCP can be used to prrvide a service of this type, and, if no one complains to loudly, one could state that this memo really just describes a method for encapsulating TPO inside of TCP!

The changes in going from version 1 of the protocol to version 2 and then to version 3 are all relatively small. Initially, in describing version 1, we decided to use the TPDU formats from the ISO transport protocol. This naturally led to the evolution described above.

8. References

[GOSIP86] The U.S. Government OSI User's Committee. "Government Open Systems Interconnection Procurement (GOSIP) Specification for Fiscal years 1987 and 1988." (December, 1986) [draft status]

[ISO8072] ISO. "International Standard 8072. Information Processing Systems -- Open Systems Interconnection: Transport Service Definition." (June, 1984)

[ISO8073] ISO. "International Standard 8073. Information Processing Systems -- Open Systems Interconnection: Transport Protocol Specification." (June, 1984)

[ISO8327] ISO. "International Standard 8327. Information Processing Systems -- Open Systems Interconnection: Session Protocol Specification." (June, 1984)

[RFC791] Internet Protocol. Request for Comments 791 (MILSTD 1777) (September, 1981)

[RFC793] Transmission Control Protocol. Request for Comments 793 (MILSTD 1778) (September, 1981)

[RFC983] ISO Transport Services on Top of the TCP. Request for Comments 983 (April, 1986)

[X.214] CCITT. "Recommendation X.214. Transport Service Definitions for Open Systems Interconnection (OSI) for CCITT Applications." (October, 1984)

[X.224] CCITT. "Recommendation X.224. Transport Protocol Specification for Open Systems Interconnection (OSI) for CCITT Applications." (October, 1984)

[X.225] CCITT.
"Recommendation X.225. Session Protocol Specification for Open Systems Interconnection (OSI) for CCITT Applications."
(October, 1984)

MANDATORY APPENDIX C

REQUEST FOR COMMENTS: RFC 1086

ISO -- TP0 BRIDGE BETWEEN TCP AND X.25

Scope. This appendix supplements the information provided in appendix B.

Network Working Group
Request for Comments: 1086

J. Onions
Nottingham
M. Rose
TWG

December 1988

ISO-TP0 bridge between TCP and X.25

Status of this Memo

This memo proposes a standard for the Internet community. Hosts on the Internet that choose to implement ISO TP0 transport connectivity between TCP and X.25 based hosts are expected to experiment with this proposal. TCP port 146 is reserved for this proposal. Distribution of this memo is unlimited and comments are highly encouraged.

Introduction

This memo specifies a protocol that is used to bridge ISO TP0 packets between X.25 and TCP networks. This technique is useful when interconnecting a DDN IP internet to an X.25 subnetwork. This is not a "magic bullet" solution to the DDN/ISO interoperability problem. Rather, if one is running higher-layer ISO protocols in both networks (namely ISO TP0), then a TP0 bridge can be used to achieve connectivity.

The protocol itself is fairly simple as the method of operation for running TP0 over the TCP and X.25 protocols have previously been defined. A bridge offering ISO-TP0 gateway services simply applies both methods as appropriate. The protocol works by TP0/TCP hosts "registering" an X.25 subaddress (and corresponding TCP port/IP address) with the bridge. TP0/X.25 hosts use the standard method for establishing, maintaining, and releasing connections. When a connection is established, the bridge establishes the corresponding TCP connection and simply shuffles TP0 packets between the two. When a TP0/TCP host initiates a connection, it establishes a TCP connection to the bridge using port number 146 and communicates the desired X.25 address. The bridge establishes a connection to the native X.25 host and simply shuffles TP0 packets between the two.

1. Introduction and Motivation

The migratory protocol described in [RFC1006] makes possible the transmission of TP0 packets between hosts on TCP/IP internets. With the addition of a small protocol converter, a TCP/IP host can be made to appear in the X.25 addressing space and be able to accept and make

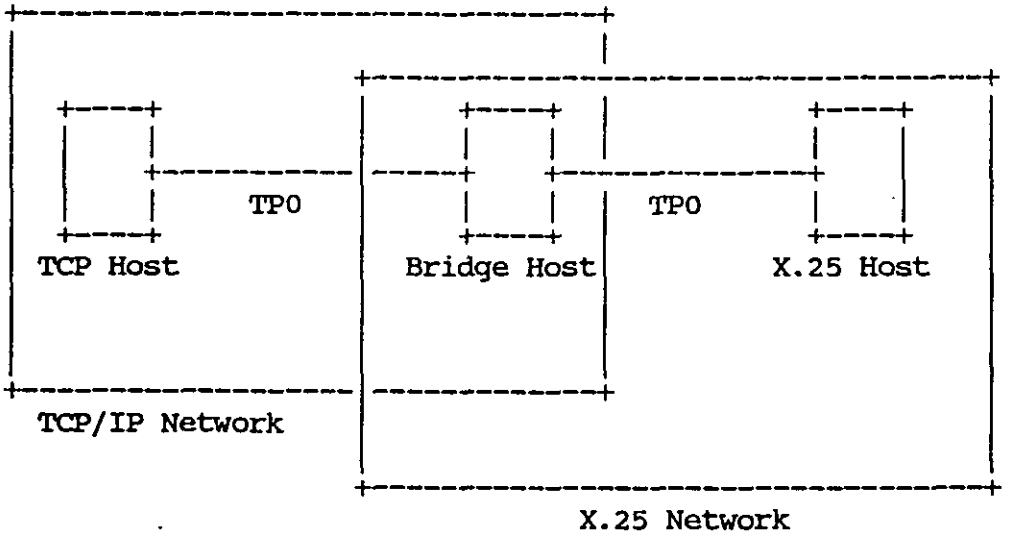
connections using the TP0 protocol.

This procedure is particularly useful in the following cases:

1. A host on an IP based internet can communicate with hosts on X.25 based networks providing the hosts are running ISO protocols. This also assumes a friendly gateway willing to run the actual TP0 bridge and make available to the IP host part of its X.25 address space.

2. A site having sparse connections to an X.25 network and using a TCP/IP based local area network for local communications. In this case all hosts on the LAN can have access to hosts on the X.25 network running ISO TP0.

Pictorially, this memo describes interoperation in the following environment:



2. Definitions and Philosophy

Some modest terminology and philosophy is introduced to aid readability and stir interest.

The ISO Transport Service (TS) provides a reliable, packet-stream to its users [ISO8072]. The ISO Transport Protocol (TP) implements this service [ISO8073]. There are five classes of this protocol. The class is selected on the basis of the services offered by the underlying network service. Transport class 0 (TP0) is used when the network service offered is connection-oriented and error-detecting.

As should be expected, TP0 is a rather simple protocol, since the underlying network service actually provides most of the qualities offered by the transport service.

CCITT Recommendation X.25 [ISO8208,X.25] offers such a network service. It is beyond the scope of this memo to describe X.25 in any detail, but two observations are pertinent: First, X.25 is offered as a wide-area network service by many commercial and (non-U.S.) government carriers. Second, the TP0/X.25 combination is very popular in Europe and other communities with a strong PTT-oriented market.

It has been argued that the DoD Transmission Control Protocol (TCP) [MIL1778, RFC793] can also be seen as providing a connection-oriented and error-detecting network service. This remark is controversial in the sense that the TCP is actually an end-to-end transport protocol and not a network protocol; the DoD Internet Protocol (IP) [MIL1777, RFC791] is the network protocol in the DoD Protocol Suite. However, one of the advantages of layering is that, when properly architected, it enhances flexibility. This notion led to the development of [RFC983] and its successor [RFC1006], which described how to provide the ISO transport service on top of TCP/IP internetworks.

3. The Model

The model is simple. The method for transmitting TP0 packets using TCP is defined in [RFC1006]. The method for transmitting TP0 packets using X.25 is defined in [ISO8878]. The TP0 bridge merely has to convert between the two forms. As with most protocols, there are three well-defined phases of interaction: connection establishment, data transfer, and connection release. The method of operation for the data transfer and connection release phases are quite similar when using TP0 over either network service. Hence the resulting protocol mapping functions are quite simple.

The difficult part is in managing connection establishment. A small "registration" protocol is used to aid the protocol mapping function for the connection establishment phase. The protocol performs one of two operations: an X.25 address is specified for an outgoing call, or an X.25 address is specified to accept incoming calls.

This memo ignores the problems of authentication and authorization. These areas are presumed to be a local matter. It is worth pointing out that running such a TP0 bridge with unrestricted access allows any TCP/IP host to lay claim to part of the TP0 bridge host's X.25 address space. This address space is limited and will not support many foreign hosts registering listening addresses.

The protocol makes no attempt to report errors other than those transmitted by the TP0 protocol. To attempt such additions would require other mechanism such as a new protocol layer or equivalent. The chosen model is kept as simple as possible with network errors being ignored if recoverable, and resulting in disconnection otherwise. This actually enhances the transparency of the gateway, in that the only gateway specific functions are collected together in the connection phase. The resultant circuit, once established, is indistinguishable from an [RFC1006] implementation.

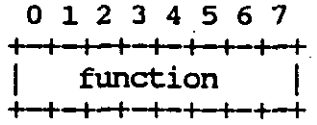
4. The Protocol

The protocol is quite simple. A successful connection establishment phase results in two network connections being established. TP0 is used over each network connection, though one network connection is provided by X.25 and the other by the TCP.

During the data transfer phase, the TP0 bridge reads TPDUs (transport protocol data units) from one network connection and writes them to the other network connection. During the connection release phase, when one network indicates a disconnect, the bridge disconnects the other network connection; or in the case of simultaneous network disconnects, no action is taken by the bridge.

As expected, the method of operation for the connection establishment phase is more complex. Connection establishment is driven by a registration procedure which is initiated by a TCP/IP host initiating a connection with the TP0 bridge. This procedure takes on one of two "flavors" depending on whether the initiating host wishes to establish a connection to a particular X.25 address or listen for connections on a particular X.25 address.

The initiating host initiates the registration procedure by establishing a connection to TCP port 146 on the TP0 bridge. It then sends one octet which indicates the flavor the registration procedure will take:



The value of this octet is a binary-encoded value:

value	meaning
0	illegal
1	connect to a particular X.25 host
2	listen for incoming X.25 connections
3-255	reserved

The method of operation for the registration procedure now diverges, based on the function chosen.

FUNCTION 1: CONNECTION THROUGH THE TP0 BRIDGE

The X.25 address to call is now sent by the initiating host to the TP0 bridge. The format of an X.25 address is described in Section 5 of this memo.

The TP0 bridge now attempts to call the specified address. If this succeeds, the connection establishment phase has succeeded and the data transfer phase is begun. If the call fails, then the TP0 bridge closes the TCP connection.

FUNCTION 2: ESTABLISHING A LISTENING ADDRESS

The X.25 address, which should be a subaddress of the TP0 bridge's X.25 address, on which to listen for incoming X.25 connections is now sent by the initiating host to the TP0 bridge.

Next, the initiating host sends an IP address and TCP port number which will service incoming calls for the indicated X.25 address. The format of a TCP/IP address is described in Section 6 of this memo.

The TP0 bridge now listens, on behalf of the initiating host, on the indicated X.25 address.

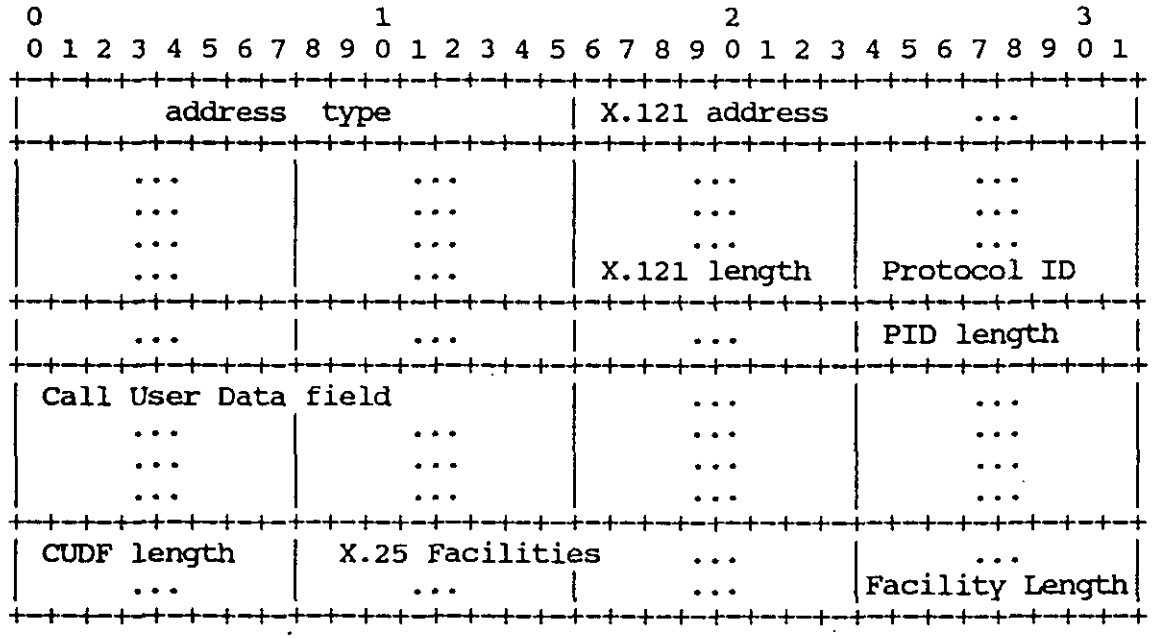
If an incoming call is received, a TCP connection is established to the corresponding TCP/IP address. If this connection is successful, then the connection establishment phase has succeeded and the data transfer phase is begun. If the connection fails, the incoming call is refused.

The TCP/IP connection between the initiating host and the TP0 bridge is a "heartbeat" connection for the registration function. If this connection closes, the TP0 bridge assumes hat the listening function has been terminated by the initiating host, and consequently, the TP0 bridge no longer listens for incoming calls

on the indicated X.25 address. If such a facility were not present, then the indicated X.25 address could not be recovered for reuse.

5. Format of X.25 Addresses

A standardized octet-encoding of X.25 addresses is used by the protocol described in this memo. The encoding has a fixed-length of 68 octets and contains 10 fields:



The fields are:

address type (2 octets) - a binary-encoded value in network order indicating the address type. The value 3 is used for X.25 addressing of this format.

X.121 address (16 octets) - the ascii-encoded value of the X.121 address.

address length (1 octet) - a binary-encoded value in network order indicating how many octets of the X.121 address are meaningful.

Protocol ID (4 octets) - meaningful at the remote system.

Protocol ID length (1 octet) - a binary-encoded value indicating the number of protocol ID octets are meaningful.

User Data (16 octets) - meaningful at the remote system.

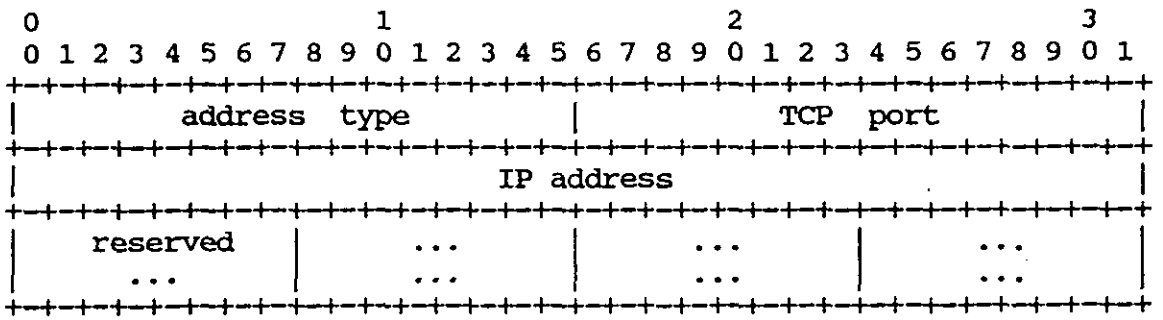
User Data Length (1 octet) - a binary-encoded value indicating the number of User Data octets are meaningful.

X.25 Facilities (6 octets) - meaningful at the remote system.

X.25 Facilities length (1 octet) - a binary-encoded value indicating the number of Facility octets are meaningful.

6. Format of TCP/IP Addresses

A standardized octet-encoding of TCP/IP addresses is used by the protocol described in this memo. The encoding has a fixed-length of 16 octets and contains 4 fields:



The fields are:

address type (2 octets) - a binary-encoded value in network order. The value 2 is used.

TCP port (2 octets) - a binary-encoded value in network order.

IP address (4 octets) - a binary-encoded value in network order.

reserved (16 octets) - null-value padding.

Comments

At present, the structure of the X.25 address and the internet address are rather ad-hoc and specific to the UNIX operating system. These structures may change in the future as experience is gained in the use of the TP0 bridge.

References

[ISO8072] Information processing systems -- Open systems interconnection, "Transport Service Definition", International Standard, June, 1985.

[ISO8073] Information processing systems -- Open systems interconnection, "Transport Protocol Specification", International Standard, July, 1986.

[ISO8208] Information processing systems, "X.25 package level protocol for data terminal equipment", Draft International Standard, July, 1985.

[ISO8878] Information processing systems -- Data communications, Use of X.25 to provide the OSI connection-mode network service", Draft International Standard, January, 1987.

[MIL1777] Military Standard 1777, "Internet Protocol".

[MIL1778] Military Standard 1778, "Transmission Control Protocol".

[RFC791] Postel, J., "Internet Protocol - DARPA Internet Program Protocol Specification", RFC 791, USC/ISI, September 1981.

[RFC793] Postel, J., "Transmission Control Protocol - DARPA Internet Program Protocol Specification", RFC 793, USC/ISI, September 1981.

[RFC983] Cass, D., and M. Rose, "ISO Transport Services on Top of the TCP", RFC 983, NTRC, April 1986.

[RFC1006] Rose, M., and D. Cass, "ISO Transport Service on Top of the TCP Version: 3", NTRC, May 1987.

[X.25] CCITT Recommendation X.25, "Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks," International Telegraph and Telephone Consultative Committee Yellow book, Vol. VIII.2, Geneva, 1981.

Authors' Addresses:

Julian P. Onions
Computer Science Department
Nottingham University
University Park
Nottingham, NG7 2RD
United Kingdom

EMail: JPO@CS.NOTT.AC.UK

Marshall Rose
The Wollongong Group
1129 San Antonio Road
Palo Alto, CA 94303

Phone: (415) 962-7100

EMail: mrose@TWG.COM

(This page intentionally left blank.)

MANDATORY APPENDIX D

DSN NO. 7 COMMON CHANNEL SIGNALING

SCOPE. This appendix specifies Defense Switched Network (DSN) No. 7 Common Channel Signaling.

GENERAL INFORMATION ON DSN No 7. The following DSN No. 7 specification is contained in Paragraph 7.8 of the Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR). The numbering and format from the GSCR have been retained for ease of use.

7.8 Common Channel Signaling-DSN No.7 CCS

7.8.1 ANSI T1.110.1 - Overview of the Signaling System. The DSN No.7 CCS conforms to the Signaling System Number 7 (SS7) overview provided in ANSI T1.110, Chapter 1. An overview of DSN specific requirements is provided in the following paragraphs, citing the applicable paragraphs of the standard, e.g., 1.0.

a. 1.0 Introduction. The DSN No.7 CCS network shall be compatible with the national signaling networks based on the ANSI T1.100 series of standards and shall be capable of interworking with networks based on SS7, as standardized internationally in the Blue Book (1988) by the International Telephone and Telegraph Consultative Committee (CCITT) (i.e., CCITT SS7).

The DSN No.7 CCS consists of the following American National Standard Institute (ANSI) communications protocols: (1) Message Transfer Part (MTP), (2) Signaling Connection Control Part (SCCP), (3) ISDN-User Part (ISDN-UP), (4) Transaction Capability Application Part (TCAP), (5) Monitoring and Measurements, and (6) Operation and Maintenance Application Part (OMAP). These protocols shall provide the capability necessary to meet DSN requirements for ISDN-based services, circuit-switched call control, and signaling network management.

b. 2.0 Scope, Purpose and Application

(1) 2.1 Objectives and Fields of Application

(a) Objectives. The objectives of the CCS No.7 implementation in DSN go beyond basic circuit-switched call control signaling. DSN No.7 CCS emphasizes supporting ISDN advanced capabilities. This support directly applies to the DSN management, administration, and operation applications, and lays the groundwork for the present and future requirements for information transfer in DSN. The general objective of DSN No.7 CCS system is to provide standardization of CCS No.7 system in the DSN.

The DSN-specific objective is to provide the universal signaling protocol for use throughout the entire DSN; Signaling Gateways within the DSN network between the major geographical areas will not be required.

It is anticipated that interconnections will be made with both public and military networks in the DSN host countries. Signaling Gateways may be required between the DSN and these interconnecting areas. These interface requirements shall be based on the DSN No.7 CCS protocol, DSN User-Network Signaling Protocol, and the DSN Interface Criteria.

(b) Applications. In general, the DSN No.7 CCS system meets DSN requirements for call control signaling of telecommunication services (such as telephone and circuit-switched data transmission services). It can also provide a reliable transport system for information transfer between exchanges and specialized centers in the DSN (e.g., for management and maintenance).

The system is optimized for operation over 64 kilobits per second (kb/s) digital channels and is suitable for use on point-to-point and point-to-multipoint terrestrial and satellite links. The DSN No.7 CCS system is intended to be implemented with components developed in commercial applications that follow the ANSI standards for CCS No.7. Specifically, DSN No.7 CCS applies the necessary protocols applicable to services essential for DSN, such as Multi-Level Precedence and Preemption (MLPP), Conferencing (i.e., Preset), Community of Interest, Management, and transfer of data different from signaling data.

(2) 2.2 General Characteristics. Critical characteristics for the DSN are operability and reliability. The DSN No.7 CCS standardizes a number of features contributing to high operability and reliability, such as decentralized distributed architecture, uniform management protocol, error detection and correction, redundancy of signaling links and nodes, and diversion of signaling traffic to alternative paths.

(3) 2.3 Modularity. DSN No.7 CCS is a subset of the modular structure of CCITT SS7. The following specifications represent the set of features standardized for DSN No.7 CCS in the DSN. They are derived from the ANSI standards for the U.S. SS7 system, which is one of a set of national standards based on CCITT. The CCITT SS7 includes a wide range of functions, of which the ANSI SS7 is a subset. The DSN No.7 CCS includes the ANSI SS7 features and extends to meet specific DSN requirements.

c. 3.0 Signaling System Structure

(1) 3.1 Basic Functional Division. The basic composition of functional blocks applicable to DSN No.7 CCS consists of the ANSI specified protocols, a subset of the functional blocks (protocols) found in the CCITT Blue Book (Q.700 series). These blocks are: MTP, ISDN-UP, SCCP, TCAP, OMAP, and Monitoring and Measurements. The fundamental principle of this structure is the division of the functions into the MTP and SCCP, which serve as transport systems for transfer of signaling messages, and the user parts--ISDN-UP, TCAP, OMAP and Monitoring and Measurements--which directly or indirectly utilize the capabilities provided by the MTP.

(2) 3.2 Functional Levels. The protocol needed for DSN No.7 CCS is compatible with the model specified by the ANSI

T1.110 standard, and can be related to the seven-layer Open System Interconnect (OSI) Reference Model (RM), as described in the above standard.

d. 4.0 DSN No.7 CCS Specification Guide

(1) 4.1 Support Information. The DSN No.7 CCS specifications are based on Issue 1 of ANSI SS7 Standards finalized in 1987 and 1988, plus the revisions being developed for Issue 2. The specifications are subdivided as shown in the following paragraphs. Each specification fully incorporates the applicable standard, except where explicitly noted in the subsections of the applicable specification. In these subsections, particular options, procedures, or parameters specific to the DSN are specified.

(2) 4.2 Message Transfer Part (MTP). The MTP of the DSN No.7 CCS shall be as specified in Section 7.8.2. The MTP Specification is subdivided into the following subsections, which correlate to chapters in ANSI T1.111: (1) 7.8.2.1, ANSI T1.111.1- Functional Description of the Signaling System Message Transfer Part (MTP); (2) 7.8.2.2, ANSI T1.111.2-Signaling Data Link; (3) 7.8.2.3, ANSI T1.111.3-Signaling Link (MTP); (4) 7.8.2.4, ANSI T1.111.4-Signaling Network Functions and Messages (MTP); (5) 7.8.2.5, ANSI T1.111.5-DSN Signaling Network Structure (MTP); (6) 7.8.2.6, ANSI T1.111.6-DSN Message Transfer Part Signaling Performance (MTP); (7) 7.8.2.7, ANSI T1.111.7-DSN Testing and Maintenance (MTP); and (8) 7.8.2.8 ANSI T1.111.8-Numbering of Signaling Point Codes (MTP).

(3) 4.3 Signaling Connection Control Part (SCCP). The SCCP of the DSN No.7 CCS shall be as specified in Section 7.8.3. The SCCP Specification is subdivided into the following subsections, which correlate to chapters in ANSI T1.112: (1) 7.8.3.1, ANSI T1.112.1-Functional Description Of The Signaling Connection Control Part (SCCP); (2) 7.8.3.2, ANSI T1.112.2-Definition and Function of SCCP Messages (SCCP); (3) 7.8.3.3, ANSI T1.112.3-SCCP Format and Codes (SCCP); and (4) 7.8.3.4, ANSI T1.112.4-Signaling Connection Control Part Procedures (SCCP).

(4) 4.4 Integrated Services Digital Network (ISDN) User Part (UP). The ISDN-UP of the DSN No.7 CCS shall be as specified in Section 7.8.4. The ISDN-UP Specification is subdivided into the following subsections, which correlate to chapters in ANSI T1.113: (1) 7.8.4.1, ANSI T1.113.1-Functional Description of ISDN User Part (ISDN-UP); (2) 7.8.4.2, ANSI T1.113.2-General Function Of Messages and Signals; (3) 7.8.4.3, ANSI T1.113.3-Formats and Codes; (4) 7.8.4.4, ANSI T1.113.4-Signaling Procedures; and (5) 7.8.4.5, ANSI T1.113.5-Performance Objectives In The ISDN Application.

(5) 4.5 Transaction Capabilities Application Part (TCAP). The TCAP of the DSN No.7 CCS shall be as specified in Section 7.8.5. The TCAP Specification is subdivided into the following subsections, which correlate to chapters in ANSI T1.114: (1) 7.8.5.1, ANSI T1.114.1-Functional Description and Transaction Capabilities (TCAP); (2) 7.8.5.2, ANSI T1.114.2-Definition and Function Of Transaction Capabilities Messages (TCAP); (3) 7.8.5.3, ANSI T1.114.3-TC Format and Codes (TCAP); and (4) 7.8.5.4, ANSI T1.114.4-Transaction Capability Procedure (TCAP).

(6) 4.6 DSN No.7 System Management. The DSN No.7 CCS Monitoring and Measurements shall be as specified in Section 7.8.6.1, ANSI T1.115-Monitoring and Measurements of SS7. The DSN No.7 CCS Operations, Maintenance and Administration Part (OMAP) shall be as specified in Section 7.8.6.2, ANSI T1.116-Operations, Maintenance and Administration Part (OMAP).

7.8.2 DSN No.7 CCS Message Transfer Part (MTP). The DSN No.7 CCS Message Transfer Part (MTP) shall be as specified in ANSI T1.111-1988, Chapters 1-8. Specific requirements for DSN application are given in the following subsections.

7.8.2.1 ANSI T1.111.1-Functional Description of the Signaling System Message Transfer Part (MTP). The Functional Description of the DSN No.7 CCS Message Transfer Part (MTP) shall be as specified in ANSI T1.111.1. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

a. 2.0 Signaling System Structure

(1) 2.2 Functional Levels

(a) 2.2.2 Signaling Data Link Functions (Level 1). The Signaling Data Link is a bidirectional digital transmission path comprised of digital signaling links. A maximum of 72 Digital Signaling Links* shall be supported at an individual DSN Signaling Point (SP). Because of its worldwide scope, the DSN No.7 shall support both terrestrial and satellite transmission for the Signaling Data Links at bit rates of 56 or 64 kb/s. These functions are specified in detail in ANSI T1.111.2.

*Note: A future expansion on the number of signaling links supported by a DSN SP is not prevented by this specification.

(b) 2.2.3 Signaling Link Functions (Level 2). The DSN Signaling Link Functions apply to both terrestrial and satellite transmission. These shall require the implementation of both types of error correction methods specified in Signaling System No.7: the Basic Error Correction method for use on

terrestrial Signaling Data Links and the Preventive Cyclic Retransmission method for use on Satellite Signaling Data Links. Detailed requirements are specified in ANSI T1.111.3.

(c) 2.2.4 Signaling Network Functions (Level 3). The DSN Signaling Network Functions include the Signaling Message Handling and Signaling Network Management requirements. The DSN network architecture imposes special requirements on the routing, addressing, and management of the CCS network. A detailed specification of signaling network functions is found in T1.111.4. Network testing information is found in T1.111.7.

b. 3.0 Signaling Network

(1) 3.1 DSN Basic Concepts and Features

(a) 3.1.2 Signaling Modes. The DSN Network structure is based on an associated architecture with decentralized STP capability. The signaling network replicates the connectivity of the switched network it serves. Each trunk group in the network is assigned one associated signaling channel. The associated mode of signaling is thus the first choice to establish a signaling relation between adjacent signaling points. The decentralized STP capability provides quasi-associated signaling as a backup to the associated signaling link in case of link failure or other unavailability, or as a second choice to establish adjacent signaling point signaling relations. Signaling relations between non-adjacent signaling points may be established by the Signaling Connection Control Part (SCCP).

One Signaling Data Link is required between any two adjacent signaling points. Backup to this signaling link is provided by utilizing a quasi-associated route until a new direct link is available. When a path for associated signaling fails, a procedure is started to restore the path by activating and switching into service a new circuit to perform as a Signaling Data Link. This concept results in an associated signaling network architecture with quasi-associated capability.

(b) 3.1.3 Signaling Point Modes. The common channel signaling equipment associated with each DSN nodal switch shall provide the functions of a Signaling Point (SP) and Signaling Transfer Point (STP), unless specifically noted otherwise. This is designated as a DSN SP/STP node. The DSN nodes, which do not include the STP function, are designated as DSN SP nodes. A DSN SP/STP node has the ability to originate signaling messages, to receive signaling messages from an origination signaling point (node), and to transfer signaling messages destined for another signaling point node. A DSN SP node without the STP capability can originate and receive

signaling messages only. Messages destined to other signaling points are never routed through a DSN SP-only node.

(c) 3.1.4 Message Labeling. The North American Routing Label, which is utilized in the DSN, is optimized for use with a quasi-associated, paired STP network architecture different from the DSN architecture. Section 7.8.2.4 specifies how the routing label is to be used in the DSN Network.

(2) 3.2 Signaling Message Handling Functions

(a) 3.2.1 Message Routing. Message routing is based on analysis of the routing label of the message in respect to predetermined routing data at a signaling point. This process provides a selection of succession of signaling links for each message-"message route" and/or succession of link sets-"signaling route." Each signaling message route in the DSN is predetermined and fixed at a given point in time. A message routed toward a specific destination in the DSN is always based on the associated signaling links. If the associated link is not available, quasi-associated routing is used based upon a predetermined selection of signaling links that support the first alternate trunk route. This selection proceeds through the remaining predetermined alternate circuit routes until an available supporting link is found.

DSN routing includes load sharing capability, allowing different portions of the signaling traffic sent to a particular destination to be distributed over two or more signaling links in a link set.

A service indicator included in each message provides the potential to use different routing plans for different user parts.

(b) 3.2.2 Message Distribution. Message Distribution is required at all DSN signaling nodes.

(c) 3.2.3 Message Discrimination. This function is not required at the DSN SP-only node.

(3) 3.3 Signaling Network Management Functions

(a) 3.3.2 Signaling Link Management. In the DSN, where the signaling links are also routed through the circuit switched channels, signaling link management requires DSN- specific implementation guidance.

(b) 3.3.3 Signaling Route Management. In the DSN this function is used for backup signaling and in cases where the primary associated signaling routes may present difficulties.

Implementation of this function in the DSN No.7 CCS requires DSN-specific implementation guidance.

(4) 3.4 Testing and Maintenance Functions. Testing and maintenance in the DSN environment is implementation-specific and requires DSN-specific implementation guidance.

(5) 3.5 Use of the Signaling Network

(a) 3.5.1 The DSN Signaling Network Structure. The DSN No.7 CCS system provision is planned to be based on associated signaling, supplemented by quasi-associated signaling. The DSN No.7 CCS is seen as a common resource that must meet DSN needs that go beyond each signaling relation. These needs will also require the DSN-specific implementation of quasi-associated signaling to allow the full potential of CCS No.7 to support the DSN communication needs.

(b) 3.5.2 Provision of Signaling Facilities. Redundancy is required within the DSN signaling network. The DSN-specific requirements are implementation dependent and shall be a part of the DSN No.7 CCS implementation guidance.

(c) 3.5.3 Application of Signaling Network Functions. These DSN No.7 CCS functions are a subset of the range of functions offered by the ANSI T1.111 standards. They will depend on the specific needs of the DSN subnetworks, which are spread over several geographical regions. The ANSI T1.111 standard provides for the DSN-preferred signaling modes, specific composition of SPs and STPs, and a degree of Level 3 use dictated by different implementations of DSN No.7 CCS.

7.8.2.2 ANSI T1.111.2-Signaling Data Link. The DSN No.7 CCS signaling data link shall be as specified in ANSI T1.111.2. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 1.0.

a. 1.0 General Information. The DSN No.7 CCS Signaling Data Link is derived from Pulse Code Modulation (PCM) multiplexed channels, circuit-switched transmission channels, and the digital streams of data circuits.

b. 4.0 Interface Specification Points

(1) 4.2 National/International Applications. The DSN Signaling Data Link shall conform to ANSI T1.111.2. A Signaling Data Link located entirely in North America, shall utilize the North American transmission and equipment standards, and require no framing or Law conversions if interfaced with other U.S. networks. A Signaling Data Links required to interwork with the links specified by CCITT will require conversion to be fully compatible.

(2) 4.4 Interface Requirements-Analog. Analog signaling is not required in the DSN; therefore, no interface requirements are specified.

c. 5.0 Digital Signaling Data Link. The DSN Digital Signaling Data Link is derived from the 1.544 or 2.048 Mb/s digital path. The latter is the case when the CCITT specified signaling link is required.

The DSN Signaling Data Link is derived from one of the trunk group circuits serving each pair of switching nodes. Access to the link in the DSN implementation shall be provided through the switching matrix. Semi-permanent switched connections shall be utilized in establishing the data link access.

A digital signaling data link shall be made up of digital transmission channels and digital switches or their terminating equipment, providing an interface to signaling terminals.

Selection of Digital Time Slots to serve as signaling channels must be coordinated between both ends of the Signaling Data Link. The order for the selection of backup signaling channels must be similarly coordinated.

d. 6.0 Analog Signaling Data Link. Analog signaling is not required in the DSN.

7.8.2.3 ANSI T1.111.3-Signaling Link (MTP). The DSN No.7 CCS Signaling Link functions and procedures shall be as specified in ANSI T1.111.3. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard (e.g., 5.0).

a. 5.0 Basic Error Correction Method. The DSN shall use the Basic Error Correction Method on links composed entirely of terrestrial transmission media, unless the Preventive Cyclic Retransmission (PCR) method is used as described in paragraph "b" below.

b. 6.0 Error Correction by Preventive Cyclic Retransmission (PCR). The DSN shall use the PCR method when a satellite path is used in a combined link. In the DSN regions where a satellite path is used as an alternate route, the specification does not preclude the use of the PCR for all the links in the region, terrestrial and satellite.

7.8.2.4 ANSI T1.111.4-Signaling Network Functions and Messages (MTP). The DSN No.7 CCS signaling network functions and messages shall be as specified in ANSI T1.111.4. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard (e.g., 2.0).

a. 2.0 Signaling Message Handling.

(1) 2.2 Routing Label. The DSN uses the U.S. National Routing Label structure (specified in ANSI T1.111.4) for signaling messages between DSN SPs. The Routing Label shall also be used for routing signaling messages to other U.S. networks that comply with the ANSI SS7 Standard. The U.S. Routing Label is adapted for use in the DSN architecture according to the DSN Signaling Point Code Allocation Plan as specified in Section 7.8.2.8. The DSN Routing Label shall comply with the routing label structure for U.S. networks as shown in Figures 3A and 3B/T1.111.4.

The Network Cluster Member Subfield is assigned by the DSN Network Administrator to identify individual SP/STP as the DSN nodes. When used in this manner, the Cluster Member Subfield code 00000000 is reserved for addressing the DSN SP/STPs.

The Cluster Subfield may also be assigned to a selection of DSN SP nodes to be identified as a group. When utilized in this second manner, the Cluster Member Subfield may, for example, identify a cluster of DSN SP only nodes connected to a single DSN SP/STP or identify all signaling points in a particular geographic area or country. These particular instances of assignments do not limit the implementation of the DSN routing label in specific geographic regions.

The Signaling Link Selection (SLS) Field identifies the link set and individual signaling data link to be utilized as a message between two DSN signaling points. Use of the SLS Field in the DSN is affected by the DSN associated Network architecture and is specified in Section 7.8.2.5.

Interconnection between the DSN and non-U.S. signaling network may require use of the international routing label at the point of interconnection. The requirements for this use and the label translation shall be determined on a case-by-case basis as part of the interconnection agreement.

(2) 2.3 Message Routing Function

(a) 2.3.1 Signaling Link Selection. The message routing function provides rules for selection of a signaling link for an outgoing message. In DSN No.7 CCS, an outgoing link is a part of combined link set that directly connects two DSN signaling nodes. The link set is determined by the Destination Point Code (DPC) in the message routing label; the particular link is determined on the basis of the Signaling Link Selection (SLS) field.

1. DSN Link Set. A link set in the DSN consists of a collection of signaling links that directly connect

two DSN signaling nodes. The associated mode architecture of the DSN requires one signaling link set between any two directly-connected DSN switching center nodes. These DSN Link Sets are categorized at each signaling point as either a Normal Link Set, Current Link Set, or Alternative Link Set. Either a combined or a single link set is implemented between adjacent DSN signaling nodes.

2. Normal Link Set. The Normal Link Set provides the associated link that directly connects two adjacent DSN signaling nodes. This link set is assigned the highest priority and is always chosen by the routing functions when it is available.

3. Alternative Link Sets. Alternative Link Sets are utilized in the DSN to provide backup quasi-associated signaling capability when the associated signaling link (or a higher priority alternative link set) is unavailable. The priority assigned to the selection of alternative signaling links corresponds to the priority of the alternative routing selection in the circuit-switched network routing table. That is, the alternative signaling link set of the first alternative route for a circuit-switched call is assigned next in priority after the Normal Link set. This process of assignment continues until all Alternative Link Set priorities are assigned.

4. Current Link Set. The Current Link Set is the link set currently assigned to convey signaling messages to a particular destination signaling point. This link set should normally correspond to the current highest priority of link set availability.

5. DSN Signaling Links. The associated mode architecture of the DSN requires an active signaling data link between any two directly connected (adjacent) DSN switching center nodes. Backup is provided by inactive signaling data links, redundancy in signaling terminals, and switched access to other circuits normally used for other purposes (e.g., voice circuits). Automatic allocation of signaling terminals and signaling data links according to the Signaling Network Management procedures of ANSI T1.111.4 generally shall be provided.

(b) 2.3.3 Specifics of DSN Signaling Message Routing. Each DSN SP/STP shall have routing tables that determine the Signaling Link Set and a Signaling Link to be used to convey signaling messages for each Destination Point Code. These tables shall indicate the Current Link Set in use to each DSN destination. Use of associated and quasi-associated signaling is mandated by procedures in the MTP that will provide a signaling relation to all signaling points in the network.

A key requirement is to simplify administration of the DSN SP/STP and DSN SP routing functions. The associated architecture of the DSN allows the signaling routing table to replicate the circuit-switched routing table. That is, for circuit-related calls, selection of an outgoing circuit is translated into selection of the current link set serving that destination point code. The signaling link set selected usually will correspond to the Normal (Associated) Link Set for that destination. When the Normal Link Set is unavailable, the indication is given of the highest Priority Alternative Link Set available.

Signaling for non-circuit-related purposes shall perform the same translation to the Current Link Set based upon the DPC.

A means shall be provided to reconfigure signaling routing changes in response to changes made to the circuit-switched call routing. Such reconfigurations may consist of the addition and deletion of routes, or changes to the priorities of alternate routes. These updates shall be in agreement with local coordination between the DSN Generic Switching Center and its common channel signaling equipment to ensure the transfer of circuit-switched and signaling routing information.

Agreement between the circuit-switched (call) routing and signaling routing tables does not require that the signaling data must follow the circuit-switched call route. This means that the signaling links associated with the adjacent switch's inter-exchange circuits are designated as part of the Normal Link Set (Highest Priority) for that destination. Alternate routes to that destination in the call routing plan are assigned to the Alternative Link Sets, which may be used for signaling to that destination according to their priority. The Current Link Set for signaling is chosen according to the availability of the Normal and the Alternative Link Sets. For example, a call may use a direct trunk circuit between two switches; however, a failure in the Normal Link Set may require use of quasi-associated signaling over an Alternative Link Set.

This procedure is intended to ensure that the prioritization of call routes and signaling routes is identical. The actual routes selected to serve the call and signaling may differ depending upon availability.

The following procedure is used to select a signaling route. As the DPC of the signaling message is determined, a circuit-related call destination is determined by the designation of the outgoing circuit. The DPC is translated into the link set available at the highest priority. An individual signaling link within the Current Link Set is chosen based on the SLS code.

(c) 2.3.5 Handling Messages Under Signaling Time Congestion. Each message is assigned one of four levels of priority, from 0 (the lowest) to 3 (the highest level). Priorities are assigned by the message's generating user part and are taken into consideration by the congestion control to determine whether a message should be discarded under signaling link congestion conditions. The highest priority is assigned to signaling network management messages (priority 3). Priorities are assigned to categories of messages in the DSN; they could be dynamically reassigned under DSN-specific requirements. For example, the priority 2 assigned to the IAM with the precedence Flash and Flash Override and the priority 1 assigned to the IAM with the Immediate must be recognized under congestion conditions in the DSN and at the boundaries with other networks.

(3) 2.4 Message Discrimination and Distribution Functions. The Message Discrimination function examines the Destination Point Code of a received signaling message to determine whether or not it is destined to the receiving SP. This function is required in every DSN signaling node equipped with an STP. Message Distribution determines to which user of the MTP a received signaling message will be directed. This function is also required in all DSN signaling nodes.

b. 3.0 Signaling Network Management

(1) 3.6 Signaling Network Congestion (and Priority Levels). Signaling links and signaling link sets determine the network overall operability during network element congestion. Criteria for the determination of DSN signaling congestion status shall be as specified by ANSI T1.111.4, Section 3.6 for U.S. networks. In case of congestion, IAMs carrying FLASH or FLASH OVERRIDE calls shall be assigned Level 2 and IMMEDIATE calls shall be assigned level 1 in the DSN.

c. 6.0 Changeback

(1) 6.3 Sequence Control Procedure. The Sequence Control Procedure is not used in the DSN.

(2) 6.4 Time-Controlled Diversion Procedure. DSN No.7 CCS uses the Time-Controlled Diversion procedure for changeover since specifics of the DSN No.7 CCS architecture permit communication with the remote signaling point via a signaling link that became available. As sending of the changeback declaration is impossible when changeback is initiated, the changeback initiating signaling point stops the traffic to be diverted and stores it in a "changeback buffer" for a time T3, then reopens the traffic on the signaling link made available.

d. 11.0 DSN Signaling Link Management. There are three signaling link management methods specified in ANSI T1.111.4. The automatic allocation of signaling data links and signaling terminals shall be the method implemented in the DSN.

e. 12.0 DSN Signaling Route Management

(1) 12.1 General. The Signaling Route Management procedures are required to control signaling routes in the DSN nodes implemented with the SP/STP function. However, both DSN SP and SP/STP nodes shall be capable of responding appropriately to the receipt of Signaling Route Management messages. For example, a DSN SP node may be required to alter its routing information in response to a Transfer Prohibited, Restricted, or Allowed message.

The DSN use of Transfer Cluster Prohibited, Transfer Cluster Allowed, or Transfer Cluster Restricted procedures may be allowed by the DSN No.7 CCS specifications. Due to the limited initial use of quasi-associated signaling and clustering, these procedures are viewed as a future enhancement that shall not be precluded by the current implementations.

(2) 12.7 Transfer Controlled Procedure. Transfer Controlled is initiated at a DSN SP/STP node to notify one or more originating signaling points that they should no longer send messages to a destination with a give priority or lower. The Transfer Controlled message is sent in response to receipt of a signaling message, the priority of which is less than the current link congestion status. Suggested timer values shall initially be implemented. The DSN Network Administrator shall have control over timer values to accommodate specific DSN application requirements. A means to control timer value settings shall be provided.

f. 13.0 Common Characteristics of Message Unit (MSU) Formats

(1) 13.2 Service Information Octet. The Service Information Octet of the MSU contains the service indicator and the subservice field. The subservice field is used to distinguish between internationally coded messages and messages coded according to the DSN standard and also contains an indication of the message priority levels.

(a) 13.2.1 Service Indicator. Not all coded users of the MTP are accommodated by DSN No.7. A listing of the service indicator codings and their current DSN implementation status is shown in the following:

D C B A		DSN
0 0 0 0	Signaling network management messages	YES
0 0 0 1	Signaling network testing and maintenance regular messages	YES
0 0 1 0	Signaling network testing and maintenance special messages	YES
0 0 1 1	SCCP	YES
0 1 0 0	Telephone User Part	NO
0 1 0 1	ISDN User Part	YES
0 1 1 0	Data User Part (call and circuit related messages)	NO
0 1 1 1	Data User Part (facility registration and cancellation messages)	NO
1 0 0 0	Spare	
1 0 0 1	Spare	
1 0 1 0	Spare	
1 0 1 1	Spare	
1 1 0 0	Spare	
1 1 0 1	Reserved for DSN only use	
1 1 1 0	Reserved for DSN only use	
1 1 1 1	Spare	

(b) 13.2.2 Subservice Field. The DSN shall use the network code (10) as specified in ANSI T1.111.4. DSN messages originating and terminating within the DSN or another network conforming to the ANSI standard shall also be coded with the National Network code (10).

DSN interconnections with international networks, via gateways or other methods, are a subject of separate specifications and agreements with the networks and countries concerned. Whether the international or other network indicator is used will be specified as a part of that agreement.

Priority 3 is the highest message priority code and is reserved for network management and other messages critical to the performance of the MTP. Assignment of priority levels to other messages and user parts shall be in accordance with the DSN specific guidelines. The IAM messages that carry the FLASH and FLASH OVERRIDE precedence levels are assigned the priority 2. The IAM messages with the IMMEDIATE are assigned the priority 1. The PRIORITY and ROUTINE precedence levels are at the 0 priority. This priority shall not be changed if a DSN call must cross the network boundaries. However, it is subject to bilateral agreements negotiated with other network providers. The DSN Network Administrator shall have the ability to assign and change priority levels for messages of specific user parts within the DSN and to agree with interconnecting networks for messages that enter and leave the DSN.

g. 14.0 Formats and Codes of DSN Signaling Network Management Messages. The following paragraphs specify DSN requirements for the formats and codes of DSN Signaling Network Management Messages.

(1) The Signal Link Code (SLC), used to identify one of 16 possible signaling links between each pair of adjacent (directly connected) signaling nodes, indicates the identity of a signaling link to which a network management message pertains.

(2) Each adjacent DSN SP pair shall coordinate the assignment of SLCs to ensure compatibility.

(3) The SLC may be used in the DSN to identify the preferred order of signaling data link selection from among the inter-exchange circuits. Normally, one associated signaling link between two DSN signaling points will be implemented and designated with an SLC at both ends of 0000. The order of selection of backup signaling data links to be obtained from the inter-exchange circuit group may be pre-coordinated and prioritized at both ends. SLC 0001 is assigned to the circuit normally selected first as a backup signaling link. The remaining SLCs are assigned to inter-exchange circuits in the order of their selection as signaling data links. This order of selection should not be interpreted as prioritizing the signaling links. Any circuit selected to serve as a signaling link remains in service for that purpose until it becomes unavailable (e.g., by failure or management withdrawal, etc.)

(4) This pre-assignment can be overridden when communication between both DSN signaling points over alternative links is possible. In this case, a Signaling Data Link Connection Order message may be utilized to indicate which inter-exchange circuit will be assigned as a signaling data link and which corresponding SLC will be used.

7.8.2.5 ANSI T1.111.5-DSN Signaling Network Structure (MTP). The DSN No.7 CCS Signaling Network Structure shall be as specified in ANSI T1.111.5. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 1.0.

a. 1.0 Scope, Purpose, and Application. The DSN No.7 CCS network shall serve as a totally separate call control and management network that is overlaid on the DSN circuit- switched network. DSN signaling points connected by signaling links shall interface with DSN switch processors to provide the necessary messages and procedures to control voice and data related connections.

The DSN signaling network consists of SPs and SP/STPs colocated with DSN multi-function switches and interconnected by a network of signaling links. The DSN Signaling Network concept is based upon a fully-associated architecture. It consists of origination and destination SPs connected by signaling links which are capable of sharing the load between them. It is supplemented by quasi-associated signaling routes in which the information between origination and destination points may be transferred via a number of STPs. This architecture differs from the examples of a centralized paired-STP architecture shown in ANSI T1.111.5. The DSN architecture is built upon associated signaling links supplemented by a large number of dispersed (decentralized) STPs.

The DSN architecture, while different from commercial architectures based on the quasi-associated principles, is not in violation of ANSI T1.111.5. The major DSN No.7 CCS components are signaling points, signaling transfer points, and signaling links that are in compliance with the ANSI standard. The remainder of this section specifies DSN applications of these components in the signaling network.

b. 2.0 Signaling Network Components. This section describes the signaling network structure and individual components: the SP, the SP colocated with an STP, and a network of signaling links arranged in an associated network architecture.

(1) 2.1 Signaling Links. A DSN Signaling Link is a basic component that connects signaling points in a signaling network. The signaling links encompass the "level 2" functions that are specified in ANSI T1.111.3.

A signaling link connecting two signaling points shall correspond to the inter-exchange circuits connecting adjacent DSN switches in the circuit-switched network.

The associated architecture of the DSN requires one directly-connected active signaling link set between any two DSN switching centers. This link is drawn from one of the inter-exchange circuits serving these two switching locations. The remaining inter-exchange circuits (up to 15) may be used as backup signaling links and for the purposes of load sharing. They are considered to be inactive signaling links under normal circumstances and could be made available for a different purpose (e.g., voice transmission).

The signaling links directly connecting two DSN switches in the network constitute a single signaling link set.

Parallel signaling link sets (combined link sets) shall not be precluded by implementations.

(2) 2.2 Signaling Points. The typical signaling component installed at DSN switches shall consist of a SP colocated with an STP (SP/STP), unless specifically stated otherwise. The SP/STP shall serve as signaling message origination, transfer point, and destination point.

The signaling component that has been specifically stated as not requiring the STP function shall consist of an SP only. These DSN SPs shall serve as origination and destination points for signaling messages, but not as transfer points.

Typical locations of DSN SPs without the STP capability will be switches that connect to either a single switch or a very limited number of adjacent DSN switches.

The switches limited to the SP capability do not provide alternate routing for another switch served by common channel signaling. Upgrade of a DSN SP to a DSN SP/STP should not be precluded by the SP implementation.

As a minimum, a single signaling link shall exist between every adjacent switch in the DSN backbone network. Up to 16 inter-exchange circuits to the adjacent switches are available in DSN No.7 CCS.

All of the DSN backbone switches are considered to be network SPs. Each SP and SP/STP shall be assigned a unique signaling point code for addressing signaling messages.

SPs and SP/STPs shall interface directly to the DSN switch processor. The DSN SP only nodes shall provide at least two of the level 3 functions: 1) the message distribution function, which delivers a received message to the appropriate user part or to the local MTP levels of the home SP; and 2) the routing function, which makes a choice of an outgoing signaling link that routes a message to a destination SP.

The DSN network concept is based on the decentralization and dispersion of STP capability throughout the signaling network. This concept requires STPs to be colocated with most DSN switch signaling points.

As described above, an SP/STP is used for quasi-associated backup of an unavailable associated route. Under the DSN concept, a quasi-associated link cannot be used for backup of another quasi-associated unavailable route.

The STP capability in the DSN requires at least two of the level 3 functions to be present: message discrimination function and message routing function. The discrimination function allows the DSN to determine that a message is destined to another STP. It

initiates the routing function which selects an outgoing signaling link.

Figure 1, Typical DSN SP/STP Location shows a typical network configuration with primary and alternate signaling routes for setting up calls from A to B. The nodes represent both circuit switches and signaling nodes. A and B are adjacent switches connected by associated signal links that form the normal or primary route. Most calls under normal conditions will flow over this route. When all trunks/links on the normal route are busy, calls from A to B are set up over the alternate nodes..

The failure of any signal link shall be backed up with the DSN quasi-associated capability. For example, quasi-associated signaling route (shown in Figure 1, Typical DSN SP/STP Location) provides a backup capability for the failed associated signaling link between A and B. Calls will be set up over the A to B trunk circuits. For this to work, the node at C must have the STP capability, where a call from A to B may be set up via the C signaling node without being routed through switch C.

Any DSN signaling point that is a part of a backup signaling route for two adjacent DSN signaling points must be an SP/STP. In order to allow future upgrading of the DSN network, all DSN SPs shall have the potential to be upgraded to a DSN SP/STP.

c. 3.0 Structural Division of DSN Signaling Network (National and International Requirements). The worldwide signaling network outside the DSN network consists of two functionally independent levels: the international level and the national level. The overall DSN structure reflected by the signaling network management and the numbering plans of signaling points provides the network with the capability to function on both the national and the international levels. A DSN SP/STP shall be assigned to one of two categories:

(1) A node that functions as an ANSI specified (T1.111.5) national signaling point (signaling transfer point). This type belongs to the DSN signaling network only and is identified by a signaling point code [Originating Point Code (OPC) or DPC] according to the DSN numbering plan of signaling points

(2) A node that functions both as an international signaling point (signaling transfer point), and a DSN signaling point (signaling transfer point), and therefore belongs to both the DSN and the international signaling network, and is identified by a specific signaling point code (OPC or DPC) in each of the signaling networks accordingly.

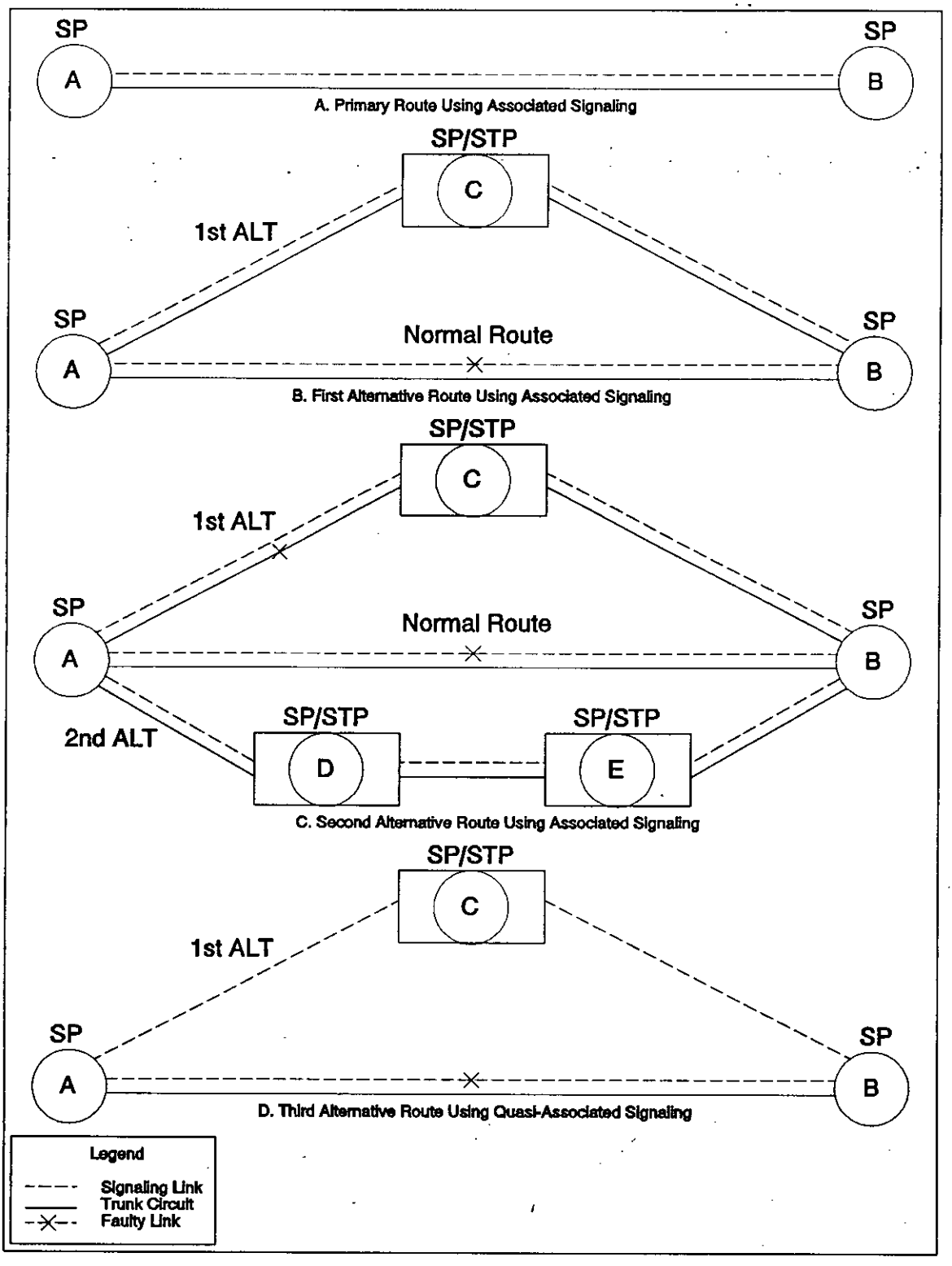


Figure 1. Typical DSN SP/STP Location

d. 4.0 Considerations Common to Both International and National Signaling Networks

(1) 4.4 Number of Signaling Links Used in Load Sharing. Load sharing among parallel link sets is not precluded by this specification if the parallel sets (combined link sets) are implemented in DSN No.7 CCS. If implemented, the number of signaling links used in load sharing is implementation dependent, and shall be part of the DSN No.7 implementation guidance.

(2) 4.5 Satellite Link Use. The DSN circuit switched backbone shall encompass satellite routes. Calls traversing different calling areas could encounter several satellite circuits. The DSN Satellite Link Use is for further Study.

e. 6.A Signaling Network for Internetwork Traffic

(1) 6A.1 General. The traffic between DSN SP/STPs requires extended protocol capabilities (to be defined) to provide for appropriate monitoring and measurements. Unlike the national networks specified in the corresponding section of the ANSI Standard, the DSN network employs associated signaling with quasi-associated capabilities. Based on this architecture, the internetwork traffic requirements for the DSN network are different. The internetwork traffic requirements are specified in the following paragraphs.

(2) 6A.2 Integrated Numbering of National Signaling Networks. Signaling Gateways are not required within the DSN because DSN No.7 CCS operates under a uniform protocol throughout all DSN areas. Gateways may become a requirement to interconnect the DSN with other international CCITT No.7 networks. This can only be determined by agreement with each interconnecting network.

(3) 6A.5 Routing in the Absence of Failures. The SLC bit rotation procedure used for load sharing in the U.S. national networks shall be implemented in the DSN network only for load sharing within the link set.

f. 7.0 DSN Signaling Network Framework. The DSN network shall employ "F" links to connect every SP and SP/STP together. These "F" links shall provide the associated architecture of the DSN. That is, every pair of directly connected (adjacent) DSN switches shall be connected by an "F" type of associated signaling link (Figure 2, F-links).

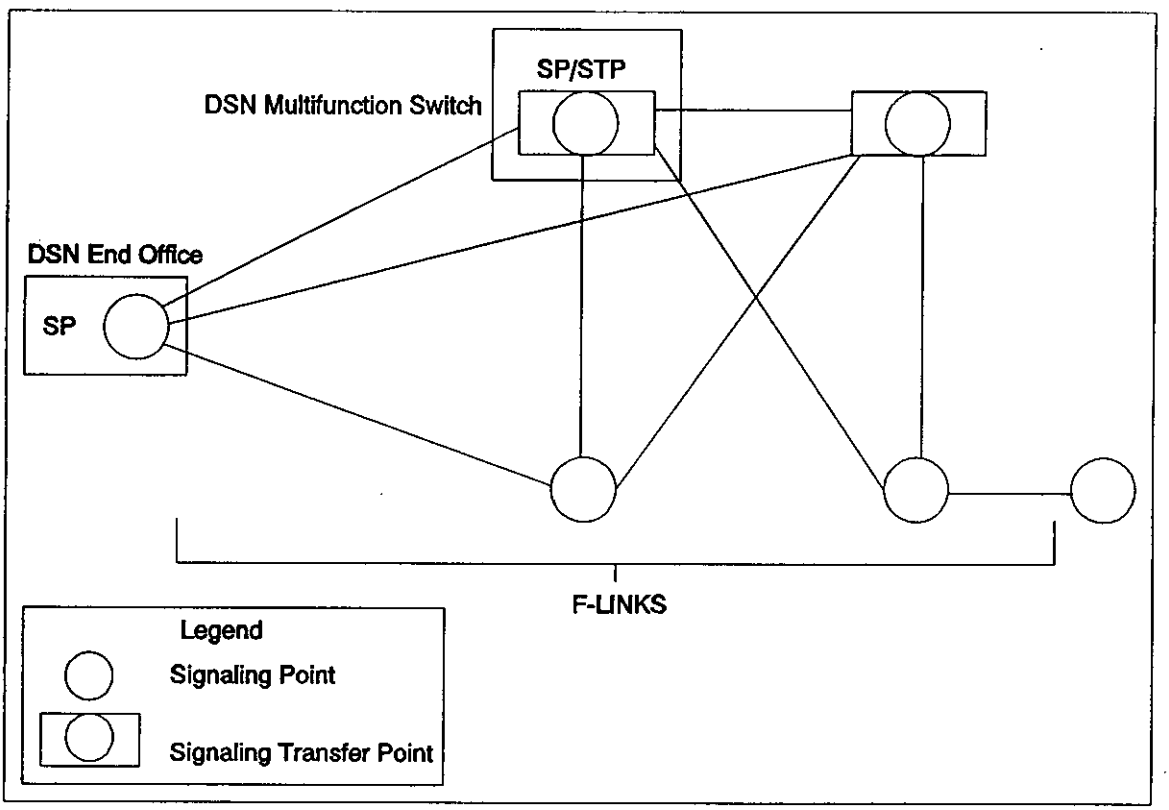


Figure 2. F-Links

These signaling links may also carry signaling traffic that is characteristic of other types of signaling links. For example, when quasi-associated backup signaling is employed, the "F" signaling link will logically appear to be an "A" link providing access from a SP to a STP. Similarly, an "F" between two DSN SP/STPs could in some cases carry quasi-associated signaling between the two STPs and appear as a logical "B" link. Similar examples can be stated where the DSN "F" link carries traffic that will provide the logical appearance of "D" and "E" type links. Because the DSN SP/STPs do not operate in mated pairs, no "C" link implementations will occur in the DSN.

7.8.2.6 ANSI T1.111.6-DSN Message Transfer Part Signaling Performance (MTP). The DSN No.7 CCS requirements and guidelines for the MTP signaling performance shall be as specified in ANSI T1.111.6.

7.8.2.7 ANSI T1.111.7-DSN Testing and Maintenance (MTP). The DSN No.7 CCS Testing and Maintenance requirements shall be as specified in ANSI T1.111.7.

7.8.2.8 ANSI T1.111.8-Numbering of Signaling Point Codes (MTP). The DSN No.7 Numbering of Signaling Point Codes shall be as specified in ANSI T1.111.8. The DSN meets the ANSI requirements for a large network and has been granted a network code value of 241. ANSI T1.111.8, Table B1, shows the current list of assigned large network codes. Signaling point codes in the DSN are assigned by the Network Administrator in accordance with ANSI guidelines.

7.8.3 Signaling Connection Control Part (SCCP). The DSN No.7 CCS SCCP shall be as specified in ANSI T1.112-1988, Chapters 1-4. Specific requirements for DSN application are given in the following subsections.

7.8.3.1 ANSI T1.112.1-Functional Description of the Signaling Connection Control Part. The DSN No.7 CCS SCCP functional description shall be as specified in ANSI T1.112.1. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

a. 2.0 Services Provided by the SCCP. The SCCP provides additional functions to the MTP to provide both connectionless as well as connection oriented network services to transfer circuit related and noncircuit-related signaling information and other types of information between exchanges. The connectionless services requires a function which maps the called address to Signaling Point Codes of the MTP-Service. This function shall be provided within each DSN No.7 CCS node. (See ANSI T1.112.1 Section 2.2).

7.8.3.2 ANSI T1.112.2-Definition and Function of SCCP Messages. The definition and function of DSN No.7 CCS SCCP messages shall be as specified in ANSI T1.112.2.

7.8.3.3 ANSI T1.112.3-SCCP Format and Codes. The DSN No.7 CCS SCCP formats and codes shall be as specified in ANSI T1.112.3.

7.8.3.4 ANSI T1.112.4-Signaling Connection Control Part Procedure. The DSN No.7 CCS SCCP procedures shall be as specified in ANSI T1.112.4. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

a. 2.0 Addressing and Routing

(1) SCCP Routing Principles. The SCCP Routing Control (SCRC) shall be required to translate a calling party address from PC + SSN to GT.

b. 5.0 SCCP Management Procedures. SCCP management procedures defines how replicated nodes or subsystems may relate. Within DSN, nodes/subsystems shall operate in the dominate role, which is consistent with the philosophy of main-associated and backup-quasi-associated signaling.

7.8.4 DSN No.7 CCS Integrated Services Digital Network User Part (ISDN-UP). The DSN No.7 CCS ISDN-UP shall be as specified in ANSI T1.113-1990, Chapters 1-5. Specific requirements for DSN application are given in the following subsections.

7.8.4.1 ANSI T1.113.1-Functional Descriptions of ISDN User Part (ISDN-UP). The DSN No.7 CCS ISDN-UP functional description shall be as specified in ANSI T1.113.1-1990. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 1.0.

a. 1.0 Scope, Purpose, and Application. The ISDN-UP specifies the signaling functions, codes, messages, and procedures needed to provide services for circuit-switched voice and data services in the DSN. The ISDN-UP serves analog, digital, mixed analog/digital, and ISDN Networks. The broad applicational base of the ISDN-UP provides accommodation for the evolution of the DSN from an analog to an all digital network.

b. 2.0 Services Supported By The ISDN User Part. In addition to the basic service and the non-ISDN supplementary services specified in the standard, the Multi-Level Precedence and Preemption service, as specified in T1.619, is mandatory.

c. 4.0 End-To-End Signaling. End-to-end signaling transports signaling information between the end points of a circuit-switched connection or between any two points in the

signaling network. Both end-to-end signaling methods (i.e., pass along and SCCP) shall be supported in DSN No.7 CCS.

7.8.4.2 ANSI T1.113.2-General Function of Messages and Signals. The DSN No.7 CCS ISDN-UP general functional of messages and signals shall be as specified in ANSI T1.113.2-1990. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 1.0.

a. 1.0 Signaling Messages. The signaling messages available for DSN No.7 are specified in ANSI T1.113.2-1990. Table 2/T1.113.2 lists the ISDN-UP messages and their acronyms. These messages could be divided into several categories with respect to their functional content pertinent to connection setup, operations, supervision, tests, and maintenance.

b. 2.0 Signaling Information. Signaling information is identified in subsections 2.1 through 2.77. The following has specific DSN comments:

(1) 2.41 End-to-End Method Indicator. In the DSN both the SCCP and the Pass Along methods shall be available.

7.8.4.3 ANSI T1.113.3-Formats and Codes. The DSN No.7 CCS ISDN-UP Formats and Codes shall be as specified in ANSI T1.113.3-1990. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 3.0.

a. 3.0 ISDN-UP Parameters. The format of the various ISDN-UP parameters are given in subsections 3.1 through 3.33 of the ANSI standard, all of which are applicable to the DSN. The following has specific DSN comments:

(1) Precedence Parameter. In the DSN No.7 System, a Precedence parameter of one octet in length shall be used in the Initial Address Message to indicate the precedence level, service domain, and LFB status of each call. Table I provides the DSN No.7 CCS system coding for each subfield.

7.8.4.4 ANSI T1.113.4-Signaling Procedures. The DSN No.7 CCS ISDN-UP Signaling Procedures shall be as specified in ANSI T1.113.4-1990. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

Table I. Precedence Parameter

PRECEDENCE PARAMETER	
SUBFIELDS	DSN NO. 7 CODING
PRECEDENCE LEVEL	BITS 3-1
FLASH OVERIDE (0)	0 0 0
FLASH (1)	0 0 1
IMMEDIATE (2)	0 1 0
PRIORITY (3)	0 1 1
ROUTINE (4)	1 0 0
	*
MLPP SERVICE DOMAINS	BITS 6-4
DSN	0 0 0
	*
LFB STATUS	BITS 7-8
LFB ALLOWED	0 0
LFB NOT ALLOWED	1 0
PATH RESERVED	0 1

* all other values are spare

a. 2.0 Basic Call Control and Signaling Procedures.

(1) 2.1.1.1 Actions Required at Originating Exchange. Routing information in the DSN shall be supplied by the originating exchange. However, the design shall not preclude requests to a remote database for routing information.

b. Multilevel Precedence and Preemption. Multi-level Precedence and Preemption (MLPP) Service provides a set of optional call handling procedures for use in an ISDN network. These procedures are applicable to any network that provides the MLPP capability. Utilization of MLPP procedures provides essentially nonblocking service to very high priority users. This ensures the ability to communicate during network congestion periods. The ISDN-UP signaling procedures for the MLPP Service are covered in T1.619.

7.8.4.5 ANSI T1.113.5-Performance Objectives in the ISDN Application. The DSN No.7 CCS performance requirements for an ISDN application shall be as specified in ANSI T1.113.5.

7.8.5 Transaction Capability Application Part (TCAP). The DSN No.7 CCS TCAP shall be as specified in ANSI T1.114-1990, Chapters 1-5. Specific requirements for DSN application are given in the following subsections.

7.8.5.1 ANSI T1.114.1-Functional Description and Transaction Capabilities. The DSN No.7 CCS Transaction Capabilities shall be as specified in ANSI T1.114.1-1990.

7.8.5.2 ANSI T1.114.2-Definition and Functions of Transaction Capabilities Messages. The elements and functions of DSN No.7 CCS TCAP messages shall be as specified in ANSI T1.114.2-1990.

7.8.5.3 ANSI T1.114.3-TC Format and Codes. The DSN No.7 CCS formats and encodings for TCAP messages shall be as specified in ANSI T1.114.3-1990.

7.8.5.4 ANSI T1.114.4-Transaction Capability Procedure. The DSN No.7 CCS TCAP procedures shall be as specified in ANSI T1.114.4-1990.

7.8.5.5 ANSI T1.114.5-Definitions of Operations, Parameters and Error Codes. The DSN No.7 CCS functions and encoding for the Operation, Parameter and Error Code elements used by the TCAP protocol shall be as specified in ANSI T1.114.5-1990. DSN specific requirements not covered by the standards are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

a. 2.0 Operations

(1) 2.1.1 Parameter Family Identifier - 0000001. This indicates that the following operations on Parameters is to be performed. In DSN No.7 CCS the Parameter - Provide Value Specifier - 00000001, is used in the MLPP service for the Look-ahead for busy option that will determine if circuits are available before action is taken to preempt the call. The operation of this parameter is used to indicate that the values in the Parameters identified in the Parameter Set are to be provided. In the case of MLPP service, this operation specifies the following mandatory parameters:

(a) The Look-ahead For Busy Response*

(b) Bearer Capability Supported*

(c) The Service Key which encompasses the following:

-- The Called Party number
-- The Calling Party number
-- The Circuit Identification Code*
-- The Bearer Capability Requested
-- The Precedence*
-- The Call Reference.*

When the operation is performed successfully, a Return Result with the following parameters are returned:

-- The Look-ahead for Busy Response*
-- The Bearer Capability Supported*

If the operation cannot be performed, the Return Error cause may be one of the following:

-- Unexpected Data Value-if the argument of the operation is not as expected
-- Data Unavailable-if the data identified was not available
-- Task Refused-if the entity is unable to do the task at this time.

* These parameters are either not in T1.114.5 or must be modified. See paragraph 7.8.5.5 (b) for details.

b. 4.0 Parameters Several Parameters needed to support the MLPP Service are not yet fully defined in T1.114.5-1990. The DSN-specific Parameters are specified in the following paragraphs, citing the applicable sections in the standard if they exist:

(1) 4.19 Bearer Capability Requested - 10010010. The Bearer Capability Requested parameter is used to indicate the Bearer Capability requested by the calling party. It is coded contextual (in the context of the Parameter Set) and has a primitive form. The format and contents of the Bearer Capability Requested parameter is provided in T1.114.5

(2) 4.20 Bearer Capability Supported - 10010011. This parameter indicates whether or not a requested bearer capability is supported and is used to indicate the reason a bearer capability requested was not available. The format of the Bearer Capability Supported parameter is illustrated in Figure 3/T1.114.5. The contents of this Parameter are defined and coded as follows:

(a) 00000001 - Bearer Capability is not supported

(b) 00000010 - Bearer Capability is supported

(c) 00000011 - Bearer Capability is not authorized

(d) 00000100 - Bearer Capability is not presently available

(e) 00000101 - Bearer Capability is not implemented

(3) Look-ahead for Busy Response - XXXXXXXX. The Look- ahead For Busy Response Parameter is used to indicate whether the preemptable resources were found. The parameter is coded contextual. It is 1 octet long and is of type OCTET STRING. Its format is illustrated in Figure 3. The contents of are defined and coded as follows:

	H	G	F	E	D	C	B	A
Look-ahead For Busy Response	X	X	Spare		X	X	X	X

The Look-ahead for busy response length is one octet.

The location field is coded as follows:

Location	D	C	B	A
User	0	0	0	0
Private Network Serving the Local User	0	0	0	1
Public Network Serving the Local User	0	0	1	0
Transit Network	0	0	1	1
Public Network Service the Remote User	0	1	0	0
Private Network Serving the Remote User	0	1	0	1
Local Interface Controlled by this Signaling Link	0	1	1	0
International Network	0	1	1	1
Beyond an Interworking Point	1	0	1	0
All other values are reserved				

The Acknowledgement Type field is coded as follows:

Acknowledgement Type	H	G
Path Reservation Denied	0	0
Negative Acknowledgement	0	1
Positive Acknowledgement	1	0
Spare	1	1

Figure 3. Look-ahead For Busy Response

(a) Location. Bits DCBA indicate the location which initiated the response and are defined and coded as follows:

0000 - User
0001 - Private network serving the local user
0010 - Public network serving the local user
0011 - Transit network
0100 - Public network serving the remote user
0101 - Private network serving the remote user
0110 - Local interface controlled by this signaling link
0111 - International network
1010 - Beyond an interworking point
All other values are spare.

(b) Acknowledgement Type. Bits HG indicate the acknowledgement type. This indicates whether the request for search and reservation of circuits was accepted. Bits HG are defined and coded as follows:

00 - Path reservation is denied
01 - Negative acknowledgement
10 - Positive acknowledgement
11 - Spare.

(4) Circuit Identification Code - XXXXXXXX. The Circuit Identification Code Parameter is used to identify the physical path between two exchanges. The parameter is coded contextual, is 2 octets in length and is of type OCTET STRING. The format and coding is as described in T1.113.3 Section 1.2.

(5) Precedence - XXXXXXXX. The Precedence Parameter is used to identify the MLPP call in terms of priority treatment and MLPP Service Domain. It is of variable length and is of the type OCTET STRING. The format is illustrated in Figure 4 and the contents are coded as follows:

First octet - Bits DCBA indicate the Precedence Level and are coded as follows:

(a) 0 0 0 0 - FLASH OVERRIDE(0)
(b) 0 0 0 1 - FLASH(1)
(c) 0 0 1 0 - IMMEDIATE(2)
(d) 0 0 1 1 - PRIORITY(3)
(e) 0 1 0 0 - ROUTINE(4).
Bits GFE are spare
Bit H is extension indicator

	H	G	F	E	D	C	B	A
Precedence	ext	Spare			X	X	X	X
Domain	ext	X	X	X	X	X	X	X

The precedence parameter length is 2 octet.

The precedence octet is coded as follows:

Location	D	C	B	A
Flash Override (0)	0	0	0	0
Flash (1)	0	0	0	1
Immediate (2)	0	0	1	0
Priority (3)	0	0	1	1
Routine (4)	0	1	0	0

The MLPP Service Domain octet is coded as follows:

MLPP Service Domain	G	F	E	D	C	B	A
Defense Switched Network	0	0	0	0	0	0	0
Spare	0	0	0	0	0	0	1
	To						
	1	1	1	1	1	1	1

Figure 4. Precedence Format

Second octet - Bits GFEDCBA indicate an identity of the MLPP service domain and are coded as follows:

(a) 0 0 0 0 0 0 0 - Defense Switched Network
All other values are spare.
Bit H is extension bit

(6) Call Reference - XXXXXXXX. The Call Reference Parameter is used to identify a particular MLPP call within an exchange independent of the physical circuits. The parameter is 6 octets in length and is of type OCTET STRING. The format contents are as specified in Section 3.5 and Figure 7 in T1.113.3.

7.8.6 DSN No.7 CCS Management. The DSN No.7 Management specifications shall be as specified in Sections 7.8.6.1 and 7.8.6.2.

7.8.6.1 ANSI T1.115-Monitoring and Measurements of SS7. DSN No.7 CCS Monitoring and Measurements shall be as specified in ANSI T1.115.

7.8.6.2 ANSI T1.116-Operations, Maintenance and Administration Part (OMAP). The DSN No.7 CCS Operations, Maintenance and Administration Part shall be as specified in ANSI T1.116. DSN specific requirements are specified in the following paragraphs, citing the applicable sections of the standard, e.g., 2.0.

a. 2.0 Operations and Maintenance Procedures for the Signaling Network

(1) 2.3.2 Screening. Both options of screening shall be available in the DSN.

(2) 2.5.4.2.3 Duplex Translation. This option is not supported in the DSN.

KEY WORD LISTING

The following key words, phrases, and acronyms apply to MIL-STD-187-700:

Asynchronous transfer mode

Broadband ISDN

Circuit-switched networks

Defense Data Network

Distributed queue dual bus

Digital subscriber signaling system number 1

Fiber Distributed Data Interface

GOSIP

Hypothetical reference circuit

ISDN

Local area network

Metropolitan area network

Multi-level precedence and preemption

Military Message Handling System

Military messaging system

Network management

Packet-switched network

Personal telecommunications service

Switched multi-megabit data service

Synchronous optical hierarchy

Synchronous optical network

Signaling system number 7

Tactical-to-strategic interface

Wide area network

(This page intentionally left blank.)

CONCLUDING MATERIAL

Custodians:

Army - CR

Navy - EC

Air Force - 90

DISA-DC

NSA-NS

Preparing Activity:

DISA (JIEO) - DC

(Project SLHC-7000)

Review Activities:

Army - CR, SC

Navy - EC, MC

Air Force - 02, 13, 17, 18, 19, 90, 93

NSA - NS

DISA - DC

User Activities:

Army - CR, SC

Navy - EC, MC, SH, AS

Air Force - 13, 17, 18, 19, 90, 93

DISA

NSA

Civilian Agency Coordinating Activities:

NCS

(This page intentionally left blank.)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-STD-187-700	2. DOCUMENT DATE (YYMMDD) 920601

3. DOCUMENT TITLE

Interop. & Performance Stds. for the Defense Info Sys.

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (Last, First, Middle Initial)	b. ORGANIZATION	
c. ADDRESS (Include Zip Code)	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON (If applicable)	7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME Director Joint Interoperability and Engineering	b. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON
c. ADDRESS (Include Zip Code) Organization (JIEO) ATTN: TBBB Fort Monmouth, NJ 07[illegible]	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340