NEMA TS*3.3 96 6470247 0509554 821

NEMA STANDARDS PUBLICATION NO. TS 3.3

NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (NTCIP) CLASS B PROFILE

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

NEMA Standards Publication TS 3.3-1996

NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (NTCIP) CLASS B PROFILE

Published by

National Electrical Manufacturers Association
1300 N. 17th Street
Rosslyn, Virginia 22209

©1996 by National Electrical Manufacturers Association

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

CONTENTS

Page

Foreword iii

Section 1 GENERAL

1.1 Scope 1
1.2 References 1
1.2.1 Normative References 1
1.2.2 Other References 3
1.3 Networking Related Definitions 4
1.4 Serial Interface Related Terms 6
1.5 Abbreviations and Acronyms 7

Section 2 CLASS B PROFILE OVERVIEW

2.1 General Aspects 9
2.2 The Class B Profile Layers 14
2.2.1 Physical Layer 14
2.2.2 Data Link Layer 15
2.2.3 Bit Error Rate 18
2.2.4 Network Layer 18
2.2.5 Transport Layer 19
2.2.6 Session Layer 19
2.2.7 Presentation Layer 19
2.2.8 Application Layer 19
2.2.9 Management Information Base (MIB) 20
2.2.10 Simple Network Management Protocol (SNMP) 20
2.2.11 Simple Transportation Management Protocol (STMP) 21
2.2.12 Information Registration Authority Hierarchy 22
2.2.13 Object Management 23
2.2.14 NTCIP Managed Objects 24
2.2.15 Device and Application Specific Managed Objects 24
2.2.16 Traffic Controller Managed Objects 24
2.2.17 Dynamic Objects 25
2.3 Conformance and Protocol Implementation Conformance Statement (PICS) 25

Section 3 DATA TRANSPORT ASPECTS

3.1 General Protocol Aspects 27
3.1.1 Protocol Stacks and Conformance 27
3.1.2 Descriptive Technique for Service Definitions 27
3.2 Physical Layer Definition 27
3.2.1 Scope 27
3.2.2 EIA/TIA-232-E Interface 28
3.2.3 FSK Modem Interface 28
3.3 Data Link Layer Definition 29
3.3.1 Scope 29
3.3.2 Data Link Layer Service Definition 30
3.3.3 Data Link Layer Protocol 30
3.3.4 Mapping of Protocol to Service 33

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

3.4 Network Layer Definition 33
3.4.1 Scope 33
3.4.2 Protocol Identification 34
3.4.3 Network Layer Service Definition 34
3.4.4 Network Layer Protocol 35
3.4.5 Mapping of Protocol to Service 35
3.5 Transport Layer Definition 35

Section 4 DATA PROCESSING ASPECTS

4.1 Session Layer Definition 37
4.2 Presentation Layer Definition 37
4.3 Application Layer Definition 37
4.3.1 Scope 37
4.3.2 General 37
4.3.3 Application Layer Service Definition 38
4.3.4 Application Layer Protocol 38
4.3.5 Mapping of Service to Protocol 38
4.4 Conformances 38

Annex A FSK MODEM INTERFACE TIMING ANALYSIS 39

Annex B CLASS B PROFILE MIB 41

B.1. Overview 41
B.2. Class B MIB Definition 41
B.3. MIB Compliance 43
B.4. Agent Capabilities MIB 45

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

This document provides an introduction, outline, and definition of the National Transportation Communications for ITS Protocol—Class B Profile. It is intended as a communications protocol standard for interconnecting transportation and traffic control equipment. NTCIP represents a suite of protocols and information management standards that apply to the entire industry. The Class B Profile addresses the need for a specific protocol that is geared to the communications requirements of field devices such as traffic controllers, variable message signs, camera controllers, and other similar devices. It is, by design, capable of being implemented in current, state-of-the-art field devices that are part of traffic control or traffic management systems.

The genesis of NTCIP began with the NEMA TS 2 Standard for traffic control hardware and a desire to cover the more complex issues of systems interoperability and communications standards. The initial goal was to develop a common protocol and define a minimum set of control and status messages so that end users could intermix controllers from different manufacturers on a single system. Over time, the scope of NTCIP was broadened to include not just NEMA and 170 Type controllers, but all other field related devices. It currently is being extended to cover traffic management and control center communications. The ultimate goal is to define standard protocols for all aspects of communications for transportation and traffic control networks that are needed for ITS. The Class B Profile is just one set of protocols in the NTCIP suite.

A communications protocol allows devices to talk to one another. Other NEMA standards ensure that they speak a common language. A major portion of the NTCIP development has been spent on defining the structure and identification of information that will be conveyed by the communication protocols. A message must be understood by the device it was intended for. It is also equally important that it not be misunderstood by some other device that shares the network interface. An integral part of the Class B Profile is the Simple Transportation Management Framework. It defines the procedures for that ensuring that any devices can use the Class B communications protocols.

The text of the material presented as mandatory requirements is NEMA Standard. Other information (non-mandatory references) is Authorized Engineering Information. The definition of both types of these NEMA Standards is listed.

In the preparation of this Standards Publication, input of users and other interested parties has been sought and evaluated. Inquiries, comments, and proposed or recommended revisions should be submitted to:

Vice President Engineering
National Electrical Manufacturers Association
1300 North 17th Street
Rosslyn, Virginia 22209

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

This standard publication was developed by the Transportation Management Systems and Associated Control Devices section of the National Electrical Manufacturers Association. Section approval of the standard does not necessarily imply that all section members voted for its approval or participated in its development. At the time it was approved, the Transportation Management Sytems and Associated Control Devices section had the following members.

ADDCO Manufacturing Co.—St. Paul, MN
American Electric Sign—Spokane, WA
Automatic Signal/Eagle Signal Corporation—Austin, TX
BI Tran Systems, Inc.—Sacramento, CA
Cylink Cooperation—Sunnyvale, CA
Eberle Design, Inc.—Phoenix, AZ
Econolite Control Products, Inc.—Anaheim, CA
Fiberoptic Display Systems, Inc.—Smithfield, RI
Intersection Development Corp.—Fullerton, CA
ITS Product Group—Ormond Beach, FL
McCain Traffic Supply, Inc.—Vista, CA
P B Farradyne Inc.—Rockville, MD
Peek Traffic - Transyt—Tallahassee, FL
Rockwell Automation—Mayfield Heights, OH
Skyline Products, Inc.—Colorado Springs, CO
3M Traffic Control Systems—St Paul, MN
Traffic Sensor Corp.—Corona, CA
Vultron, Inc.—Rochester Hills, MI

Motivation

As transportation control equipment became more sophisticated, planners, users, and equipment manufacturers recognized the need to establish system inter-operability and integration standards. Different manufacturers and agencies defined protocols to work with their specific hardware, but a problem arose when there were attempts to enhance operation or integrate additional hardware into a system. There was no common protocol with which the equipment could communicate since the various systems utilized different protocols and messaging techniques.

The problem was exemplified by considering just the integration issues related to traffic signal controllers. There was no standardized method to communicate with either NEMA type controllers or 170 type controllers. In systems that used a remote communications unit to interface with the input/output backpanel signals of the controllers, severe limitations were imposed on the capabilities of the system. Alternatively, when systems from different manufacturers were integrated into the same central control system, the communications protocol to each system was both different and manufacturer specific. Local controller units operating within the system normally had to be from the same manufacturer of the system.

The integration problem was compounded when existing systems were tied into transportation management systems. Not only did these systems have to deal with traffic controllers, but also with such devices as surveillance cameras, variable message signs, and other ITS related hardware. All of this equipment should have been able to share the same communications channel and not interfere with each other. Industry wide communications standards were needed not just for connectivity and inter-operability reasons but also to accommodate future technology growth. As the needs of ITS became clearer, the ability to transfer data throughout the system was crucial. This Standard needed to accommodate these recognized needs as well as the yet undefined needs of the future.

Purpose

The purpose of this document is to provide an introduction, overview, and definition of the *National Transportation Control for ITS Communications Protocol Standard (NTCIP) Class B Profile.* Whereas

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

NTCIP is a set of communications protocols for integrating all of the various ITS components, the Class B Profile is specifically tailored to meet the requirements of field equipment. Unlike typical central computer hardware, field equipment may have limited hardware resources and not need to support all the features of a fully interconnected system. For example, an isolated arterial master system would need to pass information between the master and controller. There may not be a requirement to pass information from the controller through the master to a TMC. The Class B Profile is an easy to implement, low overhead protocol that provides inter-operability and the inter-changability of transportation and traffic control equipment. It is specifically designed to be compatible with other NTCIP Profiles that address the inter-networking aspects of data communications.

Section 2 of this document provides an overview of the Class B Profile. In addition to highlighting the protocol to be used, it also provides a background on the traffic control and ITS environment. This includes the various topologies in which communications are to take place and the resulting requirements that NTCIP addresses. The reader may refer to TS 3.1 for more detailed information. Section 3 provides the definition of the data transport aspects of the NTCIP Class B Profile. These are the formats and procedures needed to establish communications and move data between devices that share a single communications channel. Section 4 provides the definition of the data processing aspects of the NTCIP Class B Profile. This section deals with the issues of how the end application interfaces with the communications application layer, converting end application data into a form suitable for transmission, and interfacing with the lower layers. The end application messages that are be used to control, monitor, and manage the traffic control and transportation related devices are covered in separate NEMA TS 3 documents.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Section 1
GENERAL

1.1 SCOPE

The Class B Profile Standard establishes a common method of interconnecting ITS field equipment such as traffic controllers and variable message signs (VMS), defines the protocol and procedures for establishing communications between those components, and references common data sets to be used by all such equipment. Its application is intended for equipment sharing a single communications channel or subnetwork (subnet). The Class B Profile is just one part of NTCIP. NTCIP is a suite of protocols and standards that address all different aspects of transportation and traffic control communications. The Class B Profile addresses the need for a common field device communications standard. It establishes a method for interconnecting field devices, defines the protocol and procedures to establish communications link between them, and defines a common set of operation information variables.

1.2 REFERENCES

1.2.1 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. While end users of the NTCIP Class B Protocol do not need to obtain these documents, they do provide a complete understanding of the protocol. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Contact information regarding the referenced standards is given at the end of this section.

Electronic Industries Association
Engineering Department
2500 Wilson Blvd.
Arlington, VA 22201-3834

EIA /TIA-232-E-1991, *Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange.*

ANSI
11 West 42nd Street, 13th Floor
New York, New York 10036

ISO/IEC 3309:1994, *Information Technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Frame structure*

ISO/IEC 4335:1994, *Information Technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Elements of procedures*

ISO/IEC 7498-1:1994, *Information Technology—Open Systems Interconnection—Basic reference model: The basic model*

ISO/IEC 7498-4:1994, *Information Technology—Open Systems Interconnection—Basic reference model—Part 4: Management framework*

ISO/IEC 7809:1994, *Information Technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Classes of procedures*

ISO/IEC 8348: 1993, *Information Technology—Open Systems Interconnection—Network service definition*

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 8824-1:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Specification of Basic Notation*

ISO/IEC 8824-2:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Information Object Specification*

ISO/IEC 8824-3:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Constraint Specification*

ISO/IEC 8824-4:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Parametrization of ASN.1 Specifications*

ISO/IEC 8825-1:1995, Information Technology—Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (BER)

ISO/IEC 8886:1992, *Information Technology—Telecommunications and information exchange between systems—Data link service definition for Open Systems Interconnection*

ISO/IEC 11575, *Information Technology—Telecommunications and information exchange between systems—Protocol mapping for the OSI Data Link service*

DDN Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets.* K. McCloghrie; M. Rose; 05/10/1990

RFC 1157, *A Simple Network Management Protocol (SNMP).* M. Schoffstall; M. Feder; J. Davin; J. Case; 05/10/1990

RFC 1212, *Concise MIB Definitions.* K. McCloghrie; M. Rose; 03/26/1991

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II,* K. McCloghrie; M. Rose; TCP/IP-base

RFC 1317, *Definitions of Managed Objects for RS-232-like Hardware Devices,* B. Stewart, 04/16/1992

Motorola / Universal Data Systems
5000 Bradford Drive
Huntsville, Alabama 35805

Bell 202T, *Data Sets 202S and 202T Interface Specification,* American Telephone and Telegraph, 1978

International Telecommunications Union
Place des Nations
CH-1211
Geneva 20
Switzerland

CCITT Recommendation X.212 (1988), *Data Link service definition for Open Systems Interconnection for CCITT applications*

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

CCITT Recommendation X.213 (1992) | ISO/IEC 8348:1992, *Information technology—Network service definition for Open Systems Interconnection*

ITU-T Recommendation X.210 | ISO/IEC 10731, *Information technology—Open Systems Interconnection—Conventions for the definition of OSI services*

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209

NEMA TS 3.2, *National Transportation Communications for ITS Protocol (NTCIP) Simple Transportation Management Framework*

1.2.2 Other References

The following list of documents may also be applicable to NTCIP or are referenced by documents listed in 1.2.

ANSI
11 West 42nd Street, 13th Floor
New York, New York 10036

ISO/IEC 2382-9: 1995, *Data Processing—Vocabulary—Part 09: Data Communication*

ISO/IEC 7478: 1987, *Information Processing Systems—Data communication—Multilink procedures*

ISO/IEC 8072: 1994, *Information Processing Systems—Open Systems Interconnection—Transport Service Definition*

ISO/IEC 8471: 1987, *Information Processing Systems—Data communication—High-level data link control balanced classes of procedures—Data link layer address resolution/negotiation in switched environments*

ISO/IEC 8880-2: 1992, *Information Technology—Data Communications—Protocol combinations to provide and support the OSI network service—Part 2: Provision and support of the connection-mode network service*

ISO/IEC 8885:1991 (E), *Information technology—Telecommunications and information exchange between systems—High-level data link control (HDLC) procedures—General purpose XID frame information field content and format*

DDN Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

RFC 1214, *OSI Internet Management: Management Information Base*, L. Labarre, 04/05/1991

RFC 1229, *Extensions to the Generic-Interface MIB*, K. McCloghrie, 08/03/1992 (Historic)

RFC 1238, *CLNS MIB—for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)*, G. Satz, 06/25/1991 (Experimental)

RFC 1304, *Definitions of Managed Objects for the SIP Interface Type*, T. Cox, K. Tesink, 02/28/1992

RFC 1316, *Definitions of Managed Objects for Character Stream Devices*, B. Stewart, 04/16/1992

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

RFC 1414, *Indent MIB*, M. St. Johns, M. Rose, 02/04/1993

RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1442, *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1443, *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1444, *Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

1.3 NETWORKING RELATED TERMS

application services: The services collectively offered by the upper four layers of the OSI model.

Applications Programmer Interface: A set of calling conventions defining how a service is invoked through a software package.

authentication: The process whereby a message is associated with a particular originating entity.

authorization: The process whereby an access policy determines whether an entity is allowed to perform an operation.

Basic Encoding Rules: The OSI language for describing transfer syntax.

broadcast address: An address referring to all stations on a medium.

checksum: An arithmetic sum used to verify data integrity.

cyclic redundancy checking: A polynomial division algorithm used to verify data integrity.

data: Information before it is interpreted.

data link layer: That portion of an OSI system responsible for transmission, framing, and error control over a single communications link.

datagram: A self-contained unit of data transmitted independently of other datagrams.

end-to-end services: The services collectively offered by the lower three layers of the OSI model.

gateway: a router; also, (imprecise usage) an entity responsible for complex topology mappings.

hardware address: The address of a physical interface.

host: (Internet usage) An end-system's application.

Intelligent Transportation Systems: A major national initiative to improve information, communication and control technologies in order to improve the efficiency of surface transportation.

Intelligent Vehicle Highway System: Obsolete term. See Intelligent Transportation Systems.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

intermediate system: A network device performing functions from the lower three layers of the OSI model. Intermediate systems are commonly thought of as routing data for end-systems.

International Organization for Standardization: An international standards organization. ANSI is the primary interface to ISO within the US. Often thought to be International Standards Organization because of the usage ISO for short.

Internet: A large collection of connected networks, primarily in the United States, running the Internet suite of protocols. Sometimes referred to as the *DARPA Internet, NSF/DARPA, Internet,* or the *Federal Research Internet.*

internet layer: The layer in the Internet suite of protocols responsible for providing transparency over both the topology of the internet and the transmission media used in each physical network.

Internet Protocol: The network protocol offering a connection-less mode network service in the Internet suite of protocols.

Internet suite of protocols: A collection of computer-communication protocols original developed under DARPA sponsorship.

IP address: A 32-bit quantity used to represent a point of attachment in an internet.

Local Area Network: Any one of a number of technologies providing high speed, low-latency transfer and being limited in geographic size.

Management Information Base: A collection of objects that can be accessed via a network management protocol. See Structure of Management Information.

network: A collection of sub-networks connected by intermediate-systems and populated by end-systems.

network layer: That portion of an OSI system responsible for data transfer across the network, independent of both the media comprising the underlying subnetworks and the topology of those subnetworks.

network management: The technology used to manage in a network. Usually referring to the management of networking specific devices such as routers. In the context of this document, refers to all devices including end systems that are present on the network or inter-network.

Open Systems Interconnection: an international effort to facilitate communications among computers of different manufacture and technology.

physical layer: That portion of an OSI system responsible for the electro-mechanical interface to the communications media.

port number: Identifies an application-entity to a transport service in the Internet suite of protocols. The concept of ports are often present in OSI literature, however, ports are not internetwork standard, but exists as local network conventions only.

presentation layer: That portion of an OSI system responsible for adding structure to the units of data that are exchanged.

protocol data unit: A data object exchanged by protocol machines, usually containing both protocol control information and user-data.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

prototype: The object type corresponding to an instance (management usage).

retransmission: The process of repeatedly sending a unit of data while waiting for an acknowledgment.

router: A level-3 (network layer) relay.

service primitive: An artifact modeling how a service is requested or accepted by a user.

session layer: That portion of an OSI system responsible for adding control mechanisms to the data exchange.

socket: A pairing of an IP address and a port number.

subnet: A physical network within a network on which all devices share the same physical media.

subnetwork: See subnet.

system management: The OSI equivalent of network management.

Transmission Control Protocol: The transport protocol offering a connection-oriented transport service in the Internet suite of protocols.

transport layer: That portion of an OSI system responsible for reliability and multiplexing of data transfer across the network (over and above that provided by the network layer) to the level required by the application.

transportation management: Short for the management of networks of transportation devices and the network itself.

transportation network: A network of transportation devices. Usually in the context of transportation management.

upper-layer protocol number: Identifies a transport entity to the IP.

User Datagram Protocol: The transport protocol offering a connection-less mode transport service in the Internet suite of protocols.

user data: Conceptually, the part of a protocol data unit used to transparently communicate information between the users of the protocol. Prefixed by the protocol control information.

wide area network: any one of a number of technologies providing geographically distant transfer.

1.4 SERIAL INTERFACE RELATED TERMS

These terms define the nomenclature frequently used in regard to the EIA/TIA-232 interfaces and modems.

ASCII: American Standard Code for Information Interchange. A 7-bit binary code representation of letters, numbers and special characters. It is universally supported in computer data transfer.

asynchronous: Data transmission in which the actual data is preceded by a start bit and followed by a stop bit since the time between transmitted characters varies.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

baud rate: The number of discrete signal events per second occurring on a communications channel. It is often referred to as bits per second (BPS) which is technically inaccurate but widely accepted.

bit: Binary Digit. A single basic computer signal consisting of a value of 0 or 1, off or on.

byte: A group of bits acted upon as a group, which may have a readable ASCII value as a letter or number or some other coded meaning to the computer. It is commonly used to refer to 8-bit groups.

carrier: A continuous frequency capable of being either modulated or impressed with another information-carrying signal. Carriers are generated and maintained by modems via the transmission lines of the telephone companies.

CRC: Cyclical Redundancy Check. An error-detection technique consisting of a cyclic algorithm performed on each "block" of data at the sending and receiving end of the transmission. As each block is received, the CRC value is checked against the CRC value sent along with the block.

DTE: Data Terminal Equipment. The device that is the originator or destination of the data sent by a modem.

DTR: Data Terminal Ready. A signal generated by most modems indicating a connection between the DTE (computer) and the modem. When DTR is "high" the computer is connected.

data transmission protocols: These are standards for modulation and transmission of data at various speeds. The standards are Bell 103 & V.21 for 300bps, Bell 202T, Bell 212A, and V.22 for 1200bps, V.22bis for 2400bps, V.32 for 9600bps and V.32 bis for 14,400bps. Proprietary protocols are also used extensively for higher baud rates.

echo: The display of transmitted data on a local display. See also full and half duplex below.

flow control: A mechanism that compensates for differences in the flow of data to and output from a modem or computer. Either hardware or software can be used for this control to prevent data loss. Hardware flow control using the modem makes use of a buffer to store data to be sent and data received. Flow control is necessary if the Communications port is locked at a higher rate than the connection rate.

full duplex: Signal flow in both directions at the same time. It is sometimes used to refer to the suppression of online LOCAL ECHO and allowing the remote system to provide a REMOTE ECHO.

half duplex: Signal flow in both directions, but only one way at a time. It is sometimes used to refer to activation of LOCAL ECHO which causes a copy of sent data to be displayed on the sending display.

parity: An error detection method used in both communications and computer memory checking to determine character validity. Communications now makes use of more efficient cyclic redundancy checking algorithms.

protocol: A system of rules and procedures governing communications between two devices. File transfer protocols in your communications program refer to a set of rules governing how error checking will be performed on blocks of data.

1.5 ABBREVIATIONS AND ACRONYMS

ANSI—American National Standards Institute
ASN.1—Abstract Syntax Notation One
ATMS—Advanced Traffic Management System
BER—Basic Encoding Rules in the context of the Application Layer. Bit Error Rate in the context of the Data Link Layer.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

CCITT—International Consultative Committee on Telephone and Telegraphy
CCITT—International Telegraph and Telephone Consultative Committee
CLNS—Connectionless-mode Network Service
CONS—Connection Oriented Network Service
CRC—Cyclic Redundancy Check
DARPA—Defense Advanced Research Projects Agency
DCE—Data Circuit Terminating Equipment
DLSAP—Data Link Service Access Point
DLSDU—Data Link Service Data Unit
DTE—Data Terminal Equipment
EIA—Electronic Industries Association
FCS—Frame Check Sequence
FHWA—Federal Highway Administration
FSK—Frequency Shift Keying
FTP—File Transfer Protocol
HDLC—High-level Data Link Control
IANA—Internet Assigned Numbers Authority
IEC—International Electrotechnical Commission
IETF—Internet Engineering Task Force
IP—Internet Protocol
IPI—Initial Protocol Identifier
ISO—International Organization for Standardization
ITS—Intelligent Transportation Systems
ITU-T—International Telecommunications Union, Telecommunications Sector
IVHS—Intelligent Vehicle Highway System
LAN—Local Area Network
LLC—Logical Link Control
MIB—Management Information Base
NEMA—National Electrical Manufacturers Association
NSDU—Network Service Data Unit
OSI—Open Systems Interconnection
PDU—Protocol Data Unit
PER—Packed Encoding Rules
PICS—Protocol Implementation Conformance Statement
RFC—Request for Comment
RM-OSI—Reference Model OSI
SAP—Service Access Point
SDLC—Synchronous Data Link Control
SDU—Service Data Unit
SNMP—Simple Network Management Protocol
STMP—Simple Transportation Management Protocol
STMF—Simple Transportation Management Framework
STMI—Structure and Identification of Transportation Management Information
TIA—Telecommunications Industries Association
TCP—Transmission Control Protocol
TMC—Traffic Management Center
TMIB—Transportation MIB
UCC—Unbalanced Connectionless Class
UDP—User Datagram Protocol
UI—Unnumbered Information (Frame)
UP—Unnumbered Poll (Frame)
VMS—Variable Message Sign

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Section 2
CLASS B PROFILE OVERVIEW

2.1 GENERAL ASPECTS

The NTCIP Class B Profile defines a set of communication protocols to be used in field devices and their management systems that are part of an integrated transportation system. The profile provides for exchange of information between a primary station and each secondary station on a particular communications channel or subnet. The profile sets forth standards to allow devices to share a common interconnect, establish a common language for them to communicate with, and to define the structure under which the data in these devices is structured and managed. It does not address the need for the exchange of information between devices on different subnets.

NTCIP was originally conceived to be an extension of NEMA TS 2 covering traffic controller communications. The NEMA traffic control equipment manufacturers recognized that for true hardware inter-changeability the Standard had to cover the more complex issues of systems inter-operability and communications standards. As word of the NEMA development work spread out into the traffic control community, a general industry forum evolved. Representatives from the user community, consultants, and non-NEMA manufacturers participated in the talks. With the participation of other component manufacturers, NTCIP was moving towards a true traffic control industry wide standard. As consensus grew, the Federal Highway Administration (FHWA) brought to the table the concerns of Intelligent Transportation Systems (ITS, formerly IVHS) planners.

For ITS to be a reality, all the components that make up the traffic and transportation monitoring and control community must be able to communicate with a common or at least understandable language. The words that are spoken must have a clear and unambiguous meaning to everyone. The NTCIP development participants, started out defining a language and the words needed for a traffic controller and extended it to not only include traffic controllers and related devices but also traffic management centers (TMC). It has been further refined into an "open" set of protocols to that meet the diverse needs of ITS.

This openness is achieved by embracing features of several existing worldwide communications standards established by the International Organization for Standardization (ISO), the International Telecommunications Union, Telecommunications Sector (ITU-T; formerly CCITT), and the Internet Engineering Task Force (IETF). These standards map into the ISO Open Systems Interconnect Reference Model (OSI Model) which deals with how information can be passed through the various processing layers in an open system. The OSI Model breaks down the aspects of communications into seven layers or discrete functions to reduce complexity. Each layer is built upon its predecessor[1]. These seven layers are shown in Figure 2-1.

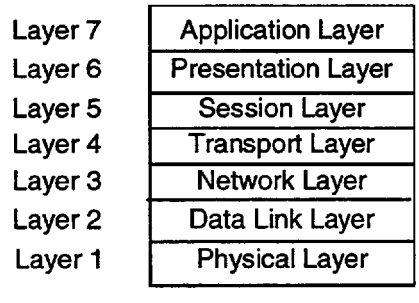


Figure 2-1
OSI LAYERS

[1]Tanenbaum, A.S., *Computer Networks*, Second Edition, Prentice-Hall, 1988.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The seven layers of the RM-OSI are defined as the Physical, Data Link, Network, Transport, Session, Presentation, and Application Layers. These seven layers can be viewed as forming two groups of functionality to support open communications. The first group (Layers 1–4) is responsible for data transport while the second group (Layers 5–7) is responsible for data processing.

The first layer, the Physical Layer, deals with how the bits of information are transmitted over a communications channel. It deals with the mechanical and electrical interfaces, and the physical transmission medium. The second layer, the Data Link Layer, has the task of transforming the information that came in over the wire into data that appears to be free of transmission errors. It should incorporate mechanisms to ensure the integrity of the data and provide a method of ensuring that, if need be, no data is lost. The next layer, the Network Layer, controls how packets of data are routed from source to destination. It is responsible for ensuring that information sent through several sequential physical subnets arrives intact. The primary purpose of the Transport Layer is to organize data to be passed to and from the lower layers. This entails breaking messages into smaller units (packets) so that they are handled efficiently by the lower layers, and assembling packets from the lower layers into messages for the higher layers. This layer is the first to deal with end-to-end communications.

The next three layers, the Session, Presentation, and Application Layers, deal with application and information specific uses of data provided by the lower layers. As described in the OSI Model, the Session Layer allows different equipment to establish dialogues. A dialogue allows one piece of equipment to transfer a file or log from another machine. The Presentation Layer is concerned with the syntax and semantics of the information transferred. As an example, consider what a TMC needs to know about information that is to be presented on a map display. It has to know the exact location and meaning of each bit in a message that contains current intersection status. The Application Layer is concerned with such things as file transfers, file and device access methods, and management of messages. In terms of a computer network, it handles terminal translators, file structures, and attributes.

One of the basic tenets of the RM-OSI is the principle of layer independence. This allows the protocol of one layer to be independent of the protocol of an adjacent layer as long as the boundary between them provides a consistent interface. This has lead to the concept of a layer service definition as the specification of that interface; it defines the set of abstract capabilities (i.e., the semantics) made available by the layer below the boundary to the layer above the boundary. Using this concept, it is then possible to swap protocols below a boundary without affecting the protocol of the upper layer. Each layer of the RM-OSI has a service definition described in terms of the layer providing the service to the layer using the service. The services themselves are made available through a conceptual link between the layers known as a service access point (SAP); they are provided through an exchange of primitives and associated parameters between the service user and service provider. The primary objective of the service provider is the transparent transfer of the data, known as a service data unit (SDU), given to it in a data parameter of a primitive from the service user.

The idea of layer boundaries with well-defined service definitions (including SAPs) is a technique used for descriptive purposes. It is not intended to require that implementations be developed in such a fashion but also does not preclude it. Indeed, implementation of the service definition within a system is not visible to other systems. The service definition concept is not intended to prohibit "streamlined" implementations that may couple several layers of protocol (and any associated state machines), nor to force each layer protocol to be implemented separately with a "clean" layer boundary above and below it.

The concept of a service definition, along with the associated SAP and primitive/parameter exchange, is generic in that it applies to every layer of the RM-OSI. One can refer to an (n)SAP, where (n) can be any layer. When referring to a specific layer, the abbreviation for that layer is used as a prefix (e.g., DLSAP being a Data Link Layer SAP or DLSDU being the SDU given to the Data Link Layer by the Network Layer for transfer to the remote Network Layer).

The concept of layers is reflected in the following list of some of the OSI and Internet protocols being considered for inclusion in NTCIP. Conceptually, at the lower three layers, one protocol could be

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

substituted for another. In the upper layers, several could co-exist because they are optimized for certain tasks.

Application	X.400	Messaging Handling Protocols
	RFC 959	File Transfer Protocol (FTP)
	RFC 11571	SNMP
Presentation	ISO/IEC 8824	Abstract Syntax Notation (ASN.1)
	ISO/IEC 8825	Basic Encoding Rules (BER)
Session	RFC 1121	Simple Network Management Protocol (SNMPV2)
Transport Layer:	RFC 768	User Datagram Protocol (UDP)
	RFC 793	Transport Control Protocol (TCP)
Network Layer:	ISO/IEC 8878	X.25 PLP
	RFC 791	Internet Protocol
Data Link Layer:	ISO/IEC 8802	LAN Protocols
	ISO/IEC 9314-2	FDDI Token Ring MAC
	ISO/IEC 3309	HDLC
Physical Layer:	EIA/TIA-232-E	Serial Interface
	EIA RS-530	High Speed Serial Interface
	EIA RS-485	
	Bell 202T	FSK Modem
	IEEE 802 LAN	Ethernet
	ISO/IEC 9314-1	FDDI

Figure 2-2
LAYER PROTOCOLS

In NTCIP a class profile defines a protocol or set of protocols to be used at each layer in the ISO Model. For example, at the Application Layer, a TMC may need to transfer a large file to another TMC. For transferring files to a bulletin board service (BBS), XMODEM is one of the most popular file transfer protocols. It does not, however, meet the desire for a layered approach. The File Transfer Protocol (FTP) is more suitable in a TMC to TMC environment were the computers communicate over standard Internet protocols. There is also a need to retrieve, change, and store field device data. For this purpose, one might consider any one of a dozen popular spreadsheet programs. However, these tend to be specific to personal computers and not available for a TMC mini-computer or main frame. The Simple Network Management Protocol (SNMP) offers both data transfer and data manipulation capabilities. It is hardware and data independent and is also relatively easy to implement in the microprocessors that are typically used in field devices. If a TMC has to perform file transfers to other TMCs and also manage the data in field devices, both FTP and SNMP would be needed. A field device such as a pollution monitor would not need to perform file transfers but would need to be SNMP compliant to work with the TMC. The Class B Profile Application Layer is defined as SNMP and a variation of it called Simple Transportation Management Protocol (STMP).

The same choices appear at the lower end of the protocol stack. The typical physical interface for interconnecting traffic controllers is to lease twisted pair circuits from the telephone company and use FSK modems. EIA/TIA-232 is another option but the cable length is limited to about 50 feet. If a laptop PC was connected to a vehicle counter cabinet to transfer the count data, however, an EIA/TIA-232 interface at

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

the Physical Layer would be more practical. While an EIA/TIA-232 or FSK interface would be appropriate for a field device, they would not be the only interfaces a TMC computer should support. If the computer is part of a Wide Area Network, it might be desirable to communicate with other TMCs over a fiber optic interface such as FDDI. The current scope of the Class B Profile is aimed at the present generation of field devices and therefore defines EIA/TIA-232 and Bell 202T for the Physical Layer protocols.

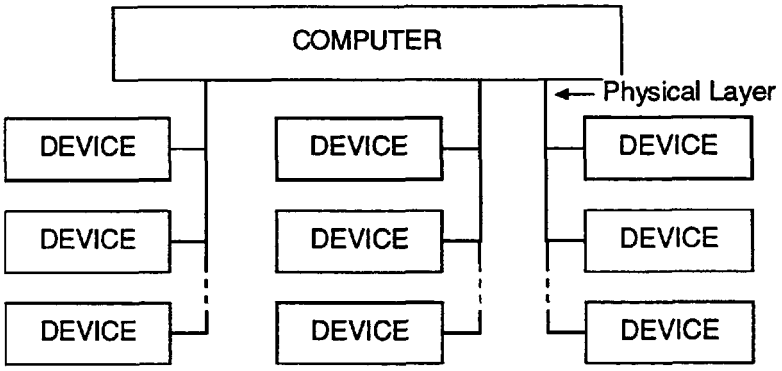


Figure 2-3
CENTRALIZED SYSTEM

Above the Physical Layer is the Data Link Layer. Different class profiles would apply to different topologies and the specific communications requirements. In a centralized system, a central computer might communicate directly with devices (Figure 2-3). The basic functions needed for this application are relatively simple. Data is sent down to a device correctly and if appropriate, the device can send data back at that time. The HDLC protocol is well suited for that purpose. If devices were allowed to also communicate directly to each other at any time, then one of the 8802 LAN protocols would be more appropriate. Because the Class B Profile uses a polled response method of communication at the Data Link Layer, it has been defined using HDLC.

In distributed or multi-level transportation control systems (Figure 2-4) there is another level of control that resides in a device called an arterial master or link controller. Whereas the Data Link Layer controls how data is transmitted on a single subnet, additional control is needed to bridge two or more subnets. The protocols at the Network Layer are designed to address this issue. Basically, they add additional information that specifies which subnet a device is on and allows packets on one subnet to be passed over to another.

The choice of a Network Layer protocol depends on many factors. Typically, it is determined by the amount of bandwidth or speed of the Physical Layer and the type of communications that takes place. Where bandwidth is limited and a connection between two devices on different subnets is held for a long time, X.25 might be the appropriate protocol to implement. On the other hand, if there is adequate bandwidth and only short messages are passed between the two subnets, then the IP protocol might be a better choice. If there is no traffic between subnets, then a Network Layer is not needed. This principle applies to all the layers. If the functions provided by a layer are not needed, then there is no need to incorporate a protocol at that layer.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

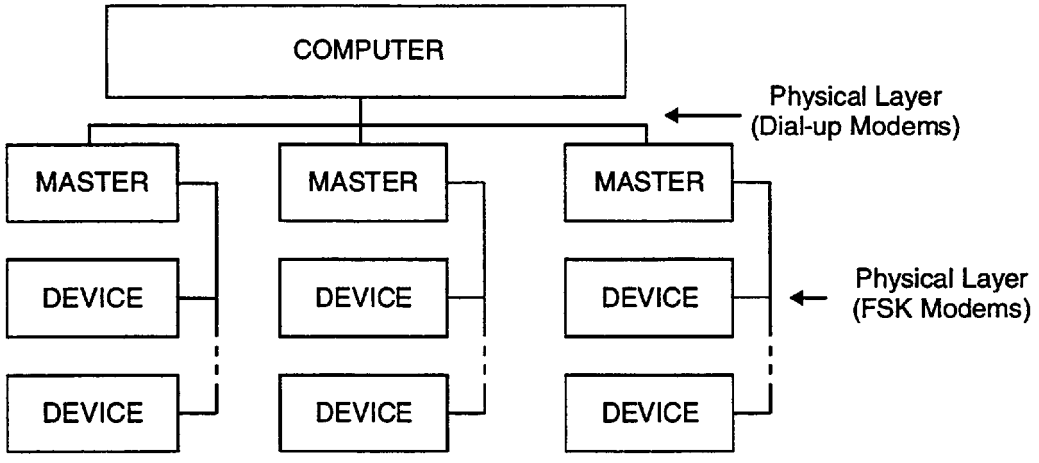


Figure 2-4
DISTRIBUTED OR MULTI-LEVEL SYSTEM

At the Transport Layer, consideration must be given to some of the characteristics of the data being passed back and forth. There may be a need to break down messages into smaller packets. If a large file is being transferred, it is usually desirable to explicitly acknowledge each packet so that any error does not require retransmission of the entire file. If these typified the data, then TCP might be the logical choice for the Transport Layer protocol. If messages can be treated as letters which are sent and forgotten about until a letter comes back, then UDP is better suited. If some of these functions are duplicated in other protocols then a specific Transport protocol may not be needed. For the types of field devices that the Class B Profile is intended for, the messages are assumed to be relatively short and that the devices are polled in a round-robin fashion. Under these circumstances, no transport protocol is used.

At the Session Layer and above, the need for distinct protocols at each of the layers becomes very blurry. SNMP is a perfect example. It provides a security function that is normally associated with the Session Layer. It uses Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER) to address the issues of syntax and semantics normally associated with the Presentation Layer. It could be argued that SNMP Version 2 provides better security but its use has to weighed against its complexity and ease of implementation. The Class B Profile uses features of SNMP and STMP to support functions normally associated with the Session and Presentation Layers.

The choice of a profile should not preclude the intermixing of devices with different communications requirements and protocol implementations. It is assumed that other Class Profiles will be defined. As long as the Physical and Data Link Layers are the same, and the subnet has sufficient bandwidth to handle the traffic, Class B Profile devices can co-exist on the same subnet. NTCIP tries to ensure this by building the layers on top of each other and using protocol identifiers to specify the protocol to be used at the next layer. This method allows a simple camera positioning device to reside on the same subnet as a sophisticated field processor[2]. The NTCIP protocols were chosen so that this principle applies to all the layers. At the Data Link Layer, an Initial Protocol Identifier (IPI) indicates the Network Layer protocol. At the Network Layer, IP has a Transport Layer protocol identifier. TCP and UDP use a socket id for the same purpose.

The communication stack's Application Layer does not address the end application. Up to this point, the profile could be used for any end application. It could just as easily be used for controlling and monitoring the equipment found in a large oil refinery processing plant. NTCIP ties the class profiles to the end application by also specifying common data sets for ITS components. However, a necessary

[2]Federal Highway Administration, Signal Manufacturers Symposium Proceedings, May 1993.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

condition for an integrated system of transportation devices is that components must be managed in a heterogeneous fashion. Information should be interpreted in a manufacturer and hardware independent manner. It should also be accessible via well defined interfaces and protocols. NTCIP includes a formal definition of how messages or managed objects are classified, constructed, and supported. The procedures associated with this definition are modeled around the Internet-Standard Network Management Framework and the OSI Framework. These procedures, entitled the Simple Transportation Management Framework (STMF), and the Application Layer protocol definition provide the interface between communications and the control and/or management application.

The use of layer service definitions results in even greater benefits during migration of an existing base of (proprietary, non-open) protocols to a standardized set of protocols. That is, by defining the services available below a boundary, then all protocol stacks that provide those set of services can support a common protocol above the boundary. For example, the NTCIP upper layers could operate over different Layer 1-4 stacks as long as each such stack provides the same set of services. It should be recognized, however, that different Layer 1-4 stacks require an internetworking function to provide protocol translation between environments using different stacks. This, in turn, could affect overall performance.

Connection-oriented protocols such as X.25 and TCP ensure delivery, or signal when a message could not be delivered correctly. They typically use sequence and acknowledge information and timers to make sure the individual packets are received and are put in their proper order. If a packet is garbled or lost, retransmissions are attempted. If a packet cannot be delivered, the upper layer is notified. This class of service ensures data integrity and correctness.

Connectionless-oriented protocols such as IP and UDP do not ensure delivery. If a packet is garbled, it is simply discarded. If retransmissions are needed, it is the responsibility of the upper layer to provide them. This class of service is primarily intended for short command and reply messages where delivery time is a strong consideration.

While a connection-oriented protocol may seem to provide the ideal service, this type of service comes with a price. Before any information can be passed, a connection between the parties must be established. Data integrity is ensured but this may involve retransmissions which decrease throughput. When the information transfer is completed, the virtual connection must be formally closed. The advantage of connectionless is that it eliminates the overhead associated with setting up and tearing down connections to optimize message throughput.

2.2 THE CLASS B PROFILE LAYERS

2.2.1 Physical Layer

The Physical Layer defines what constitutes the channel and establishes how the raw bits are transferred over the channel. The design issues are to define what a logic 1 or 0 is and what the physical transmission media is. The definition should include the mechanical, electrical, and procedural interfaces. It should also establish how a bit stream is sent or received but not address its meaning or structure.

Two Physical Layer standards are currently defined in the Class B Profile; EIA/TIA-232-E and an FSK Modem interface. The EIA/TIA-232 interface is the most common method for interfacing external communications equipment. The FSK Modem is specified because it is the most prevalent means of interconnecting devices in current traffic control systems. Other Physical Layer definitions may be added in future versions.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.2.2 Data Link Layer

2.2.2.1 General

In choosing a protocol reference for Data Link Layer communications, compliance to an established standard and the adaptability to the existing infrastructure were the prime prerequisites. Over public-switched networks, a number of closely related, bit-oriented protocols are widely used[3]. Early work at IBM defined SDLC for use in their computer networks. To promote SDLC as a U.S. and international standard, ANSI and then ISO modified it to become HDLC. Subsequently, CCITT made several minor changes and adopted it as part of X.25. A variant of HDLC is also used as the lower layer protocol of several Local Area Networks (LANs). IEEE 802 LANs use a protocol called Logical Link Control (LLC). Although conceptually similar to HDLC, LLC adds a source address and uses a more complex control mechanism. Additionally, it is oriented towards peer-to-peer communications and not centralized polling. The previously mentioned protocols have only 6 to 8 bytes of overhead. To address network complexity, the Ethernet Data Link Layer protocol[3] uses fields similar to those in LLC but allows a greater range of values. The overhead cost goes up to over 20 bytes however. The Internet Protocol (IP) portion of TCP/IP alone has 20 bytes of overhead.

For the transportation control application, overhead, complexity, and the current topologies favor one of the bit-oriented protocols. Because HDLC is an internationally recognized standard, has a minimum of overhead, is applicable to asynchronous and synchronous operation, and has a number of inexpensive hardware implementations, it was chosen as the reference for the Class B Profile Data Link Layer protocol.

Data Link Layer communications are defined as the frames or groups of bits and bytes that are transmitted over a single communication channel. The communication channel, whether it be EIA/TIA-232-E, a fiber-optic modem, or radio, in ISO parlance, is called the Physical Layer. Since the information that is passed is independent of how it is passed, the Data Link Layer is distinct from the Physical Layer and can be addressed as a separate function or level of abstraction.

In the Class B Profile of NTCIP, the Data Link Layer frames will consist of data that needs to be passed between two physically connected stations. Because there may be several stations on the same physical channel, an address field is used to indicate who the data is for. To indicate how the data is to be treated when it is received, a control field is also added. The Data Link Layer does not define the meaning of the data; only the meaning of address and control fields. The definition of the "data" is left up to the higher layers. This makes the Data Link Layer communications distinct not only from the Physical Layer below it but also distinct from any higher layer function, i.e., open and application independent.

Today's typical system uses what is called an unbalanced configuration. A single station controls access to the Physical Layer. All other stations connected to the Physical Layer do not have open access. The station controlling access is called the primary station. All other stations are referred to as secondary stations. This unbalanced configuration is illustrated in Figure 2-5. The HDLC standards also define a balanced configuration where any station can initiate access. The Class B Profile will only support the unbalanced configuration. Balanced operation may be considered for a different class profile of NTCIP in order to support a more peer-to-peer oriented communications structure.

---

[3]Comer, D.E., *Internetworking with TCP/IP*, Volume I, Second Edition, Prentice Hall, 1991

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

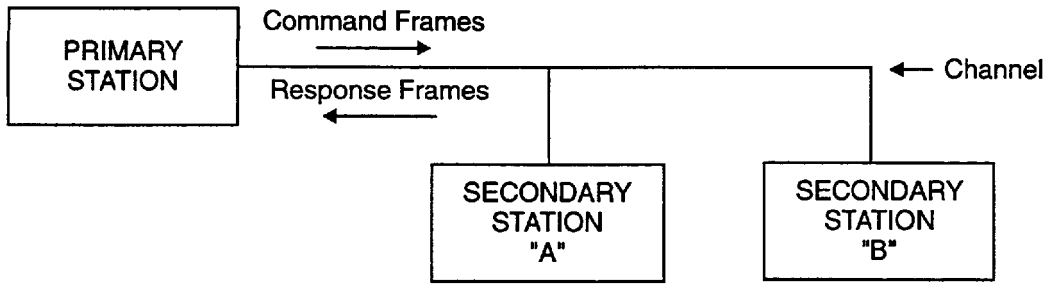


Figure 2-5
UNBALANCED, MULTI-DROP LINE

In systems with a centralized topology, the central computer would be the primary station and the ITS devices connected directly to it would be the secondary stations. In a distributed closed loop traffic control topology, the arterial master would be the primary station to the controllers (secondaries) connected to it. The arterial masters would also be secondaries, but only with respect to the central computer. A similar relationship exists for ITS devices. When operating over a switched network such as the one shown in the upper half of Figure 2-4, the calling station acts as the primary, once the physical connection has been established. The method of establishing the physical connection over a public switched network is the responsibility of the calling station, and is beyond the scope of this document.

It is recognized that there may be instances where a secondary wants to "log on" or to initiate an information transfer. To facilitate this, primary stations that have one or more physically connected secondaries incorporate a polling mechanism. Even if the primary station has nothing to send, it periodically solicits the secondaries to see if they want to come on-line or if they have anything to send.

In the Class B Profile, secondary station replies are limited to a single frame per response opportunity. This provides two advantages. First, the primary station in control of the subnet timing; a secondary cannot hog the line and prevent the primary from polling another station. Second, it simplifies fault handling. Since the primary station always knows that there will be one and only one response frame to any command, it can take responsibility for detecting any missed frames. The secondary stations do not need to time-out or retry, since they can count on the primary to be aware of any errors. A mechanism to force a secondary response to each primary command frame is included in the protocol.

2.2.2.2 Data Link Layer Protocol Overview

As discussed above, HDLC forms the basis for the Data Link Layer protocol of the Class B Profile. HDLC is comprised of four ISO/IEC standards. Each provides numerous tools from which to draw when building a Data Link Layer protocol specification. The Data Link Layer protocol is based on a subset of these tools. This subsection provides an overview of HDLC, especially as it relates to NTCIP in general. The detailed specifications of the Class B Data Link Layer protocol are given in Section 3.3.

In HDLC, bits are transmitted in groups called frames. The basic frame structure of HDLC is defined in ISO/IEC 3309 and depicted in Figure 2-6.

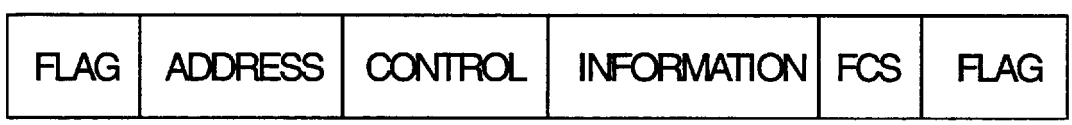


Figure 2-6
HDLC FRAME STRUCTURE

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The flag sequence is a unique bit pattern (0x7E) used to delimit the start and end of a frame. A transparency technique is applied to bytes between, but not including, the flags to ensure that any occurrence of 0x7E is not mistaken for a flag. In cases where throughput must be maximized, the closing flag of one frame can serve as the opening flag of the next.

As depicted in Figure 2-6, each secondary station is assigned a physical address that is unique among all secondary stations on the subnet. The primary station need not be given an explicit address since there is only one such station on a subnet in an unbalanced configuration. When the primary station and a secondary station exchange frames, the address field contains the secondary stations address. The address field may also contain a group address. This allows the primary station to send a frame to multiple secondary stations. When a secondary sends a reply, it places its own physical address in the address field.

The control field identifies the type of frame and the actions to be taken on receipt of it. HDLC groups frames types into three general formats known as Information-format frames, Supervisory-format frames and Unnumbered-format frames. Depending on the frame type, additional information such as sequence numbers may be part of this field. The control field of all frame types contain one bit that is known as the Poll/Final (P/F) bit. The interpretation of this bit position as a Poll or Final bit depends on whether it is in a command type frame, which can only be sent by a primary station, or a response type frame, which can only be sent by a secondary. Setting the Poll bit to 1 in a command type frame indicates that the primary station expects a response; setting the Final bit to 1 in a response frame indicates that it is the last one to be sent as part of the sequence of response frames. Definitions of HDLC frames types are given in ISO/IEC 4335.

Although there are over twenty frame types in HDLC, the Class B Profile Data Link Layer uses only two frame types known as the Unnumbered Information (UI) frame and the Unnumbered Poll (UP) frame. The information field of the UI frame is used to carry the Network Layer protocol and any higher layer information. Since there are no sequence numbers in a UI frame and no associated recovery mechanisms at the Data Link Layer, the contents of the UI frame may be lost. Recovery actions, if needed, are left to a higher layer.

The information field is used to carry information received from the user of the Data Link Layer (i.e., a higher layer protocol). As such, the Data Link Layer does not impose any constraints on the contents of this information. An information field of zero length is permitted.

The frame check sequence (FCS) field is used to guard against bit errors in the frame. HDLC uses a CRC polynomial to generate the contents of this field based on the transmitted bits. On receipt of a frame, the same polynomial is used to check the incoming bits. If the calculated value of the FCS field does not match its contents, then the frame is discarded as having at least one bit in error. The 16-bit CRC polynomial defined in ISO/IEC 3309. Traditional 8-bit checksums have an undetected error rate of $4x10^{-3}$. With the 16 bit CRC polynomial, the probability of accepting a bad frame is approximately $1.5x10^{-5}$.

In addition to defining the frame formats and fields, procedures are also defined for using each frame type. The HDLC elements of procedure are defined in ISO/IEC 4335. Groups of frame types and their associated procedures for doing different Data Link Layer tasks are associated with a class of procedure; ISO/IEC 7809 defines five classes of procedure. The Class B Profile uses the "Unbalanced Connectionless Class" (UCC) class of procedures.

For proper operation of a class of procedures, there are also a number of system parameters. For the UCC class used by the Class B Profile, the only parameters are the maximum number of bytes allowed in the information field of a UI frame and four timers. The maximum number of bytes specification ensures the a frame does not monopolize the line. The timers insure that frames are send efficiently and that lost frames do not tie up the network.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.2.3 Bit Error Rate

In communications, a bit error rate (BER) represents a measurement of the quality of the circuit connection. Computer and traffic control systems require a BER of 10^{-6} or better[4]. The basic BER of any system is primarily determined by the physical media and the modulation technique used. With properly designed and implemented physical wiring, typical Bell 202 type FSK modems have a $1x10^{-5}$ BER.

In designing how a system is to respond to a fault, it is important to understand how errors are introduced. Typical arterial master and closed-loop systems use twisted pair wiring for interconnect and are subject to many types of electrical noise. Lightning and power system faults can produce impulses or noise spikes that can last up to 1000 microseconds. In a modem, this kind of spike would effect a single bit at 1200 bps. However at 9600 bps, that same spike could effect 7 bits. As data rates increase, error detection has to address not only single bit errors but, also, burst errors.

Rather than employ the traditional 8 bit checksum, the Data Link Layer uses a CRC polynomial division algorithm to detect errors. With the 16-bit CRC polynomial defined in ISO/IEC 3309, the probability of accepting a bad frame is approximately $1.5x10^{-5}$. This polynomial detects all single and double bit errors, all errors with an odd number of bit errors, all burst errors of 16 bits or less, 99.9969% of all 17-bit burst errors, and 99.9984% of all 18-bit or longer burst errors[4,5]. Combining the probability of an error occurring with the probability of not detecting it results in an overall BER of $1.5x10^{-10}$. In practical terms, this means that for every 7 billion bits transmitted, there will be 1 bit that is wrong and will not be detected. In terms of a frame size of 64 bytes, an undetected error would occur about once every 1 million times.

2.2.4 Network Layer

In the Class B Profile, the functions of the Network Layer are null or empty. Its function to route messages to the appropriate upper or lower layers is not required since all messaging takes place from a primary to the secondaries on the same subnet. As such, it does not reference an existing standard. The Network Layer is normally concerned with how to pass packets across networks consisting of more than one subnet or Physical Layer. This function will be addressed by other class profiles within NTCIP. Class B is intended solely for communications that take place over a single physical communications channel or subnet.

In Figure 2-7, the Class B profile would be appropriate for communications between the computer and the field processor or master. It would also be appropriate for communications between the Field processor and the "A" field devices or the Master and the "B" field devices. Other class profiles would be appropriate for communications between the computer and the "A" or "B" field devices. This does not preclude the a field processor or on-street master application from assuming the role of bridging information transfers across multiple subnets.

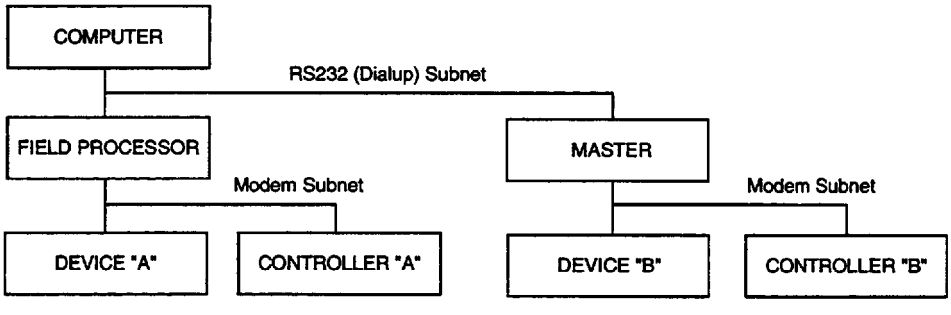


Figure 2-7
MULTIPLE SUBNET NETWORKS

[4] *Communications Handbook for Traffic Control Systems*, FHWA Publication No. FHWA-SA-93-052, April 1993
[5] Hummel, R.L., *Programmer's Technical Reference: Data and Fax Communications*, Ziff Davis Press, 1993

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

In the Class B Profile, a protocol identifier is used to indicate how an incoming message is to be processed.

2.2.5 Transport Layer

The NTCIP Class B Profile Transport Layer protocol does not have a formal definition or reference. Its only function is to ensure that the maximum frame size of the Data Link Layer is not exceeded. As such, it adds no addition overhead to the information passed to or from the Application Layer.

2.2.6 Session Layer

The NTCIP Class B Profile Session Layer protocol is also a null or empty protocol. The services normally provided by this layer are performed by the Application Layer. In the OSI Model, one of the Session Layers functions is to set up and terminate application-to-application communications. A dialogue would allow one piece of equipment to "login" to another. These functions are provided by the SNMP Header. All SNMP messages contain a community name that serves the purpose of a password. The community name is an ASCII string and, by default, is set to "public."

2.2.7 Presentation Layer

There is no formal Presentation Layer in the NTCIP Class B Profile. In the OSI Model, the function of the Presentation Layer is to represent the application data so that it is properly understood. It defines the format of the data and how it is transmitted. Both of these functions are provided by SNMP. It specifies the use of ASN.1 and BER. ASN.1 defines the abstract syntax for messages in that it specifies the basic language elements and provides the rules for combining the elements into messages. BER provides the transfer syntax on how the bits and bytes are transmitted.

2.2.8 Application Layer

2.2.8.1 General

The content of the end-application messages must be independent of the communications protocol. Without an organizational model or structure, it would be impossible to administer and maintain any standard. A method for structuring, representing, encoding and decoding data is needed. That method is defined as the Simple Transportation Management Framework (STMF). The NEMA TS 3.2 Standard provides detailed background information on STMF. Its use by the Class B Profile provides an Internet approach that not only specifies the Applications layer protocol but also how end-application information is organized and quantified.

2.2.8.2 Simple Transportation Management Framework (STMF)

The Application Layer of NTCIP is based upon the Simple Transportation Management Framework. It is the result of studying the Internet Standard Network Management Framework and applying it to the management of transportation equipment and transportation networks. It is intended to satisfy the requirements for integrated management within the transportation industry.

STMF has four components:

a. Structure and Identification of Management Information (SMI)
b. Management Information Base (MIB)
c. Simple Network Management Protocol version 1 (SNMPv1)
d. Simple Transportation Management Protocol (STMP)

SMI, SNMP, and STMP are the components that apply specifically to the Applications layer definition. They define the syntax and semantics of the information being transferred. Their task is to encode data from its internal representation to a form suitable for transmission and decode received data into a form used internally.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.2.8.3 Structure and Identification of Management Information (SMI)

The SMI describes the common structures and identification scheme for the definition of the information used in a system or network. The SMI structure is specified in Abstract Syntax Notation One (ASN.1). ASN.1 was first standardized in 1984 by CCITT and is now covered in ISO/IEC 8824. ASN.1 is a language designed for the purpose of describing structured information. It has been used to describe Protocol Data Units (PDU) or message formats of various communications protocols. A companion standard, Basic Encoding Rules (BER) ISO/IEC 8825, is then used for encoding data for transmission by the lower layer services.

For information identification, a data variable or groups of data variables are defined as objects. These objects are then unambiguously identified by constructed names composed of one component from each level of the Registration Authority hierarchy under which the information object is registered. NEMA has been registered under the Internet network management portion of the global name tree as the information registration authority for NTCIP. All information defined under NTCIP is initially identified with the registered name, *iso.org.dod.internet.private.enterprises.nema*. It can also be represented by the numerical naming convention as *1.3.6.1.4.1.1206*.

2.2.9 Management Information Base (MIB)

A Management Information Base (MIB) is text or machine readable document written in ASN.1 describing the information that is used in a device. The definition of a unit of information is termed a management object and it is the smallest entity that can be exchanged between a device and a management application. Basically, it is nothing more than a single variable. Managed objects can also be constructed from more primitive objects. In other words, it could be a sequence of variables. A collection of related management objects is defined in a document termed a Management Information Base (MIB) module. A single module or multiple modules may define the complete Management Information Base for a transportation system.

The result of creating and identifying management objects using ASN.1 is that a computer readable description of the information exists. A manufacturer can distribute a MIB module with its products. Users who purchase the equipment with a MIB module can utilize the module to update their management applications. Many SNMP management applications can dynamically load and unload modules (MIB) describing the information within remote networking devices. Management applications running on central control hosts can read this module, and other modules such as controller MIBs and vendor specific MIBs, in order to gain information about the capabilities of remote devices.

It should be stressed that these modules are text, not binary, and therefore should not present any significant distribution problems. Validation, compliance statements, and MIB compiler compatibility are subjects to be addressed by the future NTCIP deliberations. For developers, it is important to understand that in order to compile MIB modules, SMI definitions (ASN.1 specifications) must be included in a MIB module. The distinction is made because SMI does not define objects but instead defines how to create management objects. In other words, SMI defines how to utilize ASN.1 in order to create and identify management information (objects) within a tree like structure.

2.2.10 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is used in the Internet networking community for management of a multitude of intelligent devices in a network. It is the dominant network management protocol used in computer networks today. For use within NTCIP, SNMP is used with no changes. SNMP uses BER to encode data for transmission by the lower layer services.

In concept, a network management system consists of three components:

a. one or more managed devices, each with an (SNMP) agent which sends and receives SNMP messages

--`,,`,`,-`-`,,`,,`,`,,`---

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

b. at least one network management station (NMS), each with at least one network management application—each sending and receiving SNMP messages
c. the network management protocol, SNMP, which is used by the agent and manager to exchange management information

Each managed device has management information (configuration, operating parameters, and monitored variables) within the device. These variables are referred to as the managed objects. By changing the value of these variables, the managed device is controlled. This means that imperative commands, such as restart device, are not needed. Any necessary command can be realized by changing the value of a variable defined for this purpose. In addition to changing (configuring or controlling) variables within a device, other variables can be defined for the purpose of monitoring.

The SNMP protocol specifies four basic operations:
a. get—read information variables (managed objects)
b. set—write information variables (managed objects)
c. get-next—allows interrogation of a device for supported features
d. trap—allows a device to indicate to a management application that an event has occurred

A *get-request* is the basic command to ask for data and the *get-response* is the reply to its request. The *set-request* and *set-response* are used to send data and confirm its reception. Although information within a device managed with SNMP is described with MIB modules, there still needs to be a method to perform explorations of the management information within the device. In SNMP that need is satisfied with the *get-next* operation. This traversal operation retrieves the left bottom-most object (upside down tree -- root highest) ID. This ID is then used for the next traversal operation, retrieving the ID of the next object.

In network management terminology, an interrupt or the occurrence of an event is a trap. The easiest way to configure, monitor and control traps is by using a variable (managed object) for that purpose. For example, an information variable called "Cabinet Door Open" could be identified. If this variable is enabled, a trap message containing the object identifier of the variable could be sent to the management application to indicate the event has occurred.

A *get-next* might be considered essential in the area of pre-defined MIBs outside of the NEMA standard area. For example, a MIB module for a device would not include the object *interfaces.rs-232...various_counters* because this object is already defined in other MIBs already written for the Internet. Because conformance statements in some MIBs are not readable, there are only two ways to determine if a controller supports the various error counters in the *interfaces.rs-232 branch*; *get-next* or documentation with the device.

To encode the data for use by the lower layers, Basic Encoding Rules (BER) are used as specified in ISO/IEC 8825. Although ASN.1 can describe any complex data structure, the representation on a communication medium requires additional rules. These rules are encompassed within the BER. SNMP specifically limits the usage of ASN.1 types in order to reduce the complexity of the mapping. The definition of an object includes its syntax or how it is encoded. Implicitly tied to the notion of an object's syntax and encoding is how the object is represented when being transmitted on the network; i.e., BER.

2.2.11 Simple Transportation Management Protocol (STMP)

The purpose of the Simple Transportation Management Protocol (STMP) is to offer a method of setting or getting objects in an intelligent device with the least amount of overhead possible. SNMP trades communication efficiency for maximum flexibility while STMP makes exactly the opposite trade-off.

SNMP is optimized for flexibility and extensibility, and can get or set multiple objects in one message. STMP is used to manipulate objects with a minimum of overhead; in some cases only a single byte. Both SNMP and STMP perform the same basic operations (get, set, and trap) on most objects. The only

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

exception is that SNMP does not normally allow getting or setting aggregate or constructed objects. STMP is optimized for retrieving aggregate or constructed objects. It can also manage dynamic objects with a single byte of overhead. A dynamic object consists of both its definition and its actual (instance) data. Where the definition is a list of pointers to other objects, the data is the information retrieved via the objects pointed to. Formally, it is a sequence of object identifiers.

Dynamic objects are not a matter of SNMP or STMP protocol, but instead a convention allowing an object to contain the information present in any other object. For example, if objects 1.2.1, 7.6.4 and 3.17.9 are desired to be retrieved with one message, combine them into a single dynamic object. This is done by using an SNMP or STMP *set-request* on the managed object *dynDefTable* with the contents or value of the message set to 1.2.1, 7.6.4, and 3.17.9. SNMP and STMP are intended to be complimentary members of the NTCIP Application Layer protocol.

The basic idea is to define all the objects needed by an application starting with what are called primitive objects. For example, *byte* and *word* are the primitive objects used in a computer. These primitives are then be combined to build more complex or constructed objects. For example, the computer term *string* is a nothing more than a sequence of bytes and *file* is basically a sequence of bytes or words. If these primitive objects are individually identifiable then a new object can be created dynamically.

2.2.12 Information Registration Authority Hierarchy

Standard and proprietary information objects must be unambiguously identifiable. Ideally, all the operational characteristics of a class of equipment should be exactly the same. The information that each device handles and stores would then be exactly the same. However, individual manufacturers and agencies tailor equipment to specific needs. To provide standardization but still handle the special needs, it is imperative that all information be registered to ensure that there are no conflicts.

The organization of information under the NEMA node is arranged in four subtrees as shown in Figure 2-8.

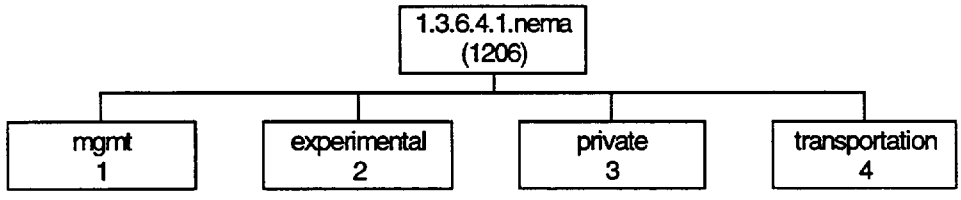


Figure 2-8
THE NEMA TREE

The *transportation* node is subtreed to identify objects which are defined in individual NTCIP documents. Administration of the *transportation* subtree is solely under the authority of NEMA. As proposals which define new versions of the NEMA Transportation Management Information Base (TMIB) are approved, they are assigned an identifier by NEMA for identifying the objects defined by that proposal. The *experimental* subtree is used to identify objects that are under investigation and trial. Objects under the *experimental* subtree might include an initial proposal for a new untested device. The *private* subtree is used to identify objects defined unilaterally. Administration of the *private* subtree is by NEMA. A subtree under *private* called *enterprises* is typically used to identify proprietary but published information about an organizations device information database. This allows NEMA to ensure unique product identification and yet delegate the role of assigned numbers to those members requesting them, except of course for the initial *enterprise* numbers.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

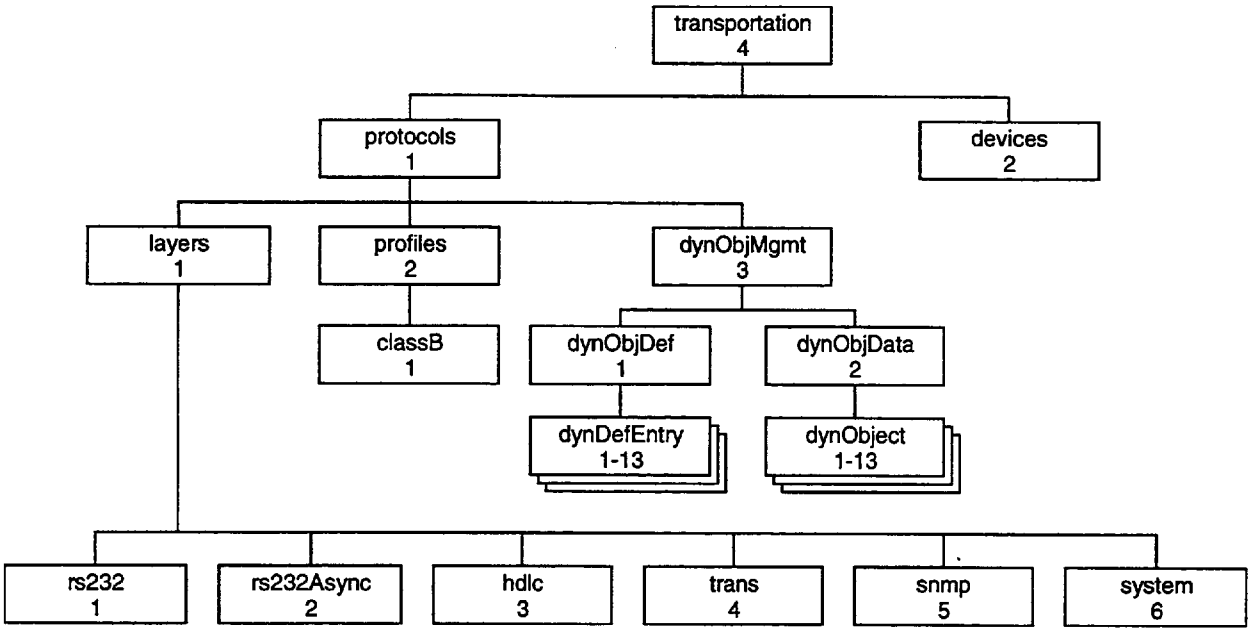


Figure 2-9
TRANSPORTATION SUBTREE

The branches under the *transportation* node segment related information into 2 subtrees; *protocols* and *devices* as shown in Figure 2-9.

The *protocols* branch covers information related to the data or objects specific to management of the layers, various profiles that are part of NTCIP, and dynamic object management. Under the *layers* node are the groups of objects that relate to specific layers of the protocol. The groups are sets of individual objects which must be implemented and supported by a device supporting that layer. The groups do not define the objects but rather which objects from the larger Internet tree are applicable to the layer or specific implementation of a layer. For example, a number of objects for RS232 like devices are already defined in the Internet tree. Most are applicable to the FSK and RS232 Interfaces defined in NTCIP. Rather than redefine the objects, the groups define which of them are pertinent to the NTCIP.

The *profiles* node covers the description of object groups that are applicable to each profile. For example, the Class B Profile consists of objects that relate to the RS232 Physical Layer and the HDLC Data Link Layer and the STMP Applications layer. It does not include a reference to a Network Layer group. If other class profiles are defined by NTCIP, the groups of objects needed to support that profile would be defined here. It is anticipated that a Class A Profile would include references to IP and UDP group objects.

The *dynamic object management* subtree is used to define information related to the use of objects that are made up of more primitive objects but also whose construction is done in real-time. Dynamic objects are discussed further in 2.2.17.

The second subtree under *transportation* is the *device* branch. This is where the standardized transportation information objects are defined. Because they are application specific and not related to the communications protocol they are covered under separate documents called NTCIP Object Definitions.

2.2.13 Object Management

In ASN.1, an object type definition consists of five fields:

a. Object name—A textual name and an identifier for the object type

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

b. Syntax—The abstract syntax of the object, i.e., how it is built.
c. Definition—A textual description of the semantics or meaning of the object type
d. Access—The object can be read-only, read-write, write-only, or not-accessible
e. Status—Support is either mandatory, optional, or obsolete

The object name is represented uniquely as an object descriptor and an object identifier. Each object descriptor corresponding to an object type in the STMF standard MIB will be a unique mnemonic and be composed of printable characters. This promotes a common language for humans to use when discussing the MIB and also facilitates simple table mapping for user interfaces. The object identifier is a sequence of integers which traverse a global tree and is an administratively assigned value. Central to the notion of the object identifier is the understanding that administrative control of the meanings assigned to the nodes may be delegated as one traverses the tree.

The syntax of an object type defines the abstract data structure corresponding to that object type. For example, the structure of a given object type might be an integer, octet string, or a sequence of bytes. The encoding of an object type is then simply how instances of that object type are represented using the objects type syntax.

The definition field is ASCII text that describes the object and can be used to describe its operational use. In the access field read-only, read-write, and write-only are as commonly used. The not-accessible attribute is used to note that this object is used for definition purposes and is not substantiated or an actual object. The status field describes whether an object is mandatory or optional. Refer to clause 3.3.5 of NEMA TS 3.2 for further definition.

2.2.14 NTCIP Managed Objects

In the NTCIP environment, there are certain objects that must be supported by all devices complying with the standard. These objects would be referenced by branches under the layers and profiles nodes of Figure 2-9. A description of the objects is provided in Annex B. To provide a sense of what is covered, several of the objects under the layers node are listed:

a. Physical Address—The subnet address of a station.
b. Address Translation Table—A routing table object.
c. Frame Size—The frame size at the Data Link Layer
d. EIA/TIA-232 Parameters

2.2.15 Device and Application Specific Managed Objects

A transportation management human interface application and any device complying with NTCIP would use the definition, services and functions of the communications profile protocols. What a system does, how it is managed, and the functions (the managed objects) of any managed device are not part of NTCIP. NTCIP provides the framework for communicating, not the operational and functional characteristics of devices using it. However, the original intent of NTCIP was to develop a common communications protocol for transportation devices and the equipment controlling them. The managed objects for actuated traffic signal controllers are specified in NEMA TS 3.5.

2.2.16 Traffic Controller Managed Objects

The following list summarizes some of the managed object types that are defined for the traffic control and coordination functions. A full description of how the set and get operations can manipulate them is provided in NTCIP Object Definitions.

a. Current Time—Time and date object
b. Pattern—Current timing plan object
c. Sync Command—An object to synchronize a timing plan
d. Special Functions—An object for application specific outputs

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

e. Local Status—Long form controller status
f. Short Status—Short form controller status
g. Detector Data—Detector data

2.2.17 Dynamic Objects

The objects described in the various NTCIP Object Definitions documents provide a minimal set of constructed objects to ensure inter-operability. If these were the only objects allowed however, it would inhibit innovation and customization. There is also the case where one of the defined objects may be too large to retrieve in a timely manner or several messages are needed to retrieve what is wanted. STMP allows an object to consist of pointers to other objects. Many of the constructed objects use primitive objects that are individually identifiable. Rather than revise a Standard to incorporate manufacturer or end user specific constructed objects, STMF (NEMA TS 3.2) defines the Dynamic Object mechanism and structure to add support for it if needed. A separate Standard is used since all devices need not support dynamic objects. Within the Class B profile, a device supporting the Dynamic Objects would have an associated line added to its conformance statement in its MIB.

2.3 CONFORMANCE AND PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS)

Implementation of a protocol from a common specification does not ensure that two systems can inter-operate with each other. The situation is exacerbated when the specification includes ranges of parameters or various options that may or may not be included in the implementation. To maximize the potential of inter-operability, a protocol specification should state the mandatory features that all conforming implementations shall include. A Protocol Implementation Conformance Statement (PICS) is a questionnaire that implementors fill out describing the features of the system. Questions about mandatory features allow only for a "Yes" answer while questions about optional features allow a "Yes" or "No" answer. In this way, the PICS proforma can be used to determine if a system conforms to the specification (all mandatory features checked as "Yes") and what also options have been implemented.

A completed PICS proforma can be used for several purposes:

a. To allow an implementor to verify that all mandatory features have been implemented
b. To allow a tester to determine which features to test (i.e., tests should not be run on optional features that have not been implemented, but a system is considered not to conform to the standard if it does not implement one or more mandatory features)
c. To allow the procurer of the system to know what features have been included in the product.

To insure that the integrity of this Standard is maintained, the main body of the protocol is copyrighted. The intention of providing the PICS proforma as an attachment is to point out that it can be copied and used by agencies to ensure conformance to the standard.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Section 3
DATA TRANSPORT ASPECTS

3.1 GENERAL PROTOCOL ASPECTS

To support the needs of the traffic control environment, numerous requirements have been described in Section 2 of this Standard. Clause 2.2, in particular, provided an overview of the protocol elements of NTCIP in terms of a layered approach to communications. Clause 3.1 provides material that transcends a particular layer but will be applied in subsequent clauses.

3.1.1 Protocol Stacks and Conformance

The Class B Profile shall be defined as one of several protocol stacks consisting of layers 1, 2, 3, and 7. These layers are defined according to the following:

a. Layer 1 supports at least one of the protocols specified in clause 3.2.
b. Layer 2 supports the protocol specified in clause 3.3.
c. Layer 3 supports the protocol specified in clause 3.4.
d. Layer 7 supports the protocol specified in clause 4.3.

3.1.2 Descriptive Technique for Service Definitions

Clause 2.4 of the NEMA TS 3.1 NTCIP—Overview, develops the concept of service definitions for layered protocols. As mentioned there, such definitions are included in this Standard for the services provided by the Data Link and Network Layers. These definitions make use of the concepts developed in ITU-T Rec. X.210 | ISO/IEC 10731. In particular, service definitions are specified in terms of:

a. A set of primitives exchanged between the two layers through their common service access point. This includes specification of which direction the primitive flows (from service user to service provider or vice-versa)
b. For each primitive, a set of parameters and, as necessary, limits on parameter values
c. The allowed sequence of primitives

Primitives can be thought of corresponding to subroutine calls when viewed in an abstract fashion. However, services and their associated primitives do not have to be implemented separately from the protocols as discussed in 2.2.

3.2 PHYSICAL LAYER DEFINITION

3.2.1 Scope

Two physical layer standards are defined for the Class B Protocol Stack in NTCIP, EIA/TIA-232-E and an FSK Modem interface. EIA/TIA-232-E is the most common method of interfacing to external communications equipment. The FSK Modem is specified because it is the typical method by which current traffic control systems implement communications. Both the EIA/TIA-232-E and FSK Modem interfaces operate in asynchronous mode. The need for inclusion of other interfaces is under consideration in future Class Profile definitions of NTCIP.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

3.2.2 EIA/TIA-232-E Interface

The EIA/TIA-232-E Data Terminal Equipment (DTE) interface shall provide for interconnection to external communications devices at a minimum of 1200 bps. The EIA/TIA-232-E interface shall use asynchronous transmission and the byte structure shall be 1 start bit, 8 data bits, no parity, and 1 stop bit. The connector shall be a female 25 pin metal shell "D" subminiature type connector. The signals shall consist of:

Pin	Function	Input / Output
1	Earth Ground	[-]
2	Transmit Data	[O]
3	Receive Data	[I]
4	Request To Send	[O]
5	Clear To Send	[I]
6	Reserved (Data Set Ready)	[I]
7	Logic Ground	[-]
8	Data Carrier Detect	[I]
9-14	Not Used	
15	Reserved (Synchronous Mode Transmit Clock)	[I]
16	Not Used	
17	Reserved (Synchronous Mode Receive Clock)	[I]
18-19	Not Used	
20	Data Terminal Ready	[O]
21	Not Used	
22	Reserved (Ring Indicator)	[I]
23	Not Used	
24	Reserved (Synchronous Mode Transmit Clock)	[O]
25	Not Used	

The EIA/TIA-232-E function reference for Pin 1 is Frame Ground and Pin 7 is Signal Ground. References to Synchronous Mode signals are made only to ensure future compatibility.

3.2.3 FSK Modem Interface

The FSK modem interface shall provide half duplex two-wire or full duplex four-wire communications over an unconditioned Type 3002 voice grade private line channel or equivalent customer owned cable. The nominal impedance of the line or cable shall be 600 ohms. Communications over the system interface shall utilize time division multiplex techniques. Transmissions shall use phase coherent frequency shift keying (FSK) modulation at a data rate of 1200 bps. Data format shall be asynchronous, bit serial. The receiver portion of the system interface shall be an FSK to digital demodulator. Receiver sensitivity shall be a minimum of -34dBm, with in band signal-to-noise ratio of 10dB or better.

Support of the following parameters shall be provided:

Data Rate	1200 Baud
Modulation	FSK, Asynchronous
Frequencies	Mark=1200 Hz, Space=2200 Hz
Transmit Output Range	+6, 0, -2,-4, -6, -8, -10 dBm
Receiver Input Level	0 to -34 dBm
Line Impedance	600 Ohms
Clear-To-Send Delay	8 ms
Carrier Detect	6 ms
CTS Turn off delay	10 ms
Receive Squelch	9 ms

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The connector shall be a male, 9 pin metal shell "D" subminiature type connector. The pin connections shall be as follows:

Pin	Function	Input / Output
1	Transmit 1	[O]
2	Transmit 2	[O]
3	Reserved	
4	Receive 1	[I]
5	Receive 2	[I]
6	Earth Ground	[-]
7	Reserved	
8	Reserved	
9	Earth Ground	[-]

Pins 6 and 9 are provided for connection to an external cable shield, if appropriate.

3.2.3.1 FSK Modem Terms

The following terms are critical to any throughput timing analysis. They are included here to avoid any ambiguity in their meanings.

a. Clear-to-Send Delay—When there is data to send (RTS goes true), this is the minimum time a transmitter is held in the MARK condition (carrier) before sending data so that a receiver is given enough time to recognize a valid carrier signal.

b. Carrier Detect—This is the maximum time for a receiver to recognize the presence of a carrier signal.

c. Soft Carrier Turn Off—After sending data (RTS goes false), this is the time during which the transmitter should transmit the soft carrier frequency (900hz). This is done because at the end of a message transients may occur and this could cause spurious space signals to be received at a remote modem.

d. Receiver Squelch—After transmitting (RTS goes false), this is the maximum time for receiver carrier detect to be clamped off so that line transients are not demodulated. After this time, the receiver can search for carrier. This is also known as the turn around time.

3.3 DATA LINK LAYER DEFINITION

3.3.1 Scope

This subclause defines the service (abstract set of capabilities) provided to the user of the Data Link Layer as well as the associated protocol encoding (syntax) and procedures. Figure 3-1 depicts the aspects of Data Link Layer operation described in this subclause. In the figure, (a) indicates the service provided by the Data Link Layer (3.2), (b) indicates the protocol used by the Data Link Layer (3.3), and (c) indicates the mapping between service and protocol (3.4).

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

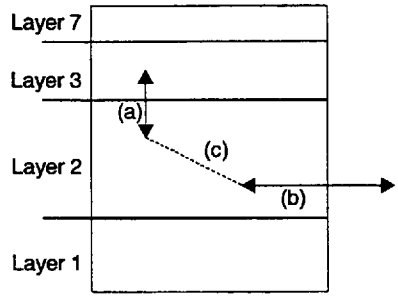


Figure 3-1
DATA LINK LAYER SERVICES, PROTOCOL, AND MAPPING

3.3.2 Data Link Layer Service Definition

The service provided by the NTCIP Data Link Layer shall be the connectionless-mode service as defined in ISO/IEC 8886, clauses 1-7 (general) and 15-19. Within these clauses, those aspects dealing with Quality of Service shall not apply (this includes all of clause 17 and applicable parts of the other clauses). In particular, the following aspects of these clauses are noted.

a. Clause 15 of ISO/IEC 8886, describes the features of the Data Link Layer service: all implementations shall support a DLSDU length as specified in 3.3.3.4.
b. Clause 16 of ISO/IEC 8886, dealing with the model of the Data Link Layer service, shall apply with the additional assumptions that the service shall not duplicate SDUs nor exchange the order of SDUs.
c. Clause 18 of ISO/IEC 8886, dealing with the sequence of primitives, shall apply.
d. Clause 19 of ISO/IEC 8886, dealing with data transfer by the Data Link Layer, shall apply. The mapping between this service definition and the protocol elements specified in 3.3.3 is given in 3.3.4.

3.3.3 Data Link Layer Protocol

In terms of HDLC, the NTCIP Data Link Layer protocol shall be the Unbalanced Connectionless Class (UCC) of procedures defined in ISO/IEC 7809 with HDLC optional function number 7 applied for multi-octet addressing and number 15.1 for start/stop transmission with basic transparency. This is designated as UCC-7,15.1.

Those clauses of ISO/IEC 3309, 4335, and 7809 dealing with the following shall not apply to NTCIP:

a. synchronous transmission
b. classes and associated modes other than UCC
c. HDLC optional functions other than 7 and 15.1

3.3.3.1 Frame Structure

The frame structure shall be as shown in ISO/IEC 3309. The ISO/IEC 3309 HDLC frame structure is shown in Figure 3-2.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

FLAG	ADDRESS	CONTROL	INFORMATION	FCS	FLAG

Figure 3-2
HDLC FRAME STRUCTURE

Transmission shall be in start/stop mode with basic transparency applied. The other transparency modes shall not apply.

The address field of data link layer frames shall use single or extended byte addressing, as provided for in clause 5.1 of ISO/IEC 3309, and shall incorporate support for group addressing. The low order bit of the first byte of an address shall be set to 0 to indicate that the next byte is part of the address field. The second low order bit of the first byte can be set to 1 to indicate that the frame is intended only for a selected group of addresses. Address 0 shall be never assigned and address 63 is reserved. Figure 3-3 through Figure 3-4 illustrate how the address field can be used.

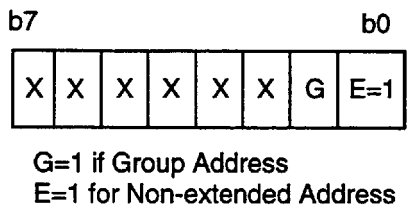


Figure 3-3
SINGLE BYTE ADDRESS FIELD

Figure 3-3 illustrates a single byte address field. With bit 0 and bit 1 set to 1 and 0 respectively, the upper 6 bits can be used to address stations 1 to 63 If the second low order bit is set to 1, the upper 6 bits shall indicate that the frame is intended for a group of secondary addresses. Group address 63 (0xff) is reserved for the "all stations address" and this shall always be transmitted as a single byte.

Figure 3-4 indicates the structure of a two byte address field. The low order bit of the first byte shall be set to 0 to indicate an extended field and the low order bit of the second byte set equal to 1 to indicate the last byte of address field. The second low order bit of the first byte is still used to indicate a group address.

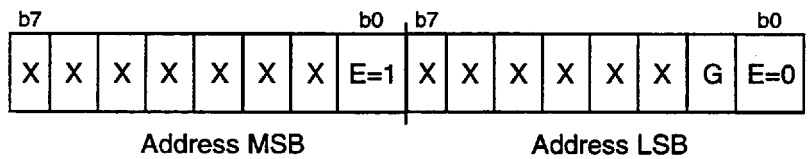


Figure 3-4
TWO BYTE ADDRESS FIELD

The maximum number of bytes in the address field shall be limited to two and the low order bit of the second byte shall therefore always set to 1. The upper seven bits of the second byte shall be concatenated to the previous 6 bits of the first byte to provide an address space of 2^{13}.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Support for 1 byte addressing is mandatory. Recognition of extended addressing is mandatory. Support for 2 byte addressing shall be provisional. If a 1 byte address is received, the high order bits of the equivalent two byte address are assumed to be 0's.

The control field shall be one octet in length; it shall not be extended.

The 16-bit FCS procedure defined in clause 4.6.2 of ISO/IEC 3309 shall be used.

3.3.3.2 Supported Frame Types

NTCIP shall make use of the following HDLC frames types, as defined in ISO/IEC 4335 and in ISO/IEC 7809 for use with the UCC procedures:

Command:	Response:
Unnumbered Information (UI)	Unnumbered Information (UI)
Unnumbered Poll (UP)	Unnumbered Information (UI)

The encoding for the control field of the above frames is given in ISO/IEC 4335. The Poll/Final bit of the control field shall be used as described in the referenced standards except that the Poll bit shall always be set in an unnumbered poll. An unnumbered poll shall never be used with a broadcast or group address. An unnumbered poll shall never contain an information field.

3.3.3.3 Procedures

Transmission of frames on the link shall be in Unbalanced mode as described in the Introduction of ISO/IEC 4335 and clause 6 of ISO/IEC 7809. That is, transmission shall be controlled by the Data Link layer of the station designated as the Primary station (referred to as the "control" station in ISO/IEC 7809) on that link and shall be responded to by the addressed Secondary station (referred to as the "tributary" station in ISO/IEC 7809). Transmission by the Primary station to a group address shall have no response. All group communications shall be sent in a UI with P=0.

Provisionally, the Data Link layer of a Primary station may support a scheduler that periodically sends a polling message in the next available frame. An unnumbered poll frame type shall be used for this purpose. The T4 timer shall determine the interval.

A Secondary station shall transmit only one UI response frame per respond opportunity. The response of the secondary shall contain its address in the address field, not the address of the primary. Clause 6.4.2.2 of ISO/IEC 7809, which states that the last UI response frame (F-bit=1) must have an information field length of zero, shall be ignored.

When a switched connection (e.g., a telephone connection) is used to establish the link, the roles of Primary and Secondary stations shall be based on which station initiated the connection; the calling station assumes the role of Primary while the called station assumes the role of the Secondary.

The procedures for establishing a switched connection and identifying the calling station are beyond the scope of the data link layer. The Application Layer should provide a means of access and authentication of the parties participating in the exchange.

3.3.3.4 Protocol Parameters

A system conforming to this Standard shall support an information field length (DLSDU) of at least 515 octets; a system supporting lengths greater than this value shall also state what lengths are supported in the PICs.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

There shall be four timers normally associated with the Data Link Layer; T1 through T4. They shall be setable in the range of 1 to 2147483647 milliseconds, by 1. Their context only applies to the Data Link Layer; not other layers.

a. T1—This specifies the maximum time a primary station shall wait for acknowledgment of a frame. T1 is only activated for a command frame with the poll bit set.
b. T2—This specifies the maximum time a secondary station can delay before sending an acknowledgment. A value of 0 means that there shall be no delay in acknowledgment generation. This timer ensures that secondary starts a response so that it is received by a primary before T1 times out (T2 < T1). T2 is only activated when the receiving station accepts a frame with the poll bit set.
c. T3—This specifies the time to wait before considering a link disconnected.
d. T4—This specifies the maximum time to allow without frames being exchanged on the data link. A value of 0x7FFFFFFFH indicates that no idle timer is being kept.

To ensure that data is transmitted as rapidly as possible, the maximum total byte-to-byte delay time in a frame shall be one bit time (e.g. 0.83 ms for 1200 BPS). In full duplex operation at a primary station, the transmission of the closing flag may exceed the byte-to-byte delay.

3.3.4 Mapping of Protocol to Service

ISO/IEC 11575, clause 10.2, specifies the mapping of the UCC procedures of HDLC to the connectionless-mode Data Link Layer service. This mapping shall apply to NTCIP and provides for:

a. the mapping between DL-UNITDATA primitives to UI frames of non-zero length
b. the mapping between the address parameters in the DL-UNITDATA primitives to the address field in UI frames
c. the mapping between the user data parameter in DL-UNITDATA primitives to the information field in UI frames

3.4 NETWORK LAYER DEFINITION

3.4.1 Scope

This subclause defines the service (abstract set of capabilities) provided to the user of the Class B Network Layer (the NTCIP Application Layer) as well as the associated protocol encoding (syntax) and procedures. Figure 3-6 depicts the aspects of Network Layer operation described in this subclause. The legend for the figure is as follows:

a. Service provided by the Network Layer (3.4.3)
b. Protocol(s) used by the Network Layer (3.4.4)
c. Mapping between service and protocol(s) (3.4.5)
d. Protocol Identification Function (3.4.2)

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

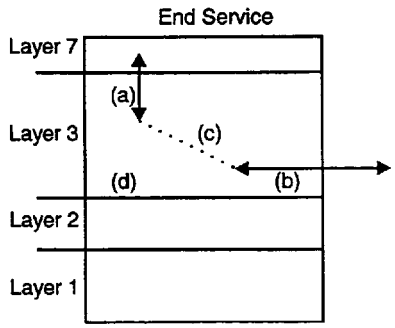


Figure 3-2
NETWORK LAYER SERVICES, PROTOCOL, AND MAPPING

3.4.2 Protocol Identification

The protocol identification function allows for multiple Network Layer protocols to be distinguished from each other. In the case of NTCIP, a system may have other classes and protocols other than those defined in the Class B Profile.

RFC 1700 defines an initial protocol (in the Network Layer) as that protocol "operating directly over the Data Link Layer." This protocol is identified by the Initial Protocol Identifier (IPI). The IPI is the first byte of information passed between the Network and Data Link Layers in the user data parameter of a DL-UNITDATA primitive. It is through this IPI that the NTCIP Network Layer shall distinguish different protocols.

The value of the IPI supported by the data link layer of the Class B Profile is 0xC1.

The protocol identification function shall examine the IPI value. It shall pass the DLS-User-Data parameter (including the IPI) received from the Data Link Layer in a DL-UNITDATA indication primitive to the corresponding protocol as identified above. For the Class B Profile, only support for the Class B Protocol Identifier is required. If an IPI, as defined above, is not supported then the DLS-User-Data shall be discarded and no further action taken.

3.4.3 Network Layer Service Definition

Class B Profile communications take place between devices on the same physical link. Therefore, little functionality is needed to convey real-time application layer messages.

The service provided when supporting Class B communications is the connectionless-mode service (CLNS) as defined in ISO/IEC 8348, clauses 1-7 (general) and 15-19. Within these clauses, those aspects dealing with Quality of Service shall not apply (this includes all of clause 17 and applicable parts of the other clauses). In particular, the following aspects of these clauses are noted.

a. Clause 15 of ISO/IEC 8348 describes the features of the CLNS: all implementations shall support an NSDU length (i.e., the length of the NS-User-Data parameter) of at least the DLSDU size (given in 3.3.2) minus one byte (to account for the one byte Class B header).
b. Clause 16 of ISO/IEC 8348, dealing with the model of the CLNS, shall apply with the additional assumptions that the service shall not duplicate SDUs nor exchange the order of SDUs.
c. Clause 18 of ISO/IEC 8348, dealing with the sequence of primitives, shall apply.
d. Clause 19 of ISO/IEC 8348, dealing with data transfer by the Network Layer, shall apply. The relationship of the service definition to the protocol elements defined in 3.4.3.2 is given in 3.4.3.3.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

3.4.3.1 Usage of Underlying Data Link Layer Service

This protocol shall use the DL-UNITDATA primitives for transfer of its packets. The DLS-User-Data parameter of these primitives shall carry the packets defined by this protocol.

3.4.3.2 Packet Structure and Supported Packets

The packet structure for this protocol shall be as given in Figure 3-7.



Figure 3-3
NETWORK LAYER PACKET STRUCTURE

Only one packet type is defined by this protocol: a data packet.

3.4.3.3 Procedures

This protocol shall take the contents in the NS-User-Data parameter of an N-UNITDATA request primitive and embeds it in the higher-layer information field of the data packet. The resulting packet is then passed down to the Data Link Layer as described in 3.4.3.1.

On receipt of a data packet, the opposite mapping shall be performed.

3.4.4 Network Layer Protocol

A system conforming to this Standard shall support a higher-layer information-field length of at least the DLSDU size (given in clause 3.3.2) minus one byte (to account for the one byte IPI header).

3.4.5 Mapping of Protocol to Service

The mapping of this protocol to the CLNS shall provide for:

a. the mapping between N-UNITDATA primitives to Data packets
b. the source and destination addresses of N-UNITDATA request primitives are not carried by this protocol
c. the mapping between the NS-User-Data parameter in N-UNITDATA primitives to the higher-layer information field in Data packets

3.5 TRANSPORT LAYER DEFINITION

For the NTCIP Class B Profile, there is no Transport Layer. Any segmentation and reassembly functions shall be performed by the Application Layer or the end application.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Section 4
DATA PROCESSING ASPECTS

This section defines the data processing aspects of the NTCIP Class B Profile. The data processing aspects deal with application and information specific uses of data provided by the lower layers of the OSI Model. The lower layers are made up of the Physical, Data Link, Network, and Transport Layers. The upper layers addressing the data processing aspects are made up of the Session, Presentation, and Application Layers.

4.1 SESSION LAYER DEFINTION

There is no Session Layer definition in the NTCIP Class B Profile. Authentication and security, which are normally associated with the Session Layer, shall be performed at the Application Layer by the use of the community name defined in SNMP.

4.2 PRESENTATION LAYER DEFINITION

There is no Presentation Layer definition in the NTCIP Class B Profile. The syntax and semantics of information transfers shall be performed by ASN.1, BER, and PER. These are defined as part of the Application Layer definition. See NEMA TS 3.2 STMF.

4.3 APPLICATION LAYER DEFINTION

4.3.1 Scope

The scope is the structure and identification of transportation information within transportation equipment and the protocols that act on defined information entities. This clause defines the service (abstract set of capabilities) provided to the user of the Application Layer as well as the associated protocol encoding (syntax) and procedures. Figure 4-1 depicts the aspects of Application Layer operation described in this clause. In the figure, (a) indicates the service provided by the Application Layer (4.3.3), (b) indicates the protocol used by the Application Layer (4.3.4), and (c) indicates the mapping between service and protocol (4.3.5).

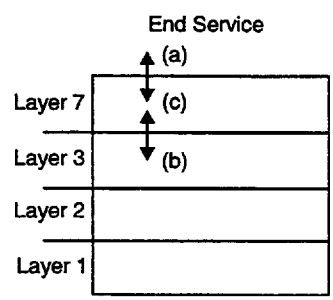


Figure 4-1
APPLICATION LAYER SERVICES, PROTOCOL, AND MAPPING

4.3.2 General

The Simple Transportation Management Framework (STMF) shall be the architecture or framework that specifies the set of rules and protocols for organizing, describing and exchanging transportation management information between transportation management applications and transportation equipment. The specification for STMF is covered in NEMA TS 3.2 STMF.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The four major components within the STMF are:

a. Structure and Identification of Transportation Management Information (STMI)
b. Transportation Management Information Base (TMIB)
c. Simple Network Management Protocol version 1 (SNMP)
d. Simple Transportation Management Protocol (STMP)

4.3.3 Application Layer Service Defintion

4.3.3.1 Structure and Identification of Transportation Management Information

STMI describes the common structures and identification scheme for the definition of management information used in managing transportation networks. It is based upon RFC 1155. STMI shall be specified in ASN.1 and that can be compiled by MIB compilers. In order to compile MIB modules, STMI definitions (ASN.1 specifications) must be included in a MIB module. The distinction is made because STMI does not define objects but instead defines how to create management objects. In other words, STMI defines how to utilize ASN.1 in order to create and identify management information (objects) within a tree like structure.

4.3.4 Application Layer Protocol

The Application Layer protocol of the Class B Profile shall consist of STMP and provisionally SNMP.

4.3.4.1 Simple Network Management Protocol

This is fully specified in RFC 1157. SNMP is an Application Layer protocol that allows data (managed objects) in field and management devices to be inspected and changed. It specifies the exchange of messages between protocol entities that effect these functions. The RFC constitutes one part of the definition of the protocol used at the Application Layer in the Class B Profile.

4.3.4.2 Simple Transportation Management Protocol

The STMP makes up the second component of the Application Layer protocol. It is derived from SNMP and is specifically designed to satisfy the unique technical requirements of low overhead and efficiency. It is defined in NEMA TS 3.2.

4.3.5 Mapping of Service to Protocol

4.3.5.1 Transportaion Management Information Base

TMIB shall contain the groups below the STMI groups, and objects defined by the NTCIP. MIBs must be created in conformance with RFC 1212. Objects within the greater Internet community included in TMIB are defined in the Management Information Base II (RFC 1213).

4.4 CONFORMANCE

Manufacturers shall conform to either conformance level 1 or 2 as stated NEMA TS 3.2. In addition, the objects defined in the Class-B-PROFILE-MIB shall be supported.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
FSK MODEM INTERFACE TIMING ANALYSIS

Most traffic control systems allow an end user to view a system map of the green indications at individual intersections. The number of the secondaries on a channel or resolution of a map can be dependent upon the throughput of the communications channel. To portray a map in real-time, it is typical to poll each intersection on a once-per-second basis. In current systems that address multiply secondaries on a channel, overhead is minimized, data content is kept to a minimal, and message length is held constant. NTCIP in comparison, has a fair amount of overhead and the message length can vary significantly. It is important to understand the overhead imposed by the protocol and the timing constraints of a low speed communications channel such as the 1200 Baud FSK Modem Interface.

At the application layer, an STMP dynamic object Get Request or Get Response AL-PDU consists of 1 byte for the Format, Type, Message Type, and Object ID. At the network layer, the NL-PDU consists of a 1 byte Initial Protocol Identifier and the AL-PDU. At the data link layer, the DL-PDU consists of a 1 byte opening flag, 1 to 2 bytes for the physical address, a 1 byte control field, the NL-PDU, a 2 byte FCS and a 1 byte closing flag. This is illustrated in Figure A-1.

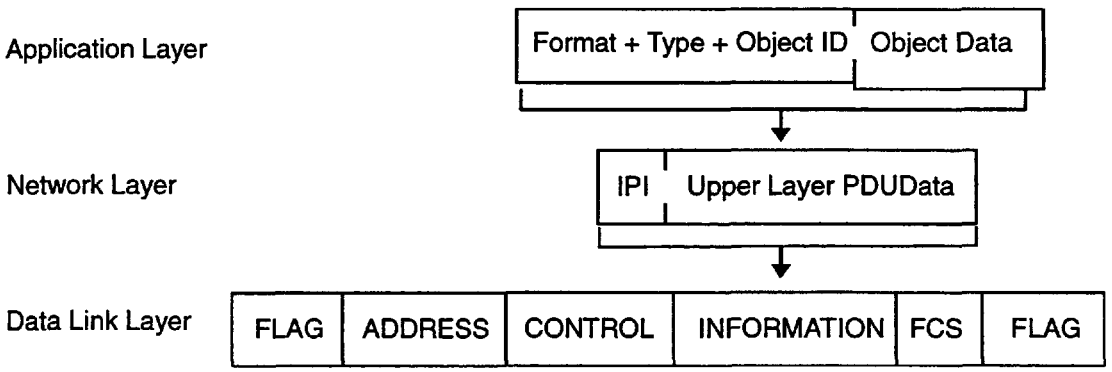


Figure A-1
UPPER LAYER PDU EMBEDDING

Thus the overhead of a Class B Profile dynamic object message could be 8 bytes. If two messages are sent back-to-back, the closing flag of the first frame can serve as the opening flag of the next . This would result in a minimum of 7 bytes of overhead.

Another factor that effects throughput is the byte stuffing algorithm that ensures that the opening and closing flags are unique characters. Any flag or escape byte naturally occurring in the data stream between the opening and closing flags is padded with an addition byte. Assuming a truly random data stream, this would occur only twice every 256 bytes. While statistically, this amounts to less than 1% overhead, one needs to be aware that specific sequences could have significant padding.

Polling of multiple secondaries will cause overall throughput to be less than the channel bandwidth because of carrier detect and turn off times. Figure A-2 illustrates the timing characteristics of a full duplex channel that is polling the intersections for the data needed for a systems map display using the dynamic object mechanism. The AL-PDU for the Get Request is 1 byte. The Get Response AL-PDU is assumed to

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

be 5 bytes; 1 byte for the Get Response tag and 4 bytes of data. The DL-PDUs are then 8 and 12 bytes long respectively.

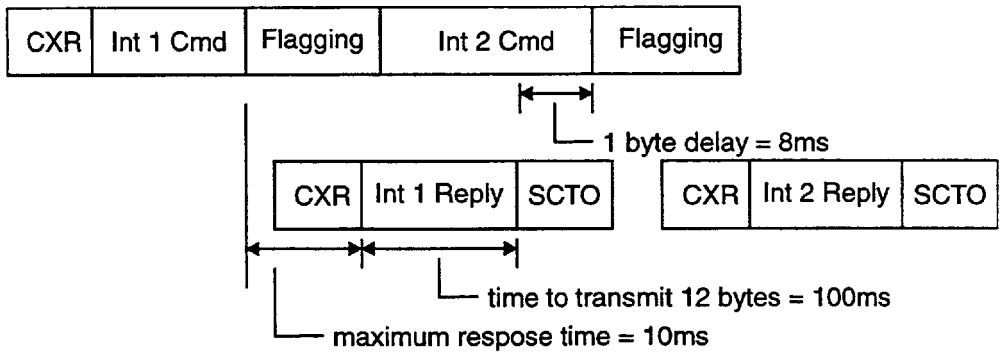


Figure A-2
FULL DUPLEX TIMING

In full duplex operation, a primary station can start transmission of the next command before the response to the last command is received. However, to ensure that two secondaries are not transmitting at the same time, a primary station shall not transmit the closing flag of the next command until the closing flag of the reply from the previous command has been received; an 8 ms, 1 byte delay. The maximum response delay is the time between the end of a command and the start of the response to it. This is assumed to be 10 ms. If a sequence of messages is to maintain a one second resolution, the maximum number of intersections polled in one second is 8 (1 s / 118 ms). This parameter is valid if byte stuffing is random.

For timing purposes in full duplex, the minimum response time of a secondary has been specified as 10 ms. This is the expected delay before a secondary station starts transmitting its opening flag after receiving a closing flag. It is based upon the 8 ms Clear-To-Send Delay plus a 2 ms delay in terms of recognizing a command needs a response. Figure A-3 applies to half duplex.

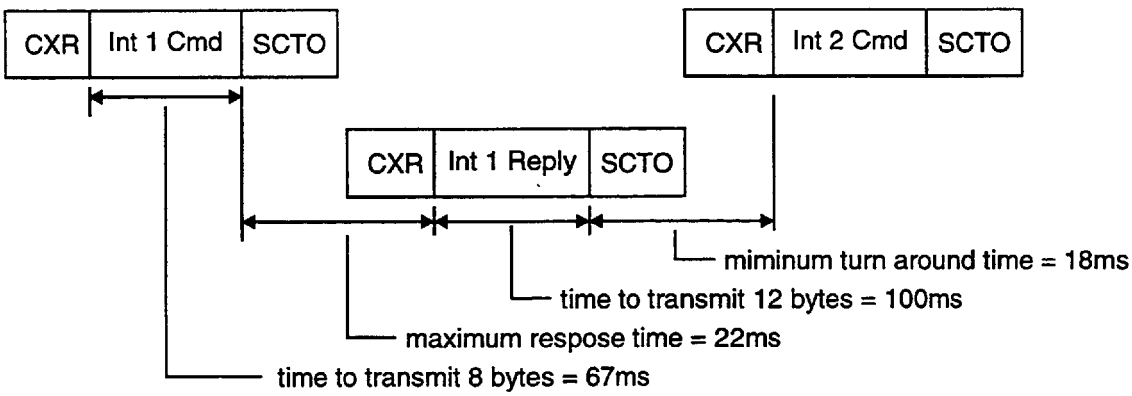


Figure A-3
HALF DUPLEX TIMING

For the sequence of messages, as stated above, and using a half duplex FSK Modem Interface, then the maximum number of intersections polled in one second is slightly over 4 (1 s / 207 ms).

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(Normative)
CLASS B PROFILE MIB

B.1 OVERVIEW

To manage any network, whether it be the Internet or a traffic control network, there are various objects that are defined to set up and monitor the network. There are also objects that are applicable to any installation. For example, an RS232 port can be set up for various baud rates and parity options. A station that implements NTCIP should also be identifiable in a standard method. The following MIBs define the objects and groups of objects that constitute the lowest acceptable bounds of implementation for the communications protocol. The first MIB is written in conformance to RFC 1212 for those agent or management stations that only support SNMP(v1). Since SNMP(v1) does not have a formal method for defining conformance and compliance, the first MIB can be extended by comparable statements that are defined in other RFC's. Only those agent or management stations that may support those RFCs may use them.

The MIB shown in B.2 contains the objects that appear in the Internet tree and are applicable to specific layers in the Class B Profile. Objects related to the Physical, Data Link, Network, and Application Layers are referenced. It also organizes those objects into specific groups. Following the guideline that predefined objects should be reused rather than creating new ones, the Class-B-PROFILE-MIB references which Internet objects apply to the Class B Profile.

The MIB shown in B.3 uses MODULE-IDENTITY and MODULE-COMPLIANCE notation to formally define which groups are applicable to the Class B Profile. It also incorporates a means of identifying the supplier of a MIBs. While its use it not mandated, this organization will be beneficial when there are multiple class profiles and several profiles supported within one entity.

The MIB shown in B.4 uses the AGENT-CAPABILITIES macro from RFC 1444 to state the variances from the standard Internet objects. For example, the Internet maximum frame size at the data link layer is 4500 bytes. For the Internet this may be a suitable value, but for the expected traffic of NTCIP, a limit of 512 is a more appropriate value. The MIB is presented as an example of how a specific implementation can further refine its capabilities and add clarification to various objects.

B.2 CLASS B MIB DEFINITION

The following is the Class B Profile MIB. All devices supporting the Class B Profile shall support the objects and object identifiers defined herein.

```
Class-B-PROFILE-MIB  DEFINITIONS ::= BEGIN

  IMPORTS

    sysDescr,
    sysObjectID,
    sysUpTime,
    sysContact,
    sysName,
    sysLocation,
    sysServices
```

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

FROM RFC 1213-MIB

atTable,
atEntry,
atIfIndex,
atPhysAddress,
atNetAddress
FROM RFC 1213-MIB

rs232Number,
rs232PortTable,
rs232PortEntry,
rs232PortIndex,
rs232PortType,
rs232PortInSpeed,
rs232PortOutSpeed,
rs232AsyncPortTable,
rs232AsyncPortEntry,
rs232AsyncPortIndex,
rs232AsyncPortFramingErrs,
rs232AsyncPortOverrunErrs
FROM RFC 1317-MIB

lapbOperTable,
lapbOperEntry,
lapbOperIndex,
lapbOperTransmitN1FrameSize,
lapbOperReceiveN1FrameSize,
lapbOperT1AckTimer,
lapbOperT2AckDelayTimer,
lapbOperT3DisconnectTimer,
lapbOperT4IdleTimer,
lapbOperPortId
FROM RFC 1381-MIB

snmpInPkts,
snmpOutPkts,
snmpInBadVersions,
snmpInBadCommunityNames,
snmpInBadCommunityUses,
snmpInASNParseErrs,
snmpInTooBigs,
snmpInNoSuchNames,
snmpInBadValues,
snmpInReadOnlys,
snmpInGenErrs,
snmpInGetRequests,
snmpInGetNexts,
snmpInSetRequests,
snmpInGetResponses,
snmpInTraps,
snmpOutTooBigs,
snmpOutNoSuchNames,
snmpOutBadValues,
snmpInGenErrs,

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

```
    snmpOutGetRequests,
    snmpOutGetNexts,
    snmpOutSetRequests,
    snmpOutGetResponses,
    snmpOutTraps,
    snmpEnableAuthenTraps
      FROM RFC 1213-MIB
END
```

B.3 MIB COMPLIANCE

The following is an extension to the Class B Profile MIB that adds formal compliance statements. It is written in terms of SNMPv2. It is only intended for those stations supporting SNMPv2.

```
Class-B-PROFILE-MIB II DEFINITIONS ::= BEGIN

  IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE
      FROM SNMPV2-SMI

    MODULE-COMPLIANCE, OBJECT-GROUP
      FROM SNMPV2-CONF

layers ::= { nema transportation protocols 1 }

NTCIPrs232Group   OBJECT-GROUP
    OBJECTS { rs232Number, rs232PortTable,
              rs232PortEntry, rs232PortIndex, rs232PortType,
              rs232PortInSpeed, rs232PortOutSpeed}
    STATUS  current
    DESCRIPTION
        "A collection of objects providing information applicable to all RS-232-like interfaces. This
        includes the FSK interface."
    ::= { layers 1}

NTCIPrs232AsyncGrp OBJECT-GROUP
    OBJECTS { rs232AsyncPortTable,  rs232AsyncPortEntry, rs232AsyncPortIndex,
              rs232AsyncPortFramingErrs, rs232AsyncPortOverrunErrs }
    STATUS  current
    DESCRIPTION
        "A collection of objects providing information applicable to asynchronous RS-232-like
        interfaces. This includes the FSK interface."
    ::= { layers  2 }

NTCIPhdlcGroup OBJECT-GROUP
    OBJECTS {lapbOperTable, lapbOperEntry, lapbOperIndex,
              lapbOperTransmitN1FrameSize, lapbOperReceiveN1FrameSize,
              lapbOperT1AckTimer, lapbOperT2AckDelayTimer,
              lapbOperT3DisconnectTimer, lapbOperT4IdleTimer,
              lapbOperPortId }
    STATUS  current
    DESCRIPTION
```

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

```
        "A collection of objects related to the HDLC data link layer."
    ::= { layers 3 }

NTCIPtransGroup   OBJECT-GROUP
    OBJECTS { atTable, atEntry, atIfIndex,
              atPhysAddress, atNetAddress}
    STATUS  current
    DESCRIPTION
        "The Address Translation group contains one table which is
         the union across all interfaces of the translation tables
         for converting a NetworkAddress (e.g., an IP address) into
        a subnetwork-specific address.  For lack of a better term,
        this document refers to such a subnetwork-specific address
        as a 'physical' address."
    ::= { layers 4 }

NTCIPsnmpGroup OBJECT-GROUP
    OBJECTS { snmpInPkts, snmpOutPkts,
              snmpInBadVersions, snmpInBadCommunityNames,
              snmpInBadCommunityUses, snmpInASNParseErrs,
              snmpInTooBigs, snmpInNoSuchNames,
              snmpInBadValues, snmpInReadOnlys,
              snmpInGetRequests,
              snmpInGetNexts, snmpInSetRequests,
              snmpInGetResponses, snmpInTraps,
              snmpOutTooBigs, snmpOutNoSuchNames,
              snmpOutBadValues, snmpOutGenErrs,
              snmpOutGetRequests, snmpOutGetNexts,
              snmpOutSetRequests, snmpOutGetResponses,
              snmpOutTraps, snmpEnableAuthenTraps }
    STATUS  current
    DESCRIPTION
        "A collection of objects providing status and control of the
         SNMP / STMP entity."
    ::= { layers 5 }

NTCIPsystemGroup   OBJECT-GROUP
    OBJECTS { SysDescr, sysObjectID, sysUpTime,
              sysContact, sysName, sysLocation,
              sysServices }
    STATUS  current
    DESCRIPTION
        "A collection of objects providing system information about the device implementing
         NTCIP."
    ::= { layers 6 }

profiles ::=  { nema transportation protocols 2 }

classB ::= { profiles 1 }

  classBprofile MODULE-IDENTITY
    LAST-UPDATED "9511072215Z"
    ORGANIZATION "National Electrical Manufacturers Association"
```

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

```
    CONTACT-INFO
          "     V.P. Engineering
                National Electrical Manufacturers Association
                1300 N. 17th Street
                Rosslyn, Virginia 22209 "
    DESCRIPTION
          "The MIB module for the NTCIP Class B Profile devices."
    ::= {classB 1}

-- compliance statements

  classBCompliances MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
          "The compliance statement for all NTCIP Class B Profile entities."
    MODULE  -- this module
      MANDATORY-GROUPS {NTCIPrs232Group,
                        NTCIPrs232AsyncGroup,
                        NTCIPhdlcGroup,
                        NTCIPtransGroup,
                        NTCIPsnmpGroup,
                        NTCIPsystemGroup }
      DESCRIPTION
          "The above groups are mandatory for all NTCIP
           Class B profile entities"

    ::= {classB 2}

END
```

B.4 AGENT CAPABILITIES MIB

The following is an example of how the AGENT-CAPABILITIES macro can be used to refine an implementation of standard objects defined by other RFCs. For example, the RFC covering RS 232 like devices does not have an identifier for an FSK interface. It is possible to add an identifier using this a VARIATION statement. Another change may state that the access of an object is read-only instead of read-write. For example, the baud rate of an FSK Interface is fixed at 1200 bps and cannot be changed. The AGENT-CAPABILITIES macro is only applicable to stations that support it.

```
exampleAgent AGENT-CAPABILITIES
        PRODUCT-RELEASE  "Traffic Controller Agent release 1.0 for NTCIP Class B"
        STATUS           current
        DESCRIPTION      "Traffic Controller agent for NTCIP Class B"

        SUPPORTS         RFC1213-MIB
          INCLUDES      {NTCIPrs232Group,
                         NTCIPrs232AsyncGrp,
                         NTCIPhdlcGroup,
                         NTCIPtransGroup,
                         NTCIPsnmpGroup,
                         NTCIPsystemGroup,
                         NTCIPsystemGroup },
```

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

```
        VARIATION       atPhysAddress
                SYNTAX          OCTET STRING  ( SIZE (2) )
                DESCRIPTION     "The 2 byte physical address of  the device in the range of 1..2^13. Value
                                may indicate a group address. In transmission, the address may be
                                shortened to one byte."

-->>>>
```

NEMA STANDARDIZATION BACKGROUND

The purpose of NEMA standards, their classification, and status are set forth in certain clauses of the NEMA *Standardization Policies and Procedures* manual and are referenced below:

Purpose of Standards

National Electrical Manufacturers Association Standards are adopted in the public interest and are designed to eliminate misunderstandings between the manufacturer and the purchaser and to assist the purchaser in selecting and obtaining the proper product for their particular needs. Existence of a National Electrical Manufacturers Association Standard does not in any respect preclude any member or nonmember from manufacturing or selling products not conforming to the standard.

Definition of a Standard

A standard of the National Electrical Manufacturers Association defines a product, process, or procedure with reference to one or more of the following; nomenclature, composition, construction, dimensions, tolerances, safety, operating characteristics, performance, rating, testing, and the service for which they are designed.

(Standardization Policies and Procedures, p. 1)

Dimensions

Where dimensions are given for interchangeability purposes, alternate dimensions satisfying the other provisions of the Standards Publication may be capable of otherwise equivalent performance.

(Standardization Policies and Procedures, p. 6)

Categories of Standards

National Electrical Manufacturers Association Standards are of three classes, which have received the affirmative vote of at least two-thirds of the Subdivision votes cast in the affirmative or negative:

NEMA Standard, which relates to a product, process, or procedure commercially standardized and subject to repetitive manufacture.

Suggested Standard for Future Design, which may not have been regularly applied to a commercial product, but which suggests a sound engineering approach to future development.

Adoptive Standard, which is adopted in whole or in part from the standards of another organization, either domestic, regional, or international.

(Standardization Policies and Procedures, p. 5)

Authorized Engineering Information

Authorized Engineering Information consists of explanatory data or other engineering information of an informative character not falling within the classification of NEMA Standard or Suggested Standard for Future Design, which standard has received the affirmative vote of at least two-thirds of the Subdivision votes cast in the affirmative or negative.

(Standardization Policies and Procedures, p. 5)

Identification of Status

Standards in NEMA Standards Publications are identified as "NEMA Standard," "Suggested Standard for Future Design," or "Adoptive Standard." These indicate the status of the standard. A statement incorporating the auxiliary verb "shall" indicates that compliance with a requirement is mandatory for compliance with the standard. These classes of standards are identified in the foreword or throughout the text.

The material identified as "Authorized Engineering Information" is designated similarly. Statements incorporating other auxiliary verbs such as "should," "may," etc. refer to the authorized engineering information and not to procedures required for compliance with the standard.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale



NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION • 1300 N. 17TH STREET • ROSSLYN, VA 22209

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale