A Joint Standard of AASHTO, ITE, and NEMA

NTCIP 2202:2001 v01.05

National Transportation Communications for ITS Protocol

Internet (TCP/IP and UDP/IP) Transport Profile

December 2001

This Adobe® PDF copy of an NTCIP standard is available at no-cost for a limited time through support from the U.S. DOT / Federal Highway Administration, whose assistance is gratefully acknowledged.

Published by

American Association of State Highway and Transportation Officials (AASHTO)
444 North Capitol Street, N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)
1099 14th Street, N.W., Suite 300 West
Washington, D.C. 20005-3438

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209-3801

ACKNOWLEDGEMENTS

This publication was prepared by the NTCIP Profiles Working Group, which is a subdivision of the Joint Committee on the NTCIP. The Joint Committee is organized under a Memorandum of Understanding among the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA). The Joint Committee on the NTCIP consists of six representatives from each of the standards organizations, and provides guidance for NTCIP development.

At the time that this document was prepared, the following individuals were active members of the NTCIP Profiles Working Group:

- Robert De Roche (Chair)
- Robert Force
- W. L. (Bud) Kent
- Gary Meredith
- Alexis Mousadi
- Brian Paulsmeyer
- Mike Robinson
- Nu Rosenbohm
- Kenneth Vaughn
- Hoi Wong

Other individuals providing input to the document include:

- Joey Baumgartner
- Al Bonificio
- Ken Earnest
- Michael Forbis
- Joseph Herr
- Dave Kingery
- Doug Lowe
- Don Ninke
- Jeff Racz

In addition to the many volunteer efforts, recognition is also given to those organizations who supported the efforts of the working groups by providing comments and funding for the standard, including:

- ARINC, Inc.
- Caltrans
- Eagle Traffic Control Systems
- Econolite Control Products, Inc
- Ministry of Transportation, Ontario
- Naztec, Inc
- New York State DOT
- Odetics ITS, Inc.
- PB Farradyne, Inc.
- Peek Traffic Systems, Inc.
- Southwest Research Institute
- Texas DOT
- Vanasse, Hagen, & Brustlin, Inc.
- Washington State DOT

The Internet (TCP/IP and UDP/IP) Transport Profile is based upon a Department of Defense Standardized Profile for the specification and implementation of the TCP/IP and UDP/IP Protocols; MIL-STD-2045-14502-1A: 27 July 1995. NTCIP 2202 borrows heavily from that work and special credit is due the Data Communications Protocol Standards Technical Management Panel for publishing the standard and placing it in the public domain.

FOREWORD

This document uses only metric units.

This publication defines a transport profile that is a combination of standards intended to meet specific requirements for transport services in transportation devices and management centers in a networked environment. The scope covers the transport and network layers of the OSI Reference Model. This publication contains mandatory requirement statements that are applicable to all devices claiming conformance to this standard. This publication also contains optional and conditional requirements that may be applicable to a specific environment in which a device is used.

The text includes mandatory requirements in Annex A that are defined as normative.

For more information about NTCIP standards, visit the NTCIP Web Site at http://www.ntcip.org. For a hardcopy summary of NTCIP information, contact the NTCIP Coordinator at the address below.

In preparation of this NTCIP document, input of users and other interested parties was sought and evaluated. Inquires, comments, and proposed or recommended revisions should be submitted to:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1847
Rosslyn, VA 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

Approvals

This document was separately balloted and approved by AASHTO, ITE, and NEMA after recommendation by the Joint Committee on the NTCIP. Each organization has approved this standard as the following standard type, as of the date:

AASHTO – Standard Specification; May 2000
ITE – Software Standard; May 2001
NEMA – Standard; January 2001

History

From 1998 to 1999, this document was referenced as TS 3.TP-INTERNET or TS 3.TUI. However, to provide an organized numbering scheme for the NTCIP documents, this document is now referenced as NTCIP 2202. The technical specifications of NTCIP 2202 are identical to the former reference, except as noted in the development history below:

TS 3.TP-INTERNET v98.01.09. October 1998 – Accepted as a User Comment Draft by the Joint Committee on the NTCIP.

NTCIP 2202 v99.01.04. July 1999 – Version 01.03 accepted as a Recommended Standard by the Joint Committee on the NTCIP. NTCIP Standards Bulletin B0043 reported typographic corrections from the prior version. Approved by AASHTO in May 2000, approved by ITE in May 2001, and approved by NEMA in January 2001.

NTCIP 2202:2001 v01.05. December 2001 – Reformatted for printing: Incremented version number and updated date; added and revised front matter to conform to NTCIP 8002, and updated headers, footers, and page numbers.

<This page is intentionally left blank>

INTRODUCTION

The context of the NTCIP is one part of the Intelligent Transportation Systems standardization activities covering base standards, profiles, and registration mechanisms.

- Base Standards define procedures and rules for providing the fundamental operations associated with communications and information that is exchanged over fixed-point communications links.

- Profiles define subsets or combinations of base standards used to provide specific functions or services. Profiles prescribe particular subsets or options available in base standards necessary for accomplishing a particular function or service. This provides a basis for the development of uniform, nationally recognized conformance.

- Registration Mechanisms provide a means to specify and uniquely identify detailed parameters within the framework of base standards and/or profiles.

The Profiles Working Group is concerned with the methodology of defining profiles, and their documentation in Standards Publications. This standard defines a transport profile that provides connectionless and connection-oriented transport services over a connectionless network service and is based upon the Internet TCP/IP Protocol Suite. The objective is to facilitate the specification of ITS characterized by a high degree of interoperability and interchangeability of its components.

In 1992, the NEMA 3-TS Transportation Management Systems and Associated Control Devices Section began the effort to develop the NTCIP. Under the guidance of the Federal Highway Administration's NTCIP Steering Group, the NEMA effort was expanded to include the development of communications standards for all transportation field devices that could be used in an ITS network.

In September 1996, an agreement was executed among AASHTO, ITE, and NEMA to jointly develop, approve, and maintain the NTCIP standards.

After research into how national and international standards organizations combine protocols and standards to address all seven layers of the ISO-OSI Reference Model, the committee adopted the approach defined in the *NTCIP Profile Framework.* Following that approach, a protocol stack is specified by application, transport, and subnetwork profiles. An application profile addresses the application, presentation, and session layers. A transport profile addresses the transport and network layers. A subnetwork profile addresses the data link and physical layers. The *NTCIP Internet (TCP/IP and UDP/IP) Transport Profile* (TP-Internet) is a transport profile for use in center-to-roadside and center-to-center communications.

If you are not willing to abide by the following notices, return these materials immediately.

Joint AASHTO, ITE, and NEMA
NTCIP Profile Requirements List
REPRODUCTION NOTICE

AASHTO / ITE / NEMA extend permission to the purchaser of this standards publication to make and/or distribute unlimited copies (including derivative works, which will then be known as PICS) of the excerpt identified as the Profile Requirements List, including copies for commercial distribution, provided that each copy made or distributed contains the notice “Based on an NTCIP Profile Requirements List. Used by permission of AASHTO / ITE / NEMA.”

Disclaimer

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

AASHTO, ITE, and NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While AASHTO, ITE, and NEMA administer the process and establish rules to promote fairness in the development of consensus, they do not write the document and they do not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in their standards and guideline publications.

AASHTO, ITE, and NEMA disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. AASHTO, ITE, and NEMA disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. AASHTO, ITE, and NEMA do not undertake to guarantee the performance of any individual manufacturer or seller’s products or services by virtue of this standard or guide.

In publishing and making this document available, AASHTO, ITE, and NEMA are not undertaking to render professional or other services for or on behalf of any person or entity, nor are AASHTO, ITE, and NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

AASHTO, ITE, and NEMA have no power, nor do they undertake to police or enforce compliance with the contents of this document. AASHTO, ITE, and NEMA do not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety–related information in this document shall not be attributable to AASHTO, ITE, or NEMA and is solely the responsibility of the certifier or maker of the statement.

CONTENTS

Section 1
GENERAL

1.1 SCOPE

This standard is applicable to transportation devices and management systems that must operate in Intelligent Transportation Systems. As a transport profile, it specifies a set of protocols and standards applicable to the transport and network layers of the ISO - OSI Reference Model. The set of protocols provides a connectionless or connection-oriented transport service over a connectionless network service. This standard is intended to provide message transport and delivery services between transportation devices and a management station or among multiple centers. This standard applies to end systems concerned with implementing the TCP/IP protocol suite.

1.2 PROFILE-PROTOCOL-LAYER RELATIONSHIP

This transport profile specifies the provision for connectionless or connection-oriented transport service between an end system connected to a subnetwork and another compatible end system through the IP connectionless network service. The interoperable end system may use mutually agreed upon access methods contained within this TP, or may conform to a mutually agreed upon alternative access method. An end system is compatible only if the suboptions (e.g., TCP) are compatible. A complete transport profile requires knowledge of the subnetwork type, access method, circuit type, and service type. The layers, base standards and profile taxonomy that make up this profile are shown in Figure 1.

ISO Layers	Base Standards	Profile
TRANSPORT LAYER	IAB STD 7 (TCP) IAB STD 6 (UDP)	NTCIP 2202 (Internet Transport Profile)
NETWORK LAYER	IAB STD 5 (IP and ICMP)	

Figure 1
TCP/IP and UDP/IP - Transport Profile Relationship

1.3 REFERENCES

For approved revisions, contact:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1847
Rosslyn, VA 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

For draft revisions of this document, which are under discussion by the relevant NTCIP Working Group, and recommended revisions of the NTCIP Joint Committee, visit the World Wide Web at http://www.ntcip.org.

The following standards (normative references) contain provisions which, through reference in this text, constitute provisions of this Standard. Other documents and standards (other references) are referenced in these documents, which might provide a complete understanding of the structure and use of profiles. 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.

1.3.1 Normative References

Internet Activities Board
available via electronic file transfer
use anonymous FTP from
nic.ddn.mil or ds.internic.net

IAB STD 3 *(RFC 1122: 1989, Requirements For Internet Hosts - Communication Layers, RFC 1123: 1989, Requirements For Internet Hosts - Application and Support)*

IAB STD 5 *RFC 791: 1981, Internet Protocol, RFC 950: 1985, Internet standard subnetting procedure, RFC 919: 1984, Broadcasting Internet datagrams, RFC 922: 1984, Broadcasting Internet datagrams in the presence of subnets, RFC 792: 1981, Internet Control Message Protocol, RFC 1112: 1989, Host extensions for IP multicasting)*

IAB STD 6 *(RFC 768: 1980, User Datagram Protocol)*

IAB STD 7 *(RFC 793: 1981, Transmission Control Protocol)*

IAB STD 17 *(RFC 1213: 1991, Management Information Base)*

1.3.2 Other References

Guide to Open System Specifications, European Workshop for Open Systems, http://www.ewos.be/goss/top.htm, June 9, 1997

US-DOD Internet Related Standardized Profiles, DISA Internet Librarian, http://www-library.itsi.disa.mil/org/mil_std.html, October 31, 1997

1.4 DEFINITIONS

For the purposes of this standard, the following definitions apply:

Application Layer: That portion of the OSI Reference Model (Layer 7) that provides access to the communications services.

data: Information before it is interpreted.

Data Link Layer: That portion of the OSI Reference Model (Layer 2) responsible for flow control, framing, synchronization, and error control over a communications link.

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

end system: The source or destination of an information exchange.

host: (Internet usage) The physical and/or logical part of the end-system's application. A computer attached to one or more networks that supports users and runs application programs.

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

intermediate system: A system that participates in an information exchange but is not the source or destination of the exchange.

internet: Any collection of connected networks where information can be passed form one network to another.

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 protocol: The network protocol offering a connectionless mode network service in the Internet suite of protocols.

Internet Protocol Suite: A collection of computer-communication protocols originally developed under DARPA sponsorship.

internetwork: The ability of devices to communicate across multiple networks.

network: A collection of subnetworks connected by intermediate systems and populated by end systems.

Network Layer: That portion of an OSI Reference Model (Layer 3) 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 a network, usually referring to the management of devices that contain information about setup, control, and status of the layers in a communications stack. The term refers to all devices, both intermediate and end systems, that are present on the network or internetwork.

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

OSI Reference Model: A widely accepted structuring technique that provides an abstract representation of the communication process that is divided into seven basic, functional layers.

Physical Layer: That portion of an OSI Reference Model (Layer 1) responsible for the electrical and mechanical interface between communicating systems.

Presentation Layer: That portion of an OSI Reference Model (Layer 6) responsible for converting and organizing data from one format to another.

proforma: A guide provided in advance to prescribe form or describe items.

Session Layer: That portion of an OSI Reference Model (Layer 5) which manages a series of data exchanges between end-system applications.

subnetwork: A physical network within a network. All devices on a subnetwork share a common physical medium.

taxonomy: A classification scheme for referencing profiles or sets of profiles unambiguously.

TCP/IP Reference Model: An alternate to the OSI Reference Model that organizes the communications process into 4 layers. It consists of host-to-network, internet, transport, and application layers.

Transport Layer: That portion of an OSI Reference Model (Layer 4) which attempts to guarantee reliable data transfer between two end-systems, using flow control and error recovery, and may provide multiplexing.

1.5 ABBREVIATIONS AND ACRONYMS

The abbreviations used in this Standard Publication are defined as follows:

AASHTO American Association of State Highway and Transportation Officials
EIA Electronic Industries Association
FTP File Transfer Protocol
IAB STD Internet Advisory Board Standard
IEEE Institute of Electrical and Electronic Engineers
IP Internet Protocol
ISO International Organization for Standardization
ITE Institute of Transportation Engineers
ITS Intelligent Transportation Systems
NEMA National Electrical Manufacturers Association
NTCIP National Transportation Communications for ITS Protocol
OSI Open Systems Interconnection
PICS Protocol Implementation Conformance Statement
PMPP Point to Multi-Point Protocol
PPP Point-to-Point Protocol
RFC (Internet) Request for Comments
SNMP Simple Network Management Protocol
STMF Simple Transportation Management Framework
TCP Transmission Control Protocol
TP Transport profile
UDP User Datagram Protocol

Section 2
CONFORMANCE

2.1 GENERAL REQUIREMENTS

Implementations claiming conformance to the TCP/IP Configuration of the Internet (TCP/IP and UDP/IP) Transport Profile shall support the following elements as stated.

a. All requirements in the remainder of Section 2 of this profile.
b. All of the constraints specified in Annex A (normative) of this profile.
c. All mandatory requirements of the standards referenced by this profile.

Implementations claiming conformance to the UDP/IP Configuration of the Internet (TCP/IP and UDP/IP) Transport Profile shall support the following elements as stated.

a. All requirements in the remainder of Section 2 except for Section 2.2.1 of this profile.
b. All of the constraints specified in Annex A (normative) of this profile.
c. All mandatory requirements of the standards referenced by this profile.

2.2 TRANSPORT LAYER REQUIREMENTS

A conforming implementation of this profile shall use TCP (IAB STD 7, RFC 793) and/or UDP (IAB STD 6, RFC 768), and shall conform to Requirements for Internet Hosts - Communication Layers (IAB STD 3, RFC 1122).

2.2.1 Transmission Control Protocol (TCP)

2.2.1.1 Major Capabilities

A conforming implementation of TCP shall support the following capabilities in accordance with the indicated base standards:

a. data transfer as specified in RFC 793, Sections 1.5, 2.8, and 3.7.
b. addressing (especially well-known ports) as specified in RFC 793, Section 2.7 and RFC 1122, Section 4.2.2.1.
c. fragmentation and reassembly as specified in RFC 793, Sections 1.5, 2.7, and 3.3 and RFC 1122, Sections 3.3.2, 3.3.3, and 4.2.2.6.
d. piggyback acknowledgment as specified in RFC 793, Sections 1.5, 2.6, 3.7, and 3.9 and RFC 1122, Section 4.2.3.2.
e. flow control as specified in RFC 793, Section 1.5, 2.6, and 3.7 and RFC 1122, Section 4.2.3.3.
f. checksum computation as specified in RFC 793, Sections 1.5, 3.1, and 3.8, and RFC 1122, Section 4.2.2.7.
g. error recovery as specified in RFC 793, Sections 1.5 and 3.7, and RFC 1122, Sections 4.2.3.1 and 4.2.2.15.
h. precedence and security as specified in RFC 793, Sections 1.5, 2.9, and 3.6.
i. multiplexing as specified in RFC 793, Sections 1.5, 2.7, and 3.8 and RFC 1122, Section 4.2.2.1 and 4.2.2.18.
j. MIB-II tcp group as specified in RFC 1213, Sections 3.9 and 6.8.

2.2.1.2 Header Format

A conforming implementation shall support the following fields as described in RFC 793, Section 3.1:

a. source port
b. destination port
c. sequence number
d. acknowledgment number
e. data offset
f. reserved field
g. control bits (urgent, acknowledgment, push, reset, synchronize, finish data send)
h. window field
i. checksum
j. urgent pointer
k. options (end of option list, no-operation, maximum segment size)
l. padding
m. data

2.2.1.3 Detailed Requirements

This paragraph identifies additional requirements, or clarifications of requirements to support the transportation industry use of Internet standards referenced by this TP.

2.2.1.3.1 Interface Requirements

2.2.1.3.1.1 ICMP messages from IP

A conforming implementation shall act upon ICMP messages as stated in RFC 1122, Section 4.2.3.9.

2.2.1.3.1.2 TCP to Application Layer Interface

A conforming implementation shall support the TCP to Application Layer Interface requirements as defined in RFC 1122, Section 4.2.4.

2.2.1.3.1.3 IP Options

A conforming implementation shall support the IP options delineated in RFC 1122, Section 4.2.3.8.

2.2.1.3.1.4 Address Validation

A conforming implementation shall perform the functions described in RFC 1122, Section 4.2.3.10.

2.2.1.3.2 Connection Management and Data Transfer Requirements

2.2.1.3.2.1 Push Flag

The push flag shall be implemented as described in RFC 793, Section 2.8 and RFC 1122, Section 4.2.2.2.

2.2.1.3.2.2 Window Management

Window management shall be implemented as described in RFC 793, Sections 3.1 and 3.7, and RFC 1122, Sections 4.2.2.3, 4.2.2.16, and 4.2.2.17.

2.2.1.3.2.3 Urgent Data

Urgent Data shall be labeled as described in RFC 793, Section 3.1, and RFC 1122, Section 4.2.2.4.

2.2.1.3.2.4 TCP Options

TCP Options shall be implemented as described in RFC 793, Section 3.1, and RFC 1122, Sections 4.2.2.5 and 4.2.2.6.

2.2.1.3.2.5 TCP Checksums

A conforming implementation shall compute and check checksums as stated in RFC 793, Section 3.1, and RFC 1122, Section 4.2.2.7.

2.2.1.3.2.6 Initial Sequence Number (ISN) Selection

ISN selection shall be performed as described in RFC 793, Section 3.3, and RFC 1122, Section 4.2.2.9.

2.2.1.3.2.7 Opening Connections

The opening connection shall be implemented as described in RFC 793, Section 3.4 and RFC 1122, Sections 4.2.2.10, 4.2.2.11, 4.2.2.18, 4.2.3.7, and 4.2.3.10.

2.2.1.3.2.8 Closing Connection

Closing a connection shall be implemented as described in RFC 793, Section 3.5 and RFC 1122, Section 4.2.2.12 and 4.2.2.13.

2.2.1.3.2.9 Retransmissions

Retransmission shall be implemented as described in RFC 793 Section 3.7 and RFC 1122, Sections 4.2.2.15 and 4.2.3.1.

2.2.1.3.2.10 Generating ACKnowledgments (ACKs)

A conforming implementation shall generate ACKs as described in RFC 793, Section 3.9, and RFC 1122, Sections 4.2.2.20, 4.2.2.21, 4.2.3.2, and 4.2.3.3.

2.2.1.3.2.11 Sending Data

A conforming implementation shall perform the functions described in RFC 1122, Sections 4.2.2.19, and 4.2.3.4. The Nagle algorithm shall be used, and implementations shall retain the capability to disable the Nagle algorithm when necessary.

2.2.1.3.2.12 Connection Failures

A conforming implementation shall act upon a connection failure as described in RFC 1122, Section 4.2.3.5.

2.2.1.3.2.13 Send Keep-Alive Packets

Keep-alive packets are recommended for use in transportation implementations, but are not mandatory. There are no additional requirements to those described in RFC 1122, Section 4.2.3.6.

2.2.1.3.2.14 MIB-II TCP Group Object Definitions

A conforming implementation shall support the MIB-II tcp group object definitions as defined in RFC 1213 Sections 3.9 and 6.8.

2.2.2 User Datagram Protocol (UDP)

2.2.2.1 Major Capabilities

A conforming implementation of UDP shall support the following capabilities in accordance with the indicated base standards:

a. data transfer as specified in RFC 768, page 2 and RFC 1122, Section 4.1.1.
b. port addressing as specified in RFC 768, pages 1 and 2 and RFC 1122, Sections 4.1.1, 4.1.3.1, 4.1.3.5, and 4.1.3.6.
c. checksum as specified in RFC 768, page 2 and RFC 1122, Sections 4.1.1 and 4.1.3.4.
d. MIB-II udp group as specified in RFC 1213, Sections 3.10 and 6.9.

2.2.2.1.1 Header Format

A conforming implementation shall support the following fields as described in RFC 768:

a. source port
b. destination port
c. length
d. checksum

2.2.2.2 Detailed Requirements

2.2.2.2.1 Interface Requirements

General Interface requirements are as specified in RFC 768.

2.2.2.2.1.1 ICMP Messages from IP

A conforming implementation shall act upon all ICMP messages as stated in RFC 1122, Section 4.1.3.3.

2.2.2.2.1.2 UDP to Application Layer Interface

A conforming implementation shall support the UDP to Application Layer Interface requirements as defined in RFC 1122, Section 4.1.4.

2.2.2.2.1.3 IP Options

A conforming implementation shall pass IP options as described in RFC 1122, Section 4.1.3.2. A user-defined IP option is described for use with multiple addressing. This transport profile defines this option.

2.2.2.2.2 Data Transfer Requirements

2.2.2.2.2.1 UDP Checksum

A conforming implementation shall implement and use the checksum as described in RFC 1122, Section 4.1.3.4.

2.2.2.2.2.2 UDP Multihoming

A conforming implementation shall provide for UDP Multihoming as described in RFC 1122, Section 4.1.3.5.

2.2.2.2.2.3 MIB-II UDP Group Object Definitions

A conforming implementation shall support the MIB-II udp group object definitions as defined in RFC 1213, Sections 3.10 and 6.9.

2.3 NETWORK LAYER REQUIREMENTS

A conforming implementation of this profile shall use IAB STD 5, specifically the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). A conforming implementation of the IP protocol shall conform to IAB STD 3, RFC 1122 (Requirements For Internet Hosts - Communication Layers).

The Internet Protocol, IP, forms the network layer of this profile. IP is specified in RFC 791, as amended by RFC 950 (IP Subnet Extensions), RFC 919 (IP Broadcast Datagrams), and RFC 922 (IP Broadcast Datagrams with subnets). It also includes ICMP, the Internet Control Message Protocol, specified by RFC 792, which provides a mechanism for communicating control and error information between hosts or between hosts and gateways. Although ICMP is an integral part of IP, it uses the support of IP as if it (ICMP) were a higher layer protocol.

2.3.1 Internet Protocol

2.3.1.1 Major Capabilities

A conforming implementation shall support the following capabilities:

a. data transfer as specified in RFC 791, Sections 1.1 and 2.3.
b. addressing as specified in RFC 791, Sections 1.4, 2.3, 3.1, and 3.2 and RFC 1122, Section 3.2.1.3.
c. fragmentation/reassembly as specified in RFC 791, Section 1.4, 2.3, 3.1, 3.2 and RFC 1122, Section 3.3.2, 3.3.3, and 3.2.1.4.
d. header checksum as specified in RFC 791, Section 1.4, 3.1 (page 14), and RFC 1122, Section 3.2.1.2.
e. Type of Service (TOS) field as specified in RFC 791, Section 1.4, 3.1, 3.2 and RFC 1122, Section 3.2.1.6.
f. time-to-live as described in RFC 1122, Section 3.2.1.7
g. additional options as described in RFC 1122, Section 3.2.1.8, as further modified by this standard.
h. MIB-II ip group as specified in RFC 1213, Section 3.7 and 6.6.

2.3.1.2 Datagram Format

A conforming implementation shall support the following fields as described in RFC 791, Section 3.1 and 3.2:

a. version number, also as specified in RFC 1122, Section 3.2.1.1
b. Internet Header Length (IHL)

c. type of service (TOS), also as specified in RFC 1122, Section 3.2.1.6
d. total length of datagram
e. segment identification, also as specified in RFC 1122, Section 3.2.1.5
f. control flags
g. fragment offset, also as specified in RFC 791, Section 3.2 and RFC 1122, Sections 3.2.1.4 and 3.2.1.5
h. time-to-live (TTL), also as specified in RFC 1122, Section 3.2.1.7
i. protocol
j. header checksum, also as specified in RFC 1122, Section 3.2.1.2
k. source address, also as specified in RFC 1122, Section 3.2.1.3
l. destination address, also as specified in RFC 1122, Section 3.2.1.3
m. IP options, also as specified in RFC 1122, Section 3.2.1.8.
n. padding
o. data

2.3.1.3 Detailed Requirements

2.3.1.3.1 Interface Requirements

2.3.1.3.1.1 IP to Transport Layer Interface

The procedure calls described in RFC 791, Section 3.3 and RFC 1122, Section 3.1, 3.3.4, and 3.4 shall constitute the Internet/Transport Interface.

2.3.1.3.2 Data Transfer

2.3.1.3.2.1 Address Handling

A conforming implementation shall structure its addresses as a class A, B, C, or D addresses and follow the procedures described in RFC 1122, Section 3.2.1.3 or, optionally, use the Classless Inter-Domain Routing address structure and the procedures described in RFC 1517 through RFC 1520. For use within a transportation system, an IP Address may be allocated from the Private Address Space as described in RFC 1918, Section 3.

2.3.1.3.2.1.1 Routing Outbound Datagrams

A conforming implementation providing gateway functionality shall support the functions described in RFC 1122, Section 3.3.1.

2.3.1.3.2.1.2 Local Multihoming

A conforming implementation shall provide for the requirements as described in RFC 1122, Section 3.3.4.

2.3.1.3.2.1.3 Source Route Forwarding

A conforming implementation shall provide for the requirements as described in RFC 1122, Section 3.3.5.

2.3.1.3.2.1.4 Broadcasts

A conforming implementation shall provide for the requirements as described in RFC 1122, Section 3.3.6.

2.3.1.3.2.1.5 Multicasting

A conforming implementation shall provide for the requirement as described in RFC 1122, Sections 3.2.3 and 3.3.7.

2.3.1.3.2.2 Fragmentation and Reassembly

A conforming implementation shall provide for the requirement as described in RFC 791, Sections 3.1, 3.2, and RFC 1122, Sections 3.2.1.4, 3.2.1.5, 3.3.2 and 3.3.3.

For use within the transportation environment, IP shall support a datagram size of at least 576 bytes per RFC 1122, Section 3.3.3.

2.3.1.3.2.3 Type Of Service (TOS)

A conforming implementation shall provide the TOS field as specified in RFC 791, Sections 1.4, 3.1, 3.2, and RFC 1122, Section 3.2.1.6.

2.3.1.3.2.4 Time-To-Live (TTL)

A conforming implementation shall provide the TTL field as specified in RFC 791, Sections 3.1, 3.2, and RFC 1122, Section 3.2.1.7. This field shall be used as a "hop counter" as described in RFC 1122, Section 3.2.1.7.

2.3.1.3.3 Options

All the options specified in RFC 791, Sections 3.1, 3.2 and RFC 1122, Section 3.2.1.8 shall be mandatory to implement but optional to use.

2.3.1.3.4 MIB-II IP Group Object Definitions

A conforming implementation shall support the MIB-II ip group object definitions as defined in RFC 1213, Sections 3.7 and 6.6.

2.3.2 Internet Control Message Protocol (ICMP)

2.3.2.1 Major Capabilities

A conforming implementation shall support the following capabilities in accordance with the indicated base standards.

a. error reporting as described in RFC 792 and RFC 1122, Section 3.2.2
b. control messages as described in RFC 792 and RFC 1122, Section 3.2.2
c. MIB-II icmp group as specified in RFC 1212, Sections 3.8 and 6.7.

2.3.2.2 ICMP Message Format

ICMP messages are sent using the basic IP header. The first octet of the data portion of the datagram is an ICMP type field; the value of this field determines the format of the remaining data. Any field labeled "unused" is reserved for later extensions and shall be zero when sent, but receivers shall not use these fields (except to include them in the header checksum). Each ICMP message also contains a code field. ICMP uses the following IP header fields, as described in RFC 792, Message Format (pages 2-3):

a. version
b. Internet Header Length (IHL)

c. type of service (TOS)
d. total length
e. identification
f. flags
g. fragment offset
h. Time To Live (TTL)
i. protocol
j. checksum
k. source address
l. destination address

2.3.2.2.1 ICMP Messages

The following messages shall be implemented but are optional for use as described in RFC 792, pages 4-20 and RFC 1122, Section 3.2.2:

a. destination unreachable
b. time exceeding
c. parameter problem
d. source quench
e. redirect
f. echo
g. echo reply
h. timestamp
i. timestamp reply
j. address mask request
k. address mask reply
l. information request messages
m. information reply messages

2.3.2.3 Detailed Requirements

2.3.2.3.1 Error Reporting

A conforming implementation shall use the error messages described in RFC 792 and RFC 1122, Sections 3.2.2.1 through 3.2.2.5.

2.3.2.3.1.1 ICMP Error Message Prohibition

A conforming host shall not send ICMP error messages as a result of receiving the messages described in RFC 1122, Section 3.2.2.

2.3.2.3.2 Query Messaging

A conforming implementation shall use the Query Messages in accordance with the procedures described in RFC 792 and RFC 1122, Section 3.2.2.6 through 3.2.2.9.

2.3.2.3.3 MIB-II ICMP Group Object Definitions

A conforming implementation shall support the MIB-II icmp group object definitions as defined in RFC 1213, Sections 3.8 and 6.7.

2.3.3 Internet Group Management Protocol (IGMP)

2.3.3.1 Major Capabilities

Internet Group Management Protocol (IGMP), described in RFC 1112 and RFC 1122, is used by IP hosts to report their host membership to any immediately neighboring multicast routers. It lets all the systems on a network know which hosts currently belong to which multicast groups. IGMP is an asymmetric protocol and is specified from the point of view of a host. IGMP is an integral part of IP, and although optional in the general sense, is to be implemented by all hosts conforming to level 2 of the IP multicasting specification.

2.3.3.2 IGMP Message Format

IGMP messages are transmitted in IP datagrams. The IGMP message is encapsulated within the IP datagram and is a fixed size of 8 bytes. The format for IGMP messages is contained in RFC 1112.

2.3.3.3 Version

The Version field shall indicate which version of IGMP is being used. The current value is one (1).

2.3.3.4 Type

There are two types of IGMP messages of concern to hosts:

1 = Host Membership Query (Query sent by Multicast Router)
2 = Host Membership Report (Response sent by Host)

2.3.3.5 Unused Field

This field is not used. It shall be set to zero when sent and ignored when received.

2.3.3.6 Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the 8-octet IGMP message. For computing the checksum, the checksum field is zeroed. (The checksum is calculated in the same manner as the ICMP checksum.)

2.3.3.7 Group Address

The group address is a class "D" IP address. In a query the group address is set to zero, and in a report it contains the 32-bit group address being reported.

2.3.4 Routing Information Protocols

The requirements for specific routing information protocols, such as RIP, ES-IS, OSPF, or BGP, are not within the scope of this standard.

2.4 NETWORK TO DATA LINK LAYER INTERFACE

2.4.1 MIB-II Interfaces Group Object Definitions

If a device claims to function as an NTCIP router, it shall support the MIB-II interfaces group object definitions as defined in RFC 1213, Sections 3.5 and 6.4. Otherwise, the interfaces group is optional. If implemented, all objects within the group are required to be supported.

2.4.2 MIB-II IP Address Translation Group Object Definitions

A conforming implementation shall support the MIB-II IP Network to Media address translation group object definitions as defined in RFC 1213, Sections 3.7 and 6.6.

MIB-II also contains an earlier "generic" address translation group but this group is given the status of deprecated. In the RFC, deprecated is used to describe an object which must be supported, but one which will most likely be removed from the next version of the MIB. Even though the definition implies that the status of the generic group should be mandatory, its support is not required. The new "IP Network to Media" address translation table contains the same parameters as the original but adds a type parameter to indicate how a address entry was learned, e.g., static or dynamic through the use of ARP.

Annex A
TCP/ IP AND UDP/IP - TRANSPORT PROFILE REQUIREMENTS LIST
(Normative)

A.1 INTRODUCTION

This annex provides the Profile Requirements List (PRL) for implementations of the Internet (TCP/IP and UDP/IP) – Transport Profile. A Profile Implementation Conformance Specification (PICS) for an implementation is generated by an implementer or supplier by indicating the appropriate level of support provided by an implementation.

To claim conformance with this profile, an implementation shall satisfy the mandatory conformance requirements of this profile.

An implementation's completed PRL is called the PICS. The PICS states which capabilities and options of the protocol have been implemented. The following can use the PICS:

a. The protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight.

b. The supplier and user, as a detailed indication of the capabilities of the implementation.

c. The user, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to do so can often be predicted from incompatible PICSs).

d. A user, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.1.1 Notation

The following notations and symbols are used to indicate status and conditional status in the PRL and PICS within all NTCIP standards. Not all of these notations and symbols may be used within this standard.

A.1.1.1 Status Symbols

The following symbols are used to indicate base standard and profile status:

m	mandatory
m.<n>	support of every item of the group labeled by the same numeral <n> required, but only one is active at time
o	optional
o.<n>	optional, but support of at least one of the group of options labeled by the same numeral <n> is required
c	conditional
n/a	not-applicable (i.e., logically impossible in the scope of the profile)
x	excluded or prohibited

The o.<n> notation is used to show a set of selectable options (i.e., one or more of the set must be implemented) with the same identifier <n>. Two character combinations are used for dynamic conformance requirements. In this case, the first character refers to the static (implementation) status, and the second refers to the dynamic (use); thus "mo" means "mandatory to be implemented, optional to be used." Base standard requirements are shown using the equivalent notations in upper case (e.g., M, O, X).

The classification of the requirements and options in Internet RFCs does not correspond to the convention described in above, and shall be mapped into the profile as follows:

RFC	Profile
MUST	Mandatory[1]
SHOULD	Mandatory[1]
MAY	Optional
SHOULD NOT	Prohibited
MUST NOT	Prohibited

A.1.1.2 Conditional Status Notation

The following predicate notations may be used:

<predicate>:	This notation introduces a single item that is conditional on the <predicate>.
<predicate>::	This notation introduces a table or a group of tables, all of which are conditional on the <predicate>.

The <predicate>: notation means that the status following it applies only when the PRL or PICS states that the feature or features identified by the predicate are supported. In the simplest case, <predicate> is the identifying tag of a single PICS item. The <predicate>:: notation may precede a table or group of tables in a clause or subclause. When the group predicate is true then the associated clause shall be completed. The symbol <predicate> also may be a Boolean expression composed of several indices. "AND", "OR", and "NOT" shall be used to indicate the Boolean logical operations.

A.1.1.3 Support Column Symbols

This profile is in the form of a PICS and, therefore, includes a support column. An implementer claims support of an item by circling the appropriate answer (Yes, No, or N/A) in the support column:

Yes	Supported by the implementation.
No	Not supported by the implementation.
N/A	Not applicable

A.1.1.4 Footnotes

Footnotes to the proforma are indicated by superscript numerals. The footnote appears on the page of the first occurrence of the numeral. Subsequent occurrences of a numeral refer to the footnote of the first occurrence.

[1] In the course of adapting communications industry standards to the transportation industry, there may be exceptions where specific mandatory requirements are not applicable to the new environment. Where these exceptions are made, a justification shall be provided.

A.1.1.5 Instructions for Completing the PRL

A Profile implementer shows the extent of compliance to a Profile by completing the PRL. The implementer indicates whether mandatory requirements are complied with, and whether optional functions are supported. The resulting completed PRL is called a PICS. Where this profile refines the features of the base standards, the requirements expressed in this PRL shall be applied (as indicated in PRL items with no "Profile Support" column) to constrain the allowable responses in the base standard PICS proforma. When this profile makes additional requirements, the "Support" column for such PRLs shall be completed. In this column, each response shall be selected either from the indicated set of responses, or it shall comprise one or more parameter values as requested. If a conditional requirement is inapplicable, use the Not Applicable (NA) choice. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference Xi, where i is a unique identifier, to an accompanying rationale for the noncompliance. When the profile requirement is expressed as a two-character combination (as defined in A.1.1 above), the response shall address each element of the requirement; e.g., for the requirement "mo," the possible compliant responses are "yy" or "yn."

A.2 STANDARDS REFERENCED

This profile specifies the provisions for connection-oriented transport services over a connectionless network service (TCP/IP) and for connectionless transport services over a connectionless network service (UDP/IP). Either or both types of services would apply to end systems. The services of connectionless network service apply to intermediate systems. It references the following standards:

IAB STD 3	(RFC 1122: 1989, Requirements For Internet Hosts - Communication Layers, RFC 1123: 1989, Requirements For Internet Hosts - Application and Support)
IAB STD 5	(RFC 791: 1981, Internet Protocol, RFC 950: 1985, Internet standard subnetting procedure, RFC 919: 1984, Broadcasting Internet datagrams, RFC 922: 1984, Broadcasting Internet datagrams in the presence of subnets, RFC 792: 1981, Internet Control Message Protocol, RFC 1112: 1989, Host extensions for IP multicasting)
IAB STD 6	(RFC 768: 1980, User Datagram Protocol)
IAB STD 7	(RFC 793: 1981, Transmission Control Protocol)
IAB STD 17	(RFC 1213:1991, Management Information Base)

A.3 PICS REQUIREMENTS LISTS

A.3.1 Implementation Identification

Ref	Question	Response
1	Supplier	
2	Contact point for queries about the profile	
3	Implementation Name(s) and Version(s)	
4	Date of statement	
5	Other Information: Machine Name, Operating Systems, System Name	
6	Amendments or revisions to the base standards or profiles that are applicable.	

A.3.2 TCP/IP Global Statement of Conformance

For the TCP/IP Configuration, are all mandatory requirements met for:

TCP/IP Configuration		
Ref	Standard	Response
1	IAB STD 3 (Internet Hosts)	
2	IAB STD 7 (TCP)	
3	IAB STD 6 (UDP)	
4	IAB STD 5 (IP,ICMP, IGMP) NOTE: IGMP is not required by this profile. However if IGMP is implemented, there are mandatory provisions called out in this profile.	
5	IAB STD 17 (MIB-II) TCP, UDP, IP, and ICMP group objects definitions implemented?	

A.3.3 UDP/IP Global Statement of Conformance

For the UCP/IP Configuration, are all mandatory requirements met for:

UDP/IP Configuration		
Ref	Standard	Response
1	IAB STD 3 (Internet Hosts)	
2	IAB STD 6 (UDP)	
3	IAB STD 5 (IP,ICMP, IGMP) NOTE: IGMP is not required by this profile. However if IGMP is implemented, there are mandatory provisions called out in this profile.	
4	IAB STD 17 (MIB-II) TCP, UDP, IP, and ICMP group objects definitions implemented?	

A.4 BASIC REQUIREMENTS

The following table lists the major requirements for a TCP/IP or UDP/IP implementation, and asks if the listed protocols and object definition groups have been implemented:

Index	Protocol	Clause of Profile	Profile Status	Support
tcp	IAB STD 7 (RFC 793), TCP and IAB STD 3 (RFC 1122), InHost Section 4.2, implemented?	2.2.1	o	Yes No
udp	IAB STD 6 and IAB STD 3, RFC1122, Section 4.1, UDP, implemented?	2.2.2	m	Yes
ip	IAB STD 5 and IAB STD 3, RFC 1122, Section 3, IP, implemented?	2.3.1	m	Yes
icmp	IAB STD 5 and IAB STD 3, RFC 1122, Section 3, ICMP, implemented?	2.3.2	m	Yes
inhost	IAB STD 3 (InHost) Requirements, implemented?	2.2.1, 2.2.2, 2.3.1, and 2.3.2	m	Yes
tcp-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.9 and 6.8, tcp group objects implemented?	2.2.1.3.2.14	tcp:m	Yes No
udp-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.10 and 6.9, udp group objects implemented?	2.2.2.2.2.3	m	Yes
ip-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.7 and 6.6, ip group objects implemented?	2.3.1.3.4	m	Yes
icmp-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.8 and 6.7, icmp group objects implemented?	2.3.2.3.3	m	Yes
if-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.5 and 6.4, interfaces group objects implemented?	2.4.1	m	Yes
at-group	IAB STD 17 (RFC 1213), MIB-II, Sections 3.7 and 6.6, IP address translation group objects implemented?	2.4.2	m	Yes

A.5 TCP PICS PROFORMA

A.5.1 TCP Protocol Summary

Protocol Version	
Addenda Implemented?	
Amendments Implemented?	
Have any exceptions been required? (Note: A YES answer means that the implementation does not conform to the Transmission Control Protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes_____ No_____
Date of Statement	

A.5.2 TCP General/Major Capabilities

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
dt	Data Transfer	RFC 793:1.5, 2.8,3.7	M	2.2.1.1	m	Yes
pa	Addressing	RFC 793: 2.7 RFC 1122: 4.2.2.1	M		m	Yes
frg	Fragmentation	RFC 793: 1.5, 2.7, 3.3	M		m	Yes
ras	Reassembly	RFC 1122: 3.3.2, 3.3.3, 4.2.2.6	M		m	Yes
pa	Piggyback Acknowledgment	RFC 793: 1.5,2.6, 3.7,3.9 RFC 1122: 4.2.3.2	M		m	Yes
flc	Flow Control	RFC 793: 1.5,2.6,3.7 RFC 1122: 4.2.3.3	M		m	Yes
chks	Checksum	RFC 793: 1.5,3.1 RFC 1122: 4.2.2.7	M		m	Yes
errec	Error Recovery	RFC 793: 1.5,3.7 RFC1122: 4.2.3.1, 4.2.2.15	M		m	Yes
secpr	Precedence and Security	RFC 793: 1.5, 2.9	M		m	Yes
tcp-group	MIB-II TCP Group Object Definitions Support	RFC 1213, Sections 3.9 and 6.8	M	2.2.1.3.2.14	m	Yes

A.5.3 TCP Interfaces

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
icmp	Internet Control Message Protocol	RFC 1122: 4.2.3.9.	M	2.2.1.3.1	m	Yes
alp	TCP to Application Layer Interface	RFC 1122: 4.2.4.	M	2.2.1.3.1.2	m	Yes N/A
ip	Internet Protocol Options	RFC 1122: 4.2.3.8	M	2.2.1.3.1	m	Yes
av	Remote Address Validation	RFC 1122: 4.2.3.10	M		m	Yes

A.5.4 TCP Frame Structure

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
hdr	Header Format	RFC 793: 3.1	M	2.2.1.2	m	Yes
sp	Source Port		M		m	Yes
dp	Destination Port		M		m	Yes
sn	Sequence Number		M		m	Yes
an	Acknowledgment Number		M		m	Yes
dof	Data Offset		M		m	Yes
res	Reserved field (must be zero)		M		m	Yes
Control Bits: (following six fields)						
urg	Urgent Pointer field – significant	RFC 793: 3.1 RFC1122:4.2.2.4	M	2.2.1.2	m	Yes
ack	Acknowledgment field – significant	RFC 793: 3.1	M		m	Yes
psh	Push function	RFC 793: 3.1 RFC1122:4.2.2.2	M		m	Yes
rst	Reset the connection	RFC 793: 3.1	M		m	Yes
syn	Synchronize sequence numbers		M		m	Yes
fin	No more data from sender		M		m	Yes
win	Window	RFC 793: 3.1 RFC1122:4.2.2.3 4.2.2.16, 4.2.2.17	M		m	Yes
cks	Checksum	RFC 793: 3.1 RFC 1122:4.2.2.7	M		m	Yes
opt	Options	RFC 793: 3.1 RFC1122;4.2.2.5, 4.2.2.6	M		m	Yes
eol	End of Option List	RFC 793: 3.1	M		mo	Yes Yes No
nop	No-Operation		M		mo	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
						Yes No
mss	Maximum Segment size		M		mo	Yes Yes No
pad	Padding		M		mo	Yes Yes No

A.5.5 TCP Procedures

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
mux	Multiplexing	RFC 793: 1.5, 2.7, 3.8 RFC 1122: 4.2.2.1, 4.2.2.18	M	2.2.1.1	m	Yes
isnsel	Use clock-driven ISN selection	RFC 793: 3.3 RFC 1122: 4.2.2.9	M	2.2.1.3.2.6	m	Yes
	Opening Connections					
op1	Support simultaneous open attempts	RFC 793: 3.4 RFC 1122: 4.2.2.10	M	2.2.1.3.2.7	m	Yes
op2	SYN-RCVD remembers last state	RFC 793: 3.4 RFC 1122: 4.2.2.11	M		m	Yes
op3	Passive open call interfere with others	RFC 793: 3.8 RFC 1122: 4.2.2.18	x		x	No
op4	Function: simultaneous LISTENs for same port	RFC 793: 3.8 RFC 1122: 4.2.2.18	M		m	Yes
op5	Ask IP for source address for SYN if necessary.	RFC 1122: 4.2.3.7	M		m	Yes
op5a	Otherwise, use local address of connection	RFC 1122: 4.2.3.7	M		m	Yes
op6	OPEN to broadcast/multicast IP Address	RFC 1122:	X		x	No
op7	Silently discard segment to broadcast/multicast address	4.2.3.10	M		m	Yes
	Closing Connections:					
cl1	RST can contain data	RFC 1122: 4.2.2.12	O	2.2.1.3.2.8	m	Yes
cl2	Inform application if connection is aborted	RFC 793: 3.4	M		m	Yes
cl3	Half-duplex close connections	RFC 1122:	O		o	Yes No
cl31	Send RST to indicate data lost	4.2.2.13	O		m	Yes
cl4	In TIME-WAIT state for 2xMSL seconds		M		m	Yes
cl41	Accept SYN from TIME-WAIT state		O		o	Yes No
	Retransmissions:					
rtc	Retransmission Timeout Calculation	RFC 793, 1.5,3.7, RFC 1122, 4.2.3.1 , 4.2.2.15	M	2.2.1.3.2.9	m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
rt1	Jacobsen slow start algorithm	RFC 1122: 4.2.2.15	M	2.2.1.3.2.9	m	Yes
rt2	Jacobson congestion avoidance algorithm		M		m	Yes
rt3	Retransmit with same IP ident		O		o	Yes No
rt4	Karn's algorithm	RFC 1122: 4.2.3.1	M		m	Yes
rt5	Jacobson's RTO estimation algorithm		M		m	Yes
rt6	Exponential Backoff		M		m	Yes
rt7	SYN RTO calculation same as data		O		m	Yes
rt8	Recommended initial values and bounds		O		m	Yes
	Generating ACK's:					
ga1	Queue out of order segment	RFC 1122: 4.2.2.20	O	2.2.1.3.2.10	m	Yes
ga2	Process all queued before send ACK		M		m	Yes
ga3	Send ACK for out of order segment	RFC 1122: 4.2.2.21	O		o	Yes No
ga4	Delayed ACK's	RFC 1122: 4.2.3.2	O		m	Yes
ga41	Delay < 0.5 seconds		ga4:M		m	Yes
ga42	Every 2nd full sized segment ACK'd		ga4:M		m	Yes
ga5	Receiver SWS-Avoidance Algorithm	RFC 1122: 4.2.3.3	M		m	Yes
	Sending Data:					
sd1	Configurable TTL	RFC 1122: 4.2.2.19	M	2.2.1.3.2.11	m	Yes
sd2	Sender SWS-avoidance algorithm	RFC 1122: 4.2.3.4	M		m	Yes
sd3	Nagle algorithm		O		m	Yes
sd31	Application can disable Nagle algorithm		sd3:M		m	Yes
	Connection Failures:					
cf1	Negative advice to IP on R1 retransmissions	RFC 1122: 4.2.3.5	M	2.2.1.3.2.12	m	Yes
cf2	Close connection on R2 retransmissions	RFC 1122: 4.2.3.5	M		m	Yes
cf3	Application Layer protocol can set R2	RFC 1122: 4.2.3.5	M		m	Yes
cf4	Inform Application Layer protocol of R1<=retransmissions<R2	RFC 1122: 4.2.3.5	O		m	Yes
cf5	Recommend values for R1, R2	RFC 1122: 4.2.3.5	O		m	Yes
cf6	Same mechanism for SYNs	RFC 1122: 4.2.3.5	M		m	Yes
cf6a	R2 at least 3 minute for SYN	RFC 1122: 4.2.3.5	M		m	Yes
cf6b	Send Keep alive packets:	RFC 1122: 4.2.3.6	O	2.2.1.3.2.13	o	Yes No
ka1	Application can request	RFC 1122: 4.2.3.6	M		m	Yes
ka2	Default is "off"	RFC 1122: 4.2.3.6	M	2.2.1.3.2.13	m	Yes
ka3	Only send if idle for interval		M		m	Yes
ka4	Interval configurable		M		m	Yes
ka5	Default at least 2 Hrs		M		m	Yes
ka6	Implementation must be tolerant of lost ACKs		M		m	Yes

A.5.6 TCP MIB-II Group Support

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
tcpg.1	tcpRtoAlgorithm	INTEGER	read-only	RFC 1213, Section 6.8	tcp:M	2.2.1.3.2.14	tcp:m	Yes No
tcpg.1.1	other	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.1.2	constant	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.1.3	rsre	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.1.4	vanj	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.2	tcpRtoMin	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.3	tcpRtoMax	INTEGER	read-only	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No
tcpg.4	tcpMaxConn	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.5	tcpActiveOpens	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.6	tcpPassiveOpens	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.7	tcpAttemptFails	Counter	read-only	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No
tcpg.8	tcpEstabResets	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.9	tcpCurrEstab	Gauge	read-only		tcp:M		tcp:m	Yes No
tcpg.10	tcpInSegs	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.11	tcpOutSegs	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.12	tcpRetransSegs	Counter	read-only	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
tcpg.13	tcpConnTable	SEQUENCE OF TcpConn Entry	not-accessible		tcp:M		tcp:m	Yes No
tcpg.13.1	tcpConnEntry	TcpConn Entry	not-accessible		tcp:M		tcp:m	Yes No
tcpg.13.1.1	tcpConnState	INTEGER	read-write	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No
tcpg.13.2	tcpConnLocal Address	IpAddress	read-only	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No
tcpg.13.3	tcpConnLocalPort	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.13.4	tcpConnRem Address	IpAddress	read-only		tcp:M		tcp:m	Yes No
tcpg.13.5	tcpConnRemPort	INTEGER	read-only		tcp:M		tcp:m	Yes No
tcpg.14	tcpInErrs	Counter	read-only		tcp:M		tcp:m	Yes No
tcpg.15	tcpOutRsts	Counter	read-only	RFC 1213, Section 6.8	tcp:M		tcp:m	Yes No

A.6 UDP PICS PROFORMA

A.6.1 UDP Protocol Summary

Protocol Version	
Addenda Implemented	
Amendments Implemented	
Have any exceptions been required? (Note: A YES answer means that the implementation does not conform to the Transmission Control Protocol/User Datagram Protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes _____ No _____
Date of Statement	

A.6.2 UDP General/Major Capabilities

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
dt	Data Transfer	RFC 768, RFC 1122: 4.1.1	M	2.2.2.1	m	Yes
pa	Port Addressing	RFC 768, RFC 1122: 4.1.1, 4.1.3.1, 4.1.3.5, 4.1.3.6	M		m	Yes
uchks	Checksum	RFC 768 RFC 1122: 4.1.1, 4.1.3.4	M		m	Yes
udp-groupI	UDP MIB-II Object Definitions Support	RFC 1213, Sections 3.10 and 6.9	M	2.2.2.2.2.3	m	Yes

A.6.3 UDP Interfaces

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
uuc	User/UDP Interface	RFC 768	M	2.2.2.1	m	Yes
urp	Creation of new receive ports	RFC 768	M		m	Yes
usend	Send operations that specify data, source and destination ports	RFC 768	M		m	Yes
urecc	Receive operations that return the data octets and source port and source address	RFC 768	M		m	Yes
ulli1	Determine Source Internet Address	RFC 768	M		m	Yes
ulli2	Determine Destination Internet Address	RFC 768	M		m	Yes

A.6.4 UDP Frame Structure

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
uhf	Header Format	RFC 768	M	2.2.2.1.1	m	Yes
usp	Source Port	RFC 768	M		m	Yes
udp	Destination Port	RFC 768	M		m	Yes
ucb	Length	RFC 768	M		m	Yes
ucks	Checksum	RFC 768	M		m	Yes

A.6.5 UDP Procedures

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
us	UDP Send port unreachable	RFC 1122: 4.1.3.1	O	2.2.2.1	m	Yes
IP options in UDP:						
iu1	Pass received IP options to application layer	RFC 1122: 4.1.3.2	M	2.2.2.2.1.3	m	Yes
iu2	Application layer can specify IP options to Send	RFC 1122: 4.1.3.2	M		m	Yes
iu3	UDP passes IP options down to IP layer	RFC 1122: 4.1.3.2	M		m	Yes
icm	Pass ICMP msgs up to application layer	RFC 1122: 4.1.3.3	M		m	Yes
UDP checksums:						
uc1	Able to generate/check checksum	RFC 1122: 4.1.3.4	M	2.2.2.2.2.1	m	Yes
uc2	Silently discard bad checksum	RFC 1122: 4.1.3.4	M		m	Yes
uc3	Sender Option to not generate checksum	RFC 1122: 4.1.3.4	O		o	Yes No
uc31	Default is to checksum	RFC 1122: 4.1.3.4	M		m	Yes
uc4	Receiver Option to require checksum	RFC 1122: 4.1.3.4	O		o	Yes No
UDP Multihoming:						
um1	Pass specific-dest address to application	RFC 1122: 4.1.3.5	M	2.2.2.2.2.2	m	Yes
um2	Application Layer can specify local IP addr	RFC 1122: 4.1.3.5	M		m	Yes
um3	Application layer specify wild local IP addr	RFC 1122: 4.1.3.5	M		m	Yes
um4	Application layer notified of local IP address used	RFC 1122: 4.1.3.5	O		m	Yes
bip	Bad IP source address silently discarded by	RFC 1122: 4.1.3.6	M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
	UDP/IP					
vip	Only send valid IP source address	RFC 1122: 4.1.3.6	M		m	Yes
UDP Application Interface Services:						
ua1	Full IP interface described in Section 3.4 of RFC 1122 for application	RFC 1122: 4.1.4	M	2.2.2.2.1.2	m	Yes
ua11	Able to specify TTL, TOS, IP options when sending	RFC 1122: 4.1.4	M		m	Yes
ua12	Pass received TOS up to application layer	RFC 1122: 4.1.4	O	2.2.2.2.1.2	o	Yes No

A.6.6 UDP MIB-II Group Support

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
A.6.6.1	udpInDatagrams	Counter	read-only	RFC 1213, Section 6, p.52	M	2.2.2.2.2.3	m	Yes
A.6.6.2	udpNoPorts	Counter	read-only		M		m	Yes
A.6.6.3	udpInErrors	Counter	read-only		M		m	Yes
A.6.6.4	udpOut Datagrams	Counter	read-only	RFC 1213, Section 6.9	M		m	Yes
A.6.6.5	udpTable	SEQUENCE OF UdpEntry	not-accessible		M		m	Yes
A.6.6.5.1	udpEntry	UdpEntry	not-accessible		M		m	Yes
A.6.6.5.1.1	udpLocalAddress	IpAddress	read-only		M		m	Yes
A.6.6.5.1.2	udpLocalPort	INTEGER	read-only	RFC 1213, Section 6.9	M		m	Yes

A.7 IP PICS PROFORMA

A.7.1 IP Protocol Summary

Protocol Version	
Addenda Implemented	
Amendments Implemented	
Have any exceptions been required? (Note: A YES answer means that the implementation does not conform to the Internet Protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes_____ No_____
Date of Statement	

A.7.2 IP General/Major Capabilities

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
dt	Data Transfer	RFC 791: 1.1, 2.3	M	2.3.1.1	m	Yes
add	Addressing	RFC 791: 1.4, 2.3, 3.1, 3.2, RFC 1122: 3.2.1.3	M	2.3.1.3.2.1	m	Yes
add-a	Class A addresses supported		M		m	Yes
add-b	Class B addresses supported		M		m	Yes
add-c	Class C addresses supported		M		m	Yes
add-d	Class D addresses supported		M		m	Yes
add-cidr1	Classless Inter-Domain addresses supported	RFC 1517 - RFC 1520	O		o	Yes No
frg	Fragmentation and Reassembly	RFC 791: 1.4, 3.1,2.3, 3.2, RFC 1122: 3.2.1.4	M	2.3.1.1	m	Yes
frg1	Forward datagrams of 68 octets without fragmentation	RFC 791: 3.2 RFC 1122: 3.2.1.4	M		m	Yes
frg2	Receive datagrams of 576 octets either in one piece or in fragments		M		m	Yes
frg3	Don't Fragment Supported		M		m	Yes
frg4	Forward datagrams of 576 octets without fragmentation	RFC 1122: 3.3.3	O	2.3.1.3.2.2	m	Yes
reass1	IP Datagram reassembly supported	RFC 1122: 3.3.2	M		m	Yes
reass2	Reassembly timeout period supported		M		m	Yes
tos	Type Of Service	RFC 791: 1.4, 3.1, 3.2 RFC 1122: 3.2.1.6	M	2.3.1.1	m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
tpre	Precedence	RFC 791: 3.1,3.2 RFC 1122: 3.2.1.6	M		m	Yes
tdel	Delay	RFC 791: 3.1,3.2	M		m	Yes
tthr	Throughput		M		m	Yes
trel	Reliability		M		m	Yes
ttl	Time To Live	RFC 791: 3.1,3.2 RFC 1122: 3.2.1.7	M		m	Yes
opt	Options	RFC 791: 3.1,3.2 RFC 3.2.1.8	M		m	Yes
chk	Checksum	RFC 791: 1.4, 3.1, 3.2 RFC 1122: 3.2.1.2	M		m	Yes
mib-II	MIB-II IP Group Object Definitions Support	RFC1213, Sections 3.7 and 6	M	2.3.1.3.4	m	yes

A.7.3 IP Interfaces

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
lni	Local Network Interface	RFC 791: 3.3, RFC 1122: 3.4	M	2.3.1.3.1.1	m	Yes
uli	Upper Level Interface	RFC 791: 3.3, RFC 1122: 3.4	M		m	Yes

A.7.4 IP Frame Structure

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
Internet/Transport Layer Interface						
iii	Implement IP and ICMP	RFC 1122: 3.1	M	2.3.1.3.1.1	m	Yes
rm	Handle remote multihoming in application layer		M		m	Yes
lm	Support local multihoming		O		o	Yes No
lm1	Devices with multiple physical interfaces shall implement local multi-homing	RFC 1122: 3.3.4	O		m	Yes
gs	Meet gateway specs if forward datagrams	RFC 1122: 3.1	M		m	Yes
cs	Configuration switch for embedded gateway		M		m	Yes
cs1	Config. switch default to non-gateway		M		m	Yes
cs2	Automatic move by host into gateway mode		X		x	No
ldd	Able to log discarded datagrams		O		m	Yes
ldd1	Record in counter		O		m	Yes
sdv	Silently discard version not equal to 4	RFC 1122: 3.2.1.1	M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
vchk	Verify IP checksum, silently discard bad datagram	RFC 1122: 3.2.1.2	M		m	Yes
in1	Allow transport layer to use all IP mechanisms	RFC 1122: 3.4	M		m	Yes
in2	Pass interface ident up to transport layer	RFC 1122: 3.4	O		m	Yes
in3	Pass all IP options up to transport layer	RFC 1122: 3.4	M		m	Yes
in4	Transport layer can send certain ICMP messages	RFC 1122: 3.4	M		m	Yes
in5	Pass specified ICMP messages up to transport layer	RFC 1122: 3.4	M		m	Yes
in51	Include IP header + 8 octets or more from originator	RFC 1122: 3.4	M		m	Yes
Addressing:						
add1	Subnet and Class A, B, and C special addressing restrictions (RFC 950)	RFC 1122: 3.2.1.3	M	2.3.1.3.2.1	m	Yes
add2	Source address must be host's own IP address	RFC 1122: 3.2.1.3	M		m	Yes
add3	Silently discard datagram with bad destination address	RFC 1122: 3.2.1.3	M		m	Yes
add4	Silently discard datagram with bad source address	RFC 1122: 3.2.1.3	M		m	Yes
add-cidr2	Classless Inter-Domain Routing addresses	RFC 1517 - RFC 1520	O		o	Yes No
Datagram Fragmentation and Reassembly:						
rea	Support datagram fragmentation and reassembly	RFC 1122: 3.2.1.4	M	2.3.1.3.2.2	m	Yes
idf	Retain same ID field in identical datagram	RFC 1122: 3.2.1.5	O		o	Yes No
TOS:						
tos1	Allow transport layer to set TOS	RFC 1122: 3.2.1.6	M	2.3.1.3.2.3	m	Yes
tos2	Pass received TOS up to transport layer	RFC 1122: 3.2.1.6	O		m	Yes
tos3	Use RFC 975 link layer mappings for TOS	RFC 1122: 3.2.1.6	O		x	No
TTL:						
ttl1	Send packet with TTL of 0	RFC 1122: 3.2.1.7	X	2.3.1.3.2.4	x	No
ttl2	Discard received packets with TTL < 2	RFC 1122: 3.2.1.7	X		x	No
ttl3	Allow transport layer to set TTL	RFC 1122: 3.2.1.7	M		m	Yes
ttl4	Fixed TTL is configurable	RFC 1122: 3.2.1.7	M		m	Yes
IP Options:						
op1b	Allow transport layer to send IP options	RFC 1122: 3.2.1.8	M	2.3.1.3.3	m	Yes
op2b	Pass all IP options received to higher layer	RFC 1122: 3.2.1.8	M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
op3b	IP layer silently ignore unknown options	RFC 1122: 3.2.1.8	M		m	Yes
Source Route Option:						
sr1	Originate and terminate Source Route Options	RFC 1122: 3.2.1.8(c)	M	2.3.1.3.3	m	Yes
sr2	Datagram with completed SR passed up to transport layer	RFC 1122: 3.2.1.8(c)	M		m	Yes
sr3	Build correct (non-redundant) return route	RFC 1122: 3.2.1.8(c)	M		m	Yes
sr4	Send multiple SR options in one header	RFC 1122: 3.2.1.8(c)	X		x	No
Routing Outbound Datagrams:						
ro1	Use address mask in local/remote decision	RFC 1122: 3.3.1.1	M	2.3.1.3.2.1.1	m	Yes
ro2	Operate with no gateways on connection network	RFC 1122: 3.3.1.1	M		m	Yes
ro3	Maintain "route cache" of next-hop gateways	RFC 1122: 3.3.1.2	M	2.3.1.3.2.1.1	m	Yes
ro4	Treat Host and Net Redirect the same		O		m	Yes
ro5	If no cache entry, use default gateway		M		m	Yes
ro51	Support multiple default gateways		M		m	Yes
ro6	Provide table of static routes		O		o	Yes No
ro61	Flag: route overridable by Redirects		O		o	Yes No
ro7	Key route cache on host, not net address	RFC 1122: 3.3.1.3	O		o	Yes No
ro8	Include TOS in route cache	RFC 1122: 3.3.1.3	O		m	Yes
ro9	Able to detect failure in next-hop gateway	RFC 1122: 3.3.1.4	M		m	Yes
ro10	Assume route is good forever	RFC 1122: 3.3.1.4	O		x	No
ro11	Ping gateways continuously	RFC 1122: 3.3.1.4	X		x	No
ro12	Ping only when traffic is being sent	RFC 1122: 3.3.1.4	M		m	Yes
ro13	Ping only when no positive indication	RFC 1122: 3.3.1.4	M		m	Yes
ro14	Higher and lower layers give advice	RFC 1122: 3.3.1.4	O		m	Yes
ro15	Switch from failed default gateway to another	RFC 1122: 3.3.1.5	M		m	Yes
ro15a	If the current gateway fails, the host shall use round-robin selection of a new default gateway from its list of alternative gateways	RFC 1122: 3.3.1.5	M		m	Yes
ro16	Manual method of entering config info	RFC 1122: 3.3.1.6	M		m	Yes
Reassembly and fragmentation:						
rf1	Able to reassemble incoming datagrams	RFC 1122: 3.3.2	M	2.3.1.3.2.2	m	Yes
rf11	At least 576 byte datagrams		M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
rf12	EMTU_R configurable or indefinite		O		m	Yes
rf121	EMTU_R equal or greater than MTU of connected network(s)		O		m	Yes
rf2	Transport layer able to learn MMS_R		M		m	Yes
rf3	Send ICMP Time Exceeded Message on reassembly timeout	RFC 1122: 3.3.2	M		m	Yes
rf31	Fixed reassembly timeout value	RFC 1122: 3.3.2	O		m	Yes
rf4	Pass MMS_S to higher layers	RFC 1122: 3.3.3	M	2.3.1.3.2.2	m	Yes
rf5	Local fragmentation of outgoing packets	RFC 1122: 3.3.3	O		o	Yes No
rf51	Else do not send bigger than MMS_S	RFC 1122: 3.3.3	M		m	Yes
rf6	Send max 576 to off-net destination	RFC 1122: 3.3.3	O		m	Yes
rf7	All-Subnets-MTU configuration flag	RFC 1122: 3.3.3	O		o	Yes No
Multihoming:						
mh1	Reply with same address as specific destination address	RFC 1122: 3.3.4.2	O	2.3.1.3.2.1.2	m	Yes
mh2	Allow application to choose local IP address	RFC 1122: 3.3.4.2	M		m	Yes
mh3	Silently discard datagram in "wrong" interface	RFC 1122: 3.3.4.2	O		o	Yes No
mh4	Only send datagram through "right" interface	RFC 1122: 3.3.4.2	O		o[2]	Yes No
Source Route Forwarding:						
sf1	Forward datagram with Source Route option	RFC 1122: 3.3.5	O	2.3.1.3.2.1.3	o	Yes No
sf11	Obey corresponding gateway rules	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf111	Update TTL by gateway rules	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf112	Able to generate ICMP error code 4,5	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf113	IP source address not local host	RFC 1122: 3.3.5	sf1:O		sf1:o	Yes No
sf114	Update Timestamp, Record Route options	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf12	Configurable for non-local SRing	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf121	Defaults to OFF	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf13	Satisfy gateway access rules for non-local SRing	RFC 1122: 3.3.5	sf1:M		sf1:m	Yes N/A
sf14	If not forward, send Destination Unreachable (cd 5)	RFC 1122: 3.3.5	sf1:O		sf1:m[3]	Yes N/A

[2] Unless has embedded gateway functionality or is source routed.

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
Broadcast:						
br1	Broadcast address as IP source address	RFC 1122: 3.2.1.3	X	2.3.1.3.2.1.4	x	No
br2	Receive 0 or -1 broadcast formats OK	RFC 1122: 3.3.6	O		m	Yes
br3	Configurable option to send 0 or -1 broadcast	RFC 1122: 3.3.6	O		o	Yes No
br31	Default to -1 broadcast	RFC 1122: 3.3.6	O		m	Yes
br4	Recognize all broadcast address formats	RFC 1122: 3.3.6	M		m	Yes
br5	Use IP broadcast/multicast address in link layer broadcast	RFC 1122: 3.3.6	M		m	Yes
br6	Silently discard link layer only broadcast datagrams	RFC 1122: 3.3.6	O		m	Yes
br7	Use limited broadcast address for connected network	RFC 1122: 3.3.6	O		m	Yes
Multicast/multi-addressing:						
mc1	Support local IP multicast/multi-addressing (RFC 1112)	RFC 1122: 3.3.7	O	2.3.1.3.2.1.5	o	Yes No
mc2	Support IGMP (RFC 1112)	RFC 1122: 3.3.7	O		o	Yes No
mc21	Support IGMP Messages	RFC 1122: 3.3.7	mc2:O	2.3.3.2	mc2:m	Yes N/A
ver	version	RFC 1112: Appendix I	O	2.3.3.3	mc2:m	Yes N/A
typ	type	RFC 1112: Appendix I	O	2.3.3.4	mc2:m	Yes N/A
qury	Host Membership Query	RFC 1112: Appendix I	O		mc2:m	Yes N/A
rprt	Host Membership Report	RFC 1112: Appendix I	O		mc2:m	Yes N/A
unsd	unused (set to "0" on send, ignore upon receipt)	RFC 1112: Appendix I	O	2.3.3.5	mc2:m	Yes N/A
chks	checksum	RFC 1112: Appendix I	O	2.3.3.6	mc2:m	Yes N/A
grpad	group address (class "D")	RFC 1122: 3.3.7	O	2.3.3.7	mc2:m	Yes N/A
mc3	Join all hosts group at startup	RFC 1122: 3.3.7	O	2.3.1.3.2.1.5	mc2:m	Yes N/A
mc4	Higher layers learn interface multicast capability	RFC 1122: 3.3.7	O		mc2:m	Yes N/A

A.7.5 IP MIB-II Group Support

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	

[3] This requirement is overruled if datagram is an ICMP error message.

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ipg.1	ipForwarding	INTEGER	read-write	RFC1213, Section 6.6	M	2.3.1.3.4	m	Yes
ipg.2	ipDefaultTTL	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.3	ipInReceives	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.4	ipInHdrErrors	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.5	ipInAddrErrors	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.6	ipForwDatagrams	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.7	ipInUnknown Protos	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.8	ipInDiscards	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.9	ipInDelivers	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.10	ipOutRequests	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.11	ipOutDiscards	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.12	ipOutNoRoutes	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.13	ipReasmTimeout	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.14	ipReasmReqds	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.15	ipReasmOKs	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.16	ipReasmFails	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.17	ipFragOKs	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.18	ipFragFails	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.19	ipFragCreates	Counter	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.20	ipAddrTable	SEQUENCE OF IpAddrEntry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ipg.20.1	ipAddrEntry	IpAddrEntry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ipg.20.1.1	ipAdEntAddr	IpAddress	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.20.1.2	ipAdEntIfIndex	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.20.1.3	ipAdEntNetMask	IpAddress	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.20.1.4	ipAdEntBcast Addr	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ipg.20.1.5	ipAdEntReasmMaxSize	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21	ipRouteTable	SEQUENCE OF IpRoute Entry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ipg.21.1	ipRouteEntry	IpRoute Entry	not-accessible	RFC1213, Section 6.6	M	2.3.1.3.4	m	Yes
ipg.21.1.1	ipRouteDest	IpAddress	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.2	ipRouteIfIndex	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.3	ipRouteMetric1	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.4	ipRouteMetric2	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.5	ipRouteMetric3	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.6	ipRouteMetric4	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.7	ipRouteNextHop	IpAddress	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.8	ipRouteType	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.8.1	other	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.8.2	invalid	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.8.3	direct	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.8.4	indirect	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9	ipRouteProto	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.1	other	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.2	local	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.3	netmgmt	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.4	icmp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.5	egp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.6	ggp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ipg.21.1.9.7	hello	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.8	rip	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.9	is-is	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.10	es-is	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.11	ciscoIgrp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.12	bbnSpfIgp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.13	ospf	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.9.14	bgp	INTEGER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.10	ipRouteAge	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.11	ipRouteMask	IpAddress	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.12	ipRouteMetric5	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.21.1.13	ipRouteInfo	OBJECT IDENTIFIER	read-only	RFC1213, Section 6.6	M		m	Yes
ipg.22	ipNetToMediaTable	SEQUENCE OF IpNetToMediaEntry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ipg.22.1	ipNetToMediaEntry	IpNetToMediaEntry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.1	ipNetToMediaIfIndex	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.2	ipNetToMediaPhysAddress	PhysAddress	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.3	ipNetToMediaNetAddress	IpAddress	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.4	ipNetToMediaType	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.4.1	other	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.4.2	invalid	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ipg.22.1.4.3	dynamic	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ipg.22.1.4.4	static	INTEGER	read-write	RFC1213, Section 6.6	M	2.3.1.3.4	m	Yes
ipg.23	ipRouting Discards	Counter	read-only	RFC1213, Section 6.6	M		m	Yes

A.8 ICMP PICS PROFORMA

A.8.1 ICMP Protocol Summary

Protocol Version	
Addenda Implemented	
Amendments Implemented	
Have any exceptions been required? (Note: A YES answer means that the implementation does not conform to the Internet Control Message Protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes_____ No_____
Date of Statement	

A.8.2 ICMP General/Major Capabilities

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
er	Error Reporting	RFC 792, RFC 1122: 3.2.2	M	2.3.2.3.1	m	Yes
cm	Control Messages	RFC 792, RFC 1122: 3.2.2	M	2.3.2.3.2	m	Yes
icmp-group	ICMP MIB-II Object Definitions Support	RFC 1213, Section 3.8	M	2.3.2.3.3	m	Yes

A.8.3 ICMP Interfaces

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
iui	ICMP Uses IP	RFC 792	M	2.3.2.2	m	Yes

A.8.4 ICMP PDU Structure

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
mf	Message Format	RFC 792	M	2.3.2.2	m	Yes
vs	version 4		M		m	Yes
ihl	Internet Header Length		M		m	Yes
htos	Type of Service = 0		M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
totl	Total Length in octets		M		m	Yes
id	Identification field		M		m	Yes
flg	Flags		M		m	Yes
frgo	Fragmentation Offset		M		m	Yes
httl	Time to Live		M		m	Yes
prot	Protocol – ICMP = 1		M		m	Yes
hchk	Checksum		M		m	Yes
sadd	Source Address		M		m	Yes
dadd	Destination Address		M		m	Yes

A.8.5 ICMP Message Formats

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
du	Destination Unreachable	RFC 792 RFC 1122: 3.2.2.1	M	2.3.2.3.1	m	Yes
duda	Destination Address	RFC 792	M		m	Yes
dut3	Type = 3		M		m	Yes
duc	Code (0 or 1)		M		m	Yes
ducks	Checksum		M		m	Yes
duih	Internet Header		M	2.3.2.3.1	m	Yes
du64	64 bits of data datagram		M		m	Yes
tem	Time Exceeded Message Gateway: Host Send: Host receive:	RFC 792 RFC 1122:3.2.2.4	M X M		m x m	Yes No Yes
temda	Destination address	RFC 792	M		m	Yes
temtt	Type = 11	RFC 792	M		m	Yes
temcd	Code (0 or 1)	RFC 792	M		m	Yes
temchk	Checksum	RFC 792	M		m	Yes
temih	Internet Header	RFC 792	M		m	Yes
tem64	64 bits of data datagram	RFC 792	M		m	Yes
ppm	Parameter Problem Message	RFC 792 RFC 1122: 3.2.2.5	M		m	Yes
ppmda	Destination address	RFC 792	M		m	Yes
ppmtt	Type = 12	RFC 792	M		m	Yes
ppmcc	Code (0 or 1)	RFC 792	M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
ppmck	Checksum	RFC 792	M		m	Yes
ppmp	Pointer	RFC 792	M		m	Yes
ppmih	Internet Header	RFC 792	M		m	Yes
ppm64	64 bits of data datagram	RFC 792	M		m	Yes
sqm	Source Quench Message	RFC 792 RFC 1122: 3.2.2.3	M		m	Yes
sqmda	Destination address	RFC 792	M		m	Yes
sqmtt	Type = 4	RFC 792	M		m	Yes
sqmcc	Code = 0	RFC 792	M		m	Yes
sqmck	Checksum	RFC 792	M		m	Yes
sqmih	Internet Header	RFC 792	M		m	Yes
sqm64	64 bits of data datagram	RFC 792	M		m	Yes
rm	Redirect Message Gateway: Host send: Host receive:	RFC 792 RFC 1122: 3.2.2.2	 M X M		 m x m	 Yes No Yes
rmda	Destination address	RFC 792 RFC 1122: 3.2.2.2	M	2.3.2.3.1	m	Yes
rmtt	Type = 5	RFC 792	M	2.3.2.3.1	m	Yes
rmcc	Code (0 to 3)	RFC 792	M		m	Yes
rmcks	Checksum	RFC 792	M		m	Yes
rmgia	Gateway Internet Address	RFC 792	M		m	Yes
rmih	Internet Header	RFC 792	M		m	Yes
rm64	64 bits of data datagram	RFC 792	M		m	Yes
emm	Echo Message	RFC 792 RFC 1122: 3.2.2.6	M	2.3.2.3.1	m	Yes
emmda	Destination address	RFC 792 RFC 1122: 3.2.2.6	M	2.3.2.3.1	m	Yes
emmtt	Type = 8	RFC 792	M		m	Yes
emmcc	Code = 0	RFC 792	M		m	Yes
emcks	Checksum	RFC 792	M		m	Yes
emmid	Identifier	RFC 792	M		m	Yes
emmsn	Sequence number	RFC 792	M		m	Yes
erm	Echo Reply Message	RFC 792 RFC 1122: 3.2.2.6	M		m	Yes
ermsa	Source Address	RFC 792 RFC 1122: 3.2.2.6	M		m	Yes
ermtt	Type = 0	RFC 792	M		m	Yes
ermcc	Code = 0	RFC 792	M		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
ermck	Checksum	RFC 792	M		m	Yes
ermid	Identifier	RFC 792	M		m	Yes
ermsn	Sequence number	RFC 792	M		m	Yes
tsp	Timestamp Message	RFC 792 RFC 1122: 3.2.2.8	M		m	Yes
tspda	Destination address	RFC 792 RFC 1122: 3.2.2.8	M		m	Yes
tsptt	Type = 13	RFC 792	M		m	Yes
tspcc	Code = 0	RFC 792	M		m	Yes
tspck	Checksum	RFC 792	M		m	Yes
tspid	Identifier	RFC 792	M		m	Yes
tspsn	Sequence number	RFC 792	M		m	Yes
tsr	Timestamp Reply Message	RFC 792 RFC 1122: 3.2.2.8	M	2.3.2.3.2	m	Yes
tsrsa	Source Address	RFC 792 RFC 1122: 3.2.2.8	M		m	Yes
tsrtt	Type = 14	RFC 792	M		m	Yes
tsrcc	Code = 0	RFC 792	M		m	Yes
tsrck	Checksum	RFC 792	M		m	Yes
tsrid	Identifier	RFC 792	M		m	Yes
tsrsn	Sequence number	RFC 792	M		m	Yes
adrms	Address Mask Request/Reply	RFC 950: Appendix I RFC 1122: 3.2.2.9	M		m	Yes
irm	Information Request Message	RFC 792 RFC 1122: 3.2.2.7	X		x	No
irrm	Information Reply Message	RFC 792 RFC 1122: 3.2.2.7	X		x	No

A.8.6 ICMP Procedures

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
sd	Silently discard ICMP msg with unknown type	RFC 1122: 3.2.2	M	2.3.2.3	m	Yes
oc	Include more than 8 octets of orig datagram		O		o	Yes No
oc1	Included octets same as received		M		m	Yes
dm	Demux ICMP error to transport protocol		M		m	Yes
stos	Send ICMP error message with TOS=0		O		m	Yes
si Send ICMP error message for:						
si1	ICMP error message	RFC 1122:3.2.2	X	2.3.2.3.1.1	x	No
si2	IP broadcast or IP multicast/multiaddress		X		x	No
si3	Link layer broadcast	RFC 1122: 3.2.2	X		x	No
si4	Non-initial fragment		X		x	No
si5	Datagram with non-unique source address		X	2.3.2.3.1.1	x	No
ricm	Return ICMP error messages	RFC 1122: 3.3.8	M		m	Yes
Destination Unreachable:						
du1	Generate Dest. Unreachable (code 2/3)	RFC 1122: 3.2.2.1	O	2.3.2.3.1	m	Yes
du2	Pass ICMP Dest. Unreachable to higher layer	RFC 1122: 3.2.2.1	M		m	Yes
du3	Higher layer act on Dest. Unreachable	RFC 1122: 3.2.2.1	O		m	Yes
du31	Interpret Destination Unreachable as only hint	RFC 1122: 3.2.2.1	M		m	Yes
Redirect:						
rd1	Host send redirect	RFC 1122: 3.2.2.2	X	2.3.2.3.1	x	No
rd2	Update route cache when receive Redirect	RFC 1122: 3.2.2.2	M		m	Yes
rd3	Handle both host and Net redirect	RFC 1122: 3.2.2.2	M		m	Yes
rd4	Discard illegal redirect	RFC 1122: 3.2.2.2	O	2.3.2.3.1	m	Yes
Source Quench:						
sq1	Send Source Quench if buffering exceeded	RFC 1122: 3.2.2.3	O	2.3.2.3.1	o	Yes No
sq2	Pass Source Quench to higher layer	RFC 1122: 3.2.2.3	M		m	Yes
sq3	Higher layer act on Source Quench	RFC 1122:	O		m	Yes

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
		3.2.2.3				
Time Exceeded:						
tmxe	Time Exceeded: pass to higher layer	RFC 1122: 3.2.2.4	M		m	Yes
Parameter Problem:						
pp1	Host send parameter problem messages	RFC 1122: 3.2.2.5	O	2.3.2.3.1	m	Yes
pp2	Pass Parameter Problem to higher layer	RFC 1122: 3.2.2.5	M		m	Yes
pp3	Report parameter problem to user	RFC 1122: 3.2.2.5	O	2.3.2.3.1	o	Yes No
Echo request or Reply:						
ec1	Echo server and echo client	RFC 1122: 3.2.2.6	M	2.3.2.3.1	m	Yes
ec2	Echo client	RFC 1122: 3.2.2.6	O		m	Yes
ec3	Discard Echo Request to broadcast address	RFC 1122: 3.2.2.6	O		o	Yes No
ec4	Discard Echo Request to multicast address	RFC 1122: 3.2.2.6	O		o	Yes No
ec5	Use specific-dest address as Echo-Reply source	RFC 1122: 3.2.2.6	M		m	Yes
ec6	Send same data in Echo Reply	RFC 1122: 3.2.2.6	M		m	Yes
ec7	Pass Echo Reply to higher layer	RFC 1122: 3.2.2.6	M		m	Yes
ec71	If fragmentation of Echo Reply is required but not implemented, truncate datagram to max transmission size	RFC 1122: 3.2.2.6	M		m	Yes
ec8	Reflect Record Route, Time Stamp options	RFC 1122: 3.2.2.6	O		m	Yes
ec9	Reverse and reflect Source Route option	RFC 1122: 3.2.2.6	M		m	Yes
Information Request/Reply:						
irr	ICMP Information Request or Reply:	RFC 1122: 3.2.2.7	O	2.3.2.3.2	x	No
Timestamp and Timestamp Reply:						
itr	Host implement Timestamp and Timestamp Reply:	RFC 1122: 3.2.2.8	O	2.3.2.3.2	o	Yes No
itr1	Minimize delay variability	RFC 1122: 3.2.2.8	itr:O		itr:m	Yes N/A
itr2	Silently discard broadcast Timestamp	RFC 1122: 3.2.2.8	itr:O		itr:o	Yes No
itr3	Silently discard multicast Timestamp	RFC 1122: 3.2.2.8	itr:O		itr:o	Yes No
itr4	Use specific-dest address as TS reply source	RFC 1122: 3.2.2.8	itr:M		itr:m	Yes N/A
itr5	Reflect Record Route, Time Stamp Options	RFC 1122: 3.2.2.6	itr:O		itr:m	Yes N/A

Item	Protocol Feature	Base Standard		Profile		Support
		Reference	Status	Clause	Status	
itr6	Reverse and reflect source route option	RFC 1122: 3.2.2.8	itr:M		itr:m	Yes N/A
itr7	Pass timestamp reply to higher layer	RFC 1122: 3.2.2.8	itr:M		itr:m	Yes N/A
itr8	Obey rules for "standard value"	RFC 1122: 3.2.2.8	itr:M		itr:m	Yes N/A
Address Mask Request and Reply:						
iar1	Address Mask Method is Configurable	RFC 1122: 3.2.2.9	M	2.3.2.3.2	m	Yes
iar2	Support static configuration of address mask		M		m	Yes
iar3	Get address mask dynamically during booting		O		o	Yes No
iar4	Host Send ICMP Address Mask Request/receive Address Mask Reply		O		o	Yes No
iar41	Retransmit Address Mask Req. if no reply		iar4:M		iar4:m	Yes N/A
iar42	Assume default mask if no reply		iar4:O		iar4:m	Yes N/A
iar43	Update address mask from first reply only		iar4:M		iar4:m	Yes N/A
iar5	Reasonableness check on Address Mask		O		m	Yes
iar6	Send unauthorized Address Mask Reply Message		X		x	No
iar61	Explicitly configured to be agent		M		m	Yes
iar7	Static Configuration ==> Addr-Mask-Authoritative flag		O		m	Yes
iar71	Broadcast Address Mask Reply when initiated		M		m	Yes

A.8.7 ICMP MIB-II Group Support

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
icmpg.1	icmpInMsgs	Counter	read-only	RFC1213, Section 6.7	M	2.3.2.3.3	m	Yes
icmpg.2	icmpInErrors	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.3	icmpInDest Unreachs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.4	icmpInTimeExcds	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.5	icmpInParmProbs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.6	icmpInSrc Quenchs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.7	icmpInRedirects	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.	icmpInEchos	Counter	read-only	RFC1213,	M		m	Yes

Item	Object Definition			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
8				Section 6.7				
icmpg.9	icmpEchoReps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.10	icmpIn Timestamps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.11	icmpInTimestamp Reps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.12	icmpInAddrMasks	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.13	icmpInAddrMask Reps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.14	icmpOutMsgs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.15	icmpOutErrors	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.16	icmpOutDest Unreachs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.17	icmpOutTime Excds	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.18	icmpOutParm Probs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.19	icmpOutSrc Quenchs	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.20	icmpOutRedirects	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.21	icmpOutEchos	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.22	icmpOutEcho Reps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.23	icmpOut Timestamps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.24	icmpOut Timestamp Reps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmpg.25	icmpOutAddr Masks	Counter	read-only	RFC1213, Section 6.7	M		m	Yes
icmp 26	icmpOutAddr MaskReps	Counter	read-only	RFC1213, Section 6.7	M		m	Yes

A.9 NETWORK TO DATA LINK INTERFACE PICS PROFOMA

A.9.1 IF MIB-II Group Support

Item	Object Definitions			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ifg.1	ifNumber	INTEGER	read-only	RFC1213, Section 6.4	M	2.4.1	if-group: m	Yes
ifg.2	ifTable	SEQUENCE OF IfEntry	not-accessible	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1	ifEntry	IfEntry	not-accessible	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.1	ifIndex	INTEGER	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.2	ifDescr	Display String	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.3	ifType	INTEGER	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.4	ifMtu	INTEGER	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.5	ifSpeed	Gauge	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.6	ifPhysAddress	Phys Address	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.7	ifAdminStatus	INTEGER	read-write	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.8	ifOperStatus	INTEGER	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.9	ifLastChange	TimeTicks	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.10	ifInOctets	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.11	ifInUcastPkts	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.12	ifInNUcastPkts	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.13	ifInDiscards	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.14	ifInErrors	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.15	ifInUnknown Protos	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.16	ifOutOctets	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.17	ifOutUcastPkts	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.18	ifOutNUcastPkts	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes

Item	Object Definitions			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ifg.2.1.19	ifOutDiscards	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.20	ifOutErrors	Counter	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.21	ifOutQLen	Gauge	read-only	RFC1213, Section 6.4	M		if-group: m	Yes
ifg.2.1.22	ifSpecific	OBJECT IDENTIFIER	read-only	RFC1213, Section 6.4	M		if-group: m	Yes

A.9.2 IP Address Translation MIB-II Group Support

Item	Object Definitions			Base Standard		Profile		Support
	Object	Syntax	Access	Reference	Status	Clause	Status	
ntm.1	ipNetToMedia Table	SEQUENCE OF IpNetTo MediaEntry	not-accessible	RFC1213, Section 6.6	M	2.4.2	m	Yes
ntm.1.1	ipNetTo MediaEntry	IpNetTo MediaEntry	not-accessible	RFC1213, Section 6.6	M		m	Yes
ntm.1.1.1	ipNetTo MediaIndex	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes
ntm.1.1.2	ipNetTo MediaEntry PhysAddress	Phys Address	read-write	RFC1213, Section 6.6	M		m	Yes
ntm.1.1.3	IpNetTo MediaNetAddress	IP Address	read-write	RFC1213, Section 6.6	M		m	Yes
ntm.1.1.4	IpNetTo MediaNetType	INTEGER	read-write	RFC1213, Section 6.6	M		m	Yes

§