Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—

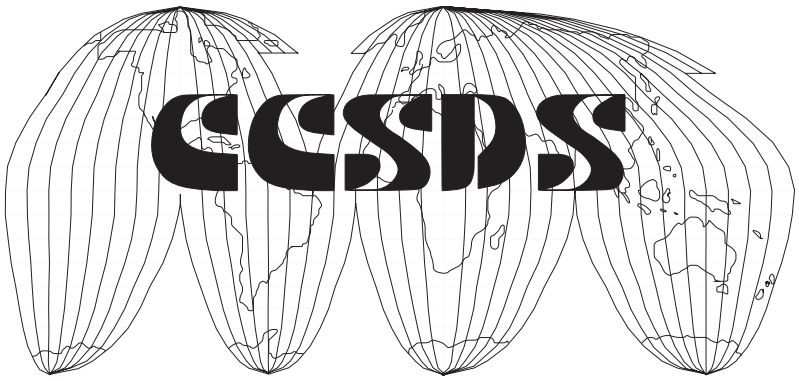
NETWORK PROTOCOL

(SCPS-NP)

CCSDS 713.0-B-1

BLUE BOOK

May 1999



AUTHORITY

Issue:	Blue Book, Issue 1
Date:	May 1999
Location:	Newport Beach, California, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS Recommendations is detailed in reference [B1], and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This Recommendation is published and maintained by:

CCSDS Secretariat
Program Integration Division (Code MT)
National Aeronautics and Space Administration
Washington, DC 20546, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of member space Agencies. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not considered binding on any Agency.

This **Recommendation** is issued by, and represents the consensus of, the CCSDS Plenary body. Agency endorsement of this **Recommendation** is entirely voluntary. Endorsement, however, indicates the following understandings:

- Whenever an Agency establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommendation**. Establishing such a **standard** does not preclude other provisions which an Agency may develop.

- Whenever an Agency establishes a CCSDS-related **standard**, the Agency will provide other CCSDS member Agencies with the following information:

  -- The **standard** itself.

  -- The anticipated date of initial operational capability.

  -- The anticipated duration of operational service.

- Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommendation** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than five years from its date of issuance, this **Recommendation** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or, (3) be retired or canceled.

In those instances when a new version of a **Recommendation** is issued, existing CCSDS-related Agency standards and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each Agency to determine when such standards or implementations are to be modified. Each Agency is, however, strongly encouraged to direct planning for its new standards and implementations towards the later version of the Recommendation.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommendation is therefore subject to CCSDS document management and change control procedures as defined in reference [B1]. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were

Member Agencies

- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- National Aeronautics and Space Administration (NASA)/USA.
- National Space Development Agency of Japan (NASDA)/Japan.
- Russian Space Agency (RSA)/Russian Federation.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Communications Research Laboratory (CRL)/Japan.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Federal Service of Scientific, Technical & Cultural Affairs (FSST&CA)/Belgium.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Industry Canada/Communications Research Centre (CRC)/Canada.
- Institute of Space and Astronautical Science (ISAS)/Japan.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Program Office (NSPO)/Taipei.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 713.0-B-1	Space Communications Protocol Specification (SCPS)—Network Protocol (SCPS-NP)	May 1999	Original issue

CONTENTS

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Recommendation is to define the services and protocols of the Space Communications Protocol Specification (SCPS) Network layer. This definition will allow independent implementations of the protocols in the space and ground segments of the SCPS Network to interoperate.

1.2 SCOPE

This Recommendation is intended to be applied to all systems that claim conformance to the SCPS Network protocols.

1.3 APPLICABILITY

This Recommendation is designed to be applicable to any kind of space mission or infrastructure, regardless of complexity. It is intended that this Recommendation become a uniform standard among all CCSDS Agencies.

1.4 RATIONALE

The CCSDS believes it is important to document the rationale underlying the recommendations chosen, so that future evaluations of proposed changes or improvements will not lose sight of previous decisions. The concept and rationale for SCPS-NP may be found in reference [B3].

1.5 ORGANIZATION OF THIS RECOMMENDATION

This Recommendation contains four sections and four annexes. This section presents introductory material that establishes the context for the remainder of the document. Section 2 contains an overview of the protocol, summarizing the main technical requirements and describing the approach used to provide the protocol's services. Section 3 presents the protocol specifications. Section 4 establishes the requirements for maintaining management information.

The four annexes to this Recommendation provide supporting information. Some of the annexes contain normative material, while some contain informative material. Annex A is informative and contains the acronyms and abbreviations used commonly throughout the document. Annex B is informative and contains the informative references cited throughout the document. Annex C is normative and contains the proforma for the Protocol Implementation Conformance Statement (PICS). The PICS unambiguously describes the capabilities provided by an implementation of the protocol. Annex D is normative and contains the service specification.

1.6 CONVENTIONS AND DEFINITIONS

1.6.1 OCTET NUMBERING CONVENTION AND NOMENCLATURE

This document does not deal with transmission of any elements smaller than one octet. As such, the transmission order of bits within an octet is an issue to be dealt with at lower layers. However, the relative ordering of octets within a word and the unambiguous numbering of bits within an octet are relevant here. The order in which multi-octet fields defined in this document are submitted for transmission is called 'Big Endian' byte ordering. When applied to networking, this is called 'network byte order'. In this ordering scheme, bit 0 of a 32-bit value is the Most Significant Bit (MSB); bit 31 is the least significant bit. The octet containing bits 0-7 is transmitted first, followed by the octet containing bits 8-15, followed by the octet containing bits 16-23, and finally the octet containing bits 24-31. Note also that 'Big Endian' byte ordering is NOT what some machines (notably the 80x86 class of machines) use internally. Implementers must ensure that headers are converted to network byte order for transmission.

The following conventions apply throughout this Recommendation:

- the words 'shall' and 'must' imply a binding and verifiable recommendation;
- the word 'should' implies an optional, but desirable, recommendation;
- the word 'may' implies an optional recommendation;
- the words 'is', 'are', and 'will' imply statements of fact.

1.6.2 DEFINITIONS

Address Family: An address family specifies the structural rules required to interpret the internal fields of an address. The SCPS Network supports three address families: the SCPS address family, the Internet Protocol (IP) address family, and the Internet Protocol version Six (IPv6) address family.

Address Type: An address type defines the meaning that the addresses have (that is, whether they identify end systems or a path between end systems), the number of addresses that appear in a SCPS Network Protocol header (two addresses if the addresses identify end systems, only one if the address identifies a path between end systems), and the address family that is valid for the addresses. Refer to table 3-5 for a list of Address Types supported in the SCPS Network.

Basic End System Address: A Basic End System Address identifies a single end system or an end-system group. The Basic End System Address conforms to the structural rules of the SCPS Address Family, and consists of the least-significant octet of an Extended End System Address. Basic End System Addresses may be used in networks in which it can be guaranteed (through network configuration) that the remaining portion of the address will be unambiguous through the life of the datagram. (Note that Basic End System Addresses are NOT parameters to the Unit Data service primitives.)

Basic Path Address: A Basic Path Address identifies a managed virtual connection between two or more end systems. The Path Address conforms to the structural rules of the SCPS Address Family and consists of the least-significant octet of an Extended Path Address. Basic Path Addresses may be used in networks in which it can be guaranteed (through network configuration) that the remaining portion of the address will be unambiguous through the life of the datagram. (Note that Basic Path Addresses are NOT parameters to the Unit Data service primitives.)

Confirm (primitive): A primitive issued by a service-provider to complete, at a particular service-access-point, some procedure previously invoked by a request at that service-access-point.

Domain Identifier: The Domain Identifier (D-ID) is an element of the Extended End System Address and of the Extended Path Address. When part of the Extended End System Address, it identifies groups of Basic End System Addresses. When part of the SCPS Extended Path Address, it identifies groups of Basic Path Addresses. (Note that groups of addresses does *not* mean group addresses.)

End System Identifier: The End System Identifier (ES-ID) is an element of Basic End System Addresses and of Extended End System Addresses. It allows the identification of individual systems or of multicast groups (when qualified by the multicast flag). It has valid values between 0 and 127, although specific programs may choose not to make all of these available.

End System: An addressable network entity within the SCPS Network.

Extended End System Address: The Extended End System Address identifies a single end system or an end-system group. The Extended End System Address conforms to the structural rules of either the SCPS Address Family or the IP Address Family. Extended End System Addresses may be parameters to the primitives of the Unit Data service.

Extended Path Address: The Extended Path Address identifies a managed virtual connection between two or more end systems. The Path Address conforms to the structural rules of the SCPS Address Family. (Note that Extended Path Addresses are NOT parameters to the Unit Data service primitives.)

Gateway: A network-addressable system that terminates a protocol at a given layer and invokes similar services at the same layer of an adjacent network.

Host: A network-addressable system that may send or receive network-layer datagrams but does not forward datagrams.

Indication (primitive): A primitive issued by a service provider either to invoke some procedure or to indicate that a procedure has been invoked by the service user at a peer service-access-point.

Intermediate Delivery flag: A control field element that indicates whether the network user data (the N-SDU) should be delivered to the destination system only (the typical case) or to the destination and all intermediate systems. The parameter has two values: DESTINATION (the default, value '0'), which indicates that the N-SDU shall be delivered only to the destination address; and INTERMEDIATE (value '1'), which indicates that the N-SDU shall be delivered to the destination address and to all intermediate systems encountered.

NOTE – The INTERMEDIATE setting of Intermediate Delivery flag is intended for diagnostic use, to provide a single-transmission 'traceroute' service. The 'traceroute' service, used in the Internet, provides a response from each intermediate router between a source and destination by repeatedly sending echo messages to the destination, but starting the maximum hops at one, and incrementing it one for each message. This results in the return of an error message to the source from the router that discarded the datagram. The traceroute service is simple, but it generates a significant amount of traffic and takes a significant amount of time to trace a route. The Intermediate Delivery capability is intended to cause all intermediate systems to provide a response to the same Echo Request. The address information and hop count information can be used to construct the route to the destination.

Internet Protocol Number: The Internet Protocol Number is the transport protocol identifier used by Internet Protocols. Values may range from 0 through 255, and valid values are defined in reference [B14].

IP Address Family: The IP Address Family specifies a set of structural rules for the interpretation of Extended End System Addresses; it is defined in reference [B11], and the possible formats are refined in section 3.2.1.3 of reference [B12].

IPv6 Address: The IPv6 Address Architecture is defined in RFC 2373 (see reference [B16]). Note that the IPv6 address is not currently one of the valid types for the N-Destination_Address or the N-Source_Address (refer to Annex D).

Maximum Transmission Unit: The Maximum Transmission Unit (MTU) specifies the maximum amount of data that the subnetwork layer will accept in a single subnetwork service request. The MTU for a route is the minimum of all known MTUs along that route.

NOTE – It is anticipated that this value will be known and managed as part of the routing table information; however, techniques for dynamically discovering the MTU of a route exist. Refer to RFC 1191, *Path MTU Discovery* (reference [B2]) for more information.

Multicast Flag: The Multicast Flag (M-Flag) is an element of addresses within the SCPS Address Family. The M-Flag indicates whether the address refers to a single end system or path, or identifies a group address. Group addresses may identify zero or more end systems or paths.

N-Address: an address in the SCPS Network. The attributes of an N-Address are the Address Type and the Address Family.

Network Service Data Unit: See N-SDU.

N-SDU: The Network Service Data Unit (N-SDU) is a parameter of the Unit Data service primitives. It is a variable-length, octet-aligned data unit of arbitrary format. The maximum length of an N-SDU is 8141 octets. Local restrictions on datagram size or extensions to the protocol may further limit this size; the maximum length of an N-SDU for an implementation **shall** be documented by the implementer.

NOTE – The maximum size of the N-SDU field is limited to the length resulting from subtracting the maximum length of a SCPS-NP header from the maximum SCPS-NP PDU length. The maximum length of the SCPS-NP header is 50 octets. The length field in the SCPS-NP header is 13-bits, which allows an 8191-octet total datagram length. Therefore, the maximum size of an N-SDU that is guaranteed to fit in a SCPS-NP PDU is 8141 octets.

Path Identifier: The Path Identifier (P-ID) is an element of the Basic Path Address and the Extended Path Address. It identifies a static, managed communication path between two (or more) systems. Path Identifiers may range in value from 0 through 127, although specific programs may restrict the P-IDs available.

Precedence field: A sub-field within the Basic Quality of Service field of the SCPS Network Protocol header. When present, the Precedence field may vary from 0 to 15, with 0 being the lowest precedence and 15 being the highest.

Primitive (also known as service-primitive): An abstract, implementation-independent interaction between a service-user and the service-provider.

Program Specific field: A sub-field within the Basic Quality of Service field of the SCPS Network Protocol header. When present, the Program Specific field may vary from 0 to 3.

Request (primitive): A primitive issued by a service-user to invoke some procedure.

Response (primitive): A primitive issued by a service-user to complete, at a particular service-access-point, some procedure previously invoked by an indication at that service-access-point.

Router: A network-addressable system that may send, receive, or forward network-layer datagrams.

Routing Requirements field: A sub-field within the Basic Quality of Service field of the SCPS Network Protocol header. When present, the Routing Requirements field may vary from 0 to 3. Refer to 3.2.3.6 for the assigned values of this field. The default value for the Routing Requirements field is 0, which indicates ‘normal’ routing.

SCPS Network Address: A SCPS Network Address specifies one of the possible SCPS Address formats and the values of the parameters required by that format.

Service-Access-Point: A point at which the services of a layer are made available to the layer above it.

Service-Primitive: See Primitive.

Silently Discard: A datagram is 'silently discarded' if no error message is generated (either to a local user or to a remote user) as a result of the discard. The practice of silently discarding datagrams reduces the possibility that a misconfigured host will uncontrollably generate erroneous traffic. The term 'silent discard' differs from 'discard' in that certain actions, such as informing network service users about the discard, are not performed in a silent discard. When the term 'discard' is used, other information must be used to determine whether the network service user is informed.

Transport Protocol Identifier field: The Transport Protocol Identifier (TP-ID) is a field in the SCPS-NP header that identifies the SCPS Network user (i.e., the transport protocol) from which the datagram originated and to which the datagram should be delivered at its destination(s). It is a 4-bit field that carries a translation of the N-User_Internet_Protocol_Number parameter of the Unit Data service primitives. The translation table appears in table 3-3.

Tuple: A tuple is an ordered set of arbitrary length.

1.7 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommendation are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS Recommendations.

[1] K. Nichols, S. Blake, F. Baker, and D. Black. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, December 1998.†

[2] *Time Code Formats*. Recommendation for Space Data Systems Standards, CCSDS 301.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, April 1990.

† Internet Request for Comments (RFC) texts are available on line in various locations (e.g., http://ietf.org/rfc/).

2 OVERVIEW

This Recommendation specifies a new service and protocol to meet the needs of current and future space missions. It supports communication environments with static, highly managed communication through fully connectionless communication with dynamic routing. All of these types of operations are supported with near-optimal bit efficiency.

This Recommendation is based on concepts that have been drawn from a number of sources: the notion of 'Path Service', or essentially a permanent-virtual-circuit form of addressing, is drawn from the Consultative Committee for Space Data Systems (CCSDS) Recommendation for Advanced Orbiting Systems, CCSDS-701.0-B-2 (reference [B4]), from the CCSDS Recommendation for Telecommand, Part 2, CCSDS-202.0-B-2 (reference [B5]), and from the CCSDS Recommendation for Packet Telemetry, CCSDS 102.0-B-3 (reference [B6]); other ideas are taken directly or indirectly from the Internet Protocol specification and numerous explanatory publications; and the SCPS-NP header construction approach is based on the header compression concepts elaborated in RFC 1144 (reference [B17]—see annex B).

The Technical Requirements for the Recommendation include:

- support for connectionless and managed-connection operation;
- efficient operation in constrained bandwidth conditions;
- support for precedence (priority) based handling;
- support for datagram lifetime control;
- support for multiple routing options;
- signaling of information pertinent to upper-layer protocol processing.

The SCPS Network Protocol (SCPS-NP) uses a technique called 'capability-driven header construction' as a means to control bit overhead. Capability-driven header construction simply means that the format of the SCPS-NP header is based (exclusively) on the protocol capabilities required for the communication of the particular datagram in question. That is, a datagram carries those header elements that are required to provide service properly to the datagram, but no others.

The capabilities required to support a datagram are derived from three sources: the protocol itself, the operating environment, and the network service user. Some capabilities are required to support a particular protocol version. An example of this is the capability of datagram length delimiting. Other capabilities are required to address particular network environmental conditions. An example of an environmentally required capability is header error protection. The third source of capability requirements is the network service user. An example of a user-required capability is precedence (priority).

The capability requirements from these three sources are used to select the set of header elements necessary to provide the required services in the transmission of the datagram. One key header element is a variable-length control field that identifies the remaining header elements that are included in the datagram. This control field is present in all versions of the SCPS-NP, and is the last header element before those header elements specified in the control field.

In addition to user data transfer, this Recommendation specifies the means for exchanging network-layer control information through the SCPS Network, and for selectively passing that information to SCPS Network users.

3 PROTOCOL SPECIFICATION

3.1 ADDRESSING

3.1.1 ADDRESS FAMILIES

A Network Address (N-Address) in the SCPS Network shall meet the structural requirements of one of three address families:

a) **SCPS Address Family**. The SCPS address family contains both End System Addresses (identifying a single end system) and Path Addresses (identifying a pair of communication systems). SCPS-family N-Addresses are structured as follows:

1) N-Addresses in the SCPS family are four octets in length and are represented in this text as four eight-bit quantities separated by periods, e.g., w.x.y.z, where the range of each of the alphabetic characters is from 0 to 255 decimal.

NOTE – The form w.x.y.z is the Extended form of a SCPS address. The Basic form of the SCPS address (z) may be used if it can be guaranteed (through network configuration) that the w.x.y portion of the address will be unambiguous through the life of the datagram.

2) The most-significant octet (the w octet) of a SCPS-family N-Address contains the value 10 (decimal), which is the value reserved by the Internet Assigned Numbers Authority (IANA) for private Internet address spaces.

3) The x and y octets are combined to form the addressing domain for various programs; the x.y field is known as the Domain Identifier (D-ID).

NOTE – A single mission may be allocated more than one D-ID for its needs. Determination of the registration authority to allocate and deallocate domain identifiers is beyond the scope of this Recommendation.

4) The z octet is administered by the program to which the D-ID is allocated and is subdivided as follows:

– bits 0-6 form a field, which contains either an End System Identifier (ES-ID) or a Path Identifier (P-ID) in the range 0 to 126 (the value of 127 is reserved for use in conjunction with the Multicast Flag to form the broadcast address);

– bit 7 is the Multicast Flag (M-Flag), which signals whether the address is a multicast or unicast address:

• the M-Flag shall be set to ‘1’ for multicast addresses;

• the M-Flag shall be set to ‘0’ for unicast addresses.

b) **Internet Protocol (IP) Address Family**. The IP address family contains End-System Addresses that are appropriate for routing and delivery across the Internet. The structure of Internet addresses is defined in reference [B11] (RFC 791, section 2.3, and RFC 1112, section 4) and reference [B12] (RFC 1122, section 3.2.1.3).

c) **Internet Protocol version Six (IPv6) Address Family**. IPv6 format addresses are intended for those programs that do not have significant bit-efficiency issues and require global addressability. IPv6 address formats are specified in reference [B16].

3.1.2 BROADCAST ADDRESS DEFINITION

3.1.2.1 SCPS Address Family Broadcast Address Definition

3.1.2.1.1 Unless otherwise stated, the SCPS Address family conforms to the same broadcast address definitions as the IP Address Family, described in 3.1.1.

3.1.2.1.2 A SCPS Address of 10.x.y.255 is the broadcast address for the x.y addressing domain and shall be treated in the same manner as an IP-address family subnet-directed broadcast with a subnet mask of 255.255.255.0 (refer to 3.1.2.2, below).

3.1.2.1.3 A SCPS Address of 10.255.255.255 is the broadcast address for the entire SCPS addressing domain and shall be treated in the same manner as an IP-address family net-directed broadcast (refer to 3.1.2.2, below).

3.1.2.2 Internet Protocol Address Family Broadcast Address Definition

NOTE - much of this text is from reference [B18].

3.1.2.2.1 Limited Broadcast Address

a) The *limited broadcast address* is defined as 255.255.255.255, where the form of the address is specified in 3.1.1 a) 1), above.

b) Datagrams destined to the limited broadcast address shall be transmitted on all local interfaces that support broadcasting.

c) Datagrams destined to the limited broadcast address shall not be forwarded upon receipt.

3.1.2.2.2 Net-Directed Broadcast Address

a) The net-directed broadcast address has as its host ID all one-bits.

b) The Class A net-directed broadcast address is netid.255.255.255.

NOTE – The net-directed broadcast address for the entire SCPS Address Family is 10.255.255.255.

c) The Class B net-directed broadcast address is netid.255.255, since the network identifier of a Class B network is the most-significant 16 bits of the address and the host identifier is the least-significant 16 bits.

d) The Class C net-directed broadcast address is netid.255, since the network identifier of a Class C network is the most-significant 24 bits of the address and the host identifier is the least-significant 8 bits.

e) Routers shall be capable of forwarding datagrams addressed to net-directed broadcast addresses.

f) Routers shall be capable of disabling the forwarding of net-directed broadcasts.

3.1.2.2.3 Subnet-Directed Broadcast Address

a) The subnet-directed broadcast address has as its host ID all one-bits with the exception of those bits that specify the subnetwork.

b) Identification of an address as a subnet-directed broadcast address requires knowledge of the subnet mask. If the subnet mask is not known, the datagram shall be treated as a unicast transmission.

c) Datagrams addressed to subnet-directed broadcast addresses shall be broadcast only within the specified subnetwork.

3.1.2.2.4 All-Subnets-Directed Broadcast Addresses

All-subnets-directed broadcast addresses shall not be supported.

NOTE – These addresses are identical in structure to *net-directed broadcast addresses*; however, there is a subnet mask defined for the destination.

3.1.2.3 IPv6 Address Family Broadcast Address Definition

There are no broadcast addresses defined in IPv6.

3.2 SCPS NETWORK PROTOCOL SPECIFICATION

3.2.1 SCPS-NP DATAGRAM

A SCPS-NP datagram shall consist of a header followed by zero or more octets of N-SDU.

3.2.2 SCPS-NP HEADER

3.2.2.1 SCPS-NP Header Format

The SCPS-NP header is mandatory for the SCPS-NP datagram and shall consist of mandatory and capability-defined elements positioned contiguously in the following sequence:

	Length in bits
– Version/Protocol Identifier Field (mandatory)	3
– Datagram Length Field (mandatory)	13
– Transport Protocol ID Field (mandatory)	4
– Control Field (first four bits mandatory)	4, 12, or 20
– Destination Address Field (mandatory)	8, 32, or 128
– Source Address Field (capability dependent)	8, 32, or 128
– Basic QOS Field (capability dependent)	8
– Hop Count Field (capability dependent)	8
– Timestamp Field (capability dependent)	24 or 32
– Expanded QOS Field (capability dependent)	8
– Header Checksum Field (capability dependent)	16

NOTE – The general format of the SCPS-NP datagram is shown in figure 3-1. Fields that are included based on capability requirements are shaded.

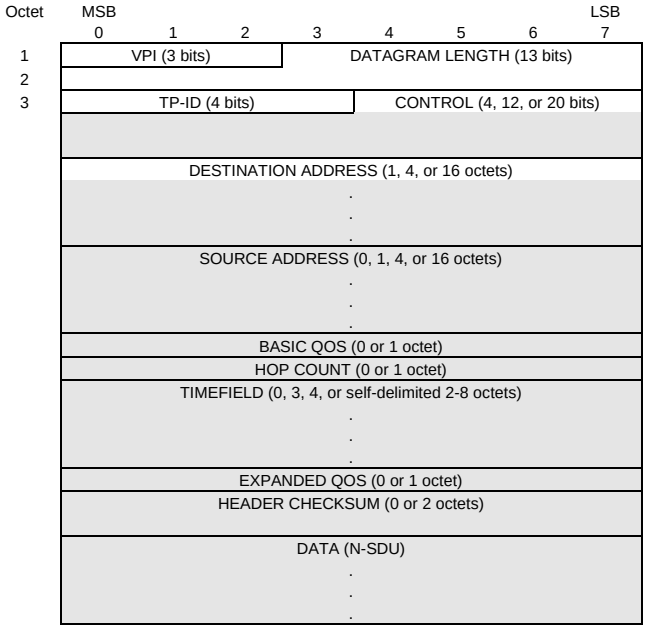


Figure 3-1: SCPS-NP Datagram

3.2.2.2 SCPS-NP Header Construction

The SCPS-NP header shall be constructed by concatenating elements that satisfy the datagram capability requirements of the protocol, the network, and the user, as shown in table 3-1.

Table 3-1: Relationship of Header Elements to Selected Protocol Capabilities

Requirement Origin	Selected Protocol Capability	Header Element
Protocol	Version and protocol identification	Version/Protocol ID
	Datagram length delimiting	Datagram Length Field
	Transport protocol selection	Transport Protocol ID Field
	Requirements-based capability selection	Control Field
	Destination address	Destination Address Field
Network	Header error protection	Header Checksum Field
	Routing loop control	Hop Count or Timestamp Field
User	Source address	Source Address Field
	Time of transmission signaling	Timestamp Field
	Precedence	Basic QOS Field
	Routing requirements	Basic QOS Field
	Intermediate system delivery	Control Field
	Program-specific signaling	Basic QOS Field
	Ground type-of-service request	Expanded QOS Field

3.2.3 SCPS-NP HEADER ELEMENTS

3.2.3.1 Version/Protocol Identifier Field

3.2.3.1.1 The Version/Protocol Identifier (VPI) Field shall be three bits in length and shall occupy bits 0–2 of the SCPS-NP header.

3.2.3.1.2 The VPI field shall be set to ‘001’.

3.2.3.2 Datagram Length Indicator Field

3.2.3.2.1 The Datagram Length Indicator field shall be 13 bits in length and shall occupy bits 3–15 of the SCPS-NP header.

3.2.3.2.2 The Datagram Length Indicator field shall contain the total length of the datagram, including all network-layer header information, in octets.

NOTE – When the VPI is set to ‘001’, the minimum legal value for the Datagram Length field is four, corresponding to a SCPS-NP Data Unit consisting only of a header, with the header containing only the VPI, Datagram Length Indicator, TP-ID, the first four bits of the Control Field, and an eight-bit destination address.

3.2.3.3 Transport Protocol Identifier Field

3.2.3.3.1 The TP-ID field shall be four bits in length and shall occupy bits 16–19 of the SCPS-NP header.

3.2.3.3.2 The TP-ID field shall contain a binary value corresponding to a network service user number as defined in table 3-2.

Table 3-2: Assigned TP-ID Values

Binary Value	Protocol	Binary Value	Protocol
0000	Reserved	1000	SCPS-SP (reference [B7])
0001	SCMP (see 3.1.2.1)	1001	Unassigned
0010	Unassigned	1010	IPv6 ATH (reference [B9])
0011	Unassigned	1011	IPv6 ESP (reference [B10])
0100	Compressed SCPS-TP TCP (reference [B8])	1100	Unassigned
0101	SCPS-TP UDP (reference [B8])	1101	Unassigned
0110	SCPS-TP TCP (reference [B8])	1110	Unassigned
0111	Unassigned	1111	Unassigned

NOTE – Correspondence between TP-ID values and IP numbers is indicated in table 3-3.

Table 3-3: Mapping of Assigned SCPS TP-ID Values to IP Numbers

Protocol	SCPS TP-ID Number	IP Number
SCMP	1	None
Compressed SCPS-TP TCP (reference [B8])	4	105
(SCPS-TP) UDP (reference [B8])	5	17
(SCPS-TP) TCP (reference [B8])	6	6
SCPS-SP (reference [B7])	8	99
IPv6 ATH (reference [B9])	10	51
IPv6 ESP (reference [B10])	11	50

3.2.3.4 Control Field

3.2.3.4.1 The Control Field shall be either 4, 12, or 20 bits[1] in length and shall begin in bit 20 of the SCPS-NP header:

3.2.3.4.2 The Control Field shall consist of some or all of the subfields described in table 3-4.

3.2.3.4.3 When an octet of the Control Field is not present, the values of the subfields of that octet shall be assumed to be zero.

[1] The maximum length of the Control field may be increased in future versions of this specification.

Table 3-4: Control Field Elements

Header Bit #	Control Field Element	Permitted Values	Cf. Sub-section	Notes
20	Bit Field Continues	'1' Control field continues in octet 4 of the SCPS-NP header '0' Control field is contained within octet 3 of the SCPS-NP header		1,2
21	Reserved by CCSDS	'0' Undefined		1
22	Destination Address Present (Dest Addr)	'1' Destination Address field present '0' Undefined	3.2.3.5	1, 3
23	Header Checksum	'1' Checksum present '0' Checksum not present	3.2.3.10	1
24	Bit Field Continues	'1' Control field continues in octet 5 of the SCPS-NP header '0' Control field is contained within octets 3 and 4 of the SCPS-NP header		2
25	Source Address Present (Source Addr)	'1' Source Address field present '0' Source Address field not present	3.2.3.5	4
26	Hop Count	'1' Hop Count field present '0' Hop Count field not present	3.2.3.7	
27-28	Timestamp Format	'11' 32-bit Binary Timestamp present '10' CCSDS CUC Timestamp (Explicit P-field) present '01' CCSDS 24-bit CUC Timestamp (Implicit P-field) present '00' Timestamp field not present	3.2.3.8	
29	Reserved by CCSDS	'0' Undefined		
30	Basic QOS	'1' Basic QOS field present '0' Basic QOS field not present	3.2.3.6	
31	Extended Addresses	'1' Extended Addresses '0' Basic Addresses	3.2.3.5	4
32	Bit Field Continues	'0' Control field is contained within octets 3, 4, and 5 of the SCPS-NP header		2
33	IPv6 Addresses (IPv6)	'1' IPv6 Addresses present '0' IPv6 Addresses not present	3.2.3.5	5
34	Expanded QOS	'1' Expanded QOS field present '0' Expanded QOS field not present	3.2.3.9	
35	Intermediate Delivery	'1' intermediate systems should deliver the datagram to the local transport protocol identified by the TP-ID as well as queue for forwarding to the destination '0' no special actions required for intermediate systems		
36	Not Assigned	'0' Undefined		
37	Not Assigned	'0' Undefined		
38	Not Assigned	'0' Undefined		
39	Not Assigned	'0' Undefined		

NOTES

1 Inclusion of this subfield is mandatory regardless of its value.

2 The 'Bit Field Continues' bits in the control field bit-vector are used to determine its length. If bit 20 of the header = '0', the control field bit vector length = 4 bits. If bit 20 = '1' and bit 24 = '0', the control field bit vector length = 12 bits. If bits 20 and 24 = '1' and bit 32 = '0', the control field bit vector length = 20 bits. If bits 20, 24, and 32 = '1', the control field bit vector length exceeds 20 bits.

3 When the Destination Address Present Flag is set to '1', the header contains a destination address. A value of '0' for the Destination Address Present flag is undefined. When this flag is set to '1' and the Source Address Present flag is not set to '1', the Destination Address is treated as a unidirectional permanent virtual circuit (a Path). When the Destination Address Present flag and the Source Address Present flag are both set to '1', the Destination Address is treated as a connectionless datagram address.

4 Shall not be set to '1' unless Destination Address Flag is set to '1'.

5 Shall not be set to '1' unless both Destination and Source Address Flags are set to '1'.

NOTE – The elements of the control field are illustrated in figure 3-2.

Octet	MSB							LSB
3					20 Bit Field Continues	21 Reserved by CCSDS	22 Dest Addr	23 Header Cksum
	24 Bit Field Continues	25 Source Addr	26 Hop Count	27 Timestamp Format	28	29 Reserved by CCSDS	30 Basic QOS	31 Extended Addrs
	32 Bit Field Continues	33 IPv6 Addrs	34 Expanded QOS	35 Intermed. Delivery	36 Reserved by CCSDS	37 Reserved by CCSDS	38 Reserved by CCSDS	39 Reserved by CCSDS

Figure 3-2: Control Field Subfields

3.2.3.5 Address Fields

An N-Address used in the SCPS-NP header shall be one of five address types, shown in table 3-5, encoded from the three address families described in 3.1.1.

Table 3-5: SCPS Network Protocol Address Types

Address Type	Address Length	Addresses per header	Address Family	Description
Extended End System Address	4 octets	2	IP or SCPS	Registered IP addresses or SCPS Address family addresses
Extended Path Address	4 octets	1	SCPS	Managed connection between source and destination(s)
Basic End System Address	1 octet	2	SCPS	Least significant octet of SCPS Extended End System Addresses
Basic Path Address	1 octet	1	SCPS	Least significant octet of SCPS Extended Path Addresses
IPv6 Address	16 octets	2	IPv6	Registered IP Version 6 addresses

NOTE – The relationship between the four address flags in the Control field, as well as the significance of their possible combinations of values, is indicated in table 3-6.

Table 3-6: Control Field Flag Settings for SCPS Address Formats

Address Format	Control Field Flags			
	Dest Addr	Src Addr	Extended Addrs	IPv6 Addrs
Extended End System	‘1’	‘1’	‘1’	‘0’
Extended Path	‘1’	‘0’	‘1’	‘0’
Basic End System	‘1’	‘1’	‘0’	‘0’
Basic Path	‘1’	‘0’	‘0’	‘0’
IPv6	‘1’	‘1’	‘0’	‘1’

NOTE – The broadcast addresses for 'Basic' Format addresses (End System and Path) are consistent with other types of Basic Format addresses: the least significant octet of the Extended Format address becomes the Basic Format of the address. The most significant three octets are assumed to be the local address domain. Therefore, the Extended Format broadcast address for addressing domain x.y would be 10.x.y.255, and the Basic Format would be 255. Note that this Basic Format has meaning *only within addressing domain x.y.*

3.2.3.6 Basic QOS Field

3.2.3.6.1 The Basic QOS field shall be one octet in length and shall begin on the next octet boundary following the location of the header address field(s).

3.2.3.6.2 The Basic QOS field, shown in figure 3-3, shall consist of the following three subfields in the following sequence:

	Length in bits
– Precedence subfield	4
– Routing Requirements subfield	2
– Program Specific subfield	2

3.2.3.6.3 Precedence Subfield

a) The Precedence subfield shall contain a value between 0 (lowest precedence) and 15 (highest precedence) describing the precedence of the datagram.

b) The SCPS-NP shall use the precedence field as described in 3.2.6.2 and 3.3.

c) If the Basic QOS field is not present in a datagram header, the precedence of the datagram shall be the default value specified in the Management Information Base (MIB) parameter npDefaultPrecedence (see 4.1.3.3).

3.2.3.6.4 Routing Requirements Subfield

The Routing Requirements subfield shall contain a value between 0 and 3 signaling a routing method selected from table 3-7.

Table 3-7: Routing Requirements Field Values

Routing Rqts Value	Interpretation
'00'	Point-to-point routing
'01'	Reserved by CCSDS
'10'	Reserved by CCSDS
'11'	Flood routing

3.2.3.6.5 Program Specific Subfield

a) The Program Specific subfield shall contain a value between 0 and 3 and shall be used by the user application to convey control information that is parsed in a program-specific way.

b) The default value of the Program Specific subfield shall be 0, which corresponds to 'No program-specific action'.

NOTE – The Program Specific subfield is present to allow program-specific extensions to SCPS-NP, and the appropriate mechanisms to parse and respond to the values of this field are the responsibility of the program implementing the modifications.

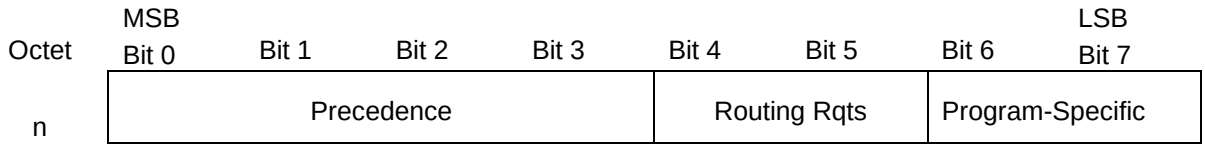


Figure 3-3: SCPS-NP Header - Basic Quality of Service Field

3.2.3.7 Hop Count Field

3.2.3.7.1 The Hop Count field shall be one octet in length and shall be located on the next octet boundary following the location for the Basic Quality of Service field(s).

3.2.3.7.2 The Hop Count field shall contain an eight-bit decrementing counter that shall be initialized to the maximum number of hops (relays through an intermediate system) that a SCPS-NP datagram is permitted to experience before being discarded.

3.2.3.8 Timestamp Field

NOTE – The Timestamp field may be used for two purposes:

– to provide a limit on the time that datagrams can exist in the network (to eliminate routing loops or to bound the time that TCP segments exist);

– to provide datagram identification for flood-routed datagrams (this use of timestamps is discussed in more detail in 3.2.5.5).

3.2.3.8.1 Timestamp Field Length and Location

a) The Timestamp field, if present, shall either be three or four octets in length, or shall be of a self-delimiting format as specified in this subsection.

b) The Timestamp field shall be located on the next octet boundary following the location for the Hop Count field.

3.2.3.8.2 General Timestamp Formats

a) The Timestamp field shall conform to one of two general formats:

   1) the CCSDS Unsegmented Time Code (CUC), or

   2) the Binary Timestamp Format.

b) Within the CUC format, there are two supported versions:

   1) one with an *implicit* Preamble Field (P-Field), and

   2) one with an *explicit* P-Field.

c) All implementations of the SCPS-NP shall support at least one of the formats specified in this subsection.

d) Implementations of the SCPS-NP SHOULD support all formats.

NOTE – In particular, ground-based routers that may support more than one flight element SHOULD support all timestamp formats in order to minimize the possibility that the router may not be able to perform routing loop control for some datagrams.

e) The supported formats shall be documented in the Protocol Implementation Conformance Statement, the proforma for which appears in annex C.

3.2.3.8.3 Timestamp Field Formats

The Timestamp field shall contain a timestamp in one of the following formats:

a) CCSDS Unsegmented Time Code (CUC) Timestamp Format with Implicit P-Field:

   1) When the Timestamp Format bits of the Control Field (bits 27–28) are set to ‘01’ then the CUC Timestamp Format with Implicit P-Field shall be included in the header.

   2) The length of the CUC Timestamp Format with Implicit P-Field shall be three octets.

3) CUC Format:

   – the CUC shall be composed of two fields, the Preamble field (P-field) and the Time field (T-field), as specified in reference [2];

   – the P-field shall *not* be carried with the timestamp, but is constant and defined in this subsection;

   – the T-field shall be carried in the SCPS-NP header and shall consist of three contiguous eight-bit time elements.

4) Timestamp definition:

   – the P-Field shall be set to '0010 0010', or hexadecimal 22:

     • the Extension flag of the P-field shall be set to '0',

     • the time code identification field (bits 1-3) shall be set to '010', indicating an Agency-defined epoch,

     • bits 4 and 5 of the P-field shall be set to '00' (the value resulting from subtracting one from the number of octets of coarse time),

     • bits 6 and 7 of the P-field shall be set to '10' (the number of octets of fine time);

   – the T-Field shall consist of one octet of whole seconds (coarse time) and two octets of fractional seconds (fine time), which establishes the range of the time code to be 256 seconds, and the resolution to be 1/65536 seconds (approximately 15 microseconds).

5) The time-to-live value for datagrams carrying the CUC Timestamp Format with Implicit P-Field shall be taken from the MIB parameter npTimeToLivePField1.

b) CCSDS Unsegmented Time Code (CUC) Timestamp Format with Explicit P-Field:

1) When the Timestamp Format bits of the Control Field (bits 27–28) are set to '10' then the CUC Timestamp Format with Explicit P-Field shall be included in the header.

2) The length of the CUC Timestamp Format with Explicit P-Field shall be variable, as determined by the P-Field, and shall be greater than or equal to two octets in length and less than or equal to eight octets in length.

3) The CUC Timestamp Format with Explicit P-Field shall be transmitted with the P-Field as the most significant octet of the timestamp and the T-Field as the least significant octet(s). The order of octets within the T-Field shall be in accordance with reference [2].

4) The time-to-live value for datagrams carrying this timestamp format shall be taken from the MIB parameter npTimeToLivePField2.

c) Binary Timestamp Format (four octets):

1) When the Timestamp Format bits of the Control Field (bits 27–28) are set to '11' then the binary timestamp shall be included in the header.

2) The binary timestamp shall be a 32-bit quantity representing the microseconds since 00:00 GMT, 1 January 1970, modulo 2^{32}.

3) The time-to-live value for datagrams carrying this timestamp format shall be taken from the MIB parameter npTimeToLivePField2.

3.2.3.9 Expanded QOS Field

3.2.3.9.1 The Expanded QOS field shall be one octet in length and shall begin on the next octet boundary following the location of the Timestamp field.

3.2.3.9.2 The format and content of the Expanded QOS field shall conform to the requirements of RFC 2474 (reference [1]).

3.2.3.9.3 When carried in the SCPS-NP header, the information in the Expanded QOS field shall be supplied to IP-based internetworks (on the ground) for provision of the appropriate service through the ground internetwork.

NOTE – The role of the SCPS-NP regarding this field is merely to convey the Differentiated Services Field information and to request it at gateways in which the SCPS-NP data is carried by IP.

3.2.3.10 Header Checksum Field

3.2.3.10.1 The Header Checksum field shall be two octets in length and shall occupy the final two octets of the SCPS-NP header.

3.2.3.10.2 The Header Checksum field shall contain the 16-bit one's complement of the one's complement sum of all 16-bit words in the SCPS-NP header.

3.2.3.10.3 For purposes of computing the checksum,

a) the value of the Header Checksum field shall be zero;

b) if the SCPS-NP header contains an odd number of octets, the header shall be conceptually padded with a single zero-valued octet, which shall not be transmitted with the header.

3.2.4 HEADER PARSING

3.2.4.1 A receiving system must parse the SCPS-NP header to locate the fields within the header and to verify the validity of the header. Specific header elements that must be verified are given in table 3-8.

3.2.4.2 For errors that caused the datagram to be discarded, the system parsing the header **may** send an SCMP Parameter Problem message to the source, with the pointer indicating the length field for npInBadLength errors, the destination address field for npInBadAddress errors, and the checksum field for the npInBadChecksum error.

NOTE – Checksum failure may mean the ability to identify the source has been compromised.

Table 3-8: Verification of Header Validity

Test performed by Receiving System	Actions on Verification Failure	
	Datagram Handling	Increment MIB Parameter
Verify that the datagram length reported by the data link layer is ≥ the minimum-length legal SCPS-NP data unit (four octets)	discard datagram	npInBadLength
Verify that the SCPS-NP version is set to '001'	locally defined	npInBadVersion
Verify that the NP datagram length indicator ≤ datagram length reported by the link layer	discard datagram	npInBadLength
Verify that the control field is ≤ 20 bits; unassigned bits = 0	locally defined	-
Verify that the control field length is consistent with length of datagram (that is, the datagram length is ≥ 3 + the number of octets or partial octets in the control field)	discard datagram	npInBadLength
Verify that the Extended Addresses and IPv6 control flags are not both set to '1'	discard datagram	npInBadAddress
Verify that if the IPv6 control flag is set to '1', both source address present and destination address present control flags are also set to '1'	discard datagram	npInBadAddress
Verify that the header checksum, if present, indicates that the header is not corrupted	discard datagram	npInBadChecksum

3.2.5 SYSTEM OPERATION

NOTE – This subsection refers to the terms 'end system' and 'router'. Routers are configured to forward received datagrams under certain conditions (such as, if the destination address is not one of the local addresses, or if the destination address is a multicast or broadcast address). End systems do not perform this forwarding function.

3.2.5.1 Origination of Datagrams

All routers and end systems shall be capable of originating datagrams, in order to be able to send user data or control messages.

3.2.5.2 Receipt of Datagrams

3.2.5.2.1 Datagrams Addressed to a Local Address

All routers and end systems shall be capable of recognizing their local addresses and delivering datagrams addressed to one or more of those local addresses to the specified network service users.

3.2.5.2.2 Datagrams Requiring Intermediate Delivery

All routers shall be capable of recognizing the Intermediate Delivery flag and delivering datagrams with the Intermediate Delivery flag set to '1' to the specified network service users.

3.2.5.3 Datagram Transmission Procedures

3.2.5.3.1 Overview

To originate a SCPS-NP datagram, a system must perform five distinct actions:

- ensure that the user's request is valid;
- determine the first-hop destination of the datagram;
- format the datagram's header;
- pass the datagram to the appropriate lower-layer interface for transmission;
- provide any diagnostic or error reporting required.

3.2.5.3.2 Ensure Validity of User's Request

3.2.5.3.2.1 The network service user may specify the following parameters with an N-UNITDATA.request:

- Destination Extended End System Address;
- Source Extended End System Address;
- Internet Protocol Number;
- Source Timestamp;
- Basic QOS;
- Expanded QOS;
- N-SDU.

NOTE – This portion of the Recommendation does not specify the Application Program Interface (API) to the network services, so the exact parameters to a function call to invoke the network services may differ from these. For example, the API will most likely accept a pointer to the N-SDU and its length rather than the user data itself.

3.2.5.3.2.2 If the Source Extended End System Address is not specified, the SCPS-NP shall choose one for the user.

NOTE – The decision by a user to specify a Source Extended End System Address may have the (possibly intended) side effect of selecting the outbound interface over which the datagram is transmitted. Under most circumstances, users should allow the network service provider to choose the appropriate Source Extended End System Address.

3.2.5.3.2.3 The SCPS-NP shall perform address translation by

a) determining if the source and destination addresses appear in the address translation tables (refer to 4.3.1.8) and if so replacing the source and destination addresses with the translated address(es);

b) selecting the SCPS-NP TP-ID that corresponds to the Internet Protocol Number supplied by the user per table 3-3.

3.2.5.3.2.4 If a Basic QOS parameter is supplied,

a) the SCPS-NP shall check to ensure that the requested routing is supported on this system and if not return an error to the network service user and discard the datagram;

b) if the Basic QOS service is not supported by this implementation of the SCPS-NP (refer to the Protocol Implementation Conformance Statement, the proforma for which appears in annex C), the SCPS-NP shall return an error and discard the datagram;

c) if the precedence requested is not supported or not available to the particular network service user, the SCPS-NP shall return an error and discard the datagram.

3.2.5.3.2.5 If a hop count parameter is supplied, the SCPS-NP shall check to ensure that the value of the hop count parameter is less than 255 and if not return an error and discard the datagram.

3.2.5.3.2.6 If a Source Timestamp is supplied by the network service user, the SCPS-NP shall check to ensure that the identified format is supported by the network service and that the supplied timestamp conforms to that format:

a) the format check shall consist of a verification that the asserted length of the timestamp and the actual length of the timestamp are consistent;

b) if the user-requested format of the timestamp is not supported by this implementation of the SCPS-NP (refer to the Protocol Implementation Conformance Statement, the

proforma for which appears in annex C), the SCPS-NP shall return an error and discard the datagram;

c) if the format of the timestamp is inconsistent with the stated format, the SCPS-NP shall return an error and discard the datagram.

NOTE – These checks are on information supplied to the network service by the network service user. The interface to the network service, which is implementation-dependent, must supply sufficient information to perform the format tests identified in this paragraph.

3.2.5.3.2.7 If an Expanded QOS parameter is supplied,

a) the SCPS-NP shall check to ensure that its length is consistent with the length specified in RFC 2474 (one octet—see reference [1]) and if not return an error and discard the datagram;

b) if the Expanded QOS service is not supported by this implementation of the SCPS-NP (refer to the Protocol Implementation Conformance Statement, the proforma for which appears in annex C), the SCPS-NP shall return an error and discard the datagram;

c) no checks of the content shall be performed.

3.2.5.3.2.8 If the length of the N-SDU is greater than the maximum user data length supported on this system, the SCPS-NP shall return an error and discard the datagram.

3.2.5.3.3 Determine First-Hop Destination(s)

3.2.5.3.3.1 Routing Tables

The SCPS-NP protocol shall use the information from locally maintained routing tables to select a first-hop destination for the datagram.

NOTE – The means of maintaining the currency of the routing tables is discussed in 3.2.6. A routing-table entry specifies a routing structure or list of structures, each associated with a selected route and containing information necessary for appropriate header formatting (e.g., whether to use a header checksum). Refer to 4.3 for more information regarding the content of routing entries.

3.2.5.3.3.2 Unicast Transmission

3.2.5.3.3.2.1 If the translated address is of type Basic End System, Extended End System, or IPv6, then the SCPS-NP shall determine in an address-format-specific manner whether the address is a unicast or a multicast address:

a) if the address is a multicast address, the specifications of 3.2.5.3.3.3 shall apply;

b) if the address is a unicast address, the SCPS-NP shall

   1) consult the npESRouteTable to identify the appropriate route for the datagram;

   2) compare the Destination Address to the routing table entries in the manner specified in 3.2.6.1 in order to select a route.

3.2.5.3.3.2.2 If the translated address specifies a Path Address, the SCPS-NP shall

a) consult the npPathRouteTable to identify the appropriate route for the datagram;

b) compare the Path Address to the routing table entries in the manner specified in 3.2.6.1 in order to select a route.

3.2.5.3.3.3 Multicast Transmission

If the translated address specifies a multicast Destination End System Address along with the Source End System Address, the SCPS-NP shall

a) examine the multicast routing table for the entry corresponding to this Destination Address;

b) compare the Destination Address to the routing table entries in the manner specified in 3.2.6.1 in order to select a route.

3.2.5.3.3.4 Broadcast Transmission

3.2.5.3.3.4.1 If the translated address specifies a broadcast address, then the SCPS-NP shall send the datagram according to the rules for propagating broadcast transmissions (refer to 3.1.2).

3.2.5.3.3.4.2 If the network supports flood routing, it may be used as a means of suppressing duplication of broadcast datagrams. The rules for propagating broadcast transmissions specified in 3.1.2 still apply.

3.2.5.3.3.5 Flood Routing

3.2.5.3.3.5.1 If the network service user specifies flood routing, then the SCPS-NP shall send the datagram over all local link interfaces.

3.2.5.3.3.5.2 Flood routed datagrams shall be accompanied by a source timestamp:

a) the source address and timestamp shall be entered into a locally maintained flood routing table for subsequent routing loop control;

b) datagrams shall not be flood routed from a particular SCPS-NP Source Address at a rate that exceeds once per source timestamp tick;

NOTE – This plus time-to-live enforcement ensures that flood routed datagrams can be identified by routers and duplicates can be suppressed.

c) if there are entries in the flood routing table, the flood routing table shall be scanned at a locally determined interval not to exceed once per 128 seconds:

1) the timestamps shall be compared with the current time and the time-to-live value to determine whether the datagram no longer exists in the network;

2) if the datagram no longer exists in the network, the entry in the flood routing table shall be removed.

3.2.5.3.3.6 Identify Route-specific Information Affecting Datagram Formatting

The input to 3.2.5.3.4 shall be the minimum MTU from the routes and route-specific header formatting requirements (such as a requirement for header checksums).

3.2.5.3.3.7 Identify Route-specific Information Affecting Lower-Layer Transmission

The input to 3.2.5.3.5 shall be the formatted datagram and a (unique) list of routes, specifying the link-layer interface, possibly link-specific destination, and Maximum Transmission Unit (MTU) for each route.

3.2.5.3.4 Format Outgoing Datagram

NOTE – The information required to construct the protocol header is completely specified once the determination of first-hop destination has been made. (Recall that some protocol capabilities, specifically, routing loop control and header error detection, depend on the characteristics of the communication environment. The routing tables contain information regarding whether these capabilities are required for a particular route. This information is associated with the routes through configuration or network management. In addition, the routes maintain the MTU size for that route. The size of the N-SDU is checked to ensure that it will fit. This check is performed after the header size is calculated.)

3.2.5.3.4.1 The header formatting rules described in 3.2.2 shall be invoked to create the SCPS-NP header, which is appended at the beginning of the N-SDU.

3.2.5.3.4.2 Once the length of the SCPS-NP header has been calculated, a final check of the SCPS-NP PDU size versus the route's MTU shall be performed.

3.2.5.3.4.3 If the SCPS-NP PDU is too large, a route-specific error shall be returned to the network service user and the datagram shall be discarded.

3.2.5.3.5 Submit Datagram to Lower Layer for Transmission

NOTE – The result of determining the first-hop destination(s) for the datagram is a reference to a routing structure as defined in 4.3. Each route contains, at a minimum, the lower-layer interface over which the datagram should be transmitted. Depending upon the characteristics of the particular subnetwork, the route may also specify a subnetwork-specific destination and a means of mapping SCPS Network QOS parameters to subnetwork-specific QOS parameters (e.g., precedence). The availability and operation of these mappings are implementation dependent and subnetwork dependent.

For each next-hop destination, the SCPS-NP datagram shall be submitted to the subnetwork-specific transmission procedure, along with the subnetwork-specific destination address, if available, and the subnetwork-specific QOS parameters.

3.2.5.3.6 Perform Diagnostic and Error Processing

The SCPS-NP entity shall update the appropriate MIB statistics in accordance with the actions taken. The relevant MIB statistics are listed below:

- npOutRequests—the total number of datagrams supplied to SCPS-NP by local upper-layer protocols (including SCMP), not including forwarded datagrams;

- npOutDiscards—the number of output SCPS-NP datagrams for which no problem was encountered to prevent their transmission, but which were discarded (e.g., for purposes of congestion control);

- npOutNoRoutes—the number of SCPS-NP datagrams discarded because no route could be found to transmit them to their destination.

NOTE – Refer to section 4 for more details on SCPS-NP MIB contents.

3.2.5.4 Datagram Receipt Procedures

3.2.5.4.1 Overview

To receive a SCPS-NP datagram, a system must perform five distinct actions:

- acquire the lower-layer data;
- verify that the datagram's format is valid;
- determine whether the local system is the destination of the datagram;
- deliver the datagram to the appropriate transport protocol;
- provide any diagnostic or error reporting required.

3.2.5.4.2 Acquire Lower-Layer Data

3.2.5.4.2.1 The SCPS-NP shall acquire the lower-layer data via the SN-UNITDATA.indication primitive (refer to annex D).

NOTES

1 The SN-UNITDATA.indication primitive specifies a conceptual service, and the actual interface to that service may depend on the local subnetwork interface implementation.

2 The SN-UNITDATA.indication primitive returns an identifier for the local lower-layer interface that received the data.

3.2.5.4.2.2 The interface identifier returned by The SN-UNITDATA.indication primitive shall be used in subsequent routing decisions and must remain associated with the datagram until those routing decisions are made.

3.2.5.4.3 Verify Datagram Format

The SCPS-NP must verify that the format of the incoming datagram is correct.

NOTE – The elements of the format verification activity are described in 3.2.4.

3.2.5.4.4 Determine Whether the Datagram Is to Be Delivered Locally

3.2.5.4.4.1 When a SCPS-NP router receives a SCPS-NP datagram, it must decide whether the datagram should be delivered locally, forwarded, or both.

NOTE – There are cases in which the datagram should be both delivered locally and forwarded (for example, multicast datagrams, flood routed datagrams, broadcast datagrams, and datagrams marked for intermediate delivery).

3.2.5.4.4.2 The datagram shall be delivered locally and shall not be considered for forwarding in the following cases:

– the datagram's destination address exactly matches one of the recipient's SCPS-NP addresses;

– the datagram has been broadcast and there are no local logical interfaces other than the one on which the datagram was received;

NOTES

1 A logical interface differs from a physical interface. For example, a spacecraft may maintain many logical interfaces to nearby spacecraft that are all multiplexed over a single physical interface to a steerable transmit antenna.

2 A flood-routed datagram may be delivered locally more than once. This is to accommodate the case in which an error not detected by the network or lower layers is detectable by the network service user.

– the datagram's destination address is a multicast address with one or more local subscribers associated with the physical interface over which the datagram was received, and there are no other local logical interfaces than the one on which the datagram was received.

3.2.5.4.4.3 The datagram shall be delivered locally and shall be considered for forwarding in the following cases:

– the datagram's destination address does not match any of the router's SCPS-NP addresses, but the intermediate delivery flag is set to '1';

– the datagram has been broadcast to a *net-directed broadcast address* or to a *subnet-directed broadcast address* that matches the local host's network and subnetwork address;

– the datagram's destination address is a multicast address with one or more local subscribers associated with the physical interface on which the datagram was received.

3.2.5.4.4.4 For systems not configured as routers, the local-delivery clauses above shall apply but the datagrams shall not be forwarded.

3.2.5.4.5 Deliver to Appropriate Transport Protocol

3.2.5.4.5.1 The datagram shall be placed in the receive queue associated with the transport protocol indicated by the TP-ID:

a) if multiple queues are used for providing precedence service, the datagrams shall be entered in the queue in a First In, First Out (FIFO) manner;

b) if a single, sorted queue is used to provide precedence-based delivery, the datagram shall be inserted in the queue just ahead of the datagram with the next lower precedence (or at the end of the queue, if no lower-precedence datagrams are in queue).

3.2.5.4.5.2 If the transport protocol indicated by the TP-ID does not exist on the local system:

a) the system shall increment the MIB statistic ipInUnknownProtos;

b) the system **may** generate an SCMP Destination Unreachable error message and return it to the source of the datagram;

c) the system shall discard the datagram.

3.2.5.4.5.3 The SCPS-NP shall perform address translation by

a) determining if the address(es) that appear in the datagram header correspond to addresses for which address translation is performed and if so replacing the address(es) from the datagram with the Source and Destination Extended End System addresses resulting from the translation (refer to 4.1.3.8);

b) selecting the Internet Protocol Number that corresponds to the SCPS-NP TP-ID per table 3-3.

3.2.5.4.6 Perform Diagnostic and Error Processing

The SCPS-NP entity shall update the appropriate MIB statistics in accordance with the actions taken. The relevant MIB statistics are listed below:

– npInReceives—the total number of input datagrams received from interfaces, including those received with errors;

– npInBadLength—the total number of input datagrams discarded because of problems with the length indicator;

– npInBadVersion—the total number of input datagrams discarded because of problems with the version/protocol indicator;

– npInBadAddress—the total number of input datagrams discarded because of header format problems with the addresses;

– npInBadChecksum—the total number of input datagrams discarded because of header checksum failure;

– npInAddrErrors—the total number of input datagrams discarded because of an invalid destination address (for systems not configured as routers, this includes any datagrams received with a destination address other than one of the local addresses);

– npInUnknownProtos—the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol;

– npInDiscards—the number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., because of local congestion);

– npInDelivers—the number of input datagrams successfully delivered to SCPS-NP user protocols.

NOTE – Refer to section 4 for more details on SCPS-NP MIB contents.

3.2.5.5 Datagram Forwarding Procedures

NOTE – The process of datagram forwarding is similar to the first portions of datagram receipt and to the final portions of datagram transmission. Between the two are two aspects unique to forwarding: routing loop control and determining the next-hop address(es). These procedures are invoked only when the SCPS-NP entity is configured as a router, indicated by the npForwarding MIB parameter's being set to the value forwarding (1).

3.2.5.5.1 Acquire Lower-Layer Data

Lower-layer data shall be acquired as in 3.2.5.4.2.

3.2.5.5.2 Verify Datagram Format

Datagram format shall be verified as in 3.2.5.4.3.

3.2.5.5.3 Make Local Delivery and Forwarding Decisions

Local delivery and forwarding decisions shall be made as in 3.2.5.4.4, except that for all cases not covered by 3.2.5.4.4, the datagram shall be considered for forwarding.

3.2.5.5.4 Perform Any Required Routing Loop Control Processing

For those datagrams considered for forwarding, the following actions shall be performed:

a) If there is a hop count present in the datagram, the hop count shall be decremented:

1) if the hop count has reached zero (or less), the forwarding system shall:

   – discard the datagram,
   – increment the npForwHopDiscard MIB statistic,
   – send an SCMP Time Exceeded message to the source;

2) if the hop count has not reached zero, the forwarding system shall recompute the header checksum.

b) If no hop count is present, a timestamp is present, and the network is configured such that system clocks are synchronized throughout the network, the forwarding system shall:

   1) add the MIB value npTimeToLivePField1 or npTimeToLivePfield2, as appropriate, to the timestamp and compare the sum to the current time;

   2) if the sum is less than the current time, indicating the datagram's lifetime has expired, the forwarding system shall

      – discard the datagram,
      – increment the npForwTTLDiscard MIB statistic,
      – send an SCMP Time Exceeded message to the source.

c) If the Basic QOS field is present and indicates that the datagram is to be flood routed, the forwarding system shall scan the flood routing table to determine whether the source address and timestamp are present:

   1) if source address and timestamp are present, the forwarding system shall discard the datagram;

   2) if source address and timestamp are not present, the forwarding system shall enter them.

d) The forwarding system shall queue for forwarding all datagrams that are not discarded.

3.2.5.5.5 Determine Next-Hop Address(es)

Next-hop address(es) shall be determined as in 3.2.5.3.3.

3.2.5.5.6 Submit Datagram to Link Layer for Transmission

3.2.5.5.6.1 The datagram shall not be forwarded over the interface from which it was received unless the router determines that a better route exists, forwards the datagram to its appropriate next hop, and sends an SCMP Redirect message to the source informing it of the proper next hop address.

3.2.5.5.6.2 The interface identifier recorded in 3.2.5.4.2 shall be compared to the list of first-hop addresses determined in 3.2.5.5.5 and removed from the list, if present.

3.2.5.5.6.3 The datagram shall be submitted to the link layer for transmission as specified in 3.2.5.3.5.

3.2.5.5.7 Perform Diagnostic and Error Processing

3.2.5.5.7.1 The SCPS-NP entity shall update the appropriate MIB statistics in accordance with the actions taken. The relevant MIB statistics are listed below:

- npOutRequests—as above;
- npOutDiscards—as above;
- npOutNoRoutes—as above;
- npInReceives—as above;
- npInBadLength—as above;
- npInBadVersion—as above;
- npInBadAddress—as above;
- npInBadChecksum—as above;
- npInAddrErrors—as above;
- npInUnknownProtos—as above;
- npInDiscards—as above;
- npInDelivers—as above;
- npForwHopDiscard—the number of datagrams that were discarded before being queued for forwarding because the hop count had reached zero (or less);
- npForwTTLDiscard—the number of datagrams that were discarded before being queued for forwarding because the elapsed time in transit had exceeded the npTimeToLive value;
- npForwDatagrams—the number of input datagrams which were queued for forwarding.

3.2.6 SUPPORTING PROCEDURES

3.2.6.1 Routing Procedures

3.2.6.1.1 Overview

NOTE – The Routing Procedures describe the process by which an end system routes a SCPS-NP datagram. Routers may exchange state information among each other for the purpose of building locally maintained routing tables. There are several possible methods to maintain state between routers: static configuration, remote configuration via network management, program-specific routing state exchange, or program-independent routing state exchange. Subsection 4.3 defines the entries in the routing databases that support maintenance of this information.

3.2.6.1.1.1 Routing tables shall be kept for

- End System Addresses;
- Path Addresses;
- Multicast End System Addresses.

3.2.6.1.1.2 A router manufacturer **must** state which routing tables and routing methods are supported by an implementation of this specification.

NOTES

1 Annex C identifies the minimum routing requirements and the format for stating which routing capabilities are supported.

2 Throughout this subsection, specific routing algorithms will not be required, though specific functionality may be. For the exchange of routing information that affects interoperability between programs and administrative authorities, network management means may be used to transfer relevant portions of routing database entries. Refer to 4.3 for the interface requirements between the routing tables and the MIB.

3.2.6.1.1.3 Routing tables shall be searched to attempt to match the address that accompanies a datagram (either the destination address, in the case of end-system addressing and multicast end-system addressing, or the path address, in the case of path addressing):

a) an address shall be considered to match a routing table entry if the address, when logically ANDed with the npRouteNetmask of that routing table entry, is equal to the npRouteDest of that routing table entry logically ANDed with the npRouteNetmask;

b) if multiple entries in the routing table match the address, the route that has the most bits set to ‘1’ in the npRouteNetmask is the route that shall be selected;

c) if multiple routing table entries tie with the maximum number of bits set to ‘1’ in their respective npRouteNetmask entries, one of these entries shall be selected using locally defined criteria;

d) An npRouteNetmask with all bits set to ‘0’ will match any destination address and shall be used to specify a default route.

3.2.6.1.2 End System Routing

3.2.6.1.2.1 If the translated address specifies a destination address and that address is not a multicast address, then the npESRouteTable shall be consulted to identify the next hop destination for the datagram.

3.2.6.1.2.2 The system shall select the single routing table entry that best matches the destination address according the criteria specified in 3.2.6.1.1.3.

3.2.6.1.2.3 The system shall forward the datagram to the address specified in the npRouteNextHop parameter of the selected routing table entry.

3.2.6.1.3 Path Routing

3.2.6.1.3.1 If the translated address specifies a path address, then the npPathRoute table shall be consulted to identify the next hop destination(s) for the datagram.

3.2.6.1.3.2 The system shall select the single routing table entry that best matches the destination address according the criteria specified in 3.2.6.1.1.3.

3.2.6.1.3.3 The system shall forward the datagram to all addresses specified in the sequence of npRouteNextHop parameter of the selected routing table entry.

3.2.6.1.4 Multicast Routing

3.2.6.1.4.1 If the translated address specifies a destination address and that address is a multicast address, then the npMCRouteTable shall be consulted to identify the next hop destination for the datagram.

3.2.6.1.4.2 The system shall select the single routing table entry that best matches the destination address according to the criteria specified in 3.2.6.1.1.3.

3.2.6.1.4.3 The system shall forward the datagram to all addresses specified in the sequence of npRouteNextHop parameter of the selected routing table entry.

3.2.6.1.5 Flood Routing

NOTE – Flood routing uses datagram replication to send many copies of a datagram through the network to one or more final destinations. The flood routing technique used in the SCPS Network uses a ‘serial number’ created from the source address and the source timestamp to identify and suppress duplicates.

3.2.6.1.5.1 When an end system originates, rather than forwards, a flood-routed datagram, it shall transmit the datagram over all local interfaces (consistent with any broadcast addressing restrictions specified in 3.1.2) and shall enter the serial number of the datagram into the flood routing table.

3.2.6.1.5.2 When an end-system or router receives a flood routed datagram, it shall determine whether the datagram should be delivered locally (based on the address) and deliver it if required.

3.2.6.1.5.3 If the system receiving the flood-routed datagram is configured as a router (that is, the system is configured to forward datagrams), the router shall scan the flood routing table to determine if the serial number of the received datagram is present:

a) if the serial number is present, indicating the datagram has been forwarded by this system before, the datagram shall be silently discarded;

b) if the serial number is not in the table, the router shall enter it and forward the datagram over all local interfaces except the one over which it was received.

3.2.6.1.5.4 If there are any entries in the flood routing table, then the table shall be scanned no less frequently than once per 128 seconds to determine if entries are old and, if so, remove them from the table.

NOTES

1 The serial number of a flood-routed datagram includes a timestamp. The format of that timestamp specifies the period of time before the timestamp value 'wraps' (becomes ambiguous). The minimum-period CUC timestamp wraps after 256 seconds.

2 An entry is old if the timestamp in the serial number indicates that the datagram is older than the maximum time-to-live entry in the MIB. If this is the case, the routing loop control software will prevent forwarding of the datagram, removing it from the network. As a result, the entry may be removed from the flood routing table. It is important to remove old entries from the routing loop table before the timestamp 'wraps' and a new flood routed datagram is mistaken for an old one.

3 The actual scan rate supported by a system will depend on the rate at which flood routed traffic arrives and the amount of memory that can be devoted to the table.

3.2.6.2 Precedence Procedures

NOTE – Precedence is a method of placing relative importance to each datagram, and using that relative importance to affect the delivery order of the network traffic.

3.2.6.2.1 Default Precedence

If the precedence of a datagram is not explicit, then the default value defined in the MIB parameter npDefaultPrecedence (see 4.1.3.3) shall be used for the datagram.

3.2.6.2.2 Order of Datagram Processing

3.2.6.2.2.1 Datagrams shall be processed in the order of highest precedence to lowest precedence.

3.2.6.2.2.2 If separate queues exist for each precedence level:

a) if a higher-level queue contains datagrams, that queue shall be serviced before any lower-precedence queue;

b) only after all higher-precedence datagrams have been serviced and their queues emptied shall a lower-precedence queue begin service.

3.2.6.2.2.3 Preemptive processing is not supported:

a) a higher-precedence datagram that arrives after a lower-level datagram has begun service must wait until the latter completes processing;

b) all queues shall then be re-examined and the order of processing shall resume as normal, highest to lowest.

3.2.6.2.3 Congestion Control Procedures

3.2.6.2.3.1 If congestion exists, then precedence-based queues shall be purged (emptied to the extent necessary to alleviate the congestion):

a) congestion is defined to exist when buffers fill to a certain percentage of their capacity;

b) congestion shall be monitored separately for inbound and outbound queues.

3.2.6.2.3.2 For inbound queues:

a) the congestion threshold shall be specified by the MIB parameter npInCongThreshold;

b) when the inbound congestion threshold is reached, inbound queues shall be purged starting with the lowest-precedence queue and proceeding in order to the highest-precedence queue;

c) inbound queues shall be purged until the buffer use is reduced to the percent of capacity specified by the MIB parameter npInCongPurgeExtent.

NOTE – The order of datagram purging within a given precedence level is a local issue.

3.2.6.2.3.3 For outbound queues:

a) the congestion threshold shall be specified by the MIB parameter npOutCongThreshold;

b) when the outbound congestion threshold is reached, outbound queues shall be purged starting with the lowest-precedence queue and proceeding in order to the highest-precedence queue;

c) outbound queues shall be purged until the buffer use is reduced to the percent of capacity specified by the MIB parameter npOutCongPurgeExtent.

3.2.6.3 Multihoming

The following requirements apply to the selection of a SCPS-NP source address for sending a datagram from a multihomed system:

a) if the datagram is sent to a path address, no source address shall be used;

b) if the datagram is sent in response to a received datagram, the source address for the response **should** be the SCPS-NP address of the interface over which the datagram was received (in the format that matches the received datagram's address format);

c) an application **must** be able to specify explicitly the source address for an outgoing datagram;

d) in the absence of an application's specifying a source address, the source address shall be chosen based on the information in the routing tables and the local-address table (npAddrTable).

3.3 SCPS CONTROL MESSAGE PROTOCOL SPECIFICATION

3.3.1 GENERAL

3.3.1.1 SCMP messages shall be used to convey information regarding errors or changes in network conditions between network entities.

3.3.1.2 SCMP messages shall be located in the data field of the SCPS-NP datagram and shall consist of a SCMP message header followed by, if required by the message type, a message-specific data field.

3.3.1.3 The TP-ID field of the SCPS-NP header shall be set to '1' for SCMP.

3.3.1.4 The Source Timestamp shall be supplied in either the 24-bit CUC or the 32-bit binary Timestamp Format, at the option of the implementer.

3.3.1.5 The Basic QOS parameter subfields shall contain values as follows:

a) the precedence level of SCMP error messages shall be set to the precedence level assigned to network control,[1] with the exception of the Source Quench message (see 3.3.4.2);

b) Routing Requirements subfield shall be set to '00' for 'point to point';

c) Program Specific subfield shall be set to '00'.

3.3.1.6 The Expanded QOS shall not be used.

3.3.2 SCMP MESSAGE HEADER

3.3.2.1 The SCMP message header shall be four octets in length and shall contain the following fields in the following sequence:

	Length in octets
– Message Type (mandatory)	1
– Message Code (mandatory)	1
– Checksum (mandatory)	2

3.3.2.2 The general format for SCMP messages is shown in figure 3-4. Note that SCMP messages appear as the N-SDU (i.e., the user data) within a SCPS-NP packet.

3.3.2.3 The checksum algorithm used is the same as that specified in 3.2.3.10, but applied to the SCMP message, rather than the SCPS-NP header.

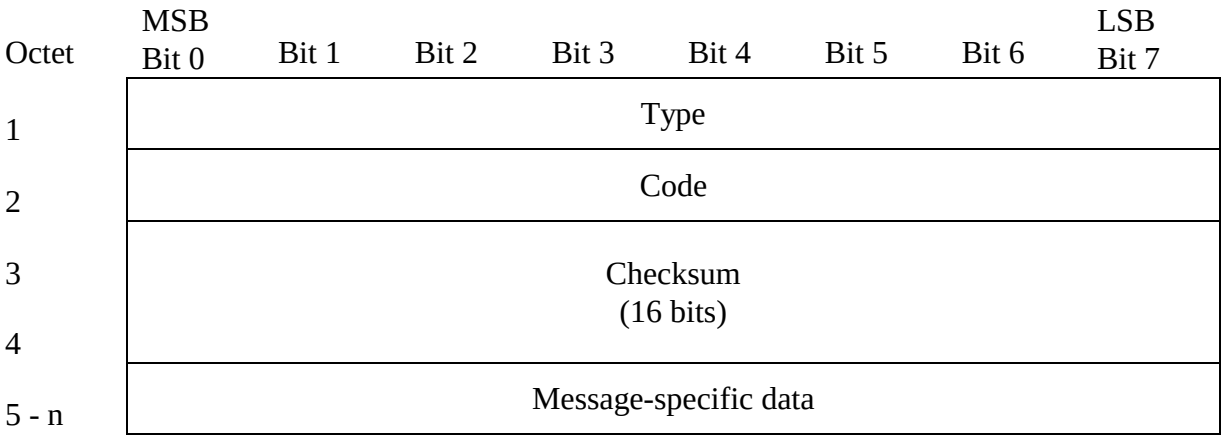


Figure 3-4: SCPS Control Message Protocol Header Format

[1] The precedence level assigned to Network Control is not specified in this document. Rather, it should be established as a result of overall system design considerations.

3.3.3 SCMP HEADER FIELDS

3.3.3.1 Message Type Field

3.3.3.1.1 The Message Type field shall be eight bits in length and shall occupy the first octet of the SCMP header.

3.3.3.1.2 The Message Type field shall contain a value corresponding to one of the Type values defined in table 3-9.

Table 3-9: SCMP Message Types

Type Value	Message	Kind
0	Echo Reply	Query
3	Destination Unreachable	Error
4	Source Quench	Error
5	Redirect	Error
8	Echo Request	Query
11	Time Exceeded	Error
12	Parameter Problem	Error
19	Corruption Experienced	Error

3.3.3.2 Message Code Field

3.3.3.2.1 The Message Code field shall be eight bits in length and shall occupy the second octet of the SCMP header.

3.3.3.2.2 The Message Code field shall contain a value selected from the list of permitted values for a given SCMP Message Type (see 3.3.4).

3.3.4 SCMP MESSAGE TYPES

3.3.4.1 Destination Unreachable Message

NOTE – The decision to send Destination Unreachable messages is local. Routers **may** send such messages, but are not required to if doing so would adversely affect the operation of the router.

3.3.4.1.1 The destination address of the message shall be the source address of the original datagram.

3.3.4.1.2 The message type shall be 3.

3.3.4.1.3 The message code shall be chosen according to the list in table 3-10 to most closely match the reason the message is being generated.

Table 3-10: Destination Unreachable Message Codes

Code	Meaning	When Generated
0	network unreachable	generated by a router if forwarding path (route) to the destination network is not available
1	host unreachable	generated by a router if a forwarding path (route) to a destination host on a directly connected network is not available
2	protocol unreachable	generated if the transport protocol designated in the SCPS-NP header is not supported in the transport layer of the destination host
3	port unreachable	generated if the designated transport protocol is unable to demultiplex the datagram in the transport layer of the final destination, but has no protocol mechanism to inform the sender (e.g., UDP)
4	datagram too large for subnetwork	generated if the size of the datagram is larger than the MTU of the route to the destination
5	reserved	
6	reserved	
7	destination host unknown	generated only when a router can determine (from link-layer information) that the destination host does not exist
8	reserved	
9	reserved	
10	reserved	
11	destination network unreachable for QOS	generated by a router if a forwarding path (route) to the destination network with the requested or default QOS is not available
12	destination host unreachable for QOS	generated by a router if it cannot forward a datagram because its route(s) to the destination do not match the QOS requested in the datagram or the default QOS
13	communication admin-istratively prohibited	generated if a router cannot forward a datagram because of administrative filtering
14	host precedence violation	generated to indicate that a requested precedence is not permitted for the particular combination of source/destination host or network, upper-layer protocol, and source/destination port
15	precedence cutoff in effect	generated if network administrators or congestion control procedures have imposed a minimum level of precedence required for operation and the datagram was sent with a precedence below this level
16	link outage	generated to indicate that a link has transitioned or will transition in the immediate future from the ‘up’ to the ‘down’ state

NOTE – Routers may have configuration options that cause codes 13, 14, and/or 15 messages not to be generated. When these options, if present, are enabled, no SCMP error message is sent in response to a datagram that is dropped because of the stated conditions.

3.3.4.1.4 Message-specific data of the general message format

a) shall be a one-octet length indicator followed by the SCPS-NP header of the datagram that resulted in the issuance of the SCMP message;

b) the first several octets (typically eight) of the data of the original SCPS-NP datagram may be included;

c) the length indicator shall specify the length of the message-specific data, in octets, including the one-octet length indicator itself.

NOTE – Inclusion of the original datagram's data is a local option and is intended to support those applications that do not require encryption (thus ensuring that the data is intelligible to the SCMP).

3.3.4.2 Source Quench Message

3.3.4.2.1 The Source Quench message shall be used to indicate that a router has reached or is reaching a state of congestion.

3.3.4.2.2 The destination address of the message shall be the source address of the original datagram; if the original datagram contained a Path address, the Path Address Translation Table (refer to 4.1.3.8.3) shall be consulted to determine the source address.

3.3.4.2.3 The message type shall be 4.

3.3.4.2.4 The message code shall be 0.

3.3.4.2.5 Message-specific data of the general message format shall be a one-octet length indicator followed by the SCPS-NP header of the datagram that resulted in the issuance of the SCMP message; the first several octets (typically eight) of the data of the original SCPS-NP datagram may be included.

3.3.4.2.6 The Source Quench message shall be generated in accordance with the rate-limiting procedures described in 3.3.5.2 when a SCPS-NP router is forced to invoke congestion-control procedures such as precedence-based queue purges.

3.3.4.2.7 If the system generating the Source Quench message supports the Basic Quality of Service capability, the Source Quench message shall be sent with the precedence level set to the same value as the precedence level of the datagram that provoked the sending of the Source Quench message.

3.3.4.3 Redirect Message

3.3.4.3.1 The SCMP Redirect message shall be used to inform an end system that the router used by that system to route certain datagrams should be changed.

3.3.4.3.2 The destination address of the message shall be the source address of the original datagram; if the original datagram contained a Path address, the Path Address Translation Table (refer to 4.1.3.8.3) shall be consulted to determine the source address.

3.3.4.3.3 The message type shall be 5.

3.3.4.3.4 The message code shall be one of the following:

0 Reserved;
1 Redirect datagrams for the host;
2 Reserved;
3 Redirect datagrams for the QOS and Host;
4 Previously unavailable link now available.

3.3.4.3.5 The message-specific data of the general message format shall be, in sequence:

a) a one-octet address type indicator having one of the following values:

0 SCPS-NP End System Address;
1 SCPS-NP Extended End System Address;
2 IPv6 Address;

NOTE – Since SCPS-NP Path Addresses imply both source and destination addresses, they are not used in Redirect messages.

b) the SCPS-NP address of the new router;

c) a one-octet length indicator;

d) the SCPS-NP header of the datagram that resulted in the issuance of the SCMP message;

e) optionally, the first several octets (typically eight) of the data of the original SCPS-NP datagram.

3.3.4.3.6 A router **may** ignore SCMP Redirects when choosing a path for a datagram originated by the router if the router is running a routing protocol.

3.3.4.3.7 Routers shall be able to generate the Redirect for host messages.

3.3.4.3.8 Routers **should** be able to generate the Redirect for QOS and host messages.

3.3.4.3.9 Routers that are attached to links that are prone to scheduled or unscheduled outage **should** be able to generate the Redirect for link availability messages.

NOTES

1 It is acceptable that a router specify its own address in a Redirect for link availability message if the affected link becomes available without the need to change routers. (This may occur if a single ground station supports an orbiting system. The link outage is signaled with a destination-unreachable–link-outage message. When the orbiting system is reacquired, the link-reacquired message is sent to previous users of the link as indicated by a least-recently used queue maintained by the router.)

2 While the Redirect message is considered an error message, the Redirect for link availability message does not indicate an error condition.

3.3.4.4 Time Exceeded Message

3.3.4.4.1 The Time Exceeded message shall be used to indicate that a datagram was discarded before it reached its destination because the hop count (if present) was decremented to zero or the difference between the current time and the source timestamp exceeded the maximum time-to-live for the network.

3.3.4.4.2 The destination address of the message shall be the source address of the original datagram.

3.3.4.4.3 The message type shall be 11 (decimal).

3.3.4.4.4 The message code shall be 0.

3.3.4.4.5 Message-specific data of the general message format shall be a one-octet length indicator followed by the SCPS-NP header of the datagram that resulted in the issuance of the SCMP message; the first several octets (typically eight) of the data of the original SCPS-NP datagram may be included.

3.3.4.5 Parameter Problem Message

3.3.4.5.1 The Parameter Problem message shall be generated:

- when a router or the destination system detects a problem with the SCPS-NP header of the message that it was processing;
- for any other error not specifically covered by another SCMP message.

3.3.4.5.2 The destination address of the message shall be the source address of the original datagram; if the original datagram contained a Path address, the Path Address Translation Table (refer to 4.1.3.8.3) shall be consulted to determine the source address.

3.3.4.5.3 The message type shall be 12.

3.3.4.5.4 The message code shall be 0.

3.3.4.5.5 Message-specific data of the general message format shall be, in sequence:

- a one-octet pointer, which is an offset from the beginning of the SCPS-NP header to the octet where the error was detected;
- a one-octet length indicator;
- the SCPS-NP header of the datagram that resulted in the issuance of the SCMP message;
- optionally, the first several octets (typically eight) of the data of the original SCPS-NP datagram.

3.3.4.5.6 The Parameter Problem message shall be sent only if the detected error caused the datagram to be discarded.

3.3.4.6 Corruption Experienced Message

3.3.4.6.1 The Corruption Experienced message shall be used to indicate that an attached link has indicated to the router that a trend of corrupted datagrams has been detected. The means of determining that a trend of corrupted datagrams has been detected is link specific and implementation specific.

3.3.4.6.2 The destination addresses of the message shall be drawn from the most recent sources of data to cross the link (on the sending router side) and shall additionally include the SCPS-NP router at the other end of the corrupted link.

NOTES

1 The determination of what constitutes a 'recent' source of data is implementation specific and affects that amount of data that must be maintained and how it should be aged out.

2 The number of destinations that shall be informed via the Corruption Experienced message, and when those destinations shall be informed, is implementation dependent.

3 If the link is corrupted in both directions, the Corruption Experienced message will probably be damaged in transit to the router at the other end of the corrupted link. If this is the case, it is likely that the remote terminus is informing its sources that the link is corrupted independently of the router notification.

3.3.4.6.3 The message type shall be 19.

3.3.4.6.4 The message code shall be 0.

3.3.4.6.5 The Corruption Experienced Message shall carry as message-specific data a one-octet length indicator followed by the header of a datagram recently received from the system to which the Corruption Experienced message is being sent.

3.3.4.7 Echo and Echo Reply Messages

3.3.4.7.1 All systems supporting the SCPS-NP protocol shall implement an SCMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. A router must be prepared to receive and echo an SCMP Echo Request that is at least as large as the maximum MTU specified in its routing tables.

3.3.4.7.2 The Echo Request and Echo Reply messages shall be sent with a hop-count parameter in the SCPS-NP header. The initial value of the hop count is a local issue.

3.3.4.7.3 The type value shall be 8 for the Echo Request message and 0 for the Echo Reply message.

3.3.4.7.4 The code value for both shall be 0.

3.3.4.7.5 The message-specific portion of the Echo Request and Reply messages shall include

a) a two-octet identifier:

   – if the type is 8 (an Echo Request), the identifier shall be a number selected by the generator of the Echo Request to assist in identifying the reply;

   – if the type is 0 (an Echo Reply), the identifier shall be that specified by the request (the generator of the Echo Request may specify an identifier with value 0);

b) a two-octet sequence number:

   – if the type is 8 (an Echo Request), the sequence number shall be a number selected by the generator of the Echo Request to assist in identifying the reply;

   – if the type is 0 (an Echo Reply), the sequence number shall be that specified by the request (the generator of the Echo Request may specify a sequence number with value 0);

c) an Echo Reply message shall contain the following additional data in the message-specific data area:

   1) a one-octet field containing the hop-count parameter of the received Echo Request message;

   2) a one-octet field containing in its least significant two bits the timestamp format bits (bits 27 and 28) of the received Echo Request message;

   3) an eight-octet field containing the timestamp field of the received Echo Request message (if the timestamp field is less than eight octets in length, it shall be placed in the least-significant octets of the field and the unused octets shall be set to all ‘0s’);

   4) a four-octet field containing the MTU of the interface over which the Echo Request was received;

   5) a four-octet field containing the receive data rate in bits per second of the interface over which the Echo Request was received (if this information is unavailable to the SCMP, the field shall be set to all ‘0s’);

   6) any data supplied in the optional data field of the Echo Request, to the limit specified in 3.3.4.7.1.

3.3.4.7.6 The Echo server function **may** choose not to respond to SCMP Echo Requests addressed to SCPS-NP broadcast or multicast addresses.

3.3.4.7.7 All SCMP implementations **should** have a configuration option which, if enabled, causes SCMP to silently discard all SCMP Echo Requests. If provided, this option shall default to allowing echo responses (that is, the default value for the option to silently discard SCMP Echo Requests shall be ‘disabled’).

3.3.4.7.8 All SCMP implementations shall, for diagnostic purposes, implement a user/application-layer programming interface for sending an Echo Request and receiving an Echo Reply, and all SCMP Echo Reply messages received shall be passed to this interface.

3.3.4.7.9 The SCPS-NP source address in an SCMP Echo Reply shall be the same as the specific-destination address of the entity responding to the SCMP Echo Request message.

3.3.5 CONTROL MESSAGE GENERATION

3.3.5.1 Rules for Error Message Generation

3.3.5.1.1 An SCMP message shall **not** be sent as the result of receiving any of the following messages:

- an SCMP error message;
- a datagram that fails the SCPS-NP header validation tests described elsewhere in this document except where that subsection specifically permits the transmission of an SCMP error message;
- a datagram destined for a SCPS-NP broadcast or SCPS-NP multicast address;
- a datagram sent as a link-layer broadcast or multicast;
- a datagram with an invalid source address;
- a datagram that has been flood routed.

3.3.5.1.2 An SCMP error message shall **not** be sent in any case where this document states that a datagram is to be silently discarded.

3.3.5.2 Rate Limiting

3.3.5.2.1 All SCPS-NP routers shall have the ability to control the rate at which SCMP error messages are generated.

3.3.5.2.2 The rate-limit parameters shall be settable by administration personnel via an SCMP MIB entry.

NOTE – Separate rate limits are defined in the MIB for Source Quench messages (scmpSrcQuenchRate), for other SCMP error messages (scmpErrorRate), and for SCMP query messages (scmpQueryRate). Refer to 4.2 for the description of these limits. How rate limits are applied (e.g., per router or per individual interface) is an implementation decision.

4 MANAGEMENT INFORMATION BASE REQUIREMENTS[1]

4.1 MIB REQUIREMENTS FOR THE SCPS-NP

4.1.1 GENERAL

The MIB for systems implementing the SCPS-NP shall include, at a minimum, the following entries.

4.1.2 STATISTICS

4.1.2.1 Output Requests

The Output Requests parameter contains the total number of SCPS-NP datagrams supplied by local user-protocols (including SCMP) to SCPS-NP in requests for transmission. This counter does not include any datagrams counted in npForwDatagrams.

Name: npOutRequests
Syntax: Counter
NP Access: Write

4.1.2.2 Output Discards

The Output Discards parameter contains the total number of output SCPS-NP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., because of local congestion). This counter may include datagrams counted in npForwDatagrams if any such datagrams met the discretionary discard criterion.

Name: npOutDiscards
Syntax: Counter
NP Access: Write

4.1.2.3 No Outbound Routes

The No Outbound Routes parameter contains the number of SCPS-NP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any datagrams counted in npForwDatagrams that meet this ‘no-route’ criterion.

Name: npOutNoRoutes
Syntax: Counter
NP Access: Write

[1] The information in this section has been adapted from *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*, RFC 1213 (see reference [B13]).

4.1.2.4 Datagrams Received

The Datagrams Received parameter contains the total number of SCPS-NP datagrams received from interfaces, including those received with errors.

Name: npInReceives
Syntax: Counter
NP Access: Write

4.1.2.5 Received Length Errors

The Received Length Errors parameter contains the total number of input SCPS datagrams discarded because of problems with the length indicator.

Name: npInBadLength
Syntax: Counter
NP Access: Write

4.1.2.6 Received Version Errors

The Received Version Errors parameter contains the total number of input SCPS datagrams discarded because of problems with the version/protocol indicator.

Name: npInBadVersion
Syntax: Counter
NP Access: Write

4.1.2.7 Received Address Errors

The Received Address Errors parameter contains the total number of input datagrams discarded because of header format problems with the addresses.

Name: npInBadAddress
Syntax: Counter
NP Access: Write

4.1.2.8 Received Checksum Errors

The Received Checksum Errors parameter contains the total number of input datagrams discarded because of header checksum failure.

Name: npInBadChecksum
Syntax: Counter
NP Access: Write

4.1.2.9 Received Invalid Address Errors

The Received Invalid Address Errors parameter contains the total number of input datagrams discarded because of an invalid destination address. (For systems not configured as routers, this includes any datagrams received with a destination address other than one of the local addresses.)

Name: npInAddrErrors
Syntax: Counter
NP Access: Write

4.1.2.10 Inbound Unknown Protocols

The Inbound Unknown Protocols parameter contains the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Name: npInUnknownProtos
Syntax: Counter
NP Access: Write

4.1.2.11 Inbound Discards

The Inbound Discards parameter contains the number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., because of local congestion).

Name: npInDiscards
Syntax: Counter
NP Access: Write

4.1.2.12 Inbound Deliveries

The Inbound Deliveries parameter contains the number of input datagrams successfully delivered to SCPS-NP user protocols.

Name: npInDelivers
Syntax: Counter
NP Access: Write

4.1.2.13 Forwarded Datagrams

The Forwarded Datagrams parameter contains the number of input datagrams that were queued for forwarding.

Name: npForwDatagrams
Syntax: Counter
NP Access: Write

4.1.2.14 Hop Count Exceeded

The Hop Count Exceeded parameter contains the number of datagrams that were discarded before being queued for forwarding because the hop count had reached zero (or less).

Name: npForwHopDiscard
Syntax: Counter
NP Access: Write

4.1.2.15 Time To Live Exceeded

The Time To Live Exceeded parameter contains the number of datagrams that were discarded before being queued for forwarding because the elapsed time in transit had exceeded the npTimeToLive value.

Name: npForwTTLDiscard
Syntax: Counter
NP Access: Write

4.1.3 CONFIGURATION PARAMETERS

4.1.3.1 Time To Live

The Time To Live parameter contains the time, in whole seconds, that a datagram is permitted to exist while in transit in the SCPS Network. For the CUC 24-bit Timestamp Format with Implicit P-Field, the npTimeToLivePField1 is used; for all other timestamp formats, npTimeToLivePField2 is used.

Name: npTimeToLivePField1
Syntax: Integer (0..255)
NP Access: Read Only

Name: npTimeToLivePField2
Syntax: Integer (0..2^{32}-1)
NP Access: Read Only

4.1.3.2 Default Maximum Hops

The Default Maximum Hops parameter contains the default for the maximum number of intermediate systems that a SCPS-NP datagram may encounter before being discarded.

Name: npDefaultHopCount
Syntax: Integer
NP Access: Read Only

4.1.3.3 Default Precedence

The Default Precedence parameter contains the default value for the precedence level to be assigned to a SCPS-NP datagram upon its creation if the network service user does not explicitly specify a precedence level.

Name: npDefaultPrecedence
Syntax: Integer (0..15)
NP Access: Read Only

4.1.3.4 Congestion Thresholds

The Congestion Thresholds define the percent of used buffer capacity at which precedence-based queue purging is invoked and the extent to which the queues are emptied as a result of the purge. The invocation threshold shall be greater than the extent value. Separate threshold/extent pairs are maintained for input and output buffers. The values are expressed as a percent of total buffer capacity.

Name: npInCongThreshold
Syntax: Integer (0..100)
NP Access: Read Only

Name: npInCongPurgeExtent
Syntax: Integer (0..100)
NP Access: Read Only

Name: npOutCongThreshold
Syntax: Integer (0..100)
NP Access: Read Only

Name: npOutCongPurgeExtent
Syntax: Integer (0..100)
NP Access: Read Only

4.1.3.5 End System or Router Configuration

The End System or Router Configuration parameter contains the indication of whether this entity is acting as a SCPS-NP router with respect to the forwarding of datagrams received by, but not addressed to, this entity.

Name: npForwarding
Syntax: Integer {
not-forwarding (0),
forwarding (1)
}
NP Access: Read Only

4.1.3.6 SCPS Network Address Representation

The SCPS-NP Address type specifies the syntax of a SCPS-NP Address and is used in several MIB entries. The SCPS-NP Address type does not, in itself, define a MIB entry. The syntax shall consist of an element that specifies the address type and an octet array that contains the address value. The octet array shall be sized to contain the maximum-sized SCPS-NP addresses defined (that is, IPv6 addresses). Addresses shorter than the maximum size shall begin at array index 0. Addresses shall be stored in network byte order.

```
Name:       SCPS-NP Address
Syntax:     sequence of {
                npAddrType,
                npAddrValue
            }

Name:       npAddrType
Syntax:     Integer {
                Null (0),
                Basic Path (1),
                Extended Path (2),
                Basic End System (3),
                Extended End System (4),
                IPv6 (5)
            }

Name:       npAddrValue
Syntax:     Octet String (Size (16))
```

4.1.3.7 Local Address Information

4.1.3.7.1 The npAddrTable table shall contain SCPS-NP addresses for the local entity.

```
Name:       npAddrTable
Syntax:     sequence of npAddrEntry
NP Access:  Read Only
```

4.1.3.7.2 Each npAddrEntry shall consist of a sequence that relates SCPS-NP addresses of various formats with a particular interface. This parameter constitutes the addressing information for one of this entity's SCPS-NP addresses.

```
Name:       npAddrEntry
Syntax:     sequence of {
                npAdEntSCPSAddr,
                npAdEntIfIndex
            }
NP Access:  Read Only
```

4.1.3.7.3 The npAdEntSCPSAddr entries can be any of the various format SCPS-NP addresses associated with the interface that appears in this sequence. When using this interface (and end-system addressing), the value of the npAdEntSCPSAddr entry corresponding to this interface shall be the source address to use (when the user does not specify one).

Name: npAdEntSCPSAddr
Syntax: SCPS-NP Address
NP Access: Read Only

4.1.3.7.4 The npAdEntIfIndex is the entity-unique identifier for the link interface. The interface identified by a particular value of npAdEntIfIndex is the same interface identified by the same value of ifIndex (see reference [B13]).

Name: npAdEntIfIndex
Syntax: Integer
NP Access: Read Only

4.1.3.8 Address Translation Table Format

4.1.3.8.1 General

Two address translation tables shall be maintained: the end system address translation table (esAddrTranslationTable) and the path address translation table (pathAddrTranslationTable). Either of these tables may be empty.

4.1.3.8.2 End System Address Translation Table

The esAddrTranslationTable shall be used to translate a single Extended End System Address to another end system address (Basic, Extended, or IPv6), and vice-versa. The originator of a datagram shall replace the source Extended End System Address and the destination Extended End System Address with translated end system addresses if *both* the source and destination addresses appear in the End System Address Translation Table. At the destination of the datagram, the inverse translation shall be performed, and the original Extended End System Addresses shall be passed to the network service user.

Name: esAddrTranslationTable
Syntax: Sequence of esAddressPair
Access by NP: Read only

Name: esAddressPair
Syntax: sequence of {
    inputAddress,
    translatedEndSystemAddress
}

Name: inputAddress
Syntax: SCPS-NP Address (Type = Extended End System Address)

Name: translatedEndSystemAddress
Syntax: SCPS-NP Address (Type = Basic End System Address or Extended End System Address or IPv6 Address)

4.1.3.8.3 Path Address Translation Table

The pathAddrTranslationTable shall be used to relate a pair of Extended End System Addresses with a corresponding Path address (either Basic or Extended). The originator of a datagram shall replace the source Extended End System Address and the destination Extended End System Address with the path address if the source and destination addresses appear in the *same* Path Address Translation Table entry. At the destination of the datagram, the inverse translation shall be performed, and the original Extended End System Addresses shall be passed to the network service user. Intermediate systems (routers) that must send SCPS Control Messages to the source or destination of the path-addressed datagram shall use the Path Address Translation Table to determine the appropriate destination of the control message.

Name: pathAddrTranslationTable
Syntax: Sequence of pathAddressTriple
Access by NP: Read only

Name: pathAddressTriple
Syntax: sequence of {
    sourceAddress,
    destinationAddress,
    translatedPathAddress
}

Name: sourceAddress, destinationAddress
Syntax: SCPS-NP Address (Type = Extended End System Address)

Name: translatedPathAddress
Syntax: SCPS-NP Address (Type = Basic Path Address or Extended Path Address)

4.1.3.9 Physical Address Information

4.1.3.9.1 The npExtendedToMediaTable and npIPv6ToMediaTable tables shall contain address translation information for converting between a SCPS-NP address and a physical address on a local link. These tables shall provide the physical addresses for systems that are 'one hop' away from the local system. These tables are not *required* to be maintained separately; that is, in an implementation the two may be combined, so long as it is possible to index by either Extended addresses or IPv6 addresses.

Name: npExtendedToMediaTable
Syntax: Sequence of npExtendedToMediaEntry
NP Access: Read/Write

4.1.3.9.2 The npExtendedToMediaEntry structure is indexed by the tuple of the interface Index (same value as ifIndex) and the SCPS-NP Extended Address. These form the index into the table that contains as its members the interface Index, the (remote) SCPS-NP Extended Address, the (remote) physical address that corresponds to the interface and the SCPS-NP Extended Address, an indication of whether the entry is currently valid, and its means of entry.

Name: npExtendedToMediaEntry
Syntax: Sequence of {
    npExtendedToMediaIfIndex,
    npExtendedToMediaNetAddress,
    npExtendedToMediaPhysAddress,
    npExtendedToMediaType
}
Access: Read/Write

Name: npExtendedToMediaIfIndex
Syntax: Integer
NP Access: Read/Write

Name: npExtendedToMediaNetAddress
Syntax: SCPS-NP Address (Type = Extended Path or Extended End System)
NP Access: Read/Write

Name: npExtendedToMediaPhysAddress
Syntax: Medium-dependent physical address
NP Access: Read/Write

Name: npExtendedToMediaType
Syntax: Integer { other (1), invalid (2), dynamic (3), static (4) }
NP Access: Read/Write

Name: npIPv6ToMediaTable
Syntax: Sequence of npIPv6ToMediaEntry
NP Access: Read/Write

Name: npIPv6ToMediaEntry
Syntax: Sequence of {
    npIPv6ToMediaIfIndex,
    npIPv6ToMediaNetAddress,
    npIPv6ToMediaPhysAddress,
    npIPv6ToMediaType
}
Access: Read/Write

Name: npIPv6ToMediaIfIndex
Syntax: Integer
NP Access: Read/Write

Name: npIPv6ToMediaNetAddress
Syntax: SCPS-NP Address (Type = IPv6)
NP Access: Read/Write

Name: npIPv6ToMediaPhysAddress
Syntax: Medium-dependent physical address
NP Access: Read/Write

Name: npIPv6ToMediaType
Syntax: Integer { other(1), invalid(2), dynamic(3), static(4) }
NP Access: Read/Write

4.2 MIB REQUIREMENTS FOR THE SCPS CONTROL MESSAGE PROTOCOL

4.2.1 GENERAL

The MIB for systems implementing the SCPS Control Message Protocol shall include, at a minimum, the following entries.

4.2.2 STATISTICS

4.2.2.1 Messages Received

The Messages Received parameter shall contain the total number of SCMP messages that the entity received. This counter shall include the count of all messages counted by scmpInErrors.

Name: scmpInMsgs
Syntax: Counter
NP Access: Write

4.2.2.2 Messages Received With Errors

The Messages Received With Errors parameter shall contain the number of SCMP messages that the entity received but determined as having SCMP-specific errors (SCMP checksum failures, bad length, etc.).

Name: scmpInErrors
Syntax: Counter
NP Access: Write

4.2.2.3 Destination Unreachable Messages Received

The Destination Unreachable Messages Received parameter shall contain the number of SCMP Destination Unreachable messages received.

Name: scmpInDestUnreachs
Syntax: Counter
NP Access: Write

4.2.2.4 Time Exceeded Messages Received

The Time Exceeded Messages Received parameter shall contain the number of SCMP Time Exceeded messages received.

Name: scmpInTimeExcds
Syntax: Counter
NP Access: Write

4.2.2.5 Parameter Problem Messages Received

The Parameter Problem Messages Received parameter shall contain the number of SCMP Parameter Problem messages received.

Name: scmpInParmProbs
Syntax: Counter
NP Access: Write

4.2.2.6 Source Quench Messages Received

The Source Quench Messages Received parameter shall contain the number of SCMP Source Quench messages received.

Name: scmpInSrcQuenchs
Syntax: Counter
NP Access: Write

4.2.2.7 Corruption Experienced Messages Received

The Corruption Experienced Messages Received parameter shall contain the number of SCMP Corruption Experienced messages received.

Name: scmpInCorrExps
Syntax: Counter
NP Access: Write

4.2.2.8 Redirect Messages Received

The Redirect Messages Received parameter shall contain the number of SCMP Redirect messages received.

Name: scmpInRedirects
Syntax: Counter
NP Access: Write

4.2.2.9 Echo Request Messages Received

The Echo Request Messages Received parameter shall contain the number of SCMP Echo Request messages received.

Name: scmpInEchos
Syntax: Counter
NP Access: Write

4.2.2.10 Echo Reply Messages Received

The Echo Reply Messages Received parameter shall contain the number of SCMP Echo Reply messages received.

Name: scmpInEchoReps
Syntax: Counter
NP Access: Write

4.2.2.11 Messages Sent

The Messages Sent parameter shall contain the total number of SCMP messages that this entity attempted to send. This counter shall include the count of all messages counted by scmpOutErrors.

Name: scmpOutMsgs
Syntax: Counter
NP Access: Write

4.2.2.12 Outbound Errors Detected

The Outbound Errors Detected parameter shall contain the number of SCMP messages that this entity did not send because of problems discovered within SCMP (such as a lack of buffers). This value should not include errors discovered outside the SCMP layer, such as the inability of SCPS-NP to route the resultant datagram.

Name: scmpOutErrors
Syntax: Counter
NP Access: Write

4.2.2.13 Destination Unreachable Messages Sent

The Destination Unreachable Messages Sent parameter shall contain the number of SCMP Destination Unreachable messages sent.

Name: scmpOutDestUnreachs
Syntax: Counter
NP Access: Write

4.2.2.14 Time Exceeded Messages Sent

The Time Exceeded Messages Sent parameter shall contain the number of SCMP Time Exceeded messages sent.

Name: scmpOutTimeExcds
Syntax: Counter
NP Access: Write

4.2.2.15 Parameter Problem Messages Sent

The Parameter Problem Messages Sent parameter shall contain the number of SCMP Parameter Problem messages sent.

Name: scmpOutParmProbs
Syntax: Counter
NP Access: Write

4.2.2.16 Source Quench Messages Sent

The Source Quench Messages Sent parameter shall contain the number of SCMP Source Quench messages sent.

Name: scmpOutSrcQuenchs
Syntax: Counter
NP Access: Write

4.2.2.17 Corruption Experienced Messages Sent

The Corruption Experienced Messages Sent parameter shall contain the number of SCMP Corruption Experienced messages sent.

Name: scmpOutCorrExps
Syntax: Counter
NP Access: Write

4.2.2.18 Redirect Messages Sent

The Redirect Messages Sent parameter shall contain the number of SCMP Redirect messages sent.

Name: scmpOutRedirects
Syntax: Counter
NP Access: Write

4.2.2.19 Echo Request Messages Sent

The Echo Request Messages Sent parameter shall contain the number of SCMP Echo Request messages sent.

Name: scmpOutEchos
Syntax: Counter
NP Access: Write

4.2.2.20 Echo Reply Messages Sent

The Echo Reply Messages Sent parameter shall contain the number of SCMP Echo Reply messages sent.

Name: scmpOutEchoReps
Syntax: Counter
NP Access: Write

4.2.3 CONFIGURATION PARAMETERS

4.2.3.1 General

The following SCMP configuration parameters shall be used to support the rate-limiting requirements described in 3.3.5.2.

4.2.3.2 Source Quench Rate Limit

The Source Quench Rate Limit parameter shall be used to configure the maximum rate at which Source Quench messages may be issued by an SCMP entity. The rate is defined in messages per 100 milliseconds.

Name: scmpSrcQuenchRate
Syntax: Integer
NP Access: Read/Write

4.2.3.3 Error Rate Limit

The Error Rate Limit parameter shall be used to configure the maximum rate at which SCMP error messages other than Source Quench may be issued by an SCMP entity. The rate is defined in messages per 100 milliseconds.

Name: scmpErrorRate
Syntax: Integer
NP Access: Read/Write

4.2.3.4 Query Rate Limit

The Query Rate Limit parameter shall be used to configure the maximum rate at which SCMP query messages (requests or replies) may be issued by an SCMP entity. The rate is defined in messages per 100 milliseconds.

Name: scmpQueryRate
Syntax: Integer
NP Access: Read/Write

4.3 MIB REQUIREMENTS FOR THE SCPS ROUTING DATABASES

4.3.1 Three distinct routing tables that may be maintained in SCPS-NP systems, depending on the addressing modes supported: End System Address routing tables, multicast routing tables, and path routing tables.

NOTES

1 No separate routing tables for multicast path addresses are required.

2 The multicast routing tables and path routing tables support multiple next-hop choices for a single routing entry.

4.3.2 The routing database may contain routing information that indicates that there are multiple routes available to a destination. The choice of which one to use is implementation-specific. The selection criteria may be as simple as 'choose the one encountered first in the routing table'. However, the routing database entries provide for more sophisticated selection criteria. There are five 'route metrics' available for each routing table entry. These are to record 'scores' of the various routes, such as number of hops to a destination or round-trip time to a destination. The route metric entries are filled in by the routing protocol in use. (If routing is performed manually or by network management, one of the metrics may be used to set preferred and alternate routes, so that if the preferred route becomes unavailable, communication may continue automatically through the secondary route.)

Name: npESRouteTable
Syntax: Sequence of npRouteEntry
NP Access: Read/Write

Name: npMCRouteTable
Syntax: Sequence of npMultiNextHopRouteEntry
NP Access: Read/Write

Name: npPathRouteTable
Syntax: Sequence of npMultiNextHopRouteEntry
NP Access: Read/Write

4.3.3 Routing entries in each table shall be indexed by the destination address. The table shall contain the link interface to use, several routing metrics that are routing protocol specific, the next-hop SCPS-NP address, the route type, the routing protocol used, the routing protocol-specific route age, and a reference to other routing protocol-specific information.

```
Name:       npRouteEntry
Syntax:     Sequence {
                npRouteDest,
                npRouteNetmask,
                npRouteIfIndex,
                npRouteNextHop,
                npRouteMetric1,
                npRouteMetric2,
                npRouteMetric3,
```

```
                    npRouteMetric4,
                    npRouteMetric5,
                    npRouteType,
                    npRouteProto,
                    npRouteAge,
                    npRouteMTUout,
                    npRouteMTUin,
                    npRouteSendBPS,
                    npRouteRcvPipe,
                    npRouteSendPipe,
                    npRouteSSThresh,
                    npRouteRTT,
                    npRouteRTTVar,
                    npRouteAvail,
                    npRouteCorrupt,
                    npRouteCongest,
                    npRouteCapabilities,
                    npRouteInfo
                }
NP Access:      Read/Write

Name:           npMultiNextHopRouteEntry
Syntax:         Sequence {
                    npRouteDest,
                    npRouteNetmask,
                    Sequence of npRouteIfIndex,
                    Sequence of npRouteNextHop,
                    npRouteMetric1,
                    npRouteMetric2,
                    npRouteMetric3,
                    npRouteMetric4,
                    npRouteMetric5,
                    npRouteType,
                    npRouteProto,
                    npRouteAge,
                    npRouteMTUout,
                    npRouteMTUin,
                    npRouteSendBPS,
                    npRouteRcvPipe,
                    npRouteSendPipe,
                    npRouteSSThresh,
                    npRouteRTT,
                    npRouteRTTVar,
                    npRouteAvail,
                    npRouteCorrupt,
                    npRouteCongest,
                    npRouteCapabilities,
                    npRouteInfo
                }
NP Access:      Read/Write
```

4.3.4 In the npMultiNextHopRouteEntry, there is a sequence of npRouteIfIndex values, but only a single value for the characteristics of the route (npRouteType through npRouteInfo). When multiple npRouteIfIndex values exist, then the characteristics shall be set as follows:

- The npRouteType shall be set to 'invalid'.
- The npRouteProto entry shall be unaffected.
- The npRouteAge entry shall be unaffected.
- The npRouteMTUout entry shall be set to the minimum value of the outbound MTUs supported by each of the interfaces specified by npRouteIfIndex values.
- The npRouteMTUin entry shall be set to the minimum value of the inbound MTUs supported by each of the interfaces specified by npRouteIfIndex values.
- The npRouteSendBPS entry shall be set to the minimum value of the outbound data rates supported by each of the interfaces specified by npRouteIfIndex values.
- The npRouteAvail entry shall be set to 'up' if any of the interfaces specified by npRouteIfIndex values are up.
- The npRouteCorrupt entry shall be set to 'Corruption Experienced' on receipt of an SCMP Corruption Experienced message that contains the multicast address in the optional data of the message.
- The npRouteCongest entry shall be set to 'congestion experienced' on receipt of an SCMP Source Quench message that contains the multicast address in the optional data of the message.
- The npRouteCapabilities entry shall be configured to require the use of NP header checksums if any of the routes corresponding to npRouteIfIndex values requires the use of NP header checksums. Additionally, the npRouteCapabilities entry shall be configured to require the use of a hop count if any of the routes corresponding to npRouteIfIndex values requires the use of a hop count.
- The npRouteInfo entry shall be unaffected.

NOTE – The following values apply only to connection-oriented traffic, and are hence not applicable to multicast traffic:

- npRouteRcvPipe,
- npRouteSendPipe,
- npRouteSSThresh,
- npRouteRTT,
- npRouteRTTVar.

4.3.5 The npRouteDest parameter shall contain the destination SCPS-NP address of this route. An entry with a value of zero shall be considered to be a default route. Multiple routes to a single destination may appear in the table.

Name: npRouteDest
Syntax: SCPS-NP Address
NP Access: Read/Write

4.3.6 The npRouteNetmask parameter shall contain the mask that identifies which bits of the destination address should be compared to the address specified by npRouteDest in order to determine whether the addresses match. The npRouteNetmask shall be of the same address type as the corresponding npRouteDest entry. The presence of a '1' bit in the npRouteNetmask shall indicate that the corresponding bits in the destination address and the npRouteDest entry are valid for comparison. The npRouteNetmask for a default route shall be all '0s'.

Name: npRouteNetmask
Syntax: SCPS-NP Address
NP Access: Read/Write

4.3.7 The npRouteIfIndex parameter shall contain a value that uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index shall be the same interface identified by the same value of ifIndex.

Name: npRouteIfIndex
Syntax: Integer
NP Access: Read/Write

4.3.8 The npRouteNextHop parameter shall contain the SCPS-NP address of the next hop of this route.

Name: npRouteNextHop
Syntax: SCPS-NP Address
NP Access: Read/Write

4.3.9 The npRouteMetric1 parameter is the primary routing metric for the route. The semantics of the metric (and all of the other npRouteMetrics) shall be determined by the routing protocol specified in the route's npRouteProto value. If this metric is not used, its value should be -1.

Name: npRouteMetric1
Syntax: Integer
NP Access: Read/Write

4.3.10 The npRouteMetric2 parameter is an alternate routing metric for the route. The semantics of the metric shall be determined by the routing protocol specified in the route's npRouteProto value. If this metric is not used, its value should be -1.

Name: npRouteMetric2
Syntax: Integer
NP Access: Read/Write

4.3.11 The npRouteMetric3 parameter is an alternate routing metric for the route. The semantics of the metric shall be determined by the routing protocol specified in the route's npRouteProto value. If this metric is not used, its value should be -1.

Name: npRouteMetric3
Syntax: Integer
NP Access: Read/Write

4.3.12 The npRouteMetric4 parameter is an alternate routing metric for the route. The semantics of the metric shall be determined by the routing protocol specified in the route's npRouteProto value. If this metric is not used, its value should be -1.

Name: npRouteMetric4
Syntax: Integer
NP Access: Read/Write

4.3.13 The npRouteMetric5 parameter is an alternate routing metric for the route. The semantics of the metric shall be determined by the routing protocol specified in the route's npRouteProto value. If this metric is not used, its value should be -1.

Name: npRouteMetric5
Syntax: Integer
NP Access: Read/Write

4.3.14 The npRouteType parameter shall describe the type of the route (primarily, whether it is a direct or an indirect route to the destination). Setting this variable to the value invalid (2) has the effect of invalidating the corresponding entry in the routing table.

Name: npRouteType
Syntax: Integer { other (1), invalid (2), direct (3), indirect (3) }
NP Access: Read/Write

4.3.15 The npRouteProto parameter shall identify the routing mechanism by which this route was learned.

NOTE – Inclusion of various routing protocols as valid values does not imply a requirement to support those protocols. Note that local (2) refers to manually configured routing-table entries, netmgmt (3) refers to entries set via the network management protocol, scmp (4) refers to entries that were the result of an SCMP Redirect message, and the remainder are all specific routing protocols that may be supported.

Name: npRouteProto
Syntax: Integer { other (1), local (2), netmgmt (3), scmp (4), ospf (5), egp (6), rip (7) }
NP Access: Read/Write

4.3.16 The npRouteAge parameter shall contain the number of seconds since this route was last updated or otherwise determined to be correct. A determination of whether this route is 'too old' is routing-protocol specific.

Name: npRouteAge
Syntax: Integer
NP Access: Read/Write

4.3.17 The npRouteMTUout parameter shall identify the maximum message size that can be transmitted over this route. This information shall be used in maximum datagram size enforcement.

Name: npRouteMTUout
Syntax: Integer
NP Access: Read/Write

4.3.18 The npRouteMTUin parameter shall identify the maximum message size that can be received over this route. It shall be initialized to the MTU of the local inbound interface associated with the route. This information shall be used in maximum datagram size enforcement.

Name: npRouteMTUin
Syntax: Integer
NP Access: Read/Write

4.3.19 The npRouteSendBPS parameter shall contain a measure of the estimated data rate, in bits per second, available on this route. This information is used by the SCPS-TP to apply a form of rate-based flow control.

Name: npRouteSendBPS
Syntax: Gauge
NP Access: Read/Write

4.3.20 The npRouteRcvPipe parameter shall contain an estimate of the inbound bandwidth-delay product of this route. This information is used by the SCPS-TP to allocate memory to the receive buffers for this endpoint. This statistic may be updated to reflect a revised round-trip time by SCPS-TP TCP upon close of a connection.

Name: npRouteRcvPipe
Syntax: Gauge
NP Access: Read/Write

4.3.21 The npRouteSendPipe parameter shall contain an estimate of the outbound bandwidth-delay product of this route. This information is used by the SCPS-TP to allocate memory to the send buffers for this endpoint. This statistic may be updated to reflect a revised round-trip time by SCPS-TP TCP upon close of a connection.

Name: npRouteSendPipe
Syntax: Gauge
NP Access: Read/Write

4.3.22 The npRouteSSThresh parameter shall contain the initial value, in octets, at which a SCPS-TP TCP using this route should convert from slow start operation to congestion avoidance operation. This statistic may be updated by SCPS-TP TCP upon close of a connection.

Name: npRouteSSThresh
Syntax: Integer
NP Access: Read/Write

4.3.23 The npRouteRTT parameter shall contain the round-trip time, in milliseconds, expected on this route. This statistic may be updated by SCPS-TP TCP upon close of a connection.

Name: npRouteRTT
Syntax: Integer
NP Access: Read/Write

4.3.24 The npRouteRTTVar parameter shall contain an estimate of the mean deviation, in milliseconds, expected for this route. This statistic may be updated by SCPS-TP TCP upon close of a connection.

Name: npRouteRTTVar
Syntax: Integer
NP Access: Read/Write

4.3.25 The npRouteAvail parameter shall contain an indication of the current operational status of this route. If a TCP is experiencing retransmission, it may examine this parameter to attempt to determine the reason. The down (2) state shall indicate that the local interface associated with the route has been disabled as a result of a configuration action, or has not been initialized, and no alternate route is available. The testing (3) state shall indicate that no operational datagrams can be passed. The out (4) state shall indicate that a link-outage has been reported for some link associated with this route and is currently in effect.

Name: npRouteAvail
Syntax: Integer {
up (1),
down (2),
testing (3),
out(4)
}
NP Access: Read/Write

4.3.26 The npRouteCorrupt parameter shall indicate whether some element associated with this route has reported corruption within an administratively controlled time interval. The SCPS-TP TCP uses this indication to enable its corruption response in the event of a requirement for retransmissions.

Name: npRouteCorrupt
Syntax: Boolean
NP Access: Read/Write

4.3.27 The npRouteCongest parameter shall indicate whether some element associated with this route has reported congestion within an administratively controlled time interval. The SCPS-TP TCP uses this indication to enable its congestion response in the event of a requirement for retransmissions.

Name: npRouteCongest
Syntax: Boolean
NP Access: Read/Write

4.3.28 The npRouteCapabilities parameter shall indicate whether datagrams transmitted over this route should use the header checksum capability or the hop count capability or both.

Name: npRouteInfo
Syntax: Integer {
No capabilities (0),
Header checksum (1),
Hop count (2),
Both header checksum and hop count (4)
}
NP Access: Read/Write

4.3.29 The npRouteInfo parameter shall contain a reference to routing protocol-specific MIB entries.

Name: npRouteInfo
Syntax: Pointer
NP Access: Read/Write

ANNEX A

ACRONYMS AND ABBREVIATIONS

(This annex **is not** part of the Recommendation.)

AOS	Advanced Orbiting Systems
CCSDS	Consultative Committee for Space Data Systems
CUC	CCSDS Unsegmented Time Code
D-ID	Domain Identifier
ES-ID	End System Identifier
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IPv6	Internet Protocol Version Six
M-Flag	Multicast Flag
MIB	Management Information Base
MTU	Maximum Transmission Unit
N-SDU	Network Service Data Unit
N-ID	Network Identifier
NP	Network Protocol
P-Field	Preamble Field
P-ID	Path Identifier
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
QOS	Quality of Service
SCMP	SCPS Control Message Protocol

SCPS	Space Communications Protocol Specification
SDU	Service Data Unit
T-Field	Time Field
TCP	Transmission Control Protocol
TP-ID	Transport Protocol Identifier
UDP	User Datagram Protocol
VPI	Version/Protocol Identifier

ANNEX B

INFORMATIVE REFERENCES

(This annex **is not** part of the Recommendation.)

[B1] *Procedures Manual for the Consultative Committee for Space Data Systems*. CCSDS A00.0-Y-7. Yellow Book. Issue 7. Washington, D.C.: CCSDS, November 1996.

[B2] J. Mogul and S. Deering. *Path MTU Discovery.* RFC 1191. November 1990.†

[B3] *Space Communications Protocol Specification (SCPS)—Rationale, Requirements, and Application Notes*. Report Concerning Space Data System Standards, CCSDS 710.0-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[B4] *Advanced Orbiting Systems, Networks and Data Links: Architectural Specification.* Recommendation for Space Data Systems Standards, CCSDS 701.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, November 1992.

[B5] *Telecommand Part 2 — Data Routing Service.* Recommendation for Space Data Systems Standards, CCSDS 202.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, November 1992.

[B6] *Packet Telemetry*. Recommendation for Space Data System Standards, CCSDS 102.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, November 1995.

[B7] *Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP).* Recommendation for Space Data System Standards, CCSDS 713.5-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[B8] *Space Communications Protocol Specification (SCPS)—Transport Protocol (SCPS-TP).* Recommendation for Space Data System Standards, CCSDS 714.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[B9] S. Kent and R. Atkinson. *IP Authentication Header*. RFC 2402, November 1998.

[B10] S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP).* RFC 2406, November 1998.

[B11] J. Postel. *Internet Protocol*. STD 5, September 1981. [RFC 791, RFC 950, RFC 919, RFC 922, RFC 792, RFC 1112]

† Internet Request for Comments (RFC) texts are available on line in various locations (e.g., http://ietf.org/rfc/). In this list, Internet Standards are identified by 'STD' followed by the number of the standard, and RFCs are identified by 'RFC' followed by the number of the RFC. RFCs comprised by Internet Standards are given in square brackets following the citation.

[B12] R. Braden. *Hosts Requirements*. STD 3, October 1989. [RFC 1122, RFC 1123]

[B13] K. McCloghrie and M. Rose. *Management Information Base*. STD 17, March 1991. [RFC1213]

[B14] J. Reynolds and J. Postel. *Assigned Numbers*. STD 2, October 1994. [RFC 1700]

[B15] P. Almquist. *Towards Requirements for IP Routers*. Ed. F. Kastenholz. RFC 1761, November 1994.

[B16] R. Hinden and S. Deering. *IP Version 6 Addressing Architecture*. RFC 2373, July 1998.

[B17] V. Jacobson. *Compressing TCP/IP Headers for Low-Speed Serial Links*. RFC 1144, February 1990.

[B18] W. Richard Stevens. *TCP/IP Illustrated*. Vol. 1. Reading, Mass.: Addison-Wesley, 1994.

[B19] W. Richard Stevens and Gary R. Wright. *TCP/IP Illustrated*. Vol. 2. Reading, Mass.: Addison-Wesley, 1995.

ANNEX C

PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(This annex **is** part of the Recommendation.)

C1 INTRODUCTION

This annex provides the Protocol Implementation Conformance Statement (PICS) Requirements List (PRL) for implementations of SCPS-NP. The PICS for an implementation is generated by completing the PRL in accordance with the instructions below. An implementation shall satisfy the mandatory conformance requirements of the base standards referenced in the PRL.

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:

- the protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;
- the supplier and acquirer or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSes);
- a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

C1.1 NOTATION

The following are used in the PRL to indicate the status of features:

Status Symbols

M mandatory.

M.<n> support of every item of the group labeled by the same numeral <n> required, but only one is active at a 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.

- non-applicable field/function (i.e., logically impossible in the scope of the PRL).

I out of scope of PRL (left as an implementation choice).

X excluded or prohibited.

Two character combinations may be 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) status; thus 'MO' means 'mandatory to be implemented, optional to be used'.

Notations for Conditional Status

The following predicate notations are used:

<predicate>:: This notation introduces a group of items, all of which are conditional on <predicate>.

<predicate>: This notation introduces a single item which is conditional on <predicate>.

In each case, the predicate may identify a protocol feature, or a Boolean combination of predicates. ('^' is the symbol for logical negation, '|' is the symbol for logical OR, and '&' is the symbol for logical AND.)

<index>: This notation indicates that the status following it applies only when the PICS states that the features identified by the index are supported. In the simplest case, <index> is the identifying tag of a single PRL item. The symbol <index> also may be a Boolean expression composed of several indices.

<index>:: This notation indicates that the associated clause should be completed.

Notations Used in the Protocol Feature Column

<r> Symbol used to denote the receiving system.

<t> Symbol used to denote the transmitting system.

Support Column Symbols

The support of every item as claimed by the implementer is stated by entering the appropriate answer (Y, N, or N/A) in the support column:

Y Yes, supported by the implementation.

N No, not supported by the implementation.

N/A Not applicable.

C1.2 REFERENCED BASE STANDARDS

SCPS-NP (this document) is the only base standard referenced in the PRL. In the tables below, numbers in the Reference column refer to applicable subsections within this document.

C1.3 GENERAL INFORMATION

C1.3.1 IDENTIFICATION OF PICS

Ref	Question	
1	Date of Statement (DD/MM/YYYY)	
2	PICS serial number	
3	System Conformance statement cross-reference	

C1.3.2 IDENTIFICATION OF IMPLEMENTATION UNDER TEST (IUT)

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating System name	
6	Operating System version	
7	Special Configuration	
8	Other Information	

C1.3.3 IDENTIFICATION

Supplier	
Contact Point for Queries	
Implementation name(s) and Versions	
Other Information Necessary for full identification - e.g., name(s) and version(s) for machines and/or operating systems; System Name(s)	

C1.3.4 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 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	

C1.4 INSTRUCTIONS FOR COMPLETING THE PRL

An implementer shows the extent of compliance to the protocol by completing the PRL; that is, compliance to all mandatory requirements and the options that are not supported are shown. The resulting completed PRL is called a PICS. In the Support 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, N/A should be used. 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 requirement is expressed as a two-character combination (as defined above), the response shall address each element of the requirement; e.g., for the requirement ‘MO’, the possible compliant responses are ‘YY’ or ‘YN’.

C2 SERVICES

Item	Protocol Feature	Reference	Status	Support
	Services			
udr	N-Unitdata.request	D2.1.1	M	
udi	N-Unitdata.indication	D2.1.2	M	
jgr	N-Join host group request	D2.2.1	O	
lgr	N-Leave host group request	D2.2.2	O	
maxs	Get Max Sizes request	D2.3.1	M	
advdel	Advise Delivery Probability request	D2.3.2	O	
erq	Echo Request	D2.4.1	M	
ec	Echo confirm	D2.4.2	M	

C3 FRAME STRUCTURE

C3.1 SCPS-NP FRAME STRUCTURE

Item	Protocol Feature	Reference	Status	Support
vpi	Version/Protocol Identifier	3.2.3	M	
len	Datagram Length Field	3.2.3.2	M	
tpid	Transport protocol identifier	3.2.3.3	M	
ctlfld	Control field	3.2.3.4	M	
da	Destination Address Field	3.2.3.5	M	
sa	Source Address Field	3.2.3.5	MO	
hc	Hop Count Field	3.2.3.7	MO	
ts	Time Stamp Field	3.2.3.8	MO	
ts1	CCSDS 24-bit CUC Implicit P-Field Timestamp		O.1	
ts2	CCSDS Variable sized CUC Explicit P-Field Timestamp		O.1	
ts3	32-bit Binary Timestamp		O.1	
bqos	Basic Quality of Service	3.2.3.6	O	
eqos	Expanded Quality of Service	3.2.3.9	O	
hchk	Header Checksum	3.2.3.10	MO	
hdrfmt	Header formatting	3.2.2	M	
hdrprs	Header parsing	3.2.3.10	M	

C3.2 SCMP FRAME STRUCTURE

Item	Protocol Feature	Reference	Status	Support
type	Type field	3.3.3.1	M	
code	Code field		M	
chksm	Checksum field		M	
msd	Message-specific data		M	

NOTE – The SCMP Frame Structure is carried as user data within the SCPS-NP Frame Structure.

C4 SCPS-NP PROCEDURES

Item	Protocol Feature	Reference	Status	Support
	Datagram Transmission Procedures			
val	Validate user request and parameters	3.2.5.3.2	M	
hop1	Determine first hop destination	3.2.5.3.3	M	
fmtout	Format outgoing datagram	3.2.5.3.4	M	
linkout	Invoke link transmission procedures	3.2.5.3.5	M	
diagout	Perform diagnostic and error processing	3.2.5.3.6	M	
	Datagram receipt procedures			
linkin	Acquire link layer data	3.2.5.4.2	M	
verin	Verify datagram format	3.2.5.4.3	M	
local	Determine local delivery	3.2.5.4.4	M	
toxport	Deliver to transport protocol	3.2.5.4.5	M	
diagin	Perform diagnostic and error processing	3.2.5.4.6	M	
	Datagram Forwarding Procedures			
fwd	Determine need to forward	3.2.5.4.4, 3.2.5.5.3	O	
loop1	Decrement hop count field	3.2.5.5.4	fwd&hc:M	
hc1	If ≤ zero, discard datagram, increment npForwHopDiscard		fwd&hc:M	
hc2	If ≤ zero, send SCMP Time Exceeded message to source		fwd&hc:M	
hc3	If > zero, revise header checksum if present		fwd&hc&hchk:M	
loop2	Check timestamp		fwd&^hc&ts:M	
ts4	If Timestamp+npTimeToLive < current time, discard datagram and increment npForwTTLDiscard	3.2.5.5.4	fwd&^hc&ts:M	
ts5	If Timestamp+npTimeToLive < current time, send SCMP Time Exceeded message to source		fwd&^hc&ts:M	
loop3	If BQOS present and flood routing requested and this segment has been seen before, discard		fwd&flood:M	
loop3a	If BQOS present and flood routing requested and this segment has not been seen before, enter into flood routing table and flood route		fwd&flood:M	
loop3b	If BQOS present and flood routing not requested and segment not seen before, forward as for unicast		fwd&^flood:M	
hop2	Determine next hop address	3.2.5.5.5	fwd:M	
lout2	Invoke link transmission procedures	3.2.5.5.6	M	
diagf	Perform diagnostic and error processing	3.2.5.5.7	M	
	Routing Procedures			
dfr	Default route	3.2.6.1.1	M	
esr	End system routing	3.2.6.1.2	M	
pathr	Path routing	3.2.6.1.3	O	
multir	Multicast routing	3.2.6.1.4	O	
flood	Flood routing	3.2.6.1.5	O	
	Precedence Procedures			
pr1	Order of datagram processing	3.2.6.2.2	bqos:M	
pr2	Congestion control	3.2.6.2.3	bqos:M	
	Multihoming			
	Source address selection:			
sa1	If path addressing, no source address	3.2.6.3	pathr:M	
sa2	If replying to inbound datagram, source address = interface address over which inbound datagram was received	3.2.6.3	O	
sa3	Application can select source address on multihomed host	3.2.6.3	M	
sa4	If no application specification of source address, network service selects	3.2.6.3	M	

C5 SCMP PROCEDURES

Item	Protocol Feature	Reference	Status	Support
scmp1	Use SCPS-NP N-Unitdata service to carry messages	3.3.1	M	
scmp2	TP-ID set to SCMP	3.2.3.3, 3.3.1	M	
scmp3	CCSDS 24-bit CUC Implicit P-Field Timestamp	3.2.3.8, 3.3.1	ts:M	
scmp4	Precedence = network control (if not Source Quench message)	3.3.1	bqos:M	
scmp5	Routing method = pt-to-pt	3.3.1	bqos:M	
scmp6	Program specific info = 0	3.3.1	bqos:M	
scmp7	Use Expanded QOS	3.2.3.9, 3.3.1	X	
	Error Message Generation			
	Generate Error message in response to			
err1	SCMP Error message	3.3.5.1	X	
err2	Invalid SCPS-NP header		X	
err3	Network layer Multicast or Broadcast messages		X	
err4	Link layer Multicast or Broadcast messages		X	
err5	Datagram with invalid Source address		X	
err6	Flood-routed or 2-path routed datagram		X	
err7	Silent discard of a datagram		X	
rate1	Rate limit error messages other than Source Quench	3.3.5.2	M	
rate2	Rate limit Source Quench error messages	3.3.5.2	M	
rate3	Method of imposing rate limit	3.3.5.2	I	
du	Send Destination Unreachable message	3.3.4.1	O	
du1	Send message to source address in network layer datagram		du:M	
du2	Type = 3		du:M	
du3	Code 0..16		du:M	
du4	Checksum		du:M	
du5	msd - 1 octet length		du:M	
du6	msd - network layer header		du:M	
du7	msd - first eight octets of transport header		O	
du8	Send host unreachable if other hosts on same network are known to be accessible		du:M	
du9	Send protocol or port unreachable		O	
sq	Send Source Quench messages	3.3.4.2	M	
sq1	Send message to source address in network layer datagram		M	
sq2	Type = 4		M	
sq3	Code = 0		M	
sq4	Checksum		M	
sq5	msd - 1 octet length		M	
sq6	msd - network layer header		M	
sq7	msd - first eight octets of transport header		O	
sq8	Observe Source Quench rate-limiting procedures		M	
sq9	Set precedence to same value of incoming datagram		bqos:M	
re	Send Redirect message	3.3.4.3	M	
re1	Send message to source address in network layer datagram		M	
re2	Type = 5		M	
re3	Code = 0,2		X	
re4	Code = 1,4		M	
re5	Code = 3		O	
re6	Checksum		M	
re7	msd - 1 octet address type = 0..2		M	
re8	msd - SCPS-NP address		M	

Item	Protocol Feature	Reference	Status	Support
re9	msd - 1 octet length	3.3.4.3	M	
re10	msd - network layer header		M	
re11	msd - first eight octets of transport header		O	
te	Send Time Exceeded message	3.3.4.4	fwd& (loop1 | loop2):M	
te1	Send message to source address in network layer datagram		M	
te2	Type = 11 (decimal)		M	
te3	Code = 0		M	
te4	Checksum		M	
te5	msd - 1 octet length		M	
te6	msd - network layer header		M	
te7	msd - first eight octets of transport header		O	
pp	Send Parameter Problem message	3.3.4.5	M	
pp1	Send message to source address in network layer datagram		M	
pp2	Type = 12		M	
pp3	Code = 0		M	
pp4	Checksum		M	
pp5	msd - 1 octet pointer		M	
pp6	msd - 1 octet length		M	
pp7	msd - network layer header		M	
pp8	msd - first eight octets of transport header		O	
pp9	Send only if error caused datagram to be discarded		M	
ce	Send Corruption Experienced message	3.3.4.6	M	
ce1	Send message to router at remote end of corrupted link		M	
ce2	Send message to implementation-defined number of recent users of the link		M	
ce3	Type = 19		M	
ce3	Code = 0		M	
ce4	Checksum		M	
ce5	Send message-specific data		M	
er	Send and receive Echo Requests and replies	3.3.4.7	M	
er1	Receive and echo up to MTU-sized Echo Request		M	
er2	Echo Request type = 8		M	
er3	Echo Reply type = 0		M	
er4	First 2 octets of msd = identifier		M	
er5	Second 2 octets of msd = sequence number		M	
er6	Octets 5-n of request contain data		O	
er7	Identifier and sequence number in reply identical to identifier and sequence number in request		M	
er8	Echo Reply additional data: hop count, timestamp, MTU, data rate		M	
er9	Data in request returned in reply without modification, to maximum message size		M	
er10	Respond to Echo Requests addressed to broadcast or multicast addresses		O	
er11	Configuration option to permit Echo Requests to be silently discarded		O	
er12	Option defaults to off (i.e., Echo Requests are NOT discarded)		er11:M	
er13	Provide API for Echo Request/Reply		M	
er14	All Echo Replies received passed to API		M	
er15	Source address in reply is same as specific destination address of request		M	

C6 MIB SUPPORT

Item	Protocol Feature	Reference	Status	Support
npstat	SCPS-NP Statistics	4.1.2	M	
npcon	SCPS-NP Configuration parameters	4.1.3	M	
cmstat	SCMP Statistics	4.2.2	M	
cmcon	SCMP Configuration parameters	4.2.3	M	
rtcon	Routing table contents	4.3	M	
esrt	End System routing table	4.3	M	
pathrt	Path routing table	4.3	pathr:M	
multirt	Multicast routing tables	4.3	multir:M	

ANNEX D

SCPS NETWORK SERVICE SPECIFICATION

(This annex **is** part of the Recommendation.)

D1 OVERVIEW OF THE NETWORK SERVICE

This section identifies the services provided by the SCPS Network. The prefixes used to distinguish between the SCPS Network and underlying services are listed here:

– N- Network (specifically, the SCPS Network);

– SN- Subnetwork (the underlying communication service over which the SCPS-Network Protocol operates).

The SCPS Network services provide for the end-to-end unreliable transfer of SCPS N-SDUs through the SCPS Network within SCPS N-PDUs.

The Unit Data Service provides the ability to send and receive service data units of variable length, with the length of the service data unit accompanying the data across the service interface.

The Multicast Service allows a network service user to enable delivery of datagrams sent to a multicast group address and received by that host. The Multicast Service also allows a network service user subsequently to disable delivery of datagrams addressed to that group.

The Support Services provide the SCPS Network user with two services of potential use: the ability to determine maximum datagram sizes to and from a remote destination, and the ability to provide delivery success information to the SCPS Network service.

The SCPS Network provides internal control mechanisms that may convey information of use to SCPS Network users. As a result, the SCPS Control Message Service allows the SCPS-Network to inform SCPS Network users of events within the SCPS Network that may affect the operation of the SCPS Network users.

D1.1 DEFINITIONS

Intermediate Delivery parameter: A parameter of the N-ECHO.request service primitive that allows a user to request that the network user data (the N-SDU) be delivered only to the destination system (the typical case) or to the destination and all intermediate systems. The parameter has two values: DESTINATION (the default), which indicates that the N-SDU shall be delivered only to the destination address; and INTERMEDIATE, which indicates that the N-SDU shall be delivered to the destination address and to all intermediate systems encountered.

NOTE – The INTERMEDIATE setting of Intermediate Delivery flag is intended for diagnostic use, to provide a single-transmission 'traceroute' service. The 'traceroute' service, used in the Internet, provides a response from each intermediate router between a source and destination by repeatedly sending echo messages to the destination, but starting the maximum hops at one and incrementing it one for each message. This results in return of an error message to the source from the router that discarded the datagram. The traceroute service is simple but generates a significant amount of traffic and takes a significant amount of time to trace a route. The Intermediate Delivery capability is intended to cause all intermediate systems to provide a response to the same Echo Request. The address information and hop count information can be used to construct the route to the destination.

N-Basic_Quality_of_Service parameter: The Basic Quality of Service (QOS) parameter of the N-UNITDATA service primitives carries information necessary to provide special network processing services for the datagram. It is a data structure that contains three sub-parameters: precedence, routing requirements, and a program-specific field.

N-Delivery_Probability_Sense parameter: A parameter of the N-ADVISE-DELIVPROB.request service primitive that allows the SCPS Network user to indicate to the SCPS Network service provider that the data quality being provided by the SCPS Network is acceptable or unacceptable. The user makes a determination of acceptability using feedback mechanisms that are specific to the user and outside the scope of this Recommendation. The Delivery Probability Sense parameter has two values: Acceptable and Unacceptable (numeric values associated with these values are local implementation issues).

N-Destination_Address: The N-Destination_Address is a parameter of all of the SCPS Network service primitives. It is an N-Address that identifies the destination end system of a datagram in the SCPS Network. The N-Destination_Address parameter must be of the Extended End System address type, and may be of either the IP or the SCPS address family. (Local implementations may define additional primitives of the Unit Data service that provide additional flexibility in specifying address types. This is a local extension, outside the scope of this Recommendation.)

N-Expanded_Quality_of_Service parameter: The Expanded QOS parameter provides a mechanism for specifying ground-relevant QOS requests. The valid values of this parameter are defined in RFC 2474 (reference [1]).

N-Hop_Count_Field_Value parameter: The N-Hop_Count_Field_Value is a parameter to the N-Echo.request and N-Echo.confirm service primitives. In the request primitive, it specifies the initial value for the hop count parameter in the SCPS-NP header that carries the Echo Request message. In the confirm primitive, it indicates the value of the hop count parameter of the SCPS-NP header carrying the Echo Request message at the time it was received by the remote system.

N-Source_Address: The N-Source_Address is a parameter to many of the primitives of the SCPS Network service. It is an N-Address that identifies the end system originating a datagram in the SCPS Network. The N-Source_Address must be of the Extended End System address type, and may be of either the IP or the SCPS address family. The N-Source_Address may not be a multicast or a broadcast address. (Local implementations may define additional primitives of the Unit Data service that provide additional flexibility in specifying address types. This is a local extension, outside the scope of this Recommendation.)

N-Source_Timestamp parameter: The N-Source_Timestamp is a parameter of several SCPS Network service primitives. This parameter permits the network service user to provide a source timestamp to accompany the N-SDU. The Source Timestamp parameter consists of a timestamp format field and a timestamp value field. As a parameter of the N-Echo.confirm primitive, it contains the value of the timestamp field of the SCPS-NP header as it was received by the remote system and thus facilitates round trip time calculations.

N-User_Internet_Protocol_Number parameter: The N-User_Internet_Protocol_Number is a parameter to several of the SCPS Network service primitives. The valid values of this parameter are a subset of the full range of Internet Protocol Numbers, as shown in table D-1.

Table D-1: Valid Values of the N-User_Internet_Protocol_Number Parameter

Network Service User	Internet Protocol Number
TCP	6
UDP	17
IPv6 Authentication Header	50
IPv6 Encapsulating Security Payload	51
SCPS Security Protocol	99
Compressed TCP	105

Precedence parameter: The precedence parameter is an element of the N-Basic_Quality_of_Service parameter of the N-UNITDATA service primitives. The precedence parameter is specified by a network service user to identify the relative importance of this data compared to other data within the network. It is an integer with a valid range from 0 to 15, with 0 being the lowest precedence and 15 being the highest. Local policy may result in the user-specified precedence parameter's being overridden. The network service user may also supply a null value for the precedence parameter. In this case, the network service shall assign a default value for the precedence parameter.

Program Specific parameter: The program-specific parameter is an element of the N-Basic_Quality_of_Service parameter that provides a mechanism for programs to carry two bits of information in the SCPS-NP header. This information is interpreted by program-specific extensions to the SCPS-NP and has a default value of 0.

Routing Requirements parameter: The Routing Requirements parameter is an element of the N-Basic_Quality_of_Service parameter of the N-UNITDATA service primitives. The

Routing Requirements parameter has two currently defined values: 'normal' routing and 'flood' routing.

SN-Interface parameter: The SN-Interface parameter specifies a particular subnetwork interface unit. The valid values of this parameter are host-specific.

Timestamp Format field: The Timestamp Format field of the N-Source_Timestamp parameter identifies the format of the source timestamp that is supplied by the network user. The available formats are specified in 3.2.3.8.

Timestamp Value: The Source Timestamp Value field of the N-Source_Timestamp parameter contains the value of the timestamp that shall accompany the N-SDU.

D2 SERVICES PROVIDED BY THE NETWORK LAYER

This subsection describes in detail the primitives and parameters associated with each SCPS Network service. This subsection does not define an Application Programming Interface; the parameters are specified in an abstract manner, and a conforming implementation is not constrained in the method of making this information available.

D2.1 UNIT DATA SERVICE

D2.1.1 N-UNITDATA.request

D2.1.1.1 Function

The N-UNITDATA.request primitive requests that the user-supplied N-SDU be transmitted to the specified Destination End System Address and delivered to the SCPS Network service user identified by the N-User_Internet_Protocol_Number parameter. Additional parameters to the request qualify the manner in which this service is provided.

D2.1.1.2 Semantics

The primitive shall provide the following parameters:

```
N-UNITDATA.request      (N-Destination_Address,
                         N-Source_Address,
                         N-User_Internet_Protocol_Number,
                         N-Source_Timestamp,
                         N-Basic_Quality_of_Service,
                         N-Expanded_Quality_of_Service,
                         N-SDU)
```

D2.1.1.3 When Generated

This primitive is passed to the SCPS Network to request it to send the N-SDU to the remote entity identified by the N-Destination_Address and N-User_Internet_Protocol_Number.

D2.1.1.4 Effect on Receipt

Receipt of this primitive causes the SCPS Network to create an N-PDU containing the N-SDU and to send the N-PDU to the destination by issuing an SN-UNITDATA.request.

D2.1.1.5 Additional Comments

The N-Destination_Address shall be of either the IP Address Family or the SCPS Address Family, and shall be of the Extended End System format. The N-Source_Address may be null, in which case the network service shall select an appropriate address. Alternatively, the network service user may specify an N-Source_Address. If specified, the N-Source_Address shall be of either the IP Address Family or the SCPS Address Family, shall be of the Extended End System format, and must be a valid source address for the local system.

NOTE – Local implementations may define additional primitives of the Unit Data service that provide additional flexibility in specifying address formats. This local extension is outside the scope of this Recommendation.

The N-User_Internet_Protocol_Number may assume the values defined in table D-2.

Table D-2: SCPS-NP-Supported Internet Protocol Numbers

Network Service User	Internet Protocol Number
TCP	6
UDP	17
IPv6 Authentication	50
IPv6 Encapsulating Security Header	51
SCPS Security Protocol	99
Compressed TCP	105

D2.1.2 N-UNITDATA.indication

D2.1.2.1 Function

The N-UNITDATA.indication primitive is issued by the SCPS Network to the network service user to indicate the arrival of data addressed to the user.

D2.1.2.2 Semantics

The primitive shall provide the following parameters:

```
N-UNITDATA.indication      (N-Destination_Address,
                            N-Source_Address,
                            N-User_Internet_Protocol_Number,
```

N-Source_Timestamp,
N-Basic_Quality_of_Service,
N-Expanded_Quality_of_Service,
N-SDU)

D2.1.2.3 When Generated

The primitive is passed from the SCPS Network to the SCPS Network service user to indicate the arrival of network user data (an N-SDU).

D2.1.2.4 Effect on Receipt

The effect of receipt of this primitive on the SCPS Network service user is not specified.

D2.1.2.5 Additional Comments

The N-Destination_Address, N-User_Internet_Protocol_Number, N-Source_Timestamp, and N-SDU shall be identical to the parameters submitted with the corresponding N-UNITDATA.request primitive.

D2.2 MULTICAST GROUP MANAGEMENT SERVICE

There are two multicast group management service primitives provided by the SCPS Network: Join Host Group and Leave Host Group. The multicast group management service is optional within the SCPS-NP. Specific mission requirements will determine whether it is incorporated. The presence of the multicast group management service shall be noted in the Protocol Implementation Conformance Statement (PICS). (Refer to annex C for a proforma of the PICS.)[1]

D2.2.1 N-JOIN_HOST_GROUP.request

D2.2.1.1 Function

The N-JOIN_HOST_GROUP.request primitive requests that the network service user identified by the TP-ID receive multicast datagrams that are addressed to a particular group address.

[1] The network entities belonging to a multicast group are defined statically. The decision to receive or not to receive multicast data using the primitives defined in this section has scope locally within the destination system, once the data has been received by the statically defined destination(s). Routers are configured through external means with the multicast routing tables that represent the complete (infrequently changing) membership of the multicast group. Applications at various destination systems use the primitives defined in this section to join and leave a group locally.

D2.2.1.2 Semantics

The form of the service request is as follows:

N-JOIN_HOST_GROUP.request (N-Destination_Address,
N-User_Internet_Protocol_Number,
SN-Interface)

The N-Destination_Address parameter contains the SCPS Network Address of the multicast group in the Extended End System Address format. The address may be either of the SCPS Address Family or of the IP Address Family.

The N-User_Internet_Protocol_Number parameter identifies the SCPS Network service user to which the data should be delivered.

The SN-Interface parameter identifies the particular subnetwork interface over which to receive the multicast traffic. Valid values include subnetwork-specific interface identifiers and a null value. If null, data addressed to the specified N-Destination_Address that arrives on any subnetwork interface is delivered to the SCPS Network service user identified by the N-User_Internet_Protocol_Number.

D2.2.1.3 When Generated

The Join Host Group request is generated by a SCPS Network user when it wishes to receive data that is transmitted to the specified group address.

D2.2.1.4 Effect on Receipt

The SCPS Network shall begin delivering the traffic sent to the specified N-Destination_Address to the network service user specified by the N-User_Internet_Protocol_Number service parameter.

D2.2.1.5 Additional Comments

A network service user may issue the N-JOIN_HOST_GROUP service request for the same N-Destination_Address on multiple subnetwork interfaces.

D2.2.2 N-LEAVE_HOST_GROUP.request

D2.2.2.1 Function

The N-LEAVE_HOST_GROUP.request primitive requests that a network service user no longer receive multicast datagrams that are addressed to the specified group address.

D2.2.2.2 Semantics

The service primitive shall provide the following parameters:

N-LEAVE_HOST_GROUP.request (N-Destination_Address,
N-User_Internet_Protocol_Number,
SN-Interface)

The SN-Interface parameter identifies the particular hardware interface to cease scanning for multicast traffic. If unspecified, all subscribed interfaces are assumed.

D2.2.2.3 When Generated

The Leave Host Group request is issued when a network service user no longer wishes to receive data from a particular group address.

D2.2.2.4 Effect on Receipt

Data sent to the specified group address via the specified interface shall no longer be delivered to the network service user identified by the N-User_Internet_Protocol_Number.

D2.3 SCPS NETWORK SUPPORT SERVICES

There are two SCPS Network Support services: the Get Maximum Datagram Sizes service and the Advise Delivery Probability service.

D2.3.1 N-GET_MAX_SIZES.request

D2.3.1.1 Function

The N-GET_MAX_SIZES.request primitive informs the SCPS Network user of the maximum size datagrams that the network service user may send to and receive from a particular remote endpoint.

D2.3.1.2 Semantics

The service primitive shall provide the following parameters:

N-GET_MAX_SIZES.request (N-Destination_Address,
N-Source_Address,
N-Source_Timestamp_Format,
N-Basic_Quality_of_Service,
N-Expanded_Quality_of_Service,
N-Maximum_Send_Size,
N-Maximum_Receive_Size,
N-Time_of_Update)

D2.3.1.3 When Generated

The N-GET_MAX_SIZES.request primitive is issued by the SCPS Network user in order to determine the maximum datagram sizes that can be supported by the network. This operation may be performed, for example, at the beginning of a SCPS-TP connection.

D2.3.1.4 Effect Upon Receipt

The SCPS Network determines, by locally defined means, the maximum send and receive datagrams for the SCPS Network user and returns them to the user, along with the time that this information was last updated. This information is returned in the corresponding parameters of the request primitive.

D2.3.1.5 Additional Comments

The N-Destination_Address and the N-Source_Address shall be of the Extended End System Address type. They may be of either the SCPS Address Family or the IP Address Family. The N-Source_Address shall be an address that is valid for the local SCPS Network entity. If the N-Source_Address parameter is null, an address shall be selected by the network service.

The N-Source_Timestamp_Format, N-Basic_Quality_of_Service, and N-Expanded_Quality_of_Service fields may be null. If null, the maximum send and receive sizes shall be calculated assuming that these fields will not be present in the SCPS-NP header.

D2.3.2 N-ADVISE-DELIVPROB.request

D2.3.2.1 Function

The N-ADVISE-DELIVPROB.request primitive allows the SCPS Network user (e.g., the SCPS-TP or SCPS-SP) to provide information to the SCPS Network about known success or failure in sending data to a particular remote destination.

NOTE – This service is typically invoked when the SCPS-TP TCP protocol has retransmitted a number of times over a connection without receiving an acknowledgment for the retransmitted data. At a point *before* the connection is abandoned for having exceeded the maximum retransmissions threshold, the SCPS-TP TCP entity would inform the SCPS-NP that SCPS-TP TCP suspected that the particular route through the network was faulty (this is termed giving ‘negative advice’ to the network layer). In response to this negative advice, the SCPS-NP would typically attempt to identify an alternate route to the destination.

D2.3.2.2 Semantics

The service primitive shall provide the following parameters:

N-ADVISE-DELIVPROB.request (N-Destination_Address,
N-Source_Address,
N-Basic_Quality_of_Service,
N-Expanded_Quality_of_Service,
N-Delivery_Probability_Sense)

D2.3.2.3 When Generated

The Advise Delivery Probability service is invoked at the discretion of the SCPS Network user.

D2.3.2.4 Effect Upon Receipt

The SCPS Network will determine whether or not to attempt to find another route to the specified N-Destination_Address.

D2.3.2.5 Additional Comments

The N-Destination_Address and the N-Source_Address shall be of the Extended End System Address type. They may be of either the SCPS Address Family or the IP Address Family. The N-Source_Address shall be an address that is valid for the local SCPS Network entity. If the N-Source_Address parameter is null, an address shall be selected by the network service.

In general, this service SHOULD NOT be invoked upon receipt of every acknowledgment by a transport protocol. Rather, it should be issued when, for example, a particular transport connection experiences multiple retransmission time-outs for a datagram.

For diagnostic and debugging purposes, it may be useful for the network layer to maintain some history about delivery probability information received, possibly including the time at which advice (positive or negative) was received regarding a particular destination. The specifics of such history are implementation dependent, and as such are beyond the scope of this protocol definition.

D2.4 SCPS CONTROL MESSAGE SERVICE

There is one SCPS Control Message Service that is available to users: the Echo service. Two primitives support this service: the Echo request and Echo confirm primitives. Note that the corresponding primitives, the Echo indication and Echo response primitives, are not defined here because they are not exposed to the network service user. Rather, these capabilities are implemented within the SCPS Control Message Protocol.

D2.4.1 N-ECHO.request

D2.4.1.1 Function

The N-ECHO.request primitive requests that the destination system and, optionally, intervening systems reflect the Echo Request message back to the source system, including some information in the confirmation that supports network diagnostics.

D2.4.1.2 Semantics

The service primitive shall provide the following parameters:

```
N-ECHO.request      (N-Destination_Address,
                     N-Source_Address,
                     N-Intermediate_Delivery,
                     N-Hop_Count_Field_Value)
```

The N-Intermediate_Delivery parameter, when TRUE, requests that the Echo Request be delivered to all intermediate systems encountered between the source end system and the destination end system.

D2.4.1.3 When Generated

The Echo Request is generated by a network service user to determine information about the accessibility of systems in the SCPS Network, the round-trip delays, and the routing connectivity.

D2.4.1.4 Effect Upon Receipt

The network service shall issue an SCMP Echo Request message.

D2.4.1.5 Additional Comments

The N-Destination_Address and the N-Source_Address shall be of the Extended End System Address type. They may be of either the SCPS Address Family or the IP Address Family. The N-Source_Address shall be an address that is valid for the local SCPS Network entity. If the N-Source_Address parameter is null, an address shall be selected by the network service.

D2.4.2 N-ECHO.confirm

D2.4.2.1 Function

The N-ECHO.confirm primitive indicates that the local system has received an Echo Reply message back to the source system, including some information in the reply that supports network diagnostics.

D2.4.2.2 Semantics

The service primitive shall provide the following parameters:

```
N-ECHO.confirm   (N-Destination_Address,
                  N-Source_Address,
                  N-Hop_Count_Field_Value,
                  N-Source_Timestamp,
                  SCMP Echo Reply Protocol Data Unit)
```

The format of the SCMP Echo Reply Protocol Data Unit is specified in 3.3.4.7.

D2.4.2.3 When Generated

The Echo confirm is generated upon receipt of an SCMP Echo Reply message.

D2.4.2.4 Effect Upon Receipt

The SCPS Network service does not specify the effect upon receipt.

D2.4.2.5 Additional Comments

The N-Hop_Count_Field_Value and N-Source_Timestamp parameters contain the values that were *received* by the system responding to the Echo Request (that is, the remote system). They represent the values contained in the outbound SCPS-NP datagram carrying the Echo Request at the time that the response was generated. As such, the difference between the initial value of the hop count field and the reported value is the number of hops to the responding system. Similarly, the Source Time Stamp field is the locally generated time stamp that accompanied the outgoing datagram carrying the original Echo Request.

D3 SERVICES ASSUMED FROM THE LOWER LAYERS

D3.1 PERFORMANCE REQUIREMENTS

D3.1.1 Required Error Performance of the Subnetwork Service

The required error performance of the Subnetwork service depends on the requirements of the particular mission incorporating the SCPS-NP. Missions may specify a required probability that a SCPS-NP datagram be routed to the correct destination. This probability is affected by the probability that the data in the SCPS-NP header has been corrupted by bit-errors. Figure D-1 shows the relationship between SCPS-NP header length, bit-error rate, and the probability that the SCPS-NP header is not corrupted.

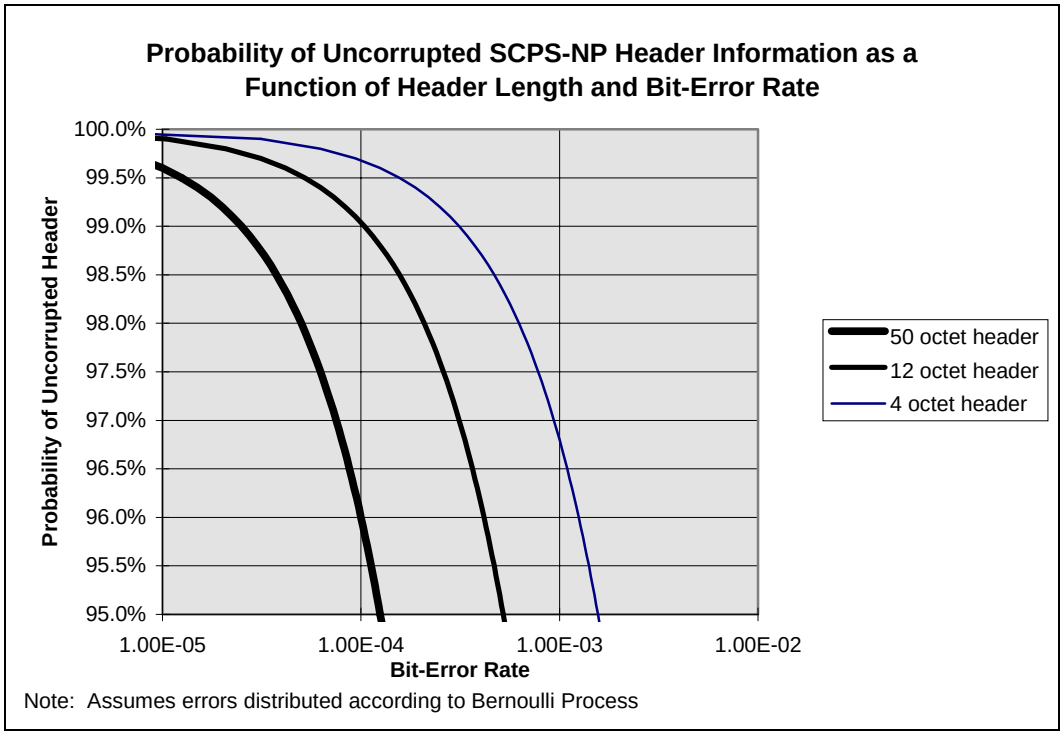


Figure D-1: Effects of Bit-Errors on Integrity of SCPS-NP Header Information

This probability is based on an assumption that errors are distributed according to a Bernoulli process, and may therefore be affected if link-layer error correction techniques are applied to achieve the listed bit-error rate. Missions should regenerate this graph accordingly if their error distributions differ. The purpose of this graph is to assist missions in determining whether the error characteristics exhibited by the data link layer to the SCPS-NP are adequate to meet the mission's requirements regarding the probability of misrouted data. The mission should decide which SCPS-NP capabilities will be used, in order to determine the appropriate SCPS-NP header length. Equation 1 provides the formula for determining the probability that a SCPS-NP header is corrupted. In this equation, BER is the Bit-Error Rate of the link, and N is the number of octets in the SCPS-NP header.

$$P\{\text{SCPS - NP Header Corrupted}\} = 1 - (1 - BER)^{8N} \quad (1)$$

Figure D-2 shows the probability that one or more bit errors affecting the SCPS-NP header will *not* be detected if the header is protected by the Header Checksum (refer to subsection 3.2.3). As with figure D-1, these computations assume that bit-errors are distributed according to a Bernoulli process. The Internet checksum is confounded when two bits spaced a multiple of 16 bits apart have opposite values. Therefore, these computations calculate the probability of a datagram's being affected by two-bit errors, then halve that to reflect the opposite-value requirements, and then use combinations to calculate the proportion of two-bit errors that will be spaced a multiple of 16 bits apart. Note that these computations consider only the first- and second-order error effects (the probabilities of one and two bit errors affecting the SCPS-NP header).

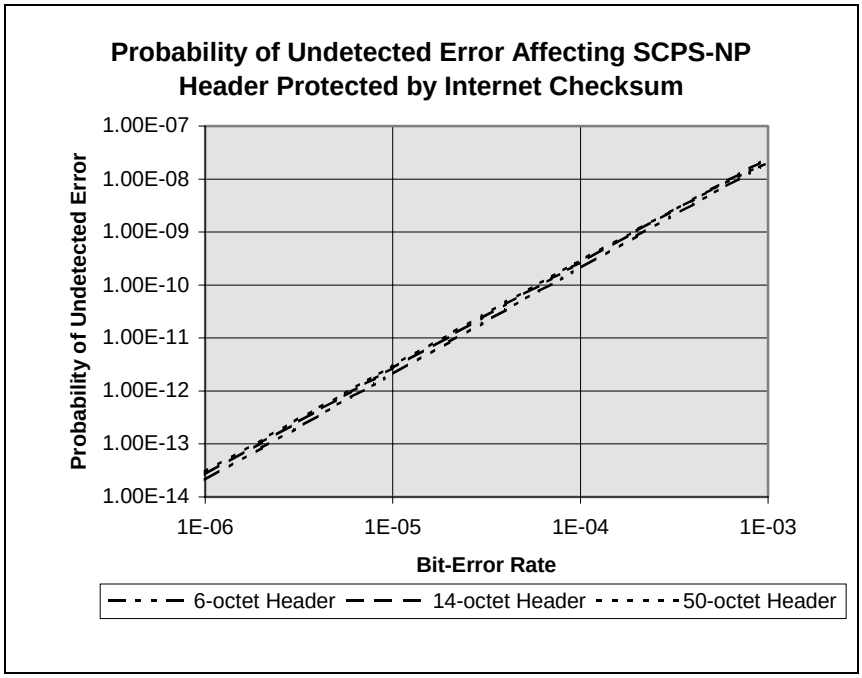


Figure D-2: Probability of Undetected Bit Errors' Affecting SCPS-NP Header When Protected by Internet Checksum

The equation for calculating the curves shown in figure D-2 is given in equation 2.

$$P\{\text{Undetected Error}\} \cong \left\{BER^2 \cdot (1 - BER)^{(8N-2)}\right\} \cdot \left\{\frac{\binom{\frac{N}{2}}{2}}{\binom{8N}{2}} \cdot 0.5 \cdot 16\right\} \quad (2)$$

In equation 2, BER is the bit-error rate and N is the number of octets in the header. The first term of the equation, delimited by curly braces, calculates the probability of the header's being affected by *exactly* two bit errors. The second term calculates the probability that those two errors will affect opposite-valued bits spaced a multiple of 16 bits apart. Note that, as

before, if a Bernoulli process is not a sufficiently accurate estimation of the error process for a particular mission, that mission should modify equation 2 accordingly.

D3.1.2 Probability of correct datagram transmission

The service provided by the SCPS Network is an unreliable one, meaning the network protocol does not provide acknowledgment and retransmission capability. However, the SCPS Network provides for routing options, specifically flood routing, which can increase the probability of correct datagram receipt without retransmission. However, this is at the cost of greatly increased traffic throughout the network. The specifics of exactly how much traffic is generated and the extent of any improvement in reliability depend on the topology of a specific network.

The following graph illustrates the probability of correct datagram transmission for datagrams of various lengths, given a range of bit-error rates presented to the SCPS-NP by the underlying subnetwork and an error distribution consistent with a Bernoulli process. The operation of the SCPS-NP (in the absence of flood routing) neither improves nor degrades this performance. Missions must determine their reliability requirements and the effect of any retransmission protocols at higher layers on their ability to sustain the bit-error rate presented to the SCPS-NP.

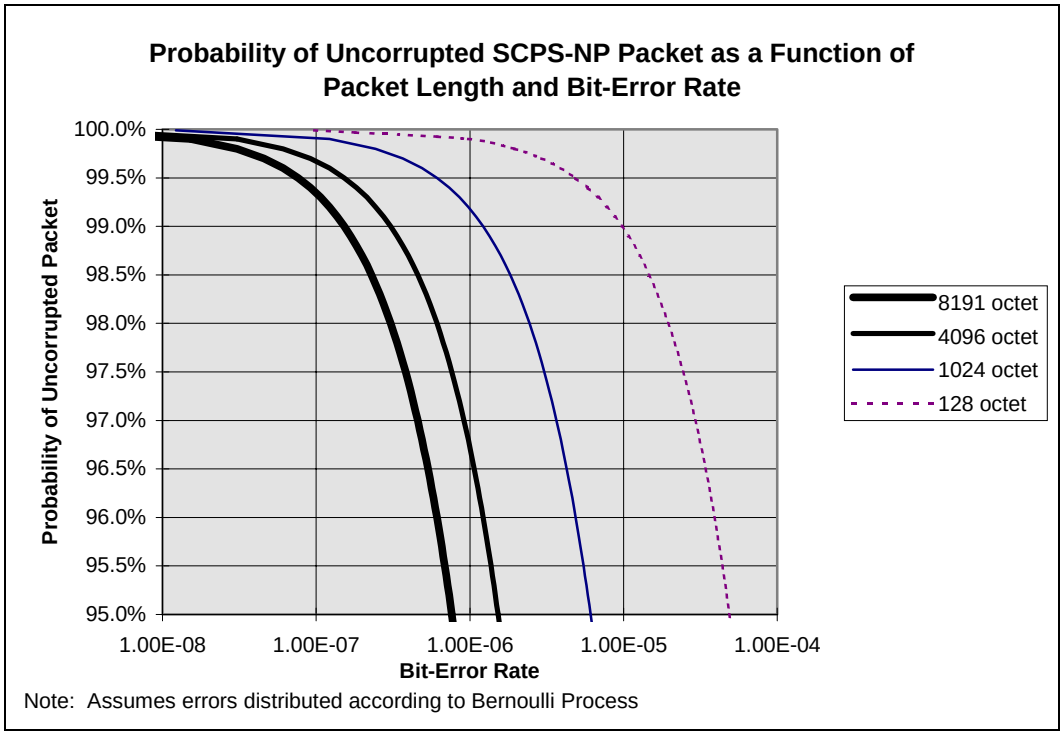


Figure D-3: Probability of Uncorrupted SCPS-NP Datagram as a Function of Datagram Length and Bit-Error Rate

The equation used to generate the graph in figure D-3 is identical to equation 1, with *N* set to the entire length of the datagram rather than just to the length of the SCPS-NP header.

D3.2 SERVICES ASSUMED FROM UNDERLYING LAYERS

The SCPS-NP is designed to operate over a wide variety of underlying communication services, either at the data-link layer or the network layer of the OSI reference model. One consistent characteristic of the underlying service assumed by the SCPS-NP is that the service not require explicit connection establishment and connection release. For underlying services that *do* require such operations, a 'Subnetwork-Dependent Convergence Function' may be developed to emulate a connectionless service.

The SCPS-NP requires a minimum set of services from underlying protocols. This subsection presents an abstraction of those services. However, the manner in which those services are provided and the specific protocols used to provide them are outside the scope of this Recommendation. We refer to the abstraction of underlying protocols as the 'subnetwork', and the services provided by the subnetwork as 'subnetwork services'.

The SCPS-NP requires the subnetwork (SN) unit data service (SN-UNITDATA) of the underlying data link layer. The form of the service primitives is shown below:

SN-UNITDATA.request	(SN-Destination_Address, SN-Source_Address, SN-Quality_of_Service, SN-SDU)
SN-UNITDATA.indication	(SN-Destination_Address, SN-Source_Address, SN-Quality_of_Service, SN-SDU_Length, SN-Interface, SN-SDU)

The specifics of the subnetwork UNITDATA primitives are subnetwork-dependent. All parameters to the SN-UNITDATA.request and SN-UNITDATA.indication primitives are optional except the SN-SDU parameter and the SN-SDU_Length parameter (on the indication primitive).

The SN-Destination_Address and SN-Source_Address parameters are subnetwork dependent and maintained in the physical address information tables, specified in 4.1.3.9, for use in SN-UNITDATA.requests.

The only element of SN-Quality_of_Service of which the SCPS-NP will make use is the priority element. When priority is supported by a subnetwork, a local mapping between SCPS Network precedence and the subnetwork priority shall be defined for generation of the SN-UNITDATA.request primitive.

The SN-UNITDATA.request primitive should be able to accept an SN-SDU of at least 256 octets in length. SN-UNITDATA.requests generated by SCPS-NP will not exceed 8191 octets in length.

The underlying subnetwork service shall provide the length of the received SN-SDU on an SN-UNITDATA.indication. The local implementation of the subnetwork service shall provide the identity of the subnetwork interface from which the SCPS-NP datagram was received.

In addition to the services required for data transmission, the SCPS Network requires information from network management or supporting subnetwork entities regarding the availability and quality of the subnetwork services (as presented to the SCPS-NP). This information is requested and provided in the following service primitives: SN-FACILITY.request and SN-FACILITY.indication.

SN-FACILITY.request	(SN-Interface, SN-Interface_Status, SN-Outbound_Subnetwork_Status, SN-Inbound_Subnetwork_Status, SN-Outbound_MTU, SN-Inbound_MTU, SN-Outbound_Data_Rate, SN-Inbound_Data_Rate)
SN-FACILITY.indication	(SN-Interface, SN-Interface_Status, SN-Outbound_Subnetwork_Status, SN-Inbound_Subnetwork_Status, SN-Outbound_MTU, SN-Inbound_MTU, SN-Outbound_Data_Rate, SN-Inbound_Data_Rate)

The SN-FACILITY.request is generated by the SCPS-NP to determine the status of a particular subnetwork (e.g., a link) via its local interface. The association of interfaces with particular communication subnetworks is a locally managed issue. The SN-Interface parameter of the SN-FACILITY.request is supplied by the subnetwork service user (i.e., SCPS-NP). The remainder of the parameters are results that shall be provided by the subnetwork service.

There are no requirements placed on the SCPS-NP regarding the frequency with which SN-FACILITY.requests are issued.

The SN-FACILITY.indication is issued by the subnetwork service provider independent of any request by the subnetwork service user, typically to report a change in the state of a particular subnetwork.

The parameters of the SN-FACILITY.request and SN-FACILITY.indication are identical. The format of the local interface identifier is system dependent. The interface status indication shall include at least the following values: 'interface up', 'interface down'. The interface status indication may provide optional values, including but not limited to the following: 'interface degraded', 'interface in test'.

The outbound subnetwork status and inbound subnetwork status parameters shall include at least the following values: 'available', 'out', 'corrupted', 'congested', and 'status unknown'. Criteria for transitioning between these states is subnetwork and implementation dependent.

The SN-Outbound_MTU indicates the largest data unit, in octets, that may be submitted to the interface for transmission.

The SN-Inbound_MTU indicates the largest data unit, in octets, that may be received from the interface.

The SN-Outbound_Data_Rate indicates the data rate, in bits per second, at which data will be transmitted over the interface.

The SN-Inbound_Data_Rate indicates the data rate, in bits per second, at which data are received over the interface.

D4 SERVICES ASSUMED FROM THE OPERATING ENVIRONMENT

SCPS-NP assumes that the operating environment provides the ability to interrogate a clock resource to obtain the current time of day. This is used both for timestamp generation purposes and, in the event that clocks are synchronized throughout the network, to provide routing loop control.

SCPS-NP assumes that buffer memory is available to queue datagrams when transient bursts in the arrival rate of data temporarily exceed the outbound subnetwork capacity. The amount of buffer memory dedicated to SCPS-NP queuing is a local issue.