Network Working Group
Requests for Comments 1277

S.E. Hardcastle-Kille
University College London

November 1991

Encoding Network Addresses to support operation over non-OSI lower layers

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The OSI Directory specifies an encoding of Presentation Address, which utilises OSI Network Addresses as defined in the OSI Network Layer standards [CCI88] [ISO87a]. The OSI Directory, and any OSI application utilising the OSI Directory must be able use these Network Addresses to identify end systems. Currently, OSI applications are often run over lower layers other than the OSI Network Service. It is neither reasonable nor desirable for groups wishing to investigate and use OSI Applications in conjunction with the OSI Directory to be dependent on a global OSI Network Service. This document defines a new network address format, and rules for using some existing network address formats. The scope of this document is:

1. Any TCP/IP network supporting COTS using RFC 1006.

2. Any mapping of COTS onto X.25 (usually X.25(80)), where X.25 is not used to provide CONS (i.e., only DTE and not Network address is carried).

The approach could also be extended to use with other means of providing COTS (or CLTS). It is not appropriate for use where CONS or CLNS is used to provide COTS (or CLTS).

1 Introduction

The OSI Directory specifies an encoding of Presentation Address, which utilises OSI Network Addresses as defined in the OSI Network Layer standards [CCI88] [ISO87a]. The OSI Directory, and any OSI application utilising the OSI Directory must be able use these Network Addresses to identify end systems.

Currently, OSI applications are often run over lower layers other than the OSI Network Service. It is neither reasonable nor desirable for groups wishing to investigate and use OSI Applications in conjunction with the OSI Directory to be dependent on a global OSI Network Service. This RFCdefines mechanisms to encode addressing information within Network Addresses, in order to support this type of working. In particular, support is defined for RFC 1006 mapping of COTS onto TCP/IP and COTS mapped onto X.25(1980) [RC87, CCI80].

Where an OSI application is run over CLNS on the internet, the NSAP Guidelines of RFC 1237 should be followed [CGC91].

This document must be read in the context of ISO 8348 Addendum 2 [ISO87b]. It will not be meaningful on its own.

1.1 Historical Note

This document was originally published as UCL Research Note RN/89/13 and as a project THORN internal document [Kil89]. It was devised in response to two projects which faced this requirement, and was agreed as a common approach. The projects were:

- The THORN project, which is an Esprit Project building an OSI Directory [SA88].
- The ISODE project [Ros90], and in particular the QUIPU directory being developed at UCL [Kil88].

The proposal has been implemented, and the viability of the solution demonstrated.

2 Problem Statement

When utilising the OSI Directory, the OSI location of an End System will be determined by a Network Address, which is taken from a Presentation Address, looked up in the OSI Directory.

OSI applications are currently operated over the following lower layers.

- An international X.25 network, which routes on the basis of X.121 addresses. By and large this is X.25(80), but some parts are now

X.25(84) and will carry Network Addresses as user data. OSI Transport is mapped onto the variant of X.25 which is available.

- Large private X.25 networks, which do not have DNICs, but are otherwise similar to the previous (in particular Janet).
- Isolated networks running Connection Oriented Network Service (e.g., Pink Book Ethernets).
- Isolated networks running Connectionless Network Service (e.g., MAP LANs).
- The Connectionless Network Service Protocol (CLNP) pilot, currently taking place in the NSFNet and NORDUNet communities.
- Isolated TCP/IP LANs, utilising RFC 1006 to support the OSI Transport Service[RC87].
- The DARPA/NSF Internet, using RFC 1006.

In general, these systems need to be interconnected by the use of transport bridging or application relaying. Operation of transport bridges causes a number of problems which it is desirable to avoid. Only some applications can support relaying, and this is not always satisfactory.

2.1 The "Right Solution"

It is worth noting briefly what the intended (OSI) solution is. There is a single global network service. Network Addresses are globally allocated, and do not imply anything about routing or location. An End System is attached to one or more subnetworks at Subnetwork Points of Attachment (SNPAs). Intermediate Systems join subnetworks, again being attached at SNPAs. Routing is achieved by repeated binding of Network Address to SNPA (initially at the Originating End System, and then at each Intermediate System). This binding is achieved by network level routing mechanisms.

This can only work in a pure OSI environment with a single ubiquitous network service (either connectionless or connection-oriented), and so is not sufficient for the problem being addressed by this note.

2.2 General Approach

This section describes the use of network addresses, and gives a functional overview of the problem being takceled. The means of connecting to a remote Application Entity is broadly as follows.

1. Look up the Application Entity in the OSI Directory to obtain the Presentation Address [1].
2. Extract each Network Address from the Presentation Address, and determine if it can be used (and how).
3. Determine an order of preference for the Network Addresses.
4. Attempt to connect to one or more of the Network Addresses.

This note is concerned with the second step, and will probably have implications on the third. There is currently no directory service to provide step 2, and so this (interim) approach must be algorithmic. All addressing information required for the network must be extracted from the network address.

This note describes the use of Network Addresses for networks which do not provide the OSI Network Service (CLNS or CONS), and places constraints on the use of X.121 form network addresses when used for an OSI Network Service. The following types of Network Address are discussed in this note:

- Use of X.121 form Network Addresses.
- A special encoding of Telex form Network Addresses.

3 Network addresses with X.121 AFI

This note defines an approach for use of network addresses with the X.121 AFI.

The IDP of network addresses is used to allow worldwide administration of the NSAP address space. As such, not all values of the IDP will in practice have topological significance (which implies that in some cases the IDP will not be sufficient for network layer routing). However, it is recommended that any End System using the Connection Oriented Network Service and with access to the international X.25 service uses the X.121 form of NSAP address relative to its access point. This allows routing across the worldwide X.25 based public data networks to be based on the X.121 addresses. Allocation of DSP (Domain Specific Part) within this form of address is a private issue.

The IDP is primarily an allocation mechanism, and the user (end system) cannot in principle assume any implied routing. However, due to the lack of a network directory service, it is recommended that any End System with Connection Oriented Network Service and access to the international X.25 service uses X.121 form relative to its access point. Allocation of DSP (Domain Specific Part) is a private issue.

[1] Strictly an Application Entity should have only one Presentation Address. In practice it may have several, and the network addresses of each Presentation Address should be considered.

Conversely it is recommended that if an X.121 IDP (Initial Domain Part) form Network Address is interpreted, then the X.121 address will provide a route (by defining an SNPA on the international X.25 network). There may be additional and perhaps preferable routes which can be determined by private means.

If the DSP is absent, the form should be interpreted as implying a mapping of Transport onto X.25(80).

4 New Network Address Format

This section defines a new network address format. The scope of this format is currently:

1. Any TCP/IP network supporting COTS using RFC 1006.
2. Any mapping of COTS onto X.25 (usually X.25(80)), where X.25 is not used to provide CONS (i.e., only DTE and not Network address is carried), except where the international X.25 service is used and no PID or CUDF is required.

   These exceptions are the cases which are handled by use of X.121 AFI (Section 3). The intention is to use the X.121 AFI wherever possible, and the formats defined in this section are for the remaining cases.

The approach could also be extended to use with other means of providing COTS (or CLTS). It is not appropriate for use where CONS or CLNS is used to provide COTS (or CLTS).

4.1 Requirements

The requirements for use of OSI over existing networks not supporting CONS or CLNS, when using the OSI Directory are:

1. The information for the layers below Transport must be obtained from the Network Address. This is essential, because we wish to use the OSI Directory in a standard manner, and the Network Address is the information available.
2. The Network Addresses must be globally unique, as they can be looked up by anyone with access to the Directory.
3. The Network Address should be allocated so that confusion with a "real" Network Address (i.e., one which defines an NSAP using CONS or CLNS as opposed to X.25(80) or RFC 1006) is unlikely.

4. Network Addresses must be interpretable on the basis of a well known information, or on information which can be obtained from the (application level) OSI Directory. (This RFConly uses well known information).

5. The identity of the network in question must be deducible from the Network Address

6. All network specific addressing information (including the SNPA) must be deducible from the Network Address

4.2 IDP Choice

The IDP is used with Telex AFI. The Telex AFI is used because:

- It gives the largest DSP
- It is less likely than other forms to be used for "real" Network Addresses

The following AFIs might have been chosen, but are not used for the reasons given:

- Local (the values must be globally unique)
- X.121 (because it may be confused with other uses of OSI network addresses)
- DCC and ICD (because it may be confused with other uses of OSI network addresses)

The IDI should be assigned in a manner appropriate to the use of the encoding. For example, for operation on a private network within an organisation, the telex number of that organisation would be a good choice. Some well known networks are given assignments in Appendix A.

4.3 The DSP Encoding

The network address is used as follows.

- A (sub)network is identified by the IDP and a *small* part of the DSP.
- The remainder of the DSP encodes network specific information

The DSP format is now defined. The top level format is independent of the means used to provde COTS. Two formats for the remainder of the DSP are then defined, for specific means of providing COTS.

A decimal abstract encoding is defined for the DSP. The ECMA 117 format might have been used, but it is not suitable. [TC386]. Use of a binary encoding, with the DSP structured in ASN.1 would have been a very attractive approach. However, there is insufficient space in the Network Address for this to be feasible.

The following structure is defined:

Digit	1-2	3-27
Meaning	Prefix	Network Specific

2 digits Prefix. This allows for multiple usage of the same DSP, by not consuming it all. It also allows for the DSP to be used with different encodings.

Network Specific The network specific allocation should be less than 20 digits if this DSP structure is to be used with any IDI format. This is increased to 27 for the Telex format.

The IDP + 2 digit prefix identify a subnetwork in which the value of the remainder of the DSP (Network Specific Part) is to be interpreted.

4.4 X.25(80) Network Specific Format

The IDP/Prefix identifies an X.25(80) subnetwork. There is a need to represent a DTE Number, and optionally an X.25 Protocol ID or CUDF (many implementations require these due to shortage of X.121 address space) in the DSP. This is structured in one of two possible ways:

Digit	1	Remainder
Meaning	0	DTE

Digit	1	2	3 – (n*3)+2	Remainder
Meaning	Type	PID/CUDF Length	PID/CUDF	DTE
Values	1 or 2	n		

The network specific part is structured as follows:

Type This has the following values

- **0** DTE only
- **1** DTE + PID
- **2** DTE + CUDF
- **3-9** Reserved

PID/CUDF Length The length of the PID/CUDF in octets

PID/CUDF The PID/CUDF takes as many digits as indicated by 3 times octet 2. Each octet of the PID/CUDF is encoded as three decimal digits, representing the decimal value of the octet.

DTE The DTE is terminated by the end of the Network Address.

For example, the JANET DTE 000005111600 with ASCII CUDF "12" would be encoded in the following way. The first lines describe the abstract notation. Note that where the IDI is not of maximum length, that the translation to concrete decimal is not mechanical

Part	IDP		DSP			
Comp	AFI	IDI	Prefix	Dte+Cudf	Len	CUDF + DTE
Octet			1-2	3	4	5-20
Value	Telex	007 28722	02	2	2	049050 000005111600
Ct Dec	54	007 28722	02	2	2	049050 000005111600
Ct Bin	54	00 72 87 22	02	22		04 90 50 00 00 51 11 60 0f

Note that concrete binary is representing octets in hexadecimal. This is the syntax most likely to be used in practice. The CUDF is represented by two octets 049 and 050 (decimal), which map to six digits.

4.5 TCP/IP (RFC 1006) Network Specific Format

The IDP and 2 digit prefix identifies a TCP/IP network where RFC 1006 is applied. It is necessary to use an IP Address, as there are insufficient bits to fit in a domain. It is structured as follows:

Digit	1-12	13-17 (optional)	18-22 (optional)
Meaning	IP Address	port	Transport Set

For TCP/IP there shall be a 20 digit long network-specific part. First 12 digits are for the IP address. The port number can be up to 65535, and needs 5 digits (this is optional, and is defaulted as defined in RFC 1006). Finally, there is a third part to the address, which is defined here as "transport set" that indicates what kind of IP-based transport protocols is used. This is a decimal number from 0-65535 which is really a 16-bit flag word. 1 is TCP, 2 is UDP. Further values of this code are assigned by the IANA. If the transport set is not there or no bits are set, it means "default" which is TCP. This is encoded in 5 digits.

For example, the IP Address 10.0.0.6 with port 9 over UDP is encoded as:

Part	IDP		DSP			
Component	AFI	IDI	Prefix	IP Address	Port	T Set
Octet			1-2	3-14	15-19	20-24
Value	Telex	007 28722	03	010 000 000 006	00009	00002
Cncrt Dec	54	007 28722	03	010 000 000 006	00009	00002
Cncrt Bin	54	00 72 87 22	03	01 00 00 00 00 06	00 00 9	0 00 02

5 Encoding

This document describes allocation of Network Addresses, with the DSP considered in Abstract Decimal. The encoding of this for use in protocols (typically as Concrete Binary) is described in ISO 8348 Addendum 2 [ISO87a].

6 References

References

[CCI80] CCITT. Recommendation X.25, interface between DTE and DCE for packet mode terminals, 1980.

[CCI88] The Directory — overview of concepts, models and services, December 1988. CCITT X.500 Series Recommendations.

[CGC91] R. Colella, E. Gardner, and R. Callon. Guidelines for OSI NSAP Allocation in the Internet. Request for Comments 1237, NIST, July 1991.

[ISO87a] Information processing systems - data communications - network services definition: Addendum 2 - network layer addressing, March 1987. ISO TC 97/SC 6.

[ISO87b] ISO DIS 7498-3 on naming and addressing, May 1987. ISO/IEC/JTC-1/SC 21.

[Kil88] S.E. Kille. The QUIPU directory service. In *IFIP WG 6.5 Conference on Message Handling Systems and Distributed Applications*, pages 173–186. North Holland Publishing, October 1988.

[Kil89] S.E. Kille. An interim approach to use of network addresses. Research Note RN/89/13, Department of Computer Science, University College London, February 1989.

[RC87] Marshall T. Rose and Dwight E. Cass. ISO Transport Services on top of the TCP. Request for Comments 1006, Northrop Corporation Technology Center, May 1987.

[Ros90] M.T. Rose. The ISO development environment: User's manual (version 6.0), January 1990.

[SA88] F. Sirovich and M. Antonellini. The THORN X.500 distributed directory environment. In *Esprit Conference Week*, November 1988.

[TC386] ECMA TC32. Domain specific part of network layer addresses. ECMA Standard 117, ECMA, June 1986.

7 Security Considerations

Security considerations are not discussed in this memo.

8 Author's Address

Steve Hardcastle-Kille
Department of Computer Science
University College London
Gower Street
WC1E 6BT
England

Phone: +44-71-380-7294

EMail: S.Kille@CS.UCL.AC.UK

A Allocations for well known networks

A.1 Values

This appendix gives an allocation for three well known networks. All are allocated on the basis of the supposed Telex number 00728722. This number is being used in pilot operations, and so is retained here.

Net	Telex	Prefix
International X.25	007 28722	01
Janet	007 28722	02
Darpa/NSF Internet	007 28722	03
IXI	007 28722	06

The international X.25 allocation is only used where a CUDF or PID is needed. In other cases, an X.121 form Network Address with no DSP should be used.

A.2 Delegation

The values assigned in this document are now in widespread use. As the number is arbitrary, it would be undesirable to change the numbers without a sound technical reason. However, it is important to guarantee that the numbers are stable.

This Internet Draft commits UCL not to reassign the portions of the number space allocated here.

The DARPA/NSF Internet space (Prefix 03) is delegated to the IANA.