ECMA

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

# LAYER 4 TO 1 ADDRESSING

## TR/20

March 1984

Free copies of this document are available from ECMA,
European Computer Manufacturers Association
114 Rue du Rhône – 1204 Geneva (Switzerland)

ECMA
EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

# LAYER 4 TO 1 ADDRESSING

## TR/20

March 1984

TABLE OF CONTENTS

# 1 General

# 1. GENERAL

## 1.1 Scope

To facilitate compatible interconnection of data processing equipment conforming to the Open Systems Interconnection architecture and protocols, this Technical Report ECMA TR/20:

- describes the general principles of OSI addressing;
- describes the syntax and semantics of addresses carried in certain protocols operating in layers 4 to 1 of the OSI Reference Model.

The following are outside of the scope of this Technical Report:

- the syntax and semantics of OSI Names or Titles;
- the encoding of addresses passed across real service interfaces;
- the rules governing Connection End Point identifiers, Protocol Reference Numbers and the like.

## 1.2 References

| | |
|---|---|
| ECMA-72 | Transport Protocol |
| ECMA-80 | Local Area Networks (CSMA/CD Baseband) Coaxial Cable System |
| ECMA-81 | Local Area Networks (CSMA/CD Baseband) Physical Layer |
| ECMA-82 | Local Area Networks (CSMA/CD Baseband) Link Layer |
| ECMA-92 | Connectionless Internetwork Protocol |
| IEEE Project 802 | Local Network Standards |
| ISO 7498 | Data Processing - Open Systems Interconnection - Basic Reference Model |
| CCITT Rec. S.70 | Network-Independent Basic Transport Service for Teletex |
| CCITT Rec. X.25 | Interface between Data Terminal Equipment and Data Circuit Terminating Equipment for Terminals operating in the Packet Mode on Public Data Networks |
| CCITT Rec. X.121 | International Numbering Plan for Public Data Networks |

## 1.3 Definitions

### 1.3.1 Reference Model Definitions

The following terms in this Technical Report have the definition given in ISO 7498.

#### 1.3.1.1 Address

An identifier which tells where an (N)-service-access-point may be found.

1.3.1.2 Entity

An active element within an (N)-subsystem.

1.3.1.3 Layer

A subdivision of the OSI architecture, constituted by subsystems of the same rank.

1.3.1.4 Link Layer

The Data Link layer provides functional and procedural means to establish, maintain and release data-link-connections among network-entities and to transfer data-link-service-data-units. A data-link-connection is built upon one or several physical connections.

1.3.1.5 Network Layer

The Network layer provides the means to establish, maintain and terminate network-connections between systems containing communicating application-entities and the functional and procedural means to exchange network-service-data-units between transport-entities over network connections.

1.3.1.6 Physical Layer

The Physical layer provides mechanical, electrical, functional and procedural means to activate, maintain and deactivate physical connections for bit transmission between data-link entities. A physical connection may involve intermediate systems, each relaying bit transmission within the Physical layer. Physical layer entities are interconnected by means of a physical medium.

1.3.1.6 Protocol

A set of rules (semantic and syntactic) which determines the communication behaviour of (N)-entities in the performance of (N)-functions.

1.3.1.6 Service

A capability of the (N)-layer and of the layers beneath it, which is provided to (N+1)-entities at the boundary between the (N)-layer and the (N+1)-layer.

1.3.1.7 Service Access Point

The point at which (N)-services are provided by an (N)-entity to an (N+1)-entity.

1.3.1.8 Sub-Layer

A subdivision of a layer.

1.3.1.9 Subnetwork

A set of one or more intermediate systems which provide relaying and through which end systems may establish network-connections.

1.3.1.1Ø <u>Title</u>

A permanent identifier for an entity.

1.3.1.11 <u>Transport Layer</u>

The Transport layer optimizes the use of the available network-service to provide the performance required by each session-entity at minimum cost.

1.3.2 <u>Additional Definitions</u>

For the purpose of this Technical Report the following additional definitions apply.

1.3.2.1 <u>Domain</u>

A part of an address space which is subject to uniform control.

1.3.2.2 <u>Domain Identifier (D-ID)</u>

The means whereby a domain is unambiguously specified.

1.3.2.3 <u>Data Terminal Equipment (DTE)</u>

A piece of data processing equipment which is connected to a public or private sub-network. This extends the use of the term DTE which normally refers to an equipment attached to a public sub-network.

1.3.2.4 <u>Flat Address</u>

An address with no internal structure which is constructed without reference to any lower layer address.

1.2.3.5 <u>Gateway</u>

A set of functions which effect the interconnection of subnetworks, also known as an interworking unit.

1.2.3.6 <u>Hierarchic Address</u>

An address which is constructed relative to a lower layer address; it consists of the lower layer address plus a selector component as a suffix.

1.3.2.7 <u>Individual Address</u>

An address which identifies a single Service Access Point.

1.3.2.8 <u>Multicast Address</u>

An address which identifies one or more Service Access Points.

1.3.2.9 <u>Partitioned Address</u>

An address built from a set of nested addressing domains which is constructed without reference to any lower layer address.

1.3.2.10 Selector

The suffix of a hierarchic address which specifies a Service Access Point relative to a lower layer Service Access Point.

1.3.2.11 Service Access Point Identifier (SAP-ID)

The means whereby a Service Access Point is specified within a protocol.

1.3.2.12 Source Routing

The selection by the originating system of the route that a message should take to reach its destination.

1.3.2.13 Sub-domain

A domain which is considered part of a larger domain; domains never overlap and are always strictly nested.

1.3.2.14 Sub-domain Address (SDA)

An address which unambiguously specifies a Service Access Point within a sub-domain.

1.3.2.15 Synonymous Address

One of a set of addresses which all specify the same Service Access Point.

1.3.2.16 Well-known Address

An address which always identifies the same Service User.

## 1.4 Acronyms

The following acronyms are used in this Technical report.

| | |
|---|---|
| CSMA/CD | Carrier Sense, Multiple Access with Carrier Detection |
| D-ID | Domain Identifier |
| DTE | Data Terminal Equipment |
| L | Link |
| N | Network |
| Ph | Physical |
| SAP | Service Access Point |
| SAP-ID | Service Access Point Identifier |
| SDA | Sub-domain Address |
| SN | Subnetwork |
| T | Transport |

# 2 Addressing Principles

# 2. ADDRESSING PRINCIPLES

## 2.1 Introduction

This section discusses some general addressing principles which are elaborated in later sections.

## 2.2 Concept of an Address

The Reference Model defines an Address as the identifier of a Service Access Point (SAP). Layer entities using a Service attach themselves to its SAPs, but never more than one entity per SAP at a time. Addresses therefore identify entities indirectly. The association between an entity and an SAP may be fixed or variable. Entities have location independent permanent identifiers, called Titles in the Reference Model. The Title to Address mapping as performed by a directory function, is therefore always one-to-one or one-to-many, and may be fixed or variable.

It is also useful to allow an SAP to have several synonymous addresses. For example, the same SAP could have a local or a global address for use according to the context.

A general picture of addressing within a layer is shown in Figure 1.

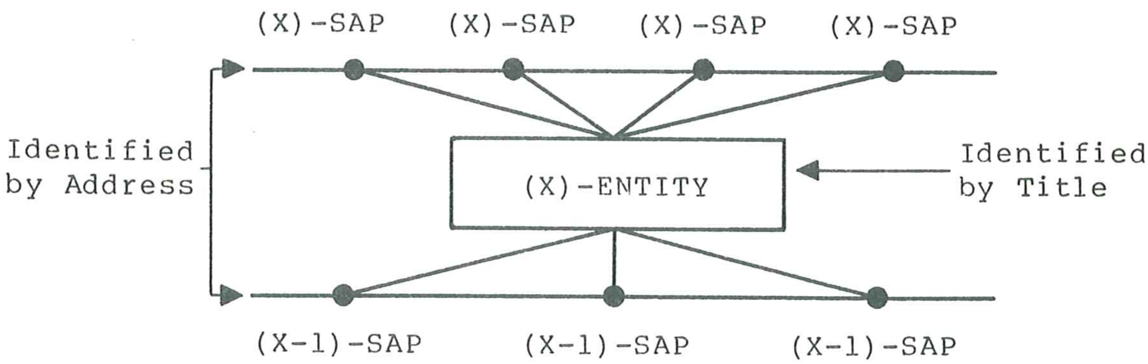


Fig. 1

Note that management of the directory function to achieve variability of association between (X)-entities and (X-1)-SAPs is the subject of continuing study.

## 2.3 Address Structuring

An address may be Flat, Hierarchic or Partitioned. In the flat case the addresses for a layer are allocated without regard to the addresses in any lower layer. In the hierarchic case the address for a layer is constructed from the address in the next lower layer plus a Selector component for the layer itself. This is represented in pictorial form in Figure 2 next page.

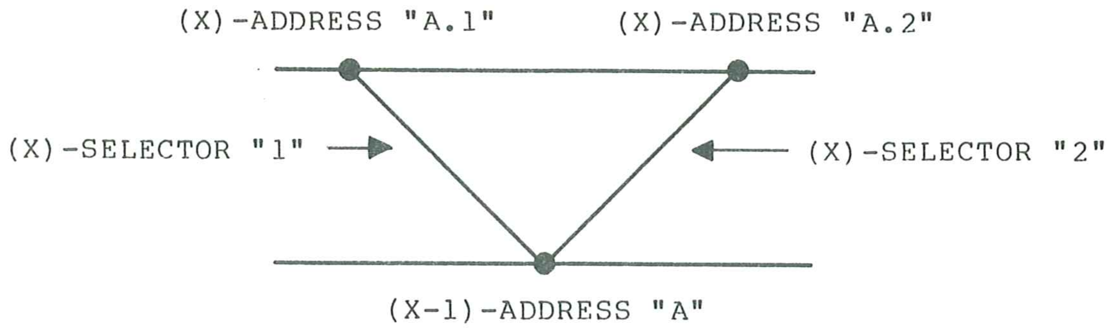


Fig. 2

An example of hierarchic addressing can be seen in the extended addressing of the Transport layer in the Teletex environment (see Rec. S.70, 1.2).

The term hierarchic is also used in other work to describe the case where the layer address space is divided into domains, these into sub-domains, and so on. To avoid confusion, the term partitioned is used in this document for this case. Domains never overlap and sub-domains are always strictly nested within domains. In pictorial form this can be represented as a tree, see Figure 3.

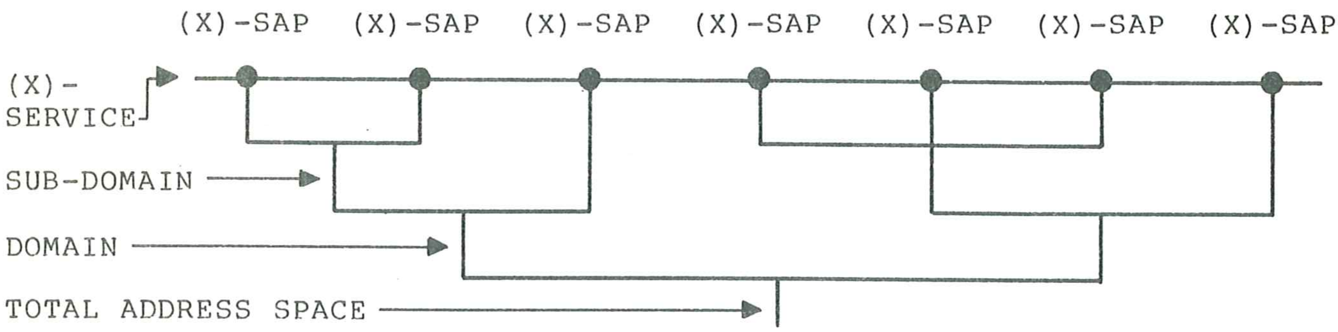


Fig. 3

At any level in this tree an address may be identified by two components: the Domain Identifier (D-ID) and the Sub-domain Address (SDA). The Sub-domain Address may of course be further sub-divided, hence the address structure is recursive. The smallest possible domain is one SAP, but in practice it is unlikely that addressing schemes will go down to this level of granularity. The general structure of a partitioned address is therefore:

Domain Identifier + Sub-domain Identifier +...+ Sub-domain Address.

A partitioned address may be constructed in a top-down or bottom-up fashion. Top-down construction requires the initial appointment of a global address administration. This administration may allocate portions of the gobal address space to subordinate administrations, and so on.

Bottom-up construction allows independent administrations to allocate addresses as they wish. If these independent administrations have to merge then they must agree to form a higher level authority whose sole purpose is to allocate address prefixes to distinguish the different administrations.

Following the terminology of Standard ECMA-72, the address field of a protocol is called a Service Access Point Identifier (SAP-ID). In the flat or partitioned case the SAP-ID carry full addresses. In the hierarchic case the SAP-ID carry the selector values.

The partitioned addressing scheme is considered to provide the principles for sub-addressing and can also be considered as a way to distribute the routing function within a layer.

## 2.4 Address Manipulation

In abstract terms, a Request to a layer conveys the address of the destination SAP. The layer processes this address to obtain two addresses: the address to be carried in the layer protocol, and the address to be passed in the Request to the next lower layer. Of course, a layer protocol may not require any addressing information. At the destination, the original destination address is reconstituted from the protocol address and the lower layer address. Source addresses are processed in the same fashion. The general picture of addressing within a layer is represented in Figure 4.

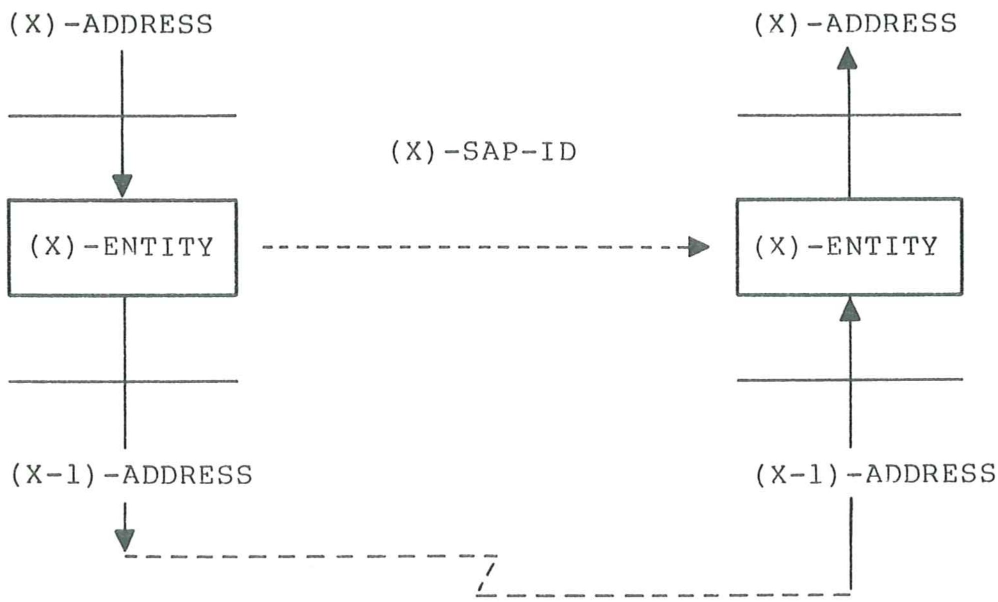


Fig. 4

In the flat or partitioned case the address processing is complex and in general requires appeal to layer management directory facilities. In the hierarchic case the address processing is particularly simple: the selector components are peeled off the end in the outward direction and are

appended in the inward direction.
The encoding of the address passed across a real service interface is implementation-dependent. For example, it could be the index to an address table, an abbreviated address, the address strings as they would be encapsulated in lower layer protocols, or even the title of the entity attached to the remote SAP. The only requirement for an address parameter is that it should unambiguously specify the SAP.

2.5 Addressing within Layers 4 to 1

Within the lower four layers there are three important service boundaries at which addressing takes place:

- the Transport Service (layer 4): here the objective is to identify the data processing functions supported by the telecommunications capability;

- the Network Service (layer 3c): here the objective is internet-wide unambiguous Network Addresses;

- the Sub-Network Service (layer 3a): here the address structure is pre-determined and the address values are imposed by the sub-network authority;

Sections 3.1, 3.2 and 3.3 consider addressing for these three service boundaries.

2.6 Addressing within Sub-Layers

Addressing within sub-layers is a requirement, particularly for the Network layer. However, it is understood that this may be in conflict with the definition of sub-layering in the Reference Model. This requires further study.

# 3 Addresses Definition

# 3. ADDRESSES DEFINITION

## 3.1 Transport Addresses

### 3.1.1 Introduction

The scope of this section is the definition of Transport Addresses and their encoding in Standard ECMA-72.

### 3.1.2 Description of Standard ECMA-72

Standard ECMA-72 defines address parameters to be carried in Connection Request and Connection Confirm TPDUs. These are called Transport Service Access Point Identifiers (TSAP-IDs). The structure and allocation of the address values is not defined.

### 3.1.3 Interpretation

The Reference Model requires both Network Addresses and Transport Addresses to be globally unique. The Network Address serves to specify the end system; higher layer addresses merely identify SAPs within the end system. It is therefore natural to construct all addresses above the network layer hierarchically. This takes advantage of the global uniqueness of Network Addresses and offers simple fan-out within the end-system. Using the terminology of section 2, the Standard ECMA-72 TSAP-ID is used to carry a Transport Selector component. This is represented in pictorial form in Figure 5.

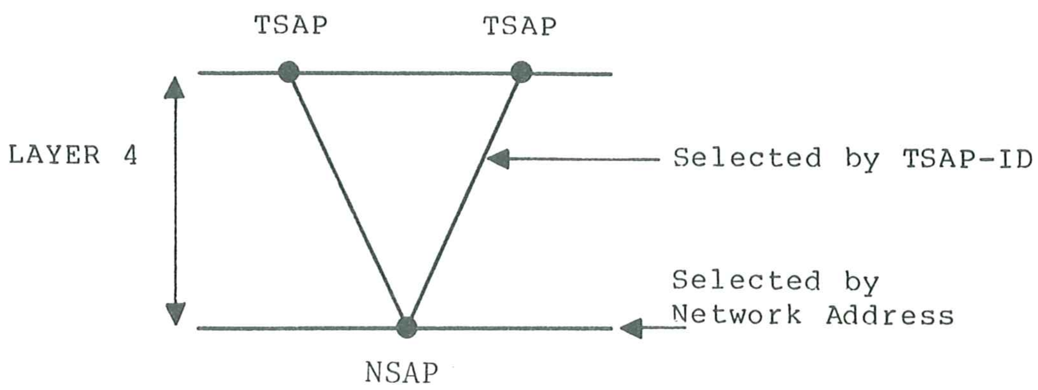


Fig. 5

If the TSAP-ID is not supplied in the Transport Protocol a single TSAP is supported by the NSAP.

### 3.1.4 TSAP-ID Address Field

TSAP-IDs may have standard values (which are globally administered) or non-standard values (which are privately administered). TSAP-IDs may carry full Transport Addresses (in the flat or partitioned case) or Transport Selectors (in the flat or partitioned case). The kind of TSAP-ID is indicated by an initial Type octet in the TSAP-ID value field as defined in

Figure 6.

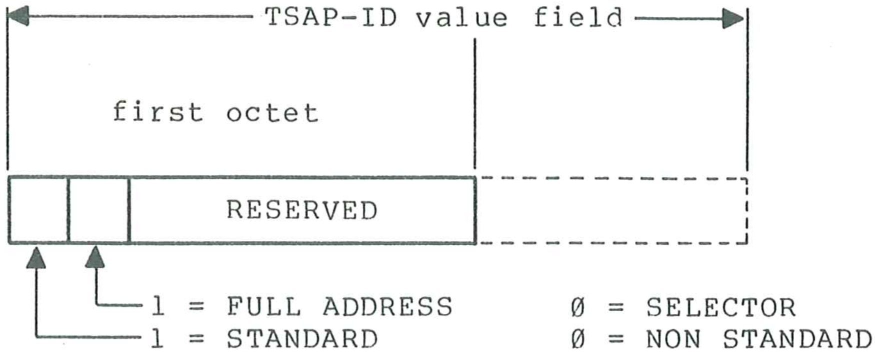


Fig. 6

The length of the TSAP-ID is for further study.

## 3.2 Network Addresses

### 3.2.1 Introduction

The scope of this section is the definition of the addressing structure in the Network layer and its encoding in the Internet Protocol.

### 3.2.2 Description of Standard ECMA-92

Standard ECMA-92 defines a variable length format Internet Protocol datagram which contains variable length Destination and Source Network Addresses. The structure and allocation of these address values is not defined.

### 3.2.3 Interpretation

The Reference Model requires Network Addresses to be unambiguous within an internet. The Network Address serves to specify the end-system. Sub-network Addresses are allocated by the sub-network authority and are in general not globally unique. The most natural choice of Network Address is a partitioned one as described in section 2.3.

No fixed relationship between network addressing domains and sub-networks is assumed. However, it is required that an addressing domain consists of one or more integral sub-networks or that a sub-network consists of one or more integral domains. This ensures that a mapping can be made from the abstract network addressing domains to the real sub-network address spaces. The Domain Identifier (and possibly also part of the Sub-domain Address) is used by Internet Entities to route a message to an appropriate gateway for that domain. Once the domain is reached, the Sub-domain Address is used to perform routing within that domain. At some level of the Network Address a Domain Identifier may correspond to a Sub-network Identifier. Similarly, a Sub-domain Address may correspond to a Sub-network Address. Although the Network Address is in

principle always quoted in full, administrations may choose to allow the use of abbreviated addresses, address escape codes, etc.
An appropriate gateway for a domain does not necessarily imply any possible gateway into that domain. For example, a gateway on the boundary of two domains may have knowledge of both, be jointly under the administrative control of both, and may be considered to be within both domains. Also, in some situations the choice of gateway may depend on the destination within the domain. Examples of this include:

- geographically large networks in which the grade of service and/or charging is a function of distance.

- partitioned networks.

Network Service Access Points (layer 3c) are supported by Sub-network Service Access Points (layer 3a). The sub-network addressing capability varies, of course, from one sub-network to another. However, it is sufficient to view a sub-network as providing a number of SNSAPs in a manner which is of no concern to the upper part of the Network layer. Section 3.3 discusses sub-network addressing for a number of different types of sub-networks.

The Network Harmonisation sub-layer (3b) is concerned with providing a homogeneous service across all sub-networks and so is involved with service enhancement and de-enhancement; it does not confer any addressing capability of its own. It follows that there are as many 3b SAPs as there are 3a SAPs. Traffic through an NSAP may pass through more than one SNSAP if alternative or parallel routes are possible, through possibly different sub-networks; this requires one NSAP to be supported by more than one SNSAP. There is then a need for address fan-in in layer 3c. No requirement has been identified for address fan-out in layer 3c using a suffix to the Network Address. In pictorial form the addressing structure proposed in the Network layer is described in Figure 7 next page.

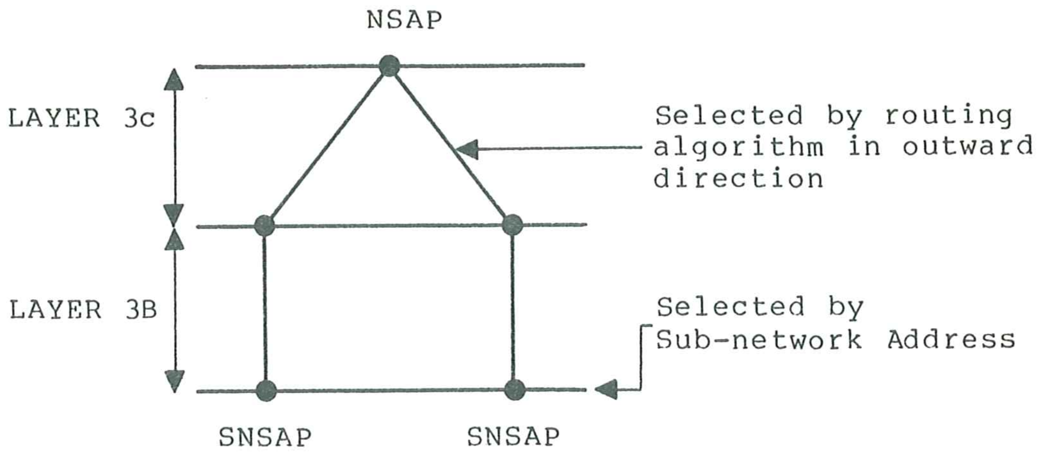


Fig. 7

### 3.2.4 Internet Address Field

The foregoing arguments lead to the choice of a multi-component address field as defined in Figure 8.

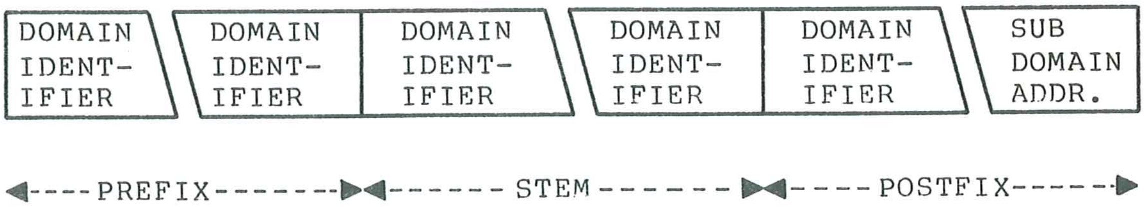


Fig. 8

A Network Address consists of a string of digits, which from one point of view may be considered as a list of Domain Identifiers followed by a Sub-domain Address. Each Internet entity parses this string according to its own knowledge into three parts:

- Prefix - the part which conveys no information to the entity (i.e. it indicates the current domain, which the entity is aware of anyway).

- Stem - the part which is used by the entity to determine the onward route of the message to the next Internet entity.

- Postfix - the part which the entity is unable to interpret and which is passed along with the unchanged Network Address to the next Internet entity.

### 3.2.5 Specific Applications

The most important benefit of the Internet Address format above is that it allows a wide variety of addressing styles to be encompassed. It therefore avoids designing the Internet Protocol around a particular addressing technique. Since the outcome of addressing studies cannot be predicted with confidence at present, it is felt that the Internet Protocol should be designed for flexibility. By way of example the following styles of addressing can easily be accommodated:

- Sub-network identifier + host identifier.
- X.121 address.
- XEROX Ethernet address.
- Private one-level or multi-level schemes.

### 3.2.6 Other Requirements

A number of other network addressing issues are for further study:

- Source Routing
  In specialised cases it will be necessary to specify part or all of a route; possible reasons for doing so include diagnostic testing and forcing part of a route for cost or security reasons. Source routing could be achieved by including "via" parameters or "route selection criteria" parameters. This issue is considered to be an Internet protocol matter only.

- Multicast Addresses
  It is important to be able to invoke sub-network multicast addressing facilities at the Network Service. It would be feasible to provide a Multicast Network Address feature, which was translated into sub-network multicast addresses or into a number of sub-network individual addresses. The characteristics of particular sub-networks (e.g. whether they support multicast and if so, how) must be hidden by the Network Service.

- Well-Known Addresses
  The concept of a well-known address is needed for services whose location is dynamically established. This is needed for mobile or distributed systems and where the same service is offered in a number of places.

## 3.3 CSMA/CD Addresses

### 3.3.1 Introduction

Standard ECMA-82 defines two link level address fields: the "DTE Address" and the "LSAP". The scope of this section is the definition of the structure and allocation of these addresses.

### 3.3.2 Description of Standard ECMA-82

Standard ECMA-82 defines the DTE Address as comprising 6 octets. The first two transmitted bits of this are the "Multicast" and "Locally Administered" flags. The first bit selects a group of DTEs when it is set to ONE, and selects an individual DTE when it is set to ZERO. The second bit indicates a locally administered address when it is set to ONE, and indicates a globally administered address when it is set to ZERO. No further structure for the remaining bits is defined, except that all bits of the DTE address set to ONE mean "broadcast" (i.e. all DTEs).

ECMA-82 defines the LSAP as comprising a single octet. The first transmitted bit is the "Multicast" flag which selects a group of LSAPs when it is set to ONE, and selects an individual LSAP when it is set to ZERO. No further structure for the remaining bits is defined, except that all bits of the LSAP set to ONE mean "broadcast" (i.e. all LSAPs in the DTE).

### 3.3.3 Interpretation

Like all addresses, the DTE Address and LSAP fields select Service Access Point. The obvious interpretation for the DTE Address is that it selects a physical LAN station. The obvious interpretation for the LSAP is that it selects a logical component within the specified station. Note that in the terminology of section 2.3, the LSAP field should properly be called an LSAP-ID and is a Selector. Since the two address fields are link layer mechanisms, they play the role defined in Figure 9.

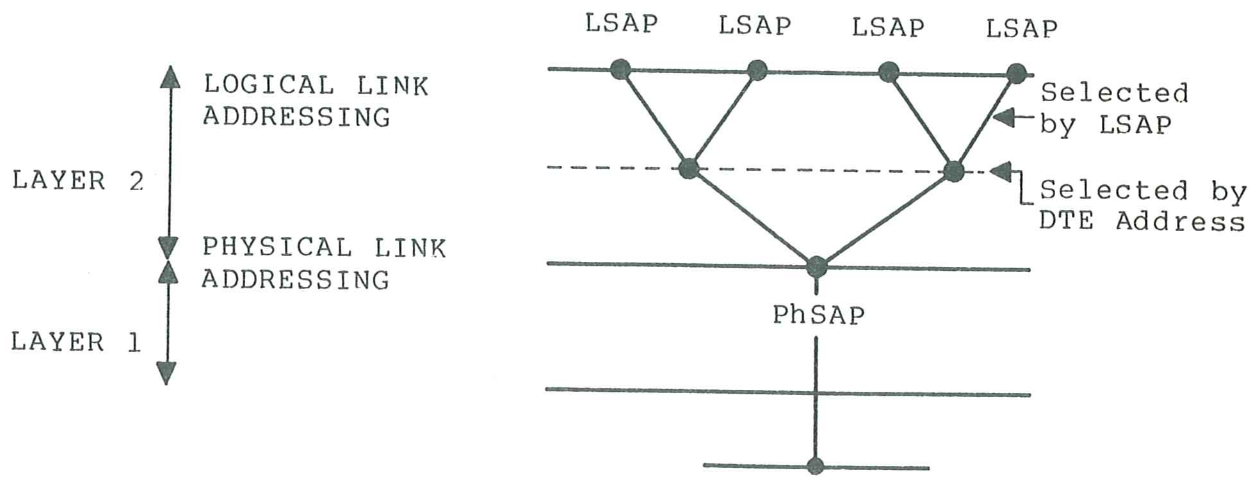


Fig. 9

Note that in this particular case the DTE address is a Link layer address, whereas for X.25 (see section 6) it is a Network layer address.

### 3.3.4 DTE Address Field

#### 3.3.4.1 Individual and Globally Administered

For globally administered addresses the XEROX Ethernet address scheme is used for the following reasons:

- It is simple and offers adequate addressing capabilities.
- It is in widespread use already.
- An effective scheme exists to ensure global uniqueness.

The XEROX scheme is that blocks of DTE addresses are allocated to suitable applicants. These blocks consist of $2^{24}$ unique address values which are administered by the applicant to ensure uniqueness in his own equipment. These blocks correspond to settings of the last 3 octets transmitted of the DTE Address field. It is recommended that these addreses are allocated densely; they must not be used for any purpose other than addressing (e.g. they must not be used to indicate equipment type or location). XEROX ensure uniqueness of these address blocks by prescribing a 3-octet value which the applicant must use as the first part of the DTE Address transmitted. This value uniquely identifies the applicant and has its first two bits transmitted reserved to allow for the Multicast and Locally Administered flags. In pictorial form the scheme employed is defined, in transmission order, in Figure 10.

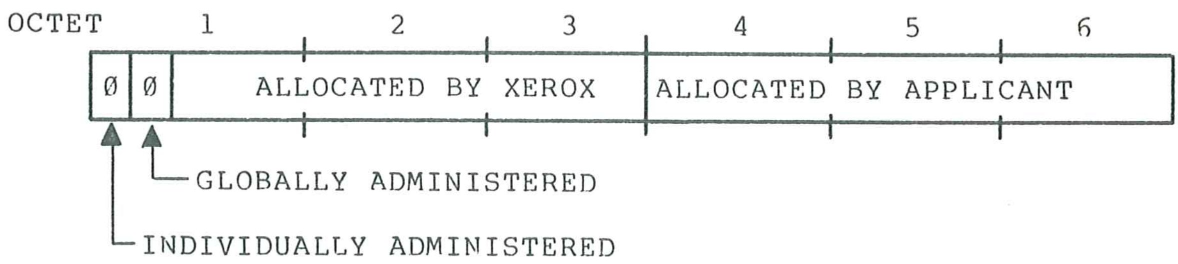


Fig. 10

#### 3.3.4.2 Individual and Locally Administered

This combination is for further study. Some interesting possibilities that might be considered are:

- Structuring the DTE Address into Sub-network Identifier and Station Identifier fields; this would facilitate the construction of efficient LAN-LAN link layer bridges.

- Conveying the private part of an X.121-like address; this would facilitate the adoption of a global network addressing scheme covering both public and private sub-networks.

- Some entirely private scheme.

In order to allow these schemes to co-exist, further address flags may be defined following the two current ones.

3.3.4.3 Multicast and Globally Administered

Global multicast addresses are formatted exactly as for global individual addresses, except that the leading bit is set to ONE to indicate Multicast. This allows ample scope for the definition of multicast addresses without the risk of different manufacturers or administrators accidentally choosing the same values. The possibility of defining certain standard values for the last 3 octets is for further study. A source multicast address should not be precluded. In pictorial form the scheme proposed is defined, in transmission order, in Figure 11.

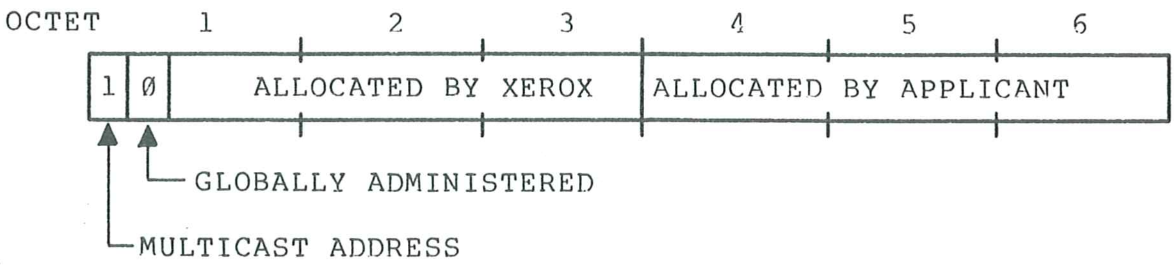


Fig. 11

3.3.4.4 Multicast and Locally Administered

This is for further study. The same format as for local individual addresses would be desirable, except that the leading bit would be set to indicate Multicast.

3.3.5 LSAP Field

The addressing scheme developed by IEEE Project 802 is employed. The first transmitted bit when set indicates Multicast (in the case of a Destination LSAP) and Response (in the case of a Source LSAP). The first transmitted bit when unset indicates Individual (in the case of a Destination LSAP) and Command (in the case of a Source LSAP). The second transmitted bit is set to indicate standard values. Non-standard values are always subject to private administration. Standard values are the subject of further study.

3.3.5.1 Individual or Command

The combination of a Multicast DTE Address with an Individual LSAP is permitted. In pictorial form the scheme proposed is defined, in transmission order, in Figure 12.


Fig. 12

Multiple LSAPs may be necessary to distinguish between sub-network service users (e.g. layer 3b protocol entity or a management entity).

3.3.5.2 Multicast or Response

Multicast is the subject of further study in the case of a Destination LSAP. For a source LSAP the following scheme defined in Figure 13 is used.

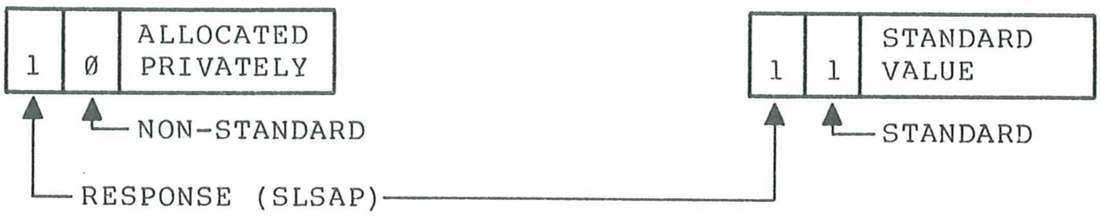


Fig. 13

## 3.4 X.25 Addresses

### 3.4.1 Introduction

X.25 DTE addresses are formatted in accordance with Recommendation X.121. The scope of this section is the meaning of addresses in X.25 and the use of sub-addressing.

### 3.4.2 Description of Recommendation X.121

X.121 is the CCITT Recommendation which defines addressing for Public Data Networks. X.121 specifies two formats for addresses, see Fig. 14 next page.

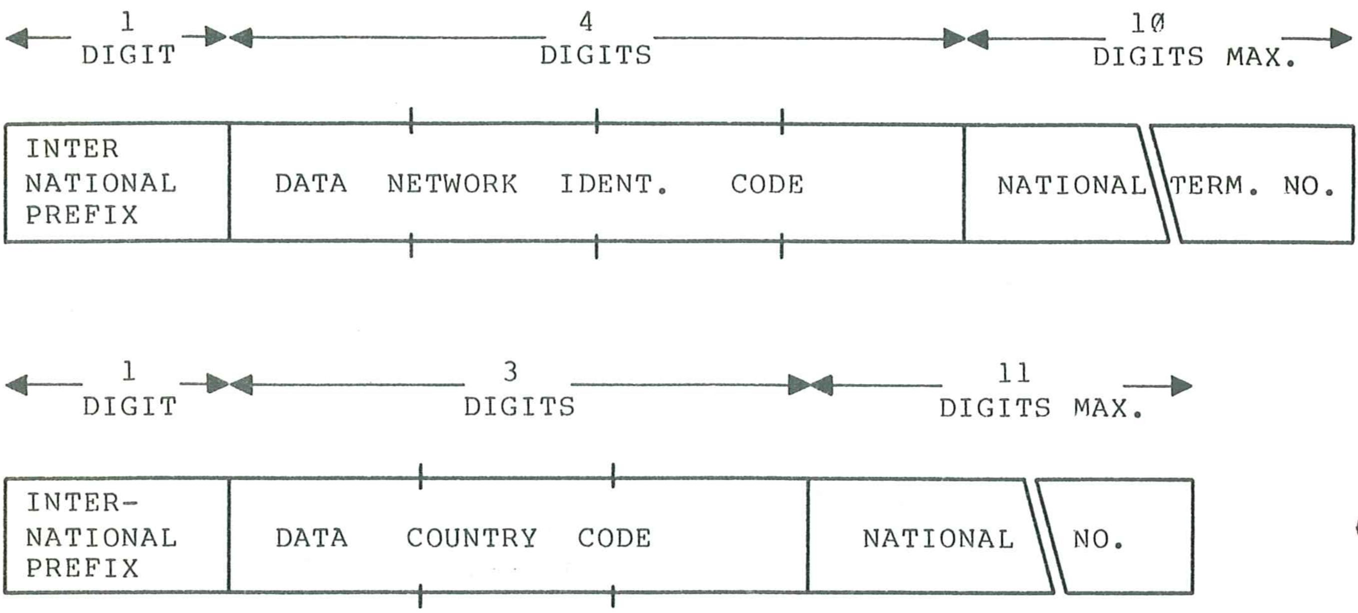


Fig. 14

X.121 does not mention sub-addressing, but it is common for individual authorities to allow some of the trailing address digits (typically one or two) to be used for this purpose. Such sub-addresses are conveyed transparently by the sub-network and are processed by the DTE.

### 3.4.3 Interpretation

#### 3.4.3.1 Link Level Address

X.25 link level carries the usual kind of HDLC address. It is important to realize, however, that this is only to distinguish commands and responses, and that it does not perform any address fan-out. The link level addresses are also conventional and so do not need to be conveyed across the sub-network.

#### 3.4.3.2 Packet Level Address

X.25 packet level carries an X.121 address in call packets to identify the DTE. This is a sub-network SAP (layer 3a) identifier, but it also implies the Link and Physical SAPs because there is no lower layer addressing. If sub-addressing is used this has the effect of fan-out in layer 3a.

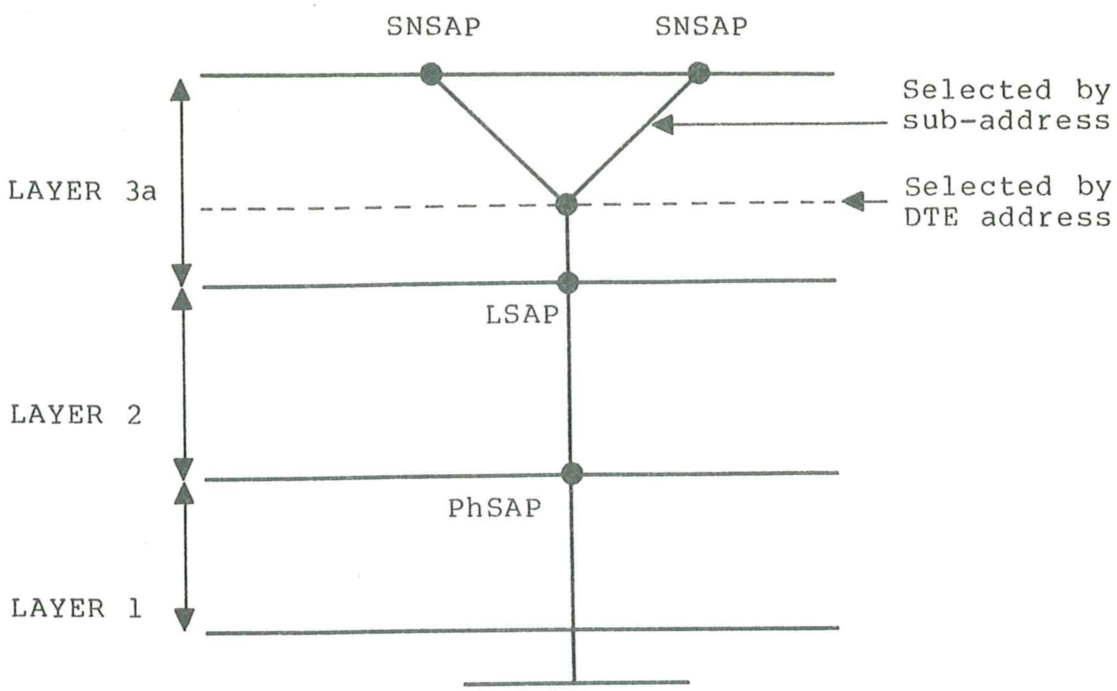


Fig. 15

Note that in this particular case the DTE address is a Network layer address, whereas for CSMA/CD (see section 3.3) it is a Link layer address.

3.4.4 DTE Address Field

For public X.25 networks this is prescribed by the network authority. The extension of X.121 addressing to cover private sub-networks is the subject of current debate in CCITT. A scheme has been proposed for structuring the National Terminal Number into two components: a Private Network Identifiation Code (4 digits) and a Private DTE Number (6 digits maximum).

3.4.5 Sub-address Field

The size or even presence of this field varies from one X.25 network to another. Multiple SNSAPs may be necessary to distinguish between sub-network service users (e.g. a layer 3b protocol entity or a management entity). If multiple SNSAPs are required but sub-addressing is not possible, then the sub-address must be carried in the call packet user data.

Some X.25 networks may not, however, be totally transparent to call user data. As one means of overcoming variability in the handling of sub-addresses between different X.25 networks, it is tentatively proposed that call user data always be used. See also section 4 on an alternative means of fanning out to NSAPs. It is noted that CCITT is actively working on the subject of sub-addressing: it is ECMA's intention to follow this work.

# APPENDIX A

## ITEMS FOR FURTHER STUDY

The following items are for further study:

- Addressing within sub-layers (see 2.6).

- TSAP-ID length and standard values (see 3.1.4)

- Internet Address encoding (see 3.2.4).

- Network source-routing, multicast Network Address capability, and Well-Known Network Address capability (see 3.2.6).

- CSMA/CD standard Multicast and Globally Administered DTE Address, and format of Locally Administered DTE Addresses (see 3.3.4).

- CSMA/CD standard LSAP Addresses, and Multicast LSAP Addresses (see 3.3.5).

- X.121 extensions for Global Network Addresses (see 3.4.4).

- X.25 sub-addressing (see 3.4.5).

Further considerations are needed for the following aspects which relate to the layer management functionality:

- Location and format of inter-network routing information.

- Addressing directory functionality and maintenance considering the issue of validity of end-system components.