ECMA
EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

AN ARCHITECTURAL FRAMEWORK FOR PRIVATE NETWORKS

ECMA TR/44

2nd Edition - December 1989

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

Phone: +41 22 735 36 34 Fax: +41 22 786 52 31

ECMA
EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

AN ARCHITECTURAL FRAMEWORK FOR PRIVATE NETWORKS

ECMA TR/44

2nd Edition - December 1989

BRIEF HISTORY

This ECMA Technical Report has been developed in response to growing industry recognition of the inadequacy of all existing and previous reference models to cover the domain of private networks.

The roots of these available reference models are all of different origin and are based on particular communication aspects, representing only a fraction of the full range of considerations relevant to private networks. The ISO OSI Reference Model, for example, does not adequately cover the real aspects of all the various kinds of networks encountered in practice, e.g. LANs, ISDNs and multidrop configurations.

To respond to these recognized inadequacies and deficiencies this Technical Report establishes a common architectural framework, itself provided by five logically-related companion models whose structure, principles and features are presented and explained.

Although they have their origins in several international standards and reports concerned principally with the Network and lower layers of the OSI Reference Model, the architectural concepts and global framework provided by this Technical Report invite the reader to venture beyond the constraints of OSI into a wider, generic realm offering universal applicability.

In reaching beyond OSI to encompass the domain of networking in its entirely it has, understandably, proven difficult to preserve full compatibility with the ISO OSI Reference Model; generalities have been found useful, necessary and inevitable. Equally, attempts have been made when defining the architecture to maintain a measure of consistency with the CCITT ISDN Protocol Reference Model and the IEEE 802.1 Reference Model for Local Area Networks.

It has to be recognized that the progressive and necessary development of architectural concepts addressed previously in a plethora of ECMA, CCITT, ISO, IEEE and other standards and reports has naturally led to some overlaps in scope and content with respect to the present Technical Report, in particular with regard to:

ECMA TR/13	Network Layer Principles,
ECMA TR/14	LAN Layer 1-4 Architecture and Protocols,
ECMA TR/20	Layer 1-4 Addressing,
ECMA TR/21	LAN Interworking Unit for Distributed Systems,
ECMA TR/25	OSI Subnetwork Interconnection Scenarios permitted within the Framework of the OSI Reference Model,

and with regard to:

ISO 8648	Internal Organization of the Network Layer (IONL), ISO 8802 LAN Standards.

To a large extent the material of ECMA Technical Reports TR/13 and TR/25 should be taken as being superseded by the now stable ISO 8648, to the development of which they contributed, and by this Technical Report. Not superseded by either ISO 8648 or by this Technical Report is the material of Annex A of TR/25 providing the rationale for the development of TR/21.

The non-data environment is also encompassed by the architecture presented in this Technical Report, although the work in this area is considered far from complete and mature. The current status of the work on that subject is nevertheless included, to respond to and accommodate the growing industry interest in the modelling of non-data applications, and data/non-data integration.

It is believed that the global standardization of generic architecture for private networking will be further advanced as the industry progresses further beyond the frontiers of pure data applications and OSI.

Accepted as an ECMA Technical Report by the General Assembly of 14th December 1989.

Table of Contents

SECTION I

GENERAL

1. SCOPE

This Technical Report provides a common architectural framework for the analysis, selection, development and standardization of protocols and protocol sets located below the Network Service boundary as specified in ISO 8348, supporting the transfer of data between Systems attached to Private Networks.

2. FIELD OF APPLICATION

The framework is applicable to data and non-data applications in both dedicated and integrated services private networks.

Furthermore, it is felt that the material is equally applicable to scenarios involving public environments.

3. REFERENCES

ECMA TR/13	Network Layer Principles
ECMA TR/14	LAN Layer 1-4 Architecture and Protocols
ECMA TR/20	Layer 4-1 Addressing
ECMA TR/21	LAN Interworking Unit for Distributed Systems
ECMA TR/25	OSI Subnetwork Interconnection Scenarios permitted within the Framework of the OSI Reference Model
IS 7498-1984	Information Processing Systems - Open Systems Inter-connection - Basic Reference Model, UDC 681.3.1
ISO 8072	Information Processing Systems - Data Processing Systems - Transport Service Definition
ISO 8073	Information Processing Systems - Data Processing Systems - Transport Protocol Specification
ISO 8208	Information Processing Systems - X.25 Packet Level Protocol for Data Terminal Equipment
ISO 8348	Information Processing Systems - Data Communication - Network Service Definition
ISO 8348/AD2	Information Processing Systems - Data Communication - Network Service Definition, Addendum 2: Network Layer Addressing
ISO 8473	Information Processing Systems - Data Communication - Protocol for the provision of the CLNS
ISO 8648	Information Processing Systems - Data Communication - Internal Organization of the Network Layer (IONL)
ISO 8802/1	LAN - Part 1 : General Introduction
ISO 8802/2	LAN - Part 2 : Logical Link Control
CCITT Rec. G.704	Functional Characteristics of Interfaces associated with Network Nodes
CCITT Rec. I.112	Vocabulary of Terms for ISDN

CCITT Rec. I.320	ISDN Protocol Reference Model
CCITT Rec. I.430	Basic User-Network Interface - Layer 1 Specification
CCITT Rec. I.431	Primary User-Network Interface - Layer 1 Specification
CCITT Rec. Q.921/I.441	ISDN User-Network Interface Data Link Layer I.441 Specifications
CCITT Rec. Q.931/I.451	ISDN User-Network Interface Layer 3 Specification I.451
CCITT Rec. X.21	Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Synchronous Operation on Public Data Networks
CCITT Rec. X.22	Multiplex DTE/DCE Interface for User-Classes 3- 6
CCITT Rec. X.25	Interface between DTE and DCE for terminals operating in the packet mode and connected to PDNs by dedicated circuit
CCITT Rec. X.50	Fundamental Parameters of a Multiplexing Scheme for the International Interface between Synchronous Data Networks
CCITT Rec. X.75	Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits between Packet-Switched Data Networks

4. INTRODUCTION

A number of reference models falling within the scope of this Technical Report are already available. Each has its own particular, and to some extent limited, field of application. The OSI Reference Model, for example, is concerned with data applications. It provides, however, little guidance on how to model circuit switched networks and the separate channel signalling mechanisms that might be defined to support circuit switching. Additionally, its provisions are not in accord with the provision of ISO 8802 standards concerned specifically with LAN technology. The ISDN Protocol Reference Model on the other hand models ISDN services and protocols, including signalling, but does not deal with LAN services and protocols.

This Technical Report aims to provide an architectural framework for private networking environments, which include the use of public network services, bringing together these different architectures. In addition, this framework is developed in such a way as to facilitate future extension to cover non-data applications.

As a working strategy, the OSI Reference Model is taken as a basis, and the concepts developed in the OSI Reference Model are used unchanged as far as possible. However, where needed, the OSI concepts are generalized to facilitate adequate modelling of real-world objects.

To establish the new framework, this Technical Report takes the following approach:

i) First, in Section I a set of definitions is given in Clause 5 and some basic concepts are developed and explained in Clause 6. These are all needed to provide a sound basis for the introduction of the material presented in Sections II and III hereafter.

ii) In Section II, three models for a Network Service Provider are developed. The service provider is seen as possibly offering a range of global services one of which might be the OSI Network Service.

All three models are based on protocol layering principles and represent different elaborations on the concepts defined in ISO 8648, specifically the subnetwork concept.

The first model, referred to as the Unconstrained Network Service Provider Model (UNSPM), is one that aims to permit any real network to exist as a subnetwork of the global network irrespective of the standards to which its access protocols may conform. It is based on the observation that given the prior existence of a configuration of real subnetworks the architecture of end systems making use of the configuration will vary dependent on their location and the degree of visibility each has of the access protocols of subnetwork remote from it.

The second model, referred to as Multi Layer Addressing Model (MLAM), focuses on the addressing aspects of a layered architecture. It is based on the observation that addressing is the single most important component of any networking system, and that the addition of new layers is mainly driven by the desire to enrich the addressing capabilities beyond those already available. Starting from the OSI layering principles, a layered addressing architecture is developed, focusing on the relationship between an address in a certain layer, and the addresses in the adjacent layers below and above. The global datum is introduced as the boundary between layers addressing end systems or groups of end systems, and layers addressing entities within an end system.

The third model, referred to as the Constrained Network Service Provider Model (CNSPM) aims to achieve a greater degree of standardization of end system architecture. It adds the constraint that Subnetwork Service boundaries should be restricted to a certain defined set, in order to avoid unnecessary proliferation of protocol stacks. This set includes the layer service boundaries corresponding to the OSI layers 1, 2 and 3, and the sublayer service boundaries corresponding to MAC and LLC.

iii) In Section III, the internal structure of a single protocol is clarified, so that layer 1-4 protocols can be analyzed, understood and compared one with respect to another. This is denoted as the "Generic Layer Architecture (GLA) Model".

iv) Section IV analyses the subnetwork access protocols that have been made subject to International Standardization, in terms of the models developed in Sections II and III.

v) In Section V a composite model for the architecture of end systems and subnetworks for data and non-data is developed. This is done on the basis of a generalization of the UNSPM, allowing application of the latter to any layer of a data or non-data subnetwork or end system. An analysis and classification of relay functions, in combination with the addressing principles developed in the MLAM, is then developed into the Relaying and Addressing based Model. Some applications of the model for non-data relay functions complete the section.

vi) In Section VI the concept of Supplementary Services is investigated. For that purpose, representative Supplementary Services are analyzed with respect to their effect on connections and connection establishment, their visibility to one, the other or both parties, and the relationship of each Supplementary Service with the OSI Network Service primitives.

During the development of this Technical Report some specific material was generated that was considered worthwhile to maintain, but recognized as not constituting an integral part of one of the models mentioned above. This material is therefore attached to the body of this Technical Report as a set of Appendices (Section VII):

Appendix A expands the material of Clause 7 and provides a classification scheme covering all the different mechanisms commonly referred to, sometimes incorrectly, as multiplexers.

Appendix B classifies the various types of connection multiplexing, and introduces the concepts of Continuous Bitstream Oriented (CBO) and Delimited Bitstring Oriented (DBO) services in relation to these different multiplexing types.

Appendix C discusses the distinction between the use of the word "service" by CCITT and the use of the word "service" by ISO.

Appendix D lists the acronyms used throughout this Technical Report.

5. DEFINITIONS

The following set of definitions applies for terms used throughout this Technical Report, in particular in Clause 10. The definitions are ordered logically to avoid forward referencing.

5.1 Real system (system)

A set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, and so on, that forms an autonomous whole, capable of performing information processing and/or information transfer. Access to a system is always across a physical boundary. OSI is concerned with communication between systems, and therefore only applies to communication across physical boundaries.

5.2 Physical medium (medium)

The physical means to interconnect systems.

5.3 End system (ES)

A system which contains application processes, which from the OSI point of view are considered as sources and sinks of information. Communication protocols are expected to support the communication needs of these application processes.

NOTE 1

End systems are modelled by the description of the way in which information is transferred from an application process to the medium and vice versa.

5.4 Intermediate system (IS)

A system which does not contain application processes, and is used only to enable interconnection of other systems through relaying mechanisms at or below the Network Service boundary.

NOTE 2

Intermediate systems are modelled by the description of the way in which information is transferred from medium to medium.

NOTE 3

This definition deviates slightly from the one given in ISO 8648, since this Technical Report also discusses relaying below the OSI Network Layer.

NOTE 4

According to the definition of a system given above, information transfer between application processes within the same system is outside the scope of this Technical Report.

5.5 Syntax check of protocol elements

The checking of conformance to syntactical rules which apply to the internal structure of the PCI-field(s) of a PDU.

NOTE 5

A PDU may also have other attributes that may be subject for checking in a receiving system. Examples are: possible requirements with respect to the minimum or maximum length of the user data field, the possible requirement that the length of the user data field should be an integral number of *octets, and so on. However, in this Technical Report this type of checking will not be considered as syntax checking.*

5.6 Active and passive operations on protocol elements

If an IS has the capability to recognize certain protocol elements belonging to the protocols used over the media to which it is attached, then we say that the IS "operates" on these elements.

If the IS does recognize and check the semantics of these protocol elements (and acts according to these semantics) then we say that the IS operates "actively" on these protocol elements.

If the IS only checks (partially or completely) the syntax of these protocol elements, but does not check the semantics, then we say that the IS operates "passively" on these protocol elements.

Apart from these protocol elements there may be protocol elements which pass the IS unchanged simply because the IS considers these elements as user data, and is therefore not aware of their existence as protocol elements. We then say that the IS does not operate on these elements.

5.7 Actual protocol intervention level (of an IS)

The implied service boundary between protocols or protocol elements on which the IS operates actively, and the protocols or protocol elements on which it operates only passively or does not operate at all.

5.8 Potential protocol intervention level (of an IS)

The implied service boundary between the protocols or protocol elements on which the IS operates passively or actively or reserves the right to do so, and the protocols or protocol elements on which under no circumstances the IS will operate, neither actively nor passively.

NOTE 6

Throughout this Technical Report, all instances of use of the term "intervention level" without further qualification should be read as "actual protocol intervention level".

5.9 Visibility of a system

If a certain system, say system A, executes at least one protocol which has its peer in some other system, say system B, then we say that system B is "visible" to system A.

NOTE 7

This includes the case where system B is an IS.

NOTE 8

Visibility of system B is not affected if some other IS, say system C, is located between systems A and B, and system C has a protocol intervention level which is lower than that of system B.

5.10 Subnetwork (real subnetwork) (SN)

A physical medium (media), or a collection of both equipment and physical media, which form(s) an autonomous whole and which can be used to interconnect systems for the purpose of communications.

If the subnetwork consists of a collection of both equipment and physical media, then it may be represented as an IS (including the media that are used to access the IS).

NOTE 9

There is no identified need to introduce the concept of "abstract subnetwork" since it is felt that this abstraction is already covered by the IS concept.

NOTE 10

This definition deliberately differs from the definitions given in the OSI Reference Model and in ISO 8648, since the latter definitions do not allow a bridgeless LAN to be considered as a subnetwork.

5.11 Interworking unit (IWU)

An intermediate system used to interconnect subnetworks.

NOTE 11

If a number of IWUs are used to interconnect a number of subnetworks, the result can also be seen as a number of subnetworks which interconnect a number of IWUs!

There is therefore no rigid architectural distinction between subnetworks and IWUs.

However, in practice, subnetworks are usually associated with carrier-like networks built to interconnect a relatively large number of geographically distributed systems. These networks usually cover a relatively large geographical area and are usually built in a distributed way. On the other hand, IWUs are usually built in a centralized way and are designed to interconnect a number of existing subnetworks.

Therefore, in practice, the distinction between subnetworks and IWUs is given by the answer to the questions:

- *What was first ?*
- *What has been added to interconnect what was already there ?*

5.12 Subnetwork access protocol

A protocol which has to be executed by a system that wishes to access that subnetwork, irrespective of conformance of that protocol to OSI standards.

NOTE 12

A subnetwork access protocol should be seen as the way in which a subnetwork presents itself to its users (i.e. its attached systems).

NOTE 13

If a subnetwork is present in the form of a collection of equipment which can be represented as an intermediate system (i.e. if it has at least the functionalities of OSI Layer 1), then a subnetwork access protocol consists of those protocols executed over a user-network interface, which are located below the potential intervention level of that subnetwork.

If a subnetwork cannot be represented as an intermediate system (i.e. if it has no functionalities corresponding with any OSI layer), then a subnetwork access protocol mainly encompasses functions supporting the achievement of a fair use of the (shared) medium. In a LAN environment, it usually corresponds with the MAC protocol.

5.13 Subnetwork Access Service

The highest level of service capable of being supported by the subnetwork access protocol, excluding the routing and relaying capability of the subnetwork.

5.14 Potential Subnetwork Service (or potential service supported by the subnetwork)

Subnetwork access service in combination with the routing and relaying capability of the subnetwork.

NOTE 14

Any subnetwork presents itself to an attached system as a certain subnetwork access protocol. The same subnetwork may present itself to different attached systems as different subnetwork access *protocols, supporting the same subnetwork service. The subnetwork access protocol is supported in an attached system by a set of functions, distinct from other functions in that attached system.*

The boundary in that attached system between both sets of functions corresponds exactly with the potential subnetwork service boundary in that attached system.

We may therefore say that any subnetwork generates a certain, well-defined, subnetwork-specific potential subnetwork service boundary in all systems attached to that subnetwork.

NOTE 15

If a subnetwork is present in the form of a collection of equipment, then the subnetwork service boundary in an end system corresponds precisely with the potential protocol intervention level of that collection of equipment. However, if a subnetwork cannot be represented as an intermediate system (such as is the case when end systems are interconnected by a single physical medium), then the subnetwork service boundary in an end system corresponds exactly with the MAC service boundary in that end system.

5.15 Actual Subnetwork Service (or actual service supported by the subnetwork)

Service provided by those elements of the subnetwork access protocol on which the subnetwork actively operates in combination with the routing and relaying capability of the subnetwork service.

NOTE 16

Throughout this Technical Report, all instances of use of the term "subnetwork service" without further qualification should be read as "actual subnetwork service".

5.16 Subnetwork Convergence Protocol

A protocol used on top of a subnetwork service, which creates a new service boundary that is used as the basis for interconnection with one or more other subnetworks.

5.17 Enhancement Protocol

A subnetwork convergence protocol where the original subnetwork service as well as the new service are both explicitly identified in a certain multi-layer model (see Clause 11).

5.18 (N)-Layer Routing

The capability of a system to derive from (at least) the destination (N)-SAP address, the destination (N-1)-SAP address and the local (N-1)-SAP address which are both needed to reach the next peer (N)-entity across the accessed (N-1)-service.

NOTE 17

N denotes a layer or sublayer.

5.19 (N)-Layer Relaying

The capability of an IS to perform the actual forwarding of data in layer (N) from an incoming (N-1)-SAP to an outgoing (N-1)-SAP.

NOTE 18

N denotes a layer or sublayer.

5.20 Global (N) Addressing Domain

The (N) addressing domain consisting of all the (N) SAP addresses in the OSI environment (Global (N) addressing domain is a generalisation of Global Network addressing domain as defined by IS 8348/AD2).

5.21 (N) Addressing Domain

A subset of the Global (N) addressing domain consisting of all the (N) addresses allocated by one or more addressing authorities. ((N) addressing domain is a generalisation of Network addressing domain as defined by 8348/AD2).

5.22 (N) Addressing Sub-domain

A subset of an (N) addressing domain which is disjoint from all other (N) addressing sub-domains of that (N) addressing domain. ((N) addressing sub-domain is an application of the definition of naming sub-domain as given by IS 7498-3 to (N) layer addressing.

5.23 (N) Demesne

The set of (N) SAP addresses of a subset of the (N+1) entities of the OSIE, all members of which are able to exchange (N) service data units of a defined type, with all other members if the subset without calling upon the services of a relaying entity of any kind in layer (N+1) or any higher layer.

Notes :

1. The above definition is framed in the terminology of the OSI Reference model, but with a view to its extension to apply to a wider, Integrated Services environment embracing the OSIE as a sub-environment.

2. In terms of the above definition, (N+1) or higher layer relaying entities may be of various kinds. Some of the examples that may be given are the following :

- *(N+1) relaying entities providing relaying between (N) SAP addresses existing in different Demesnes.*
- *data type converting (N+1) entities between (N) Demesnes supporting non-overlapping sets of (N) services.*

3. It should be noted that the definition can be applied recursively, an (N+1) Demesne being defined as some number of (N) Demesnes interconnected by means of some number of (N+1) relaying entities.

4. An (N) Demesne is to be distinguished from an (N) addressing domain in being an abstract modelling concept divorced from all considerations relating to (N) address allocation and administration.

5.24 Hierarchical Addressing

A method of addressing in which the address an (N) SAP is expressed in terms of (N) prefix, (N) address and/or (N) suffix components.

5.25 (N) Prefix

The component of an (N) address used to identify within an (N) addressing DEMESNE the (N-1) DEMESNE to which the (N-1) address component of the (N) address relates.

5.26 (N) Suffix

The component of an (N) address used to identify within the DOMAIN of the (N-1) address component the (N) SAP to which the (N) address relates.

Notes :

(i) IS 7498-1 defines the concept of an (N) suffix (section 5.4.1.15) but does not defines that of an (N) prefix.

(ii) IS 7498-3 uses the term (N) selector throughout as a synonym for the term (N) suffix but this is nowhere explicitly stated.

(iii) *Nowhere in the range of ISO-OSI source documents is the concept of an (N) prefix defined. However, IS 8348/AD2 (section 7.1) introduces the concept in the form of an initial part of a Network address unambiguously identifying a Network addressing sub-domain of the global Network addressing domain.*

6. BASIC CONCEPTS

6.1 The Generic Header Format Concept

This Clause introduces the concept of Generic Header Formats. These are abstract Protocol Control Information (PCI) structures designed strictly in accordance with the same layering principles as are used to define the system and subsystem architectures they are intended to support.

6.1.1 OSI Reference Model Multi-Layer Header Syntax

The OSI Reference Model is based on the view that a complex protocol should be defined by decomposing it into a set of hierarchically related less complex protocols, each positioned in a certain protocol layer.

Inherent to this hierarchy is the exchange of (N)-layer PCI between (N)-layer peer entities. Layer (N) entities combine (N)-layer PCI with user data received from the adjacent higher layer, and offer the result as a single composite whole to the underlying (N-1)-layer as an (N-1)-SDU.

This means that the coupling of (N) PCI and user data by a transmitting entity, and its corresponding separation by a receiving entity, has to be done without any support of the underlying (N-1)-layer.

The most straightforward (but not the only) way to achieve this is to place a header in front of the user data, and to define the header in such a way that the boundary between it and the user data can be derived from the header itself.

In a multi-layer environment this results in a nested header- structure where a header belonging to a higher layer is located behind a header belonging to a lower layer.

The resulting sequence of headers then precisely reflects the "natural" order of processing steps of a multi-layer protocol within the transmitting and receiving systems (see figure 1).

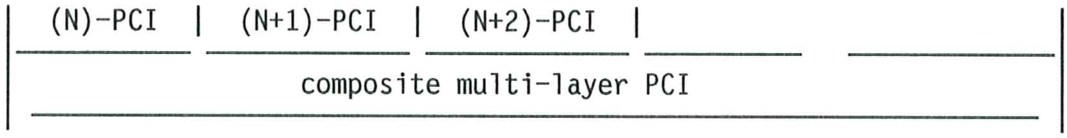


Figure 1 - Nested header structure

The overall structure of a composite header designed in accordance with these principles is referred to as the syntax of the header. For some of the lower layers of the model the (N)-PCI comprises both a header and a trailer. The same nesting principles apply to trailers as to headers.

There is no absolute necessity to define the syntax for a multi-layer protocol set as a sequence of "lesser" headers each belonging to a single layer. Indeed, a composite multi- layer header can also be generated and processed if it exhibits a disordered structure, as long as the syntax rules for this composite header are defined and known. However, it should be emphasized that such a header will be unnecessarily complex for the reason that its processing will require an entity possessing an overall knowledge spanning more than one layer. The existence of such an entity violates the principle of layer-independence. It also prevents a multi-layer protocol set being implemented in a partitioned way. This constraint can only be removed if the header syntax indeed reflects the multi-layer structure it is required to support. Such a header structure will be referred to as "Multi-Layer Generic Header Format" (GHF). Its syntax will be referred to as its "Abstract Syntax".

The GHF should be distinguished from the format which is actually used. This latter format will be denoted as the "Concrete Header Format" and its syntax as its "Concrete Syntax".

Since most protocols which are developed in the context of the OSI Reference Model are based on a definition of layer- specific headers, the structure of which is only relevant for the specific layer, there is no discrepancy between the Generic Header Format and the Concrete Header Format of the multi-layer composite header (a layer 2 header is followed by a layer 3 header, followed by a layer 4 header, and so on). For this reason an (N)-layer protocol can usually very easily be implemented as a distinct software or hardware module, with minimal interactions with other modules supporting protocols in other layers.

Hereafter in this Technical Report, each figure showing a multi-layer structure will be accompanied by a companion figure showing the corresponding Generic Header Format. This header format is intended both to clarify the proposed multi- layer model, and to suggest a concrete format which optimally fits into this structure.

6.1.2 The Single-Layer Generic Header Format (GHF) and Abstract Header Syntax

If a single (N)-layer can be decomposed into a number of sublayers, a corresponding (N)-layer Generic Header Format (GHF) and Abstract Syntax can be defined in exactly the same way as described above for the multi-layer case. Here also, this abstract syntax precisely reflects this decomposition into a number of sublayers, and the same nesting rules apply also in this case. This permits the information operated on by a layer/sublayer to be treated as user data by a lower layer/sublayer. However, in contrast with multi-layer protocols, most single- layer protocol encoding rules do not respect the natural order of processing steps needed to execute the protocol rules, and the corresponding Generic Header Format differs from the chosen Concrete Header Format.

Therefore, a non-monolithic (also called "modular") implementation of these protocols is usually not possible.

This topic is further elaborated upon in Clause 11.

6.1.3 More about the relation between the GHF and the Concrete Header Format

The GHF concept is useful to describe the functionality and internal structure of protocols. It suggests the use of a Concrete Format being a copy of the GHF. However, there may be reasons to have the Concrete Header Format deviating from the GHF.

To illustrate this, consider the way in which a connection is identified during its lifetime in a CO environment. In Clause 11 hereafter it will be shown that the identification of a connection should be modelled as being supported by three sublayers (b1, b2 and b3, see 11.4), each corresponding with a distinct field in the GHF.

In most Concrete Header Formats, however, connection identification is achieved by a single monolithic identifier (channel number, time slot, reference number, and so on), which was agreed during the set-up phase of that connection. In terms of the GHF, we say that this identifier contains "three semantic components" (b1, b2 and b3, see 11.4). But the fact that these three components are not explicitly visible in the Concrete Format inevitably leads to a certain loss of sublayer independence.

Since, however, the introduction of this discrepancy usually leads to a saving in terms of transmission bandwidth, we may not conclude that such discrepancies are always "wrong". For each particular case, the advantages of so doing have to be balanced against the disadvantages.

6.2 Signalling

6.2.1 Introduction

The concept of Signalling was originally developed in the context of (public) telephone networks. In this context, telephone circuits had to be established and cleared. For this purpose, digital information had to be exchanged between users and networks and between the exchanges within networks. This information was called "Signalling".

It was also in this telephony context that the notions "in- band", "out-of-band", "channel associated" and "common channel" signalling were developed.

In the context of ISDN, Recommendation I.112 provides the most recent definition of signalling: "The exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunication network". This definition assumes that the distinctions between a "connection" and the "control of that connection" is clear. Unfortunately for non circuit switched networks this distinction is very unclear. For example, does the header of a data packet constitute a part of a virtual connection ("virtual circuit") or does it constitute a part of the control of that connection ?

The same Recommendation also gives definitions of the notions in-slot, out-slot, channel associated and common channel signalling. Unfortunately, these definitions are written in the context of circuits, channels and time-slots in a fixed cycle TDM environment (see Appendix B), so that their meaning in other environments (for example demand multiplex TDM; see Appendix B) is unclear.

6.2.2 Classification of three Types of Control Information

The concept of signalling is apparently closely related to the concept of "control information" in the OSI Reference Model.

In order to examine the relation between both concepts more closely, it is first necessary to classify different types of control information that can be exchanged between (N)-layer entities within an (N)-layer.

The following three types can be identified:

a) Type 1: Environmental Control Information

This includes signals which influence the environment in which (N)-layer user data may be transferred at some later point in time. At the completion of the exchange of this type of control information, user data may not yet be sent.

Examples:

- Dynamic creation of closed user groups, - Exchange of routing information used to update (N)- layer routing tables, - Restart packets in X.25, - Registration packets in X.25,

- Exchange of management information as far as it is related to the user data flow within this layer at some later point in time.

b) Type 2: Connection Control Information

These are signals which are exchanged to support the establishing and clearing of (N)-connections.

NOTE 19

It is not yet clear to what extent administrative arrangements, such as those needed to install an X.25 PVC, should be included here as well.

c) Type 3: Control Information used to directly control the exchange of user data

These are signals which are exchanged simultaneously, or interleaved, with user data.

Examples:

- X.25 headers of Data and Interrupt packets,
- X.25 Reset packets.

NOTE 20

It is not yet clear how control information which is exchanged in a CL environment should be classified. Some control information might be regarded as type 1 (PDUs of the ES-IS routing protocol which use elements of ISO 8473 and ISO 8208), while other control information might be regarded as type 3 (headers of the CLNP protocol).

6.2.3 The concept of signalling

If we now compare these groups of control information signals with the original meaning of "signalling", then it is recognized that types 1 and 2 will generally be regarded as signalling. The situation is less clear with respect to type 3, and we have now to make up our mind carefully. The choice that has to be made here will specifically have implications for the way in which signalling has to be included in the GLA (see Clause 12 hereafter).

The implications of both choices have been examined, with the conclusion that the inclusion of type 3 in signalling would result in a considerable complication of the contents of Clause 8.

Therefore, in this Technical Report we will restrict the concept of signalling to control types 1 and 2 only. Type 3 represents a special category and will not be seen as signalling.

Evidently, also qualified user data on which the (N)-layer imposes no rules other than the length of the field, like for user data, is not considered as (N)-layer signalling.

6.2.4 The distinction between in-band and out-of-band signalling

6.2.4.1 The definitions

In a layered model, an (N-1)-service provider allocates resources to provide a service that supports the exchange of information between a number of (N)-entities. This information includes (N)-control information as well as (N)-user data. The resources allocated by the (N-1)-service provider may be shared by both types of (N)-flows.

It is suggested to base the difference between in-band and out-of-band signalling upon the way in which these resources are shared. This can alternatively be viewed as whether there is contention for the (N-1)-service and its associated resources.

NOTE 21

The resources associated with the (N-1)-service include the resources of layer (N-1) and all lower layers.

Out-of-band (N)-layer signalling reflects the case where the exchange of (N)-layer control information is supported by resources allocated by the (N-1)-service provider on a deterministic basis, and which are exclusively used for this purpose by the (N)-layer. This is illustrated in figure 2.

In-band (N)-layer signalling reflects the case where the exchange of (N)-layer control information and (N)-layer user data is supported by resources allocated by the (N-1)- service provider on a non-deterministic (i.e. statistical and therefore competitive) basis.

This is illustrated in figure 3.

NOTE 22

The triangle symbol in the middle of figure 3 is assumed to represent a multiplexer of the "demand multiplexing" type (see Appendix B). If the multiplexer is of the "cyclic multiplexing" type, then figure 3 represents "out-of-band signalling" as well.

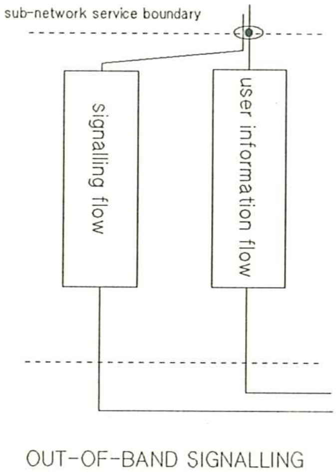


Figure 2:
out-of-band signalling

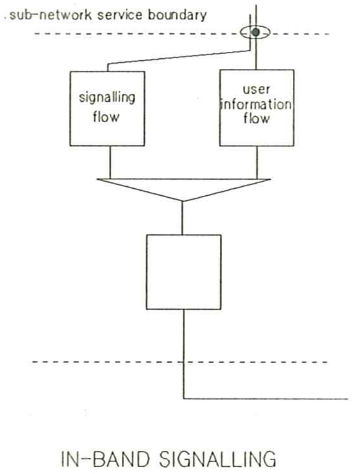


Figure 3:
in-band signalling

6.2.4.2 Relation to the use of (N-1)-connections

If (N)-layer signalling and (N)-layer user data are both guided over a single (N-1)-connection (or if the (N-1)- service is connectionless), then the (N-1)-service provider is not able to make any distinction between both flow types. All (N)-layer signalling has then to be seen as "in-band".

If (N)-layer signalling and (N)-layer user data are using separate (N-1)-connections, each reserved for that purpose, then this may or may not imply out-of-band signalling.

If the multiple (N-1)-connections still have to compete for resources within the (N-1)-service provider then we speak of in-band; if not, then we speak of out-of-band.

6.2.5 The distinction between common channel and channel associated signalling

In contrast with the distinction between in-band and out-of- band, the resource sharing strategy should be seen as irrelevant for the distinction between common channel and channel associated signalling.

Instead, the distinction should be based on the way in which channels are defined to support the transfer of signalling information.

Common channel signalling reflects the case where the exchange of (N)-layer control information uses a dedicated "management connection" within the (N)-layer to control the exchange of (N)-layer user data (for a multiplicity of (N)- layer user data flows).

Channel associated signalling reflects the case where the exchange of (N)-layer control information is supported by a set of k "management connections" each of which has the capability to set up and disconnect a single (N)-layer connection, which is one-to-one related to that "management connection".

NOTE 23

"Management-connection" is placed here between quotation marks because this "connection" has no individual connection endpoints at the (N)-service boundary.

6.2.6 Some examples

Table 1 gives some examples of the application of the definitions given in 6.2.4 and 6.2.5.

	Common channel	Channel associated
In-band	- X.25 Restart - Q.931 controlling D-channel data transfer	- X.25 Call Control - X.21 Call Control
Out-of-band	- G.704 common channel signalling - Q.931 controlling B-channel data transfer	- G.704 channel associated signalling

Table 1 - Some examples

6.2.7 The aspect of subnetwork intervention

In the preceding discussion, signalling is considered without any assumption whether there is some subnetwork that does or does not intervene in the signalling flow. This has the advantage that the analysis can now be applied in a broader context than that of the original signalling concept.

However, the aspect of subnetwork intervention also requires attention, since clarification is needed of:

- the distinction between (N)-layer signalling and subnetwork signalling,
- the distinction between User-to-Network (UtN) subnetwork signalling (which includes Network-to-User subnetwork signalling) and User-to-User (UtU) subnetwork signalling, and
- the relation of this to the concepts of active and passive operation on protocol elements (see clause 5.6).

Suppose the subnetwork under consideration has a protocol intervention level up to and including layer (N). If signalling information is exchanged between peer entities in layer (N), then we may identify four cases:

1) (N)-layer signalling information is exchanged between user and subnetwork (active operation). No other party is involved.

2) (N)-layer signalling information is exchanged between two users across the subnetwork, the subnetwork has knowledge of the semantics of that information, and it wishes to be involved as third party (active operation).

3) (N)-layer signalling information is exchanged between two users across the subnetwork, the subnetwork has knowledge of the semantics of that information, but does not wish to be involved in it as third party, and does therefore not check the semantics (passive operation).

4) (N)-layer signalling information is exchanged between two users across the subnetwork, but the subnetwork has no knowledge of the semantics of that signalling information. Its role is restricted to the transparent transfer of the (N)-layer control information as user data or qualified user data (no operation).

Case 1

Denoted as (N)-layer User-to-Network (UtN) subnetwork signalling without end-to-end significance.

Case 2

Denoted as (N)-layer User-to-Network (UtN) subnetwork signalling with end-to-end significance.

Case 3

Denoted as (N)-layer User-to-User (UtU) subnetwork signalling.

Case 4

Still denoted as (N)-layer signalling, but not as subnetwork signalling, since the subnetwork is not able to identify it is signalling information.

As examples, let us consider some cases from the X.25 PLP:

- A Registration packet is a form of UtN subnetwork signalling without end-to-end significance.
- A Restart packet is a form of UtN subnetwork signalling with end-to-end significance (as far as virtual calls or PVCs are operational at the interface under consideration).
- Parameters in Call Request packets are treated in the following way:

i) Called address :

UtN with end-to-end significance (as far as this address is delivered at the destination DTE).

ii) CCITT-specified DTE facilities :

UtU subnetwork signalling (unless subnetwork performs active operations in which case it should be seen as UtN subnetwork signalling with end-to-end significance).

iii) Flow control parameter negotiation :

UtN subnetwork signalling, with or without end-to-end significance.

iv) Call User data :

Not considered as subnetwork signalling (it may still be considered as Network Layer Signalling if it is used by DTEs to support additional Network Layer functions).

- A Reset Request packet is neither considered as subnetwork signalling, nor as any other form of (N)-layer signalling (it represents type 3 control information, see clause 6.2.3).

SECTION II

GLOBAL NETWORK SERVICE PROVIDER MODELS

7. INTRODUCTION

In this Section two models for a Global Network Service Provider are developed. The service provider is seen as possibly offering a range of global services one of which might be the OSI Network Service.

Both models are based on protocol layering principles and both represent different elaborations on the concepts defined in ISO 8648, specifically the subnetwork concept.

The first model, referred to as the Unconstrained Network Service Provider Model (UNSPM), is one that aims to permit any real network to exist as a subnetwork of the global network irrespective of the standards to which its access protocols may conform. It is based on the observation that given the prior existence of a configuration of real subnetworks the architectures of end systems making use of the configuration will vary dependent on their location and the degree of visibility each has of the access protocols of subnetworks remote from it.

The second model, referred to as the Constrained Network Service Provider Model (CNSPM) aims to achieve a greater degree of standardization of end system architecture. It adds the constraint that Subnetwork Service boundaries should be restricted to a certain defined set, in order to avoid unnecessary proliferation of protocol stacks. This set includes the service boundaries corresponding to the OSI layers 1, 2 and 3, and the sublayer service boundaries corresponding to MAC and LLC sublayers.

8. UNCONSTRAINED NETWORK SERVICE PROVIDER MODEL (UNSPM)

8.1 Introduction

In the OSI Reference Model three layers are identified below the OSI Network Service boundary: the Physical Layer, the Data Link Layer and the Network Layer.

Apart from this, the concept of "subnetwork" is introduced in the OSI Reference Model. This concept is elaborated upon in more detail in ISO 8648 (IONL), where the concept "subnetwork service" is introduced as "the abstraction of the subnetwork- provided functions along with the functions performed within open systems needed to exploit the subnetwork-provided functions".

In this Clause it will be shown that the validity and usefulness of the subnetwork concept goes far beyond that of open systems only. Indeed, the fact that a system connected to a subnetwork has to conform to the rules imposed by that subnetwork in terms of a certain subnetwork access protocol, creates an inter-protocol boundary in such a system which has far-reaching consequences for the layered structure of protocols performed by that system, irrespective of the question whether such a system does conform or does not conform to the OSI Reference Model.

Therefore, it is worthwhile to exploit the significance of the subnetwork concept for all real-world systems, and to separate the aspects which are valid for all real-world systems from the aspects which are only applicable to OSI open systems.

In this Clause full emphasis is laid on the first-mentioned "universal" aspects. It is explained that a layered structure of protocols in real-world configurations is heavily determined by the presence (or potential presence) of subnetworks. As a result, a model is presented which is based on this observation, and which is therefore applicable to all systems that have adopted some form of Global Network Service as the basis for their communication, irrespective of whether or not the protocols and services used conform to OSI.

8.2 The Subnetwork Concept

8.2.1 Architectural observations on intermediate systems (ISs)

Figure 4 shows an IS which interconnects a number of systems. Two of them are shown as systems Sa and Sb. Sa and Sb may be either ESs or ISs. Sa accesses the IS using protocol stack Pa, while Sb accesses the IS using protocol stack Pb.

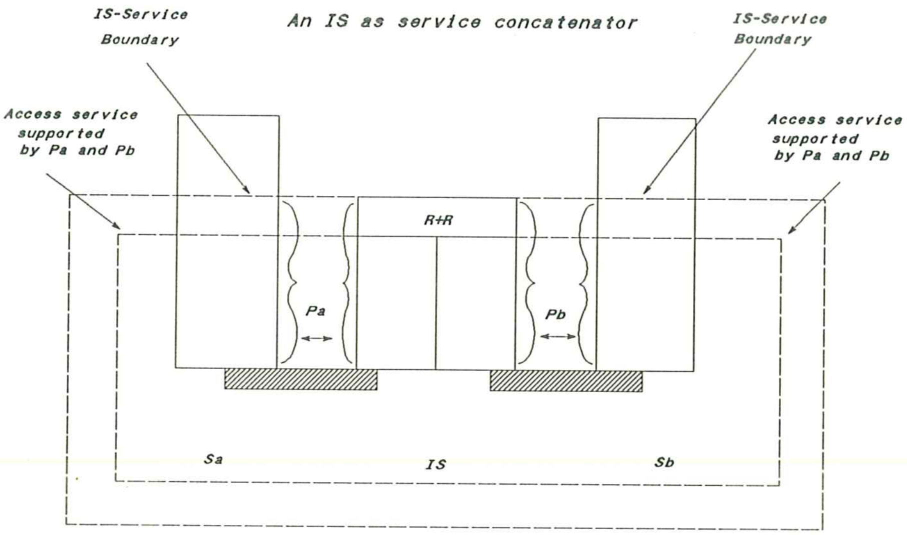


Figure 4 - An IS as service concatenator

The following observations can now be made:

i) If the intermediate system is representing a subnetwork, then the protocol stacks Pa and Pb shall be seen as subnetwork access protocols.

ii) The IS can conveniently be modelled as a "routing and relaying" (R + R) function, which is accessed by protocol stacks Pa and Pb. This means that by definition the access protocol functionality of Pa and Pb is restricted to support the interaction between the IS and Sa and Sb respectively; Pa and Pb are only "locally significant".

iii) In figure 4, the R + R functionality can be defined as follows:

  - Routing is the capability of the IS to derive (at least) from the destination address the correct outgoing media and source and destination points of attachment to the outgoing media.

  - Relaying is the capability of the IS to perform the actual forwarding of information received from Sa via Pa to Sb via Pb, and vice versa. This is sometimes referred to as "service primitive mapping".

iv) Service primitive mapping imposes two requirements on the access protocols Pa and Pb:

  - Firstly, the services supported by protocols Pa and Pb need not be identical. However, users can only use those service elements (i.e. service primitives and associated parameters) that are supported by both access protocols. Indeed, no information may get lost during this mapping process.

- Secondly, all information needed by the R+R function may be conveyed as parameters by access protocols Pa and Pb. In that case, the R+R function does not require the definition of a (sub)layer of protocol independent of Pa and Pb and the R+R "layer" could be thought of as "protocol-less".

v) The service supported by the IS is defined as the intersection of the sets of service elements supported by both access protocols, in combination with the R+R function.

NOTE 24

Real-world access protocol specifications usually contain a mixture of "pure" access protocol definitions (as described above) and R+R function descriptions. The advantage of the model shown in figure 4 is that it makes this distinction explicit.

vi) According to figure 4, the IS generates in all its attached systems an IS service boundary which corresponds with the so-called "intervention level" of the IS.

It should be emphasized that, seen from systems Sa and Sb, the IS service boundary is not determined by some intuitive feelings on the question of which functions in these systems should be combined in one layer. On the contrary, this boundary is completely determined by the presence of that IS, and is just as real as the IS to which these systems are attached. This boundary is in effect created in all systems attached to that IS, and effectively separates the protocols needed to communicate with the IS from protocols needed to communicate with systems located "beyond" that IS. This separation is especially significant if the different systems are subject to different design authorities.

The conclusion is that the presence of an IS imposes a de-facto service boundary in its attached systems which they are constrained to recognize. The implications of this statement for configurations where a system is connected with a number of ISs in tandem are further discussed in 8.3.3 and 8.4.

8.2.2 More about "protocol intervention level"

As stated above, an IS creates a service boundary in each of its attached (end) systems. This service boundary is always characterized by its capability to forward certain data unchanged between the systems attached to the IS.

If the IS represents a subnetwork with protocol intervention level (N) (i.e. if the subnetwork access protocol is described as a protocol stack up to and including layer (N), and the subnet service boundary is described as an (N)-service boundary in terms of the OSI Reference Model), then the rules for the transfer of data, as specified in 6.2 of the OSI Reference Model apply. These rules permit the notions (N)-SDU and (N)-protocol user data to be used to indicate that the subnetwork is committed to forwarding this data unmodified, provided it is of a single specific datatype: a delimited bitstring. By doing so, the (N+1) protocol entity can map its (N+1)-PDU onto the underlying (N)-SDU, and can be sure that the subnetwork will not interfere in the (N+1)-protocol, not even by a simple syntax check.

The subnetwork, however, may also have the property of passing certain elements of the (N)-protocol control information unchanged. This can be seen as some form of "(N)-protocol control information (PCI) transparency". A distinction must therefore be made between the transparency of a subnetwork to user data and its transparency to elements of PCI. The essential distinction is that the syntax of user data is not checked, while the syntax of the PCI is checked.

The (N+1)-layer has no visibility of any (N)-layer PCI transparency and no capability to exercise control via the (N)-layer service boundary over the choice of the (N)-layer elements that it wishes the (N)-layer to handle either transparently or non-transparently. For the adjacent layer (N + 1) this means that, if it unconditionally requires that some control parameters are passed unchanged and the content of these parameters is not checked by the subnetwork (neither syntactically nor semantically), then they must be transferred as (N)-user data.

8.2.3 Subnetwork access protocol header syntax and semantics

The concepts of "protocol control information transparency" as described above, and those of "active operation", "passive operation", "actual protocol intervention level" and "potential protocol intervention level", as defined in Clause 5, can be clarified with reference to the structure of the PCI encoded in the header of a typical PDU.

Figure 5 shows a typical structure of an (N)-PDU, used to access a subnetwork with protocol intervention level (N).

```
|<-------------------------(N)-PDU------------------------------>|
|<----------(N)-PCI (header)-------------->|<----User data field|

|<--Mandatory part-->|<---Optional part--->|                     |
b1                   b2                    b3                    b4
|--------------------|---------------------|---------------------|
                                            \
                                             \
|<-Mandatory fields->|<----(facilities)--->|Corresponds with    |
|                    |      fields         |potential protocol  |
|                    |                     |intervention level  |
|                    |                     |                    |
|                    |<--limits of actual->|                    |
|                    |   protocol inter-   |                    |
|                    |   vention level     |

      Subnetwork          Subnetwork           Subnetwork forwards
      operates            operates partly      this "transparently"
      always              actively, and
      actively            partly passively
```

Figure 5 - Relation between protocol intervention level and PDU format

Three fields can be recognized:

- Mandatory part of the header

  This is the part of the elements on which the subnetwork always operates actively; the contents are inspected syntactically and semantically, and are processed according to the (N)-protocol-rules.

  At the receiving side, left boundary b1 is provided by the underlying (N-1)-service (first bit of the (N)-SDU).

  Right boundary b2 is reconstructed as a result of the syntax check, and corresponds with the leftmost possible position of the actual protocol intervention level of the subnetwork (see clause 5.7).

- Optional part of the header

  This is the part upon which the subnetwork may operate actively (syntax and semantics check, possibly including processing), but if it does not, it at least operates passively (syntax check only) so that the position of right boundary b3 can always be determined.

  Boundary b3 corresponds with the potential protocol intervention level as defined in Clause 5.8. The actual protocol intervention level corresponds with a certain point in the optional part of the header if all fields positioned left of it are operated upon actively and all fields positioned right of it are operated upon passively. If such a point does not exist (i.e. if both field types are not ordered) then such a point can still be found (by definition) in the "Generic Header Format" corresponding to this protocol (see 6.1).

- User data field

  This is the part that the subnetwork has to handle as one field containing a single delimited bitstring, without any syntax check. This is usually formulated as the subnetwork's commitment to forward the data "transparently". At the receiving side, right boundary b4 is in most cases not reconstructed by the receiving (N)-protocol entity, but by the underlying (N-1)-service (last bit of the (N-1)-SDU).

8.3 Subnetwork Interconnection Principles

8.3.1 Introduction

A number of subnetworks can be interconnected by an Interworking Unit (IWU). The result can be seen as a larger composite subnetwork. This larger subnetwork can in turn be subject to interconnection with other subnetworks in the same way. This means that the interconnection mechanism described in this Clause can be applied iteratively.

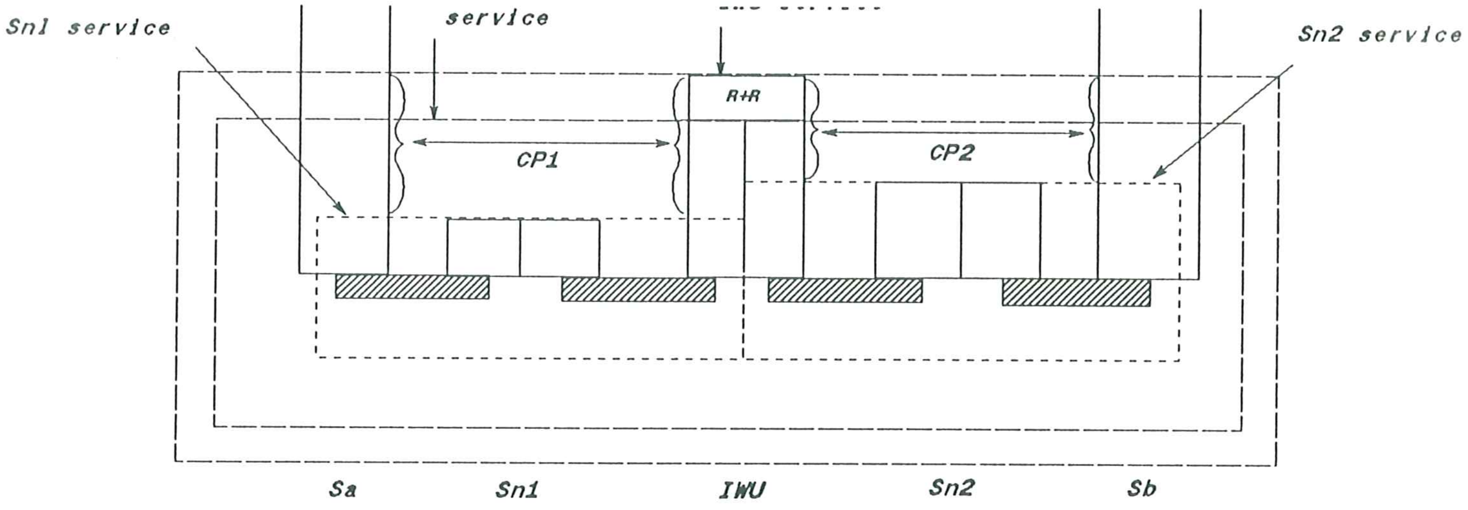
The objective of subnetwork interconnection is usually the wish to increase the number of terminals which can be interconnected. Therefore, subnetwork interconnection has usually direct implications for the applied address conventions. This is further discussed in 8.3.4.

Another implication may be that the service supported by the resulting composite subnetwork differs from that of the smaller subnetwork to which a system was (and still is) directly attached. In that case a new subnetwork service boundary and a new protocol layer containing a protocol which supports this new "aggregate" service is generated in this system. This does not mean that this additional protocol is always imposed by the IWU. Dependent on the protocol intervention level of the IWU, the additional protocol can also be imposed by one of the subnetworks which are located "further" in the chain of interconnected networks.

This is discussed further in 8.3.2 and 8.3.3 in which the term "intervention level" is not qualified as "potential" or "actual". However, all instances of use of the term "intervention level" should be read as "actual intervention level."

8.3.2 The IWU as service concatenator

Figure 6 shows two systems Sa and Sb. System Sa is connected to subnetwork Sn1. System Sb is connected to subnetwork Sn2.



(CP1 and CP2 are convergence protocols)

Figure 6 - The IWU as service concatenator

An Interworking Unit (IWU) is placed between both subnetworks to enable communication between Sa and Sb.

The subnetworks and the IWU are all represented as intermediate systems with a certain protocol intervention level (see Clause 5.7).

Subnetwork Sn2 is deliberately drawn higher than subnetwork Sn1 in figure 6; its protocol intervention level is higher, and it supports a service which differs from that of Sn1.

According to the observations made in 8.2.1, both subnetworks are represented as ISs with some routing and relaying capability R+R (not explicitly shown) and some service Sn1 and Sn2. The IWU is also represented as an IS with some routing and relaying capability R+R and some "IWU service".

Since an IWU is a special type of IS, everything that is stated on ISs in 8.2 also applies to IWUs. Therefore, the service supported by the IWU is the service supported by the IWU access protocols in combination with its R+R capability.

In figure 6 it is assumed that the protocol intervention level of the IWU is higher than that of both subnetworks. This means that some additional "convergence" protocols are needed over the top of the subnetwork access protocols, which may be subnetwork-specific (and therefore different) but create two "harmonized" service boundaries in the IWU (including harmonization of address conventions) on the basis of which the two subnetworks may be interconnected (as described in 8.2.1 for all intermediate systems).

These boundaries are indicated in figure 6 as the "IWU access service" boundary.

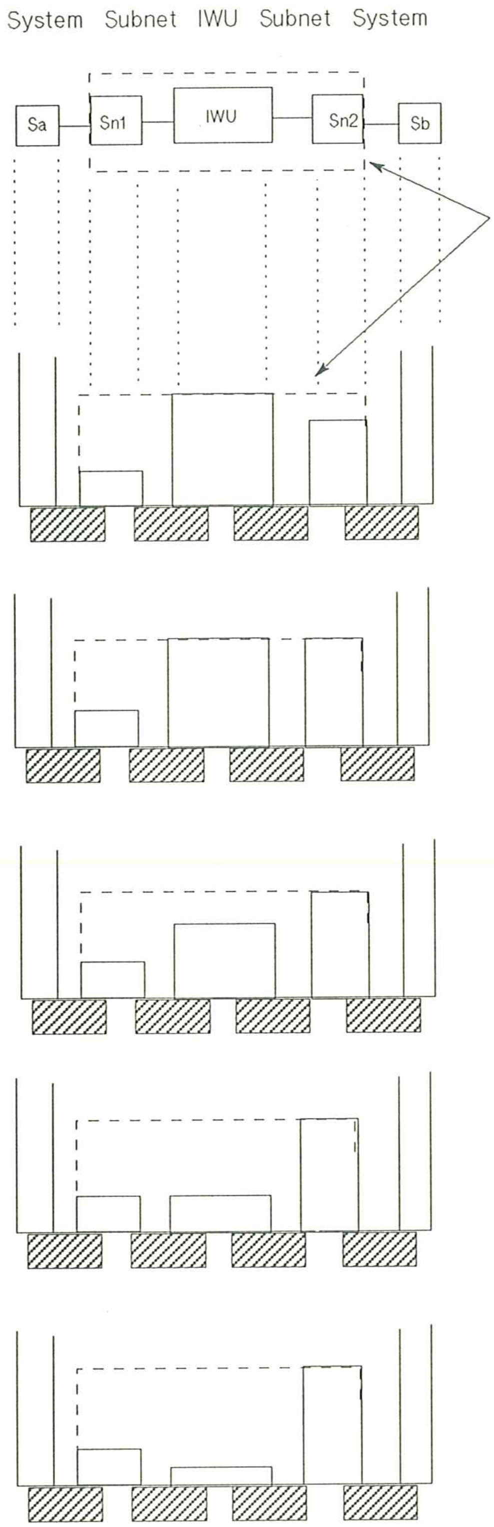
The IWU access service differs from the IWU service in that the first does not include the R+R functionality of the IWU, while the second does include this functionality.

The use of convergence protocols is not always needed. This is further discussed in 8.3.3 below.

8.3.3 The significance of the protocol intervention level of the IWU

Although it is true that an IWU always creates a service on the basis of which the subnetworks are interconnected, this service does not always need to affect the systems attached to both subnetworks and does not always need to be supported by convergence protocols over the attached subnetworks.

In order to illustrate this, five typical possible protocol intervention levels for the IWU are shown in figure 7 (the R + R functionalities are not explicitly shown).



Intermediate systems visible for Sa	Intermediate systems visible for Sb	
Sn1 + IWU	Sn2 + IWU	Case 1
Sn1 + IWU	Sn2	Case 2
Sn1 + IWU + Sn2	Sn2	Case 3
Sn1 + Sn2	Sn2	Case 4
Sn1 + Sn2	Sn2	Case 5

Figure 7 - Five typical IWU protocol intervention levels

These five levels are as follows:

Case 1

The IWU protocol intervention level is higher than that of Sn2.

Case 2

The IWU protocol intervention level is the same as that of Sn2.

Case 3

The IWU protocol intervention level is lower than that of Sn2, but higher than that of Sn1.

Case 4

The IWU protocol intervention level is the same as that of Sn1.

Case 5

The IWU protocol intervention level is lower than that of Sn1 and Sn2. This includes the degenerate case where the IWU is degenerated to the medium, then no longer a system in the strict OSI sense of the word.

In the same figure 7 the visibility of Sn1, Sn2 and the IWU is indicated in two columns at the right side of the picture for system Sa as well as for system Sb for all five cases.

The following observations can now be made:

i) In all cases a new composite subnetwork is constructed, the protocol intervention level of which corresponds with the protocol intervention level of the highest IS in the chain.

ii) For Sa the IWU is visible in cases 1, 2 and 3. For Sb however, the IWU is visible in case 1 only.

iii) Everything that is stated in 8.2.1 on intermediate systems applies for both subnetworks and the IWU. Therefore, the layered structure that should be chosen to describe systems Sa and Sb precisely reflects the number of visible systems. The most complex case is therefore case 3, where the protocols supporting the composite subnetwork service in Sa should be modelled on the basis of three layers, the lowest one supporting communication with Sn1, the middle one supporting communication with the IWU, and the highest one supporting communication with Sn2.

iv) Choice of case 1 rather than cases 2, 3, 4 or 5 will usually be based on the requirement to increase the address space or to enhance the service or quality of service (QoS).

Cases 2, 3, 4 and 5 all lead to the same composite subnet service (i.e. the service supported by Sn2). Preference for one of these cases will usually be based on the requirements with respect to the use of the IWU as protocol converter. This is especially relevant if the IWU interconnects a number of subnetworks which differ in their access protocols. For example, if there are a number of different Sn2s, then Sa "sees" in case 2 only one IWU rather than all Sn2s, while in cases 3, 4 and 5 the Sa "sees" all Sn2s rather than the IWU. If these Sn2s have different access protocols, then the IWU could mask these differences by choosing the protocol intervention level corresponding with case 2.

v) As stated in 8.3.1 the described interconnection principle may be applied recursively. Depending on the difference in protocol intervention levels of the subnetworks to be interconnected, and on the protocol intervention level of the chosen IWU, this may or may not lead to the addition of new protocol layers and new corresponding service boundaries in end systems.

8.3.4 Addressing aspects

Most subnetworks have the property that they can only operate on addresses that point to terminals directly connected to that subnetwork.

Other subnetworks have the capability to interpret addresses that do not point to terminals directly attached to the same subnetwork. These networks are able to derive from these addresses the address of an Interworking Unit (IWU) which is directly attached to that subnetwork, and forward to this IWU all addressing information needed by this IWU.

If an IWU is used to interconnect a number of subnetworks, then it needs address information. This can either be delivered by the subnetwork that accesses the IWU, or transferred by a convergence protocol used over this subnetwork. In some circumstances it may even happen that the only justification of the introduction of a subnetwork convergence protocol is given by the inability of the subnetwork to transfer the required address information !

8.4 Relaying as Service Mapping versus Relaying as Protocol Mapping

In 8.2 and 8.3, relaying is described as service mapping. This reflects the view that it is in principle always possible to describe a relay as a concatenation of subnetwork services which are identical in terms of service primitive definitions. Such an approach is, of course, only possible if the service supported by a subnetwork access protocol is specified, or can be derived from that access protocol in some way.

If this is not the case, then the only alternative to describing the functionality of an intermediate system is that of "protocol mapping". This means that a description has to be made of how each element of the access protocol at the incoming side is mapped onto each element (if any) of the access protocol at the outgoing side. Since the number of protocol elements supporting a certain service is usually an order of magnitude larger than the number of service elements that the protocol supports, and since the protocols used to access a certain IS may substantially differ on different IS points of attachment, the protocol mapping approach is usually much more complex than the service mapping approach. Therefore protocol mapping should not be the preferred method of describing a relay.

8.5 Representation of Signalling

For circuit switched networks the establishment (or clearing) of a connection requires the execution of a specific signalling protocol between network and user. If the connection establishment protocol is successfully completed, then a connection becomes available between the users, which is characterized by a continuous flow of data. The service supported by such a connection is denoted as a "Continuous Bitstream Oriented" (CBO) service (see Appendix B).

In the model that will be described in 8.6, a circuit switched network should clearly be represented as a "subnetwork", and the signalling protocol is clearly a protocol which is imposed by that subnetwork.

Therefore the signalling protocol should be positioned in the model below the subnetwork service boundary.

Consider now a user-to-user protocol executed during the lifetime of the connection over the top of that established connection. This protocol can be freely chosen by the users; the network does not impose anything, and does not interfere in this protocol. This user-to-user protocol should therefore be positioned above the subnetwork service boundary.

Suppose now that the signalling protocol is described as a three-layer protocol. It then contains a layer 2 and a layer 3 protocol which, according to the above-made observations, should be represented as protocols located below the subnetwork service boundary. Suppose also that the user-to-user protocol is also described as a three-layer protocol. These protocols should be represented as protocols above the subnetwork service boundary.

The result is that we have now a layer 2 and a layer 3 protocol below and above the subnetwork service boundary.

The question that now arises is: how should this be represented in our subnet-based model ?

There seem to be two alternatives:

Alternative 1 (figure 8)

Layers 2 of both protocols are represented on the same horizontal level. The same holds for layers 3 of both protocols. In this case the subnetwork service boundary has to be represented as a "staircase".

Alternative 2 (figure 9)

The subnetwork service boundary is represented as a flat horizontal boundary. In this case the two layer 2 protocols and the two layer 3 protocols are represented on completely different levels.

Both representation styles have their pro's and con's.

Alternative 1 respects the layer numbering conventions of layers 2 and 3, but necessitates modelling the system attached to the subnetwork as a set of layers, which each contain functions that partly are related to protocols in which the subnetwork does not intervene, and partly are related to protocols in which the subnetwork does intervene. These functions, although located in the same layer, have in fact nothing to do with each other, since their peer entities are located in completely different remote systems.

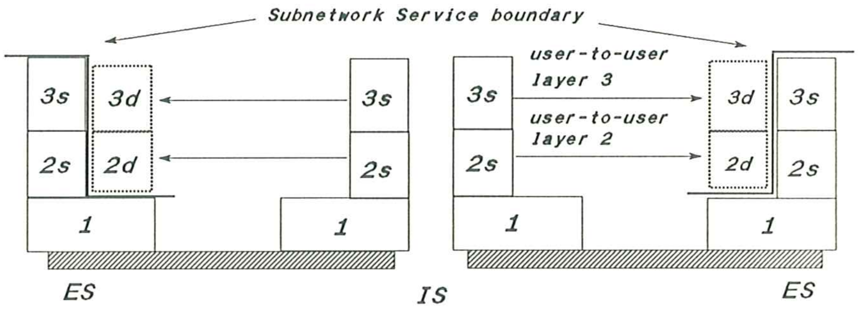


Figure 8 - "staircase" subnetwork service boundary

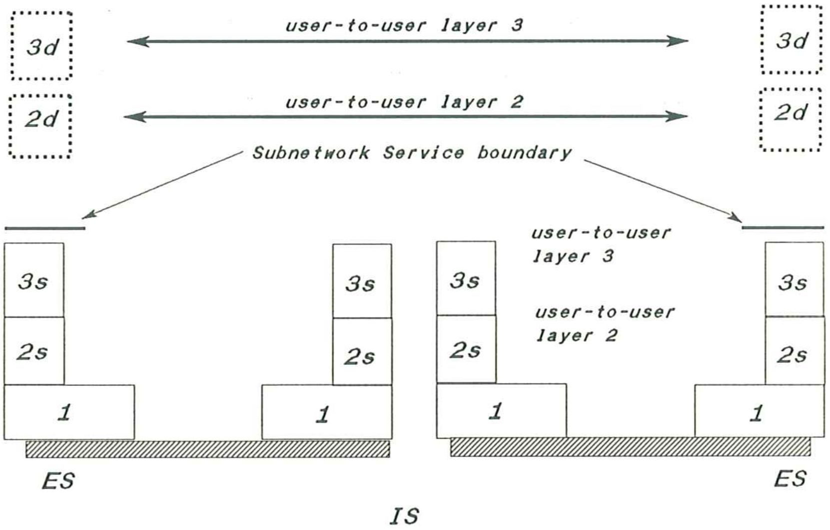


Figure 9 - "flat" subnetwork service boundary

Legend for figure 8 and 9

IS: Intermediate system, representing a subnetwork
ES: End system
3d: Layer 3 user data entity
2d: Layer 2 user data entity
3s: Layer 3 signalling entity
2s: Layer 2 signalling entity

Alternative 2 emphasizes the implication of the presence of the subnetwork in the representation of the system attached to that subnetwork. It emphasizes that the two protocols, which are both called "layer 2" or "layer 3" protocols, have in fact nothing to do with each other. Alternative 2 clearly separates functions related to protocol entities with a peer entity in the subnetwork from functions related to protocol entities with peer entities in systems located "behind" the subnetwork, by representing them as running on different levels.

There is, however, an additional advantage. Alternative 2 allows all operations performed on the continuous bitstream to be regarded as equivalent from the subnetwork point of view. Indeed, in a subnetwork-based model it is unimportant whether in a circuit switched network a protocol is used over the top of a circuit switched connection which for example supports some type of delimiting and error correction (such as HDLC), or a protocol is used for example to transform an audio signal into a bitstream and vice versa (such as a PCM-CODEC). This means that alternative 2 is more appropriate to model both integrated data and non-data services.

Although this Technical Report does not yet cover non-data services, it is believed that this aspect should be taken into account for making the best choice between the two alternatives.

Considering these pro's and con's it is ultimately felt that alternative 2 should be chosen; subnetwork service boundaries should be represented as flat boundaries, and all implications of this decision should be fully accepted.

8.6 The Resulting Model

8.6.1 Introduction

In the OSI Reference Model, only three layers are identified below the OSI Network Service (NS) boundary: The Physical Layer, the Link Layer, and the Network Layer.

However, the service boundaries corresponding with these layers were defined without any concern for the presence or absence of intermediate systems, and hence these boundaries usually do not correspond with the protocol intervention levels of intermediate systems such as existing subnetworks and IWUs. The result is that the OSI Reference Model can not always successfully be applied to real-world configurations.

In 8.6.2 hereafter a subnet-based model will be described, which is expected to offer greater capability to describe real-world configurations. The tools needed to describe this model can all be found in the preceding part of this Clause.

8.6.2 The model

The model is based on the view that layers below the NS boundary are created by the fact that subnetworks have different intervention levels. A subnetwork with a certain intervention level can be decomposed into a set of "lesser" subnetworks interconnected by Interworking Units (IWUs), where each subnetwork has an intervention level that is lower than that of the original subnetwork. This process of decomposition ends when the lesser subnetwork appears to be the medium itself.

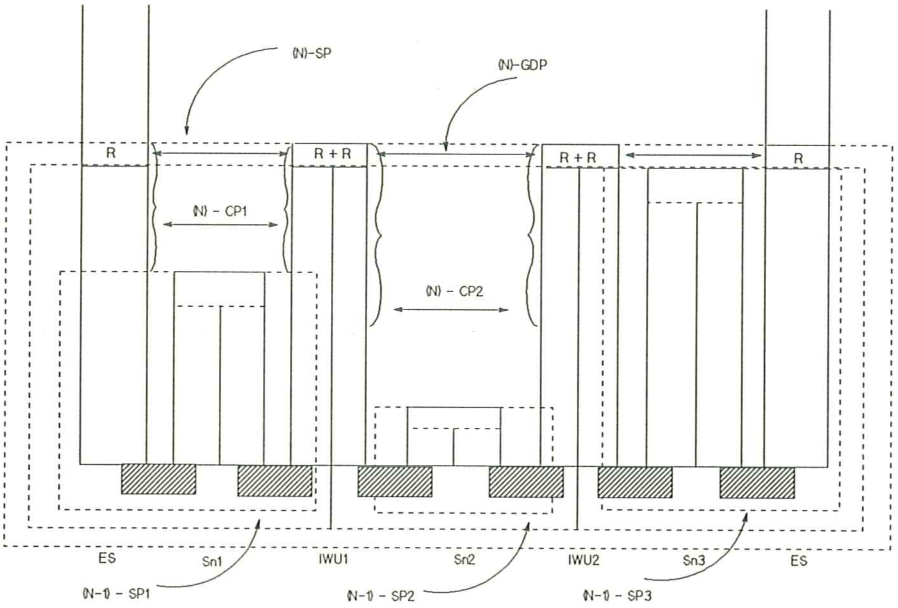
Figure 10 shows one step in this decomposition process. (N)- SP represents a certain (N)-layer subnetwork service provider. All ISs which have the same protocol, relaying and routing intervention level as that of the (N)-SP are considered as IWUs. These IWUs contain R+R functions that operate on parameters that are valid for the whole (N)-SP (for example (N)-SP addresses), and which can be accessed by means of an IWU-specific IWU access protocol.

Between these IWUs we find SPs of a lower level (level (N- 1)). In Figure 10 this corresponds with Sn1, Sn2 and Sn3, supporting respectively services (N-1)-SP1, (N-1)-SP2 and (N- 1)-SP3.

All these SPs have the property that they do not have any R+R functionality operating on parameters that are valid for the whole (N)-SP. Apart from this, it may happen that the service that they support differs from that of the (N)-SP in more respects than that of R+R functionality alone.

- If the service provided by the (N-1)-SP differs from that of the (N)-SP only in terms of R+R capabilities, then the lesser subnetwork might still be capable of transparently conveying the parameters needed by the R+R entities in the IWUs. In that case no distinct convergence protocol is needed to raise the service of the (N-1)-SP to that of the (N)-SP. In figure 10 this situation holds for the Sn3 subnetwork.
- If however, the lesser subnetwork does not have this capability, or if the service provided by the (N-1)-SP differs from that provided by the (N)-SP in more aspects than those of routing and relaying alone, then a distinct convergence protocol is needed to bridge the gap between both services. In figure 10 this situation holds for the subnetworks Sn1 and Sn2. The convergence protocols are denoted as (N)-CP1 and (N)-CP2 respectively.

Figure 10 has a resemblance to figure 6. The main difference between these figures is that figure 10 makes the R+R function explicitly visible, and represents a single step in the decomposition process.



Legend

(N)-SP : (N)-layer service provider
(N)-GDP : (N)-layer globally defined parameters
(N)-CP : (N)-layer convergence protocol
(N-1)-SP : (N-1)-layer service provider
R : Routing
R+R : Routing and relaying

Figure 10 - The subnetwork service provider model

8.6.3 Implications for end systems

Figure 11 shows two end systems, interconnected via six subnetworks with different intervention levels. If the decomposition step described in 8.6.2 is applied four successive times, then four subnetwork service boundaries are created in ESa, and one is created in ESb. Indeed, as already said in 8.2.1, the layered structure of an end system, as far as applicable below the OSI Network Service boundary, should reflect the protocol intervention levels of all visible intermediate systems (such as subnetworks and IWUs). Figure 11 shows that, by so doing, a precise modelling of real-world configurations can be achieved. As a result, the set of visible intermediate systems generates the layered structure up to the service supported by the IS with the highest intervention level (see also figure 7).

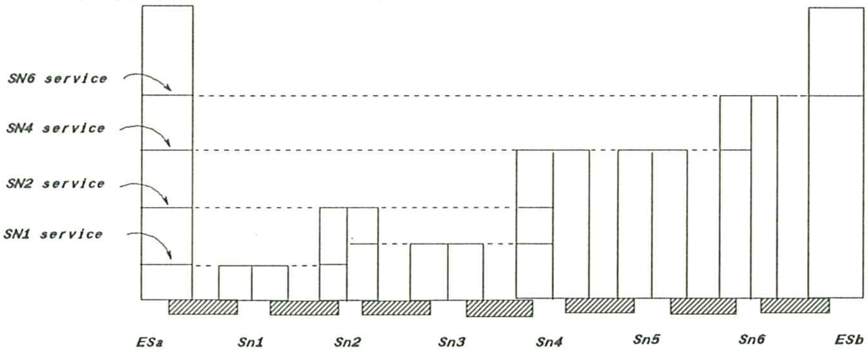


Figure 11 - The unconstrained Network Service Provider Model (UNSPM)

8.6.4 Relation to the OSI NS

In 8.6.3 it was shown how in an end system the set of "visible" intermediate systems generates the layered structure up to the service supported by the IS with the highest intervention level (see figure 11). This service may, but need not, correspond with the OSI Network Service (NS).

If the OSI NS is required in a certain end system, but is not supported by the highest subnetservice boundary in that end system, then communication on the basis of the OSI NS can still be achieved if some convergence protocol is used by the communicating end systems over the top of the subnetwork service created by the IS with the highest intervention level, which does support the OSI NS. Figure 12 shows how figure 11 has to be enhanced to cover this situation.

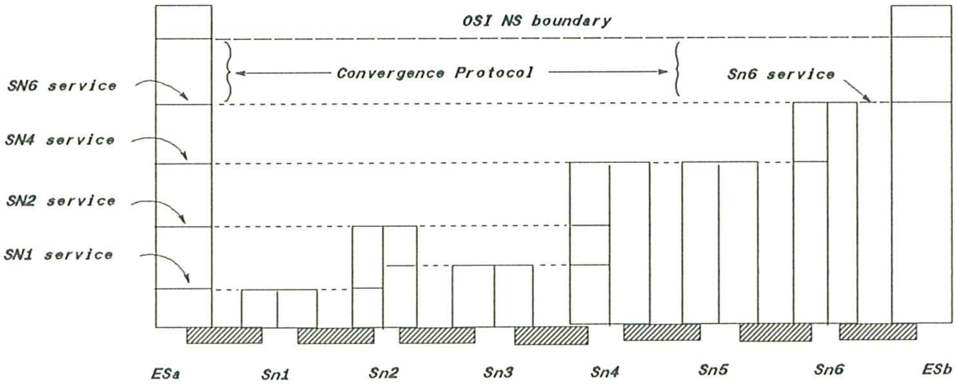


Figure 12 - The Unconstrained Network Service Provider Model (UNSPM) in the case where the OSI NS needs to be supported

9. MULTILAYER ADDRESSING MODEL (MLAM)

In this clause, a multi-layer architecture for the OSI Network Service Provider is defined, which is derived from the first principles of the OSI Reference Model as they relate to the topics of:

- adjacent layer address mapping, and
- relaying and routing at the (N) layer between logically or physically disjoint sets of (N-1) addresses.

To facilitate the development of the model, the concept of an (N) Demesne is used (see section 5).

The result is a multi-layer Addressing Model (MLAM) the layered structure of which reflects the way in which addresses are structured and processed.

Although the MLAM identifies a "global addressing datum " which (almost) completely corresponds with the OSI Network Service, MLAM layers do not always map 1 to 1 into OSI layers.

However, for certain protocol stacks and addressing conventions, the relation between MLAM layers and OSI layers can be specified quite well.

Examples can be found in clause 14 of section IV.

9.1 OSI Reference Model First Principles

9.1.1 Base concept

The OSI base concept, central to all aspects of OSI standardisation, is that of an OSI environment served by a single global Network service provider enabling, in principle, any OSI End System attached to the service to interwork with any other similarly attached.

The concept of a single global Network service provider, embracing all the Network and lower layer entities of the entire OSI environment, is basic to, and represents the starting point for, all considerations relating to the subjects of naming and addressing within the environment. It is also basic to the subject of routing between End Systems via the Intermediate Systems (sub-networks and gateways) going, in part, to make up the global network service provider.

The significance of the base concept from an addressing and routing perspective stems, amongst other things, from the following:

- The concept is one requiring the layers of the Reference Model to be seen as being subject to a basic division of kind about the Network service boundary. All functions within an End System below the boundary must be seen as forming part of the global network service provider. They exist to interwork with the Intermediate systems of the environment. All functions above the boundary exist only to interwork with those of other End systems.
- The concept is one that must be supported by a restriction on relaying above the Network Layer. Failing this restriction the OSI concept of a sub-network (of the OSI global network) would have no meaning, nor, in their turn, would the concepts of: Interworking Unit (or inter(sub)network gateway) ; Intermediate system as the abstraction of both a sub-network and an interworking unit ; End System as a system existing topologically on the periphery of the global network.
- The concept is one requiring the Network service boundary in the Model to be taken as an addressing datum for all other layer service boundaries ; lower layer addressing mechanisms existing to support the datum, those of higher layers to build on it.
- The concept is one leading naturally to the provisions of the addressing addendum to the Model that call for only two layers to be supported by directory functions, the Application Layer and the Network Layer ; the first to translate Application process names to Application

Layer entity addresses and the second to provide End System to End System routing capabilities via Intermediate systems.

However, in spite of the importance attaching to the Network service boundary as the OSI addressing datum, nowhere in the range of OSI documents dealing with addressing issues are the basic principles of adjacent layer service access point address mapping fully worked out.

More specifically, the different forms of hierarchic, or relative, address mapping applying above and below the Network service boundary are not distinguished and those applying below the boundary are not related, as they need to be, to the subjects of relaying and routing below this boundary.

Additionally, the naming and addressing provisions of the OSI model are restricted to those needed to support interworking between OSI conforming systems. They take no account of those needed to support the OSI environment within a wider complex of public and private networking environments embracing conforming, non-conforming and hybrid systems.

The following makes good these deficiencies of the model and shows that companion with the concept of hierarchic Network address to higher layer address mapping based on Network address suffix definition, is the inverse concept of hierarchic Network address to lower layer address mapping based on Physical layer address prefix definition. The first provides a means for progressively expanding upwards through the higher layers the datum Network address space. The second may be looked upon as potentially providing a means for either its progressive division downwards through the lower layers or its progressive generation upwards.

It identifies the internetwork sub-layer of the Network layer as that within which the transition from higher layer to lower layer hierarchic addressing should be seen as being effected, and hence this sub-layer as that which should be seen as supporting, at the crossover point, the true global addressing datum.

Having identified the principles applying within the context of the OSI environment considered in isolation the section goes on to show how the same address mapping principles can be applied within the wider environment to support both OSI conforming and non-OSI conforming services and protocols within a single framework.

9.1.2 Reference model address mapping principles

9.1.2.1 Introduction

The Reference Model does not give any guidance with respect to the question what architectural relations can be identified between addresses used in the layers below the network Service boundary, and to which extent hierarchical address-mappings can be used in these layers.

Section 5.3 of the Reference Model deals with the subject of routing and section 5.4 provides some enlargement on the topic from the addressing perspective. In neither of these two sections, however, any attempt is made to explain the relation between the functions that perform (N)-address to (N-1)-address mapping and the functions that transform an address into a route.

It is felt that this omission is the major reason that there is up to now no consensus about the potential benefits of hierarchical address mapping and the possible benefit of any address-structuring that could lead to simplification of (N)-address to (N-1)-address mappings below the network service boundary. In addition, there is no architectural justification for a number of phenomena that can be observed in protocol- specifications applicable to layers below the network service boundary. How, for example, can it be explained that certain OSI Network Layer protocols require the use of Data Link Layer addresses as integral part of Network Layer addresses (see e.g. ECMA-117, Domain Specific Part of Network Layer Address). It is the intention of subsequent paragraphs to clarify the presence and benefits of hierarchic address structures in existing and future protocol definitions not only above, but also below the OSI Network Service boundary.

9.1.2.2 The approach taken by the OSI Reference Model.

Section 5.4 of the Reference Model deals with the subject of Identifiers in general and the mapping of (N)-addresses to (N-1)-addresses in particular. It states that two kinds of (N)-address mapping functions may exist within a layer:

(a) hierarchical (N)-address-mapping, and
(b) (N)-address-mapping by tables.

ad (a)

This kind of mapping is directly associated with the presence of a hierarchically structured (N)-address. Given such a structure, the (N-1)-address can be derived from the contents of the (N)-address. More precisely: a hierarchically structured (N)-address consists of an (N-1)-address, followed by an " (N)-suffix", or "(N)-selector". This (N)-suffix is used by the (N)-entity to perform the (N)-address to (N-1)-address mapping function and vice versa.

Since this structure allows a more to one mapping, but excludes a one to more mapping of (N)-addresses into (N-1)-addresses, this mapping will in this report be referred to as hierarchical "n:1 address mapping".

NOTE 25

The x:y notation will always be used in this report in the sense of "<higher layer>:<lower layer> "

Two observations are of immediate relevance here:

1) The Reference Model restricts the application of hierarchical (N)-address mapping as discussed above to layers 4 up to 7. More precisely: Part three of the reference model (ISO 7498-3, OSI Ref. Model - part 3: Naming and Addressing) explicitly states in its note to paragraph 3.2, that the concept of (N)-address selectors only applies above the network layer.

2) Hierarchical address mapping is always n:1, and never 1:n. Section 5.4 of the Ref. Model indeed discusses the possibility of 1:n address mapping. However, it mentions this case only in the context of case (b) (see below). Therefore, according to the Ref. Model, the use of hierarchical 1:n address mapping is not foreseen.

ad (b)

Section 5.4 of the Ref. Model states, that case (b) covers all cases where either an (N)-address can be mapped into several (N-1)-addresses, or an (N)-address is not permanently mapped into the same (N-1)-address. It is then stated that in these cases the "(N)-address mapping function may use tables to translate (N)-addresses into (N-1)-addresses". In our terminology: 1:n mapping is possible, but it requires the use of tables, and should not be "confused" with the use of hierarchical address mapping.

9.2 Development of MLAM

This model is based on the acceptance of two distinct hierarchical addressing mechanisms. One is based on the use of suffixes. The other is based on the use of prefixes. Layers identified in this section have no a-priori relationship to OSI-layers. This relationship is discussed in section 9.3 hereafter.

9.2.1 Hierarchic Addressing by Address Suffix Definition

The suffix mechanism is fully recognized in the OSI reference Model, and is introduced there as the only possible way of multi-layer address structuring.

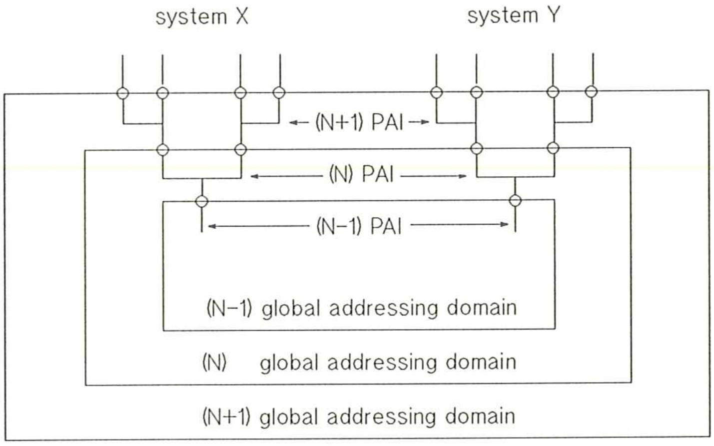
According to this definition:

- a set of (N)-addresses is mapped onto a single (N-1) address
- each (N)-address is structured into two parts:

  Part one: the (N-1)-address to which all (N) addresses are attached, followed by
  Part two: the (N)-suffix, identifying the correct (N) address within this set.

The resulting address structure is as follows:

(N)-address =
(N-1)-address / (N)-suffix =
(N-2)-address / (N-1)-suffix / (N)-suffix =
(N-3)-address / (N-2)-suffix / (N-1)-suffix / (N)-suffix =
(etc.)



(N) PAI = (N) Protocol Addressing Information
= (N) suffix to (N-1) PAI

Fig 13 - Hierarchical n : 1 mapping of adjacent layer addresses

Figure 13 illustrates such a mapping. It shows two systems X and Y, between which Protocol Addressing Information (PAI) is being exchanged to support hierarchical n : 1 mapping of adjacent layer SAPs.

Note that the mechanism of address suffixing ultimately rests on the designation of some lowest layer in the hierarchy that provides the "addressing datum". This datum is the basis, upon which higher layer address spaces are built by means of the suffix mechanism. If that datum supports "global addressing", then all higher layers also support "global addressing". This clarifies why part 3 of the Reference Model restricts the application of the suffixing mechanism to the layers above the OSI Network Service. The Reference Model and its related protocol and service standards do consider the Network Service, with some qualification (see 9.3.1), of all OSI Open Systems. If address suffixing would have been allowed below this boundary, then the key-position of the Network-Service with respect to global addressing would have been lost.

9.2.2 Hierarchic Addressing by Prefix Definition

9.2.2.1. General

According to the Reference Model, "there are instances where services provided by the (N)-layer do not permit direct access between all of the (N + 1)-entities which have to communicate. If this is the case, communication can still occur if some other (N + 1)-entity can act as a relay between them".

With reference to the definition of (N)-DEMESNE given in clause 5, the same can be reformulated by saying, that the (N)-layer may present itself to the (N + 1)-entities as a number of disjoint (N)-DEMESNEs, each only supporting communication between members of some subset of these (N + 1) entities.

(N + 1)-Relays in the (N + 1)-layer may be used to interconnect some of these disjoint (N)-DEMESNEs. The result is that (N + 1)-Demesnes are constructed, the address-space of which potentially encompasses the combination of the address-spaces of all interconnected (N)-Demesnes.

Within such an (N + 1)-DEMESNE, the (N)-DEMESNEs which are interconnected are of course fully visible in the (N + 1) layer, and the (N + 1)-DEMESNE has within its (N + 1) layer the means to identify the various (N) DEMESNEs upon which it is built.

Suppose now, that there is an (N + 1)-layer that provides the global addressing datum mentioned above. The (N + 1)-service can then be represented as a single global (N + 1)-DEMESNE. This (N + 1)-DEMESNE can be built on top of a number of (N)-DEMESNEs, by placing relays between them in the (N + 1)-layer. By doing so, the address-space offered by the (N + 1)-DEMESNE can be decomposed into a number of lesser address-spaces, each corresponding to the address space of each individual (N)-DEMESNE.

9.2.2.2. The use of prefixes

Suppose now that a certain open system is identified by an (N + 1)-address. Given the fact that the entities within the (N + 1)-layer of the (N + 1)-DEMESNE do have means to identify the underlying (N)-DEMESNEs, the (N + 1)-SAP address of that system can be constructed as a concatenation of two parts:

- part 1, identifying within the (N + 1)-DEMESNE the (N)-DEMESNE, to which the system is attached, followed by
- part 2, identifying within that (N)-DEMESNE the (N)-SAP, that gives access to that system.

NOTE 26

Emphasis should be placed on the use of the words "can be constructed". No suggestion is made here, that there are no other ways of structuring. If, however, the prefixing technique is used as a basis for address-structuring, then the resulting address-structure is as described above.

This mechanism to decompose an (N + 1)-address in an (N + 1)-layer, in which relays are located, is called: prefixing. Part 1 is called the (N + 1)-prefix. Part 2 is called the (N)-address.

Apparently, the mentioned system may have direct access to more than one (N)-DEMESNE. In that case its (N + 1)-SAP can be identified by as many (N + 1)-addresses as there are directly accessible (N)-DEMESNEs.

If not only the (N + 1)-layer, but also the (N)-layer, the (N-1)-layer, etc., contain relay function, then the decomposition of an (N + 1)-address into a (N + 1) prefix component and an (N)-address can be recursively applied downward. Assuming that all layers below the (N)-service boundary, that provides the global addressing datum, do contain relaying functions, the resulting address structure for an (N)-address becomes as follows:

(N)-address =
(N)-prefix / (N-1)-address =
(N)-prefix / (N-1)-prefix / (N-2)-address =
(N)-prefix / (N-1)-prefix / (N-2)-prefix / (N-3)-address =
(N)-prefix / (N-1)-prefix /..../ (2) prefix / (1) address

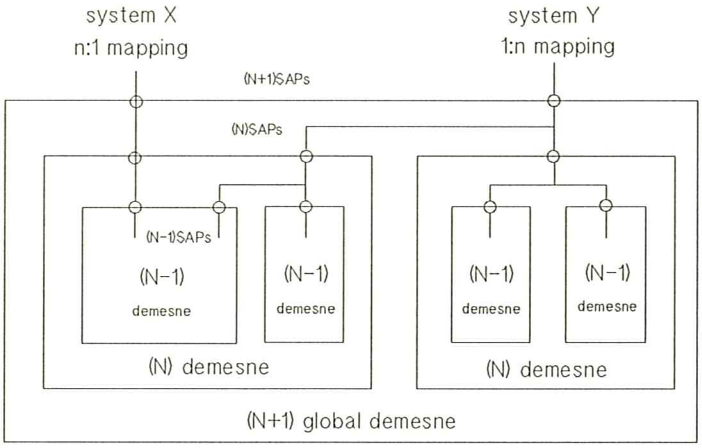


Figure 14 - Hierarchical 1 : n mapping of adjacent layer addresses

As an illustration, figure 14 shows the (N + 1)-SAPs that identify systems X and Y respectively. According to this figure, System Y has direct access to all DEMESNEs shown in the figure, i.e. to the single ("global") (N + 1)-DEMESNE, to the two (N)-DEMESNEs, and to the four (N-1)-DEMESNEs. System X has, of course, also direct access to the global (N + 1) DEMESNE. It has, however, restricted access to the lower levelled DEMESNEs, i.e. only to the leftmost (N)-DEMESNE, and only to the leftmost (N-1)-DEMESNE.

Note that in this figure, the (N + 1)-DEMESNE is the only common datum that can be used by all systems attached to all shown DEMESNEs to identify each other.

The (N + 1)-SAP for system X is:

(N + 1)-prefix / (N)-prefix / (N-1) address

where:

- the (N + 1)-prefix points to the leftmost (N)-DEMESNE
- the (N)-prefix points to the leftmost (N-1)-DEMESNE
- the (N-1)-address points to the leftmost (N-1)-SAP

The (N + 1)-SAP for system Y shows the same structure, but:

- the (N + 1)-prefix may have two possible values
- each of these values can be followed by two possible (N)-prefix values
- each possible (N)-prefix is followed by an (N-1)-DEMESNE specific (N-1)-address

Note that figure 14 does not show any relay. Since, however, system Y has access to several (N)-DEMESNEs and several (N-1)-DEMESNEs, it may offer relaying functions to other systems that want to communicate. These other systems are, however, not shown in the figure. The figure therefore illustrates, that the applicability of the prefixing mechanism is not restricted to the presence of relays. Prefixing is applicable to all situations where systems are identified by an (N)-address allocated by a global (N)-DEMESNE, but this global (N)-DEMESNE is built on top of more than one lower levelled DEMESNE.

9.2.2.3 Introduction of routing tables

Figure 15 shows a more "realistic" scenario, involving an intermediate system I performing a relay function to support communication between systems X and Y.

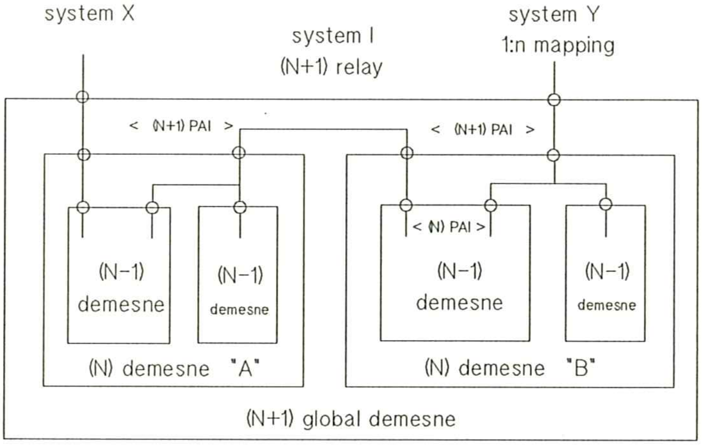


Fig 15 - Hierarchical 1 : n mapping of adjacent layer addresses with the presence of an (N+1)-relay

The similarities and differences between figures 14 and 15 should be noted.

The similarity is that systems X and Y can be identified by an (N+1) address that can be decomposed into prefixes and lower level addresses, dependent on the lower level DEMESNEs to which it has direct access. The difference is that there is no common (N)-DEMESNE to which both systems X and Y have direct access.

Consider, for example, the case where System X wishes to communicate with System Y. System X clearly has no direct access to the (N)-DEMESNE indicated in the (N+1) address of system Y ((N)-DEMESNE B in the figure).

System I, however, is capable to do that, since I and Y have both direct access to the same (N)-DEMESNE B.

System X has now to execute two additional functions:

- It has to offer the (N)-DEMESNE identifier of Y to some routing table, which should return an (N)-DEMESNE identifier of an (N)-DEMESNE to which X has direct access, and an (N)-DEMESNE specific (N)-address which points to some Intermediate System I, which is expected to be located "closer" to system Y.
- It has to transfer the full (N+1) address of system Y to system I as protocol address information (PAI), so that system I can perform its task.

In the scenario shown in the figure, system I will be capable to directly access the destination (N)-DEMESNE. If not, system I will in its turn perform the same action as described above for system X.

Two tables are shown as illustration of the above.

Table 2 shows the structure and content of an (N)-layer routing table for system X.

Table 3 illustrates the structure of a multi-layer routing table given that relaying is being performed at a number of adjacent layers below the (N + 1) layer.

input

returned

path to an I-system located "closer" to
the destination (N)-DEMESNE

Destination (N)-Demesne	local (N)-Demesnes	local (N)-DEMESNE specific I-system address
l	m	p
		q
		r
	n	s
		t
		u

Table 2 - (N + 1) Layer routing table

input

returned

path to an I-system located "closer" to
the destination (N)-DEMESNE

dest (N) DEMESNES	directly accessible (N)-DEMESNEs	(N)-DEMESNE specific I-system address		
		directly accessible (N-1) DEMESNEs	(N-1)-DEMESNE specific I-system address	
			directly accessible (N-2) DEMESNEs	(N-2)-DEMESNE specific I-system address

Table 3 - Composite (N + 1) / (N) / (N-1) Routing table

9.2.2.4 (N)-layer synonyms

If the prefixing mechanism is used, then, if an open system has direct access to more than one DEMESNE, the system has at least as many addresses as there are lowest-levelled DEMESNEs to which it has direct access. This fact suggests that a prefix-based address contains a routing-specific component.

Indeed, if for example a destination system is attached to more than one destination DEMESNE, and if there exists a path from the source system to the DEMESNE to which the destination system address is pointing, then this DEMESNE will usually indeed be chosen to access the destination system. The route to that DEMESNE is, however, in no way implied by that destination address, and independent routing decisions have still to be made by the source system and all intermediate systems which have no direct access to the destination DEMESNE.

9.2.3 Composite Multi-layer Addressing Model (MLAM)

All open systems can be identified by a global address, provided at a certain, say (N), service boundary. The set of all (N)-addresses is called the "global address domain", or the "global addressing datum". This (N)-service has the property that all open systems can exchange data, without calling upon the services of any relaying entity in any higher layer. Therefore the global address domain can be seen as an (N)-DEMESNE (see the definition of DEMESNE in clause 5). We will call this DEMESNE the "global (N)-DEMESNE".

The (N)-DEMESNE can be seen as the result of the interconnection of a number of (N-1)-DEMESNEs by some number of (N)-relays. Each (N-1)-DEMESNE, on its turn, can be seen as the result of the interconnection of a number of (N-2)-DEMESNEs by some number of (N-1)-relays. This rule may be applied repeatedly until the physical level is reached.

If the global (N) address is structured in a hierarchic way on basis of lower levelled DEMESNEs to which it is directly attached, then we speak of the use of PREFIX definitions, or "downward selection by prefixes", and the address syntax is as indicated in section 9.2.2.2. If an address used to identify higher layer SAPs ((N+1)-SAPs, (N+2)-SAPs, and so forth), is structured in a hierarchic way by adding suffixes to the (N)-address, then we speak of the use of SUFFIX definitions, or "upwards selection by suffixes".

The resulting syntax of a hierarchically structured (N+p) address is therefore as follows:

(N+p)-address =
(N)-prefix / (N-1)-prefix / ..../ (2)-prefix / (1)-address /
(N+1)-suffix / (N+2)-suffix / ... / (N+p) suffix

Figure 16 summarises the preceding discussion and shows a composite address mapping based on selection of the (N) layer as that providing the global addressing datum, above which adjacent layer address mapping is performed by means of address suffix definition, and below which adjacent layer address mapping is performed by means of address prefix definition.

All mappings which are shown in the figure are applicable to a single End-System. The part of the figure at the outer side of the global addressing datum represent functions in that system in layers above layer (N). The part in the figure below the global addressing datum represents functions which take care of the access of that system at the lowest level DEMESNE. Other systems which are attached to the (N), (N-1), (N-2) DEMESNEs (and with which the End System can communicate) are NOT shown in the figure.

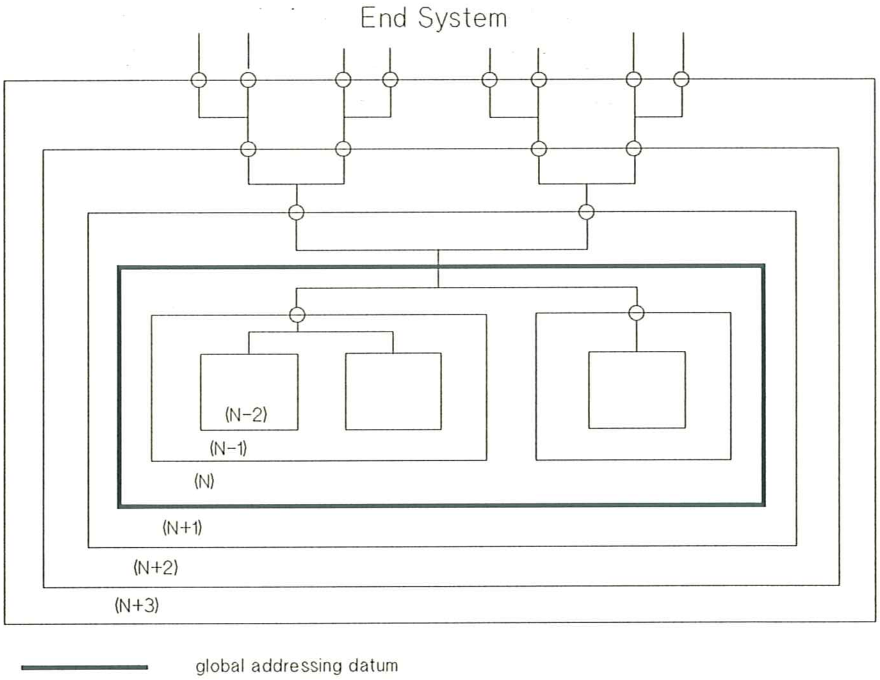


Fig 16 - Composite addressing model

9.3 Relationship to the OSI-Reference Model

9.3.1 Location of the service corresponding to the MLAM global addressing datum

The MLAM, as describes above, is based on the presence of a global addressing datum, by means of which all Open Systems can be identified, and the presence of a hierarchic address-structure at the level of that datum. The level of this global datum was indicated as "the (N)-level".

The degree of success of mapping the MLAM into the OSI-Reference Model depends on the degree in which it is possible to identify such a global datum in the OSI-Reference Model.

The prime candidate for the position of this global datum in the OSI Reference Model is apparently the OSI Network Service (NS). Indeed, the NS represents the service, which is capable to identify all open systems, and is therefore expected to be equal, or at least close, to the global datum identified in the MLAM.

There are, however, two observations that need clarification.

1) The first observation is, that certain standards specifying the structure of OSI Network addresses (such as ECMA-117) allocate the last part of the OSI NS address-structure to a suffix.

   This suffix may be useful, but is not needed to support unique identification of Open Systems.

   Given the fact, however, that such a suffix structure is identified in a NS address, our conclusion must be that, since these addresses standards exist, the global addressing datum in the OSI Reference Model is not located at the OSI NS boundary, but "slightly below" it, i.e. there, where addressing is defined without any suffixing.

2) The second observation is that there are Network Addresses which are conforming to the Network Layer Address standard, but which have no relation to the Subnetwork to which they are attached. As an example, it may be expected that in the near future mobile systems will get an OSI NS address, which has no relation to any geographical or topological network structure.

In this case, however, it remains needed to route data from source to destination. The "natural" way to accomplish that is to start this routing work with a translation from this "flat" address to a structured address that is better suitable to use as a basis for further routing decisions.

Also here, the best way to model this is the location of the global addressing datum "slightly below" the OSI NS boundary. The just mentioned mapping function can then be placed between this global (structured) addressing datum and the OSI NS boundary.

9.3.2 Mapping of MLAM layers on OSI-layers

MLAM-layers below the Global addressing datum are defined on the presence of prefixes. A sequence of prefixes therefore represents a set of MLAM layers. The implication of this is as follows: If e.g. a Network Layer address is structured on basis of three levels of prefixing without the use of Link layer addresses, then three MLAM layers are mapped into one OSI-layer (i.e. the OSI Network Layer). Clause 14 of section IV gives some more details about the implications of this approach.

9.4 Relation to non-OSI Environments

9.4.1 Introduction

According to the MLAM described above, upwards selection by suffixing below the addressing datum and downward selection by prefixing above the addressing datum is excluded. However, if interworking with non-OSI environments is foreseen, then extensions to the model are needed to incorporate this possibility. This will be further explained in the following two sections.

9.4.2 Upwards selection by suffix below the global addressing datum.

There are situations where systems wish to communicate both with OSI systems and non-OSI systems. There is then a need to be able to indicate whether an address, used at the global addressing datum to identify a remote system, points to an OSI-system or to a non-OSI-system. This capability can be achieved by using suffixes below the global addressing datum. This address-suffix can the be used to escape to non-OSI addressing conventions and to non-OSI protocols above the level where such a suffixing is used.

9.4.3 Downward selection by prefix above the global addressing datum

There are situations where systems identified within the OSI Global addressing Datum wish to communicate with other systems which cannot be identified within the OSI Global addressing Datum. In these cases it is needed to be able to indicate whether an address, used in a layer placed above the global addressing datum to identify an entity in a remote system, is or is not built according to the conventions defined for the global addressing datum. This capability can be achieved by using prefixing above the global addressing datum. This address-prefix can then be used to escape to non-OSI addressing conventions (and to non-OSI protocols) on and below the level where such a prefix is used.

9.5 Protocol Identification Methods

On the specific topic of (N+1) layer protocol identification the OSI reference model permits both (N) layer addressing and explicit (N+1) layer PCI encoding to be used.

The problem arising from these alternative methods is that, taken individually, they imply fundamentally different internal (N + 1) layer architectures, or, in Network layer terminology, organisations. The following considers each in turn.

9.5.1 Separation by (N) Layer Addressing

The Reference Model says that an (N + 1) layer sub-system is made up of (N + 1) entities. The Addressing addendum to the Model says that (N) addresses are used to identify (N + 1) entities.

The Model further says that an (N + 1) layer sub-system may support different (N + 1) protocols.

If the (N + 1) layer subsystem of an End system is made up of more than one (N + 1) entities, and each of these (N + 1) entities supports exclusively a single (N + 1) protocol, then (N) layer addressing can be used to differentiate between the (N + 1) protocols. This is illustrated in figure 17. In this figure, X and Y are (N + 1) protocol entities each supporting a single (N + 1) protocol.

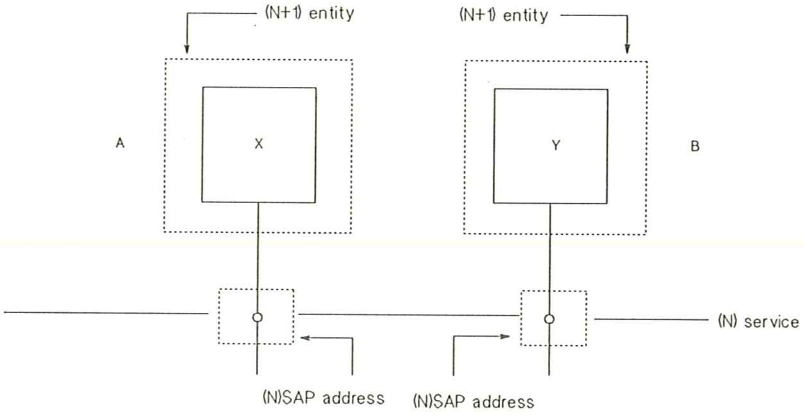


Figure 17 - Protocol identification by (N) layer addressing

Note: in the case of the network layer, different Transport entities are identified by NSAP addresses belonging to different Network addresses

Note: identification of (N + 1) protocols by (N) layer addressing is in agreement with the reference model as long as the principle of layer independence is respected; this requirement is met, if: - the rules for the identification of (N + 1) protocols are known only only in layer (N + 1), and - layer (N + 1) is only relying on knowledge of the structure of (N) addresses as far as defined in the (N) service definition

9.5.2 Separation by (N + 1) Protocol Identifier

The differentiation of (N + 1) protocols by means of protocol identifiers encoded as (N + 1) PCI implies the concept of an (N + 1) entity containing a number of (N + 1) protocol entities each supporting exclusively a single (N + 1) protocol. Differentiation between the different (N + 1) protocol entities is made by a protocol identification function, operating on the protocol identifier part of the PCI of the (N + 1) protocols (the protocol selection function a1 of clause 11.3). The constraint that applies is that all (N + 1) protocols supported within a single (N + 1) entity must conform to a common protocol identifier convention. Figure 18 illustrates the internal organisation of the (N + 1) layer implied by this method of separation. In this figure, X, Y and Z are (N + 1) protocol entities each supporting a single (N + 1) protocol.

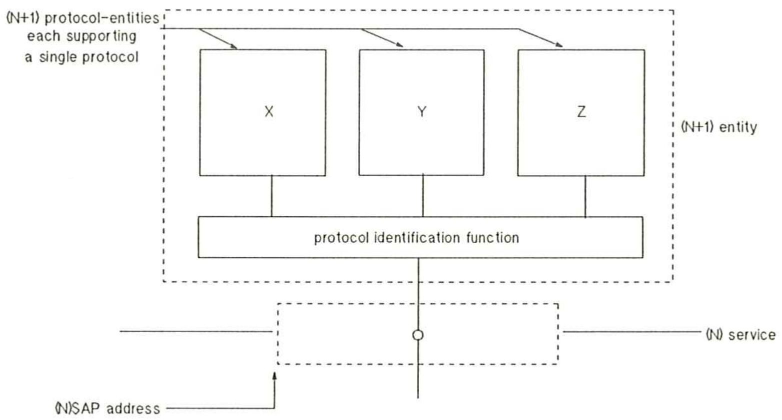


Figure 18 - Protocol identification by (N + 1) protocol identifiers

9.5.3 Comparison of methods and areas of application

It may be seen that, taken individually, the essential distinction to be made between the foregoing methods is the degree, or level, of freedom each offers with respect to the possible mixes of protocols that may be supported by the (N + 1) layer sub-system of an open system:

- non-OSI, and in general protocols not conforming to a single protocol identifier convention, require to be separated by addressing
- OSI, and in general protocols that do conform to a single protocol identifier convention, could be separated by means of protocol identifiers

NOTE 27

Protocols belonging to the same OSI set may still be separated by means of addressing; this effectively treats them as belonging to different sets.

10. CONSTRAINED NETWORK SERVICE PROVIDER MODEL (CNSPM)

10.1 Introduction

In this Clause a multi-layer architecture for the OSI Network Service Provider is defined, which embodies all the layer and sublayer service boundaries that have been found useful in practice to separately identify and standardize. This model will be denoted as the "Constrained Network Service Provider Model" (CNSPM).

The architecture is consistent with the concepts of Clause 10 and should be seen as a constrained version of the unconstrained model UNSPM given that the only protocol intervention levels permitted within the framework of OSI were those identified by the CNSPM.

The architecture is also consistent with the principles of ISO 8648 as they have been defined by ISO as applying to the Network Layer. These principles are applied recursively to those lower layers of the constrained model which are supported by protocols defined as carrying layer addressing parameters.

This Clause also gives examples of the way in which the architecture maps to the protocol structures of existing networks.

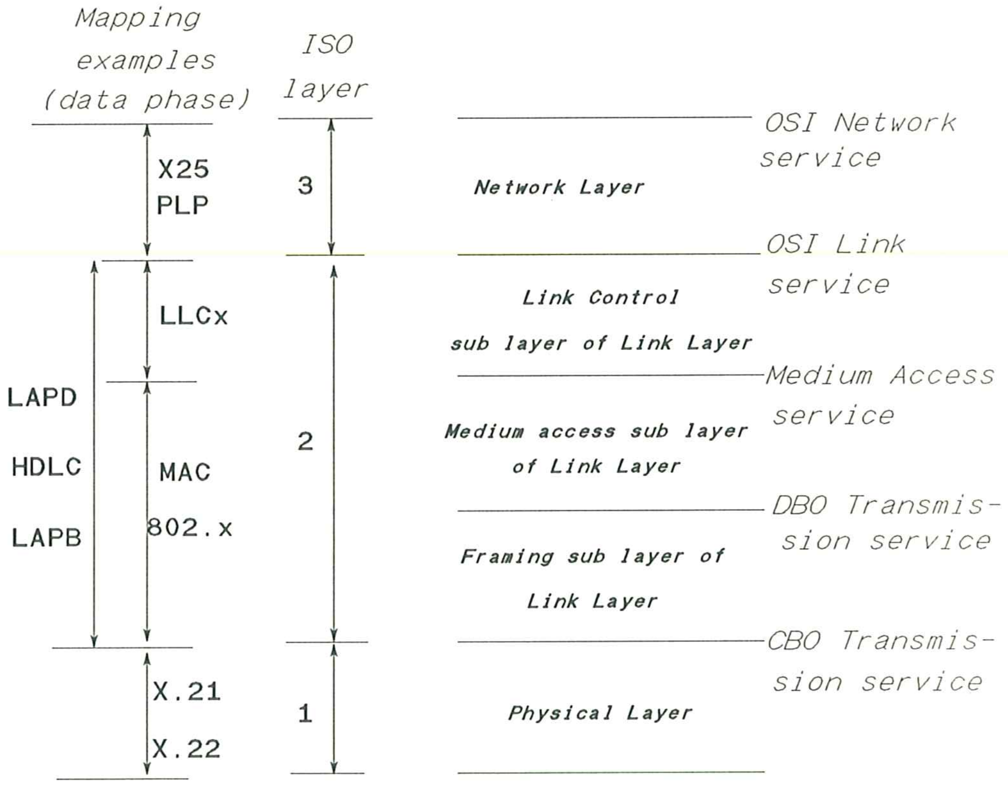
10.2 The Basic CNSPM

The Basic CNSPM embodying the service boundaries that it has so far been found useful to separately identify and make subject to standardization is illustrated in figure 19(a). The corresponding Generic Header Format is illustrated in figure 19(b).

NOTE 28

In these figures it is assumed that the OSI Data Link Service corresponds to that defined by the IEEE.

a) Basic Network Layer Service Provider Model



b) corresponding Generic Header Format

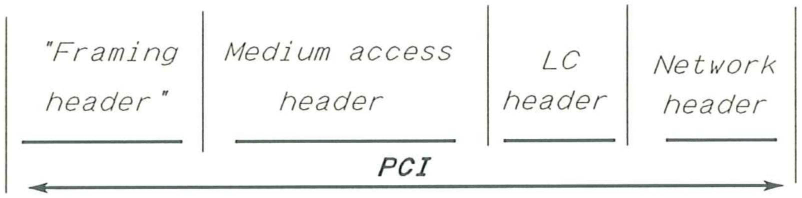


Figure 19 - Basic Network Layer Service Provider Model and Corresponding Generic Header Format

10.3 Refinement of the Basic CNSPM

Refinement of the Basic CNSPM can be performed by incorporating the contents of ISO 8648 into the Network Layer. Before doing this, the contents of ISO 8648 will first be examined and modelled to determine what, if any, IS 8648 concepts are relevant to other layers.

10.3.1 Interpretation of ISO 8648

The following identifies and gives the substance of the clauses of ISO 8648 relevant to the construction of the Network-Layer Model:

- clause 5.3 states that the term subnetwork may be applied recursively to collections of subnetworks interconnected in such a way that, to an attaching system, they can be viewed and treated as a single subnetwork ;
- clause 6.1 states that an element in determining the role of a protocol is the definition of both the agreed service to be provided by the protocol and the service assumed to underlay it ;
- clause 6.3 states that relay and routing functions in Network entities "inside" a real subnetwork are associated with the operation of protocols fulfilling the SNAcP role ;
- clause 6.6 makes an explicit distinction between relay and routing functions that are located in Network entities "outside" real subnetworks and those located "inside".

The above may be taken as implying the need to make a distinction between the following two kinds of relay and routing functions at the Network Layer:

i) the kind outside a subnetwork and existing to operate on parameters that are globally defined within the Network Layer as a whole;

ii) the kind inside a subnetwork and existing to operate on parameters which are only significant in the context of this particular subnetwork.

Considering the connection-oriented case and making the assumptions that:

- all subnetworks are of the X.25 (1984) kind in the sense that their access protocols are designed to fully support the OSI Network Service;
- all subnetworks are at a stage in their evolutionary development where they have chosen not to actively operate on globally defined parameters but merely to transfer them as, in effect, subnetwork user data;
- a number of interconnected subnetworks sharing the same addressing conventions and guaranteeing the uniqueness of the addresses are treated as a single subnetwork;

then it becomes clear for this case that:

- the relay and routing functions outside of the subnetworks can be treated as being of the "inter-subnetwork service relaying" type;
- the relay and routing functions inside of the subnetworks can be treated as being of the "intra-subnetwork protocol relaying" type.

It should be particularly noted that both types of relay are, for the case being considered, Network Layer relays.

These considerations are sufficient to enable a Network Layer Model to be constructed in terms of Link Service Providers and the different kinds of relay and routing functions that have been identified. The model is illustrated in figure 20.

In this figure the term "Service Enhancement Protocol" is used to mean the special case of a convergence protocol (see Clause 5.16) defined to raise a standardized lower layer service to the level of a standardized next-higher layer service.

This figure shows that the functions of the Network Layer (indicated as the (N)-layer) can be subdivided into two hierarchically related functional groupings. The lower level functional grouping is called the intra-subnetwork r+r functionality, the higher level functional grouping is called the inter-subnetwork R+R functionality.

Apart from relaying and routing, the r+r functionality performs the (N)-EP protocol operation which raises the (N- 1)-service up to the (N)-service. The r+r functionality is however not capable of interpreting and operating on parameters which are significant for the whole (N)-service address space. Therefore, this (N)-EP protocol is said to operate "within an (N)-subnetwork only".

The R+R functionality is not supported by an independent protocol. It does not perform any protocol operation but is capable of interpreting and acting upon GDPs (transparently transferred by the (N)-EP protocol). Therefore, this R+R functionality is said to operate "within the whole Network-Layer".

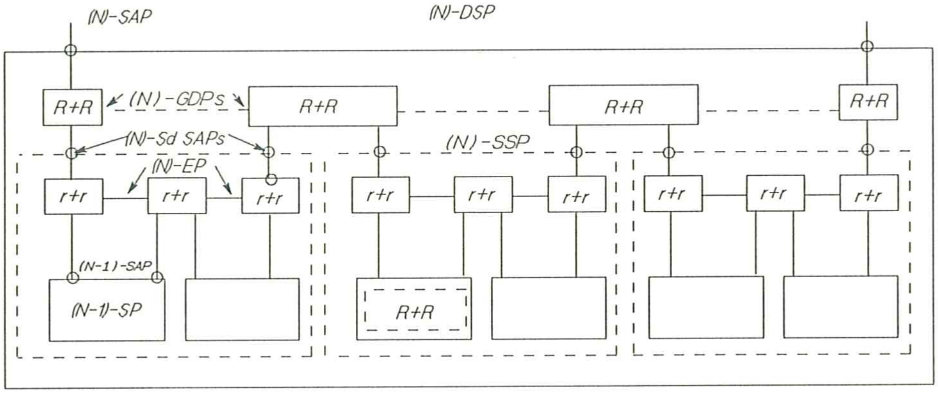
GDPs embrace both global addresses and globally defined Quality of Service (QoS) parameters. The R+R functionality is concerned with generation of the local address and local QoS parameters to be given to its associated subnetworks to satisfy global requirements.

Two kinds of QoS parameters may be distinguished:

i) those which require the local QoS parameters of the concatenated subnetworks to be summed to yield a global QoS parameter, and

ii) those where the global QoS parameters are the minimum quality of the local QoS parameters of the concatenated subnetworks.

a) Generic (N)-Layer Service Provider Model



Legend

(N)-SP : (N)-domain service provider

(N-1)-SP : (N-1)- service provider

(N)-GDP : (N)-layer globally defined parameters

(N)-SSP : (N)-subnetwork service provider

R+R : Inter-subnetwork relay + routing function

r+r : Intra-subnetwork relay + routing function

(N)-EP : (N-1) to (N)-service enhancement protocol + GPD carrier

N : 3

b) Corresponding Generic Header Format

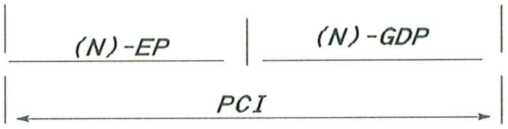


Figure 20 - Generic (N)-layer Service Provider Model and Corresponding Generic Header Format

Transit delay is an example of the first type. Throughput might be an example of the second, given restrictions on the number of parallel connections that can be established via a SN to support a global connection.

As for global addressing parameters all subnetwork access protocols should be defined to at least support the transparent transfer of globally defined QoS sub-parameters to support the R+R functionality.

NOTE 29

The R+R functionality in figure 20(a) corresponds with the R+R functionality defined in the UNSPM developed in Clause 10. However, since in Clause 10 a layer is defined as the set of functions located between two adjacent protocol intervention levels of de facto existing *subnetworks, a single layer in the UNSPM can only contain one R + R functionality. Therefore, the network layer as shown in figure 20(a) has to be seen as embodying greater than one layer of the UNSPM to the extent of embodying two levels of R + R functionality.*

Intermediate systems can be built which intervene up to and including the R + R functionality, or up to and including the R + R functionality. The first category creates a subnet service boundary denoted as (N)-SSP; the second category creates a subnet service boundary denoted as (N)-SP.

Figure 20(b) shows the corresponding Generic Header Format (see 6.1).

Further refinement of this format is given in Clause 11.

10.3.2 The refined Network Layer Service Provider Model

10.3.2.1 The relation between ISO 8648 and the OSI Reference Model

With respect to routing and relaying, the reference model states, that:

1) logically or physically disjoint (N) layer addressing domains can still be interconnected by the use of (N + 1) layer relays.

2) Relaying above the Network Service boundary is not permitted.

Taking these two statements in combination, it has to be concluded that subnetworks supporting logically or physically disjoint Network layer domains cannot be interconnected: if this interconnection is realised within the Network Layer, statement 1 is violated ; if it is realised in the Transport layer, statement 2 is violated.

Nevertheless, ISO 8648 was developed, resulting in the identification of two distinct routing functional groups (in 10.3.1 denoted as R + R and r + r) within the Network layer. In fact, this approach was unavoidable, since many physical networks claimed to support the protocols located in the Network layer, but could not claim to actively operate on all parameters needed to support routing between all N-SAPs.

10.3.2.2 Implications for possible refinement of the layers located below the Network layer

The layers below the Network layer all have the property that there is an adjacent higher layer available, where disjoint addressing domains can be interconnected by relays in that adjacent higher layer. Therefore, there is no need to introduce here new levels of routing and relaying in the same layer, and therefore there is no need to violate any statement made in the Reference Model related to the principles of Relaying and Routing. ISO 8648 is, and should be, restricted to the Network layer only.

```
_______________________________________________ OSI NETWORK SERVICE

3 B                    Inter-subnetwork R+R

----------------------------------------------- OSI SUBNET SERVICE *)

3 A                    Inter link R + R
                   (or intra subnetwork r+r)

----------------------------------------------- LINK SERVICE

2 C                    Inter MAC R + R

----------------------------------------------- MAC SERVICE #)

2 B                    Inter DBO R+R

----------------------------------------------- DBO SERVICE

2 A                    Inter CBO R

----------------------------------------------- CBO SERVICE

1                      Inter medium R

-----------------------------------------------
```

*) an OSI subnet is a subnetwork that supports the ISO NS in all aspects other than addressing.

#) a MAC service is defined according to the emerging MAC service definition standard

Figure 21 - Refined Multi-Layer Architecture

Figure 21 shows the resulting refined Network Service Provider Model.

In this refined model, R+R functions located in layer (N) are always used to interconnect disjoint address domains in layer (N-1).

Note that layers 2A and 1 only contain relaying, and no routing, since addressing functions are absent in these layers. The lowest level where addressing is supported is the MAC service. The lowest level where connections are supported is the Link service.

10.3.3 Reduction of refined multi-layer architecture

The multi-layer architecture of figure 21 permits a total of six different kinds of IS, four performing either an intelligent inter- or intra- subnetwork relay and routing function and two performing an unintelligent frame or bit broadcast relay function.

However, we note that a number of the theoretical possibilities provided for by the refined model have no practical counterpart in terms of real-world systems. Specifically, the current 8802 MAC bridging proposals provide for the interconnection of LANs that can be heterogeneous with respect to all aspects of their access protocols except for the addressing conventions they support. The latter must be homogeneous. Accordingly, the proposals in effect preclude the differentiation of the two kinds of MAC bridging provided for in the refined multi-layer architecture model.

10.3.4 Application of the multi-layer architecture to switched DBO and CBO services

We note that the lowest service boundary in figure 21 at which the concept of a connection becomes meaningful is the Link subnetwork service boundary (2c). Below this boundary all other boundaries provide a connectionless service.

Accordingly, in the same way that the 8802 set of LAN standards adopts the MAC service boundary as that below which LAN technology dependent issues will be differentiated, so too we adopt the Link Service boundary as that below which different forms of connection-oriented network technology will be differentiated.

Figure 22 gives an interpretation of figure 21 reflecting this choice of common datum and shows the functions of the various sublayers for various kinds of CL and CO technologies.

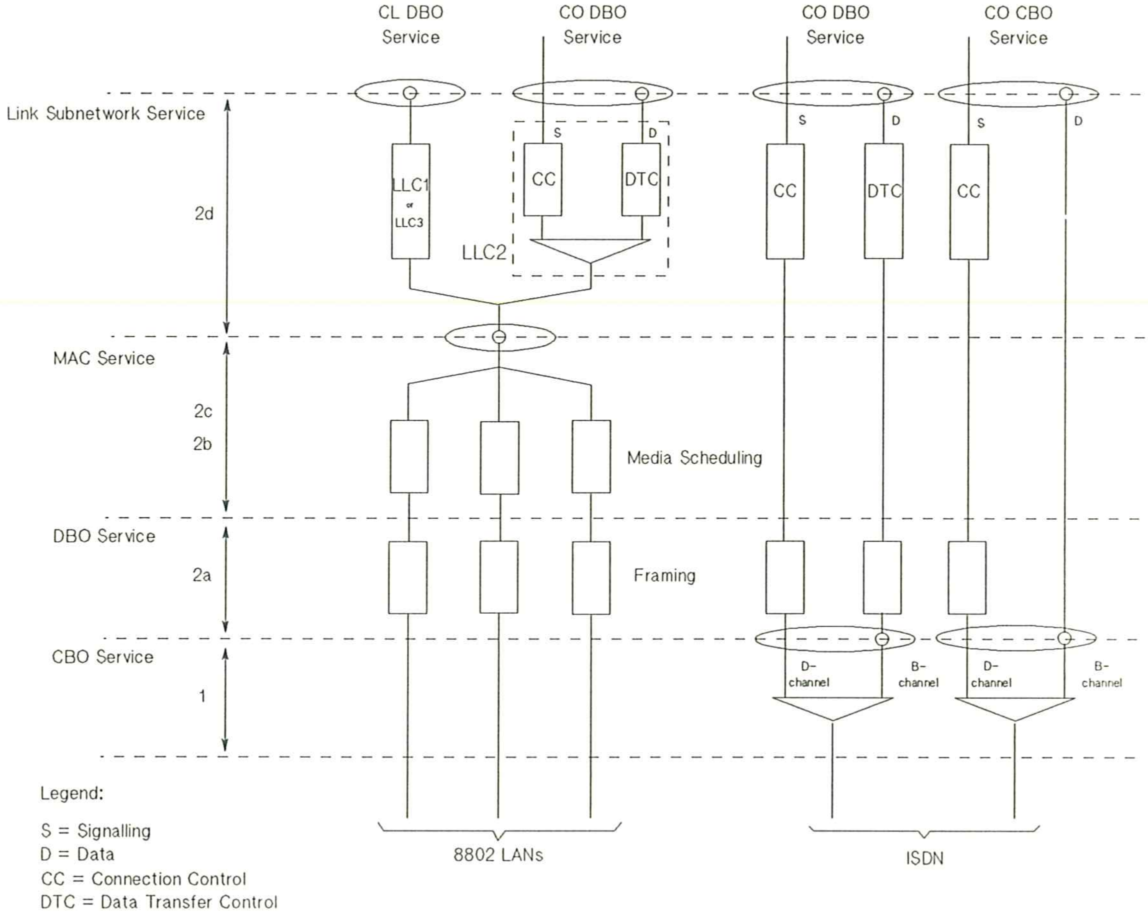


Figure 22 - Interpretation of multi-layer model for different technologies

10.3.5 Expansion of functions of multi-layer model

Figure 23 gives an expansion of functions of the model of figure 21 in accordance with the considerations of 10.3.3 and 10.3.4.

```
OSI Layers
--------------------OSI Network service-----------------------
|     Network Layer inter-subnetwork relay and routing N (R+R)
| 3b  - Global network addressing and QoS functions
|     - Network Layer subnetwork bridging
|
| -----------------Network Layer subnetwork Service------------
|     Inter-link relay and routing (r+r)
3     - Network Layer subnetwork addressing
| 3a  - Fragmentation/reassembly
|     - Network Layer subnetwork protocol conversion
|     - Network Layer subnetwork connection control
|     - Link service bridging
|
| -----------------Link Service ------------------------------
|     Inter MAC relay and routing L(R+R)
|     - Link service addressing
| 2c  - Flow control
|     - Error control
|     - Link protocol conversion
|     - MA service bridging
|
|------------------ Medium Access Service----------------------
|     Inter DBO relay and routing MA (R+R)
|     - MA service addressing
2 2b  - MA subnetwork bridging
|     - MA protocol conversion
|     - DBO Service  Bridging
|------------------ DBO Transmission Service ------------------
|     Inter CBO relaying
|     - Frame delimiting
| 2a  - Frame level repeater
|     - Frame code conversion
|     - Error detection
|
|------------------- CBO Transmission Service -----------------
|
|     Inter medium relaying
1     - Bit stream transmission
|     - Bit coding conversion
|     - Bit level repeater
|
```

The corresponding Generic Header Format corresponds with that shown in Figure 19(b)

Figure 23 - Expansion of functions of the refined multi-layer architecture

SECTION III

GENERIC LAYER ARCHITECTURE MODEL

11. GENERIC LAYER ARCHITECTURE (GLA) MODEL

11.1 Introduction

This Clause describes a layer-protocol reference model or "Generic Layer Architecture" (GLA), based on sub-layering principles, which can be applied to any protocol which is described in terms of a specification of one layer-entity spanning a complete layer. The sub-layering principles adopted are those defined by the OSI Reference Model (IS 7498).

The architecture is "generic" in the same sense that the OSI Reference Model is generic. The latter is an abstract model applying equally to all open systems of the OSI environment irrespective of implementation considerations. The GLA is an abstract model applying equally to all OSI layer 1-4 protocols irrespective of their particular protocol elements and the particular techniques used to encode these elements. Companion with the concept of a Generic Layer Architecture is the related concept of the "Generic Header Format" as defined in 6.1.

Throughout this Clause, each figure showing a sublayer structure will be accompanied by a figure showing the corresponding Generic Header Format.

In the development of the GLA, attention is focused on those protocol functions which are seen as being common to most lower layer protocols within the public domain, up to and including the OSI Transport Protocol.

The GLA and GHF cover both CO and CL modes of interworking. To achieve consistency in the modelling of these modes it was found necessary to introduce a new modelling concept not defined by the OSI Reference Model. The concept is that of a CL Service End Point (SEP) within the domain of a Service Access Point (SAP).

This concept of a SEP is introduced specifically to achieve consistency between CO and CL concepts as they relate to the fan-in/fan-out functions of CO, CL, and hybrid CO/CL layers. In the same way as a (CO) CEP is defined as an entirely abstract construct that may in reality be implemented as a CEP-ID parameter of a layer interface primitive, so too a (CL) SEP is defined as an entirely abstract construct that may in reality be implemented as a remote SAP-ID parameter.

If no distinction need be made between CO (CEP) and CL (SEP), the term "Information Flow Identifier for an instance of communication" (IFI) will be used.

NOTE 30

Consistency of CO and CL modelling concepts could otherwise have been achieved by abandoning the OSI Reference Model concept of a (CO) CEP in favour of specific parameterization of connection identification in service primitives. Of the two possible approaches the one adopted is consistent with existing OSI Reference Model connection-oriented modelling concepts. This Clause deals primarily with the modelling of data transfer functions. The modelling of signalling is discussed further in Clause 12.

The benefits deriving from the definition of a GLA are seen to be the following:

i) It provides a framework for the comparison of existing layer 1-4 protocols and hence layer 1-4 protocol sets.

ii) it facilitates the further development of existing protocols and protocol sets to satisfy new applications.

iii) It facilitates the design of new protocols optimized for specific applications.

iv) It provides a framework for the ongoing rationalization of OSI layer 1-4 services and protocols.

The additional benefits seen as deriving from the definition of the GHF are the following:

v) It gives insights into the way in which PCI should be encoded (see 6.1). Since the GHF precisely reflects the "natural" order of processing steps of a protocol, the degree of correspondence between the GHF and the format which is in concreto used (called "Concrete Header Format") is directly related to the degree to which it is possible to implement a protocol in a partitioned way.

vi) It may have application in the areas of analysis and formal specification of protocols.

11.2 Protocol Control Functions and Fan-in/Fan-out Functions

As a first step in the development of the GLA and GHF, the PCI encoded in a concrete layer header (i.e. the Concrete Header Format) is divided into three parts:

- That part which embraces all information relating to the functions performed on a common basis for all individual connections, or information streams, within a layer.
- That part which embraces all information relating to the fan-in/fan-out functions performed within a layer as they relate to SAP selection and connection identification.
- That part which embraces all information relating to the functions performed on each individual connection, or information stream, within a layer.

PCI in the first category embraces control information relating to, for example, error checking, PDU delimiting, and protocol selection.

PCI in the second category embraces, for both CO and CL modes of interworking, source and destination address, or address- related, information. For CO mode it additionally includes connection identification and/or referencing information.

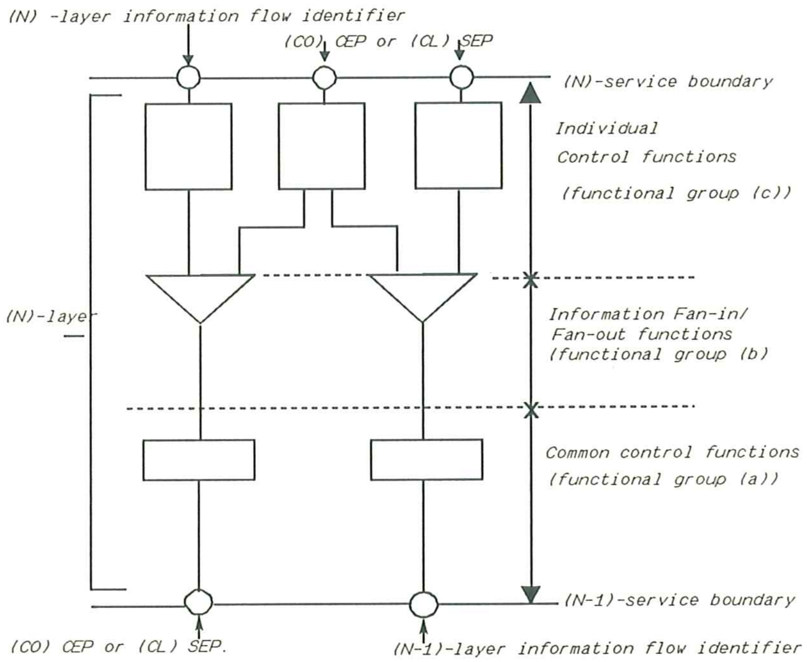
PCI in the third category embraces, for CO mode, control information relating to, for example, the functions of error control, flow control, maintenance of sequence integrity, and so on. For both CO and CL modes it includes control information relating to the functions of segmentation and blocking.

In general, the layer functions supported by these different categories of PCI exist in a hierarchical relationship to one another. For example, following reception it is necessary to operate on fan-in/fan-out information before performing operations that relate to a specific connection or, for CL mode, a specific information stream. The reverse order applies for transmission.

Accordingly a layer protocol is taken as conforming, at a first level of magnification, to the architecture of figure 24.

Protocols not conforming to this architecture are treated as special, or hybrid cases.

a) Positioning of control functions and fan-in/fan-out functions in an (N)-layer



b) Corresponding Generic Header Format

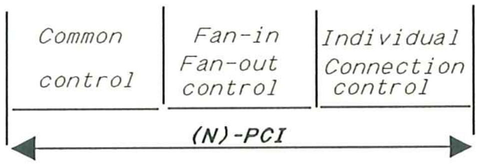


Figure 24 - Positioning of control functions and fan-in/fan-out functions in an (N)-layer, and Corresponding Generic Header Format

11.3 Expansion of Common Control Functions

Figure 25 shows the five most frequently used common control functions of a layer, implemented as sublayers a1, a2, a3, a4 and a5 of the GLA. The lowest sublayer (a1) takes care of the selection of the current protocol and is called the "protocol selection sublayer". This function is placed at the bottom of the layer since for the receiving system this information is needed to chose the correct functionality of the adjacent higher sublayer. In terms of the GHF it means that this part of the (N)-header is needed to enable interpretation of the subsequent parts of the (N-1)-SDU.

The adjacent higher sublayer (a2) executes a PDU delimiting function. This function is needed in all cases where the (N)- PDU has no one-to-one relationship with the (N-1)-SDU. This function may manifest itself in two ways:

i) As a mechanism to reconstruct a PDU out of an incoming continuous bitstream. In other words, it occurs if a DBO service is built on top of a CBO service (see Appendix B of this Technical Report). A classic example is the HDLC flag mechanism.

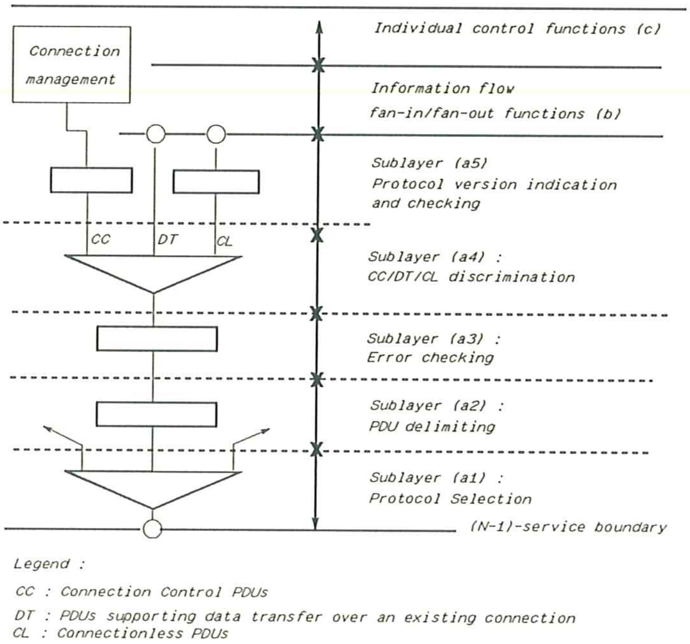
ii) As a concatenation/separation function. In this case an (N-1)-SDU carries more than one (N)-PDU. At the receiving side, the boundaries of these PDUs are reconstructed in this sublayer.

The PDU delimiting function is placed above the protocol selector because coding rules which apply to this delimiting means that concatenation of PDUs can only be achieved on the basis of one common delimiting coding rule which applies to all (N)-PDUs carried in a single (N-1)-SDU.

The adjacent higher sublayer (a3) executes, if desired, an error check to detect transmission errors on a shared rather than on an individual connection basis. This checksum function does not include error correction by means of some PDU repeat mechanism since this assumes the execution of an explicit protocol which is almost always only done on individual connection basis. Therefore, the occurrence of an error is either reported to the error correction functionality at the top of layer (N), or the data unit is simply discarded.

The checksum function is placed above the protocol selection function and the PDU delimiting function, because the CRC calculation method may be dependent on the protocol selector value, and the checksum has to be calculated for each individual PDU.

a) Sublayers of the GLA with expanded common control functions



b) Corresponding Generic Header Format

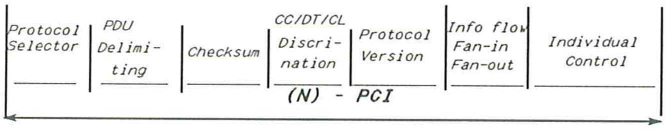


Figure 25 - Sublayers of the GLA with expanded common control and corresponding generic header format

NOTE 31

It should be noted that in some existing protocols the checksum calculation includes the protocol selector and/or PDU delimiting function. In these cases, sublayers a1, a2 and a3 cannot be implemented as independent sublayers.

The checksum is also placed below the CC/DT/CL discrimination function since this is the lowest possible location, and the checksum should protect the information exchanged between a maximum number of sublayers.

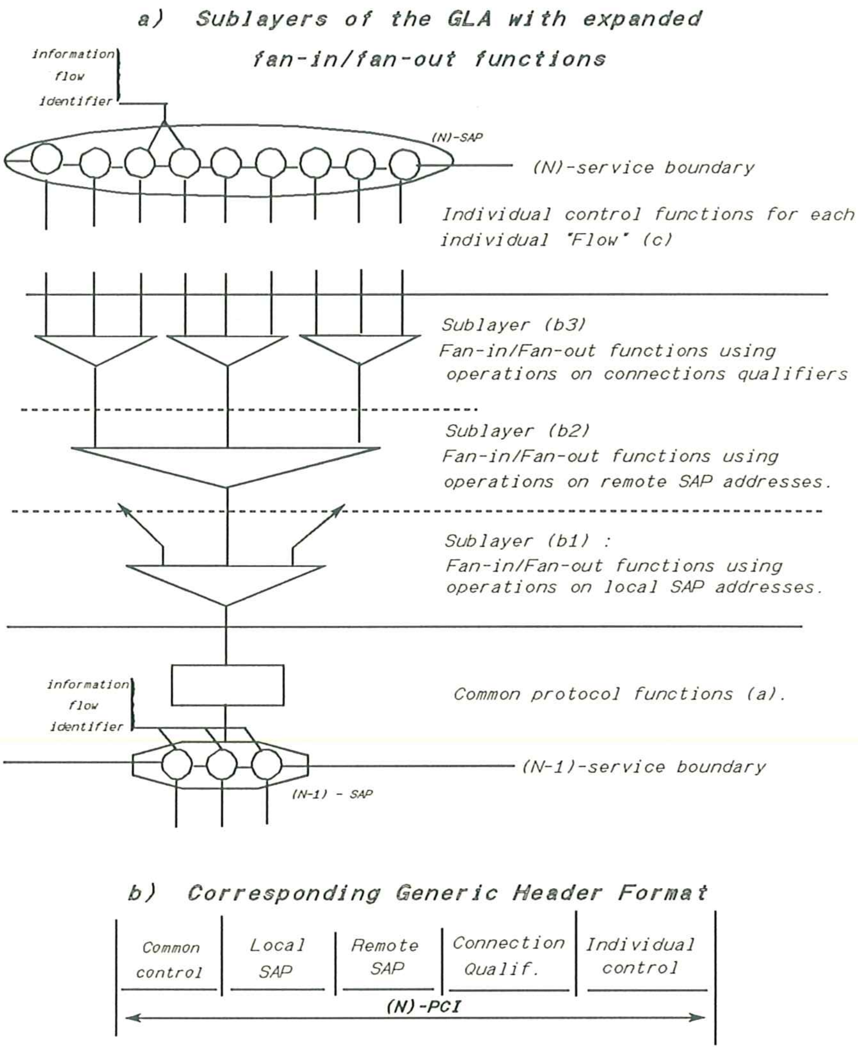
NOTE 32

In the GHF of figure 25(b) the checksum is placed after the protocol selector. However, the checksum is traditionally calculated at the sender side "on the fly". Therefore in most concrete formats the checksum field is located at the end of the PDU. In the Generic Header Format (which is abstract), however, this field is located as shown in figure 25(b). The adjacent higher sublayer (a4) takes care of the discrimination between CL and CO data flows, and in addition within the CO data flow between call control and data transfer PDUs. The separation of call control has to be done at this sublayer because the coding of the address fan-in/fan-out fields associated with sublayers b1, b2 and b3 (see 7.4 hereafter) is usually different for call control (CC), CO data transfer (DT), and CL data transfer PDUs (CO data transfer PDUs usually contain reference numbers in the concrete header syntax; see 11.4.3). The adjacent higher sublayer (a5) takes care of the checking of the protocol version numbers. This function is absent in CO data transfer PDUs because the corresponding connection set-up PDU usually takes care of that.

Since the address fan-in/fan-out in the adjacent higher sublayer has to work without a priori knowledge of the individual connection (this is only known at the top of sublayer b2), sublayer a2, a3, a4, a5, b1, b2, and b3 functions must be common for all protocol versions sharing a single (N-1)-SAP.

NOTE 33

If this constraint is unacceptable, then the different protocol versions have to be considered as different protocols (to be handled by sublayer a1).



*) In a connection-oriented environment, an "information flow identifier" is denoted as a "connection end point identifier"; in a connectionless environment it is denoted as a "service end point identifier".

Figure 26 - Sublayers of the GLA with expanded fan-in/fan-out functions and corresponding generic header format

11.4 Expansion of GLA Fan-in/Fan-out Functions

11.4.1 General

Figure 26 gives an expansion of the GLA of figure 24 as it relates to the fan-in/fan-out functions performed by an (N)- layer protocol. The illustration is of a layer entity supporting three (N)-SAPs. For clarity only one of these is shown completely.

With reference to figure 26 the functions of sublayers b1, b2 and b3 are as follows:

Sublayer b1

This sublayer embodies the fan-in/fan-out functions of a protocol which are based on operations performed on local (N)-SAP addressing information, i.e. received destination address information and transmitted source address information.

The sublayer is non-empty in all cases where a protocol supports multiple (N)-SAPs over a single (N-1)-SAP.

If the protocol does not support this, then the sublayer is empty and the local (N)-SAP may be taken as implied.

Sublayer b2

This sublayer embodies the fan-in/fan-out functions of a protocol which are based on operations performed on remote (N)-SAP addressing information, i.e. received source address information and transmitted destination address information.

The sublayer is non-empty for all cases where a protocol supports discrimination between information flows sharing a single local (N)-SAP but each related to a different remote (N)-SAP, irrespective of whether or not the remote (N)-SAPs are distributed or co-located in the same remote system.

In a CO environment this sublayer represents the capability of a protocol to support simultaneously a number of (N)- connections sharing a single local (N)-SAP but each related to a different remote (N)-SAP.

If a protocol does not support this, then the sublayer is empty and the remote (N)-SAP may be taken as implied.

Sublayer b3

This sublayer embodies the fan-in/fan-out capabilities of a protocol which are based on operations performed on connection identification within the domain of a pair of local and remote (N)-SAPs. These identifiers are called "Connection Qualifiers", and the operation is called "Connection Qualification".

In a CO environment this sublayer is non-empty in all cases where a protocol simultaneously supports a number of parallel (N)-connections between a local (N)-SAP and a particular remote (N)-SAP. If a protocol does not support this, then the sublayer is empty.

It should be noted with respect to the above sublayers that in a CO environment all sublayers may be referred to as multiplexing sublayers. Accordingly, precision in the use of the term "multiplexing" requires the term to be qualified as being of the b1, b2, b3 type or some hybrid variety.

Note also with respect to sublayer b3 that the term "connection qualification" is used to mean something different to "connection referencing" as for example used in the Transport Protocol. The term "qualification" is used to mean identification within the domain of a specific pair of local and remote SAPs. The term "referencing" is used to mean referencing within the domain of a set of local SAPs (see 11.4.3).

11.4.2 Nesting Rules and the Generic Header Format

In the GHF shown in figure 26(b) the remote SAP field is placed after the local SAP field. Since the notions "local" and "remote" are by definition dependent on the position of the observer, a local system would not naturally generate for transmission a layer header format with sub-fields in the order required by the receiver of a remote system. Indeed, the natural order for the transmitting system in terms of source and destination address fields is:

Source Address / Destination Address / Connection Qualifier,

while that appropriate to the receiving system is:

Destination Address / Source Address / Connection / Qualifier

Therefore, sublayers b1 and b2 of the GLA represent an interesting exception to straightforward nesting rules. As a consequence, they should be treated for nesting purposes as a single sublayer subject to an agreed convention with respect to the order of the address fields.

11.4.3 Protocol Connection Referencing

A number of CO layer 1-4 protocols define PCI to support connection referencing in some form or another, for example the OSI Transport Protocol, and the X.25 Packet Level Protocol.

When connection referencing is used, connection reference numbers are exchanged during the establishment phase for use during the data phase.

A connection reference uniquely identifies a particular connection within the domain of a local (N)-SAP and therefore includes a remote (N)-SAP component (sublayer b2) and possibly a connection qualifying component (sublayer b3).

It may also identify the connection within the domain of a set of more than one local (N)-SAP; it then includes a local (N)-SAP component as well (sublayer b1).

If connection reference numbers are exclusively assigned by the receiving entities at both sides of the connection, they will usually be different for both directions of data transfer, and may then even embody a fourth, implementation- specific, component (for example a pointer to a local memory location related to the processing of this incoming data flow). This is, however, not visible for the remote system and therefore goes beyond the scope of the GLA.

When connection reference numbers are not used, the fan- in/fan-out capability of a layer can still be achieved, but sublayer b1, b2, and b3 protocol elements have then to be coded explicitly in the concrete header.

Therefore, the GLA and GHF are taken to apply generally to all layer 1-4 protocols irrespective of whether or not they make use of connection referencing mechanisms. If they do, then the GLA and GHF are taken as applying in an abstract sense. If they do not, then the GLA and GHF are taken as applying in a real sense.

11.5 Expansion of Individual Connection Control Functions

Figure 27 gives an expansion of the GLA of figure 24 as it relates to the individual connection control functions of an (N)-layer protocol. The error control sublayer (c1) protects the higher sublayers from protocol errors. This function detects protocol errors and takes recovery action within the confines of the information flow in which the error occurred.

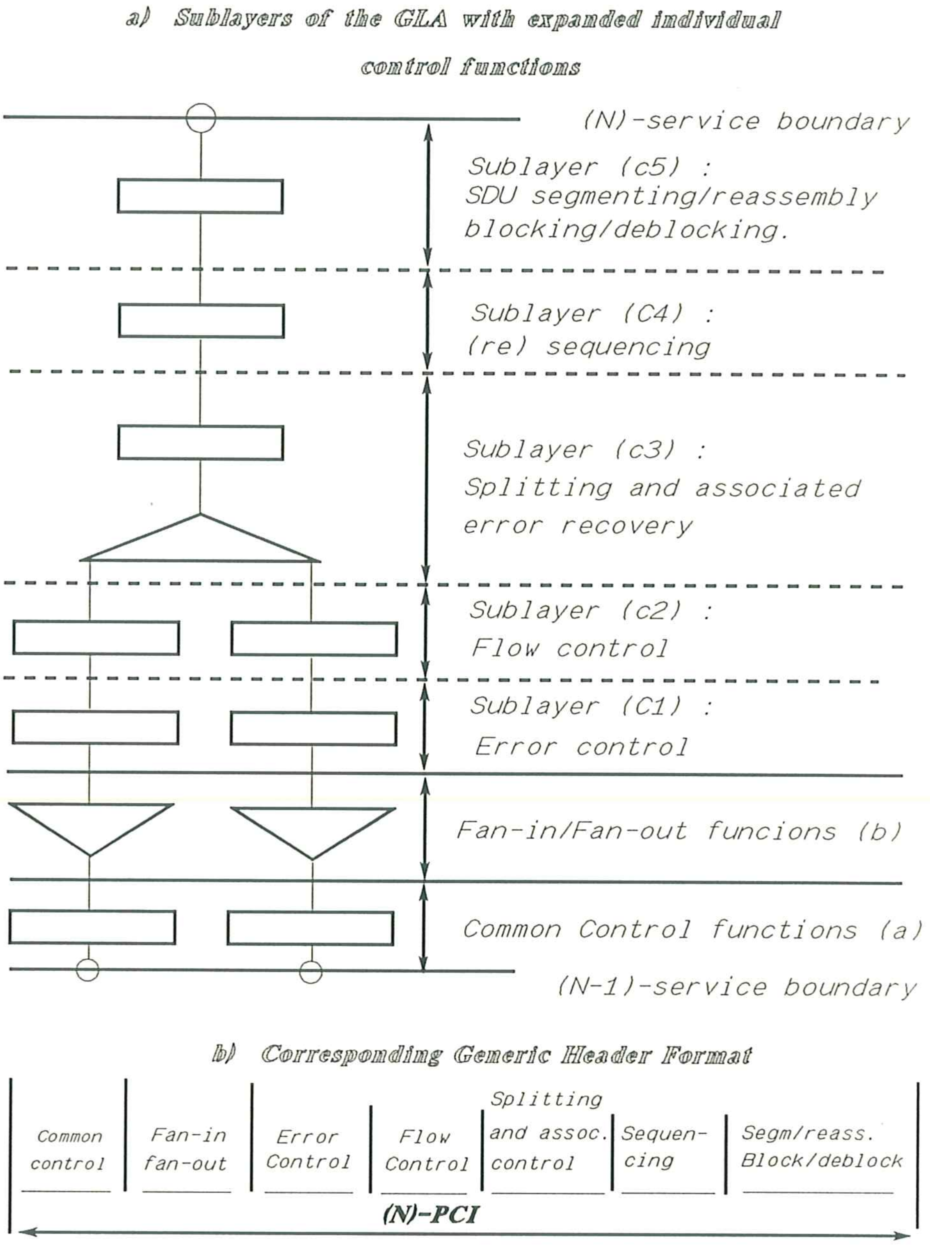


Figure 27 - Sublayers of the GLA with expanded individual control functions, and Corresponding Generic Header Format

The flow control sublayer (c2) provides functions that allow the receiver to control the number of outstanding PDUs on a connection and therefore the ability to manage the buffer requirements placed on the end system by the connection.

NOTE 34

The location of this function below the splitting function allows an implementation to individually manage the buffers associated with connections supporting the splitting function if it wishes to do so.

Sublayer c3 contains two functions:

- *a splitting function, which allows the transfer of PDUs associated with a connection over several individual information flows;*
- *a splitting error recovery function, which allows error recovery making use of the fact that alternative flows are available.*

The resequencing function (c4) allows PDUs to be (re)sequenced so that they are presented to sublayer c5 in the receiving system in the same order as they were presented to sublayer c4 in the transmitting system.

NOTE 35

The structural principles adopted by the GLA require that each sublayer has its own individual PCI which no other sublayer is allowed to act upon. The implication is that sublayers c1, c2, c3 and c4 each operate a numbering scheme that is part of their individual PCI. In practice however, most current protocols are using one numbering scheme that is used to achieve all these functions.

The highest sublayer (c5) contains the segmenting/reassembly function and the blocking/deblocking function. With respect to the blocking/deblocking function the following additional observations can be made:

i) *Blocking/deblocking can be seen as "SDU-delimiting" (in contrast with concatenation/separation, which is a form of "PDU-delimiting"; see 11.3).*

ii) *Blocking/deblocking in layer (N) has the same objective as concatenation/separation in the adjacent layer (N+1). Both provide a mechanism to map more (N+1)-PDUs into a single (N)-PDU. However, if the (N+1)-PDU boundaries are reconstructed on the basis of (N+1)-PCI information, then it is called concatenation; if reconstruction is on the basis of (N)-PCI information, then it is called blocking.*

iii) *Blocking implies that all SDUs located in a PDU after the first one are made available only after processing (large parts of) the PCI of the first SDU. If these subsequent (N)-SDUs belong to other (N)-connections, then the functionality of lower sublayers becomes dependent on the functionality of higher sublayers. Therefore, blocking shall be restricted to combining SDUs belonging to the same connections only. Violating this rule leads to reduction of sublayer independence.*

11.6 Hybrid Implementations of the GLA

Given the sublayer structure of 11.3, 11.4 and 11.5, it becomes possible to envisage a large number of hybrid layer implementations in which the members of the sublayer sets a, b and c are interleaved. If the number of sublayers within a set is increased and their order allowed to vary, then the number of possibilities becomes even larger.

A hybrid of particular interest is that in which the error control sublayer is implemented as a common connection control function below the fan-in/fan-out sublayers.

This is seen as the particular hybrid that describes the X.25 level 2 and level 3 protocol structure, if both protocol levels in combination are seen as a single GLA layer.

11.7 An Example of the Application of the GLA to a Protocol

As an illustration of the way in which the GLA can be applied to the real world, the OSI CO Transport Protocol is chosen here as subject to GLA analysis.

The result is figure 28. It is clearly visible in this figure that the selection of a higher protocol class in general leads to the invocation of more GLA sublayers.

The fan-in/fan-out sublayers b1, b2 and b3 are a special case here. They are either all empty, or they are all non-empty. This is caused by the fact that classes 2, 3 and 4 do not only support addressing during the connection set-up phase, but also connection referencing during the data phase. Classes 0 and 1 do not support any of them.

GLA application:

Sublayer		class	0	1	2	3	4
Segmenting/reassembly	C5		o	o	o	o	o
Sequencing	C4		•	•	•	•	o
Splitting	C3		•	•	•	•	o
Flow control	C2		•	•	o	o	o
Error control	C1		•	o	•	o	o
Connection qualification	B3		•	•	o	o	o
Remote SAP processing	B2		•	•	o	o	o
Local SAP processing	B1		•	•	o	o	o
Protocol version identification	A5		•	•	•	•	•
CC/DT/CL discrimination	A4		o	o	o	o	o
Error detection	A3		•	•	•	•	o
PDU delimiting	A2		•	o	o	o	o
Protocol identification	A1		o	o	o	o	o

Figure 28 - Application of the GLA to the CO Transport Protocol

12. EXTENSION OF THE GLA MODEL FOR SIGNALLING

12.1 General

We will now introduce extensions to the GLA model (Clause 11), and further develop this to demonstrate the different signalling methods described in 6.2.

Figure 29 shows the GLA model, as it has been developed in Clause 11.

Adding the signalling functions can be accomplished in the following way. In the common control functions, a4 provides the separation of CL, CO, and CO-signalling flows. In the individual control function group, c3 provides splitting facilities which facilitate the mapping of a single (N)-connection into a number of (N-1)-connections. Treating separation of signalling and data in the c-group as similar to the splitting of data over different (N-1)-SAPs, we can now introduce an additional splitting function (c6) and an associated resequencing function (c7) into the GLA (see figure 30). The connection management function, connected to a4 at the bottom, is then connected to the c6 splitting function. The signalling primitives provided by the (N)-service user will appear at the (N)-SAPs. From there, they will have to be propagated to the connection management function, where they will result in signalling protocol elements.

Although handled by layer (N-1) as user data, this information flow will likely follow a different path, to a different peer, from the associated data flow(s). This then justifies the treatment similar to the splitting of a data flow.

In addition, the different path and different peer will likely result in different processing and propagation delays from the associated data flows. The c7 function, resequencing, can now provide the resequencing, or resynchronization, of signalling versus data flows.

In our representation we assume that an (N)-SAP that can accommodate n CEPs always contains k CEPs, and n-k PCEPs (potential CEPs), where k denotes the number of established connections that terminate in that SAP. If an (N)-service user initiates an (N)-connect establishment procedure, it transfers signalling primitives over the PCEPs, the result of which can be the promotion of a PCEP to a CEP. The (N)-service user will address itself to that CEP for data transfer and signalling primitive exchange during the lifetime of that (N)-connection.

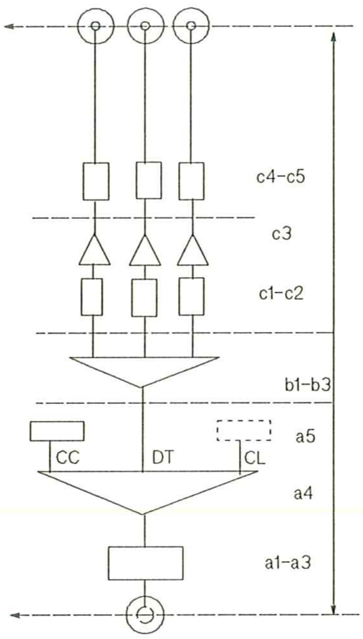


Figure 29
- GLA Model

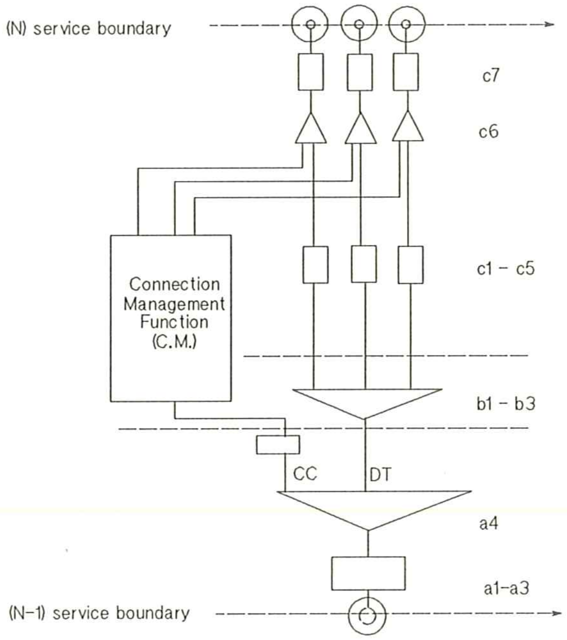
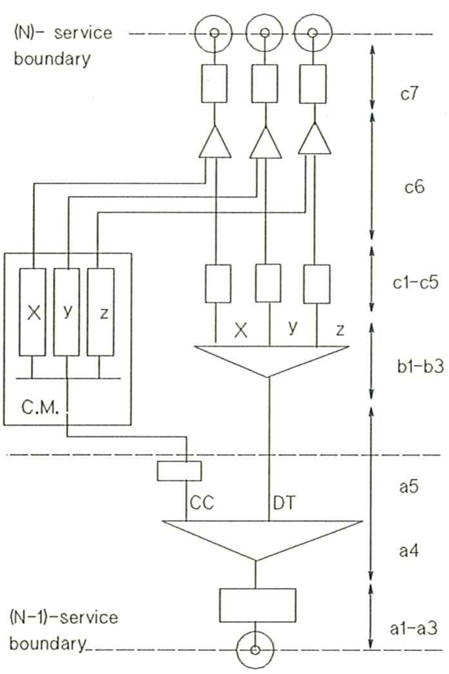


Figure 30
- Extended GLA Model



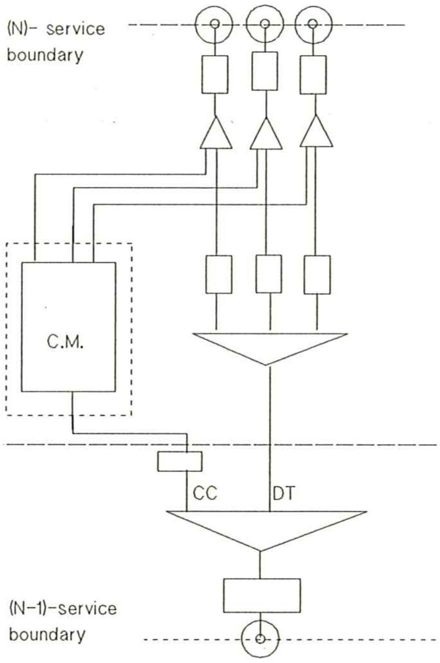


Figure 31
- Example of X.25 application

Figure 32
- Example of X.25 with alternate channel assignment

NOTE 36

There is a large degree of resemblance between a PCEP as here introduced, and a SEP as introduced in Clause 11.2: both are extensions of the CEP concept as defined in the OSI Reference Model. However, in contrast with a SEP, a PCEP is transformable into a CEP.

To illustrate the application of this modified GLA model, we show in figure 31 an example of X.25 with its associated signalling. In the connection management (C.M.) function we find the b1, b2 and b3 functions duplicated; signalling flow and associated data flow use the same reference (logical channel identifier) for fan-in/fan-out. X.25 then becomes a representative of in-band, channel associated signalling, except the restart function, which should be seen in-band, common channel signalling.

Figure 32 shows a possible modified X.25 variant, where all signalling information uses LCI = 0. This X.25 variant now becomes an example of in-band common channel signalling (signalling and data compete for bandwidth on the same (N-1)- SAP, therefore in-band). All signalling is concentrated on LCI = 0, separate from the associated data flows, and is therefore common channel.

To illustrate out-of-band signalling, we now further modify the X.25 variant of figure 32 by introducing a second instance of X.25 PLP, and by using the second instance exclusively to transfer the signalling information of the first (see figure 33). As in figure 32, all signalling information is concentrated in a single channel (either a single virtual circuit with LCI = 0, as is suggested by figure 33, or in multiple virtual circuits), over a different (N-1)-SAP. We recognize here common channel signalling. With the signalling and data flows now on different (N-1)-SAPs, the requirements for out- of-band signalling are also fulfilled when the (N-1)-SAPs (X and Y) do not compete for bandwidth. This is for example the case when layer (N-1) is LAPB, and different physical media are used for the two instances of LAPB.

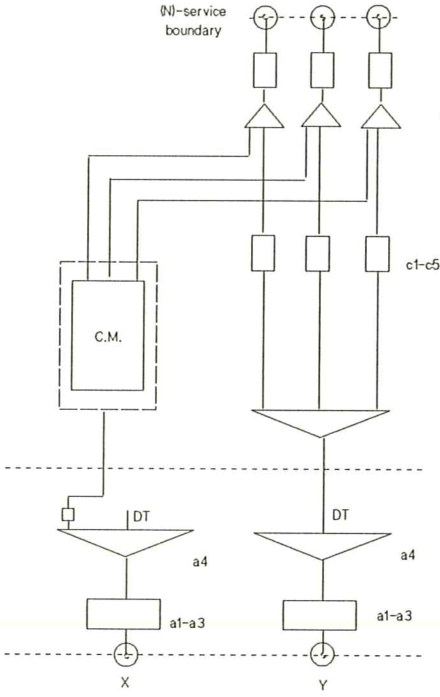


Figure 33 - Example of two instances of X.25 in an out-of-band signalling configuration

It should be noted here that the example of figure 33 can be further developed by introducing a "Lower Layer Management Entity" (LLME) spanning a number of layers. Such an entity can be used to describe all control activities in a layered model which do not follow the rules of layering. The introduction of such an entity is unavoidable in many configurations, since the exchange of signalling information in an (N)-layer may have direct consequences for functions in other layers within the same system. This is of particular interest in the ISDN environment.

12.2 Synchronization Aspects

It is of prime importance that there is a strict sequencing of events (hereafter referred to as "synchronization") at the service boundary between service user and service provider between the data transfer process and the activities performed by the signalling.

The user of a service in the OSI sense will itself respect this synchronization in all activities it performs via the exchange of primitives over the SAPs provided by the service provider. Moreover, the service user will expect strict adherence by the service provider to similar synchronization rules. We may therefore expect a subnetwork service to explicitly state this synchronization in its service definition.

However, it may happen that a subnetwork service provider is not able to guarantee this synchronization. This is in particular the case when a subnetwork access protocol bases itself on out-of-band or common channel signalling methods, and suggests the presence of different "SAPs" for signalling and data flows. The use of these methods usually destroys the temporal relationships between protocol events in the signalling protocol and events in the data flow, as perceived by the ES and by the subnetwork. Refining figure 33, this means that the subnetwork service boundary is not the (N)- service boundary, but instead is a lower service boundary between c6 and c5. See figure 34.

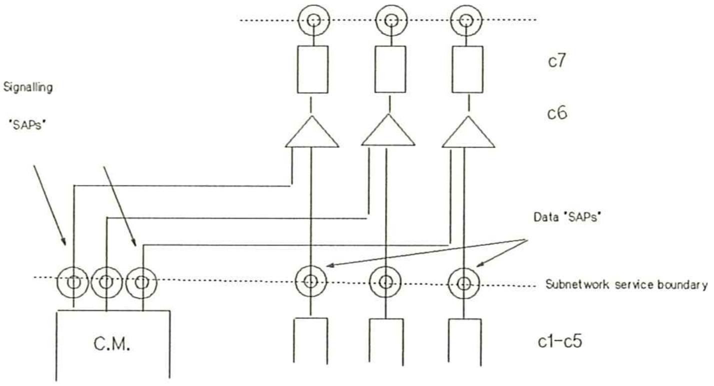


Figure 34 - Subnetwork service definition with independent "SAPs" for signalling and data

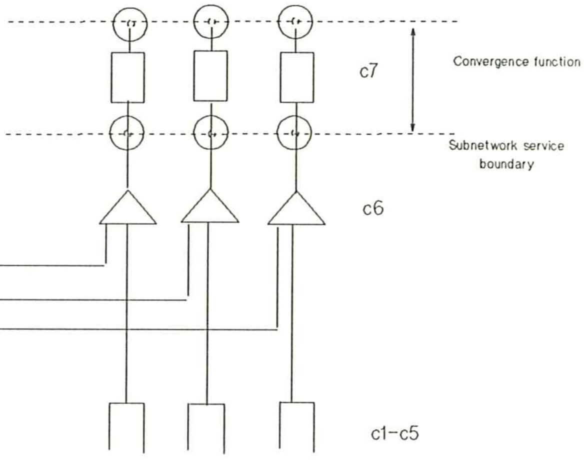


Figure 35 - Preferred representation of subnetwork service with insufficient synchronization

In the modelling technique used here, we prefer to model this as a subnetwork service boundary between c6 and c7, using the knowledge that data transfer and signalling primitives can always be differentiated by their very nature, and stressing the fact that synchronization, to be provided by c7, is missing (see figure 35).

12.3 Drawing Conventions

For reasons of simplicity and clarity, we will use some drawing conventions for SAPs and related issues in the examples given in Clause 13:

i) According to the GLA (Clause 11), a CL SAP is represented as a SAP comprising a data flow across the local SAP and coming from, or going to, a distinct other SAP.

ii) According to 12.1, a CO SAP contains a PCEP for each potential CEP. This facilitates the relating of a signalling primitive to a PCEP before it is transformed into a CEP, and the modelling of the relation of the signalling with the data even during call set-up (when there is not yet an established CEP for that connection). As explained in 12.2, this relation may or may not imply synchronization between signalling and user data.

Table 4 shows the symbols used to represent these different cases.

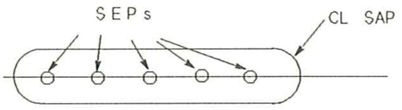
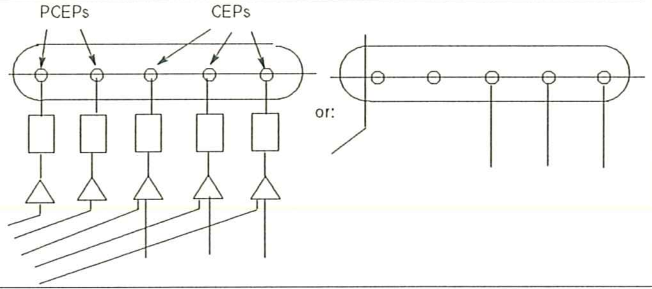
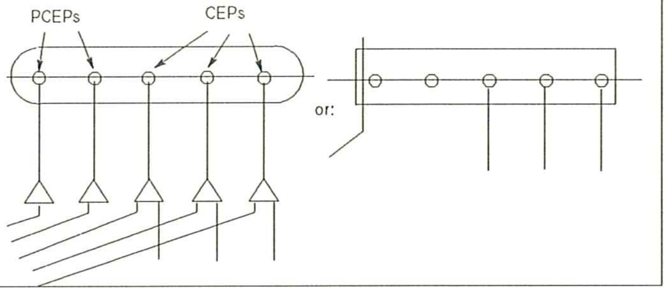
Symbol	Meaning
CL SAP: SAP in a CL service where the identification of the remote SAP is indicated by a SEP within the local SAP.	
Synchronized CO SAP: Two potential CEPs and three established CEPs within one SAP, where the synchronization is guaranteed by the service provider.	
Unsynchronized CO SAP: Two potential CEPs and three established CEPs within one SAP, where the synchronization between signalling and data is not guaranteed by the service provider.	

Table 4 - Symbols used in the adopted drawing conventions

12.4 Extended GLA

The results of the discussions of 12.1, 12.2 and 12.3 are summarized in figures 36, 37 and 38.

Figure 36 shows the GLA, as extended to enable the modelling of signalling, in case the signalling flow and the corresponding user data flow are both sharing the same (N-1)- connection.

Figure 37 shows how the function group (a) in figure 36 has to be modified if the signalling flow and the corresponding data flow are each using their own dedicated (N-1)-connections.

Figure 38 shows how the function-group (a) in figure 36 has to be modified if the signalling flow does not use (directly) the services provided by layer (N-1), but uses any other appropriate means to get the job of transferring signalling information done. The layered principles are (and probably have to be) violated. This is represented (as stated at the end of 12.1) by the use of the so-called "Lower Layer Management Entity" (LLME).

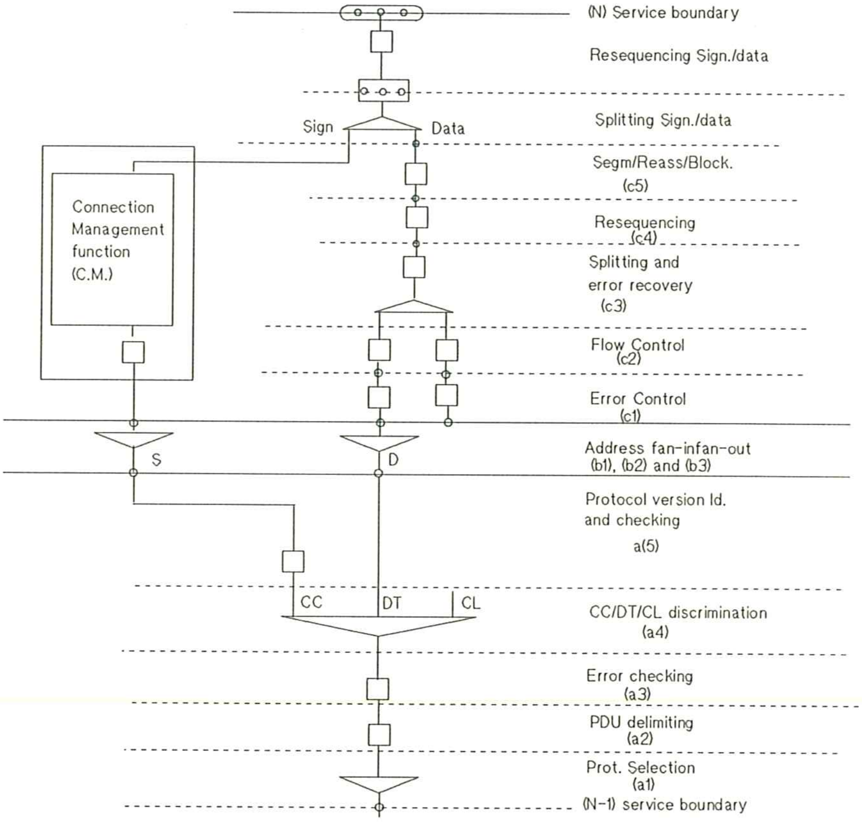


Figure 36 - Extended GLA, in case a common (N-1)-connection is used for signalling and user data

(sublayers c1 to c5 are as in figure 36)

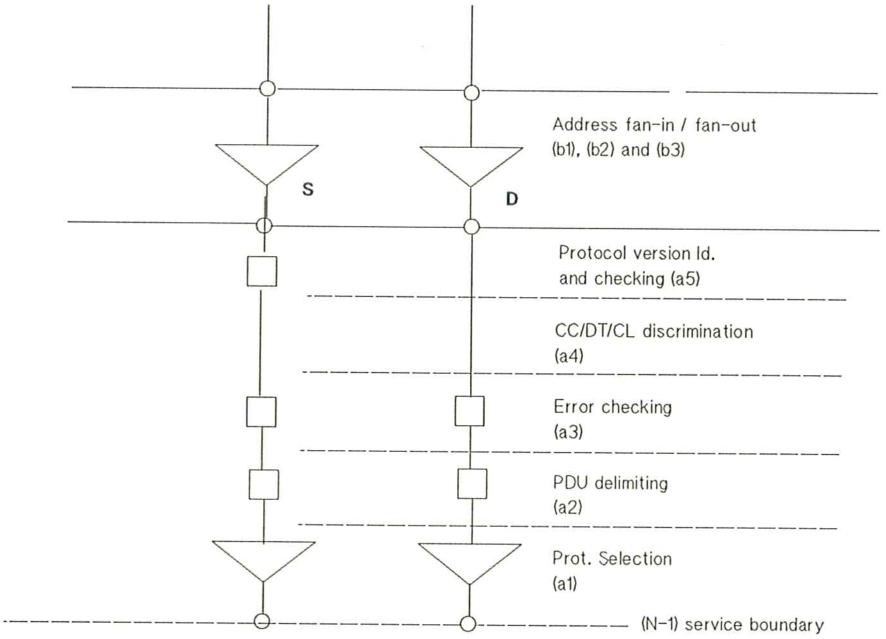


Figure 37 - Extended GLA, in case different (N-1)-connections are used for signalling and user data

(sublayers c1 to c5 are as in figure 36)

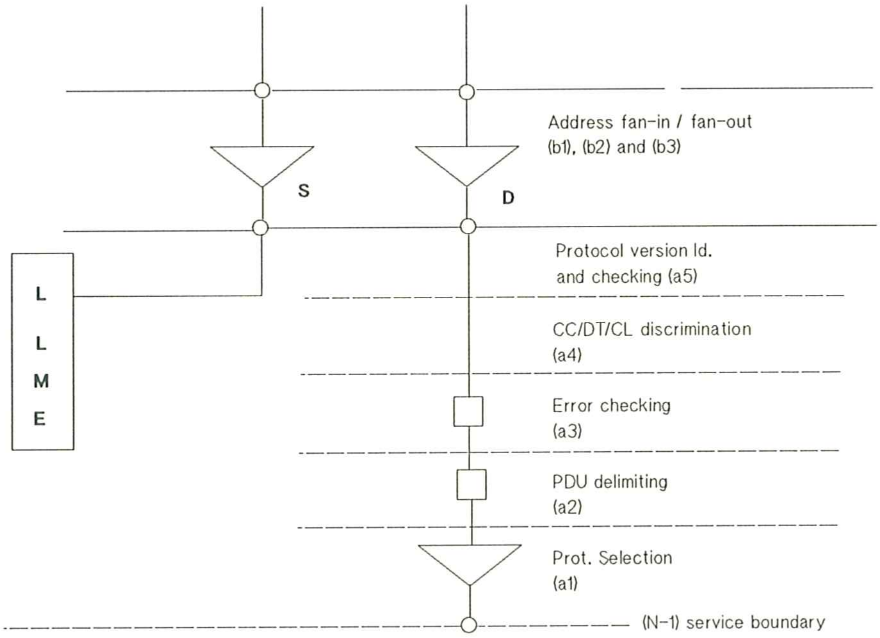


Figure 38 - Extended GLA, in case no (direct) use is made of the (N-1)-service for signalling transfer purposes

SECTION IV

EXAMPLES

13. ANALYSIS OF SOME SPECIFIC SUBNETWORKS

We will now show how the models developed in this Technical Report can be applied in the analysis of some specific subnetworks.

13.1 Methodology Used

Each of the subnetworks under consideration will be described using the following three methods:

i) The Unconstrained Network Service Provider Model (UNSPM):

We will model the subnetwork service as the upper service boundary, below which we will identify the main functional blocks participating in the provision of the service.

In addition, other service boundaries explicitly defined within the subnetwork access protocol will be shown. Where possible, reference will be made here to layers identified in the CNSPM (Clause 10). See also 12.3 for the drawing conventions which are used.

ii) The Generic Layer Architecture (GLA) Model:

The GLA will then be applied to the subnetwork access protocol as a whole, as well as to each explicitly defined component independently. In some cases we add the description of the combination of the subnetwork access protocol with a convergence protocol.

NOTE 38

The tables that represent the result of this analysis use the symbols "o", "x" and ".". The Symbol "o" denotes the presence of the function in agreement with the GLA hierarchy. The symbol "x" denotes the presence of the function, but not in agreement with the GLA hierarchy (hybrid implementation). The symbol "." denotes the absence of the function.

iii) A Subnetwork Service Classification Scheme:

Finally, we will characterize the subnetwork service, using the classification scheme introduced below.

13.2 Subnetwork Service Classification Scheme

The objective of our classification scheme is to provide a tool for the comparison of specific subnetworks on the basis of simplified service characteristics. Recognizing the fact that different subnetworks serve different purposes, the classification should only be used to compare different subnetwork services, with regard to a target service only, and not as a measure of "quality".

We will apply the classification scheme without asking ourselves the question as to where the subnetwork service boundary should precisely be positioned in the OSI Reference Model.

The classification itself is based on a two-dimensional scheme, assigning different identifiers to the aspects:

i) The reach or scope of the subnetwork service:

- physical characteristics that limit the number of ESs that could be connected;
- logical characteristics that limit the number of ESs that could be connected;
- the physical/geographical area that could be covered;
- the capability to supply information to a subnetwork or IS.

ii) The properties of the mechanisms for the transfer of user data:

We will now introduce the following definition for a Global Subnetwork Service:

A subnetwork service is called global if:

- a very large geographical area with a radius of, say, 20000 kms could be covered, and
- a very large number of ESs, say 10 power 10, could be interconnected.

We then assign the following identifiers to (i):

A	for a subnetwork that we call non-global,
B	for a subnetwork that we call global, but restricted to the use of SNPA addressing,
C	for a subnetwork that we call global, uses SNPA addressing and is capable of transferring NSAP addresses and other global parameters transparently (passive operation),
D	for a subnetwork that we call global, and operates on NSAP addresses and other global parameters (active operation),

and we assign the following identifiers to (ii):

P	for a CBO (Continuous Bitstream Oriented) data service,
Q	for a DBO (Delimited Bitstring oriented) data service,

NOTE 38

We will assume that the SDU contains an integral number of octets.

Rx	for a DBO data service with flow control,
Sx	for a DBO data service with flow control and unlimited SDU size, where

x = 0 denotes: no Reset, no Expedited,
x = 1 denotes: no Reset, with Expedited,
x = 2 denotes: with Reset, no Expedited,
x = 3 denotes: with Reset, with Expedited.

Applying this classification scheme to specific subnetworks will give two results:

- one for the Potential Subnetwork Service, notation: PSS = ((i), (ii)),
- one for the Actual Subnetwork Service, notation: ASS = ((i), (ii)).

Examples:

- an X.25 (1984) subnetwork would be classified as PSS = (D,S3), ASS = (C,S3),
- a CLNP subnetwork would be classified as PSS = ASS = (D,Q).

13.3 X.25 (1984) and X.25 (1980)

The UNSPM is given in figure 39.

The X.25 SNAcP consists of X.21 or X.21bis, LAPB and X.25 layer 3. Only X.25 layer 3 supports multiplexing: multiple virtual circuits support a single SAP, unless subaddressing is used to subdivide into multiple SAPs. The same connection referencing mechanism, Logical Channel Identifiers (LCIs), is used for Data and Call Control packets.

The GLA model and subnetwork service classification are given in Table 5.

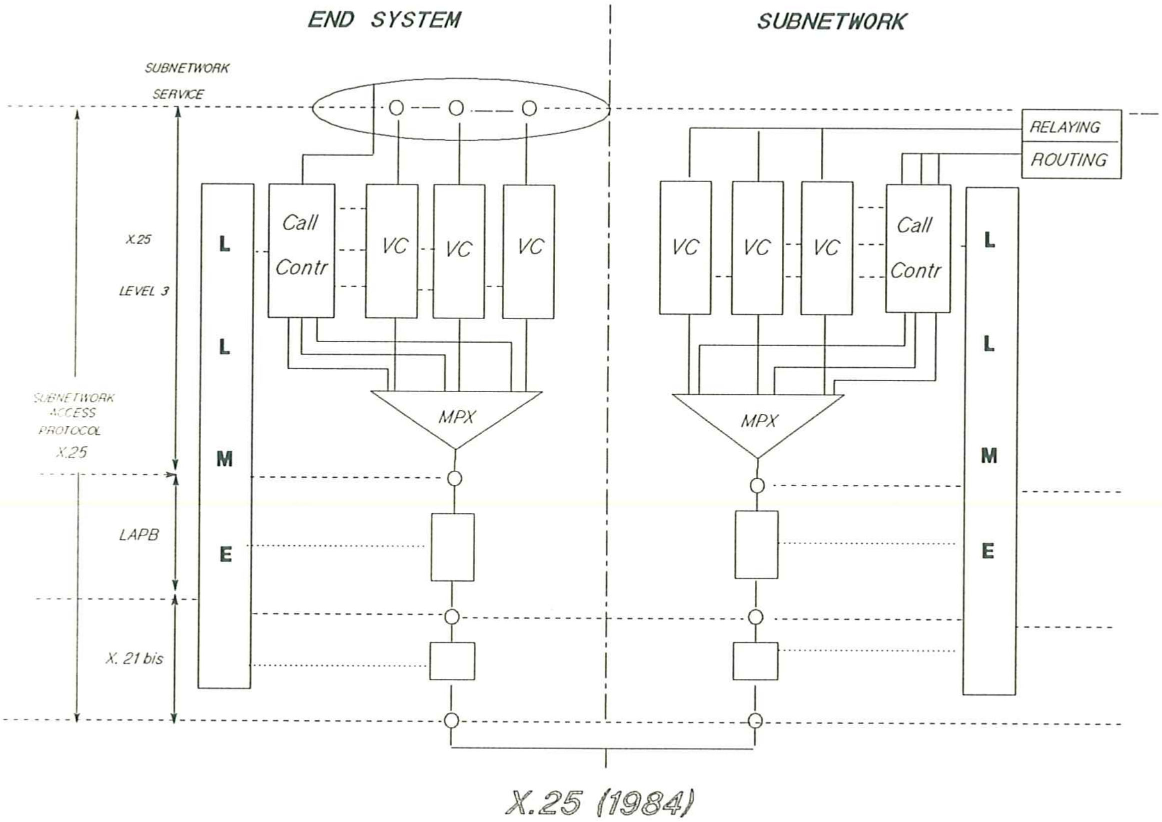
X.25 layer 3 depends for error control on LAPB, as is shown in the GLA analysis. When X.25 layer 3 and LAPB are seen as a single protocol layer, the LAPB error control becomes the common error control function of the combined protocol.

The data service belonging to X.25 (1984) has all the attributes of U, the subnetwork service is global, and supports transfer of NSAP addresses, although potentially NSAP addresses could even be operated on. The classification of X.25 (1984) is therefore PSS = (D,S3), ASS = (C,S3).

X.25 (1980) differs in two respects:

- The data service is classified as S2, as 32 octets expedited is not supported;
- The subnetwork service is global but lacks any support for the transfer of NSAP addresses.

The resulting classification is PSS = ASS = (B,S2).



Note

If subaddressing is used, then the single SAP is split into a number of SAPs either at or above the subnetwork service boundary, dependent on whether the subnetwork operates on these subaddresses actively or possibly.

Figure 39 - X.25 (1984)

GLA application:

Sublayer		LAPB	Layer	Combined
Segmenting/reassembly	C5 3	.	o	o
Sequencing	C4 3	.	.	.
Splitting	C3 3	o (a)	.	x(a)
Flow control	C2 3	o	o	o
Error control	C1 3	o	.	x
Connection qualification	B3 3	.	o	o
Remote SAP processing	B2 3	.	o	o
Local SAP processing	B1 3	.	o (b)	o(b)
Protocol version identification	A5 3	.	.	.
CC/DT/CL discrimination	A4 3	o	o	o
Error detection	A3 3	o	.	o
PDU delimiting	A2 3	o	.	o
Protocol identification	A1 3	.	o	.(c)

Notes

(a) If the multi-link procedure is used.
(b) If subaddressing is used.
(c) Hidden in combined protocol.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,S3) (d)
Actual Intervention Level	(C,S3) (d)

Note

(d) X.25 (1980) would be classified as (B,S2) for both potential and actual intervention level.

Table 5 - X.25 (1984)

13.4 X.21 and X.22

The UNSPM is given in figure 40. As can be seen from the figure, X.22 is a point-to-point multiplexing of several X.21 circuits over a single physical circuit.

The X.21 procedures should be interpreted as an example of in-band signalling. Call Control related PDUs follow the same logical and physical path as other PDUs.

The SAPs are of the normal, synchronized type.

The GLA model and subnetwork service classification are given in Table 6.

The GLA analysis is rather simple, as only a destination address and (implied) source address are supported (when multiple instances of X.21 support the same SAP, which is for example the case for a hunt group, then the physical channel could be seen as an implied connection qualifier).

Classification is PSS = ASS = (B,P), as a global CBO service is provided without NSAP support.

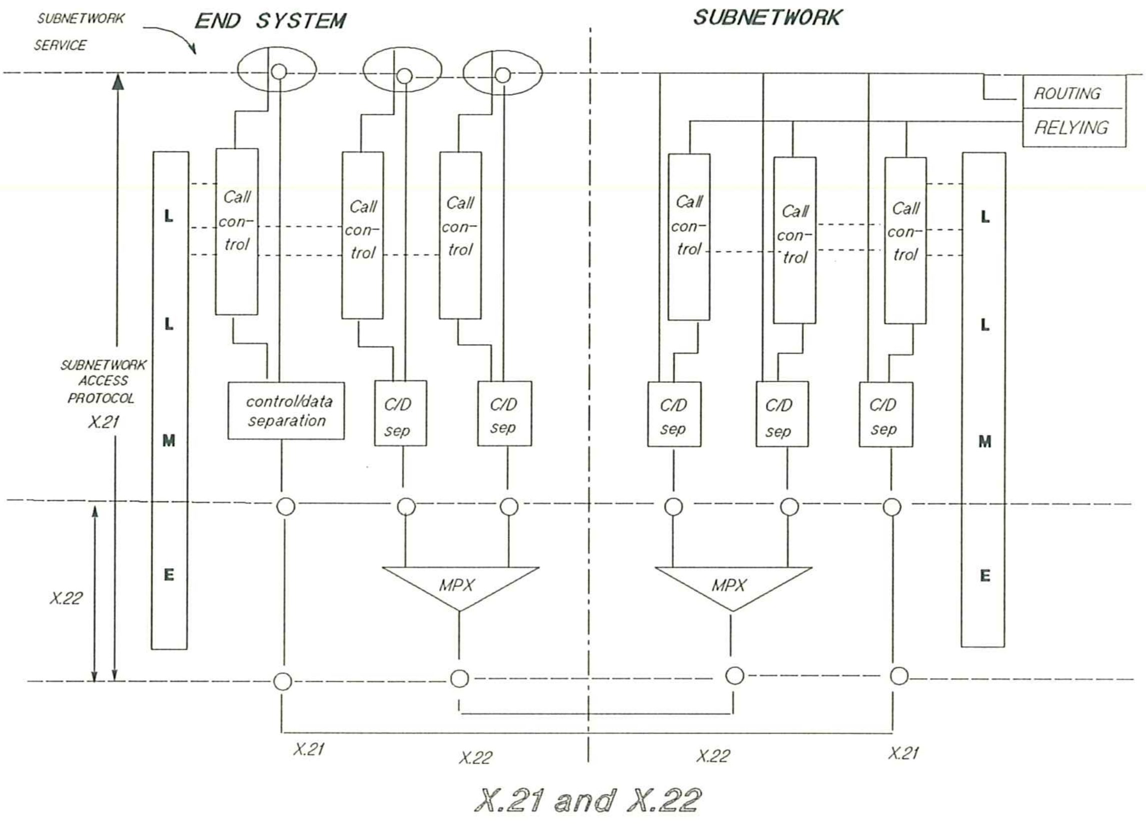


Figure 40 - X.21 and X.22

GLA application:

Sublayer		X.21
Segmenting/reassembly	C5	•
Sequencing	C4	•
Splitting	C3	•
Flow control	C2	•
Error control	C1	•
Connection qualification	B3	•
Remote SAP processing	B2	o
Local SAP processing	B1	•
Protocol version identification	A5	•
CC/DT/CL discrimination	A4	o
Error detection	A3	•
PDU delimiting	A2	•
Protocol identification	A1	•

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(B,P) (a)
Actual Intervention Level	(B,P) (a)

Note

(a) With extensions to the signalling, the classification could be raised to (C,P).

Table 6 - X.21 and X.22

13.5 8802.x LAN and Bridged LAN

The UNSPM is given in figure 41.

In our modelling we assume that the MAC source address is always operated on within the MAC layer. The SEP identifier which could be a parameter derived from this operation is in this case always the MAC service address.

A MAC bridge performs a relaying and routing operation on the MAC destination address. At the same time, the MAC source address may be evaluated for the purpose of updating routing tables.

The GLA model and subnetwork service classification are given in Table 7.

The connectionless MAC service has only a source and destination address, and evidently no connection identifier. The LLC convergence protocol provides for an additional source and destination address.

Standardized LSAP values are used to provide higher layer protocol identification. When a standardized value is used it will be repeated in source and destination LSAP fields, hereby loosing sublayer independence between b1 and b2. When non-standardized values are used the values in the two fields may be different.

If the LLC and MAC are used in combination, then the MAC and LLC address fields still correspond with sublayers b1 and b2, but again, sublayer independence is lost. This is indicated in Table 5 by "x".

LLC type II can be seen as a CO convergence protocol, where type I can be seen as a CL convergence protocol.

The classification for an 8802.x type LAN is PSS = ASS = (A,Q); the physical properties of the LAN limit the physical coverage as well as the number of end systems that can be supported, while the data service is of the DBO type.

Bridges take away the physical limitations, and thereby raise the classification to PSS = ASS = (B,Q).

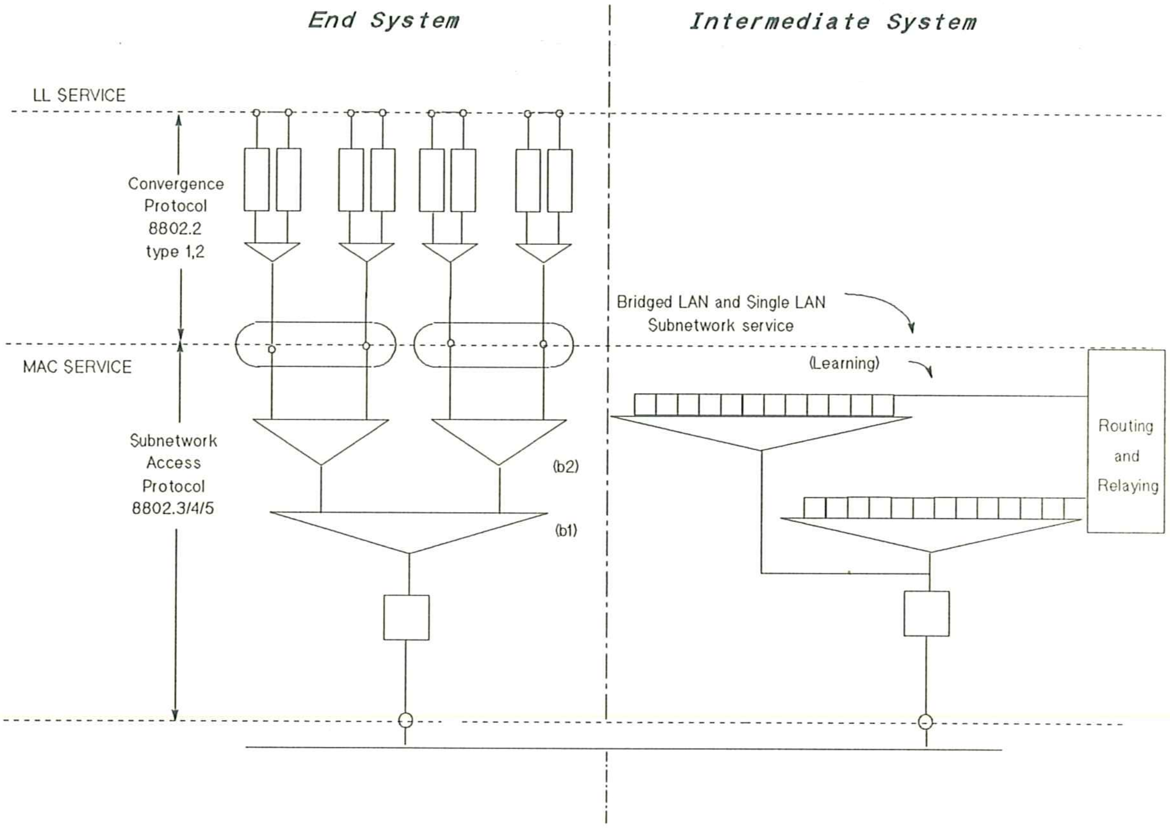


Figure 41 - 8802.x Single LAN and Bridged LAN

GLA application:

Sublayer		MAC	LLC1 (a)	LLC2 (a)	LLC1	LLC2
Segmenting/reassembly	C5	•	•	•	•	•
Sequencing	C4	•	•	•	•	•
Splitting	C3	•	•	•	•	•
Flow control	C2	•	•	o	•	o
Error control	C1	•	•	o	•	o
Connection qualification	B3	•	•	•	•	•
Remote SAP processing	B2	o	o (b)	o	x	x
Local SAP processing	B1	o	o (b)	o	x	x
Protocol version identification	A5	•	•	•	•	•
CC/DT/CL discrimination	A4	•	•	o	•	o
Error detection	A3	o	•	•	o	o
PDU delimiting	A2	o	•	•	o	o
Protocol identification	A1	•	•	•	•	•

Notes

(a) LLC1 and LLC2 are convergence protocols used over the MAC service.

(b) B1 and B2 as currently defined always carry an equal value.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	Single LAN (A,Q)	Bridged LAN (B,Q)
Actual Intervention Level	(A,Q)	(B,Q)

Table 7 - 8802.x Single LAN and Bridged LAN

13.6 PSN with Multiple Services

A PSN is a certain class of private network, defined by the following terms: "A subnetwork with digital transmission capabilities bounded by S-interfaces, providing circuit-, frame- and/or packet-switched services between S-interfaces by means of the common channel signalling procedures defined in Standard ECMA-106 and in CCITT Recommendation Q.931." Figure 42 illustrates the model appropriate to a PSN offering the option at the subnetwork service boundary of a variety of services below the OSI NS boundary. The service provided for any instance of communication is a matter of negotiation between the subnetwork service provider entity in the end system and the subnetwork service provider entity in the subnetwork, across the points of attachment to the subnetwork. In clauses 13.6.2 to 13.6.4 each of the important services is modelled and described in more detail.

13.6.1 General Considerations

13.6.1.1 Modelling conventions

Our modelling conventions for the PSN intend to emphasize some architecturally relevant points. For example, we model all signalling to be handled by the Lower Layer Management Entity (LLME): that part of the system management responsible for the lower layers. The LLME then uses Q.931 as a management communication protocol, to communicate with its peer(s). Also, the unconstrained assignment of B-channels to SAPs is explicitly modelled with a multiplexer/demultiplexer, under control of the LLME. Furthermore, the subnetwork SAPs are modelled here as unsynchronized SAPs: the different service definitions for the PSN do not explicitly state the synchronization required by the higher layer user.

On the other hand, we simplify some of the PSN specifics, here considered of less importance. For example, the collision detection mechanism available on the D-channel of the basic access interface is not explicitly shown. Moreover, D-channel use for applications other than signalling are generally not shown: in figure 42 the possible frame layer and packet layer applications of the D-channel are omitted. As a further simplification, no multiplexing is shown in the packet layer in this figure; this should not be interpreted as a limitation inherent to PSNs.

13.6.1.2 SAPs in Multiple Service Environment

It should be noted that the choice of a subnetwork service may be seen as being offered via a single subnetwork SAP, corresponding in OSI terminology with a SubNetwork Point of Attachment (SNPA), as is shown in figure 42. A consequence of this interpretation is that parameters identifying the service have to be passed over the subnet SAP. Alternatively, the different subnetwork services may be one-to-one coupled with different SAPs. This requires the subnetwork to actively operate on the service identifiers for the purpose of routing and relaying to the proper SAP.

13.6.1.3 Basic and Supplementary Services

Each of the ISDN and PSN Services itself is described as a family of services:

- A Basic Service, and
- a set of Supplementary Services, incremental modifications of the Basic Service, subject to additional subscription and registration procedures.

The concept of Supplementary Services is further discussed in clause 16.

13.6.1.4 Service modification

ISDNs, and therefore PSNs, intend to provide for modification of the service during the life-time of an established connection ("in call service modification"), although the appropriate signalling procedures for this function have not yet been described. Modification of the service during the lifetime of an established connection means that during the lifetime of an established connection the actual subnetwork service is modified. This may be the result of invocation of a supplementary service, or an explicit service modification request. This of course excludes the case where during the lifetime of an established connection the actual subnetwork service is a constant, but different higher layer functions or protocols are used in the end systems (or TEs) at different moments in time (for example over a voice-quality circuit switched connection, first voice then data is transmitted).

The following observations can be made on service modification:

- Modification of service can be modelled as chaining connection establishment requests, where each request implies the release of the previous connection.
- Modifying the service rather than establishing a new connection seems only justified if the time required to process the service modification is considerably shorter than the time to execute and process the combination of disconnect and connect request.
- In more complex network topologies, the routing within the subnetwork may be a function of the requested subnetwork service; if this is the case, then modification of the service may require rerouting of the established connection, unless the subnetwork had chosen an appropriate routing based on an advance knowledge of the services to be used.
- Modification of the service should not automatically be interpreted as modifying the service provided over a certain SAP or CEP. On the contrary, if one wishes to have SAPs or PCEPs (potential CEPs) uniquely identifying a service, then modifying services should indeed be seen as establishing a new connection, using a different SAP or CEP, with the re-use of some of the resources involved in a previous connection (for example a certain B-channel).

13.6.1.5 Convergence Protocols and Coordinating Entity

In case a subnetwork service does not explicitly define the synchronization of signalling and data primitives handed to the higher layer, as is the case in PSNs, then the resynchronisation function (C7 in GLA terms) should be provided by a subnetwork convergence function, sometimes referred to as "coordinating entity" or "glue".

In case a convergence protocol is intended to be used to enhance the data transfer attributes of the subnetwork service, then two possibilities exist to integrate this convergence protocol:

- The convergence protocol is above the resynchronization function (on top of the "coordinating entity"); in this case the convergence protocol will be required to handle Network Layer type primitives (for example N_Connect Request) at both its upper and lower boundaries.
- The convergence protocol is run directly over the data part of the subnetwork service, under the resynchronization function (under the "coordinating entity"); in this case the protocol may implement reduced signalling type primitives, as the resynchronization function now provides an isolation from Network Layer type primitives (notably the addressing parameters may be absent).

NOTE 39

In both cases however, one may find that the convergence protocol entity differs significantly from a protocol entity that provides a similar enhancement of the data transfer attributes in a different environment, e.g. HDLC based protocol entities applied to run "over" or "under" the resynchronization function differ from a traditional HDLC based protocol entity.

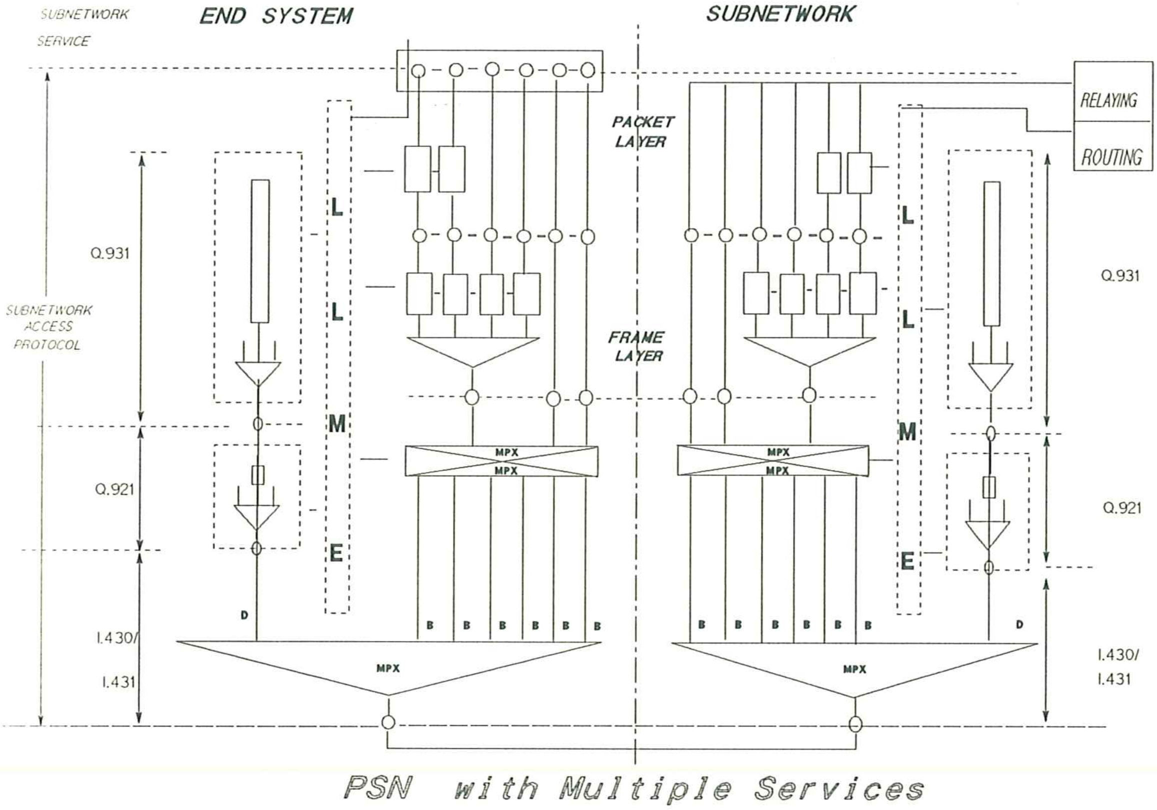


Figure 42 - PSN with Multiple Services

13.6.2 PSN with Circuit Switching Service

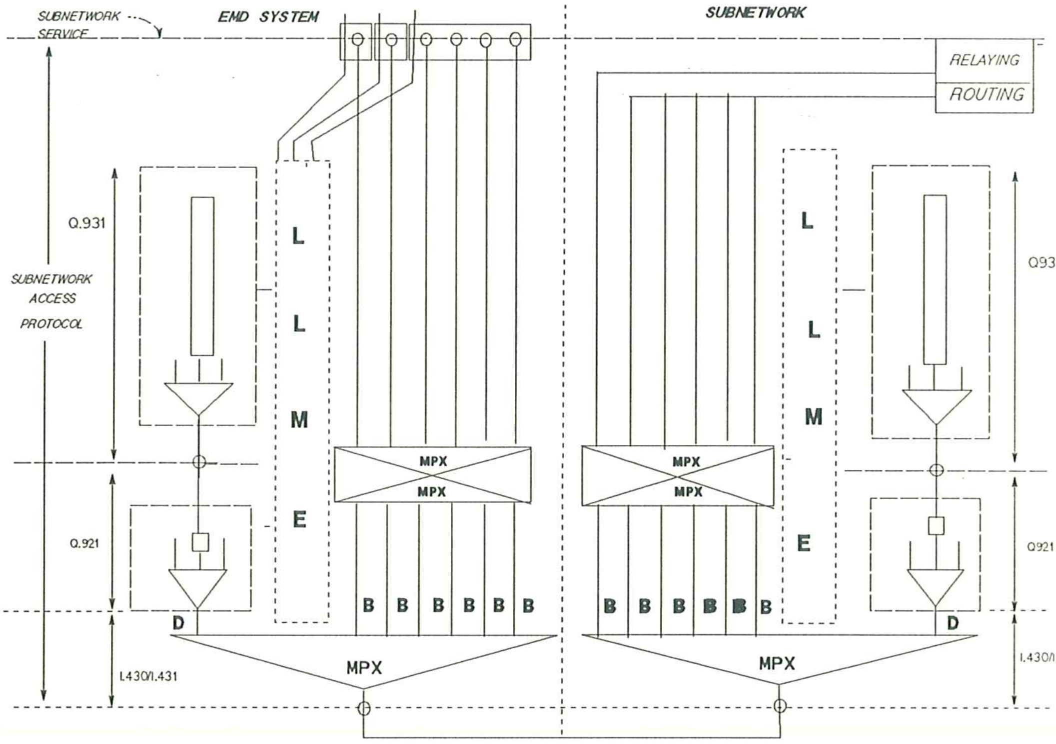
The UNSPM is given in figure 43.

Whilst in the case of circuit switching as modelled here the data circuits are identified by their channel number over a certain S reference point, the accompanying signalling streams are identified by a separate connection referencing mechanism, the Connection Reference (CR).

The unsynchronized SAP, in combination with the absence of flow control mechanisms, may result in loss of data during the connection establishment process.

The GLA model and subnetwork service classification are given in Table 8.

The circuit switching PSN has a data service of the CBO type which is bit- and octet-synchronized and is global. Q.931 capabilities anticipated are transparent NSAP transfer, and potential processing. The classification is therefore PSS = (D,P), ASS = (C,P).



PSN with Circuit Switching Service

Synchronization at the Subnetwork Service boundary is not included in the service description.

Figure 43 - PSN with Circuit Switching Service

GLA application:

Sublayer		PSN/CS
Segmenting/reassembly	C5	•
Sequencing	C4	•
Splitting	C3	•
Flow control	C2	•
Error control	C1	•
Connection qualification	B3	o
Remote SAP processing	B2	o
Local SAP processing	B1	o
Protocol version identification	A5	•
CC/DT/CL discrimination	A4	•
Error detection	A3	•
PDU delimiting	A2	•
Protocol identification	A1	•

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,P)
Actual Intervention Level	(C,P)

Table 8 - PSN with Circuit Switching Service

13.6.3 PSN with Frame Switching Service

The UNSPM is given in figure 44.

The analysis of the circuit switching PSN holds, but a multiplexing mechanism in the LAPD-like frame layer is added, with a connection referencing mechanism using the LAPD address field: Data Link Channel Identifier (DLCI) (a data stream is identified by a DLCI on a certain channel number over a certain S reference point; the associated signalling stream is identified by a CR over a certain S reference point).

The GLA model and subnetwork service classification are given in Table 9, assuming a multi-frame acknowledge service.

The GLA analysis shows that the frame switching service would in fact need a segmentation/reassembly function to bring it closer to the CONS. This can be accomplished by using for example X.25 layer 3 as a convergence protocol.

The classification for the multiframe acknowledged service, anticipating Q.931 NSAP support, is PSS = (D,R2), ASS = (C,R2), assuming no segmentation/reassembly in the frame layer protocol. In case a segmentation/reassembly function is included in the frame layer protocol, but is not supported in the subnetwork, the classification would be PSS = (D,S2), ASS = (C,R2).

The actual subnetwork service with flow control implemented in the subnetwork is ASS = (C,R2), ASS = (C,Q) if flow control is not supported.

A subnetwork only supporting error detection and routing and relaying of frames (referred to as "frame relay" or "LAPD core" is shown in Table 10. The classification of this service, that can be seen as a CO MAC service equivalent, is PSS = (D,R2), but ASS = (C,Q).

The absence of flow control may result in an increased frame loss, unless other mechanisms to control frame loss due to congestion are provided.

In Tables 11 and 12 a frame switching PSN is shown with X.25 layer 3 "DTP" (without Call Control) and CLNP respectively as convergence protocols.

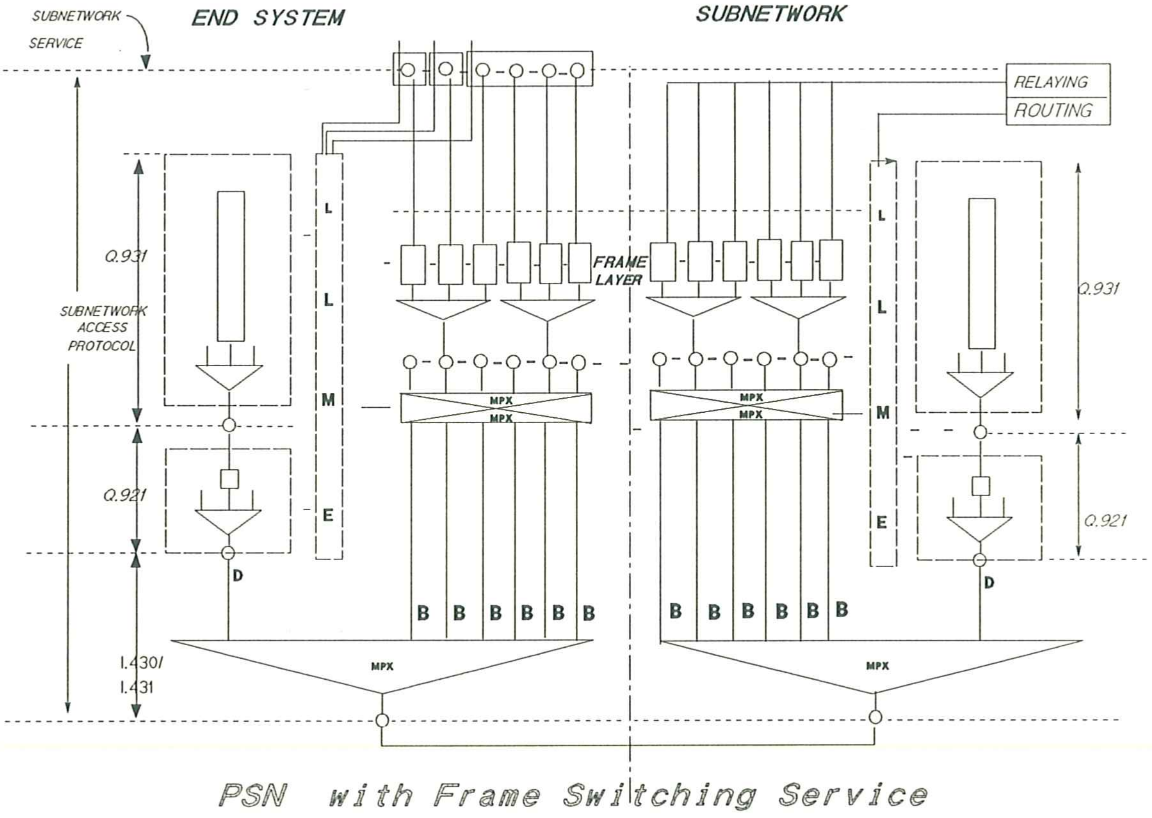


Figure 44 - PSN with Frame Switching Service

GLA application:

Sublayer		PSN/FS
Segmenting/reassembly	C5	.
Sequencing	C4	.
Splitting	C3	.
Flow control	C2	o
Error control	C1	o
Connection qualification	B3	o
Remote SAP processing	B2	o
Local SAP processing	B1	o
Protocol version identification	A5	.
CC/DT/CL discrimination	A4	o
Error detection	A3	o
PDU delimiting	A2	o
Protocol identification	A1	.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,R2)
Actual Intervention Level	(C,R2)

Table 9 - PSN with Frame Switching Service (LAPD multiframe)

GLA application:

Sublayer		PSN/FR
Segmenting/reassembly	C5	.
Sequencing	C4	.
Splitting	C3	.
Flow control	C2	.
Error control	C1	.
Connection qualification	B3	o
Remote SAP processing	B2	o
Local SAP processing	B1	o
Protocol version identification	A5	.
CC/DT/CL discrimination	A4	o
Error detection	A3	o
PDU delimiting	A2	o
Protocol identification	A1	.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,R2)
Actual Intervention Level	(C,Q)

Table 10 - PSN with Frame Relaying Service

GLA application:

Sublayer		PSN/FS	X.25 Layer 3 (a)	combined
Segmenting/reassembly	C5	.	o	o
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	o	o	o
Error control	C1	o	.	x
Connection qualification	B3	o	o	o
Remote SAP processing	B2	o	o	o
Local SAP processing	B1	o	o	o
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	o	.	o
Error detection	A3	o	.	o
PDU delimiting	A2	o	.	o
Protocol identification	A1	.	o	.(b)

Notes

(a) Convergence protocol.

(b) Hidden in combined protocol.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,R2) (c)
Actual Intervention Level	(C,R2) (c)

Note

(c) Convergence protocol does not affect classification of the subnetwork.

Table 11 - PSN with Frame Switching Service and X.25 Layer 3 as convergence protocol

GLA application:

Sublayer		PSN/FS	CLNP (a)	combined
Segmenting/reassembly	C5	.	o (b)	o(b)
Sequencing	C4	.	.	.
Splitting	C3	.	o	o
Flow control	C2	o	.	o
Error control	C1	o	.	o
Connection qualification	B3	o	.	o
Remote SAP processing	B2	o	o	o
Local SAP processing	B1	o	o	o
Protocol version identification	A5	.	o	o
CC/DT/CL discrimination	A4	o	.	o
Error detection	A3	o	.	o
PDU delimiting	A2	o	.	o
Protocol identification	A1	.	o	.(c)

Notes

(a) Convergence protocol.

(b) Error control and resequencing provided by optional PDU segmentation/reassembly facility.

(c) Hidden in combined protocol.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,R2) (d)
Actual Intervention Level	(C,R2) (d)

Note

(d) Convergence protocol does not affect classification of the subnetwork.

Table 12 - PSN with Frame Switching Service and CLNP as convergence protocol

13.6.4 PSN with Packet Switching Service

In the case where packet switching service is provided by the PSN, several scenarios are possible.

13.6.4.1 Based on X.31 scenarios

CCITT Recommendation X.31 covers the case of the packet service offered by ISDN-like subnetworks.

13.6.4.1.1 X.25 Packet Switching Services according to X.31 case B

In this case the packet handler capabilities are present in the subnetwork and may be accessed either by D- or B- channels.

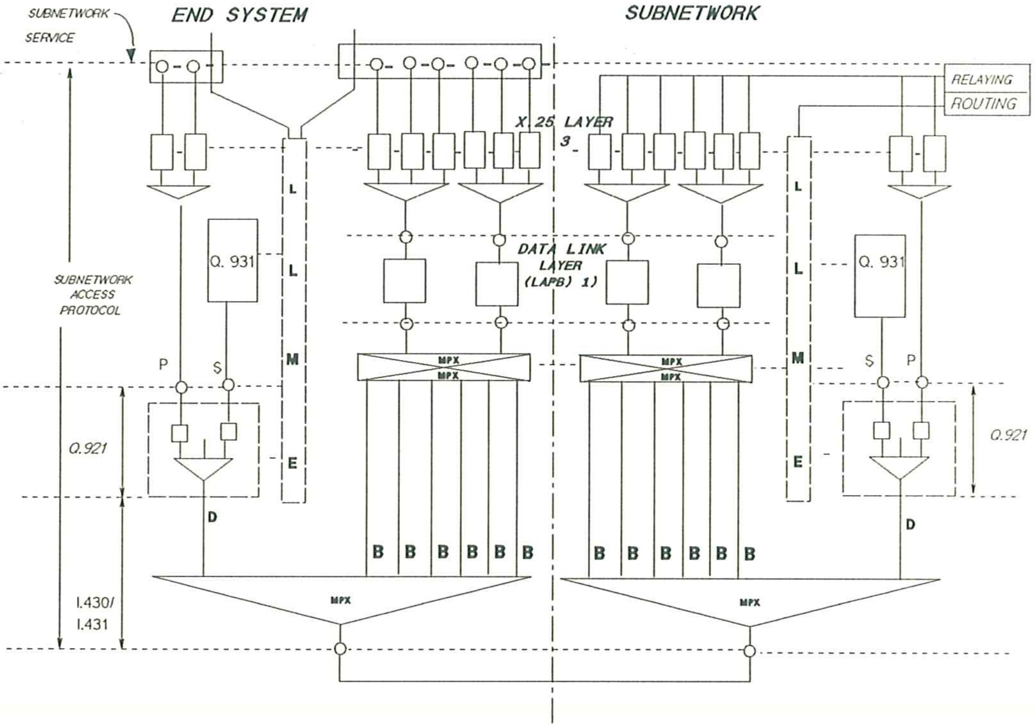
The UNSPM is given in figure 45.

It has to be noted that the Data Link Layer protocol in the case of D-channel is LAPD and in the case of B-channel may be LAPB or LAPD (with multiplexing capability not used).

The GLA model and subnetwork service classification (for the case of B-channel access based on LAPB) is given in Table 13.

13.6.4.1.2 X.25 DCE Access mode according to X.31 case A

This scenario, also described in X.31, allows an end system to access an X.25 DCE by use of a circuit switching subnetwork service as described in 13.6.2. This scenario should be seen as a concatenation of different subnetworks with different subnetwork services, and is therefore outside the scope of this clause. It is referred to here for completeness only.



Instead of LAPB, LAPD may be used, in which case multiplexing is available in this layer.

Figure 45 - PSN with Packet Switching Service ("Maximum" Scenario)

GLA application:

Sublayer		PSN/ LAPB	X.25 Layer 3	Combined
Segmenting/reassembly	C5	.	o	o
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	o	o	o
Error control	C1	o	.	x
Connection qualification	B3	.	o	o
Remote SAP processing	B2	.	o	o
Local SAP processing	B1	.	o	o
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	o	o	o
Error detection	A3	o	.	o
PDU delimiting	A2	o	.	o
Protocol identification	A1	.	o	.(a)

Note

(a) Hidden in combined protocol.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,S3)
Actual Intervention Level	(C,S3)

Table 13 - X.25 Packet Switching Service ("maximum" scenario)

13.6.4.2 PSN with Packet Switching Service based on Frame Switching

13.6.4.2.1 With one level of multiplexing (at layer 2)

The UNSPM is given in figure 46.

Assuming that no additional multiplexing in X.25 layer 3 is supported, the analysis of the frame switching PSN can be applied. If neither multiplexing, nor flow control, nor expedited data of X.25 layer 3 are supported by the subnetwork, then the modelling becomes ambiguous: no difference can be made between the packet switching PSN and the enhanced frame switching PSN as described in 13.6.3.

The GLA model and subnetwork service classification are given in Table 14.

With a data service of type S3, and anticipated support for NSAPs in Q.931, the classification is PSS = (D,S3). For the actual subnetwork service the classification is:

- ASS = (C,S3) if only NSAP operation lacks, or
- ASS = (C,S2), or (C,R2), or even (C,Q), if the PSN chooses not to support expedited, segmentation/reassembly, or flow control respectively.

13.6.4.2.2 With two levels of multiplexing

In this case, the layer 3 protocol is X.25 Permanent Virtual Circuit PLP, including multiplexing. It does not provide advantages over 13.6.4.2.1 in terms of service provided, and the models are identical to those of 13.6.4.2.1, with the exception of the multiplexing capability in layer 3.

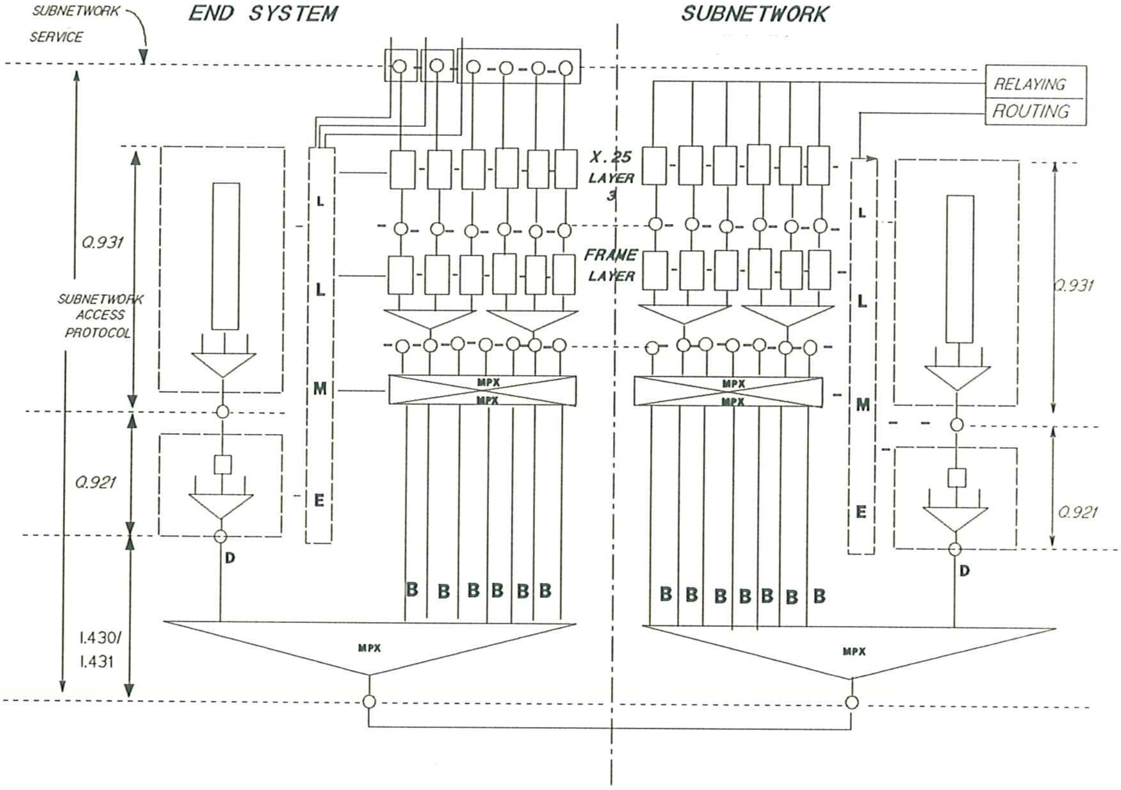


Figure 46 - PSN with Packet Switching Service based on Frame Switching

GLA application:

Sublayer		Frame Layer	Layer 3	combined
Segmenting/reassembly	C5	.	o	o
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	o	o	o
Error control	C1	o	.	x
Connection qualification	B3	o	o	o
Remote SAP processing	B2	o	o (a)	o
Local SAP processing	B1	o	o	o
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	o	.	o
Error detection	A3	o	.	o
PDU delimiting	A2	o	.	o
Protocol identification	A1	.	o	.(b)

Notes

(a) Not used.

(b) Hidden in combined protocol.

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on

PCBO

Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,S3)
Actual Intervention Level	(C,S3) or (C,R2) (c)

Note

(c) In the case of an actual intervention level equivalent to or below frame switching, the modelling becomes not unambiguous (see PSN with frame switching service and convergence protocols).

Table 14 - PSN with Packet Switching Service based on Frame Switching

13.7 B-ISDN with ATM Service

The UNSPM is given in figure 47.

The ATM layer, a layer with a high speed DBO service with fixed frame (cell) size, forms the common support for synchronous and asynchronous CO services, signalling, and possibly CL services. The ATM layer is transmission system independent.

Figure 47 shows the UNSPM of the ATM subnetwork service, assuming a common-channel signalling configuration.

The ATM subnetwork service is a DBO CO service, therefore includes the signalling aspects. Each cell contains an address field in its header (consisting of VPI and VCI), that can be used for connection referencing for switched virtual circuits. Signalling may use one or more switched virtual circuits, then controls the establishment and release of other switched virtual circuits for the transfer of user data. According to the definition in clause 6.2.4, this signalling should be seen as in-band. Depending on the association between signalling flow and data flow (yet to be defined), the signalling could be channel associated, or common-channel as shown in the figure.

The GLA model and subnetwork service classification are given in Table 15.

The GLA analysis shows that the ATM service would in fact need segmentation/reassembly and flow control functions and possibly an error control function to bring it closer to the CONS. This can be accomplished by using an appropriate ATM Adaptation Layer (AAL).

The classification for the unacknowledged ATM service, anticipating support by a subnetwork access signalling protocol like Q.931 including NSAP support, is PSS = (D,Q), ASS = (C,Q).

The absence of flow control may result in an increased cell loss, unless other mechanisms to control cell loss due to congestion are provided. On the other hand, no existing flow control mechanism is seen as suitable for and compatible with the high data rate of the ATM layer.

There is a strong similarity between B-ISDN with ATM service, and the PSN with frame relaying service of clause 13.6.3, especially when the latter is considered in a minimum functionality configuration.

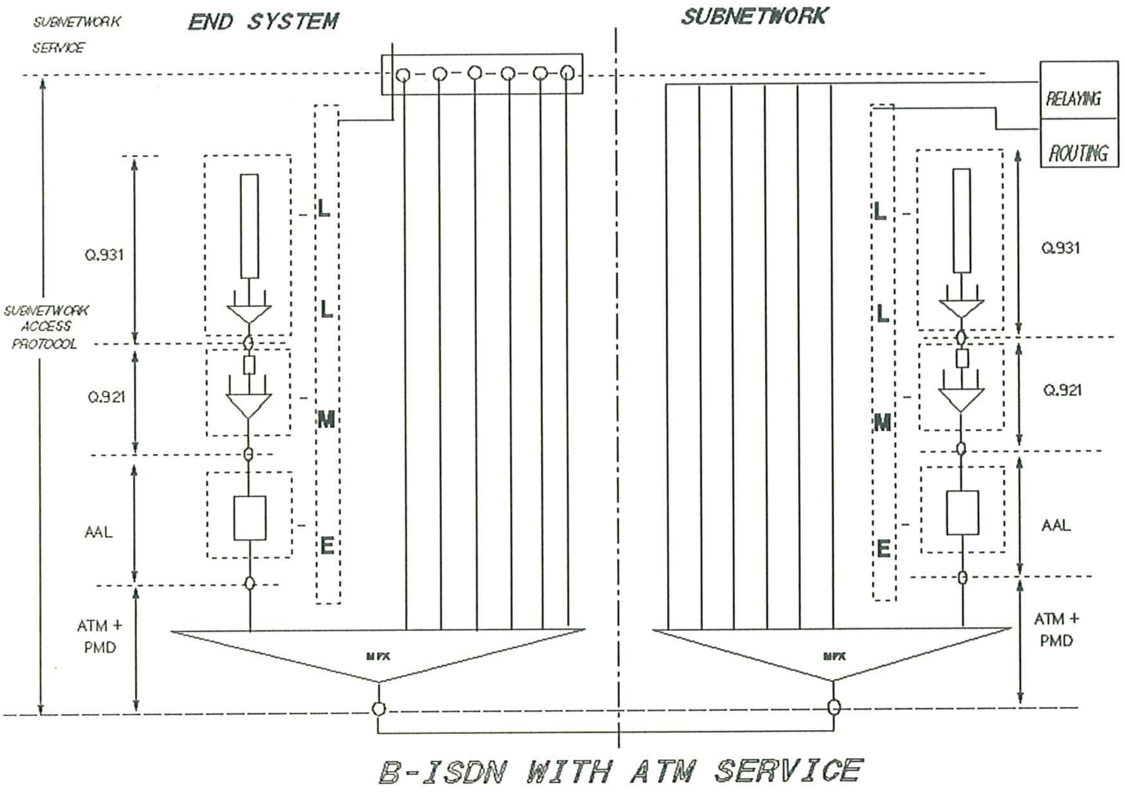


Figure 47 - B-ISDN with ATM Service

GLA application:

Sublayer		B-ISDN/ATM
Segmenting/reassembly	C5	•
Sequencing	C4	•
Splitting	C3	•
Flow control	C2	•
Error control	C1	•
Connection qualification	B3	o
Remote SAP processing	B2	o
Local SAP processing	B1	o
Protocol version identification	A5	•
CC/DT/CL discrimination	A4	o
Error detection	A3	o (a)
PDU delimiting	A2	o
Protocol identification	A1	•

Note

(a) error detection, and possibly error correction, provided on the PCI only

Subnet classification:

A	non-global
B	global, without NSAP
C	global, NSAP transferred
D	global, with NSAP operated on
P	CBO
Q	DBO
Rx	DBO with flow control
Sx	Rx with SDU of any finite length

Potential Intervention Level	(D,Q)
Actual Intervention Level	(C,Q)

Table 15 - B-ISDN with ATM Service

14. APPLICATION OF MLAM TO EXISTING STANDARDS

14.1 Network Layer Addressing Standard

The OSI NL address is defined in ISO 8348/AD2.

Its structure is as follows:

NL address = Initial Domain Part / Domain Specific Part

IDP DSP

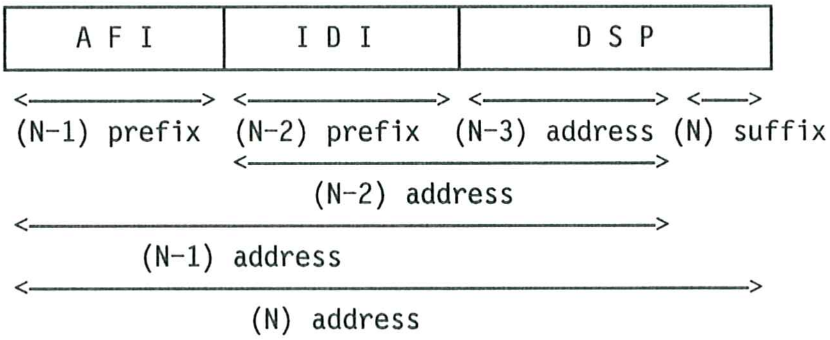
The IDP consists of two parts: the Authority and Format Identifier (AFI), and the Initial Domain Identifier (IDI). This leads to the following structure for the NL address:

NL address = AFI / IDI / DSP

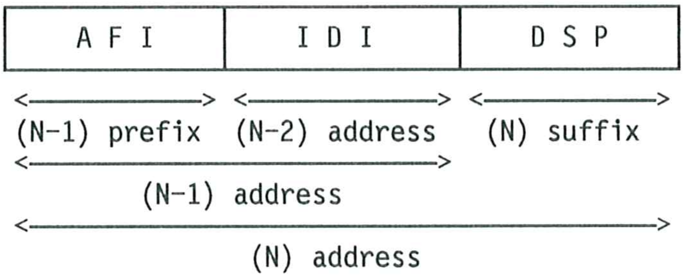
In terms of MLAM this can be read as follows:

- The NL address is associated with layer (N) in the model.
- In the general case, and assuming a selector component in the DSP, the following structure applies. The (N)-suffix corresponds to the DSP selector component; the (N-3)-address corresponds to the upper part of the DSP, while (N-1)-prefix and (N-2)-prefix correspond to AFI and IDI respectively.

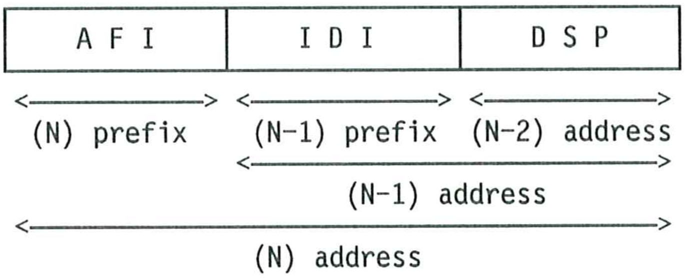
  Note: in the case of the DCC and IDC formats, the leftmost part of the upper part of the DSP contains sub-authority identification information. Depending on the view taken, this component may be seen as belonging to the (N-2)-prefix, as an (N-3)-prefix, or as part of the (N-3) address; the latter is shown in the figure.



- Two special cases, each leading to a simplified mapping, are of some interest:
  - For the CCITT derived NL addresses, and assuming that the CCITT address directly identifies the End system, the three parts AFI, IDI, and DSP are mapped into layers (N-1), (N-2), and (N) respectively:



- For the DCC and IDC formats, and assuming the absence of a selector component in the DSP, the three parts AFI, IDI, and DSP are mapped into layers (N), (N-1), and (N-2) respectively:



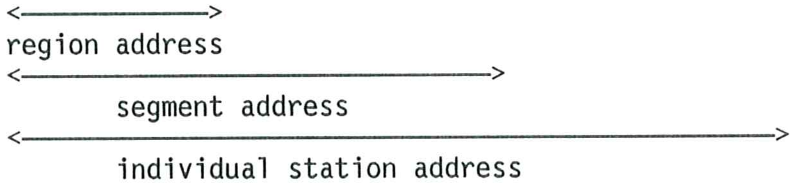
14.2 Application to IEEE MAC Address Standard

14.2.1 Application of MLAM

The Medium Access Control (MAC) address is defined in ISO 8802-x protocols. As an example the case of ISO 8802-4 is taken into consideration. Two different formats are defined for the MAC address: 16 bit address , and 48 bit address. For the 48 bit format a structure is proposed, which is as follows:

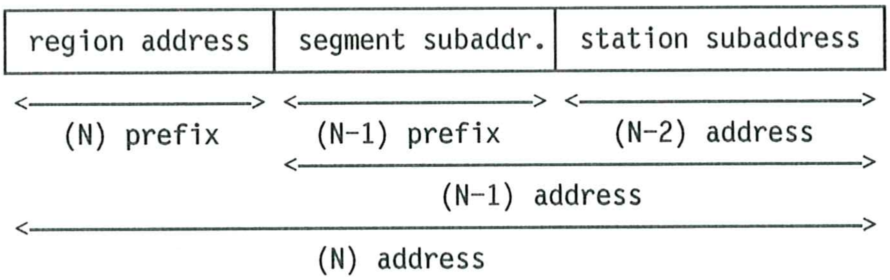
48 bits address:

`MAC address = I/G bit / region addr./ segment subaddr./ station subaddr.`



The mapping into the MLAM is as follows:

- The MAC address is associated with layer (N) in the model (where N can be any arbitrary number).
- The three parts region address, segment subaddress and station subaddress are related to the (N)-demesne, (N-1)-demesne and to the (N-2)-demesne respectively.
- This results into the following:



NOTE 40

In this model, the LLC SAP could be seen as an (N+1) suffix.

- the protocol that carries the MAC address is placed in the (N-2) layer. The (N-1) and (N) prefixes are seen as being transferred transparently by the (N-2) layer protocol.

14.2.2 Mapping into the OSI BRM

MLAM layers (N), (N-1) and (N-2) are all mapped into the MAC layer, often seen as a sublayer of the data link layer.

14.3 Application to E.164 Numbering Plan

14.3.1 Application of MLAM

The ISDN numbering plan is defined in CCITT Rec. E.164. In general the ISDN address is structured into two parts: the ISDN number, and the ISDN Sub-Address (SA). In case the SA is absent, the ISDN address is the same as the ISDN number. In the following we will consider the two cases, without SA and with SA, separately.

We will start with the case in which the ISDN number constitutes the ISDN address (SA absent). In this case the structure of the ISDN address is as follows:

E.164 address - International prefix / National significant number

CC NSN

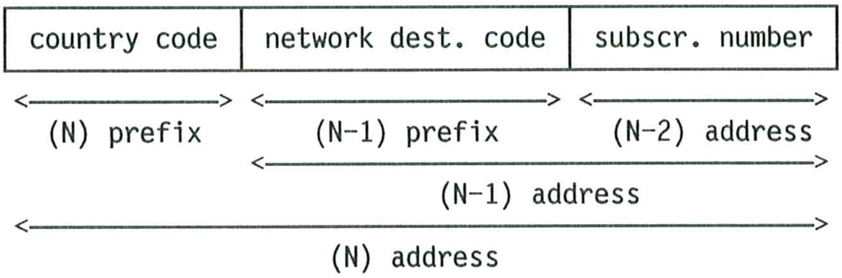
The international prefix (country code: CC) is used to select the destination country, while the national significant number is used to select the destination subscriber. In selecting the destination subscriber, sometimes it may be necessary to select a destination network first. This leads to the following structure:

E.164 address - CC / Destination network / Subscriber number

NDC SN

In terms of MLAM this can be read as follows:

- The E.164 address is associated with layer (N) in the model.
- The three parts CC, DNC, and SN are related to the (N)-demesne, an (N-1)-demesne, and an (N-2)-demesne respectively.
- This results into the following:

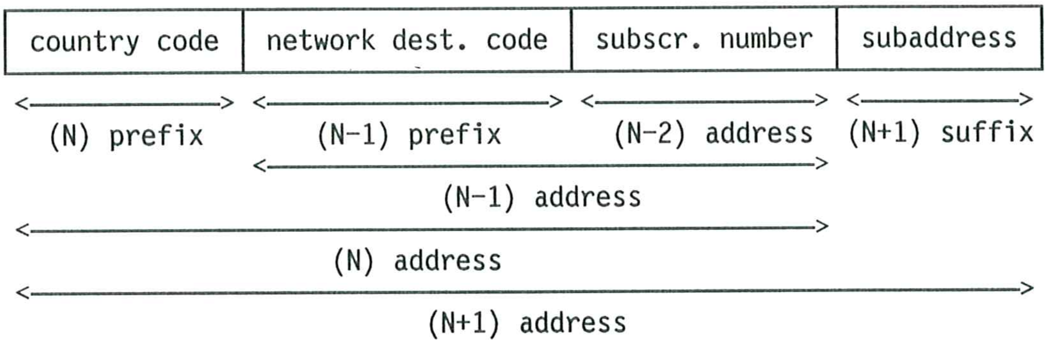


- The protocol that carries the ISDN address is placed in the (N-2) layer. The (N-1) and (N) prefixes are seen as being transferred transparently by the (N-2) layer protocol.

  Rec. E.164 defines the Sub-Address field as not being part of the ISDN number, but offering additional addressing capabilities and constituting an integral part of the ISDN addressing capabilities.

When Sub-Address is used and when this sub-address only supports a fan-out within the end system, then the mapping in the MLAM is as follows:

- The E.164 address (E.164 number + SA) is associated with (N + 1) layer in the model.
- The SA is related to the (N + 1)-demesne, while the E.164 number is related to the (N)-demesne.
- This results into the following:



- The protocol that carries the ISDN address is placed in the (N-2) layer. The (N-1) and (N) prefixes, and the (N + 1) suffix are seen as being transferred transparently by the (N-2) layer protocol.

  Note

  The ISDN access signalling protocol Q.931 allows for the possible use of other numbering schemes besides E.164, via the use of a numbering plan identifier. The latter could be seen as an (N + 1) prefix.

14.3.2 Mapping into the OSI BRM

MLAM layers (N), (N-1), (N-2), and (N + 1) if present, are all mapped into the OSI Network Layer.

14.4 Application to E.163 Numbering Plan

14.4.1 Application of MLAM

The PSTN numbering plan is defined in CCITT Recommendation E.163. Its structure is:

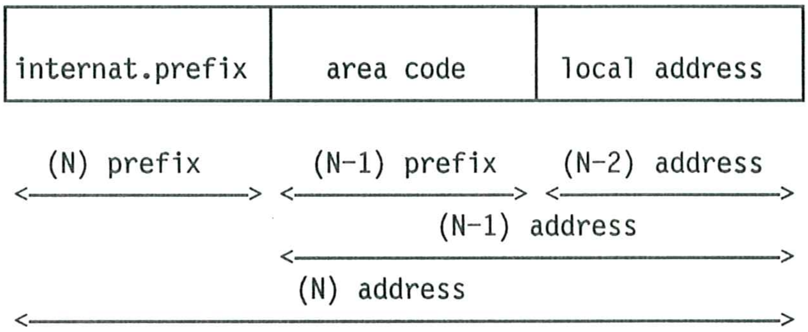
E.163 address = internat. prefix / national address

Most countries structure their national address on basis of area codes. The resulting structure is:

E.163 address = internat. prefix / area code / local address

Mapping into the MLAM is as follows:

- the E.163 address is associated with layer (N) in the model (where N can be any arbitrary number)
- the three parts: internat. prefix, area code, and local address, are related to the (N)-demesne, an (N-1)-demesne, and an (N-2)-demesne
- this results into the following:



- the protocol that carries the PSTN addresses is placed in the (N-2) layer. The (N-1) and (N) prefix information is then seen as being transferred transparently by the (N-2) layer protocol.

14.4.2 Mapping into the OSI BRM

MLAM layers (N), (N-1) and (N-2) are all mapped into the OSI Network Layer, since the Link Layer is completely transparent for all three MLAM layers.

14.5 Application to X.121 Numbering Plan

14.5.1 Application of MLAM

The PSDN numbering plan is defined in CCITT Recommendation X.121. The mapping is complicated by the fact that X.121 addresses are allocated to both Circuit Switched (C.S.) and packed switched (P.S.) compatible End-systems, which usually are not capable to inter-operate. However, it is also true that the address space allocated to C.S. terminals is disjoint from the address space allocated to P.S. terminals. Therefore, if an Interworking Unit is introduced to facilitate communication between both terminal types (using some appropriate convergence protocol over the C.S. network), then the addressing requirements are not affected.

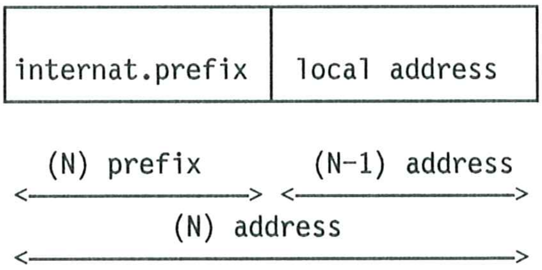
We can distinguish two Demesnes :

- the X.121 P.S. type (N) Demesne
- the X.121 C.S. type (N) Demesne.

X.21 terminals that can interwork with X.25 terminals via an IWU belong to both Demesnes. Equally, X.25 terminals that can interwork with X.21 terminals via an IWU belong to both Demesnes.

The structure of an X.121 address = internat. prefix/national address (=DNIC)

Assuming the national address space as flat, we get :



The protocol that carries the X.121 address is placed in layer (N-1). The layer (N) addressing information (the (N) prefix) is carried transparently by that protocol.

14.5.2 Mapping into the OSI BRM

MLAM layers (N) and (N-1) are both mapped into the OSI Network layer for the same reasons as mentioned under 6.5.5.2.

SECTION V

NON - DATA EXTENSIONS

15. NON - DATA EXTENSIONS

15.1 Non-Data Typing and Classification

15.1.1 Introduction

Information can only be transferred over some geographical distance if it is first transformed into a "signal". A signal can be seen as the result of attachment of information to a "carrier". This attachment process can be seen as a form of "coding".

Suppose first, that the signal as sent by the transmitter arrives at the receiver without any modification. It is then clear, that the information will only be preserved if the process of attachment of the information to the carrier at the sending side (coding) is precisely the reverse of the process of extraction of the information from the carrier at the receiver side (decoding).

If, however, this assumption is not valid, and the signal is intercepted by some intermediate equipment (from now on indicated as "telecommunications network"), then it is not always true that the signal reproduced at the exit point of that network is a precise copy of the signal received at the entry point of that network.

In fact, most telecommunication networks do not reproduce signals at the exit point which are exact copies of the signals received at the entry point. The only reason that Telecommunication networks are still capable to provide an acceptable service is, that they are aware of the way in which these signals represent information. To be more precise : telecommunication networks are at the entry point aware of the coding-rule used by the source-user, and are aware of the decoding-rule used by the destination-user. This knowledge facilitates (or may even necessitate) the network to deliver at the exit point signals which differ from the signals offered at the entry point, since the network guarantees that the information carried by these signals (rather than the signal itself) is preserved.

15.1.2 Examples

a) Video information is offered in a three dimensional form, and the colours are offered as a waveform with a certain frequency distribution. The information is however reproduced at the receiver in a two dimensional form, and the colours are either completely suppressed (black-white TV) or reproduced with a significantly different frequency distribution (people that are partially colour-blind are usually aware of this modification and see the differences). Moreover, the pictures are sampled with a rate of 25 pictures per second.

b) Audio information is offered to the transmitting telephone as a signal in the frequency range 0-20000 Hz. It is reproduced at the receiving side as a waveform in the frequency range 300-3400 Hz, while the waveform as time function is even totally distorted, since small frequency shifts may occur (up to 3 Hz) and frequencies in the corners of the frequency range suffer from significantly longer delay than the frequencies in the middle of the range (group-delay distortion).

15.1.3 Characterisation of Information

Information can be characterised by the way it is (potentially) processed. If information needs to be transferred from source to destination, then it is needed to explicitly identify the set of variables which are of importance and the set of possible values of each variable. A telecommunication network can then be seen as a network that is expected to transfer (periodically or only once) the current values of these variables transparently.

It is convenient to specify these variables on basis of the "type" concept developed in the environment of programming languages. It should, however, be noted that, in contrast with the environment of programming languages (i.e. the "processing" environment), a telecommunications network is expected to preserve the values of the variables, rather than to change them.

15.1.4 Information Classes

Hereafter follows a list of information classes, each specified in terms of a set of variables, the values of which are expected to be preserved by a telecommunications service provider. The approach taken is based on the use of digital techniques for information transfer.

Two groups are identified:

- Group 1: the data group This group is characterized by the fact that the information is essentially of discrete nature at presentation and/or application level.
- Group 2: the non data group This group is characterized by the fact that the information is essentially of analog nature at presentation and/or application level.

Group 1: the data group

Subgroup 1a: digital data without any graphic semantics

This subgroup encompasses all forms of discrete information where the representation aspect in terms of graphic objects is of no relevance. This is usually the case where this data, after being transferred, is directly used as input for processing, rather than printed on paper or presented on other visual means. Three classes are identified under this subgroup.

Class 1 : DBO binary transfer

General description : sequential transfer of SDUs
SDU type : array of bits
Bit type : boolean (values : true and false)
Throughput attribute : SDUs/sec, average SDU size
QoS parameters : bit error probability
SDU mis-sequence probability
SDU loss probability

Class 2 : CBO binary transfer

General description : transfer of a continuous bitstream
Bit type : boolean
Throughput attribute : bits/s
QoS parameters : bit error probability

Class 3 : other non-graphic digital data

This class encompasses all forms of discrete information of non-binary nature where the representation aspect in terms of graphic objects is irrelevant.

Subgroup 1b: digital data with graphic semantics

This subgroup encompasses all forms of discrete information where the representation aspect in terms of graphic objects is relevant. This is usually the case where this data, after being transferred, is printed on paper or is presented by other visual means. This subgroup encompasses only one class: the graphics class. This class includes text.

Class 4 : graphics

General description : transfer of synthetic images, described as graphic objects with associated attributes
Object type : image description with associated attributes
Throughput attribute : objects per second
QoS parameters : 1) error probability
2) precision of the reproduction of the specified image

NOTE 41

The transfer of text is seen as a special case of graphics: the objects consist of a set of printable and some non-printable characters. Transfer of documents (e.g. ODA) is seen as an other special case of graphics, as far as these documents contain graphic information, including text. The picture parts of these documents may belong to group 2, the non-data group.

Group 2: the non-data group

Three classes are identified,

- the image class,
- the video class, and
- the audio class

All classes have in common that the description is based on the use of some form of sampling. The resolution of an image and the bandwidth of audio information is directly related to the sampling density. Therefore, resolution and bandwidth are not treated as QoS parameters, but as integral parts of the type-definition.

Class 5 : Image

General description : transfer of a single picture
Picture type : two dimensional arrays [1..Xmax, 1..Ymax] of pixels (Xmax and Ymax to be determined by required resolution)
Pixel type : record of : intensity, X-colour, Y-colour
Intensity type : scalar; range : 0.. Max Intensity
X-colour type : scalar; range : 0.. Max X-colour
Y-colour type : scalar; range : 0.. Max Y-colour
Throughput attribute : time needed to transfer the picture
QoS parameters : 1) signal to noise ratio of Intensity, X-colour, Y-colour
2) Inter-pixel and quantization distortion

Class 6 : Video

General description : transfer of moving pictures
Picture type : two dimensional arrays [1..Xmax, 1..Ymax] of pixels (Xmax and Ymax to be determined by required resolution)
Pixel type : record of : intensity, X-colour, Y-colour
Intensity type : scalar; range : 0.. Max Intensity
X-colour type : scalar; range : 0.. Max X-colour

Y-colour type : scalar; range : 0.. Max Y-colour
Throughput attribute : picture refreshment rate
QoS parameters : 1) signal to noise ratio of Intensity, X-colour, Y-colour
2) Inter-pixel and quantization distortion

Class 7 : Audio

General description : transfer of an audio waveform
Waveform type : a stream of samples, resulting from sampling the original audio waveform
Sample type : scalar, range -Amax ... +Amax
Throughput attribute : samples per second (directly related to the bandwidth of the audio waveform)
QoS parameters : 1) signal to noise ratio
2) inter-sample and quantization distortion

NOTE 42

1) it might be argued that the audio waveform, rather than its sampled derivative, should be chosen as basis for typing. However, this approach is not taken here, since it is preferred to keep alignment with the image and video typing approach above

2) stereophonic audio is seen as an enhancement of this type

3) voice is seen as a special case of audio: the distortion QoS parameter has a much higher allowed value. This higher distortion is the result of speech bandwidth and amplitude reduction techniques, allowing the use of channels with reduced bandwidth for the encoded signal. The characteristics of this distortion are chosen in such a way that the semantics of the speech information, rather than the waveform that carries this information, is expected to be preserved.

15.1.5 Application to Person to Person communication

It is now necessary for telecommunication services, and useful for data services, to analyze what role these services play in the process of information transfer between a person and an other person. We look at the following situation, to develop a representation of the processes involved.

A person A wants to transfer the message/information Z to another person B.

If A and B are physically in the same location, A could express himself in the form X or Y, each a representation of one or more aspects of Z, chosen in such a way that the expected perception Z* of X or Y by B is as much as possible identical to the message Z. For example, X could be a verbal explanation, Y could be a written explanation including some graphic representations. Both X and Y are a function of, but not identical to Z. Figure 48 illustrates this. In formula form:

X = Repr__A(Z) = f(Z)

Z* = Perc__B(X) = Perc__B(Repr__A(Z))

It should be noted here that A and B are handicapped by their limitations in both expression and perception, but are assisted by the possible use of additional agreements and protocols that exists between them.

Figure 50 then expands this representation with the functions necessary to convey the telecommunication representation to the remote location:

- a coding/decoding function
- a transmission functions

NOTE 43

It is assumed that the coding/decoding and transmission functions are operating ideally, i.e. X' *is transferred unmodified.*

The necessary transmission functions may have requirements that differ from those of data services:

1) a strict upper boundary may apply to both maximum transit delay and the variation of the actual transit delay
2) the timing requirements of 1) may be incompatible with the use of error correction techniques (other than discard and "forward error correction")
3) the semantics of the transferred information may provide for a relative tolerance to transmission errors

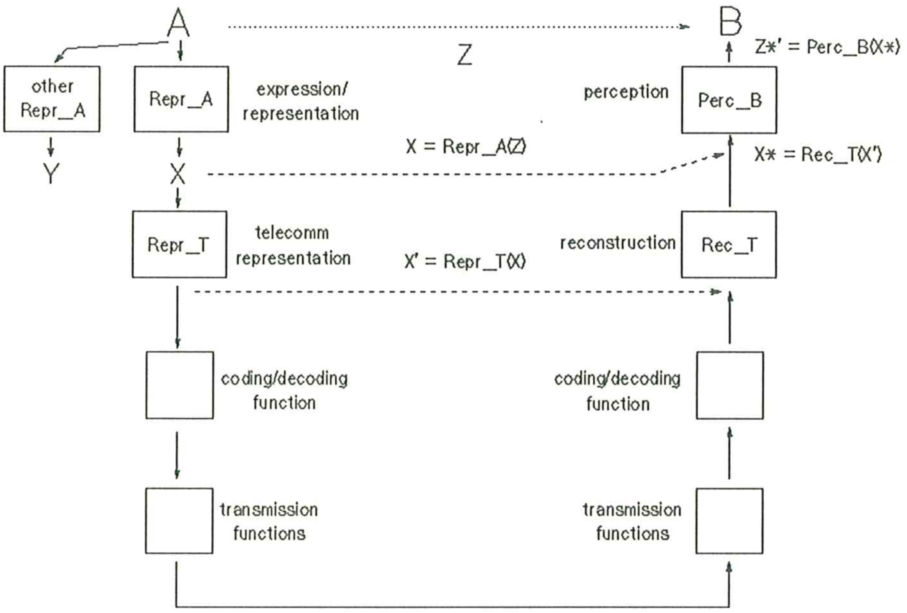


Figure 50 - information conveyance via a telecommunication service showing the main functions involved

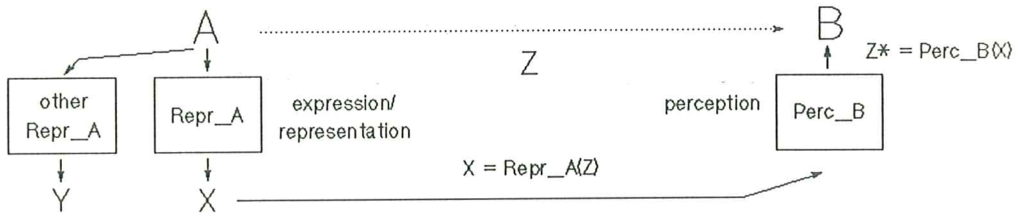


Figure 48 - concept of information conveyance and perception

If A and B are physically remote, than A will have to choose a telecommunication service (or a data service with additional protocols and functions) to convey the representation X or Y. It has to be noted that there exist limitations on what can be conveyed, some representations being not suitable for conveyance by a telecommunication service.

In addition, a telecommunication service can only transfer to another location a further representation, suitable for transmission, within the limits of technical and economical feasibility.

In other words, instead of X, X' is transferred, where the perception of X' and X is as much as possible the same, given technical and economical limitations. For example, the information conveyed X' is the representation by the telecommunication service telephony of the verbal expression of A, intended to convey the message Z. B actually receives X', which he perceives as Z*'. In formula form:

$$X' = \mathrm{Repr\_T}(\mathrm{Repr\_A}(Z)) = f(f(Z))$$

$$\begin{aligned} Z^{*\prime} = \mathrm{Perc\_B}(X^*) &= \mathrm{Perc\_B}(\mathrm{Rec\_T}(X')) \\ &= \mathrm{Perc\_B}(\mathrm{Rec\_T}(\mathrm{Repr\_T}(X))) \\ &= \mathrm{Perc\_B}(\mathrm{Rec\_T}(\mathrm{Repr\_T}(\mathrm{Repr\_A}(Z)))) \end{aligned}$$

Figure 49 illustrates this. In this figure, the functions to support the conveyance of the telecommunication representation are abstracted.

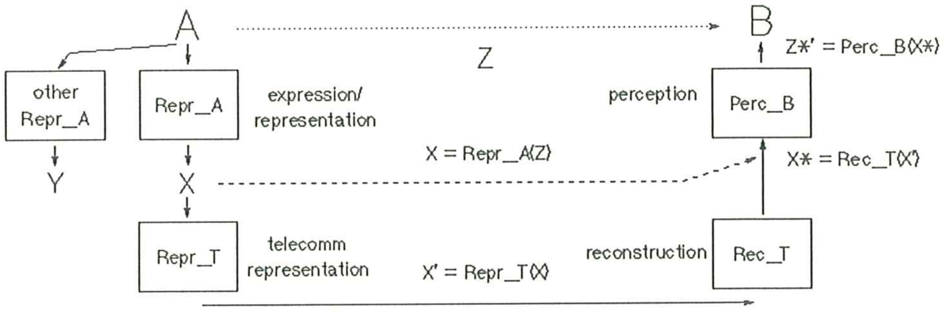


Figure 49 - information conveyance via a telecommunication service

15.1.6 Implications for the definition of telecommunication services

The responsibility for the correct definition and functioning of the different levels identified in figure 49 can now be more precisely identified.

1) The expression/representation/perception level The source end-user chooses the way in which he expresses his message Z, taking into account the expected perception by the destination end-user. The end-users are responsible for the correct functioning of these functions, which are beyond the control of any telecommunication service provider.

2) The telecomm representation/reconstruction level Given the way the end-users decide to express the message, the telecommunication service provider is responsible for the telecomm representation and reconstruction, taking again into account the expected perception aspects of the destination end-user. Note that the representation function at the source side almost always and inevitably leads to irrecoverable loss of data that was present at level X, even if the reconstruction function at the destination side functions perfectly! Any telecomm service provider will, however, argue that this data loss does not harm as long as the message as perceived by the destination (i.e. X*) remains unaffected.

3) The coding/decoding and transmission level In addition, the telecomm service provider has to perform the coding, transmission and decoding functions. The net result of all this should be a precise reconstruction of X' at the destination. The degree of precision of this reconstruction is usually denoted as "quality of service".

The specification of the characteristics of X' can effectively be done on the basis of the type classification, as discussed in the preceding section. More precisely: type classification provides a tool to precisely specify the attributes of X' that need to be preserved from source to destination. Application of the type classification to the X-level is less relevant, since:

1) such a classification is extremely difficult, given the richness of the information at that level

2) preservation of the attribute values is neither viable nor needed, as explained above.

Summarizing we may say that:

1) The responsibility of the integrity of any telecomm service can be expressed by:

   - its commitment to preserve X' during the transfer, to the highest possible degree

   - its commitment to preserve X during the transfer, within the limits of the destination's perception

2) Information typing as discussed in the preceding section can be effectively applied to describe X'. Only if X' is correctly typed, can the coding/decoding function be specified.

15.2 Extended Model

15.2.1 Introduction

In clause 8 we developed the UNSPM from the observation that an IS imposes its protocol(s) and service in the form of SNAcP and Subnet Service on an ES or another relay/IS connected to it. In clause 8, and in the examples in clause 14, we have restricted our attention to relay functions for data transmission positioned below or at the OSI NS boundary.

In the following, we will use the same principles as in clause 8, but without the restrictions assumed there, to develop the extended application of the UNSPM to data and non-data relaying functions in general.

For that purpose we will first investigate a number of important and representative relaying functions for data and non-data. Next, we will classify the characteristics of these relays. Then, we will extend the application of the UNSPM to include configurations encompassing one or more of these relay functions.

With the help of this extended UNSPM, we will then develop a conceptual model that encompasses data and non-data, while keeping close links with the OSI Basic Reference Model, at least for the data part.

15.2.2 Classification of generic relay functions

Examples of important non-data relaying functions, that we consider as representative, are given in table 16.

The following observations can be made on the content of table 16:

- the relays 2 and 3 contain the same basic relaying function with routing capability as relay 1, but add additional relaying functions
- relay 5 is an example of a relaying function without routing capability (i.e. without the capability to route to different destinations)
- the relays 6 and 7 isolate the additional relay functions of relays 2 and 3 with respect to relay 1; this leads to examples of relays with protocol conversion (6) or with irreversible information processing (7), but without routing capability (i.e. without the capability to route to different destinations)

1 - Circuit switching relaying function with routing capability, restricted to the transparent relaying of a bit- or byte-stream; e.g. the representation of a switching node for the support of 64 kbit/s unrestricted, 8 kHz structured bearer service in ISDN

2 - Circuit switching relaying function with routing capability, for the relaying of a bit- or byte-stream, with the possibility of protocol conversion (e.g. A/mu law conversion) being applied; e.g. the representation of a switching node for the support of 64 kbit/s, 8 kHz structured, 3.1 kHz audio bearer service in ISDN

3 - Circuit switching relaying function with routing capability, for the relaying of a bit- or byte-stream, with the possibility of protocol conversion (e.g. A/mu law conversion) and/or irreversible processing of information (e.g. echo suppressor, silence suppressor) being applied; e.g. the representation of a switching node for the support of 64 kbit/s, 8 kHz structured, speech bearer service in ISDN

4 - Frame mode relaying function with routing capability, restricted to the transparent relaying of bit- or byte-strings; e.g. the representation of a switching node for the support of the Frame Switching type of Additional Packet Mode Bearer Service in ISDN, or the representation of an ATM switching node

5 - Circuit switching relaying function without routing capability, restricted to the transparent relaying of a bit- or byte-stream; e.g. a line repeater

6 - Protocol converter without routing capability; e.g. A/mu law conversion, DTMF in-band signalling to Q.931 signalling conversion, code conversion in general

7 - Irreversible processing of information, without routing capability; e.g. echo suppressor, silence suppressor/TASI, etc.

Table 16 - Examples of non-data relaying functions

When considering relaying functions for non-data applications in the following, we will apply two restrictions:

1. we will only consider digital implementations of non-data relay functions; we will then consider that the extrapolation to analog implementations is possible, but outside the scope of this document.
2. we will only consider "simple" relay functions; i.e. whenever a complex relay function can be thought of as consisting of a number of simpler relay functions that are independent of each other, then we will make this conceptual substitution.

Table 17 gives examples of relaying functions for data that have not been considered in clause 8 and 14.

8 - Protocol converter with routing capability based on addressing information of a layer above the OSI NS, e.g. a transport relay of the DSG type
9 - SDU or message relay restricted to the transparent transfer or store&forward of SDUs or messages; e.g. the representation of a MHS (MTA) message transfer node (excluding possible conversion capabilities)
10 - Protocol converter without routing capability; e.g. transport layer relay of the MSDSG type, telex/teletex converter, etc.

Table 17 - Examples of additional data relaying functions

The following observations can be made on the content of table 17:

- the relays 8 and 9 illustrate the existence of relaying functions beyond the OSI Network layer
- the relay 9 can be seen as a special case of the more general concept of relay 8: routing is performed on application layer addresses or information
- the relay 10 is an example of a relay without routing capability in the data environment

Some additional observations can be made on the relays without routing capability, the relays 5, 6, 7, and 10:

- a relay operating on layer (N) information (e.g. for protocol conversion) without routing on the layer (N) addresses (if provided), will generally transparently pass addressing information belonging to lower layers. If this is the case, then layer (N-1) addressing rules are violated, since (N-1) SDUs are delivered to an (N) entity which is not attached to the destination (N-1) address.
- In a relay using common channel or out-of-band signalling principles, this violation is less visible: the relay can be thought of as operating on all (N) layer information sent in its direction

The relaying functions introduced above, as well as a number of more traditional relaying functions, will now be classified according to the following aspects:

1. the routing capability of the relay
2. the protocol conversion capability of the relay, the nature of the conversion (with or without loss of functionality)
3. the nature of the processing performed by the relay, in terms of reversible or irreversible processing
4. the nature of the forwarding mechanism used by the relay.

For the latter, we will use the following definitions:

- Direct relaying: delay between reception and forwarding of the relayed objects is kept minimal, no intermediate storage occurs, other than output queues; e.g. circuit switching node, ATM node.
- Intermediate storage relaying: the relay's objective is to minimize the delay between reception and forwarding of the relayed objects, however, a delay can be introduced as intermediate storage is required for processing; e.g. X.25 node, CLNP node ("router").
- Store&Forward: a delay between reception and retransmission of the relayed objects is part of the service definition; e.g. MHS message transfer node.

Table 18 gives the classification. In this table, the following abbreviations are used:

routing capab. - routing capability
convers. capab. - conversion capability
type of proc. - type of processing
forw. mech. - forwarding mechanism

rev. - reversible (processing)
irrev. - irreversible (processing)
int.st. - intermediate storage (relaying)
st&fw - store & forward (relaying)
opt. - optional

relay	routing capab.	convers. capab.	type of proc.	forward. mech.
- ISDN Circuit switching node for				
- 64 kbit/s unrestricted bearer	yes	no	none	direct
- 64 kbit/s audio bearer	yes	yes	rev.	direct
- 64 kbit/s speech bearer	yes	yes	irrev.	direct
- ISDN APMBS switching node for				
- frame switching bearer for data	yes	no	none	int.st.
- frame relaying bearer for data	yes	no	none	int.st.
- frame relaying bearer for non-data	yes	yes	rev.	int.st.
- frame relaying bearer for voice	yes	yes	irrev.	int.st
- ATM switching node				
- ATM bearer	yes	no	none	int.st.
- traditional data ISs				
- X.25 packet switching node	yes	opt. a	rev. b	int.st.
- CLNP "router"	yes	no	none	int.st.
- MAC bridge	yes	yes	rev.	int.st.
- additional relays for data				
- transport relay	no c	yes	rev.	int.st.
- MHS message transfer node	yes d	opt.	rev. b	st&fw
- telex/teletex conversion	no	yes	rev.	st&fw
- telex/fax conversion	no	yes	rev. e	st&fw

Table 18 - classification of some important relays

Notes to the Table:

a) *X.25 switching node may convert between X.25 and a network internal protocol*

b) *if protocol conversion implemented*

c) *the MSDSG transport relay, in which an End system is addressed by a network layer address, does not perform a routing function; a transport relay in which an End system is addressed by a transport selector does perform a routing function* *d)* *routing is performed on an address that identifies a user entry within an application, rather than the address of a (a part of a) system*

e) *conversion fax to telex requires character recognition, and therefore may not always be possible ; given this restriction the processing is reversible, however.*

From the non-data relaying functions for which the classification is given above, we now isolate the relaying functions including a routing capability by splitting of all other relaying functions. For example, a relaying function for a 64 kbit/s speech bearer, we separate into three relays:

- a relay with routing capability, similar to the relay function for 64 kbit/s unrestricted bearer
- a relay function restricted to code conversion (A/mu law)
- a relay restricted to irreversible processing (echo control/suppression

The result is given in table 19. Note that the relaying functions with routing capability are identical to those for data. From this table, the conclusion can be drawn that relays for non-data services differ from relays for data services in two respects:

- the use of additional, non-routing relaying functions for protocol conversion or signal processing
- the set of Quality of Service parameters asked from or negotiated with the network

relay	routing capab.	convers. capab.	type of proc.	forward. mech.
- ISDN Circuit switching node for				
A - 64 kbit/s unrestricted bearer	yes	no	none	direct
- ISDN APMBS switching node for				
B - frame switching bearer	yes	no	none	int.st.
C - frame relaying bearer	yes	no	none	int.st.
- ATM switching node				
D - ATM bearer	yes	no	none	int.st.
- voice/speech support functions				
E - A/mu law conversion	no	yes	rev.	direct
F - echo control/suppression	no	yes	irrev.	direct
G - silence suppression/TASI	no	yes	irrev.	direct

Table 19 - classification of elementary non-data relays

15.2.3 A Relaying and Addressing based Model (RAM)

The relays with routing capability introduced above can be subdivided into three categories:

- relays with a routing function, operating on addresses of (end)systems, e.g. X.25 packet switching node
- relays with a routing function, operating on addresses of part of (end)systems, e.g. a transport relay of the DSG type

- relays with a routing function, operating on addresses identifying an application or part of an application, or a user, rather than an (end)system, e.g. as represented by the MHS relaying function

We now build our model , giving different places to the three different categories.

Our model then is built as follows (see figure 51):

- the lower boundary of our model is the physical medium
- the upper boundary of our model is the user or the application; we reserve a sub-layer for the communication aspects of user or application (the representation of the user or application as far as the modelling of communication aspects is concerned)

The area in between we divide into two parts, the dividing boundary being the global datum, the set of addresses allowing identification of and routing to all (end)systems in the OSI environment (see clause 9.2.4 and 9.3). The resulting division is the following:

- the area between the physical media, and (below) the global datum; this area is concerned with addressing of and routing to (end)systems, and with enhancements of the data transfer attributes of as long as they go hand in hand with enhancements in the capabilities for addressing of and routing to (end)systems
- the area between the communication aspects of user or application, and (above) the global datum; this area is concerned with addressing of and routing to parts of an (end)system, and with enhancements of the data attributes that are independent of enhancements in the capabilities for addressing of and routing to (end)systems

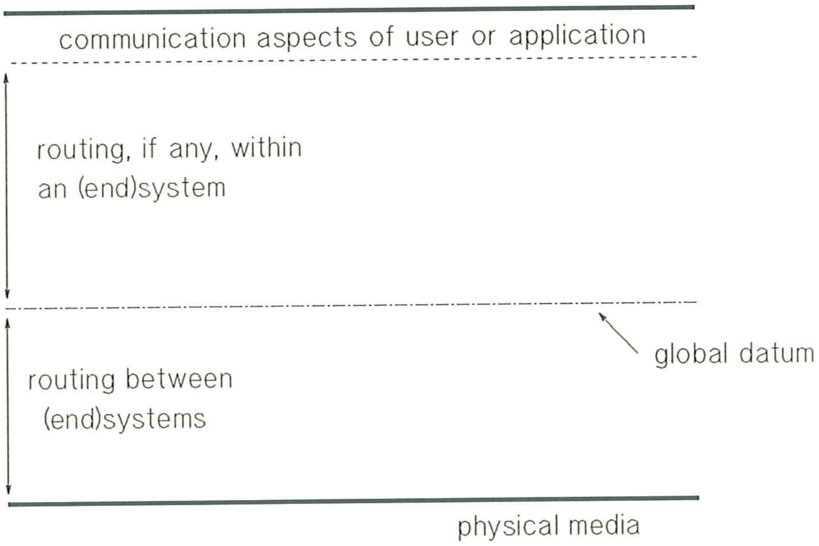


Figure 51 - the Relaying and Addressing based Model

Figure 52 shows the modelling concepts for OSI data applications in the Relaying and Addressing based Model (RAM). As explained in clause 9.3, the OSI NS boundary should be considered as positioned above the global datum.

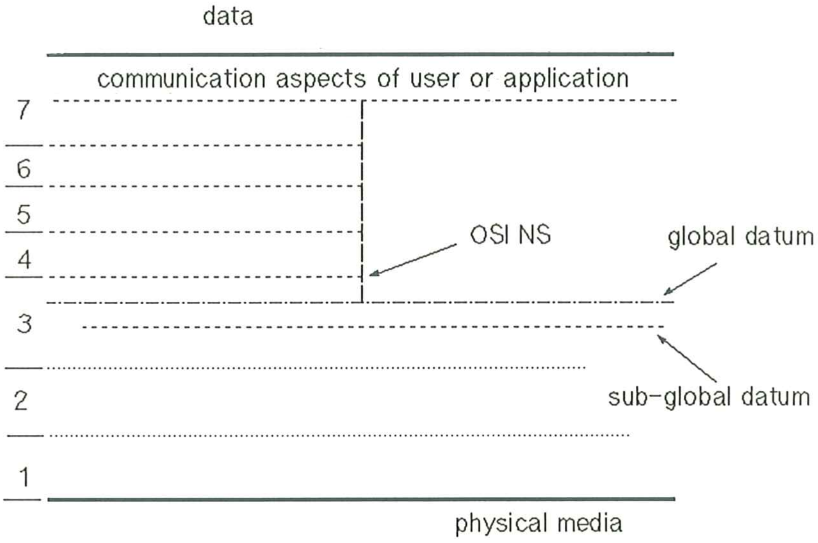


Figure 52 - the Relaying and Addressing based Model for data

The OSI NS differs in two respects from the global datum:

- the global datum consists of the addresses of all addressable endsystems of the OSI environment; the OSI NL addresses may in addition contain a selector value (and possibly a translation from an abstract to a topological structured address)
- the OSI NS imposes a well defined set of data transfer attributes and parameters for both the CO or the CL NS; the global datum imposes only the parameters for the signalling oriented primitives, but leaves a degree of freedom for the choice of data transfer attributes;

This means that any CBO or DBO service supporting the addresses of the global datum and the mandatory parameters for signalling oriented primitives of the global datum, should be considered as supporting the global datum.

NOTE 44

The classification introduced in clause 13.2 can be used to compare a subnetwork service against the global datum, the latter being classified as (C,x) or (D,x), where x can have the values P, Q, R or S.

In the area below the global datum, we introduce one refinement, the sub-global datum. The sub-global datum is introduced to reflect the existence of addressing conventions that can be seen as a global datum for a specific set of applications, for example E.164 for ISDN, or X.121 for data networks, but are a subset of the "real" global datum.

NOTE 45

According to the classification introduced in clause 13.2 the sub-global datum is classified as (B,x), where x can have the values P, Q, R or S.

Figure 53 shows the modelling concepts for non-data applications in the Relaying and Addressing based Model (RAM).

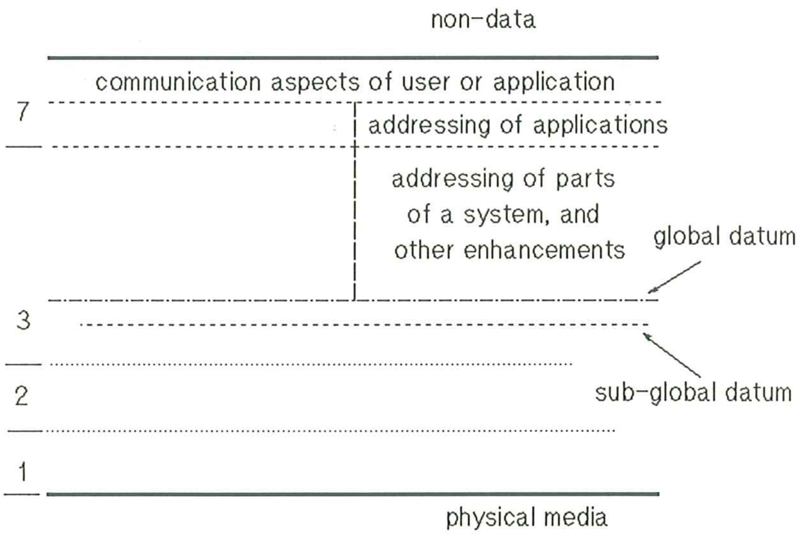


Figure 53 - the Relaying and Addressing based Model for non-data

The area between the global datum and the user or application is subdivided into two areas:

- the (lower) application layer, responsible for user/application addressing, and all other functions that should be seen as positioned in the application layer because they require application layer knowledge or decision power, e.g. irreversible processing of data
- the area between the application layer and the global datum, responsible for the addressing of parts of a (end)system, and for enhancements of the data transfer attributes as a separate function. No need is identified to subdivide this area in three or more distinct layers, e.g. layers 6, 5 and 4. Given the large variety of non-data transfer attributes, a fixed subdivision is not seen as appropriate.

Figure 54 shows the composite Relaying and Addressing based Model.

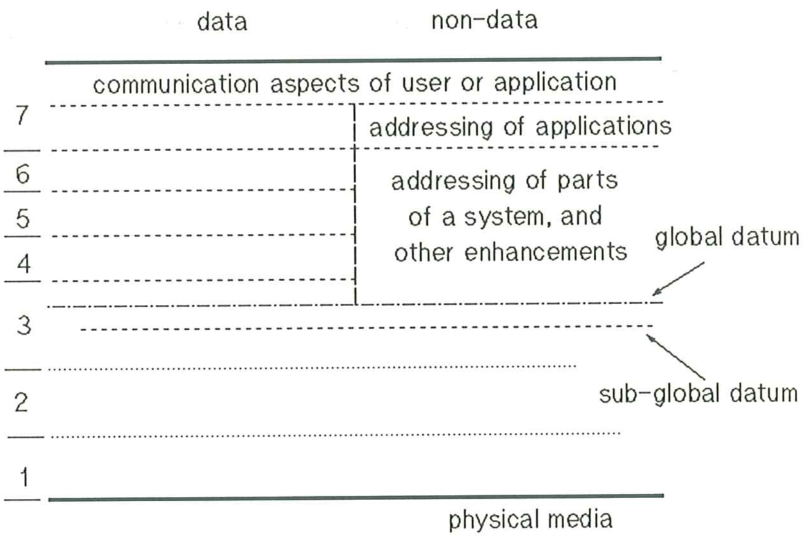


Figure 54 - the composite Relaying and Addressing based Model

Figure 55 shows a number of applications of the Relaying and Addressing based Model:

A: an ISDN circuit switching node for an unrestricted bearer, e.g. 64 kbit/s, supporting exclusively E.164 addressing; the subnetwork service boundary is positioned at the sub-global datum

B: an ISDN circuit switching node for a speech bearer, e.g. 64 kbit/s, supporting NSAP addressing in addition to E.164 addressing, and implementing A/mu coding/decoding; the subnetwork service boundary is positioned at the upper boundary of the A/mu coding/decoding function, above the global datum

C: an ISDN circuit switching node for a speech bearer, e.g. 64 kbit/s, supporting NSAP addressing in addition to E.164 addressing, and implementing A/mu coding/decoding and echo control/suppression; the subnetwork service boundary is positioned at the upper boundary of the echo control/suppression function, above the global datum

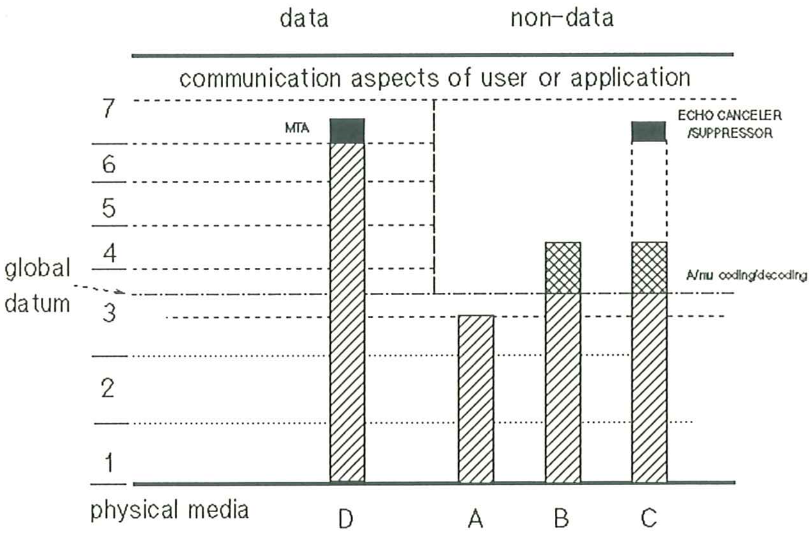


Figure 55 - applications of the Relaying and Addressing based Model

D: an MHS Message Transfer Node;

the subnetwork service boundary is positioned at the upper boundary of the MTA function

SECTION VI

SUPPLEMENTARY SERVICES

16. MODELLING OF SUPPLEMENTARY SERVICES

16.1 Introduction

Clause 6.2 of this TR discusses "signalling" as a basic concept.

In clause 6.2.2 three types of control information are identified:

- type 1: Environmental Control Information
- type 2: Connection Control Information
- type 3: Control Information used to directly control the exchange of user data

Signalling is seen as related to control information of types 1 and 2.

In clause 12 of this TR, an extension to the GLA model is introduced for signalling related to control information of type 2 (Connection Control Information).

The type 1 control information introduced in clause 6.2.2 is seen as directly related to "facilities" in protocols for data networks.

In the following, the concept of supplementary services as it exists in ISDN for data as well as for non-data services will be discussed in relation with the concepts of type 1 and type 2 control information.

The concept of call, different from the concept of connection used in this technical report, is not elaborated on here, merely because the concept requires more study.

16.2 Overview of Supplementary Services

Supplementary Services in ISDN are services which can be invoked only in combination with other services, the Basic ISDN Services. Additional control information must be exchanged for the invocation and control of Supplementary Services. This additional control information is carried in additional protocol messages in the "signalling" protocol family Q.93X.

NOTE 46

The Q.93X family of protocols is referred to as DSS1 (Digital Signalling System # 1), and is the signalling protocol to access an ISDN and ISDN services.

Table 20 gives an overview of the most important supplementary services (SSs), as identified in ECMA. Table 21 then shows some typical characteristics for each SS. In particular, for each SS is indicated:

- its "visibility" for the remote party, i.e. the party that does not invoke the SS itself
- its "visibility" for the initiator in a call
- its "visibility" for the responder in a call
- its relevance for the call establishment and data transfer phase
- its applicability on a call by call basis
- the relevant type of control information
- its expected usefulness for a data environment

supplementary service name	abbreviation used
Calling Line Identification Presentation	- CLIP
Connected Line Identification Presentation	- CoLP
Calling/Connected Line Identification Restriction	- CLIR
Diversion Unconditional	- DU
Diversion on No Reply	- DNR
Diversion on Busy	- DB
Do Not Disturb	- DND
Do Not Disturb Override	- DNDO
Completion of Calls to Busy Subscriber (Call back when free")	- CCBS
Completion of Calls on No Reply	- CCNR
Closed User Group	- CUG
Network Interception	- NI
Call Deflection	
Call Waiting	
Intrusion	
Hold	
Call Transfer	
Conference	
Call Pick-up	
User-to-User Signalling type 1	
User-to-User Signalling type 2	
User-to-User Signalling type 3	

Table 20 : Important Supplementary Services

Table 20 gives an overview of the most important supplementary services (SSs), as identified in ECMA. Table 21 then shows some typical characteristics for each SS. In particular, for each SS is indicated:

- its status in the OSI Network Service

- its "visibility" for the remote party, i.e. the party that does not invoke the SS itself
- its "visibility" for the initiator in a call
- its "visibility" for the responder in a call
- its relevance for the call establishment and data transfer phase
- its applicability on a call by call basis
- the relevant type of control information
- its expected usefulness for a data environment.

Service family	Service name	OSI Network Service	"visibility" for SS req.	"visibility" for other party	"visibility" for initiator	"visibility" for responder	3-party arrangement	relevant during call set-up/release	relevant during connection lifetime	invoked on a per call basis	type of control information	useful for data
User-to-User Signalling	type 1+2	M	Y	Y	Y	Y	–	Y	–	Yq	2q	Yo
	type 3	O	Y	Y	Y	Y	–	–	Y	Yq	2q	Yp
Identification SSs	CLIP	M	Y	–	–	Y	–	Y	–	–	1	Yo
	CoLP	M	Y	–	Y	–	–	Y	–	–	1	Yo
	CLIR	–	–	Ya	Yb	Yc	–	Y	–	–	1	–
Call Diversion SSs	DU	O	–	Yb	Yb	Y	Y	Y	–	–	1	Y
	DNR	O	–	Yb	Yb	Y	Y	Y	–	–	1	Y
	DB	O	–	Yb	Yb	Y	Y	Y	–	–	1	Y
	Call Defl	–	Y	Yb	Yb	Y	Y	Y	–	Y	2	–
	DND	O	–	Yd	Yd	–	–	Y	–	–	1	–
	DNDO	O	–	Ye	–	Ye	–	Y	–	–	1	–
Unsuccessful Call SSs	Call Wait	M	Y	–	–	Y	–	Y	–	–	1	Yo
	CCBS	–	Y	–	Y	–	–	Y	–	Y	2	–
	CCNR	–	Y	–	Y	–	–	Y	–	Y	2	–
	Intrusion	–	Y	Y	Y	Yf	Y	Y	–	Y	2	–
Multi-party SSs	Hold	–	Y	Yg	X	X	Y	–	Y	Y	2	–
	Call Xfer	–	Y	Y	X	X	Y	–	Y	Y	2	–
	Confer.	–	Y	Y	Y	Y	Y	Y	Y	Y	2	–
Cluster SSs	CUG	O	Y	Yh	Y	Yh	–	Y	–	–	1	Y
	Call P.U.	–	Y	Yb	Yb	Y	Y	Y	–	Y	2	–
Network SSs	NI	O	Yj	Y	Y	–	Y	Y	–	Y	2	Yk

Legend:

M = mandatory service
O = optional service
Y = yes
X = independent of initiator/responder
– = no

Table 21 : Characteristics of important Supplementary Services

Notes to Table 21:

a - *if CLIP/CoLP invoked*
b - *if CoLP invoked*
c - *if CLIP invoked*
d - *if DND indication provided*
e - *if DND invoked*
f - *always visible to intruded into party*
g - *if indication of Hold provided*
h - *if remote party belongs to CUG(s) and no incoming access*
j - *network is invoking party*
k - *similar to network generated error message (RESET + cause)*
o - *required or assumed in OSI environment*
p - *available as the optional expedited data facility in OSI environment*
q - *user-to-user signalling requires a subscription and/or registration, after which the use is optional on a per call basis; the latter only is shown in the table*

16.3 Concluding Remarks

16.3.1 Relationship with Subnetwork Service

Some of the Supplementary Services have an effect on the end-to-end communication, and therefore on the subnetwork service, e.g. Calling/Connected Line Identification Restriction, Closed User Group, User-to-User signalling.

The following observations can be made for these Supplementary Services:

- The actual subnetwork service at a given moment in time is equal to the sum of the basic service and the supplementary services subscribed/registered to.
- The potential subnetwork service is equal to, or higher than, the combination of the basic service and the sum all of the supplementary services that increment the subnetwork service.
- The Basic Service may define a subset of the Subnetwork Service, by excluding the use of some protocol elements and/or parameter ranges from the subnetwork access protocol, or excluding some active operations on them.
- Some Supplementary Services describe an incremental service, by the incremental use of protocol elements and/or parameter ranges in the subnetwork access protocol, or additional active operations on them; these Supplementary Services then are increments in the actual subnetwork service and intervention level, towards the potential subnetwork service and intervention level.
- Some other Supplementary Services describe an incremental service, by restricting the use of protocol elements and/or parameter ranges in the subnetwork access protocol, or restricting active operations on them; these Supplementary Services then in fact are decrements in the actual subnetwork service and intervention level.

Other Supplementary Services, e.g. Calling Line Identification Presentation, Call Waiting, cannot simply be described in terms of a modification of the end-to-end service (they cover agreements between one party and the network on the presentation of information transferred by and available in the network to this party, the other party not even being informed of the existence of these agreements).

16.3.2 Correlation analysis of characteristics of Supplementary Services

Table 21 shows that it is extremely difficult to construct some sort of "universal" classification of the different supplementary services: the values in the different columns are hardly inter-related, with the following exceptions.

The column "invoked on a per call basis" reflects the distinction between type 1 and type 2 control information in the adjacent column. Furthermore, there appears to be a correspondence between these two columns and the column "OSI Network Service": the OSI Network Service does not support the SSs corresponding to type 2 control information (with the exception of user-to-user signalling and Network Interception, both are seen as special cases). The explanation of this observation could be that these services are usually not seen as very useful in data environments. The column "useful for data" seems to confirm this view.

The protocols that support supplementary services can probably best be structured on the basis of the distinction between type 1 and type 2 control information, since the first type has to be supported by protocols which have no direct relation to specific calls/connections (usually seen as "management"), while the second type is supported by the addition of relevant protocol elements to (existing) call/connection control protocols. It seems, however, too ambitious to claim that this can be seen as a sufficient way to model SSs in general. More study on this topic is required, especially in relation to the ongoing study in the area of modelling and specification of OSI management protocols.

SECTION VII

APPENDICES

APPENDIX A

CLASSIFICATION OF FAN-IN/FAN-OUT FUNCTIONS OF A LAYER IN TERMS OF MULTIPLEXING AND ROUTING FUNCTIONS

A.1 Introduction

This Appendix describes a classification which can be used to classify the fan-in/fan-out functions of a layer in terms of multiplexing and routing.

It should be noted that the notion "routing" in this Appendix is different from the notion "routing" as used in the context of functionalities of subnetworks. "Routing" in this Appendix is used as the functionality of an (N)-layer entity in an end system that maps an (N-1)-connection (or information flow) into an (N)-connection (or Information Flow), while "routing" in the context of subnetworks is used as the functionality of an (N)-layer relay entity in an intermediate system that maps an (N-1)-connection into another (N-1)-connection.

NOTE A.1

This Appendix discusses the multiplexing issue solely from the perspective of addressing capabilities, while Appendix B discusses the same subject solely in the context of connection multiplexing with emphasis on the different types of multiplex mechanisms such as FDM/TDM and delimiting aspects.

A.2 The Classification

As described in Clause 11, fan-in/fan-out functions in a certain layer (N) can be grouped into three sublayers (b1, b2 and b3), and can operate in CO and CL environments.

A.2.1 CO Environments

For CO environments, we may distinguish four cases:

(a) The simplest case

This occurs where a single (N)-SAP can only be connected with one certain single other remote (N)-SAP. No other remote (N)-SAP can be chosen, and only one connection may exist between both (N)-SAPs.

In terms of the GLA this covers the case where sublayers b1, b2 and b3 are all empty.

(b) The CO multiplexing case

This occurs where a single (N)-SAP can only be connected with a single other remote (N)-SAP, but several connections can simultaneously be established to that remote (N)-SAP.

In terms of the GLA this covers the case where layers b1 and b2 are empty, but layer b3 is non-empty.

(c) The CO routing case

This occurs where each member of a group of (N)-SAPs in one system has the capability to establish a connection to each member of a group of other remote (N)-SAPs, but between two (N)-SAP pairs only one connection can exist at the same time.

In terms of the GLA this covers the case where layers b1 and/or b2 are non-empty, but layer b3 is empty.

(d) The CO routing/multiplexing case

This occurs where each member of a group of (N)-SAPs in one system has the capability to establish connections to each member of a group of remote (N)-SAPs, while more than one connection can be established between a local and a remote (N)-SAP.

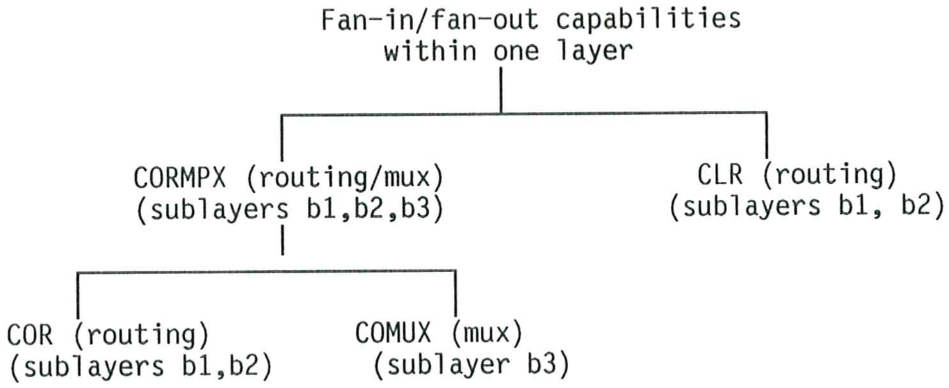
In terms of the GLA this covers the case where layer b1 and/or b2 is non-empty, and layer b3 is also non-empty.

A.2.2 CL Environments

According to the GLA, sublayer b3 is always empty in CL environments. Therefore the only case that can occur is the routing case, where each member of a group of (N)-SAPs in one system has the capability to communicate with each member of a group of other remote (N)-SAPs. Indeed, multiplexing (i.e. the functionality of sublayer b3) is a privilege of CO- environments.

A.3 Summary

Figure A-1 illustrates the classification.



Legend

CORMPX :	Connection-based routing/multiplexing: Multi-SAP to multi-SAP connections are possible, and more than one connection may exist between a local and a remote SAP.
COR :	Connection-based routing: Multi-SAP to multi-SAP connections, but only one connection between a local and a remote SAP.
COMUX :	Connection-based multiplexing: Single-SAP to single-SAP communication with more connections between a local and a remote SAP.
CLR :	Connectionless routing: Multi-SAP to multi-SAP communication on a CL basis.

Figure A-1 - Illustration of the classification.

APPENDIX B

MULTIPLEX MECHANISMS AND THEIR RELATION TO CBO AND DBO SERVICES

B.1 Introduction

This Appendix discusses the relation between two types of multiplex mechanisms (i.e. cyclic multiplexing and demand multiplexing) on the one hand, and the concept of CBO and DBO services on the other hand.

In order to do this, a precise terminology with respect to these concepts is developed first. Thereafter a classification of multiplex mechanisms is given, and the relation with CBO and DBO services is explained.

NOTE B.1

This Appendix discusses the multiplexing issue solely in the context of connection multiplexing with emphasis on the different types of multiplex mechanisms such as FDM/TDM and delimiting aspects, while Appendix A discusses the same subject solely from the perspective of addressing capabilities.

B.2 Terminology

This gives a set of definitions which are used as the basis for the subsequent discussion. Most of these definitions are derived from publications from D. Davies during the seventies (See for example Davies and Barber "Communication Networks for Computers").

(a) Multiplexing

The provision of several connections over a single aggregate connection.

NOTE B.2

If a multiplexer is considered as an (N)-layer function in the sense of the OSI Reference Model, then the connections to be multiplexed can be denoted as (N)-connections, and the aggregate connection can be denoted as an (N-1)- connection.

(b) Space Division Multiplexing (SDM)

A multiplex mechanism where a certain available space is divided into space segments, each assigned to a single physical circuit.

NOTE B.3

An example is a multipair cable. In this case the shared space is provided by the cable shield. The space segment corresponds with a single (twisted) pair.

(c) Frequency Division Multiplexing (FDM)

A multiplexing mechanism where the available bandwidth is divided into frequency slots, each assigned to one individual connection.

(d) Time Division Multiplexing (TDM)

A multiplexing mechanism where the available time is divided into time fragments, each assigned to a single connection according to some assignment rule. This may or may not be done on a strict cyclic basis (see (e) and (f) hereafter).

Depending on the unit of information transferred during one time fragment, one can speak of bit-interleaved, octet-interleaved, character-interleaved, envelope- interleaved, packet-interleaved, or "whatever else"- interleaved multiplexing.

NOTE B.4

This definition is kept very close to its literal meaning. It includes statistical multiplexing as used in packet switching environments (see (f) and Figure B-1 hereafter).

(e) Cyclic Multiplexing

Time Division Multiplexing where the available time is assigned to the connections on a cyclic basis. One cycle is called a "multiplex frame". A contiguous time-period used by an individual connection within that frame is called a "time-slot". The identification of a connection is derived from the relative position of its time-slot (with respect to the position of other time-slots) in a multiplex frame.

The duration of time-slots used by an individual connection need not be constant. If they are not constant, the multiplex frame duration is also not constant, and we then speak of "variable cycle multiplexing".

If, however, they are constant, then the multiplex frame duration is also constant, and we then speak of "fixed cycle multiplexing". In this case, a unit of information is usually a bit, an octet, an envelope (X.50) or a character.

(f) Demand Multiplexing

Time Division Multiplexing, where the available time is assigned to the individual connections on a demand basis without any predetermined order. Identification of a connection is achieved by means of a "header" added to the user data to be transferred.

Examples are: statistical character multiplexing, and X.75 (which is a packet-interleaved Time Division Multiplexer).

(g) Data delimiting

The function which takes care of the mapping of a finite non-zero number of bits offered by the user as one single piece of data (called a "delimited bitstring") into a continuous bitstream at the sending side, and the corre- sponding reconstruction of this delimited bitstring out of the incoming continuous bitstream and the subsequent delivery of this as one integral piece of data at the receiving side.

Two types of data delimiting can be distinguished:

- Asynchronous delimiting

  This covers the case where the number of transmitted delimited bitstrings per time unit and the size of each delimited bitstring are both not necessarily constant. If they are not constant, then the delimited bitstrings are transferred with some explicitly or implicitly coded note of their length.

- Synchronous delimiting

  This covers the case where the delimited bitstrings are offered and delivered at a fixed rate, and all have the same length.

NOTE B.5

Synchronous delimiting could be seen as a degenerate form of asynchronous delimiting.

Two well-known examples of asynchronous data delimiting are:

- The framing mechanism of HDLC (which includes the addition and deletion of flags, the zero insertion and deletion in the user data to prevent flag simulation, and the interframe time-fill using contiguous flags or con- tiguous binary ONEs).
- The start-stop mechanism in start-stop transmission where the opening flag consists of a binary ZERO, and the length is constant. Therefore, strictly speaking, a closing flag is not needed. Interframe time-fill is realized by contiguous binary ONEs, while small bit-clock deviations are handled by the requirement that the minimum length of the interframe time-fill shall be at least one bit-period (stop-bit).

A well-known example of synchronous delimiting can be found in PCM multiplex systems. We recognize here two levels of synchronous delimiting:

- The highest level is the mechanism which guarantees that user octets (representing coded speech samples) generated by one CODER are transferred as a composite whole, so that the corresponding remote DECODER can perform its task. This is achieved by a one-to-one mapping of user octets (the delimited bitstrings which are offered by the user) into the unit of information transferred during one time fragment in the PCM/TDM multiplexer.
- The lower level is the mechanism which guarantees that the aggregate octet string produced by the multiplexer during one sampling period is transferred as a composite whole, so that the remote demultiplexer can perform its task. Synchronous delimiting is here achieved by the addition of a unique bit pattern on which the receiver can synchronize itself, so that it can reconstruct the aggregate octet string produced by the multiplexer and offer this as a composite whole to the demultiplexer.

(h) CBO (Continuous Bitstream Oriented) Service

A connection is said to support a CBO service if it transfers a bitstream with a constant bit rate and transfer delay during the lifetime of the connection, while delimiting (if any) is restricted to synchronous delimiting only.

Usually the bitstream cannot be stopped by the receiver and also not by the sender.

NOTE B.6

CBO is particularly applicable to the service offered by circuit switching networks.

(i) DBO (Delimited Bitstring Oriented) Service

A connection is said to support a DBO service if it supports the transfer of delimited bitstrings during the lifetime of the connection, and the delimiting is restricted to asynchronous delimiting only. The transfer delay and throughput can only be specified in statistical terms (such as average values). There is no commitment at the sending side to offer delimited bitstrings all the time. In addition, for data applications it is usually possible to exercise backpressure flow control at the receiver side so that (at least to some extent) the receiver can (temporarily) regulate the flow of information.

NOTE B.7

DBO is particularly applicable to the service offered by packet switching networks.

NOTE B.8

DBO is also a useful notion in CL environments. However, since there is no concept of multiplexing in CL environments, this is not further elaborated upon in this Appendix.

B.3 Classification of Multiplexing Mechanisms

Figure B-1 shows the classification. The figure directly follows from the definitions given in B.2.

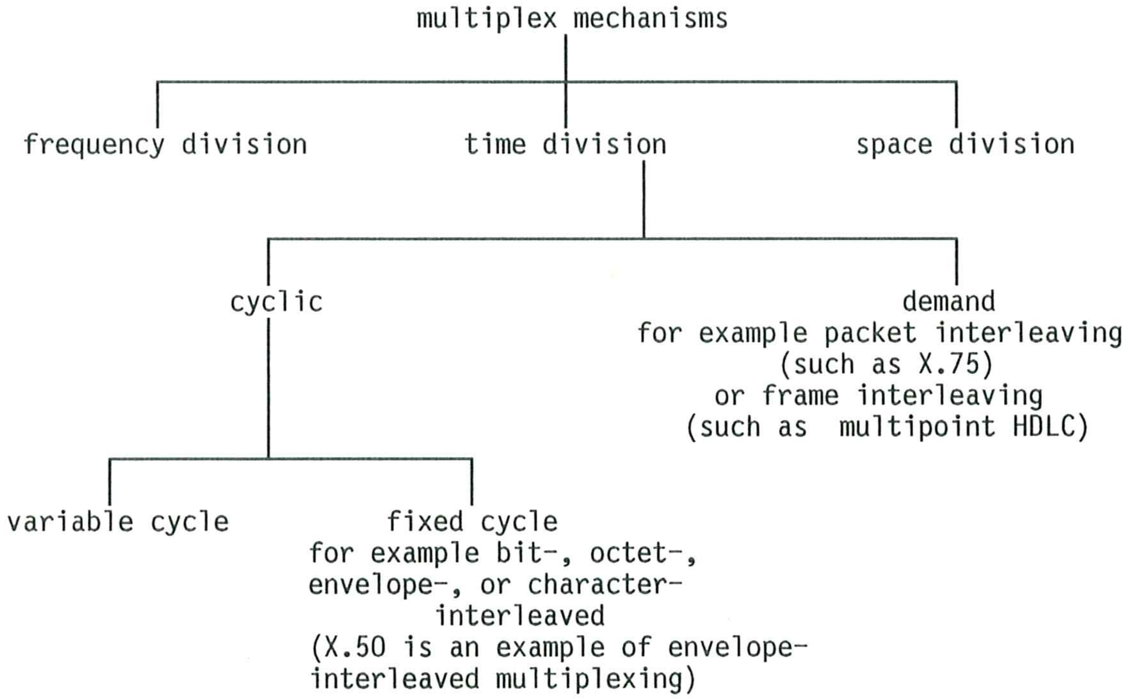


Figure B-1 - Classification of multiplex mechanisms

B.4 Relation between multiplexing mechanisms and the provision of CBO and DBO services

Fixed cycle TDM multiplexers as well as FDM multiplexers offer connections which are characterized by a constant bandwidth (bit rate) and transfer delay. If delimiting is supported, it is always synchronous delimiting. Therefore these multiplexers can be characterized as multiplexers which provide a CBO service.

Demand TDM multiplexers always transfer information which is offered as groups of bits which have to be transferred and delivered "on demand" as a composite whole. The users accept that the properties with respect to delay and throughput are expressed only in statistical terms. Therefore, this type of multiplexer can be characterized as multiplexers which provide a DBO service.

B.5 Some Mapping Aspects of DBO/CBO (N)-Connections onto DBO/CBO (N-1)-Connections

B.5.1 The Provision of a DBO Connection over a CBO Connection

This can be accomplished by an asynchronous delimiting function (see definition (g) in B.2), which guarantees that the sender always sends "something".

B.5.2 The Provision of a CBO Connection over a DBO Connection

This can be accomplished by the use of a (bit-oriented) FIFO at the sending side and at the receiving side, so that the time fluctuations imposed by the underlying DBO connection can be compensated at the penalty of additional delay.

In addition, if some statistical properties of the offered continuous bitstring are known, then this knowledge can be used to apply source encoding to reduce the bandwidth requirements of the underlying DBO connection. A classic example of this is "packetized voice".

B.5.3 The Provision of a low Bandwidth CBO Connection over a high Bandwidth CBO Connection

This can be accomplished:

- either by the use of a fixed cycle TDM multiplexer which allows sharing the high bandwidth connection with one or more other low bandwidth connections,
- or by some rate adaptation (stuffing) technique, which could be considered as multiplexing with one or more dummy connections. This method is simple, but inevitably leads to a waste of available bandwidth.

APPENDIX C

SERVICE CONCEPT ACCORDING TO CCITT AND ISO

Subnetwork services up to the OSI Network Service as defined in CCITT use a service concept that differs from the ISO service concept for subnetwork services: for example, the bearer services defined for ISDNs and PSNs define the transfer of different types of user data between a pair of user-network interfaces via a subnetwork service provider entity (see Figure C-1). This then can easily be related to the use of ISDNs in the public domain, and the need to define services on which tariffing can be applied.

The link between this concept of service and the ISO concept of service can be made as follows. The conformance or type approval requirement for the connection of end systems to user-network interfaces for the support of a certain bearer service, requires the end system to implement the appropriate subnetwork access protocol and related functions, thus to implement the subnetwork service provider entity (see Figure C-2). The combination of the two subnetwork service provider entities in the two end systems, and the subnetwork service provider entity in the intermediate system, constitute the subnetwork service provider, in accordance with the ISO view of the subnetwork service.

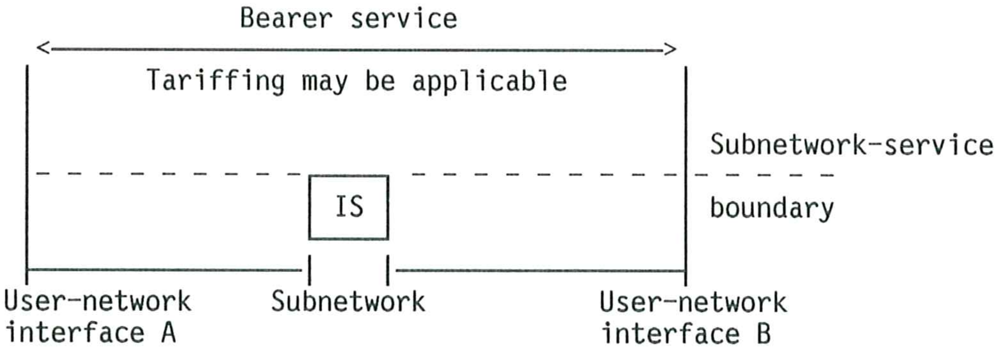


Figure C-1 - Bearer Service Concept

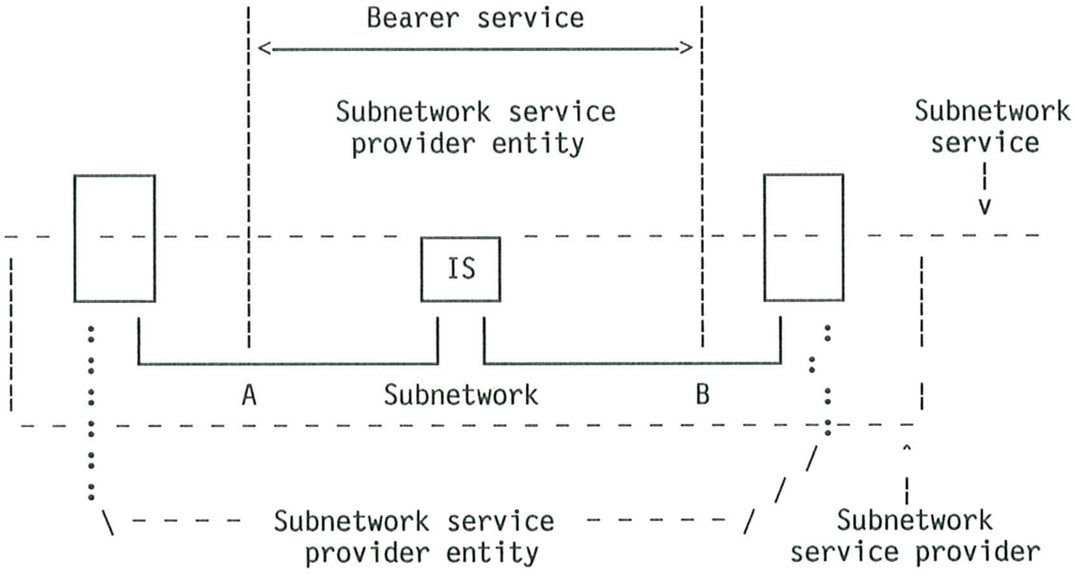


Figure C-2 - Relation between Bearer Service and Subnetwork Service Provider

APPENDIX D

ACRONYMS AND NOTATION

A	Subnetwork classification
Add	Address
ASS	Actual Subnetwork Service
B	Subnetwork classification (without NSAP)
C	Subnetwork classification (NSAP transferred)
CBO	Continuous Bitstream Oriented
CC	Connection Control
CCITT	International Telegraph and Telephone Consultative Committee
CEP	Connection End-Point
CL	ConnectionLess
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network Service
CLR	ConnectionLess Routing
CM	Connection Management
CNSPM	Constrained Network Service Provider Model
CO	Connection-Oriented
CODEC	COder DECoder
COMUX	COnnection-based MUltipleXing
CONS	Connection Oriented Network Service
COR	COnnection-based Routing
CORMPX	COnnection-based Routing/MultiPleXing
CP	Convergence Protocol
CR	Connection Reference
CRC	Cyclic Redundancy Check
CS	Circuit Switching
D	Subnetwork Classification
DBO	Delimited Bitstring Oriented
DCE	Data Circuit-terminating Equipment
DLCI	Data Link Channel Identifier (of LAPD)
DSP	Domain Service Provider
DT	Data Transfer
DTE	Data Terminal Equipment
EP	Enhancement Protocol
ES	End System
FDM	Frequency Division Multiplexing
FIFO	First In First Out
FS	Frame Switching

GDP	Globally-Defined Parameters
GHF	Generic Header Format
GLA	Generic Layer Architecture
HDLC	High Data Link Control
Id	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IFI	Information Flow Identifier
IONL	Internal Organization of the Network Layer
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IWU	InterWorking Unit
LAN	Local Area Network
LAPB	Link Access Protocol Balanced
LAPD	Link Access Control D-channel
LC	Link Control
LCI	Logical Channel Identifier
LL	Logical Link
LLC	Logical Link Control
LLC1	Logical Link Control type 1
LLC2	Logical Link Control type 2
LLME	Lower Layer Management Entity
LLCx	LLC1 or LLC2
LSAP	Link Service Access Point
MA	Medium Access
MAC	Medium Access Control
MPX	MultiPleX/deMultiPleX function
MUX	MUltipleXing
(N)	Any specific Layer or Sublayer, where (N-1) is the adjacent lower, and (N+1) is the adjacent higher layer or sublayer
(N)-CP	(N)-layer Convergence Protocol
(N)-EP	(N-1)- to (N)-Service Enhancement Protocol
(N)-GDP	(N)-layer Globally-Defined Parameters
(N)-PDU	(N)-Protocol Data Unit
(N)-SAP	(N)-Service Access Point
(N)-SDU	(N)-Service Data Unit
(N)-SP	(N)-layer Service Provider
(N)-SSP	(N)-Subnetwork Service Provider
NS	Network Service
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
P	Subnetwork classification
PAD	Packet Assembler/Disassembler
PCEP	Potential CEP
PCI	Protocol Control Information
PCM	Pulse Code Modulation
PCM-CODEC	COder DECoder for Pulse Code Modulation

PDN	Public Data Network
PDU	Protocol Data Unit
PLP	Packet Level Protocol (of X.25)
PS	Packet Switching
PSN	Private Switching Network
PSS	Potential Subnetwork Service
PVC	Permanent Virtual Circuit (of X.25)
Q	Subnetwork classification
QoS	Quality of Service
R	Routing
R+R	Relaying and Routing (inter-subdomain)
r+r	relaying and routing (intra-subdomain)
Rx	Subnetwork classification
SAP	Service Access Point
Sd	Subdomain
SDM	Space Division Multiplexing
SdSP	Subdomain Service Provider
SDU	Service Data Unit
Sel	Selector
SEP	Service End Point
SN	SubNetwork
Sn	SubNetwork
SNAcP	SubNetwork Access Protocol
SNPA	SubNetwork Point of Attachment
SP	Service Provider
Sx	Subnetwork classification
TDM	Time Division Multiplexing
TR	Technical Report
TS	Transport Service
UNSPM	Unconstrained Network Service Provider Model
UtN	User-to-Network
UtU	User-to-User
VC	Virtual Circuit (of X.25)