

ECMA

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

AN ARCHITECTURAL FRAMEWORK FOR PRIVATE NETWORKS

ECMA TR/44

December 1987

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

ECMA

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

AN ARCHITECTURAL FRAMEWORK FOR PRIVATE NETWORKS

ECMA TR/44

December 1987

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 three 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 entirety 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.

Although the non-data environment is also encompassed by the architecture presented in this Technical Report, practicalities are at present restricted to data applications. It is intended to respond to and accommodate the growing industry interest in the modelling of non-data applications, and data/non-data in-

tegration, in a future Edition. Experts are indeed already progressing industry studies such as these within the ECMA forum. It is believed that this global standardization of generic architecture for private networking will be further advanced as the industry progresses beyond the frontiers of pure data applications and OSI.

Adopted as an ECMA Technical Report by the General Assembly of 10th December 1987.

TABLE OF CONTENTS

	Page
SECTION I : GENERAL	1
1. SCOPE	3
2. FIELD OF APPLICATION	3
3. REFERENCES	3
4. INTRODUCTION	4
5. DEFINITIONS	5
5.1 Real system (system)	5
5.2 Physical medium (medium)	6
5.3 End system (ES)	6
5.4 Intermediate system (IS)	6
5.5 Syntax check of protocol elements	6
5.6 Active and passive operations on protocol elements	6
5.7 Actual protocol intervention level (of an IS)	6
5.8 Potential protocol intervention level (of an IS)	7
5.9 Visibility of a system	7
5.10 Subnetwork (real subnetwork) (SN)	7
5.11 Interworking unit (IWU)	7
5.12 Subnetwork access protocol	8
5.13 Subnetwork access service	8
5.14 Potential subnetwork service (or potential service supported by the subnetwork)	8
5.15 Actual subnetwork service (or actual service supported by the subnetwork)	8
5.16 Subnetwork convergence protocol	9
5.17 Enhancement protocol	9
5.18 (N)-layer routing	9
5.19 (N)-layer relaying	9
6. BASIC CONCEPTS	9
6.1 The Generic Header Format Concept	9
6.1.1 OSI Reference Model Multi-Layer Header Syntax	9
6.1.2 The Single-Layer Generic Header Format (GHF) and Abstract Header Syntax	10
6.1.3 More about the relation between the GHF and the Concrete Header Format	11
6.2 Signalling	11
6.2.1 Introduction	11
6.2.2 Classification of three Types of Control Information	11
6.2.3 The concept of signalling	12
6.2.4 The distinction between in-band and out-of-band signalling	13
6.2.5 The distinction between common channel and channel associated signalling	13

6.2.6	Some examples	14
6.2.7	The aspect of subnetwork intervention	14
SECTION II : GENERIC LAYER ARCHITECTURE MODEL		17
7.	GENERIC LAYER ARCHITECTURE (GLA) MODEL	19
7.1	Introduction	19
7.2	Protocol Control Functions and Fan-in/Fan-out Functions	20
7.3	Expansion of Common Control Functions	21
7.4	Expansion of GLA Fan-in/Fan-out Functions	25
7.4.1	General	25
7.4.2	Nesting Rules and the Generic Header Format	26
7.4.3	Protocol Connection Referencing	26
7.5	Expansion of Individual Connection Control Functions	27
7.6	Hybrid implementations of the GLA	28
7.7	An example of the application of the GLA to a protocol	28
8.	EXTENSION OF THE GLA MODEL FOR SIGNALLING	29
8.1	General	29
8.2	Synchronization aspects	33
8.3	Drawing conventions	34
8.4	Extended GLA	35
SECTION III : GLOBAL NETWORK SERVICE PROVIDER MODELS		39
9.	INTRODUCTION	41
10.	UNCONSTRAINED NETWORK SERVICE PROVIDER MODEL (UNSPM)	41
10.1	Introduction	41
10.2	The subnetwork concept	41
10.2.1	Architectural observations on intermediate systems (ISs)	41
10.2.2	More about "protocol intervention level"	43
10.2.3	Subnetwork access protocol header syntax and semantics	43
10.3	Subnetwork interconnection principles	45
10.3.1	Introduction	45
10.3.2	The IWU as service concatenator	45
10.3.3	The significance of the protocol intervention level of the IWU	47
10.3.4	Addressing aspects	50
10.4	Relaying as service mapping versus relaying as protocol mapping	50
10.5	Representation of signalling	50
10.6	The resulting model	53
10.6.1	Introduction	53
10.6.2	The model	53
10.6.3	Implications for end systems	54
10.6.4	Relation to the OSI NS	55
11.	CONSTRAINED NETWORK SERVICE PROVIDER MODEL (CNSPM)	56
11.1	Introduction	56
11.2	The Basic CNSPM	56
11.3	Refinement of the Basic CNSPM	57

11.3.1 Interpretation of ISO 8648	57
11.3.2 Application of the principle of recursion	60
11.3.3 Reduction of refined multi-layer architecture	61
11.3.4 Application of the multi-layer architecture to switched DBO and CBO services	61
11.3.5 Expansion of functions of multi-layer model	64
11.4 Subsettings of the CNSPM	65
SECTION IV : EXAMPLES	67
12. ANALYSIS OF SOME SPECIFIC SUBNETWORKS	69
12.1 Methodology used	69
12.2 Subnetwork Service Classification Scheme	69
12.3 X.25 (1984) and X.25 (1980)	70
12.4 X.21 and X.22	74
12.5 8802.x LAN and Bridged LAN	77
12.6 PSN with Multiple Services	80
12.6.1 General Considerations	80
12.6.2 PSN with Circuit Switching Service	84
12.6.3 PSN with Frame Switching Service	87
12.6.4 PSN with Packet Switching Service	93
SECTION V : APPENDICES	99
APPENDIX A - CLASSIFICATION OF FAN-IN / FAN-OUT FUNCTIONS OF A LAYER IN TERMS OF MULTIPLEXING AND ROUTING FUNCTIONS	101
APPENDIX B - MULTIPLEX MECHANISMS AND THEIR RELATION TO CBO AND DBO SERVICES	103
APPENDIX C - ABSTRACT SYNTAX OF NETWORK LAYER ADDRESS	109
APPENDIX D - SERVICE CONCEPT ACCORDING TO CCITT AND ISO	111
APPENDIX E - ACRONYMS AND NOTATION	113

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 applications in both dedicated and integrated services private networks.

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

The material presented encompasses the provision for future applicability to non-data. The practicalities of this extended applicability however are not currently included in this Technical Report since within ECMA the subject is presently under development.

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 Specifications
CCITT Rec. Q.931/ I.451	ISDN User-Network Interface Layer 3 Specification
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

D.W.Davies and D.L.A.Barber: "Communication Networks for Computers", John Wiley & Sons, London, 1973

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 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".

- iii) In Section III, two 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.

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 layer service boundaries corresponding to the OSI layers 1, 2 and 3, and the sublayer service boundaries corresponding to MAC and LLC.

- 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.

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 V).

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 analyses the structure of a full Network Layer address based on the Multi-Layer Service Provider Model developed in Clause 11.

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

Appendix E 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.

In the second case, the subnetwork 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.

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).

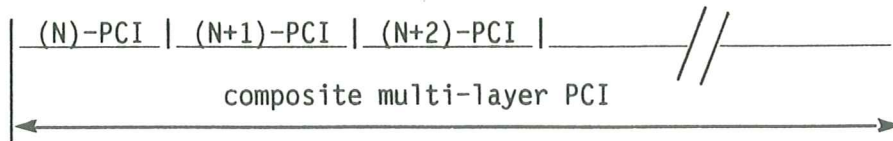


Figure 1 - Nested header structure

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 7.

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 7 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 7.4), 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 7.4). 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 8 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.

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.

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 22

"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

GENERIC LAYER ARCHITECTURE MODEL

7. GENERIC LAYER ARCHITECTURE (GLA) MODEL

7.1 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 focussed 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 23

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 8.

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.

7.2 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 2.

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

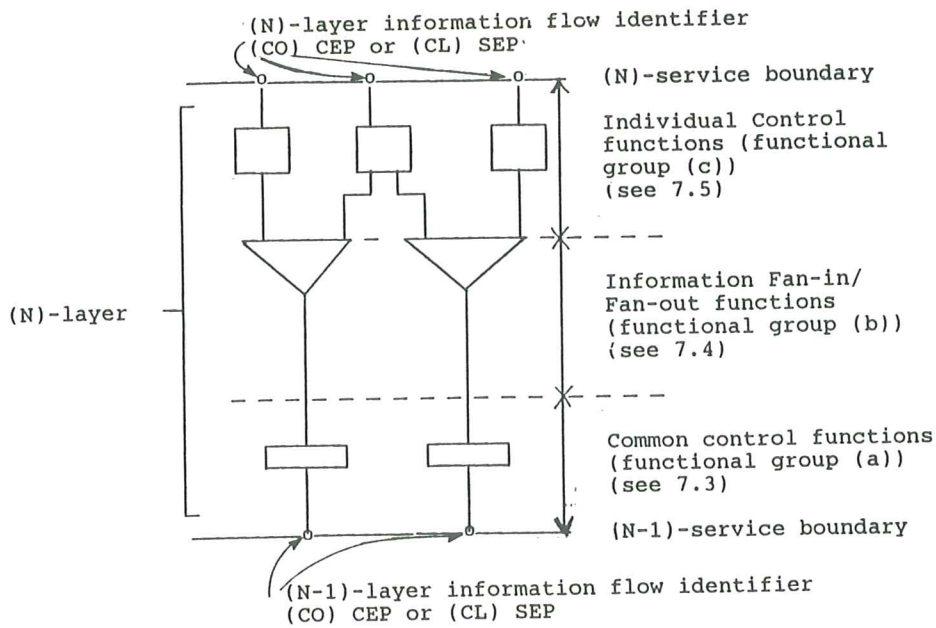


Figure 2(a) - Positioning of control functions and fan-in/fan-out functions in an (N)-layer

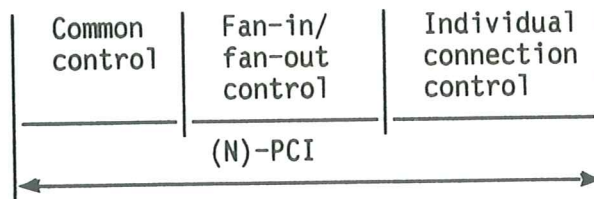


Figure 2(b) - Corresponding Generic Header Format

7.3 Expansion of Common Control Functions

Figure 3(a) 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 choose 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:

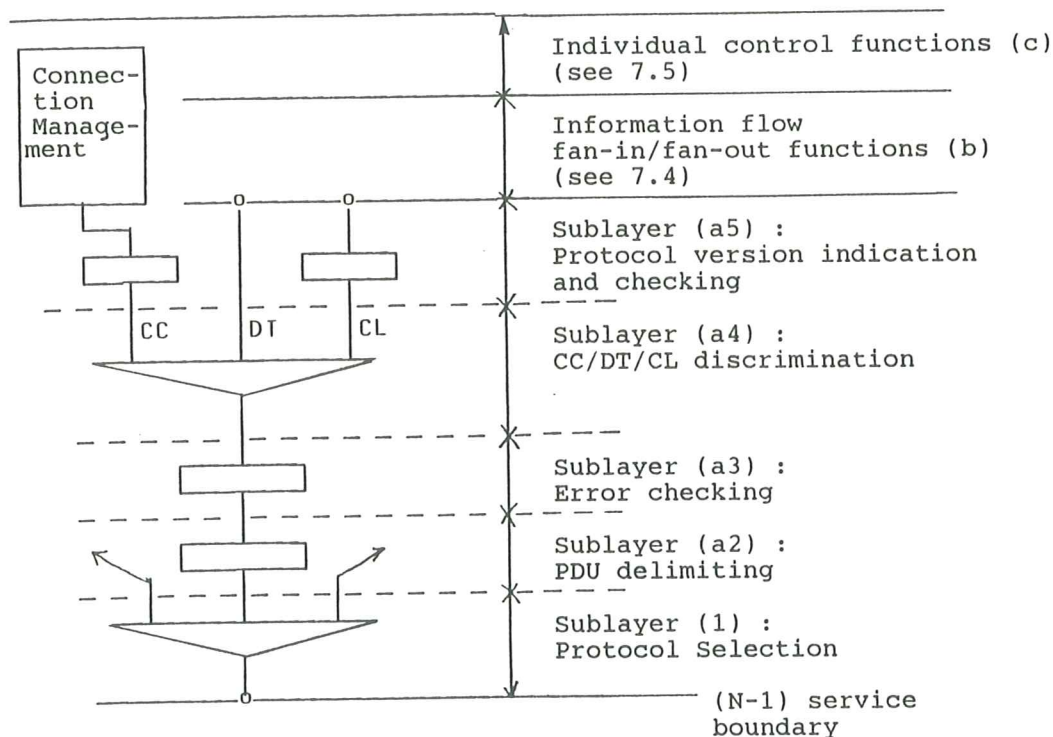
- i) As a mechanism to reconstruct a PDU out of an incoming continuous bitstream. In other words, it occurs if a DBO service is built on top of a CBO service (see Appendix B of this Technical Report). A classic example is the HDLC flag mechanism.
- ii) As a concatenation/separation function. In this 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 function may be dependent on the protocol selector value. This 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.



Legend:

CC : Connection Control PDUs

DT : PDUs supporting data transfer over an existing connection

CL : Connectionless PDUs

Figure 3(a) - Sublayers of the GLA with expanded common control functions

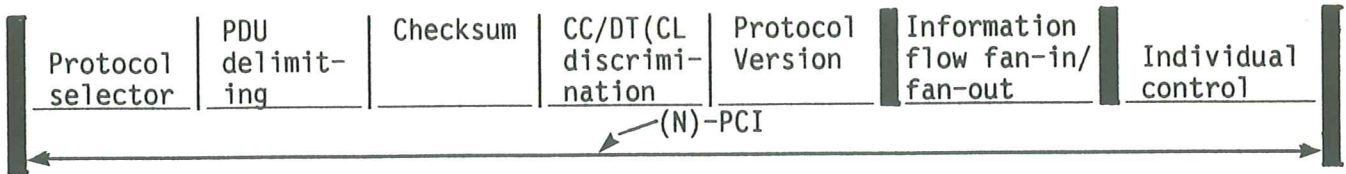


Figure 3(b) - Corresponding Generic Header Format

Note 24

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 25

In the GHF of Figure 3(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 3(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.

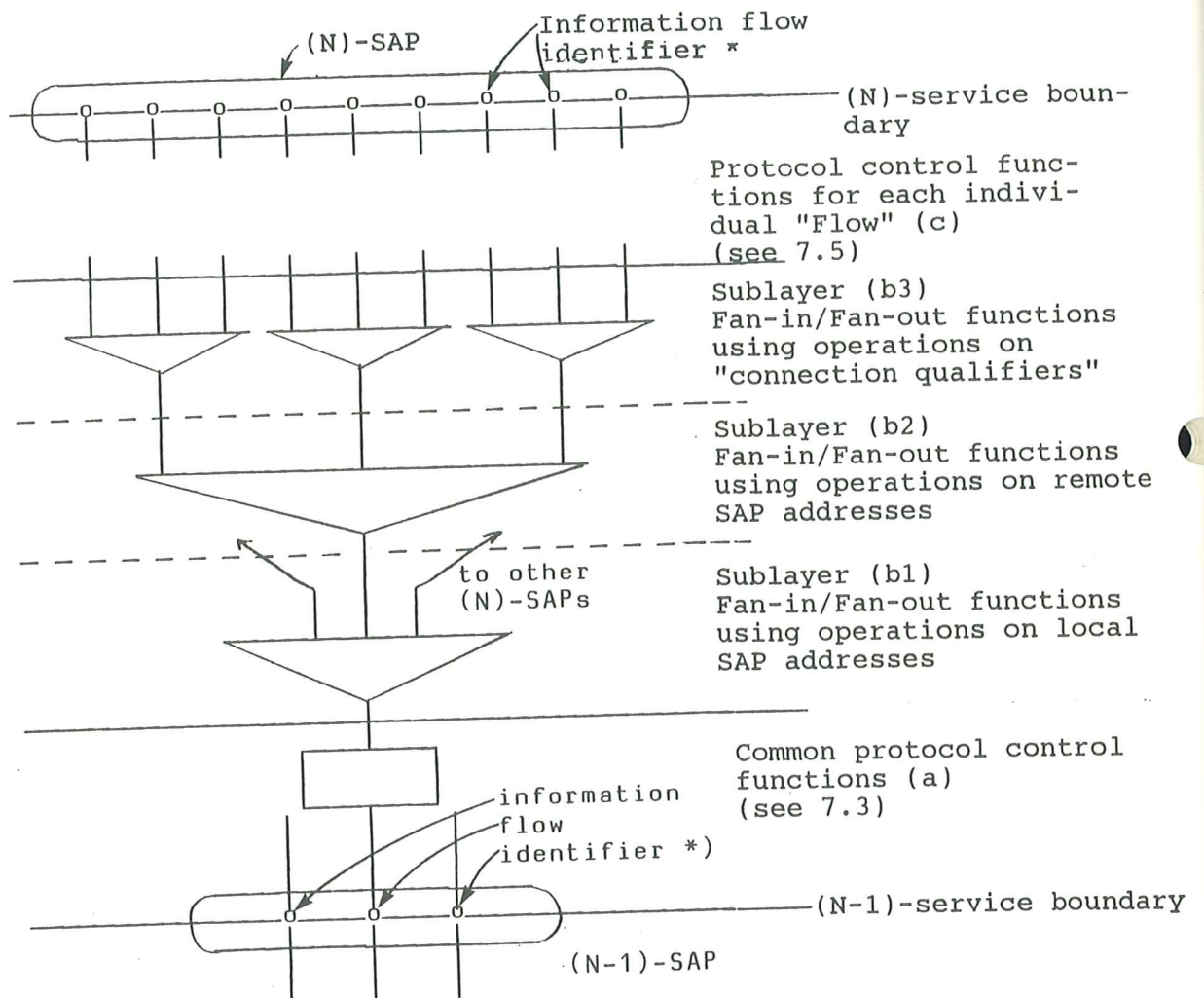
The separation of call control has to be done at this sublayer because the coding of the address fan-in/fan-out fields associated with sublayers b1, b2 and b3 (see 7.4 hereafter) is usually different for call control (CC), CO data transfer (DT), and CL data transfer PDUs (CO data transfer PDUs usually contain reference numbers in the concrete header syntax; see 7.4.3).

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 26

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 4(a) - Sublayers of the GLA with expanded fan-in/fan-out functions

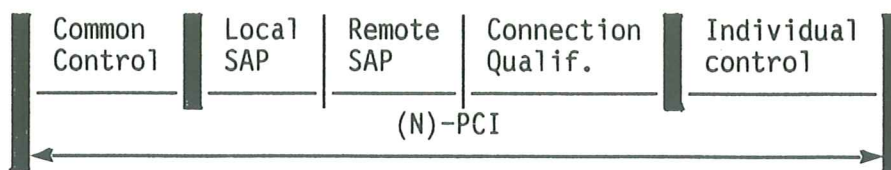


Figure 4(b) - Corresponding Generic Header Format

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

7.4.1 General

Figure 4 gives an expansion of the GLA of Figure 2 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 4 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 7.4.3).

7.4.2 Nesting Rules and the Generic Header Format

In the GHF shown in Figure 4(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 subfields 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.

7.4.3 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.

7.5 Expansion of Individual Connection Control Functions

Figure 5 gives an expansion of the GLA of Figure 2 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.

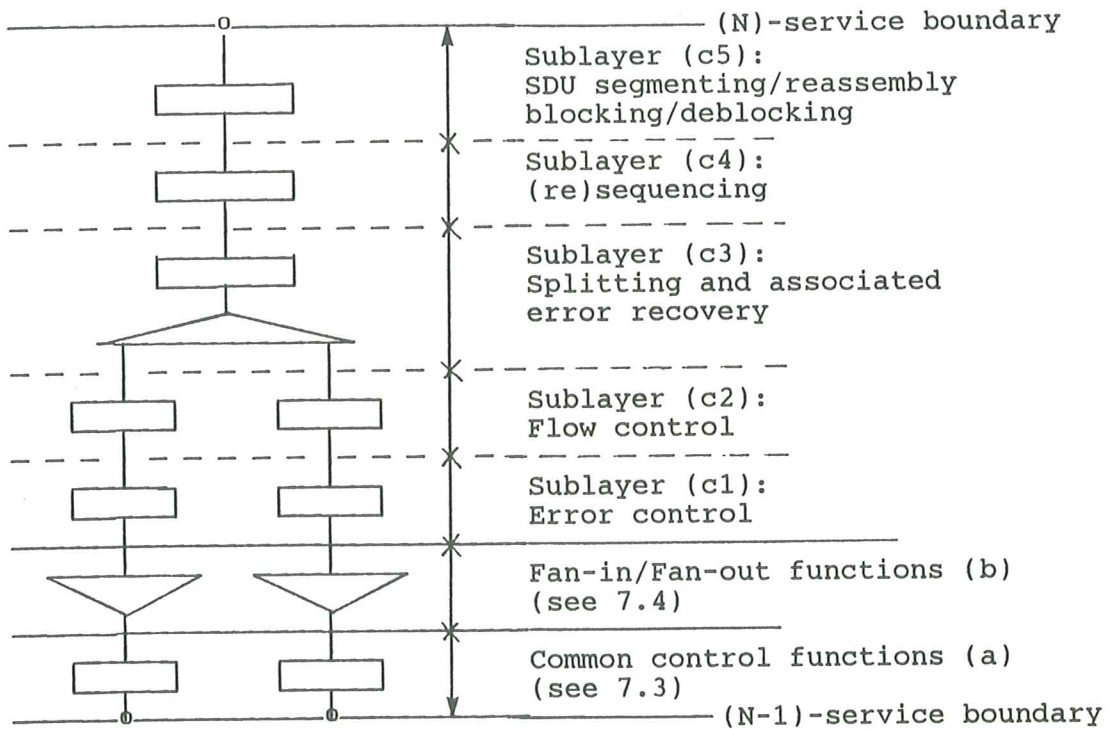


Figure 5(a) - Sublayers of the GLA with expanded individual control functions

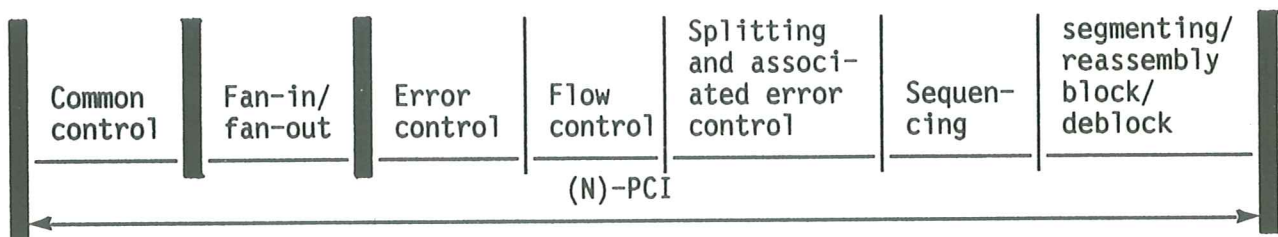


Figure 5(b) - Corresponding Generic Header Format

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 27

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 28

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 7.3).
- 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.

7.6 Hybrid implementations of the GLA

Given the sublayer structure of 7.3, 7.4 and 7.5, 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.

7.7 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 6. 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	0	0	0	0	0
Sequencing	C4	0
Splitting	C3	0
Flow control	C2	.	.	0	0	0
Error control	C1	.	0	.	0	0
Connection qualification	B3	.	.	0	0	0
Remote SAP processing	B2	.	.	0	0	0
Local SAP processing	B1	.	.	0	0	0
Protocol version identification	A5
CC/DT/CL discrimination	A4	0	0	0	0	0
Error detection	A3	0
PDU delimiting	A2	.	0	0	0	0
Protocol identification	A1	0	0	0	0	0

Figure 6 - Application of the GLA to the CO Transport Protocol

8. EXTENSION OF THE GLA MODEL FOR SIGNALLING

8.1 General

We will now introduce extensions to the GLA model (Clause 7), and further develop this to demonstrate the different signalling methods described in 6.2.

Figure 7 shows the GLA model, as it has been developed in Clause 7.

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 8). 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.

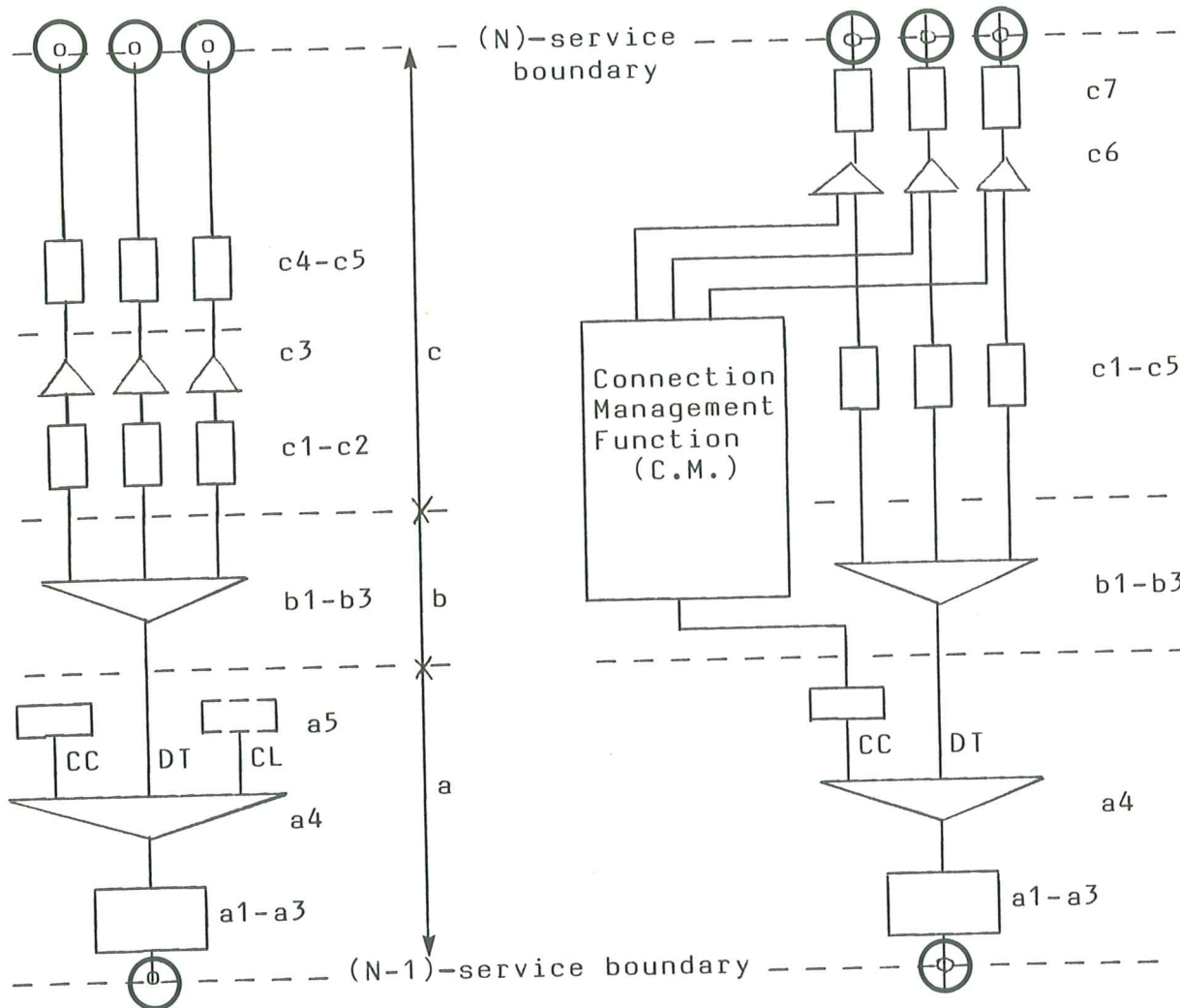


Figure 7 - GLA Model

Figure 8 - Extended GLA Model

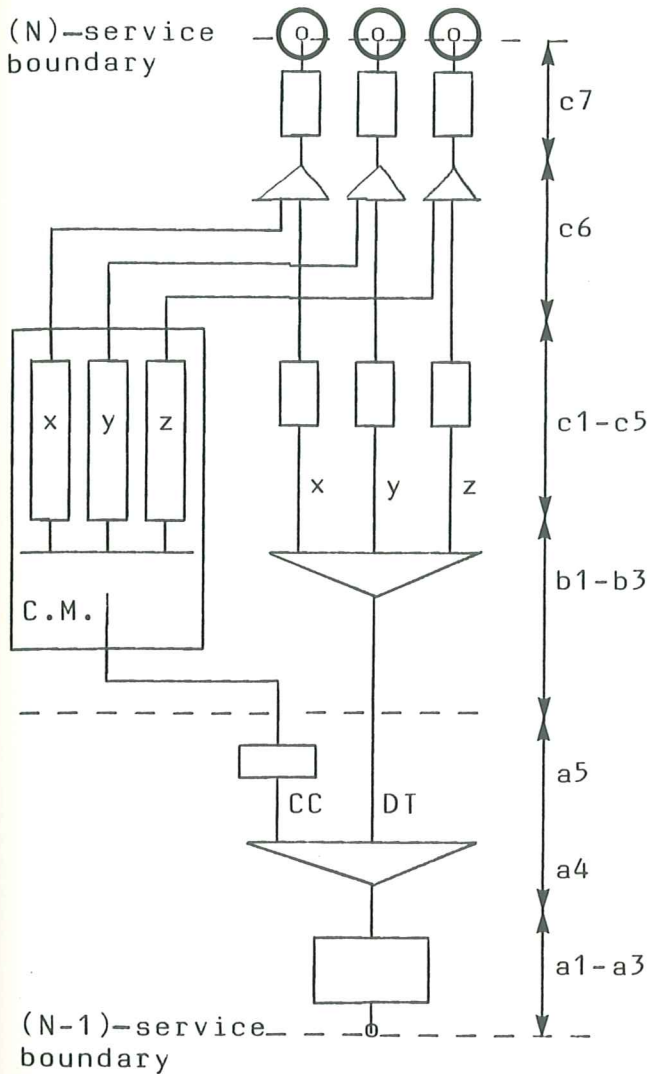


Figure 9 - Example of X.25 application

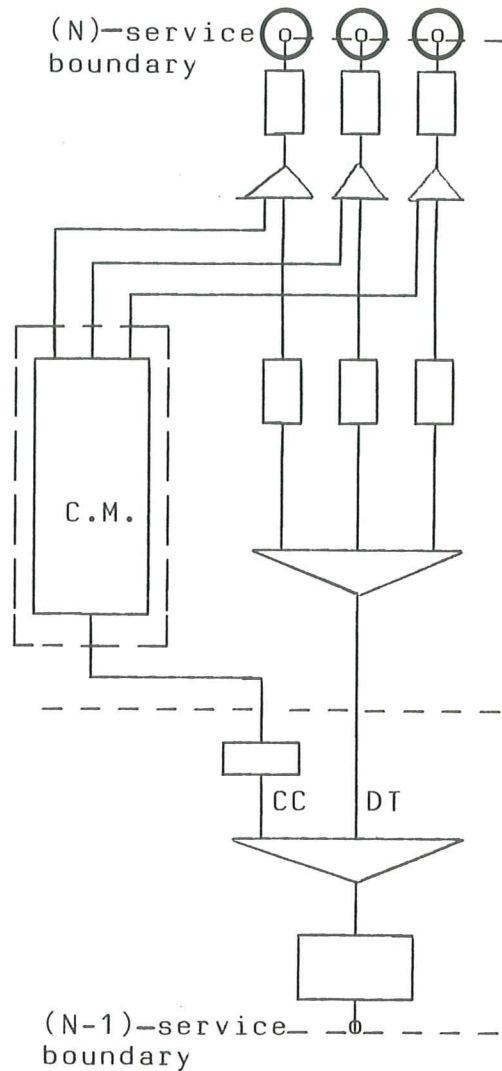


Figure 10 - Example of X.25 with alternate channel assignment

Note 29

There is a large degree of resemblance between a PCEP as here introduced, and a SEP as introduced in Clause 11: 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 9 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 10 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 10 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 11). As in Figure 10, all signalling information is concentrated in a single channel (either a single virtual circuit with LCI=0, as is suggested by Figure 11, 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.

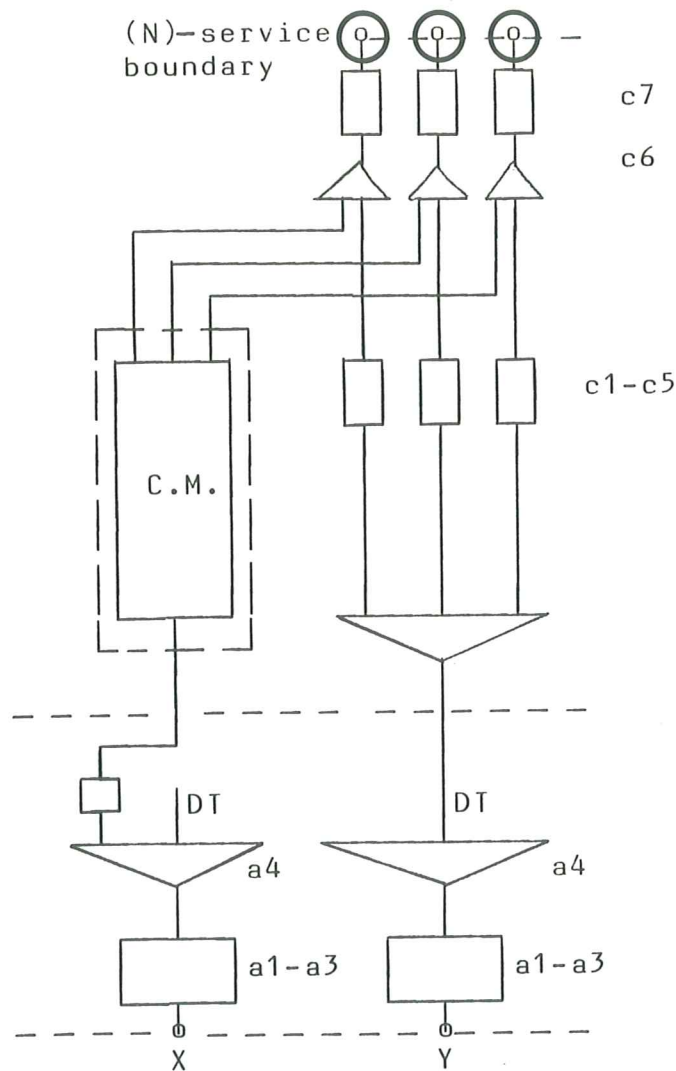


Figure 11 - Example of two instances of X.25 with in-band signalling

It should be noted here that the example of Figure 11 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.

8.2 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 11, 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 12.

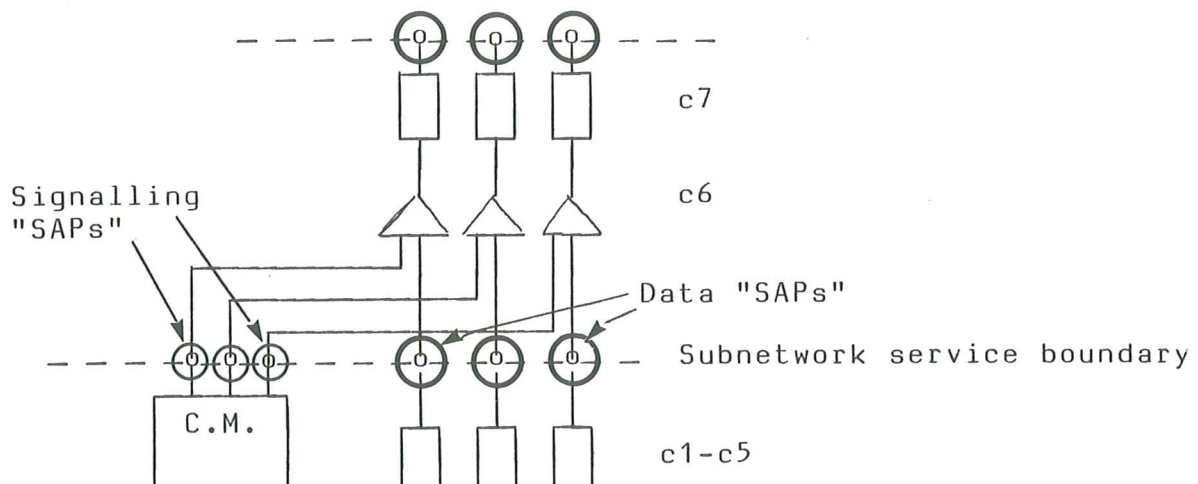


Figure 12 - Subnetwork service definition with independent "SAPs" for signalling and data

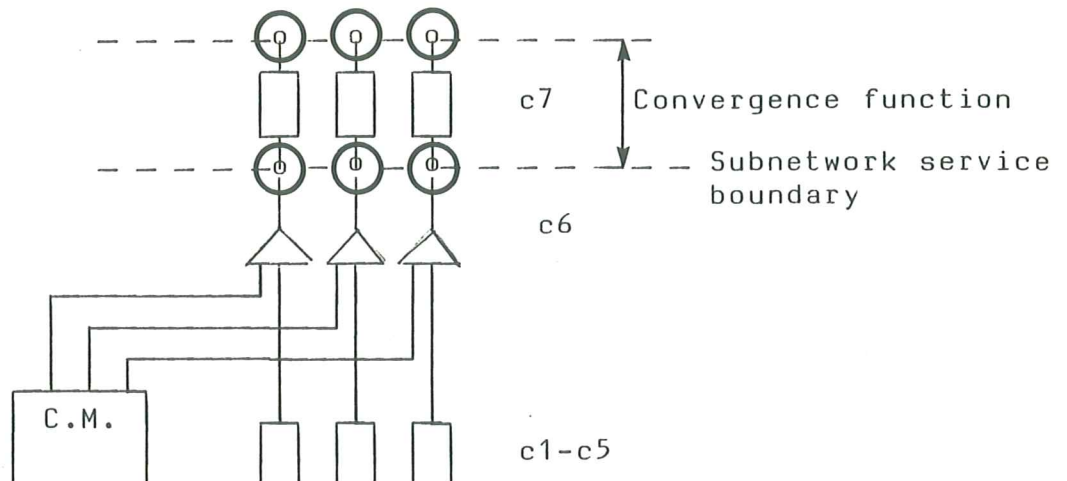


Figure 13 - Preferred representation of subnetwork service with insufficient synchronization

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 13).

8.3 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 12:

- i) According to the GLA (Clause 7), 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 8.1, 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 8.2, this relation may or may not imply synchronization between signalling and user data.

Table 2 shows the symbols used to represent these different cases.

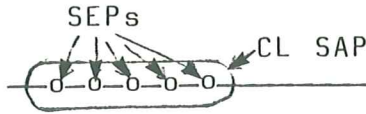
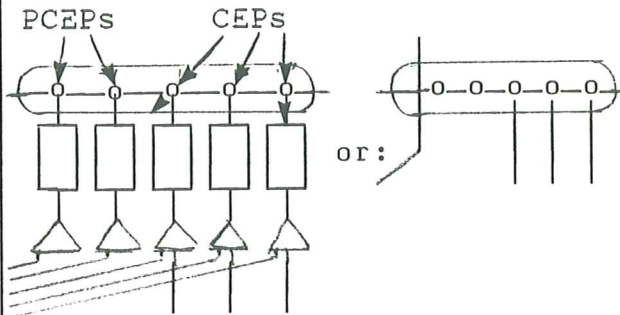
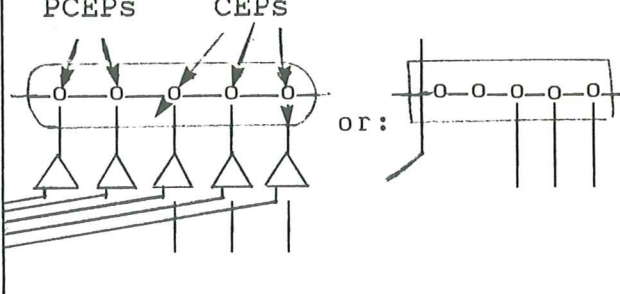
Symbol	Meaning
<p>CL SAP: SAP in a CL service where the identification of the remote SAP is indicated by a SEP within the local SAP.</p>	
<p>Synchronized CO SAP: Two potential CEPs and three established CEPs within one SAP, where the synchronization is guaranteed by the service provider.</p>	
<p>Unsynchronized 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.</p>	

Table 2 - Symbols used in the adopted drawing conventions

8.4 Extended GLA

The results of the discussions of 8.1, 8.2 and 8.3 are summarized in Figures 14, 15 and 16.

Figure 14 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 15 shows how the function group (a) in Figure 14 has to be modified if the signalling flow and the corresponding data flow are each using their own dedicated (N-1)-connections.

Figure 16 shows how the function-group (a) in Figure 14 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 8.1) by the use of the so-called "Lower Layer Management Entity" (LLME).

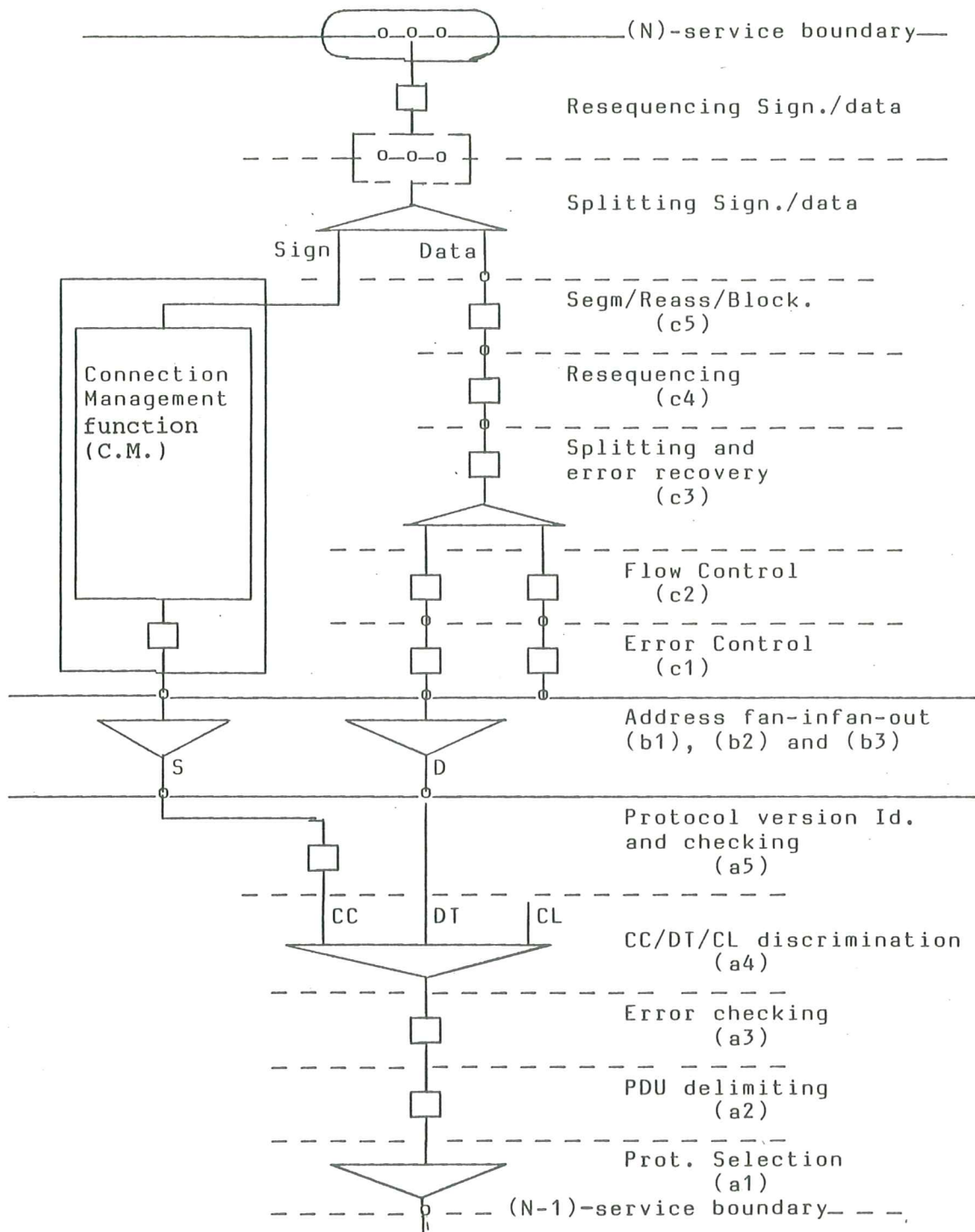


Figure 14 - Extended GLA, in case a common (N-1)-connection is used for signalling and user data

(sublayers c1 to c5 are as in Figure 14)

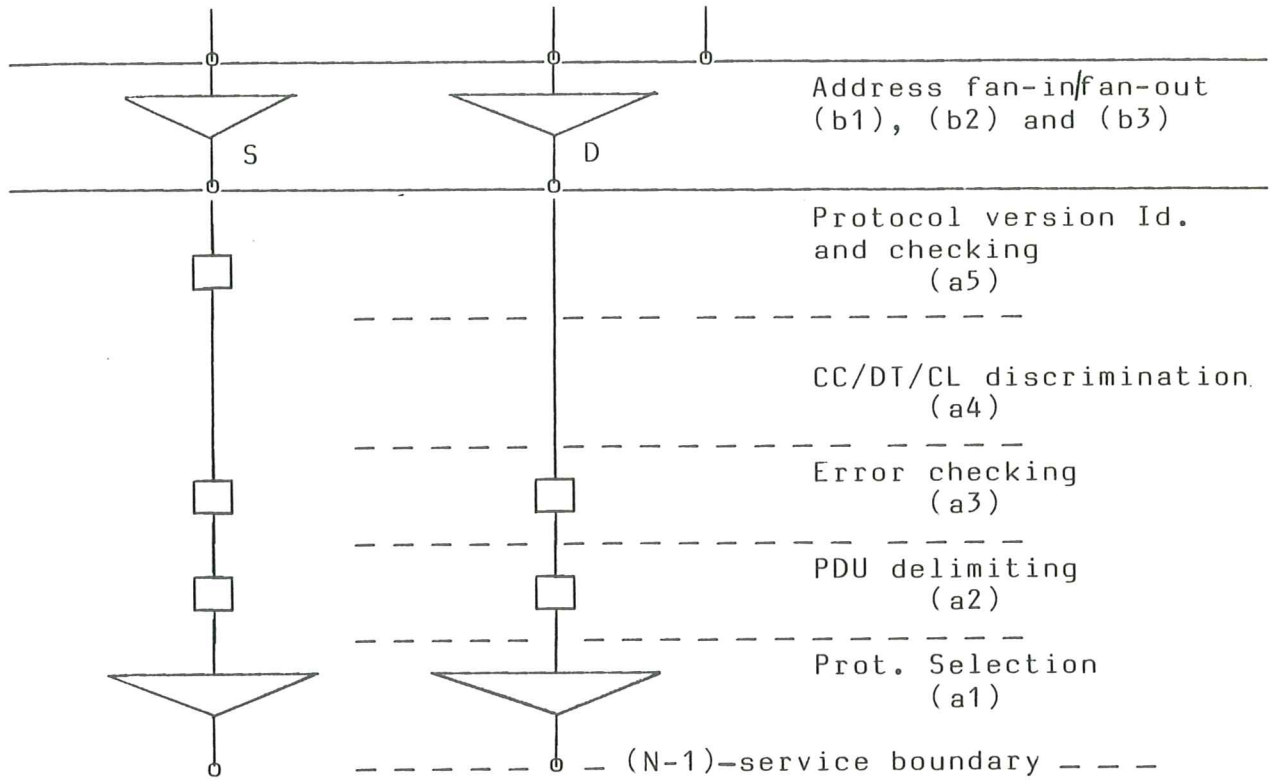


Figure 15 - Extended GLA, in case different (N-1)-connections are used for signalling and user data

(sublayers c1 to c5 are as in Figure 14)

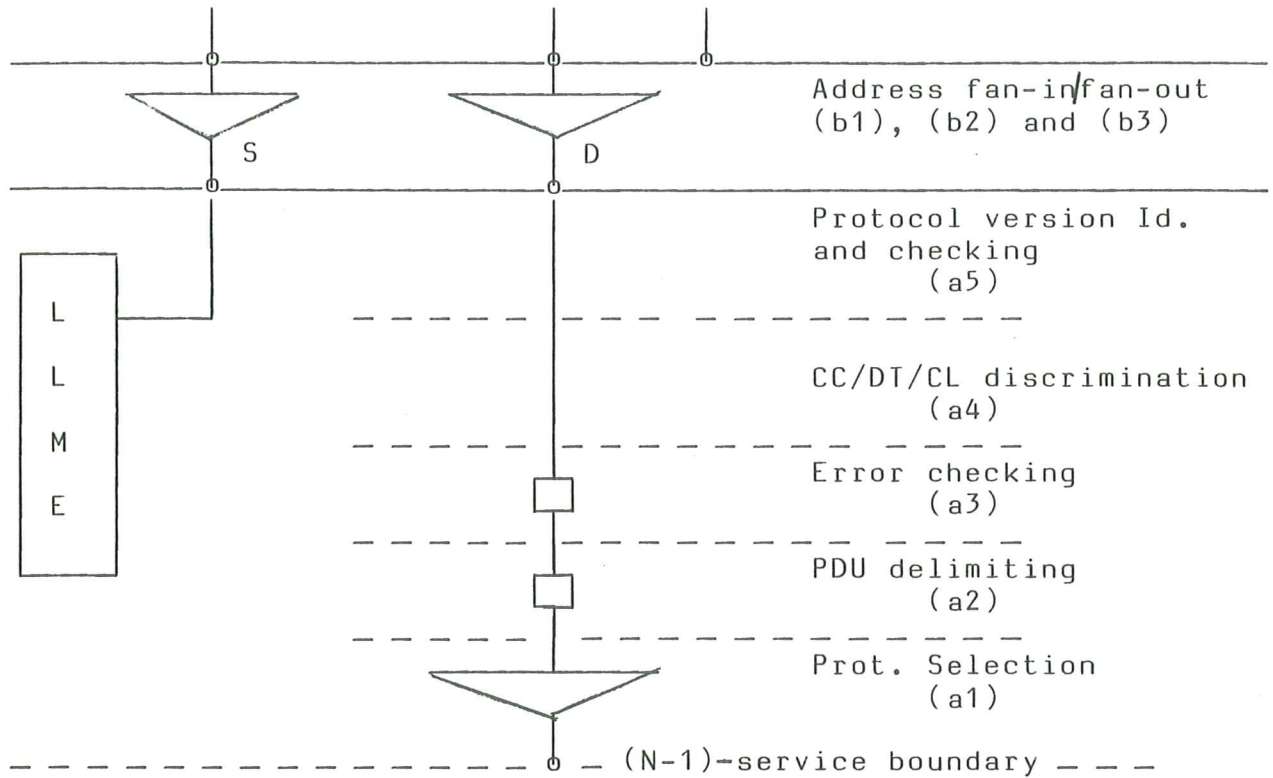


Figure 16 - Extended GLA, in case no (direct) use is made of the (N-1)-service for signalling transfer purposes

SECTION III

GLOBAL NETWORK SERVICE PROVIDER MODELS

9. 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.

10. UNCONSTRAINED NETWORK SERVICE PROVIDER MODEL (UNSPM)

10.1 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 interprotocol 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.

10.2 The subnetwork concept

10.2.1 Architectural observations on intermediate systems (ISs)

Figure 17 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.

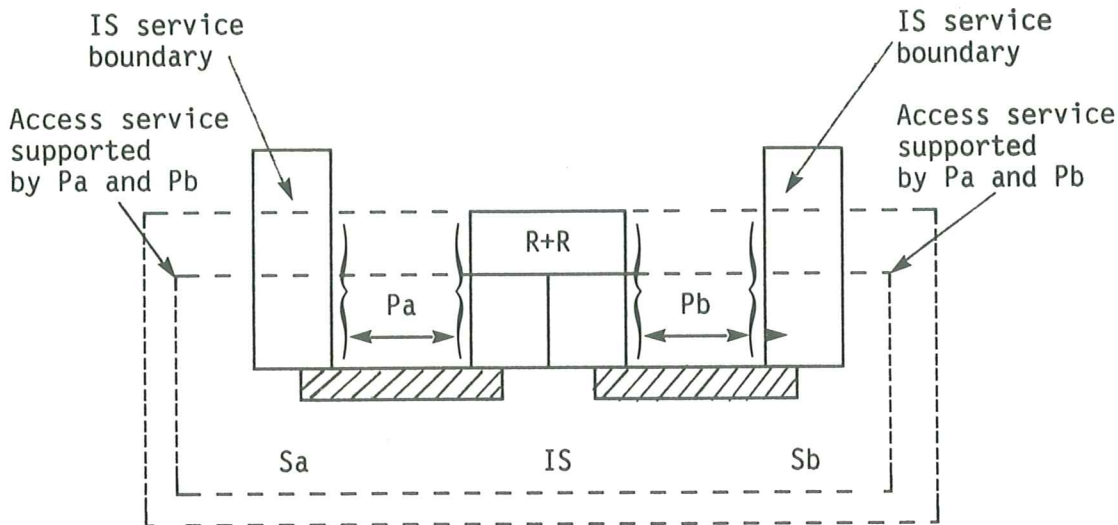


Figure 17 - An IS as service concatenator

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 17, 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" is said to be "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 30

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 17 is that it makes this distinction explicit.

- vi) According to Figure 17, 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 10.3.3 and 10.4.

10.2.2 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 subnetservice 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.

10.2.3 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 18 shows a typical structure of an (N)-PDU, used to access a subnetwork with protocol intervention level (N).

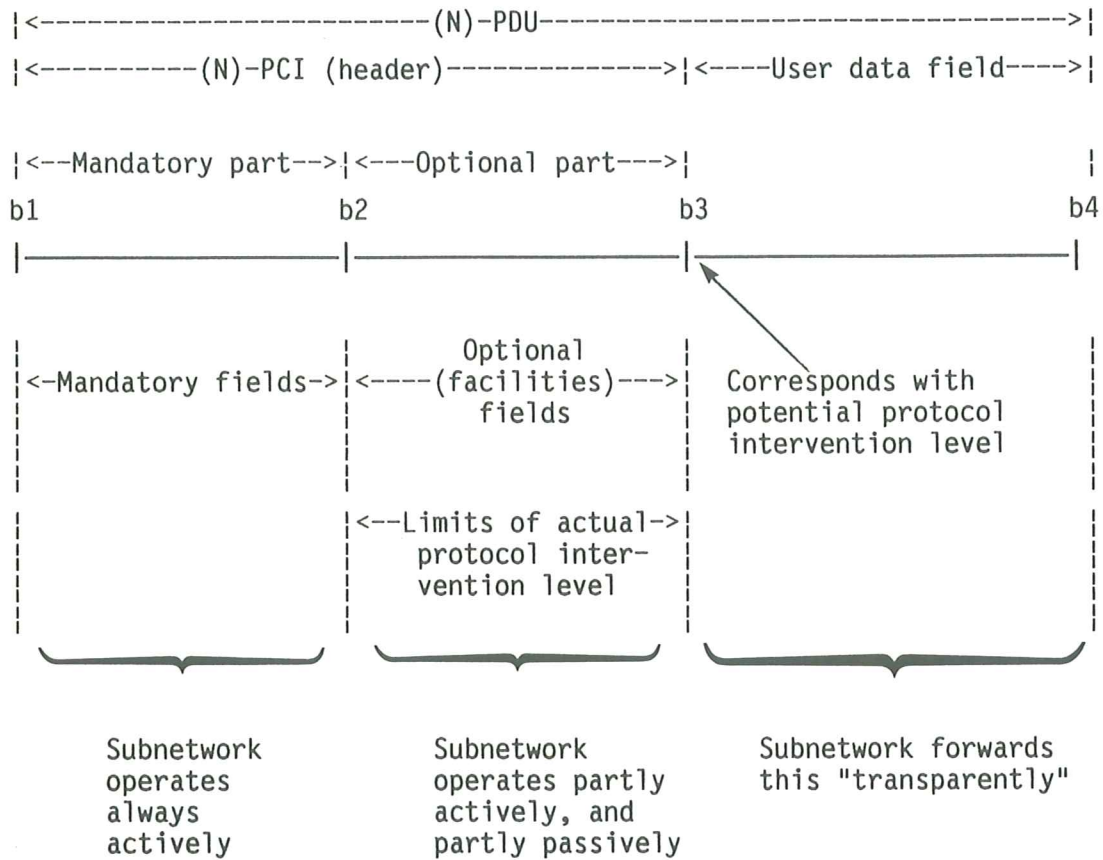


Figure 18 - Relation between protocol intervention level and PDU format

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).

10.3 Subnetwork interconnection principles

10.3.1 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.

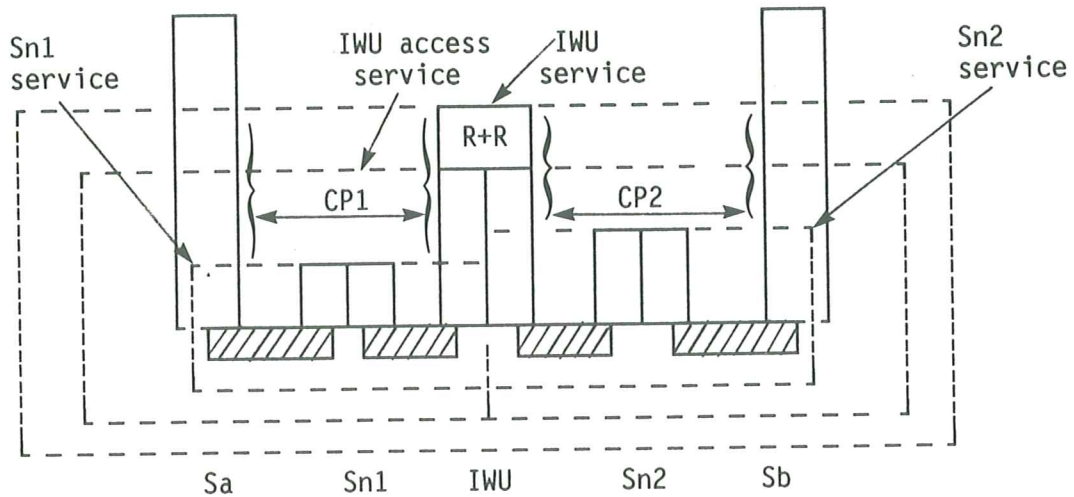
The objective of subnetwork interconnection is usually the wish to increase the number of terminals which can be interconnected. Therefore, subnetwork interconnection has usually direct implications for the applied address conventions. This is further discussed in 10.3.4.

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 10.3.2 and 10.3.3 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."

10.3.2 The IWU as service concatenator

Figure 19 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 19 - 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 19; its protocol intervention level is higher, and it supports a service which differs from that of Sn1.

According to the observations made in 10.2.1, 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 10.2 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 19 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 10.2.1 for all intermediate systems).

These boundaries are indicated in Figure 19 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.

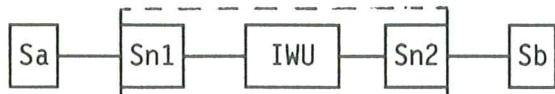
The use of convergence protocols is not always needed. This is further discussed in 10.3.3 below.

10.3.3 The significance of the protocol intervention level of the IWU

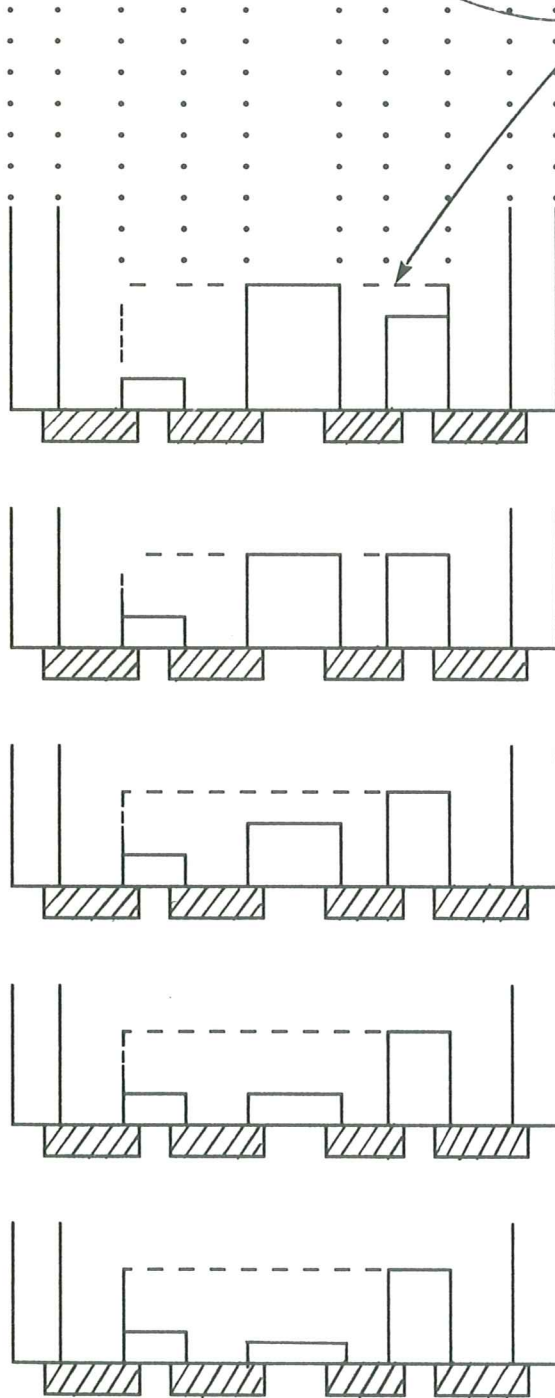
Although it is true that an IWU always creates a service on the basis of which the subnetworks are interconnected, this service does not always need to affect the systems attached to both subnetworks and does not always need to be supported by convergence protocols over the attached subnetworks.

In order to illustrate this, five typical possible protocol intervention levels for the IWU are shown in Figure 20 (the R+R functionalities are not explicitly shown).

System Subnet IWU Subnet System



composite subnetwork



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 20 - 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 20 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 10.2.1 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 10.3.1 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.

10.3.4 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 !

10.4 Relaying as service mapping versus relaying as protocol mapping

In 10.2 and 10.3, 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 ingoing 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.

10.5 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 10.6, 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 21)

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 22)

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.

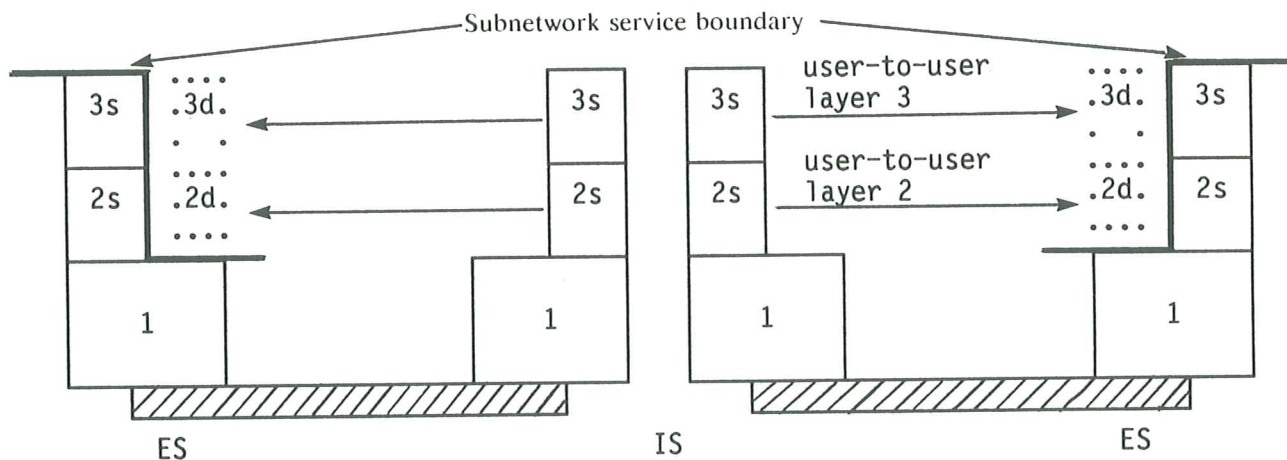


Figure 21 - "Staircase" subnetwork service boundary (alternative 1)

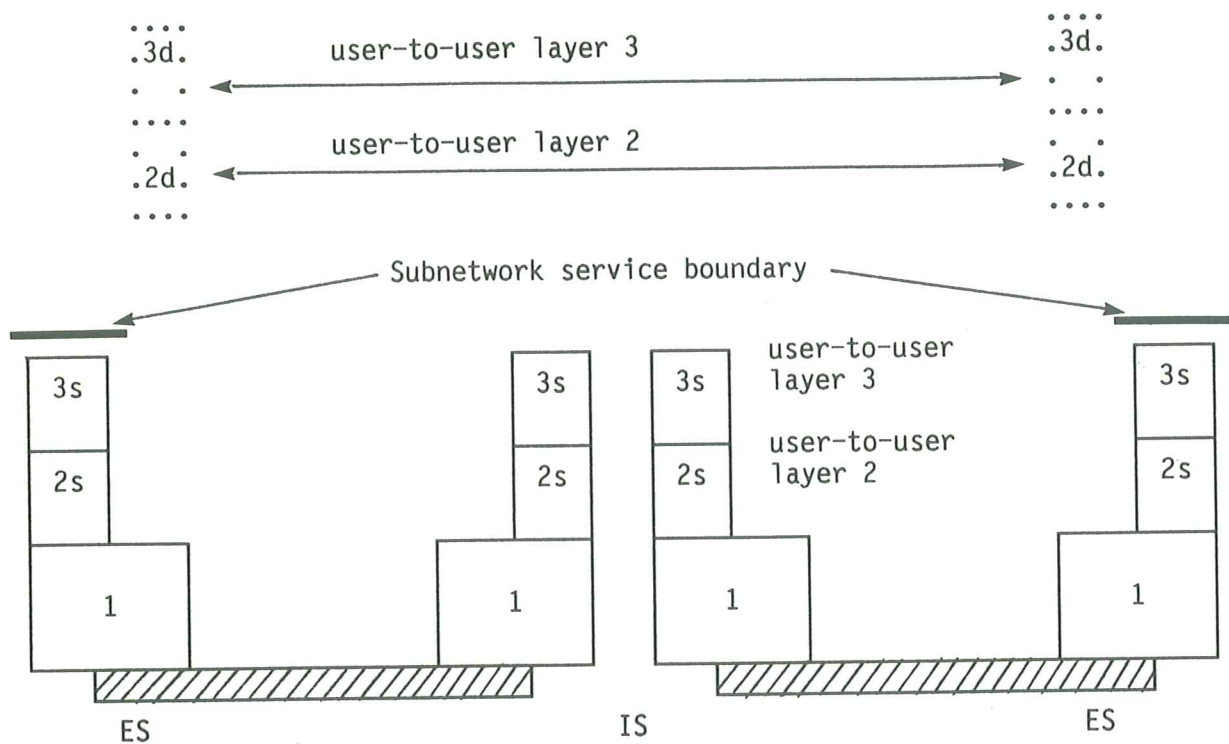


Figure 22 - "Flat" subnetwork service boundary (alternative 2)

Legend for Figures 21 and 22

- 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.

10.6 The resulting model

10.6.1 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 10.6.2 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.

10.6.2 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.

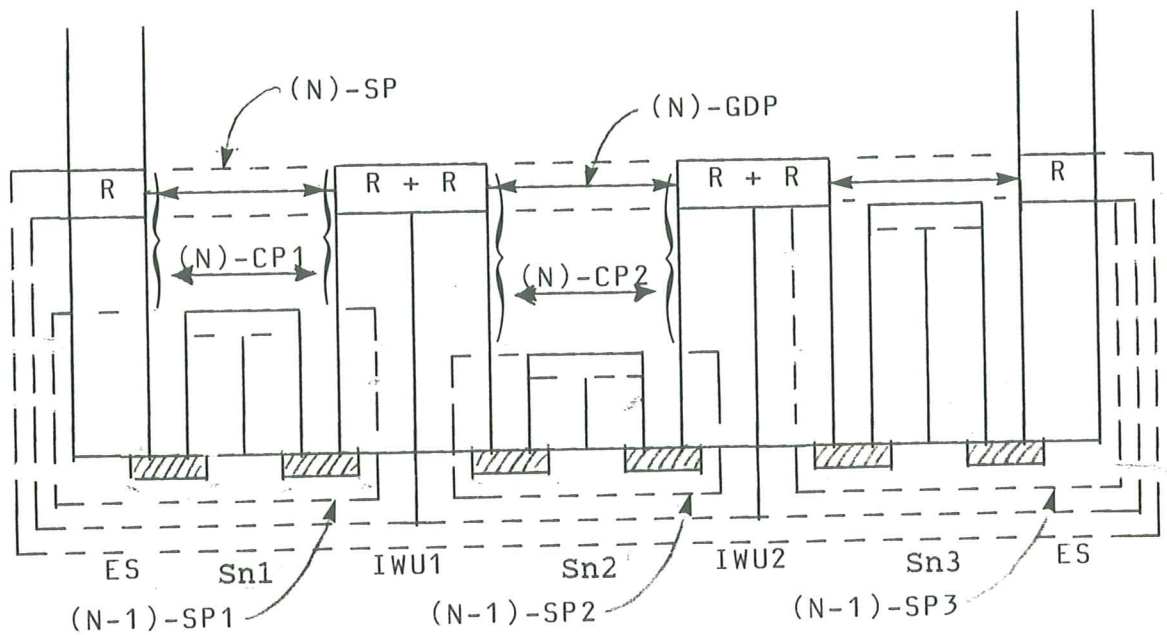
Figure 23 shows one step in this decomposition process. (N)-SP represents a certain (N)-layer subnetwork service provider. All ISs which have the same protocol, relaying and routing intervention level as that of the (N)-SP are considered as IWUs. These IWUs contain R+R functions that operate on parameters 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 23 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 23 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 23 this situation holds for the subnetworks Sn1 and Sn2. The convergence protocols are denoted as (N)-CP1 and (N)-CP2 respectively.

Figure 23 has a resemblance to Figure 19. The main difference between these figures is that Figure 23 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 23 - The subnetwork service provider model

10.6.3 Implications for end systems

Figure 24 shows two end systems, interconnected via six subnetworks with different intervention levels. If the decomposition step described in 10.6.2 is applied four successive times, then four subnetwork service boundaries are created in ES_a , and one is created in ES_b . Indeed, as already said in 10.2.1, 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 24 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 20).

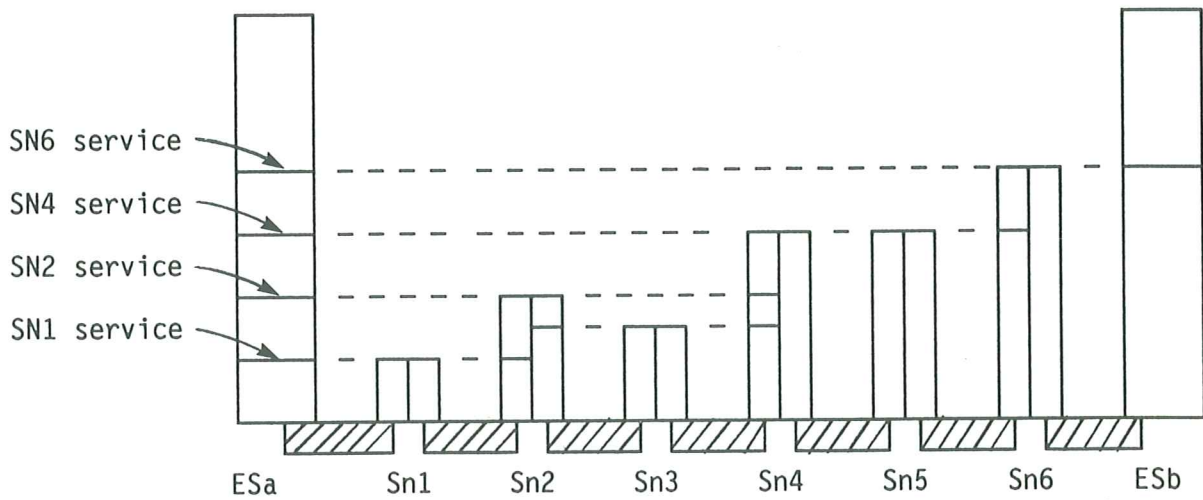


Figure 24 - The Unconstrained Network Service Provider Model (UNSPM)

10.6.4 Relation to the OSI NS

In 10.6.3 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 24). 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 25 shows how Figure 24 has to be enhanced to cover this situation.

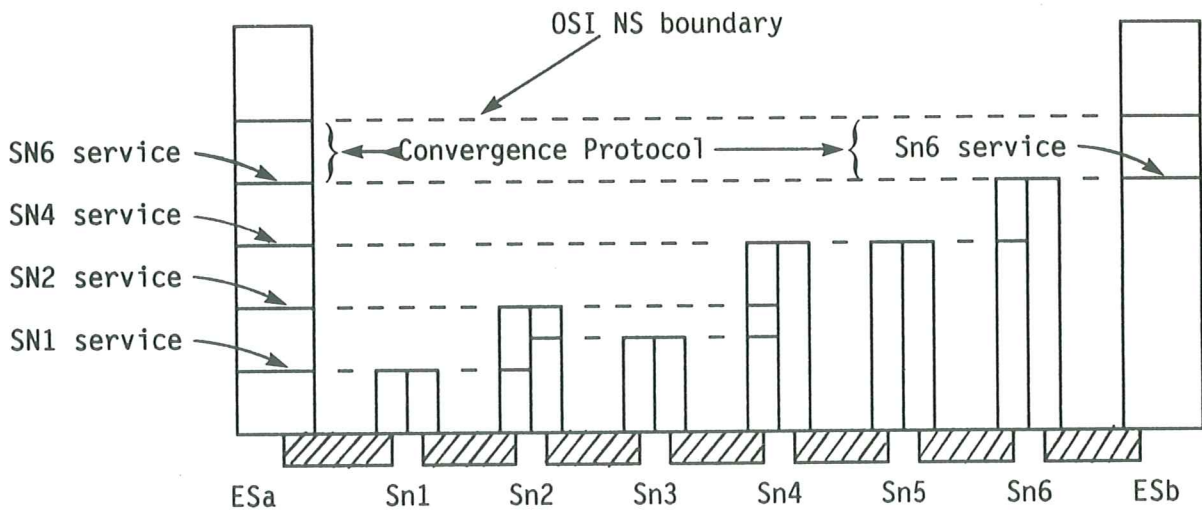


Figure 25 - The Unconstrained Network Service Provider Model (UNSPM) in the case where the OSI NS needs to be supported

11. CONSTRAINED NETWORK SERVICE PROVIDER MODEL (CNSPM)

11.1 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.

Note 31

A discussion of the abstract syntax of a Network Layer Address in terms of lower layer addressing domains identified in the CNSPM can be found in Appendix C.

11.2 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 26(a). The corresponding Generic Header Format is illustrated in Figure 26(b).

Note 22

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

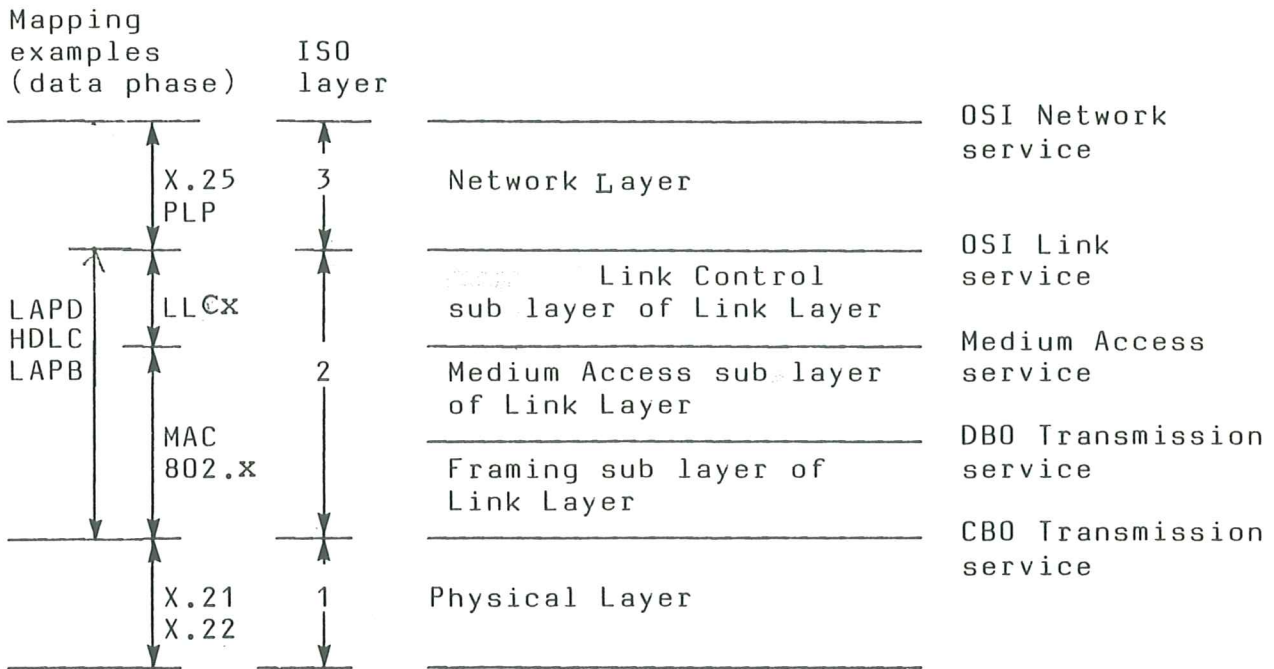


Figure 26(a) - Basic Network Layer Service Provider Model

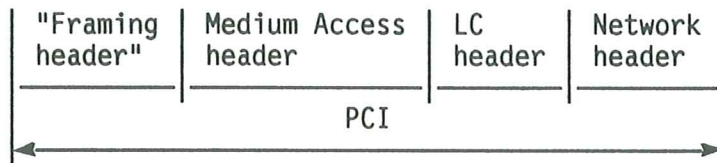


Figure 26(b) - Corresponding Generic Header Format

11.3 Refinement of the Basic CNSPM

Refinement of the Basic CNSPM is performed below by developing a Generic (N)-layer Service Provider Model based on the principles of ISO 8648 with regard to the Network Layer. This generic model is then applied to each of the layers of the Basic CNSPM (Figure 26) to which it is seen as being theoretically applicable.

11.3.1 Interpretation of ISO 8648

The following identifies and gives the substance of the clauses of ISO 8648 relevant to the construction of the Generic (N)-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 rôle of a protocol is the definition of both the agreed service to be provided by the protocol and the service assumed to underly 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 rôle;
- 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 generalized Network Service Provider 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 27.

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.

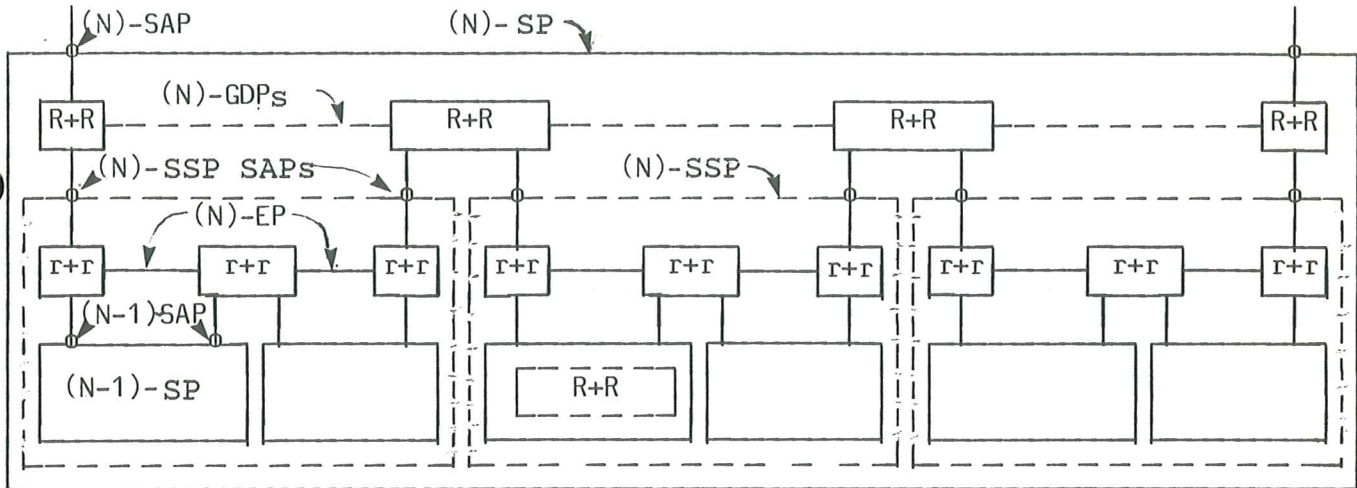
Apart from relaying and routing, the $r+r$ functionality performs the (N)-EP protocol operation which raises the (N-1)-service up to the (N)-service. The $r+r$ functionality is however not capable of interpreting and operating on parameters which are significant for the whole (N)-service address space.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



Legend

- (N)-SP : (N)-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 + GDP carrier
- N : 3

Figure 27(a) - Generic (N)-Layer Service Provider Model

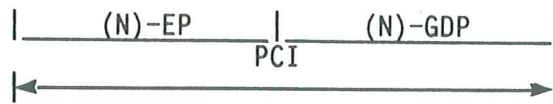


Figure 27(b) - Corresponding Generic Header Format

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 32

The R+R functionality in Figure 27(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 27(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 27(b) shows the corresponding Generic Header Format (see 6.1).

Further refinement of this format is given in Clause 7.

11.3.2 Application of the principle of recursion

The generic (N)-layer model of Figure 27 is seen as being applicable in theory to the Medium Access, Link and Network Layers of the basic multi-layer model of Figure 26.

For each of these layers protocols have been defined making provision for the transfer of addressing information.

No barrier exists in principle to the structuring of this information to facilitate routing both within a subnetwork and between subnetworks as for the Network Layer.

Given application of the model of Figure 27 to the upper three layers of the model of Figure 26, the refined multi-layer architecture emerges as illustrated in Figure 28.

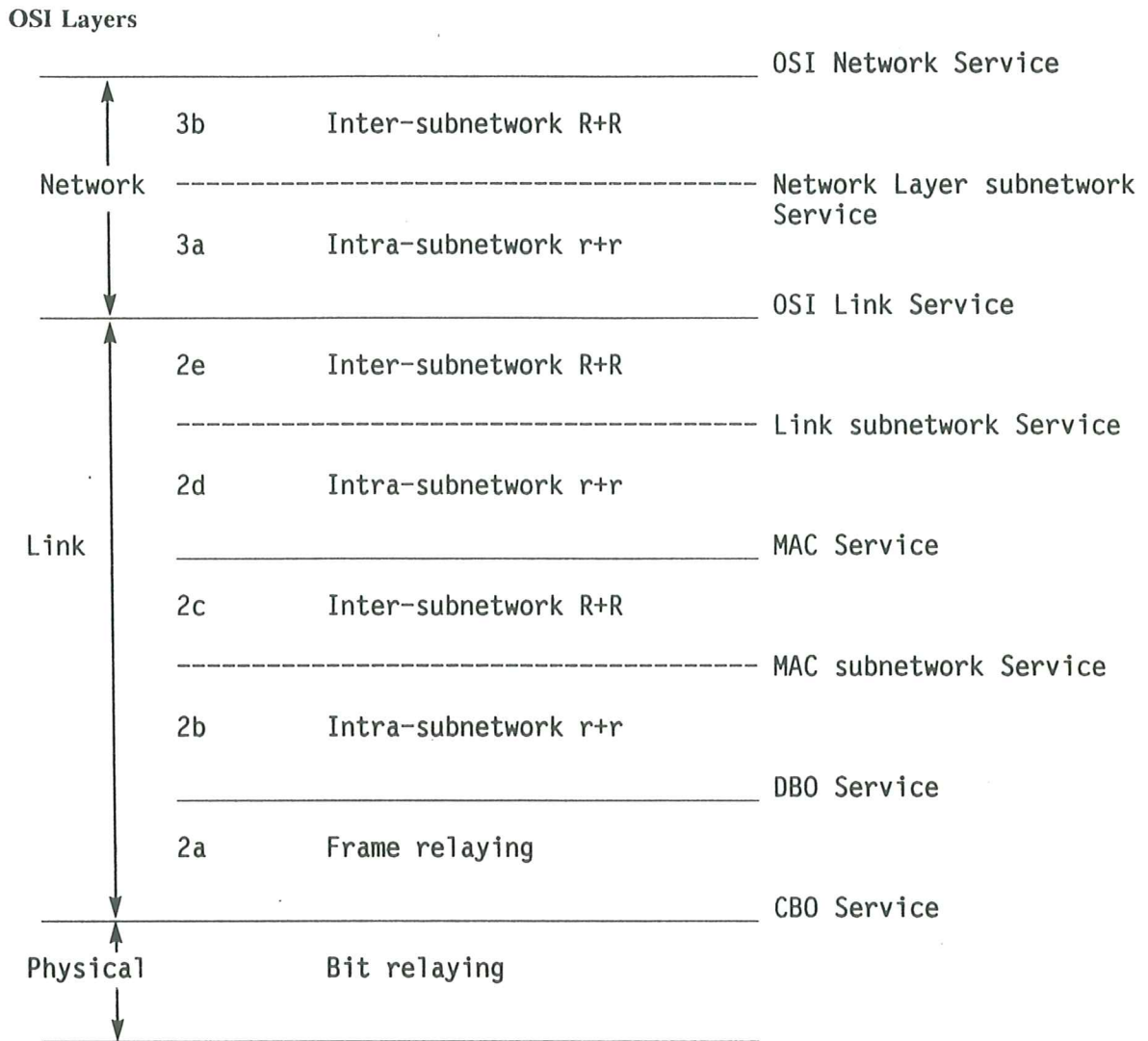


Figure 28 - Refined multi-layer architecture

11.3.3 Reduction of refined multi-layer architecture

The multi-layer architecture of Figure 28 permits a total of eight different kinds of IS, six 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. These 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.

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

We note that the lowest service boundary in Figure 28 at which the concept of a connection becomes meaningful is the Link subnetwork service boundary (2d). 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 29 gives an interpretation of Figure 28 reflecting this choice of common datum and shows the functions of the various sublayers for various kinds of CL and CO technologies.

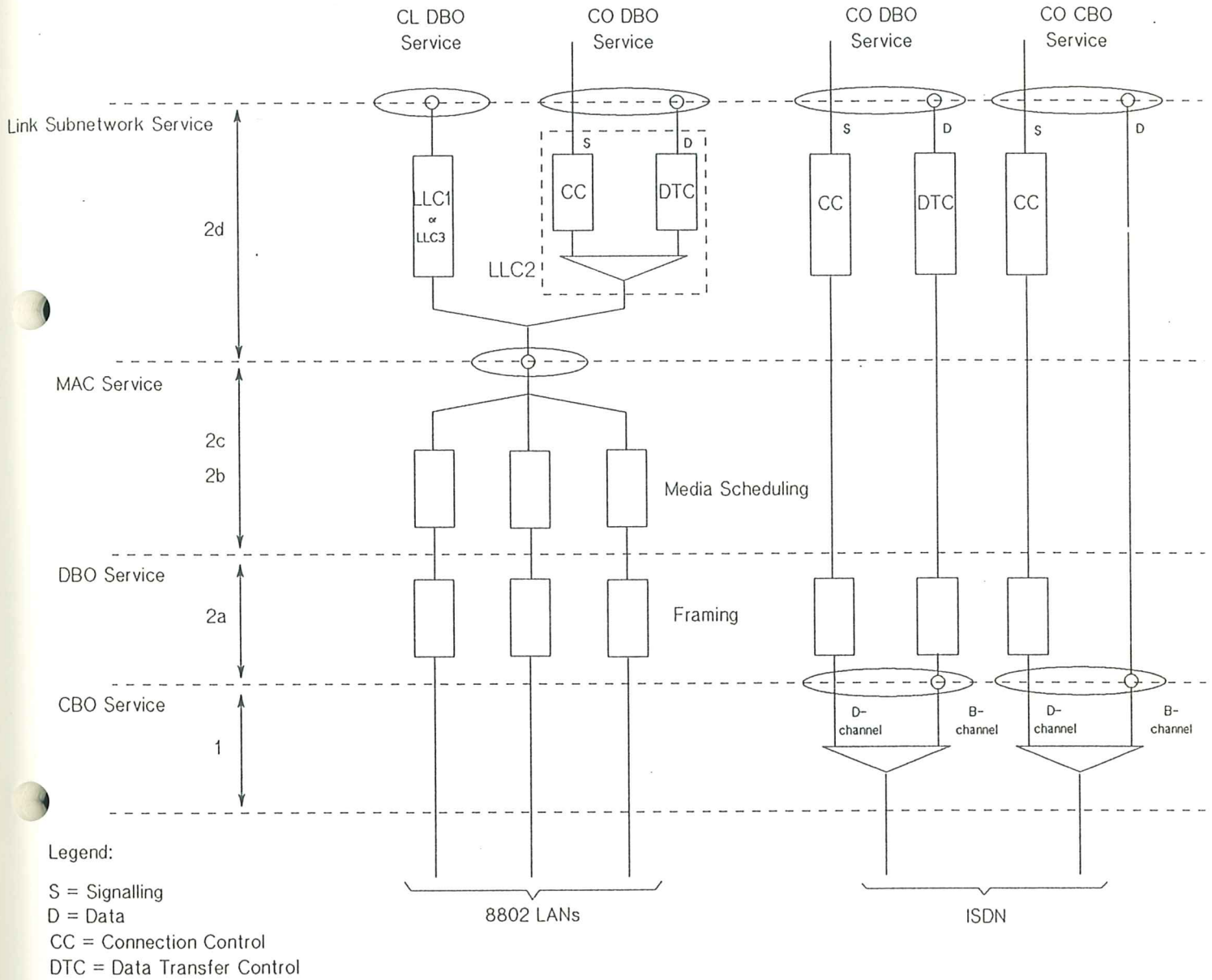
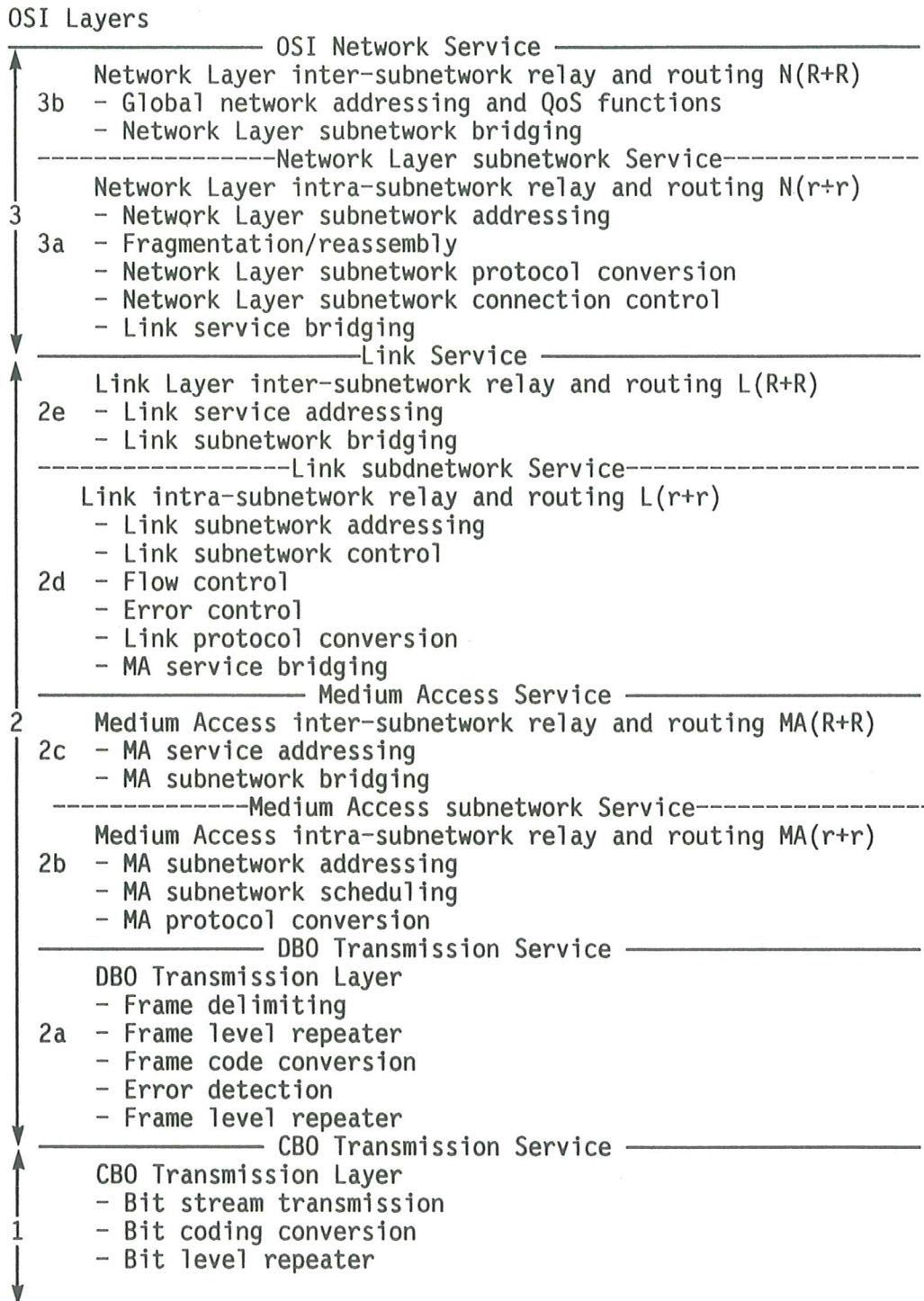


Figure 29 - Interpretation of multi-layer model for different technologies

11.3.5 Expansion of functions of multi-layer model

Figure 30 gives an expansion of functions of the model of Figure 28 in accordance with the considerations of 11.3.3 and 11.3.4.



The corresponding Generic Header Format corresponds with that shown in Figure 26(b)

Figure 30 - Expansion of functions of the refined multi-layer architecture

11.4 Subsettings of the CNSPM

Figure 31 shows a number of subsetting possibilities, each corresponding with a certain specific subnetwork service.

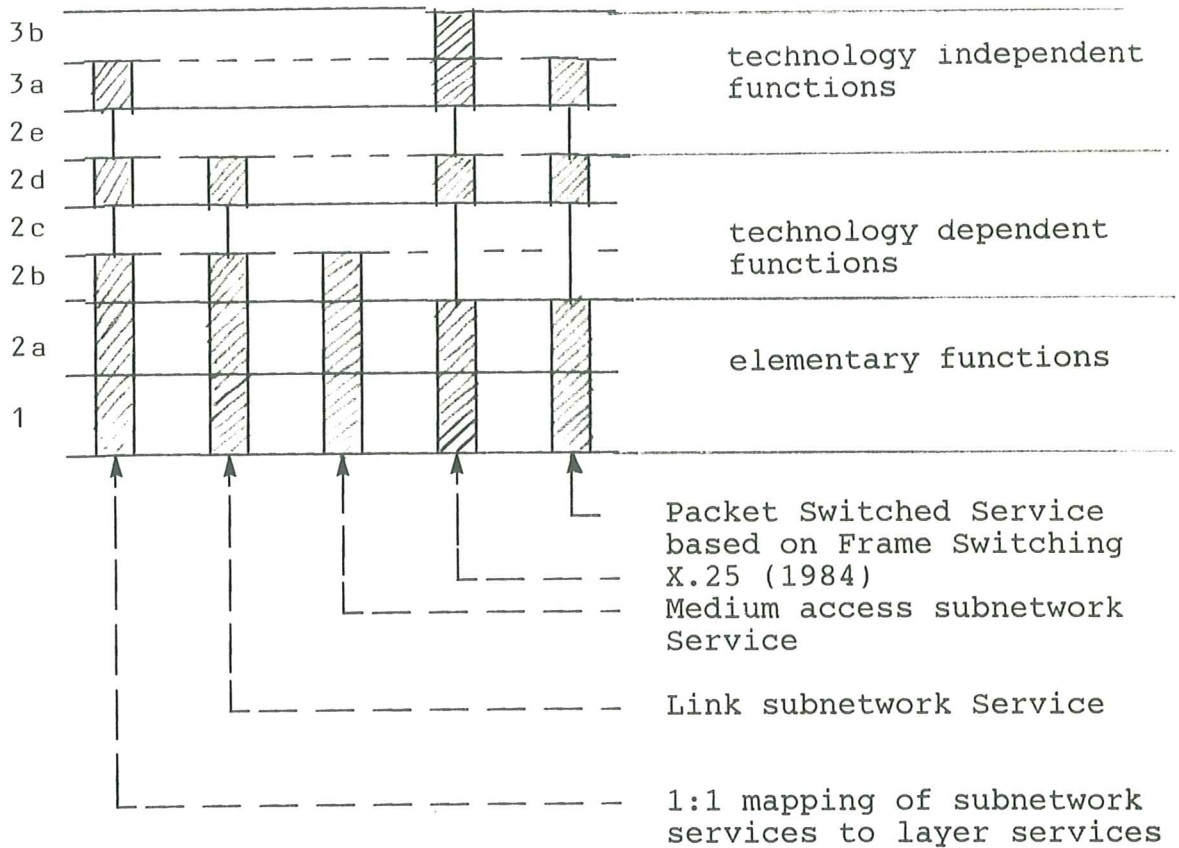


Figure 31 - Some subsetting possibilities

SECTION IV

EXAMPLES

12. 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.

12.1 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 11). See also 8.3 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 33

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.

12.2 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^{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 34

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).

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

The UNSPM is given in Figure 32.

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 3.

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.

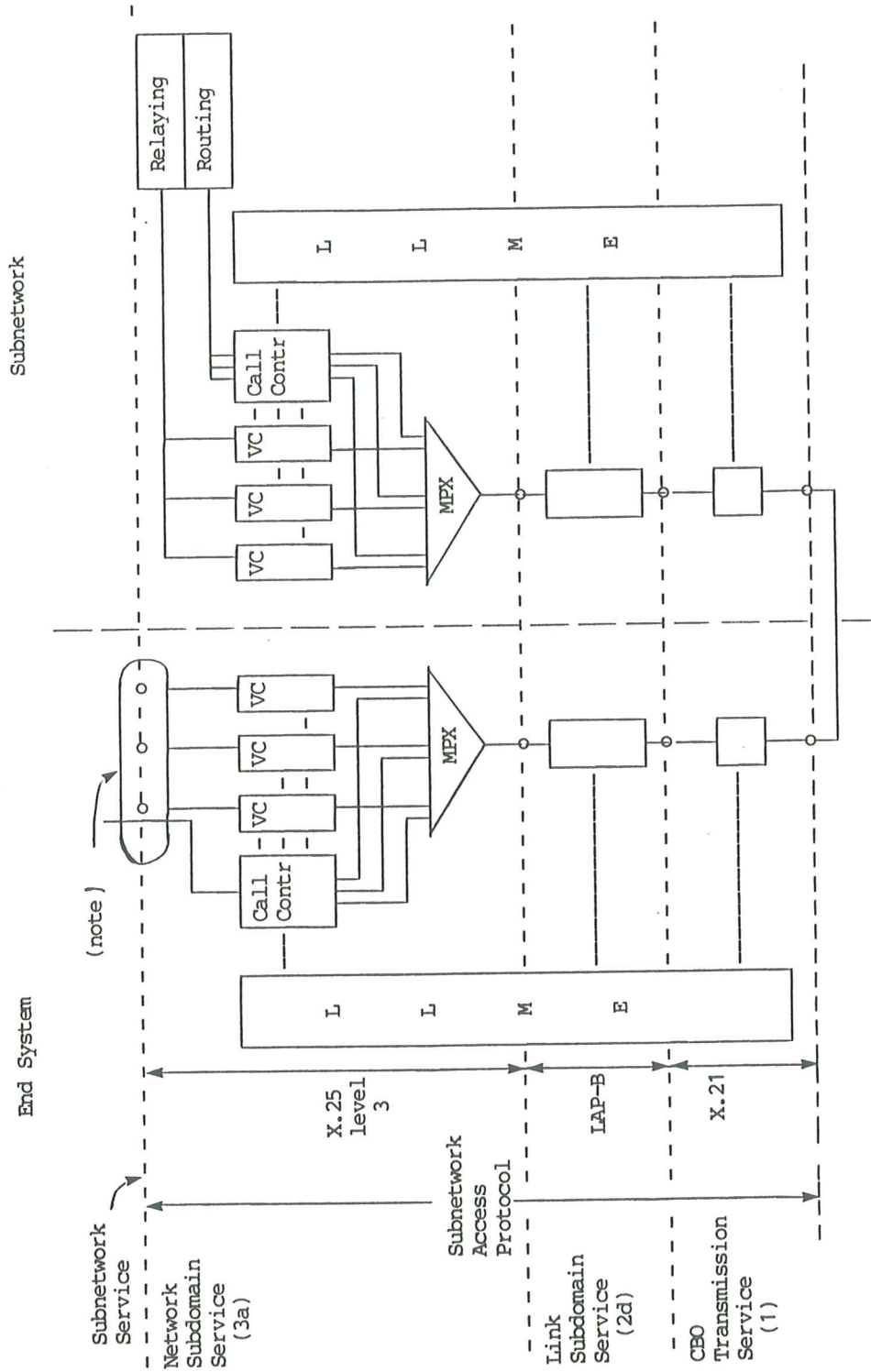
The data service belonging to X.25 (1984) has all the attributes of U, the subnetwork service is global, and supports transfer of NSAP addresses, although potentially NSAP addresses could even be operated on. The classification of X.25 (1984) is therefore PSS = (D,S3), ASS = (C,S3).

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).

This also means that X.25 (1980) should be seen as a Link Subdomain Service, whilst X.25 (1984) should be seen as a Network Subdomain Service according to the CNSPM.



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 passively.

Figure 32 - X.25 (1984)

GLA application:

Sublayer		LAPB	Layer 3	Combined
Segmenting/reassembly	C5	.	0	0
Sequencing	C4	.	.	.
Splitting	C3	0 (a)	.	X (a)
Flow control	C2	0	0	0
Error control	C1	0	.	X
Connection qualification	B3	.	0	0
Remote SAP processing	B2	.	0	0
Local SAP processing	B1	.	0 (b)	0 (b)
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	0	0	0
Error detection	A3	0	.	0
PDU delimiting	A2	0	.	0
Protocol identification	A1	.	0	. (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 3 - X.25 (1984)

12.4 X.21 and X.22

The UNSPM is given in Figure 33. 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 4.

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.

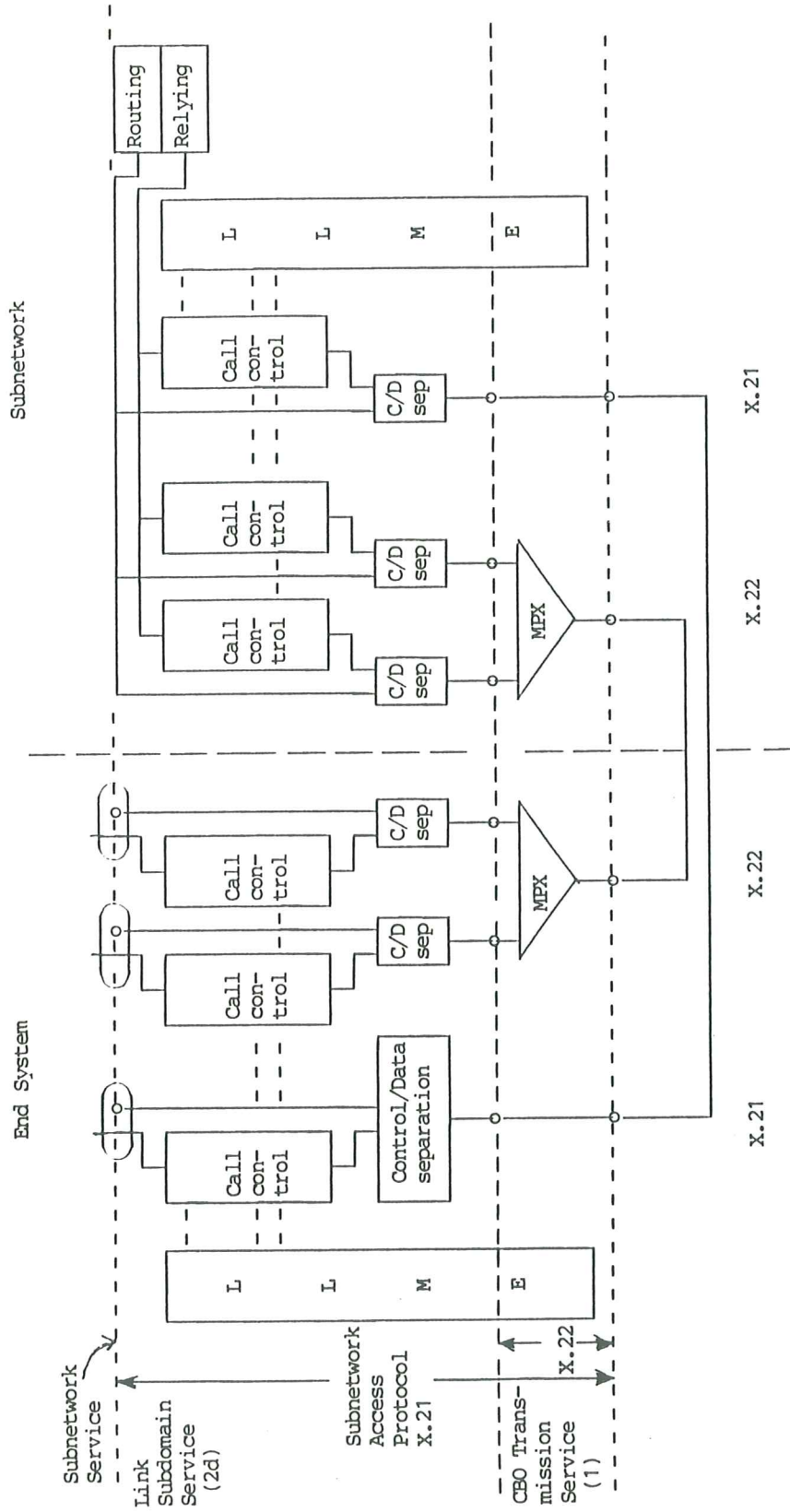


Figure 33 - X.21 and X.22

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	0
Local SAP processing	B1	.
Protocol version identification	A5	.
CC/DT/CL discrimination	A4	0
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 4 - X.21 and X.22

12.5 8802.x LAN and Bridged LAN

The UNSPM is given in Figure 34.

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 5.

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 losing 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 $PSS = ASS = (B,Q)$.

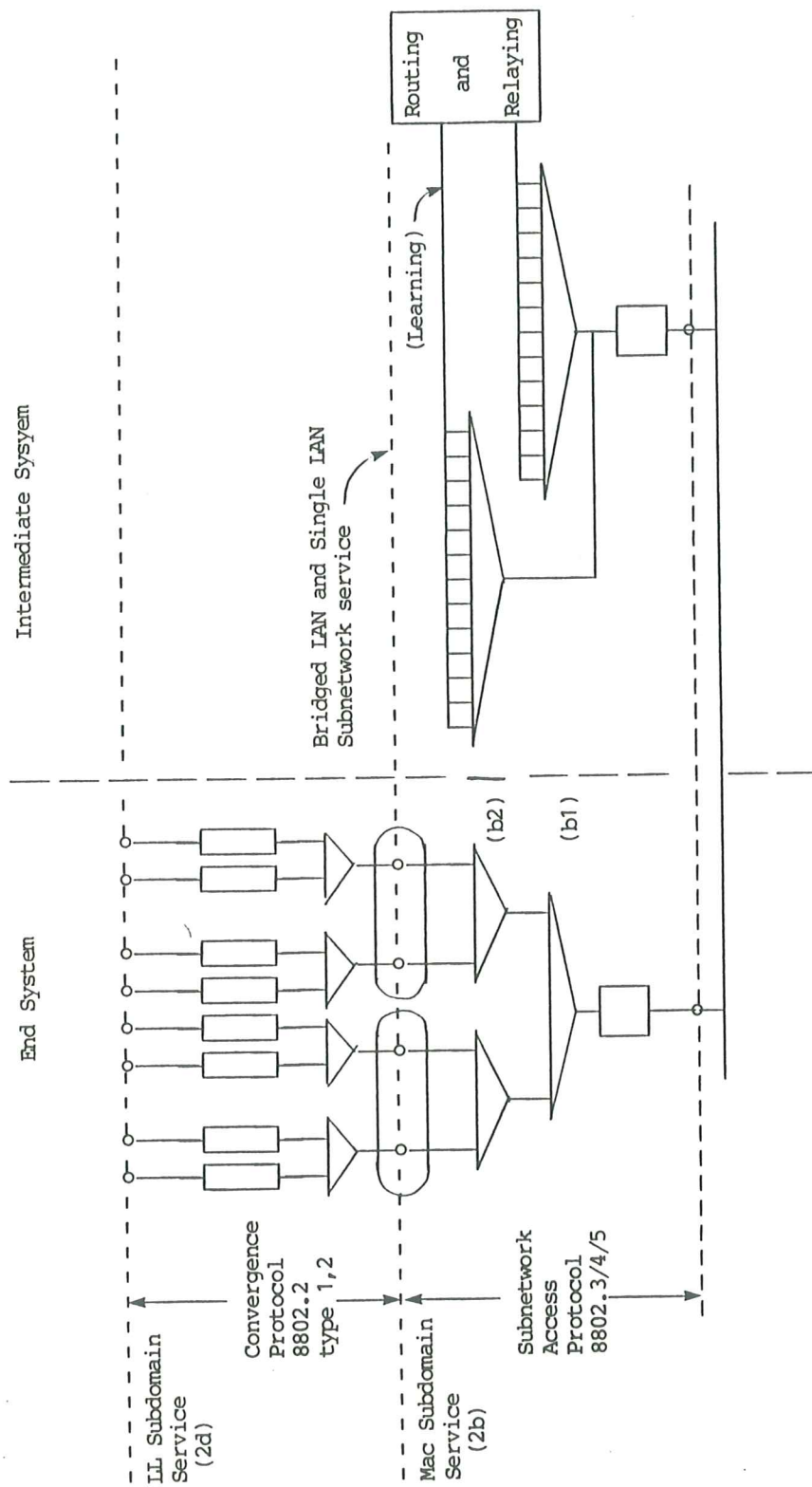


Figure 34 - 8802.x Single LAN and Bridged LAN

GLA application:

Sublayer		MAC	LLC1 (a)	LLC2 (a)	LLC1 +MAC	LLC2 +MAC
Segmenting/reassembly	C5
Sequencing	C4
Splitting	C3
Flow control	C2	.	.	0	.	0
Error control	C1	.	.	0	.	0
Connection qualification	B3
Remote SAP processing	B2	0	0 (b)	0 (b)	X	X
Local SAP processing	B1	0	0 (b)	0 (b)	X	X
Protocol version identification	A5
CC/DT/CL discrimination	A4	.	.	0	.	0
Error detection	A3	0	.	.	0	0
PDU delimiting	A2	0	.	.	0	0
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 5 - 8802.x Single LAN and Bridged LAN

12.6 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 35 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 12.6.2 - 12.6.4 each of the important services is modelled and described in more detail.

12.6.1 General Considerations

12.6.1.1 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 peers. 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 35 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.

12.6.1.2 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 35. 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.

12.6.1.3 Basic and Supplementary Services

Each of the ISDN and PSN Subnetwork 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 following observations can be made:

- The Basic Service defines 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; this then also defines the actual subnetwork service and

intervention level corresponding to the Basic Service.

- Each Supplementary Service describes 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; each Supplementary Service then is an increment in the actual subnetwork service and intervention level, towards the potential subnetwork service and intervention level.

Note 35

The description given here certainly applies to those of the supplementary services that clearly enhance the subnetwork service, for example Calling SNPA Indication. For other supplementary services, that seem to reduce the capabilities of users (for example Closed User Group) or seem to invoke fairly different services, this description may be less appropriate.

- The actual subnetwork service at a given moment in time now is equal to the sum of the basic service and the supplementary services subscribed to and registered.
- The potential subnetwork service is equal to (or higher than) the sum of the basic service and all of the supplementary services.

12.6.1.4 Service Modification

ISDNs, and therefore PSNs, intend to provide for modification of the service during the lifetime 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 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 reuse of some of the resources involved in a previous connection (for example a certain B-channel).

12.6.1.5 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 resynchronization 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 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 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 only minimal signalling type primitives, as the resynchronization function now provides an isolation from Network Layer type primitives.

12.6.2 PSN with Circuit Switching Service

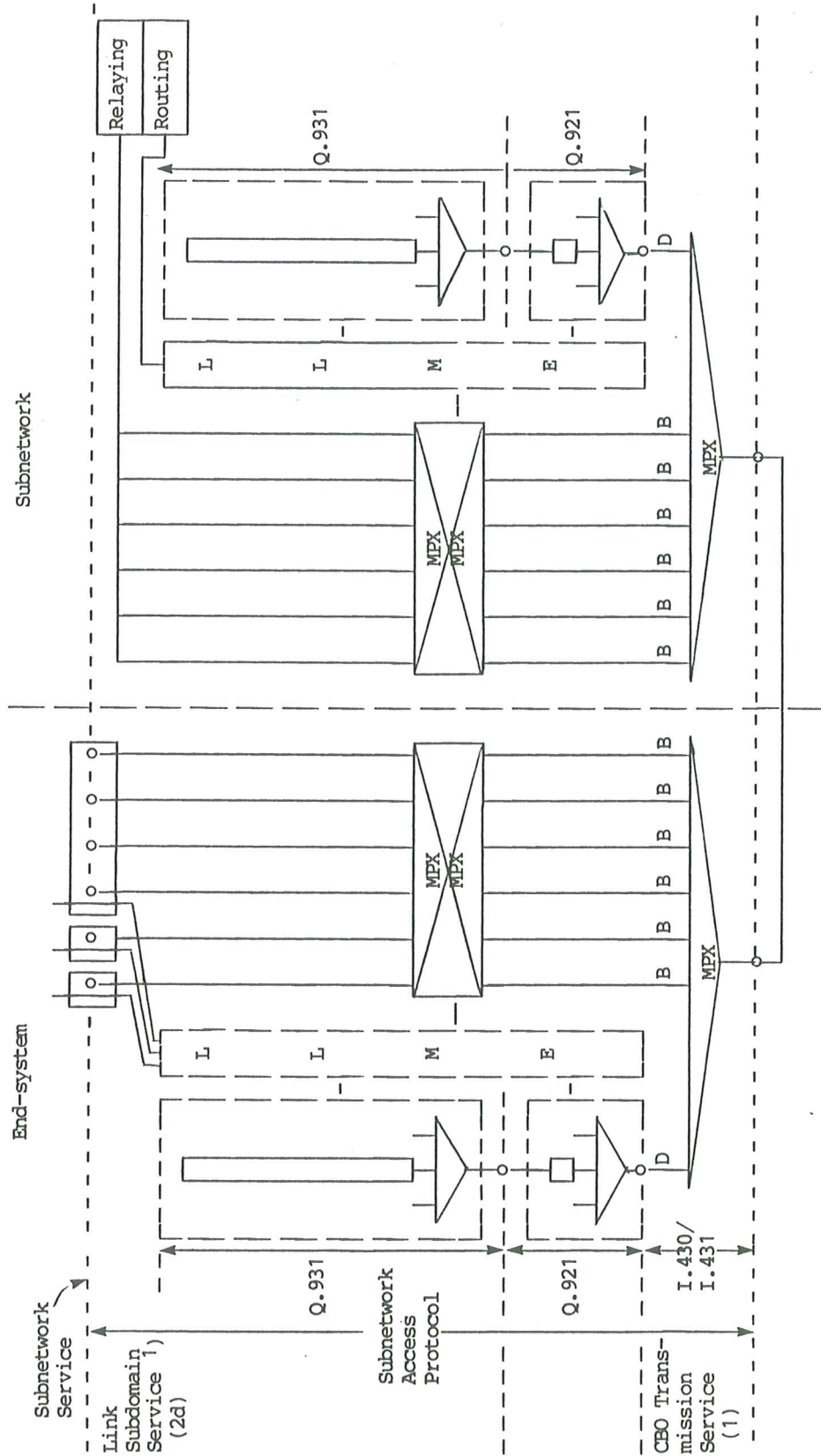
The UNSPM is given in Figure 36.

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 6.

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).



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

Figure 36 - 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	0
Remote SAP processing	B2	0
Local SAP processing	B1	0
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 6 - PSN with Circuit Switching Service

12.6.3 PSN with Frame Switching Service

The UNSPM is given in Figure 37.

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 7, assuming a multiframe 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 $PSS = (D,R2)$, $ASS = (C,R2)$.

The actual subnetwork service is $ASS = (C,R2)$ if flow control is implemented in the subnetwork, or $ASS = (C,Q)$ 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 8. 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 control are provided.

In Tables 9 and 10 a frame switching PSN is shown with X.25 layer 3 without Call Control and CLNP respectively as convergence protocols.

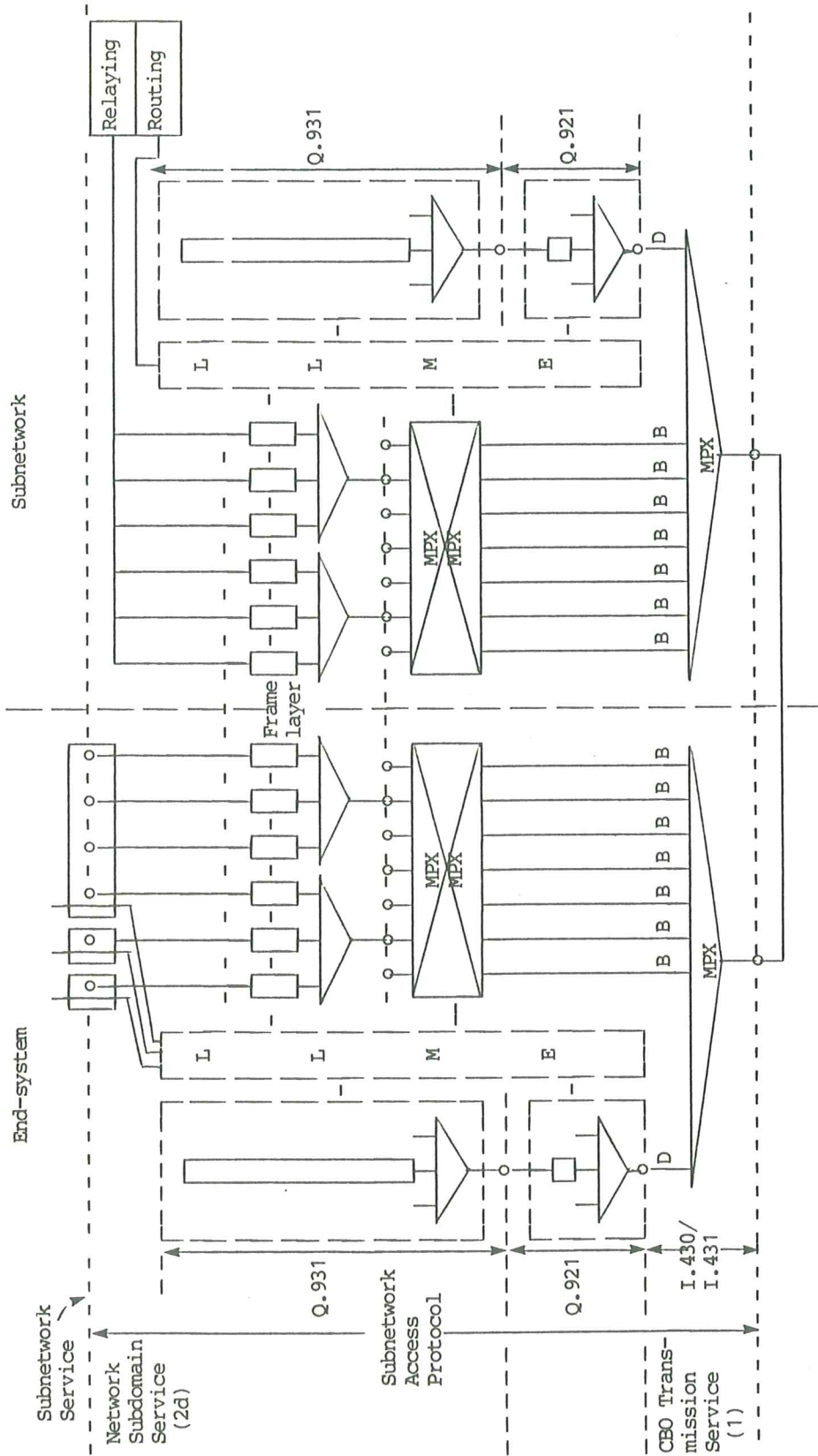


Figure 37 - PSN with Frame Switching Service

GLA application:

Sublayer		PSN/FS
Segmenting/reassembly	C5	.
Sequencing	C4	.
Splitting	C3	.
Flow control	C2	0
Error control	C1	0
Connection qualification	B3	0
Remote SAP processing	B2	0
Local SAP processing	B1	0
Protocol version identification	A5	.
CC/DT/CL discrimination	A4	0
Error detection	A3	0
PDU delimiting	A2	0
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 7 - 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	0
Remote SAP processing	B2	0
Local SAP processing	B1	0
Protocol version identification	A5	.
CC/DT/CL discrimination	A4	0
Error detection	A3	0
PDU delimiting	A2	0
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 8 - PSN with Frame Relaying Service

GLA application:

Sublayer		PSN/FS	X.25 Layer 3 (a)	Combined
Segmenting/reassembly	C5	.	0	0
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	0	0	0
Error control	C1	0	.	X
Connection qualification	B3	0	0	0
Remote SAP processing	B2	0	0	0
Local SAP processing	B1	0	0	0
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	0	.	0
Error detection	A3	0	.	0
PDU delimiting	A2	0	.	0
Protocol identification	A1	.	0	. (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 9 - PSN with Frame Switching Service and X.25 Layer 3 as convergence protocol

GLA application:

Sublayer		PSN/FS	CLNP (a)	Combined
Segmenting/reassembly	C5	.	0 (b)	0 (b)
Sequencing	C4	.	.	.
Splitting	C3	.	0	0
Flow control	C2	0	.	0
Error control	C1	0	.	0
Connection qualification	B3	0	.	0
Remote SAP processing	B2	0	0	0
Local SAP processing	B1	0	0	0
Protocol version identification	A5	.	0	0
CC/DT/CL discrimination	A4	0	.	0
Error detection	A3	0	.	0
PDU delimiting	A2	0	.	0
Protocol identification	A1	.	0	. (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 10 - PSN with Frame Switching Service and CLNP as convergence protocol

12.6.4 PSN with Packet Switching Service

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

12.6.4.1 Based on X.31 scenarios

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

12.6.4.1.1 X.25 Packet Switching Services ("maximum" scenario)

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

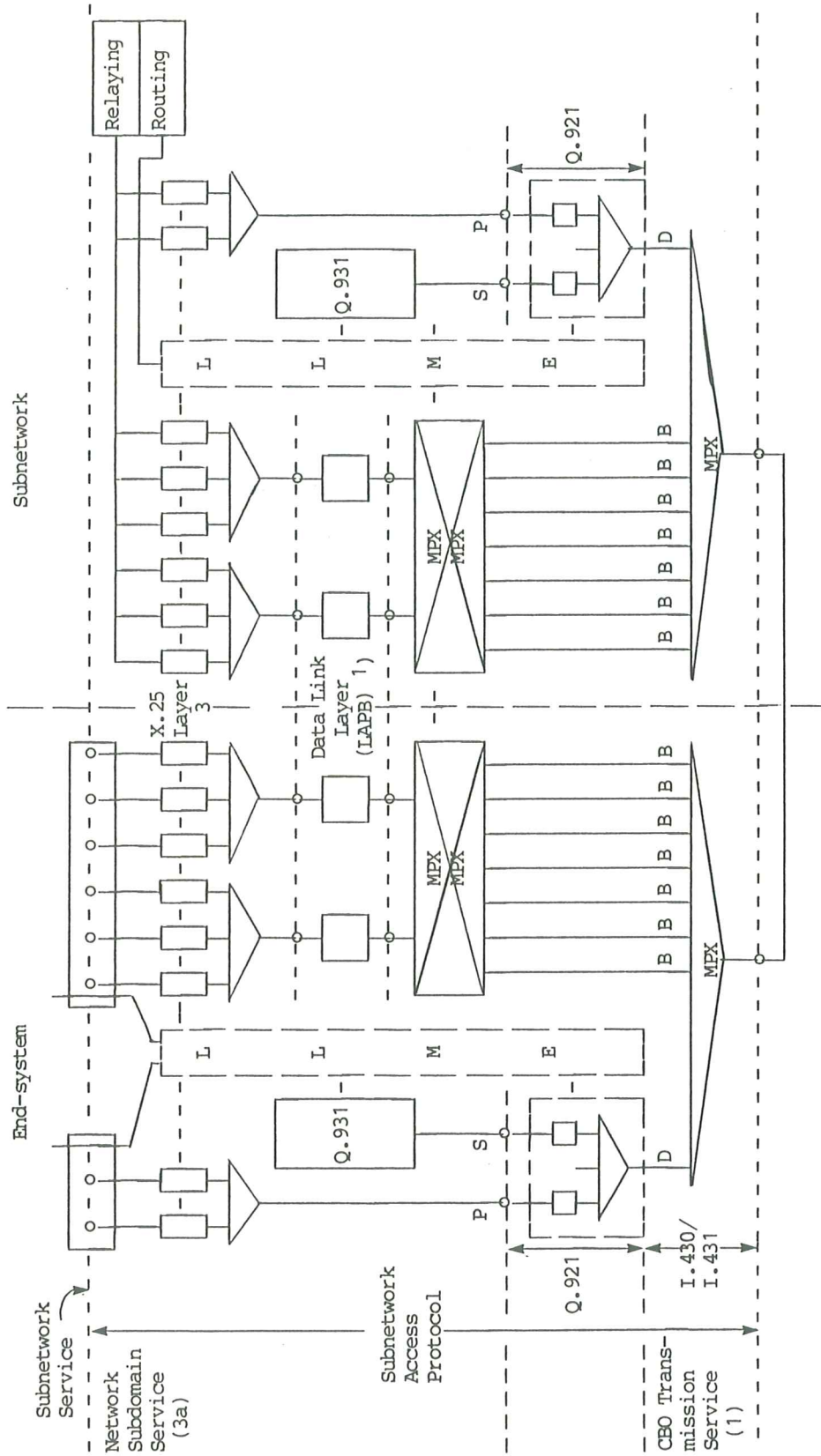
The UNSPM is given in Figure 38.

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 11.

12.6.4.1.2 X.25 DCE Access mode ("minimum" scenario)

This scenario, also described in X.31, is outside the scope, and is referred to here for completeness only. It allows an end system to access an X.25 DCE by use of a circuit switching subnetwork service as described in 12.6.2.



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

Figure 38 - PSN with Packet Switching Service ("Maximum" Scenario)

GLA application:

Sublayer		PSN/ LAPB	X.25 Layer 3	Combined
Segmenting/reassembly	C5	.	0	0
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	0	0	0
Error control	C1	0	.	X
Connection qualification	B3	.	0	0
Remote SAP processing	B2	.	0	0
Local SAP processing	B1	.	0	0
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	0	0	0
Error detection	A3	0	.	0
PDU delimiting	A2	0	.	0
Protocol identification	A1	.	0	. (a)

Notes

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

12.6.4.2 PSN with Packet Switching Service based on Frame Switching

12.6.4.2.1 With one level of multiplexing (at layer 2)

The UNSPM is given in Figure 39.

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 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 12.6.3.

The GLA model and subnetwork service classification are given in Table 12.

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.

12.6.4.2.2 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 12.6.4.2.1 in terms of service provided, and the models are identical to those of 12.6.4.2.1, with the exception of the multiplexing capability in layer 3.

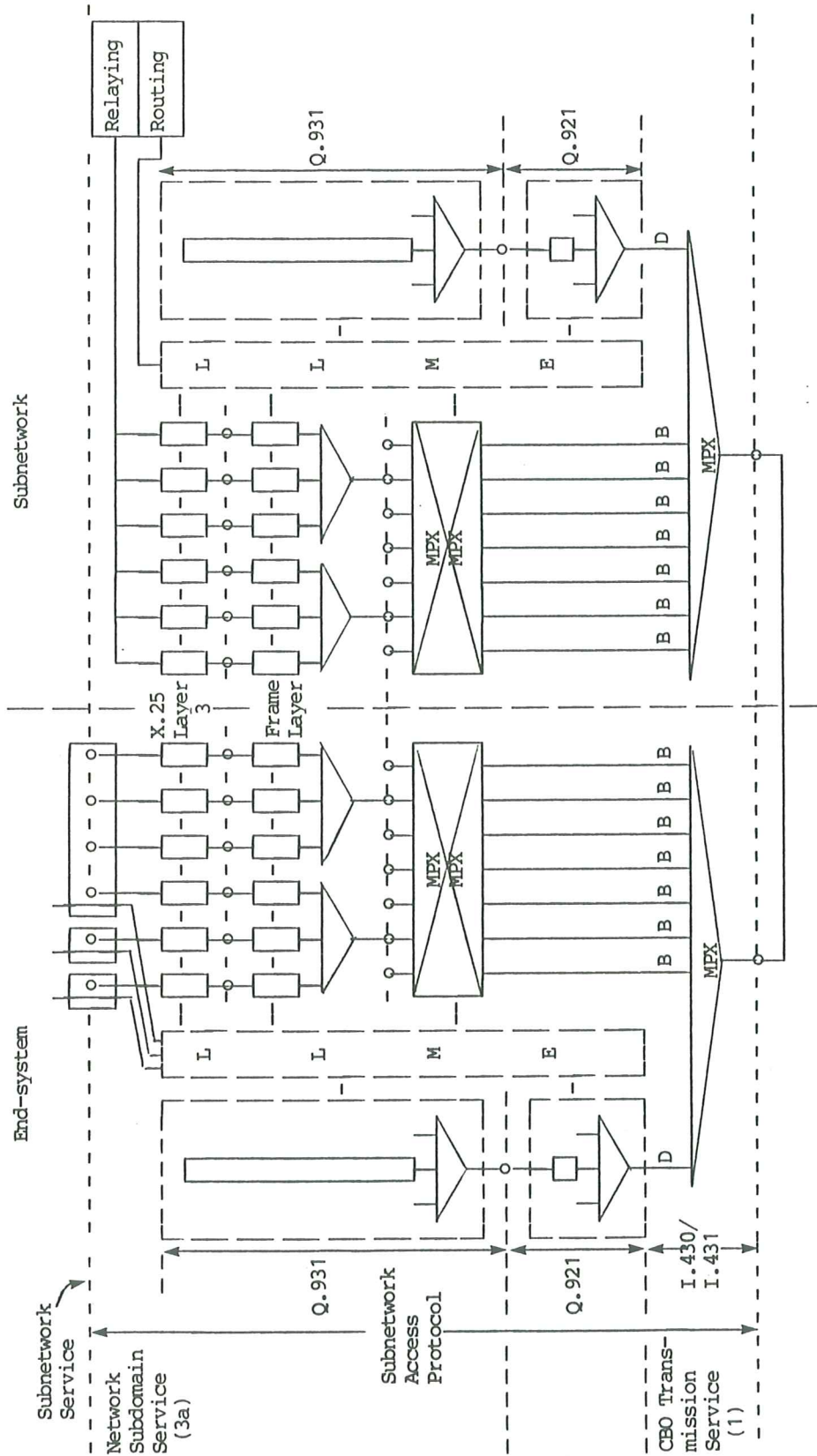


Figure 39 - PSN with Packet Switching Service based on Frame Switching

GLA application:

Sublayer		Frame Layer	Layer 3	Combined
Segmenting/reassembly	C5	.	0	0
Sequencing	C4	.	.	.
Splitting	C3	.	.	.
Flow control	C2	0	0	0
Error control	C1	0	.	X
Connection qualification	B3	0	0	0
Remote SAP processing	B2	0	0 (a)	0
Local SAP processing	B1	0	0	0
Protocol version identification	A5	.	.	.
CC/DT/CL discrimination	A4	0	.	0
Error detection	A3	0	.	0
PDU delimiting	A2	0	.	0
Protocol identification	A1	.	0	. (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
- 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) 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 12 - PSN with Packet Switching Service based on Frame Switching

SECTION V

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

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 7, 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.

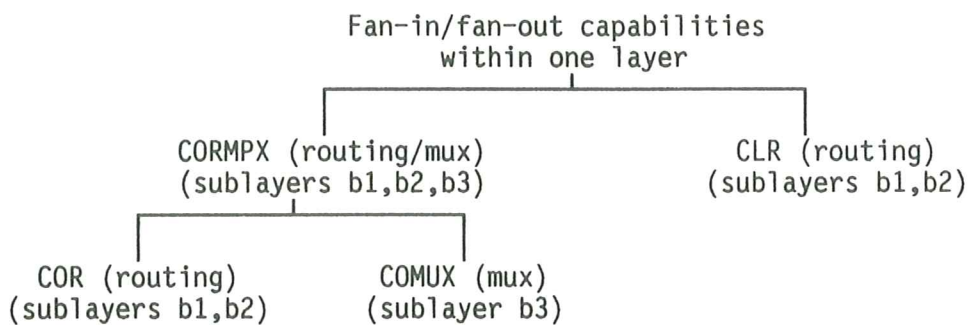
In terms of the GLA this covers the case where layer b1 and/or b2 is non-empty, and layer b3 is also non-empty.

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

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

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

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

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 corresponding 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

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 contiguous 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

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

DBO is particularly applicable to the service offered by packet switching networks.

Note

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.

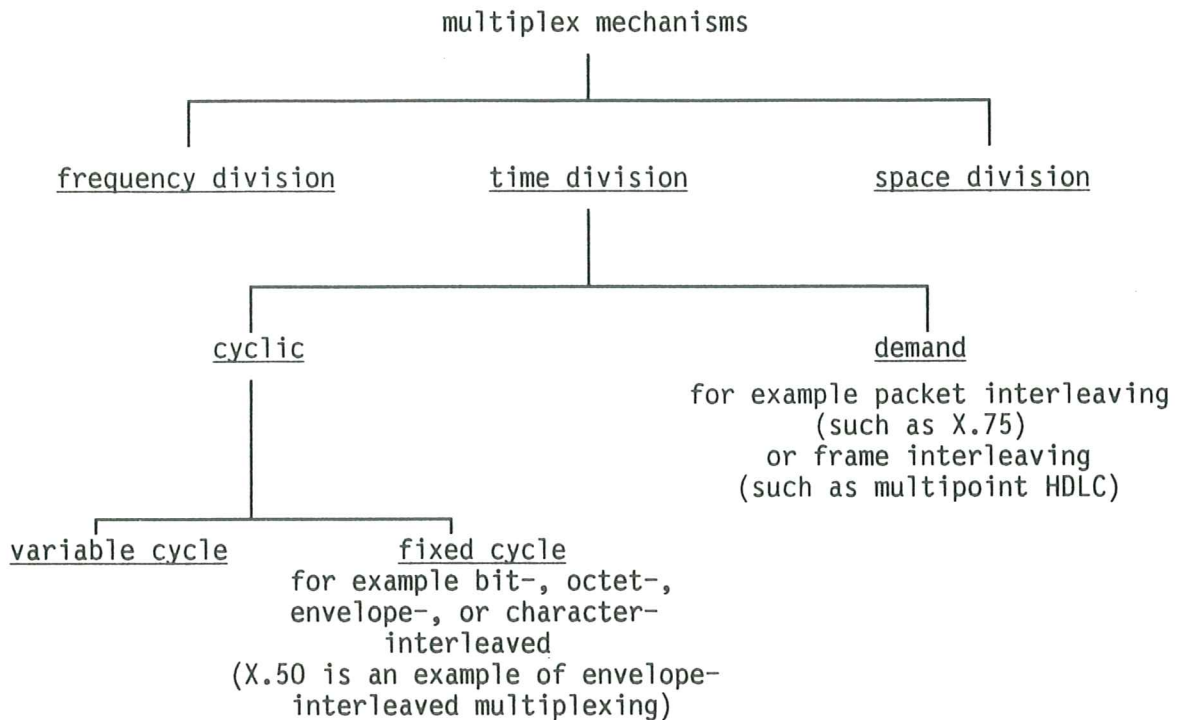


Figure B-1 - Classification of multiplex mechanisms

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

ABSTRACT SYNTAX OF NETWORK LAYER ADDRESS

In this Appendix an abstract syntax of a full Network Layer address is developed. It is based on the Generic Service Provider Model of 11.3.1 and the Multilayer Architecture of 11.3.2.

The abstract syntax must be subset as appropriate to satisfy any constraints that may be imposed in practice with respect to inter-subdomain service and intra-subdomain protocol relaying at a layer.

The abstract syntax of the address operated on at the (N)-inter-subdomain service relaying sublayer is assumed to be of the form:

$$(N)\text{-SdSP Id} / (N)\text{-SdSP Add} / (N)\text{-DSP Sel},$$

where:

- (N)-SdSP Id = Source/Destination (N)-Subdomain Service Provider Identifier,
- (N)-SdSP Add = Source/Destination (N)-Subdomain Address within the domain of the designated (N)-SdSP Id,
- (N)-DSP Sel = (N)-Domain SAP Selector within the domain of the designated (N)-SdSP Add.

Similarly the abstract syntax of the (N)-SdSP Add component operated on at the (N)-intra-subdomain protocol relaying sublayer is assumed to be of the form:

$$(N-1)\text{-DSP Id} / (N-1)\text{-DSP Add} / (N)\text{-SdSP Sel}.$$

By substitution the abstract syntax of the address operated on at the inter-subdomain relaying sublayer expands to:

$$(N)\text{-SdSP Id} / (N-1)\text{-DSP Id} / (N-1)\text{-DSP Add} / (N)\text{-SdSP Sel} / (N)\text{-DSP Sel}.$$

By progressive expansion of the (N-1) Add component and substitution of the sublayer designations of Figure 30 the abstract syntax of a Network Layer address becomes:

$$(3a)\text{-SdSP Id} / (2e)\text{-DSP Id} / (2d)\text{-SdSP Id} / (2c)\text{-DSP Id} / (2b)\text{-SdSP Id} / \\ (2b)\text{-SdSP Add} / (2c)\text{-DSP Sel} / (2d)\text{-SdSP Sel} / (2e)\text{-DSP Sel} / (3a)\text{-SdSP Sel} / (3b)\text{-DSP Sel}.$$

APPENDIX D

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 D-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 D-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.

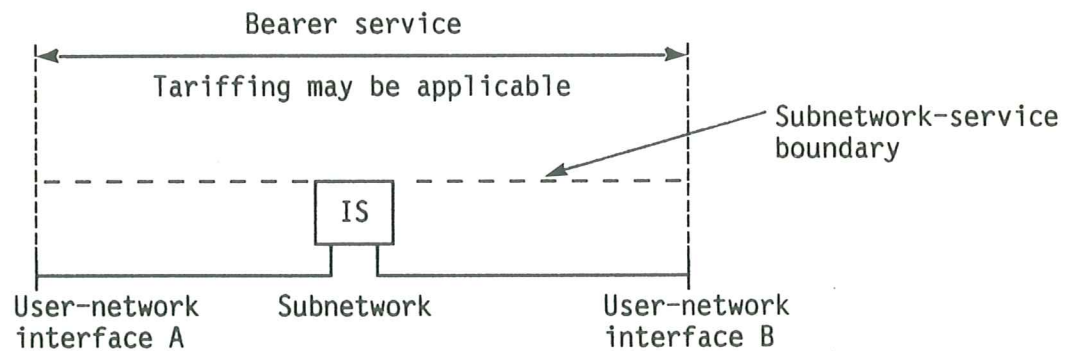


Figure D-1 - Bearer Service Concept

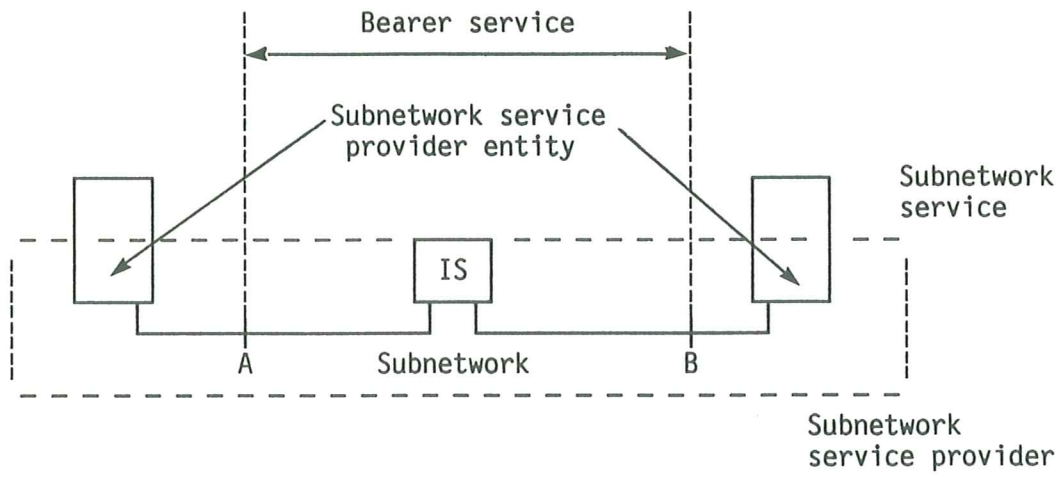


Figure D-2 - Relation between Bearer Service and Subnetwork Service Provider

APPENDIX E

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	COnection-based MUltipleXing
CONS	Connection Oriented Network Service
COR	COnection-based ROuting
CORMPX	COnection-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)

