ETSI TECHNICAL REPORT

ETR 085

June 1993

Source: ETSI TC-TM

Reference: DTR/TM-3016

ICS: 33.020, 33.040.40

Key words: Functional architecture, transport networks

Transmission and Multiplexing (TM);
Generic functional architecture of transport network

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Contents

Foreword

This ETSI Technical Report (ETR) has been produced by the Transmission and Multiplexing (TM) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or application of an ETS or I-ETS, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

A telecommunications network is a complex network which can be described in a number of different ways depending on the particular purpose of the description. This ETR describes the network as a transport network from the viewpoint of the information transfer capability.

More specifically, this ETR describes the functional and structural architectures of transport networks independently of networking technology.

Blank page

1 Scope

This ETR describes the functional architecture of transport networks in a technology independent way. The generic functional architecture of transport networks should be taken as the basis for a harmonised set of functional architecture standards for 1 (ATM), 2 (SDH), (PDH) networks and corresponding management standards, performance analysis and equipment specification.

2 References

For the purpose of this ETR, the following references apply:

[1]	ITU-T Recommendation G.803: "Architecture of transport networks based on the synchronous digital hierarchy (SDH)".
[2]	CCITT Recommendation E.164: "Numbering plan for the ISDN era".
[3]	PDH CCITT Recommendation G.702: "Digital hierarchy bit rates".
[4]	PDH CCITT Recommendation G.703: "Physical/electrical characteristics of hierarchical digital interfaces".

3 Abbreviations

For the purposes of this ETR, the following abbreviations apply.

ADM	Add/Drop Multiplex
AIS	Alarm Indication Signal
APS	Automatic Protection Switch
ATM	Asynchronous Transfer Mode
AU-n	Administrative Unit (level) n
AUG	Administrative Unit Group
B-ISDN	Broadband aspects of Integrated Services Digital Network
BIP-n	Bit Interleaved Parity (of order) n
DXC	Digital Cross-Connect
LTE	Line Termination Equipment
MST	Multiplex Section Termination
NNI	Network Node Interface
PDH	Plesiochronous Digital Hierarchy
PRC	Primary Reference Clock
PSTN	Public Switched Telephony Network
SDH	Synchronous Digital Hierarchy
STM-N	Synchronous Transport Module (level) N
TCP	Termination Connection Point

TMN	Telecommunication Management Network
TU-n	Tributary Unit (level) n
VC-n	Virtual Container (level) n

Clause 4 contains a vocabulary of terms for defining network architecture. Clause 5 contains the detailed description of the architecture in functional terms. The degree of rigour used is consistent with that required for the purposes of network design, network management and network performance analysis. Clause 6 uses the functional description and applies it to actual network topologies, structures and network elements which are likely to be required. Clause 7 contains a description of protection and restoration from a functional architecture viewpoint.

4 Vocabulary for network architecture

NOTE 1: The terms used here are specific to this ETR and should not be confused with the same terms used in, for example, CCITT Recommendations I.320, I.321, I.324, I.340.

NOTE 2: Where a definition contains a term which is itself defined, that term is given in quotation marks.

The terms entities can be further qualified in references to specific layers by adding the appropriate layer qualifier (e.g. SDH higher-order path termination, PDH 44736 kbit/s path termination, ATM virtual path connection).

Access group: a group of co-located "access points" together with their associated "trail termination" functions.

Access point: a "reference point" where the output of an "adaptation" source function is bound to an input of a "trail termination source" or the output of a "trail termination sink" is bound to the input of an "adaptation" sink function. The "access point" is characterised by the adapted client layer "characteristic information" which passes across it. A bi-directional "access point" is formed by an associated contra-directional pair.

Adaptation: a "transport processing function" which adapts a server layer to the needs of a client layer. The "adaptation" function defines the "server/client" association between the "connection point" and "access point" and these points therefore delimit the "adaptation" function. "Adaptation" functions have been defined for many "client/server" interactions.

Architectural component: any item required to generically describe "transport network" functionality independent of implementation technology.

Bidirectional connection: a "connection" consisting of an associated pair of "unidirectional connections" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs.

Binding: a direct relationship between the output of a "transport processing function" or "transport entity" and the input of another "transport processing functions" or "transport entity" with no intervening points of interest. "Bindings" represent the static connectivity within a network element. "Binding" relationships can never extend outside of network elements.

Characteristic information: a signal of characteristic rate and format which is transferred within and between "sub-networks" and presented to an "adaptation" function for "transport" by the server layer network.

Circuit layer network: a "layer network" which is concerned with the transfer of information between circuit layer "access points" in direct support of telecommunication services.

Client/server: an association represented by the "adaptation" function performed at the periphery of a "transport network layer". "Client/server" relationships never exist outside of network elements.

Commissioning process: configuration of network resources prior to network operation.

Connection point: a "reference point" where the output of a "trail termination source" or a "connection" is bound to the input of another "connection" or where the output of a "connection" is bound to the input of a "trail termination sink" or another "connection". The "connection point" is characterised by the information which passes across it. A bi-directional "connection point" is formed by the association of a contra-directional pair.

Connection supervision: the process of monitoring the integrity of a "connection" or "tandem connection" which is part of a "trail".

Connection: a "transport entity" which is capable of transferring information transparently between "connection points". A "connection" defines the association between the "connection points" and the "connection points" delimit the "connection".

Dedicated protection: a protection architecture that provides capacity dedicated to the protection of traffic-carrying capacity (1+1).

Dual ended operation: a protection operation method which takes switching action at both ends of the protected entity (e.g. "connection", "path"), even in the case of a unidirectional failure.

Link connection: a "transport entity" provided by the "client/server" association. It is formed by a near-end "adaptation" function, a server "trail" and a far-end "adaptation" function between "connection points". It can be configured as part of the "trail management process" in the associated server layer.

Link: a "topological component" which describes the fixed relationship between a "sub-network" and another "sub-network" or "access group".

Matrix connection: a "sub-network connection" that is a "connection" across a "matrix". It may be configured as part of the "trail management process" or it may be fixed.

Matrix: a "topological component" used to effect routeing and management. It describes the potential for "matrix connections" across the "matrix". A "matrix" is contained within one physical node. As such, it represents the limit to the recursive partitioning of a "sub-network".

Network connection: a "transport entity" formed by the series of "connections" between "termination connection points".

Network: all of the entities which together provide communication services (such as equipment, plant, facilities).

Pairing: a relationship between sink and source "transport processing functions" or "transport entities" which have been associated for the purposes of bi-directional transport.

Path layer network: a "layer network" which is concerned with the transfer of information between path layer "access points" in support of one or more "circuit layer networks".

Point-to-multipoint connection: a "connection" capable of transferring information from a single input to multiple outputs.

Reference point: an "architectural component" which describes the "binding" between inputs and outputs of "transport processing functions" and "transport entities". It is characterised by the information which passes across it.

Shared protection: a protection architecture using m protection entities shared amongst n working entities (m:n). The protection entities may also be used to carry extra traffic when not in use for protection.

Single ended operation: a protection operation method which takes switching action only at the affected end of the protected entity (e.g. "trail", "sub-network connection"), in the case of a unidirectional failure.

Sub-network connection protection: a protection type that is modeled by sub-layer that is generated by expanding the "sub-network" "connection point".

Sub-network connection: a "transport entity" formed by a "connection" across a "sub-network" between "connection points". It can be configured as part of the "trail management process".

Sub-network: a "topological component" used to effect routeing and management. It describes the potential for "sub-network connections" across the "sub-network". It can be partitioned into interconnected "sub-networks" and "links". Each "sub-network" in turn can be partitioned into smaller "sub-networks" and "links" and so on. A "sub-network" may be contained within one physical node.

Tandem connection bundle: a parallel set of "tandem connections" with co-located end points.

Tandem connection: an arbitrary series of "link connections" and "sub-network connections".

Termination connection point: a special case of a "connection point" where a "trail termination" function is bound to an "adaptation" function or a "matrix".

Topological component: an "architectural component" which describes the "transport network" in terms of the topological relationships between sets of "reference points". A topological description in terms of these components describes the routeing possibilities of the network and hence its ability to support "transport entities".

Trail management process: configuration of network resources during network operation for the purposes of allocation, re-allocation and routeing of "trails" to provide "transport" to client networks.

Trail protection: a protection type that is modelled by a sub-layer that is generated by expanding the "trail" "access points".

Trail termination sink: a "transport processing function" which terminates a "trail", extracts the "trail" overhead information, checks validity and passes the adapted client layer network "characteristic information" to the "adaptation" function.

Trail termination source: "transport processing function" which accepts adapted client layer network "characteristic information", adds "trail" overhead and assigns it to an associated "network connection" in the same "transport network layer".

Trail termination: a "transport processing function" which generates the "characteristic information" of a layer network and ensures integrity of that "characteristic information". The "trail termination" defines the association between the "access point" and "termination connection point" and these points therefore delimit the "trail termination".

Trail: a "transport entity" in a server layer responsible for the integrity of transfer of "characteristic information" from one or more client network layers between server layer "access points". It defines the association between "access points" in the same "transport network layer". It is formed by combining a near-end "trail termination" function, a "network connection" and a far-end "trail termination" function.

Transmission media layer network: a "layer network" which may be media dependent and which is concerned with the transfer of information between transmission media layer "access points" in support of one or more "path layer networks".

Transmission: the physical process of propagating information signals through a physical medium.

Transport entity: an "architectural component" which transfers information transparently between points at different locations. Information is transferred into the "transport entity" at its input and out of the "transport entity" at its output. "Transport entities" may be bound to each other or to "transport processing functions". The points at which they are bound are the "reference points" of the "transport network".

Transport network layer (or **layer network**): a "topological component" solely concerned with the generation and transfer of particular "characteristic information".

NOTE 3: "Transport networks" are built up of successive "transport network layers", one upon another. Each "transport network layer" provides "transport" for the layer above and uses "transport" provided by the layer below. The layer providing "transport" is termed a server and the layer using "transport" is termed a client. Two such layers are said to participate in a "client/server" relationship. A "transport network layer" is defined, at the highest level, by the "trails" which it supports or is capable of supporting and is characterised by its "characteristic information".

NOTE 4: A "layer network" should not be confused with the layer concept used in the protocol reference model described in CCITT Recommendation I.311.

Transport network: the functional resources of the "network" which conveys user information between locations.

Transport processing function: an "architectural component" defined by the information processing which is performed between its inputs and outputs. It has one or more inputs and one or more outputs which may be associated with inputs and outputs of other functions and entities. Such associations are termed "binding" relationships.

Transport: the functional process of transferring information between points at different locations.

Unidirectional connection: a "connection" which is capable of transparently transferring information from input to output.

5 Transport functional architecture of networks

5.1 Introduction

The various functions which constitute a telecommunications network can be classified into two broad functional groups. One is the transport functional group which transfers any telecommunications information from one point to another point(s). The other is the control functional group which realises various ancillary services and operations and maintenance functions. This ETR is concerned with the transport functional group.

A transport network transfers user information from one point to another point(s) bidirectionally, or unidirectionally. A transport network can also transfer various kinds of network control information such as signalling and operations and maintenance information for the control functional group as well as for its own use.

Since the transport network is a large, complex network with various components, an appropriate network model with well defined functional entities is essential for its design and management. The transport network can be described by defining the associations between points in the network. In order to simplify the description, a transport network model, based on the concepts of layering and partitioning within each layer, is used in a manner which allows a high degree of recursiveness. It is recommended that this method is used for describing the transport network.

5.2 Architectural components

The transport network has been analysed to identify generic functionality which is independent of implementation technology. This has provided a means to describe network functionality in an abstract way in terms of a small number of architectural components. These are defined by the function they perform in information processing terms, or by the relationships they describe between other architectural components. In general, the functions described here act on information presented at one or more inputs and present processed information at one or more outputs. They are defined and characterised by the information process between their inputs and outputs. The architectural components are associated together in particular ways to form the network elements from which real networks are constructed. The points at which the inputs and outputs of processing functions and transport entities are bound are the reference points of the transport network architecture.

Some diagrammatic conventions have been developed to support the descriptions which follow and these are illustrated in figures 1 to 4.

5.2.1 Topological components

The topological components provide the most abstract description of a network in terms of the topological relationships between sets of like reference points. Three topological components have been distinguished; these are the layer network, the sub-network and the link. Using only these components it is possible to completely describe the logical topology of a network.

5.2.1.1 Layer network

A layer network is defined by the complete set of like access points which may be associated for the purpose of transferring information. The information transferred is characteristic of the layer and is termed characteristic information. Access point associations in a layer network may be made and broken by a layer management process thus changing its connectivity. A separate, logically distinct layer network exists for each access point type. A layer network is made up of sub-networks and links between them. The structures within and between layer networks are described by the components defined in subclauses 5.2.1.2 and 5.2.1.3.

5.2.1.2 Sub-network

A sub-network is defined by the complete set of like connection points which may be associated for the purpose of transferring characteristic information. The connection point associations in a sub-network may be made and broken by a layer management process, thus changing its connectivity. Sub-networks are generally made up of lower level (i.e. smaller) sub-networks and links between them. The lowest level of this recursion that is of network architectural interest is the matrix (contained in an individual network element).

5.2.1.3 Link

A link is defined by the sub-set of connection points in one sub-network which are associated with a sub-set of connection points on another sub-network for the purpose of transferring characteristic information between sub-networks. The set of connection point associations which define the link cannot be made or broken by the layer management process. The link represents the topological relationship between a pair of sub-networks. In general, the link is used to describe the association between connection points contained in one network element with those in another. The lowest level of recursion of a link (through the layering concept) represents the transmission media.

5.2.2 Transport entities

The transport entities provide transparent information transfer between layer network reference points. That is to say, there is no information change between input and output other than that resulting from degradations in the transfer process.

Two basic entities are distinguished according to whether the information transferred is monitored for integrity. These are termed connections and trails. Connections are further distinguished into network connections, sub-network connections and link connections according to the topological component to which they belong.

5.2.2.1 Network connection

A network connection is capable of transferring information transparently across a layer network. It is delimited by Termination Connection Points (TCPs). It is the highest level of abstraction within a layer and may be partitioned into a concatenation of sub-network connections and link connections. There is no information as to the integrity of the transferred information, although information on the integrity of the connection itself can often be implied from other sources.

5.2.2.2 Sub-network connection

A sub-network connection is capable of transferring information transparently across a sub-network. It is delimited by connection points at the boundary of the sub-network and represents the association between connection points. Sub-network connections are, in general, made up of a concatenation of lower level sub-network connections and link connections and can be viewed as an abstraction of this more complex entity. The lowest level of this recursion, the matrix connection, represents a cross-connection on an individual matrix in a network element.

5.2.2.3 Link connection

A link connection is capable of transferring information transparently across a link between two sub-networks. It is delimited by connection points at the boundary of the link and the sub-networks and represents the association between such a connection point pair. Link connections are provided by trails in the server layer network.

5.2.2.4 Trail

A trail represents the transfer of validated characteristic information between access points therefore it represents the association between access points together with the incremental information regarding the information transfer integrity. A trail is formed from a network connection by including trail termination functions between the TCPs and the access points.

5.2.3 Transport processing functions

The two generic processing functions of adaptation and termination are distinguished in describing the architecture of layer networks. They occur together at layer boundaries and are defined by the information processing which is performed between their inputs and outputs.

5.2.3.1 Adaptation function

The adaptation source function is the process whereby the characteristic information of the client layer network is adapted to a form suitable for transport in the server layer network. The complementary function of recovering information which had been adapted is the adaptation sink function. The specific adaptation function depends on the characteristic information in the two layers. The following are examples of processes which may occur singly or in combination in inter-layer adaptation functions; coding, rate changing, aligning, justification, multiplexing.

5.2.3.2 Trail termination function

Trail termination functions provide information related to the integrity of information transfer in a trail. This is typically achieved by inserting incremental information at a trail termination source function which is monitored at a corresponding sink function.

5.2.4 Reference points

Reference points in the layer network are formed by binding the input of one transport processing function or transport entity to the output of another. They are bi-directional if the associated transport processing function or transport entity inputs or outputs are paired. These binding relationships can never extend outside a network element. The allowable bindings and resultant specific types of reference points are shown in figure 2. The connection types supported by these reference points are also shown in figure 2.

5.3 Partitioning and layering

5.3.1 Introduction

A transport network can be broken down into a number of independent transport network layers with a client/server association between adjacent layers. Each layer network can be separately partitioned in a way which reflects the internal structure of that layer. Thus the concepts of partitioning and layering are orthogonal, as shown in figure 5.

5.3.1.1 Importance of the partitioning concept

The partitioning concept is important as a framework for defining:

a) the network structure within a network layer;

b) significant administrative boundaries between network operators jointly providing end-to-end paths within a single layer;

c) domain boundaries within the layer network of a single operator with a view to apportioning performance objectives to the sub-systems of which the network is composed;

d) independent routeing domain boundaries in relation to the operation of the path management process.

5.3.1.2 Importance of the layering concept

The layering concept of the transport network is based on the following assumptions:

a) each layer network can be classified into similar functions;

b) it is simpler to design and operate each layer separately than it is to design and operate the entire transport network as a single entity;

c) a layered network model can be useful in defining the managed objects in the Telecommunications Management Network (TMN);

d) each layer network is able to have its own operations and maintenance capability such as protection switching and automatic failure recovery against malfunctions or failures and mis-operations. This capability minimises the operations and maintenance action and influences in other layers;

e) it is possible to add or change a layer without affecting other layers from the architectural viewpoint;

f) each network layer may be defined independently of the other layers.

5.3.2 Partitioning concept

The partitioning concept can be divided into two related areas: the partitioning of sub-networks which describes topology, and the partitioning of network connections which describes connectivity.

5.3.2.1 Partitioning of sub-networks

A sub-network simply describes the capability to associate a number of connection points, or TCPs, and does not directly describe the topology of architectural components used to make up the sub-network. In general, any sub-network can be partitioned into a number of smaller sub-networks interconnected by links. The way in which the smaller sub-networks and links are bound to each other describes the topology of the sub-network. This can be expressed as follows:

Sub-network = Smaller sub-networks + Links + Topology

Thus it is possible with the partitioning concept to recursively break down any layer network to reveal the desired level of detail. This level of detail is likely to coincide with the individual equipments which implement connection matrices in individual network elements which provide the flexible connection capability of the layer network.

Examples of sub-networks are the international portion and the national portions of a layer network, which can be further divided into transit portions and access portions and so on, as shown in figure 6.

5.3.2.2 Partitioning of network connections and sub-network connections

A trail is an transport entity formed by the binding of trail terminations to a network connection as shown in figure 7 and is a particular instance of the capability of a layer network. The network connection is an instance of the capability of the largest sub-network definable within the layer network. In the same way that it is possible to partition a sub-network, it is also possible to partition a network connection. In general, a network connection can be partitioned into a serial combination of sub-network connections and link connections as follows:

Network connection = TCP + sub-network connections + link connections + TCP

Each of the sub-network connections can be further partitioned into a serial combination of sub-network connections and link connections. In this case the partitioning shall start and finish with a sub-network connection as follows:

Sub-network connection = CP + smaller sub-network connections + link connections + CP

The partitioning of network connections and sub-network connections mirrors the partitioning of the sub-networks. In this case, the normal limit of the recursive partitioning would be individual connection point associations on the basic matrices which are used to construct the layer network.

The way the partitioning of sub-network connections into smaller sub-network connections and link connections mirrors that of the sub-networks is shown in figure 8.

5.3.2.3 Link connections and the layering concept

When a network connection has been fully broken down into constituent link connections and sub-network connections, each link connection may be considered as an abstract transport entity composed of adaptation functions and a trail using the layering concept.

5.3.3 Layering concept

The client/server association between adjacent layer networks is one where a link connection in the client layer network is provided by a trail in the server layer network. Table 1 provides examples of client/server associations currently defined in CCITT Recommendations.

The layer networks which have been identified in the transport network functional model should not be confused with the layers of the OSI Protocol Reference Model (PRM).

The concept of adaptation is introduced to allow layer networks with different characteristic information structure to support one another by the client/server relationship and this is the source of the recursion which is evident in the transport network model. It is also the reason why there is not the same concept of contiguous layer boundaries in the transport network model as in the OSI PRM. All the reference points belonging to a single layer network can be visualised as lying on a single plane as illustrated in figure 4 (m). From a transport network functional viewpoint therefore the adaptation function falls between the layer network planes. However it is considered to belong from an administrative viewpoint to the server layer trail to which it is attached. This is the rationale behind the administrative layer boundary illustrated in figure 4 (n).

5.3.3.1 Transport network layers

Figure 9 illustrates the layered model of the transport network. Features of the layered model are as follows:

- it is classified broadly into three classes of layer network: a circuit layer network, a path layer network and a transmission media layer network;
- the association between any two adjacent layers is a server/client association;
- each layer has its own operations and maintenance capability.

The three classes of layer networks are described as follows:

- circuit layer networks - provides users with telecommunications services such as circuit switched services, packet switched services and leased line services. Different circuit layer networks can be identified according to the services provided. Circuit layer networks are independent of path layer networks;

- path layer networks - are used to support different types of circuit layer networks or other path layer networks. Path layer networks are independent of transmission media layer networks;

- transmission media layer networks - are dependent on the transmission medium such as optical fibre and radio. Transmission media layer networks may be divided into other layer networks, according to the transmission technology being used.

5.3.3.2 Client/server association

The client/server association between adjacent layer networks is one where a link connection in the client layer network is provided by a trail in the server layer network.

5.3.3.3 Decomposition of layer networks

5.3.3.3.1 General principles of decomposition of layers

It is possible to decompose a layer by expanding either the adaptations, terminations, or (termination) connection points of the layer. In each case, this decomposition results in a new layer boundary as illustrated in figure 10. It should be noted that the new layer boundary will be different in each case.

5.3.3.3.2 Decomposition of the path layer into administrative path layers

It is possible to identify a set of layers within the path layer which are likely to be independently administered by a network operator by decomposing the path layer.

Each administrative path layer can have both the circuit layer and other administrative path layers as clients and can have the transmission media layer and other path layers as servers. The selection of the administrative path layers is likely to be the result of international agreement and meet the diverse requirements of the circuit layer. Each administrative path layer can have independent topology and it is likely that paths across an administrative path layer will be set up in independence from the set up of paths in other administrative path layers. This is illustrated generically in figure 11.

5.3.3.3.3 Decomposition of the transmission media layer into administrative transmission media layers

A set of layers within the transmission media layer can be identified which are likely to be independently administered by a network operator by decomposing the transmission media layer.

While the transmission media layer is dependent on the media used, it may be useful for some media to identify administrative transmission media layers. For example, both optical fibre systems and radio relay systems distinguish an administrative layer which describes trails between path handling centres and a layer which describes trails between repeaters or regenerators.

Again this is illustrated in figure 11.

In the future it may be desirable to identify further layers to describe wavelength division multiplexing and wavelength routeing on optical systems.

5.3.3.3.4 Decomposition of administrative layers into sub-layers

While the administrative layers are the layers of main interest to a network operator in the administration of the transport network, it is often important to distinguish sub-layers within the administrative layer. This can be done by decomposing the administrative layer. Examples include:

- identification of sub-layer protection schemes (see Clause 7) by the decomposition of the adaptation;
- identification of a sub-layer describing a trail which monitors a tandem connection across a sub-network by decomposing the termination;
- identification of a sub-layer describing a trail which an operator may add to a cross-connection to monitor its integrity across the cross-connect by decomposing the connection point.

This procedure has been used in developing functional models for protection and tandem connection monitoring.

5.4 Tandem connection monitoring [connection supervision]

The intended role of tandem connections is to represent the segment of a trail that exists within a particular administrative region. In this role, the following functions shall be supported by the tandem connection (refer to figure 12):

- tandem connection performance monitoring (error performance and failure/alarm conditions);
- tandem connection far end performance monitoring (error performance and failure/alarm conditions);
- tandem connection incoming failure indication (failures before the tandem connection);
- tandem connection connectivity verification (i.e., trace) (between the ends of the tandem connection);
- tandem connection idle signal (including idle signal identity).

A proposed solution uses "sub-layer monitoring" (as described in subclause 5.4.4). It uses the combination of an incoming error count and a data link, to support the needs above. This solution is for further study.

5.4.1 Inherent monitoring (refer to figure 13 (a))

The tandem connection is indirectly monitored by using the inherently available data from the server layers and computing the approximate state of the client tandem connection from the available data.

The use of inherent monitoring will depend heavily on the use of a data network and distributed processing to correlate failure events, determine if they are, or are not, within the administration, and report the results to the appropriate management locations (such as both ends of the tandem connection).

When the adaptation function includes multiplexing the error performance statistics for each of the tandem connections are not available individually but can be deduced from error performance of the server layers if uniform distribution of errors amongst the clients is assumed.

Connection verification can only be implied from the verification of connections in the server layer between nodes, and the assumption that each node verifies its client layer connections internally.

Data channel emulation can be provided by addressing messages to the other node over an open system communications network.

This technique requires distributed processing, and so may be difficult to standardise. However, this technique will support arbitrary nesting or overlapping of tandem connections.

5.4.2 Non-intrusive monitoring (refer to figure 13 (b))

The tandem connection is directly monitored by use of listen only (non-intrusive) monitoring of the original data and overhead and then computing the approximate state of the tandem connection from the difference between the monitored states at each end of the tandem connection.

The use of non-intrusive monitoring will depend less on the use of a data network and distributed processing to correlate failure events in order to determine if they are or are not within the administration, and report the results to the appropriate management locations (such as both ends of the tandem connection). In this case the desired information is available from the two ends and does not require communication with the nodes in the middle of the tandem connection.

The non-intrusive monitoring function may be dedicated to a single sub-network connection or it may be shared between a number of sub-network connections that require monitoring.

Error performance statistics for each of the tandem connections are available directly from the difference in the error performance records at the two ends. Error performance difference calculations cannot be perfect, but statistically meaningful derived measurements should be possible.

Connection verification can be performed if the original signal was provided with a globally unique trace identifier (such as the CCITT Recommendation E.164 code [2]). Reasonable connection verification may also be possible by capturing some form of signature from the content of the signal at the head end and matching that signature at the tail end.

Data channel emulation can be provided by addressing messages to the other node over an open system communications network.

This technique requires some data communications requiring standardisation. However, this technique will support arbitrary nesting or overlapping of tandem connections.

5.4.3 Intrusive monitoring (refer to figure 13 (c))

The tandem connection is directly monitored by breaking the original trail and introducing a test trail that extends over the tandem connection for the duration of the test.

In this way all parameters can be monitored directly, but the user trail is not complete so this can only be done either just at the start of the trail set-up, or possibly in an intermittent fashion.

This technique supports arbitrary nesting or overlapping of the tandem connections, but not simultaneous testing.

5.4.4 Sub-layer monitoring (refer to figure 13 (d))

Part way between intrusive and non-intrusive monitoring, some portion of the original trail's overhead is over-written such that the tandem connection can be directly monitored. In this case, the tandem connection is the network connection of the monitored sub-layer. If the original overhead was unused then this monitoring is effectively non-intrusive on the original trail.

With this technique all parameters can be tested directly, assuming that sufficient bandwidth can be over-written in the original overhead. This scheme is unlikely to be able to support overlapping or nested tandem connections.

Table 1: Examples of adaptation function references

Client layer	Server layer	Adaptation reference	Client network characteristic information
1 544 kbit/s asynch	VC-11 path	G.709	1 544 kbit/s ± 50 ppm
1 544 kbit/s bit synch	VC-11 path	G.709	1 544 kbit/s nominal
1 544 kbit/s byte synch	VC-11 path	G.709	1 544 kbit/s nominal G.704 octet structured
2 048 kbit/s asynch	VC-12 path	G.709	2 048 kbit/s ± 50 ppm
2 048 kbit/s bit synch	VC-12 path	G.709	2 048 kbit/s nominal
2 048 kbit/s byte synch	VC-12 path	G.709	2 048 kbit/s nominal G.704 octet structured
6 312 kbit/s asynch	VC-2 path	G.709	6 312 kbit/s ± 30 ppm
34 368 kbit/s asynch	VC-3 path	G.709	34 368 kbit/s ± 20ppm
44 736 kbit/s asynch	VC-3 path	G.709	44 736 kbit/s ± 20 ppm
139 264 kbit/s asynch	VC-4 path	G.709	139 264 kbit/s ± 15 ppm
B-ISDN ATM Virtual path	VC-4 path or VC-4-4c (NOTE)	G.709	53-octet cells
VC-11 path	VC-3 HO path or VC-4 path	G.709	VC-11 + frame offset
VC-12 path	VC-3 HO path or VC-4 path	G.709	VC-12 + frame offset
VC-2 path	VC-3 HO path or VC-4 path	G.709	VC-2 + frame offset
VC-3 LO path	VC-4 path	G.709	VC-3 + frame offset
VC-3 HO path	STM-N section	G.709	VC-3 + frame offset
VC-4 path	STM-N section	G.709	VC-4 + frame offset

Key: LO = Lower-order
HO = Higher-order

NOTE: Mappings into other SDH virtual containers are under study.

6 Application of concepts to network topologies and structures

6.1 PDH layers supported on SDH layers

Figure 14 shows an example of the case where PDH signals are supported on SDH. Five layer networks are shown:

a) PDH CCITT Recommendation G.702 [3] path (e.g. 2 048 kbit/s) layer;

b) PDH CCITT Recommendation G.703 [4] intra-office section layer;

c) SDH lower-order path (e.g. VC-12) layer;

d) SDH higher-order path (e.g. VC-4) layer;

e) SDH Synchronous Transport Model (level) N (STM-N) section layer.

The example shows two SDH multiplexers with tributaries at the PDH path bit rates interconnected with a SDH lower-order path cross-connect and a SDH higher-order path cross-connect at intermediate locations. All interfacing (except the tributaries at the PDH path bit rates) uses the SDH STM-N section layer.

6.2 ATM cell layers supported on SDH layers

Figure 15 shows an example of the case where ATM cells are supported on SDH. Four layer networks are shown:

a) ATM virtual channel layer;

b) ATM virtual path layer;

c) SDH higher-order path (e.g. the VC-4) layer;

d) SDH (STM-N) section layer.

The example shows two ATM virtual channel terminations interconnected with an ATM virtual channel switch/cross connect and two ATM virtual path terminations interconnected with an ATM virtual path switch/cross connect, and a SDH higher-order path cross-connect at intermediate locations. All interfacing uses the SDH STM-N section layer.

7 Transport network availability enhancement techniques

7.1 Introduction

This subclause describes the architectural features of the main strategies which may be used to enhance the availability of a transport network. This enhancement is achieved by the replacement of failed or degraded transport entities. The replacement is normally initiated by the detection of a defect, performance degradation or an external (e.g. network management) request.

Protection: this makes use of pre-assigned capacity between nodes. The simplest architecture has one dedicated protection entity for each working entity (1+1). The most complex architecture has m protection entities shared amongst n working entities (m:n).

Restoration: this makes use of any capacity available between nodes. In general, the algorithms used for restoration will involve re-routeing. When restoration is used, some percentage of the transport network capacity will be reserved for re-routeing working traffic.

7.2 Restoration

For further study.

7.3 Protection

Two types of protection architecture have been identified.

7.3.1 Trail protection

A working trail is replaced by a protection trail if the working trail fails or if the performance falls below the required level. This is modeled by introducing a protection sub-layer as shown in figure 16. The layer access point is expanded, according to the rules given in figure 11, into the protection adaptation function and protection trail termination function to provide the protection sub-layer. A protection matrix is used to model the switching between the protection and working connections. The status of the trails in the protection sub-layer is made available to the protection matrix (trail signal fail in figure 16). The protection adaptation function provides access to an Automatic Protection Switch (APS) channel. This supports communication between the control functions of the protection matrices. The trail termination provides the status of the server trail, the protection trail termination provides the status of the protected trail.

7.3.2 Sub-network connection protection

A working sub-network connection is replaced by a protection sub-network connection if the working sub-network connection fails or if the performance falls below the required level.

NOTE: Sub-network connection protection may be applied at any layer in a layer network, also the sub-network connection being protected may be made up of a concatenation of lower level sub-network connections and link connections.

Some network operators have indicated that it may be desirable to use dual ended operation in certain applications. The need for this method of operation and the implementation is for further study.

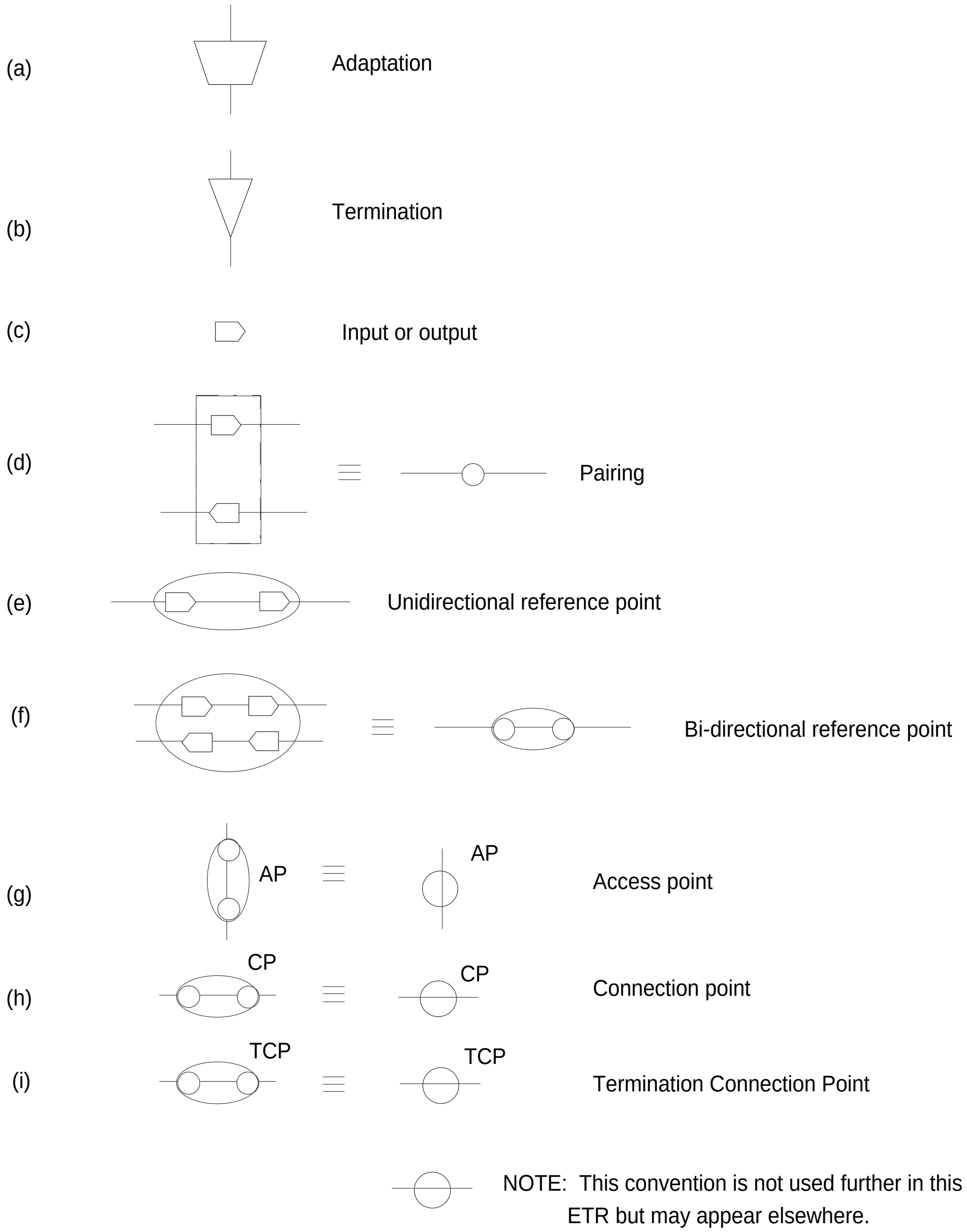
Sub-network connections have no inherent monitoring capability, hence sub-network protection schemes may be further characterised by the method used to monitor the sub-network connection. This is modeled by a protection sub-layer as shown in figure 17. The sub-network connection points are expanded, according to the rules given in figure 10. The general case, using protection trail termination and adaptation functions, is illustrated in figure 18. The status of the trails in the server layer is made available to the matrix (server signal fail in figure 18). The protection functions may be implemented by using one of the connection supervision schemes identified in subclause 5.4.

Inherent monitoring: the information derived by the server layer, as described in subclause 5.4.1, is used to initiate protection switching. This is illustrated in figure 19.

Non-intrusive monitoring: the sub-network connection is monitored by employing a trail termination function that is bridged onto the sub-network connection as illustrated in figure 20.

Intrusive monitoring: use of this type of monitor is not recommended as part of a protection scheme.

Sub-layer Monitoring: the introduction of a monitoring sub-layer allows the use of trail protection.



NOTE: This convention is not used further in this ETR but may appear elsewhere.

Figure 1: Diagrammatic conventions for processing functions and reference points

Input / **Output**		**Adaptation** Source	**Adaptation** Sink	**Trail termination** Source	**Trail termination** Sink	**Connection**
Adaptation	Source	X	CP	AP	X	X
	Sink	CP	X	X	TCP	CP
Trail termination	Source	TCP	X	X	X	TCP
	Sink	X	AP	X	X	X
Connection		CP	X	X	TCP	CP

Allowable bindings

X = Not allowed
CP = Connection point
TCP = Termination connection point
AP = Access point

Reference point	**Connection point**	**Termination connection point**	**Access point**
Connection point	Link connection / Sub-network connection *	Sub-network connection *	X
Termination connection point	Sub-network connection *	Network connection	X
Access point	X	X	Trail

Supported connection types between reference points

X = No connection supported

* The matrix connection is not shown explicitly because it is the limit of the recursion of sub-network connection

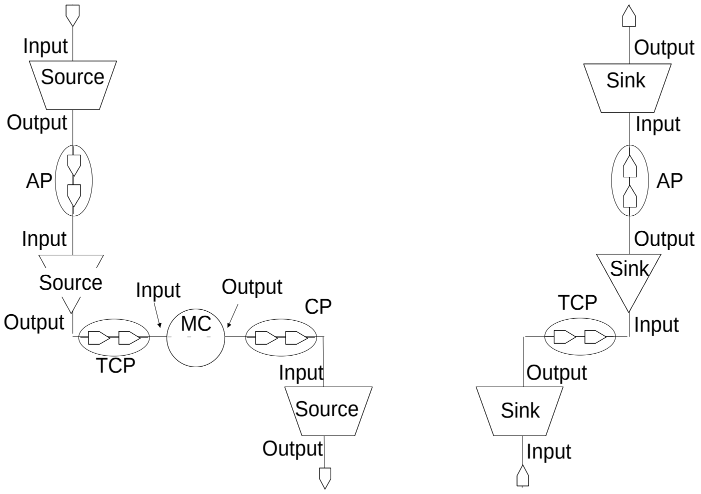


Figure 2: Allowable bindings and types of reference points

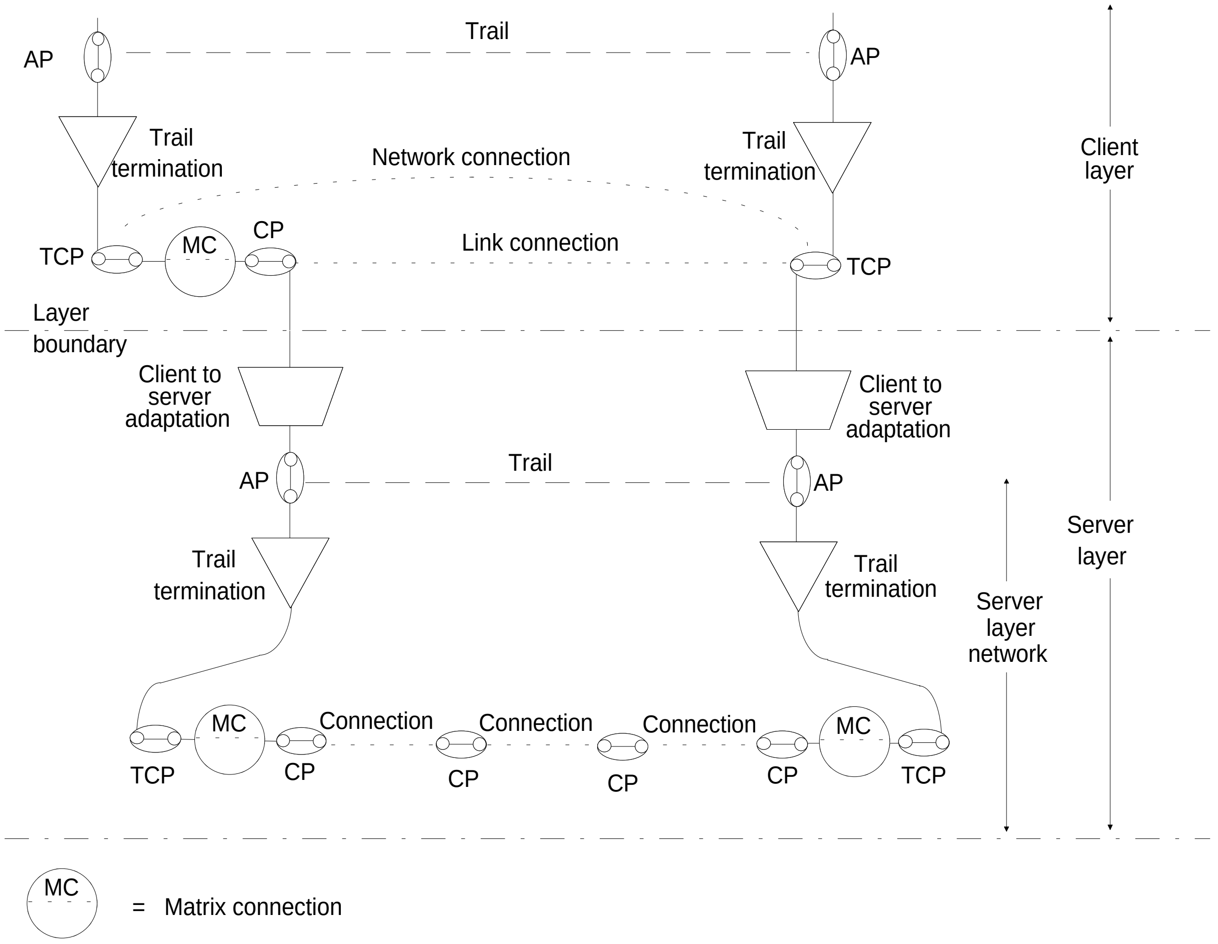


Figure 3: Example of functional model illustrating use of some architectural components

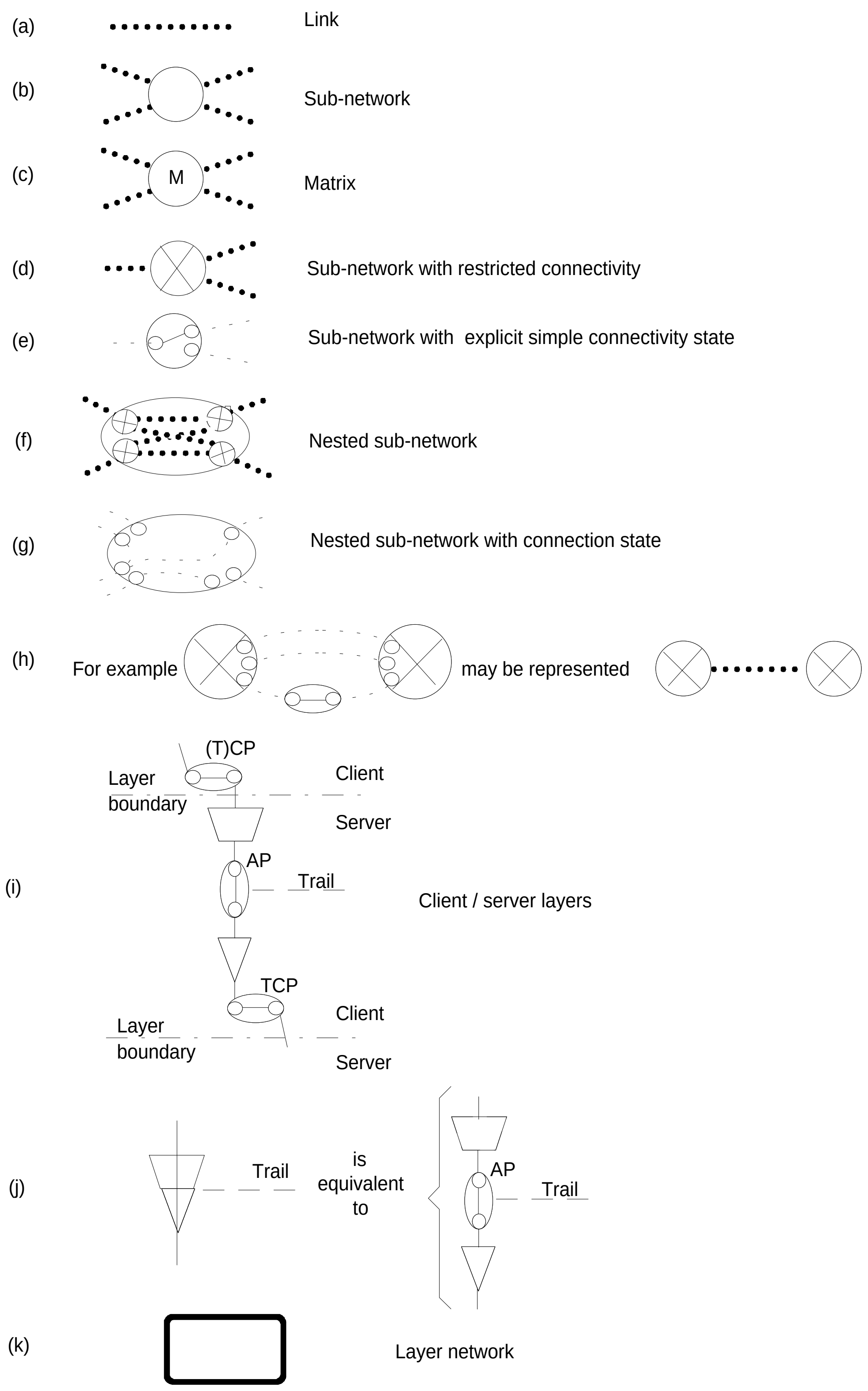


Figure 4: Other diagrammatic conventions (continued)

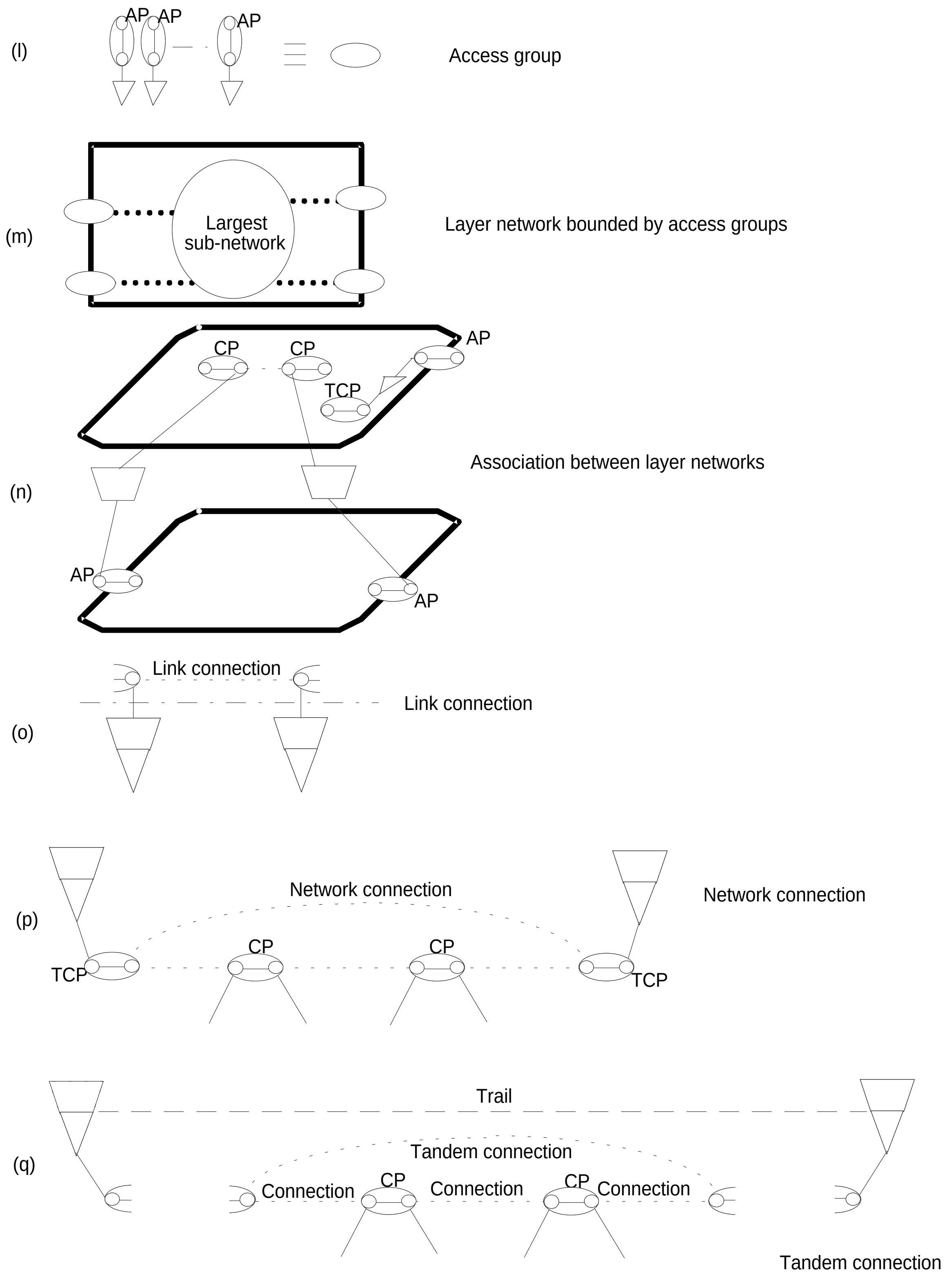


Figure 4: Other diagrammatic conventions (concluded)

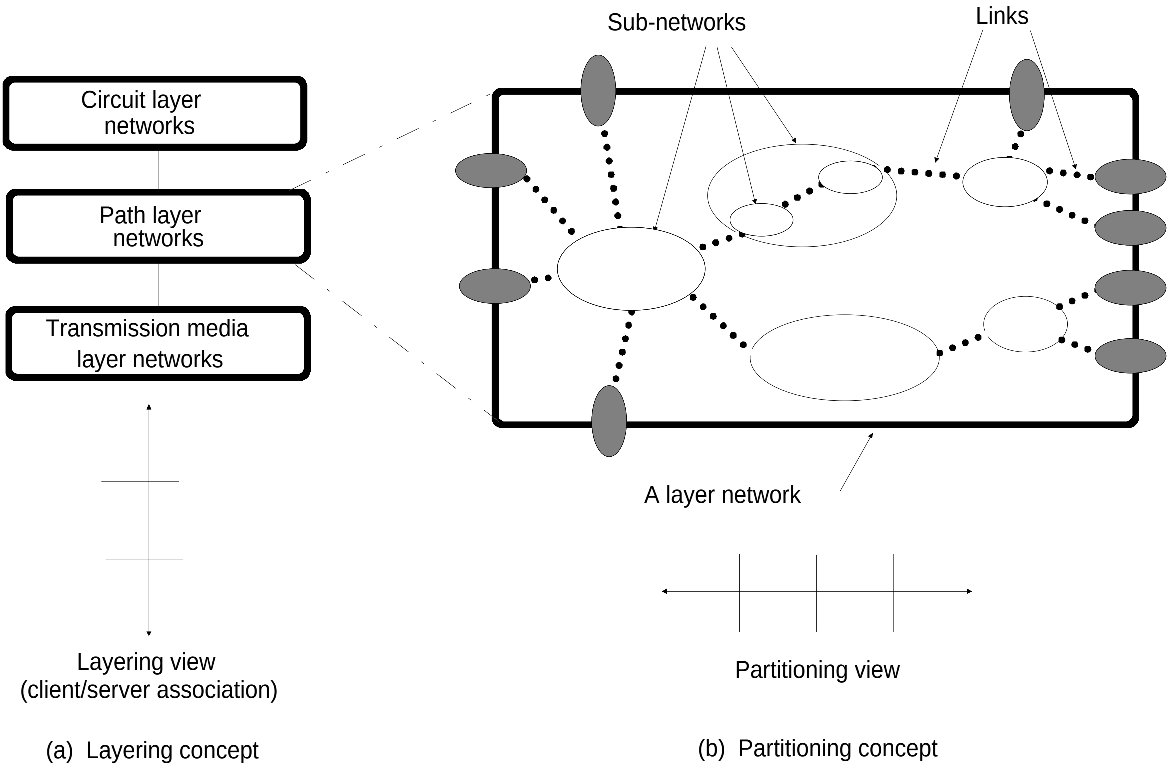


Figure 5: Orthogonal views of layering and partitioning

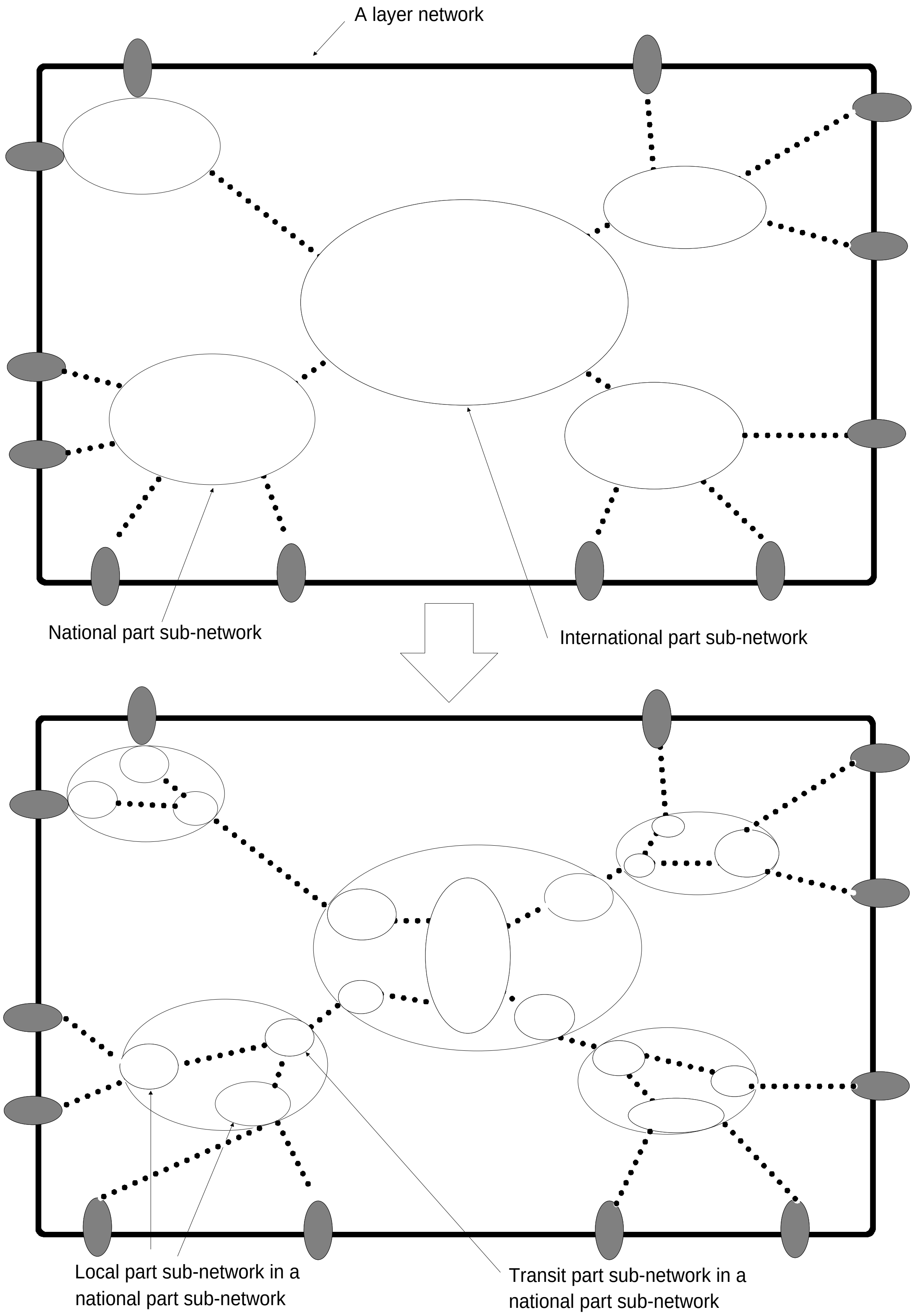
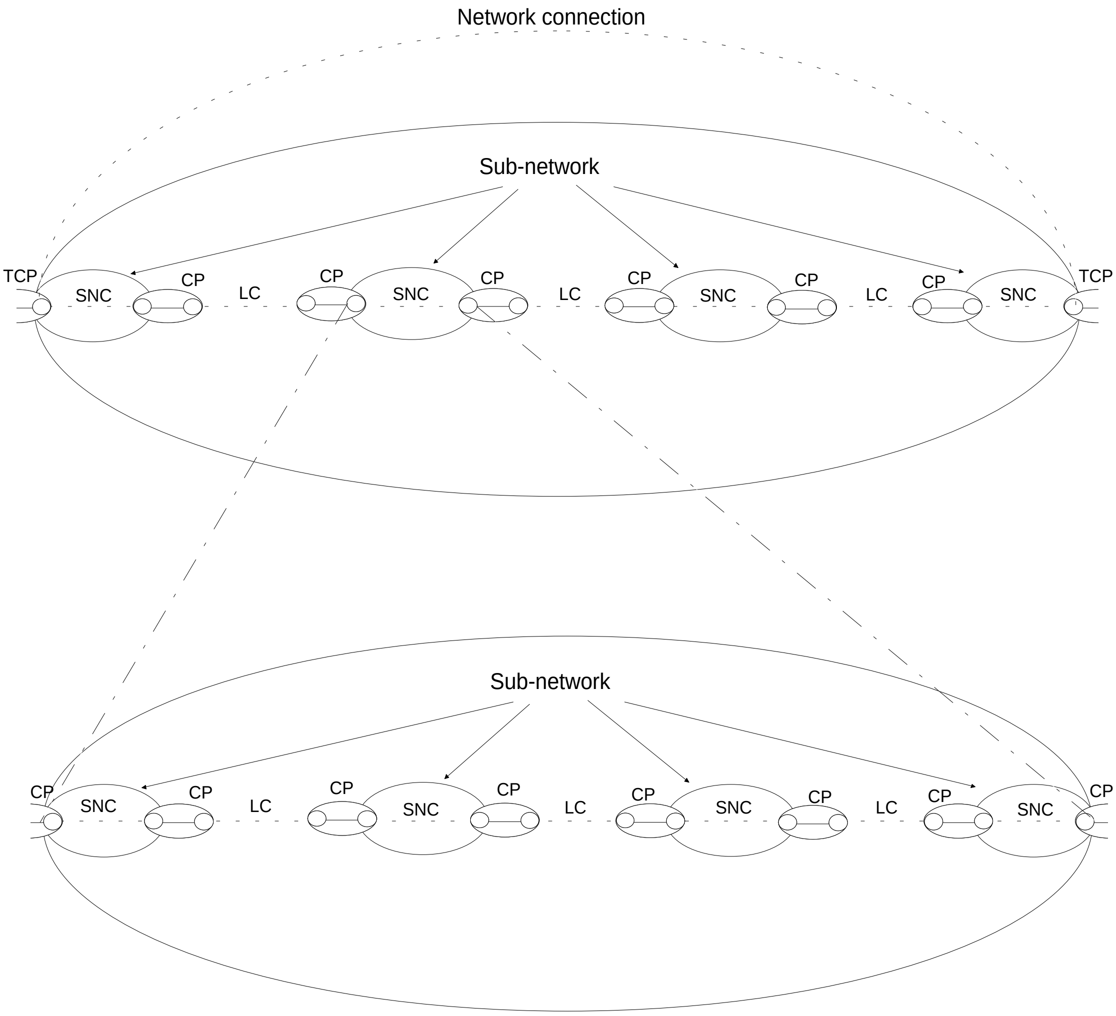


Figure 6: Partitioning of layer networks and sub-networks



LC Link connection
SNC Sub-network connection

Figure 7: Partitioning of a network connection into sub-network connections

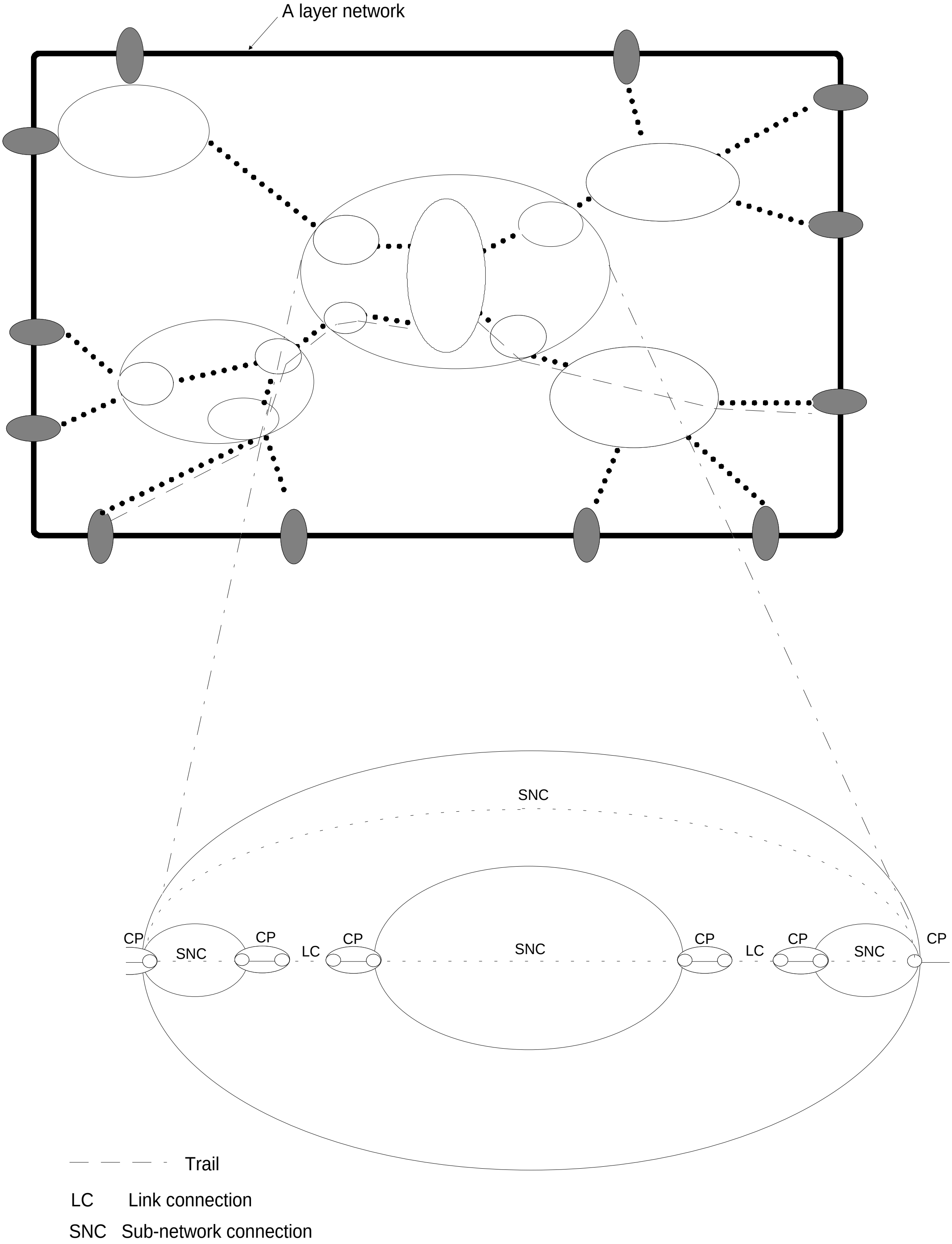


Figure 8: Relationship between partitioning of sub-networks and partitioning of sub-network connections

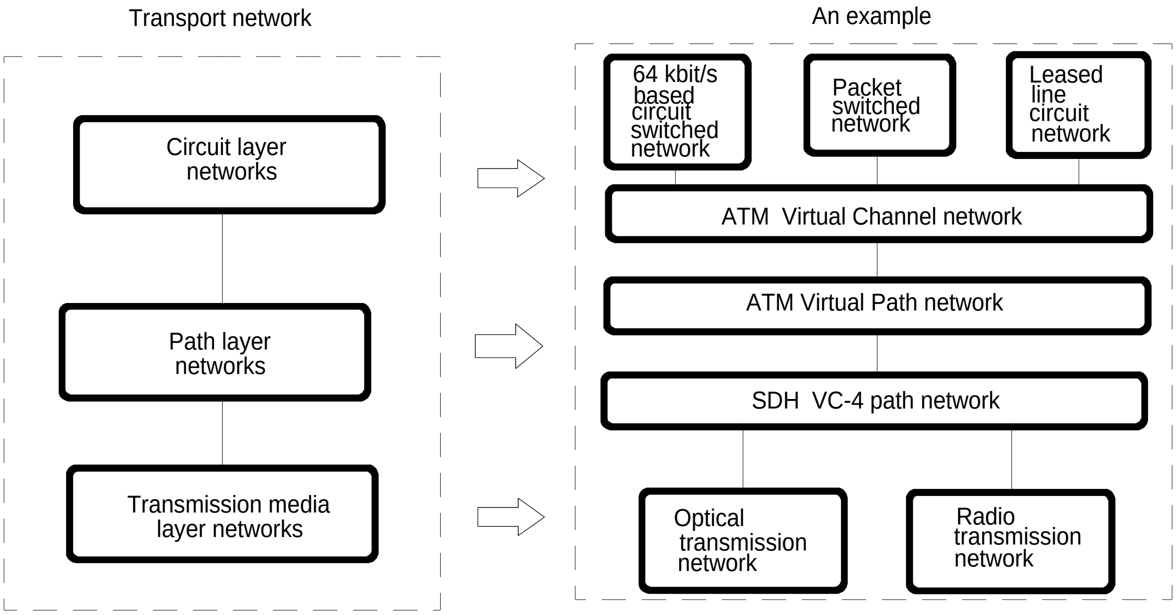
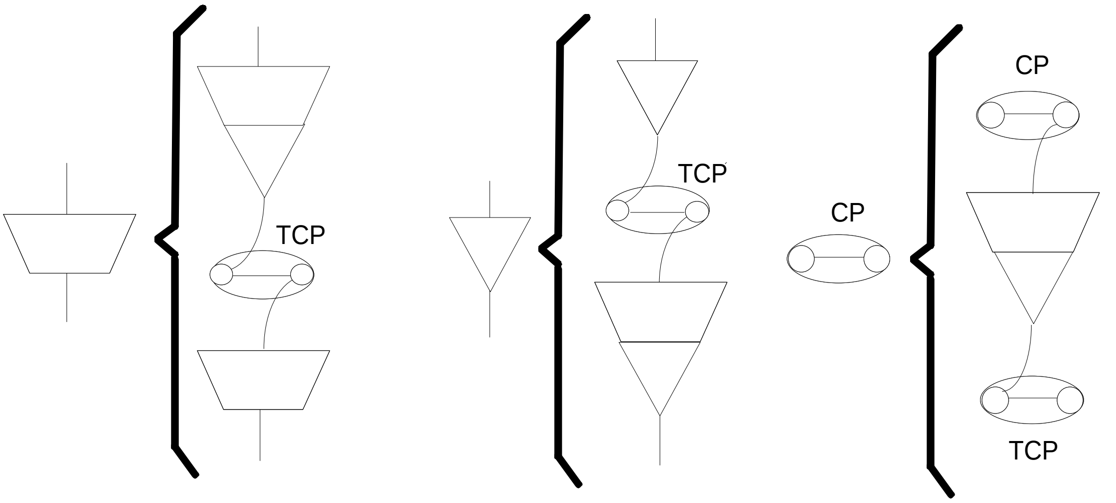


Figure 9: Layered model of the transport network



a) Expansion of the adaptation function

b) Expansion of the termination function

c) Expansion of a connection point

Figure 10: Generation of sub-layers

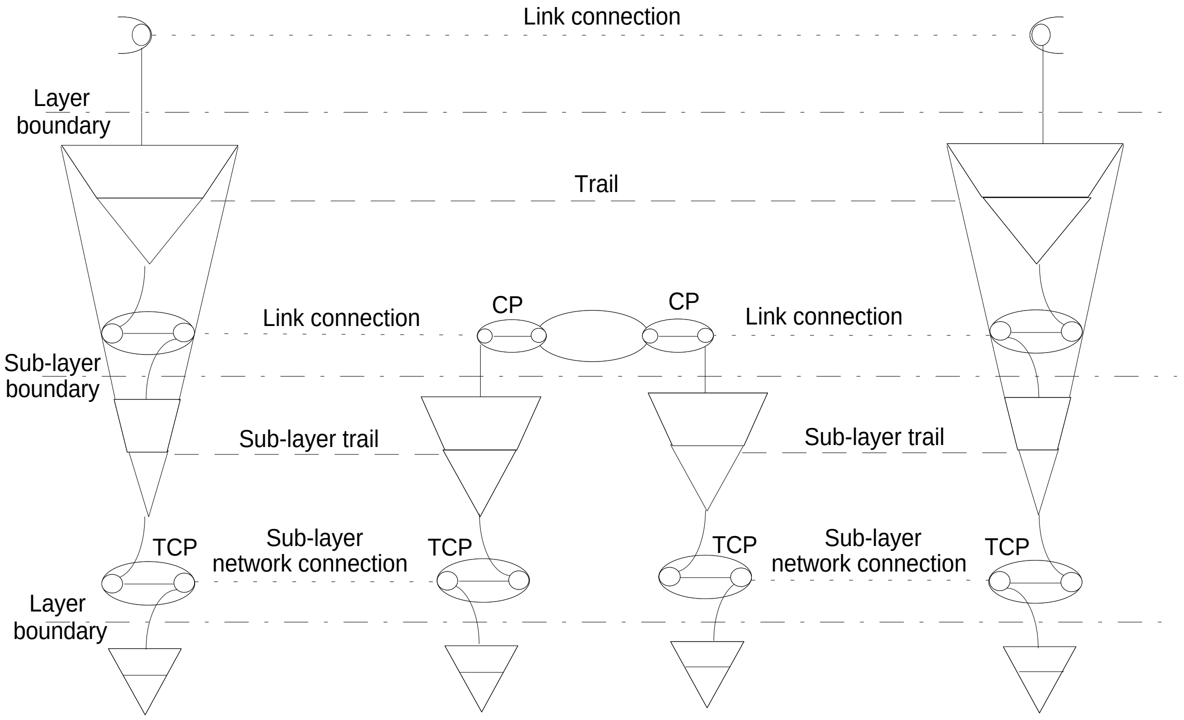


Figure 11: The concept of sub-layering

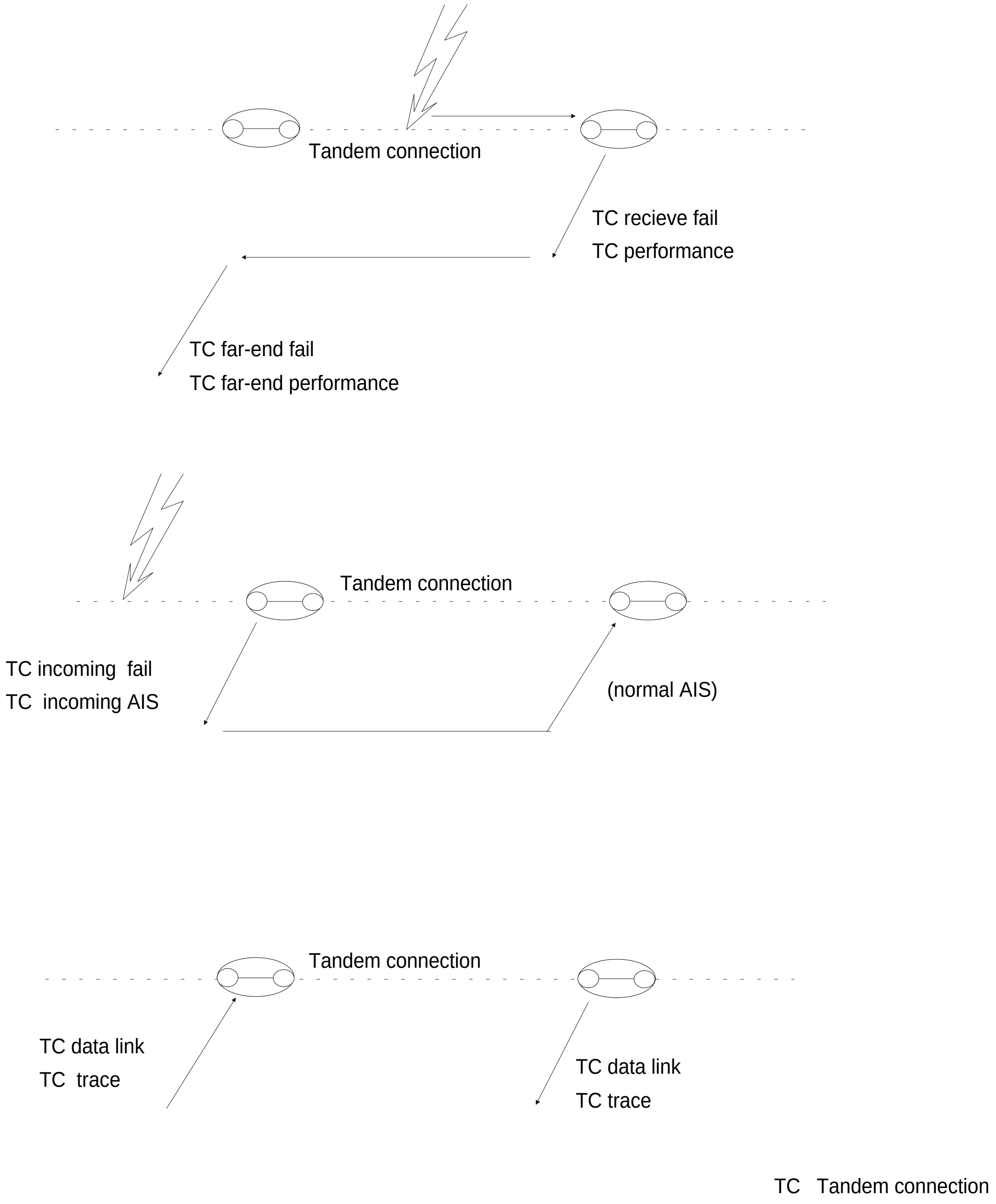


Figure 12: Explanation of tandem connection terms

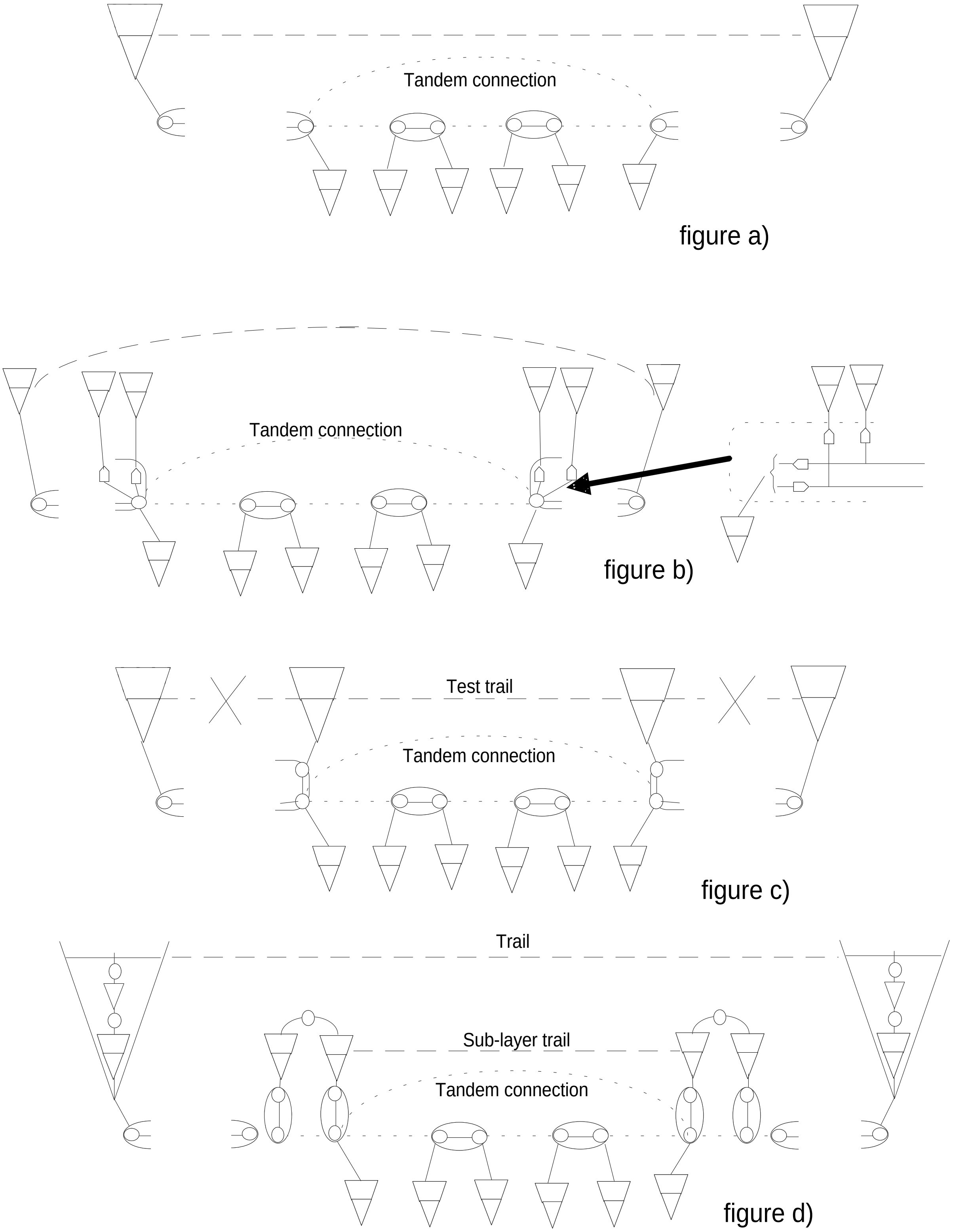
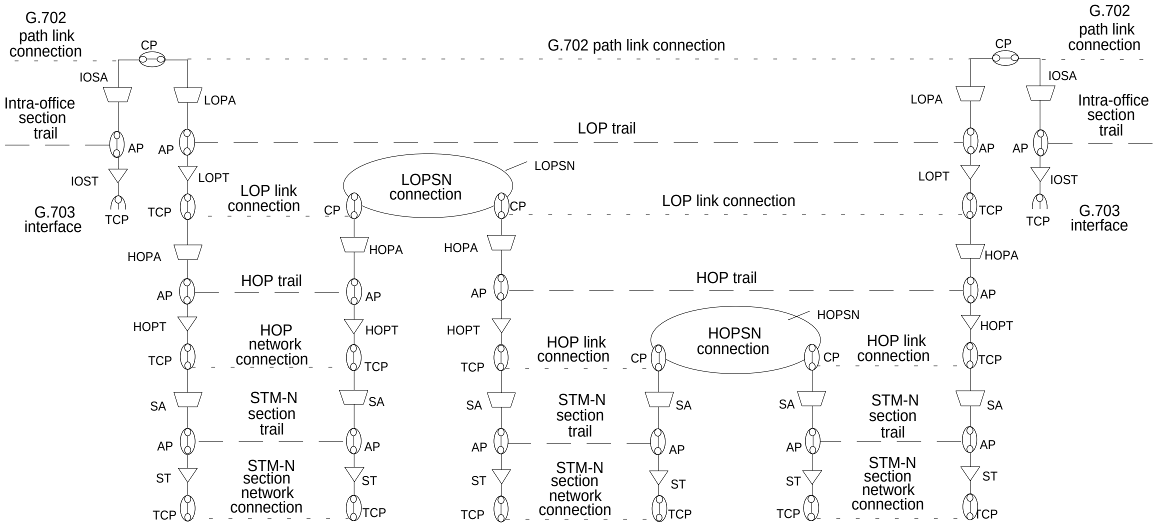


Figure 13: Tandem connection monitoring

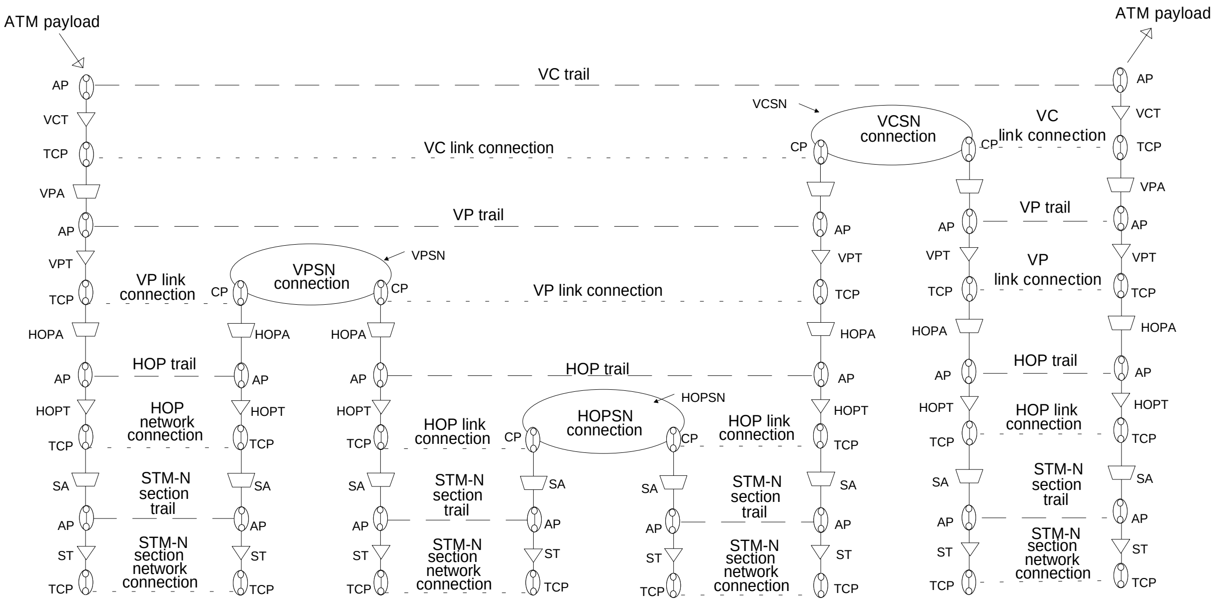


IOST	Intra-office section termination
IOSA	Intra-office section adaptation
LOP	Lower-order path (eg VC-12)
LOPA	Lower-order path adaptation
LOPT	Lower-order path termination
LOPSN	Lower-order path sub-network

HOP	Higher-order path (eg VC-4)
HOPA	Higher-order path adaptation
HOPT	Higher-order path termination
HOPSN	Higher-order path sub-network

SA	STM-N section adaptation
ST	STM-N section termination
AP	Access point
TCP	Termination connection point
CP	Connection point

Figure 14: Application of functional architecture to case of PDH supported on SDH



VP	Virtual path
VPT	Virtual path termination
VPSN	Virtual path sub-network
HOP	Higher-order path (eg VC-4)
HOPA	Higher-order path adaptation
HOPT	Higher-order path termination
HOPSN	Higher-order path sub-network

SA	STM-N section adaptation
ST	STM-N section termination
AP	Access point
TCP	Termination connection point
CP	Connection point

Figure 15: Application of functional architecture to case of ATM supported on SDH

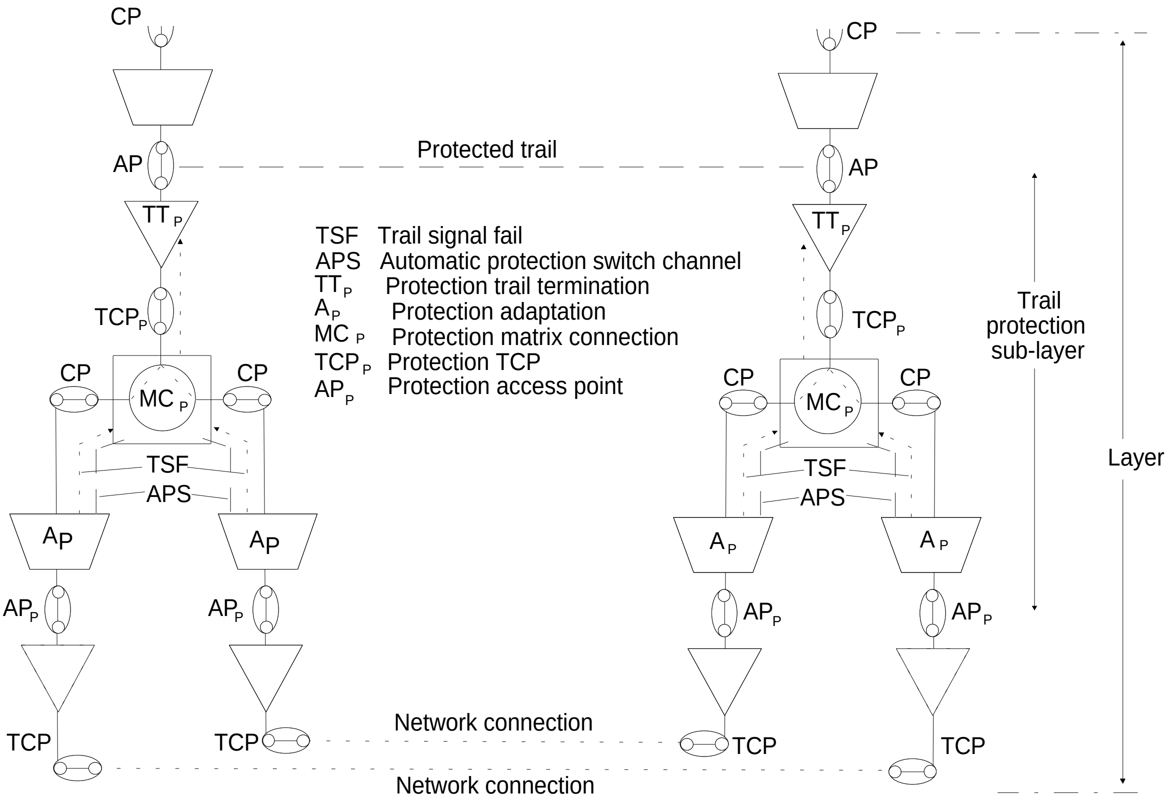


Figure 16: Generic trail protection odel (1+1 protection)

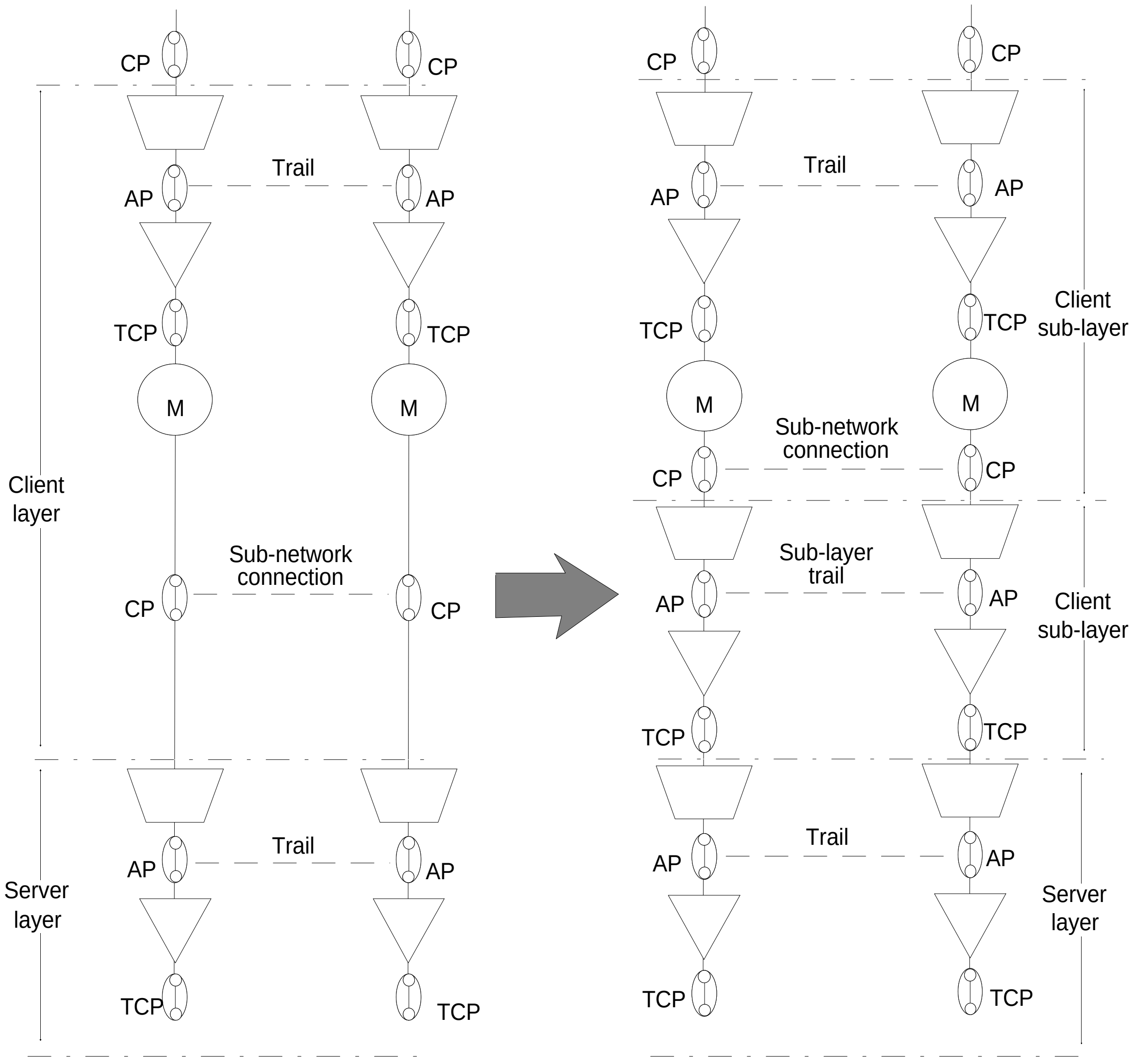
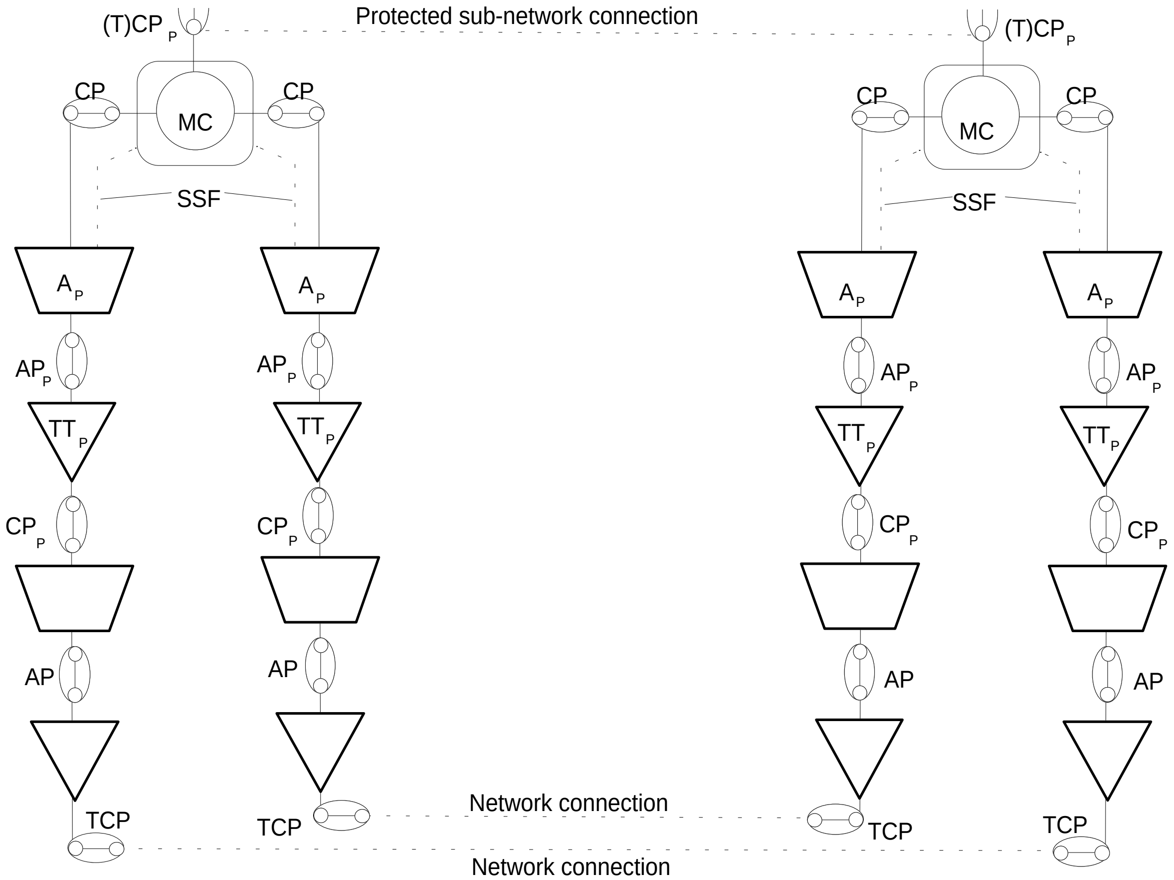
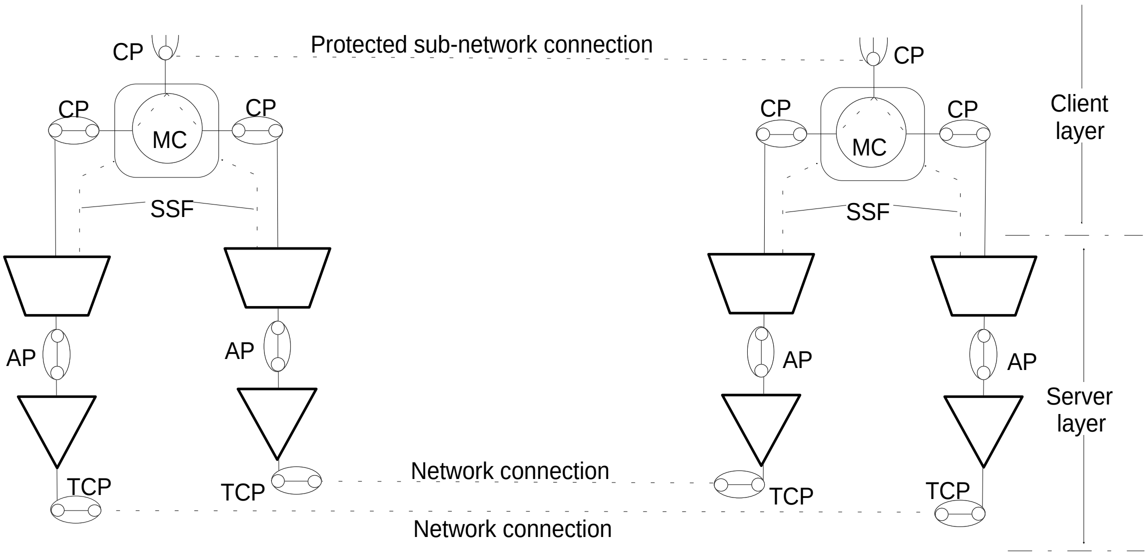


Figure 17: Expansion of connection points to provide sub-network protection



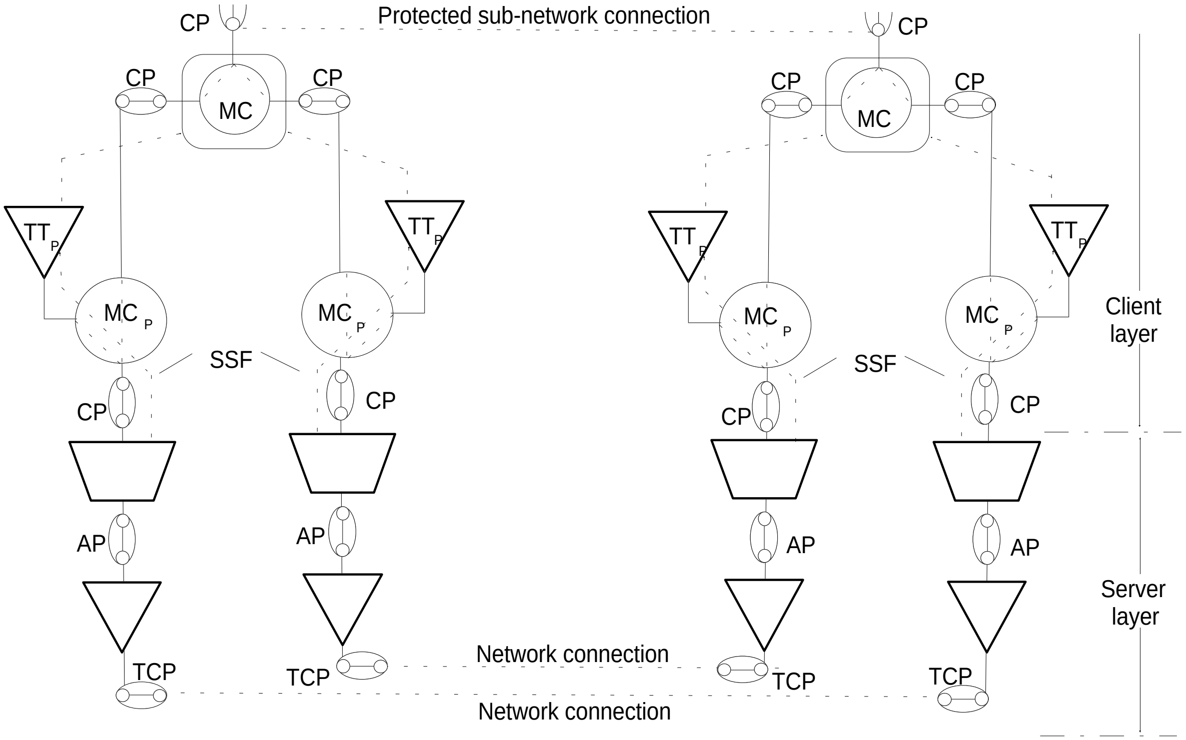
SSF	Server signal fail
TT_P	Protection trail termination
A_P	Protection adaption
MC	Matrix connection
TCP_P	Protection TCP
AP_P	Protection access point
CP_P	Protection connection point

Figure 18: Generic sub-network connection protection model



SSF Server signal fail
MC Matrix connection

Figure 19: Sub-network connection protection with inherent monitoring by means of server signal fail



SSF Server signal fail
MC Matrix connection
MC_P Protection matrix connection
TT_P Protection trail termination

Figure 20: Sub-network connection protection with non-intrusive monitoring

History

Document history	
June 1993	First Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)