INTERNATIONAL TELECOMMUNICATION UNION

ITU-T G.8080/Y.1304

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Amendment 1
(03/2003)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital networks – General aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

Internet protocol aspects – Transport

Architecture for the automatically switched optical network (ASON)

Amendment 1

ITU-T Recommendation G.8080/Y.1304 (2001) – Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DIGITAL TERMINAL EQUIPMENTS	G.7000–G.7999
DIGITAL NETWORKS	G.8000–G.8999
General aspects	**G.8000–G.8099**
Design objectives for digital networks	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Network capabilities and functions	G.8300–G.8399
SDH network characteristics	G.8400–G.8499
Management of transport network	G.8500–G.8599
SDH radio and satellite systems integration	G.8600–G.8699
Optical transport networks	G.8700–G.8799

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation G.8080/Y.1304

Architecture for the automatically switched optical network (ASON)

Amendment 1

Summary

This amendment contains addition material to be incorporated into ITU-T Rec. G.8080/Y.1304, Architecture for the Automatically Switched Optical Network (ASON).

Source

Amendment 1 to ITU-T Recommendation G.8080/Y.1304 (2001) was approved by ITU-T Study Group 15 (2001-2004) under the ITU-T Recommendation A.8 procedure on 16 March 2003.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation G.8080/Y.1304

Architecture for the automatically switched optical network (ASON)

Amendment 1

1) Scope

This amendment provides updated material pertaining to the Architecture of the Automatically Switched Optical Network as described in ITU-T Rec. G.8080/Y.1304.

2) Clause 2 References

No new references are to be added.

3) Clause 3 Definitions

No new definitions are to be added.

4) Abbreviations

Add the following new abbreviations alphabetically:

ACG Access Group Container

DA Discovery Agent

MI Management Information

MO Managed Object

TAP Termination and Adaptation Performer

5) Conventions

This amendment introduces new figures and tables into ITU-T Rec. G.8080/Y.1304. Figures in the original ITU-T Rec. G.8080/Y.1304 are in the form: Figure X/G.8080/Y.1304, where X is a numerical value. In order to avoid the possibility of duplicate figure and table references, additional figures provided in this amendment will take the form Figure X.Y/G.8080/Y.1304, where Y is a numerical index and represents the location of the new figure relative to the original figure in ITU-T Rec. G.8080/Y.1304. For example, Figure 5.1 represents a figure in this amendment that would occur as the first figure following Figure 5 in the main body of the Recommendation.

6) Clarifications to terminology usage in ITU-T Rec. G.8080/Y.1304

Based on review of the original text of ITU-T Rec. G.8080/Y.1304, it was noted that it is necessary to resolve differences in the usage of multiple terms such as created, allocated, assigned, or setup. This was not felt to represent a difficulty for the initial version of ITU-T Rec. G.8080/Y.1304, but should be clarified. The following are changes to the text in ITU-T Rec. G.8080/Y.1304:

Clause 5.1.1 Call control

Change the term "established" *to* "setup".

Clause 5.1.3 Connection control

Change "set-up" *to* "setup".

Clause 6.3 Topology discovery

Change the second sentence in the second to last paragraph form:

"If test connections are used, the discovery process may establish..."

to

"If test connections are used, the discovery process may setup…".

Clause 7.3.1 Connection Controller (CC) component

Change "set-up/s" *to* "setup" *in several occurrences in this clause.*

In the final paragraph, change "teardown" *to* "release".

Clause 7.3.2 Routing Controller (RC) component

Change "set-up" *to* "setup".

Clause 7.3.3 Link Resource Manager (LRMA and LRMZ) component

In the first sentence, change the term "deallocation" *to* "unallocation".

Clause 7.3.3.1 LRMA

Change all the occurrences of "deallocation" *to* "unallocation".

Clause 7.3.5.1 Calling/Called part call controller

In the sentence starting "**Call Request**: This …"*, change the term* "cessation" *to* "release".

In the sentence starting "**Call Teardown**: This …"*, change the phrase* "confirm teardown" *to* "confirm release".

Clause 7.3.5.2 Network call controller

Change the second sentence of the paragraph starting "**Call Request Accept**: …"*, as follows:*

"This interface also confirms or rejects call setup request."

In the paragraph starting "**Connection Request Out**: ..."*, add the term* "setup" *as follows:*

"… to place a connection setup request...".

7) Clause 5 Overview

7.1) *Add the following new paragraph as the second and last paragraph to clause 5.1:*

Call control is provided at the ingress to the network (i.e., UNI reference point) and may also be provided at gateways between domains (i.e., E-NNI reference point). The functions performed by the call controllers at domain boundaries are defined by the policies associated by the interactions allowed between the domains. Policies are established by the operator. As such, an end-to-end call is considered to consist of multiple call segments, depending on whether the call traverses multiple domains. This allows for flexibility in the choice of signalling, routing and recovery paradigms in different domains.

7.2) *Add the following new clause 5.2:*

5.2 Interaction between control, transport and management planes

Figure 1 illustrates the general relationships between the control, management and transport planes. Each plane is autonomous, but some interaction will occur. The following provides further details on the interactions between the various planes.

5.2.1 Management – Transport interaction

The management plane interacts with transport resources by operating on a suitable information model, which presents a management view of the underlying resource. The objects of the information model are physically located with the transport resource, and interact with that resource via the Management Information (MI) interfaces of the layer specific functional model. These interfaces should be collocated with the managed object and the control component.

5.2.2 Control – Transport interaction

Only two architectural components have a strong relationship to a physical transport resource.

At the lower limit of recursion, the Connection Controller (CC) provides a signalling interface to control a connection function. This component is physically located with the connection function and all further hardware details are hidden. However, given the limited information flow, a new protocol may be useful to optimize this communication. The Termination and Adaptation Performer (TAP) is physically located with the equipment that provides adaptation and termination functions, and provides a control plane view of link connections. The TAP hides the interaction with the hardware.

5.2.3 Management – Control interaction

Clause 7.1 states that every component has a set of special interfaces to allow for monitoring of the component operation, and dynamically setting policies and affecting internal behaviour. These interfaces are equivalent to the MI interface of the transport functional model, and allow the component to present a view to a management system, and to be configured by a management system.

The management plane interacts with control components by operating on a suitable information model which presents a management view of the underlying component. The objects of the information model are physically located with a control component, and interact with that component via the monitor and configuration interfaces of that component. These interfaces should be collocated with the managed object and the control component.

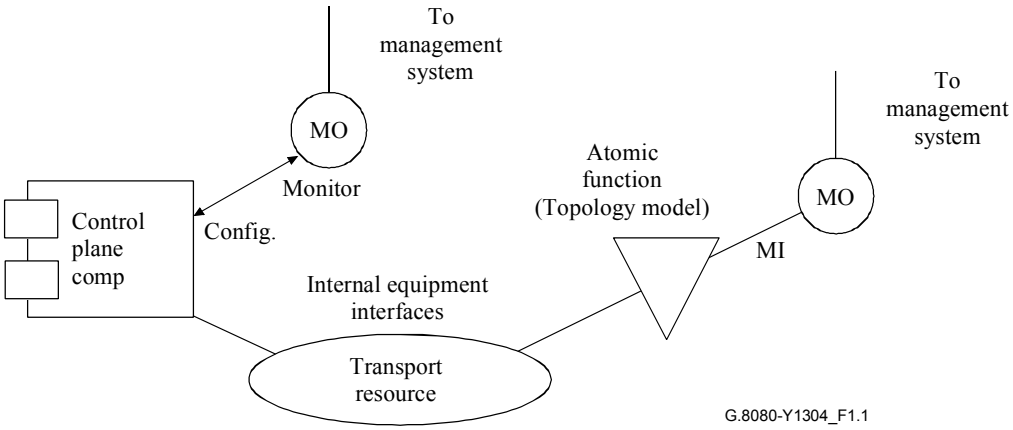

Figure 1.1/G.8080/Y.1304 – Management/transport plane interactions with transport resources

At the bottom of Figure 1.1 is a set of physical transport resources, which represent the physical reality of the equipment. This reality is described in terms of G.805 atomic functions. Managed objects (MO), which represent the external management view of the equipment, interact with the functional model specified in equipment recommendations via the MI reference points, which are also completely within the equipment. Note that the managed object represents the management view regardless of the management protocol used. The information is independent of the protocol used.

From the control plane view, control plane components operate directly on the G.805 functions, so control plane operation appears autonomous to the management plane. Likewise, management plane operations appear autonomous to the control plane. This is exactly the same situation we have when multiple managers manage equipment. Each manager is unaware of each other's existence, and simply sees autonomous equipment behaviour. Although the information presented to the control plane is similar to that presented to management, it is not identical to the MI information. Control plane information overlaps the MI data because the control plane requires some but not all management information. For example, restoration is likely to be triggered by the same conditions that normally trigger protection actions.

Component specific managed objects present a management view of control plane components via the monitor interfaces on the component. It is critical to realize that this is the view of the manageable aspects of the component, and not a view of the transport resource, which is obtained via the management view.

8) Clause 6 Transport resources and their organization

Add the following new clauses 6.2.1, 6.2.2, 6.4 and 6.5 to clause 6:

6.2.1 Aggregation of links and routing areas

Figure 5.1 illustrates the relationships between routing areas and subnetwork point pools (SNPP links). Routing areas and SNPP links may be related hierarchically. In the example, routing area A is partitioned to create a lower level of routing areas, B, C, D, E, F, G and interconnecting SNPP links. This recursion can continue as many times as necessary. For example, routing area E is further partitioned to reveal routing areas H and I. In the example given, there is a single top level routing area. In creating a hierarchical routing area structure based upon "containment" (in which the lower level routing areas are completely contained within a single higher level routing area),

only a subset of lower level routing areas, and a subset of their SNPP links are on the boundary of the higher level routing area. The internal structure of the lower level is visible to the higher level when viewed from inside of A, but not from outside of A. Consequently, only the SNPP links at the boundary between a higher and lower level are visible to the higher level when viewed from outside of A. Hence, the outermost SNPP links of B and C and F and G are visible from outside of A, but not the internal SNPP links associated with D and E or those between B and D, C and D, C and E or between E and F or E and G. The same visibility applies between E and its subordinates H and I. This visibility of the boundary between levels is recursive. SNPP link hierarchies are therefore only created at the points where higher layer routing areas are bounded by SNPP links in lower level routing areas.

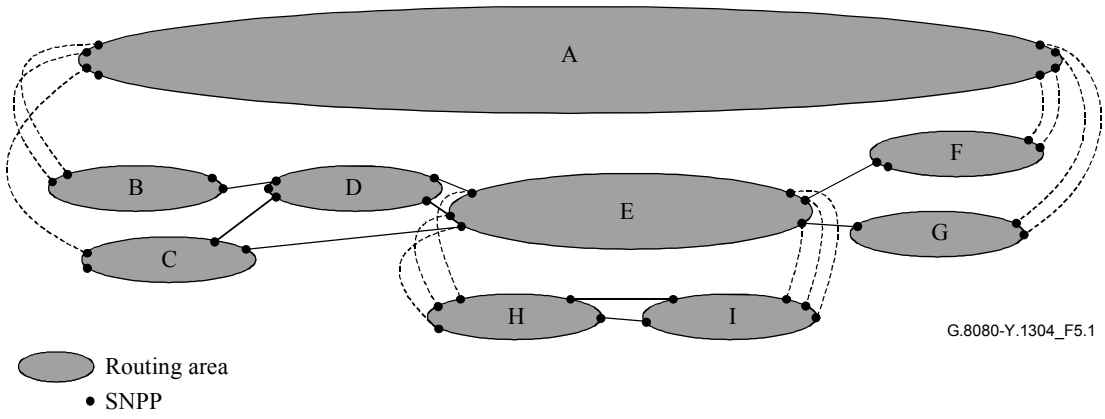

Figure 5.1/G.8080/Y.1304 – Example of a routing area hierarchy and SNPP link relationships

Subnetwork points are allocated to an SNPP link at the lowest level of the routing hierarchy and can only be allocated to a single subnetwork point pool at that level. At the routing area hierarchy boundaries, the SNPP link pool at a lower level is fully contained by an SNPP link at a higher level. A higher level SNPP link pool may contain one or more lower level SNPP links. In any level of this hierarchy, an SNPP link is associated with only one routing area. As such, routing areas do not overlap at any level of the hierarchy. SNPP links within a level of the routing area hierarchy that are not at the boundary of a higher level may be at the boundary with a lower level thereby creating an SNPP link hierarchy from that point (e.g., routing area E). This provides for the creation of a containment hierarchy for SNPP links.

6.2.2 Relationship to links and link aggregation

A number of SNP link connections within a routing area can be assigned to the same SNPP link if, and only if, they go between the same two subnetworks. This is illustrated in Figure 5.2. Four subnetworks, SNa, SNb, SNc and SNd and SNPP links 1, 2 and 3 are within a single routing area. SNP link connections A and B are in the SNPP link 1. SNP link connections B and C cannot be in the same SNPP link because they do not connect the same two subnetworks. Similar behaviour also applies to the grouping of SNPs between routing areas.

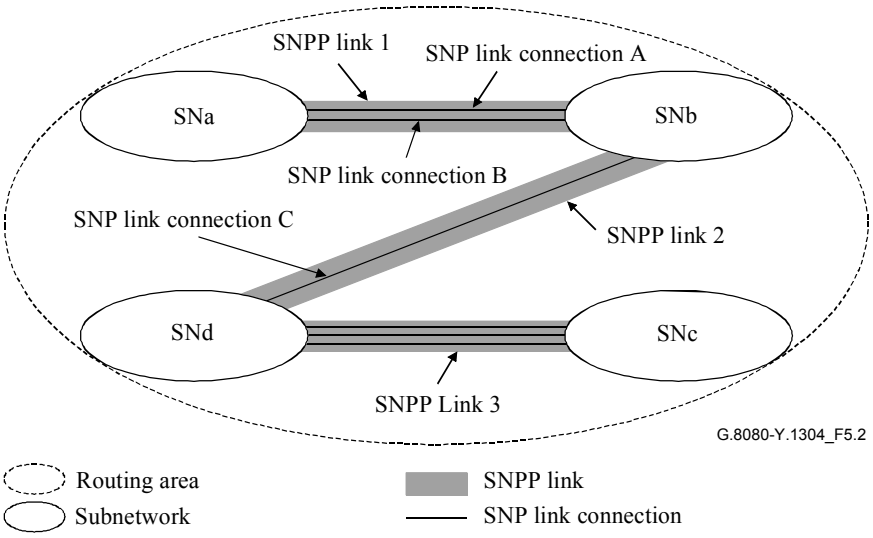

Figure 5.2/G.8080/Y.1304 – SNPP link relationship to subnetworks

Figure 5.3 shows three routing areas, RA-1, RA-2 and RA-3 and SNPP links 1 and 2. SNP link connections A, B and C cannot be in the same SNPP link because more than two routing areas are found in their endpoints. SNP link connections A and B are not equivalent to SNP link connection C for routing from Routing Area 3 (RA-3).

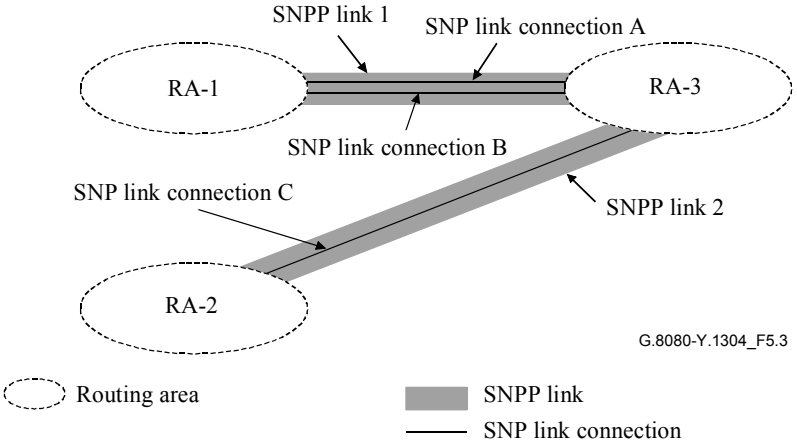

Figure 5.3/G.8080/Y.1304 – SNPP link relationships to routing areas

SNP link connections between two routing areas, or subnetworks, can be grouped into one or more SNPP links. Grouping into multiple SNPP links may be required:

– if they are not equivalent for routing purposes with respect to the routing areas they are attached to, or to the containing routing area;

– if smaller groupings are required for administrative purposes.

There may be more than one routing scope to consider when organizing SNP link connections into SNPP links. In Figure 5.4, there are two SNP link connections between routing areas 1 and 3. If those two routing areas are at the top of the routing hierarchy (there is therefore no single top level routing area), then the routing scope of RA-1 and RA-3 is used to determine if the SNP link connections are equivalent for the purpose of routing.

The situation may, however, be as shown in Figure 5.4. Here RA-0 is a containing routing area. From RA-0's point of view, SNP link connections A and B could be in one (a) or two (b) SNPP links. An example of when one SNPP link suffices is if the routing paradigm for RA-0 is step-by-step. Path computation sees no distinction between SNP link connection A and B as a next step to get from say RA-1 to RA-2.

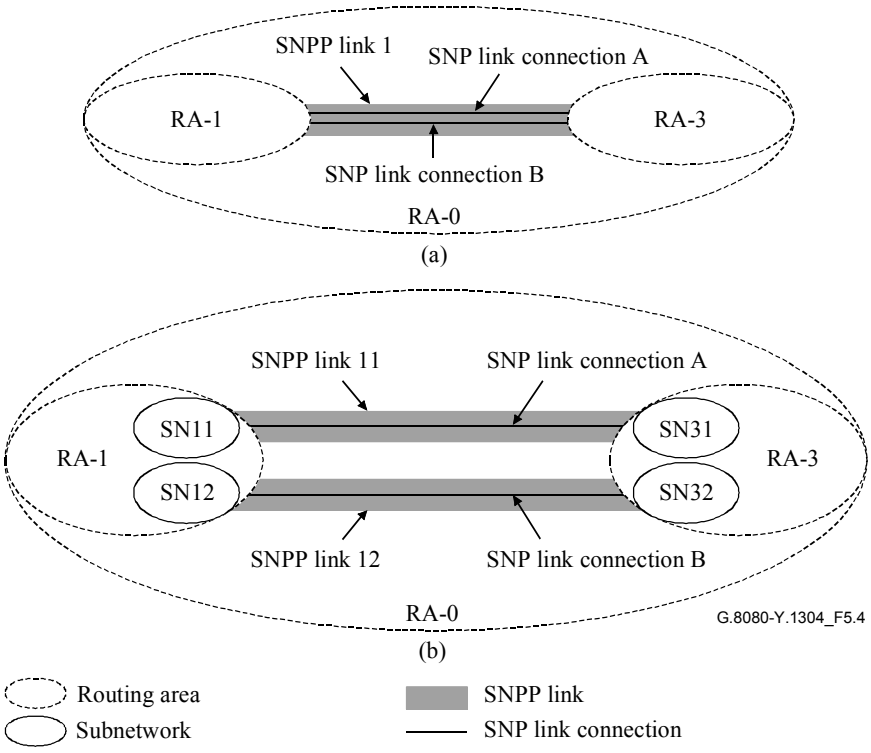

Figure 5.4/G.8080/Y.1304 – Routing scope

From RA-1 and RA-3's point of view, though the SNP link connections may be quite distinct from a routing point of view as choosing SNP link connection, A may be more desirable than SNP link connection B for cost, protection or other reason. In this case, placing each SNP link connection into its own SNPP link meets the requirement of "equivalent for the purpose of routing". Note that in Figure 5.4, SNPP link 11, Link 12 and Link 1 can all coexist.

6.4 Domains

A domain represents a collection of entities that are grouped for a particular purpose. ITU-T Rec. G.805 defines two particular forms, the administrative domain and the management domain. This concept can also be applied in the control plane in the form of a control domain. The entities that are grouped in a control domain are components of the control plane.

A control domain is an architectural construct that encapsulates and hides the detail of a distributed implementation of a particular group of architectural component of one or more types. It allows for the description of a group of distributed components in such a way that the group can be represented by distribution interfaces on a single entity, the domain, that has identical characteristics to that of the interfaces of the original component distribution interfaces. The nature of the information exchanged between control domains captures the common semantics of the information exchanged between component distribution interfaces, while allowing for different representations inside the domain.

Generally, a control domain is derived from a particular component type, or types, that interact for a particular purpose. For example, routing (control) domains are derived from routing controller components whilst a rerouting domain is derived from a set of connection controller and network call controller components that share responsibility for the rerouting/restoration of connections/calls that traverse that domain. In both examples, the operation that occurs, routing or rerouting, is contained entirely within the domain. In this Recommendation, control domains are described in relation to components associated with a layer network.

As a domain is defined in terms of a purpose, it is evident that domains defined for one purpose need not coincide with domains defined for another purpose. Domains of the same type are restricted in that they may:

- fully contain other domains of the same type, but do not overlap;
- border each other;
- be isolated from each other.

An example of the relationships between components, domains and reference points is provided in Figure 6.3 which shows a domain, B, and its relationship to domains A, C and D. Each domain is derived from a component of type Z. The internal structure and interactions may be different in each domain, e.g., they may use different federation models.

The same example is shown in Figure 6.4 with the relationships between components, domains and interfaces. The components interact via their protocol controllers, using protocol I on the I-PCs and protocol E on the E-PCs. It is also possible for the protocol used internal to A, for example, to be different to that used in B, and the protocol used between B and C to be different to that between A and B. The I-NNI interfaces are located between protocol controllers within domains whilst E-NNI interfaces are located on protocol controllers between domains.

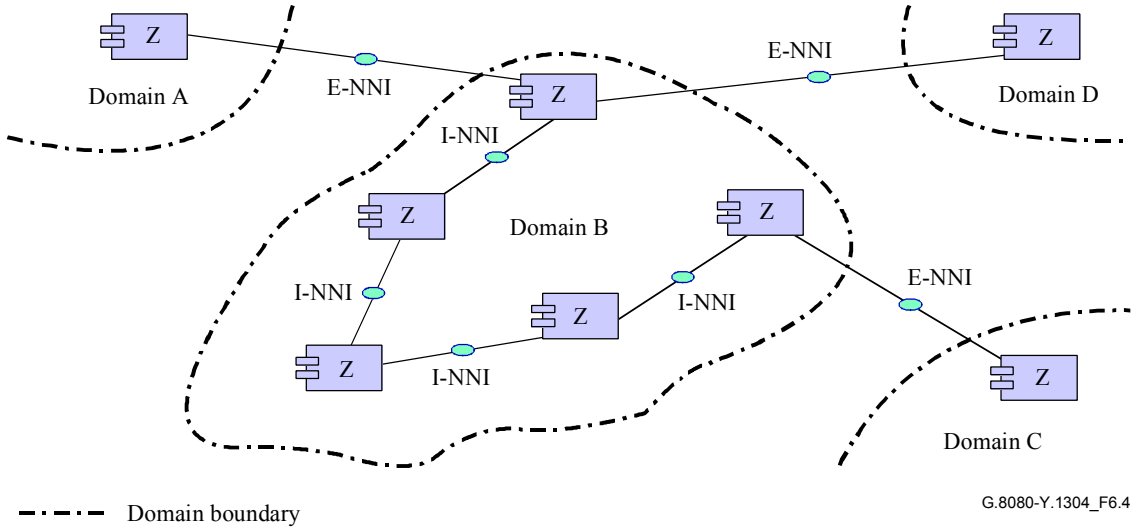

Figure 6.4/G.8080/Y.1304 – Relationship between domains, protocol controllers and reference points

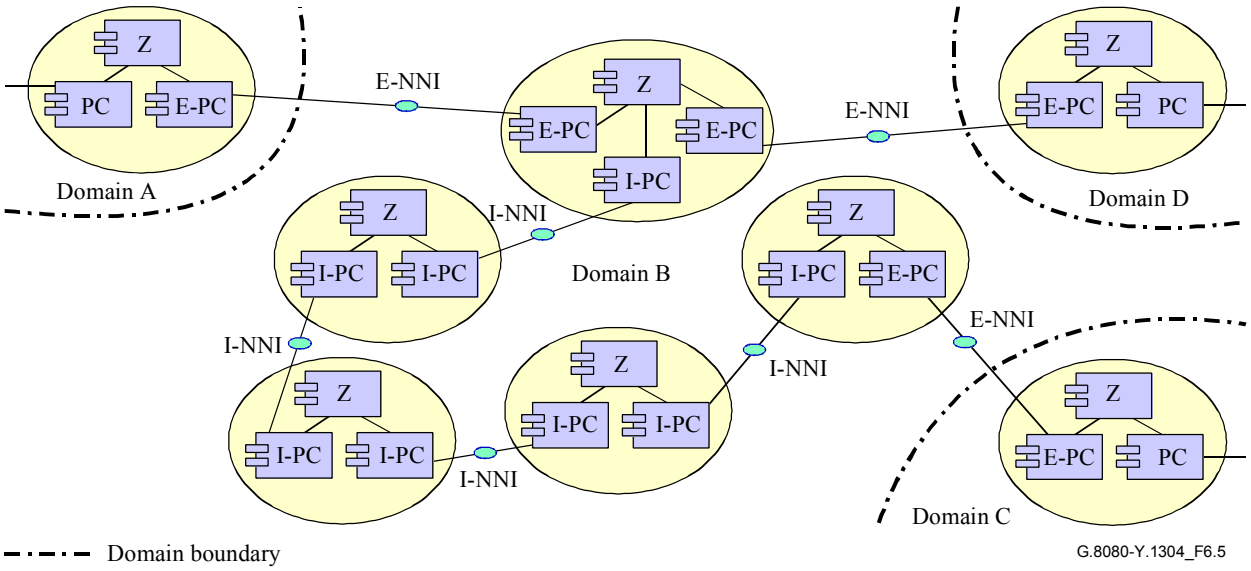

Figure 6.5/G.8080/Y.1304 – Relationship between domains, protocol controllers and interfaces

6.4.1 Relationship between control domains and control plane resources

The components of a domain may, depending on purpose, reflect the underlying transport network resources. A routing domain may, for example, contain components that represent one or more routing areas at one or more levels of aggregation, depending upon the routing method/protocol used throughout the domain. If a routing domain contains more than one routing protocol, the aggregation of routing areas can be different for each routing protocol reflecting different views of the underlying resources.

6.4.2 Relationship between control domains, interfaces and reference points

I-NNI and E-NNI interfaces are always between protocol controllers. The protocols running between protocol controllers may or may not use SNPP links in the transport network under control and, as such, it is incorrect to show I-NNI and E-NNI interfaces on SNPP links.

I-NNI and E-NNI reference points are between components of the same type, where the component type is not a protocol controller, and represents primitive message flows (see clause 7).

In a diagram showing only domains and the relationships between them (and not revealing the internal structure of the domains), the information transfer is assumed to be over a reference point.

6.5 Multi-layer aspects

The description of the control plane can be divided into those aspects related to a single layer network, such as routing, creation and deletion of connections, etc., and those that relate to multiple layers. The client/server relationship between layer networks is managed by means of the Termination and Adaptation Performers (see clause 7.3.7). The topology and connectivity of all of the underlying server layers is not explicitly visible to the client layer, rather these aspects of the server layers are encapsulated and presented to the client layer network as an SNPP link. Where connectivity cannot be achieved in the client layer as a result of an inadequate resources, additional resources can only be created by means of new connections in one or more server layer networks, thereby creating new SNP link connections in the client layer network. This can be achieved by modifying SNPs from potential to available, or by adding more infrastructure as an output of a planning process. The ability to create new client layer resource, by means of new connections in one or more server layer networks, is therefore a prerequisite to providing connectivity in the client layer network. The model provided in this Recommendation allows this process to be repeated in each layer network. The timescale at which server layer connectivity is provided for the creation of

client layer topology, is subject to a number of external constraints (such as long term traffic forecasting for the link, network planning and financial authority) and is operator specific. The architecture supports server layer connectivity being created in response to a demand for new topology from a client layer by means of potential SNPs which need to be discovered.

9) Clause 7 Control plane architecture

9.1) *Add the following new text at the end of the introductory paragraphs to clause 7:*

Special components are defined in this Recommendation and are provided to allow for implementation flexibility. These components are Protocol Controllers and Port Controllers. The detail of the interfaces of these and other components are provided in other technology-specific Recommendations.

Protocol Controllers are provided to take the primitive interface supplied by one or more architectural components, and multiplex those interfaces into a single instance of a protocol. This is described in 7.4 and illustrated in Figure 23. In this way, a Protocol Controller absorbs variations among various protocol choices, and the architecture remains invariant. One, or more, protocol controllers are responsible for managing the information flows across a reference point.

Policy Ports are provided to apply rules to system interfaces. Their purpose is to provide a secure environment for the architectural components to execute in, thereby isolating the architectural components from security considerations. In particular, they isolate the architecture from distribution decisions made involving security issues. This is described in 7.2.1 and Figure 8.

9.2) *Add the following new clauses to clause 7:*

7.3.6 Discovery Agent (DA)

The federation of Discovery Agents operates in the transport plane name space, and provides for separation between that space and the control plane names. The federation has knowledge of Connection Points (CPs) and Termination Connection Points (TCPs) in the network, while a local DA has knowledge of only those points assigned to it. Discovery coordination involves accepting potential hints about pre-existing CPs and link connections. The DA holds the CP-CP link connections to enable SNP-SNP link connections to be bound to them later. The resolution interfaces assist in discovery by providing name translation from global TCP handles to the address of the DA responsible for the point, together with the local name of the TCP. Note that hints come from cooperation with other components, or from external provisioning systems.

Discovery agents have no private equipment interfaces, and can be located on any suitable platform.

Table 7.1/G.8080/Y.1304 – Discovery Agent (DA) component interface

Input interface	Basic input parameters	Basic return parameters
Coordination In		
Hints in	CP pairs	
Resolution Request	TCP Name	
Output interface	**Basic output parameters**	**Basic return parameters**
Coordination Out		
CP link connection	CP pair	
Resolution Result		DA DCN Address, TCP Index

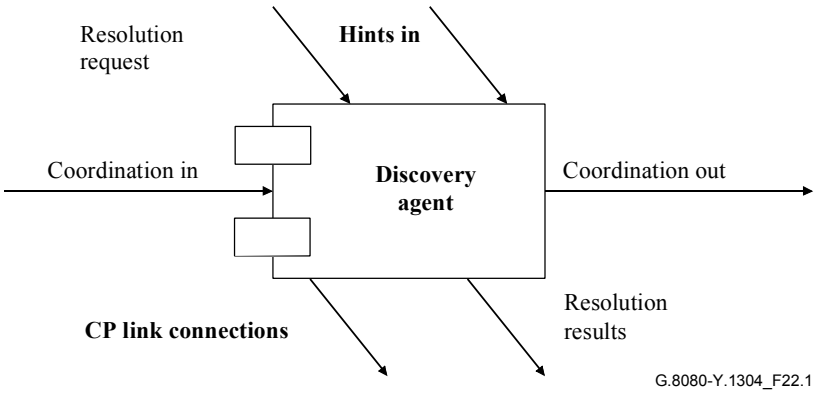

Figure 22.1/G.8080/Y.1304 – Discovery agent component

7.3.7 Termination and adaptation performers

The Termination and Adaptation Performer (TAP) operates at two different times and provides two different functions.

When SNP link connections are bound to their corresponding CP link connection, the TAP is responsible for holding the SNP-CP binding. A local TAP cooperates with a remote TAP to coordinate any variable adaptation or other coordination required when forming the CP link connections.

During connection setup, a pair of TAPs cooperate to coordinate any adaptation setup required by the link connection, provides link connection transmission status information and accepts link connection state information to ensure that the management plane indications are consistent. Management plane consistency includes ensuring that the alarm state of the link connection is consistent, so that spurious alarms are neither generated nor reported.

The TAP is physically located on the equipment providing the adaptation and termination function. It provides a control plane view of the link connection, and hides any hardware and technology specific details of the adaptation and termination control.

Table 7.2/G.8080/Y.1304 – Termination and Adaptation Performer (TAP) component interface

Input interface	**Basic input parameters**	**Basic return parameters**
LC connection State (SNP-SNP)	Enum: In service, Out of Service	
Coordination In	Technology dependent	
Output interface	**Basic output parameters**	**Basic return parameters**
LC transport state (SNP-SNP)	Enum: Up, Down	
Coordination Out	Technology dependent	Technology dependent
Control	Hardware specific	Hardware specific

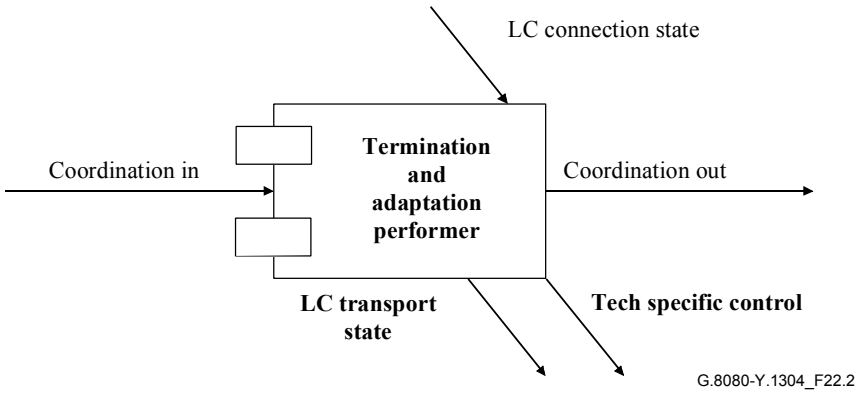

Figure 22.2/G.8080/Y.1304 – Termination and adaptation performer component

7.3.8 Discovery process

The generic process of discovery is split into two separate and distinct times and name spaces The first part takes place entirely in the transport plane name space (CPs and CTPs).

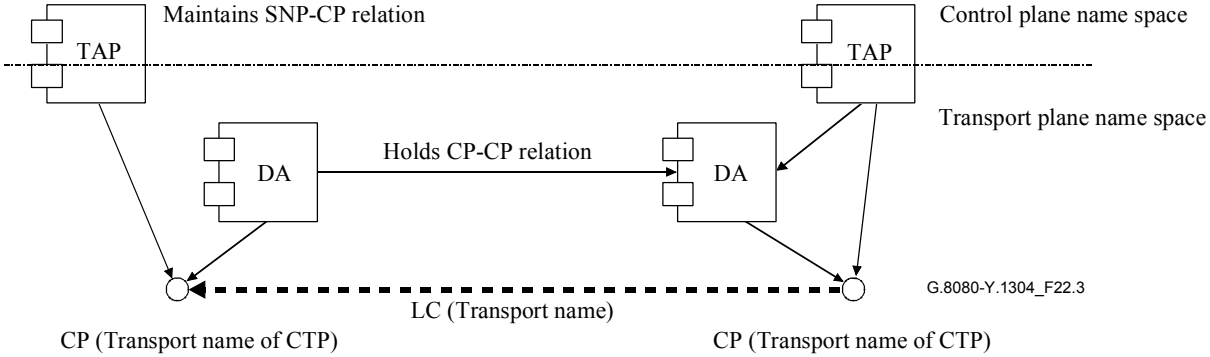

Figure 22.3/G.8080/Y.1304 – Discovery of transport link connections (LC)

The DA operates entirely within the transport name space, and is responsible for holding the transport name of the link connection (associated with each CP). This information may be obtained by using transport mechanisms invisible to the control plane name space, by holding previously obtained relation information or by provisioning. The DA assists in an underlying automatic discovery process by cooperatively resolving transport CP names among all the DAs in the network, thus enabling the DAs (or other components) responsible for each end of the transport link connection to communicate about that link connection.

The second part takes place entirely within the control plane name space (SNPs).

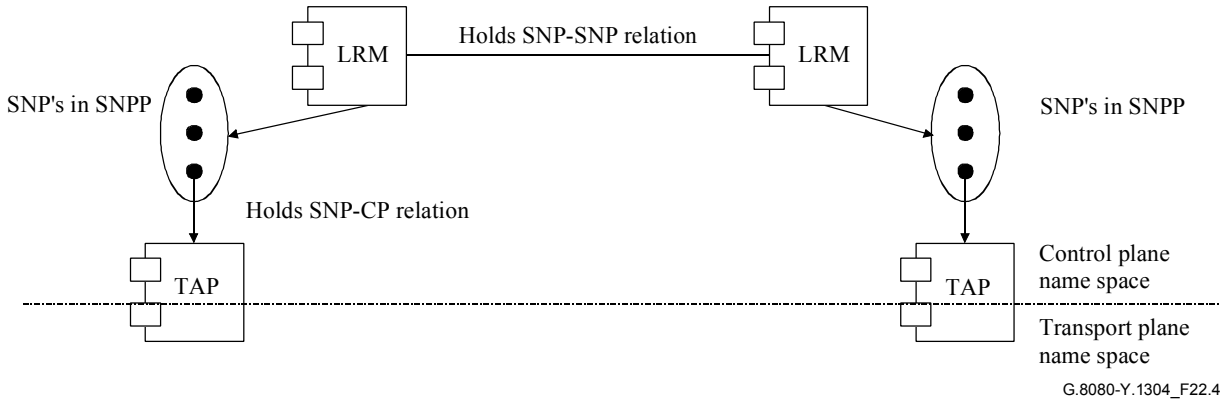

Figure 22.4/G.8080/Y.1304 – Population of control plane link connections

The Link Resource Manager (LRM) holds the SNP-SNP binding information necessary for the control plane name of the link connection, while the TAP holds the relation between the control plane name (SNP) and the transport plane name (CP) of resource. This separation allows control plane names to be completely separate from transport plane names, and completely independent of the method used to populate the DAs with those transport names.

In order to assign an SNP-SNP link connection to an SNPP link, it is only necessary for the transport name for the link connection to exist. Thus, it is possible to assign link connections to the control plane without the link connection being physically connected. This assignment procedure may be verified by the LRMs exchanging the Transport link name that corresponds to the SNP.

Note that the fully qualified SNPP link name is a control plane name reflecting the structure of transport plane resources.

10) Clause 8 Reference points

10.1) *Add the following text and figure at the end of the introduction to clause 8:*

A Reference Point represents a collection of services, provided via interfaces on one or more pairs of components. The component interface is independent of the reference point, hence the same interface may be involved with more than one reference point. From the viewpoint of the reference point, the components supporting the interface are not visible, hence, the interface specification can be treated independently of the component.

The information flows that carry services across the reference point are terminated (or sourced) by components, and multiple flows need not be terminated at the same physical location. These may traverse different sequences of reference points as illustrated in Figure 29.1.

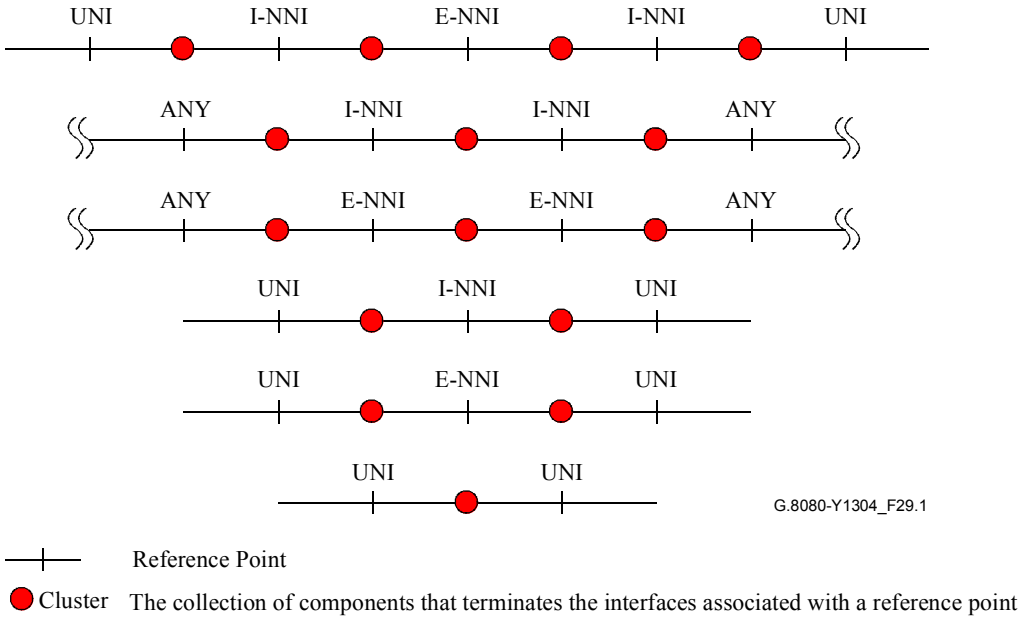

Figure 29.1/G.8080/Y.1304 – Reference points

10.2) *Add the following new clause to clause 8:*

8.4 User architecture

The user side will be referred to as the UNI-C (for "client"), and the network side will be referred to as the UNI-N (for "network").

The G.8080/Y.1304 UNI Transport Resource address (see clause 10) defines one or more globally unique addresses to each SNPP Link that is part of a UNI. These addresses are used to identify call destinations. Given that a UNI may contain multiple SNPP links, a UNI may therefore have multiple globally unique addresses for its bearer resources. Note that these addresses are not user names.

When there are multiple SNPP links that are part of the same UNI, those addresses can be used to discriminate between which SNPP link to use. Factors such as diversity or cost, could be used by callers to select the appropriate SNPP link.

UNI Transport Resource addresses can be used to differentiate between UNIs to a user. When there are multiple UNIs, each has distinct UNI Transport Resource addresses and they do not share a common address.

The following describes the UNI-C architecture:

1) There exists a transport entity called an Access Group Container (AGC) that can terminate multiple SNPP links. This entity can contain a set of G.805 access groups.

2) An AGC is a single layer entity that contains access groups, LRMs, and TAPs. It is similar to G.805 subnetworks except that it is not recursively defined, may or may not be a matrix (it does not have to be specified), and has no defined subnetwork connections. Multiple AGCs from different layers may be co-incident in the same equipment.

3) Control plane functions associated with a UNI-C in an AGC are call control (Calling/Called Party Call Controller), and resource discovery (LRM). Limited connection control and connection selection is present to interact with the connection controller on the UNI-N side. This is because the connection control on the UNI-N has a routing interface whereas connection control on the UNI-C tracks connection acceptance/teardown from the UNI-N side.

4) Applications that use one or more trails on an AGC are known as "<application name> connection users". They interact directly with G.805 access points by presenting and receiving adapted information. For each connection user there may be an "<application name> connection requestor". These entities interact with UNI-Cs to request/teardown connections. A single connection requestor could obtain connections from one or more UNI-Cs for a related connection user.

11) Clause 10 Addresses

11.1) *Add the following new clause to clause 10:*

10.1 Name spaces

There are three separate Transport names spaces in the ASON naming syntax:

1) A Routing Area name space.

2) A subnetwork name space.

3) A link context name space.

The first two spaces follow the transport subnetwork structure and need not be related. Taken together, they define the topological point where an SNPP is located. The link context name space specifies within the SNPP where the SNP is. It can be used to reflect sub-SNPP structure, and different types of link names.

An SNPP name is a concatenation of:

- one or more nested routing area names;
- an optional subnetwork name within the lowest routing area level. This can only exist if the containing RA names are present;
- one or more nested resource context names.

Using this design, the SNPP name can recourse with routing areas down to the lowest subnetwork and link subpartitions (SNPP subpools). This scheme allows SNPs to be identified at any routing level.

SNP name: An SNP is given an address used for link connection assignment and, in some cases, routing. The SNP name is derived from the SNPP name concatenated with a locally significant SNP index.

11.2) *Add the following subheading to introduce the existing text in clause 10:*

10.2 Addresses

12) Clause 11 Connection availability enhancement techniques

Add the following new clauses after the current text in clause 11:

11.1 Protection

Protection is a mechanism for enhancing availability of a connection through the use of additional, assigned capacity. Once capacity is assigned for protection purposes there is no rerouting and the SNPs allocated at intermediate points to support the protection capacity do not change as a result of a protection event. The control plane, specifically the connection control component, is responsible for the creation of a connection. This includes creating both a working connection and a protection connection, or providing connection-specific configuration information for a protection scheme. For transport plane protection, the configuration of protection is made under the direction of the management plane. For control plane protection, the configuration of protection is under the direction of the control plane rather than the management plane.

Control plane protection occurs between the source connection controller and the destination connection controller of a control plane protection domain where the source and destination are defined in relation to the connection. The operation of the protection mechanism is coordinated between the source and destination. In the event of a failure, the protection does not involve rerouting or additional connection setup at intermediate connection controllers, only the source and destination connection controllers are involved. This represents the main difference between protection and restoration.

11.2 Restoration

The restoration of a call is the replacement of a failed connection by rerouting the call using spare capacity. In contrast to protection, some, or all, of the SNPs used to support the connection may be changed during a restoration event. Control plane restoration occurs in relation to rerouting domains. A rerouting domain is a group of call and connection controllers that share control of domain-based rerouting. The components at the edges of the rerouting domains coordinate domain-based rerouting operations for all calls/connections that traverse the rerouting domain. A rerouting domain must be entirely contained within a routing domain or area. A routing domain may fully contain several rerouting domains. The network resources associated with a rerouting domain must therefore be contained entirely within a routing area. Where a call/connection is rerouted inside a rerouting domain, the domain-based rerouting operation takes place between the edges of the rerouting domain and is entirely contained within it.

The activation of a rerouting service is negotiated as part of the initial call establishment phase. For a single domain, an intra-domain rerouting service is negotiated between the source (connection and call controllers) and destination (connection and call controller) components within the rerouting domain. Requests for an intra-domain rerouting service do not cross the domain boundary.

Where multiple rerouting domains are involved, the edge components of each rerouting domain negotiate the activation of the rerouting services across the rerouting domain for each call. Once the call has been established, each of the rerouting domains in the path of the call have knowledge as to which rerouting services are activated for the call. As for the case of a single rerouting domain, once the call has been established the rerouting services cannot be renegotiated. This negotiation also allows the components associated with both the calling and called parties to request a rerouting service. In this case, the service is referred to as an inter-domain service because the requests are passed across rerouting domain boundaries. Although a rerouting service can be requested on an end-to-end basis, the service is performed on a per-rerouting domain basis (that is, between the source and destination components within each rerouting domain traversed by the call).

During the negotiation of the rerouting services, the edge components of a rerouting domain exchange their rerouting capabilities and the request for a rerouting service can only be supported if the service is available in both the source and destination at the edge of the rerouting domain.

A hard rerouting service offers a failure recovery mechanism for calls and is always in response to a failure event. When a link or a network element fails in a rerouting domain, the call is cleared to the edges of the rerouting domain. For a hard rerouting service that has been activated for that call, the source blocks the call release and attempts to create an alternative connection segment to the destination at the edge of the rerouting domain. This alternative connection is the rerouting connection. The destination at the edge of the rerouting domain also blocks the release of the call and waits for the source at the edge of the rerouting domain to create the rerouting connection. In hard rerouting, the original connection segment is released prior to the creation of an alternative connection segment. This is known as break-before-make. An example of hard rerouting is provided in Figure 29.2. In this example, the routing domain is associated with a single routing area and a single rerouting domain. The call is rerouted between the source and destination nodes and the components associated with them.

Soft rerouting service is a mechanism for the rerouting of a call for administrative purposes (e.g., path optimization, network maintenance, and planned engineering works). When a rerouting operation is triggered (generally via a request from the management plane) and sent to the location of the rerouting components, the rerouting components establish a rerouting connection to the location of the rendez-vous components. Once the rerouting connection is created, the rerouting components use the rerouting connection and delete the initial connection. This is known as make-before-break.

During a soft rerouting procedure a failure may occur on the initial connection. In this case, the hard rerouting operation pre-empts the soft rerouting operation and the source and destination components within the rerouting domain proceed according to the hard rerouting process.

If revertive behaviour is required (i.e., the call must be restored to the original connections when the failure has been repaired), network call controllers must not release the original (failed) connections. The network call controllers must continue monitoring the original connections, and when the failure is repaired the call is restored to the original connections.

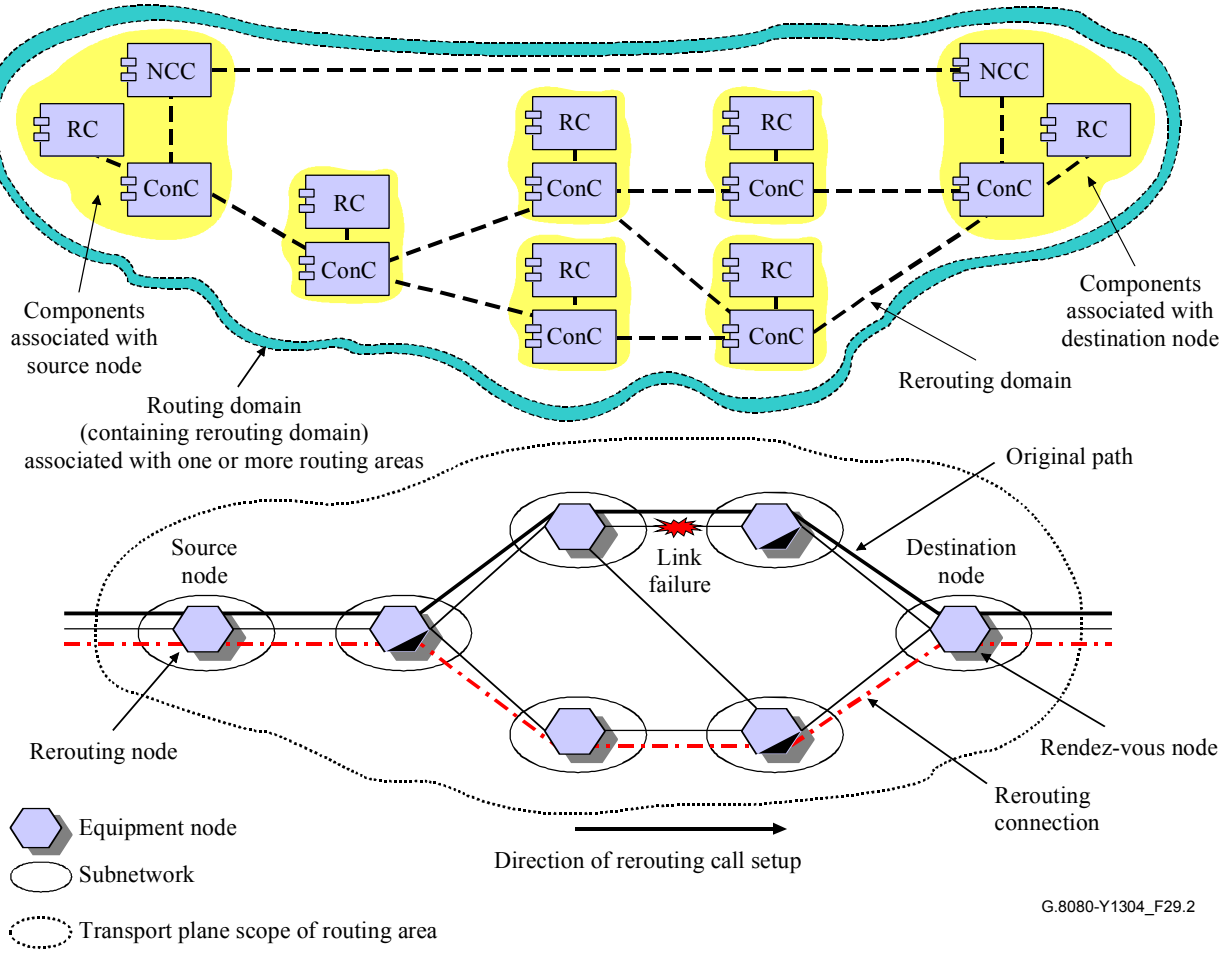

Figure 29.2/G.8080/Y.1304 – Example of hard rerouting

11.2.1 Rerouting in response to failure

11.2.1.1 Intra-domain failures

Any failures within a rerouting domain should result in a rerouting (restoration) action within that domain such that any down stream domains only observe a momentary incoming signal failure (or previous section fail). The connections supporting the call must continue to use the same source (ingress) and destination (egress) gateways nodes in the rerouting domain.

11.2.1.2 Inter-domain failures

Two failure cases must be considered, failure of a link between two gateway network elements in different rerouting domains, and failure of inter-domain gateway network elements.

11.2.1.3 Link failure between adjacent gateway network elements

When a failure occurs outside of the rerouting domains (e.g., the link between gateway network elements in different rerouting domains A and B in Figure 29.3a) no rerouting operation can be performed. In this case, alternative protection mechanisms may be employed between the domains.

Figure 29.3b shows the example with two links between domain A and domain B. The path selection function at the A (originating) end of the call must select a link between domains with the appropriate level of protection. The simplest method of providing protection in this scenario is via a protection mechanism that is pre-established (e.g., in a server layer network. Such a scheme is transparent to the connections that run over the top of it). If the protected link fails, the link protection scheme will initiate the protection operation. In this case, the call is still routed over the same ingress and egress gateway network elements of the adjacent domains and the failure recovery is confined to the inter-domain link.

11.2.1.4 Gateway network element failure

This case is shown in Figure 29.4. To recover a call when B-1 fails, a different gateway node, B-3, must be used for domain B. In general, this will also require the use of a different gateway in domain A, in this case A-3. In response to the failure of gateway NE B-1 (detected by gateway NE A-2), the source node in domain A, A-1, must issue a request for a new connection to support the call. The indication to this node must indicate that rerouting within domain A between A-1 and A-2 is to be avoided, and that a new route and path to B-2 is required. This can be considered as rerouting in a larger domain, C, which occurs only if rerouting in A or B cannot recover the connection.

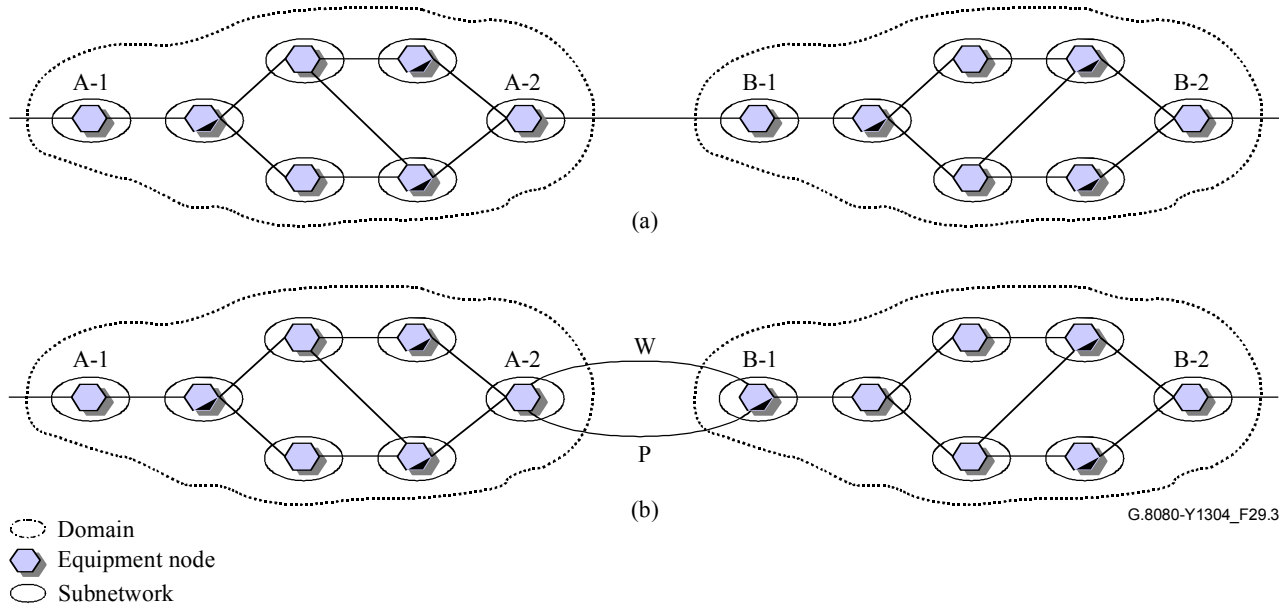

Figure 29.3/G.8080/Y.1304 – Link failure scenarios

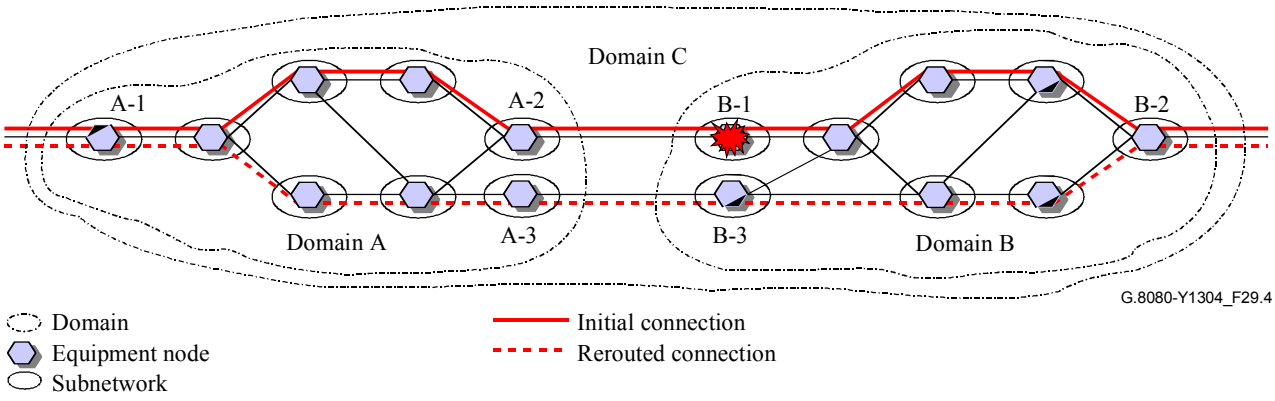

Figure 29.4/G.8080/Y.1304 – Rerouting in event of a gateway network element failure

13) New clause 12 Resilience

Add the following clauses:

12 Resilience

Resilience refers to the ability of the control plane to continue operating under failure conditions. Operation of the control plane depends upon elements of the Data Communications Network (DCN), the transport plane, the management plane and the internal components of the control plane itself (refer to Figure 1). Additional information is provided in Appendix II.

12.1 Principles of control and transport plane interactions

The following principles are used for control and transport plane interactions when communications become available between the two planes.

1) The control plane relies on the transport plane for information about transport plane resources.

2) Consistency between the control plane view and the corresponding transport network element is established first (vertical consistency).

3) Once local consistency is established, horizontal consistency is attempted. Here, control plane components synchronize with their adjacent components. This is used to re-establish a consistent view of routing, call, and connection state.

Another principle of control and transport plane interaction is that:

4) Existing connections in the transport plane are not altered if the control plane fails and/or recovers. Control plane components are therefore dependent on the SNC state.

For resiliency, the transport plane resource and SNC state information should be maintained in non-volatile store. Further some information about the control plane use of the SNC should be stored. This includes whether the SNC was created by Connection Management and how it was used. For example, which end of the SNC is towards the head end of the whole connection. At a given node, the control plane must ensure it has the resource and SNC state information that is consistent with the resource and SNC state information maintained by the transport NE. If not, the control components responsible for that node must:

- advertise zero bandwidth available to adjacent nodes to ensure there will be no network requests to route a new connection through that node;
- not perform any connection changes (e.g., teardowns).

The SNC state is the most important information to recover first because it is the basis of connections that provide service to end users. This follows the principle above. During recovery,

the control plane reconstructs the call and connection state corresponding to existing connections. For example, routing will need to disseminate correct SNP information after it is synchronized by the local control plane components (LRM).

The control plane re-establishment of information consistency with the transport NE should occur in the following sequence:

- the Link Resource Manager synchronizes with the transport NE state information;
- the Connection Controller then synchronizes with the Link Resource Manager;
- the Network Call Controller then synchronizes with the Connection Controller.

Following the re-establishment of local state consistency, the control plane must then ensure SNC state information consistency with adjacent nodes, as discussed in principle 3 above, prior to participating in control plane connection set-up or teardown requests.

12.2 Principles of protocol controller communication

When communication between protocol controllers is disrupted, existing calls and their connections are not altered. The management plane may be notified if the failure persists and requires operator intervention (for example, to release a call).

A failure of the DCN may affect one or more Protocol Controller to Protocol Controller communication sessions. The Protocol Controller associated with each signalling channel must detect and alarm a signalling channel failure.

When a Protocol Controller to Protocol Controller communication session recovers, state resynchronization between the Protocol Controllers should be performed.

Failure of a Protocol Controller is handled in a similar way to a failure of a Protocol Controller to Protocol Controller session.

12.3 Control and management plane interactions

Should management plane functions become unavailable, various control functions may be impaired. When management plane functions become available, the control plane components may need to report to the management plane actions that they took while the management plane was unavailable (e.g., call records).

14) Bibliography

Renumber Appendix II to Appendix IV.

15) New Appendix II Illustrative examples of implementations

Add the following new informative Appendix II:

Appendix II

Illustrative examples of implementations

The architecture of the Automatically Switched Optical Networks is defined in terms of various functions. These are specified in clause 7 and support the requirements specified in ITU-T Rec. G.8070.

The architecture, as specified in this Recommendation, allows flexibility in implementation and recognizes that network operators may have differing practices. The architecture also recognizes

that the functions may be implemented in a variety of ways. Furthermore, depending on the functionality required, not all components may be necessary. For example, the architecture described in ITU-T Rec. G.8080/Y.1304 provides flexibility in routing and allows both centralized and distributed routing. In the case of distributed routing, there are interactions between a number of routing controller functions whilst, in a centralized scheme, routing can, as an alternative, be maintained by the management plane, removing the need for a routing controller component. Requests for circuits, including their routes, are passed to the control plane from the management plane.

Although flexibility is provided within the architecture, defined interfaces and information flows enable interconnection of the various components. One such example is illustrated in Figure II.1. An additional example is contained in Figure III.2.

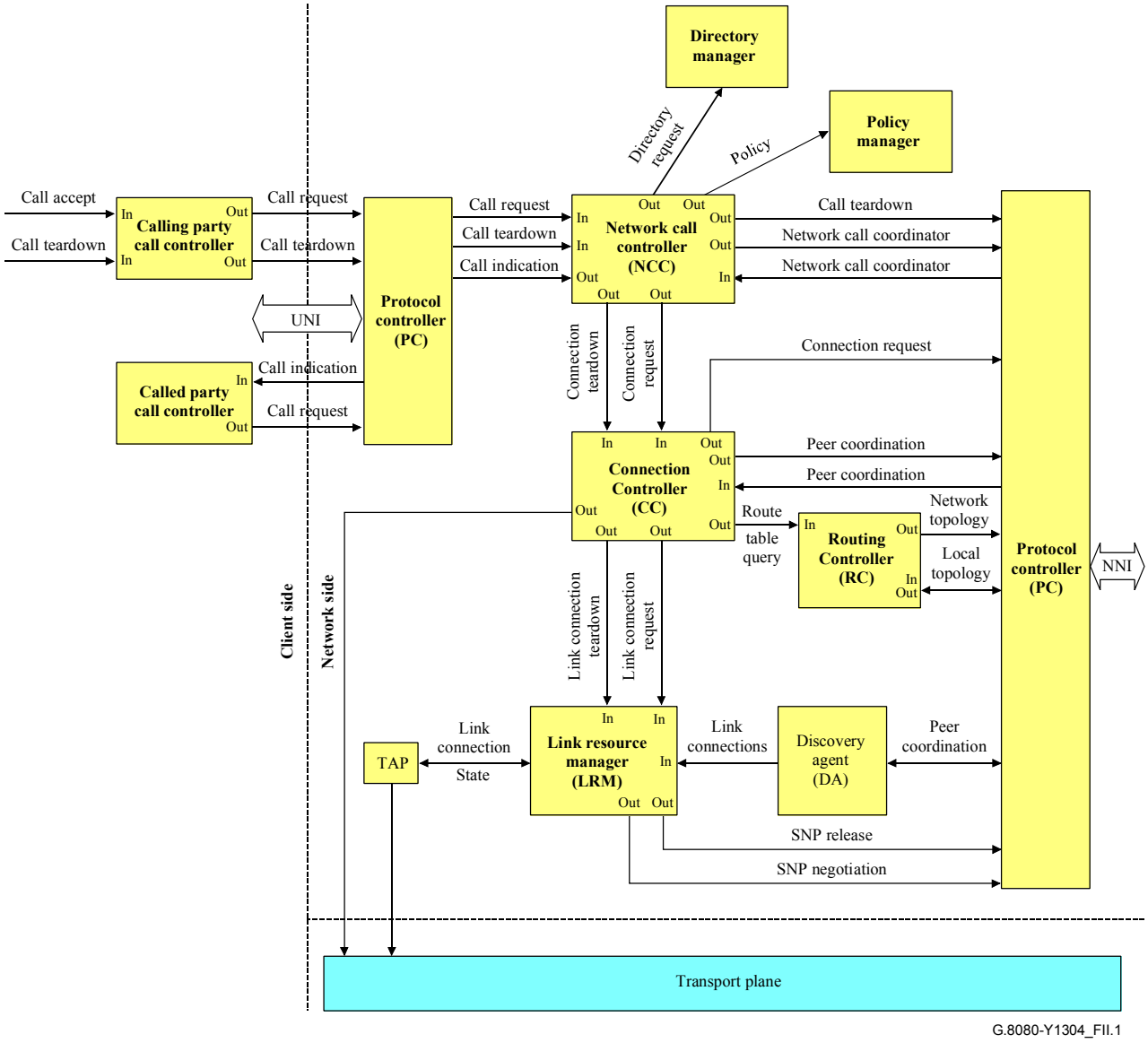

Figure II.1/G.8080/Y.1304 – Illustrative example of interconnection of components

16) New Appendix III Resilience relationships

Add the following new informative Appendix III:

Appendix III

Resilience relationships

Resilience refers to the ability of the control plane to continue operating under failure conditions. Operation of the control plane depends upon elements of the Data Communications Network (DCN), the transport plane, the management plane and the internal components of the control plane itself (refer to Figure 1). The following clauses identify the control plane dependencies on those areas. The desired degree of control plane resiliency can then be engineered by providing appropriate redundancy for the dependent functions.

III.1 Control Plane – DCN relationships

The control plane relies on the DCN for the transfer of signalling messages over some or all of the following interfaces (refer to Figure III.1): UNI, NNI, NMI. The impact of a signalling channel failure on the operation of the control plane will be examined for each of the Protocol Controllers associated with each interface.

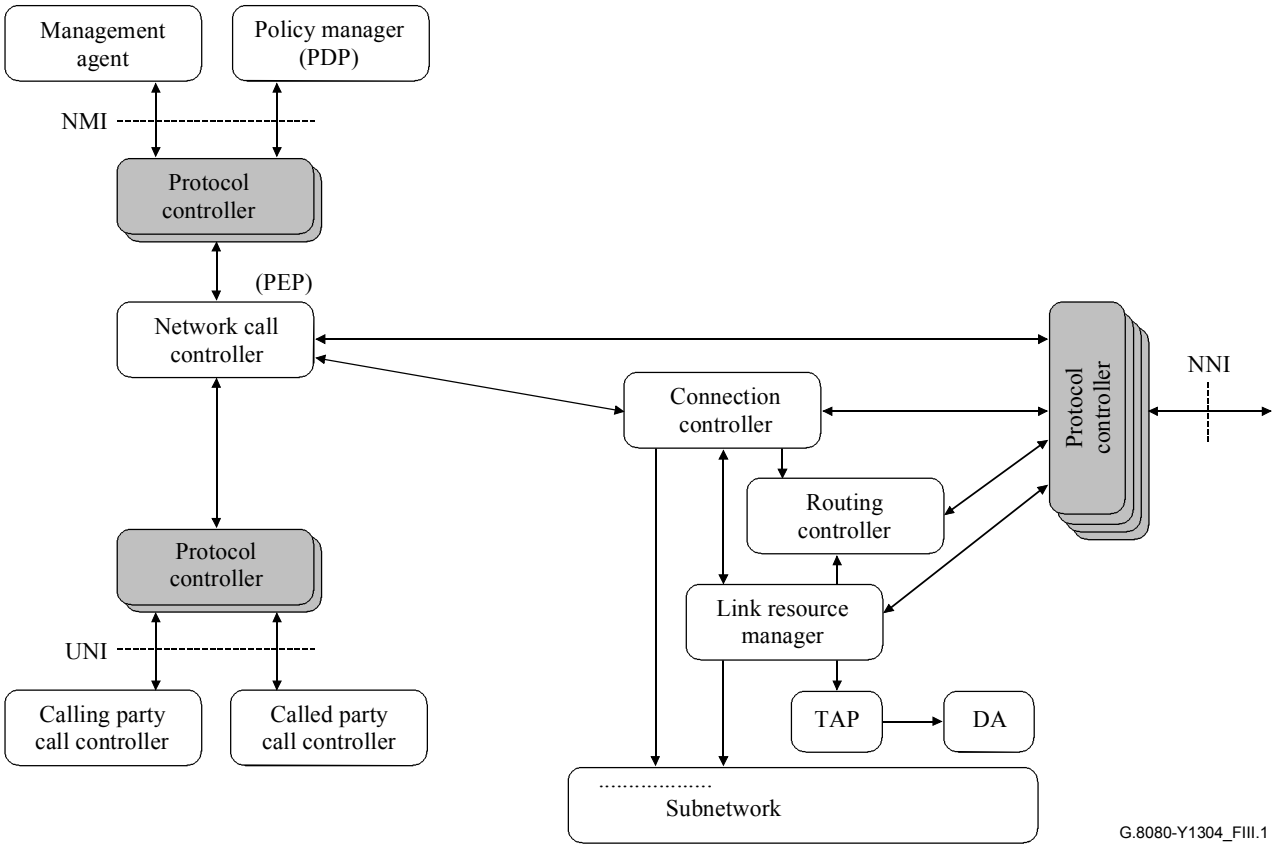

Figure III.1/G.8080/Y.1304 – Control plane components (an interpretation)

III.1.1 UNI

There are potentially two separate Protocol Controllers handling the signalling sessions over the UNI: one for the Calling Party Call Controller link and one for the Called Party Call Controller link.

III.1.1.1 Failure case

A failure of the signalling session supporting the UNI for the Calling Party Call Controller link will result in the loss of the Call Request/Call Teardown control flows.

A failure of the signalling session supporting the UNI for the Called Party Call Controller link will result in the loss of the Call Request/Call Indication control flows.

A failure of either of the UNI-related signalling session impacts the Network Call Controller function.

In all cases above, existing calls and their connections are not altered. The management plane may be notified if the failure persists and requires operator intervention (for example, to release a call).

III.1.1.2 Recovery case

When the signalling channel recovers, state resynchronization between the client call controllers and the network call controller, and the connection controllers over the UNI, should be performed.

III.1.2 NNI

There are potentially four separate Protocol Controllers handling the signalling sessions over the NNI: one for the Network Call Controller link, one for the Connection Controller link, one for the Routing Controller link and one for the Link Resource Manager link.

III.1.2.1 Failure case

A failure of the signalling session supporting the NNI for the Network Call Controller link will result in the loss of the Network Call Controller Coordination control flows. Call set-up or teardown will not be possible, but there is no impact on connection set-up or teardown.

A failure of the signalling session supporting the NNI for the Connection Controller link will result in the loss of the Connection Controller Coordination and Connection Request/Call Teardown control flows. Connection set-up or teardown will not be possible. Further, if Call Control is piggybacked on Connection Control, no call set-up or teardown will be possible either.

A failure of the signalling session supporting the NNI for the Routing Controller link will result in the loss of the Network/Local Topology control flows.

A failure of the signalling session supporting the NNI for the Link Resource Manager link will result in the loss of the SNP Negotiation/Release control flows.

A failure of the Link Resource Manager signalling session impacts the Routing Controller function and the Connection Controller function. A failure of the Routing Controller signalling session impacts the Connection Controller function. A failure of the Connection Controller signalling session impacts the Network Call Controller function.

In all cases above, existing calls and their connections are not altered. The management plane may be notified if the failure persists and requires operator intervention (for example, to release a call).

Note that a failure of the DCN may affect one or more or all of the above signalling sessions simultaneously. The Protocol Controller associated with each signalling channel must detect and alarm a signalling channel failure.

III.1.2.2 Recovery case

Upon restoral of a previously failed signalling channel, the corresponding Protocol Controller must ensure all messaging resumes in sequence. Components are responsible for re-establishing state information after Protocol Controller recovery.

III.2 Control plane – Transport plane relationships

This clause considers only those transport plane failures that affect the ability of the control plane to perform its functions, for example, when an LRM cannot be informed. Transport plane failures, such as port failures, are not in the scope of this Recommendation as it is expected that the control plane is informed of this situation. Information consistency between the two planes is treated in 12.1.

III.2.1 Transport plane information – Query

The control plane will query the transport plane under the following scenarios:

– when a Connection Controller signalling session activates, or re-activates (for example, following the recovery of a data link or transport NE);

– control plane queries about the transport resources;

– as part of transport resource information synchronization (for example, when the control plane recovers following a failure).

III.2.2 Transport plane information – Event driven

The transport plane will inform the control plane on an event basis under the following scenarios:

– failure of a transport resource;

– addition/removal of a transport resource.

III.2.3 Transport plane protection

Transport plane protection actions, which are successful, are largely transparent to the control plane. The transport plane is only required to notify the control plane of changes in availability of transport resources.

Transport plane protection attempts, which are unsuccessful, appear to the control plane as connection failures and may trigger control plane restoration actions, if such functionality is provided. Given that the control plane supports restoration functionality, the following relationships exist.

The Routing Controller must be informed of the failure of a transport plane link or node and update the network/local topology database accordingly. The Routing Controller may inform the local Connection Controller of the faults.

III.2.4 Transport plane dependency on control plane

If the control plane fails, new connection requests, that require the use of the failed control plane components, cannot be processed. Note, however, that the management plane could be used as a fallback to respond to new connection requests. Established connections must not be affected by a control plane failure.

III.3 Control plane – Management plane relationships

The control plane may obtain directory and policy information from the management plane during the call admission control validation process. Failure of the directory or policy servers could result in the failure of connection set-up requests.

Examples of this are:

– At the Network Call Controller (at the calling or called party end), call requests may need to be validated by policy checking.

– When connection controllers request a path from the Routing Controller, a policy server may need to be consulted.

– Call release actions can take place in the control plane if the management plane is not available. A record of these actions must be maintained by the control plane so that when the management plane becomes available, a log can be sent to the management plane or the control plane can be queried for this information.

III.3.1 NMI

All control components have monitor, policy and configuration ports which provide the management view of the control plane components (see 7.2.1).

There are potentially two separate Protocol Controllers/signalling sessions involving management information flows: one for the Policy Manager session and one for a transport management session. Other Protocol Controllers may be introduced in the future for other management functions.

III.3.1.1 Failure case

A failure of the signalling session supporting the Policy Manager link will result in the loss of the Policy Out control flows.

A failure of the transport management signalling session will result in the loss of FCAPS (Fault, Configuration, Accounting, Performance, Security) information exchange.

A failure of the Policy session impacts the Network Call Controller function. For example, the potential failure of new connection set-up requests when the call admission control validation process requires Policy Manager access.

III.3.1.2 Recovery case

When management signalling communication is recovered, information stored in the control plane that should be sent to management plane is sent (e.g., call records). Information pending from the management plane to the control plane should be sent (e.g., revised policy or configuration).

III.4 Intra-control plane relationships

The impact of control plane component failures on the operation of the control plane overall will be examined per the component relationship illustrated in Figure III.1. To achieve continuous operation of the control plane under a component failure, the ability to detect a component failure and switch to a redundant component, without loss of messages and state information, is required.

If control plane components are not redundant, then when a failed component recovers, it must re-establish a sufficient view of the transport plane resources in order to be operational.

It is assumed that the communications between components other than Protocol Controllers (i.e., non-PC communications) is highly reliable. Such communications is likely to be internal to a control plane node and is implementation specific, thus it is outside the scope of this Recommendation.

III.4.1 Network call controller

The failure of a Network Call Controller will result in the loss of new call set-up requests and existing call teardown requests.

III.4.2 Connection controller

The failure of a Connection Controller will result in the loss of new connection set-up requests and existing connection teardown requests. As Call Control signalling is often implemented via the Connection Controller and its Protocol Controller, a failure of the Connection Controller may impact the Network Call Controller function (e.g., may not be able to teardown existing calls).

III.4.3 Routing controller

The failure of a Routing Controller will result in the loss of new connection set-up requests and loss of topology database synchronization. As the Connection Controller depends on the Routing Controller for path selection, a failure of the Routing Controller impacts the Connection Controller. Management plane queries for routing information will also be impacted by a Routing Controller failure.

III.4.4 Link resource manager

The failure of a Link Resource Manager will result in the loss of new connection set-up requests and existing connection teardown requests, and loss of SNP database synchronization. As the Routing Controller depends on the Link Resource Manager for transport resource information, the Routing Controller function is impacted by a Link Resource Manager failure.

III.4.5 Protocol controllers

The failure of any of the Protocol Controllers has the same effect as the failure of the corresponding DCN signalling sessions as identified above. The failure of an entire control plane node must be detected by the neighbouring nodes NNI Protocol Controllers.

III.4.6 Intra-control plane information consistency

As discussed in point 2 of 12.1 at a given node, control plane component resource and SNC state information consistency with the local transport NE resource and state information must be established first. Then, control plane components must ensure SNC state information consistency with its adjacent control plane components. Any connection differences must be resolved such that no connection fragments remain, or misconnections occur. Following the control plane information consistency cross-check, the control plane components are permitted to participate in control plane connection set-up or teardown requests.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	**Global information infrastructure and Internet protocol aspects**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2003