INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 15

TD 279 Rev.1 (PLEN/15)

English only

Original: English

Question(s): 12, 14/15 Geneva, 31 May - 11 June 2010

TEMPORARY DOCUMENT

Source: Editor

Title: G.8080 Amendment 2 (for consent)

ITU-T Recommendation G.8080 (06/2006)

Architecture for the Automatically Switched Optical Network (ASON)

Amendment 2

Summary

Amendment 2 to ITU-T Rec. G.8080/Y.1304 contains:

- Additions for multi-layer topology representation
- Addition of a directory service component
- An appendix illustrating rerouting and protection domain interaction

1 Scope

2 References

Remove references to ITU-T Recommendations G.707, G.709, G.783, G.798, G.803, G.872, M.3000, and M.3010.

3 Definitions

Add the following definition:

3.59 Transitional SNPP link: See [ITU-T Rec. G.8081].

6 Transport resources and their organization

For clause 6.1 of G.8080. Add after the sentence "The association of SNPPs on different subnetworks is an SNPP link".

Contact: Stephen Shew
Ciena Corporation
USA
Tel: +1 613 763 2462
Fax: +1 613 763 7204
Email: sshew@ciena.com

Attention: This is not a publication made available to the public, but **an internal ITU-T Document** intended only for use by the Member States of ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of ITU-T.

An SNPP link where each subnetwork is in a different layer is known as a transitional SNPP link. It may also be an SNPP link in which the subnetworks are in different sublayers of the same layer. They only occur across boundaries between layers or sublayers where [ITU-T G.800] transitional links can exist.

For clause 6.2 of G.8080. Add at the end of the clause.

Routing areas in different layers may be connected by transitional SNPP links. This enables multi-layer routing topology construction. Routing areas in different sublayers of the same layer may also be connected by transitional SNPP links.

Add new clause 6.5.3 "Multilayer Routing Topology".

6.5.3 Multilayer Routing Topology

In addition to the single layer topology representation in clause 6.5.2, a routing topology representative of a multi-layer network may be constructed using transitional SNPP links that connect routing areas in different layers. Paths may be determined that traverse link and subnetwork connections in more than one layer and/or sublayer. Control plane components that are involved in configuring the resulting connection configure link connections, subnetwork connections, and transitional link connections.

The use of a transitional SNPP link implies that a sequence of adaptations between layers, or sequence of layer processors within a layer, is used. The transitional SNPP link enables a connected graph to be constructed that represents a multi-layer network for the purpose of routing.

Figure 14.1 illustrates the [ITU-T G.800] representation and the corresponding multilayer routing topologies.

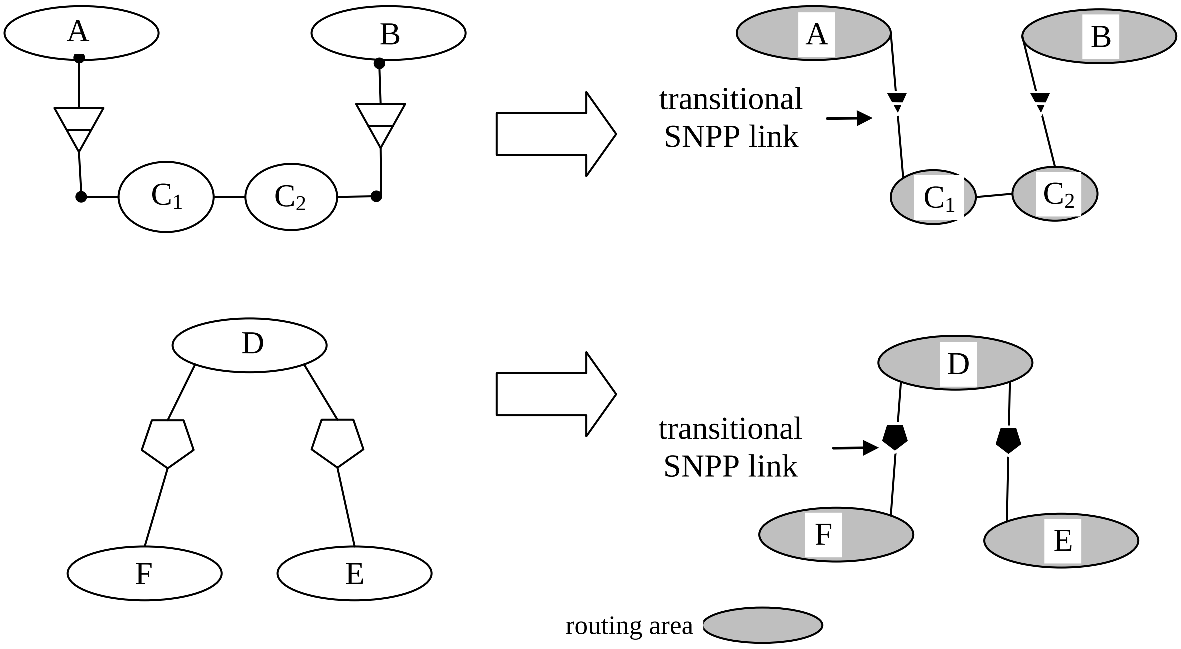


Figure 14.1. Multilayer routing topology representations

A multilayer topology corresponding to the model in Figure 14 is illustrated in Figure 14.2 on the left. It differs from the model in Figure 14 in that the topology is multilayer (i.e., contains both client and server SNPPs).

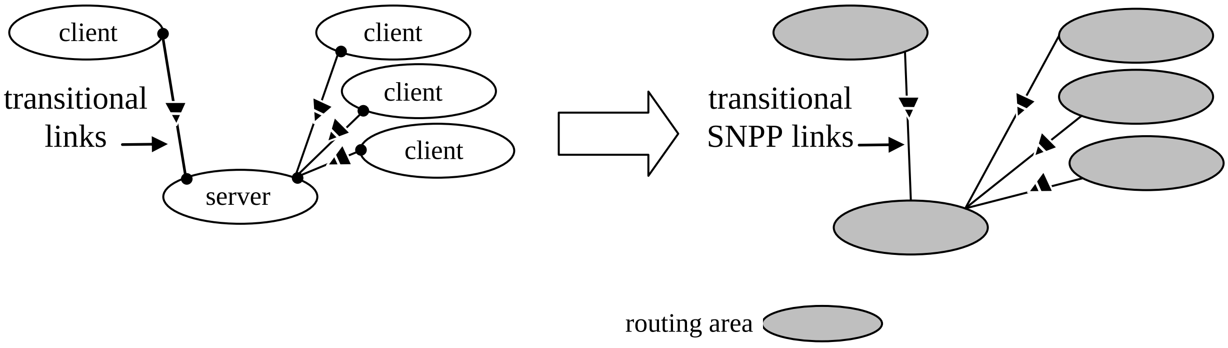


Figure 14.2 Multilayer routing topology representation of Figure 14.

A path computation begins by selecting two (sets of) points at the boundary of a routing area. The path computation may be accomplished using a set of subordinate path computations involving contained routing areas. The routing areas relevant to the path computation are selected by the path computation algorithm, and these routing areas may belong to one or more layers (i.e., they may be part of a multi-layer topology).

In a multilayer routing topology, when a transitional SNPP link is used between a routing area in a first layer to another routing area in an adjacent second layer and the first layer is traversed further in a route, it is expected that a corresponding transitional link is used to eventually return to the first layer in computed paths.

For segments of a path computed between sublayers, traversal of a single transitional SNPP link is allowed.

An additional example of a multilayer topology is shown in Appendix VII.

Note: Use of transitional links for a 1:1 adaptation is described in this section. Usage for 1:n and m:1 is for further study.

Add the following new section.

6.8 Mapped Server Interlayer Relationships

When a client layer CI is mapped to a server layer as described in Sections 6.5 and 6.6, several types of arrangements can exist. They include client/servers in 1:1 and 1:n relationships. The ratio refers to the number of Connection Points in each layer.

6.8.1 1:1 Relationship

In the 1:1 relationship support for a client communication is supported by the server layer as a single trail. The NCC_{client}:NCC_{server} relationship is also 1:1. A specific example of this is shown in Appendix IV where Ethernet CI is mapped to a single VC-3. Another example is a DS-3 into an STS-1.

As the NCC_{client} is trying to use the server layer, it must have knowledge of the relevant the call parameters of the NCC_{server} including whether the client initiated the server layer call (Server NCC Coordination Out interface) or whether the server layer already existed for client layer use (Client NCC Coordination Out interface).

The NCC$_{server}$ is not required to possess knowledge of the client layer call parameters, but should inform the NCC$_{client}$ if there are changes in the server layer call.

6.8.2 1:n Relationship

In a 1:n relationship, the client communication is supported by multiple connections in the server layer. This is supported either by the server NCC supporting multiple connections or multiple NCCs in the server layer supporting the one client layer NCC.

The example below in Figure 16.1 illustrates the latter case. The Ethernet call is mapped to a VC-4-2v VCAT call. The VCAT call is related to multiple server layer VC-4 calls. The Ethernet/GFP layer to VCAT relationship is 1:1.

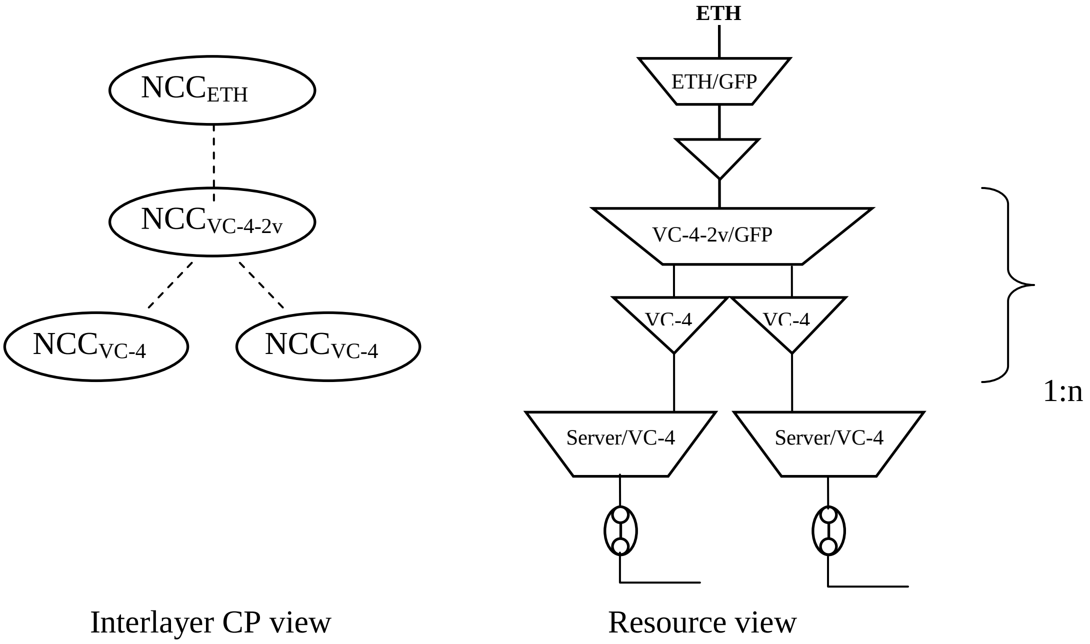


Figure 16.1/G.8080/Y.1304 –Example 1:n Mapped Server

It is necessary for the client layer NCC (the VC-4-2v layer) to know about the call parameters of the server layer as it must ensure that there are sufficient number of server layer calls as well as what their aggregate characteristics are. The server layer is not required to possess knowledge of the client layer call parameters, but should inform the client call if there are changes in the server layer call.

Change the following bullet in list in section 7.3.5.2

- call state management.

To

- state management of client calls and itself.

Add the following to the first list in section 7.3.5.2

- adaptation management of transport resources via the TAP component

7 Control plane architecture

Re-number section 7.3.6 to 7.3.7 and propagate change in lowest index number to rest of 7.3

Add the following new section.

7.3.6 Directory Service

The Directory Service Component is responsible for identifier resolution and coordination among peer Directory Service components. The role of this component is provide mappings between identifier spaces for other components.

NOTE:

1. All interfaces as Table 7.1 below are not intended to be used in one instance of this component. Only Directory Request interface might be required for basic usage, but Distributed implementations might use more interfaces.
2. Directory service functions can be implemented in both distributed and centralized applications. In a centralized application, peer coordination interfaces of the DS component might be unused.

Table 7.1/G.8080/Y.1304 – Directory Service component interfaces

Input interface	Basic input parameters	Basic return parameters
Directory Request In	1) UNI/E-NNI Transport Resource Identifier; or 2) UNI/E-NNI Transport Resource Identifier alias; or 3) SNPP identifier; or 4) SNPP alias;	1) SNPP identifier; or 2) UNI/E-NNI Transport Resource Identifier; or 3) UNI/E-NNI Transport Resource Identifier; or 4) SNPP identifier;
Peer coordination In	1) <UNI/E-NNI Transport Resource Identifier, SNPP identifier> 2) <UNI/E-NNI Transport Resource Identifier alias, UNI/E-NNI Transport Resource Identifier> 3) <SNPP identifier, UNI/E-NNI Transport Resource Identifier> 4) <SNPP alias, SNPP identifier> 5) <SNPP identifier, SNPP alias>	
Directory information in	1) <UNI/E-NNI Transport Resource Identifier, SNPP identifier> 2) <UNI/E-NNI Transport Resource Identifier alias, UNI/E-NNI Transport Resource Identifier> 3) <SNPP identifier, UNI/E-NNI Transport Resource Identifier> 4) <SNPP alias, SNPP identifier >	

	5) <SNPP identifier, SNPP alias>	
Output interface	**Basic output parameters**	**Basic return parameters**
Directory Request Out	1) UNI/E-NNI Transport Resource Identifier; or 2) UNI/E-NNI Transport Resource Identifier alias; or 3) SNPP identifier; or 4) SNPP alias;	1) SNPP identifier; or 2) UNI/E-NNI Transport Resource Identifier; or 3) UNI/E-NNI Transport Resource Identifier; or 4) SNPP identifier;
Peer coordination Out	1) <UNI/E-NNI Transport Resource Identifier, SNPP identifier> 2) <UNI/E-NNI Transport Resource Identifier alias, UNI/E-NNI Transport Resource Identifier> 3) <SNPP identifier, UNI/E-NNI Transport Resource Identifier> 4) <SNPP alias, SNPP identifier> 5) <SNPP identifier, SNPP alias>	
Directory information out	1) <UNI/E-NNI Transport Resource Identifier, SNPP identifier> 2) <UNI/E-NNI Transport Resource Identifier alias, UNI/E-NNI Transport Resource Identifier> 3) <SNPP identifier, UNI/E-NNI Transport Resource Identifier> 4) <SNPP alias, SNPP identifier> 5) <SNPP identifier, SNPP alias>	

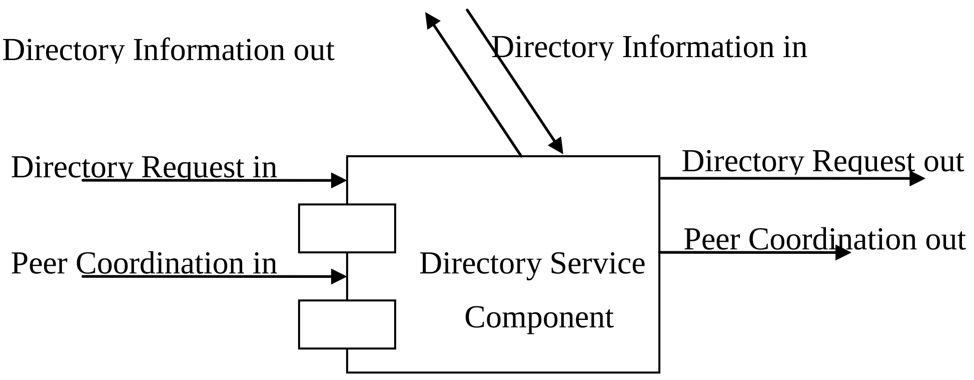


Figure 32.1/G.8080/Y.1304 –Directory Service component

Directory Request In /Out:

This interface is used to get an SNPP identifier from a UNI/E-NNI Transport Resource Identifier or alias. And this interface is also used to get UNI/E-NNI Transport Resource Identifier from a UNI Transport Resource Identifier alias or SNPP identifier. Directory request should be bidirectional. CC could initialize a Directory Request and send to/receive from DS component when it needs to decode DS.

Peer Coordination in:

This interface is used to get directory information from peer Directory Service Component.

Peer Coordination out:

This interface is used to transmit directory information to peer Directory Service Component.

Directory information in/out:

This interface is used to receive/send directory information from other components which could include management plane applications, and equipment management functions (EMFs) on subnetworks (e.g., NEs).

Add the following to the list at the end of section 7.4

For the Route Query interface between the Connection Controller and Routing Controller, authenticated, and secure information transfer with appropriate policy in the port for domain scope.

Add the following new section.

11.3 Nested routing domains

CP protection and restoration domains are types of routing control domains. As such, they inherit the containment property of control domains. Coordination between the actions taken by two domains in a containment relationship to a resource failure is a matter of policy.

Remove Appendix I.

Remove Appendix II.

Add the following new appendix.

Appendix VI

Combining Protection and Restoration Domains

(This appendix does not form an integral part of this Recommendation)

The coordination between CP protection and restoration is performed by the control plane. CP protection and restoration domains are routing domains since they require path computation to create connections in a domain. Thus the relationship between protection and restoration domains is a containment relationship. It is possible for a protection domain and restoration domain to share the same routing controller scope.

When a fault (or repair) occurs, the smallest containing protection/restoration domain should act first, followed by successively larger protection/restoration domains should they be necessary. When the containing domain cannot fix the connection, it must notify the failure to the larger domains. Then the larger domain may use the rerouting or protection action to fix the failure.

What has been mentioned above is the general principle for protection/restoration domain interaction. For example, the smallest domain where error occurs is a protection domain, thus a protection action is applied first. Only when it cannot fix the connection (the 2nd error), the connection failure is signalled to the immediate containing domain.

When the smallest domain where error occurs is a restoration domain, a rerouting action is applied first. If restoration fails, the connection failure is signalled to the larger domain. The larger domain is either restoration domain or protection domain. Subsequent restoration/protection actions are taken in the ever increasingly larger containment domains as needed.

Following is an example for this general principle. In a 1+1 SNCP, after a working connection failure is detected, the source and destination controllers are involved to complete the protection switching operation from the original working connection to protection connection. During the protection operation, there is no rerouting operation involved. If the protection connection fails, restoration becomes active because the containing domain is a rerouting domain. The control plane is in charge of the coordination between protection and restoration.

Figure VI.1 shows an example of the coordination between a rerouting domain and a protection domain. The rerouting domain contains the protection domain. After a working connection failure is detected (SNC [A, C, E, F]), the transport plane is involved to complete the protection switching operation from the original working connection to protection connection (SNC [A, B, D, F]). When the protection connection (SNC [A, B, D, F]) fails, connection controllers in the control plane activate the rerouting mechanism, and restoration is performed in rerouting domain resulting in connection [G, H, I, J, K].

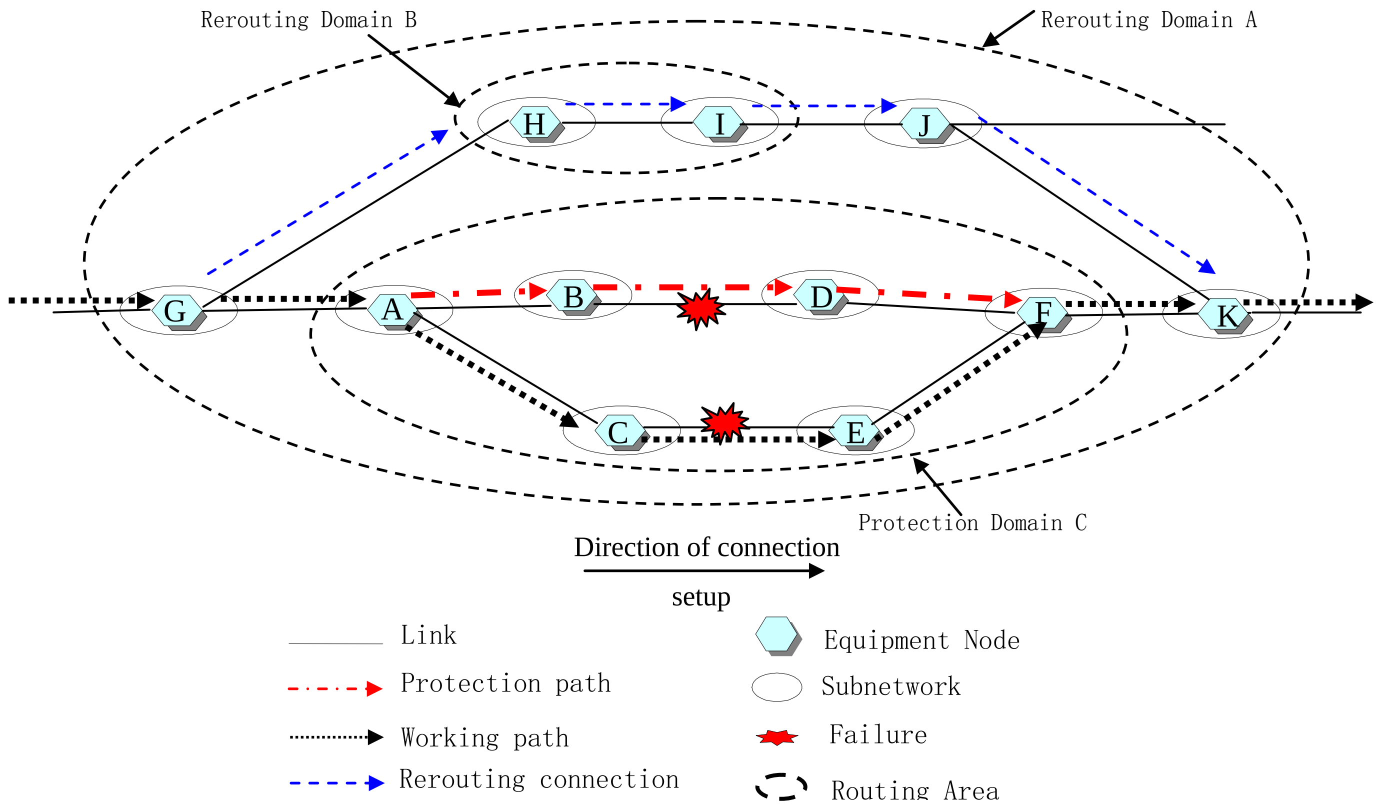
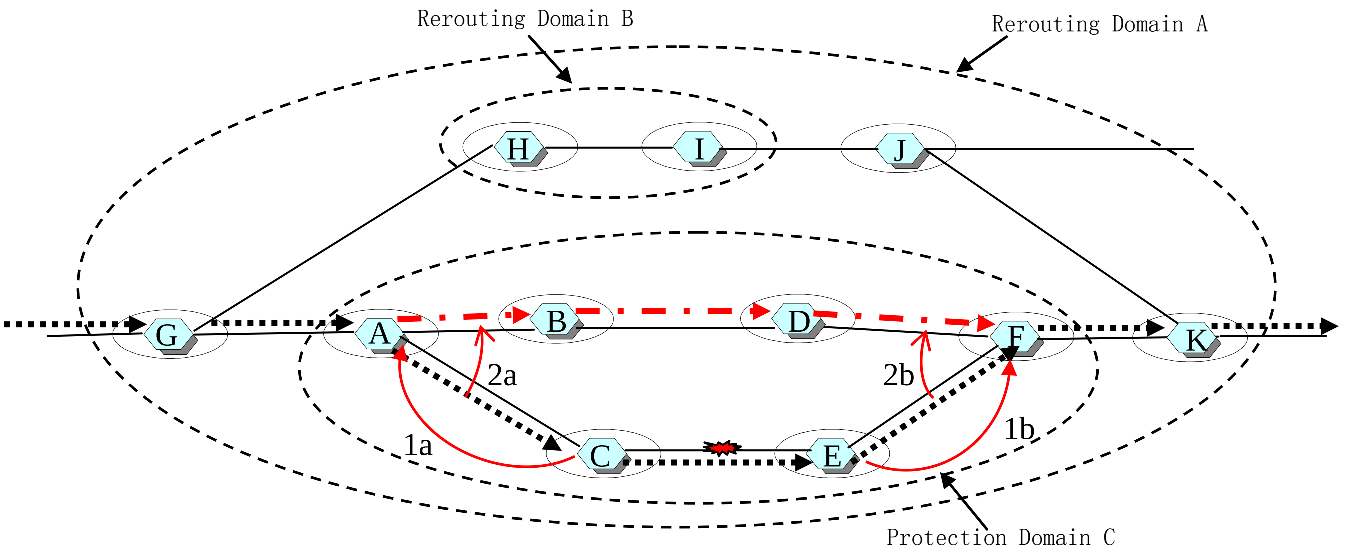


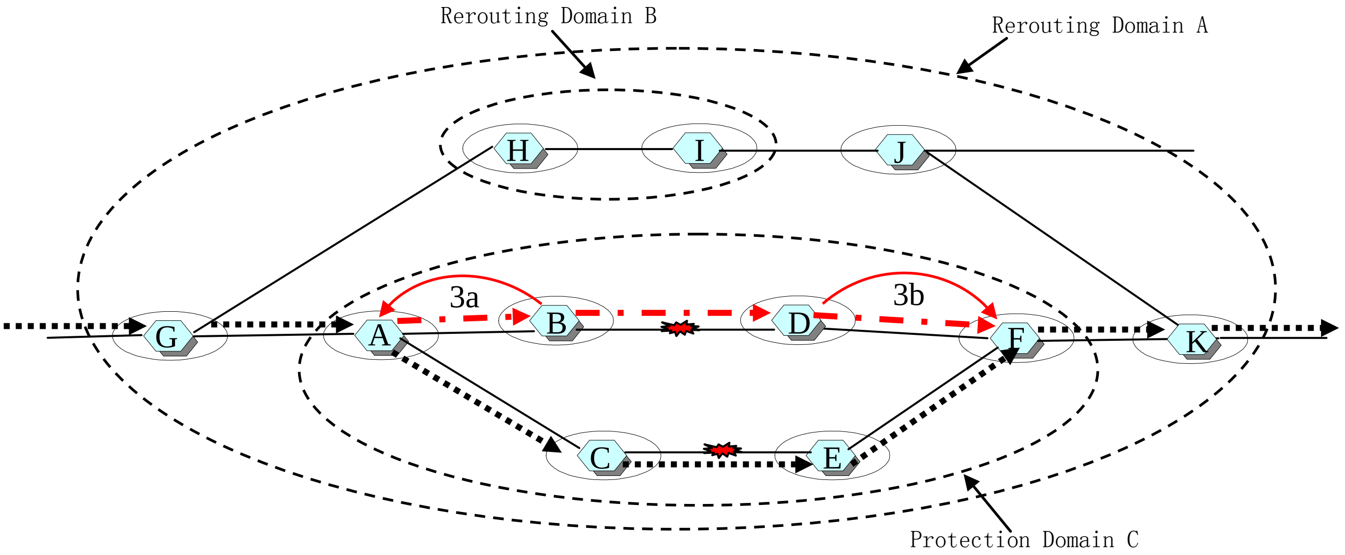
Figure VI.1/G.8080/Y.1304 – Nested protection and restoration domains

Figure VI.2 shows the signalling flow of a rerouting scenario with source (or step-by-step) routing connection control after protection domain failure events corresponding to Figure VI.1.

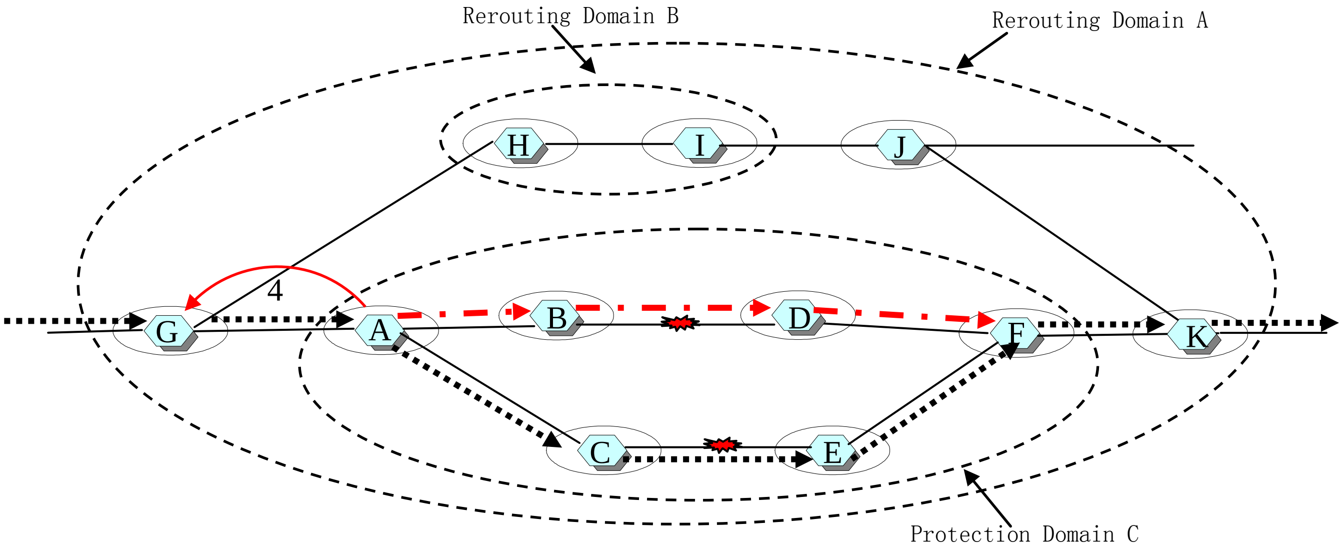
Step 1 The protection mechanism is coordinated between Node A and Node F in Protection Domain C after a failure of working path.



Step 2 Both Node A and Node F receive a failure notify after the protection path fails again.



Step 3 If the protection domain cannot repair the connection, the connection failure is signalled to the containing restoration domain



Step 4 Rerouting Domain A creates the rerouting connection excluding Protection Domain C

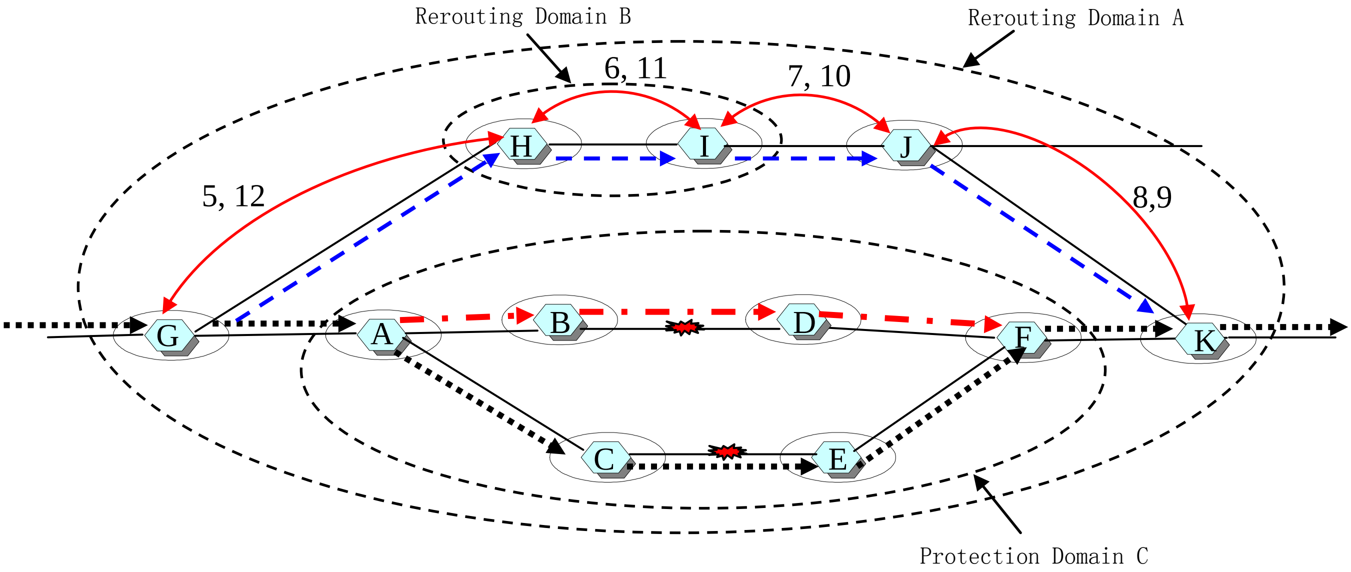


Figure VI.2/G.8080/Y.1304 – Signalling flow of combination of protection and restoration

In Figure VI.3, the detailed sequence of operations using source routing method is described after the protection path fails. This corresponds to the steps 2-4 of Figure VI.2. The steps involved are listed below:

1) A bidirectional link failure notification generated by the Link Resource Managers (LRM) arrives at the Connection Controller (CC) containing the failure link information. This occurs in node B or node D.

2) The link failure notification is forwarded to CC_A from CC_B and to CC_F from CC_D.

3) At both CC$_A$ and CC$_F$, the NCCs are alerted to the failure of the protection path.

4) NCC$_A$ identifies that there is not any additional assigned capacity to protect working path in protection domain.

5) The failure is propagated outside of protection domain C to rerouting domain A. Protection domain failure notification is generated by the Connection Controller (CC), containing the crankback routing information which specifies the failure domain. The protection failure notification is forwarded to CC$_G$ from CC$_A$.

6) RC$_G$ is queried for rerouting connection with crankback routing information and returns the set of Links excluding protection domain C.

7)-29) Steps 8 to 29 describe the flow of connection set-up using source routing algorithm which is identical to that described in V.2.3 Source and step-by-step routing.

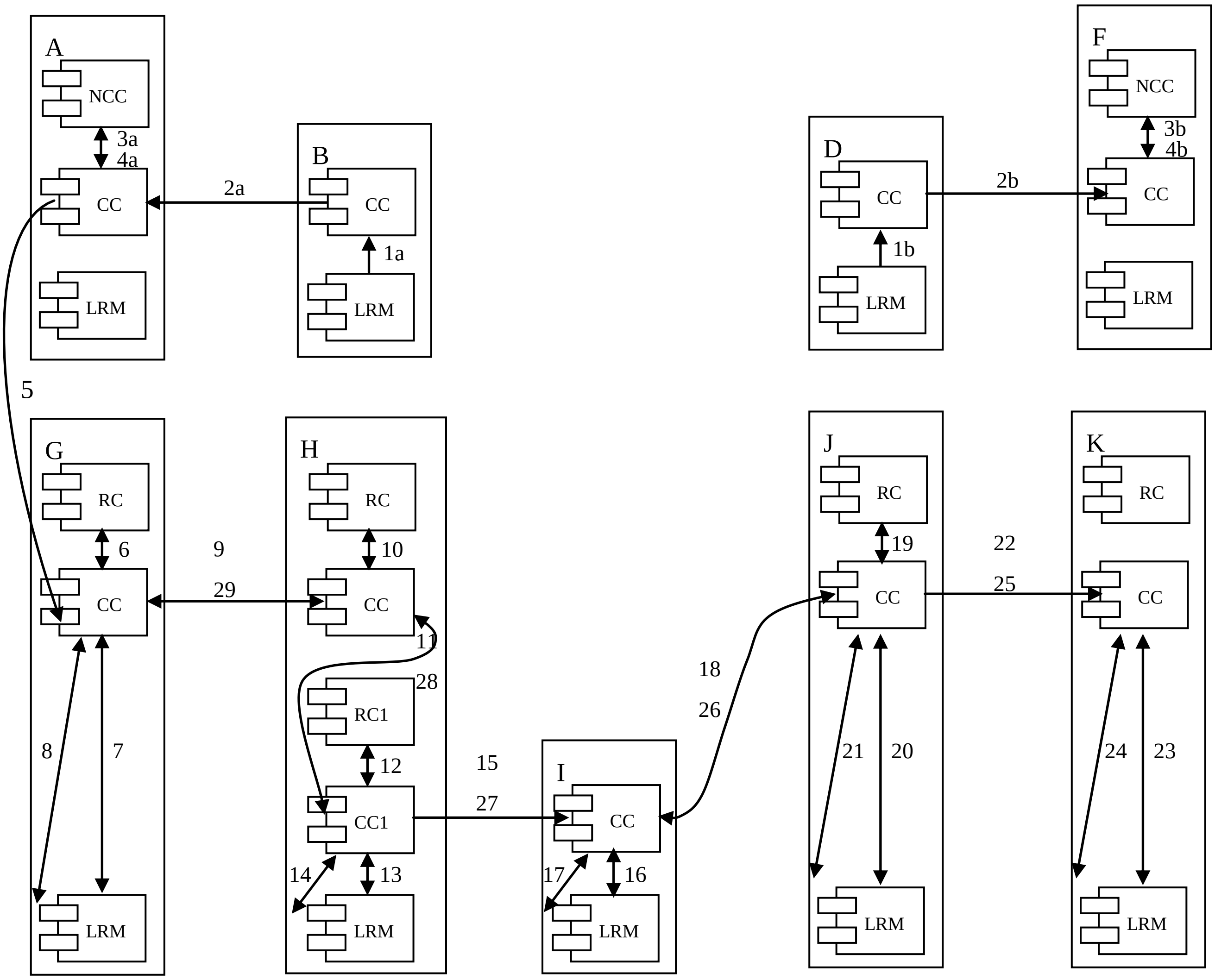


Figure VI.3/G.8080/Y.1304 – Component interactions of combination of protection and restoration

In Bibliography, remove reference to G.8110.1.

Add the following new appendix.

Appendix VII

Example of explicit multi-layer routing topology

(This appendix does not form an integral part of this Recommendation)

In some situations connection routing can benefit from a topology view that includes explicit detail from multiple layer networks. One example of this is an ODU layer network that contains within it subnetworks supported by transparent optical (OCh) layer networks.

If the OCh server layer network topology is projected into the ODU client layer it is not possible to associate different routing attributes or constraints specific to the transparent optical subnetworks with that topology. Figure VII.1 shows an example of an explicit multilayer topology for such a network. In this example the transitions from the ODU layer to the OCh layer are shown using transitional SNPP links with an adaptation/termination icon. This indicates the transition from ODUk to OTUk to OCh occurs between the routing areas connected by these links. The structure of the OCh layer topology is two rings interconnected via 3R regenerators. The presence of the regenerators is shown using transitional SNPP links with singleton layer processor icons (diamond shape). This indicates the presence of a client layer (OTU) dependent function between the ends of these links.

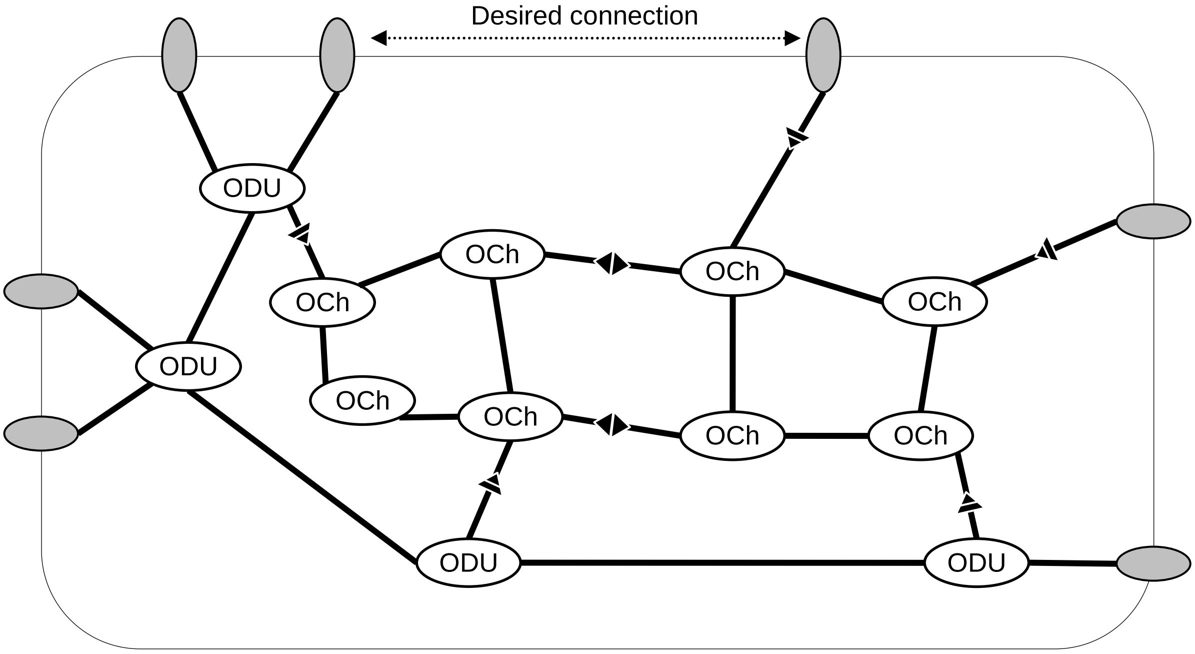


Figure VII.1/G.8080/Y.1304 – Explicit multi-layer topology example

Attributes can be associated with the transitional SNPP links and OCh layer SNPP links that are specific to OCh layer network routing (e.g., modulation type, FEC type, wavelength, etc.). These OCh specific attributes would not be associated with the ODU SNPP links (i.e., those between a pair of ODU routing areas).

This topology may be used to calculate ODUk paths that cross both ODU and OCh routing areas and meet both ODU path constraints and, where necessary, OCh path constraints. This facilitates more optimal route selection across the entire network. The use of an explicit multilayer topology in this case is particularly straightforward since the relationship between ODUk, OTUk, and OCh is 1:1:1. Therefore potential concerns about allocating more server layer resources than are required by the client layer path do not arise.