Question(s):	14			**Meeting, date:**	Chicago, June 9-13, 2003
Study Group:	15	**Working Party**:	3	**Intended type of document** (**R-C-D-TD**): **WD**	**15r1**
Source:	Editors*				
Title:	Draft G.7713 Living List v1.1				

Contact*:

Deborah Brungard
AT&T
200 Laurel Ave., Rm. D1-3C22
Middletown, NJ 07748 USA

Tel: +1 732-420-1573
Email: dbrungard@att.com

Erning Ye
Nortel Networks
PO Box 3511 Station C
Ottawa ON K1Y4H7

Tel: +1 613-765-1058
Email: erningye@nortelnetworks.com

ITU-T Draft Recommendation G.7713 Living List

This document contains the living list for draft Recommendation G.7713. This Living List serves as a basis for future work to enhance and/or modify draft Recommendation G.7713.

Structure

Points of interest for future discussions at Q14 / SG15 meetings are called Study Points. The Study Points are numbered and a brief Title is provided; a status is assigned according to the rules as described below. Dates are given for the creation and the latest modification of a Study Point or as well as a reference to the source document from where the proposal originates.

Beneath each Study Point a description of the problem and one or more possible solutions can be given.

Status of Study Points

U - Under Study: There was a general agreement about the importance and relevance of a given Study Point. Even if a proposal is available, this state indicates that no consensus could be reached.

P - Provisionally Agreed: This is a transitory state. The proposal is in principle accepted but further enhancements are possible at the next meeting if contributions on this subject are available.

A - Agreed: Agreed solutions will be included in the next version of Draft Recommendation G.7713.

D - Deleted: Decision which may be taken i) when relevant material is incorporated in G.7713 or ii) in case of no contributions for a given Study Point.

Living List Procedures

General Principles:

Q14 / SG15 has to decide about the Study Points and their Status to be taken on the Living List;

Insertion of a new Study Point into the Living List is based on contributions submitted to Q14 / SG15 meetings;

A Study Point with Status U will be deleted from the Living List if no contribution addresses this specific issue at the next two subsequent Q14 / SG15 meetings;

All proposed modifications to G.7713 or the corresponding Living List should be made available in a PC compatible electronic version.

Status Transition Rules for Study Points:

Transition from U to P (or A) happens if a agreement on the proposal could be reached during the meeting;

Transition from P to A automatically happens at the next Q14 / SG15 meeting if no contribution contradicts the provisionally agreed solution;

Transition from P to U happens at the next Q14 / SG15 meeting if contradicting contributions are submitted and no consensus can be achieved.

G.7713 Study Point Summary

ID	Title	Old Status	New Status	Remark
1	Misalignment of text on call and connection separation between G.8080 and G.7713		A	
2	Alignment of G.7713 and G.8080 on Call Release Mechanism		U	
3	Alignment of terminology between G.7713 and G.8080		A	
4	Crankback capability		U	
5	Control plane resilience		U	
6	Support for priority and pre-emption		U	
7	SPC and relation to call model		U	
8	Support for value added services		U	
9	Control plane interactions with ring sub-networks		U	
10	Control plane rerouting (restoration)		U	
11	Control plane protection		U	
12	Network Service Category - Policy		U	
13	Separation of call parameter and connection parameter in signalling message		U	

G.7713 Study Points

ID	Title	Status
1	Misalignment of text on call and connection separation between G.8080 and G.7713	A
Created: 11 Feb 02	WD23 and WD03 (Q.14/15 Feb. 2002) discussions	
Modified: 11 Jun 03	WD24 (Q.14/15 June, 2003) discussions	

Description:

G.8080 describes call and connection separation, and call segmentation when a call is across multiple domains . To align with description in G.8080, new figure and text will be added in section 6 in G.7713 to include NCC:

As described in G.8080, the calling party call controller interacts with a called party call controller by means of one or more intermediate network call controllers (NCC). The NCC function is provided at the network edge (i.e., UNI reference point) and may also be provided at gateways between domains (i.e., E-NNI reference point). The functions performed by NCCs at the network edge are defined by the policies associated by interactions between users and network, and the functions performed by NCCs at domain boundaries are defined by the policies associated by the interactions between the domains. As such, an end-to-end call is considered to consist of multiple call segments, when the call traverses multiple domains. Each call segment could have one or more connections (LC or SNC) associated. This allows for flexibility in the choices of signalling, protection and recovery paradigms in different domains.

The number of connections associated with call segments may not be the same even in one end-to-end call. In following Figure, the UNI call segment has one LC associated, the subnetwork call segment for domain 1 has 2 associated SNCs. This allows the network to different policies in their domain.

Note that both calls and connections could be across intra carrier E-NNI reference points. The concept of call segments and call/connection separation enables the following applications:

- Domain based protection. The number of SNCs could be different between domains.
- Domain based restoration. The SNC failure may not cause the LC to go down, and a rerouting procedure could be provided by network to restore the failed SNC (refer to G.8080 amendment).

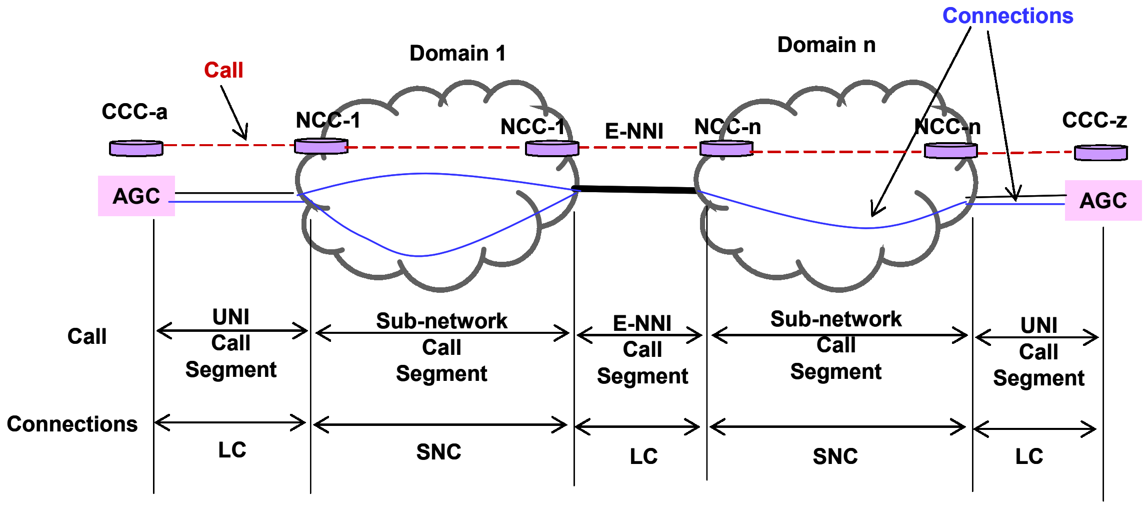


Figure New /G.7713/Y.1704 – Call segmentation and connections

The NCC at domain boundaries will also allow each domain to have independent functions, e.g., one domain could have Vcat capability and other domain does not.

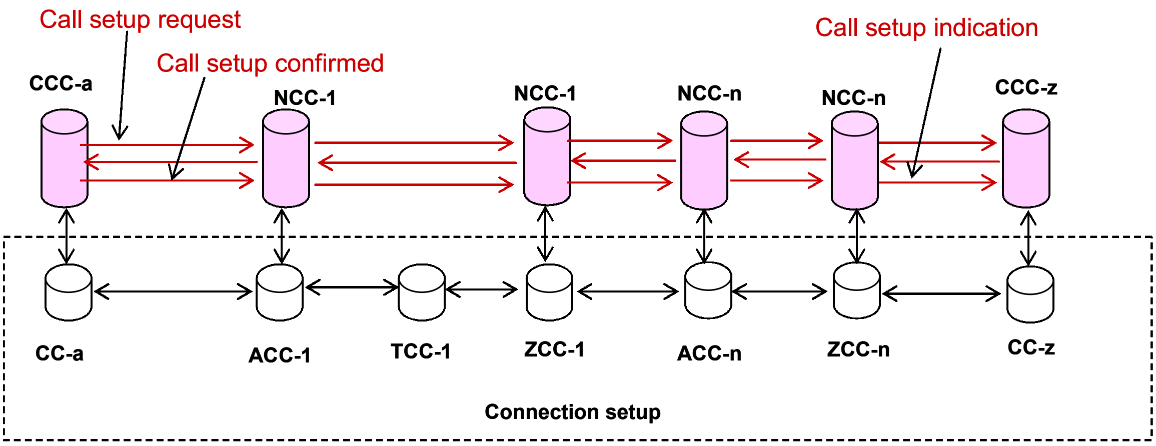
The CallC and CC at network edge and boundaries perform different functions.

The call controllers perform the following:

- The NCC correlates the SNCs to the call.
- The NCC works with the CCC at network edge to correlate LC(s) to the call.
- The NCC works with its peer NCC at domain boundaries to correlate LC(s) to a call.
- NCC correlates the LC and SNCs that associated with the same call.

The CC establishes the connections that are associated to each call segment.

The Figure 6-4 is modified as:

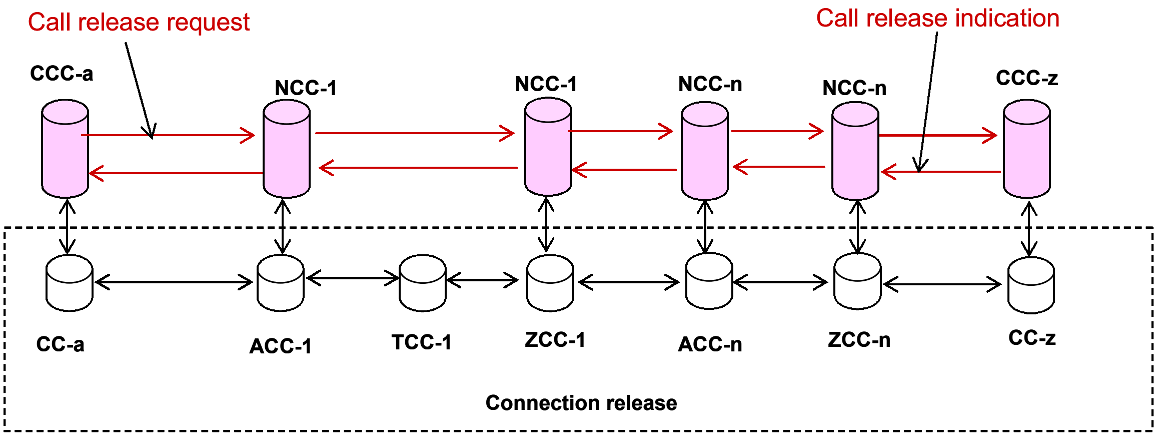


(Modified) Figure 6-4/G.7713/Y.1704 – Call Setup Request Processing: Logical Request Progression

And the text should include:

- interaction between CCC to NCC, NCC to NCC and NCC to CCC
- In the case of multiple SNCs in domain 1, the call setup request should not be forwarded until ZCC-1 receives the connection setup request for all SNCs.
- If the connection setup request process for any connection in the call was unsuccessful, a call denied notification is sent to the user.

Update the Figures 6-5 as:



(Modified) Figure 6-5/G.7713/Y.1704 – Call Release Request Processing: Logical Request Progression

And the text should include:

- interaction between CCC to NCC, NCC to NCC and NCC to CCC
- In the case of multiple SNCs in domain 1, the call release causes releasing of all connections.
- Description of call release sequence and connection release sequence.

To have better understanding on call and connection separation, add following ITU-T Rec. into G.7713 reference list:

- ITU-T Q.1901, Bearer independent call control protocol
- ITU-T Q.2982, Q.2931-based separated call control protocol
- ITU-T Q.2931, User –network interface (UNI) layer 3 specification for basic call/connection control

In addition, there may be other text in G.7713 that may need to be updated. Contributions are solicited on any modifications needed to G.7713.

ID	Title	Status
2	Alignment of G.7713 and G.8080 on Call Release Mechanism	U
Created: 11 Feb 02	WD23 and WD03 (Q.14/15 Feb. 2002) discussions	
Modified: 11 Jun 03	WD24 (Q.14/15 June, 2003) discussions	

Description:

G.8080 provides descriptions of call setup procedures. However, call release procedure were not completed in G.8080. G.7713 provides call release procedures based on assumptions on the requirements for call release. As Q.12/15 initiates work to describe the requirements for call release procedures, G.7713 may need to be updated to align with G.8080.

It was indicated that a communication needs to be sent to Q.12/15 during development of call release.

The call release sequence and connection release sequence in the case of multiple connections are associated to one call needs to be discussed. Whether the call release request should be forwarded to the user when connection release is unsuccessful should be described in section 6.1.1.2.

ID	Title	Status
3	Alignment of terminology between G.7713 and G.8080	A
Created: 11 Feb 02	WD23 and WD03 (Q.14/15 Feb. 2002) discussions	
Modified: 11 Jun 03	WD24 (Q.14/15 June, 2003) discussions	

Description:

To clean up the terms used in existing G.7713 to align with newly proved G.8080, the following terms and definitions will be added:

- Domain – See Recommendation G.8080.
- Access Group Container – See Recommendation G.8080.

With the new terms and definitions, the following sentence in section 5 should be removed:

"NOTE – This Recommendation uses "domain" synonymously with administrative domain and uses requester agent synonymously with user Call Controller."

Other clean up on G.7713 text might be required to make sure the term "domain" is correctly used.

The new term "signalling controller" will be added to include functions of both call control and connection control. The identifier of signalling controller is used to identify the signalling channel that is separated from routing control channel, and used by protocol controller to send signalling messages that is used by connection controllers and/or call controllers. The definition is as follows:

- Signalling controller – A signalling controller contains the functions of connection control and/or call control. An address for signalling control is assigned to the signalling controller and is used by protocol controller to exchange information between call controllers or between connection controllers. The signalling controller address is a control address, and the signalling channel will be identified by two signalling controller names.[S1] The signalling channel is supported by DCN communication.

The figures and text in section 6 should be modified to use new terms and abbreviations. Specially, use correct names (e.g., signalling controller, call controller, connection controller) depends on the context.

The following Abbreviations will be used in G.7713:

Abbreviations for transport components:

➢ AGC	replace User with Access Group Container (AGC).
➢ AGC-a	A-end AGC
➢ AGC-z	Z-end AGC
➢ ASN-n	A-end SN in domain n.
➢ TSN-n	Transit SN in domain n
➢ ZSN-n	Z-end SN in domain n

Abbreviations for control plane components:

For connection controllers:

➢ CC	Connection Controller
➢ CC-a	A-end CC
➢ CC-z	Z-end CC
➢ ACC-n	A-end CC at domain n

- TCC-n Transit CC in domain n
- ZCC-n Z-end CC at domain n

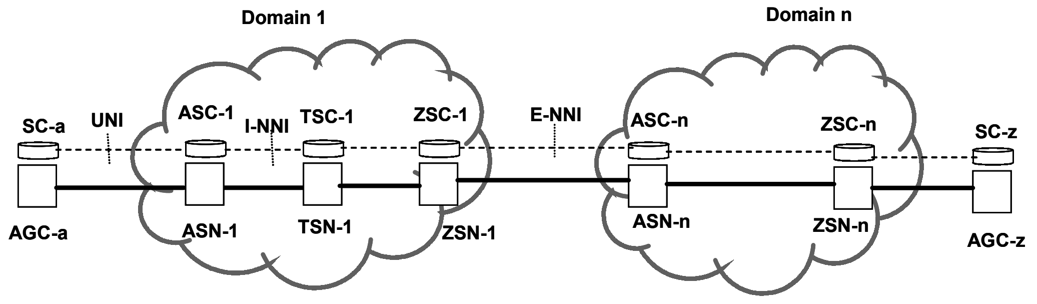
For call controllers:

- CCC Calling/Called Party Call Controller
- CCC-a A-end CCC
- CCC-z Z-end CCC
- NCC Network Call Controller
- NCC-n NCC in domain n

For signalling controllers:

- ASC-n A-end signalling controller in domain n
- TSC-n Transit signalling controller in domain n
- SC Signalling controller
- SC-a A-end user signalling controller
- SC-z Z-end user signalling controller
- ZSC-n Z-end signalling controller at domain n

With these changes, the Figure 5-1 will be updated as:



AGC-a	A-end user	SC-a	A-end user signaling controller (CCC and CC)
AGC-z	Z-end user	SC-z	Z-end user signaling controller (CCC and CC)
ASN-1	A-end subnetwork in domain 1	ASC-1	A-end signaling controller in domain 1 (NCC and CC)
TSN-1	Transit subnetwork in domain 1	TSC-1	Transit signaling controller in domain 1 (CC)
ZSN-1	Z-end subnetwork in domain 1	ZSC-1	Z-end signaling controller in domain 1 (NCC and CC)
ASN-n	A-end subnetwork in domain n	ASC-n	A-end signaling controller in domain n (NCC and CC)
ZSN-n	Z-end subnetwork in domain n	ASC-n	Z-end signaling controller in domain n (NCC and CC)

(Modified) Figure5-1/G.7713/Y1704 – Reference diagram for distributed connection management

In addition to these terminologies, G.7713 will also align with terminologies introduced in SP5 of G.8080 living list.

ID	Title	Status
4	Crankback capability	U
Created: 11 Feb 02	WD16 discussions	

Description:

G.7713 currently describes crankback in Section 6.1.2.1 in a high level view. However, the protocols currently do not support this capability. Prior to supporting this, an architectural model and requirements need to first be specified by Q.12/15 for this capability.

ID	Title	Status
5	Control plane resilience	U
Created: 3 May 02	TD33 (WP3), 29 April – 10 May 2002	

Description:

Control plane needs to support the necessary options to ensure that no service-affecting module of the control plane (software module or control plane communications) is a single point of failure. Existing connections must not be affected by any failures within the control plane of any node.

The control plane should support options to enable it to self-heal, i.e., if the control plane node fails it should have the capability to automatically recover from the failure.

A failure detection mechanism that detects control plane failures should be provided that allows for reporting of such failures to the management system. The detection mechanism should allow for detection of control plane failure types. Additionally the control plane detection mechanism may provide information that allows for localization of the faults. The types of failure are for further study.

ID	Title	Status
6	Support for priority and pre-emption	U
Created: 3 May 02	TD33 (WP3), 29 April – 10 May 2002	

Description:

ID	Title	Status
7	SPC and relation to call model	U
Created: 6 May 02	D.427 (WP3), 29 April – 10 May 2002	

Description:

SPC service uses the control plane to establish connections between two clients whose connection to the network do not have UNI signalling capability, only bearer service. While G.8080 has call and connection separation this is described generally and the use of the call model is quite clear for Switched Service. Additional clarity is needed regarding the use of the call model for SPC. Applications of the call model to SPC service should be explored including interworking between an SC user and SPC user, and multiple connections associated with a single SPC service instance.

ID	Title	Status
8	Support for value added services	U
Created: 8 Oct 02	WD 16, WD17 – Q14/15 Rapporteur’s Meeting, Ottawa, 7-11 October 2002	

Description:

The CoS, GoS, Security, and Recovery attributes have been nominated as the means for specifying value added services as well as other basic service features. The following have been proposed as issues to be resolved in version 2 of G.7713.

1. ASON specific definitions are needed for both CoS and GoS. Recommendation G.7713 offers no definition for either term..
2. It is expected that the CoS, GoS, Security, and Recovery cannot be scalar valued.
3. A procedure for allocating UNI CoS and GoS component service levels across domains is required. In some instances it is expected that process for apportioning numeric values among domains would be required. In other cases, binary values may be used.
4. The requirement for interoperability between signalling protocols implies that all protocols defined the attributes with an end-to-end scope using the same set of primitive terms. This does not imply that all protocols use the same attributes.
5. A specific document(s) should be identified to record the mapping between protocols. Ideally, these mappings should be one to one and onto.
6. As SPC and SC both use I-NNI and E-NNI signalling, it is desirable that common definitions be used for both.
7. Policy Attributes must be used consistently in Call Signalling and in connection signalling.

Contributions on these topics are invited.

ID	Title	Status
9	Control plane interactions with ring sub-networks	U
Created: 9 Oct 02	WD 06 – Q14/15 Rapporteur’s Meeting, Ottawa, 7-11 October 2002	

Description:

In many networks, control plane functional components may co-exist with ring sub-network protection mechanisms. The above contribution shows how existing control plane mechanisms are adequate to provide initial (simple) support for ASON control plane connection management to be added to an ASON ring sub-network (i.e. existing protocol specification is adequate and no new extensions are needed). There may be impacts on what information is exchanged for the discovery process (e.g. service capability exchange) and what information is exchanged for the route information dissemination.

Further study is needed to examine the general interaction of the control plane components with the transport plane’s protection mechanisms.

ID	Title	Status
10	Control plane rerouting (restoration)	U
Created: 9 Jun 03	TD33 (WP3), 29 April – 10 May 2002, WD 30 – Q14/15 Rapporteur’s Meeting, Naperville, 9-12 June 2003	

Description:

TD33 (WP3):

During the course of trying to protect a failed connection, the restoration attempt also fails, the control plane must clean up any partial connections left as a result of unsuccessful restoration attempt.

Any restoration actions should be notified to the management plane.

For scenarios with nested restoration domains set up to support restoration, a failed connection may cause alarms to propagate to more than one restoration domain. A mechanism should be defined to prevent alarms from propagating beyond a restoration domain. Alternatively a mechanism should be available that notifies downstream restoration domains to suppress restoration action. This is similar to the use of ARCmode, but for the control plane.

Control channel and signaling software failures shall not cause management plane failures. G.7713 currently does not cover the case of detecting control plane failure and preventing a control plane failure from affecting the management plane. Example failures may include CP messages flooding the MP. Note that the control plane may detect the type of failure, but mechanism to ensure control plane misbehavior does not impact the management plane may reside in the management plane itself.

Bulk restoration capability, e.g., recovering at link instead of link connection.

Protection mechanism could protect against fiber cuts. This implies the protection is at the physical layer.

Which of the protection mechanism should be supported: 1+1/1:1/1:n protection.

Should support shared protection and restoration

Dual ended restoration action, even in the case of single-ended failure.

Support for dual interconnection between domains.

The control plane must identify, assign, and track multiple protection and restoration options.

WD30:

Provides terminology on restoration from G.8080 as a basis for developing signalling requirements:

restoration: a network survivability technique for which the recovery resource is established at the time of the restoration action. For control plane restoration the configuration of the restoration and restoration action is under the direction of the control plane (vs. the management plane controls the resources for management-based restoration).

control plane rerouting domain: a rerouting domain provides a restoration survivability mechanism for a connection in the event of an impairment affecting the connection. 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. Restoration of a call is the replacement of a failed connection by rerouting the call using spare capacity. Some or all of the SNPs used to support the connection may be changed during a restoration event. A rerouting domain must be entirely contained within a routing domain or area. A routing domain may fully contain several rerouting domains.

inter-domain interface: an interface at the ingress or egress of a rerouting domain.

intra-domain (single domain) rerouting service: rerouting service for a call within a rerouting domain. Negotiated between the source and destination (connection and call controller) components within the rerouting domain. Connections are not rerouted across an inter-domain interface.

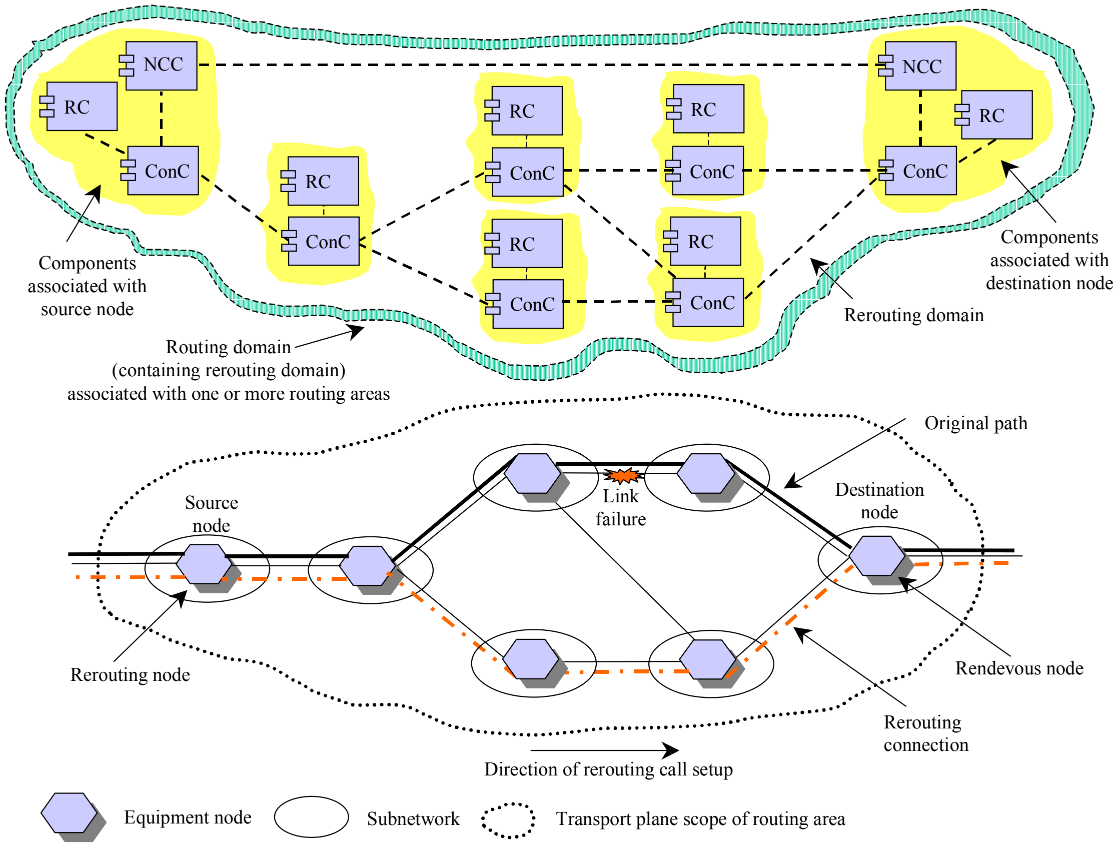
inter-domain rerouting service: rerouting service for a call across multiple rerouting domains. Edge components of each rerouting domain negotiate the activation of the rerouting services across the rerouting domain for each call. The rerouting service is requested on an end-to-end basis, the service is performed per rerouting domain.

hard rerouting (break-before-make): failure recovery mechanism for calls and is always in response to a failure event.

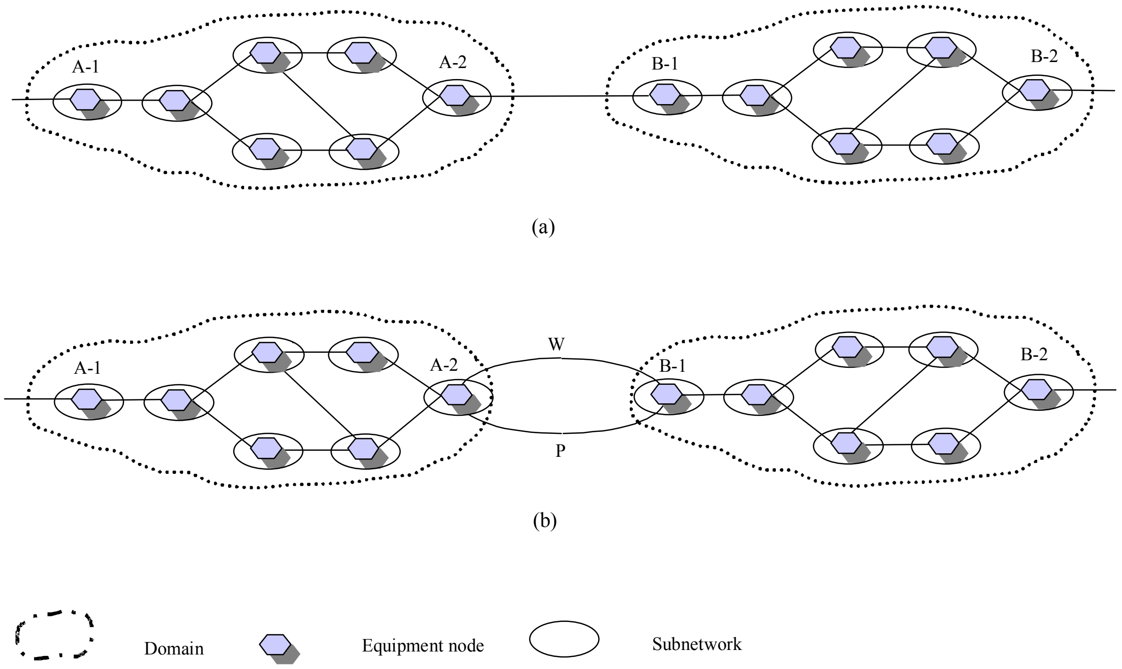
soft rerouting (make-before-break) service can be used for path optimisation, network maintenance, and planned engineering work. When a rerouting operation is triggered (generally via a request from the management plane) and sent to the rerouting component. The rerouting component establishes a rerouting connection, once it is established and the connection switches over to use it, the initial connection is deleted.

The following three scenarios from G.8080 Amendment can be used for developing rerouting requirements:

Figure 29.2 showing an intra-domain failure/hard rerouting:

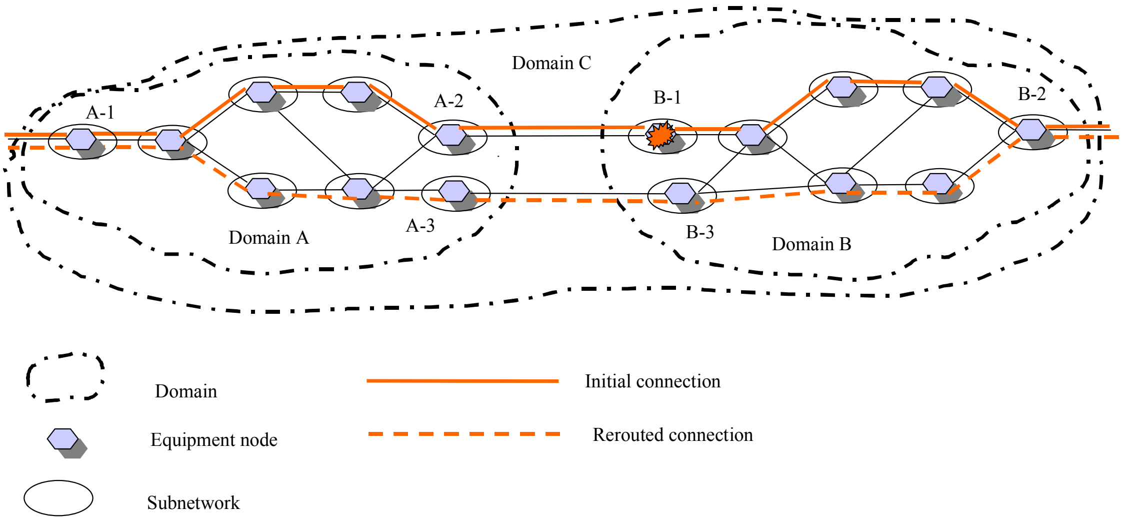


And Fig 29.3 and Fig 29.4 on inter-domain:



(a)

(b)



Note, in the above figure, to recover using a different gateway (B-1 failure), the failure indication message needs to indicate (in addition to the failure notification) that rerouting between A-1 and A-2 is to be avoided.

ID	Title	Status
11	Control plane protection	U
Created: 9 Jun 03	WD 30 – Q14/15 Rapporteur's Meeting, Naperville, 9-12 June 2003	

Description:

WD30:

Provides terminology from G.8080 to be used as a basis for developing signalling requirements:
recovery domain: A recovery domain provides a single type of survivability mechanism. A recovery domain may contain other recovery domains and recovery domains may overlap.

transport recovery mechanism: recovery mechanism provided by the transport plane. The transport plane provides resource management for the recovery resources.

control plane recovery mechanism: recovery mechanism provided by the control plane. The control plane provides resource management for the recovery resources.

protection: a network survivability technique with dedicated protection resource allocation policy for the recovery resource. For control plane protection the configuration of the protection is under the direction of the control plane (vs. the management plane which controls the resources for transport protection).

control plane protection domain: a protection domain provides a survivability mechanism for a connection in the event of impairment affecting the connection. Control plane protection occurs between the source connection controller and the destination connection controller of the protection domain. Protection uses additional assigned capacity, 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. A protection domain must be entirely contained within a routing domain or area. Multiple protection schemes will be needed e.g. 1+1, m:n.

ID	Title	Status
12	Network Service Category - Policy	12
Created: 9 Jun 03	WD 30 – Q14/15 Rapporteur's Meeting, Naperville, 9-12 June 2003	

Description:

WD30:

In addition to control plane recovery, an operator needs the ability to control connection set-ups across a domain using a transport plane-based or management plane-based recovery scheme. Transport plane protection may be provided by a server layer or within a layer. Transport plane protection by a server layer is invisible to the SNP of the client layer. Transport plane protection within a layer is modelled as a sub-layer connection; the resources are allocated/managed by the management/transport plane. The SNP for this sub-layer connection is invisible to the control plane. WD30 proposes defining a generic policy routing constraint attribute "network service category (NSC)" that a service provider can use to manage resources with a greater service granularity to indicate network specific criteria or resource utilisation strategy for a domain. For example, a NSC may be used to identify links in the network that have different server layer resiliency capabilities (and then use this to differentiate the associated resources for routing, including resource partitioning). The semantics (definitions) associated with a NSC are not necessarily limited to resiliency aspects; they are specific to each service provider's network and are beyond the scope of standardisation.

Terminology:

Policy routing within the same routing domain: supported at an interface between different domains within the same routing domain, with the constraint that the semantics associated with advertised NSCs must be consistent throughout the entire routing domain. At UNIs and interfaces between routing domains, procedures are required to map policy constraints.

Network Service Category: generic policy attribute that a service provider can use to indicate if a network node, set of resources, bypass (tunnel), area, set of reachable addresses, etc., is acceptable for carrying a given connection.

Policy: set of requirements on network entities and resources (expressed via policy operators and lists of NSCs) that may be used to route a connection. When performing path selection, the topological map of the network is pruned, leaving only the network entities and resources that match the policy. The resulting network topology map is then used during path selection.

Policy constraint: ordered list of one or more policies that must be considered during connection routing and connection establishment for a given connection.

Policy operator: policy operator defines how a list of NSCs specified in a policy is used to prune a network topology map, allowing or forbidding access to network entities or resources during connection establishment. The supported policy operators are “require logical set of NSCs”, or “must avoid logical set of NSCs”.

ID	Title	Status
13	Separation of call parameter and connection parameter in signalling message	U
Created: 11 Jun 03	WD24 (Q.14/15 June, 2003) discussions	

Description:

It is agreed that the call is different from the connection, so that they have the different attributes. Since the same information elements in the signalling messages are used by both call and connection. It is important to give clear description to separate the call attributes from the connection attributes in section 7. The table 7-1, 7-2 and 7-3 are also required to be updated to reflect call/connection separation.

Also, for all attributes related to address should separate transport address from signalling address space. The identifier of connection termination point must use transport address.