INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 15 – LS 1 – E

English only

Original: English

Question(s): 9/15

LIAISON STATEMENT

Source: ITU-T SG15 Qs.9 & 12/15

Title: Liaison to IEEE P802.1 & 802.17 from ITU-T SG15 on protection and Restoration

LIAISON STATEMENT

To: **Mike Takefman, chair IEEE 802.17** (tak@cisco.com)**, Tony Jeffree, chair IEEE 802.1** (tony@jeffree.co.uk)

Cc: **Paul Nikolich, IEEE 802 Chair (**p.nikolich@ieee.org)

Approval: **Agreed to at Q.9 interim meeting at Sophia Antipolis, September 2006**

For: **Information**

Deadline: **November 2006**

Contact: Ghani Abbas
Rapporteur Q.9/15
Email: ghani.abbas@marconi.com

We would like to thank you for your liaison informing us of the potential issues with defining Ethernet ring protection and of the applicability of RPR. We would like to offer some clarity on our work.

In ITU-T, we distinguish between protection and restoration of connections. This is clearly defined in G.805-2000 “Functional Architecture of Transport Networks” Clause 7.1 and further explained in G.8080-2006 “Automatically Switched Optical Network” Clause 11 (both are attached to this liaison for reference). However, some of the differences could be summarized as:

Protection makes use of pre-assigned capacity between nodes.

Restoration makes use of any capacity available between nodes.

It is not clear if there is any distinction in IEEE.

Note that 50 ms is the target time for protection switching in G.841-1998 “SDH Network Characteristics” and G.8031-2006 “Ethernet Protection Switching”.

It is our view that STP as defined in 802.1Q provides Ethernet restoration. The work of Q9 is specifically on Ethernet protection. ITU-T G.8031 currently defines Ethernet linear protection, and we are evaluating Ethernet ring protection.

We wish to thank IEEE 802 for your response to our previous liaison and look forward to the continuation of the exchange of information on topics of common interest to our organizations.

Regards,

Ghani Abbas

ANNEX A
Excerpt from G.805-2000

7 Transport network availability enhancement techniques

7.1 Introduction

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

Protection – This makes use of pre-assigned capacity between nodes. The simplest architecture has one dedicated protection entity for each working entity (1 + 1). The most complex architecture has m protection entities shared amongst n working entities (m:n). Protection switching may be either unidirectional or bidirectional. Bidirectional protection switching takes switching actions for both traffic directions, even when the failure is unidirectional. Unidirectional protection switching takes switching actions only for the affected traffic direction in the case of a unidirectional failure.

Restoration – This makes use of any capacity available between nodes. In general the algorithms used for restoration will involve rerouting. When restoration is used some percentage of the transport network capacity will be reserved for rerouting of working traffic. Further description of restoration is not within the scope of this Recommendation.

ANNEX B
Excerpt from G.8080-2006

11 Connection availability enhancement techniques

This clause describes the strategies that can be used to maintain the integrity of an existing call in the event of failures within the transport network.

ITU-T Rec. G.805 describes transport network availability enhancement techniques. The terms "Protection" (replacement of a failed resource with a pre-assigned standby) and "Restoration" (replacement of a failed resource by re-routing using spare capacity) are used to classify these techniques. In general, protection actions complete in the tens of millisecond range, while restoration actions normally complete in times ranging from hundreds of milliseconds to up to a few seconds.

The ASON control plane provides a network operator with the ability to offer a user calls with a selectable class of service (CoS), (e.g. availability, duration of interruptions, Errored Seconds, etc). Protection and restoration are mechanisms (used by the network) to support the CoS requested by the user. The selection of the survivability mechanism (protection, restoration or none) for a particular connection that supports a call will be based on: the policy of the network operator, the topology of the network and the capability of the equipment deployed. Different survivability mechanisms may be used on the connections that are concatenated to provide a call. If a call transits the network of more than one operator then each network should be responsible for the survivability of the transit connections. Connection requests at the UNI or E-NNI will contain only the requested CoS, not an explicit protection or restoration type.

The protection or restoration of a connection may be invoked or temporarily disabled by a command from the management plane. These commands may be used to allow scheduled maintenance activities to be performed. They may also be used to override the automatic operations under some exceptional failure conditions.

The Protection or Restoration mechanism should:

Be independent of, and support any, client type (e.g. IP, ATM, SDH, Ethernet).

Provide scalability to accommodate a catastrophic failure in a server layer, such as a fiber cable cut, which impacts a large number client layer connections that need to be restored simultaneously and rapidly.

Utilize a robust and efficient signalling mechanism, which remains functional even after a failure in the transport or signalling network.

Not rely on functions which are non-time critical to initiate protection or restoration actions. Therefore consideration should be given to protection or restoration schemes that do not depend on fault localization.

The description of how protection and restoration capabilities are used by the transport, control and management planes of an ASON enabled network is for further study.

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 control domain or area. A Routing control 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 41. In this example the Routing control 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 connection for administrative purposes (e.g. path optimisation, 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 rendezvous 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.

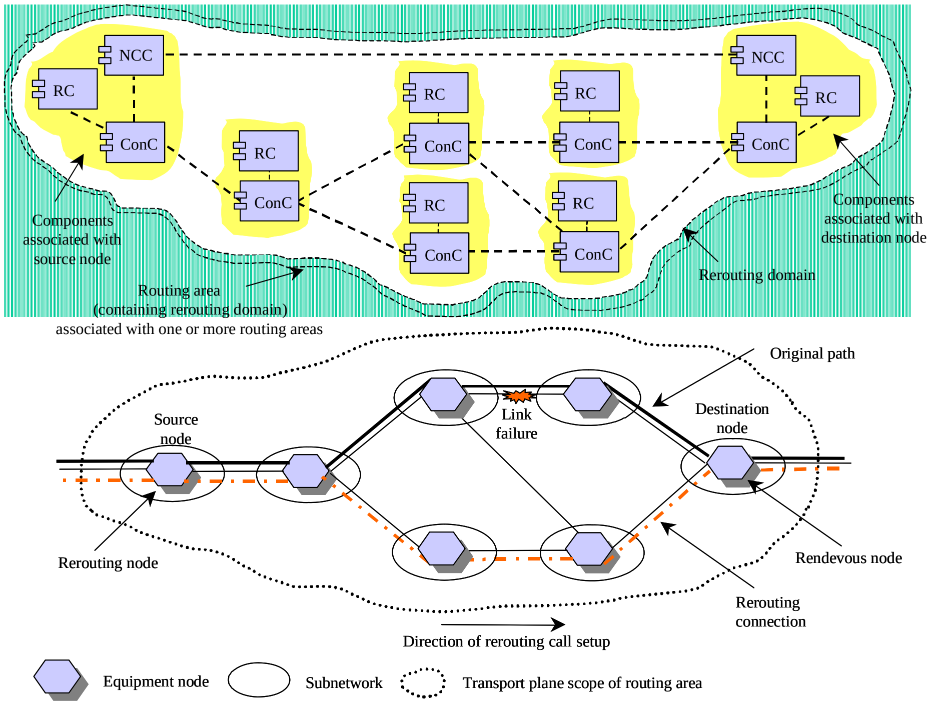
NCC
RC
ConC
RC
ConC
RC
ConC
RC
ConC
RC
ConC
RC
ConC
NCC
RC
ConC
Components associated with source node
Routing area (containing rerouting domain) associated with one or more routing areas
Rerouting domain
Components associated with destination node
Original path
Source node
Link failure
Destination node
Rerouting node
Rendevous node
Rerouting connection
Direction of rerouting call setup
Equipment node
Subnetwork
Transport plane scope of routing area

Figure 41/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 42a no rerouting operation can be performed. In this case alternative protection mechanisms may be employed between the domains. Figure 42b 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.

Comment [MGM1]: Figure 42 moved to section 11.2.1.3 as per AAP comment NN9

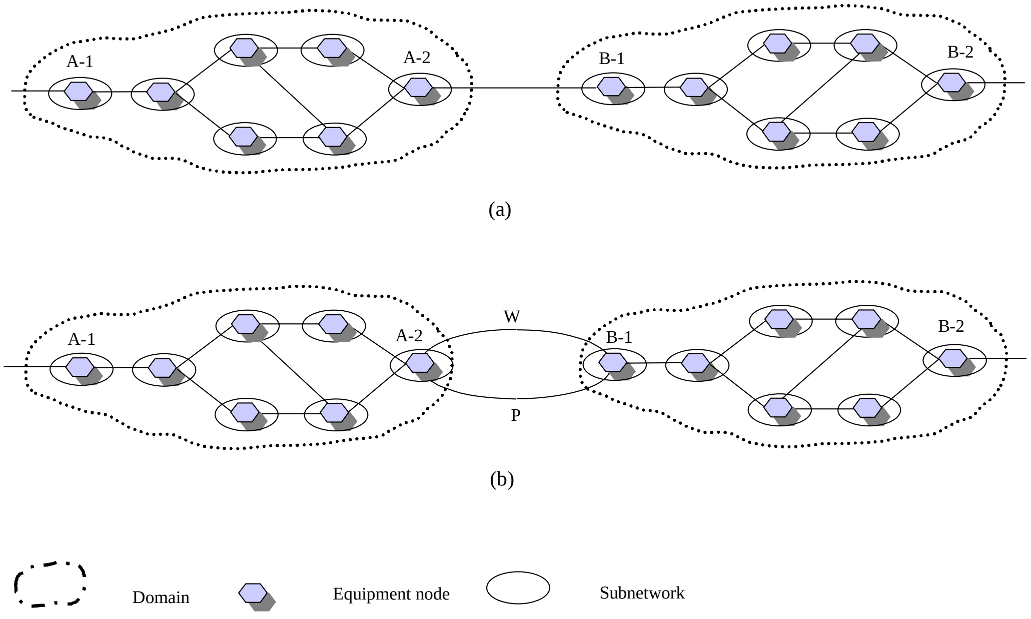

Figure 42/G.8080/Y.1304: Link failure scenarios

11.2.1.4 Gateway Network Element Failure

This case is shown in Figure 43. 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.

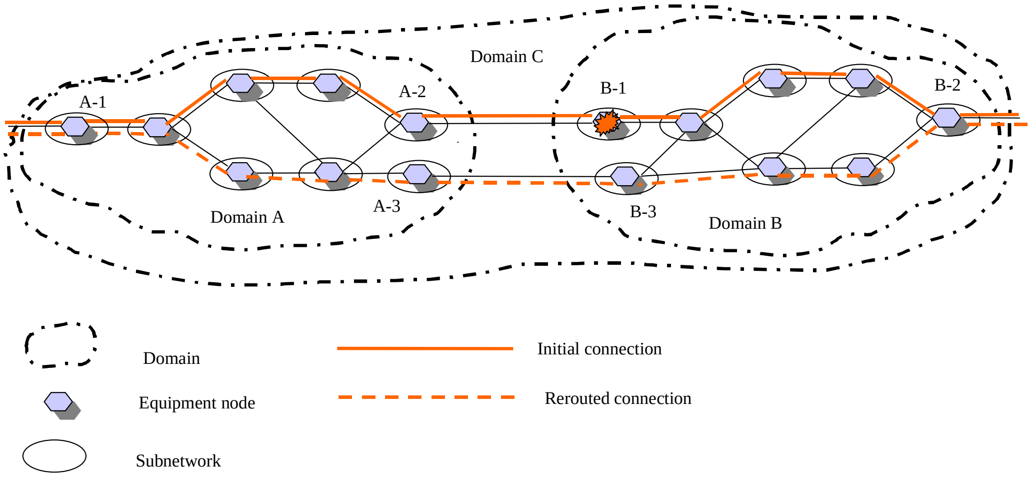

Figure 43/G.8080/Y.1304: Rerouting in event of a gateway network element failure