Network Interconnect Resiliency Requirements

János Farkas
The two independent providers have equal rights, none of them is inferior to the other; thus

The network providers may have independent decisions

The **Network Interconnect (NI)** has to adapt to providers’ decisions and provide the connectivity

NI has its own control: the **Network Interconnect Protocol (NIP)**, which is independent from the control of the attached networks
A provider may select an NI node for a service independently of the peering provider’s selection.

The service assignment is done by the provider (either by configuration or by a protocol run by the provider).

For example:

- Network 1 selects NI node A for service S
- Network 2 selects NI node D for service S

Bundling maybe supported.
R2 – NI failure isolation

› NI failure should not cause state change in the provider networks’ control protocols
  - Link failure
    › NI failure should not cause state change in any of the attached networks
  - Node failure
    › Affects the provider network comprising the node
    › Provider has to re-assign affected services
    › NI failure should not cause state change in the non-affected network

› Provider network failure may cause state change in the NI (e.g. a service is re-assigned due to a failure)
R3 – Failover time

› Link failure
  – NI should provide sub 50 msec failover time for link failures

› Node failure
  – Time constraint shouldn’t be put on the entire failover
  – The provider has to re-assign the affected service(s)
  – NI then adapts to the service re-assignment
  – Time constraint could be put on NI adaptation
R4 – Connectivity

- NIP should provide loop-free connectivity between the attached networks
- NIP should adapt to service assignments

- NIP should ensure that frames are not looped
R5 – Congruency

› Congruency should be supported
  – The same path used in the NI for the two directions of a service

› Forwarding path may not be optimal due to the independent assignments
  – Providers may agree in the service assignments in order to use a direct link
  – Or one of them may relax service assignment for optimal path
If congruency is not applied

- Non-congruent NI forwarding paths

- Other means are needed to avoid loops
R6 – NI topology

› NI topology should be at least two-connected
› Connection between NI nodes of the same provider
  – An NI node should be connected to at least another NI node belonging to the same provider
  – The connection maybe physical or virtual

› NI topology might be arbitrary otherwise
Consequence – Load balancing

› Service by service assignment provides support for load balancing
Mapping the list of "criteria or potential requirements" from the Webex meetings

- 01 Protect a single service (VLAN) or a group of services (VLAN) – R2
- 02 Protect against any single failure or degradation of a facility (link or node) in the interconnected zone – R2
- 03 Support interconnection between different network types (e.g. CN-PBN, PBN-PBN, PBN-PBBN, PBBN-PBBN, etc.) – R4
- 04 Provide sub-50 ms fault recovery – R3
- 05 Provide a clear indication of the protection state – R2
- 06 Avoid modifying the protocols running inside each of the interconnected networks – R2
- 07 Maintain an agnostic approach regarding – R4:
  - the network technology running on each of the interconnected networks, and
  - any protection mechanism deployed by each of the interconnected networks
- 08 Allow load-balancing between the interfaces that connect the networks to ensure efficient utilization of resources – R1
- 09 The effects of protection events in the interconnected zone on the topology of the related attached networks should be minimized. – R2
- 10 Design the interconnected zone in a way that will ensure determinism and predictability.
- 11 There can be at least one failure in every provider cloud, and at least one failure in every interconnect cloud, and connectivity will still be maintained. – R2
- 12 Support topologies with more than two nodes and more than two inter-cloud links, so that equipment can be taken down and replaced without a period of unprotected operation. – R6
- 13 Control packets cannot be 1:1 with customer services; that is, some kind of bundling is necessary in order to support thousands of services. – R1
- 14 The bundling of services for protection purposes (e.g. MST instances) can be completely different in different service provider clouds. – R1
- 15 The NNI protects services, not parts of services. – R1
- 16 If one service provider cloud becomes split into multiple disjoint clouds, it cannot depend on the interconnect cloud or any adjacent service provider cloud to provide connectivity among its parts.
- 17 We cannot assume an ultra-reliable link. – R6
- 18 It must be possible to ensure the use of the same link in both directions for every service. – R5
- 19 Inter-domain coordination should be minimized. – R1
- 20 Support asymmetrical links – not all the same speed or cost – R5
- 21 Do we support a encapsulation scheme in the interconnect cloud, or is the ENNI independent of the encapsulation?
- 22 Do we assume that the bandwidth (or other Traffic Engineering parameter) of the interconnect cloud is adequate for all of the services, or do we do something special if it is insufficient?
- 23 Do we need protocol for conveying service creating/deletion or traffic engineering requirements between Service Providers?