Requirements for Carrier Ethernet Service Protection over UNIs and E-NNIs

Zehavit Alon
Nurit Sprecher
Rao Cherukuri
John Lemon

January 2010

Nokia Siemens Networks

Recap

The subject of Carrier Ethernet Service Protection over external interfaces (UNIs and E-NNIs) was discussed. The proposal to define a protection mechanism for these interfaces appears to have aroused significant interest.

The MEF created an ad hoc project and is initiating a study that will define the MEF requirements for protection over external interfaces.

The IEEE also needs to finalize the requirements on the protection mechanism in the interconnected zone and the connectivity construct.

Requirements
Agreed (1)

1. Protect a single service (VLAN) or a group of services (VLAN)
2. Ensure that all frame types (unicast, multicast, and broadcast) are delivered once only over the interconnected zone
3. Protect against any single failure or degradation of a facility (link or node) in the interconnected zone
4. Support interconnection between different network types (e.g. CN-PBN, PBN-PBN, PBN-PBBN, PBBN-PBBN, etc.)
5. Provide sub-50 ms protection switching
6. Provide pre-provisioned protection paths
7. Provide a clear indication of the protection state
8. Avoid modifying the protocols running inside each of the interconnected networks

Requirements (cont'd)

Agreed (2)

9. Maintain an agnostic approach regarding:
   - the network technology running on each of the interconnected networks, and
   - any protection mechanism deployed by each of the interconnected networks
10. Allow load-balancing between the interfaces that connect the networks to ensure efficient utilization of resources
11. The effects of protection events in the interconnected zone on the topology of the related attached networks should be minimized and reduced to the level of unavoidable effects.
12. Design the interconnected zone in a way that will ensure determinism and predictability.

Requirements (cont'd.)

Open issues (1)

1. Supported topologies – should the protocol support any arbitrary topology connecting the attached network, or should it be optimized for the topology which is perceived to be the best? ▶
2. Connectivity type – should the protecting nodes be connected directly/indirectly? ▶
3. Number of links and nodes to protect a single service. Should the number of links and nodes be fixed and pre-determined, or should it be variable with dynamic changes? ▶
4. Should all the nodes participating in the protection mechanism be perceived as a single node (from the network perspective) to avoid modifying the EVC and OVC configuration, and to obviate MAC learning issues (as described in Steve's presentation http://www.ieee802.org/1/files/public/docs2009/new-haddock-ENNI-redundancy-1109-v1.pdf)? ▶

Requirements (cont'd.)

Open issues (2)

5. Should the links be used for other purposes (such as conveying data inside the network), or should they be dedicated links, used solely to transmit traffic between the networks?
6. Should the mechanism support the I-interface and be capable of functioning at the I-SID level (2^24 services)?

Recommendations

- Close the open issues
- Start a new project in the IEEE 802.1 aimed at defining a protection mechanism for Ethernet services over UNI/E-NNI (interconnected networks) with the following scope:
  - Static configuration in the first phase.
    - Add dynamicity (if required) in future projects
  - Maximum of two nodes in each network and two links traversing the interconnected zone in each node in the first phase.
    - Add nodes and links (if required) in future projects
  - Provide bypass functionality to minimize effects of a protection event caused by a link failure on the attached network.

Thank You

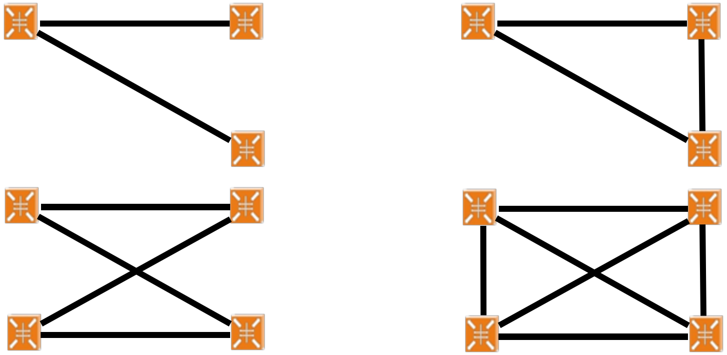
zehavit.alon@nsn.com
nurit.sprecher@nsn.com
cherukuri@juniper.net
jlemon@ieee.org

Backup slides

Supported topologies

As described in the past, mesh (full/partial) is the most efficient topology for the interconnected zone.

(http://www.ieee802.org/1/files/public/docs2009/new-alon-service-protection-in-interconnectned-areas-0509-v01.ppt)



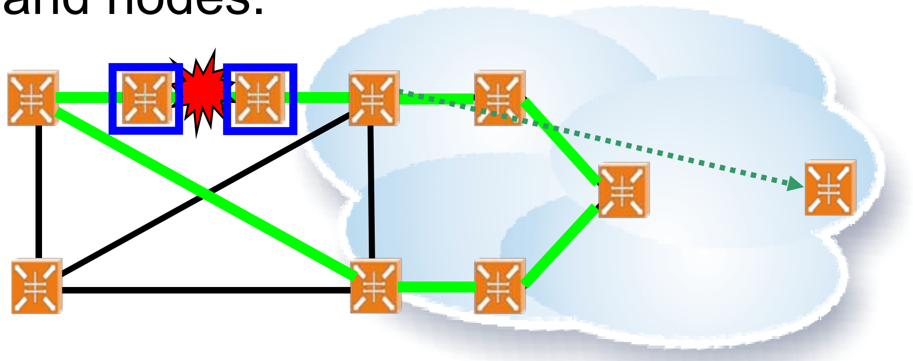
Creating a general protocol to support any arbitrary topology will complicate the protocol and may fail to provide the optimal and simplest functionality.

Example: As xSTP was designed to be applicable to any arbitrary topology, it was necessary to define an optimized mechanism for ring topologies – G.8032.

Connectivity type (1)

Direct or indirect

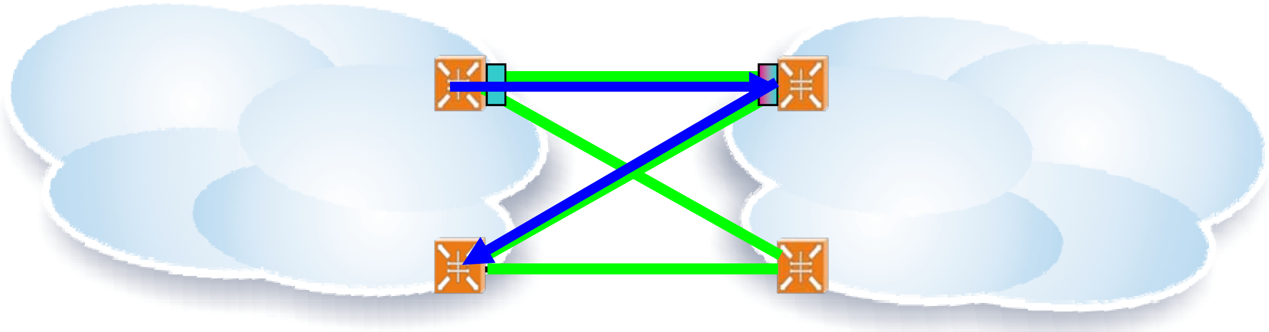
- Do we want inter-network connectivity to span more than one hop?
  - In this scenario, who will own the intermediate links and nodes and who will be responsible for their configuration and maintenance?
- Do we want the internal connectivity to use existing network resources instead of a dedicated link?
  - When attempting to avoid topology changes in the attached network in case of link failure, data packets will travel inside the attached network, consuming network resources and increasing latency.
  - Connectivity will be less robust, since it will be subject to failure of the additional links and nodes.



Connectivity type (2)

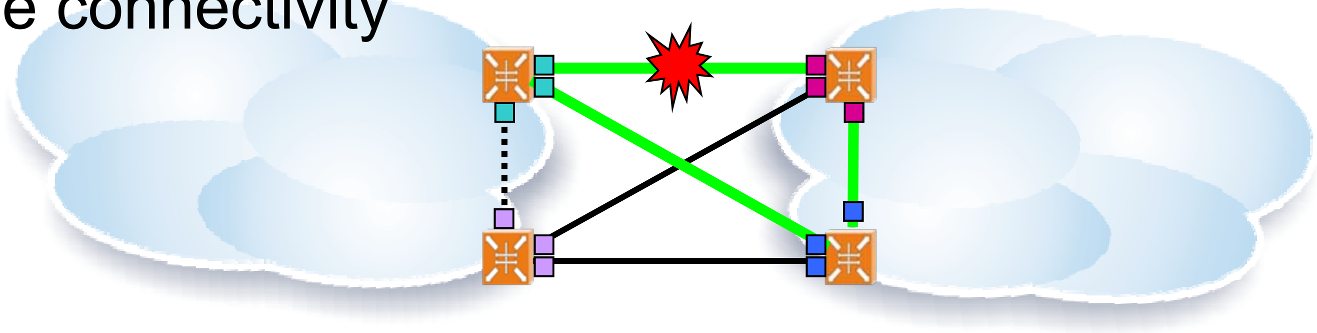
Data and control packets without internal link

- Connectivity between the networks is mandatory.
- Data packets are transmitted from one network to another over one of the links connecting the networks.
- In principle, protection states can be synchronized between the nodes owing to existing, indirect connectivity between the nodes. There is no need for additional, indirect connectivity for synchronization.



Connectivity type (3)
Data and control packets with internal link

- Direct connectivity between nodes in the same network (internal link) is optional.
- The main benefit of the internal link is that it minimizes the effects of protection events in the interconnected zone on the topology of the related attached networks by reducing them to the level of unavoidable effects.
  - The internal link can be used by data traffic to bypass a failed link
- State is synchronized between control nodes using all available connectivity



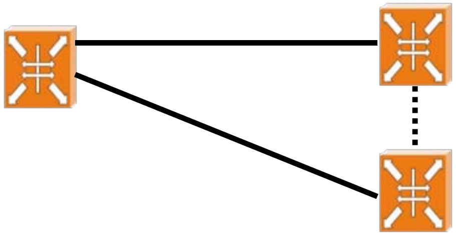
Connectivity type (4)

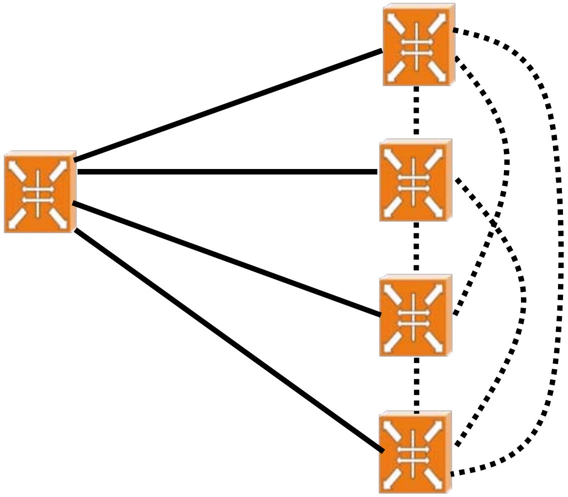
Date and control packets

- Connectivity between the networks is mandatory. This is the way data packets are transmitted from one network to the next.
- Connectivity between nodes in the same network is optional.
- **Data** frames
  - are always transmitted over one specific link which traverses the interconnected zone
  - may optionally traverse the internal link so as to avoid topology changes in the attached network.
- **Control** frames are link-level messages which are continuously transmitted over all links in order to monitor link health and coordinate the protection state.

Number of links and nodes (1)
Number of links per service per node

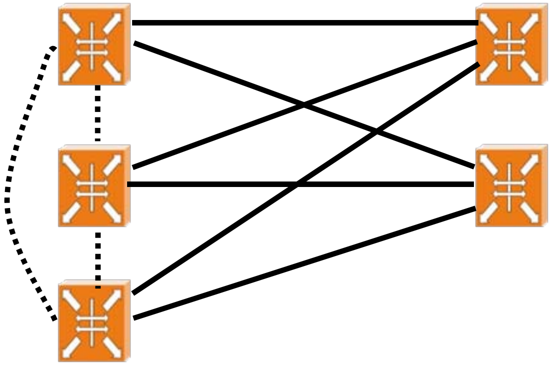
- Two links are needed to protect a service in a single node. These links can be prioritized by configuration. The highest available priority link will be chosen to convey traffic.
  - An optional, internal link may also be present to prevent topology changes.
- More than two links can be considered (to support bulk maintenance operations).
- Full mesh connectivity between the nodes in the attached network is required to minimize interruption in the attached network,
  - This will introduce significant complexity while its benefits are debatable. (Maintenance operations are usually performed gradually.)





Number of links and nodes (2)
Number of nodes

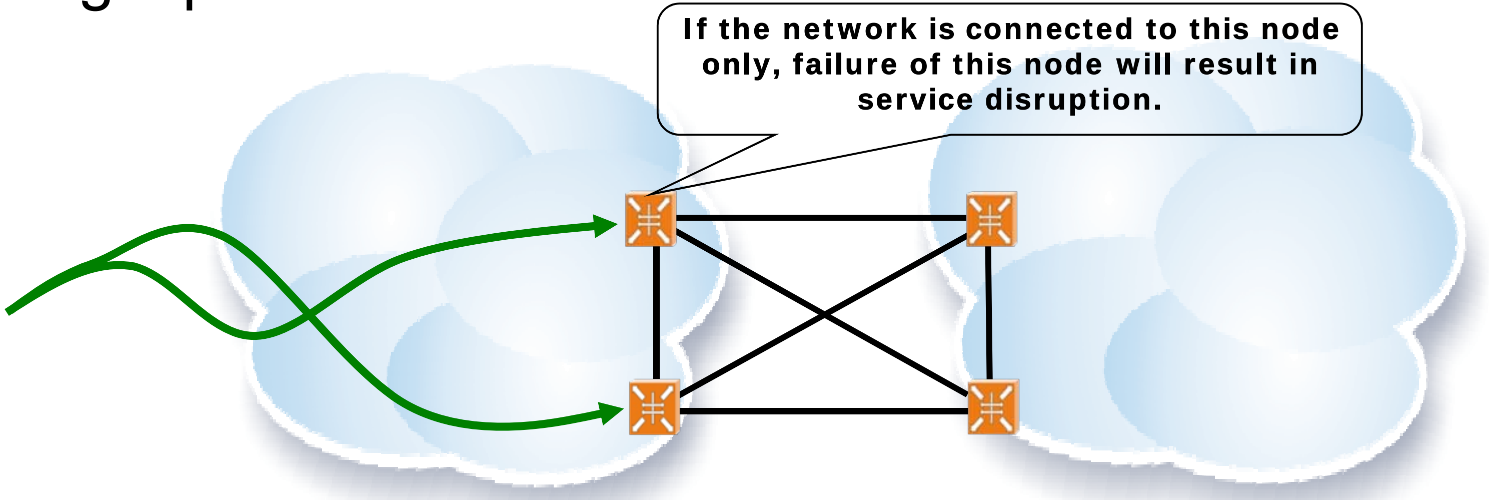
- Two node in each network are needed to protect a service. These nodes can be prioritized by configuration. The highest available priority node will be chosen to convey traffic.
- Additional nodes can be added.
- A protocol for selecting the node to convey traffic is needed.
  - To enable this protocol, connectivity between the nodes is mandatory.
  - Recovery may take longer.
  - This will introduce significant complexity while its benefits are debatable.



Issue (1)

Intra-network traffic

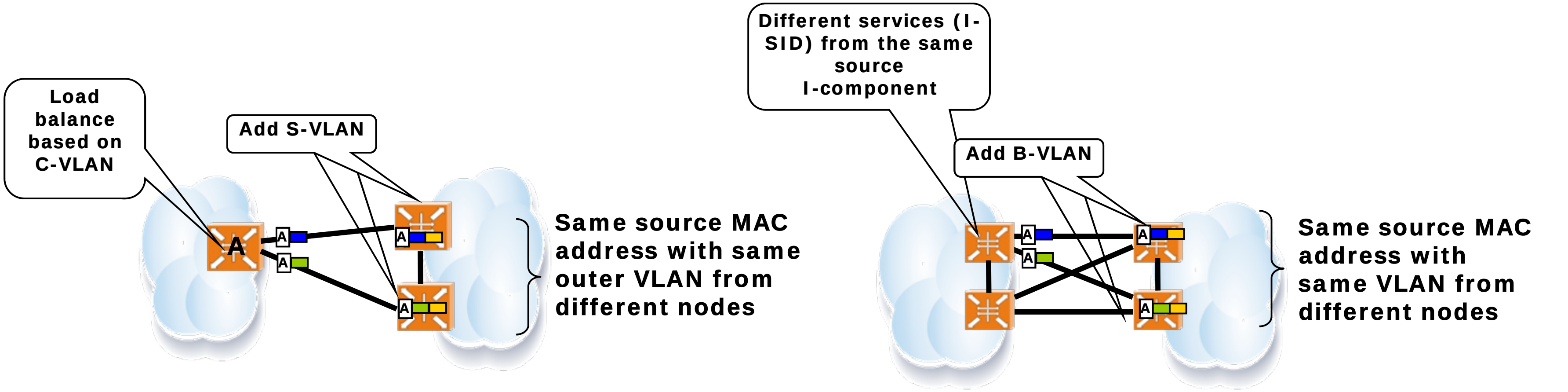
- Traffic in the network should reach both nodes to provide protection without a single point of failure.
  - This may result in the allocation of extra resources inside the network.
- Using one node as a bypass to the other node results in degradation of the protection capabilities and re-introduces a single point of failure.


If the network is connected to this node only, failure of this node will result in service disruption.

Allocating resources for protection inside the network is common

Issue (2)
MAC learning

MAC learning of frames sent from encapsulation spots. packets with the same MAC source addresses, coupled to different tag values, are encapsulated with the same external tag value and are sent from different nodes. (as described in http://www.ieee802.org/1/files/public/docs2009/new-haddock-ENNI-redundancy-1109-v1.pdf)



Load balance based on C-VLAN

Add S-VLAN

Same source MAC address with same outer VLAN from different nodes

Different services (I-SID) from the same source I-component

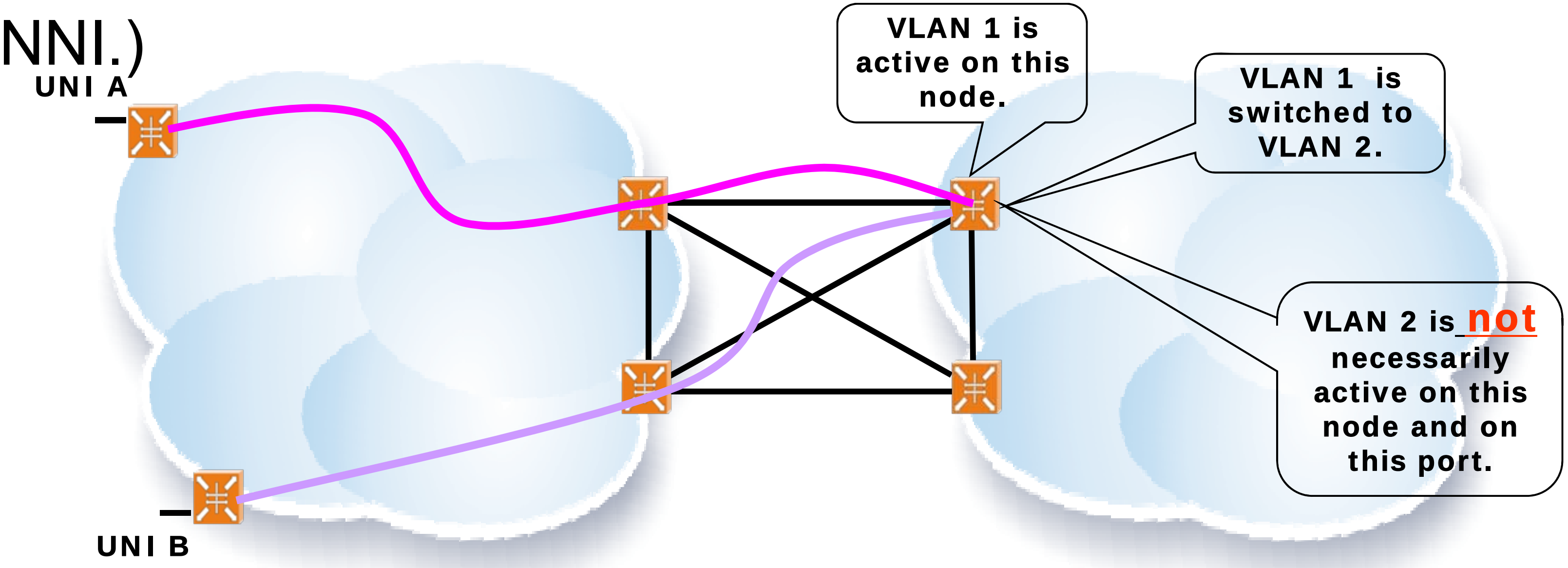
Add B-VLAN

Same source MAC address with same VLAN from different nodes

Proposed solution: Allocating VLANs to nodes is possible (splitting the S-VLAN space between the nodes), although this will double the number of consumed VLANs.

Issue (3)
Hairpin switching

Hairpin in a protected E-NNI – the VLAN of the two OVCs is active on a different E-NNI. (One VLAN, representing an OOF UNI, is attached by a hairpin to another VLAN, representing another OOF UNI, and the new VLAN is activated on the other E-NNI.)



VLAN 1 is active on this node.

VLAN 1 is switched to VLAN 2.

VLAN 2 is <u>not</u> necessarily active on this node and on this port.

Proposed solution: Ensure that the VLANs belonging to OVCs that require hairpin switching functionality are configured in the same way.