Service Protection over External Interfaces (UNIs and E-NNIs)

Zehavit Alon
Nurit Sprecher

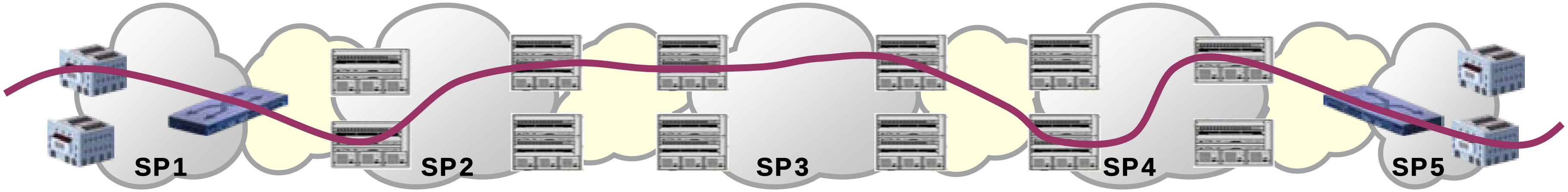
May 2010

Preface

- The concept of local service protection in the areas spanning network boundaries aroused great interest during the past year. It was a topic of discussion both in the IEEE802.1 interworking TG and in the MEF.
- The purpose of this presentation is to:
  - reiterate the basic ideas and principles of the Inter Network Service Protection (INSP) mechanism
  - encourage the group members to undertake a project on this subject in the 802.1 Interworking TG, and to start drafting a PAR

Ethernet Services over Interconnected Networks

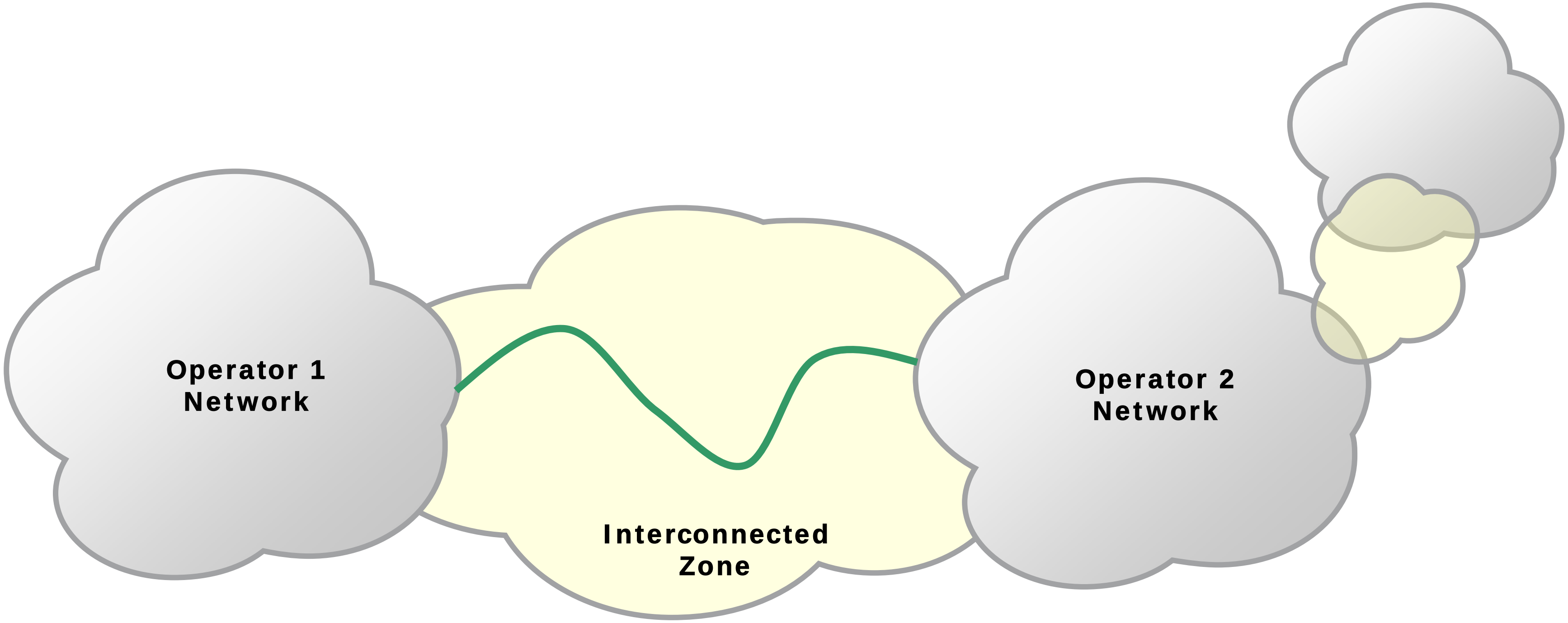
- An end-to-end carrier Ethernet service can span several interconnected packet networks.
- The current MEF definitions for NNI external interfaces (UNI and E-NNI) do not include node protection requirements (only link protection is defined using LAG).
- A new project was recently started in the MEF which aims to define the requirements for providing service protection across external interfaces. Key requirements should include both node and link failure protection.



Network-to-Network Interconnection

A method is required which will enable two networks to interconnect with no single point of failure, providing sub 50 ms protection switching.

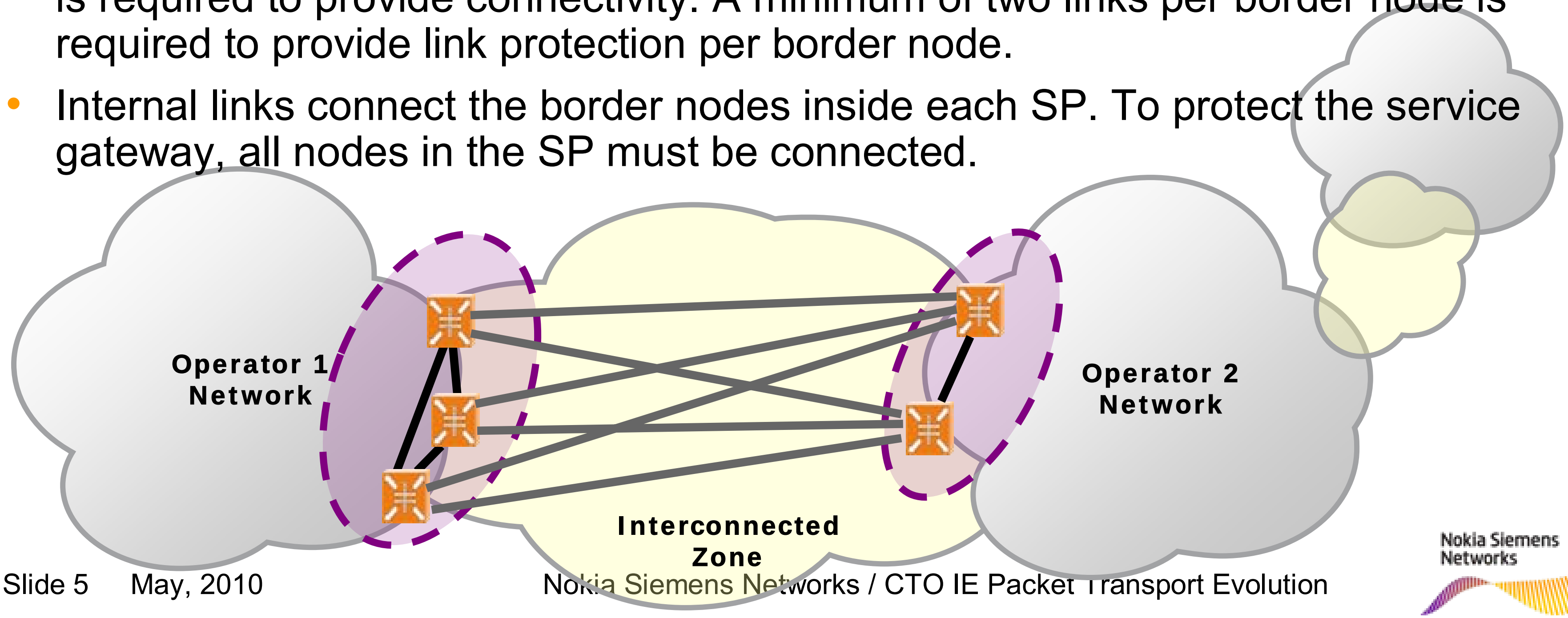
This method should provide a path in the interconnected zone (IZ) over which a service will be transmitted between the two networks.



INSP - Inter Network Service Protection

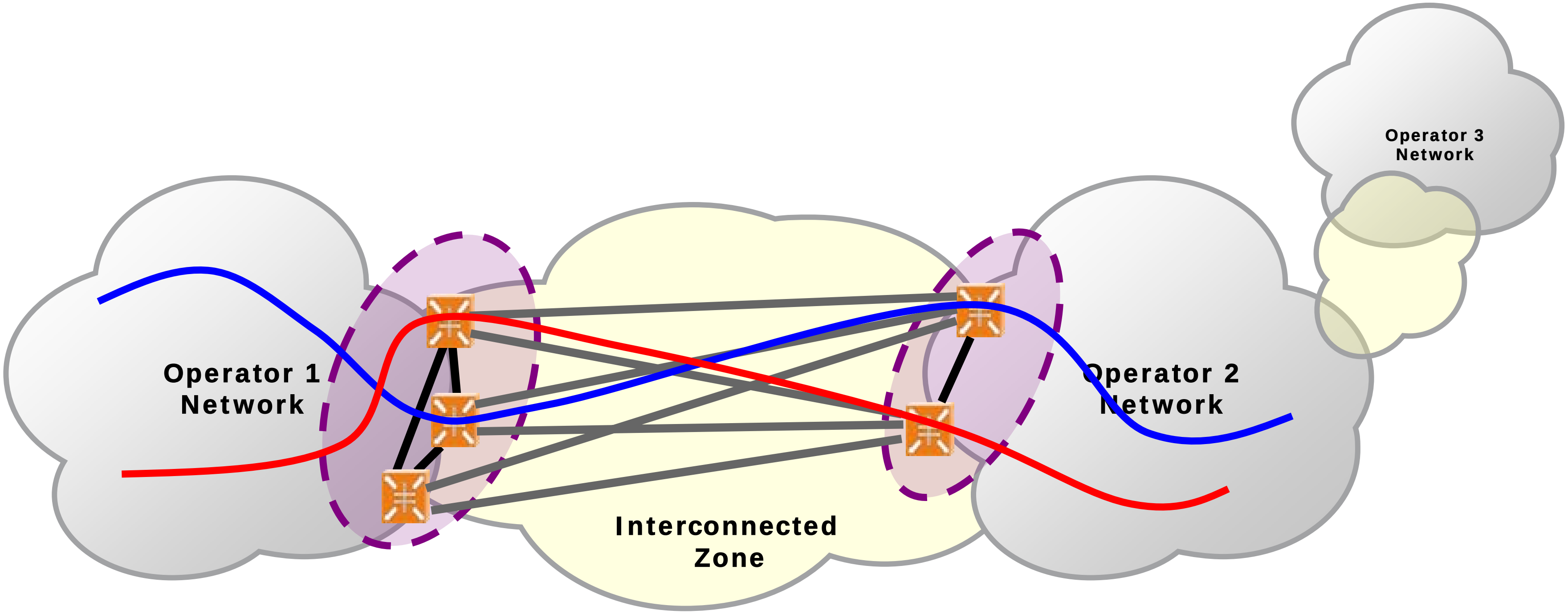
Inter Network Service Protection (INSP) is a method that provides protection capabilities for interconnected networks. It operates between *two* networks and is composed of:

- Border nodes that are responsible for conveying services. The border nodes are clustered in service portals (SP). To provide node protection in an SP, a minimum of two border nodes per SP is required.
- External links connecting the border nodes of the two SPs. A minimum of two links is required to provide connectivity. A minimum of two links per border node is required to provide link protection per border node.
- Internal links connect the border nodes inside each SP. To protect the service gateway, all nodes in the SP must be connected.



INSP (2)

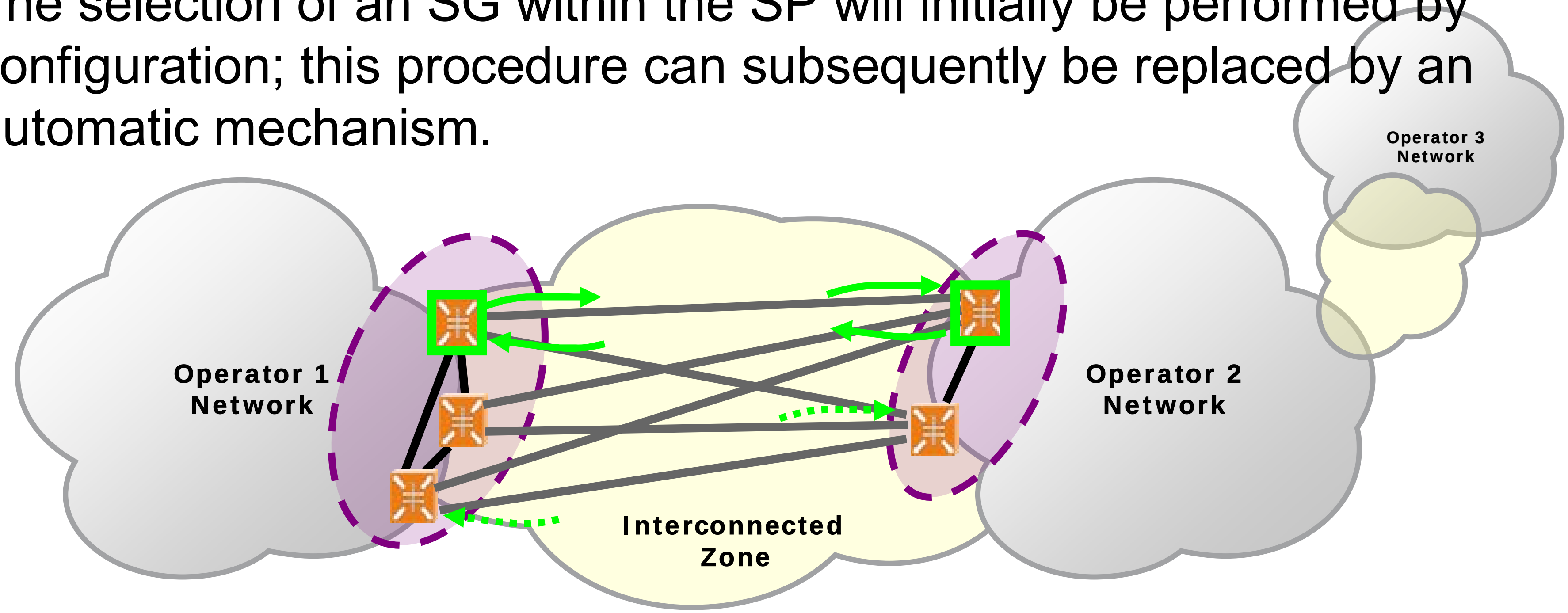
The INSP provides a safe connection between adjacent networks to guarantee service delivery from one network to the other. The INSP operates per service, i.e. per VLAN (or group of VLANs).



INSP (3)

To ensure that a service enters and leaves a network via the same border node, the SP selects a single border node as a Service Gateway (SG). This is the only border node through which the service can be conveyed from and to the IZ at any specific moment.

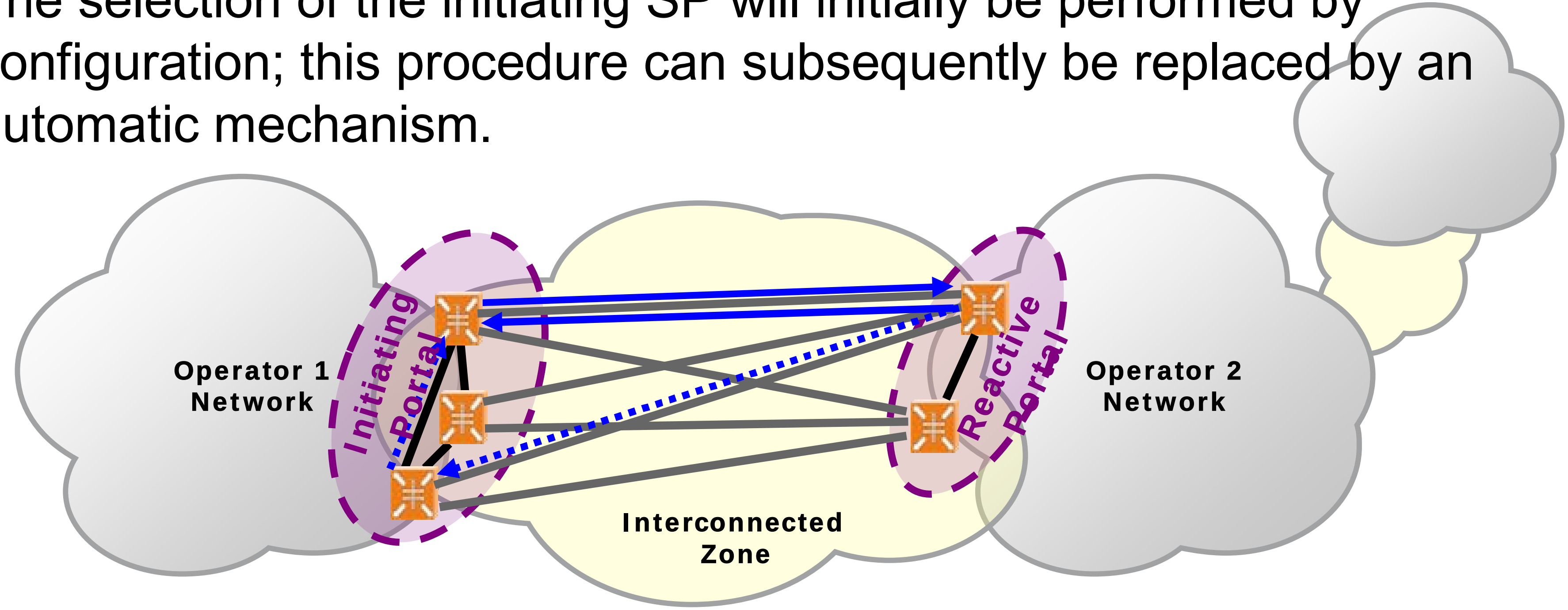
The selection of an SG within the SP will initially be performed by configuration; this procedure can subsequently be replaced by an automatic mechanism.



INSP (4)

One SP needs to initiate connectivity with the other SP to ensure that a service is co-routed in the IZ. The SP that initiates connectivity is referred to as the “initiating SP”, while the other network’s SP is referred to as the “reactive SP”.

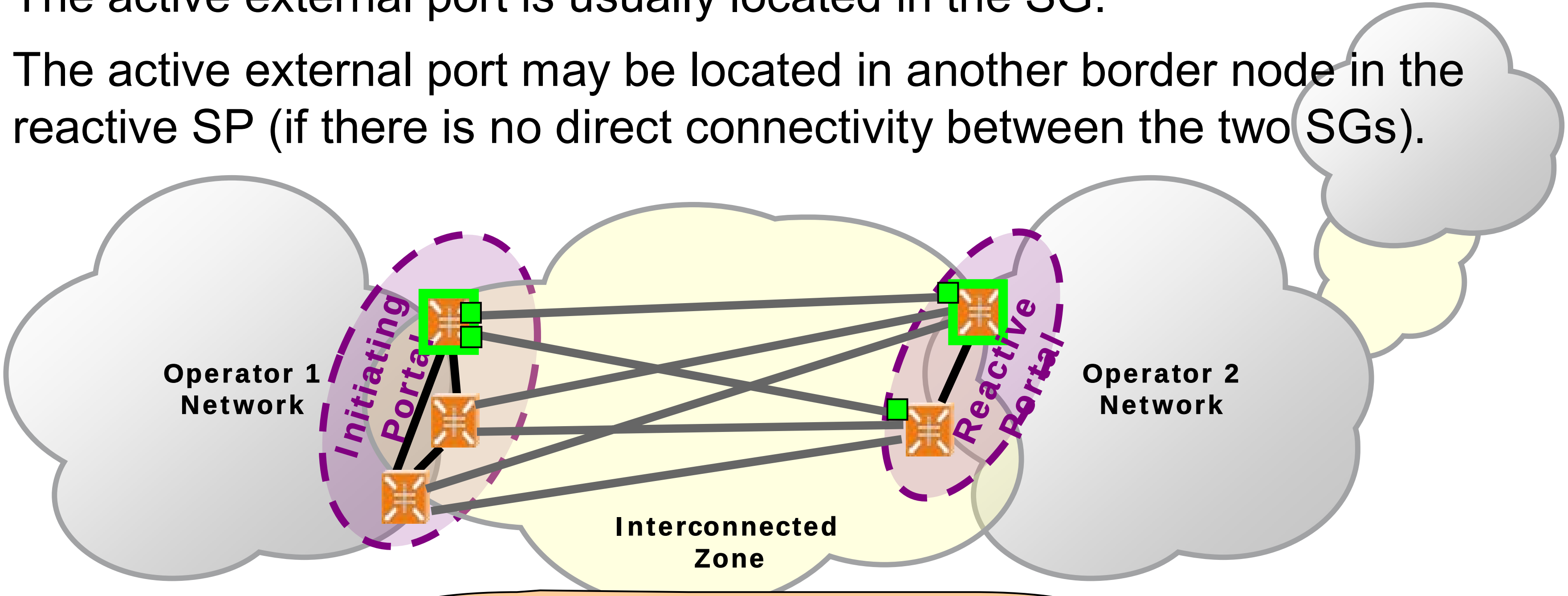
The selection of the initiating SP will initially be performed by configuration; this procedure can subsequently be replaced by an automatic mechanism.



INSP (5)

An SP possesses only one active external port. (The active external port is the port that sends and receives frames to and from the external link, i.e. the link traversing the IZ.) An external port is activated only when there is no other active external port in the SP.

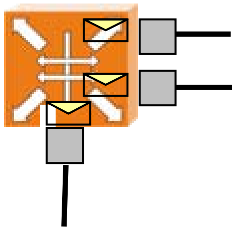
- The active external port is usually located in the SG.
- The active external port may be located in another border node in the reactive SP (if there is no direct connectivity between the two SGs).



It is guaranteed that a a frame is sent from the SP to the IZ once only (and received by the adjacent SP once only).

INSP (6)

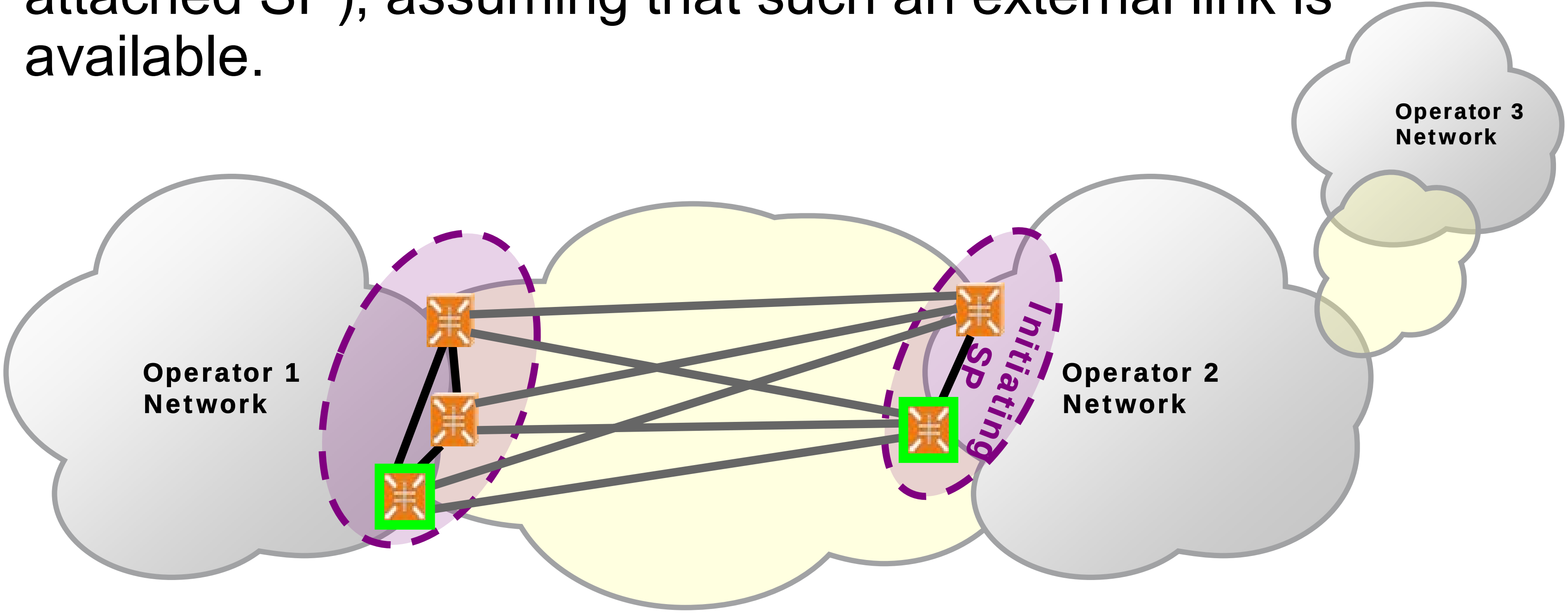
- Each border node in an SP periodically creates and sends a message via all of its internal and external ports.
- For each service, the message contains the following information:



  - whether the node is an SG for the specified service
  - whether the port conveys the traffic of the specific service (i.e. whether the port is active)
- The messages contain information, rather than commands. The information received is sufficient to trigger the next action.
- The next action may result in a change of state.
- The border node calculates the state of each service independently (and does not relate to information on other services).

INSP - Principles of Operation
SG and link selection

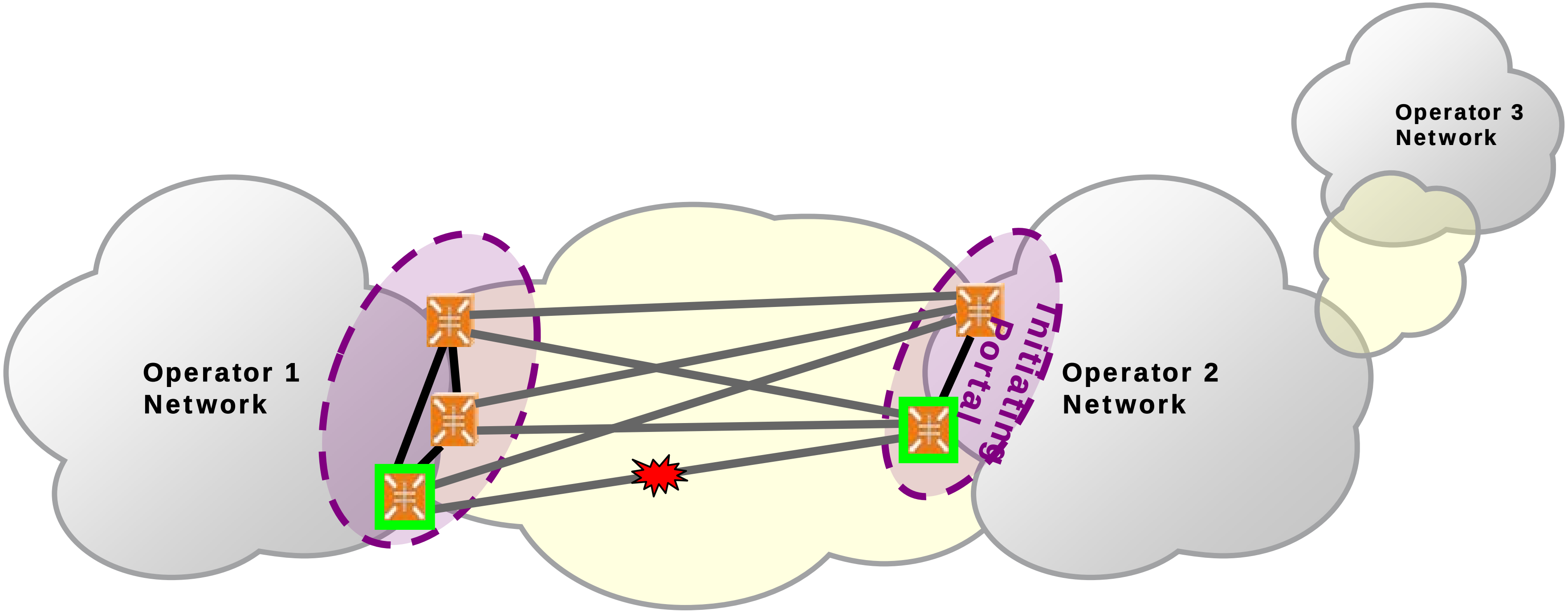
- An SG is selected on both SPs according to a predefined algorithm.
- The SG in the initiating SP (initiating SG) selects the external link which is connected to the reactive SG (the SG in the attached SP), assuming that such an external link is available.



INSP - Principles of Operation

Overcoming external link failure or deficiency

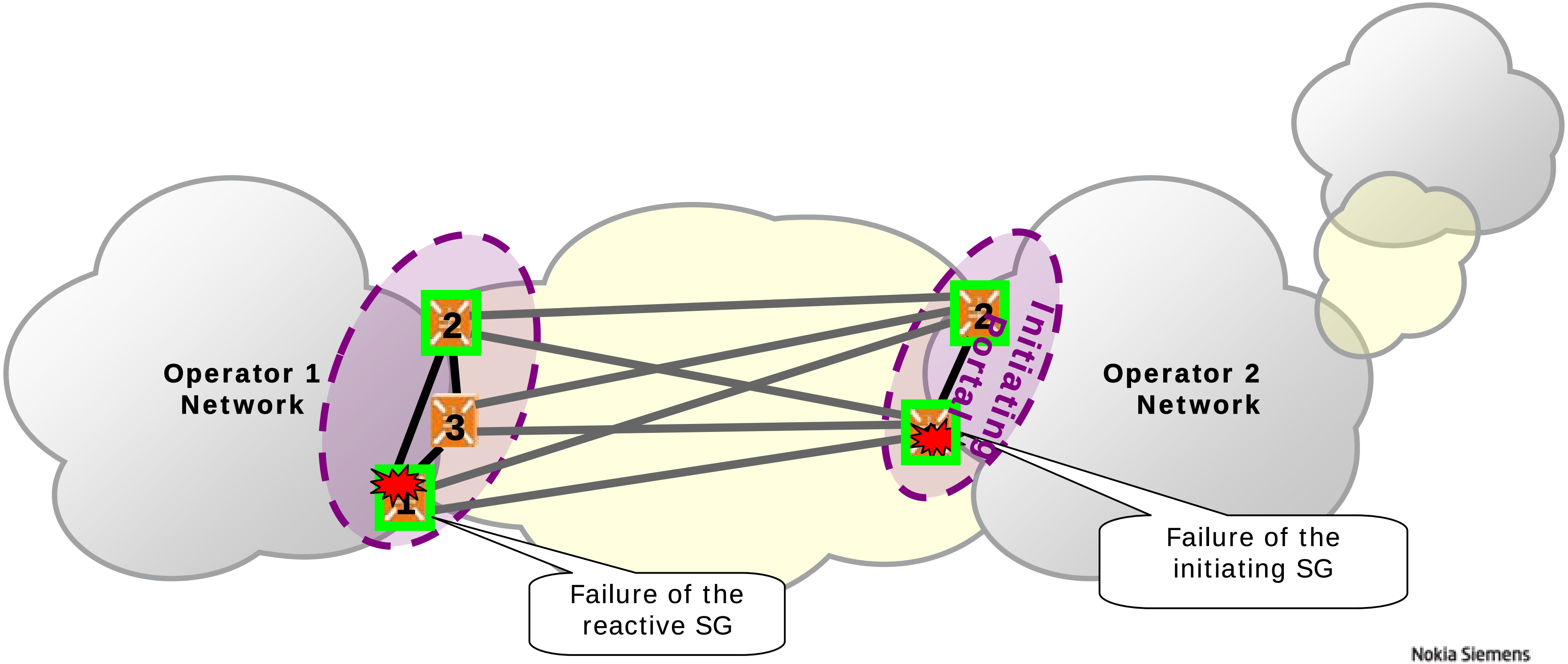
- If the initiating SG has no connectivity with the reactive SG, it selects an external link according to a predefined algorithm.
- The border node in the reactive SP, which is not an SG, redirects the received traffic to the SG in its SP.



INSP - Principles of Operation

Overcoming SG failure

When there is no SG in the SP (owing to SG failure), a new SG is elected according to a predefined algorithm. Connectivity between the SPs is established as previously defined.



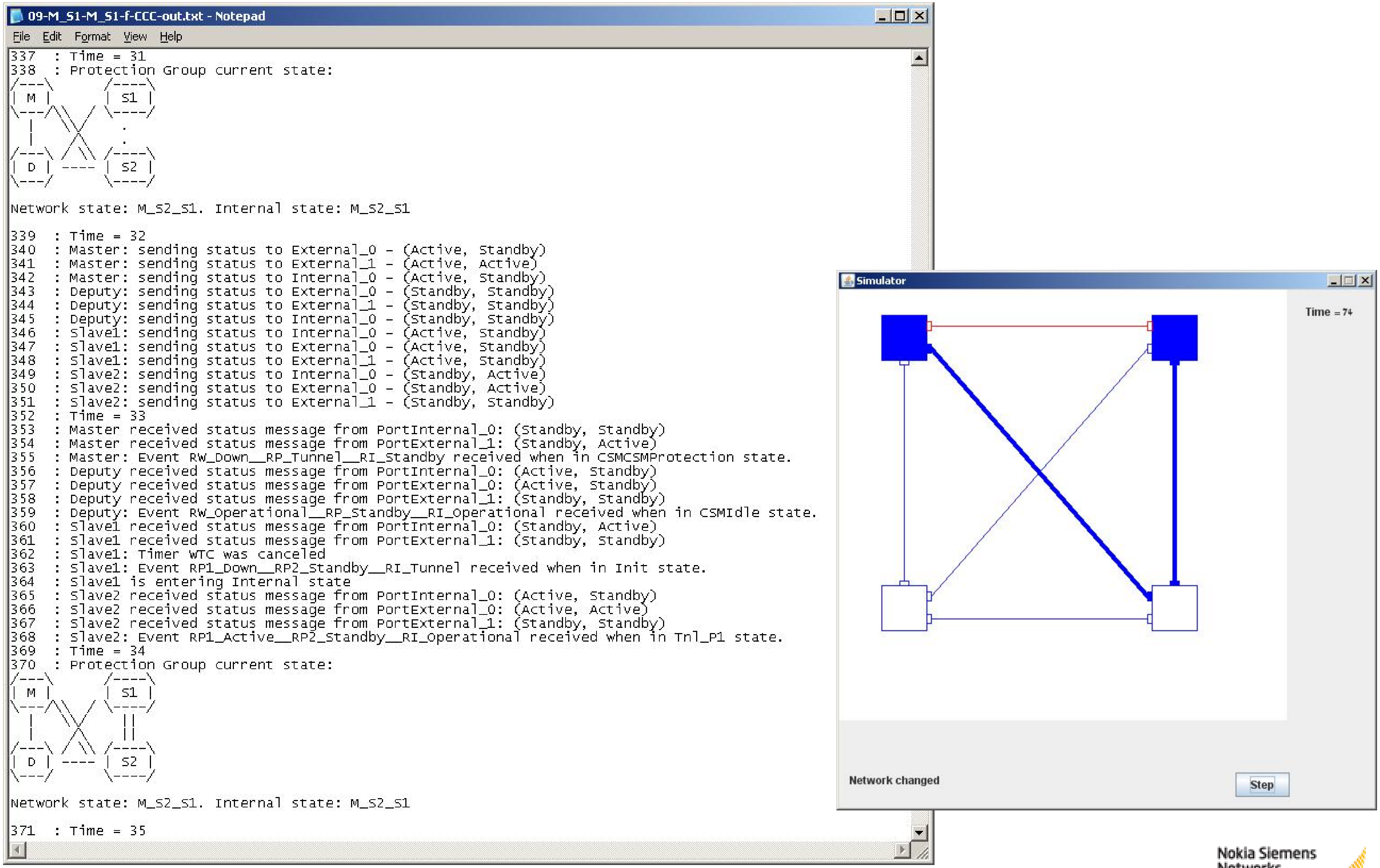
Failure of the reactive SG

Failure of the initiating SG

Proof of Concept

- A simulation was developed to prove that the concepts of the INSP are correct.
- The simulator was written in Java, and it provides a simple way to run different scenarios.
- Simulation scenarios are represented as an input XML file containing the following information:
  - configuration parameters (such as timing and delays settings)
  - scenario steps (in the form of simple commands, such as enable / disable link)
- Human-readable output is generated, displaying the messages exchanged between the nodes in the IZ as well as their status at any given time.

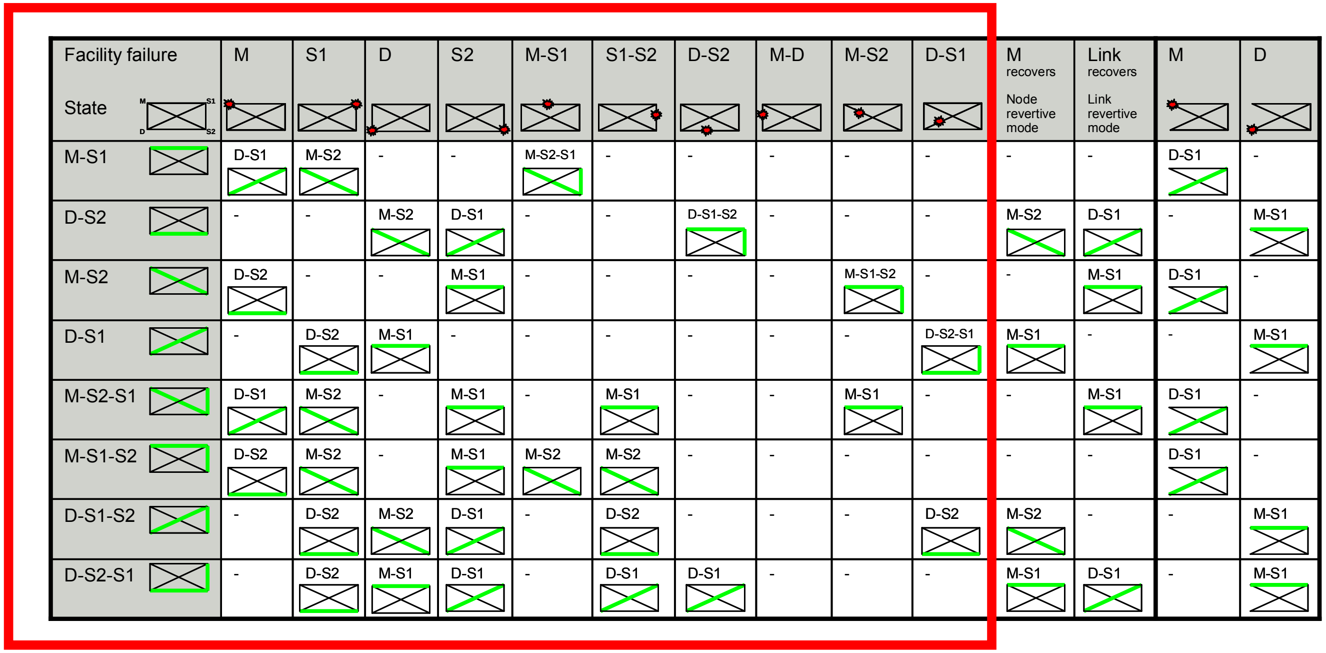
Proof of Concept (2)



```
337  : Time = 31
338  : Protection Group current state:
/---\      /----\
| M |      | S1 |
\---/\\  / \----/
  |   \\/    .
  |    /\\   .
/---\ / \\ /----\
| D | ---- | S2 |
\---/      \----/

Network state: M_S2_S1. Internal state: M_S2_S1

339  : Time = 32
340  : Master: sending status to External_0 - (Active, Standby)
341  : Master: sending status to External_1 - (Active, Active)
342  : Master: sending status to Internal_0 - (Active, Standby)
343  : Deputy: sending status to External_0 - (Standby, Standby)
344  : Deputy: sending status to External_1 - (Standby, Standby)
345  : Deputy: sending status to Internal_0 - (Standby, Standby)
346  : Slave1: sending status to Internal_0 - (Active, Standby)
347  : Slave1: sending status to External_0 - (Active, Standby)
348  : Slave1: sending status to External_1 - (Active, Standby)
349  : Slave2: sending status to Internal_0 - (Standby, Active)
350  : Slave2: sending status to External_0 - (Standby, Active)
351  : Slave2: sending status to External_1 - (Standby, Standby)
352  : Time = 33
353  : Master received status message from PortInternal_0: (Standby, Standby)
354  : Master received status message from PortExternal_1: (Standby, Active)
355  : Master: Event RW_Down__RP_Tunnel__RI_Standby received when in CSMCSMProtection state.
356  : Deputy received status message from PortInternal_0: (Active, Standby)
357  : Deputy received status message from PortExternal_0: (Active, Standby)
358  : Deputy received status message from PortExternal_1: (Standby, Standby)
359  : Deputy: Event RW_Operational__RP_Standby__RI_Operational received when in CSMIdle state.
360  : Slave1 received status message from PortInternal_0: (Standby, Active)
361  : Slave1 received status message from PortExternal_1: (Standby, Standby)
362  : Slave1: Timer WTC was canceled
363  : Slave1: Event RP1_Down__RP2_Standby__RI_Tunnel received when in Init state.
364  : Slave1 is entering Internal state
365  : Slave2 received status message from PortInternal_0: (Active, Standby)
366  : Slave2 received status message from PortExternal_0: (Active, Active)
367  : Slave2 received status message from PortExternal_1: (Standby, Standby)
368  : Slave2: Event RP1_Active__RP2_Standby__RI_Operational received when in Tnl_P1 state.
369  : Time = 34
370  : Protection Group current state:
/---\      /----\
| M |      | S1 |
\---/\\  / \----/
  |   \\/    ||
  |    /\\   ||
/---\ / \\ /----\
| D | ---- | S2 |
\---/      \----/

Network state: M_S2_S1. Internal state: M_S2_S1

371  : Time = 35
```

Proof of Concept (3)

- All single-failure, non-revertive scenarios were verified by the simulation.



Facility failure	M	S1	D	S2	M-S1	S1-S2	D-S2	M-D	M-S2	D-S1	M recovers Node revertive mode	Link recovers Link revertive mode	M	D
State														
M-S1	D-S1	M-S2	-	-	M-S2-S1	-	-	-	-	-	-	-	D-S1	-
D-S2	-	-	M-S2	D-S1	-	-	D-S1-S2	-	-	-	M-S2	D-S1	-	M-S1
M-S2	D-S2	-	-	M-S1	-	-	-	-	M-S1-S2	-	-	M-S1	D-S1	-
D-S1	-	D-S2	M-S1	-	-	-	-	-	-	D-S2-S1	M-S1	-	-	M-S1
M-S2-S1	D-S1	M-S2	-	M-S1	-	M-S1	-	-	M-S1	-	-	M-S1	D-S1	-
M-S1-S2	D-S2	M-S2	-	M-S1	M-S2	M-S2	-	-	-	-	-	-	D-S1	-
D-S1-S2	-	D-S2	M-S2	D-S1	-	D-S2	-	-	-	D-S2	M-S2	-	-	M-S1
D-S2-S1	-	D-S2	M-S1	D-S1	-	D-S1	D-S1	-	-	-	M-S1	D-S1	-	M-S1

- Work is in progress on additional scenarios, including different link delays, and additional nodes and links.

Recommendations

- Launch a new project in the IEEE 802.1 aimed at defining a protection mechanism for Ethernet services over external interfaces.
- Suggestions:
  - Begin with the real-time protocol running in the IZ which will enable the protection switching functionality
  - Continue with:
    - Inter-service-portal protocol for initiating SP selection
    - Intra-portal protocol for SG selection
    - Intra-node protocol for link selection (i.e. active external port selection)

Thank You

zehavit.alon@nsn.com

nurit.sprecher@nsn.com