Cooperative Protection Management for Guaranteed User-driven VC (Connection) Services on NSI Extension

H. Lim, A. Barczyk and C. Guok

KISTI/Caltech, Caltech and ESnet

NSI conference call

Feb 12, 2014

Introduction

Why Cooperative Protection Management on NSI Extension ?

Why Cooperative Protection Management on NSI Extension (1)

- Fault management of network virtualization environments is crucial for guaranteeing seamless virtual network services, irrespective of physical infrastructure impairments.
- In user-driven VC connection services, a link or node fault in one domain results in end-to-end data plane VC failures within a multi-domain setup.
- Disjoint backup VCs should be reserved and provisioned in advance to support a protection scheme in a user-driven manner for fault management.
- Among the cooperative protection management issues, investigating how network and protection event information, as well as transport path coordination information, is captured, managed, and disseminated across the domains of interest is a crucial key challenge in multiple production networks.

Why Cooperative Protection Management on NSI Extension (2)

- Exchanging a fault trigger between control planes in multiple production networks to switch failover is non-trivial.
- Monitoring of primary/backup VC transitions within a global network, is essential for data plane VC state/topology management required for a user-driven protection method.
- Simple extensions to NSI messages can help cooperative protection management (per-domain and end-to-end protection management) in multiple production networks.
- The exchange of protection management information between NSAs for successive VCs is essential for monitoring global network and VC status change, and coordinating transport paths across domains of interests.

Issues and Challenges for Cooperative Protection Management on NSI Extension

Network Issues

➢Protection Capabilities

- To allow user driven protection by an NSA, network devices must support protection switching capabilities (e.g., MPLS, SONET, etc).
- For per domain protection service, any independent protection scheme (e.g., 1:1, 1:N, M:N, and 1+1 protection) can be supported within the domain.
- However, to allow an end-to-end protection service, all domains must support an interoperable and consistent protection switching scheme.
- In the case of 1:1 protection, a backup path on a disjoint physical path can be used to protect the primary path, in an “active/standby” configuration.

➢Detection of Network Fault/Repair Events

- Fault signals from network devices need to be sent to an NSA in each domain in order to report a link or node fault.
- Use of SNMP for the detection of a link or node fault.
- For detection of a node repair event, use of periodic polling messages.

NSA Issues and Challenges (1)

- **Protection Service Request**
  - The selection of protection options by the user (e.g., per-domain protection or complete end-to-end protection, etc.).
  - For per-domain protection, domain specific protection by a user-driven NSA can be enabled on a user VC protection request.
- **VC Reservation and Provisioning for Protection**
  - Corresponding requests (e.g., a reserve, provision, release, terminate, and modify request) for each primary/backup VC independently.
- **Path Computation**
  - Search of path-disjoint VCs in each domain for per-domain protection and also end-to-end protection.
  - For per-domain protection, an NSA needs to find path-disjoint VCs in its domain only.
  - For end-to-end protection, a path computation engine to find path-disjoint diverse VCs, using a global network topology view.
  - Existing algorithms for disjoint-path computation.
- **Network Topology Exchange Service**
  - A standard topology exchange API service in current NSI for path computation.
- **VC Switching Control**
  - Explicit control over both primary and backup VCs.
  - When primary VCs have failures due to a network fault, an NSA should be able to control and manage backup VCs implicitly via user requests.

NSA Issues and Challenges (2)

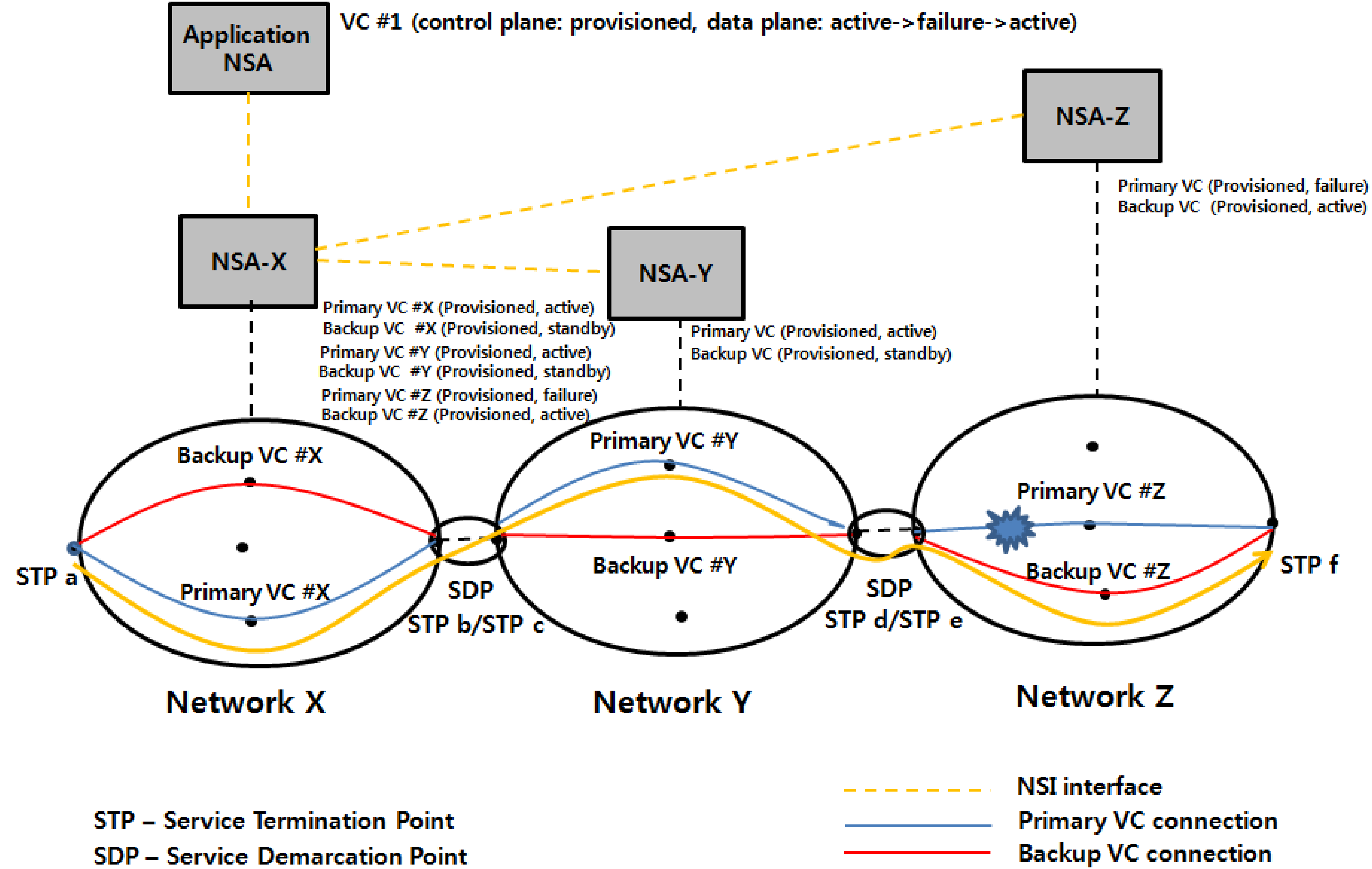
- **VC Reservation Table Management**
  - Management of the data plane status of the primary/backup VCs.
  - It can be provided by management information for cooperative protection across domains of interest.
  - Data plane VC status management enables a user to control each VC tentatively via user VC service requests.
  - Standby state on NSI extension.
- **Multi-Layer Protection**
  - The use of lower network layer VCs leads to cheaper operational cost.
  - Multi-layer VCs make multi-layer protection difficult, as it should be determined which layer of protection offers the best cost/benefit tradeoff.
  - Path computation algorithms for considering multi-layers.
- **Exchange of Management Information between NSAs**
  - The exchange of fault/repair, and VC protection/retrieval information, and the coordination information of transport paths between NSAs are essential to support cooperative protection management.
  - An *errorEvent* message defined in current NSI.
    - ✓ It can not support transport path coordination required for end-to-end protection between NSAs.
    - ✓ Also an aggregator NSA cannot capture global network and VC state change, due to a network repair and VC protection/retrieval success in component domains, with it only.

NSA Issues and Challenges (3)

- A management API message strategy on NSI extension is essentially required to solve the key challenge.
- Using the message strategy, flow mechanisms for the exchange of protection management information are investigated based on the NSI framework later.
- **Required management API messages on NSI extension**
  - ✓ An *InterfaceDown* message to notify an NSA of a faulty link on a network device and an *InterfaceUp* message to notify an NSA of a repaired link on a network device.
  - ✓ A *NodeDown* message to notify an NSA of a faulty network device and a *NodeUp* message to notify an NSA of a repaired network device.
  - ✓ A *ProtectionSuccess* message to notify that backup VCs pre-assigned in backup links or nodes are currently operating in the active state and a *ProtectionFail* message to notify that at least one backup VC is not operating in the active state.
  - ✓ A *RetrievalSuccess* message to notify that all VCs in a repaired primary link or node have been restored in the active state, and a *RetrievalFail* message to notify that at least one VC has not currently been restored in the active state.
  - ✓ A *ProtectionSwitchingRequest* message to request an NSA to switch the VCs transport path from the primary to the backup path and a *RetrievalSwitchingRequest* message to request a switch of the VCs back to the primary path.

Cooperative Protection Management Mechanisms

Per-domain Protection Management Scenario (Tree model)

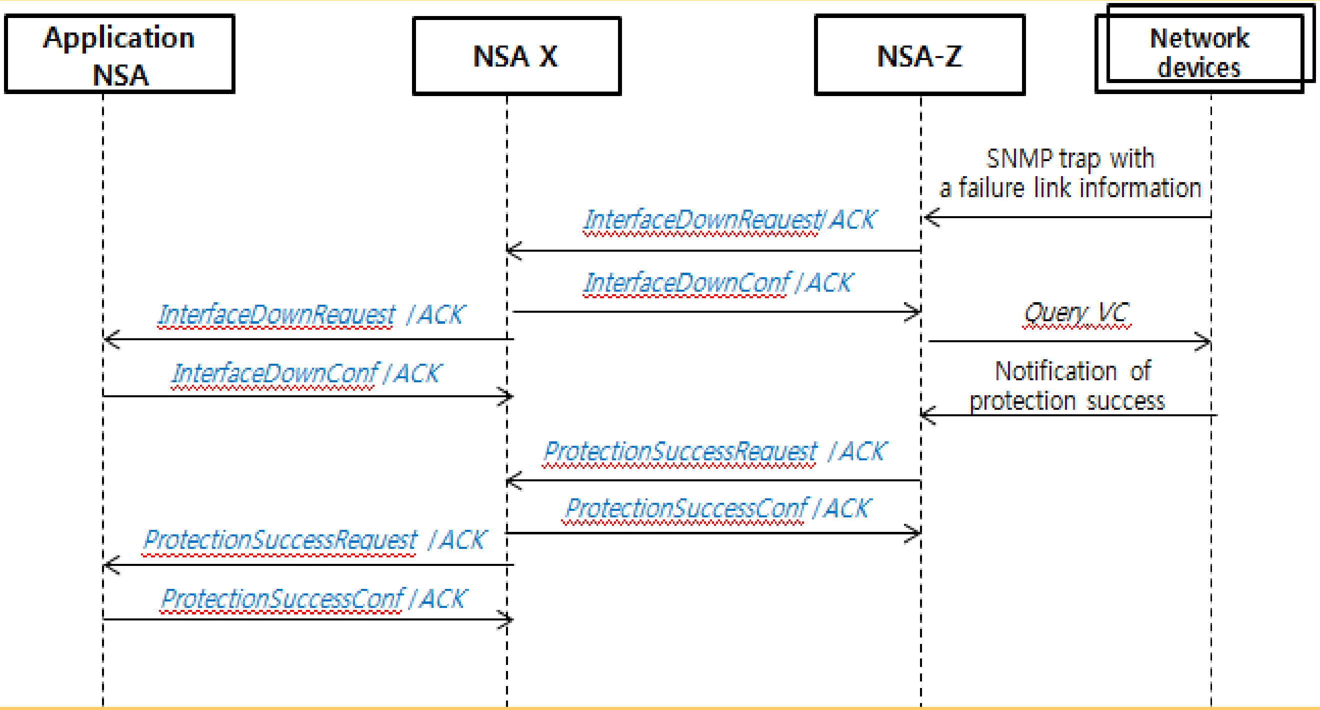


Application NSA
VC #1 (control plane: provisioned, data plane: active->failure->active)
NSA-Z
Primary VC (Provisioned, failure)
Backup VC (Provisioned, active)
NSA-X
NSA-Y
Primary VC #X (Provisioned, active)
Backup VC #X (Provisioned, standby)
Primary VC #Y (Provisioned, active)
Backup VC #Y (Provisioned, standby)
Primary VC #Z (Provisioned, failure)
Backup VC #Z (Provisioned, active)
Primary VC (Provisioned, active)
Backup VC (Provisioned, standby)
Backup VC #X
Primary VC #X
STP a
SDP
STP b/STP c
Primary VC #Y
Backup VC #Y
SDP
STP d/STP e
Primary VC #Z
Backup VC #Z
STP f
Network X
Network Y
Network Z
NSI interface
Primary VC connection
Backup VC connection
STP – Service Termination Point
SDP – Service Demarcation Point

< One per-domain protection management service scenario in the multi-domain environment (1:1 protection scheme in each domain is assumed). >

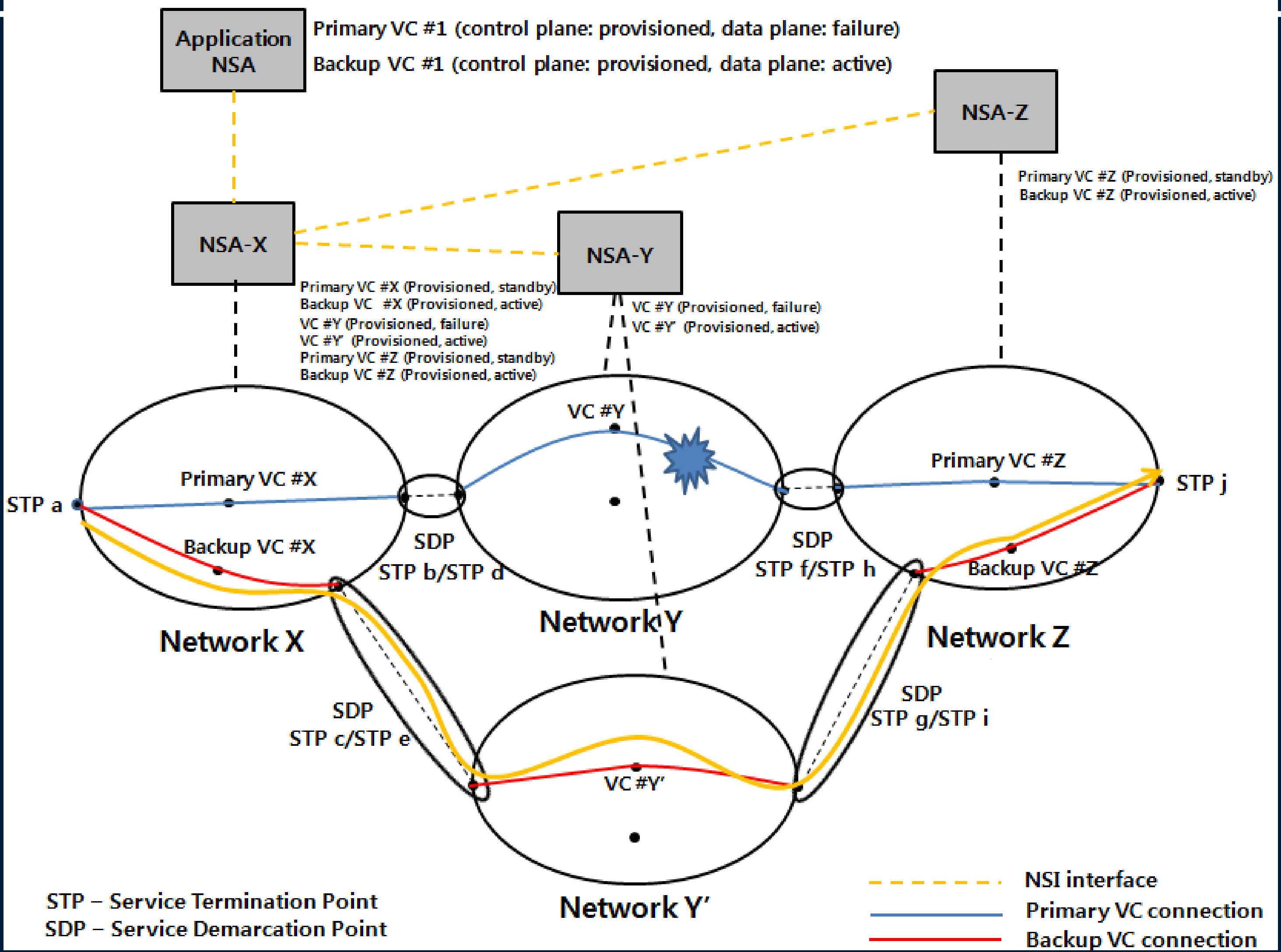
Per-domain Protection Management Mechanism (Tree model)

One API message flow mechanism for the per-domain protection management scenario


Application NSA
NSA X
NSA-Z
Network devices
SNMP trap with a failure link information
InterfaceDownRequest/ ACK
InterfaceDownConf / ACK
InterfaceDownRequest / ACK
Query VC
InterfaceDownConf / ACK
Notification of protection success
ProtectionSuccessRequest / ACK
ProtectionSuccessConf / ACK
ProtectionSuccessRequest / ACK
ProtectionSuccessConf / ACK

- Aggregator (global) NSA needs to monitor and update a global network topology change due to a fault or repair across domains of interests.
- Aggregator NSA also needs to monitor and update data plane state of primary and backup VCs due to a fault or repair.
- NSI message extension for per-domain protection management can help global network/VC monitoring and state update.

End-to-End Protection Management Scenario Considering Diversity (Tree model)



Application NSA

Primary VC #1 (control plane: provisioned, data plane: failure)

Backup VC #1 (control plane: provisioned, data plane: active)

NSA-Z

Primary VC #Z (Provisioned, standby)

Backup VC #Z (Provisioned, active)

NSA-X

NSA-Y

Primary VC #X (Provisioned, standby)

Backup VC #X (Provisioned, active)

VC #Y (Provisioned, failure)

VC #Y' (Provisioned, active)

Primary VC #Z (Provisioned, standby)

Backup VC #Z (Provisioned, active)

VC #Y (Provisioned, failure)

VC #Y' (Provisioned, active)

VC #Y

Primary VC #X

STP a

Backup VC #X

SDP

STP b/STP d

Network X

Network Y

SDP

STP f/STP h

Primary VC #Z

STP j

Backup VC #Z

Network Z

SDP

STP c/STP e

SDP

STP g/STP i

VC #Y'

Network Y'

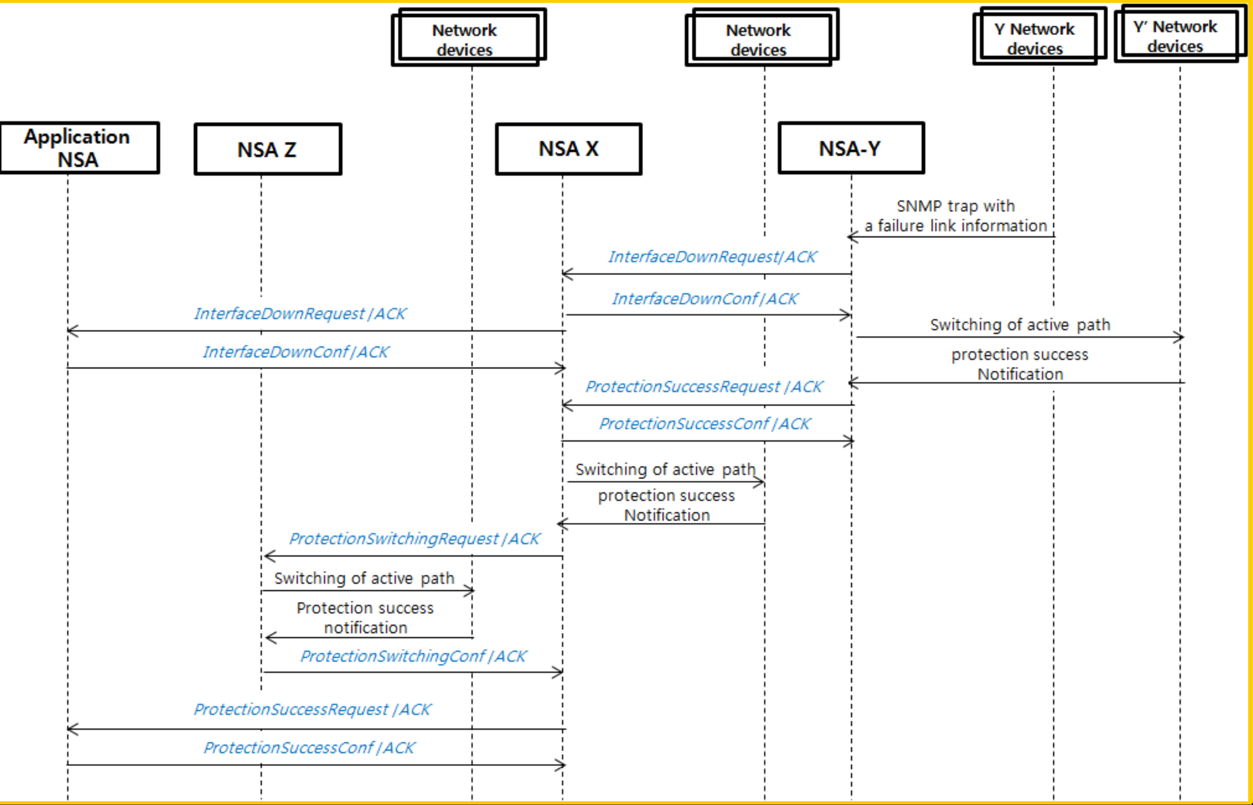
STP – Service Termination Point

SDP – Service Demarcation Point

<One end-to-end protection management service scenario in the multi-domain environment (1:1 end-to-end protection is assumed in multi-domain)>.

End-to-End Protection Management Mechanism Considering Diversity (Tree model)

One API message flow mechanism for the end-to-end protection management scenario


Network devices
Network devices
Y Network devices
Y' Network devices
Application NSA
NSA Z
NSA X
NSA-Y
SNMP trap with a failure link information
InterfaceDownRequest/ACK
InterfaceDownConf/ACK
InterfaceDownRequest /ACK
Switching of active path
InterfaceDownConf/ACK
protection success Notification
ProtectionSuccessRequest /ACK
ProtectionSuccessConf /ACK
Switching of active path
protection success Notification
ProtectionSwitchingRequest /ACK
Switching of active path
Protection success notification
ProtectionSwitchingConf /ACK
ProtectionSuccessRequest /ACK
ProtectionSuccessConf /ACK

- Aggregator (global) NSA needs to coordinate transport paths in component domains from primary to backup paths or vice versa.
- Aggregator NSA needs to monitor and update a global network topology change due to a fault or repair.
- Aggregator NSA also needs to monitor and update data plane state of primary/backup VCs due to a fault or repair.
- NSI message extension for end-to-end protection management can help transport path coordination, global network/VC monitoring and state update

Discussions

- While end-to-end protection is desirable, it is relatively difficult to set up because it requires switching of transport paths in multiple domains.
- It also leads to higher switchover times, as a fault trigger has to traverse multiple domains.
- Moreover, exchanging a fault trigger between control planes in multiple production networks is non-trivial.
- A management API message capability in component domains is a promising alternative for the communication of cooperative protection management information.
- It allows monitoring of the state of the primary/backup VCs across the end-to-end domains, as well as a global topology change.
- It also enables coordination of the VC transport path from primary to backup, or vice-versa, in one component domain.
- Using cooperative protection management mechanisms on NSI extension, it is possible to support both per-domain and end-to-end protection service.

Cooperative Protection Management on NSI Extension: Summary and Conclusions

- **Issues and Challenges**
  - ***Network issues***
    - Protection Capabilities
    - Detection of Network Fault/Repair Events
  - ***NSA issues and challenges***
    - Protection Service Request
    - VC Reservation and Provisioning for Protection
    - Path Computation and Network Topology Service
    - VC Switching Control
    - Exchange of Management Information
    - VC Reservation Table Management
    - Multi-Layer Protection
- Cooperative protection management issues and challenges must be integrated into the workflow to support data plane resiliency.
- The investigation of flow mechanisms of cooperative protection management information based on an open standard NSI framework is a key challenge for the realistic multi-domain protection scenario.
- To serve as the basis for the key challenge, cooperative protection management mechanisms using a management API message strategy extension to NSI are identified to support user-driven per-domain and end-to-end protection.

Thank you !

Questions ?

hklim@kisti.re.kr
(hklim@caltech.edu)