# Minutes for Delft meeting

Attendees

John M

Tomohiro

Chin

Roman

Hans Trompert

Radek

Freek

Takahiro Miyamoto

Jeroen

Jerry

Paul Boven

Fede

Cess de Laat

Leon Gommans

Paula Grosso

Joan

Jeonghoon Moon

Atsuko Takefusa

## John MacAuley – Modify command

* Modify limited to B/W and time
* Proposed state machine
* 2 phase commit required due to partially successful modify command cannot be rolled back.
* Modify is agreed to be useful by the team
* TK believes that 2 phase commit is needed to make modify work
* Chin would like a 1 phase Modify…
* Generally agree that if Modify uses 2 phase commit then the SM should be re-written with 2 phase commit.
* Modify should only be supported if hitless rollback is available.
* Issue: need a decision on addition of Modfiy command, following options are raised
  + Possible solution A: 1 phase commit Modify with tight constraints defined in SD?
  + Possible solution B: pseudo 2 phase commit Modify command
  + Possible solution c: full 2 phase commit – requires re-write of SM as 2-phase commit.

# Inder: NSI framework

* Framework presented
* Decision: Topology service – not part of connection service
* Decisions: Topology referenced in several places:
  + STP concepts introduced in NSI Framework
  + Use of STP for CS described in the CS protocol
  + Topology service will describe how STPs map to NML
* Decision: The details of STPs and their syntax remains in the framework
* Decision: The details of how NML is used to describe topology should not be part of NSI CS.
* Decision: Discovery service will be separate service
* Decision: Security profile belongs in NSI framework

# Inder security

* Need to understand security requirements
* 3 proposed requirements:
  + Mutual authentication between NSAs
  + Message integrity
  + Authorisation
* 2 additional requirements:
  + Message encryption
  + confidentiality
* Should service level security agreements be defined in the Service Definition?
* Mutual authentication
  + Authenticate NSA host using HTTPS for transport
  + General agreement that this is sufficient for v2.0
* Message integrity
  + Use WS security to integrity checking of message. Encryption is not necessary
* Decision summary for v2.0:
  + HTTPs for message transport for mutual auth
  + WS-Security at the message layer
  + Decide on supporting 3 token mechanisms for carrying identity information
  + SAML assertion for AuthZ, common attributes, optional pre-negotiated parameters.

## John McAuley

* How do messages get forwarded to non-peering NSAs?
* NSAs have to build up a directed graph of ‘control plane’ topology
* Every time a new reservation request is received a new SM is spawned… lead to SM bloat.. Choice of where to do aggregation will affect the number of SMs
* Summary of decisions at Oxford:
  + No assumption of congruency of data-plane and control-plane
  + No assumption that the request must start at any particular NSA (i.e head end NSA)
  + Chaining not mandated
  + Full NSA mesh not supported (N squared problem)
* Proposal:
  + Decision: Add NSA ‘connected-to’ attribute (all NSA peerings) to NSA declaration in topology. This will allow NSAs to build a graph of connected NSAs.
  + Issue: Should we also capture NSA role: Provider, Aggregator etc. YES?

## Chin: State machine

* Decision: Need to document that MDL function handles both the in-coming and out-going messages (update diagrams to reflect this)
* Changes to Delft state machine v1
  + In uRA/Agg Prov.fl added to return back to reservation state
  + In uPA Rel.fl added to return back to scheduled
* John would like ‘releasing’ state back in the SM
* Delft v2 SM to be sent out to the list at lunch time. Agreement needed by the end of the day.
* Decision: In general SM Delft v2 has been approved

## Miyamoto-san: switching service

* A switching service was proposed.
* Proposal to instantiate a new object called a ‘switching point’ SP. This is a ‘virtual’ STP with multicast ability.
* Then normal reservations are made with one end as an STP and the other as the SP.
* General agreement that a switching service is needed, more discussion scheduled for Chigago.

## Jeroen & Freek: NSI & NML topology

* Explained NML
* Proposed mappings between NSI and NML
* Inder: How physical boundaries between providers is mapped to logical STPs - important to document clearly.
* Port groups…
* Identifiers – globally unique and persistent
* URN – syntax urn:ogf:network:<DNSname>:<date>:<opaque>.
  + urn:ogf:network is as per Freek’s RFC
  + DNSname is registered domain name
  + Date is year in case domain name is reused
* Decisions:
  + STP and network concepts remain as currently described in the Framework.
  + STP is a label which will point to an NML port and syntax will use NML port syntax
  + Topology service will be a new service and will define:
    - How to describe topology (NML topology with NSI extensions)
    - How to exchange topology
  + Topology service document will be written by Jeroen/Inder
  + Freek and Jeroen will translate the automated GOLE topology into NML to see how this works.

## Jerry Sobieski: Path object ambiguity problem and STPs

* Jerry presented 3 possible solutions to prevent ERO ambiguity existing when using the current STP topology with only bidirectional STPs without direction.
* Note that there is no ambiguity when describing unidirectional paths as unidirectional STPs must be used - this removes any the ambiguity.
* Goal is to overcome the non-deterministic ERO path designation problem that arises when using bidirectional STPs.
* Kudoh-san: the way in which we solve the routing ambiguity should be independent of the uni/bi directionality of an STP. Solution that requires unidirectional STPs is inelegant.
* John: 3 options to solve the problem:
  + Option 1: source and destination STPs MUST be of type unidirectional STP (NSA then looks up bidirectional STP and reserves bidirectional path)
  + Option 2: source and destination STPs can be bidirectional but MUST be identified as ingress or egress. And user must specify sufficient STPs in path to make it unambiguous.
* Decisions:
  + STPs can be either unidirectional or bidirectional (described using NML)

## Jerry Sobieski: End System notification

* We should allow end points to terminate on a network without and internal connection on the network
* In this case should the end system be able to apply policy to a connection request? Yes