Topology Distribution Requirements

Requirements based on core principles (Compulsory)

Requirement	**Supported?**	**Explanation**
Solution **must** allow the topology information to be shared between NSAs	Yes	Any NSA can participate in the DDS protocol to share documents, and have visibility to any documents shared by other NSA. NSA can query peers directly for their local documents, allowing for discovery of the peer NSA and its capabilities.
Solution **must** allow AG NSAs to aggregate topology	Yes	Aggregator NSA can connect as a client to a DDS server, or participate in the DDS protocol to get access to all advertised topology documents.
Solution **must** support chain based path signalling	Yes	DDS can follow control plane peering of NSI CS to propagate all documents, or allow only direct peer discovery. This allows for both source and hop-by-hop routing in chain configuration.
Solution **must** support tree based path signalling	Yes	DDS can follow control plane peering of NSI CS to propagate all documents between NSA in a tree signalling configuration.
Solution **must** support centralized path finding for source-based routing decisions	Yes	DDS support collection of all NSA documents within the network for use in source-based path finding.
Solution **must** support distributed path finding for hop-by-hop routing decisions	Yes	DDS support adjacent peer document discovery for hop-by-hop routing decisions.
Solution **must** allow the creation of a full view of network topology to perform advanced "intelligent" routing decisions	Yes	DDS support collection of all NSA documents within the network for use in source-based path finding, allowing advanced routing decision like inter-layer adaptation.

Topology distribution requirements based on discussions and slides presented at Oxford meeting (Highly desired)

Requirement	**Supported?**	**Explanation**
Topology **must** contain versioning information (e.g. Creation/modify time stamp used to determine if an older version of the topology can be replaced with a newer one)	Yes	The DDS maintains a version field within metadata allowing for newer versions of topology documents to be tracked as they are introduced into the document space.
Topology **must** be verifiable (e.g. Topology must be signed by the author before uploading to topology server. Note: Key signing infrastructure and trust relationships must be in place for this to work and only complete topologies can be signed)	Yes	Documents can be signed by originating entity if required, with the DDS providing a dedicated field within the document metadata for storing digital signature if needed. A standard such as xmldsig can be used for signing documents and providing signature representations that can be stored in the DDS document meta-data.
Topology service **should** support temporal related queries (e.g. give me anything new you have learned since <date/time>)	Yes	DDS protocol supports a query for documents created/updated after a specific date, as well as any document discovered by the DDS server since the last query operation. These are two distinct queries performing different functions.
Topology service **should** support stand-alone model: single server serving single topology	Yes	The DDS is independent from the documents stored, so a stand-alone DDS server will serve whatever is added to the document space. If the local NSA adds a single topology document then that is all what will be served.
Topology service **should** support central model: single server serving multiple topologies	Yes	The DDS is independent from the documents stored, so a stand-alone DDS server will serve whatever is added to the document space. If all documents in the network are added then that is what will be served.

Topology service **should** support distributed model: topology information can be “flooded” between topology servers	Yes	The DDS is primarily based on a flooding model.
Should support getTopology - allows a user (which can be behind a firewall) to get one or more topologies	Yes	User queries for documents stored within the DDS using filter criteria (NSA identifier, document type, document identifier). Queries are firewall safe, and the metadata model is navigable.
Should support putTopology - allows a service provider to upload its topology onto the topology server	Yes	Clients of the DDS can publish documents as required.
Should support subscribeTopology - allows a user to subscribe to receive any changes in the topology information, resulting in a “push” of the new data	Yes	DDS protocol supports both a subscription mechanism for receiving autonomous notifications of document events, as well as a query to discover document changes.
Should support unsubscribeTopology - allows a user to delete their subscription	Yes	Supports desired mechanism.

Policy, scoping, and other functionality (Not yet formalized)

Requirement	**Supported?**	**Explanation**
Support distribution of topology for purposes other than pathfinding, e.g. monitoring, measurements, and visualization	Yes	DDS is agnostic to the documents being carried and their end uses.
Support separate topology views for different user groups	Yes	Documents representing user specific views can be published within the DDS document space. These documents can also be encrypted for confidentiality if desired.
Support distribution of documents other than topology (e.d. NSA description document, SLAs, etc)	Yes	DDS is agnostic to the documents being carried and their end uses.

Support application/project/deployment specific path finding for different user groups	Yes	DDS is agnostic to the documents being carried and their end uses. These specific pathfinders can get access needed topology/policy/service definitions/NSA documents via the DDS.
Support expiration or revocation of topology	Yes	DDS document metadata has an expiry date field for each document allowing a specific lifetime to be attached to each document. Documents can be revoked/deleted from the space by updating the document with expiry date to now.
Support for applying local policy via modification of the topology/reachability information	Yes	DDS permits the distribution of documents representing specific views of topology if required. In the case of chain signaling with hop-by-hop path finding the DDS can support filtering based on requesting client (context of the querying client on /local allows the DDS server to return a specific view if required).
Supports policy-based routing enforcement	Yes	The DDS does not hinder policy-based routing enforcement. If this is intended to mean "policy-based path finding" then the DDS can distribute any policy documents/information needed to perform policy evaluation in a source-based or hop-by-hop path finding model. If this is intended to mean policy enforcement within the network, then this is a uPA issue and not related to the distribution of documents.
Support for notification and removal of misbehaving topology services	Yes	Is this a requirement? How does someone decide there is a misbehaving topology service? Whom is responsible for this decision? How do we know they are not the misbehaving service? How do we want the trigger for removal kicked off? Is this a human administration task? Has anyone thought this through to any extent?

		It is easy enough to add administration specific messages to the DDS protocol, flooding these messages to all DDS connected to the document space. The additional of a “peer block” message could easily allow for all direct peers of a misbehaving DDS to cut it off from the space.

Appendix A: NSI fundamental principles

1) NSI Architecture

a) The Network Service Interface (NSI) provides secure and reliable sessions for service-related communication between two NSAs. [Ref: OGF GFD.213, pg. 4, sec. 3.2, para. 1]

b) NSI supports the ability to add new Network Services as they emerge. [Ref: OGF GFD.213, pg. 3, sec. 2.1.1, para. 1]

c) The basic building block of the NSI architecture is Network Service Agents (NSAs) that communicate using the Network Service Interface (NSI) protocol. [Ref: OGF GFD.213, pg. 4, sec. 3.1, para. 1]

d) The NSA that initiates a service request is known as a Requester Agent (RA). The NSA that responds to an incoming request is known as the Provider Agent (PA). [Ref: OGF GFD.213, pg 6, sec. 3.6]

e) The ultimate Requester Agent (uRA) is the originator of a service request. Service requests may originate from an application, from grid middleware, or from a network provider. [Ref: OGF GFD.213, pg 6, sec. 3.6]

f) The Aggregator (AG) has more than one child NSA, and has the responsibility of aggregating the responses from each child NSA. [Ref: OGF GFD.213, pg 6, sec. 3.6]

g) The ultimate Provider Agent (uPA) services requests, the ‘ultimate’ designation indicates that this is the final Provider Agent, and has management control over resources in the transport plane. [Ref: OGF GFD.213, pg 6, sec. 3.6]

h) The Message Transport Layer (MTL) provides a message delivery mechanism, which is decoupled from the NSI layer. In NSI v2.0 only a SOAP MTL has been defined. [Ref: OGF GFD.213, pg. 5 sec. 3.3, para. 1]

2) NSI Topology

a) In the NSI Topology the Transport Plane is modelled as interconnected Networks. [Ref: OGF GFD.213, pg. 9, sec. 4.1, para. 1]

b) A Network is a grouping of Service Termination Points (STPs). [Ref: OGF GFD.213, pg. 9, sec. 4.1, para. 1]

c) Each Network topology can only be associated with a single NSA. [Ref: OGF GFD.213, pg. 9, sec. 4.2, para. 1]

d) STPs are identifiers that refer to a network resource that is capable of terminating an NSI Connection. [Ref: OGF GFD.213, pg. 9, sec. 4.1, para. 1]

e) A Network is divided into Service Domains that groups a set of STP that has a common Service Definition. [Ref: OGF GFD.213, pg. 9, sec. 4.3, para. 1]

f) A Network can include one or more Service Domains. [Ref: OGF GFD.213, pg. 9, sec. 4.3, para. 1]

g) Each STP within a Service Domain will be able to be connected to every other STP in the same service domain. [Ref: OGF GFD.213, pg. 9, sec. 4.3, para. 1]

h) Each Service Domain has an associated Service Definition that describes the service offered by the domain. [Ref: OGF GFD.213, pg. 9, sec. 4.3, para. 1]

i) Externally visible STP are used for inter-domain interconnection to peer networks or customer sites. Internal STP are used to connect the internal Service subdomain as well as to the Domain’s external STP points. [Ref: OGF GFD.213, pg. 11, sec. 4.5, para. 1-2]

j) Service Demarcation Points (SDPs) are NSI topology objects that identify a grouping of two Edge Points at the boundary between two Networks. [Ref: OGF GFD.213, pg. 10, sec. 4.5]

k) By definition, Service Domains of different Service Types cannot be directly connected due to the differing Service Definitions, however, an Adaptation can be defined that permits interconnection of STP from two different Service Domains using the concepts of encapsulation and adaptation. [Ref: OGF GFD.213, pg. 10, sec. 4.4, para. 1]

l) Adaptation STP are added to each Service Domain to anchor the transitional SDP associated with the Adaptation. [Ref: OGF GFD.213, pg. 10, sec. 4.4]

3) Service Plane, NSI Signalling and Pathfinding

a) The NSAs and NSI interface exist in a notional NSI Service Plane.

b) The NSA signalling plane topology does not need to be congruent with data plane topology. [Ref: OGF GFD.213, pg. 9, sec. 3.8, para. 3; NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 1]

c) No assumptions are made about the reachability of participating NSAs. Reachability is determined by the peering policy between providers. [Ref: OGF GFD.213, pg. 7, sec 3.7, para. 1]

d) Aggregator NSAs may be "stand-alone" and may not be associated with any uPAs or network domains (i.e. dataplane resources). [Ref: OGF GFD.213, pg 6, sec. 3.6]

e) Requests may result in arbitrary (message) tree workflows with only the leaf NSAs controlling resources (i.e. uPAs). [Ref: OGF GFD.213, pg. 7, sec. 3.7]

f) Not all NSAs will be directly interconnected with every other NSA through the signalling plane. [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 2]

g) Pair-wise peering arrangements will dictate the signalling plane topology. [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 2]

h) NSA inter-connectivity will be guided by security and administration considerations and NOT exclusively data plane considerations. [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 2]

i) Users may request a reservation from an NSA that is not directly managing resources in the data plane (i.e. AG). [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 3]

j) The NSA servicing the request may not have direct signalling plane peering with all the NSAs involved in the reservation request. [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 3]

k) Users may request reservations between endpoints that are not in their network, or the network of their NSA, which implies the user request may not originate from the NSA managing the source end of the data path. [Ref: NSI_Signaling_and_Path_Finding, pg. 2, sec. 2, para. 2, pt. 4]