GFD-I-213
NSI-WG

Guy Roberts, DANTE
Tomohiro Kudoh, AIST
Inder Monga, ESnet
Jerry Sobieski, NORDUnet
Chin Guok, ESnet
John MacAuley, SURFnet

Network Services Framework v2.0

Status of This Document
Grid Forum Document (GFD), Informational (I).
This document obsoletes GFD.173 Network Services Framework v1.0.
This document should be read in conjunction with OGF GFD.212 Network Service Interface Connection Service, v2.0.

Abstract
The Network Services Framework describes a framework to support the request and management of Network Services that use the Network Service Interface (NSI) protocol.

The NSI is a web-service based Application Programming Interface (API) that operates between a requester software agent and a provider software agent. The full suite of NSI services allows an application or network provider to request and manage network service instances. These services include the Connection Service and the Document Distribution Service.

Contents

1. Context and Overview

Over the last decade, global networks have begun delivering high-performance transport services directly to applications that require performance levels or capabilities unavailable in conventional best-effort Internet Protocol (IP) networks. The ability to create connections between a fixed set of ports worldwide, with specific, predictable, and often demanding performance characteristics, enables emerging global collaborations to establish well-defined and highly customized network environments to support the end users and their applications. This has been particularly true within the Research and Higher Education environment and the Grid community.

Historically, connections across these transport networks have been reserved and provisioned in a variety of ways. The most common approach is manual provisioning – typically performed by a network engineer. More recently, some networking communities have developed tools and protocols to automate the process of network resource allocation and to allow the user or application to participate directly in the path creation process. These new approaches to automating transport connection provisioning are the basis for the standardization effort described in this recommendation.

Automated connection-oriented transport provisioning capabilities are currently being deployed by Research and Education (R&E) providers as well as by commercial providers. These automated provisioning systems, while being developed independently by different groups, all have common elements. They have developed software-based control and/or management agents to regulate access to these resources, to schedule and reserve resources, to trigger or control timely provisioning of the network resources, and to monitor and release resources. These controllers are deployed in two different contexts. One context is application-centric (or Grid-centric), where a network provides a resource to an application or middleware. The other context is network centric, where network resources are collaboratively shared among networks to expand or improve network performance or reach. In the former context, a user or application agent is requesting the service from a network provider. In the latter context, one network is interacting with one or more other networks to manage these resources and deliver a comprehensive and well-integrated service portfolio to the user community. This informational document defines a framework for the NSI protocol to support both of these contexts.

The Network Services Framework (NSF) defines several key architectural elements: the Network Service Interface (NSI), the NSI Protocol, the Network Service Agent (NSA), the Network Services, and the Inter-Network Topology. These elements exist in a notional NSI Service Plane. The framework describes an environment within which network objects are defined as manageable resources. Within the framework, these network resources can be selected, allocated, interrogated, and manipulated by software agents on behalf of requesting users.

Federated Network Services are delivered by combining the capabilities of participating providers. To manage federated services, a range of network-related functional capabilities such as topology sharing, path finding, resource reservation, hardware provisioning, and other ancillary services and functions are required.

NSI delivers a key enabling technology in accordance with the Software Defined Networking (SDN) approach. The NSI can be used as a north-bound API that supports multi-domain network service delivery and management.

A suite of documents defines the NSI Protocol. This informational document describes the Network Services Framework version 2.0. In addition, each Network Service is defined in its own protocol recommendation.

2. NSI Services

2.1 Introduction to Network Services

Network Services allow applications to monitor, control, interrogate, and support network resources that are made available by the provider of the network. Typical transport network resources include a range of technologies such as wavelengths delivered using Reconfigurable Optical Add Drop Multiplexers (ROADMs), Time Division Multiplexing (TDM) cross-connect equipment or packet switches. The Network Service Framework is designed to support a wide range of Network Services using all of these technologies.

Service requests may originate from an application, from grid middleware, or from a network provider. A service can be requested by any application that has implemented an agent with a Network Service Interface. Similarly, any network provider who has implemented an agent with an NSI protocol interface can service the request.

Each service has an associated Service Definition (SD). This SD sets the scope of the service and identifies any parameter that is needed for the request to be fulfilled. SDs are normatively defined in the NSI CS protocol [3].

Each service is managed by an exchange of NSI Messages between agents. These messages operate using a set of service primitives. Service primitives are the set of instructions that allow the requester to set up and manage a service. Each service request will result in the allocation of a service id for the new service instance.

Network resource capabilities are made available to the consumer through a set of network services; the NSF presents a unified framework for these services. Network Services include the ability to create Connections (the Connection Service), and to disseminate information (the Document Distribution Service) such as topologies, service definitions, and NSA descriptions.

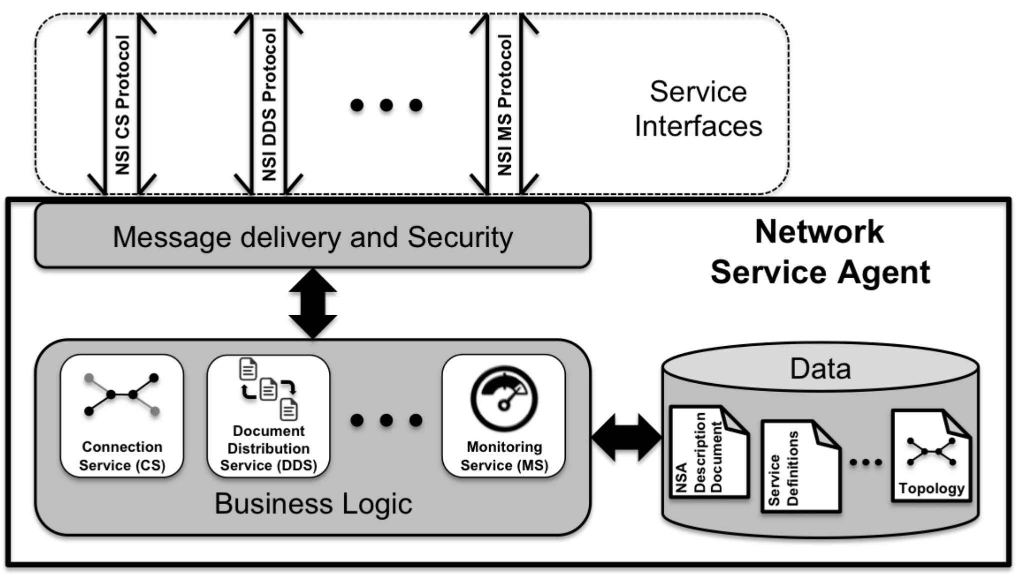

Figure 1: NSI Framework

2.1.1 NSI Extensibility

The Network Services Framework is built around an architecture that is extensible; it inherently supports the ability to add new Network Services as they emerge. Network Service Agents support services and functions in that are delivered as an integrated service within the NSF.

2.1.2 The NSI Connection Service

The NSF includes the NSI Connection Service (CS) as one of the key NSI services. The Connection Service allows a range of different types of Connection to be managed. The NSI Connection Service is normatively described in GFD.212 Network Service Interface Connection Service version 2.0 [3]

2.1.3 The NSI Document Distribution Service

The role of the NSI Document Distribution Service (DDS) is to provide an information dissemination channel to support other NSI services. In the general case, the NSAs can learn about another NSAs capabilities by retrieving their NSA Description Document. This document specifies the services provided by the NSA (e.g. CS), and relevant information about those services (e.g. location of those services, protocol versions, and supported functions (e.g. modify)).

In the case of the NSI CS, two additional documents are needed; i) the NSI Service Definitions, which provide details about the service (e.g. connections are Ethernet VLAN Private Lines, supported Maximum Transmission Units (MTUs) of 1500 and 9000 bytes, etc.), and ii) the NSI Topology, which is a standard ontology and schema to describe network resources that are managed to create the NSI service. The NSI Topology is described in: GWD-R-P: Network Service Interface Topology Representation [5]. The document describes a normative extension to the Network Markup Language (NML) base schema version 1 that includes the description of service plane objects required for the NSI CS.

3. NSI Architecture

The NSI provides an environment within which network resources are treated as explicitly manageable objects. The NSI Connection Service allows network resources to be selected, allocated, queried, and managed by using NSI messages between the Network Service Agents (NSAs).

3.1 Network Service Agents

The NSF describes a set of architectural elements that make up the NSI architecture; this provides a framework that applies to all of the NSI services. The basic building block of the NSI architecture is Network Service Agents (NSAs) that communicate using the Network Service Interface (NSI) protocol.

The NSA is a software agent that implements the NSI protocol state machines that define the message exchange. 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).

3.2 The Network Service Interface

The Network Service Interface (NSI) provides secure and reliable sessions for service-related communication between two NSAs. An instance of the NSI exists at the boundary between two NSAs, the RA and the PA (see Figure 2).

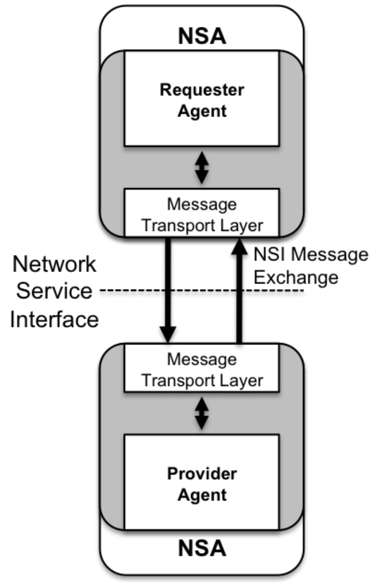

Figure 2: Network Service Interface

3.3 The Message Transport Layer

The Message Transport Layer (MTL) is the function responsible for ensuring reliable and secure delivery of messages between NSAs. The MTL also provides a message delivery mechanism, which is decoupled from the NSI layer. This independence of message from transport has been formalized to allow the transport layer to be readily changed if necessary. Multiple service-to-service sessions can be multiplexed over the common NSA-to-NSA session. Each service-to-service session can establish its own security based on the credentials offered by the requesting service.

The MTL as used by the Connection Service is specified in detail in the NSI CS protocol [3].

3.4 The Coordinator function

The Coordinator function has the role of providing intelligent message and process coordination, which includes the tracking and aggregation of messages, replies and notifications and the servicing of query requests. Each service has its own coordinator function. The NSI CS coordination function is included in the NSI CS protocol [3].

3.5 The Network Resource Manager

The Provider NSA and Aggregator NSA may include a Network Resource Manager (NRM). The NRM manages the part of the Network Service implemented over local network resources. The NRM has the ultimate authority for the local resources; this means that it can choose to accept or reject any request from the NSI for local resources. Typically the NRM might be an equipment vendor’s network management system.

Figure 3 shows an NSA with all of its sub-functions.

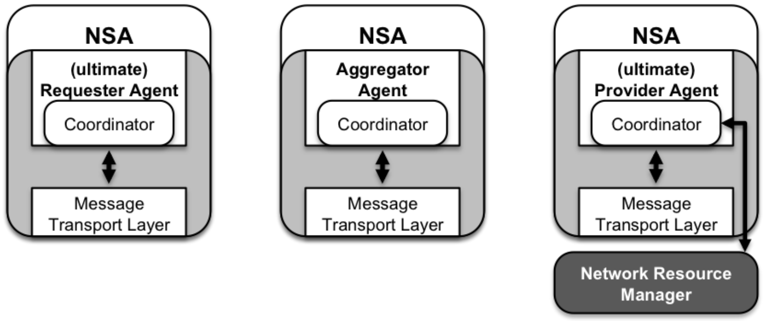

Figure 3: NSA sub-functions

3.6 NSA roles

An NSA can take on the following roles:

- uRA: The ultimate Requester Agent is the originator of a service request. Here the 'ultimate' designation indicates that this is the originating Requester Agent. This could, for example, exist in a middleware application.
- AG: The Aggregator has more than one child NSA, and has the responsibility of aggregating the responses from each child NSA.
- uPA: The ultimate Provider Agent services requests by coordinating with the local Network Resource Manager (NRM) to manage network resources. Here the 'ultimate' designation indicates that this is the final Provider Agent.

The Network Service Agent may at times act as a requester over one interface while acting as a provider at a different interface. This is the case in an Aggregator NSA that acts as a gateway to other providers; in this role the NSA can forward messages on to a child NSAs.

For a given service instance, an NSA is considered to be a parent to the NSA that it has sent a request to. Similarly an NSA that receives a request is considered to be the child of the NSA that it received the request from.

Also present in the AG are additional peripheral functions such as the path-finding function and a Topology database. These supporting functions may be used to deliver Network Services and may be locally or remotely located. A description of these functions is outside the scope of this document.

Each service type may support multiple simultaneous service instances; these instances are created in response to a service request and may be addressed by a unique service identifier. For example, a physical instance of a Connection has its own Connection Service identifier.

3.7 Flexible communication model

The Network Services Framework is intended to allow services to be delivered across many participating networks. To facilitate this, flexible NSI Message forwarding is supported. This section describes the communications models supported for NSI Message handling.

No assumptions are made about the reachability of participating NSAs. Reachability is determined by the policy of the each provider; the provider decides which NSAs it will peer with. So an NSA may be directly reachable or reachable only via a third NSA. For instance, an arbitrary set of networks may band together under NSI rules and peer exclusively via a single AG NSA. This NSA may have no transport resources of its own – just those resources under management of the child NSAs. Service requests will flow along the trusted sessions hierarchically among NSAs.

The NSI protocol supports both tree and chain models of message communication. In a chain model, messages follow the same NSA sequence as traversed by the requested Connection. This emulates a Multi Protocol Label Switching (MPLS)-like mode. In a tree model, the message is split into its constituent segments and messages are forwarded to NSAs that are able to implement each segment of the Connection. The tree model does not restrict messages to follow the NSA sequence traversed by the requested Connection, so more flexibility is provided for message routing. The tree mode supports a centralized SDN model of network architecture.

The NSI architectural elements can be flexibly combined to build the NSI hierarchy. Figure 4 below shows an example of a possible hierarchical relationship between NSI agents.

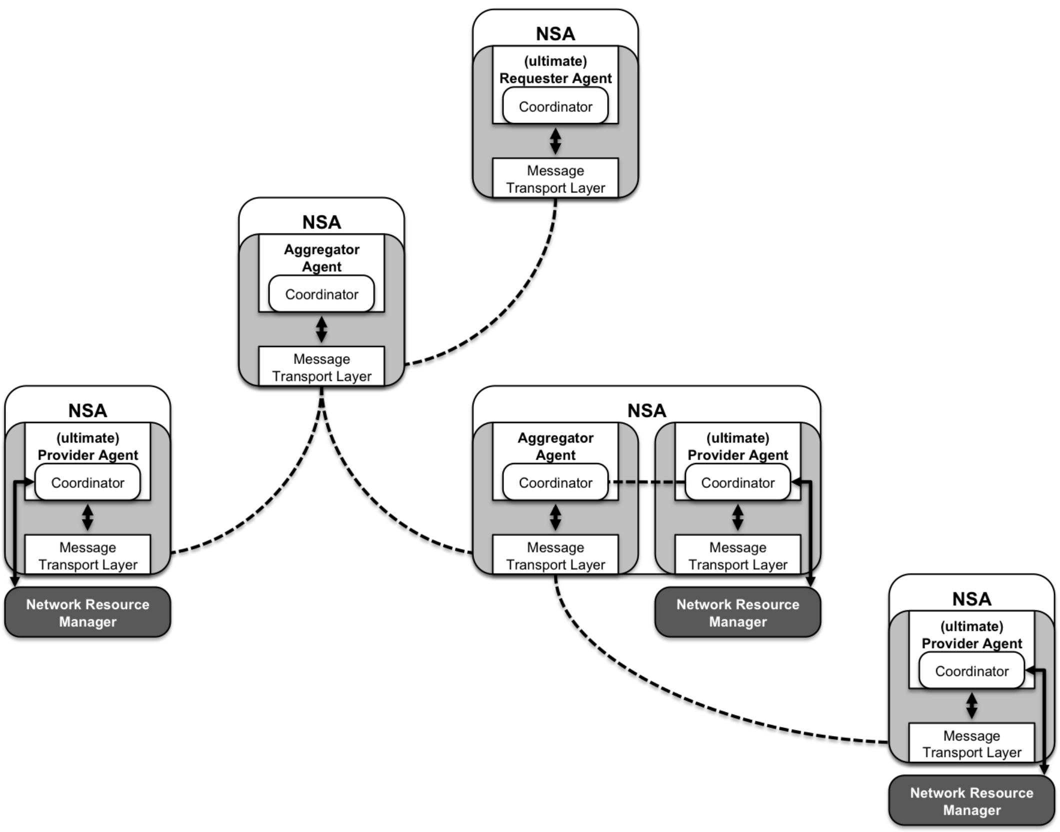

Figure 4: Flexible hierarchical NSA relationship

In general the following rules apply the composition of an NSA to support the flexible hierarchical model of communication:

First NSA in a message sequence:

- If the request originates from the middleware (no local network resources): The first NSA in the sequence is a uRA (e.g. residing in middleware).

- Request originates from a network provider (local network resources are present that are part of the Connection): The first NSA in a sequence includes an Aggregator and a uPA.

Intermediate NSAs in a message sequence:
- All intermediate NSAs in a sequence include an aggregator.
- All intermediate NSAs in a sequence include a uPA if resources associated with the Network are to be requested.

Final NSA in a message sequence:
- The last NSA in a sequence includes a uPA.
- The last NSA in a sequence may include an aggregator, though this may not be used in the resource reservation process.

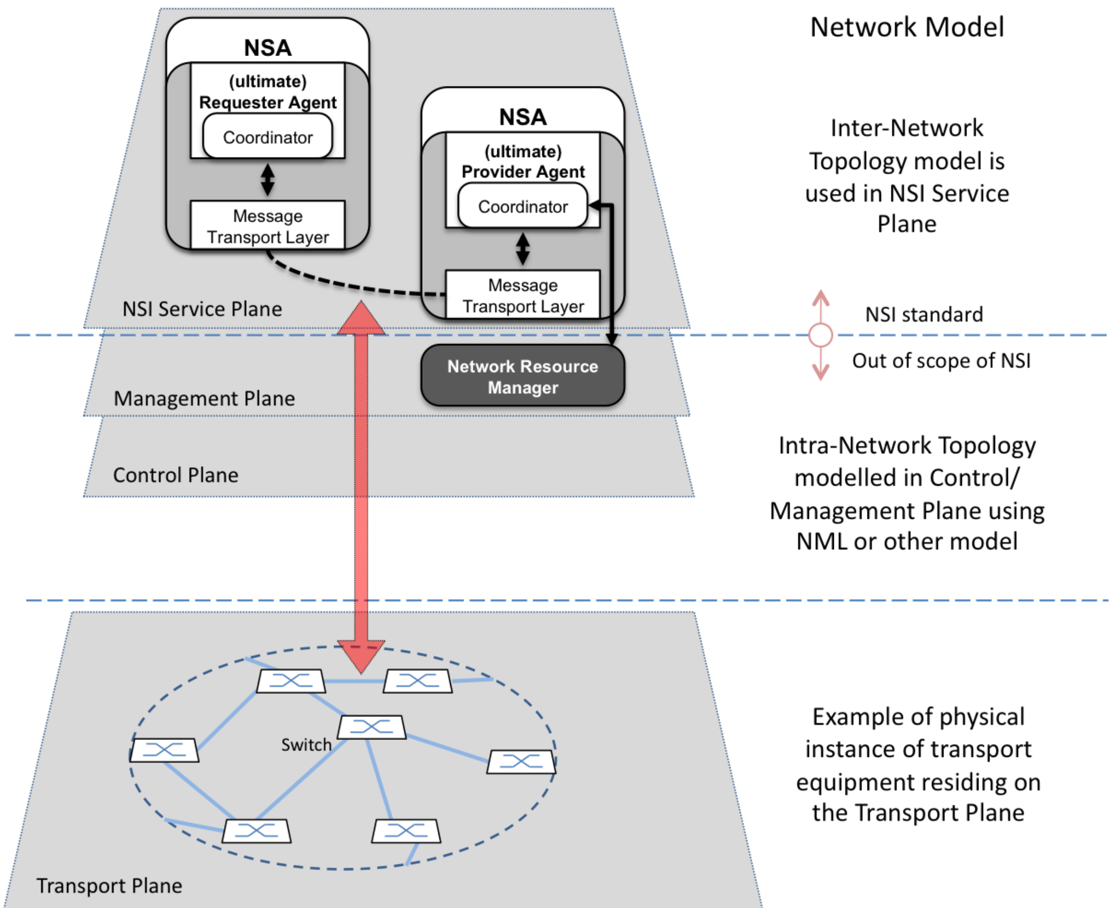

Figure 5: Transport Plane and NSI Service Plane

3.8 NSI layering model

The Network Service Framework assigns the NSI to a notional NSI Service Plane. Here we define the Service Plane as including participating NSAs and the associated NSI sessions between these NSAs. The transport equipment (switches, X-connects, etc.) resides in the Transport Plane. Each Network in the Transport Plane has an associated NSA in the Service Plane. The NSI Service Plane relationship to other planes is depicted in Figure 5.

In general, the NSI Service Plane relies on the capabilities of the Control Plane and/or Management Plane to effect changes in the Transport Plane, where the Control and Management

Planes follow conventional definitions. The transport resources and the physical instance of the Connection reside on the Transport Plane.

The topology of the transport equipment is described on the NSI Service Plane using the NSI Topology; this model is introduced in Section 4.

Central to the NSI architecture is the decoupling of the Service Plane from the Transport Plane. NSI messages do not need to transit the NSA/Networks pairings in the same sequence that the Connection itself transits the Transport Plane.

4. Representing Network Resources

4.1 STPs

In the NSI Topology the Transport Plane is modeled as interconnected Networks, were a Network is a grouping of Service Termination Points (STPs). STPs are identifiers that refer to a network resource that is capable of terminating an NSI Connection. STPs are typically identifiers of physical network ports (e.g.Gigabit Ethernet) or virtual network ports (e.g.Ethernet Virtual Local Area Networks (VLANs). The normative definition of the NSI Topology representation can be found in GWD-R-P: Network Service Interface Topology Representation [5].

4.2 NSI Networks

In the NSI Topology a Network is a grouping of STPs associated with a single NSA. An NSA can have multiple Networks, but each Network can have only one NSA.

4.3 Service Domains and Service Definitions

A Network is divided into Service Domains. A Service Domain groups a set of STP that has a common Service Definition. A Network can include one or more Service Domains. Each STP within a Service Domain will be able to be connected to every other STP in the same service domain. Each Service Domain has an associated Service Definition that describes the service offered by the domain. A common Service Definition can be defined for more than one Service Domain, however, each of these Service Domains will offer the described service.

Service Domains can be nested to model internal structure. Externally visible STP are used for inter-domain interconnection to peer networks. Internal STP are used to connect the internal Service subdomain as well as to the Domain's external STP points.

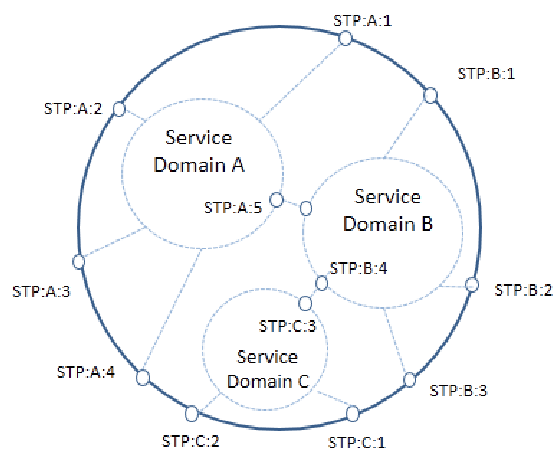

Figure 6: Service Domains

4.4 Adaptations

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.

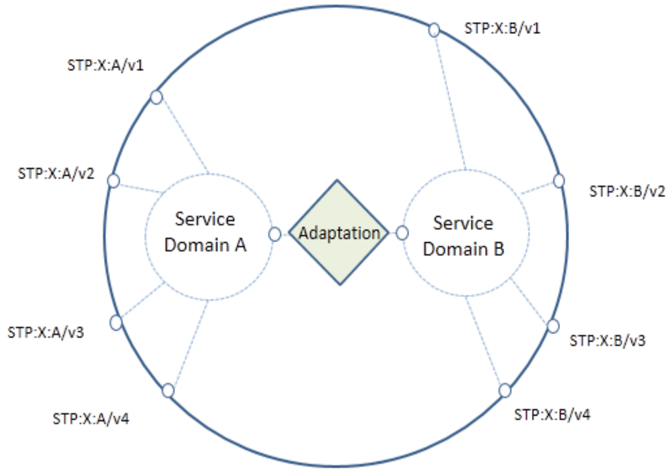

Figure 7: Service Adaptations

An Adaptation defines the (de) encapsulation or (de) adaptation of one service type into another service type if the Network is capable of offering the service. Furthermore, an Adaptation has directionality i.e. adaptation and de-adaptation. Both unidirectional and bidirectional Adaptations are supported, with bidirectional Adaptations containing a symmetrical pair of adaptation and de-adaptation functions.

Adaptation STP are added to each Service Domain to anchor the transitional SDP associated with the Adaptation. This transitional SDP is not used in connections, and is only present to enable path finding between the domains. These Adaptations are defined with their own associated Service Definition, describing the capabilities of the Service Adaptation, service specific parameters needed by the adaptation, attributes of the service, and any restrictions/ limitations.

An Adaptation can also be defined between STPs of the same service type in the case where encapsulation/adaptation of the input service type results in the same output service type.

4.5 Mapping NSI Topology to NML

For the purposes of the Network Services Framework, two topologies are identified: the Intra-Network and Inter-Network Topologies. Only the Inter-Network Topology is within the scope of the NSI protocol.

The NSI topology is an Inter-Network topology and is an object-oriented representation of network resources. The NSI network topology is used by the NSI for path-finding and resource reservation.

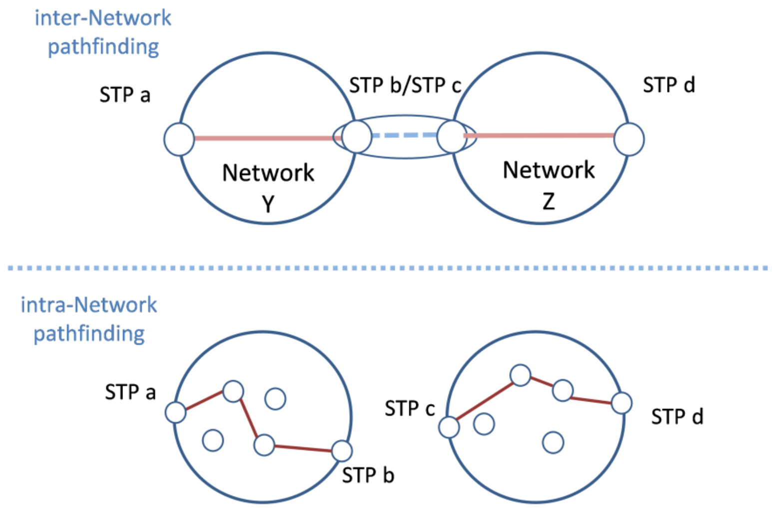

Figure 8: Pathfinding types

The Intra-Network Topology refers to the topology of the resources within a Network, where a Network is defined as the group of network resources managed by a single network provider and a single NSA. The network provider is expected to have a pre-existing management or control system with its own method for resource modeling.

The Inter-Network Topology refers to the topology of interconnected Networks. Here a Network is a topology object. The Inter-Network Topology is concerned with describing the way in which Networks are statically interconnected. It treats each Network as an aggregated set of Network capabilities with Edge Points. This Network Service Framework defines a representation of the Inter-Network Topology that should be used by the NSI.

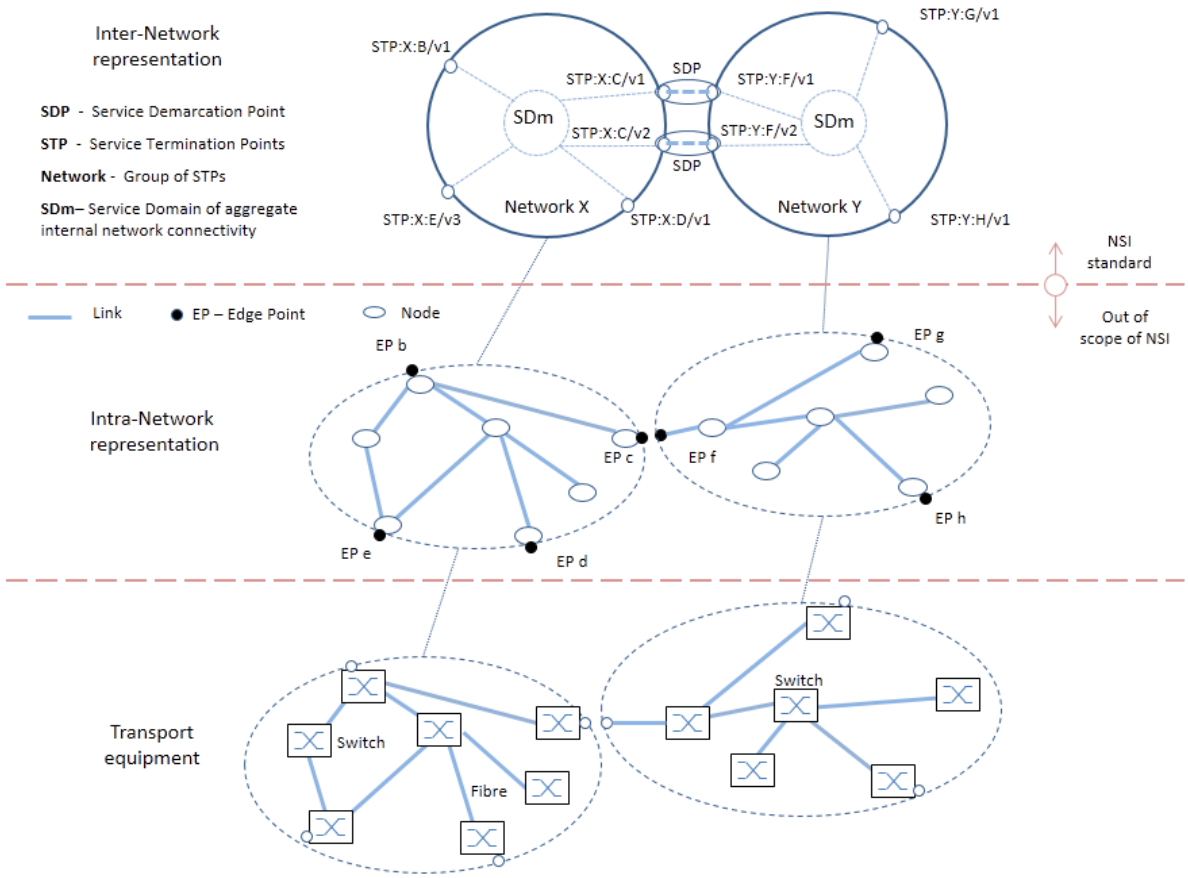

Figure 9: Inter-Network Topology

Figure 9: shows an example of an Inter-Network Topology. This example demonstrates how Inter-Network topology is described using NSI Topology definitions consisting of Networks and STPs. The NSI Topology is used to describe an aggregated representation of Intra-Network topology. The Intra-Network topology is modelled using the OGF Network Markup Language (NML).

As shown in Figure 9: 8, more than one STP may be mapped to a single port in the Intra-Network Topology representation. The instances in the figure are STP:Y:F/v1 and STP:Y:F/v2, both being VLANs and associated with port F.

The Inter-Network Topology as seen by an Aggregator NSA maybe aggregated and reported as a single Intra-Network topology to parent NSAs. This can be done only if that Aggregator NSA is the only NSA providing Service Plane connectivity for the children NSA.

By aggregating the detailed transport topology into a single Network, or by grouping several Networks together to form an aggregated Network object, the network topology may be reduced substantially. Successful implementation for a particular deployment will allow pathfinders to inexpensively compute coarse-grained paths between any pair of Networks. Each NSA along the candidate path is then consulted to reserve and confirm the resources.

Note that it should not be assumed that a Connection between Networks on the Transport Plane implies the existence of an NSI Service Plane connection between associated NSAs; the Transport Plane connectivity and NSI Service Plane connectivity are not necessarily congruent.

5. Summary

The Network Services Framework defines several key architectural elements required to request and build services within the NSI Service Plane. The framework describes an environment within which Network objects are defined as manageable resources. Within the framework, these network resources can be selected, allocated, interrogated, and manipulated by software agents on behalf of requesting users.

Federated network services are delivered by bring together the capabilities of participating providers. To manage federated services, a range of network-related functional capabilities such as topology sharing, path finding, resource reservation, hardware provisioning, and other ancillary services and functions are required. These may be formalized in future versions of the NSI protocol.

A suite of informational documents and recommendations define the NSI protocol. In addition to the Network Services Framework document, each Network Service, such as a Connection Service, is defined in its own information document and counterpart protocol recommendation.

6. Contributors

Chin Guok, ESnet
Freek Dijkstra, SARA
Radek Krzywania, PSNC
Tomohiro Kudoh, AIST
John MacAuley, SURFnet
Takahiro Miyamoto, KDDI R&D Laboratories
Inder Monga, ESnet
Guy Roberts, DANTE
Jerry Sobieski, NORDUnet
Henrik Thostrup Jensen, NORDUnet
Jeroen van der Ham, University of Amsterdam

7. Glossary

Activate	When provisioning of a Connection has been completed the Connection is considered to be Active. A dataPlaneStateChange notification is sent to the RA with "active" set to "true" informing them that the Connection is Active.
Aggregator (AG)	The Aggregator is an NSA that has more than one child NSA, and has the responsibility of aggregating the responses from each child NSA.
Connection	A Connection is an NSI construct that identifies the physical instance of a circuit in the Transport Plane. A Connection has a set of properties (for instance, Connection identifier, ingress and egress STPs, capacity, or start time). Connections can be either unidirectional or bidirectional.
Connection Service (CS)	The NSI Connection Service is a service that allows an RA to request and manage a Connection from a PA.
Connection Service Protocol	The Connection Service Protocol is the protocol that describes the messages and associated attributes that are exchanged between RA and PA.
Control and Management Planes	The Control Plane and/or Management Plane are not defined in this document, but follow common usage.
Coordinator	The Coordinator function has the role of providing intelligent message and process coordination, this includes tracking and aggregating messages, replies and notifications and the servicing of query requests.
Discovery Service	The NSI discovery service is a web service that allows an RA to discover information about the services available in a PA and the versions of these services.
Edge Point	A network resource that resides at the boundary of an intra-network topology, this may include for example a connector on a distribution frame, a port on an Ethernet switch, or a connector at the end of a fibre.
ero	An Explicit Routing Object (ero) is a parameter in a Connection request. It is an ordered list of STP constraints to be used by the inter-Network pathfinder.
Inter-Network Topology	This is a topological description of a set of Networks and their transfer functions, and the connectivity between Networks.
Lifecycle State Machine (LSM)	The LSM allows messages relating to terminating a Connection to be sent and received.
Message Transport Layer (MTL)	The MTL delivers an abstracted message delivery mechanism to the NSI layer.
Network	A Network is an Inter-Network topology object that describes a set of STPs with a Transfer Function between STPs.
Network Markup Language (NML)	The Network Markup Language is an XML based network resource description language developed in the OGF.
Network Resource Manager (NRM)	The Network Resource Manager is the entity that manages a network, typically this will be the equipment vendor's network management system.
Network Services	Network Services are the full set of services offered by an NSA. Each NSA will support one or more Network Services.
Network Service Agent (NSA)	The Network Service Agent is a concrete piece of software that sends and receives NSI Messages. The NSA includes a set of capabilities that allow Network Services to be delivered.
Network Services Framework (NSF)	The Network Services framework describes an NSI message-based platform capable of supporting a suite of Network Services such as the Connection Service and the Topology Service.
Network Service Interface (NSI)	The NSI is the interface between RAs and PAs. The NSI defines a set of interactions or transactions between these NSAs to realize a Network Service.
NSI Message	An NSI Message is a structured unit of data sent between an RA and a PA.
NSI Topology	The NSI Topology defines a standard ontology and a schema to describe network resources that are managed to create the NSI service. The NSI Topology as used by the NSI CS (and in future other NSI services) is described in: GWD-R-P: Network Service Interface Topology Representation [3].
Open Grid Forum (OGF)	The OGF is the Standards Developing Organization (SDO) that is home to the NSI

	Standards.
Provision	Provisioning is the process of requesting the creation of the physical instance of a Connection in the data plane.
Provision State Machine (PSM)	The Provision State Machine is a simple state machine which transits between the Provisioned and the Released state.
Release	Releasing is the process of de-provisioning resources on the data-plane. When a Connection is Released on the data-plane, the Reservation is retained.
Requester/Provider Agent (RA/PA)	An NSA acts in one of two possible roles relative to a particular instance of an NSI. When an NSA requests a service, it is called a Requester Agent (RA). When an NSA realizes a service, it is called a Provider Agent (PA). A particular NSA may act in different roles at different interfaces.
Reservation State Machine (RSM)	The state machine that defines the message sequence for creating Connection reservations and managing these reservations.
Service Definition (SD)	The Service Definition is an XML document describes the attributes of a service that a user can request.
Service Demarcation Point (SDP)	Service Demarcation Points (SDPs) are NSI topology objects that identify a grouping of two Edge Points at the boundary between two Networks.
Service Termination Point (STP)	Service Termination Points (STPs) are NSI topology objects that identify the Edge Points of a Network in the intra-network topology.
Service Plane	The Service Plane is a plane in which services are requested and managed; these services include the Network Service. The Service Plane contains a set of Network Service Agents communicating using Network Service Interfaces.
Simple Object Access Protocol (SOAP)	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks.
Reservation State Machine (RSM)	The Reservation State Machine state machine defines the sequence of operation of messages for creating or modifying a reservation.
Reserve	When a Provider Agent receives (and then confirms) a Connection Reservation request the Provider Agent then holds the resources needed by the Connection.
Terminate	Terminating is the process which will completely remove a Reservation and Release any associated Connections. This term has a formal definition in the CS state-machine.
Topology Distribution Service	The NSI Topology distribution Service is a service that allows the NSI topology to be exchanged between NSAs.
Transport Plane	The Transport Plane refers to the infrastructure that carries the physical instance of the Connection, e.g. the Ethernet switches that deliver the circuit.
Ultimate PA (uPA)	The ultimate PA is a Provider Agent that has an associated NRM.
Ultimate RA (uRA)	The ultimate RA is a Requester Agent is the originator of a service request.
XML Schema Definition (XSD)	XSD is a schema language for XML.
eXtensible Markup Language (XML)	XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

8. Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

9. Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

10. Full Copyright Notice

11. References

1. ITU-T, G.805: Generic functional architecture of transport networks OGF GWD-R-P “NSI Connection Service v2.0”
2. ITU-T G.8080/Y.1304: Architecture for the automatically switched optical network (ASON)
3. OGF GFD.212 Network Service Interface Connection Service, v2.0
4. OGF GWD-I Network Service Interface Topology Service Distribution Mechanisms https://redmine.ogf.org/dmsf_files/12980?download=
5. GWD-R-P Network Service Interface Topology Representation
6. OGF GFD.206: Network Markup Language Base Schema version 1 http://www.gridforum.org/documents/GFD.206.pdf
7. OGF GFD.202 A URN Namespace for Network Resources
8. IETF RFC 4122, A Universally Unique IDdentifier (UUID) URN Namespace
9. IETF RFC 4655, "A Path Computation Element (PCE)-Based Architecture", http://www.rfc-editor.org/rfc/rfc4655.txt
10. IETF RFC 6453, “A URN Namespace for the Open Grid Forum (OGF)”, http://tools.ietf.org/html/rfc6453
11. OGF GFD-CP.191 "Procedure for Registration of Subnamespace Identifiers in the URN:OGF Hierarchy”, http://www.ogf.org/gf/docs/