**Network Services Framework**

Status of This Document

This document provides information to the Grid community on the service interface between a requesting software agent and a provider software agent that offers and delivers a Network Service. It is intended to describe the processes and environment in which software agents interact to deliver the service(s). Representing applications or other networks, these agents may request certain services of other network agents. Distribution is unlimited.

Copyright Notice

Copyright © Open Grid Forum (2008-2010). All Rights Reserved.

Trademark

OGSA is a registered trademark and service mark of the Open Grid Forum.

Abstract

The Network Services Framework describes a framework to support the request and management of Network Services; it allows an application or network provider to request Network Services from other network providers. This framework incorporates the interface, agent and associated services. The Network Service Interface (NSI) is defined to be the set of protocols and parameters that are used between a software agent requesting a Network Service and the software agent providing that Network Service. This document and its partner Network Service recommendations make up the complete NSI specification.

Contents

[1. Context and Overview 2](#_Toc266803628)

[2. NSI framework 3](#_Toc266803629)

[2.1 Network Services 3](#_Toc266803630)

[2.2 The Network Service Interface 3](#_Toc266803631)

[2.3 The Network Service Agent 4](#_Toc266803632)

[2.3.1 The Network Resource Manager 5](#_Toc266803633)

[2.4 NSI Sessions 5](#_Toc266803634)

[2.5 NSI service extensibility 5](#_Toc266803635)

[2.6 The NSI Service Plane 6](#_Toc266803636)

[2.7 Hierarchical communications model and federation 7](#_Toc266803637)

[3. The NSI Protocol 8](#_Toc266803638)

[3.1 NSI Protocol overview 8](#_Toc266803639)

[3.2 NSI messages 8](#_Toc266803640)

[3.3 NSI Service Definitions 9](#_Toc266803641)

[3.4 Temporal aspects of NSI services 10](#_Toc266803642)

[3.5 Trust and authentication in NSI 10](#_Toc266803643)

[3.6 NSI Service Plane error handling 10](#_Toc266803644)

[4. Representing network resources 12](#_Toc266803645)

[4.1 Describing network topologies 12](#_Toc266803646)

[4.2 Using Service Termination Points 14](#_Toc266803647)

[4.2.1 Service Termination Point 14](#_Toc266803648)

[4.2.2 Service demarcation point 14](#_Toc266803649)

[4.3 Managing Connections with the intra-Network topology 15](#_Toc266803650)

[5. Contributors 16](#_Toc266803651)

[6. Glossary 17](#_Toc266803652)

[7. Intellectual Property Statement 18](#_Toc266803653)

[8. Disclaimer 18](#_Toc266803654)

[9. Full Copyright Notice 19](#_Toc266803655)

[10. References 19](#_Toc266803656)

# 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 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 is particularly true within the Research and Higher Education space and the growing Grid community.

Connections across these transport networks have been historically 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 being described in this recommendation.

Automated connection-oriented transport provisioning capabilities are currently being deployed by Research & Education (R&E) providers as well as by commercial providers, and could eventually be implemented in home/ retail networks as deployment progresses. 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 (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 of a network provider. In the latter context, one network is interacting with other network(s) 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 defines several key architectural elements: a Network, a Network Service, the Network Service Agent (NSA), the Network Service Interface (NSI), and the NSI Protocol. These elements exist in a notional Network 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.

Network resources and capabilities are presented to the consumer through a set of ‘Network Services’. The Network Services Framework presents a unified model for interacting with these services. Network services include the ability to create connections, to share topology information, and to do other services needed by a set of federated NSAs.

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. These may be formalized in future versions of the NSI protocol.

The NSI protocol is defined by a suite of documents. This informational document describes the NSI Framework. In addition, each Network Service is defined in its own recommendation document.

# NSI framework

This section discusses the architectural concepts that provide the Network Service context and high-level definitions for NSI protocol recommendations.

## Network Services

Network Services are services that can monitor, control, interrogate and support the network capabilities available to the provider of the Network. Typically transport network resources will include a range of technologies such as wavelengths delivered using ROADMs, TDM on cross-connect equipment or packets over switches. The NSI framework is designed to deliver a wide range of Network Services.

An example of a Network Service is the Connection Service, a service used to request and manage transport connections. Another example is the Topology Service; this is used to exchange network topologies.

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

Each service offered 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.

The NSI protocol deals with an abstracted model of transport services. This abstract concept is a simplified and convenient means of presenting the key functional aspects of the service object while hiding most or all of technical details and real-world complexities that are not relevant to the application.

Each service is managed by an exchange of NSI messages between agents. These messages operate using a set of service primitives. These service primitives are the set of instructions that allow the requestor set up and manage a service.

Each service request will result in the allocation of a service id and the creation of a new service instance. The responsibility for allocating the service id lies with the Requester NSA.

In the remaining part of this section, the architectural components that make up the Network Services framework are described.

## 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 communicating software agents: the Requester NSA and the Provider NSA. These agents interact to realize the delivery of a Network Service intrinsic to the network infrastructure. In this model, the Requester NSA requests some service, and the Provider NSA attempts to deliver it (see **Figure 1**).

**Figure 1: NSI interface**

## The Network Service Agent

The Network Service Agent (NSA) is a software entity that implements the NSI interface as well as the supporting processes to interact with the transport resources and/or middleware to deliver the requested service. The NSA is central to the NSI architecture since all NSI processes are implemented within the Network Service Agent (NSA). The NSA can support many different types of NSI Service. Each service type can have multiple service instances; these instances are created in response to a service request. For example, each NSA shown in Figure 2 includes two instances of a Network Service, these are depicted as the green ‘Network Service’ boxes.

The NSA assumes three possible roles – Requester, Provider and Federating NSA. As a Requester, the NSA requests network resources and as a Provider it delivers these network resources to create a service. The Network Service Agent may at times act as a requester over one NSI interface while acting as a provider at a different NSI interface. This is the case in a Federating NSA acts as a gateway to other providers; in this role the NSA can forward requests to other Provider NSAs. Federations of networks are described further in section 2.7. These three modes of operation are depicted in Figure 2.

Figure 2: Network Service Agent modes

Also present in the NSA, but not shown, are some additional supporting functions such as path-finding function or an NSA forwarding look up service. These functions may be local or remote, the definition of these functions is out of scope of this document.

### The Network Resource Manager

The Provider and Federating NSAs may incorporate a Network Resource Manager (NRM). The NRM manages the part the Network Service implemented over local network resources; two examples of NSAs with NRMs are shown in Figure 3.

Figure 3: NRMs in an NSA

## NSI Sessions

The NSI protocol supports two types of secure session. A NSA-to-NSA session provides a common session between NSAs, the service-to-service sessions provide per NSI service instance session, as depicted in Figure 4.

Figure 4: NSI sessions

## NSI service extensibility

The Network Services Framework provides a common platform on which Network Services can be delivered. To achieve this aim, the NSI Architecture is extensible; it inherently supports the ability to add new Network Services as they emerge. Examples of anticipated services include a Topology Service to distribute topology information and a Connection Monitoring service. The Network Service Agents must support these services and functions in order to provide the integrated service envisioned.

## The NSI Service Plane

This architecture assigns the NSI to a notional Service Plane. Here we define the Service Plane as incorporating participating NSAs and the associated NSI sessions between these NSAs. The transport equipment (switches, X-connects etc) resides in the Transport Plane. This 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.

Figure 5: Transport Plane and Service Plane

## Hierarchical communications model and federation

The Network Services Framework is intended to allow services to be delivered across a chain of multiple 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, an NSA may be directly reachable or reachable only via a gateway NSA. For instance, an arbitrary set of Networks may band together under NSI rules and peer exclusively with a single Federating NSA. The Federating NSA may have no transport resources of its own – just those resources under management of the children NSAs. Service requests will flow along the trusted sessions hierarchically among NSAs.

Figure 6 shows an example of the hierarchical model of communications. In the case of a federation of NSAs, the Federating NSA becomes a communications parent for its child NSAs. An example of this is shown where NSA A communicates with NSA D via NSA B.

Figure 6: Hierarchical communications model

It should be noted that in the case of highly meshed NSAs, a destination NSA may be reachable by more than one path. An example of this is shown in the next figure. The NSI protocol places no constraints on how to forward NSI messages. For example NSA A wishing to control a resource at E may choose to do this via intermediate NSAs B or C.

Figure 7: Complex communications model

The following is a legitimate scenario that could apply to the complex communications model shown in Figure 7:

1. The upper left Requester NSA requests a Connection X-Z from NSA A.
2. NSA A divides the request in two parts and creates two new requests:
 - a request for Connection X-Y is sent to NSA B
 - a request for Connection Y-Z is sent to NSA C
3. NSA E can provide both a part of Connection X-Y and Connection Y-Z. So both NSA B and NSA C forward their request to NSA E.
 - NSA B sends a request for a part of Connection X-Y to NSA E
 - NSA C sends a request for a part of Connection Y-Z to NSA E
4. NSA E provides the Connections of both requests independently and simultaneously.

# The NSI Protocol

## NSI Protocol overview

Network Services are delivered with the use of the NSI Protocol. This protocol defines the constructs, state machines, messages, and parameters associated with the NSI services model. An NSA, by definition, is an agent that implements the NSI Protocol. The details of this protocol are out of scope of this document; the NSI Protocol recommendation (GWD-R-XXX) provides a detailed definition of the NSI framework protocol. In addition, each Network Service has its own recommendation document.

## NSI messages

The NSI protocol describes an exchange of NSI messages between the requestor and provider, the details of these messages are defined by the NSI service. Each message contains:

* Identification of the Network Service type. (eg Connection Service, Topology Service, etc)
* Identification of the Network Service version (v1.0, v2.0 etc).
* Identification of a specific service instance
* Identification of a message thread
* A service primitive.

The base NSI protocol handler recognizes NSI messages between NSAs. The protocol examines each message received for its Service Identifier and forwards that message to the appropriate service specific handler. The service and its associated Service Definition define the full set of capabilities that are offered to requesters and the service instance defines one specific instance of the service.

Each NSI service defines a service instance which is an independent, uniquely identifiable deliverable unit of the service. For example, the NSI Connection Service refers to a particular connection as a service instance; a topology distribution service may define an instance to be a particular topology graph, or a topology transaction such as a full dump or incremental update.

Each Network Service type includes set of service primitives. These primitives form a set of instructions that pass from the requester to the provider. In general, a service specific state machine allocated and associated with each service instance, and the service primitives drive the transitions of that state machine. A service primitive may require a sequence of messages or even its own state machine to affect an exchange of messages.

An NSI Message also includes a mechanism to associate it with an NSI Message Thread to allow differentiation of message streams associated with simultaneous and asynchronous service functions occurring between pairs of NSAs. NSI Messages include a mechanism to ensure that ordering is maintained in a NSI Message Thread.

Service Instances are processed asynchronously with respect to other service instances. For example, one connection may transition from reserving, to scheduled, to in-service, to release at a vastly different speed than another connection established by the same service agent.

Each service instance must have a locally unique identifier.

## NSI Service Definitions

The concept of Service Definitions is introduced to allow network providers to formally identify and define the characteristics associated with each service offering.

The Service Definition consists of a set of attributes that formally and explicitly define the complete scope of a service offering. In particular, the NSI Connection Service uses the Service Definition as a baseline set of parameters to bound the scope of the service that will be offered to requesters.

The Service Definition specifies the set of service parameters that completely specify a service instance. For example, the Service Definition might identify “capacity”, “mtu\_size”, and “maximum\_frame\_loss\_rate” as three aspects of the service. The Service Definition also describes the *range* of allowed values for each service parameter, and a default value can be specified. In the context of the previous example, the range of allowed values for the “capacity” parameter may be 50 mbps to 10 gbps in increments of 150 mbps. Or the “mtu\_size” may be defined to be 1500 Bytes to 9000 Bytes with a default of 1500. The parameters in the Service Definition form a kind of template that the service request must fill in. I.e. A service request must fill in the template with an explicit value - or a default value taken from the service definition - for each parameter of the service it is requesting. A service request is fully specified when all parameters associated with that service have been determined either by explicit user specification or by implicit default values found in the Service Definition. This fully specified request is then processed by the NSA and, if all service specifications can be satisfied, a service instance is created (and reserved).

The Service Definition is an integral component of the NSI architecture in that it is key to vetting service requests against the multi-domain service offerings encountered along a candidate path.

The Service Definition is a public document that can serve as a both a human readable guide to available service capabilities and a machine readable file that can be processed by automated agents in the NSI Architecture.

## Temporal aspects of NSI services

Services, in which resources are dynamically requested, reserved and provisioned, require temporal aspects to be understood and deterministic. Any service that supports advance reservation must maintain its own real-time clock and it is necessary for the requester and provider clocks to be aligned.

When resources are sought by a requester NSA from a provider NSA, a service instance is created and an identifier is assigned to that service instance. Then, according to the parameters of the request (i.e. its Service Definition), the provider NSA identifies and reserves a set of available resources that satisfy the request and associates them to the instance. The resources are provisioned and released at some point on the temporal axis. The time information and signaling are used to specify the time boundary of the requested connection in-service period. It is the responsibility of the Provider NSA to attempt to deliver the connection as close to the start and end times as it is able. It should be noted that this may have some uncertainty as typically the duration of the provisioning phase cannot be precisely predicted.

## Trust and authentication in NSI

This section describes the approach taken to trust and authentication in the NSI protocol; the detailed mechanisms for providing security and authentication are described in the NSI protocol recommendation.

Each NSA establishes NSI sessions with one or more other NSAs. An NSA will know for example that it is physically connected to its neighbor NSA; it may also have an identifier for that neighbor. Four types of trust are identified; types 1 and 2 are depicted in Figure 4 - NSA-NSA and service-to-service. Types 3 and 4 relate to trust beyond a Requester/Provider NSA pair.

1) NSA-to-NSA relationship: The Requestor and Provider NSAs establish a secure session between Agents.

2) Service-to-Service relationship: Secure sessions are established between the requester and provider parts of a Service. Standard methods for securing these sessions are described in the protocol document. These include a) piggybacking trust on the NSI trusted connection and b) using separate ids and keys for the services.

3) Trust between attribute provider and policy server (attribute user): attributes included in a message must be trusted by the message receiver. When the sender and receiver are in adjacent NSAs this trust may be piggybacked on NSI trusted connection. When an attribute received by an NSA is passed on in a message to another NSA a mechanism to provide trust between non-adjacent NSAs is required. [This requires input from security for better definition of options]

4) Trust between connection reservations authorized on the service plane and connections provisioned on the transport plane is required. A connection may not be provisioned unless it has been scheduled. Provisioning must know that the connection has been approved and scheduled.

## NSI Service Plane error handling

The Network Service Framework is based on a distributed, multi-agent architecture that is designed to handle error cases in such a way as to ensure predictable and deterministic behavior. This section describes the basis of error handling for this protocol.

Network service errors can be broadly categorized as soft or hard failures. A soft failure occurs when two NSA agents lose communication with each other. A hard failure occurs if the NSA software restarts for any reason.. Such failures may cause a loss of information about state information about services that were previously scheduled or are in process of being scheduled.

The NSI protocol incorporates mechanisms to recover to a consistent and predictable state after detecting an anomaly. The following architectural principles guide error handling and recovery:

Handling of failures should result in deterministic behavior that is user centric and oriented towards the service model, for example: A failure in the Service Plane should not affect resources that are provisioned and active in the Transport Plane. A failure in the Service Plane should not result in an incomplete service.

Recovery of Transport and/or Service Plane should not be reliant on external entities or mechanisms. For example, an NSA recovering from a hard failure error condition will not depend on peer NSAs to reconstruct its state. This does not prevent a query function to validate its own view with its peers.

Failures in the Service Plane can result in NSA state faults. Examples of Service Plane errors include: losing communication with an NSA, losing communication with the transport network, corruption/crash in the platform etc. These errors may result in service disruptions until these states can be synchronized, hence the NSI protocol and state machine design should account for such scenarios.



Figure 8: Local/Remote Failures within the context of a provider NSA

Regardless of where the error originates, it is important that the NSA recover to a deterministic state. This means that both the user service state and the resource state should be consistent between NSAs.

The distributed model of servicing user requests using tree/chain model allows each NSA to assume the role of a requester or provider. When Service Plane failures occur, it is possible that an NSA will become entirely disconnected from other NSAs involved in a service instance. This scenario imposes a requirement on the NSA to have a linkage between its Requester and Provider Agent state machines to understand the impact of the failure on the service tree and recover from it. The state machines should be designed so the outcome of a distributed failure ends each state machine in a deterministic state.

# Representing network resources

## Describing network topologies

A Network topology is an object-oriented representation of Network resources. The Network topology may be used by functions such as path-finding and resource reservation.

For the purposes of the Network Services Framework, two topologies are identified; these are the intra-Network and inter-Network topologies. Only the inter-Network topology is in-scope for the NSI protocol.

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 operator and a single NSA. The network operator is expected to have a preexisting management or control system with its own method for network modeling. It is assumed that each NSA has access to its topology information, and no assumptions are made as to how this has been gathered or how it is represented. In other words, the method by which the intra-Network topology is represented is out-of-scope for the Network Service Framework. Many languages and models have been proposed to describe networks; some examples are OGF NML and ITU-T G.805, it is expected that these and others could be used.

The *inter-Network* topology refers to the topology of interconnected Networks. The inter-Network topology is only concerned with describing the way in which Networks are interconnected and an aggregated set of Network capabilities. This Network Service Framework defines a representation of the inter-Network topology that should be used by the NSI. This is referred to as the NSI inter-Network topology or the inter-Network topology.

The inter-Network topology describes objects known as Service Termination Points (STPs) which are the edge points of a Network. These points represent resources (typically ports) where Networks can be interconnected. A Network is a grouping of STPs that are owned by a single operator. A Network may have an associated internal transfer function matrix between STPs; this matrix describes the aggregated connectivity inside the Network.

Each operator can advertize a set of STPs. It is important to note that the operator advertises STP capabilities, and the NSA instantiates instances of an STP. Details for using STPs are described in the next section.

Figure 9 depicts an example of an inter-Network topology. It shows an example of how a Networks and STPs can be used to describe an aggregated representation of a conventional Network model such as OGF-NML.

Figure 9: Inter-Network Topology

From a global perspective, the use of the Intra-Network topology to aggregate detailed transport topology within a Network object substantially reduces the size and complexity of the topology information base. This has positive implications for coherence and convergence, for dynamic topology distribution, path finding efficiency, and for scalability in the global environment. It has the less desirable effect of reducing optimality – it becomes increasingly difficult to choose a resource efficient path. The trade off is an issue of pragmatism, and will be steered by best practices as the experience base improves.

By aggregating detailed transport topology into a single Network, or by grouping several Networks together to form a Federating Network object, the global network topology may be reduced substantially. Successful implementation for a particular deployment will allow Pathfinders to inexpensively compute coarse grained path(s) 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 a NSI connection between associated NSAs. I.e the Transport Plane connectivity and Service Plane connectivity cannot be assumed to be congruent.

## Using Service Termination Points

The NSI Architecture adopts generalized notion of a Service Termination Points (STPs) and a pairing of STPs at a service demarcation point. An STP names a topological location that is the ingress/egress point of a Network. For the purposes of the Connection Service, the demarcation point also forms the point at which Connections can be concatenated. This is the junction between the ingress of a Connection in one Network and the egress of a Connection in the next Network.

### Service Termination Point

A prerequisite for an STP is the existence of a physical connection into a Network. This preexisting capability (typically made up of a physical port on a Network) can be advertised to an NSA. Note that the choice about which resources to advertize is subject to local policy. Once advertised, these capabilities may be used by the path-finding function of the NSA.

STPs are advertised as ‘capabilities’ to the NSA. I.e., they are not instantiated resources, but rather capabilities available for use in creating a Network Service. For example this would include advertising that a VLAN id 30 is available for use. When the NSA wishes to instantiate VLAN 30 this is signaled to the NRM and the VLAN 30 instance is created. Both STP capabilities and STP instances are represented in the Service Plane with STP ids.

An STP is a symbolic reference, i.e. it is an identifier which comprised of a parsable alphanumeric string containing two components: 1) a Network identifier string in the higher order portion, and 2) a local STP identifier in the lower order portion. An STP must always resolve to a specific topological port object as defined in the intra-Network topology representation.

STPs may be uni or bi-directional. In the uni-directional case, the STP functions either as an ingress point or an egress point, this is defined by the flow polarity of the associated port, and which side of the junction is the user side, and which side is the network side.

An STP capability can be represented as a group of possible STP instances, or a more flexible representation like wildcard and constraints. For example, if there are 10 links these may be represented as a list (a,b, c, d, … j) or as a range (a-j).

A hierarchy of STPs may be represented using such groupings. For example an STP group A may contain 10 STPs (a-j). This can be represented as: A/a, A/b … A/j.

To support aggregation functions (Ethernet LAG or SDH virtual concatenation), two or more STPs can be aggregated. For example, if there are 10 links (1, 2, 3, …, 10) and any two of these links can be aggregated, in this example there are 90 possible STP instances (1-2, 1-3, …, 9-10). The use of hierarchical STP groups is important for aggregation since only STPs within a group can be aggregated.

Some examples are shown in Figure 10.

### Service demarcation point

Two adjacent networks agree on the connectivity capability between the two networks. The process for this agreement is out-of-scope of the NSI. When two STPs in adjacent networks with matching capabilities are paired, the resulting pairing forms a service demarcation point. This is depicted in Figure 10.

Figure 10: STP examples

Using the example shown in Figure 10, assume there are two networks, Y and Z. The STPs are advertised and then the pairing process matches STPs in each network as follows:

STP A group:

(STP:Y:A/v1, STP:Z:A/v1)

(STP:Y:A/v2, STP:Z:A/v2)

(STP:Y:A/v3, STP:Z:A/w7)

(STP:Y:A/v4, STP:Z:A/w8)

STP B group:

(STP:Y:B/c1, STP:Z:B/d7 )

(STP:Y:B/agg(c5,c9) -STP:Z:B/agg(d8,d9)

(STP:Y:B/c20-STP:Z:B/d20)

It is important to note that the NSI inter-network topology model is composed of Networks interconnected by pairs of STPs. It should be noted that this topology is neither a standard nor does it imply that an NSI implementation must adopt specifically any particular schema for its database in the code.

## Managing Connections with the intra-Network topology

The Network Services Framework supports many services. The first of these is the Connection Service. The purpose of this service is to manage Connections. A Connection is defined to be the connectivity between STPs. Connections may be concatenated at service demarcation points (STP pairs) to create longer Connections.

The process of instantiating a Connection requires the NSA to send a Connection instantiation instruction to the NRM. This is identified using the ingress and egress STPs.

Once instantiated, an STP may have properties such as a framing, bandwidth and a VLAN id. Some of these properties may reflect the requirements specified in the service definition. Labeling (cf. fiber id, wavelength, VLAN id) and aggregation (cf. combining multiple switch ports) can be modeled as a property of an STP.

A service demarcation point can function as both an ingress point on one side and an egress point on the other. Two such connections that share a single service demarcation point in this way are said to be concatenated. These two concatenated connections then appear to the user payload as a single end-to-end transport plane data-path. In this way a service demarcation point becomes intermediate transit-point of a path or connection, i.e a routing point through which the connection must pass.

Figure 11 depicts an example of a connection service between hosts, one internal to Network W and the other attached to an STP of Network Z. The Connection is created by requesting a Connection in Networks X, Y and Z. In Network W the Host is internally connected, (i.e not advertised to the NSA). In Network Z the host is connected to an STP it may be reached directly by using an NSI connection to STP k.

Figure 11: Representing Connections

Using the example in Figure 11, to request the shown inter-Network connection, the NSA will request:

• To network X: instantiate a connection between STPs: X::b and X::c

• To network Y: instantiate a connection between STPs: Y::f and Y::h

• To network Z: instantiate a connection between STPs: Z::j and Z::k

Each NSA looks up its own calendar and checks availability of the STPs. Note that the NSAs for Networks X, Y and Z may have differing availability information in their local calendars.

# Contributors

Joan A. García-Espín, I2CAT

Chin Guok, ESNET

Radek Krzywania, PSNC

Tomohiro Kudoh, AIST

John MacAuley, Surfnet

Takahiro Miyamoto, KDDI R&D Laboratories

Inder Monga, ESnet

Guy Roberts, DANTE

Jerry Sobieski, NORDUNET

Sebastien Soudan, Laboratoire de l'Informatique du Parallèlisme

John Vollbrecht, Internet2

Freek Dijkstra, SARA

Jeroen van der Ham, University of Amsterdam

# Glossary

Connection

A Connection is a conduit that transparently moves user information across a Network from an ingress point to an egress point. A Connection has a set of properties (for instance, capacity, or authorization, or start time).  These properties, and their allowed range of values, are defined by a service definition. A Connection instance on the Transport Plane is identified by a Connection Identifier exchanged on the Service Plane

Connection Identifier

A Connection Identifier is a label which can be used to identify a Connection for the purposes of request, instantiation and management.

Connection Service

A Connection Service is a service that allows a Requester NSA to request and manage a Connection from a Provider NSA

Control and Management Planes

The Control Plane and/or Management Plane are not defined in this document, but follow common usage.

Network
A Network is an inter-Network topology object that describes the transport resources that are managed by a single NSA.

Network Resource Manager (NRM)

The Network Resource Manager owns a particular set of transport resources and has ultimate responsibility for authorizing and managing the use of these resources.

Network Services

Network Services are the full set of services offered by an NSA. A Network Service is an abstract service that must be implemented by a concrete network service agent (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 Service Interface (NSI)

The NSI is the interface between Requester NSAs and Provider NSAs.  The NSI defines a set of interactions or transactions between these NSAs to realize a Network Service.

Network Services Framework

The Network Services framework describes a message based platform capable of supporting a range of Network Services.

NSI Message

A NSI Message is a structured unit of data sent between a Requester NSA and a Provider NSA.

Path

A Path is an ordered list of Routing Objects.

Requester/ Provider NSA

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 NSA. When an NSA realizes a service, it is called a Provider NSA.

Routing Object

A Routing Object may include the following transport resources.

Service Definition

The Service Definition is the set of attributes associated with connection services (for instance, capacity, or authorization, or start time) and a range of allowed values for these attributes. Each Connection has an associated Service Definition instance.

Service Termination Point (STP)

An STP is an edge port in a Network that is available for connection to other Networks or clients.

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 set Network Service Agents communicating using Network Service Interfaces.

Topology

The Topology resides in the Service Plane.  The Topology describes the physical resources and their interconnection as well as the non-physical groupings of various components.

Transfer Function

The Transfer Function is a matrix that describes the transport capabilities between STPs.

Transport Plane

The Transport Plane contains is the set of transport equipment and associated resources that carry user data through the network.

# 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.

# 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.

# Full Copyright Notice

Copyright (C) Open Grid Forum (2008-2010). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the OGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the OGF Document process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assignees.

# References