Network Services Interface

Document Distribution Service

John MacAuley, ESnet

2nd March 2015

Introduction

The chosen topology distribution protocol needs to fit into the overall NSI architecture and maintain existing NSI fundamental principles

- Centralized path finding for source-based routing decisions in both TREE and CHAIN signaling models.
- Distributed path finding for hop-by-hop routing decisions in the CHAIN signaling model.

The question of routing policy enforcement needs to be address within the NSI architecture before any impacts on topology distribution can be determined

- See “Example Routing Policies”, “Policy-based routing enforcement”, and “Policy-based routing enforcement through explicit approval with digital signatures” presentations for GENI/OGF/GLIF 2015 meetings.

Where are requirements for topology distribution?

- Many can be derived from the NSI fundamental principles document.
- Chin’s topology requirements proposal from Oxford.
- NSI Path finding presentation from GENI/OGF/GLIF 2014.
- Learning's from AutoGOLE deployment.

Tree signaling requirements

TREE deployments utilizing source-based routing require an aggregator NSA has access to:

- NSA description documents for all NSA within the network
  - <peersWith> and <feature> elements are used to build a directed control plane graph for message routing.
  - nsaId to networkId mappings to determine which NSA gets messages for a specific network.
  - <interface> elements for protocol endpoints.
- A full view of network topology to perform advanced "intelligent" routing decisions.
- Service description documents for all networks to determine the constraints and parameters of the services offered.

Chain signaling requirements

In a CHAIN deployment with source-based routing an aggregator NSA requires:

- NSA Discovery Documents from its directly connected peers.
- NML Topology Documents of all interconnected networks.
- Service description documents for all networks to determine the constraints and parameters of the services offered.

In a Gof3 CHAIN deployment with hop-by-hop routing an aggregator NSA requires:

- NSA Discovery Documents from its directly connected peers
  - This information is augmented with distance vector information to determine neighbor with least cost path to target network
- NML Topology Documents from its directly connected peers
  - This information is used to determine local bidirectional STP mappings to remote STP in adjacent networks.

Additional notes

We must be able to support application/project/deployment specific aggregators for use by specialized user groups.

We must be able to deploy core aggregators that perform path finding but are user agnostic. These aggregators will not know the identity of the user, nor the end user authentication schemes (uPA specific).

In most cases the uRA associated with the end user will have no concept of path finding or network topology, but instead delegates the path finding function to an aggregator within the network.

Document Distribution Service

A simple peer-to-peer flooding protocol for exchange and distribution data documents between NSA within the interconnected control plane or “document space”.

Supports both polling and subscription based notification mechanisms for exchange of documents.

What it is not

It knows nothing about path finding, topology, or routing policies.

It knows nothing about the digital signatures or encryption used on the documents it carries, but does provide support for external mechanisms.

It does not provide user specific views, however, it does allow user specific documents to be published (a document is a document).

What is a document?

A document is any piece of information that needs to be distributed to all peers participating in the service.

A document is wrapped in meta-data within the document space to allow for identification and maintenance – the protocol does not care about the document contents.

The original document contents and associated meta-data are propagated untouched throughout the document space.

Documents

Parameter	Description
nsa	The source NSA associated with the generation and management of the document within the network. This is assumed to be the NSA to which the document relates, however, there may be situations where this assumption is not true.
type	The unique string identifying the type of this document. A document type is defined by the type and release of a data document. For example, vnd.ogf.nsi.topology.v1+xml vnd.ogf.nsi.nsa.v1+xml vnd.ogf.nsi.topology.v2+xml vnd.ogf.nsi.sd.v1+xml
id	The identifier of the document. This value must be unique in the context of the nsa and type values.
version	The version of the document, or more specifically, the date this version of the document was created. Any updates to the document must be tagged with a new version.
expires	The date this version of the document expires and should be deleted from document space and any clients caching the document.
signature	An OPTIONAL digital signature of the document contents.
content	The content of the document modeled by this document meta-data.

Example document fragment


```
<document
    id="urn:ogf:network:es.net:2013:nsa"
    href="https://nsi-aggr-west.es.net/discovery/documents/urn%3Aogf%3Anetwork%3Aes.net%3A2013%3Ansa/vnd.ogf.nsi.nsa.v1%2B>
    version="2015-01-27T12:12:00Z"
    expires="2016-01-27T12:34:34.701-04:00">
    <nsa>urn:ogf:network:es.net:2013:nsa</nsa>
    <type>vnd.ogf.nsi.nsa.v1+xml</type>
    <content>
        <nsa id="urn:ogf:network:es.net:2013:nsa" version="2015-01-27T12:12:00Z" expires="2016-01-27T12:34:34.701-04:00">
            <name>ESnet OSCARS uPA</name>
            <softwareVersion>nsibridge-v1</softwareVersion>
            <adminContact>
                <vcard>
                    <uid>
                        <uri>urn:uuid:c8cdbb80-dac7-11e3-9c1a-0800200c9a66</uri>
                    </uid>
                    <prodid>
                        <text>ESnet - OSCARS NSI Bridge"</text>
                    </prodid>
                    <rev>
                        <timestamp>20140513T195243Z</timestamp>
                    </rev>
```

Subscriptions

Parameter	Description
id	The provider assigned subscription identifier that uniquely identifies the subscription in the context of the provider.
href	The direct URI reference to the resource.
version	The version of the subscription. Indicates the last time the subscription was modified by the requester.
requesterId	The identifier of the requester client that created the subscription. An NSA must use its unique NSA identifier for requesterId.
callback	The protocol endpoint on the requester that will receive the notifications delivered for this subscription.
filter	The OPTIONAL filter criteria to apply to document events to determine if a notification should be sent to the client.

Example subscription fragment


```
<subscriptions>
    <subscription id="09a1cff7-19f8-4609-9954-5b34b1112b60"
            href="https://nsi-aggr-west.es.net/discovery/subscriptions/09a1cff7-19f8-4609-9954-5b34b1112b60"
            version="2015-03-02T17:06:09.37-08:00">
        <requesterId>urn:ogf:network:netherlight.net:2013:nsa:safnari</requesterId>
        <callback>https://agg.netherlight.net/dds/notifications</callback>
        <filter>
            <include>
                <event>All</event>
            </include>
        </filter>
    </subscription>
    <subscription id="eae8d2ef-e4c5-43cd-b44f-926ec7cbd21d"
            href="https://nsi-aggr-west.es.net/discovery/subscriptions/eae8d2ef-e4c5-43cd-b44f-926ec7cbd21d"
            version="2015-03-01T19:05:02.062-08:00">
        <requesterId>urn:ogf:network:icair.org:2013:nsa:nsi-am-sl</requesterId>
        <callback>https://nsi-am-sl.northwestern.edu/dds/notifications</callback>
        <filter>
            <include>
                <event>All</event>
            </include>
        </filter>
    </subscription>
</subscriptions>
```

Example notification fragment


```
<notifications id="687b1f65-4013-4b27-8557-54219e3a179a"
        providerId="urn:ogf:network:icair.org:2013:nsa:nsi-am-sl"
        href="https://nsi-am-sl.northwestern.edu/dds/subscriptions/687b1f65-4013-4b27-8557-54219e3a179a">
    <notification>
        <discovered>2015-03-03T16:25:40-06:00</discovered>
        <event>Updated</event>
        <document id="urn:ogf:network:funet.fi:2013:topology"
            href="https://nsi-am-sl.northwestern.edu/dds/documents/urn%3Aogf%3Anetwork%3Ageant.net%3A2013%3Ansa/vnd.ogf.nsi.topology.v2%2Bxml/urn%3Aogf
            version="2015-03-03T22:25:52.251Z"
            expires="2016-03-02T14:25:52.51-08:00">
            <nsa>urn:ogf:network:geant.net:2013:nsa</nsa>
            <type>vnd.ogf.nsi.topology.v2+xml</type>
            <content>
                <Topology id="urn:ogf:network:funet.fi:2013:topology" version="2015-03-03T22:25:52.251Z">
                    <name>funet.fi</name>
                    <BidirectionalPort id="urn:ogf:network:funet.fi:2013:topology:espoo1-nordunet">
                        <name>espoo1-nordunet</name>
                        <PortGroup id="urn:ogf:network:funet.fi:2013:topology:espoo1-nordunet-in"/>
                        <PortGroup id="urn:ogf:network:funet.fi:2013:topology:espoo1-nordunet-out"/>
                    </BidirectionalPort>
                    <BidirectionalPort id="urn:ogf:network:funet.fi:2013:topology:test2-autobahn-2">
                        <name>test2-autobahn-2</name>
                        <PortGroup id="urn:ogf:network:funet.fi:2013:topology:test2-autobahn-2-in"/>
                        <PortGroup id="urn:ogf:network:funet.fi:2013:topology:test2-autobahn-2-out"/>
                    </BidirectionalPort>
```

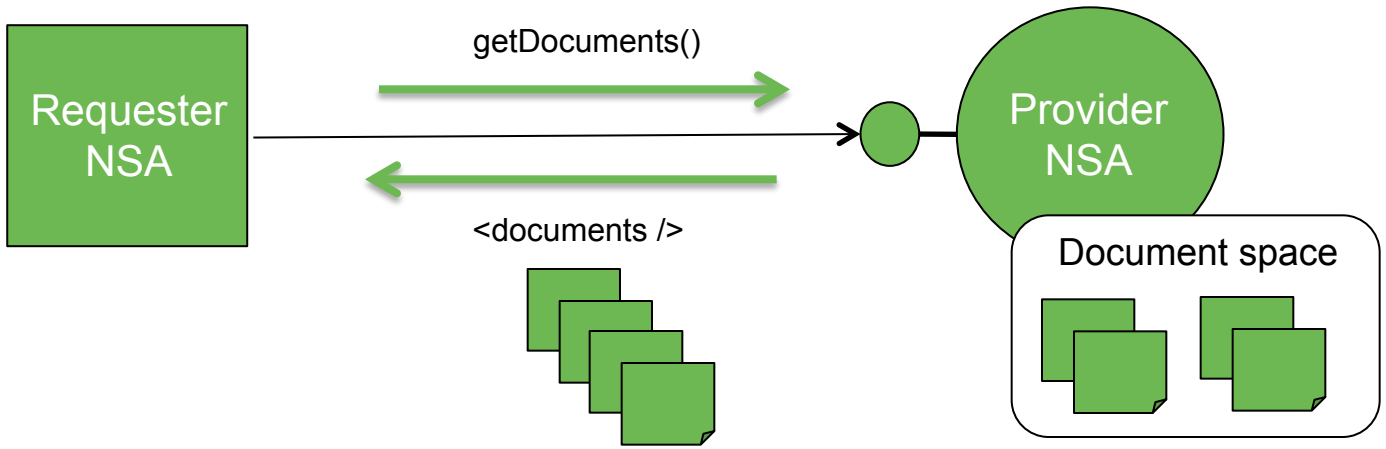
Abstract Operations

getDocuments([nsa], [type], [id], [lastDiscoveredTime])
getLocalDocuments([type], [id], [lastDiscoveredTime])
getDocument(nsa, type, id, [lastDiscoveredTime])
addDocument(nsa, type, id, version, expires, [signature], contents)
updateDocument(nsa, type, id, version, expires, [signature], contents)
** Notice no deleteDocument(nsa, type, id) operation

addSubscription(requesterId, callback, filter)
editSubscription(id, requesterId, callback, filter)
deleteSubscription(id)
getSubscriptions([requesterId], [lastDiscoveredTime])
getSubscription(id, [lastDiscoveredTime])

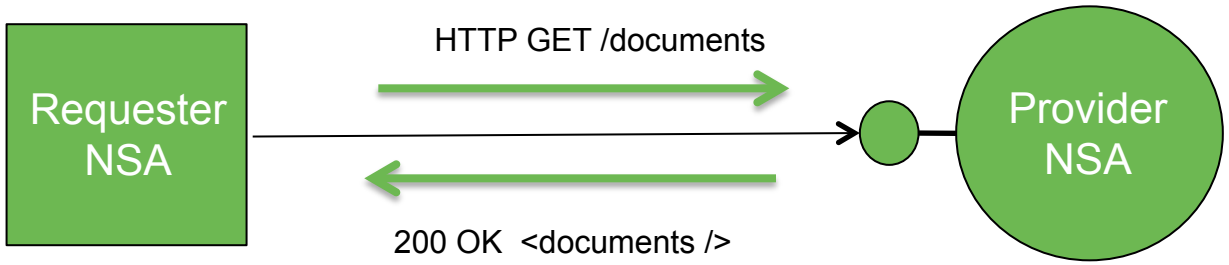
getAll([lastDiscoveredTime])

Basic Request/Response

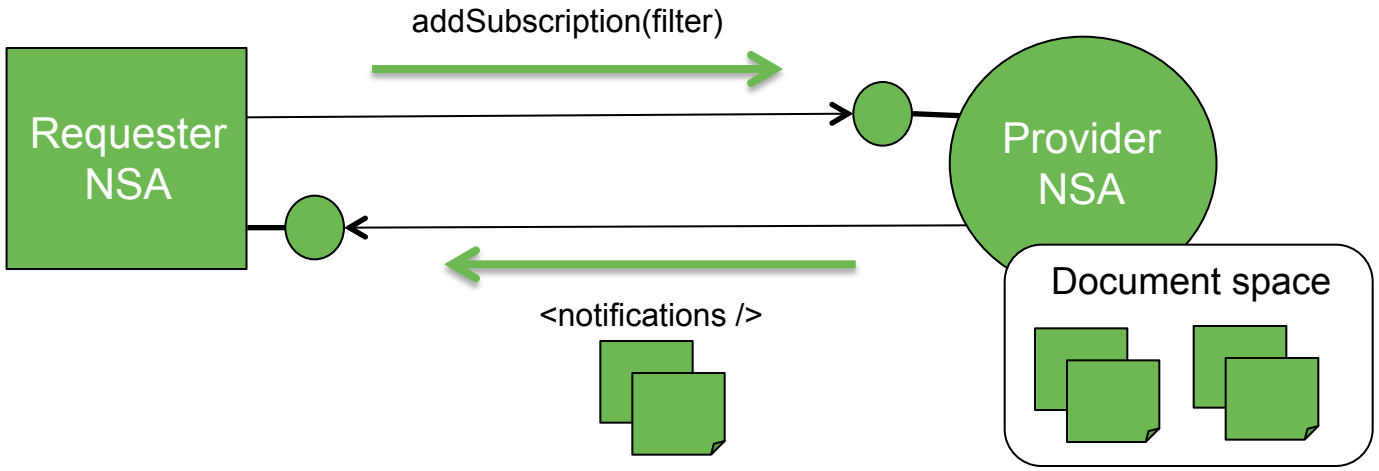


Basic Request/Response

- DDS uses a basic request/response messaging model with an HTTP binding:
  - HTTP GET carries the DDS request operation
  - HTTP 200 OK response carries result of the operation
  - HTTP socket blocks until result it returned (synchronous)

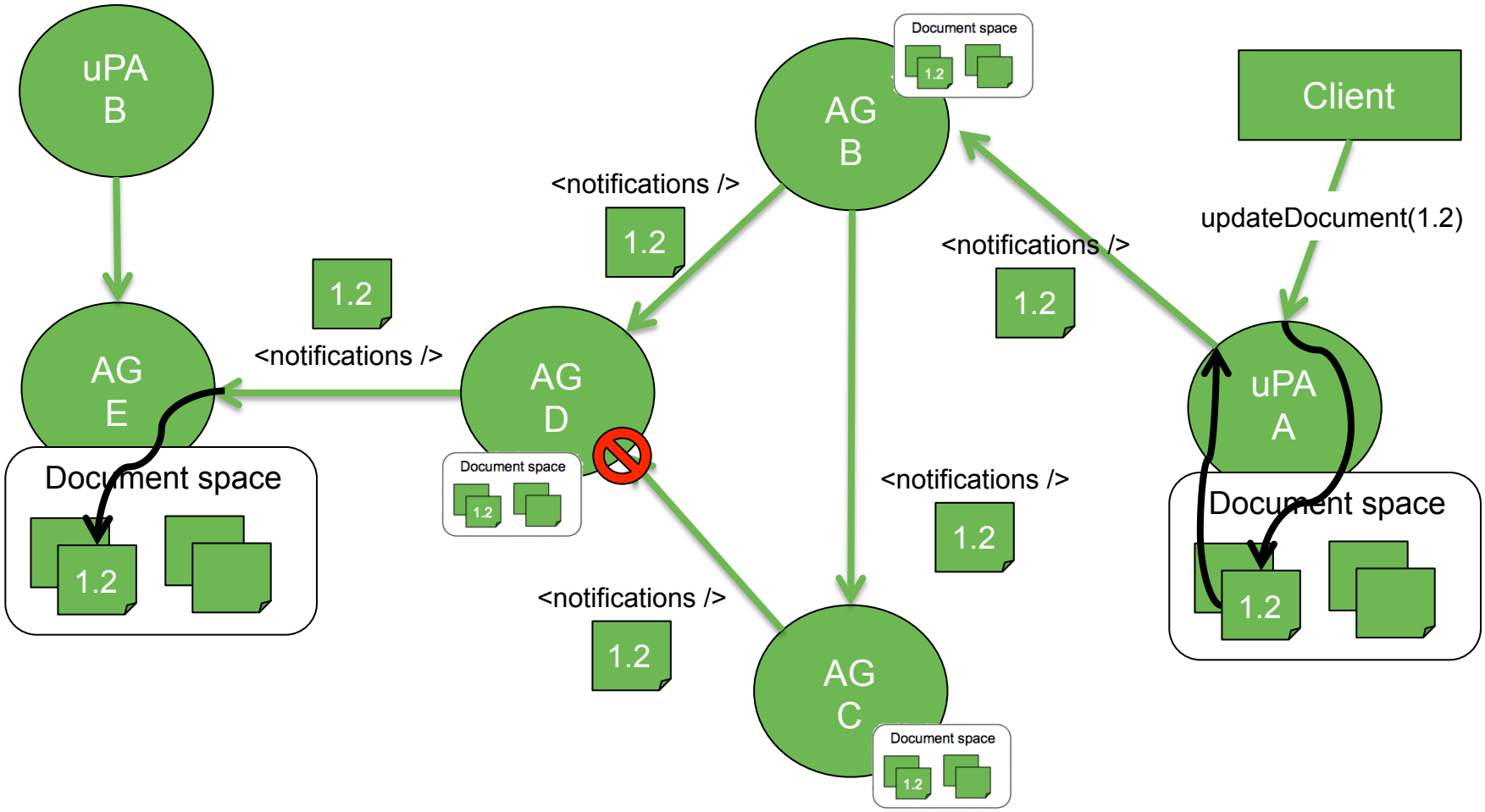


Subscriptions

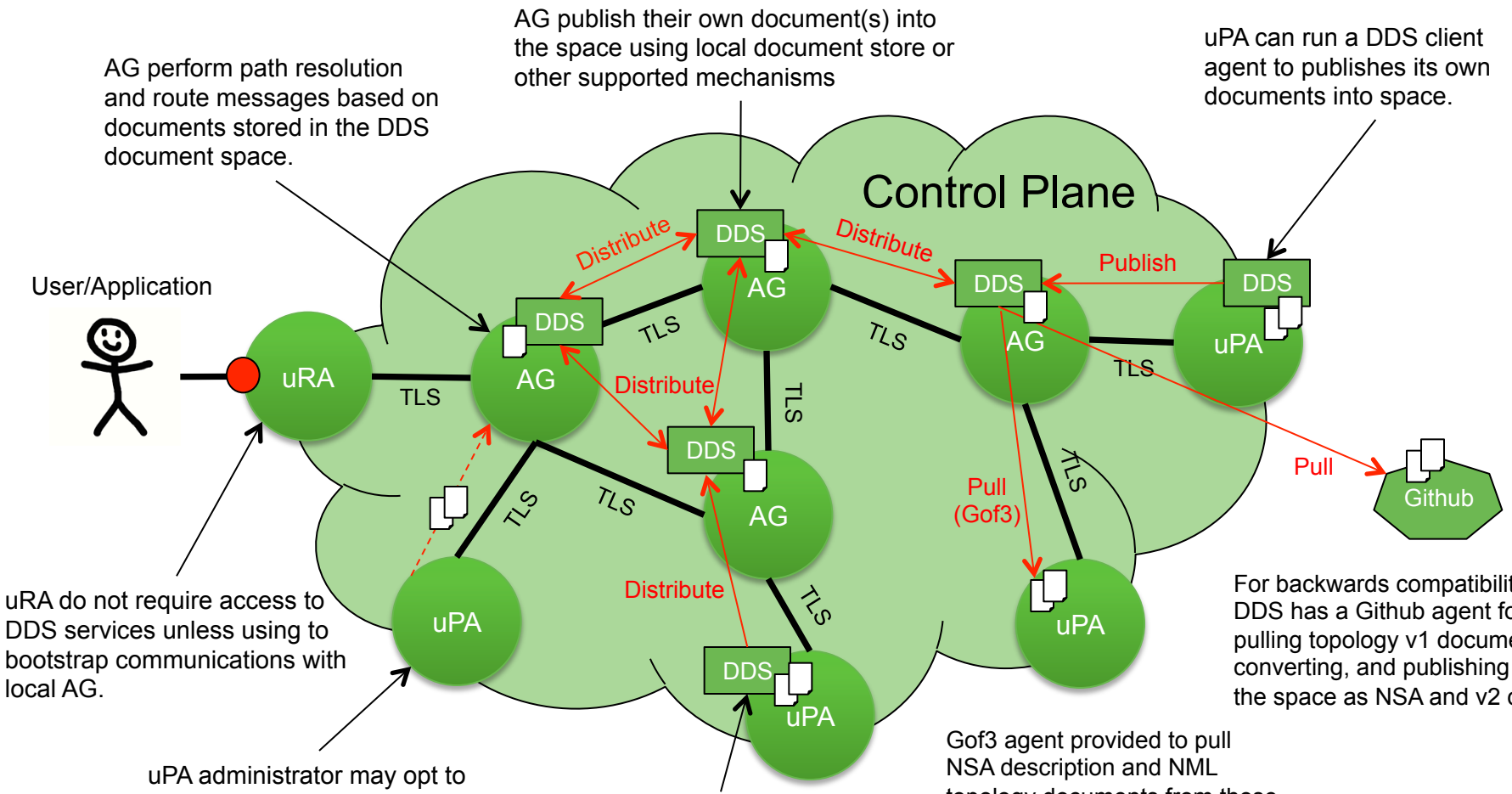


Initial subscription request, or modifications to an existing subscription result in sending of all notifications matching the subscription filter.

Flooding through notifications



Making it work in real life



AGOLE documents

```
Welcome to the DDS command shell.  Enter ?list for available commands.
dds> ls
/subscriptions (2)
/local (1)
/documents (54)
dds> cd documents
https://nsi-aggr-west.es.net/discovery/documents
dds/documents> ls
urn:ogf:network:es.net:2013:nsa (2)
urn:ogf:network:es.net:2013:nsa:nsi-aggr-west (1)
urn:ogf:network:manlan.internet2.edu:2013:nsa (3)
urn:ogf:network:southernlight.net.br:2013:nsa (2)
urn:ogf:network:sinet.ac.jp:2013:nsa (2)
urn:ogf:network:icair.org:2013:nsa (2)
urn:ogf:network:cipo.rnp.br:2014:nsa (3)
urn:ogf:network:czechlight.cesnet.cz:2013:nsa (2)
urn:ogf:network:icair.org:2013:nsa:nsi-am-sl (1)
urn:ogf:network:caltech.edu:2013:nsa (2)
urn:ogf:network:kddilabs.jp:2013:nsa (2)
urn:ogf:network:surfnet.nl:1990:nsa:bod7 (2)
urn:ogf:network:krlight.net:2013:nsa (2)
urn:ogf:network:jgn-x.jp:2013:nsa (2)
urn:ogf:network:uvalight.net:2013:nsa (2)
urn:ogf:network:geant.net:2013:nsa (10)
urn:ogf:network:ampath.net:2013:nsa (2)
urn:ogf:network:surfnet.nl:1990:nsa:bod-acc (5)
urn:ogf:network:aist.go.jp:2013:nsa (2)
urn:ogf:network:nordu.net:2013:nsa (2)
urn:ogf:network:netherlight.net:2013:nsa:safnari (1)
urn:ogf:network:netherlight.net:2013:nsa:bod (2)
dds/documents> cd urn:ogf:network:es.net:2013:nsa
https://nsi-aggr-west.es.net/discovery/documents/urn:ogf:network:es.net:2013:nsa
dds/documents/urn:ogf:network:es.net:2013:nsa> ls
vnd.ogf.nsi.topology.v2+xml (1)
vnd.ogf.nsi.nsa.v1+xml (1)
dds/documents/urn:ogf:network:es.net:2013:nsa>
```

Security

Identical to the existing NSI CS control plane of trust allowing for reuse of existing peering arrangements.

The DDS document space consists of a set of DDS severs that are allowed to connect to each other through a prearranged administrative agreement

- The DDS uses Client Authenticated TLS as a transport protocol to ensure the integrity and confidentiality of the messages traveling through the document space.
- DDS servers will mutually authenticate each other using X.509 certificates.
- All traffic between two peering DDS servers will be encrypted while in transit.

The DDS document space security model is based on transitive trust: I trust my peers and the peers they trust.

A DDS server is contractually obligated to participate in correct operation of the protocol.

Security (continued)

A group of DDS servers that form a document space will be self-regulating.

Misbehaving DDS servers will be called to account by the community, and in the worst case the offending server will be removed from the document space.

There are no automated mechanisms for removing a DDS sever deemed to be “misbehaving”.

A DDS client will connect to the document space using either Client Authenticated TLS, or a locally chosen mechanism deemed to be equally secure.

Document validation

Mechanisms for proving the correctness or validation of a document can be added on top of the document space as needed (i.e. Document Validation Service)

- A single mechanism supporting all documents could be provided, or perhaps one that is specific to document type, or even a per NSA solution.
- These mechanism can be invoked on demand by clients when validation is required, or layered between the client and DDS server to transparently validate documents.

Validation of XML documents can be done using standard XML digital signatures, either including the digital signature within the document itself (enveloped), or separately in the provided meta-data signature field.

User specific views

The DDS protocol itself does not have the concept of a user specific view, however, NSA are free to publish additional documents as needed, using the meta-data envelope to uniquely distinguish (and identify) each document.

For example, the ESnet uPA may publish two views of the same topology, one for mass consumption and one for the LHCONE user community

- These topologies would be rooted under the same NSA identifier and document type, but would have different topology identifiers: one for the masses, and one for the LHCONE community.

  /urn:ogf:network:es.net:2013:nsa/vnd.ogf.nsi.topology.v2+xml/

  urn:ogf:network:es.net:2013:

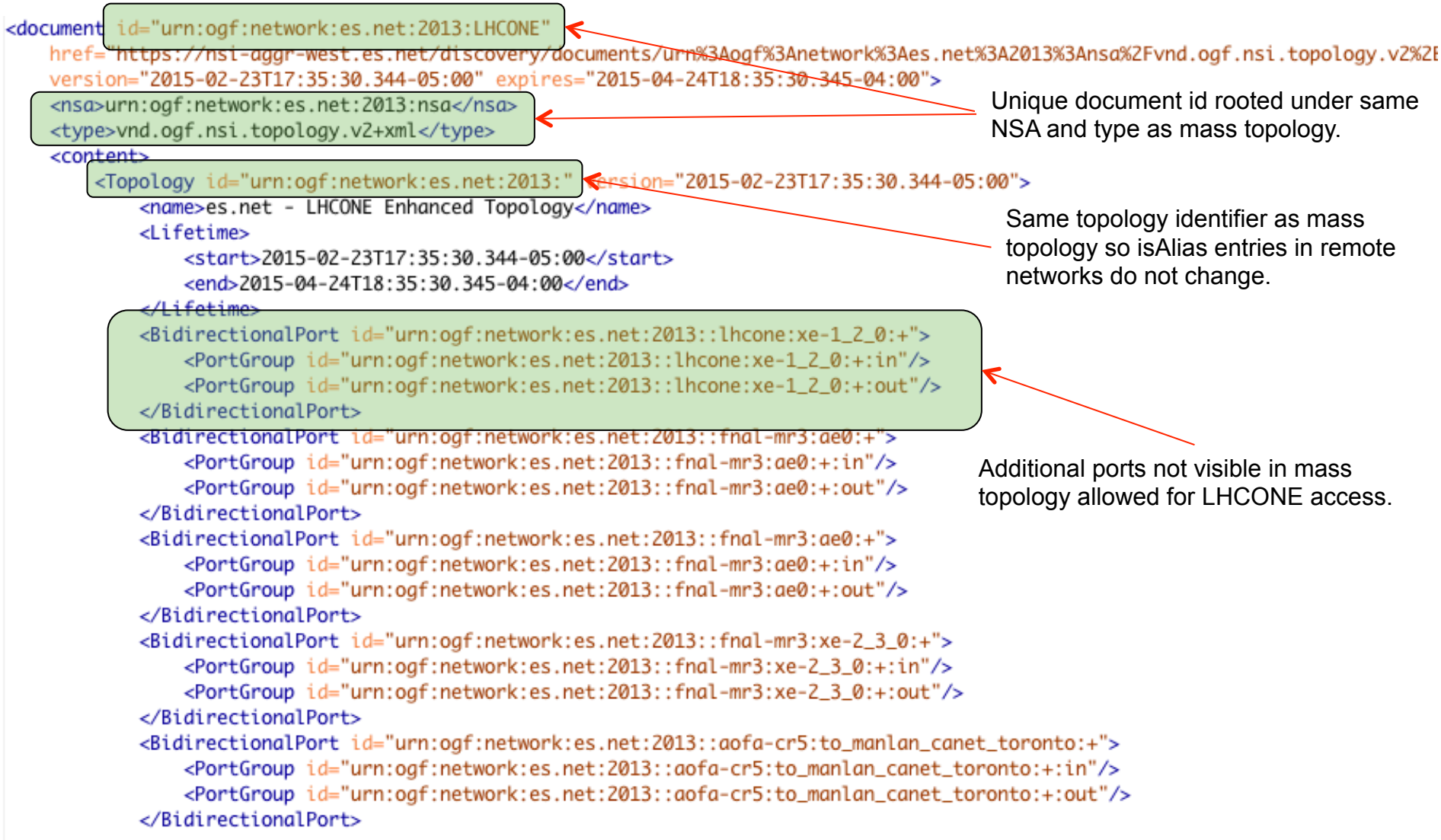
  urn:ogf:network:es.net:2013:LHCONE
- The contents of the LHCONE specific topology document does not have to contain the “urn:ogf:network:es.net:2013:LHCONE” topology identifier, but could be a specific view of the “urn:ogf:network:es.net:2013:” topology.

Privacy for special documents can be achieved through public key encryption of the document contents, independent of the document meta-data.

Document for the masses

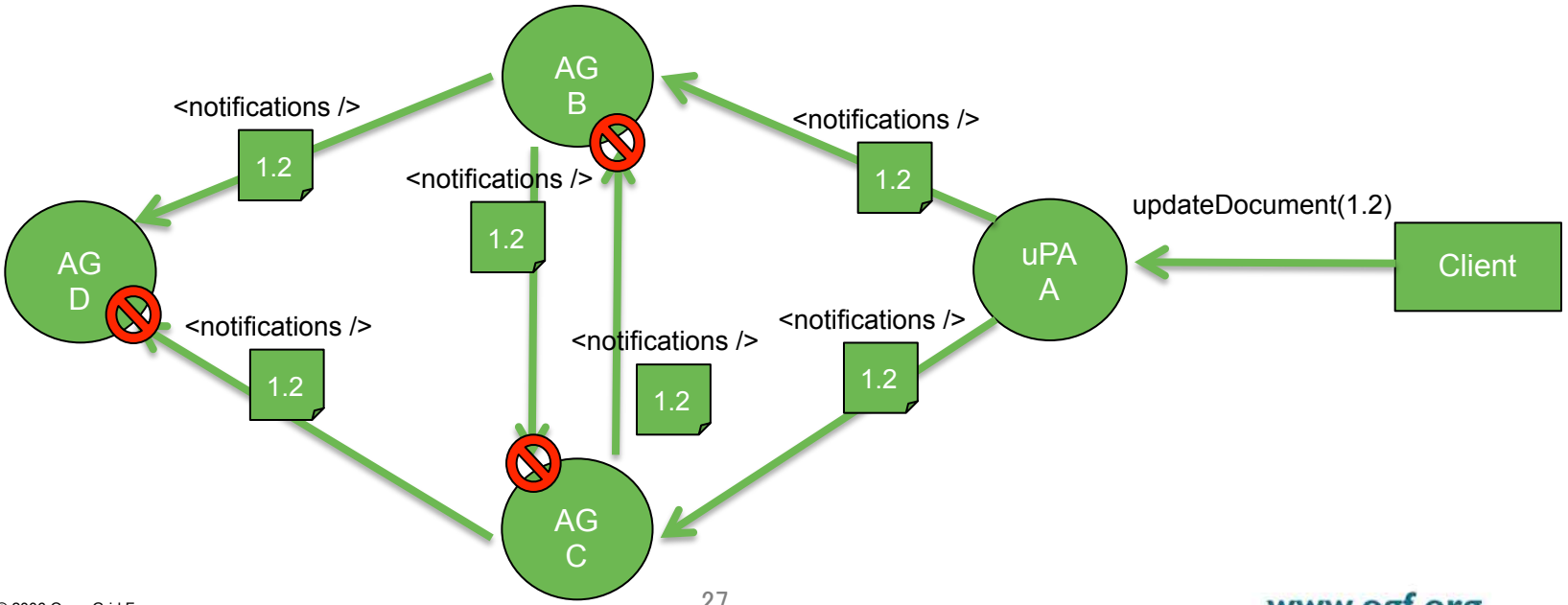

```
<document id="urn:ogf:network:es.net:2013:"
    href="https://nsi-aggr-west.es.net/discovery/documents/urn%3Aogf%3Anetwork%3Aes.net%3A2013%3Ansa/vnd.ogf.nsi.topology.v2%
    version="2015-02-23T17:35:30.344-05:00" expires="2015-04-24T18:35:30.345-04:00">
    <nsa>urn:ogf:network:es.net:2013:nsa</nsa>
    <type>vnd.ogf.nsi.topology.v2+xml</type>
    <content>
        <Topology id="urn:ogf:network:es.net:2013:" version="2015-02-23T17:35:30.344-05:00">
            <name>es.net</name>
            <Lifetime>
                <start>2015-02-23T17:35:30.344-05:00</start>
                <end>2015-04-24T18:35:30.345-04:00</end>
            </Lifetime>
            <BidirectionalPort id="urn:ogf:network:es.net:2013::fnal-mr3:ae0:+">
                <PortGroup id="urn:ogf:network:es.net:2013::fnal-mr3:ae0:+:in"/>
                <PortGroup id="urn:ogf:network:es.net:2013::fnal-mr3:ae0:+:out"/>
            </BidirectionalPort>
            <BidirectionalPort id="urn:ogf:network:es.net:2013::fnal-mr3:xe-2_3_0:+">
                <PortGroup id="urn:ogf:network:es.net:2013::fnal-mr3:xe-2_3_0:+:in"/>
                <PortGroup id="urn:ogf:network:es.net:2013::fnal-mr3:xe-2_3_0:+:out"/>
            </BidirectionalPort>
            <BidirectionalPort id="urn:ogf:network:es.net:2013::aofa-cr5:to_manlan_canet_toronto:+">
                <PortGroup id="urn:ogf:network:es.net:2013::aofa-cr5:to_manlan_canet_toronto:+:in"/>
                <PortGroup id="urn:ogf:network:es.net:2013::aofa-cr5:to_manlan_canet_toronto:+:out"/>
            </BidirectionalPort>
            <BidirectionalPort id="urn:ogf:network:es.net:2013::bnl-mr2:xe-4_2_0:+">
                <PortGroup id="urn:ogf:network:es.net:2013::bnl-mr2:xe-4_2_0:+:in"/>
                <PortGroup id="urn:ogf:network:es.net:2013::bnl-mr2:xe-4_2_0:+:out"/>
            </BidirectionalPort>
```

Example user specific view



Redundancy/Resiliency

- Each DDS server has a complete view of the document space allowing any DDS to act as a document source for NSA, path finders, and other clients.
- Publish, pull, and notification mechanisms all allow a uPA to act as a source to multiple DDS servers, protecting against the failure of a single DDS server.
- A redundantly connected peering model (loose mesh) will allow for document space connectivity protection in the event of DDS server failure.



Resource Model

Resource	Methods	Description
collection	GET	This root resource contains a collection of zero or more subscriptions and documents held within the NSA.
subscriptions	GET, POST	This resource represents a group of zero or more subscription instances.
subscription	GET, PUT, DELETE	This resource represents a single subscription instance.
documents	GET, POST	This resource represents a group of zero or more document instances.
document	GET, PUT, DELETE	This resource represents a single document instance.
local	GET	This resource represents a group of zero or more document instances associated with the local NSA.

URI definitions

Resource	URI	Description
collection	/	Using root URI with a GET operation will return a collection of zero or more subscriptions and documents held within the NSA.
subscriptions	/subscriptions	Using this URI with a GET operation will return a group of zero or more subscription instances. Using this URI with a POST operation will create a new subscription with the supplied criteria.
subscription	/subscriptions/{subscriptionId}	Use this URI template to access a single subscription instance based on subscription identifier. Using a GET operation will get the subscription identified by {*subscriptionId}*. Using a PUT operation will update the subscription identified by *{subscriptionId*} with the values supplied in the PUT body (*subscriptionRequest* element). Using a DELETE operation will remove the subscription identified by {*subscriptionId}*.

URI definitions

documents	/documents	Using this URI with a GET operation will return a group of zero or more document instances. Using this URI with a POST operation will create a new document with the supplied values (*document* element).
documents	/documents/{nsaId}	Use this URI template to access a list of document instances associated with an NSA identifier. Using this URI with a GET operation will return a group of zero or more document instances associated with the NSA identified by {*nsaId}*.
documents	/documents/{nsaId}/{type}	Use this URI template to access a list of document instances associated with an NSA identifier and specific document type. Using this URI with a GET operation will return a group of zero or more document instances of the document type *{type}* associated with the NSA identified by {*nsaId}.*

URI definitions

document	/documents/{nsaId}/{type}/{id}	Use this URI template to access a single document instance associated with an NSA identifier, document type, and document identifier. Using this URI with a GET operation will return a single document instance (*document* element) associated with the document identifier *{id},* the type *{type}, and* the NSA identified by {*nsaId}.* Using a PUT operation will update the document identified by *{id}* with the values supplied in the PUT body (*document* element). This can only be done by an authorized entity. Using a DELETE operation will remove the document identified by {*Id}*. This can only be done by an authorized entity.
local	/local	Using this URI with a GET operation will return a group of zero or more document instances associated with the local NSA.

Numbers

Document	Uncompressed	Compressed
NSA Discovery	5 KB	2 KB
NML Topology (1,000 ports)	1.5 MB	85 KB
NML Topology (300 ports)	450 KB	26 KB

Global network size	Combined sizes (uncompressed)	Combined sizes (compressed)
10,000 networks	14.6 GB	850 MB
5,000 networks	7.3 GB	425 MB
1,000 networks	1.5 GB	85 MB
500 networks	750 MB	42 MB

Global network size	Combined sizes (uncompressed)	Combined sizes (compressed)
10,000 networks	4.3 GB	273 MB
5,000 networks	2.2 GB	137 MB
1,000 networks	444 MB	27 MB
500 networks	222 MB	14 MB

THE END