ESnet

ENERGY SCIENCES NETWORK

OGF NSI

Chin Guok, ESnet

Lawrence Berkeley National Laboratory

14th Global LambdaGrid Workshop

Queenstown, New Zealand

October 1st, 2014

U.S. DEPARTMENT OF ENERGY

Office of Science

BERKELEY LAB

GLIF NSI Implementation Update

John MacAuley, Chin Guok

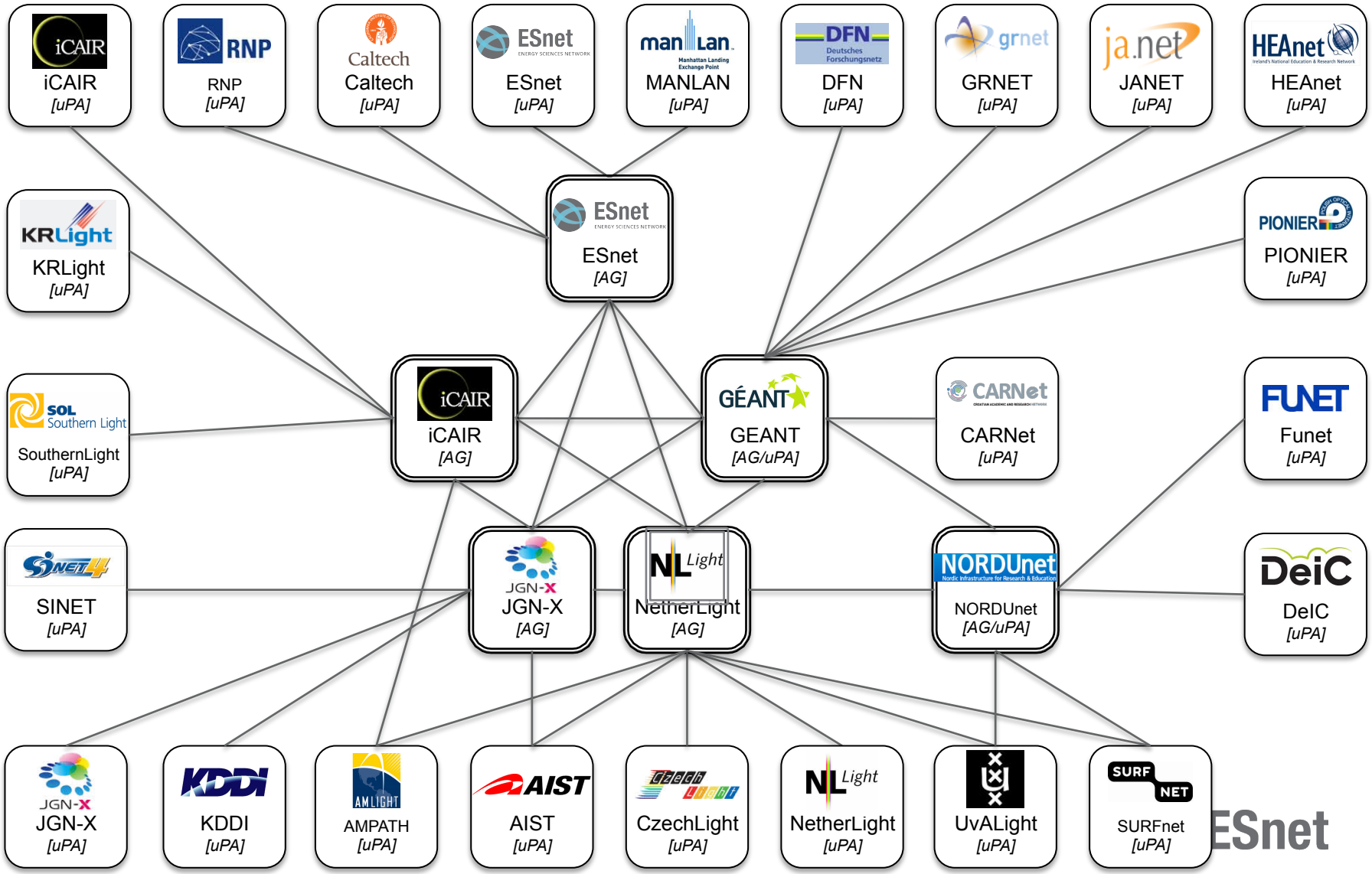
Contributions back into the OGF NSI-WG

- Collection of feedback for errata to NSI CSv2 specification as issues discovered during implementation.
- Requirements gathering and creation of the NSA Description Document.
- Defined NSI use of NML SwitchingService with both default and wildcard support for NSI Service Domains.

- Consistent connection reservation lifecycle (proper handling of terminate and dataPlaneStateChange messages).
- Proper population of protocol error messages for consistent error handling.
- Definition and consensus on new error messages as needed.

ESnet

Protocol Testing (using AGOLE)



Control plane testing

Control Plane: Testing implementation of two-way TLS and NSI-CSv2.0R117

		TO							
		AutoBAHN	*DynamicKL*	*G-lambda/A (PA)*	*G-lambda/K*	*OpenNSA*	*OSCARS*	*SURFnet BoD*	nsi-safnari
FROM	*AutoBAHN*	X							
	DynamicKL		X				X		
	G-lambda/A			X			X		
	G-lambda/K				X		X		
	OpenNSA					X	X		
	OSCARS		X	X	X	X	X	X	
	SURFnet BoD						X		
	nsi-safnari								
	nsi-requester								
	G-lambda/A (Aggr)								

	NSI-CSv2-R117 & Two-way TLS OK
	Two-way TLS OK
	NSI-CSv2-R117 OK
	Started testing
	Found errors/On-Hold
	Not started testing

ESnet

Data plane testing

Data Plane: Testing implementation of two-way TLS and NSI-CSv2.0R117

(!) Please see Result table below

		TO																			
		AIST	AMPATH	CESNET	ESnet	GEANT	GRnet	Interne	JGN-X	KDDI	KISTI	MANLA	Nether	NORDU	PSNC	RNP	SINET	StarLig	Southe	SURFnet	UvA	Funet
FROM	AIST	X																				
	AMPATH		X																			
	CESNET			X																		
	ESnet				X																	
	GEANT					X																
	GRnet						X															
	Internet2							X														
	JGN-X								X													
	KDDI									X												
	KISTI										X											
	MANLAN											X										
	NetherLight												X									
	NORDUnet													X								
	PSNC														X							
	RNP															X						
	SINET																X					
	StarLight																	X				
	SouthernLight																		X			
	SURFnet																			X		
	UvA												1781 w	1781 worked						1781 Could	X	
	Funet																					

	Data plane fully working (ping succesful)
	Not sure if data plane is working (control plane works, no ping yet)
	Started testing
	Found errors/On-Hold

ESnet

Short Term Tasks

- Additional formalization of serviceException generation for common NSI errors.
  - Enables common and consistent error feedback from NSAs
- Unique identification of protocol and service attributes/parameters in serviceExceptions as well as in reservation parameters.
  - To differentiate and facilitate parsing of arbitrary parameters
- Formalization of schema for Inclusion and/or Exclusion Explicit Route Object (ERO)
  - To support NSA path finding guidance
- “Intelligent Feedback” of constrains (e.g. resource contention, policy, etc)
  - To provide information to increase chances of success on subsequent requests

ESnet

OGF NSI Update

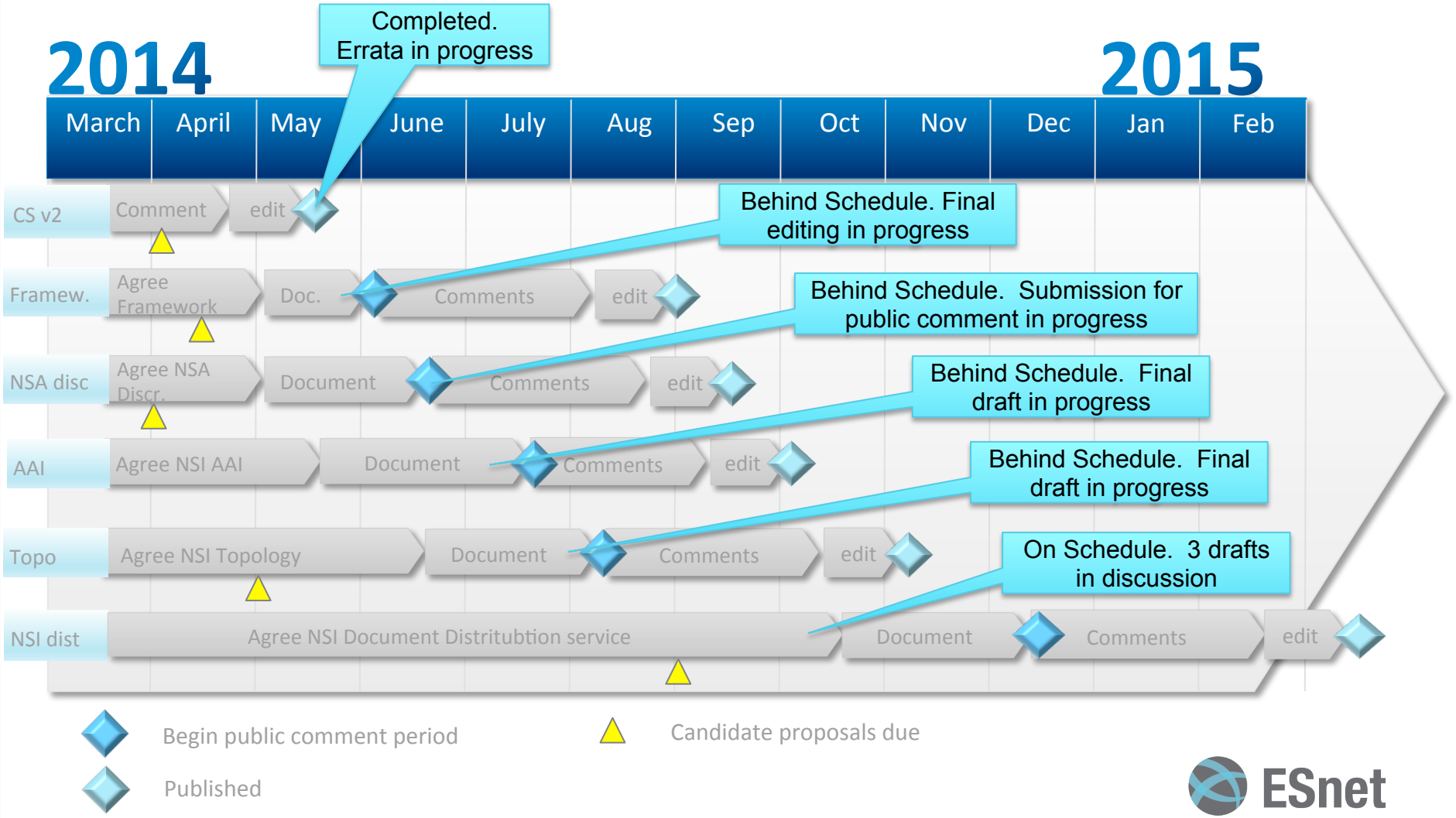
Guy Roberts, Tomohiro Kudoh, Chin Guok

NSI Documents Roadmap

- NSI Connection Service (CS) v2.0 [Standard]
  - http://www.ogf.org/documents/GFD.212.pdf
  - https://redmine.ogf.org/dmsf_files/13281?download=
- NSI Framework [Standard]
  - https://redmine.ogf.org/dmsf_files/13168?download=
  - https://redmine.ogf.org/dmsf_files/13327?download=
- NSI NSA Description Document [Standard]
  - https://redmine.ogf.org/dmsf_files/13338?download=
- NSI AAI best practices [Informational]
  - https://redmine.ogf.org/dmsf_files/13324?download=
- NSI Topology [Standard]
  - https://redmine.ogf.org/dmsf_files/12981?download=
  - https://redmine.ogf.org/dmsf_files/13254?download=
- NSI Document Distribution Service [Standard]
  - https://redmine.ogf.org/dmsf_files/13243?download=
  - https://redmine.ogf.org/dmsf_files/13323?download=

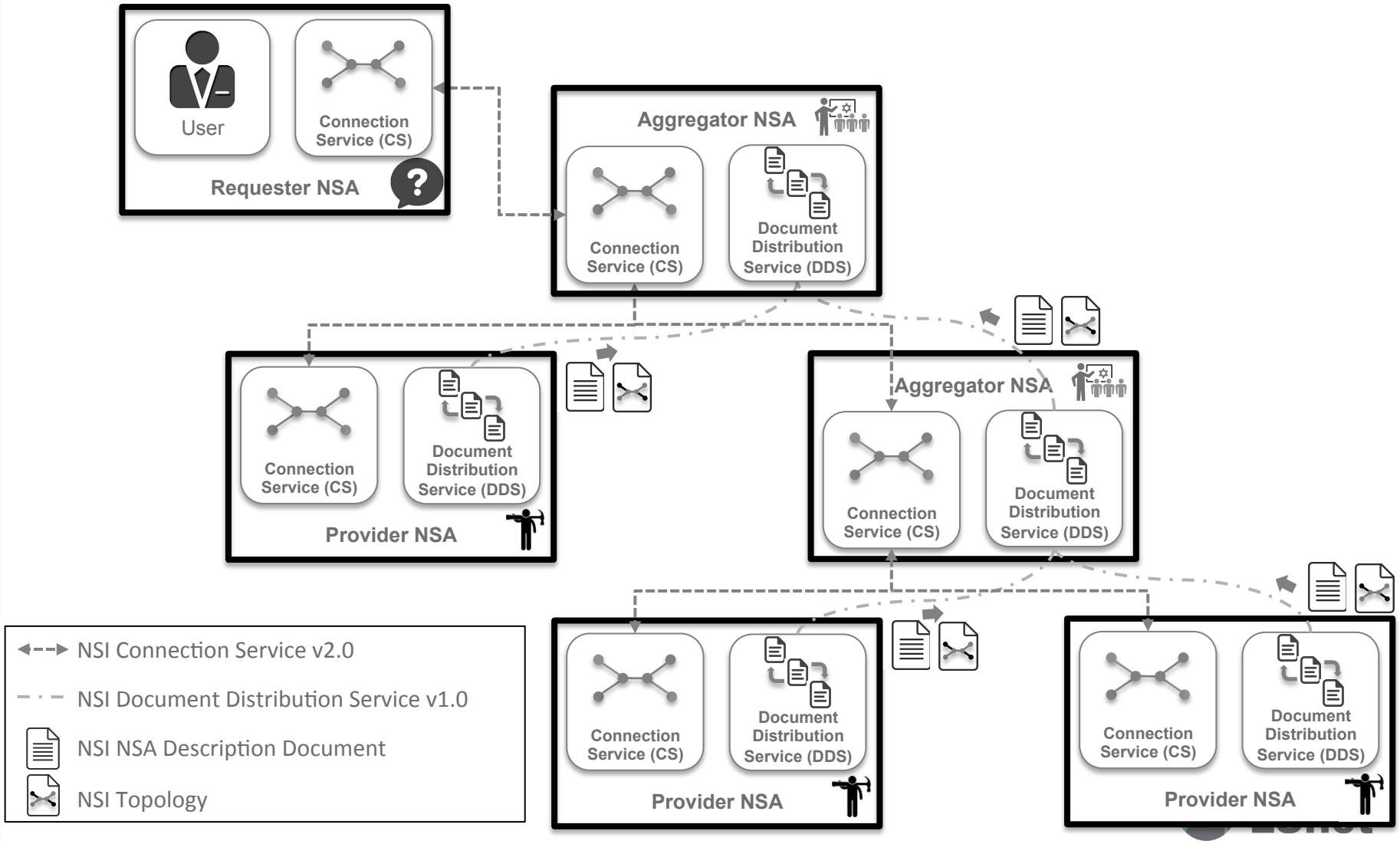
ESnet

NSI Roadmap (Intended Schedule)



ESnet

Putting it Together*



*Based on current proposals, pending alternative proposals

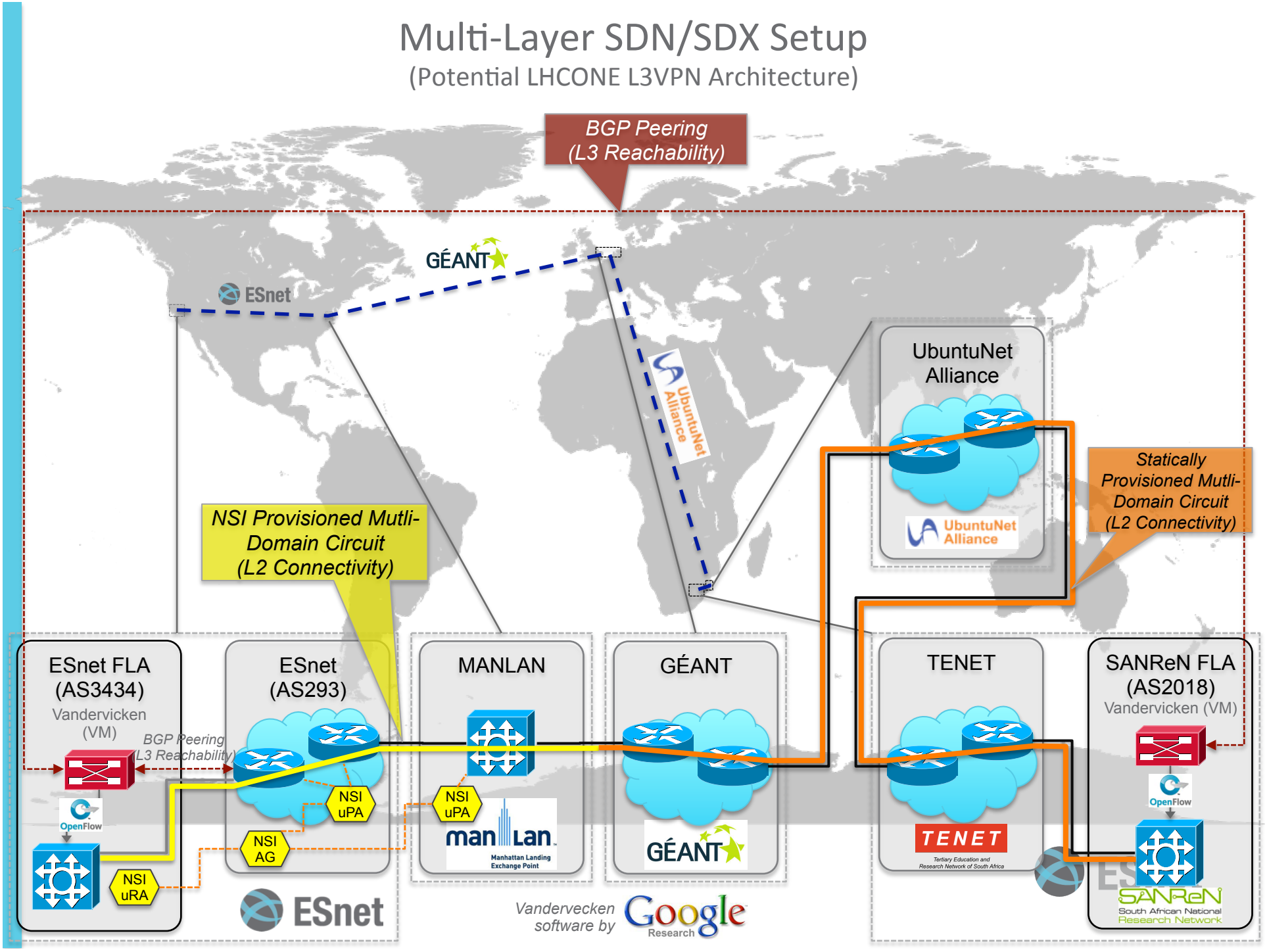
(Other) NSI Active Discussions

- Multi-Layer Topology and Path Finding
  - How to generically model adaptation/de-adaptation
  - Explore hierarchical path computation
- Policy Description and Dissemination
  - How to model simple/complex AUPs / SLAs / SLEs
  - How to scale the dissemination of context-sensitive policies (e.g. customized policies per peer/customer)
- Resource Negotiation
  - How would you negotiate for resources

ESnet

Multi-Layer SDN/SDX Setup

(Potential LHCONE L3VPN Architecture)



Questions?

ESnet

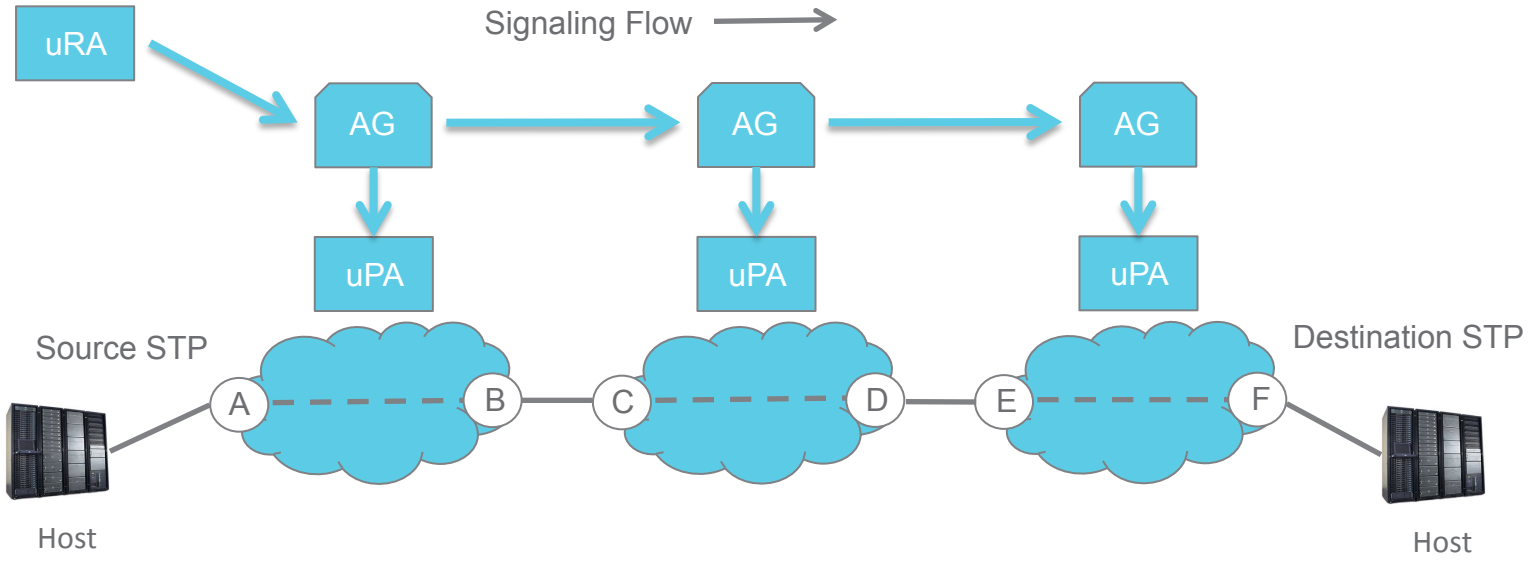
Backup Slides

NSI Values

- Complete decoupling of signaling plane from the data plane.
- Deployment of Network Service Agents with no network associations.
- Ability to perform centralized path finding with a complete view of the inter-domain topology.
- Facilitate advanced network resource workflows for network aware applications.
- Support for both tree and chain based signaling as a deployment option.

ESnet

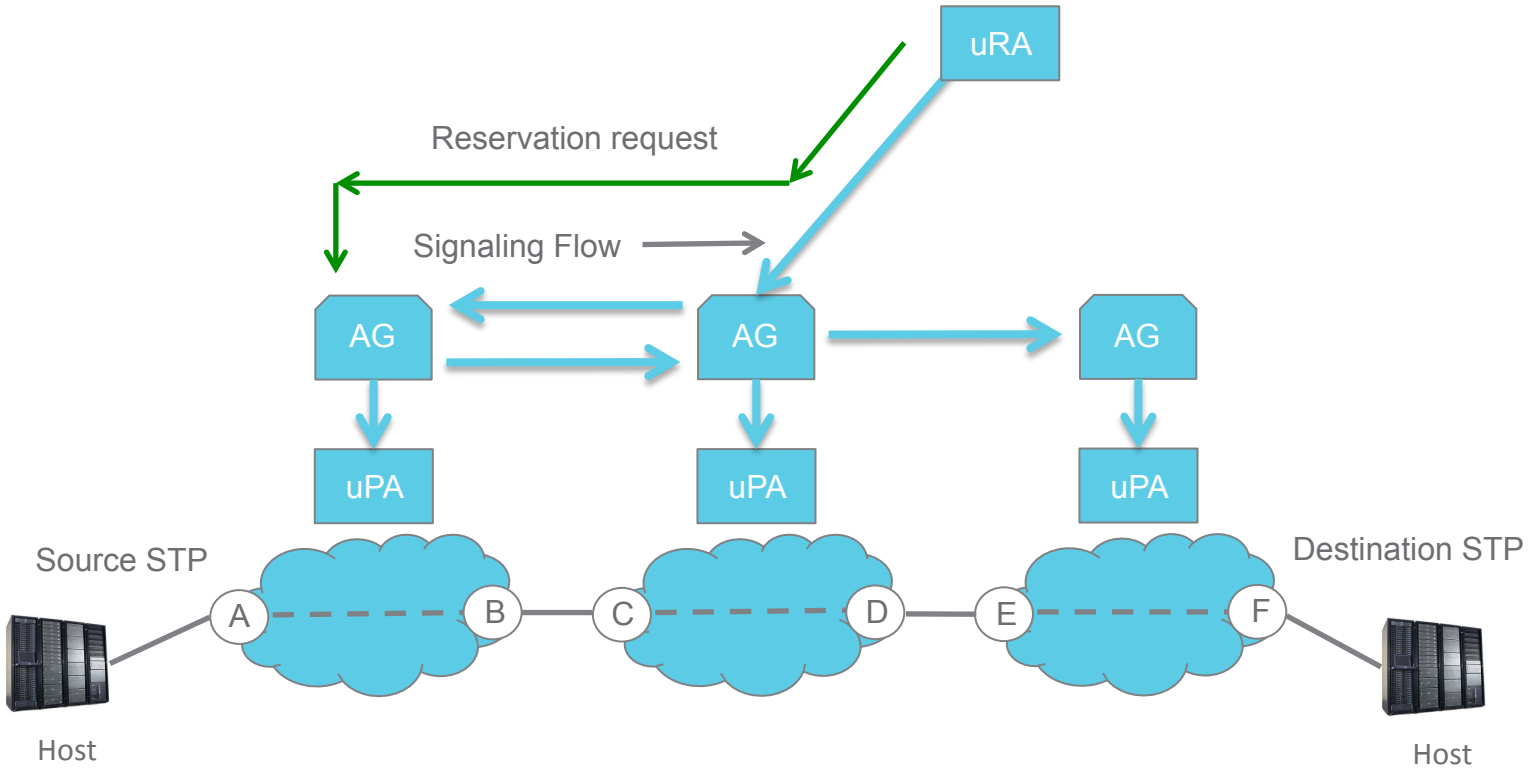
NSI Chain-based signaling model



Every NSA associated with network resources must be an Aggregator capable of propagating a reservation request to the local uPA component and at most one adjacent (child) NSA associated with the next connection segment in the data path.

ESnet

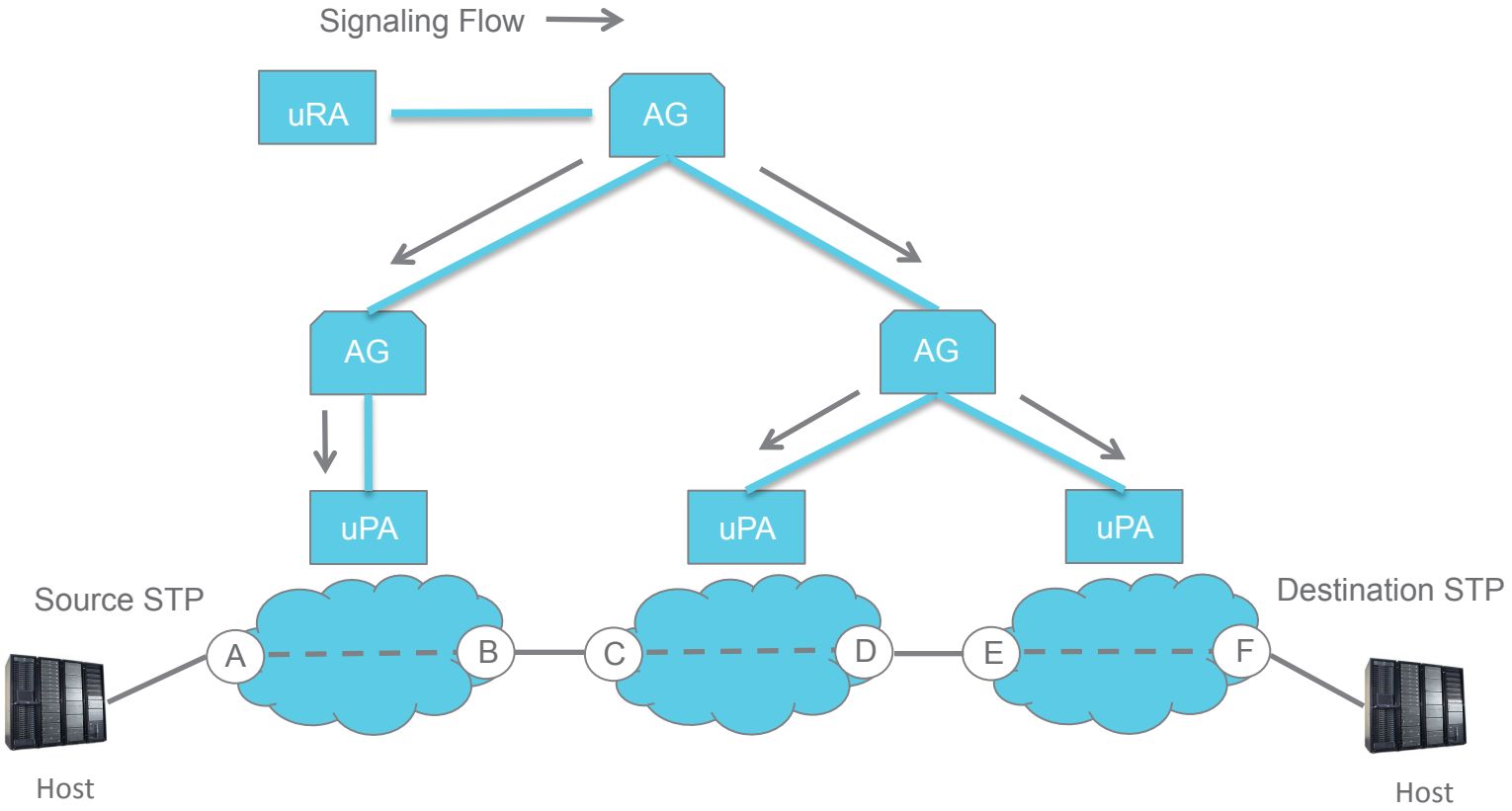
NSI Enhanced chain-based signaling model



Control plane will “forward” a reservation request to the head-end node before beginning reservation of data plane segments..

ESnet

NSI Tree-based signaling model



An Aggregator involved in a connection reservation does not have to be associated with any network resources involved in creation of that service. A uRA can issue a service request to an Aggregator NSA anywhere in the network if authorized to do so, and the NSI CS protocol with handle creating the reservation.

ESnet

GLIF AGOLE dynamic circuit addressing

AutoGOLE VLAN and IP addressing

Test hosts provisioned on allocated VLAN an IP address ranges for connectivity testing using ping and iperf.

Please see this list for L2 and L3 addressing for the AutoGOLE environment.

Layer 2: VLANs 1779-1799 will be used for the Automated GOLE on all interconnecting links.

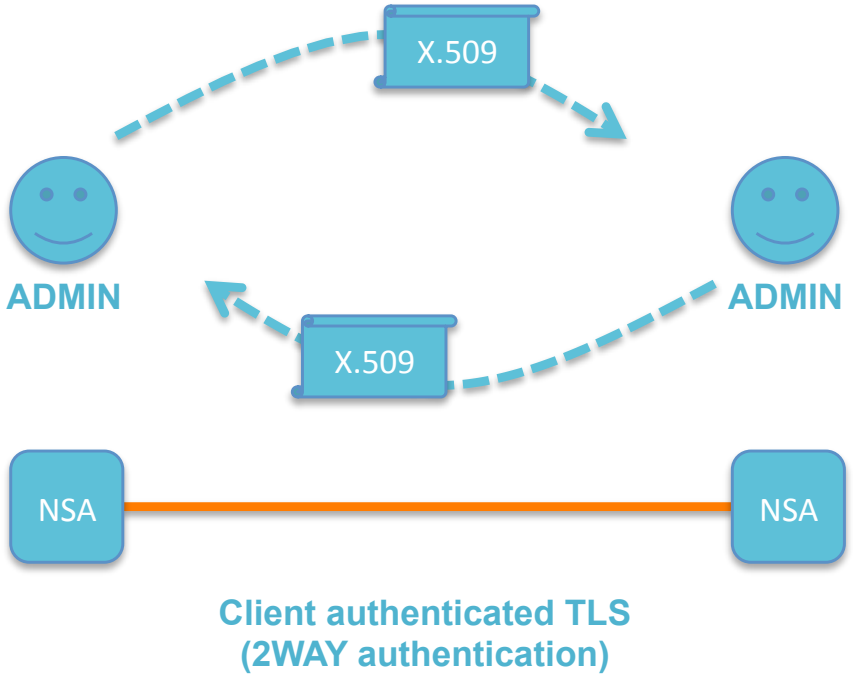
Layer 3: The AutoGOLE uses prefix 10.250.xx.yy/24 where xx are the AutoGOLE VLAN numbers 79-97 (abbreviation of full AutoGOLE VLAN range: 1779-1799) and yy is the GOLE/Network Identifier, this is assigned as below:

	IP prefix	Domain	Hostname	STPs
GOLEs & Networks	10.250.xx.1	NetherLight		
	10.250.xx.2	StarLight		
	10.250.xx.3	MAN LAN		
	10.250.xx.4	CzechLight		
	10.250.xx.5	NORDUnet		
	10.250.xx.6	CERN		
	10.250.xx.7	UvA		
	10.250.xx.8	PSNC		
	10.250.xx.9	JGN2		

ESnet

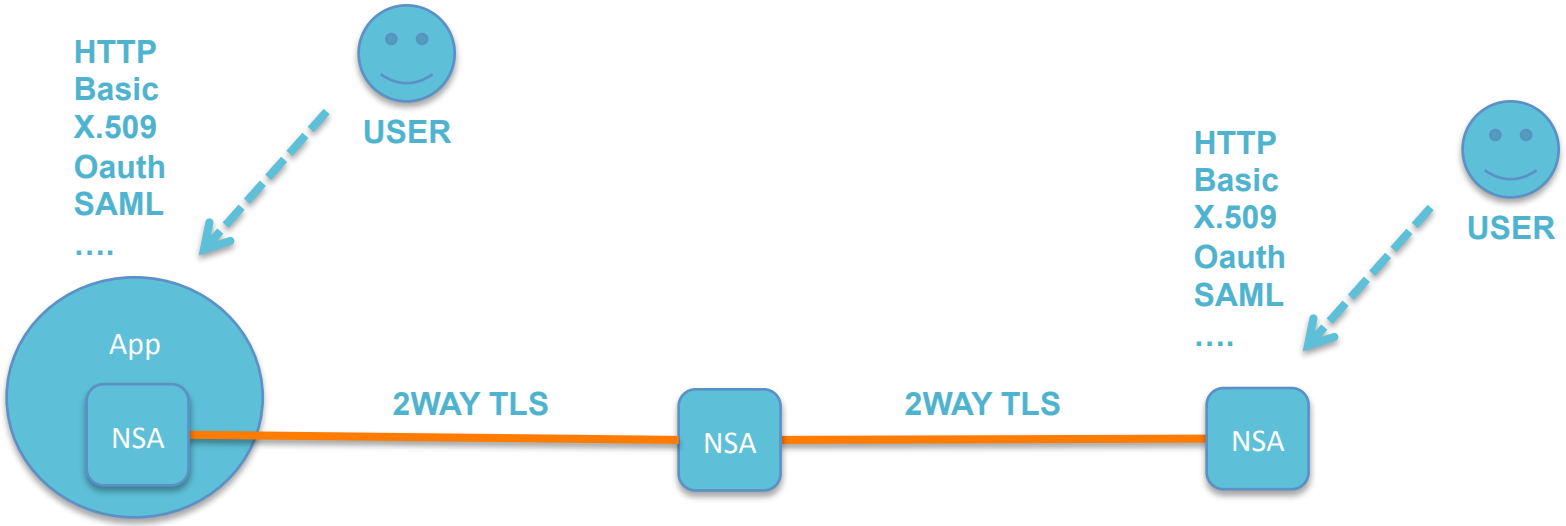
NSI AAI Control Plane of Trust

- The control plane is built up through a series of NSA peering agreements (may or may not follow data plane peering).
- Client authenticated TLS is used to authenticate peer NSA, as well as ensure the integrity and confidentiality of the messages traveling through the control plane.
- Control plane security is based on transitive trust: I trust my neighbors and the neighbors they trust.



ESnet

NSI AAI User access to control plane



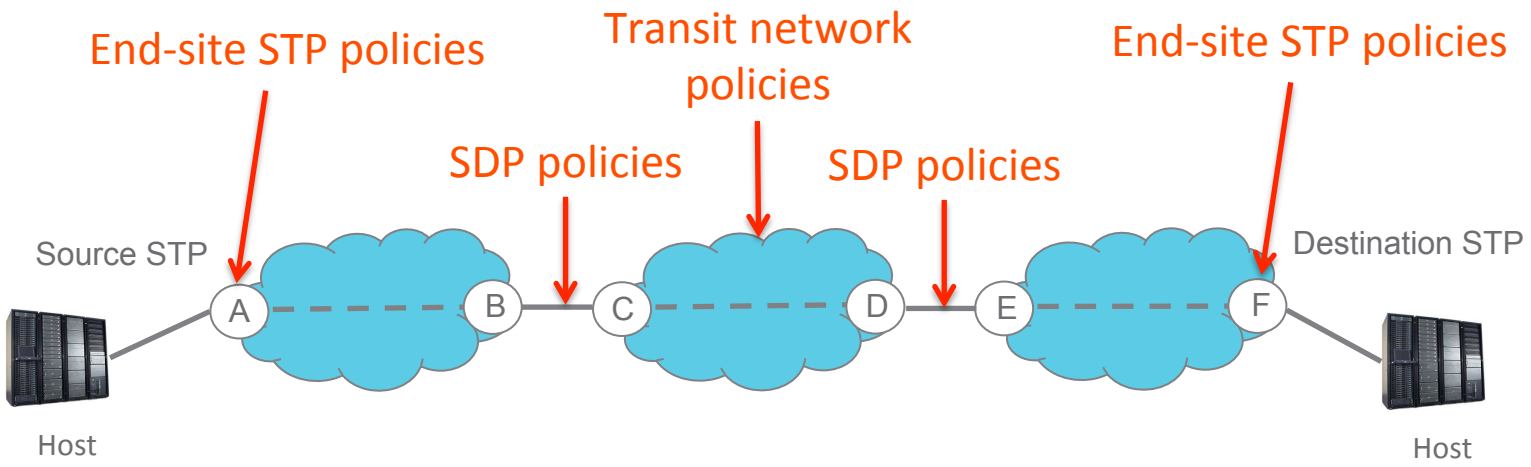
- uRA must authenticate originating user using locally defined authentication schemes.
- Identity information of the originating user can be added to the NSI message header and passed to peer NSA along with the reservation request.
- NSA along the reservation path can utilize identity information if needed for local policy enforcement.

NSI AAI Authorization policies

- Any NSA within the reservation path can do authorization on the request using local policies.
- Once in the reservation path, and NSA will receive all further messaging related to that reservation, applying additional policies as needed.
- Examples of authorization policies that could be made by an NSA include:
  - Transit policies - can the reservation transit the network?
  - Restricting STP access – can the reservation use the specified STP?
  - Bandwidth limits – is the reservation within allowable bandwidth limits.
  - Time-of-day access restrictions
  - Maximum number of reservations per day/week/year/…
  - Etc…

ESnet

NSI AAI Policy impacts on path finding



- Each uPA is ultimately responsible for enforcing any local policies on the reservation independent of any view of policy used by the path finder when choosing the path.
- End-site STP policies have minimal impact on path finding
  - An end-user is usually aware of any policies enforced on ports connected into their sites, and can provide the needed credentials.
- SDP and transit policies have a much greater impact as they are invisible to the end-user.

ESnet