Network Services Interface

Chain and Tree-based signaling

John MacAuley, ESnet

11th March 2014

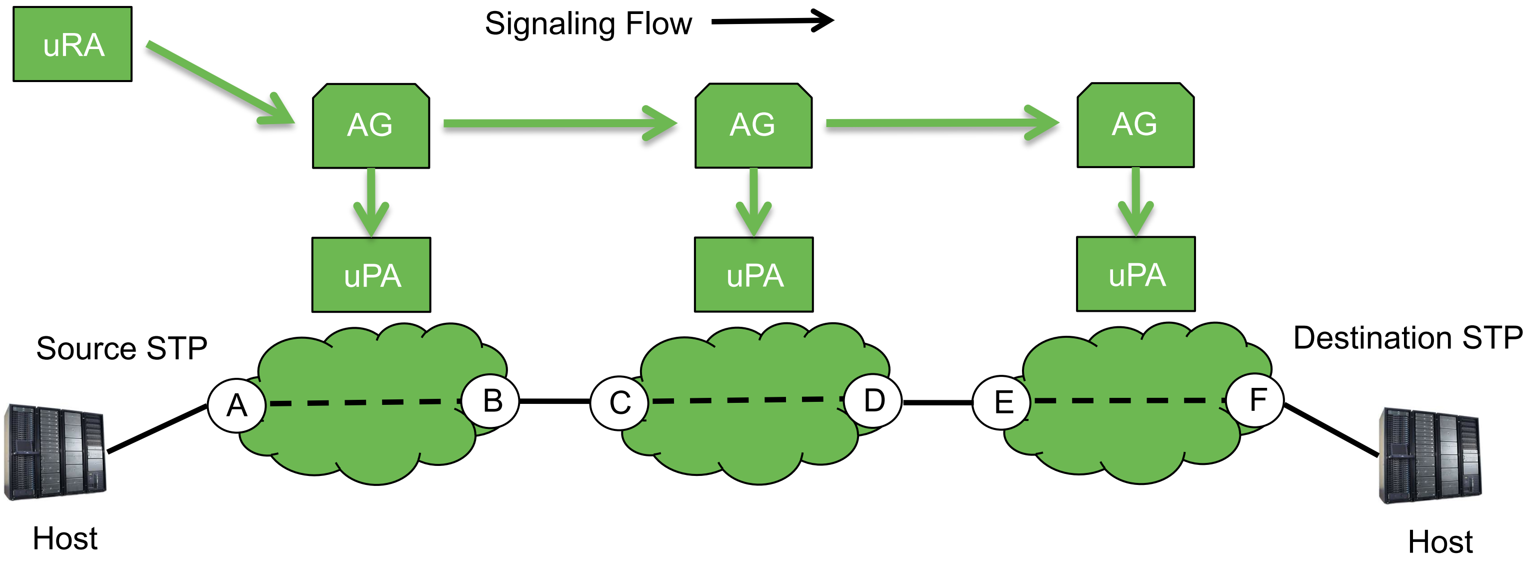
NSI Values

- Complete decoupling of the 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 where required.

Basics

- All protocols defined in the Network Services Framework must be as secure as the NSI CS 2.0 protocol
  - It is assumed that mutually authenticated TLS is a standard requirement for all NSA-to-NSA communications.
- An Aggregator NSA is restricted to communicating with only direct peer NSA based on administrative policies
  - It is assumed that an NSA administrator is not going to have a peering relationship with every other NSA in the network, and therefore, direct connectivity between every NSA is not possible.
  - As a result, the signaling plane graph is not fully connected.

Chain-based signaling model

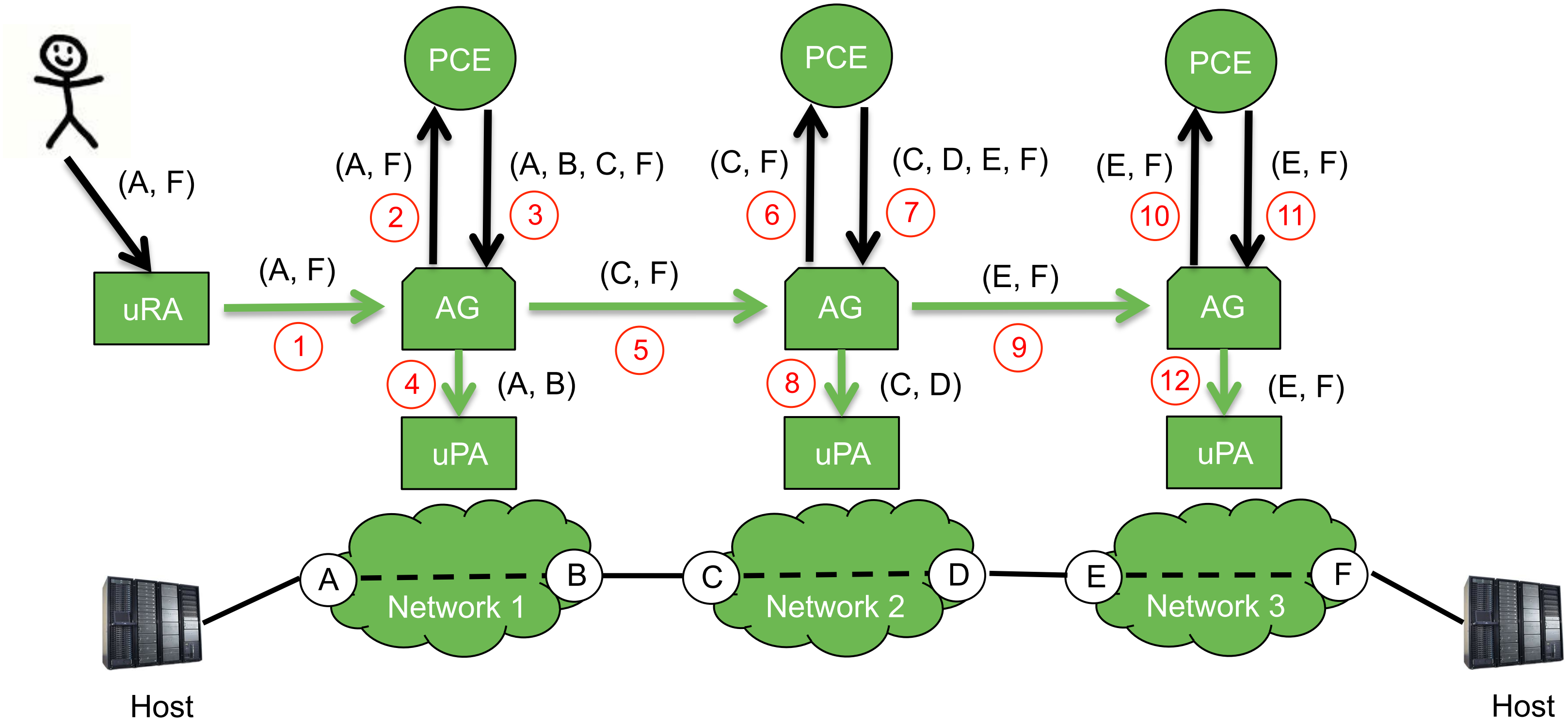


Every NSA associated with network resources must be an Aggregator capable of propagating a reservation request to the local uPA component and at most one adjacent (child) NSA associated with the next connection segment in the data path.

Initiating a request

- A connection request issued by an uRA must be to the aggregator NSA associated with the head end STP of the service.
- The service request will only be signaled in one direction, from the NSA associated with source STP through to the NSA associated with the destination STP.
- All NSA in the chain request must contain a data plane connection segment associated with the reservation request.
- An NSA in the chain must have a peering relationship with all NSA managing network resources directly connected to that NSA at the data plane.
- This implies that the signaling plane MUST be congruent with the data plane.

Hop-by-hop routing



In NSI CS 2.0 hop-by-hop routing in a chain-based solution makes a localized routing decision at each NSA along the service path while using global topology to guide next hop decisions through the data plane.

Hop-by-hop sequence

① The uRA make a reservation request to the head-end Aggregator NSA on behalf of the user to interconnect STP A to STP F. This request is made to the head-end Aggregator NSA associated with the source STP in Network 1.

② The Aggregator NSA receives the request (A, F), and after validation, performs path finding to determine which local STP should be involved in the connection reservation, and therefore, the peer NSA that will be next in the chain.

③ The Path Computation Element uses global topology to determine a loose path for the request, returning the local connection segment (A, B), and the remaining path segment in the form of two STPs: the ingress STP in the adjacent Network 2 and the original destination STP (C, F).

④ The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (A, B).

⑤ The Aggregator NSA sends a new reservation request to the next NSA (Network 2) in the chain for the remaining connection segment (C, F).

⑥ Network 2's Aggregator NSA receives the request (C, F), and after validation, performs path finding to determine which local STP should be involved in the connection reservation, and therefore, the peer NSA that will be next in the chain.

⑦ The Path Computation Element for Network 2 uses global topology to determine a loose path for the request, returning the local connection segment (C, D), and the remaining path segment in the form of two STPs: the ingress STP in adjacent Network 3 and the original destination STP (E, F).

⑧ The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (C, D).

⑨ The Aggregator NSA sends a new reservation request to the next NSA (Network 3) in the chain for the remaining connection segment (E, F).

⑩ Network 3's Aggregator NSA receives the request (E, F), and after validation, performs path finding to determine which local STP should be involved in the connection reservation.

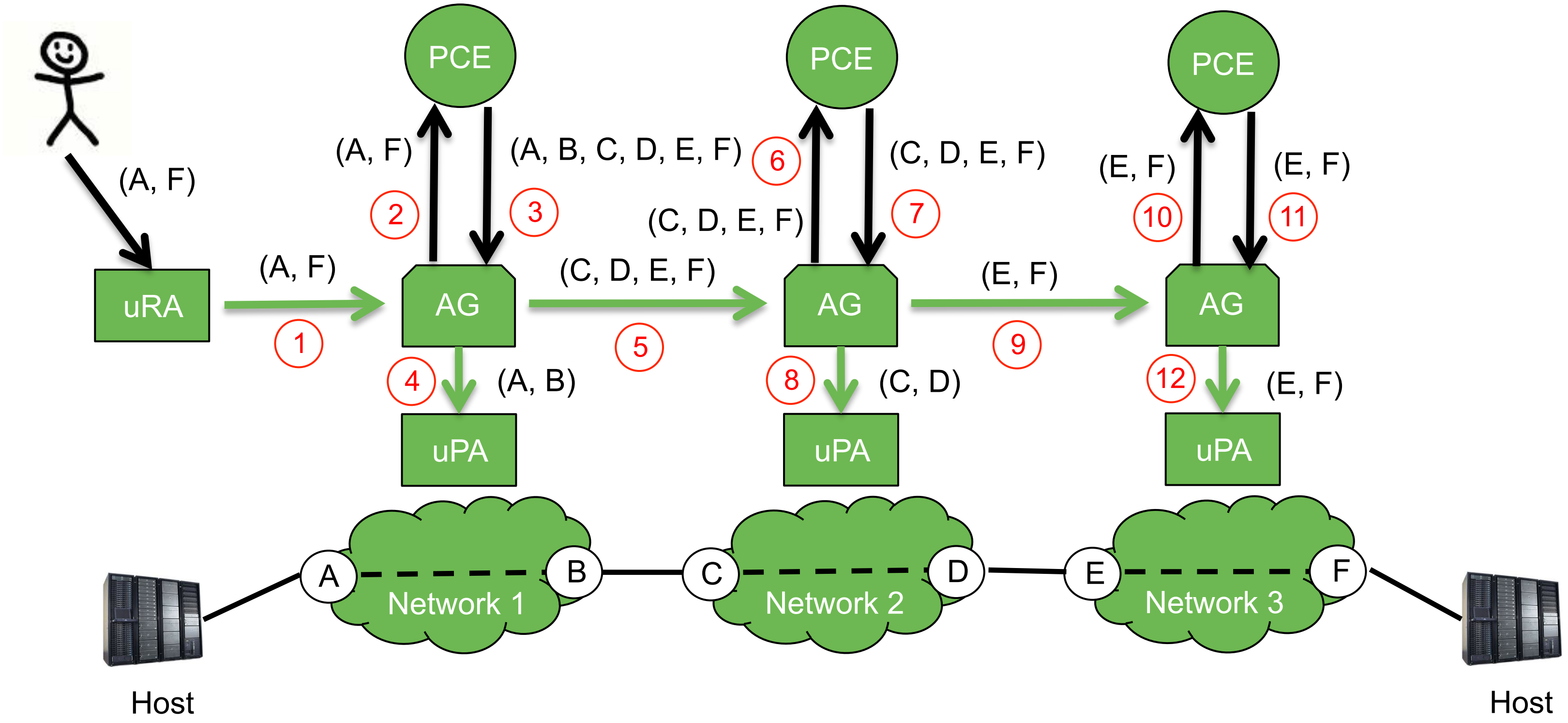
11 The Path Computation Element for Network 3 determines that both the source and destination STP are within the local domain, so returns the local connection segment (E, F). The chain is complete and no further segments are returned.

12 The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (E, F).

Required information

- NSA Discovery Documents from its directly connected peers
  - Must learn the versions of protocol interfaces available for communication.
  - Discovers adjacent networks identifiers associated with directly connected peer NSA.
- NML Topology Documents of all interconnected networks
  - A global view of topology is required for path finding to guide the path a reservation should take through the data plane, and therefore, the signaling plane.

Source Routing



Source routing is a chain-based solution where the head-end Aggregator NSA (or uRA) uses global topology to partially or completely specify a path the connection service will take through the data plane. This detailed path information is passed from NSA to NSA along signaling path using the Explicit Route Object (ERO) within the NSI CS 2.0 service request. Each NSA is bound by the ERO to follow the path segments specified during its own path finding activities. If an NSA along the path cannot meet the constraints specified in the ERO, the reservation request is rejected and an error is returned to the head-end Aggregator (or uRA) that can attempt an alternative path.

Source routing sequence

① The uRA make a reservation request to the head-end Aggregator NSA on behalf of the user to interconnect STP A to STP F. This request is made to the head-end Aggregator NSA associated with the source STP in Network 1.

② The Aggregator NSA receives the request (A, F), and after validation, performs path finding to determine an end-to-end path through the network.

③ The Path Computation Element uses global topology to determine an explicit path for the request, returning the local connection segment (A, B), and the remaining path segment in the form of a set of STP in other network to include in the service (C, D, E, F). The egress STP B from Network 1 is connected to the ingress STP C in the adjacent Network 2, and therefore, the peer NSA that will be next in the chain.

④ The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (A, B).

⑤ The Aggregator NSA sends a new reservation request to the next NSA (Network 2) in the chain for the remaining connection segments (C, D, E, F).

⑥ Network 2's Aggregator NSA receives the request (C, D, E, F), and after validation, performs path finding to determine which local STP should be involved in the connection reservation, and therefore, the peer NSA that will be next in the chain.

⑦ The Path Computation Element for Network 2 uses global topology to determine path for the request, returning the local connection segment (C, D), and the remaining path segment in the form of two STPs: the ingress STP in adjacent Network 3 and the original destination STP (E, F).

⑧ The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (C, D).

⑨ The Aggregator NSA sends a new reservation request to the next NSA (Network 3) in the chain for the remaining connection segment (E, F).

⑩ Network 3's Aggregator NSA receives the request (E, F), and after validation, performs path finding to determine which local STP should be involved in the connection reservation.

11 The Path Computation Element for Network 3 determines that both the source and destination STP are within the local domain, so returns the local connection segment (E, F). The chain is complete and no further segments are returned.

12 The Aggregator NSA makes a reservation request to the local uPA for the local connection segment (E, F).

Required information

- NSA Discovery Documents from its directly connected peers
  - Must learn the versions of protocol interfaces available for communication.
  - Discovers adjacent networks identifiers associated with directly connected peer NSA.
- NML Topology Documents of all interconnected networks
  - A global view of topology is required for path finding to guide the path a reservation should take through the data plane, and therefore, the signaling plane.

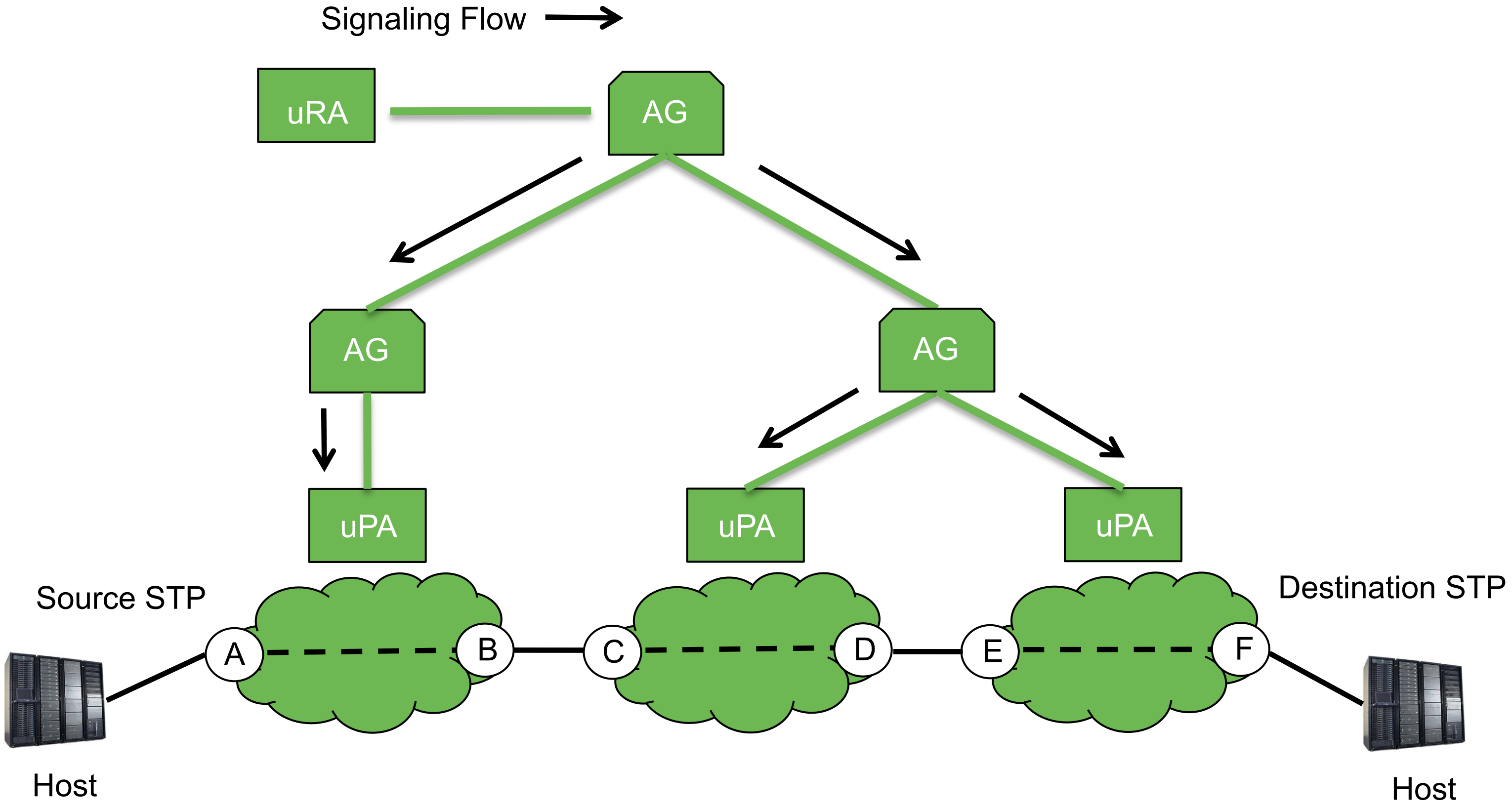
Vector routing (Not in NSI CS 2.0)

- A chain-based solution that can be deployed without a global topology view of the network if one of distance or path vector routing is employed.
- In vector routing adjacent NSA report summary route information to their own network, and to other networks reachable through them.
- In distance vector routing an NSA provides its neighbors a list of distances to networks that can be reached through it.
- In path vector routing a list of networks and ”active” paths to reach that network are provided.
- In both cases only high-level network connectivity information is related, and nothing down to the STP level. As a result, an STP identifier must be structured in such a way, as the containing network is derivable.

Required information

- NSA Discovery Documents from its directly connected peers
  - Must learn the versions of protocol interfaces available for communication.
  - Discovers adjacent networks identifiers associated with directly connected peer NSA.
  - Discovers routing vectors advertised by peer NSA so routing decisions can be made based on vector information to the network associated with the destination STP.
  - When using routing vectors a global view of topology is not required, however, NSA Discovery Documents will need to be updated and distributed anytime there is a change in network topology impacting the vector calculations.
- NML Topology Documents of peer networks only
  - Used to derive remote peering STP in these adjacent networks.
  - These STP are associated with the SDP between the local network and the remote peer's network.

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.

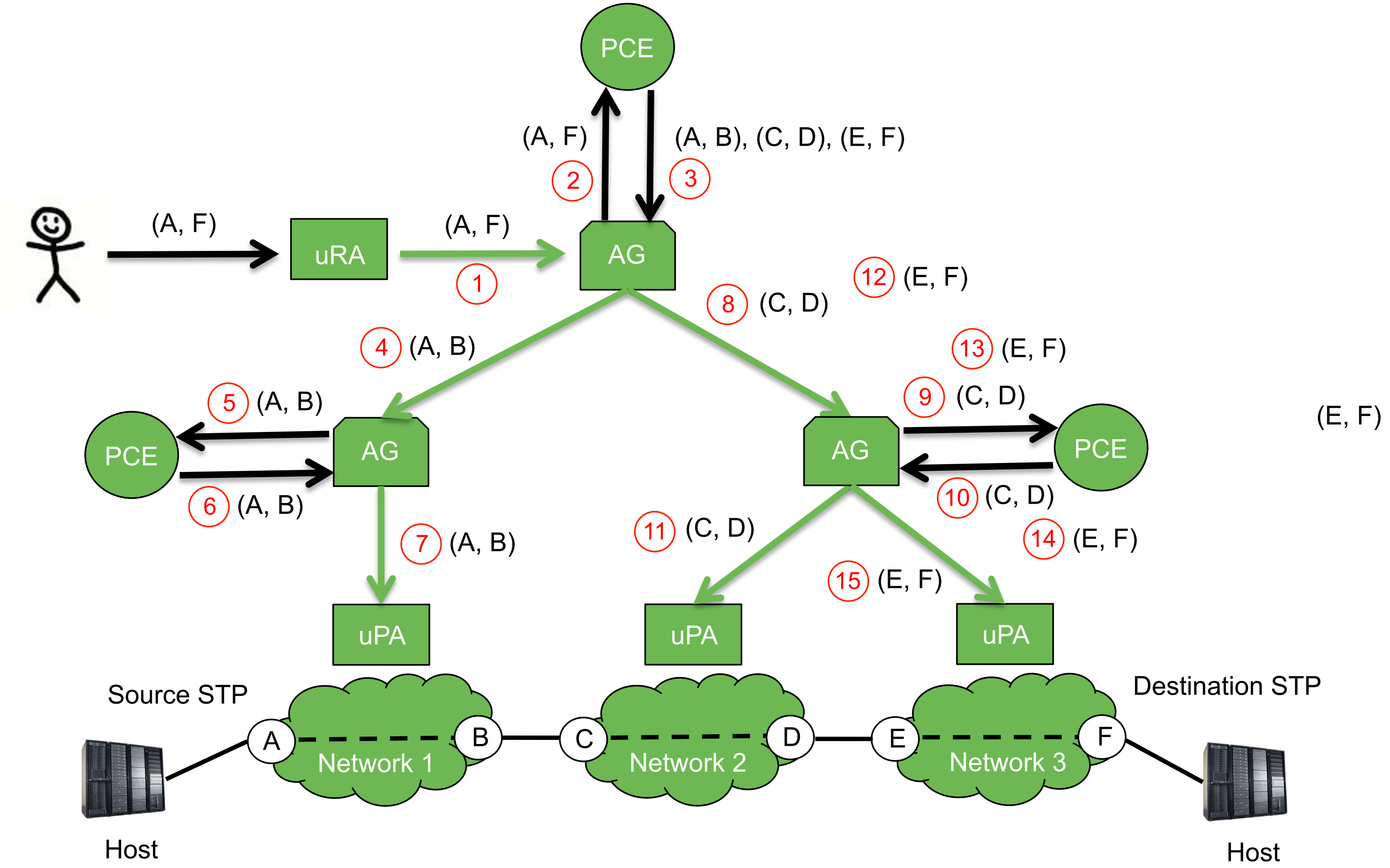
Tree-based signaling model

- A service request can be initiated to an Aggregator NSA anywhere in the network.
- An Aggregator involved in a connection reservation does not have to be associated with any network resources involved in creation of the service.
- A service request can be propagated to many NSA as it traverses the signaling tree to the individual uPA associated with connection segments.
- An NSA that propagates a connection reservation is considered part of the reservation workflow, and participates in the lifecycle of the reservation.
- An Aggregator does not need to fully resolve the connection, but can delegate the task further down the tree to other aggregators if desired.
- An Aggregator is restricted to communicating with only direct peer NSA based on local administrative policies

Required information

- Each Aggregator NSA requires NSA discovery documents for all NSA within the network:
  - Needs to know the networks managed by each NSA in the network.
  - Needs each NSA’s signaling plane topology to determine routing paths of requests in the connected signaling graph.
  - Need to know the role of each NSA in the signaling graph (Aggregator, uPA) to determine if reservation messages can be routed through the NSA to reach a peer NSA.
- The Aggregator NSA needs a full view of network topology to perform advanced "intelligent" routing decisions
  - The topology documents from each network are used to build a global topology view for routing of the connection.
  - At a minimum, the Aggregator NSA needs all the networks, the peering ports (to derive SDP), the services offered, associated service domains (SwitchingServices), and any adaptations within the network.
- An Aggregator may hide network details for child networks if desired
  - Advertises summarized network topology as needed, but the aggregator assumes public ownership of those networks.
  - The key with this model is that external NSA need not know the details of these internal child NSA.

Source routing


PCE
(A, F)
2
(A, B), (C, D), (E, F)
3
(A, F)
uRA
(A, F)
1
AG
12 (E, F)
8 (C, D)
4 (A, B)
13 (E, F)
5 (A, B)
9 (C, D)
(E, F)
PCE
AG
AG
PCE
6 (A, B)
10 (C, D)
7 (A, B)
11 (C, D)
14 (E, F)
15 (E, F)
uPA
uPA
uPA
Source STP
Destination STP
A
B
C
D
E
F
Network 1
Network 2
Network 3
Host
Host