Phosphorus-Internet2 Interoperability
GLIF 1-2 October 2008

Fred Wan

University of Amsterdam

Overview

- Problem/subject
  - Connecting Phosphorus and Internet2
  - US infrastructure: Internet2/DCN
  - EU infrastructure: Phosphorus/Harmony
    - ARGIA (UCLP-based used by I2CAT): Virtualization Network Elements
    - ARGON (Network Virtualization used in the VIOLA testbed; MPLS/GMPLS enabled)
    - DRAC (Commercial, so what’s under the hood?)
  - Goal: Create multi-domain circuits (p2p ckts) controlled by different control-planes.
  - Problem: abstract a common service interface from heterogeneous control-plane interfaces: Generic Network Interface.
  - Method: create Phosphorous-Internet2 testbed (I2CAT-UvA-I2), explore request mapping and interoperability.
- Participants:
  - University of Bonn: Alexander Willner, Christian de Waal, Jan Gassen
  - I2CAT: Joan Antoni Garcia Espin, Jordi Ferrrer Riera, Carlos Baez Ruiz
  - Internet2: John Vollbrecht, Andrew Lake

Control-plane/Service-plane separation

- NRPS
  - Control-plane vs Service-plane
  - **Control-plane**: provisioning network resources
  - Path-finding/signalling network elements, e.g., label switching, RSVP-TE, protocol adaptation (beyond the scope of GNI).
  - **Service-plane**: advance resource reservation managers/ resource access managers
  - Security, AAA, Scheduling, Policy Enforcement
- Security and QoS issues have had less priority than technical ones.

Security/AAA

- Security
  - TLS/MLS
  - Phosphorus: VPN (tinc)
  - DRAC: SSL/username-password
  - Internet2: WSS MCS (Axis)
- AAA
  - Authentication: Web access/WS signaling (WSSE)
    - Issue: is AuthN in the WS message header sufficient for AAA?
    - AuthZ info in the body?
  - Authorization: Probing resources for availability, examining existing resource schedule, matching access permission user (role)/resource
  - Multi-domain AAA: tree - vs chain model
    - Central ***or*** per domain user administration/role assignment & resource state admin?
  - AuthZ in Harmony: none
  - AuthZ in DCN: Limited number of roles

Reservations (GNI)

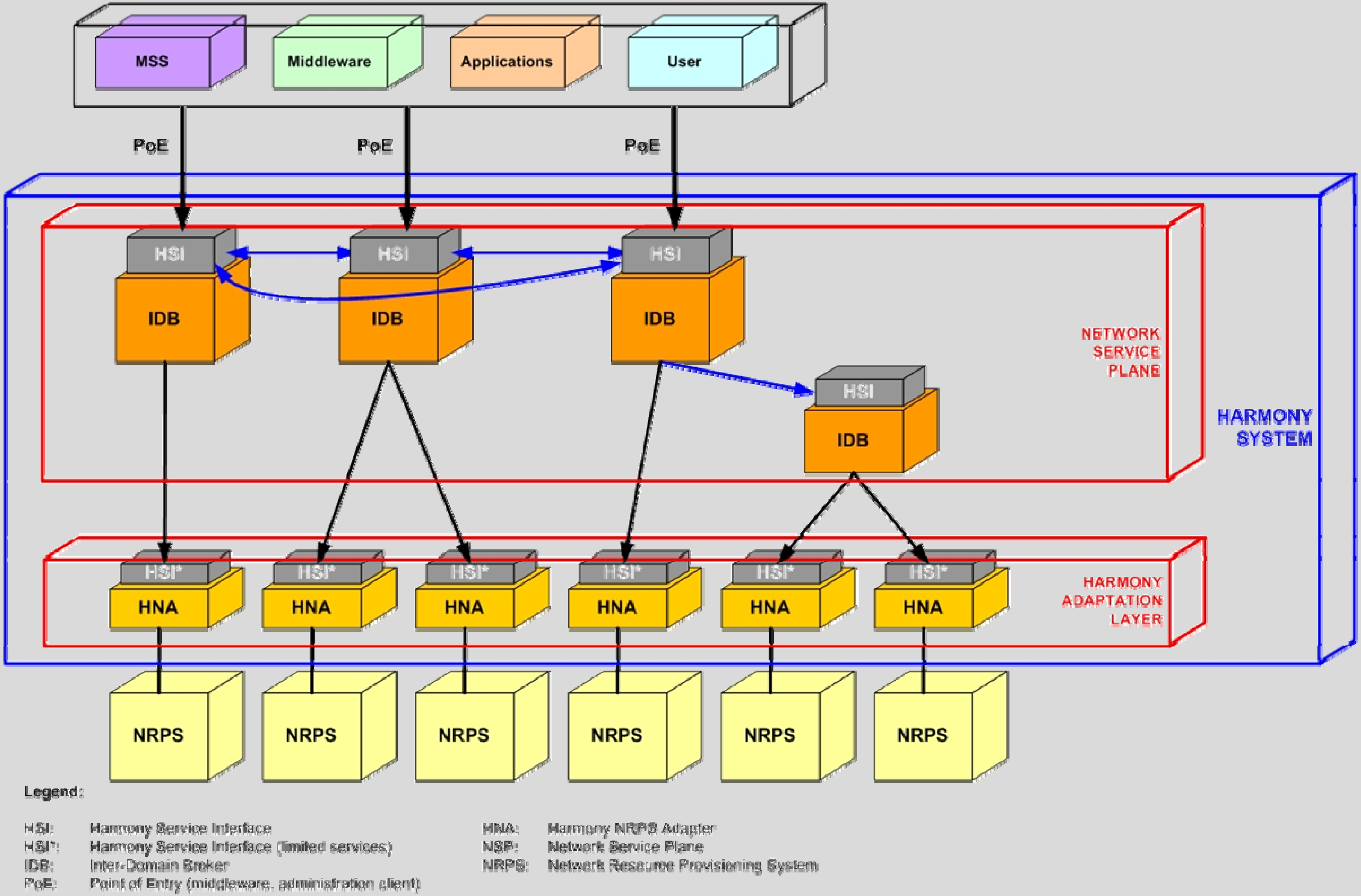
- Reservation Managers
  - What is reserved? Bandwidth? Time? Resources?
  - How? Request-Response? Reservation units fixed? Deadlines? Contiguous?
  - **Operations**:

    Create, Cancel, Modify, Delete, Query (Retrieve Info), Reschedule , Confirm
  - Reservations in Harmony/IDC: fail on first pass (fast-fail)
- Accessing reserved resources
  - Automatic activation/user signalling/policy enforcement (tokens)
  - Access mechanisms in Harmony/IDC

GNI open issues

- Issues/Discussion: GNI philosophy & Missing components
  - Resource oriented (no broad WSRF standard acceptance)
  - Minimalist approach: Simplest WSS option, no AAA
  - Only functional component: reservation service (without rescheduling).
  - No concept of an ‘owner’ of a reservation.
- Proposal:
  - Add multi-domain authz mechanism using a trusted STS, and let it issue SAML attr/authz assertions
  - Add rescheduling functionalities/reservation tracking mechanism (Subject SAML HOK Assrt = owner)
- Current Harmony/IDC IOP (I2CAT-UvA-Internet2 testbed)
  - Request translation works
  - Path setup doesn’t work yet
  - Dynamic switching doesn’t work (yet)

Harmony overview

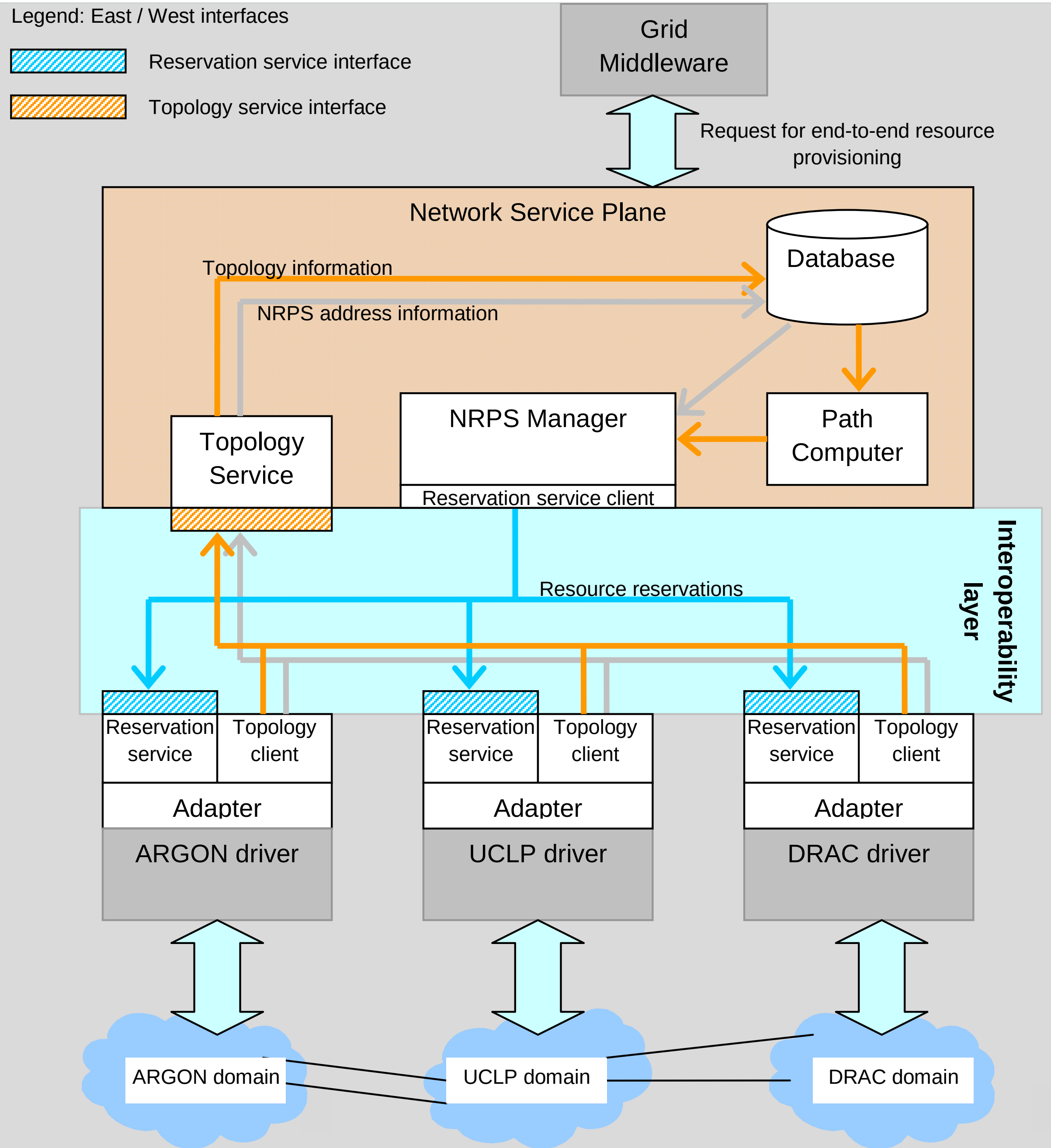


Legend:

HSI: Harmony Service Interface
HSI*: Harmony Service Interface (limited services)
IDB: Inter-Domain Broker
PoE: Point of Entry (middleware, administration client)

HNA: Harmony NRPS Adapter
NSP: Network Service Plane
NRPS: Network Resource Provisioning System

Harmony: NRPS and NSP Interfaces



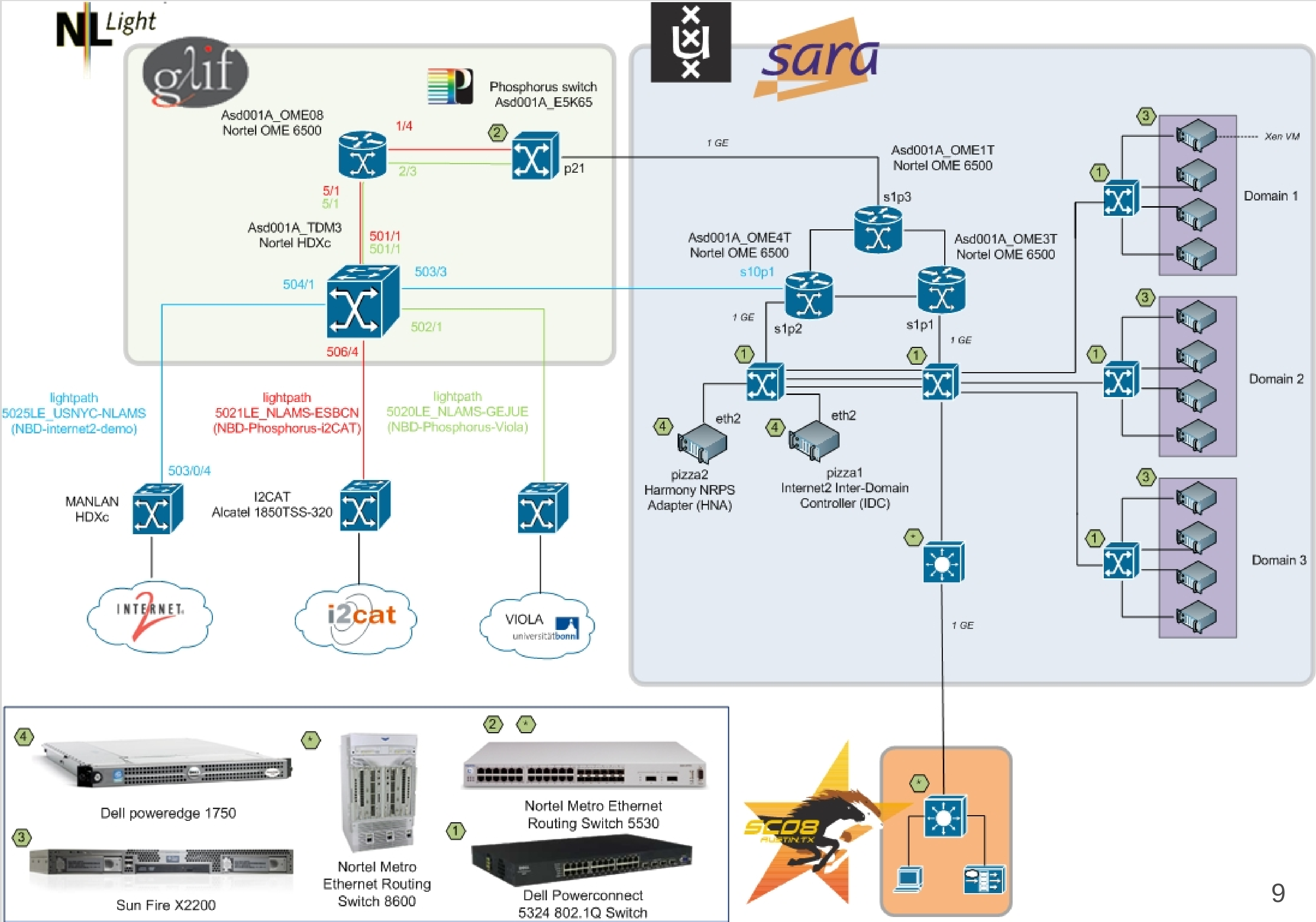
Reservation WS:

- Availability Request
- Reservation Request
- Cancel Reservation
- Status Request
- Retrieve Features
- Retrieve Endpoints

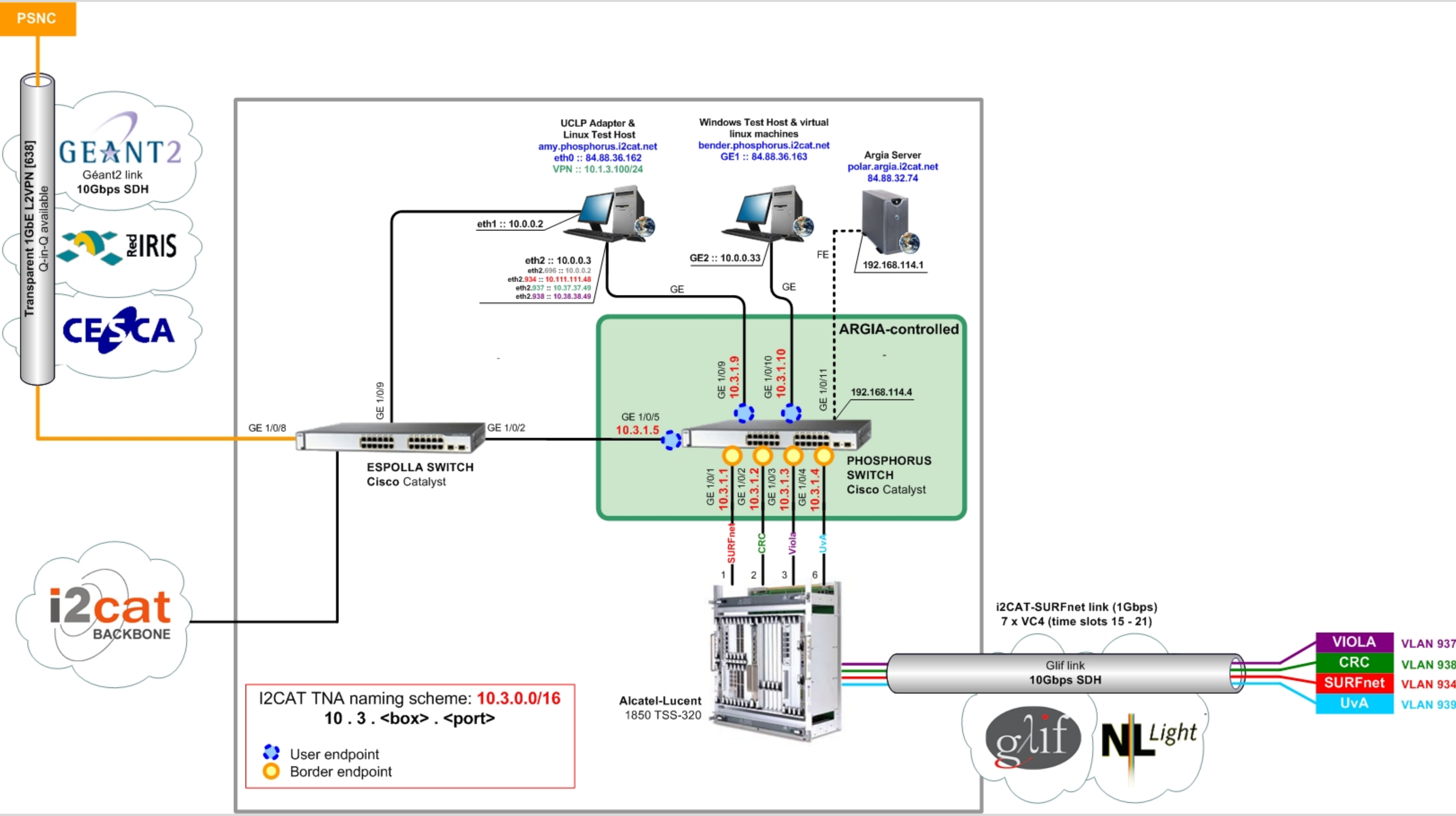
Topology WS:

- Add domain
- Delete domain
- Edit domain
- Retrieve domain
- Add Endpoints
- Delete Endpoint
- Edit Endpoints
- Retrieve Endpoints
- Add Link
- Delete Link
- Edit Link
- Retrieve Link

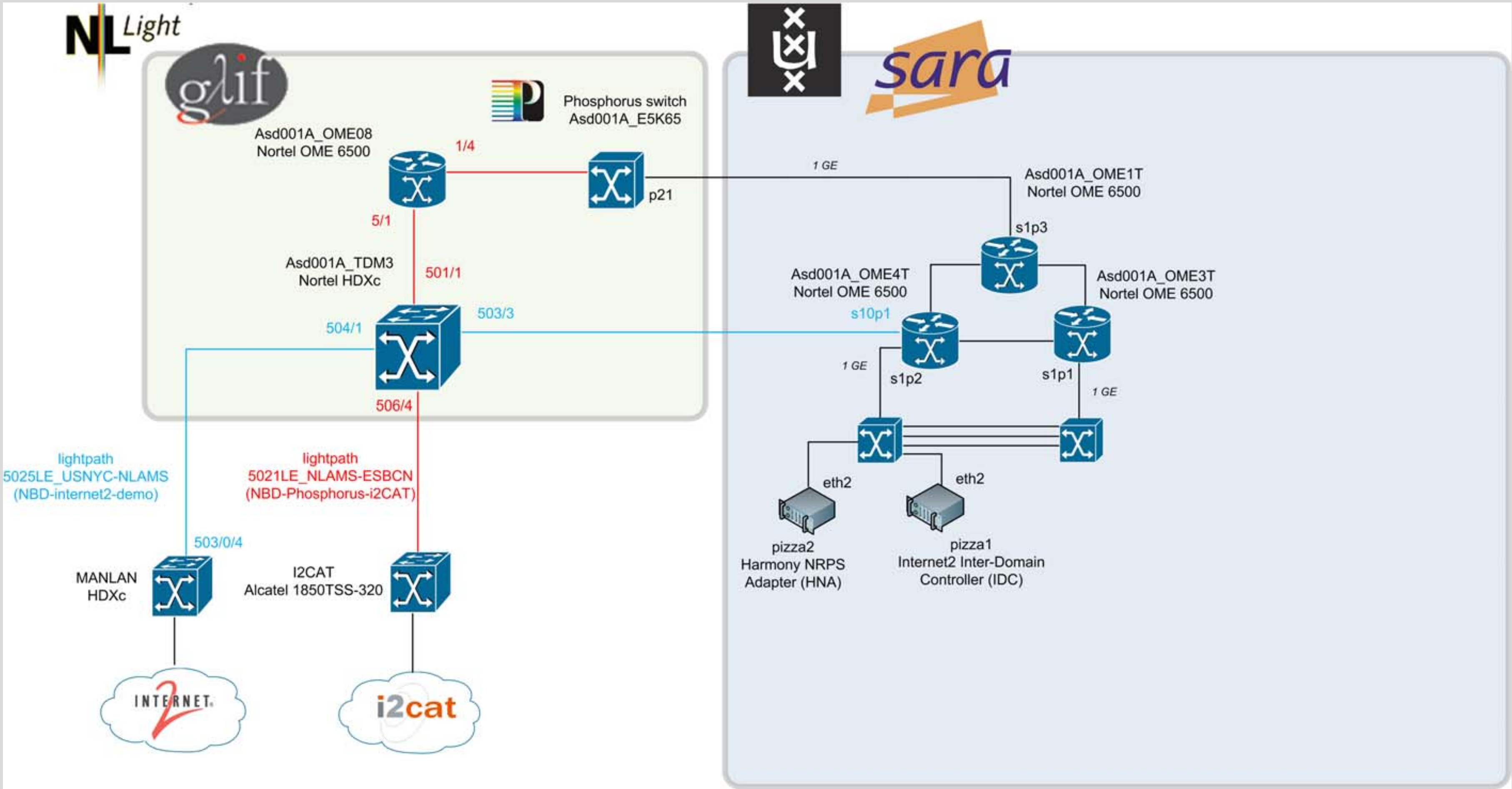
Netherlight/Phosphorus topology (UvA view)



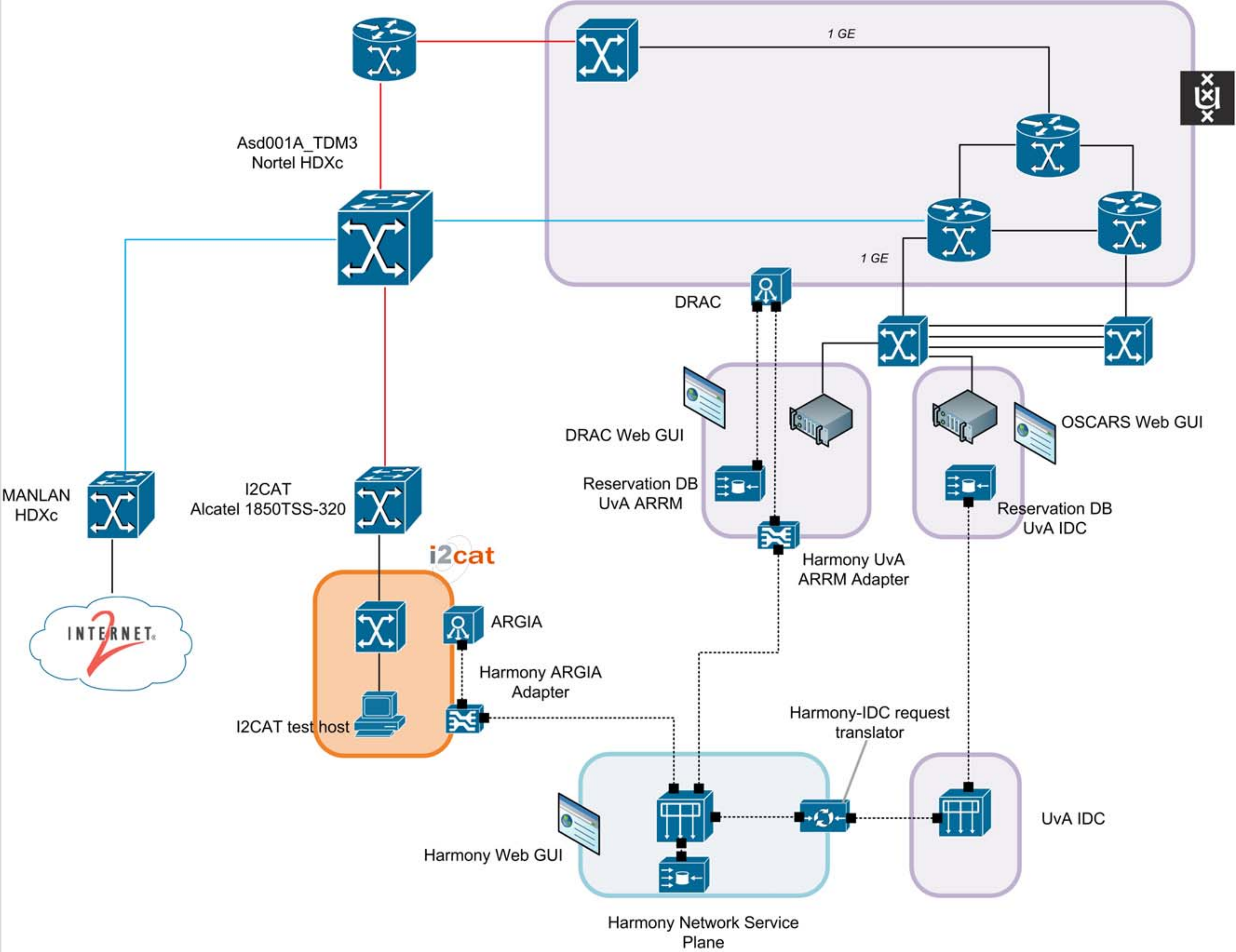
I2CAT/Phosphorus topology



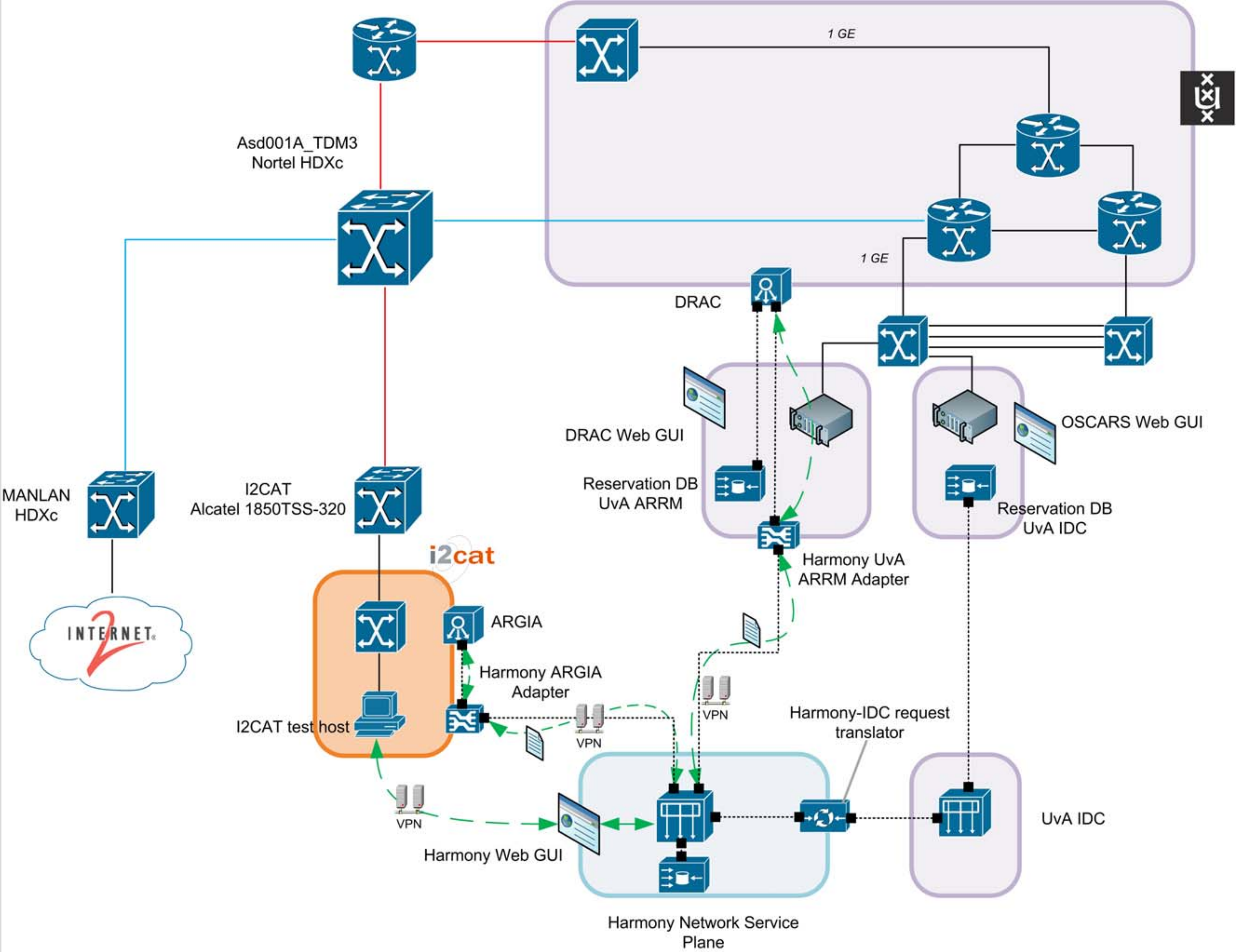
I2CAT-UvA-Internet2 Setup



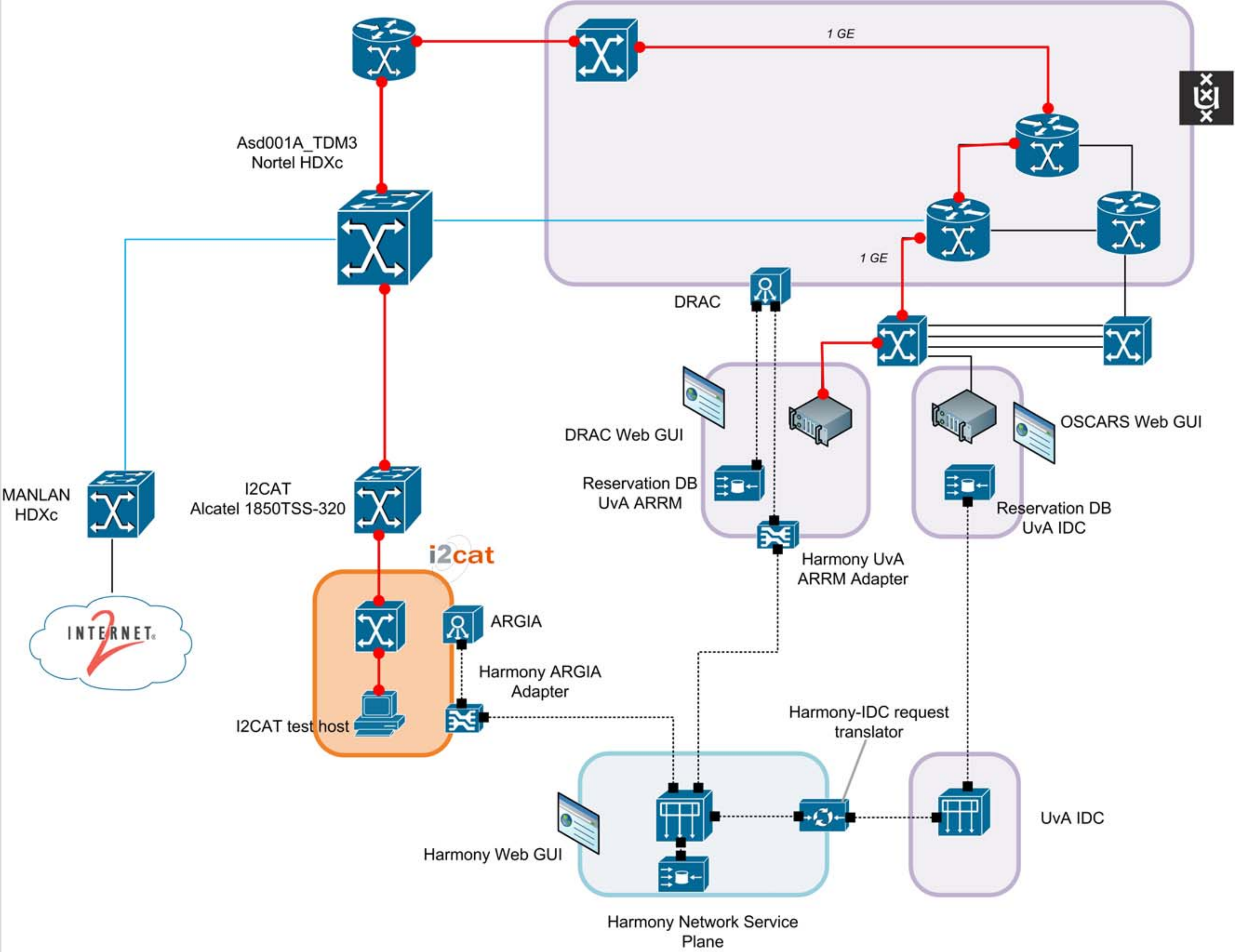
I2CAT-UvA Service Plane



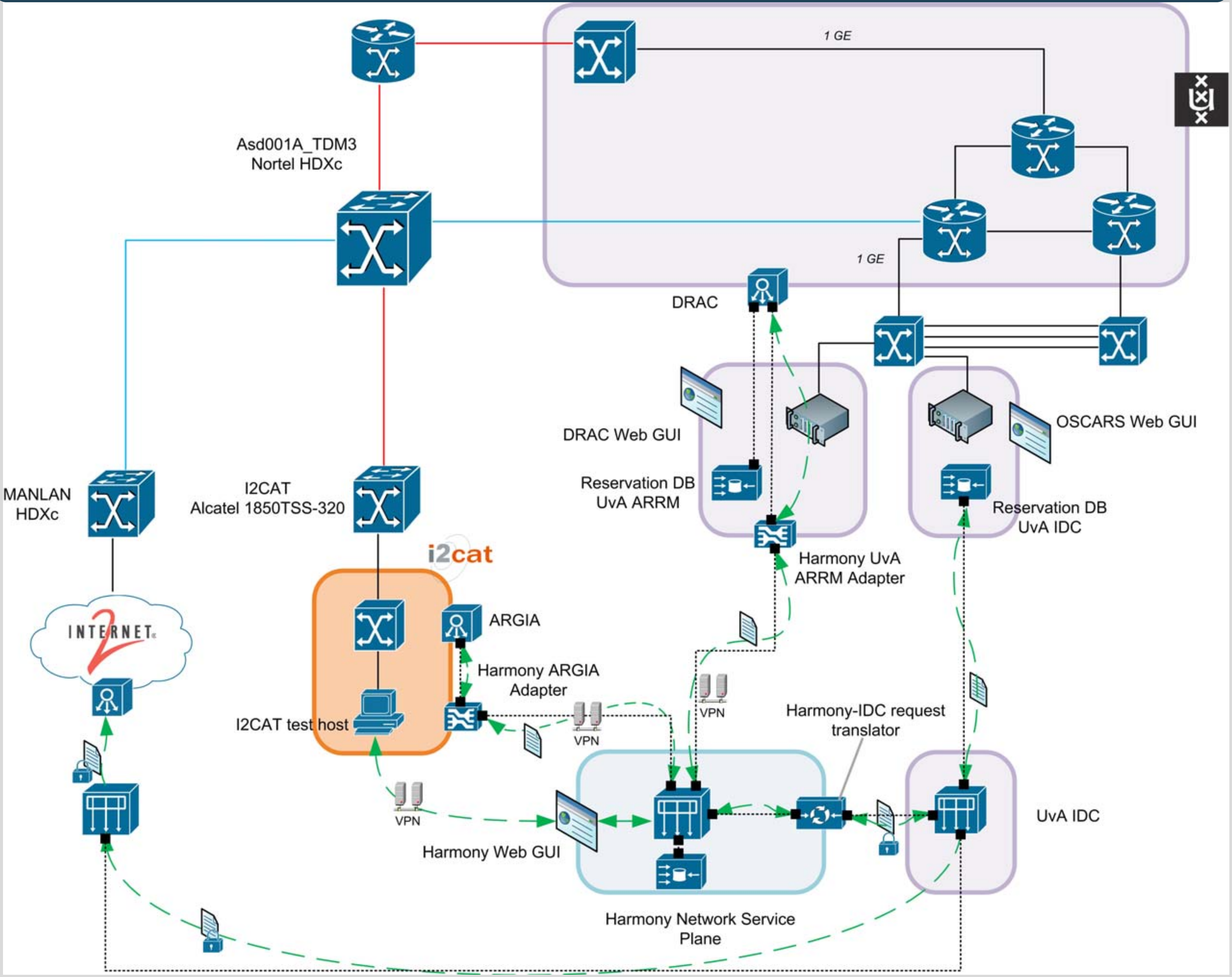
I2CAT-UvA Reservation Request



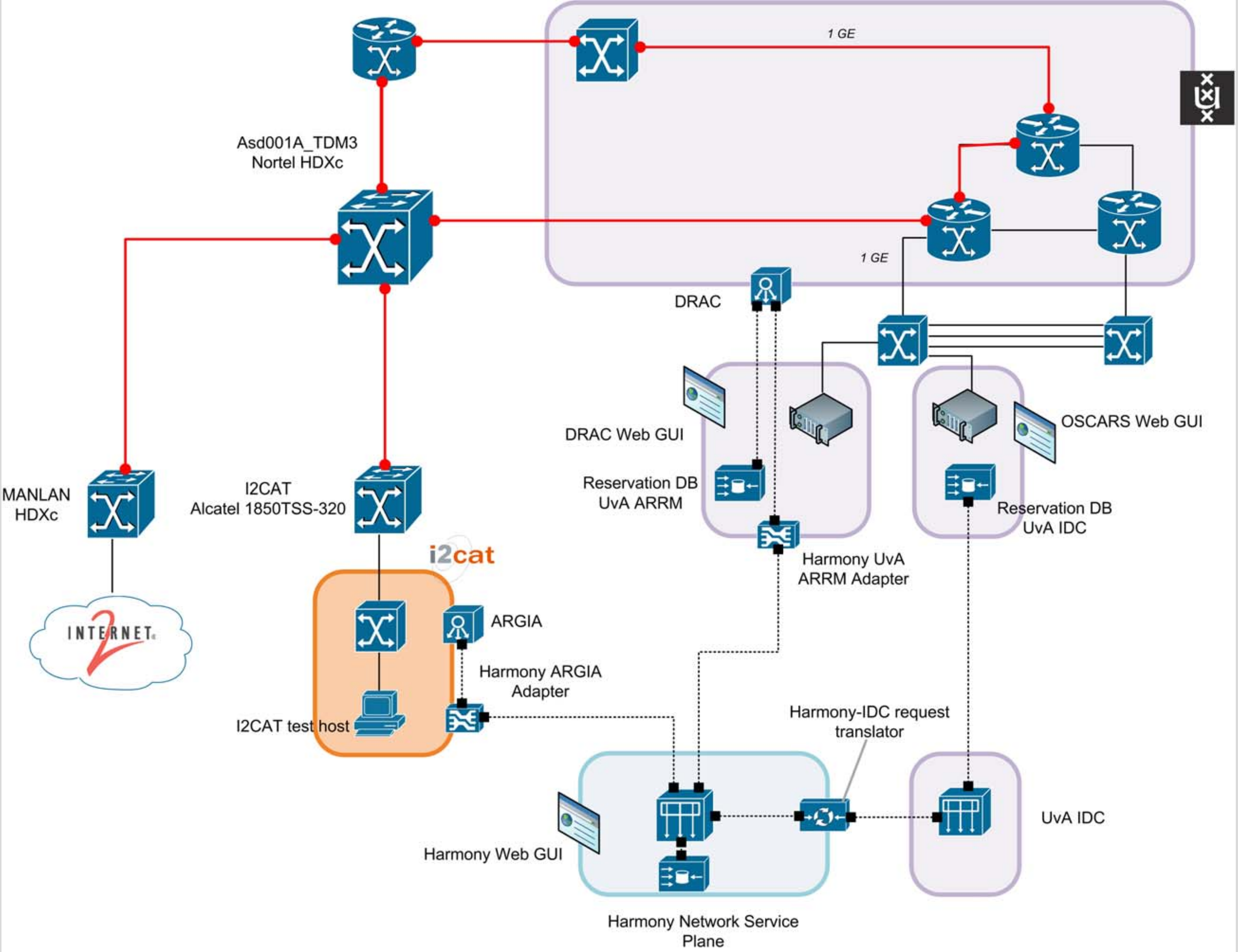
I2CAT-UvA Reservation Activation/Provisioning



I2CAT-Internet2 Reservation Request

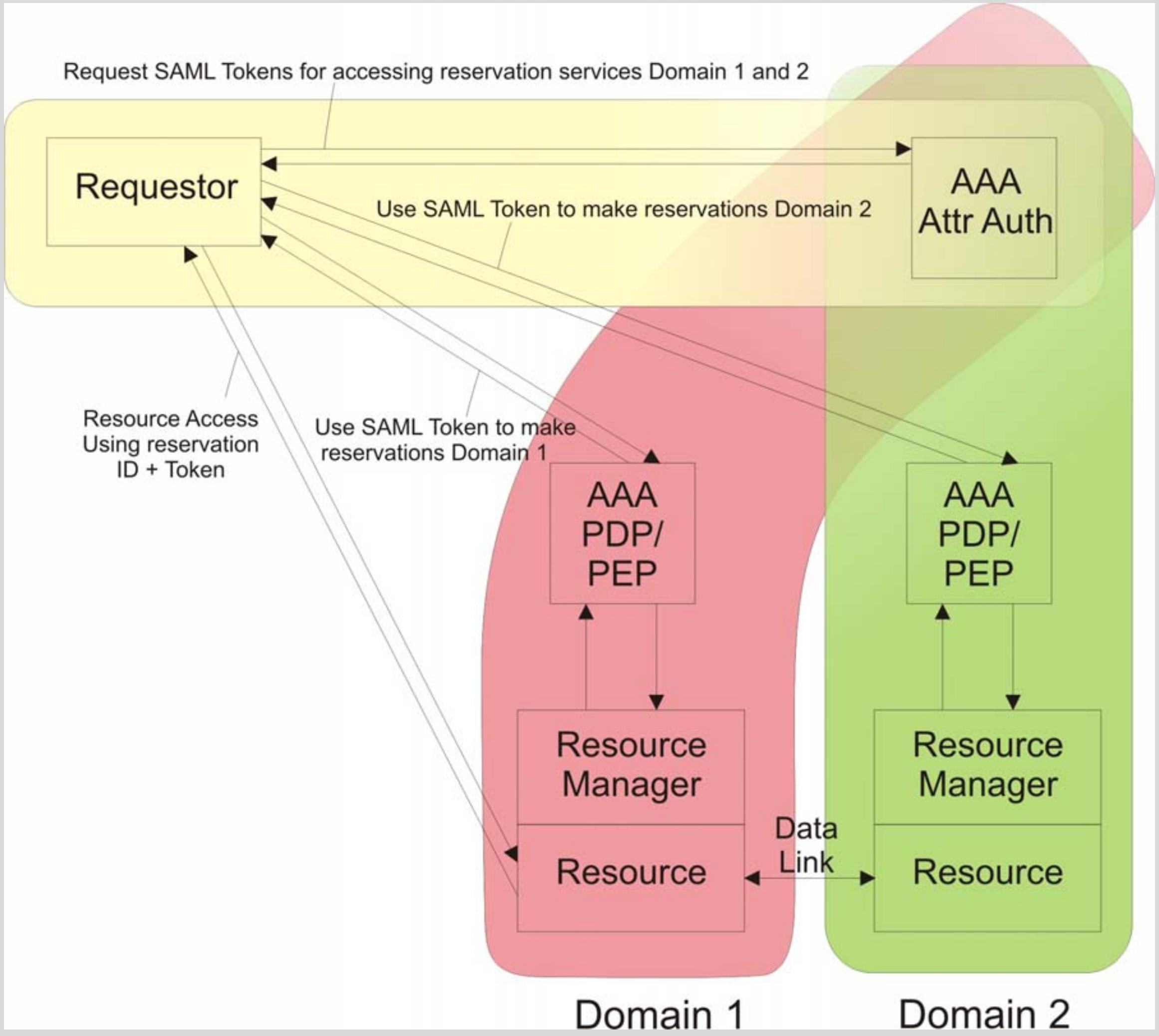


I2CAT-Internet2 Reservation Activation/Provisioning

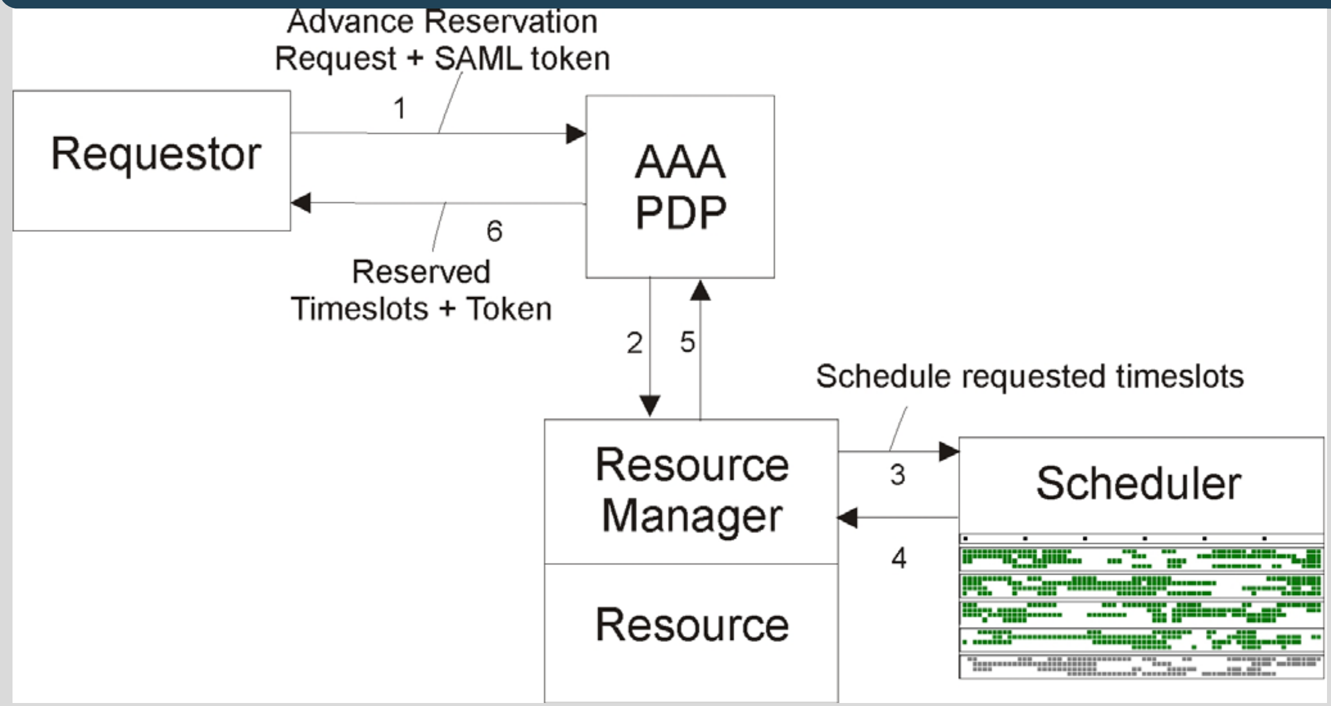


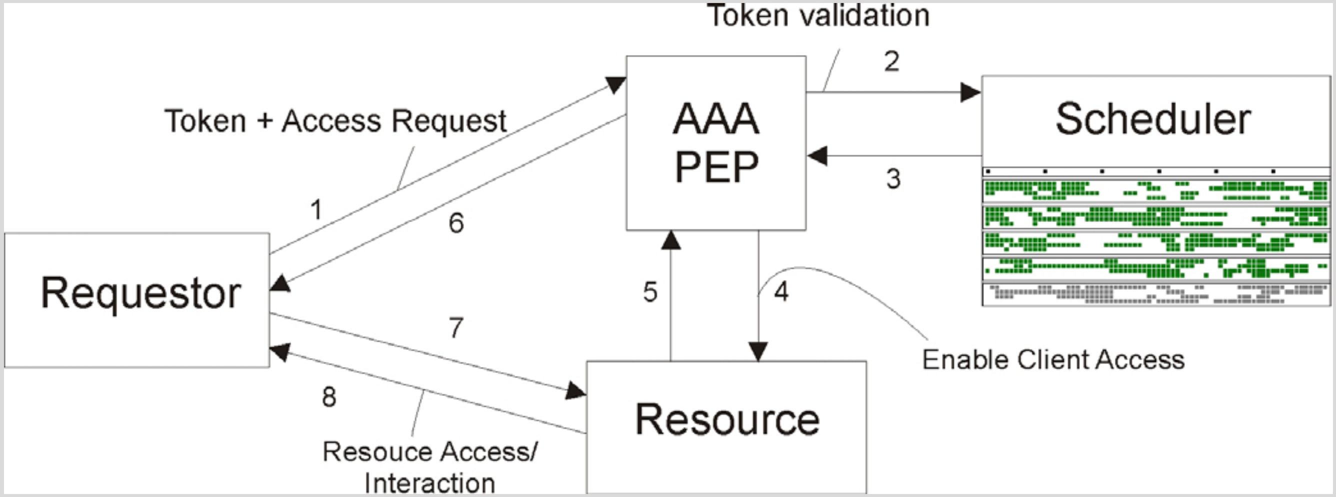
Moving on: multi-domain reservations

- Add multi-domain authz mechanism using a trusted STS, and let it issue SAML attr/authz assertions
- Add rescheduling functionalities/reservation tracking mechanism (Subject SAML HOK = owner)



Reservation request/resource access





Conclusion

- The experiment to create a Phosphorus-Internet2 setup and demo is still underway (and not demonstrable yet) because of organizational problems.
- The component that works (request translator) shows the GNI goal is feasible.
- To reach the GNI goal to detach the reservation system from AAA, the AAA has to be done by a trusted third party (Phosphorus STS).
- To create a useful GNI implementation a scheduler is needed to handle conflicting reservation requests.

- Demonstrable now: Harmony-IDC request translation
- Advance Resource Reservation Management system
- DRAC circuit creation (uncertain)
- Full demo: SC08