The Lambda Grid Control Planes

www.science.uva.nl/~delaat

Cees de Laat

GigaPort EU

University of Amsterdam

SARA
NIKHEF
NCF

Talk contents

- Just wait 20 minutes

Group

- **Advanced Internet Research: About 9 people**
- **Located Science Park Amsterdam, Watergraafsmeer**
  - **Producers**
  - **Consumers**
  - **Researchers**
- **Local Collaborations**
  - **UvA**
    - **VLE**
  - **NIKHEF apps from HEF**
    - **Grids and DataTransport**
    - **DAS**
  - **SARA**
    - **Optical lab / housing**
    - **Integration LambdaGrid node**

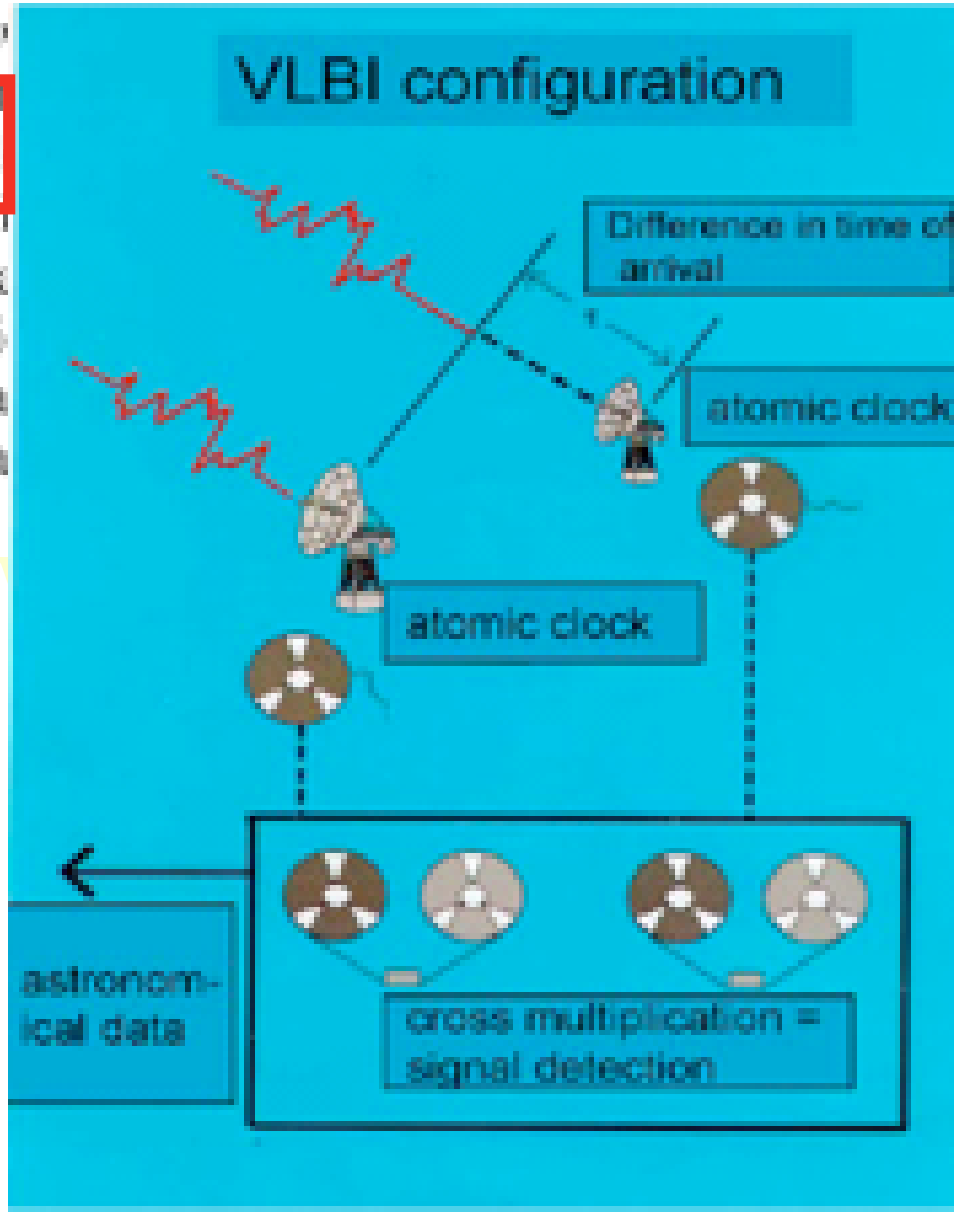
Research topics

- Optical networking architectures and models for usage
- Transport protocols for massive amounts of data
- Authorization of complex resources in multiple domains
- Embedding in Grid environments

VLBI

ger term VLBI is easily capable of generating many Gb of data per
The sensitivity of the VLBI array scales v
(data-rate) and there is a strong push to
. Rates of 8Gb/s or more are entirely feasibl
ider development. It is expected that paral
orrelator will remain the most efficient approa
s distributed processing may have an appli
lti-gigabit data streams will aggregate into la
or and the capacity of the final link to the da
tor.

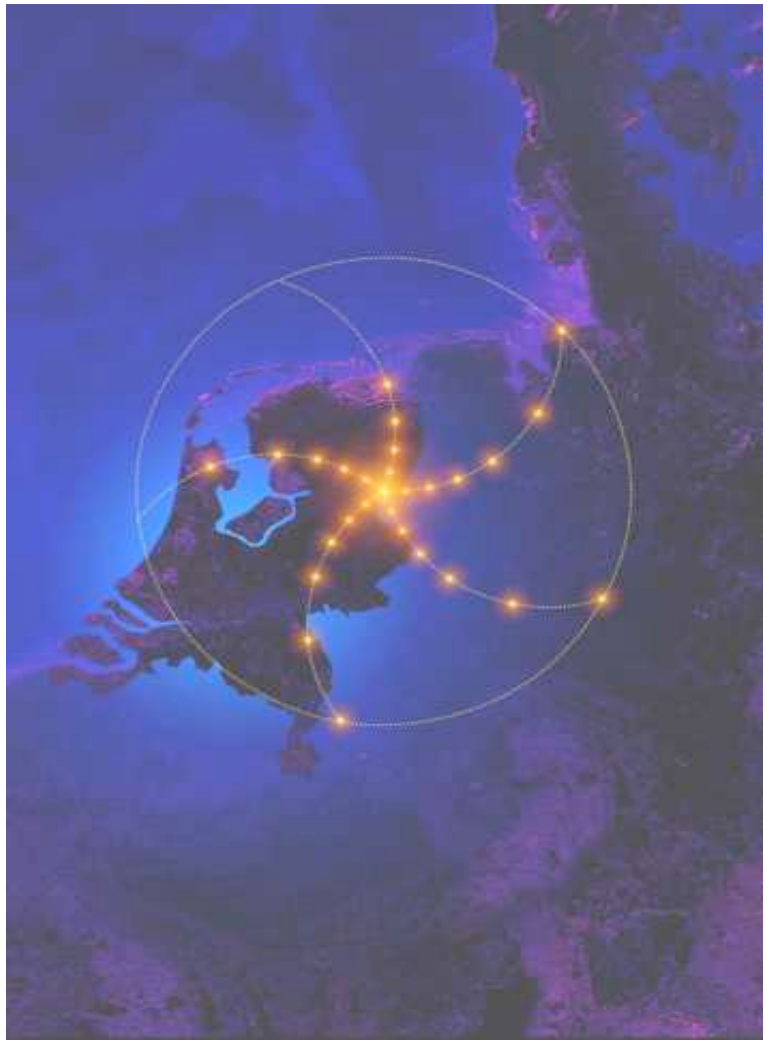
Westerbork Synthesis Radio Telescope - Netherlands



Lambdas as part of instruments

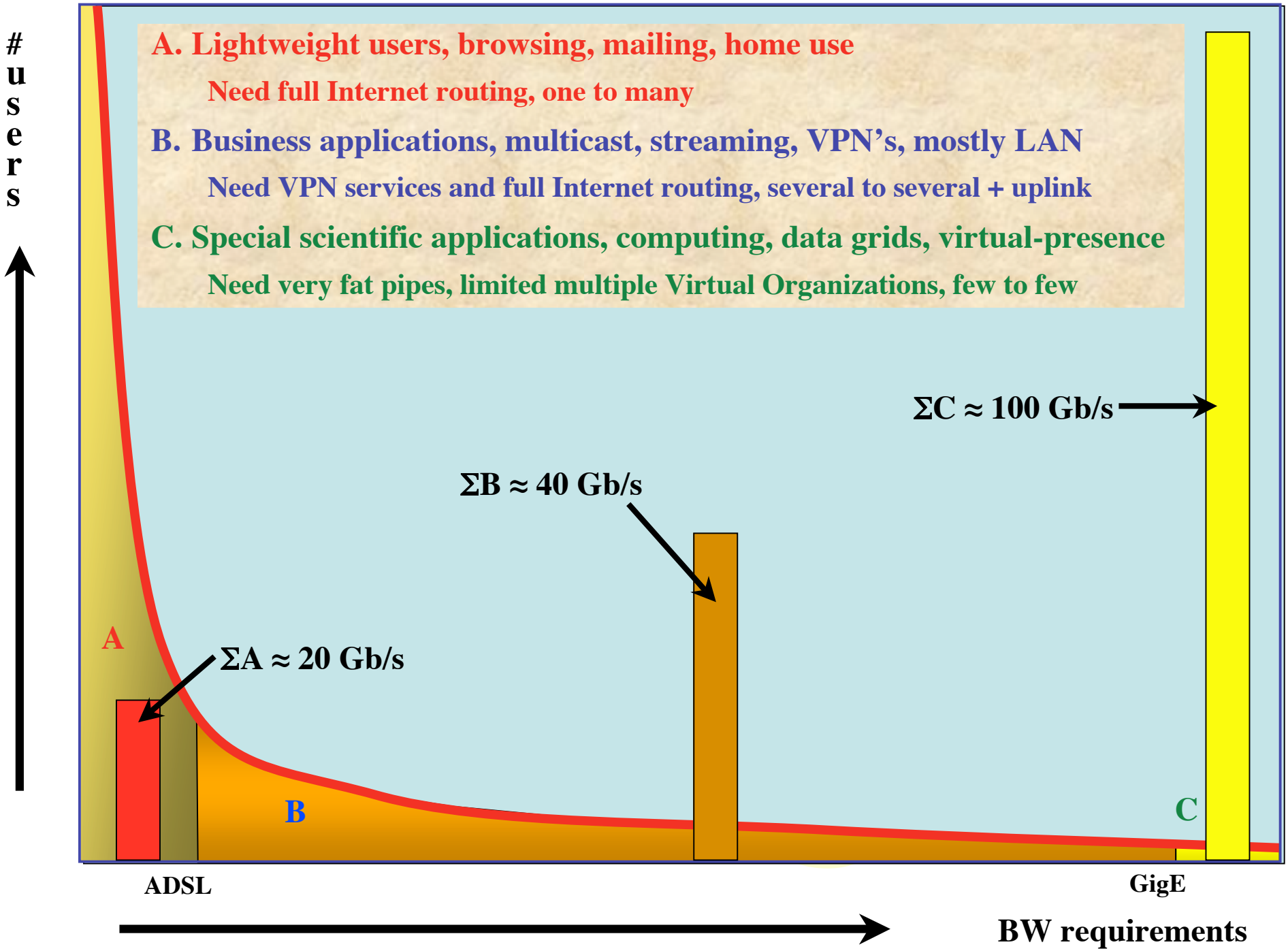
GigaPort

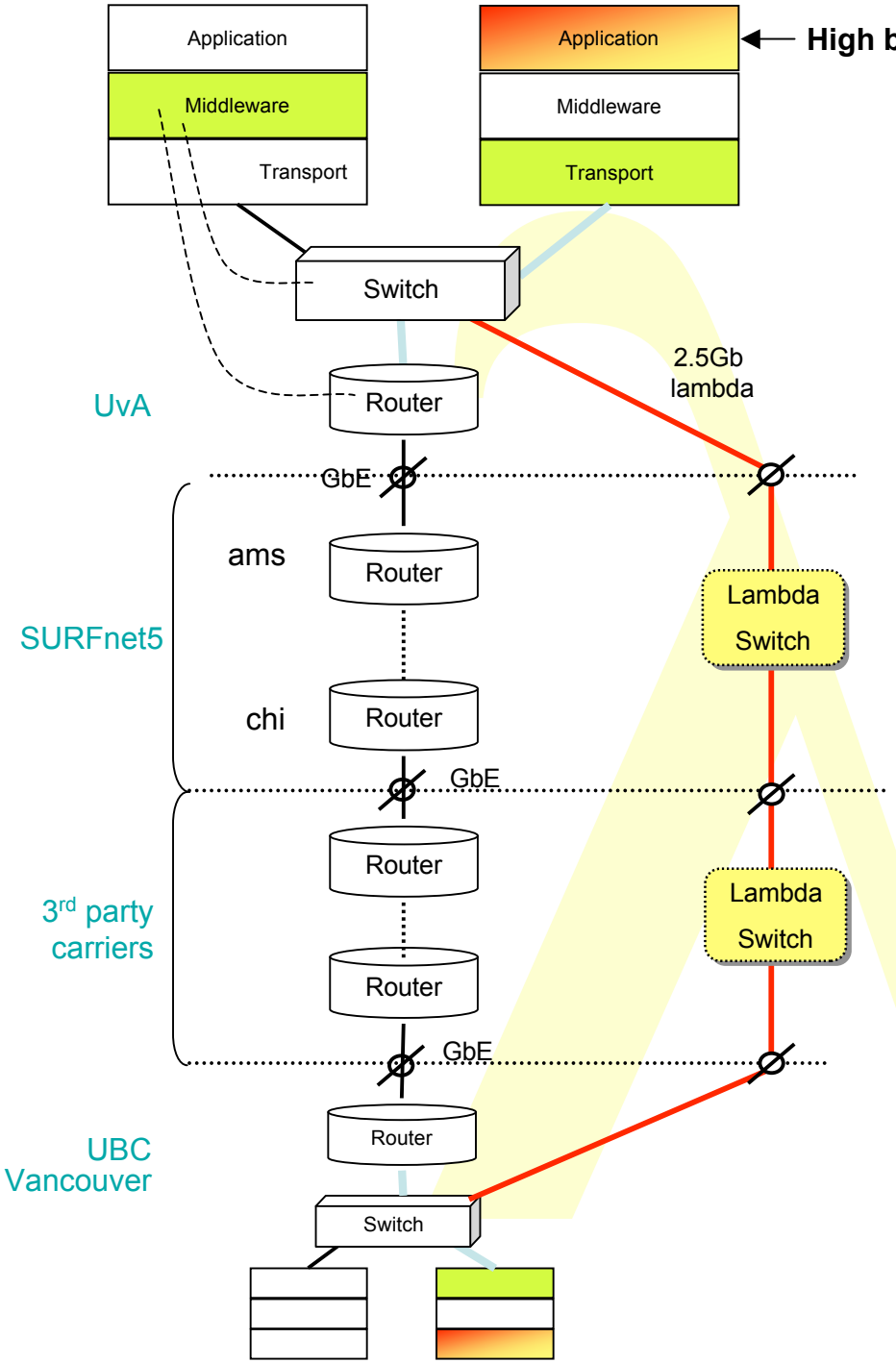
LOFAR



www.lofar.org

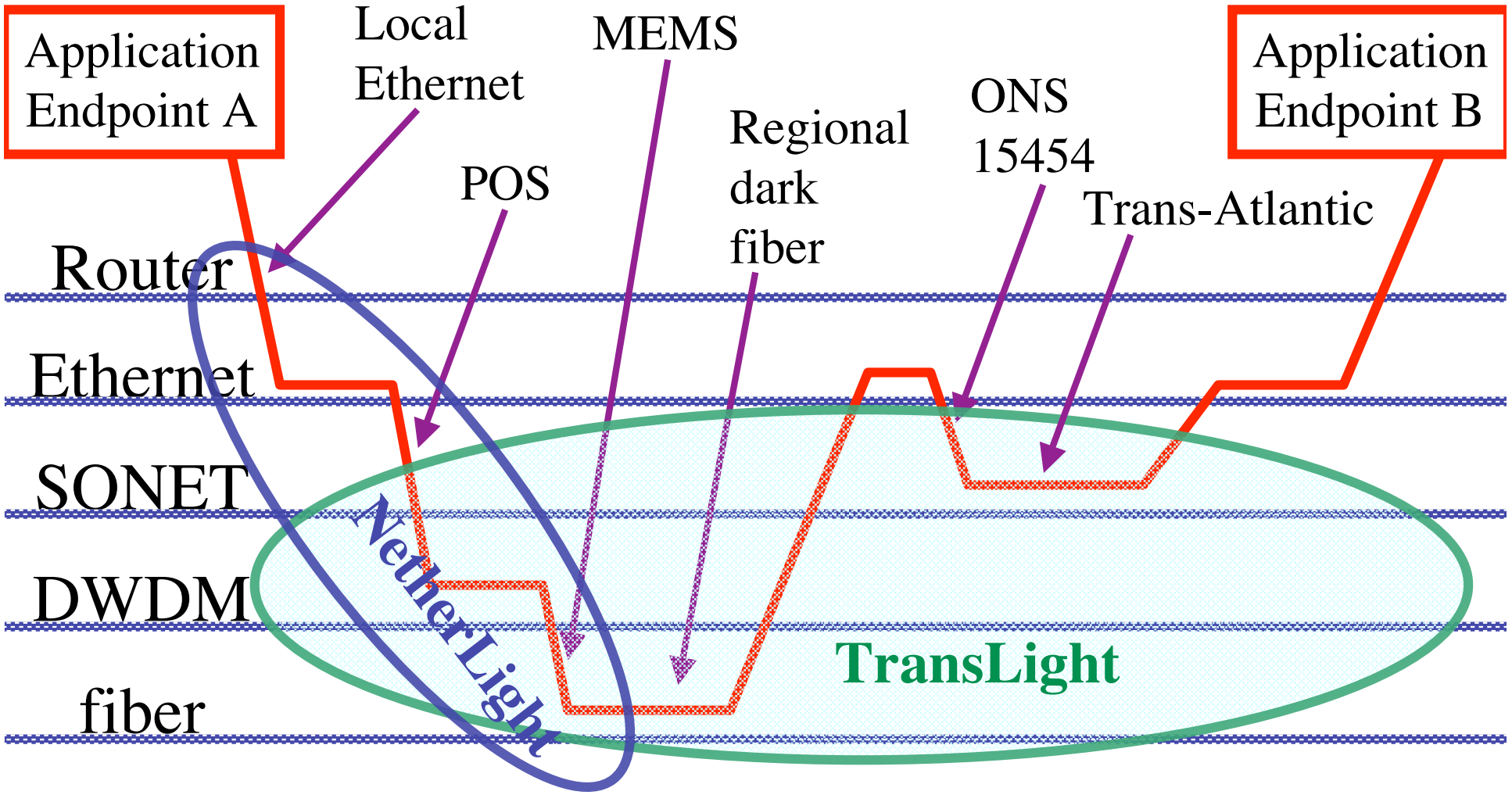
SURFnet


A. Lightweight users, browsing, mailing, home use
Need full Internet routing, one to many
B. Business applications, multicast, streaming, VPN's, mostly LAN
Need VPN services and full Internet routing, several to several + uplink
C. Special scientific applications, computing, data grids, virtual-presence
Need very fat pipes, limited multiple Virtual Organizations, few to few
users
ΣC ≈ 100 Gb/s
ΣB ≈ 40 Gb/s
ΣA ≈ 20 Gb/s
A
B
C
ADSL
GigE
BW requirements

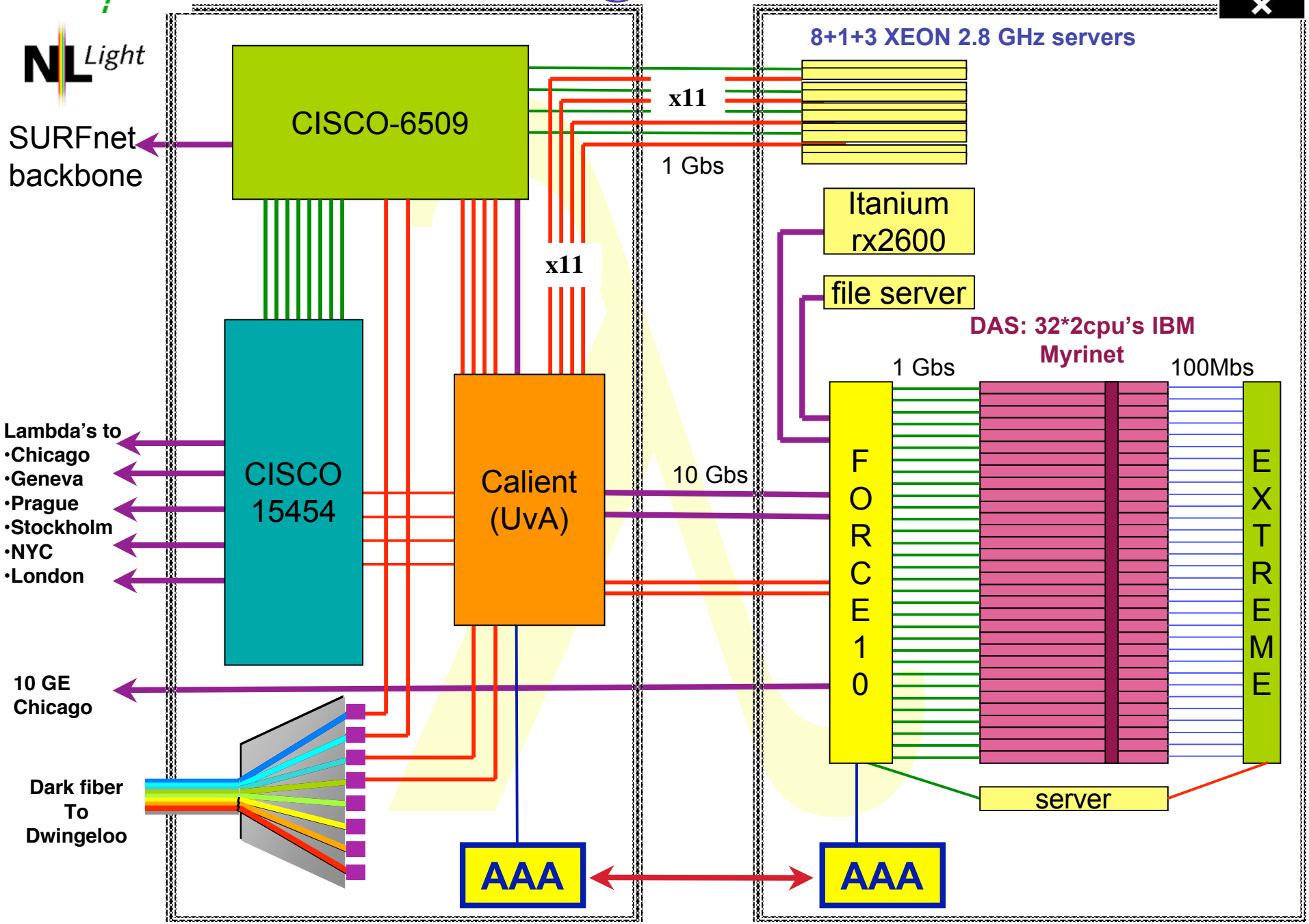


- lambda for high bandwidth applications
  - Bypass of production network
  - Middleware may request (optical) pipe
- RATIONALE:
  - Lower the cost of transport per packet
  - Use Internet as controlplane!

How low can you go?



NetherLight <-> UvA



UVA/EVL's
64*64
Optical Switch
@ NetherLight
in SURFnet POP @
SARA

Costs 1/100th of a similar throughput router or 1/10th of an Ethernet switch but with specific services!

History & Charter

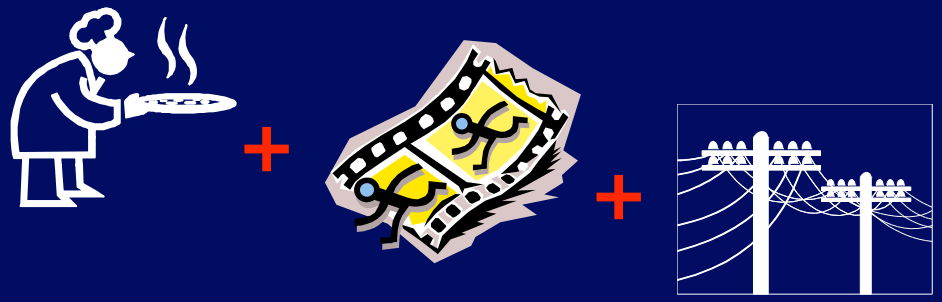
- Authorization subgroup of AAA-WG
- Commonality in authorization space
- Tie in policy from all WG's
- IRTF-RG chartered in Dec 1999
  - This RG will work to define a next generation AAA architecture that incorporates a set of interconnected "generic" AAA servers and an application interface that allows Application Specific Modules access to AAA functions.

From charter

- The architecture's focus is to support AAA services that:
  - can inter-operate across organizational boundaries
  - are extensible yet common across a wide variety of Internet services
  - enables a concept of an AAA transaction spanning many stakeholders
  - provides application independent session management mechanisms
  - contains strong security mechanisms that be tuned to local policies
  - is a scalable to the size of the global Internet

High level use case

- I want:
  - a pizza,
  - movie on demand
  - the bandwidth allocation from the movie service to my screen.

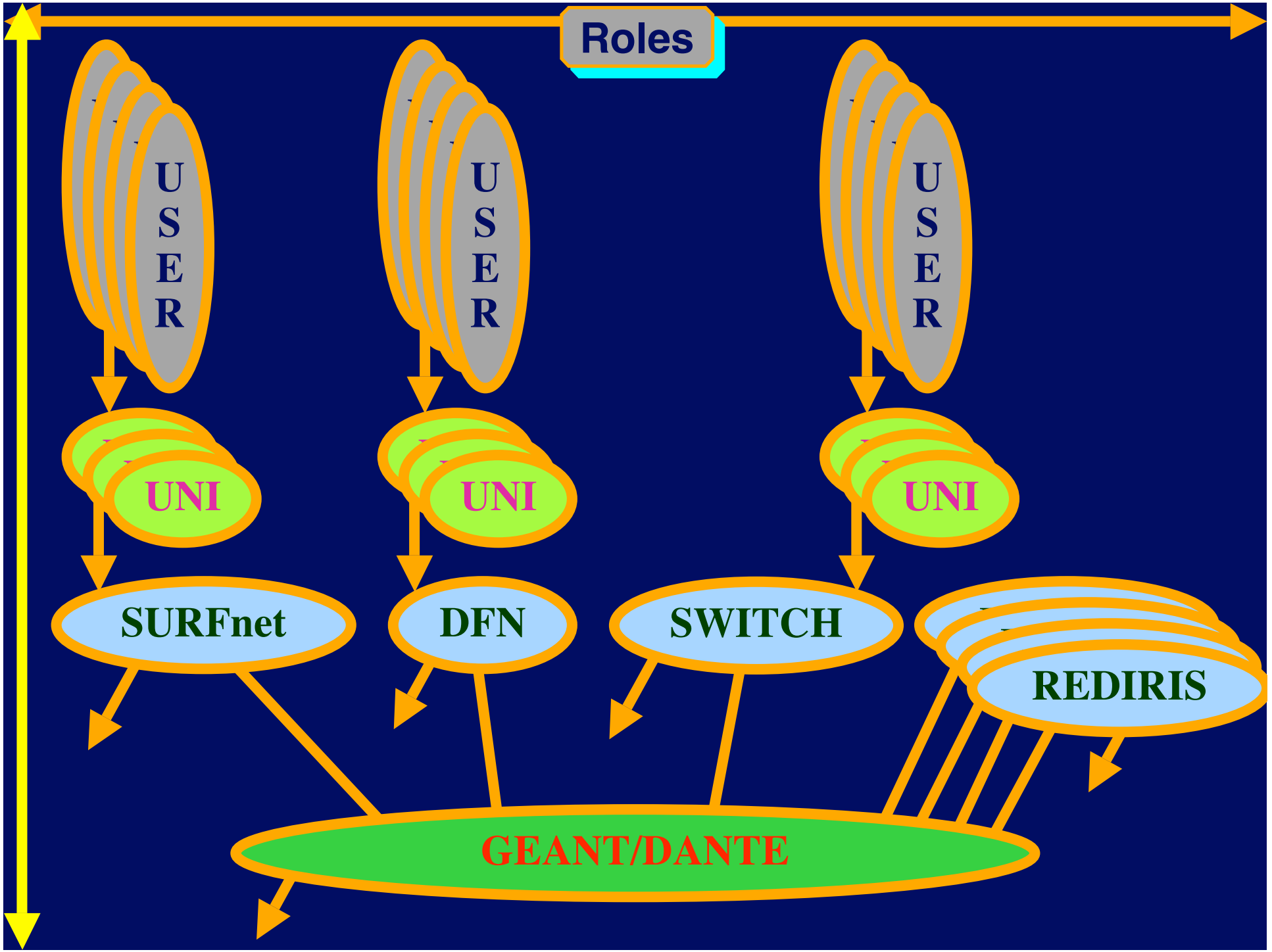


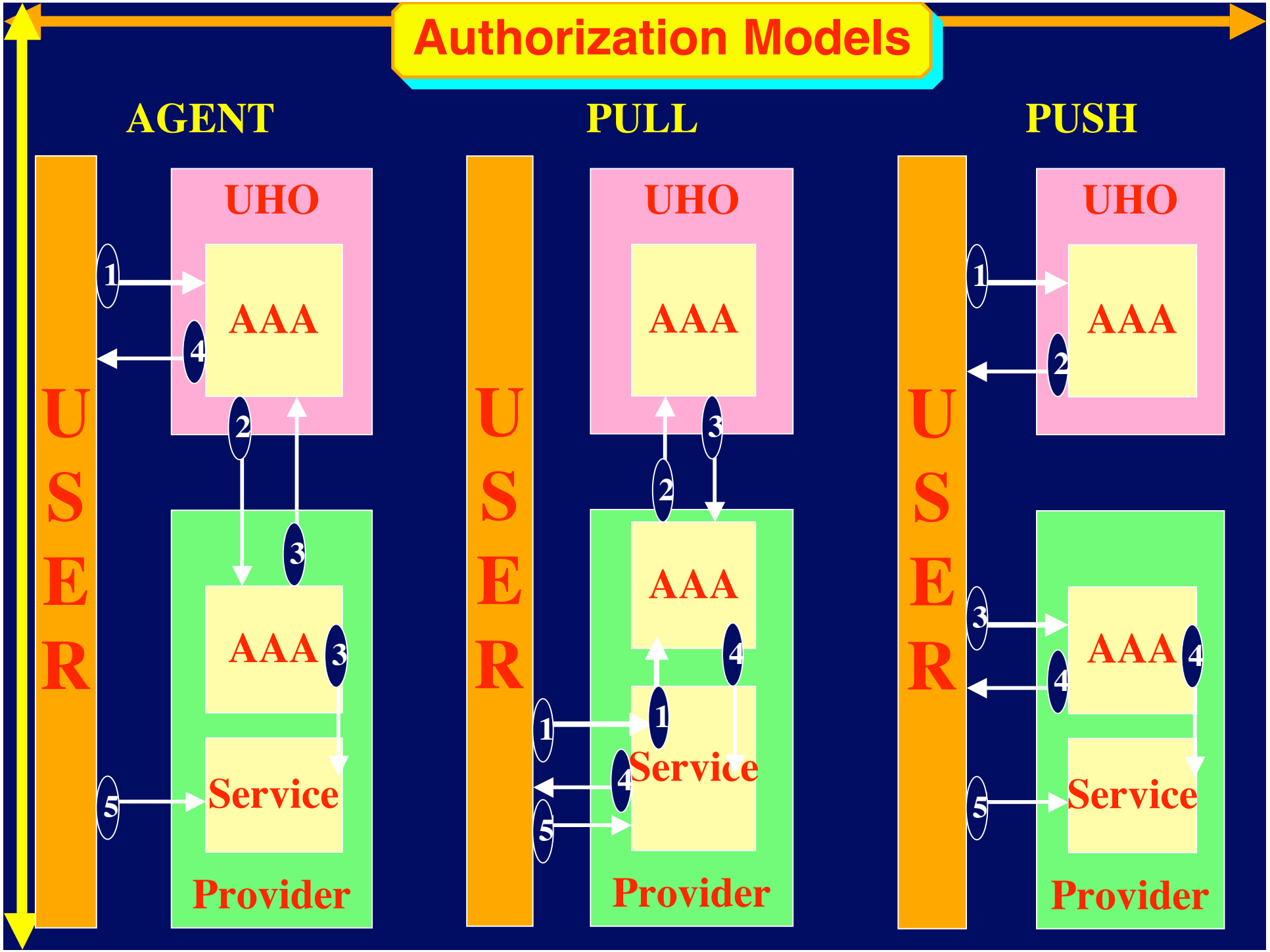
- Then:
  - I am :-) :-) :-)

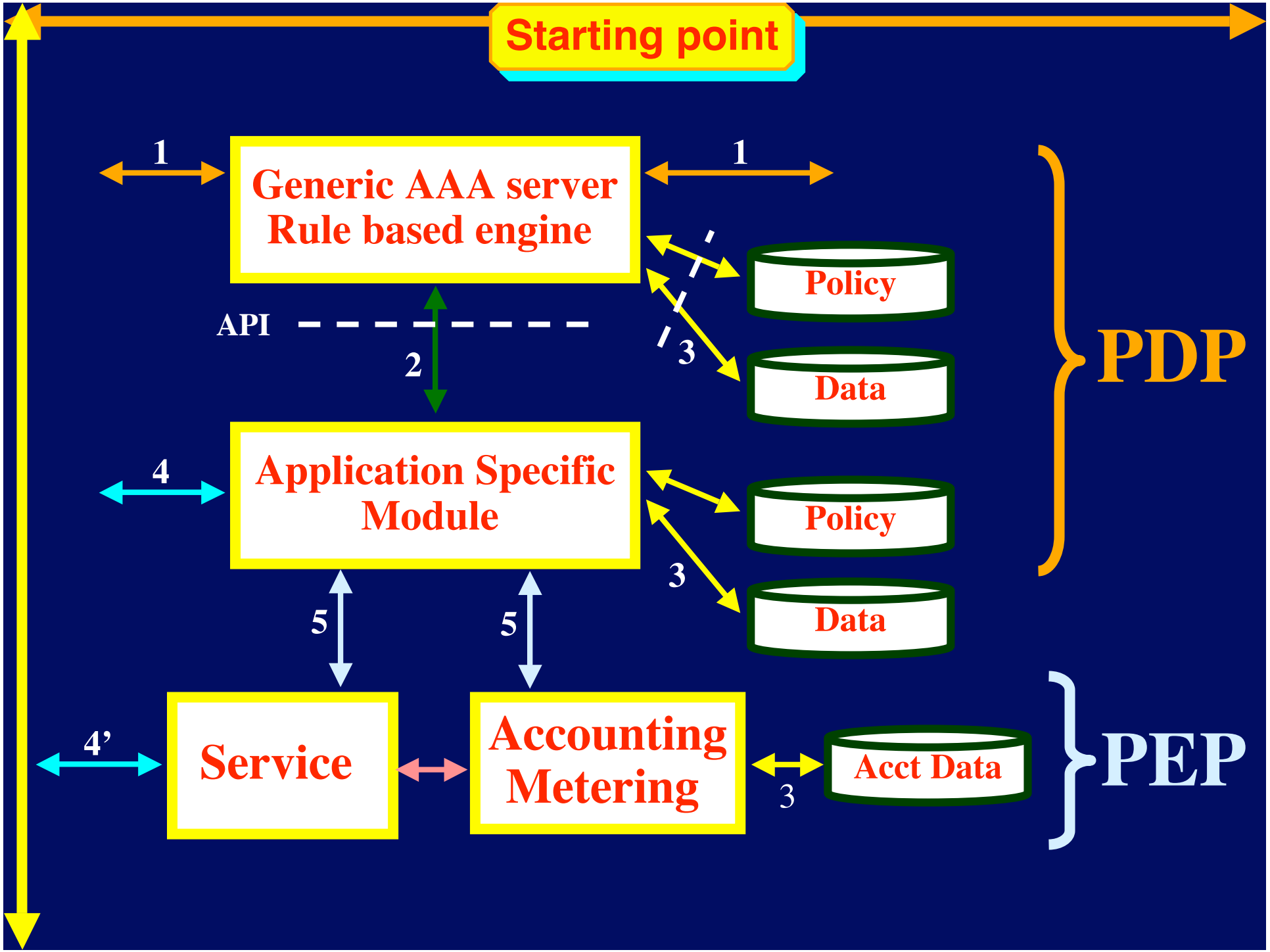
- This authorization:
  - has more stakeholders
  - is multi domain
  - is a combination of different types of resources

Basic AAA

- **Service perspective:**
  - Who is it who wants to use my resource
    - » Establish security context
  - Do I allow him to access my resource
    - » Create a capability / ticket /authorization
  - Can I track the usage of the resource
    - » Based on type of request (policy) track the usage
- **User perspective**
  - Where do I find this or that service
  - What am I allowed to do
  - What do I need to do to get authorization
  - What does it cost
- **Intermediaries perspective**
  - Service creation
  - Brokerage / portals
- **Organizational perspective**
  - What do I allow my people to do
  - Contractual relationships (SLA's)


Roles
USER
USER
USER
UNI
UNI
UNI
SURFnet
DFN
SWITCH
REDIRIS
GEANT/DANTE


Authorization Models
AGENT
PULL
PUSH
USER
UHO
AAA
Service
Provider
1
2
3
4
5


Starting point
1
Generic AAA server
Rule based engine
1
Policy
API
2
3
Data
PDP
4
Application Specific
Module
Policy
3
Data
5
5
4'
Service
Accounting
Metering
3
Acct Data
PEP

Current drafts

- **Experiences from sc2003 demonstrator**

  Title : Prototype of a Generic AAA Server

  Author(s) : C. de Laat, et al.

  Date : 2004-3-26

  http://www.ietf.org/internet-drafts/draft-irtf-aaaarch-prototype-00.txt

- **Policy language**

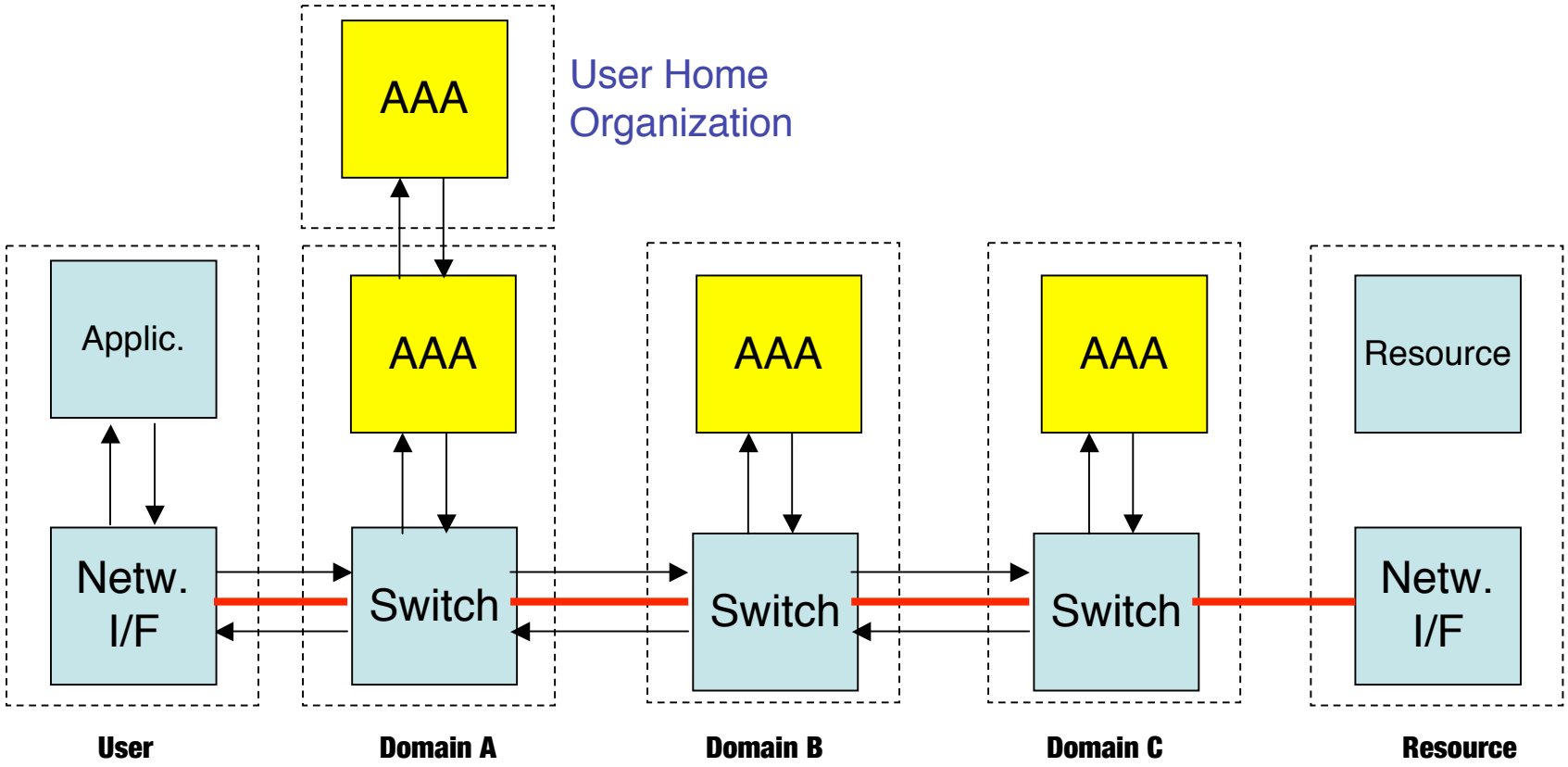
  Title : A grammar for Policies in a Generic AAA Environment

  Author(s) : A. Taal, et al.

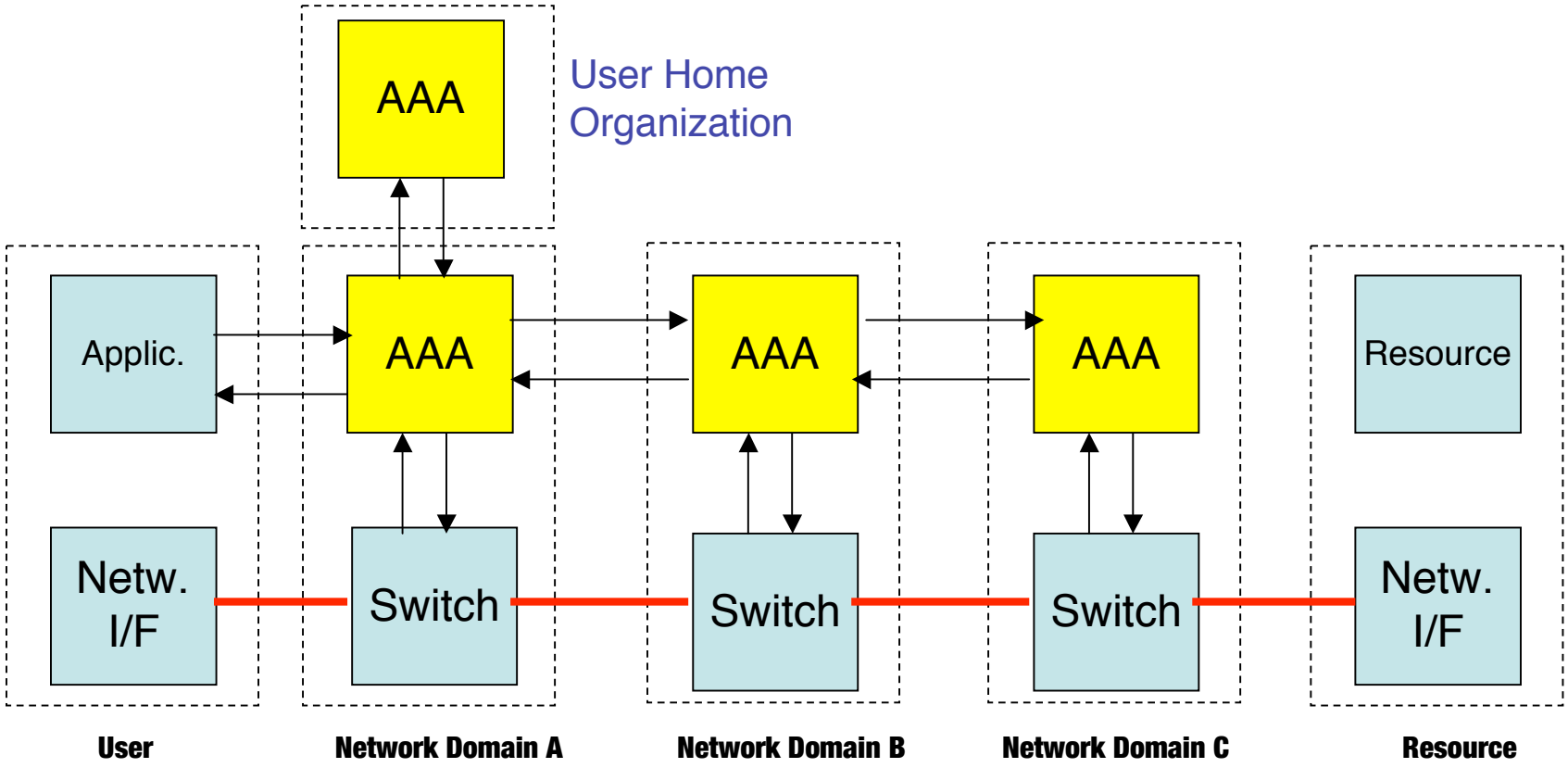
  Date : 2004-3-22

  http://www.ietf.org/internet-drafts/draft-irtf-aaaarch-generic-policy-04.txt

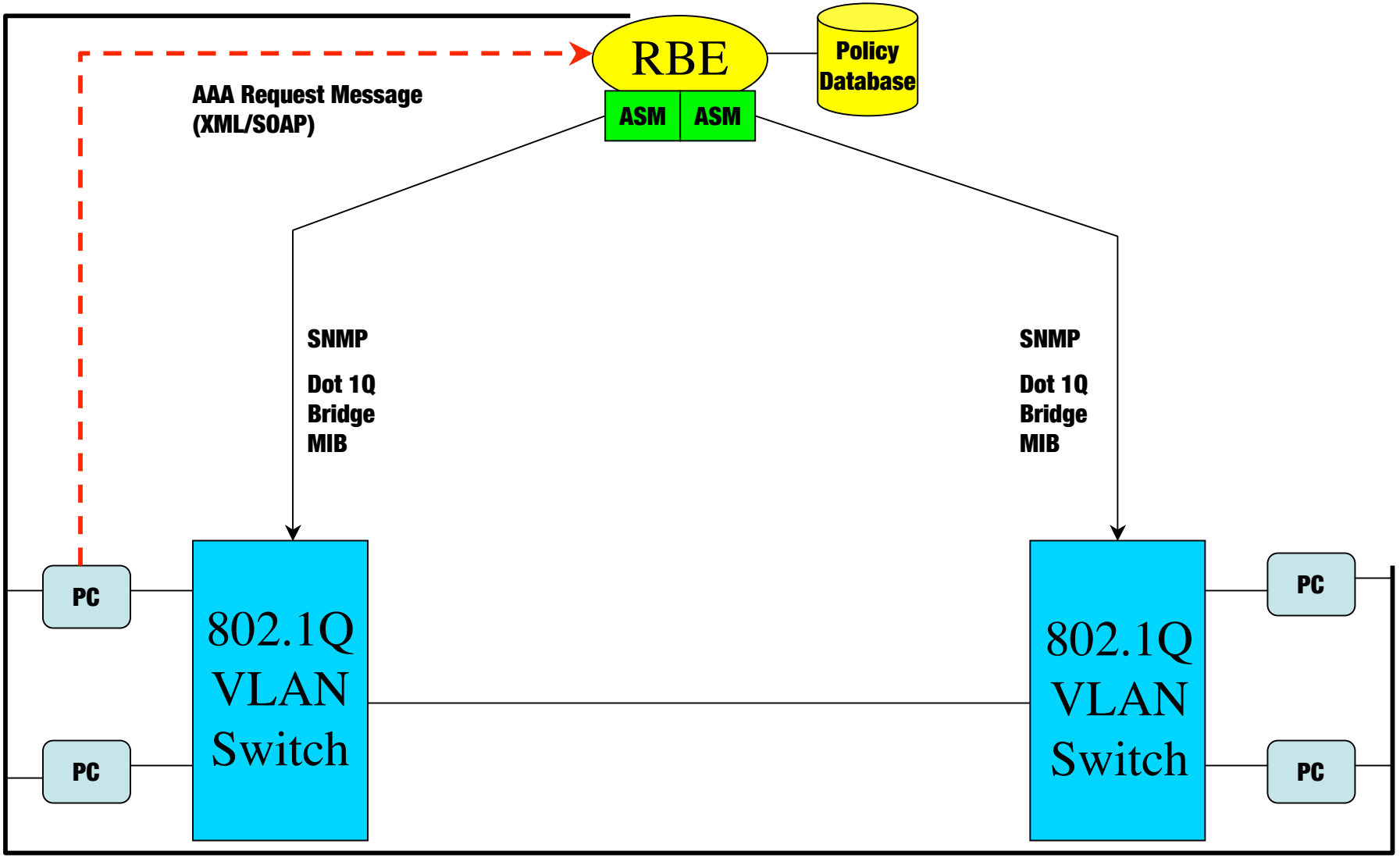
Example AuthZ RFC 2904 pull sequence



Example AuthZ RFC 2904 agent / pull sequence



Single - domain 802.1Q VLAN setup
Demo iGrid 2002



Example XML request message

WHY

WHAT

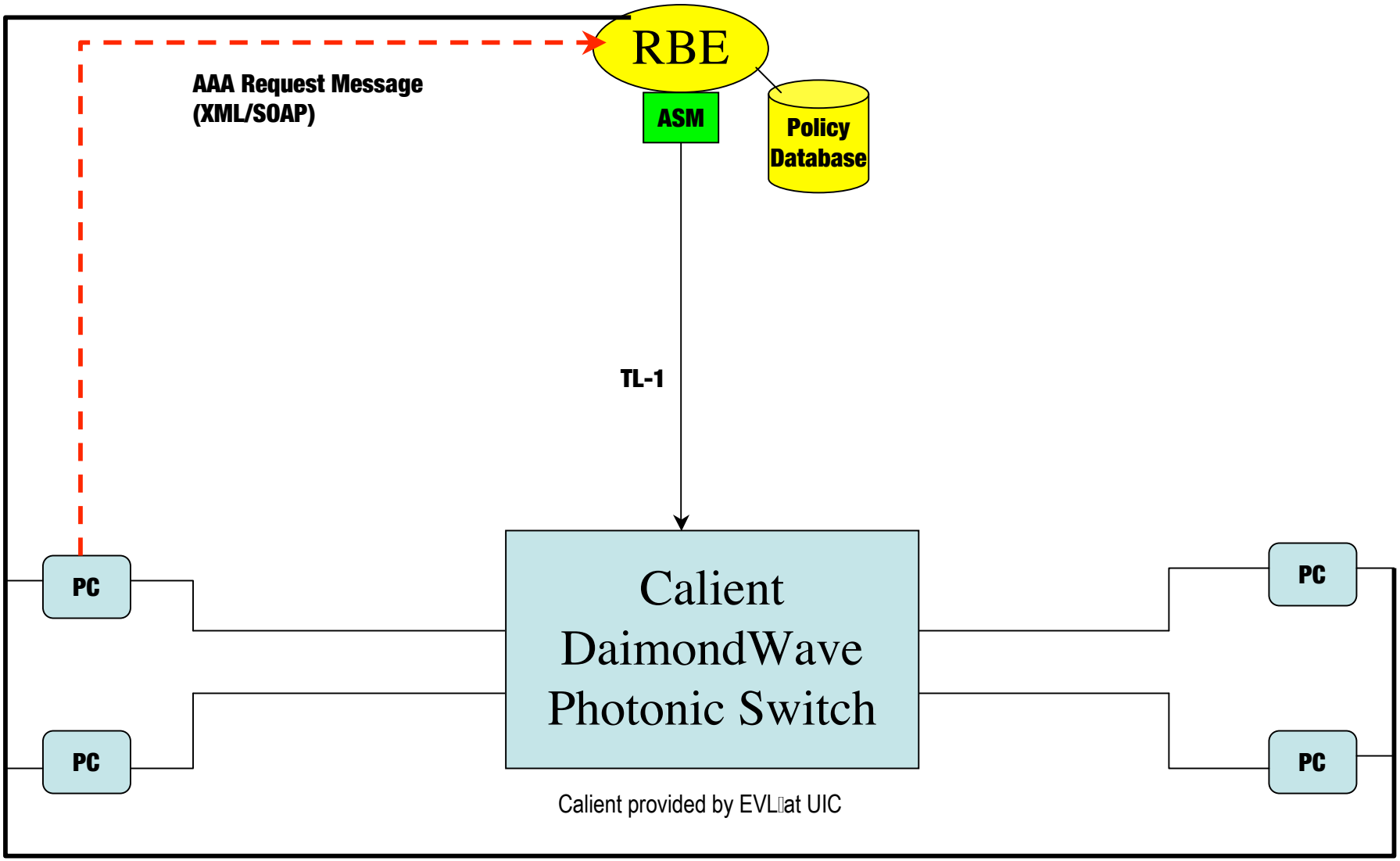
```
<AAARequest version="0.1" type="BoD" >
  <Authorization>
      <credential>
         <credential_type>simple</credential_type>
         <credential_ID>JanJansen</credential_ID>
         <credential_secret>#f034d</credential_secret>
      </credential>
  </Authorization>
  <BodData>
      <Source>192.168.1.5</Source>
      <Destination>192.168.1.6</Destination>
      <Bandwidth>1000</Bandwidth>
      <StartTime>now</StartTime>
      <Duration>20</Duration>
  </BodData>
</AAARequest>
```

Example part of a Driving Policy (is an ID)

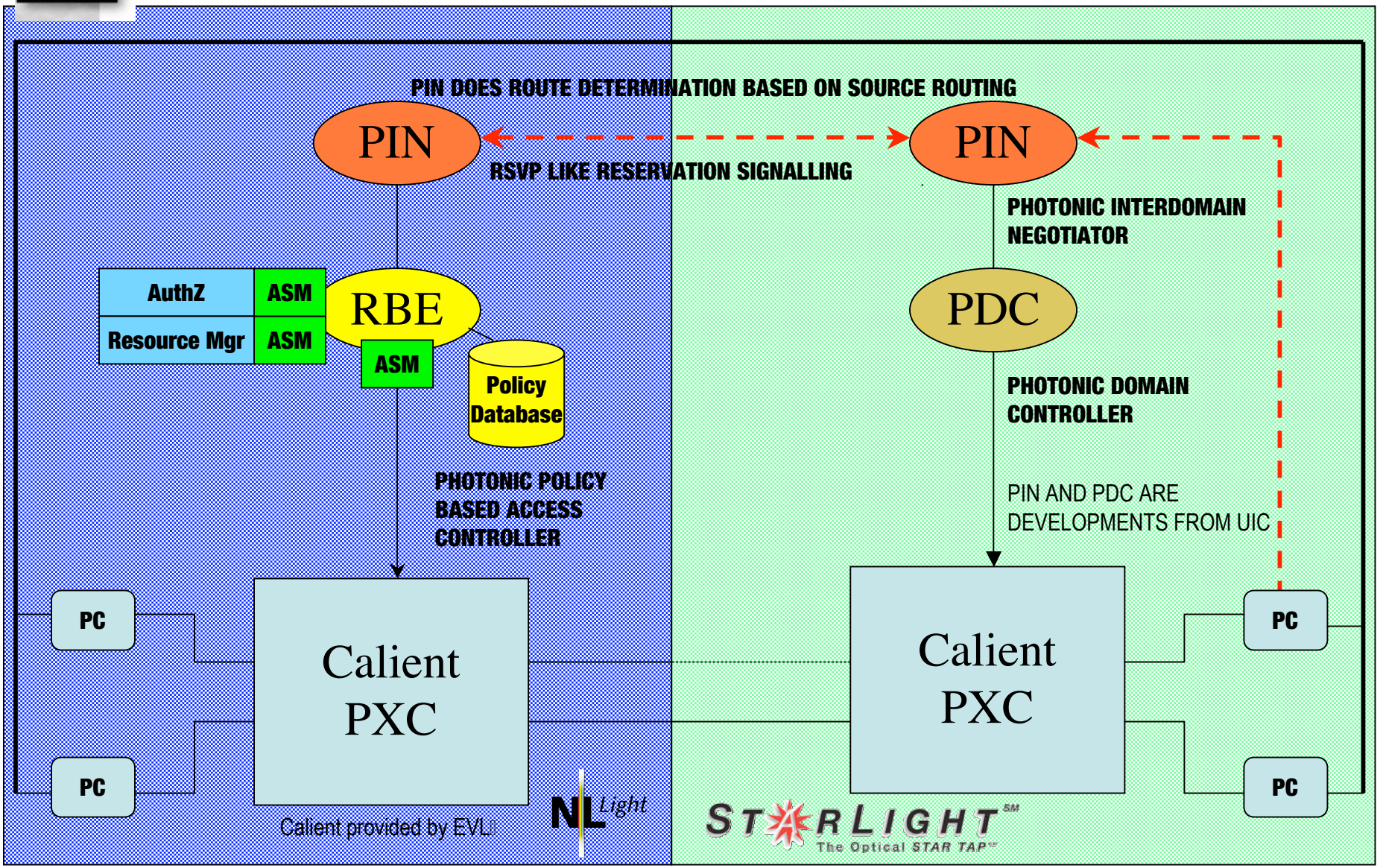
```
if
(
  (
    ASM::RM.CheckConnection(
                          Request::BodData.Source,
                          Request::BodData.Destination
                               )
    &&

    ( Request::BodData.Bandwidth <= 1000 )
  )
)
then
(
  ASM::RM.RequestConnection(
              Request::BodData.Source,
              Request::BodData.Destination,
              Request::BodData.Bandwidth,
              Request::BodData.StartTime,
              Request::BodData.Duration
                 )
  ;
  Reply::Answer.Message = "Request successful"
)
else
(
  Reply::Error.Message = "Request failed"
```

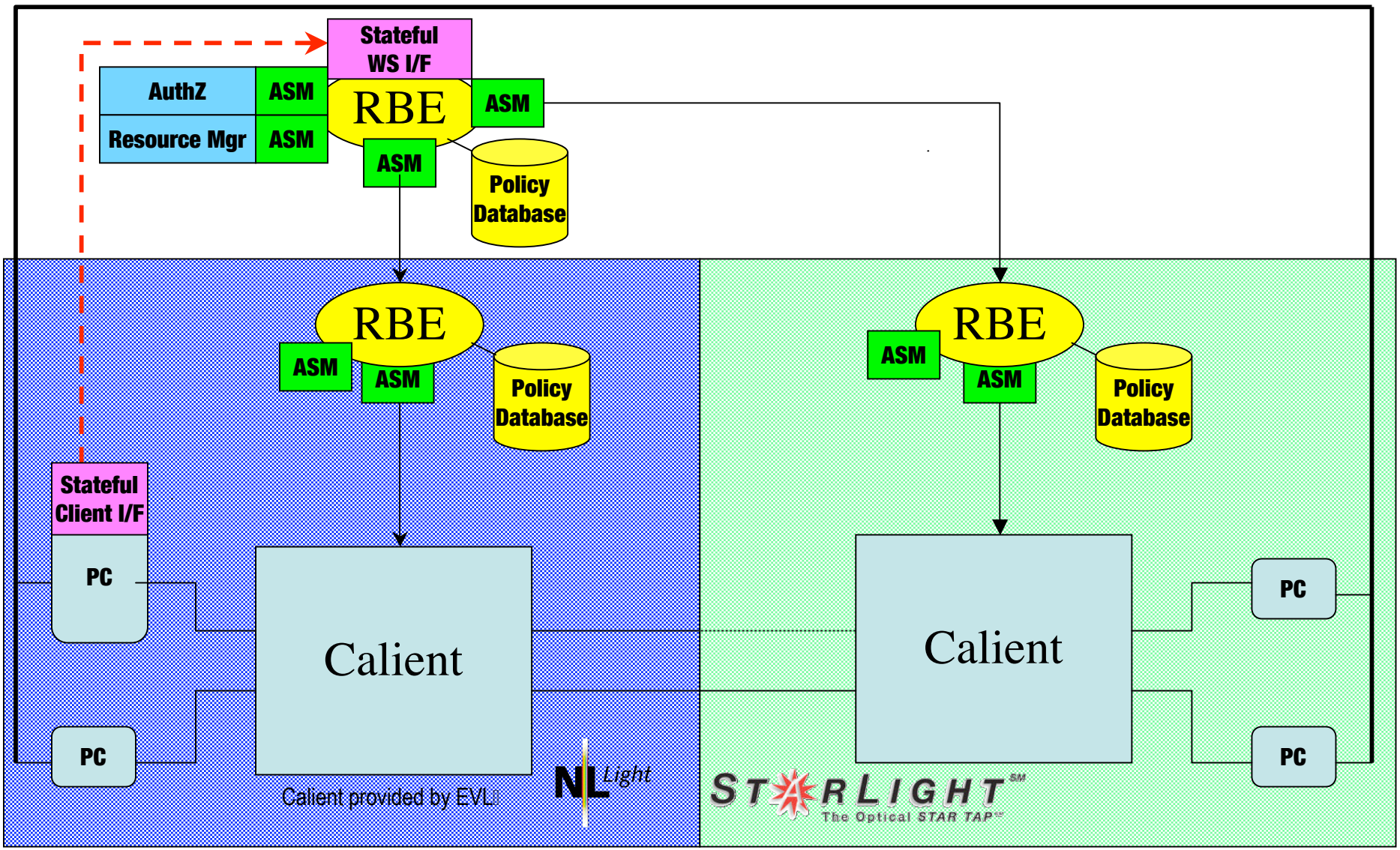
Single - Domain Calient OXC setup



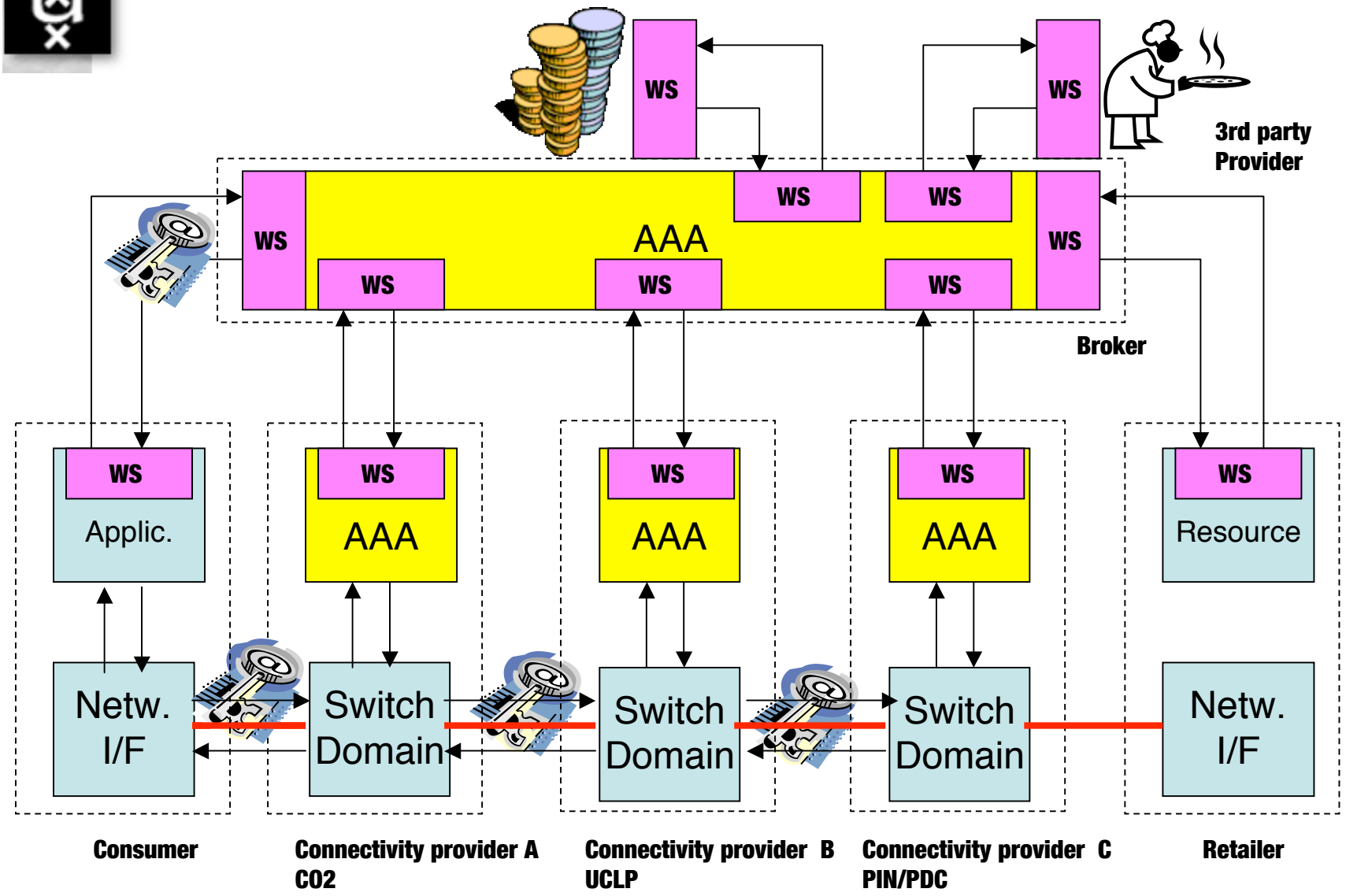
Collaborative Multi-domain experiment at SC2003



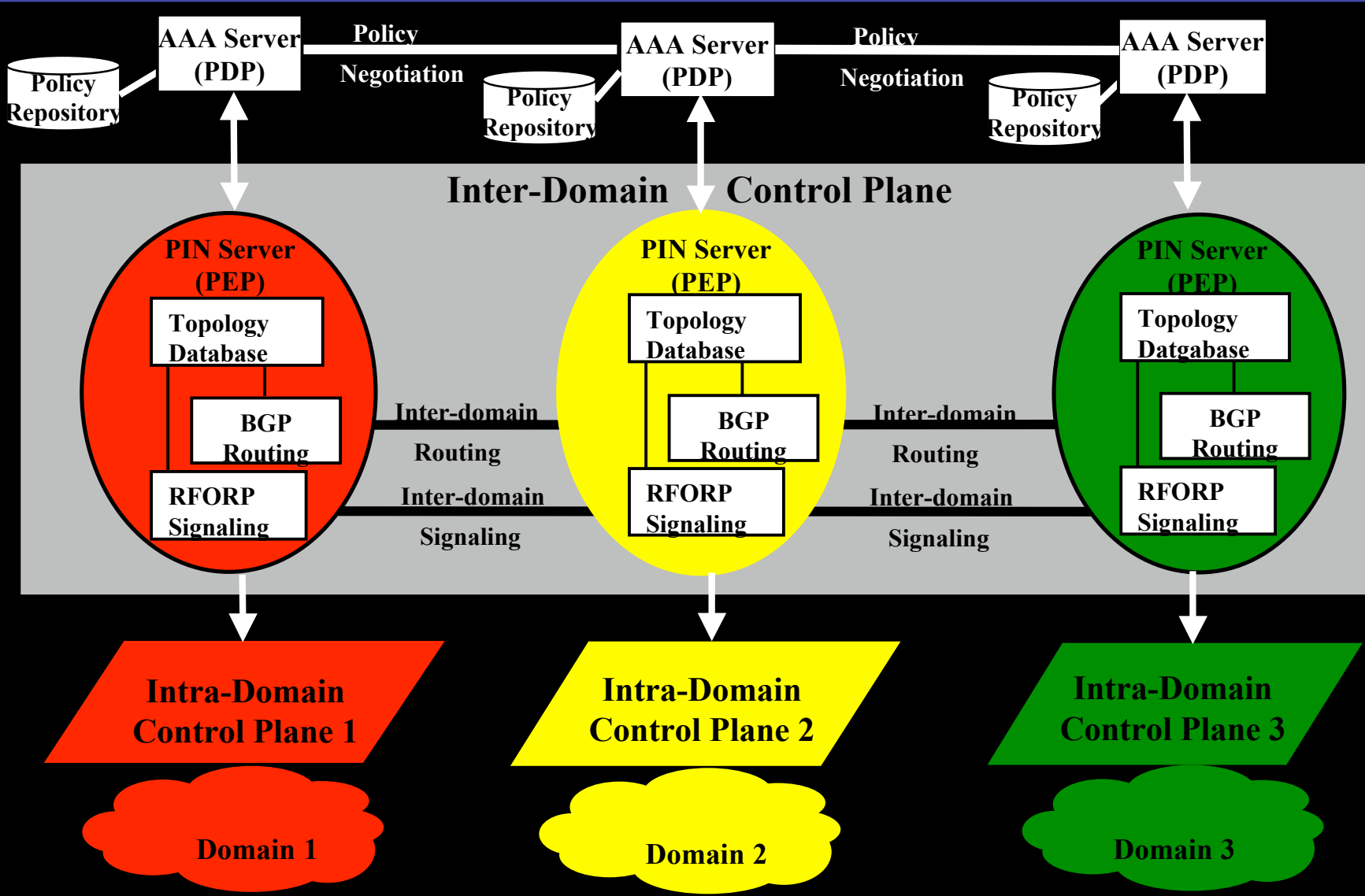
AAA based demo at SC2003



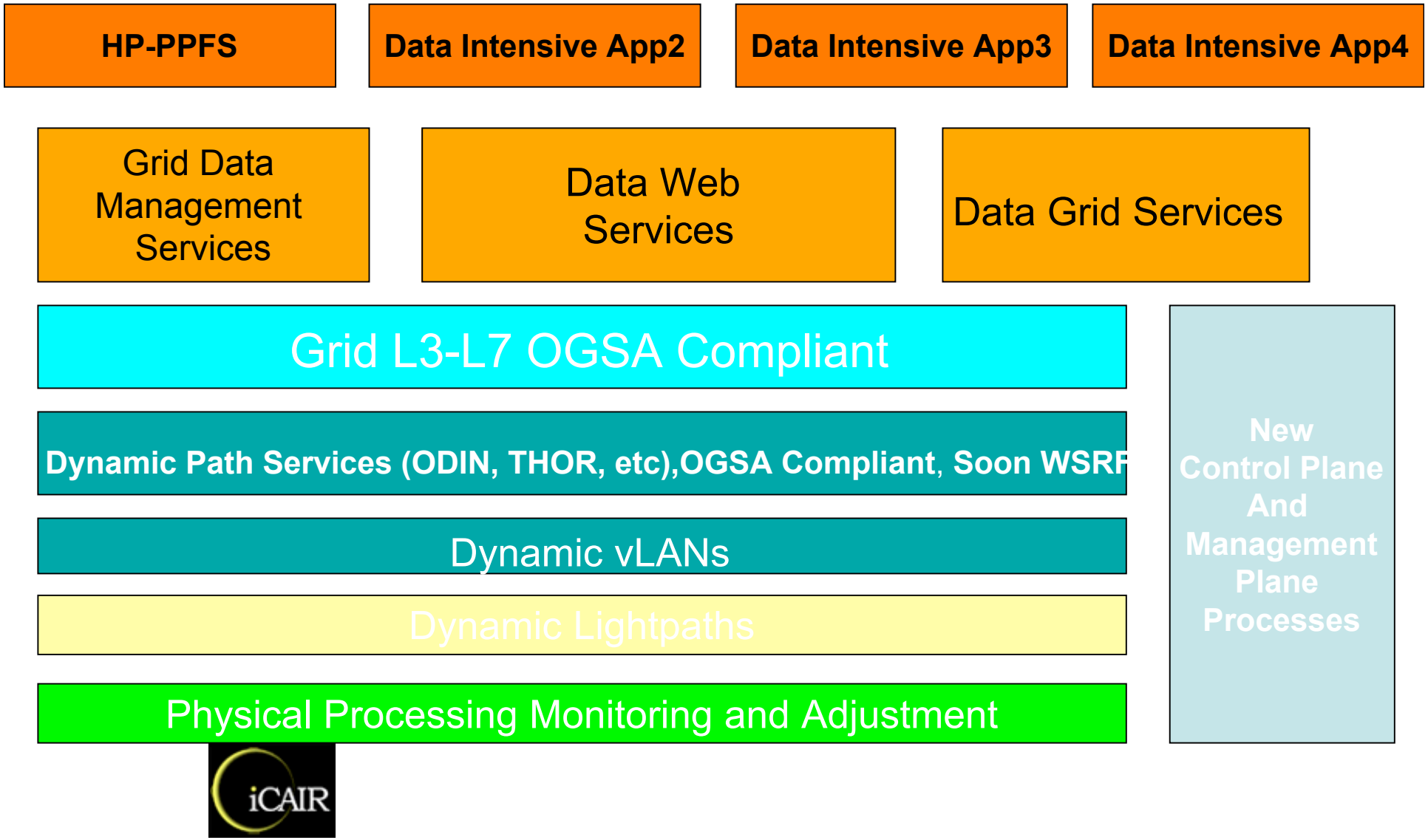
Research idea: WS/Token based TINA like model.



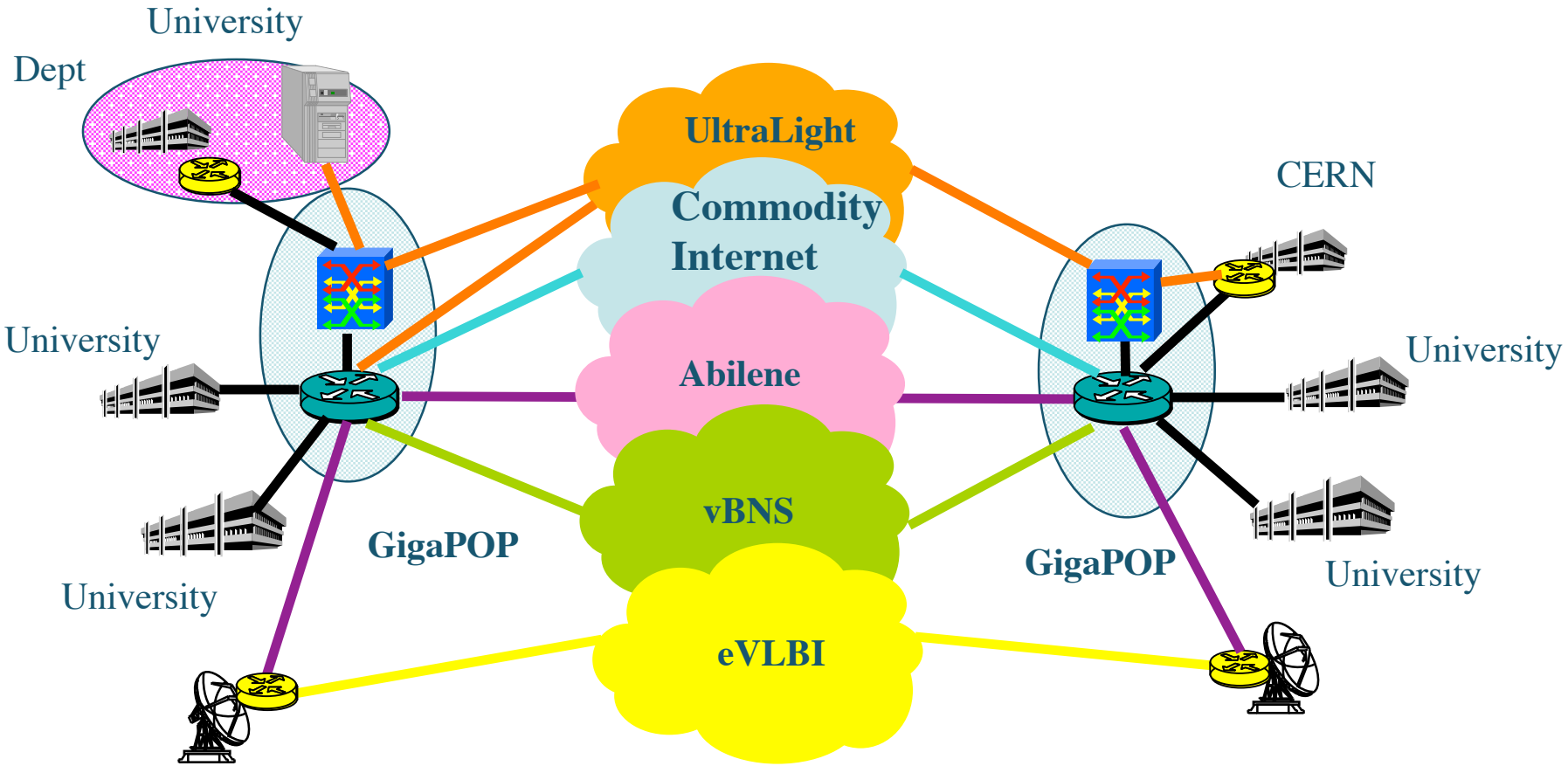
PIN Architecture



DARPA DWDM-RAM Large Scale Data+Dynamic Lambdas – Demonstrated at GGF9 & SC2003

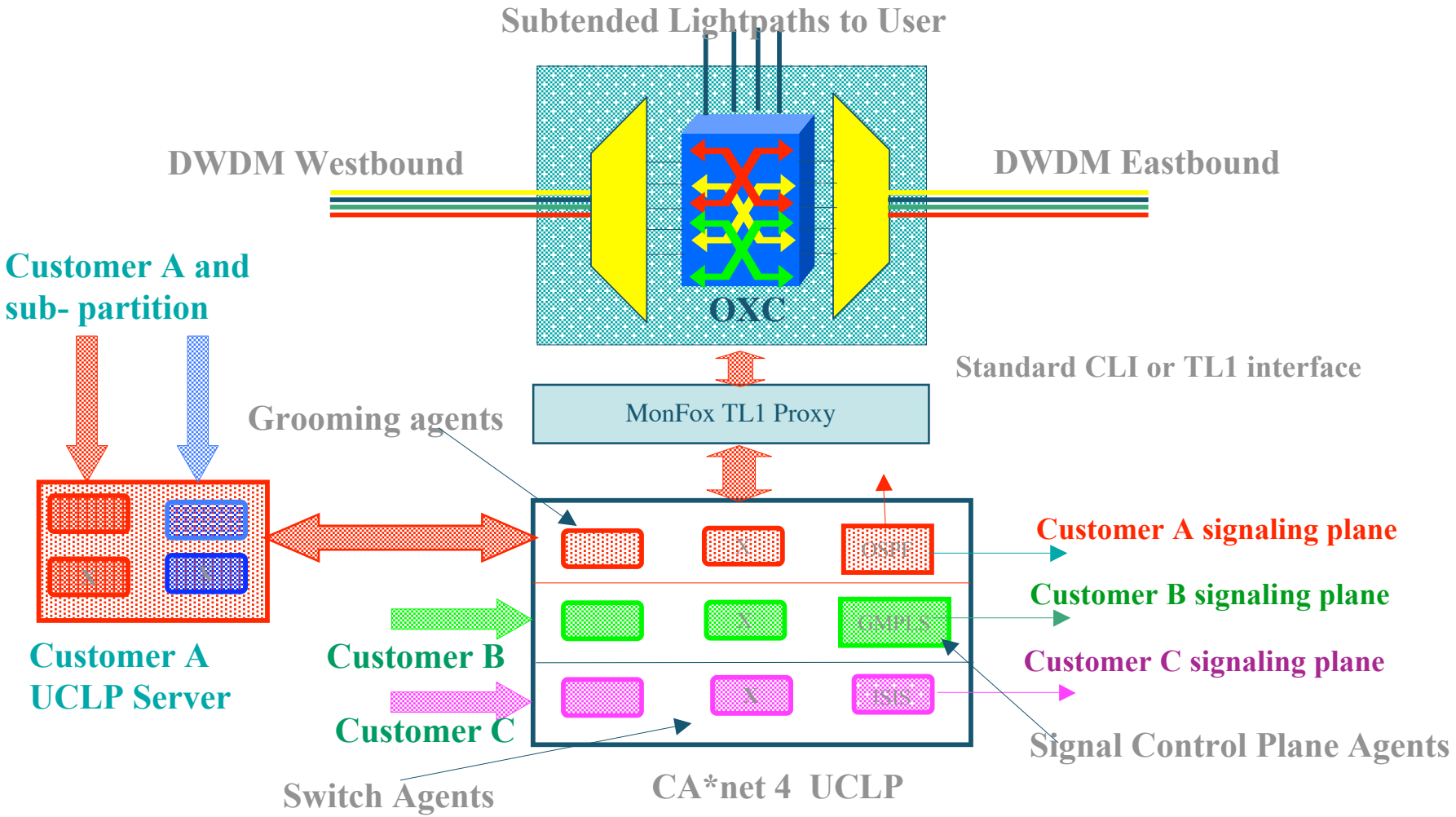


CA*net 4 == Internet 3?

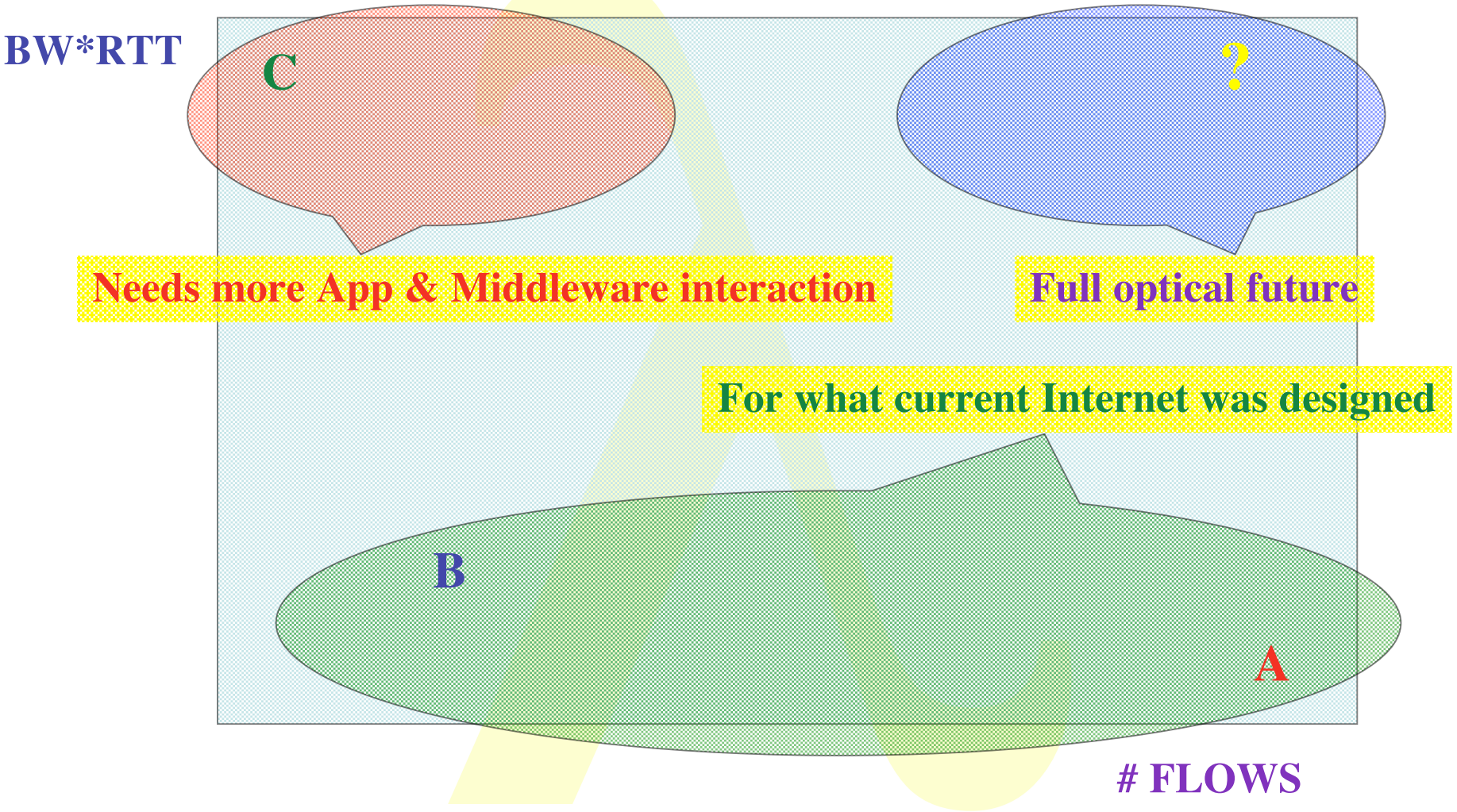


Only possible with DWDM network

UCLP general operation



Transport in the corners



The END

Thanks to

Kees Neggers, Tom DeFanti, Joel Mambretti, Bill St. Arnaud, Larry Smarr

John Vollbrecht,Freek Dijkstra, Hans Blom, Leon Gommans, Bas van oudenaarde, Arie Taal, Pieter de Boer, Bert Andree, Martijn de Munnik, Antony Antony, Rob Meijer, Yuri Demchenko,, David Groep, Oliver Yu, Franco Travestino, Bill St. Arnaud, John Vollbrecht, Eric He, Tom DiMaggio and many more .

Partially complete list:

Caas

Chase

Cess

Kess

Case

GigaPort

NWO/NCF

SURFnet