The Lambda Grid / AAA

www.science.uva.nl/~delaat

Cees de Laat

SURFnet

EU

University of Amsterdam

SARA

NIKHEF

NCF

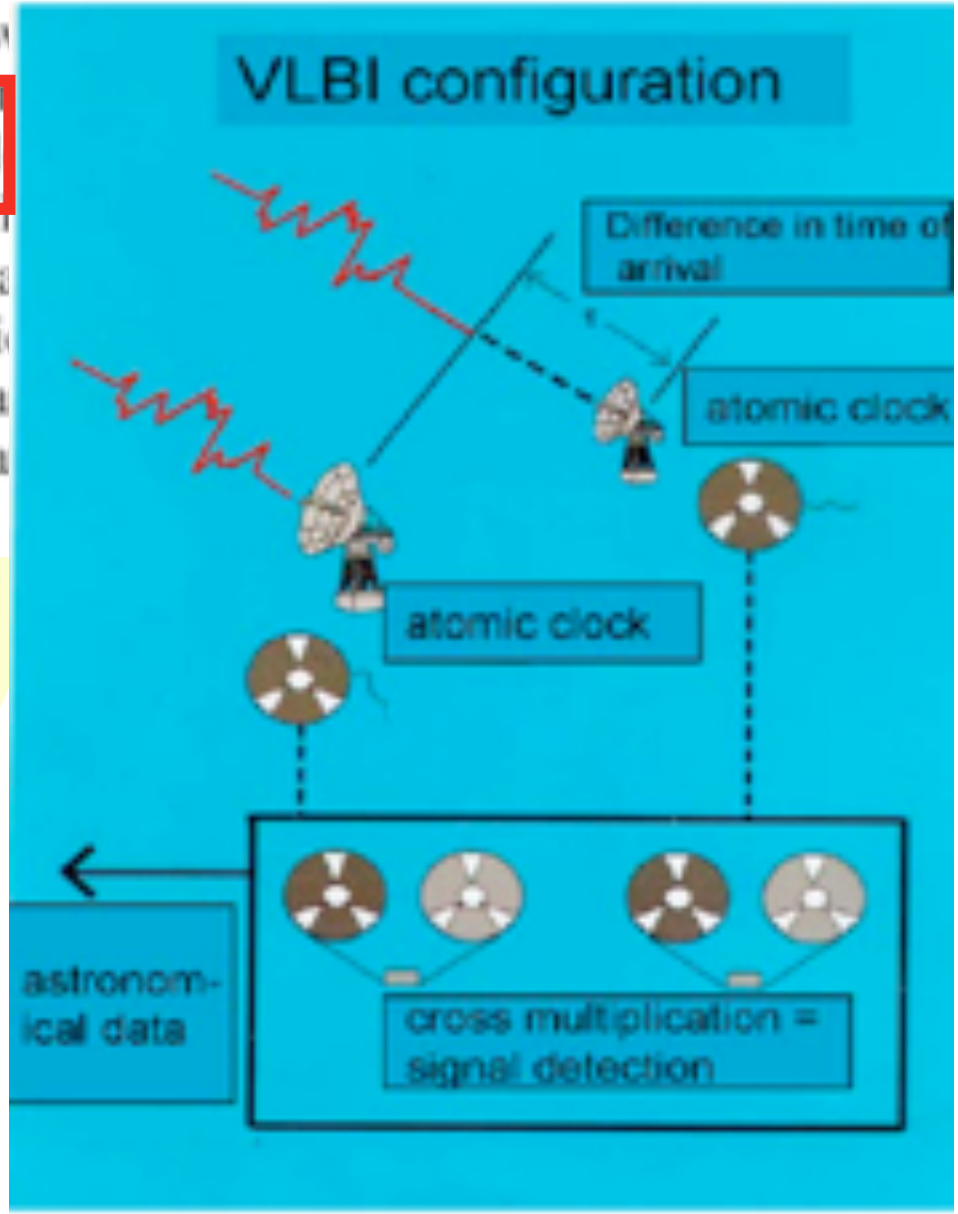
Talk contents

- Just wait 20 minutes

VLBI

ger term VLBI is easily capable of generating many Gb of data per
The sensitivity of the VLBI array scales w
(data-rate) and there is a strong push to
. Rates of 8Gb/s or more are entirely feasibl
der development. It is expected that parall
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



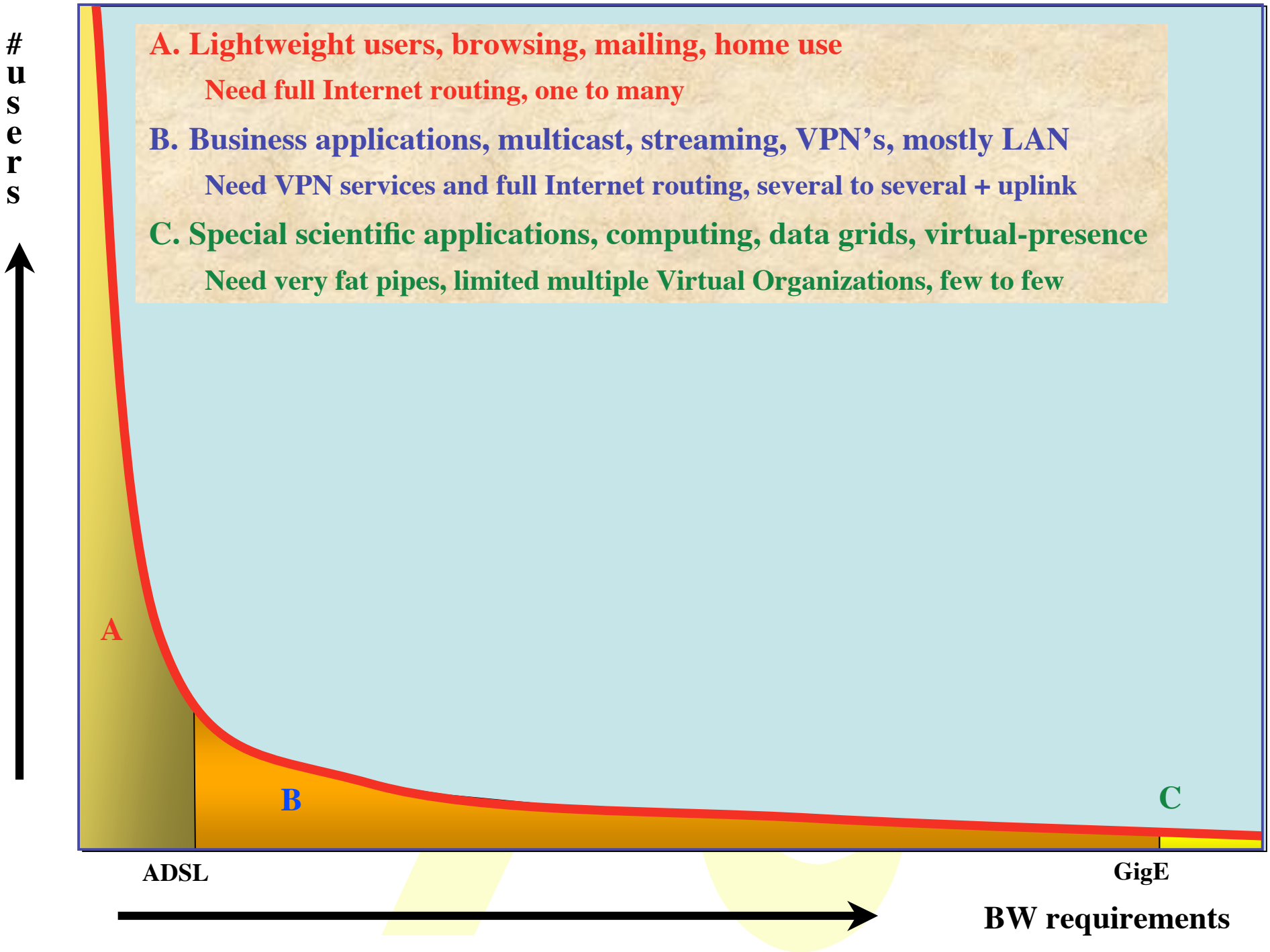
Lambdas as part of instruments

GigaPort

LOFAR

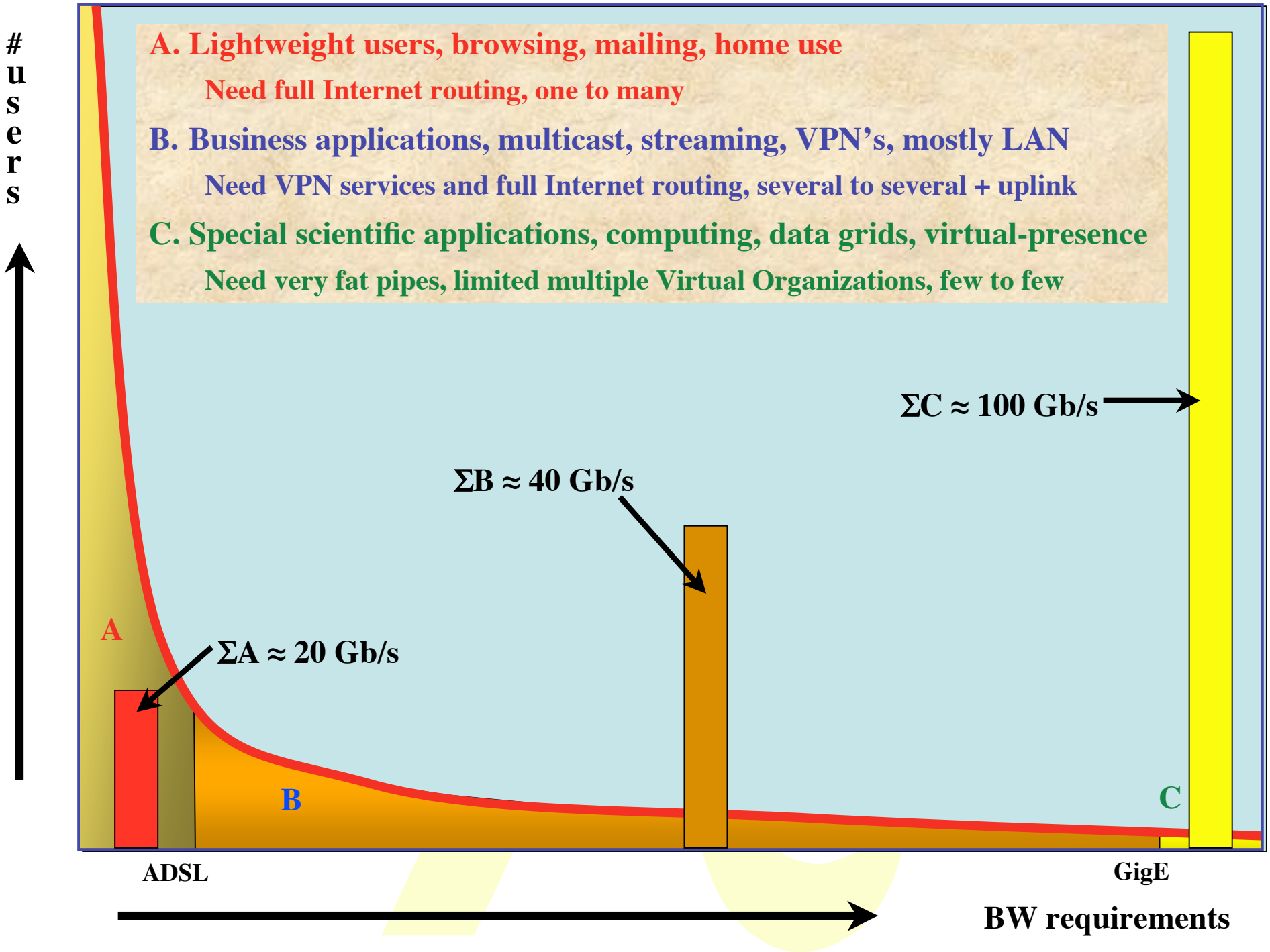
www.lofar.org

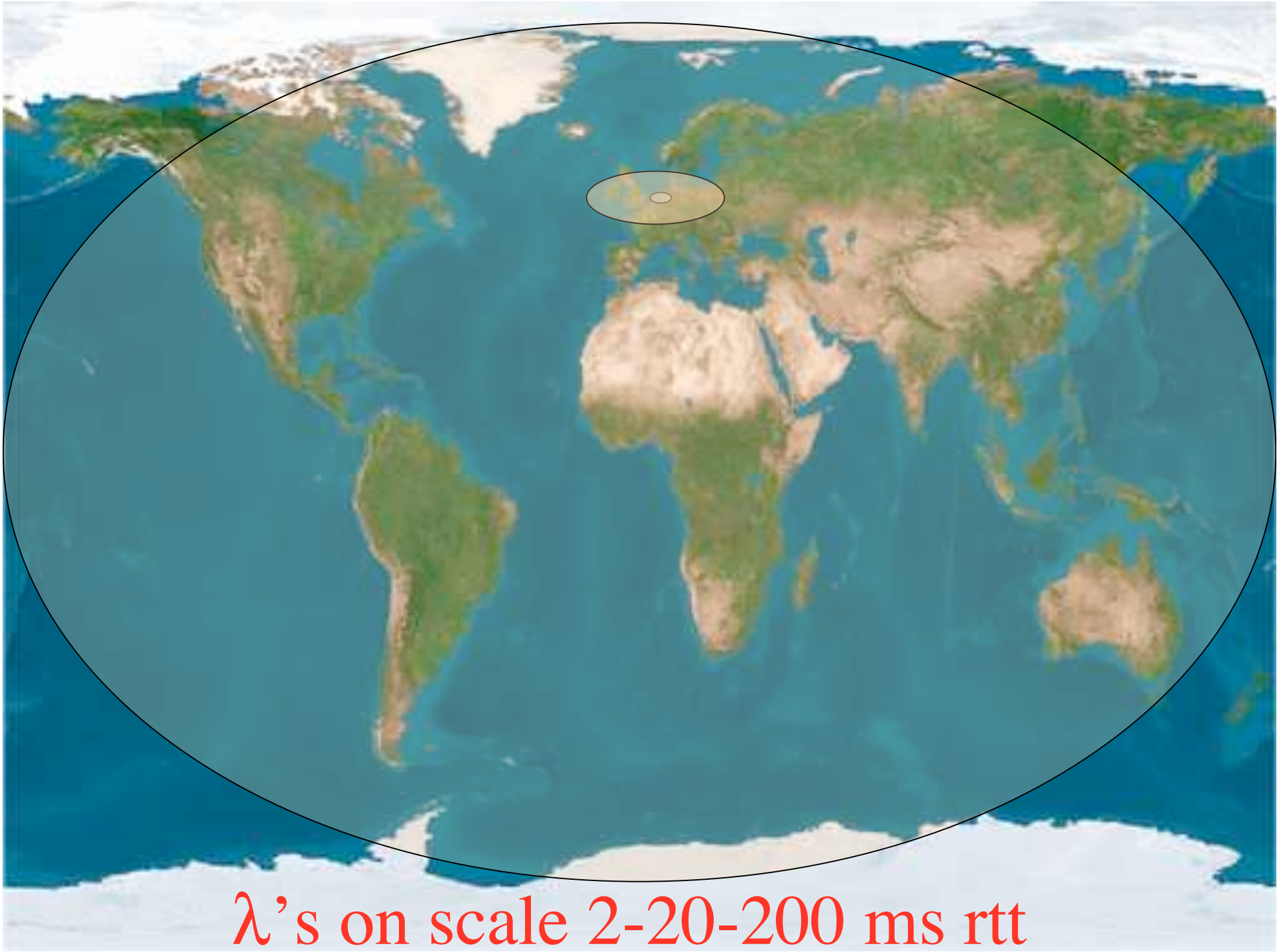
SURFnet


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
A
B
C
ADSL
GigE
BW requirements

The Dutch Situation

- **Estimate A**
  - **17 M people, 6.4 M households, 25 % penetration of 0.5 Mb/s ADSL, 40 times under-provisioning ==> 20 Gb/s**
- **Estimate B**
  - **SURFnet has 10 Gb/s to about 12 institutes and 0.1 to 1 Gb/s to 180 customers, estimate same for industry (overestimation) ==> 20-40 Gb/s**
- **Estimate C**
  - **Leading HEF and ASTRO + rest ==> 80-120 Gb/s**
  - **LOFAR ==> 20 TByte/s**

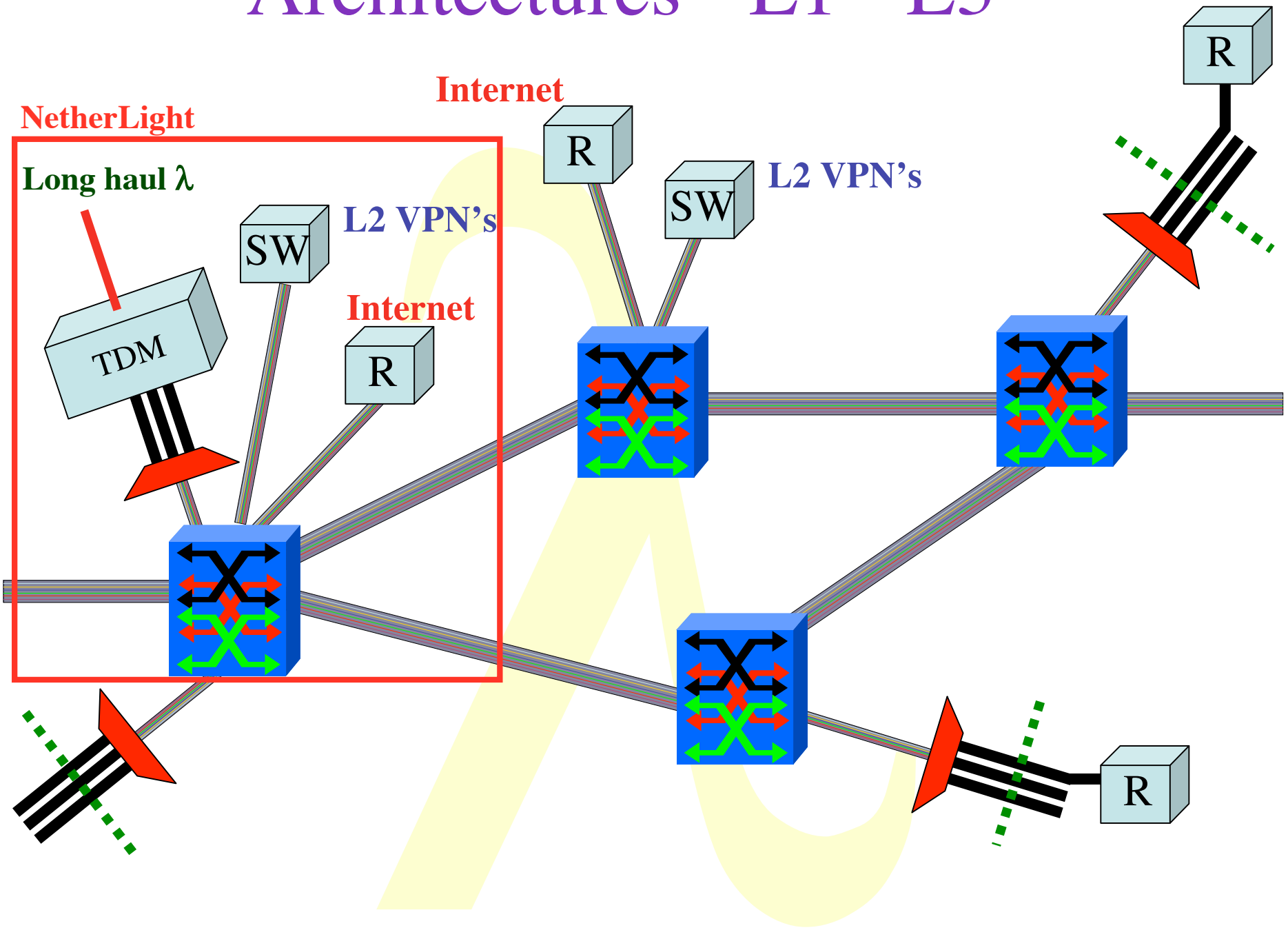

A. Lightweight users, browsing, mailing, home use
Need full Internet routing, one to many
B. Business applications, multicast, streaming, VPN's, mostly LAN
Need VPN services and full Internet routing, several to several + uplink
C. Special scientific applications, computing, data grids, virtual-presence
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


λ's on scale 2-20-200 ms rtt

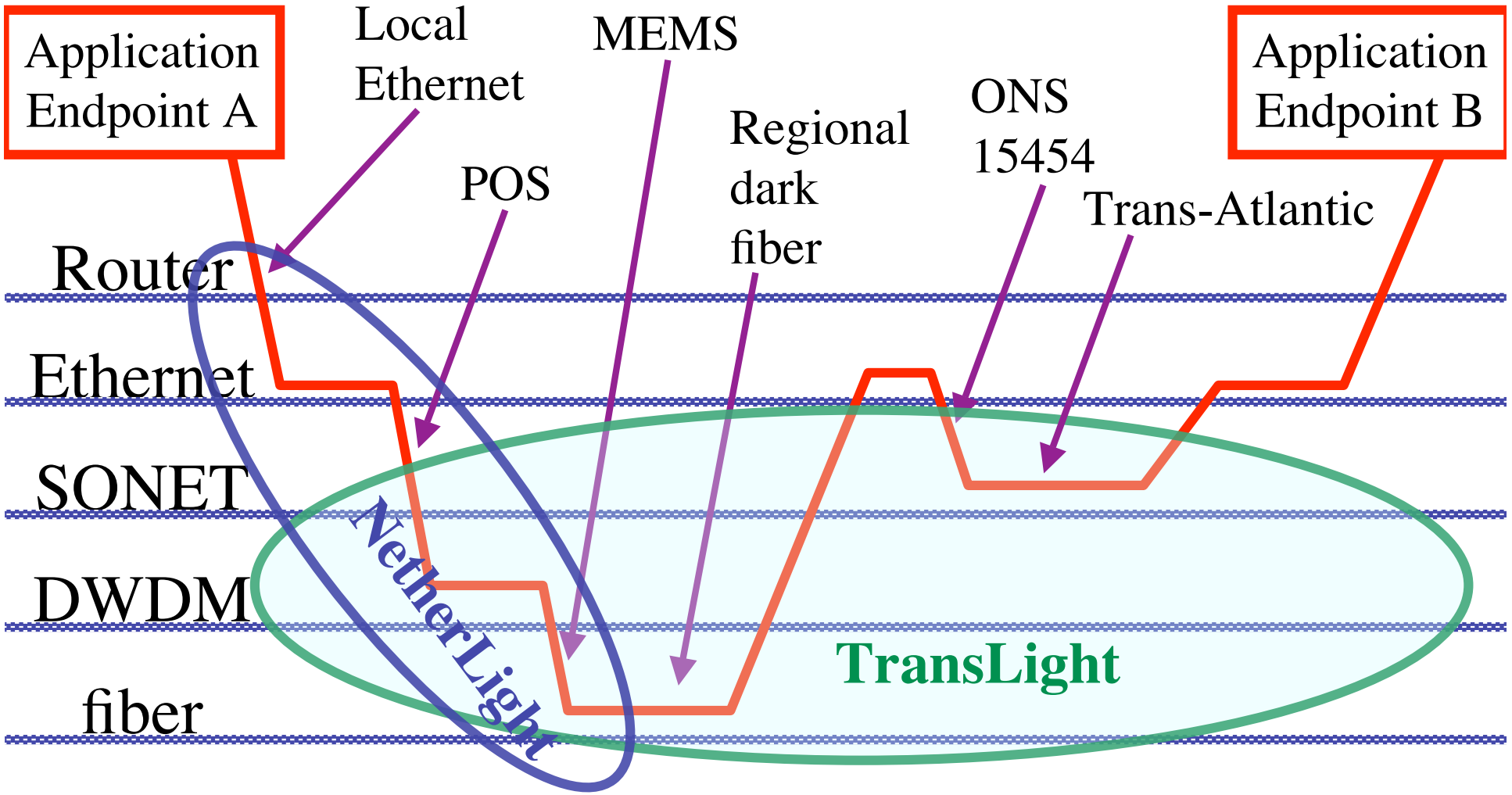
Services

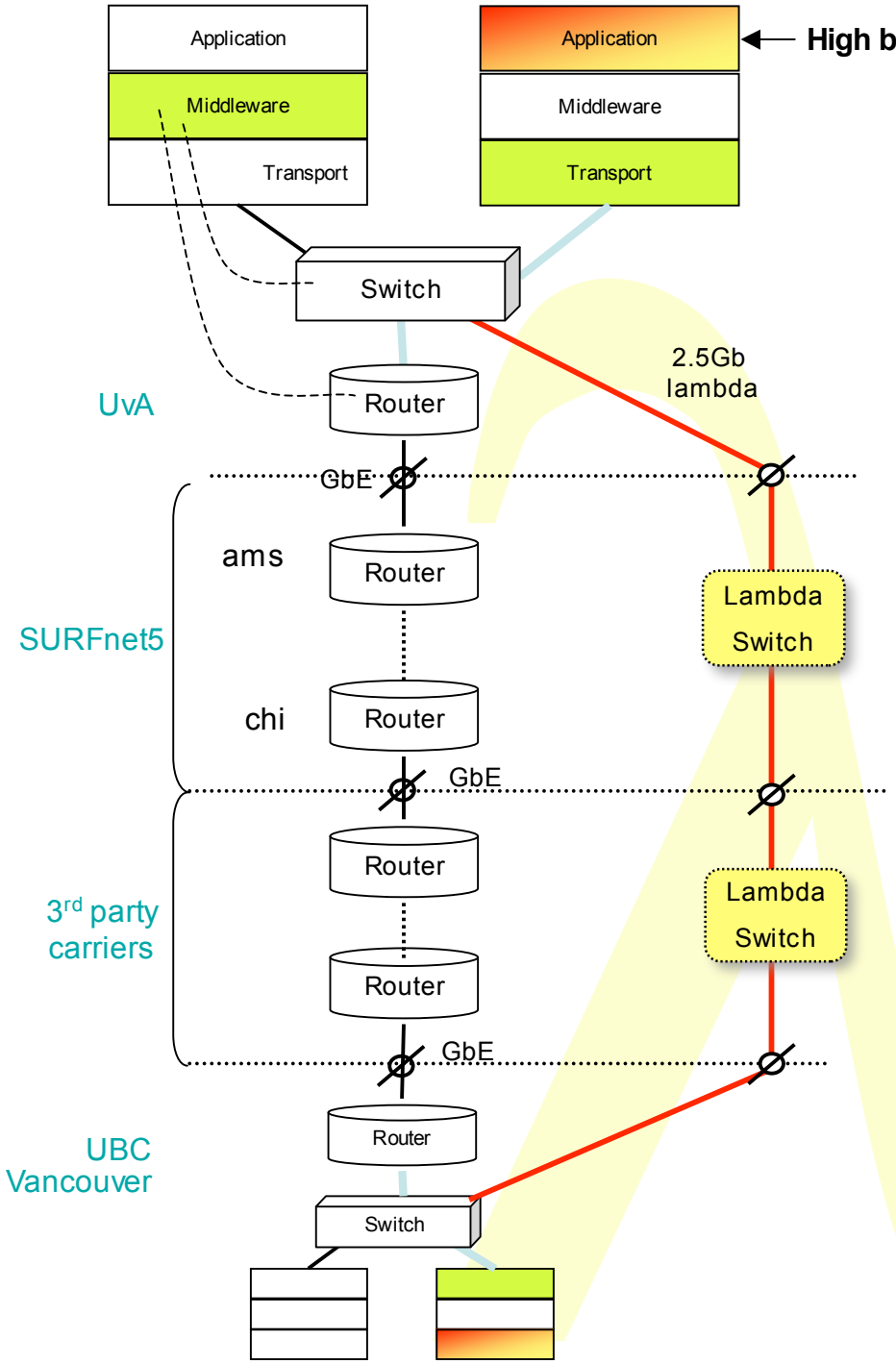
SCALE / CLASS	2 Metro	20 National/ regional	200 World
A	Switching/ routing	Routing	ROUTER$
B	Switches + E-WANPHY VPN's,	Switches + E-WANPHY (G)MPLS	ROUTER$
C	dark fiber Optical switching	Lambda switching	Sub- lambdas, ethernet-sdh

Architectures - L1 - L3



How low can you go?





- 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!

IRTF - AAAARCH - RG

Authentication Authorisation Accounting ARCHitecture RG

chairs:

C. de Laat and J. Vollbrecht

www.aaaarch.org

RFC 2903, 2904, 2905, 2906, 3334

History & Charter

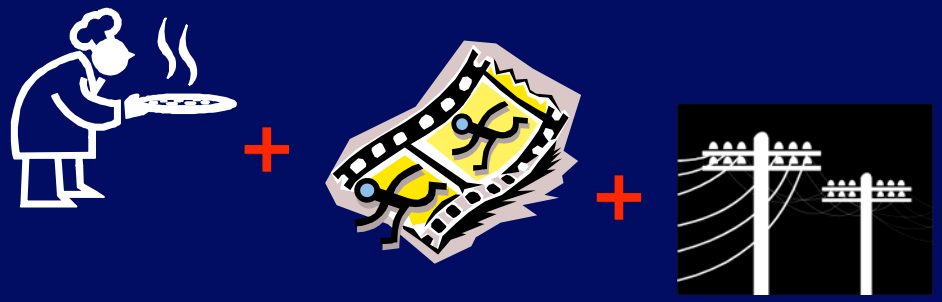
- Authorization subgroup of AAA-WG
- Commonality in authorization space
- Tie in policy from all WG's
- IRTF-RG chartered in Dec 1999
  - This RG will work to define a next generation AAA architecture that incorporates a set of interconnected "generic" AAA servers and an application interface that allows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

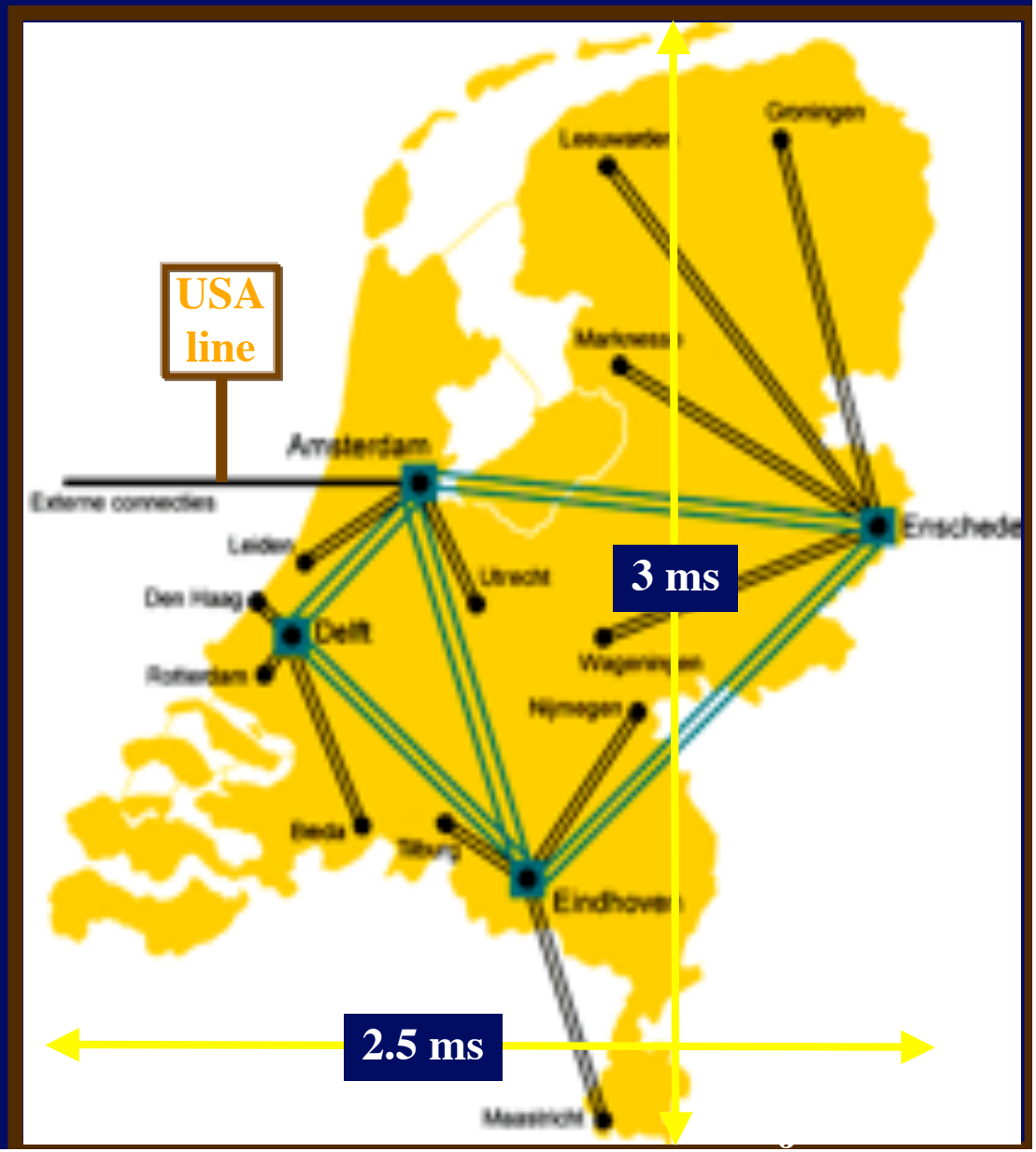
Basic AAA

- **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)

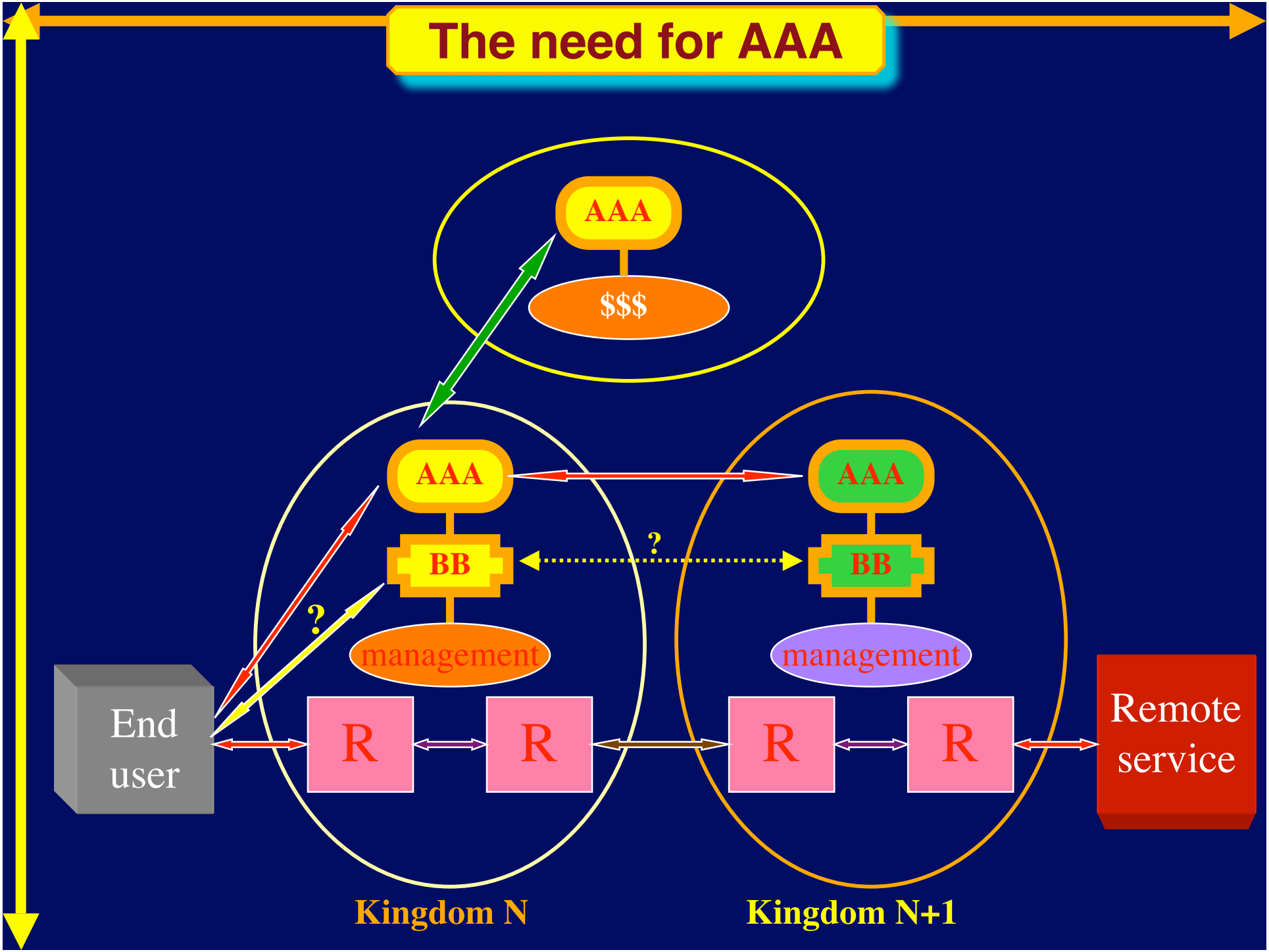
Multi Kingdom Problem

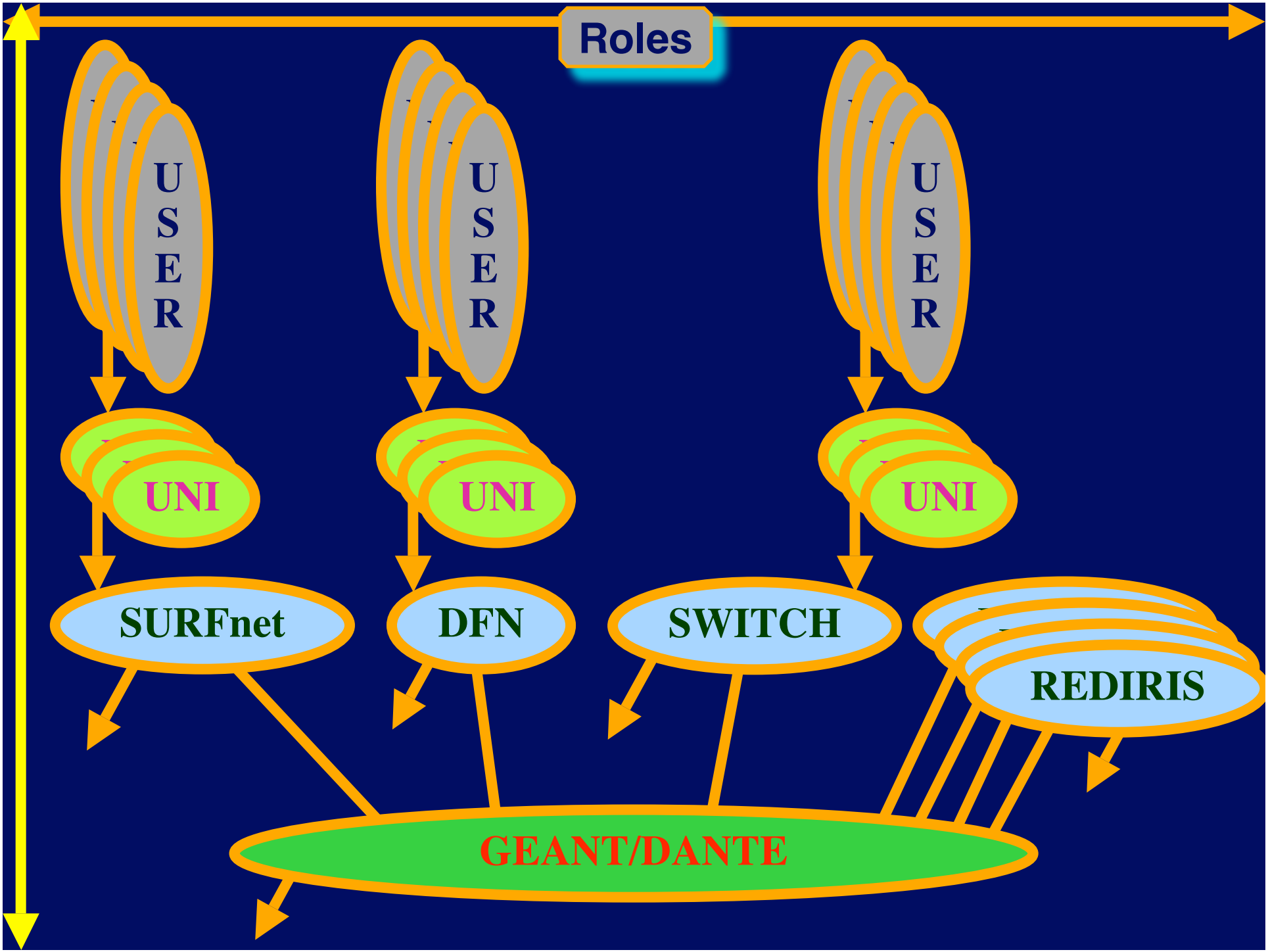
Physics-UU to IPP-FZJ => 7 kingdoms

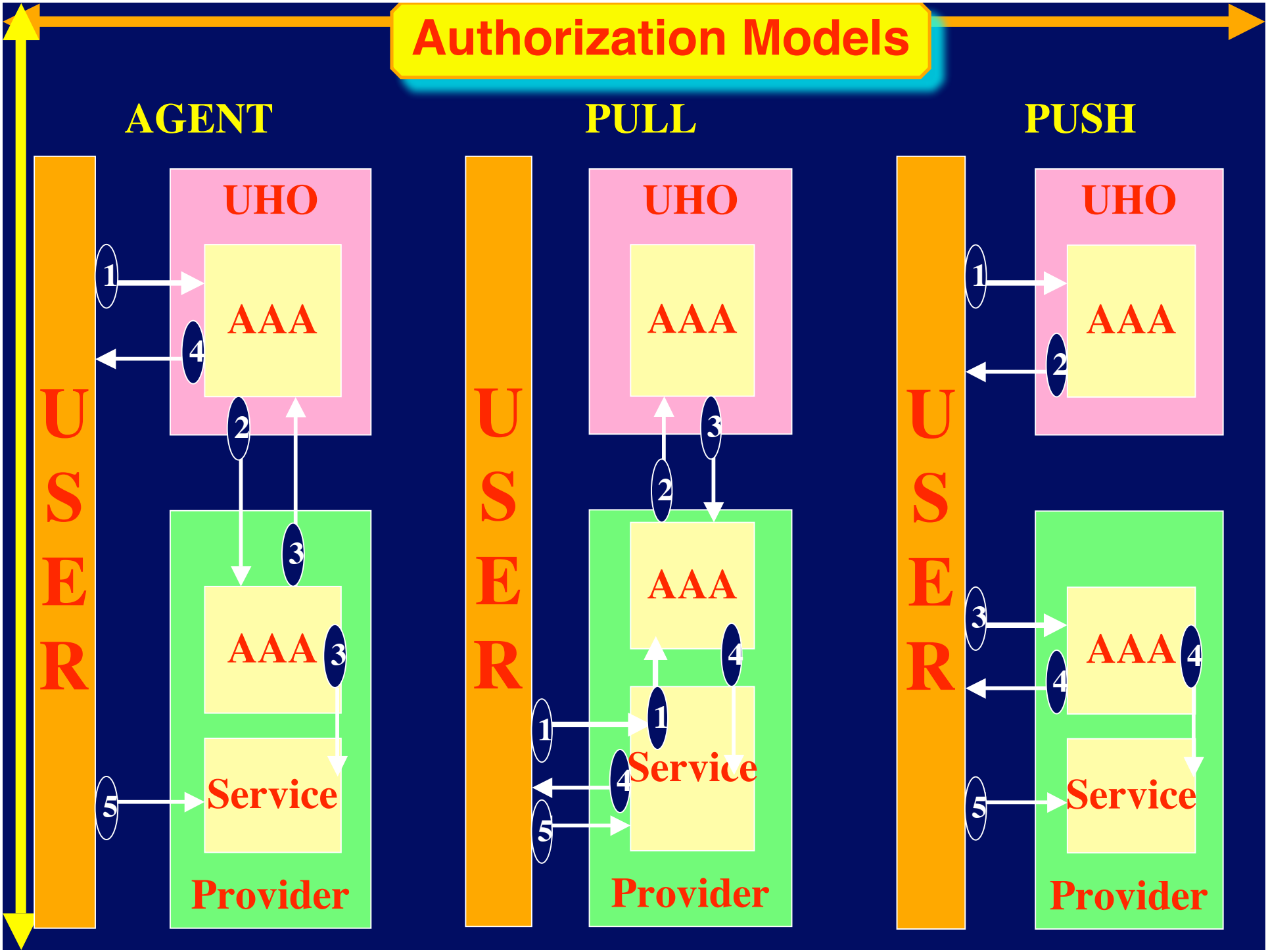
- Netherlands
  - »Physics dept
  - »Campus net
  - »SURFnet
- Europe
  - »GEANT
- Germany
  - »WINS/DFN
  - »Juelich, Campus
  - »Plasma Physics dept

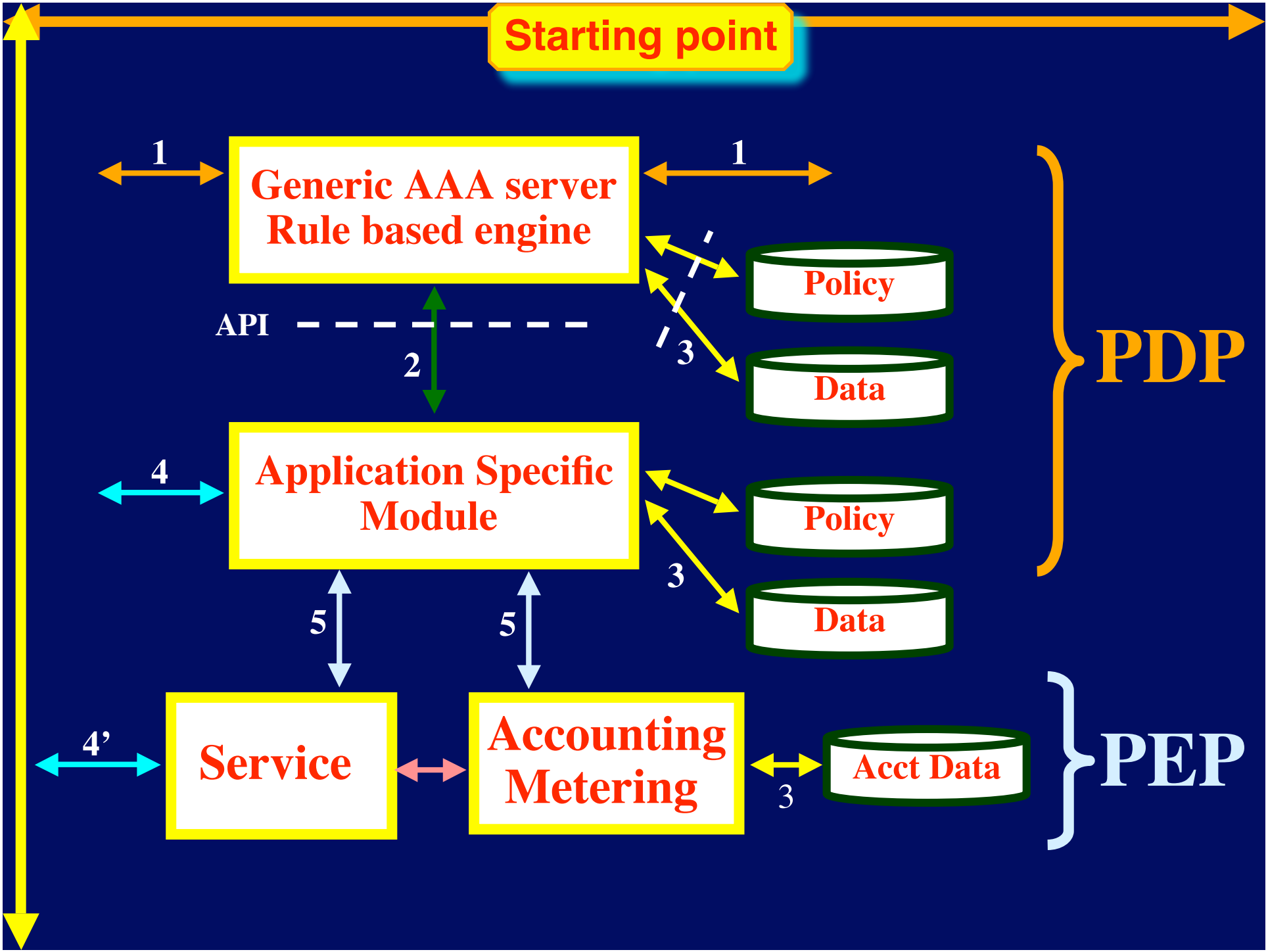


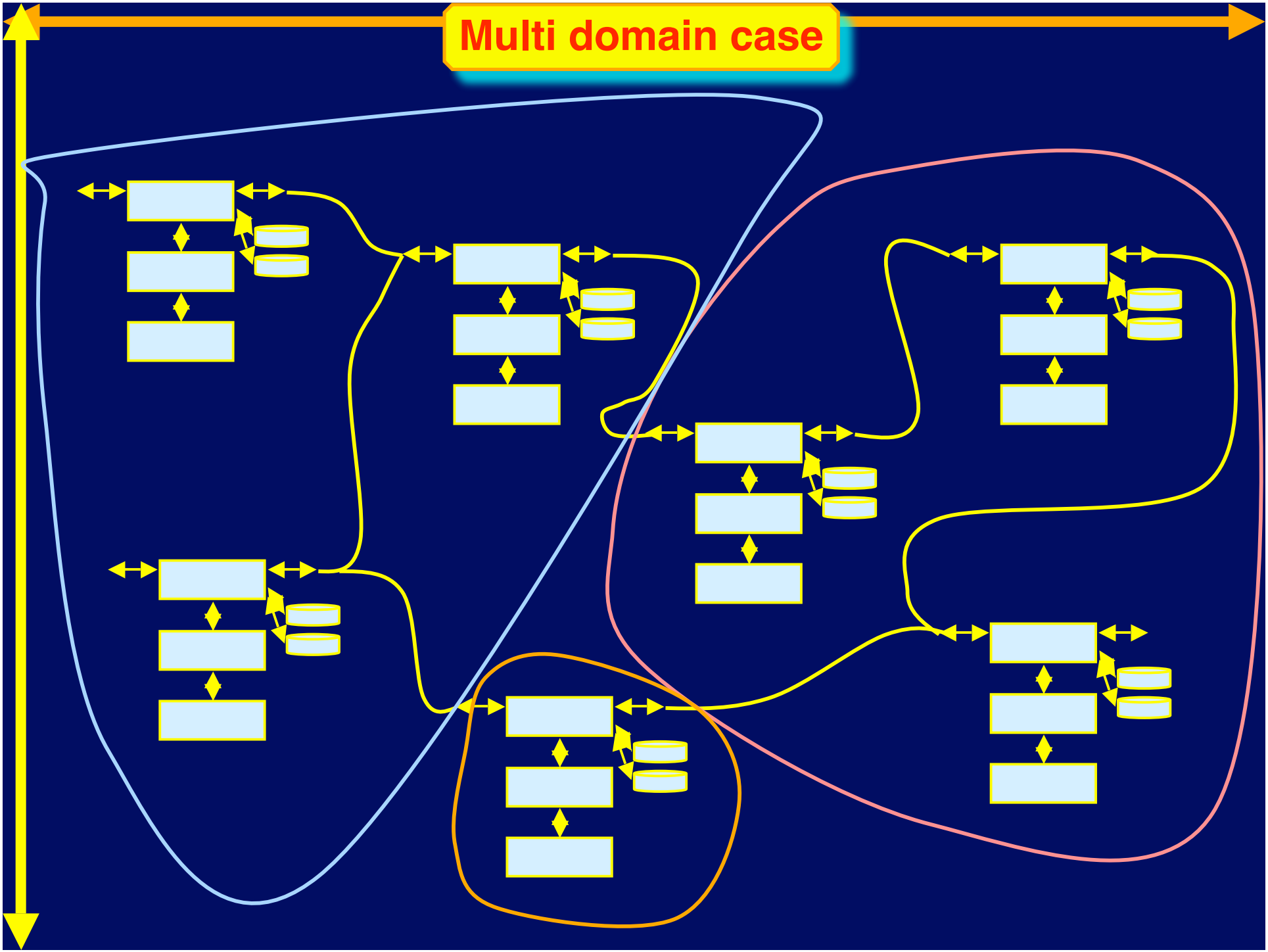
The need for AAA




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


Multi domain case

Example BoD request

```
<AAA:AAARequest
   xmlns:AAA="http://www.aaaarch.org/ns/AAA_BoD"
   xmlns:xsi ="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.aaaarch.org/ns/AAA_BoD
                http://169.254.0.1/LambdaBoDRequest.xsd"
                version="0.1" type="LambdaBoDCross" >
   <Authentication>
      <Signature>17520</Signature>
      <User>Joe</User>
   </Authentication>
   <Authorization>
      <CredentialID>7531</CredentialID>
   </Authorization>
   <BoDData>
      <Source>
         <Hostname>hp2</Hostname>
         <OXCName>BeautyCees</OXCName>
         <OXCDomain>NetherLight</OXCDomain>
         <OXCPort>2</OXCPort>
      </Source>
      <Destination>
          <Hostname>scyalla5</Hostname>
          <OXCName>CHI</OXCName>
          <OXCDomain>StarLight</OXCDomain>
          <OXCPort>2</OXCPort>
      </Destination>
      <Bandwidth>1000</Bandwidth>
      <StartTime>now</StartTime>
      <Duration>20</Duration>
   </BoDData>
</AAA:AAARequest>
```

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

Research Group - info

- **Research Group Name:**
  - AAAARCH - RG
- **Chair(s)**
  - John Vollbrecht -- jrv@interlinknetworks.com
  - Cees de Laat -- delaat@science.uva.nl
- **Web page**
  - www.irtf.org
  - www.aaaarch.org
- **Next steps:**
  - Get drafts through last call and published
  - May well close down after the current drafts are published as experimental RFC's
  - Carry over the work in the GGF

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.

Partially complete list:

Caas

Chase

Cess

Kess

Case

NWO/NCF

SURFnet