IRTF - AAAARCH - RG

Authentication Authorisation Accounting ARCHitecture RG

chairs:

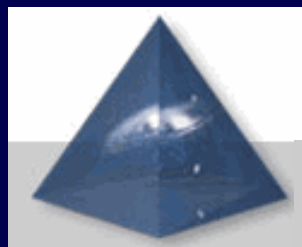
C. de Laat and J. Vollbrecht

www.aaaarch.org

RFC 2903, 2904, 2905, 2906, 3334

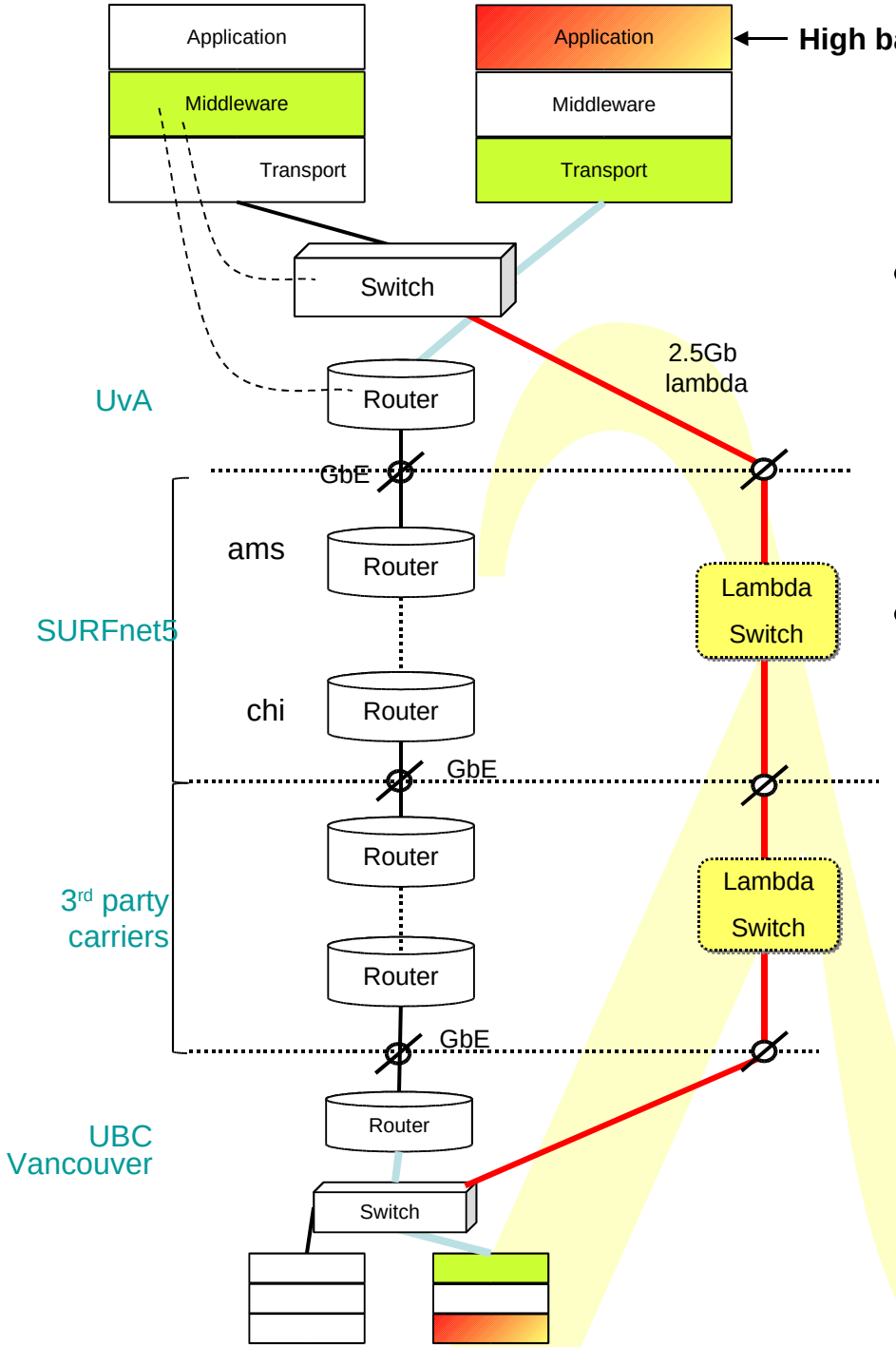
Contents of this talk

- This space is intentionally left blank



Except for:

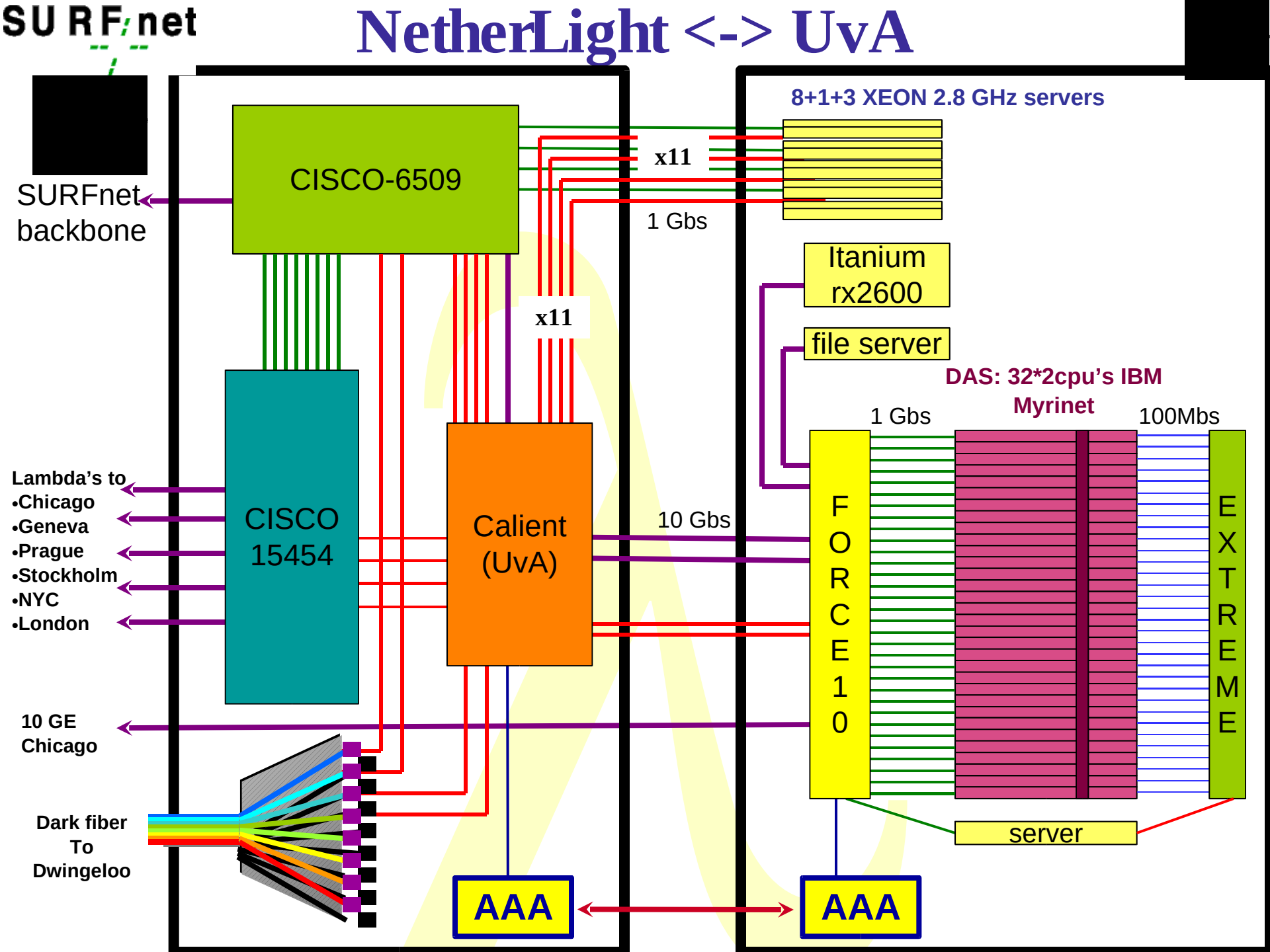
Faculty of Science



- 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!

QuickTime[a] and a Cinepak decompressor are needed to see this picture

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!

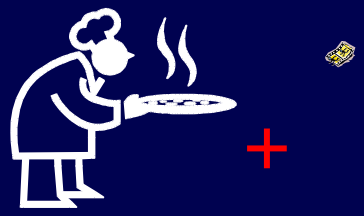
History & Charter

- 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

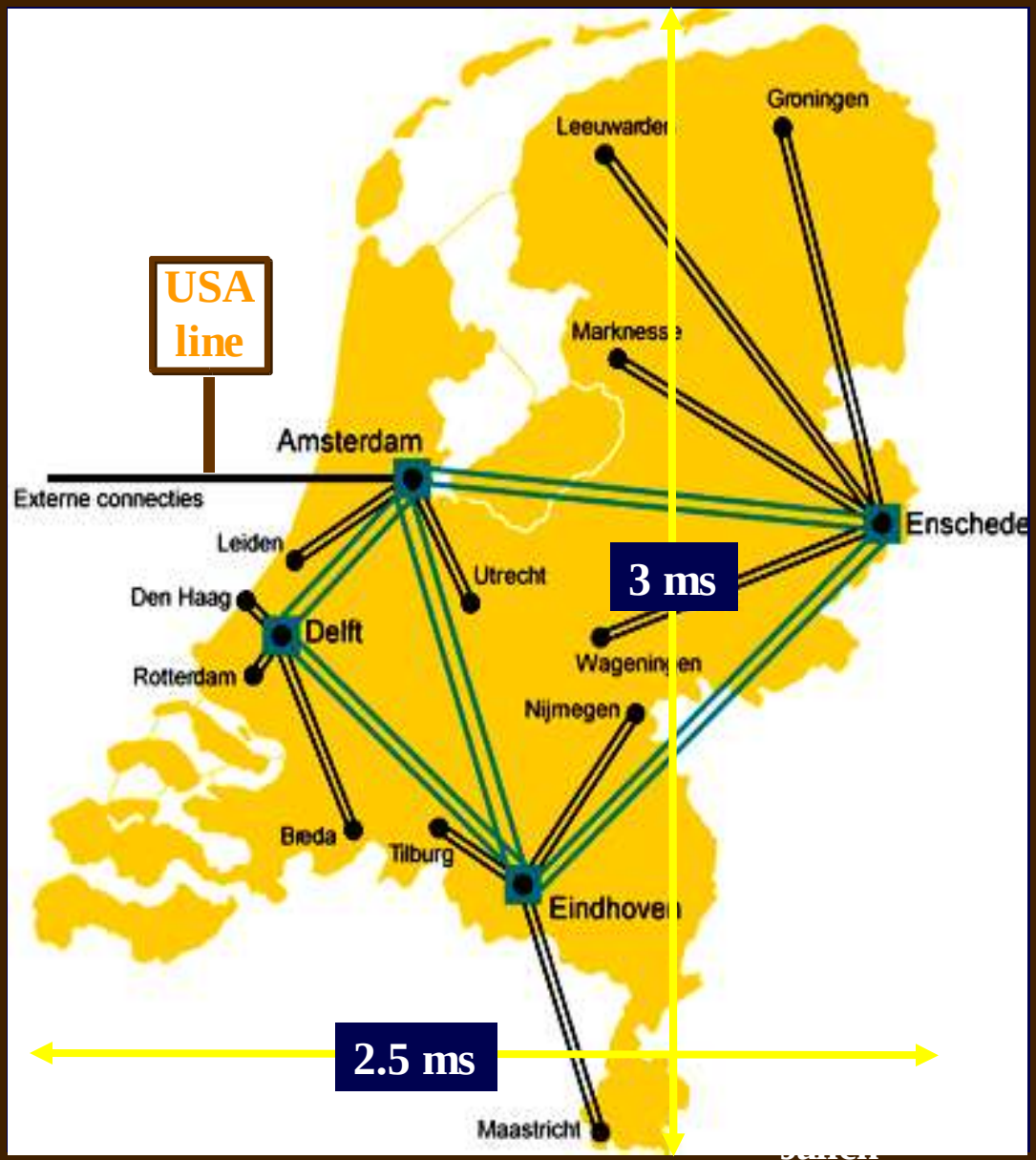
Basic AAA

- **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)

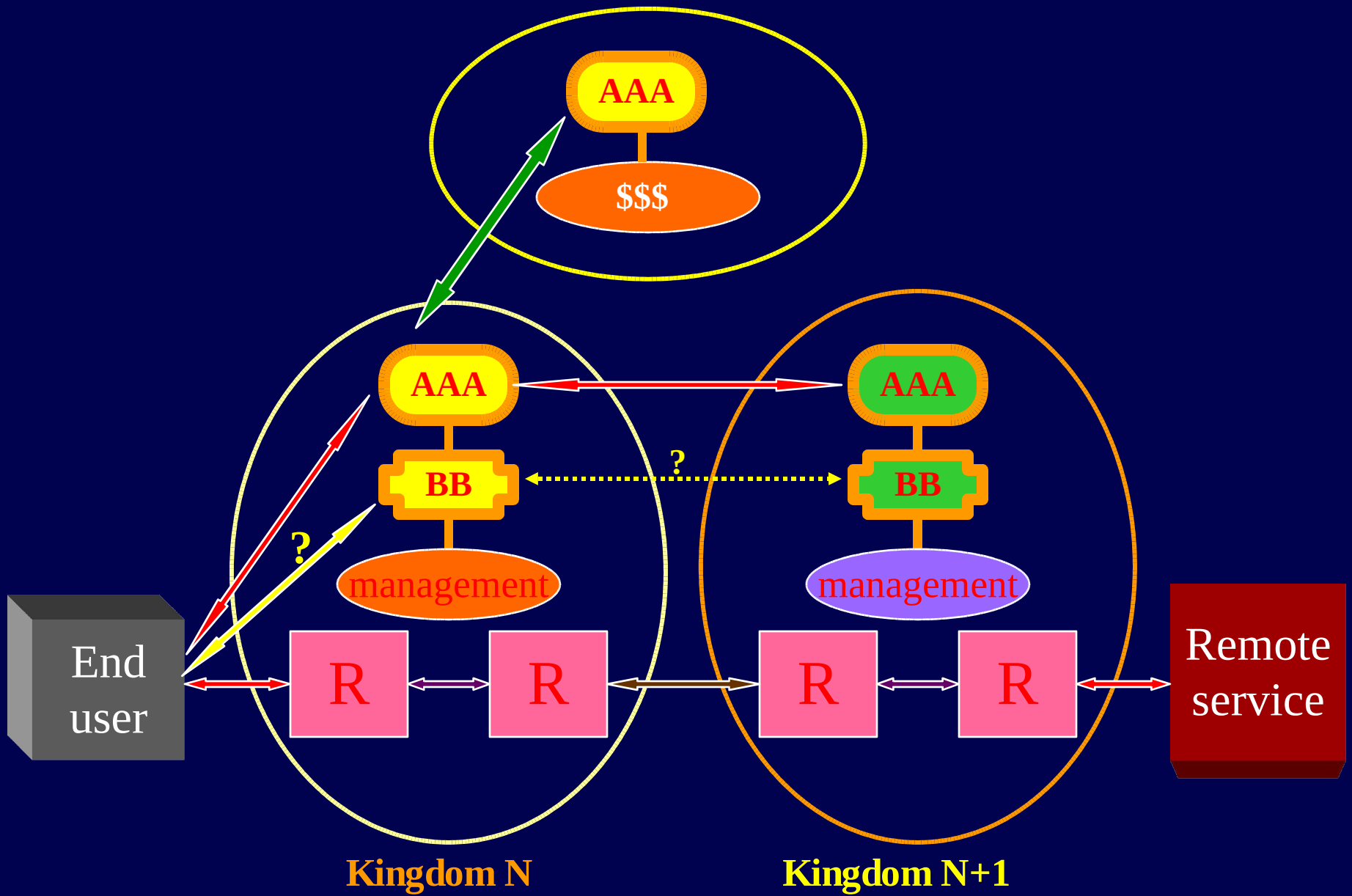
Multi Kingdom Problem

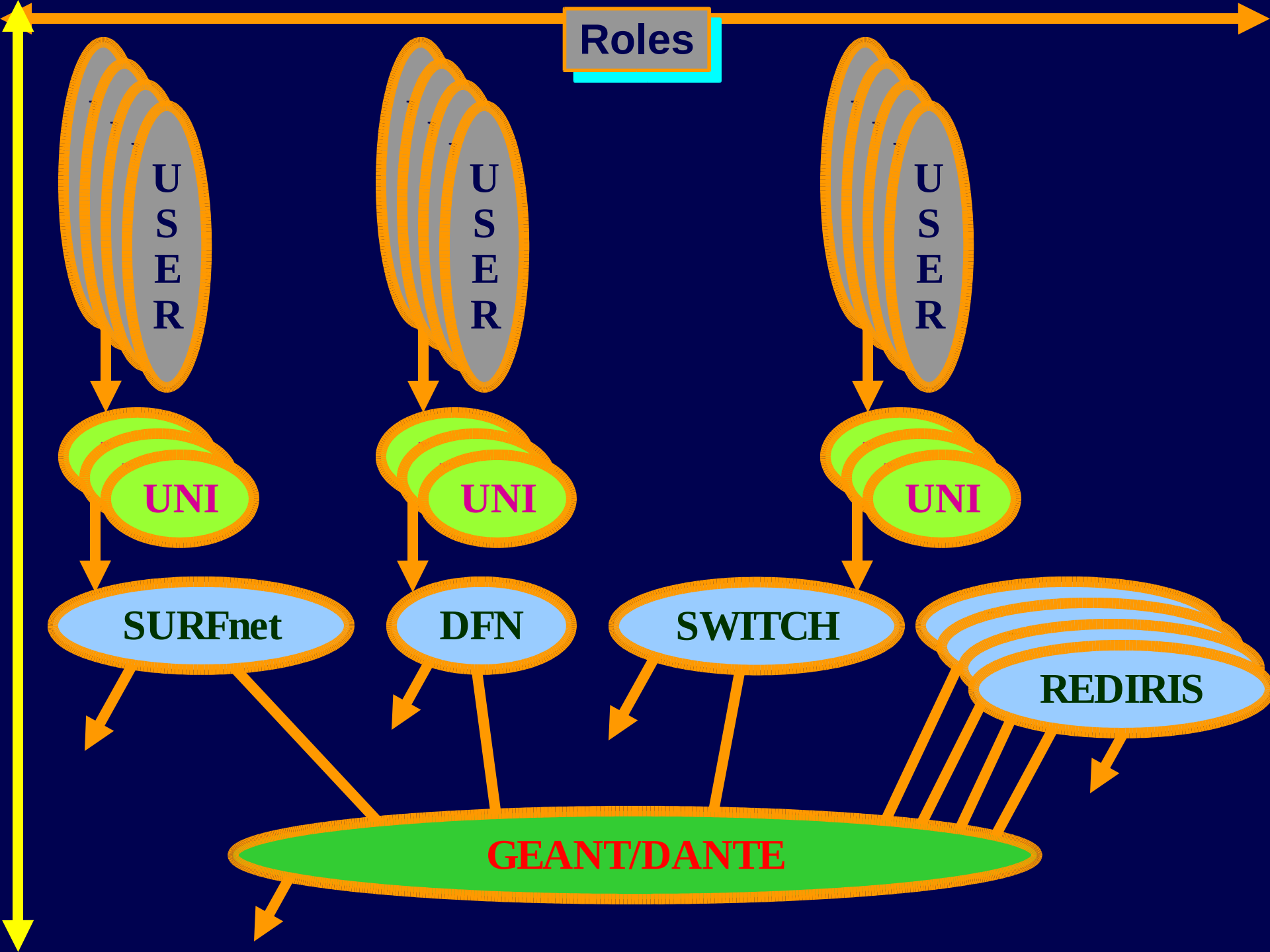
Physics-UU to IPP-FZJ => 7 kingdoms

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

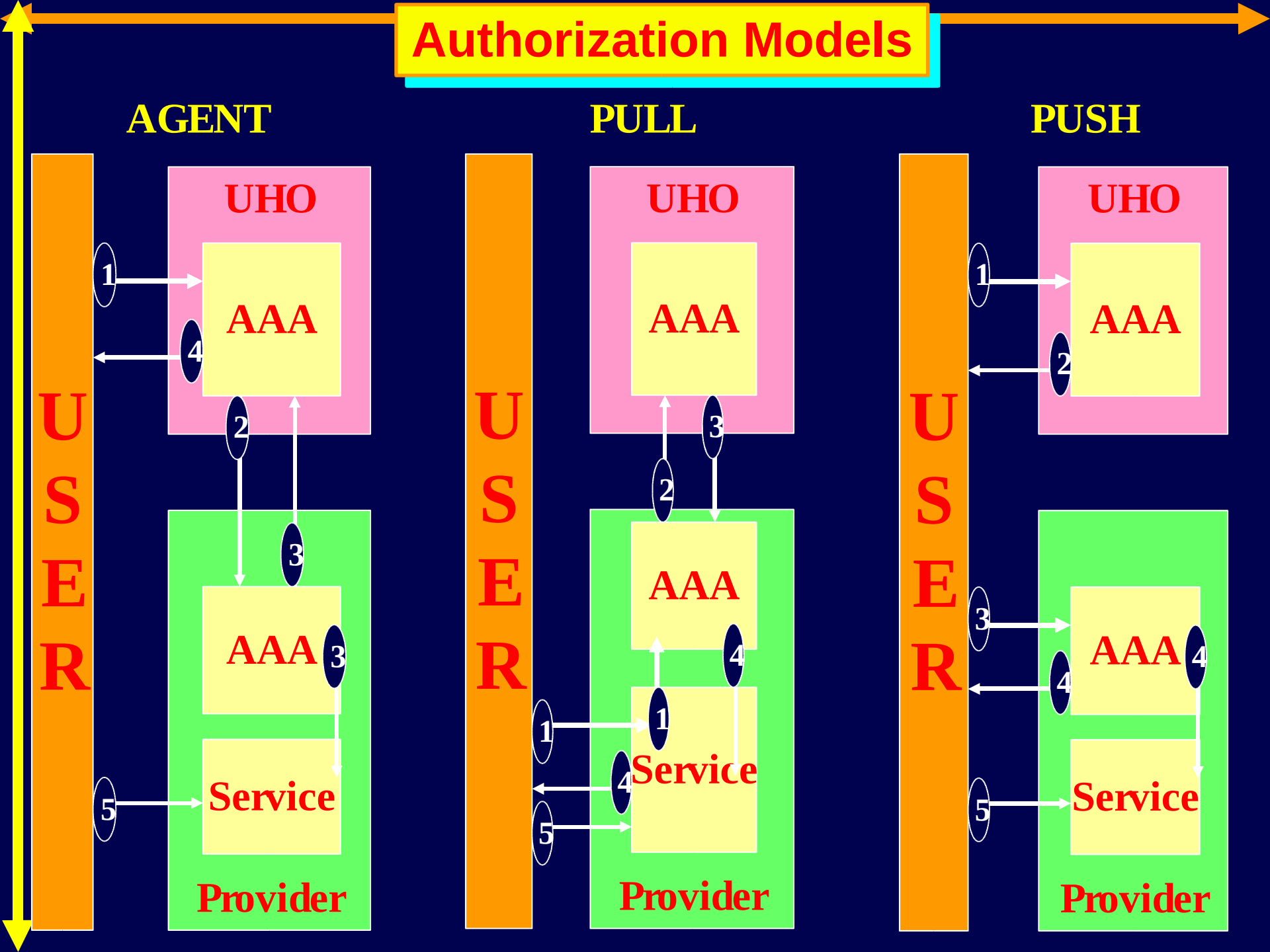


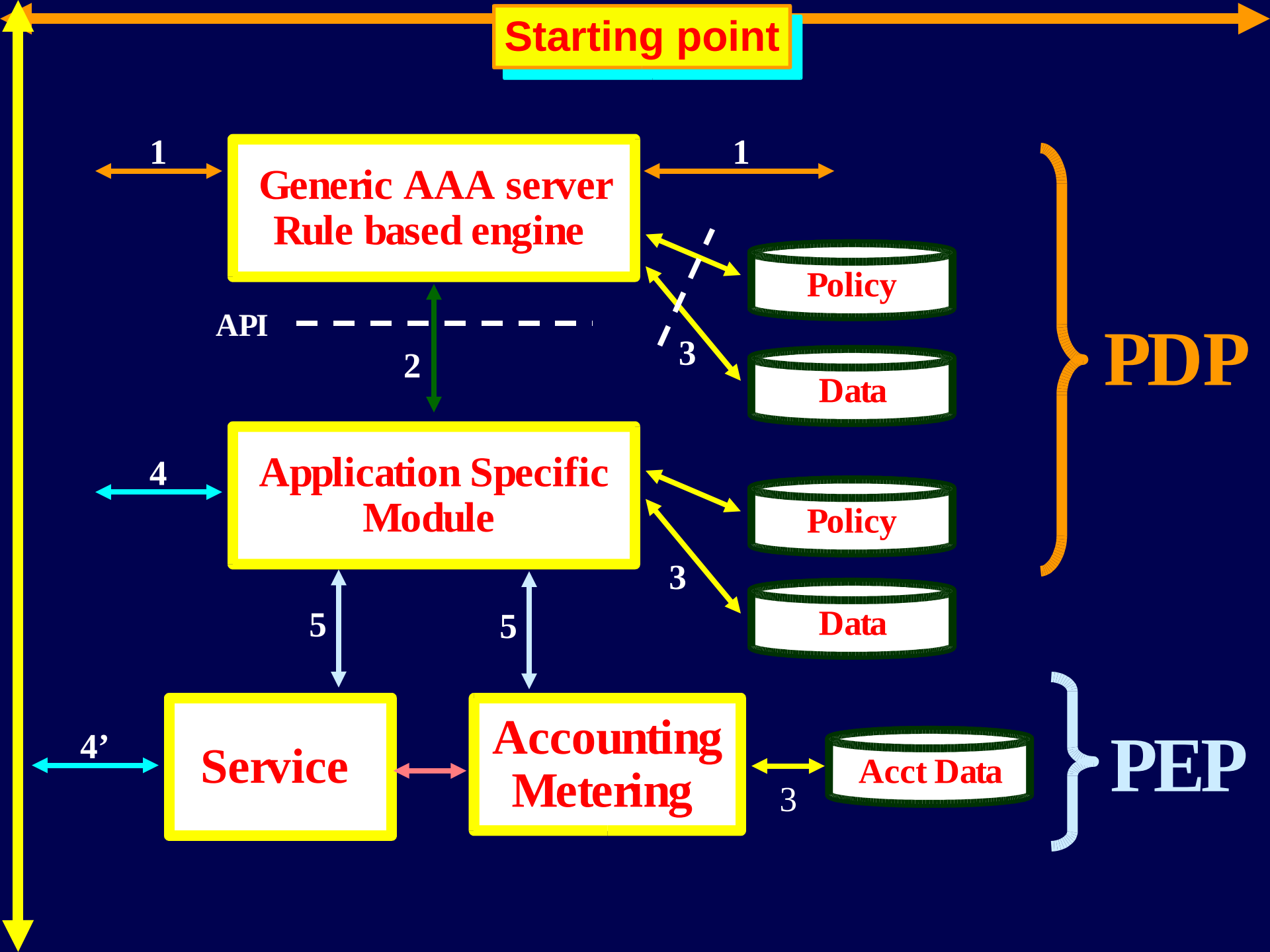
The need for AAA



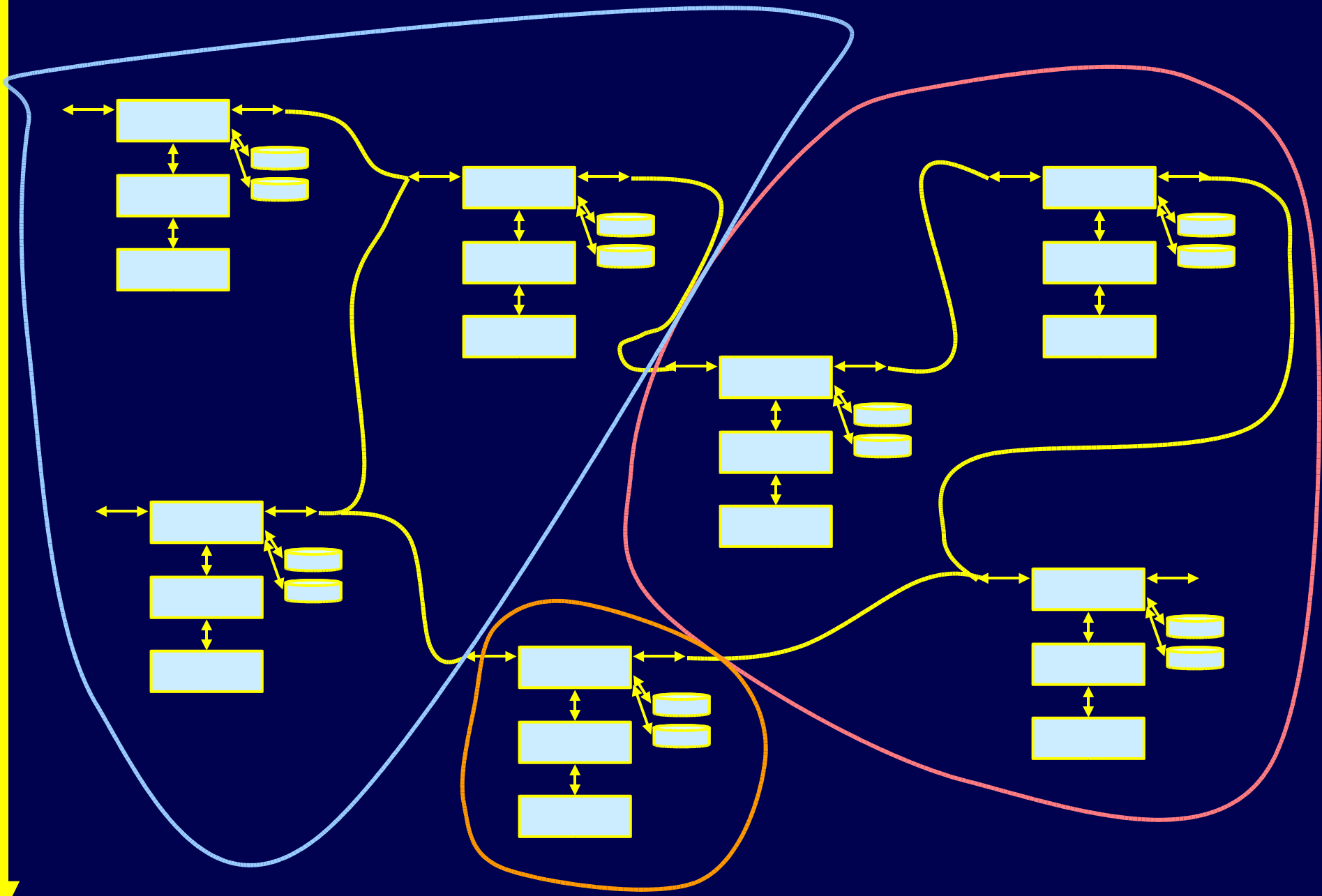

Roles
USER
USER
USER
UNI
UNI
UNI
SURFnet
DFN
SWITCH
REDIRIS
GEANT/DANTE

Authorization Models




Starting point
1
Generic AAA server
Rule based engine
1
API
2
3
Policy
Data
PDP
4
Application Specific
Module
3
Policy
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>
```

Example of BoD driving Policy

```
if
(
  (
    ASM::Authorizer.authorize(
                Request::AuthorizationData.Credential.ID,
                Request::AuthorizationData.Credential.Key
                                )
)
then
(
  ASM::RM.BoD(
                Request::ServiceData.SwitchData.Source,
                Request::ServiceData.SwitchData.Destination,
                Request::ServiceData.SwitchData.Bandwidth,
                Request::ServiceData.SwitchData.StartTime,
                Request::ServiceData.SwitchData.Duration
                   )
  ;
  Reply::Answer.Message = "Request successful"
)
else
(
  Reply::Error.Message = "Request failed"
)
```

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

Charter - research items

- develop generic AAA model by specifically including Authentication and Accounting UNDERWAY
- develop auditability framework specification that allows the AAA system functions to be checked in a multi-organization environment NJET
- develop a model for management of a "mesh" of interconnected AAA Servers NJET
- describe inter domain issues using generic model under study
- define in a high level and abstract way the interfaces between the different components in the architecture UNDERWAY
- define distributed AAA related policy framework ON THE TABLE
- develop an accounting model that allows authorization to define the type of accounting processing required for each session ON THE TABLE
- implement a simulation model that allows experimentation with the proposed architecture UNDERWAY
- work with RAP-WG to develop an Authentication Information management model ON THE TABLE (off the table :-(
- work with GGF to align the security and AAA architectural ideas UNDERWAY

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**

AAAARCH