# IRTF - AAAARCH - RG

# Authentication Authorisation Accounting ARCHitecture RG

chairs:

C. de Laat and J. Vollbrecht

www.phys.uu.nl/~wwwfi/aaaarch

RFC 2903, 2904, 2905, 2906

# Contents of this talk

- This space is intentionally left blank

# 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

# 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)

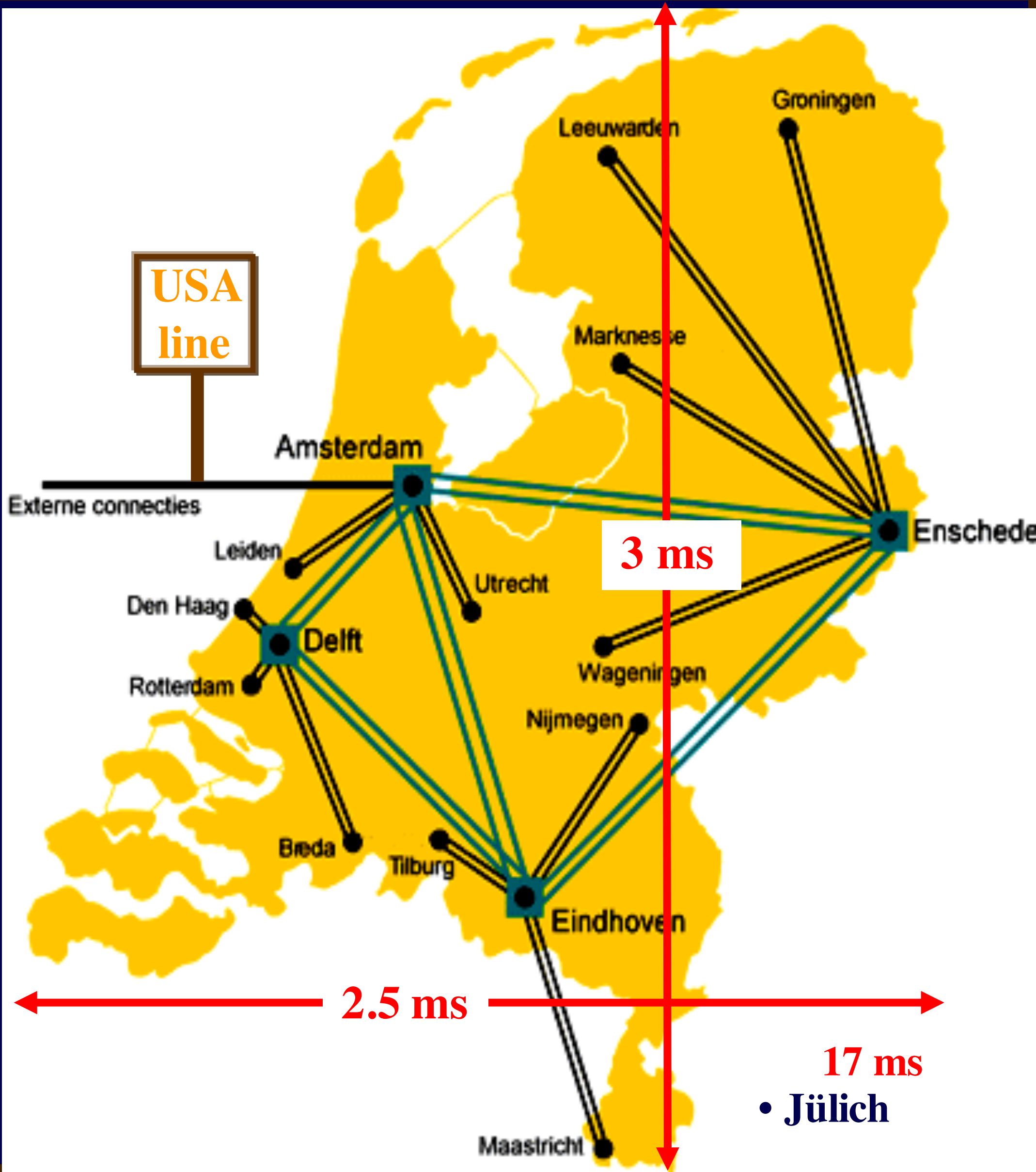
# Applications

- Web access
- Network Access
- Bandwidth Broker, VLL service
- Authorization of usage of combination of resources living in many administrative domains
- Computing grids, data grids, HEP community
- Budget system
- Library system
- Tele-learning
- E-Commerce
- Micro-payments

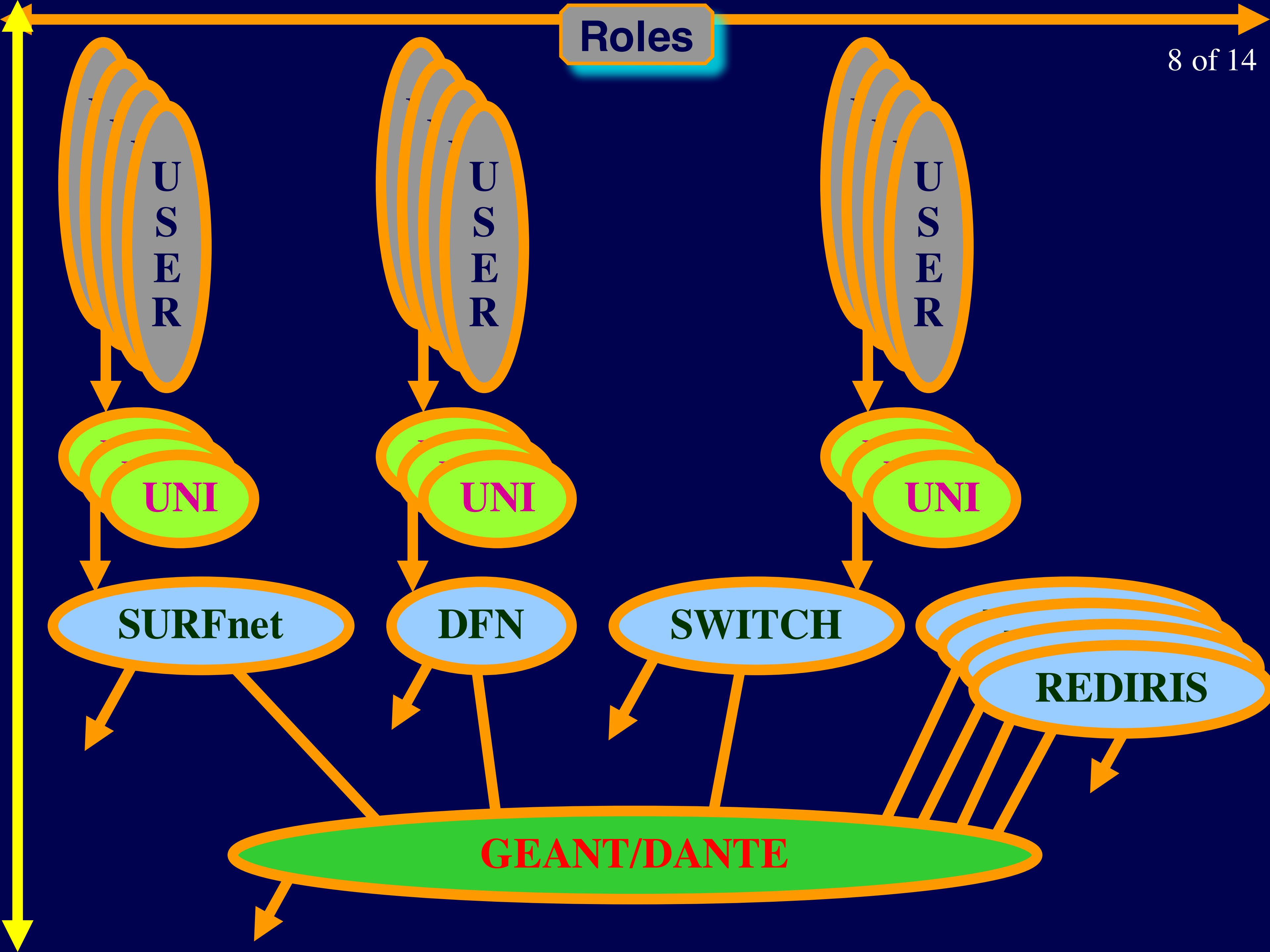
# Multi Kingdom Problems

## Physics-UU to IPP-FZJ => 7 kingdoms

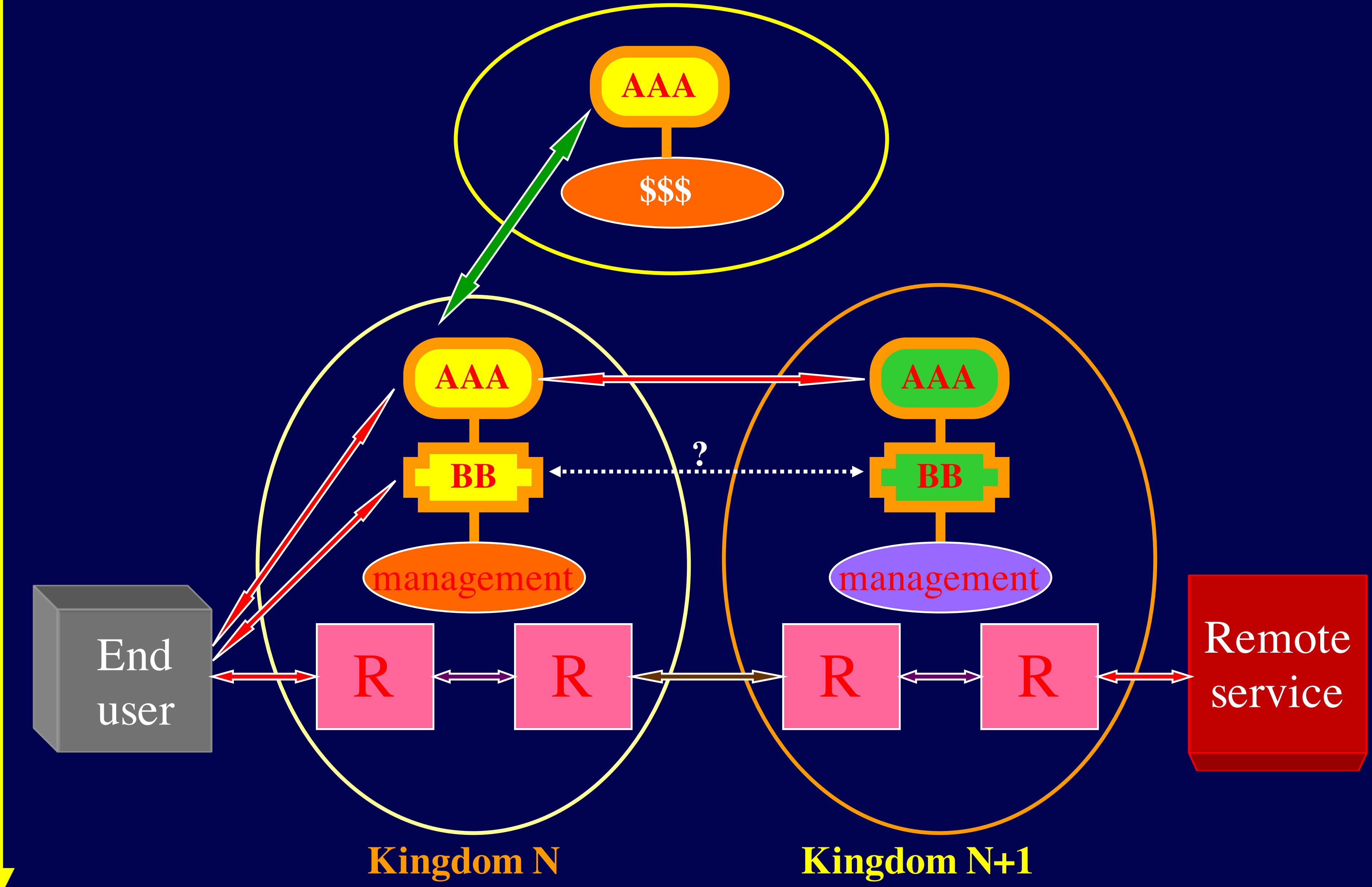
- Netherlands
  - »Physics dept
  - »Campus net
  - »SURFnet
- Europe
  - »GEANT
- Germany
  - »WINS/DFN
  - »Juelich, Campus
  - »Plasma Physics dept



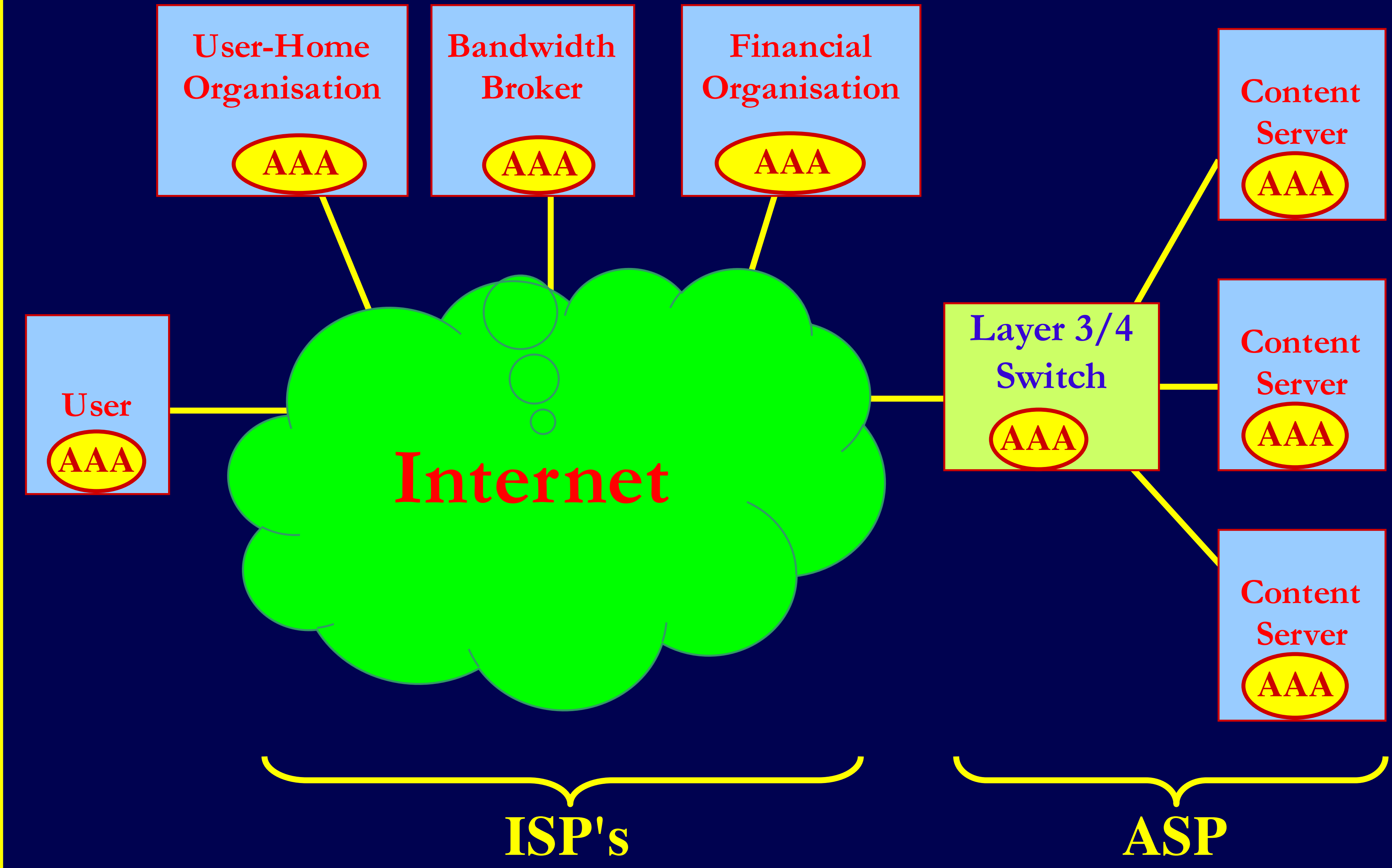
# Roles


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

# The need for AAA



# ASP



User-Home Organisation

AAA

Bandwidth Broker

AAA

Financial Organisation

AAA

User

AAA

Internet

Layer 3/4 Switch

AAA

Content Server

AAA

Content Server

AAA

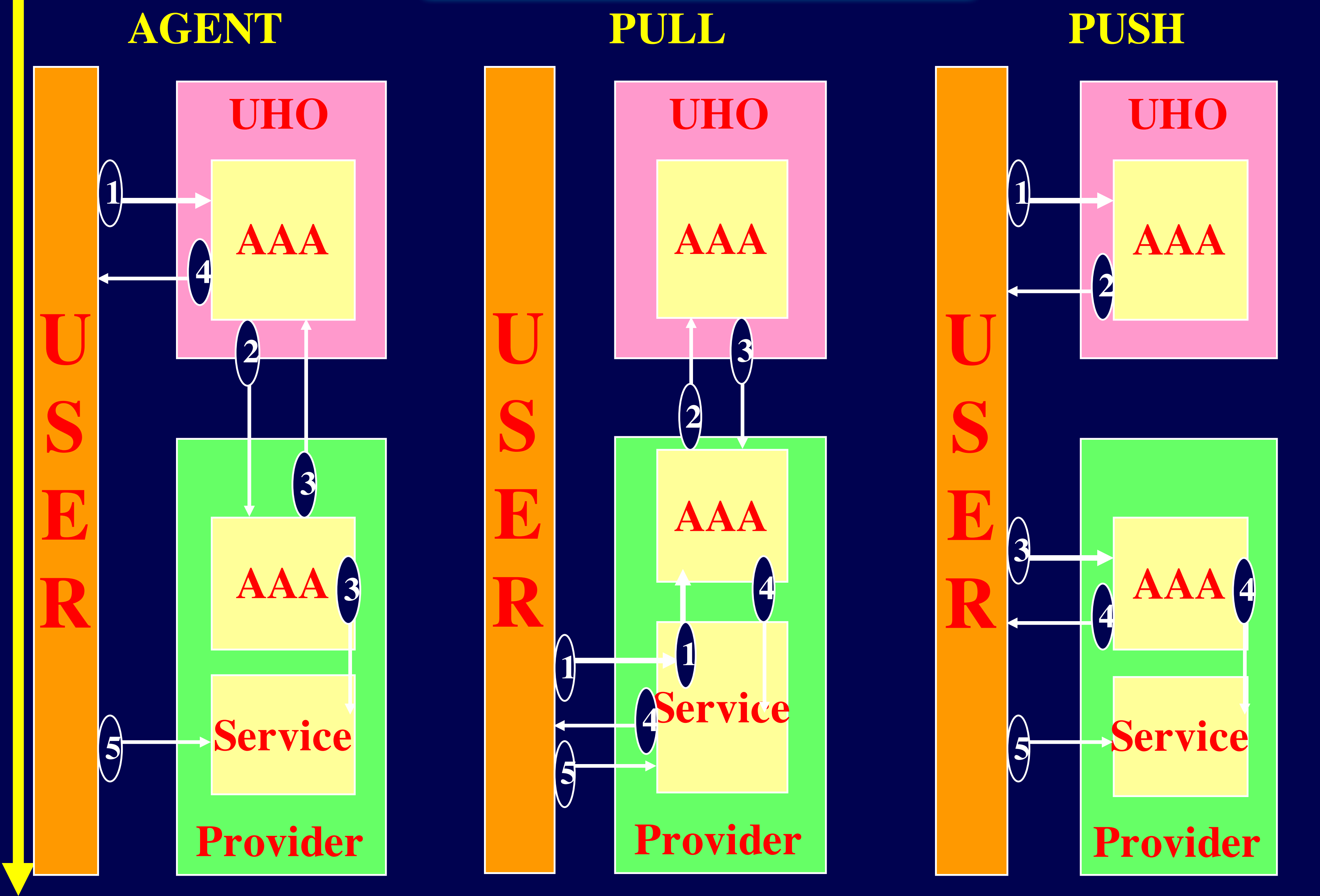
Content Server

AAA

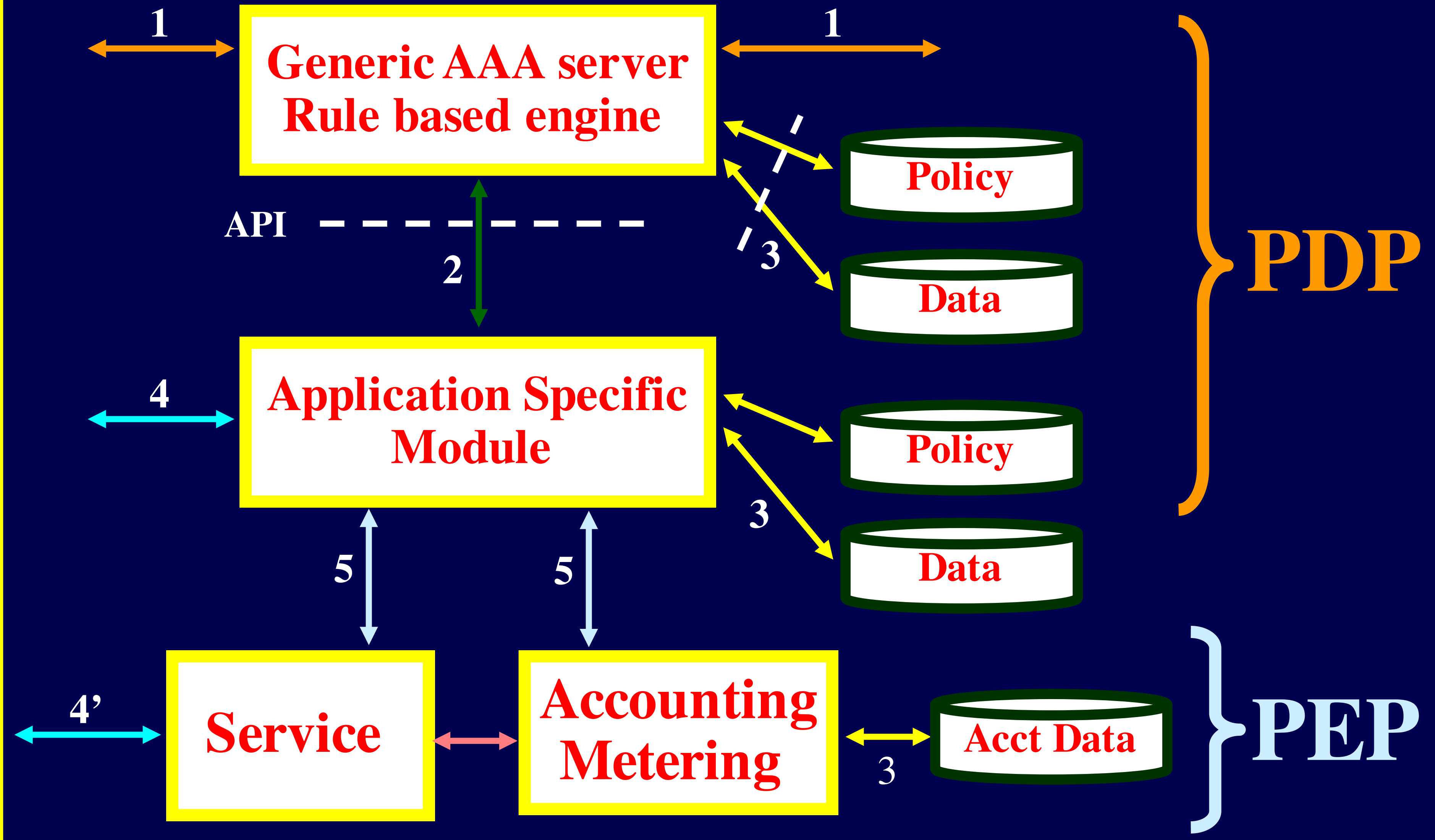
ISP's

ASP

# Authorization Models



# Starting point



Generic AAA server
Rule based engine

Application Specific Module

Service

Accounting
Metering

Policy

Data

Policy

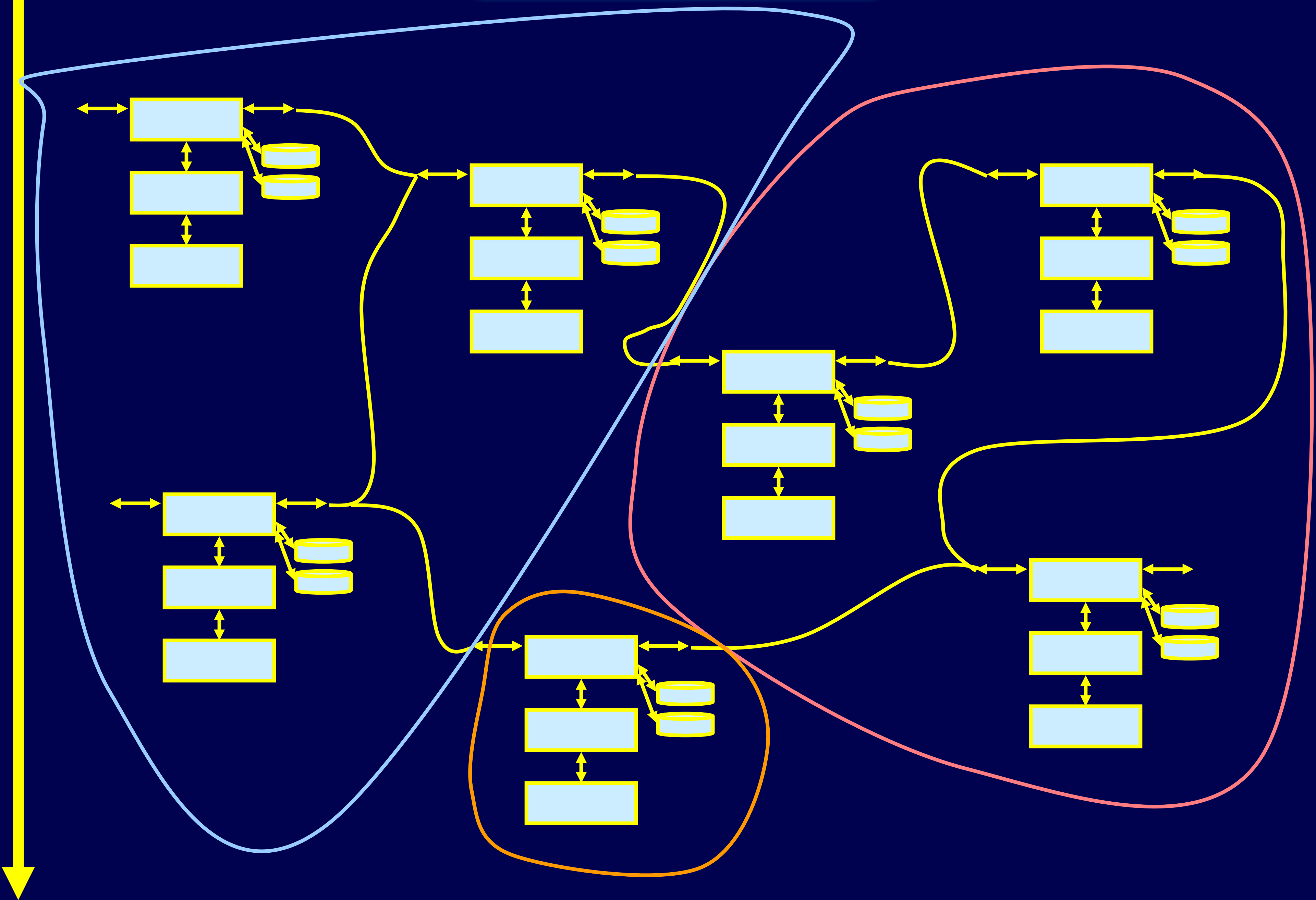
Data

Acct Data

PDP

PEP

# Multi domain case



# Basic principles

## Principles of Generic AAA

1. Three building blocks:
    1. RBE
    2. ASM
    3. Service Equipment
2. There is a global address space between the RBE and the ASM.
3. There is only generic stuff in the RBE and all the application specific stuff is in the ASMs.
4. The relationship between AAA servers is symmetric.
5. Different servers may have different capabilities.

# Message types

- Service request/reply
- Authorization request/reply
- Solicit Service Offer request/reply
- Authentication request/reply
- Authentication Challenge request/reply
- Policy request/reply
- Policy Evaluation request/reply
- Data request/reply
- Event Log indication/confirmation
- Accounting indication/confirmation
- Service (session) Configuration indication/confirmation
- Service (session) Management indication/confirmation
- Capability request/reply (supports resource discovery)

# Top Level Objects

- Identity
- Authentication Data
- Authentication Challenge
- Service Data
- Service Offer
- Answer
- Error
- Policy
  - [service specification policy, authorization policy, provisioning policy, configuration policy, accounting policy, metering policy]
- Policy Reference
- Policy Data
- Configuration Data
- Service Management
- Accounting
- Event

# Status authorization framework

- Authorization model
  - <draft-taal-aaaarch-generic-pol-00.txt>
- Policy definition
  - <draft-salowey-aaaarch-xxxxxxx.txt>
- Primitives model for authorization requests
- Data model for authorization
- Context of AAA usage
  - <www.phys.uu.nl/~wwwfi/aaaarch/doc06/aaa_context.doc>
- Authentication model
  - <www.phys.uu.nl/~wwwfi/aaaarch/doc12/kaushik-radius-sec-ext-04.txt>
- session-id
- policy based accounting
  - <draft-irtf-aaaarch-pol-acct-01.txt>

# Status-2

- relation to other groups:
  - AAA --> DATA model
  - Policy Framework
  - SLS BOF
  - GAAAPI (Generic Authorization and Access control API)
  - GSSAPI (Generic Security Services API)
  - RAP (BB)
  - SIP <session initiation protocol>
  - Computing/data grids < www.gridforum.org/>
  - Middleware

# Future work

- develop audibility framework specification that allows the AAA system functions to be checked in a multi-organization environment
- develop a model that supports management of a "mesh" of interconnected AAA Servers
- implement a simulation model that allows experimentation with the proposed architectural models (UU)
- describe inter-domain issues using generic model
- Future issues:
  - AAA-WG-actions
  - unresolved topics
  - (protocol) work for WG's
  - future AAAARCH work
- complete the work in Q1 - 2001 (ambitious)

# Research Group - info

- Research Group Name: AAAARCH - RG
- Chair(s)
  - John Vollbrecht -- jrv@interlinknetworks.com
  - Cees de Laat -- delaat@phys.uu.nl
- Web page
  - www.irtf.org
  - www.phys.uu.nl/~wwwfi/aaaarch
- Mailing list(s)
  - aaaarch@fokus.gmd.de
  - For subscription to the mailing list, send e-mail to

    majordomo@fokus.gmd.de with content of message

    subscribe aaaarch

    end
  - will be archived, retrieval with frames and in plain ascii:
    - http://www.fokus.gmd.de/glone/research/aaaarch/
    - http://www.fokus.gmd.de/glone/research/mail-archive/aaaarch-current
    - ftp://ftp.fokus.gmd.de/pub/glone/mail-archive/aaaarch-current

AAAARCH