IRTF

Authentication Authorisation and Accounting ARCHitecture Research Group

chairs:

C. de Laat and J. Vollbrecht

Content of this talk has contributions from many persons including:

B. de Bruijn, C&K Dobbins, S. Farrell, G. Gross, T. Zseby,

L. Gommans, D. Spence, E. Verharen, T. Verschuren

Utrecht University

Contents of this talk

- This space is intentionally left blank

Research Subjects

- Networking
  - Focus on applications for Physics
  - QoS networks for computing, collaboratories and telelearning
  - Distributed systems topics:
    - Modeling
    - Optimization
    - Simulation
    - Emulation

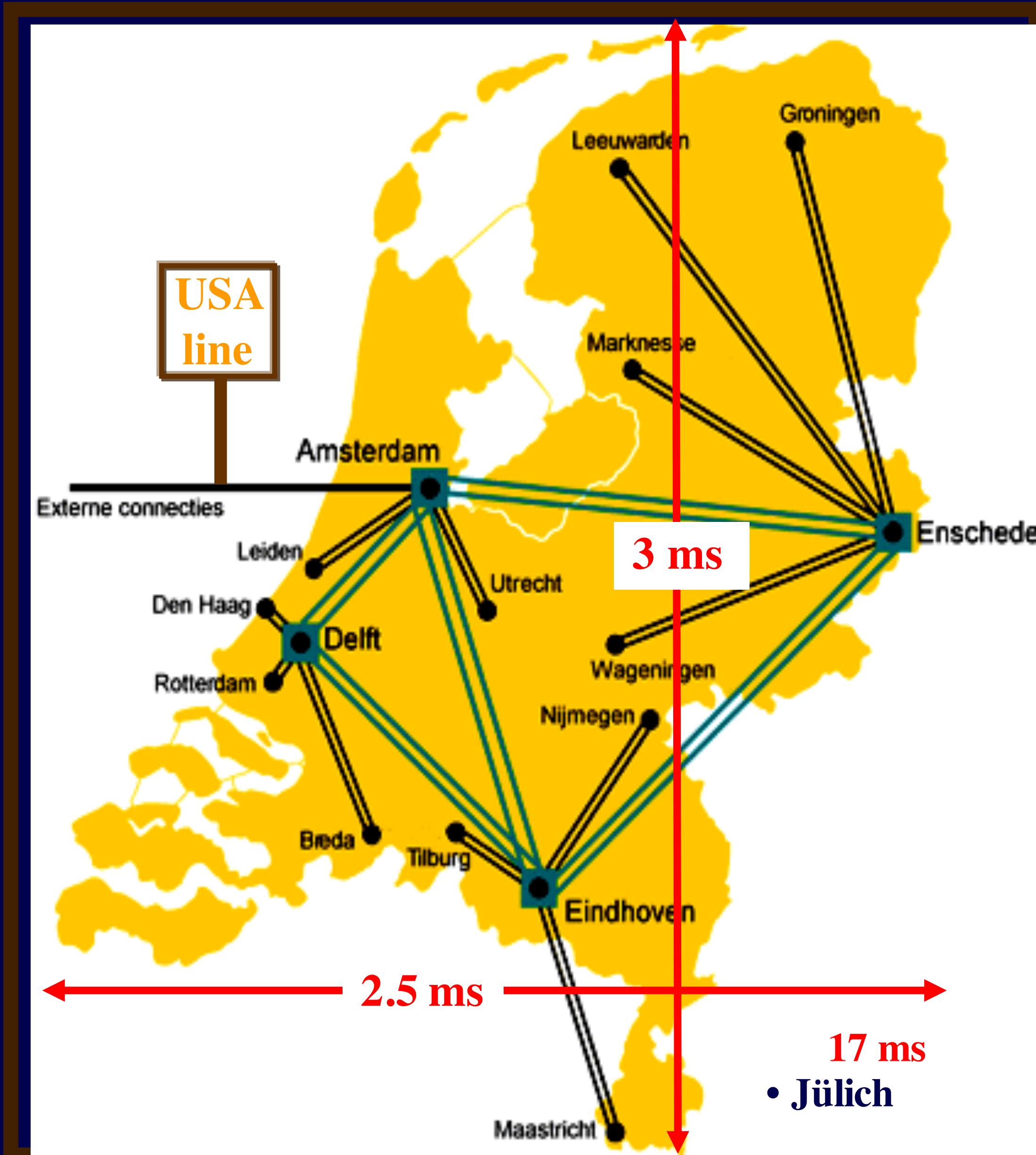
Research Subject example

- EU project REMOT / DYNACORE
  - Collaboratories, virtual control rooms
  - Support science at the home institutes
  - Groupware, Videoconference tools point to point and point to multipoint
  - Corba services, distributed object db
  - www.phys.uu.nl/~dynacore

Multi Kingdom Problems

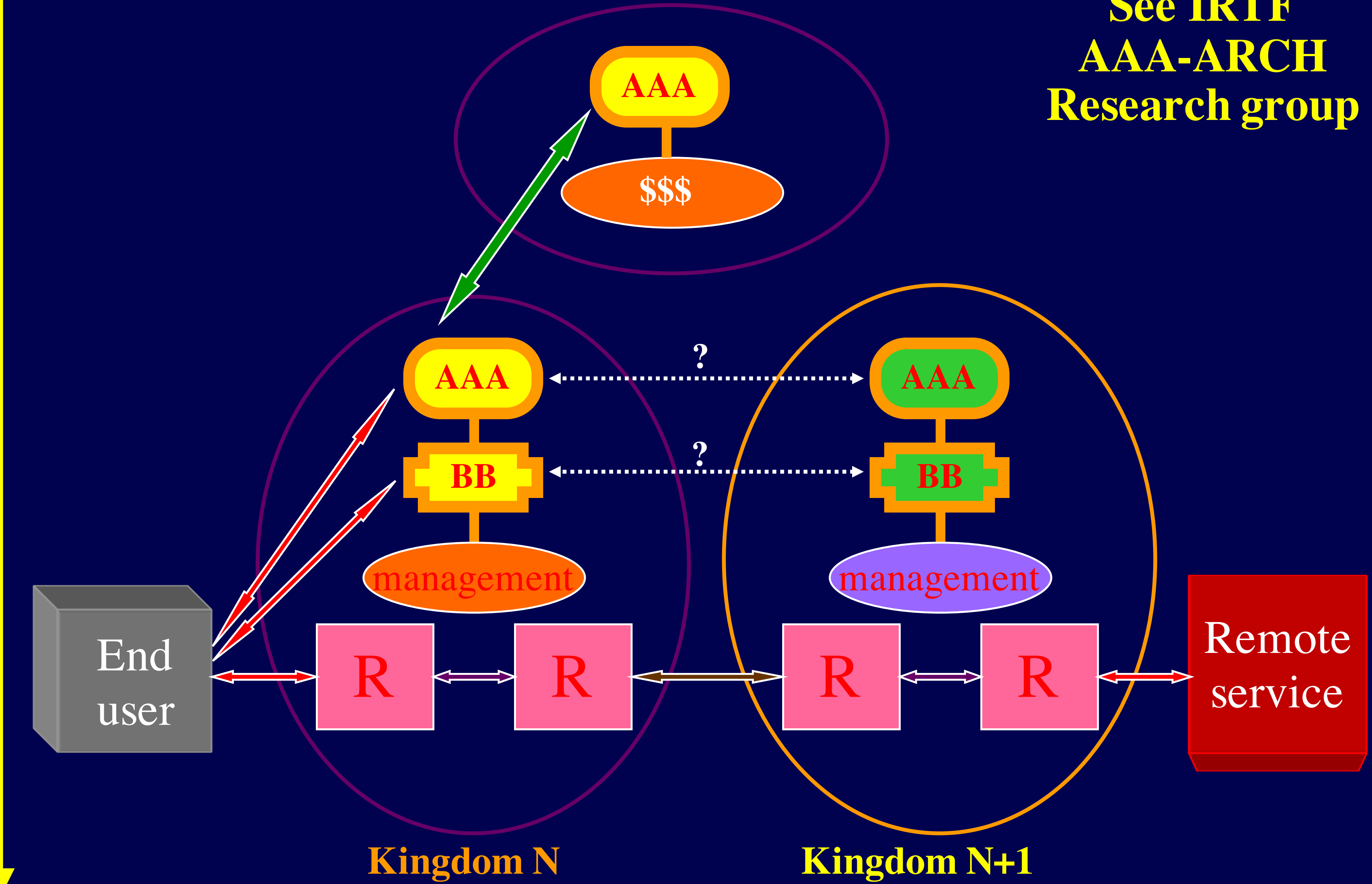
Physics-UU to IPP-FZJ => 7 kingdoms

- Netherlands
  - »Physics dept
  - »Campus net
  - »SURFnet
- Europe
  - »TEN 155
- Germany
  - »WINS/DFN
  - »Juelich, Campus
  - »Plasma Physics dept

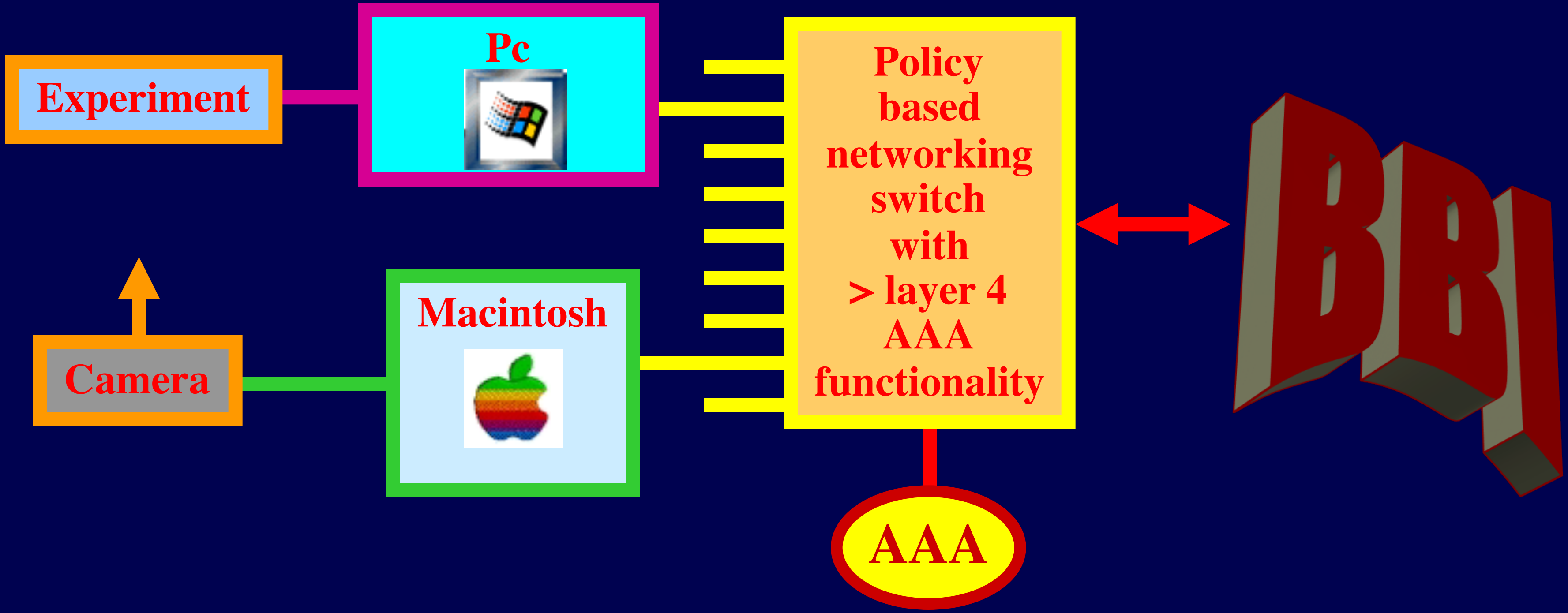


The need for AAA

See IRTF AAA-ARCH Research group



Policy based networking example



Experiment

Pc

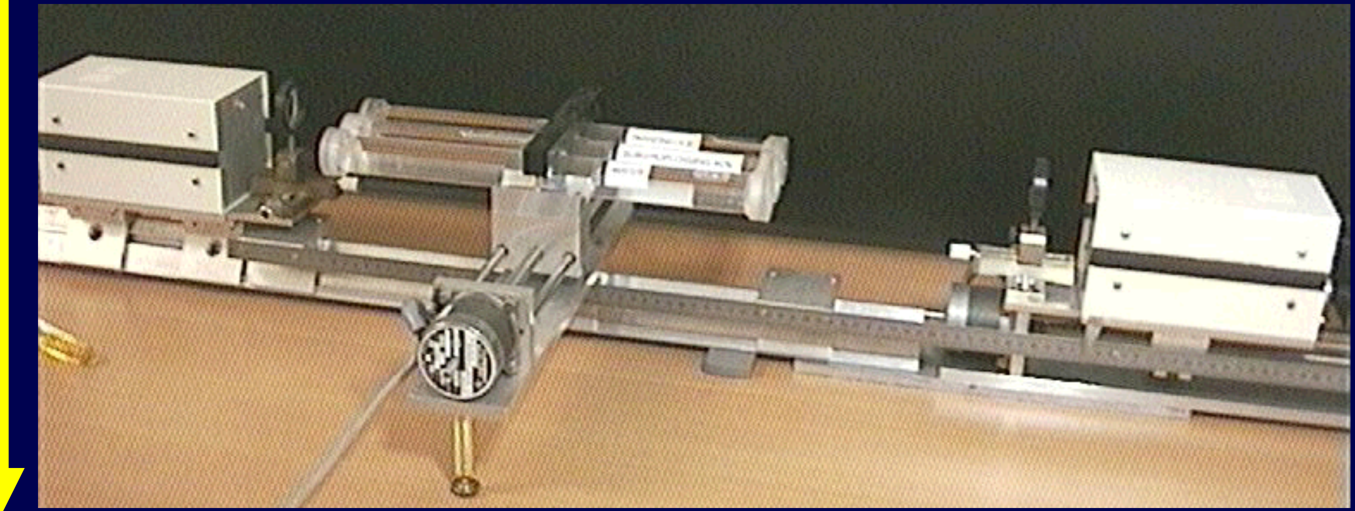
Camera

Macintosh

Policy based networking switch with > layer 4 AAA functionality

AAA

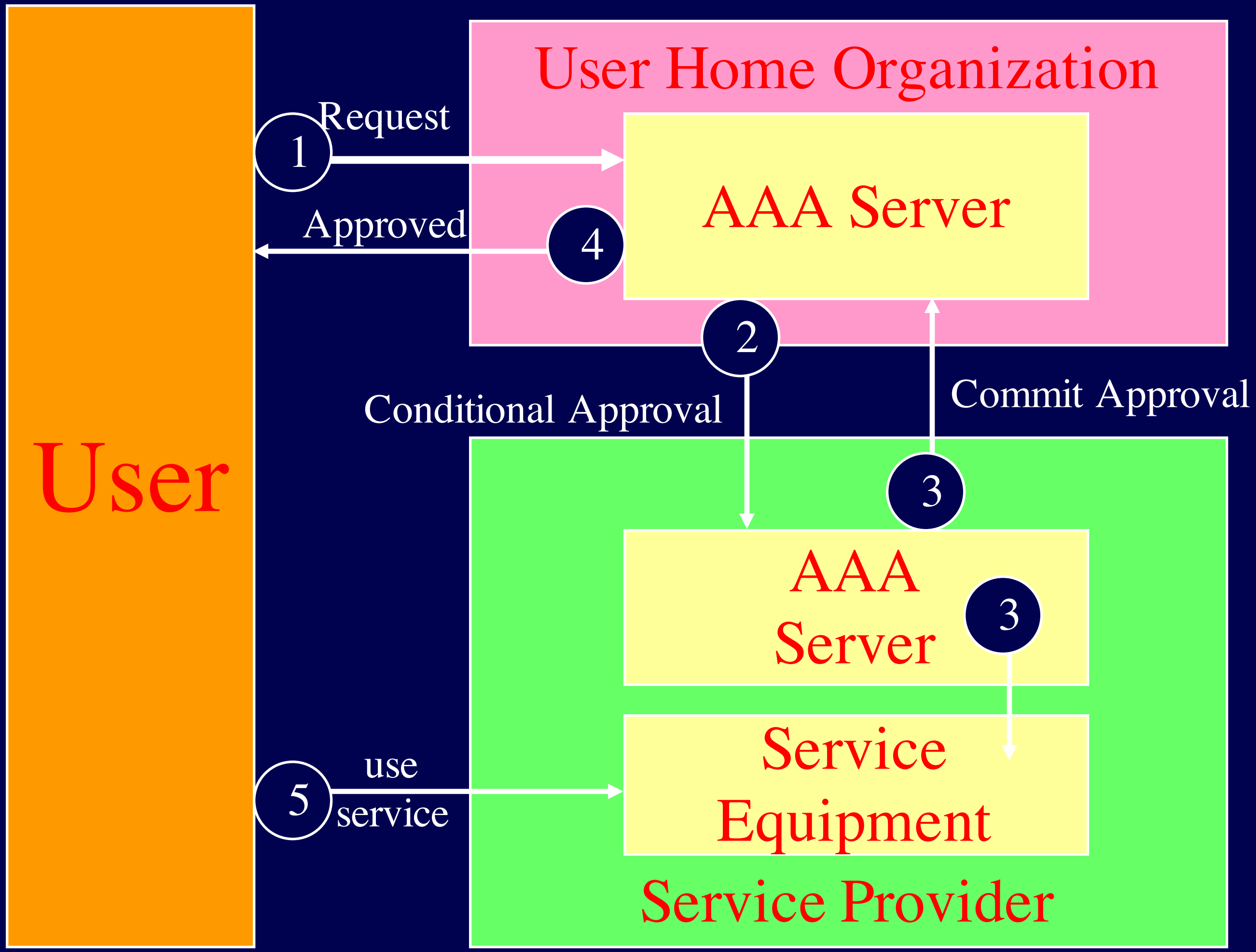
BBI



Applications

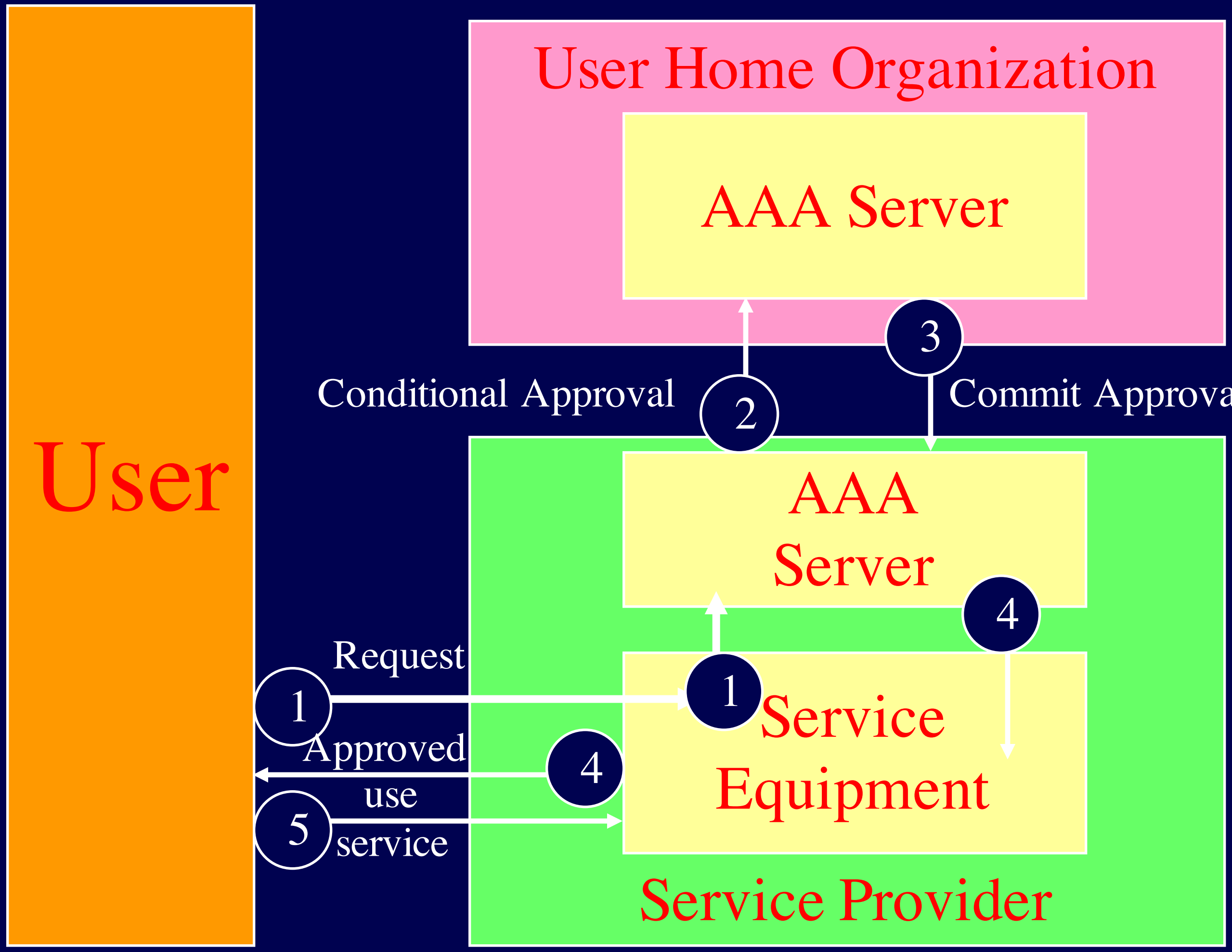
- Network Access
- Bandwidth Broker
- Authorization of resources living in many administrative domains
- Grids of any kind
- Budget system
- Library system
- Computer based education system
- E-Commerce
- Micro-payments
- Car Rental
- Daily life

Roaming "Agent" Authorization Model



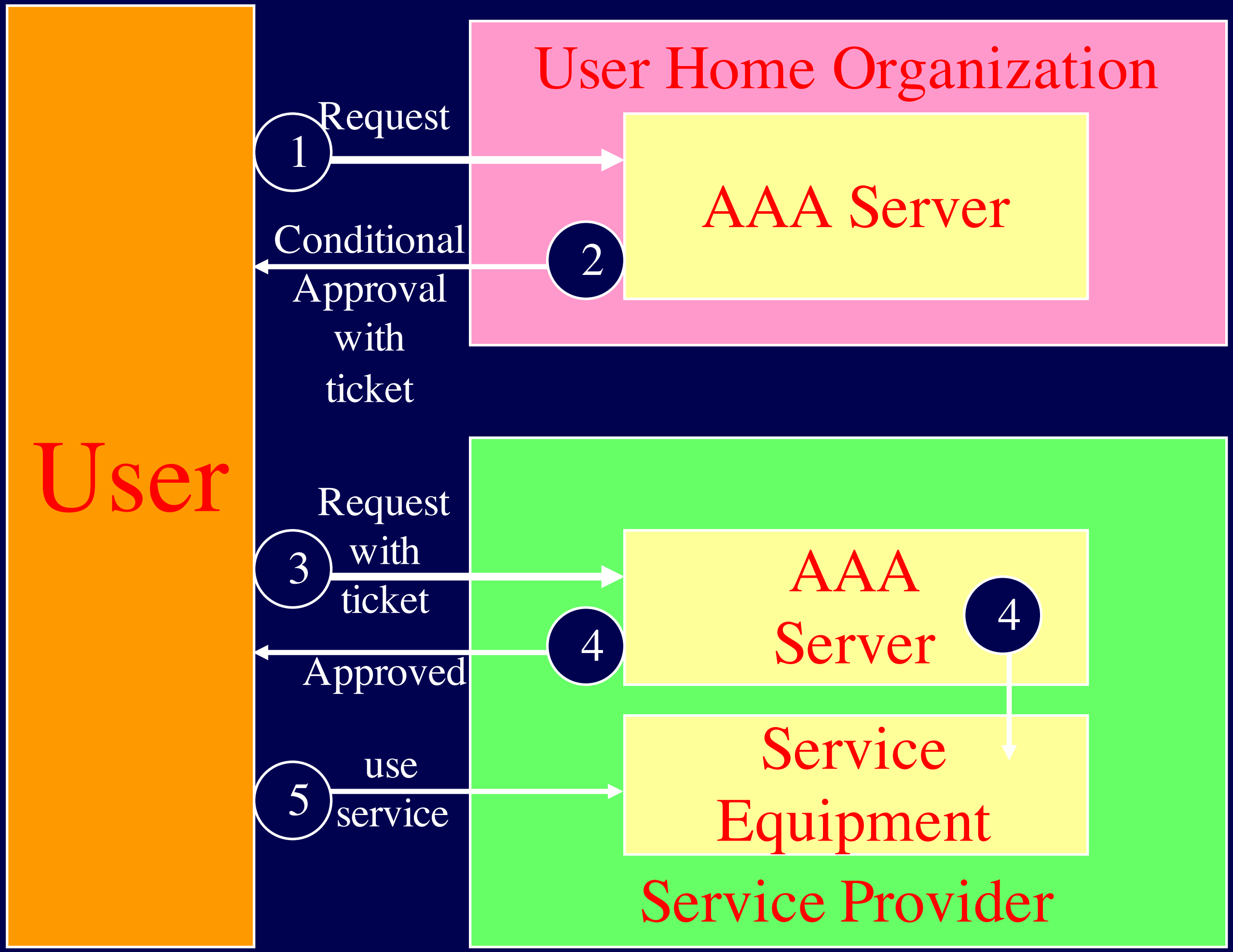
Example application: bandwidth brokerage at Enterprise/Service Provider boundary

Roaming “Pull” Authorization Model



Example applications: Mobile IP, PPP dial-in to NAS

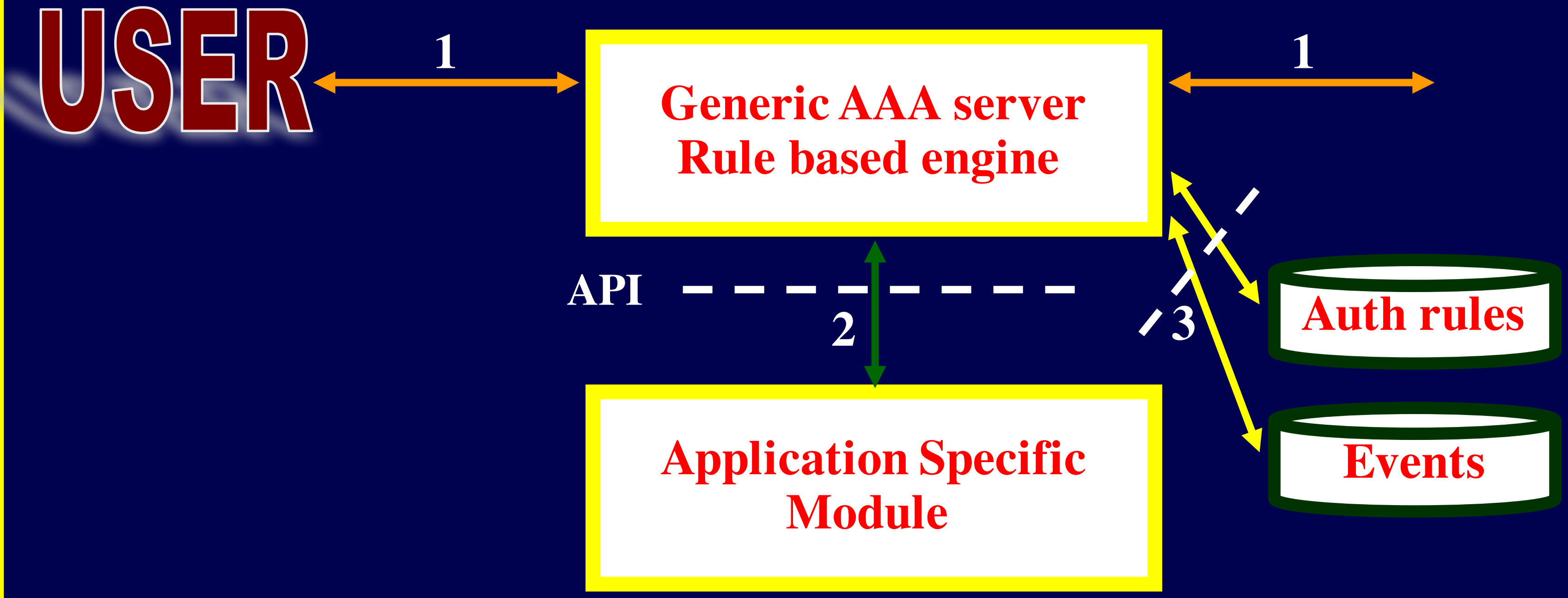
Roaming “Push” Authorization Model



Example application: Internet printing, where file and print servers are in different admin domains

AAA Server building block

Rule example: Auth_A = (B>9) .or. C .and. D



USER

Generic AAA server
Rule based engine

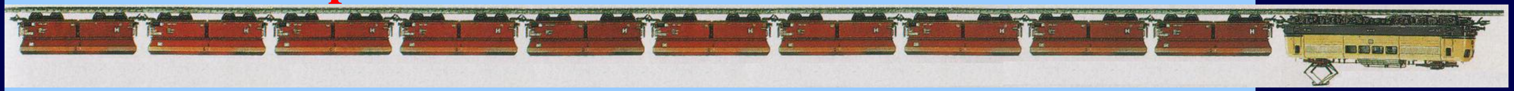
Application Specific
Module

Auth rules

Events

Types of communication:

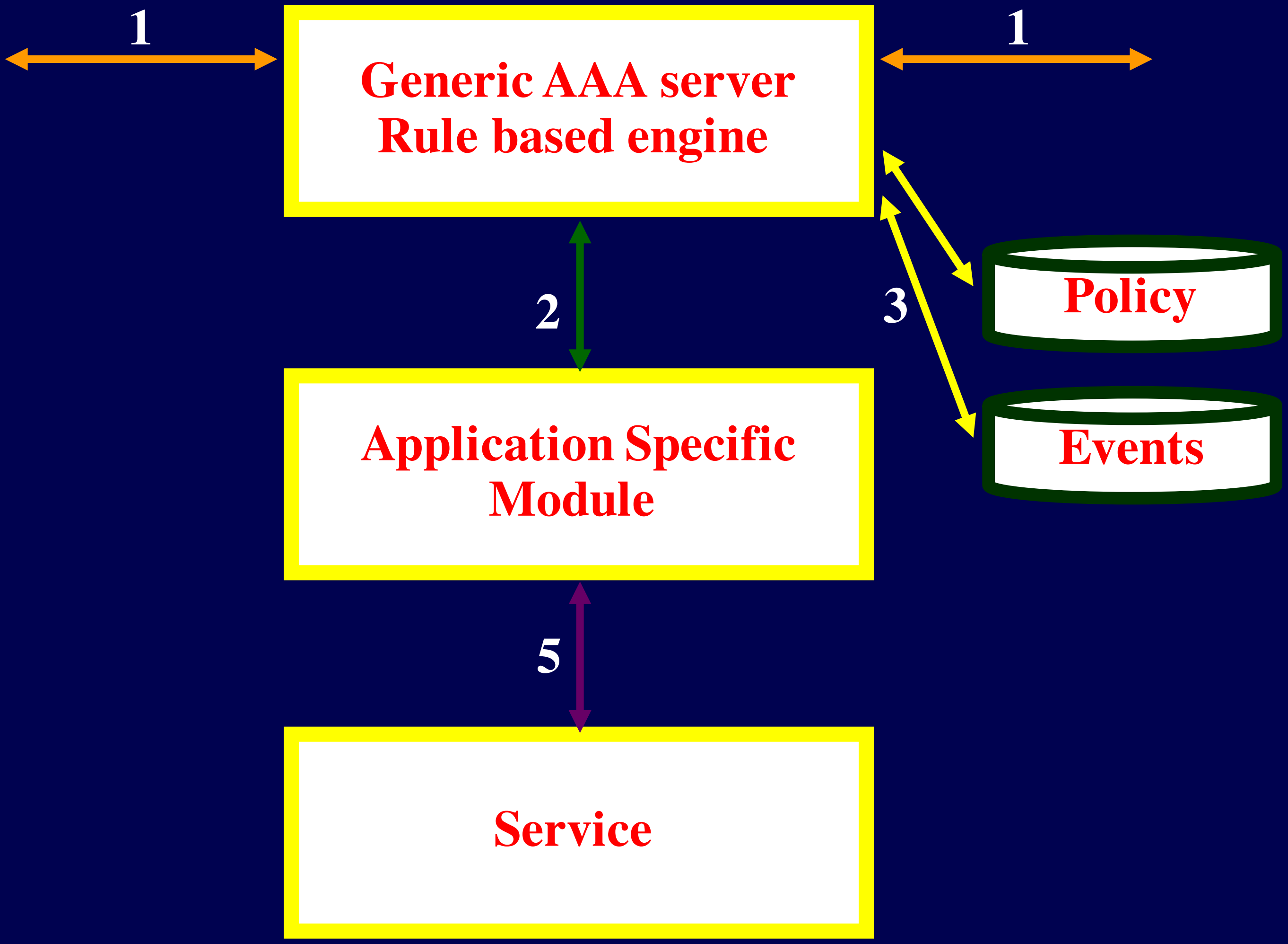
1: “The” AAA protocol



2: interface (API) to app specific module (addressing!)

3: interface (API or connection) to repositories (e.g. LDAP)

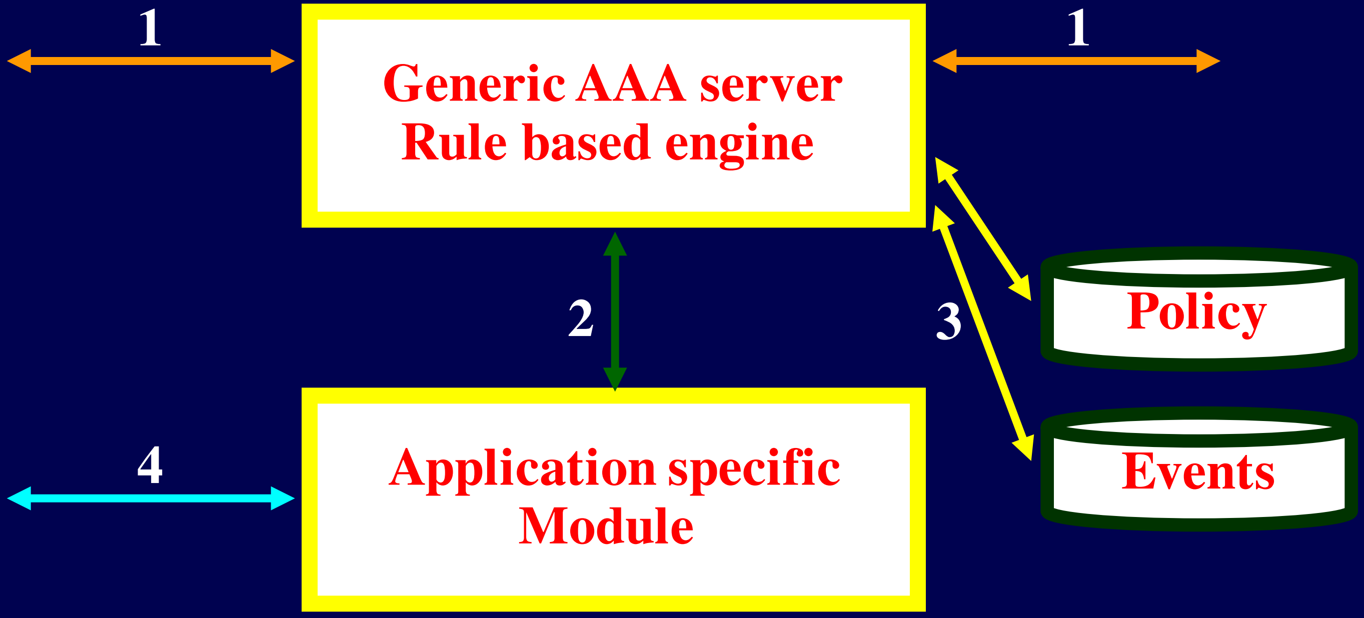
Pushing the buttons



Types of communication:

5: Towards service (f.e. COPS, CLI, SNMPv3)

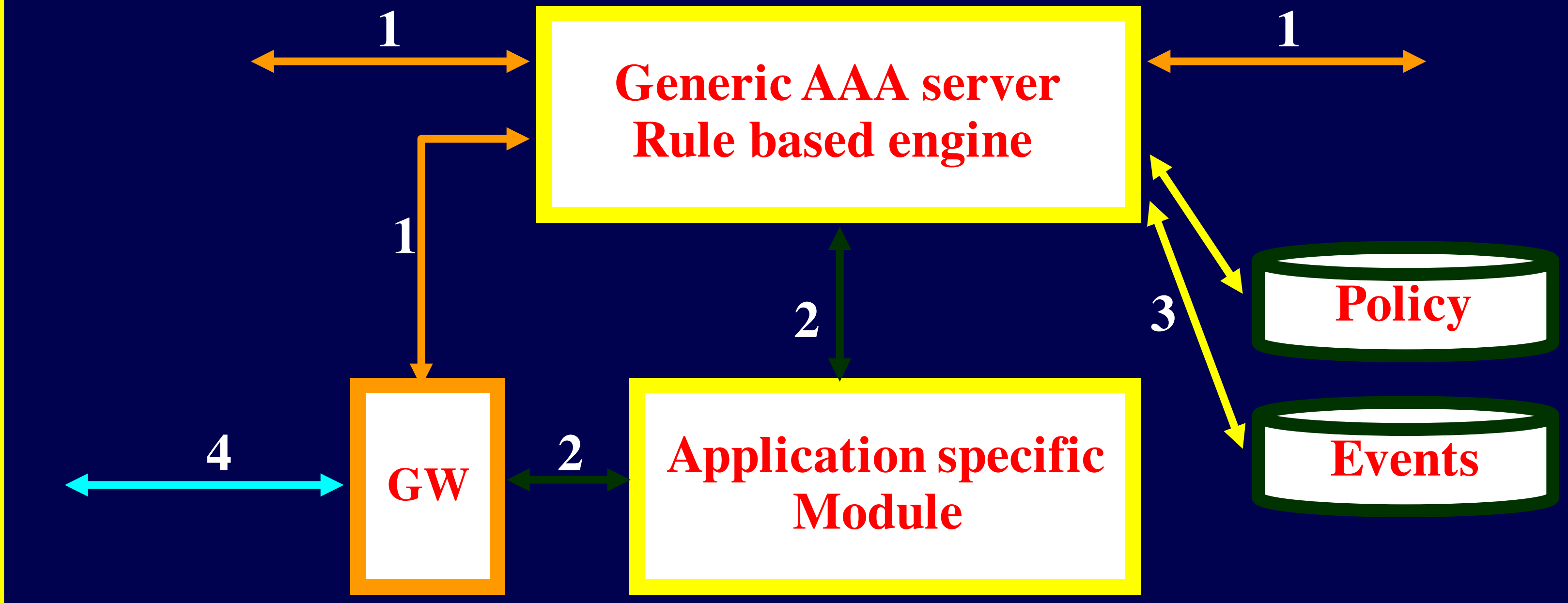
Legacy protocols



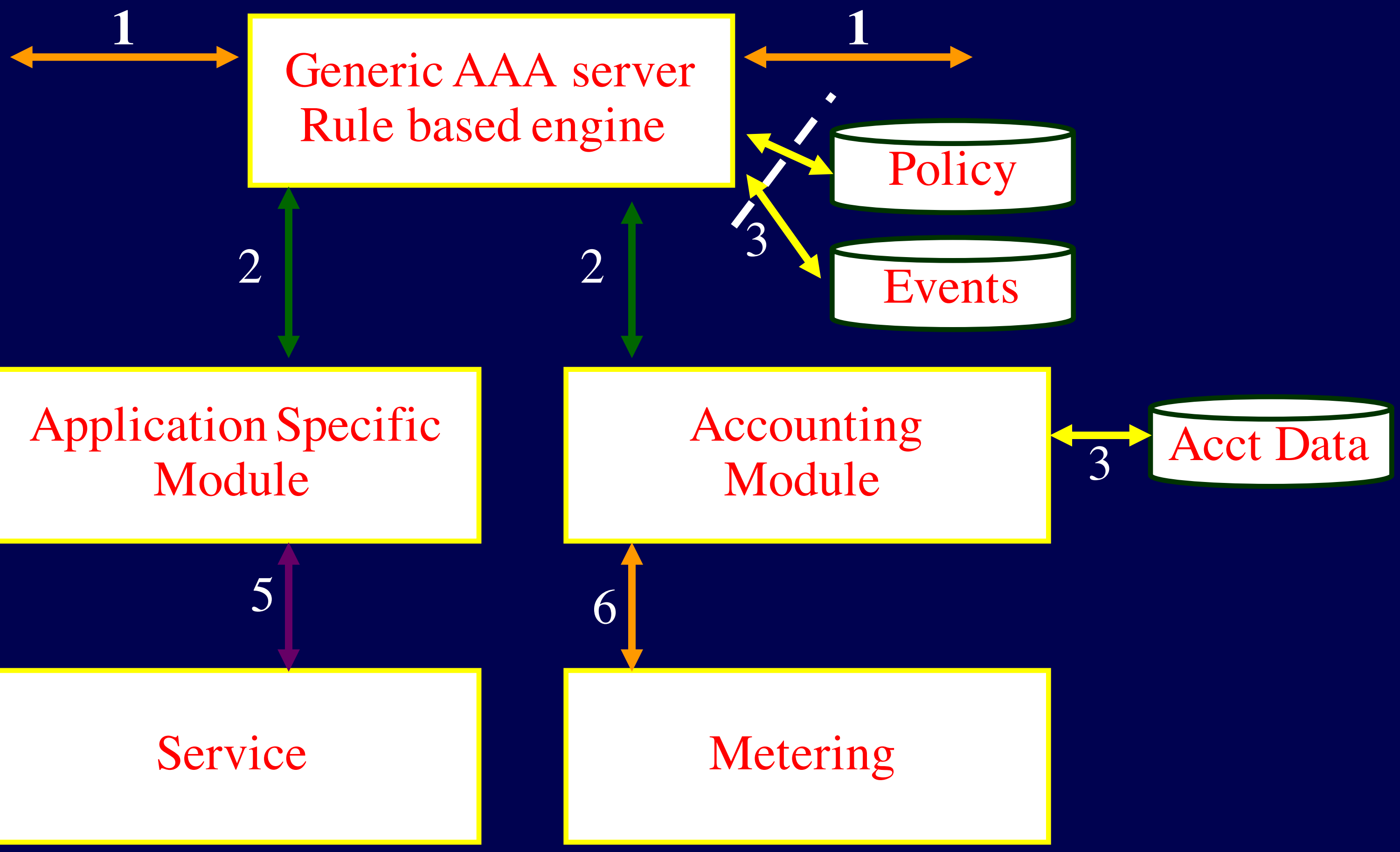
Types of communication:

4: Legacy protocols (Radius, Diameter, …)

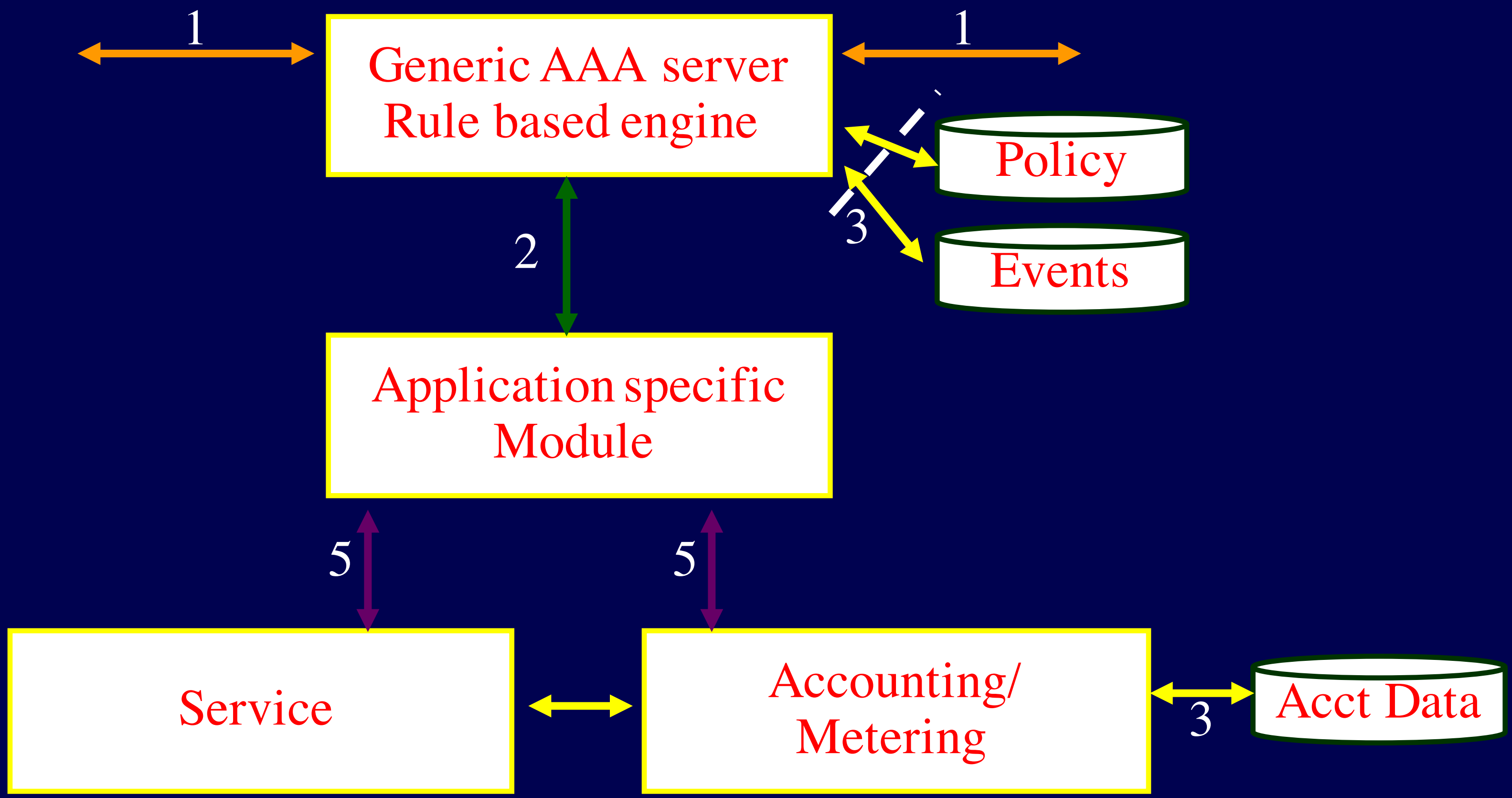
Gateway


1
1
Generic AAA server
Rule based engine
1
2
3
Policy
Events
4
GW
2
Application specific
Module

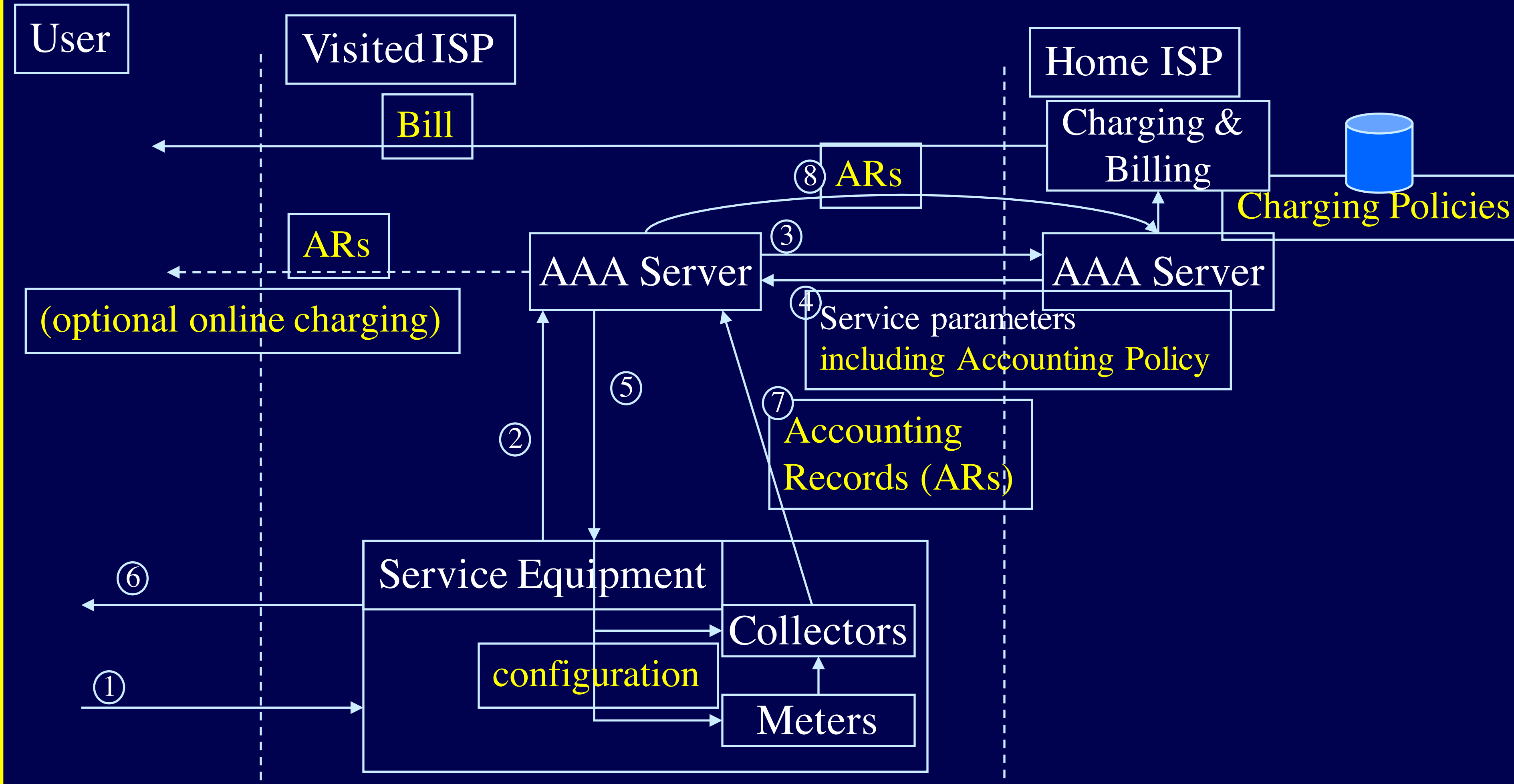
AAA Server with Accounting as Separate Service



AAA Server with Accounting as Part of the Service



Example: Interaction with Authorization



RG-Goals-1

Specific goals of the RG are:

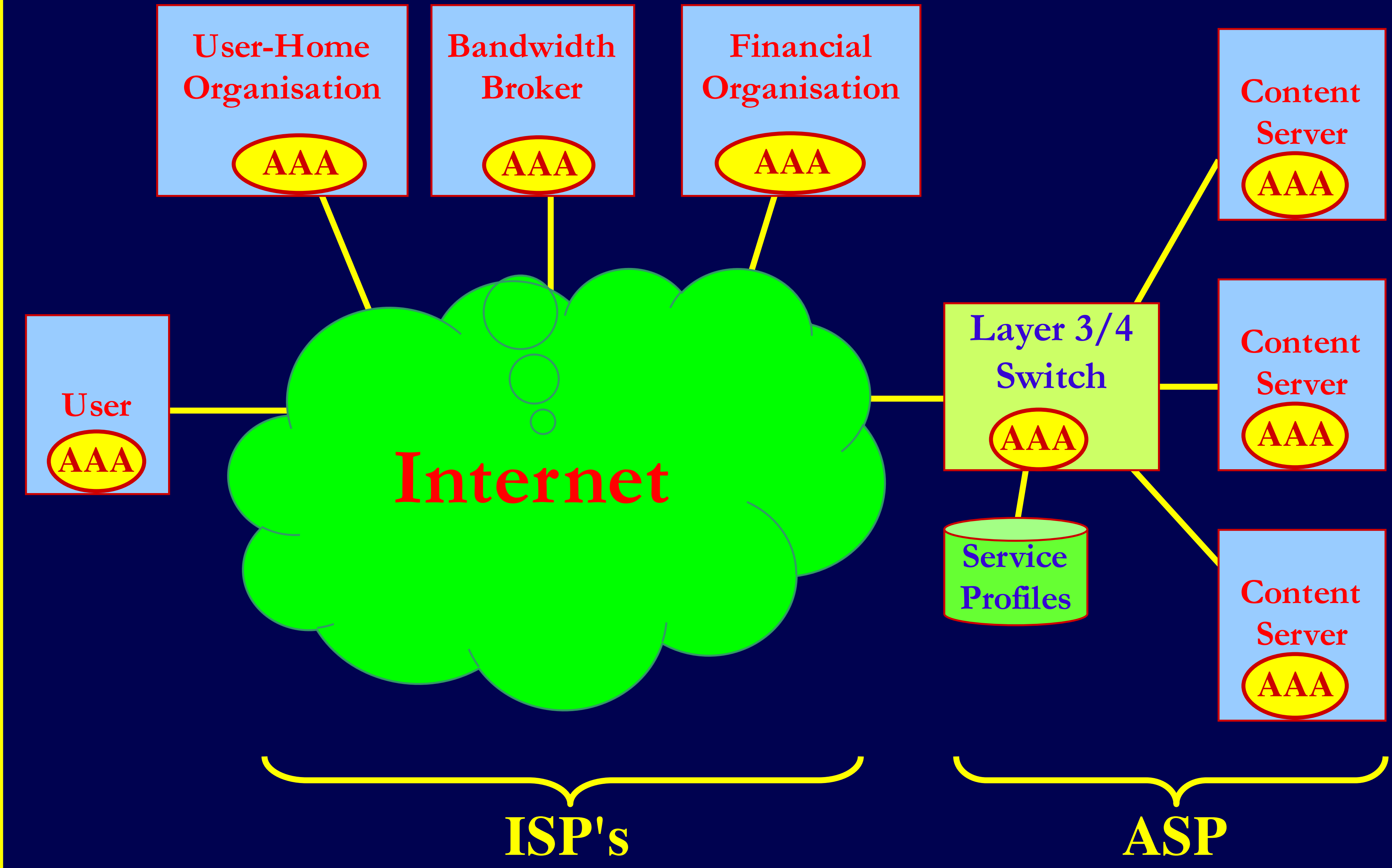
- develop generic AAA model by specifically including Authentication and Accounting
- develop audibility framework specification that allows the AAA system functions to be checked in a multi-organization environment
- develop a model that supports management of a "mesh" of interconnected AAA Servers
- define distributed policy framework, coordinate with policy framework WG and others
- develop an accounting model that allows authorization to define the type of accounting processing required for each session

RG-Goals-2

Specific goals of the RG are:

- implement a simulation model that allows experimentation with the the proposed architectural models (also work on an emulation)
- describe interdomain issues using generic model
- work with AAA WG to align short term AAA protocol requirements with long term requirements as much as possible
- complete the work in Q4 - 2000 (ambitious)

ASP



User-Home Organisation

AAA

Bandwidth Broker

AAA

Financial Organisation

AAA

Content Server

AAA

User

AAA

Internet

Layer 3/4 Switch

AAA

Content Server

AAA

Service Profiles

Content Server

AAA

ISP's

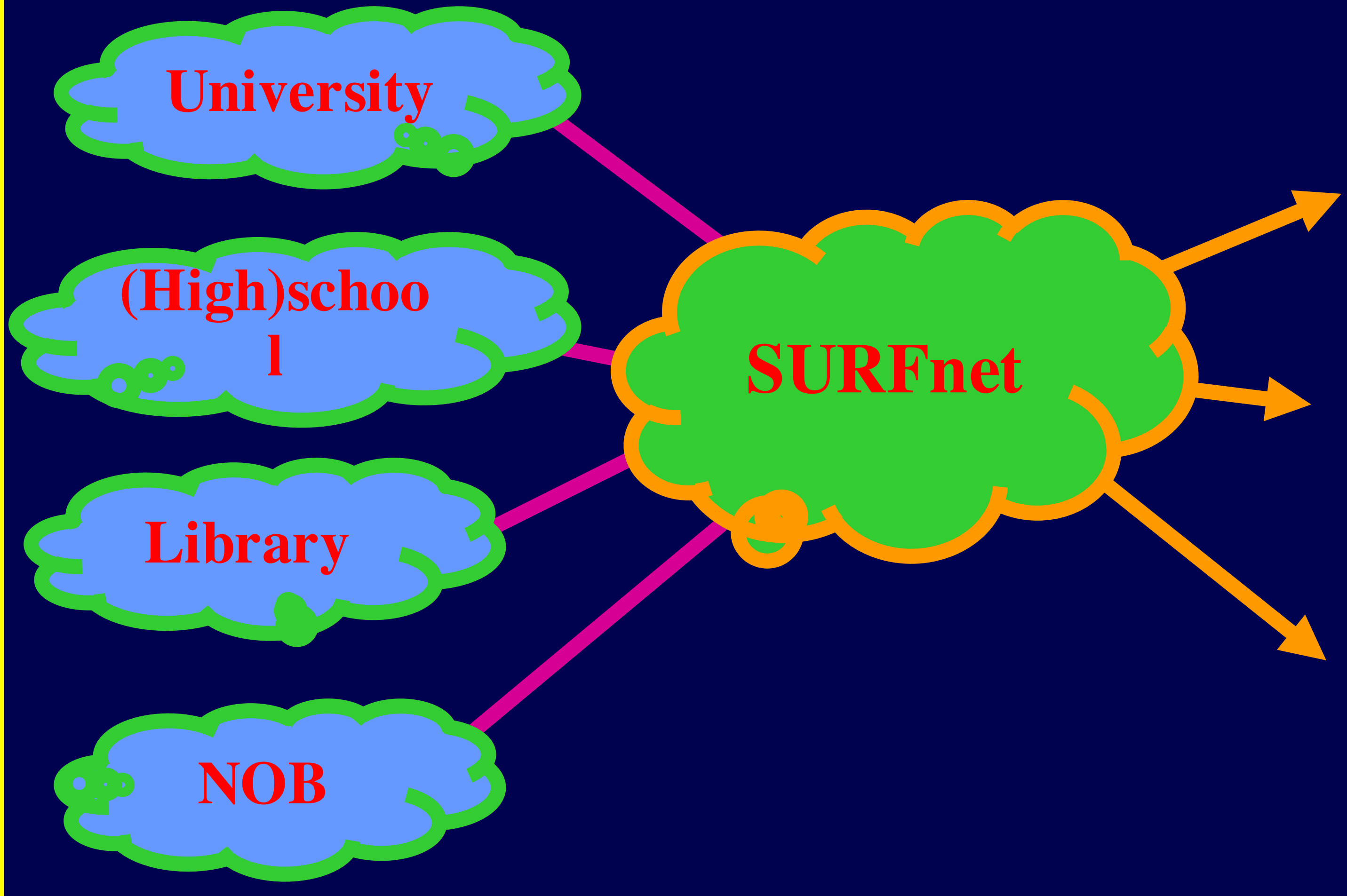
ASP

Roles

Content

Portals
Brokers

Customers



University

(High)schoo
l

Library

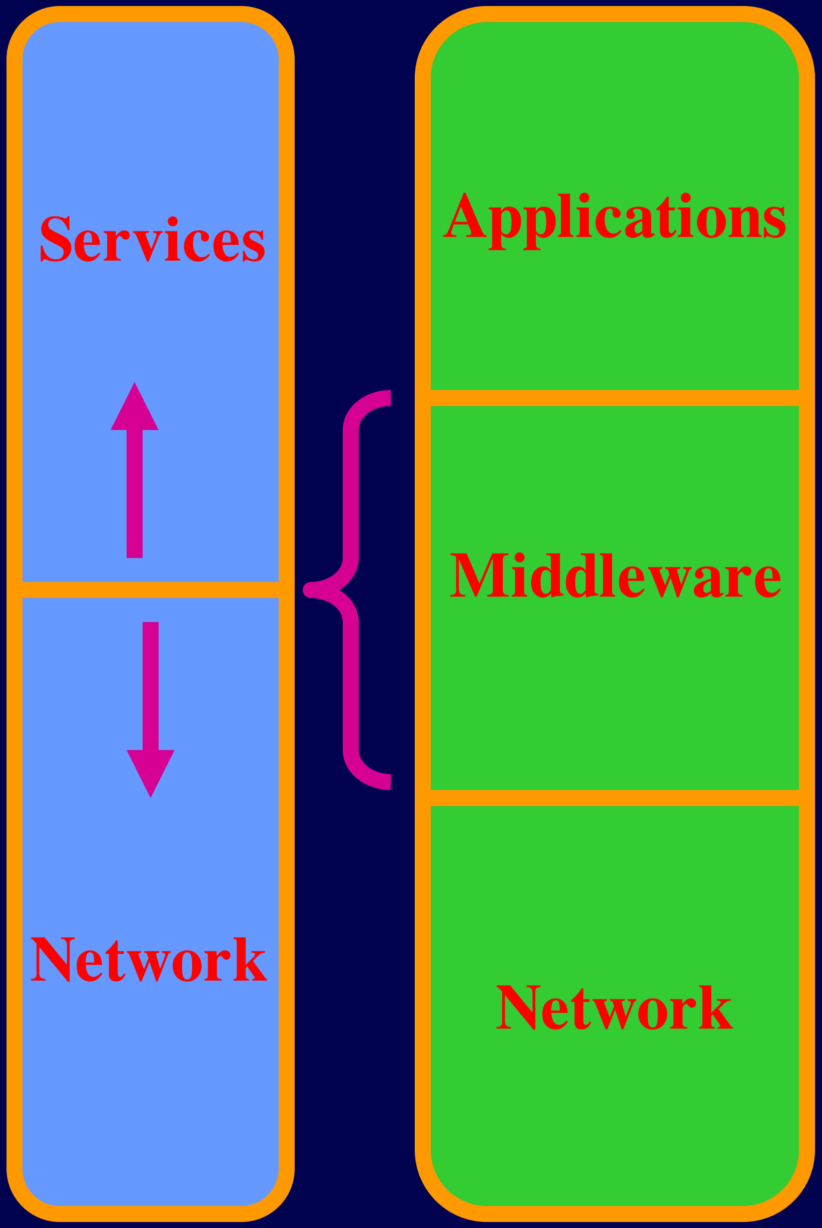
NOB

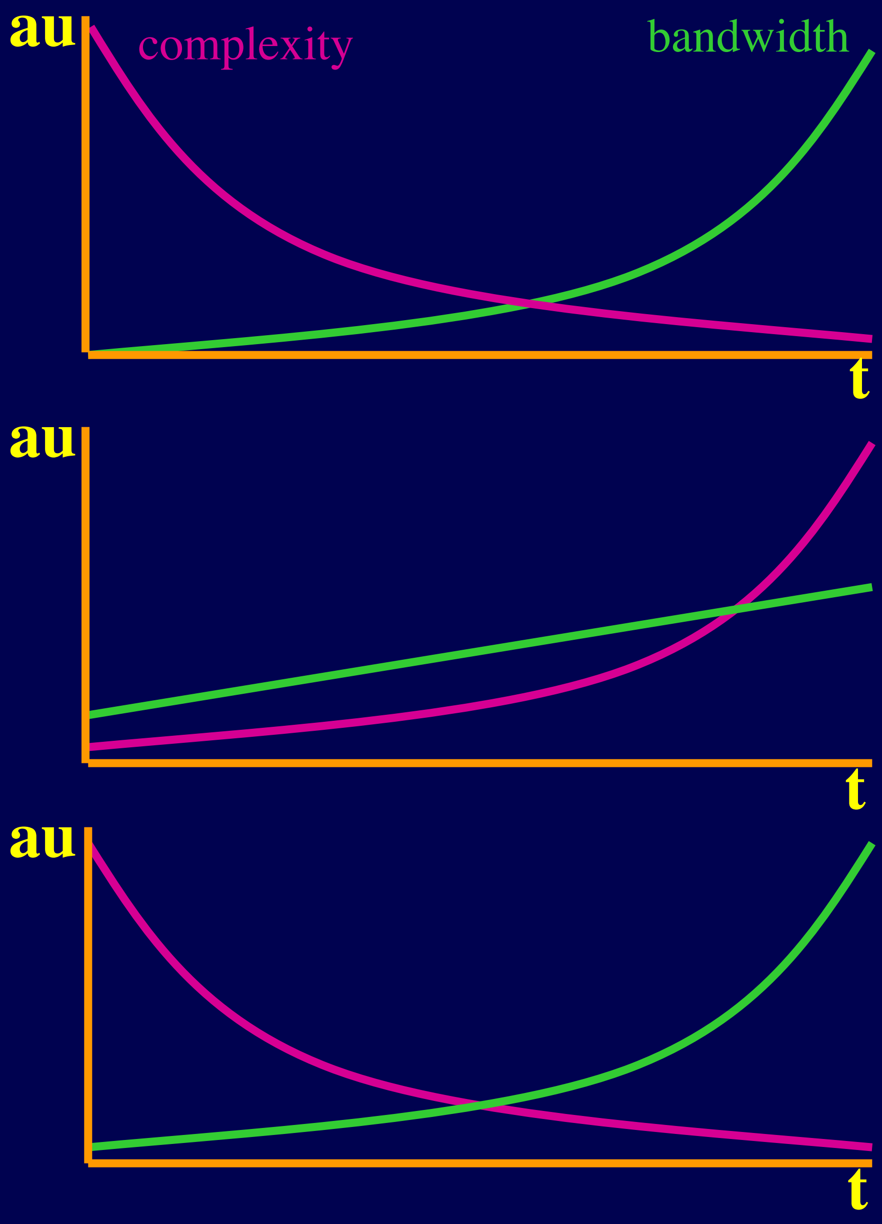
SURFnet

The three scenario's

- Bureaucracy
  - Do the advanced applications by hand
  - Long turnaround (rtt ≈ days)
- Complexity
  - Automatic application setup
  - Need advanced middleware and probably also bureaucracy
- Throw Bandwidth at the problem
  - Might go wrong at bottlenecks
  - Easiest solution
  - Do it yourself services

Stretching the OSI model



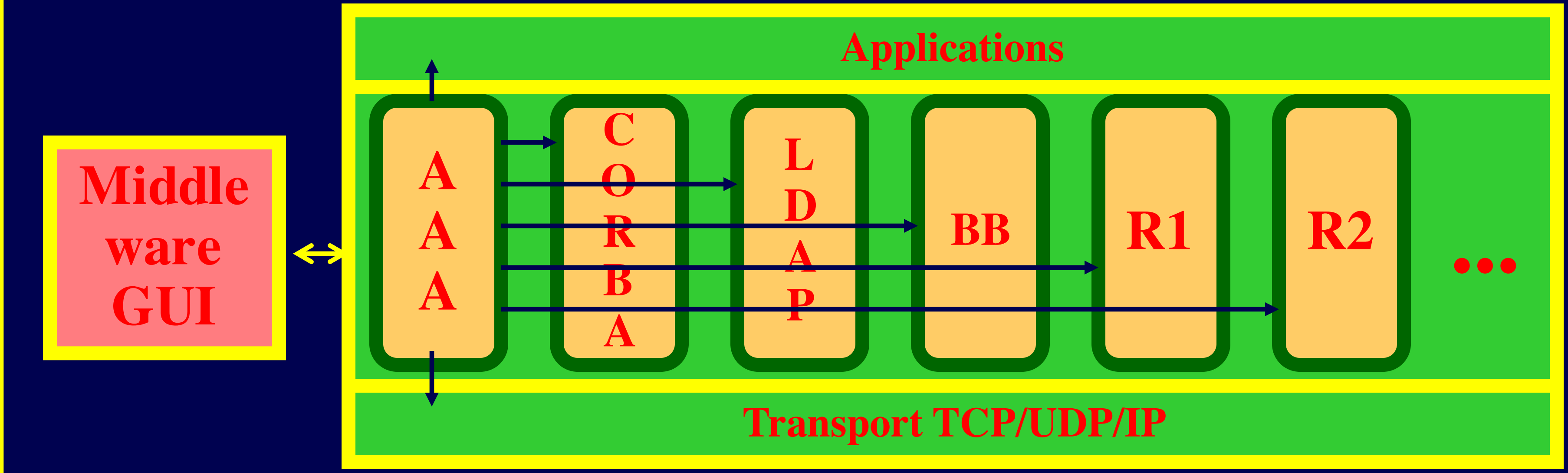


Current topics in the RG (Dublin 26-27 june)

- accounting model development in relation to generic architecture
- authentication: what is identity, model of authentication
- security, is that only a transport layer problem, encryption
- PKI infrastructure
- simulation, progress, what do we want to learn
- in light of the AAA-WG discussion, do we think of backward compatibility
- session identification (the need for layered modeling?)
- SIP (session initialisation protocol)
- Policy Definition Language
- inter kingdom relations and consequences for generic model
- management and auditing
- RG reaction to AAA-WG protocol discussions
- organizational stuff: IETF meeting, other meetings, drafts to produce ...

Questions

- Resource discovery <-> AAA discovery
- Is AAA high or low in middleware?
- All A's together or not?
- Should AAA be visible in the app or only stay in middleware and this way solve its user interface problem



Research Group - info

- Research Group Name: AAAARCH - RG
- Chair(s)
  - John Vollbrecht -- jrv@merit.edu
  - 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