IRTF - AAAARCH - RG

Authentication Authorisation Accounting ARCHitecture RG

chairs:

C. de Laat and J. Vollbrecht

www.aaaarch.org

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.

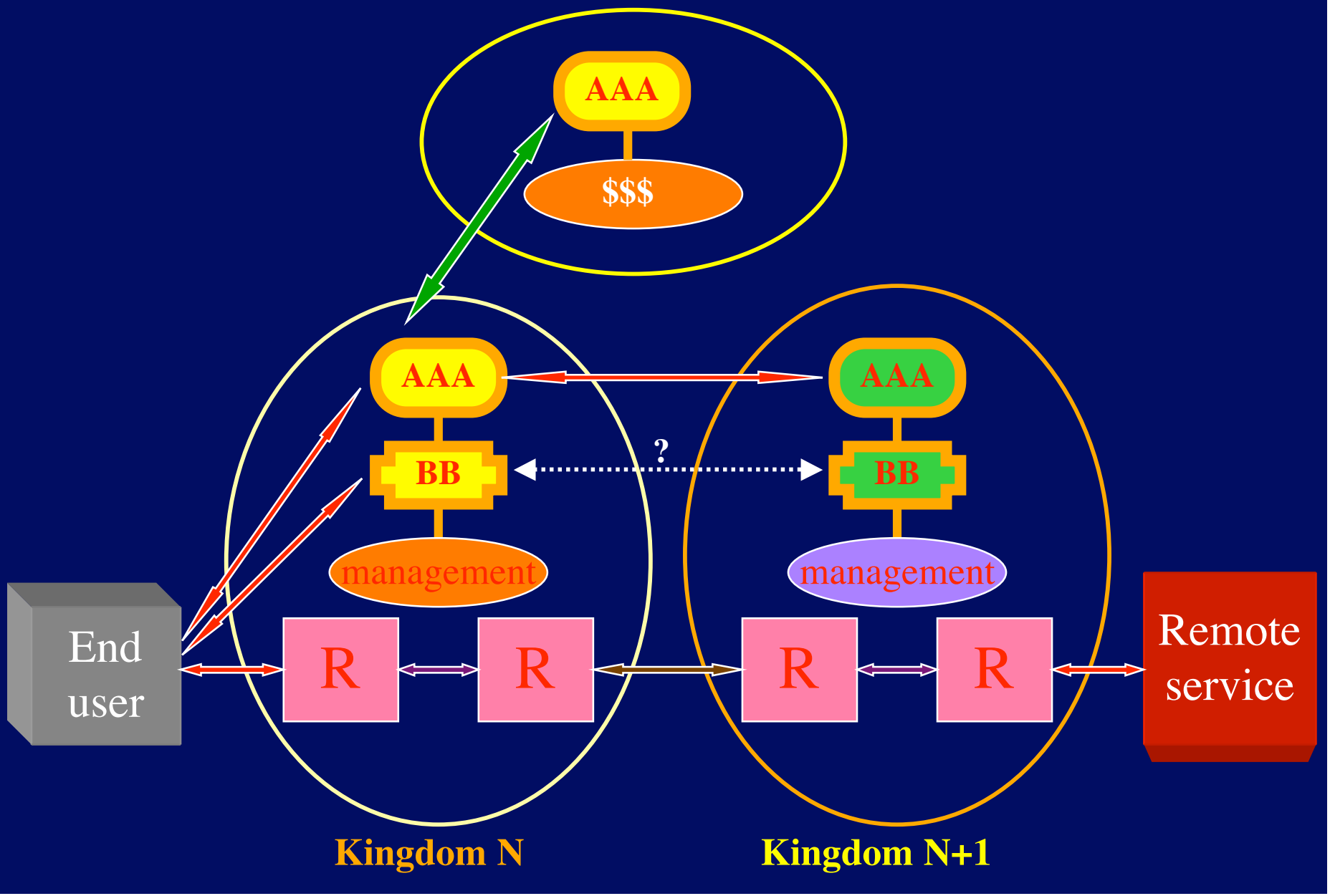
From charter

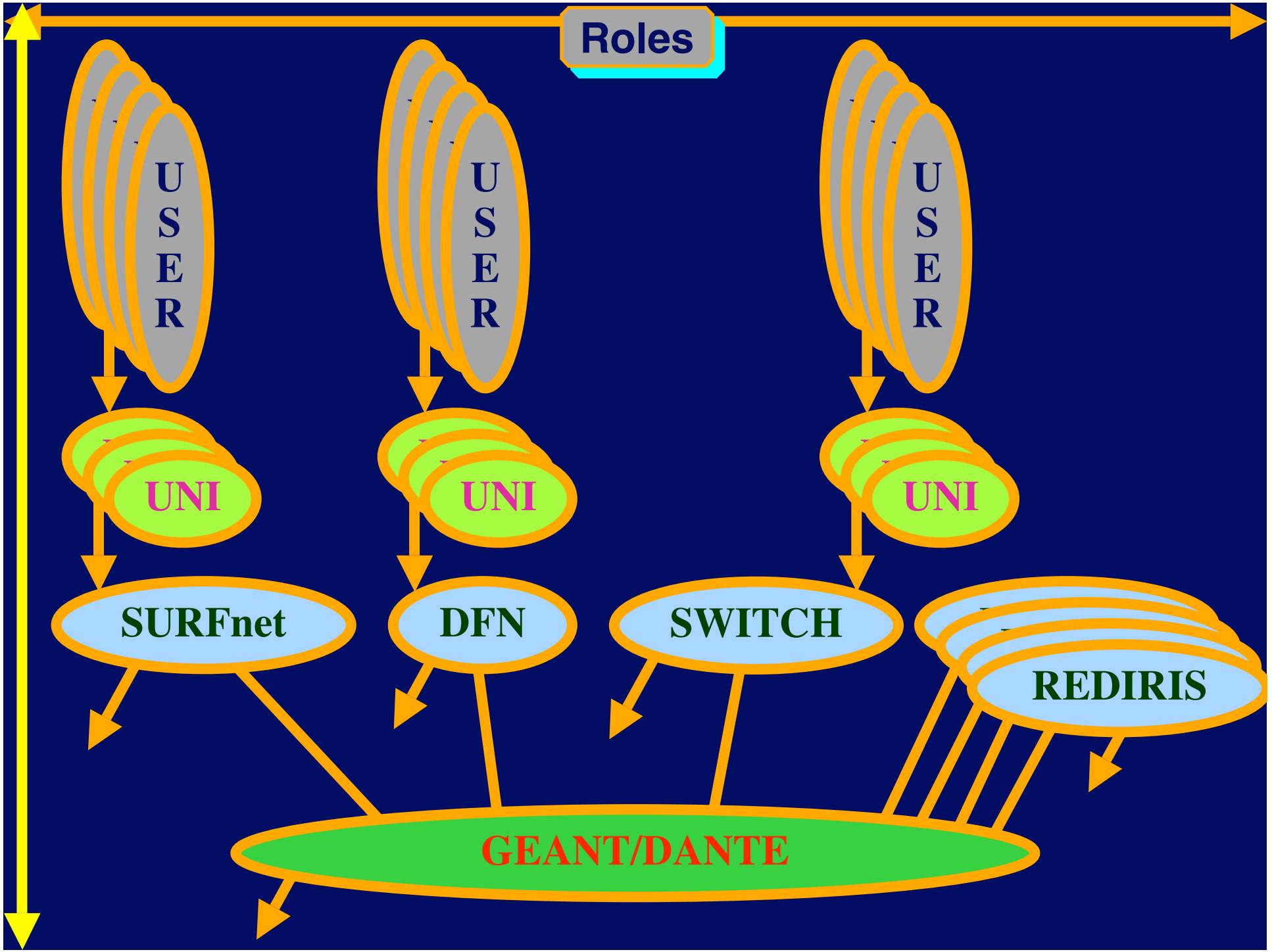
- **The architecture's focus is to support AAA services that:**
  - **can inter-operate across organizational boundaries**
  - **are extensible yet common across a wide variety of Internet services**
  - **enables a concept of an AAA transaction spanning many stakeholders**
  - **provides application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

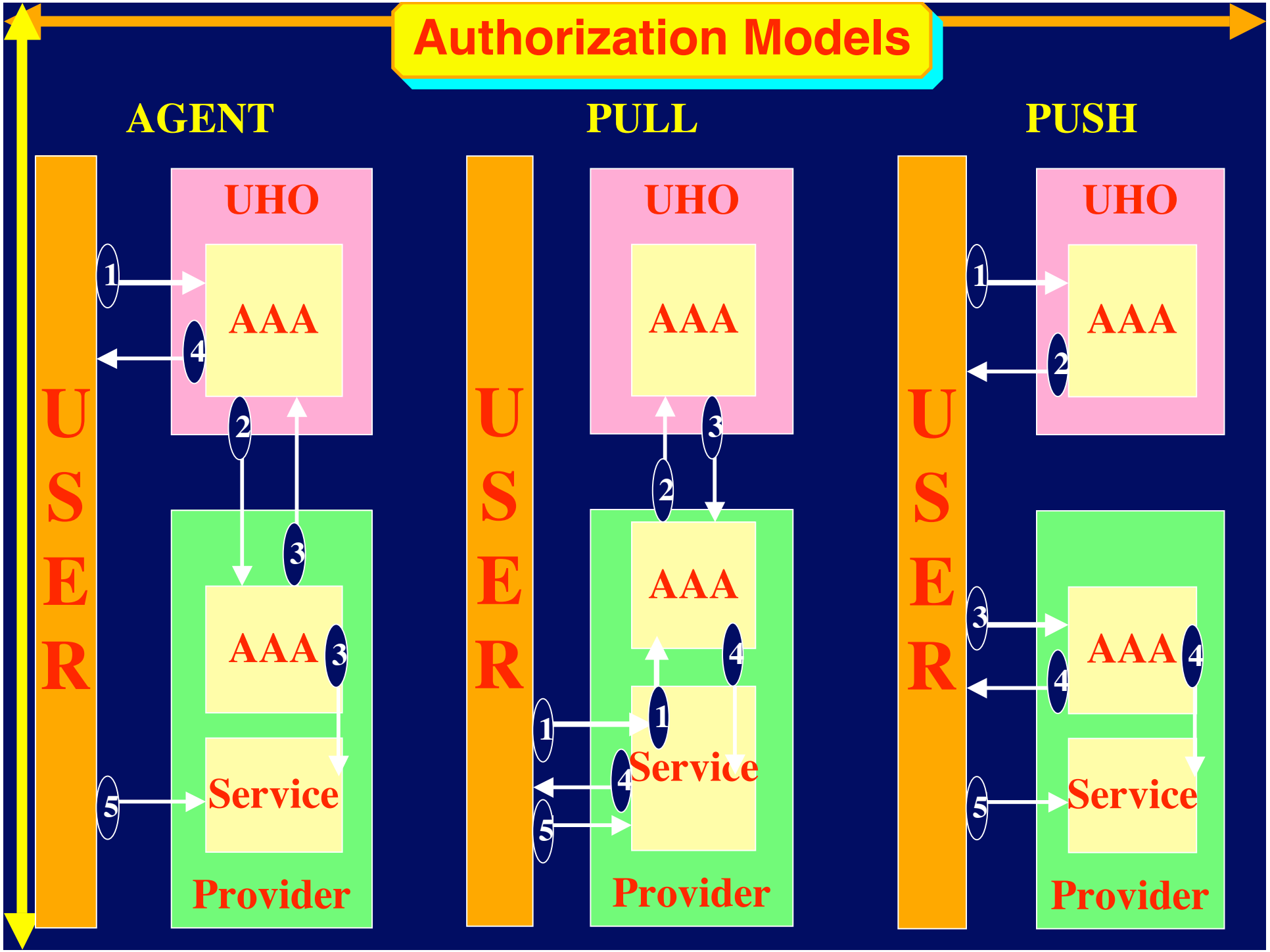
Basic AAA

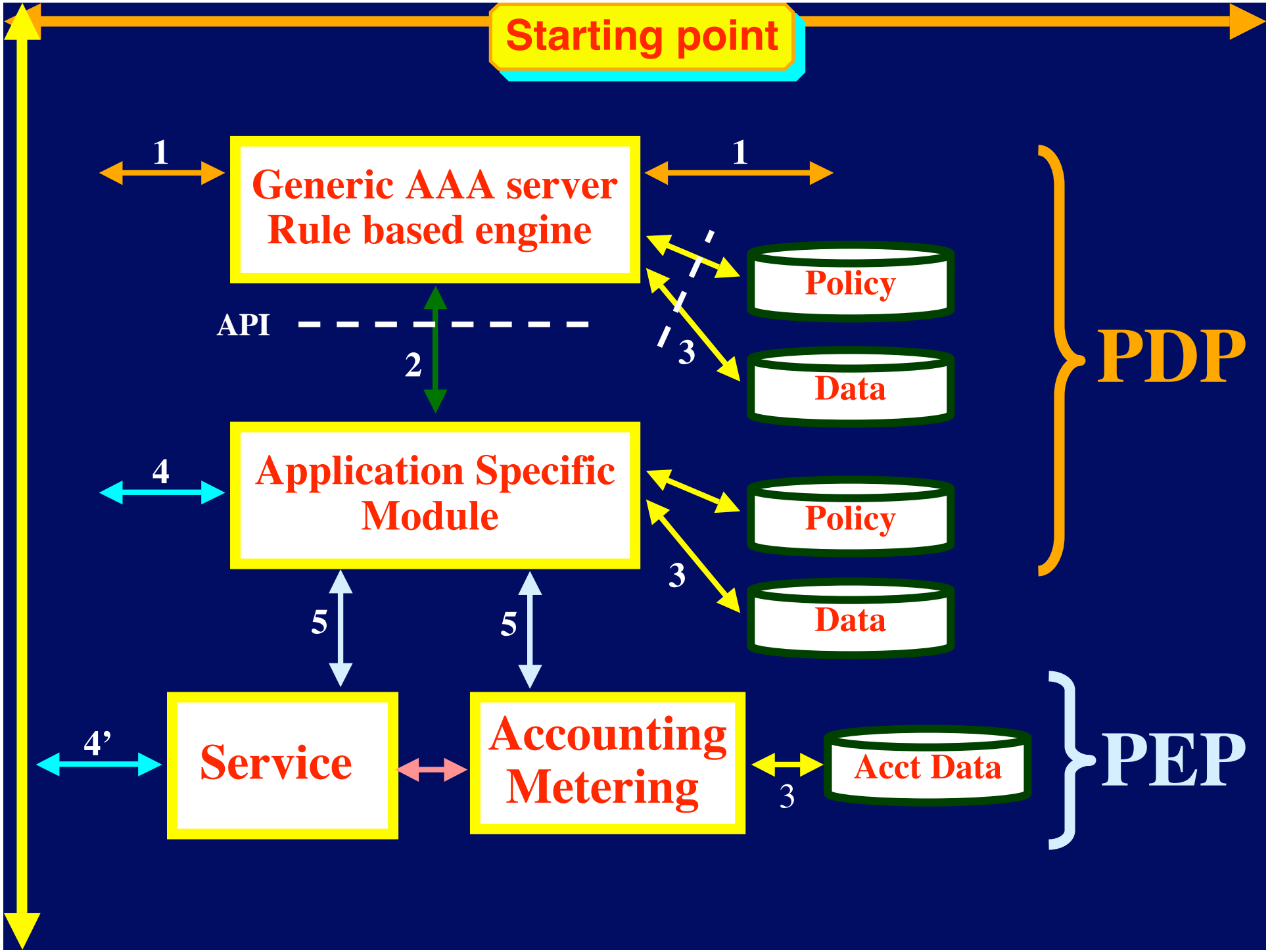
- **Service perspective:**
  - Who is it who wants to use my resource
    - » Establish security context
  - Do I allow him to access my resource
    - » Create a capability / ticket /authorization
  - Can I track the usage of the resource
    - » Based on type of request (policy) track the usage
- **User 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)

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

Agenda 50th IETF

CHAIRS: Cees de Laat <delaat@phys.uu.nl>
John Vollbrecht <jrv@interlinknetworks.com>

Cees de Laat	Agenda bashing, FNT and opening remarks
Cees de Laat	draft-irtf-aaaarch-generic-struct-00.txt
John Vollbrecht	draft-irtf-aaaarch-session-id-00.txt
Sebastian Zander	draft-irtf-aaaarch-pol-acct-02.txt
Guus Sliepen	draft-irtf-aaaarch-aaa-pol-01.txt
Guus Sliepen	draft-taal-aaaarch-generic-pol-01.txt
Steven Tuecke	security in the grid, overview
Bob Morgan	Shibboleth update
Bob Morgan	OASIS security-services TC
Henk Jonkers	Accounting Examples
chairs	closing remarks, next steps, summary, collect pink sheets

Opening remarks

- since San Diego:
  - interim meeting in Utrecht -> draft
  - 3 new drafts
  - 2 reworked
  - 2 teleconferences
    - About 8 participants
  - Discussion started with Grid-Forum
- Participation/contribution
  - Apart from about 3 or 4 places -> POOR!
- Evening meeting
- Re-charter (or not)

- 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

Charter - research items

- develop generic AAA model by specifically including Authentication and Accounting UNDERWAY
- develop audit-ability framework specification that allows the AAA system functions to be checked in a multi-organization environment NJET
- develop a model that supports management of a "mesh" of interconnected AAA Servers UNDERWAY
- describe inter-domain issues using generic model NJET
- work with AAA WG to align short term AAA protocol requirements with long term requirements as much as possible COULD be WORSE
- define distributed policy framework, coordinate with policy framework WG and others UNDERWAY
- develop an accounting model that allows authorization to define the type of accounting processing required for each session DONE
- implement a simulation model that allows experimentation with the the proposed architectural models UNDERWAY
- complete the work in Q3 - 2000 (ambitious) FAILED!

Revised charter

- ADD:

1. Define the type 1 interface in a high level and abstract way.
2. Define the functionality of the Driver Policy.
3. Define the functionality of the type 2 interface.
4. Work with GridForum and Internet2 to include APP-SEC
5. Work with RAP group on standards
6. Define exactly which doc's to produce and get it done (see table).

- REMOVE

1. Time constrain to create room for research

- FIND

1. Draft authors

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.aaaarch.org
- **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


AAARCH