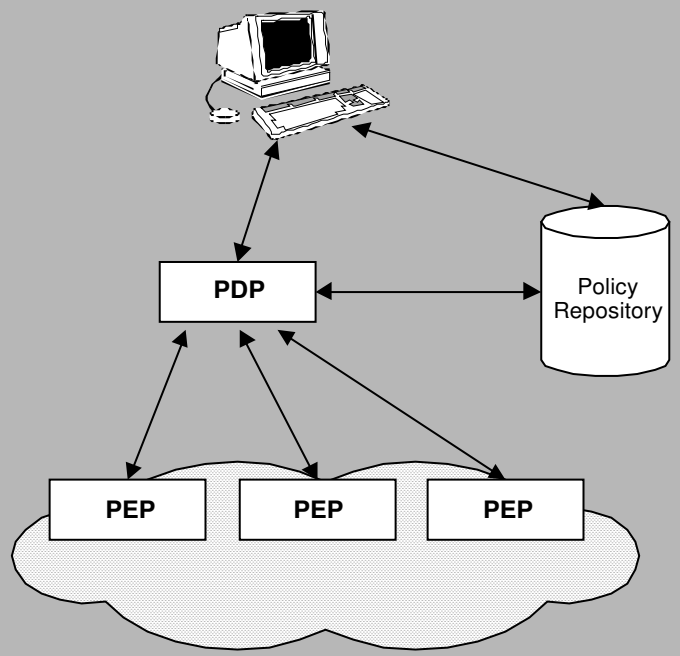
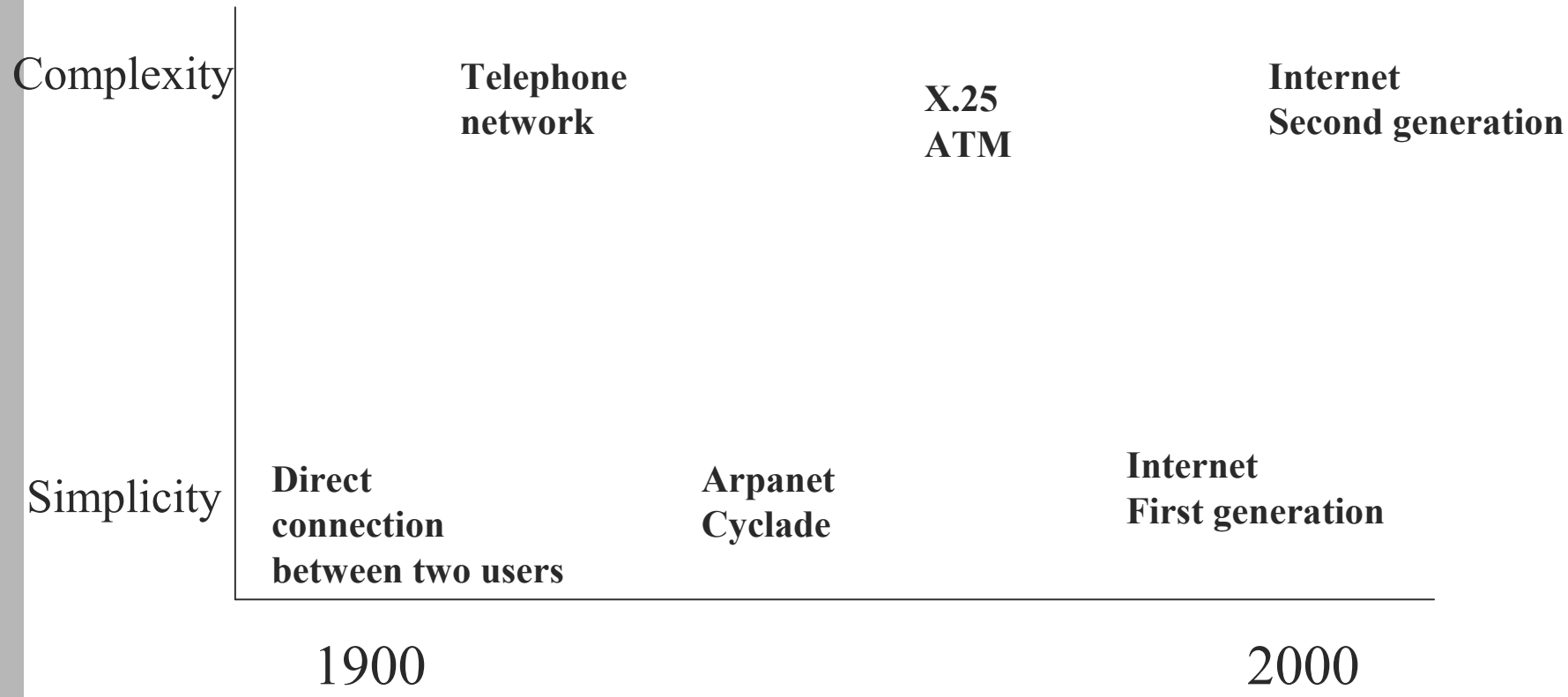
Policy and Network



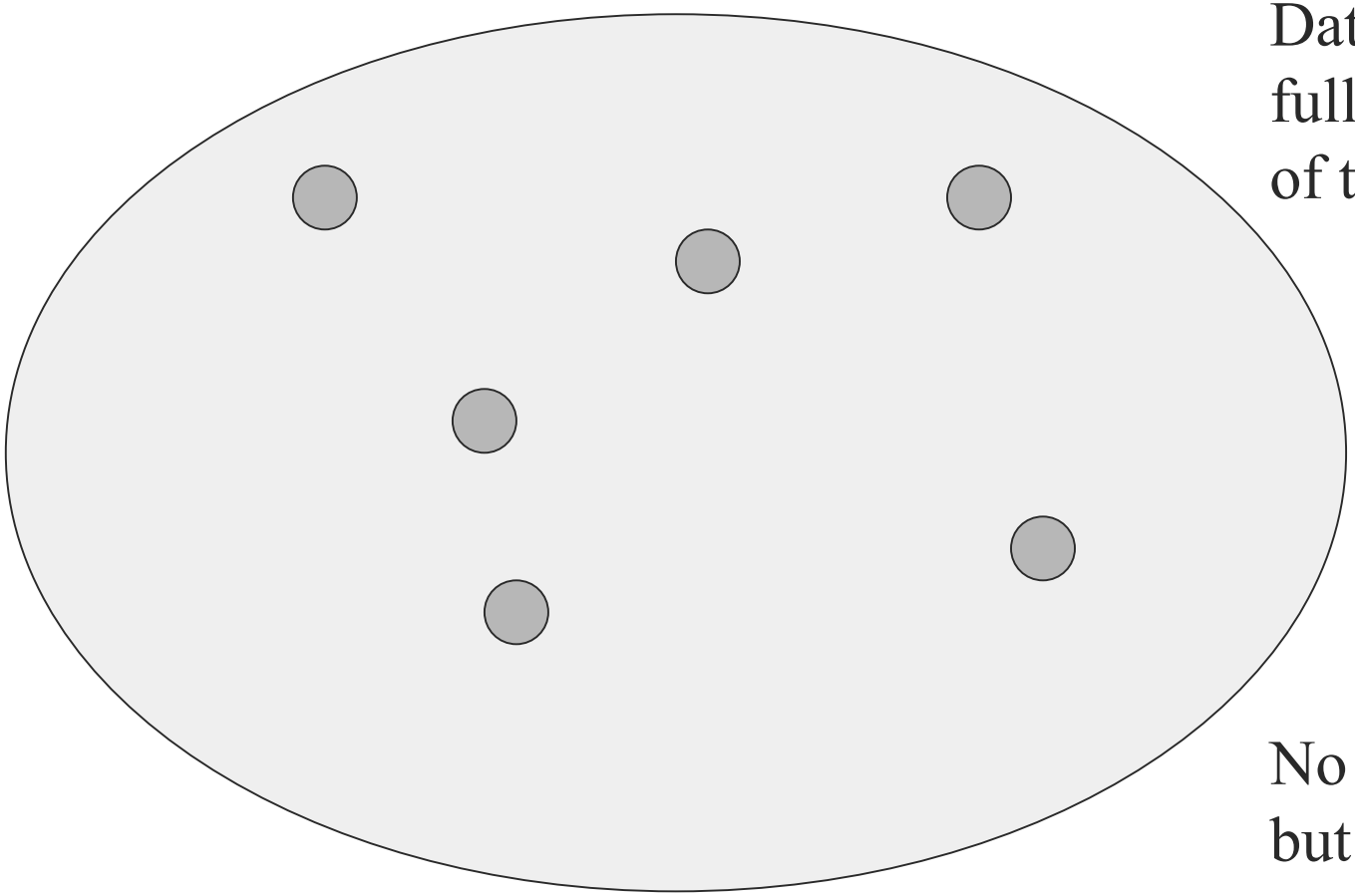
Policy and networks

- Introduction
  - context
- Information model
  - principles, QoS, …
- Architecture
  - principles, componants, …
- Implementation
  - performance

Evolutions


Complexity
Telephone network
X.25
ATM
Internet
Second generation
Simplicity
Direct connection between two users
Arpanet
Cyclade
Internet
First generation
1900
2000

Internet: No signalling

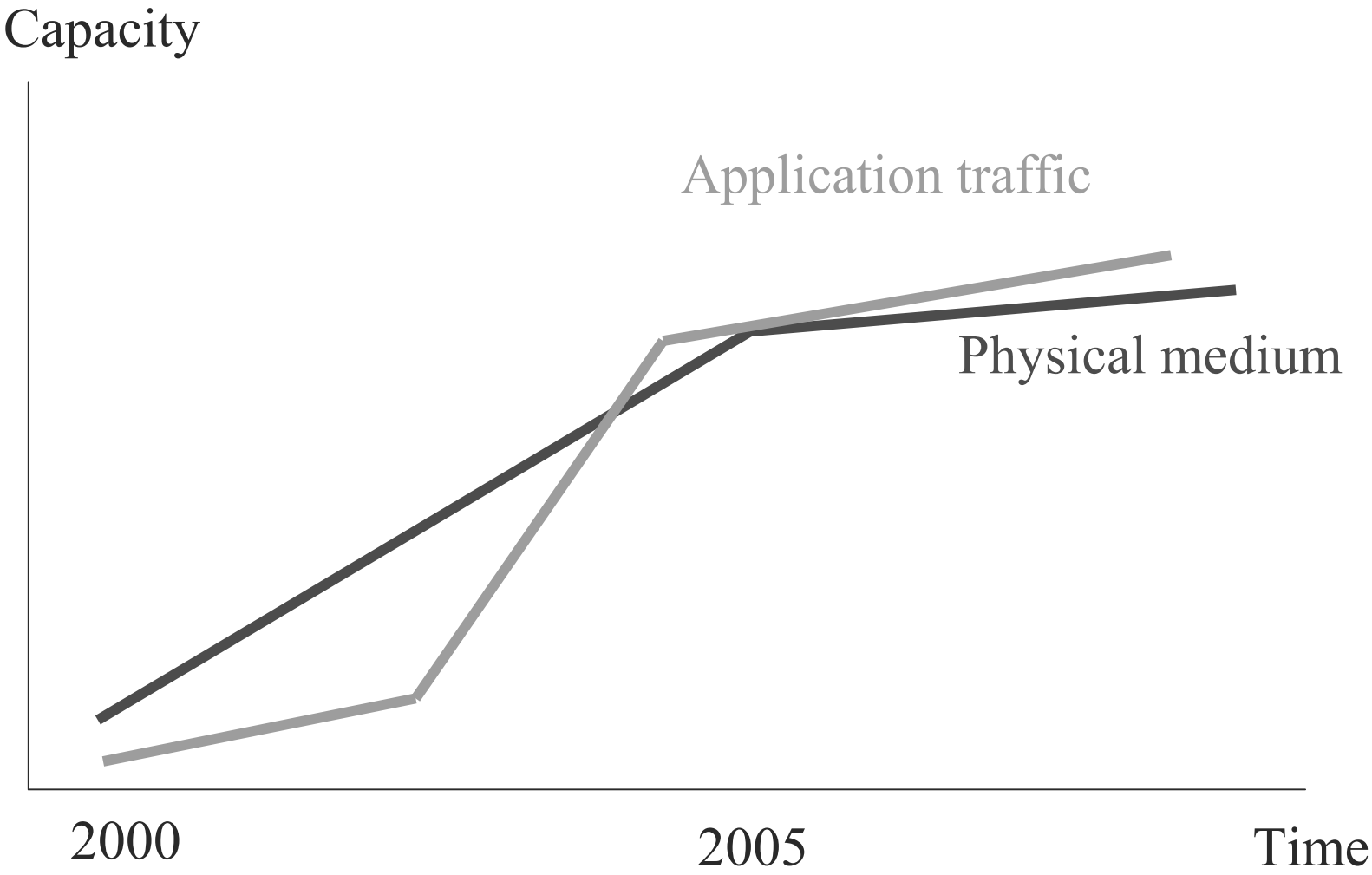


Datagram:
full address
of the receiver

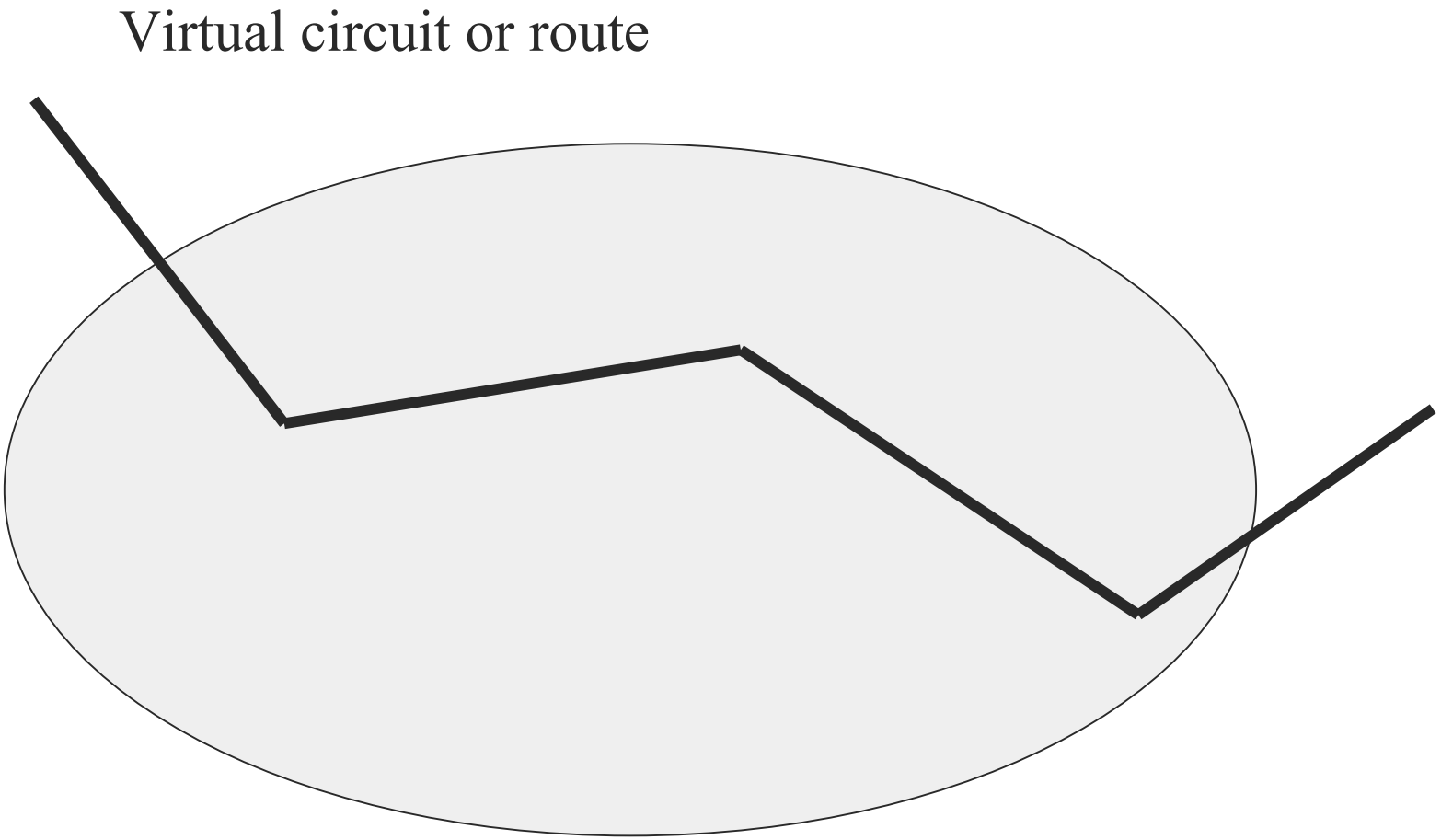
No QoS
but simple

Indeed, it's an excellent signalling network

Oversizing


Capacity
Application traffic
Physical medium
2000
2005
Time

X.25, ATM, …: Signalling

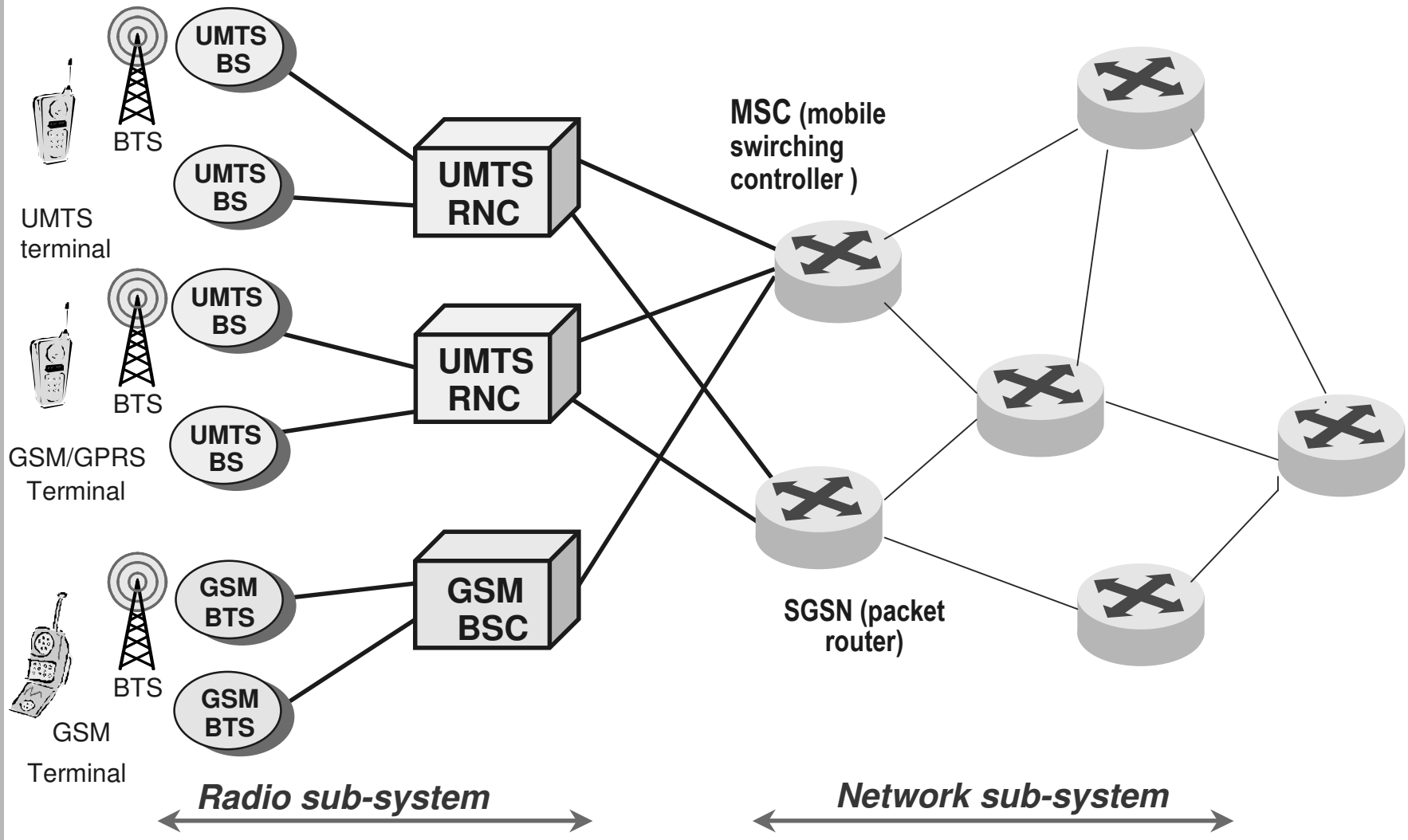


Soft signalling

General direction: determine a route to allow reservation and get a quality of service

- Virtual connection
  - « hard state »
  - A signalling for set-up and resume a communication
  - Changing a route is quite complex
- Fixed route
  - « soft state »
  - First packet of the flow to set-up the route
  - Modification of the route is simple
  - A time-out to close a route

IMT-2000 and UMTS architecture



Origin

Control and management of different areas

⟹ QoS, security, network management, …

- Centralized management
- Abstract objects
- Independence of equipments
- Automatization
- More homogeneous interfaces

Policy-based Management

The more advanced field : QoS

- New signaling protocol (COPS) and new architecture (PEP/PDP)
- Extension of RSVP for COPS

Generalization

- Need to generalize this approach to insure interoperability of the different implementations

Terminology

Politicy

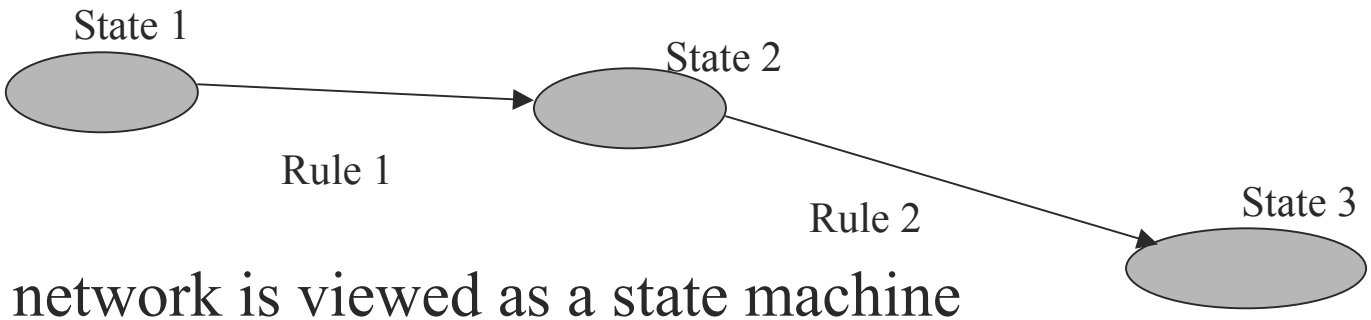
- A representation of a business objective to be implemented in the management domain by means of policy agents or policy enforcement points.
- A policy defines one or more rules. Each rule binds one or more actions to sets of conditions that describe by whom (users), for what (systems, applications), and in which circumstances (time, day of week, date) the actions may be triggered.

≠ Management of the configuration of routers

What is network policy?

Policy rule : If <condition> then <Action>

Example: If <Hour is less than 11 p.m.> then <Do not accept best effort trafic in the network>



The network is viewed as a state machine

Application areas (policy disciplines)

2 main fields

- Management of the quality of service (QoS)
- Security in IP networks

Other possible fields

- Mobility
- Access control
- Address allocation (DHCP)
- Routing
- …

Working group

Definition of models and the architecture

- DMTF SLA WG
- Policy Framework
- IP Security Policy
- Resource Allocation Protocol

Working groups

- AAA / IRTF AAAARCH
- BuDS (Building Differentiated Services)
- ISSLL (IntServ over Specific Link Layers)
- DiffServ
- …

Abstract views of a network policy

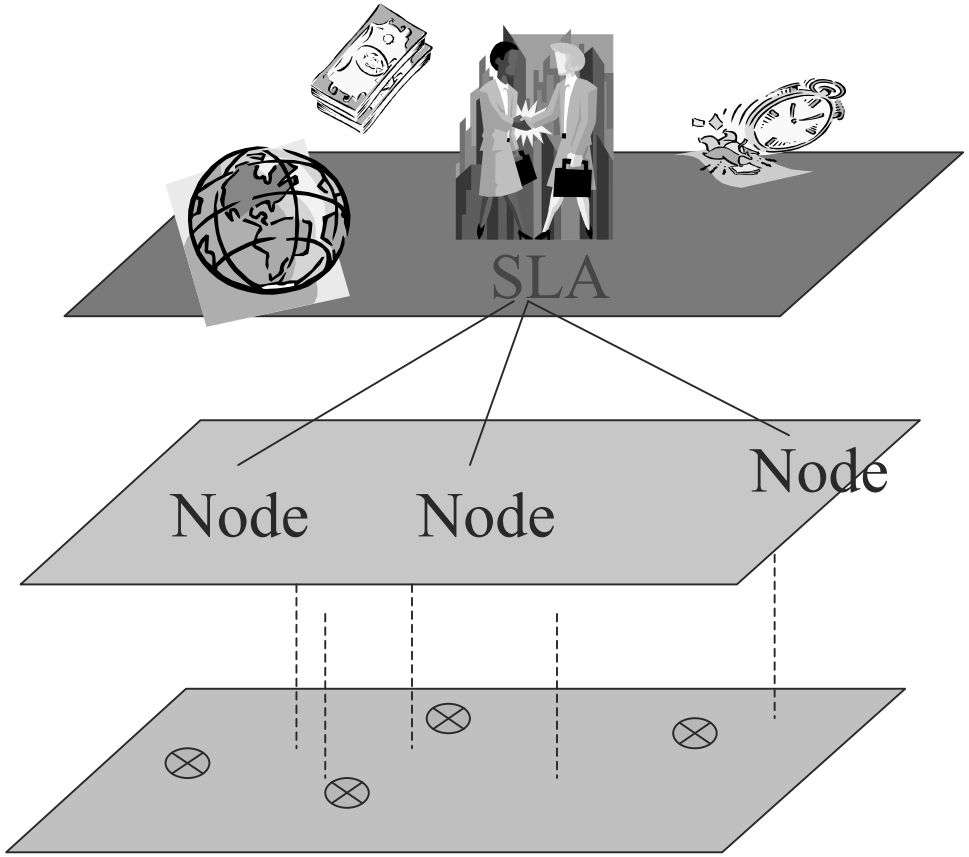
Network Level
(topology, network objectives, global ressources utilization, SLA, SLS)

Node level

(Policy rules, QoS objectives)

Device level

(Classification, policing, buffer management, scheduling)



Three important areas for Network policy

Usage policy

Diffserv classes, VPN, encryption capabilty, …

- Describes which services will be used to maintain the current state of the network or to move to a new state.
- Describes how these services will be used.

Policy triggering

- **Static**
- **Dynamic**

Policy level of application

- User level
- Application level
- Service level
- Class level

Network policy : relevant areas

How to translate economic goals into their realization in the network?

Network policy architecture

Policy representation

Policy storage

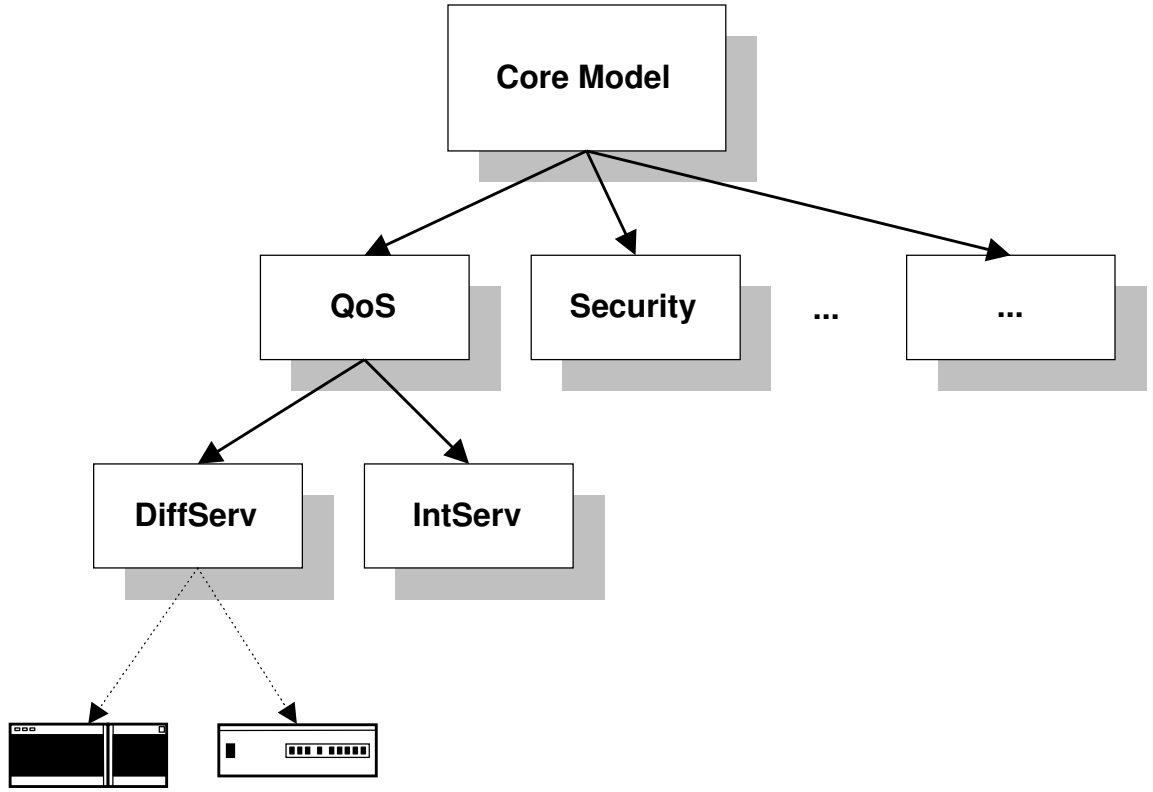
Policy protocols

Information model

Domains

Technologies
(Device Independent)

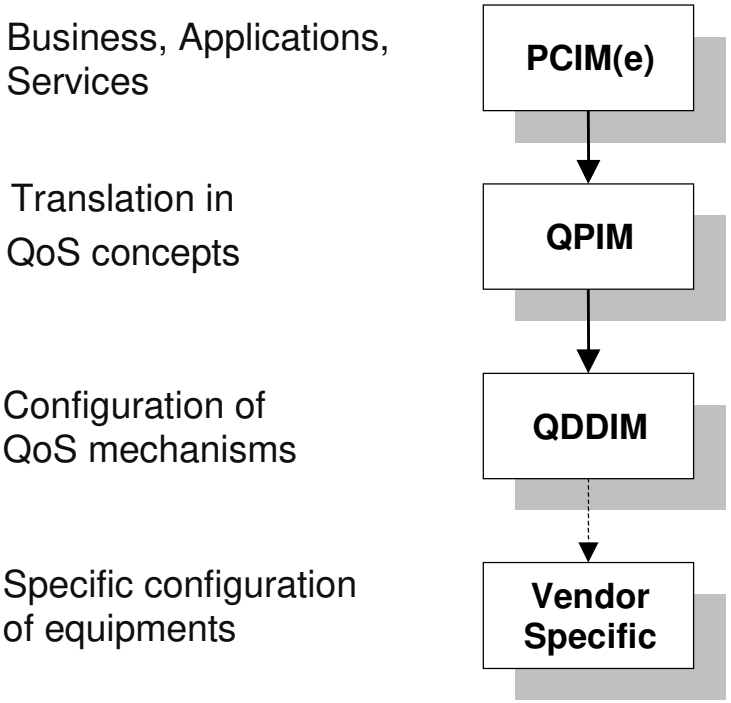
Equipments



Information model

Hierarchy of the rules

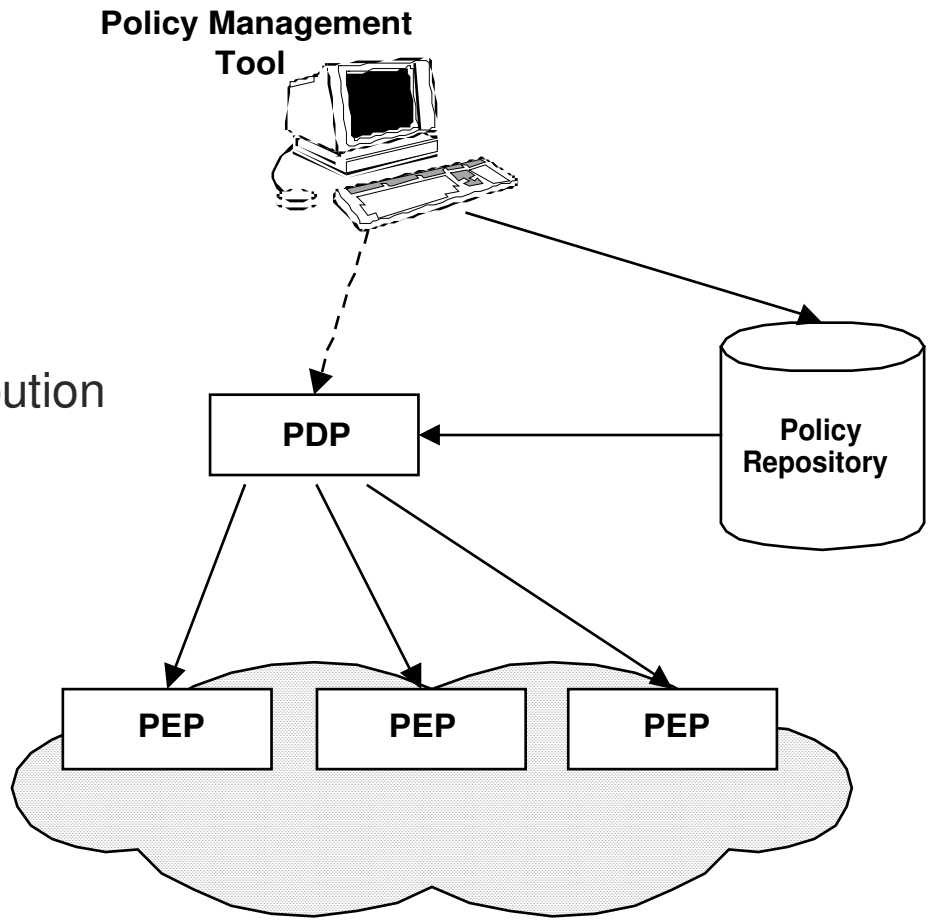
- Abstract rules ⟹ Equipment configuration



Architecture

Principles

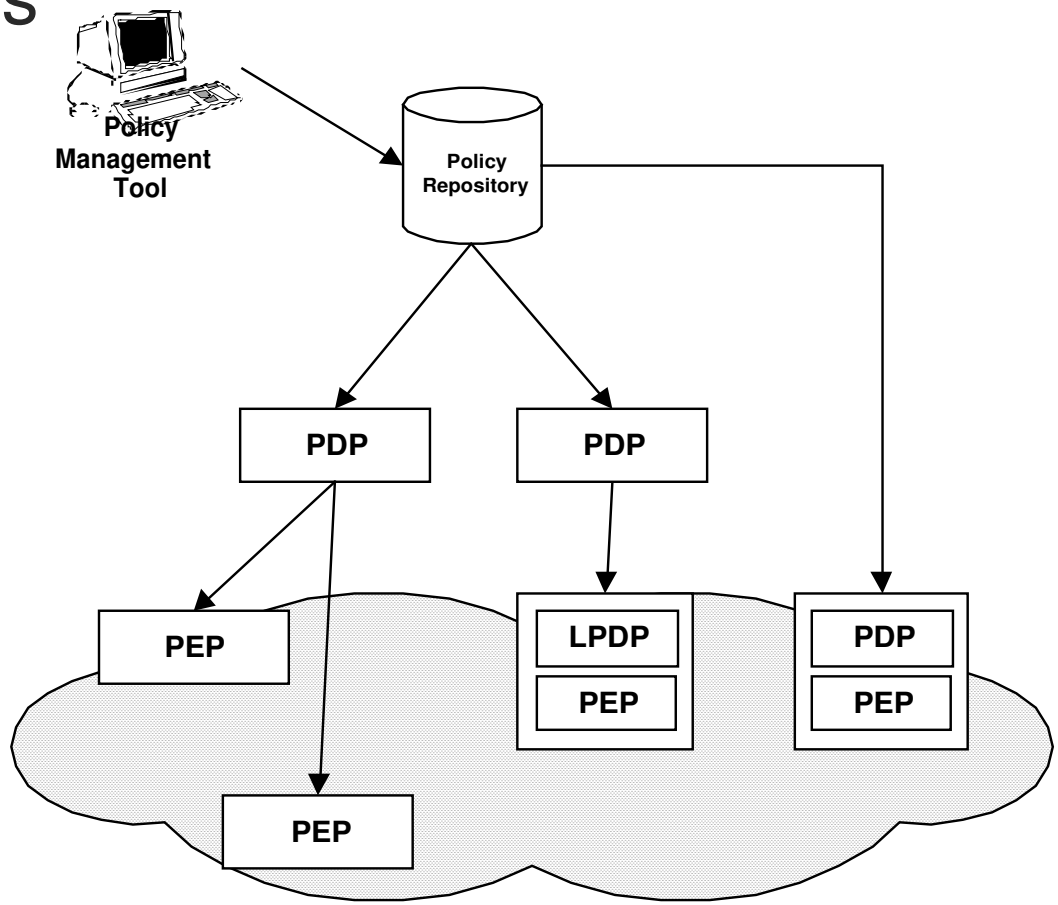
- Centralized model
  - Policy management
  - Policy repository
  - Policy decision
  - Configuration distribution



Architecture

Possible variations

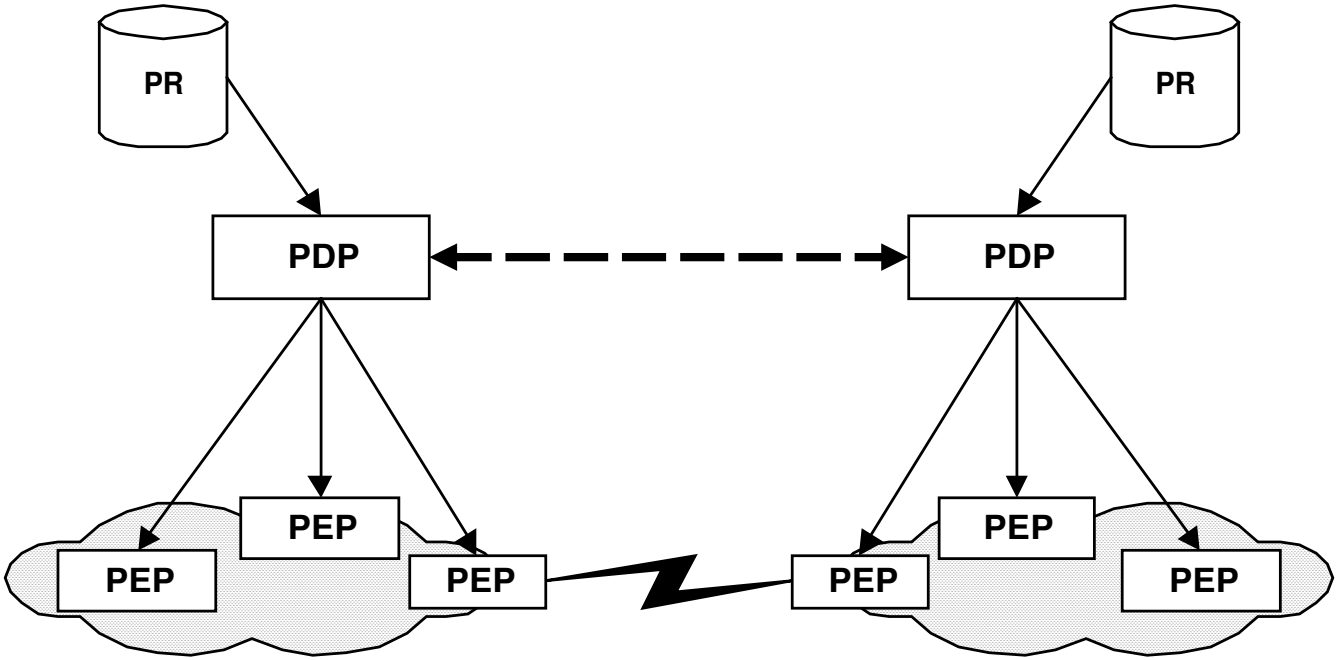
- Several PDPs
- Local PDP
- PDP integrated (*local*)



Architecture

Possible variations

- Several domaines



Terminology

Definition (IETF Policy WG)

- PEP
  - « A logical entity that enforces policy decisions »
- PDP
  - « A logical entity that makes policy decisions for itself or for other network elements that request such decisions »

Other versions (more general ?)

- PEP
  - An agent running on or within a resource that enforces a policy decision and/or makes a configuration change.
- PDP
  - The core component of a policy-based networking system; it persists policy information in a policy repository, support one or more policy consoles for the construction of policies, and utilizes one or more policy agents to enforce policies.

PEP

Functions

- May be accessible and configurable
  - COPS client, SNMP agent, …
- Link between the external representation (PIB/MIB) and the internal configuration of the equipment.
- Can ask validation by the PDP
- Insure the coherence of local policies and check their good application
- Check the exactness of accounting
- …

PDP

Functions

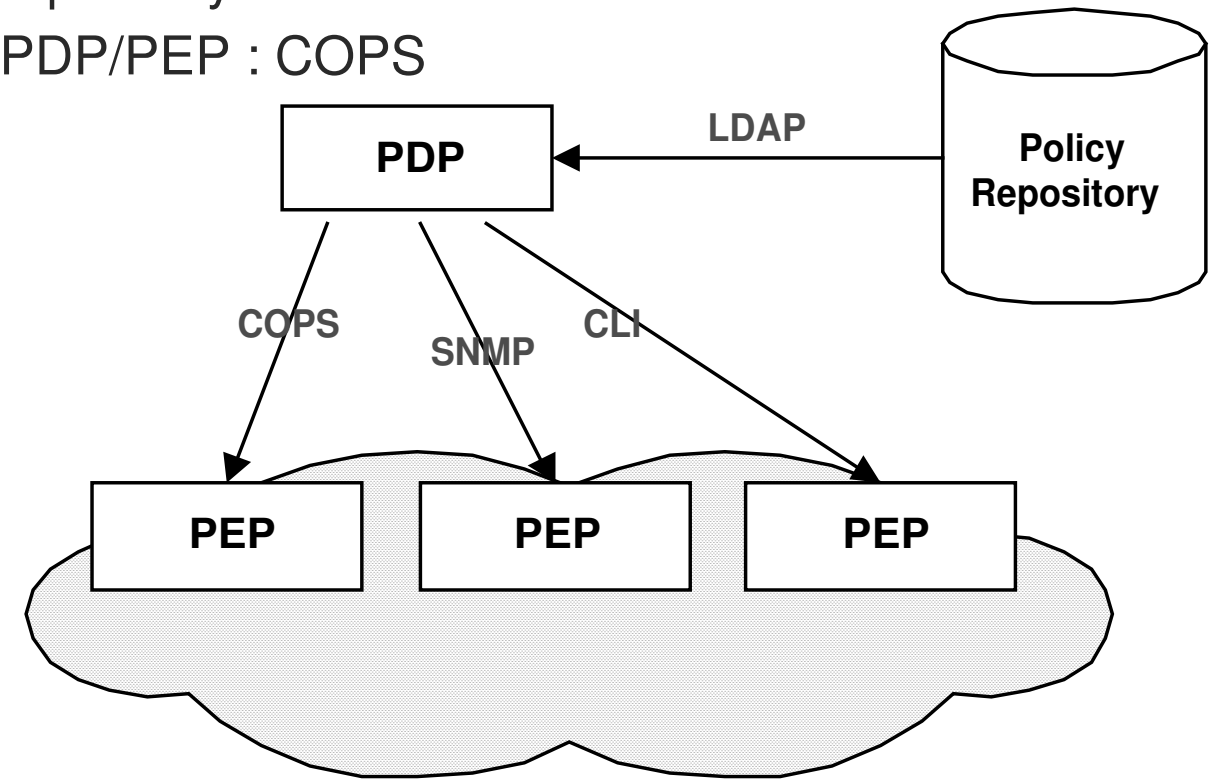
- Identify the rules that can be applied to the PEPs
- Determine what rules to apply
- Transform the rules in a understandable format to be applied on the PEPs (PIB/MIB/…)
- Propose an interface with external servers, if necessary.
  - authentication
  - billing
  - …
- Take care of the distribution of configurations (provisionning, scheduling)
- Management of the negotiation with PDPs
- …

Decide of the rules to apply

Communications

General architecture

- No mandatory protocol …
- repository : LDAPv3 ?
- PDP/PEP : COPS

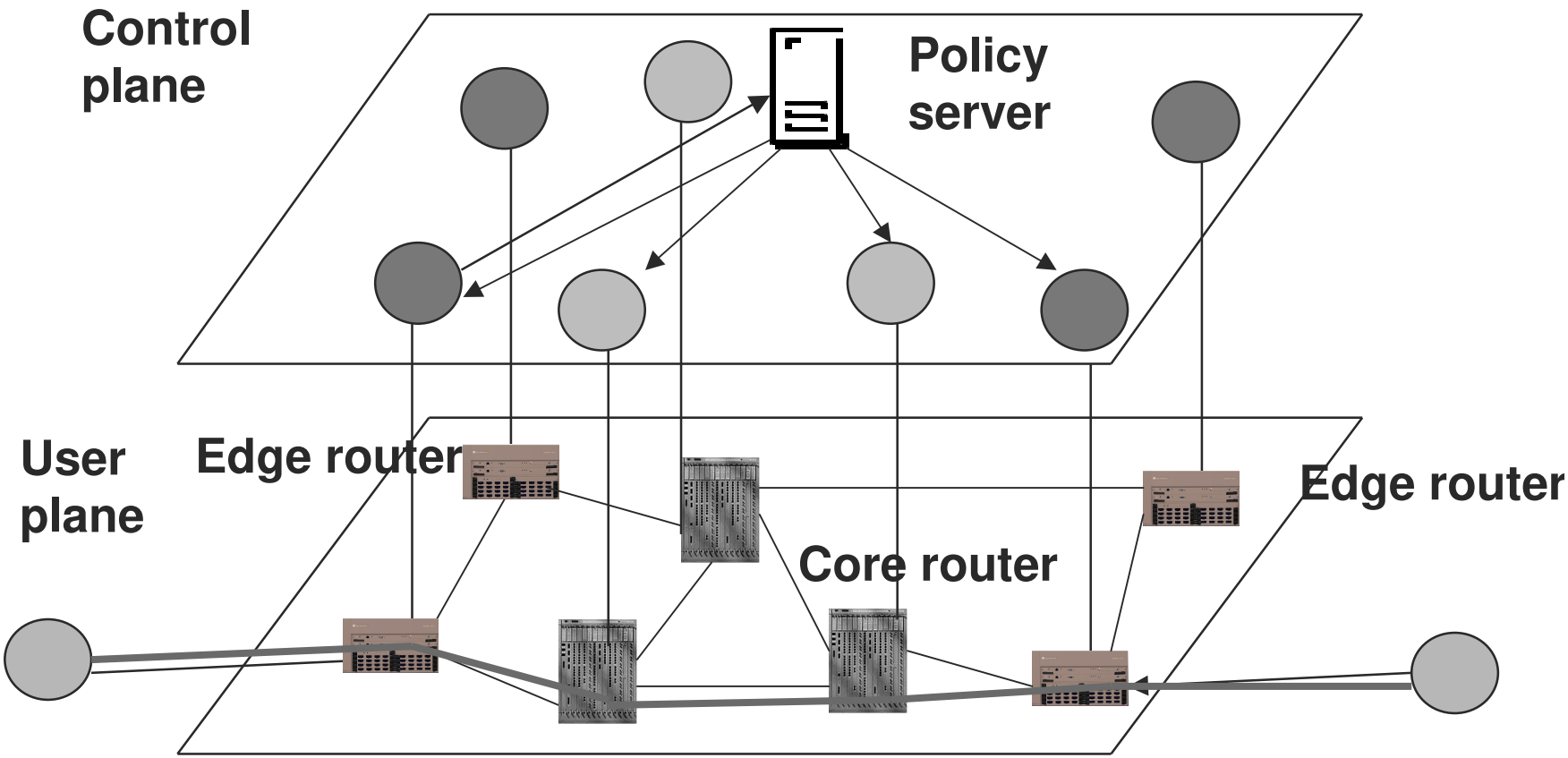


Implementations

Difficulties

- Translation of the rules from the abstract definition to the configuration of equipments
- Validation of rules, detection of conflicts and …
- Automatic discovering of resources
- Algorithms for PDPs
- Management of dynamic rules
- …

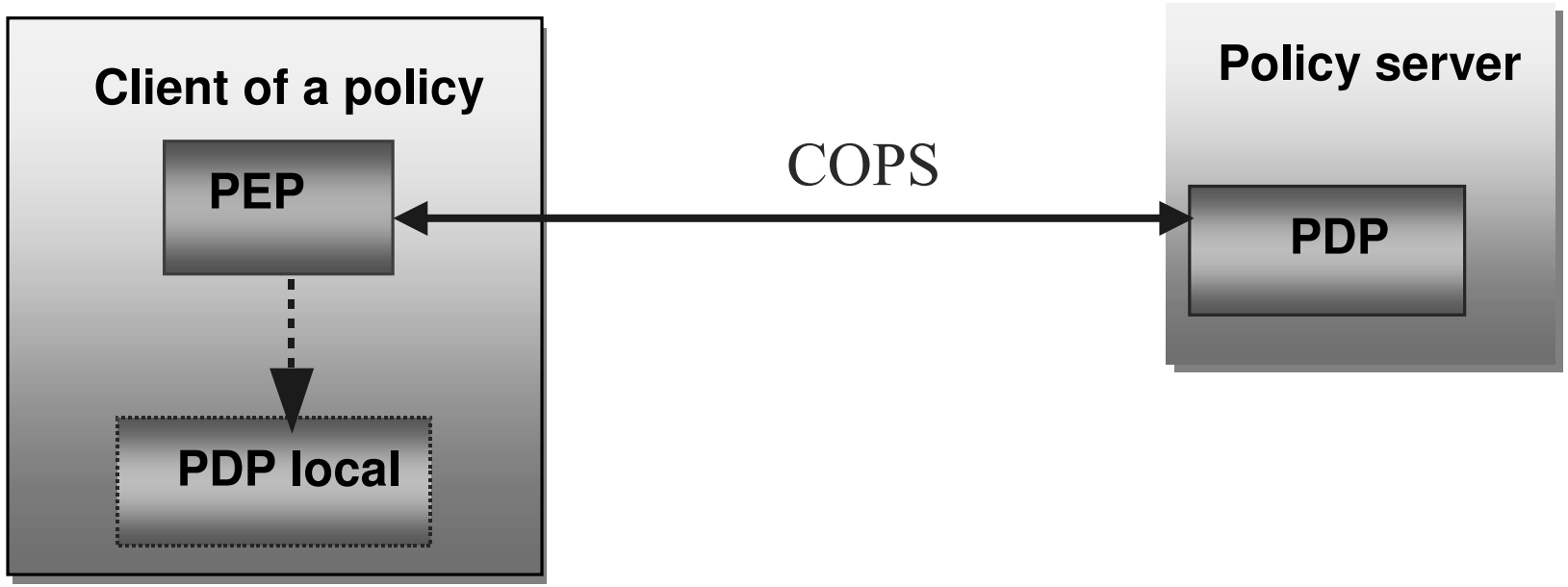
The signalling: COPS (Common Open Policy Service)



Configuration of the edge router

The COPS Protocol

PEP (Policy Enforcement Point)
PDP (Policy Decision Point)
LPDP (Local PDP)



COPS

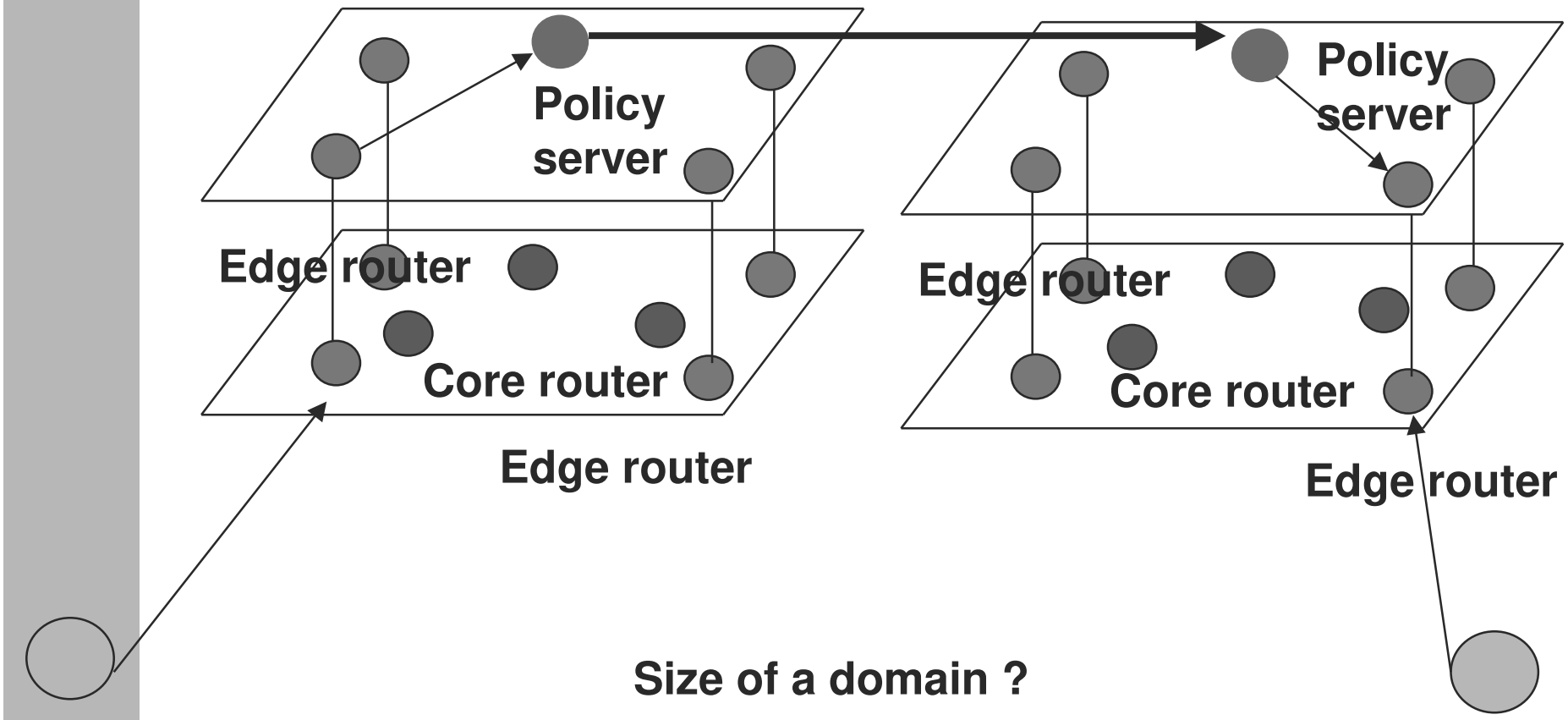
COPS Common Open Policy Service

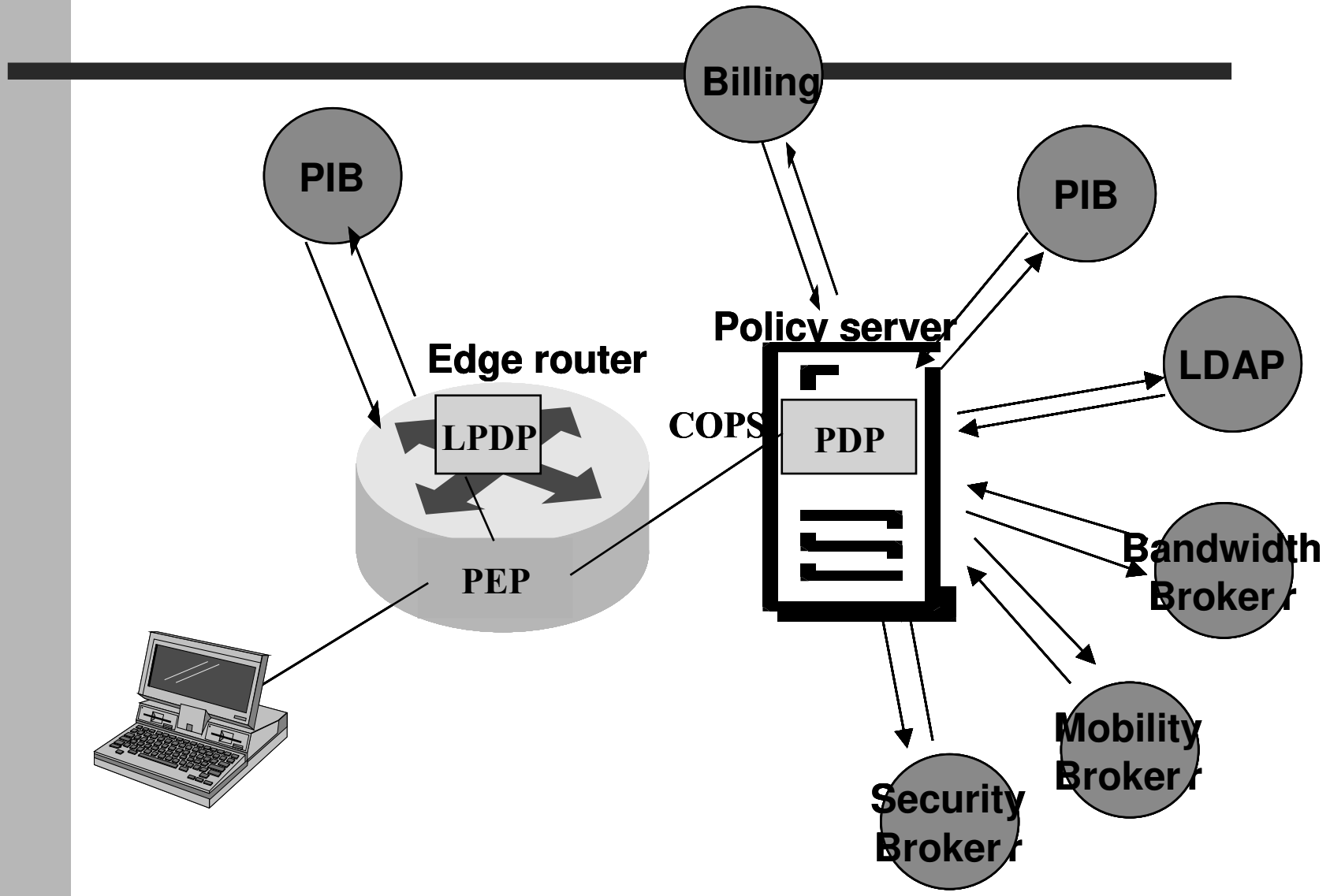
Simple request/response protocol for the exchange of rules (policy)

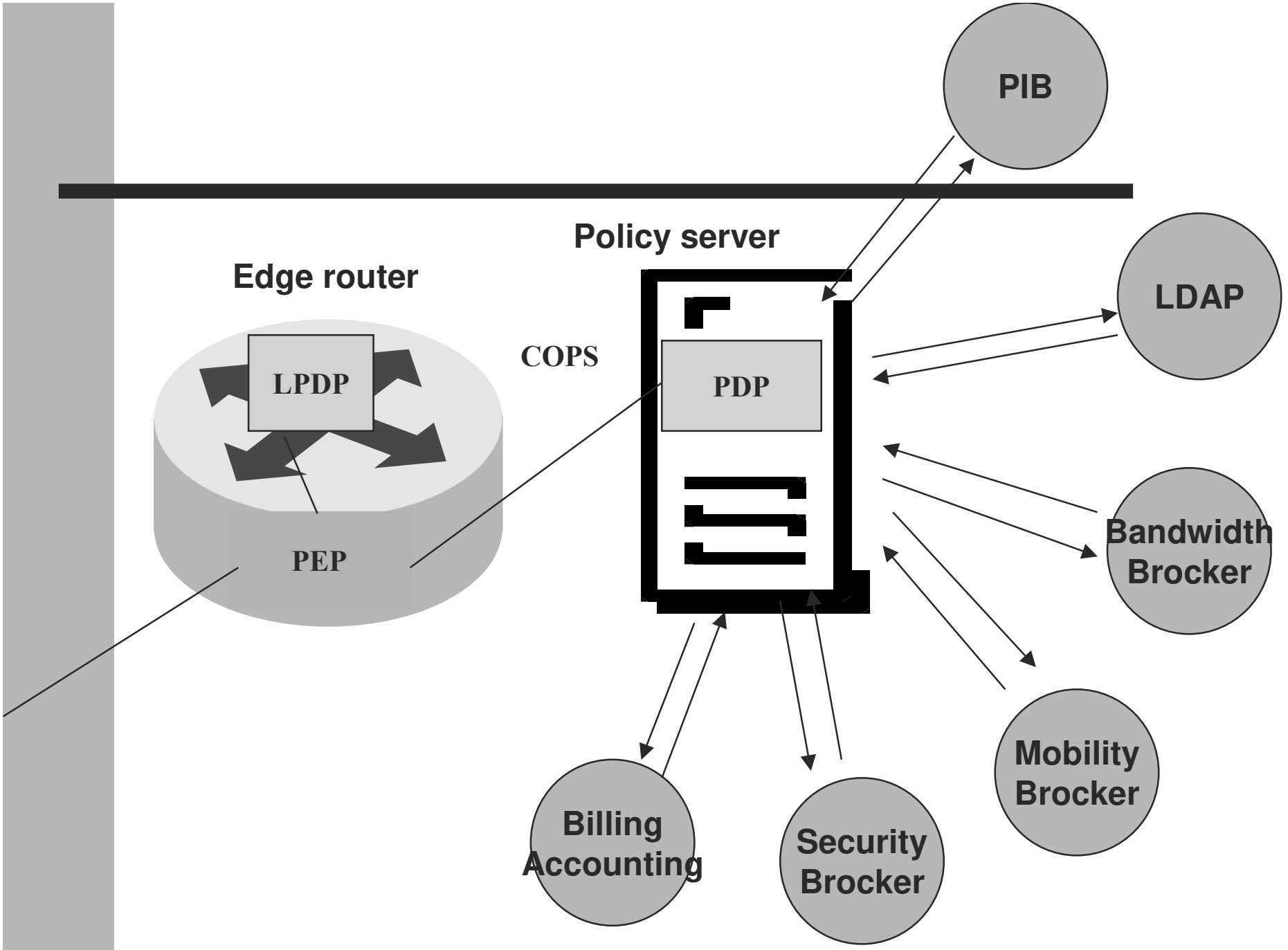
- Admission control based on domains
- Between a PDP (Policy Decision Point) and a client or PEP (Policy Enforcement Point)
- A PEP is generally a router

Based on TCP to insure a good quality

Inter domain signalling




Billing
PIB
PIB
Policy server
Edge router
LDAP
COPS
LPDP
PDP
PEP
Bandwidth Broker
Mobility Broker
Security Broker


PIB
Policy server
Edge router
LDAP
COPS
LPDP
PDP
PEP
Bandwidth
Brocker
Mobility
Brocker
Billing
Accounting
Security
Brocker

COPS and signalling systems

COPS outsourcing

- COPS-RSVP
- COPS Mobile IP
- COPS-ODRA (COPS Outsourcing DiffServ Ressource Allocation)

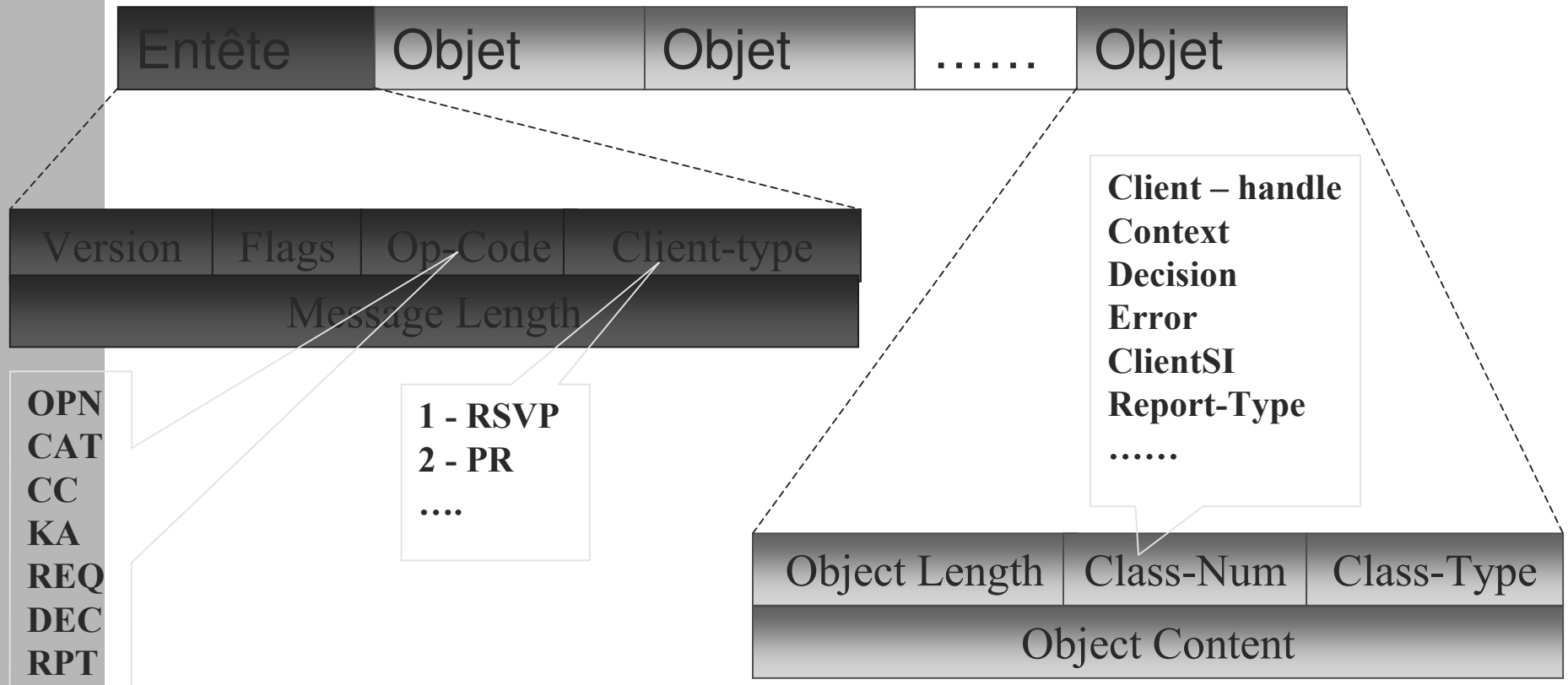
COPS provisionning

COPS-PR for Diffserv,

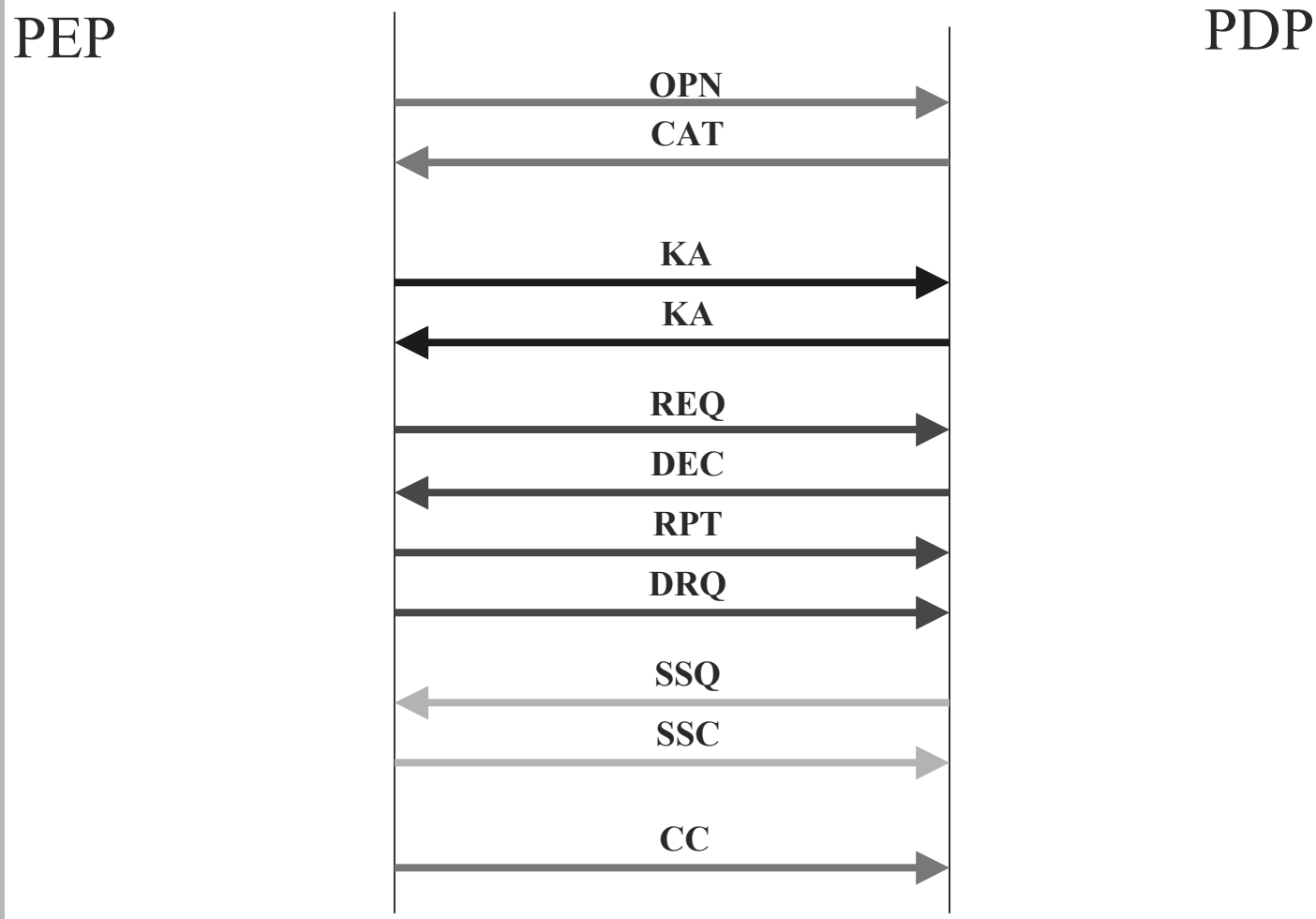
COPS-PR pour IPSec

- SLA
- COPS-PR
- PIB

Format of the message

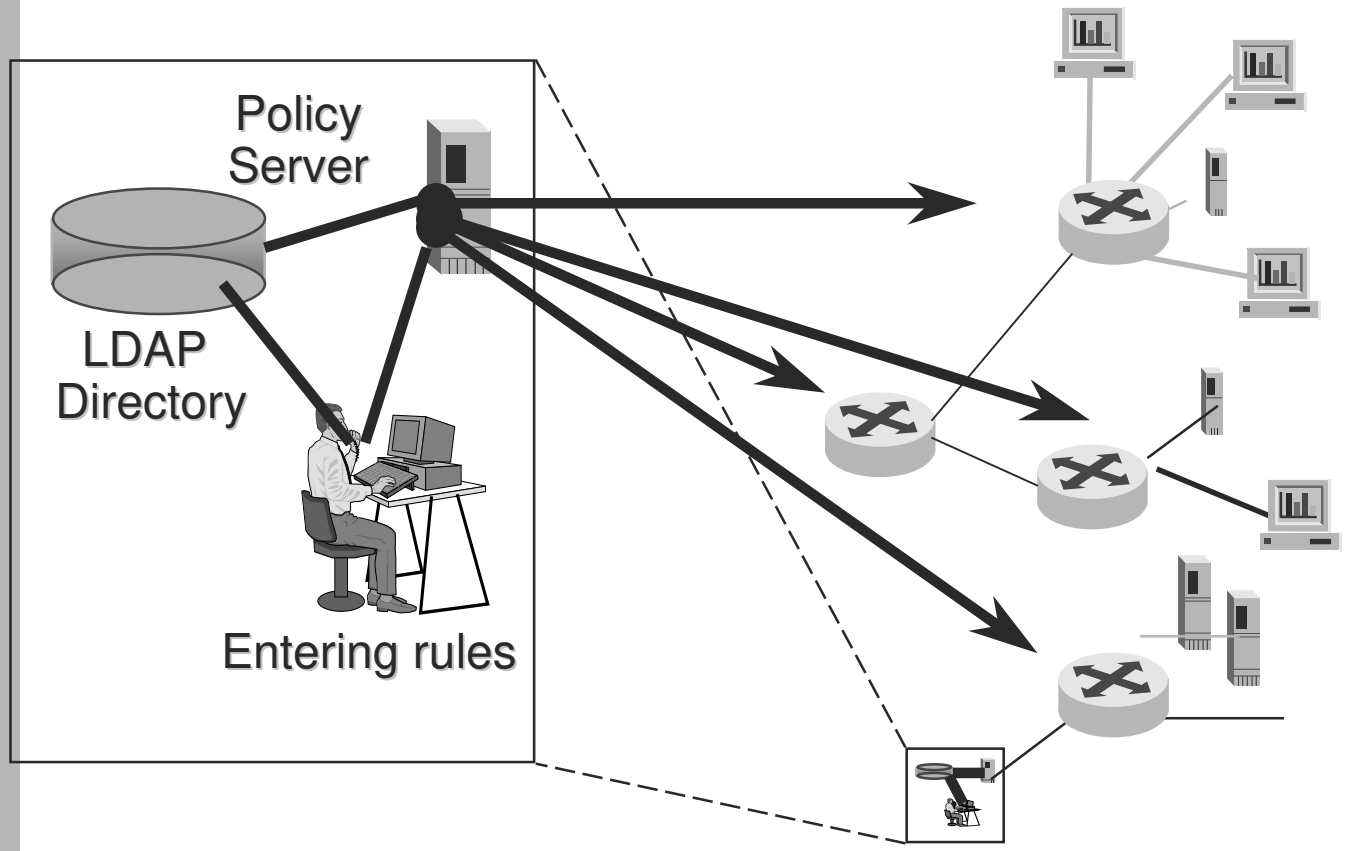


Message exchange

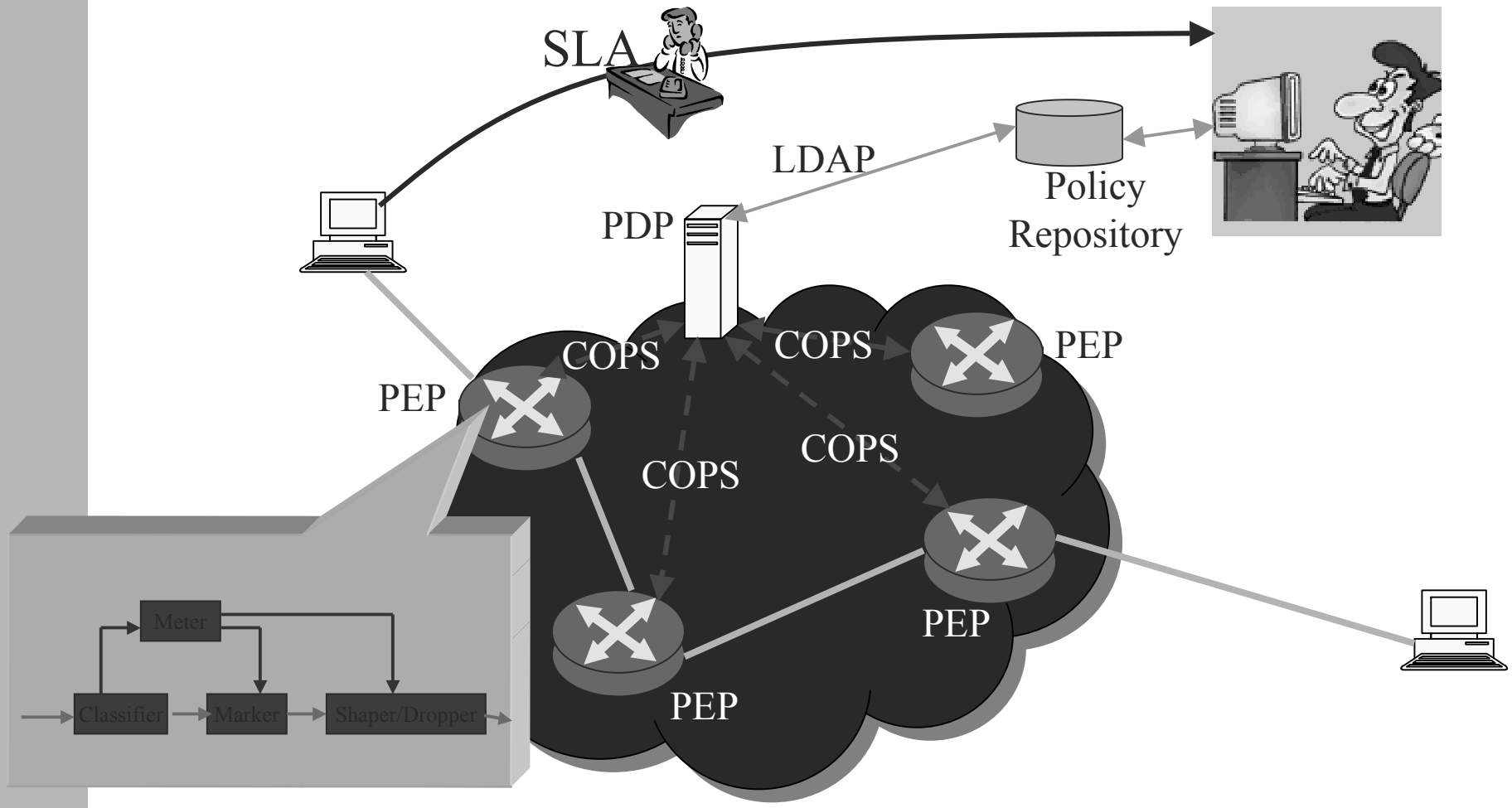


Policy : management and control

Intégration of Directory and Policy Server



COPS-PR and Diff-Serv

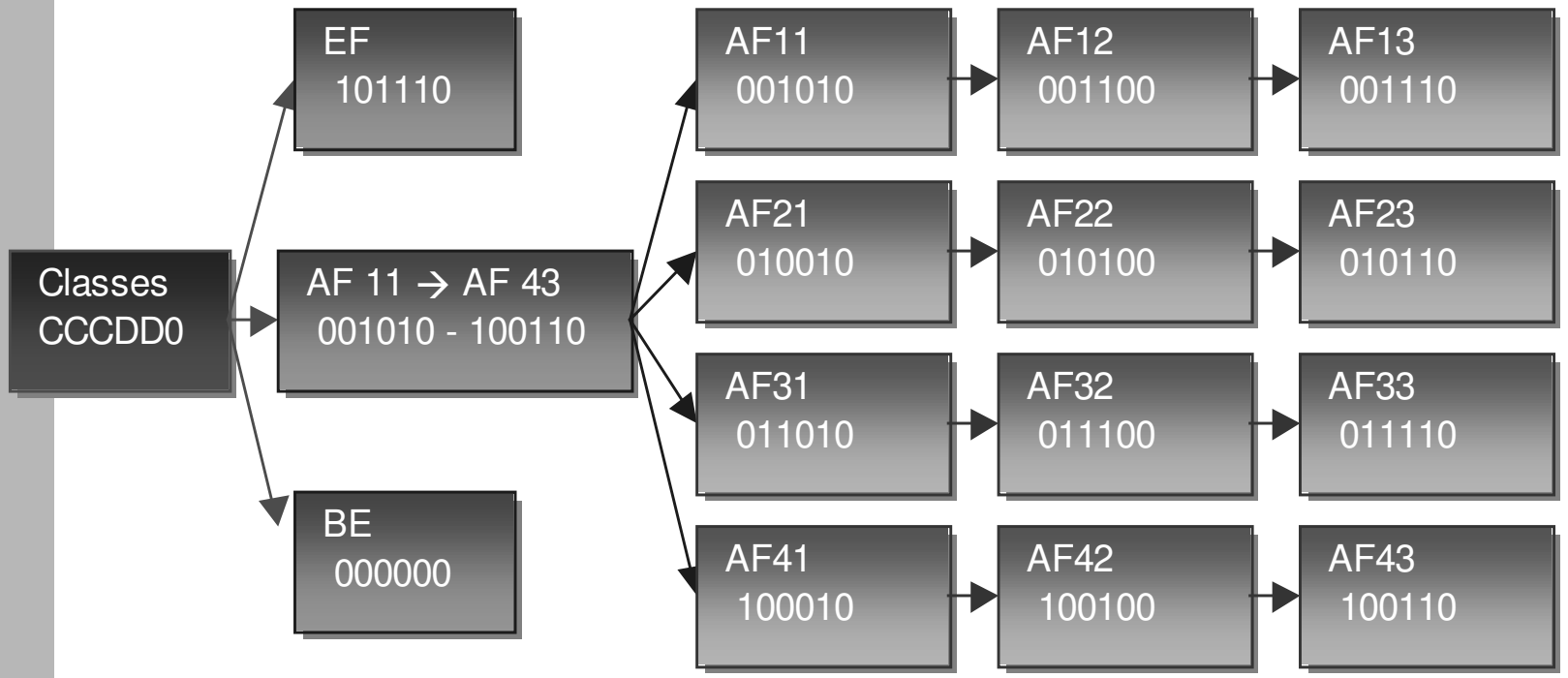


DiffServ

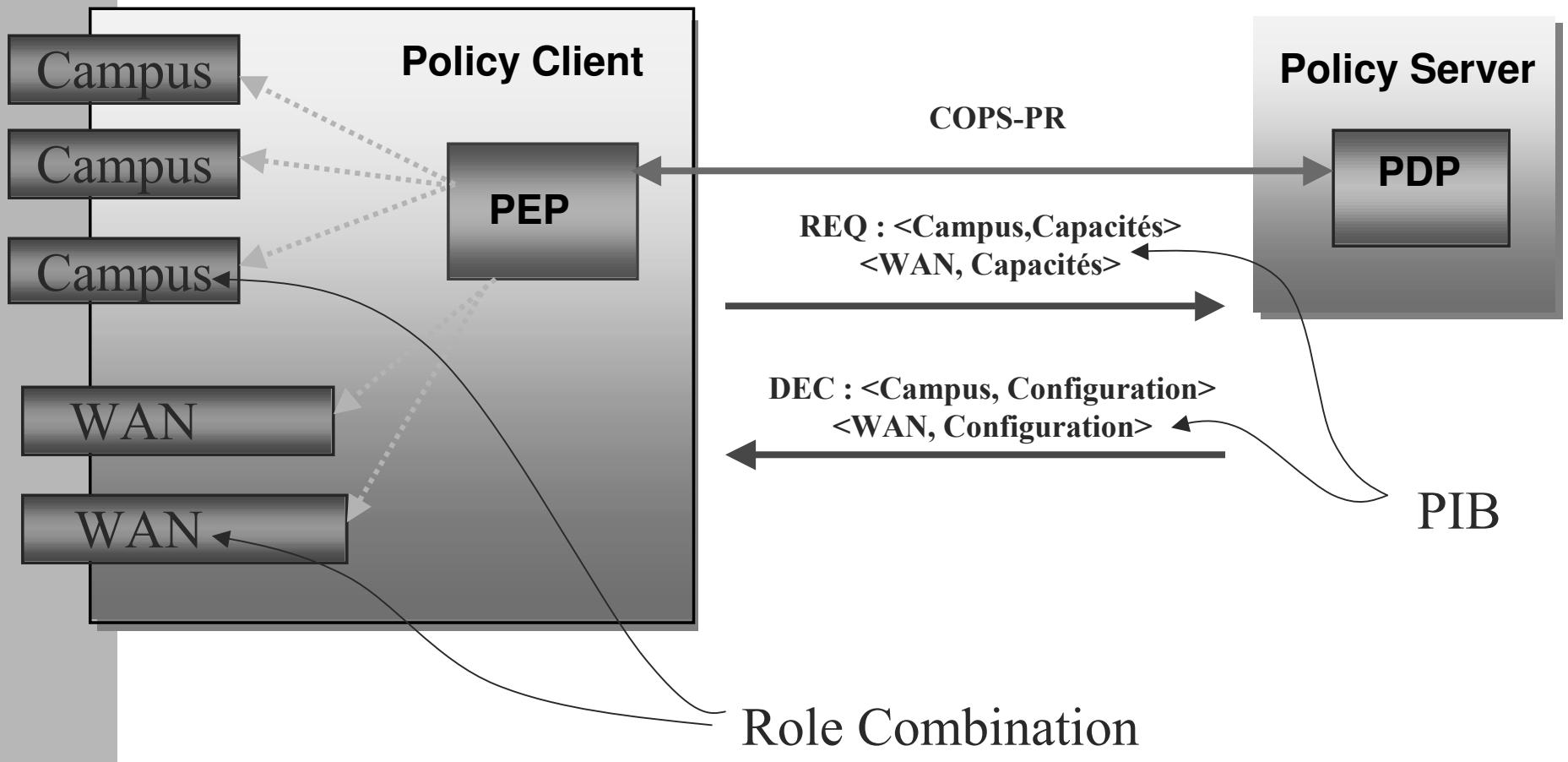
Differentiation of services using the DSCP (8 bits) of the TOS field (IPv4) / TC field (IPv6) of the IP packet.

Each DSCP corresponds to a PHB (Per Hop Behavior)

Diffserv Code Point



COPS-PR for Diffserv



Example

Negociated SLS :

DSCP	PHB	Profil	Treatment
001001	EF	Profil1	Reject non-conform packet
001100	AF11	Profil2	Shape on Profil 2, tail-drop when the buffers are full
001101	AF21	Profil3	DSCP 00100, tail-drop when the buffers are full
Others	BE	No	Red-like droping

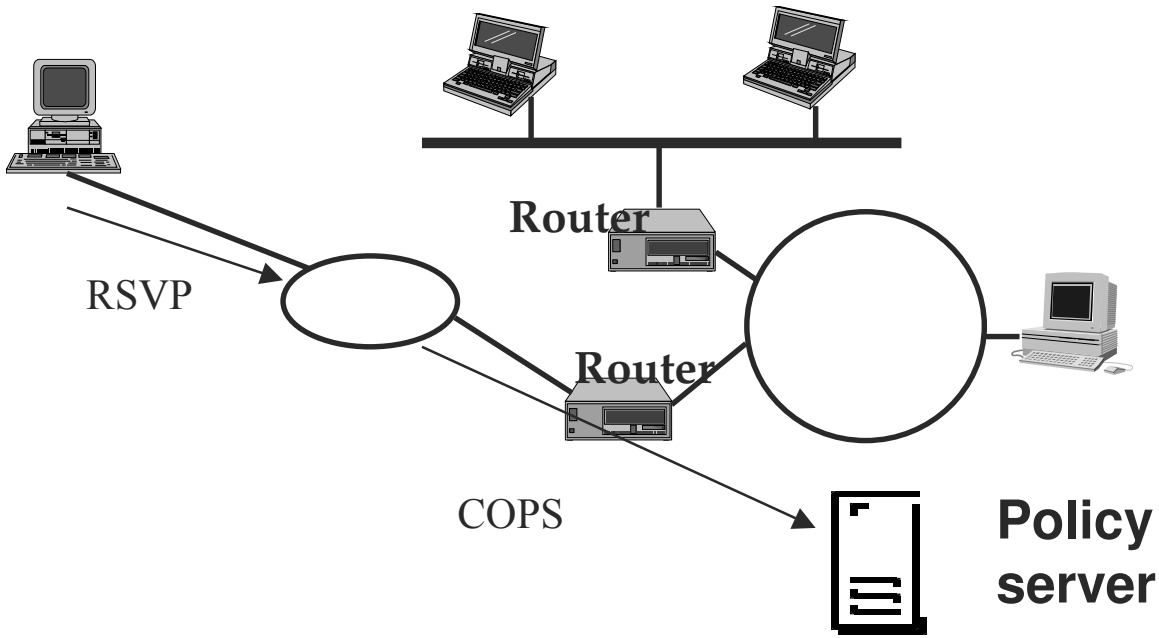
Trafic profil

Profil1	Type : SimpleTokenBucket Rate : 100 Kbps BurstSize : 20 kbytes
Profil2	Type : SimpleTokenBucket Rate : 100 Kbps BurstSize : 100 kbytes
Profil3	Type : SimpleTokenBucket Rate : 200 Kbps BurstSize : 100 kbytes

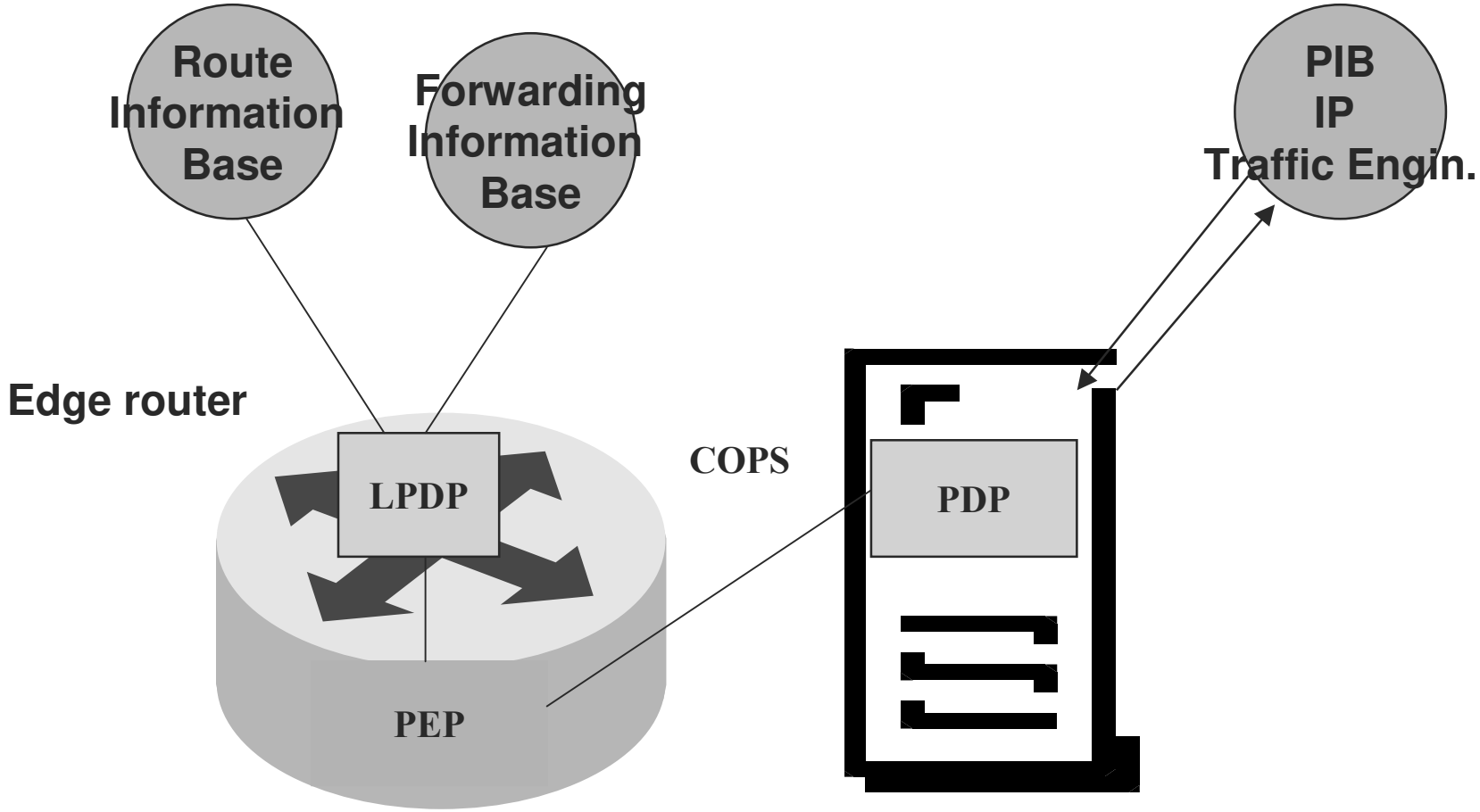
COPS-Outsourcing

COPS-Outsourcing is a proposal to have a dynamicity in the SLA (Service Level Agreement)

RSVP-COPS



COPS for IP traffic engineering



COPS-SLS

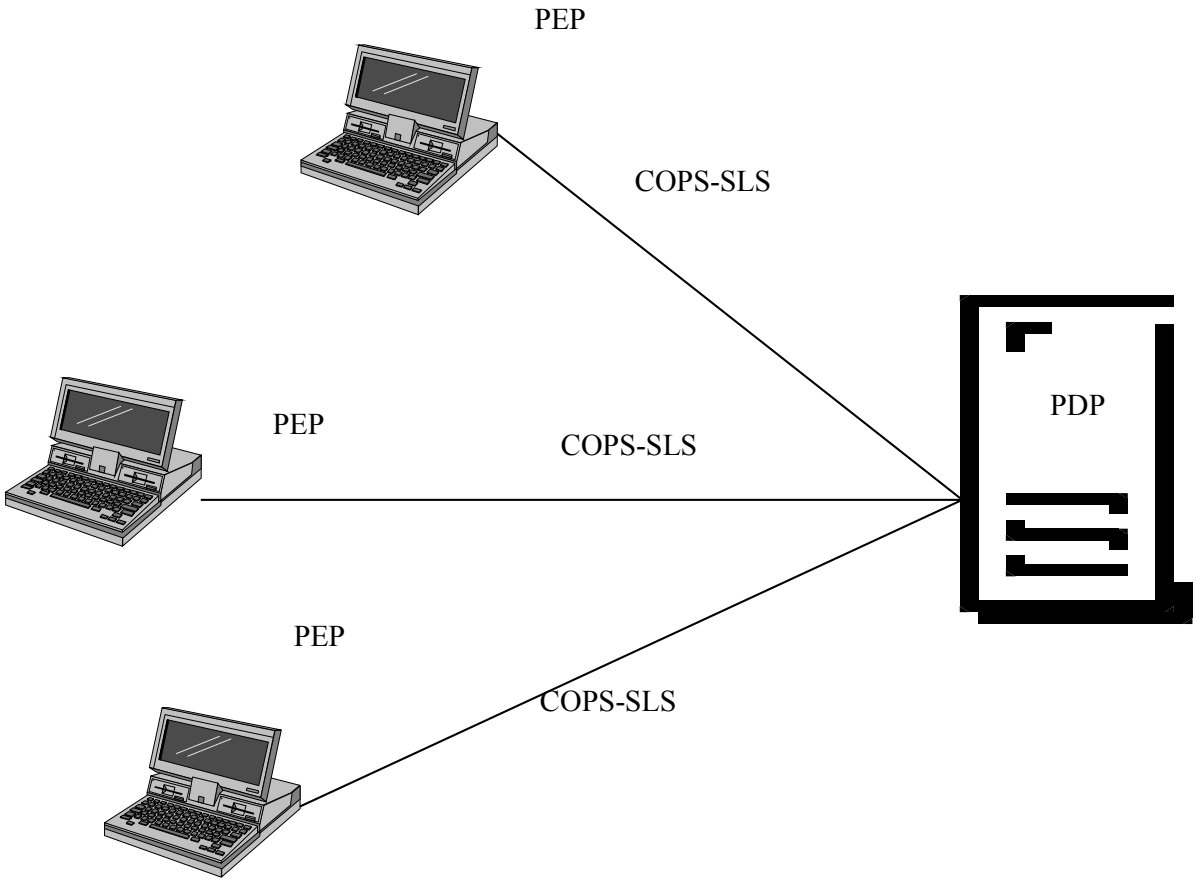
Goal : permit to have dynamic request from the usersand compatible with COPS

COPS : End-to-end

- policy client of COPS-SLA in the terminal equipment.
- policy server of COPS-SLA within the edge router

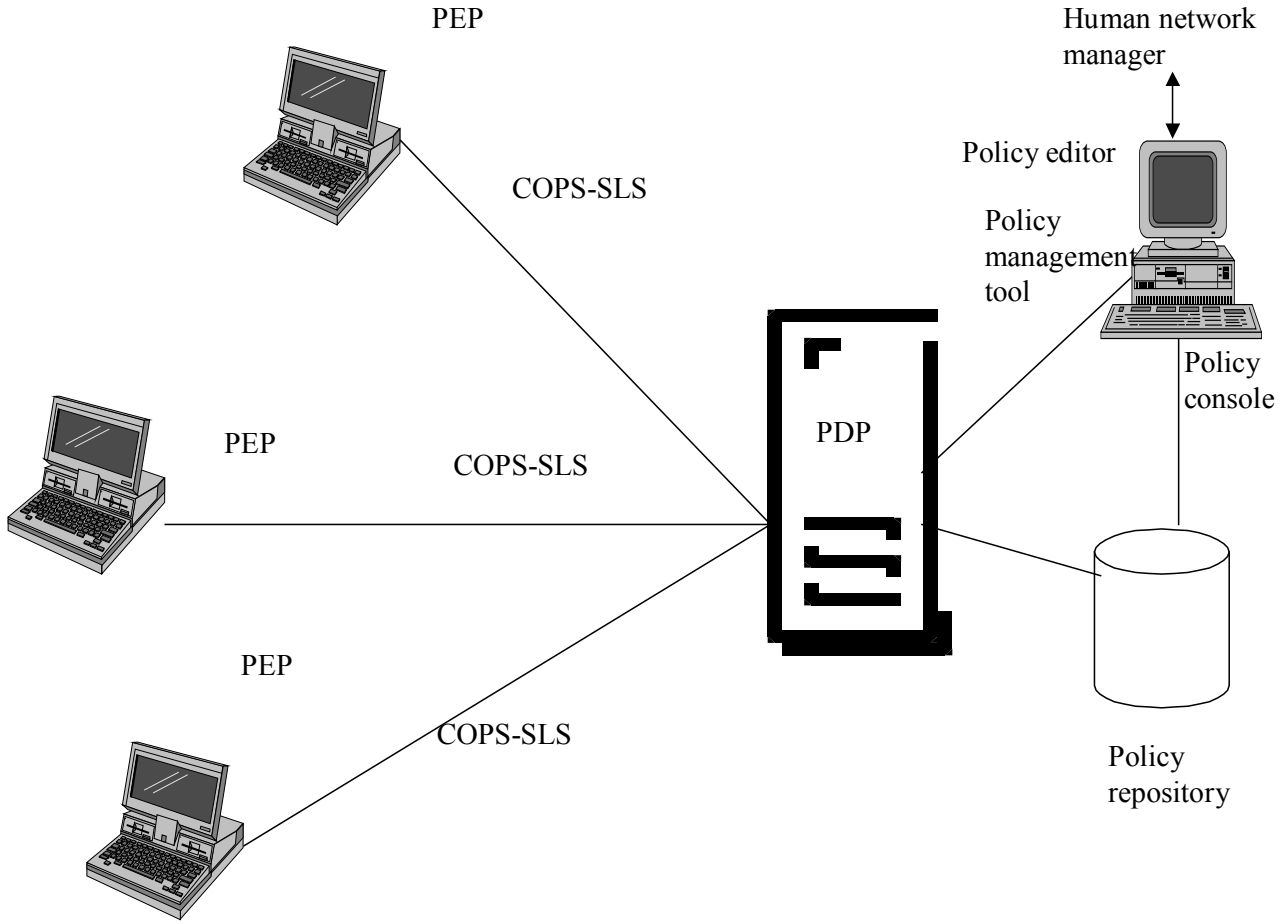
Proposal to IETF (London)

COPS-SLS

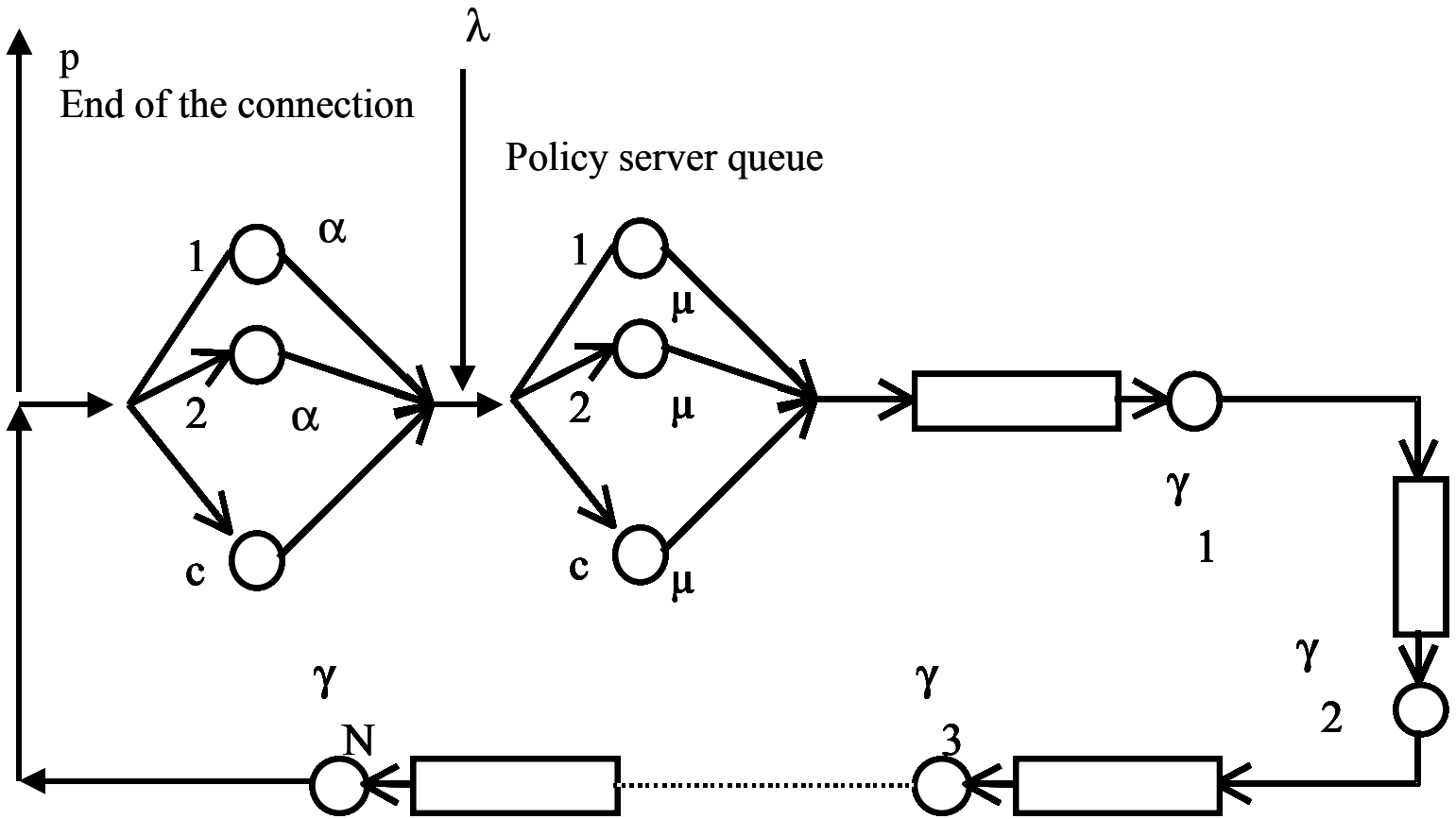


COPS-SLS

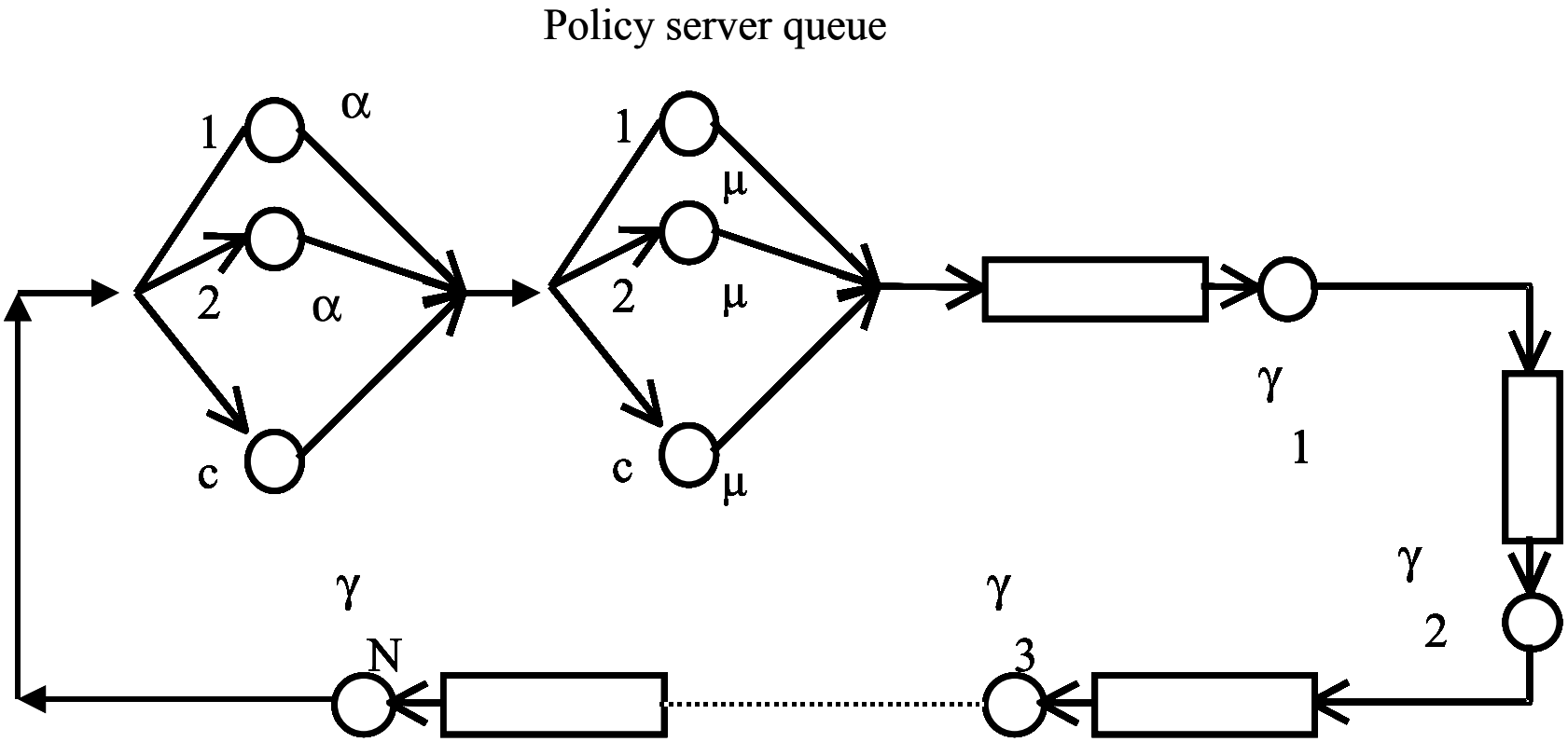
Classification



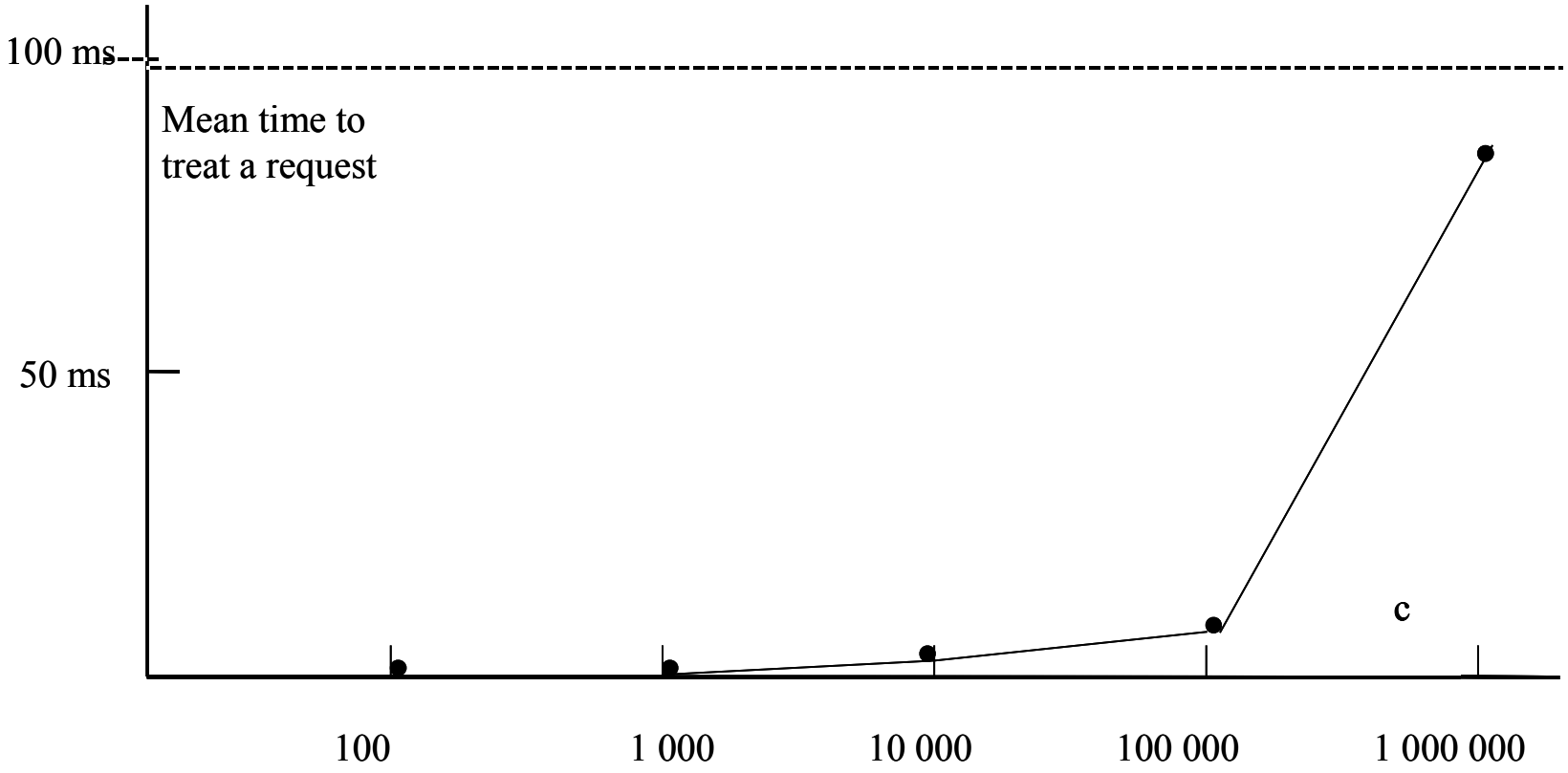
Performance evaluation



Performance evaluation



Performance evaluation



Questions ?