# Security Services on IPv6 Networks: PKIv6 and IPv6-VPNs

Antonio F. Gómez Skarmeta
<skarmeta@dif.um.es>

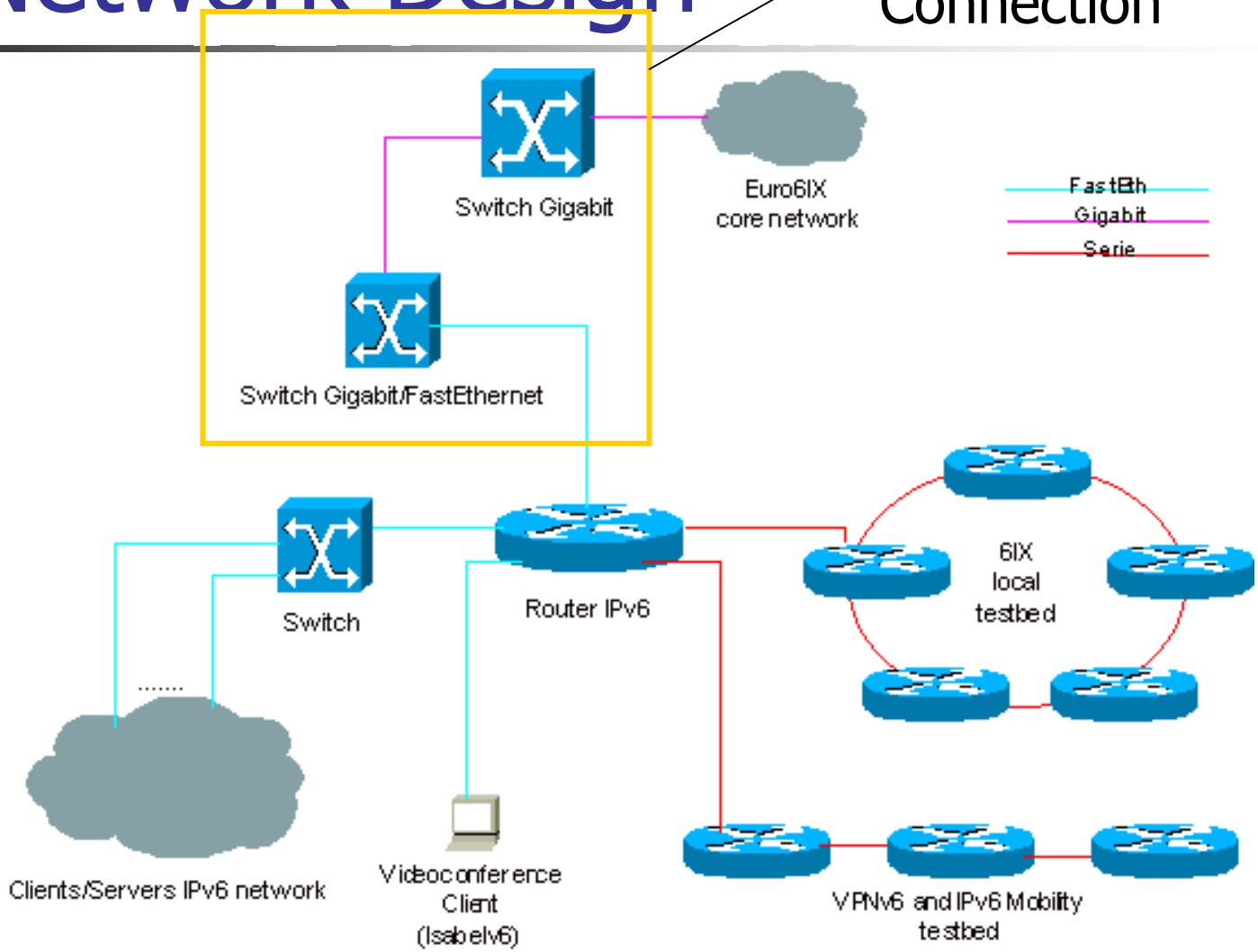
University of Murcia
SPAIN

# 1Year Subactivity Description

- Mobility on IPv6 networks
  - Going to be coordinated with 6Net
- Security on IPv6:
  - Static VPNs with IPv6 and PKIv6
  - Collaboration with 6Net via UCL test on VPNs
- Multihoming and Renumbering
- QoS over IPv6
- Mobility and VPNs using MPLS

UM-IPV6 2001:0720:1710::/48

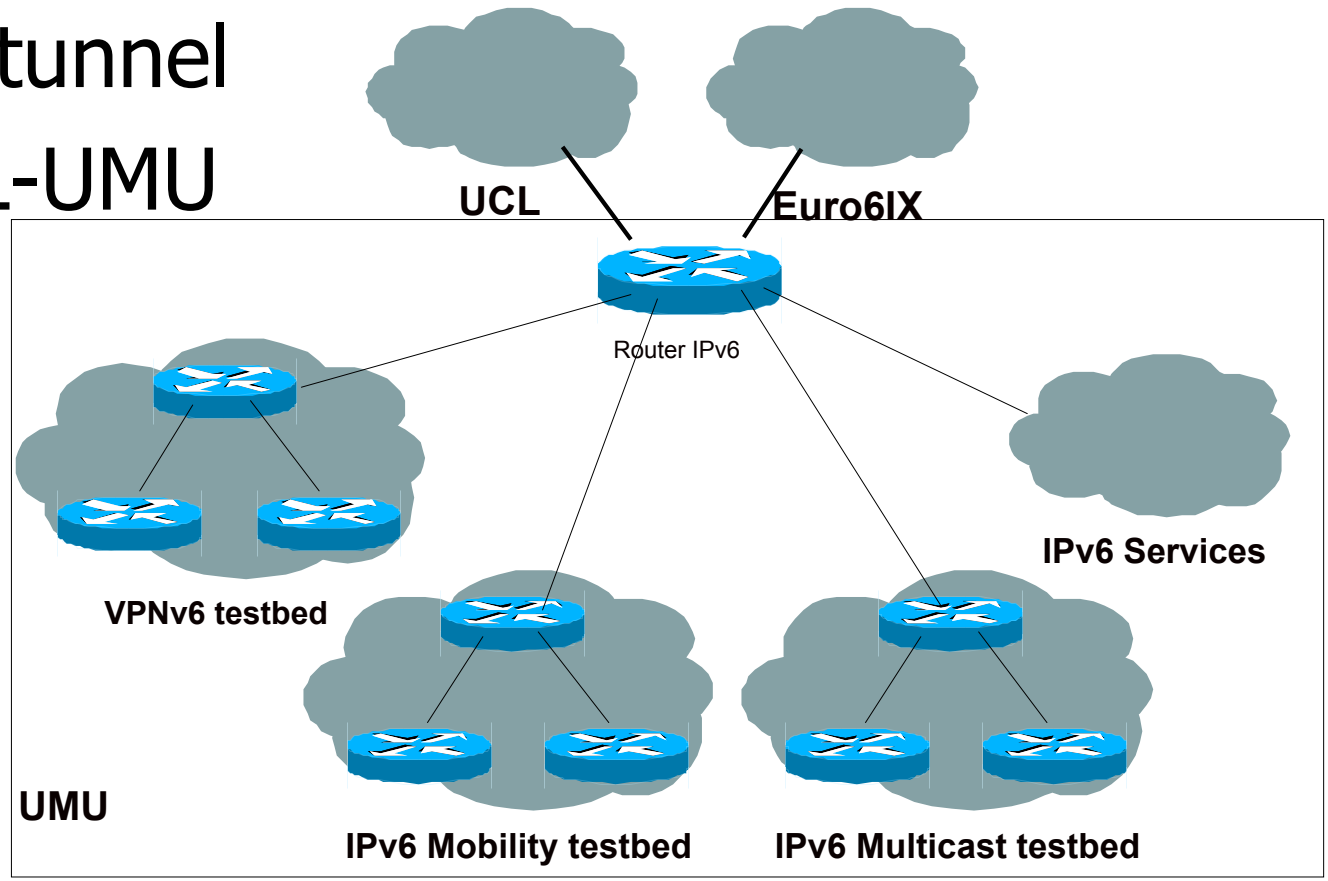
# Network Design



# IPv6 network design

- Native connection to Euro6IX
- IPv6 tunnel

  UCL-UMU



# The UMU-PKIv6 Service

Departamento de
Ingeniería de la Información
y las Comunicaciones

Euro6IX
IPv6:The New Internet

# UMU-PKIv6 Description

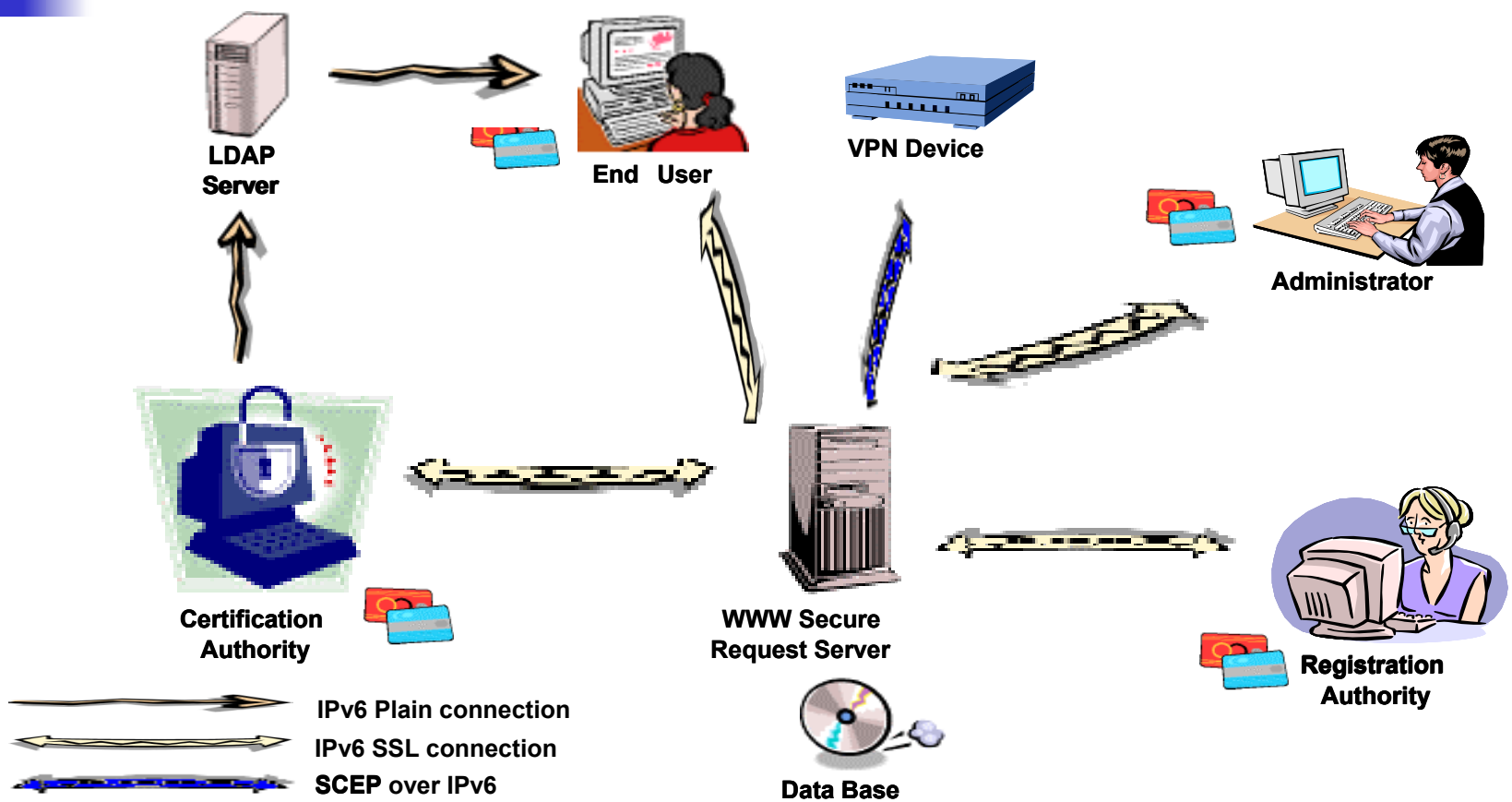
- Main Objective ... to establish a high security infrastructure for distributed systems
- Main Features:
  - PKI supporting the IPv6 protocol
  - Developed in Java ➔ multiplatform
  - Issue, renew and revoke certificates for every

    es for every entity (person or process)
    ng to one organization
    ither RAs or Web browsers to make their own

# UMU-PKIv6 Description (II)

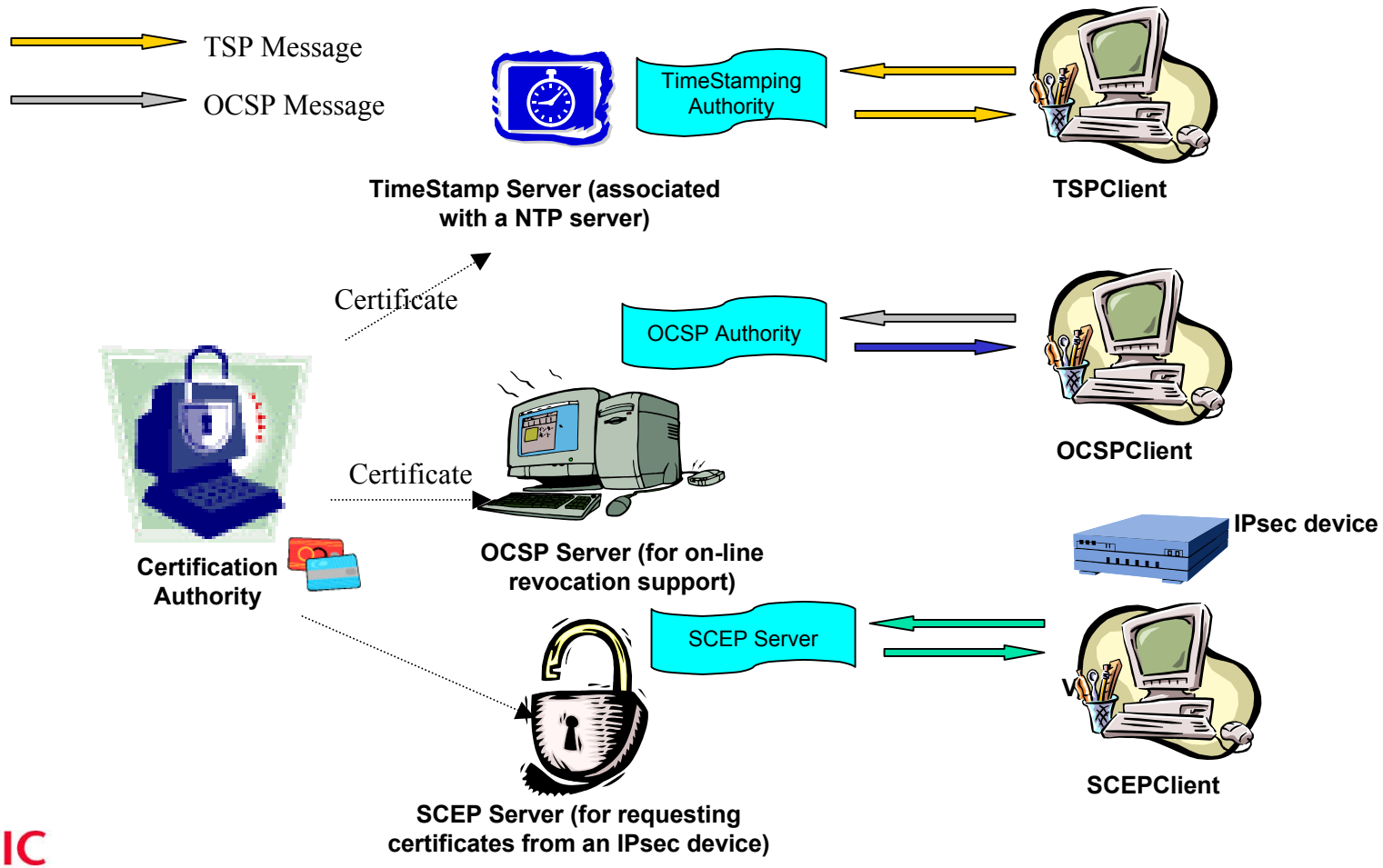
- Main Features: (II)
  - LDAPv6 directory support
  - Use of smart cards (file system, RSA or Java Cards) ... allowing user mobility and increasing security
  - PKI Certification Policy support
  - VPN devices certification support (using the SCEP protocol)
  - Support for the OCSP protocol and Time Stamp
  - Web administration
  - Used in both Euro6IX and 6NET projects (cross-certification)

# UMU-PKIv6 Architecture




https://pki.ipv6.um.es

# UMU-PKIv6 Advanced Services



# UMU-PKIv6 RA Snapshot

Introduction of certificate content information

Subject data

Common Name

User ID

Organisational Unit: CIRCuS

Organization: ANTS

Country: ES

Email

Contact Email

Contact Phone

Device Selector

Smart Card — Hard Disk

Private Key

Private Key Type: RSA

Private Key Length: 256

Password for Private Key

Private Key File...

Certificate Extensions

SSLClient ☑

SSLServer ☐

Secure Mail ☑

Accept — Cancel

Requesting a certificate

Pending Request Dialog

Search Request:

Min Value: 0 Max Value: 100

Pending Requests:

9

Request Data:

CN: web1010

UID: web1010

OU: CIRCuS

O: ANTS

C: ES

Email: gabilm@dif.um.es

Phone:

Contact Email: gabilm@dif.um.es

Extensions:

SSLClient ☑

SSLServer ☐

Secure Mail ☑

Validate — Delete

Close

Validating a certificate

# UMU-PKIv6 CA Snapshot

Configuration Enviroment

Certificates | LDAP | Data Base | Notification | CRL

LDAP Active ☑

LDAP password ********

LDAP url

LDAP root

Configuration Enviroment

Certificates | LDAP | Data Base | Notification | CRL

CRL Active ☑

CRL every certificate ☑

CRL every time ☑

CRL time (minutes) 60

CRL Distribution Point Ext. ☐

URL pirania.dif.um.es

Update CRL

Close

# UMU-PKIv6 Final User Operation Snapshot

Mozilla: The UCL-CS implementation of the UMU's PKI

Archivo Modificar Ver Ir Communicator Ayuda

Anterior Siguiente Recargar Inicio Buscar Mozilla Imprimir Seguridad Compras Parar

Marcadores Dirección: http://cornetto.cs.ucl.ac.uk/piscis/ Sitios parecidos

www.wordreference....late_to_Spanish.js www.wordreference....nish_to_English.js Red

PISCIS

Main Page
New User
Search for a Certificate
Revocation
Renewal Request
Certification Authority and CRL

Request a new Personal Certificate

This form will help you to fill in all information needed to request a new digital certific
this browser to perform certification operations. But, if you are using a smart card, you will

**Request Data**

Please, fill in the form with the right information. Do not use accented letters.

Full Name:
E-Mail Address:
Organizative Unit:
Organization: University College London
Country: UK

**Contact Information**

Please, enter your e-mail address or phone contact.

E-Mail Address:
Phone:

**Certificate Extensions**

SSL Client SSL Server S/MIME

100%

Mozilla: The UCL-CS implementation of the UMU's PKI

Archivo Modificar Ver Ir Communicator Ayuda

Anterior Siguiente Recargar Inicio Buscar Mozilla Imprimir Seguridad Compras Parar

Marcadores Dirección: http://cornetto.cs.ucl.ac.uk/piscis/ Sitios parecidos

www.wordreference....late_to_Spanish.js www.wordreference....nish_to_English.js Red Hat Network Training Support Software Hardware Develope

PISCIS

Revocation Menu
Revocation Request
Self-Revocation
Main Menu

Self-Revocation

This page allows you to register for self-revocation and later on, when needed (e.g. private key compromised) proceed to self-revoke your certificate. The self-revocation process is divided into two phases:

Phase 1. You must register with the self-revocation process. Your certificate must be valid (not revoked and private key not compromised) to proceed. This phase will require a login name and password that you will use in phase 2 when you need to self-revoke your certificate.

Phase 2. In this phase you can actually revoke your certificate whenever you need to (e.g. private key compromised) by using the login name and password information from Phase 1.

| | | |
|---|---|---|
| Phase 1. Register for Self-Revocation | Click for Phase 1 | Help |
| Phase 2. Self-Revoke your certificate | Click for Phase 2 | Help |

100%

DIIC Departamento de Ingeniería de la Información y las Comunicaciones

Euro6IX IPv6:The New Internet

# PKIv6

- PKIv6 running in both sites, UCL and UMU.
  - UMU:
    - IPv6-only: https://pki.ipv6.um.es
    - IPv4: https://pki.dif.um.es
  - UCL (test site, not production PKI):
    - IPv6-only: https://persephone.ip6.cs.ucl.ac.uk
    - IPv4: https://persephone.cs.ucl.ac.uk
- Interoperability tests between both of them.
  - certification, revocation and renewal request, etc.

# Test suite (Current Work)

- ISABELv6,
- AGWSv6, and
- The UCL-CS Secure Conference Store

For a **Joint Euro6IX-6NET Demo**

- Others (with IPv6 Support)

# Static VPNs with IPv6

Departamento de
Ingeniería de la Información
y las Comunicaciones

Euro6IX
IPv6:The New Internet

# Main objectives of this Service

- Evaluation of currently available open-source and some commercial IPv6 IPsec/IKE solutions
- Design and deployment of a static IPv6 VPN service according to the Euro6IX testbed or related-applications requirements
- Establish **Joint IPv6 VPN(s)** between some (interested) Euro6IX and 6NET partners

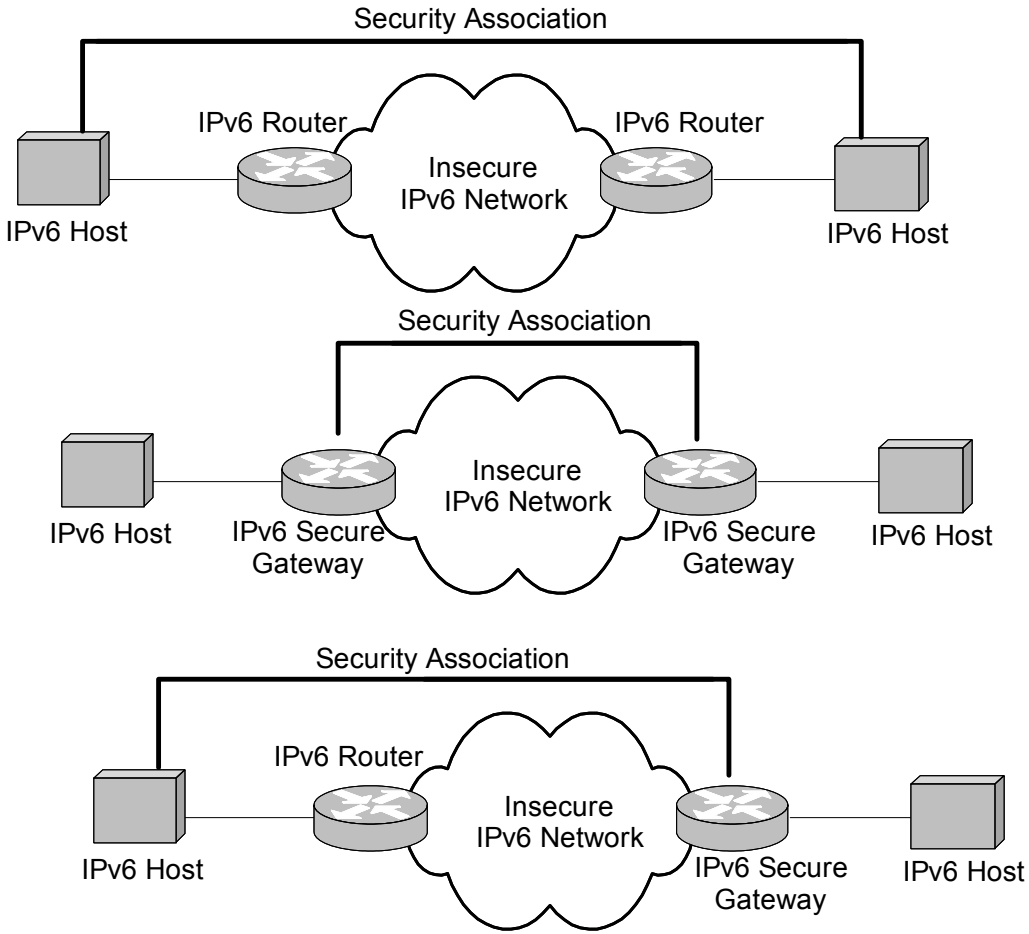
# IPsec/IKE solutions being currently analyzed

- One-year activity in Euro6IX (until Dec. 2002)
- Open-Source Solutions
  - FreeS/WAN IPv6 (Linux)
  - USAGI Project (Linux)
  - KAME Project (FreeBSD)
- Commercial Solutions
  - Microsoft IPv6 (Windows XP)
  - Solaris 9
  - 6WIND
  - Others with IPv6 support

# Designed evaluation plan

- Background: TAHI Project
  - http://www.tahi.org
- Interoperability tests
  - Test scenarios
  - Test suite
  - Final reports
    - Configuration and installations guides
    - Test reports

# Basic IPsec scenarios



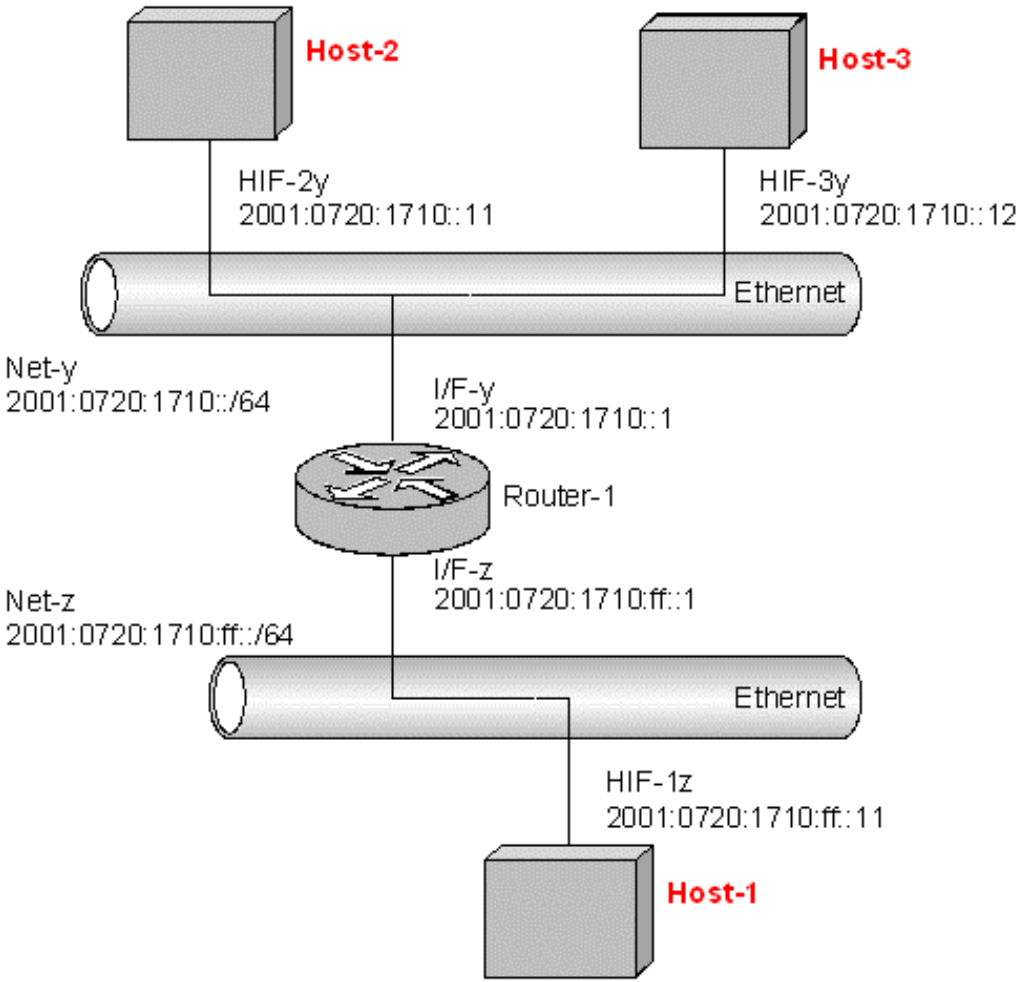
# Defined Test Scenarios

| No. | Category | Target |
|---|---|---|
| (1) | Transport mode AH | Host |
| (1) | Transport mode ESP | |
| (3) | Transport mode AH & ESP | |
| (4) | Tunnel mode AH | |
| (5) | Tunnel mode ESP | |
| (6) | Transport mode AH & tunnel mode ESP | |
| (7) | Transport mode & tunnel mode | |
| (8) | Tunnel mode AH | Router |
| (9) | Tunnel mode ESP | |
| (10) | IPSec Tunnel mode with HOST | |
| (11) | IPsec Tunnel to IPsec Tunnel mode | |
| (12) | IPsec Tunnel to IPsec Tunnel mode with HOST | |
| (13) | AH Transport to ESP Tunnel mode | |

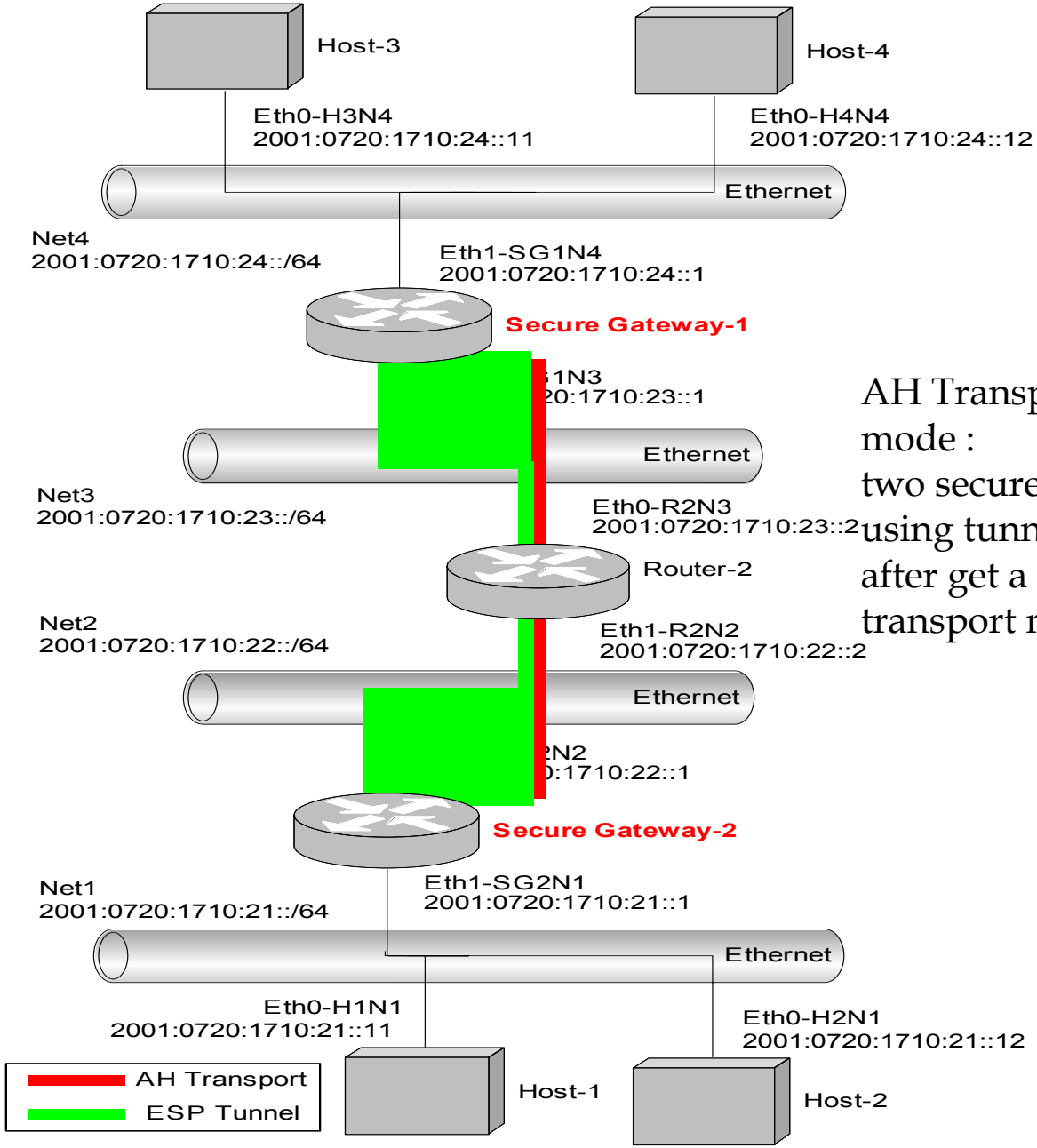
AH: Authentication Header

ESP: Encapsulating Security Payload

# Example of test scenario: Transport mode AH (Host)



# Other example




AH Transport to ESP Tunnel mode :
two secure gateways get a SA using tunnel mode ESP and after get a new SA using transport mode AH.

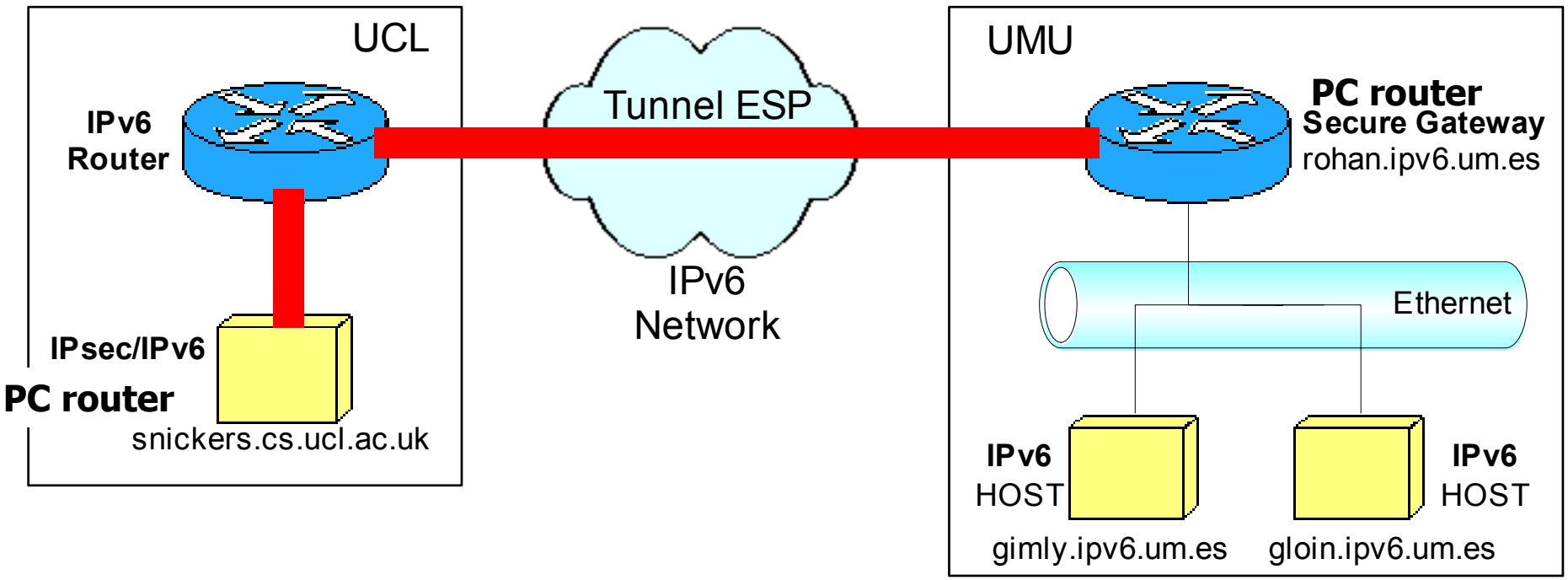
# Defined Test Suite

- Basic applications
  - Ping6 (ICMPv6)
  - Telnet6 (TCP)
  - Host6 (UDP)
- Another IPv6 applications within the project

# VPNv6

- Scenario UCL-UMU:
  - Tunnel ESP
  - IKE with certificates of PKIv6
- Implementation: KAME integrated in FreeBSD 4.5 release.
- CISCO 2600 actually just IPv4 waiting for releases

# VPNv6 - Scenario UCL-UMU

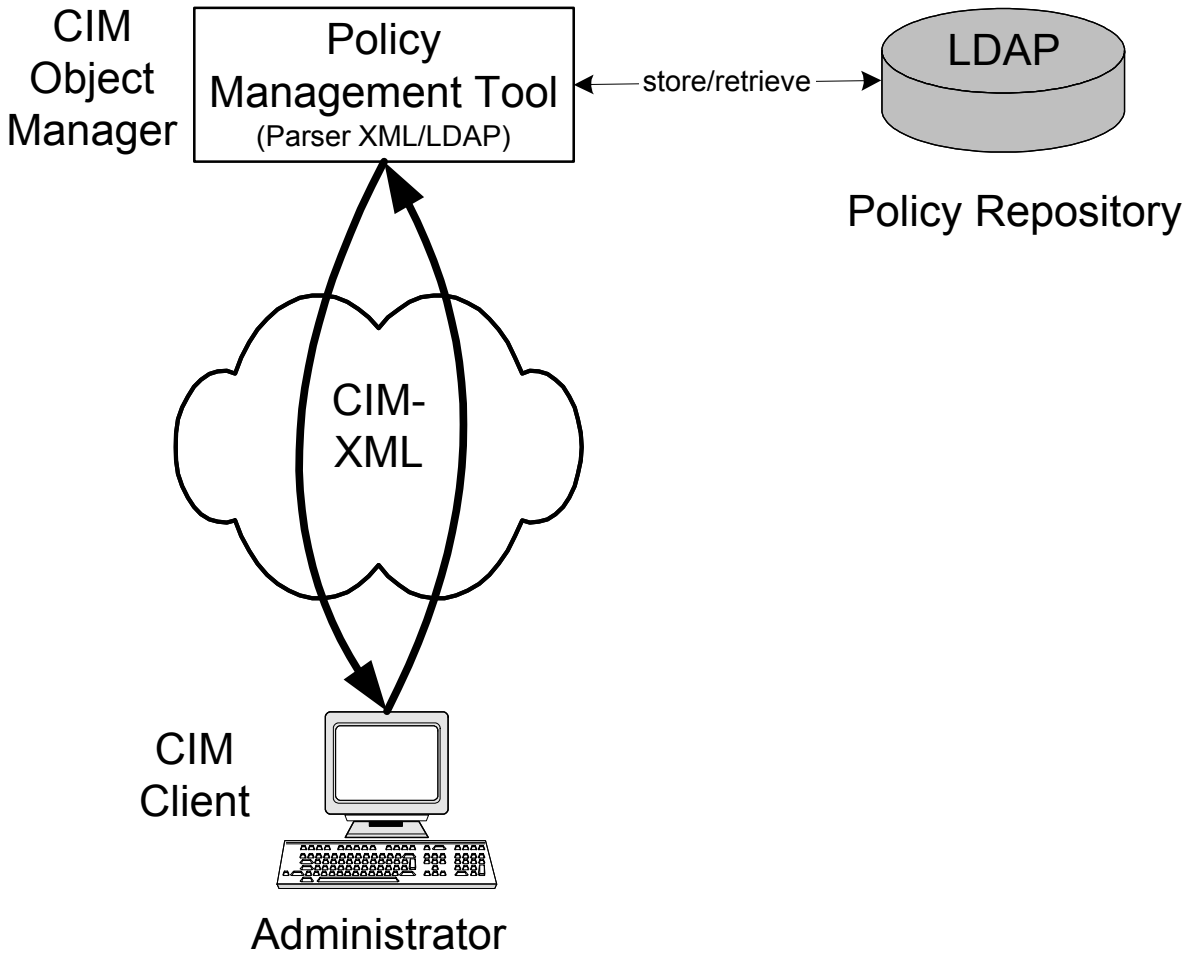


# Next/Current work

- Evaluation of the IPsec/IKE solutions
  - Running interoperability tests
  - Test Reports
- Design of a Dynamic VPN Service (based on the concept of Security Policy defined by the IETF/DMTF)
- Atribute certificate support for VPN and authorization procedures
- Definition of AAA scenarios to relate mobility testbed and PKIv6

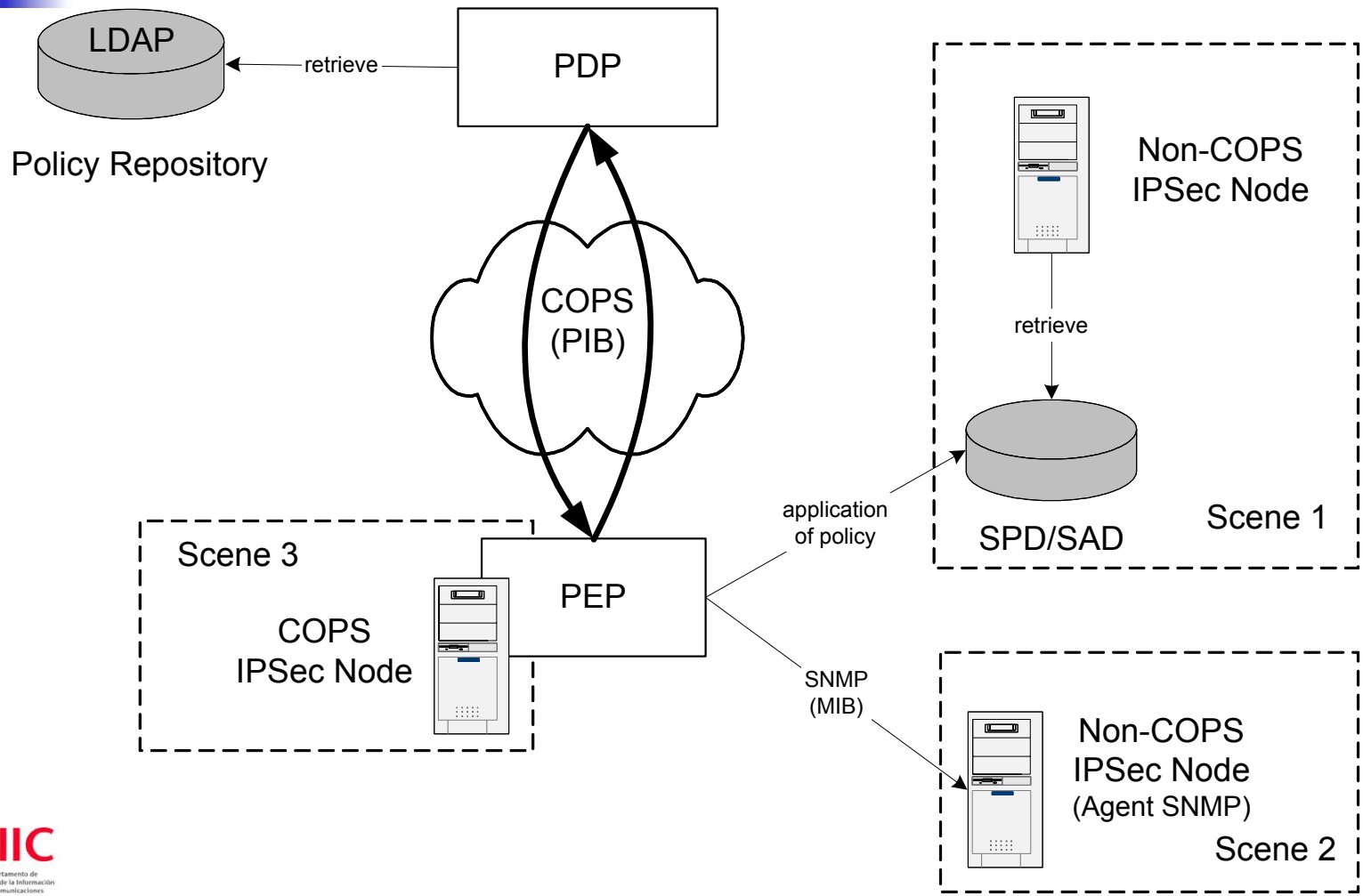
# Security Policies for VPNs (I)

## Policy Definition Process Schema



# Security Policies for VPNs (II)

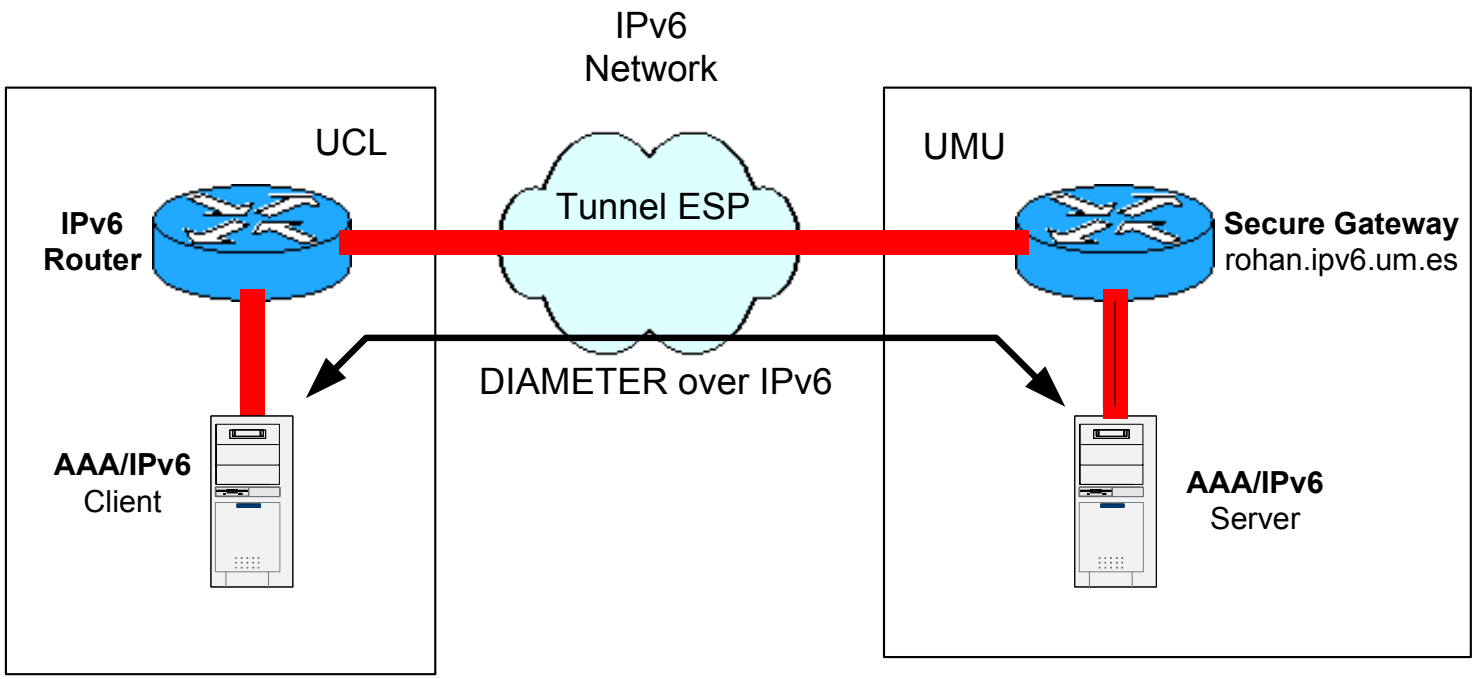
## Policy Recovery Process Schema



# AAAv6

- To define a chain of AAA servers managed by AAA protocol (DIAMETER) over IPv6 between both Universities
- To use established VPNs to secure communications between AAA servers
- Future MIPv6 and AAA tests

# Planned AAAv6 testbed



# Security Services on IPv6 Networks: PKIv6 and IPv6-VPNs

Antonio F. Gómez Skarmeta
<skarmeta@dif.um.es>

University of Murcia
SPAIN