

SECURITY IN BROADBAND ACCESS CONNECTION SHARING

MAPTELE WORKSHOP
2 DEZ 2009

CONCEIÇÃO TAVARES
cbt@ua.pt

ANDRÉ ZÚQUETE
andre.zuquete@ua.pt



Outline

Introduction to connection sharing

Survey and analysis of existing proposals

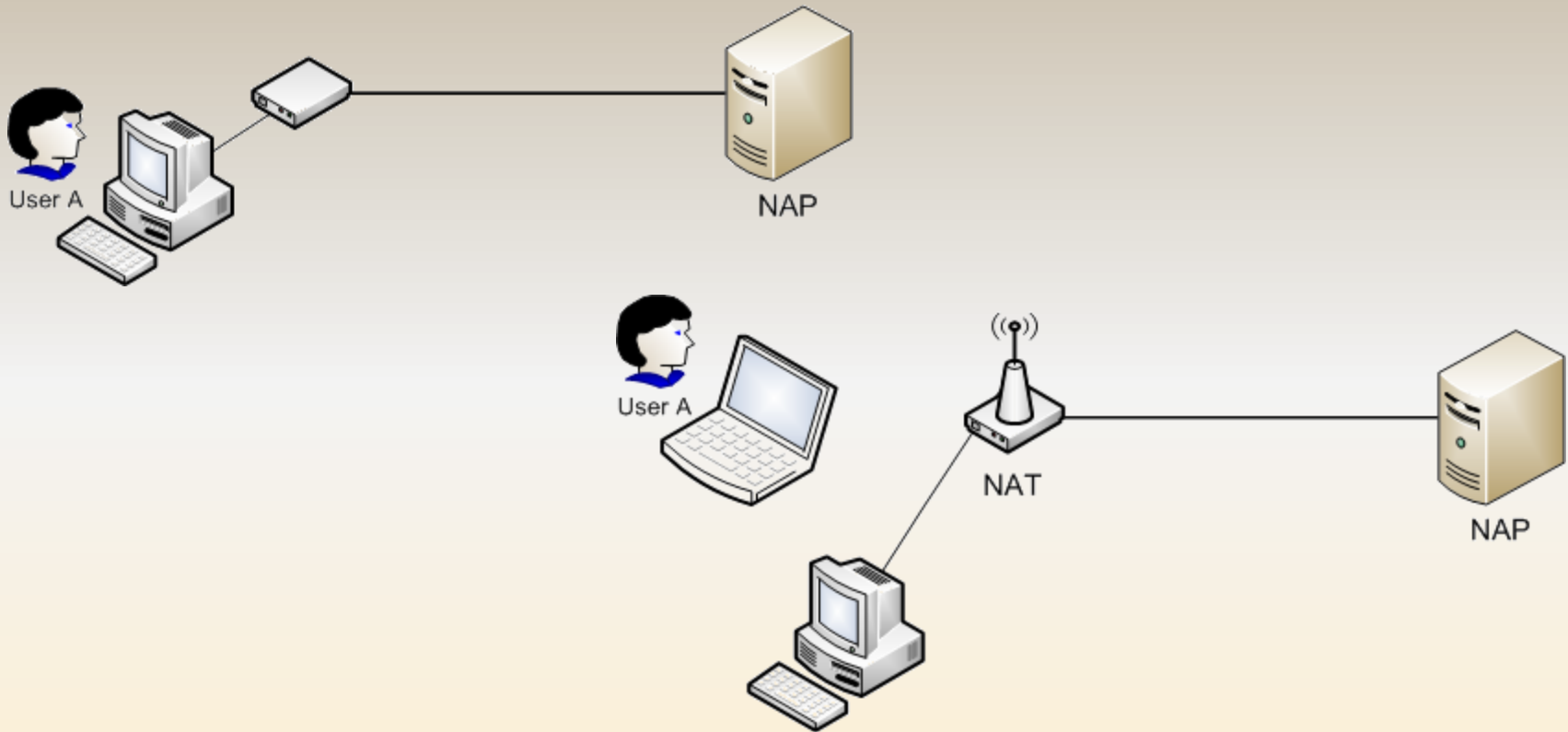
Research objectives

Conclusions

Internet access

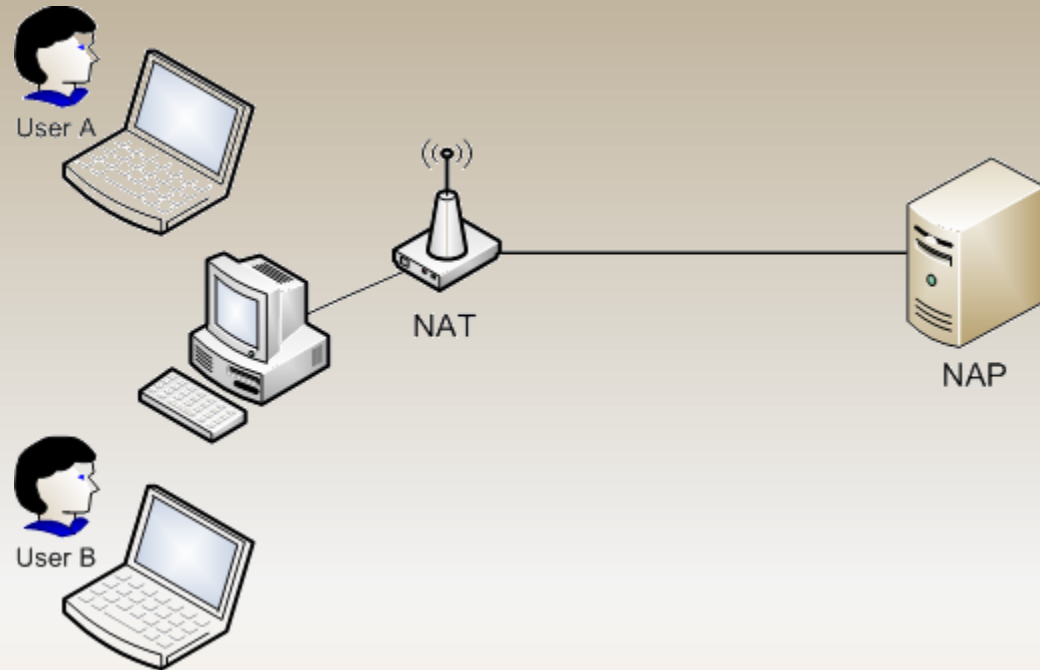
Traditionally:

One user per subscription



Internet access

Introduction to connection sharing



New paradigm

Several users per subscription

Examples: hotspots, wireless cities, etc.

Connection Sharing

Introduction to connection sharing

- This concept fosters the creation of an Internet access infrastructure based on already-existent subscriptions to Networks Access Providers (NAP) that may potentially bring benefits for all involved stakeholders.
 - NAPs
 - Fixed network subscribers
 - Roaming people
 - Service Providers

Connection Sharing

Introduction to connection sharing

The advantages:

- Coverage
- Equipement already deployed
- Sporadic users
- Profit for the subscription's owner

The disadvantages

- Legal compliant
- Security risks created either for access providers (the user that shares the connection) or visiting users.

Connection sharing risks

Introduction to connection sharing

- Confidentiality and integrity
- Traffic responsibility (non repudiation)
- Anonymity/Privacy

- ... and compliant with legal and other regulations (e.g. data retention)

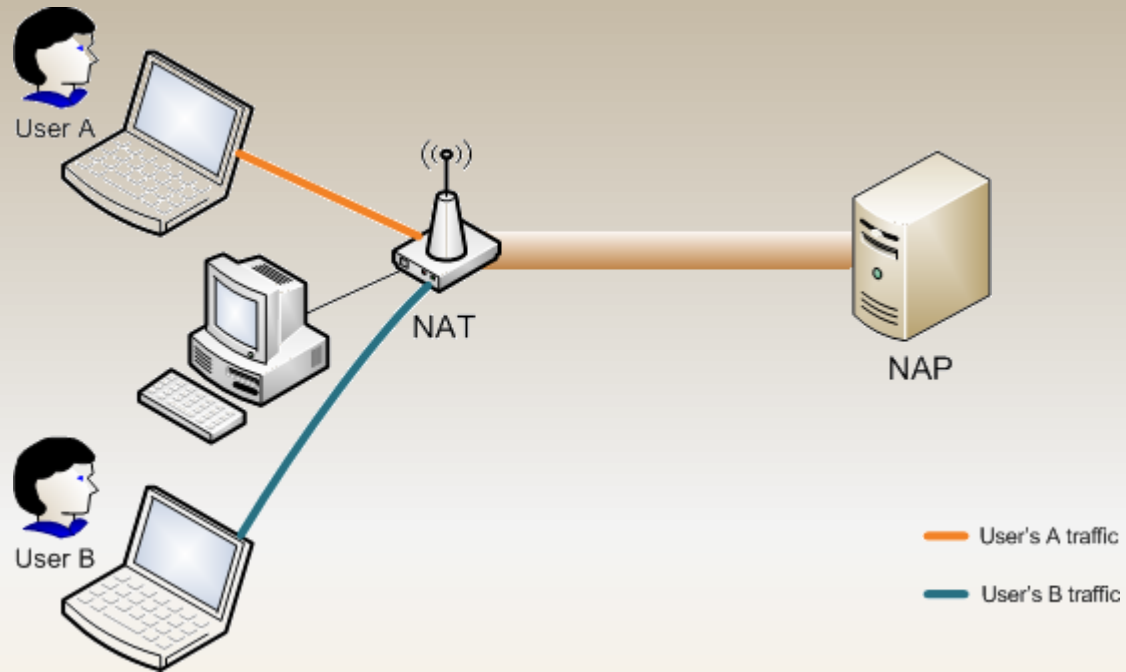
Connection sharing initiatives

- FON
 - VLANs
 - Authentication (Captive Portal)
 - La Fonera (APs)
- LinSpot
- OpenSpark
 - Authentication (RADIUS)
 - APs

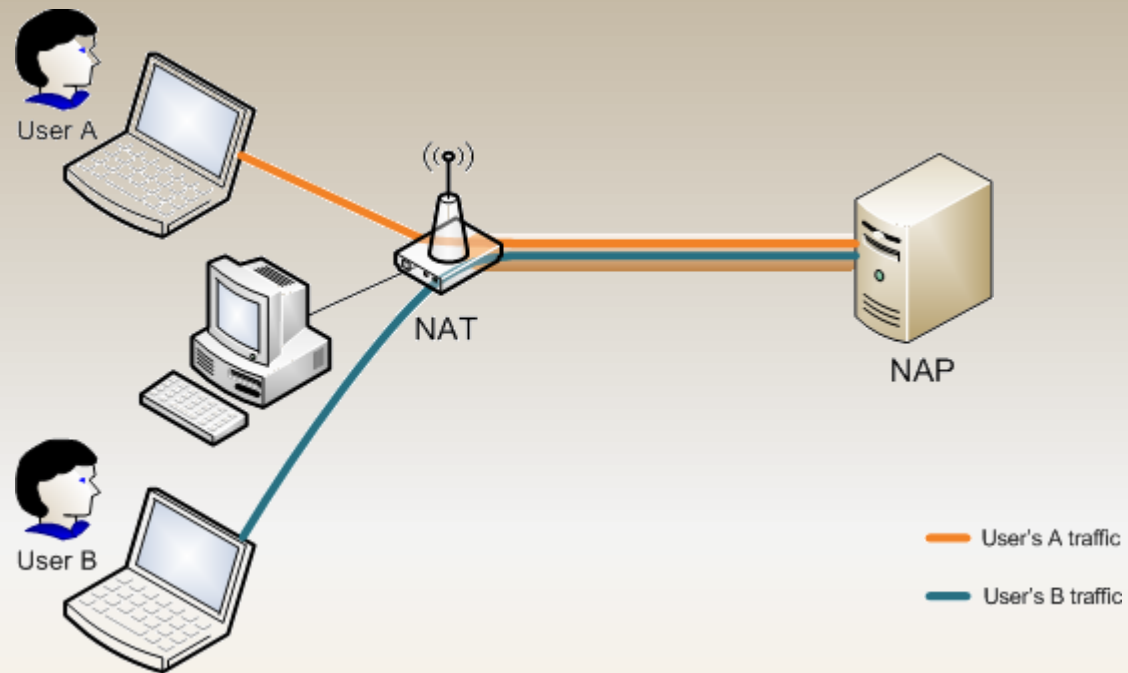
Existing proposals

- NetShare (operator)
 - No security
 - Only for Netshare customers
- Wifi.com
 - Access is of user provider responsibility
- Meraki
- PERM
 - Collaborative access

Traffic responsibility

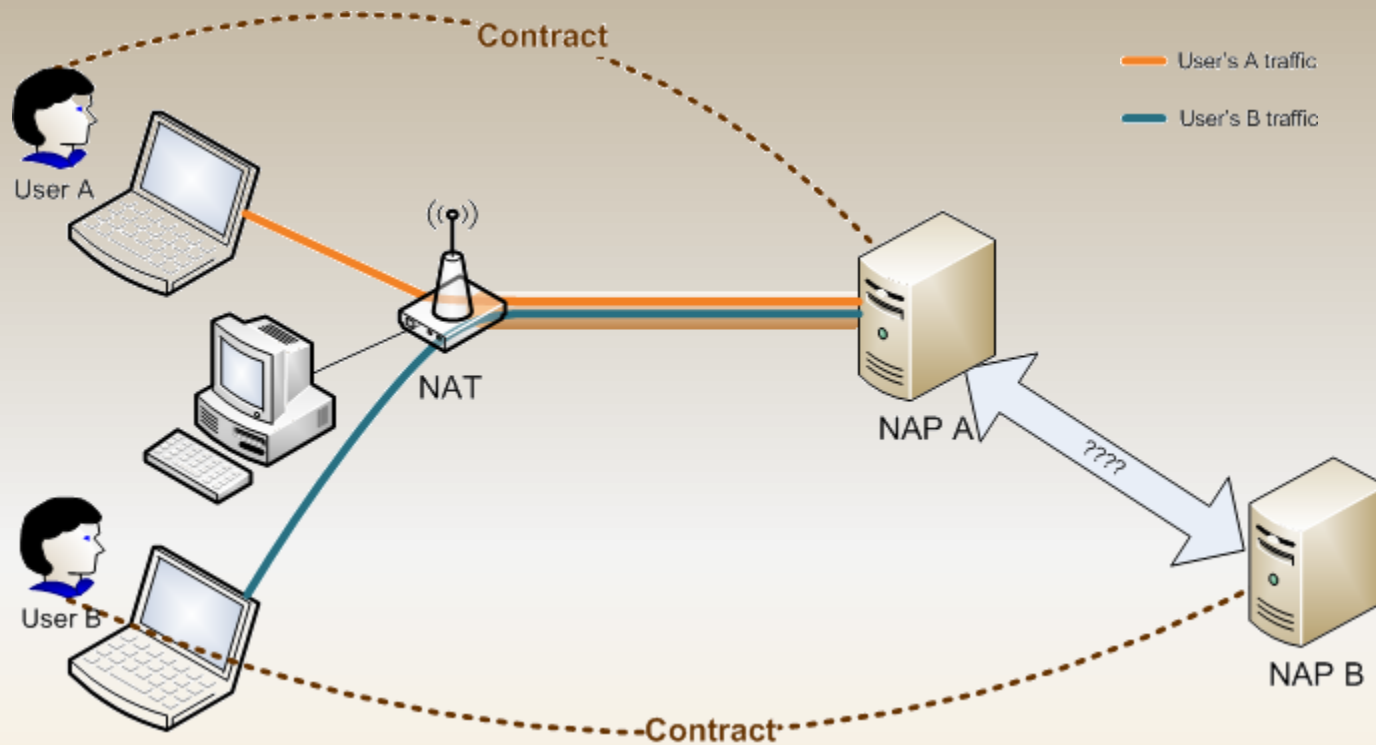


Traffic responsibility



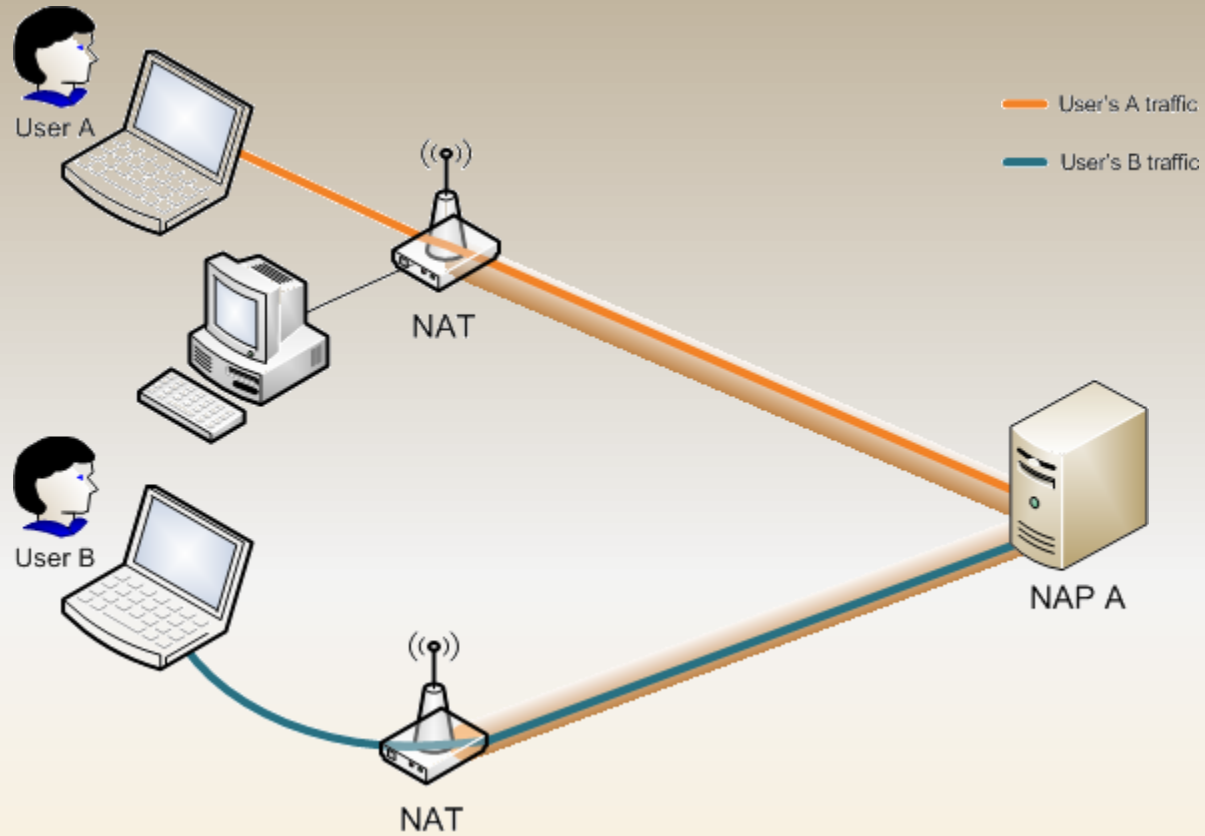
Use without NAP contract

Research objectives



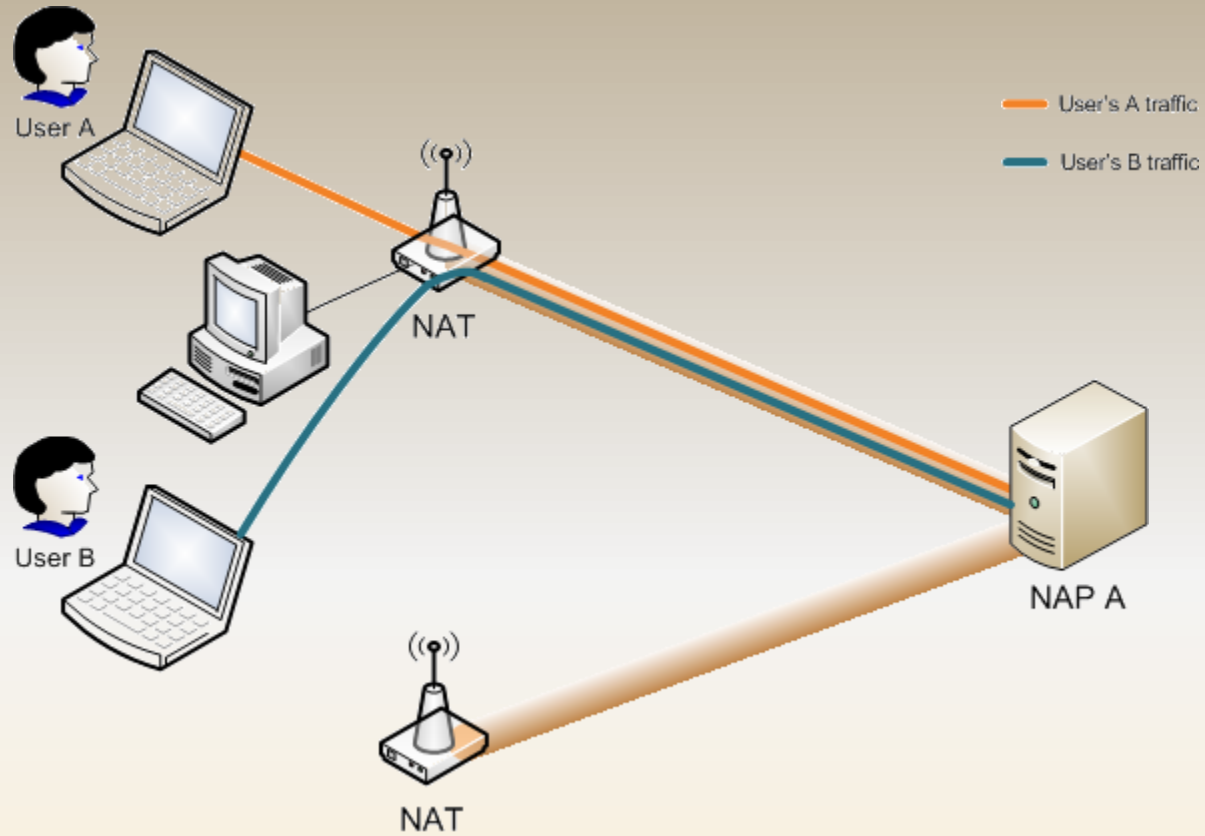
Mobility

Research objectives



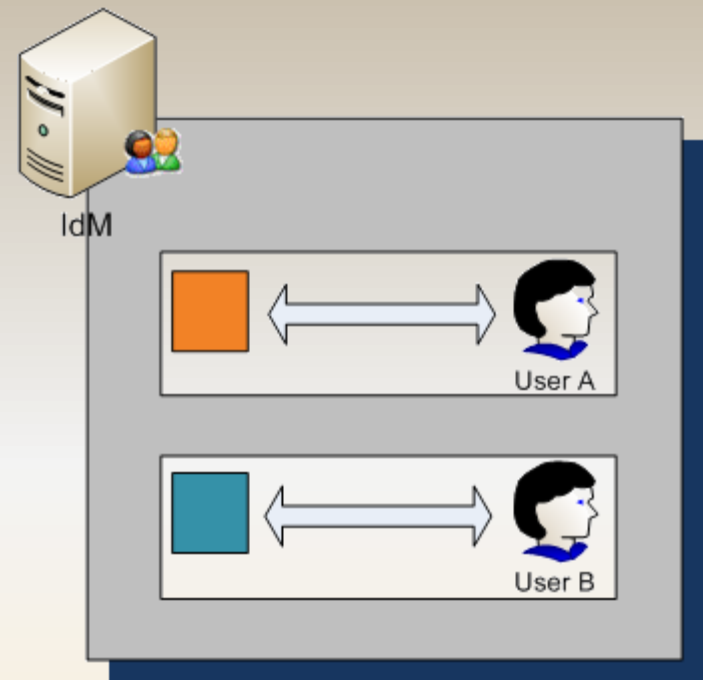
Mobility

Research objectives



Identity Manager

- It can identify the user responsible for the traffic.
- Although the traffic has a “signature”, only the IdM can identify the owner of that signature.
- The IdM can reveal the users’ identity if legally authorized or requested.



Challenges on Internet architecture

Conclusions

Problems widely reconized:

- Multihomming
- Mobility
- Interoperability IPv4/IPv6
- Protection against DoS (and other security issues)
- Convergence of IP-based solutions for telecommunications network
- Security

A complete and adequate solution that allows future evolution still missing.
Just patches that are not integrated with one another .

... to conclude

Conclusions

It is worthwhile to explore connection sharing

The actual proposals have severe security flaws

The key idea is user identification instead of interface or even host identification

Wrong at the basis is that IP addresses mean:

- Location
- Device identification
- User identification

Use of cryptography (public) allows:

- User Identification
- Anonymity