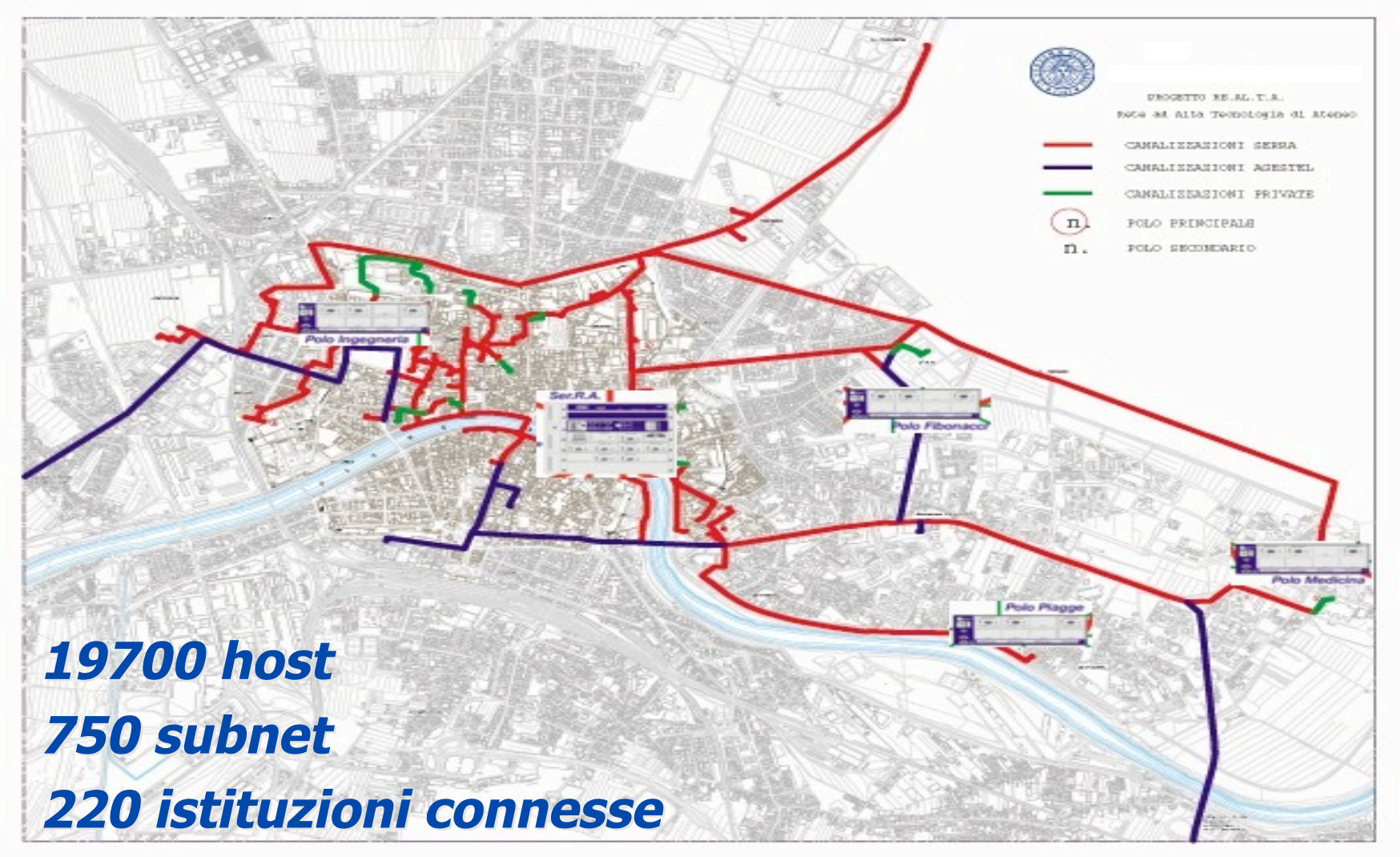
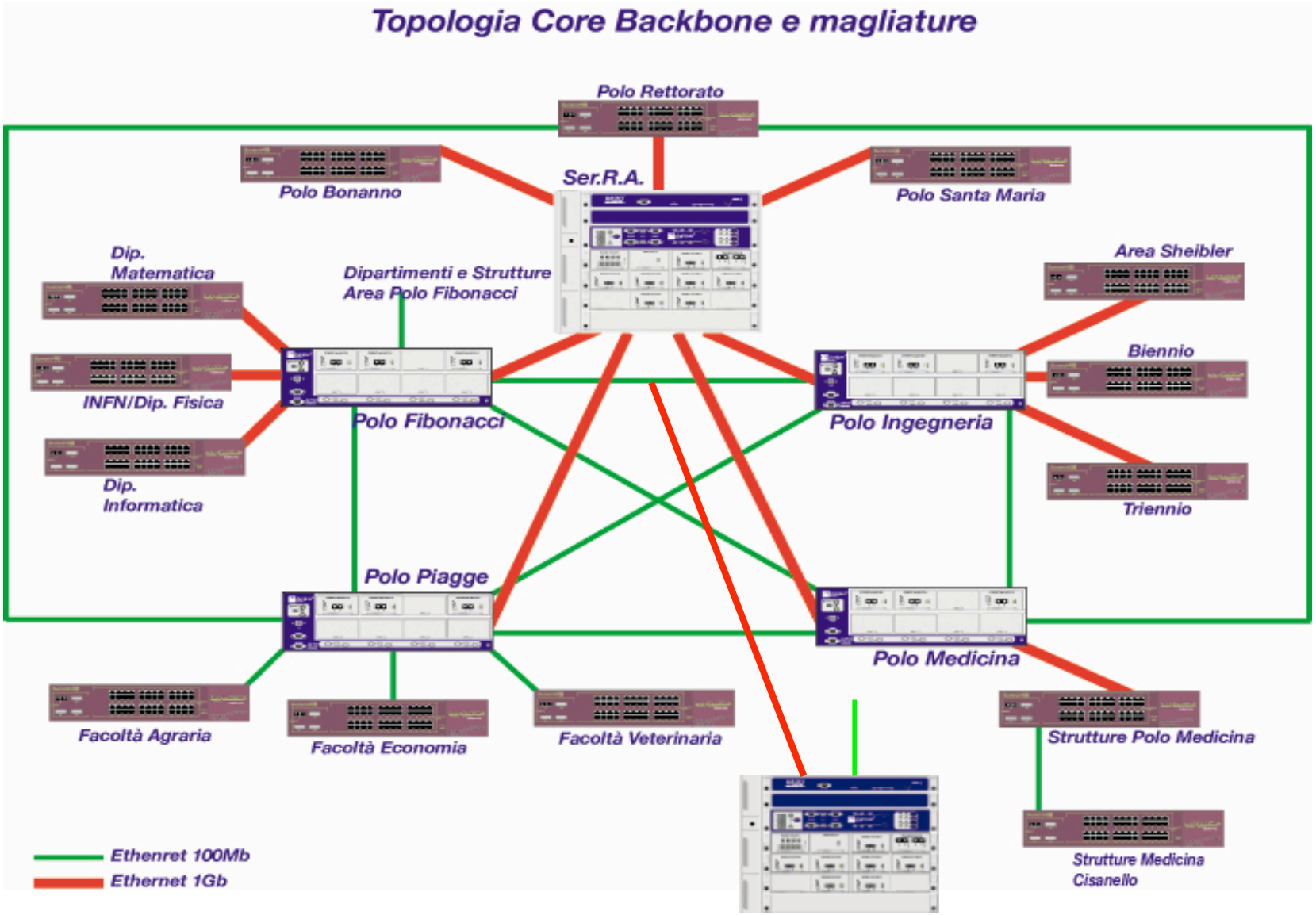
Pisa Multiservice network: una gestione semplice per una utenza eterogenea

Stefano Suin *stefano@unipi.it*
Paolo Caturegli *paolo@unipi.it*

Man Pisana: Core Backbone



Man Pisana: topologia di rete

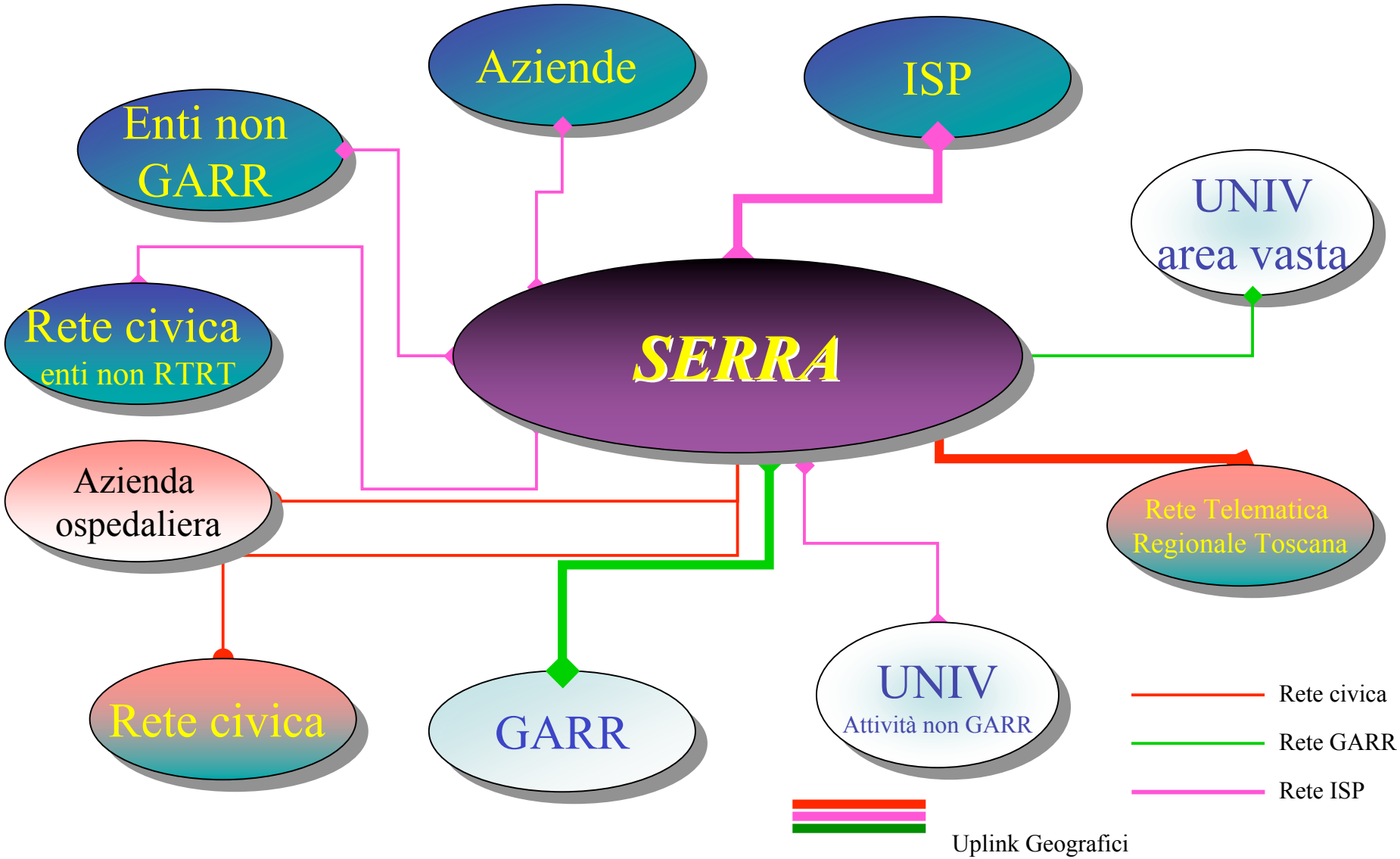


Scrivania di stefano e paolo

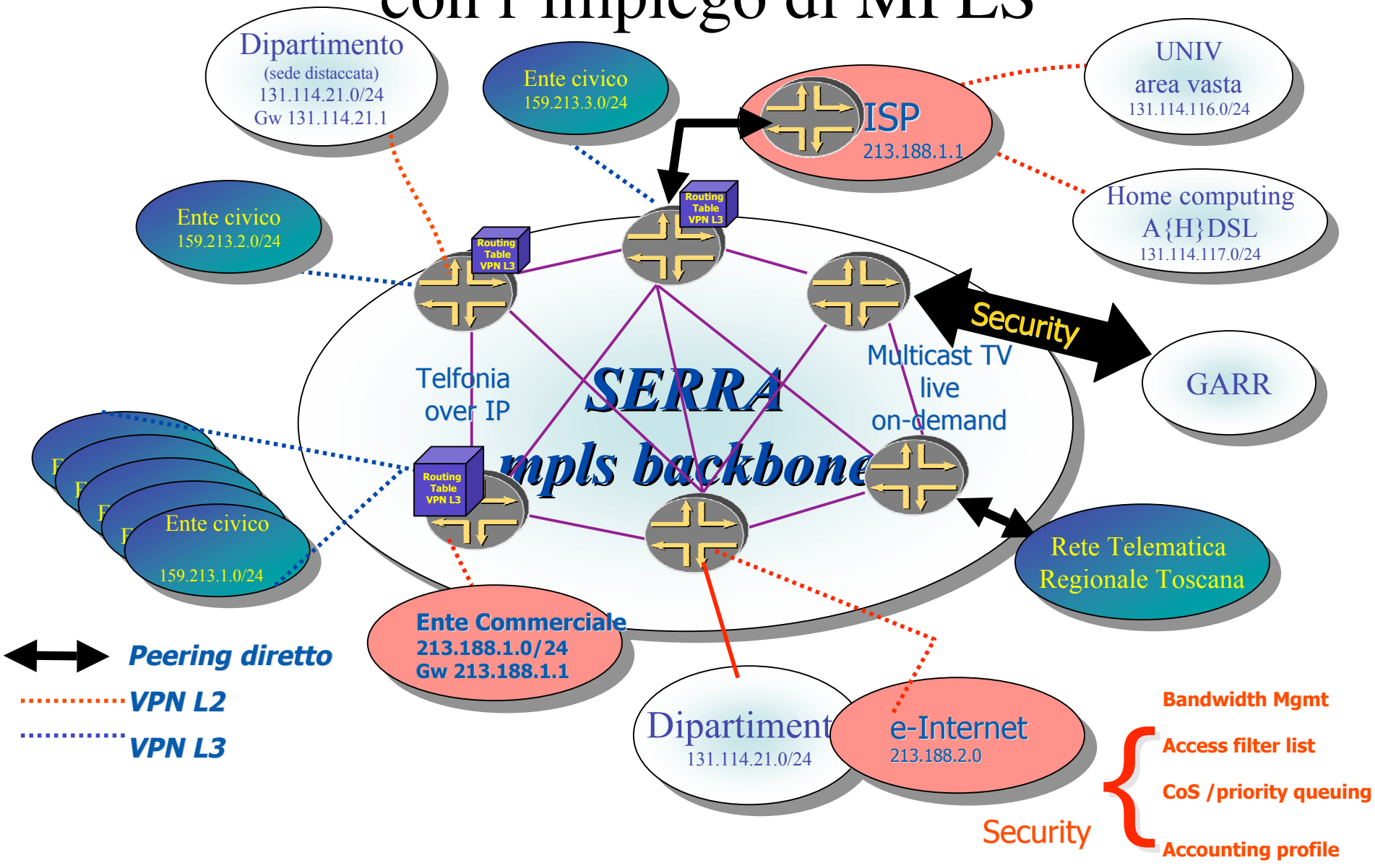
Trasporto

- Scelta iniziale ATM
  - ridondanza e protezione alla base della scelta
- Migrazione MPLS
  - traffic engineering
  - traffic protection
  - VPN L2 e BGP/MPLS
  - Scelta per l'utenza
- Igp
  - core in ibgp full mesh, edge in Ospf

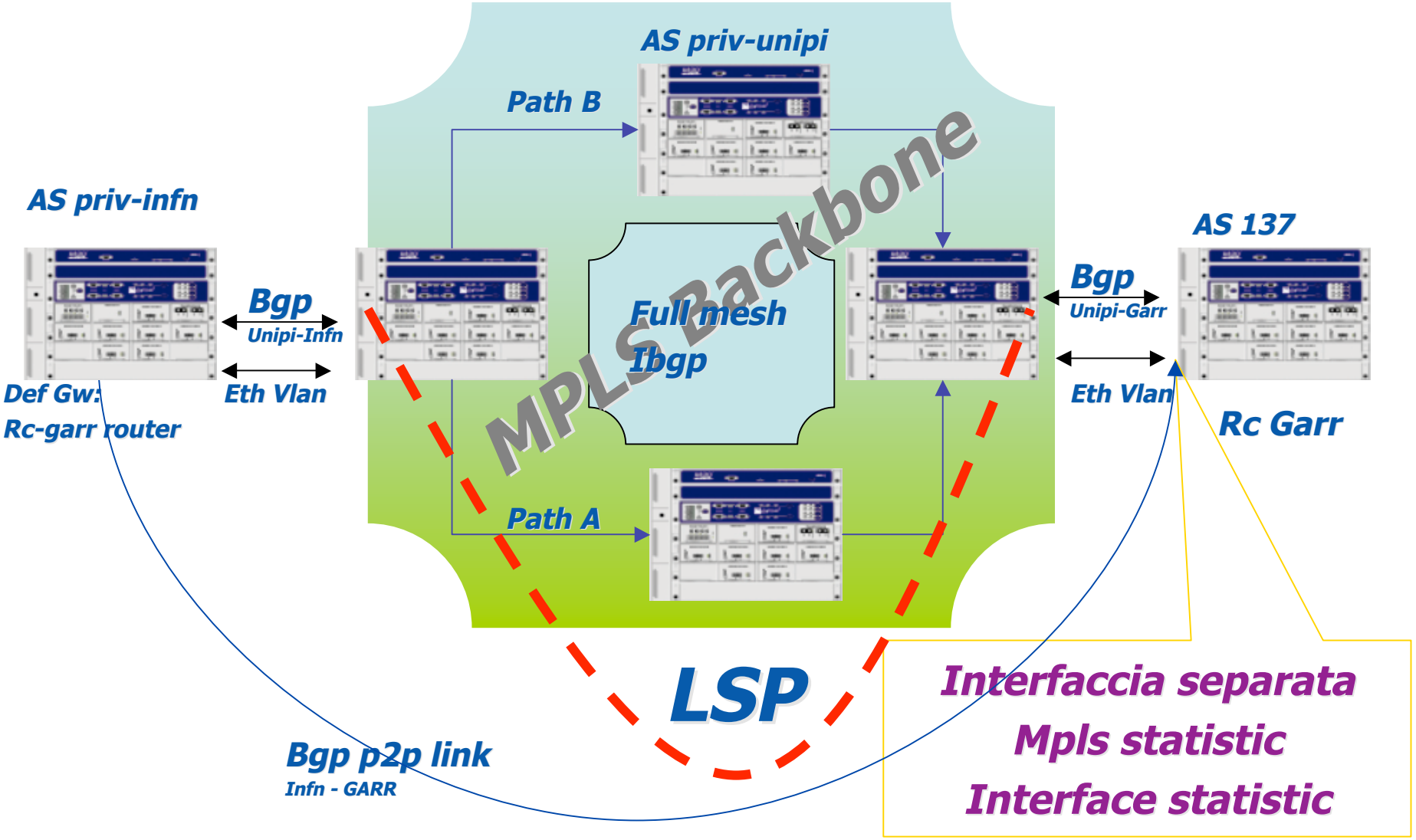
L'utenza della rete Pisana



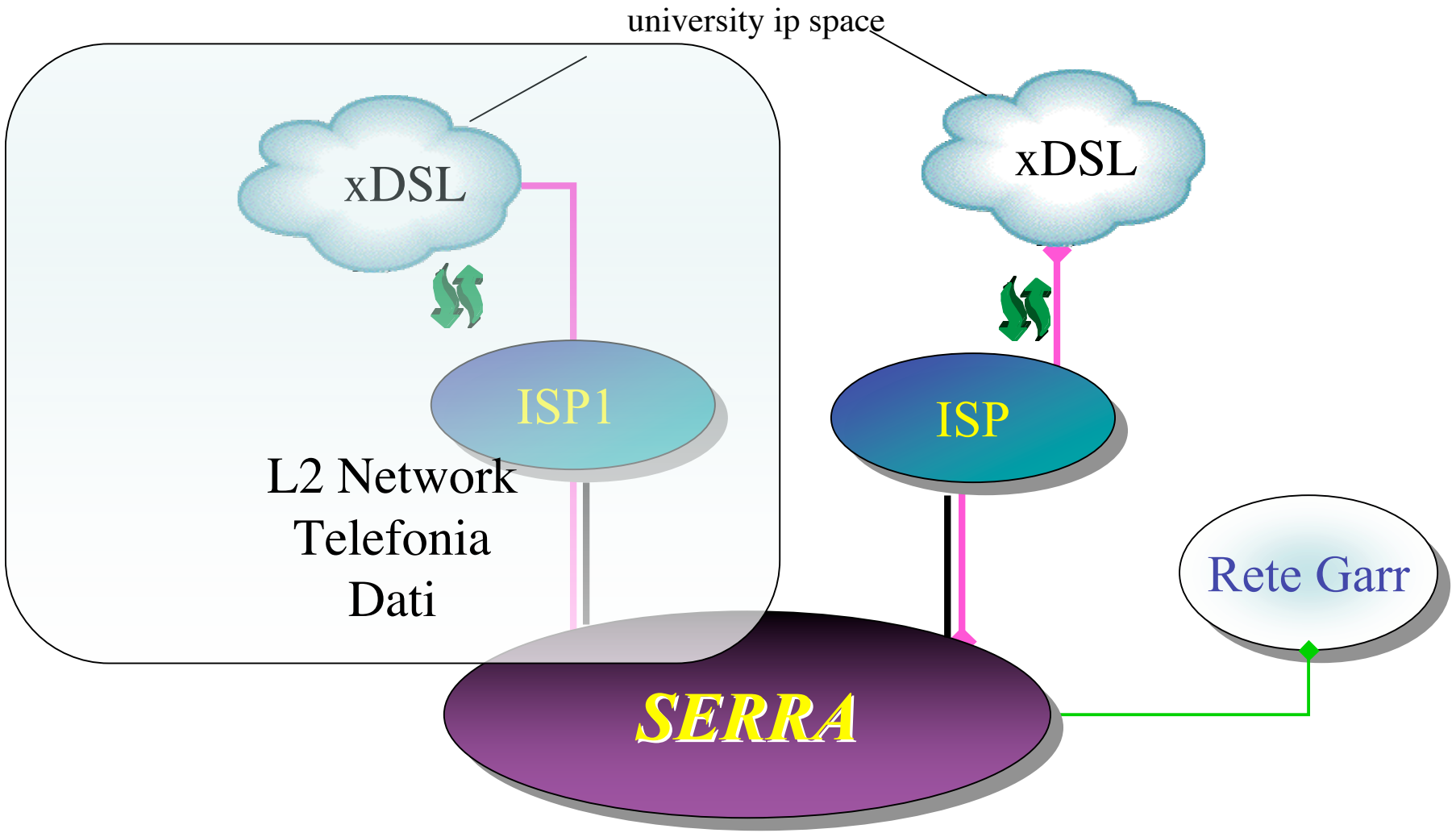
Soluzioni di trasporto e ridondanza con l'impiego di MPLS



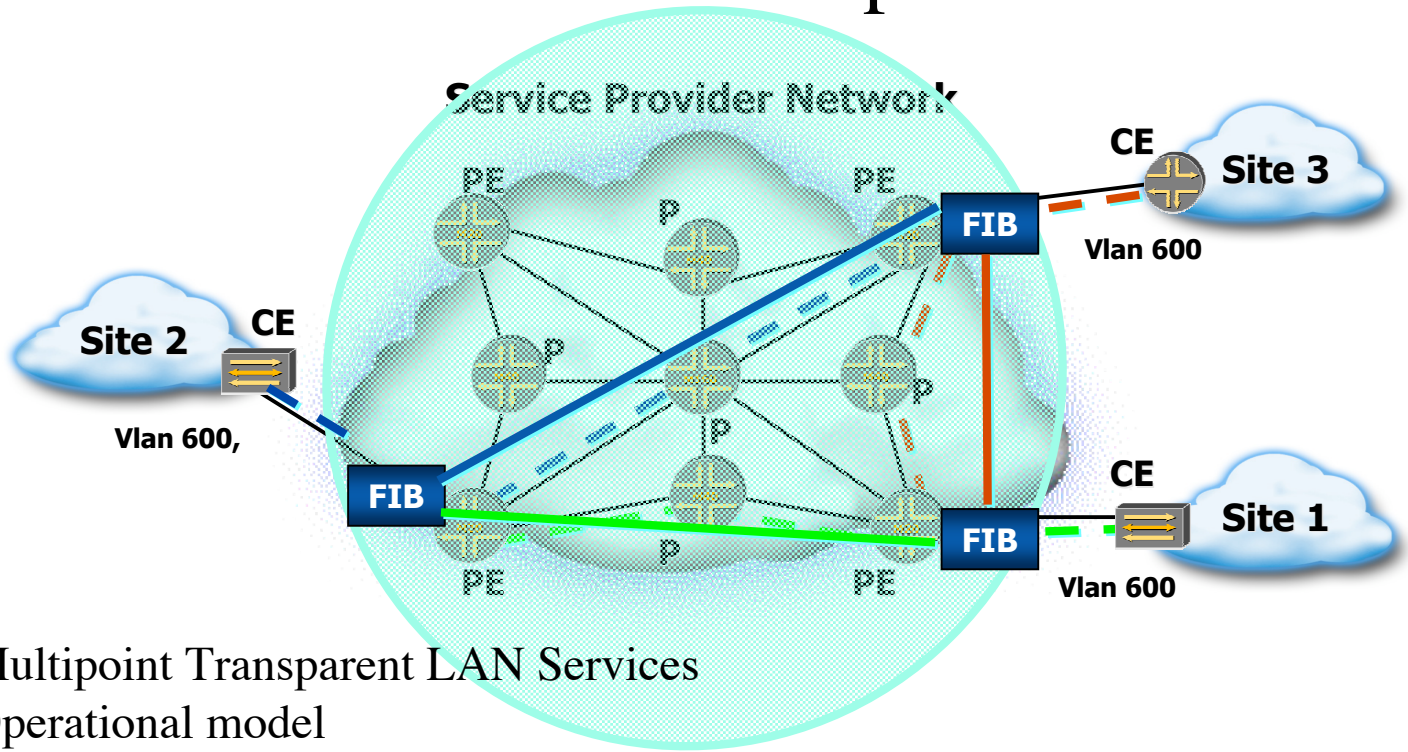
Utilizzo delle VPN di livello 2 per il trasporto trasparente: case study



L’estensione capillare della rete



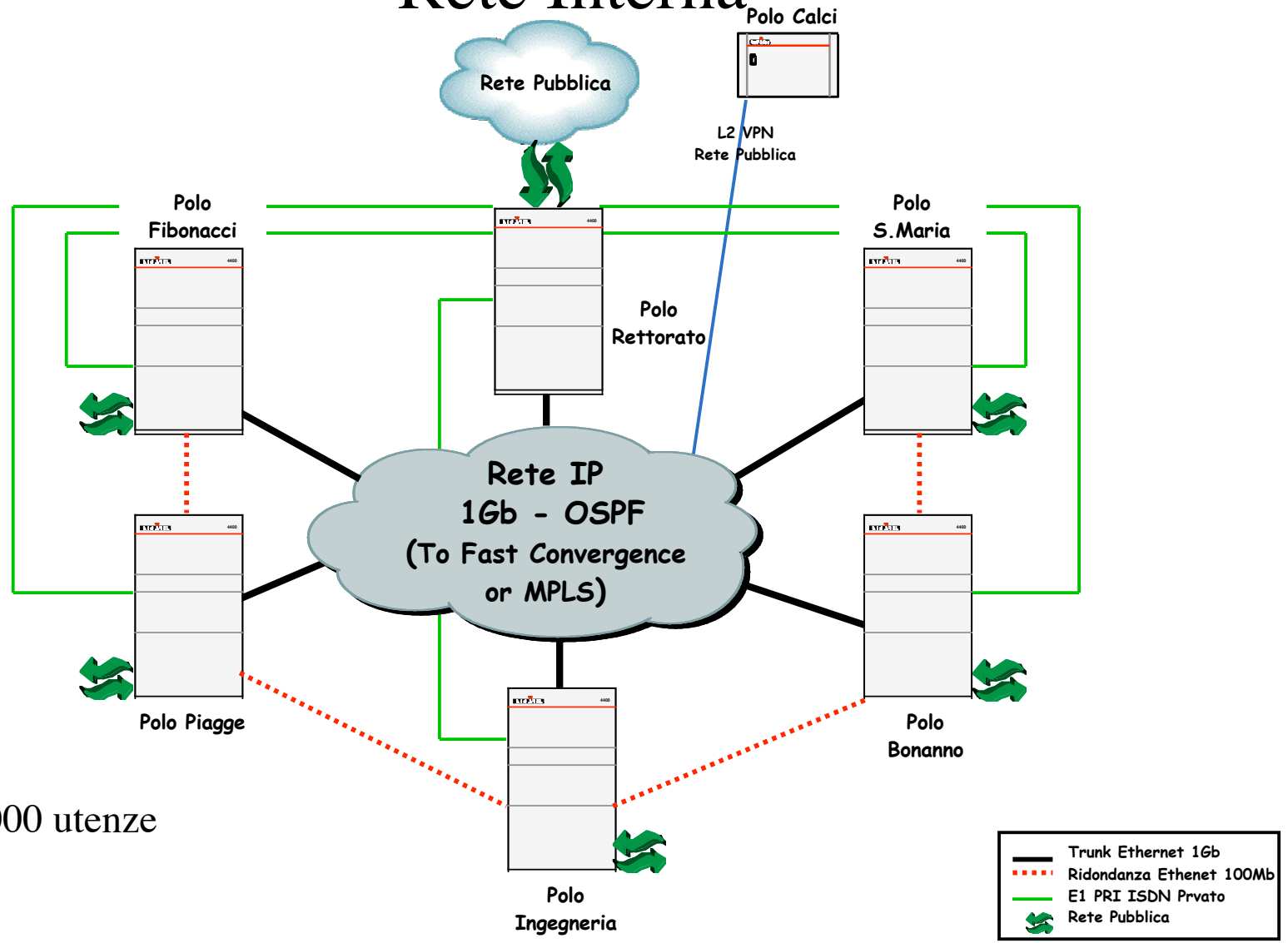
Virtual Private LAN Services (VPLS)
Draft-Kompella



- Multipoint Transparent LAN Services
- Operational model
  - **Full mesh of LSP between PEs (LDP or RSVP TE)**
  - **PE maintains site-specific VPLS bridging table (FIB)**
  - **VPLS discovery and signalling based on L2VPN (BGP)**
  - **VPLS traffic forwarded across provider backbone using MPLS**
  - **Auto-provisioning VPLS**
- Allows Inter-Provider and Carrier's Carriers applications

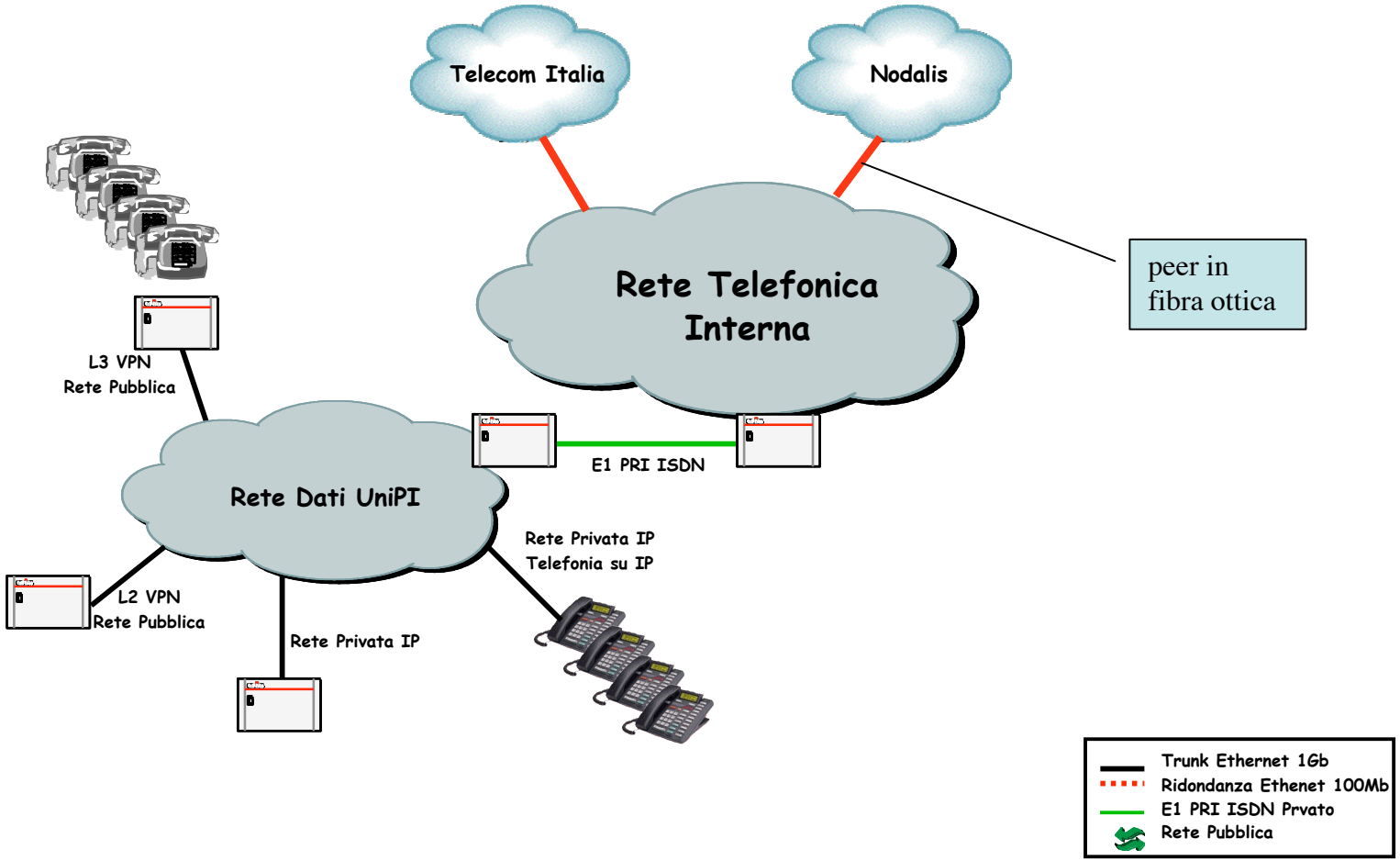
Sistema Telefonico Integrato di Ateneo

Rete Interna



Circa 8000 utenze

Sistema Telefonico Integrato di Ateneo
Collegamenti Esterni



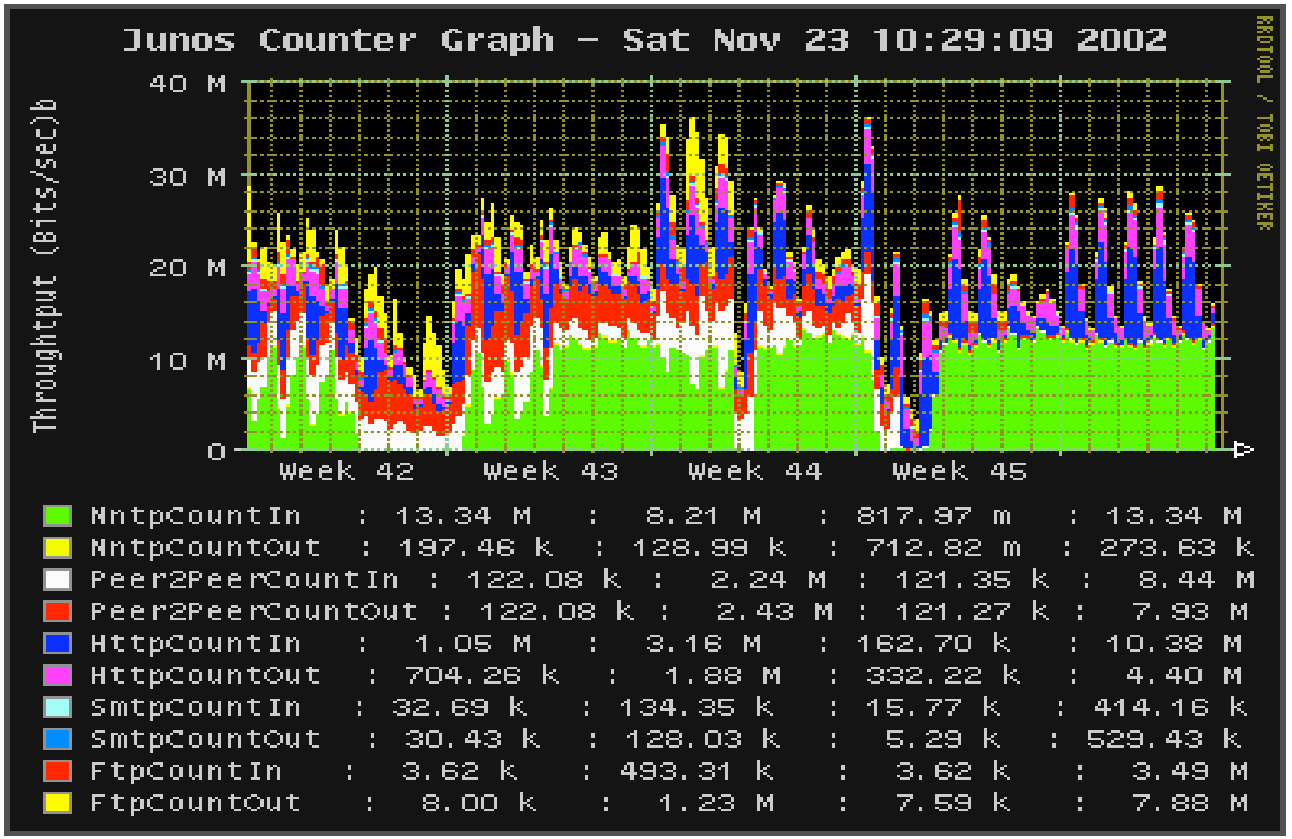
Sistema integrato telefonico di Ateneo

- VOIP
  - Utilizzo della magliatura
  - Linee di backup per il trasporto dei sistemi incompatibili con voip (fax 64, modem etc.)
- Beneficio immediato RISPARMIO
  - riduzione dei contratti da circa 1000 contratti a 300 in un anno in diminuzione
  - Sistema di amministrazione centralizzato
  - politiche di sconto significative
  - routing telefonico

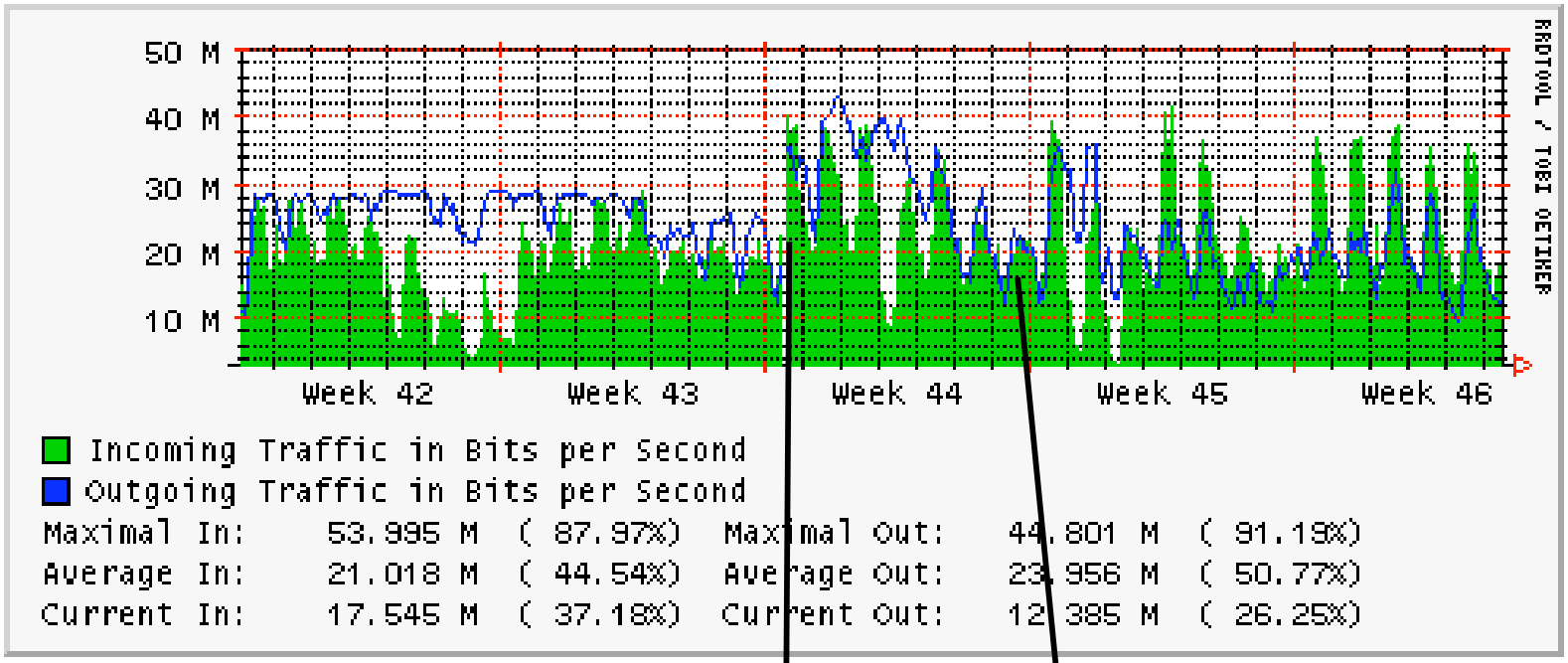
Il router di frontiera e la gestione degli utenti

- Hardening del router di frontiera dal punto di vista della sicurezza
- L'apm non è generalmente responsabile delle politiche di sicurezza delle istituzioni collegate
- Quale politica si applica, dunque?
  - Default deny sulle porte "insicure storicamente" e apertura su richiesta, anti-spoofing, loose reverse path forwarding check...
- Ma il primo passo è rendersi conto di come viene utilizzata la propria banda (la soluzione non è aumentarla ma gestirla correttamente)

Analisi dei protocolli noti



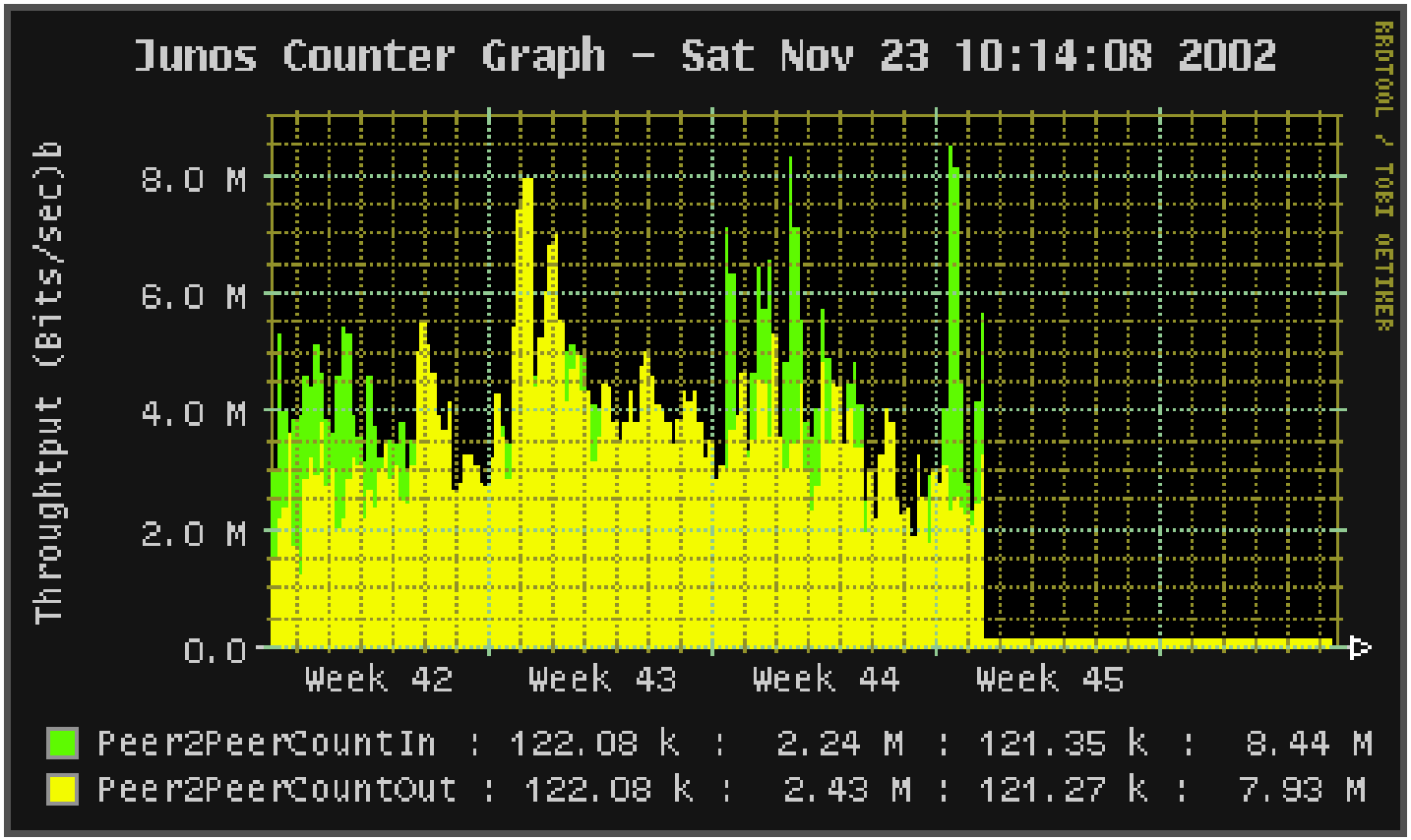
Gli effetti disastrosi del traffico p2p



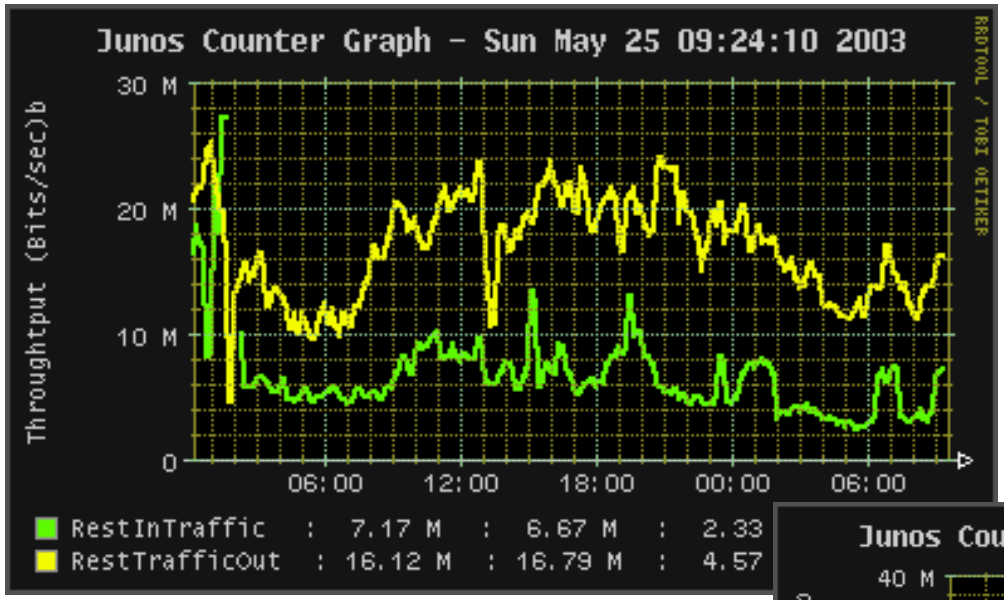
Upgrade di banda da 34 a 45 Mbit

Politiche CoS sul p2p

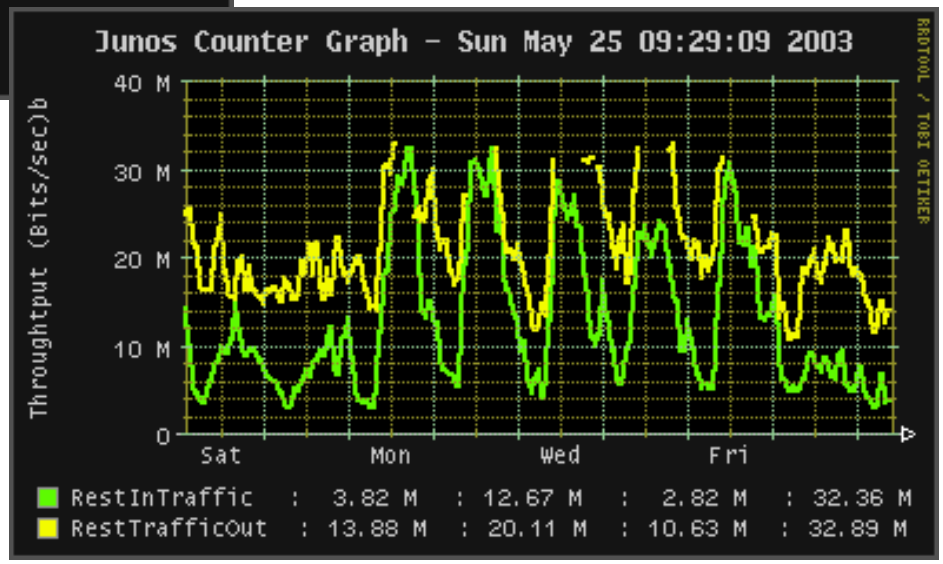
CoS sulle well-known: ma la situazione non cambia di molto, perché?



Tolti i protocolli noti, e messe le acl su titti i più noti p2p:



Oltre il 65% del traffico in entrata e/o in uscita risultava non identificato



Il traffico in uscita non segue la "normale" sinusoidale, rimanendo inalterata anche nel periodo notturno

Le motivazioni

- Configurazioni di default (upload illimitato in peer e banda)
- Installazionie di circuiti paralleli
  - Es Kazaa, si diventa nodi inconsapevoli di una rete utilizzata per scopi a noi ignoti
  - La licenza di Kazaa (dopo l'acquisizione della Brillant Digital Ent.) garantisce che non vi sia alcun tipo di trojan....

'No Spyware' Policy Kazaa Media Desktop Does Not Contain Spyware

Nor support the distribution of spyware to others.

[..]you must install software from third party software vendors pursuant to licences or other arrangements between such vendors and yourself ("Third Party Software").
Please note that the THIRD PARTY SOFTWARE is subject to different licences or other arrangements, which you should read carefully. By installing and using this THIRD PARTY SOFTWARE you accept these.[..]

Ed ecco il busillis...

- Questo è un estratto di una licenza di questi (AltNet Inc.) software...

"You hereby grant (Brilliant) the right to access and **use the unused computing power and storage space on your computer/s and/or Internet access or bandwidth** for the aggregation of content and use in distributed computing," the terms of service read. "The user acknowledges and authorizes this use without the right of compensation."

- E non è l'unico caso...altri file, invece (dlder.exe) effettuano il monitoring dei siti web visitati per poi riferire le scoperte ad altri

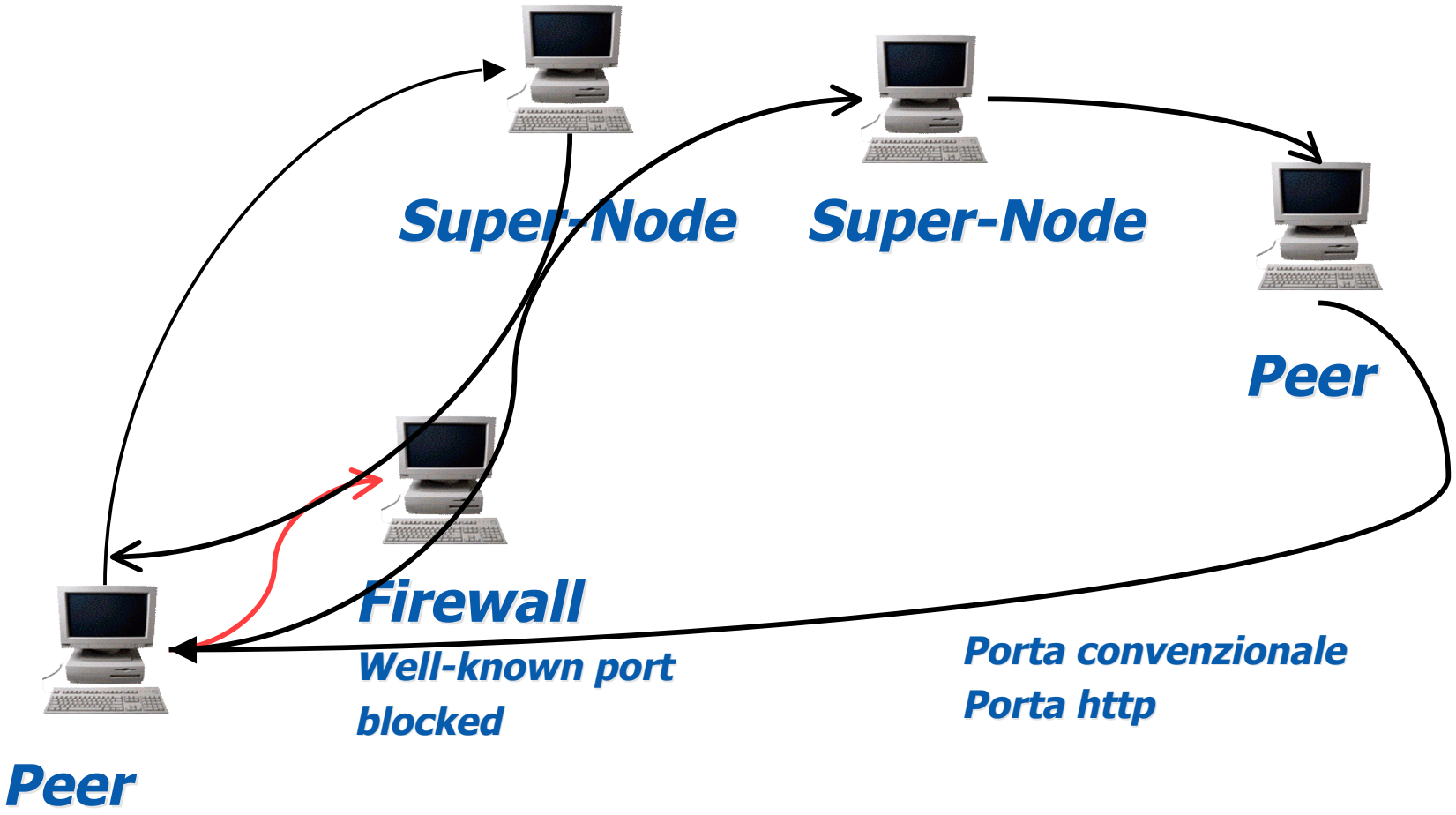
Perche' non vengono limitati i parametri?

- Incompetenza
- Premio
  - Più materiale è condiviso...
  - Più download verso il nostro nodo vengono registrati....
  - Più banda in downstream viene riservata, più privilegio assumono le richieste verso i super-nodi
  - Non solo ma gli oggetti più gettonati vengono mostrati come risultato di query solo a chi condivide più di una certa quantità di materiale
  - In alcuni peer network, ad esempio in DirectConnect

Il controllo dei traffici p2p

- Non bastano i normali packet filtering
- port 80
- tecniche di push

La tecnica di Push: ovvero come aggirare i firewall packet filtering



Ptop

- Utilizzo di parametri statistici sul volume di traffico e di peer contattati al secondo
- Falsi positivi inferiori al 1.5%
- Il problema è risolto? No, è cominciato.
- L'ISP è non responsabile dei contenuti nella misura in cui non li conosce: salviamo la banda e andiamo in galera, o ponziopilateggiamo?

Il monitoraggio “legale”

- Politica di sicurezza, accettata e appriovata dal management, e adeguatamente diffusa agli utenti
- Assunzione di responsabilità dell’utente che deve essere consapevole che l’azienda, nel rispetto delle normative, mette in atto tutti i controlli necesssari alla tutela del proprio patrimonio di risorse
  - sistemi, indirizzi e.mail, telefoni etc..
- L’ottica deve comunque essere che tutte le azioni sono intraprese per una gestione corretta della banda, nel normale espletamento della proprria attività quotidiana