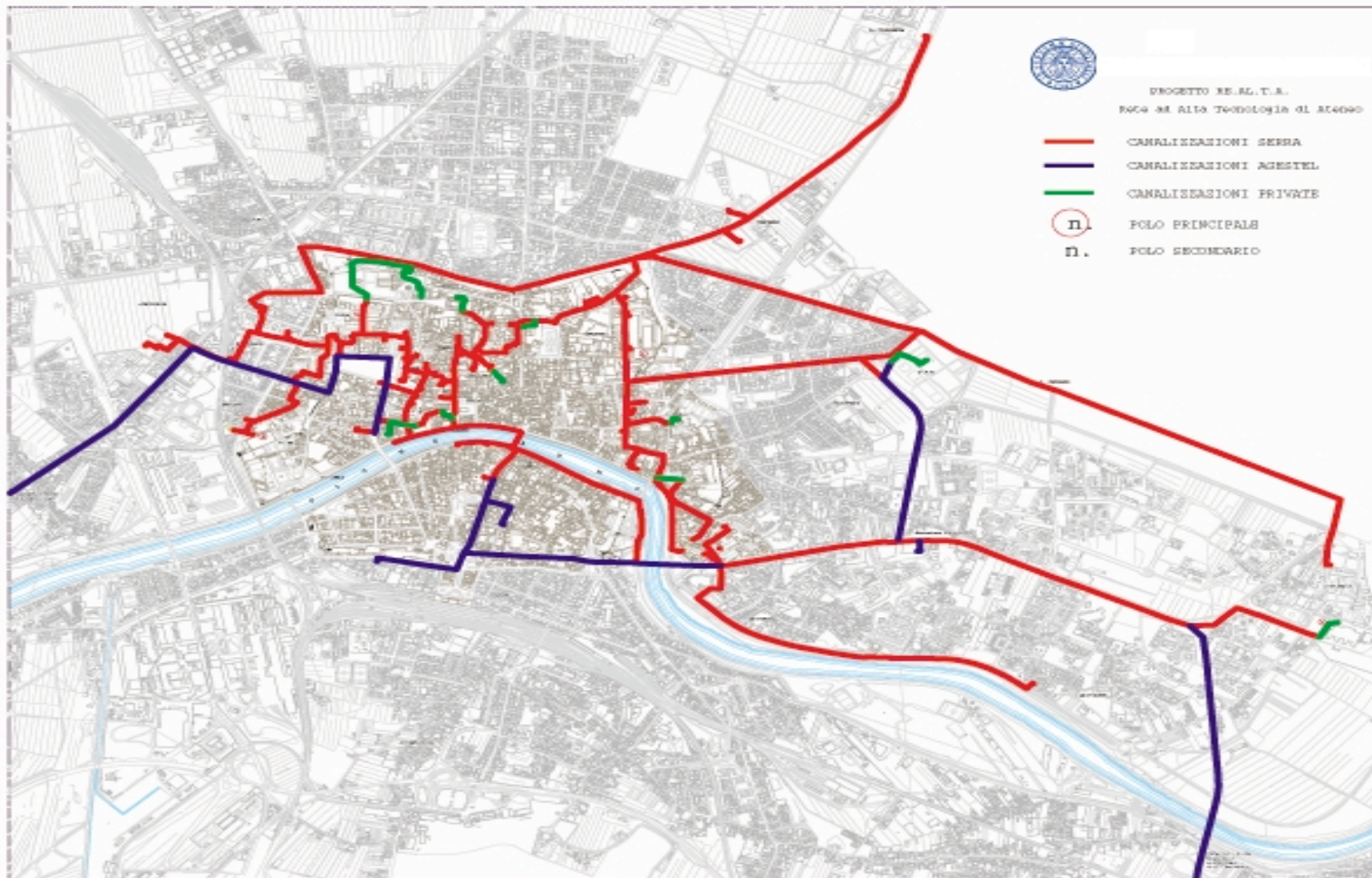


P2P - tecniche di riconoscimento e confinamento del fenomeno in una rete Metropolitana

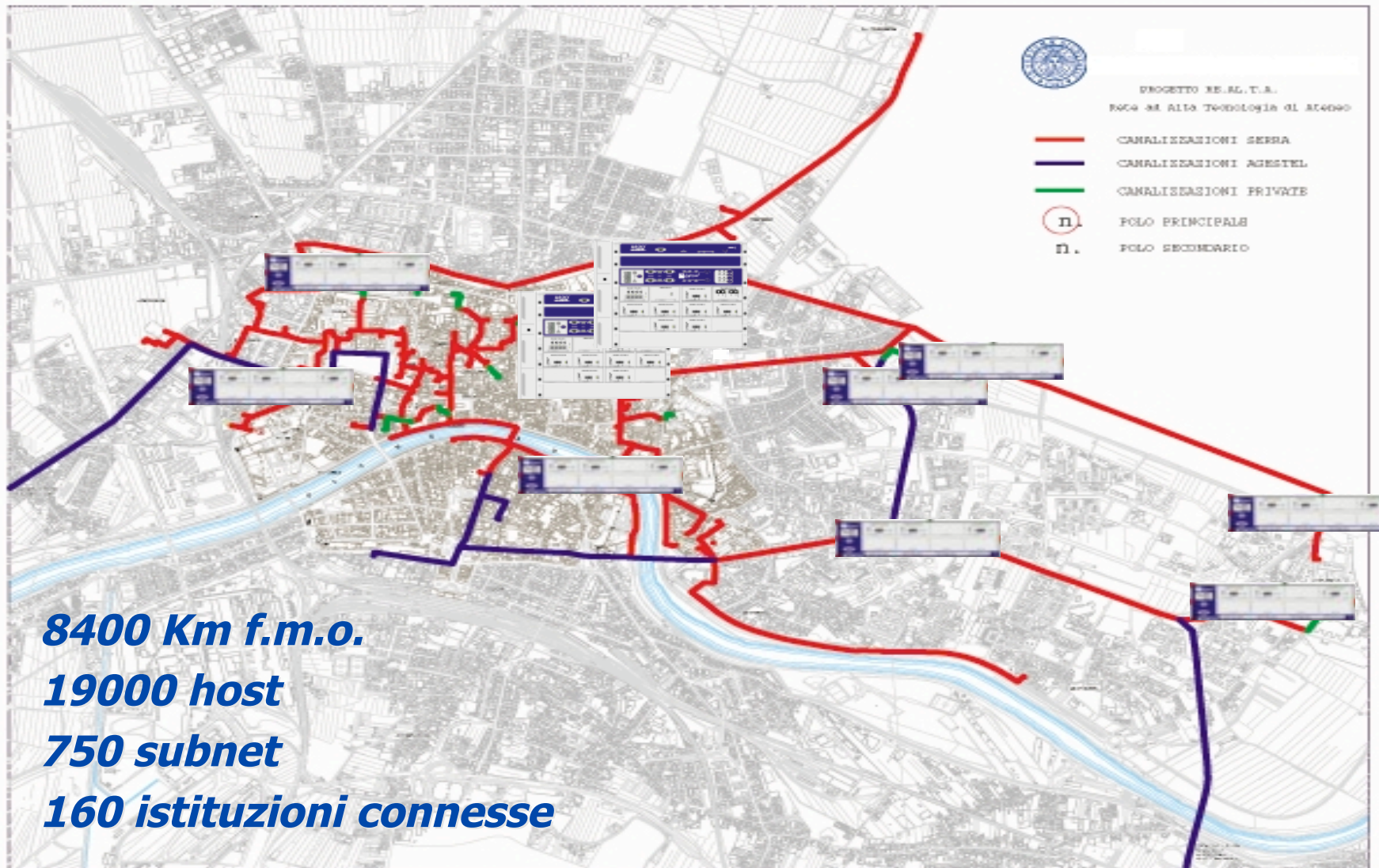
Stefano Suin stefano@unipi.it

Centro SERRA - Università d Pisa

Man Pisana: infrastruttura

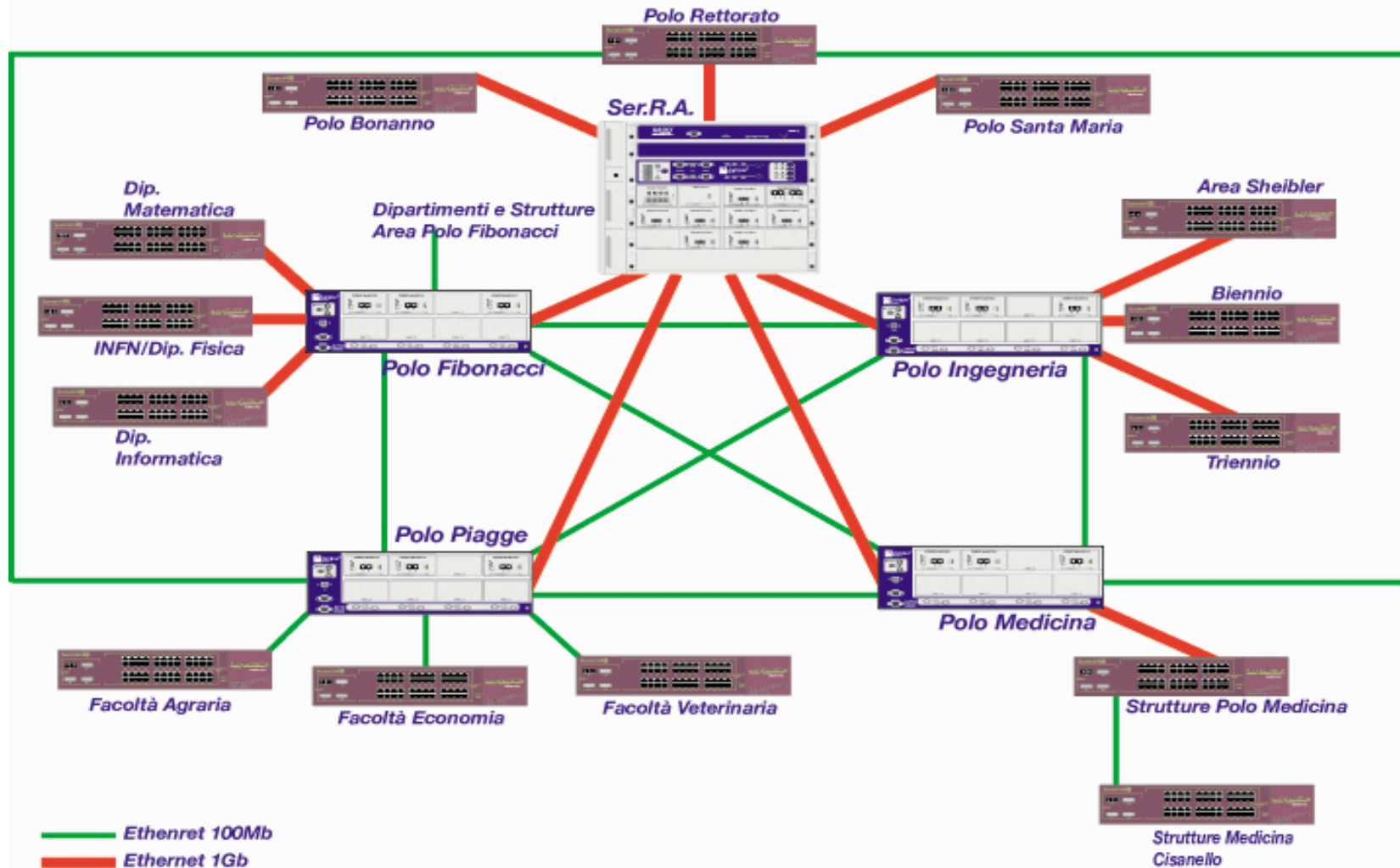


Man Pisana: core backbone

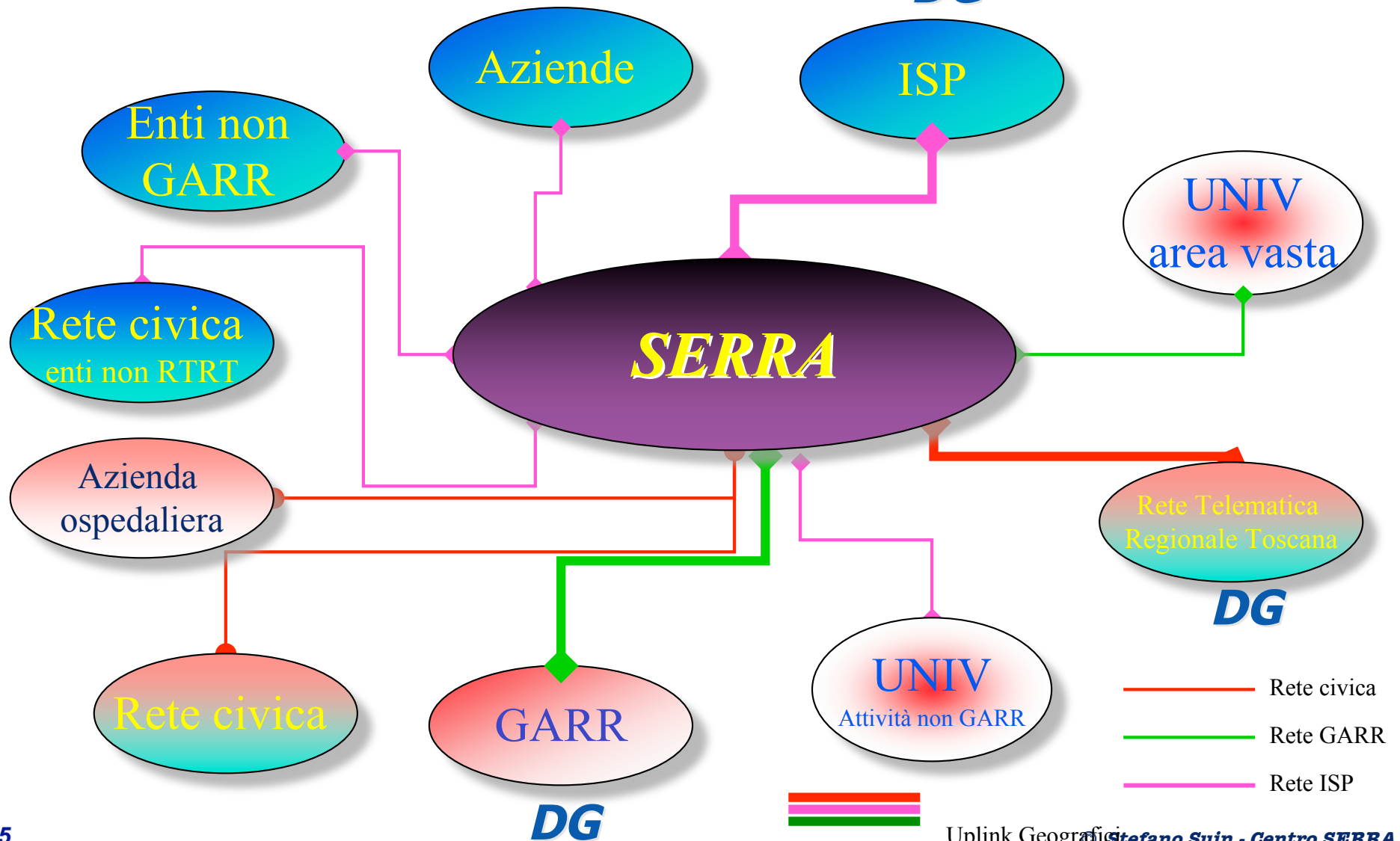


Man Pisana: topologia di rete

Topologia Core Backbone e magliature



L'utenza della rete Pisana ^{DG}



Multiservice network: la gestione semplice di una rete per una utenza eterogenea

I problemi da risolvere: La gestione della banda

- I problemi di banda non si risolvono aumentando la risorsa, ma gestendola
- Cosa ci passa sopra? E' veramente ciò che mi aspetto?
- Controlli che consentono un utilizzo ottimale
 - analisi della distribuzione di protocolli (ma come viene usata la banda?)
 - matrici di traffico (chi la usa e quali sono i vettori di traffico?)
 - matrici di flusso (chi parla e con chi?)

Controlli di banda - 2

- **Controlli che consentono un utilizzo funzionale alle esigenze**
 - controllo degli effetti del best effort nel traffico della nuova Internet (client-server, peer-to-peer, service location protocol)
 - ridondanza a tutti i livelli (fisico, apparati, trasporto) ma anche controllo dei fallimenti
- **Una volta che conosco la rete, devo gestirla:**
 - Strumenti per la scalabilità di banda
 - scalabilità nella allocazione della banda
 - Filter-based traffic shaping
 - prioritizzazione del traffico
 - CoS
 - policy routing

I problemi da risolvere: Comunità

- **Gestione delle comunità a diversi livelli di criticità**
- **Deleghe di servizio e gestione**
- **Policy di gestione delle risorse (es norme di accesso a internet)**
- **Il riconoscimento delle comunità per le attività di security policy, routing etc.**
 - **Piano di indirizzamento numerico IP**
 - **Routing protocol extension**
 - **VPN**

I problemi da risolvere: Sicurezza processo non prodotto (BS7799)...

- ... ma anche i prodotti sono importanti!
- I controlli perimetrali (hacker, worm, virus, spam etc.)
- Il controllo “dietro le spalle”: i problemi che provengono dalle propria comunità
- Controlli che consentono un’ efficiente attack mitigation durante la finestra di esposizione
 - Implica -> disponibilità di dati dettagliati in fase critica di attacco (sessioni, ip accounting, protocolli, picchi di traffico per protocollo, matrici di traffico per protocollo e volume di traffico) e (perché no?) disponibilità di sniffing del traffico IP!!!!
- Pro-active detection

**I presupposti di gestione:
Modello KISS: keep it simple,
stupid**

**● Le cose complesse sono difficili
da rendere sicure**

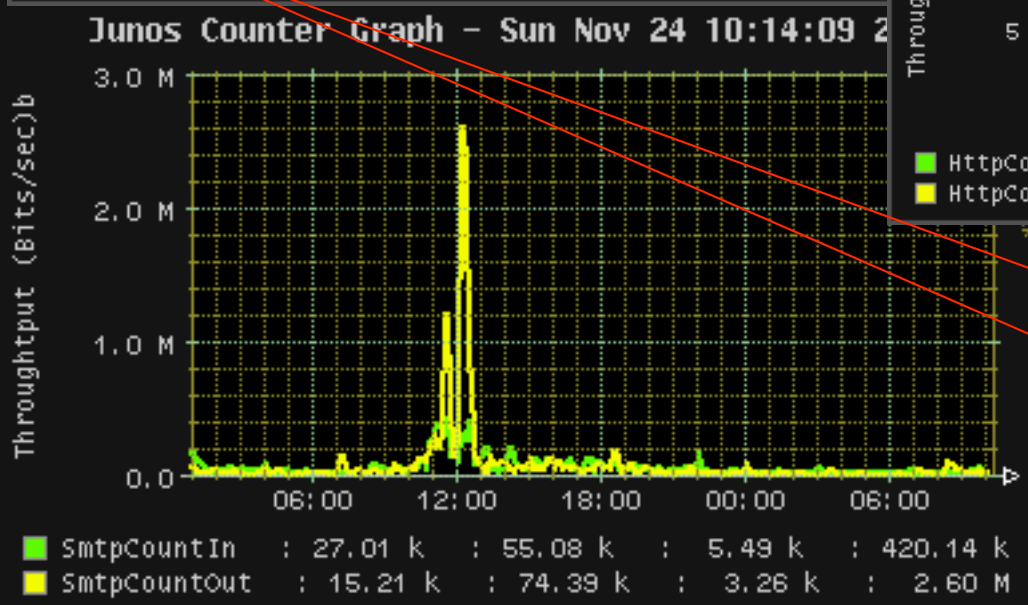
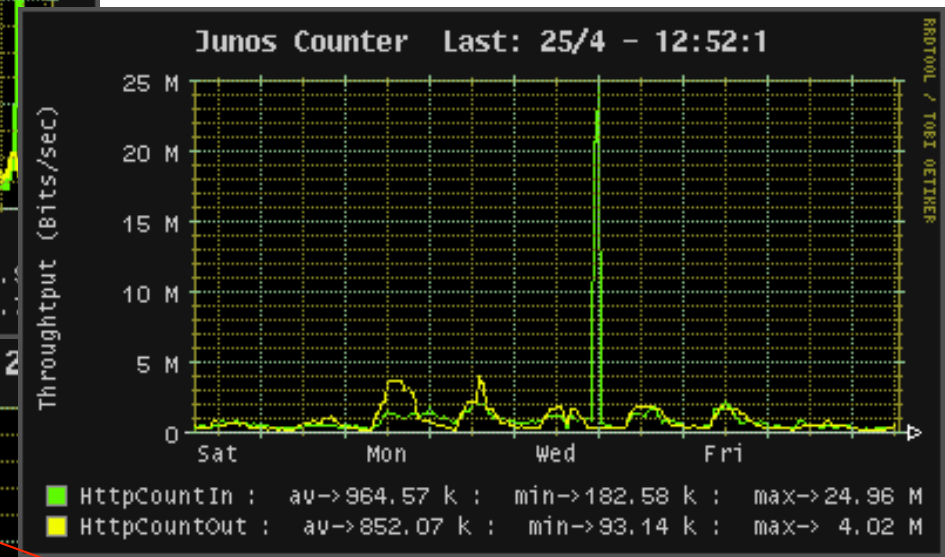
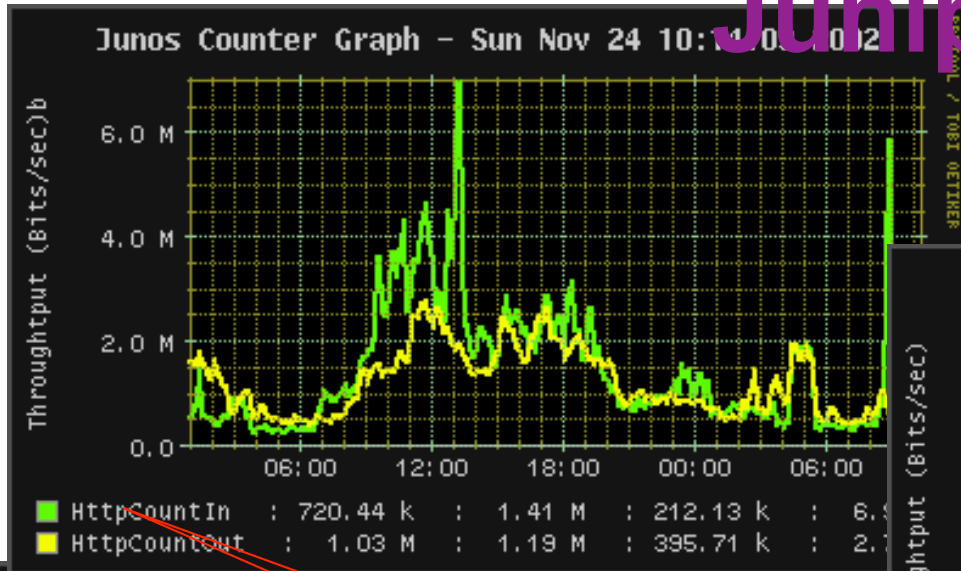
- **da progettare**
- **da implementare correttamente**
- **da capire/analizzare/monitorare**
- **da verificare**
- **da aggiornare/ modificare**
- **Plan-Do-Check-Act (BS7799)**

I presupposti di gestione: Economicità e rendimento

- **Il costo del meccanismo non deve superare il valore, in termini di perdita, del bene da proteggere**
- **L'investimento deve essere protetto, in termini di evoluzione della rete**
- **Le risorse devono poter essere assegnate in modo scalabile**
- **L'utilizzo delle risorse deve poter essere monitorato e rendicontato**

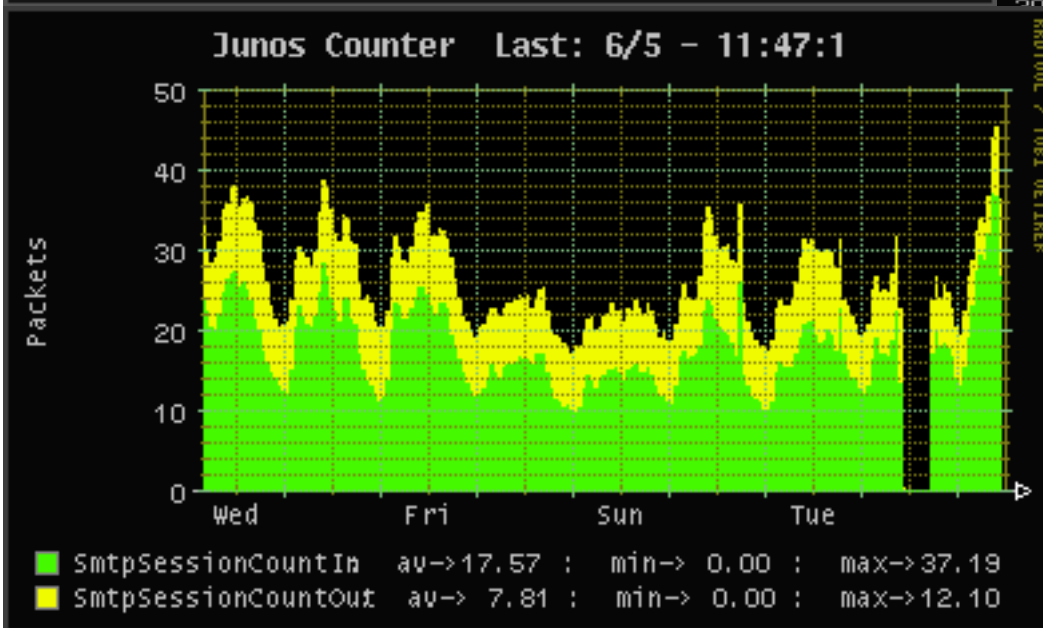
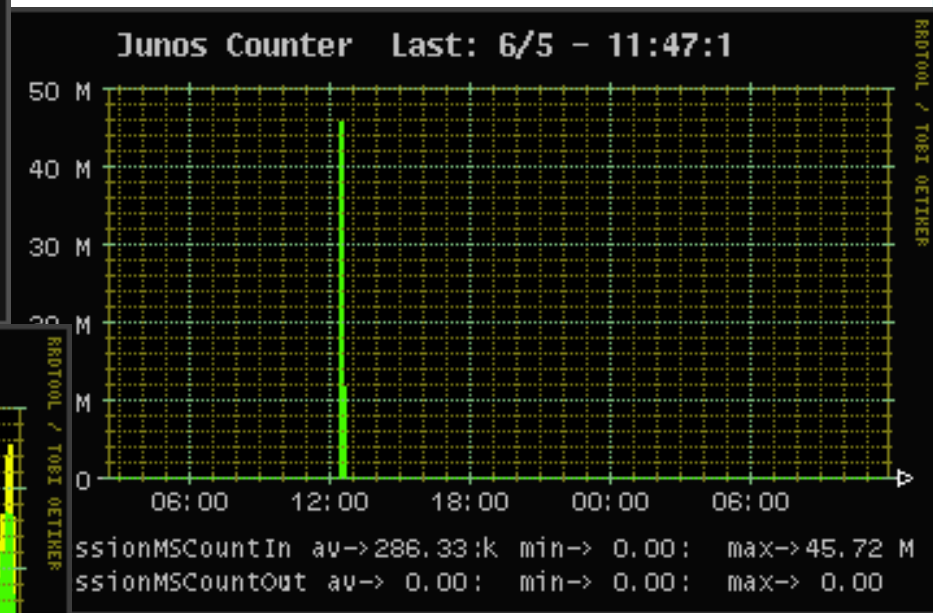
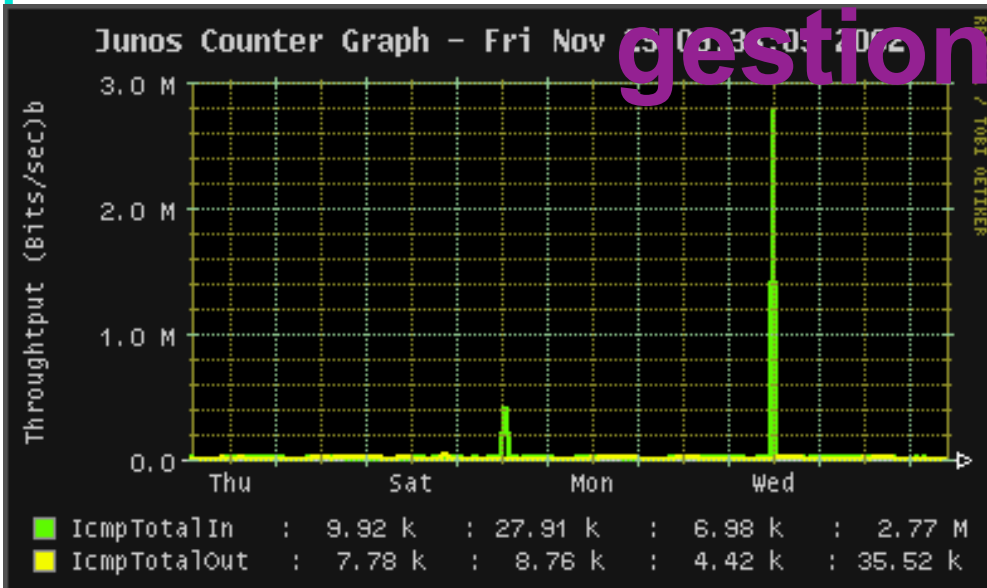
Sicurezza/ controllo di banda: l'analisi dei comportamenti attesi

Analisi di protocollo: i counter Juniper

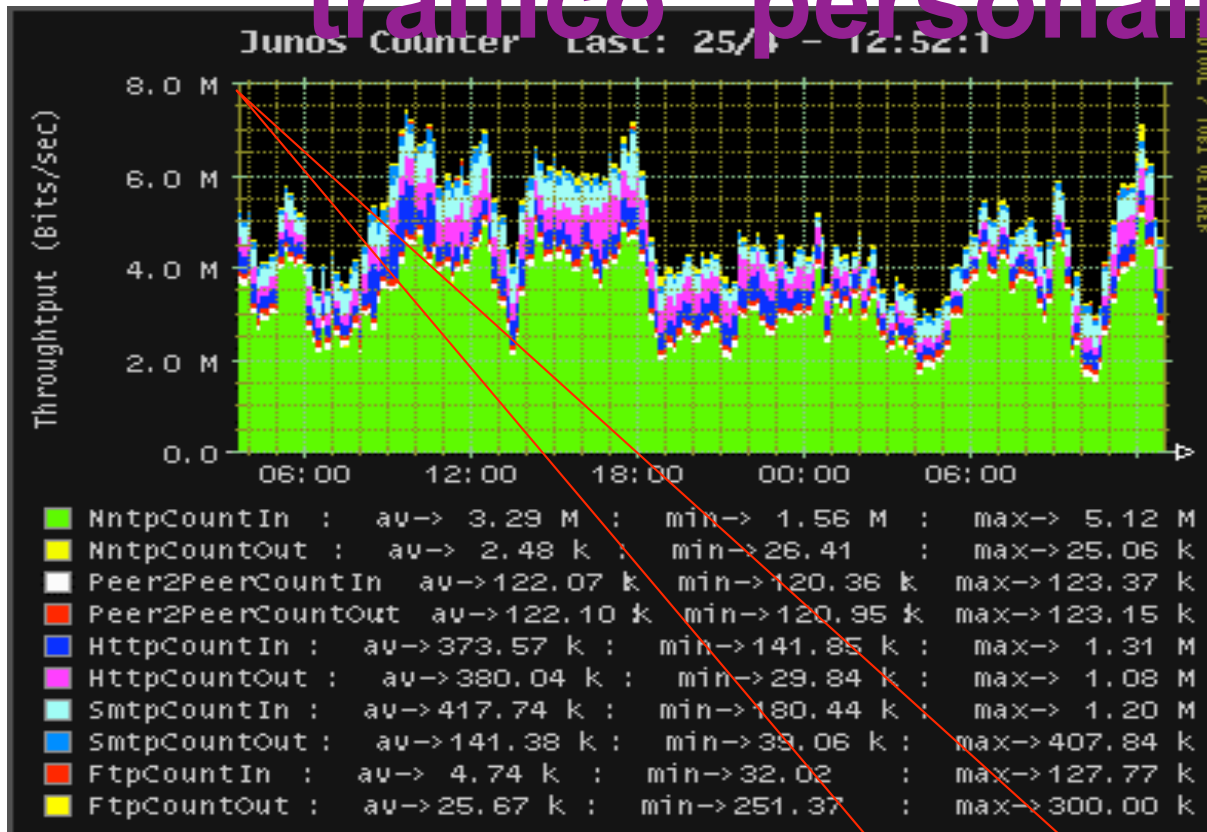


Ma posso fare counter di qualsiasi tipo di traffico

contatori per la sicurezza o la gestione reti?



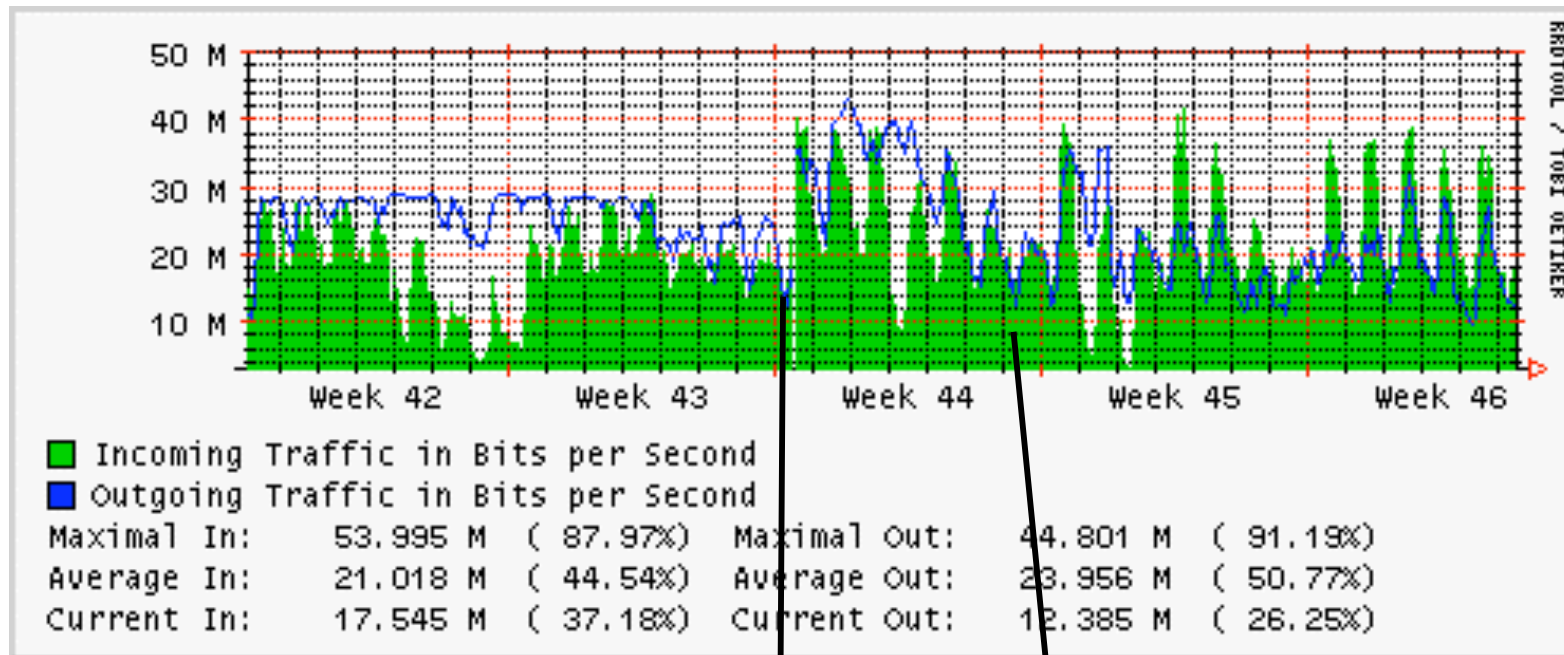
Il valore aggiunto: Contatori di traffico "personalizzati"



Bisogna disporre di uno strumento che consenta un facile "reporting" di dati

Ma la mia banda è 100 Mbit/s...

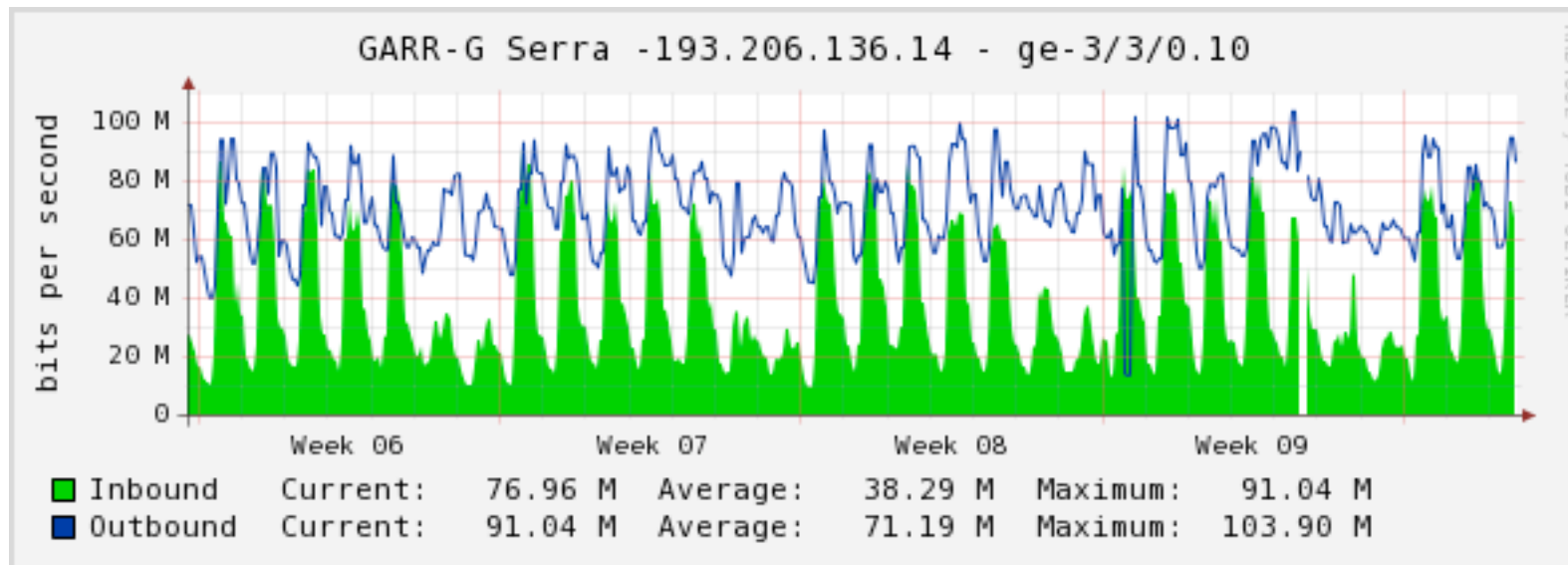
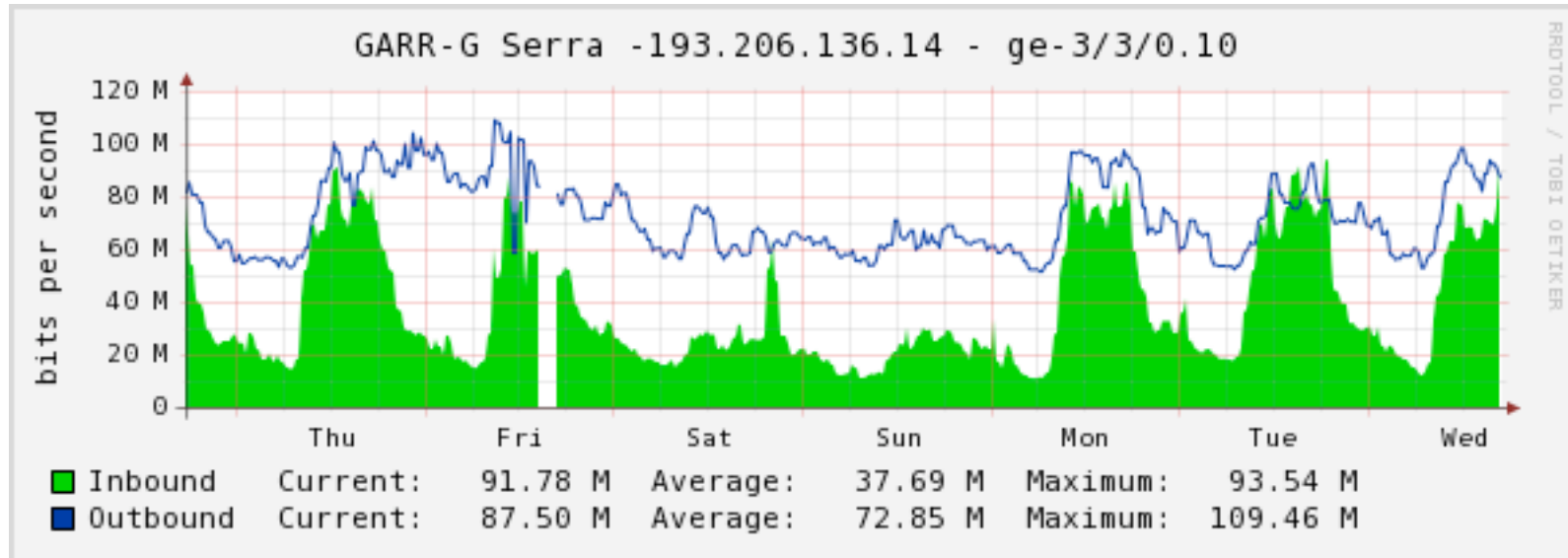
Gli effetti disastrosi del traffico p2p



Upgrade di banda da 34 a 45 Mbit

Politiche CoS sul p2p

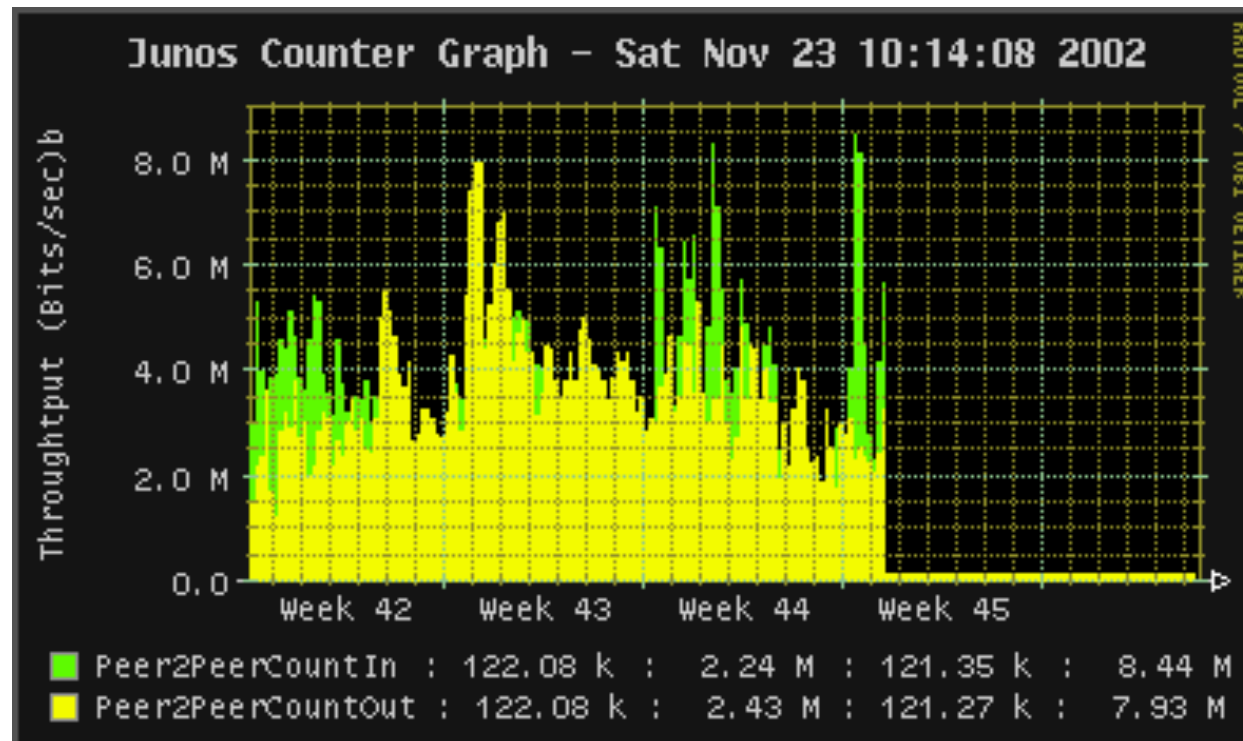
situazione attuale



Case study

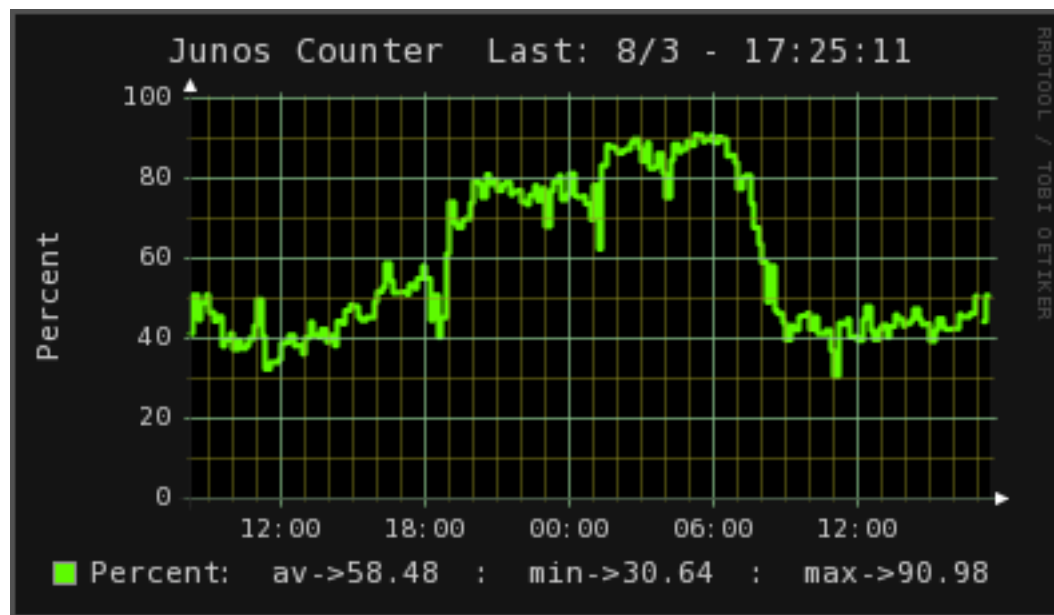
- **lo studio e il confinamento di un problema: il peer to peer: ovvero *come il controllo della banda (e quindi anche certi aspetti di sicurezza) non possa dipendere dal riconoscimento di sequenze note (fingerprint), ma unicamente dalla rilevazione di anomalie, intese come deviazione dai comportamenti attesi.***

CoS sulle well-known (ma il router lo deve supportare...)
Bisogna disporre di uno strumento che consenta un facile contenimento di un profilo di traffico (traffic shaping)



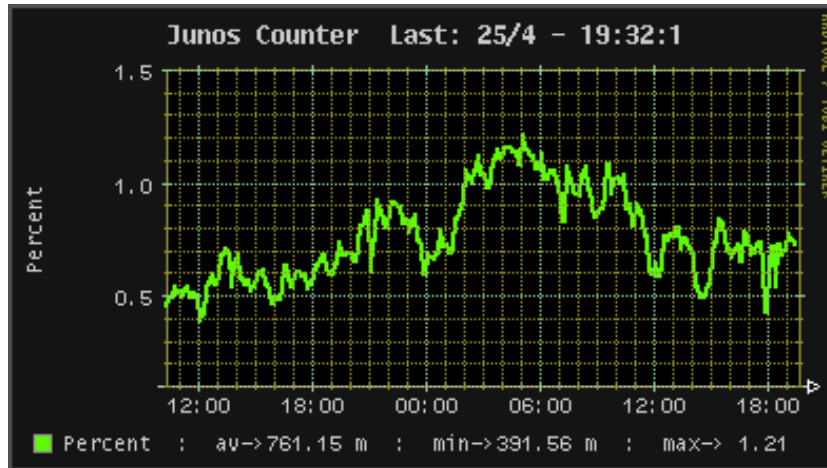
Ma il resto del traffico?

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

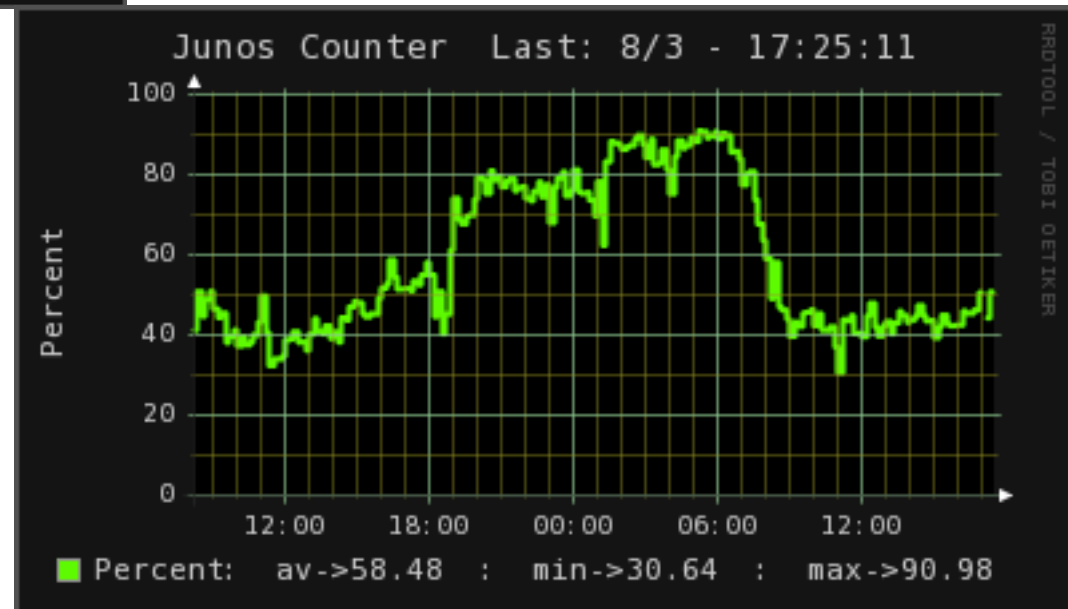


...potenza dei contatori...

Peer2Peer su porte note



Client to Client



Slide di giugno 2003:

- Alcuni protocolli stabiliscono sessioni con la porta client usata per la search, ad un'altra porta client su cui il peer mette a disposizione l'"oggetto"
- Basta limitare la banda per le search, che avvengono sulle well-known port?
- **Per ora abbiamo comunque 7/8 mbit/sec di banda in uscita utilizzata da protocolli "ignoti"**
- L'idea che stiamo perseguendo è quella di cambiare l'ottica: non dal protocollo alla porta, ma dalla porta al protocollo. Serve un accounting di traffico per porta.
- ...la battaglia continua...

Peer to Peer e Service Location Protocol: le nuove frontiere della comunicazione

- **Modello Client/Server non è più l'unico**
- Per i server i protocolli noti sono identificati da un "numero di porta" convenzionale (eg. 80 per http/web), per i client il numero e' un arbitrario > 1024 (e fino a 65536)
- Le politiche di filtraggio del traffico si basano sul riconoscimento di questa porta per i numeri convenzionali
- I service Location protocol si scambiano informazioni su Multicast
- Il traffico p2p (tutti i nodi sono allo stesso livello, e non c'e' un server) viene, per la quasi interezza, supportato su porte arbitrarie, quindi:

E' molto difficile contenere

il traffico basandosi sulle normali

politiche di packet filtering (firewall)

Come funzionano i Peer to Peer

- Ricerca degli oggetti su porte di solito convenzionali, anche se l'implementazione più diffusa è quella di utilizzare dei super-nodi che contengono la lista dei file condivisi su server che possono essere contattati per le richieste
- Non esiste più una memorizzazione centralizzata (Napster)
- I super-nodi (SN), e le relative porte di listening, sono noti al programma p2p attraverso vari sistemi
 - Built-in nel codice
 - Via web
 - Via file aggiornati periodicamente
- Ogni nodo è eleggibile come SN (condizione di default) ovviamente preferite le macchine che sono sempre on-line e hanno a disposizione banda

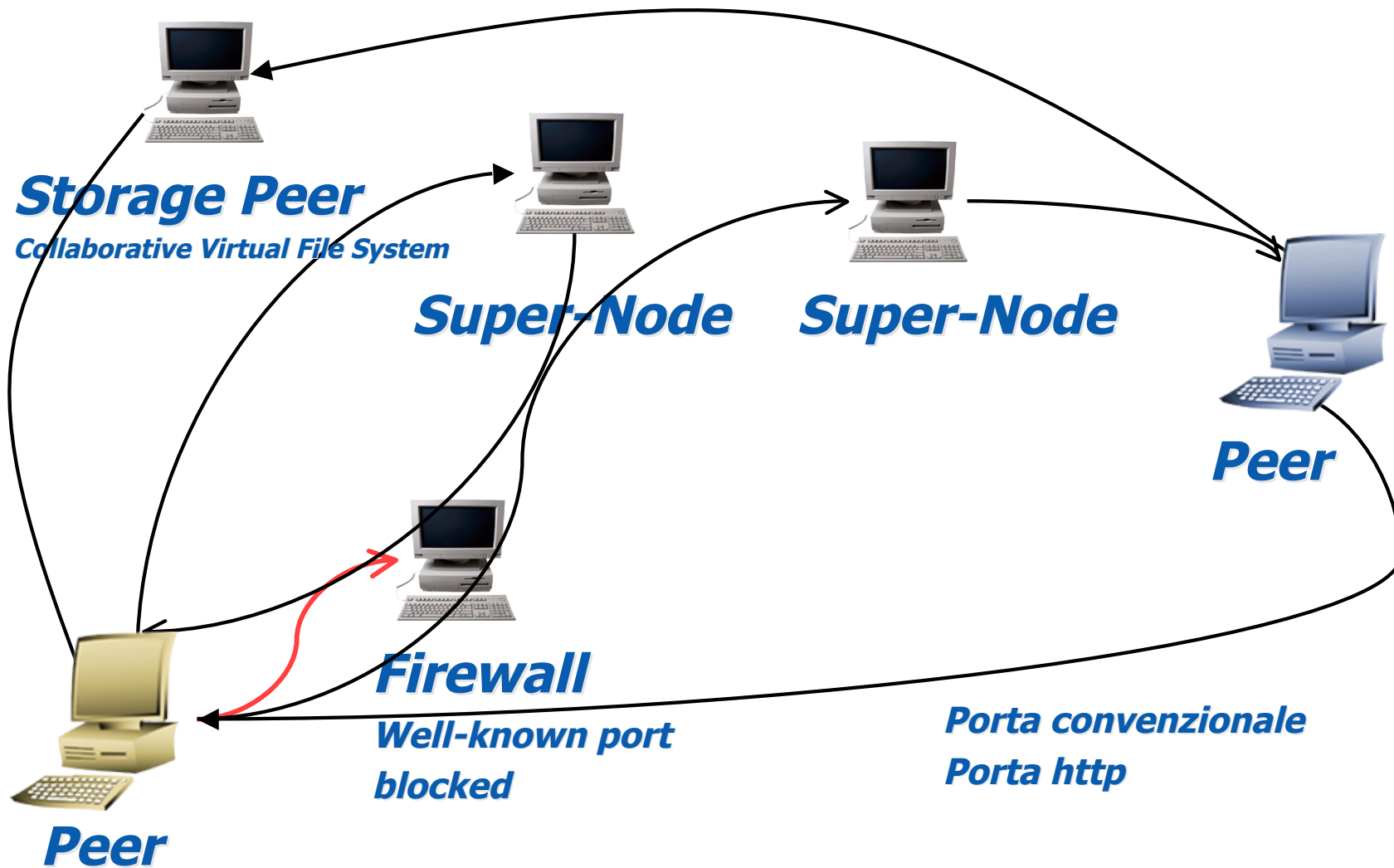
Come funzionano i Peer to Peer -2

- **Contatto del possessore dell'oggetto, attraverso le indicazioni del SN**
- **Inizio del trasferimento da molte sorgenti (aggiornate dinamicamente), ognuno per una porzione dell'oggetto interessato Dal momento in cui si inizia a eseguire il download diventiamo anche distributori per la porzione scaricata (aspetto legale)**
- **di peer contattati, i download e gli upload contemporanei dipendono in gran parte dalla configurazione del programma per l'utilizzo del circuito p2p**

Anonimizzazione

- **Nel circuito Freenet la memorizzazione e' su altri client che hanno dato la loro adesione "inconsapevole" all'uso del proprio spazio disco - l'obiettivo testualmente "enable anybody to publish and read information with complete anonymity"**
 - **Il possessore dei dati puo`tranquillamente negare di esserlo, chi vuol vedere i dati non deve possederli, e la persona che li possiede puo` affermare (e in parte è vero) che egli non aveva alcuna consapevolezza di cosa veniva registrato e per chi**
 - **Dal momento che l'area su disco è criptata il possessore del disco puo` in modo non smentibile asserire di non conoscere la chiave per il decode e quindi di non sapere cosa è registrato sul disco. Il possesso della chiave non implica il possesso dei dati e viceversa.**

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





[Informazioni importanti](#)

Contratto di licenza con l'utente finale di Kazaa Media Desktop

[Contratti di licenza con l'utente finale di Altnet Peer Points Manager e della barra di ricerca My Search](#)

[Versione stampabile](#)

Informazioni legali

Passaggio 2 di 6

Prima di eseguire il download e l'installazione di Kazaa Media Desktop occorre leggere e accettare il Contratto di licenza con l'utente finale di Kazaa Media Desktop e il Contratto di licenza con l'utente finale di Altnet Peer Points Manager.

Il software è fornito per accettare o rifiutare tali file, aggiornamenti e upgrade di software, in base agli aggiornamenti della versione a sua sola discrezione.

4.3 Installazione. Quando l'utente installa il Software, il programma di installazione (ad es. kmd260.exe) viene salvato nella Cartella miei condivisi e condiviso con altri utenti. L'utente riconosce e accetta che altri utenti possano scaricare questo file dal suo computer, e che in questo caso verrà usata la sua connessione a Internet. Se l'utente non desidera che questo accada, può eliminare il file o farvi clic con il pulsante destro del mouse e selezionare "Non condividere questo file".

4.4 Cartella miei condivisi. Quando l'utente salva un file nella Cartella miei condivisi, riconosce che esso sarà disponibile per qualsiasi altro utente di Kazaa Media Desktop e di programmi compatibili. Questi utenti possono trovare tali file, quindi



Accetto il [Contratto di licenza con l'utente finale di Kazaa Media Desktop](#) e i [Contratti di licenza con l'utente finale del pacchetto Altnet Peer Points Manager](#).

Annulla

Indietro

Avanti



[Informazioni importanti](#)

[Contratto di licenza con l'utente finale di Kazaa Media Desktop](#)

[Contratti di licenza con l'utente finale di Altnet Peer Points Manager e della barra di ricerca My Search](#)

[Versione stampabile](#)

Informazioni legali

Prima di eseguire il download e l'installazione di Kazaa Media Desktop occorre leggere e accettare il Contratto di licenza con l'utente finale di Kazaa Media Desktop e il Contratto di licenza con l'utente finale di Altnet Peer Points Manager.

4.5 Supernodo. La copia del Software dell'utente può servire come supernodo. Il processo di selezione è automatizzato. Quando il computer dell'utente è un supernodo, altri pari eseguono sul suo computer l'upload di un indice di file condivisi e inviano richieste di ricerca al suo computer. Il computer dell'utente risponde a queste richieste di ricerca e invia la richiesta ad altri supernodi.

Se l'utente non desidera che il computer funzioni come supernodo, andare a Strumenti > Opzioni > Avanzate e selezionare la casella "Non funzionare come supernodo". Quando il computer dell'utente funziona come supernodo, vengono utilizzate la sua CPU e la sua connessione a Internet, ma non oltre il 10% delle risorse.

Accetto il [Contratto di licenza con l'utente finale di Kazaa Media Desktop](#) e i [Contratti di licenza con l'utente finale del pacchetto Altnet Peer Points Manager](#).

Passaggio 2 di 6

Annulla

Indietro

Avanti

[Informazioni importanti](#)

[Contratto di licenza con l'utente finale di Kazaa Media Desktop](#)

[Contratti di licenza con l'utente finale di Altnet Peer Points Manager e della barra di ricerca My Search](#)

[Versione stampabile](#)

Informazioni legali

Prima di eseguire il download e l'installazione di Kazaa Media Desktop occorre leggere e accettare il Contratto di licenza con l'utente finale di Kazaa Media Desktop e il Contratto di licenza con l'utente finale di Altnet Peer Points Manager.

9 Software di terzi

9.1 Nel corso della procedura di installazione di Kazaa Media Desktop, l'utente **deve** installare software di terzi fornitori di software in base a licenze o altri contratti tra tali fornitori e l'utente ("Software di terzi"), inclusi a titolo esemplificativo i componenti software riportati nella Sezione 9.4 di seguito. Notare che il Software di terzi può essere soggetto a licenze diverse o altri accordi, che l'utente dovrà leggere con attenzione. Installando e utilizzando questo Software di terzi l'utente accetta queste licenze o questi accordi di terzi e dichiara di averli letti e compresi. Sharman non vende, non rivende e non concede in licenza alcun Software di terzi e declina nella massima misura consentita dalla legge applicabile qualunque responsabilità correlata a Software di terzi. Qualunque domanda, reclamo o richiesta relativa a Software di terzi dovrà essere diretta al fornitore appropriato.



Accetto il [Contratto di licenza con l'utente finale di Kazaa Media Desktop](#) e i [Contratti di licenza con l'utente finale del pacchetto Altnet Peer Points Manager](#).

Passaggio 2 di 6

Annulla

Indietro

Avanti



[Informazioni importanti](#)

[Contratto di licenza con l'utente finale di Kazaa Media Desktop](#)

[Contratti di licenza con l'utente finale di Altnet Peer Points Manager e alla barra di ricerca My Search](#)

[Versione stampabile](#)

Informazioni legali

Passaggio 2 di 6

Prima di eseguire il download e l'installazione di Kazaa Media Desktop occorre leggere e accettare il Contratto di licenza con l'utente finale di Kazaa Media Desktop e il Contratto di licenza con l'utente finale di Altnet Peer Points Manager.

9.2 Sharman non rilascia dichiarazioni o garanzie di alcun tipo relative alla qualità, sicurezza o adeguatezza di questo software, siano esse esplicite o implicite, incluse a titolo esemplificativo garanzie implicite di commerciabilità, idoneità per uno scopo specifico o non violazione di regole nella massima misura consentita dalla legge applicabile; Sharman non sarà in alcun caso responsabile di danni indiretti, punitivi, speciali, incidentali o consequenziali comunque possano verificarsi e anche se Sharman fosse stata informata della possibilità del verificarsi di tali danni.

9.3 L'uso di software scaricabile in Internet presenta rischi intrinseci e Sharman ammonisce l'utente di accertarsi di comprendere completamente i rischi potenziali prima di accettare di installare qualsiasi Software di terzi. L'utente è l'unico responsabile dell'adeguata protezione e dell'adeguato backup dei dati e delle apparecchiature utilizzate in relazione a Software di terzi e Sharman non è responsabile di alcun danno che l'utente potrebbe subire in relazione all'uso, alla modifica o alla distribuzione di Software di terzi



Accetto il [Contratto di licenza con l'utente finale di Kazaa Media Desktop](#) e i [Contratti di licenza con l'utente finale del pacchetto Altnet Peer Points Manager](#).

Annulla

Indietro

Avanti



[Informazioni importanti](#)

[Contratto di licenza con l'utente finale di Kazaa Media Desktop](#)

Contratti di licenza con utente finale di Altnet Peer Points Manager e della barra di ricerca My Search

[Versione stampabile](#)

Informazioni legali

Altnet Peer Points Manager permette di raccogliere punti caricando file contrassegnati dalle icone dorate. Prima di installare il software, occorre accettare questo contratto di licenza con l'utente finale.

applicazioni software.

3. Autorizzazione all'uso

Per ricevere i benefici offerti dal Software Altnet, con questo documento l'utente concede l'autorizzazione ad Altnet e/o ai Provider Altnet per utilizzare lo spazio su disco e l'ampiezza di banda del proprio computer per la condivisione dei file che ha scaricato usando la Rete. Il Software Altnet proteggerà la privacy e l'integrità delle risorse e dei file del computer dell'utente nella misura indicata nella Informativa sulla Privacy di Altnet, riportata all'indirizzo <http://www.altnet.com/privacy>.



Accetto il [Contratto di licenza con l'utente finale di Kazaa Media Desktop](#) e i [Contratti di licenza con l'utente finale di Altnet Peer Points Manager e della barra di ricerca My Search](#).

Passaggio 2 di 6



Annulla

Indietro

Avanti

Qualche software di terzi incorporato

- **Cydoor.** Il Software include un programma di invio di annunci pubblicitari di Cydoor Technologies che può visualizzare contenuto Web come avvisi in banner, offerte di e-commerce, titoli di notizie e altri contenuti a valore aggiunto. **Il componente Cydoor utilizza la connessione a Internet dell'utente per aggiornare la sua scelta di annunci e li memorizza sul disco rigido.**
- **Topsearch.** Il Software include il programma Topsearch fornito da Altnet. **Il componente Topsearch scarica regolarmente, attraverso la connessione a Internet dell'utente, l'indice dei contenuti.** Questo indice contiene l'elenco dei file con diritti gestiti disponibili che possono essere visualizzati nei risultati della ricerca.
- **GAIN.** Kazaa Media Desktop include un componente software denominato GAIN AdServer, fornito da GAIN Publishing. **Il software GAIN AdServer identifica gli interessi dell'utente in base a parte dell'utilizzo del computer e usa tali informazioni per inviare all'utente messaggi pubblicitari.** Questo software contribuisce a rendere possibile la distribuzione gratuita di Kazaa Media Desktop [...] Se l'utente desidera smettere di ricevere pubblicità attraverso GAIN AdServer, deve rimuovere tutto il software supportato da GAIN presente sul proprio computer, incluso Kazaa Media Desktop....

Altnet

- **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**

l'educazione degli utenti: serve ma non basta..

- **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**

mirroring

***Bisogna disporre di un apparato
che possa rendere disponibile
un efficace mirror di un profilo di traffico***

- **Deve essere ASIC (nessun impatto sulla CPU)**
- **Flessibilità di configurazione**
- **Possibilità di associare un profilo di mirroring ad una interfaccia e disponibilità di poter disporre di più profili su interfacce diverse**

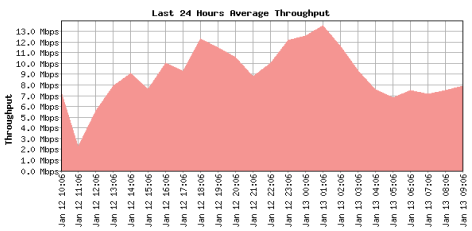
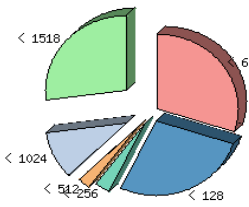
Port mirroring

Ptop
stefano suin & devide vagotti

List of First 10 ports, Traffic monitored since 5 minutes

| Port | Top Sent | Port | Top Rcvd | Port | Udp Sent | Port | Udp Rcvd |
|------|-------------------------|------|-------------------------|-------|-----------------------|-------|------------------------|
| 22 | 81.85M 2.389GBytes | 119 | 761.41M 20.989GBytes | 8829 | 2.05M 54.989GBytes | 3829 | 3.76M 102.889GBytes |
| 2446 | 78.34M 2.099GBytes | 2464 | 65.31M 1.799GBytes | 3209 | 1.81M 49.589GBytes | 2068 | 1.51M 41.189GBytes |
| 6701 | 68.87M 1.889GBytes | 22 | 24.42M 666.489GBytes | 2068 | 1.78M 46.889GBytes | 3762 | 718.4K 19.749GBytes |
| 407 | 42.01M 1.129GBytes | 7000 | 16.15M 441.389GBytes | 2446 | 1.76M 46.189GBytes | 2446 | 635.3K 16.989GBytes |
| 80 | 34.03M 929.149GBytes | 3550 | 14.54M 396.249GBytes | 1912 | 1.70M 46.289GBytes | 1834 | 811.3K 16.389GBytes |
| 7000 | 31.01M 846.789GBytes | 4666 | 7.70M 210.289GBytes | 3762 | 1.66M 43.289GBytes | 3209 | 565.0K 15.189GBytes |
| 8293 | 24.14M 659.249GBytes | 3552 | 2.23M 597.289GBytes | 1834 | 1.64M 44.889GBytes | 2484 | 479.0K 12.889GBytes |
| 2464 | 19.34M 523.249GBytes | 1595 | 7.23M 197.389GBytes | 2484 | 1.54M 41.889GBytes | 2634 | 414.9K 11.389GBytes |
| 3184 | 17.44M 467.249GBytes | 80 | 7.21M 197.289GBytes | 191 | 309.4K 8.389GBytes | 1912 | 348.0K 9.389GBytes |
| 4666 | 13.64M 372.489GBytes | 6701 | 7.14M 195.189GBytes | 19145 | 284.1K 7.889GBytes | 19145 | 220.8K 5.989GBytes |

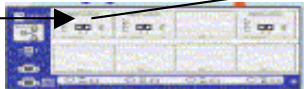
Ptop



Mirrored traffic



Public Link



| Host | Domain | IP Address | MAC Address | Other Name(s) | Sent Bandwidth | Nw Board Vendor |
|----------------------------|--------|----------------|-------------|---------------|----------------|-----------------|
| serra.unipi.it | | 131.114.21.10 | | | [Bar] | |
| hausdorff.ing.unipi.it | | 131.114.29.48 | | | [Bar] | |
| get.dsea.unipi.it | | 131.114.30.190 | | | [Bar] | |
| mercurio.iet.unipi.it | | 131.114.5.192 | | | [Bar] | |
| valentini.lsm.cci.unipi.it | | 131.114.28.129 | | | [Bar] | |
| 131.114.13.104 | | 131.114.13.104 | | | [Bar] | |
| croci.unipi.it | | 131.114.21.11 | | | [Bar] | |
| pasero.dst.unipi.it | | 131.114.12.47 | | | [Bar] | |
| luise.eth.iet.unipi.it | | 131.114.9.160 | | | [Bar] | |
| segreteria.cci.unipi.it | | 131.114.28.17 | | | [Bar] | |
| 131.114.21.131 | | 131.114.21.131 | | | [Bar] | |
| ares.cci.unipi.it | | 131.114.28.19 | | | [Bar] | |
| docent.ing.unipi.it | | 131.114.28.20 | | | [Bar] | |
| 131.114.21.133 | | 131.114.21.133 | | | [Bar] | |
| 131.114.28.22 | | 131.114.28.22 | | | [Bar] | |
| 131.114.21.135 | | 131.114.21.135 | | | [Bar] | |

Ntop: a deep traffic flows, sessions & protocol distribution using Port Mirroring

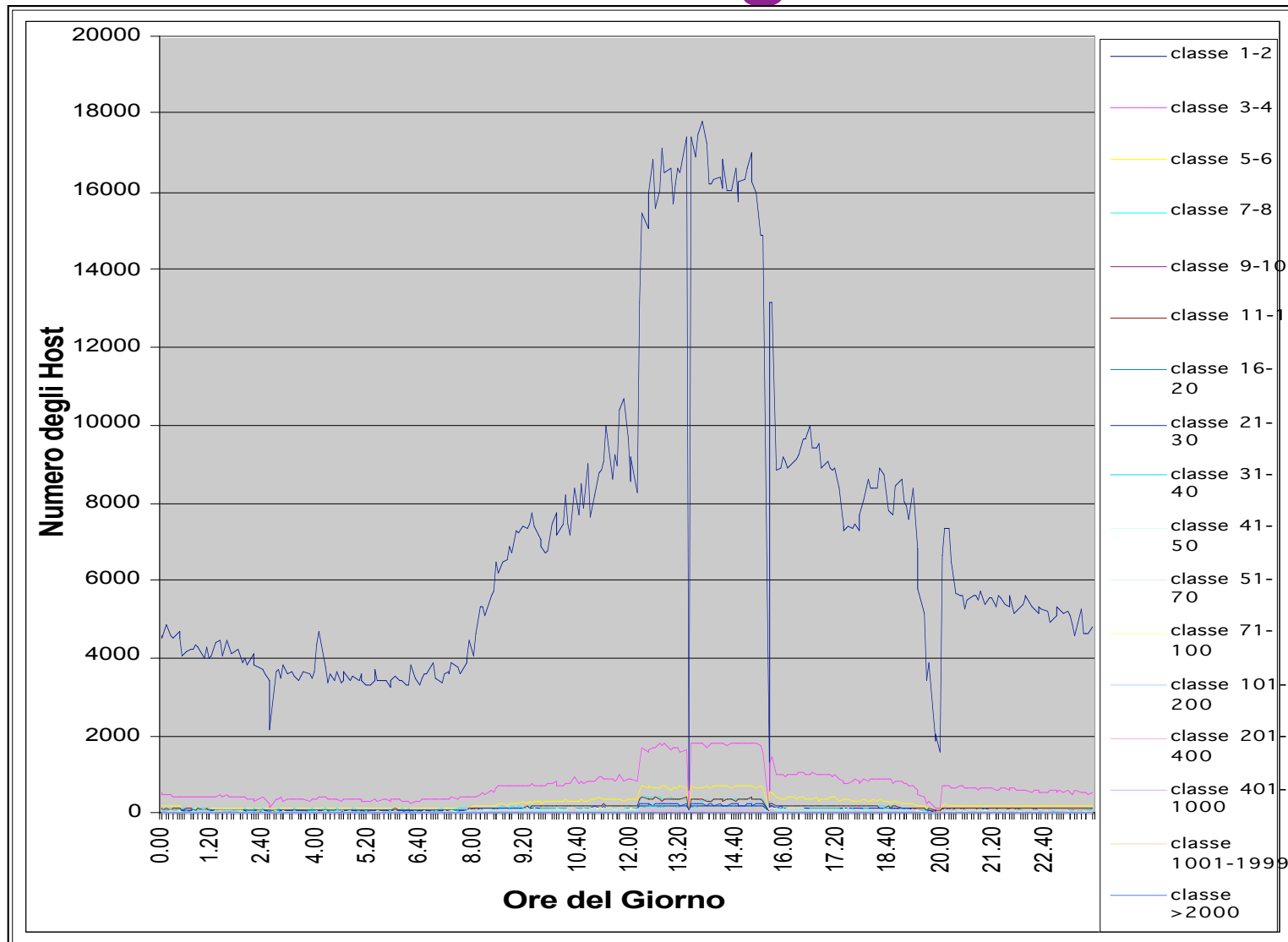
Fattori caratteristici (ineludibili)

- **Volume di traffico insolito**
 - Soprattutto in uscita
- **Numero Peering host**
 - Gli host contattati sono un numero elevato rispetto alla normale attività di consultazione
- **Port Traffic**
 - Matrici di traffico indipendenti dalle convenzioni (analisi di tutte le porte)

Fattori caratteristici

- **per ogni circuito esistono delle “fingerprint” di comportamento**
 - **es. traffici via web, con indicazione dei Super Node in modo numerico**
- **non esiste documentazione affidabile**
- **il database è difficile da manetenerne aggiornato**
- **bisogna mettere in conto la il numero di falsi positivi possa alzarsi significativamente**

Distribuzione gaussiana



Ptop

stefano suin & davide vaghetti

List of First 10 ports, Traffic monitored since 5 minutes

| Port | Tcp Sent | Port | Tcp Rcvd | Port | Udp Sent | Port | Udp Rcvd |
|---|-------------------------|---|--------------------------|--|-----------------------|--|------------------------|
| 22 host graph | 81.85M 2.18Mbit/sec | 119 host graph | 763.43M 20.36Mbit/sec | 3829 host graph | 2.05M 56.1Kbit/sec | 3829 host graph | 3.76M 102.8Kbit/sec |
| 2446 host graph | 78.34M 2.09Mbit/sec | 2464 host graph | 65.31M 1.74Mbit/sec | 3209 host graph | 1.81M 49.5Kbit/sec | 2068 host graph | 1.51M 41.1Kbit/sec |
| 6701 host graph | 68.97M 1.84Mbit/sec | 22 host graph | 24.42M 666.8Kbit/sec | 2068 host graph | 1.78M 48.6Kbit/sec | 3762 host graph | 718.4K 19.2Kbit/sec |
| 407 host graph | 42.01M 1.12Mbit/sec | 7000 host graph | 16.15M 441.0Kbit/sec | 2446 host graph | 1.76M 48.1Kbit/sec | 2446 host graph | 635.3K 16.9Kbit/sec |
| 80 host graph | 34.03M 929.1Kbit/sec | 3550 host graph | 14.54M 396.9Kbit/sec | 1912 host graph | 1.70M 46.3Kbit/sec | 1434 host graph | 611.1K 16.3Kbit/sec |
| 7000 host graph | 31.01M 846.7Kbit/sec | 4666 host graph | 7.70M 210.2Kbit/sec | 3762 host graph | 1.66M 45.2Kbit/sec | 3209 host graph | 565.0K 15.1Kbit/sec |
| 3293 host graph | 24.14M 659.2Kbit/sec | 3552 host graph | 7.23M 197.3Kbit/sec | 2634 host graph | 1.64M 44.9Kbit/sec | 2484 host graph | 479.0K 12.8Kbit/sec |
| 2464 host graph | 19.34M 528.2Kbit/sec | 1595 host graph | 7.23M 197.3Kbit/sec | 2484 host graph | 1.54M 42.0Kbit/sec | 2634 host graph | 414.9K 11.1Kbit/sec |
| 3184 host graph | 17.84M 487.2Kbit/sec | 80 host graph | 7.21M 197.0Kbit/sec | 53 host graph | 309.4K 8.3Kbit/sec | 1912 host graph | 348.0K 9.3Kbit/sec |
| 4666 host graph | 13.64M 372.4Kbit/sec | 6701 host graph | 7.14M 195.1Kbit/sec | 19145 host graph | 284.1K 7.6Kbit/sec | 19145 host graph | 220.6K 5.9Kbit/sec |

day hour minutes interval
 Limit to first ports Show ports

La banda su una porta è di solito associabile ad un solo host

Bytes Sent Host percent for Tcp 2446 port in last 5 minutes Total: 78.34M

| Host | Sniffers | Traffic | Percent | Bandwidth |
|--|------------------|---------|---------|--------------|
| 131.114.69.100.vet.unipi.it (131.114.69.100) | session analysys | 78.34M | 99% | 2.09Mbit/sec |
| 131.114.87.100.farm.unipi.it (131.114.87.100) | session analysys | 614 | 0% | 16bit/sec |
| 131.114.111.100.ing.unipi.it (131.114.111.100) | session analysys | 608 | 0% | 16bit/sec |
| 131.114.33.100.meta.cpr.it (131.114.33.100) | session analysys | 322 | 0% | 8bit/sec |

© PTOPI rel 0.98 - [S.Suin](#) [D.Vaghetti](#), 2003

Come si distribuisce il traffico sulla macchina?

Last 5 minutes connections for Host `131.114.69.114` (131.114.69.114)

| Port | Traffic | Percent | Bandwidth |
|------|---------|---------|--------------|
| 2446 | 78.34M | 99.98% | 2.09Mbit/sec |
| 80 | 5.9K | 0.01% | 161bit/sec |
| 4072 | 5.6K | 0.01% | 153bit/sec |
| 4070 | 3.6K | 0.00% | 98bit/sec |
| 4067 | 982 | 0.00% | 26bit/sec |
| 4079 | 725 | 0.00% | 19bit/sec |
| 4075 | 589 | 0.00% | 15bit/sec |
| 4078 | 583 | 0.00% | 15bit/sec |
| 4074 | 507 | 0.00% | 13bit/sec |
| 4077 | 463 | 0.00% | 12bit/sec |
| 4076 | 417 | 0.00% | 11bit/sec |

Ma quanti host mi contatti?

Actual Peering for host `131.114.69.114.vet.unipi.it(131.114.69.114)` on port 2446 (sender)

| Peering Host | Peering Port |
|-----------------|--------------|
| 130.239.130.113 | 1944 |
| 62.211.4.237 | 3590 |
| 131.111.231.35 | 1169 |
| 212.217.129.19 | 1831 |
| 80.117.31.36 | 1113 |
| 80.116.97.196 | 4033 |
| 82.37.0.31 | 1054 |
| 62.211.166.52 | 4022 |
| 212.171.30.93 | 1776 |
| 80.181.82.104 | 1834 |
| 213.239.82.124 | 1348 |
| 80.117.38.84 | 4331 |
| 80.213.217.122 | 1488 |
| 80.116.2.252 | 3211 |
| 81.8.217.36 | 3023 |
| 130.209.97.51 | 4228 |
| 81.152.134.164 | 2576 |
| 131.211.225.0 | 1353 |

Saranno tutti dei proxy?

Intervallo di 5 minuti

Interval

Min porte

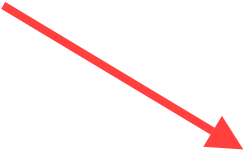
Min traffic

Resolution of hostnames

Ignore Ports 1-1024

Protocols

Output as .txt



| <i>IP</i> | <i>Porte</i> | <i>Traffico</i> |
|-----------------------------|--------------|-----------------|
| 131.81.64 | 23 | 58.01M |
| 131.53.47 | 125 | 18.12M |
| 131.48.210 | 36 | 100.8K |
| 131.9.63 | 186 | 296.8K |
| 131.28.23 | 148 | 195.6K |
| 131.20.25 | 108 | 1.28M |
| 131.188.198 | 35 | 136.0K |
| 131.53.124 | 56 | 6.33M |
| 131.79.188 | 121 | 302.1K |
| 131.29.25 | 367 | 229.9K |
| 131.49.209 | 611 | 622.9K |
| 131.28.81 | 53 | 1.63M |
| 131.49.5 | 20 | 181.4K |
| 131.130.10 | 65 | 658.4K |
| 131.69.43 | 76 | 329.6K |
| 131.69.232 | 68 | 1.50M |
| 131.40.29 | 24 | 103.1K |
| 131.69.44 | 33 | 168.5K |
| 131.72.73 | 24 | 120.6K |
| 131.79.184 | 71 | 1.02M |

Session detail

| TCP Connections | | Directed to | | Rcvd From |
|--------------------|-----------|--|------------|--|
| Attempted | 46 | <ul style="list-style-type: none"> • host251-202.pool80117.interbusiness.it 🍺 • host153-11.pool80117.interbusiness.it • host174-35.pool80116.interbusiness.it • host15-254.pool80117.interbusiness.it • ppp-217-133-219-232.dialup.tiscali.it 🍺 • host234-228.pool80117.interbusiness.it • r-ts016-5b171.tin.it 🍺 • ppp-217-133-246-87.dialup.tiscali.it 🍺 | 248 | <ul style="list-style-type: none"> • host244-82.pool80116.interbusiness.it 🍺 • host95-37.pool21345.interbusiness.it 🍺 • host73-20.pool80180.interbusiness.it • host237-122.pool80207.interbusiness.it 🍺 • 150.146.150.201 🍺 • r-pd037-8b136.tin.it 🍺 • adsl-62-123-58-110.dial.ipervia.it 🍺 • r-ts016-5b136.tin.it 🍺 |
| Established | 20 [43 %] | <ul style="list-style-type: none"> • host54-232.pool80117.interbusiness.it 🍺 • host251-202.pool80117.interbusiness.it 🍺 • host15-254.pool80117.interbusiness.it • host174-35.pool80116.interbusiness.it • ppp-217-133-219-232.dialup.tiscali.it 🍺 • host234-228.pool80117.interbusiness.it 🍺 • r-ts016-5b171.tin.it 🍺 • ppp-217-133-246-87.dialup.tiscali.it 🍺 | 207 [83 %] | <ul style="list-style-type: none"> • host244-82.pool80116.interbusiness.it 🍺 • host73-20.pool80180.interbusiness.it • host237-122.pool80207.interbusiness.it 🍺 • host95-37.pool21345.interbusiness.it 🍺 • 150.146.150.201 🍺 • r-pd037-8b136.tin.it 🍺 • adsl-62-123-58-110.dial.ipervia.it 🍺 • r-ts016-5b136.tin.it 🍺 |
| Terminated | 7 | <ul style="list-style-type: none"> • host5-193.pool212171.interbusiness.it • host153-11.pool80117.interbusiness.it | 38 | <ul style="list-style-type: none"> • ppp-217-133-219-232.dialup.tiscali.it 🍺 • 139.128.168.2 • r-ts016-5b136.tin.it 🍺 • ppp-217-133-237-219.dialup.tiscali.it 🍺 • host163-126.pool21758.interbusiness.it 🍺 • host54-232.pool80117.interbusiness.it 🍺 • host237-122.pool80207.interbusiness.it 🍺 |

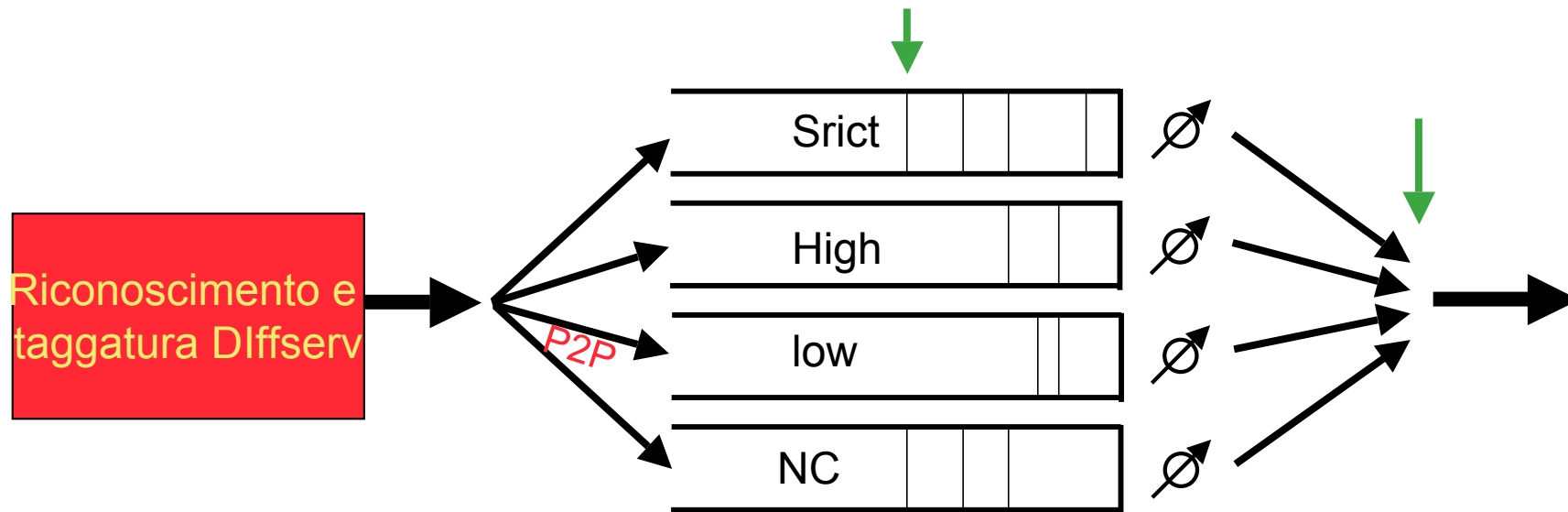
Chi usa la banda?

NETWORK TRAFFIC: Total Data (Sent+Received)

| Host | Domain | Data | TCP | UDP | ICMP | DLC | IPX | Decnet | (R)ARP | AppleTalk | OSPF | NetBios | IGMP | OSI | IPv6 |
|---------------------|--------|----------------|----------|----------|----------|-----|-----|--------|--------|-----------|------|---------|------|-----|------|
| newsserver.unipi.it | 🇮🇹 | 1.6 GB 11.4 % | 1.6 GB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193.206.140.66 | | 1.6 GB 11.4 % | 1.6 GB | 1.2 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.96.253 | | 338.6 MB 2.3 % | 338.3 MB | 214.5 KB | 40.6 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.13.45 | | 326.3 MB 2.2 % | 320.9 MB | 4.9 MB | 228.7 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193.205.80.236 | | 246.4 MB 1.7 % | 246.4 MB | 4.1 KB | 224 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| [REDACTED].unipi.it | 🇮🇹 | 199.7 MB 1.4 % | 198.0 MB | 1.6 MB | 58.0 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.87.153 | | 196.2 MB 1.4 % | 196.2 MB | 6.2 KB | 280 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.48.128 | | 185.6 MB 1.3 % | 185.6 MB | 1.1 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.2.41 | | 173.5 MB 1.2 % | 173.5 MB | 804 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.20.44 | | 172.9 MB 1.2 % | 172.9 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.9.160 | | 169.7 MB 1.2 % | 169.7 MB | 6.5 KB | 56 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 192.167.207.130 | | 159.0 MB 1.1 % | 159.0 MB | 29.3 KB | 972 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.9.114 | | 149.9 MB 1.0 % | 149.7 MB | 171.1 KB | 7.5 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 66.65.33.240 | | 142.5 MB 1.0 % | 142.5 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.5.192 | | 119.3 MB 0.8 % | 119.3 MB | 9.9 KB | 522 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 217.211.125.182 | | 104.8 MB 0.7 % | 104.8 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 217.121.48.188 | | 101.0 MB 0.7 % | 101.0 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.11.52 | | 99.9 MB 0.7 % | 99.9 MB | 27.0 KB | 728 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.40.135 | | 97.4 MB 0.7 % | 97.4 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 64.215.213.239 | | 95.9 MB 0.7 % | 95.9 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.31.232 | | 92.4 MB 0.6 % | 92.3 MB | 84.4 KB | 3.4 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.188.94 | | 85.2 MB 0.6 % | 85.2 MB | 468 | 168 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 213.113.202.103 | | 83.1 MB 0.6 % | 83.1 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.4.241 | | 82.2 MB 0.6 % | 82.2 MB | 2.0 KB | 2.9 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 130.94.70.241 | | 79.3 MB 0.5 % | 79.3 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 80.117.108.161 | | 79.0 MB 0.5 % | 79.0 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.27.153 | | 76.2 MB 0.5 % | 76.2 MB | 9.5 KB | 1.5 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 216.40.230.7 | | 74.8 MB 0.5 % | 74.8 MB | 1012 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193.205.82.103 | | 74.5 MB 0.5 % | 74.5 MB | 4.9 KB | 4.0 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 205.251.209.64 | | 74.3 MB 0.5 % | 74.3 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.30.135 | | 74.3 MB 0.5 % | 73.7 MB | 543.9 KB | 24.0 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193.205.82.100 | | 72.7 MB 0.5 % | 72.6 MB | 58.8 KB | 3.0 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 213.67.23.217 | | 63.7 MB 0.4 % | 63.7 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 62.94.0.11 | | 63.6 MB 0.4 % | 63.6 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.17.2 | | 62.6 MB 0.4 % | 62.6 MB | 96.3 KB | 168 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 131.114.12.47 | | 62.0 MB 0.4 % | 62.0 MB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193.205.82.98 | | 60.6 MB 0.4 % | 60.5 MB | 7.8 KB | 40.0 KB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Trattamento dei traffici individuati (proactive action)

quando il numero dei falsi positivi è basso



trattamento attraverso code di prioritá'

CONCLUSIONI

- **E' probabile che i controlli euristici siano l'unico strumento di rilevazione perseguibile**
- **Gli stessi firewall riescono difficilmente ad arginare il fenomeno (traffico interamente su porte client)**
- **Si lavora quindi sulla rilevazione delle anomalie di traffico, sia in termini di volume che in termini di numero di sessioni, che comunque il downstream provoca**