GIUSEPPE AUGIERO

COME MONITORARE IL TRAFFICO DI RETE IN UNA RETE MEDIO/GRANDE

IL NETWORK

Da cosa è composto (controllo verticale)

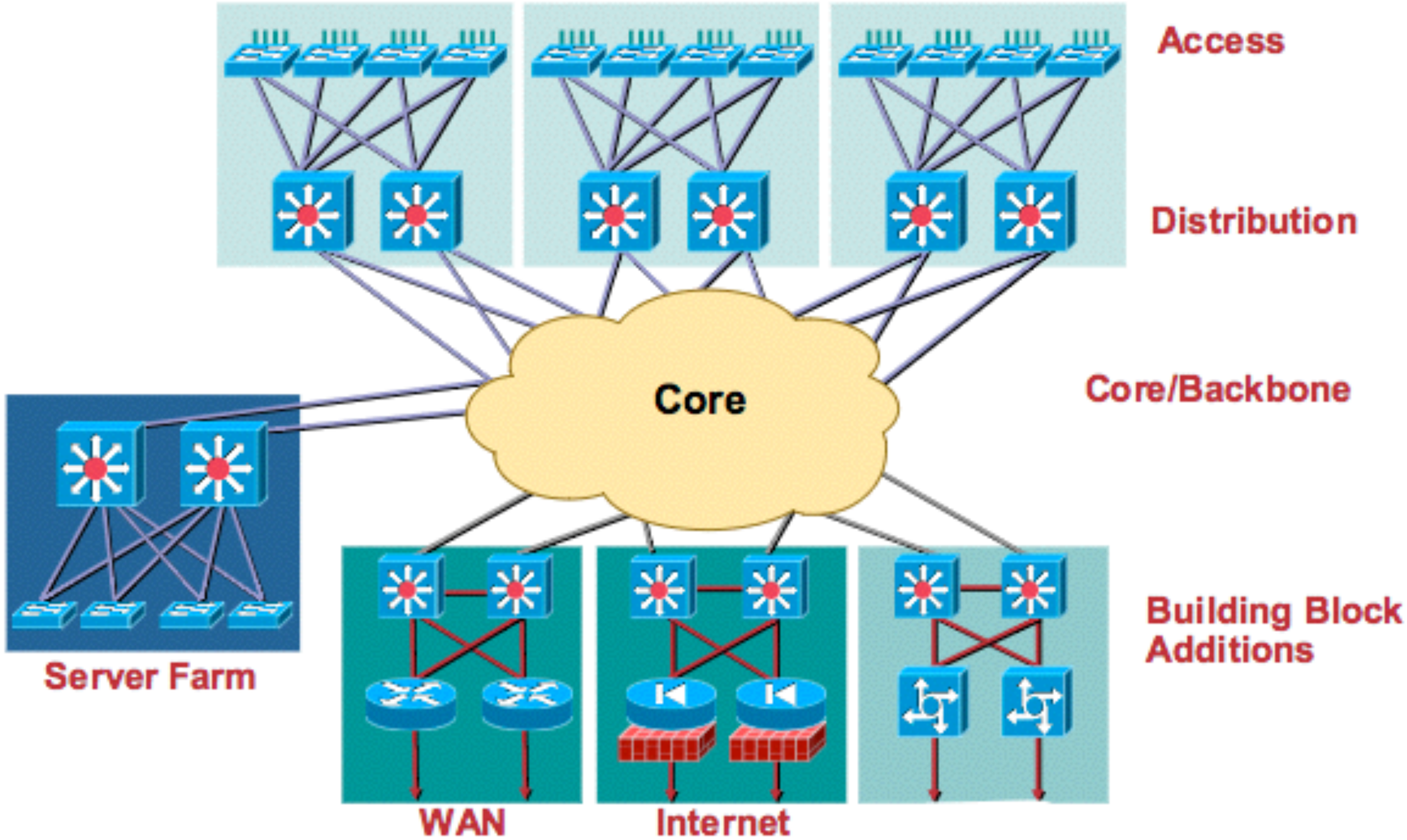
- Insieme di apparati L2/L3 che vanno a comporre i tre livelli canonici di una rete (**accesso, distribuzione, core**).
- Apparati L3/L4 per filtrare il traffico e fare deep inspection.
- Insieme di server che erogano servizi di rete (Dhcp, Radius, Sistemi di analisi, Sistemi di monitoraggio).
- Il network può essere composto da elementi che vanno a definire la **rete locale** e quella **geografica**.

IL NETWORK

Da cosa è composto (II)

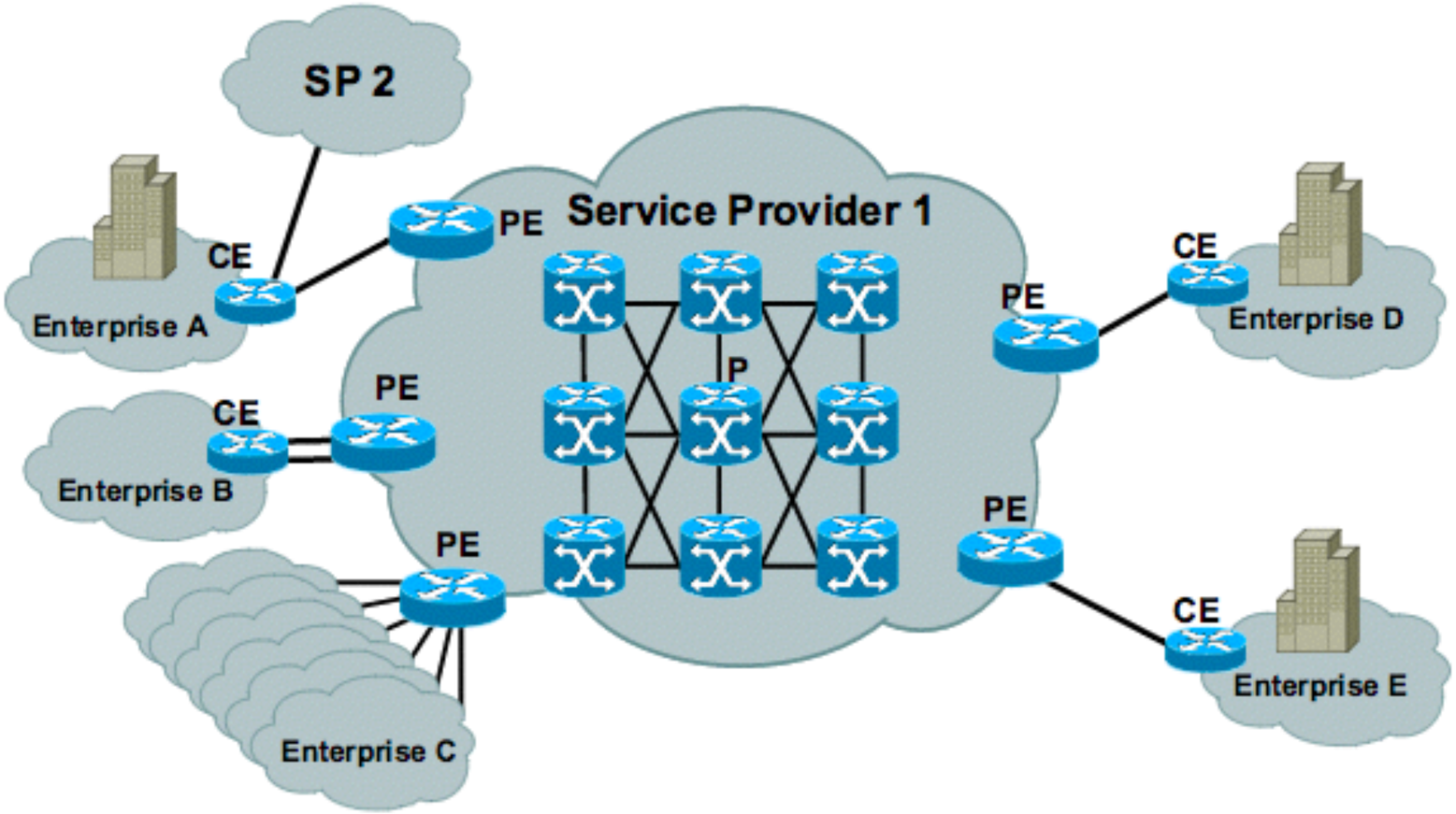
- La rete può essere:
  - fisica o virtualizzata.
- Può essere definita attraverso **SDN**.
- Sempre più spesso occorre gestire il **BYOD**.
- Internet of thing (**IOT**).
- Aumento della complessità della rete che porta a un troubleshooting che richiede maggiore esperienza.

IL NETWORK


Access
Distribution
Core
Core/Backbone
Server Farm
Building Block
Additions
WAN
Internet

IL NETWORK

ISP Network



IL NETWORK

Convergenza

- Al giorno d'oggi una rete dati medio/grande è un **sistema convergente** che trasporta diversi protocolli al fine di erogare molteplici servizi.
- Ad esempio: Voip, FCoE, IpTv - (Telemetria, Dicom, Chiamata, Allarmistica).
- Lo scopo è ridurre i costi, evitare inutili duplicazioni di servizi, avere una maggiore efficienza operativa, potenziamento dei servizi, affidabilità e protezione…

IL NETWORK

Alcune considerazioni

- Le attività che eseguiamo e i nostri dati sono spesso lontani da noi e richiedono l'uso della rete e di Internet per arrivare "a destinazione".
- Le risorse di rete sono, in ogni caso, finite (cardinalità).
- **La rete è come l'ossigeno**, si capisce l'importanza solo quando viene a mancare.
- Il grado di affidabilità deve essere alto.
- Essere un passo avanti rispetto alle richieste degli utenti.

KISS

NETWORK MANAGEMENT

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

NETWORK MANAGEMENT

Cosa si intende

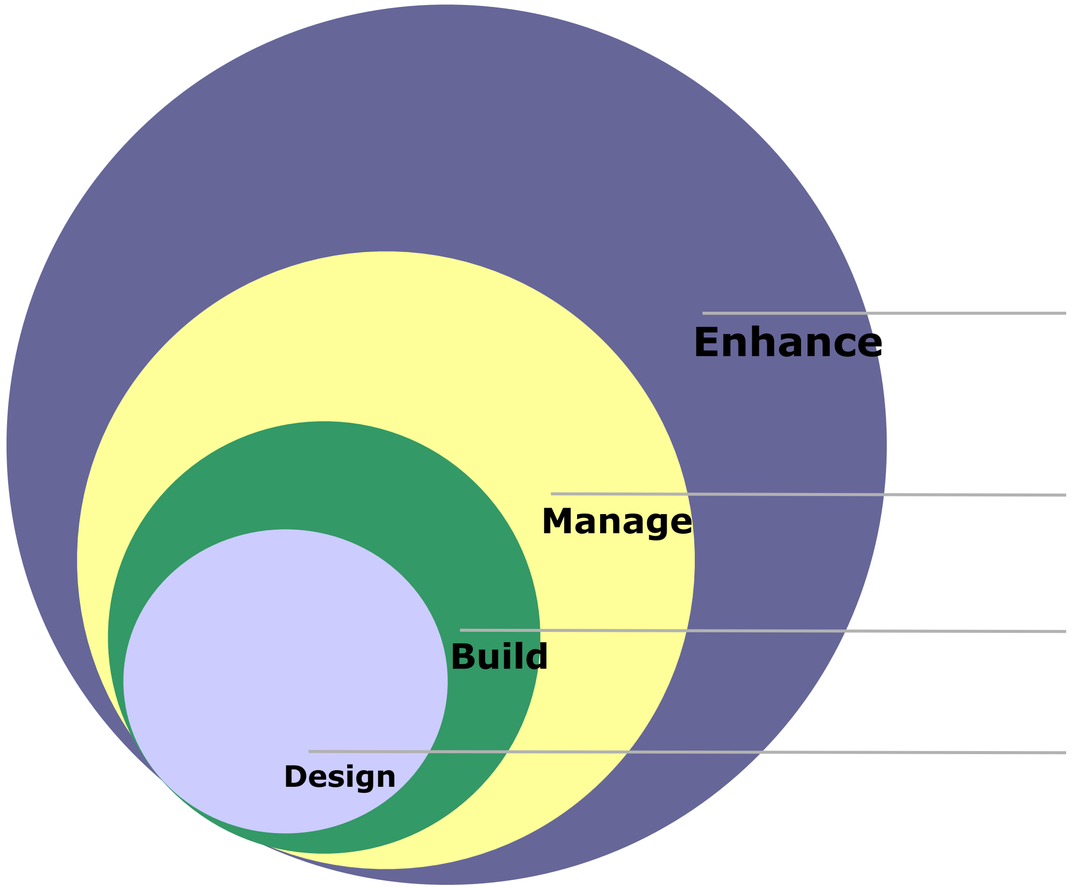
- L'attività di network management è il processo di controllo di una rete di dati al fine di massimizzare l'efficienza e la produttività.
- Consiste nell'attività di **monitorare** e **controllare** le risorse di rete.
- Dovremmo avere, sempre, la necessità di effettuare management al fine di capire cosa succede sulla nostra rete.
- Effettuare misure per capire lo **stato di salute** del network.

NETWORK MANAGEMENT

Processo interattivo

- Il management fa parte di un processo molto più grande che parte del design del network.
  - Tra le altre cose dovrebbe permettere di fornire informazioni utili per apportare correzioni a quanto progettato o che nel tempo è evoluto.

NETWORK MANAGEMENT



NETWORK MANAGEMENT

Esigenze

- Attraverso il network management è possibile:
  - conoscere gli errori di trasmissione.
  - effettuare misure.
  - capire cosa succede.
  - conoscere lo stato della rete.

NETWORK MANAGEMENT

ISO

- La ISO Network management forum divide il network management in cinque aree funzionali:
  - Gestione dei fault.
  - Gestione delle configurazioni.
  - Security.
  - Performance.
  - Accounting.

NETWORK MANAGEMENT

Fault Management

- E’ il processo per localizzare problemi o fault sul network.
- E’ composto dai seguenti step:
  - Ricerca del problema.
  - Isolamento del problema.
  - Risoluzione del problema.

NETWORK MANAGEMENT

Configuration Management

- La diversa o errata configurazione di alcuni dispositivi di rete può variare il comportamento del network.
- La gestione della configurazione è il processo che permette di creare e gestire la configurazione di questi dispositivi critici.

NETWORK MANAGEMENT

Security Management

- È il processo che controlla l'accesso alle informazioni sulla rete di dati.
- Fornisce un modo per monitorare i punti di accesso e registra informazioni su base periodica.
- Fornisce audit trail e allarmi per violazioni della sicurezza.

NETWORK MANAGEMENT

Performance Management

- Offre le misure delle prestazioni dell'hardware di rete, del software e dei media.
- Possibili misure possono essere:
  - Throughput complessivo.
  - Percentuale di utilizzo.
  - Tassi di errore.
  - Tempi di risposta.

NETWORK MANAGEMENT

Accounting Management

- Monitora l'utilizzo dei singoli utenti nell'utilizzo della rete al fine di garantire che gli utenti dispongano di risorse sufficienti (secondo SLA).
- Coinvolge il sistema che concede o rimuove il permesso per l'accesso alla rete.

LE MISURE

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

LE MISURE

Misure

- E’ chiaro che per effettuare un controllo del network o il monitoraggio occorre effettuare continue misure.
- Basta un semplice ping per capire se tutto va bene?
- Avete definito una corretta metodica per effettuare il monitoraggio?

LE MISURE

Misure (II)

- Sapete cosa sta succedendo sulla vostra rete?
- Conoscete lo stato di “salute” del vostro network?
- Le informazioni che raccogliete sono corrette?
- Riuscite a misure e monitorare tutto quello che vorreste?

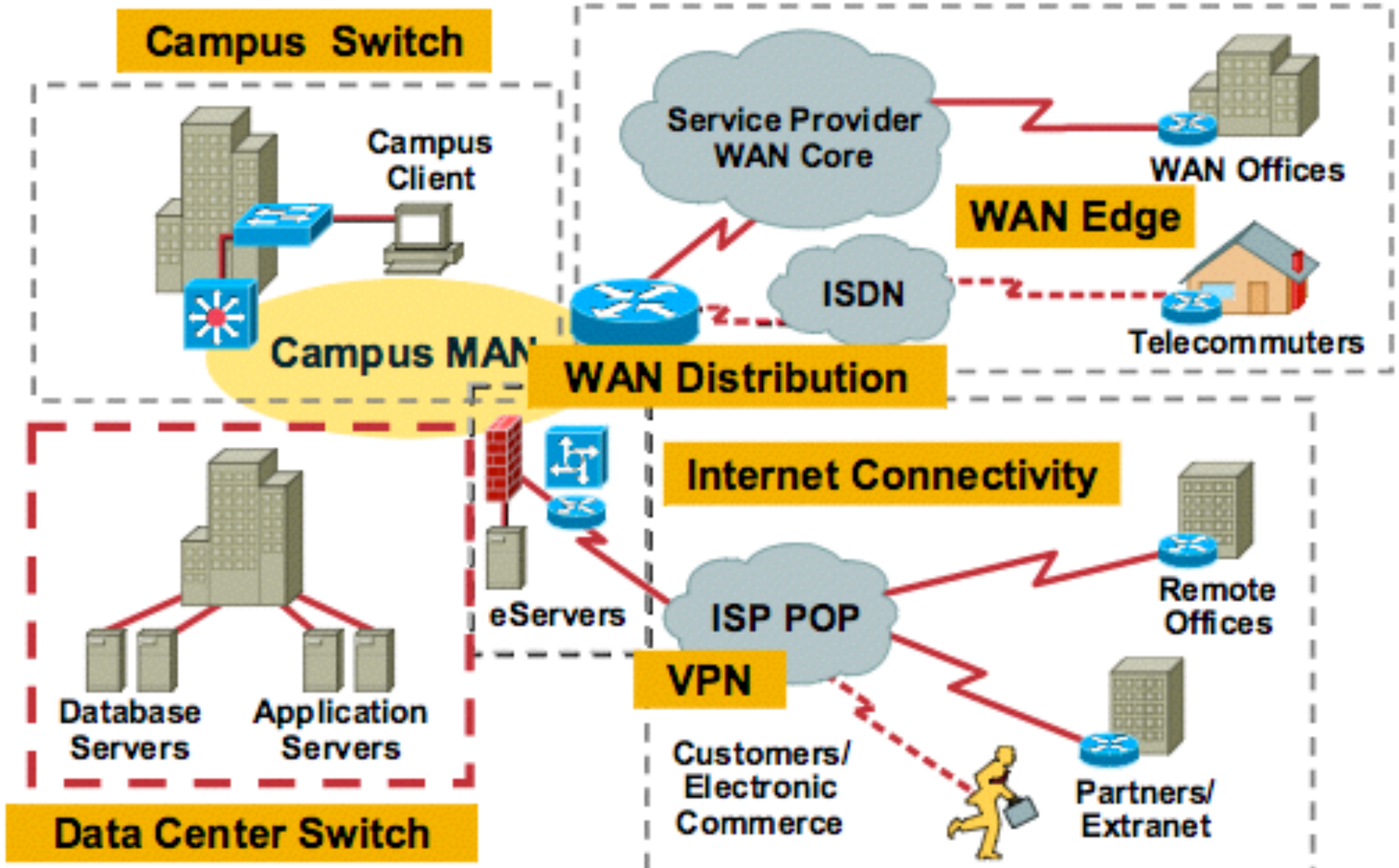
LE MISURE

Misure (III)

- Occorre definire un metodo.
- Definire gli obiettivi di business (e vederli come delle metriche).
- Tenere traccia delle failure e delle relative cause.
- Agire per risolvere la causa principale (dovrebbe essere ovvio).

LE MISURE

Metriche



LE MISURE

Metodologie di misura

- Ping (per sapere se la rete o il device è funzionante).
- Agent sui device.
- Trouble ticket reporting (DPM, IUM).
- Sonde.
- Richieste applicative.

LE MISURE

SNMP

- Protocollo vendor-indipendent che permette l'estrazione dal network di informazioni riguardanti lo stato operativo della rete.
- SNMP risolve tutti i problemi?

LE MISURE

Traffico di rete

- Se vogliamo catturare il traffico di rete per poi analizzarlo (magari per scopi di sicurezza), abbiamo bisogno di non perdere nemmeno un pacchetto.

- Il Futuro della sicurezza di basa sull'**analisi delle anomalie**.

LE MISURE

Computo

- Ogni volta che effettuerete una misura o un monitoraggio richiederete, di fatto, al vostro switch o al vostro router o a un vostro server, potenza di calcolo e tempo macchina per avere la risposta.
- Ogni misura ha un peso dal punto di vista computazionale.
- Overhead che non possiamo trascurare.

LE MISURE

Visione periferia

- Effettuare misure in maniera centralizzata non è una buona soluzione.
- E' fondamentale avere una visione completa del proprio network.
- Solo in questa maniera è possibile effettuare un buon troubleshooting.
- Valorizzare la periferia.

LE MISURE

Necessità di probe

- Attraverso dei probe, installati in punti diversi della rete, è possibile effettuare misure puntuali e catturare il traffico di rete che passa in un determinato punto.
- Maggiori informazioni sono in nostro possesso e più preciso sarà il monitoraggio che effettuiamo.

LE MISURE

Rottura dei vecchi paradigmi.

- L'analisi dei flussi non basta più per capire cosa succede sul network.
- Occorre continuare a caratterizzare il traffico di rete:
  - analizzando il livello applicativo.
  - performance vs velocità del link di rete.
  - posizionando il probe nel punto giusto della rete.

LE MISURE

Analisi del ritardo.

- Il ritardo associato a ogni link è composto da quattro componenti:
  - Processing Delay.
  - Queueing Delay.
  - Transmission Delay.
  - Propagation Delay.

LE MISURE

Correlazione

- E’ necessario effettuare, al fine di effettuare un buon monitoraggio, la correlazione di eventi.
- La somma (e l’analisi) di attività atomiche di poco conto (**mice**) possono portare alla luce gravi problemi di rete o situazioni anomale.
- Per esempio: Slow Dos.

LA RETE NELLA RETE

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

LA RETE NELLA RETE

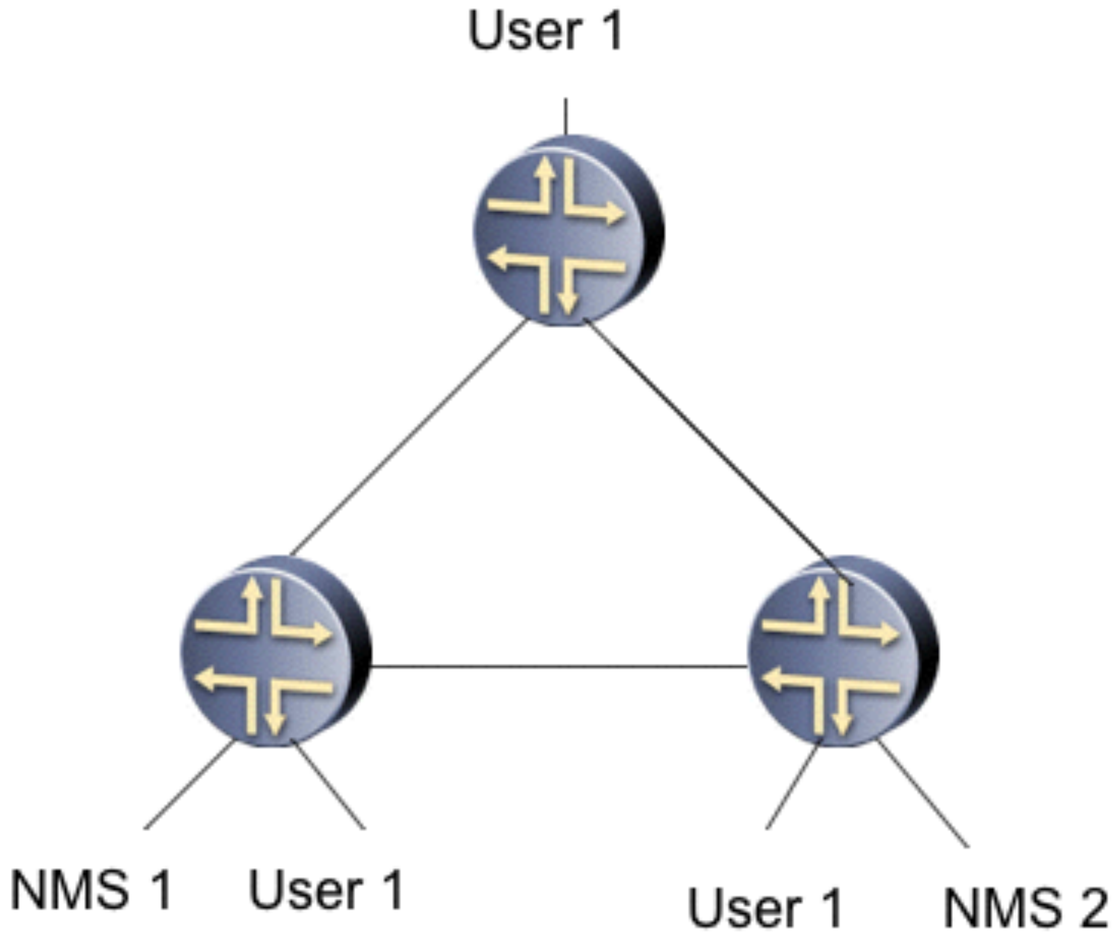
Monitoraggio

- Come effettuare il monitoraggio della rete?
- L'attività che vado ad effettuare ha un impatto sulla rete?

- Tre possibili scenari.

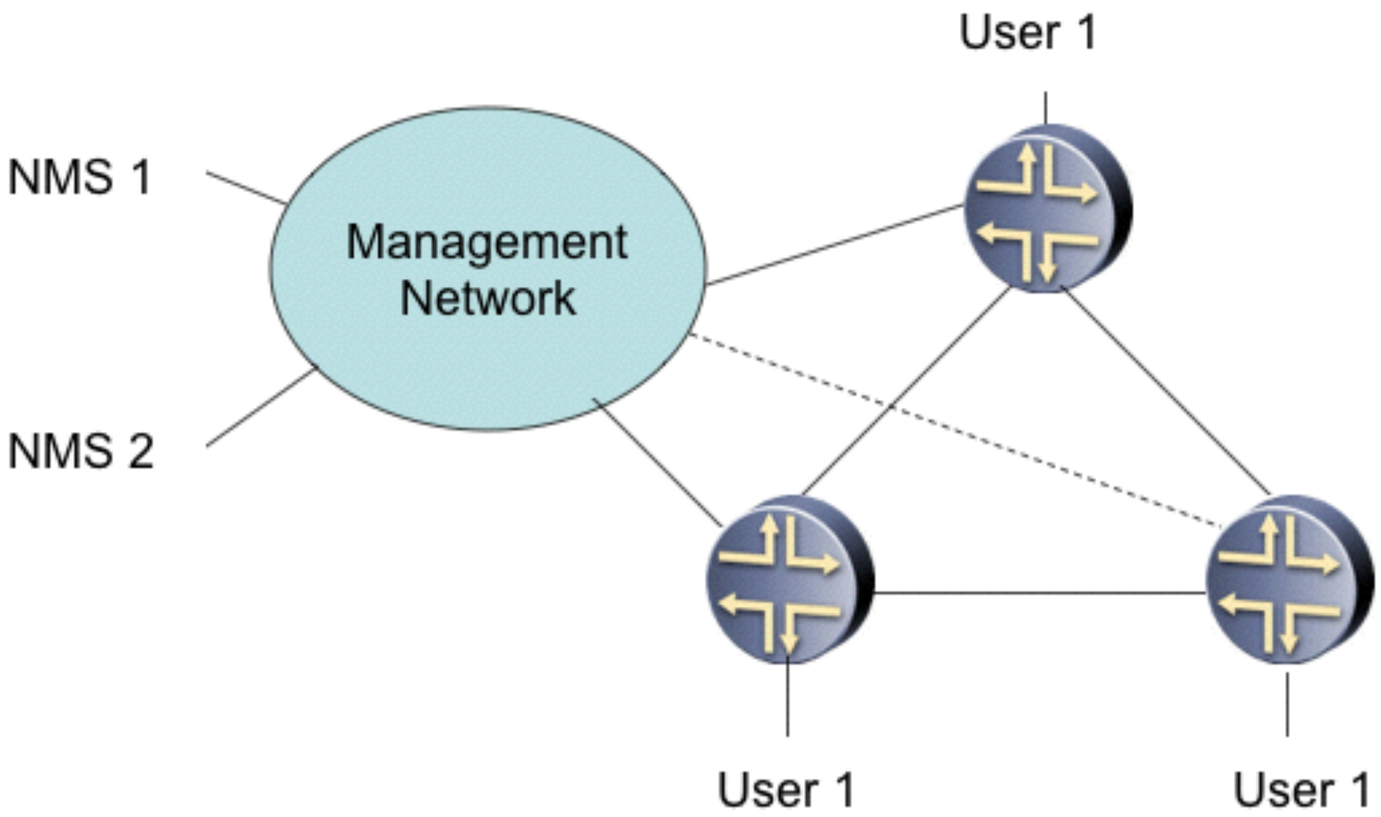
LA RETE NELLA RETE

InBound



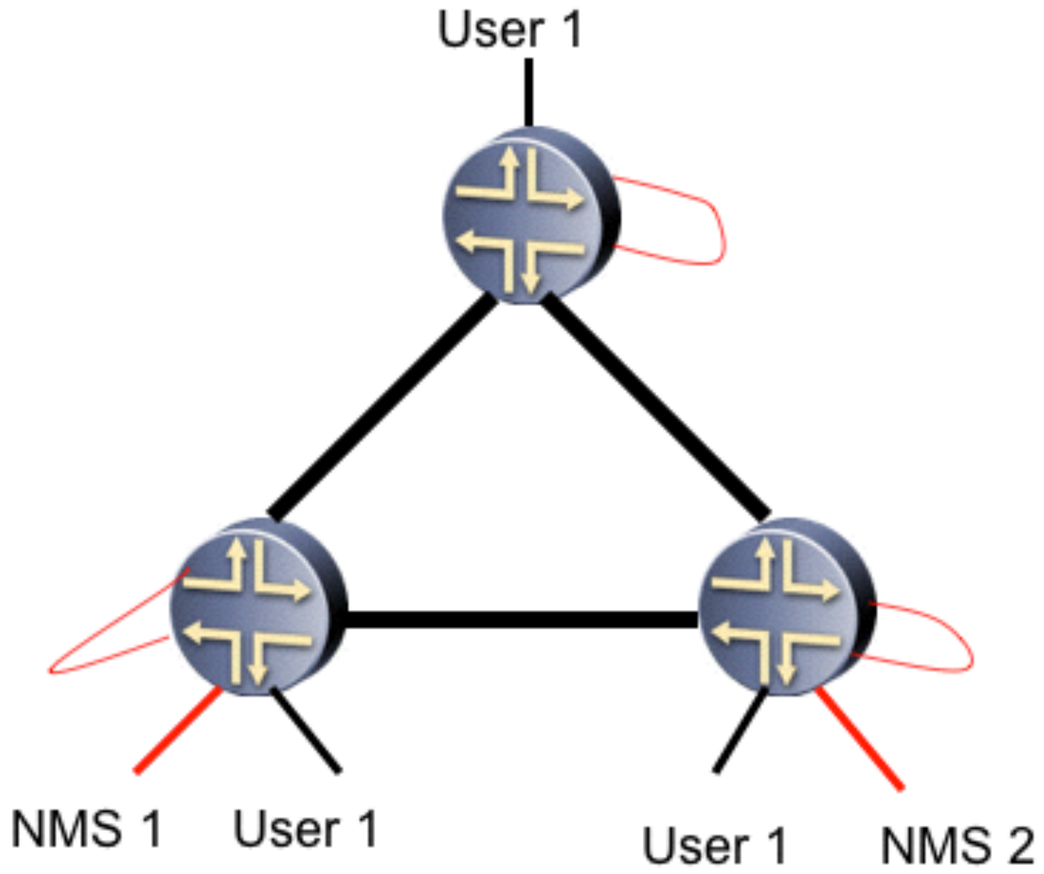
LA RETE NELLA RETE

OutBound



LA RETE NELLA RETE

Virtual outbound



LA RETE NELLA RETE

Differenze

- **Inbound:**
  - Espone la rete di management agli utenti.
  - La banda è condivisa tra utenti e NMS.
- **Outbound:**
  - La rete di NMS è isolata rispetto agli utenti.
  - NMS non condivide la banda con gli utenti.

Differenze (II)

- **Virtual Outbound**
  - La rete di NMS è isolata rispetto agli utenti.
  - La banda è condivisa tra utenti e NMS.

LA RETE NELLA RETE

I consigli della nonna

- Organizzazione.
- No routing.
- Impiego (se possibile) di una lambda ad hoc.
- Utilizzo di Drac/Ilom.
- Due Firmware a bordo degli apparati L2/L3.
- Attenzione ai virtual chassis.
- Porta di management sempre libera.

IL SOFTWARE

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

IL SOFTWARE

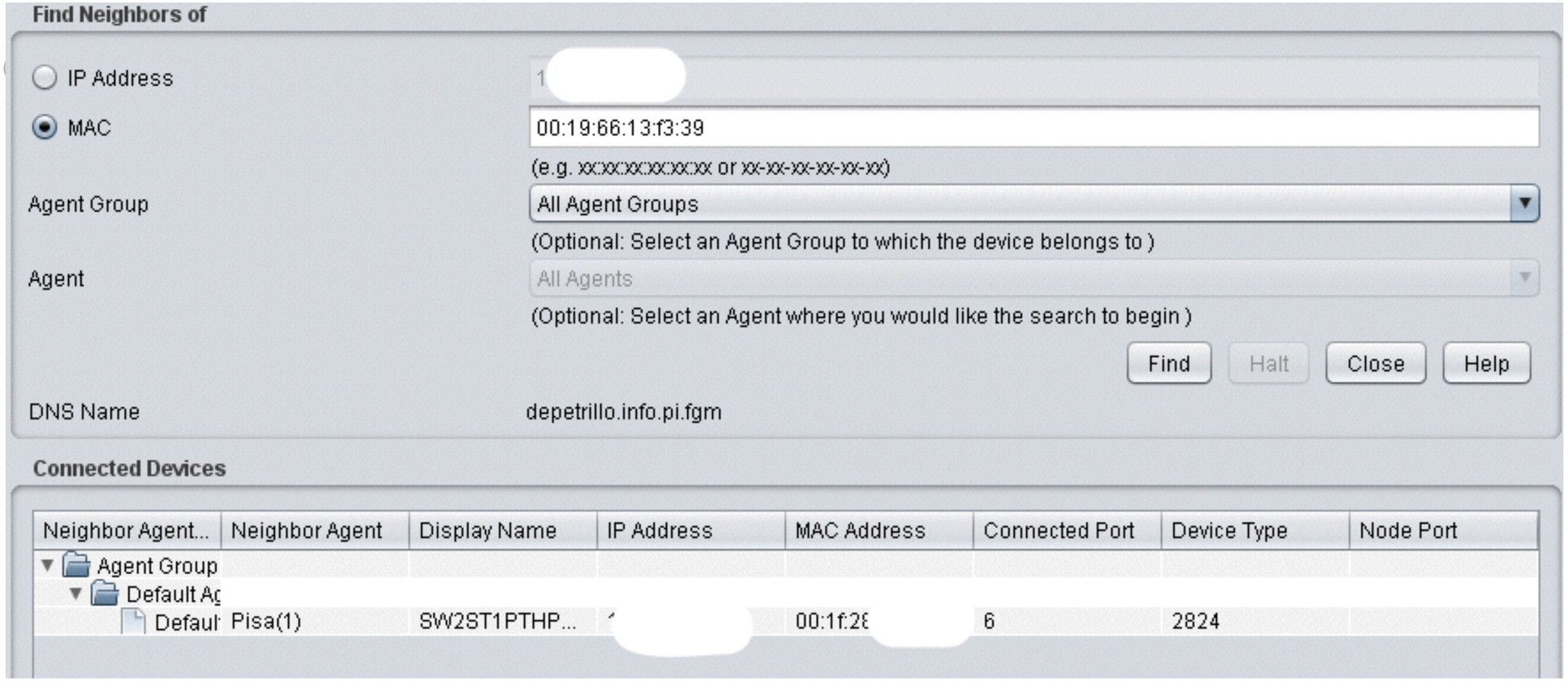
NMS centralizzato

- Non esiste un unico prodotto software che soddisfi tutte le esigenze di monitoraggio di rete.
- Ogni singolo prodotto di management svolge in maniera efficiente un singola operazione.
- E' necessario identificare cosa vi occorre per gestire la vostra rete.

Spanning tree

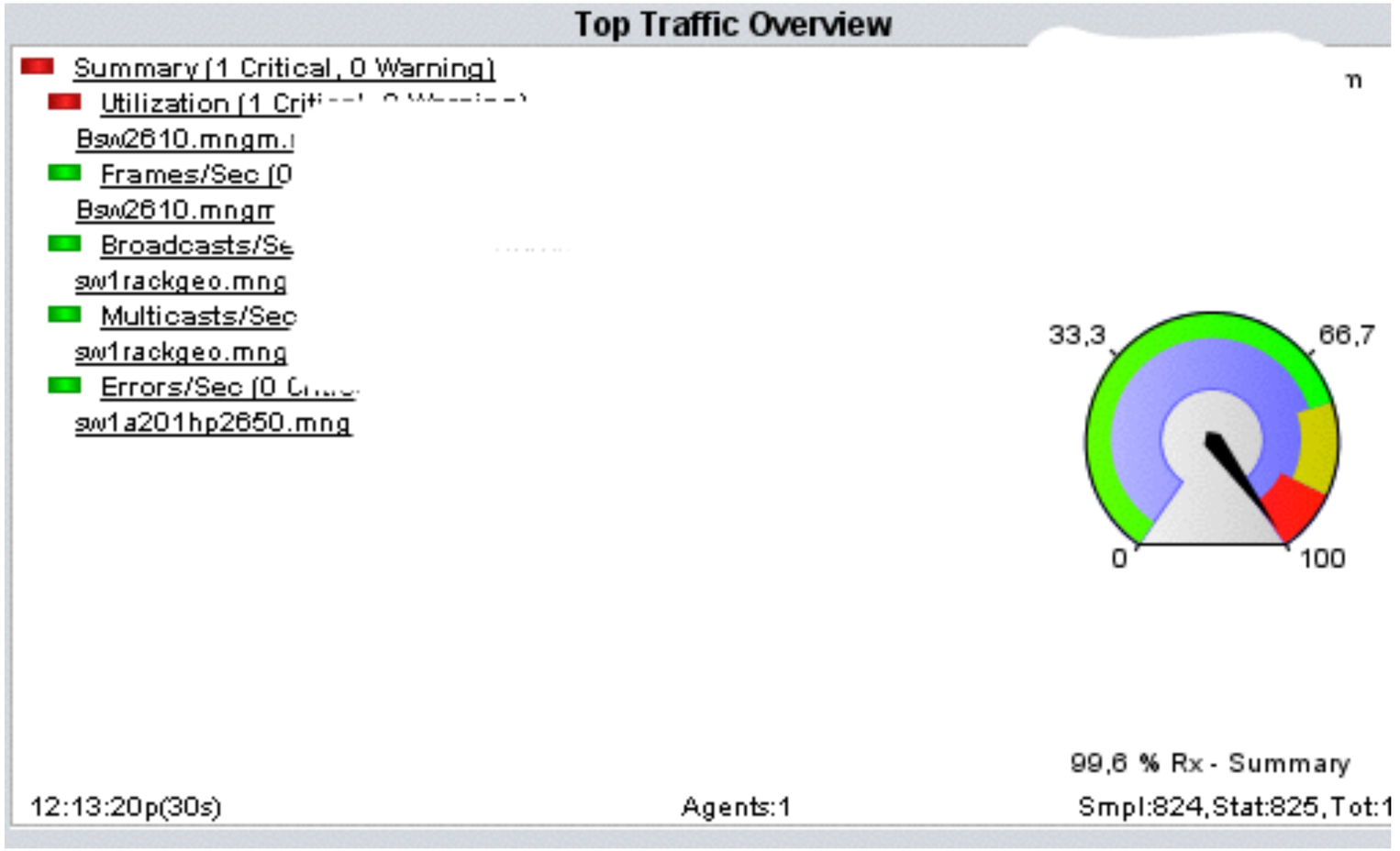
IL SOFTWARE

Mac find



IL SOFTWARE

Traffic Load



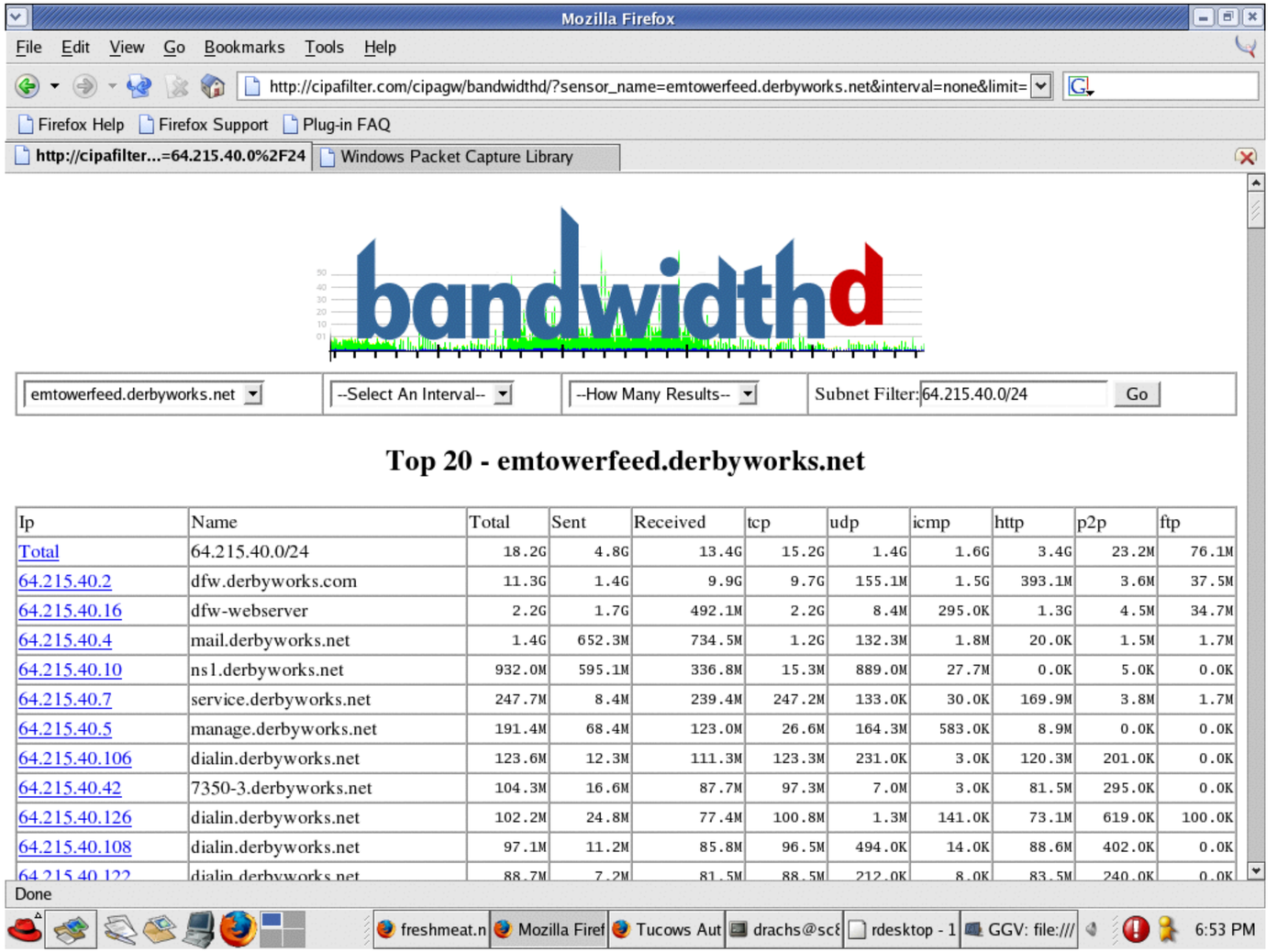
IL SOFTWARE

Arpwatch

```
      hostname: axis-disimpegno
    ip address: 172.16.1.104
     interface: vlan2
ethernet address: 00:40:8c:f1:66:e4
 ethernet vendor: AXIS COMMUNICATIONS AB
old ethernet address: 00:40:8c:a1:19:18
old ethernet vendor: AXIS COMMUNICATIONS AB
      timestamp: Tuesday, February 2, 2016 14:08:32 +0100
previous timestamp: Monday, February 1, 2016 20:01:33 +0100
      delta: 18 hours
```

IL SOFTWARE

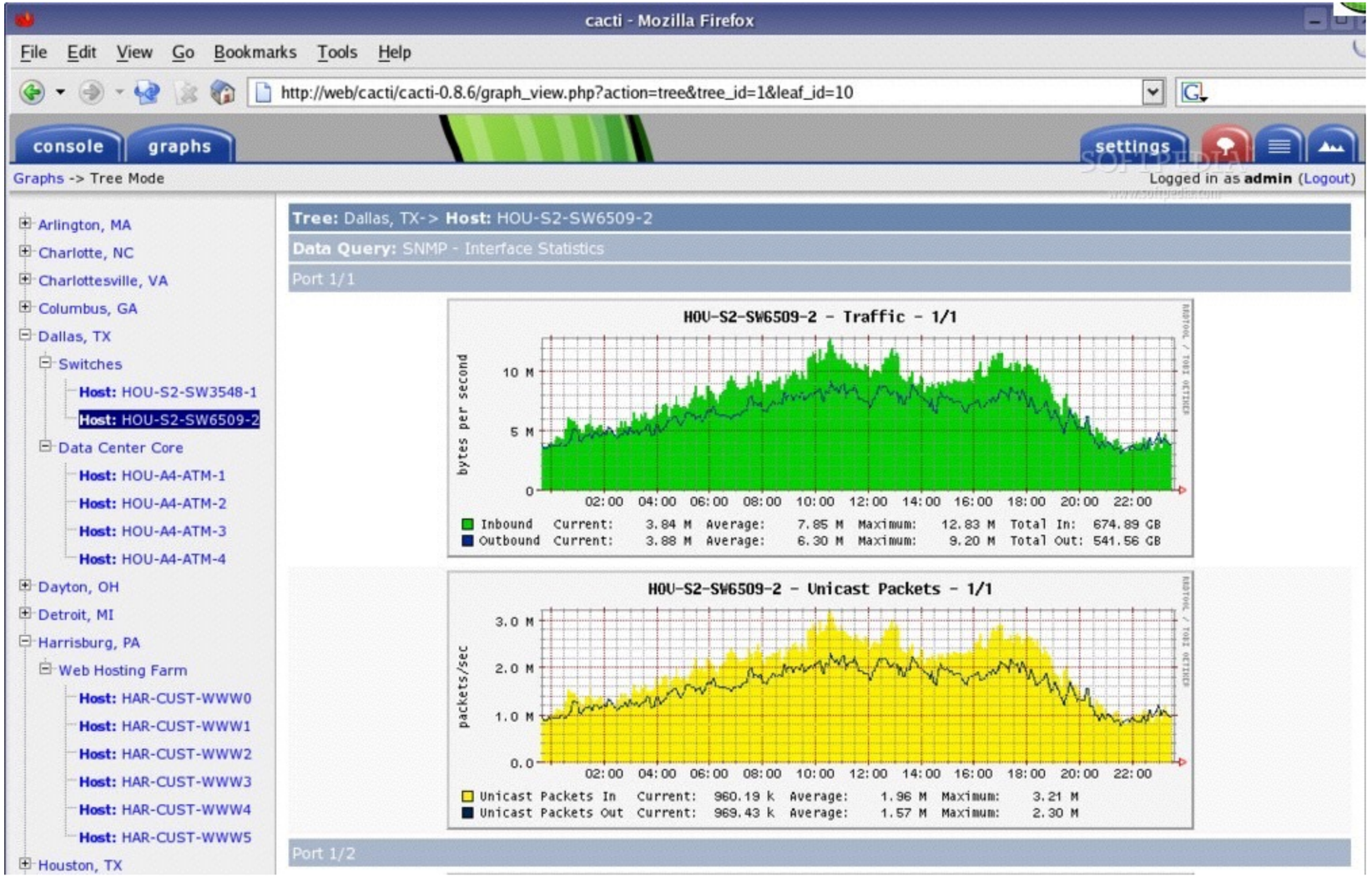
BandwidthD



Ip	Name	Total	Sent	Received	tcp	udp	icmp	http	p2p	ftp
Total	64.215.40.0/24	18.2G	4.8G	13.4G	15.2G	1.4G	1.6G	3.4G	23.2M	76.1M
64.215.40.2	dfw.derbyworks.com	11.3G	1.4G	9.9G	9.7G	155.1M	1.5G	393.1M	3.6M	37.5M
64.215.40.16	dfw-webserver	2.2G	1.7G	492.1M	2.2G	8.4M	295.0K	1.3G	4.5M	34.7M
64.215.40.4	mail.derbyworks.net	1.4G	652.3M	734.5M	1.2G	132.3M	1.8M	20.0K	1.5M	1.7M
64.215.40.10	ns1.derbyworks.net	932.0M	595.1M	336.8M	15.3M	889.0M	27.7M	0.0K	5.0K	0.0K
64.215.40.7	service.derbyworks.net	247.7M	8.4M	239.4M	247.2M	133.0K	30.0K	169.9M	3.8M	1.7M
64.215.40.5	manage.derbyworks.net	191.4M	68.4M	123.0M	26.6M	164.3M	583.0K	8.9M	0.0K	0.0K
64.215.40.106	dialin.derbyworks.net	123.6M	12.3M	111.3M	123.3M	231.0K	3.0K	120.3M	201.0K	0.0K
64.215.40.42	7350-3.derbyworks.net	104.3M	16.6M	87.7M	97.3M	7.0M	3.0K	81.5M	295.0K	0.0K
64.215.40.126	dialin.derbyworks.net	102.2M	24.8M	77.4M	100.8M	1.3M	141.0K	73.1M	619.0K	100.0K
64.215.40.108	dialin.derbyworks.net	97.1M	11.2M	85.8M	96.5M	494.0K	14.0K	88.6M	402.0K	0.0K
64.215.40.122	dialin.derbyworks.net	88.7M	7.2M	81.5M	88.5M	212.0K	8.0K	83.5M	240.0K	0.0K

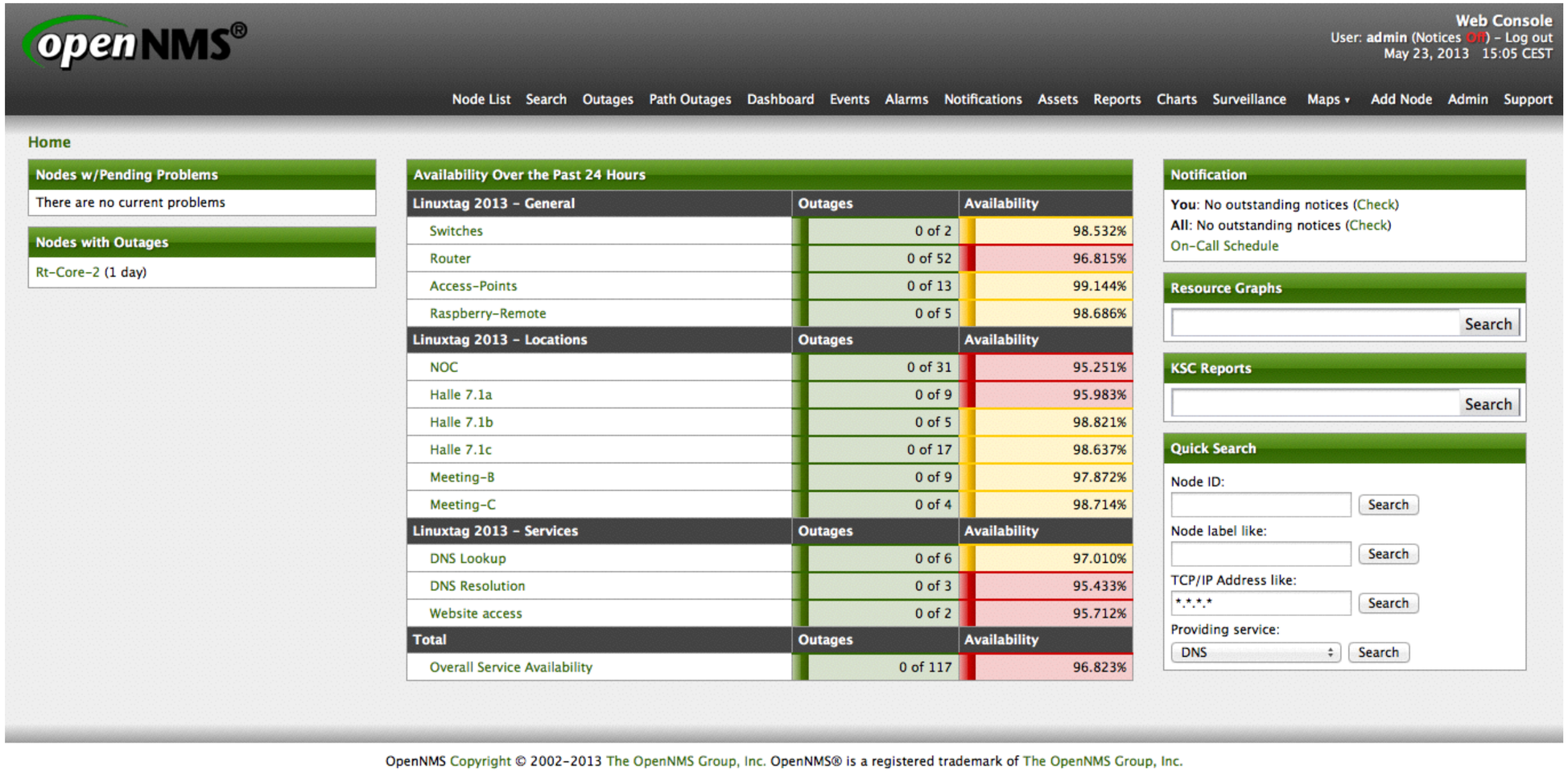
IL SOFTWARE

Cacti



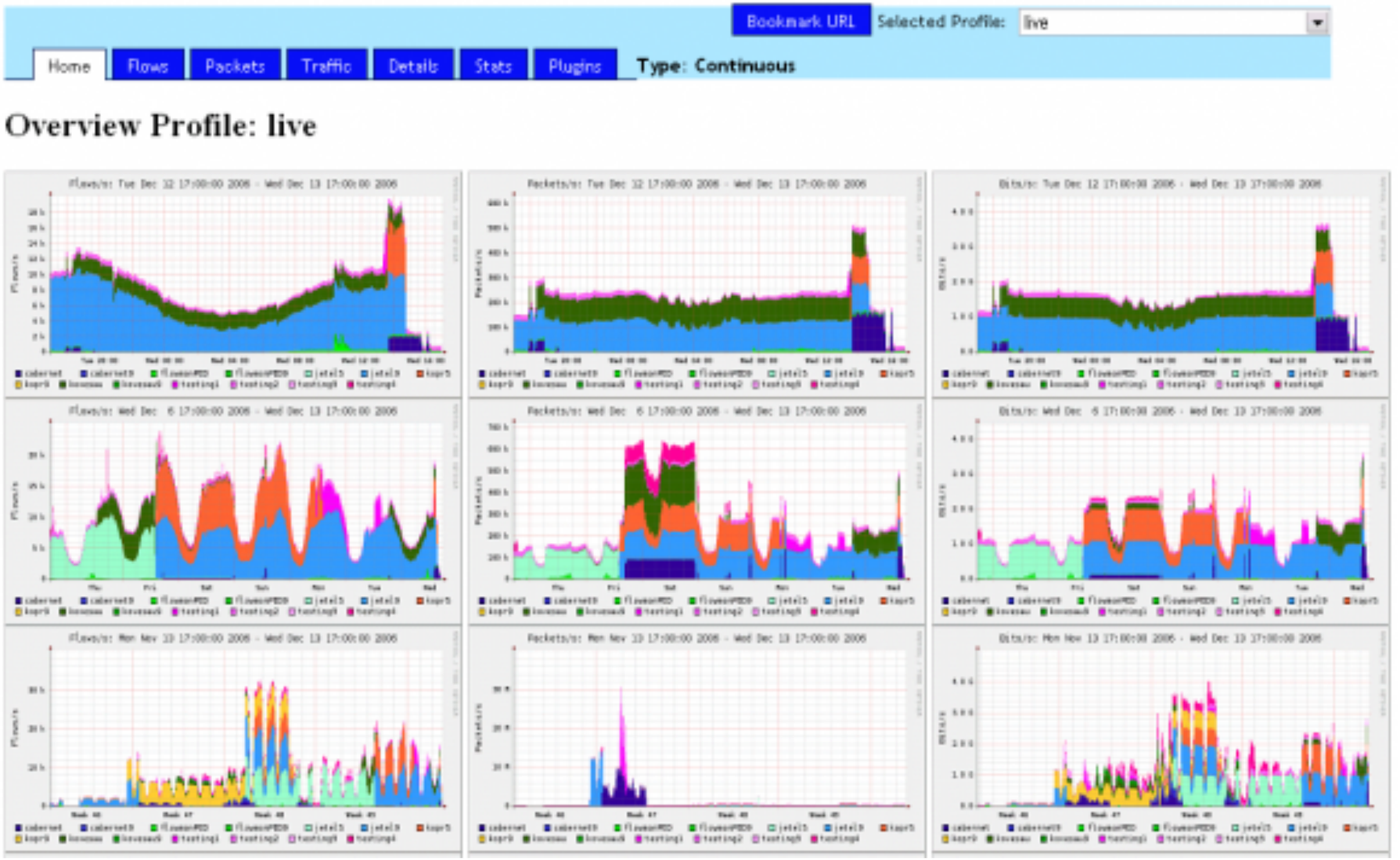
IL SOFTWARE

Opennms



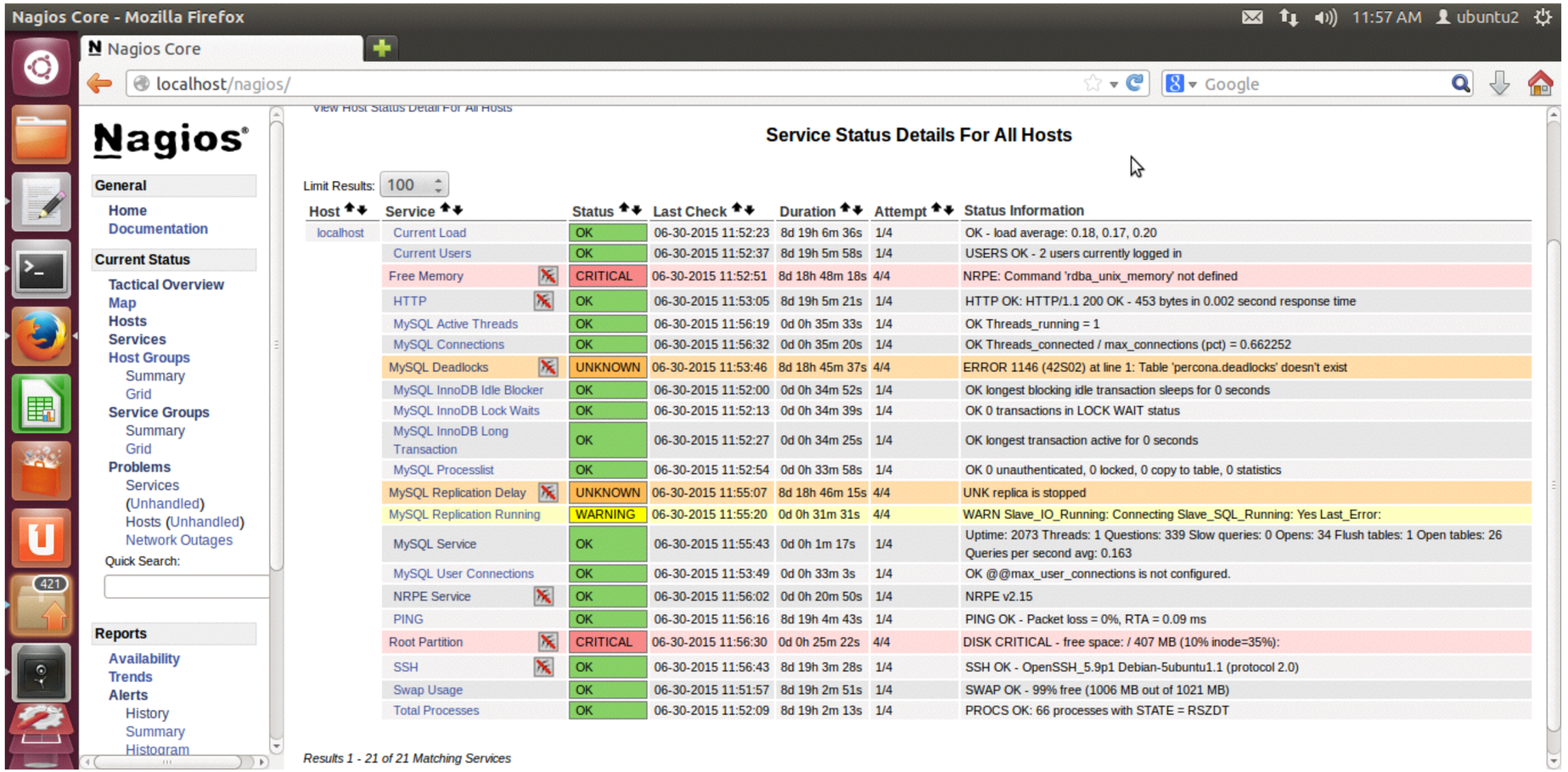
IL SOFTWARE

Nfsen



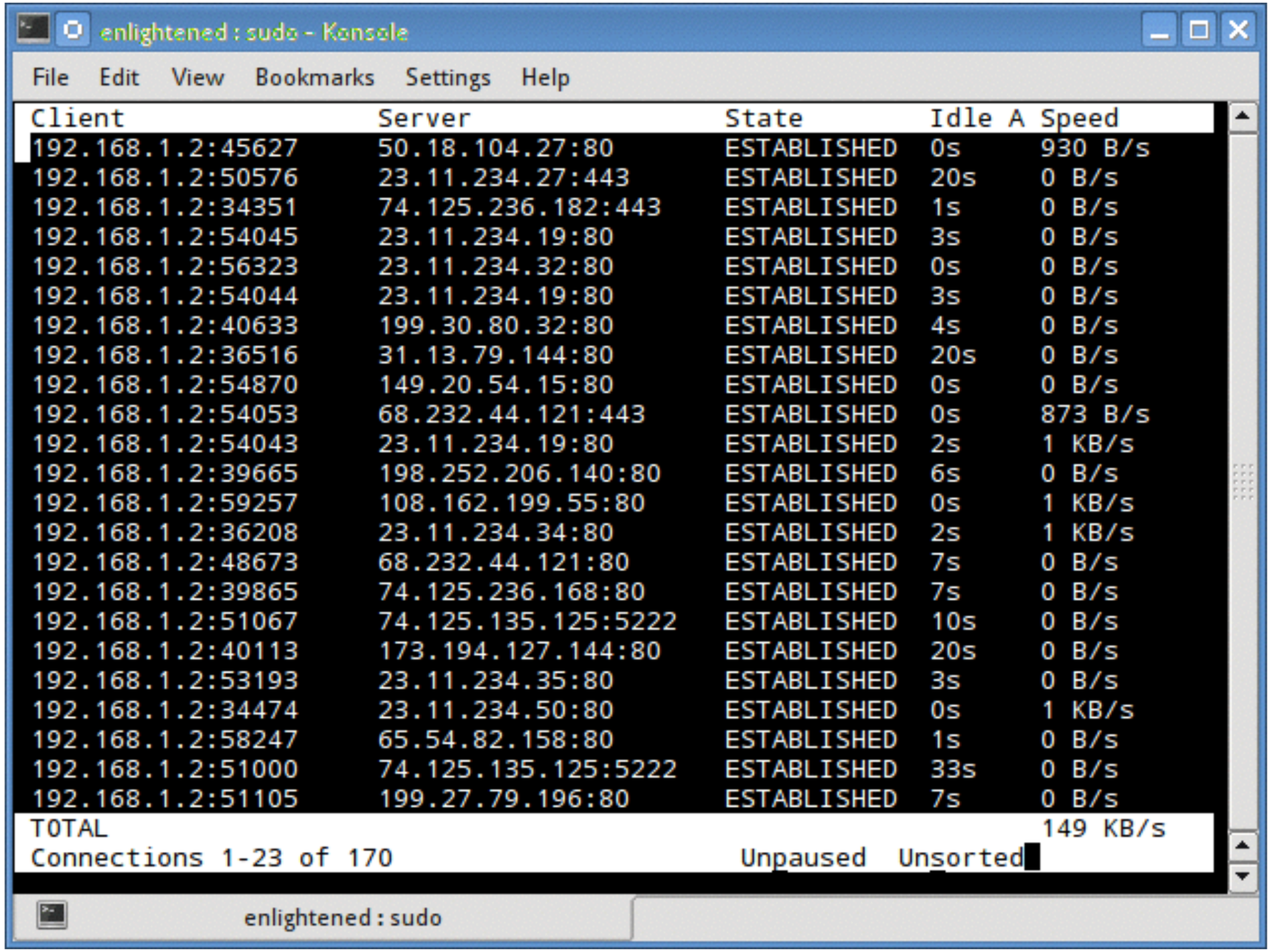
IL SOFTWARE

Nagios



IL SOFTWARE

Tcptrack



IL SOFTWARE

Dsniff

- Insieme di tool di sniffing e di analisi del traffico di rete.
  - Arpspoof
  - Tcpkill
  - Sshmitm (ssh v.1)
  - Webspy
  - Macof

IL TRASPORTO

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

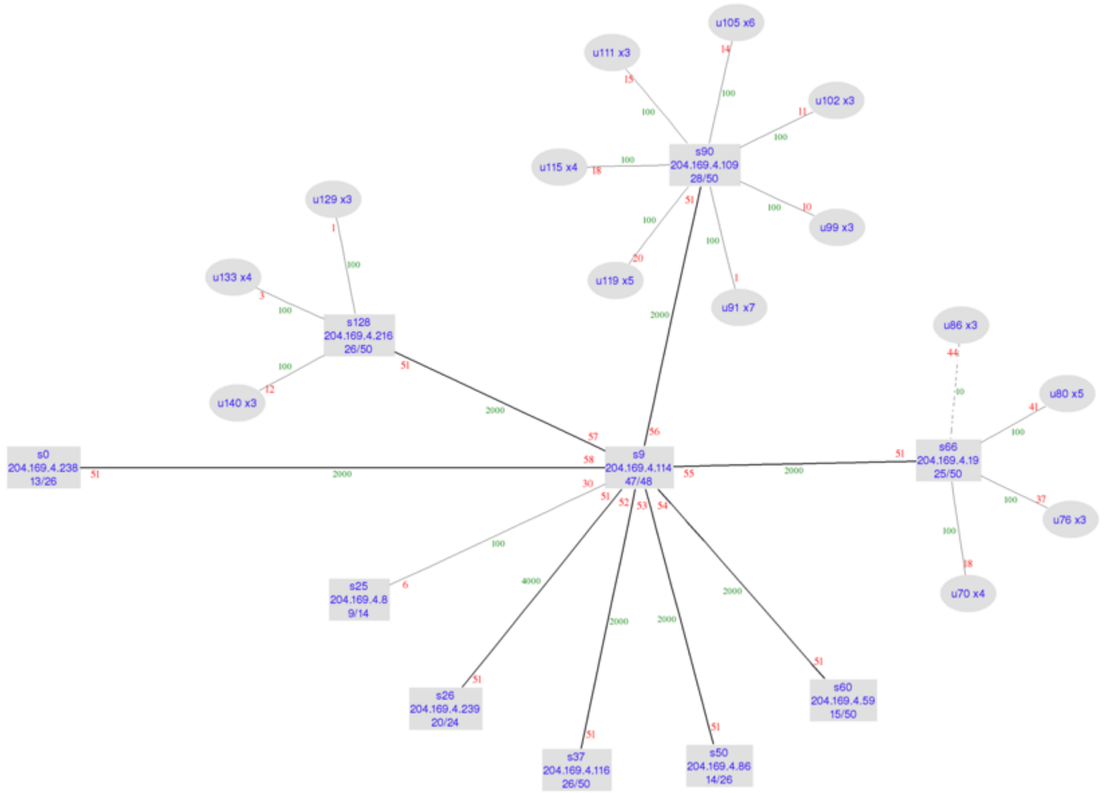
IL TRASPORTO

Perché monitorare

- Conoscere lo stato dei link.
- Tenere sotto controllo la congestione del network.
- Verificare i percorsi.
- Misurare il BER.
- Riconoscere alcuni attacchi di rete.
- Distribuire il traffico di rete.

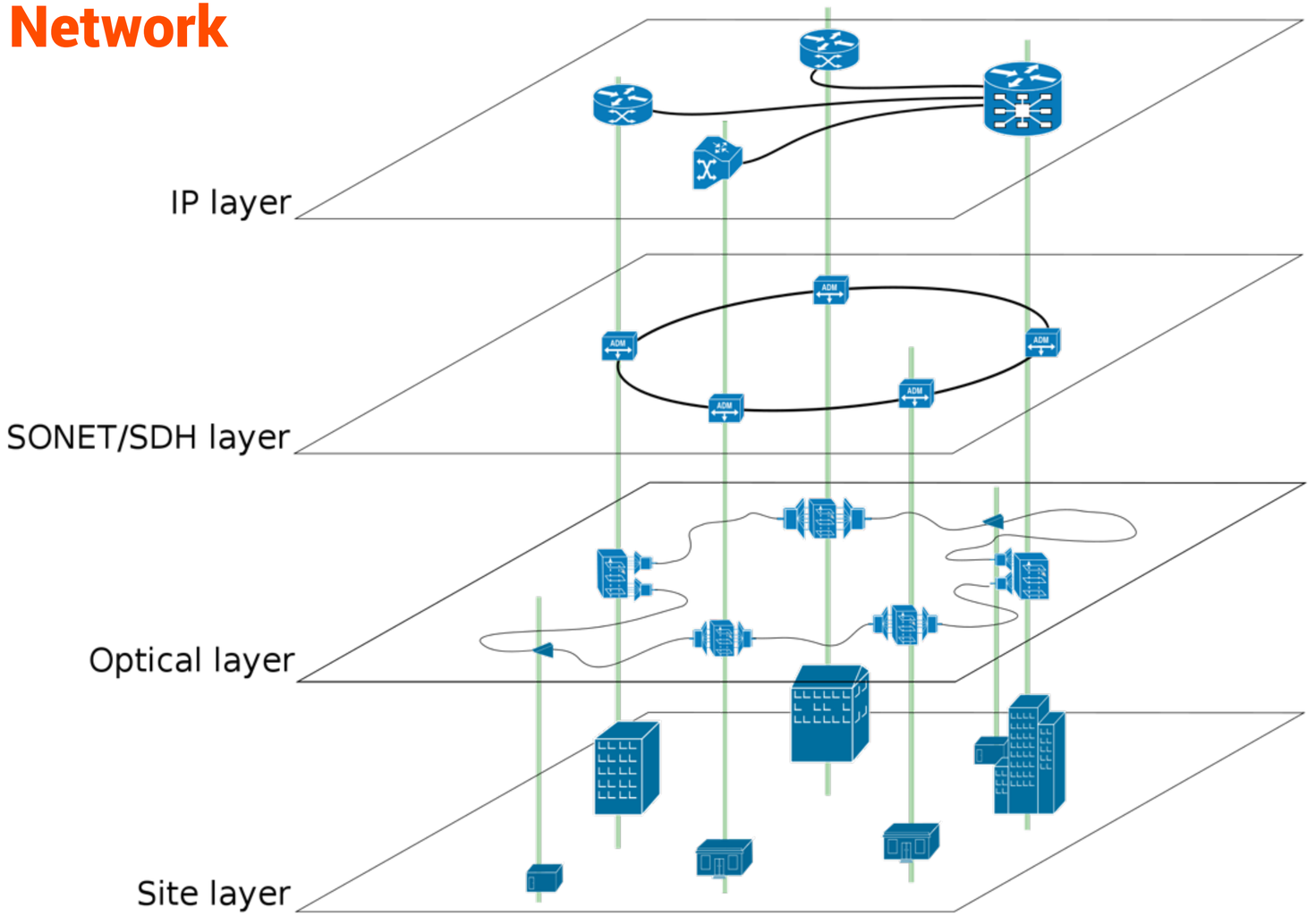
IL TRASPORTO

SNMP + GraphViz = Topology Map



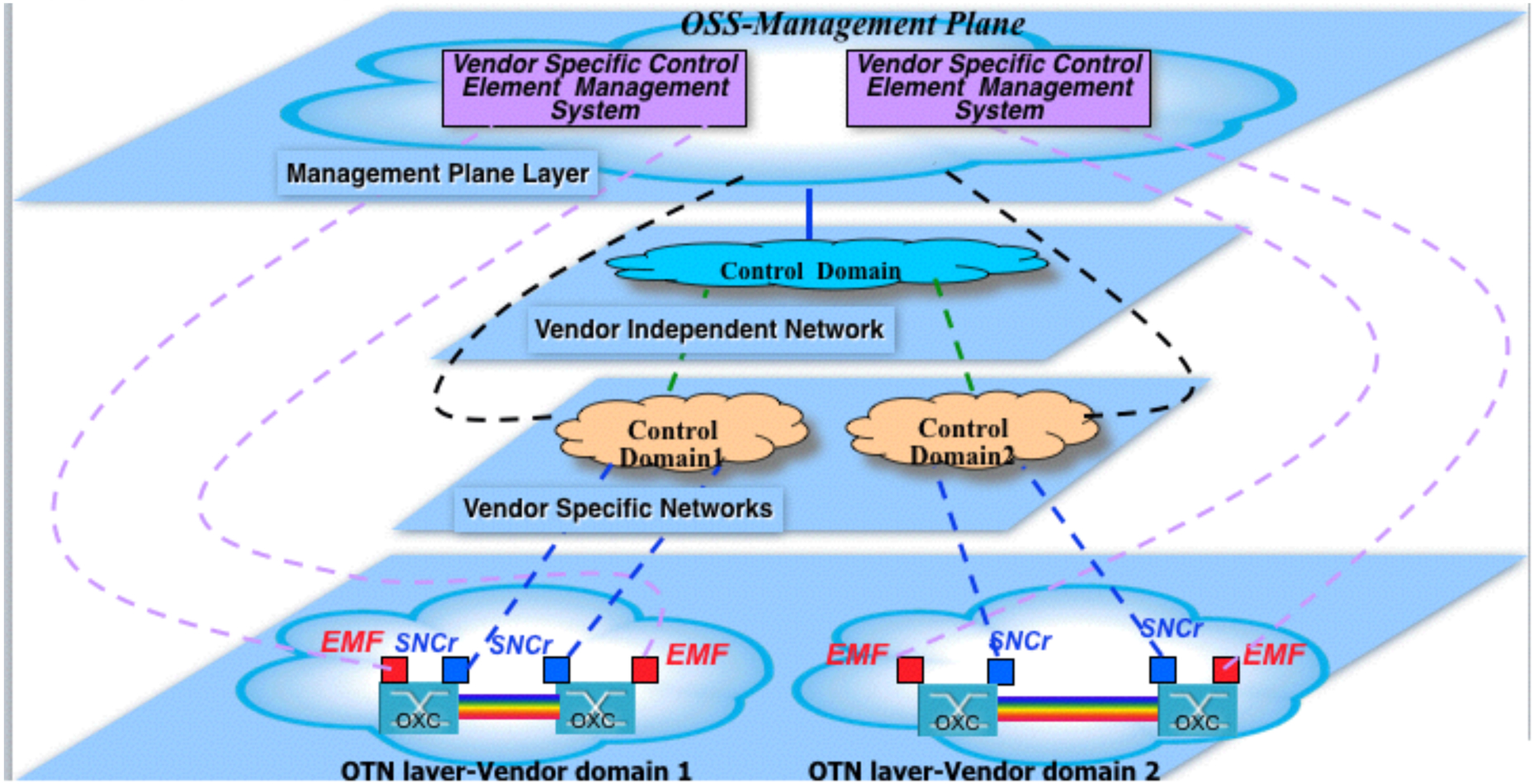
IL TRASPORTO

Overlay Network



IL TRASPORTO

OTN e Control Plane



IL ROUTING

Ip Routing Management

- La rete cambia costantemente
- Continuo reinstradamento del traffico in base al carico di rete o a link failure.
- Le soluzioni che fanno monitoraggio statico (magari via polling) non riescono a mostrare la dinamicità del cambiamento delle rotte.

IL ROUTING

BlackHoling

- Attraverso il monitoraggio (L3+L4) è possibile:
  - Riconoscere eventuali DOS.
  - Mitigarli.

- Nel caso di Sparkle è possibile effettuare il blackholing via bgp usando la community 6762:666
- Il blackholing non è la soluzione migliore per gestire un dos.

ALTA AFFIDABILITA’

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

ALTA AFFIDABILITA’

Disponibilità

- Occorre avere alta disponibilità e alta affidabilità della rete.
- Ci aspettiamo che la rete funzioni sempre.
- Servizi sempre più pervasivi.
- Resilenza.
- Point of failure.

ALTA AFFIDABILITA’

Servizio sempre disponibile.

Availability	Downtime per Year (24x7x365)		
99.000%	3 Days	15 Hours	36 Minutes
99.500%	1 Day	19 Hours	48 Minutes
99.900%		8 Hours	46 Minutes
99.950%		4 Hours	23 Minutes
99.990%			53 Minutes
99.999%			5 Minutes
99.9999%			30 Seconds

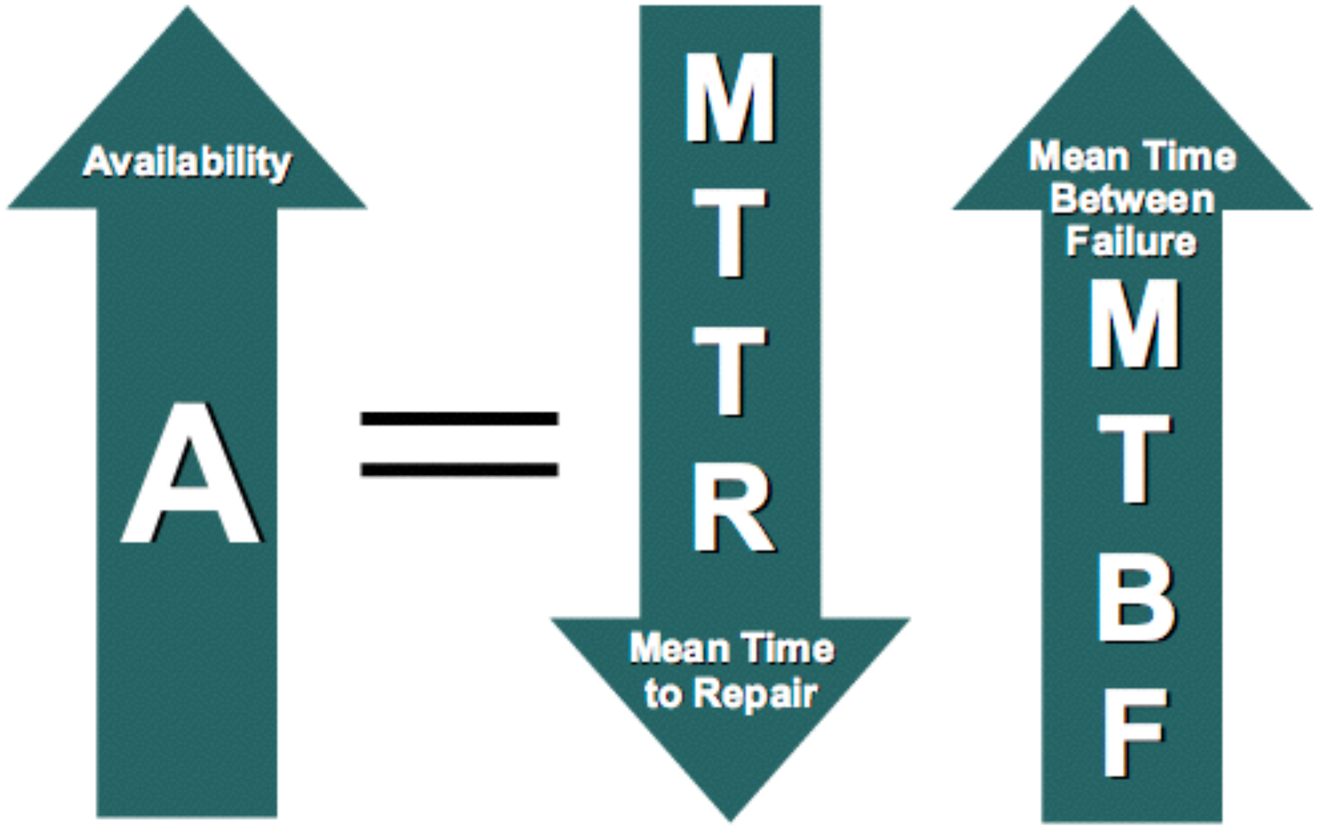
ALTA AFFIDABILITA’

Affidabilità e robustezza

- **Disponibilità = MTBF / (MTBF + MTTR)**
  - **MTBF è Mean Time Between Failure**
  - **MTTR è tempo medio di riparazione**

ALTA AFFIDABILITA’

Aumentare il grado di disponibilità.



ALTA AFFIDABILITA’

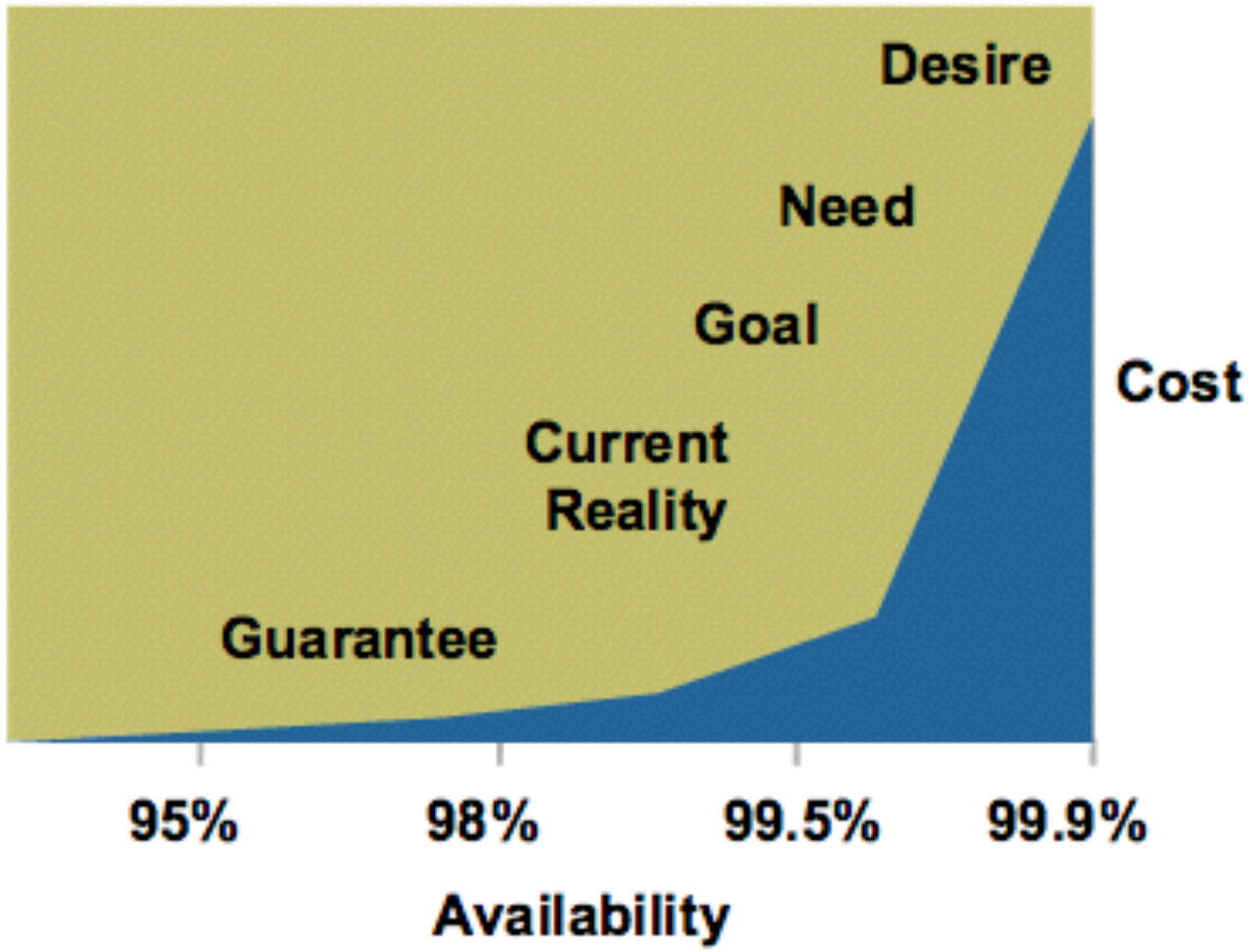
Gestione

- Costa il downtime
- Costa aumentare il grado di disponibilità.

- Gestione del rischio.
- Disaster recovery.
- Cultura della “alta affidabilità”.

ALTA AFFIDABILITA’

Costi



IT SECURITY

Seminario “Monitoraggio Traffico e Sicurezza di Rete” - Dipartimento di Informatica dell’Università di Pisa

Monitorare per la sicurezza

- Gli statefull firewall non garantiscono più una elevata sicurezza (se usati da soli).
- E' possibile analizzare il traffico di rete per riconoscere bloccare traffico malevolo.
- Occorre effettuare deep inspection.
- Ne parleremo al prossimo seminario…

GIUSEPPE AUGIERO

COME MONITORARE IL TRAFFICO DI RETE IN UNA RETE MEDIO/GRANDE

Web: www.augiero.it