Monitoraggio e Management del Network con strumenti open source

Fondazione CNR / Regione Toscana Gabriele Monasterio

Giuseppe Augiero

Agenda

- Al giorno d'oggi è gestire nel modo corretto grande network.
- Una buona gestione permette di prevenire molti malfunzionamenti e di diagnosticare in modo corretto situazioni anomale.
- Cosa si intende per "monitoring" o "management" del network?
- Parte del lavoro presentato è quanto realizzato all'interno del Network Geografico della Fondazione G. Monasterio.

Focus

Il network

- La rete è un elemento fondamentale all'interno di una infrastruttura informatica.
- Tutti i servizi informatici di nuova generazione richiedono alla rete il trasporto di dati e informazioni.
- Il network diventa un elemento dinamico che deve erogare il servizio h24 senza mai fermarsi.

Gestione

- La gestione di una infrastruttura di rete complessa si basa sulla capacità di :
  - Misurare tutti i fenomeni fondamentali.
  - Rappresentare il valori misurati.
  - Interpretare il senso delle misure e trarne le conseguenze.

Network Monitoring?

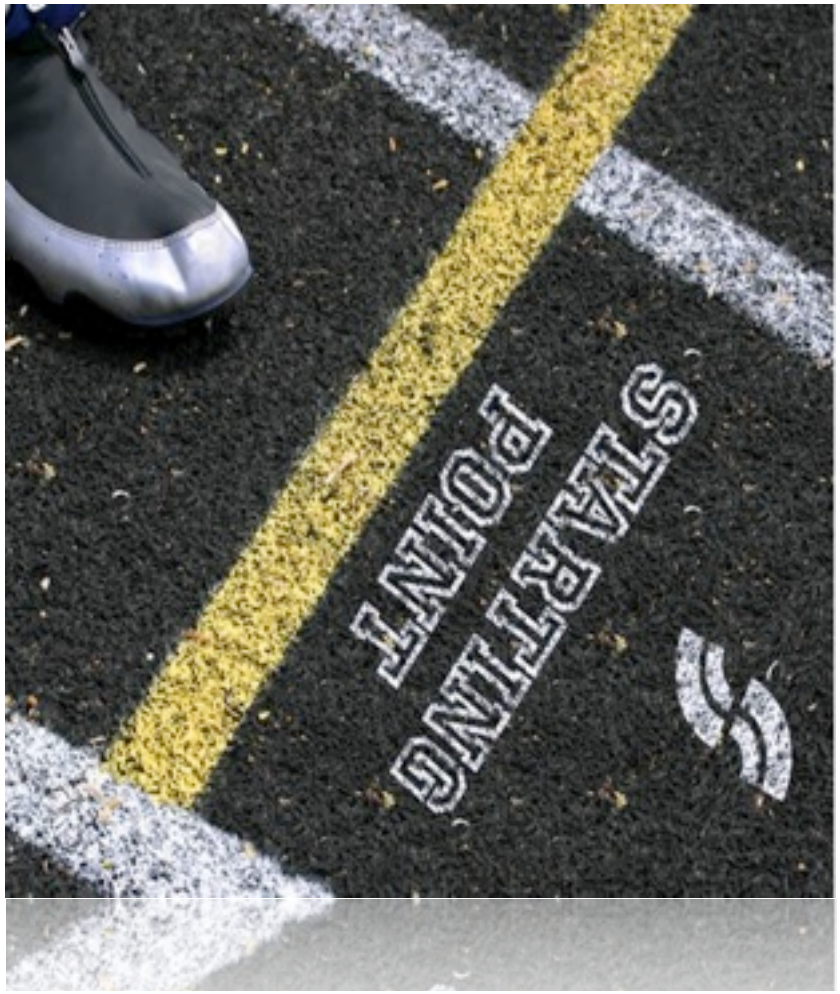
- Lo scopo del monitoraggio è quello di diagnosticare i problemi e raccogliere le statistiche da utilizzare da parte dell'amministratore e per una corretta messa a punto della rete stessa.
- Il monitoraggio deve essere costante.
- In caso di problemi deve avvisare automaticamente l'ammistratore di rete dell'anomalia.

Network Management?

- La gestione della rete permette di capire cosa sta succedendo sull'infrastruttura di trasporto e quali devo essere le azioni da compiere.
- Attraverso alcuni appropriati tool è possibile "gestire la rete".
- La gestione della rete permette di garantire diversi aspetti:
  - Sicurezza
  - Affidabilità
  - Performance

Il punto di partenza

- La nostra esigenza iniziale è quella di avere una rete attiva e funzionante.
- Per definire cosa si intende per "funzionante" occorre specificare:
  - Politiche
  - Aspettative
  - Interventi
  - Uptime
  - Service level agreement



Uptime

- Non esiste nessuna apparecchiatura che abbia un uptime del 100%.
- Cosa significa avere un uptime del 99.9%?
- Facciamo due calcoli:
  - 30,5 x 24 = 762 ore al mese
  - (762 -(762 x 0,999)) x 60 = 45
- Soli 45 minuti di inattività in un mese!
- Come viene calcolata la disponibilità?

Misure

- Quante volte vi hanno chiesto: "La rete funziona in maniera corretta?".
- Per rispondere a questa domanda bisogna, almeno una volta, aver misurato i seguenti parametri:
  - Carico dei link
  - Jitter tra due end point.
  - Carico dei processori.
  - Pacchetti scartati.
  - Quantità di rumore.

Management (I)

- L'informazione generata da un buon network management ci permetterà di :
- Sapere quando effettuare l'upgrade del network.
  - poichè c'è un uso massivo della banda.
  - perchè gli apparati sono troppo vecchi.
  - esigenza di utilizzare più fornitori di accesso.

Management (II)

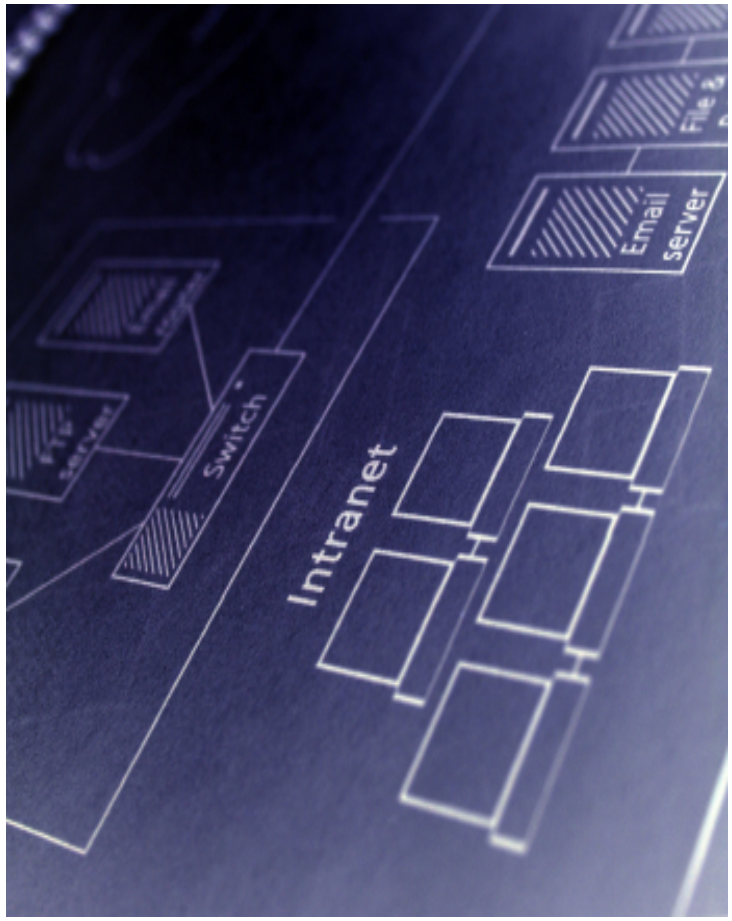
- Gestione e traccia dei cambi di configurazione degli apparati.
- Accounting
- Conoscere immediatamente dove sono presenti problemi o malfunzionamenti.
- Evidenziare i trend di crescita in modo da poter pianificare, in maniera opportuna, nuove estensioni o per migliorare la capacità di progettazione.

Sicurezza

- Dall'analisi dei trend è possibile capire se si la rete e' sotto attacco.
- Attraverso i tool di management è possibile mitigare eventuali attacchi.
- I tool possono permettere di conoscere le seguenti informazioni:
  - Link saturi.
  - Analisi dei flussi di rete.
  - Server o apparati attaccati.

Progettazione

- Progettare non è mai una operazione banale, soprattutto quando occorre prevedere il trend di crescita e di utilizzo di una determinata infrastruttura.
- Dimensionare in modo non corretto un progetto significa gestire lavorare due volte ed avere un aggravio economico che impatta.
- Un buon network management permette di conoscere con la giusta oculatezza di trend di crescita.

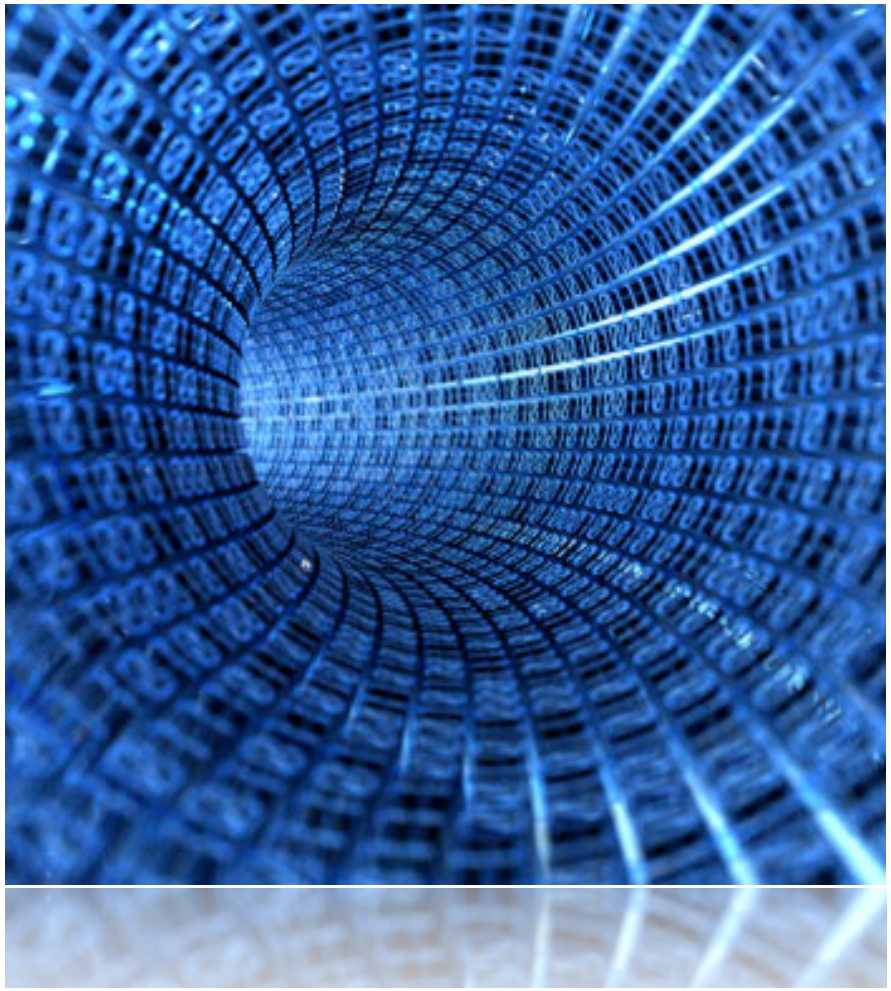


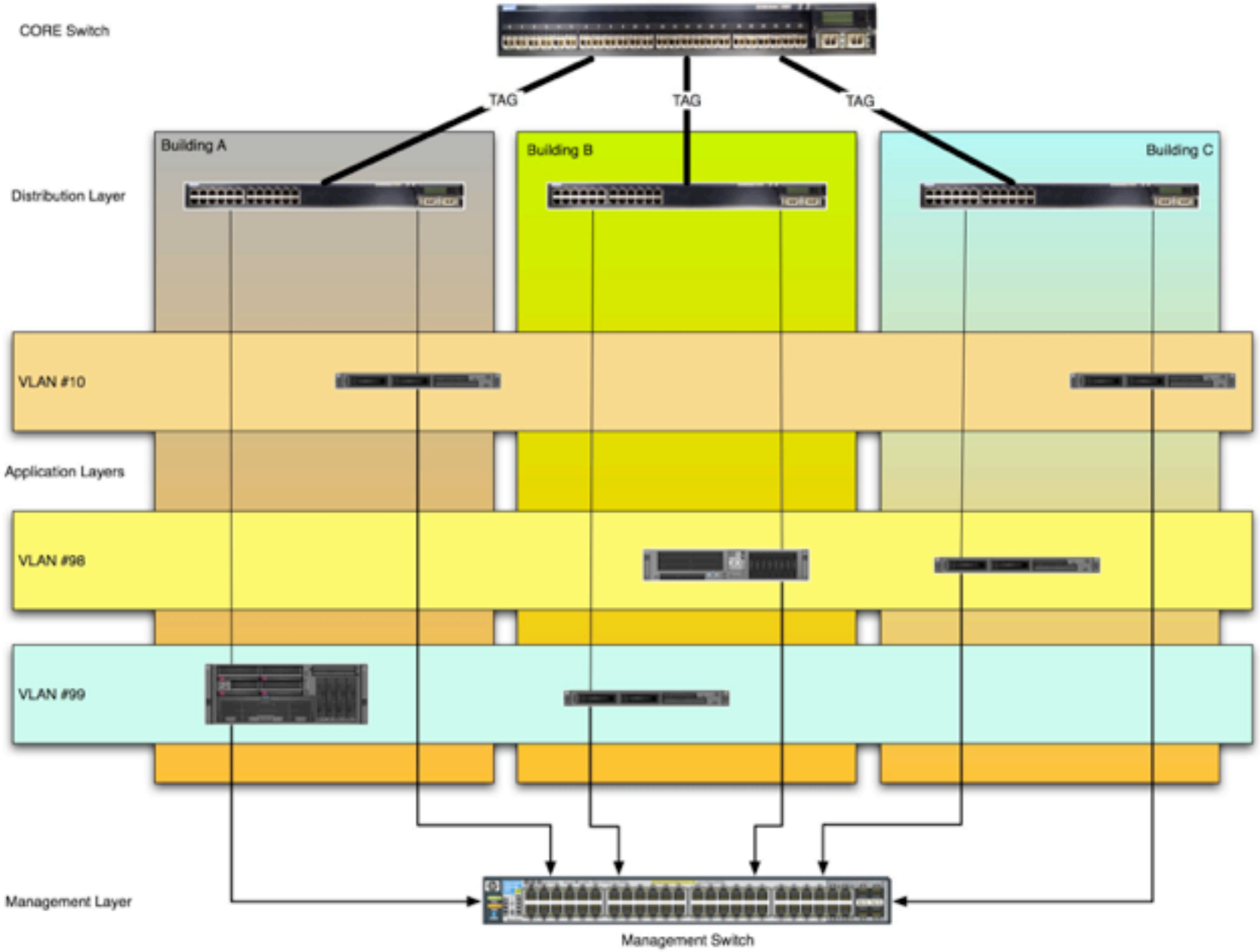
Open Source

- Esiste una ampia varietà di software e tool per la gestione del monitoraggio e del managemente della rete.
- Perchè scegliere prodotti open source?
  - Flessibilità.
  - Aggiornamenti.
  - Possibilità di modificare il codice sorgente.
  - Comunità.

Rete di management (I)

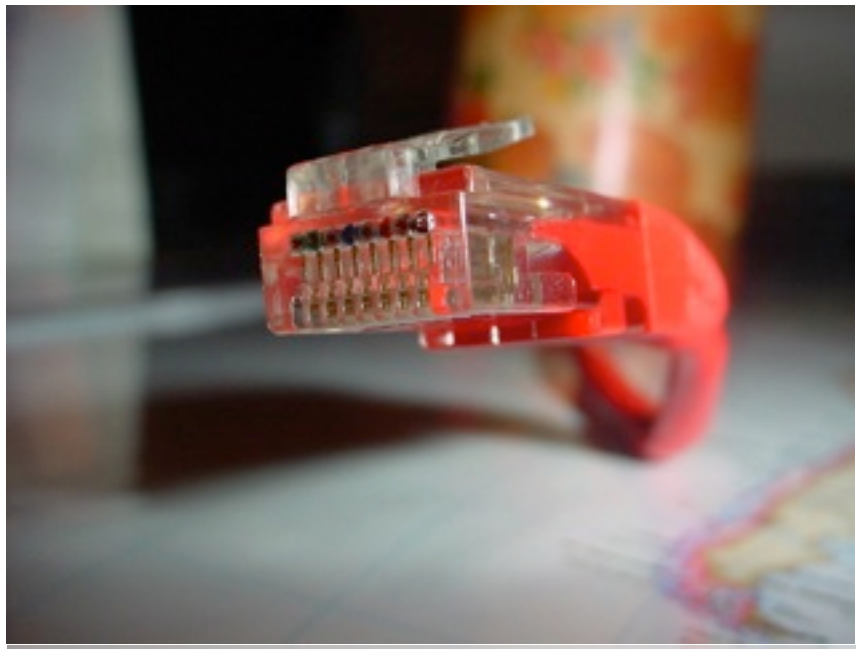
- E' molto importante gestire l'intera infrastruttura di rete avendo il minor numero di punti di fallimento.
- La soluzione migliore e' avere una rete di gestione che interconnette tutti gli apparati e dispositivi di network attraverso una rete flat.
- La rete di gestione deve essere attiva e funzionante anche in caso di guasti o anomalie.




CORE Switch
TAG
TAG
TAG
Building A
Building B
Building C
Distribution Layer
VLAN #10
Application Layers
VLAN #98
VLAN #99
Management Layer
Management Switch

Rete di management (II)

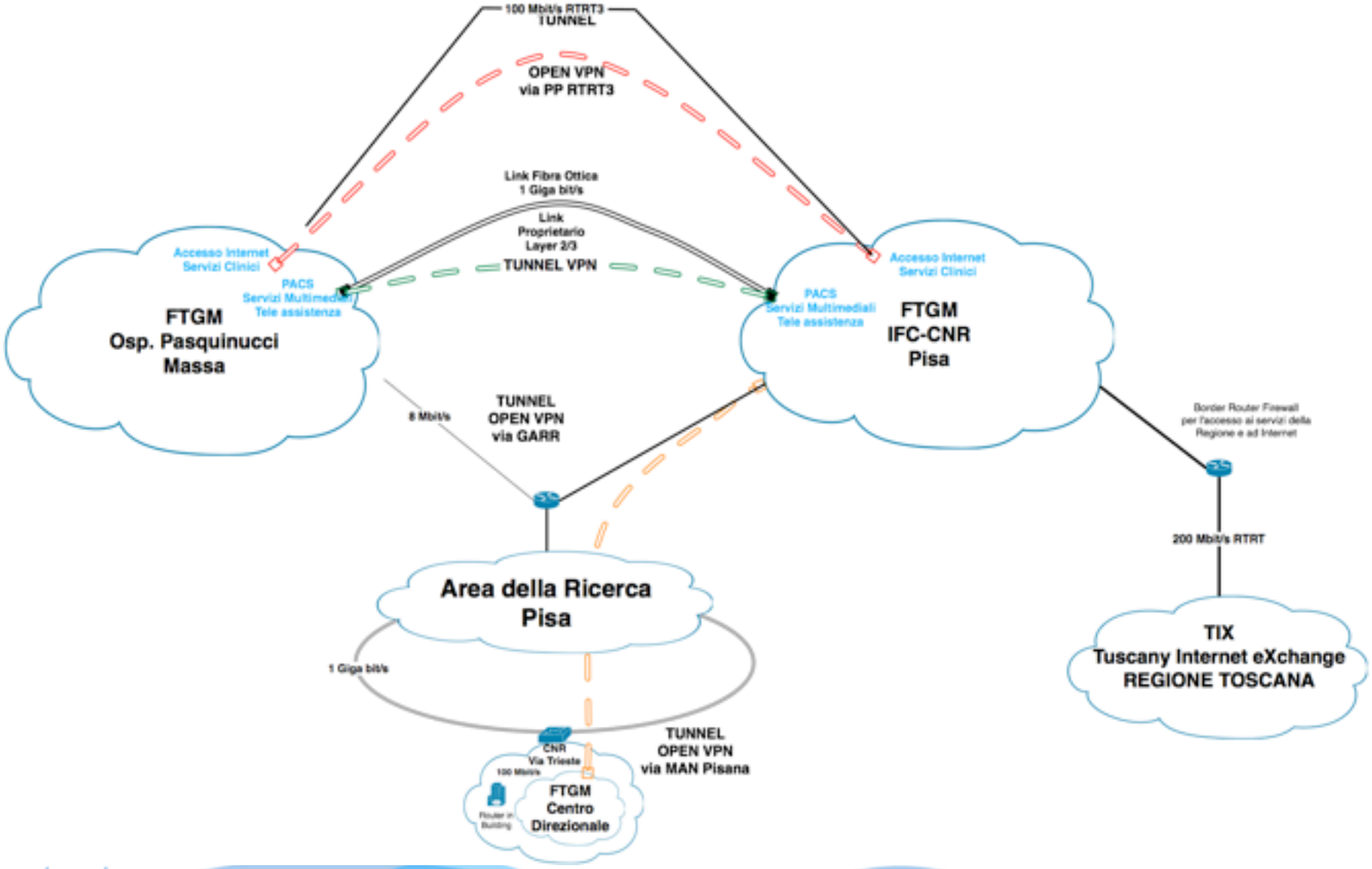
- Best practices:
  - Rete semplice.
  - Configurare la vlan di default.
  - Lasciare una porta di management su ogni switch.
  - Avere un accesso diverso da Internet per la rete di management.
  - Proteggere nel modo corretto la rete di gestione.
  - Separare, se necessario, le interfacce di gestione degli apparati da quelli dei server.



Concatenazione di eventi

- Attraverso la concatenazione degli eventi è possibile riconoscere anomalie, problemi o eventuali attacchi che normalmente non potrebbero essere riconosciuti.
- La relazione tra accadimenti permette di definire uno scenario ben determinato di un eventuale anomalia riscontrata.
- E' fondamentale il supporto NTP su tutti gli apparati.
- Falsi positivi.

Schema iniziale rete geografica FTGM



Flows

Flussi

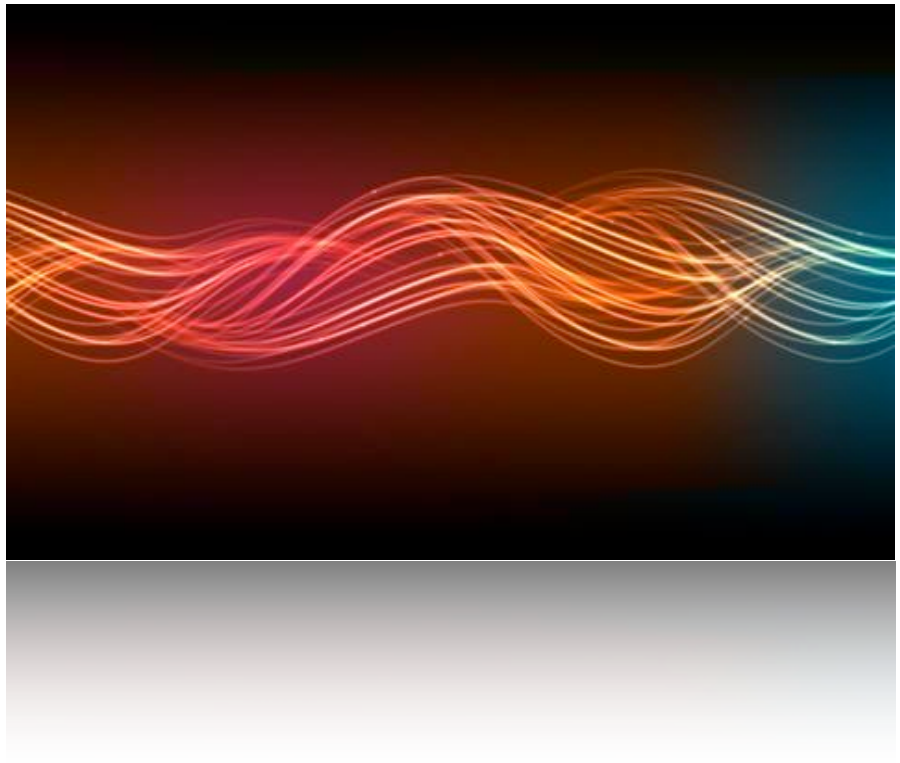
- Attraverso i flussi di rete è possibile aggregare tipologie di traffico dati con determinate caratteristiche.
- Analizzare i flussi al posto dei singoli pacchetti trasportati risultare essere più semplice e di più semplice rappresentazione.
- In fase di aggregazione i dati trasportati dal network sono campionati.
- Diversi protocolli di gestione dei flussi.

Netflow - Sflow

- Netflow e Sflow sono due standard tecnologici per monitorare, attraverso l'aggregazione dei dati, reti ad altà velocità.
- Risolvono egregiamente il problema di implementare una coda circolare o altre soluzioni per evitare la perdita di pacchetti in fase di acquisizione.
- Possono essere utilizzati anche per funzionalità di accounting o di billing.
- Non mostrano il payload.

Fprobe

- Fprobe è uno strumento che raccoglie dati sul traffico di rete e li spedisce , sotto forma di flussi netflow a uno specifico collettore.
- Esiste una versione particolare chiamata fprobe-ulog che può essere integrata con netfilter (iptables).
- Fprobe permette di avere buone prestazioni anche su macchine obsolete.



Ntop

- Ntop (Network Top) è una applicazione per l'analisi e il monitoraggio della rete.
- Include funzionalità di Intrusion detection system anche se non è stato sviluppato esattamente per questi scopi.
- Utilizza una interfaccia web per visualizzare i dati raccolti.
- E' sviluppato da Luca Deri.

Nfsen

- Nfsen è l'interfaccia grafica dei tool nfdump.
- Permette:
  - Visualizzazione dei dati (RRD).
  - Funzionalità di data mining con molteplici possibilità di selezione dei dati .
  - Meccanismi di alerting su varie condizioni.
  - Possibilità di estendere le funzionalità tramite plugin.

Monitoraggio

Protocollo SNMP

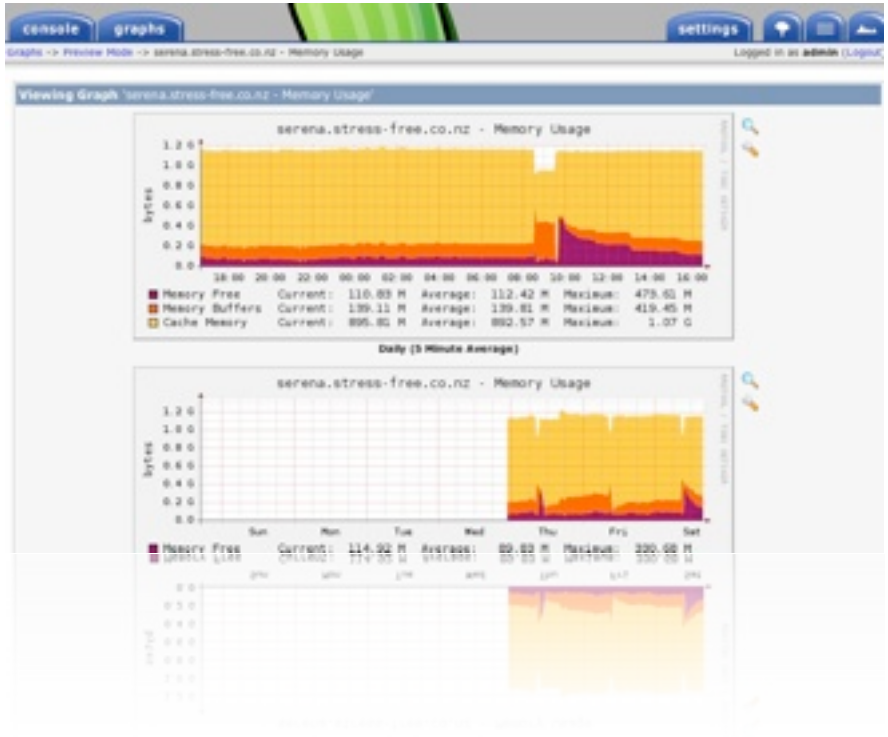
- Il protocollo snmp (simple network management protocol) nasce per la gestione e supervisione di apparati collegati in rete.
- Il sistema di gestione è basato su due elementi:
  - supervisore
  - agente
- Il supervisore effettua le richieste di management, l'agente permette di recuperare le informazioni volute dai device.

Mrtg

- E' probabilmente il software open source di monitoraggio, più anziano e conosciuto, che usa il protocollo snmp.
- Nella configurazione di default raccoglie i dati ogni 5 minuti.
- I dati provenienti dale singole interfacce possono essere riuniti in una singola pagina web.
- E' possibile utilizzarlo anche per monitorare le informazioni di sistema di un server linux.

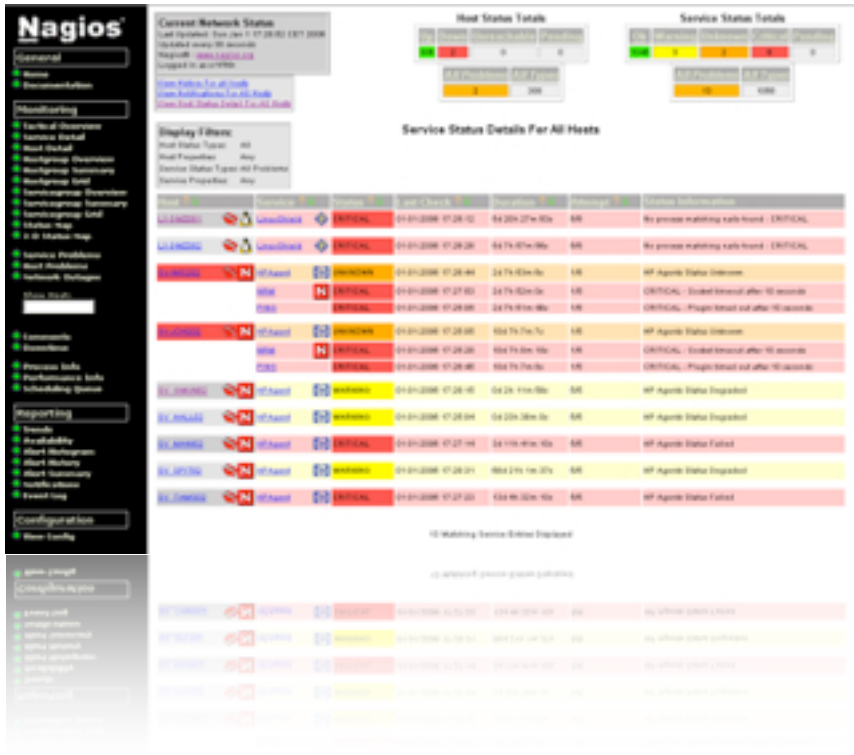
Cacti

- Interfaccia grafica per visualizzare lo stato di funzionamento di device di rete che supportano il protocollo snmp.
- Più completo rispetto a Mrtg.
- Utilizza il database Mysql per la conservazione delle misure effettuate.
- E' possibile usare o sviluppare scriiti ad hoc per cacti.
- Supporta AAA.



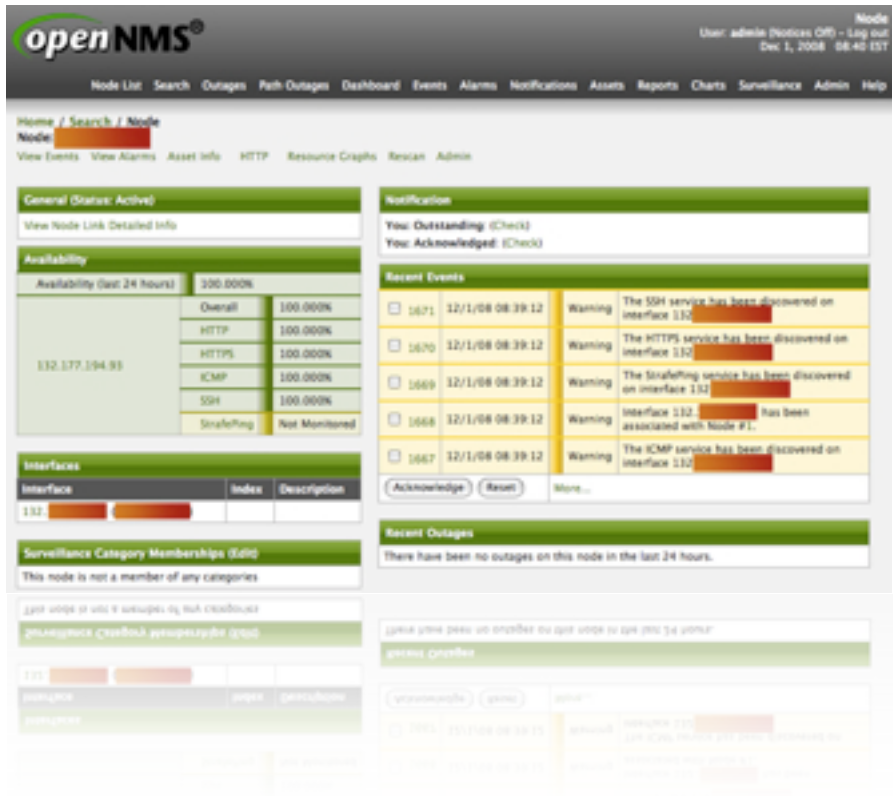
Nagios

- Nagios permette il monitoraggio e risorse di rete.
- In caso di malfunzionamento di un componente monitorato nagios può intraprendere una azione di segnalazione inviando mail o sms o altro.
- E' fortemente personalizzabile.
- Esistono tantissimi componenti aggiuntivi ed è molto facile scrivere un nuovo plug-in.
- Può lavorare in maniera distribuita o dialogando con altri nagios.



OpenNMS

- Il software permette di tenere sotto controllo, di misurare le prestazione, e di conoscere lo stato di apparati o nodi di rete.
- Rappresenta una ottima soluzione sopratutto per grandi reti o per carrier.
- Pieno supporto di IPv6.
- Portabilità della soluzione.
- Per il controllo dei nodi può usare i protocolli snmp, http, jmx (java management extensions).

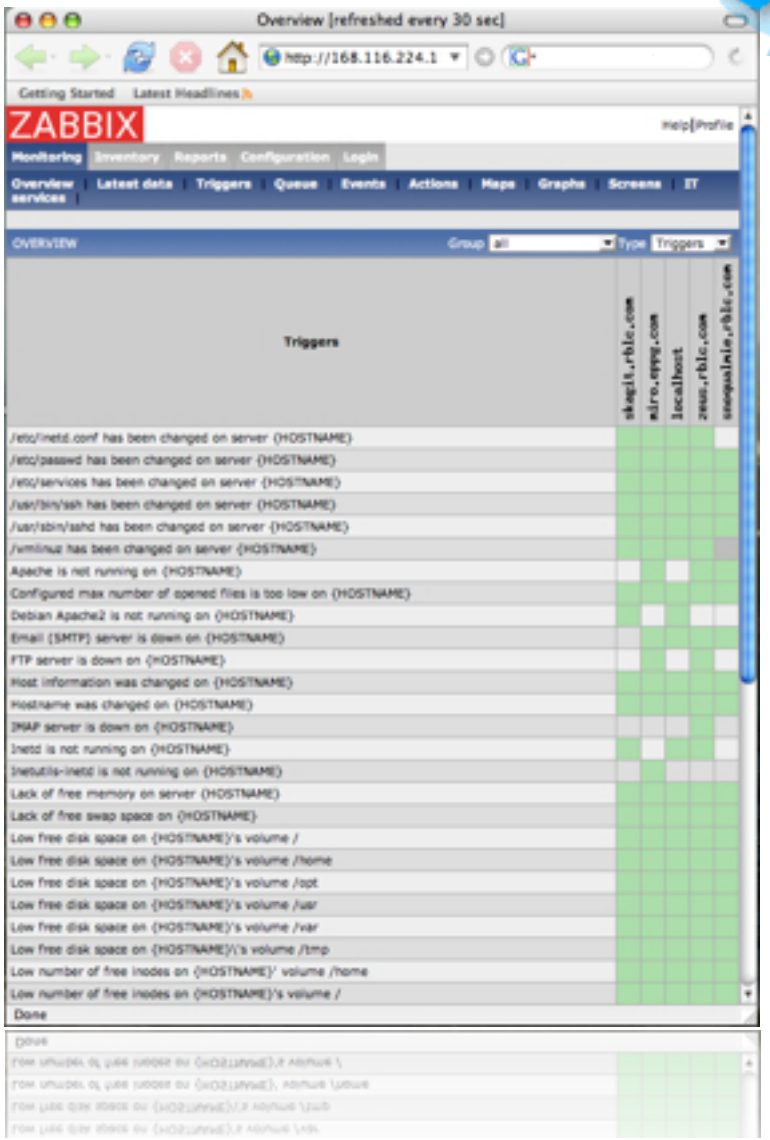


Zenoss

- Zenoss è una piattaforma per il monitoraggio di sistemi interconnessi in rete.
- Ricco e completo, ha uno sviluppo molto rapido.
- Suite completa che prevede diverse funzionalità.
- Esiste una versione Enterprise a pagamento.
- Look and feel accattivante.
- E' utilizzato da nomi famosi del mondo della tecnlogia.

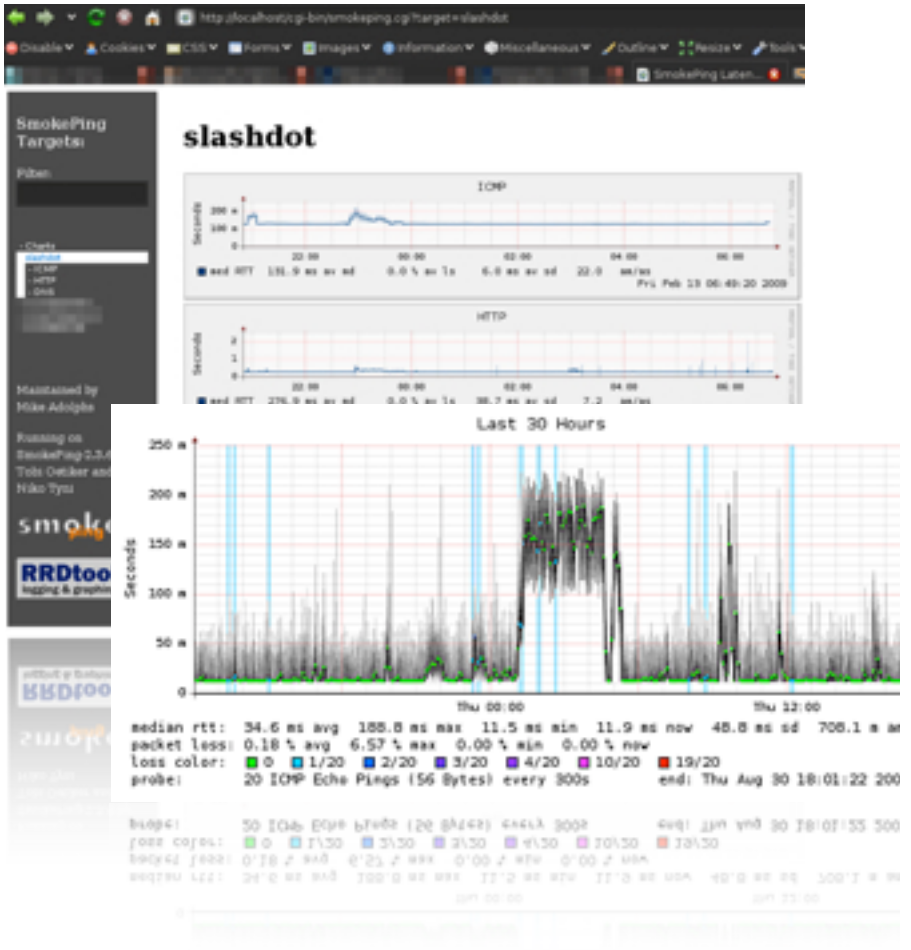
Zabbix

- Zabbix, completo e flessibile, effettua il monitoraggio della rete.
- Può lavorare in modalità polling o trapping.
- Si propone come alternativa a nagios e a cacti.
- I requisiti hardware non sono esosi.
- Multipiattaforma.
- E' possibile trovare sul mercato degli appliance con Zabbix pronti ad effettuare monitoraggio dei sistemi.



Smokeping

- Smokeping permette di monitorare le latenze di rete.
- E' possibile organizzare il monitoraggio per domini e sottodomini.
- Possiede una ampia gamma di librerie per testare e monitorare diversi protocolli o nodi.
- Può lavorare in maniera distribuita.
- Supporta un sistema di allarme per segnalare eventuali anomalie.
- Scritto dal creatore di mrtg e rrdtool.



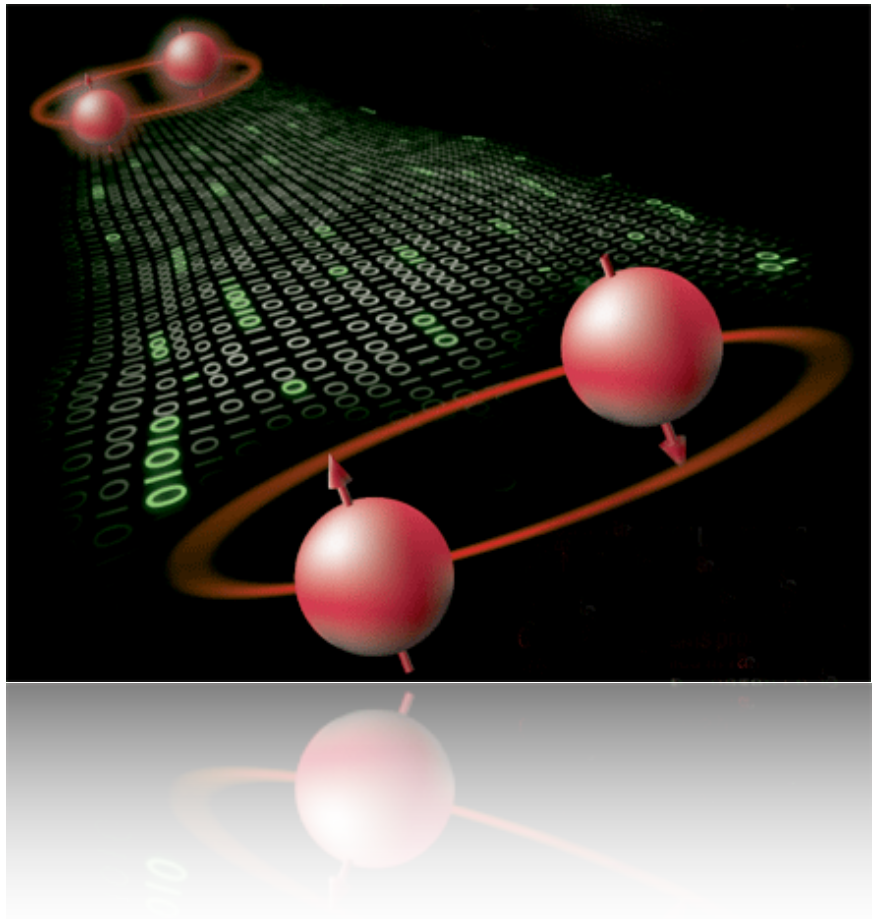
Munin

- Munin è uno strumento di monitoraggio di elementi di rete che permette di avere informazioni sull'utilizzo delle risorse di un determinato nodo.
- Può inviare allarmi nel caso di anomalie o di utilizzo intensivo di una risorsa.
- E' progettato per essere plug & play.
- Esistono plug-in (anche di terze parti) per munin.

Management

Sec

- Sec è uno dei software opensource indipendente dalla piattaforma utilizzata.
- E' stato scritto per integrare tutte quelle funzionalità che a volte mancano nei sistemi di correlazione commerciali.
- Può essere utilizzato in maniera proattiva, facendogli eseguire azioni automatizzate.
- Usabile anche in altri campi.



Arpwatch

- Arpwatch permette di monitorare il protocollo Arp (address resolution protocol) di una rete.
- Attraverso questo tool è possibile:
  - Avere uno storico dei mac adr.
  - Essere informati sui conflitti ip
  - Tenere sotto traccia l'attività arp di una rete.
- Permette di riconoscere attacchi di tipo arp spoofing.
- Utilizza la librerua libpcap per la cattura dei pacchetti.

Dhcpprobe

- Permette di riconoscere eventuali server dhcp abusivi.
- E' possibile disconnettere un client che ha ricevuto l'ip da un fake server dhcp.
- Attivare se possibile il dhcp snooping sugli switch.
- Implementare autenticazione basata su 802.1x

IPv6 tools

- IPv6 autoconfiguration può creare problemi se non ben configurato.
- Esistono tools ad hoc per riconoscere situazioni in cui un client con indirizzi ipv6 si propone come "router della lan".
- Ipv6 mobility.

Tools

Configurazioni

- E' necessario avere una copia di backup delle configurazioni degli apparati di rete.
- Un'ottima soluzione è utilizzare un software di versionamento per conservare e storicizzare le configurazioni.
- Software opensource:
  - Svn
  - Git
  - Cvs
  - Mercurial

Snort

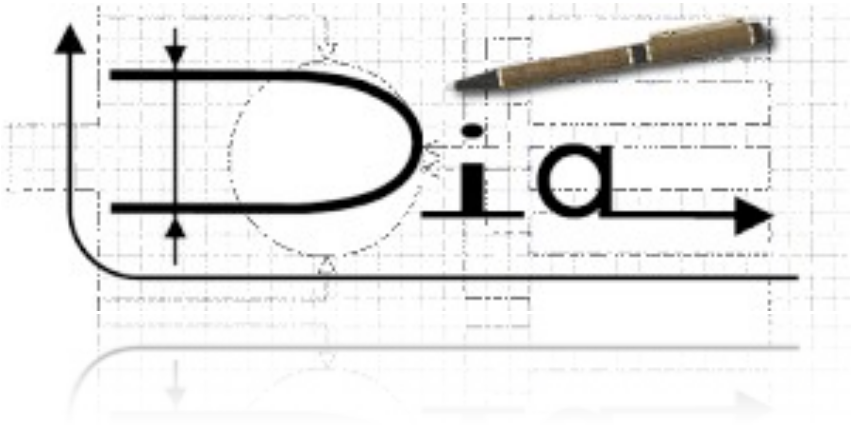
- Snort e' risultato la scelta vincente per identificare traffico anomalo e accessi non autorizzati verso computer della nostra rete.
- Numero basso di falsi positivi.
- Non e' possibile analizzare traffico crittografato.
- E' possibile utilizzare snort in due modalità: attivo/passivo

Ipplan

- Tool scritto in php pensato per semplificare la gestione del proprio spazio di indirizzamento IP.
- Permette di gestire la configurazione del dns, i file di configurazione di tutti gli apparati, e la memorizzazione di informazioni riguardanti l'hardware utilizzato.
- Può gestire una o più reti supportando anche la sovrapposizione di subnet uguali.

Dia

- Dia permette di disegnare il layout di rete.
- E' inspirato a Microsoft Visio ed è sviluppato in GTK.
- E' possibile salvare diagrammi in formato XML o qualsiasi formato di immagine.
- Multipiattaforma.



Conclusioni

Rumore

- E' fondamentale per un buono stato di salute della rete effettuare il network management.
- Il management genera "rumore di fondo".
- Richiede utilizzo delle infrastrutture per poter funzionare.
- E' necessario un buon tunning per evitare falsi allarmi.
- La rete e' controllata e gestita dalla rete.

DOMANDE?
RISPOSTE!

Giuseppe Augiero – giuseppe at ftgm.it -
Email: giuseppe at augiero.it Web: www.augiero.it

Grazie