

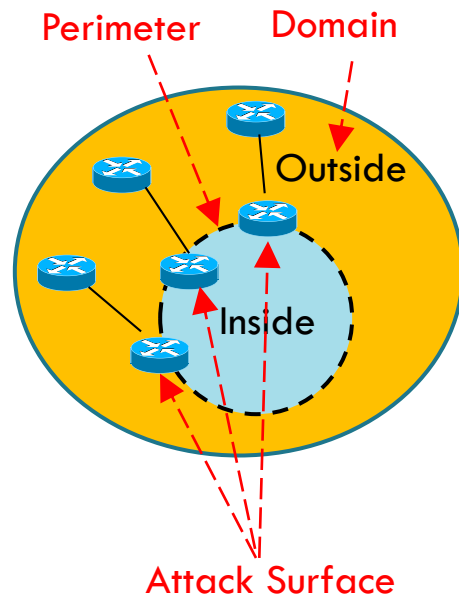
Monitoraggio e Network Analysis

Francesco Palmieri

fpalmieri@unisa.it

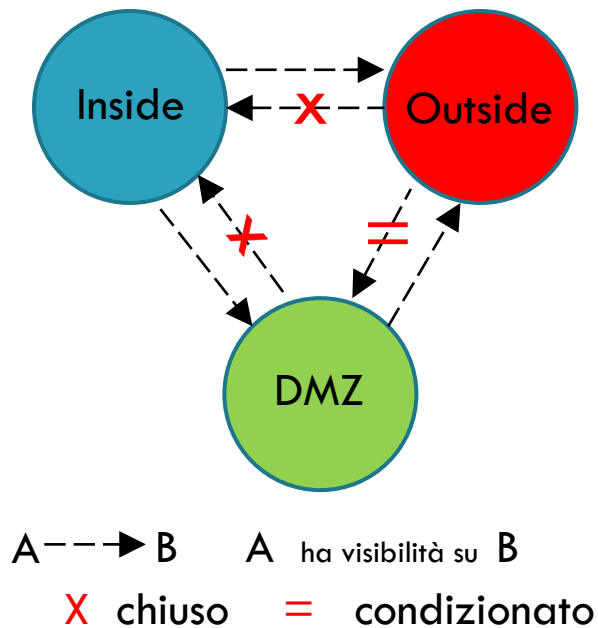
Domini, perimetro e superficie di attacco

- Un **dominio di sicurezza** è un insieme di entità/risorse da gestire come una singola zona/area di amministrazione in accordo a una politica di sicurezza comune, formalizzata attraverso specifiche regole di security enforcement)
- Un **perimetro** di sicurezza è il confine protetto tra il lato esterno e quello interno di un dominio di sicurezza
 - per esempio. una rete interna e il suo lato pubblico, in genere Internet
- Il perimetro può essere protetto da diversi dispositivi
- La **superficie di attacco** di un dominio è la somma dei diversi punti ("vettori di attacco") in cui un'entità non autorizzata ("attaccante") può tentare di inserire o estrarre dati o svolgere qualsiasi tipo di attività non autorizzata o ostile.
 - Contenere le dimensioni della superficie di attacco è una misura fondamentale alla base di qualsiasi politica di sicurezza

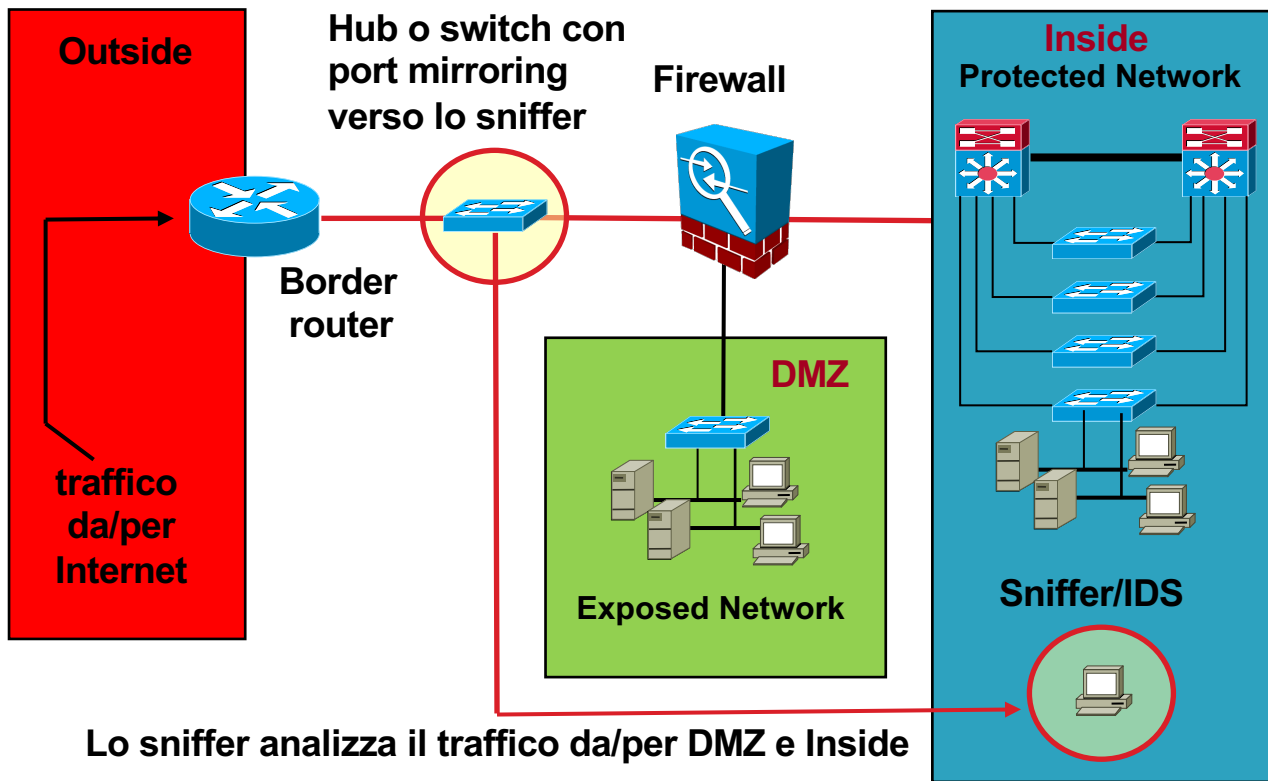


Domini di Sicurezza - Gerarchia

- A ogni dominio di sicurezza è assegnato un **grado di affidabilità** (trust) o **livello di sicurezza** che ne definisce le regole di visibilità rispetto agli altri
 - Un dominio con grado di trust maggiore può avere piena visibilità di quelli con grado inferiore
 - Viceversa la visibilità è bloccata a meno di specifiche eccezioni (filtraggio/regole di visibilità)
 - DMZ e INSIDE hanno piena visibilità su OUTSIDE
 - INSIDE ha piena visibilità su DMZ
 - Ogni altro accesso non è consentito



Architettura di base

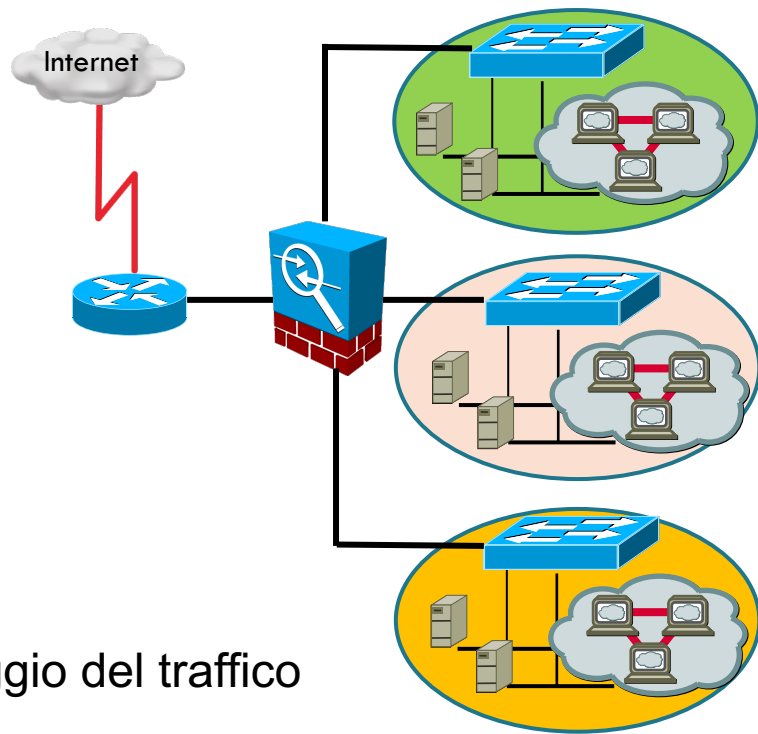


In una comune architettura di rete abbiamo almeno tre domini:

- Outside (tutto il mondo Internet esterno): grado di trust 0
- Inside (l'organizzazione interna da proteggere e nascondere): grado di trust 100
- DMZ (l'insieme di macchine interne che espongono servizi all'esterno): grado di trust $0 < x < 100$

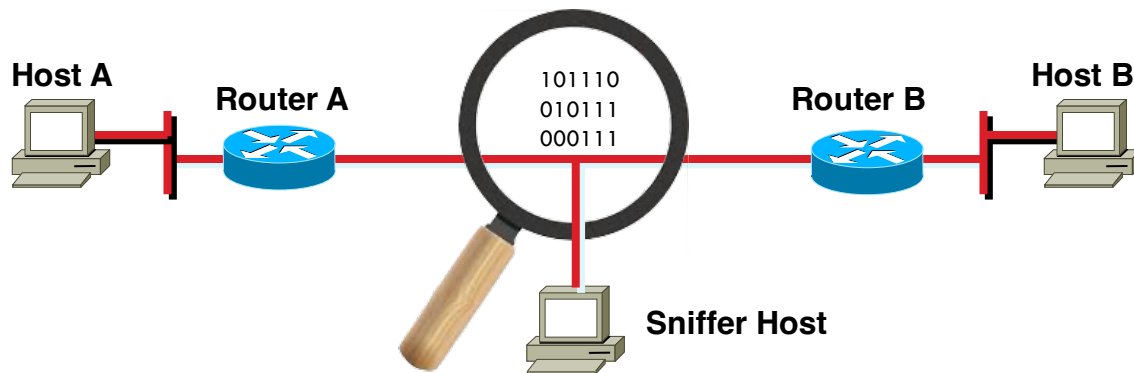
Router, Firewall e Sonda

- Un **router** è responsabile dell'inoltro del traffico tra rete interna ed Internet
 - E' il primo punto di sbarramento o demarcazione
 - Spesso di proprietà del provider
- Un **firewall** è un componente attivo di difesa perimetrale preposto a controllare il traffico fra due o più segmenti di rete:
 - Separazione di zone amministrativamente diverse (**domini di sicurezza**)
 - Filtraggio traffico fra le diverse zone tramite regole di visibilità fra domini (controllo accessi)
 - Mediazione accessi a specifiche applicazioni
- Una **sonda** garantisce la visibilità e il monitoraggio del traffico



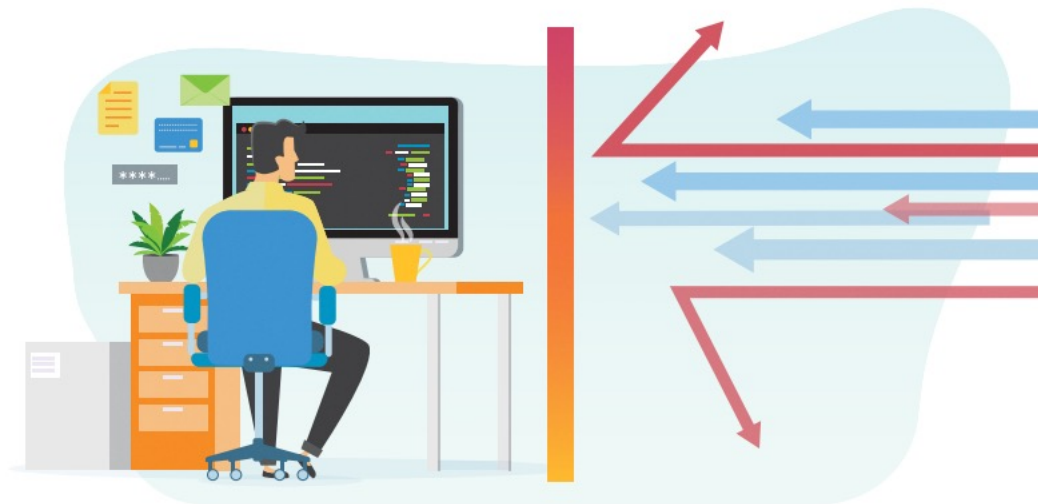
Osservare il Traffico: Sniffing

- Uno sniffer è un'applicazione software che è in grado di acquisire i pacchetti a livello datalink
- E' in grado di interpretare informazioni in chiaro riferite agli header di livello 2, 3 e 4 dei pacchetti nonché a protocolli di livello di applicazione quali: FTP, HTTP, etc.
- Un adattatore di rete (NIC/TAP) programmato ad hoc (promiscuous mode) legge tutti i pacchetti in transito



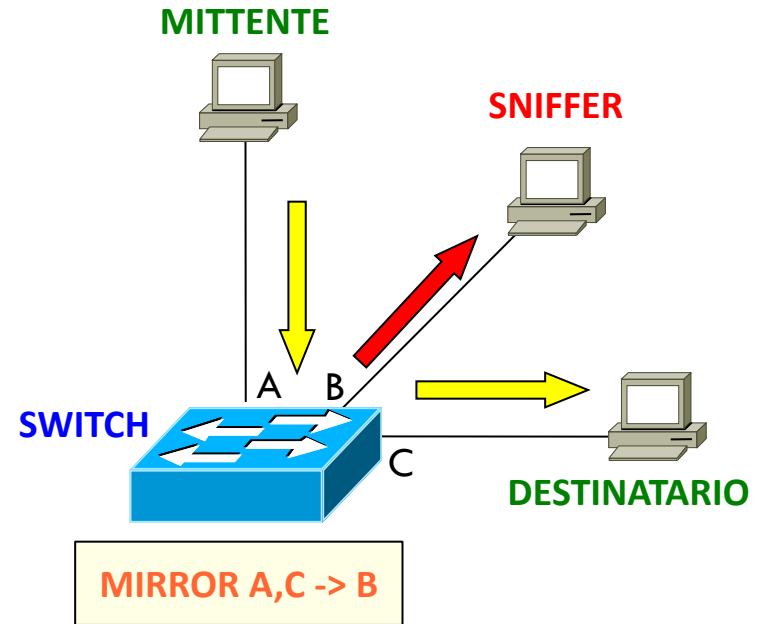
Applicazioni

- **Analisi automatica** della rete alla ricerca di specifici pattern es. passwords e nomi utente in chiaro: questo è un uso comune per gli hackers/crackers;
- **Analisi delle anomalie**: per scoprire eventuali problemi all'interno delle reti, come ad esempio, perchè il computer A non può comunicare con il computer B;
- **Analisi delle prestazioni**: per scoprire problemi o colli di bottiglia nelle reti;
- **Rilevazione delle intrusioni di rete**: così da rilevare attacchi o minacce in corso;
- **Registrazione del traffico di rete**: per creare logs delle transazioni in rete a disposizione per successive analisi “post-mortem”.



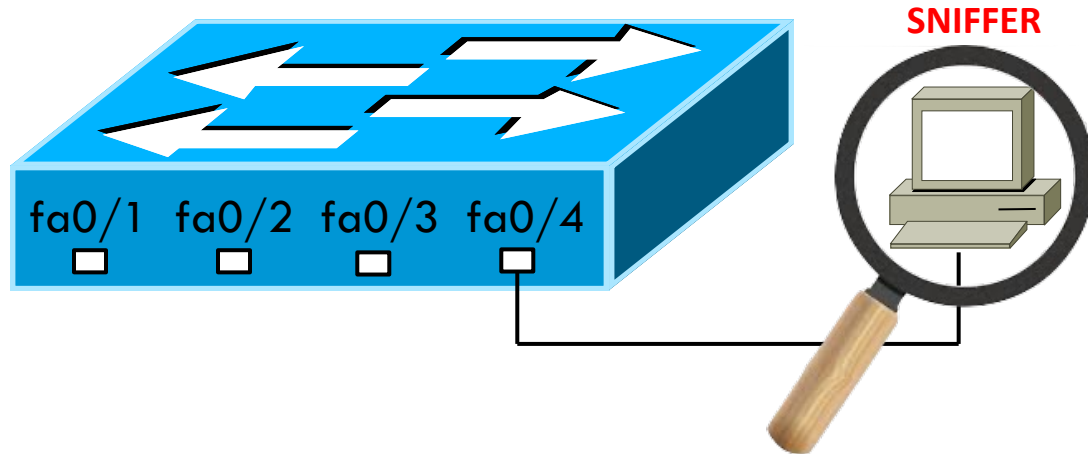
Sniffing su reti switched

- Su reti switched il traffico viene instradato secondo l'associazione MAC address + Porta, escludendo i terminali non interessati al traffico
- Pertanto uno sniffer è solo in grado di intercettare il traffico destinato alla macchina che lo ospita e quello broadcast
- L'alternativa è configurare la porta dello switch cui è connesso lo sniffer in modalita' mirroring, da quel momento replicherà tutto il traffico ricevuto da specifiche porte sulla porta dello sniffer



Configurazione Mirroring

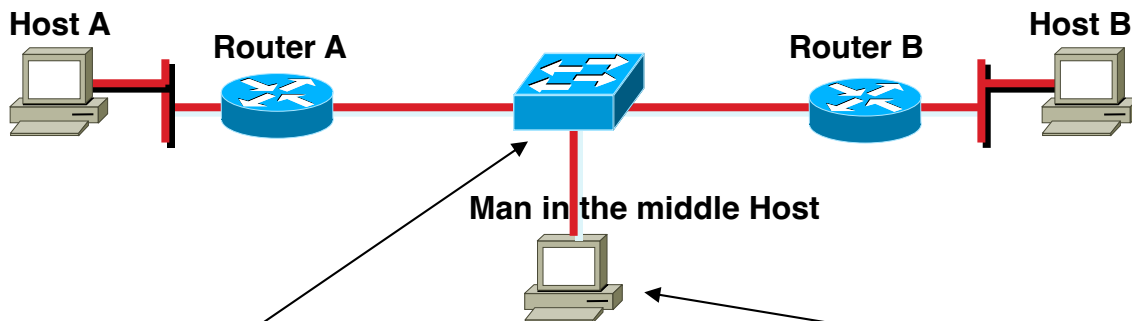
- Configurazione port mirroring di:
 - 1 porta su 1 porta
 - Range porte su 1 porta
 - Intera VLAN su una porta



```
Switch(config)#monitor session 1 source interface fa0/2
Switch(config)#monitor session 1 source interface fa0/1 - 3
Switch(config)#monitor session 1 source vlan 2
Switch(config)#monitor session 1 destination interface fa0/4
```

Cattura via port mirroring

- Il traffico che fluisce fra due reti va intercettato da un terzo componente (Man in the middle) prima attraverso la configurazione del port mirroring sullo switch di collegamento e analizzato con tcpdump per catturare ed esaminare traffico ftp

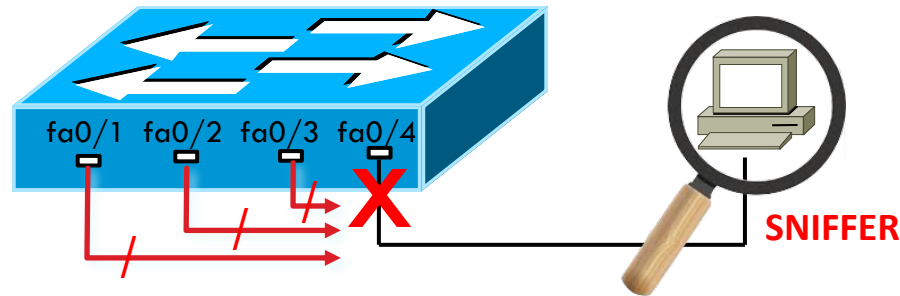


```
monitor session 1 source interface fa 1/0 - 2  
monitor session 1 destination interface fa 1/15
```

```
tcpdump -i eth0 port 21
```

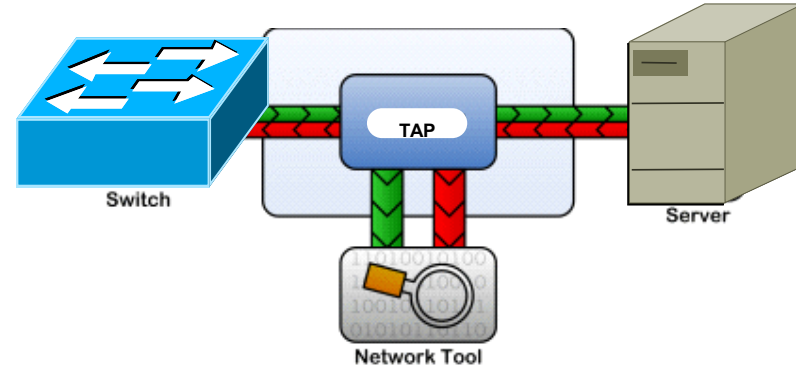
Sniffing senza port mirroring

- In assenza della funzionalità di port mirroring:
 - Uso di dispositivi repeater (bande limitate)
 - Disponibilità di sonde HW dedicate (TAP)
 - Diversione del traffico attraverso attacchi (ARP Poisoning)

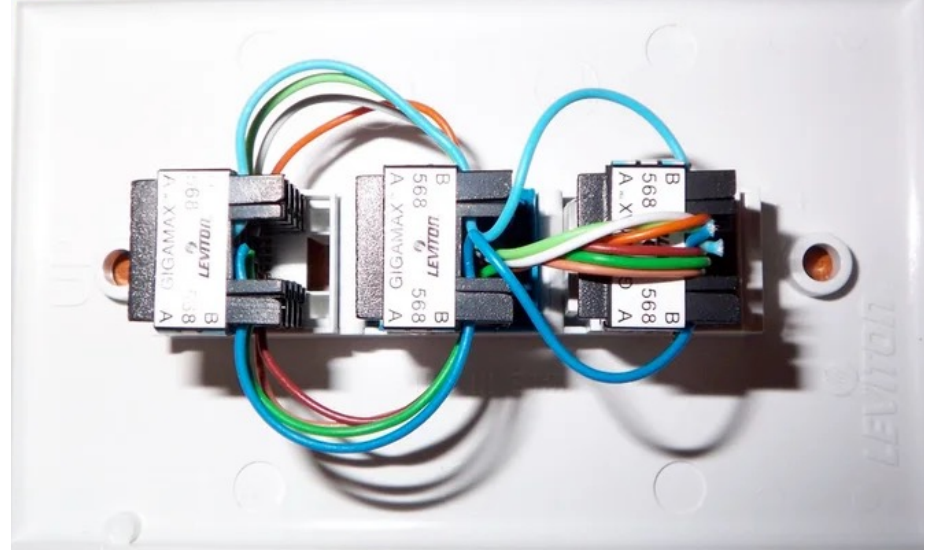
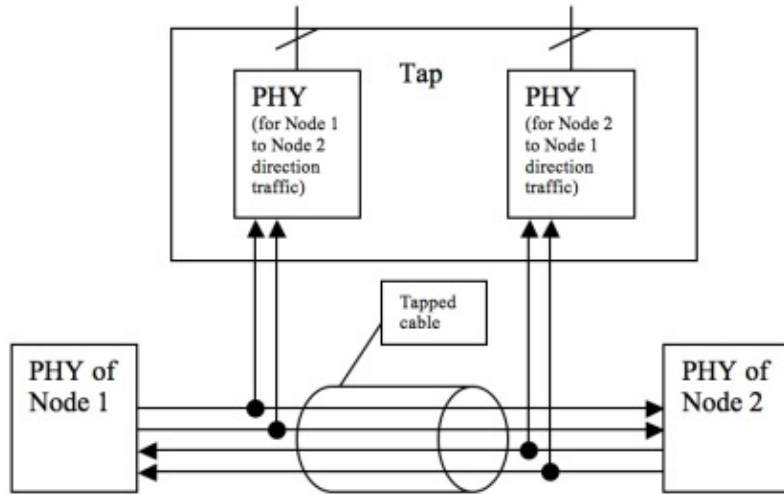


Traffic Access Port (TAP)

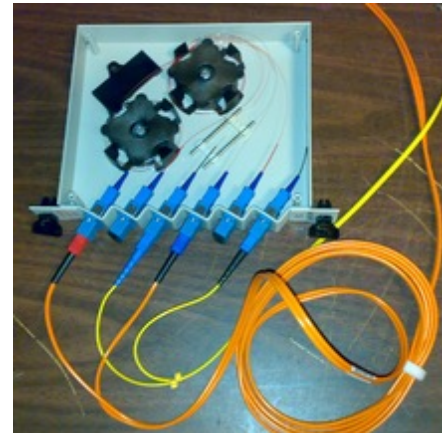
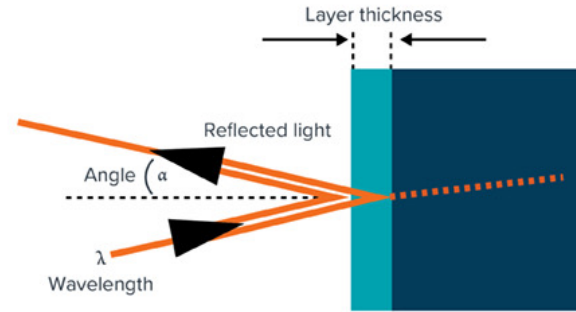
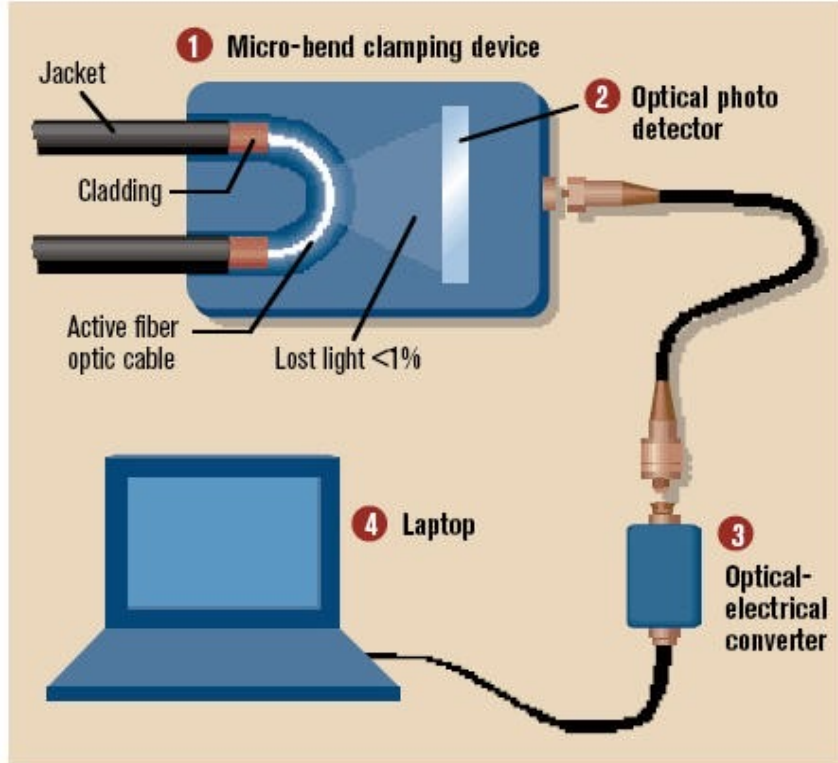
- Soluzione HW che fornisce una copia del traffico su una tratta fra 2 dispositivi
- Non richiede alimentazione elettrica
- Visibilità 100 % del Traffico Full Duplex incluso Errori o Anomalie a livello 1 & 2
- Totale isolamento e sicurezza dello sniffer
- Opera a livello 1 ed è molto facile da installare e gestire (spesso trasparente)
- Non richiede configurazioni specifiche su switch o server



Tap in rame

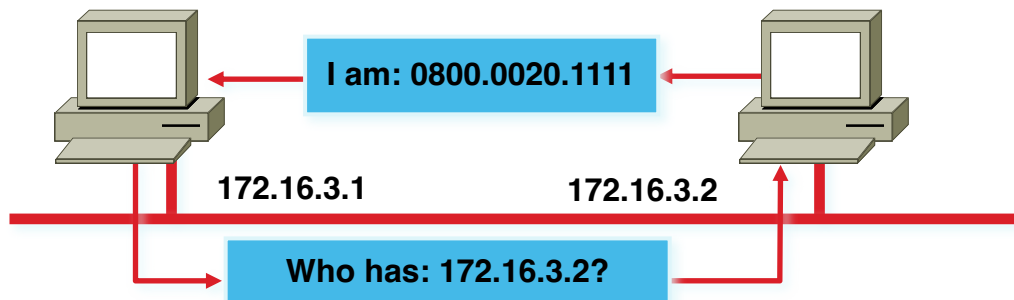


Tap Ottico



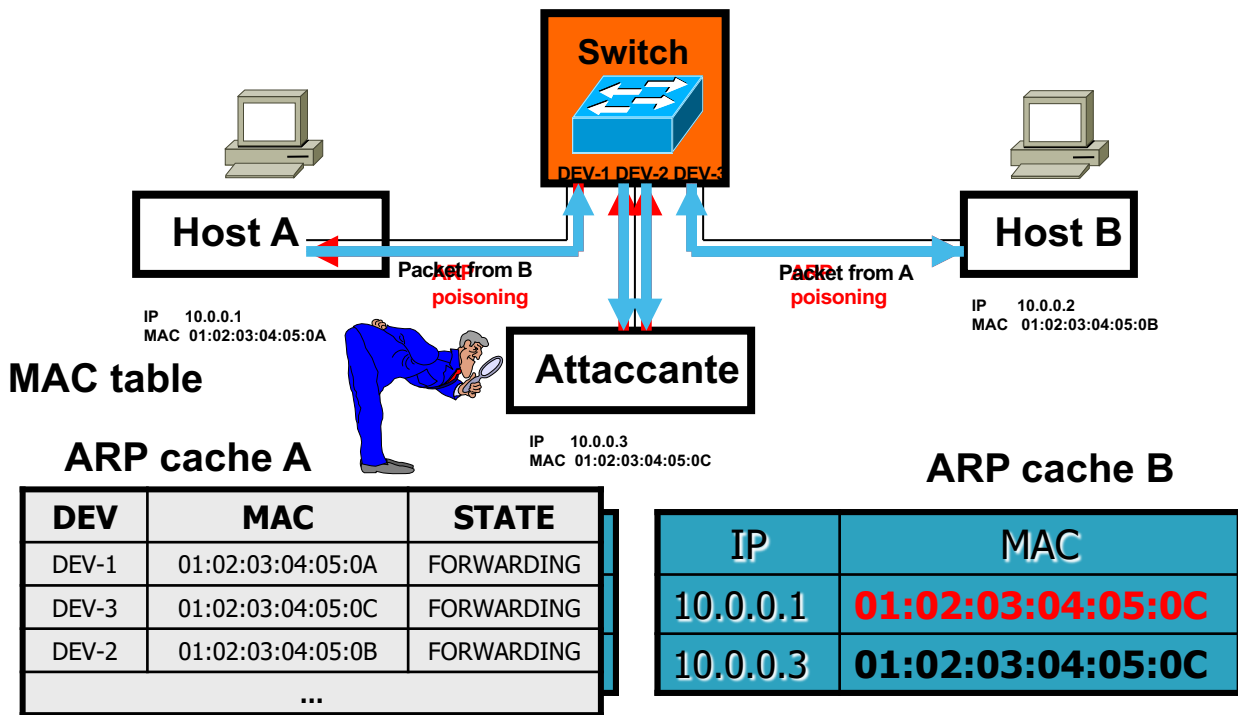
ARP Poisoning

- Il protocollo ARP (Address Resolution Protocol) si preoccupa di mappare i 32 bit di indirizzo IP (versione 4) in 48 bit di indirizzo ETH (MAC)
- Due tipi principali di messaggi:
 - ARP request (richiesta di risoluzione indirizzo IP)
 - ARP reply (risposta contenente un indirizzo eth)
- Le risposte sono memorizzate nella ARP CACHE, per limitare il traffico sulla rete



ARP poisoning

- Sfrutta il comportamento stateless del protocollo
- Se l'attaccante invia una ARP reply (spoofata) verso un host, questo la salverà nella propria ARP cache
- Le ARP reply sono salvate in cache anche se non erano state sollecitate (migliori prestazioni a discapito sicurezza)
- Le entries della cache sono provviste di timeout, quindi l'attaccante deve fare periodici "refresh"



Esempio

- Allavvio A e B dovranno scambiarsi dei messaggi che permettano di associare i loro indirizzi IP a quelli fisici Ethernet, mentre l'attaccante vedrà l'unico pacchetto:

```
16:38:36.501274 arp who-has 10.0.0.2 tell 10.0.0.1  
16:38:36.509581 arp reply 10.0.0.2 is at 08:00:20:77:4d:db
```

- Per intercettare una comunicazione bilaterale occorre lanciare due volte il programma:

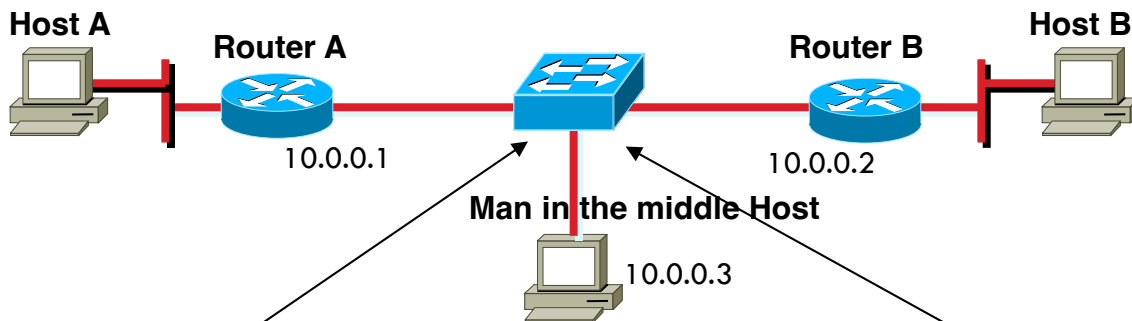
```
#!/arpspoof -i eth0 -t 10.0.0.1 10.0.0.2  
#!/arpspoof -i eth0 -t 10.0.0.2 10.0.0.1
```

- Affinché i pacchetti ritornino poi al reale destinatario occorre che l'attaccante li reinoltri verso la corretta destinazione

```
#echo 1 > /proc/sys/net/ipv4/ip_forward
```

Cattura via ARP poisoning

- Il traffico che fluisce fra due reti va intercettato da un terzo componente (Man in the middle) prima attraverso un attacco di ARP spoofing verso i 2 routers e analizzato con tcpdump per catturare ed esaminare traffico ftp



```
echo '1' > /proc/sys/net/ipv4/ip_forward  
cat /proc/sys/net/ipv4/ip_forward
```

```
arp spoof -i eth0 -t 10.0.0.1 10.0.0.2 2> /dev/null &  
arp spoof -i eth0 -t 10.0.0.2 10.0.0.1 2> /dev/null &
```

Necessità di strumenti di monitoraggio

- A seguito dell'evoluzione delle linee guida di sicurezza delle informazioni risulta estremamente utile dotarsi di uno strumento per il monitoring, l'analisi e la correlazione di eventi di sicurezza (ma non solo), a supporto della difesa attiva, della compliance e dell'analisi forense.
- Grandi quantità di dati prodotti dai sistemi di monitoraggio sono spesso inutilizzati fino all'evento negativo. Esistono strumenti per l'analisi e lo studio real-time delle direttrici di traffico sia opensource che commerciali.



Tcpdump: un semplice CLI sniffer

Sniffer: Strumento software o hardware che sfruttando il promiscuous mode cattura e consente l'analisi di tutti i pacchetti che attraversano un segmento di rete

tcpdump : Sniffer public domain basato su Berkeley packet filter (BPF)

Disponibile per il download: `ftp://ftp.ee.lbl.gov/tcpdump.tar.Z`

<u>23:06:37</u>	<u>10.1.101.1</u>	>	<u>224.0.0.10</u> :	<u>ip-proto-88</u>	<u>40</u>	<u>[tos 0xc0]</u>
time	source IP		dest IP	protocol	bytes	type of srv

Tcpdump: un semplice CLI sniffer

```
08:08:16.155 spoofed.target.net.7 > 172.31.203.17.chargen: udp
```

timestamp	src IP	src port	dst IP	dst port	protocol
-----------	--------	----------	--------	----------	----------

- gli hosts possono essere referenziati per nome o indirizzo IP
- le porte possono essere specificate per numero o nome del servizio
- per specificare un range di valori vanno indicizzati i bytes specifici

Tcpdump: espressioni

- Con le espressioni si definiscono i criteri coi quali scegliere i cosa visualizzare.
- Le expression consistono in una o più primitive precedute da “qualificatori”.

host sorgente o di destinazione:	<code>host spoofed.target.net</code>
rete di destinazione 172.31.x.x:	<code>dst net 172.31</code>
reti di destinazione 172.16 - 172.31:	<code>dst net 172 and (ip[17]>15) and (ip[17]<32)</code>
porta sorgente 7:	<code>src port 7</code>
porta destinazione 19:	<code>dst port chargen</code>
porta sorgente minore di 20:	<code>udp[0:2] < 20</code>
porta destinazione minore di 20:	<code>udp[2:2] < 20</code>

Tcpdump: qualificatori

- Type: host, net e port
 - Es. `'host 155.185.54.156'`, `'port 22'`, ecc.
- Dir: src, dst, src or dst
 - Es. `'src 155.185.54.156'`
- Proto: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp and udp
 - Es. `'tcp port 21'`, `'arp net 155.185.54'`

Esempi di pacchetti

```
# tcpdump 'port 23'
```

```
10.6.1.9.4548 > 10.6.1.2.23: S 2115515278:2115515278(0) win 32120 <mss 1460,  
  nop,nop,sackOK,nop,wscale 0> (DF)
```

```
10.6.1.2.23 > 10.6.1.9.4548: S 1220480853:1220480853(0)  
ack 2115515279 win 32120 <mss 1460,nop,nop,sackOK,nop,wscale 0> (DF)
```

```
10.6.1.9.4548 > 10.6.1.2.23: . ack 1220480854 win 32120 (DF)
```


Wireshark



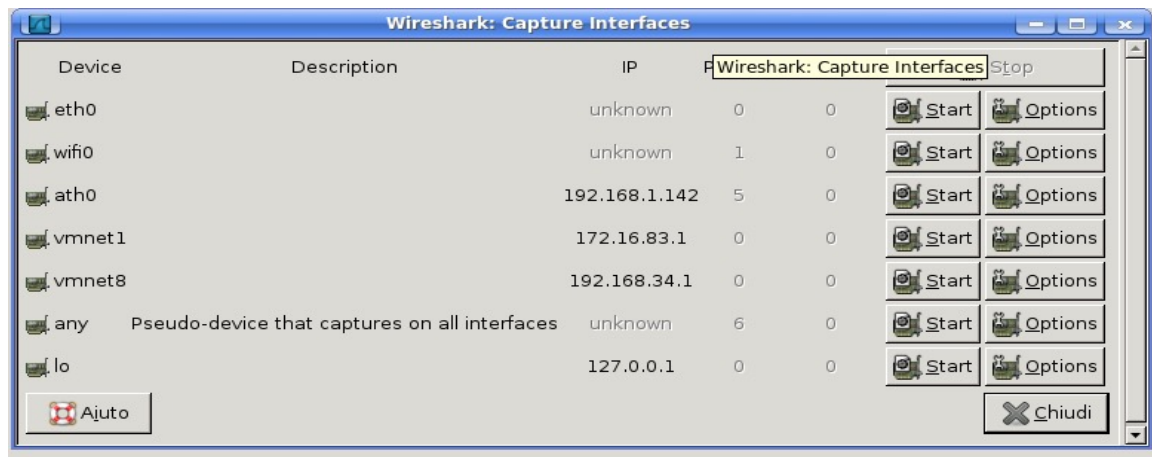
- Wireshark è un packet sniffer sofisticato di nuova generazione
- Ha funzioni di filtraggio e permette di osservare tutto il traffico presente su una rete.
- Individua gli incapsulamenti e riconosce tutti i singoli campi.
- Per la cattura non ha codice proprio, ma usa *libpcap/WinPcap*.
- È open source e compatibile con sistemi Unix e Windows.

Sito ufficiale: <http://www.wireshark.org/>

[Wikipedia: <http://it.wikipedia.org/wiki/Wireshark>]

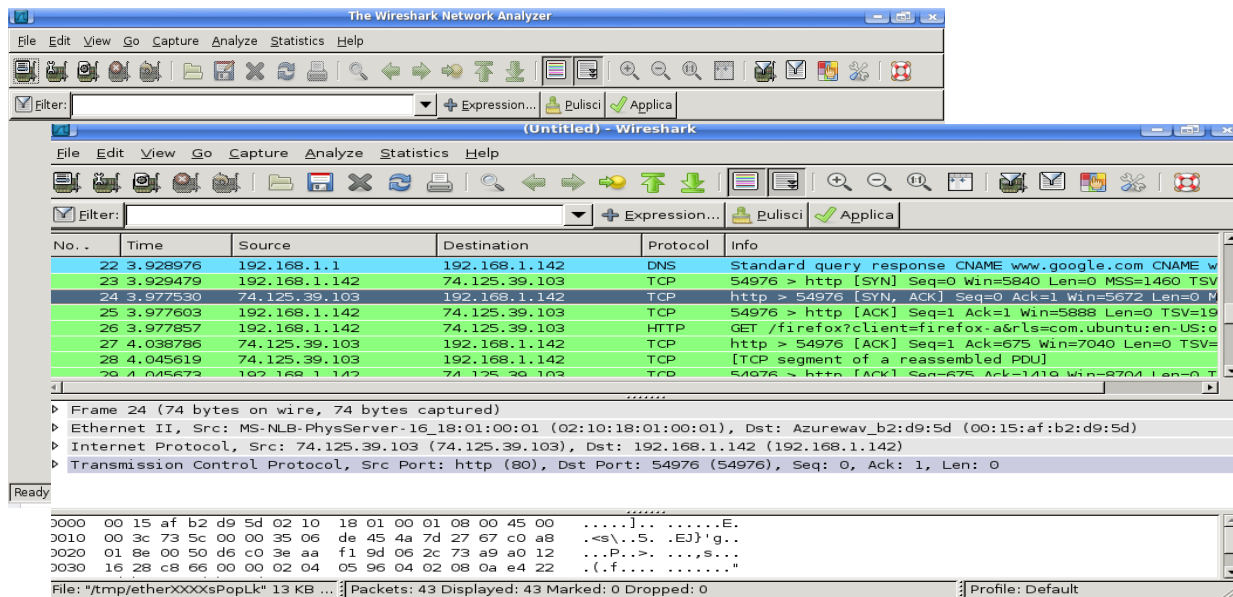
Wireshark

- Avviamo la nostra prima cattura, cliccando sul primo pulsante da sinistra:
- si aprirà la schermata di selezione delle interfacce dalla quale possiamo vedere tutte le interfacce sulle quali possiamo andare ad operare, modificare le opzioni relative ad ogni interfaccia o semplicemente avviare la cattura dei pacchetti direttamente con le opzioni di default.



Wireshark

- Una volta avviata la cattura, lo schermo passerà ad una suddivisione in tre sezioni, e ci si presenteranno tutta una serie di righe e dati, corrispondenti al traffico ethernet catturato,



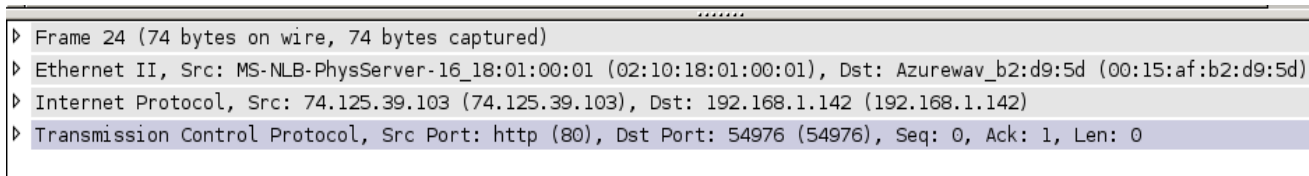
Wireshark

- Lo schermo e' diviso in tre sezioni, nella prima sezione (sommario), quella piu' in alto, abbiamo un' ulteriore suddivisione in colonne, esse rappresentano (da sinistra verso destra) :

No. .	Time	Source	Destination	Protocol	Info
22	3.928976	192.168.1.1	192.168.1.142	DNS	Standard query respons
23	3.929479	192.168.1.142	74.125.39.103	TCP	54976 > http [SYN] Seq
24	3.977530	74.125.39.103	192.168.1.142	TCP	http > 54976 [SYN, ACK
25	3.977603	192.168.1.142	74.125.39.103	TCP	54976 > http [ACK] Seq

- il numero progressivo del pacchetto
- il tempo intercorso tra l' inizio della cattura e l'arrivo del pacchetto
- chi ha generato il pacchetto (mac address o indirizzo ip)
- chi e' il destinatario del pacchetto (mac address, IP, broadcast)
- il protocollo utilizzato
- in questa sezione possiamo selezionare una singola riga da esplorare meglio

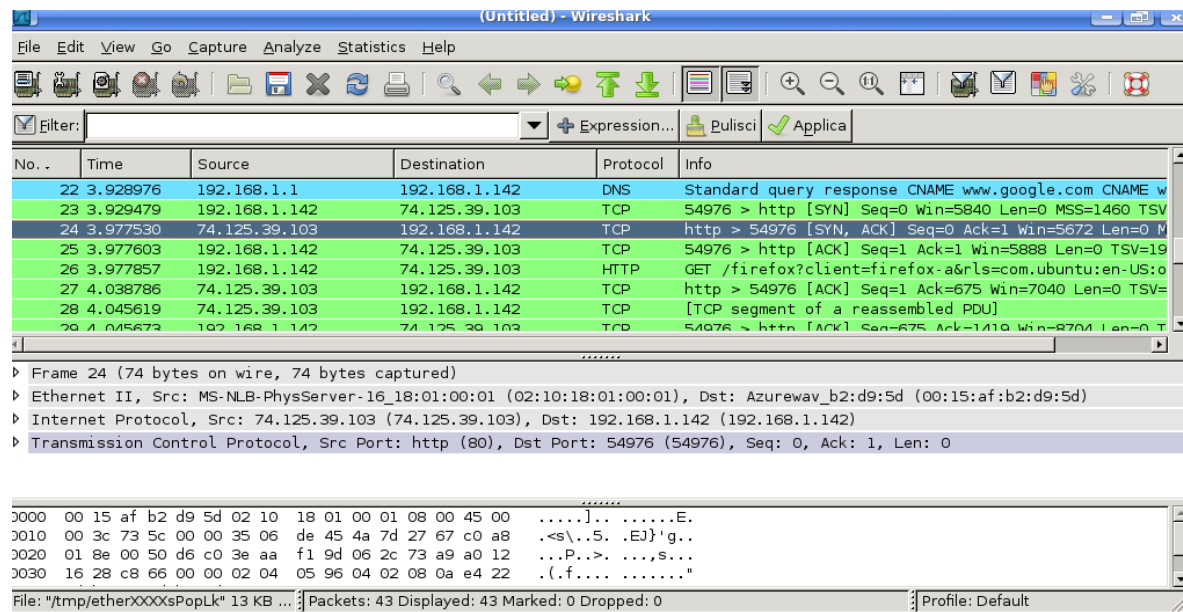
Wireshark



- Nella seconda sezione (protocollo) sono riportati dettagliatamente i dati relativi alla riga selezionata nella prima sezione,
 - possiamo quindi meglio vedere
 - il tipo di frame,
 - il protocollo dal quale proviene il frame,
 - l'indirizzo mac address sorgente e destinatario in forma estesa,
 - l'eventuale payload del frame ed altri dati utili, sempre organizzati secondo gerarchie ispezionabili tramite un click sul segno ▶ a lato

Wireshark

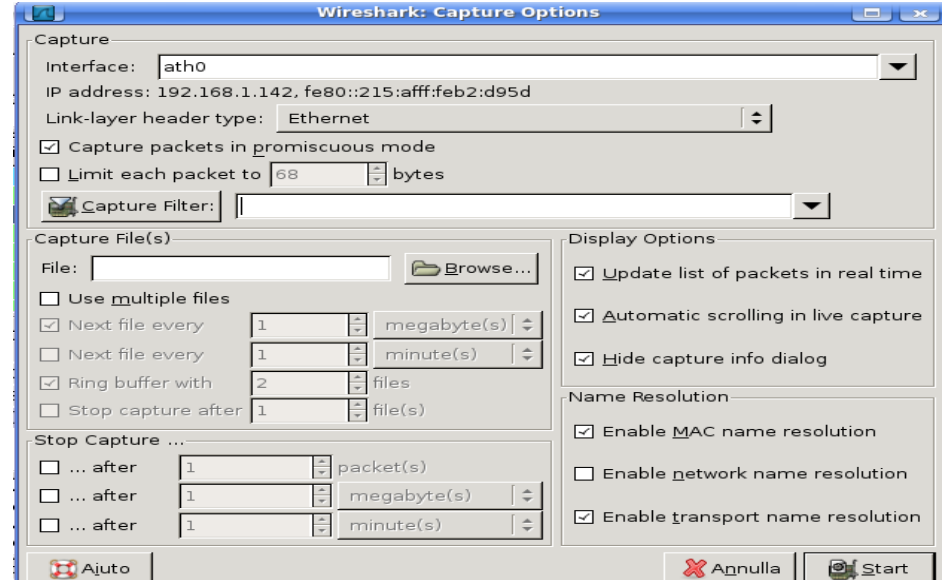
- Nella terza sezione (dati) invece vediamo il frame nativo, in formato hex e ascii, così per come e' acquiito dal driver di cattura direttamente sulla scheda ethernet, ed eventualmente evidenziati i byte relativi alla sezione selezionata precedentemente.



Wireshark: uso dei filtri



- Esistono due tipi di filtri:
 - filtri di visualizzazione
 - Permettono di visualizzare solo quanto definito dal filtro
 - filtri di cattura
 - Catturano solo i pacchetti che soddisfano i criteri definiti dal filtro



Wireshark: uso dei filtri

- I filtri di visualizzazione, oltre ad essere molto utili sono anche facilitati nell' utilizzo dall' esistenza di numerosi filtri preimpostati (pulsante Filter della barra dei filtri)



- Esiste anche un facilitatore che ci consente di scrivere con pochi clic nuovi filtri, accessibile pulsante “+ Expression” ,
- Mano mano che scriviamo nella riga dei filtri, essa cambierà colorazione in base alla correttezza di ciò che stiamo scrivendo.
- Una volta selezionato il filtro non ci resta che di applicarlo.
- Per eliminare un filtro basta cliccare sul pulsante “pulisci”

Wireshark: es. espressioni di filtraggio

Ecco alcune espressioni di filtraggio di uso comune:

- `eth.addr == ff:ff:ff:ff:ff:ff`
- `ip.addr == 192.168.1.7`
- `ip.src == 192.168.1.17 and ip.dst == 192.168.1.19`
- `ip.addr 192.168.1 and pop`
- `ip.addr 192.168.1 and messenger`

Wireshark: es. espressioni di filtraggio

- Se invece vogliamo filtrare tutti i pacchetti che non provengono/vanno verso un' IP, quindi l' opposto di

```
ip.addr==192.168.1.1
```

- saremmo tentati di usare:

```
ip.addr!=192.168.1.1
```

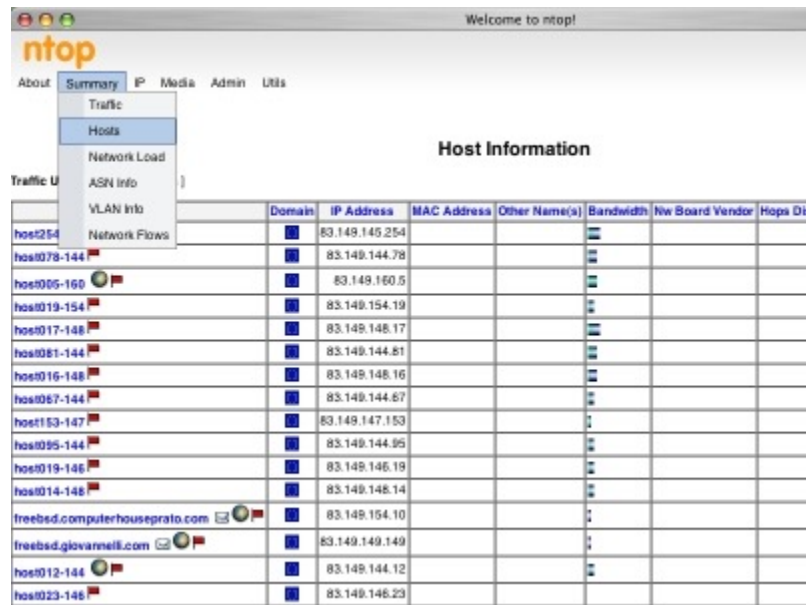
- il quale pero' non ci filtrera' niente!! L' espressione giusta da usare e' :

```
!(ip.addr == 192.168.0.1)
```

- La differenza tra le due righe se pur semanticamente giuste e' che usando l' operatore != chiediamo di eliminare le righe dove abbiamo l' indirizzo IP indicato, ma senza specificare se nel campo sorgente o destinatario.

Ntop

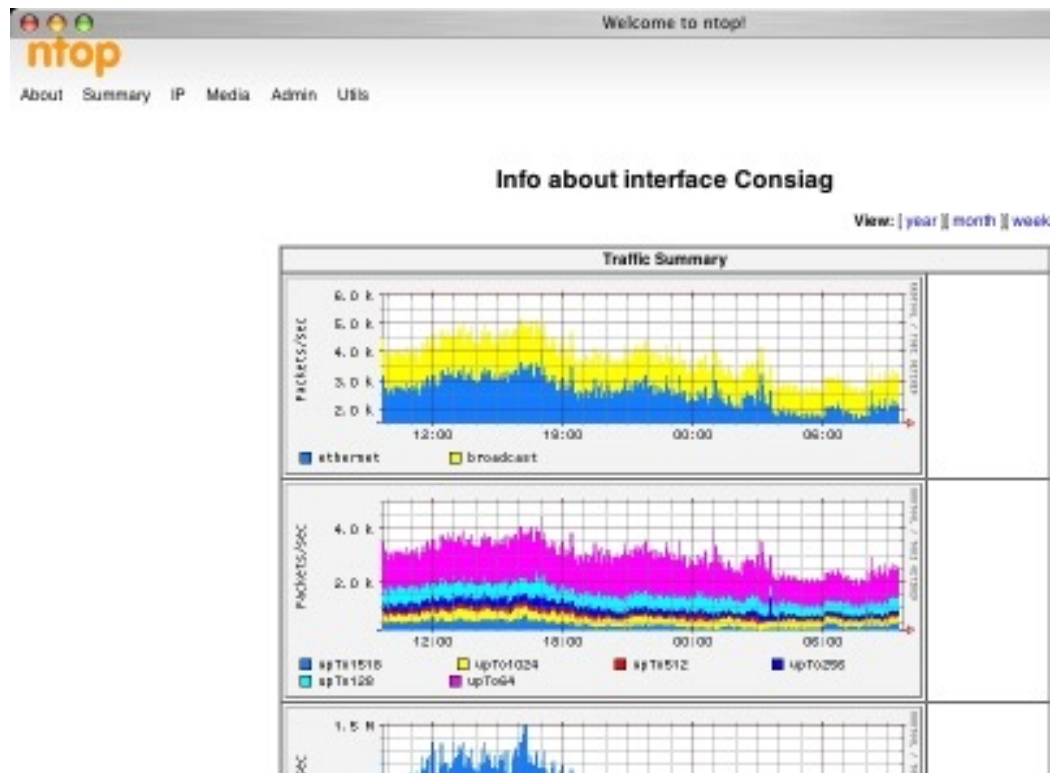
- ntop è una sonda per il traffico di rete che ne mostra l'utilizzo come fa il popolare comando top Unix.
- ntop è basato su libpcap ed è portatile per funzionare virtualmente su ogni piattaforma Unix o Windows.
- Gli utenti di ntop possono utilizzare un browser Web per navigare attraverso le informazioni sul traffico di ntop (che funge da server Web) e ottenere un dump dello stato della rete.



The screenshot shows the ntop web interface. The top navigation bar includes links for About, Summary, IP, Media, Admin, and Utils. A dropdown menu is open under 'Summary', showing options for Traffic, Hosts, Network Load, ASN Info, and VLAN Info. The 'Hosts' option is selected. The main content area is titled 'Host Information' and displays a table of network hosts. The table has columns for Host, Domain, IP Address, MAC Address, Other Name(s), Bandwidth, Net Board Vendor, and Hops Dis. The table lists various hosts, including those with IP addresses in the 83.149.145.0/24 range and some with domain names like freebsd.computerhouseprato.com and freebsd.giovannelli.com.

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Net Board Vendor	Hops Dis
host0254		83.149.145.254					
host0078-144		83.149.144.78					
host0005-160		83.149.160.5					
host0019-154		83.149.154.19					
host0017-148		83.149.148.17					
host0081-144		83.149.144.81					
host0016-148		83.149.148.16					
host0067-144		83.149.144.67					
host0153-147		83.149.147.153					
host0095-144		83.149.144.95					
host0019-146		83.149.146.19					
host0014-148		83.149.148.14					
freebsd.computerhouseprato.com		83.149.154.10					
freebsd.giovannelli.com		83.149.149.149					
host0012-144		83.149.144.12					
host0023-148		83.149.148.23					

Ntop



Sniffing su dispositivi di rete

- La funzionalità di debugging può essere usata per visualizzare i pacchetti in transito
- E' buona pratica effettuare debug selettivo basato su ACL

```
access-list 100 permit ...  
debug ip packet detail 100
```

- E' consigliabile usare gli internal buffers e non la console

```
logging buffered 64000 debugging
```

- E' sempre necessario controllare il carico di CPU indotto!

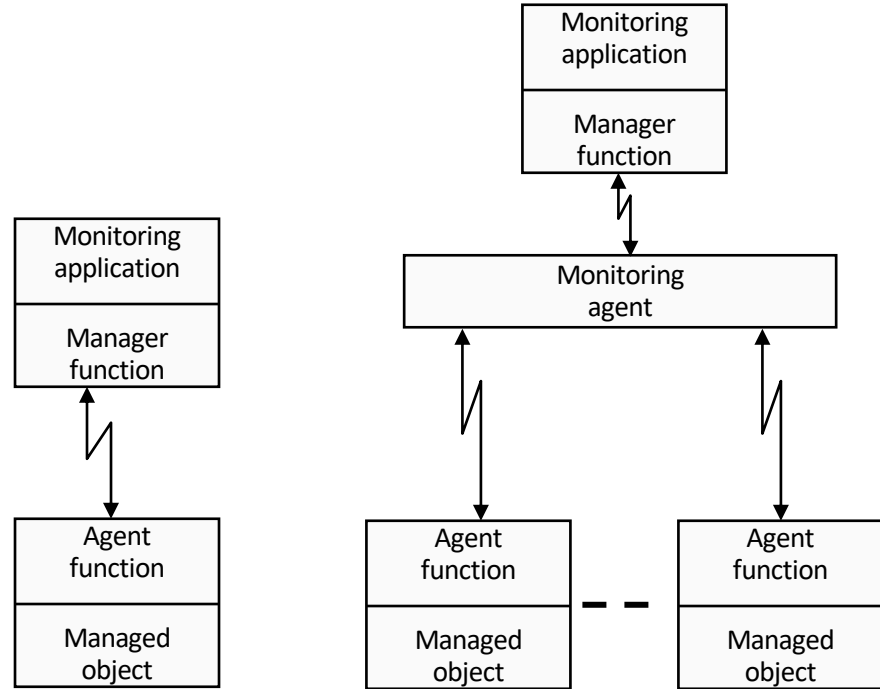
Sniffing su dispositivi di rete

- Esempio

```
R2(config)#access-list 155 permit icmp any any
R2(config)#do debug ip packet detail 155
IP packet debugging is on (detailed) for access list 155
R2(config)#
*Mar 1 01:17:16.039: IP: tableid=0, s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2
(Loopback0), routed via RIB
*Mar 1 01:17:16.043: IP: s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2, len 100, rcvd 4
*Mar 1 01:17:16.047: ICMP type=8, code=0
*Mar 1 01:17:16.047: IP: tableid=0, s=2.2.2.2 (local), d=10.1.1.1
(FastEthernet0/0), routed via FIB
*Mar 1 01:17:16.051: IP: s=2.2.2.2 (local), d=10.1.1.1 (FastEthernet0/0), len 100,
sending
*Mar 1 01:17:16.055: ICMP type=0, code=0
*Mar 1 01:17:16.095: IP: tableid=0, s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2
(Loopback0), routed via RIB
```

Network monitoring

- Le architetture per il network monitoring sono strutturate accord a un modello Manager-Agent
 - La funzione di management interfaccia l'applicazione
 - L'agente di management interfaccia l'oggetto da monitorare
 - Un agente di monitoraggio può aggregare più funzioni agente associate a oggetti multipli



Modello Manager-agent

Modello di aggregazione

Polling e event reporting

- Le informazioni vengono raccolte e archiviate da agenti e usate da multipli sistemi di management
- Due tecniche possibili
 - **polling** : Interazione request-response fra manager e agent
 - querying periodica di ogni agent con richiesta dei valori degli elementi di interesse
 - Ogni agent risponde con informazioni dalla propria MIB
 - **event reporting** : iniziativa dell'agent con il manager che ascolta e raccoglie
 - Notifica di cambiamenti di stato
 - Reporting periodico preconfigurato dal manager
 - Generazione di report in presenza di eventi significativi o inusuali (es., un guasto))
 - Più efficiente del polling per monitorare oggetti il cui stato cambia poco di frequente

Osservazione del traffico via SNMP

- E' possibile monitorare i dati statistici aggregati di traffico di una rete attraverso il protocollo SNMP
- Nell'esempio che segue viene fatta una query a una specifica MIB associata ad un'interfaccia ottenendo informazioni su volumi di traffico in ingresso e uscita

```
% snmpwalk -v2c -c test 10.106.65.131 1.3.6.1.2.1.2.2.1.16.7 IF-MIB::ifOutOctets.7  
= Counter32: 1874894  
  
% snmpwalk -v2c -c test 10.106.65.131 1.3.6.1.2.1.2.2.1.10.7 IF-MIB::ifInOctets.7  
= Counter32: 2275304
```

- L'osservazione di come i volumi di traffico variano nel tempo può fornirci informazioni di grande interesse per la sicurezza di una rete

Osservazione del traffico via SNMP

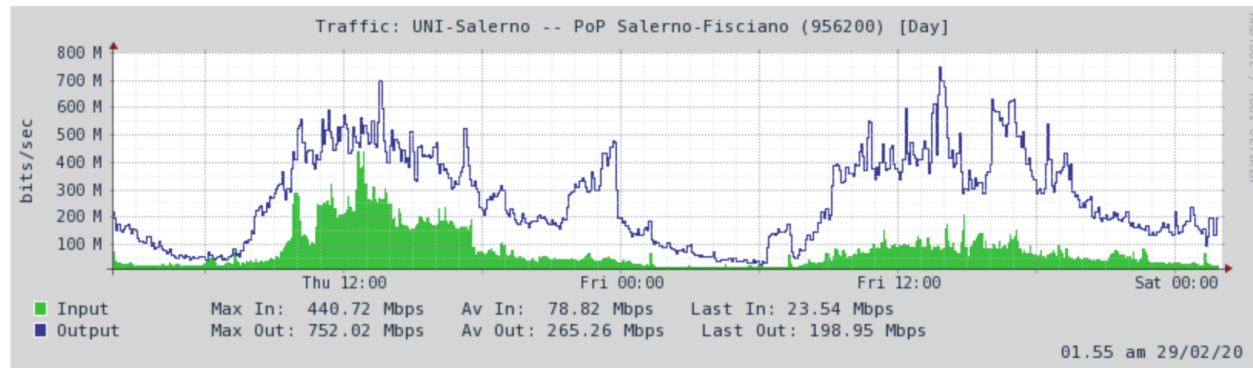
- Tools come **MRTG** o **CACTI** si occupano di collezionare in automatico le statistiche SNMP di utilizzo della banda di tutte le interfacce degli apparati presenti in rete.
- I contatori di ciascuna interfaccia vengono letti ogni 5 min (letura SNMP temporizzata via **cron**) e salvati su log file (1 logfile/interfaccia):
 - Rappresentazione Grafica del Throughput
 - **LoadMap**: ci permette di visualizzare “at a glance” il Livello di Carico degli **Uplink** di tutti gli apparati di rete

Osservazione del traffico via SNMP

UNI-Salerno -- PoP Salerno-Fisciano (956200)

close

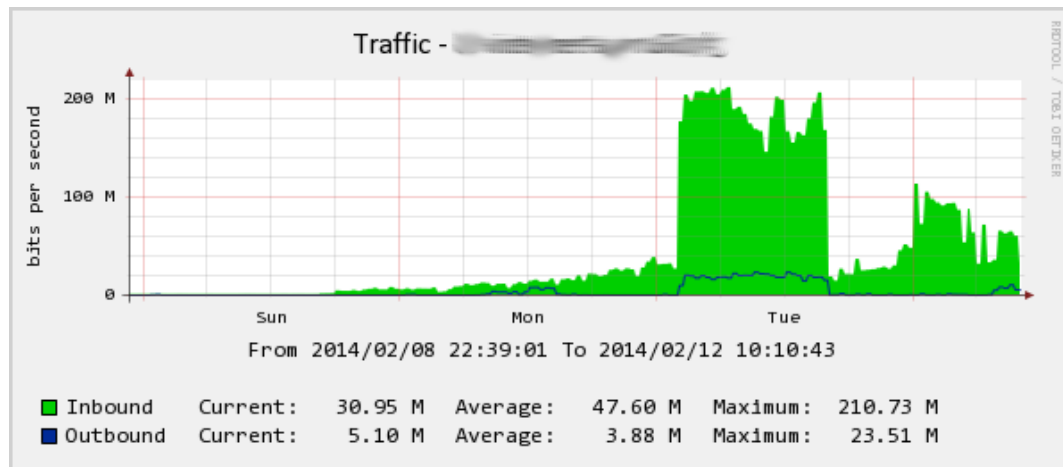
Link name	Use	BW	Side A	Side B	Target options
UNI-Salerno -- PoP Salerno-Fisciano	access	10,00 Gbps	UNI-Salerno 193.204.219.202	PoP Salerno-Fisciano rx1.sa.garr.net (MX480) irb.200 193.204.219.201	



- Osservando l'andamento del traffico è possibile farsi un'idea del comportamento «normale» di una rete (**baseline**)

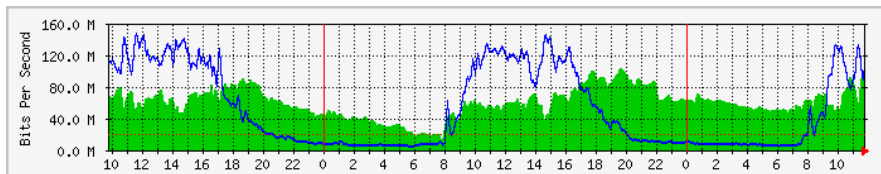
Identificazione Attacco

- E' facile riconoscere attacchi «volumetrici» identificando plafond sostenuti di traffico che esulano dal comportamento normalmente osservato

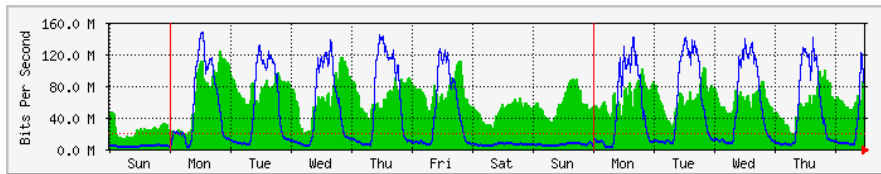


- Questa attività può essere facilmente automatizzata attraverso semplici funzioni di monitoraggio associate a MRTG o CACTI che generano allarmi (mail, SMS, etc.) su base superamento di **specifiche soglie** di traffico

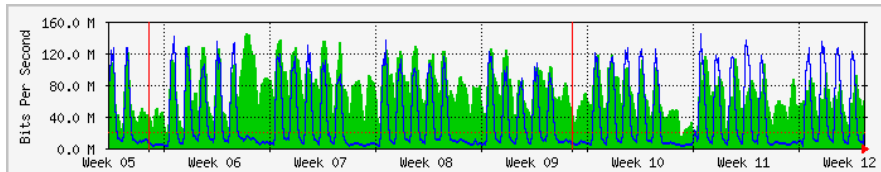
Attenzione al contesto!



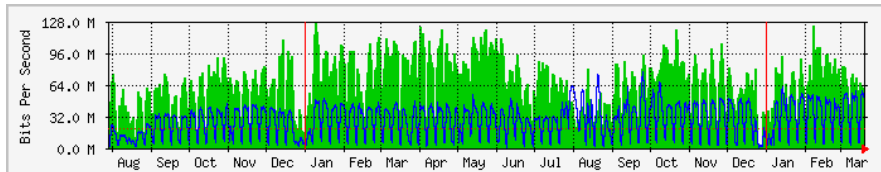
Day



Week



Month



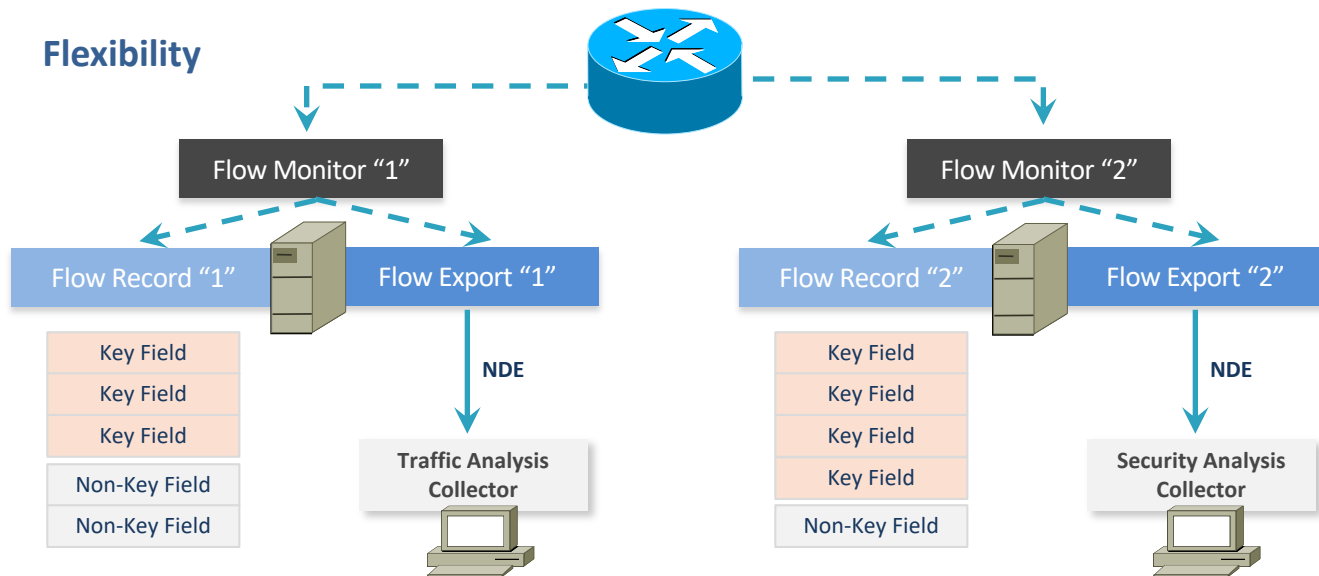
Year

- Questa analisi può essere semplicistica e va sempre legata al contesto
 - Conoscere i profili di traffico che caratterizzano l'infrastruttura o il collegamento
 - Considerare l'inquadramento temporale e i fenomeni di ricorrenza
 - Tenere conto di eventi straordinari o situazioni particolari

Osservazione del traffico via Netflow

- Tutti i dati di traffico possono essere raccolti ed inviati periodicamente da ciascun router a un apposito data-collector per successive analisi
- Con l'analisi dei flussi di traffico riusciamo a capire chi la sta utilizzando le risorse di rete (host conversation) e come (protocol):
 - Top Speaker / Top Conversation
 - Top Application (web, dns, gridFTP, P2P, GRE, ...)
 - Security Analysis: identificazione attività di rete non autorizzate
 - Troubleshooting
 - Traffic Engineering

Osservazione del traffico via Netflow



Osservazione del traffico via Netflow

- Le informazioni sui flussi si ottengono abilitando sugli apparati di rete gli agenti:
 - Netflow (Cisco): per **IP** interface (Full/Sampled Mode)
 - J-Flow (JunOS)
 - sFlow (standard): per port (Extreme Sampled Mode)
- L'agente Netflow salva le informazioni sui flussi in una cache e periodicamente le esporta verso un collettore/analizzatore.

Osservazione del traffico via Netflow

- E' possibile osservare anche a livello di CLI il dettaglio aggregato dei flussi di traffico individuando dati di origine, destinazione, protocolli, porte e volumi di traffico

```
#show ip cache flow
```

```
...
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Fa4/0/0    192.132.34.17  AT1/0/0.1  148.240.104.176 06 080C 1388    1
Fa4/0/0    192.132.34.17  AT1/0/0.1  63.34.210.22    06 0AEB 0666   15K
Fa4/0/0    192.132.34.17  AT1/0/0.1  216.207.62.22   06 0FD2 0578  7195
Fa4/0/0    143.225.231.7  AT1/0/0.1  143.225.255.255 11 007F 007D    1
Fa4/0/0    192.132.34.17  AT1/0/0.1  148.240.104.176 06 0015 1381   13
Fa4/0/0    192.132.34.17  AT1/0/0.1  148.240.104.176 06 0015 1382   12
Fa4/0/0    192.133.28.7   AT1/0/0.1  164.124.101.44  11 0035 0035    2
Fa4/0/0    143.225.209.72 AT1/0/0.1  209.178.128.121 01 0000 0000  561K
Fa4/0/0    192.133.28.7   AT1/0/0.1  192.5.5.242     11 0035 0682    1
Fa4/0/0    192.133.28.1   AT1/0/0.1  198.41.0.4       11 0444 0035    1
Se6/7      156.14.1.122   AT1/0/0.1  130.186.1.53    11 0035 0035    1
Fa4/0/0    192.132.34.17  AT1/0/0.1  61.159.200.203  06 0553 042F   75
Fa4/0/0    192.132.34.17  AT1/0/0.1  61.159.200.203  06 052C 0428  12K
...
```

Origine

Destinazione

Volume Traffico

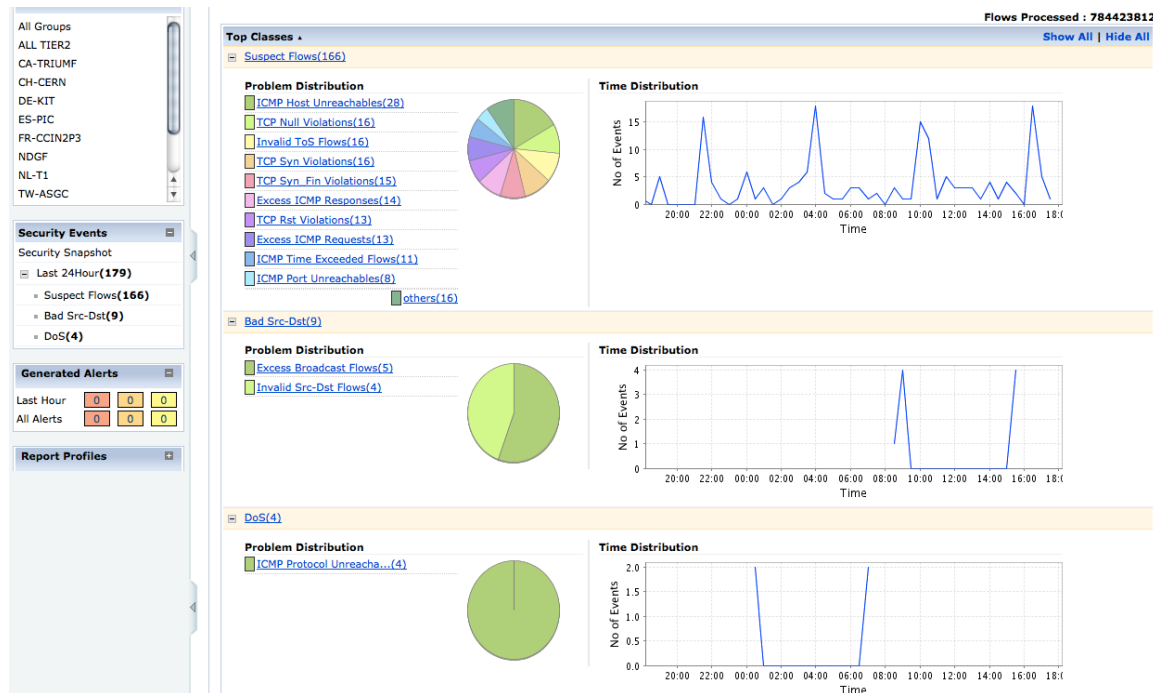
Osservazione del traffico via Netflow

The screenshot displays a Netflow analysis tool interface. On the left, there are three sidebar panels: 'Device Group' (showing 'All Devices sw-104-05' and a 'Google Map View' button), 'IP Group' (listing various groups like 'ALL TIER2', 'CA-TRIUMF', etc.), and 'Security Events' (showing 'Last 24Hour(254)', 'Suspect Flows(236)', 'Bad Src-Dst(13)', and 'DoS(5)'). The main panel is titled 'T1-GENERAL' and has tabs for 'Traffic', 'Application', 'Source', 'Destination', 'QoS', and 'Conversation' (which is selected). Below the tabs, there are filters for 'IN' and 'OUT' traffic, a 'Last 15 Minutes' time range, and 'From' and 'To' date/time selectors (both set to 2011-05-17 18:20 to 18:35). The main data area shows a table of traffic records with columns: 'Resolve DNS | Show Network', 'Group by' (set to 'None'), 'Src IP', 'Dst IP', 'Application', 'Port', 'Dst Port', 'Protocol', 'DSCP', and 'Traffic'. The table lists 25 records of traffic, all using TCP and Default DSCP, with traffic volumes ranging from 2.79 GB to 16.17 GB.

Resolve DNS Show Network	Group by	Src IP	Dst IP	Application	Port	Dst Port	Protocol	DSCP	Traffic
	None	131.154.130.4	140.181.0.12	TCP_App	1095	62832	TCP	Default	16.17 GB
	None	131.154.130.5	140.181.0.12	TCP_App	1095	1033	TCP	Default	12.07 GB
	None	131.154.130.66	192.101.161.156	TCP_App	58800	23540	TCP	Default	8.3 GB
	None	131.154.130.75	147.156.116.239	TCP_App	42565	24421	TCP	Default	6.64 GB
	None	131.154.130.67	192.101.161.155	TCP_App	51069	24223	TCP	Default	6.41 GB
	None	131.154.130.66	193.48.85.41	TCP_App	60751	24579	TCP	Default	4.59 GB
	None	131.154.130.67	192.101.161.156	TCP_App	44155	24936	TCP	Default	4.44 GB
	None	131.154.130.66	192.101.161.158	TCP_App	36851	23355	TCP	Default	4.35 GB
	None	131.154.130.66	192.101.161.155	TCP_App	53877	24118	TCP	Default	4.32 GB
	None	131.154.130.67	192.101.161.157	TCP_App	40485	24501	TCP	Default	3.56 GB
	None	131.154.130.67	193.48.85.40	TCP_App	34209	24676	TCP	Default	3.53 GB
	None	131.154.130.66	193.48.85.40	TCP_App	34995	24672	TCP	Default	3.52 GB
	None	131.154.130.67	192.101.161.158	TCP_App	44087	21291	TCP	Default	3.44 GB
	None	131.154.130.4	193.206.184.7	TCP_App	1095	41395	TCP	Default	2.96 GB
	None	131.154.130.67	193.48.85.41	TCP_App	42535	24578	TCP	Default	2.95 GB
	None	131.154.130.67	134.61.24.77	TCP_App	50232	21934	TCP	Default	2.81 GB
	None	131.154.130.66	193.40.150.227	TCP_App	52264	33822	TCP	Default	2.81 GB
	None	131.154.130.66	193.40.150.225	TCP_App	48442	46254	TCP	Default	2.81 GB
	None	131.154.130.66	192.101.161.160	TCP_App	37637	24109	TCP	Default	2.79 GB
	None	131.154.130.66	134.61.24.78	TCP_App	50128	24159	TCP	Default	2.79 GB
	None	131.154.130.67	141.108.36.204	TCP_App	33348	22390	TCP	Default	2.79 GB
	None	131.154.130.66	134.158.132.100	TCP_App	50522	24383	TCP	Default	2.79 GB

- Strumenti di analisi più sofisticati offrono un'ottima alternativa web-based alla CLI tradizionale

Osservazione del traffico via Netflow



- Attraverso un'interfaccia grafica più espressiva diventa più semplice identificare flussi anomali e situazioni patologiche
- Grafici e filtri specifici facilitano il compito dell'analista

Osservazione del traffico via Netflow

Device Group

- All Devices
- sw-104-05
- Google Map View

IP Group

- All Groups
- ALL TIER2
- CA-TRIUMF
- CH-CERN
- DE-KIT
- ES-PIC
- FR-CCIN2P3
- NDGF
- NL-T1
- TW-ASGC

Security Events

- Security Snapshot
- Last 24Hour(182)
- Suspect Flows(169)
- Bad Src-Dst(9)
- DoS(4)

Generated Alerts

- Last Hour
- All Alerts

Report Profiles

Event List

[Show Filter](#)

Ignore Events | View Ignored | Discard Flows | View Discarded | More Actions ▾ [Show DNS](#) **Flows Processed : 784522279**

Report Details 1 - 25 Per Page : 25

<input type="checkbox"/>	ID	Problem (Manage)	Offender(s)	Routed via	Target(s)	Time ▲	Hits		
<input type="checkbox"/>	1398	Suspect Flows - Excess Empty UDP Packets	1: [192.84.143.158]	1: [CISCO-7600 (TenGigabitEthernet3/3)]	61: [131.154.3.0, 131.154.3.5, 131.154.3.9, 131.154.3.10, 131.154.3.11, 1...	2011-05-16 18:10:30 --- 2011-05-16 18:10:31	100		View
<input type="checkbox"/>	1397	Suspect Flows - Excess Empty UDP Packets	1: [192.84.143.158]	1: [CISCO-7600 (TenGigabitEthernet3/3)]	59: [131.154.3.0, 131.154.3.1, 131.154.3.2, 131.154.3.3, 131.154.3.4, 131...	2011-05-16 18:10:26 --- 2011-05-16 18:10:30	100		View
<input type="checkbox"/>	1399	Suspect Flows - ICMP Host Unreachables	20: [128.2.0.249, 130.79.208.209, 131.154.8.2, 131.154.129.15, 137.112.40...	2: [NEXUS-7018 (Vlan1), NEXUS-7018 (Ifindex151060608)]	38: [10.0.1.188, 10.10.208.4, 10.10.208.41, 10.100.208.8, 10.100.208.14, ...	2011-05-16 18:02:24 --- 2011-05-16 18:10:54	100		View
<input type="checkbox"/>	1396	Suspect Flows - Excess ICMP Requests	48: [1.225.30.57, 2.95.196.82, 46.174.114.3, 61.163.164.241, 61.188.185.8...	3: [CISCO-7600 (Vlan1), CISCO-7600 (TenGigabitEthernet3/3), CISCO-7600 (V...	35: [10.154.110.254, 131.154.0.28, 131.154.0.138, 131.154.0.157, 131.154....	2011-05-16 17:30:55 --- 2011-05-16 17:39:17	100		View
<input type="checkbox"/>	1395	Suspect Flows - TCP Null Violations	68: [50.63.248.142, 74.55.97.21, 77.47.192.50, 79.38.0.230, 85.195.108.70...	12: [NEXUS-7018 (Vlan1002), NEXUS-7018 (Vlan1), NEXUS-7018 (Vlan1001), NE...	60: [128.142.162.83, 128.142.216.110, 128.142.241.45, 131.154.3.201, 131....	2011-05-16 17:07:36 --- 2011-05-16 17:08:55	100		View
<input type="checkbox"/>	1394	Suspect Flows - TCP Rst Violations	73: [128.142.167.74, 128.142.167.209, 128.142.241.45,	11: [NEXUS-7018 (Vlan216), NEXUS-7018 (Vlan1002), NEXUS-7018	50: [50.63.248.142, 72.8.174.28, 74.55.97.21, 85.195.108.70,	2011-05-16 17:06:46 --- 2011-05-16 17:07:42	100		View

- E diventa immediato isolare i singoli flussi sospetti per esaminare i fenomeni in dettaglio