Monitoraggio di rete, in pratica

Luca Deri
Traduzione a cura di Emanuele Tomasi

Indice

1 Introduzione al testo

Il testo che segue è la traduzione, in italiano, delle slide "Network Monitoring in Practice" del professor Luca Deri. Le slide originali possono essere scaricate dal link http://luca.ntop.org/Teaching/tm2010.pdf.

La traduzione non è stata fatta in maniera del tutto fedele: alcune volte sono state fatte delle aggiunte volte a chiarire (si spera) meglio i concetti.

In questo primo capitolo verranno spiegati alcuni argomenti di background che nel testo sono dati per scontato.

1.1 TODO

Cosa da inserire in questo capitolo:

- Pila ISO/OSI
- TCP handshake
- Header IP
- VLAN
- Cosa fa e a che livello (ISO/OSI) opera:
  - hub
  - bridge
  - switch
  - router
- Due righe su SNMP (architettura agent-manager) e MIB
- Com'è fatto un cavo di rete (RX/TX, etc...)
- Come funziona una ethernet (CMSA e CMSA/CD)

Cose da inserire nel glossario:

- Benchmark
- Frame Relay
- NAT
- CDP
- Failover
- IPX
- NeBEUI
- RTP
- NetBIOS
- AppleTalk
- TCP
- UDP
- ICMP
- MPLS
- SCTP
- IDS

- BPF
- MRGT
- SAP
- SPAM
- Workstation
- SMTP
- ICMP
- Backbone
- NIC
- NPU

Una volta fatto il glossario vanno controllate le note a piè di pagina ed eliminati i termini che sono stati spostati nel glossario.

2 Introduzione

2.1 Esigenze del monitoraggio

- Garantire la disponibilità delle funzioni di rete.
  - Gestione dei servizi (disponibilità, tempi di risposta) necessari a far fronte cambiamenti ai tecnologici e ad un incremento dei dati.
    - Sicurezza dei servizi attraverso il controllo dei componenti di sicurezza.
    - Prevenzione degli errori (umani) e identificazione/recupero dei colli di bottiglia.
  - Reazione automatica o semi-automatica alle anomalie.
    - Modifica della configurazione, in real-time, in caso di errori.
    - Attivazione di componenti ridondanti in caso di errori.
- Reazione dinamica ai cambiamenti dell'ambiente e della rete.
  - Cambiamenti riguardanti applicazioni, utenti, componenti, servizi.
  - Adattamento dinamico della larghezza di banda di trasmissione disponibile secondo le richieste fatte dal sistema gestionale.
- Controllo della rete.
  - Collezione e (compressa) rappresentazione delle informazioni di rete importanti.
  - Definizione e manutenzione di un database delle configurazioni di rete.
  - Quando è possibile, centralizzazione del controllo sulle periferiche e delle funzioni implementate (central management console).
  - Integrazione di procedure gestionali su ambienti eterogenei.
- Miglioramento delle condizioni di lavoro degli amministratori di sistema/rete.
  - Migliorare e standardizzare gli strumenti disponibili.
  - Identificare e implementare una graduale automazione delle funzioni di amministrazione.
  - Buona integrazione degli strumenti nelle sequenze operazionali esistenti.
- Andare verso la standardizzazione.
  - Transizione delle esistenti, spesso proprietarie soluzioni, verso un ambiente standardizzato.

2.2 Vari attori, varie metriche

- Utenti finali verso (Internet) Service Provider.
  - Utente finale (dial-up o xDSL) verso AOL[1].
    - Utenza internet (nessun servizio).
    - Per lo più traffico P2P (Peer-to-peer), Email, WWW.
  - ntop.org verso Telecom Italia.
    - Fornisce servizi (es. DNS, mail, WWW).
    - Connesso ad un ISP regionale (no ramo globale).
  - Interroute/Level3 verso Telecom Italia.
    - Necessità di acquistare la larghezza di banda necessaria per utenti nazionali.
    - Necessita di firmare uno SLA (Service Level Agreement) per i consumatori influenzati dal contratto SLA con il vettore globale.

2.3 Esigenze degli utenti finali

- Monitorare la performance delle applicazioni.
  - Come mai le pagine web ci mettono così tanto a caricarsi?
  - Perché il video in multicast non è fluido?
  - Controllare che lo SLA aspettato può essere fornito dall'infrastruttura di rete disponibile.
    - Ho sufficiente larghezza di banda e risorse di rete per le mie necessità e aspettative?
  - La scarsa performance è "normale" o ci sono degli attacchi o attività sospette?
    - C'è un virus che prende molte delle risorse disponibili?
    - C'è qualcuno che scarica molti file ad alte priorità (cioè monopolizza la larghezza di banda)?

2.4 Esigenze del service provider

- Monitorare lo SLA e le attività di rete correnti.
- Applicare lo SLA e controllare le eventuali violazioni.
- Individuare problemi o errori di rete.
- Ridisegnare la rete e i suoi servizi basandosi sui feedback degli utenti e sui risultati del monitoraggio.
- Fare delle previsioni per pianificare l'uso futuro della rete e quindi implementare le estensioni prima che sia troppo tardi (scavare per mettere cavi o fibre prende molto tempo).

2.5 I problemi

- Gli utenti finali e l'ISP parlano linguaggi differenti.
  - Gli utenti finali capiscono i servizi di rete.
    - Outlook non può aprire la mia mailbox.
    - Mozilla non è capace di connettersi a Google.
  - L'ISP parla di reti.
    - Gli annunci BGP (Border Gateway Protocol) contengono dati sbagliati.
    - La connessione internet principale è al 90% occupata.
    - C'è bisogno di firmare un contratto con l'AS (Automous System) XYZ per risparmiare la larghezza di banda.

[1] La America On Line (AOL) è il più importante ISP (Internet Service Provider) del mondo.

2.6 Applicazioni per l'analisi del traffico: qualche esigenza

- Cosa: misurazione del volume e della velocità delle applicazioni host analizzando le conversazioni.
  Perché: identificare la crescita e gli eventi anormali che occorrono in rete.
- Cosa: gruppi di traffico personalizzabili attraverso gruppi logici (es: compagnie, classi di utenti), geografia (es: regioni), sottoreti.
  Perché: associare il traffico con le entità business e il trend di crescita per i gruppi (i dati aggregati non sono molto importanti in questo contesto: si ha bisogno di analizzare i dati a livello utente).
- Cosa: filtri parametrizzabili e eccezioni basate sul traffico di rete.
  Perché: i filtri possono essere associati alle notifiche di allarmi di eventi anomali occorsi in rete.
- Cosa: periodi di tempo personalizzabili in modo da aiutare il report giornaliero (cosa è successo nella giornata).
  Perché: analizzare i dati in base al calendario aiuta ad identificare i problemi (es: il DHCP (Dynamic Host Configuration Protocol) finisce gli indirizzi ogni lunedì mattina tra le 9 e le 10, ma il problema non si presenta durante tutto il resto della settimana).

2.7 Ulteriori problemi di misurazione

- Le apparecchiature di rete hanno una limitata capacità di misurazione (un router deve prima switchare i pacchetti).
  - Sono limitate a pochi protocolli selezionati.
  - Eseguono misurazioni aggregate (ad esempio per interfacce).
  - Solo alcune possono essere usate per misurazioni di rete (ad esempio un router è troppo carico da nuovi compiti, lo switch di livello 2 non è amministrabile via SNMP).
  - Reti ad alta velocità introducono nuovi problemi: gli strumenti di misurazione non possono far fronte all'alta velocità.
  - C'è la necessità di sviluppare costantemente nuovi servizi e applicazioni (ad esempio il video sui telefoni 3G).
  - Molti servizi non sono pensati per essere monitorati.
  - Molto del traffico internet viene consumato da quelle applicazioni (P2P) che sono pensate per rendere difficile l'individuazione e l'accounting.
  - I servizi internet moderni sono:
    * Mobili e quindi non legati ad un posto o ad un indirizzo IP.
    * Criptati e basati su porte dinamiche TCP/UDP (nessuna impronta digitare, cioè il mappaggio 1:1 tra porta e servizio).

2.8 Monitorare le capacità delle attrezzature di rete

- Sistemi finali (ad esempio PC Windows).
  - Completamente sotto il controllo dell'utente.
  - Semplici strumenti (solo installazione di nuove applicazioni).
- Apparecchiature di rete standard (ad esempio i router ADSL).
  - Accesso limitato ai soli operatori di rete.
  - Scarse capacità di misurazione.
  - Solo dati aggregati (ad esempio per interfaccia).
- Apparecchiature personalizzate (Measurement Gears).
  - Capaci di collezionare dati specifici.
  - Problemi di dislocamento a volte ne impediscono l'installazione dove fluisce molto traffico.

2.9 I problemi

- Gli utenti chiedono la misurazione dei servizi.
- Gli strumenti di rete forniscono misurazioni semplici e aggregate.
- Non si può sempre installare gli strumenti dove si vuole (problemi di cablaggio, problemi di privacy).
- Nuovi protocolli nascono ogni mese e gli strumenti di misurazione sono statici e lenti ad evolversi.

2.10 Terminologia per il benchmark

- Le metriche per il traffico sono spesso non standardizzate, al contrario delle metriche della vita quotidiana (ad esempio i litri, i kg, etc. . .).
- Le misurazioni proprietarie sono spesso fatte in maniera differente tra loro rendendo i risultati difficili da comparare.
- Le RFC 1242 "Benchmarking Terminology for Network Interconnection Devices" definiscono qualche metrica comune usata nella misurazione del traffico.

2.10.1 RFC 1242: qualche definizione

- Throughput.
- Latenza (latency).
- Velocità di perdita di frame (frame loss rate).
- Dimensione dei frame a livello di data link (datalink frame size).
- Back-to-back.
- etc. . . .

Le RFC sono veramente generali, non "formali/precise"

2.10.2 Le RFC 2285: "Benchmarking Terminology for LAN Switching Devices"

- Estende le RFC 1242 aggiungendo definizioni che possono essere usate in altre RFC, includendo:
  - Burst del traffico (traffic burst).
  - Carico/sovraccarico della rete (network load/overload).
  - Velocità di forwarding (forwarding rate).
  - Frame errati (errored frame).
  - Broadcast.

2.10.3 Le RFC 2432: "Terminology for IP Multicast Benchmarking"

- RFC peculiari, mirate alla misurazione del traffico multicast.
- Qualche metrica:
  - Forwarding e throughput (ad esempio Aggregated Multicast Throughput).
  - Overhead (ad esempio Group Join/Leave Delay).
  - Capacità (ad esempio Multicast Group Capacity).

2.10.4 RFC 1944 e 2544: Metodologie di benchmarking per i dispositivi di rete interconnessi

Le RFC 1944: Definisce come fare le misurazioni del traffico di rete:

- Come testare le architetture (dove sistemare i sistemi sotto test).
- Dimensione dei pacchetti usati per le misurazioni.
- Gli indirizzi IP da assegnare ai SUT (System Under Test - sistemi sotto test).
- Protocolli IP da usare per il test (ad esempio UDP, TCP).
- Uso del burst del traffico durante le misurazioni (burst verso traffico costante).

In parole povere definisce l'ambiente di testing da usare per l'analisi del traffico di rete.

Le RFC 2544: Definisce e specifica come:

- Verificare e valutare i risultati dei test.
- Metriche di misurazione comuni definite nelle RFC 1242 come:
  - Throughput.
  - Latenza (latency).
  - Perdita di frame (frame loss).
- Gestire i "modificatori dei test" come:
  - Traffico di broadcast (come questo traffico influenza i risultati).
  - Durata del test (quanto tempo dovrebbe durare il test).

2.10.5 Altre RFC per le metodologie di benchmarking (BM - Benchmarking Methodology)

- 2647/3511: BM per le performance dei firewall.
- 2761/3116: BM per l'ATM (Asynchronous Transfer Mode).
- 2889: BM per i dispositivi di LAN (Local Area Network) switching.
- 3918: BM per IP Multicast.

2.11 Metriche di misurazione comuni

- Misurazione della performance:
  - Disponibilità.
  - Tempo di risposta.
  - Accuratezza.
  - Throughput.
  - Utilizzo.
  - Latenza e Jitter.

2.11.1 Disponibilità

- La disponibilità può essere espressa come la percentuale di tempo che un sistema di rete, componente o applicazione, è disponibile per un utente.
- È basata sull'affidabilità del componente di rete individuale.

$$\%disponibilità = \frac{MTFB}{MTFB + MTTR} \times 100$$

MTFB = mean time betwen failures (tempo medio tra i fallimenti).
MTRR = mean time for repair following failure (tempo medio per rimediare ai fallimenti).

Si noti che, indipendentemente dal tempo medio tra i fallimenti, più è basso il tempo medio per rimediare ai fallimenti e più la disponibilità arriva verso il 100%. Ovviamente però, se il tempo medio tra i fallimenti tende a 0, allora anche la disponibilità tende a zero (si hanno continui fallimenti).

2.11.2 Tempo di risposta

- Il tempo di risposta è il tempo che impiega un sistema a reagire ad un input (ad esempio, in una transizione interattiva, potrebbe essere definito come il tempo tra l'ultimo tasto premuto da un utente e l'inizio dell'apparizione del risultato sul display del computer).
- È desiderabile che sia breve.
- È importante che il tempo di risposta sia breve per le applicazioni interattive (ad esempio telnet/ssh), mentre per le applicazioni batch (ad esempio il trasferimento di un file) questo requisito non è necessario.

2.11.3 Throughput

- Metrica per misurare la quantità di dati che possono essere inviati su di un link in una specificata quantità di tempo.
- Spesso viene usata per dare una stima sulla disponibilità della larghezza di banda di un link (più è alto il throughput più è alta la disponibilità).
- Da notare che la larghezza di banda e il throughput sono cose molto differenti. Il throughput è una misura che si basa sull'applicazione.
- Esempi:
  - Il numero di transazioni di un certo tipo in uno specifico periodo di tempo.
  - Il numero di sessioni utente per una data applicazione in un certo periodo di tempo.

2.11.4 Utilizzo

- L'utilizzo è una stima a grana più sottile rispetto al throughput. Si riferisce alla percentuale di tempo che una risorsa viene usata in un determinato periodo di tempo.
- Spesso un basso utilizzo indica che qualcosa non sta andando come aspettato (ad esempio si può avere poco traffico perché il file server è crashato).

2.11.5 Latenza e Jitter

- Sono espresse in ms (millisecondi).
- Latenza: la quantità di tempo che impiega un pacchetto per andare dalla sorgente alla destinazione. È molto importante per le applicazioni interattive che necessitano di scambiarsi molti dati in un breve periodo di tempo (ad esempio giochi online). Ovviamente più è alta la latenza e più le applicazioni peggiorano in performance.
- Jitter: la variazione del ritardo di tempo con il quale arrivano i pacchetti inviati in una sola direzione. È molto importante nelle applicazioni multimediali (ad esempio telefonate internet o video in broadcast).

Se la latenza è costante in media ma il jitter è molto alto, allora vuol dire che ci sono dei pacchetti che arrivano rapidamente uno dopo l'altro e dei pacchetti che arrivano molto più lentamente. Questo fa si che, se ad esempio si sta guardando un video via internet, questo vada "a scatti".

2.11.6 Larghezza di banda

- Intervallo di misura (Time committed - Tc): l'intervallo di tempo o "l'intervallo della larghezza di banda" usato per controllare il burst del traffico.
- Burst committed (Bc): il massimo numero di bit che la rete garantisce di trasferire durante un qualsiasi Tc.
- CIR (Committed Information Rate): la velocità garantita della rete in condizioni normali. Il CIR viene misurato in bit per secondo ed è una delle chiavi della negoziazione per le tariffe metriche. $CIR = \frac{Bc}{Tc}$.
- Burst excess (Be): il numero di bit che si tenta di trasmettere dopo il raggiungimento del valore di Bc.
- Velocità massima di trasferimento (Maximum data Rate - MaxR) misurata in bit per secondi. $MaxR = \frac{Bc+Be}{Bc} \times CIR = \frac{Bc+Be}{Tc}$.

Ad esempio:

$$\begin{cases} Tc = 10 \text{ ms} \\ Bc = 7680 \text{ b} \\ Be = 320 \text{ b} \end{cases} \implies \begin{cases} CIR = \frac{Bc}{Tc} = \frac{7680 \text{ b}}{0.01 \text{ s}} = 768 \text{ Kbps} & \text{(velocità garantita, quella per cui si paga)} \\ \\ MaxR = \frac{Bc+Be}{Tc} = \frac{(7680+320) \text{ b}}{0.01 \text{ s}} = 800 \text{ Kbps} & \text{(massima velocità possibile)} \end{cases}$$

2.12 Misurazioni per link

- Metriche disponibili per un link (# = cardinalità, numero di).
  - #pacchetti, #byte, #pacchetti scartati su di una specifica interfaccia nell'ultimo minuto.
  - #flussi, #pacchetti per flussi.
- Non fornisce statistiche globali della rete.
- Usato dagli ISP per misurare il traffico.
- Esempi:
  - SNMP MIBs.
  - RTFM (Real-Time Flow Measurement).
  - Cisco NetFlow.

2.13 Misurazioni End-to-End

- La performance della rete è diversa dalla performance delle applicazioni.
  - Wire-time verso web-server performance.
- Molte delle misurazioni di rete sono di natura end-to-end.
- Statistiche per percorso.
  - Sono percorsi simmetrici? Generalmente non lo sono (problemi di routing).
  - Come si deve comportare la rete per sondare grandi/piccoli pacchetti?
- È necessario per dedurre le misurazioni della performance per-link.

2.14 Approcci al monitoraggio

- Attive.
  - Iniettare (inject) traffico in rete e controllare come questa reagisce (ad esempio, ping).
- Passive.
  - Monitorare il traffico di rete al solo scopo di misurazione (ad esempio la stretta di mano a tre vie del TCP per misurare il RTT (Round Trip Time) della rete).
- Le misurazioni attive sono spesso end-to-end, mentre le misurazioni passive sono limitate ai link interessati dalla cattura del traffico.
- Non ne esiste uno buono o uno cattivo, entrambi gli approcci sono buoni a seconda dei casi:
  - Il monitoraggio passivo sugli switch può essere un problema.
  - Non si può sempre iniettare il traffico che si vuole. Ad esempio, su di un link satellitare (rete satellitare) si può solo ricevere quello che è stato iniettato dal produttore del satellite.
- Generalmente la soluzione migliore è di combinare entrambi gli approcci e confrontare i risultati.

2.15 Misurazioni inline e offline

- Misurazioni inline: metodi basati su di un protocollo che fluisce sulla stessa rete dove sono prese le misurazioni (ad esempio SNMP)
- Misurazioni offline: metodi che usano reti differenti per la lettura delle misurazioni (ad esempio, leggere i contatori del traffico usando una porta seriale o una rete/VLAN (virtaul LAN)) amministrata.

3 Monitoraggio SNMP

3.1 SNMP MIB II

- MIB II (RFC 1213) definisce i tipi di oggetto per i protocolli internet IP, ICMP, UDP, TCP, SNMP (e altre definizioni). In pratica modella la gestione dello stack TCP/IP.
- In tutto definisce 170 tipi di oggetto.
- Qualche definizione risulta essere troppo semplice e minimale (tabella di routing, tabella delle interfacce).
- Qualche definizione presuppone indirizzi a 4-byte e quindi devono essere ridefinite per l'IP versione 6 (IPv6) dove gli indirizzi sono a 16-byte.

3.1.1 Scopi

- Definisce semplici errori e configurazioni per gestire i protocolli internet.
- Veramente pochi e semplici oggetti di controllo.
- Si cerca di evitare le ridondanze nel MIB.
- L'implementazione del MIB non dovrebbe interferire con le normali attività della rete.
- Non ci sono tipi di oggetti dipendenti dall'implementazione.

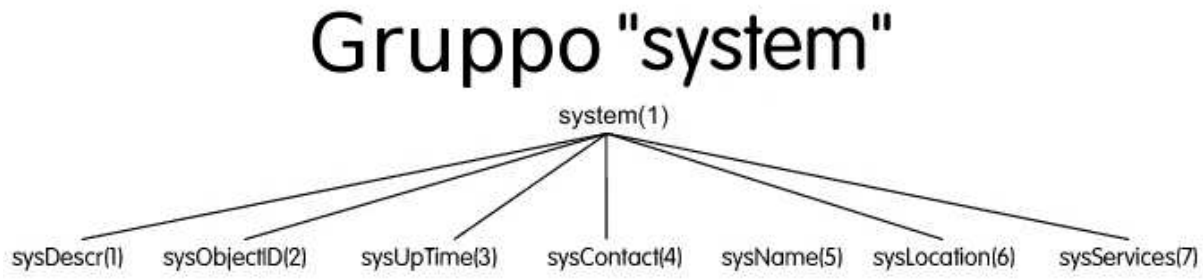


Figura 1: MIB II: gruppo "system"

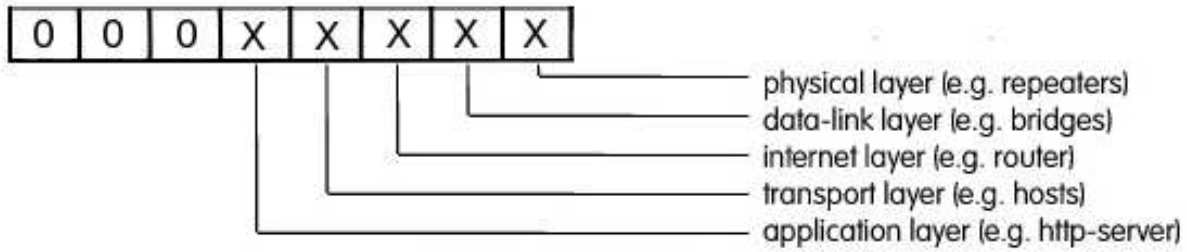


Figura 2: MIB II: gruppo "system", variabile sysService

3.1.2 Gruppo "system"

- La variabile `sysUpTime.0` è veramente importante dato che serve a determinare le discontinuità del servizio:
  - se $sysUpTime.0_{t1} > sysUpTime.0_{t2}$ dove $t2 > t1$ allora l'agent è stato reinizializzato e le applicazioni di gestione si affidano a valori precedenti.
- `sysService` riporta informazioni circa i servizi forniti dal sistema (si veda figura 2).
- `sysObjectId.0` ha il formato `enterprises.<prodotto>.<id>+` ed è usato per identificare il prodotto e il modello. Per esempio `enterprises.9.1.208` identifica il Cisco (.9) 2600 router (.1.208).
- `sysDescr.0` fornisce una precisa descrizione del dispositivo (ad esempio "Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-I-M), Version 12.2(23), RELEASE SOFTWARE (fc2) Copyright (c) 1986-2004 by cisco Systems, Inc.").
- In breve il gruppo "system" è importante per:
  - Mappare i dispositivi (via `sysObjectId.0`, `sysDescr.0` e `sysLocation.0`[2]).
  - Controllare il contatore del dispositivo (`sysUpTime.0`).
  - Riportare i problemi all'amministratore (`sysContact.0`).

3.1.3 Gruppo "interface"

Informazioni sulle interfacce. Esiste una riga per ogni interfaccia "attiva". Se un'interfaccia viene "spenta" in un secondo momento, la sua riga rimane vuota (le righe successive non vengono spostate per chiudere il buco), quindi la variabile `ifIndex` può presentare dei "buchi".

[2]Specifica dove si trova fisicamente il dispositivo

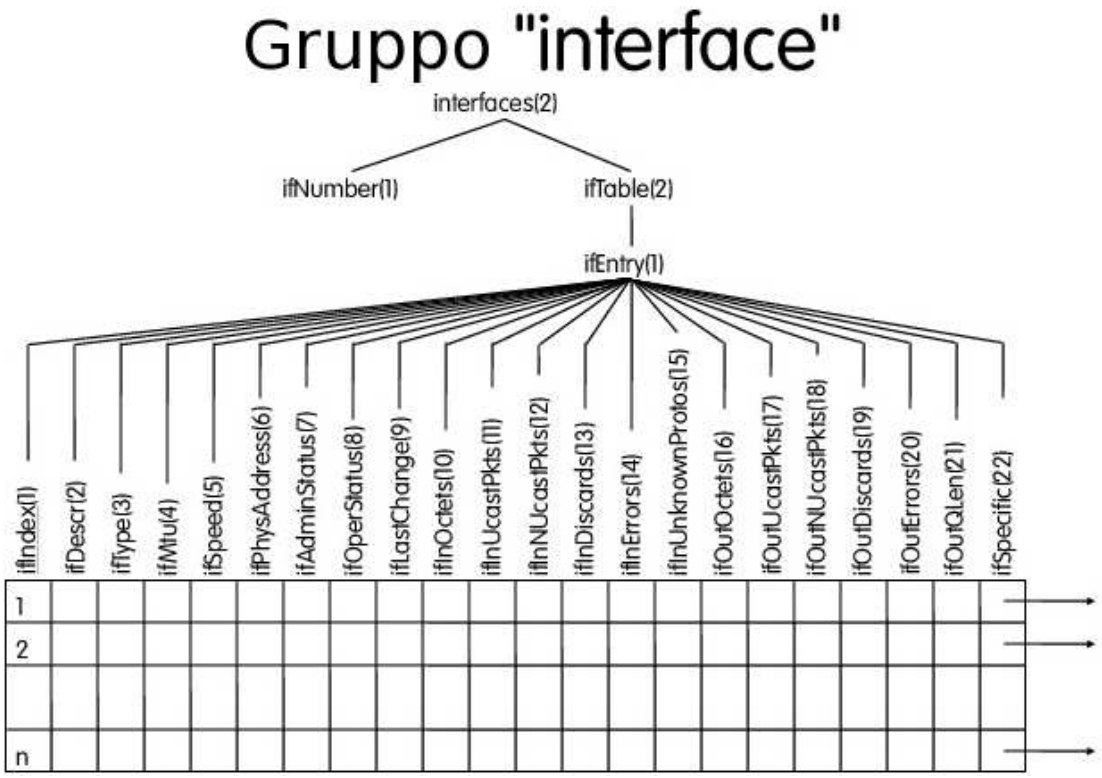


Figura 3: MIB II: gruppo "interface"

- `sysAdminStatus`: il corrente stato amministrativo dell'interfaccia. Può essere: `up(1)`, `down(2)`, `test(3)`. Un valore diverso da `up` significa che l'interfaccia non è fisicamente presente oppure c'è ma non è disponibile al sistema operativo (ad esempio il driver non è stato caricato).
- `ifOperStatus`: il corrente stato operazionale dell'interfaccia. Può essere: `up(1)`, `down(2)`, `test(3)`. Simile a `ifconfig <device> up/down`.
- `ifOutQLen`: la lunghezza della coda dei pacchetti in uscita (misurata in pacchetti). È usata per conoscere qualcosa in più a proposito della velocità di trasmissione e del throughput (se il buffer è pieno allora il destinatario non è veloce come il mittente).
- `ifLastChange`: contiene il valore del `sysUpTime` al momento in cui l'interfaccia è entrata nello stato operazionale corrente. Usata per determinare quando un'interfaccia ha cambiato il suo stato operazionale (vedi `ifOperStatus`).

  Il diagramma dei casi d'uso (figura 4) mostra le dipendenze tra le variabili:

  - Il numero di pacchetti consegnati dall'interfaccia di rete al protocollo di livello superiore si calcola come: `ifInUcastPkts`[3] + `ifInNUcastPkts`[4]
  - Il numero di pacchetti ricevuti dalla rete si calcola come: (`ifInUcastPkts` + `ifInNUcastPkts`) + `ifInDiscards`[5] + `ifInUnknownProtos`[6] + `ifInErrors`[7]

Uso del gruppo "interface":

- È la base del monitoraggio basato su SNMP.

[3] Il numero di pacchetti che non sono né multicast né broadcast.
[4] Il numero di pacchetti che sono o multicast o broadcast.
[5] Il numero di pacchetti scartati benché non sono affetti da errore ed hanno un protocollo conosciuto (un esempio sono i pacchetti scartati per lasciare spazio nel buffer).
[6] Il numero di pacchetti scartati perché, o non si conosce il protocollo, oppure non è gestito.
[7] Il numero di pacchetti scartati perché affetti da errore.

Figura 4: MIB II: gruppo "interface": diagramma dei casi d'uso

- Molti strumenti periodicamente prelevano i valori delle interfaccia (per lo più `ifInOctets`[8] e `ifOutOctets`[9]).
- I valori sono aggregati e non divisi per protocollo di destinazione, AS. Questa è la maggiore limitazione se si vuole fare un monitoraggio più mirato. La ragione è che i contatori SNMP sono semplicemente i contatori del kernel "esposti" via SNMP.
- Errori delle interfacce possono essere usati per scovare dei problemi di comunicazione, specialmente con i link WAN (Wide Area Network).
- Le statistiche sulla dimensione dei pacchetti non vengono riportate, ma comunque si posso calcolare semplici statistiche usando il numero totale di ottetti e di pacchetti.
- Molti produttori (ad esempio Cisco, Juniper) riportano delle informazioni a proposito sia delle interfacce fisiche che di quelle logiche (anche conosciute come sottointerfacce). Altri (ad esempio Extreme) hanno delle entry nella tabella ma i contatori sono sempre a zero.
- Usando i contatori dell'interfaccia è possibile produrre un resoconto a proposito di:
  - VLAN (Virtual LAN).
  - PVC (Private Virtual Circuit) sui link Frame Relay[10].

3.2 Come calcolare la percentuale di utilizzo della larghezza di banda con SNMP

$$\%utilizzo\ della\ larghezza\ di\ banda = \frac{(\Delta ifInOctets + \Delta ifOutOctets) \times 8}{(\Delta tempo) \times IfSpeed} \times 100$$

$$\%utilizzo\ in\ input = \frac{(\Delta ifInOctets) \times 8}{(\Delta tempo) \times IfSpeed} \times 100$$

$$\%utilizzo\ in\ output = \frac{(\Delta ifOutOctets) \times 8}{(\Delta tempo) \times IfSpeed} \times 100$$

Si noti che tutte le variabili necessarie si trovano nel gruppo `interface`, mentre il $\Delta tempo$ viene ottenuto con la variabile `sysUpTime.0`.

[8] Il numero di "ottetti" (byte) ricevuti dall'interfaccia.
[9] Il numero di "ottetti" (byte) inviati dall'interfaccia.
[10] Il Frame Relay è una tecnica di trasmissione a commutazione di pacchetti (una tecnica di accesso multiplo a ripartizione nel tempo, usata per condividere un canale di comunicazione tra più stazioni in modo non deterministico).

3.2.1 Usare il gruppo "arp"

- Usato per accedere alla tabella ARP (Address Resolution Protocol) dei dispositivi remoti.
- Può essere usato per identificare gli attacchi di ARP poisoning oppure host mal configurati (ad esempio se ci sono indirizzi IP duplicati).
- Esempio:

```
RFC1213-MIB::atIfIndex.4.1.172.22.6.168 = INTEGER: 4
RFC1213-MIB::atIfIndex.4.1.172.22.7.255 = INTEGER: 4
RFC1213-MIB::atPhysAddress.4.1.172.22.6.168 = Hex-STRING: 00 40 F4 67 49 08
RFC1213-MIB::atPhysAddress.4.1.172.22.7.255 = Hex-STRING: FF FF FF FF FF FF
RFC1213-MIB::atNetAddress.4.1.172.22.6.168 = Network Address: AC:16:06:A8
RFC1213-MIB::atNetAddress.4.1.172.22.7.255 = Network Address: AC:16:07:FF
```

3.3 Il MIB Bridge

- Usato per controllare lo stato degli switch L2/L3. Non si commetta l'errore comune di credere che viene usato solo sui bridge[11]
- È qualcosa di complementare al MIB II, dato che fornisce informazioni sugli host connessi alle porte dello switch.
- Gli usi comuni del MIB bridge sono:
  - Conoscere l'indirizzo MAC di un host connesso alla porta X/unità Y dello switch[12] `dot1dTpFdbTable`[13]`.dot1dTpFdbAddress`[14] (nota: il MIB II ha l'indirizzo MAC della porta dello switch).
  - L'associazione porta/indirizzo MAC è la base per determinare dove si trova fisicamente un host. Infatti le porte dello switch sono generalmente connessehttp://42cows.org/ilfatto20101102.pdf alle prese della parete, e questo è un buon metodo per sapere chi c'è e dov'è (*utente* → *computer* → *porta dello switch* → *stanza/scrivania*).
  - Tiene traccia del "precedente" indirizzo MAC (e del tempo) connesso ad una porta, in questo modo è possibile tracciare gli utenti che si spostano da una stanza ad un altra.
  - Può essere usato per trovare le porte che hanno più indirizzi MAC associati (un trunk) e quindi trovare gli utenti che hanno più indirizzi MAC (ad esempio gli utenti che hanno avviato una macchina virtuale come VMware, oppure gli utenti che hanno un virus/worm), oppure le porte che sono direttamente connesse ad un altro switch.

3.3.1 Esempio: prelevare indirizzi MAC e le porte fisiche

1. Del bridge con indirizzo IP 14.32.6.17 si prelevano tutte le VLAN, vtpVlanState (.1.3.6.1.4.1.9.9.46.1.3.1.1.2):

```
# snmpwalk -c public 14.32.6.17 vtpVlanState
CISCO-VTP-MIB::vtpVlanState.1.1 = INTEGER: operational(1)
CISCO-VTP-MIB::vtpVlanState.1.2 = INTEGER: operational(1)
CISCO-VTP-MIB::vtpVlanState.1.6 = INTEGER: operational(1)
CISCO-VTP-MIB::vtpVlanState.1.7 = INTEGER: operational(1)
CISCO-VTP-MIB::vtpVlanState.1.8 = INTEGER: operational(1)
...
```

2. Per ogni VLAN si prende la tabella degli indirizzi MAC (si noti la forma `<read_community>@<vlan_number>`), dot1dTpFdbAddress (.1.3.6.1.2.1.17.4.3.1.1). Nell'esempio che segue, la VLAN 2 non ha niente nella sua tabella:

```
# snmpwalk -c public@1 14.32.6.17 dot1dTpFdbAddress
.1.3.6.1.2.1.17.4.3.1.1.0.208.211.106.71.251 = Hex-STRING: 00 D0 D3 6A 47 FB

# snmpwalk -c public@2 14.32.6.17 dot1dTpFdbAddress
```

[11] I bridge, gli switch e gli hub lavorano a livello 2 (Data Link) mentre a livello 3 (Network) troviamo i router. L'hub smista i pacchetti a tutte le interfacce con cui è collegato, un bridge o uno switch invece sanno indirizzare il pacchetto ad una specifica interfaccia. La differenza sostanziale tra un bridge e uno switch sta nel fatto che quest'ultimo ha molte più porte.

[12] I grandi switch sono divisi per unità poste una sopra l'altra, ogni unità ha un insieme di porte.

[13] È la tabella che contiene le informazioni a proposito degli host per i quali il bridge ha inviato o filtrato informazioni.

[14] L'indirizzo MAC.

```
# snmpwalk -c public@6 14.32.6.17 dot1dTpFdbAddress
.1.3.6.1.2.1.17.4.3.1.1.0.2.185.144.76.102 = Hex-STRING: 00 02 B9 90 4C 66
.1.3.6.1.2.1.17.4.3.1.1.0.2.253.106.170.243 = Hex-STRING: 00 02 FD 6A AA F3
.1.3.6.1.2.1.17.4.3.1.1.0.224.30.159.10.210 = Hex-STRING: 00 E0 1E 9F 0A D2

... e così via per tutte le VLAN scoperte al primo passaggio.
```

3. Per ogni VLAN si preleva il numero di porta del bridge, dot1dTpFdbPort (.1.3.6.1.2.1.17.4.3.1.2):

```
# snmpwalk -c public@1 14.32.6.17 dot1dTpFdbPort
.1.3.6.1.2.1.17.4.3.1.2.0.208.211.106.71.251 = INTEGER: 113

# snmpwalk -c public@2 14.32.6.17 dot1dTpFdbPort

# snmpwalk -c public@6 14.32.6.17 dot1dTpFdbPort
.1.3.6.1.2.1.17.4.3.1.2.0.2.185.144.76.102 = INTEGER: 113
.1.3.6.1.2.1.17.4.3.1.2.0.2.253.106.170.243 = INTEGER: 113
.1.3.6.1.2.1.17.4.3.1.2.0.224.30.159.10.210 = INTEGER: 65

... e così via per tutte le VLAN scoperte al primo passaggio.
```

4. Si prendono gli ifIndex delle porte del bridge, dot1dBasePortIfIndex (.1.3.6.1.2.1.17.1.4.1.2):

```
# snmpwalk -c public@1 14.32.6.17 dot1dBasePortIfIndex
.1.3.6.1.2.1.17.1.4.1.2.68 = INTEGER: 12
.1.3.6.1.2.1.17.1.4.1.2.69 = INTEGER: 13
.1.3.6.1.2.1.17.1.4.1.2.70 = INTEGER: 14
...
.1.3.6.1.2.1.17.1.4.1.2.113 = INTEGER: 57
...

... e così via per tutte le VLAN scoperte al primo passaggio.
```

5. Quindi si attraversa ifName (.1.3.6.1.2.1.31.1.1.1.1) in modo che gli ifIndex ottenuti nel passaggio precedente possano essere associati al relativo nome della porta:

```
# snmpwalk -On -c public 14.32.6.17 ifName
.1.3.6.1.2.1.31.1.1.1.1.1 = STRING: sc0
.1.3.6.1.2.1.31.1.1.1.1.2 = STRING: sl0
.1.3.6.1.2.1.31.1.1.1.1.3 = STRING: me1
...
.1.3.6.1.2.1.31.1.1.1.1.57 = STRING: 2/49
...
```

Le informazioni raccolte possono essere usate, ad esempio:

1. Dal passo 2, c'è un indirizzo MAC:
   `.1.3.6.1.2.1.17.4.3.1.1.0.208.211.106.71.251 = Hex-STRING: 00 D0 D3 6A 47 FB`
2. Il passo 3 ci dice che l'indirizzo MAC (`00 D0 D3 6A 47 FB`) si trova alla porta del bridge `113`:
   `.1.3.6.1.2.1.17.4.3.1.2.0.208.211.106.71.251 = INTEGER: 113`
3. Dal passo 4, la porta `113` del bridge ha un ifIndex numero `57`:
   `.1.3.6.1.2.1.17.1.4.1.2.113 = INTEGER: 57`
4. Dal passo 5, l'ifIndex `57` corrisponde alla porta fisica `2/49`:
   `.1.3.6.1.2.1.31.1.1.1.1.57 = STRING: 2/49`

3.3.2 Note a margine: SNMP verso contatori CLI

- È una comune convinzione tra le community degli amministratori di rete pensare che SNMP e i contatori CLI (Command Line Interface) siano due modi diversi di vedere la stessa cosa[15].
- Molti amministratori preferisco di più i contatori CLI perché:

[15] In questo contesto i contatori CLI sono dei contatori forniti dai device attraverso altre vie che non usano SNMP, ad esempio anche attraverso un'interfaccia HTML. La differenza sostanziale tra i contatori CLI e i contatori SNMP e che gli ultimi hanno il formato dell'output ben specifico, mentre i primi no, dipende da produttore a produttore.

  - Hanno un formato direttamente consultabile dall'uomo
    - 0 pacchetti in input, 0 pacchetti in output
  - Molte implementazioni forniscono comandi per cancellare/resettare i contatori
    - clear interface ethernet 3

- Nota: la definizione di cosa conta un contatore dipende dalla documentazione del prodotto.

- ```
  c4500#sh int e1
  Ethernet1 is up, line protocol is down
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  0 packets input, 0 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 input packets with dribble condition detected
       187352 packets output, 11347294 bytes, 0 underruns
       187352 output errors, 0 collisions, 3 interface resets
  ```

- Note:
  - I contatori CLI rimangono la via basilare per la gestione degli elementi.
  - Il formato/apparenza dei contatori cambiano da produttore a produttore (spesso anche con lo stesso prodotto, ad esempio Cisco IOS verso CatOS verso PIX).
  - Nota: IOS, CatOS e PIX sono rispettivamente router, switch e firewall OS usati dalle apparecchiature Cisco.

- I contatori SNMP invece:
  - Offrono la possibilità di confrontare le apparecchiature:
    - Sono contatori definiti da uno standard
      - Come definita da IETF[16], IEEE[17], qualche produttore, etc...
      - Non dipendono dai tipi di elementi di rete o dai produttori.
    - Sono unici a livello globale, con nomi difficili da pronunciare
      - `1.3.6.1.2.1.17.2.4 dot1dStpTopChanges`
  - Hanno una dimensione ben specifica
    - Larghezza a 32 o a 64 bit (i 64 bit sono disponibili in SNMP v2c o v3).
  - I contatori non necessariamente partono da zero
    - I produttori sono liberi di fare quello che vogliono.
  - Non sono pensati per essere consultati direttamente dall'uomo.
  - ```
    dot1dTpPortInFrames OBJECT-TYPE
                  SYNTAX Counter
                  ACCESS read-only
                  STATUS mandatory
                  DESCRIPTION
                        "The number of frames that have been received by
                        this port from its segment. Note that a frame
                        received on the interface corresponding to this
                        port is only counted by this object if and only if
                        it is for a protocol being processed by the local
                        bridging function, including bridge management
                        frames."
                  REFERENCE
                        "IEEE 802.1D-1990: Section 6.6.1.1.3"
    ```
  - Nota: i buoni contatori generalmente derivano da una specificazione del protocollo sottostante.

[16] Internet Engineering Task Force
[17] Institute of Electrical and Electronics Engineering

3.4 Cos'altro si può fare con SNMP?

- Individuare ed eliminare le connessioni TCP pendenti.
- Manipolare la tabella ARP.
- Prelevare la temperatura ambientale.
- Controllare l'utilizzo della CPU.
- Monitorare gli alimentatori e/o i gruppi di continuità.
- Trovare gli utenti che usano P2P (utilizzando la tabella NAT[18]).
- Visualizzare la topologia della rete (ad esempio con CDP[19]).

4 Monitoraggio remoto

4.1 Le reti stanno cambiando

Internet:

- La sicurezza di rete inizierà ad essere un elemento più critico nel futuro.
- Le reti aziendali diventeranno reti pubbliche.

Telefonia:

- Il supporto alla telefonia attraverso reti wired e wireless saranno un elemento chiave delle reti future.
- La rete diventerà sempre e dovunque una risorsa.

Comunicazioni dinamiche:

- Il supporto ad un ampio numero di applicazioni sarà l'elemento chiave del futuro: convergenza.
- I dati della rete saranno la rete.

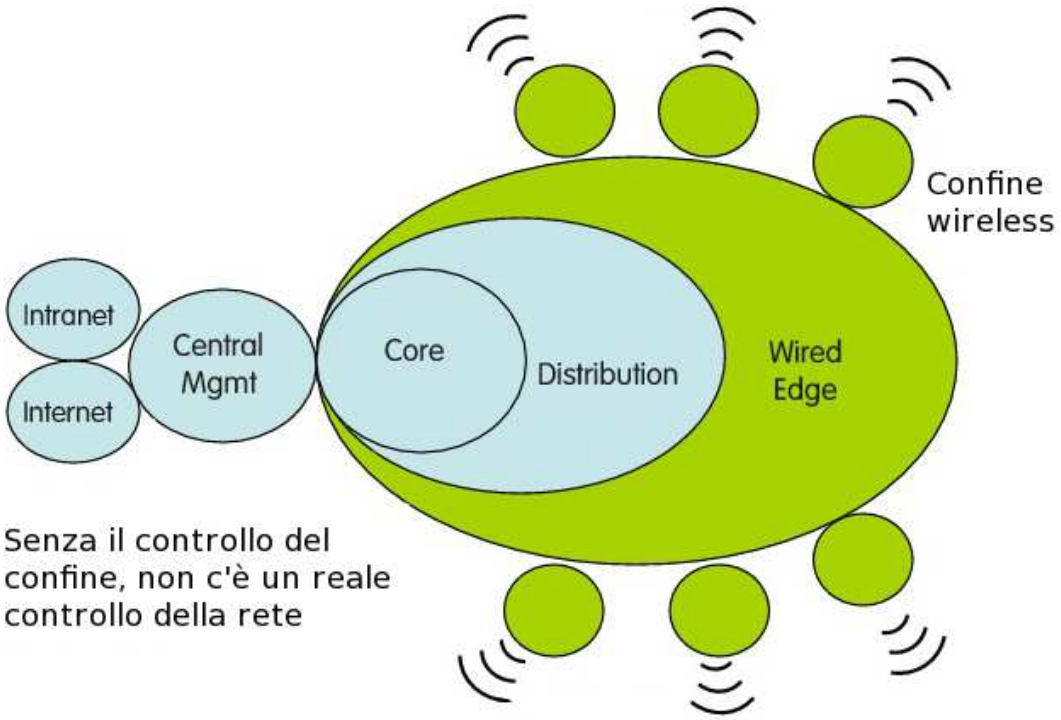


Figura 5: La rete sta cambiando

[18] Network Address Translation.
[19] Cisco Discovery Protocol.

4.2 Verso il monitoraggio remoto

- Le reti moderne sono distribuite tra varie costruzioni, amministrate da persone differenti con varie competenze (sicurezza, analizzatore di traffico, amministratore di database).
- È necessario raccogliere le statistiche del traffico su ogni tronco della rete e spedirle ad un (limitato) numero di collezionatori, in modo da produrre una vista globale.
- Qualche capacità di analisi distribuita è necessaria perché una rete centralizzata non è scalabile e non supporta gli errori.
- Sistemare gli analizzatori di traffico (ad esempio sonde basate su pcap) non è sempre fattibile perché:
  - I server non sempre permettono l'installazione di generici software non testati (ad esempio, la licenza può obbligare di installare su di un server Oracle solo applicazioni certificate da Oracle).
  - I server moderni hanno spesso molte interfacce di rete (1 Gb principale più failover per i dati e 100 Mbit per l'accesso al server). Su questi server è necessario installare delle sonde multi-interfacce.
  - Monitorare una 1 GE richiede 2xGE (una per ogni RX[20] dell'originale GE).
- Soluzione: usare le capacità di analisi del traffico delle apparecchiature di rete.
- Svantaggi:
  - Non tutte le apparecchiature sono fornite di capacità di analisi del traffico (ad esempio molti router ADSL non le hanno).
  - Anche se supportate, non sempre queste capacità possono essere abilitate (forte impatto sulla CPU e la memoria).
  - Le capacità di monitoraggio base fornite dai sistemi operativi di default sono piuttosto limitate e quindi è necessario una scheda personalizzata.
  - Le schede personalizzate per l'analisi del traffico non sono economiche.
- Ecco i prezzi di qualche scheda di monitoraggio in commercio (il software va comprato a parte):

Prodotto	Prezzo (solo scheda)
Cisco MSFC-2	46'000 $
Juniper PM-PIC	30'000 $

4.3 RMON: Monitoraggio remoto usando SNMP

- Presente su molte medio/alte apparecchiature di rete: spesso queste sono povere/limitate implementazioni.
- Qualche produttore vende delle sonde stand-alone. Quelle preferite sono quelle che:
  - sono piene implementazioni del protocollo.
  - non aggiungono altro carico al router.
- Esistono due versioni di RMON, RMON1 (RMON v1) e RMON2 (RMON v2). Mentre RMON1 è specializzato solo per i primi 2 livelli della pila ISO/OSI, RMON2 si concentra sui livelli dal 3 al 6.
- Non tutte le implementazioni (in particolare quelle embedded nei router/switch) supportano l'intero standard ma solo alcuni selezionati gruppi SNMP.
- Insieme con Cisco NetFlow è l'industriale, "fidato", standard di monitoraggio.

[20] Comunicazione in entrata (receive).

4.3.1 Cosa può fare RMON

- Raccogliere dati e periodicamente inviarli a dei centri di gestione, i quali potenzialmente riducono il traffico sui link WAN e spostano l'overhead sui centri di gestione.
- Riportano ciò che fanno gli host della rete, quanto "parlano", e verso chi.
- "Vedere" tutto il traffico LAN, l'utilizzo della LAN, e non solo il traffico verso o attraverso il router.
- Filtra e cattura i pacchetti (quindi non c'è bisogno di controllare o inserire un analizzatore LAN): è in pratica uno sniffer remoto che può catturare il traffico in real-time (finché non finisce la memoria integrata).
- Automaticamente raccoglie i dati, confronta le soglie, e spedisce segnali al centro di gestione - il quale scarica molto del lavoro che potrebbe impantanare il centro di gestione.

4.3.2 RMON verso SNMP

- Il protocollo SNMP viene usato per configurare e controllare una sonda. Generalmente la gestione con le interfacce grafiche utente (GUI - Graphic User Interface) nasconde la complessità della configurazione basata su SNMP.
- Usando SNMP le applicazioni di amministrazione possono ricevere le statistiche e il traffico salvato in modo da registrare le statistiche di una rete con la possibilità di selezionarne una parte.
- SNMP e RMON differiscono nel modo in cui raccolgono le statistiche sul traffico:
  - Con SNMP vengono fatte delle richieste periodiche: richiede una query al dispositivo SNMP per prendere le statistiche di rete (lo stato della rete viene preso dal manager).
  - RMON, in modo diverso, riduce il lavoro del manager raccogliendo e salvando le statistiche in contatori o buckets pronte per essere ricevute da un centro di amministrazione.

4.3.3 RMON1 filtri e canali

- I pacchetti ricevuti possono essere filtrati. I filtri sono semplici espressioni di valori/maschere (come indirizzo IP, rete e maschera).
- Un canale RMON è definito come un'insieme di coppie di filtri: uno sui dati (sul pacchetto) e uno sullo stato (sulle informazioni del pacchetto, come ad esempio la dimensione).
- Un pacchetto viene accettato da un canale quando:
  - ha una corrispondenza con almeno una coppia di filtri (`acceptMatched channel`).
  - almeno un filtro di tutte le coppie di filtri fallisce il test (`acceptFailed channel`).

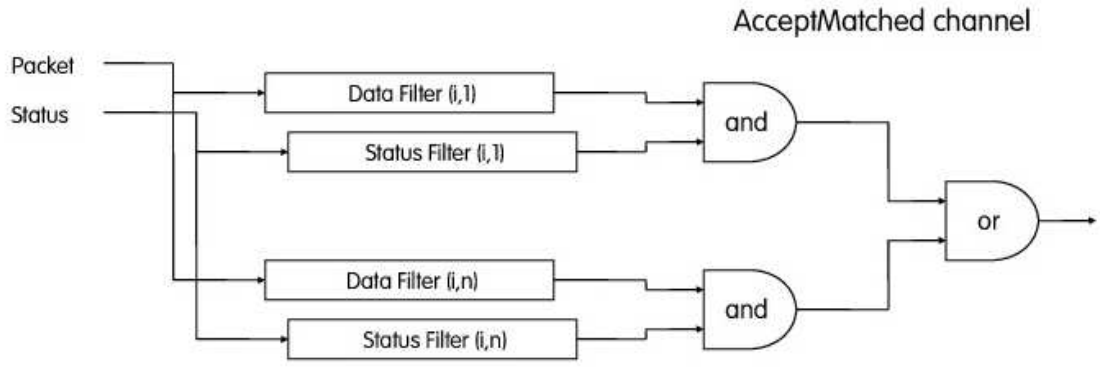


Figura 6: RMON: `acceptMatched channel`. Nell'`acceptFailed channel`, le porte AND diventano OR e la porta OR diventa AND.

4.3.4 I gruppi di monitoraggio RMON1

Gruppi	Funzioni	Elementi
Statistics	Contiene le statistiche misurate dalla sonda per ogni interfaccia monitorata su questo dispositivo.	Pacchetti scartati, pacchetti spediti, byte spediti ("ottetti"), pacchetti di broadcast, pacchetti multicast.
History	Registra alcune statistiche campione dalla rete e le salva per essere prelevate più tardi.	Periodo campione, numero di campioni, i campioni.
Alarm	Periodicamente preleva dei campioni statistici dalla sonda e li confronta con delle soglie configurate precedentemente. Se la variabile monitorata supera una soglia, allora si genera un evento.	Tipo di allarme, soglia inferiore, soglia superiore.
Host	Contiene le statistiche associate ad ogni host scoperto in rete.	Indirizzo dell'host e byte ricevuti e trasmessi sia su broadcast che su multicast e pacchetti errati.
HostTopN	Prepara tabelle che descrivono i top-host (quelli che usano di più la rete) in una lista ordinata per un tipo di statistica sull'intervallo specificato dal centro di gestione. Perciò queste statistiche sono dipendenti dalla velocità.	Statistiche, host, inizio e fine del periodo campione, velocità di base, durata.
Matrix	Salva le statistiche sulle conversazioni tra due indirizzi settati. Come il dispositivo determina una nuova conversazione, crea una nuova entry nella tabella.	Tipo di filtro per i bit (maschera o non maschera), espressione del filtro (livello di bit), espressione condizionale (and, or, not) verso gli altri filtri.
Filters	Abilita dei filtri sui pacchetti. I pacchetti che passano il filtro formano un flusso di dati che può essere catturato oppure che può generare eventi.	Tipo di filtro per i bit (maschera o non maschera), espressione del filtro (livello di bit), espressione condizionale (and, or, not) verso gli altri filtri.
Packet Capture	Abilita la cattura dei pacchetti dopo che sono passati da un canale.	Dimensione del buffer per la cattura dei pacchetti, intero stato (allarme), numero dei pacchetti catturati.
Events	Controlla la generazione e la notifica degli eventi del dispositivo.	Tipo di evento, descrizione, il tempo di ultimo invio dell'evento.

4.3.5 Il gruppo "alarm" di RMON1

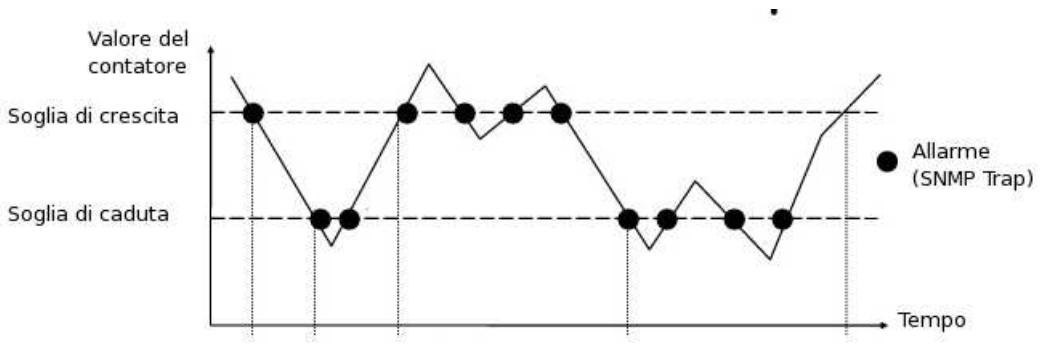


Figura 7: RMON: allarmi

- Un evento viene generato ogni volta che viene superata una soglia (o superiore o inferiore) o quando un valore sopra (o sotto) la soglia ritorna nei limiti.
- Le soglie possono essere misurate o con un valore specifico (assoluto) oppure come differenza tra il valore attuale e l'ultimo valore misurato (valore delta).

4.3.6 Statistiche ethernet di RMON

Pacchetti: un unità di dati formattati per la trasmissione sulla rete.

Pacchetti multicast: comunicazione tra un singolo mittente e più destinatari nella rete.

Pacchetti broadcast: un pacchetto trasmesso a tutti gli host della ethernet.

Eventi di scarto: un superamento del limite della porta. La porta logica non è in grado di ricevere i pacchetti alla piena velocità della linea e quindi inizia a scartarne qualcuno.

Frammenti: un pezzo di un pacchetto. Qualche volta un pacchetto di comunicazione che viene spedito in rete deve essere spezzato temporaneamente in frammenti; il pacchetto dovrebbe essere riassemblato quando raggiunge la destinazione.

Jabber: pacchetti ricevuti di dimensione maggiore a 1518 ottetti e che contengono anche errori di allineamento.

Pacchetti sovradimensionati: pacchetti di dimensione maggiore a 1518 ottetti ma che sono ben formati.

4.3.7 Utilizzo della rete con RMON

- Molti amministratori usano i contatori di RMON per calcolare l'utilizzo della rete.
- L'utilizzo della rete può essere calcolata per tutte le porte dello switch ad intervalli regolari. Queste informazioni possono essere raccolte durante l'arco della giornata per poi generare un profilo dell'utilizzo dello switch o dell'hub.

$$\%utilizzo\ della\ rete = \frac{(\#pacchetti \times 160) + (\#ottetti \times 8)}{(velocità\ \ della\ \ porta) \times (secondi)} \times 100$$

4.3.8 Caso di studio: intervallo di campionamento del contatore

Esempio 1: (intervallo di campionamento di 10 secondi, valore di soglia 20, intervallo di test di 10 secondi)

Tempo:	0	10	20
Valore:	0	19	32
Delta:		19	13
Soglia attuale da controllare:		19	13

Esempio 2: (intervallo di campionamento di 5 secondi, valore di soglia 20, intervallo di test di 10 secondi)

Tempo:	0	5	10	15	20
Valore:	0	10	19	30	32
Delta:		10	9	11	2

- Il valore campione istanziato dal MIB deve essere fatto due volte per ogni intervallo di campionamento, altrimenti il superamento della soglia potrebbe non essere rilevato quando gli intervalli si sovrappongono.
- Prelevare i valori velocemente (fast polling) ha questi svantaggi:
  - Vengono collezionati molti dati.
  - Si incrementa il carico dell'agent SNMP.
  - Vengono rilevati molti cambiamenti (questo può portare a dei falsi positivi).
- Prelevare i valori lentamente (slow polling) ha questi svantaggi:
  - Qualche allarme può essere perso (inesattezza).

4.4 Sonde migliorate in stile RMON

- Ogni router/switch (spaziando da quelli Cisco a quelli basati su Linux) hanno la capacità di definire delle liste di accesso controllato (ACL - Access Control List) per evitare in maniera preventiva un selezionato flusso di traffico.
- Le ACL con la politica di "accesso" possono essere usate molto bene per controllare il traffico.
- Svantaggi:
  - Le ACL sono limitate agli IP laddove RMON no (ad esempio IPX, NeBEUI).
  - Su molti sistemi, le ACL impattano sulla CPU.
  - Il numero totale di ACL, per porta, è limitato.
  - Spesso le ACL si limitano a controllare l'header del pacchetto (non il carico utile, il payload).

Esempi di definizione delle ACL:

- Cisco

```
access-list 102 permit icmp any any
```

- Juniper

```
filter HTTPcounter {
  from {
    destination-address {
      10.10.20/24;
      10.40.30/25;
      11.11/8;
    }
    destination-port [http https];
  }
  then {
    count Count-Http;
    accept
```

- Linux (iptables)

```
# /sbin/iptables -xnvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
   pkts       bytes                target   prot opt  in   out       source        destination
 236675   169960206   RH-Firewall-1-INPUT    all  --   *     *    0.0.0.0/0          0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
   pkts       bytes                target   prot opt  in   out       source        destination
      0           0   RH-Firewall-1-INPUT    all  --   *     *    0.0.0.0/0          0.0.0.0/0

Chain OUTPUT (policy ACCEPT 262868 packets, 233122676 bytes)
   pkts       bytes                target   prot opt  in   out       source        destination

Chain RH-Firewall-1-INPUT (2 references)
   pkts       bytes                target   prot opt  in   out       source        destination
  68169    81214627                ACCEPT    all  --  lo    *    0.0.0.0/0          0.0.0.0/0
    677       53751                ACCEPT   icmp  --   *     *    0.0.0.0/0          0.0.0.0/0
      0           0                ACCEPT    esp  --   *     *    0.0.0.0/0          0.0.0.0/0
      0           0                ACCEPT     ah  --   *     *    0.0.0.0/0          0.0.0.0/0
```

- I contatori sono in genere accessibili via SNMP con l'aiuto di un'interfaccia a riga di comando (CLI).
- I MIB proprietari abilitano la lettura dei valori anche in remoto.
- La Cisco ha recentemente introdotto una nuova tecnologia chiamata "Static NetFlow" che abilita i router ad emettere i flussi per ogni ACL definita.
- Il "ClearFlow" della Extreme Network è una tecnologia simile, ma con inoltre la capacità di lanciare degli allarmi settando delle soglie sui valori dei contatori.

4.5 NBAR: statistiche sul traffico in stile RMON

- Cisco NBAR (Network Based Application Recognition) è un motore per la classificazione del traffico con il supporto a QoS (Quality of Service) (cioè possono modellare il traffico in base alle statistiche).
- Esegue l'analisi dei modelli di traffico in real-time (con l'analisi del payload) e scopre i protocolli.
- Esempio di NBAR: fermare il traffico KaZaA e dare priorità al traffico di video conferenza.
- Ha la capacità di classificare le applicazioni che hanno:
  - I numeri di porta UDP o TCP staticamente assegnati.
  - Protocolli che non sono TCP o UDP IP.
  - Numeri di porta UDP o TCP assegnati dinamicamente durante la connessione.
  - Classificazione basata su una ispezione profonda del pacchetto: NBAR può guardare all'interno di un pacchetto per identificare le applicazioni.
  - Traffico HTTP via URL, nome dell'host o tipo MIME usando le espressioni regolari (*, ?, [ ]), Citrix ICA traffic, classificazione in base al tipo di payload RTP.
  - Attualmente supporta 88 protocolli/applicazioni.
- Le statistiche di NBAR possono essere lette usando SNMP (Cisco NBAR Protocol Discovery MIB).
- Attenzione:
  - Tecnologia proprietaria: disponibile solo sulle apparecchiature Cisco con una recente versione di IOS[21]
  - Forte impatto sulla CPU dei router (più di NetFlow).
  - Non riconosce tutti i protocolli.
  - Difficile da configurare, in particolare se associato con l'amministrazione di QoS/Larghezza di banda.

```
Router# conf t
Router(config)# ip cef
Router(config)# int eth0/0
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# exit
Router(config)# int se0/0
Router(config-if)# ip nbar protocol-discovery

Router# show ip nbar protocol discovery int eth0/0 top 3

FastEthernet0/0
Input                    Output
Protocol                 Packet Count             Packet Count
Byte Count               Byte Count
5 minute bit rate (bps)  5 minute bit rate (bps)
------------------------ ------------------------ ------------------------
ftp                      64175242                 45153848
89351513113              2484576000
1073000                  28000
http                     58194017                 32519125
82356099996              1958417833

Router# show policy-map int eth0/0

Ethernet0/0
Service-policy input: dscp_mark

Class-map: stream (match-any)
130521 packets, 97066868 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: protocol rtp
0 packets, 0 bytes
5 minute rate 0 bps
```

[21] Il software Cisco IOS è la piattaforma che consente l'implementazione dei servizi di rete e abilita le applicazioni di networking basate su infrastrutture Cisco Systems.

```
Match: protocol rtspplayer
117857 packets, 79344153 bytes
5 minute rate 0 bps
Match: protocol netshow
12664 packets, 17722715 bytes
5 minute rate 0 bps
Match: ip dscp ef
0 packets, 0 bytes
5 minute rate 0 bps
QoS Set
```

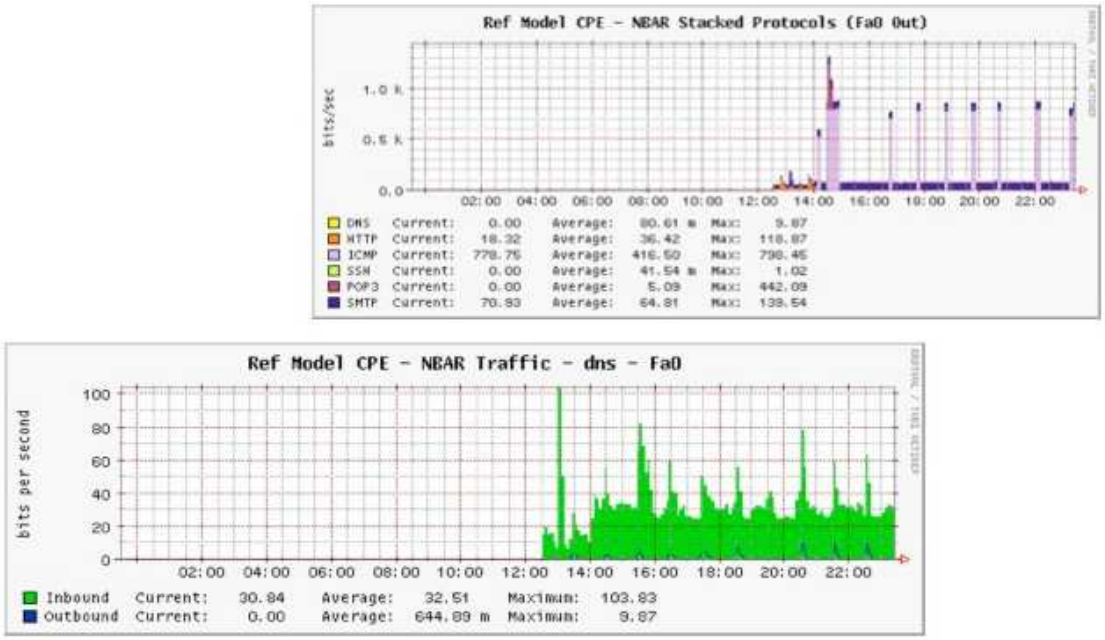
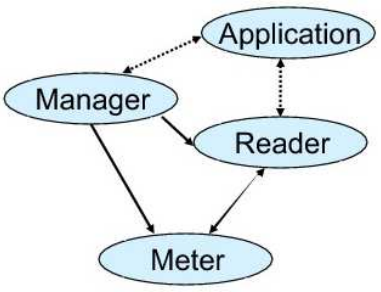


Figura 8: NBAR

4.6 Misurazioni del flusso in real-time (RTFM - Real-Time Flow Measurement)

- Un “Meter” veramente flessibile e potente.
  - Insiemi di regole programmabili.
  - Può servire molti utenti.
  - Si può programmare il comportamento al sovraccarico.
- Il “Reader” può prendere i sondaggi.
- Realizzato sul MIB SNMP Meter.
- Esiste un’implementazione free software NeTraMet.
- I produttori non lo accettano volentieri, sebbene sia standard.
- Complicato da usare (troppo potente).
- Specificato dalle RFC 2720-2742.



5 Monitoraggio del flusso

5.1 I flussi

- SNMP è basato su un paradigma manager-agent.

  - L'agent monitora la rete ed informa il manager (via trap) quando qualcosa di importante è successo (ad esempio, un interfaccia ha cambiato stato).
  - Il manager preleva l'intero stato del sistema periodicamente leggendo (polling) le variabili (ad esempio con le SNMP Get) dall'agent.
  - Le variabili SNMP possono essere usate sia per la gestione di elementi/dispositivi/sistema (ad esempio sullo spazio del disco e sulle partizioni) che il monitoraggio del traffico.

- I flussi di rete invece sono emessi da una sonda verso uno o più collezionatori a seconda delle condizioni di traffico.
  - I flussi contengono informazioni a proposito dell'analisi del traffico (cioè non contengono informazioni a proposito del dispositivo/sonda come con le variabili del MIB II).
  - I flussi emessi hanno un formato ben definito (ad esempio Cisco NetFlow v5) e spesso usano UDP come livello di trasporto (non protocolli specializzati come SNMP).
  - Non esiste il concetto di "allarme" sui flussi e la sonda non ha la capacità di eseguire delle operazioni in base al traffico: tutta la parte intelligente sta nel collezionatore.
  - L'instrumentazione della sonda viene fatta offline.
  - Le sonde vengono attivate dove fluisce il traffico di rete (ad esempio nei router o negli switch).

5.1.1 Quindi, cosa ci si aspetta di misurare con i flussi

- Con chi vi è uno scambio di traffico a seconda degli indirizzi IP, prefissi IP, o ASN (Automous System Number).
- Quanto traffico e di che tipo (SMTP, WEB, file sharing, etc. . .).
- Che servizi girano ad esempio in un ateneo universitario.
- Sommario dei traffici dei dipartimenti universitari.
- Tracciare la sorgente degli attacchi DoS (Denial of Service), ad esempio i 100 server che hanno inondato il dominio XXX.com.
- Trovare gli host che usano molto la rete (top host).
- Con quante destinazioni ogni host ha del traffico.
- Contare gli host che hanno dei servizi attivi, ad esempio quanti sono i server web attivi.

5.1.2 Cosa non si può misurare con i flussi

- Il traffico Non-IP (ad esempio NetBIOS, AppleTalk).
- Le informazioni a livello 2 (ad esempio il cambiamento di stato down/up delle interfacce).
- Il traffico filtrato (contare le politiche di un firewall).
- Statistiche per link (ad esempio l'uso del link, congestione, il ritardo, i pacchetti persi).
- Statistiche sulle applicazioni (ad esempio la latenza delle transazioni, il numero di risposte positive/negative, errori di protocollo).

5.1.3 I flussi di rete: cosa sono?

Un flusso è un insieme di pacchetti legati da un insieme comune di proprietà (ad esempio hanno stesso indirizzo IP e la stessa porta).

5.1.4 Emissione dei flussi

Un flusso viene (accodato) emesso solo quando lo si considera terminato.

- Politica di creazione e terminazione:
  - Quali condizioni fanno iniziare e finire un flusso?
  - Massima durata di un flusso senza considerare lo stato della connessione (ad esempio una connessione TCP finisce quando entrambi gli host si sono messi d'accordo sul FIN/RST).
  - Emettere un flusso quando non c'è traffico per una certa quantità di tempo.

5.1.5 I contenuti dei flussi di rete

- Un flusso contiene:
  - Host: sorgente e destinazione
  - Contatori: pacchetti, byte, tempo.
  - Informazioni sul routing: AS, maschera di rete, interfacce.
- I flussi possono essere unidirezionali (di default) o bidirezionali (solo NetFlow v9 e IPFIX[22]).
- Due opposti flussi unidirezionali corrispondono ad un unico flusso bidirezionale.
- I flussi bidirezionali possono contenere altre informazioni coma il round trip time o il comportamento del TCP.

5.1.6 I problemi dei flussi di rete

- Overhead (carico della CPU) contro accuratezza:
  - Molte misurazioni risultano in più dati collezionati.
  - Molta aggregazione, meno granularità.
  - Overhead sui router, switch e host.
- Sicurezza contro condivisione dati:
  - Il flusso emesso deve raggiungere il collezionatore attraverso un percorso protetto (ad esempio usando una differente rete/VLAN).
  - La privacy dell'utente deve essere rispettata.
  - Le misurazioni devono essere protette in modo da non divulgare informazioni importanti sulla rete a terze parti.

5.1.7 Esempi di flussi

5.1.8 Aggregazione del flusso

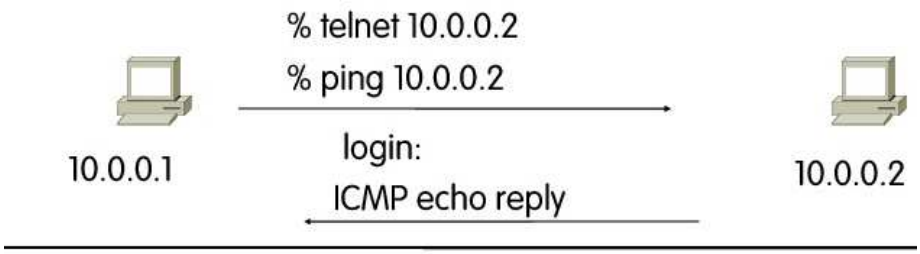
Vengono usati i flussi grezzi, ma spesso è necessario rispondere ad alcune domande, tipo:

- Quanto del traffico è web, mail, news, quake?
- Quanto del traffico va verso o parte da un dipartimento.
- Quanto del traffico va verso altri specifici dipartimenti, il provider X, Goolge, etc. . . ?
- Quanto traffico passa dall'interfaccia X?

Lo stesso flusso può essere aggregato più volte usando criteri differenti. Ad esempio, dai flussi grezzi è possibile generare:

- Lista dei protocolli.
- Matrice delle conversazioni (chi parla con chi).

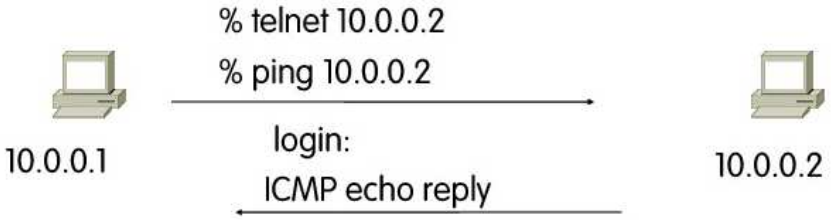
[22] Internet Protocol Flow Information Export (IPFIX) è la versione standardizzata dalla IETF del NetFlow v9 della Cisco.



Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Figura 9: Flussi unidirezionali tramite indirizzo IP sorgente/destinazione



Active Flows

Flow	Source IP	Destination IP	Proto	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Figura 10: Flussi unidirezionali tramite indirizzo IP, porta e protocollo

Main Active Flow Table

Flow	Source IP	Destination IP	Proto	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Source/Destination IP Aggregation

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Figura 11: Aggregazione del flusso

- Le porte TCP/UDP più usate.

L'aggregazione del flusso è più veloce e usa meno memoria se viene fatta subito, piuttosto che farla dopo. Ad esempio, la matrice delle conversazioni è molto più semplice farla sulla sonda invece di usare grezzi flussi aggregati.

- I flussi possono essere aggregati usando anche criteri "esterni" e non solo usando i grezzi campi del flusso.
- Generalmente questi criteri esterni sono applicati su delle "chiavi" (e non sui "valori") dei campi come una porta, l'indirizzo IP, protocollo, etc. . . , e sono usati per raggruppare insieme i valori.
- I criteri sono aggiunti (e non rimpiazzano) i campi esistenti.
- Esempio: port-map, protocol-map, ip-address

```
       IP src   IP dst   Proto Src port Dst port
Before 10.0.0.1 10.0.0.2 UDP   32000    53
       10.0.0.2 10.0.0.1 TCP   34354    80

      IP src   IP dst   Proto Src port Dst port Src port map Dst port map
After 10.0.0.1 10.0.0.2 TCP   32000    53       udp_other    domain
      10.0.0.2 10.0.0.1 TCP   34354    80       tcp_other    http
```

- I flussi possono essere aggregati secondo:
  - Porta TCP/UDP, ToS (Type of Service), protocollo (ad esempio ICMP, UDP), AS.
  - IP sorgente/destinazione.
  - Sottorete, ora del giorno.
- L'aggregazione può essere fatta sulla sonda, sul collezionatore o su entrambi.
- L'aggregazione fatta sulla sonda è veramente efficace in termini di uso delle risorse e di flusso del traffico di rete.
- L'aggregazione sul collezionatore è più potente (ad esempio aggregando i flussi prodotti da più sonde) ma è piuttosto costosa (riceve tutti gli aggregati).

5.1.9 Filtrare i flussi

Filtrare i flussi significa: scartare i flussi in base a qualche criterio come:

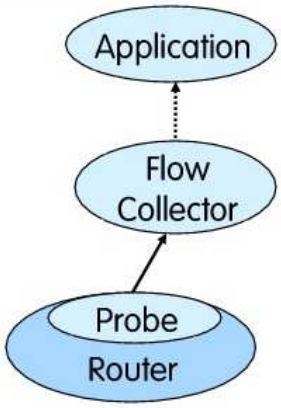
- Durata del flusso (ad esempio, scartare i flussi che non sono stati visti per più di X secondi).
- Sorgente/destinazione del flusso (ad esempio, ignorare i flussi che contengono indirizzi broadcast).
- Porta del flusso (ad esempio, ignorare i flussi originati sulla porta X).

Si noti che:

- Il filtraggio è diverso dall'aggregazione: fanno due lavori differenti.
- Il filtraggio e l'aggregazione possono coesistere.
- Il filtraggio viene generalmente applicato prima dell'aggregazione e non dopo.

5.2 Architettura di NetFlow

- I flussi sono esportati (push) dalla sonda quando questi finiscono, al contrario di SNMP dove il manager interroga (pull) l'agent periodicamente.
- Il protocollo di trasporto è NetFlow (e non SNMP).
- La configurazione della sonda e del collezionatore non è specificata dal protocollo NetFlow.
- Il collezionatore NetFlow ha il compito di assemblare e capire i flussi esportati e combinarli o aggregarli in modo da creare report significativi del traffico e per l'analisi della sicurezza.



Le figure 12 e 13 mostrano degli esempi di come si possono collezionare i dati.

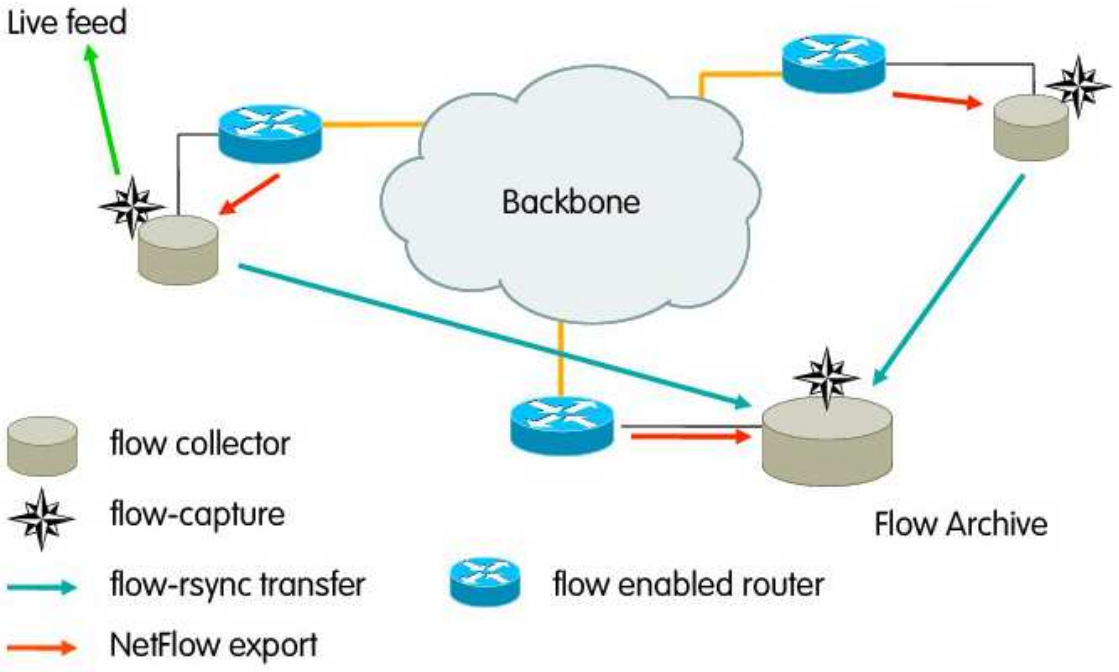


Figura 12: Architettura di NetFlow

5.2.1 Vincoli di spazio per il collezionatore

- Lo spazio richiesto dipende dal traffico.
- Qualche cifra media:
  - 67.320 ottetti/flusso, 92 pacchetti/flusso.
  - Occupazione dei router: 397 GB di traffico/giorno, 548.000.000 di pacchetti/giorno == 5.900.000 pacchetti/giorno.
  - A 60 byte/flusso ci vogliono 350 MB di log/giorno.
  - Con una compressione di livello 6 si ha 4.3:1.
  - Lavoro per 82 MB/giorno per un router.

5.2.2 Nozioni di base per Cisco NetFlow

- Flussi unidirezionali (fino alla v8), bidirezionali sulla v9.
- Molte versioni, v1,5,6,7,8,9. La più comune è la v5, l'ultima è la v9.
- Si analizza solo il traffico IP (non su tutte le piattaforme) e solo inbound (cioè il traffico che entra nel router).
- IPv4 unicast e multicast: tutte le versioni di NetFlow. IPv6 è supportata solo dalla v9.
- Protocollo aperto definito dalla Cisco e supportato dalle piattaforme IOS e CatIOS (nessun NetFlow è supportato dai firewall PIX) così come sulle piattaforme on-Cisco.

5.2.3 Versioni di Cisco NetFlow

- Ogni versione ha proprio formato per il pacchetto:
  - v1,5,6,7,8 hanno un loro fissato/chiuso, specifico formato.

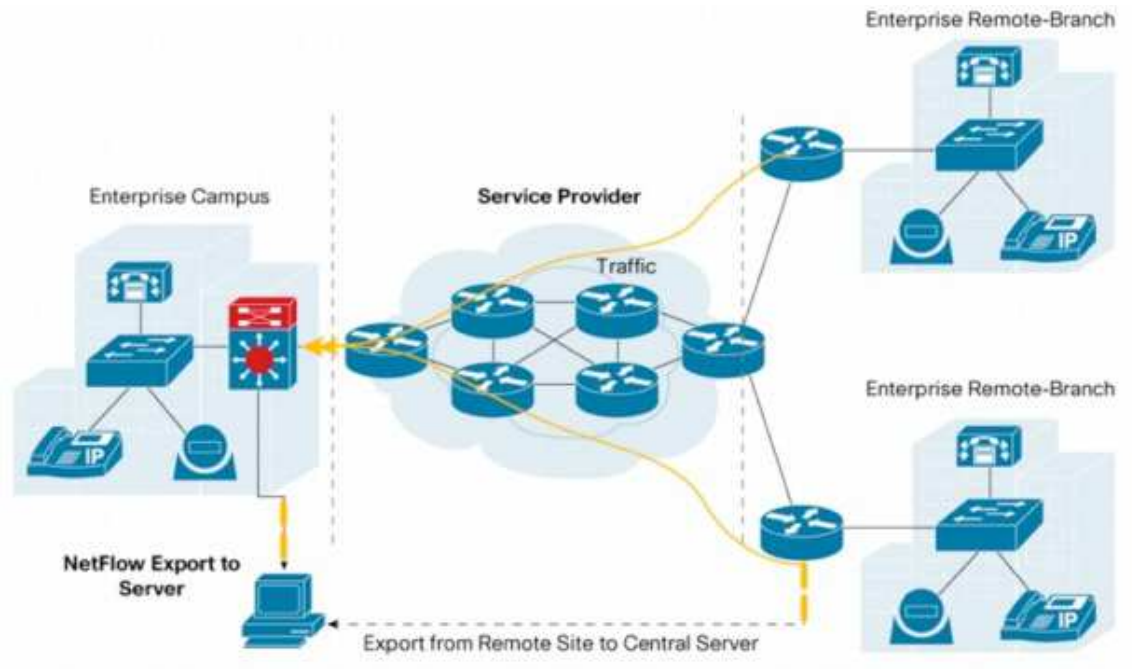


Figura 13: Architettura di NetFlow

  - v9 è dinamico e aperto alle estensioni.

- Numeri di sequenza:
  - v1 non ha numeri di sequenza (nessun modo per determinare la perdita di flussi).
  - v5,6,7,8 i numeri di sequenza per i flussi (cioè tiene traccia del numero di flussi emessi).
  - v9 ha i numeri di sequenza per i pacchetti (no per i flusso) (cioè è facile capire il numero di pacchetti persi, ma non di flussi persi).
- La "versione" stabilisce che tipo di dato c'è nel flusso.
- Qualche versione (ad esempio la v7) è specifico per le piattaforme Catalyst della Cisco.

5.2.4 Netflow: nascita e morte di un flusso

- Di ogni pacchetto che è stato inviato al router o ad uno switch di livello 3 viene analizzato un insieme di attributi IP.
- Tutti i pacchetti che hanno lo stesso:
  - indirizzo IP di sorgente e destinazione.
  - porta sorgente e destinazione.
  - protocollo.

  sono raggruppati insieme e vengono contati sia i byte che i pacchetti.
- I flussi attivi vengono salvati in memoria, in quella che viene chiamata, cache NetFlow.

La figura 14 mostra come avviene la creazione del flusso.
I flussi terminano quando avviene una di queste condizioni:

- La comunicazione è finita (ad esempio la comunicazione contiene il flag TCP FIN o RST).
- È durato troppo (di default 30 minuti).
- Il flusso non è più attivo (non sono stati ricevuti pacchetti) da troppo tempo (di default 15 secondi).

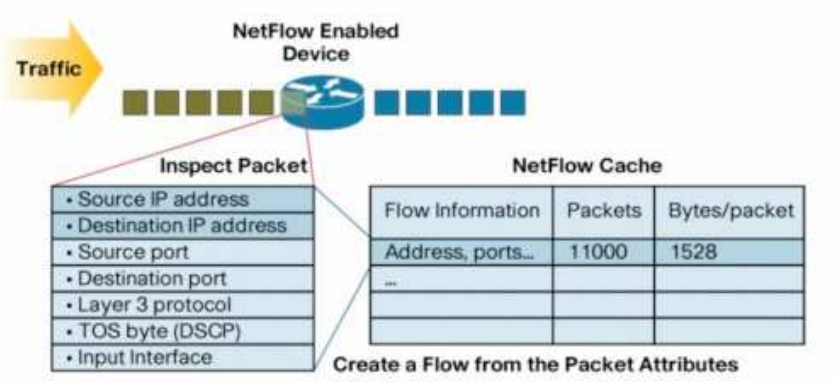


Figura 14: NetFlow: nascita del flusso

- La cache NetFlow è piena e il gestore della cache deve eliminare qualche dato.

Si noti che la cache NetFlow ha una dimensione limitata, quindi spesso non è possibile inserirvi tutti i flussi (si veda la figura 15).

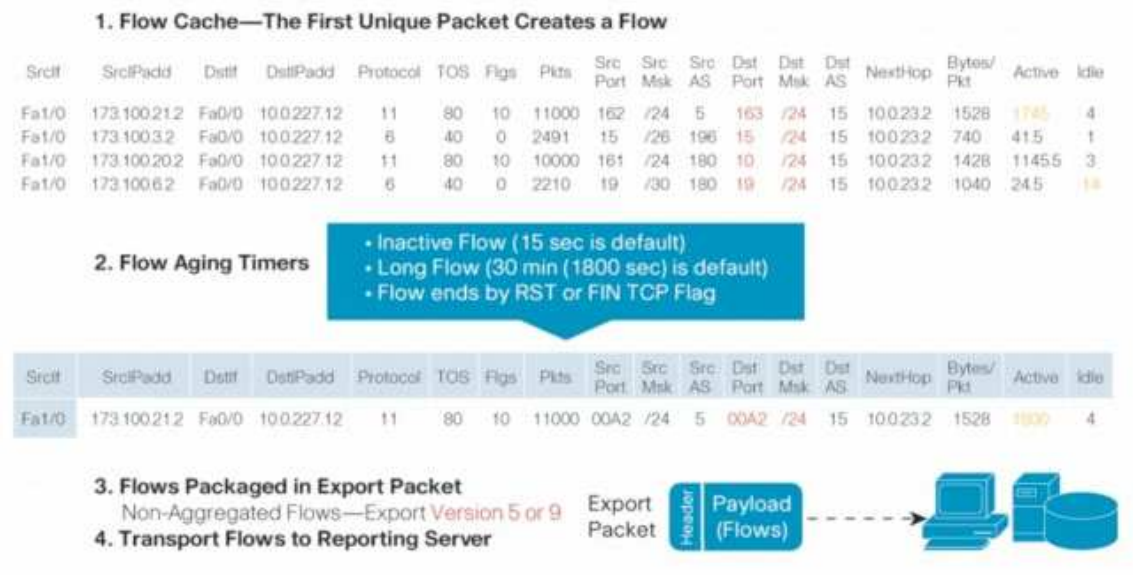


Figura 15: NetFlow: politiche di esportazione dei flussi dalla cache NetFlow

- La cache NetFlow si riempie costantemente di flussi, quindi il software all'interno del router o dello switch va in cerca di quei flussi che sono terminati o scaduti e li esporta verso il collezionatore.
- Una conseguenza è che il flusso di rete viene spezzato in molti flussi NetFlow che, se necessario, vengono riassemblati dal collezionatore.

5.2.5 Formato del pacchetto del flusso

- Un header comune tra le versioni esportate.
- Vengono esportati N record e la versione specifica cosa contengono.
- N viene determinato dalla definizione del flusso (ad esempi N=30 per v5). La dimensione del pacchetto viene mantenuta sotto i 1480 byte circa in modo da non avere nessuna frammentazione a livello ethernet.

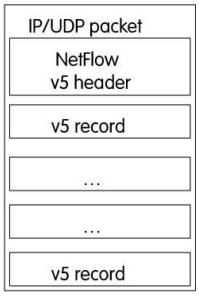


Figura 16: Pacchetto NetFlow v5

5.3 Cisco NetFlow v5

```
struct netflow5_record {
  struct flow_ver5_hdr flowHeader;
  struct flow_ver5_rec flowRecord[30];
} NetFlow5Record;

struct flow_ver5_hdr {
  u_int16_t version;                /* Current version=5*/
  u_int16_t count;                  /* The number of records in PDU. */
  u_int32_t sysUptime;              /* Current time in msecs since router booted */
  u_int32_t unix_secs;              /* Current seconds since 0000 UTC 1970 */
  u_int32_t unix_nsecs;             /* Residual nanoseconds since 0000 UTC 1970 *
  u_int32_t flow_sequence;          /* Sequence number of total flows seen */
  u_int8_t engine_type;             /* Type of flow switching engine (RP,VIP,etc.)*/
  u_int8_t engine_id;               /* Slot number of the flow switching engine */

  struct flow_ver5_rec {
    u_int32_t srcaddr;   /* Source IP Address */
    u_int32_t dstaddr;   /* Destination IP Address */
    u_int32_t nexthop;   /* Next hop router's IP Address */
    u_int16_t input;     /* Input interface index */
    u_int16_t output;    /* Output interface index */
    u_int32_t dPkts;     /* Packets sent */
    u_int32_t dOctets;   /* Octets sent */
    u_int32_t First;     /* SysUptime at start of flow */
    u_int32_t Last;      /* and of last packet of the flow */
    u_int16_t srcport;   /* TCP/UDP source port number (.e.g, FTP, Telnet, etc.,or equivalent) */
    u_int16_t dstport;   /* TCP/UDP destination port number (.e.g, FTP, Telnet, etc.,or equivalent) */
    u_int8_t pad1;       /* pad to word boundary */
    u_int8_t tcp_flags;  /* Cumulative OR of tcp flags */
    u_int8_t prot;       /* IP protocol, e.g., 6=TCP, 17=UDP, etc... */
    u_int8_t tos;        /* IP Type-of-Service */
    u_int16_t src_as;    /* source peer/origin Autonomous System */
    u_int16_t dst_as;    /* dst peer/origin Autonomous System */
    u_int8_t src_mask;   /* source route's mask bits */
    u_int8_t dst_mask;   /* destination route's mask bits */
    u_int16_t pad2;      /* pad to word boundary */
  };
```

5.4 NetFlow v9

5.4.1 Perché se ne ha bisogno?

- I formati fissi (dalla versione 1 alla 8) sono:
  - Facili da implementare.
  - Consumano poca larghezza di banda.
  - Sono facili da decifrare per il collezionatore.
  - Non flessibili (molti ???)
  - Non estensibili (non c'è modo di estendere il flusso a meno che non venga definita una nuova versione).

– Qualche caratteristica viene persa: livello 2, VLAN, IPv6, MPLS[23].

5.4.2 I principi

- Protocollo aperto definito da Cisco (non è proprietario) nelle RFC 3954.
- Template di flusso + record di flusso
  - Il template è composto da tipo e lunghezza.
  - Il record di un flusso è composto da un template ID e da un valore.
  - I template sono spediti periodicamente e sono il prerequisito per decodificare i record del flusso.
  - I record del flusso contengono "la ciccia".
- Template di opzioni + record di opzioni, contengono la configurazione della sonda (ad esempio, la velocità di campionamento, interfaccia dei pacchetti).
- Modello push della sonda verso il collezionatore (come nelle precedenti versioni).
- Spedisce i template regolarmente: ogni X flussi, ogni X secondi.
- Indipendente dal protocollo sottostante, pronto per ogni protocollo affidabile.
- Può spedire sia i template che i record di flusso in una sola esportazione.
- Può inserire differenti record di flussi in una sola esportazione.

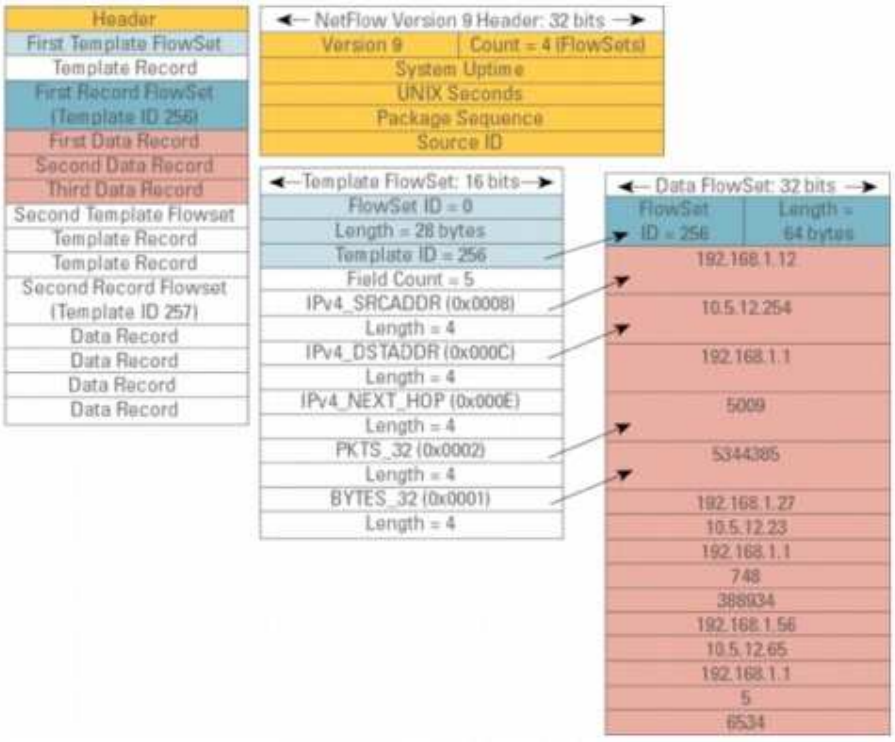


Figura 17: Formato di NetFlow v9

[23]Multiprotocol Label Switching (MPLS) è un meccanismo delle reti performanti che dirige e trasporta i dati direttamente da un nodo della rete ad un altro. MPLS rende facile la creazione di "link virtuali" tra due nodi distanti. È in grado di incapsulare vari tipi di protocolli.

5.4.3 Qualche tag

```
[ 1] %IN_BYTES                Incoming flow bytes
[ 2] %IN_PKTS                 Incoming flow packets
[ 3] %FLOWS                   Number of flows
[ 4] %PROTOCOL                IP protocol byte
[ 5] %SRC_TOS                 Type of service byte
[ 6] %TCP_FLAGS               Cumulative of all flow TCP flags
[ 7] %L4_SRC_PORT             IPv4 source port
[ 8] %IPV4_SRC_ADDR           IPv4 source address
[ 9] %SRC_MASK                Source subnet mask (/<bits>)
[ 10] %INPUT_SNMP             Input interface SNMP idx
[ 11] %L4_DST_PORT            IPv4 destination port
[ 12] %IPV4_DST_ADDR          IPv4 destination address
[ 13] %DST_MASK               Dest subnet mask (/<bits>)
[ 16] %SRC_AS                 Source BGP AS
[ 17] %DST_AS                 Destination BGP AS
[ 21] %LAST_SWITCHED          SysUptime (msec) of the last flow pkt
[ 22] %FIRST_SWITCHED         SysUptime (msec) of the first flow pkt
[ 23] %OUT_BYTES              Outgoing flow bytes
[ 24] %OUT_PKTS               Outgoing flow packets
[ 27] %IPV6_SRC_ADDR          IPv6 source address
[ 28] %IPV6_DST_ADDR          IPv6 destination address
[ 29] %IPV6_SRC_MASK          IPv6 source mask
[ 30] %IPV6_DST_MASK          IPv6 destination mask
[ 32] %ICMP_TYPE              ICMP Type * 256 + ICMP code
[ 34] %SAMPLING_INTERVAL      Sampling rate
[ 37] %FLOW_INACTIVE_TIMEOUT  Inactivity timeout of flow cache entries
[ 38] %ENGINE_TYPE            Flow switching engine
[ 39] %ENGINE_ID              Id of the flow switching engine
[ 40] %TOTAL_BYTES_EXP        Total bytes exported
[ 41] %TOTAL_PKTS_EXP         Total flow packets exported
[ 42] %TOTAL_FLOWS_EXP        Total number of exported flows
[ 56] %IN_SRC_MAC             Source MAC Address
[ 57] %OUT_DST_MAC            Destination MAC Address
[ 58] %SRC_VLAN               Source VLAN
[ 59] %DST_VLAN               Destination VLAN
[ 60] %IP_PROTOCOL_VERSION    [4=IPv4][6=IPv6]
[ 70] %MPLS_LABEL_1           MPLS label at position 1
[ 71] %MPLS_LABEL_2           MPLS label at position 2
[ 72] %MPLS_LABEL_3           MPLS label at position 3
[ 73] %MPLS_LABEL_4           MPLS label at position 4
[ 74] %MPLS_LABEL_5           MPLS label at position 5
[ 75] %MPLS_LABEL_6           MPLS label at position 6
[ 76] %MPLS_LABEL_7           MPLS label at position 7
[ 77] %MPLS_LABEL_8           MPLS label at position 8
[ 78] %MPLS_LABEL_9           MPLS label at position 9
[ 79] %MPLS_LABEL_10          MPLS label at position 10
[ 80] %IN_DST_MAC             Source MAC Address
[ 81] %OUT_SRC_MAC            Destination MAC Address
```

5.4.4 Esempio

```
Cisco NetFlow
    Version: 9
    Count: 4
    SysUptime: 1132427188
    Timestamp: Aug 18, 2000 23:49:25.000012271
        CurrentSecs: 966635365
    FlowSequence: 12271
    SourceId: 0
    FlowSet 1/4
 FlowSet 1/4
        Template FlowSet: 0
        FlowSet Length: 164
        Template Id: 257
        Field Count: 18
        Field (1/18)
            Type: LAST_SWITCHED (21)
            Length: 4

Cisco NetFlow
```

```
    Version: 9
    Count: 1
    SysUptime: 1133350352
    Timestamp: Aug 19, 2000 00:04:48.000012307
        CurrentSecs: 966636288
    FlowSequence: 12307
    SourceId: 0
    FlowSet 1/1
        Data FlowSet (Template Id): 257
        FlowSet Length: 52
        pdu 1
            EndTime: 1133334.000000000 seconds
            StartTime: 1133334.000000000 seconds
            Octets: 84
            Packets: 1
            InputInt: 15
```

5.4.5 Template di opzioni

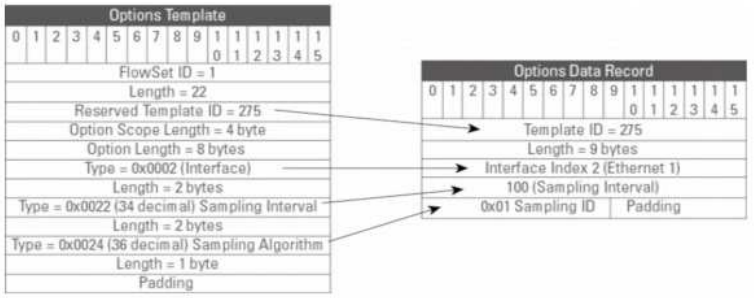


Figura 18: NetFlow v9: template di opzioni

5.4.6 v5 contro v9

	v5	v9
Formato del flusso	Fisso	Definito dall'utente
Estensibile	No	Si (definendo un nuovo campo FlowSet)
Tipo di flusso	Unidirezionale	Bidirezionale
Dimensione del flusso	48 byte (fisso)	Dipende dal formato
IPv6	No	IPv4 e IPv6
MPLS/VLAN	No	Si

5.5 Cisco IOS

5.5.1 Configurazione

- Configurato su ogni interfaccia di input.
- Definire la versione.
- Definire l'indirizzo IP del collezionatore (dove esportare i flussi).
- Opzionalmente abilita l'aggregazione delle tabelle.
- Opzionalmente configura il timeout del flusso e la principale (v5) dimensione della tabella di flusso.
- Opzionalmente configura la velocità di campionamento.

```
interface FastEthernet0/0/0
 ip address 10.0.0.1 255.255.255.0
 no ip directed-broadcast
 ip route-cache flow
```

```
interface ATM1/0/0
 no ip address
 no ip directed-broadcast
 ip route-cache flow

interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast

ip flow-export version 5 origin-as
ip flow-export destination 10.0.0.10 5004
ip flow-export source loopback 0

ip flow-aggregation cache prefix
 export destination 10.0.0.10 5555
 enabled
```

5.5.2 Report

```
#sh ip flow export
Flow export is enabled
  Exporting flows to 10.0.0.10 (5004)
  Exporting using source IP address 10.10.10.10
  Version 5 flow records, origin-as
  Cache for prefix aggregation:
    Exporting flows to 10.0.0.10 (5555)
    Exporting using source IP address 10.10.10.10
  3176848179 flows exported in 105898459 udp datagrams
  0 flows failed due to lack of export packet
  45 export packets were sent up to process level
  0 export packets were punted to the RP
  5 export packets were dropped due to no fib
  31 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to output drops

#sho ip ca fl
IP packet size distribution (106519M total packets):
   1-32    64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002  .405 .076 .017 .011 .010 .007 .005 .004 .005 .004 .004 .003 .002 .002

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .002 .006 .024 .032 .368 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  36418 active, 29118 inactive, 3141073565 added
  3132256745 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol          Total   Flows   Packets Bytes Packets Active(Sec) Idle(Sec)
--------          Flows    /Sec     /Flow  /Pkt      /Sec    /Flow     /Flow
TCP-Telnet      2951815     0.6        61   216      42.2     26.6      21.4
TCP-FTP        24128311     5.6        71   748     402.3     15.0      26.3
TCP-FTPD        2865416     0.6       916   843     611.6     34.7      19.8
TCP-WWW       467748914   108.9        15   566    1675.8      4.9      21.6
TCP-SMTP       46697428    10.8        14   370     159.6      4.0      20.1
TCP-X            521071     0.1       203   608      24.7     24.5      24.2
TCP-BGP         2835505     0.6         5    94       3.3     16.2      20.7
TCP-other    1620253066   377.2        47   631   18001.6     27.3      23.4
UDP-DNS       125622144    29.2         2    78      82.5      4.6      24.7
UDP-NTP        67332976    15.6         1    76      22.0      2.7      23.4
UDP-TFTP          37173     0.0         2    76       0.0      4.1      24.6
UDP-Frag          68421     0.0       474   900       7.5    111.7      21.6
UDP-other     493337764   114.8        17   479    1990.3      3.8      20.2
ICMP          243659509    56.7         3   166     179.7      3.3      23.3
IGMP              18601     0.0        96    35       0.4    941.4       8.1
IPINIP            12246     0.0        69    52       0.1    548.4      15.2
```

```
GRE              125763     0.0       235   156       6.9     50.3      21.1
IP-other       75976755    17.6         2    78      45.4      3.9      22.8
Total:       3176854246   739.6        33   619   24797.4     16.2      22.6

SrcIf         SrcIPaddress     DstIf        DstIPaddress   Pr  SrcP DstP   Pkts
AT5/0/0.4     206.21.162.150   AT1/0/0.1    141.219.73.45  06  0E4B A029    507
AT4/0/0.10    132.235.174.9    AT1/0/0.1    137.99.166.126 06  04BE 074C      3
AT4/0/0.12    131.123.59.33    AT1/0/0.1    137.229.58.168 06  04BE 09BB    646
AT1/0/0.1     137.99.166.126   AT4/0/0.10   132.235.174.9  06  074C 04BE      3

#show ip flow top-talkers
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et1/0  172.16.10.2 Et0/0  172.16.1.84 06 0087 0087 2100
Et1/0  172.16.10.2 Et0/0  172.16.1.85 06 0089 0089 1892
Et1/0  172.16.10.2 Et0/0  172.16.1.86 06 0185 0185 1762
Et1/0  172.16.10.2 Et0/0  172.16.1.86 06 00B3 00B3 2
Et1/0  172.16.10.2 Et0/0  172.16.1.84 06 0050 0050 1
Et1/0  172.16.10.2 Et0/0  172.16.1.85 06 0050 0050

17 of 10 top talkers shown. 7 flows processed.

#show ip flow top 10 aggregate destination-address
There are 3 top talkers:
IPV4 DST-ADDR        bytes       pkts      flows
=============== ========== ========== ==========
172.16.1.86            160          4          2
172.16.1.85            160          4          2
172.16.1.84            160          4          2

#show ip flow top 10 aggregate destination-address sorted-by bytes match
source-port min 0 max 1000
There are 3 top talkers:
IPV4 DST-ADDR        bytes       pkts      flows
=============== ========== ========== ==========
172.16.1.84             80          2          2
172.16.1.85             80          2          2
172.16.1.86             80          2         26 of 6 flows matched.
```

5.6 Configurazione JunOS

- Pacchetti campione filtrati da un firewall e inviati verso un motore di routing.
- La velocità di campionamento è limitata a 7000pps (packets per seconds) indirizzati al prossimo PIC (Physical Interface Card).
- Buono per il controllo del traffico, ma non troppo efficace per scoprire attacchi DoS o le intrusioni.
- Juniper [24] chiama NetFlow cflowd (un popolare collezionatore fornito dalla CAIDA).

Filtri per il firewall

```
firewall {
  filter all {
    term all {
      then {
        sample;
        accept;
      }
    }
  }
}
```

Abilitare il campionamento/flusso

```
forwarding-options {
  sampling {
    input {
      family inet {
        rate 100;
      }
    }
    output {
      cflowd 10.0.0.16{
        port 2055;
        version 5;
      }
    }
  }
}
```

Applicare i filtri del firewall ad ogni interfaccia

```
interfaces {
  ge-0/3/0 {
    unit 0 {
      family inet {
        filter {
          input all;
          output all;
        }
        address 192.148.244.1/24;
      }
    }
  }
```

[24] JunOS è un sistema operativo di rete affidabile e ad alte prestazioni per router, switch e dispositivi di sicurezza sviluppato da Juniper.

5.7 Sonde NetFlow basate sui PC

- Ci sono sonde NetFlow basate sui PC.
- Molte di queste si basano sulla libreria pcap.
- nProbe (www.ntop.org/nProbe.html):
  - Open Source (GPL2).
  - Una sonda veloce sul mercato.
  - Supporta sia NetFlow v5,v9 che IPFIX.
  - Formato flessibile per i flussi esportati.
  - Supporta IPv4/v6, un template flessibile (non sempre supportato da Cisco).
  - Disponibile sia per Linux che per Windows.

5.8 IPFIX

5.8.1 Campo di applicazione e requisiti generali

- Scopo: trovare o sviluppare una base comune per la misurazione del flusso di traffico IP in modo che sia disponibile su (quasi) tutti i router futuri.
- Requisiti che soddisfano molte applicazioni.
- Basso costo hardware/software.
- Semplice e scalabile.
- Dovrebbe essere integrabile su tutti i router IP e altri dispositivi (sonde o middle boxe[25]).
- Processare i dati in modo che sia integrato su varie applicazioni.
- Interoperabilità sia nell'apertura che nella standardizzazione.

5.8.2 In breve

- Fortemente basato su NetFlow v9.
- Capacità di definire nuovi campi per il flusso usando un formato standard (OID).
- Il trasporto del flusso è basato su SCTP (Stream Control Transport Protocol), opzionalmente su supporto UDP/TCP.
- Stato corrente: bozza della specifica di protocollo.
- In pratica: IPFIX = NetFlow v9 su SCTP.

5.9 Flussi e sicurezza

NetFlow e IPFIX possono essere usati anche a livello di sicurezza e non solo per la gestione del traffico:

- Possono individuare portscan[26]/portmap[27].
- Scovare attività su porte sospette.
- Identificare la sorgente di uno SPAM, disabilitare i server (ad esempio un server file).

[25] I middle boxe sono quei dispositivi che si trovano nel mezzo del traffico, come appunto i router, switch, etc....
[26] Si scansionano tutte le porte alla ricerca dei servizi attivi.
[27] Scovare un host con il servizio RPC (Remote Procedure Call) attivo. Questo servizio permette di eseguire delle elaborazioni remote.

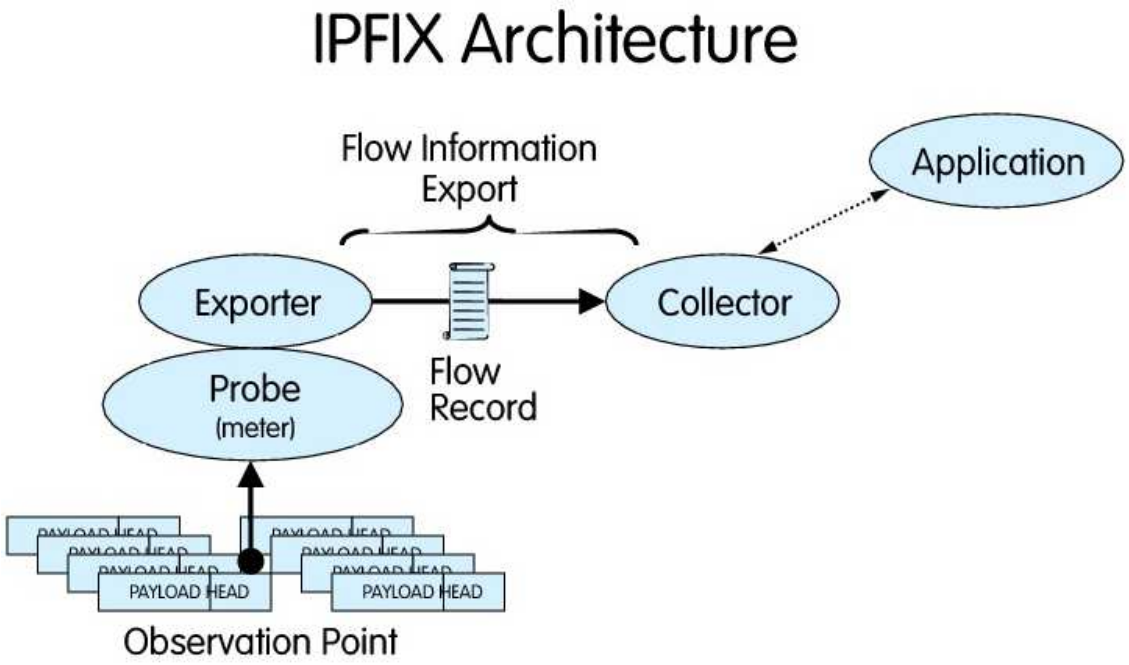


Figura 19: Architettura di IPFIX

5.9.1 Portmap

```
Start       SrcIPaddress    SrcP DstIPaddress DstP P Pkts
10:53:42.50 165.132.86.201  9781 128.146.0.76  111 6    1
10:53:42.54 165.132.86.201  9874 128.146.0.7   111 6    1
10:53:42.54 165.132.86.201  9982 128.146.0.80  111 6    1
10:53:42.54 165.132.86.201  9652 128.146.0.74  111 6    1
10:53:42.54 165.132.86.201  9726 128.146.0.75  111 6    1
10:53:42.54 165.132.86.201  9855 128.146.0.77  111 6    1
10:53:42.58 165.132.86.201 10107 128.146.0.82  111 6    1
```

In un breve lasso di tempo ci sono molti pacchetti con lo stesso indirizzo sorgente ma con differenti indirizzi di destinazione e tutti sulla stessa porta di destinazione (porta 111=RPC (Remote Procedure Call)).

5.9.2 Trovare le backdoor

```
Start    SrcIPaddress   SrcP DstIPaddress    DstP P Pkts
19:08:40 165.132.86.201 8401 128.146.172.232 1524 6  19
19:08:40 165.132.86.201 8422 128.146.172.230 1524 6  16
19:08:40 165.132.86.201 8486 128.146.172.234 1524 6  19
19:08:40 165.132.86.201 8529 128.146.172.236 1524 6  10
19:08:41 165.132.86.201 8614 128.146.172.237 1524 6  16
19:08:41 165.132.86.201 8657 128.146.172.238 1524 6  22
```

Come il portmap, solo si cercano porte aperte da applicazioni conosciute, nell'esempio la porta di destinazione è la 1524 (trinoo backdoor port http://www.auditmypc.com/port/tcp-port-1524.asp).

5.9.3 Trovare le intrusioni

Semplice sistema IDS[28] basato sui flussi:

- I flussi che hanno troppi ottetti o troppi pacchetti (troppi dati: floods - inondazione).
- Lo stesso IP sorgente contatta più di N destinazioni - host scanning.
- Lo stesso IP sorgente contatta più di M porte per la stessa destinazione - port scanning.

[28] Intrusion Detection System

6 sFlow

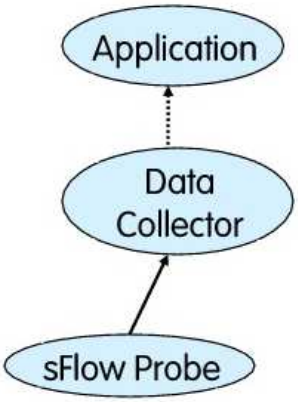
6.1 sFlow

6.1.1 Principi

- Non si pretenda di essere veloce come la rete che si vuole monitorare: si perderanno comunque dei dati.
- Anche se si riesce a monitorare tutto, si avranno comunque delle difficoltà nel gestire tutti i flussi generati.
- Analizzare 1 pacchetto ogni X pacchetti (campionamento).
- Più pacchetti si analizza, più si avranno dati precisi.
- Se la rete è troppo veloce, si aumenta il valore di campionamento.

6.1.2 Architettura

- La sonda campiona il traffico.
- I pacchetti campione sono spediti (nel formato sFlow) al collezionatore.
- Periodicamente la sonda invia le statistiche raccolte sulle interfacce (i contatori MIB II SNMP) dentro i pacchetti sFlow. I pacchetti sono usati per "scalare" il traffico.



6.1.3 Specifiche

- Specificato nelle RFC 3176 (RFC informative) proposte dalla InMon Inc..
- Definisce:
  - Formato del pacchetto sFlow (UDP, no SNMP).
  - Un MIB SNMP per accedere ai dati sFlow raccolti (http://support.ipmonitor.com/mibs/SFLOW-MIB/tree.aspx).
- L'architettura di sFlow è simile a quella di NetFlow: la sonda spedisce i pacchetti sFlow al collezionatore.
- La sonda sFlow è in pratica uno sniffer che cattura 1 pacchetto su X (la proporzione di default è 1:400).
- Questi pacchetti sono spediti al collezionatore codificati nel formato sFlow.
- Periodicamente la sonda spedisce altri pacchetti sFlow che contengono statistiche sulle interfacce di rete (ad esempio i contatori del traffico dell'interfaccia), statistiche che sono usate per scalare i dati raccolti.
- Usando delle formule statistiche è possibile produrre un rapporto abbastanza preciso del traffico.
- $\%Errore\ di\ campionamento \leq 196 \times \sqrt{\frac{1}{numero\ di\ campioni}}$

  http://www.sflow.org/packetSamplingBasics/.
- sFlow è scalabile (basta incrementare il rapporto di campionamento) anche sulle 10 GB e oltre.
- ntop.org è parte del consorzio sFlow.org.

6.1.4 Il pacchetto

```
struct sample_datagram_v5 {
   address agent_address          /* IP address of sampling agent,
                                     sFlowAgentAddress. */
   unsigned int sub_agent_id;     /* Used to distinguishing between datagram
                                     streams from separate agent sub entities
                                     within an device. */
   unsigned int sequence_number;  /* Incremented with each sample datagram
                                     generated by a sub-agent within an
                                     agent. */
   unsigned int uptime;           /* Current time (in milliseconds since device
                                     last booted). Should be set as close to
                                     datagram transmission time as possible.
                                     Note: While a sub-agents should try and
                                           track the global sysUptime value
                                           a receiver of sFlow packets must
                                           not assume that values are
                                           synchronised between sub-agents. */
   sample_record samples<>;        /* An array of sample records */
}

struct flow_sample {
   unsigned int sequence_number;  /* Incremented with each flow sample
                                     generated by this source_id.
                                     Note: If the agent resets the
                                           sample_pool then it must
                                           also reset the sequence_number.*/
   sflow_data_source source_id;   /* sFlowDataSource */
   unsigned int sampling_rate;    /* sFlowPacketSamplingRate */
   unsigned int sample_pool;      /* Total number of packets that could have
                                     been sampled (i.e. packets skipped by
                                     sampling process + total number of
                                     samples) */
   unsigned int drops;            /* Number of times that the sFlow agent
                                     detected that a packet marked to be
                                     sampled was dropped due to
                                     lack of resources. The drops counter
                                     reports the total number of drops
                                     detected since the agent was last reset.
                                     A high drop rate indicates that the
                                     management agent is unable to process
                                     samples as fast as they are being
                                     generated by hardware. Increasing
                                     sampling_rate will reduce the drop
                                     rate. Note: An agent that cannot
                                     detect drops will always report
                                     zero. */

   interface input;               /* Interface packet was received on. */
   interface output;              /* Interface packet was sent on. */

   flow_record flow_records<>;    /* Information about a sampled packet */
}
```

6.1.5 sFlow verso NetFlow

	sFlow	NetFlow
Ambiente nativo	Switch	Router
Velocità a cui può operare	Multigigabit	1 GB o meno
Campionamento	Sempre	Qualche volta
Monitoraggio	Statistico	Accurato (nessuna perdita)

6.2 RADIUS [RFC 2139, 1997]

RADIUS è l'acronimo di Remote Authentication Dial In User Service, specificato nelle seguenti RFC:

- Protocollo di autenticazione

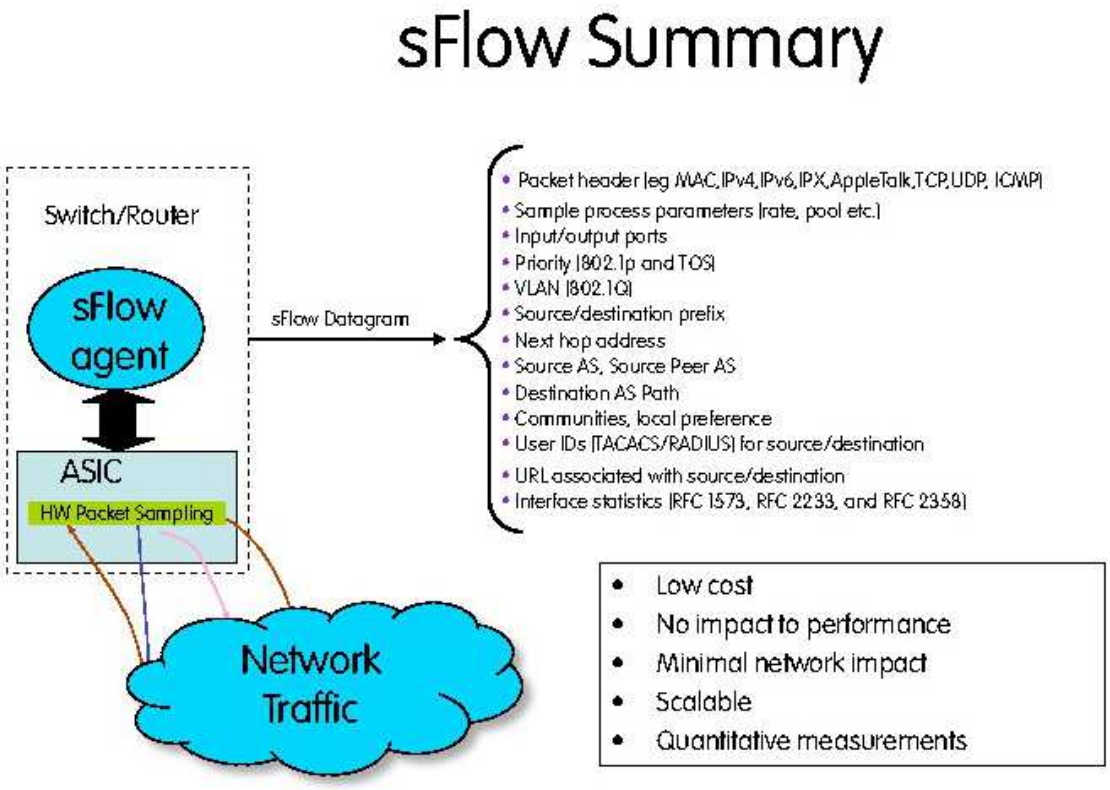


Figura 20: sFlow: sommario

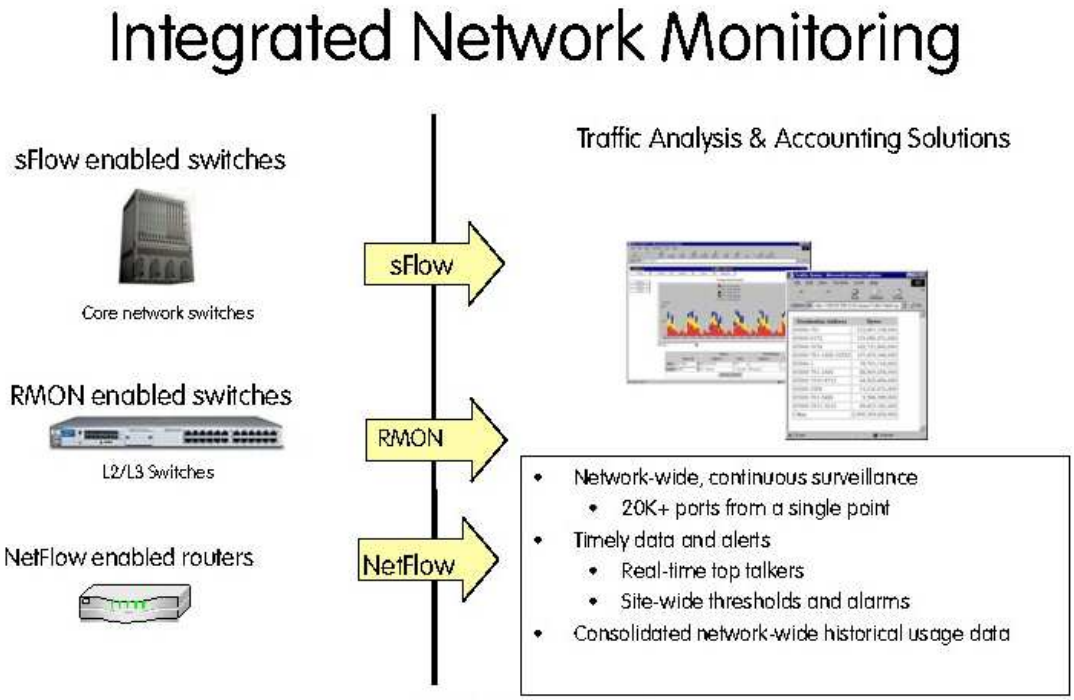


Figura 21: Monitoraggio di rete integrato

Rigney, C., Rubens, A., Simpson, W, and Willens, S.; Remote Authentication Dial In User Service (RADIUS), RFC 2138, January 1997.

- Gestione dei dati
  Rigney, C.; RADIUS Accounting, RFC 2139, January 1997.

6.2.1 RADIUS

RADIUS è importante perché:

- È il protocollo più usato per implementare l'autenticazione sui dispositivi di rete.
- Usato per la fatturazione sulle reti cablate (wired lines) (ad esempio ADSL, Modem).
- Abilita la gestione della durata della connessione o della quantità di dati.
- Supportato da tutti i dispositivi di rete (esclusi quelli di basso costo).

6.2.2 Protocollo: le primitive

La figura 22 mostra un esempio di come il client RADIUS (il server per i clienti che intendono utilizzare la rete) e il server RADIUS (il server che gestisce gli account dei clienti) si scambiano i messaggi al fine di autenticare un cliente. Se il server RADIUS risponde positivamente alla richiesta di accounting, allora il cliente è libero di utilizzare la rete, altrimenti il client RADIUS gli nega l'accesso.

Access Request (*client* → *server*):

- Richiesta per accedere al servizio di rete (ad esempio autenticazione dell'utente).
- Possibile risposta:
  - Access Accept (*server* → *client*).
  - Access Reject (*server* → *client*).
  - Access Challenge (*server* → *client*): usata per l'autenticazione CHAP.

Accounting Request (*client* → *server*):

- Richiesta di scrivere i dati dell'account sul server degli account.
- Risposte:
  - Accounting Response (*server* → *client*).

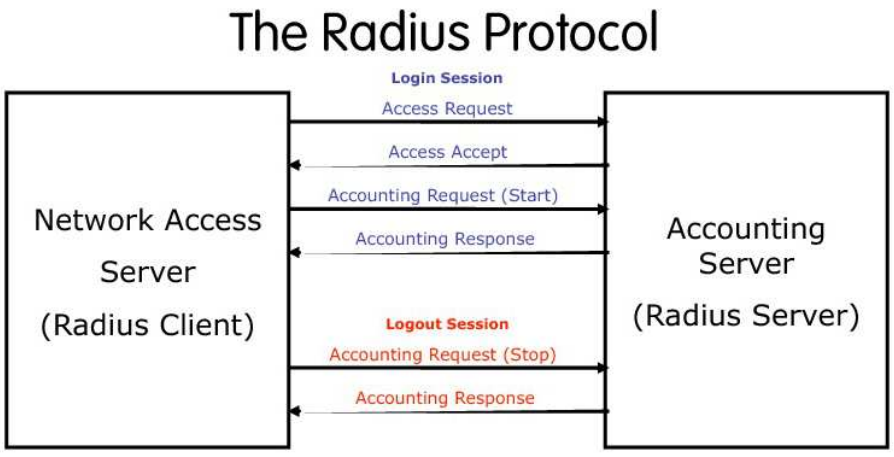


Figura 22: Il protocollo RADIUS

6.2.3 Protocollo: messaggi

La figura 23 mostra i messaggi scambiati dal protocollo RADIUS.

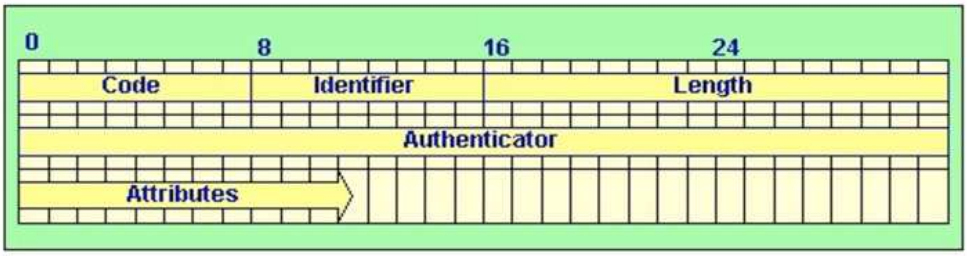


Figura 23: Messaggi del protocollo RADIUS

Code: Il byte che contengono il comando/risposta RADIUS.

Identifier: Il byte che identifica il comando/risposta RADIUS.

Length: Lunghezza del pacchetto.

Authenticator: Valore usato per la risposta del server all'autenticazione RADIUS.

Attributes: Attributi del comando/risposta.

6.3 Cattura dei pacchetti

6.3.1 libpcap

Usando la libreria libpcap si fa si che tutti i pacchetti che arrivano alla scheda di rete vengano copiati e inviati al driver BPF (si veda figura 24). Mentre il pacchetto originale segue il naturale percorso e quindi può anche essere scartato dalla scheda di rete se l'indirizzo MAC non corrisponde, il pacchetto copiato viene gestito dall'applicazione (quindi con l'ausilio della CPU).

6.3.2 libpcap: esempio d'uso

```
pcapPtr = pcap_open_live(deviceName,
     maxCaptureLen, setPromiscousMode,
     pktDelay, errorBuffer);
while(pcap_dispatch(pcapPtr, 1,
          processPacket, NULL) != -1);
void processPacket(u_char *_deviceId,
     const struct pcap_pkthdr *h,
     const u_char *p) {
     ...
}
```

```
int main(int argc, char* argv[]) {
  /* open a network interface */
descr = pcap_open_live(dev,BUFSIZ,0, 1,errbuf);
/* install a filter */
pcap_compile(descr,&fp,"dst port 80",0,netp);
pcap_setfilter(descr,&fp);
while (1) {
    /* Grab packets forever */
    packet = pcap_next(descr,&hdr);
    /* print its length */
    printf("Grabbed packet of length %d\n", hdr.len);
  }
}
```

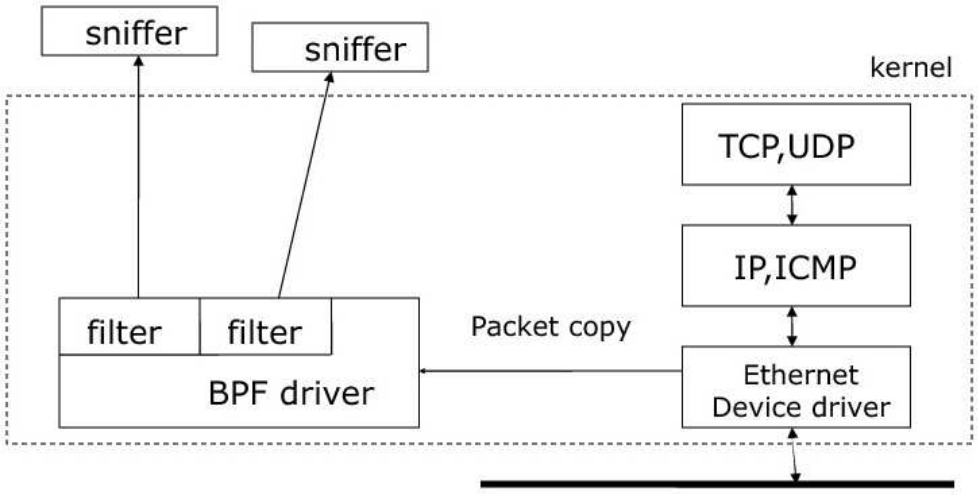


Figura 24: libpcap: cattura dei pacchetti

6.3.3 Problemi comuni con la cattura dei pacchetti

- Problemi di sicurezza:
  - Viene catturato tutto il traffico di rete e non solo quello destinato all'host che "sniffa".
  - Se c'è una rete switchata viene catturato solo una parte del traffico (ARP poisoning).
  - L'usabilità è limitata ha chi ha i privilegi di root
    Nota: questo succede anche con il comando ICMP (ad esempio ping) e perciò questo comando ha il setuid abilitato.
- Performance:
  - Lo sniffer implica anche carico di lavoro sulla CPU perché tutti i pacchetti catturati devono essere analizzati dal programma e non solo quelli diretti verso l'host.

6.3.4 Cattura dei pacchetti: soluzioni

- Usare una NIC (Network Interface Cart - scheda di rete) punta sulla NPU (Network Process Unit[29]). Ogni moderna NIC ha un limitato numero di NPU (multicast e ethernet). Se si possiede un driver che sfrutta al meglio la NPU allora si possono fare anche altre cose, oltre al filtraggio per MAC address.
- Usare una scheda programmabile (ad esempio Napatech, si veda figura 25).
- Eseguire il codice di gestione/amministrazione del traffico direttamente sulla NIC (ad esempio Inter IPX Family).
- Accesso ad alta velocità (via mmap()) per prendere i pacchetti direttamente dalla NIC via bus PCI (ad esempio Endage DAG Card, si veda figura 26).

6.4 Mirror del traffico: possibili soluzioni

Hardware:

- Hub (ethernet in rame, token ring).
- Divisione ottica (fibra ottica).
- Tap (Rame/fibra) (si veda figura 28)

[29] Una Network Process Unit (NPU) è un array di una o più CPU specializzate per gestire le funzioni di rete. Le NPU hanno l'obiettivo di esaminare e manipolare in maniera efficiente l'header dei pacchetti.

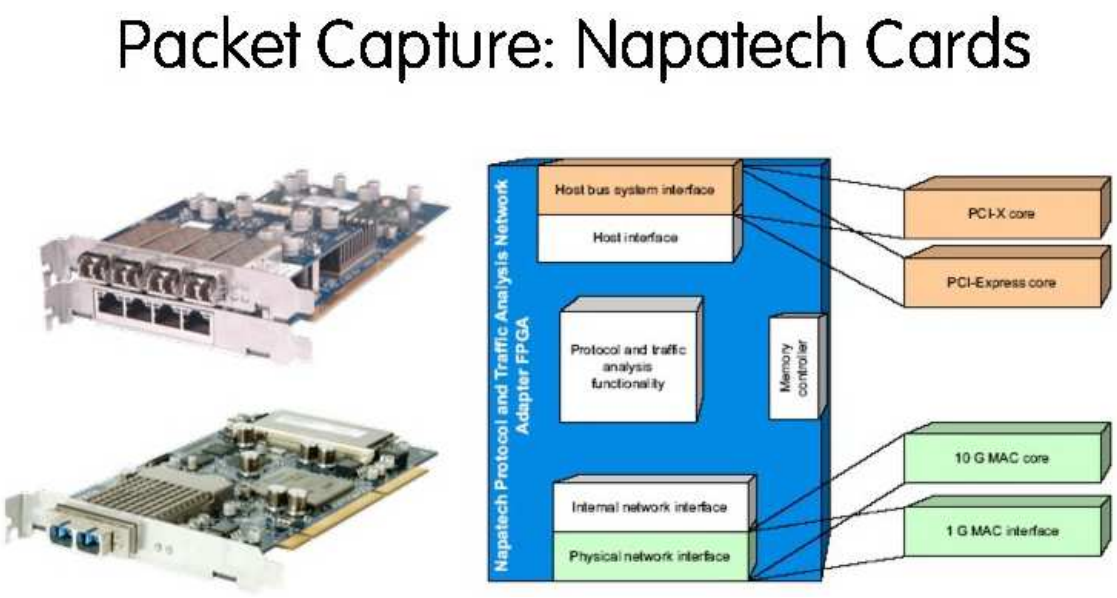


Figura 25: Cattura dei pacchetti: schede di rete Napatech

Figura 26: Cattura dei pacchetti: scheda di rete DAG

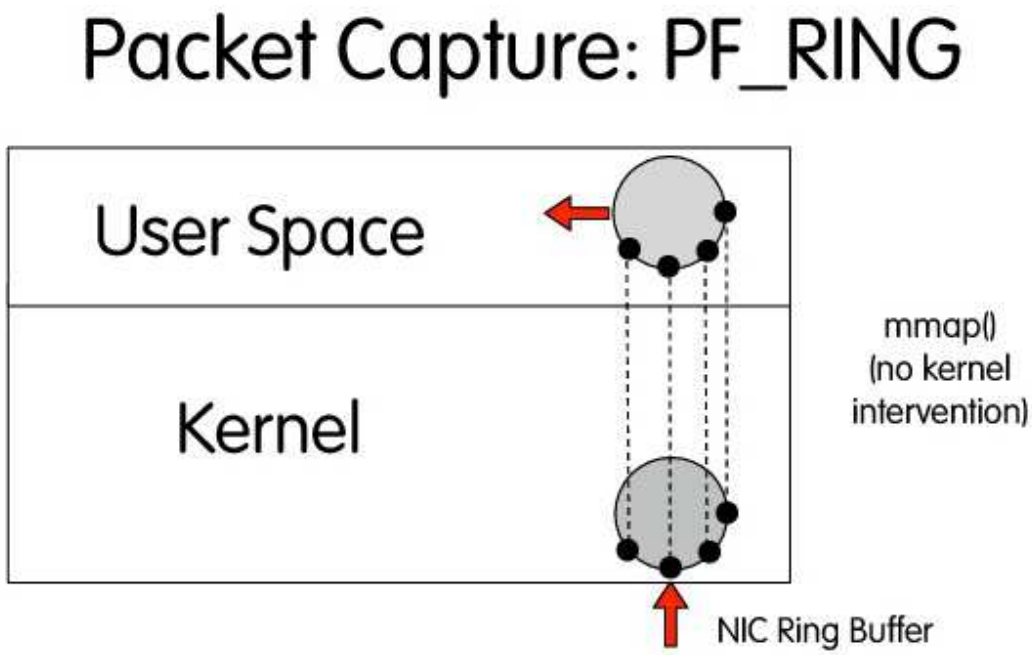


Figura 27: Cattura dei pacchetti: PF Ring in DNA (Direct NIC Access) mode

Software:

- Switch Port Mirror (1:1, 1:N).
- Switch VLAN Mirror (N:1).
- Switch Traffic Filter/Mirroring (Juniper).

6.5 Collezionare i dati: RRD

- RRD (http://www.rrdtool.org/)
  - Round Robin Database: strumento per scrivere e visualizzare i dati basato su MRTG (Multi Router Traffic Grapher).
  - I dati sono scritti in un formato "compresso" che non aumenta nel tempo (i dati vengono aggregati automaticamente) lasciando inalterata la dimensione del file.
  - Interfacce Perl/C per accedere ai dati e produrre i grafici.

6.5.1 Esempio in Perl

```
$rrd = "$dataDir/$agent-$ifIndex.rrd";
if(! -e $rrd) {
    RRDs::create ($rrd, "--start",$now-1, "--step",20,
      "DS:bytesIn:COUNTER:120:0:10000000",
      "DS:bytesOut:COUNTER:120:0:10000000",
      "RRA:AVERAGE:0.5:3:288");
    $ERROR = RRDs::error;
    die "$0: unable to create `$rrd': $ERROR\n" if $ERROR;
}
    RRDs::update $rrd, "$now:$ifInOctets:$ifOutOctets";
   if ($ERROR = RRDs::error) {
    die "$0: unable to update `$rrd': $ERROR\n";
}
```

Figura 28: Mirror del traffico: Tap

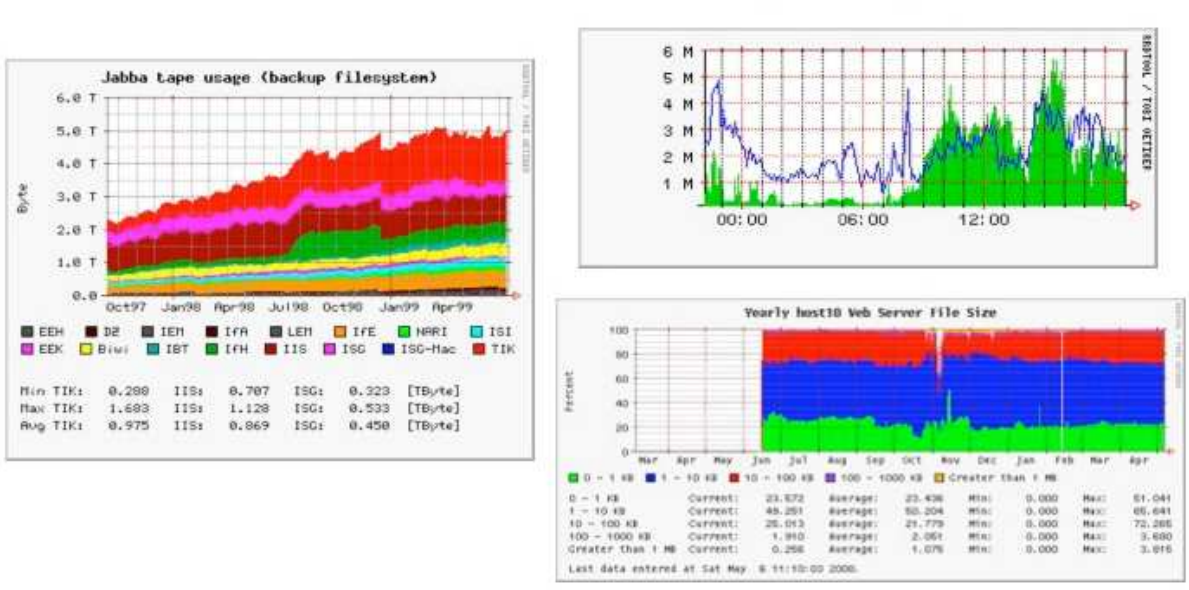


Figura 29: Collezionare i dati: RRD

7 Misurazione del traffico: qualche caso di studio

7.1 Caratterizzazione del percorso: patchar

Pathchar ftp://ftp.ee.lbl.gov/pathchar/

- Spedisce vari pacchetti (di differenti dimensioni) verso tutti i router, che devono essere analizzati, di un dato percorso.
- Misura il tempo di risposta più breve per ogni hop:
  - Ritardo dell'hop.
  - Larghezza di banda.
  - Coda
- Studia il RTT respetto alla dimensione del pacchetto, misura la disponibilità della larghezza di banda.
- Svantaggi: il test dura troppo. I calcoli sono complessi e necessitano l'invio di un gran numero di pacchetti per dare misurazioni precise.

Altri strumenti: pchar, pipechar.

7.2 Throughput della rete: Iperf

Iperf http://dast.nlanr.net/Projects/Iperf/

- Architettura client/server: qualche binario viene eseguito in due modi differenti.
- L'applicazione client spedisce al server pacchetti TCP/UDP. Può essere specificata la porta, la durata del test, la dimensione della finestra TCP, il volume dei dati del test.
- Statistiche: larghezza di banda, perdita/ritardo dei pacchetti, jitter.
- Svantaggi:
  - L'applicazione server deve essere installata sull'host di destinazione.
  - Non lo si può installare/usare sui router.

7.3 Di che tipo di report sul traffico abbiamo bisogno?

- La top N dei parlatori (chi trasmette molto traffico).
- La top N delle conversazioni (le coppie di host che si trasmettono molto traffico).
- La top N delle applicazioni (ad esempio SAP usa il 70% della larghezza di banda disponibile).
- Il volume dei dati per entità di base (link, locazione, regione, classe di utenti).
- Volume dei dati e velocità per AS (per sapere ad esempio se si ha bisogno di stipulare un nuovo contratto).
- Marca QoS per le applicazioni o per le entità di base (ad esempio, il BGP può dire se si sta spedendo il traffico sul percorso migliore?).
- Rapporti sul traffico che non ci si aspetta di vedere sulla rete (ad esempio perché l'host X sta spedendo un pacchetto IPX anche se si parla usando solamente IP?).

7.4 Monitoraggio integrato: Cacti

Cacti http://www.raxnet.net/products/cacti è uno strumento open source capace di:

- Collezionare i dati con l'ausilio di metodi SNMP e altri non-SNMP.
- La configurazione viene fatta via web e la scrittura su un database MySQL.
- Statistiche salvate in RRD.
- Estensibilità attraverso script e XML.

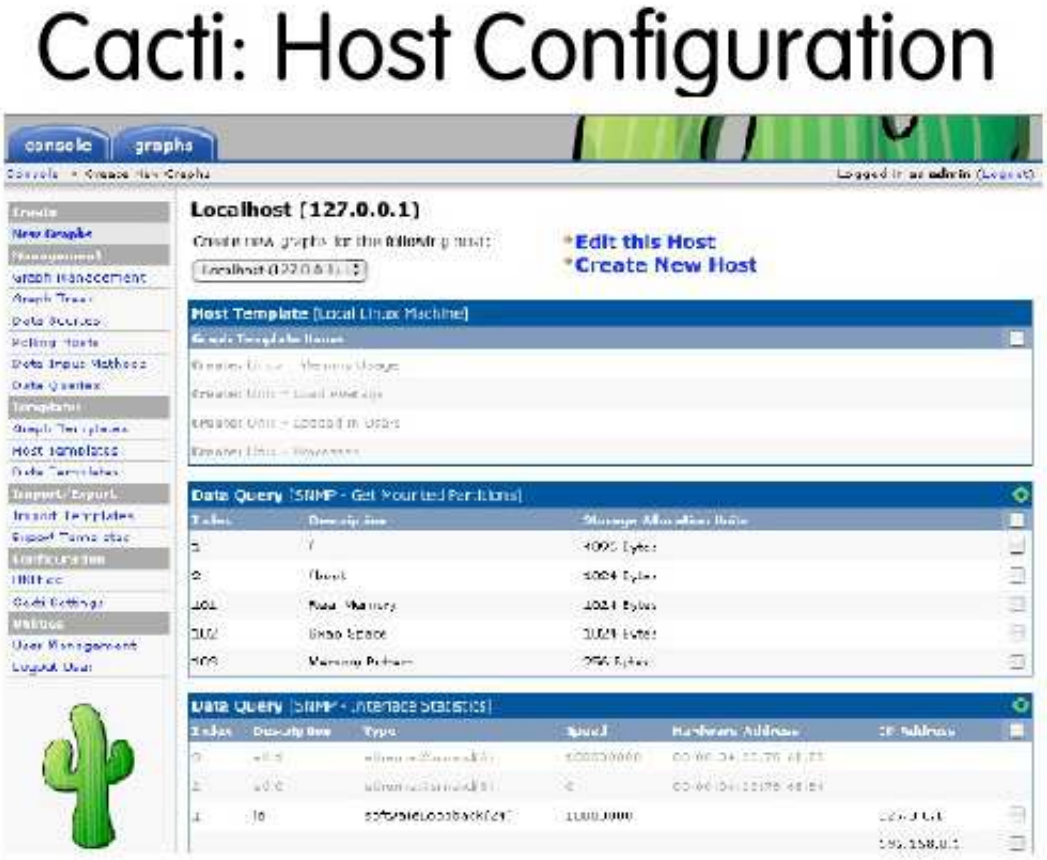


Figura 30: Cacti: configurazione

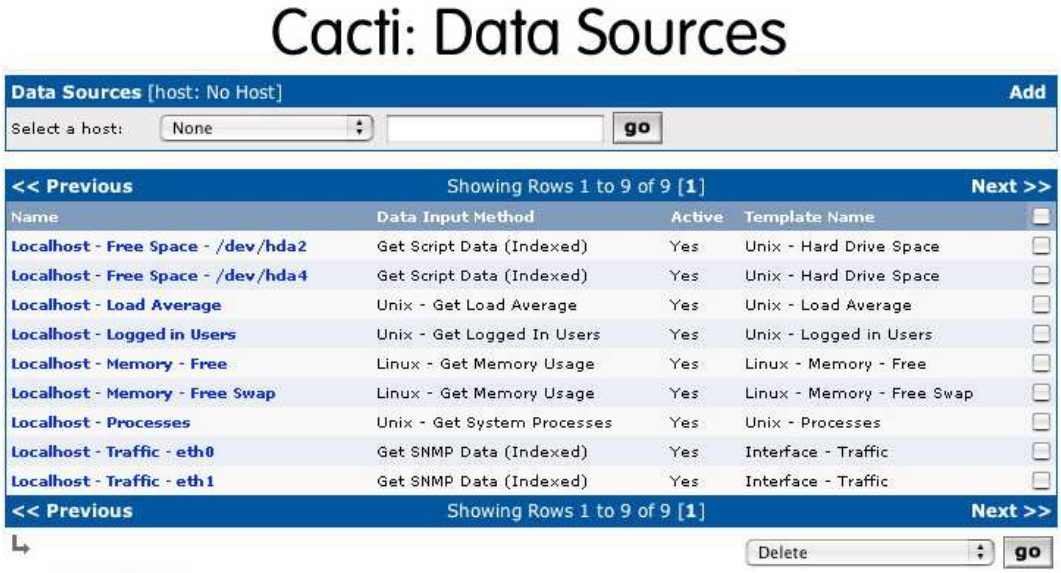


Figura 31: Cacti: dati

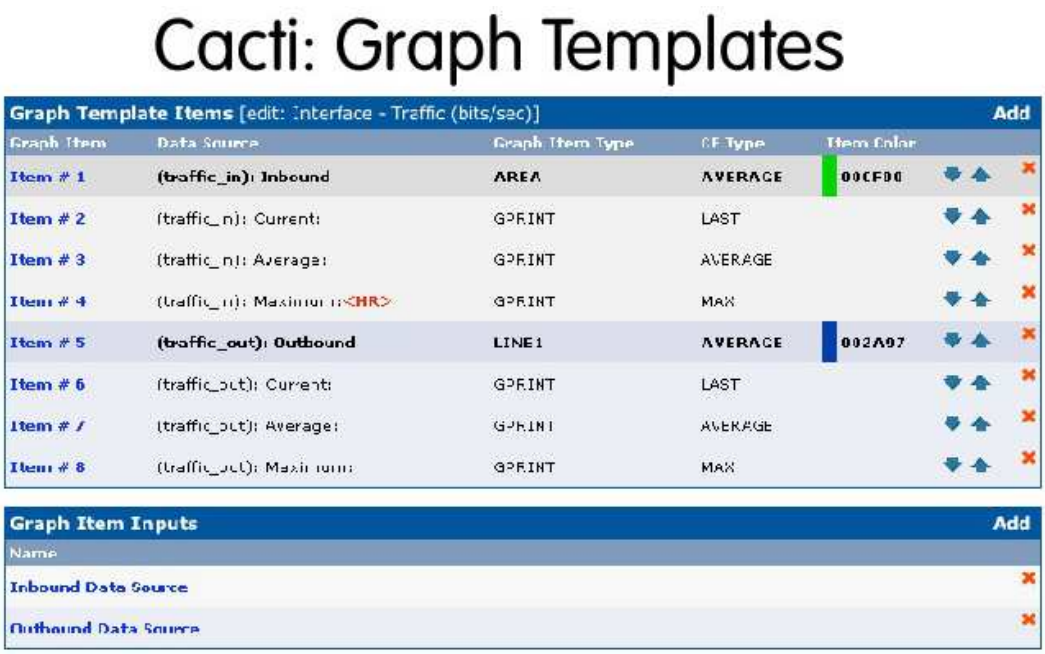


Figura 32: Cacti: grafico dei template

7.5 Caso di studio: gestione della larghezza di banda

- I problemi che non sono legati all'acquisto di nuova larghezza di banda ma alla gestione di quella attuale.
  - Lezione appresa: più larghezza di banda si ha, più verrà usata.

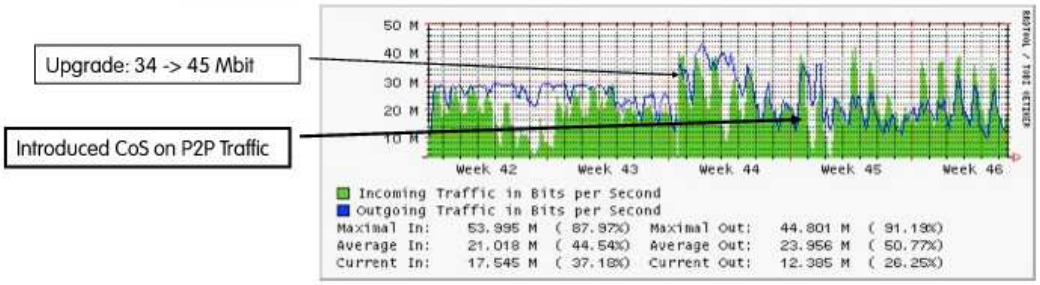


Figura 33: Gestione della larghezza di banda

- Soluzione: monitorare e trovare le risposte per le proprie esigenze (non ci sono soluzioni generali).
  - Analizzare quanta della larghezza di banda viene utilizzata (ad esempio, perché viene utilizzato il protocollo X?).
  - Traffico e matrice del flusso: chi parla con chi e quali dati si scambiano?
- Lezioni apprese dalla pratica:
  - Scarse performance possono essere causate dall'uso dei link di backup perché quelli primari non sono disponibili (si sta monitorando il failovers - attraverso le trap SNMP - come STP, stato delle porte?).
  - La rete va bene ma non è al massimo (suboptimal) o è molto dinamica? (SNMP fornisce molti MIB a questo scopo).
  - Si sta tagliando troppo la banda (shaping[30])? Le CoS (Class of Service) sono ottime, ma non se ne dovrebbe abusare (si dovrebbe invece monitorare la quantità di traffico tagliata dalle proprie politiche)!

[30] Lo shaping si effettua introducendo delle classi di servizio (CoS) per impedire che un tipo di traffico monopolizzi tutto.

7.6 Caso di studio: dov'è un host?

- Associazione tra indirizzo IP e nome:

```
deri@tar:~$ nslookup 131.114.21.22
   Server: localhost
   Address: 127.0.0.1
   Name: jake.unipi.it
   Address: 131.114.21.22
```

- Associazione tra host e proprietario
  - namenslookup-type=SOA.
  - WAIS (Wide Area Information System) http://www.ai.mit.edu/extra/the-net/wais.html.
  - WHOIS [RFC-812].

7.6.1 Esempio di whois

```
Domain:         unipi.it
Status:         ACTIVE
Created:        1996-01-29 00:00:00
Last Update:    2008-02-14 00:02:47
Expire Date:    2009-01-29

Registrant
  Name:         Universita' degli Studi di Pisa
  ContactID:    UNIV302-ITNIC
  Address:      Centro SERRA
                Pisa
                56100
                PI
                IT
  Created:      2007-03-01 10:42:01
  Last Update:  2008-01-19 09:46:08

Registrar
  Organization: Consortium GARR
  Name:         GARR-MNT
```

7.7 Dov'è l'host X nel mondo?

- RFC 1876: un mezzo per Expressing Location Information nel Domain Name System,
- http://www.caida.org/tools/utilities/netgeo/
- http://www.maxmind.com/
- http://www.geobytes.com/

7.8 Caso di studio: impronta digitale degli OS (Operating System - sistema operativo)

- Attivo:
  Spedire pacchetti di prova per capire il sistema operativo dell'host (http://nmap.org/).
- Passivo:
  Guardare la stretta di mano a 3 vie (handshake) del TCP e confrontarla con un database di firme conosciute in modo da capire il sistema operativo dell'host (http://ettercap.sf.net/).

7.8.1 Ettercap

```
WWWW:MSS:TTL:WS:S:N:D:T:F:LEN:OS

WWWW: 4 digit hex field indicating the TCP Window Size
MSS : 4 digit hex field indicating the TCP Option Maximum Segment Size
      if omitted in the packet or unknown it is "_MSS"
TTL : 2 digit hex field indicating the IP Time To Live
```

```
WS  : 2 digit hex field indicating the TCP Option Window Scale
      if omitted in the packet or unknown it is "WS"
S   : 1 digit field indicating if the TCP Option SACK permitted is true
N   : 1 digit field indicating if the TCP Options contain a NOP
D   : 1 digit field indicating if the IP Don't Fragment flag is set
T   : 1 digit field indicating if the TCP Timestamp is present
F   : 1 digit ascii field indicating the flag of the packet
      S = SYN
      A = SYN + ACK
```

7.9 Caso di studio: scanner per la sicurezza

- Nessus http://www.nessus.org/.
- Saint http://www.saintcorporation.com/.

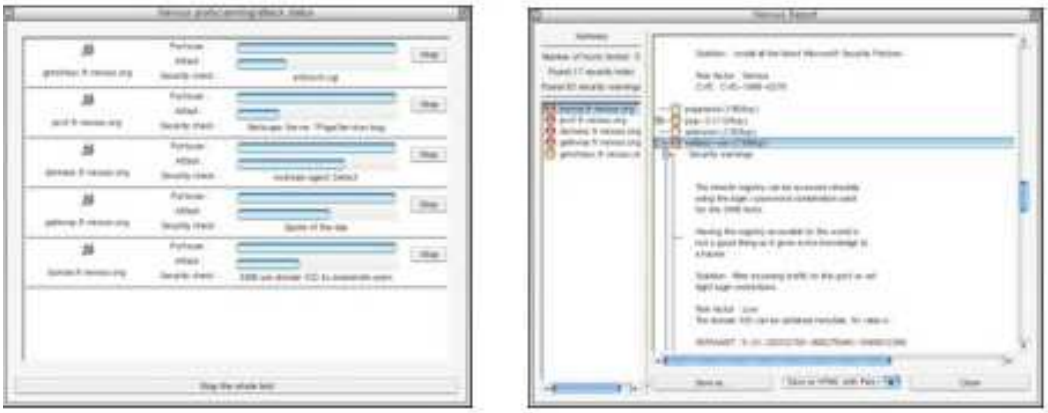


Figura 34: Scanner per la sicurezza

7.10 Caso di studio: sicurezza di rete

La sicurezza è un processo, non un prodotto (Standard BS 7799, B. Schneier).

- Si è capaci di determinare le anomalie del traffico?
- Si è sicuri di sapere cosa monitorare? Molti problemi sono prodotti dal traffico che non ci si aspetta di vedere sulla rete: monitorare ogni cosa, filtrare solo quello che dovrebbe passare, vedere il resto e spiegarsi cos'è successo.
- Si possiede un meccanismo automatico per recuperare i fallimenti? Si supponga di aver individuato un problema (ad esempio attraverso le trap SNMP) il sistema è capace di reagire in maniera automatica o si deve aspettare il rientro dell'amministratore dalle vacanze?

7.11 Caso di studio: individuazione del traffico P2P

- Il P2P è difficile da individuare con i metodo classici:
  - Non lo si può individuare attraverso l'uso di impronte digitali (ad esempio con l'associazione porta-protocollo).
- Comunque:
  - Lo si può individuare in termini di modifica di un comportamento standard (ad esempio una workstation non può aprire più di X connessioni al minuto, e non può nemmeno avere più di Y connessioni aperte).
  - Analizzare una parte iniziale del payload per individuare il protocollo.
  - Alta percentuale di connessione TCP fallite.

  - Il rapporto pacchetti/byte e sopra la media (le sorgenti P2P spediscono molti pacchetti, per lo più per parlare con i peer).
  - Identificare l'esistenza di comunicazione client-a-client (porte > alla 1024) anche se non si hanno canali di comunicazione FTP aperti.

7.12 Caso di studio: individuazione dello SPAM

- Reti grandi e aperte (come Università o ISP) sono il posto migliore dove inviare SPAM (email non richieste).
- Come identificare la sorgente di SPAM:
  - Problema simile all'individuazione del traffico P2P ma più semplice (solo SMTP, 1 connessione = 1 email).
  - Selezionare l'insieme dei top N mittenti SMTP.
  - Rimuovere dall'insieme tutti i server SMTP conosciuti.
  - Gli studi mostrano che in media gli host non inviano più di 8-10 email al minuto.
  - Un problema veramente semplice da affrontare usando dei protocolli basati sui flusso, come ad esempio NetFlow.

7.13 Caso di studio: individuazione dei virus/trojan

- Problema simile all'individuazione dello SPAM ma più complesso dato che i protocolli e le porte usate non sono fisse.
- Gli attacchi non hanno obiettivi mirati: in qualche modo si comportano come scanner di rete.
- Individuazione:
  - Se il problema è conosciuto (ad esempio il traffico sulla porta UDP 135) ci si focalizza su questi traffici.
  - Buttare un occhio ai messaggi ICMP (ad esempio porta o destinazione non raggiungibile) sono il modo migliore per individuare gli scanner di rete.

8 Commenti finali

8.1 Quindi, cosa bisogna aspettarsi dal monitoraggio di rete?

- Capacità di individuare in maniera automatica quei problemi che sono costantemente sotto monitoraggio (ad esempio, non c'è traffico su di un link della backbone: la rete è caduta?).
- Ricevere allarmi a proposito di potenziali (ad esempio l'utilizzo della CPU è troppo alto) e reali (ad esempio li disco è pieno) problemi.
- Notifica e ripristino automatico di problemi noti con note soluzioni (ad esempio, se il link dell'email non va viene usato un link di backup).
- Notificare all'uomo tutti quei problemi che necessitano attenzione e che non possono essere ripristinati (ad esempio l'host X non è raggiungibile).

8.2 Avvertenze sul monitoraggio

- Se un'applicazione necessita di assistenza umana per quei problemi che possono essere risolti in maniera automatica, allora l'uso di questa applicazione non è completamente vantaggioso.
- Gli allarmi (sicurezza al 100% che c'è qualcosa che non va) sono diversi dagli avvisi (potrebbe esserci qualche problema): non si pretenda di essere precisi/catastrofici se non è il caso.
- Gli allarmi sono inutili se non c'è nessuno che li controlla.
- Troppi (falsi) allarmi equivale a non avere allarmi: gli umani tendono ad ignorare i fatti quando qualcuno di essi è falso.

Glossario

A

ARP (Address Resolution Protocol)
Per inviare un pacchetto IP ad un host della stessa sottorete, è necessario incapsularlo in un pacchetto di livello datalink, che dovrà avere come indirizzo destinazione il MAC address dell'host a cui lo si vuole inviare. ARP viene utilizzato per ottenere questo indirizzo.

L'host che vuole conoscere il MAC address di un altro host, di cui conosce l'indirizzo IP, invia in broadcast una richiesta ARP (ARP-request) contenente il proprio MAC address e l'indirizzo IP dell'host di cui vuole conoscere il MAC address. Se nella sottorete esiste un host che ha proprio l'indirizzo IP settato nell'ARP-request, allora provvederà ad inviare una risposta (ARP-reply) al MAC address del richiedente, contenente il proprio MAC address. 13, 16

ARP poisoning
Detto anche ARP spoofing, è una tecnica di hacking che consente ad un attacker, in una switched lan, di concretizzare un attacco di tipo man in the middle verso tutte le macchine che si trovano nello stesso segmento di rete. L'ARP poisoning è oggi la principale tecnica di attacco alle lan commutate. Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati inesatti o, meglio, non corrispondenti a quelli reali. In questo modo la tabella ARP (ARP entry cache) di un host conterrà dati alterati (da qui i termini poisoning, letteralmente avvelenamento e spoofing, raggiro). Molto spesso lo scopo di questo tipo di attacco è quello di redirigere, in una rete commutata, i pacchetti destinati ad un host verso un altro al fine di leggere il contenuto di questi per catturare le password che in alcuni protocolli viaggiano in chiaro. 13, 44

AS (Automous System)
In riferimento ai protocolli di routing, è un gruppo di router e reti sotto il controllo di una singola e ben definita autorità amministrativa. Un'autorità amministrativa si contraddistingue sia in base a elementi informatici (specifiche policy di routing), sia per motivi amministrativi. Esempio di sistema autonomo può essere quello che contraddistingue gli utenti di un unico provider oppure, più in piccolo, quello che costituisce la rete interna di un'azienda.

All'interno di un sistema autonomo i singoli router comunicano tra loro, per scambiarsi informazioni relative alla creazione delle tabella di routing, attraverso un protocollo IGP. L'interscambio di informazioni tra router appartenenti a sistemi autonomi differenti avviene attraverso un protocollo BGP. 3, 12, 25, 27, 48

ASN (Automous System Number)
Ad ogni AS viene assegnato un ASN in modo da essere usato per il routing BGP. Gli ASN sono importanti perché ognuno di essi identifica una specifica rete di internet. 24

ATM (Asynchronous Transfer Mode)
Modalità di trasporto asincrona che trasferisce il traffico multiplo (come voce, video o dati) in cellule di lunghezza fissa di 53 byte (piuttosto che in pacchetti di lunghezza variabile come accade nelle tecnologie Ethernet e FDDI). La modalità ATM permette di raggiungere velocità elevate e diventa particolarmente diffusa nelle dorsali di rete a traffico intenso. Le apparecchiature di rete di nuova generazione permettono di supportare le trasmissioni WAN anche in ATM, rendendola interessante anche per grandi organizzazioni geograficamente distribuite. 6

B

BGP (Border Gateway Protocol)
È un protocollo di rete usato per connettere tra loro più router che appartengono a AS distinti e che vengono chiamati router gateway. È quindi un protocollo di routing inter-AS, nonostante possa essere utilizzato anche tra router appartenenti allo stesso AS (nel qual caso è indicato con il nome di iBGP, Interior Border Gateway Protocol), o tra router connessi tramite un ulteriore AS che li separa. 3, 48

Broadcast
Nelle reti di calcolatori, un pacchetto inviato ad un indirizzo di tipo broadcast verrà consegnato a tutti i computer collegati alla rete (ad esempio, tutti quelli su un segmento di rete ethernet, o tutti quelli di una sottorete IP). Si veda anche Multicast e Unicast. 5–7, 11, 19, 20, 27

C

CLI (Command Line Interface)
È la modalità di interazione tra utente ed elaboratore che avviene inviando comandi tramite tastiera e ricevendo risposte alle elaborazioni tramite testo scritto. Questo tipo di approccio deriva dalla modalità di interazione con i primi calcolatori che avveniva attraverso terminali testuali non in grado di compiere alcuna elaborazione e connessi ad un elaboratore centrale. 14, 15, 21

D

DHCP (Dynamic Host Configuration Protocol)
È un protocollo che permette agli amministratori di rete di gestire centralmente ed in modo automatico l'assegnamento dell'indirizzo IP di ogni dispositivo connesso ad una rete (che deve risultare unico). 4

DoS (Denial of Service)
Tradotto come "negazione del servizio", è un tipo di attacco internet in cui si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio. 24, 36

I

ISP (Internet Service Provider)
Società che gestisce gli accessi ad Internet. Collegando il proprio computer (via modem o router) al server dell'ISP, si entra in Internet. Gli ISP offrono spesso altri servizi aggiuntivi, come la posta elettronica, l'hosting e l'housing, soluzioni di E-commerce e di supporto ai propri clienti. 3, 8, 53

L

LAN (Local Area Network)
Rete o gruppo di segmenti di rete confinati in un edificio o un campus, che collega computer e periferiche (es. stampanti, fax, scanner) installate nella stessa sede (es. stesso palazzo, anche a piani diversi) oppure in sedi vicine (es. due palazzi adiacenti). Le LAN operano di solito ad alta velocità, per esempio Ethernet ha una velocità di trasferimento dati di 10 Mbps o di 100 Mbps nel caso della Fast Ethernet. Si veda anche WAN. 6, 18

M

Multicast
Nelle reti di calcolatori, un pacchetto inviato ad un gruppo multicast verrà consegnato a tutti i computer appartenenti a quel gruppo. Si veda anche Broadcast e Unicast. 3, 5, 6, 11, 19, 20, 28, 44

P

P2P (Peer-to-peer)
Rete paritaria: una rete di computer o qualsiasi rete informatica che non possiede nodi gerarchizzati come client o server fissi (clienti e serventi), ma un numero di nodi equivalenti (in inglese peer) che fungono sia da cliente che da servente verso altri nodi della rete.

Questo modello di rete è l'antitesi dell'architettura client-server. Mediante questa configurazione qualsiasi nodo è in grado di avviare o completare una transazione. I nodi equivalenti possono differire nella configurazione locale, nella velocità di elaborazione, nella ampiezza di banda e nella quantità di dati memorizzati. L'esempio classico di P2P è la rete per la condivisione di file (File sharing). 3, 4, 16, 52, 53

Q

QoS (Quality of Service)
Meccanismo di controllo delle risorse limitate. QoS è capace di fornire differenti priorità a differenti applicazioni, utenti o flussi di dati, oppure di garantire un certo livello di performance ad un flusso di dati. Ad esempio potrebbero essere garantiti una determinata velocità di bit, un determinato ritardo, una certa probabilità di scarto di pacchetti. Le garanzie di QoS sono importanti soprattutto se la capacità della rete insufficiente, specialmente per le applicazioni multimediali a tempo reale in streaming, applicazioni come ad esempio giochi online o televisione via IP (IP-TV), infatti questo tipo di applicazioni sono sensibili al ritardo e spesso necessitano di una velocità fissa di bit. 22, 48

R

RTT (Round Trip Time)
Detto Round Trip Delay, è il tempo impiegato da un pacchetto di dimensione trascurabile per viaggiare da un host della rete ad un altro e tornare indietro (tipicamente, un'andata client-server ed il ritorno server-client). 9, 48

S

SLA (Service Level Agreement)
Strumenti contrattuali attraverso i quali si definiscono le metriche di servizio che devono essere rispettate da un fornitore di servizi. In un mercato competitivo che opera quindi in regime di libera concorrenza, gli SLA sono diventati uno strumento comune per misurare efficacemente i servizi. In questo contesto la definizione di uno SLA consiste in un contratto tangibile tra due parti che, se da un lato assicura la fornitura dei servizi a livelli pre-negoziati, dall'altro comporta il pagamento di penalità in caso di mancato raggiungimento di tali livelli.

La definizione dello SLA è basata sulla determinazione da parte del cliente del livello di servizio ideale a garanzia del suo business. 3

T

ToS (Type of Service)
È un campo (un byte) dell'header IPv4 usato in vari modi e specificato in modi diversi da 5 RFC, (RFC 791, RFC 1122, RFC 1349, RFC 2474, e RFC 3168).

L'intenzione originaria del ToS era quella di permettere ad un host di specificare come un datagram doveva essere gestito quando attraversava la rete. Ad esempio, un host avrebbe potuto settare il ToS per indicare un basso ritardo, laddove un altro host lo avrebbe potuto settare per indicare la sua preferenza verso una maggiore affidabilità. In pratica però l'uso del ToS non è stato largamente impiegato. La sua moderna definizione lo vede diviso in 6 bit denominati Differentiated Service Code Point (DSCP) e 2 bit denominati Explicit Congestion Notification. 27

U

Unicast
Nelle reti di calcolatori, un pacchetto unicast è un pacchetto inviato ad un solo computer. Si veda anche Broadcast e Multicast. 28

W

WAN (Wide Area Network)
Rete a larga area o a lunga tratta, che si può estendere per una lunghezza massima di 100km. Si tratta di una rete di comunicazione dati, che impiega linee telefoniche dedicate o satelliti. Si veda anche LAN. 12, 18