UNIVERSITÀ DEGLI STUDI DI PISA
FACOLTÀ DI SCIENZE MATEMATICHE FISICHE E NATURALI
CORSO DI LAUREA TRIENNALE IN INFORMATICA

MONITORAGGIO DI RETI AD ALTA VELOCITÀ

Candidati:

Andrea Manzi Marco Pasquali

Tutore Aziendale
Prof. Luca Deri

Tutore Accademico
Prof. Marco Vanneschi

Anno Accademico 2001/2002

Ai nostri genitori,
ai nostri nonni.

SOMMARIO

1. Introduzione 8

1.1 Contesto Tecnologico 8
1.1.1 Tecniche di Trasmissione 8
1.1.2 Monitoraggio di Rete 9

1.2 Introduzione al Problema 10

1.3 Struttura del Documento 11

2. Stato dell'Arte 12

2.1 Misurazione del Traffico di Rete 12
2.1.1 Paradigmi di Monitoraggio 12
2.1.2 Attori ed Apparati per la Misurazione del Traffico 13
End-System 13
Apparati di Rete Standard 13
Measurement Gears 13
2.1.3 Tipi di Misurazioni 14
Analisi Per-Link / End-to-End / Aggregazione di Flussi 14
2.1.4 Modalità di Accesso ai Dati di Monitoraggio 15
SNMP 15
RMON 16

2.2 Monitoraggio Attivo 18
2.2.1 Tipi di Misurazione 18
2.2.2 Tool 20
Ping 20
Traceroute 21
Pathchar 21
IPerf 22
Mtrace 22
2.2.3 Progetti per il Monitoraggio del Traffico Internet 22
AMP 22
RIPE TTM 24
Surveyor 26
2.2.4 Considerazioni 27

2.3 Monitoraggio Passivo 29
2.3.1 Tipi di Misurazioni 31
2.3.2 Tool 32
2.3.2.1 Software 32
2.3.2.1.1 Analisi dei Flussi 32
SFlow 33
NeTraMet 35
NetFlow 37

CFlowd 38
FlowScan 39
2.3.2.1.2 Cattura dei Pacchetti..... 40
TCPDUMP 41
ETHEREAL 42
LIBPCAP 42
CoralReef 43
2.3.2.1.3 Sonde Generiche..... 45
Ntop 45
2.3.2.1.4 IDS (Intrusion Detection System)..... 46
Snort 47
2.3.2.2 Hardware..... 48
2.3.2.2.1 NIC con NPU..... 48
DAG Card 4.0 48
RADYSIS ENP-2505/ENP-2506 49
2.3.2.2.2 Apparati di Rete..... 50
TRAFFIC SPLITTER..... 50
PARTIAL PORT MIRROR..... 50
TOP LAYER IDS Balancer 51
JUNIPER M-Series 51

3. Misurazioni su Reti ad Alta Velocità..... 53

3.1 Descrizione del Problema..... 53

3.2 Requisiti di Monitoraggio Esistenti..... 55
Analisi delle Caratteristiche dei Flussi..... 56
Ingegnerizzazione della Rete..... 56
Sicurezza..... 56
Accounting..... 57
Rilevazione di Errori..... 57

3.3 Nuovi Requisiti di Monitoraggio di Rete 58

3.4 Strumenti Adeguati al Problema 60
3.4.1 Hardware..... 60
JUNIPER 61
3.4.2 Software..... 63
NetFlow..... 63
sFlow..... 64
NTOP..... 68
SNORT..... 70

3.5 Strumenti Inadeguati al Problema..... 71
3.5.1 Hardware..... 71
3.5.2 Software..... 72
TcpDump/CoralReef/Ethereal..... 72
RTFM..... 72

3.6 Considerazioni..... 73

4. Un'Architettura per il Monitoraggio di Rete..... 75

4.1 Considerazioni iniziali 76

4.2 Progettazione..... 77
4.2.1 Juniper..... 78
4.2.2 Console di Analisi 82
4.2.3 Rete di Management 84

4.3 Campi di applicazione..... 85
4.3.1 Gestione dei Fault..... 86
4.3.2 Gestione dell'Accounting..... 87
4.3.3 Gestione della Sicurezza..... 88

5. Sperimentazione..... 89
NTOP..... 92
SNORT..... 92
NetFlow..... 93

6. Conclusioni..... 94

APPENDICE A 96

7. Bibliografia..... 97

1. Introduzione

Questa tesi si inserisce nel progetto, cofinanziato dalla comunità europea, denominato Scampi (A Scaleable Monitoring Platform for the Internet), che vede tra le società partecipanti l'azienda NETikos S.p.A. di Pisa, luogo del nostro tirocinio aziendale.
Lo scopo del progetto Scampi è quello di definire un'architettura per il monitoraggio di reti ad alta velocità. La nostra tesi descrive il contesto tecnologico delle reti attuali, la definizione del problema da affrontare (vedi sez 1.1 – 1.3), la valutazione dei sistemi di monitoraggio esistenti e le linee guida del progetto. Per gli specifici argomenti trattati il lettore deve essere in possesso delle conoscenze generali riguardanti le reti per la trasmissione dati.

1.1 Contesto Tecnologico

Negli ultimi anni le reti dati hanno avuto un notevole sviluppo ed anche il numero di utenti, sia i privati che le aziende, è aumentato progressivamente. Questo sviluppo è dovuto soprattutto al fatto che le reti sono entrate nella vita degli utenti rendendole indispensabili allo svolgimento del loro lavoro quotidiano, ed accrescendo il bisogno di servizi sempre più efficienti ed affidabili.
Tutto ciò ha stimolato le aziende e le istituzioni accademiche alla ricerca di nuove tecnologie che potessero aumentare la velocità di trasmissione dei dati.

1.1.1 Tecniche di Trasmissione

Le ricerche nel settore delle telecomunicazioni hanno portato alla definizione di reti a commutazione di pacchetto su cui si basa la trasmissione dati odierna. I dati sono suddivisi in unità trasmissibili (pacchetti) che vengono instradate dinamicamente dai dispositivi (router) presenti nella rete. Con l'avvento di internet è stato sviluppato l'*Internet Protocol* [11] (IP), protocollo utilizzato per la trasmissione dati che sfrutta il meccanismo della commutazione di pacchetto[1].

[1] Per maggiori delucidazioni si rimanda al testo in bibliografia.

Allo stato attuale della tecnologia, l'IP viene supportato da vari protocolli dello strato dei link[2] che consentono di raggiungere velocità elevate, tra i quali:

- ETHERNET [11]. Usato soprattutto nelle reti locali, è una fra le tecnologie più economiche; consente velocità che vanno da 10 Mbit/s fino a 10 Gbit/s.
- ATM [11] (Asyncronous-Transfer-Mode). La sua caratteristica principale è il canale virtuale (VC, *virtual channel*), definito come percorso che unisce i vari link (collegamenti). Dal VC passano tutti i dati, e la velocità di trasmissione si aggira attorno al Gbit/s.
- PoS [12] (Packet-over-Sonet). Questo protocollo incapsula i pacchetti IP in Frame Sonet (Standard per la trasmissione dati su fibra ottica) e permette di raggiungere velocità da 155 Mbit/s a 10 Gbit/s.

1.1.2 Monitoraggio di Rete

Parallelamente all'evoluzione tecnologica delle tecniche di trasmissione dati, è stato necessario definire strumenti per il monitoraggio che consentono di controllare l'utilizzo delle reti e, attraverso i dati acquisiti, garantirne l'efficienza richiesta.
Il monitoraggio di rete consiste nella rilevazione di misurazioni che consentono di descrivere il comportamento della rete nel tempo.
Gli strumenti necessari ad eseguire il monitoraggio vengono suddivisi in cinque aree funzionali [6] (FCAPS dalle iniziali dei nomi inglesi) standardizzate dall'International Standard Organization (ISO):

1. Gestione dei malfunzionamenti (fault);
   rilevazione e correzione dei malfunzionamenti di rete.
2. Gestione della configurazione;
   produzione e amministrazione dei dati di configurazione degli apparati di rete a seconda dell'evoluzione della stessa.
3. Gestione dell'accounting;
   distribuzione ottimale delle risorse fra gli utenti e ripartizione dei costi a seconda dell'utilizzo della rete.
4. Gestione della performance;
   rilevazione delle prestazioni della rete eseguita per migliorarne l'efficienza.

[2] Livello dello stack della rete che permette l'invio dei dati su un singolo collegamento del percorso da sorgente a destinazione.

5. Gestione della sicurezza;
   protezione della rete da attacchi e accessi non autorizzati, applicazione delle politiche per la sicurezza.

Inoltre esistono tre figure che si interessano al monitoraggio con esigenze diverse tra loro:

1. *Amministratore di Rete:* richiede un monitoraggio della performance applicativa per il corretto ed efficiente funzionamento delle applicazioni di rete, la verifica del livello di servizio rispetto all'infrastruttura di rete disponibile e la verifica di malfunzionamenti (*fault*) dovuti ad attacchi e virus.
2. *Internet Service provider* (ISP), ovvero coloro che forniscono il servizio, che hanno bisogno di informazioni riguardo le attività ed il traffico di rete, la corretta applicazione degli SLA pattuiti (Service Level Agreement), la rilevazione di errori e problemi di rete, la ricerca di soluzioni di tipo ingegneristico per fornire una migliore performance.
3. *Utenti Finali:* a cui interessa, avendo scarsa conoscenza tecnica, solo il corretto funzionamento di applicazioni di semplice utilizzo (Web Browser, Posta Elettronica).

Quindi, in base all'utente, si è reso necessario sviluppare strumenti di monitoraggio per soddisfare le esigenze diverse (vedi Cap. 2 Sez. 2.1.2).

1.2 Introduzione al Problema

A causa dell'elevata velocità le moderne reti non possono essere monitorate utilizzando, senza modifiche, i tool sviluppati per le reti dell'attuale generazione. Questo perché:

1. non tutte le tecniche di monitoraggio esistenti possono essere applicate efficientemente alle reti veloci (vedi Cap. 3);
2. a causa delle limitazioni hardware dei computer attuali, non è possibile senza opportune e sostanziali modifiche, utilizzare comuni calcolatori come misuratori di rete in quanto non riescono ad essere abbastanza veloci nell'analizzare accuratamente il traffico (vedi Cap. 3 Sez. 3.1);
3. recentemente la comunità tecnologica ha avuto sempre più interesse nell'effettuare misurazioni nuove (es. violazioni della sicurezza etc.) che non erano state prese in considerazione in precedenza (vedi Cap. 3 Sez. 3.2).

I motivi sopra elencati hanno spinto gli autori ad analizzare il problema del monitoraggio di reti ad alta velocità ed a indicare i requisiti e gli strumenti che possano soddisfare le esigenze di queste reti.

Di seguito vengono riportati gli obiettivi ed i contributi originali di questa tesi:

- Analisi degli strumenti di monitoraggio esistenti;
- Definizione dei requisiti per il monitoraggio di reti ad alta velocità;
- Definizione di un'architettura adatta al supporto di sistemi di monitoraggio per reti con velocità pari a 10Gbit/s, che soddisfi i requisiti identificati e che sfrutti, con opportuni adattamenti, gli strumenti di monitoraggio esistenti.

1.3 Struttura del Documento

Il documento si sviluppa in tre capitoli:

1. Panoramica dei sistemi di monitoraggio di rete esistenti, loro classificazione ed impiego (vedi Cap. 2).
2. Verifica dell'adeguatezza dei sistemi studiati alle nuove tecnologie e alle velocità di rete (vedi Cap. 3).
3. Studio delle modifiche da apportare ai sistemi per soddisfare gli obiettivi (vedi Cap. 4).

Nel secondo capitolo oltre alla descrizione ed alla classificazione dei vari strumenti, sono definite le possibili misurazioni effettuabili con ogni sistema e i protocolli di management utilizzati.
L'orientamento che gli autori hanno seguito nella scelta degli strumenti analizzati, è stato quello di prevedere lo studio dei tool maggiormente diffusi e reperibili su Internet, cercando di darne una visione il più ampia possibile.
Nel terzo capitolo, gli strumenti che vengono ritenuti più adatti, verranno comparati con le nuove velocità trasmissive verificandone l'adeguatezza e riscontrandone pregi e difetti.
Nel quarto capitolo verrà proposta una possibile soluzione al problema del monitoraggio di reti ad alta velocità.

2. Stato dell'Arte

In questo capitolo sono descritti in modo accurato i vari tipi di misurazioni di rete e come si effettuano. Verranno definiti gli approcci per la gestione ed i tool oggi esistenti che consentono di monitorare e intervenire sulla rete.

2.1 Misurazione del Traffico di Rete

Per la misurazione del traffico di rete sono possibili differenti approcci che si differenziano uno dall'altro per vari aspetti:

- Paradigmi di monitoraggio;
- Attori delle misurazioni;
- Tipi di misurazioni;
- Modalità di accesso ai dati di monitoraggio.

2.1.1 Paradigmi di Monitoraggio

I paradigmi per il monitoraggio di rete si differenziano per la natura degli strumenti utilizzati e delle misurazioni effettuate:

- *Monitoraggio Attivo*; viene effettuato immettendo, tramite vari strumenti, i dati nella rete. Questo tipo di tecnica aumenta il volume di traffico in transito sulla rete.
- *Monitoraggio Passivo*; viene effettuato analizzando, tramite vari strumenti, i pacchetti in transito sulla rete. A differenza della tecnica precedente si analizza il traffico generato normalmente dagli utenti della rete senza iniettarne di nuovo.

2.1.2 Attori ed Apparati per la Misurazione del Traffico

Il problema della misurazione del traffico di rete, come detto, è un problema comune a più soggetti. A seconda quindi di chi effettua le rilevazioni si possono identificare degli apparati con caratteristiche specifiche come mostrato in tabella 1.

APPARATI / **ATTORI**	END-SYSTEM	APPARATI di RETE STANDARD	MEASUREMENT GEARS
AMMINISTRATORI	**X**		
GESTORI DELLA RETE (ISP)		X	**X**

Tab. 1 Relazione fra Attori delle misurazioni e Strumenti Impiegati.

End-System

Gli apparati di tipo end-system (ad esempio un PC connesso alla rete) sono completamente sotto il controllo dell'utente che può instrumentarli a suo piacere.

Apparati di Rete Standard

Gli apparati di rete standard, più costosi degli end-system, sono utilizzati unicamente dai gestori della rete. Questi dispositivi (router e switch) mettono a disposizione un limitato set di istruzioni che serve per l'instrumentazione, ed è in grado di eseguire il collezionamento di un insieme limitato di dati.

Measurement Gears

I measurement gears sono apparati di rete dedicati, progettati appositamente per eseguire misurazioni (vedi Sez. 2.2.3 RIPE TTM). Questi sono programmabili per il collezionamento

di dati specifici e generalmente dislocati in posizioni strategiche dalle quali sono in grado di monitorare tutta la rete.

2.1.3 Tipi di Misurazioni

I sistemi che sono stati sviluppati per il monitoraggio del traffico di rete consentono diversi tipi di misurazioni in base a :

1. specifiche caratteristiche della rete (vedi Sez. 1.1.1);
2. natura del tool (vedi Sez. 2.1.1);
3. tipo di analisi che si vuole implementare.

Analisi Per-Link / End-to-End / Aggregazione di Flussi

I tool, sia attivi che passivi, in genere implementano algoritmi per l'analisi di tipo:

1. *Per-link;*
2. *End-to-End;*
3. Livelli di aggregazione di flussi[3].

L'analisi *Per-link* consiste nel misurare il traffico che transita, o viene generato, fra due nodi connessi direttamente fra loro per mezzo di un *link* (collegamento). Questa non fornisce statistiche globali di rete ma è utile agli ISP per le loro misurazioni di traffico. Esempi di tool che consentono di effettuare misurazioni *Per-link* sono SNMP MIB [2], RTFM [9] (Real-Time Flow Measurement), Cisco NetFlow [14] (vedi Cap. 2.3.2.1).

L'analisi *End-to-End* consente di eseguire rilevamenti del traffico fra due nodi connessi fra loro indirettamente. Questo tipo di misurazione opera una distinzione fra la performance di rete e quella applicativa, cioè fra le prestazioni della rete e le prestazioni delle applicazioni che usufruiscono dei servizi.

La rilevazione di flussi consente di determinare l'origine, la direzione e la destinazione del traffico immesso nella rete. Aggregando le misurazioni in base a determinate regole (per porta, *Type of Service*, indirizzo sorgente/destinazione ecc.), si riescono a ricavare dei dati statistici per la gestione.

[3] Insiemi di pacchetti con uno o più attributi comuni; ad esempio stesso indirizzo sorgente/destinatario, porta o protocollo di comunicazione [7].

Ognuno dei diversi approcci presenta problemi che devono essere valutati quali, ad esempio:

- il tempo che serve per gestire lo strumento per il monitoraggio e l'accuratezza delle misurazioni. Più misure sono fatte più dati sono collezionati, ma più dispendioso diventa ricavare informazioni dal traffico.
- il problema della sicurezza e quello della condivisione. Occorre infatti rispettare la privacy degli utenti e tenere le misure protette in modo da non rivelare informazioni sullo stato della rete, per non esporre eventuali punti vulnerabili.

2.1.4 Modalità di Accesso ai Dati di Monitoraggio

In base agli strumenti utilizzati vi sono due modalità di accesso ai dati di monitoraggio:

1. Lettura periodica dei dati da parte dei sistemi di monitoraggio;
2. Instrumentazione del dispositivo per l'invio automatico dei dati al collezionatore.

A queste due modalità corrispondono diversi sistemi. In questa sezione ci limiteremo ad analizzare i protocolli di accesso ai dati, quelli cioè che vanno a definire la prima metodologia di accesso. Per i sistemi che permettono l'invio automatico delle informazioni rimandiamo alla Sezione 2.3.2.1.1, dove verranno trattati con maggiore attenzione e accuratezza.
I protocolli analizzati di seguito hanno avuto una larga diffusione per la loro semplicità di impiego e utilizzo, per questo oggi vengono riconosciuti da tutta la comunità tecnologica come standard.

SNMP

SNMP [2] è acronimo di Simple Network Management Protocol. Si tratta di un protocollo di management che permette di raccogliere informazioni di stato e allarmi, da periferiche e sistemi collegati in rete. SNMP è in grado di controllare il valore di alcuni attributi dei MIB (*Management Information Base*) che caratterizzano i dispositivi di rete che supportano l'utilizzo di questo protocollo. Le condizioni salienti di ogni dispositivo sono raccolte dall'*Agent* specifico e inviate ad un software di controllo centrale (*Manager*).
Il sistema è di facile implementazione e quasi tutti i moderni dispositivi di rete sono dotati di un Agent SNMP. Si tratta di un software installato a bordo capace di ricevere comandi dal Manager, eseguire le operazioni richieste sul sistema locale ed inoltrare le risposte all'amministratore. L'Agent viene implementato attraverso la compilazione di un MIB nel

quale vengono definiti tutti gli eventi che possono riguardarlo e le variabili che definiscono i valori che periodicamente vengono misurati sulla rete.
La console centrale è un sistema software connesso a tutti gli Agent della rete in grado di sintetizzarne lo stato generale e segnalare gli allarmi (TRAP). Il gestore non deve così controllare periodicamente ogni parametro e dispositivo per verificare la presenza di fault perché le TRAP SNMP saranno sufficienti ad avvertirlo di eventuali problemi in corso.
Dal 1990 sono state introdotte tre versioni del protocollo, ma le più usate restano la versione 1 e la 2c. La versione 3 del protocollo, benché risolva alcuni problemi di sicurezza, ha introdotto un livello di complessità eccessivo e non ha trovato molta diffusione tra gli operatori del settore.

RMON

Il Remote Network Monitoring [3] (RMON) è uno standard di monitoraggio che permette lo scambio di dati di monitoring di rete tra varie console di management e sonde di raccolta dati. Le specifiche RMON definiscono un set di funzioni e statistiche che garantiscono all'amministratore la raccolta delle informazioni necessarie per la messa a punto della performance, il Planning di rete e la diagnosi dei fault.
RMON, definito dalla comunità Internet con l'aiuto dell'IETF, è stato presentato come una proposta di standard nel 1992, ed è diventato poi draft standard nel 1995 come RFC 1757.

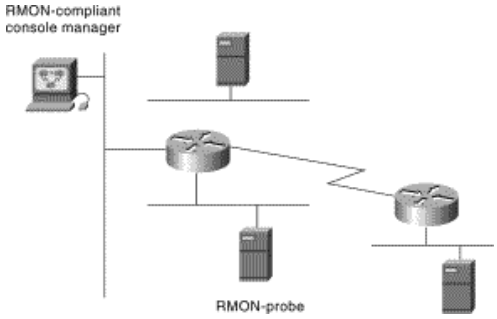


Fig. 1 Sonda RMON capace di monitorare un segmento di rete trasmettendo informazioni statistiche ad una RMON console.

Questo strumento memorizza le informazioni acquisite dalla rete in nove diversi gruppi di elementi di monitoring (insieme di oggetti SNMP che hanno caratteristiche comuni) che forniscono un set di dati standard utile per il monitoraggio di rete (Tabella 2). I gruppi non

sono tutti indispensabili ai fini dell'implementazione del sistema, ma alcuni richiedono la presenza di altri per il corretto funzionamento.

RMON è basato sull'SNMP e la sua implementazione avviene attraverso la definizione di un MIB nel quale sono definite tutte le funzioni e operazioni eseguibili da remoto.

GRUPPI RMON	FUNZIONI	ELEMENTI
Statistiche	Contiene statistiche, misurate dalle sonde, per ogni interfaccia monitorata sul dispositivo.	Pacchetti inviati/ricevuti, bytes inviati, pacchetti broadcast e multicast, collisioni, frammenti, errori CRC ecc.
Storia	Registra campioni periodici di statistiche da una rete e li memorizza per successivi utilizzi.	Periodo di campionamento, numero di campioni, elementi campionati.
Allarmi	Periodicamente prende campioni statistici dalle variabili sulla sonda, comparandoli con i valori delle soglie. Se la variabile monitorata supera la soglia viene generato un allarme.	Include tabelle di allarmi e richiede l'implementazione del gruppo eventi. Contiene vari tipi di allarmi, l'intervallo, soglie di partenza ecc.
Host	Contiene statistiche associate a ciascun host presente sulla rete.	Indirizzo di host, pacchetti, bytes ricevuti e trasmessi, pacchetti con errori ecc.
HostTopN	Genera tabelle che descrivono gli host in cima ad una lista ordinata per uno dei loro attributi base, su un intervallo di tempo definito dal manager.	Statistiche, host, periodi di campionamento iniziali e finali, durata ecc.
Matrix	Memorizza statistiche sulla comunicazione tra due indirizzi. Quando il device rileva una nuova comunicazione, aggiunge un'entry a questa tabella.	Coppie di indirizzo sorgente e destinazione, pacchetti, bytes ed errori per ogni coppia.
Filtri	Permette di confrontare i pacchetti tramite equazioni di filtraggio.	Tipi di filtri, espressioni filtro, espressioni condizionali (and, or, not) ecc.
Cattura di pacchetti	Implementa la cattura dei pacchetti che transitano su di un canale[4].	Dimensione del buffer di cattura, numero di pacchetti catturati ecc.

[4] Formato da un filtro per i dati e uno per le informazioni di stato contenute in un pacchetto.

Eventi	Controlla la generazione e la notifica di eventi.	Tipo di evento, descrizione e tempo d'invio dell'ultimo evento lanciato.

Tab 2 Gruppi RMON

2.2 Monitoraggio Attivo

I tool attivi, compresi in questa macrocategoria, generano traffico indispensabile per le misurazioni necessarie alla gestione di rete. Questo approccio consente di inviare i pacchetti da un nodo all'altro della rete, quindi i rilevamenti effettuati sono di tipo *End-to-End*. L'immissione di pacchetti nella rete comporta l'aumento del volume di traffico in transito; ciò nonostante le misurazioni attive sono importanti in quanto consentono di capire lo stato dei link (Connettività dei nodi) e specificare i tempi necessari al raggiungimento dei nodi da parte dei pacchetti.

La propagazione dei pacchetti inviati dalle varie sonde (*probe*) consente di effettuare rilevamenti riguardanti i tempi di percorrenza dei vari link, di capire se esistono dei colli di bottiglia (*Bottleneck*) che rallentano lo scambio delle informazioni, ed individuare un'ottimizzazione dello smistamento del traffico fra i vari dispositivi presenti nella rete così da renderne efficiente la struttura.

2.2.1 Tipi di Misurazione

Il monitoraggio attivo fornisce dei dati per identificare con precisione alcune misure che definiscono lo stato della rete e la sua efficienza. Queste misure sono:

- *Queueing Delay* [7]. Rappresenta la quantità di tempo che i dati attendono in coda dentro una device prima di essere instradati o, una volta ricevuti dall'host, prima di essere trasmessi alle applicazioni (*High-layer*).
- La somma fra il propagation time[5] [7] e il queueing delay fornisce la stima del tempo impiegato da un pacchetto per passare da un host ad un altro inclusi tutti i ritardi intermedi. Questo tempo prende il nome di *Trasmission Time* [7] ed è monodirezionale.

[5] Indica il limite fisico della rete; cioè la quantità di tempo necessaria per trasmettere un pacchetto una volta che questo si trova già sul supporto fisico. Questo parametro dipende dal tipo di media utilizzato, dalla sua velocità e dalla distanza che il dato inviato deve percorrere prima di arrivare a destinazione

- Il *Round Trip Time* [7] (RTT) è l`equivalente del Trasmission Time bidirezionale, cioè la somma fra i tempi che i pacchetti impiegano per raggiungere l'host di destinazione e tornare indietro.
- Il *One-Way Delay* [15] indica il ritardo di trasmissione tra un host ed un altro tra loro sincronizzati. Il formato dei pacchetti usato per la misurazione è caratterizzato dall'indirizzo del mittente, quello del destinatario e dal tempo di partenza del pacchetto (T). Indicando con dT il One-Way delay dal mittente al destinatario al tempo T, si intende che il mittente invia il primo bit del pacchetto al tempo T e il destinatario ne riceve l'ultimo bit al tempo T + dT.
- La *Bandwidth* [7] è la stima che descrive la capacità di un link, cioè la quantità di dati che possono essere trasmessi in un quanto di tempo su una sezione di rete. Questa misura viene espressa in bit-per-secondo.
- Il *Bottleneck Bandwidth* [7] indica la bandwidth del link più lento in una misurazione *End-to-End*, perciò la *Bandwidth* totale viene limitata da questa stima.
- Il *Throughtput* [7] misura la quantità di dati che possono essere inviati su un link in una quantità di tempo. Spesso questo valore viene usato come fattore per la stima della banda disponibile su un link, anche se quello che fornisce la stima più approssimata è il bandwidth. Il throughtput definisce l'effettiva disponibilità di banda in un determinato momento.
- La *Latenza* [7] rappresenta la quantità di tempo che impiega un pacchetto per andare da sorgente a destinazione, viene generalmente espressa in millisecondi (ms).
- Il *Packet Loss* [7], espresso in punti percentuali, fornisce la misura dei pacchetti inviati sul link e non ricevuti dal destinatario. Questa perdita del dato può avvenire, ad esempio, nel momento in cui il pacchetto deve attraversare una device che non riesce a smistare abbastanza velocemente il traffico e, di conseguenza, è costretta a scartare il pacchetto; oppure nel momento in cui è lo stesso host di destinazione che non riesce a ricevere tutti i pacchetti che gli vengono inviati, in quanto la sua velocità di ricezione è inferiore a quella di trasmissione della rete.
- Il *Jitter* [7] rappresenta la varianza, in un arco di tempo, del ritardo intercorso tra l'arrivo di due pacchetti consecutivi aventi lo stesso indirizzo sorgente in un link monodirezionale. Non è infatti per nulla scontato che i pacchetti arrivino a destinazione ad una distanza temporale, l'uno dall'altro, equivalente a quella di emissione; questo perché i link percorsi da ogni pacchetto possono essere diversi fra loro.

- Il *Path* [11] indica quali sono i router attraversati dai pacchetti per raggiungere la destinazione. È importante verificarne i cambiamenti in funzione del tempo in quanto, se troppo rapidi, sono indice di malfunzionamenti.

2.2.2 Tool

In questa sezione saranno analizzati i vari strumenti esistenti per l'implementazione del monitoraggio attivo delle reti. Verranno presi in considerazioni i tool maggiormente conosciuti e quelli di cui se ne prevede la diffusione nel breve periodo.

Ping

Il Ping [7] è un tool che consente di inviare uno o più pacchetti da un host ad un altro a lui remoto. In questo modo è possibile verificarne lo stato, la connettività e il trasmission time del link.
Tecnicamente il sistema trasmette un pacchetto ICMP-Echo-Request (*Internet-Control-Message-Protocol*) verso l'host di destinazione, il quale, al momento della ricezione, invia a sua volta un ICMP-Echo-Reply (pacchetto di risposta). Lo scambio dei pacchetti fra gli host sta alla base del calcolo del round trip time dato dalla differenza fra momento di invio del ICMP-Echo-Request e il successivo momento di arrivo della risposta ICMP-Echo-Reply.
Questo tool è in grado di identificare problemi di connettività fra gli host in quanto, se non si riceve risposta ai pacchetti inviati, è facile capire la mancata connessione tra i due nodi. Tuttavia è possibile che vi siano presenti dei Firewall (sistemi di filtraggio del traffico) che impediscono la ricezione dei pacchetti utilizzati dal ping. In questo caso le informazioni raccolte non sono attendibili. Facendo delle stime sul numero dei pacchetti inviati e ricevuti si riesce a determinare inoltre il Packet Loss.
Il Ping non consente di dare un valore della performance applicativa in quanto i pacchetti di scambio non vengono presi in considerazione all'high-layer, bensì dal sistema operativo. Di fatto si potrebbe avere un incongruenza fra quelle che sono le misure dei tempi di connessione fra i due host a basso livello ed a livello applicativo.

Traceroute

Il Traceroute [7] consente di scoprire il forward path seguito dai pacchetti per raggiungere l'host di destinazione. L'algoritmo che viene implementato si basa sull'invio di pacchetti ICMP e sul campo TTL (Time-To-Live, identifica il numero massimo di device che il pacchetto può attraversare prima di essere scartato) della struttura dei pacchetti nel protocollo IP (*Header IP*).

Il tool invia un pacchetto UDP con il valore del TTL uguale a 1 verso la destinazione specificata. Il primo router che instrada il pacchetto ritorna un messaggio ICMP di tipo time-exceeded (che indica che il pacchetto è stato scartato). Iterando il processo fino al contatto con l'host di destinazione si riesce a delineare il path.

Il tool non può essere utilizzato per la funzione inversa, ossia trovare il percorso seguito dai pacchetti che vengono inviati da host remoti, per la presenza di percorsi asimmetrici (ad esempio in reti con routing dinamico). Per ovviare a questo problema sono disponibili sulla rete dei server, accedibili solitamente tramite interfaccia web, che eseguono il Traceroute fino all'host locale e poi comunicano il percorso seguito dai pacchetti (Reverce-Traceroute). Questo metodo non è molto efficiente, in quanto, se si vuole verificare il path fra due host remoti, non è detto che quello identificato dai server di supporto sia effettivamente quello usato dai pacchetti.

Pathchar

Il Pathchar [7] è un tool che consente di effettuare misurazioni per la determinazione della bandwidth.

Questo tool invia dei pacchetti di dimensioni variabile ad un nodo della rete ed aspetta delle risposte da questo che gli consentono di ricavare informazioni sul percorso da analizzare. Queste informazioni sono necessarie al Pathchar per ricavare dati per la determinazione della bandwidth e del queueing delay dei vari link intercorsi fra ogni device (*Hop*). Studiando il RTT, in funzione della dimensione del pacchetto, si riesce a calcolare la bandwidth.

Questo tool richiede però dei tempi di calcolo lunghi, sia per la complessità dei calcoli da eseguire, sia per il numero e la dimensione dei pacchetti che devono essere inviati e ricevuti al fine di ottenere misurazioni realistiche .

IPerf

L'IPerf [7] è un tool che può essere implementato solo in presenza di un'architettura di tipo Client/Server. Ciò implica che lo stesso tool ha sia funzionalità da client che da server. L'algoritmo implementato prevede l'invio da parte del client di pacchetti TCP/UDP, specificando la porta su cui devono essere ricevuti, la dimensione della finestra TCP, la durata del test, e la quantità di dati da inviare.
L'IPerf consente di eseguire statistiche per la stima del throughtput, e della bandwidth, la determinazione del packet loss e del jitter. Questo tool presenta però un grosso svantaggio dato dal fatto che il sistema deve essere in esecuzione sia sulla macchina locale sia su quella in remoto e questo non è sempre possibile dato che il tool non è installabile su tutte le device di rete (ad esempio i router Cisco [29]).

Mtrace

Mtrace [7] è una variante del Traceroute, ed è usato per tracciare il multicast path dalla sorgente al destinatario. Per far questo non usa il metodo dei pacchetti ICMP + TTL, bensì si serve di alcune funzionalità implementate all'interno dei router che supportano il traffico multicast. Quello che viene misurato è infatti il path inverso dal multicast trasmitter al destinatario ottenuto applicando questo algoritmo: viene inviato un pacchetto di query al multicast trasmitter che risponderà alla query e, in parallelo, effettuerà il forward della richiesta al router multicast successivo, fino ad arrivare al destinatario. In questo modo si ottiene la traccia di tutti i router attraversati dal traffico multicast.

2.2.3 Progetti per il Monitoraggio del Traffico Internet

Alcune società ed enti hanno intrapreso numerosi progetti per il monitoraggio attivo della rete, che in generale consistono nella dislocazione di monitor in varie parti del globo (soprattutto in Nord America), in grado di effettuare vari tipi di misurazioni.

AMP

L'Active Measurement Project [16] consiste in una rete distribuita di circa 130 sonde attive che effettuano misurazioni programmate tra di loro. Questi sistemi inviano i dati ad un raccoglitore, dove sono disponibili per il download o per il pubblico accesso (http://watt.nlanr.net/active).

Tra le varie misurazioni possibili, vengono effettuate:

1. Round Trip Time, tra ognuno di questi sistemi una volta al minuto.
2. Path tra tutti i monitor di misurazione una volta ogni 5 minuti.

In maniera più dettagliata, la misurazione del RTT viene fatta usando il programma *Fping* [31]. Questa applicazione invia simultaneamente un pacchetto ICMP-Echo-Request verso ogni host e attende l'arrivo di ogni ICMP-Echo-Reply, misurando il trasmission time per tutti gli host. Usando questa variante del tool *ping* è possibile misurare più siti simultaneamente, mentre l'impiego del tool tradizionale, sequenziale, comporterebbe tempi più lunghi rispetto all'intervallo definito per la misurazione del RTT. Viene registrato un packet loss quando non si ricevono, prima del timeout, 4 ICMP-Echo-Reply alle 4 rispettive ICMP-Echo-request.
Misurare il RTT, invece della stima più precisa fornita dal One-Way Delay, è più semplice in quanto non comporta l'utilizzo di device esterni (GPS) per la sincronizzazione dei clock dei vari monitor.
Per quanto riguarda il calcolo dei path, viene utilizzato il programma traceroute, lanciato una volta ogni 5 minuti.
Si possono consultare i dati raccolti da ognuno dei sistemi tramite interfaccia Web, basta infatti selezionare uno dei siti per visualizzare i RTT medi del giorno precedente di ognuno dei sistemi all'interno della sua matrice (interconnessione completa di sistemi, in cui ogni elemento è direttamente connesso con tutti gli altri).
Oltre a questo è possibile, selezionando un sito secondario, visualizzare grafi settimanali che mostrano i RTT tra questo e il sito primario o anche consultare una lista di cambiamenti di path che sono avvenuti durante un giorno specifico.

RIPE TTM

Lo scopo del RIPE TTM [18] (www.ripe.net), sviluppato dalla RIPE NCC[6], è quello di effettuare misurazioni indipendenti su Internet di parametri di connettività quali il delay (RTT, One-way-delay) e i path.

L'idea che sta alla base del progetto è quella di analizzare il traffico tra i vari ISP. Infatti la rete locale di ogni ISP, che si occupa del traffico tra i vari client, è connessa ad una rete esterna che permette lo scambio di dati con gli altri ISP.

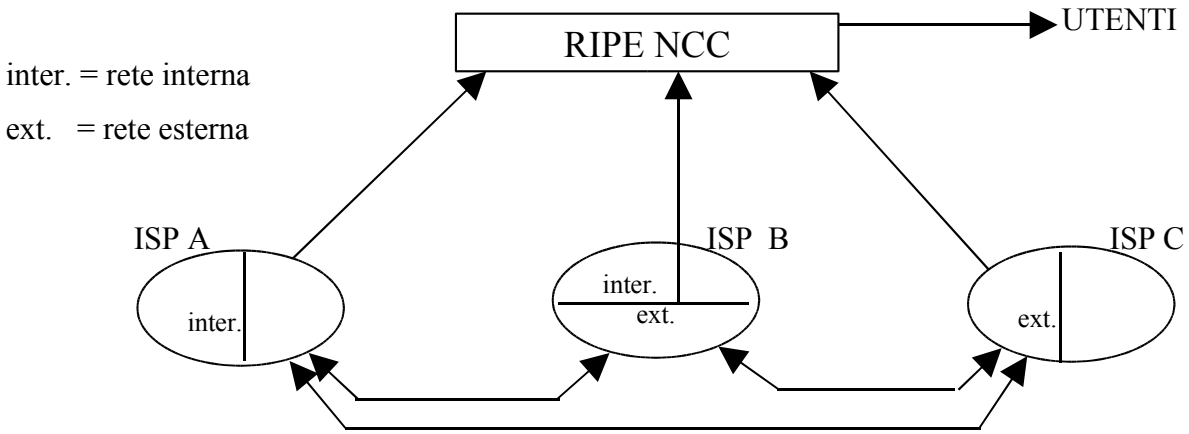


Fig. 2 Architettura RIPE TTM

I parametri da tenere in considerazione per determinare la performance della rete tra due provider, sono la bandwidth e il delay. Anche i vettori di routing (indicano la successione di

[6] Il RIPE Network Coordination Centre (RIPE NCC) è uno dei 3 Regional Internet Registries (RIR) presente nel mondo oggi, fornisce l'allocazione e la registrazione dei servizi che supportano le operazioni di Internet.

router attraversati dai pacchetti nel percorso sorgente/destinazione) sono molto importanti, in quanto danno un'idea di come il traffico viene smistato.
Per ottenere queste misurazioni, i progettisti della RIPE NCC hanno installato vari *Test Box* (specifici Measurement Gears) presso ogni provider interessato. Questi box non fanno altro che collezionare dati e trasferirli ad un server centrale, il quale li elabora e li rende disponibili agli utenti.

Il progetto è caratterizzato da 2 fasi:

1. Test One-way e Two-way.
2. Test sulle Applicazioni.

La prima fase (One-way) consiste nell'invio tra vari Test-Box di pacchetti UDP di dimensioni diverse: piccola (56 bytes, come quelli generati dal ping), media (576 bytes) e grande (maggiore 2048 bytes, per studiare gli effetti della frammentazione).
Questi pacchetti contengono:

- L'indirizzo del mittente.
- Un timestamp, che indica il momento in cui il pacchetto è stato inviato.
- Un reference number, per tenere traccia del numero dei pacchetti inviati e persi.
- Un contatore di hop.
- Informazioni amministrative, come il numero di versione del software.
- Payload, che serve a riempire il pacchetto fino alla dimensione desiderata.

Dalla parte del destinatario, una volta ricevuto, il pacchetto viene elaborato nel seguente modo:

- Viene scartato il carico inutile.
- Viene aggiunto l'indirizzo del destinatario.
- Viene aggiunto un time-stamp, che indica il tempo di arrivo del pacchetto.

Alla fine si ottiene un dato che contiene le informazioni per quella particolare misurazione.

Per quanto riguarda il path tra due ISP, per la sua capacità di variare in funzione del tempo, è necessario un tool come *traceroute*, avviato ad intervalli di tempo regolari.
Per il test two-way viene usata una procedura simile a quella illustrata in precedenza, ma questo non gode di grande considerazione essendo usato solo per confermare i dati ottenuti dal test-one-way.

La seconda fase (test sulle applicazioni) del progetto è centrata su altri tipi di misurazioni:

- Stream TCP (flussi di pacchetti che utilizzano il protocollo TCP);
- Simulazione di applicazioni;
- Packet Trains, una serie di messaggi di test inviati ad intervalli brevi, che serve a capire se i pacchetti vengono scartati sul percorso, o uniti in pacchetti più grandi lungo il tragitto.

Surveyor

Il progetto Surveyor [17] ha come obiettivo la misurazione unidirezionale *End-to-End* del delay, del packet loss e dei path lungo una serie di sonde di monitoraggio posizionate sulla rete Internet. Questo permette, sia agli utenti che agli ISP (ad ogni livello), di avere una visione comune e accurata delle performance e dell'affidabilità' di Internet.

Le principali caratteristiche del progetto sono:

- Uso di metriche standard. Senza l'utilizzo di metriche ben conosciute è impossibile capire o comparare misurazioni effettuate da applicazioni diverse. Per questo vengono usate metriche sviluppate all'interno del IETF (IPPM working group) come il One-Way-delay e il One-Way-Loss (0 se il One-Way-Delay ha valore finito, 1 se ha valore indefinito).
- Misure unidirezionali. Studi passati hanno dimostrato che molti path Internet sono asimmetrici, quindi il tradizionale RTT misura la performance di due differenti path, combinando in certi casi le performance di reti totalmente diverse. Non si deve tuttavia dimenticare che, anche in presenza di path simmetrici, è possibile che le condizioni del

traffico siano diverse durante la fase di invio e quella di ricezione dei pacchetti. Usando misurazioni unidirezionali questi problemi non si presentano.

- Uso di hardware dedicato per misurazioni accurate. Vengono usate macchine dedicate per tre motivi principali: per prima cosa questo garantisce che tutte le macchine siano uniformi ed abbiano lo stesso carico di lavoro; secondo, con l'uso di computer dedicati, è più facile usare ed installare hardware speciale per sincronizzare i clock; infine viene garantito un maggiore livello di sicurezza.
- Misurazioni continue. Surveyor è stato disegnato per essere un'infrastruttura che esegua monitoraggio continuo della rete. Invece di occupare la banda, generando un eccessivo traffico in momenti ben determinati, effettua continue misurazioni di performance tramite la generazione di un limitato volume di traffico. In questo modo, oltre a mostrare informazioni statistiche, diminuisce la probabilità di trascurare importanti situazioni anomale.
- Fornire dati delle performance a lungo termine. Accedere ai dati collezionati dalle sonde è molto importante per poter ricavare previsioni, per la capacità di planning e per il netwotk research. Per questo tutti i dati raccolti vengono archiviati in un database.
- Fornire accesso in real-time ai dati. Per la prevenzione e la rilevazione di malfunzionamenti sulla rete è necessario poter accedere a dati di performance recenti, non a report giornalieri o settimanali. Ecco perché Surveyor è stato progettato per garantire dati di performance *Near-Real-Time* (nell'arco di 5 minuti dal momento prescelto).
- Eseguire misurazioni *End-to-End*. Un Internet path, nella maggior parte dei casi, attraversa più reti appartenenti a diversi provider. Idealmente tutti vorrebbero misurare, per risolvere problemi di performance, soltanto la propria area di competenza. Siccome ciò non è sempre possibile, Surveyor garantisce misurazioni *End-to-End* che sono comunque altrettanto utili.

2.2.4 Considerazioni

Questa sezione è necessaria per chiarire degli aspetti che riguardano i progetti per il monitoraggio del traffico Internet descritti in precedenza.
Tali progetti, sviluppati per lo più da aziende private, hanno delle limitazioni che devono essere prese in considerazione:

- scalabilità delle architetture proposte;

- implementazione dei dispositivi di monitoraggio;

Per quanto riguarda il progetto AMP, la scalabilità dell'architettura proposta rappresenta un grosso limite. Di fatto, le 130 sonde sono difficilmente espandibili. Ciò significa che aggiungere delle ulteriori sonde all'architettura comporta dei notevoli costi per la sincronizzazione dei dispositivi, di conseguenza il loro numero è limitato.
Per quanto concerne Surveyor e RIPE TTM, questi si avvalgono di hardware dedicato per effettuare le misurazioni sul traffico internet, e non solo, tali dispositivi devono essere dati in uso a degli ISP che devono demandare il monitoraggio della rete alle aziende di competenza. Questo limita fortemente le possibilità di sviluppo del progetto.

	Tool	**Progetti**

CARATTERISTICHE	PING	TRACE ROUTE	PATH CHAR	IPerf	Mtrace	AMP	RipeTTM	Surveyor
Queueing Delay			●					
Trasmission Time	●		●			●		
Round Trip Time (RTT)	●		●			●	●	●
One Way Delay							●	●
Bandwidth			●	●			●	
Bottleneck Bandwidth			●	●			●	
Throughtput				●				
Latenza	●							
Packet Loss								
Jitter	●			●		●	●	●
Path				●				
Requisiti Hw/Sw Particolari		●			●	●	●	●
				●		●	●	●

Tab. 3 Tabella riassuntiva delle caratteristiche dei tool e dei progetti per il monitoraggio attivo.

2.3 Monitoraggio Passivo

L'altra grande macrocategoria di strumenti per il monitoraggio, comprende quei tool che eseguono le misurazioni passive di traffico. Questi tool hanno come caratteristica comune quella di non essere intrusivi nei confronti del traffico di rete. Infatti i dati utilizzati per le misurazioni vengono ricavati semplicemente analizzando i pacchetti che transitano attraverso una particolare device, oppure attraverso un host che ha come specifica funzione quella di ricavare dati dal traffico. In questo modo si ha la possibilità di sfruttare il normale traffico generato dagli utenti senza iniettare degli altri pacchetti come avviene nel caso del monitoraggio attivo.
Questo, se da un lato è un vantaggio in quanto le prestazioni di rete non vengono degradate, dall'altro implica il fatto che, in assenza di traffico, non è possibile eseguire nessuna misurazione.

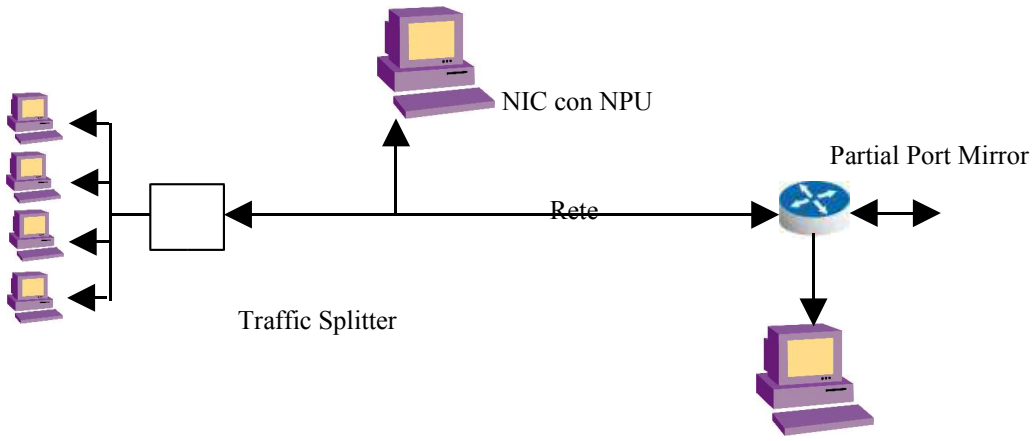


Fig. 3 Possibili architetture per il monitoraggio passivo.

La maggior parte dei dispositivi che instradano il traffico sono in grado di supportare l'implementazione dei tool passivi. Questo consente agli amministratori di instrumentare tali dispositivi (tipicamente meauserements gears, vedi Sez. 2.1.2) in modo che possano eseguire i calcoli più semplici (contare il numero dei pacchetti che hanno determinate caratteristiche, o fare aggregazione di flussi). Le informazioni raccolte vengono inviate alla console di management per eseguire l'analisi.
Le informazioni sul traffico possono essere raccolte anche direttamente da un host. Sono stati sviluppati infatti degli strumenti, hardware e software, che consentono di catturare ed analizzare i pacchetti (vedi Sez. 2.3.2).

È inoltre possibile programmare le device in modo da inviare non solo le informazioni raccolte, ma anche specifici pacchetti o flussi ad un host. Questo consente di implementare una soluzione ibrida che unisce la possibilità di instrumentare le device con la capacità dell'host di catturare il traffico.

2.3.1 Tipi di Misurazioni

I tool passivi effettuano delle misurazioni che consentono l'identificazione del traffico reale di rete. È necessario, a tal fine, che i tool verifichino le caratteristiche di ogni pacchetto che transita dal link per conoscere i parametri necessari per l'analisi del traffico. Tramite questa analisi sono in grado di conoscere l'indirizzo della sorgente/destinazione dei pacchetti, attraverso i campi dell'Header IP, e la natura dei protocolli ad esempio HTML, FTP.
Le misurazioni effettuate con gli strumenti passivi forniscono un valore reale sulle condizioni di un link della rete in un preciso istante. Questo rende i sistemi passivi indispensabili per il monitoraggio di rete. Utilizzando i sistemi attivi non si possono ricavare, con la stessa precisione, le misure ricavate con i tool passivi, in quanto le informazioni raccolte indicherebbero solo una stima della situazione reale.
Tuttavia per una gestione corretta ed efficiente della rete è necessario che gli amministratori si servano sia di tool attivi che passivi in quanto ci sono misure che possono essere ricavate solo implementando uno dei due approcci (ad esempio le misure fornite dal Ping non sono possibili con tool passivi).
La misurazione del traffico reale consente agli amministratori di capire in che misura viene sfruttata la rete. Questo tipo di misura si ottiene monitorando il traffico che transita su un determinato link in un determinato momento. È logico pensare che l'utilizzo della rete cambi durante il giorno, la settimana, l'anno perché chi usufruisce del servizio, coloro cioè che generano traffico, possono accedervi in momenti diversi. In un contesto aziendale, ad esempio, il traffico sarà nullo durante le ore notturne e nei fine settimana. Questa caratteristica fa sì che raccogliendo i valori di queste misure, ad esempio in un database, si possano ricavare informazioni statistiche, generali o specifiche, relative al funzionamento della rete in un intervallo di tempo.
Le misurazioni eseguite sul traffico reale devono avvenire con cadenza regolare proprio per permetterne l'analisi statistica. Ciò implica la determinazione di un preciso intervallo di tempo che intercorre fra una misurazione e l'altra. Ad esempio, se si desiderano dati

sull'utilizzo che viene fatto della rete durante l'arco settimanale, le misurazioni dovranno essere effettuate ogni 12-24 ore.

2.3.2 Tool

I tool passivi che consentono la rilevazione di informazioni di rete sono vari fra loro. Vi sono dei dispositivi hardware, che già implementano dei servizi di instradamento, equipaggiati con strumenti utili al monitoraggio, e dei tool software che, a seconda delle loro caratterizzazioni, si possono distinguere in più famiglie.
Di seguito verranno analizzati i tool software, specificando la famiglia di appartenenza, dopodiché i dispositivi hardware che mettono a disposizione funzionalità di monitoraggio.

2.3.2.1 Software

Come detto in precedenza gli strumenti Software possono essere distinti in diverse famiglie:

- Tool per l'analisi dei flussi:
  analizzano i flussi che transitano sulla rete;
- Tool per la cattura dei pacchetti:
  eseguono la cattura dei pacchetti dalla rete.
- Sonde generiche:
  tool che eseguono funzioni sia di cattura dei pacchetti che di analisi dei flussi (ad esempio per la rilevazione di violazioni di sicurezza).
- IDS (Intrusion Detection System):
  tool che consentono di rilevare una serie di attacchi di rete.

2.3.2.1.1 Analisi dei Flussi

L'analisi dei flussi viene fatta attraverso dei tool eseguiti in parte dagli apparati di rete in parte dai terminali degli amministratori. Gli strumenti appartenenti a questa famiglia sfruttano la capacità delle device di analizzare il contenuto dei pacchetti simultaneamente su tutte le interfacce.
L'implementazione prevede il conteggio del numero di flussi in transito, la loro identificazione, l'incapsulamento dei dati in un pacchetto e il suo invio al terminale degli amministratori. A questo punto verrà eseguita l'aggregazione delle informazioni provenienti da più device al fine di eseguirne l'analisi e trarne dati riguardanti l'intera rete.

SFlow

SFlow [19] è un protocollo per monitorare il traffico in una rete contenente switch e router. In particolare definisce:

- il meccanismo di campionamento (*sampling*) implementato all'interno degli Agent sFlow,
- il MIB sFlow per controllare i dispositivi di monitoraggio e il formato dei dati usato per inviare informazioni ad un Manager.

I principali benefici derivanti dall'utilizzo del sampling dei pacchetti sono:

- Monitoraggio accurato del traffico di rete, anche a velocità superiore al Gbit/s.
- Architettura scalare che permette di monitorare il traffico in transito da oltre 10.000 device.
- Implementazione degli Agent a basso costo.

Il sistema di monitoraggio sFlow consiste in un agent (all'interno di un router/switch o sonda specifica) e in un raccoglitore centrale dati, detto sFlow Analyzer. L'Agent sFlow si serve del meccanismo di sampling dei pacchetti (campionamento dei pacchetti in transito dalla rete) per catturare traffico in transito dalla device. In seguito vengono usati gli sFlow-datagram, pacchetti UDP, per inviare le informazioni ad un sFlow Analyzer, che effettuerà delle analisi sui dati ricevuti.

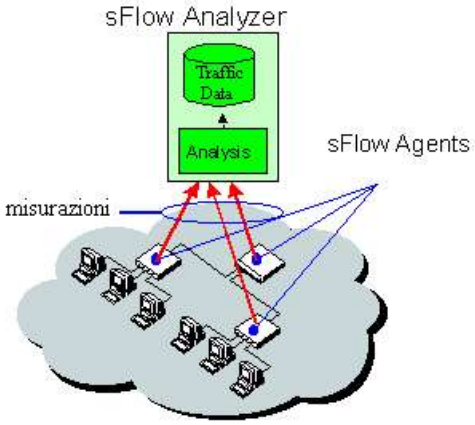


Fig. 4 Schema funzionale di sFlow.

Gli agent sFlow permettono di definire due approcci diversi per il sampling eseguito nei dispositivi:

- Sampling dei pacchetti. Analizzando un campione di pacchetti in ingresso alla device si ricostruiscono i flussi eseguendo dei calcoli statistici
- Sampling di informazioni raccolte dalle interfacce delle device. Il tool campiona, dai vari dispositivi, i valori indicati dai contatori posti sulle interfacce e riguardanti specifici flussi.

Nel primo caso il meccanismo di sampling deve garantire che tutti i pacchetti, in transito da un router o switch, abbiano la stessa probabilità di essere campionati indipendentemente da:

- il tipo di pacchetto;
- il tipo di flusso che identificano;
- la sua provenienza.

Il secondo meccanismo di sampling ha l'obiettivo di raccogliere periodicamente dati dalle device al fine di calcolare statistiche sul traffico in transito sulla rete. I dati raccolti, ad esempio, possono riguardare il numero di pacchetti inviati con un certo protocollo di comunicazione (UDP/TCP) o il numero di pacchetti che sono stati scartati dal dispositivo.
I dati raccolti attraverso i due tipi di sampling vengono aggregati in un unico sFlow-datagram che viene inviato sFlow Analyzer.
Per ragioni di efficienza e scalabilità, il sistema sFlow implementa il Counter-Polling cioè la gestione autonoma dell'invio dal parte dell'agent della risposta al manager che ha fatto richiesta di particolari informazioni. Viene assegnato, dal manager un intervallo di tempo nel

quale l'agent è costretto ad inviare la risposta di polling, ma, all'interno di questo intervallo, è libero di schedulare l'operazione in modo da migliorare la sua efficienza.

NeTraMet

NeTraMet [20] è un'implementazione Open Source (GPL) dell'architettura Realtime Traffic Flow Measurement (RTFM) [9] per la misurazione dei flussi di traffico di rete.
L'architettura RTFM è caratterizzata da una serie di strumenti (*meter*), dislocati nelle rete, che misurano i flussi di traffico e creano tabelle di report dei dati.
RTFM definisce i flussi come il traffico generato in un intervallo di tempo da uno specifico componente della rete (in questo specifico caso i componenti della rete vanno intesi come: host, gruppi di host, porzioni di rete).
I report creati dai meter vengono letti dai cosiddetti *Meter Reader*, che sono configurati dai manager contestualmente ai meter stessi. I NeTraMet meter sono Agent -SNMP che implementano il Meter-MIB-RTFM, un MIB disegnato per permetterne l'interazione con i Manager-SNMP. Questo costringe gli amministratori ad utilizzare applicazioni specifiche per interagire con i NeTraMet meter.

Ricapitolando l'architettura RTFM è formata da diversi componenti (fig. 5):

- Applicazioni di analisi,
  per l'analisi dei dati raccolti.
- Manager,
  per la configurazione dei componenti di più basso livello.
- Reader,
  per il trasporto dei dati alle applicazioni di analisi.
- Meter,
  per la raccolta dei dati dalla rete.

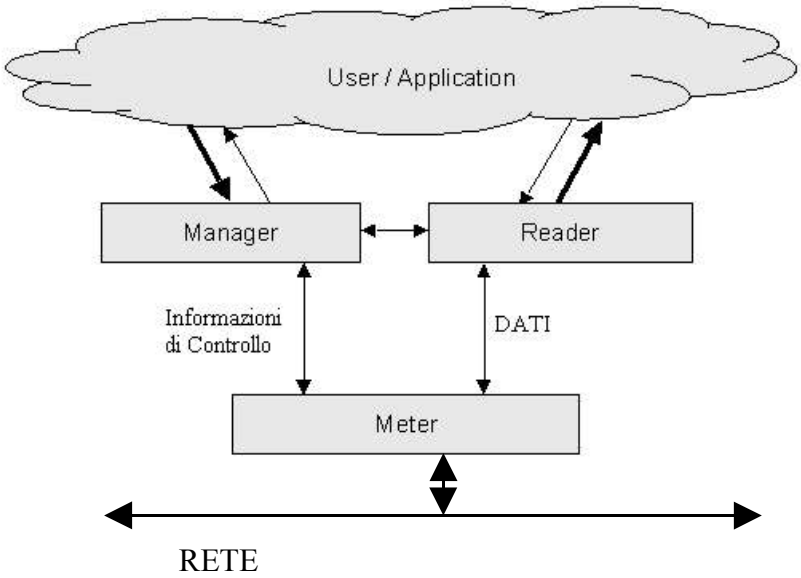


Fig. 5 Schema dell'architettura RTFM.

In particolare le applicazioni di analisi possono effettuare:

- Analisi dei flussi,
  utile per capire come variano i flussi di traffico nel tempo ed individuare il nodo di maggior traffico.
- Accounting,
  necessario per l'identificazione del traffico inviato e ricevuto da un particolare host.

RTFM definisce un set di circa 40 attributi che possono essere imputati ad ogni flusso ed usati per la descrizione dei dati. I più importanti fra questi sono gli attributi dell'indirizzo, che specificano l'indirizzo ad un particolare livello della rete. Ad esempio per i pacchetti IP, il SourcePeerAddress e il DestPeerAddress definiscono i pacchetti da e verso indirizzi IP specifici.

Per configurare un meter RTFM, un amministratore deve prima creare un set di regole (*ruleset*) in modo da indicare:

- su quali flussi effettuare le misurazioni;
- qual è la sorgente dei flussi;
- il livello di dettaglio delle misurazioni per ogni flusso.

Queste regole verranno applicate dal meter agli attributi di ogni pacchetto in transito. Se il pacchetto contiene gli attributi richiesti (*match*) viene incrementato il contatore relativo, altrimenti viene iterato il processo sugli attributi del nuovo pacchetto.

NetFlow

La tecnologia NetFlow [14] è parte integrante del sistema IOS Cisco (*Internet-Operating-System*). NetFlow è usato per raccogliere e misurare i dati in ingresso su interfacce specifiche di router o switch. Analizzando le misurazioni effettuate con NetFlow, un gestore di rete può identificare:

- Le cause di congestione di rete.
- La classe di servizio (CoS) per ogni utente ed applicazione.
- Il traffico, in ingresso e uscita, generato da ciascun utente.

NetFlow può essere usato sia con probe prodotti da Cisco, che con quelli di terze parti. Garantisce misure estremamente granulari e precise del traffico, nonché la collezione delle informazioni sui flussi.

Questo tool include tre componenti chiave:

1. *Flow Caching*. Analizza e raccoglie i flussi IP che entrano dalle interfacce di un dispositivo e prepara i dati per l'esportazione. Permette l'aggregazione dei pacchetti in flussi con caratteristiche univoche, quali gli indirizzi IP, l'applicazione e la CoS.
2. *Flow Collector*. Cattura i pacchetti inviati dai dispositivi, li filtra, li aggrega secondo specifiche politiche, ed infine li archivia in un Data-Record. Attraverso le regole (*template*) di aggregazione, il Flow Collector è in grado di filtrare diversi tipi di flussi.
3. *Network Data Analyzer*. È il componente di analisi del traffico. Combina un'interfaccia grafica con altri moduli che possono ricercare, mostrare e analizzare i dati NetFlow collezionati nei Data-Record del Flow Collector. Questo permette all'utente la visualizzazione in *near-real-time* e l'analisi dei dati già aggregati e archiviati. L'utente può inoltre specificare lo schema di aggregazione, gli intervalli di tempo e il router dal quale ricavare i dati per l'analisi.

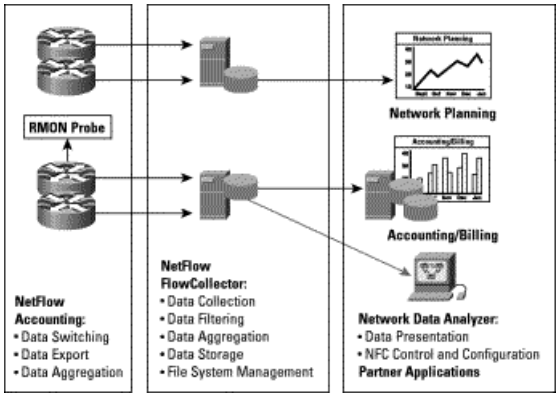


Fig. 6 Schema funzionale del NetFlow

All'interno di un Data-Record NetFlow sono presenti varie informazioni, tra cui:

- Indirizzo IP sorgente e destinazione;
- Porte TCP/UDP sorgente e destinazione;
- Type of Service;
- Conteggio di pacchetti e byte;
- Timestamp iniziali e finali;
- numero di interfacce I/O;
- Flag TCP e protocolli incapsulati (TCP/UDP);
- Informazioni di routing.

Un esempio di Flow Collector è il cFlowd, trattato nella sezione seguente.

CFlowd

Il CFlowd [21] è un importante strumento open-source per l'analisi dei flussi, principalmente quelli generati dal NetFlow della Cisco. La sua struttura è suddivisa in tre moduli ad alto livello:

1. *Cflowdmux.* È il programma responsabile della raccolta dei dati dai router/switch per renderli poi disponibili agli utenti.
2. *Cflowd.* Questo programma mantiene un'interfaccia di ingresso per i dati provenienti da ogni device, per poi inviarli, in forma tabellare, ad un raccoglitore centrale.
3. *Cfdcollect.* È il raccoglitore centrale che permette di recuperare i dati da ogni istanza di cflowd e memorizzarli in un database.

L'analisi dei pacchetti effettuata da questo tool permette agli ISP e agli ingegneri della rete, di operare delle pianificazioni, ripartire il traffico ecc. Altre aree in cui cFlowd apporta un valido aiuto sono quelle del Web-Hosting, perché permette di tener traccia dell'uso della banda, dell'accounting e del billing.

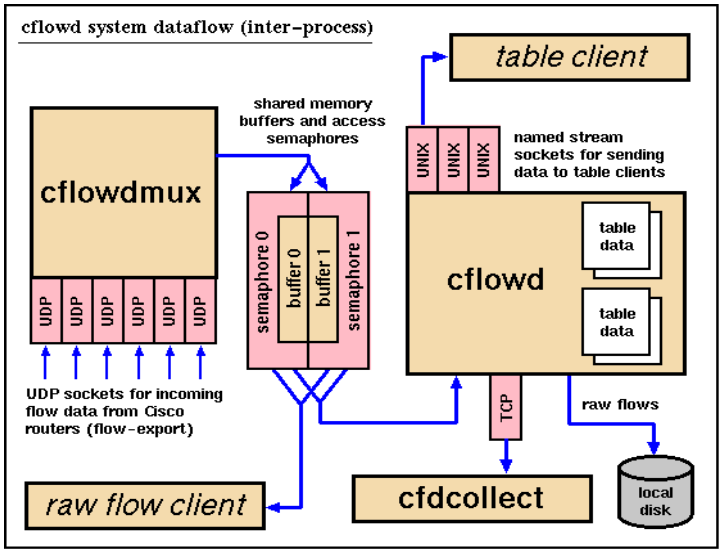


Fig. 7 Schema funzionale del cFlowd

FlowScan

FlowScan [22], simile al *Cfdcollect*, è un tool open-source per la creazione di report sui dati in formato NetFlow per consentirne la visualizzazione ai gestori di rete. Il tool in primo luogo scandisce i Data-Record cFlowd ed esamina ogni flusso. Secondariamente, tramite dei contatori relativi ad ogni tipologia di flusso, archivia periodicamente le statistiche calcolate in un Round-Robin-Data-Base (RRDtool) ad alte prestazioni. Ogni Record generato dal FlowScan contiene da una a otto statistiche di traffico, memorizzate ogni 5 minuti, basate su uno di questi attributi-flusso:

- Il protocollo usato (ICMP, UDP, TCP);
- L'applicazione o il servizio che genera il traffico (ftp, snmp, http …);
- La classe di indirizzi (A,B,C), ma anche gli indirizzi locali in forma CIDR;
- La coppia di AS (Autonomous System) tra cui il traffico viene scambiato.

Oltre a questo FlowScan mantiene un database generale che contiene informazioni sul traffico totale, multicast e quello che coinvolge reti non conosciute.

In definitiva, FlowScan utilizza le capacità di visualizzazione di RRDtool e di altri front-end al fine di creare report sui flussi di dati processati.

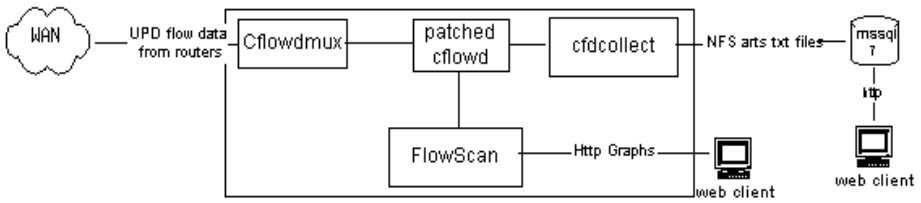


Fig. 8 Interazione fra cFlowd e FlowScan

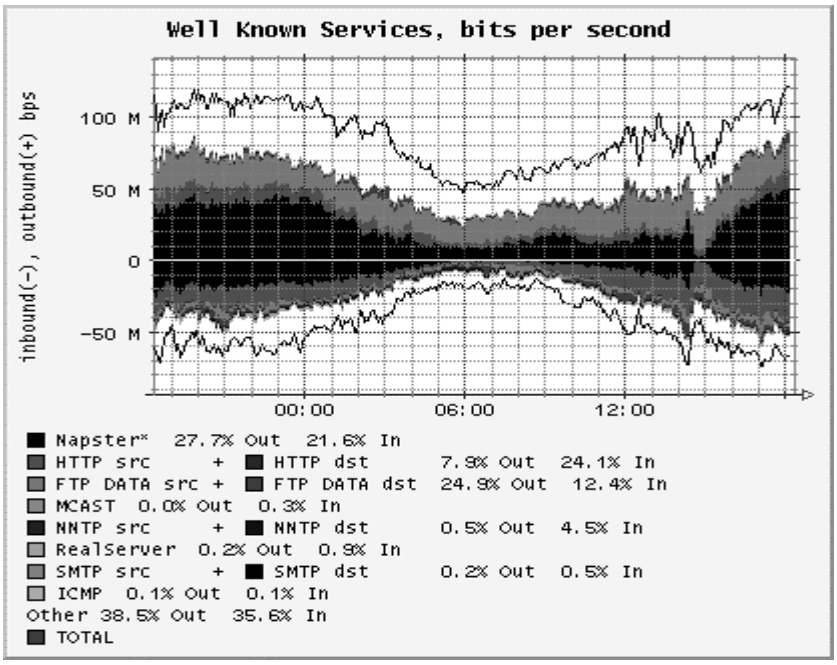


Fig. 9 Esempio di report generato da FlowScan

2.3.2.1.2 Cattura dei Pacchetti

Un altro sistema per monitorare passivamente la rete consiste nell'uso di NIC (Network Interface Card) per la cattura e l'analisi del traffico (vedi Sez. 2.3.2.2.1). Attraverso un host periferico si riescono, infatti, ad estrarre dal traffico le informazioni necessarie alla gestione di rete, senza dover demandare questo compito ai dispositivi di instradamento.

Le NIC odierne montano dei processori specializzati per l'analisi del traffico e sono in grado di catturare ed elaborare i pacchetti in transito su reti dalla velocità di circa 2.5 Gbit/s.

Nonostante ciò hanno bisogno di alcuni componenti software, che verranno studiati in questa sezione, che possano gestire le politiche di cattura dei pacchetti.

TCPDUMP

Tcpdump [7] è un tool, basato su Libpcap e da utilizzare a command-line, specializzato nella cattura e nell'analisi dei pacchetti che transitano sulla rete. Questo tool può essere utilizzato soltanto dai gestori della rete, in quanto è necessario possedere i diritti di amministratore.
Per l'utilizzo di questo tool, la NIC viene impostata di solito in modalità promiscua: viene cioè abilitata la scheda a catturare tutti i pacchetti in transito sul link, anche se non sono indirizzati ad essa. È comunque possibile impostare dei filtri per limitare la cattura dei pacchetti, cioè delle politiche che permettano di scartare le informazioni non necessarie ai fini della gestione.
TCPDUMP consente di ricavare informazioni che riguardano:

- Il tempo di trasmissione del pacchetto;
- L'host e la porta sia sorgente che destinataria;
- Il protocollo di trasferimento;
- Il payload.

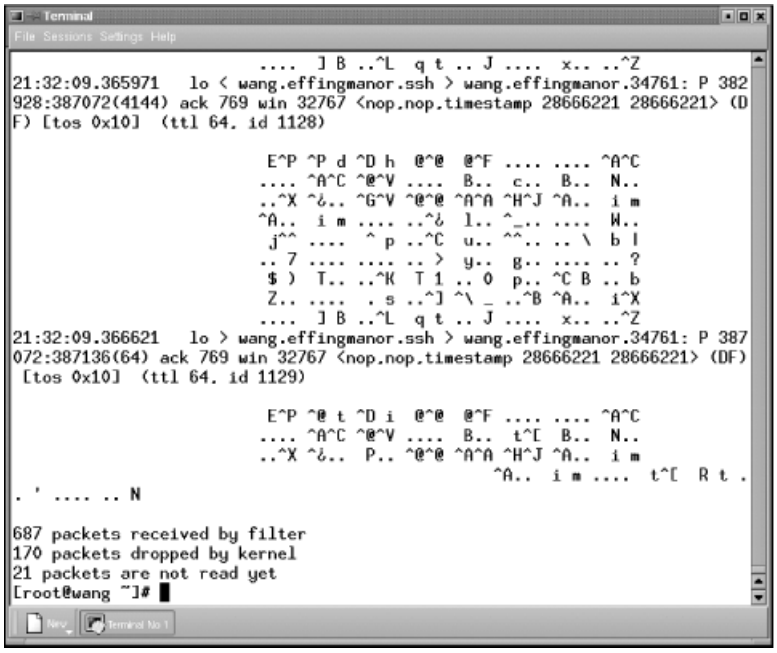


Fig. 10 Screenshot TCPDUMP.

ETHEREAL

ETHEREAL [10] è un tool grafico basato su Libpcap (simile a Tcpdump) dotato di molti decoder adatti alla maggior parte dei protocolli di rete. Fra le sue funzionalità le più importanti sono:

- La capacità di ricevere in ingresso dati compressi ed eseguire la decompressione in modalità trasparente all'utente;
- Il funzionamento sia in modalità grafica, con un interfaccia che ne rende facile l'utilizzo, sia in modalità testuale, utile nel caso della gestione di sonde multiple dislocate in diversi punti della rete.
- La capacità di ricostruire i flussi TCP senza il vincolo della trasmissione ordinata dei pacchetti. Questo consente all'analista di risparmiare tempo e potenza computazionale della macchina con cui opera, in quanto il tool effettua un ordinamento logico dei pacchetti.

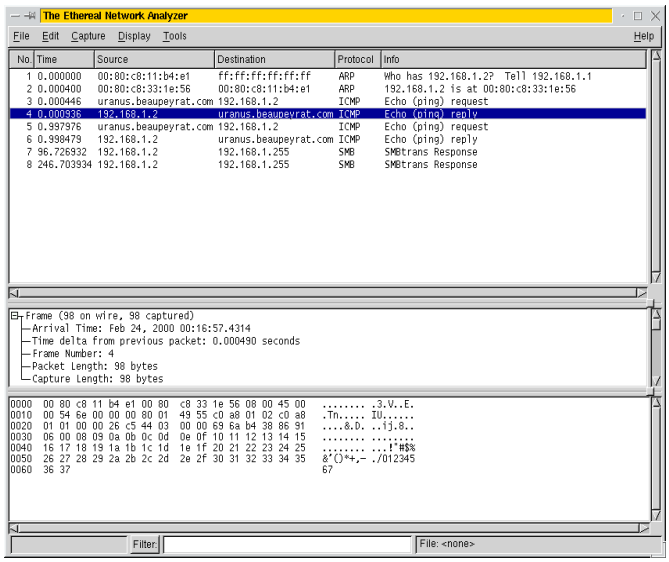


Fig. 11 Screenshot di Ethereal.

LIBPCAP

La libreria Libpcap [23] permette la cattura di pacchetti attraverso un interfaccia di rete. I passi di utilizzo della libreria sono:

1. Inizializzazione della libreria. Durante questa fase viene specificata la NIC attraverso la quale si riceveranno i dati in ingresso. È possibile indicare più interfacce di rete e gestirle separatamente assegnando ad ognuna un "nome di sessione" per riuscire a distinguere la fonte delle informazioni.
2. Descrizione delle politiche di cattura. Si tratta di impostare un filtro per limitare il tipo di traffico che si vuole catturare: distinzione per protocollo, porta o indirizzo sorgente/destinazione ecc.. Tali regole vengono compilate da un dispositivo interno alla libreria che viene invocato come una funzione.
3. Ciclo di cattura. Questa fase costituisce il nucleo della Libpcap. Durante l'esecuzione di questo ciclo infatti, si processano i dati, si applicano le regole descritte nella fase due e si decide l'azione da intraprendere sui pacchetti: aprirli per verificarne il contenuto, inviarli direttamente ai gestori o memorizzarli in un file.

CoralReef

CoralReef [8] è una suite per il monitoraggio passivo del traffico. La sua architettura è organizzata principalmente in due stack di componenti software e in altre piccole utility:

- il *raw traffic stack* gestisce direttamente i pacchetti o celle lette dalla rete;
- il *flow stack* gestisce il flussi di dati.

Il cuore del primo è la libreria *libcoral* che permette ai programmatori di accedere, con la scrittura di una singola applicazione, ai diversi formati dei dati. Questa libreria infatti fornisce delle API (*Application-Protocol-Interface*) per catturare il traffico da speciali schede ATM e PoS, nascondendo i dettagli hardware agli utenti.
Il flow stack invece include dei moduli per la memorizzazione e la manipolazione di tabelle contenenti le informazioni sui flussi collezionati. Ad esempio, le misurazioni del volume di traffico possono essere aggregate dal valore di alcuni attributi come il numero di pacchetti analizzati. Questi moduli riescono automaticamente ad organizzare i dati in tabelle, aventi diverse chiavi, che facilitano l'individuazione di coloro che generano maggior traffico. È possibile infatti, con la chiamata ad un metodo, convertire una tabella di contatori, tipicamente di flussi, ordinata per numero di AS sorgente, in una ordinata per host sorgente.
All'interno della suite troviamo anche programmi, di minor importanza per il tool, per generare flussi di dati, API per manipolarli e funzioni per la generazione di report sui flussi

stessi.

I componenti software del *raw traffic stack* sono:

- *Sorgenti di Input:*
  - Dispositivi,
  - file,
  - Libpcap,
- *Libcoral,*
- *Perl API,*
- *Raw Traffic Application.*

Il CoralReef ha introdotto nel campo delle misurazioni di rete il concetto di *Intervallo*. Per rendere il management dei flussi di dati più semplice e permettere un confronto significativo fra le informazioni, i gruppi di tabelle vengono organizzati in intervalli[7].

In questo modo, si rappresenta uno *Snapshot* di tutto il traffico di rete collezionato in un determinato momento.

All'interno del CoralReef flows stack si trovano appunto tutti programmi che generano intervalli di flussi e librerie per la loro lettura, scrittura ed elaborazione.

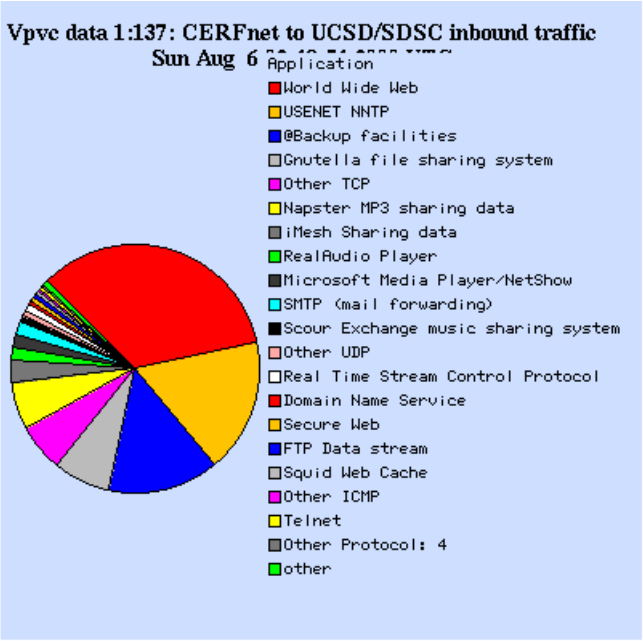


Fig. 12 Esempio di report CoralReef.

[7] La sintesi di tutti i flussi, presenti su ogni interfaccia, in un periodo fisso di tempo.

2.3.2.1.3 Sonde Generiche

Questo tipo di sonde combinano diverse funzioni, proprie di alcuni degli strumenti analizzati nella sezione precedente, in un unico tool. Di seguito viene riportata l'analisi di una sonda generica scelta dagli autori in quanto le sue funzioni incontrano, in parte, i requisiti necessari per l'analisi del traffico di reti ad alta velocità (vedi Capitolo 3 Sezione 3.2).

Ntop

Ntop [24] è un'applicazione per la misurazione del traffico e il monitoraggio delle applicazioni basata sul Web, scritta in linguaggio C e rilasciata sotto la licenza GNU. Le caratteristiche che la differenziano sono:

- Portabilità tra piattaforme Unix e non Unix;
- Kernel dell'applicazione semplice ed efficiente che comporta un bassissimo uso della CPU e della memoria;
- Abilità di monitorare una rete da remoto senza il bisogno dell'utilizzo di specifiche applicazioni client per analizzare le informazioni di traffico;
- Requisiti minimi, ma capacità di sfruttare le caratteristiche di ogni piattaforma (ad esempio utilizzo dei thread);
- Possibilità di mostrare i dati in forma tipo terminale a caratteri e anche in forma WEB;
- Analisi del traffico in uscita ricca di contenuti e facile da leggere;
- Possibilità di ampliamento delle funzionalità da parte dell'utente grazie a numerosi plugins;
- Cattura dei pacchetti e demultiplexing indipendenti dal sistema operativo e dalla NIC usati.

Per quanto riguarda la cattura dei pacchetti, per garantire la portabilità del prodotto tra diversi sistemi operativi, è stato effettuato il porting della libreria libpcap per piattaforme non-Unix. L'analisi dei pacchetti si effettua processandoli singolarmente. A seconda del protocollo utilizzato, le informazioni vengono immagazzinate in varie tabelle hash e vengono effettuati due tipi di caching: quello di primo livello basato sul *GNU gdbm,* per informazioni quali

indirizzo IP o sistema operativo usato, e quello di secondo livello che è implementato usando lo Standard Query Language (SQL).

Alla base dell'analisi dei flussi c'è il filtraggio dei pacchetti effettuato tramite il Berkley Packet Filter (BPF). Questo strumento permette di specificare delle regole, da applicare ai pacchetti, che consentono la determinazione dell'appartenenza o meno del pacchetto ad un certo tipo flusso. Verificata tale appartenenza, viene aggiornato il contatore di flusso associato.

Tutte queste caratteristiche rendono *ntop* uno strumento utilizzabile per molti scopi:

- Misurazioni di traffico.

  Ntop associa ogni pacchetto catturato con l'host di provenienza e destinazione, permettendo di determinare per ogni host alcuni parametri quali: traffico TCP, UDP, IP Multicast, tipi di S.O. ecc.
- Caratterizzazione e monitoraggio del traffico.

  Il tool permette di determinare, attraverso il monitoraggio, situazioni anomale utili agli amministratori di rete, come: uso di IP duplicati, configurazione errata di applicazioni software, eccessivo utilizzo della banda ecc.
- Rilevazione di violazioni di sicurezza.

  È molto importante poter bloccare violazioni di sicurezza ed evitare il generarsi di punti vulnerabili interni al sistema. Per questo ntop fornisce strumenti per la prevenzione e la rilevazione di molti tipi di attacchi: *portscan*, *spoofing, spy, DoS* ecc. In presenza di una violazione di sicurezza, l'applicazione riporta il problema all'amministratore, cerca di capire da dove proviene l'attacco osservando le informazioni memorizzate nel database e nel frattempo cerca di neutralizzare l'attacco stesso.
- Ottimizzazione e pianificazione della rete.

  La pianificazione accurata della rete permette di migliorare le performance ed è quindi necessario capire se alcune risorse vengono utilizzate in maniera errata. Attraverso ntop si possono identificare: protocolli non utilizzati, routing non ottimale, distribuzione del traffico non bilanciata ecc.

2.3.2.1.4 IDS (Intrusion Detection System)

La rilevazione di intrusioni nella rete (IDS), ovvero la necessità di verificarne la sicurezza, sta diventando una prospettiva importante per la gestione di rete (vedi Cap. 3 Sez. 3.2). Gli autori, analizzando il tool descritto di seguito, hanno cercato di descrivere come la comunità

internet stia cercando di proporre soluzioni adeguate alle esigenze degli amministratori di rete.

Snort

Snort [25] è un IDS open-source, basato su libpcap, usato per la rilevazione di attacchi di rete. Infatti mentre tutti i moderni IDS (intrusion detection system) hanno la caratteristica comune di avere un prezzo molto elevato, Snort è disponibile con licenza GNU GPL. Una delle sue caratteristiche principali è l'uso di un sistema di regole che permette di determinare molteplici attacchi quali: port scan, CGI attacks ecc. Inoltre, quando si verifica un evento sospetto, Snort ha la capacità di allertare in real-time l'amministratore tramite Server Message Block (SMB), messaggi "WinPopup", ecc.
Il sistema di rilevazione può essere programmato usando un semplice linguaggio, tramite il quale è possibile descrivere tutti i test e le azioni da effettuare sui pacchetti catturati.

In generale le tre componenti principali di Snort, che si basano tutte sulla libreria libpcap, sono:

1. Il decoder dei pacchetti.
   Ogni subroutine del decoder impone un ordinamento nei pacchetti, sovrapponendo strutture dati al traffico di rete. Queste routine di decoding vengono azionate per tutto lo stack dei protocolli, dal livello dei link fino a quello delle applicazioni. Il maggior compito di questo sottosistema è quello di posizionare dei puntatori all'interno dei pacchetti per una successiva e accurata analisi da parte del sistema di rilevazione.
2. Il motore di rilevazione.
   Snort mantiene le regole in una linked list bidimensionale: c'è una prima lista di regole, chiamata Chain Headers, che contiene gli attributi comuni; poi un seconda lista, chiamata Chain Options, contenente le opzioni particolari per i vari tipi di attacchi. Scorrendo queste catene di regole ricorsivamente per ogni pacchetto, si riesce velocemente a rilevare pacchetti sospetti.
3. Il sottosistema di logging e alerting.
   I tipi di log e alert vengono scelti a runtime da linea di comando fra una gamma che comprende 3 opzioni di log e 5 opzioni di alert. Tra le opzioni di log si ha la possibilità di scegliere se memorizzare i dati in un formato leggibile o binario, ma si può anche decidere di disattivare il logging per migliorare la performance. Come già detto gli allarmi

possono essere inviati ad un syslog, memorizzati in un file di testo o inviati come messaggi Winpopup usando il Samba smbclient.

2.3.2.2 Hardware

Per quello che riguarda il monitoraggio passivo, come detto in precedenza, si ha la possibilità di utilizzare dei dispositivi hardware che implementano delle funzioni necessarie per la gestione di rete. Questi offrono dei supporti più che adeguati per il corretto e veloce funzionamento dei tool che abbiamo analizzato fino a questo punto.

I componenti hardware possono essere distinti in due categorie:

- NIC con NPU (Network-Process-Unit),
  particolari schede di rete, che montano processori specializzati per la cattura del traffico.
- Apparati di rete,
  Dispositivi di rete, tipo router/switch, che mettono a disposizione funzionalità di monitoraggio.

2.3.2.2.1 NIC con NPU

Il monitoraggio passivo si basa sullo studio del traffico reale che transita sulla rete. Per questo è necessario disporre di hardware che permetta la cattura dei pacchetti che verranno poi analizzati sia da funzioni hardware, sia da funzioni software. Una soluzione naturale a questo problema è l'installazione su di un PC di una scheda particolare che possa effettuare il filtraggio del traffico catturato in modo da ottimizzare la potenza computazionale del processore centrale. Di seguito verranno analizzate alcune NIC che sono in grado di catturare pacchetti che transitano su reti ad alta velocità (ordine di alcuni Gbit/s).

DAG Card 4.0

L'università di Waikato (Nuova Zelanda) ha sviluppato una serie di schede, le Dag4 [26], studiate per la cattura del traffico con interfaccia a fibra ottica (2.488 Gb/sec).
Tra le versioni più interessanti troviamo la Dag 4.0 studiata per il traffico ATM e la Dag 4.1 in cui è stato introdotto il supporto per il PoS.

Per ovviare ai problemi dell'elevata velocità della rete e delle limitazioni del bus, la serie Dag4 introduce un chip Frame-Processor, implementato in un Xilinx FPGA. Ogni pacchetto, o cella che sia, viene datato e memorizzato temporaneamente in una coppia di code FIFO prima di essere elaborato dal processore. Tutto ciò permette al sistema la gestione di picchi di traffico full-rate.
La Dag 4.0 si interfaccia con l'host locale attraverso il bus PCI nella versione standard a 32 bit (33 Mhz) che garantisce all'incirca un terzo della banda della fibra ottica. Per questo la scheda non ha la possibilità di poter inviare tutto il traffico catturato al processore centrale a meno di un elevata perdita di informazione. Viene quindi applicato il filtraggio dei pacchetti e la compressione dei dati per inviare alle applicazioni di misurazione soltanto le informazioni necessarie, tralasciando il traffico inutile.

La versione 4.1, ancora in fase di sperimentazione, si basa su di un velocissimo Virtex FPGA della Xilinx che permette di utilizzare l'interfaccia più veloce del bus PCI a 64 bit (66 Mhz), questo la rende interessante ai fini del documento.
Entrambi i modelli supportano l'installazione di un antenna GPS per la sincronizzazione dei clock tra le varie schede distribuite sulla rete.

RADYSIS ENP-2505/ENP-2506

La serie RADYSIS ENP [27], a differenza delle schede Dag, permette la cattura del traffico Ethernet. La RADYSIS ENP-2505 ha 4 porte Ethernet 10/100 e quattro LXT 972 tranceiver. L'interfaccia utilizzata per connettere la NIC all'host locale è anche in questo caso il bus PCI.
La ENP-2506 è identica alla precedente, ma vi sono state aggiunte due porte ottiche Gigabit Ethernet; è questa la scheda più adatta, fra le due, alle esigenze del documento.
Il cuore di queste schede è l'Intel IXP1200, molto più flessibile rispetto ad una tradizionale unità ASIC di network processing. Studiato per la programmabilità sia a livello utente sia per le alte prestazioni, l' IXP1200 è formato da un nucleo StrongArm (SA) e da sei microprocessori RISC programmabili tutti integrati in un singolo chip. Questi microprocessori hanno lo stesso clock-rate del SA e sono specializzati per il trattamento ad alta velocità dei pacchetti, supportando al loro interno la programmazione multitrhead.
Il processore IXP1200 ha come caratteristica principale la possibilità di elaborare parallelamente i pacchetti. Tutti i microprocessori, infatti, possono operare in maniera concorrente in modo da raggiungere la massima efficienza.

2.3.2.2.2 Apparati di Rete

Come detto in precedenza, gli apparati di rete sono dei router/switch necessari all'instradamento dei pacchetti. Questi dispositivi, a seconda delle loro velocità di instradamento dei pacchetti, potrebbero comportare la formazione di Bottleneck-Bandwidth limitando la velocità massima di trasmissione della rete. Fortunatamente oggi tali dispositivi sono in grado di operare a velocità considerevoli e il problema dei Bottleneck-Bandwidth è dovuto ad altri fattori (ad esempio il passaggio da link veloci a link lenti).
Nell'analizzare gli apparati, che oggi caratterizzano il mondo delle reti ad alta velocità, verrà posta maggior attenzione su quelle che offrono di per sè strumenti per la gestione di rete.

Verranno studiate e specificate le caratteristiche dei dispositivi che:

- consentono di ripartire il traffico (*Traffic-Splitter*) fra più reti lente in modo da consentire l'impiego di tool di monitoraggio esistenti;
- mettono a disposizione la possibilità di selezionare un determinato tipo di traffico e ridirezionarlo su una specifica interfaccia (*Partial-Port-Mirror*).

TRAFFIC SPLITTER

L'analisi di una quantità di dati considerevole, come quella in transito su reti veloci, può essere effettuata ripartendo (*split*) il traffico fra più reti meno veloci. In seguito sarà analizzata un dispositivo che esegue lo split del traffico che può essere programmato dagli amministratori, usando determinate regole, per ripartire il traffico fra le reti da cui effettueranno l'analisi.

PARTIAL PORT MIRROR

La tecnologia, che consente di eseguire la ridirezione di alcuni specifici pacchetti in base a dei filtri su determinate interfacce del dispositivo, viene indicata col termine Partial-Port-Mirror. I dispositivi che supportano questo tipo di tecnologia sono, generalmente, switch o router. Questi consentono l'impiego dei protocolli di gestione standard visti nella specifica sezione,

tramite i quali gli amministratori hanno la possibilità di rilevare le informazioni da loro raccolte per poi programmarli per smistare il traffico su determinate porte.

TOP LAYER IDS Balancer

La TOP LAYER [28], industria produttrice di hardware, ha realizzato un componente che può essere impiegato per lo split del traffico di reti veloci. Questa device è in grado di ripetere il segnale, simultaneamente, fra quattro gruppi di lavoro collegati, ognuno, da tre linee.
L'IDS Balancer esegue lo split del traffico, attraverso la ripetizione dei pacchetti sulle interfacce in uscita, implementando delle politiche di ripartizione dettate dai gestori. In questo modo il traffico viene splittato a seconda delle caratteristiche dell'informazione che transita sulla rete. Si possono così differenziare le categorie di dati a seconda di specifiche caratteristiche determinate dagli amministratori.

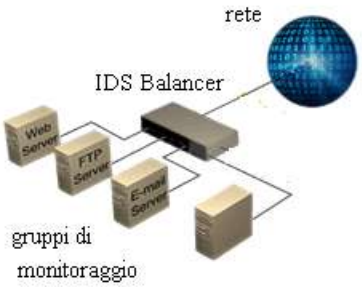


Fig. 13 Architettura TOP LAYER IDS-Balancer

JUNIPER M-Series

La Juniper [29], altra azienda che opera nel settore hardware, ha proposto sul mercato una nuova generazione di router denominata M-Series.
Questi router mettono a disposizione dei gestori di rete delle funzioni utili per ridirigere i pacchetti (mirror), con particolari caratteristiche, verso host da cui viene eseguita l'analisi del traffico.
Oltre alle caratteristiche sopra descritte, questi router, supportano l'implementazione di tool quali sFlow o NetFlow per l'analisi dei flussi in transito sulla rete.

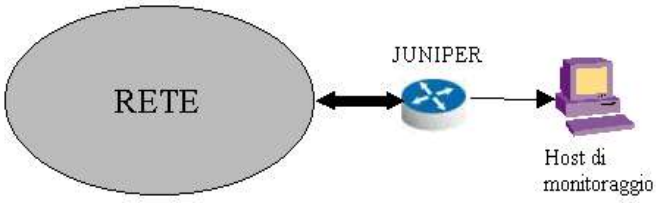


Fig. 14 Architettura JUNIPER M-Series

		CARATTERISTICHE								
		SW	**HW**	**Analisi dei Flussi**	**Cattura dei pacchetti**	**IDS**	**NIC**	**Device di sistema**	**Traffic Splitter**	**Partial Port Mirror**
TOOL	**SFlow**	●		●						
	NeTraMet	●		●						
	NetFlow	●		●						
	CFlowd	●		●						
	FlowScan	●		●						
	LIBPCAP	●			●					
	TCPDUMP	●			●					
	Ethereal	●			●					
	CoralReef	●		●	●					
	NTop	●		●	●	●				
	Snort	●				●				
	Dag card		●		●		●			
	Radysis ENP 2505/2506		●		●		●			
	Juniper		●	●				●		●
	IDS Balancer		●					●	●	

Tab. 4 Tabella riassuntiva delle caratteristiche dei tool passivi

3. Misurazioni su Reti ad Alta Velocità

Dopo aver specificato le caratteristiche degli strumenti di monitoraggio esistenti, sia hardware che software, concentriamo la nostra attenzione nel rapportare la tecnologia esistente alle nuove infrastrutture di rete ad alta velocità.
In questo capitolo daremo una dettagliata descrizione delle misurazioni utili per gestire reti molto veloci e dei problemi che nascono quando ci si appresta ad operare in questo campo. Verranno riportate delle considerazioni riguardo la conformità e l'efficacia dell'impiego dei tool e si cercherà di capire, dall'analisi fatta, quali sono i punti deboli dei suddetti strumenti.
Nel prossimo capitolo verrà proposta una soluzione che possa ovviare ai problemi rilevati nello studio dei diversi tool e sia adattabile alle moderne velocità trasmissive.

3.1 Descrizione del Problema

Col passaggio della tradizionale velocità media di trasmissione da 100 Mbit/s a velocità che oggi si orientano al Gbit/s e oltre, non tutti gli strumenti descritti nel capitolo precedente riescono a funzionare correttamente. I maggiori problemi riguardano la scalabilità dell'architettura sulla quale sono stati definiti e soprattutto l'elevata velocità delle reti odierne a cui molti tool non possono far fronte. Questo tipo di problematica caratterizza gli strumenti che effettuano monitoraggio passivo della rete. I tool attivi risentono meno dell'introduzione delle reti ad alta velocità, ma nonostante il possibile impiego, da soli non sono in grado di fornire tutte le misurazioni necessarie per eseguire il monitoraggio. I tool attivi infatti, nella maggior parte dei casi, ci offrono soltanto stime sulle condizioni della rete in un determinato momento, mentre ciò che interessa sono dei valori precisi. Per questo l'attenzione degli autori viene totalmente riposta nello studio di tool passivi per il monitoraggio di reti ad alta velocità.
Per fare un esempio delle difficoltà che si incontrano quando si passa ad una tecnologia che consente velocità trasmissive attorno al Gbit/s, viene descritto il caso particolare della cattura

dei pacchetti. Con questo metodo, per analizzare il traffico e vedere quindi ciò che passa realmente sulla rete, è necessario catturare i pacchetti tramite un dispositivo di interfacciamento alla rete stessa (vedi Cap. 2 Sez. 2.3.2.2.1) e trasmetterli al processore centrale attraverso il bus PCI. Con l'avvento delle reti ad alta velocità sono state progettate schede che possono raggiungere velocità di cattura pari a 2.5 Gbit/s. Nonostante la loro capacità computazionale, la grande quantità di informazioni inviate attraverso il bus PCI ne satura la banda causando la perdita di parte dell'informazione. Dalle ricerche effettuate [4] è emerso che la banda di 4 Gbit/s offerta dal bus PCI a 64bit, è utilizzata soltanto per il 40% (1.6 Gbit/s) per le comunicazioni tra le varie componenti interne al PC, mentre il restante 60% è speso per la gestione di tali comunicazioni (overhead di trasmissione). Tuttavia, anche se le schede riuscissero ad inviare tutti i dati, il processore centrale non sarebbe in grado di elaborare tutte le informazioni perché la sua potenza computazione è inferiore alla velocità trasmissiva della rete. Tecnicamente, mentre la potenza dei processori è aumentata di 10.000 volte dal 1975, raddoppiando ogni 18-24 mesi, la capacità di un singolo cavo di fibra ottica, nello stesso periodo, è aumentato di 1.000.000 di volte, raddoppiando ogni 12-16 mesi. Come mostra la figura 15, il punto di intersezione, si è verificato nel 1999, quando un singolo processore di allora non aveva abbastanza potenza computazionale per processare tutti i pacchetti catturati dalla rete. Tutto ciò è dovuto al fatto che le reti vengono costruite con tecnologie ottiche, mentre i processori continuano ad essere costruiti con tecnologie elettroniche, favorendo l'apertura della forbice (gap) tra la velocità del processore e la velocità della rete.

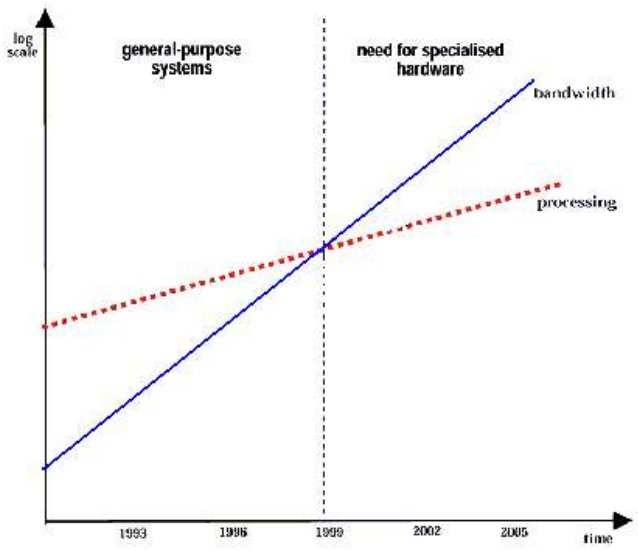


Fig. 15 confronto fra curve velocità di evoluzione reti/processori

3.2 Requisiti di Monitoraggio Esistenti

Per cercare una soluzione al problema del monitoraggio della nuova generazione di reti ad alta velocità, bisogna innanzitutto inquadrare i requisiti che caratterizzano il monitoraggio di reti a bassa velocità e capire come stanno evolvendo per adattarsi alle nuove velocità trasmissive.

I campi di applicazione definiti fino ad oggi sono:

- Analisi delle Caratteristiche dei Flussi;
- Ingegnerizzazione della rete;
- Sicurezza;
- Accounting;
- Rilevazioni di Errori.

Analisi delle Caratteristiche dei Flussi

Un punto chiave della rete Internet è la sua eterogeneità: è caratterizzata da un grande numero di reti basate su differenti tecnologie trasmissive ed è condivisa da un'enorme varietà di applicazioni che cambiano ed aumentano nel tempo. È importante determinare nel nostro progetto, sia quantitativamente che qualitativamente, come le caratteristiche dei flussi di rete (es. traffico WWW) siano alterate al verificarsi di alcune situazioni, ad esempio passaggio da link lenti a link veloci. Per far ciò è necessario collezionare e correlare misurazioni di traffico da più punti e solo così si riesce a capire come il comportamento e i requisiti di questi flussi cambino nel tempo. Per questo il monitoraggio di rete passivo è fondamentale per capire quali applicazioni usano Internet e in che modo.

Ingegnerizzazione della Rete

Per garantire la corretta erogazione dei servizi richiesti è necessario ingegnerizzare la rete. Ciò significa, ad esempio, studiare il traffico in transito per cercarne una ripartizione ottimizzata fra i vari dispositivi, al fine di aumentarne le performance.
Per raggiungere questi risultati, è utile analizzare le informazioni ricavate dal monitoraggio del comportamento degli utenti (rispetto a degli SLA), e di quello della rete (se rispetta i parametri strutturali, ad esempio il bandwidth). Inoltre, tali informazioni sono utili agli ISP che possono capire se è necessario aumentare la banda o intervenire in altro modo per offrire un servizio più qualificato. Ad esempio introducendo dei nuovi router o aggiornando il media per consentire una maggior velocità di trasmissione.

Sicurezza

Un aspetto fondamentale della gestione di rete è quello relativo alla sicurezza. Le misurazioni che vengono fatte sul traffico reale sono di prezioso aiuto agli amministratori per capire se sono in corso attacchi alla rete monitorata.
La propensione dei gestori di una rete a garantirne la sicurezza, e l'implementazione di sistemi sofisticati per la prevenzione di attacchi, può però generare l'effetto contrario a quello desiderato. È possibile, ad esempio, che si implementino sistemi per prevenire attacchi che interessano pacchetti ICMP. Catturando tutto questo tipo di traffico in una rete ad alta velocità è molto probabile che si esaurisca la potenza computazionale degli strumenti

utilizzati dagli amministratori, senza ottenere informazioni significative. Nel contempo è possibile che sia in corso un altro tipo di attacco, che non interessa pacchetti ICMP, che rimane oscuro perché non si hanno risorse sufficienti ad identificarlo e neutralizzarlo.
È necessario a questo scopo introdurre dei filtri che consentano la cattura di quei pacchetti con caratteristiche specificate dai gestori (vedi Cap.2 Sez. 2.3.2.1.4), e impediscano la cattura di tutti gli altri. A questo punto si presenta agli amministratori un altro tipo di problema: identificare le misurazioni che si intendono effettuare e implementare nelle sonde le politiche che consentano di catturare il traffico da cui ricavare le informazioni desiderate.

Accounting

I dati di accounting definiscono ad esempio:

- il volume di traffico prodotto da ogni utente;
- il controllo dell'allocazione della banda a disposizione;
- la ripartizione dei costi fra gli utilizzatori (*Billing*).

Vi sono vari tool che consentono l'identificazione delle fonti di traffico, della banda occupata da un utente e di tutte quelle informazioni utili ad un ISP per la gestione efficiente della risorsa di sua competenza (ad esempio sFlow).

Rilevazione di Errori

Sempre attraverso l'analisi del traffico reale si possono ricavare delle informazioni sullo stato della rete. Questi dati consentono di individuare problemi che degradano la performance, la cui determinazione è tutt'altro che semplice.
Questi problemi della rete possono essere raggruppati in due diverse categorie:

1. *Evidenti*, cioè riconoscibili non appena si manifestano;
2. *Non-Evidenti*, cioè riconoscibili soltanto con un'accurata analisi.

Della prima categoria fanno parte generalmente gli errori:

- Fisici, cioè quelli che non consentono la connessione fra uno più nodi a causa di guasti lungo la linea (fault).

- Strutturali, cioè quelli determinati da una progettazione sbagliata della rete (esclusione di un nodo).

Gli errori non-evidenti, la cui rilevazione è di gran lunga più interessante, richiedono un lavoro ingegnoso e originale per determinarne la presenza. Questi problemi hanno la caratteristica di essere oscuri in quanto la rete continua a "funzionare" ma in maniera non corretta. Sono possibili cioè tutti i collegamenti e tutti gli utenti possono utilizzare il mezzo trasmissivo, ma la performance della rete è di gran lunga inferiore al valore della bandwidth.
L'intervento da parte degli amministratori deve essere orientato, ad esempio, nel capire se sono presenti dei colli di bottiglia fra i dispositivi. In particolare, i bottleneck, comportano la creazione di code di attesa all'interno dei router che sono costretti a memorizzare i pacchetti in apposite aree. Nel momento in cui lo spazio di memoria viene esaurito i pacchetti in arrivo vengono eliminati. Le applicazioni, per questo motivo, sono costrette a generarne di nuovi per eseguire correttamente la comunicazione e questo degrada la performance di rete.

3.3 Nuovi Requisiti di Monitoraggio di Rete

Oltre ai requisiti base descritti nella sezione precedente, è necessario introdurne altri più specifici per il monitoraggio di reti ad alta velocità.
Per la definizione di tali esigenze si devono dapprima individuare i vari aspetti che caratterizzano il problema proposto. Si devono quindi identificare i requisiti:

- Hardware;
- Software.

Dal punto di vista dell'hardware gli autori si sono orientati verso scelte architetturali che consentano l'utilizzo di dispositivi standard (ad esempio un PC), cioè macchine non dedicate

e facilmente reperibili sul mercato (commodity hardware), sia dal punto di vista tecnologico sia da quello economico.
Inoltre è necessario che i supporti impiegati dispongano di un'ampia capacità di memorizzazione in quanto aumentando il traffico in transito sulle reti, a causa dell'aumento della velocità trasmissiva, le informazioni di monitoraggio da archiviare crescono proporzionalmente.
L'hardware impiegato deve ovviamente garantire, oltre alle caratteristiche appena descritte, il supporto di velocità di trasmissione di almeno 10 Gbit/s.
Per requisiti software si intendono quelle necessità che devono essere soddisfatte dai tool impiegati per il monitoraggio di reti ad alta velocità.
Questi possono essere suddivisi in due aree:

- Cattura dei pacchetti;
- Analisi dei dati.

Come detto in precedenza la cattura dei pacchetti è fondamentale per riuscire a ricavare informazioni sul traffico in transito sulla rete.
Per quest'area sono definiti dei requisiti specifici, quali:

- Riconoscimento dei vari protocolli di comunicazione (TCP/IP, UDP, ecc.);
- Supporto dei protocolli trasmissivi di nuova generazione (MPLS, IPv6, ecc.);
- Capacità di identificazione di ogni attributo che caratterizza i pacchetti;

È fondamentale poter classificare i pacchetti che transitano sulla rete e, a questo scopo, poter individuare ogni loro caratteristica. Per questo è necessario che durante la cattura del traffico, gli strumenti adoperati consentano il riconoscimento dei più diffusi protocolli di comunicazione. Inoltre, trattando questi studi di reti tecnologicamente avanzate, è necessario poter riconoscere i protocolli di nuova generazione di cui si prevede larga diffusione. È importante anche l'identificazione di ogni campo che caratterizza l'header dei pacchetti consente di individuare eventuali attacchi alla rete (ad esempio SYN Flood[8]).

L'altra area che identifica i requisiti necessari per il monitoraggio di reti ad alta velocità è quella che riguarda l'analisi delle informazioni raccolte.
I requisiti base per l'analisi dei dati sono:

[8] Questo tipo di attacco consiste nell'invio di molti pacchetti per la richiesta di apertura di connessioni TCP ad un server. Tali pacchetti vengono contrassegnati dal valore 1 del campo Syn nell'header IP.

- Identificazione dei flussi in transito sulla rete;
- Aggregazione delle informazioni;
- Collezionamento dei dati;
- Analisi dei dati;
- Reporting delle analisi effettuate.

L'identificazione dei flussi avviene confrontando gli attributi dei pacchetti con dei filtri definiti dagli amministratori di rete (vedi Cap.2 Sez. 2.3.2.1.1). Una volta raccolti, i dati identificativi di ogni flusso devono essere aggregati a seconda delle specifiche.
Il collezionamento dei dati è fondamentale per rendere disponibili alle applicazioni di analisi le informazioni raccolte. Inoltre in questo modo si dispone di una memoria storica, che descrive l'utilizzo della rete nel tempo, necessaria per effettuare delle previsioni sullo sviluppo dei vari servizi.
L'analisi delle informazioni deve essere implementata in base al tipo di servizio che viene erogato, dovranno essere effettuate delle analisi per garantire:

- la rilevazione di errori;
- l'accounting;
- la performance della rete;
- la rilevazione di errori di configurazione dei dispositivi;
- la sicurezza della struttura.

Infine è necessario rendere le informazioni accessibili ai gestori della rete. Queste dovranno essere organizzate in modo che risulti facile la lettura e l'interpretazione del loro significato.

3.4 Strumenti Adeguati al Problema

Una volta enunciati i requisiti per il monitoraggio di reti ad alta velocità verranno analizzati gli strumenti le cui caratteristiche meglio si adeguano alle esigenze soprascritte.
Come visto nel capitolo precedente è necessario distinguere gli strumenti software da quelli hardware.

3.4.1 Hardware

Nel caso di cattura del traffico di reti veloci, i supporti ritenuti più adeguati agli scopi sono quelli identificati dagli apparati di rete ed in particolare il router della Juniper (vedi Cap. 2 Sez. 2.3.2.2.2).
Di seguito verrà riportata un'analisi delle caratteristiche di tale router confrontata con i requisiti definiti.

JUNIPER

Analizzando le caratteristiche del Juniper (vedi Fig. 16) sono emerse delle assonanze con i requisiti definiti dalla tesi.
Per prima cosa il Juniper rientra nella categoria del commodity hardware perché è facilmente reperibile e non ha costi proibitivi come un dispositivo hardware dedicato (vedi sonde RMON).
Per quanto riguarda le caratteristiche tecniche, questo dispositivo consente l'interfacciamento con diversi tipi di link.
Grazie alla presenza di moduli aggiuntivi chiamati PIC (Physical Interface Card) il router supporta fino a quattro delle seguenti tecnologie:

- ATM OC-3 (multimode) e OC-12 (single mode);
- DS3;
- E1;
- E3;
- Fast Ethernet;
- Gigabit Ethernet;
- SONET/SDH OC-3 (multimode e single mode), OC-12 (single mode), e OC-48 SR;
- T1;
- Tunnel.

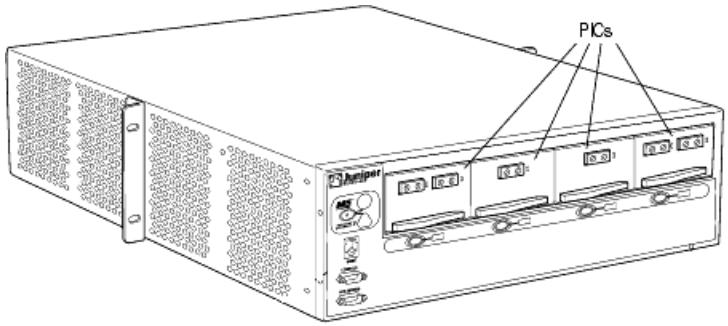


Fig.16 Vista frontale del router.

Inoltre è in grado di gestire vari protocolli di comunicazione quali:

- Protocolli di routing unicast e multicast,
  cioè quei protocolli che consentono al router di instradare i pacchetti unicast (un mittente-un destinatario) e multicast (un mittente-molti destinatari) nel miglior modo possibile, e a sua volta di gestire le affiliazioni ai gruppi multicast.
- Protocolli di ingegnerizzazione del traffico,
  cioè quei protocolli che, implementando le scelte degli amministratori, instradano il pacchetto a seconda di determinate caratteristiche che si discostano dai risultati degli algoritmi di routing (MPLS).

Una delle caratteristiche più importanti del router è la possibilità di effettuare il mirror, su alcune porte, del traffico desiderato (con o senza l'uso di appositi filtri applicati ai pacchetti in transito). Inoltre il dispositivo può effettuare il mirror fra porte che si interfacciano con due tipi di media distinti. Per esempio, se la porta di input è basata su ATM e la porta di output è di tipo Ethernet, il Juniper estrarrà i pacchetti IP-over-ATM dall'input e li trasmetterà all'output nel formato appropriato.
Tra le funzionalità che il router mette a disposizione vi è anche quella di poter effettuare un mirror parziale del traffico (per esempio soltanto il 10%). Questo può essere sfruttato per avere una visione generale di ciò che succede nella rete.

Inoltre il Juniper è in grado di:

- supportare dei tool per l'analisi dei flussi (ad esempio NetFlow[14], sFlow [19], ecc.);
- essere programmato dagli amministratori che possono lanciare programmi direttamente sul router;

In conclusione le caratteristiche del router più compatibili con i requisiti richiesti sono da riassumere nel supporto di:

1. Tipi di protocolli dei link quali PoS, ATM e Fast Ethernet;
2. I protocolli di rete come MPLS, IPv6 e IP tunnelling;
3. Velocità di instradamento di circa 6.4 Gbit/s;
4. Analisi di flussi e sampling dei pacchetti;
5. Mirror del traffico.

3.4.2 Software

Alla luce dei requisiti definiti per il monitoraggio di reti ad alta velocità, dei campi di applicazione e dei tool analizzati nel capitolo precedente, in questa sezione vengono descritte le affinità dei seguenti tool col problema da affrontare:

- NetFlow
- sFlow
- Snort
- Ntop

Gli autori hanno orientato le loro scelte verso questi tool perché, pur non soddisfacendo completamente alcuni requisiti (ad esempio solo Ntop e Snort supportano la cattura dei pacchetti), implementano delle funzioni di analisi necessarie per il monitoraggio di reti ad alta velocità.

NetFlow

NetFlow (vedi Cap. 2 Sez. 2.3.2.1.1) è un'architettura di monitoraggio prodotta dalla Cisco [30] per i suoi router, ma è diventata uno standard supportato anche da altre aziende come la Juniper.

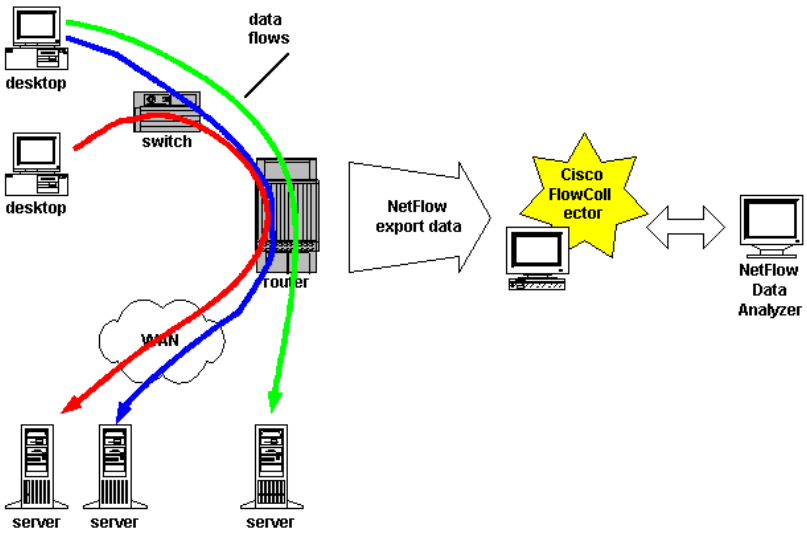


Fig. 17 Architettura NetFlow

Grazie ai suoi tre componenti precedentemente descritti (vedi figura 17), questo tool mette a disposizione funzioni per:

- L'identificazione ed aggregazione dei flussi;
- Il collezionamento dei dati;
- L'analisi e il reporting dei dati;

Le sue funzionalità lo rendono per certi aspetti conforme alle esigenze di questa tesi. Tramite il suo impiego è infatti possibile ricavare dati per:

- Accounting e Billing:
- Pianificazione di rete;
- Ingegnerizzazione del traffico;
- Monitoraggio delle applicazioni e degli utenti.

Ciò nonostante il suo utilizzo è confinato a reti dalla velocità contenuta. Il procedimento di identificazione ed aggregazione dei flussi, implementato all'interno dei router, non è ottimizzato per le reti veloci. Il software infatti, per le sue specifiche, non è adatto per velocità maggiori di 40 Mbit/s. Se impiegato per reti con velocità più elevate causa la perdita di informazioni di flusso, in quanto non riesce ad elaborare tutti i pacchetti. Tuttavia le operazioni di instradamento eseguite dal router non risentono dell'inefficienza di questo tool.
Tali lacune, già note agli amministratori di reti ad alta velocità, ne impediscono l'utilizzo a meno di modifiche sostanziali al componente che esegue l'identificazione e l'aggregazione dei flussi (Flow Caching).
Accanto al NetFlow, è possibile utilizzare due tool già descritti come il cFlowd, che funziona da Flow Collector, e il FlowScan per l'analisi e il reporting dei dati ricavati con NetFlow.

sFlow

La tecnologia sFlow applica un metodo diverso dal NetFlow per collezionare informazioni dal traffico in transito sulla rete. Pur rientrando nella categoria dei tool che eseguono l'analisi dei flussi, la tecnologia su cui si basa è quella del sampling (vedi Cap. 2 Sez. 2.3.2.1.1), cioè campionamento dei pacchetti.
Tale tecnologia rende il tool dinamico e adattabile agli obiettivi di questa tesi. L'impiego di sFlow infatti non presenta il problema della perdita di informazione descritto per il NetFlow

in quanto i pacchetti analizzati non rappresentano la totalità del traffico, ma soltanto un suo campione.
Il sampling si basa su alcune funzioni statistiche che vengono applicate al campione di dati raccolto. Il tool, generalmente, viene configurato in modo da catturare un pacchetto ogni quattrocento in transito dal dispositivo (1/400). Questa proporzione però può variare a seconda delle esigenze degli amministratori, i quali possono ottenere misure più o meno precise. Ad esempio se si raccolgono 1/200 dei pacchetti, le misure ottenute saranno sicuramente più accurate rispetto ad un campione derivato dalla raccolta di un pacchetto su 400.
La figura 18 mostra come viene implementata la tecnologia di sampling sFlow all'interno degli apparati di rete. La prima parte prevede l'inizializzazione delle variabili, necessaria per impostare:

- Il tasso di campionamento,
  nell'esempio la variabile campione viene settata a 400 come nella configurazione di default (1/400).
- Il numero di pacchetti campionati e il numero di pacchetti totali,
  questi valori sono impostati a zero in quanto il campionamento non ha ancora avuto inizio.

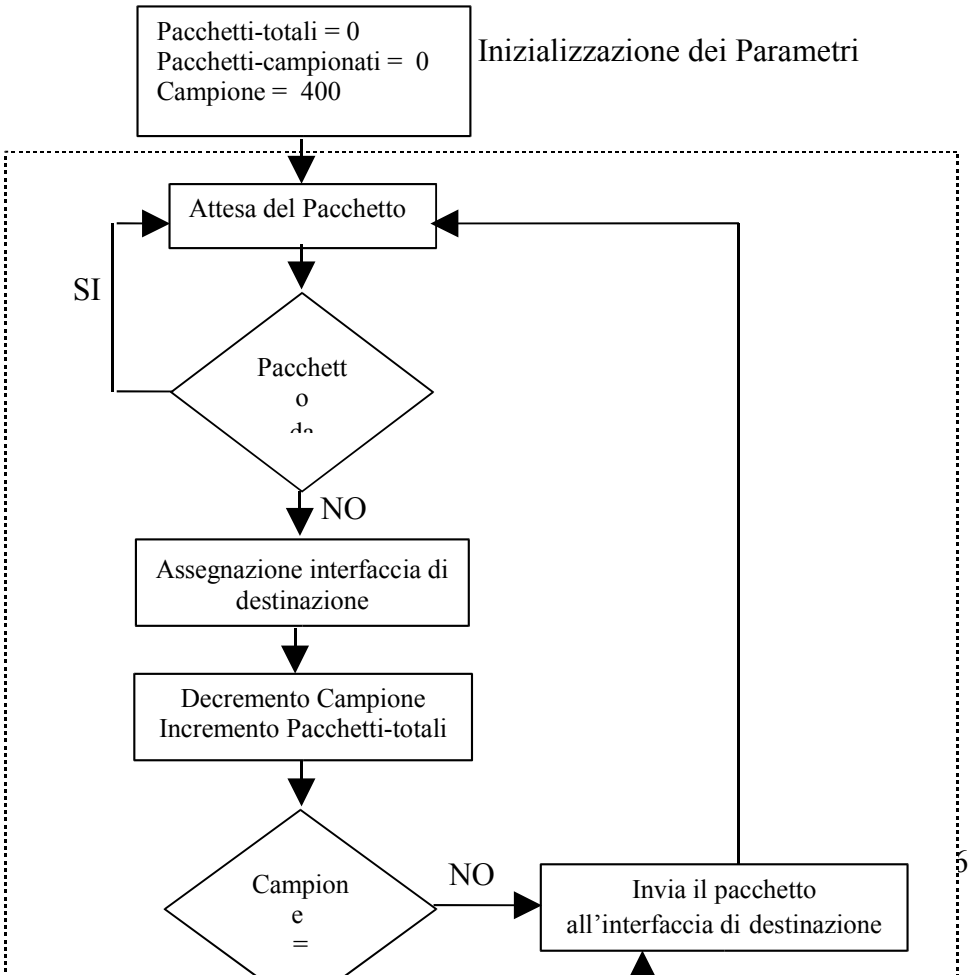
Nella seconda fase viene implementato il ciclo di sampling vero e proprio e viene previsto l'invio all'agent delle informazioni di flusso necessarie per l'analisi.
Le informazioni pervenute all'agent attraverso il meccanismo appena descritto vengono poi combinate con i dati campionanti dai contatori posti sulle interfacce dei vari router.
Una delle caratteristiche di sFlow consiste nel fatto che il meccanismo di sampling può essere implementato direttamente da dispositivi hardware. Questo rende le operazioni più veloci in quanto eseguite da strumenti dedicati. Inoltre, tali strumenti, vengono supportati da molti router commerciali.

Le caratteristiche che hanno spinto gli autori a considerare sFlow come tool impiegabile per le misurazioni di traffico su reti ad alta velocità si possono quindi riassumere in:

1. Bassi costi,
   di fatto la tecnologia sFlow non comporta costi di approvvigionamento e manutenzione eccessivamente elevati.
2. Requisiti minimi,

il tool non necessita né di una elevata potenza computazionale né di ampia capacità di memoria.

3. Implementazione in molti dispositivi,
   molte case produttrici di apparati di rete progettano i loro prodotti fornendo dei supporti hardware per sFlow.
4. Performance,
   è testato per monitorare più reti ad alta velocità senza intaccare le performance dei router di supporto.
5. Scalabilità,
   l'introduzione di nuovi router nella rete non comporta un cambiamento radicale della sua struttura ma soltanto un aggiornamento, in quanto sFlow è in grado di monitorare fino a 10.000 dispositivi.



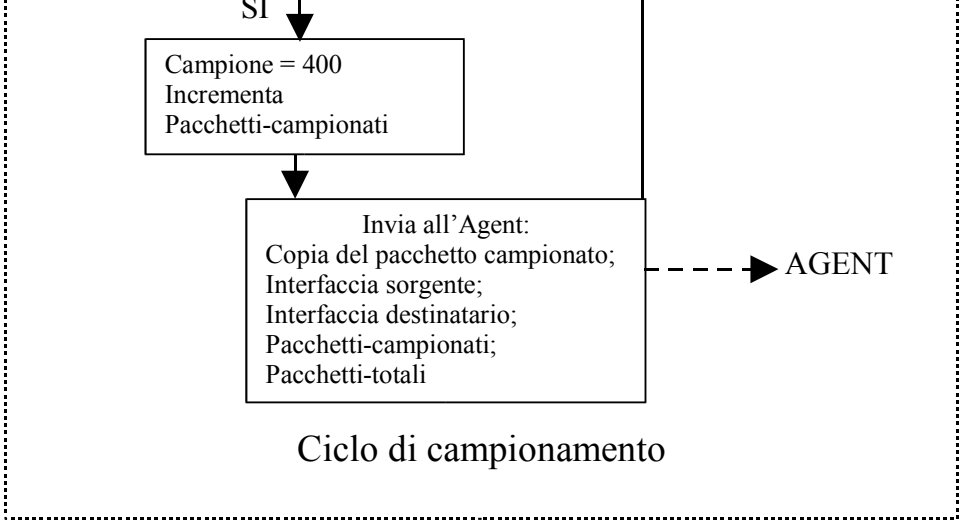


Fig. 18 Descrizione del ciclo di campionamento dei pacchetti.

Nonostante la sua grande versatilità sFlow presenta dei problemi che riguardano il suo utilizzo in determinati ambiti quali:

- Identificazione di eventi specifici o anomali;
- Rilevazioni di misurazioni con un alto grado di precisione.

Il meccanismo di sampling di fatto non è adatto per garantire la sicurezza della rete, proprio perché non è possibile, catturando solo una porzione di traffico, individuare eventi specifici che possono compromettere la stabilità della rete stessa.
Altro aspetto negativo che caratterizza sFlow è dato dal fatto che, campionando il traffico, si ottengono delle misure che rappresentano delle stime dei valori reali. Se si desiderano dei valori più precisi è necessario ampliare il campione dei dati raccolti e questo ripresenta il problema sollevato per il NetFlow, cioè l'impossibilità del suo impiego per reti ad alta velocità.

NTOP

Ntop, fra i tool presi in considerazione in questo capitolo, è l'unico che unisce la possibilità di catturare il traffico con la capacità di analisi dei flussi (vedi Cap.2 Sez. 2.3.2.1.3). Questo perché il tool si basa su Libpcap e a sua volta supporta sia sFlow che NetFlow.
Mentre la libreria per la cattura dei pacchetti viene implementata direttamente da Ntop, gli strumenti per l'analisi dei flussi sono dei plugins che consentono al tool di ricevere ed elaborare le informazioni inviate da sFlow o NetFlow. Di fatto, questi tool sono implementati dagli apparati di rete che generano e inviano i pacchetti contenenti le informazioni sui flussi, mentre Ntop esegue la raccolta di tali pacchetti e la loro elaborazione.
Queste caratteristiche rendono Ntop dinamico e adattabile a molte architetture di rete. Tramite l'impiego di questo tool si riescono a ricavare misurazioni di traffico a vari livelli di specificità:

- Accurate,
  la cattura diretta dei pacchetti dalla rete fa sì che le informazioni ricavate descrivano in maniera specifica l'utilizzo della rete. Tali informazioni sono utili nei seguenti campi di applicazione:
    - Sicurezza;
    - Rilevazione di errori.

- Generali,
  i plugins per sFlow e NetFlow consentono di ricavare informazioni più generali sullo stato della rete che possono essere usate per:
    - L'accounting;
    - L'ingegnerizzazione della rete;
    - L'analisi delle caratteristiche dei flussi.

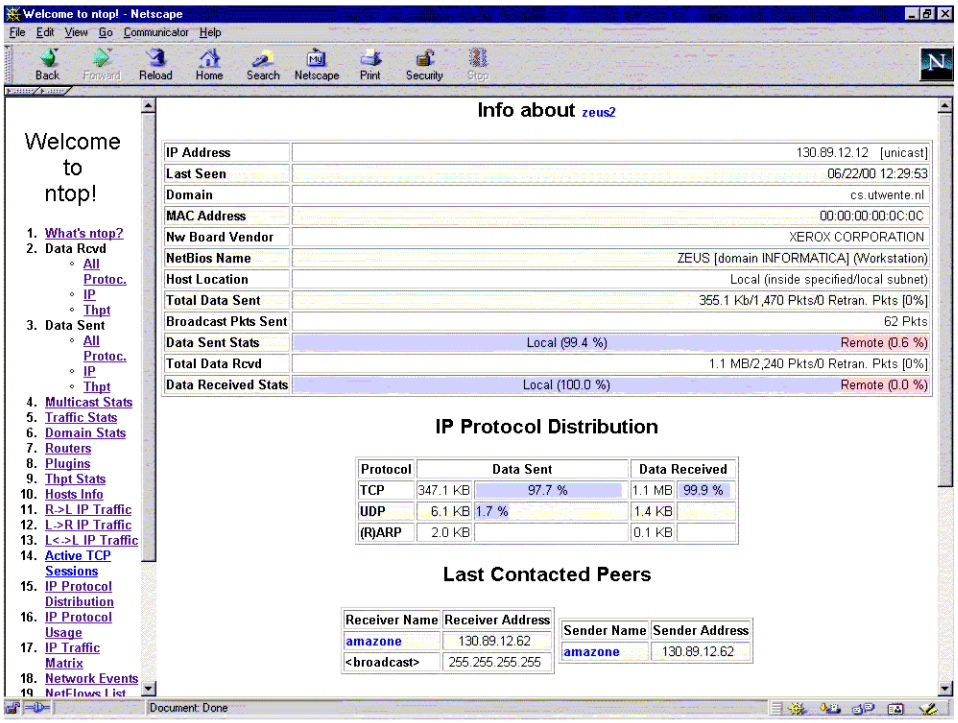


Fig. 19 Screenshot di Ntop

Altre caratteristiche di Ntop sono:

- Licenza GPL,

  questo garantisce la facile ed economica distribuzione del tool.
- Facilità d'uso,

  ntop incorpora un server http che permette di accedere ai dati di monitoring da lui analizzati attraverso un web browser (fig. 19).
- Utilizzo di commodity hardware,

  il tool viene installato su PC standard.
- Requisiti hardware minimi,

  il tool utilizza solo il 10% della CPU (Pentium III [32]) e 10 MB di memoria.

I problemi che ntop presenta al momento del suo impiego in reti ad alta velocità sono legati all'utilizzo della libreria libpcap. Da un lato questa libreria ovvia ai problemi presentati da sFlow e NetFlow, in quanto vengono ottenute le misure specifiche analizzando i pacchetti catturati dalla rete. D'altra parte si ripropongono i problemi legati alla tecnologia con cui vengono progettati i bus di comunicazione fra le normali schede di rete e il processore centrale del PC di installazione del tool (vedi Cap. 3 Sez. 3.1).

SNORT

Snort è un IDS le cui caratteristiche sono in parte conformi ai requisiti dettati dalla tesi, in modo particolare per quanto concerne la sicurezza. Questo tool si basa, per la rilevazione dei pacchetti sospetti, su alcune regole che possono essere definite dall'amministratore di rete. In generale le fasi di utilizzo dello Snort possono essere così sintetizzate:

1. Definizione delle caratteristiche degli attacchi di rete conosciuti;
2. Descrizione delle regole da applicare ai pacchetti catturati;
3. Applicazione del sistema.

La prima fase è necessaria per identificare i possibili attacchi a cui la rete monitorata potrebbe essere soggetta. Questo implica uno studio, da parte degli amministratori, atto a delineare una serie di casistiche che devono essere considerate per garantire la sicurezza della rete.
Sulla base di tali studi devono essere definite, nel linguaggio appropriato, le regole che dovranno essere applicate, dal tool stesso, ad ogni pacchetto catturato.
Una volta che le prime due fasi sono state completate è possibile avviare lo Snort (vedi Cap2. Sez. 2.3.2.1.4).

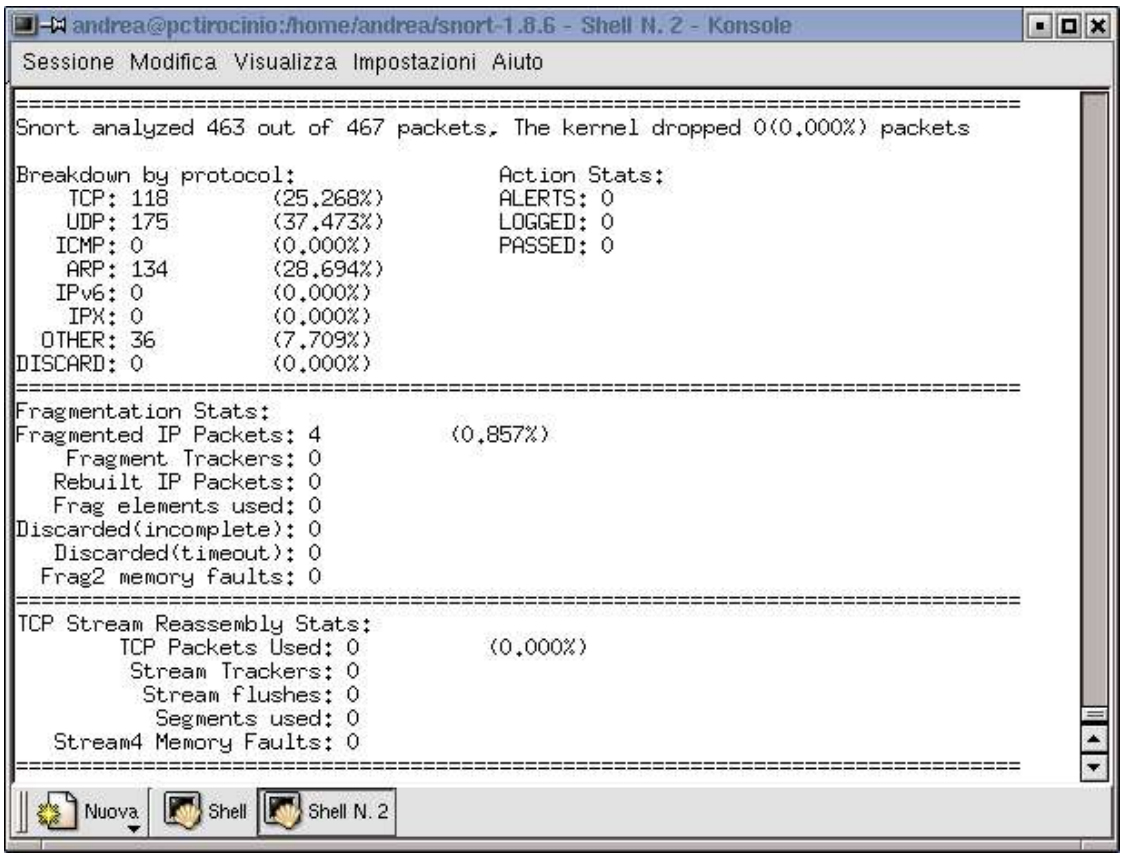


Fig. 20 Screenshot di Snort.

L'impiego dello Snort nel monitoraggio di reti ad alta velocità presenta i problemi derivanti dall'utilizzo della libreria Libpcap, sulla quale è basato il sistema, riguardanti la velocità massima di cattura dei pacchetti (400 Mbit/s). Tuttavia gli autori hanno ritenuto importante inserire lo Snort fra i tool affini agli obiettivi della tesi, in quanto consente la definizione, in modo dinamico, di regole per la sicurezza della rete che possono essere implementate all'interno di alcuni router (ad esempio il Juniper).

3.5 Strumenti Inadeguati al Problema

Di seguito vengono riportati gli strumenti, sia hardware che software, che gli autori non hanno ritenuto adatti per una valida proposta al problema del monitoraggio di reti ad alta velocità, con relative motivazioni.

3.5.1 Hardware

Gli strumenti hardware che non sono stati presi in considerazione per la risoluzione del problema sono:

- NIC con NPU;
- IDS Balancer.

Le NIC (vedi Cap. 2 Sez. 2.3.2.2.1) non offrono la scalabilità del servizio di monitoraggio. Di fatto l'utilizzo di particolari schede inserite in macchine standard (quali ad esempio un PC), non permette l'aggiornamento del sistema a meno di un cambiamento radicale dei supporti

utilizzati. Anche se infatti si riuscisse a progettare una NIC per la cattura del traffico alla velocità di 10 Gbit/s, conoscendo il trend di sviluppo delle tecnologie trasmissive (vedi figura 15), entro poco tempo risulterebbe obsoleta. Inoltre, è sconsigliato l'utilizzo di tali schede su commodity hardware per la presenza su questi ultimi di problemi ancora da risolvere (limitata banda del bus).

Per quanto concerne l'IDS Balancer (vedi Cap. 2 Sez. 2.3.2.2.2) si è ritenuto questo strumento non adatto al monitoraggio di reti ad alta velocità. Questo in quanto, pur applicando lo split del traffico con conseguente riduzione del volume di dati, non è in grado di supportare nessun software di analisi (ad esempio sFlow/NetFlow).

3.5.2 Software

TcpDump/CoralReef/Ethereal

Questi tool eseguono principalmente la cattura dei pacchetti e si basano sull'utilizzo della libreria Libpcap. Il loro impiego per il monitoraggio di reti ad alta velocità è sconsigliato perché questa libreria ha una velocità di cattura limitata a 400 Mbit/s.
Questo perché la Libpcap viene implementata dal nucleo del sistema operativo ospite; di conseguenza i pacchetti catturati devono essere trasmessi fra vari livelli prima di poter giungere alle applicazioni di analisi. I punti critici sono identificati nel passaggio da:

1 Dispositivo di interfacciamento alla rete-host di analisi;
   questo per le limitazioni del bus PCI già descritte.
2 Nucleo del sistema operativo-Applicazioni di analisi;
   anche se le comunicazioni fra sistema operativo e applicazioni avvengono velocemente non raggiungono le prestazioni delle reti odierne.

Questi motivi rendono inefficiente la libreria Libpcap quando si tratta di monitorare reti la cui velocità trasmissiva è superiore al Gbit/s.

RTFM

Nel precedente capitolo (Sez. 2.3.2.1.1) è stata descritta un'implementazione del Realtime Traffic Flow Measurement, NeTraMet. In questo paragrafo verranno enunciate le sue caratteristiche positive e negative che, in parte, la rendono conforme agli obiettivi preposti.
Pregi dell'architettura RTFM:

- Scalabilità,
  è possibile aggiungere componenti dell'architettura senza compromettere le performance della rete.
- Riduzione del traffico di management,
  data la vicinanza fra i componenti.
- Riduzione del traffico dati,
  grazie ad una elaborazione nei componenti intermedi delle informazioni, viene ridotta la mole di dati da inviare agli alti livelli.

Tuttavia uno dei problemi da affrontare riguarda il grado di granularità dei flussi. RTFM infatti definisce delle "accountable entity", cioè dei soggetti responsabili della produzione di traffico (un host , una sottorete ecc.). In questo modo si definiscono anche dei livelli che identificano la granularità delle informazioni raccolte. Di fatto, i flussi generati da un host, saranno molto più specifici dei flussi provenienti da una sottorete. Ciò, correlato al monitoraggio di reti ad alta velocità, implica l'impiego dell'architettura RTFM soltanto per la determinazione di flussi da cui è possibile ricavare informazioni generali e non di quelli che consentono un'analisi specifica. La raccolta di dati di flusso generati da un host è infatti un'operazione molto costosa in termini di risorse dei dispositivi, i quali, non consentendo l'elaborazione di tutti i dati data la velocità della rete, causano la perdita di informazioni.
Questi motivi, uniti alla difficoltà di gestione dell'architettura, portano gli autori a scartare questa soluzione, e a cercarne delle altre più compatibili con le scelte hardware fatte (Juniper).

3.6 Considerazioni

Dall'analisi effettuata in questo capitolo sono emersi dei problemi aventi la stessa natura e che, in modo diverso, riguardano tutti i tool:

- Granularità delle informazioni;
- Cattura/analisi dei pacchetti.

Di fatto i tool che eseguono l'analisi dei flussi (NetFlow/sFlow) forniscono delle misurazioni che descrivono lo stato generale della rete. Tali misurazioni sono poco utili se gli amministratori desiderano delle misure accurate che descrivono eventi specifici e di contro, se questi tool vengono impiegati per effettuare misurazioni accurate, si rivelano inefficaci ed inadatti per l'impiego in reti ad elevata velocità trasmissiva.

Per quello che riguarda i tool che eseguono la cattura dei pacchetti direttamente dalla rete (Ntop), e contestualmente la loro analisi, questi si rivelano inadatti ad elevate velocità trasmissive in quanto la potenza computazionale richiesta non è tecnologicamente implementabile. Anche se le misure ricavate dal loro impiego descrivono minuziosamente ogni evento verificatosi, la percentuale di informazioni che non riescono ad essere elaborate, e che quindi viene persa, è insostenibile per un corretto monitoraggio della rete.

● Interamente Supportato ◖ Parzialmente Supportato	TOOL				
	NetFlow	sFlow	Ntop	Snort	Juniper

REQUISITI	Software	●	●	●	●	
	Hardware		◖			●
	Analisi dei Flussi	●	●	●		
	Cattura dei Pacchetti			●	●	
	Sampling		●			
	Sicurezza			●	●	
	Rilevazione di errori	◖		●	◖	
	Mirror					●
	Ingegnerizzazione della rete	●	●	●		
	Accounting	●	●			

Tab. 5 Tabella riassuntiva delle caratteristiche degli strumenti affini agli obiettivi della tesi.

4. Un'Architettura per il Monitoraggio di Rete

In questo capitolo viene proposta un'architettura in grado di soddisfare i requisiti identificati in precedenza e di risolvere il problema del monitoraggio di reti ad alta velocità. Viene inoltre

specificato come i tool, scelti nel capitolo precedente, possano essere impiegati al fine di raggiungere gli obiettivi preposti.

4.1 Considerazioni iniziali

Le analisi effettuate nei capitoli precedenti hanno orientato le scelte degli autori verso una combinazione di tecniche passive di monitoraggio. Tale combinazione consente di ricondurre la soluzione del problema del monitoraggio di reti ad alta velocità alle soluzioni che oggi vengono implementate per il monitoraggio di reti lente.

Di fatto il monitoraggio passivo di una rete, caratterizzata da una bassa velocità trasmissiva, avviene scansionando l'intero volume di traffico in transito. Questo, ad esempio, garantisce la sicurezza della rete in quanto, analizzando ogni pacchetto, è semplice rilevare attacchi e situazioni pericolose. In questo scenario la condizione fondamentale, affinché i tool impiegati forniscano informazioni attendibili per la gestione della rete stessa, è costituita dalla possibilità di analizzare l'intero traffico.

Oggi con l'impiego di reti ad alta velocità la condizione che rendeva efficiente il monitoraggio passivo viene a mancare. Di fatto, come descritto nel capitolo 3, non è più possibile analizzare tutti i pacchetti in transito, in quanto la velocità trasmissiva della rete è di gran lunga superiore alla velocità degli strumenti impiegati per la scansione dei pacchetti. Questo fa si che le informazioni ricavate utilizzando dei tool passivi siano inattendibili perché la perdita di informazioni dovuta alla velocità trasmissiva è eccessiva. Di conseguenza, tali misurazioni, sono inutili ai fini della gestione di rete.

Per le proprietà del monitoraggio passivo, ad esempio la trasparenza nei confronti del traffico di rete, gli autori hanno proposto una soluzione che consenta il ripristino della condizione fondamentale che rende queste tecniche efficaci, e consente l'impiego di soluzioni di monitoraggio esistenti. Tale condizione è garantita dall'architettura descritta in seguito, che consente di operare una riduzione del traffico da analizzare in modo che le informazioni ricavate con i tool passivi conosciuti siano attendibili.

Il meccanismo proposto per eseguire una riduzione del traffico, che offre un compromesso accettabile fra volume di dati da analizzare e accuratezza delle informazioni raccolte, è quello basato sull'analisi di un campione di pacchetti in transito sulla rete (packet sampling). Tale tecnica deriva dallo studio di sFlow. Questo tool consente di ricavare delle informazioni significative, ai fini della gestione di rete, analizzando soltanto un campione dei dati al quale viene applicato un modello statistico.

La soluzione proposta deve inoltre essere compatibile con le piattaforme per il monitoraggio di rete esistenti, come ad esempio HPOpenView [7], date le funzionalità messe a disposizione e la loro diffusione. Queste piattaforme sono inoltre caratterizzate dall'integrazione di varie applicazioni per il monitoraggio e di vari protocolli di management in un unico sistema.
Tecnicamente, per garantire la compatibilità dei sistemi, le informazioni raccolte dovranno essere espresse in un formato accessibile da più piattaforme e le comunicazioni dei dati di management dovranno essere implementate attraverso protocolli standard (vedi Cap. 2 Sez. 2.1.4).

4.2 Progettazione

L'architettura progettata (figura 21) è composta da tre componenti:

- Router Juniper;
- Console di analisi;
- Rete di management.

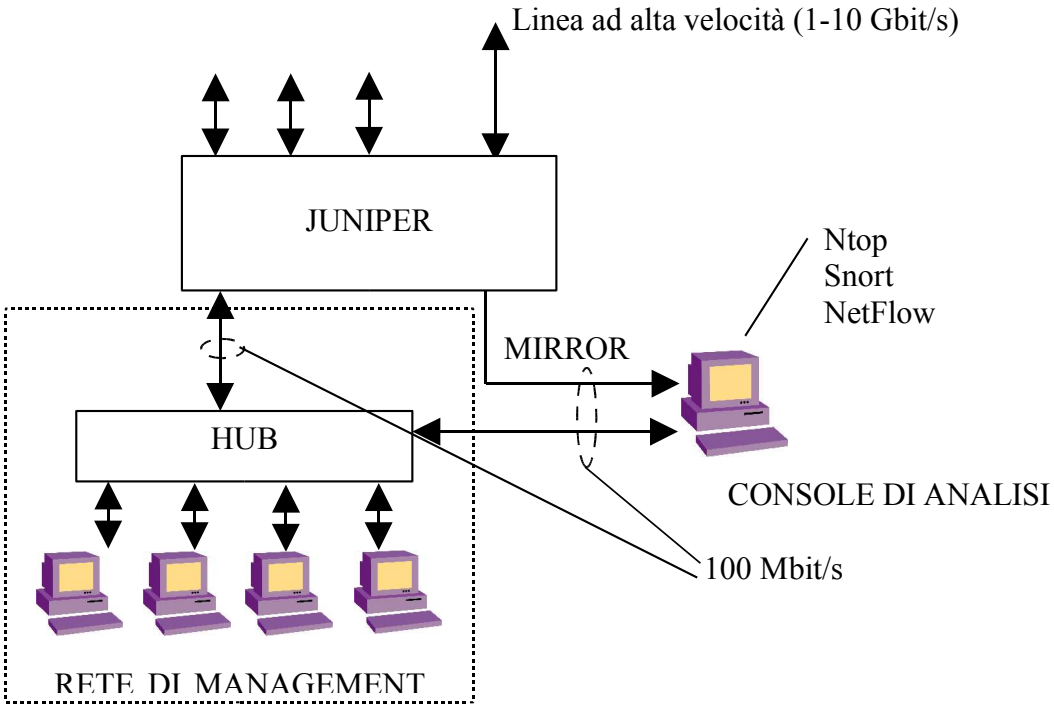


Fig. 21 Architettura per il monitoraggio di reti ad alta velocità.

Nelle sezioni seguenti viene descritto in dettaglio il funzionamento di ogni componente dell'architettura, i meccanismi attraverso i quali si implementa la cooperazione e le tecniche che consentono l'integrazione dell'architettura con le piattaforme di management.

4.2.1 Juniper

Il Juniper costituisce la parte centrale dell'architettura. Dagli studi effettuati sono state evidenziate delle caratteristiche che favoriscono il suo utilizzo nella soluzione proposta quali:

- Interfaccia a vari tipi di link ad alta velocità;

i moduli PIC offrono un'ampia gamma di supporti per vari tipi di media (vedi Cap. 3 Sez. 3.4.1).

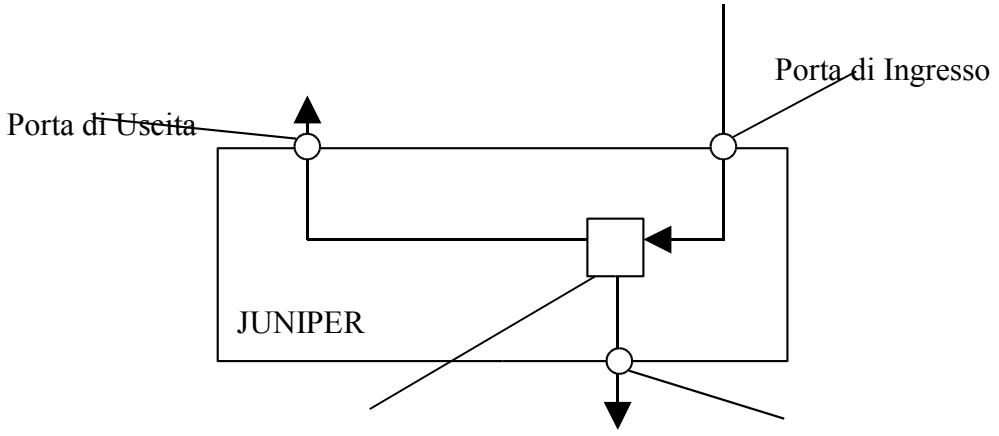
- Mirror parziale del traffico;
  questa caratteristica costituisce il punto chiave dell'architettura e viene descritta in dettaglio di seguito.
- Porta di management;
  il router ha un'interfaccia (lenta) dedicata alla configurazione da remoto.

Come già accennato la possibilità di configurare il router affinché esegua un mirror parziale del traffico stà alla base dell'architettura progettata. Questa tecnica consiste nel:

1. selezionare i pacchetti in ingresso al router che soddisfano determinate regole (ad esempio indirizzo sorgente /destinazione);
2. eseguire le normali operazioni di routing dei pacchetti;
3. prima di inviare il pacchetto sull'interfaccia di uscita eseguirne una copia da inviare sulla porta di mirror sulla quale sono in ascolto le applicazioni di analisi.

Grazie a questo, si riesce a ripristinare la condizione fondamentale che consente un corretto funzionamento dei tool passivi. Di fatto, in questo modo, viene operata una riduzione del volume di traffico (solo il traffico selezionato viene inviato sulla porta di mirror e non tutto) che consente l'impiego di tecniche di monitoraggio passive.

Il meccanismo di campionamento del Juniper tecnicamente viene eseguito da un'unità ASIC, interna al router, che, oltre ad instradare il pacchetto in ingresso sull'appropriata porta di uscita (esecuzione delle operazioni di routing), invia una copia del medesimo alla porta di mirror (figura 22). Questa unità può effettuare il mirror fra interfacce a media tecnologicamente diversi. In questo modo, ad esempio, è possibile eseguire il mirror del traffico IP-over-ATM su un interfaccia Ethernet.



Unità ASIC Porta di Mirror

Fig. 22 Meccanismo di campionamento all'interno del Juniper.

La politica di campionamento implementata dall'unità ASIC può essere fortemente condizionata, dagli amministratori di rete, agendo sui parametri di configurazione del router. Di fatto è possibile configurare il Juniper in modo da eseguire il sampling in 3 diversi modi:

1. Definizione di un tasso di campionamento;
   si configura il router per eseguire il mirror di una percentuale del traffico (ad esempio un pacchetto su 400, 1/400).
2. Definizione di filtri;
   definendo delle regole di selezione è possibile instrumentare il router in modo da eseguire il mirror dei pacchetti che hanno determinate caratteristiche (ad esempio protocollo, indirizzo sorgente/destinazione, ecc.).
3. Campionamento dei pacchetti filtrati;
   in questo modo si definisce una composizione delle due tecniche precedentemente descritte.

Gli amministratori, agendo sul tasso di campionamento del traffico, possono effettuarne una riduzione del volume in modo proporzionale, in maniera analoga a quella esaminata per sFlow.

Attraverso l'applicazione dei filtri, inviati al router tramite la rete di management (vedi Sez. 4.2.3), è possibile restringere il processo di campionamento ai soli dati che soddisfano le regole definite. Tali filtri consentono agli amministratori di selezionare il traffico in base ad alcuni valori che caratterizzano sia i campi dell'header dei pacchetti che la porta di ingresso/uscita nel dispositivo. Di seguito riportiamo due esempi di applicazione del filtraggio dei pacchetti in transito:

- Selezione dei pacchetti ICMP, ad esempio per la gestione della sicurezza (vedi Sez. 4.3.1).
- Selezione del traffico destinato all'interfaccia di accesso a Internet.

Nel primo caso viene evidenziata la possibilità di filtrare i pacchetti in base al protocollo. Nel secondo il traffico viene selezionato in base all'indirizzo di destinazione (da notare che è inutile filtrare tutto il traffico proveniente dall'interfaccia alla linea ad alta velocità).

È possibile inoltre effettuare un campionamento statistico dei pacchetti filtrati riducendo ulteriormente il volume di dati da analizzare. In questo modo non tutti i pacchetti filtrati vengono copiati sulla porta di mirror in quanto viene applicato loro un tasso di campionamento. Gli amministratori, in questo caso, definiscono tale tasso in modo da campionare un numero più elevato di pacchetti (1/200) rispetto a quello definito per il caso del semplice mirror (1/400), data l'esecuzione di un pre-filtraggio dei dati che già opera una riduzione del traffico.

Definendo:

- T= tasso di campionamento;
- B= banda della rete;
- M= banda della linea di mirror;

è facile ricavare la formula per la determinazione della banda della linea di mirror:

$$M = B * T$$

Con l'applicazione di un tasso di campionamento pari a 1/400, in una linea ad alta velocità (B = 1 Gbit/s), M risulta:

$$1 \text{ Gbit/s} * 1/400 = 2.5 \text{ Mbit/s}$$

una banda ampiamente gestibile dai tool di monitoraggio passivi.

Anche in presenza di una rete dalla banda di 10 Gbit/s, la banda finale da gestire risulta:

$$10 \text{ Gbit/s} * 1/400 = 25 \text{ Mbit/s}$$

Quindi in definitiva l'architettura riesce a sopperire ampiamente ai problemi introdotti dal monitoraggio di reti ad alta velocità. Per migliorare l'accuratezza delle informazioni raccolte

è possibile aumentare il tasso di campionamento, impostandolo a 1/200. Rispettivamente M cambierà in:

- 5 Mbit/s per link a 1 Gbit/s
- 50 Mbit/s per link a 10 Gbit/s

4.2.2 Console di Analisi

La console di analisi è composta da un PC equipaggiato con due schede di rete Ethernet 10/100 (vedi fig. 23) che vengono impiegate per:

- La prima (eth0), collegata alla porta di mirror, è necessaria per ricevere i pacchetti inviati dal router. Tale scheda non deve essere usata per l'invio dei dati (modalità read-only).
- La seconda (eth1) è collegata alla rete di management per consentire l'instrumentazione del router e l'accesso ai dati analizzati da parte degli amministratori di rete.

L'utilizzo di questo tipo di schede, ampiamente commercializzate, consente di limitare i costi del sistema, anche se vincola il router ad eseguire, se necessario, delle trasformazioni dei dati provenienti da media diversi.
L'utilizzo di tali schede, che possono raggiungere al massimo velocità trasmissive di 100 Mbit/s, non comporta i problemi (perdita dei dati inviati dalle schede al processore centrale della console di analisi) derivanti dalle limitazioni del bus PCI, in quanto la saturazione della banda si manifesta soltanto in presenza di velocità trasmissive superiori.
Inoltre, per come è stata definita l'architettura, i collegamenti fra i vari componenti possono essere limitati da una banda di 100 Mbit/s in quanto:

- per la trasmissione dei dati di management (rete di management) non sono necessarie velocità superiori a quelle definite;
- il volume di dati trasmessi sul collegamento fra la porta di mirror del router e la console di analisi è vincolato dalla definizione del tasso di campionamento e dei filtri nelle modalità viste in precedenza.

L'analisi dei dati inviati dal router viene effettuata da 3 diversi tool passivi installati sulla console di analisi:

- Ntop,
- Snort,
- NetFlow.

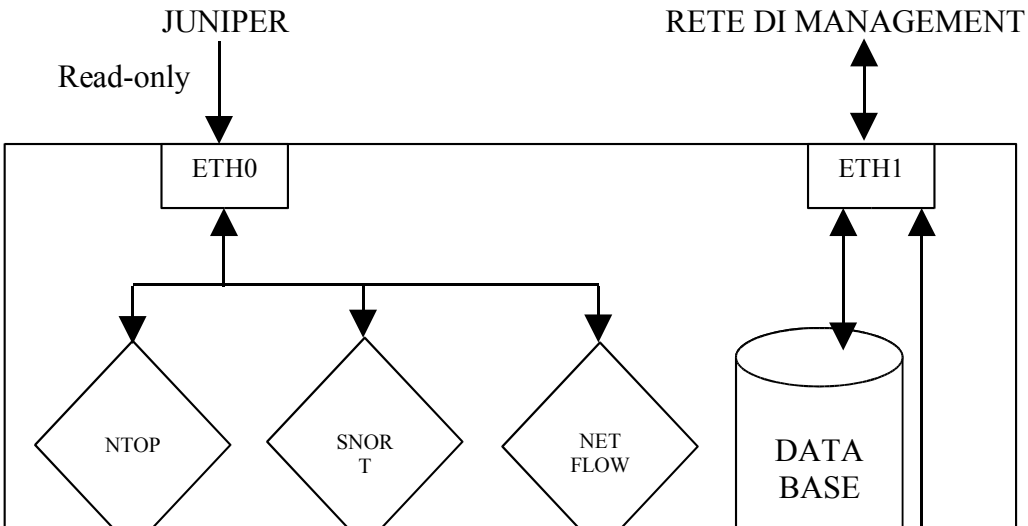
La console di analisi, oltre ad effettuare le operazioni necessarie per ottenere informazioni utili alla gestione di rete, costituisce il punto di integrazione fra l'architettura proposta e le piattaforme di management esistenti. Di fatto tutte le misurazioni effettuate dai tool vengono memorizzate in un database compatibile con quelli impiegati dalle piattaforme più diffuse. I requisiti base che vengono definiti per questo database sono:

- Interfaccia indipendente dal sistema ospite (ad esempio SQL).
- Alta tolleranza agli errori.
- Bassi tempi di risposta.
- Elevata affidabilità.
- Integrazione di procedure per la compressione e il recupero dei dati (data mining).
- Capacità di notifica automatica nel caso di cambiamento di dati significativi (trigger).

Come evidenziato il database non è soggetto a vincoli di progettazione, in questo modo, a seconda della piattaforma di management utilizzata, è possibile introdurre un database che consenta l'integrazione dei sistemi.

In definitiva grazie alla compatibilità del database, sia i tool che le piattaforme di management, possono manipolare le informazioni per consentire agli amministratori una corretta gestione della rete.
Ad esempio, attraverso l'analisi dei dati storici archiviati, è possibile ricavare delle informazioni statistiche per:

- accounting e billing;
- pianificazione della rete;
- ingegnerizzazione del traffico;



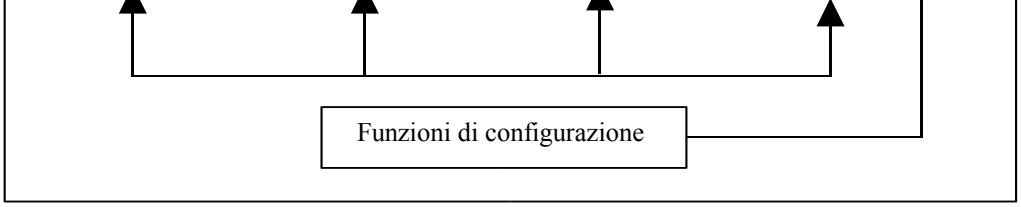


Fig. 23 Schema della console di analisi.

Nella figura 23 vengono evidenziate delle funzioni di configurazione che sono necessarie agli amministratori, che operano fisicamente sulla console di analisi, per poter intervenire tempestivamente sul router in modo da far fronte alle situazioni che si vengono a creare di volta in volta. Ad esempio, per garantire la sicurezza della rete, è necessario poter applicare dei filtri per approfondire le analisi fatte e prendere provvedimenti immediati (proactive management).

Tali operazioni sono effettuabili connettendosi al router tramite la scheda collegata alla rete di management (eth1), e configurando i parametri, ad esempio, per il campionamento, per la selezione di una particolare tipologia di traffico in modalità automatica (vedi Cap. 5).

4.2.3 Rete di Management

La configurazione del router è un'operazione che soltanto gli amministratori di rete devono poter effettuare. È pertanto necessaria una rete di management, separata dalla rete dati, a cui possa accedere soltanto questa categoria di utenti.

La rete di management deve pertanto avere, come unico requisito, la presenza di un punto di connessione fra tutti i componenti dell'architettura. Gli autori, a titolo di esempio, hanno

introdotto un hub che collega le postazioni di lavoro degli amministratori, compresa la console di analisi, e il router (Figura 21). Nonostante l'esempio riportato, l'architettura proposta non vincola la progettazione della rete di management, che può essere implementata a seconda degli accorgimenti del caso.

Sulle postazioni di lavoro facenti parte di questa rete, è possibile installare piattaforme di management come HPOpenView (Figura 24), che possono quindi interagire con il router e la console di analisi.

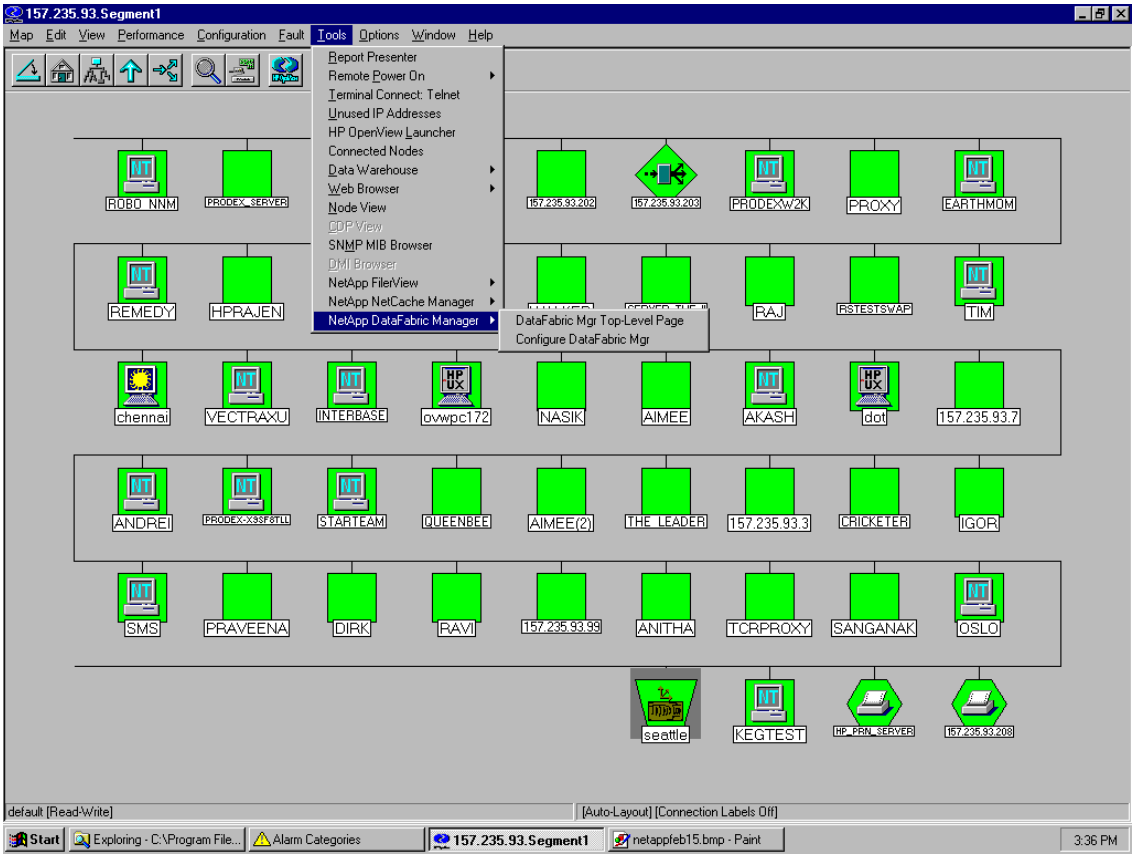


Fig. 24 Screenshot di HpOpenView.

4.3 Campi di applicazione

L'architettura progettata consente l'esecuzione di funzioni di management in reti ad alta velocità. Come già descritto in precedenza, le applicazioni di management possono essere racchiuse in 5 aree funzionali (Cap. 1 Sez. 1.1.2) per la gestione di:

- fault;

- configurazioni;
- accounting;
- performance;
- sicurezza;

Per determinare l'efficienza dell'architettura progettata è necessario descriverne in dettaglio il comportamento a seconda delle aree funzionali definite. Per quello che concerne la gestione dei fault, dell'accounting e della sicurezza saranno trattate nelle sezioni successive, mentre gli autori hanno tralasciato lo studio della gestione delle configurazioni e delle performance in quanto non significative ai fini della tesi. Questa scelta è stata dettata dal fatto che tali aspetti della gestione di rete vengono affrontati non solo con il monitoraggio passivo ma anche con strumenti attivi (ad esempio il Ping [7] permette la determinazione della connettività e della performance) che, come già specificato, non risentono delle elevate velocità trasmissive della rete.

4.3.1 Gestione dei Fault

La rilevazione dei fault di rete è certamente una funzione di primaria importanza in un sistema di monitoraggio. I malfunzionamenti ad esempio possono comportare:

- la mancata visualizzazione di una pagina web (indisponibilità di un server HTTP);
- la degradazione delle performance di rete (presenza di colli di bottiglia).

Per effettuare la rilevazione di errori di questo tipo, è necessario controllare la presenza sulla rete di alcuni pacchetti, quali ad esempio quelli ICMP e quelli TCP con il flag RST[9] (reset) impostato.

La provenienza e il tipo dei pacchetti ICMP forniscono vari tipi di informazioni, tra le quali:

- rete/host/porta/protocollo di destinazione irraggiungibile;
- rete/host di destinazione sconosciuto;

I pacchetti TCP con il flag RST sono invece indice di terminazione anomala di connessioni fra due nodi remoti.

[9] I pacchetti con il flag RST impostato vengono inviati per abortire o rifiutare una connessione TCP.

Durante il monitoraggio della rete, se viene rilevata la presenza di un numero di pacchetti dei due tipi descritti superiore alla media stimata (ricavata dalle informazioni storiche memorizzate nel database), occorre analizzare questo traffico specifico per inquadrarne la sorgente e isolare l'errore.

L'architettura proposta permette una facile risoluzione di questi problemi anche in una rete caratterizzata da un'alta velocità trasmissiva. Per selezionare una certa categoria di traffico (in questo caso pacchetti ICMP e TCP con flag RST), gli amministratori devono configurare il Juniper definendo dei filtri che permettano di riconoscere questi pacchetti. Una volta che il traffico da analizzare arriva alla console di analisi, attraverso la porta di mirror, la cattura dei pacchetti e la loro successiva analisi viene eseguita da Ntop. Questo tool può operare senza il verificarsi dei problemi descritti in precedenza (vedi Cap. 3 Sez. 3.4.2) grazie alla riduzione del volume di traffico effettuata dal router.
Ntop, analizzando i pacchetti catturati, permette di rilevare un'ampia categoria di anomalie (vedi Cap 2 Sez. 2.3.2.1.3) senza l'ausilio di altri strumenti software.

4.3.2 Gestione dell'Accounting

Capire qual è la sorgente del traffico, sia a livello applicativo che a quello fisico, è un aspetto importante del monitoraggio di una rete ad alta velocità.
In una rete tradizionale, per risolvere questo problema, è possibile impiegare il NetFlow (vedi Cap. 2 Sez. 2.3.2.1.1) che, analizzando i flussi di traffico, consente l'invio alle applicazioni di analisi di dati rilevanti per l'accounting. Gli stessi benefici l'installazione di NetFlow non li apporta su dispositivi operanti in una rete ad alta velocità dato che il tool è in grado di operare fino alla velocità di 40 Mbit/s. La riduzione del traffico, operata dal router, consente un corretto funzionamento di NetFlow anche con reti veloci, in quanto il volume di traffico da analizzare rientra nei limiti imposti dal tool stesso.
È possibile selezionare ad esempio, per la gestione dell'accounting, soltanto quei pacchetti con indirizzo di destinazione Internet, cioè indirizzo diverso da quello della rete interna (ad esempio la rete Netikos utilizza l'indirizzo 172.22.x.x della rete).
Gli amministratori devono quindi instrumentare il router, applicando appositi filtri, in modo da selezionare soltanto i pacchetti che hanno indirizzo di destinazione esterno alla rete monitorata. Questi, inviati sulla porta di mirror alla console di analisi dal Juniper, vengono analizzati da NetFlow che, tramite i suoi componenti, permette di:

- aggregare le informazioni di flusso (Flow Collector);
- analizzare i dati (Network data Analyzer)
- creare report periodici (FlowScan).

Inoltre il NetFlow consente, se necessario, di raccogliere informazioni non solo dalla porta di mirror, ma anche da una serie di sonde dislocate nella rete. Questo permette agli amministratori di specificare in modo molto accurato le informazioni necessarie per l'accounting (ad esempio specificare il traffico di un particolare host/sottorete).
In generale, la grande quantità delle informazioni per la determinazione dei dati di accounting, vincola gli amministratori ad ottimizzare i filtri in modo da selezionare un appropriato volume di traffico in quanto:

- una quantità eccessiva comporta un malfunzionamento del tool;
- una quantità troppo ridotta comporta un'inconsistenza dei dati raccolti.

4.3.3 Gestione della Sicurezza

Per quanto concerne la gestione della sicurezza, in questa sezione, vengono descritte le funzionalità dell'architettura che permettono la rilevazione, ad esempio, di Denial of Service (DoS, interruzione del servizio) tralasciandone il comportamento in presenza degli altri innumerevoli attacchi conosciuti.
In questa categoria vengono raggruppati tutti quegli attacchi che hanno come unico fine quello di interferire con la corretta erogazione dei servizi di rete (web, posta elettronica ecc.).
Alcuni esempi delle tecniche più diffuse per l'attuazione di DoS sono:

- SYN flood (vedi Sez. 3.3).
- Trojan [5],
  programmi inviati ai PC tramite e-mail, o camuffati con altri programmi, che una volta attivati possono permettere il controllo del PC da remoto.

Questi tipi di attacco possono essere individuati, rispettivamente, monitorando la frequenza dei pacchetti TCP caratterizzati dal bit SYN settato, e controllando i pacchetti che vengono inviati verso porte non convenzionali. I trojan infatti, possono essere configurati per aprire delle porte di comunicazione del PC verso l'esterno, tipicamente tenute chiuse dal sistema operativo, consentendo l'accesso da remoto alle informazioni contenute sul computer all'insaputa degli utenti autorizzati.

Impostando dei filtri appropriati, gli amministratori, possono selezionare questi tipi di pacchetti ed eseguirne un'analisi accurata dalla console di analisi. L'implementazione della sicurezza avviene tramite:

- Snort,
  che, grazie a delle regole specifiche, consente la rilevazione di accessi non autorizzati, attraverso porte di comunicazione aperte dai troyan (backdoor).
- Ntop,
  che cattura i pacchetti di richiesta di connessione e verifica se il loro numero, non supera di molto la media.

		TOOL			
		NetFlow	Ntop	Snort	Juniper
FUNZIONI	Meccanismo di campionamento				●
	Gestione dei fault		●		
	Gestione della Sicurezza		●	●	
	Ingegnerizzazione della rete		●		
	Gestione dell'Accounting	●			

Tab. 6 Funzioni svolte dagli strumenti impiegati nell'architettura proposta.

5. Sperimentazione

Come detto nelle pagine introduttive della tesi, il tirocinio si sarebbe dovuto concludere con la definizione delle linee guida per la progettazione dell'architettura. Data però la disponibilità, nell'azienda ospite del tirocinio, dei componenti richiesti dalla progettazione è stato possibile dare inizio alla fase di sperimentazione di modo da verificare l'effettivo

funzionamento dell'architettura. Purtroppo, per il poco tempo a disposizione, questa fase non è stata sviluppata in tutti i suoi aspetti.

Per verificarne l'efficienza, l'architettura progettata è stata sperimentata sulla rete interna dell'azienda NETikos (sviluppata sui tre piani della sede di Pisa) che ha un collegamento portante, in fibra ottica, dalla velocità di 1 Gbit/s.

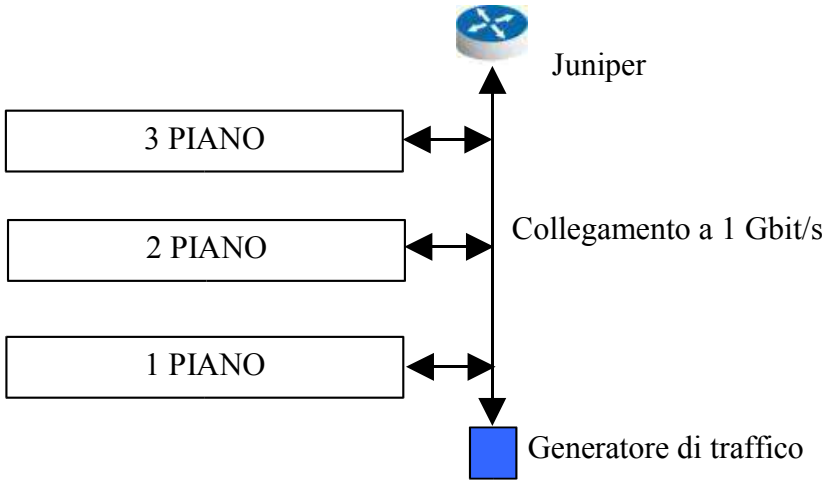


Fig.25 Schema della rete di sperimentazione.

Come mostrato dalla figura 25, il Juniper è stato impiegato per effettuare il monitoraggio del collegamento veloce della rete NETikos impostandolo come default gateway, cioè in modo tutti i pacchetti debbano necessariamente transitare dal router. In aggiunta è stato inserito un generatore di traffico per saturare la rete.

Prima di dare inizio alla fase di sperimentazione vera e propria, è stato effettuato uno studio per individuare delle classi di traffico a cui poter assegnare dei filtri per il campionamento. Ad esempio alcune classi definite per la rete locale di Pisa sono:

- traffico indirizzato al proxy internet per la determinazione dell'accounting;
- traffico ICMP per garantire la sicurezza e la rilevazione di errori;

I filtri vengono definiti in un file di configurazione del Juniper e sono composti da:

- Termini, che identificano, tramite le specifiche degli attributi, ogni classe di traffico.
- Politiche, che specificano le soglie individuate per ogni termine e le azioni da intraprendere nel caso di eccedenza delle soglie.

Gli autori durante questa fase hanno individuato, per le classi di traffico definite, dei termini quali:

- Proxy, caratterizzato dall'indirizzo destinazione dei pacchetti (nel caso specifico 172.22.4.122);
- ICMP Traffic, composto da tutti i pacchetti ICMP (protocol ICMP).

Per quello che concerne il termine "Proxy", essendo questa classe di traffico utile per la determinazione dell'accounting, viene applicato il sampling definito in seguito. Per il termine "ICMP Traffic" è stata definita invece una politica. Questa prevede il mirror di tutto il traffico ICMP (sampling con tasso di campionamento 1/1) nel caso in cui il termine superi le soglie di banda. Tali soglie sono definite, solitamente, in base alla media del volume di traffico ICMP presente nella rete.
Il meccanismo di sampling viene descritto nello stesso file di configurazione nel quale sono definiti i filtri. Nel caso preso in considerazione, per il termine "Proxy", è stato definito un "sample proxy", che specifica le opzioni di sampling:

- tasso di campionamento (1/400);
- interfaccia di mirror (nel caso specifico 172.10.0.2).

I filtri definiti sono stati applicati all'interfaccia del router collegata alla dorsale a fibra ottica. Mentre è stato definito un altro filtro, applicato all'interfaccia di mirror, che, nel caso di eccedenza di banda (100 Mbit/s), attua un'ulteriore riduzione del traffico (applicazione del Sample).

Il ciclo di funzionamento del router, per il monitoraggio del collegamento ad alta velocità, è di seguito illustrato:

- Ricezione di un pacchetto dalla linea veloce;
- Individuazione del termine di appartenenza;
- Applicazione delle politiche (se definite);
    - Se si ha un superamento del valore di soglia si intraprendono le azioni definite;
    - Se non si ha il superamento del valore di soglia si prosegue;
- Esecuzione delle operazioni di routing.

Per come sono stati definiti i filtri nella fase di sperimentazione, nel caso in cui il traffico ICMP superi la soglia di 32Kbit/s il router esegue, in modo automatico, il mirror di tutto questo tipo di traffico verso la console di analisi.

Durante la fase di sperimentazione gli autori si sono serviti di una console di analisi equipaggiata con:

- Sistema operativo RedHat Linux 7.3;
- Ntop versione 2.0.99;
- Snort versione 1.8.6;
- NetFlow versione 5.
- database Oracle.

Il funzionamento di ogni tool installato sulla console di analisi è di seguito descritto.

NTOP

Ntop, utilizzando la libreria Libpcap, cattura ogni pacchetto inviato dal Juniper ed esegue un'analisi dei dati rendendoli accessibili attraverso un'interfaccia web (formato HTML). Inoltre, per consentire l'interazione fra il tool e il database, a Ntop è stato configurato per l'interfacciamento con Oracle.

SNORT

Snort esegue un'analisi di tutto il traffico in arrivo, applicando le regole di sicurezza che il tool definisce di default. Inoltre, in caso di rilevamento di situazioni pericolose, oltre alla memorizzazione dei dati nel database, il tool invia una notifica SNMP (TRAP [2]) alla piattaforma di management che nel caso specifico è HpOpenView.

NetFlow

Durante la fase di sperimentazione, sia il componente di aggregazione (flow caching) che quello di collezionamento/analisi (flow collector/analysis) , sono stati installati sulla stessa macchina. Perciò, il flow caching, una volta creati i pacchetti identificativi di flusso, invece di inviarli ad un host remoto, li invia direttamente al componente di analisi. Questo una volta elaborati i dati, provvede alla memorizzazione degli stessi nel database.

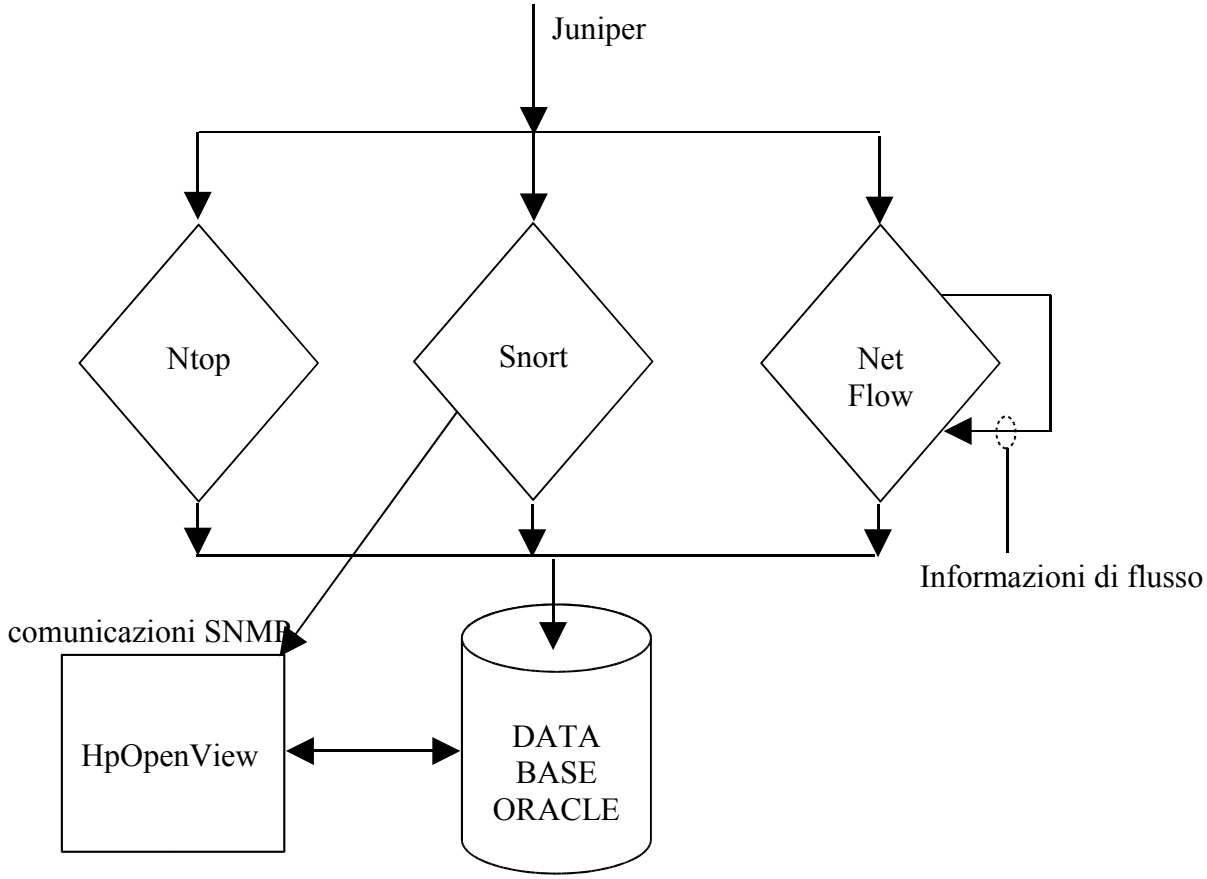


Fig. 26 Schema di funzionamento della console di analisi sperimentale.

Dai dati raccolti si è evidenziato che:

- Il traffico in arrivo alla console di analisi è facilmente gestibile dai tool installati, questo perché il Juniper riesce ad eseguire correttamente il campionamento dei dati. La punta massima di traffico in arrivo alla console è stata di circa 5 Mbit/s.
- Si è riscontrato un elevato volume del traffico ICMP dovuto all'utilizzo di applicazioni peer-to-peer (ad esempio Morpheus).

- Si sono identificate con precisione le macchine che generano e ricevono il maggior volume di traffico (ad esempio il proxy).

6. Conclusioni

Il lavoro svolto ha introdotto un nuovo modo di concepire il monitoraggio passivo di reti ad alta velocità. Di fatto la soluzione proposta capitalizza gli studi effettuati fino ad oggi consentendo l'impiego delle tecnologie esistenti per la risoluzione di un problema che, se non

ancora di attualità, si rivelerà di primaria importanza nel breve periodo. Questo perché si ha un utilizzo sempre più diffuso dei collegamenti ad alta velocità anche per le reti locali.
Da subito, gli autori hanno orientato i loro studi in una direzione che consentisse di ridurre il volume di traffico da analizzare. Tutto ciò senza che questo comportasse una perdita di informazioni utili alla gestione di rete ed, allo stesso tempo, consentisse l'impiego degli strumenti passivi che godono di larga diffusione. A questo scopo è stato approfondito il funzionamento della tecnologia sFlow, in quanto unica ad operare in modo da non analizzare l'intero traffico in transito ma soltanto un campione. Inoltre, sFlow, applicando modelli statistici sui pacchetti campionati, consente di ricavare informazioni significative per una corretta gestione di rete.
Data l'affidabilità delle misurazioni eseguite con la tecnica del packet sampling implementata da sFlow, in un primo momento è stato pensato un suo utilizzo nel monitoraggio di reti ad alta velocità, riscontrandone però grosse limitazioni. Di fatto l'impiego diretto della tecnologia sFlow, tramite l'installazione di un agent all'interno di un router, ne avrebbe rallentato le prestazioni. Il dispositivo infatti, prima di instradare i pacchetti, avrebbe dovuto applicare l'algoritmo di campionamento descritto in precedenza (vedi Cap. 3 Sez. 3.4.2) perdendo in efficienza.
Nonostante la possibilità di implementare l'agent sFlow, tramite dispositivi hardware, direttamente all'interno dei router, aumentando notevolmente la velocità di esecuzione delle operazioni di campionamento, le prestazioni ottenute non erano conformi alla velocità di trasmissione delle reti prese in considerazione da questa tesi.
Nonostante l'impossibilità di utilizzo di sFlow, si è cercato di operare in modo da implementare una riduzione del traffico tramite l'utilizzo di altri strumenti. Questo perché si è riscontrato che i problemi caratterizzanti l'impiego di sFlow in reti ad alta velocità, non derivano dall'affidabilità delle informazioni ricavate, ma dall'inefficienza del meccanismo di campionamento.
Studiando le varie tecniche di monitoraggio esistenti, si sono riscontrate delle caratteristiche di diversi strumenti che combinate fra loro consentivano di riprodurre il comportamento di sFlow (per quello che concerne il meccanismo di sampling), e di eseguire un'analisi accurata dei dati ricavati.
Il componente che sopperisce alle limitazioni di sFlow è costituito da un router che offre la possibilità di eseguire il mirror di determinate categorie di traffico (nel caso specifico Juniper). Accanto al router, per eseguire l'analisi del traffico campionato, è stato introdotto nell'architettura un componente equipaggiato con dei tool di analisi.

In questo modo si è potuta definire un'architettura modulare. Ciò significa che, nonostante la specificità dei componenti presentati in questa tesi, è possibile sostituirli con altri che mettono a disposizione le stesse funzionalità, per quello che riguarda i router, e con gli strumenti di analisi che nel tempo saranno ritenuti più efficienti. Sostituendo i componenti con altri tecnologicamente più avanzati si può garantire una certa scalabilità dell'architettura di modo da non renderla obsoleta nel breve periodo.

Come già detto la possibilità di ridurre il traffico in transito su di una rete ad alta velocità, attraverso l'utilizzo di un router appropriato, è il punto di forza dell'architettura, che permette di ricondurre il problema affrontato al monitoraggio di reti a bassa velocità. Per questo motivo è necessario individuare delle categorie di traffico che, relazionate ad ogni campo di applicazione, una volta analizzate, non forniscono informazioni significative ai fini della gestione di rete e che perciò possono essere escluse durante la fase di filtraggio.

Il fattore che rende l'architettura scalabile, fino alla velocità di 10 Gbit/s, è l'applicazione corretta dei filtri in modo da delineare il traffico da eliminare e, per quanto riguarda il sampling, il giusto bilanciamento del tasso di campionamento (aumentando la velocità, è necessario diminuire il numero dei pacchetti campionati).

Nonostante il lavoro effettuato l'architettura proposta necessita di una fase di sperimentazione più sviluppata rispetto a quella presentata in questa tesi. Perciò, compito dei realizzatori dell'architettura, sarà quello di sviluppare una fase di test che possa dimostrare le effettive capacità dell'architettura proposta.

APPENDICE A

Porzione del file di configurazione del Juniper.

```
family inet {
  filter netikos{
    policer ICMP {
                if-exceeding {
```

```
                    bandwidth-limit 32k;
                   }
                then sample ICMP;
                 }

     term proxy {
                from {
                    address {
                              172.22.4.122/32;
                              }
                    }
                then {
                         sample proxy;
                         accept;
                    }
                }
     term ICMP-Traffic{
          if{
               protocol ICMP
          }
          then{
               policer ICMP
               accept
          }
     }
     sample proxy {
             input {
                    family inet {
                              rate 400;
                         }
                    }
               output {
                    port-mirroring {
                              interface fe-0/0/3.0;
                              next-hop 172.10.0.2;
                    }
                }

          }

     }
}
```

7. Bibliografia

[1] SCAMPI:

Scaleable Monitoring Platform for the Internet, annex1 Agosto 2001.

[2] SNMP:

J. Case, M. Fedor, M. Schoffstall, J. Davin, RFC 1157 www.ietf.org/rfc/rfc1157.txt; Maggio 1990

[3] RMON:

S. Waldbusser ,RFC-1757 http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1757.html. Febbraio 1995

[4] C. M. Kozierok, *Bus Bandwidth,*

http://www.pcguide.com/ref/mbsys/buses/funcBandwidth-c.html 2001

[5] *I Troyan* http://www.crazynet.it/sicurezza/trojan.htm

[6] Future software limited, *FCAPS white paper,*http://www.futsoft.com/pdf/fcapswp001.pdf

[7] L. Deri – J. Shonwalder "Sistemi di Eleborazione dell'Informazione: Gestione di Rete". http://luca.ntop.org. Febbraio 2001.

[8] CORALREEF:

K. Keys, D. Moore, R.Koga, E.Lagache, M. Tesch , k claffy; *The Architecture of CoralReef: An Internet Traffic Monitoring Software Suite*, http://www.caida.org/outreach/papers/2001/CoralArch/,

[9] RTFM:

N. Brownlee; C. Mills; G. Ruth, RFC 2063, http://www.ietf.org/rfc/rfc2063.txt. Gennaio 1997.

[10] ETHEREAL:

Richard Forno and Kenneth R. van Wyk, *Tools of the trade* http://www.onlamp.com/pub/a/onlamp/excerpt/incidentres_07/index.html,

[11] J.F.Kurose, K.W.Ross, *Internet e reti di calcolatori*, McGraw-Hill 2001.

[12] PoS:

Designing packet over sonet-SDH (PoS); Agilent Technologies; 2000 http://literature.hp.com/litweb/pdf/5968-1614e.pdf

[13] MPLS:

R. Gallaher, *An introduction to MPLS*; http://www.rickgallaher.com/mplslinks.htm Settembre 2001.

[14] NetFlow:

Cisco System, *Cisco IOS NetFlow Tecnologies* http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosnf_ds.htm 2001

[15] One-Way-Delay:

G. Almes; S. Kalidindi; M. Zekauskas, RFC 2679. http://www.ietf.org/rfc/rfc2679.txt

Settembre 1999.

[16] AMP:

T. Hansen, J. Otero, T. McGregor; H. W. Braun, *Active measurement data analysis techniques*; Marzo 2000.

[17] SURVEYOR:

S. Kalidindi, M. Zekauskas, *Surveyor: an infrastructure for Internet Performance Measurements*; Giugno 1999.

[18] RIPE TTM:

H. Uijterwaal; O. Kolkman, *Internet delay measurements using test traffic*; Giugno 1997.

[19] SFlow:

P. Phaal; S. Panchen; N. Mckee, RFC 3176, http://www.ietf.org/rfc/rfc3176.txt. Settembre 2001.

Traffic monitoring using sFlow, http://www.inmon.com/sflowoverview.pdf; InMon corp. Gennaio 2000.

[20] NeTraMet:

N. Brownlee *NeTraMet - a network traffic flow measurement tool* http://www.caida.org/tools/measurements/netramet 1999

[21] cFlowd:

D. McRobb, *cFlowd: traffic flow analysis tool* http://www.caida.org/tools/measurements/cflowd Marzo 2000

[22] FlowScan:

D. Plonka, *FlowScan: a network traffic flow reporting and visualization tool*; Febbraio 1999.

[23] LIBPCAP:

T. Carstens, *Programming with Pcap,* http://www.tcpdump.org/pcap.html; Gennaio 2002.

[24] NTOP:

L. Deri, S. Suin, *Effective traffic measurement using NTOP*, http://luca.ntop.org; Maggio 2000.

[25] SNORT:

M. Roesch, *Snort – lightweight intrusion detection for networks* http://www.snort.org/docs/lisapapre.txt; Marzo 1998.

[26] DAG:

N. Browlee, *Dag4 architecture*

http://dag.cs.waikato.ac.nz/dag/dag4-arch.html 2001

[27] RADISYS:

D.M. Contis; W. Lee; D.E. Schimmel; W. Shi; A. Thomas; Y. Zhang; J. Li; M. Necker; *A prototype programmable network processor based intrusion detection system*; http://www.radisys.com/, Maggio 2001.

[28] TOPLAYER:

IDS-Balancer; http://www.toplayer.com/pdf/tln_ids_balancer.pdf Aprile 2001.

[29] JUNIPER:

Juniper networks Inc., *M5 and M10 Internet Backbone Routers Release Notes*

http://www.juniper.net/techpubs/hardware/m5-m10/m5-m10-rn/download/rn-m5-m10.pdf 2000

[30] Cisco:

Cisco Systems,

http://www.cisco.com

[31] FPing:

R. Schmers, *fping*

http://www.fping.com

[32] Intel:

Intel Corporation,

http://www.intel.com