

# ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Trieste

---

INFN/TC-97/24  
8 Settembre 1997

R. Gomezel, C. Strizzolo:

**IPACCOUNTING**

**MONITORAGGIO E PRODUZIONE DI STATISTICHE DI TRAFFICO**

**TCP/IP SU ROUTER CISCO PER PIATTAFORME UNIX**

**VERSIONE 2.0**

# IPaccounting



Monitoraggio e produzione di statistiche di traffico  
TCP/IP su router Cisco per piattaforme Unix

Versione 2.0

Roberto Gomezel  
Claudio Strizzolo  
(I.N.F.N. Sezione di Trieste)

## Sommario

Il software IPaccounting consente di monitorare ed effettuare l'accounting dell'utilizzo di TCP/IP su un router Cisco che collega un "dominio di accounting" al resto del mondo. Con il termine "dominio di accounting" si intende un insieme di reti il cui traffico verso il "mondo" viene monitorato per mezzo di IPaccounting.

La versione 2.0 di IPaccounting presenta notevoli innovazioni rispetto alla 1.0. Tali miglioramenti sono in buona parte basati sul feedback ottenuto dagli utenti della versione precedente.

## **IPaccounting - Versione 2.0**

Questo software è stato sviluppato presso l'Istituto Nazionale di Fisica Nucleare (INFN)  
- Sezione di Trieste, da Claudio Strizzolo e Roberto Gomezel - Luglio 1997.

Tutti i diritti riservati.

La copia, la distribuzione e la duplicazione non autorizzate non sono consentite.

Questo software è distribuito con la formula "as is", e senza alcuna garanzia implicita  
o esplicita.

Tutti i marchi registrati che compaiono in questo documento sono riconosciuti come  
tali.

2

# Indice

<b>I</b>	<b>Introduzione</b>	<b>5</b>
1	Descrizione	5
2	Release notes	6
3	Terminologia	6
4	Ulteriori informazioni	7
<b>II</b>	<b>Guida per l'amministratore</b>	<b>8</b>
5	Prerequisiti	8
6	Dove reperire i kit	8
7	Installazione e upgrade	8
	Installazione di pplot e pperl . . . . .	9
	Configurazione del router Cisco . . . . .	9
	Installazione di IPaccounting . . . . .	10
	Configurazione . . . . .	10
	Selezione dell'interprete Perl . . . . .	12
	Copia dei file di dati archiviati . . . . .	12
	Definizione dei domini, dei sottodomini e dei communication partners . . . . .	13
	Dominio di accounting . . . . .	13
	Sottodomini di accounting . . . . .	14
	Communication partners . . . . .	14
	Creazione dei report per i vecchi dati . . . . .	15
8	Raccolta dei dati	16
9	Accounting giornaliero	16
	9.1 make_all_accounting.pl - Come fare tutto con un solo comando . . . . .	16
	9.2 statistic.pl - Generazione delle liste ordinate di traffico . . . . .	18
	9.2.1 Risoluzione degli indirizzi. Caching. . . . .	18
	9.3 make_daily.pl - Generazione dei report giornalieri . . . . .	19
10	Liste di traffico	20
11	Report giornalieri	20
12	Accessibilità dei dati tramite World Wide Web	21
	12.1 Protezione delle informazioni . . . . .	21
13	Archiviazione od eliminazione dei file obsoleti	22
14	Gestione di più router	22



<b>III Guida per l'utente</b>	<b>25</b>
15 Caratteristiche dell'interfaccia utente	25
16 Simbologia nelle pagine di IPaccounting	25
17 La home page di IPaccounting	25
18 Visualizzazione dei file di definizione per i domini	27
19 Visualizzazione delle liste di traffico	27
20 Visualizzazione delle statistiche di traffico	28
20.1 Sommario "istantaneo" del traffico . . . . .	28
20.2 Andamento del traffico nel tempo . . . . .	30
20.3 Note sui grafici . . . . .	31
<b>IV Appendici</b>	<b>35</b>
A Esempio di script per la gestione di più router	35



## Parte I

# Introduzione

## 1 Descrizione

Il software IPaccounting consente di monitorare ed effettuare l'accounting dell'utilizzo di TCP/IP su un router Cisco che collega un dominio di accounting al resto del mondo.

In questo documento, con il termine *dominio di accounting* (*accounting domain*) si intende un insieme di reti il cui traffico verso il *mondo* (cioè tutto ciò che è al di fuori di tale dominio di accounting) viene monitorato per mezzo di IPaccounting. Un dominio di accounting copre generalmente tutto ciò che sta "al di qua" del router; può trattarsi di una singola rete, ma anche un'entità più complessa come un intero Autonomous System. Con il termine *sottodominio di accounting* (*accounting subdomain*) si intende invece un sottoinsieme di tale dominio, generalmente corrispondente ad una o più reti in esso comprese.

La figura 1 esemplifica questa situazione.

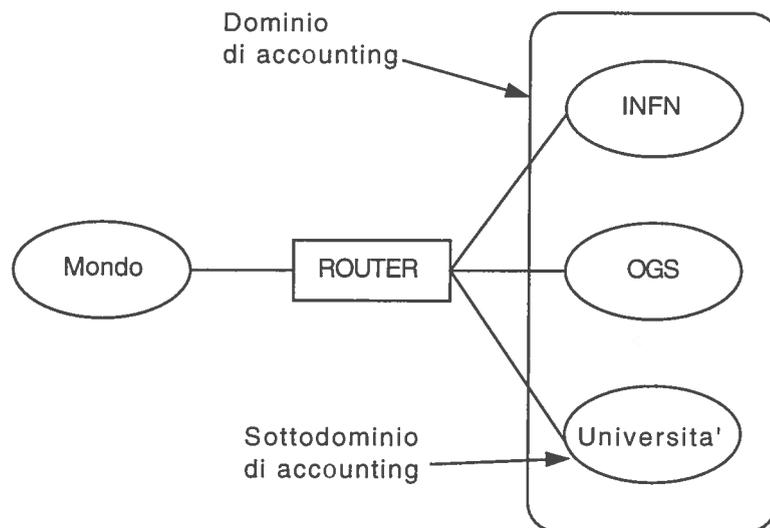


Figura 1: Dominio e sottodominio di accounting.

Questo documento è diviso in tre parti, più una dedicata alle appendici.

La prima parte, quella che state leggendo in questo momento, contiene le informazioni generali sul prodotto, ed in particolare le caratteristiche e le innovazioni rispetto alla versione precedente.

La seconda costituisce la guida per l'amministratore di IPaccounting, cioè la persona incaricata di installare, configurare e gestire il software descritto in questo documento.

La terza parte costituisce invece la guida per l'utente, ovvero la persona interessata alle statistiche prodotte da IPaccounting.

## 2 Release notes

La versione 2.0 di IPaccounting presenta notevoli innovazioni rispetto alla versione 1.0. Tali variazioni sono in buona parte basate sul feedback ottenuto dagli utenti della versione precedente.

Alcune caratteristiche particolarmente rilevanti della nuova release sono le seguenti:

- Il software è stato riscritto completamente in Perl. Ciò consente maggiore portabilità su diverse piattaforme Unix, ed anche un miglioramento delle prestazioni. La riorganizzazione ha consentito di ridurre il numero di moduli, semplificando in questo modo la gestione da parte dell'amministratore.
- È stata notevolmente potenziata l'interfaccia per l'utente, basata su HTML ed accessibile tramite World Wide Web.
- La parte grafica è ora basata sulla libreria `pgperl` (cioè sulla libreria `PGPLOT` tradotta per il linguaggio Perl).
- Il formato dei report giornalieri è stato modificato in modo da contenere una maggiore quantità di informazioni. Inoltre, il nuovo formato consente una definizione più selettiva dei dati da considerare.
- I grafici relativi ai dati raccolti sono ora generati "al volo" in risposta alle richieste espresse dall'utente tramite *form* HTML. Ciò consente di ottenere esattamente i grafici desiderati senza dover costruire a priori tutti i grafici di potenziale interesse.
- La nuova release consente una gestione semplificata anche nel caso si desideri monitorare più di un router, grazie alle aumentate possibilità di configurazione.

In breve, la nuova versione risulta essere più potente e flessibile, ma anche più semplice da amministrare ed utilizzare, rispetto alla versione precedente.

## 3 Terminologia

Abbiamo già descritto in precedenza i concetti di "dominio di accounting" e "sottodominio di accounting". IPaccounting 2.0 utilizza altre definizioni per identificare entità con un significato preciso. È bene quindi chiarire fin d'ora questi concetti, che compaiono spesso in questo documento e nei report di IPaccounting.

I sottodomini di accounting vengono classificati in "ordinari" (*ordinary subdomains*) e "speciali" (*special subdomains*). I primi devono essere tra loro complementari: essi non possono condividere sottoreti o nodi, in modo da permettere il calcolo di percentuali e totali coerenti e significativi. Di solito questo tipo di sottodomini è il più usato.

I sottodomini speciali, invece, non sottostanno ad alcuna restrizione: essi possono essere liberamente costruiti a seconda delle esigenze, comprendendo anche nodi o sottoreti appartenenti ad un altro sottodominio, ordinario o speciale che sia. Ad esempio, è possibile costruire un sottodominio speciale comprendente tutti i nodi che svolgono funzioni di server `httpd` per i vari sottodomini ordinari di un dominio di accounting, in modo da evidenziare il traffico generato da tali macchine, oppure monitorare uno specifico nodo appartenente ad un dominio ordinario, che svolge funzioni particolari (server di news, gateway di posta elettronica, repository di documenti in formato elettronico, ecc.). I calcoli dei totali basati

sui sottodomini speciali non sono direttamente confrontabili con quelli prodotti sulla base dei sottodomini ordinari, proprio a causa della libertà di definizione. Di conseguenza i sottodomini speciali possono essere visti come uno strumento per monitorare alcune situazioni particolari, piuttosto che per un normale accounting dei sottodomini.

Un altro concetto fondamentale è quello di *communication partner*. I communication partner sono definizioni di domini nel “mondo” (tipicamente ma non necessariamente al di fuori del dominio di accounting considerato), dei quali interessa monitorare il traffico da/per il dominio di accounting stesso. Ad esempio, può essere interessante monitorare il traffico generato dal dominio di accounting (o dai suoi sottodomini) verso l'Italia, oppure verso il mondo intero, oppure verso le reti che non appartengono all'Italia, e così via.

Facciamo notare che tutte le definizioni di dominio, sottodominio e partner sono completamente a carico dell'amministratore. Non sono eseguiti controlli di alcun tipo sulla coerenza o correttezza di tali definizioni.

## 4 Ulteriori informazioni

La home page di IPaccounting, accessibile tramite World Wide Web, si trova all'URL:

<http://www.ts.infn.it/computing/IPaccounting/>

## Parte II

# Guida per l'amministratore

## 5 Prerequisiti

IPaccounting è stato testato in ambiente Digital Unix (versione 3.2c e 4.0a), ma non vi dovrebbero essere problemi su sistemi Unix diversi dove siano disponibili tutti i software richiesti.

IPaccounting 2.0 è interamente realizzato in linguaggio Perl. È necessaria almeno la versione 5.003 dell'interprete Perl.

Dal momento che l'interfaccia utente per l'accesso alle statistiche è completamente basata su HTML, sulla macchina dove IPaccounting viene installato deve essere presente un server httpd. Il prodotto è stato testato in coabitazione con un server httpd Apache 1.2, ma non vi dovrebbero essere problemi con server diversi.

Sono inoltre necessarie le librerie grafiche PGPLOT versione 5.1.1 [2] e pgperl versione 1.0b [3].

Il kit di IPaccounting comprende inoltre la libreria cgi-lib [4].

## 6 Dove reperire i kit

Il kit di IPaccounting e quelli delle librerie necessarie al suo funzionamento sono tutti reperibili tramite FTP anonymous.

**IPaccounting 2.0:** Il kit è reperibile all'indirizzo `ftp://ftp.ts.infn.it/pub/unix/-IPaccounting/IPaccounting.2.0.tar.gz`.

**pgplot 5.1.1:** Il puntatore al kit si trova consultando l'URL `http://astro.caltech.edu/~tjp/pgplot/`. Copia del kit è reperibile anche all'indirizzo `ftp://ftp.ts.infn.it/pub/unix/IPaccounting/pgplot5.1_for_IPaccounting.tar.gz`. Questa copia è leggermente modificata in modo da includere tutti i driver necessari ad IPaccounting per un sistema Digital Unix, senza bisogno di effettuare modifiche in fase di installazione.

**pgperl 1.0:** Il puntatore al kit si trova consultando l'URL `http://www.aao.gov.au/local/www/kgb/pgperl`. Copia del kit è reperibile all'indirizzo `ftp://ftp.ts.infn.it/pub/unix/IPaccounting/PGPLOT-1.0.tar.gz`.

## 7 Installazione e upgrade

I seguenti passi descrivono le operazioni da effettuare sia in caso di installazione ex-novo che di upgrade dalla versione 1.0 di IPaccounting. Nel secondo caso, alcune operazioni supplementari consentono di salvaguardare i file di dati accumulati e di convertirli, se necessario, ad un formato compatibile con la nuova versione.

Per ogni passo, viene indicato se esso debba essere eseguito durante un'installazione, un upgrade oppure in entrambi i casi.

In tutti gli esempi, si assume che l'eventuale versione precedente di IPaccounting sia stata installata in `/IPaccounting_1.0`, e che la nuova venga installata in `/IPaccounting`.

### 1. Eliminazione di IPaccounting 1.0 da crontabs (UPGRADE)

In fase di upgrade, la prima cosa da fare è l'eliminazione della versione precedente di IPaccounting da crontabs, in modo da bloccare l'acquisizione dei dati da parte della versione precedentemente installata. Nel file di crontabs dell'utente che esegue IPaccounting (ad es. `/var/spool/cron/crontabs/root`) si dovrebbero trovare istruzioni simili alle seguenti:

```
0,10,20,30,40,50 * * * * /IPaccounting_1.0/collect_accounting_data >
/dev/null 2>&1
55 23 * * * /IPaccounting_1.0/make_all_accounting >
/IPaccounting_1.0/make_all_accounting.log 2>&1
```

È necessario quindi editare il file, togliere le istruzioni in questione e poi far ripartire cron in modo da fermare definitivamente l'acquisizione dei dati.

### 2. Installazione di pgplot e pgperl. (INSTALLAZIONE E UPGRADE)

In caso pgplot 5.1.1 e pgperl 1.0 non siano disponibili sul sistema dove si intende installare IPaccounting, è necessario procedere all'installazione di tali librerie.

#### • Installazione di pgplot 5.1.1

Il kit contiene il file `install.txt` con le istruzioni per l'installazione.

Devono essere installati *almeno* i driver `/GIF`, `/VGIF`, `/PS`, `/VPS`, `/CPS`, `/VCPS`, abilitandoli nel file `drivers.list`.

Su piattaforma Digital Unix il file `drivers/gidriv.f` deve essere modificato come descritto in `sys_osf1/aaaread.me`, altrimenti i driver GIF non funzionano correttamente.

Nel caso abbiate importato la versione del kit disponibile su `ftp.ts.infn.it` e lavoriate su Digital Unix, i driver sono già definiti, ed il file `drivers/gidriv.f` è modificato appropriatamente.

È necessario inoltre definire la variabile di ambiente `PGPLOT_DIR` come suggerito nel file di installazione.

Infine, è necessario installare anche il *C binding* `cpg`, altrimenti la successiva installazione di pgperl è destinata a fallire.

#### • Installazione di pgperl 1.0

Il kit contiene il file `BUILDING` con le istruzioni per l'installazione. Tali istruzioni vanno eseguite tutte, esclusa la reinstallazione dei file di pgplot (il kit di pgperl ne contiene una versione più o meno "standard"), per evitare di sovrascrivere i driver di pgplot generati al passo precedente.

### 3. Configurazione del router Cisco. (INSTALLAZIONE)

Prima di poter attivare la procedura di accounting, è necessario configurare il router Cisco al fine di abilitare l'esecuzione di comandi remoti mediante chiamata di shell remota (*rsh*). Si procede nel seguente modo:

- Si crea un entry nel database di autenticazione del Cisco per un utente remoto cui è consentito eseguire comandi *rsh* sul router in questione:

```
rcmd remote-host nome-utente-locale indirizzo-IP-host nome-utente-remoto
```

Ad esempio:

```
rcmd remote-host root 140.105.6.158 root
```

Questo abilita l'utente *root* dall'host 140.105.6.158 ad eseguire comandi *rsh* sul router.

- Di seguito, si abilita il supporto di comandi *rsh* con il seguente comando:

```
rsh-enable
```

e si abilita il comando

```
ip accounting output-packets
```

su tutte le interfacce che si intendono monitorare.

- È consigliabile modificare il default (512 entry) per quanto riguarda il numero di entry di accounting da conservare nella memoria del router finché non vengono prelevate da IPaccounting (ad esempio ogni 10 minuti), perchè si potrebbero perdere dati significativi. Un valore accettabile potrebbe essere uguale a 10000. Il comando da usare è il seguente:

```
ip accounting-threshold 10000
```

#### 4. Installazione di IPaccounting. (INSTALLAZIONE E UPGRADE)

Il kit di IPaccounting dev'essere espanso in una directory creata appositamente a priori. In caso di upgrade dalla versione 1.0, create una directory diversa da quella in cui si trova la versione precedente, ed alla fine delle operazioni eliminate la vecchia directory rinominando, se desiderato, quella nuova.

Tutte le operazioni descritte in seguito si intendono eseguite nella home directory di IPaccounting 2.0, ovvero la directory dove IPaccounting è stato espanso.

#### 5. Configurazione. (INSTALLAZIONE E UPGRADE)

Il kit comprende il file di configurazione *configuration.pl*, il quale include le definizioni per un insieme di variabili utilizzate da tutti i moduli di IPaccounting.

Questo file dev'essere editato e modificato a seconda delle esigenze. La prima parte del file (*customizable section*) comprende le definizioni aggiornabili da parte dell'amministratore; la seconda parte (indicata chiaramente nel file) non deve essere modificata.

I parametri definiti in *configuration.pl* sono i seguenti:

**ROUTER\_NAME** Indirizzo o descrizione del router da monitorare. Questa definizione è utilizzata solo nei report e nei grafici, non ha alcun valore per la raccolta dei dati.

```
$ROUTER_NAME="trieste-gw1.ts.infn.it";
$ROUTER_NAME="Main gateway in Trieste";
```

**DOMAIN\_MAME** Stringa descrittiva del dominio di accounting monitorato.

```
$DOMAIN_NAME="AS5449";
$DOMAIN_NAME="Scientific network in Trieste";
```

**HOMEDIR** Nome della directory in cui IPaccounting 2.0 è stato installato.

```
$HOMEDIR="/IPaccounting";
```

**ACCOUNTING\_FILE** Nome del file di accounting in cui verranno accumulati i dati provenienti dal router.

```
$ACCOUNTING_FILE="$HOMEDIR/IPaccounting.dat";
```

**RAW\_ARCHIVE\_PATH** Nome della directory in cui verranno archiviati i dati provenienti dal router, giorno per giorno.

```
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data_archive";
```

**ARCHIVE\_PATH** Nome della directory nella quale verranno archiviate le liste di traffico per sorgente e destinazione prodotte da IPaccounting, giorno per giorno.

```
$ARCHIVE_PATH="$HOMEDIR/archive";
```

**ACCOUNTING\_DOMAIN** Nome del file contenente la lista delle reti che compongono il dominio di accounting. In caso di upgrade, si consiglia l'utilizzo del nome `accounting_domain.dat` al posto della denominazione `subdomains.list` usata nella versione precedente.

```
$ACCOUNTING_DOMAIN="$HOMEDIR/accounting_domain.dat";
```

**DAILY\_PATH** Nome della directory in cui verranno archiviati i report giornalieri compatti, estratti dalle liste di traffico, ed utilizzati per la realizzazione dei grafici e delle tabelle.

```
$DAILY_PATH="$HOMEDIR/daily_reports";
```

**NSLOOKUP\_COMMAND** Sintassi del comando `nslookup` da utilizzare per la traduzione degli indirizzi dei nodi. La sintassi è dipendente dalla piattaforma, specialmente per quanto riguarda le opzioni.

Si consiglia di limitare il numero di retry al fine di ridurre il tempo di ricerca.

```
$NSLOOKUP_COMMAND="nslookup -retry=1";
```

**IMAGES\_URL** URL che consente l'accesso alla directory `images` di IPaccounting tramite World Wide Web.

```
$IMAGES_URL="http://www.ts.infn.it/IPaccounting/";
```

Si consiglia a questo punto di creare un link dall'albero del server `httpd` verso la directory `images` di IPaccounting, in modo da realizzare subito la raggiungibilità di tale directory, ad esempio:

```
# ln -s /IPaccounting/images
    /usr/local/etc/httpd/htdocs/IPaccounting
```

**CGI\_URL** URL che punta alla sottodirectory `cgi-bin` di IPaccounting.

```
$CGI_URL="http://www.ts.infn.it/cgi-bin/IPaccounting/";
```

Si consiglia a questo punto di creare un link dall'albero `cgi` del server `httpd` verso la sottodirectory di IPaccounting, in modo da realizzare subito la raggiungibilità di tale directory, ad esempio:

```
# ln -s /IPaccounting/cgi-bin
    /usr/local/etc/httpd/cgi-bin/IPaccounting
```

È inoltre necessario cambiare l'owner della directory `cgi-bin` di `IPaccounting`, e dei file in essa contenuti, in modo che ne risulti proprietario l'account che gestisce il server `httpd`. Si consiglia quindi di eseguire i seguenti comandi (supponendo che l'account che gestisce il server `httpd` si chiami `www`):

```
# chown -R www cgi-bin
# chmod -R 744 cgi-bin
```

**CACHE\_FILE** Nome del file di cache utilizzato da `IPaccounting` per ricercare con maggiore efficienza le traduzioni degli indirizzi IP.

```
$CACHE_FILE="$HOMEDIR/IPaccounting.cache";
```

**ORDINARY\_SUBDOMAINS\_PATH** Nome della directory contenente le definizioni dei sottodomini di `accounting` ordinari.

```
$ORDINARY_SUBDOMAINS_PATH="$HOMEDIR/ordinary_subdomains";
```

**SPECIAL\_SUBDOMAINS\_PATH** Nome della directory contenente le definizioni dei sottodomini di `accounting` speciali.

```
$SPECIAL_SUBDOMAINS_PATH="$HOMEDIR/special_subdomains";
```

**PARTNERS\_PATH** Nome della directory contenente le definizioni dei `communication partner`.

```
$PARTNERS_PATH="$HOMEDIR/communication_partners";
```

**ADMINISTRATOR** Nominativo e/o indirizzo di posta elettronica dell'amministratore locale di `IPaccounting`.

In caso abbiate deciso di indicare l'indirizzo di posta elettronica, si fa notare che il carattere "@" (che in Perl ha un significato particolare) va prefissato dal carattere "\".

```
$ADMINISTRATOR="Claudio Strizzolo (strizzolo\@trieste.infn.it)";
```

I parametri *devono* essere tutti definiti, eventualmente assegnando loro valori non significativi in caso si ritenga di non utilizzarli.

## 6. Selezione dell'interprete Perl. (INSTALLAZIONE E UPGRADE)

Per default, l'interprete Perl utilizzato deve trovarsi in `/usr/local/bin/perl`. Quando si desidera utilizzare un diverso interprete, è necessario eseguire la script `set_perl_interpreter` specificando il nome dell'interprete da utilizzare. Ad esempio:

```
# sh set_perl_interpreter /usr/local/bin/perl5
```

Questa script ridefinisce l'interprete Perl in tutte le script incluse nel kit di `IPaccounting`.

## 7. Copia dei file di dati archiviati (UPGRADE)

In fase di `upgrade` è possibile conservare i file di dati archiviati dalla versione precedente, importandoli nell'albero di `IPaccounting 2.0`. Ciò può essere fatto con le seguenti istruzioni:

```
# mv /IPaccounting_1.0/archive/* /IPaccounting/archive
# mv /IPaccounting_1.0/raw_data_archive/* /IPaccounting/raw_data_archive
```

Per i comandi sopra indicati, utilizzare i path definiti in precedenza nel file di configurazione.

## 8. Definizione dei domini, dei sottodomini e dei communication partners. (INSTALLAZIONE E UPGRADE)

Le definizioni dei domini, dei sottodomini e dei communication partners vengono effettuate creando un file per ogni entità da definire. Il file in questione contiene la lista dei nodi e/o delle reti che appartengono a tale entità, un nodo o rete per ogni riga. È possibile anche escludere un nodo o una rete facendo precedere l'indirizzo dal carattere "-". I commenti sono invece preceduti dal carattere "#". Ad esempio:

```
#
# Questo e' un esempio di sottodominio
#
# Il sottodominio include le reti 140.105. e 147.122.,
# escluse le sottoreti 140.105.6 e 140.105.7
140.105.
147.122.
-140.105.6. # Escludiamo una rete
-147.122.7. # Anzi, due...
```

È inoltre ammesso l'utilizzo della wildcard "\*", con il significato usuale di sostituire una sequenza qualsiasi di caratteri.

Tutti i file di definizione per queste entità possono essere eliminati o modificati in qualsiasi momento successivo.

Con riferimento in particolare ai sottodomini di accounting ordinari e speciali, ma anche ai communication partner, si consiglia di non scegliere nomi troppo lunghi (possibilmente massimo 12 caratteri), per evitare che essi risultino troncati nei grafici.

- **Dominio di accounting**

In fase di installazione, deve essere creato il file contenente la lista delle reti che compongono il dominio di accounting considerato. Il nome del file dev'essere quello definito con il parametro ACCOUNTING\_DOMAIN nel file di configurazione. Ad esempio:

```
#
# This is the accounting domain AS5449
#
140.105.
147.122.
193.43.109.
193.205.241.
```

In fase di upgrade, è sufficiente rinominare il vecchio file di definizione di IPaccounting 1.0, ad esempio:

```
# mv /IPaccounting_1.0/subdomains.list
    /IPaccounting/accounting_domain.dat
```

- **Sottodomini di accounting**

In fase di installazione, è necessario creare un file per ogni sottodominio ordinario di accounting nella directory specificata dal parametro `ORDINARY_SUBDOMAINS_PATH` nel file di configurazione. Il file deve contenere una lista in cui sono elencate le sottoreti e i nodi IP che appartengono al sottodominio di interesse.

Il nome del file identificherà il dominio nelle pagine HTML che vi faranno riferimento.

È a cura del gestore verificare che i sottodomini ordinari siano effettivamente complementari tra loro, in modo che i calcoli delle percentuali e dei totali risultino coerenti. Sempre a cura del gestore verificare che la lista delle reti e/o dei nodi creata nel file contenente il dominio di accounting comprenda effettivamente tutte le reti di cui si compongono i sottodomini.

Eventualmente, è possibile creare in questa fase anche i file di definizione per i sottodomini speciali, nella directory specificata dal parametro `SPECIAL_SUBDOMAINS_PATH` nel file di configurazione.

Se state effettuando un upgrade, è possibile recuperare le definizioni dei sottodomini assegnate alla versione precedente di IPaccounting, semplicemente rinominando i file che le contengono. Di solito si tratta di definizioni corrispondenti a sottodomini ordinari, quindi può essere sufficiente un comando come il seguente:

```
# mv /IPaccounting_1.0/subdomains/*
    /IPaccounting/ordinary_subdomains
```

È bene comunque verificare anche in questo caso la coerenza e la correttezza delle informazioni.

- **Communication partners**

Sia che stiate effettuando un'installazione che un upgrade, è necessario definire un insieme di *communication partner*, dei quali interessa monitorare il traffico da/verso il dominio di accounting considerato. A tale scopo, bisogna creare un file per ogni communication partner nella directory specificata dal parametro `PARTNERS_PATH` nel file di configurazione. Il file deve contenere una lista in cui sono elencate le sottoreti e i nodi IP che appartengono al communication partner in questione.

Nella versione 1.0 di IPaccounting, i communication partners erano fissi, mentre ora è possibile configurarli a piacere. Per questo motivo la loro definizione è necessaria anche se si sta effettuando un upgrade.

Per default, viene definito a priori il communication partner `ANYWHERE` che comprende tutti i nodi esistenti. La definizione di questo communication partner è la seguente (effettuata intrinsecamente al programma):

```
#
# The ANYWHERE communication partner
#
*
```

Un communication partner che risulta spesso utile è quello comprendente tutti gli oggetti esterni al dominio di accounting, ad esempio:

```
#
# All the world, but accounting domain AS5449
#
*
-140.105.
-147.122.
-193.43.109.
-193.205.241.
```

Spesso è utile differenziare il traffico da/per la nazione in cui il dominio di accounting si trova, dal resto del mondo. Il problema, in questo caso, è principalmente quello di ottenere una lista aggiornata delle reti appartenenti alla nazione di interesse. Nel caso dell'Italia, una lista aggiornata è reperibile presso il GARR-NIS (<ftp://ftp.nis.garr.it/garr/nis/dbase/lists/-elenco-reti-ip-registrate>) oppure presso RIPE (<ftp://ftp.ripe.net/ripe/dbase/split/ripe.db.inetnum.gz>). Tali elenchi vanno poi formattati in modo appropriato alla sintassi di IPaccounting; possibilmente, si consiglia di ridurre la dimensione di tali liste eliminando duplicazioni e/o raggruppando eventuali entry con parti in comune, al fine di aumentare l'efficienza delle procedure di ricerca di IPaccounting. Una copia dell'elenco di RIPE, opportunamente ridotta ed adattata per IPaccounting, è disponibile (ed aggiornata di tanto in tanto) presso <ftp://ftp.ts.infn.it/pub/unix/IPaccounting/Italy.nets>.

Una volta ottenuta la lista delle reti appartenenti alla nazione, è banale ricavare quella delle reti che non le appartengono, aggiungendo la wildcard "\*" e facendo precedere ogni indicazione di rete dal simbolo ".". Un elenco delle reti non assegnate all'Italia, ricavato dalla lista di RIPE, è disponibile presso [ftp://ftp.ts.infn.it/pub/unix/IPaccounting/outside\\_Italy.nets](ftp://ftp.ts.infn.it/pub/unix/IPaccounting/outside_Italy.nets).

## 9. Creazione dei report per i vecchi dati. (UPGRADE)

Come detto in precedenza, IPaccounting 2.0 genera dei report con un formato diverso da quello della versione precedente. Il nuovo formato consente maggiore flessibilità, ed anche la possibilità di immagazzinare una maggiore quantità di informazioni.

Un inconveniente consiste nel fatto che il nuovo formato non è compatibile con quello utilizzato in precedenza. Si rende quindi necessaria la generazione dei report relativi ai dati finora immagazzinati, in modo da renderli compatibili con la nuova versione del prodotto. A tale scopo si può utilizzare la script `upgrade_daily.pl`. Essa crea, nella directory indicata dal parametro `DAILY_PATH` del file di configurazione, un report per ogni file di dati che si trova nella directory indicata dal parametro `ARCHIVE_PATH`. Se è stata eseguita la copia dei file di dati come indicato nel passo numero 7 di questa guida all'installazione, tale directory dovrebbe contenere tutti i file di dati che erano stati raccolti dalla precedente versione di IPaccounting. È sufficiente quindi immettere il comando:

```
# upgrade_daily.pl
```

Questa script può impiegare un tempo piuttosto lungo per generare i report, specialmente se il numero di file di dati è elevato.

## 8 Raccolta dei dati

La raccolta dei dati dal Cisco dev'essere effettuata ad intervalli periodici in modo da prelevare via via tutte le informazioni che vengono memorizzate dal router. Questo compito può essere eseguito in modo automatico aggiungendo una linea come la seguente al file `/var/spool/cron/crontabs/root`:

```
0,10,20,30,40,50 * * * * /IPaccounting/collect_accounting_data.pl
router-address data-file > /dev/null 2>&1
```

Al posto di `router-address` inserire l'indirizzo del router da monitorare. Si può utilizzare sia l'indirizzo numerico che l'hostname, quest'ultimo in forma estesa o abbreviata (qualora esso sia risolvibile via `/etc/hosts` o da `bind`).

Al posto di `data-file` inserire il nome del file in cui verranno scaricati via via i dati relativi all'accounting (identificato dalla variabile `ACCOUNTING_FILE` nel file di configurazione).

Ad esempio:

```
0,10,20,30,40,50 * * * * /IPaccounting/collect_accounting_data.pl
trieste-gw1.ts.infn.it /IPaccounting/IPaccounting.dat > /dev/null 2>&1
```

Questa entry in `crontabs` esegue automaticamente ogni dieci minuti la procedura di raccolta dei dati.

La script `collect_accounting_data.pl` non si basa sui dati contenuti nel file `configuration.pl`, ma utilizza esclusivamente i parametri che le vengono passati.

## 9 Accounting giornaliero

L'accounting giornaliero si compone di due fasi:

1. Generazione delle liste ordinate di traffico in base alla sorgente, alla destinazione ed alle coppie sorgente-destinazione.
2. Generazione dei report che verranno utilizzati in fase di creazione dei grafici e delle tabelle.

La seconda fase può essere eseguita solo se la prima è stata completata, in quanto essa si basa sulle liste generate nella prima fase.

### 9.1 `make_all_accounting.pl` - Come fare tutto con un solo comando

L'intera sequenza di accounting può essere eseguita utilizzando una singola script, che richiama le script preposte al completamento delle due fasi. La script in questione è `make_all_accounting.pl`. La sintassi completa per questa script è la seguente:

```
# make_all_accounting.pl [date] [-nnumber-of-entries] [-a]
[-cconfiguration-file]
```

Il parametro `date`, se definito, deve seguire immediatamente il nome della script, con eventuali opzioni di seguito ad esso. Indica la data cui si riferiscono i dati da elaborare. Se omesso, viene considerata la data corrente.

Le opzioni hanno il seguente significato:

**-n number-of-entries** - In fase di creazione delle liste di traffico, IPaccounting tenta di risolvere gli indirizzi ricavando gli hostname, per dare maggiore comprensibilità alle liste risultanti. Tale operazione può richiedere un tempo lunghissimo, tanto maggiore quanto è grande il numero di indirizzi da risolvere. Per ridurre questo tempo, IPaccounting utilizza due meccanismi: una cache (di cui si parla più diffusamente nella sezione 9.2) e, per l'appunto, l'opzione **-n**: quest'ultima stabilisce il numero di entry (al top della lista, si tratta quindi delle entry relative ai nodi con maggior traffico) per le quali verrà tentata la risoluzione degli indirizzi. Limitando questo numero a 500, o 1000, per esempio, i tempi di elaborazione diminuiscono drasticamente, e le liste prodotte contengono comunque tutte le informazioni utili per le situazioni di maggior traffico, omettendo invece le traduzioni per quelle che, di solito, sono di minor interesse.

Se questa opzione viene omessa, viene effettuata la risoluzione di tutti gli indirizzi.

**-a** - La prima operazione eseguita dalla script di accounting consiste nel rinominare il file contenente i dati prelevati dal Cisco (identificato dalla variabile `ACCOUNTING_FILE` nel file di configurazione) nella directory dove sono salvati i raw data (ved. file di configurazione), con un nome del tipo `IPaccounting.date`, dove *date* è la data corrente. Ciò viene fatto sia per salvare i dati nella loro locazione definitiva, che per ripulire il file di dati dalle informazioni del giorno precedente, di modo che le nuove vengano salvate in un file diverso.

Se viene specificata l'opzione **-a**, tale operazione viene evitata. Ciò può essere utile per rielaborare un raw data file che sia già stato salvato, ad esempio nel caso in cui l'accounting abbia prodotto degli errori dopo che il file è stato rinominato: in questo modo è possibile effettuare l'accounting se, nella prima esecuzione, ci sono stati dei problemi.

**-c configuration-file** - Fino a questo punto, abbiamo sempre detto che il file di configurazione si chiama `configuration.pl`. Questo non è del tutto vero: in particolare se ci sono più router da monitorare, è per forza necessario creare un file di configurazione diverso per ogni router. In tal caso è ovvio che tutte le operazioni di accounting devono essere correttamente parametrizzate in modo da prelevare la configurazione dal file giusto. L'opzione **-c** serve a specificare il file di configurazione da utilizzare. Maggiori informazioni a riguardo nel capitolo 14, dove si parla per l'appunto della gestione di più router.

Normalmente, l'accounting può essere eseguito automaticamente al termine della giornata, ad esempio aggiungendo una linea come la seguente al file `/var/spool/cron/crontabs/root`:

```
58 23 * * * /IPaccounting/make_all_accounting.pl -n500 >
/IPaccounting/make_all_accounting.log 2>&1
```

Nell'esempio, la script viene eseguita ogni giorno alle ore 23:58. Il parametro *date* è stato omesso in modo che venga considerata la data corrente. Viene effettuata la risoluzione delle prime 500 entry delle liste di traffico. L'output della script è stato indirizzato verso il file `make_all_accounting.log`; in questo file verranno riportate diverse segnalazioni nel corso dell'esecuzione, in modo che sia possibile rendersi conto di eventuali problemi.

Come detto in precedenza, `make_all_accounting.pl` richiama due script che si occupano della produzione effettiva delle liste e delle statistiche. Le prossime due sezioni di

questo documento descrivono brevemente alcune caratteristiche salienti di tali script, e soprattutto forniscono alcune informazioni utili alla gestione di questa parte dell'accounting.

## 9.2 `statistic.pl` - Generazione delle liste ordinate di traffico

La script `statistic.pl` esegue le seguenti operazioni:

1. Sposta il file in cui sono salvati i dati raccolti dal router (ved. parametro `ACCOUNTING_FILE`) nella directory dove vengono conservati i raw data file (ved. parametro `RAW_ARCHIVE_PATH`); il nome del file diventa `IPaccounting.date`.
2. A partire dai dati contenuti nel raw data file `IPaccounting.date`, genera le tre liste di traffico per sorgente (`acc_source.date`), per destinazione (`acc_target.date`) e per coppia sorgente-destinazione (`acc_source_target.date`). Le liste vengono create nella directory identificata dal parametro `ARCHIVE_PATH`.

Per maggiori informazioni sulle liste di traffico prodotte, ved. capitolo 10.

La sintassi per l'esecuzione di `statistic.pl` (si consiglia comunque di eseguire questa script indirettamente, tramite `make_all_accounting.pl`) è la seguente:

```
# statistic.pl [date] [-nnumber-of-entries] [-a]
               [-cconfiguration-file] [-m]
```

Il significato delle opzioni `-n`, `-a` e `-c` è lo stesso descritto a proposito delle opzioni omonime di `make_all_accounting.pl` nella sezione 9.1.

L'opzione `-m` è l'opposto dell'opzione `-a`: verrà eseguito esclusivamente lo spostamento del file contenente i dati prelevati dal Cisco nella directory contenente i raw data (ved. file di configurazione), con un nome del tipo `IPaccounting.date`. Questa opzione di solito è utilizzata solo per particolari gestioni di più router.

### 9.2.1 Risoluzione degli indirizzi. Caching.

In fase di generazione delle liste di traffico, `IPaccounting 2.0` utilizza una cache per aumentare l'efficienza nella risoluzione degli indirizzi dei nodi che compaiono nella statistica. La cache consiste di un file (identificato dal parametro `CACHE_FILE` del file di configurazione) in cui viene archiviata la lista degli indirizzi "risolti", con le loro risoluzioni, man mano che queste vengono effettuate, ad esempio:

```
128.141.201.71 na47sun05.cern.ch
140.105.6.100 unixts.ts.infn.it
147.122.11.23 neumann.sissa.it
147.162.75.2 ?
```

Ogni volta che `IPaccounting` deve effettuare la risoluzione di un indirizzo, `IPaccounting` tenta i seguenti passi, in sequenza:

1. Verifica se l'indirizzo è nella cache. In questo caso ne ricava la risoluzione direttamente.
2. Utilizzando il comando di `nslookup` definito dal parametro `NSLOOKUP_COMMAND`, viene tentata la risoluzione dell'indirizzo. Se questa ha successo, la script scrive nel file di cache l'indirizzo e la risoluzione. Se essa fallisce, invece, assume che l'hostname non è definito, e lo traduce con "?" (ved. esempio precedente).

In questo modo, nelle successive creazioni delle liste, IPaccounting dispone già di un certo numero di risoluzioni salvate in cache, e quindi non ha bisogno di interpellare ogni volta il DNS, guadagnando così efficienza.

Ci sono però due aspetti di cui bisogna tenere conto:

1. La cache tende ad aumentare di dimensioni. Ciò può creare problemi di spazio su disco.
2. Le informazioni memorizzate in cache possono “invecchiare”: ad un indirizzo memorizzato in cache potrebbe essere stato assegnato nel tempo un hostname diverso, oppure un nodo “irrisolto” potrebbe essere stato registrato nel DNS dopo che IPaccounting aveva già memorizzato l’entry “irrisolta” in cache, e così via.

Si consiglia, pertanto, di ripulire la cache con regolarità, eliminando periodicamente il file di cache in modo che IPaccounting riprenda tutte le informazioni dal DNS. Anche questa operazione può essere inserita, con periodicità ad esempio di una settimana, nel file di `crontab`.

In caso l’esecuzione della script `statistic.pl` venga interrotta (manualmente o per un crash), sia nel caso che essa sia stata eseguita a mano che richiamata da `make_all_accounting.pl`, può capitare che la cache resti corrotta. In caso di interruzione, si consiglia di editare il file di cache, e di controllare l’ultima riga; se essa risulta incompleta, è necessario eliminarla.

### 9.3 `make_daily.pl` - Generazione dei report giornalieri

La script `make_daily.pl` genera un report giornaliero a partire dalla lista `acc_source-target.date` prodotta da `statistic.pl`. Il report contiene un sommario del traffico della giornata, per i sottodomini di accounting ed i communication partner di interesse. Le informazioni contenute nel report verranno utilizzate per la generazione delle tabelle e dei grafici accessibili tramite World Wide Web.

I report giornalieri vengono conservati nella directory identificata dal parametro `DAI-  
LY_PATH`, e sono denominati `daily.date`. In tale directory si consiglia di conservare *esclusivamente* i file in questione.

Per maggiori informazioni sui report giornalieri, ved. capitolo 11.

La sintassi per l’esecuzione di `make_daily.pl` (si consiglia comunque di eseguire questa script tramite `make_all_accounting.pl`) è la seguente:

```
# make_daily.pl date [-c configuration-file]
```

In questo caso il parametro `date` è obbligatorio. Il significato dell’opzione `-c` è lo stesso descritto a proposito dell’omonima opzione di `make_all_accounting.pl` nella sezione 9.1.

`make_daily.pl` confronta ogni indirizzo presente nelle liste di traffico con le definizioni dei vari sottodomini e communication partner. In questo modo, oltre a determinare la corretta appartenenza di un nodo ad un sottodominio, essa è in grado di individuare (e segnalare) eventuali nodi appartenenti al dominio di accounting ma non definiti in alcun sottodominio.

## 10 Liste di traffico

Ogni giorno vengono prodotte tre liste di traffico, in formato ASCII, i cui dati vengono estrapolati direttamente dal raw data file contenente le informazioni raccolte dal router.

Le liste sono conservate nella directory specificata dal parametro `ARCHIVE_PATH` del file di configurazione.

Le tre liste sono le seguenti:

- Lista per sorgente (file `acc_source.date`); contiene l'elenco, ordinato in base al numero di byte trasferiti, di tutti i nodi che hanno spedito pacchetti transitati attraverso il router in esame, appartenenti o no al dominio di accounting.

Per ogni nodo, la lista indica indirizzo, hostname e numero di byte trasferiti:

```
193.205.245.5 king.nis.garr.it 5162398
140.105.16.91 sphe1.ictp.trieste.it 5131938
140.105.6.99 cosine-gw.infn.it 4885588
193.232.223.10 ? 4794760
140.105.13.15 sci.area.trieste.it 4783823
```

- Lista per destinazione (file `acc_target.date`); contiene l'elenco, ordinato in base al numero di byte trasferiti, di tutti i nodi che hanno ricevuto pacchetti transitati attraverso il router in esame, appartenenti o no al dominio di accounting.

Il formato di questa lista è analogo a quello della lista precedente.

- Lista per coppia sorgente-destinazione (file `acc_source_target.data`); contiene l'elenco, ordinato in base al numero di bytes trasferiti, di ogni coppia sorgente-destinatario che abbia effettuato traffico attraverso il router in esame.

Per ogni coppia vengono indicate le informazioni di sorgente e destinatario, ed il numero di byte trasferiti:

```
147.162.100.180 giotto.unipd.it 140.105.6.73 ? 235097
129.187.181.23 ? 140.105.6.99 cosine-gw.infn.it 234645
131.154.1.4 server1.infn.it 140.105.6.153 axts03.ts.infn.it 234421
```

In tutte le liste, il simbolo “?” al posto dell’hostname indica che non è stata possibile la risoluzione dell’indirizzo tramite DNS. Il simbolo “-” identifica invece le entry per le quali la risoluzione non è stata eseguita perchè è stata imposta, da parte dell’amministratore, una limitazione sul numero di top entry delle quali si desidera la risoluzione.

## 11 Report giornalieri

I report giornalieri contengono un sommario del traffico in una determinata giornata, per i sottodomini di accounting ed i communication partner di interesse. Le informazioni contenute nei report vengono utilizzate per la creazione delle tabelle e dei grafici accessibili tramite World Wide Web.

I report sono conservati nella directory identificata dal parametro `DAILY_PATH` del file di configurazione.

Ogni report si presenta come un elenco di entry ognuna delle quali è così composta:

*sottodominio communication-partner byte-trasmessi byte-ricevuti*

Ogni entry rappresenta i totali in byte trasmessi e ricevuti dal sottodominio di accounting indicato rispettivamente verso e dal communication partner in questione. Ad esempio:

```
INFN * 1446525134 299621328
INFN Italy 99609556 136211570
INFN outside_Italy 1346915578 163409758
INFN world_outside_AS5449 1382869390 236502771
Universita * 165891268 563306
Universita Italy 165891268 563306
Universita outside_Italy 0 0
Universita world_outside_AS5449 161853951 0
```

Nell'esempio, si nota come siano stati definiti tre communication partner (il quarto, quello identificato come "\*", è il communication partner "ANYWHERE" di default che comprende qualsiasi indirizzo): Italy, outside\_Italy e world\_outside\_AS5449. Il report indica chiaramente il traffico prodotto dai sottodomini INFN e Universita da e verso ognuno di questi communication partner.

## 12 Accessibilità dei dati tramite World Wide Web

La descrizione dettagliata delle modalità per l'accesso ai dati tramite World Wide Web è contenuta nella terza parte di questo documento.

Nella sezione relativa all'installazione del prodotto, sono già state descritte le operazioni necessarie per rendere disponibili sul Web i dati prodotti da IPaccounting.

Resta ancora da definire l'URL che permette l'accesso alla home page di IPaccounting, da cui sono accessibili tutte le risorse. La home page è generata "al volo" da una script nella directory dove si trovano i CGI, definita in fase di configurazione. La script in questione è `cgi-bin/home.pl`. Si consiglia di inserire un puntatore a tale script in una pagina HTML utilizzando il path assegnato al parametro `CGI_URL` del file di configurazione, ad esempio:

```
<a href=http://www.ts.infn.it/cgi-bin/IPaccounting/home.pl>
TCP/IP usage statistics home page</a>
```

Nel caso si abbiano a disposizione le statistiche relative a più router, è necessario specificare nell'URL il nome del file di configurazione da utilizzare (ved. capitolo 14).

### 12.1 Protezione delle informazioni

Nel caso preferiate proteggere le informazioni prodotte da IPaccounting, con i normali metodi consentiti dal vostro server `httpd`, è sufficiente inibire l'accesso alla sottodirectory `cgi-bin`; ad esempio creando in tale directory un file `.htaccess` contenente le regole di protezione, in accordo con le specifiche del vostro server.

Per maggiori informazioni, consultate la documentazione del vostro server `httpd` a riguardo.

## 13 Archiviazione od eliminazione dei file obsoleti

I file contenenti i raw data vengono utilizzati esclusivamente per produrre le liste di traffico. Se la creazione di queste ultime viene completata senza problemi, i raw data possono essere eliminati, all'occorrenza.

Liste di traffico e report giornalieri sono invece accessibili tramite il Web. Si consiglia quindi di non eliminarli o comprimerli per l'archiviazione in modo da consentire l'accesso alla maggior quantità di dati possibile.

## 14 Gestione di più router

IPaccounting 2.0 consente di gestire le informazioni di traffico raccolte da più router contemporaneamente. Le modalità di una gestione multipla dipendono dal criterio di aggregazione scelto per i vari router. Generalmente si presentano due possibilità:

1. I router vengono gestiti separatamente: i dati vengono raccolti in modo indipendente, e tutta l'elaborazione successiva, inclusa la gestione delle pagine Web, viene eseguita in maniera completamente separata per i vari router. In questo modo è possibile evidenziare il traffico transitato per un router rispetto ad un altro.
2. I router vengono gestiti come un'unica entità: i dati vengono raccolti dai singoli router (ed eventualmente conservati separatamente, in modo da poter effettuare elaborazioni aggiuntive sui dati "separati"), e concatenati in modo da produrre un unico file che li contenga tutti. Il file viene poi elaborato come se si trattasse di un singolo router.

In entrambi i casi dev'essere predisposto un file di configurazione distinto per ogni linea di elaborazione. Come accennato in altra parte di questo documento, esiste la possibilità di specificare ad ogni modulo di IPaccounting (incluse le script per la gestione delle pagine Web) il nome del file di configurazione cui fare riferimento. I file di configurazione *devono* essere creati nella directory dove IPaccounting è stato installato.

Nel caso di una gestione completamente separata, è necessario un file di configurazione per ogni router. Tipicamente alcuni parametri devono essere diversi per i router, in particolare quelli che indicano le directory ed i nomi dei file. Ad esempio, supponiamo di avere due router, `foo.ts.infn.it` e `bar.ts.infn.it`. I file di configurazione `config-foo.pl` e `config-bar.pl` potrebbero essere questi (ricavati dal file `configuration.pl`, indichiamo solo le linee principali per brevità):

File `config-foo.pl`:

```
$ROUTER_NAME="foo.ts.infn.it";
$DOMAIN_NAME="My domain";
$HOMEDIR="/IPaccounting";
$ACCOUNTING_FILE="$HOMEDIR/IPaccounting-foo.dat";
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data_foo";
$ARCHIVE_PATH="$HOMEDIR/archive_foo";
$DAILY_PATH="$HOMEDIR/daily_reports_foo";
...
```

File `config-bar.pl`:

```
$ROUTER_NAME="bar.ts.infn.it";
$DOMAIN_NAME="My domain";
$HOMEDIR="/IPaccounting";
```

```

$ACCOUNTING_FILE="$HOMEDIR/IPaccounting-bar.dat";
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data_bar";
$ARCHIVE_PATH="$HOMEDIR/archive_bar";
$DAILY_PATH="$HOMEDIR/daily_reports_bar";
...

```

In questo modo tutti i dati, da quelli prelevati dal Cisco fino ai report giornalieri utilizzati dalle pagine Web per creare i grafici, resteranno separati.

Come detto, tutti i moduli di IPaccounting (escluso `collect_accounting_data.pl`) prevedono l'opzione `-c` che consente di specificare il file di configurazione cui fare riferimento per l'elaborazione. Nell'esempio precedente, l'intera elaborazione per i due router potrebbe essere organizzata inserendo in crontabs le seguenti linee:

```

#
# Get data from router foo every 10 minutes
#
0,10,20,30,40,50 * * * * /IPaccounting/collect_accounting_data.pl
foo.ts.infn.it /IPaccounting/IPaccounting-foo.dat > /dev/null 2>&1
#
# Get data from router bar every 10 minutes
#
0,10,20,30,40,50 * * * * /IPaccounting/collect_accounting_data.pl
bar.ts.infn.it /IPaccounting/IPaccounting-bar.dat > /dev/null 2>&1
#
# Every night, make accounting for router foo
#
58 23 * * * /IPaccounting/make_all_accounting.pl
-c/IPaccounting/config-foo.pl
-n500 > /IPaccounting/make_all_accounting-foo.log 2>&1
#
# Every night, make accounting for router bar
#
58 23 * * * /IPaccounting/make_all_accounting.pl
-c/IPaccounting/config-bar.pl
-n500 > /IPaccounting/make_all_accounting-bar.log 2>&1

```

L'accesso alle pagine Web deve anch'esso prevedere la specificazione del file di configurazione. Nell'esempio in questione, si potrebbero inserire le seguenti linee in una pagina HTML, per puntare alle home page relative ai due router:

```

<a href=http://www.ts.infn.it/cgi-bin/IPaccounting/home.pl?/IPaccounting/
config-foo.pl>TCP/IP usage statistics for router foo</a>
<a href=http://www.ts.infn.it/cgi-bin/IPaccounting/home.pl?/IPaccounting/
config-bar.pl>TCP/IP usage statistics for router bar</a>

```

Nel caso di una gestione aggregata, invece, si aggiunge un elemento di complicazione nel fatto di dover concatenare i dati provenienti da più router. Il comportamento esatto da seguire dipende dal punto della catena di elaborazione nel quale si vuole procedere all'aggregazione dei dati. Ricordiamo che la catena di elaborazione (per ogni singolo router) è la seguente:

1. Salvataggio dei dati ottenuti dal router nel raw data archive.
2. Produzione delle liste di traffico

### 3. Produzione dei daily report

Si può ad esempio decidere di concatenare fin dall'inizio i raw data ottenuti dai router in un unico file di dati, oppure di mantenere i file separati per successive analisi, e di produrre un'unica lista di traffico a partire da essi.

A seconda del comportamento prescelto, sarà necessario predisporre una script (o un insieme di script) che si occupino dei task necessari nella sequenza corretta.

Questa configurazione è strettamente site-specific; non è quindi facile esemplificarla in modo valido a coprire tutte le necessità. Tuttavia, riteniamo utile riportare brevemente la configurazione utilizzata presso la Sezione di Trieste dell'I.N.F.N., dove è monitorato in maniera aggregata il traffico gestito da due router. In questo caso, i dati provenienti dai router sono collezionati ed archiviati separatamente. In un passo successivo si procede alla concatenazione dei raw data, ed alla produzione di un unico insieme di liste di traffico complessive, e del report giornaliero corrispondente. Il tutto viene fatto utilizzando la script che si trova nell'appendice A. È questa script ad essere eseguita quotidianamente tramite cron, al posto di `make_all_accounting.pl`, in modo da completare la sequenza corretta di richiami. I file di configurazione in questo caso sono tre: uno per ognuno dei router, ad indicare principalmente i nomi dei file in cui sono via via salvati i dati provenienti dai router e le directory dove essi devono essere archiviati, più uno "globale" contenente i parametri necessari per l'elaborazione delle statistiche e l'accesso tramite Web. La stessa appendice A contiene anche il listato delle linee più significative dei tre file di configurazione. Anche in questo caso, per l'accesso alle statistiche tramite Web, è necessario specificare nell'URL il file di configurazione da utilizzare:

```
<a href=http://www.ts.infn.it/cgi-bin/IPaccounting/home.pl?/IPaccounting/
configuration-global.pl>TCP/IP usage statistics for router2</a>
```

## Parte III

# Guida per l'utente

## 15 Caratteristiche dell'interfaccia utente

Le informazioni prodotte ed immagazzinate da IPaccounting si possono consultare tramite il World Wide Web. Esse sono presentate in forma di grafici e di tabelle; la selezione dei dati da consultare viene effettuata per mezzo di *form* HTML.

È quindi necessario un browser WWW che possieda le seguenti caratteristiche:

- Possibilità di gestire i form HTML.
- Se si desiderano i dati in forma tabellare, possibilità di gestire le tabelle HTML.
- Se si desiderano i dati in forma grafica, possibilità di gestire, internamente o esternamente alla finestra principale file PostScript e/o GIF. In entrambi i casi, è consigliabile disporre di un monitor a colori in modo da poter sfruttare le possibilità cromatiche, che offrono maggiore leggibilità rispetto al bianco e nero.

Tutte le pagine relative ad IPaccounting sono dinamiche: esse vengono generate "al volo" quando sono richiamate, in modo da includere sempre i parametri di configurazione necessari. Le pagine vengono generate da un insieme di script Perl sul server IPaccounting.

Ogni pagina di IPaccounting riporta il nome del (o dei) router cui si riferisce, ed il nome del dominio di accounting, così come sono stati definiti dall'amministratore.

## 16 Simbologia nelle pagine di IPaccounting

Nelle pagine di IPaccounting sono utilizzati alcuni "tasti" con funzioni particolari. Essi hanno il seguente significato:



Questo tasto consente l'accesso ad una pagina di aiuto relativa all'argomento cui il tasto si riferisce.



Questo tasto consente il ritorno alla home page di IPaccounting.

## 17 La home page di IPaccounting

Per home page di IPaccounting si intende una pagina contenente il menu principale per un router (o un insieme di router monitorati come una singola entità).

Su un server IPaccounting vi possono essere più home page di IPaccounting, nel caso in cui vi siano più router monitorati separatamente, oppure una singola home page.

Un esempio di home page di IPaccounting si trova nella figura 2.

Il menu principale di IPaccounting consente le seguenti operazioni:



## IPAccounting home page

Router name: **trieste-gw1.ts.infn.it** and **trieste-gw2.sist.trieste.it**  
 Accounting domain: **AS5449**

Click on the desired operation (use "information" buttons for argument-specific help):

### Display domains settings:

[Display accounting domain definition](#)



[Display ordinary accounting subdomains definitions](#)



[Display special accounting subdomains definitions](#)



[Display communication partners definitions](#)



### Display traffic lists:

[Lists of top entries in the IPAccounting traffic lists](#)



### Statistics:

[IP accounting summary snapshot](#)



[IP accounting report as a function of time](#)




---

*IPAccounting 2.0 - C.Strizzolo, R.Gomez - © INFN 1997*

Figura 2: Esempio di home page di IPAccounting.

- Visualizzazione dei file di definizione per i domini:  
 I file di definizione contengono la lista delle reti e/o dei nodi che sono stati definiti dall'amministratore come appartenenti ad un determinato dominio/sottodominio. Sono possibili le seguenti visualizzazioni:
  - Visualizzazione del file di definizione del dominio di accounting.
  - Visualizzazione dei file di definizione per i sottodomini ordinari di accounting.
  - Visualizzazione dei file di definizione per i sottodomini speciali di accounting.
  - Visualizzazione dei file di definizione per i communication partner.
- Visualizzazione delle prime  $n$  entry nelle liste di traffico giornaliere, ordinate per volume di traffico.
- Visualizzazione delle statistiche di traffico in forma tabellare o grafica. Sono possibili due tipi di statistica:

- Sommario "istantaneo" del traffico per un insieme di sottodomini di accounting.
- Andamento del traffico nel tempo, per un insieme di sottodomini di accounting.

## 18 Visualizzazione dei file di definizione per i domini

Le pagine contenenti le definizioni del dominio di accounting, dei sottodomini e dei communication partner sono tutte strutturate in modo molto simile. Esse includono i file di definizione così come sono stati predisposti dall'amministratore.

I file di definizione contengono le liste dei nodi e/o delle reti che appartengono ad un dominio o sottodominio, un nodo o una rete per ogni riga. Alcuni nodi o reti possono essere stati esclusi dal dominio, facendo precedere l'indirizzo dal simbolo "-". I commenti sono invece preceduti dal simbolo "#". Ad esempio:

```
#
# Questo e' un esempio di sottodominio
#
# Il sottodominio include le reti 140.105. e 147.122.
# esclusa la sottorete 140.105.6
140.105.
147.122.
-140.105.6. # Escludiamo una rete
```

È inoltre possibile riscontrare all'interno di un indirizzo la wildcard "\*", che, come è usuale, sostituisce una sequenza qualsiasi di caratteri.

Un esempio si trova nella figura 3.

## 19 Visualizzazione delle liste di traffico

Il capitolo 10 descrive in dettaglio le liste di traffico, ed anche i dati in esse contenuti. Si consiglia pertanto di consultare tale capitolo prima di procedere.

La possibilità di accedere a tali statistiche permette di rispondere a domande del tipo: quali sono i nodi che hanno trasmesso/ricevuto più byte nel giorno  $x$ ? Quali sono state le comunicazioni più "pesanti"? Con quali nodi ha comunicato il nodo  $x$  nel giorno  $y$  (per questo basta effettuare una ricerca tra gli indirizzi in modo da isolare quelli del nodo di interesse)?

L'accesso alle liste di traffico viene effettuato tramite un form da compilare con le informazioni relative ai dati che si intende visualizzare. Il form si presenta come in figura 4.

Nel form, bisogna indicare il numero di entry da visualizzare (il default è 100); per visualizzare tutte le entry bisogna omettere del tutto la specificazione di tale valore.

In seguito, è necessario selezionare la lista cui si è interessati, fra le tre disponibili, evidenziando con il mouse la piccola icona visualizzata alla sinistra del nome della lista, e selezionare la data cui si è interessati nella lista alla destra del medesimo nome di lista.

Completata la selezione, premere il tasto selezionatore del mouse in corrispondenza dell'icona "Do it".

**ICS**

```
140.105.27. # ICS-NET
```

**ICTP**

```
#
# International Centre for Theoretical Physics
#
140.105.16. # ICTP-MB-SCI
140.105.24. # ICTP-MB-ADM
140.105.30. # ICTP-MB-AGH
140.105.28. # ICTP-AGH-SCI
140.105.29. # ICTP-AGH-ADM
140.105.25. # ICTP-MB-MLAB
140.105.26. # ICTP-MLAB
140.105.33. # ICTP-33
140.105.34. # ICTP-MB-ADM2
140.105.35. # ICTP-AGH-ADM2
140.105.36. # ICTP-36
140.105.37. # ICTP-37
140.105.38. # ICTP-38
140.105.39. # ICTP-39
140.105.40. # ICTP-40
140.105.41. # ICTP-41
140.105.42. # ICTP-42
140.105.43. # ICTP-43
140.105.44. # ICTP-44
140.105.45. # ICTP-45
140.105.46. # ICTP-46
140.105.47. # ICTP-47
```

**INFN**

```
#
# Istituto Nazionale di Fisica Nucleare
#
140.105.6. # INFN-AREA
140.105.244. # INFN-SLIP
```

Figura 3: Esempio di definizione di sottodomini.

## 20 Visualizzazione delle statistiche di traffico

### 20.1 Sommario “istantaneo” del traffico

IPaccounting consente di eseguire una “fotografia” del traffico, relativo ad uno o più sottodomini di accounting, in un determinato istante. La “fotografia” conterrà i totali di traffico che si riferiscono ad una determinata data (giorno o mese).

Questa opzione consente di rispondere a una domanda del tipo: nel giorno (o: nel mese)  $x$ , quali sono stati i totali di traffico per i vari sottodomini?

L’accesso ai dati avviene anche in questo caso tramite un form, un esempio del quale si trova nella figura 5.

Le informazioni da definire nel form sono le seguenti:

1. Selezionare se si desidera un’istantanea relativa ad un giorno o ad un mese.
2. Selezionare la data desiderata (se al punto precedente è stata selezionata l’opzione relativa al mese, verranno considerati solo il mese e l’anno).



## IPAccounting top lists form

**Router name:** trieste-gw1.ts.infn.it and trieste-gw2.sist.trieste.it  
**Accounting domain:** AS5449

Fill this form to submit a query to display the list of top  $n$  entries of daily accounting data computed by IPAccounting. When you are ready, just click on the "Do it!" button at the bottom of this form.

Number of entries to display (empty for all entries):

Top source to target communications on date
   
 Top source nodes on date
   
 Top target nodes on date

Figura 4: Form per l'accesso alle liste di traffico.

3. Selezionare la lista dei sottodomini ordinari o quella dei sottodomini speciali tramite l'apposita icona a fianco delle due liste. Il sommario può includere esclusivamente uno dei due tipi di sottodomini.
4. Nella lista relativa alla categoria di sottodomini prescelta, selezionare i sottodomini cui si è interessati.
5. Selezionare la direzione del traffico: dal sottodominio verso l'esterno, dall'esterno verso il sottodominio oppure entrambe.
6. Selezionare il communication partner del quale interessa conoscere il traffico da/verso il dominio di accounting.
7. Selezionare l'unità di misura (byte o multipli, oppure percentuale).
8. Selezionare il formato dell'output: tabella oppure grafico (PostScript o GIF).



## IPAccounting summary snapshot form

Router name: trieste-gw1.ts.infn.it and trieste-gw2.sist.trieste.it  
Accounting domain: AS5449

Do you need a summary snapshot for a day or a month? Day ▾

Choose reference date (for monthly reports only month and year are meaningful):

06-Mar-1997 ▾

◆ Use ordinary subdomains:

AREA  
BdP  
Burlo  
CARSO  
CRSTBS

▽ Use special subdomains:

ICTP\_News  
INFN\_Cosine

Which traffic direction(s) must be considered? Traffic TO/FROM each subdomain ▾

Which communication partner? Italy ▾

Which unit of measure? Percentage ▾

Which output format? Table ▾

Do it! Reset all values  

Figura 5: Form per la visualizzazione di un sommario "istantaneo" del traffico.

La tabella prodotta sarà formattata come nella figura 6.

Nell'esempio si suppone sia stata selezionata, quale unità di misura, la percentuale sul totale di traffico prodotto dall'intero dominio di accounting nella direzione considerata. Il totale che compare nella tabella indica quindi che i sottodomini elencati hanno prodotto il 94.7 % del traffico prodotto dall'intero dominio.

Gli stessi dati inclusi nella tabella si trovano in forma di grafico nella figura 7.

### 20.2 Andamento del traffico nel tempo

IPAccounting consente di visualizzare l'andamento del traffico, riferito ad uno o più sottodomini di accounting, nel corso di un mese oppure mese per mese.

Questo tipo di report consente una comparazione tra sottodomini, oppure tra communication partner che hanno prodotto traffico con diversi sottodomini, oppure ancora in base alla direzione del traffico.

L'accesso ai dati avviene anche in questo caso tramite un form, simile a quello utiliz-



## IPAccounting report

Domain name: AS5449

Router name: trieste-gw1.ts.infn.it and trieste-gw2.sist.trieste.it

Date: 06-Mar-1997

Kind of report: daily snapshot

Unit of measure: %

Traffic: to/from subdomain from/to Italy

Subdomain	
AREA	5.2
Elettra	18.3
ICTP	21.5
INFN	6.2
OAT	1.4
OGS	1.5
SISSA	23.6
Universita	17.1
<b>TOTAL</b>	<b>94.7</b>

Figura 6: Esempio di tabella con sommario "istantaneo" del traffico.

zato per i sommari "istantanei". La differenza più interessante consiste nel fatto che in questo caso è possibile selezionare più opzioni contemporaneamente per quanto riguarda la direzione del traffico ed i communication partner.

Le tabelle ed i grafici prodotti in questo caso sono tipicamente più complessi di quelli generati nei sommari istantanei. Ad esempio, una tabella potrebbe essere come quella in figura 8.

Il grafico corrispondente è in figura 9.

### 20.3 Note sui grafici

Qualora si visualizzino i dati di IPAccounting in forma grafica, per mezzo di un browser come Netscape o simili, direttamente nella finestra del browser, è possibile che si verifichi un piccolo inconveniente: se si genera un grafico in formato GIF tramite un form, e si ritorna poi al medesimo form selezionando dei valori diversi per generare un nuovo grafico (sempre in formato GIF), può capitare che venga visualizzato il grafico precedente anziché quello desiderato. Ciò succede perché il grafico precedente è nella cache del browser. Per ovviare all'inconveniente, è necessario ripulire la cache oppure eseguire il reload della pagina contenente il form. L'inconveniente non si verifica se il browser utilizza un'applicazione esterna per visualizzare i file GIF.

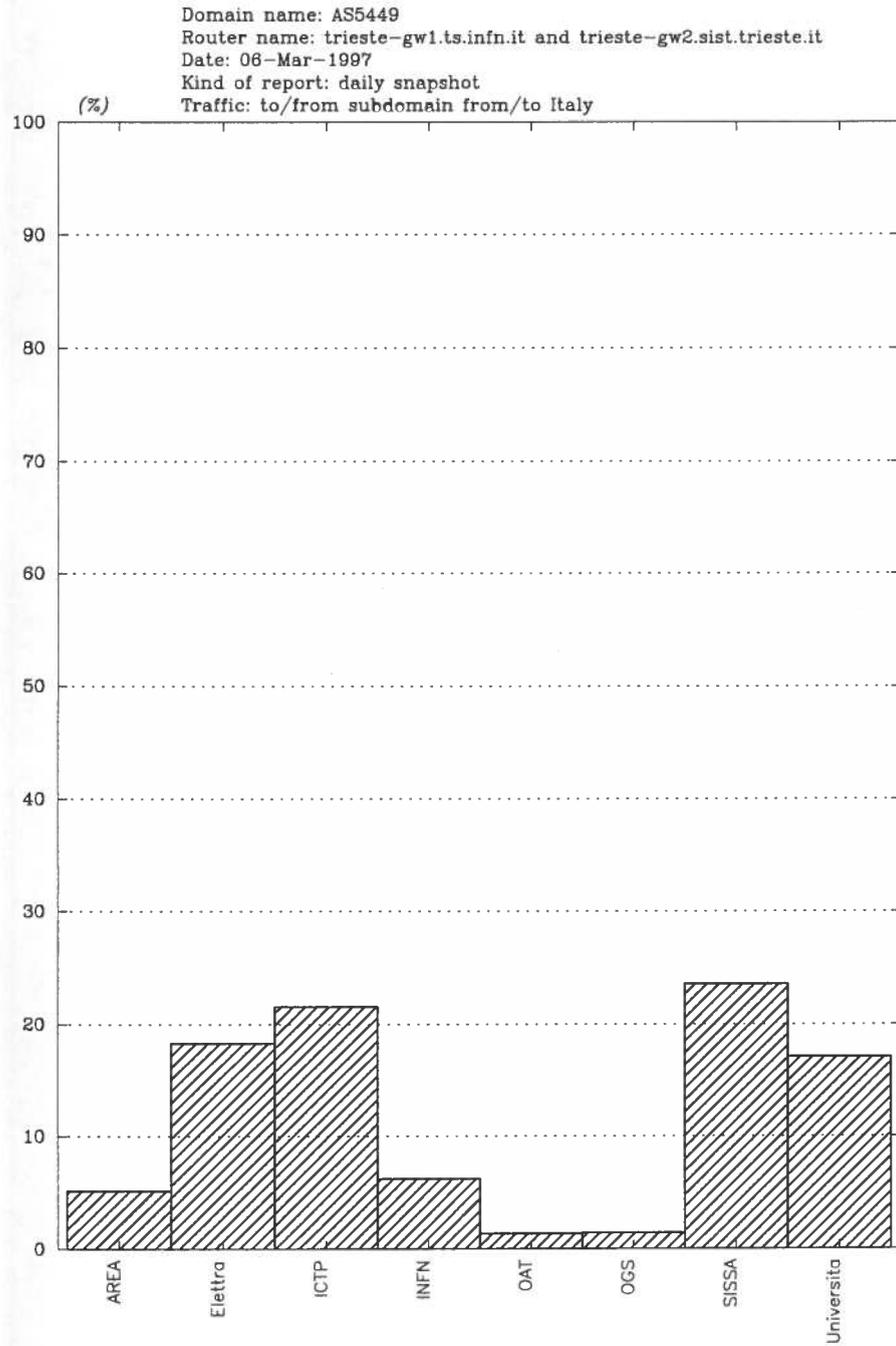


Figura 7: Esempio di grafico con sommario "istantaneo" del traffico.

Domain name: AS5449

Router name: trieste-gw1.ts.infn.it and trieste-gw2.sist.trieste.it

Date: Nov-1996

Kind of report: day-by-day report

Unit of measure: MBytes

Day	INFN from Italy	INFN to Italy	INFN from outside Italy	INFN to outside Italy	TOTAL
01	46.3	66.1	163.4	62.1	337.8
02	74.1	68.5	161.0	52.8	356.4
03	52.5	78.5	150.1	79.9	361.1
04	329.7	317.8	862.9	396.5	1906.9
05	110.9	93.2	188.6	106.9	499.7
06	76.5	96.8	221.3	102.5	497.1
07	153.0	97.5	496.3	180.4	927.2
08	312.3	149.0	1029.5	766.0	2256.8
09	35.2	70.0	143.2	139.5	387.9
10	100.5	158.7	178.2	203.2	640.7
11	166.2	82.3	684.2	325.7	1258.4
12	148.5	52.1	275.3	159.4	635.2
13	166.9	55.0	803.1	152.7	1177.7
14	167.5	106.4	1631.2	153.1	2058.3
15	235.7	88.9	1082.4	157.8	1564.8
16	-	0.0	0.0	0.0	0.0
17	24.9	62.7	552.6	42.8	683.0
18	222.3	133.4	280.5	58.0	694.2
19	216.7	118.1	333.2	116.4	784.5
20	282.2	104.0	246.1	97.5	729.9
21	215.4	83.6	1048.0	193.5	1540.6
22	342.9	121.2	2080.2	176.7	2720.9
23	30.3	71.5	1787.5	104.2	1993.5
24	28.4	62.7	564.3	64.2	719.6
25	1119.9	203.4	565.0	112.7	2000.9
26	339.8	131.0	793.4	144.0	1408.2
27	193.5	97.4	370.9	215.5	877.3
28	201.7	151.2	803.3	140.9	1297.0
29	297.5	154.6	358.9	53.6	864.6
30	119.3	64.2	218.2	31.5	433.3
<b>TOTAL</b>	<b>5810.5</b>	<b>3139.8</b>	<b>18072.9</b>	<b>4590.1</b>	

Figura 8: Esempio di tabella con andamento del traffico nel tempo.

Domain name: AS5449  
Router name: trieste-gw1.ts.infn.it and trieste-gw2.sist.trieste.it  
Date: Nov-1996  
Kind of report: day-by-day report

(MBytes)

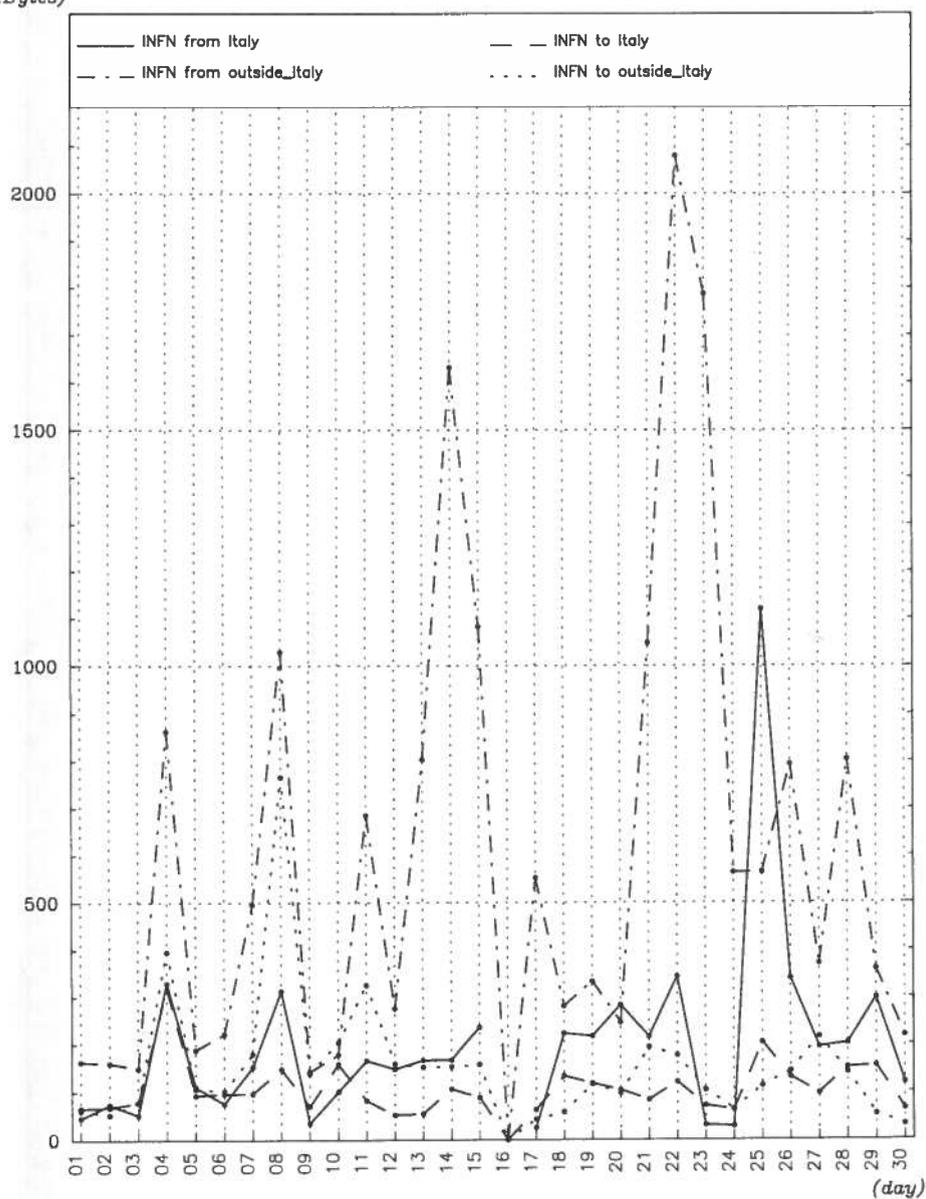


Figura 9: Esempio di grafico con andamento del traffico nel tempo.



```

./statistic.pl $current_date -m -cconfiguration-trieste-gw2.pl

# mix the two archived files to a temporary file

cat raw_data-trieste-gw1/IPaccounting.$current_date raw_data-trieste-gw2/IPaccou
nting.$current_date > raw_data-global/IPaccounting.$current_date

# make all accounting
# (no need to store raw data, they are available)

./make_all_accounting.pl $current_date -n500 -a -cconfiguration-global.pl

# remove temporary file

rm raw_data-global/IPaccounting.$current_date

```

Il file configuration-trieste-gw1.pl contiene le seguenti linee:

```

...
$ROUTER_NAME="trieste-gw1.ts.infn.it";           # NOT USED
$DOMAIN_NAME="AS5449";                          # NOT USED
$HOMEDIR="/usr/IPaccounting";
$ACCOUNTING_FILE="$HOMEDIR/IPaccounting.dat-trieste-gw1";
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data-trieste-gw1";
$ARCHIVE_PATH="$HOMEDIR/archive";               # NOT USED
$DAILY_PATH="$HOMEDIR/daily_reports";           # NOT USED
...

```

Molti parametri non sono utilizzati, dal momento che la script globale che richiama statistic.pl con questo file di configurazione esegue esclusivamente l'archiviazione.

Il file configuration-trieste-gw2.pl contiene le seguenti linee:

```

...
$ROUTER_NAME="trieste-gw2.sist.trieste.it";     # NOT USED
$DOMAIN_NAME="AS5449";                          # NOT USED
$HOMEDIR="/usr/IPaccounting";
$ACCOUNTING_FILE="$HOMEDIR/IPaccounting.dat-trieste-gw2";
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data-trieste-gw2";
$ARCHIVE_PATH="$HOMEDIR/archive";               # NOT USED
$DAILY_PATH="$HOMEDIR/daily_reports";           # NOT USED
...

```

Valgono le stesse considerazioni fatte per il file configuration-trieste-gw1.pl.

Il file configuration-global.pl contiene le seguenti linee:

```

...
$ROUTER_NAME="trieste-gw1 and trieste-gw2";
$DOMAIN_NAME="AS5449";
$HOMEDIR="/usr/IPaccounting";
$ACCOUNTING_FILE="$HOMEDIR/IPaccounting.dat";   # NOT USED
$RAW_ARCHIVE_PATH="$HOMEDIR/raw_data-global";
$ARCHIVE_PATH="$HOMEDIR/archive";
$ACCOUNTING_DOMAIN="$HOMEDIR/accounting_domain.dat";
$DAILY_PATH="$HOMEDIR/daily_reports";
...

```

## Ringraziamenti

Gli autori ringraziano tutte le persone che hanno fornito il feedback sulla versione precedente del prodotto.

Si ringrazia inoltre S.E.Brenner (autore della libreria cgi-lib) per il consenso dato all'inserimento della sua libreria nel kit di IPaccounting.

## Riferimenti bibliografici

- [1] "Router products configuration guide" - Cisco Systems
- [2] PGPLOT documentation - T.J.Pearson (<http://astro.caltech.edu/~tjp/pgplot>)
- [3] PGPERL documentation - K.Glazebrook (<http://www.aao.gov.au/local/www/kgb/-pgperl>)
- [4] cgi-lib documentation - S.E.Brenner (<http://www.bio.cam.ac.uk/cgi-lib/>)