I INFN Security Workshop
Firenze 19-20 Settembre 2000

Un sistema di Network Intrusion Detection basato su tcpdump

Massimo Gravino
INFN – Sezione di Padova

Perche` utilizzare un sistema di Network Intrusion Detection?

Tipici abusi a cui siamo esposti

- accesso non autorizzato ad un host
- compromissione del sistema
- Denial of Service
- mail spam
- utilizzo abusivo di anonymous ftp server
- virus, troiani, ...

Come prevenirli ?

- filtri sul router
- tcp-wrappers
- chiusura servizi inutili
- filtri anti-spam
- antivirus
- eliminazione trasmissione password in chiaro

ma .....

Un’intrusione nella LAN resta comunque un evento possibile e probabile

- si usano sistemi operativi intrinsecamente insicuri e/o non sempre configurati dal Servizio Calcolo
- gli utenti richiedono di utilizzare servizi insicuri
- i sistemi di autenticazione utilizzati (password) sono deboli
- tutti i sistemi operativi risultano prima o poi vulnerabili a chi riesce ad accedervi come utente locale

Un esempio: compromissione dell'account di root

- remota: mediante un servizio vulnerabile visibile all'esterno – *e` possibile difendersi*
- locale: accesso come utente non privilegiato (es. uso di password rubate) e successiva compromissione di root tramite un bug del software – *indifendibile?*

Cos’e` un sistema di Network Intrusion Detection ?

E` un sistema di monitoraggio del traffico di rete con lo scopo di evidenziare eventi critici per la security

Si puo` considerare come una valida estensione dei log di sistema

A cosa serve

Permette di rivelare:

- network scan
- traffico sospetto (IRC bot, abusi di ftp anonymous, troiani, etc.)
- traffico che coinvolge host sospetti

Puo` rivelare anche attacchi che originano da un host compromesso della nostra LAN

Permette di effettuare analisi specifiche anche a distanza di tempo, per esempio ricontrollando il traffico riguardante particolari host o servizi

A cosa non serve

- a prevenire un’intrusione
- a prevenire un Denial of Service
- a rivelare intrusioni o attacchi provenienti dall’interno della LAN

Non e` un sistema di protezione dalle intrusioni, ma di rivelazione delle intrusioni provenienti dall’esterno o di attacchi diretti verso l’esterno

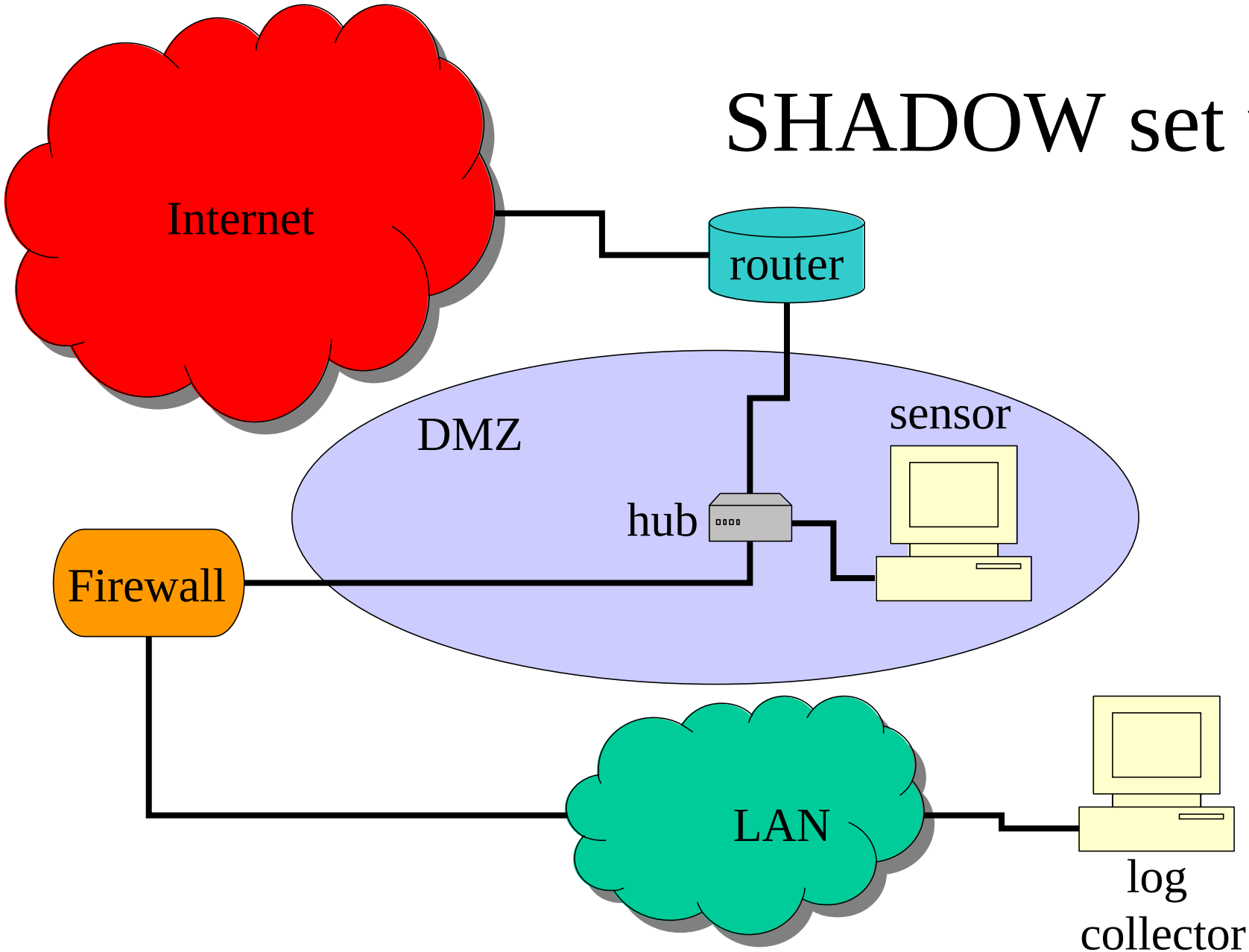
SHADOW

SANS's **H**euristic **A**nalisys system for **D**efensive **O**nline **W**arfare

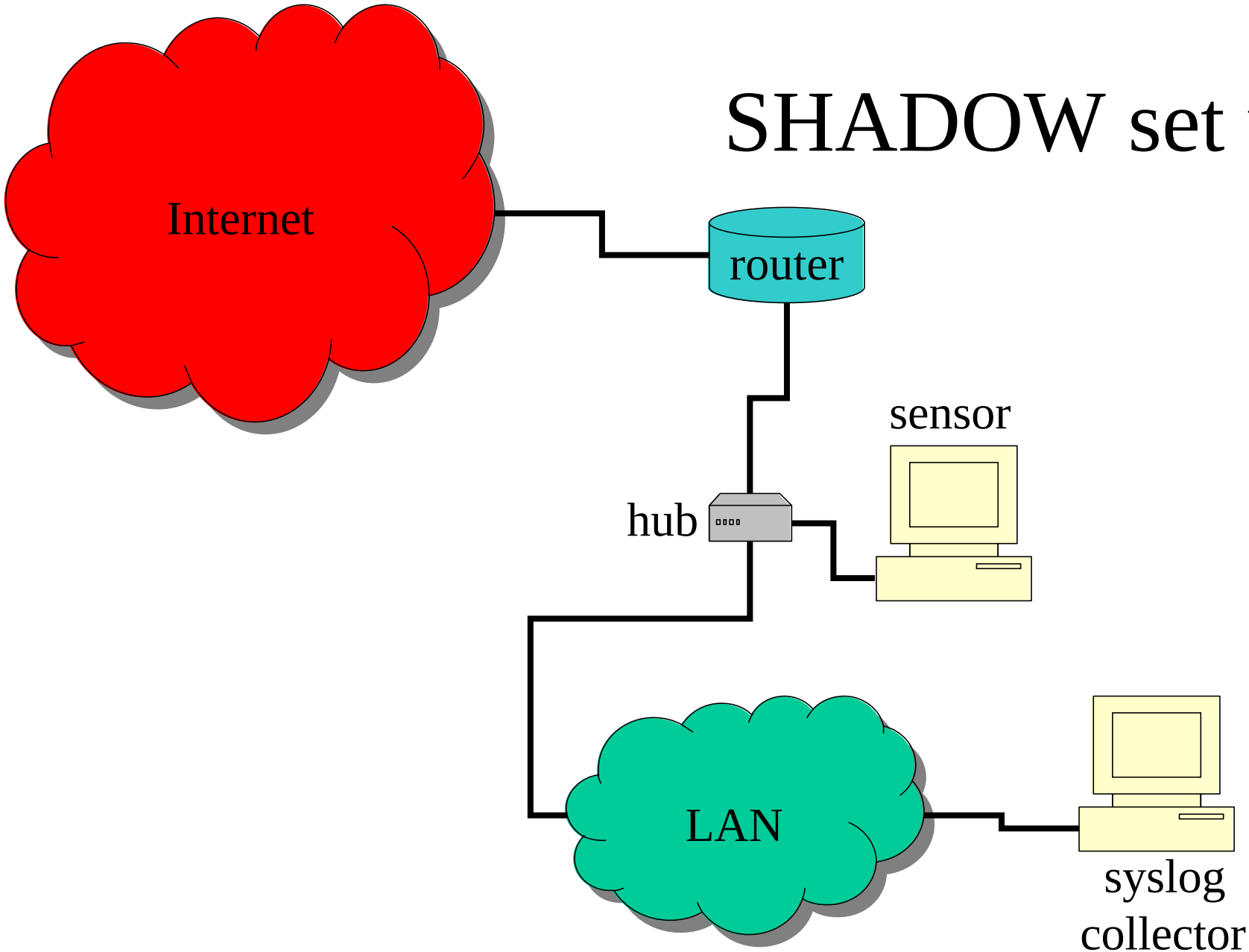
autori: Vicki Irwin, Stephen Northcutt, Bill Ralph (del Naval Surface Warfare Center) e SANS Institute

http://www.nswc.navy.mil/ISSEC/CID/

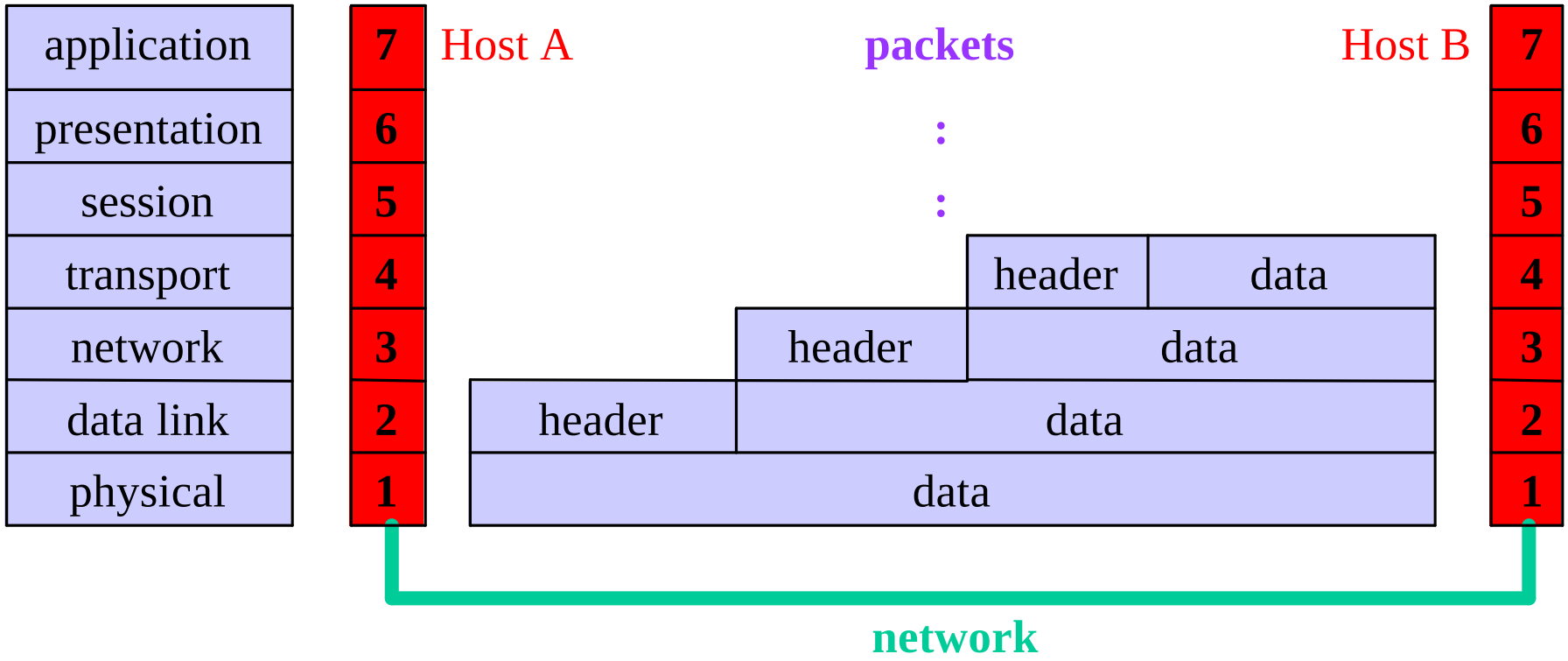
SHADOW set up



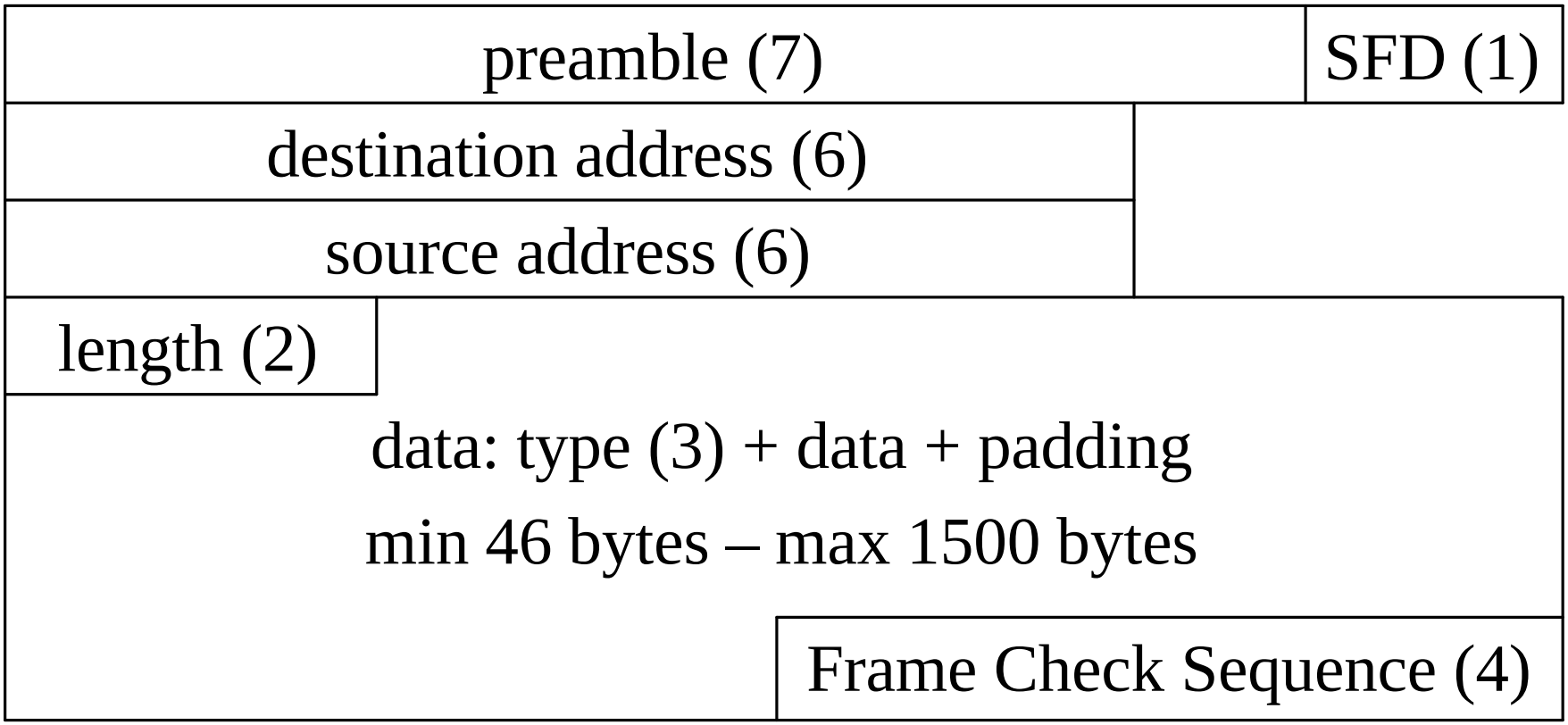
SHADOW set up



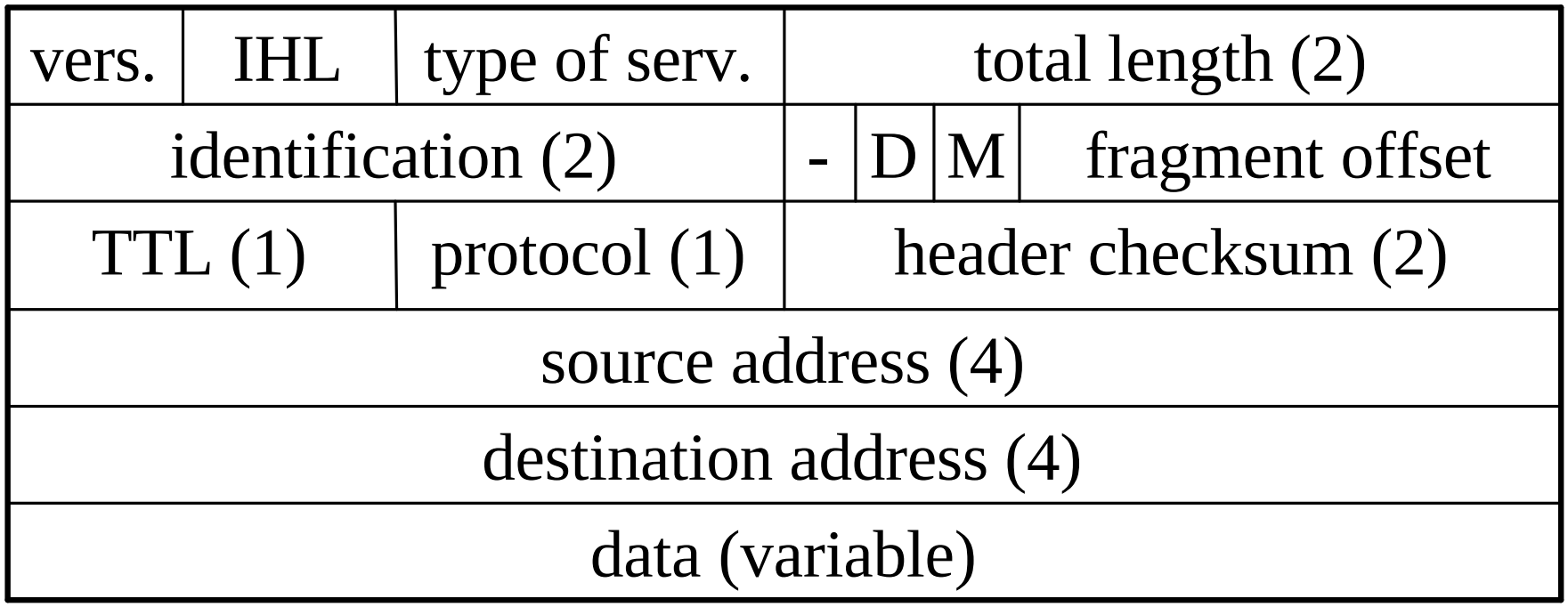
Encapsulation



Formato del pacchetto Ethernet



Formato del pacchetto IP



Formato del pacchetto TCP

<table>
<tr><td colspan="2">Source port (2)</td><td colspan="2">Destination port (2)</td></tr>
<tr><td colspan="4">Sequence number (4)</td></tr>
<tr><td colspan="4">Acknowledgment number (4)</td></tr>
<tr><td>Data offset</td><td></td><td>Flags (6 bit)</td><td>Window (2)</td></tr>
<tr><td colspan="2">Checksum (2)</td><td colspan="2">Urgent pointer (2)</td></tr>
<tr><td colspan="4">Options + padding (4)</td></tr>
<tr><td colspan="4">Data (variable)</td></tr>
</table>

Flags: (byte 14, tcp[13])

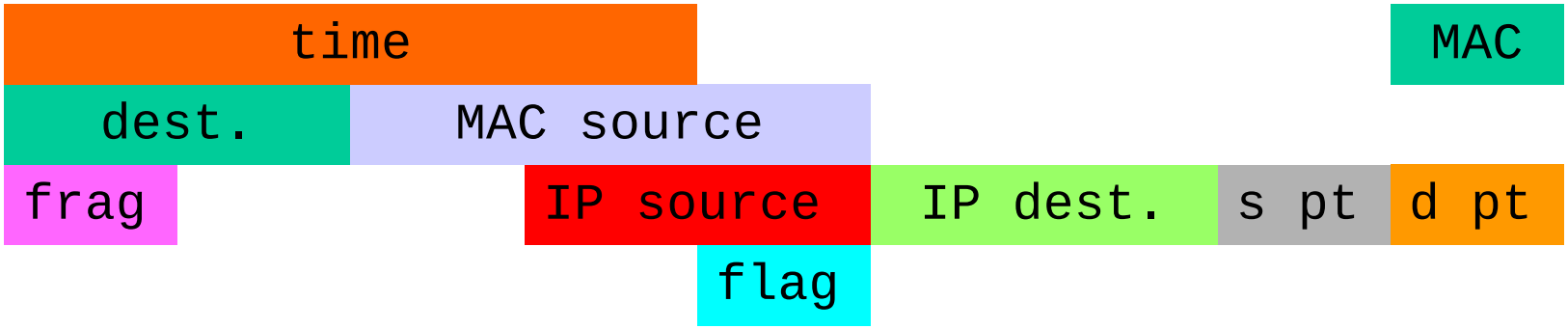
bit	flag
1	FIN
2	SYN
3	RST
4	PSH
5	ACK
6	URG

un pacchetto

```
f060  3889  041a  000d  003e  0000  003e  0000  e000
b734  60a8  0000  02f8  a4e8  0008  1045  3000  18c6
0040  063c  fde9  54c0  988f  9e86  16b8  800a  1700
9459  009e  0000  0000  0270  0080  5173  0000  0402
b405  009e  0003
```

un pacchetto

f060	3889	041a	000d	003e	0000	003e	0000	e000
b734	60a8	0000	02f8	a4e8	0008	1045	3000	18c6
0040	063c	fde9	54c0	988f	9e86	16b8	800a	1700
9459	009e	0000	0000	0270	0080	5173	0000	0402
b405	009e	0003						



tcpdump

- raccoglie da un’interfaccia di rete i pacchetti che soddisfano un criterio booleano e ne stampa l’header
- puo` salvare i pacchetti in un file
- puo` leggere l’input da un file invece che dall’interfaccia di rete

un pacchetto

f060	3889	041a	000d	003e	0000	003e	0000	e000
b734	60a8	0000	02f8	a4e8	0008	1045	3000	18c6
0040	063c	fde9	54c0	988f	9e86	16b8	800a	1700
9459	009e	0000	0000	0270	0080	5173	0000	0402
b405	009e	0003						

```
948564064.853018 0:0:f8:2:e8:a4 0:e0:34:b7:a8:60 ip 62:
192.84.143.152.2688 > 134.158.184.22.telnet: S
1502912000:1502912000(0) win 32768
<mss 1460,nop,wscale 0> (DF) [tos 0x10]
```

Caratteristiche tecniche del sensore utilizzato a PD

hardware

- Pentium II 450 MHz – RAM 128MB
- HD 18GB EIDE per i dati – NIC 3Com 3C905C

software

- Linux RedHat 5.2 – kernel 2.0.36
- libpcap 0.4
- tcpdump 3.4

Funzionamento

Basato su una serie di script (shell o perl) e di filtri utilizzati da tcpdump.

Compiti svolti:

- raccolta dati
- analisi e log
- riduzione dei dati
- controllo spazio disco

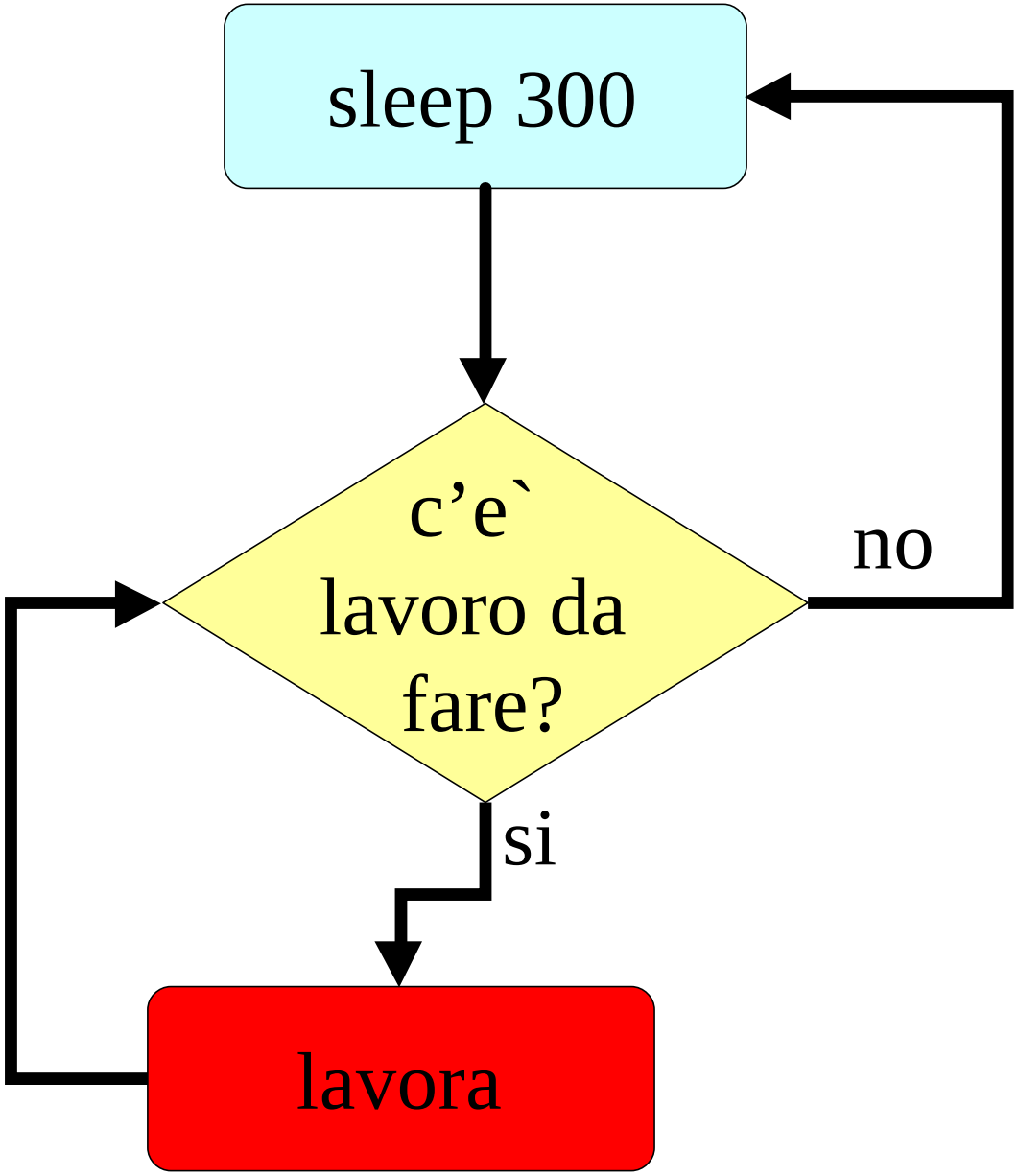
daemons

- analyzer
- filter
- cleaner

i daemons sono attivati

con l’opzione respawn

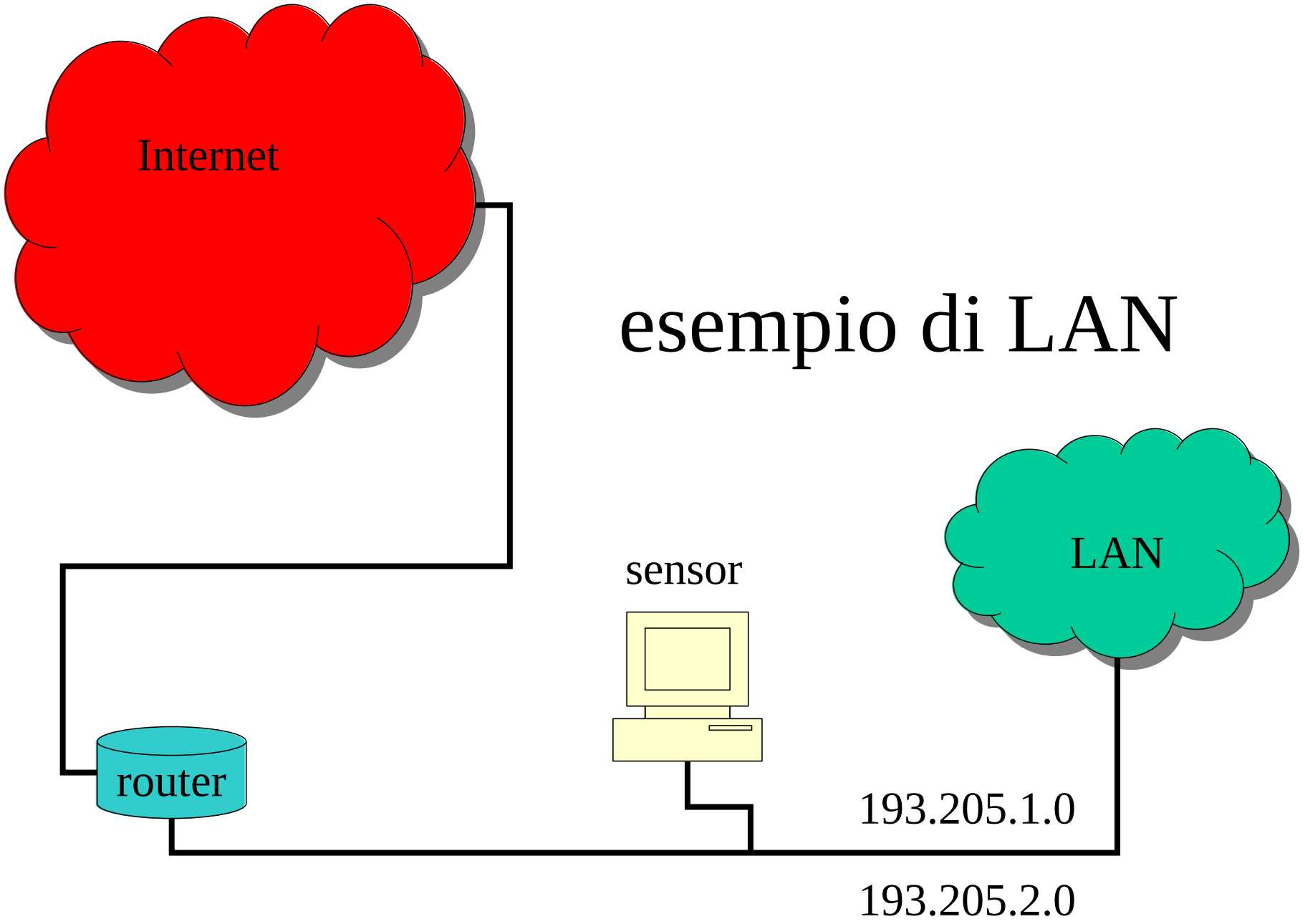
tramite inittab



crontrab

ogni ora:

- chiude una sessione di tcpdump e lancia la successiva
- copia il file di dati appena chiuso nella directory dell’“analyzer”
- sposta il file acquisito 48 ore prima nella directory di lavoro del “filter”


Internet
esempio di LAN
LAN
sensor
router
193.205.1.0
193.205.2.0

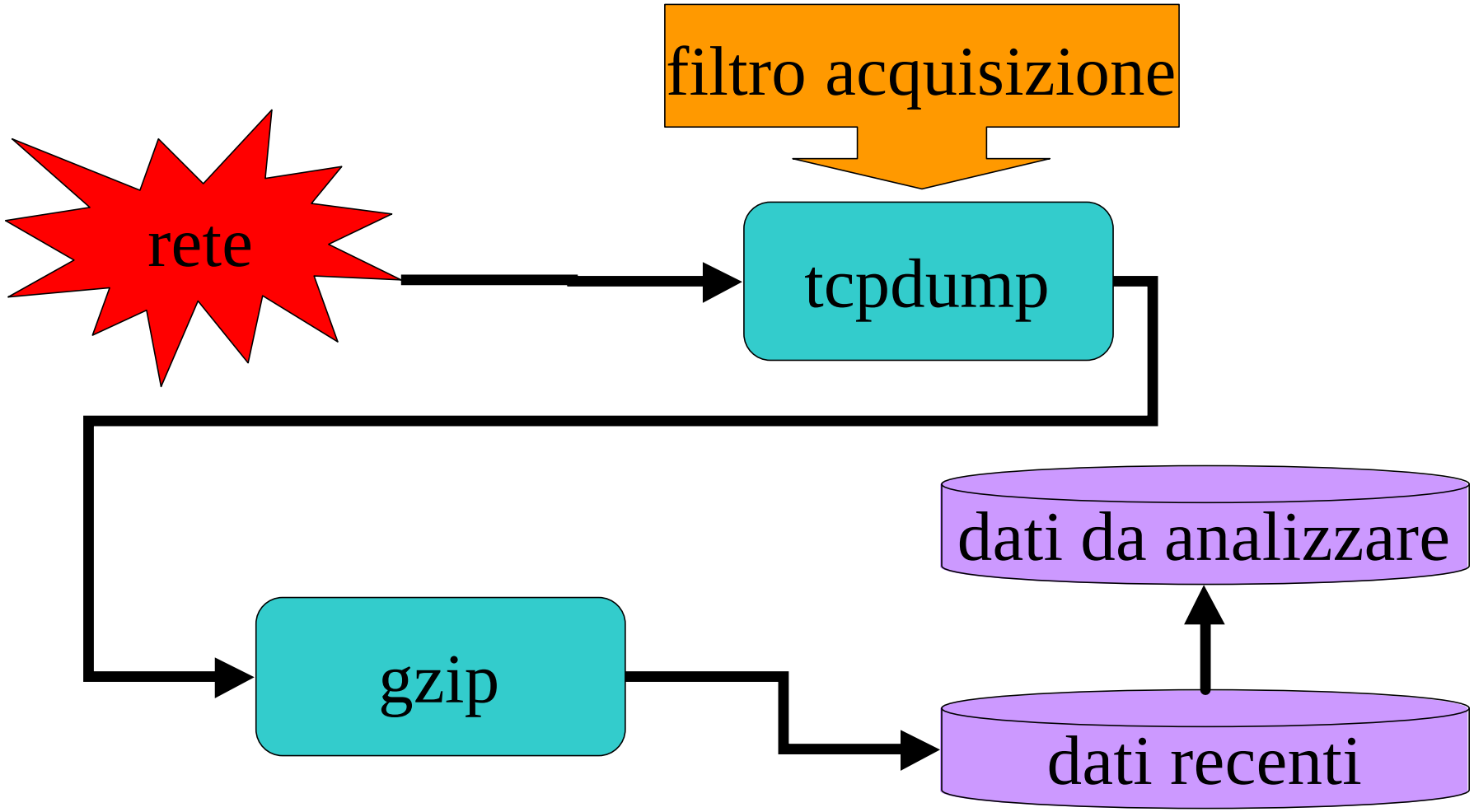
processo di acquisizione

```
tcpdump -i eth0 -F $FILTER
        -w – 2>>$err
      | gzip > $TCPLOG
```

filtro di acquisizione

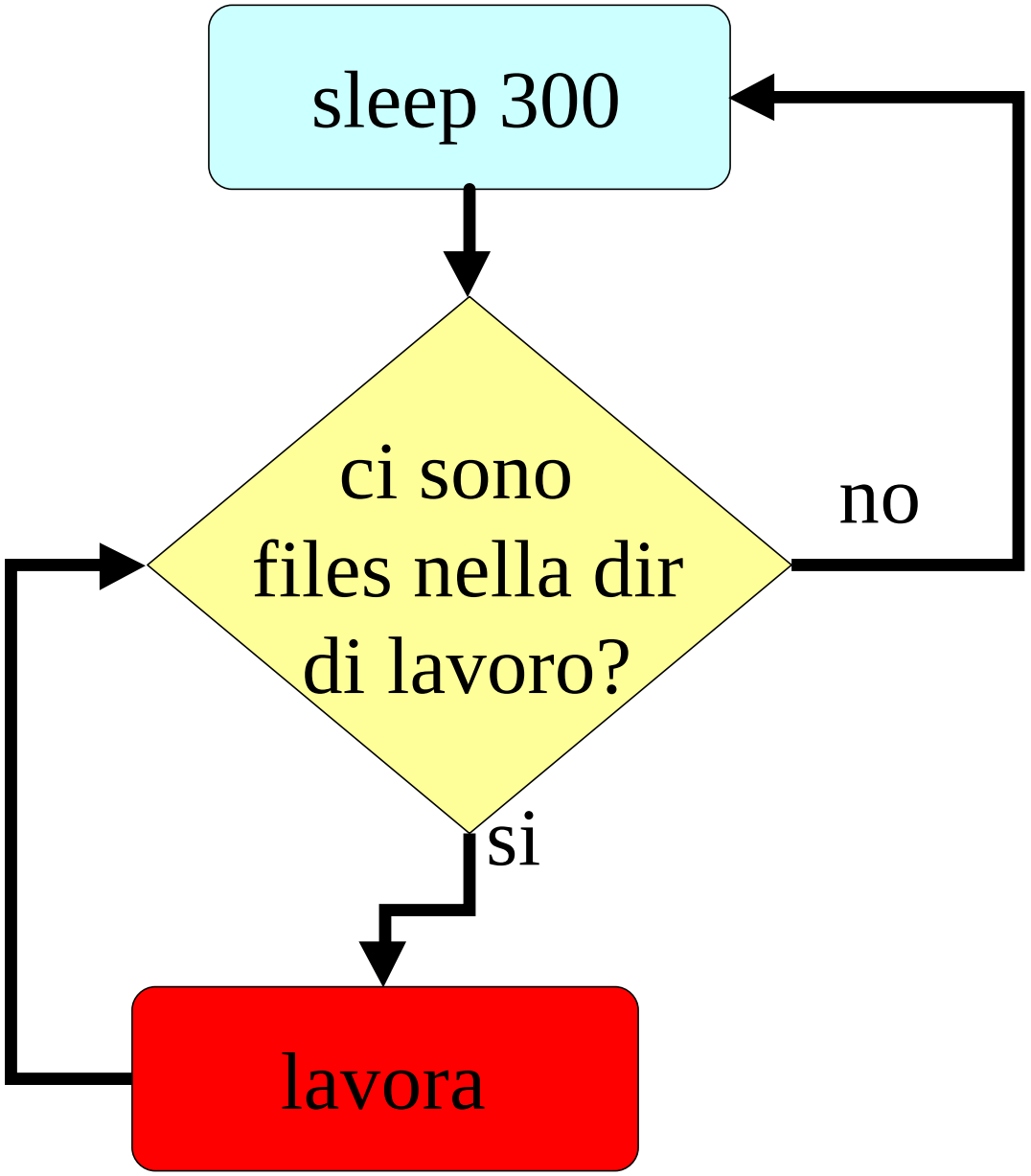
```
((dst net 193.205.1 or dst net
  193.205.2) and not (src net
  193.205.1 or src net 193.205.2)
or
((src net 193.205.1 or src net
  193.205.2) and not (dst net
  193.205.1 or dst net 193.205.2))
```

raccolta dati

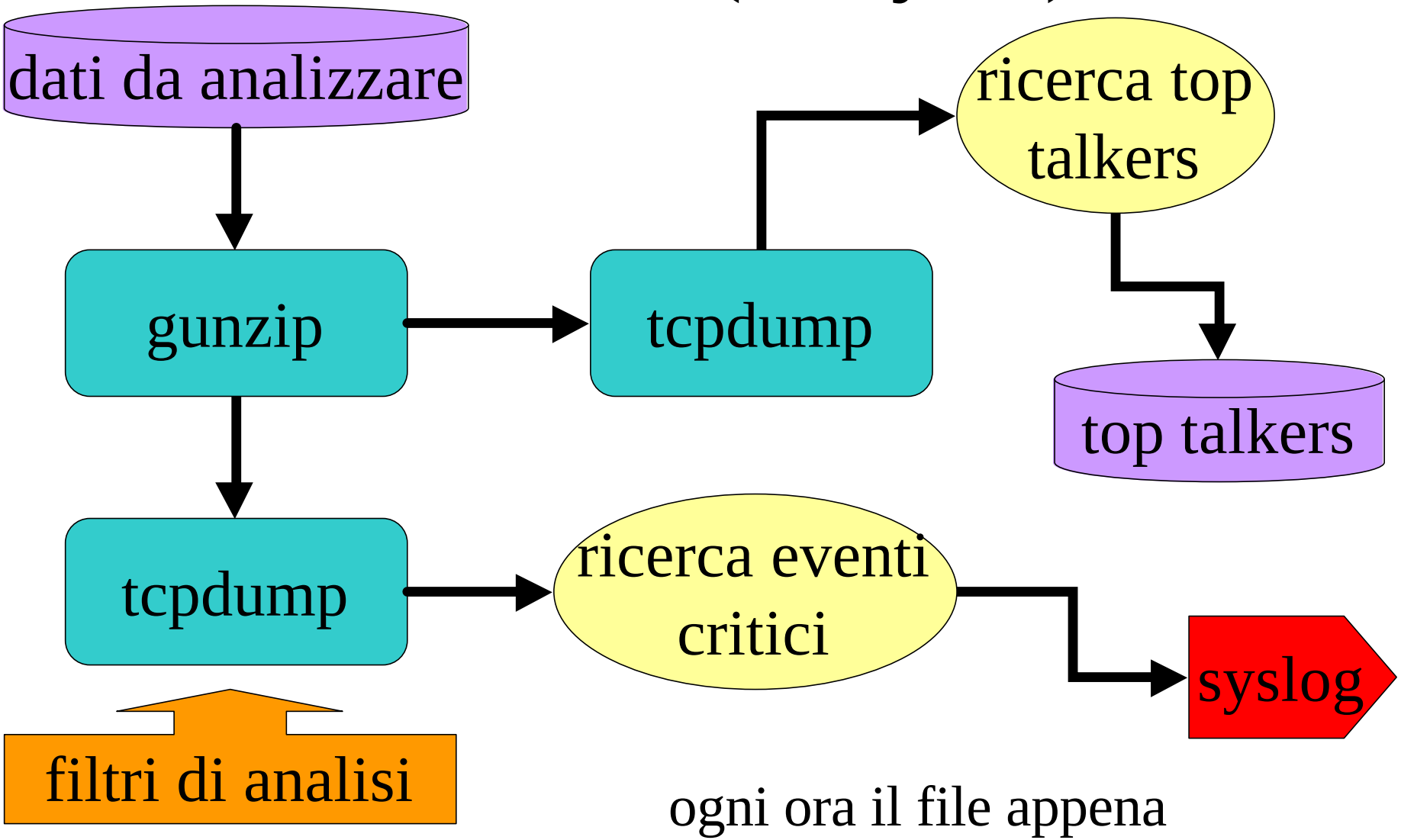


ogni ora il file di dati viene chiuso e ne viene aperto uno nuovo

analyzer e filter



analisi dati (analyzer)



ogni ora il file appena acquisito viene processato

un filtro di analisi

```
tcp
and (tcp[13] & 2 != 0)
and (dst port 21 or dst port 22
  or dst port 23 or dst port
  110 or dst port 143)
and (dst net 193.205.1 or dst
  net 193.205.2)
```

Formato del pacchetto TCP

<table>
<tr><td colspan="2">Source port (2)</td><td colspan="2">Destination port (2)</td></tr>
<tr><td colspan="4">Sequence number (4)</td></tr>
<tr><td colspan="4">Acknowledgment number (4)</td></tr>
<tr><td>Data offset</td><td></td><td>Flags (6 bit)</td><td>Window (2)</td></tr>
<tr><td colspan="2">Checksum (2)</td><td colspan="2">Urgent pointer (2)</td></tr>
<tr><td colspan="4">Options + padding (4)</td></tr>
<tr><td colspan="4">Data (variable)</td></tr>
</table>

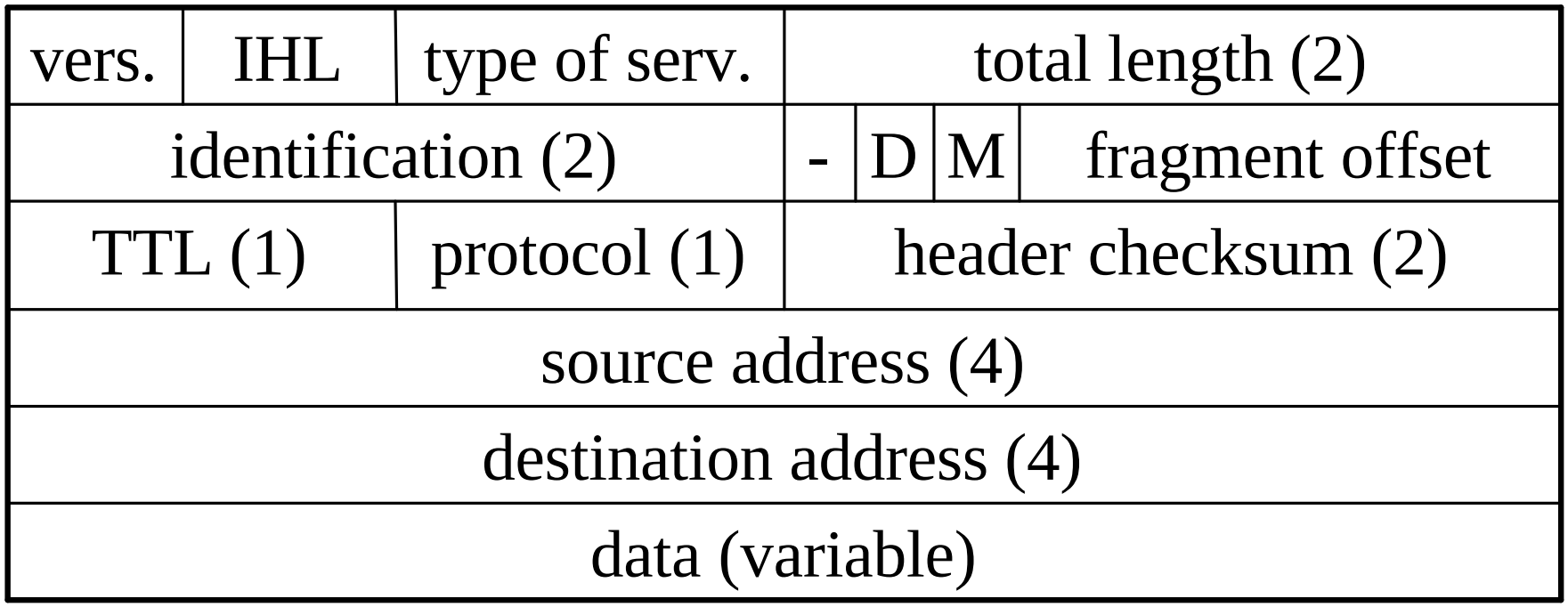
Flags: (byte 14, tcp[13])

bit	flag
1	FIN
2	SYN
3	RST
4	PSH
5	ACK
6	URG

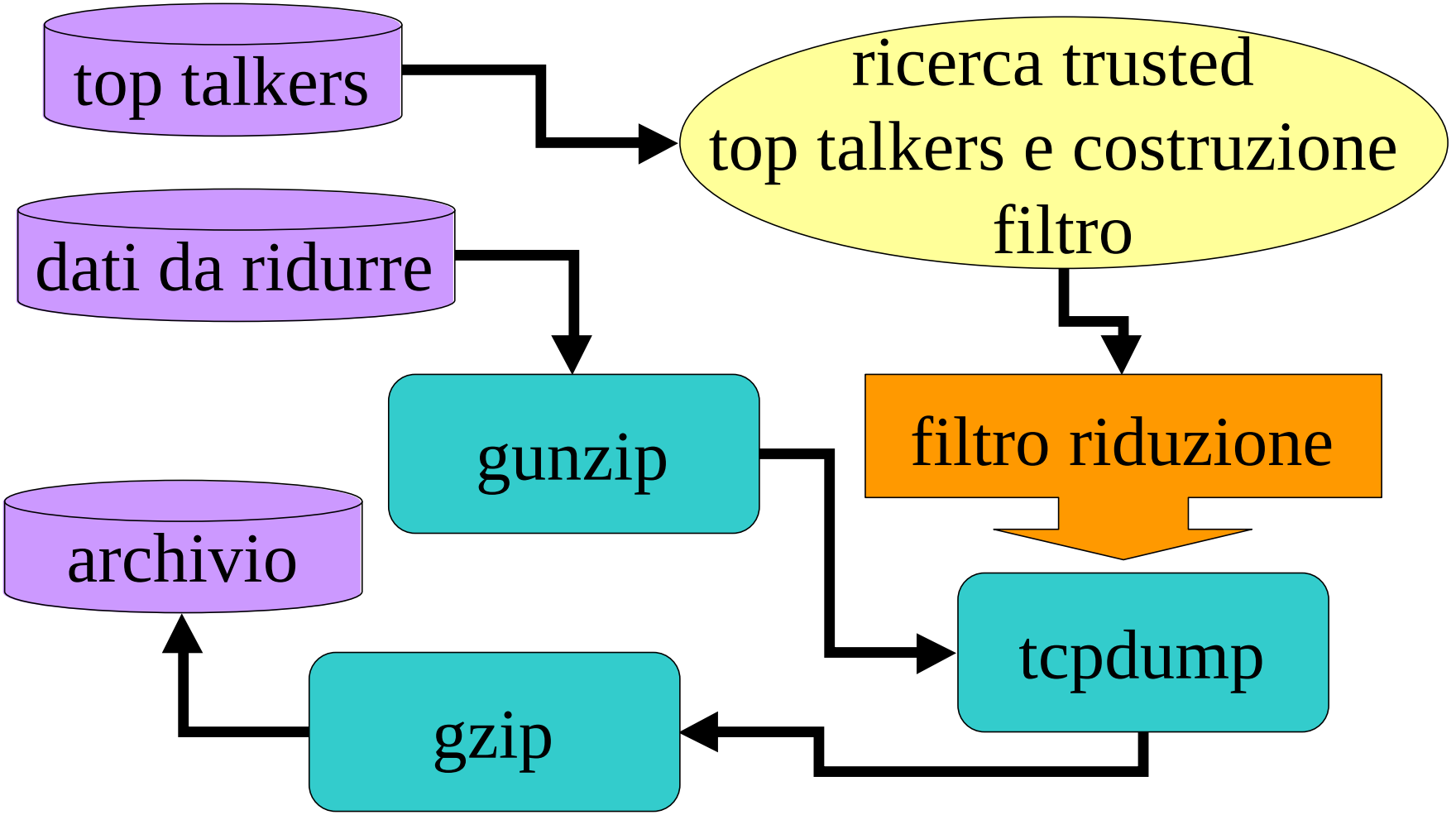
altri filtri

- `ip[6:2] & 0x2000 != 0`
- `ip[6:2] & 0x1fff > 0`
- `ip and ip[12:4] = ip[16:4]`
- `ip and ip[19] = 0xff`
- `icmp[0] != 8 and icmp[0] != 0`
- `tcp and (tcp[13] & 3 != 0)`
- `tcp and (tcp[13] & 3 = 3)`

Formato del pacchetto IP

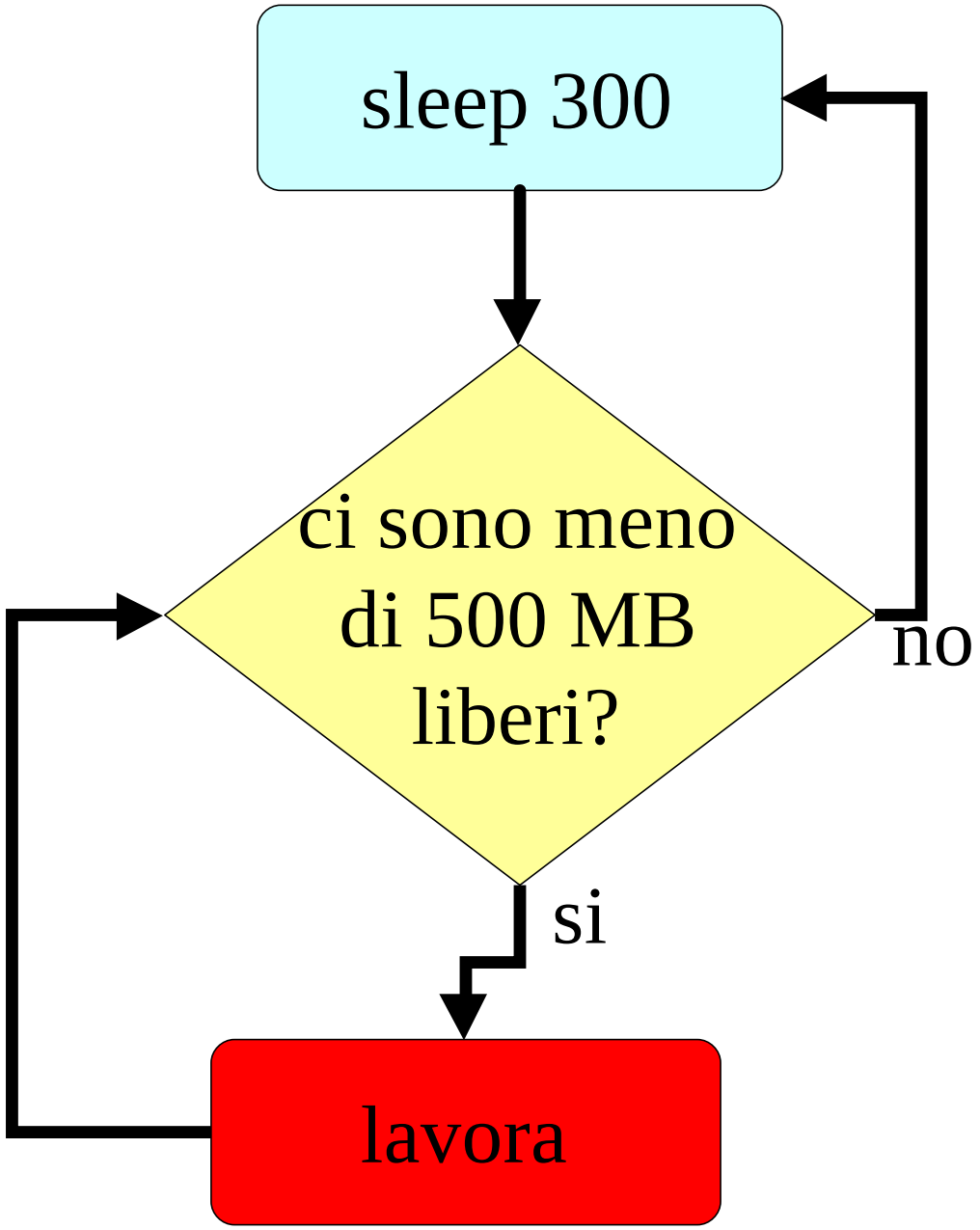


riduzione dati (filter)



ogni ora il file acquisito 48 ore prima viene spostato tra i dati da ridurre

cleaner



Archivio

Condizioni di utilizzo:

- spazio disco per i dati : 18 GB
- traffico medio con l’esterno di 2/3 Mb/s
- filtri di riduzione aggiornati
- massima lunghezza acquisita per ogni pacchetto: 68 byte

In queste condizioni si riesce a conservare online il traffico di un paio di mesi

Sviluppi futuri

... Anzi, **problemi futuri**:

- Il traffico di rete e` destinato ad aumentare esponenzialmente (GARR-G , Gigabit ethernet)
- Le LAN evolvono verso una sempre maggiore complessita` (routing interno alla LAN)

Implicazioni legali

- E` il caso di avvertire i nostri utenti che e` attivo un sistema di monitoraggio del traffico?

codice penale: art 617quater (aggiunto dall'art. 6 L. 23/12/93, n.547)

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra piu` sistemi, ovvero le impedisce o le interrompe, e` punito con la reclusione da sei mesi a 4 anni.

Salvo che il fatto costituisca piu` grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

....

Riferimenti

SHADOW

- **http://www.nswc.navy.mil/ISSEC/CID/**
- http://www.nswc.navy.mil/ISSEC/CID/step.htm
- http://www.nswc.navy.mil/ISSEC/CID/step_tar.gz

The SANS Institute

- **http://www.sans.org**

Network Intrusion Detection FAQ

- http://www.robertgraham.com/pubs/network-intrusion-detection.html
- http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html
- http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

Questa presentazione

- **http://www.pd.infn.it/~gravino**/computing/security/meeting/