# Attivita' del Servizio Calcolo

Andrea Rappoldi

Pavia, 19/02/2007

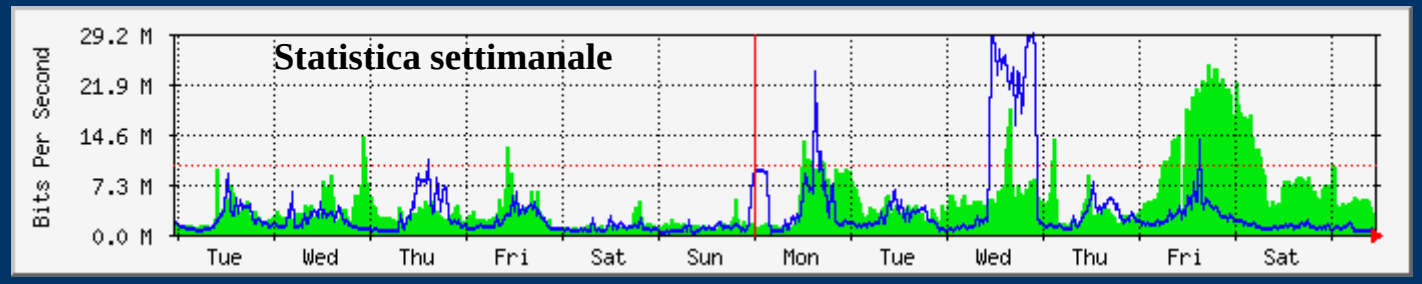
## Infrastruttura di rete

**LAN**

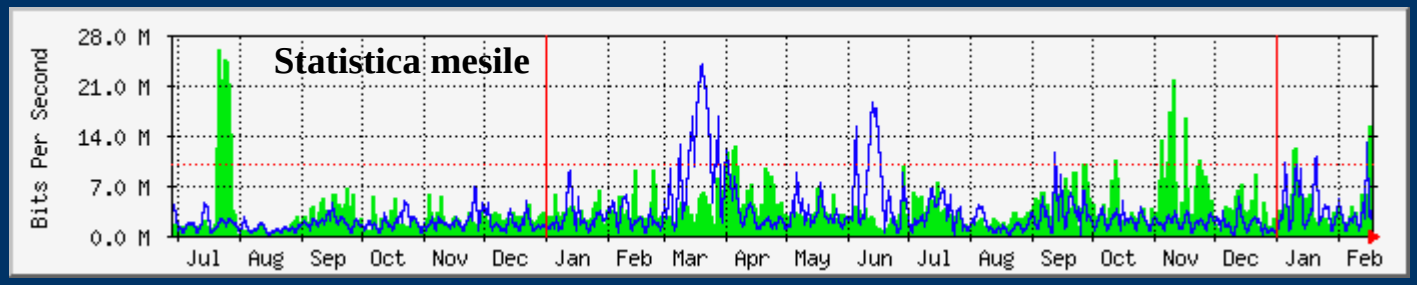
- **674** indirizzi IP utilizzati su **762** disponibili (88.5 %)
  Riutilizzo degli indirizzi non in uso (c'e' una certa “reticenza”...)
  *L' indirizzo IP e' come la targa di un autoveicolo*

**WAN**

- **10** Mbit/s BGA **30** Mbit/s BEA




**Input**
**Output**



# Gestione degli account – Posta elettronica

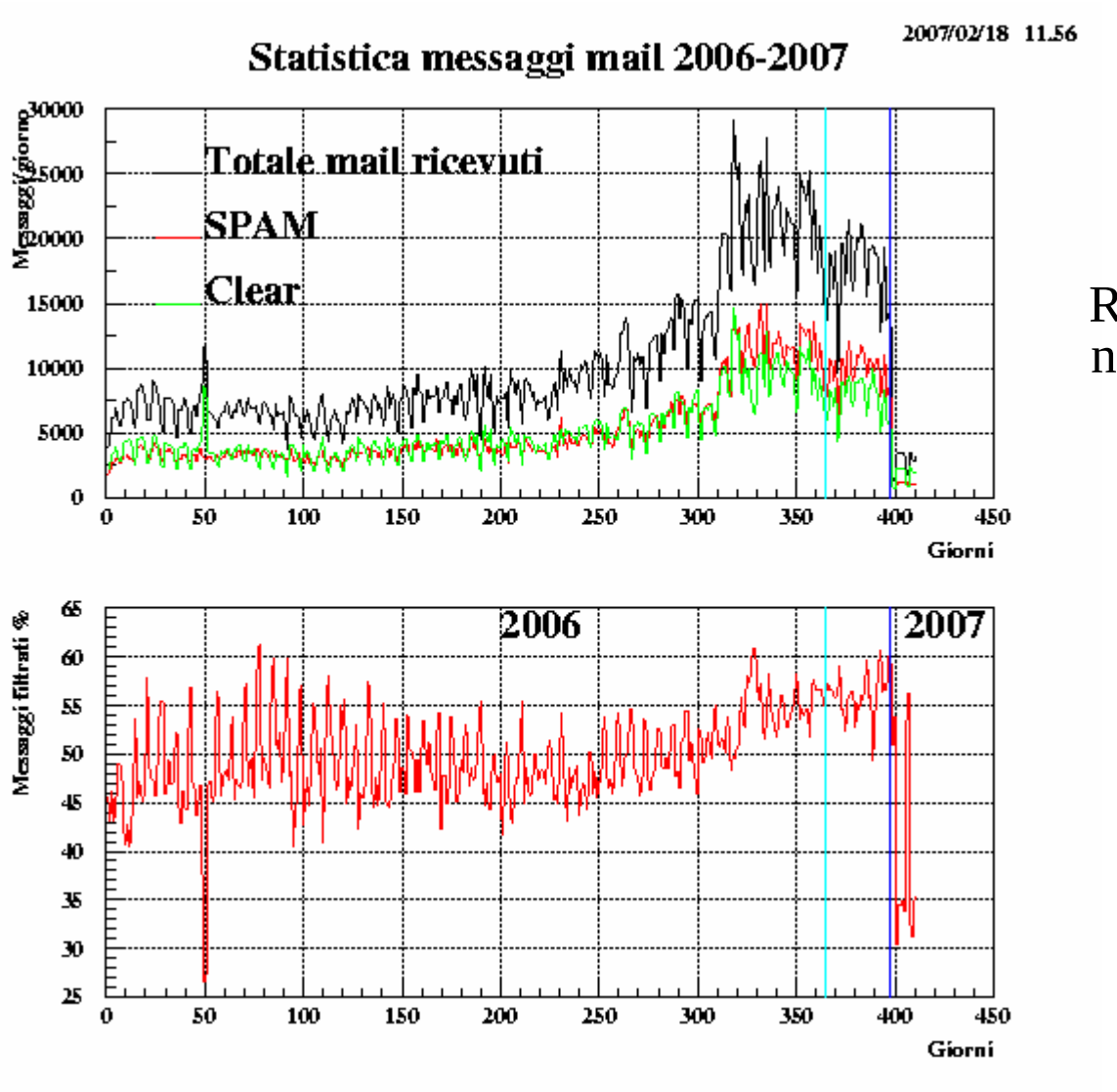
**215** account di posta elettronica: **53** GB utilizzati su **270** GB disponibili (~20 %)
acesso tramite protocollo **IMAPS** (crittografato) al server **`mailbox.pv.infn.it`**
oppure tramite ***Webmail*** (portale Web)

Filtro anti-spam "***SpamAssassin***" con meccanismo di auto-apprendimento
...purtroppo non viene molto usato... (vedi grafico seguente)

**89** utenti utilizzano il folder **SPAM** (per separare i messaggi filtrati);
**53** utenti utilizzano la cancellazione automatica periodica degli SPAM;
**86** utenti utilizzano l' auto-apprendimento del filtro.

Quindi l' efficienza media del filtro risulta "non entusiamante": circa il **50 %**
(mentre potrebbe essere il 99 %...)

# Filtro anti-spam (1)




Raddoppio traffico negli ultimi 3 mesi

**Attivazione "greylist"**

# Gestione degli account – Server Linux

**216** account interattivi: **28** GB utilizzati su **196** GB disponibili (~14 %)
Scientific Linux CERN (SLC) **3.0.8**, con aggiornamenti automatici

Il sistema Linux ospita anche il Server Web di Sezione **`www.pv.infn.it`**
con **101** siti *personali*: **`http://www.pv.infn.it/~username`**

... purtroppo sembra essere poco consultato il sito web del Servizio Calcolo...

**`http://www.pv.infn.it/sc`**

Che fornisce molte delle informazioni che vengono richieste piu' di frequente..
(*potrebbe* dare molte risposte alle domande frequenti)

# Servizi di rete – mailserver (SMTP)

Per motivi di sicurezza, un unico server SMTP (**`mailserver.pv.infn.it`**) e' abilitato a inviare/ricevere i messaggi da/per il dominio **`pv.infn.it`**

Tale server supporta il meccanismo **STARTTLS** per effettuare la trasmissione criptata dei messaggi

Utilizza un certificato X509 emesso da INFN-CA per *identificarsi* ed *autenticare* altri server SMTP dotati di certificato X509 valido

Questo consente di superare meccanismi di rigetto tipo *black-list* o *grey-list*
Purtroppo tale meccanismo non e' universalmente adottato
(16 domini INFN su 34, NO Cern, NO Fnal, NO Desy,...)

Supporto per accesso utente autenticato (**AUTH**)

# mailserver

Visto il continuo crescere del traffico SPAM, e dato lo scarso utilizzo del meccanismo di auto-apprendimento di *SpamAssassin*, e' stato recentemente attivato un ulteriore livello di filtro anti-spam, basato su **grey-list**, direttamente sul server SMTP

Meccanismo **semplice** ma **efficace**: rifiuta tutti i messaggi che non provengono dai server "***seri***", normalmente dotati di un meccanismo di coda

(Ovvero: rifiuta le operazioni di "***volantinaggio***")

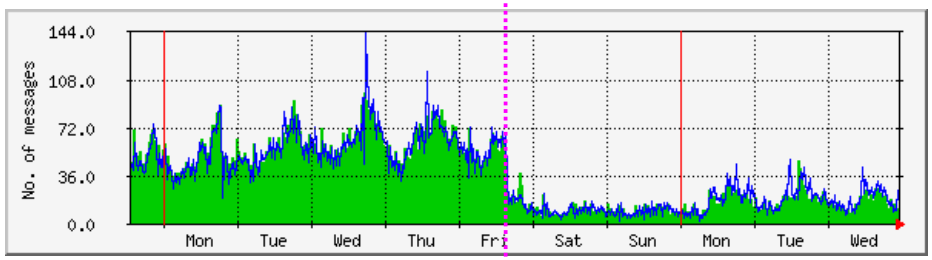
Tale meccanismo puo' introdurre un ritardo di circa *mezz'ora* sul ricevimento del *primo* messaggio proveniente da un *determinato* mittente

I messaggi successivi (entro un intervallo di 5 giorni) non subiscono alcun ritardo

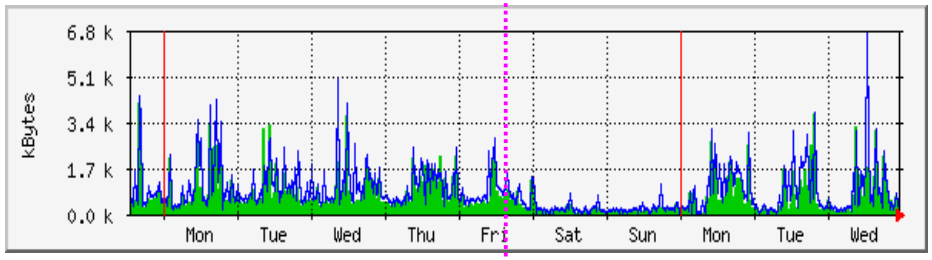
Effetto notevole: riduzione di un fattore **10** del numero di messaggi SPAM

# Filtro anti-spam (2)

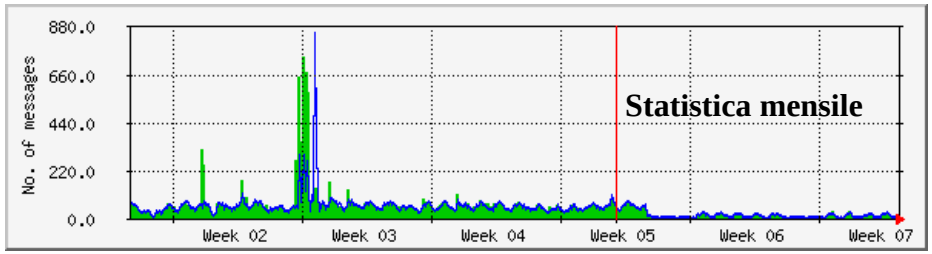
**Attivazione greylist**




Messaggi

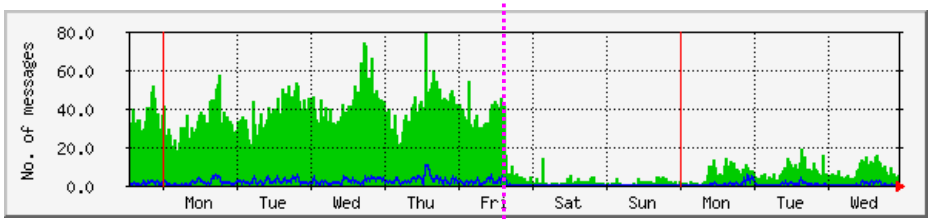



Size

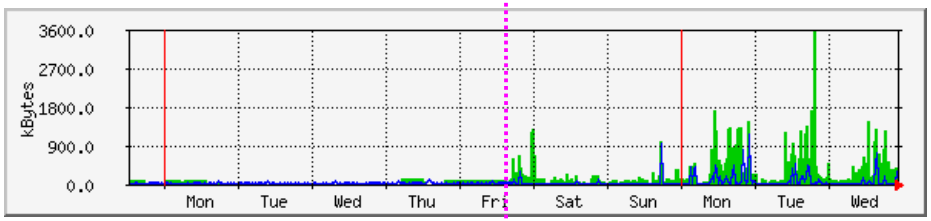



Messaggi

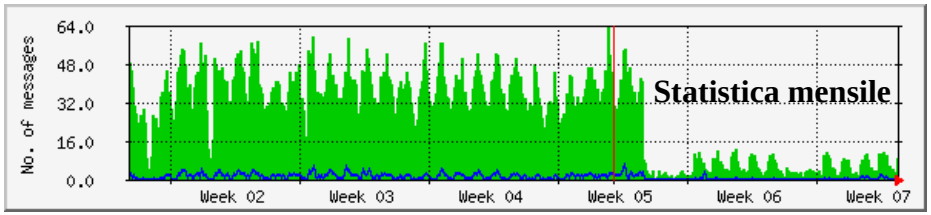
**Attivazione greylist**




Messaggi



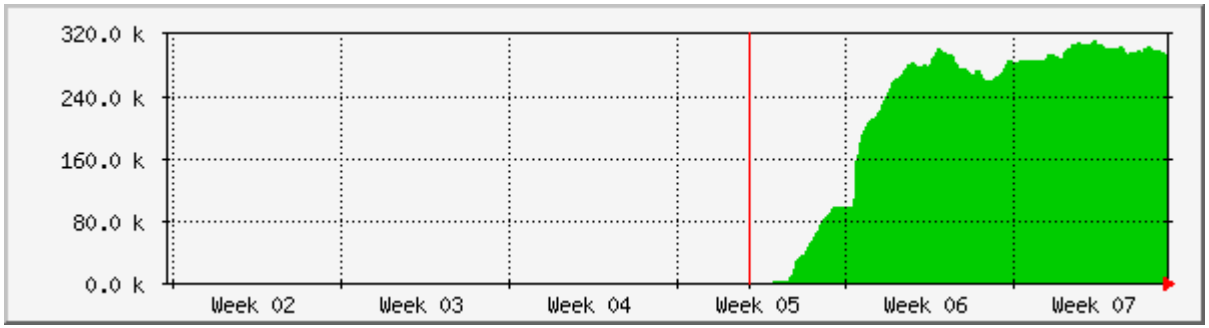

Size



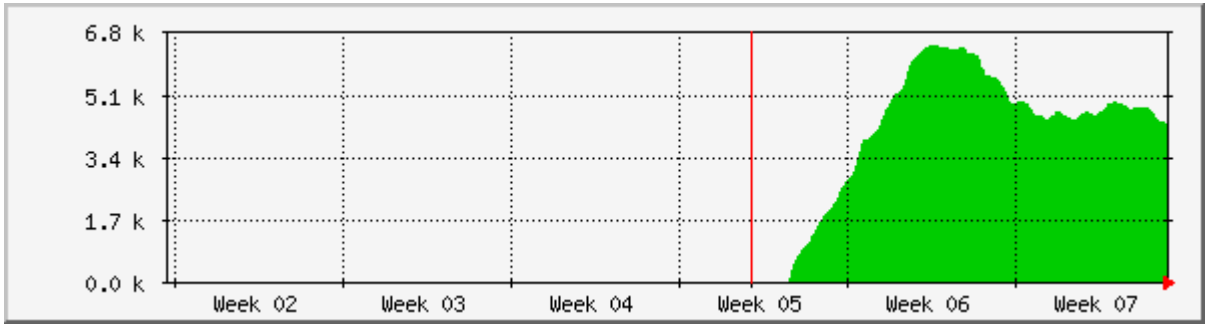

Messaggi

# Statistica di funzionamento del filtro basato su grey-list

grey-list




white-list



# Rete Wireless

5 *access point* dual-band (2.4 GHz e 5 GHz), con velocita' fino a **54 Mbit/s**

- Sala riunioni
- Zona teorici (lato scale)
- Zona teorici (lato ascensore)
- Zona Gruppo III
- Nuova palazzina (via Ferrata)

(A breve verranno installati altri 2-3 access-point per completare la copertura)

Sono possibili **3** modalita' di accesso alla rete *wireless*:

- Mediante MAC address: NON criptato, hardware-dipendente
- Tramite portale Web: NON criptato, user-dipendente, uso certificati
- Protocollo 802.1x: comunicazioni criptate, user-dipendente

# Rete Wireless

Le ultime due modalita' rientrano nel progetto **TRIP**, che si propone di semplificare la mobilita' del personale INFN tra le varie Sezioni e Laboratori

Ogni utente puo' autenticarsi (e ottenere l' uso della rete *wireless*) identificandosi con:

username@sezione.infn.it (oppure mediante certificato X509)

indipendentemente dal luogo in cui si trovi

Tale modalita' non e' ancora attiva in tutte le Sezioni (a Pavia lo e' da Agosto 2006)

E' previsto anche un sistema di gestione degli **ospiti**, che consentira' di attivare degli *account temporanei*, mediante una semplice interfaccia Web (ad uso delle Amministrazioni locali)

# Gestione degli "*incidenti*" informatici

L' ultimo episodio ha richiesto circa 2 settimane per essere risolto

Nonostante tutto, i nostri server sono **sicuri**...

- SW aggiornato alle ultime versioni (automaticamente)
- Configurazioni attente alle vulnerabilita'
- Firewall abbastanza "***severo***"

La falla e' stata creata da un utente che utilizzava uno script "***ingenuo***" sul proprio sito Web, che consentiva l' importazione di SW malevolo
(era come una finestra con i vetri appena accostati...)

**Risultati** - utilizzo del server SMTP per l' inoltro inconsapevole di messaggi SPAM
- inserimento del server SMPT nella *black-list* SORBS
(dalla quale si viene rimossi solo facendo opere di beneficenza...)

**Fortunatamente** ora ne siamo usciti (piagnucolando solo un po' !)

Questo ci ha fatto capire la debolezza dei *forward* automatici:

Non possiamo sapere come si comportano i *provider*
(se si basano o meno sull' uso di certe *black-list*)

L' ideale sarebbe far sempre ricorso all' **autenticazione**, ma il problema di base e' che la *Certification Authority INFN* non e' universalmente riconosciuta...

# Strumenti di pubblica utilita' forniti dal Servizio Calcolo

**Programma di richiesta trasferte**

E' stato presentato al Workshop di Commissione Calcolo e Reti del 2006, riscuotendo un certo successo

Altre Sezioni lo hanno utilizzato o preso come modello (es. Milano)

**Kit di installazione Scientific Linux CERN**

**Kit di installazione Windows XP e software Microsoft**

**Tool di installazione Sophos antivirus**

# Progetti futuri (lavori in corso)

**Realizzazione della nuova *"sala macchine"***

Ospitera' il nuovo Pop GARR di Pavia, destinato a servire INFN, Universita' ed I.R.C.C.S.

Riorganizzazione spazi

**Sistema unificato di *autorizzazione* ed *autenticazione***

Basato su Kerberos V e LDAP, da utilizzarsi per:

- login interattivo;
- Accesso alle caselle di posta elettronica;
- Accesso alla rete *wireless*;
- Utilizzo del server SMTP autenticato;
- AFS.

**Programma di prenotazione delle sale riunioni**

**Nuovo software amministrativo**

# Personale del Servizio Calcolo

**2 tecnologi INFN** (20 % Servizio calcolo, 80 % supporto esperimenti)
**1 tecnico INFN**
**1 tecnico Dip. Fisica Nucleare e Teorica**

Il personale INFN fornisce il supporto di base dei servizi gia' descritti, con qualche contributo specifico:

- **A.R.** Coordinamento Servizio, Commissione Calcolo e Reti, gestione incidenti, sistemi Linux
- **C.d.V.** Integrazione dei servizi, sviluppo delle nuove tecnologie
- **R.C.** Tool amministrativi e supporto Amministrazione, sistemi Windows
- **C.C.** Contratti software e manutenzioni, sistemi Macintosh

**Supporto agli esperimenti.** E' un contributo di una certa importanza

- Programmi di DAQ (C.d.V. - Gr. I)
- Analisi dati (A.R. - Gr. II)
- Simulazioni (A.R. - Gr. II)

# Considerazioni finali

## Servizi da garantire

- Infrastruttura di rete LAN e WAN (conforme GARR)
- Posta elettronica affidabile e sicura
- Utilizzo PC Windows XP, SLC, Mac (con reinstallazione in caso di problemi)
- Disponibilita' personale nelle fasce orarie comuni (9:30-12:00, 15:00-16:30)
- Intervento in caso di guasti entro 4 ore negli orari di lavoro

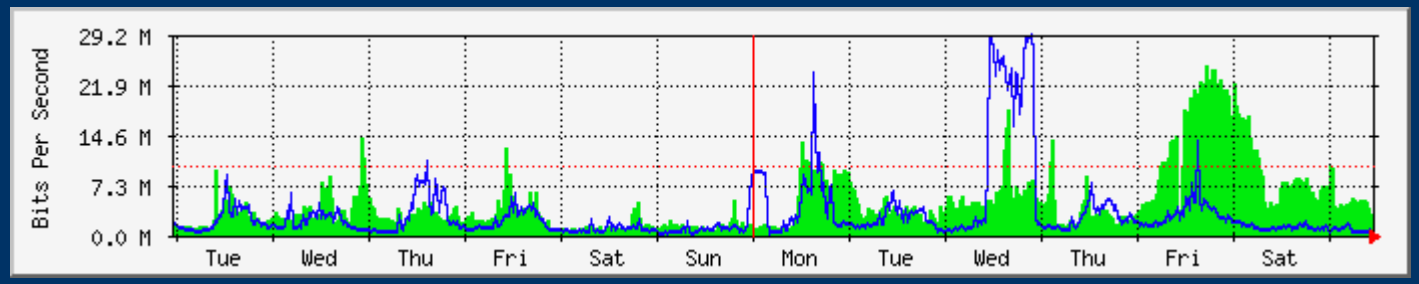
## Cosa occorre

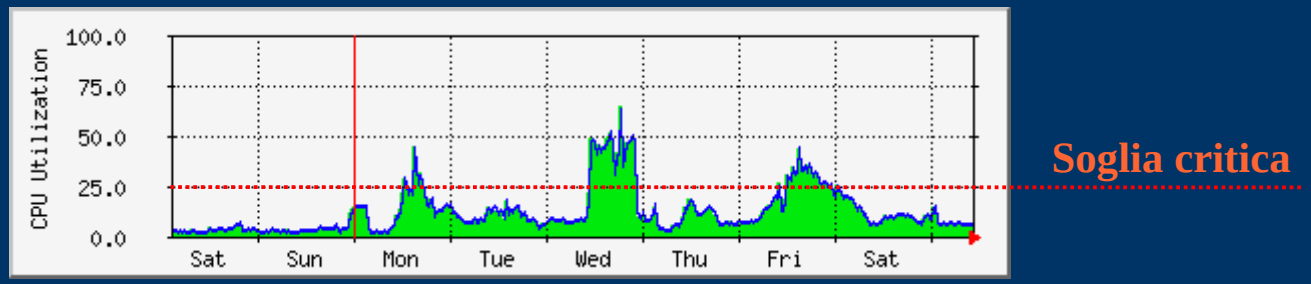
- Una persona in piu' (tecnico)
- Segreteria telefonica con registrazione messaggi
- Telefoni cellulari di servizio individuali (i *cordless* non funzionano)
- Schede di connessione tipo UMTS per i portatili (per effettuare sorveglianza)

# La Fine

# Il *router* (di accesso alla rete GARR) risulta a volte sovraccarico

Questo e' causa (talvolta) di alcuni rallentamenti generali (per via delle *access-list*)




A breve si rimediera' sostituendo il *router* con uno *switch L3*