Organizzazione servizio e-mail

Francesco Gennai

CNR - IAT

Reparto elaborazione comunicazione e sicurezza dell'informazione

Organizzazione servizio e-mail

Contenuti

- Modello CMDA (centralized management with delegated administration);
- Esperienza nell'utilizzo del modello per l'hosting del servizio di PE.

Organizzazione di un servizio di rete

- installazione/configurazione del sistema
  - personale altamente specializzato
- monitoraggio ed operatività del servizio
  - personale tecnico
- amministrazione
  - personale non specializzato

Modello per l’organizzazione di un servizio di rete

Organizzazione servizio e-mail

Centralized management with delegated administration (CMDA)

- gestione centralizzata del server (maintenance, monitoraggio, etc.)
- delega dell'amministrazione del servizio (alle singole unità dell'organizzazione)

Vantaggi del CMDA

- riduce il numero dei server al minimo numero tecnicamente richiesto
- semplifica il controllo e la gestione del servizio
- facilita l'introduzione di nuovi servizi (come integrazione con directory) perchè si ha il controllo tecnico del servizio
- riduce i costi
- flessibile (max autonomia amministratori locali)
- preserva i tempi di risposta (per gli utenti)
- applicabile a diversi servizi: posta elettronica, web, dns.

Limitazioni del modello CMDA

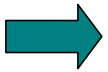
- banda garantita (se si adotta su scala geografica)
  - Infrastrutture sono affidabili, le distanze sono “virtuali” (valutare il ritardo nella comunicazione a livello locale);
  - La comunicazione tra client e server può utilizzare un canale cifrato.

Applicazione del modello nel servizio di Posta elettronica

- Sviluppo di interfacce web per gli amministratori periferici -> creazione, modifica, cancellazione di mailbox, alias, liste distribuzione, etc. nel proprio/i dominio/i di PE
- Sviluppo “accurato” di CGI che si appoggia sulle API fornite dal prodotto di PE
  - estensivo controllo degli errori

Ulteriori vantaggi del modello

- Riduce gli errori umani
- Non richiede personale specializzato
- Organizzazione host dei servizi di PE non gestisce la parte di amministrazione



aumento dei domini **non** aumenta i compiti per l'organizzazione che gestisce e monitorizza il servizio

La prima esperienza di utilizzo del modello CMDA

Hosting del servizio di PE per l'Università degli Studi di Pisa 1994/95

Interfaccia a due livelli

- Il primo livello per gestire i sotto-domini di unipi.it per aggiungere/rimuovere sottodomini dal sistema di e-mail
- Il secondo livello per gestire caselle di posta elettronica e alias per gli utenti

Realizzazione

- Instradare il traffico di PE dell'università verso il nostro sistema di e-mail -> inserito un MX record nel DNS dell'università che puntava al nostro server di e-mail
- Per rendere flessibili le configurazioni degli utenti dell'università (usare nomi di server nel dominio dell'università) -> definiti CNAME
  - mail.unipi.it -> mail.cnuce.cnr.it
  - pop.unipi.it -> pop.cnuce.cnr.it
  - smtp.unipi.it -> smtp.cnuce.cnr.it

  trasparenza della configurazione degli utenti (in caso di migrazione del servizio)

Introduzione del modello in altre realtà

Un esempio: situazione istituto CNUCE

Da una indagine fatta nel 1997 sono risultati attivi, nel solo CNUCE, 52 smtp server (vecchie versioni, non correttamente configurate, non gestite).

- Punto di debolezza nella sicurezza dei sistemi.

Problema: convincere le persone ad eliminare questi server (la flessibilità dell'interfaccia di amministrazione e la trasparenza nella configurazione del servizio).

Introduzione del modello in realtà accademiche

L'interfaccia testuale -> web

Hosting del servizio di PE per il CNR (area di Pisa, area Perugia, Istituti di Ancona, Terni, Matera)

- 18 domini

Nell'area di ricerca di Padova è attivo un analogo servizio

In attivazione presso Università di Genova

Alcune note tecniche

Organizzazione servizio e-mail

- Alcune note tecniche sul sistema di PE
  - server ad elevate prestazioni e sicuro
    - SMTP, POP e IMAP server MULTITHREAD
    - database autenticazione sono diversi da quelli di sistema
    - SASL (Simple Authentication and Security Layer - RFC2222) per supporto diversi metodi di autenticazione:
      - metodi di autenticazione standard per evitare il transito in chiaro di user e password (CRAM-MD5 - RFC 2195, DIGEST-MD5 - RFC 2831)
    - possibilità di sessioni TLS
    - flessibilità in configurazione policy di sicurezza

Organizzazione servizio e-mail

Multipurpose Internet Mail Extensions (MIME)

Headers, indirizzi

To:
From :
cc:
Subject

Multipart message (attachments)

Normale parte testo

Uno o più "attachment"

- ***Immagine GIF***
- ***Documento MS Word***

Messaggio rispedito (Forward)

Organizzazione servizio e-mail

Esempio messaggio MULTIPART

```
From: .....
Subject: ....
Content-type: multipart/mixed; boundary=AAAconfine
--AAAconfine .....
parte contenente testo in US-ASCII infatti non e' marcata con
Content-transfer-encoding
--AAAconfine .....
Content-type: multipart/parallel; boundary=XXXsepara
--XXXsepara .....
Content-type: audio/basic
Content-transfer-encoding: base64
..... dati audio codificati in base64
--XXXsepara .....
Content-type: image/gif
Content-transfer-encoding: base64
... dati per immagine gif codificati in base64
--XXXsepara-- .....
--AAAconfine .....
Content-type: text/plain; charset=ISO-8859-1
Content-transfer-encoding: quoted-printable
testo scritto in ISO-8859-1, questo testo =E8 codificato con=
  =93quoted-printable=94
--AAAconfine-- .....
```

Organizzazione servizio e-mail

- autenticazione SMTP
  - logging username di chi invia il messaggio
  - autorizzazione a fare relay (utile per consentire l'utilizzo del server SMTP da postazioni remote anche in presenza di restrittive configurazioni anti-spamming)
- potenti capacità di filtraggio messaggi
  - rimozione/sostituzione singola parte di un messaggio MIME
  - supporto di SIEVE

Organizzazione servizio e-mail

Esempio: sostituzione parte di messaggio MIME Multipart

From: .....
Subject: ....
Content-type: multipart/mixed; boundary=AAAconfine

--AAAconfine
Content-type: text/plain

Caro Guido,
ti invio il documento word
Ciao,
Antonio

--AAAconfine
Content-type: application/msword; name=relvir.doc

Il file relvir.doc presente in questa parte di messaggio
e' stato cancellato perche' probabile virus (relvir.doc)
HHHSGWFFWDDEADDADADSDADADADDAD
--AAAconfine--

Organizzazione servizio e-mail

- Politica amministrativa del servizio flessibile (NON dipende dal centro di gestione tecnica)
  - Scelta dall'amministratore del dominio
    - Controlli ORBS, MAPS
    - Filtraggio messaggi (in base MIME Content-type, nome file attachment, antivirus, dimensione, etc.)
- Delivery Notification relative ad un dominio possono essere generate come provenienti da postmaster@dominio (invece di un generico postmaster@localhost)
  Esempio (prossima pagina)**:**

Organizzazione servizio e-mail

- Esempio:
  - nome host: **mail.iat.cnr.it**
  - dominio ospitato: **ict.pi.cnr.it**
  - messaggio indirizzato a: **mari.rossi@ict.pi.cnr.it**
  - **mari.rossi** NON esiste -> il sistema genera una *Non-Delivery-Notification*
    From: **postmaster@ict.pi.cnr.it**
    (non postmaster@mail.iat.cnr.it)

Vantaggi: eventuali richieste di aiuto potranno essere indirizzate a chi veramente conosce "l'ambiente" ICT.pi.cnr.it

Organizzazione servizio e-mail

- Esempi di flessibilità amministrativa:
  - gestione ORBS/MAPS
    - se l'indirizzo IP sorgente della connessione SMTP è presente in uno dei database ORBS o MAPS:
      - ***si rifiuta la connessione***
      - ***si aggiunge una linea all'header***
        (Esempio: X-MAPSORBS: <ip-address>)

Attualmente questo controllo viene fatto solo per messaggi diretti al dominio cnuce.cnr.it

Organizzazione servizio e-mail

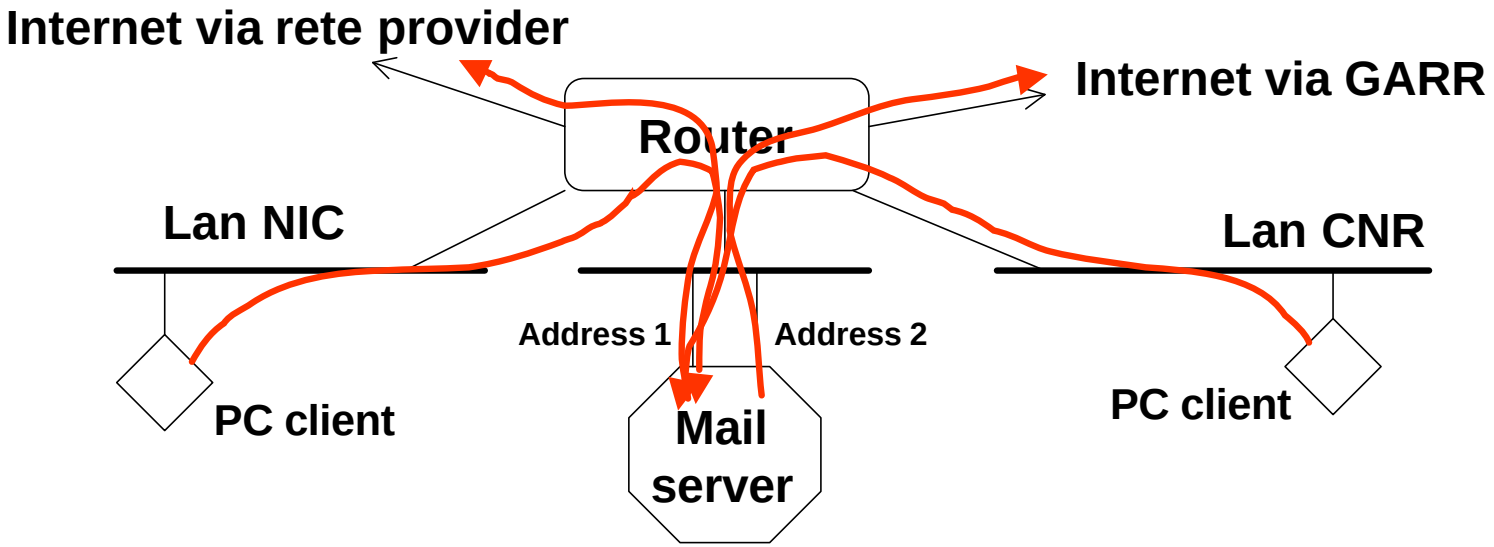
- Esempi di flessibilità amministrativa:
  - filtri su attachment in base al nome file (se specificato)

    la parte di messaggio viene sostituita con un normale testo di avviso, lasciando invariate le eventuali altre parti della struttura MIME.
    Esempio: parti con estensione nome file uguale a .vbs vengono sostituite con una parte testo contenente l'avviso su sostituzione.

Attualmente la sostituzione è limitata solo ad alcuni domini (iat.cnr.it, cnuce.cnr.it, etc…)

Organizzazione servizio e-mail

- Un caso limite (molto significativo)
  - Domini con diverse policy di routing.
    Il caso di: *xxx.pi.cnr.it* e *nic.it*
    - In ingresso soluzione semplice per mezzo di MX record
    - In uscita:



Organizzazione servizio e-mail

Affidabilità del servizio

- OpenVMS SCSI cluster costituito da due sistemi.
  Condivisione RAID disk array.
  Load balancing (a livello IP address);
- Questo ci abilita ad effettuare maintenance su un nodo, senza alcuna interruzione del servizio.

Interfacce di amministrazione

Schema di naming

- Ogni dipartimento/istituto ha una propria politica per la definizione della parte locale dell'indirizzo

  (cognome@dominio, nickname@dominio, nome.cognome@dominio)

  Le interfacce di amministrazione favoriscono l'introduzione di uno schema di indirizzamento comune.

Interfacce di amministrazione

Dal nome e cognome automaticamente creano l'indirizzo ufficiale

- nome.cognome@dominio

e gli alias:

- iniziale-nome.cognome@dominio
- cognome@dominio

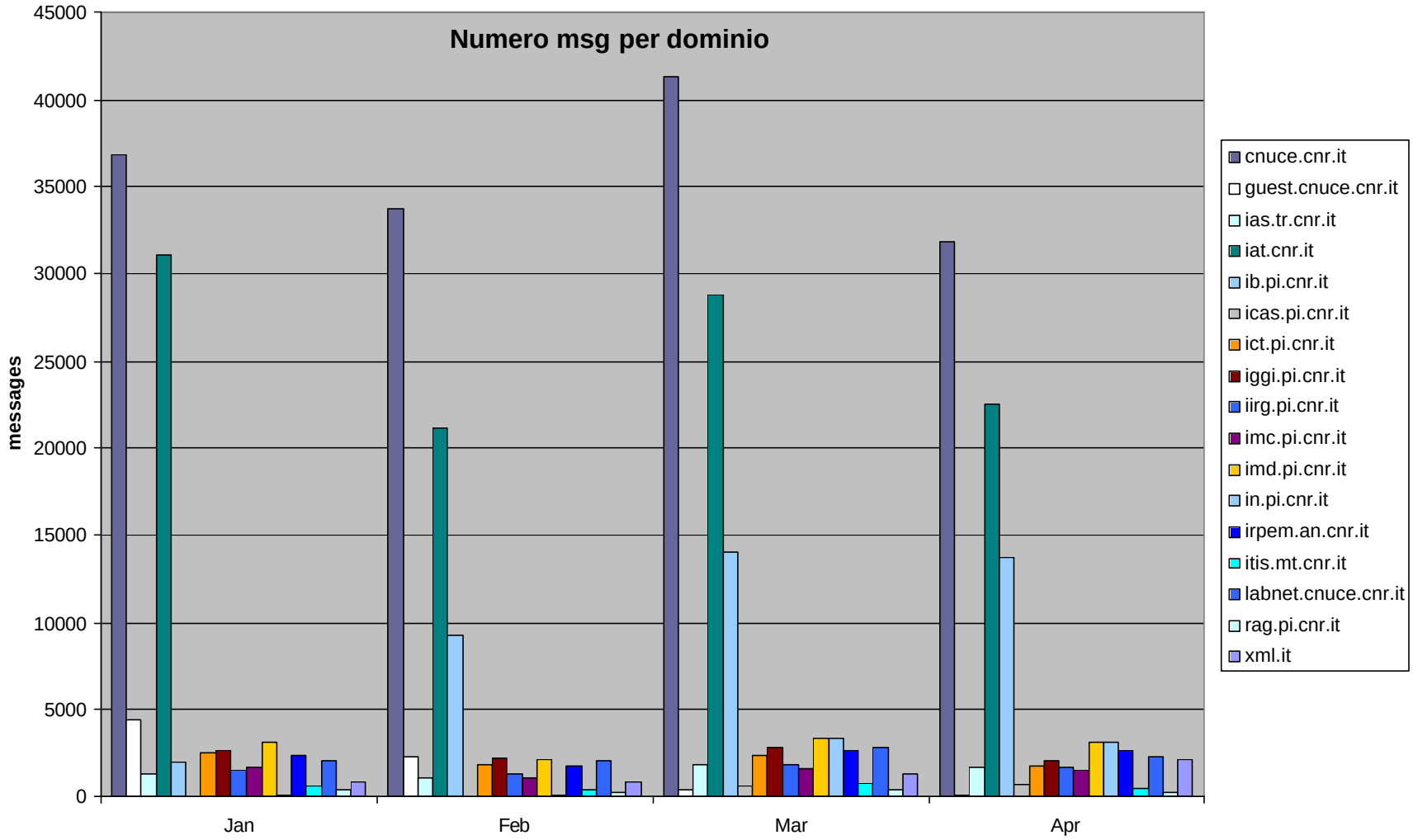
Gestiscono indirizzi di ruolo (segreteria@dominio, presidente@dominio)

Organizzazione servizio e-mail

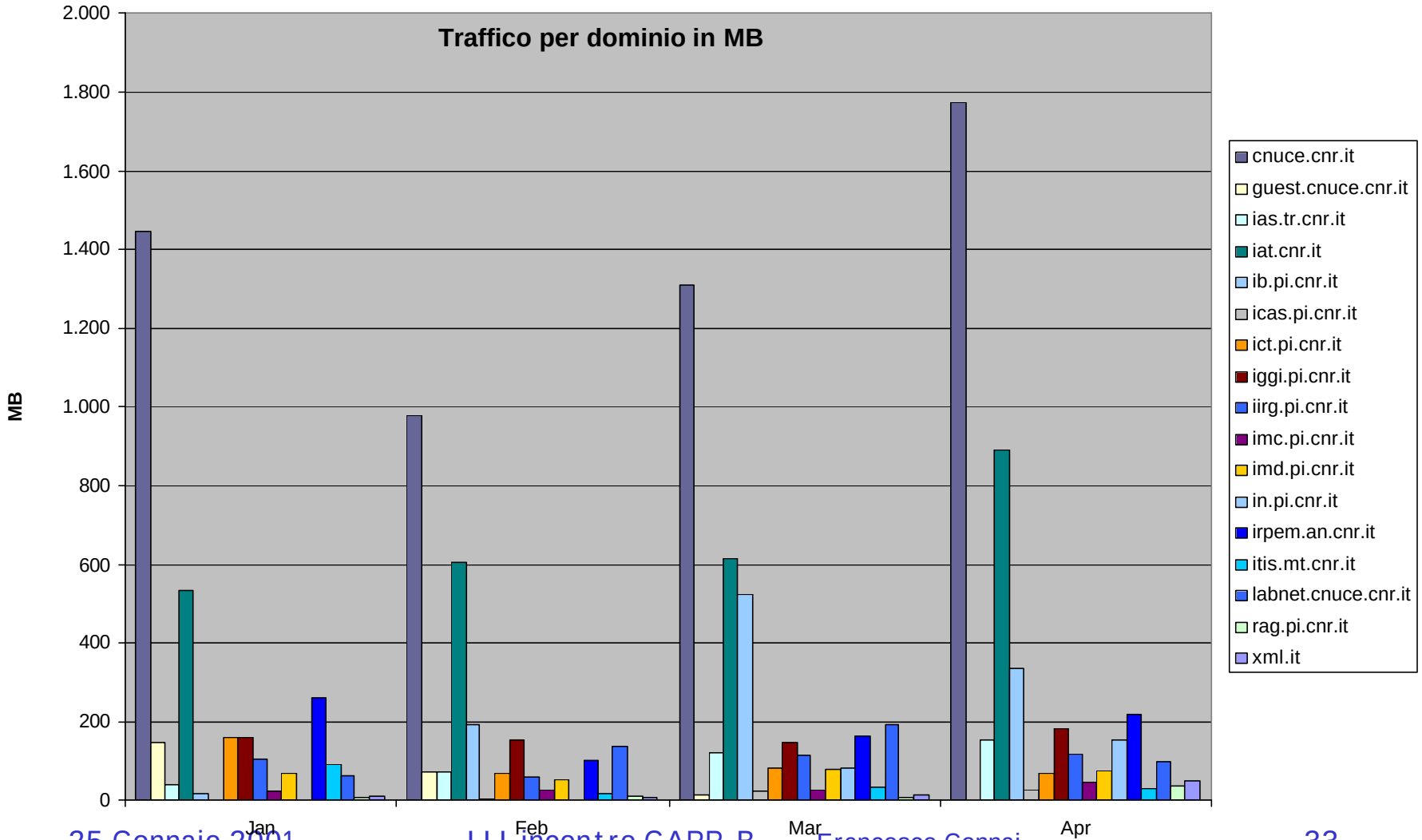
- Un approccio basato su Directory Server LDAP
  - Query LDAP per:
    - risoluzione indirizzi e alias
    - autenticazione POP, IMAP e SMTP
    - liste di distribuzione create/gestite dinamicamente
    - risoluzione inversa degli indirizzi

Le statistiche di utilizzo del servizio

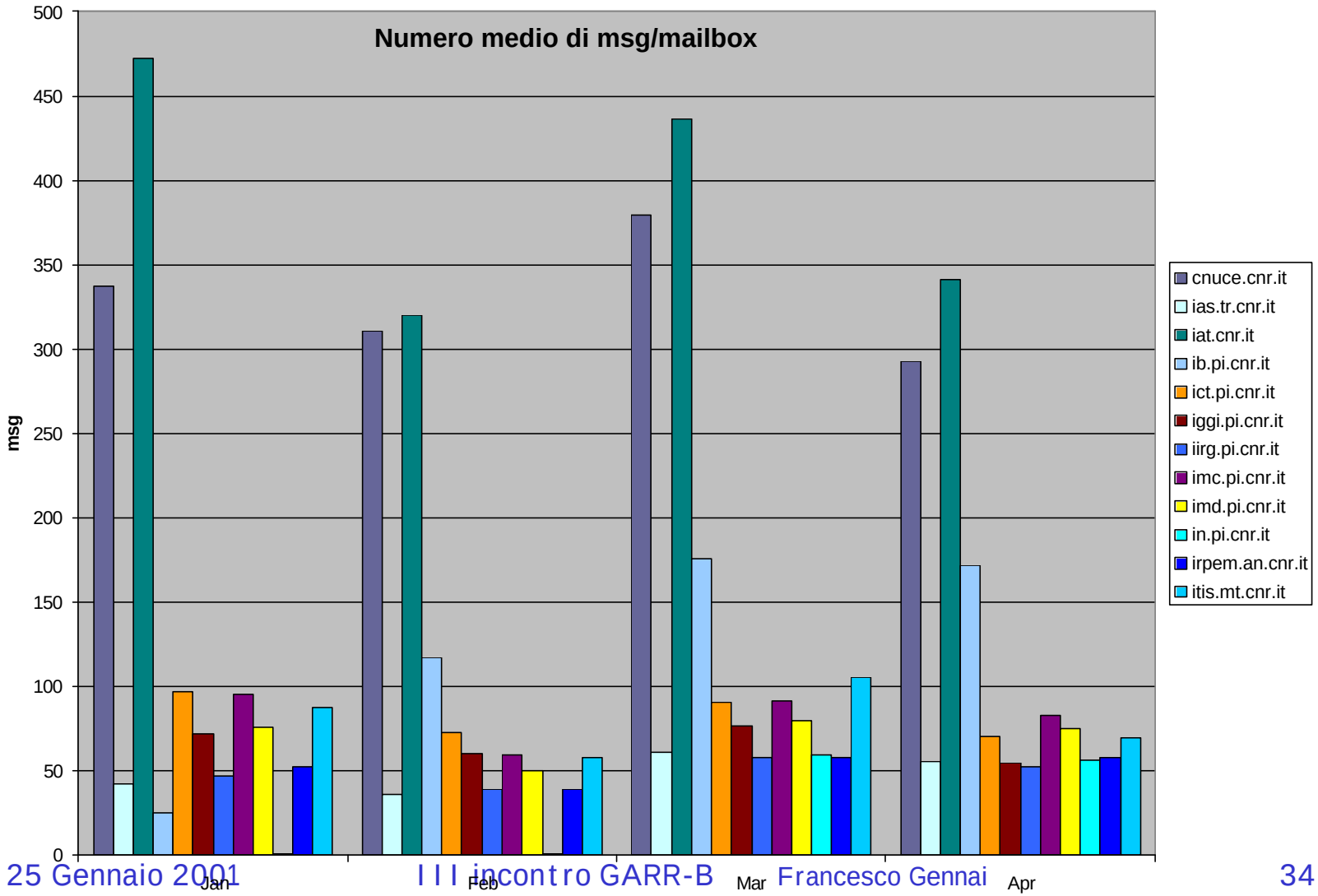
Organizzazione servizio e-mail



Organizzazione servizio e-mail



Organizzazione servizio e-mail



Organizzazione servizio e-mail

Valutazione del servizio

Istituti dove non hanno personale tecnico, hanno mostrato interesse per questo modello organizzativo.

Il carico amministrativo è suddiviso tra tutte le unità

Il server mail.iat.cnr.it gestisce 18 domini. Riduzione del numero di server da 18 (quelli ufficiali) a 1 mantenendo lo stesso numero di persone per la gestione del servizio (2)

Organizzazione servizio e-mail

Utilizzo delle interfacce web

- le operazioni “critiche” sono effettuate dal sistema (gli amministratori non devono essere utenti privilegiati);
- automaticamente implementa la policy decisa dall’organizzazione per l’indirizzamento (p. es. nome.cognome@dominio).

Conclusioni

- Investimenti nell'implementazione del modello CMDA sono velocemente compensati dalla riduzione nei costi

Ambiente di utilizzo del CMDA

- Università, Pubblica Amministrazione, medie/grandi aziende, ISP
- CNR
  - Istituti con sezioni distribuite sul territorio nazionale

    Tramite l'interfaccia web i vari amministratori possono concorrere nel creare/cancellare mailbox e alias appartenenti allo stesso dominio.

    L'interfaccia di gestione è accessibile via https.

Sviluppi futuri

- Applicazione del modello anche per i servizi di DNS in modo da distribuire i compiti amministrativi sulle unità periferiche