

Corso di Laurea in Ingegneria Informatica



**Corso di Reti di Calcolatori
(a.a. 2009/10)**

**Roberto Canonico (roberto.canonico@unina.it)
Antonio Pescapè (pescape@unina.it)**

SMTP-POP3-DNS

Il protocollo SMTP



- Una volta che una e-mail è stata scritta attraverso l'uso di un programma su un personal computer, è necessario inviarla al destinatario/i
- Come è noto, il destinatario potrebbe non essere in quel momento disponibile ad accettare messaggi di posta:
 - utente impegnato
 - computer spento
- La posta elettronica sfrutta degli intermediari per il trasferimento delle e-mail tra le parti, alla stregua degli uffici postali che ospitano pacchi nell'attesa che i destinatari passino a ritirarli
- Per trasferire messaggi di posta elettronica tra gli intermediari si utilizza un apposito protocollo
- Si chiama *Simple Mail Transfer Protocol*, definito in RFC821

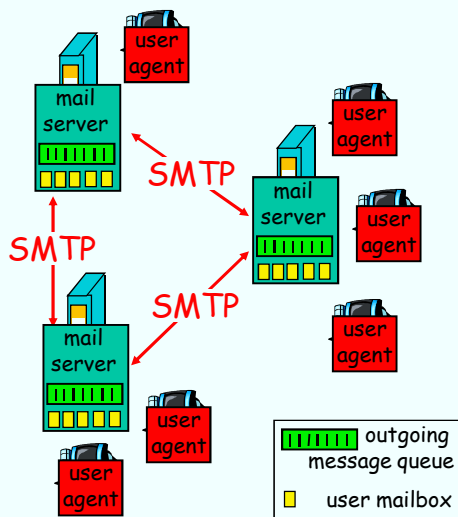
Le entità in gioco

Tre entità principali:

- user agents
- mail servers
- protocollo SMTP

User Agent

- anche detto mail reader
- composizione, modifica, lettura di messaggi
- es.: Eudora, Outlook, Netscape Messenger, Evolution, Kmail...
- messaggi in uscita ed in entrata immagazzinati sul server
- Il protocollo SMTP viene utilizzato anche tra user-agent e server durante l'invio di una mail

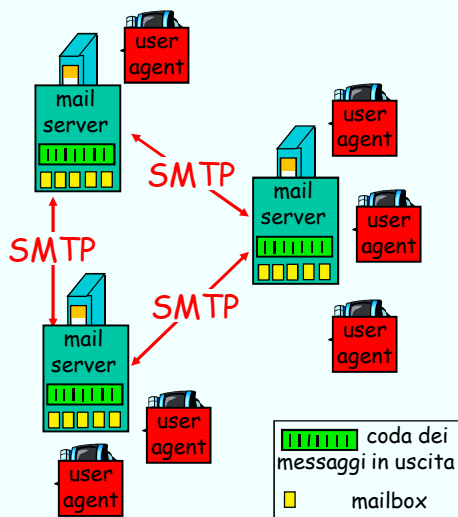


3

I mail server

Mail Server

- **mailbox** contenente messaggi in entrata (non letti) per l'utente
- **coda dei messaggi in uscita** contenente i messaggi non ancora recapitati
- **protocollo SMTP** a cavallo di due mail server.
 - "client": mail server mittente
 - "server": mail server destinatario
- Un "mail server" funge in momenti diversi da client o da server a seconda del ruolo che ricopre nello scambio del messaggio



4

Caratteristiche di SMTP (1)



- Usa il protocollo TCP (porto 25) per consegnare in modo affidabile messaggi dal client al server
- Trasferimento diretto dal server mittente al server destinatario
- Tre fasi durante il trasferimento via SMTP:
 - handshaking ("stretta di mano")
 - trasferimento del messaggio
 - chiusura della connessione
- Interazione comando/risposta (command/response)
 - **comandi:** testo ASCII
 - **risposta:** codice di stato e descrizione (facoltativa)
- Messaggi codificati con caratteri ASCII a 7-bit

5

Caratteristiche di SMTP (2)



- Usa una connessione persistente
- *push protocol* (vs. pull protocol come HTTP)
- Richiede che il messaggio, comprensivo del contenuto, sia codificato in caratteri ASCII a 7 bit
- Alcune combinazioni di caratteri non sono ammesse (p.es., CRLF . CRLF). Quando queste combinazioni si presentano il messaggio deve essere opportunamente codificato.
- SMTP usa CRLF . CRLF per determinare la fine di un messaggio

6

Esempio di interazione client → server



```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C:   How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

7

SMTP in pratica: uso con telnet (1/2)



- **telnet servername 25**
- Si osservi il codice 220 di risposta dal server
- Si inseriscano i comandi HELO, MAIL FROM, RCPT TO, DATA, QUIT
- In questo modo è possibile inviare un'e-mail senza servirsi dello user agent

8

SMTP in pratica: uso con telnet (2/2)



```
HELO grid.unina.it
250 mail.unina.it Hello [143.225.229.172], pleased to meet you
MAIL FROM: spromano@unina.it
250 2.1.0 spromano@unina.it... Sender ok
RCPT TO: spromano@unina.it
250 2.1.5 spromano@unina.it... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Ciao giovane, come stai?
Fammi sapere asap...
.
250 2.0.0 i2FC5bZc018823 Message accepted for delivery
QUIT
221 2.0.0 mail.unina.it closing connection

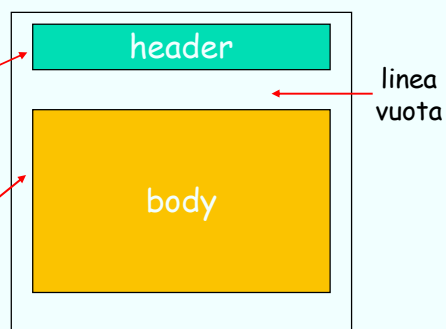
Connessione all'host perduta.
```

9

Formato del messaggio SMTP



- Linee di intestazione (header):
 - To:
 - From:
 - Subject:
 - ...*differenti da comandi smtp!*
- corpo (body):
 - il "messaggio" vero e proprio
 - solo caratteri ASCII



10

L'estensione MIME



- MIME: Multipurpose Internet Mail Extensions, RFC 2045-2056
- righe aggiuntive nell'intestazione informano della presenza di un body MIME

versione MIME
metodo utilizzato per codificare i dati
tipo, sottotipo e parametri del contenuto
dati codificati

```

From: alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data .....
.....base64 encoded data
    
```

11

Messaggi SMTP: un esempio (sniffer Ethereal)



```

14 0.002557 143.225.229.172 192.132.34.73 SMTP Message Body
Internet Protocol, Src Addr: 143.225.229.172 (143.225.229.172), Dst Addr: 192.132.34.73 (192.132.34.73)
Transmission Control Protocol, Src Port: 3419 (3419), Dst Port: smtp (25), Seq: 1829128306, Ack: 2648952608, Len: 1
Simple Mail Transfer Protocol
  Message: Message-ID: <4055A84A.9060100@unina.it>\r\n
  Message: Date: Mon, 15 Mar 2004 13:57:46 +0100\r\n
  Message: From: Simon Pietro Romano <spromano@unina.it>\r\n
  Message: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n
  Message: X-Accept-Language: en-us, en\r\n
  Message: MIME-Version: 1.0\r\n
  Message: To: spromano <spromano@unina.it>\r\n
  Message: Subject: prova SMTP da Netscape agent\r\n
  Message: Content-Type: text/plain; charset=ISO-8859-1; format=flowed\r\n
  Message: Content-Transfer-Encoding: 8bit\r\n
  Message: \r\n
  Message: Ciao.\r\n
  Message: \r\n
  Message: SP\r\n
  Message: \r\n
  Message: -- \r\n
  Message: \r\n
  Message:      /\r\n
  Message:      ( O-O )\r\n
  Message:      ~~~~~oOo~\r\n
  Message:      Simon Pietro Romano\r\n
  Message:      Università di Napoli Federico II\r\n
  Message:      Computer Science Department\r\n
  Message:      Phone: +39 081 7683823 -- Fax: +39 081 7684219\r\n
  Message:      e-mail: spromano@unina.it\r\n
  Message:      http://www.grid.unina.it/individual/sprom\r\n
  Message: \r\n
  Message: idioti. Ci rifletto un istante; e mi scoraggio>>. Magritte.\r\n
  Message: \r\n
  Message:      ~~~~~oOo~\r\n
  Message:      { } \r\n
  Message:      { } \r\n
  Message:      { } \r\n
  Message: \r\n
  Message: \r\n
  Message: \r\n
  Message: \r\n
  0190 74 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a Content-Type:
  01a0 20 74 65 78 74 2f 70 6c 61 69 6e 3b 20 63 88 61 text/plain; cha
  01b0 73 73 65 74 2d 49 53 4f 2d 38 38 35 39 2d 31 3b rset=ISO-8859-1;
  01c0 20 66 6f 72 6d 62 74 2d 66 6c 6f 77 65 64 6d 6a format=flowed
  
```

12

Esempi di tipi MIME



`Content-Type: type/subtype; parameters`

Text

- sottotipi: `plain`, `html`

Video

- sottotipi: `mpeg`, `quicktime`

Image

- sottotipi: `jpeg`, `gif`

Audio

- sottotipi: `basic` (8-bit mu-law encoded), `32kadpcm` (32 kbps coding)

Application

- altri dati che devono essere processati da specifiche applicazioni
- sottotipi: `msword`, `octet-stream`

13

Esempio di mail “multiparte”



```
From: alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=98766789
```

```
--98766789
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain
```

```
Dear Bob,
Please find a picture of a crepe.
```

```
--98766789
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
```

```
base64 encoded data .....
.....base64 encoded data
--98766789--
```

14

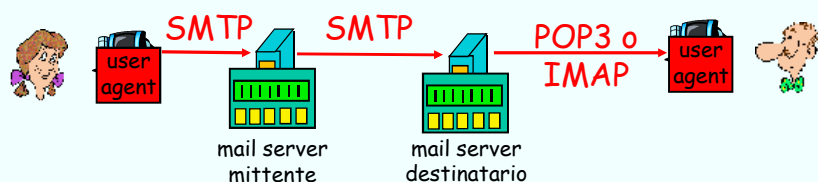
Prelievo della posta: Post Office Protocol (POP3)



- Fino ad ora abbiamo visto come sia possibile trasferire messaggi tra i vari mail server
- Non abbiamo però ancora parlato di come un utente possa, in un momento qualsiasi, accedere alla propria casella di posta elettronica per leggere i propri messaggi
- Per questa operazione è previsto un ulteriore protocollo
- Esso è chiamato POP3 (Post Office Protocol – versione 3) ed è definito in RFC 1939
- Si tratta sempre di un protocollo client server:
 - lo user agent ancora una volta gioca il ruolo di client POP
 - il mail server gioca il ruolo di server POP

15

La catena dei protocolli per la posta



- SMTP: consegna di messaggi
- Protocolli di accesso alla mail: recupero dei messaggi dai server
 - **POP: Post Office Protocol**
 - autorizzazione (agent \leftrightarrow server), transazione e aggiornamento
 - **IMAP: Internet Mail Access Protocol** [RFC 2060]
 - più complicato e potente
 - manipolazione avanzata dei messaggi sul server
 - Intestazioni e parti di messaggi
 - **HTTP**: gmail, Hotmail, Yahoo! Mail, ecc.

16

Esempio di dialogo POP3



autorizzazione

- comandi del client:
 - user**: specifica la username
 - pass**: specifica la password

- il server risponde

- +OK
- ERR

fase di scambio

- comandi del client:
 - list**: visualizza la lista dei messaggi
 - retr**: preleva il messaggio per numero
 - dele**: elimina il messaggio dal server
 - quit**: chiude la sessione

```
S: +OK POP3 server ready
C: user alice
S: +OK
C: pass hungry
S: +OK user successfully logged on

C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

17

POP3 in pratica (1/2): telnet cds.unina.it 110



```
Telnet cds.unina.it
+OK cds.unina.it Cyrus POP3 v2.1.10 server ready
user spromano
+OK Name is a valid mailbox
pass [REDACTED]
+OK Maildrop locked and ready
list_
```

...

Qui c'era la mia password! 😊

18

POP3 in pratica (2/2): telnet cds.unina.it 110



```
6292 1867
6293 2683
6294 913
.
retr 6294
+OK Message follows
Return-Path: <spromano@unina.it>
Received: from cds.unina.it ([unix socket])
    by cds.unina.it (Cyrus v2.1.10) with LMTP; Mon, 15 Mar 2004 13:13:33 +0100
X-Sieve: CMU Sieve 2.2
Received: from mail.unina.it (mail.unina.it [192.132.34.73])
    by cds.unina.it (8.12.11/8.12.9) with ESMTP id i2FCDX6G016069
    for <spromano@unina.it>; Mon, 15 Mar 2004 13:13:33 +0100 (CET)
Received: (from root@localhost)
    by mail.unina.it (8.12.11/8.12.11) id i2FCBCfe021235
    for spromano@unina.it; Mon, 15 Mar 2004 13:11:12 +0100
Received: from grid.unina.it ([143.225.229.172])
    by mail.unina.it (8.12.11/8.12.11) with SMTP id i2FC5bZc018823
    for spromano@unina.it; Mon, 15 Mar 2004 13:10:24 +0100
Date: Mon, 15 Mar 2004 13:10:24 +0100
From: spromano@unina.it
Message-Id: <200403151210.i2FC5bZc018823@mail.unina.it>
X-scanner: scanned by Inflex 1.0.12.7

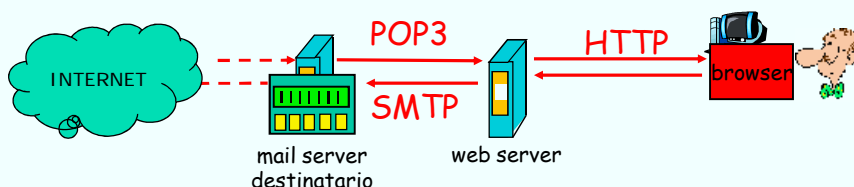
Ciao giovane, come stai?
Fammi sapere asap...
.
```

19

L'accesso alla posta via WEB



- Molti siti web forniscono accesso alle proprie caselle di posta (gmail, hotmail, Yahoo!, ecc.)
- In questo caso non serve avere uno user agent installato e correttamente configurato per ricevere ed inviare posta.
- È sufficiente disporre di un qualsiasi browser



20



DNS

21



Domain Name System (DNS)

- Tutti noi siamo oggi abituati a raggiungere un servizio (e quindi il calcolatore che lo offre) utilizzando nomi simbolici di facile memorizzazione:
 - www.google.com
 - www.rai.it
 - pippo@unina.it
- Questi nomi non sono immediatamente adatti ad essere compresi dai dispositivi che costituiscono la rete Internet.
- Un nome di questo tipo, infatti, non dà informazioni esatte sulla dislocazione sul territorio della macchina che si desidera contattare.
- I router, di conseguenza, non saprebbero come instradare i dati in maniera tale da raggiungere la destinazione.

22

Nomi simbolici vs Indirizzi IP



- La rete Internet è stata progettata invece per lavorare con indirizzi di diversa natura. Per es.:
 - 143.225.229.3
 - 217.9.64.225
- Questi indirizzi, detti indirizzi IP, sono formati da 4 numeri che vanno da 0 a 255 separati da un punto.
- Ogni dispositivo nella rete Internet ha un tale indirizzo; esso permette l'identificazione univoca a livello globale e la localizzazione.
- A differenza dei nomi simbolici, essendo gli indirizzi IP di lunghezza fissa, sono più facilmente gestibili dalle macchine
- Data la loro natura gerarchica forniscono inoltre precise informazioni sulla loro dislocazione sul territorio:
 - leggendo l'indirizzo da sinistra verso destra si ottengono informazioni sempre più dettagliate circa la rete di appartenenza (all'interno di tutte le reti di Internet)
 - c'è una similitudine con i numeri telefonici

23

Il servizio DNS



- Non volendo rinunciare alla comodità di lavorare con nomi simbolici, è stato necessario progettare un servizio di risoluzione dei nomi simbolici in indirizzi IP.
- Tale servizio associa ad un nome simbolico univoco (www.grid.unina.it) un indirizzo IP (143.225.229.3) permettendo così di raggiungere la macchina.
- Questo servizio si chiama **Domain Name System (DNS)** ed è definito in RFC1034 e RFC1035
- Esso si basa sullo scambio di messaggi UDP sul porto 53.
- Protocollo di livello applicativo, ma...

24

Altre funzionalità offerte



- Alias degli hostname:
 - ad una macchina con un nome complicato può essere associato un "soprannome" più piccolo e semplice da ricordare.
P.es.: rcsn1.roma.rai.it → www.rai.it
- Alias dei server di posta:
 - permette di associare un server di posta al nome di un dominio per facilitare la memorizzazione dell'indirizzo di posta.
P. es.: pippo@unina.it identifica l'utente [pippo](#) sulla macchina mailsrv1.cds.unina.it. L'associazione @unina.it → mailsrv1.cds.unina.it è a carico del servizio DNS.
- Distribuzione del carico:
 - quando un server gestisce un carico troppo elevato si suole replicare il suo contenuto su molte macchine differenti. Il servizio DNS distribuisce il carico tra le macchine rilasciando ciclicamente indirizzi appartenenti all'intero pool, senza che gli utenti si accorgano di nulla.

www.domain.com

–1.2.3.4

–1.2.3.15

–1.2.4.200

–1.2.15.121

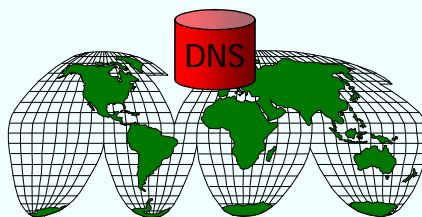
–1.5.34.12

25

DNS centralizzato?



- Si potrebbe pensare di risolvere il problema piazzando in un unico punto della terra una macchina che realizzi la risoluzione di tutti i nomi.



- Questa soluzione, sebbene teoricamente realizzabile, ha così tanti svantaggi da risultare impraticabile:
 - Single Point of Failure
 - Volume di traffico
 - Database distante
 - Manutenzione

26

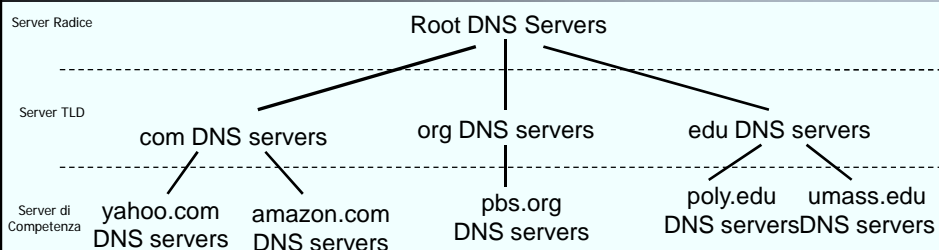
DNS distribuito!



- Quello che si fa è distribuire le informazioni sul territorio
- Ciascuno ha la responsabilità di raccogliere, gestire, aggiornare e divulgare le informazioni che lo riguardano.
- In particolare l'approccio è di tipo gerarchico:
 - gli elementi più alti nella gerarchia contengono molte informazioni non dettagliate
 - gli elementi più bassi nella gerarchia contengono poche informazioni dettagliate
- Attraverso un colloquio concertato tra le entità (di cui gli utenti non hanno percezione) si riesce a fornire il servizio di risoluzione.

27

DNS: un database gerarchico e distribuito



Un Client richiede l'IP di www.amazon.com (1st approx):

- Il client dapprima contatta uno dei root server per avere la lista degli indirizzi IP dei TLD per il dominio com
- Il client contatta uno dei TLD server che gli restituisce l'indirizzo IP del server autorizzato per amazon.com
- Infine il client contatta il server autorizzato per amazon.com che gli restituisce l'indirizzo IP di www.amazon.com

28

Server DNS Locali



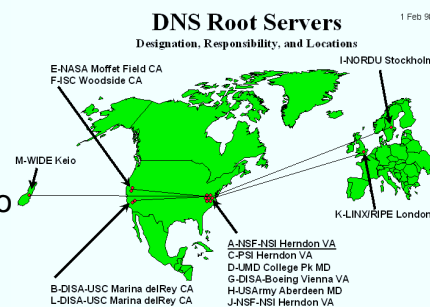
- Local Name Server (Locale)
 - Non appartengono strettamente alla gerarchia di server
 - Ciascun ente (università, società, ISP, etc...) ne installa uno (o più) nel proprio dominio.
 - Tutti gli host nel dominio richiedono a questo server il servizio di risoluzione.
 - Quando un host effettua una richiesta DNS, la query viene inviata al server DNS locale che opera da proxy e, tipicamente, invia la query attraverso la gerarchia di server.
 - Ciascun host deve essere configurato con l'indirizzo del DNS server locale per il dominio. Questa configurazione spesso avviene manualmente, ma in certi casi può avvenire anche in maniera automatica.

29

Tipologie di server DNS (Root)



- Root Name Server (Fondamentale)
 - Ne esistono 13 in Internet (etichettati da A ad M) e i loro indirizzi sono ben noti alla comunità.
 - Ad essi si riferiscono i Local Name Server che non possono soddisfare immediatamente una richiesta di risoluzione.
 - In questo caso il Local Name Server si comporta come client DNS ed invia una richiesta di risoluzione al Root Name Server.

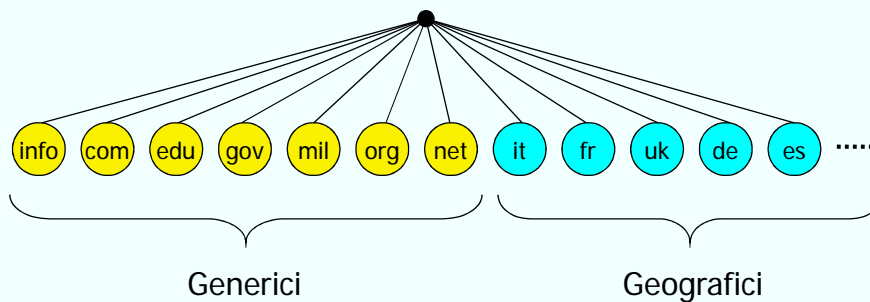


30

I “Top-Level Domain” (TLD)



- Questi server si occupano dei domini di alto livello (generici e geografici).



31

Tipologie di server DNS (Authoritative)



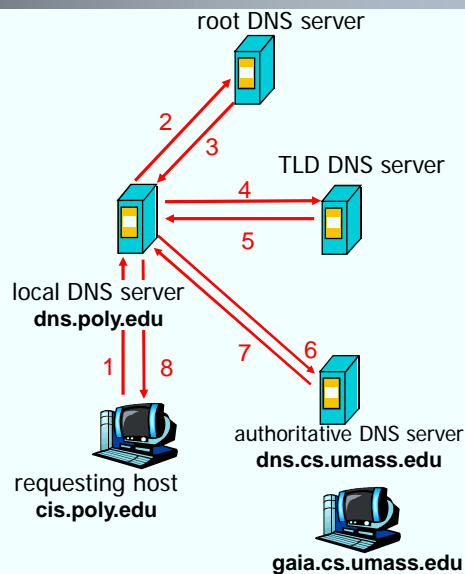
- Authoritative Name Server (Assoluto)
 - È un server dei nomi capace di risolvere tutti i nomi all'interno di un determinato dominio/organizzazione.
 - P.es.: un server dei nomi assoluto per il dominio unina.it deve essere capace di risolvere tutti i nomi del tipo xyz.unina.it
 - Può essere mantenuto dall'organizzazione o da un provider.

32

Un semplice esempio di risoluzione



- Esempio: un host di `cis.poly.edu` richiede l'indirizzo IP di `gaia.cs.umass.edu`
- **Query Iterative:**
 - Il server contattato risponde con il nome del server da contattare
 - La logica: non conosco questo nome, ma conosco il nome di qualcuno a cui poter chiedere.
 - Notiamo 8 msg DNS

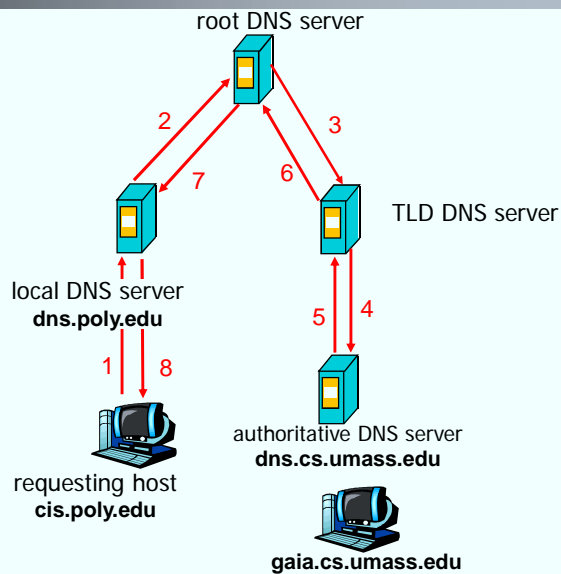


33 33

Un semplice esempio di risoluzione



- **Query Ricorsiva:**
 - Sposta il carico della risoluzione dei nomi sul server contattato, delegando al NS contattato la responsabilità di risolvere l'indirizzo.
 - Troppo carico (ad.es. RS) ?
- Il primo esempio prevede entrambe le richieste (la prima ricorsiva, le altre iterative).



34 34

Un esempio a più livelli



- Il TLD potrebbe non contattare necessariamente l'Authoritative Name Server finale, ma un Authoritative Name Server intermediario.
- Sarà il server intermedio a fornire il nome del server di competenza.
- In questi casi il numero di messaggi DNS aumenta.

35

Il caching dei nomi



- Per esigenze di efficienza un server DNS memorizza localmente un certo numero di corrispondenze.
- Per evitare che informazioni non aggiornate restino nella rete, dopo un certo tempo (circa un giorno), le associazioni vengono eliminate dalla cache.
- Ad es. un server locale può memorizzare
 - associazioni IP/nomi di non sua competenza e/o
 - gli indirizzi dei server TLD in modo da aggirare i server root.

36

Cosa memorizza un DNS



Resource records (RR)

Formato RR: (Nome, Valore, Tipo, TTL)

- **TTL**: tempo di vita residuo di un record scaduto il quale viene eliminato dalla cache.
- Il significato di **Nome** e **Valore** dipende da **Tipo**:
 - Tipo=A
 - nome=hostname
 - valore: indirizzo IP
 - Tipo=CNAME
 - **nome**=alias per il nome canonico (reale)
 - **valore**=nome canonico
 - Tipo=NS
 - nome=dominio (p.es.: unina.it)
 - valore=ind. IP dell'Authoritative NS
 - Tipo=MX
 - **nome**=dominio di posta (p.es. libero.it)
 - **valore**=nome dell'host mailserver associato a **nome**

37

Esempi di RR



- Type A
 - relay.bar.foo.com, 145.37.93.126, A
- Type NS
 - foo.com, dns.foo.com, NS
- Type CNAME
 - foo.com, relay.bar.foo.com, CNAME
- Type MX
 - foo.com, mail.bar.foo.com, MX

* Negli esempi non è mostrato il valore del campo TTL.

38

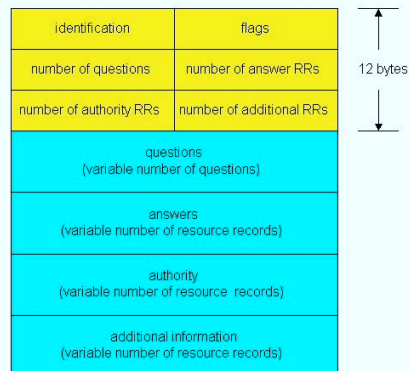
Il formato dei messaggi (1)



Protocollo DNS: *richieste e risposte*, entrambe con lo stesso formato di messaggio

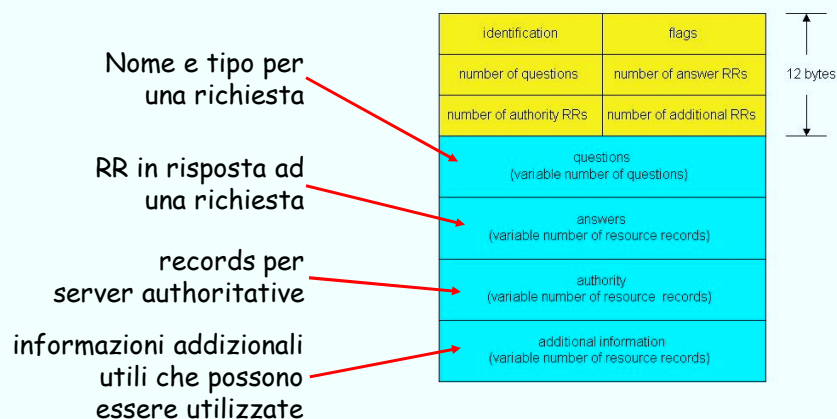
Header del mess.:

- **identification**: numero di 16bit diverso per ogni richiesta. Le risposte usano lo stesso identificativo
- **flags**:
 - risposta a richiesta
 - ricorsione desiderata
 - ricorsione disponibile
 - risposta authoritative



39

Il formato dei messaggi (2)

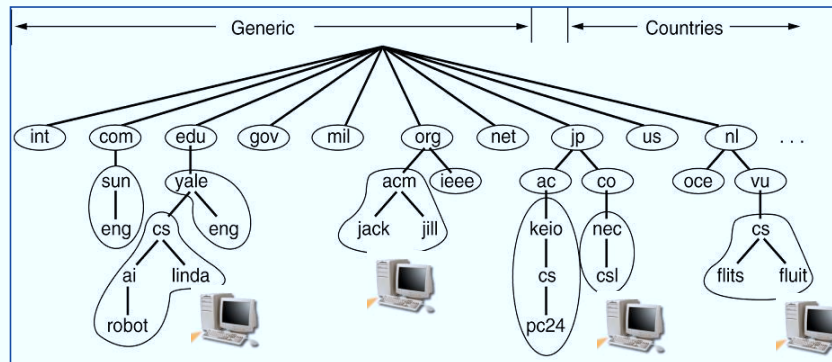


40

Name Server e Zone



- Una **zona** è un sottoalbero del DNS amministrato separatamente.
- Lo spazio dei nomi DNS è suddiviso in zone non sovrapposte.
- Ogni zona contiene un DNS server primario e uno o più DNS server secondari.



Il servizio BIND



- BIND (Berkeley Internet Name Domain) è una implementazione dei protocolli Domain Name System (DNS)
- È liberamente re-distribuibile
- È costituito dai seguenti componenti:
 - Un server DNS (named);
 - Una libreria per la risoluzione dei nomi di dominio;
 - Strumenti di diagnostica.
- Questa implementazione è di gran lunga la più utilizzata su Internet su sistemi Unix-like

Configurazione di BIND: un esempio di file di zona



```
$TTL 3600
@      IN SOA grid.grid.unina.it. root.grid.grid.unina.it. (
                                2004020901    ; Serial
                                10800          ; Refresh
                                3600           ; Retry
                                604800        ; Expire
                                86400 )       ; Minimum TTL

; Machine Name
localhost      A      127.0.0.1

vesuvio        A      143.225.229.1
grid           A      143.225.229.3
honolulu       A      143.225.229.111
comicsserver   A      143.225.229.112
...

; Aliases
www            CNAME   grid
ftp            CNAME   grid
news           CNAME   grid
tesisti        CNAME   vesuvio
www.tesisti    CNAME   vesuvio

; MX Record
              MX      10      grid.grid.unina.it.
```

* SOA: Start of Authority

43

Significato di alcuni parametri



- **Serial**: numero seriale progressivo utilizzato per rilevare aggiornamenti del file. Di solito usa il formato: aaaammggxx
- **Refresh**: intervallo in secondi tra due successivi prelievi del file di zona da parte di un DNS server
- **Retry**: intervallo in secondi tra tentativi successivi di recuperare una zona in caso di fallimento
- **Expire**: tempo in secondi che deve trascorrere per ritenere scadute le informazioni di una zona che non si riesce ad aggiornare
- **Minimum TTL**: tempo di durata di default delle singole entry del file di zona

44

Un esempio: configurazione del Reverse DNS



```
$TTL 3600

@      IN SOA  grid.grid.unina.it. root.grid.grid.unina.it. (
                                2004020901      ; Serial
                                10800            ; Refresh
                                3600             ; Retry
                                604800           ; Expire
                                86400 )          ; Minimum TTL

; DNS Servers
      NS      grid.grid.unina.it.

; Machine Name
1     PTR     vesuvio.grid.unina.it.
3     PTR     grid.grid.unina.it.
111   PTR     honolulu.grid.unina.it.
112   PTR     comicserver.grid.unina.it.
```

45

Il file named.root



```
.           3600000  IN  NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000      A      198.41.0.4
;
; formerly NS1.ISI.EDU
;
.           3600000      NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.  3600000      A      128.9.0.107
;
; formerly C.PSI.NET
...
.           3600000      NS      L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.  3600000      A      198.32.64.12
;
; housed in Japan, operated by WIDE
;
.           3600000      NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000      A      202.12.27.33
; End of File
```

46

Un esempio di uso di nslookup



```
> nslookup
> www.cisco.com
Server:      143.225.229.3
Address:     143.225.229.3#53

Non-authoritative answer:
Name:   www.cisco.com
Address: 198.133.219.25
> set ty=ns
> cisco.com
Server:      143.225.229.3
Address:     143.225.229.3#53

Non-authoritative answer:
cisco.com    nameserver = ns1.cisco.com.
cisco.com    nameserver = ns2.cisco.com.

Authoritative answers can be found from:
ns1.cisco.com internet address = 128.107.241.185
ns2.cisco.com internet address = 64.102.255.44
> server ns1.cisco.com
Default server: ns1.cisco.com
Address: 128.107.241.185#53
> set ty=a
> www.cisco.com
Server:      ns1.cisco.com
Address:     128.107.241.185#53

Name:   www.cisco.com
Address: 198.133.219.25
```

Chiedo di risolvere l'host www.cisco.com

Indirizzo del local DNS che serve la richiesta

Ecco la risposta, che non proviene da un server DNS authoritative

Imposto nslookup per l'invio di query di tipo NS: restituirà i name server authoritative di un dominio specificato

Chiedo il Name Server authoritative per il dominio cisco.com

Eccoli: sono due

E questi sono i loro indirizzi IP

Imposto nslookup per l'invio delle successive query al NS ns1.cisco.com

Reimposto nslookup per l'invio di query di tipo A (risoluzione di nomi di host) e richiedo la risoluzione del nome di host www.cisco.com

Questa volta la risposta è authoritative. La entry non-authoritative memorizzata in cache era valida.

47

Un esempio di uso di dig (1/2)



```
> dig www.cisco.com

; <>> DiG 9.3.1 <>> www.cisco.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 39786
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.cisco.com.                IN      A

;; ANSWER SECTION:
www.cisco.com.                85619   IN      A      198.133.219.25

;; AUTHORITY SECTION:
cisco.com.                    81328   IN      NS      ns2.cisco.com.
cisco.com.                    81328   IN      NS      ns1.cisco.com.

;; ADDITIONAL SECTION:
ns2.cisco.com.                86175   IN      A      64.102.255.44
ns1.cisco.com.                81857   IN      A      128.107.241.185

;; Query time: 1 msec
;; SERVER: 143.225.229.3#53(143.225.229.3)
;; WHEN: Tue Oct 10 19:54:08 2006
;; MSG SIZE  rcvd: 115
```

48

Un esempio di uso di dig (2/2)



```
> dig www.cisco.com @ns1.cisco.com

; <> DiG 9.3.1 <> www.cisco.com @ns1.cisco.com
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 7291
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.cisco.com.                IN      A

;; ANSWER SECTION:
www.cisco.com.                86400   IN      A      198.133.219.25

;; AUTHORITY SECTION:
cisco.com.                    86400   IN      NS      ns1.cisco.com.
cisco.com.                    86400   IN      NS      ns2.cisco.com.

;; ADDITIONAL SECTION:
ns1.cisco.com.                86400   IN      A      128.107.241.185
ns2.cisco.com.                86400   IN      A      64.102.255.44

;; Query time: 224 msec
;; SERVER: 128.107.241.185#53(128.107.241.185)
;; WHEN: Tue Oct 10 19:55:10 2006
;; MSG SIZE  rcvd: 115
```

49

MX server con nslookup



```
> nslookup
> set ty=mx
> unina.it
Server:      143.225.229.3
Address:     143.225.229.3#53

Non-authoritative answer:
unina.it     mail exchanger = 10 pmx1.unina.it.
unina.it     mail exchanger = 10 pmx2.unina.it.

Authoritative answers can be found from:
unina.it     nameserver = dscna1.unina.it.
unina.it     nameserver = dscna2.unina.it.
pmx1.unina.it internet address = 192.132.34.28
pmx2.unina.it internet address = 192.132.34.29
dscna1.unina.it internet address = 192.133.28.1
dscna2.unina.it internet address = 192.133.28.7
```

Imposto nslookup per l'invio di query di tipo MX (Mail eXchanger): server SMTP di dominio

Chiedo i mail server del dominio "@unina.it"

50

MX server con dig



```
> dig unina.it MX

; <<> DiG 9.3.1 <<> unina.it MX
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 433
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;unina.it.                IN      MX

;; ANSWER SECTION:
unina.it.                26684   IN      MX      10 pmx1.unina.it.
unina.it.                26684   IN      MX      10 pmx2.unina.it.

;; AUTHORITY SECTION:
unina.it.                55400   IN      NS      dscna1.unina.it.
unina.it.                55400   IN      NS      dscna2.unina.it.

;; ADDITIONAL SECTION:
pmx1.unina.it.           26684   IN      A       192.132.34.28
pmx2.unina.it.           8220    IN      A       192.132.34.29
dscna1.unina.it.         55400   IN      A       192.133.28.1
dscna2.unina.it.         55400   IN      A       192.133.28.7

;; Query time: 1 msec
;; SERVER: 143.225.229.3#53(143.225.229.3)
;; WHEN: Tue Oct 10 20:00:10 2006
;; MSG SIZE  rcvd: 174
```

51

Altre applicazioni



- Telnet; RFC 854, 855
- SSH (Secure Shell)
- SNMP, Simple Network Management Protocol; RFC 1157 e ...
- IRC (Internet Relay Chat); RFC 1459, 2810, 2811, 2812, 2813

52