Corso di Laurea in Ingegneria Informatica

Corso di Reti di Calcolatori
(a.a. 2011/12)

Roberto Canonico (roberto.canonico@unina.it)
Giorgio Ventre (giorgio.ventre@unina.it)

Protocolli applicativi: DNS

11 ottobre 2011

I lucidi presentati al corso sono uno strumento didattico
che NON sostituisce i testi indicati nel programma del corso

Nota di copyright per le slide COMICS

Nota di Copyright

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.

3

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

4

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
- Si basa sullo scambio di messaggi UDP sul porto 53

5

Altre funzionalità offerte

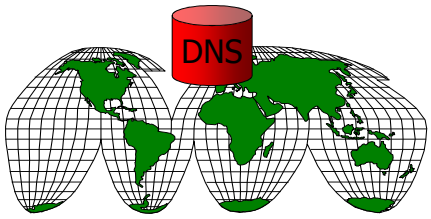
- Alias degli hostname:
  - ad una macchina con un nome complicato può essere associato un "soprannome" più piccolo e semplice da ricordare.
    P.es.: rcsn1.roma.rai.it → www.rai.it
- Alias dei server di posta:
  - permette di associare un server di posta al nome di un dominio per facilitare la memorizzazione 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

6

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

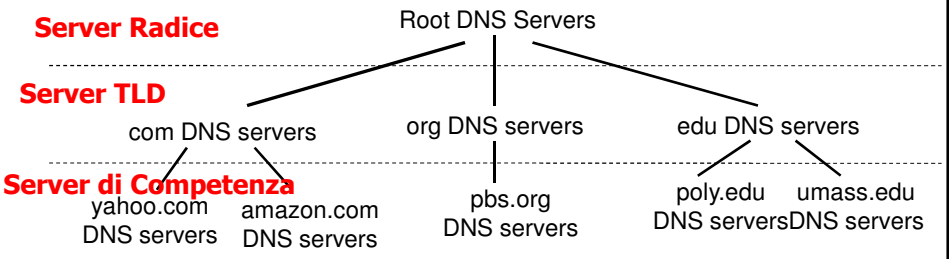
7

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

8

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

9

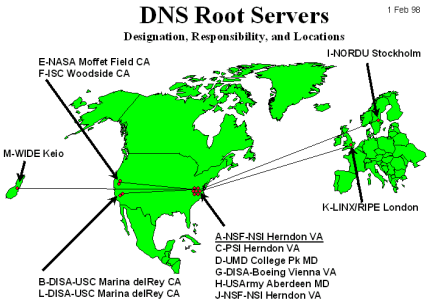
Tipologie di server DNS (Local)

- Local Name Server (Locale)
  - Non appartengono strettamente alla gerarchia di server
  - Ciascun ente (università, società, etc…) ne installa uno 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.
  - L'uso di un server DNS locale consente ai singoli host di fare una sola query DNS verso di essi: sarà poi il local DNS server a fare la sequenza di interrogazioni descritta nella slide precedente

10

Tipologie di server DNS (Root)

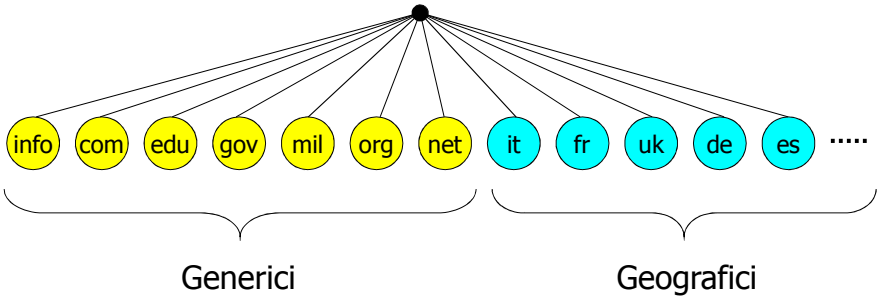
- Root Name Server (Fondamentale)
  - Ne esistono 13 in Internet (etichettati da A ad M) e i loro indirizzi sono ben noti alla comunità.
  - Ad essi si riferiscono i Local Name Server che non possono soddisfare immediatamente una richiesta di risoluzione.
  - In questo caso il Local Name Server si comporta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



11

I "top-level domain" server (TLD)

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



12

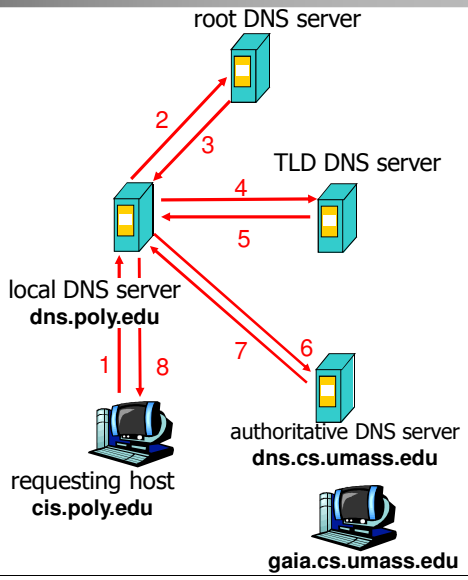
Tipologie di server DNS (Authoritative)

- 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
  - Ad essi si riferiscono i Name Server TLD quando, interpellati dai Local Name Server, devono risolvere un indirizzo.
  - Può essere mantenuto dall'organizzazione o da un provider.

13

Un semplice esempio di risoluzione

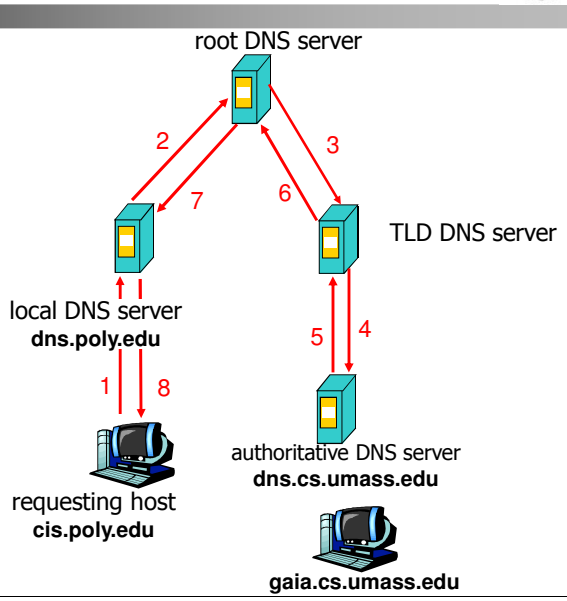
- Un host di cis.poly.edu richiede l'indirizzo IP di ***gaia.cs.umass.edu***
- Query Iterative:
  - Il server contatattato risponde con il nome del server da contattare
  - La logica: non conosco questo nome, ma conosco il nome di qualcuno a cui poter chiedere.



14

Un semplice esempio di risoluzione

- Query Ricorsive:
  - Sposta il carico della risoluzione dei nomi sul server contattato, delegando al NS contattato la responsabilità di risolvere l'indirizzo.
  - Troppo carico



15

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.

16

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.

17

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=NS
    - nome=dominio (p.es.: unina.it)
    - valore=ind. IP dell'Authoritative NS
  - Type=CNAME
    - **nome**=alias per il nome canonico (reale)
    - **valore**=nome canonico
  - Type=MX
    - **nome=dominio di posta (p.es. libero.it)**
    - **valore**=nome dell'host mailserver associato a **nome**

18

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

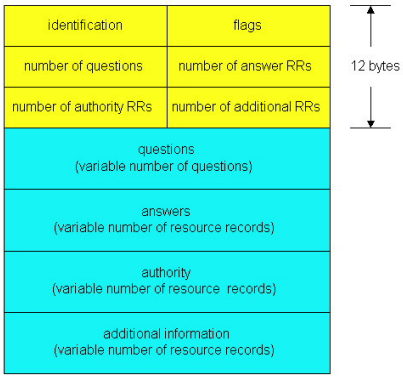
19

Il formato dei messaggi (1)

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

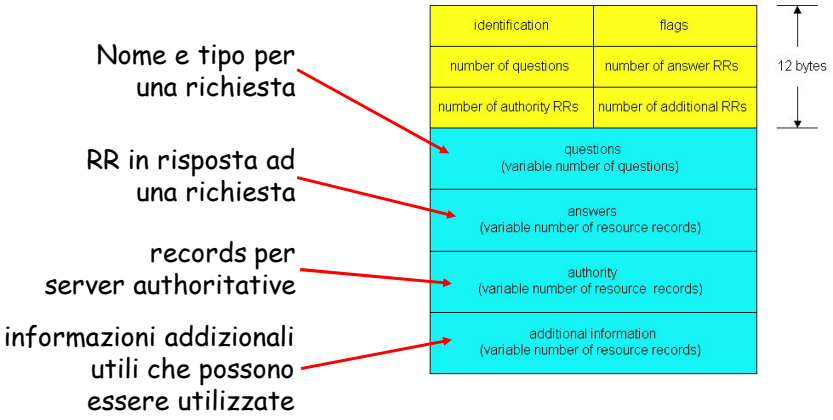
Header del mess.:

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



20

Il formato dei messaggi (2)



21

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

22

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
comicserver     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

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 zone 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

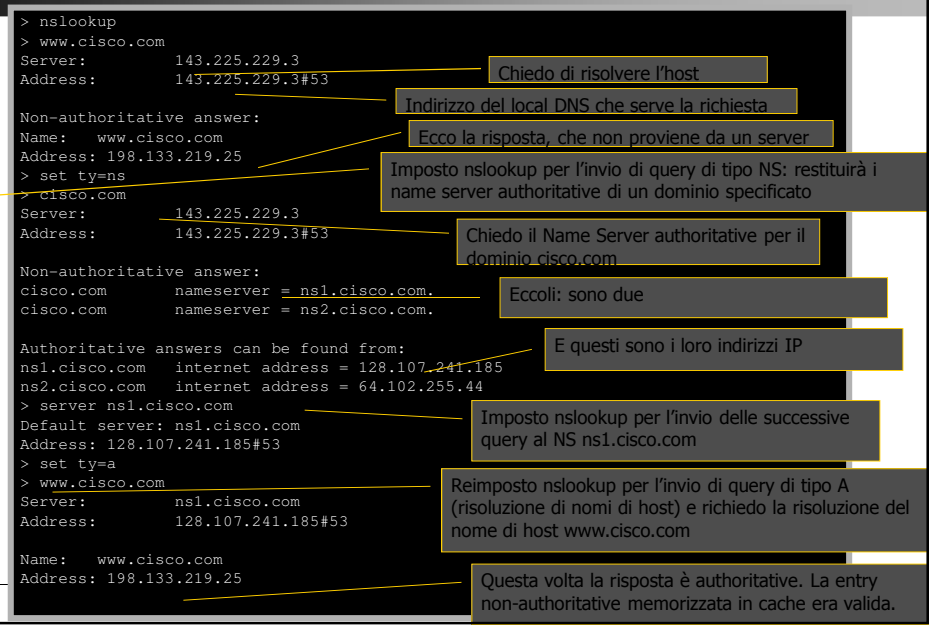
Un esempio: configurazione del Reverse DNS

```
$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.
```

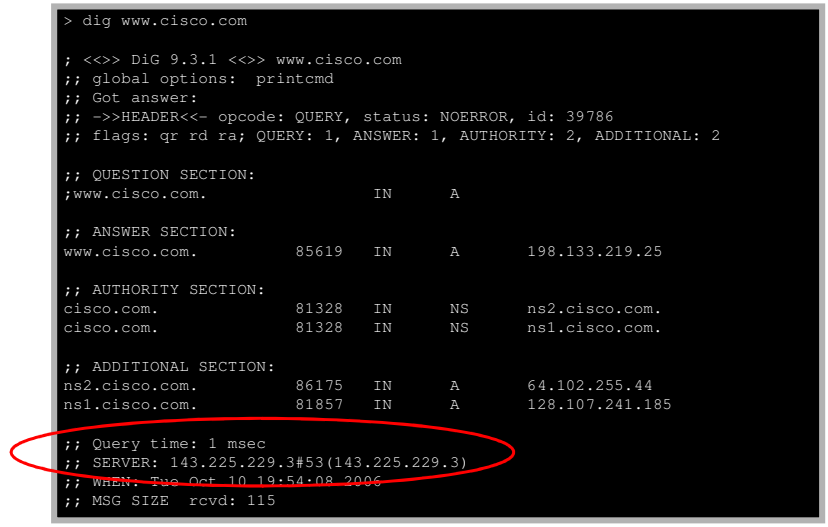

Il file named.root

```
.                       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
```

Un esempio di uso di nslookup



Un esempio di uso di dig (1/2)



28

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
```

29

MX server con nslookup

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

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

```
> 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
```

30