

Domain Name System

Indice

- [Perche' il DNS](#)
- [Principi di base del DNS](#)
- [Il Reverse Lookup](#)
- [Il meccanismo di Delega](#)
- [Come funziona il Domain Name System](#)
- [Caching NS](#)
- [La configurazione del DNS](#)
- [Come configurare la delega](#)
- [Classless delegation](#)
- [Sicurezza](#)
- [Il DNS e IPv6](#)
- [Tool e utility per il DNS](#)
- [Aggiornamento dei Dati sul DNS presso le Authority](#)

Perche' il DNS

DNS: obiettivo/esigenza

- Dare dei nomi ai calcolatori

Storia

- In ARPANET la corrispondenza nomi-indirizzi era conservata centralmente e distribuita in lettura a tutti gli hosts della rete
 - Sistema fortemente inefficiente, ritardi nella propagazione delle modifiche dipendenti da topologia e qualità dei collegamenti della rete
 - La struttura dei nomi non era gerarchica (quindi bisognava verificare che ciascun host avesse un nome univoco prima di assegnarlo)

Perche' e' nato il DNS

- All'inizio degli anni '80, l'aumento del numero degli host ha reso indispensabile l'adozione di un modello di gestione distribuita denominato Domain Name System
- Con l'aumento del commercio elettronico si e' reso necessario adottare un sistema che permettesse un piu' immediato ed intuitivo metodo per trovare gli host su Internet (piu' human readable)
- Così nasce il DNS

Cenni storici

- BIND:
 - Prima versione BIND4 (operativo fino alla fine degli anni '80)
 - Ormai non piu' supportato
 - BIND8 rilasciato nel 1997
 - BIND9 nel 2000
 - Introduce supporto per DNSSEC (crittografia a chiave pubblica) e IPv6, incremental zone transfer, notifiche asincrone master-slave, dynamic zone updates.

Cenni storici

- Versioni di BIND in alcuni sistemi:
 - Solaris 7/8 : BIND 8.1.2
 - HP-UX 11.00 : BIND 4.9.7
 - Red Hat Linux 6.1/8.2 : BIND 8.2.2
 - FreeBSD 3.4/4.0 : BIND 8.2.2
- Windows:
 - NORTEL ha effettuato il porting di BIND su NT (versione 8.2)

Riferimenti RFC

- Formalizzazione del protocollo negli RFC:
 - Paul Mockapetris (1983)
 - RFC 882
 - RFC 883
 - Aggiornamenti (1987)
 - RFC 1034
 - RFC 1035

RFC avanzati di definizione del servizio DNS

- RFC 2052:
 - definizione record SRV
- RFC 3596:
 - record AAAA per IPv6
- RFC 1996:
 - Notifica asincrona modifiche sulle zone
- RFC 2136:
 - Supporto per DHCP updates
- RFC 1995:
 - Trasferimento incrementale delle zone
- RFC 2535-41:
 - DNSSEC, supporto autenticazione e sicurezza delle zone (crittografia asimmetrica)
- RFC 2845:
 - TSIG/TKEY firme e chiavi nelle transazioni (pre-shared keys)

Che cos'è il DNS

- Domain Name Service
 - Consente di individuare un computer non attraverso il suo indirizzo IP ma mediante un nome (es. www.garr.it).
 - Nel caso di IPv4 un indirizzo è un intero a 32 bit, 4 ottetti, separati da “.”
 - es.: 192.168.0.1
 - Nel caso di IPv6 un indirizzo è formato da 8 campi di 16 bits ciascuno (128 in tutto), ogni campo è separato da “:” ed espresso in notazione esadecimale
 - es.: 3ffe:0b00:0c18:0001:0290:27ff:fe17:fc1d

Che cos'è il DNS

- Il DNS permette di associare un nome *Human-readable* ad un host, più semplice da ricordare di un indirizzo IP.
- L'univocità nella determinazione dell'host attraverso tale sistema è garantita mediante l'adozione di una struttura gerarchica "a domini" per la quale ciascun host appartiene ad un dato dominio "registrato" ufficialmente in un database distribuito.
- Es: www.garr.it individua una macchina il cui nome è www appartenente al dominio garr che è a sua volta parte del dominio globale it

Principi di base del DNS

DNS: come e' strutturato

- Suddivisione gerarchica in domini
- Struttura ad albero
- Localita' dell'informazione
 - ogni nodo detiene un database con le informazioni del proprio dominio e interroga gli altri nodi quando deve trovare le informazioni non locali
- Basato sul modello client/server
 - Le informazioni possono essere ottenute tramite interrogazioni ad una delle foglie dell'albero

Risoluzione diretta e inversa

- Nel protocollo standard DNS vengono individuate e distinte 2 tipologie di risoluzioni:
 - Risoluzione diretta:
 - Corrispondenza nome host – indirizzo IP
 - Es: `www.example.com` IN A 192.168.0.1
 - Risoluzione inversa:
 - Corrispondenza indirizzo IP – nome host
 - Es: `1.0.168.192.in-addr.arpa.` IN PTR
`www.example.com.`

Protocolli di trasporto del DNS

- Queries :
 - UDP porta 53
- Risposte :
 - Dim. < 512 bytes : UDP porta 53
 - Dim. > 512 bytes : TCP porta 53
- Trasferimenti di zona :
 - TCP porta 53

DNS: principali componenti

- tre componenti principali:
 - spazio dei nomi (namespace) e informazioni associate (Resource Record - RR)
 - nameserver
(nodi che mantengono una parte del database globale)
 - resolver
(client per l'interrogazione del nameserver)
- Aumento delle prestazioni di risposta sul DNS attraverso l'adozione di meccanismi di caching delle informazioni.
 - database in memoria RAM

Name Servers

- Un Name Server e' un host appartenente ad un dominio che contiene tutti i record (corrispondenze nomi-indirizzi e/o viceversa) di tale dominio
- Ovvero il name server di un dato dominio contiene il database locale relativo a quel dato dominio, che e' un sottoinsieme del database globale

Classificazione tipologie dei NS

- Categorizzazioni sulla base di :
 - Sorgente di dati del NS (autoritative, caching, master, slave)
 - Tipo di dati salvati (stub)
 - Percorso della query (forwarders)
 - Tipo di risposta fornita (ricorsivo, non ricorsivo)
 - Visibilita' del server (distribution)

Meccanismo di risoluzione nel namespace root

- Un nome a dominio viene analizzato da destra verso sinistra, chiedendo a ciascun nameserver di fornire informazioni soltanto sull'elemento che si trova a sinistra dell'ultimo punto.
- Tutti i nomi a dominio esistenti su Internet in realtà terminano con un “.” (punto):
garr.it.
- La stringa vuota che segue il punto finale è chiamata *dominio radice* (DNS root zone);

I root nameserver

- I root nameserver sono i server responsabili (autoritativi) delle informazioni relative al dominio ".";
- Possiedono l'elenco dei server responsabili per ognuno dei domini di primo livello riconosciuti, e lo forniscono in risposta a ciascuna richiesta.
- Contengono le informazioni per la risoluzione inversa (risoluzione indirizzo-nome)
- La lista aggiornata dei root-server è mantenuta da InterNIC

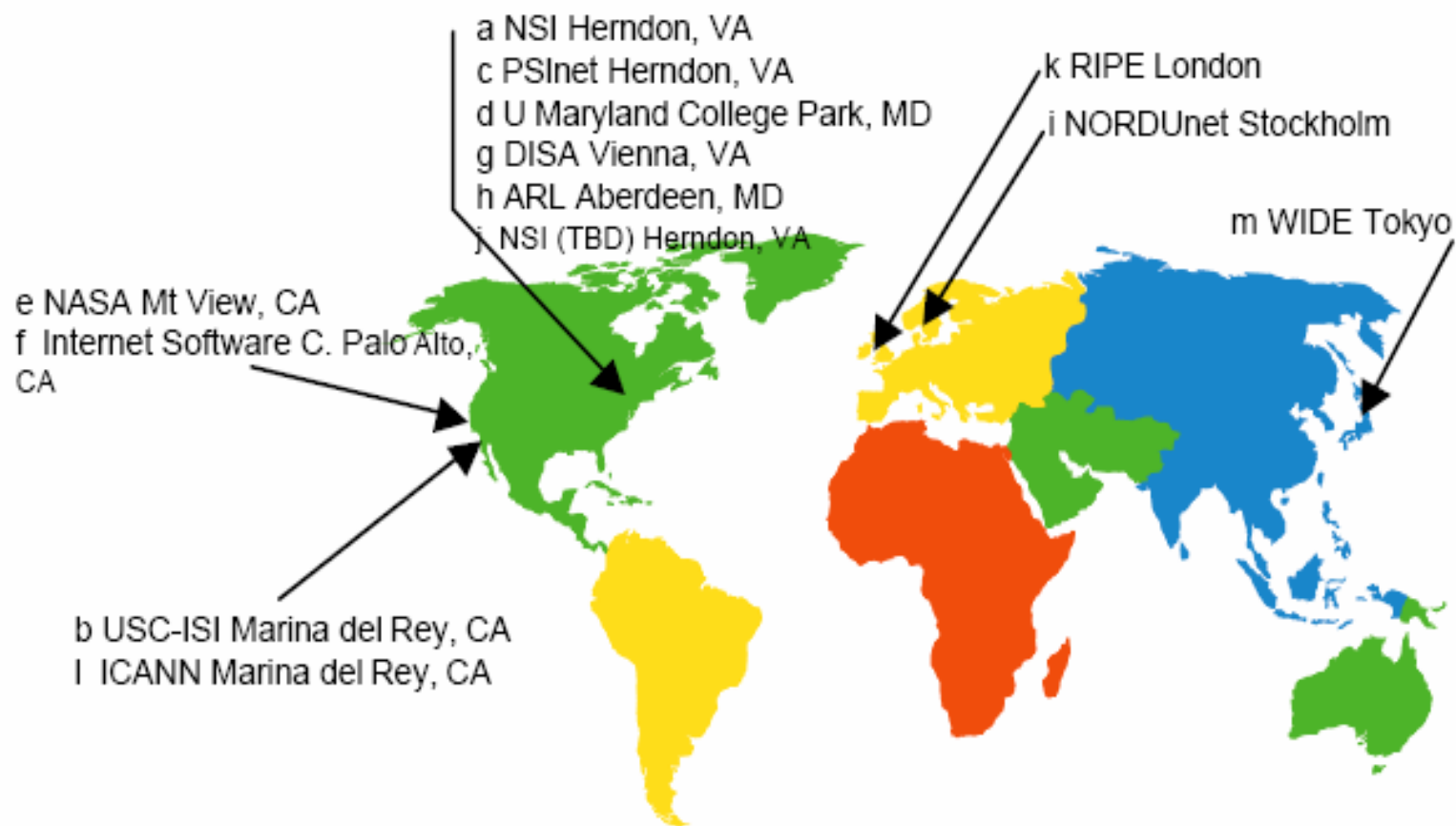
<ftp://ftp.rs.internic.net/domain/named.root>

<ftp://ftp.nic.it/pub/DNS/named.root>

I root nameserver

Server	Operator	Locations	IP Address
A	VeriSign Global Registry Services	Dulles, VA	198.41.0.4
B	Information Sciences Institute	Marina del Rey, CA	IPv4: 192.228.79.201, IPv6: 2001:478:65::53
C	Cogent Communications	Chicago; Herndon, VA; Los Angeles; New York City	IPv4: 192.33.4.12
D	University of Maryland	College Park, MD	IPv4: 128.8.10.90
E	NASA Ames Research Center	Mountain View, CA	IPv4: 192.203.230.10
F	Internet Systems Consortium, Inc. (ISC)	Auckland, Beijing, Brisbane, Dubai, Hong Kong, Jakarta, Johannesburg, Lisbon, Los Angeles, Madrid, Monterrey, Moscow, Munich, New York City, Osaka, Ottawa, Palo Alto, Paris, Prague, Rome, San Francisco, San Jose, Sao Paulo, Seoul, Singapore, Taipei, Tel Aviv, Toronto	IPv4: 192.5.5.241, IPv6: 2001:500::1035
G	US DOD Network Information Center	Vienna, VA	IPv4: 192.112.36.4
H	US Army Research Lab	Aberdeen, MD	IPv4: 128.63.2.53, IPv6: 2001:500:1::803f:235
I	Autonomica/NORDUnet	Amsterdam, Ankara, Bangkok, Brussels, Bucharest, Chicago, Geneva, Frankfurt, Helsinki, Hong Kong, Kuala Lumpur, London, Milan, Oslo, Stockholm, Tokyo, Washington DC	IPv4: 192.36.148.17
J	VeriSign Global Registry Services	Amsterdam; Atlanta; Dulles, VA (2 locations); London; Los Angeles; Miami; Mountain View, CA; Seattle; Seoul; Singapore; Sterling, VA; Stockholm; Tokyo	IPv4: 192.58.128.30
K	Réseaux IP Européens Network Coordination Centre (RIPE)	Amsterdam, Athens, Doha, Frankfurt, London, Milan	IPv4: 193.0.14.129, IPv6: 2001:7fd::1
L	Internet Corporation for Assigned Names and Numbers (ICANN)	Los Angeles	IPv4: 198.32.64.12
M	WIDE Project	Paris, Seoul, Tokyo	IPv4: 12.27.33, IPv6: 2001:dc3::35

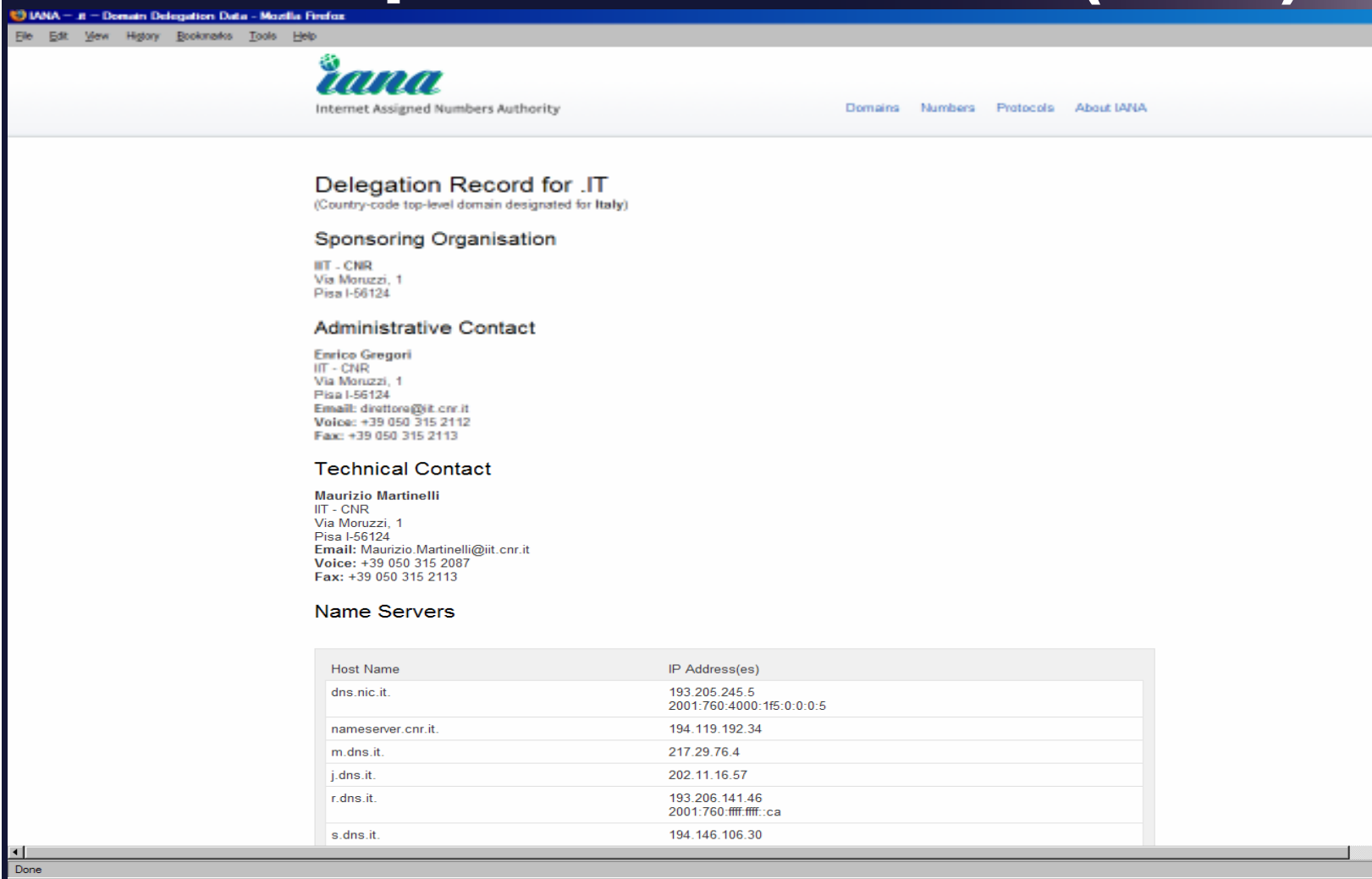
I root nameserver



I Top Level Domain (TLD)

- Esistono due tipi di TLD:
 - I domini generali (gTLD):
.com, .net, .org...
 - I domini nazionali (ccTLD):
.it, .uk, .de, .us
- IANA (Internet Assigned Numbers Authority) e' responsabile della zona di root e delega la gestione dei TLD ad a varie entita' amministrative.
- IANA è supervisionato da ICANN (Internet Corporation for Assigned Names and Numbers)

I Top Level Domain (TLD)

A screenshot of a Mozilla Firefox browser window displaying the IANA website. The browser's address bar shows "IANA - # - Domain Delegation Data - Mozilla Firefox". The website header includes the IANA logo and navigation links for Domains, Numbers, Protocols, and About IANA. The main content area is titled "Delegation Record for .IT" with a subtitle "(Country-code top-level domain designated for Italy)". It lists the Sponsoring Organisation (IIT - CNR), Administrative Contact (Enrico Gregori), and Technical Contact (Maurizio Martinelli). At the bottom, there is a table of Name Servers.

IANA - # - Domain Delegation Data - Mozilla Firefox

File Edit View History Bookmarks Tools Help

iana
Internet Assigned Numbers Authority

[Domains](#) [Numbers](#) [Protocols](#) [About IANA](#)

Delegation Record for .IT

(Country-code top-level domain designated for Italy)

Sponsoring Organisation

IIT - CNR
Via Moruzzi, 1
Pisa I-56124

Administrative Contact

Enrico Gregori
IIT - CNR
Via Moruzzi, 1
Pisa I-56124
Email: direttore@iit.cnr.it
Voice: +39 050 315 2112
Fax: +39 050 315 2113

Technical Contact

Maurizio Martinelli
IIT - CNR
Via Moruzzi, 1
Pisa I-56124
Email: Maurizio.Martinelli@iit.cnr.it
Voice: +39 050 315 2087
Fax: +39 050 315 2113

Name Servers

Host Name	IP Address(es)
dns.nic.it.	193.205.245.5 2001:760:4000:1f5:0:0:0:5
nameserver.cnr.it.	194.119.192.34
m.dns.it.	217.29.76.4
j.dns.it.	202.11.16.57
r.dns.it.	193.206.141.46 2001:760:ffff:ffff::ca
s.dns.it.	194.146.106.30

Done

I Top Level Domain (TLD)

IANA - .eu - Domain Delegation Data - Mozilla Firefox

File Edit View History Bookmarks Tools Help



Internet Assigned Numbers Authority

[Domains](#) [Numbers](#) [Protocols](#) [About IANA](#)

Delegation Record for .EU

(Country-code top-level domain designated for European Union)

Sponsoring Organisation

EURid vzw/asbl
Parkstation
Woluweaan 150
Diegem 1831

Administrative Contact

Marc Van Wesemael
EURid vzw/asbl
Parkstation
Woluweaan 150
Diegem 1831
Email: domain-admin@eurid.eu
Voice: +32-2-401.27.50
Fax: +32-2-401.27.51

Technical Contact

Peter Janssen
EURid vzw/asbl
Parkstation
Woluweaan 150
Diegem 1831
Email: domain-tech@eurid.eu
Voice: +32-2-401.27.50
Fax: +32-2-401.27.51

Name Servers

Host Name	IP Address(es)
a.nic.eu.	91.200.16.100
b.eu.dns.be.	193.190.135.100
l.nic.eu.	195.66.241.178
m.nic.eu.	217.29.76.13
l.eu.dns.be.	193.2.221.60
p.nic.eu.	195.47.235.130

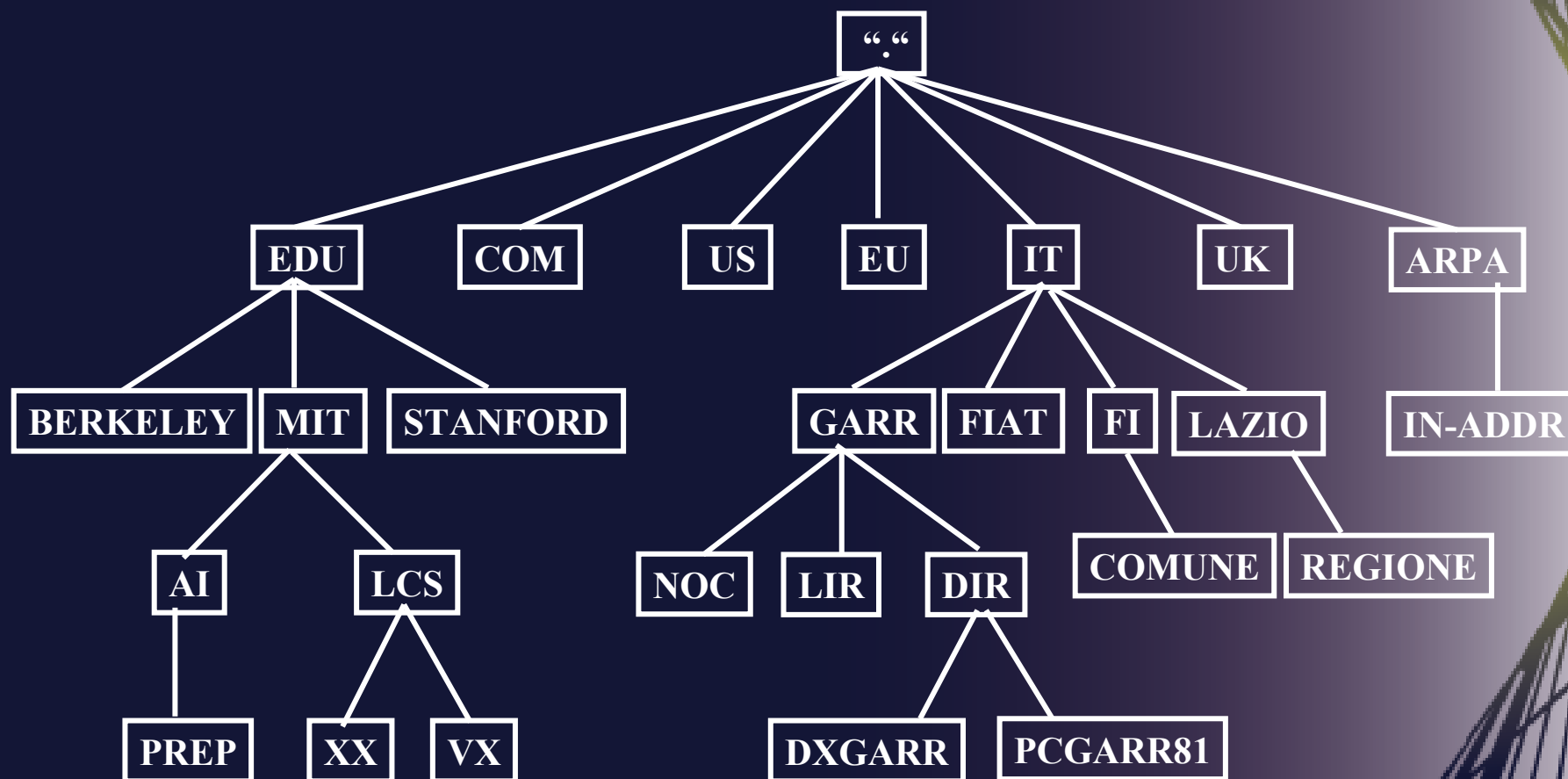
Regole sintattiche

- I nomi di dominio non sono case sensitive
 - Colorado, colorado, COLORADO sono la stessa cosa
 - BIND porta tutto in minuscolo (in contrasto con DNSSEC e firme con TSIG)
- Fino a 256 caratteri di lunghezza

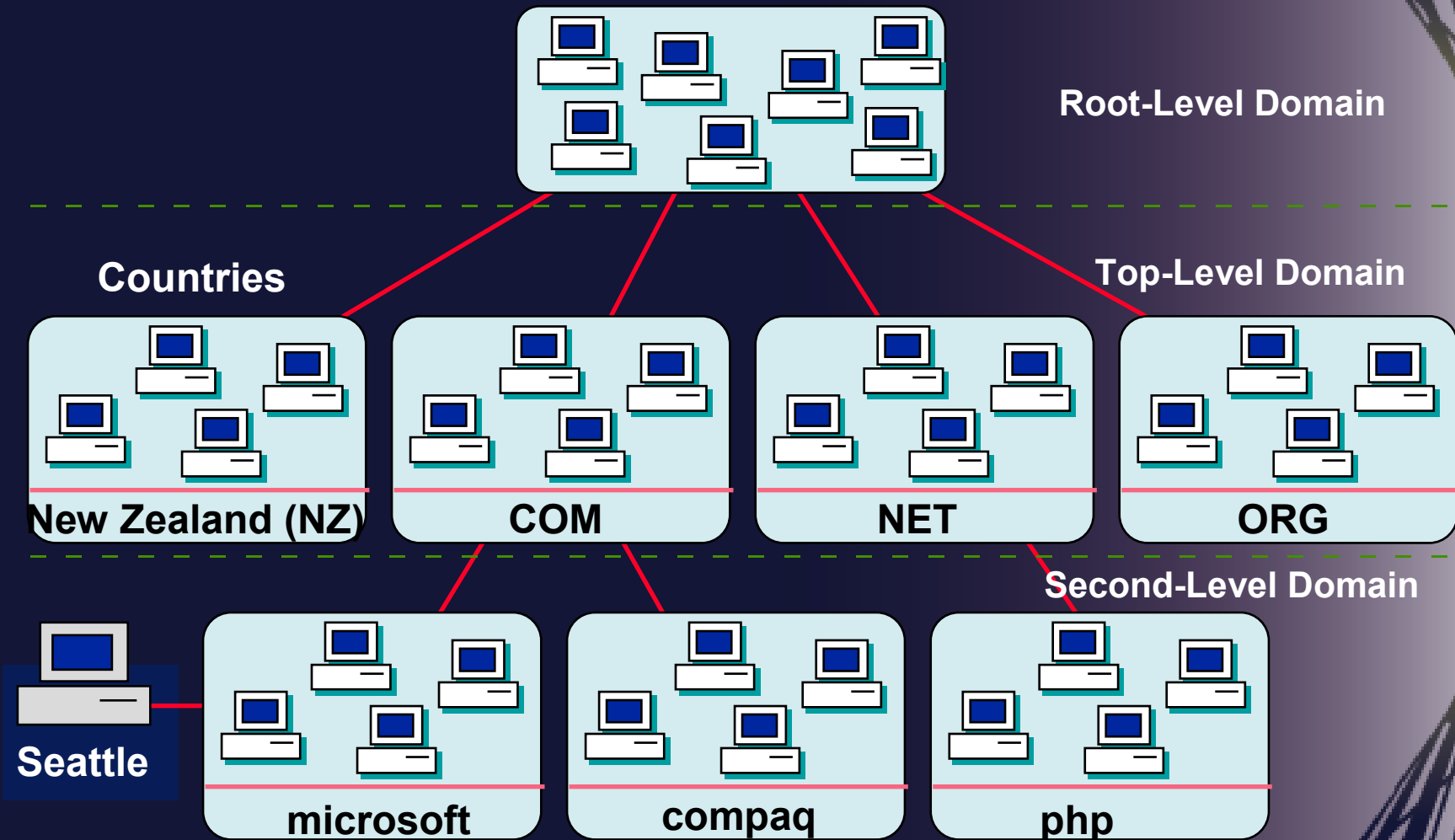
Lo spazio dei nomi

- Namespace:
 - Forma ad albero rovesciato
 - Ogni dominio e' una parte distinta del namespace, gestita da una sola entita' amministrativa

L'albero dei nomi



L'albero dei nomi



Il Reverse Lookup

Perche' fare Reverse DNS

- Corrispondenza tra indirizzi IP e nomi a dominio.
 - utilizzato da tools per troubleshooting sulla rete come traceroute o ping.
- Necessario per alcune applicazioni, in primo luogo la posta elettronica.
 - Molti mail-server rifiutano posta la cui sorgente non ha un rDNS configurato.
- Responsabilita' delle Local Internet Registry (LIR)
 - Le informazioni sul rDNS devono essere mantenute aggiornate nel DB di RIPE

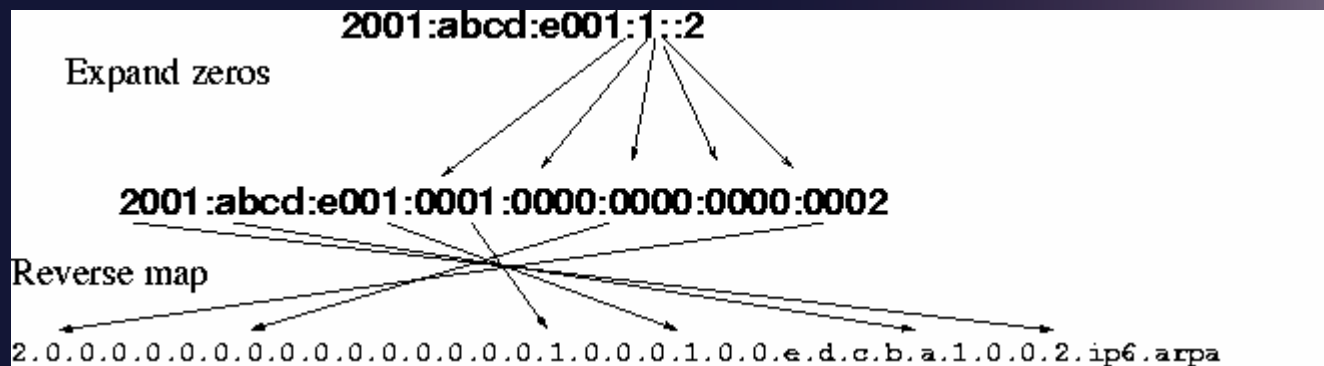
Il reverse DNS lookup

- Il reverse di un indirizzo IPv4 e' espresso, nel dominio "in-addr.arpa", da una sequenza di bytes in ordine inverso, rappresentati come numeri decimali separati da un punto
- Es:

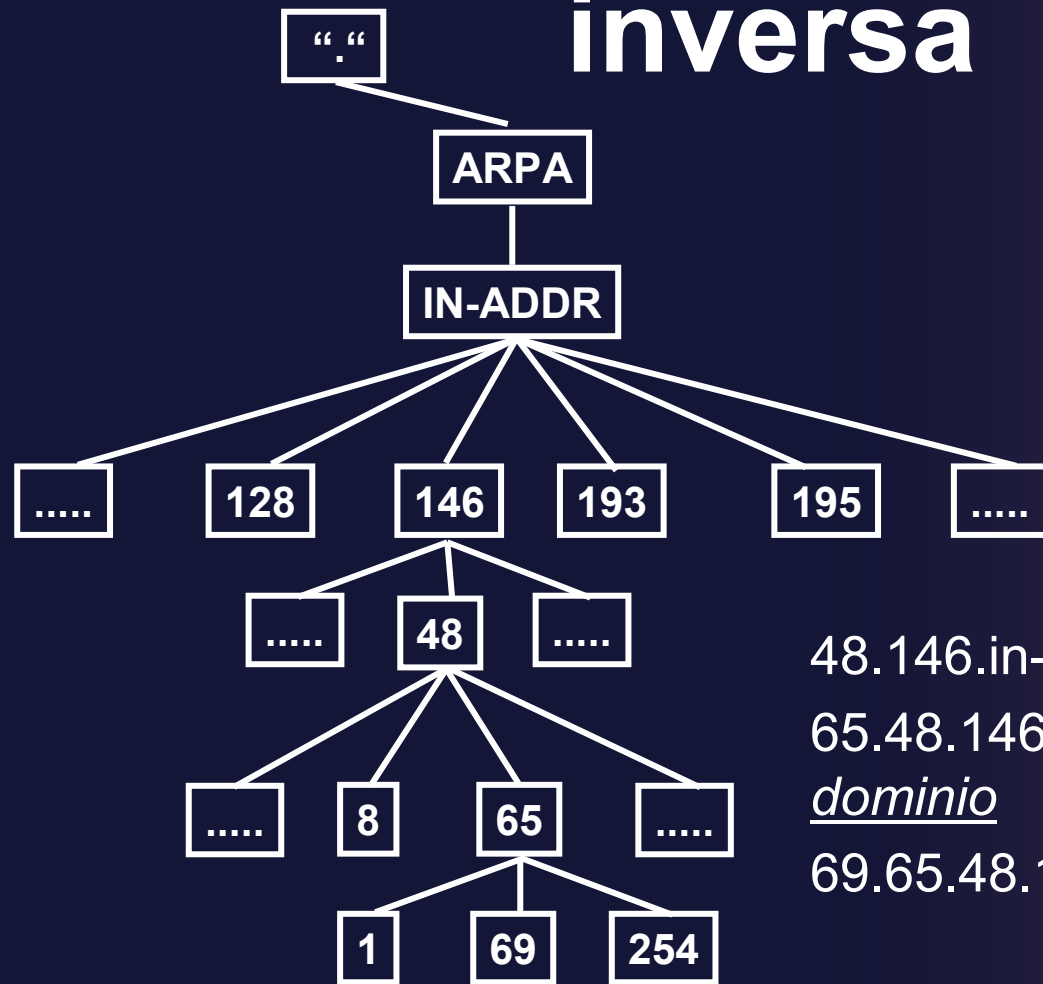
1.0.168.192.in-addr.arpa. IN PTR www.example.com.

II reverse DNS lookup

- Il reverse di un indirizzo IPv6 e' espresso, nel dominio "ip6.arpa ", da una sequenza di otto cifre esadecimali scritte in ordine inverso; i numeri e lettere sono separati da un punto



L'albero per la risoluzione inversa



48.146.in-addr.arpa dominio

65.48.146.in-addr.arpa sotto-
dominio

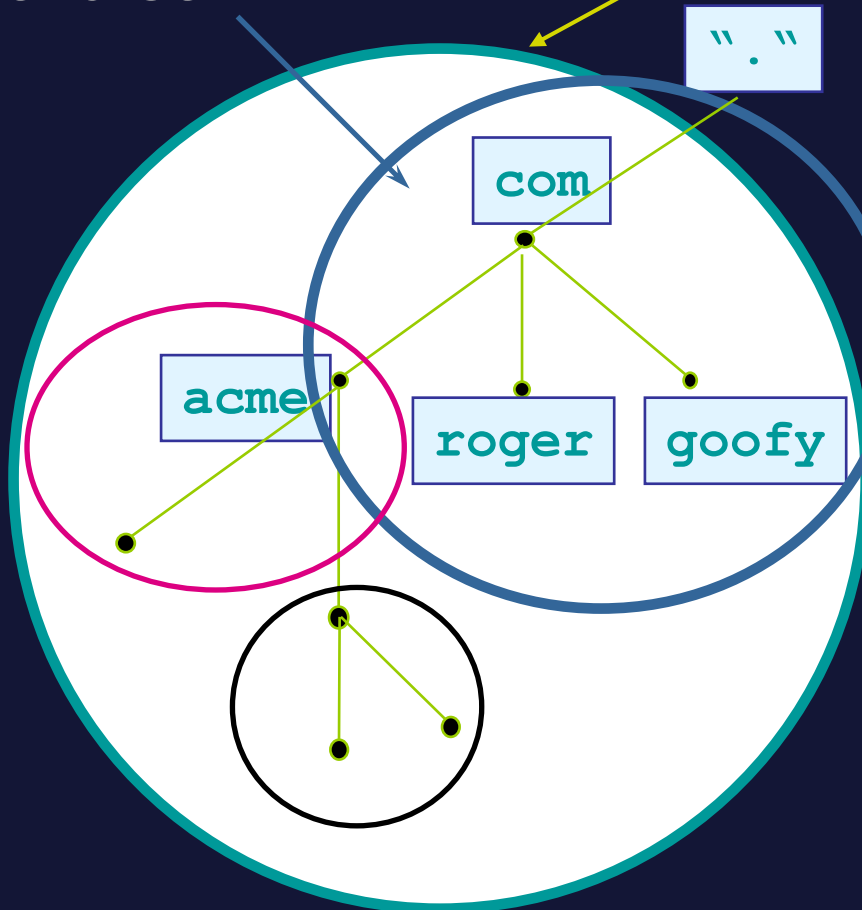
69.65.48.146.in-addr.arpa macchina

Il meccanismo di Delega

Le zone

zona com

dominio com



- un nameserver mantiene i dati di un sottoinsieme dello spazio dei nomi: *la zona*
- Una **zona** è una parte dello spazio dei nomi, costituita da un dominio e i suoi sottodomini che non sono a loro volta delegati, che è sotto una stessa gestione amministrativa ed è quindi gestita da uno o più server.
- un nameserver può gestire più *zone* disgiunte

Le zone e i nameserver

la struttura gerarchica dello spazio dei nomi si riflette nella relazione tra i *nameserver*

il meccanismo della *delega di autorità* si basa sui seguenti principi:

- ogni nameserver di un dominio, per essere conosciuto nel DNS, *deve essere stato registrato* dal nameserver del dominio di livello superiore. Questo crea la **delega**
- una volta delegata l'autorità su una zona, *il nameserver "padre" perde ogni possibilità* di modificare le informazioni dei domini contenuti nella zona delegata
- i nameserver delegati possono essere più d'uno (è consigliato averne almeno due, in alcuni casi è addirittura obbligatorio), ma *uno solo* è quello che possiede la vera autorità perché gestisce i files contenenti le informazioni

Nameserver autoritativi

- Un nameserver si definisce autoritativo quando è “in possesso dei dati” per una determinata zona dell’albero dei nomi.
- per un dominio vi possono essere più nameserver autoritativi
 - per avere una maggiore affidabilità è fortemente consigliato averne più di uno, localizzati in modo da ridurre il rischio di interruzione del servizio DNS (delocalizzati geograficamente)
- una possibile classificazione dei nameserver autoritativi e':
 - primari
 - secondari

Classificazione dei name server : Nameserver primari e secondari

Un nameserver si definisce primario (master) quando possiede i file delle informazioni (“file di zona”) e pertanto in ogni zona vi sarà un solo nameserver primario (accesso in lettura e scrittura alle info del database)

- Un nameserver si definisce secondario (slave) quando acquisisce, dal nameserver primario (quindi ha una copia in sola lettura) , i dati relativi alla zona mediante una procedura automatica denominata “zone-transfer”

i parametri che regolano il funzionamento della procedura sono contenuti in uno specifico record del nameserver primario (record Start Of Authority - SOA)

- E' necessario valutare attentamente il numero e la dislocazione dei nameserver secondari in modo da ridurre il più possibile il rischio che problemi di connessione possano impedire la risoluzione dei nomi di un dominio (configurazione fault tolerant)

Classificazione dei name server : Nameserver primari e secondari

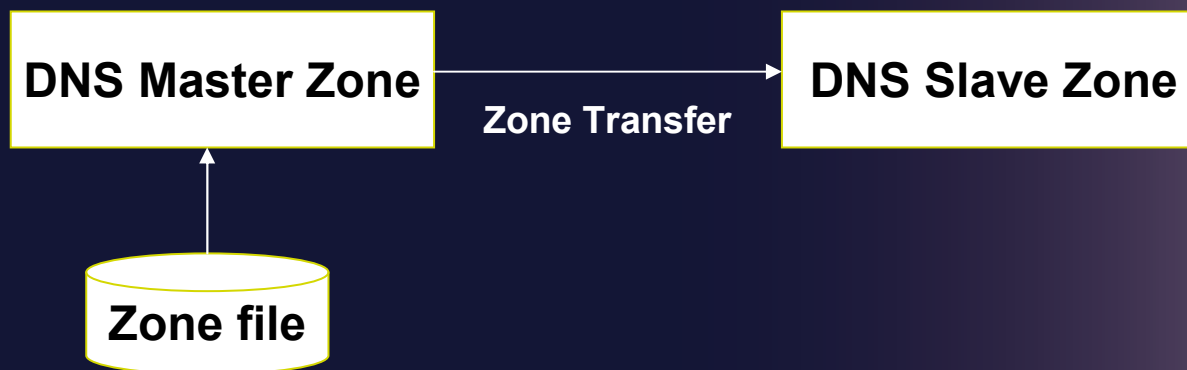
- Name server primari:
 - Direttiva type master
- Name server secondari:
 - Direttiva type slave
 - Per specificare il master da cui attingere le zone:

```
masters {  
    IP master;  
};
```

Lo Zone Transfer

- Un NS *master* ottiene i dati sulla zona da un file di zona locale a differenza del NS *slave* che ottiene i dati sulla zona mediante lo zone transfer

Lo Zone Transfer avviene su TCP, dopo ogni variazione del SERIAL del file di zona sul master



Come funziona il Domain Name System

Il processo di risoluzione: Nameserver e Resolver

Il processo di risoluzione dei nomi a dominio è basato sul modello client-server:

- il **nameserver** (server) ha il compito di fornire “risposte autoritative” ad interrogazioni sui nomi definiti nell’ambito dei domini per cui è autoritativo (cioè dei quali detiene una copia del database in lettura/scrittura);
- il **resolver** (client) è invece utilizzato dalle applicazioni che hanno necessità di effettuare una risoluzione di nomi a dominio. Esso è costituito da un insieme di routine di libreria (es. *gethostbyname*) che sono in grado di colloquiare con i nameserver, interpretarne le risposte e restituire l’informazione al programma richiedente. E’ possibile configurare il *default domain* di appartenenza, la lista dei *nameserver* da interrogare e la *search list* in un apposito file di configurazione (es. file */etc/resolv.conf* su Unix)

Configurazione del resolver

- File /etc/resolv.conf

Search domainname1 domainname2 ...domainnameN

Nameserver ipaddr1

Nameserver ipaddr2

...

Nameserver ipaddrN

Configurazione del resolver

- Search
 - Indica in quali domini cercare se un nome host non e' qualificato (FQDN)
- Nameserver
 - Indicare solo NS ricorsivi
 - Interrogati in sequenza (il secondo viene interrogato solo se il primo non e' disponibile)

Configurazione del resolver

- File `/etc/nsswitch.conf`
 - Hosts: hosts dns nis
- In esso si definisce la gerarchia dell'ordine di ricerca di un host
 - Nell'es. Corrente cerca prima in `/etc/hosts`, poi nei ns elencati in `/etc/resolv.conf` e infine interroga il DB nis

Configurazione del resolver

- Configurazione su NS :
#More /etc/resolv.conf
Nameserver 127.0.0.1
- Configurazione su host client :
#More /etc/resolv.conf
Nameserver <IP ns1>
Nameserver <IP ns2>

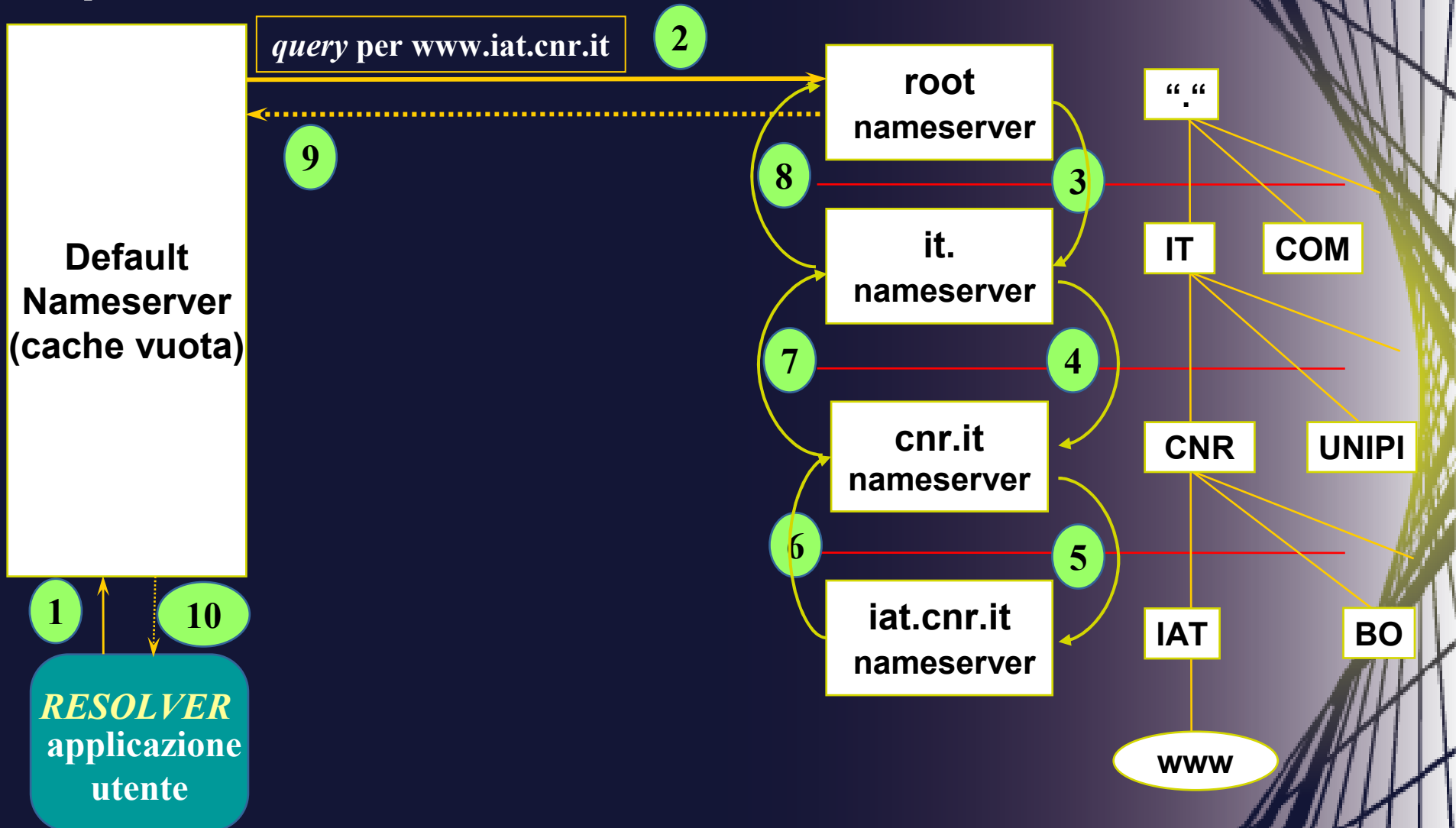
Risoluzione dei nomi

- Se il nome desiderato non è nella zona (o nella cache) del NS interrogato, si innesca il processo di risoluzione dei nomi
- La richiesta di risoluzione ripercorre l'albero fino alla radice e lo ridiscende fino ad arrivare ad un NS autoritativo la cui zona contiene il nome in questione e quindi anche gli RR
- La risposta, opportunamente salvata in tutti i cache intermedi, viene infine passata dal resolver all'utente che aveva effettuato la richiesta

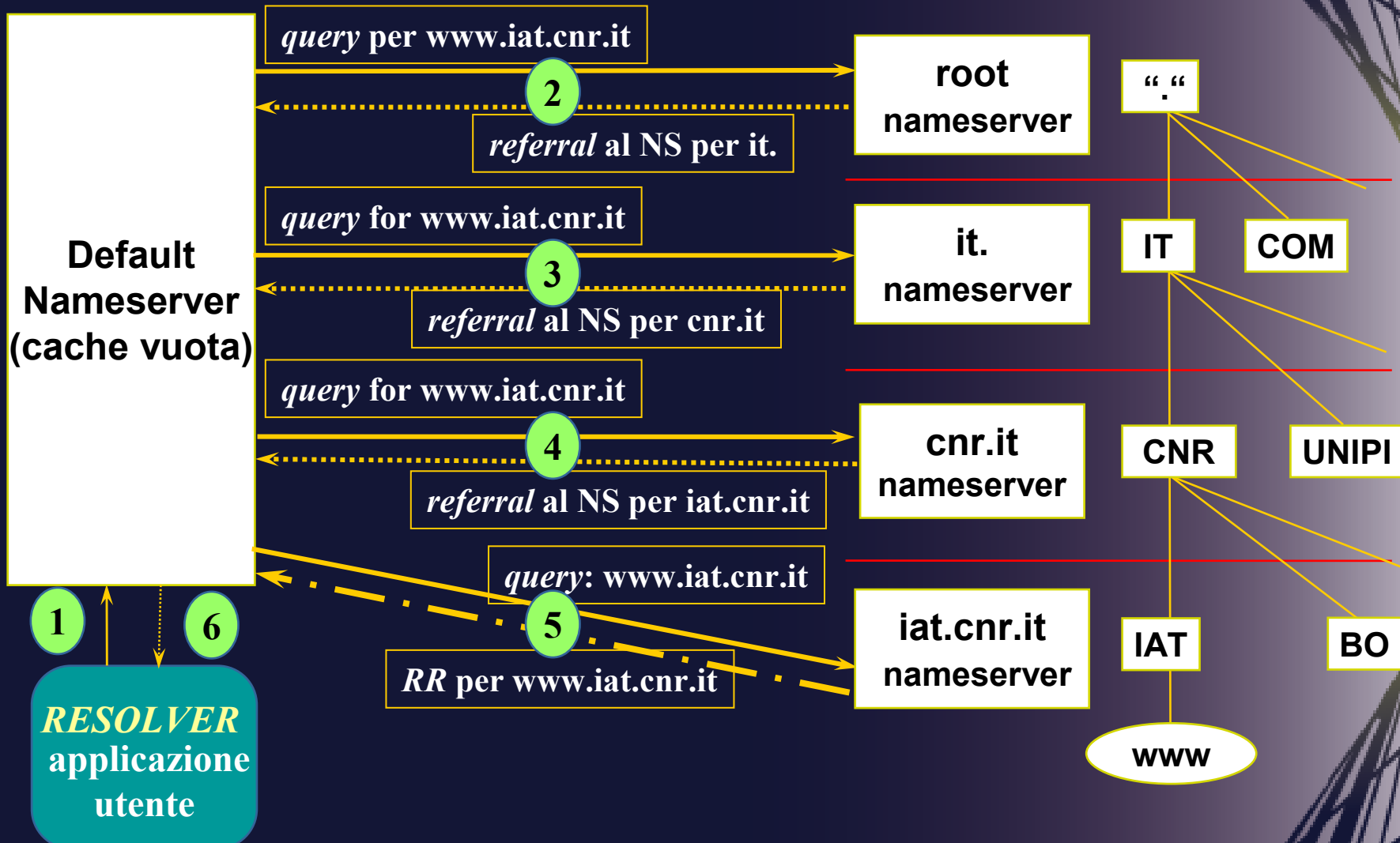
Risoluzione dei nomi

- Esistono 2 modalità di risoluzione dei nomi:
 - ricorsiva
 - Il NS di default gestisce il percorso per la risoluzione
 - viene solo restituita al client la risposta alla query o il riferimento ad un altro nameserver
 - iterativa
 - il resolver si rivolge direttamente ai vari NS della catena

Il processo ricorsivo di risoluzione dei nomi



Il processo iterativo di risoluzione dei nomi



Indirizzamento delle queries

- Che cosa accade se vi sono piu' NS autoritativi per uno stesso dominio? A quale di questi il nostro NS indirizzera' la query di risoluzione?
- L'algoritmo di indirizzamento di una interrogazione e' il seguente :
 - Il NS raggruppa i server in base al loro RTT
 - All'interno di un singolo gruppo (a parita' di RTT) l'indirizzamento avviene con ciclo round robin

Indirizzamento delle queries

- E' proprio il meccanismo di round robin nello smistamento delle interrogazioni a fornire un primitivo metodo per effettuare un bilanciamento di carico
- Es: bilanciamento di un web server
 - www IN A 192.168.0.1
 - IN A 192.168.0.2

Recursion

- Se un name server riceve una query per un dominio che non gestisce direttamente sono possibili due opzioni:
 - 1) Il name server può rispondere al client indicando un altro name server che sia in grado di rispondere in modo appropriato.
 - 2) Il name server può cercare di risolvere in modo completo la richiesta attraverso una serie di richieste agli altri name servers, fino ad aver completato la risoluzione della richiesta.

Recursion, Caching

- I name server, di solito, usano la recursion, se non hanno memorizzato le informazioni che servono per rispondere alla richiesta nella cache.
- Ogni resource record ha un campo con un valore di Time To Live (TTL) che indica il numero di secondi per i quali il record può essere mantenuto nella cache prima di essere eliminato.
- Il valore di TTL può essere specificato per ogni resource record.
- I resource record solitamente fanno riferimento al valore di TTL indicato nel campo MINIMUM del SOA.
- Anche i client possono mantenere una propria cache rispettando le stesse regole.

Authoritative Replies

- Una parte dell'intestazione di un pacchetto di DNS è il bit di Authoritative Answer (AA).
- Questo bit è marcato quanto la risposta arriva direttamente da uno dei name server primario o secondario.
- Il bit viene resettato quando la risposta arriva dalla cache locale.

Perche' avere piu' server secondari?

- Ridondanza - fault tolerance
Almeno due server DNS in posti diversi
- Localizzazione diffusa – risposta migliore alle richieste
- Ridurre il carico del server primario

Caching NS

Caching-only Name Servers

- Un name server che non ha autorità per nessuna zona e' chiamato caching-only name server.
- Un caching-only name server ottiene tutti i suoi dati da altri name server (primari o secondari).
- I server Caching-only sono name server il cui unico lavoro e' rispondere alle richieste, memorizzare le risposte e restituire i risultati.

Caching

- ogni nameserver mantiene copia di tutte le informazioni di cui è venuto a conoscenza
- tali informazioni sono utilizzate durante il processo di risoluzione dei nomi
- le risposte date dal nameserver sulla base della cache sono “*not authoritative*”
- le informazioni nella *cache* di un nameserver rimangono valide per un tempo limitato (*Time-To-Live, TTL*)

Caching

- Il caching positivo aumenta l'efficienza nelle risposte :
 - Se chiedo l'indirizzo di www.example.com al mio NS e lui lo ha in cache mi restituisce subito l'indirizzo senza passare per l'I/O su disco
- L'RFC 2038 definisce un modello di caching negativo
 - Se chiedo l'indirizzo di un host al mio DNS e non lo ha in cache lui deve chiederlo e poi memorizzarlo nella sua cache

Caching

- Perche' implementare il negative caching?
 - Una misurazione al root NS RIPE ha mostrato che il 60% delle queries chiedono dati non in cache
 - Implementare il negative caching anche negli strati bassi dell'albero DNS incrementa le prestazioni globali
- Cosa viene memorizzato nel negative caching :
 - Nessun host o dominio corrisponde all'interrogazione (default ttl 1-3 ore)
 - Il tipo di dati richiesti non esiste per questo host (default ttl 1-3 ore)
 - Il server interrogato non risponde (default ttl 5 minuti)
 - Il server e' irraggiungibile per problemi di rete (default ttl 5 minuti)

La Configurazione del Domain Name System

Le piattaforme hardware e software

- hardware

disponibile su quasi tutte le attuali piattaforme (PC, Macintosh, workstation, mainframe)

- software

prodotti di pubblico dominio (BIND per Unix e Windows, MIND/NonSequitur per MacOS)

prodotti commerciali (MacDNS, Windows server 2003)

BIND (Berkeley Internet Name Domain)

è l'implementazione di nameserver più diffusa su Internet sviluppata per Unix BSD, ne esistono *porting* per molti altri ambienti

spesso ne è inclusa una implementazione nel software di corredo di piattaforme Unix

Gestione di un NS

- Start|stop del demone:
/etc/init.d/{bind|named} start|stop
- In generale uno script di gestione di BIND potrebbe essere:

```
#!/bin/sh
```

```
Case $1 in
```

```
    Start)
```

```
        Echo "Starting BIND..."
```

```
        /usr/sbin/bind -u bind -a -f /etc/bind/named.conf
```

```
        ;;
```

```
    Stop)
```

```
        BIND_PID=`ps aux | grep bind | grep -v grep | awk '{print $2}`
```

```
        Kill -TERM $BIND_PID
```

```
        ;;
```

```
esac
```

Gestione di un NS

- Rndc:
 - Tool di gestione che permette fra le altre cose:
 - Reload di tutte o singole zone (rndc reload)
 - Schedules maintenance di una zona (rndc refresh <zone>)
 - Retransfer zone anche senza aggiornamento di un serial (rndc retransfer <zone>)
 - Ricarica soltanto file di configurazione e le zone aggiornate (rndc reconfig)
 - Abilita il logging delle queries (rndc querylog)
 - Fa un dump della cache in un file (rndc dumpdb –all)
 - Abilita la modalita' di debug (rndc trace <level>)
 - Fa il flush della cache (rndc flush)

File necessari

- il file named.conf
- il file localhost.rev
- il file named.root
- i file per la risoluzione diretta
- i file per la risoluzione inversa

Il file *named.conf* (1)

- il file *named.conf* è il file di configurazione principale per il funzionamento del processo nameserver dalla versione 8.x.y
 - definisce la directory in cui si trovano gli altri file necessari al funzionamento del nameserver (*directory*)
 - definisce la raccolta dei dati statistici relativi al processo nameserver (*statistics-interval*)
 - definisce l'ordine con cui verranno restituiti gli indirizzi delle singole macchine (*topology*)
 - definisce quali sono i nameserver che possono prelevare le zone per cui il nameserver è autoritativo (*allow-transfer*)

Il file *named.conf* (2)

- definisce il livello e la distribuzione dei “log” prodotti dal processo nameserver
- definisce i domini per i quali il nameserver è autoritativo (*master e slave*)
- definisce i riferimenti ai root nameserver (*hint*)

*Attenzione alla sintassi per i commenti
(/* */, //, # invece di ;)*

Tipi di istruzione utilizzati in named.conf

istruzione	funzione
include	interpola un file (per es. Delle chiavi fidate leggibili solo da named)
options	definisce le opzioni di configurazioni globali per il name server e I default
server	opzioni specifiche per il server
key	definisce le info di autenticazione
acl	definisce le liste di controllo di accesso
zone	definisce I RR di una zona
trusted- keys	utilizza chiavi preconfigurate
controls	definisce I canali utilizzati per controllare il demone con rndc
logging	specifica categorie di logging e loro destinazioni
view	definisce in BIND9 una vista del namespace

Tipi di istruzione utilizzati in named.conf

- Istruzione “include” permette di includere tutto il contenuto di file relativi alla customizzazione del DNS
 - Include “path”
 - Es:
 - Include “/etc/bind/named.conf.options”;
- Istruzione options permette di dichiarare una serie di opzioni relative al comportamento del NS

```
Options {  
    Option;  
    Option;  
};
```

Tipi di istruzione utilizzati in named.conf

- Es. Istruzione options

Options {

Version "string"; //la versione di BIND

Directory "path"; //directory dove sta BIND

Pid-file "/var/run/named/named.pid"; //indica il Process ID

Notify yes|no; //abilita o disabilita le automatiche notifiche master-slaves quando viene aggiornato il serial delle zone

Also-notify <server IP addr>; //notifica le modifiche di una zona anche a questo server (solo >BIND8)

Recursion yes|no; //abilita o disabilita la ricorsione

Allow-recursion { address lists match; }; //permette agli host di usare il NS come ricorsivo

Use-id-pool yes|no; //conserva gli ID delle interrogazioni in uscita, in modo da non emettere duplicati (randomizzazione dell'ID space, previene il DNS spoofing)

Maintain-ixfr-base yes|no; //abilita il logging per il trasferimento incrementale delle zone

Tipi di istruzione utilizzati in named.conf

Transfers-in <number>; //numero max di trasferimenti di zona in ingresso contemporanei

Transfers-out <number>; // numero max di trasferimenti di zona in uscita contemporanei

Listen-on port <ip port> <address_match_list>; //specifica su quale porta e interfaccia named e' in ascolto (default 53 all)

Query-source address <ip addr> port <ip port>; //specifica interfaccia e porta che questo NS usa per interrogare altri NS

Forwarders { <ip forwarder>; }; //specifica gli IP dei forwarder(s)

Forward only|first; //specifica se questo NS fa solo da forwarder o inoltra prima le sue richieste al forwarder e eventualmente poi le processa

Allow-query { <ip addr1>; }; //specifica un elenco di host ai quali e' permesso interrogare questo NS

Allow-transfer { <ip addr1>; }; //specifica a quali NS questo server puo' trasferire i RR

Blackhole { <ip addr>; }; //specifica una lista di host con cui questo NS non parlera' mai (non permette queries ne' accetta risposte)

};

Tipi di istruzione utilizzati in named.conf

- Istruzione `acl` permette di dichiarare liste di accesso per il controllo di determinate operazioni sul NS

```
Acl acl_name {  
    Address_match_list  
};
```

Es:

```
Acl lan {  
    192.168.0.0/24;  
    192.168.1.0/24;  
    Localhost;  
};
```

Tipi di istruzione utilizzati in named.conf

- Istruzione server permette di dichiarare delle opzioni specifiche di un dato NS

Server ipaddr {

Provide-ixfr yes|no; //il server ipaddr supporta I trasferimenti di zona incrementali

Request-ixfr yes|no; //il server ipaddr supporta le richieste di trasferimenti di zona incrementali

Transfers <number>; //max num. trasferimenti di zona contemporanei

Keys { <key-id>; }; //abilita l'uso di una chiave per le transazioni TSIG

};

Tipi di istruzione utilizzati in named.conf

- Istruzione logging permette di specificare le opzioni relative al logging degli eventi del NS

Logging {

file "nomefile"; //dove memorizzare il file con gli eventi di logging

Syslog local7; //scrive su syslog con la facility 7

Severity critical|debug <debug level num>; //

Print-category yes;

Print-severity yes;

Print-time yes;

Category default { default_syslog; default_debug; };

Category panic { default_stderr; };

};

Tipi di istruzione utilizzati in named.conf

- Istruzione zone permette di specificare tutte le opzioni di una zona di ricerca

```
Zone "domain_name" {  
    Type master|slave|stub|hint|forward; //tipo di ruolo  
    File "/etc/bind/db.example.com"; //path del file di zona  
    Masters {  
        Ip addr master;  
    }; //specifica gli IP address dei server master (solo per slave)  
    Allow-query { 192.168.0.0/24; 192.168.1.0/24; }; //agli hosts delle subnet 0 e 1  
        e' permesso interrogare questo NS per questa zona  
    Allow-transfer { 192.168.1.2; }; //permette il trasferimento di questa zona verso  
        il server 192.168.1.2  
    Allow-update { 192.168.1.3; }; //permette all'host (DHCP server?) di aggiornare  
        I RR di questa zona  
    Forward only|first; //specifica il comportamento del NS  
    Forwarders { ip addr forwarder; }; //specifica l'IP del o dei forwarders  
};
```

Tipi di istruzione utilizzati in named.conf

- Istruzione zone
 - Es. Config. Hint zone:

```
Zone "." {  
    Type hint;  
    File "/etc/bind/db.root";  
};
```
 - Es. Config. Master:

```
Zone "." {  
    Type master;  
    File "/etc/bind/db.example.com";  
    Allow-transfer { 192.168.1.2; };  
};
```

Tipi di istruzione utilizzati in named.conf

- Istruzione zone
 - Es. Config. slave zone:

```
Zone "." {  
    Type slave;  
    File "/etc/bind/db.example.com";  
    Masters {  
        192.168.1.1;  
    };  
};
```
 - Es. Config. forwarder:

```
Zone "." {  
    Type forward;  
    Forward only|first;  
    forwarders { 192.168.1.4; };  
}
```

Tipi di istruzione utilizzati in named.conf

- Istruzione key specifica tipo di algoritmo e valore della chiave privata utilizzata da un host per autenticarsi ed effettuare operazioni sul NS

```
Key "chiave" {  
    Algorithm "HMAC-MD5"; //algoritmo usato per generare la chiave  
    privata  
    Secret "AKLJBVUDBN"; //valore della chiave privata  
};
```

- Istruzione trusted-keys specifica algoritmo e chiavi per un insieme di zone

```
Trusted-keys {  
    Domain flags protocol algorithm key;  
    Domain flags protocol algorithm key;  
};
```

Tipi di istruzione utilizzati in named.conf

- Istruzione view specifica diversi ambiti di visibilit  delle zone rispetto a porzioni di network

```
View "internal" {  
    Match-clients { 192.168.0.0/24; 192.168.1.0/24; };  
    Recursion yes;  
    Zone "internal-zone1" ...  
    Zone "internal-zone2" ...  
    Zone "external-zone1" ...  
    Zone "external-zone2" ...  
};  
View "external" {  
    Match-clients { any; };  
    Recursion yes;  
    Zone "external-zone1" ...  
    Zone "external-zone2" ...  
};
```

Il file *named.conf*: esempio (1)

```
options {  
    // Con l'istruzione "recursion" il server tentera' di risolvere nomi anche per hosts  
    // appartenenti a domini di cui il nameserver non e' autoritativo.  
    // Se non specificato, le query ricorsive sono aperte a tutti.  
    allow-recursion {  
        10.10.0.0/16;  
        10.11.1.0/24;  
        ....  
        10.11.2/24;  
    };  
    topology { 10.0.0.1/29;  
    };  
    directory      "/etc/namedb";  
    statistics-file "/var/stats/named.stats";  
    zone-statistics yes;  
}  
logging {  
    channel query_logging {  
        file "/var/log/named_querylog"  
        versions 3 size 500M;  
        print-time yes;           // timestamp log entries  
    };  
  
    category queries {  
        query_logging;  
    };  
};
```

Il file *named.conf*: esempio (2)

```
zone "." {  
    type hint;  
    file "named.root";  
};  
  
zone "0.0.127.IN-ADDR.ARPA" {  
    type master;  
    file "master/net/localhost.rev";  
};  
//  
// Domains  
//  
zone "pippo.it" {  
    type master;  
    file "master/dom/pippo-it.soa";  
    allow-query { any; };  
    allow-transfer { 10.0.0.2;  
        };  
};  
zone "pluto.it" {  
    type slave;  
    file "slave/dom/pluto-it.for";  
    masters {  
        10.0.0.1;  
    };  
    allow-query { any; };  
    allow-transfer { none; };  
};
```


Il file *named.conf*: esempio (3)

```
//  
// Secondary for 10.0.1.0/24  
//  
zone "1.0.10.in-addr.arpa" {  
    type slave;  
    file "slave/net/10.0.1.for";  
    masters {  
        10.0.0.1;  
    };  
    allow-query { any; };  
    allow-transfer { none; };  
};  
//  
// Master for 10.0.2.0/24  
//  
zone "2.0.10.in-addr.arpa" {  
    type master;  
    file "master/bb/10.0.2.for";  
    allow-query { any; };  
    allow-transfer {  
        10.0.0.2;  
        10.0.0.3;  
    };  
};
```

Il file *named.root*

- Contiene gli indirizzi IP dei server DNS di root da cui attingere informazioni e deve essere posizionato nella directory:
`/var/named/etc/namedb`
- E' possibile reperire la versione aggiornata del file da:

`ftp://ftp.rs.internic.net/domain/named.root.`

Il file *localhost.rev*

- Contiene i dati per l'interfaccia di loopback del nameserver autoritativo.
- permette il “mapping” tra l'IP 127.0.0.1 e il localhost

Un esempio di file localhost.rev :

```
@ IN SOA nameserver.cnr.it. dns-adm.nameserver.cnr.it (
19941227 ;file Version #
86400 ;Refresh = 1 day
1800 ;Retry = 30 minutes
604800 ;Expire = 6 days
86400 ;Default TTL = 1 day
)
@ IN NS nameserver.cnr.it.
1.0.0.127.in-addr.arpa. IN PTR localhost.
```

I files di zona

- Ogni file di zona contiene:
 - Comandi per il DNS:
 - interpretati dal processo master
 - Resource Record:
 - Corrispondenze nomi-indirizzi e viceversa

Alcune regole sintattiche dei “file di zona”

- tutto quello che si trova dopo il carattere “;” e’ un commento.
- Il carattere “@” e’ sinonimo del dominio dichiarato nell’istruzione *master* del file `named.conf`
- tutti i nomi degli host specificati in un RR (eccetto i PTR) possono essere scritti in notazione assoluta (con il punto “.” finale oppure in notazione relativa (appende il nome della macchina quanto dichiarato nell’istruzione *master* di `named.conf`).

Comandi file di zona

- \$ORIGIN domain-name
- \$TTL default-ttl
- \$GENERATE vari-argomenti
- \$INCLUDE

I Records dei files di zona

- Il file di zona contiene i riferimenti necessari all'associazione tra i nomi delle macchine appartenenti ad una zona ed i loro indirizzi IP (e viceversa).
- L'associazione è fatta mediante specifici records che descrivono le caratteristiche e le funzionalità del dominio e delle macchine che gli appartengono.

I più importanti ed utilizzati sono:

SOA

NS

MX

A

CNAME

PTR

Tipi di record – SOA (1)

- Il record SOA (Start Of Authority) definisce qual'è la macchina su cui è attivo il nameserver primario per il dominio ed alcuni “parametri di funzionamento” dei nameserver secondari
- La sintassi con cui deve essere scritto è la seguente:

```
<dominio> IN SOA <host> <e-mail dns manager> (  
  <numero progressivo> ;file Version  
  <tempo in secondi> ;Refresh  
  <tempo in secondi> ;Retry  
  <tempo in secondi> ;Expire  
  <tempo in secondi> ;Minimum TTL  
)
```


Tipi di record – SOA (2)

- **Serial**

Corrisponde al numero di revisione del file della zona. Il numero viene incrementato (deve esserlo da ogni amministratore) ogni volta che si modifica un record di risorsa della zona.

- **Refresh**

Corrisponde al tempo, in secondi, che intercorre prima che un server DNS secondario invii una richiesta all'origine per effettuare il tentativo di rinnovo della zona. Alla scadenza il server DNS secondario richiede una copia del record SOA. Se i Serial risultano differenti, il server DNS secondario richiederà al server DNS primario di effettuare un trasferimento di zona.

- **Retry**

Corrisponde al tempo, in secondi, che intercorre prima che un server secondario ripeta un tentativo di trasferimento di zona non riuscito. Generalmente questo valore è inferiore a quello dell'intervallo di aggiornamento.

Tipi di record – SOA (3)

- **Expire**

Corrisponde al tempo, in secondi, che intercorre prima che un server secondario smetta di rispondere alle richieste dopo che è trascorso il tempo di refresh senza che la zona sia stata aggiornata. Alla scadenza i dati locali devono essere considerati inaffidabili dal secondario.

- **Minimum TTL**

Valore predefinito TTL (Time-To-Live) della zona e intervallo massimo per la memorizzazione nella cache delle risposte alle query dei nomi.

Tipi di record - SOA esempio

- Valori raccomandati per il SOA :

example.com. 3600 SOA dns.example.com.
hostmaster.example.com. (
1999022301 ; serial YYYYMMDDnn
86400 ; refresh (24 hours)
7200 ; retry (2 hours)
3600000 ; expire (1000 hours)
172800) ; minimum (2 days)

Tipi di record - NS

- I record NS (NameServer) definiscono quali sono i nameserver autoritativi per il dominio (è fortemente consigliato averne almeno due per ogni dominio, in certi casi è obbligatorio)
- devono essere specificati sia il nameserver primario che tutti i nameserver secondari
- La sintassi con cui deve essere scritto è la seguente:
`<dominio> <ttl> <classe> NS <nameserver host>`

Esempi:

cnr.it.	86400	IN	NS	nameserver
@	86400	IN	NS	dns.iat.cnr.it.

Tipi di record - MX

- il record MX (Mail eXchanger) definisce qual'è il *Mail eXchanger* per il dominio o per la singola macchina
- è possibile avere più record MX
- La sintassi con cui deve essere scritto è la seguente:

<dominio/host> <ttl> <classe> MX <preferenza> <mail-gateway host>

Esempi:

www.cnr.it.	86400	IN	MX	10	nameserver
www	86400	IN	MX	10	mail.iat.cnr.it.

Tipi di record - A

il record A (Address) definisce qual'è
l'indirizzo IP (numerico) per la singola
macchina

La sintassi con cui deve essere scritto è la seguente:

```
<host>      <ttr> <classe> A <indirizzo IP>
```

Esempi:

www.cnr.it. 86400 IN A 194.119.192.42

www A 146.48.65.43

Tipi di record - PTR

- Il record PTR (PoinTeR) definisce la corrispondenza tra l'indirizzo IP della singola macchina ed il suo nome a dominio
- La sintassi con cui deve essere scritto è la seguente:

<indirizzo IP> <ttl> <classe> PTR <host>

- Esempi:

11.193.114.131.in-addr.arpa.	86400	IN	PTR	www.cnr.it.
11	86400		PTR	www.cnr.it.

Tipi di record - CNAME

- il record CNAME (Canonical NAME) definisce un nome alternativo con cui può essere identificata la stessa macchina
- La sintassi con cui deve essere scritto è la seguente:

`<alias> <ttl> <classe> CNAME <host>`

Esempi:

```
dsa.cnr.it. 86400   IN      CNAME netserv
CNAME netserv.cnr.it.
```


Tipi di record - LOC

- Record LOC describe la locazione geografica e la dim. Fisica di un oggetto DNS
- Formato:
 - Name [ttl] IN LOC lat lon [alt [size [hp [vp]]]]
- Es:
 - Caida.org. IN LOC 32 53 01 N 117 14 25 W
107m 30m 18m 15m

Tipi di record - SRV

- Record SRV specifica la localizzazione di un servizio all'interno di un dominio
- Formato:
 - Service.proto.name [ttl] IN SRV pri wt port target
- Es:
 - [ftp.tcp](#) IN SRV 0 0 21 [ftp.example.com.](#) ;accetta connessioni ftp sull'host [ftp.example.com](#)
 - Finger.tcp IN SRV 0 0 79 . ;nega le connessioni al servizio finger

Tipi di record - TXT

- Record TXT utilizzato per le descrizioni all'interno del DNS
- Formato:
 - Name [ttl] IN TXT info
- Es:
 - IN TXT “name server master del dominio example.com”

Formato dei files di zona

- Formato di un file di zona diretta (risoluzione nome host – indirizzo):

```
$ORIGIN .
$TTL 86400      ; 1 day
example.garr.it      IN SOA  ns.example.garr.it. root.ns.example.garr.it. (
                        2008011601 ; serial
                        86400      ; refresh (1 day)
                        7200       ; retry (2 hours)
                        2592000    ; expire (4 weeks 2 days)
                        86400      ; minimum (1 day)
                        )
NS      ns1.garr.net.
NS      ns2.garr.net.
NS      ns.example.garr.it.
MX      0 ns.example.garr.it.
$ORIGIN example.garr.it.
srv01   A      192.168.0.1
pc01    A      192.168.1.1
lt01    A      192.168.2.1
```

Formato dei files di zona

- Formato di un file di zona inversa (risoluzione indirizzo IP – nome host):

```
$ORIGIN .
$TTL 86400      ; 1 day
0.168.192.in-addr.arpa IN SOA ns.example.garr.it. root.ns.example.garr.it. (
                                2007121401 ; serial
                                86400      ; refresh (1 day)
                                3600       ; retry (1 hour)
                                604800    ; expire (1 week)
                                86400     ; minimum (1 day)
                                )
NS      ns1.garr.net.
NS      ns2.garr.net.
NS      ns1.example.garr.it.
$ORIGIN 0.168.192.in-addr.arpa.
10      PTR      ns.example.garr.it.
1       PTR      srv01.example.garr.it.
```

Esercitazioni

- I lab sono costruiti utilizzando Linux Knoppix e User Mode Linux (UML) per le macchine virtuali
- Durante lo startup alla macchina reale è automaticamente assegnato un indirizzo IP dinamico tramite DHCP (qualora disponibile)
- Una delle macchine virtuali è connessa alla rete reale in NAT tramite l'interfaccia di tunneling tap0 e fa da default gw per tutte le altre
- Le altre sono connesse alla rete reale tramite il default gw virtuale
- Risultato:
 - Si può navigare liberamente attraverso il CDRom (macchina reale)
 - Ogni macchina virtuale accede ad Internet con IP mappato sull'interfaccia di rete reale

Esercitazioni

- Ciascuna esperienza è costruita tramite uno script (lab) che si occupa di :
 - Configurare correttamente l'interfaccia di tunneling e le NIC delle macchine virtuali
 - effettuare lo start/stop degli ambienti virtuali
 - copiare nelle opportune posizioni dei filesystems delle varie macchine virtuali i files presenti nelle cartelle ad esse relative

Lab Day 1

- Semplice configurazione a 3 macchine virtuali per mostrare la configurazione di una ipotetica zona garr.it e NS master-slave
- Le macchine sono:
 - Client (hostname clnt): 192.168.1.10
 - NS primario (ns1): 192.168.1.1
 - NS secondario (ns2): 192.168.1.2

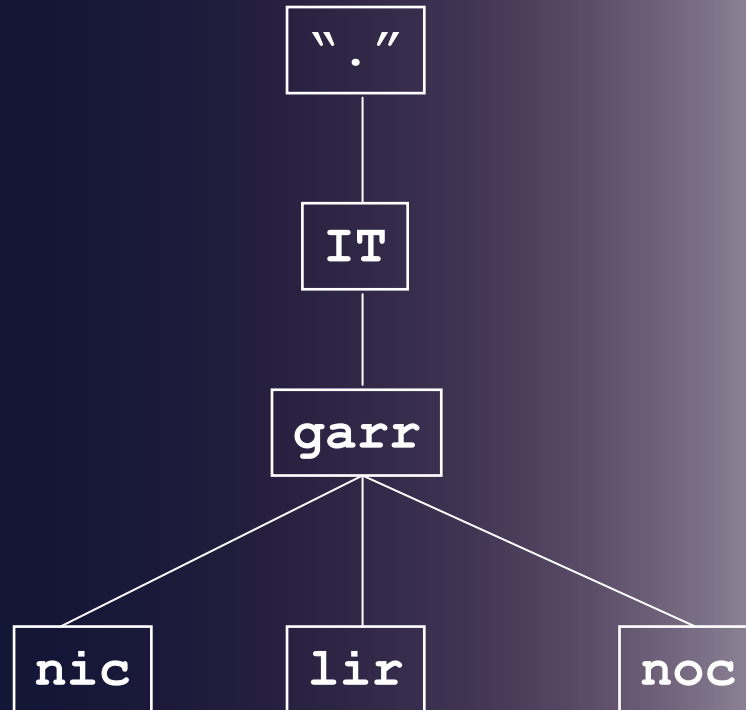
Esercitazioni

- Eseguire il boot da CDROM e premere invio al prompt
- Eventualmente per modificare il layout di tastiera da IT (default) a US(fare clic 2 volte sul simbolo in basso a destra nella barra applicazioni)
- Una volta completato il caricamento di KDE aprire una console e immettere il comando “su”
- Inserire la pennetta USB ed eseguire i comandi nella shell:
 - Mount /dev/sdb1 /media/sdb1
 - Cp -fR /media/sdb1/lab_day* /root/.
 - Cd /root/lab_day1
- Per avviare le macchine virtuali relative all’esperienza lab_day1 eseguire il comando:
 - ./lab start
- Per stoppare le macchine virtuali relative all’esperienza lab_day1 eseguire il comando:
 - ./lab stop
- Le credenziali di accesso univoche per tutte le VM sono:
 - Username: root
 - Password: root

Come configurare la delega

Il meccanismo di delega

- ogni qualvolta è necessario creare un dominio figlio (es: nic.garr.it) è necessario inserire le opportune informazioni nel dominio padre (es: garr.it).
- le deleghe si effettuano normalmente mediante i record NS ed in alcuni casi mediante i record MX



Un esempio di delega

; Domain: garr.it

```
@ IN SOA ns1.garr.net. postmaster.garr.it. (  
    2001100801 ;file Version #  
    86400      ;Refresh =    1 day  
    1800       ;Retry =    30 minutes  
    2592000    ;Expire =    30 days  
    172800     ;TTL =    2 days  
)
```

;; NAMESERVERS FOR THIS DOMAIN

```
@ 604800 NS ns1.garr.net.
```

```
@ 604800 NS ns2.garr.net.
```

;; Delegation to subdomain

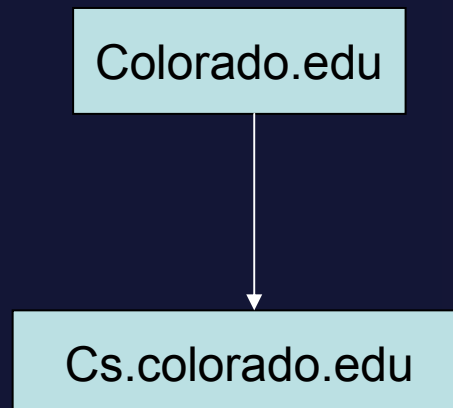
```
noc      86400  NS    ns1.garr.net.  
          86400  NS    server2.infn.it.  
dir      86400  NS    dxgarr.dir.garr.it.  
          86400  NS    ns1.garr.net.  
news     86400  NS    serra.unipi.it.  
          86400  NS    nameserver.unipi.it.  
          86400  NS    ns1.garr.net.
```

Collegamenti tra le zone : Glue record

- L'interconnessione fra le diverse zone dell'albero DNS e' garantita dichiarando nei NS padre gli indirizzi dei NS figli (autoritativi per i domini figli)
- Questo meccanismo e' alla base della delocalizzazione dell'autorita' e della struttura distribuita del DNS database

Collegamenti tra le zone : Glue record

- Ogni zona padre deve contenere I record NS di ogni zona delegata
- Es:



Collegamenti tra le zone : Glue record

- Il file della zona colorado.edu contiene :
 - More /etc/bind/db.colorado.edu

....

cs	IN	NS	ns1.cs.colorado.edu
----	----	----	---------------------

	IN	NS	ns2.cs.colorado.edu
--	----	----	---------------------

ee	IN	NS	ns1.ee.colorado.edu
----	----	----	---------------------

	IN	NS	ns2.ee.colorado.edu
--	----	----	---------------------

...

ns1.cs	IN	A	128.138.243.151
--------	----	---	-----------------

ns2.cs	IN	A	128.138.243.152
--------	----	---	-----------------

ns1.ee	IN	A	128.139.154.151
--------	----	---	-----------------

ns2.ee	IN	A	128.139.154.152
--------	----	---	-----------------

Lame delegation

- Quando si registra un nome di dominio, l'amministratore del dominio di fatto richiede formalmente una delega a gestire una parte dell'albero del DNS
- Se però le informazioni sul dominio (ad esempio i NS) non vengono correttamente comunicate all'amministratore del dominio padre (di modo che le registri) si ottiene una "delega zoppa" (lame delegation)
- Cosa accade:
 - Se un utente cerca di contattare un host nel dominio lame, il NS non rifiuterà la query
 - Il DNS ritenterà la query per molte volte, e questo colpirà sia il NS in questione che i root NS

Lame delegation

- Es:
 - Jun 5 09:07:53 Lame delegation for "www.example.com." from "63.200.24.150:53"
 - Dig www.example.com

```
;;...
;;QUESTIONS
;; www.example.com , type =A, class = IN
;; ANSWERS
www.example.com. 3600 A 209.1.23.92
Example.com 3600 NS ns1.example.com
Example.com 3600 NS ns2.example.com

Dig @ns2.example.com www.example.com
;;QUESTIONS
;; www.example.com , type =A, class = IN
;; AUTHORITY RECORDS:
Net. 244362 NS F.GTLD-SERVERS.net.
Net. 244362 NS J.GTLD-SERVERS.net.
Net. 244362 NS K.GTLD-SERVERS.net.
```
 - Cioe' ns2 e' elencato come autoritative ma non restituisce alcun record e rimanda ai root NS.
 - Quindi ns2 e' mal configurato e va corretto

Il file per la risoluzione inversa

- Il file per la risoluzione inversa contiene i riferimenti necessari all'associazione tra gli indirizzi IP delle macchine ed il loro nome.
- l'associazione è fatta mediante specifici record che descrivono le caratteristiche e le funzionalità del dominio e delle macchine che gli appartengono.

I più importanti ed utilizzati sono:

SOA

NS

PTR

Classless delegation

Risoluzione Inversa: il problema del subnetting

- Problema:

in alcuni contesti e' necessario suddividere l'uso di una classe di indirizzi su piu' domini e garantire una corretta risoluzione inversa e gestione amministrativa autonoma ai vari domini

- Soluzioni:

Reti in classe B: si procede normalmente alla delega delle singole subnet equivalenti ciascuna ad una rete in classe "C"

Reti in classe C: e' possibile effettuare la delega della risoluzione inversa anche di "parti" di una rete (RFC 2317)

Risoluzione Inversa di subnet: approccio “classico”

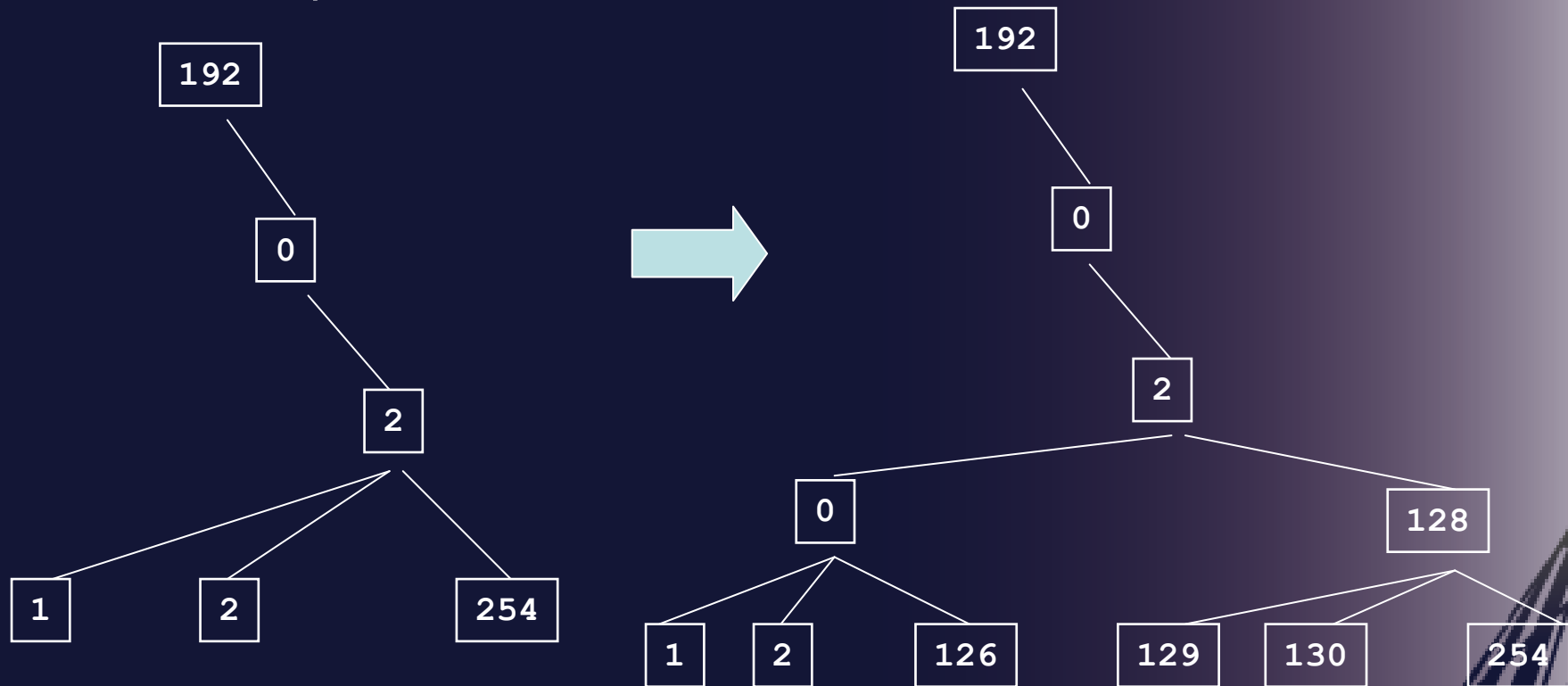
- con l'approccio classico si avrebbe:

```
;  
$ORIGIN 206.193.in-addr.arpa.  
158      IN      SOA   dxgarr.dir.garr.it. root.dxgarr.dir.garr.it. (  
          2008021501 86400 3600 604800 86400 )  
          IN      NS    dxgarr.dir.garr.it.  
          IN      NS    ns1.garr.net.  
          IN      NS    ns2.garr.net.  
;  
$ORIGIN 158.206.193.in-addr.arpa.  
;  
1         IN      PTR   dxgarr.dir.garr.it.  
2         IN      PTR   lx1.dir.garr.it.  
3         IN      PTR   lx2.dir.garr.it.  
4         IN      PTR   ns.dir.garr.it.  
....  
241       IN      PTR   vpn01.dir.garr.it.  
242       IN      PTR   vpn02.dir.garr.it.  
243       IN      PTR   vpn03.dir.garr.it.  
...  
254      IN      PTR   pcgarr.dir.garr.it.
```

Risoluzione Inversa di subnet: approccio “classless” (1)

- Si crea un nuovo “point of delegation” aggiungendo un ulteriore livello nell’albero IN-ADDR.ARPA

Esempio: suddivisione della 192.0.2.0 in due sottoreti:



Risoluzione Inversa di subnet: approccio “classless” (1)

- **Configurazione IP Classless Reverse Delegated Zone**
 - es : dominio bo.ingv.it
 - individuare la subnet assegnata tramite interrogazione sul router
 - query DNS al server del dominio bo.ingv.it
 - individuare IP del NS primario e record MX

Risoluzione Inversa di subnet: approccio “classless” (2)

Configurazione lato dominio utente

- aggiungere a named.conf la zona reverse per la subnet classless

```
zone "26/128.89.204.193.in-addr.arpa" {  
    type master;  
    file "/etc/bind/26-128.89.204.193.rev";  
};
```

- creare in /etc/namedb la zona reverse per la subnet classless

```
#vi /etc/bind/26-128.89.204.193.rev  
26-128.89.204.193.rev  
$ttl 38400  
@      IN      SOA     dns.bo.ingv.it. postmaster.bo.ingv.it. (  
        2007100401  
        86400  
        3600  
        604800  
        86400 )  
@      IN      NS      dns.bo.ingv.it.  
@      IN      NS      ns1.garr.net.  
133    IN      PTR     dns.bo.ingv.it.  
157    IN      PTR     mail2.bo.ingv.it.
```


Risoluzione Inversa di subnet: approccio “classless” (3)

Configurazione lato GARR

- modificare named.conf con direttiva slave per la zona come segue:

```
zone "128.89.204.193.in-addr.arpa" {  
    type master;  
    file "/etc/bind/128.89.204.193.rev";  
};  
  
zone "26/128.89.204.193.in-addr.arpa" {  
    type slave;  
    masters {  
        193.204.89.133; //dns.bo.ingv.it  
    };  
    file "/etc/bind/26-128.89.204.193.rev";  
};
```

Risoluzione Inversa di subnet: approccio “classless” (4)

Configurazione lato GARR

aggiungere la zona IP classless reverse delegated per la subnet nella /24 esistente (modello da RFC2317 - <http://www.ietf.org/rfc/rfc2317.txt>) :

```
#vi /etc/namedb/128.89.204.193.in-addr.arpa
$ORIGIN 128.89.204.193.in-addr.arpa.
@ IN SOA ns1.garr.net. hostmaster.ns1.garr.net. (
    2007100401
    86400
    3600
    604800
    86400 )
;
IN NS ns1.garr.net.
IN NS ns2.garr.net.
;...
; <<64-127>> /26
64/26 IN NS dns.mi.ingv.it.
64/26 IN NS ns1.garr.net.
;
65 IN CNAME 65.64/26.89.204.193.in-addr.arpa.
66 IN CNAME 66.64/26.89.204.193.in-addr.arpa.
; <<128-191>> /26
128/26 IN NS dns.bo.ingv.it.
128/26 IN NS ns1.garr.net.
;
133 IN CNAME 133.128/26.89.204.193.in-addr.arpa.
157 IN CNAME 157.128/26.89.204.193.in-addr.arpa.
;
```

La sicurezza del Domain Name System

Gli attacchi al DNS

- Gli attacchi più comuni sono :
 - Denial of service
 - Cache corruption (spoofing)
 - Acquisizione di informazioni non autorizzate
 - Modifica dei dati (dynamic update)

Attacchi: denial of service

Descrizione:

Questo genere di attacchi mira ad impedire il funzionamento del name server ('denial of service') alterando i dati in suo possesso o mandando in 'crash' il processo stesso.

Tipicamente vengono condotti inviando al server DNS delle query artefatte ('malformed') la cui elaborazione provoca, in alcune versioni di Bind, accessi errati ai dati in memoria o a volte il crash del processo named.

Soluzioni:

Mantenere aggiornato Bind

Attacchi: cache corruption (DNS poisoning)

Descrizione:

utilizzando i meccanismi di caching del named, combinato con l'esecuzione di queries ricorsive, un name server può essere forzato a contattare dei name server non autoritativi per l'ottenimento delle informazioni. Inoltre alcune vecchie versioni di named e named-xfer (antecedenti alla 4.9) conservano in memoria i 'glue record' e utilizzano tali informazioni per i processi di risoluzione.

Soluzione:

Mantenere aggiornato bind e disabilitare la ricorsione (oppure restringere l'accesso al nameserver solo alle macchine 'di fiducia')

Attacchi: acquisizione di informazioni non autorizzate

Descrizione:

utilizzando named- xfer (o altre utility come host, nslookup, etc) è possibile richiedere l'intero contenuto di una zona.

Soluzione:

utilizzare l'opzione **allow-transfer** per specificare quali indirizzi IP sono abilitati al trasferimento del contenuto di una intera zona. Ricordarsi di applicare tali restrizioni a tutti i name server autoritativi (primari e secondari)

Attacchi: modifica dei dati

Descrizione:

Dal bind 8 è stata introdotta la funzionalità del dynamic update (disabilitata per default). Essa consente di inserire o rimuovere delle informazioni da una zona in modo dinamico, utilizzando il tool nsupdate.

Soluzioni:

verificare che nel file di configurazione non vi siano istruzioni di 'allow- update'. Nella eventualità si decidesse di utilizzare tale funzionalità, è opportuno ricordare che nell'opzione allow- update è possibile specificare solo l'indirizzo IP della macchina autorizzata (e non username e/ o password).

Alcune regole pratiche per la sicurezza del named

Alcune regole pratiche per migliorare il livello di sicurezza di un server DNS:

- restringere lo zone-transfer solo ai nameserver secondari e verificare che tali restrizioni siano attivate anche su tutti gli altri nameserver autoritativi
- disabilitare la possibilità di effettuare update dinamici (nsupdate)
- disabilitare la ricorsione (se non necessaria)
- eseguire named senza i privilegi di root (named -u xxx)
- nel caso di utilizzo di un firewall per proteggere una rete, predisporre un nameserver esterno con le sole informazioni relative alle macchine visibili su Internet (es. www server, mail server, etc) e uno interno, utilizzabile solo dalle macchine locali, con le informazioni complete della zona.

Named e la sicurezza

I principali meccanismi implementati da named sono:

- restrizione degli accessi
- inibizione dei *zone-transfer*
- autenticazione
- views
- dnsec

Restrizione degli accessi

- La restrizione degli accessi avviene mediante le Access Control Lists, che consentono di specificare un gruppo di indirizzi:

Esempio:

```
// indirizzi da 194.119.200.0 a 194.119.207.255
acl cnr-bari {
    { 194.119.200.0/21 };
};

// solo l'indirizzo 194.119.192.34
acl singola_macchina {
    { 194.119.192.34/32 };
};
```

Restrizione degli accessi (2)

Le ACL possono essere applicate in vari contesti:

- allow-query autorizzazione a effettuare query
- allow-transfer autorizzazione a richiedere zonetransfer
- blackhole indirizzi di ns o client da ignorare
- listen-on interfacce e porte su cui ascoltare
- topology/sortlist consentono di stabilire una preferenza nelle reti da contattare

Il file named.conf: la restrizione degli accessi

```
options {  
  // consento zone- transfer solo alle macchine presenti sulla rete del  
  // CNR di Bari 194. 119. 200.0-> 194. 119. 207. 255 ed alla macchina  
  // 193.205.245.8  
  allow- transfer {  
    cnr- bari; // definita nell'acl precedente  
    193. 205. 245. 8;  
  };  
  // consento le query solo alle macchine  
  // 194.119.0.0 -> 194.119.255. 255  
  allow- query {  
    194. 119/ 16;  
  };  
}
```

Il file named.conf: dichiarazione delle zone

```
zone "0. 0. 127. in- addr. arpa" in {  
type master;  
file "named. local";  
};  
zone "cnr. it" in {  
type master;  
file "cnr/ soa. cnr- it";  
allow- transfer {  
cnr- bari; // definita nell'acl precedente  
193. 205. 245. 8;  
};  
};  
zone "." in {  
type hint;  
file "named. root";  
};
```

SICUREZZA: opzioni avanzate

- Speciali opzioni di avvio di named:
 - /usr/sbin/named –u 53 –g 53 –t /var/named
 - u 53 :
 - UID 53
 - g 53 :
 - GID 53
 - t /var/named :
 - Directory chroot /var/named

SICUREZZA : opzioni avanzate

- Implementazione di comunicazione sicure :
 - Crittografia a chiave privata con TSIG/TKEY
- Il comando shell utilizzato per la generazione della chiave e':
 - Dnssec-keygen
 - Es:
 - Dnssec-keygen -H 128 -h -n serv1-serv2
 - Crea la chiave a 128 bit e la salva nel file Kserv1-serv2+157+00000.private
 - Nel file c'e' la stringa "Key:" seguita dalla chiave

SICUREZZA : opzioni avanzate

- La chiave deve essere copiata sui server le cui comunicazioni devono essere messe in sicurezza e dichiarata nel file named.conf nel modo seguente:

```
Key serv1-serv2 {  
    Algorithm HMAC-MD5;  
    Secret "shared-secret-key";  
};
```

- N.B. :
 - Il file .key dovrebbe essere 600 e l'owner dovrebbe essere l'UID di named

SICUREZZA : opzioni avanzate

- Includere la chiave in named.conf :
 Include "serv1-serv2.key";
- Dichiarare su ciascun server il suo NS peer che utilizzerà la chiave per gli aggiornamenti:
 - Su serv1:
 Server serv2-IPaddr {
 Keys { serv1-serv2; };
 };
 - Su serv2:
 Server serv1-IPaddr {
 Keys { serv1-serv2; };
 };

SICUREZZA : opzioni avanzate

- A questo punto bisogna permettere agli host che si presentano con quella chiave le operazioni (ad. Es. Quella di aggiornamwento) come segue:

```
Allow-update { key serv1-serv2; };
```

SICUREZZA : opzioni avanzate

- TSIG/TKEY utilizza un meccanismo di chiave privata per gli aggiornamenti
- Limite di TSIG/TKEY:
 - Garantisce solo da dove proviene la risposta, non che questa sia corretta
- Tuttavia in BIND 9 e' disponibile anche un meccanismo a chiave pubblica (DNSSEC)
- Cioe' il meccanismo a chiave pubblica permette:
 - di verificare l'autenticita' dell'host che tenta di effettuare un aggiornamento (e' effettivamente chi dice di essere)
 - Di criptare I dati che cosi' non viaggiano in chiaro sulla rete

SICUREZZA : opzioni avanzate

- Implementazione di DNSSEC:
 - Creare una zona firmata
 - `Dnssec-keygen -a DSA -b 768 -n ZONE example.com`
 - Generare la richiesta di firma per la chiave generata da inoltrare al NS del dominio padre:
 - `Dnssec-makekeyset -t 3600 -s now+864000 Kexample.com.+003+12345`
 - Crea il file `example.com.keyset` che contiene la chiave `Kexample.com.+003+12345` con un TTL di 1 ora e chiede che la chiave firmata abbia validita' 10 giorni
 - Il padre firma la richiesta con il comando:
 - `Dnssec-signkey example.com.keyset Kcom.+003+56789`
 - Firma della zona con la chiave firmata dal padre:
 - `Dnssec-signzone -o example.com db.example.com`

SICUREZZA : opzioni avanzate

- Un record SIG contiene:
 - Tipo di record
 - Algoritmo di firma
 - TTL RR
 - Data e ora scadenza firma
 - Data e ora di firma
 - ID chiave
 - Nome del firmatario
 - La firma

SICUREZZA : opzioni avanzate

- Per usare la nuova zona firmata in named.conf sostituire “db.example.com” con “db.example.com.signed”
- Per gestire le risposte negative in zone firmate (host non esistente) si utilizzano I record NXT
 - Es:
 - Anchor.cs.colorado.edu IN NXT
 - awesome.cs.colorado.edu A MX NXT

SICUREZZA : opzioni avanzate

- DNSSEC assume che I NS contattino la zona root e seguano poi tutta la NS chain per ottenere una risposta (ignorano forwarders e cache NS)

Il DNS e IPv6

IPv6

- L'utilizzo di IPv6 non modifica i meccanismi di base del *Domain Name System*
- Per gestire gli indirizzi IPv6 sono stati introdotti:
 - Un nuovo resource record per associare gli indirizzi IPv6 ad un nome
 - Un (due) nuovo dominio per la risoluzione inversa degli indirizzi IPv6

Un nome ad un indirizzo IPv6

- **AAAA record**
 - Definisce la mappatura fra il nome a dominio e l'indirizzo IPv6
 - Equivalente al record **A** utilizzato in IPv4

Un indirizzo IPv6 ad un nome

- PTR record
 - Definisce la mappatura fra un indirizzo IPv6 e un nome a dominio
 - Lo stesso tipo di record utilizzato per IPv4
 - Un nuovo modello di *top level* usato per IPv6:
 - da ip6.int (deprecato dall'IETF 1 Giugno 2006)
 - a ip6.arpa
 - Divisione fatta su 4 bits a differenza di IPv4 in cui si utilizza una struttura *classful*

Configurazione con BIND

- **AAAA record**

\$ORIGIN 6net.garr.it

www IN AAAA 3ffe:b00:c18:1:290:27ff:fe17:fc1d

- **PTR record (*ip6.arpa*)**

\$ORIGIN 1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa

d.1.c.f.7.1.e.f.f.f.7.2.0.9.2.0 IN PTR www.6net.garr.it

Configurazione del named.conf

- Configurazione per la 2001:760:1010::/48
- Nel named.conf del master:

```
zone "0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa" {  
    type master;  
    file "master/ipv6/2001.760.1010.soa";  
    allow-transfer { 10.0.0.2; };  
    allow-query { any; };  
};
```

- Nel named.conf dello slave:

```
zone "0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa" {  
    type slave;  
    file "slave/2001.760.1010.soa";  
    masters {  
        10.0.0.1;  
    };  
    allow-query { any; };  
};
```

Configurazione dei file di zona

\$ORIGIN .

```
pluto.pippo.net      IN SOA  pluto.pippo.it. staff-lir.pippo.net. (
                    2008011101 ; serial
                    86400      ; refresh (1 day)
                    7200       ; retry (2 hours)
                    2592000    ; expire (4 weeks 2 days)
                    345600    ; minimum (4 days)
                    )
```

\$TTL 86400

```
NS    ns1.pippo.net.
NS    ns2.pippo.net.
```

\$ORIGIN pluto.pippo.net.

```
pc1      AAAA  2001:760:1010::1
pc2      AAAA  2001:760:1010::2
```

Configurazione dei file di zona

\$TTL 86400

```
@      IN      SOA      ns1.pippo.it.  nic.pippo.it. (
```

```
2006092101 ; Serial
86400       ; Refresh
7200        ; Retry
2592000     ; Expire
345600 )    ; Minimum TTL
```

```
IN      NS      ns1.pippo.net.  
IN      NS      ns2.pippo.net.
```

\$ORIGIN 0.1.0.1.0.6.7.0.1.0.0.2.ip6.arpa.

•
,
•
,
•
,

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	IN	PTR	pc1.pluto.pippo.net.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	IN	PTR	pc2.pluto.pippo.net.

□ □ □ □ □

Trasporto

- Richieste di risoluzione indirizzi IPv6 con trasporto su pacchetti IPv4 e IPv6
 - *Bind 4-8* risponde alle richieste fatte **soltanto** su trasporto IPv4
 - *Bind 9* puo' rispondere alle richieste direttamente su trasporto IPv6
- La macchina che ospita il DNS deve essere DUAL-STACK!

Trasporto

- Per rendere operativo sul nameserver il trasporto IPv6, sul `named.conf` si configura quanto segue:

```
options {  
    listen-on-v6 { any; };  
};
```

- Prima di BIND 9.3.0 l'istruzione `listen-on-v6` accettava solo *any* o *none* come argomenti. Ora e' possibile, mediante il comando *port*, configurare anche una porta alternativa alla 53:

```
options {  
    listen-on-v6 port 1055 { any; };  
};
```

I tool e le utility per il Domain Name System

Utility di supporto nella gestione di un nameserver

- nslookup
- host
- dig
- dnswalk
- nsupdate

L'RFC 1713 descrive un insieme di tools che possono essere utili per il debugging della configurazione di un nameserver

nslookup

- è normalmente distribuito insieme al S.O. o alla distribuzione di BIND
- si può utilizzare sia in modalità interattiva che tramite riga di comando
- dispone di aiuto in linea

nslookup (2)

- Query per tutti i record del dominio garr.it

```
#:~$ nslookup
> server ns1.garr.net
Default server: ns1.garr.net
Address: 2001:760:ffff:ffff::aa#53
Default server: ns1.garr.net
Address: 193.206.141.38#53
> set query=any
> garr.it
Server:      ns1.garr.net
Address:     2001:760:ffff:ffff::aa#53
```

```
garr.it
  origin = ns1.garr.net
  mail addr = postmaster.garr.it
  serial = 2008012203
  refresh = 86400
  retry = 1800
  expire = 2592000
  minimum = 172800
garr.it nameserver = ns2.garr.net.
garr.it nameserver = ns1.garr.net.
garr.it name = A$GARR.C$IT.X400.
garr.it mail exchanger = 15 lx1.dir.garr.it.
garr.it mail exchanger = 20 lx5.dir.garr.it.
```

nslookup (3)

- Query per il record SOA del dominio garr.it

```
> set query=soa
> garr.it
Server:      ns1.garr.net
Address:     2001:760:ffff:ffff::aa#53
```

```
garr.it
  origin = ns1.garr.net
  mail addr = postmaster.garr.it
  serial = 2008012203
  refresh = 86400
  retry = 1800
  expire = 2592000
  minimum = 172800
```

nslookup (4)

- Query per il record MX del dominio garr.it

```
> set query=mx
```

```
> garr.it
```

```
Server:      ns1.garr.net
```

```
Address:     2001:760:ffff:ffff::aa#53
```

```
garr.it mail exchanger = 15 lx1.dir.garr.it.
```

```
garr.it mail exchanger = 20 lx5.dir.garr.it.
```


host

- è incluso nella distribuzione di BIND ed è inoltre reperibile presso:

`ftp://ftp.nikhef.nl/pub/network/host.tar.Z`

- non è interattivo: si utilizza da *linea di comando*
- permette di fare interrogazioni complesse a qualsiasi nameserver
- è dotato di aiuto in linea

```
host
host -av cnr.it nameserver.cnr.it
host -t soa cnr.it
```

host (2)

- Query per tutti i record del dominio cnr.it

```
> host -va cnr.it
```

```
Query about cnr.it for record types ANY
```

```
Trying cnr.it ...
```

```
Query done, 6 answers, status: no error
```

```
The following answer is not authoritative:
```

```
cnr.it      542353 IN      NS      nameserver.cnr.it
cnr.it      542353 IN      NS      dns2.nic.it
cnr.it      542353 IN      NS      itgbox.iat.cnr.it
cnr.it      542353 IN      NS      simon.cs.cornell.edu
cnr.it      542353 IN      NS      ns1.surfnet.nl
cnr.it      155353 IN      SOA     nameserver.cnr.it Daniele.Vannozzi.iat.cnr.it (
2000111801 ;serial (version)
86400      ;refresh period (1 day)
1800       ;retry interval (30 minutes)
604800     ;expire time (1 week)
86400      ;default ttl (1 day)
)
```

```
.....
```

host (3)

- Query per il record SOA del dominio garr.it

```
#:~$ host -t soa garr.it
```

```
garr.it has SOA record ns1.garr.net.postmaster.garr.it. 2008012203 86400 1800  
2592000 172800
```

dig

- è incluso nella distribuzione di BIND
- non è interattivo; si utilizza da *linea di comando*
- permette di fare interrogazioni complesse ed a qualsiasi nameserver
- è dotato di aiuto in linea

```
dig -h
```

```
dig dns.iat.cnr.it
```

```
dig dns.iat.cnr.it mx
```

```
dig -x 146.48.65.3
```

```
dig @nameserver.cnr.it cnr.it
```

dig (2)

- Query per tutti i record del dominio cnr.it

```
# dig cnr.it
; <<>> DiG 9.4.1-P1 <<>> cnr.it
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62166
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;cnr.it.                IN      A
;; AUTHORITY SECTION:
cnr.it.                 8580    IN      SOA      dns.cnr.it. m\astolfi.src.cnr.it. 2008031801 86400
                   3600 604800 86400

;; Query time: 1 msec
;; SERVER: 193.206.141.38#53(193.206.141.38)
;; WHEN: Thu Mar 20 16:08:22 2008
;; MSG SIZE rcvd: 78
```

dnswalk

- DNS debugger
- Esegue il trasferimento di zona di un dominio e ne controlla la consistenza dei dati (record NS e MX che corrispondono a CNAME, catena di CNAME, mancanza della risoluzione inversa, ecc.)
- Riproduce sul file system la struttura del DNS per il dominio controllato
- Necessita del perl e di alcuni moduli aggiuntivi (Net::DNS e IO::Socket). Le vecchie versioni di dnswalk necessitano anche di 'dig'

dnswalk (2)

Effettua controlli su:

- associazione tra record A e PTR
- uso dei CNAME (es. CNAME definito verso un altro CNAME)
- uso dei record MX (MX definito verso CNAME o host inesistenti)
- presenza di un solo nameserver
- utilizzo di caratteri non validi nei nomi a dominio (es: '_')
- assenza del '.' finale nei record PTR (125 IN PTR host.cnr.it)

NSUPDATE

Consente di aggiornare una zona in modo dinamico, inviando al named i RR da inserire.

nsupdate

```
> update add cc.dynamic.ba.cnr.it 3600 IN A 100.100.100.100
```

causerà l'inserimento del RR 'cc 3600 IN A 100.100.100.100' nel dominio dynamic.ba.cnr.it

L'operazione verrà registrata in un file di log ('file di zona'.log) e propagata ai server secondari:

```
;BIND LOG V8
```

```
[DYNAMIC_UPDATE] id 8347 from [193.204.191.39].1315 at 941985572 (named pid 959)
```

```
:
```

```
zone: origin dynamic.ba.cnr.it class IN serial 1999072501
```

```
update: {add} cc.dynamic.ba.cnr.it. 3600 IN A 100.100.100.100
```

```
;BIND LOG V8
```

```
[INCR_SERIAL] from 1999072501 to 1999072502 Sat Nov 6 15:44:32 1999
```


NSUPDATE (2)

La possibilità di aggiornare una zona via nsupdate va abilitata in named.conf mediante 'allow-update'. Il controllo dell'accesso al momento è basato solo sull'indirizzo IP o chiave di autenticazione.

Esempio:

```
zone "dynamic.ba.cnr.it" {  
    type master;  
    file "dom.dynamic.ba.cnr.it";  
    allow-update {  
        193.204.191.39;  
    };  
};
```

Aggiornamento dei Dati sul DNS presso le Authority

Aggiornamento del DNS per domini sotto il “.it” e “.eu”

- Non occorre produrre documentazione
- L'Ente deve configurare:
 - Il proprio DNS primario
 - Un eventuale DNS secondario
 - Il GARR-NIC può fornire il servizio di DNS secondario.
- L'APM deve comunicare a GARR via email (staff-dns@garr.it) le modifiche eseguite richiedendo l'aggiornamento dei dati

La Procedure Interna

- Il GARR-NIC controlla la corretta configurazione dei DNS, primario e secondario.
- Il GARR-NIC invia il modulo elettronico di registrazione alle Authority.

Regole dei Registrar

- Per registrare un dominio sotto il ccTLD “.it” e’ necessario disporre di un nameserver primario e di almeno un secondario.
- Per la registrazione di un dominio sotto il ccTLD “.eu” non e’ necessario disporre di nameserver gia’ configurati al momento della registrazione.

Gli errori di configurazione piu' frequenti

- Mancata configurazione del nameserver primario
- Corretta configurazione del primario ma secondario non configurato
- Record MX non configurato
- Valori dei parametri del record SOA errati
- Serial non aggiornato dopo la modifica della configurazione del nameserver
- Non viene permesso lo zone transfer ad ns1.garr.net se configurato come secondario

Controllo automatico del Registro sui nameserver

- E' attivato al momento della ricezione del modulo di registrazione via e-mail se e solo se questo ha superato la fase del controllo sintattico
- Principali controlli:
 - Corrispondenza tra i campi nserver riportati nel modulo e quanto contenuto realmente nei DNS.
 - Configurazione dei DNS dichiarati nel modulo di registrazione
 - raggiungibilita' dei nameserver
 - verifica se il DNS e' autoritativo per quel dominio
 - presenza record MX e record A che non punti a un CNAME
 - valori di refresh (≥ 86.400), retry (≥ 1.800) e expire (≥ 604.800) se dns2.nic.it o dns3.nic.it deve svolgere la funzione di secondario
 - Notifica al GARR-NIC dell'esito del controllo

Aggiornamento dati reverse-lookup

- Le informazioni sul reverse sono registrate nel DB RIPE.
 - Le informazioni relative al DNS non vengono piu' indicate negli inetnum:

```
inetnum:      193.206.158.0 - 193.206.158.255
netname:      GARR-BNETWORK
descr:        Consortium GARR - Direzione - Roma
country:      IT
admin-c:      EV182-RIPE
tech-c:       GL965-RIPE
tech-c:       MC4743-RIPE
status:       ASSIGNED PA
remarks:      To notify abuse mailto: cert@garr.it
remarks:      GARR - Italian academic and research network
mnt-by:       GARR-LIR
source:       RIPE
```


Aggiornamento dati reverse-lookup

- I dati sui nameserver autoritativi per il reverse lookup di una rete vengono riportati nel domain object.
 - Esempio di domain object:

```
domain:      206.193.in-addr.arpa
descr:       Class C networks block for
descr:       GARR-connected Organisations
admin-c:     EV182-RIPE
tech-c:      GL965-RIPE
zone-c:      GL965-RIPE
nserver:     ns1.garr.net
nserver:     ns2.garr.net
nserver:     ns.ripe.net
mnt-by:      GARR-LIR
changed:     gallo@garr.it 20050801
source:      RIPE
```

Aggiornamento dati reverse-lookup

- Per lo spazio IPv6 non e' necessario aggiungere altri domain object oltre a quello relativo alla /32 allocata a GARR-LIR.

```
domain:      0.6.7.0.1.0.0.2.ip6.arpa
descr:       Reverse delegation for GARR sub-tla
admin-c:     EV182-RIPE
tech-c:      GL965-RIPE
zone-c:      GL965-RIPE
zone-c:      GP4562-RIPE
nserver:     ns1.garr.net
nserver:     ns2.garr.net
nserver:     ns.ripe.net
mnt-by:      GARR-LIR
changed:     paolini@garr.it 20030228
changed:     paolini@garr.it 20060728
source:      RIPE
```

Aggiornamento dati reverse-lookup: procedura interna

- Le richieste di aggiornamento del reverse devono essere inviate via email al GARR-LIR (staff-dns@garr.it).
- Il GARR-LIR controlla la corretta configurazione del DNS.
- IL GARR-LIR provvede a configurare la delega sul nameserver GARR autoritativo per le classi IP allocate da RIPE a GARR e ad aggiornare le informazioni sul DNS presso il database RIPE (ove richiesto)

Bibliografia, Bookmark e Riferimenti

Contatti

E-mail del GARR-NIC: nic@garr.it

E-mail del GARR-LIR: lir@garr.it

Staff DNS: staff-dns@garr.it

Tel.: +39-06.4962.2550

Fax: +39-06.4962.2044

Riferimenti Bibliografici

- DNS and BIND, 3rd Edition (Paul Albitz & Cricket Liu, September 1998)
- RFC 882 - Domain Names, Concepts and Facilities (P. Mockapetris, Sep 1983)
- RFC 883 - Domain Names, Implementation and Specification (P. M., Nov 1983)
- RFC 973 - Domain System Changes and Observations (P. M., Jan 1986)
- RFC 974 - Mail Routing and the Domain System (C. Partridge, Jan 1986)
- RFC 1034 - Domain Names, Concepts and Facilities (P. M., Nov 1987)
- RFC 1035 - Domain Names, Implementation and Specification (P. M., Nov 1987)
- RFC 1123 - Requirements for Internet Hosts, Application and Support (IETF, Oct 1989)
- RFC 1340 - Assigned Numbers (ISI, Jul 1992)
- RFC 1537 - Common DNS Data File Configuration Errors (P. Beertema, Oct 1993)
- RFC 1591 - Domain Name System Structure and Delegation (J. Postel, Mar 1994)
- RFC 1713 - Tools for DNS debugging (A. Romao, Nov 1994)
- RFC 1912 - Common DNS Operational and Configuration Errors (D. Barr, Feb 1996)
- RFC 2317 - Classless IN-ADDR.ARPA delegation (BSD - ISC, Mar 1998)

BookMark

- <http://www.isc.org> : Bind
- <http://www.ietf.org/rfc.html> : RFC index
- <http://www.iana.org> : IANA
- <http://www.icann.org> : ICANN
- <http://www.nic.it> : Registro
- <http://www.eurid.eu>: EURid
- <http://www.dns.net/dnsrd/> : DNS Resources Directory
- <http://www.bind9.net/>

Esercitazioni

- I lab sono costruiti utilizzando Linux Knoppix e User Mode Linux (UML) per le macchine virtuali
- Durante lo startup alla macchina reale è automaticamente assegnato un indirizzo IP dinamico tramite DHCP (qualora disponibile)
- Una delle macchine virtuali è connessa alla rete reale in NAT tramite l'interfaccia di tunneling tap0 e fa da default gw per tutte le altre
- Le altre sono connesse alla rete reale tramite il default gw virtuale
- Risultato:
 - Si può navigare liberamente attraverso il CDRom (macchina reale)
 - Ogni macchina virtuale accede ad Internet con IP mappato sull'interfaccia di rete reale

Esercitazioni

- Ciascuna esperienza è costruita tramite uno script (lab) che si occupa di :
 - Configurare correttamente l'interfaccia di tunneling e le NIC delle macchine virtuali
 - effettuare lo start/stop degli ambienti virtuali
 - copiare nelle opportune posizioni dei filesystems delle varie macchine virtuali i files presenti nelle cartelle ad esse relative

Lab Day 2

- Esempio di configurazione di delega di autorità per un dominio di terzo livello (op.garr.it, NS ns1.op.garr.it e ns2.op.garr.it) rispetto a dominio di secondo livello (garr.it, NS ns1.garr.it e ns2.garr.it)
- In totale 5 macchine:
 - Client (clnt): 192.168.1.10
 - NS Primario dominio secondo livello (ns1.garr.it): 192.168.1.1
 - NS secondario dominio secondo livello (ns2.garr.it): 192.168.1.2
 - NS Primario dominio terzo livello (ns1.op.garr.it): 192.168.2.1
 - NS secondario dominio terzo livello (ns2.op.garr.it): 192.168.2.2

Esercitazioni

- Eseguire il boot da CDROM e premere invio al prompt
- Eventualmente per modificare il layout di tastiera da IT (default) a US(fare clic 2 volte sul simbolo in basso a destra nella barra applicazioni)
- Una volta completato il caricamento di KDE aprire una console e immettere il comando “su”
- Inserire la pennetta USB ed eseguire i comandi nella shell:
 - Mount /dev/sdb1 /media/sdb1
 - Cp -fR /media/sdb1/lab_day* /root/.
 - Cd /root/lab_day1
- Per avviare le macchine virtuali relative all’esperienza lab_day1 eseguire il comando:
 - ./lab start
- Per stoppare le macchine virtuali relative all’esperienza lab_day1 eseguire il comando:
 - ./lab stop
- Le credenziali di accesso univoche per tutte le VM sono:
 - Username: root
 - Password: root

FINE