Domain Name System

Daniele Vannozzi
Istituto Applicazioni Telematiche
Via S. Maria, 36
56126 Pisa

Daniele.Vannozzi@iat.cnr.it

Argomenti trattati

- le funzioni del Domain Name System
- lo spazio dei nomi
- interazioni tra nameserver e resolver
- configurazione di un nameserver
- utility per l’interrogazione dei nameserver
- interazioni tra DNS e posta elettronica

DNS: le funzioni

- ad ogni risorsa TCP/IP può essere assegnato un *nome simbolico*

  Sono necessari:

  – un metodo per associare il nome simbolico di una macchina all'indirizzo (o agli indirizzi) IP: *risoluzione diretta*

  – un metodo per associare ad un indirizzo IP al nome simbolico della macchina: *risoluzione inversa*

DNS: breve storia

- file *HOSTS.TXT* mantenuto presso SRI-NIC (Arpanet)
  - traffico e sovraccarico del server centrale
  - collisioni dei nomi
  - consistenza dei dati gestiti centralmente
- Domain Name System (DNS)
  - definito presso ISI - USC 1984
  - RFC 882, RFC 883 (obsolete)
  - RFC 1034, RFC 1035 e successivi

DNS: caratteristiche principali

- il DNS permette ad ogni organizzazione che ha accesso ad Internet di:
  - amministrare la relazione tra nomi ed indirizzi del proprio dominio in maniera autonoma ed indipendente
  - risolvere i nomi fuori del proprio dominio accedendo alle informazioni gestite da altre organizzazioni

DNS: caratteristiche principali

- database distribuito
- basato sul modello client/server
- tre componenti principali:
  - spazio dei nomi e informazioni associate (Resource Record - RR)
  - nameserver (application server che mantiene i dati)
  - resolver (client per l'interrogazione del nameserver)

Lo spazio dei nomi

- struttura gerarchica dell'albero dei nomi
  - TLD : domini generali (gTLD), domini nazionali (ccTLD) e per la gestione della risoluzione inversa (arpa)
  - dominio e zona di autorità
  - delega di autorità e "parenting"
  - root-nameserver

Lo spazio dei nomi

- lo spazio dei nomi è organizzato secondo il modello gerarchico:
  - il database del DNS ha una struttura logica “ad albero rovesciato”
  - ciascun nodo dell’albero rappresenta un *dominio*
  - ogni dominio può essere suddiviso in altri domini: *sottodomini*
  - ogni nodo ha una etichetta che lo identifica rispetto al padre

  La radice dell'albero è unica, e la sua etichetta è vuota. In certi casi si indica anche come “.”

L’albero dei nomi

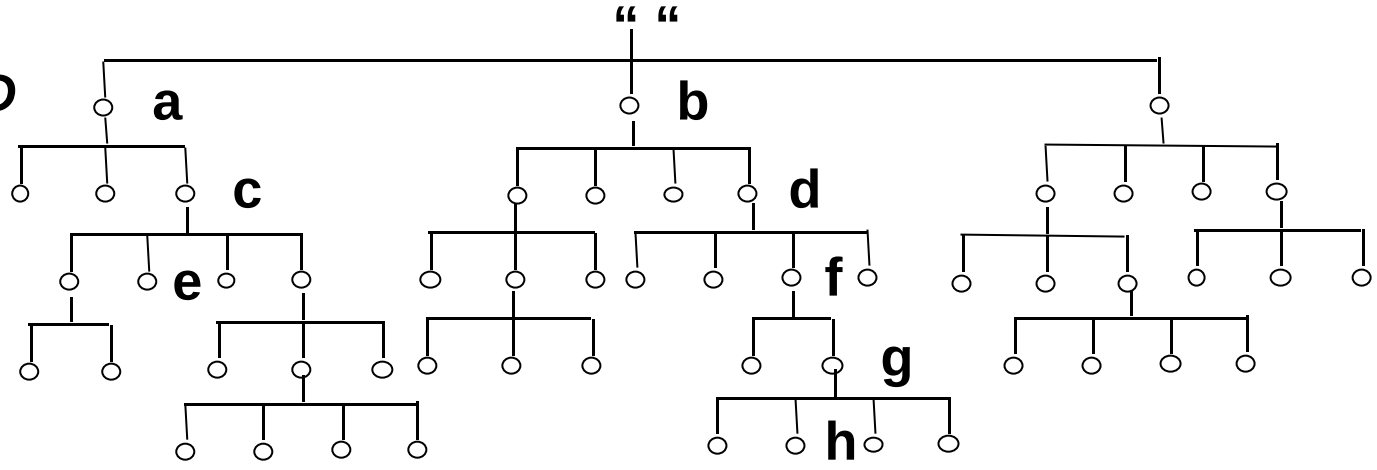
Top Level Domain, TLD

First Level Domain

Second Level Domain

.....

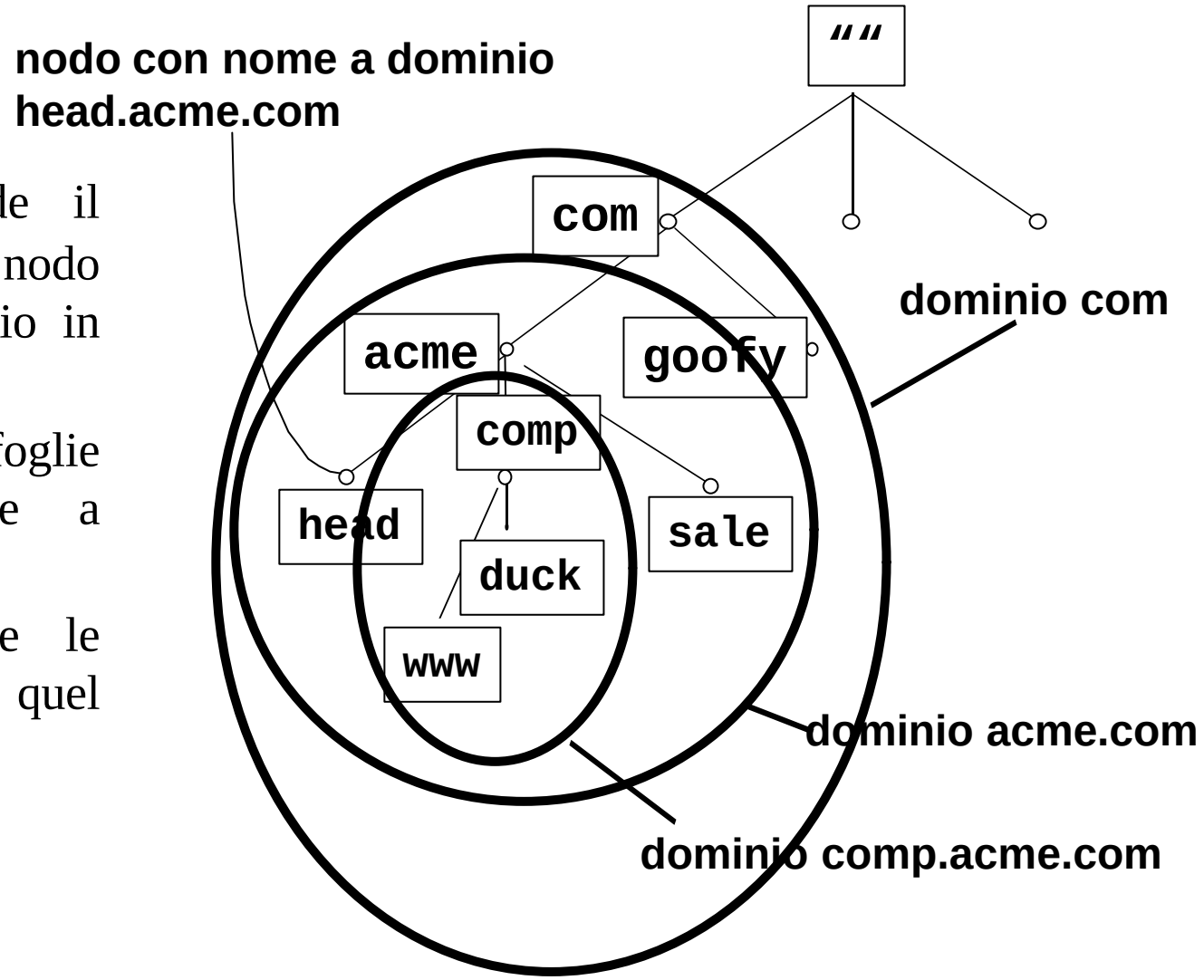
.....



- il “*domain name*” (nome a dominio) di ogni nodo è composto dalla sequenza delle etichette dal nodo a “ “ (root), separate da “.” (punto). Es: e.c.a, h.g.f.d.b
- un nome a dominio assoluto è detto anche “*fully-qualified domain name*” o *FQDN*
- il *”Distributed Information Tree”* (albero dei nomi) definisce una gerarchia dei nomi che rende ogni nome a dominio completamente qualificato univoco in tutto l’albero

I domini

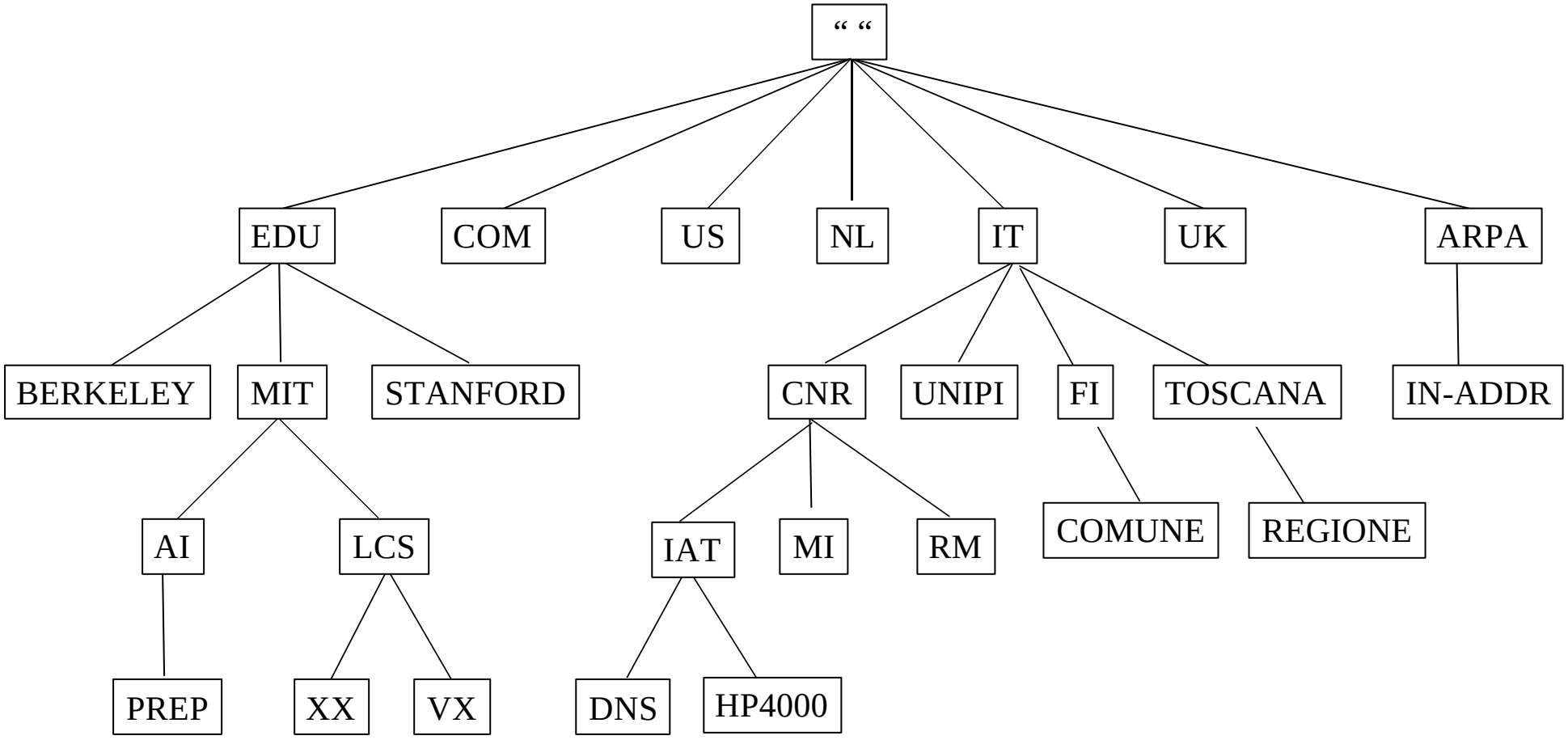
- per *dominio* si intende il sottoalbero che inizia dal nodo con il nome a dominio in questione
- di solito, le foglie rappresentano il nome a dominio di un host
- ai nodi sono associate le informazioni relative a quel nome a dominio (RR)
  - entry di host
  - entry strutturali



L’Internet Domain Name Space

- lo spazio dei nomi di Internet, per “tradizione” (rfc1591), è strutturato secondo un modello misto organizzazionale/geografico
- i *Top-Level-Domain* sono
  - domini generali “storici” di tipo organizzazionale (gTLD):
    - *com*: organizzazioni commerciali
    - *edu*: università e ricerca USA
    - *gov*: organizzazioni governative USA
    - *mil*: organizzazioni militari USA
    - *net*: provider, centri di interesse per l’Internet, ..
    - *org*: organizzazioni non governative
    - *int*: organizzazioni internazionali, trattati, ...
  - domini *nazionali*, rappresentati dai codici ISO 3166 di 2 lettere (ccTLD)
  - il dominio *arpa*

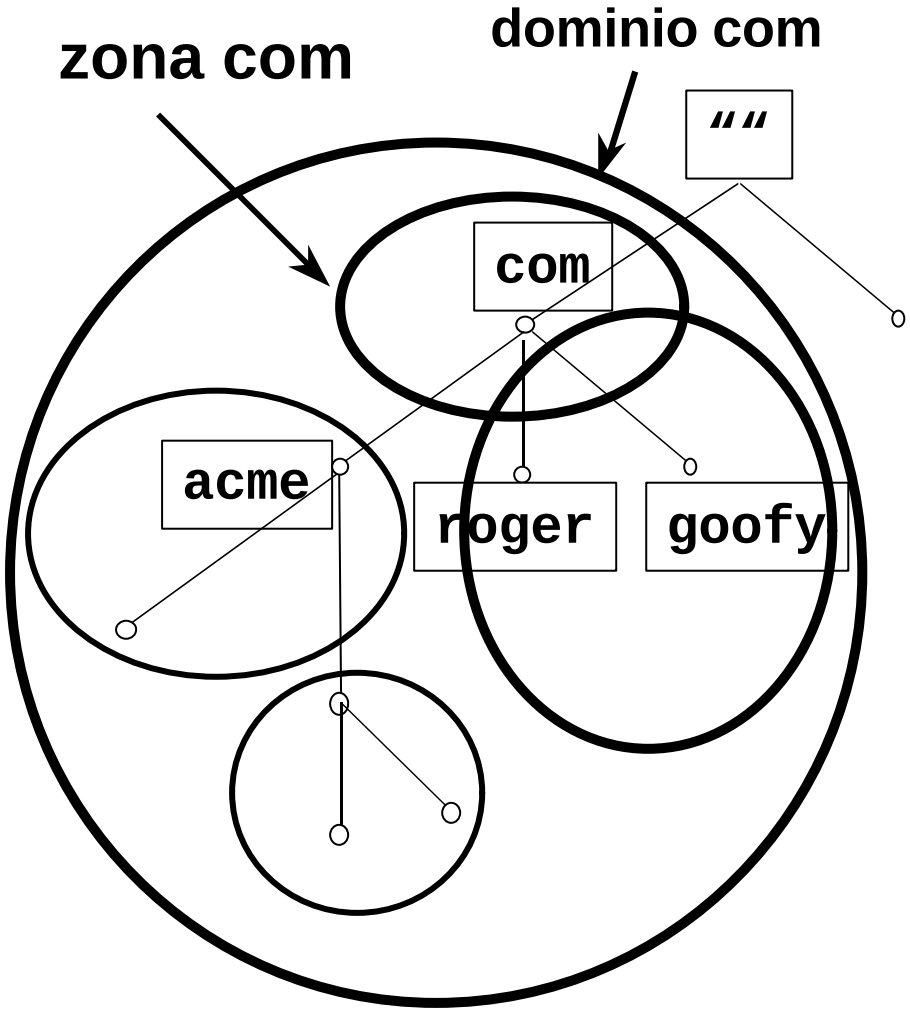
L’Internet Domain Name Space



La delega di autorità

- la *decentralizzazione* della responsabilità amministrativa è ottenuta attraverso il meccanismo della *delega*
- ogni dominio è amministrato da una autorità che è responsabile:
  - per le regole di naming valide all'interno del dominio
  - per delegare la gestione dei domini figli (*sotto-domini*)
- il gestore del dominio "." è InterNIC (per conto dello IANA/ICANN), che delega l'autorità per la gestione dei TLD
- ogni sotto-dominio può essere delegato

Domini e zone: differenze



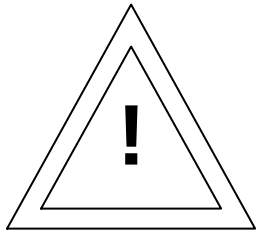
- le informazioni sono mantenute nei *nameserver*
- un nameserver mantiene i dati di una parte dello spazio dei nomi: la *zona*
- ogni *zona* può comprendere vari domini su una porzione del DIT non disgiunta
- un nameserver può gestire più *zone* disgiunte
- il dominio padre contiene solo puntatori alla sorgente dei dati dei suoi sottodomini
  - ciascuna zona contiene i nomi a dominio e i dati appartenenti ad certo dominio, esclusi i nomi e i dati dei sottodomini delegati ad altri

Domini e zone: i nameserver

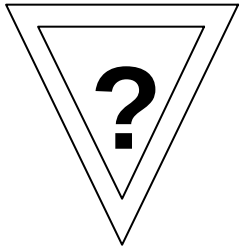
- la struttura gerarchica dello spazio dei nomi si riflette nella relazione tra i *nameserver*
- il meccanismo della *delega di autorità* si basa sui seguenti principi:
  - ogni nameserver di un dominio, per essere conosciuto nel DNS, *deve essere stato registrato* dal nameserver del dominio di livello 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

Il “parenting”

Dipende da varie considerazioni:



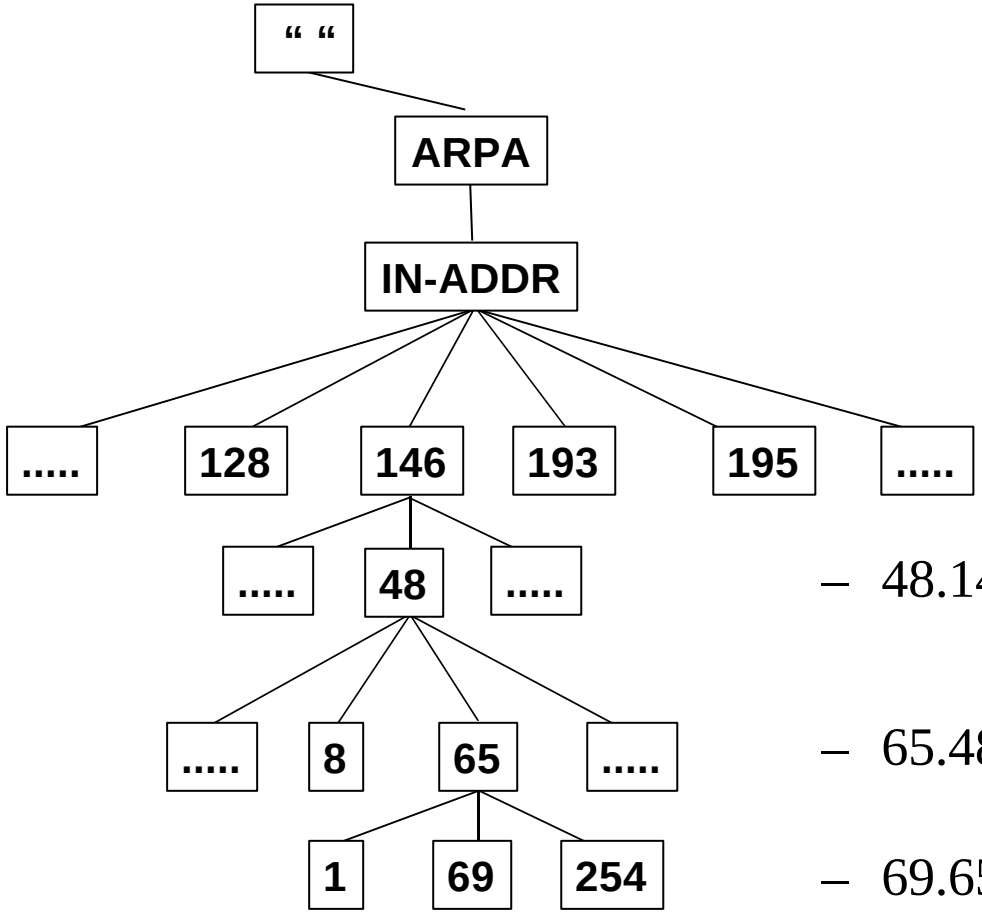
- necessità di definire sottodomini per partizionare uno spazio dei nomi piatto e molto esteso
- necessità di distinguere l’affiliazione delle macchine di un dominio
- necessità di distribuire la gestione



- quanti sottodomini definire?
- quando delegarne la gestione?
- che nome assegnare ai sottodomini?

Attenzione alla corretta gestione del meccanismo della delega per garantire la risoluzione dei nomi per tutto il dominio!!

L’albero per la risoluzione inversa



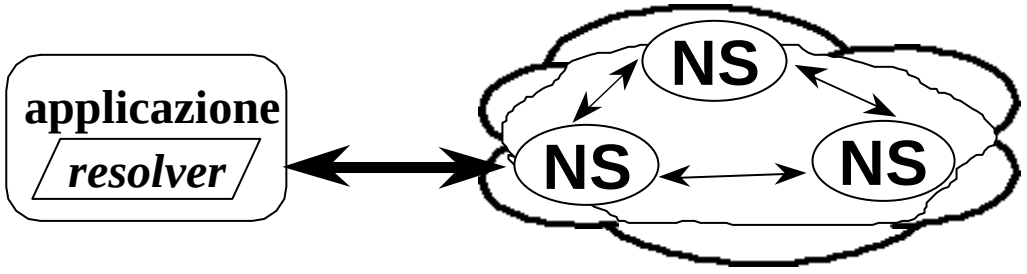
– 48.146.in-addr.arpa *dominio*

– 65.48.146.in-addr.arpa *sotto-dominio*

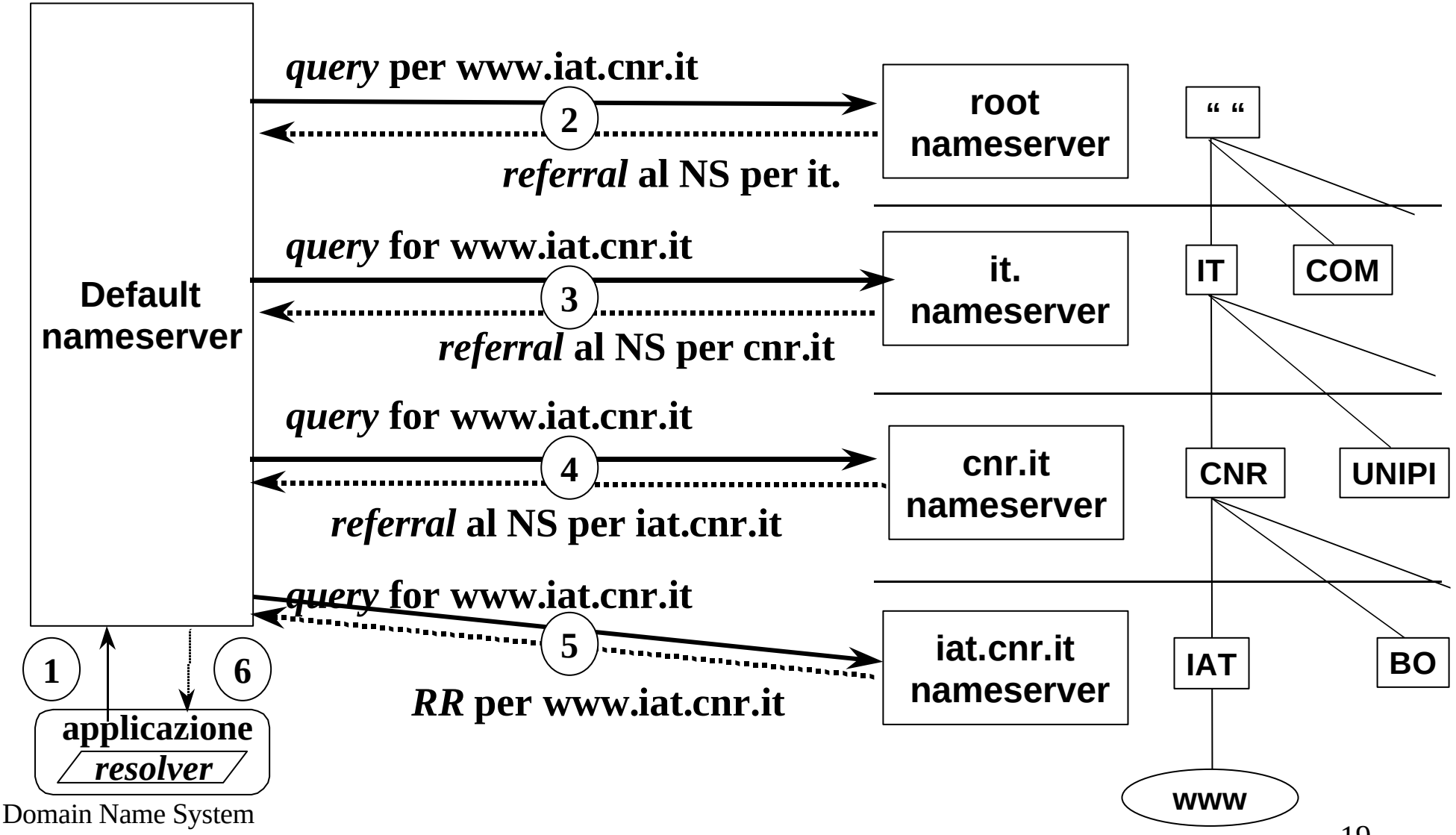
– 69.65.48.146.in-addr.arpa *macchina*

Nameserver e Resolver

- il *nameserver* è un processo che gira su una macchina IP ed è in grado di fornire “risposte autoritative” ad interrogazioni sui nomi a dominio appartenenti ai domini per cui è autoritativo
- ogni programma che utilizza nomi a dominio usa il *resolver* per accedere al nameserver. Le sue funzioni sono:
  - interrogare il nameserver
  - interpretare la risposta (un RR o un errore)
  - restituire l’informazione al programma richiedente
  - tipicamente il resolver è un insieme di routine di libreria: *stub resolver*
  - deve essere configurato (*/etc/resolv.conf* su Unix con BIND) . I fattori configurabili di solito sono:
    - default domain
    - name server



Il processo di risoluzione dei nomi



I root-servers

- i *root-server* sono i nameserver della “ “ (radice).
- sono essenziali al funzionamento del DNS perchè:
  - contengono le informazioni sui Top-Level-Domain e sui relativi nameserver ai quali ne delegano la gestione
  - contengono le informazioni per la risoluzione inversa (risoluzione Indirizzo-nome)
- ogni nameserver deve conoscere nomi ed indirizzi dei root-server
- la lista aggiornata dei root-server è mantenuta da InterNIC
  - ftp://ftp.rs.internic.net/domain/named.root

Nameserver autoritativi

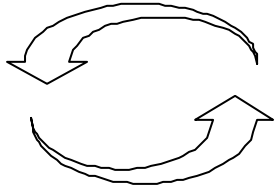
- un nameserver si definisce autoritativo quando è “in possesso dei dati” per una determinata zona dell’albero dei nomi
- per un dominio vi possono essere più nameserver autoritativi
  - per avere una maggiore affidabilità è fortemente consigliato averne più di uno

Nameserver primari e secondari

- un nameserver si definisce primario quando possiede i file delle informazioni (“file di zona”). Per ogni zona ci può essere un solo nameserver primario
- un nameserver si definisce secondario quando acquisisce in maniera automatica (mediante una procedura denominata “zone-transfer”) i dati relativi alla zona.
  - i parametri che regolano il funzionamento della procedura sono contenuti in uno specifico record del nameserver primario
- il nameserver primario ed il/i nameserver secondario/i sono chiamati nameserver autoritativi
- è necessario valutare attentamente il numero e la dislocazione dei nameserver secondari

Caching

- ogni nameserver mantiene traccia 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*)



può dare luogo a “temporanee” inconsistenze

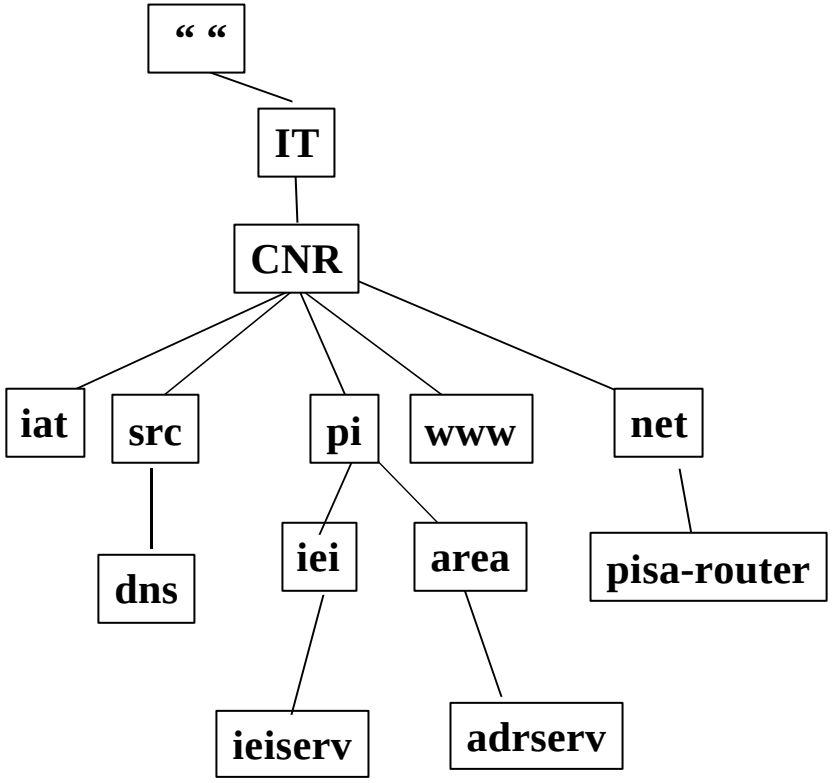
aumenta la performance del sistema

Un esempio: il dominio CNR.IT

- gestito presso l'Istituto IAT di Pisa
- organizzato in sottodomini che riflettono
  - la struttura organizzativa dell'Ente (comitati, direzioni, ecc)
    - cedrc.cnr.it
    - cmt-fis.cnr.it
  - la distribuzione sul territorio
    - pi.cnr.it
    - mlib.cnr.it
  - esigenze particolari di rete
    - net.cnr.it

Il dominio CNR.IT: naming

- è importante rispettare in maniera molto rigorosa lo schema di naming
- è necessario registrare tutti i domini presso la Registration Authority Italiana



Il dominio CNR.IT: alcune raccomandazioni

- tutti i domini devono avere almeno due nameserver
- tutti i domini di terzo livello (es: pi.cnr.it, src.cnr.it, ecc) devono avere come nameserver secondario nameserver.cnr.it
- è consigliato utilizzare come nameserver secondario per la risoluzione inversa delle reti usate dal CNR (non per le subnet delle reti in classe B) nameserver.cnr.it
- è suggerito avere un secondario sul nameserver primario del dominio padre
- è necessario “registrare” il router che assicura l’interconnessione alla dorsale della rete nel dominio net.cnr.it

Configurazione di un nameserver

- le piattaforme hw e sw
- i file necessari
- i tipi di record
- le deleghe dei sottodomini

Le piattaforme hardware e software

- hardware
  - disponibile su quasi tutte le attuali piattaforme (PC, Macintosh, workstation, mainframe)
- software
  - prodotti di pubblico dominio
  - prodotti commerciali
- BIND (Berkeley Internet Domain Name)
  - è l'implementazione di nameserver più diffusa su Internet
  - sviluppata per Unix BSD, ne esistono *porting* per altri ambienti
  - spesso ne è inclusa una implementazione nel software di corredo di piattaforme Unix

http://www.isc.org/bind.html

Le versioni attualmente disponibili

Attualmente sono ancora disponibili due versione di BIND:

- la versione “storica” 4.x.y
  - l’ultima rilasciata è la 4.9.7
- la “nuova” versione 8.x.y
  - l’ultima versione rilasciata è la 8.2.0
  - È quella su cui verranno effettuati gli sviluppi nel futuro
  - È più performante e sicura

Le maggiori differenze tra le due versioni

File di configurazione

- named.boot (4.x.y)
  - formato ormai in uso da anni
  - consente solo alcune “personalizzazioni” generali
- named.conf (8.x.y)
  - nuovo formato (stile linguaggio c)
  - funziona con IPv6
  - consente una personalizzazione completa sia generale che zona per zona

rimangono inalterati i file delle singole zone

Nuove funzionalità della versione 8.x.y

- meccanismo del notify
  - permette l'aggiornamento quasi in tempo reale tra nameserver primario e secondari
- migliore ottimizzazione della memoria centrale
  - migliora notevolmente le prestazioni del servizio, specialmente per implementazioni con molte zone attive sulla stessa macchina
- sicurezza (DNSSEC)

I file necessari

- il file named.boot/named.conf
- il file named.local
- il file named.root
- i file per la risoluzione diretta
- i file per la risoluzione inversa

Alcune regole sintattiche dei “file di zona”

- tutto quello che si trova dopo il carattere “;” è un commento
- il carattere “@” è sinonimo del dominio dichiarato nella istruzione *primary/master* del file named.boot/named.conf
- il carattere “*” è una wildcard
- 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 al nome della macchina quanto dichiarato nella istruzione *primary/master* del file *named.boot/named.conf*

Il file *named.boot*

- il file *named.boot* è il file di configurazione principale per il funzionamento del processo nameserver nella versione 4.x.y
  - definisce la directory in cui si trovano gli altri file necessari al funzionamento del nameserver *(directory)*
  - definisce l'ordine con cui verranno restituiti gli indirizzi delle singole macchine *(sortlist)*
  - definisce quali sono i nameserver che possono prelevare le zone per cui il nameserver è autoritativo *(xfernets)*
  - definisce l'interfaccia locale della macchina su cui il processo nameserver è attivo
  - definisce i domini per i quali il nameserver è autoritativo *(primary e secondary)*
  - definisce i riferimenti ai root nameserver *(cache)*

Attenzione: tutto quello che si trova dopo il carattere ";" è un commento

Il file *named.conf*

- il file *named.conf* è il file di configurazione principale per il funzionamento del processo nameserver nella 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)*
  - definisce il livello e la distribuzione dei "log" prodotti dal processo nameserver senza dover necessariamente il syslog del sistema *(logging/channel/category)*
  - definisce l'interfaccia locale della macchina su cui il processo nameserver è attivo
  - definisce i domini per i quali il nameserver è autoritativo *(master e slave)*
  - definisce i riferimenti ai root nameserver *(hint)*

  Attenzione alla sintassi ….è diversa dalla vecchia versione (/ */, //, # invece di ;)*

Un esempio del file *named.boot*

```
; Boot file for the domain cnr.it on nameserver.cnr.it
; dns-adm@nameserver.cnr.it 960308
;
; directory where all the data files are stored
directory  /usr/local/domain
;
; preferred networks
sortlist  131.114.192.0 131.114.1.0
;
primary          0.0.127.in-addr.arpa                    named.local
primary          cnr.it                                  cnr/soa.cnr-it
primary          pi.cnr.it                               cnr/pisa/soa.pi-cnr-it
primary          48.146.in-addr.arpa                     cnr/soa.pi-cnr-it-lan
secondary        iat.cnr.it                 146.48.65.2  backup/iat-cnr-it
secondary        65.48.146.in-addr-arpa     146.48.65.2  backup/iat-lan
;
; Root Nameservers
cache            .                                       named.root
```

Un esempio di file named.conf (1)

```
options {
        statistics-interval 5;
        allow-transfer {
                194.119.192/24;
                193.0.0/24;
                193.0.1/24;
                193.205.245/24;
                128.84.154.10;
                        };
        datasize 12M;
        coresize 4M;
        directory "/usr/local/dns/data";
        transfer-format many-answers;
        transfers-in 4;
logging {
        channel syslog_errors {
                syslog local0;
                severity info;
        };
channel statistics {
                file "/var/log/named/named-stat";
                print-time yes;
                severity info;
        };
```

Un esempio di file named.conf (2)

```
zone ”cnr.it" in {
        type master;
        file " cnr/soa.cnr-it ";
};
zone " 65.48.146.in-addr.arpa " in {
        type slave;
        file " backup/iat-cnr-it-lan ";
        masters { 146.48.65.3; };
};
zone "." in {
        type hint;
        file "named.root";
};
zone "0.0.127.in-addr.arpa" in {
        type master;
        file ”named.local";
};
```

Il file *named.local*

- il nameserver ha bisogno di questo file per utilizzare il loopback. Per convenzione questa rete è la 127.0.0.0 e l'indirizzo della macchina è il 127.0.0.1

  Un esempio di file named.local:

```
@                       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.
```

Un esempio del file *named.root*

(prima parte del file)

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC registration services
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.RS.INTERNIC.NET
;       -OR- under Gopher at    RS.INTERNIC.NET
;           under menu          InterNIC Registration Services (NSI)
;              submenu          InterNIC Registration Archives
;           file                named.root
;
;       last update:    Aug 22, 1997
;       related version of root zone:   1997082200
;
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
```

Il file per la risoluzione diretta

- il file per la risoluzione diretta contiene i riferimenti necessari all'associazione tra i nomi delle macchine appartenenti ad una zona ed i loro indirizzi IP
- 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
  - MX
  - A
  - CNAME
  - HINFO
  - TXT

Tipi di record - SOA

- 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>            ;Default
                )
```

Tipi di record - SOA esempio

```
@ IN SOA  nameserver  dns-adm.nameserver (
                199503081   ;file Version # yyyymmddv
                86400       ;Refresh = 1 day
                1800        ;Retry = 30 minutes
                608400      ;Expire = 7 days
                86400       ;Default TTL = 1 day
                            )
```

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
@			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 sia per il dominio che per una singola macchina

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			MX	0	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> <ttl> <classe> A <indirizzo IP>

  Esempi:

www.cnr.it.	86400	IN	A	194.119.192.42
www			A	146.48.65.43

Tipi di record - HINFO

- il record HINFO (Host INFOrmation) fornisce le informazioni relative all'hardware (cpu) ed al sistema operativo della macchina a cui è riferito

  La sintassi con cui deve essere scritto è la seguente:

  <host> <ttl> <classe> HINFO <cpu> <sistema operativo>

  Esempi:

  www.cnr.it. 86400 IN HINFO "IBM 9076 SP Power 2" "AIX 4.1"

  HINFO "IBM 9076 SP Power 2" "AIX 4.1"

Tipi di record - TXT

- il record TXT (TeXTual Information) fornisce informazioni testuali (es: dislocazione della macchina, servizi attivi, ecc)

  La sintassi con cui deve essere scritto è la seguente:

  <host> <ttl> <classe> TXT <testo>

  Esempi:

nameserver.cnr.it. 86400	IN	TXT	“Nameserver primario di cnr.it”
	IN	TXT	“Sala Macchine Stanza S08”

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.

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
  - (CNAME)

Tipi di record - PTR

- il record PTR (PoinTeR) definisce la corrispondenza tra l'indirizzo IP della singola macchina ed il suo nome a domini

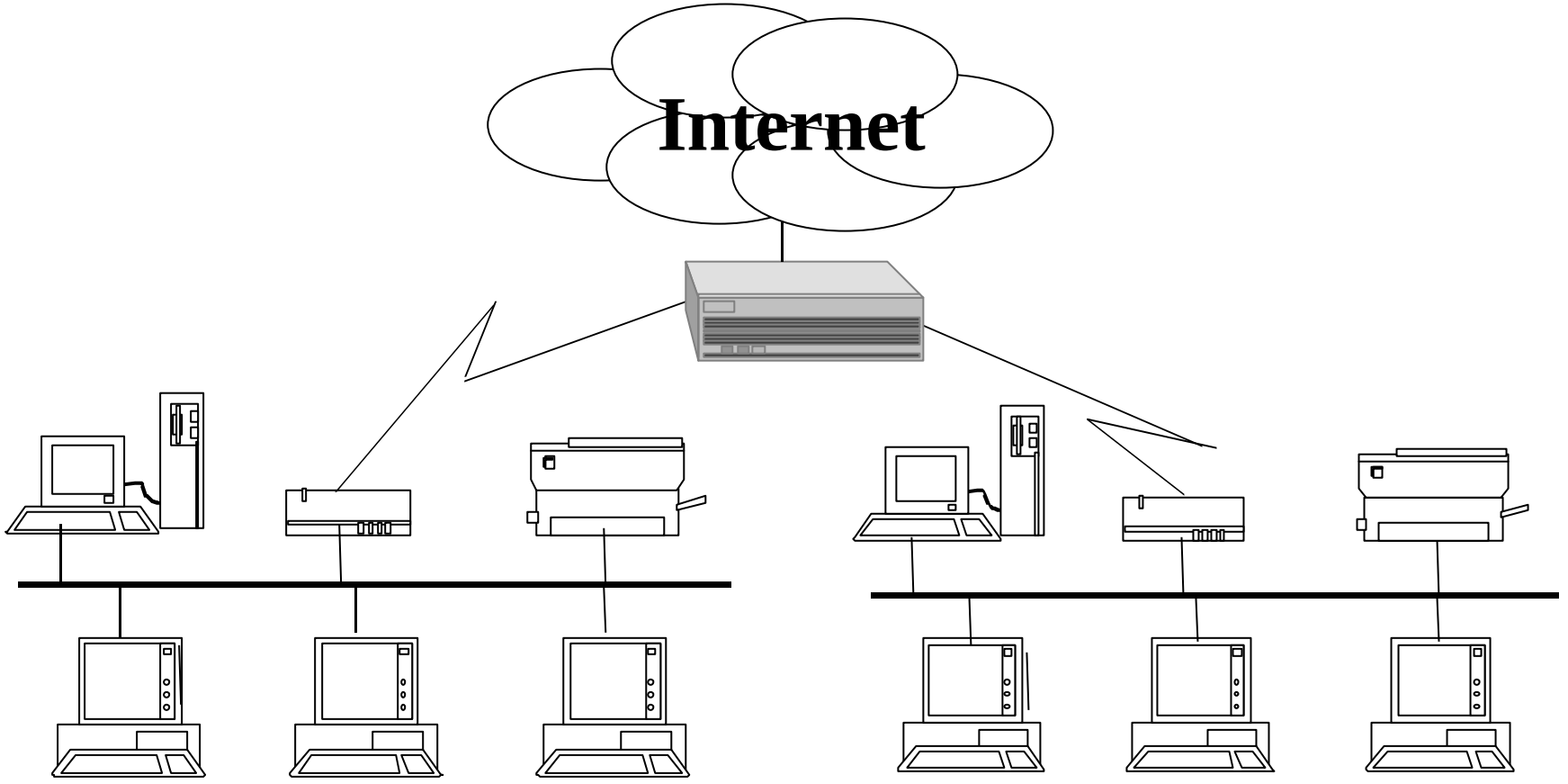
  La sintassi con cui deve essere scritto è la seguente:

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

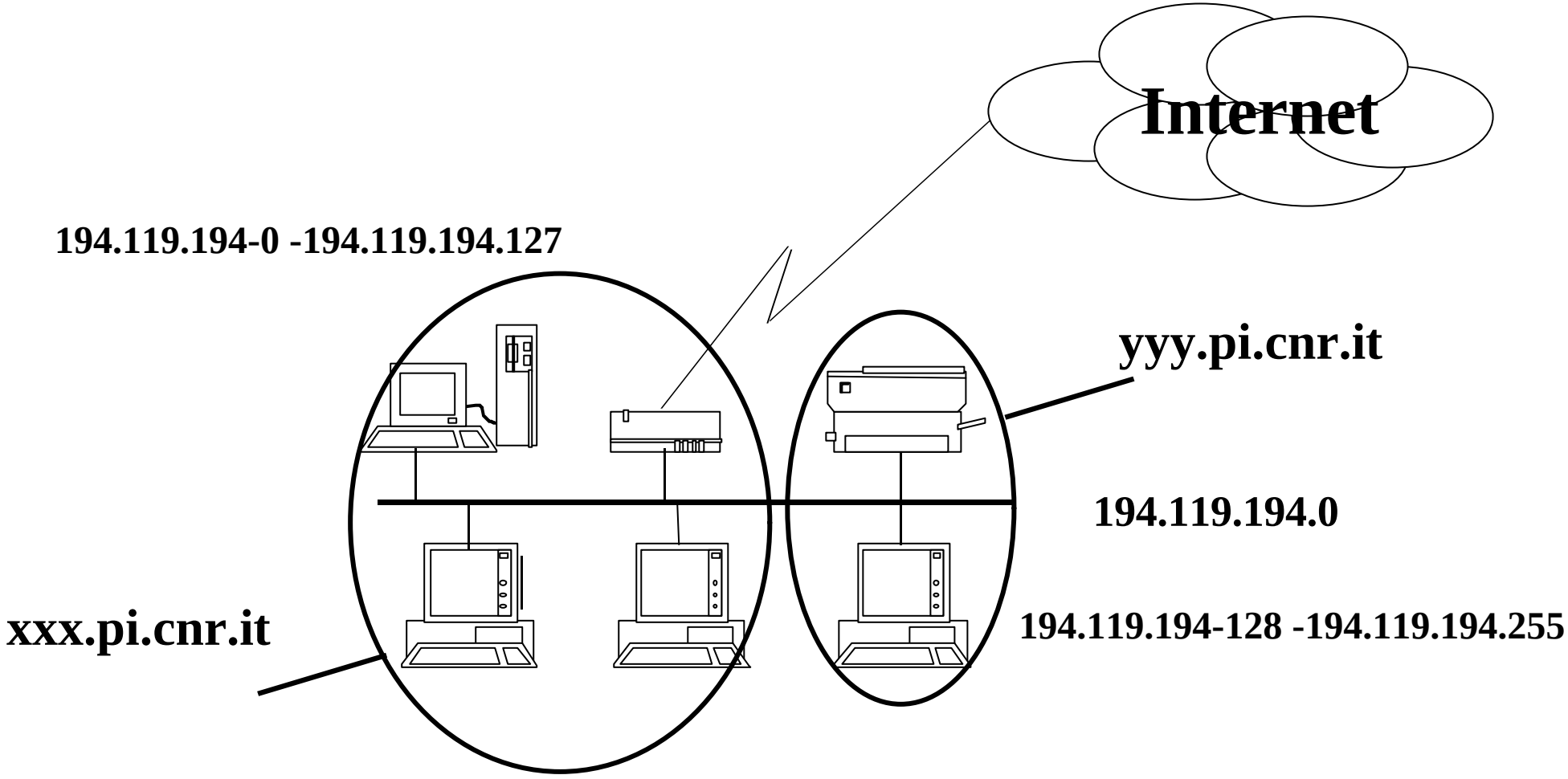
Esempi:

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

Risoluzione inversa: il problema del subnetting



Risoluzione inversa: il problema del subnetting



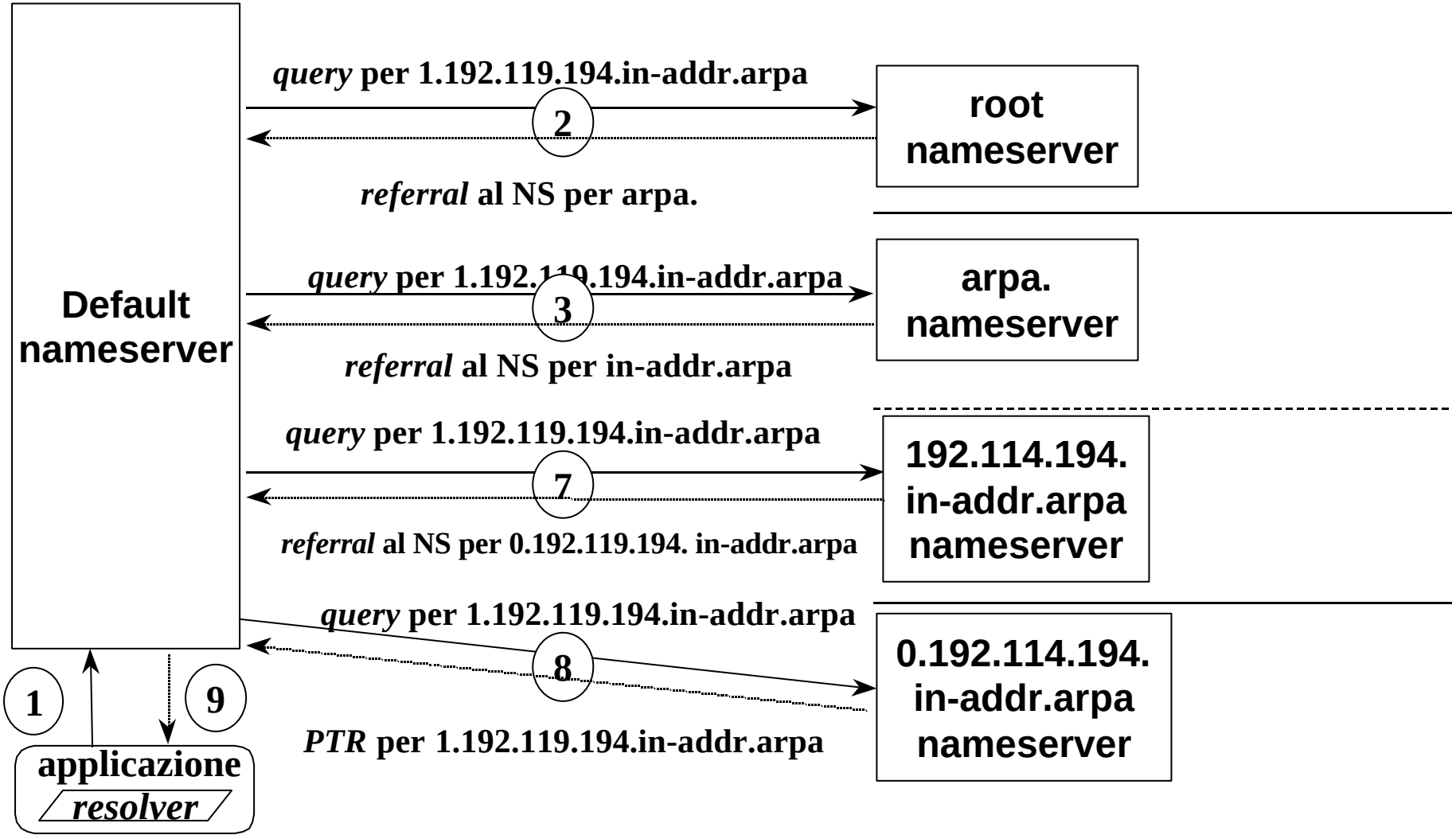
Risoluzione inversa: il problema del subnetting

- è possibile effettuare la delega della risoluzione inversa anche di “parti” di una rete
  - per le reti in classe B si procede normalmente alla delega delle singole subnet equivalenti ciascuna ad una rete in “classe C”
  - per le reti in classe C si può procedere alla delega di “porzioni di indirizzi”
    - ftp://ftp.nic.it/rfc/rfc2317.txt

Risoluzione inversa: il problema del subnetting

- si deve richiedere all'autorità competente la delega della risoluzione inversa dell'intera rete in classe C
- inserire nel file zona autoritativo per l'intera rete dei record CNAME per ogni host
  - i record CNAME devono referenziare dei nomi di host appartenenti a domini diversi corrispondenti alle singole "porzioni" in cui è stata divisa la rete
  - esistono tecniche per rendere più intuitivo il rimando dei record CNAME

Risoluzione inversa: il problema del subnetting



Risoluzione inversa: il problema del subnetting

- un esempio: la rete 194.119.193.0

```
@      IN SOA nameserver.cnr.it. dns-adm.nameserver.cnr.it.      ( ...      )

@     604800 NS nameserver.cnr.it.
@     604800 NS dns.iat.cnr.it.

0     604800 NS nameserver.cnr.it.
0     604800 NS dns.iat.cnr.it.
1      CNAME   1.0.193.119.194.in-addr.arpa.
2      CNAME   2.0.193.119.194.in-addr.arpa.
3      CNAME   3.0.193.119.194.in-addr.arpa.
.......
;
8     604800 NS dns.iat.cnr.it.
8     604800 NS nameserver.cnr.it.
9      CNAME   9.8.193.119.194.in-addr.arpa.
.......
15     CNAME   15.8.193.119.194.in-addr.arpa.
```

Risoluzione inversa: il problema del subnetting

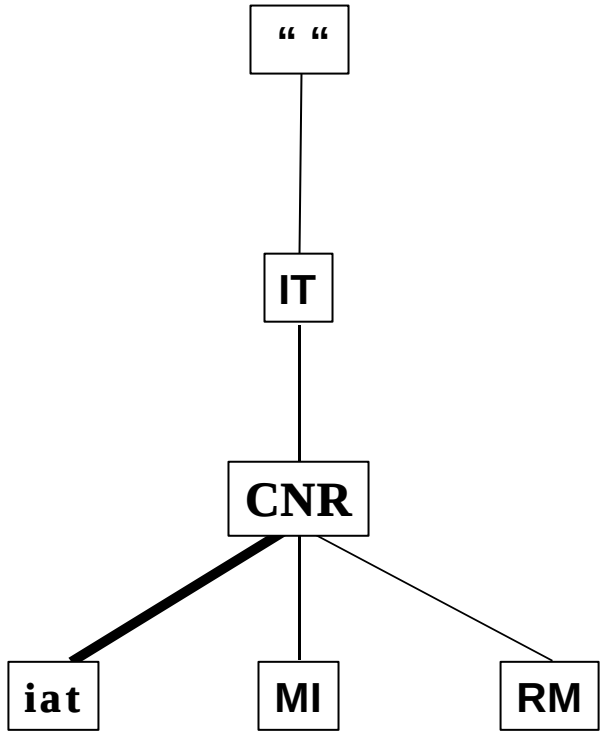
- un esempio: il file zona per la risoluzione inversa della porzione di rete 194.119.193.0-194.119.193.7

```
;;
;;    AUTHORITATIVE DATA FOR:       0.193.119.194.in-addr.arpa
@      IN SOA nameserver.cnr.it. dns-adm.nameserver.cnr.it. (
                199607181  ;FILE VERSION #
                86400   ;REFRESH = 1 DAY
                1800    ;RETRY  = 30 MIN
                604800 ;EXPIRE = 7 DAYS
                86400  ;DEFAULT TTL =  1 DAY
           )
;;
@           604800      NS          nameserver.cnr.it.
@           604800      NS          dns.iat.cnr.it.

1                       PTR         pisa-router.net.cnr.it.
2                       PTR         x-router.net.cnr.it.
3                       PTR         y-router.net.cnr.it.
```

Il meccanismo di delega

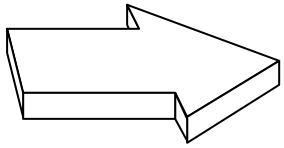
- ogni qualvolta è necessario creare un dominio figlio (es: iat.cnr.it) è necessario inserire le opportune informazioni nel dominio padre (es: cnr.it).
- le deleghe si effettuano normalmente mediante i record NS ed in alcuni casi mediante i record MX



Un esempio di delega

```
;;  AUTHORITATIVE DATA FOR: cnr.it
@     IN        SOA          nameserver  admin.nameserver (
                             199903081     ;file Version # yymmddv
                             86400         ;Refresh = 1 day
                             1800          ;Retry = 30 minutes
                             604800        ;Expire = 7 days
                             86400         ;Default TTL = 1 day
                                                          )
;; NAMESERVERS FOR THIS DOMAIN
@             NS           nameserver.cnr.it.
@             NS           simon.cs.cornell.edu.
@             NS           itgbox.cnuce.cnr.it.
@             NS           ns1.surfnet.nl.
@             NS           dns2.nic.it.

;; Delegation to subdomain
iat           86400        NS           dns,iat.cnr.it.
              86400        NS           nameserver.cnr.it.
              86400        NS           ns1.surfnet.nl.
mi                         NS           nameserver.mi.cnr.it.
                           NS           nameserver.cnr.it.
```



Utility per il controllo e l’interrogazione di un nameserver

- nslookup
- host
- dig

nslookup

- è normalmente distribuita insieme al S.O., o alla distribuzione di BIND
- è una interfaccia interattiva
- dispone di aiuto in linea

```
nslookup
 Default Server: dns.iat.cnr.it
 Address: 146.48.65.3
 >
 > set q=any
 > www.iat.cnr.it
```

host

- è incluso nella distribuzione di BIND, ma una versione più aggiornata è reperibile presso:

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

- non è interattiva; si utilizza da *linea di comando*
- permette di fare interrogazioni complesse ed a qualsiasi nameserver
- è dotata di aiuto in linea

```
host www.iat.cnr.it
host -i 146.48.65.3
host -av cnr.it nameserver.cnr.it
```

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 dotata di aiuto in linea

```
dig -h
dig dns.iat.cnr.it
dig -x 146.48.65.3
dig @nameserver.cnr.it cnr.it
```

Interazioni tra DNS e posta elettronica

- *record* MX e *record* A
- rapporti tra *record* del DNS e MTA SMTP

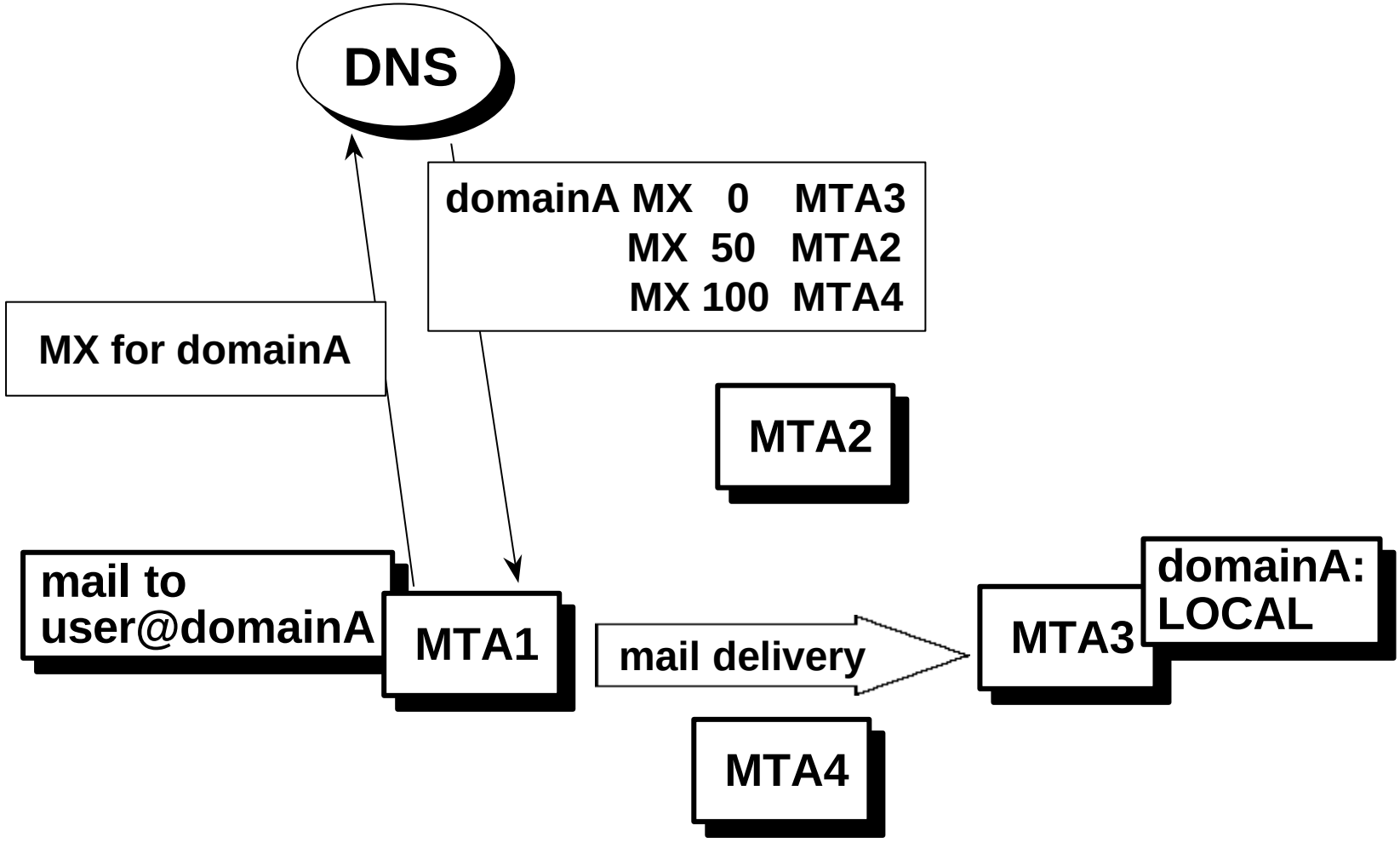
La posta su Internet relazione tra SMTP e DNS: RFC974

- l'instradamento della posta su Internet si basa sulle interazioni tra mailer (MTA) SMTP e DNS
- per ogni destinatario di un messaggio il mailer SMTP chiede al DNS la lista di RR di tipo *MX* per il nome a dominio specificato nella parte globale
- i record MX costituiscono una lista ordinata, secondo la preferenza, di *mailer* (MTA) per il dominio (host) destinazione

Mail Routing & DNS

- algoritmo di un mailer SMTP per destinazione REMOTA:
  - lista mailers vuota:
    - ripete l'interrogazione per record A e tenta la consegna all'host remoto
  - lista mailers non vuota*:*
    - se la lista contiene il mailer stesso
      - scarta se stesso ed ogni mailer con *preference* minore o uguale a se stesso (preference con valore numerico maggiore o uguale) - *loop prevention*
      - se la lista risultasse vuota: ERROR
    - tenta la consegna ai mailers della lista, partendo dal *preference* maggiore (numericamente minore).

Mail routing & DNS: esempio



Alcuni consigli pratici (1)

- aggiornare ogni volta che si modifica un file zona il campo serial del relativo record SOA
- il campo <host> del record SOA deve riportare una macchina a cui corrisponde un record A
- il campo <nameserver-host> del record NS deve riportare una macchina a cui corrisponde un record A
- la parte destra di un record MX (parte dati) deve sempre riportare una macchina a cui corrisponde un record A
  - non usare alias - CNAME
  - non costruire catene di record MX
- utilizzare dei record CNAME, ove possibile al posto dei record A, per definire le macchine su cui sono attivi servizi come www, ftp, smtp, pop, imap, ecc

Alcuni consigli pratici (2)

- utilizzare per la gestione del processo nameserver l'apposito "tools" (ndc) distribuito insieme al BIND
- analizzare con attenzione i file di log prodotti dal nameserver per identificare eventuali errori
- rispettare rigorosamente la sintassi nei singoli files
- utilizzare "tools" per il controllo della correttezza delle zone