

Lezione 11 – Livello Applicativo bind (DNS)

Claudio Ardagna, Patrizio Tufarolo – Università degli Studi di Milano

Insegnamento di Laboratorio di Reti di Calcolatori



Terminologia - 1

- ▶ ISO/OSI (Open System Interconnection)
 - ▶ Standard de iure che organizza l'architettura di una rete di calcolatori in una struttura composta da 7 livelli (stack di rete)
- ▶ Livello di rete
 - ▶ Livello dello stack ISO/OSI che permette di interconnettere reti eterogenee. Riceve dei *segmenti* dal soprastante livello di trasporto e produce dei *pacchetti* che verranno passati al livello datalink, sottostante
- ▶ Livello di trasporto
 - ▶ Livello dello stack ISO/OSI che permette il trasporto di informazioni in unità chiamate *segmenti*. Il suo compito è quello di fornire un **meccanismo di trasporto delle informazioni affidabile**, per il corretto funzionamento del livello di sessione
 - ▶ TCP
 - **Transmission Control Protocol** (RFC 793) – Protocollo multiplex, **con garanzia di consegna, orientato alla connessione**, full-duplex e con **controllo di flusso** e dell'errore.
 - ▶ UDP
 - **User Datagram Protocol** (RFC 768) – Protocollo a livello di trasporto, multiplex, **senza garanzia di consegna**, con controllo dell'errore

Terminologia - 2

- ▶ Multiplexing (multiplazione)
 - ▶ Meccanismo che permette di condividere lo **stesso mezzo di comunicazione** su **più canali trasmissivi**, con la stessa capacità disponibile in uscita.
Il multiplexing è utilizzato a **livello fisico per permettere allo stesso mezzo fisico di trasmettere più flussi di informazione** combinando in modo opportuno segnali digitali o analogici.
Nell'ambito dei protocolli a livello di trasporto (TCP e UDP) è ottenuto tramite il meccanismo **INDIRIZZO_IP:PORTA**.
I protocolli TCP e UDP prevedono un massimo di $2^{16}-1=65535$ porte
- ▶ Livello applicativo
 - ▶ Livello 7 dello Stack ISO/OSI, all'interno del quale sono collocate applicazioni e servizi di rete

Terminologia - 3

▶ DNS

- ▶ Domain Name System – **sistema dei nomi a dominio**, utilizzato per permettere la **risoluzione dei nomi degli host** nei **corrispondenti indirizzi IP** (e viceversa)

▶ Dominio

- ▶ **Insieme di host appartenenti a una rete**, amministrati all'interno di una data unità organizzativa e con **metodologie e procedure comuni** a tutti gli host, ognuno dei quali ha uno specifico ruolo

▶ Zona

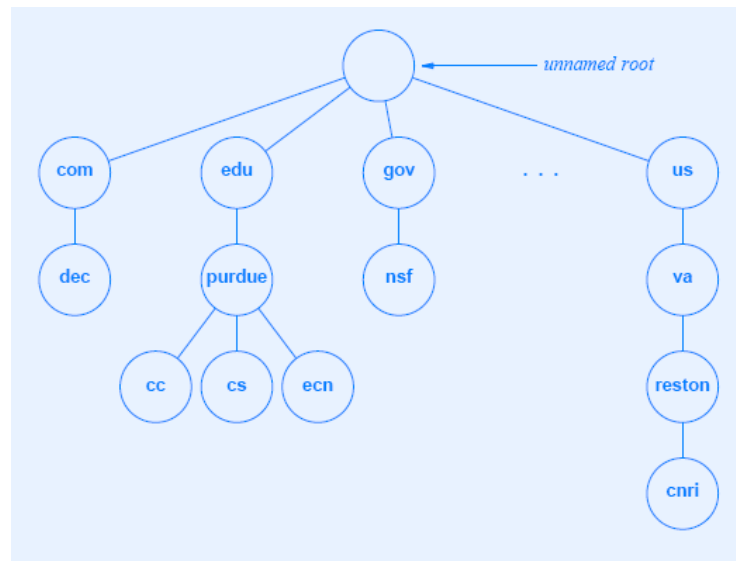
- ▶ Parte dello spazio dei nomi, **costituita da un dominio e da i suoi sottodomini non delegati**
- ▶ Ciascuna zona **può essere replicata su più server**, per motivi di ridondanza

DNS - 1

- ▶ Protocollo che **consente di assegnare un nome**, costituito da una stringa, a un host, effettuando un **mapping tra il nome e l'indirizzo IP** (RFC 1035)
- ▶ Opera sulla porta UDP 53
- ▶ Consente di definire uno *spazio dei nomi* (namespace)

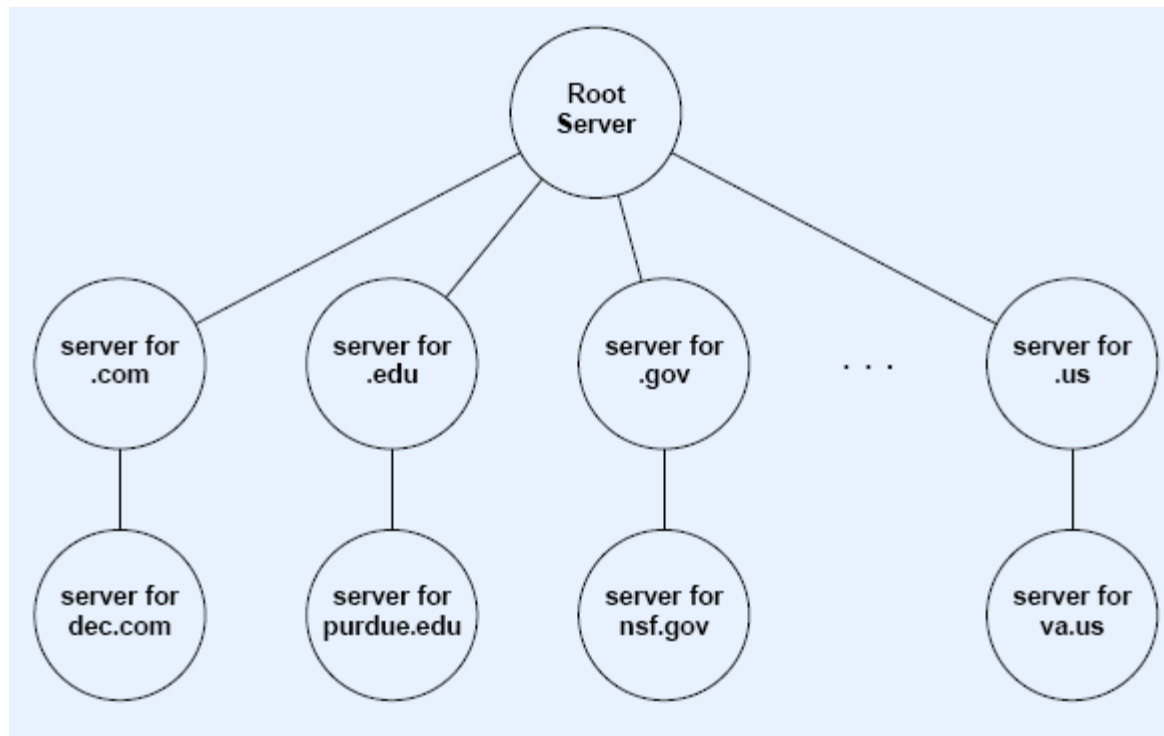
DNS - 2

- ▶ È organizzato secondo una gerarchia di *zone*, tipicamente mappate su *domini*
- ▶ Ogni associazione nome indirizzo è caratterizzata da un *record*



DNS - 3

- ▶ Ogni server DNS può delegare la gestione di una zona ad un altro server DNS



DNS - Tipi di record

- ▶ SOA
 - ▶ **Start of Authority** – record costituito da campi multipli che specifica la parte di gerarchia gestita dal server DNS corrente
- ▶ A / AAAA
 - ▶ Associa un nome a un indirizzo IPv4 (A) o IPv6 (AAAA)
- ▶ CNAME
 - ▶ **Canonical Name** – crea un alias per un nome già risolvibile
- ▶ MX
 - ▶ **Mail eXchanger** – specifica il mailserver associato al dominio
- ▶ NS
 - ▶ **NameServer** – specifica il nameserver autoritativo per una certa zona
- ▶ PTR
 - ▶ **Pointer** – Record di risoluzione inversa

Risoluzione dei nomi su Linux

- ▶ **Tipicamente gestita attraverso il file `/etc/nsswitch.conf`**
 - ▶ Questo file gestisce **l'ordine di priorità** per i meccanismi di gestione di vari aspetti del sistema operativo
 - ▶ La direttiva che riguarda la gestione della risoluzione dei nomi è la direttiva *hosts*. Tipicamente è configurata nel seguente modo:
 - ▶ `hosts: files dns myhostname`
 - ▶ Questo vuol dire che il primo elemento ad essere utilizzato per la risoluzione dei nomi è il file `/etc/hosts`. Dopodiché verrà considerato il server DNS configurato nel sistema, e infine l'hostname del sistema stesso
 - ▶ Per specificare un server DNS su un sistema Linux, occorre modificare il file **`/etc/resolv.conf`**, il file di configurazione della libreria C **`resolv.h`**
 - ▶ Questo file ha diverse opzioni di configurazione. Quella corrispondente al server dns è *nameserver*.
 - ▶ Es: `echo nameserver 8.8.8.8 > /etc/resolv.conf` imposta il DNS di Google
 - ▶ **Le altre opzioni possono essere ottenute consultando la manpage** (`man resolv.conf`)

DNS su Linux: BIND

- ▶ Il demone DNS per Linux più noto è Bind.
- ▶ Bind è preinstallato in IMUNES
- ▶ Permette di definire i **record DNS su un database**, che può essere un LDAP, un database SQL, o più semplicemente un file di testo
- ▶ Il formato testuale originariamente usato solo da Bind, è ora utilizzato in molti altri server DNS (es. PowerDNS)
- ▶ Implementa anche le **funzionalità di sicurezza (DNSSEC)**

Anatomia di un file di zona per BIND - 1

- ▶ Un file di zona è costituito da una sequenza di *resource records*
- ▶ Ogni *resource record* ha i seguenti campi:
 - ▶ **Nome:** nome del record – può essere lasciato in bianco, in tal caso viene utilizzato il nome del record precedente
 - ▶ **TTL:** time to Live – specifica la durata della validità del record nella cache del client DNS
 - ▶ **Classe:** spazio dei nomi utilizzato. Tipicamente vale IN (Internet), ma non è l'unico valore accettato (es. CHAOS per CHAOSNet)
 - ▶ **Tipo:** tipo di record (SOA, A, AAAA, CNAME, MX, etc.)
 - ▶ **Dati:** contenuto del record
- ▶ Un **resource record può occupare anche più linee**, nel caso i dati siano multi-parametrici (es. record SOA). In tal caso le linee sono racchiuse tra parentesi tonde

Anatomia di un file di zona per BIND - 2

- ▶ I **Resource Record** possono apparire in qualunque ordine all'interno del file di zona, a meno di convenzioni.
- ▶ Il file di zona:
 - ▶ può contenere linee vuote e commenti (preceduti da ;)
 - ▶ avere anche delle direttive, che hanno \$ come prefisso.
 - ▶ La direttiva **\$ORIGIN** specifica il **punto di partenza della gerarchia DNS**. Se mancante è automaticamente dedotta dal server DNS.
- ▶ Ogni **Resource Record finisce con un punto**. Se il punto non viene messo, al resource record viene **automaticamente appesa il valore della direttiva \$ORIGIN**.
- ▶ Un file di zona minimale deve contenere quantomeno **un record SOA e un record NS**

Esempio di un file di zona per BIND - 1

```
$ORIGIN ripe.net.
```

```
$TTL 1d
```

```
ripe.net. IN SOA ns.ripe.net. sesar.ripe.net.
```

```
(
```

```
2001061501; Serial number del file di zona
```

```
43200 ; Refresh 12 hours
```

```
14400 ; Retry 4 hours
```

```
345600 ; Expire 4 days
```

```
7200 ; TTL Negative cache 2 hours
```

```
) ; fine SOA
```



Esempio di un file di zona per BIND – 2

; server DNS autoritativi per la zona (RR NS)

ripe.net.	7200	IN	NS	ns.ripe.net. ; DNS primario
ripe.net.	7200	IN	NS	ns.eu.net. ; DNS secondario

; mail server (RR MX)

ripe.net.	9000	IN	MX	10 mx1.sesar.net. ; 1
mailserver				
ripe.net.	9000	IN	MX	50 mx2.sesar.net. ; 2
mailserver				

; host (RR A)

ripe.net.	7200	IN	A	193.0.1.16
ns.ripe.net.	7200	IN	A	193.0.1.33
pinkie	3600	IN	A	193.0.1.162

; alias (RR CNAME)

www	7200	IN	CNAME	ripe.net.
ftp	3600	IN	CNAME	ripe.net.



Configurare e avviare Bind

- ▶ Il file di zona **deve essere referenziato in un file di configurazione**, tipicamente memorizzato nella directory `/etc/bind`
- ▶ Noi useremo il file `/etc/bind/named.conf.local`
- ▶ Il file di configurazione contiene una **definizione espressa in questo modo:**

```
zone "<nomezona>" {  
    type <tipo>;  
    file "/var/named/db.nomezona";  
};
```

- ▶ Un'istanza di questo file può essere ad esempio la seguente:

```
zone "example.com" {  
    type master;  
    file "/etc/bind/db.example.com";  
};
```

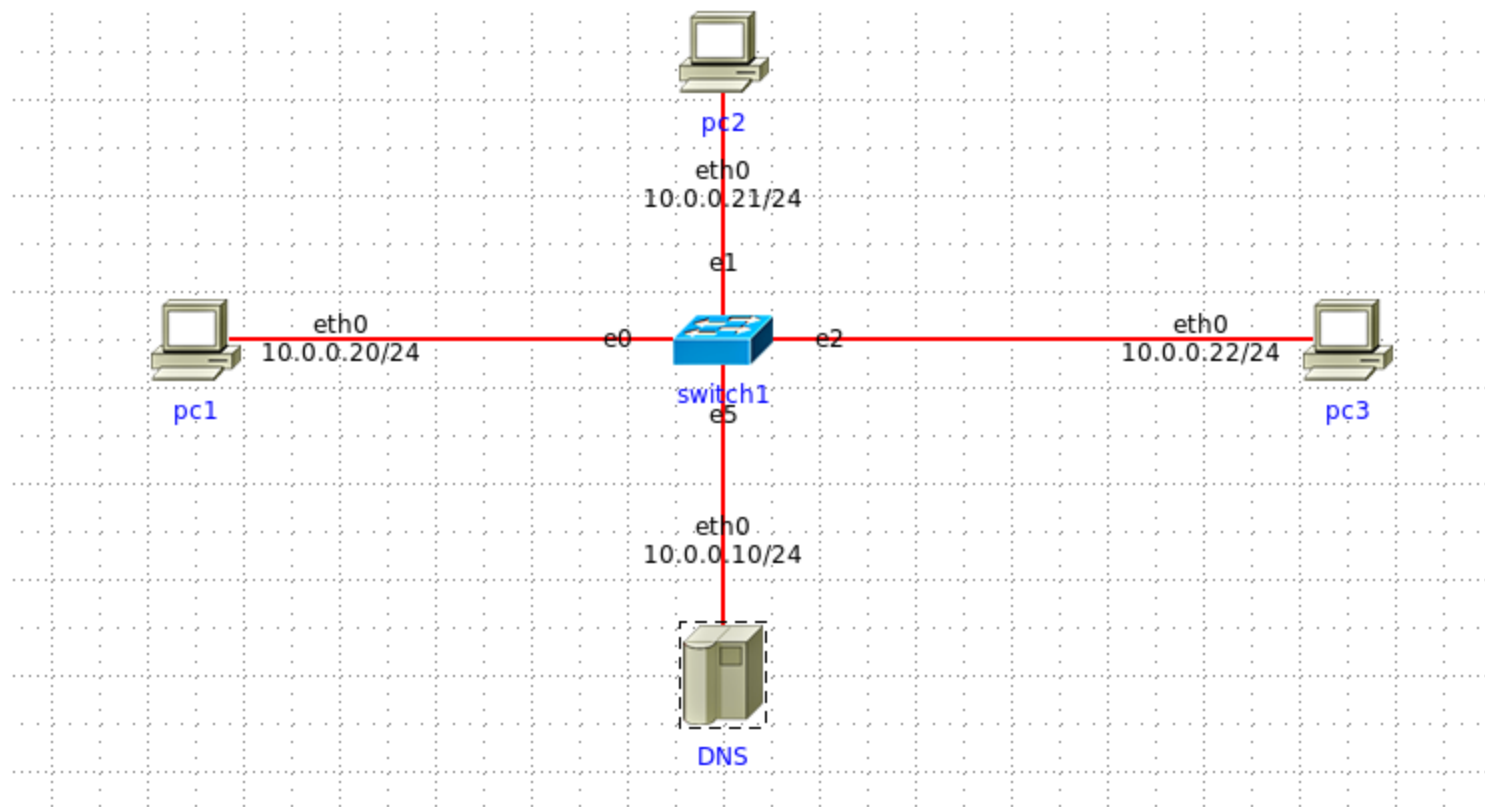
- ▶ Il demone Bind può essere avviato con il comando `named`
- ▶ Prima di avviarlo è buona norma fare una **verifica della sintassi con il comando `named-checkconf`** per prevenire errori
- ▶ Il nome di zona «.» è un wildcard, e indica «tutte le zone»

Esercizio 1

- ▶ Creare una rete con topologia a stella, composta da uno switch, tre pc, e un server DNS
- ▶ Configurare il server DNS in modo che risolva i nomi degli host per i tre pc (pc1, pc2, pc3), appartenenti alla zona example.com
- ▶ Avviare il demone DNS con il comando `named`
- ▶ Impostare il server DNS per la risoluzione dei nomi su tutti i pc
- ▶ Verificare il funzionamento del server DNS mediante i tool `nslookup` o `dig`
 - ▶ Sintassi:
 - ▶ `dig <indirizzo>`
 - ▶ `nslookup <indirizzo>`

Esercizio 1 - Soluzione

Topologia IMUNES



Esercizio 1 - Soluzione

Contenuto di /etc/bind/named.conf.local

```
zone "example.com" {  
    type master;  
    file "/etc/bind/db.example.com";  
};
```

Contenuto del file di zona /etc/bind/db.example.com

```
$ORIGIN example.com.  
$TTL 1h  
example.com. IN SOA ns.example.com admin.example.com. ( 1 43200 1440 345600 7200 )  
example.com. IN NS ns.example.com.  
ns.example.com. IN A 10.0.0.10  
pc1 IN A 10.0.0.20  
pc2 IN A 10.0.0.21  
pc3 IN A 10.0.0.22
```



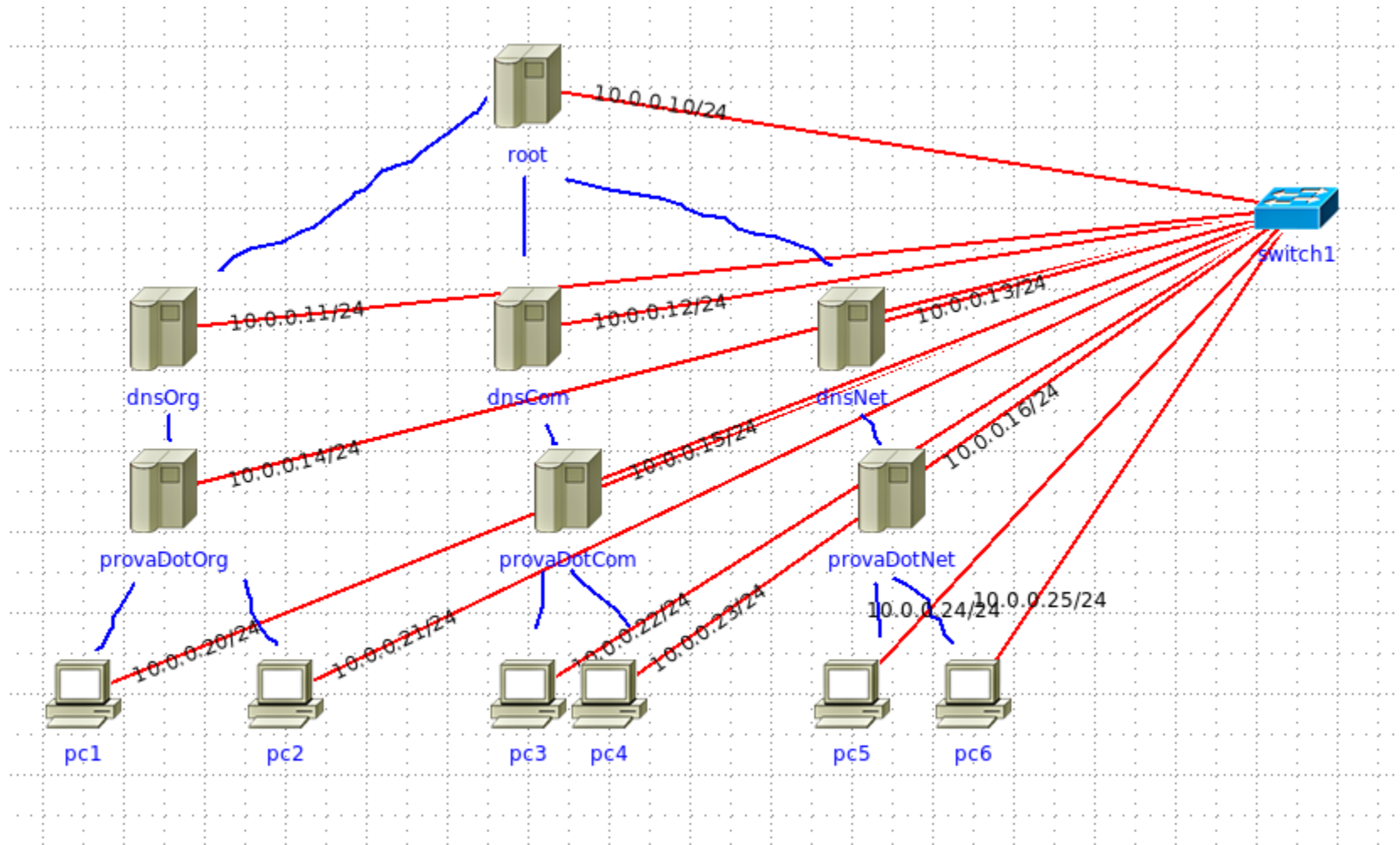
Nameserver: Delega di sottozone

- ▶ La delega di sottozone può essere effettuata specificando tramite il record NS un altro server autoritativo per una determinata sottozona
- ▶ In questo modo la risoluzione dei nomi viene effettuata in modo ricorsivo

Esercizio 2

- ▶ Riprodurre il funzionamento di un server DNS su internet su IMUNES creando una topologia a stella composta da uno switch, sette server DNS e sei PC.
- ▶ Configurare tutti gli host in modo da avere:
 - ▶ Un server DNS radice che delega ognuna delle seguenti zone
 - ▶ Org
 - ▶ Com
 - ▶ Neta ciascuno degli altri server dns.
 - ▶ Per ogni zona definire una sottozona di secondo livello sul relativo server DNS (andando a costituire un sottodominio ad es. prova.org, prova.net, prova.com)
 - ▶ Ogni sottodominio ha un proprio server DNS, che referencia due PC (per ogni sottodominio), di cui vanno configurati i record A in modo opportuno

Esercizio 2 - Soluzione



Esercizio 2 – Soluzione – Server radice

► Root server:

► /etc/bind/named.conf.local

```
zone "." {  
    type master;  
    file "/etc/bind/db.rootdns";  
}
```

► /etc/bind/db.rootdns

\$TTL 60000

@	IN	SOA	root.	root.root (1 28800 14400 36000000 0)
@	IN	NS	root.	
root.	IN	A		10.0.0.10
com.	IN	NS	dns.com.	
dns.com.	IN	A		10.0.0.12
org.	IN	NS	dns.org.	
dns.org.	IN	A		10.0.0.11
net.	IN	NS	dns.net.	
dns.net.	IN	A		10.0.0.13



Esercizio 2 – Soluzione – Server com

► Com server:

► /etc/bind/named.conf.local

```
zone "com" {  
    type master;  
    file "/etc/bind/db.com";  
}
```

► /etc/bind/db.com

```
$TTL 60000
```

```
@ IN SOA dns.com. root.dns.com (1 28800 14400 36000000 0)
```

```
@ IN NS dns.com.
```

```
dns.com. IN A 10.0.0.12
```

```
prova.com. IN NS dns.prova.com.
```

```
dns.prova.com. IN A 10.0.0.15
```

...analogamente per gli altri server



Esercizio 2 – Soluzione – Server prova.com

► Prova.com server:

► /etc/bind/named.conf.local

```
zone "prova.com" {  
    type master;  
    file "/etc/bind/db.prova.com";  
}
```

► /etc/bind/db.prova.com

```
$ORIGIN prova.com.  
$TTL 60000  
@ IN      SOA      dns.prova.com.    root.prova.com (1 28800 14400  
36000000 0)  
@ IN      NS       dns.prova.com.  
dns.prova.com. IN  A       10.0.0.15  
  
pc3       IN      A       10.0.0.22  
pc4       IN      A       10.0.0.23
```

...analogamente per gli altri server



Conclusioni

- ▶ Abbiamo ripassato il protocollo DNS
- ▶ Abbiamo imparato a scrivere un file di zona
- ▶ Abbiamo configurato il protocollo DNS con Bind

