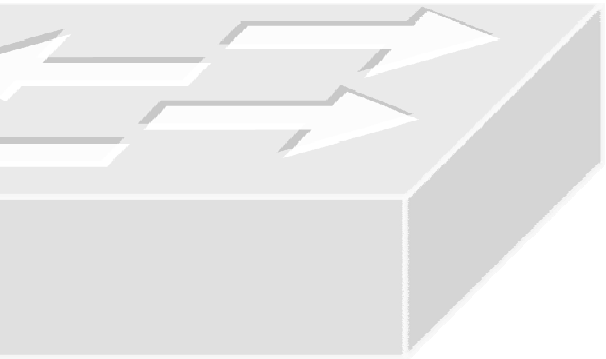
Reţele Locale de Calculatoare

DNS



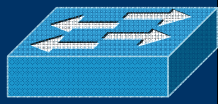
– curs 7 –

16.11.2009

18.11.2009

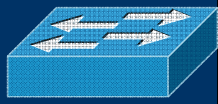
Universitatea POLITEHNICA Bucureşti

... dns



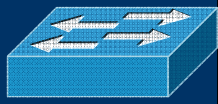
You know it's love when you memorize her IP address to skip DNS overhead.

Domain Name System



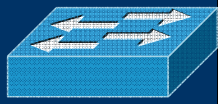
- Serviciul de nume (DNS) permite identificarea tuturor nodurilor din Internet printr-o adresa de nume
- De ce folosim rezolvarea de nume?
  1. mult mai intuitiva
  2. este independenta de alocarea adreselor IP
- Exista doua tipuri de rezolvari de nume:
  - rezolvarea directa (forward lookup) - determina adresa IP asociata unui nume
  - rezolvarea inversa (reverse lookup) - determina adresa de nume asociata unei adrese IP
- DNS este folosit si in rutarea serviciului de email:
  - acesta functie este realizata prin precizarea intrarilor MX (mail exchanger)
  - pentru un domeniu se pot preciza mai multe intrari MX

Istoric



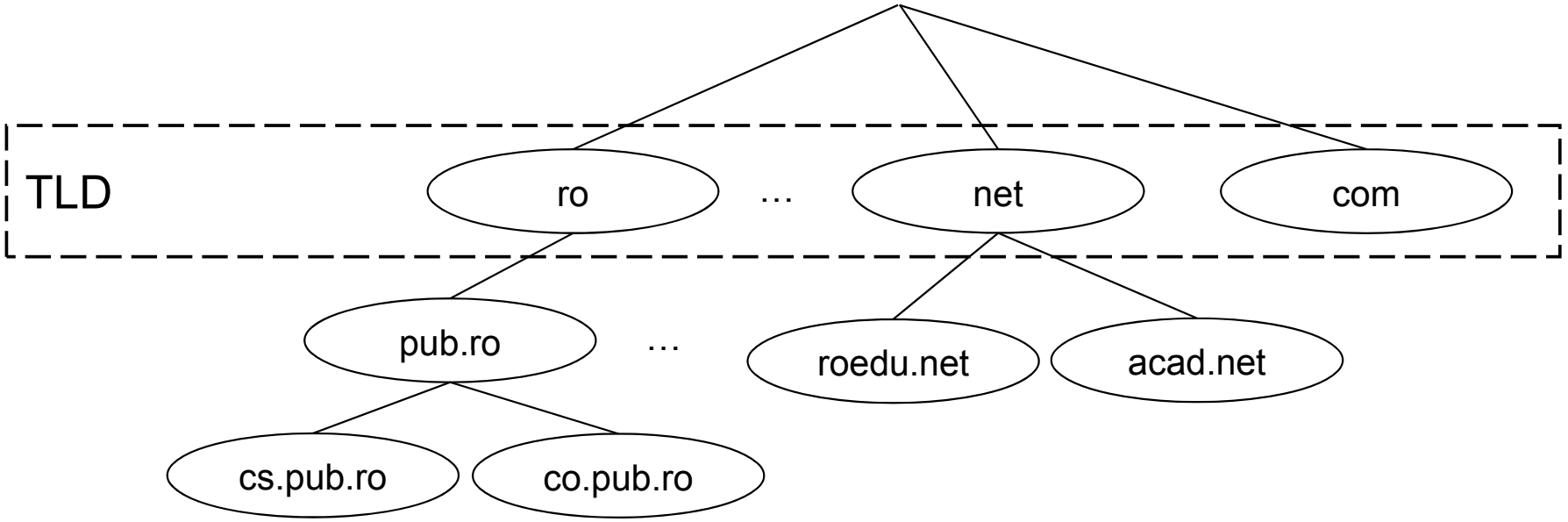
- Incă din anii ’70 a apărut ideea de a folosi o adresa de nume în loc de adresa de reţea
- Prima soluţie presupune definirea statică a asocierilor. In sistemele Unix aceasta se face în fişierul: `/etc/hosts`
- Odată cu dezvoltarea reţelelor a început să se folosească un server central, iar toate staţiile din reţea trebuiau să descarce fişierul de asocieri de pe acest server
  - Soluţia s-a dovedit mult prea puţin scalabila, slab convergentă
- In anii ’80, IETF a standardizat DNS, o soluţie de bază de date distribuită, care răspundea problemelor de scalabilitate, dar nu şi celor de convergenţă
- Standarde ulterioare au adresat probleme de securitate şi de convergenţă
- Cu toate acestea, convergenţa DNS este unul dintre cele mai lente procese din Internet

Adresa de nume



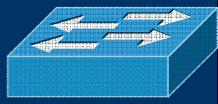
- Numele de domenii sunt separate prin puncte
  - Fiecare element poate avea maxim 63 de caractere, iar lungimea totala a adresei este de maxim 255 de caractre
  - numele sunt limitate la caractere alfanumerice (a-z, A-Z, 0-9) şi caracterul '-'
- Adresa de nume are o structrură ierarhica
  - Spre deosebire de adresa IP cel mai semnificativ element al unei adrese de nume se afla la dreapta acesteia
  - primul element dintr-o adresa de nume (cel mai din dreapta) se numeste TLD (Top Level Domain)
- Specificarea unei adrese de nume poate fi:
  - relativa. O statie din domeniul cs.pub.ro, daca face o cerere DNS pentru curs, va obtine adresa serverului curs.cs.pub.ro
  - absoluta. O astfel de adresa este denumita si FQSN (fully-qualified domain name) si este de forma: mail.yahoo.com.

Domenii



- Un domeniu este un sub-arbore al spatiului ierarhic de nume
- O zona este o parte a unui domeniu gestionat de un server
- Unele subdomenii pot fi delegate in zone separate
- O zona poate include toate subdomeniile unui domeniu dat, sau poate delega autoritatea pentru o parte dintre acestea altor zone

Functionarea DNS

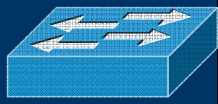


- Rezolvarea de nume se bazează pe implementarea unei aplicaţii client-server
- Componenta client rulează integrat la nivelul sistemului de operare
- Serverul de DNS va avea drept responsabilitate să raspundă la cererile despre staţiile aflate în autoritatea sa (zona sa).
- Aceasta implentare are 2 mari neajunsuri:
  - latenţa mare a procesului iterativ de rezolvare a unei cereri DNS de către serverul autoritar
  - complexitatea comunicaţiei dintre client si serverul autoritar

O cerere de rezolvare de nume va fi tratata astfel:

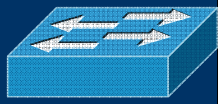
- Clientul va trimite cererea unui server DNS
- Cererea este rezolvată local dacă adresa se află sau nu în domeniul sau de autoritate
- Altfel, se va încerca rezolvarea cererii pe baza informaţiilor din memoria cache
- Daca nu exista intrare în memoria cache, se iniţiază procesul de interogare iterativa. Odată primit răspunsul este actualizată şi memoria cache

Tipuri de servere DNS



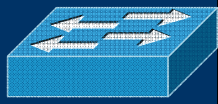
- Master/slave
  - Existența unui backup în caz că masterul nu poate fi contactat
- Caching-only
  - servere ce sunt autoritare doar pe domeniul 0.0.0.127-in.addr.arpa
  - De ce ar fi nevoie de un server caching-only?
    - reduce traficul de DNS, dar creşte timpul de convergenţă
- Servere rădăcină
  - Servere ce administrează TLD-uri
  - Câte TLD-uri există în prezent?
- Servere forwader
  - Răspund la cereri recursive sau nerecursive?
  - Sunt caching-only sau pot fi si servere DNS autoritare pe un domeniu?

Rezolvarea cererilor de DNS



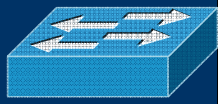
- Se pot formula doua tipuri de cereri:
  - **recursive**: trebuie neaparat rezolvata
    - aplicatiile client vor genera cereri recursive
  - **nerecursiva**: va întoarce un răspuns pozitiv doar dacă serverul interogat are intrarea în *cache* sau este autoritar pentru cerere. Altfel, serverul de nume interogat va răspunde cu un mesaj specificând faptul că răspunsul nu este cunoscut şi indicând un alt server de nume.
- Cautarea in cache se va face pornind de la cel mai specific domeniu al cererii
  - ex: pentru cererea A.B.C, va fi cautata in memorie asocierea pentru A.B.C, daca nu este gasita va fi cautata B.C si in final cea pentru C.
- In cazul esecului cautari in memorie:
  - pentru o cerere va fi indicat unul dintre serverele radacina
  - pentru o cerere recursiva va fi generata o cerere nerecursiva catre serverul de forwarding. Daca acesta nu exista catre un server radacina.
- Un *server de forwarding* se foloseşte pentru înregistrările pentru care serverul DNS nu este autoritar, şi doar dacă răspunsul nu se găseşte în cache.

Exemplu



1. Staţia lemon.cs.pub.ro trimite o cerere recursivă serverului cs.pub.ro în care se doreşte aflarea adresei asociate numelui www.linux.org;
2. Serverul va începe prin a analiza dacă adresa face parte din domeniul pe care îl gestionează; în acest caz nu face parte, aşa că va trece la următorul pas;
3. Serverul verifică dacă nu cumva numele este prezent în *cache*; presupunem că numele nu este prezent în *cache*; în acest caz se trece la pasul următor;
4. Dacă serverul are configurat un server de *forwarding*, atunci el va trimite o cerere nerecursivă serverului de *forwarding*; în caz contrar va trimite o cerere nerecursivă unuia din serverele rădăcină; în cazul de faţă considerăm că avem configurat ca server de *forwarding* serverul ns.pub.ro;
5. Cererea ajunge la serverul ns.pub.ro care va căuta în *cache* numele; presupunem că serverul nu va găsi în *cache* numele: atunci el va întoarce un răspuns negativ, specificând ca *hint root* serverul B.root-servers.net;
6. Serverul cs.pub.ro va trimite cererea la serverul rădăcină; acesta va caută intrarea în *cache* dar nu o va găsi, astfel că va trimite un răspuns negativ iar ca *hint* serverul de nume asociat domeniului org, să spunem ns1.org;
7. Serverul cs.pub.ro trimite atunci cererea serverului ns1.org; acesta va căuta intrarea în *cache* şi presupunem că nu o va găsi; va trimite deci un răspuns negativ, iar ca *hint* serverul asociat domeniului linux.org, să spunem ns.linux.org;
8. Serverul cs.pub.ro trimite atunci cererea serverului ns.linux.org; acesta, fiind serverul autoritar pentru zona linux.org va căuta adresa www.linux.org în baza de date, şi va întoarce un răspuns pozitiv şi autoritar cu adresa asociată;
9. Serverul cs.pub.ro întoarce răspunsul staţiei lemon.cs.pub.ro şi îl introduce în *cache.*

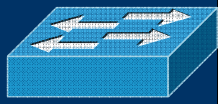
Master / slave



- fiecare domeniu trebuie sa aiba o zona de master pentru a putea genera raspunsuri autoritare pe domeniul gestionat

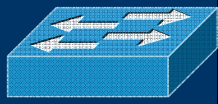
- cand un server de nume slave porneste va incerca sa contacteze serverul master pentru a obtine o copie a bazei de date de nume
- o zona de tip slave va trebui sa aiba precizat explicit zona master

Tipuri de inregistrari



- Cele mai frecvente inregistrari sunt:
  - **A** – identifică înregistrări de tip adresă, fiind folosite pentru rezolvarea directă a numelui.
  - **PTR** – identifică înregistrări de tip *pointer* şi sunt folosite pentru rezolvarea inversa.
  - **NS** – înregistrările de tip server de nume (*name server*). Sunt folosite pentru a identifica serverul de nume asociat cu un domeniu
  - **MX** – înregistrările de tip server de mail (*mail exchager*). Sunt folosite pentru a identifica serverul sau serverele de mail asociate cu un domeniu
  - **SOA** (*start of authority*) – specifică diverşi parametri pentru domeniul indicat în cheie (seria bazei de date, intervalul de timp la care serverul *slave* verifică seria, etc.).
  - **CNAME** – identifică o înregistrare de tip alias,
  - **TXT** – identifică o înregistrare de tip descriere

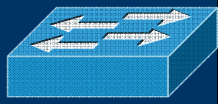
Bind



- Berkley Internet Name Domain
- este distributia cea mai folosita de DNS
- din 1995 pana in 2000 s-a folosit BIND v8
- din 2000 se foloseste BIND v9
  - imbunatatiri in domeniul securitatii
  - suport pentru IPv6

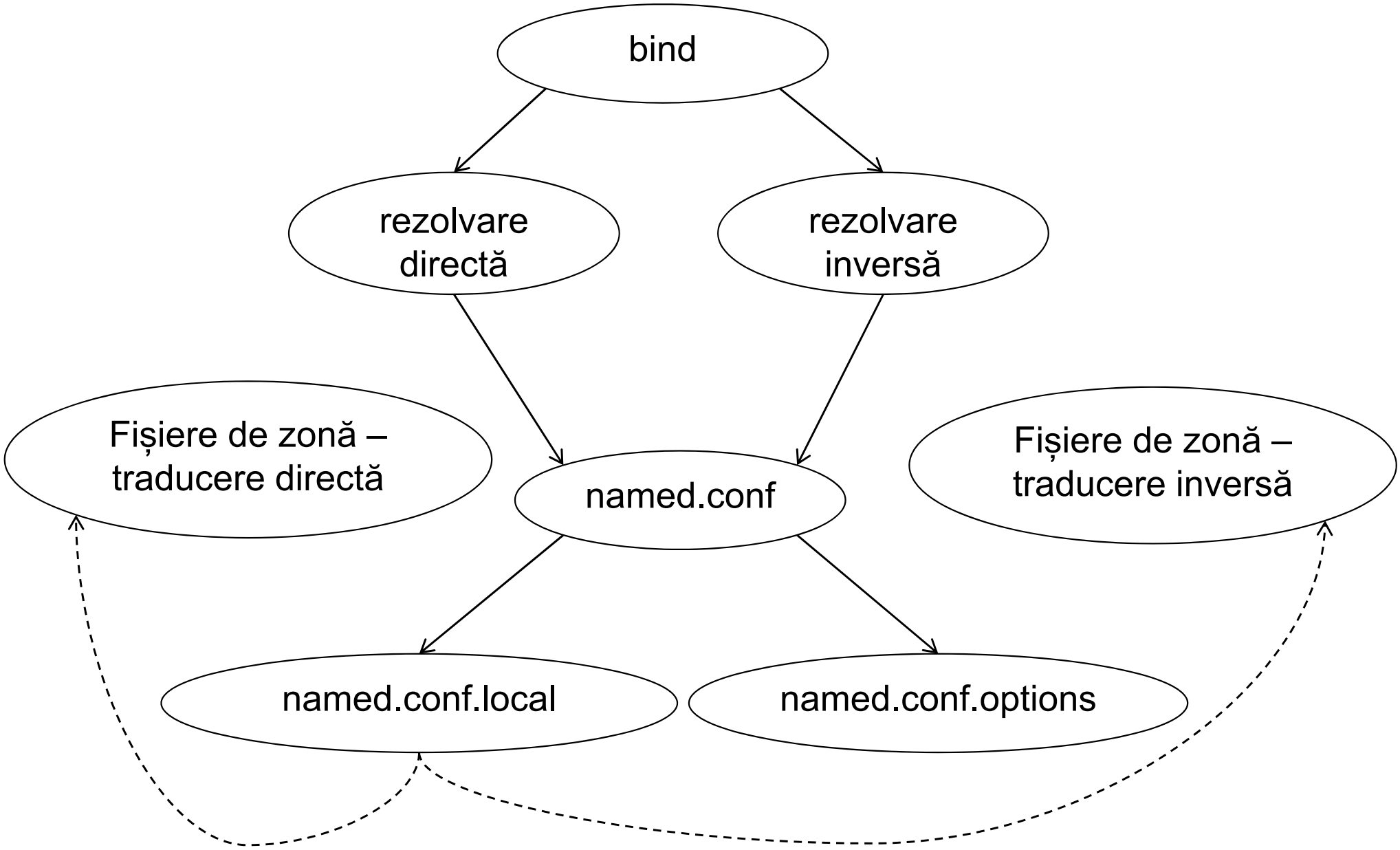
- **www.isc.org/products/BIND**

Sumar bind

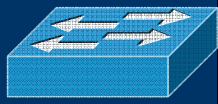


- Tip de configurare: System V
- Pachete: **`bind, bind-utils, bind-chroot`**
- Daemons: **`named, rndc`**
- Script: named
- Porturi: 53 (domain), 953 (rndc)
- Fisiere de configurare:
  - /etc/named.conf
  - /var/etc/*
  - /etc/rndc
- Alte pachete: **`caching-nameserver, openssl`**

Structura bind



named.conf

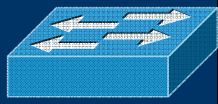


```
include "/etc/bind/named.conf.options";

zone ".”{
        type hint;
        file "root.hints”;
};
zone "localhost”{
        type master;
        file "/etc/bind/db.local”;
};

include "/etc/bind/named.conf.local”;
```

```
options{
     directory "/var/named/db”;
     forwarders { 192.129.4.1; };
     allow-query { 141.85.37.0/24; };
};
```

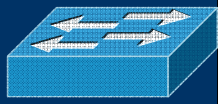
```
zone "cs.pub.ro”{
        type master;
        file "cs.pub.ro.db”;
};
zone "37.85.141.in-addr.arpa”{
        type master;
        file "141.85.37.db”;
};
```

Fișierul de zonă



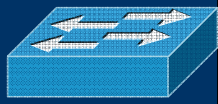
```
;cs.pub.ro.db
$ORIGIN pub.ro.
cs          IN      SOA     ns.cs.pub.ro. nsmaster.cs.pub.ro. (
                            2004101001          ; Serial
                            8H                  ; Refresh
                            2H                  ; Retry
                            1W                  ; Expire
                            1D                  ; TTL
                            )

                    TXT     "Computer Science Departament"
                    NS      ns.cs
                    NS      ns
$ORIGIN cs.pub.ro.
                    MX      5       mail
                    MX      10      mail.pub.ro.
ns                  CNAME   csrouter
csrouter            A       141.85.37.1             ; ruter
mail                A       141.85.37.3             ; serv mail
```

Fişierul de zonă reverse



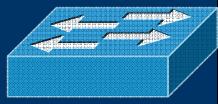
```
;141.85.37.db
$ORIGIN 85.141.in-addr.arpa.
37      IN      SOA     ns.cs.pub.ro. nsmaster.cs.pub.ro. (
                        2004101001      ; Serial
                        8H              ; Refresh
                        2H              ; Retry
                        1W              ; Expire
                        1D              ; TTL
                        )
                TXT     "Computer Science Departament"
                NS      ns.cs.pub.ro.
                NS      ns.pub.ro.
$ORIGIN 37.85.141.in-addr.arpa.
1               PTR     csrouter.cs.pub.ro.
2               PTR     catc.cs.pub.ro.
```

Nu uitaţi:



- O greşeală frecventă atunci când se editează fişierele de configuraţie pentru zone este scrierea incorectă a numelor complete, prin uitarea aplicării punctului la sfârşitul numelui.
- Sintaxa fişierelor de configuraţie trebuie respectată cu exactitate. Una dintre cele mai frecvente greşeli de sintaxă este omiterea separatorului “;”.
- Seria bazei de date trebuie incrementată la fiecare modificare făcută în domeniu, altfel modificările nu se vor propaga.
- Chiar dacă timpul de viaţă se defineşte la serverele autoritare, el se foloseşte doar în serverele neautoritare, când acestea introduc răspunsul în cache.

Verificarea configuratiilor



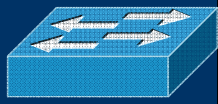
- named-checkconf

```
la:/etc/bind# named-checkconf
/etc/bind/named.conf:20: missing ';' before 'zone'
la:/etc/bind# named-checkconf
la:/etc/bind# named-checkconf named.conf
```

- named-checkzone

```
la:/etc/bind# named-checkzone la.cs.pub.ro db.la.cs.pub.ro
dns_rdata_fromtext: db.la.cs.pub.ro:14: near 'la.cs.pub.ro.': not a valid number
zone la.cs.pub.ro/IN: loading master file db.la.cs.pub.ro: not a valid number
la:/etc/bind# named-checkzone la.cs.pub.ro db.la.cs.pub.ro
zone la.cs.pub.ro/IN: loaded serial 2006091901
OK
```

host – DNS lookup utility



- Lookup

```
$ host cs.pub.ro
cs.pub.ro has address 141.85.37.5
```

- Reverse lookup

```
$ host 141.85.37.5
5.37.85.141.in-addr.arpa domain name pointer
   cursuri.cs.pub.ro.
```

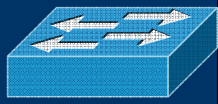
- Interogare specifica a unui server

```
$ host cs.pub.ro 141.85.37.11
Using domain server:
Name: 141.85.37.11
Address: 141.85.37.11#53
Aliases:

cs.pub.ro has address 141.85.37.5
```

- Interogare a unor campuri specifice

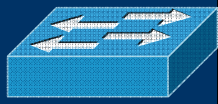
```
$ host -t NS cs.pub.ro
cs.pub.ro name server ns.cs.pub.ro.
cs.pub.ro name server pub.pub.ro.
$ host -t MX cs.pub.ro
cs.pub.ro mail is handled by 5 mail.cs.pub.ro.
```

zona



```
@ IN SOA ns1.testgroup.ro. hostmaster.testgroup.ro.  (
                          2006113002 ;serial
                          28800      ;refresh
                          5000       ;retry
                          1309500    ;expire
                          6000       ;negative ttl
                          )
                          IN NS    ns1.testgroup.ro.
                          IN NS    ns2.testgroup.ro.
                          IN MX   10 mail1.testgroup.ro.
                          IN MX   20 mail.testgroup.ro.
                          IN A    87.123.1.137

@ORIGIN testgroup.ro.
ns1                A        87.123.1.137
ns2                A        86.80.111.98
www                A        194.105.1.138
mail1              A        86.80.111.98
mail               A        194.105.1.139

; Aliases
mx                IN       CNAME    @

testgroup.ro. IN TXT "v=spf1 a mx ptr mx:mail.testgroup.ro ~all" ;inregistrare spf
```

reverse



```
@ORIGIN 123.87.in-addr.arpa.
1 IN SOA ns1.testgroup.ro. hostmaster.testgroup.ro.  (
                          2006113002        ;serial
                          28800             ;refresh
                          5000              ;retry
                          1309500           ;expire
                          6000              ;ttl
                          )
                          TXT "Zona de test reverse dns"
                          NS ns1


@ORIGIN 1.123.87.in-addr.arpa.

137                PTR       ns1.testgroup.ro.
138                PTR       www.testgroup.ro.
139                PTR       mail.testgroup.ro.
```

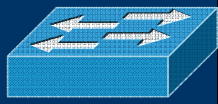
Configurarea listelor de access

```
acl inside_network {
        192.168.2.0/24;
        192.168.1.0/24;
        };
acl slaves {
        192.168.2.1;
        192.168.1.1;
        };

options {
allow-query { inside_network; }; // permit pentru cereri recursive
allow-transfer { slaves; }; // permit pentru transfer la serverele
   slave
};
```

Master (optiuni)

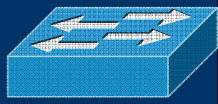
```
# /etc/namedb/named.conf - for base system's BIND 8 or 9
# /usr/local/etc/named.conf - for default install of BIND 8 or 9

options {
    directory "/etc/namedb";     //locatia unde se afla fisierele pentru zone
    dacă acestea nu sunt specificate prin cale absolută
    listen-on {87.123.1.137; }; //adresa ip pe care asculta serverul
    recursion yes;               // pentru cereri recursive
    allow-transfer { 192.168.1.1; }; // permite transferul de fisiere de zona
    doar catre serverul cu adresa 192.168.1.1
    };

logging{                         //pentru a specifica modul de logare a erorilor
  channel example_log{
    file "/var/log/named/example.log" versions 3 size 2m;
    severity info;
    print-severity yes;
    print-time yes;
    print-category yes;
 };
 category default{ example_log; };
};
```

Master (definirea de zone)



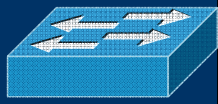
```
zone "." {                  ;zona necesara pentru queri-uri recursive
        type hint;
        file "named.root";
        };

zone "0.0.127.IN-ADDR.ARPA" {
        type master;
        file "localhost.rev";
        };

zone "1.123.87.in-addr.arpa" {          //definirea zonei pentru reverse
        type master;
        also-notify {86.80.111.98;};
        file "1.123.87.in-addr.arpa.map";
        allow-transfer {86.80.111.98;);
        };

zone "testgroup.ro" {                   //definirea zonei pentru care raspunde
serverul
        type master;
        also-notify {86.80.111.98;}; // sa notifice si dns-ul slave de
                                     // modificarile facute - pentru propagare rapida
        file "test.map";
        allow-transfer {86.80.111.98;);  // se permite transferul doar la
                                         // serverele slave
    };
```

Slave (optiuni)



```
# /etc/namedb/named.conf - for base system's BIND 8 or 9
# /usr/local/etc/named.conf - for default install of BIND 8 or 9

options {
    directory "/etc/namedb";  //locatia unde se afla fisierele pentru zone
    listen-on {86.80.111.98; }; //adresa ip pe care asculta serverul
    version "not currently available"; //in caz ca incearca cineva sa scaneze
    serverul
    recursion yes;                  // permite cereri recursive
    allow-query {86.80.111.0/24;}; //nu permite cereri decat din clasa
    86.80.111.0/24
    };

logging{                          //pentru a specifica modul de logare a erorilor
  channel example_log{
    file "/var/log/named/example.log" versions 3 size 2m;
    severity info;
    print-severity yes;
    print-time yes;
    print-category yes;
 };
category default{ example_log; };
};
```

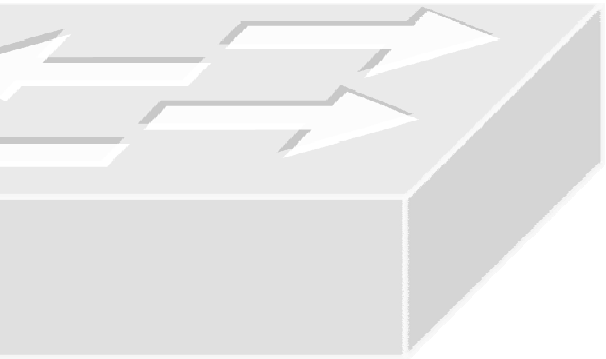
Slave (definirea de zone)



```
zone "." {                  ;zona necesara pentru queri-uri recursive
    type hint;
    file "named.root";
    };


zone "0.0.127.IN-ADDR.ARPA" {
    type master;
    file "localhost.rev";
    };

zone "1.123.87.in-addr.arpa" {          //definirea zonei pentru reverse
    type slave;
    file "1.123.87.in-addr.arpa.map";
    masters {87.123.1.137;};
    };

zone "testgroup.ro" {                   //definirea zonei pentru care
    raspunde serverul
    type slave;
    file "test.map";
    masters {87.123.1.137;};            // se specifica server-ul master
    };
```

Reţele Locale de Calculatoare

DHCP



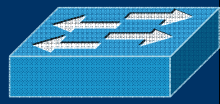
– curs 7 –

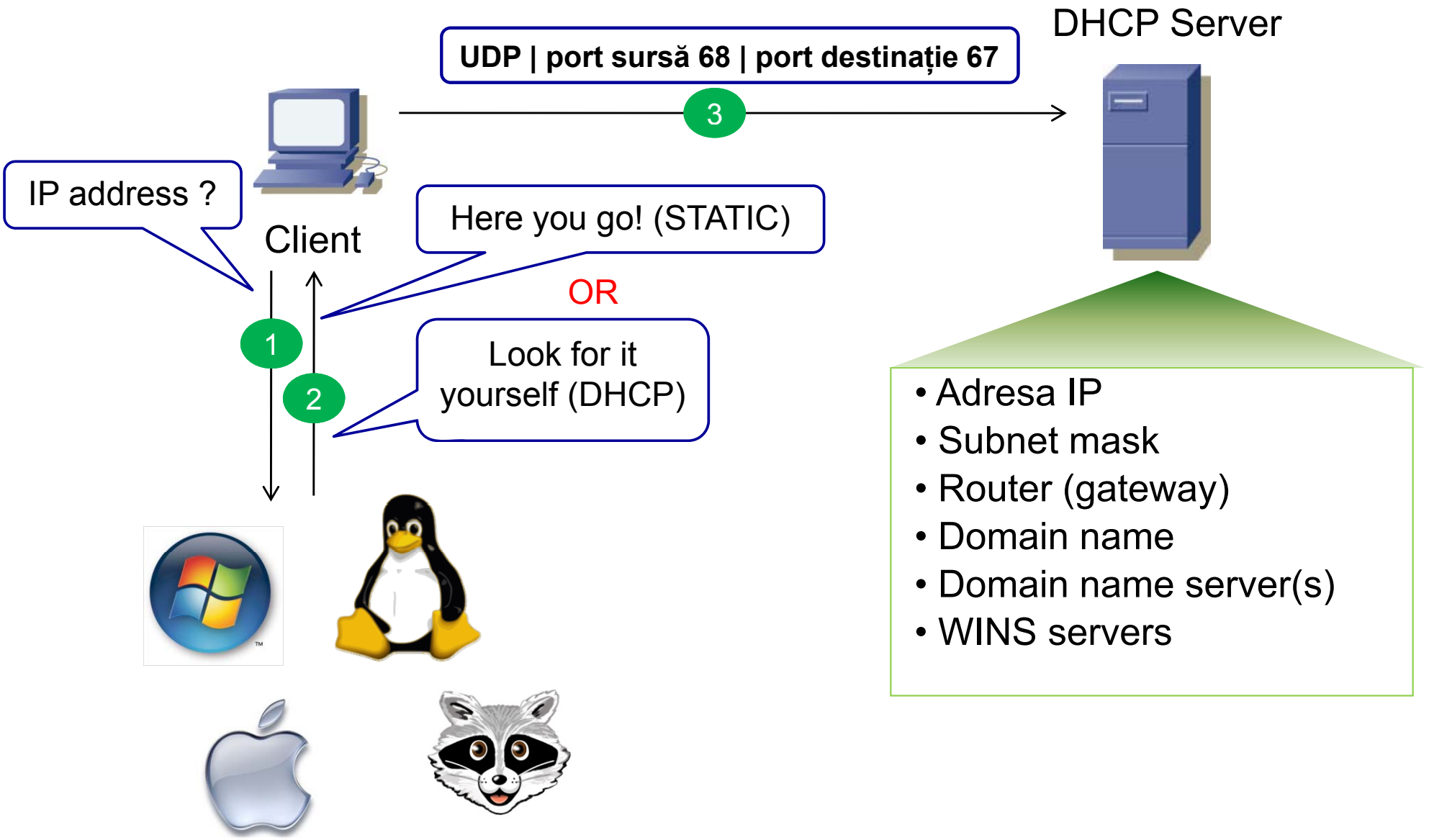
16.11.2009

18.11.2009

Universitatea POLITEHNICA Bucureşti

DHCP

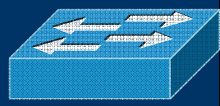


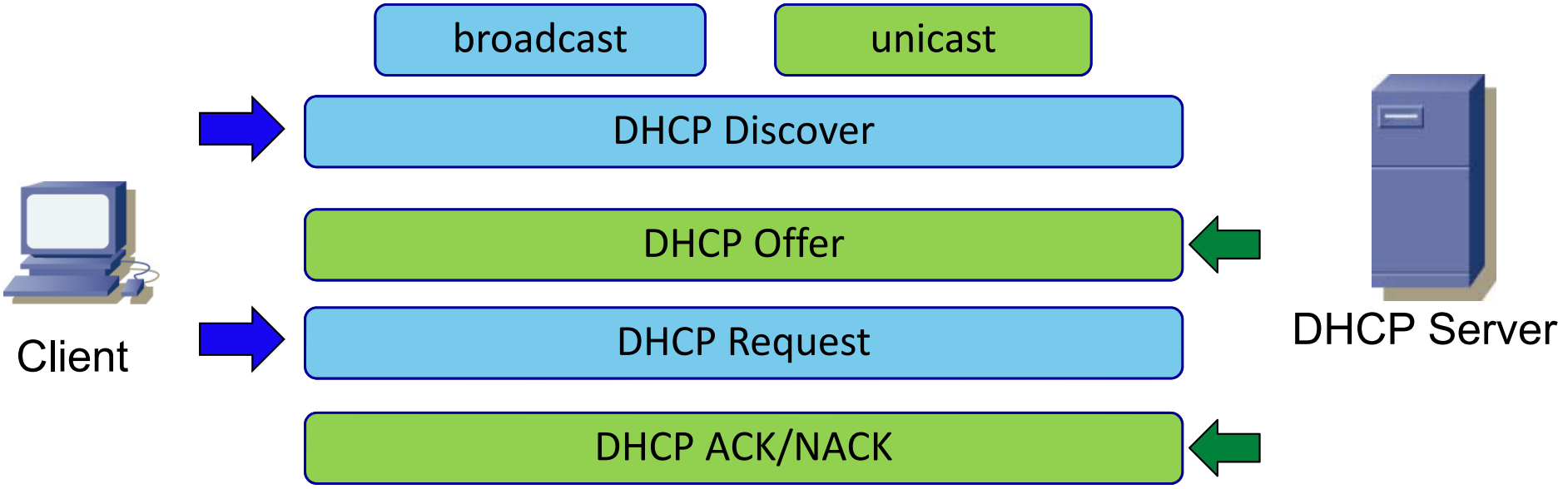

DHCP Server
UDP | port sursă 68 | port destinație 67
3
IP address ?
Client
Here you go! (STATIC)
OR
1
2
Look for it yourself (DHCP)
• Adresa IP
• Subnet mask
• Router (gateway)
• Domain name
• Domain name server(s)
• WINS servers

Istoric

BootP	DHCP
Mapare statica (dupa MAC)	Mapare dinamica
Asignare permanenta	Lease (“inchiriere” a adresei)
4 parametri de configurare	Peste 30 de parametri

Funcționare





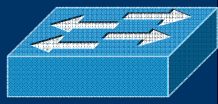
Give me an IP !!
68 | 67
0.0.0.0 | 255.255.255.255
Client_MAC | ff:ff:ff:ff:ff:ff

Here you go: 192.168.1.108
67 | 68
IP server | 255.255.255.255
Server_MAC | Client_MAC

I have chosen: 192.168.1.108 from server 192.168.1.1
68 | 67
0.0.0.0 | 255.255.255.255
Server_MAC | ff:ff:ff:ff:ff:ff

Great :-D
67 | 68
IP server | 255.255.255.255
Server_MAC | Client_MAC

Funcționare client-side



- În mod real fiecare sistem de operare va păstra un cache pe partea de client
- SO-ul va trimite direct DHCP Request pentru a obține aceeași adresă IP ca în trecut

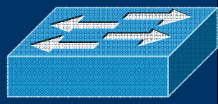
1) Cerere DHCP Linux VM imediat după bootare

8	10.220779	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transa
9	10.228300	D-Link_7d:ba:32	Broadcast	ARP	Who has 192.168.0.128?
10	11.192395	192.168.0.1	255.255.255.255	DHCP	DHCP Offer - Transa
11	11.193288	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transa
12	11.201931	192.168.0.1	255.255.255.255	DHCP	DHCP ACK - Transa

2) Cerere DHCP Linux VM la 1 minut după cerea de mai sus

30	25.222375	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Trans
31	27.038673	fe80::c837:5b20:721:f	ff02::c	SSDP	M-SEARCH * HTTP/1.1
32	27.518178	192.168.0.127	192.168.0.255	NBNS	Name query NB MSNMSGR
33	28.220570	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Trans
34	28.232980	192.168.0.1	255.255.255.255	DHCP	DHCP ACK - Trans

DHCP client/server



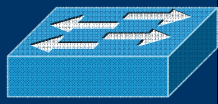
Clientul DHCP

- Linux
  - dhclient eth0
- Windows
  - ipconfig /release
  - ip config /renew

Serverul DHCP

- Linux
  - dhcp3-server
- Windows
  - Windows ☺ -> în Windows Server 2008, DHCP-Server este un "Rol" ce se poate instala

DHCP MAC address bind



Pasiv

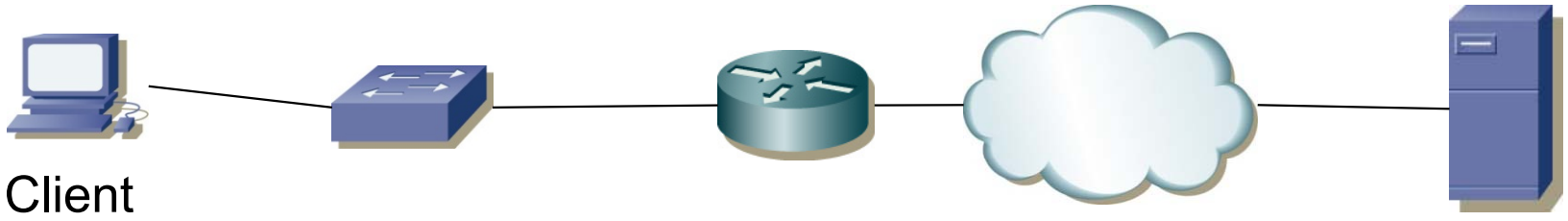
- Serverul reține binding-urile făcute în ultimele x ore
- Încearcă să ofere aceeași adresă IP pentru același MAC dacă îl are în cache

Activ

- Serverul este configurat explicit să ofere mereu aceeași adresă IP pentru același MAC
  - fișiere de configurare presistente (Linux: /etc/dhcp3/dhcpd.conf)

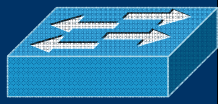
DHCP Relay

- DHCP Relay



- Problemă: DHCP folosește broadcast-uri L2
- Ruterul poate fi configurat să transforme broadcast-ul L2 (Discovery, Request) în unicast către server
- Dar…
  - … ruterul decapsulează nivelul 2 deci …
  - … cum mai funcționeaza MAC address binding explicit ?
- MAC-ul sursă e salvat în antetul DHCP

Configurare - Linux



```
# apt-get install dhcp3-server
# cat /etc/dhcp3/dhcpd.conf

# Range of IP addresses to be issued to DHCP clients
subnet 192.168.1.0 netmask 255.255.255.0 {range 192.168.1.128
   192.168.1.254;
# Default subnet mask to be used by DHCP clients
option subnet-mask 255.255.255.0;
# Default broadcastaddress to be used by DHCP clients
option broadcast-address 192.168.1.255;
option routers 192.168.1.1; # Default gateway to be used by DHCP clients
option domain-name "your-domain.org";
# Default DNS to be used by DHCP clients
option domain-name-servers 40.175.42.254, 40.175.42.253;
# Laser printer obtains IP address via DHCP. This assures that the
# printer with this MAC address will get this IP address every time.
host laser-printer-lex1 {
   hardware ethernet 08:00:2b:4c:a3:82;
   fixed-address 192.168.1.120;
}
}
```