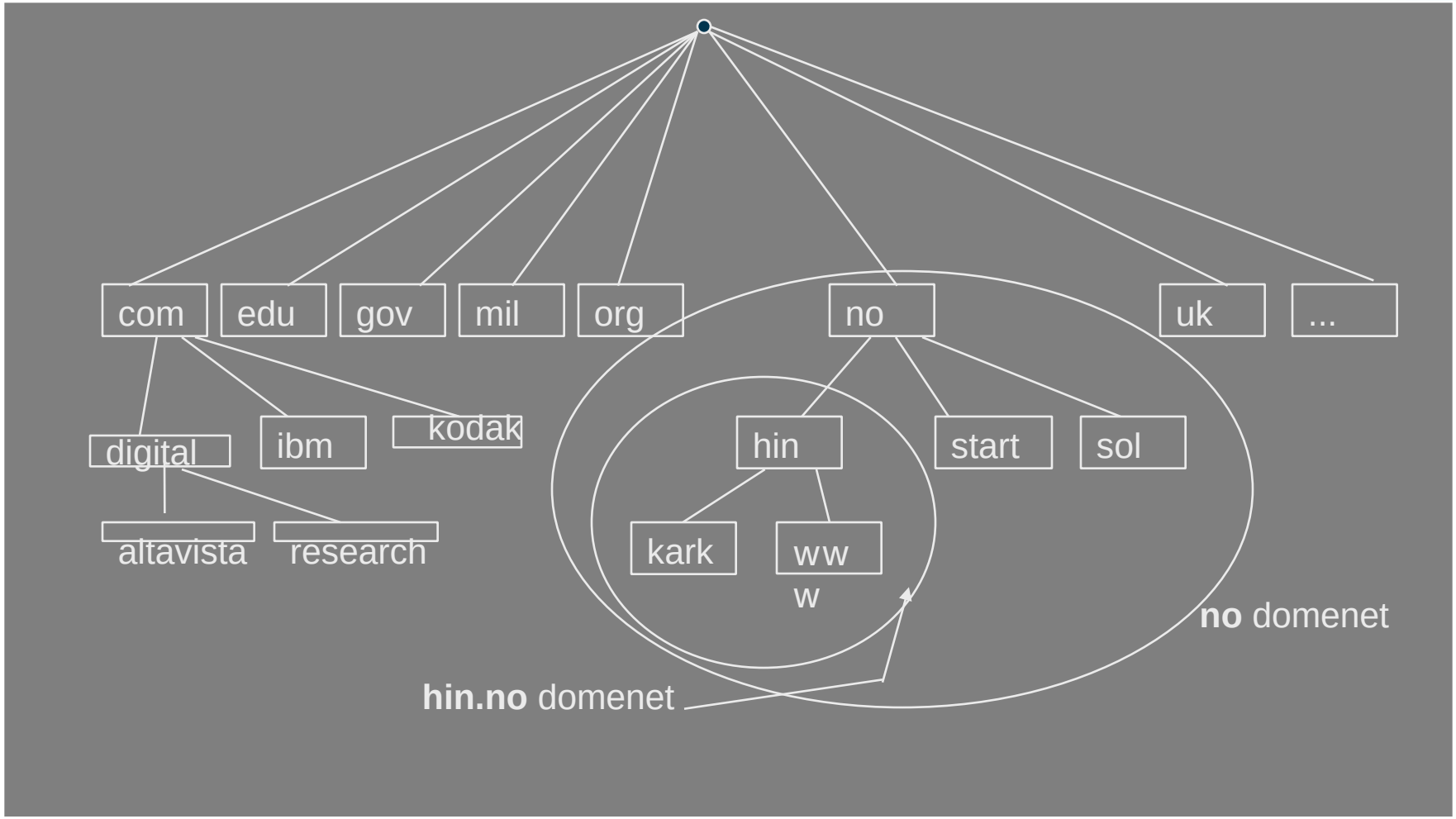
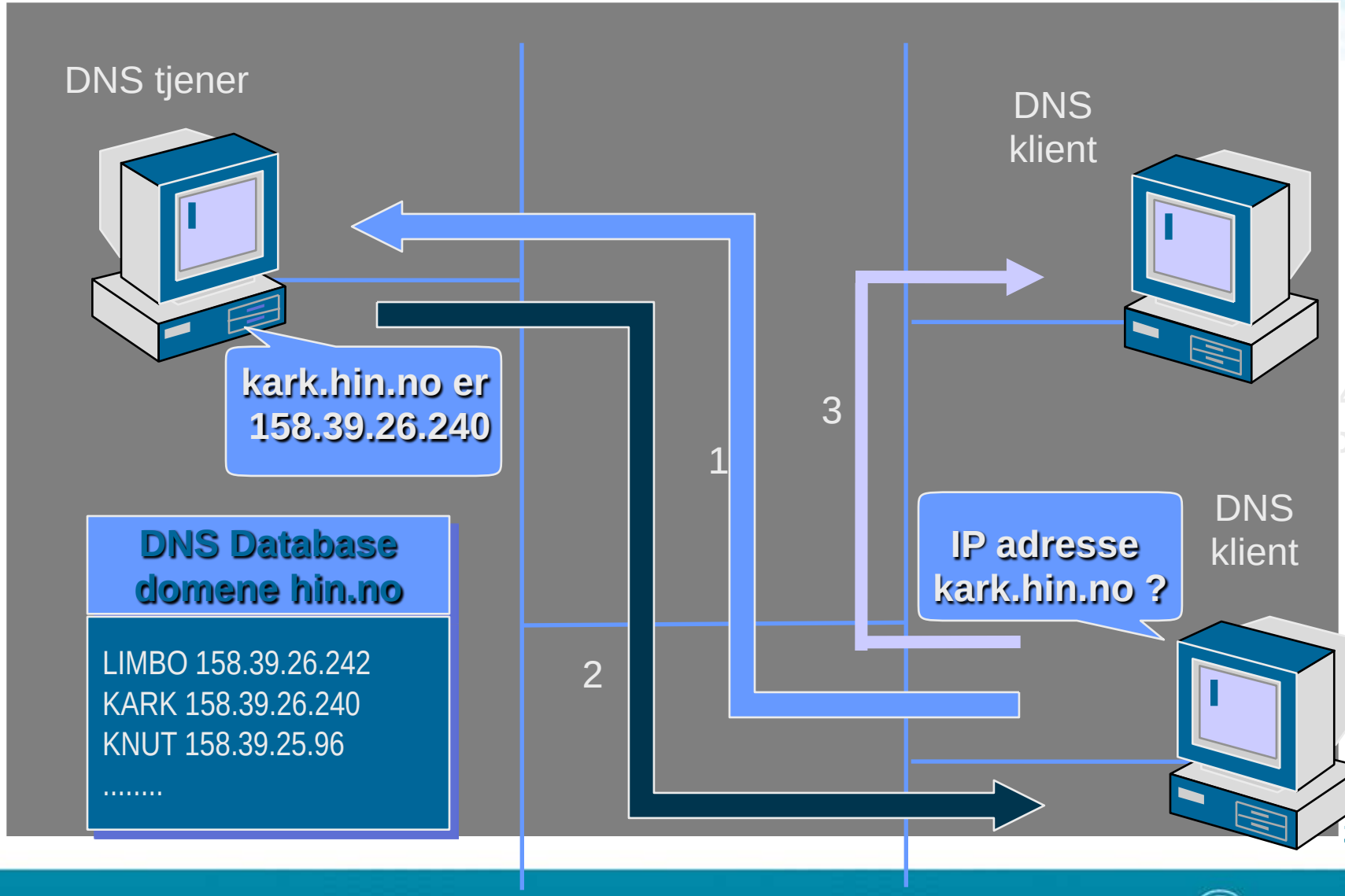
Distributed Name Server - DNS

- Oversettelse mellom domenenavn og IP nummer foretas av en DNS tjener
  - Forward oppslag fra navn til IP nummer
  - Reversoppslag fra IP nummer til navn
- Hovedtyper av DNS tjenere
  - Primær
    - Hoved navnetjener (master) for en navnesone
  - Sekundær
    - En caching-only navnetjener (slave) som benyttes for avlasting av den primære navnetjeneren

DNS navnehierarki



DNS klient/tjener prosessering

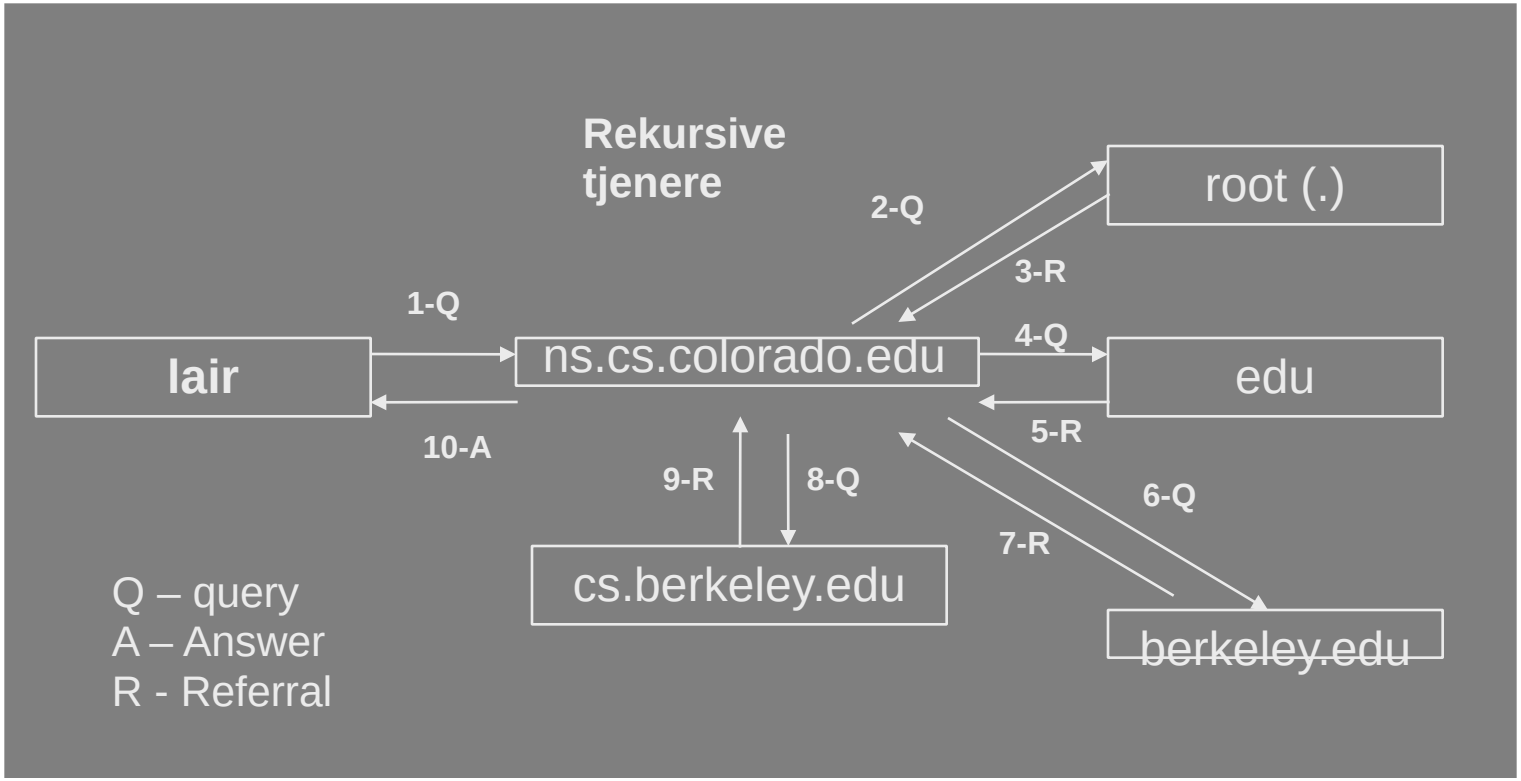


DNS tjenere

- Rekursiv DNS tjener
  - Tjeneren vil på vegne av klienten gjøre flere oppslag mot forskjellige navnetjenere for å kunne svare klienten tilfredstillende
- Ikke-rekursiv DNS tjener
  - Tjeneren vil ikke spørre andre DNS tjenere, men fortelle klienten om hvilken DNS tjener som muligens kan svare. Klienten må så selv spørre denne.
- Konfigurasjonsinstillingene styrer oppførsel for tjeneren, de fleste tjenere er rekursive.

DNS klient/tjener prosessering

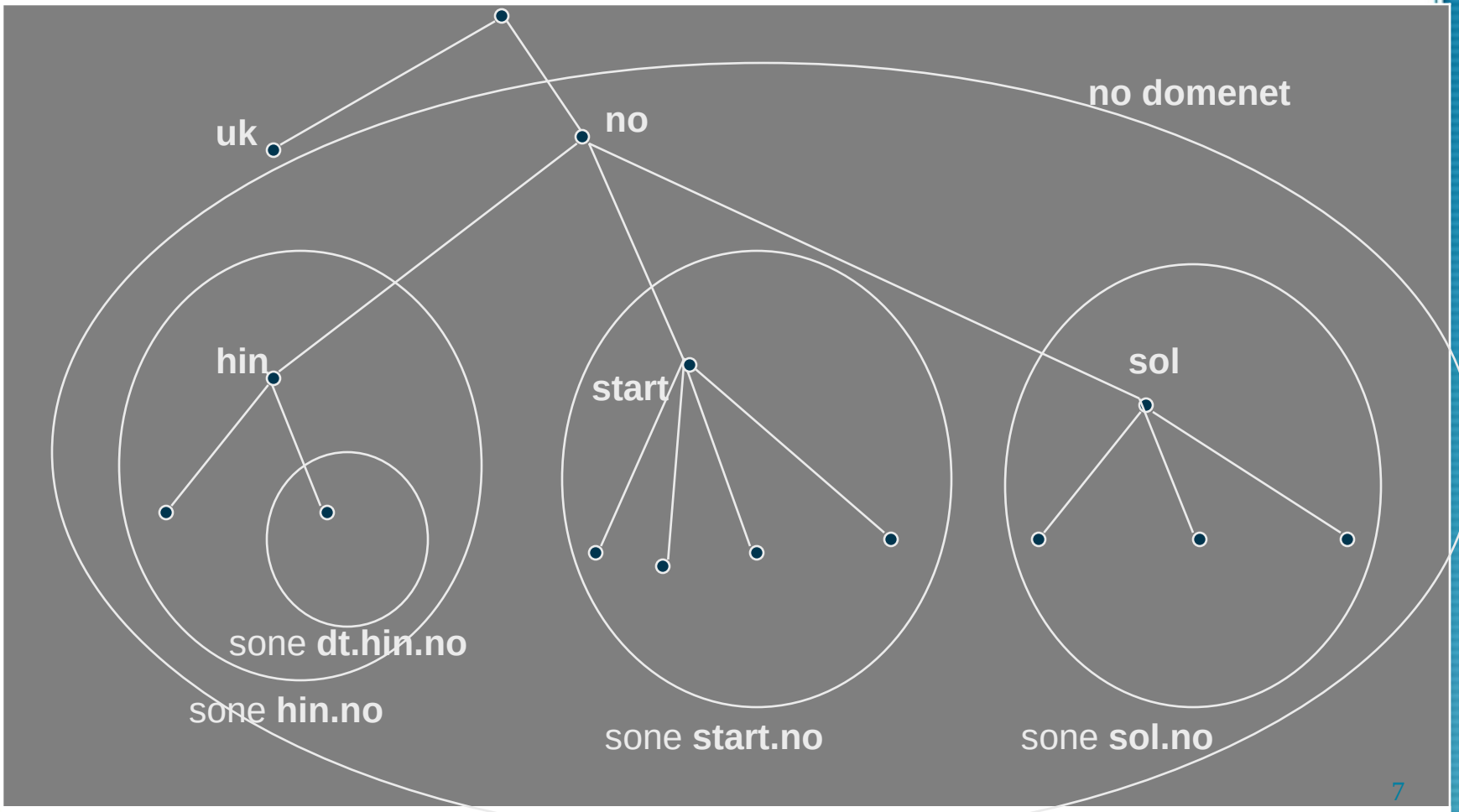
- Navneoppslag fra systemet vangogh.cs.berkeley.edu fra lair.cs.colorado.edu



DNS soner

- DNS domener deles opp i soner for delegering av kontroll og administrasjon
- Hver sone har minst to navnetjenere som er ansvarlig for denne sonen
- Modersonen delegerer ansvar for navneoppslag mot denne sonen til sonens navnetjenere
- En sone får ansvar for sin egen del av DNS treet
  - Forward lookup zone
    - Oversetter fra DNS navn til IP nummer
  - Reverse lookup zone
    - Oversetter av IP nummer til DNS navn

DNS soner


uk
no
no domenet
hin
start
sol
sone dt.hin.no
sone hin.no
sone start.no
sone sol.no

DNS og sikkerhet

- DNS navnstreet gir mye informasjon om systemene i en bedrift og kan utnyttes ved innbruddsforsøk
- DNS ressursdata bør alltid beskyttes
  - Begrensninger på hvem som kan gjøre oppslag
  - Begrensninger på hvem som kan foreta en sone transfer (kopi)
  - Begrensninger på systemer som kan foreta dynamiske oppdateringer i DNS databasen

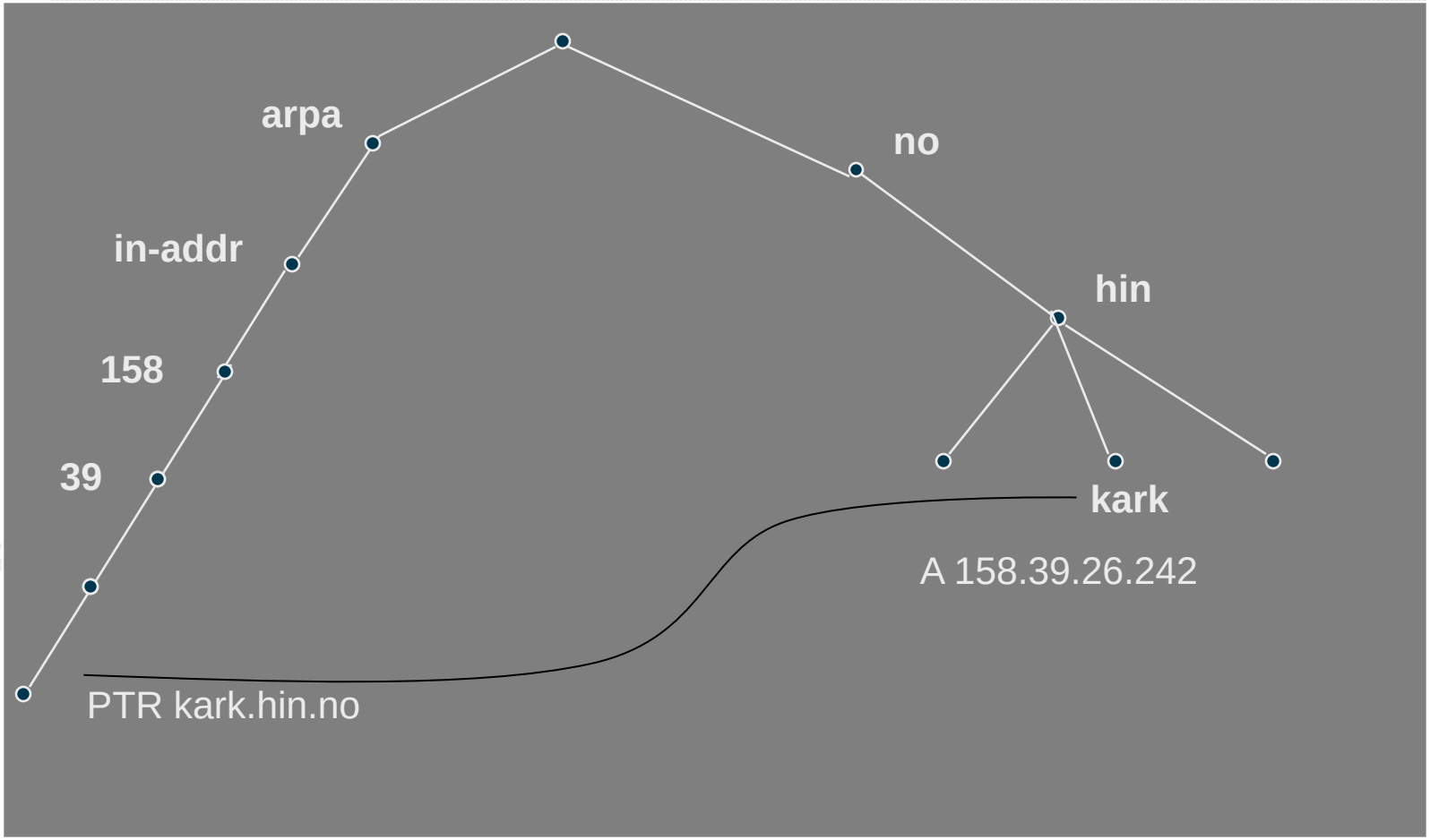
bind

- BIND – Berkeley Internet Name Domain
  - Den mest utbredte navnetjeneren i dag, kjører på ulike Unix og Linux systemer
  - V9.4.2 er siste versjon tilgjengelig fra http://www.isc.org/
  - Komponenter:
    - **named**, daemon som svarer på DNS forespørsler
    - **nslookup, dig, host**, kommandolinje basert program for forespørsel til DNS
    - **rndc**, kontrollprogram for **named**
    - **named-checkconf og named-checkzone** for verifikasjon av oppsett

Sonefiler

- En DNS navnetjener definerer et sett med *forward* og *reverse* oppslagssoner
- **`in-addr.arpa`** er en spesiell topp nivå sone som benyttes ved revers oppslag
  - Kark.hin.no har IP 158.39.26.240, angivelse av navn og IP er motsatt rekkefølge. Den mest signifikante delen no og 158 står hhv. til høyre og til venstre
  - Sonen **`26.39.158.in-addr.arpa`** er skapt for at samme programvare skal kunne operere både på navn og IP nummer, og foreta både forward og revers oppslag

in-addr.arpa



Sonefil poster

- **$ORIGIN**
  - definere hvor i navnetreet ressursdataene gjelder
- **$TTL**
  - Angir hvor lenge andre navnetjenere kan cache opplysningene fra oss
- **SOA**
  - Start of Authority, startpost for en ny sone, inneholder diverse informasjon
- **NS**
  - Name server, angir navnetjener for sonen
- **A**
  - Address, en definert adresse i sonen

Sonefil poster

- **MX**
  - Mail Exchange, posttjener for sonen, tall angir preferanse, lavest tall angir standard posttjener
- **PTR**
  - Peker post foretar revers mappingen fra IP til navn
- **ALIAS / CNAME**
  - et aliasnavn for et system i sonen
- **SRV**
  - Spesifiserer hvor en tjeneste i et domene befinner seg, for eksempel hvilket system som kjører FTP tjenesten
- **LOC**
  - Beskriver geografisk lokasjon

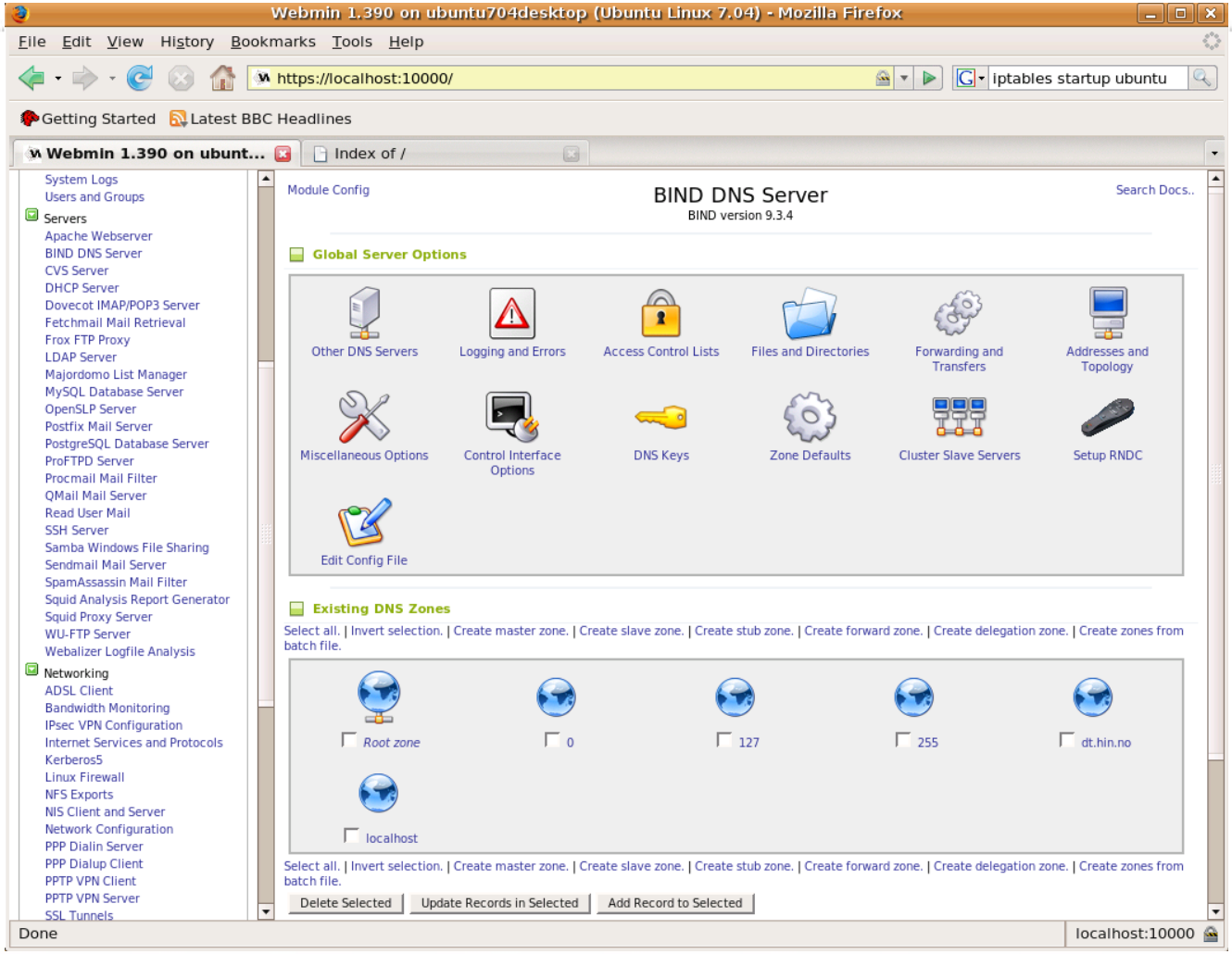
Sonefil eksempel: dt.hin.no

```
$ORIGIN dt.hin.no.
$TTL 86400      ; 1 day
@ IN SOA        bri.dt.hin.no. postmaster.dt.hin.no. (
                               2003022406 ; serial
                               28800      ; refresh (8 hours)
                               3600       ; retry (1 hour)
                               604800     ; expire (1 week)
                               86400      ; minimum (1 day)
                               )
                        NS     kark.hin.no.
                        NS     bri
                        MX     10      kark.hin.no.
                        MX     20      bri
bri                     A      192.168.100.1
gandalf                 A      192.168.100.2
www                     CNAME  gandalf
```

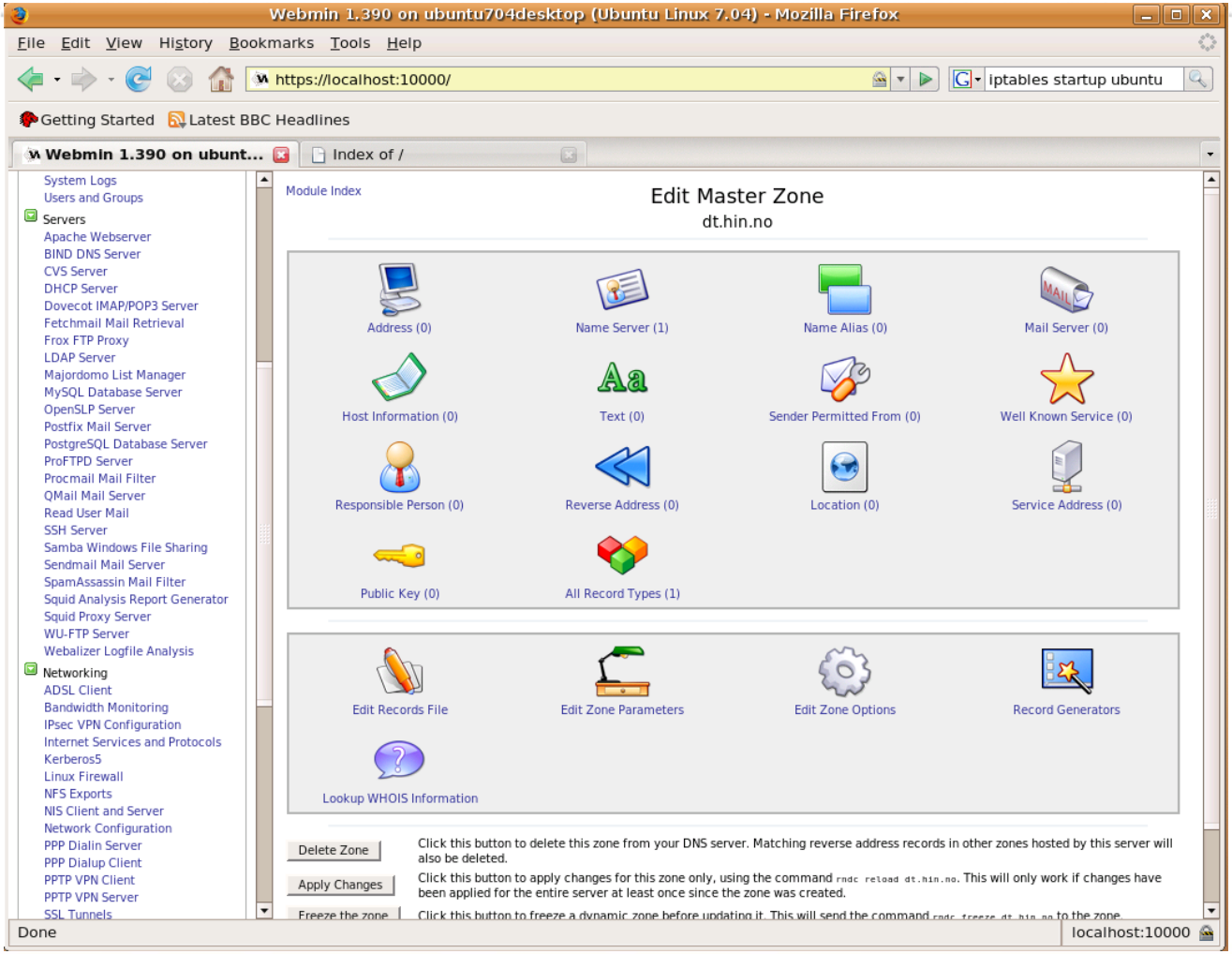
168.192.in-addr.arpa

```
$ORIGIN 100.168.192.in-addr.arpa.
$TTL 86400      ; 1 day
@ IN SOA        bri.dt.hin.no. postmaster.dt.hin.no. (
                                2003052101 ; serial
                                28800      ; refresh (8 hours)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )

                        NS      kark.hin.no.
                        NS      bri.dt.hin.no.
1                       PTR     bri.dt.hin.no.
2                       PTR     gandalf.dt.hin.no.
```

webmin DNS admin



webmin DNS admin



named.conf

- named konfigurasjonsfil
  - options, angir opsjoner for tjeneren
    - directory, katalog for sonefiler
    - recursion. rekursiv eller ikke-rekursiv tjener
    - allow-recursion, hvem foretar vi rekursjon for
    - blackhole, tjenere som skal ignoreres totalt
    - bogus, hvilke tjenere skal vi aldri spørre
  - zone, definisjon av primære og sekundære soner
    - type, master or slave
    - file, fil for lagring av sonedata
    - allow-query, hvem kan spørre
    - allow-transfers, hvem kan overføre sonen
    - allow-update, hvem kan oppdatere dynamisk
  - acl, aksessliste for hvem som kan benytte tjeneren

named.conf

```
//Cconfiguration is for an authoritative-only server that is the master server for
//"dt.hin.no" and a slave for the subdomain "hin.no".

acl bogus-nets{
 0.0.0.0/8; 1.0.0.0/8; 2.0.0.0/8; 192.0.2.0/24; 224.0.0.0/3; 10.0.0.0/8;172.16.0.0/16;};
acl our-nets{ 158.39.26.0/23; 158.39.25.0/24; 192.168.0/16; };

options {
  directory "/etc/namedb"; // Working directory
  pid-file "named.pid"; // Put pid file in working dir
  allow-query {   our-nets; };
  allow-recursion {   our-nets; };
  blackhole { bogus-nets;};
};
// Root server hints
zone "." {
  type hint;
  file "named.root";
};
```

named.conf

```
// Provide a reverse mapping for the loopback address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
  type master;
  file "localhost.rev";
  allow-update {none;};
};
zone "localhost" {
  type master;
  file "localhost.zone";
  allow-update {none;};
};
zone "dt.hin.no" {      // We are the master server for dt.hin.no
  type master;
  file "pz/dt.hin.no";
  // IP addresses of slave servers allowed to transfer dt.hin.no
  allow-transfer {
    192.168.4.14;
    192.168.5.53;
  };
};
```

named.conf

```
// Reverse lookup zones
zone ”168.192.in-addr.arpa" {
  type master;
  file "pz/168.192.in-addr.arpa";
};

// We are a slave server for hin.no
zone "hin.no" {
  type slave;
  file "sz/hin.no";
  // IP address of hin.no master server
  masters { 158.39.21.5; };
};
```

DNS glue records

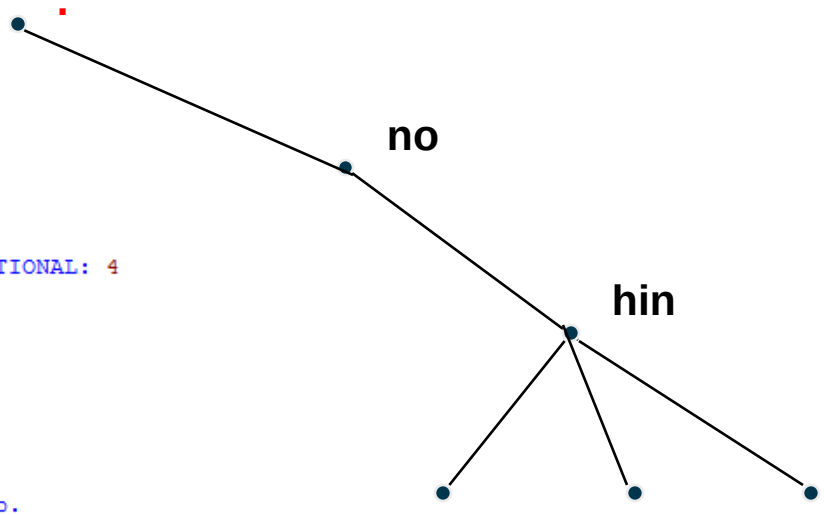
- Nødvendig lim som må inn for å binde navnetreet sammen
- Forespørsel etter www.hin.no
  1. Forespør en root navnetjener etter no navnetjener
  2. Denne er definert I sonen no
  3. Hvordan finne denne ?

Løsning:

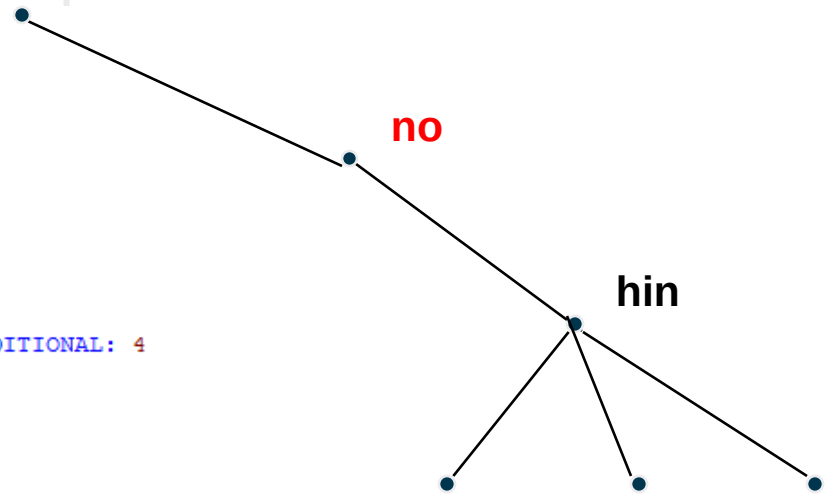
IP adressen for en barnesone må være definert i foreldresonen

glue records

```
user@ubuntu704desktop:~$ dig no ns

; <<>> DiG 9.3.4 <<>> no ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4896
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;no.                            IN      NS

;; ANSWER SECTION:
no.                     85633   IN      NS      y.nic.no.
no.                     85633   IN      NS      z.nic.no.
no.                     85633   IN      NS      not.norid.no.
no.                     85633   IN      NS      njet.norid.no.
no.                     85633   IN      NS      i.nic.no.
no.                     85633   IN      NS      x.nic.no.

;; ADDITIONAL SECTION:
y.nic.no.               11716   IN      A       193.71.199.51
z.nic.no.               11700   IN      A       158.38.8.133
i.nic.no.               86006   IN      A       194.146.106.6
x.nic.no.               11728   IN      A       128.39.8.40

;; Query time: 2 msec
;; SERVER: 158.39.21.6#53(158.39.21.6)
;; WHEN: Tue Feb 12 11:19:05 2008
;; MSG SIZE  rcvd: 195
```



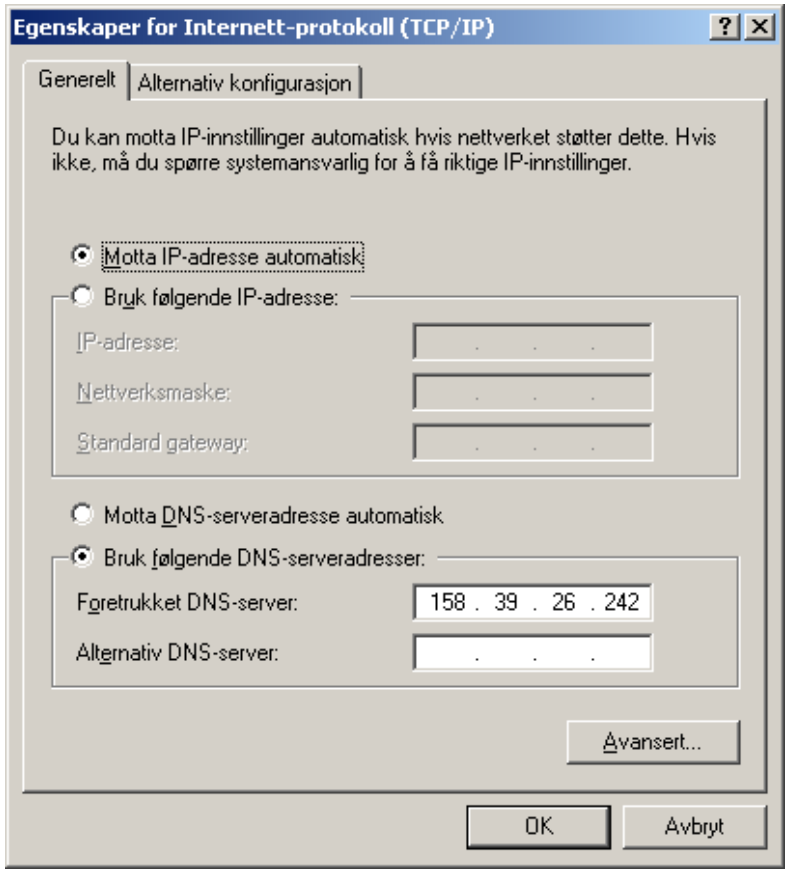
glue records




```
user@ubuntu704desktop:~$ dig hin.no ns

; <<>> DiG 9.3.4 <<>> hin.no ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3835
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;hin.no.                                IN      NS

;; ANSWER SECTION:
hin.no.                 3600    IN      NS      admserver.hin.no.
hin.no.                 3600    IN      NS      bdcstd.std.hin.no.
hin.no.                 3600    IN      NS      linken.ssin.hin.no.
hin.no.                 3600    IN      NS      bdcadm.hin.no.

;; ADDITIONAL SECTION:
admserver.hin.no.       1200    IN      A       158.39.21.4
bdcstd.std.hin.no.      1200    IN      A       158.39.26.6
linken.ssin.hin.no.     1200    IN      A       158.39.21.201
bdcadm.hin.no.          3600    IN      A       158.39.21.6

;; Query time: 2 msec
;; SERVER: 158.39.21.6#53(158.39.21.6)
;; WHEN: Tue Feb 12 11:17:01 2008
;; MSG SIZE  rcvd: 184
```

Win DNS klient

- Egenskaper for TCP/IP
  - Angir hvilke navnetjenere klienten skal benytte
- Egenskaper for datamaskin
  - angir standard domenenavn



DNS klient

- /etc/resolv.conf
  - Angir hvilke navnetjenere klienten skal benytte og standard domenenavn
  - Eksempel på /etc/resolv.conf
    - hin.no er standard domene, dersom klienten skriver kun kark vil systemet søke etter kark.hin.no
    - nameserver angir hvilke DNS tjenere som skal benyttes, maks 3 kan angis

```
search hin.no

nameserver 158.39.21.5
nameserver 158.39.26.242
```

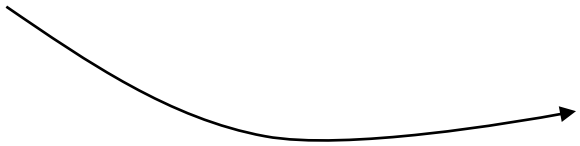
Dynamic Host Configuration Protocol (DHCP)

- DHCP
  - IP adresser tildeles automatisk fra en DHCP tjener
  - All nødvendig TCP/IP konfigurasjonsinformasjon kommer fra DHCP tjener
  - DHCP tjener er satt opp med en pool av IP adresser.
  - Mulighet for reservering av IP adresser til bestemte system.
  - Varighet på tildeling kan spesifiseres
  - Klienter ″ låner″ IP adresse, må fornye lånet når lånetiden utløper

dhclient.conf

- DHCP tjener vil normalt tildele navnetjener
- Skriver ny /etc/resolv.conf
- For å benytte egen navnetjener på Ubuntu
  - Rediger **`/etc/dhcp3/dhclient.conf`**
  - Angi egen navnetjener som første valg

```
prepend domain-name-servers 127.0.0.1;
request subnet-mask, broadcast-address, time-offset, routers,
     domain-name, domain-name-servers, host-name,
```



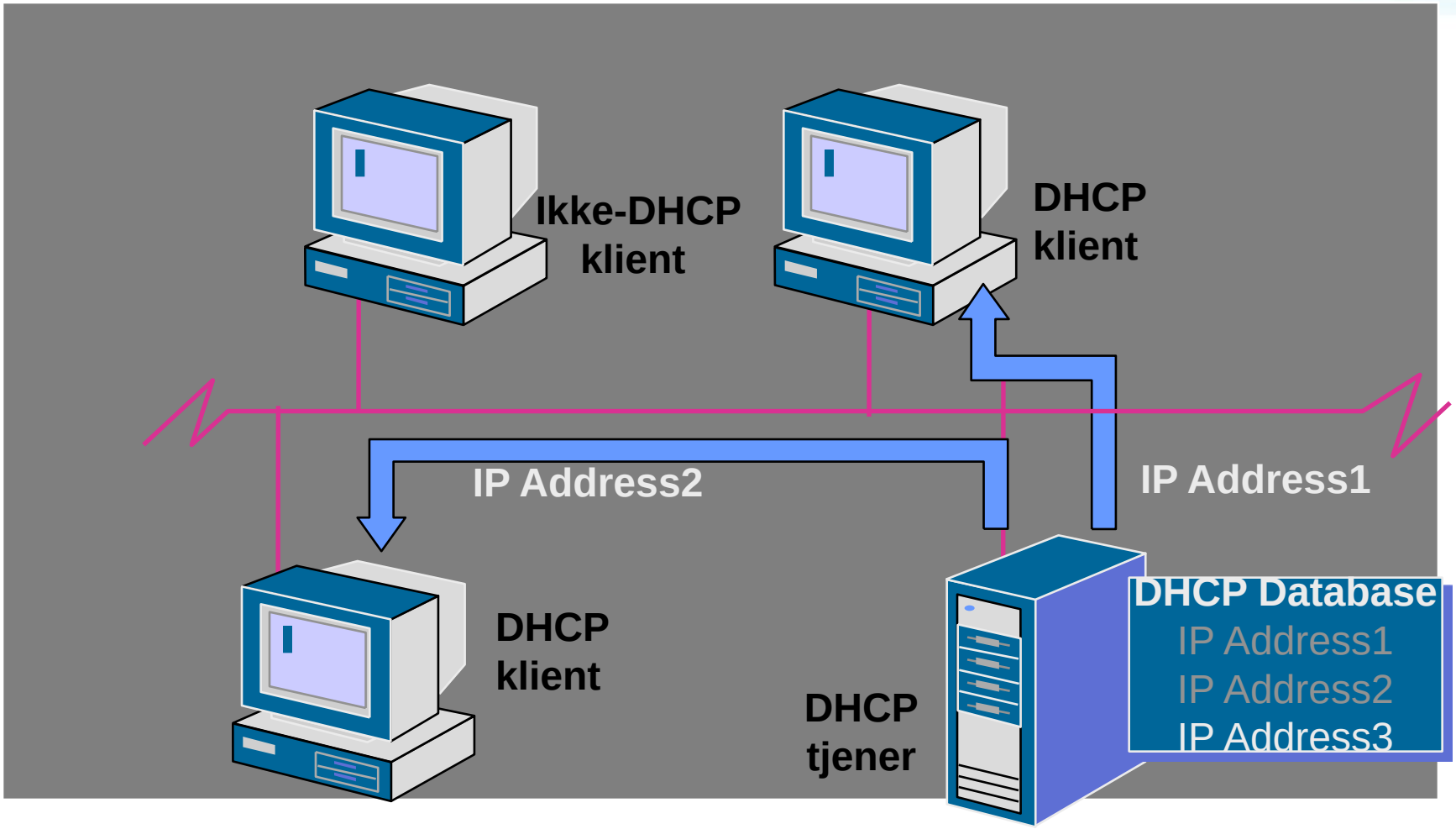
resolv.conf

```
search hin.no

nameserver 127.0.0.1
nameserver 158.39.21.5
nameserver 158.39.26.242
```

Alternativ til DHCP

- - Manuell tildeling av IP adresser
  - IP + TCP/IP parametere må konfigureres på hvert system
  - Feilkonfigurering medfører kommunikasjons problemer
  - Vanskelig feilsøkning
  - Stor jobb når endring av nettverksparametre

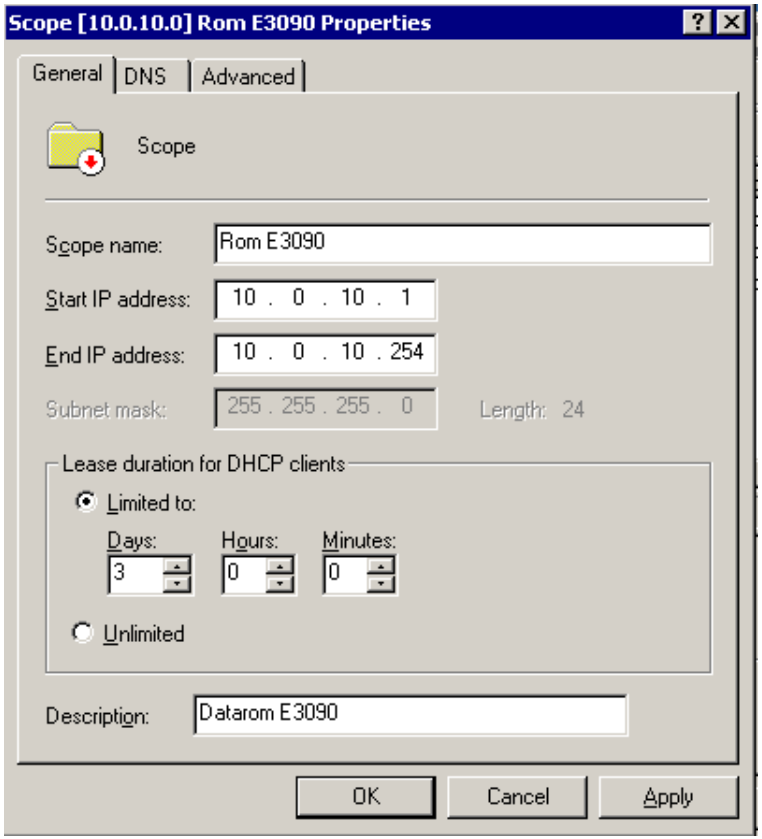
DHCP


Ikke-DHCP klient
DHCP klient
IP Address2
IP Address1
DHCP klient
DHCP tjener
DHCP Database
IP Address1
IP Address2
IP Address3

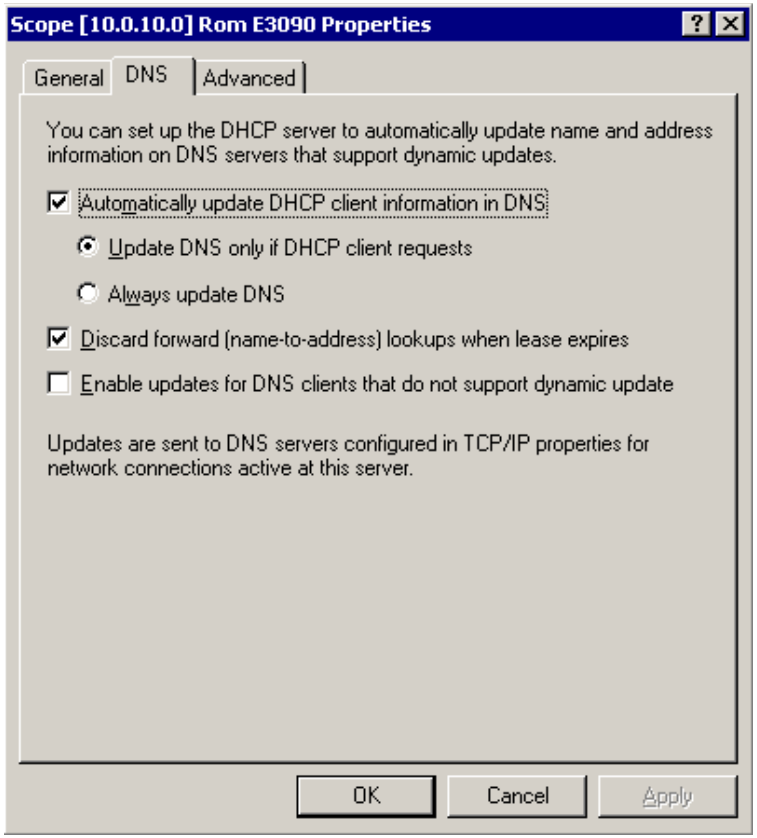
DHCP tjener oppsett

- DHCP tjener settes opp med et eller flere subnett
  - Et subnett inneholder nettverksoppsettet for et IP subnett
    - Ruter, DNS tjener, DNS domene navn etc.
    - IP adresser kan reserveres basert på MAC adresser
  - Parametere kan også angis som standard for hele DHCP tjener, alle subnett vil da arve disse

Windows DHCP subnett egenskaper



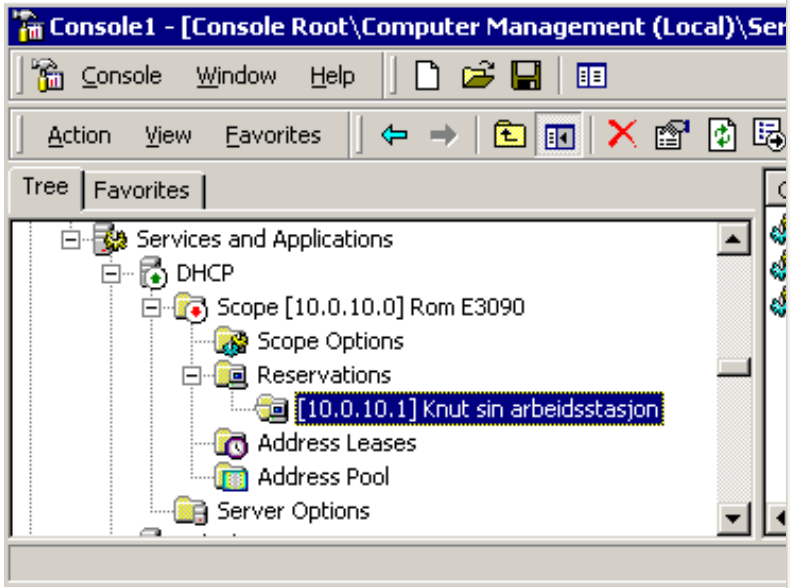
Adresseområde, subnettmaske og varighet

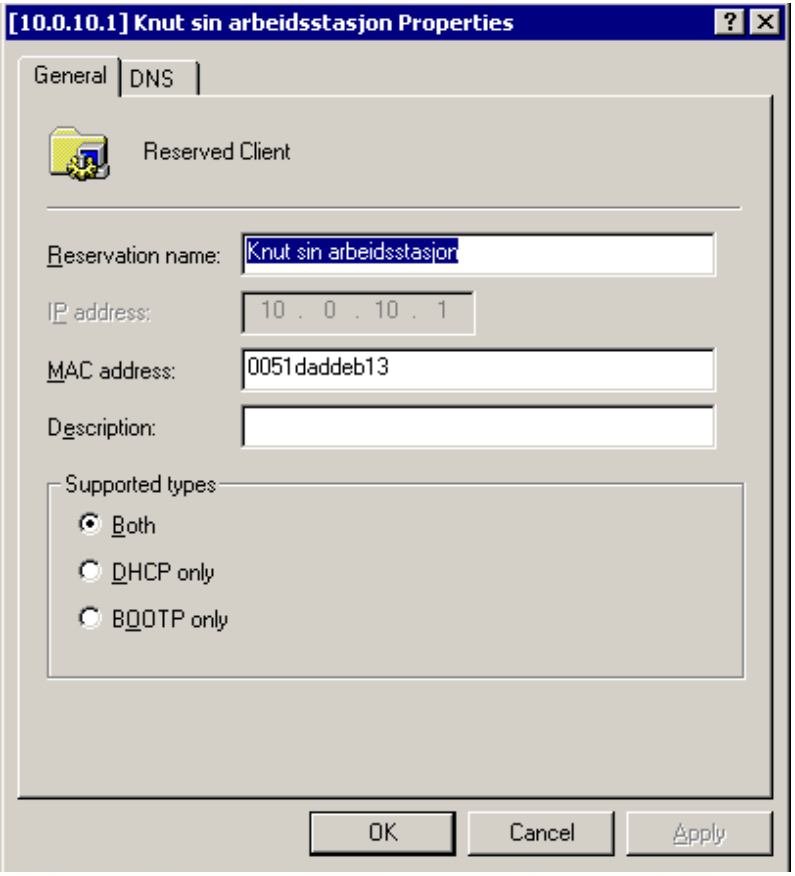


Politikk for oppdatering av DNS

DHCP reservasjoner

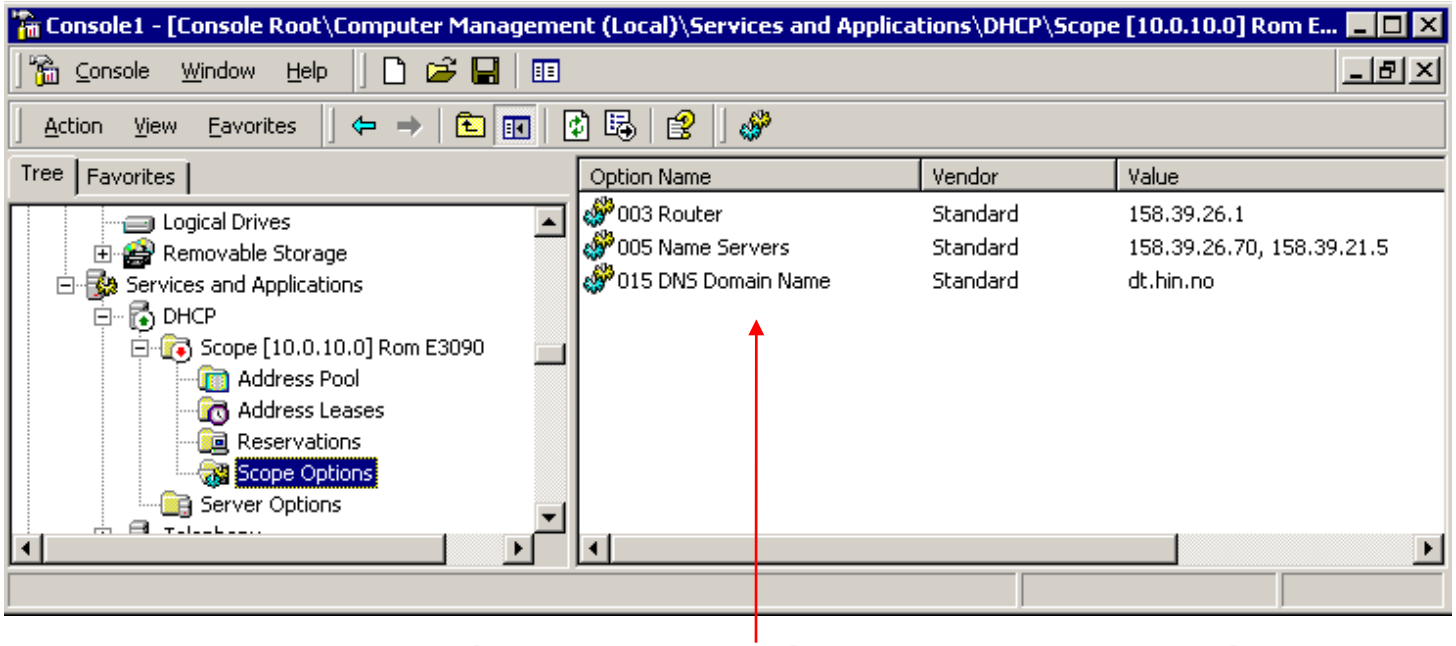
IP adresse 10.0.10.1 fast reservert til system med MAC adresse 0051daddeb13





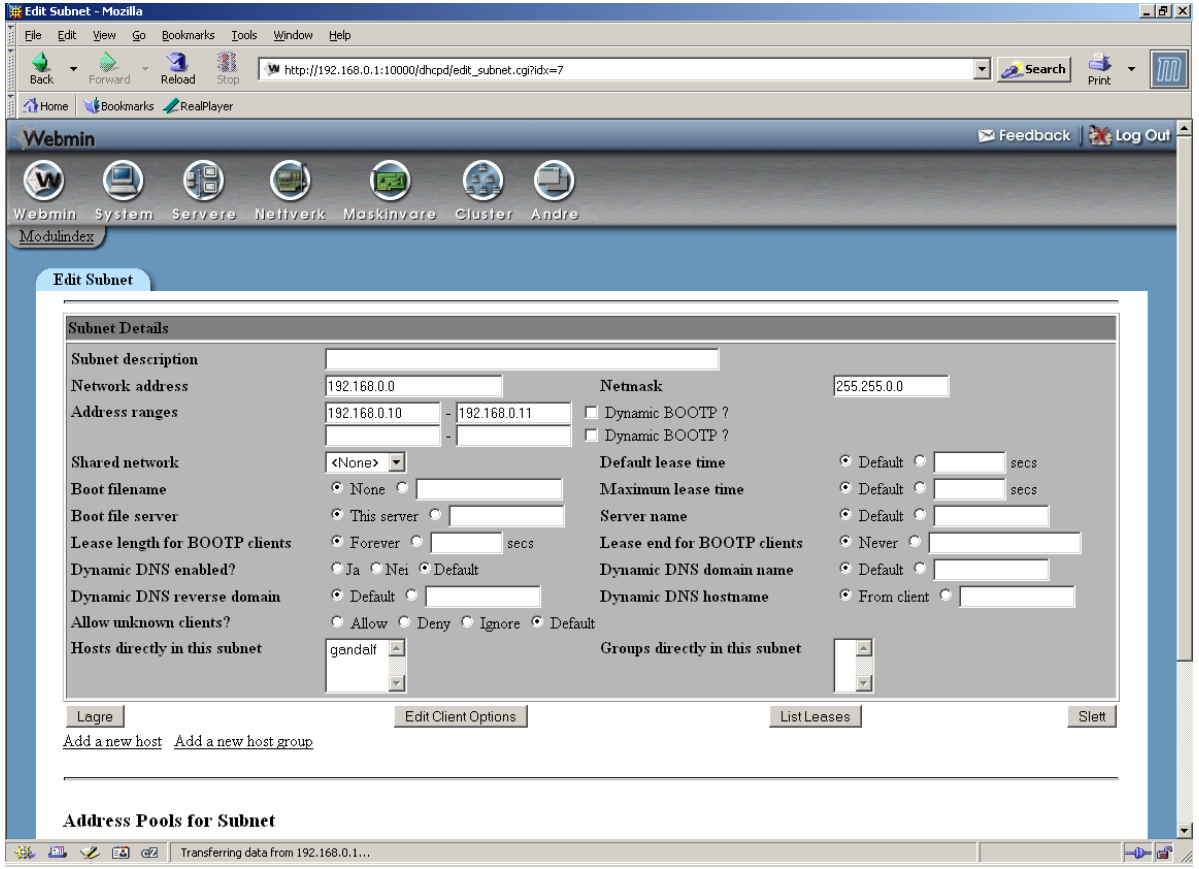
DHCP opsjoner

- Nettverksparametre legges inn som opsjoner enten pr. subnett, superscope eller som standard for DHCP tjener



Ruter, DNS navnetjener og DNS domene navn er satt for scope

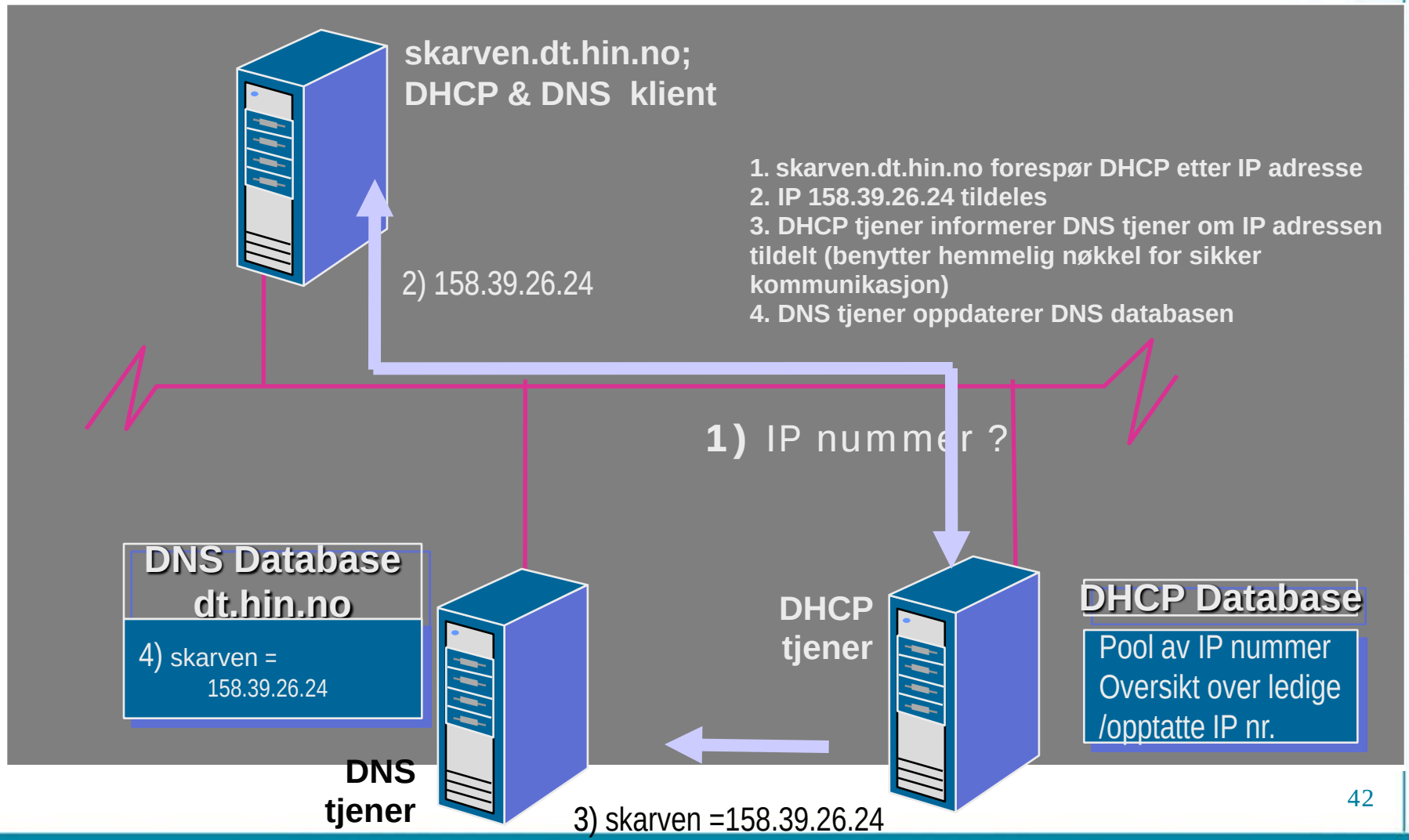
DHCP admin fra webmin



DDNS

- DNS var tidligere et statisk konsept
  - alle endringer måtte foretas manuelt
  - DDNS - Dynamic DNS gjør at systemer kan registrere seg automatisk i DNS databasen
  - Benyttes i Windows 200xx og på Linux med bind9 og dhcp3-server
  - Etter tildeling av IP adresse fra DHCP vil klientsystemet registrere seg selv i DNS databasen, alternativt vil DHCP tjeneren gjøre dette
  - Andre systemer kan dermed finne systemet med navn ved å forespørre DNS tjeneren

DDNS


skarven.dt.hin.no;
DHCP & DNS klient
1. skarven.dt.hin.no forespør DHCP etter IP adresse
2. IP 158.39.26.24 tildeles
3. DHCP tjener informerer DNS tjener om IP adressen tildelt (benytter hemmelig nøkkel for sikker kommunikasjon)
4. DNS tjener oppdaterer DNS databasen
2) 158.39.26.24
1) IP nummer ?
DNS Database
dt.hin.no
4) skarven =
158.39.26.24
DNS
tjener
DHCP
tjener
DHCP Database
Pool av IP nummer
Oversikt over ledige
/opptatte IP nr.
3) skarven =158.39.26.24