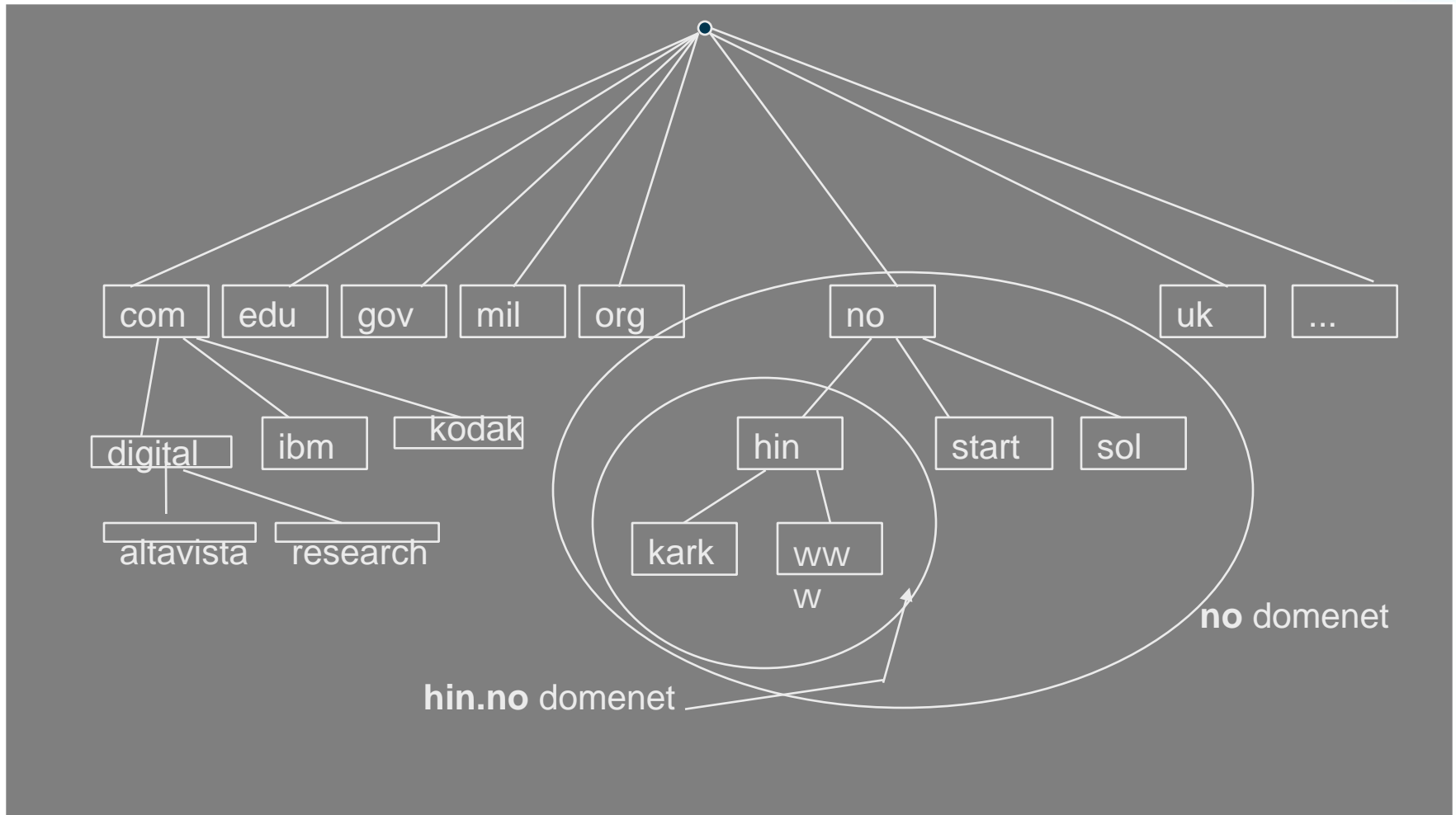


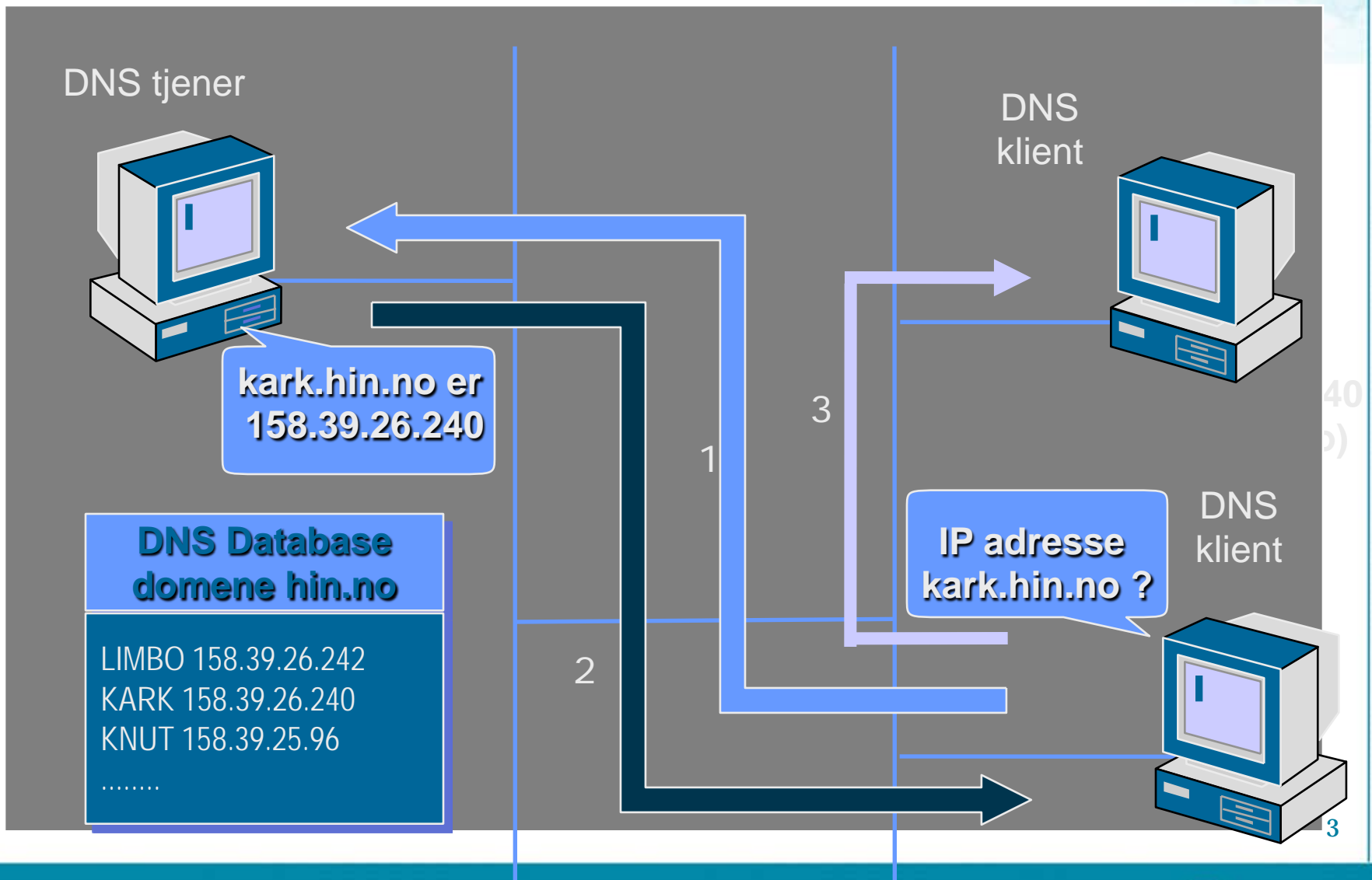
Distributed Name Server - DNS

- 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

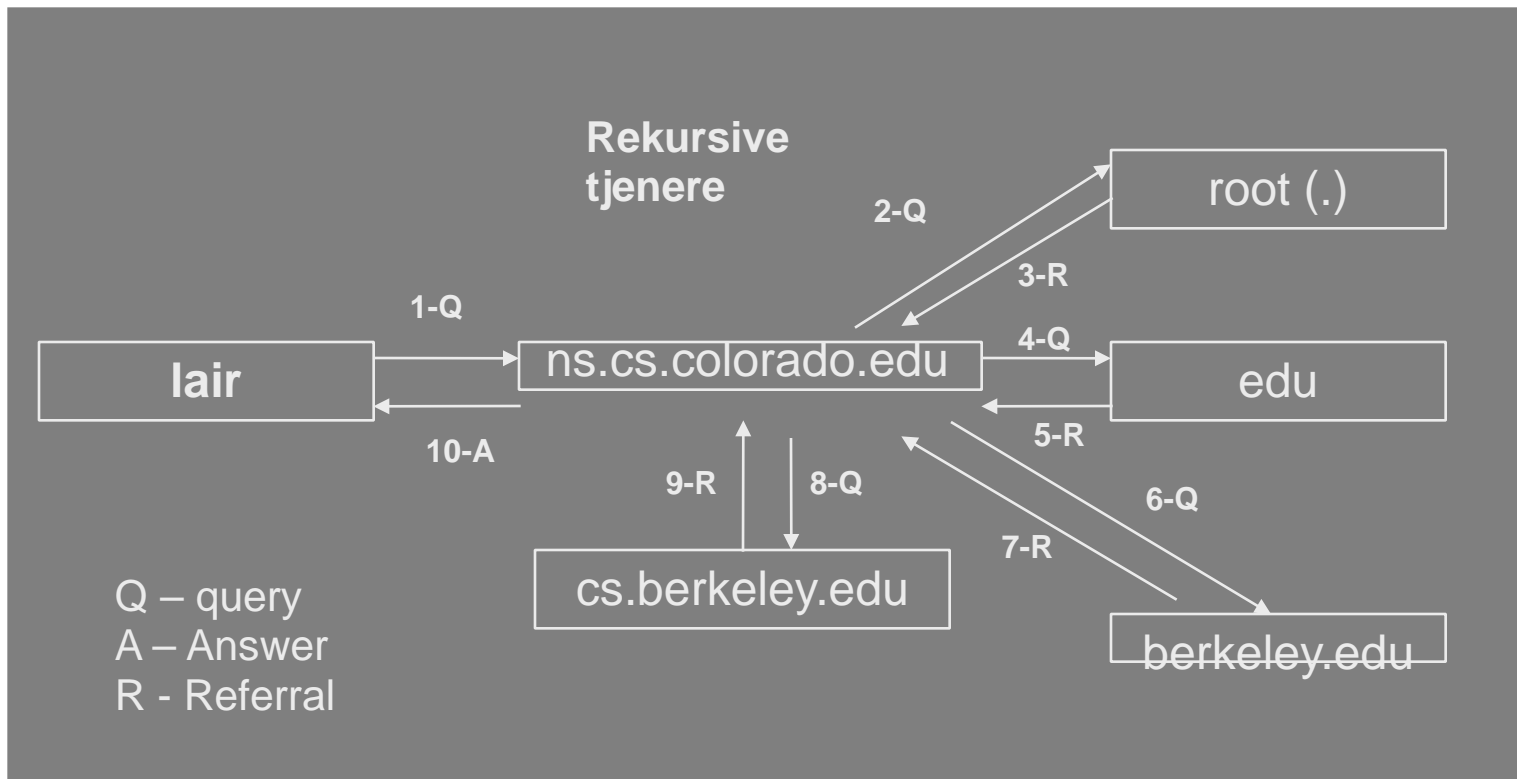


DNS tjenerer

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

DNS klient/tjener prosessering

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

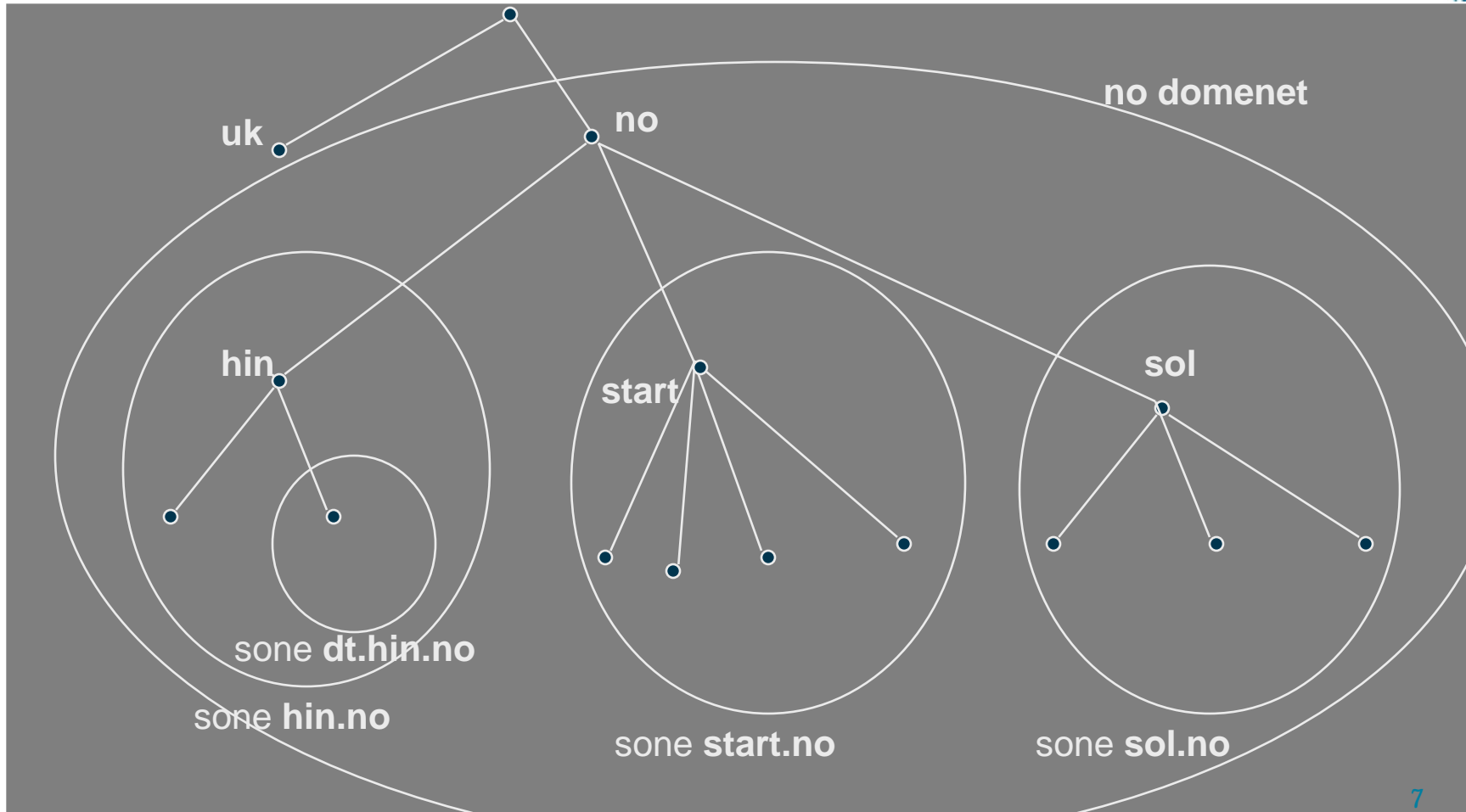


tjenere

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



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 zone transfer (kopi)
 - Begrensninger på systemer som kan foreta dynamiske oppdateringer i DNS databasen

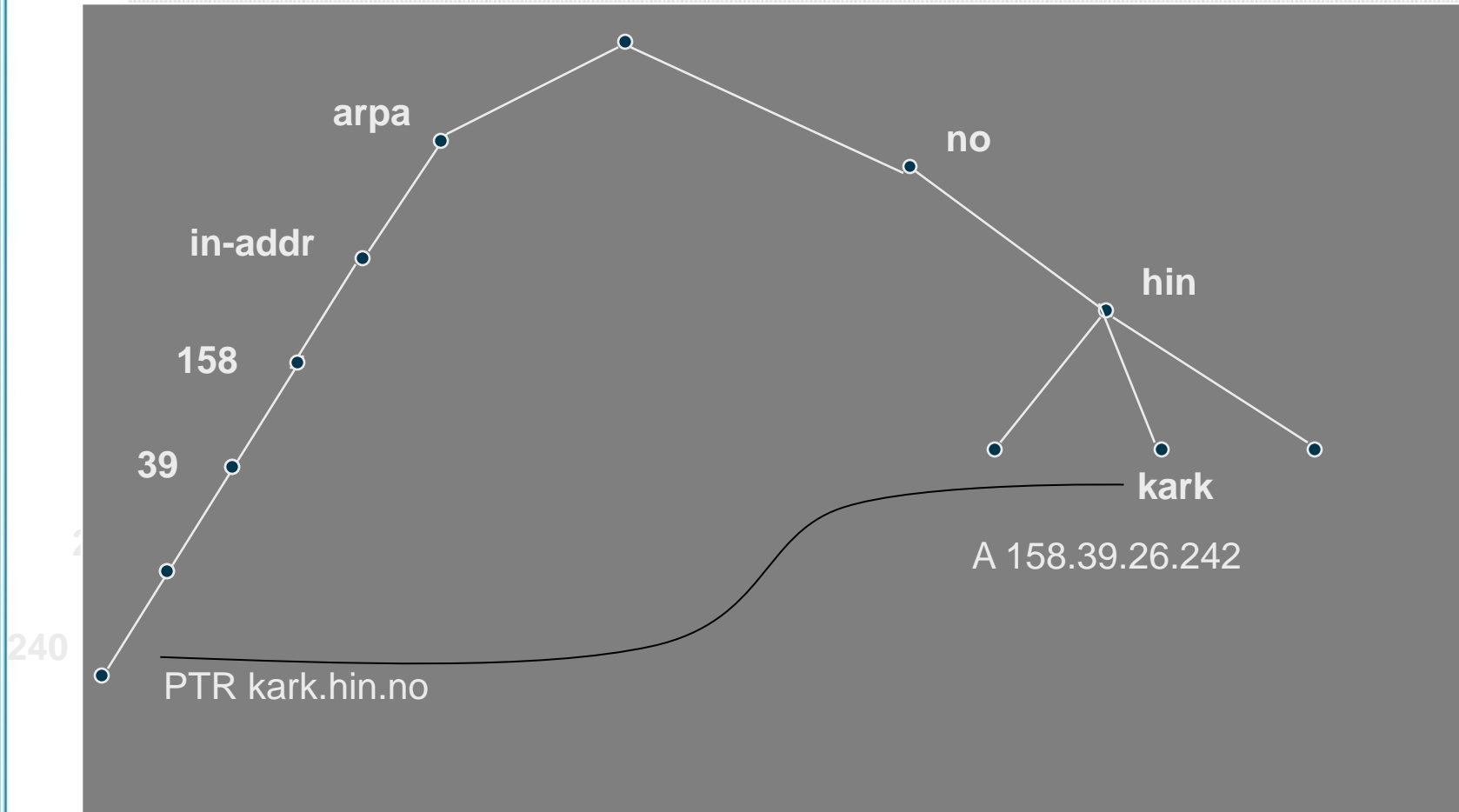
bind

- 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 1.390 on ubuntu704desktop (Ubuntu Linux 7.04) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://localhost:10000/ iptables startup ubuntu

Getting Started Latest BBC Headlines

Webmin 1.390 on ubuntu... Index of /

- System Logs
- Users and Groups
- Servers
 - Apache Webserver
 - BIND DNS Server
 - CVS Server
 - DHCP Server
 - Dovecot IMAP/POP3 Server
 - Fetchmail Mail Retrieval
 - Frox FTP Proxy
 - LDAP Server
 - Majordomo List Manager
 - MySQL Database Server
 - OpenSLP Server
 - Postfix Mail Server
 - PostgreSQL Database Server
 - ProFTPD Server
 - Procmail Mail Filter
 - QMail Mail Server
 - Read User Mail
 - SSH Server
 - Samba Windows File Sharing
 - Sendmail Mail Server
 - SpamAssassin Mail Filter
 - Squid Analysis Report Generator
 - Squid Proxy Server
 - WU-FTP Server
 - Webalizer Logfile Analysis
- Networking
 - ADSL Client
 - Bandwidth Monitoring
 - IPsec VPN Configuration
 - Internet Services and Protocols
 - Kerberos5
 - Linux Firewall
 - NFS Exports
 - NIS Client and Server
 - Network Configuration
 - PPP Dialin Server
 - PPP Dialup Client
 - PPTP VPN Client
 - PPTP VPN Server
 - SSL Tunnels

Module Config

BIND DNS Server

BIND version 9.3.4

Search Docs..

Global Server Options

- Other DNS Servers
- Logging and Errors
- Access Control Lists
- Files and Directories
- Forwarding and Transfers
- Addresses and Topology
- Miscellaneous Options
- Control Interface Options
- DNS Keys
- Zone Defaults
- Cluster Slave Servers
- Setup RNDG
- Edit Config File

Existing DNS Zones

Select all. | Invert selection. | Create master zone. | Create slave zone. | Create stub zone. | Create forward zone. | Create delegation zone. | Create zones from batch file.

- Root zone
- 0
- 127
- 255
- dt.hin.no
- localhost

Select all. | Invert selection. | Create master zone. | Create slave zone. | Create stub zone. | Create forward zone. | Create delegation zone. | Create zones from batch file.

Delete Selected Update Records in Selected Add Record to Selected

Done localhost:10000

webmin DNS admin

Webmin 1.390 on ubuntu704desktop (Ubuntu Linux 7.04) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://localhost:10000/ iptables startup ubuntu

Getting Started Latest BBC Headlines

Webmin 1.390 on ubuntu... Index of /

System Logs
Users and Groups

Servers

- Apache Webserver
- BIND DNS Server
- CVS Server
- DHCP Server
- Dovecot IMAP/POP3 Server
- Fetchmail Mail Retrieval
- Frox FTP Proxy
- LDAP Server
- Majordomo List Manager
- MySQL Database Server
- OpenSLP Server
- Postfix Mail Server
- PostgreSQL Database Server
- ProFTPD Server
- Procm Mail Filter
- QMail Mail Server
- Read User Mail
- SSH Server
- Samba Windows File Sharing
- Sendmail Mail Server
- SpamAssassin Mail Filter
- Squid Analysis Report Generator
- Squid Proxy Server
- WU-FTP Server
- Webalizer Logfile Analysis

Networking

- ADSL Client
- Bandwidth Monitoring
- IPsec VPN Configuration
- Internet Services and Protocols
- Kerberos5
- Linux Firewall
- NFS Exports
- NIS Client and Server
- Network Configuration
- PPP Dialin Server
- PPP Dialup Client
- PPTP VPN Client
- PPTP VPN Server
- SSL Tunnels

Module Index

Edit Master Zone dt.hin.no

Address (0)	Name Server (1)	Name Alias (0)	Mail Server (0)
Host Information (0)	Text (0)	Sender Permitted From (0)	Well Known Service (0)
Responsible Person (0)	Reverse Address (0)	Location (0)	Service Address (0)
Public Key (0)	All Record Types (1)		

Edit Records File	Edit Zone Parameters	Edit Zone Options	Record Generators
Lookup WHOIS Information			

Delete Zone Click this button to delete this zone from your DNS server. Matching reverse address records in other zones hosted by this server will also be deleted.

Apply Changes Click this button to apply changes for this zone only, using the command `rndc reload dt.hin.no`. This will only work if changes have been applied for the entire server at least once since the zone was created.

Freeze the zone Click this button to freeze a dynamic zone before updating it. This will send the command `rndc freeze dt.hin.no` to the zone.

Done localhost:10000

named.conf

- **named** konfigurasjonsfil
 - **options**, angir opsjoner for tjeneren
 - **directory**, katalog for soner
 - **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

```
// Configuration 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";
};
```

```
// 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;
    };
};
```

```
// 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:
```

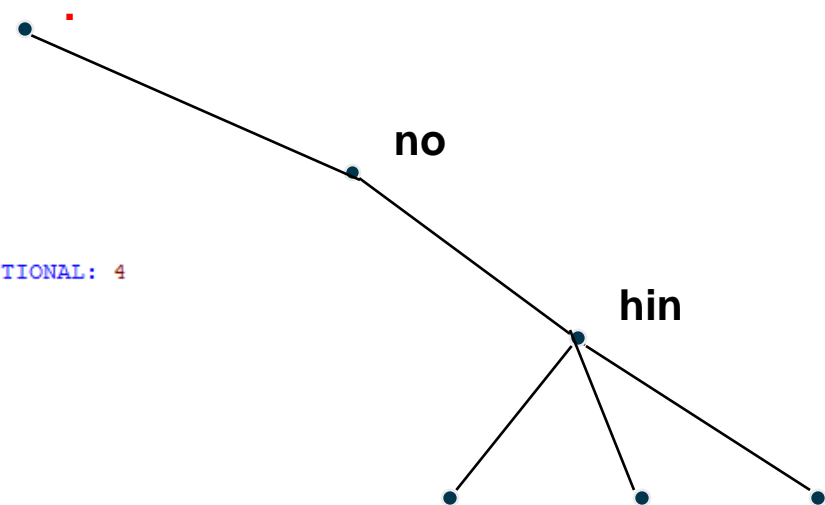
```
y.nic.no. 11716 IN A 193.71.199.51  
z.nic.no. 11700 IN A 158.38.8.133  
i.nic.no. 86006 IN A 194.146.106.6  
x.nic.no. 11728 IN A 128.39.8.40
```

```
;; 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

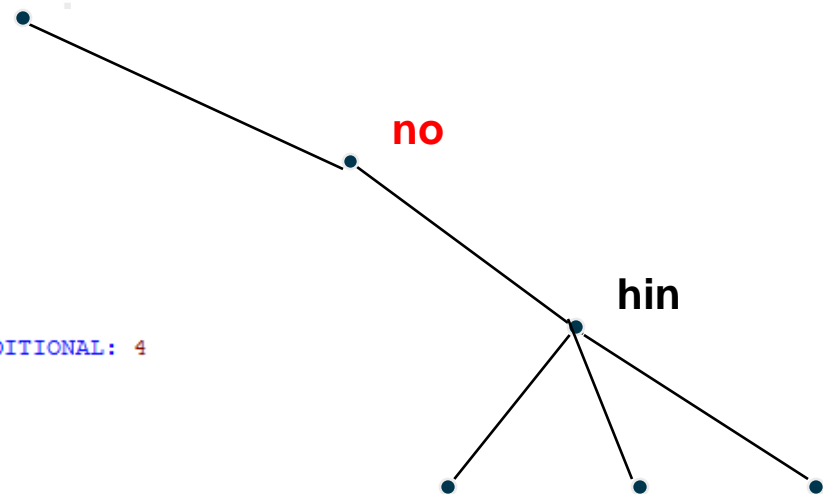
```
user@ubuntu704desktop:~$ dig hin.no ns
; <<>> DiG 9.3.4 <<>> hin.no ns
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3835
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; 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.

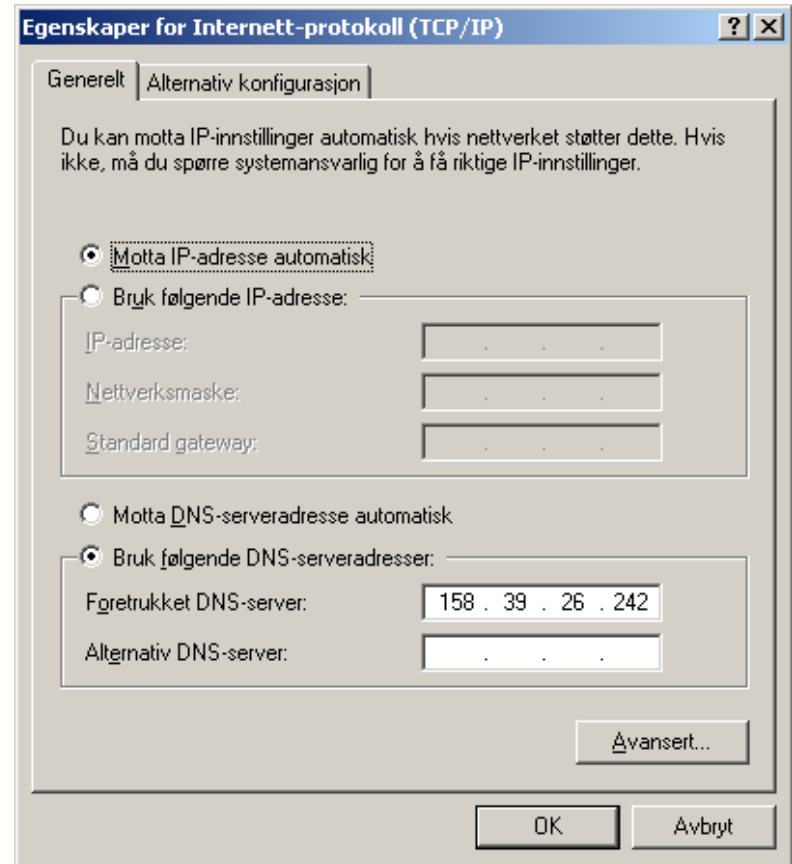
;; ADDITIONAL SECTION:
admserver.hin.no.      1200   IN      A       158.39.21.4
bdcstd.std.hin.no.    1200   IN      A       158.39.26.6
linken.ssin.hin.no.   1200   IN      A       158.39.21.201
bdcadm.hin.no.        3600   IN      A       158.39.21.6

;; 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 tjenerer 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

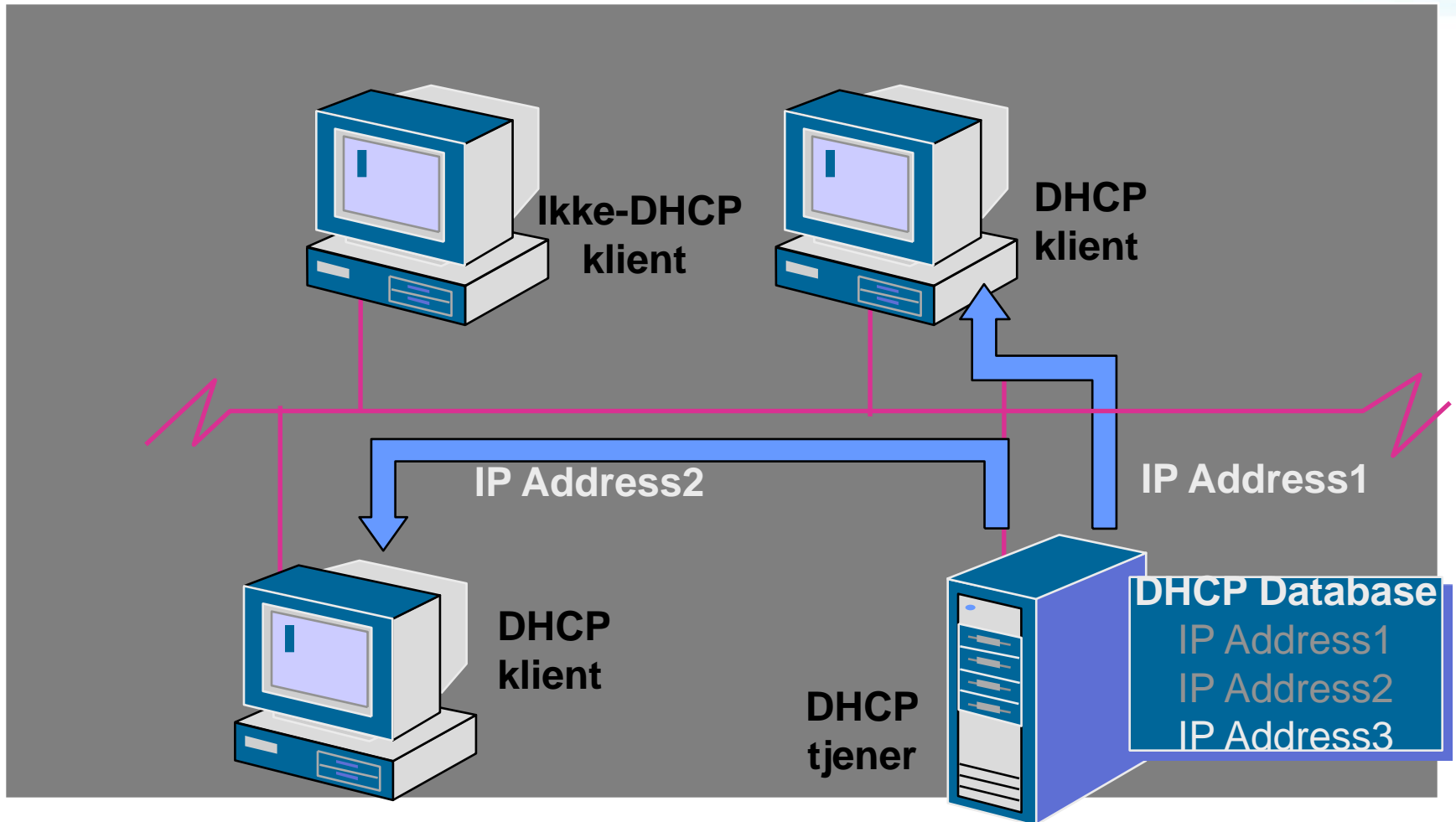
```
search hin.no
```

```
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



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

The screenshot shows the 'General' tab of the DHCP scope properties dialog. The 'Scope' folder icon is visible. The 'Scope name' is 'Rom E3090'. The 'Start IP address' is '10 . 0 . 10 . 1', the 'End IP address' is '10 . 0 . 10 . 254', and the 'Subnet mask' is '255 . 255 . 255 . 0' with a length of 24. Under 'Lease duration for DHCP clients', the 'Limited to' radio button is selected, with 'Days' set to 3, 'Hours' to 0, and 'Minutes' to 0. The 'Unlimited' radio button is unselected. The 'Description' is 'Datarom E3090'. Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom.

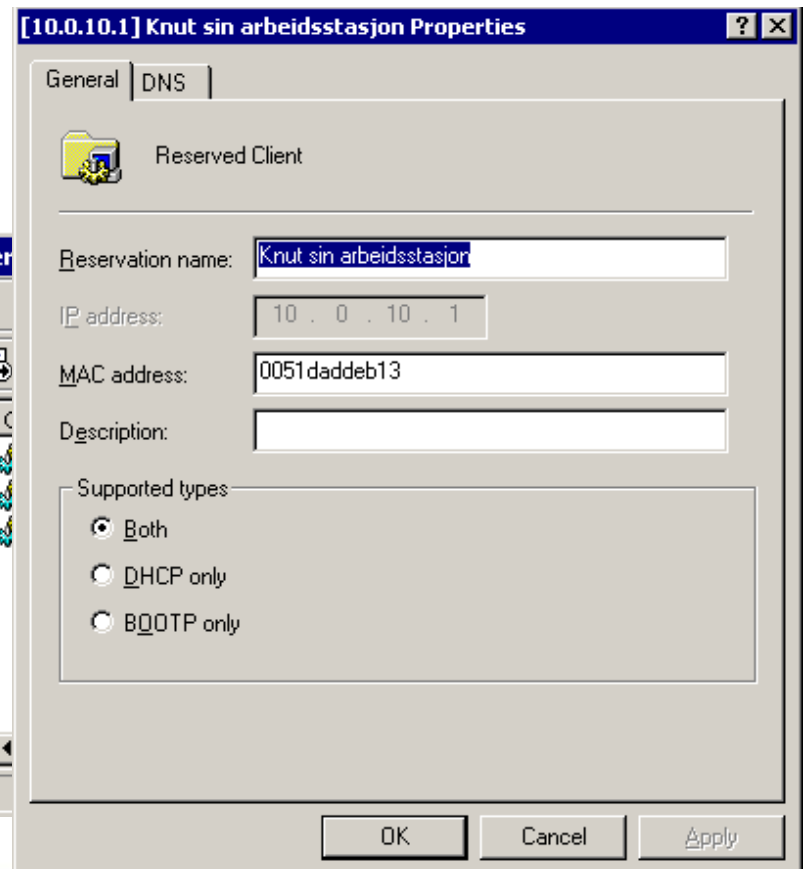
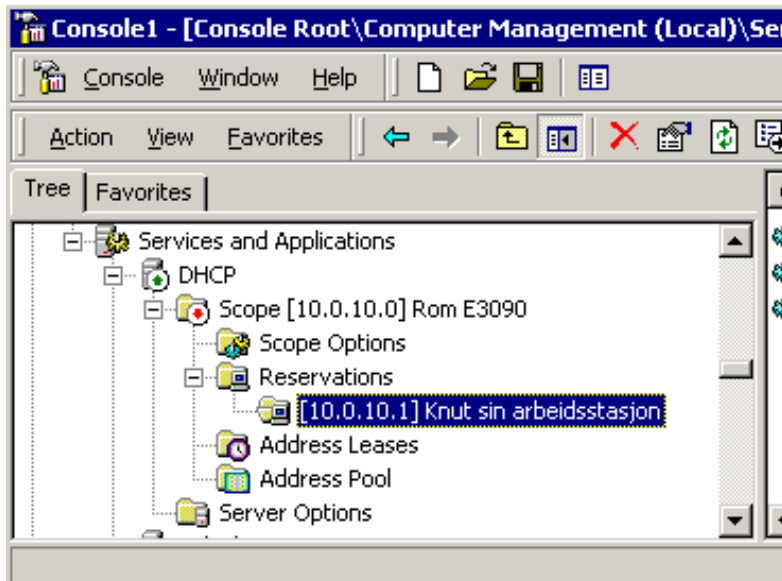
Adresseområde,
subnettmaske og varighet

The screenshot shows the 'DNS' tab of the DHCP scope properties dialog. It contains a text box with the instruction: 'You can set up the DHCP server to automatically update name and address information on DNS servers that support dynamic updates.' Below this are four checkboxes: 'Automatically update DHCP client information in DNS' (checked), 'Update DNS only if DHCP client requests' (selected with radio button), 'Always update DNS' (unselected with radio button), 'Discard forward (name-to-address) lookups when lease expires' (checked), and 'Enable updates for DNS clients that do not support dynamic update' (unchecked). A paragraph at the bottom states: 'Updates are sent to DNS servers configured in TCP/IP properties for network connections active at this server.' Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom.

Politikk for oppdatering av DNS 34

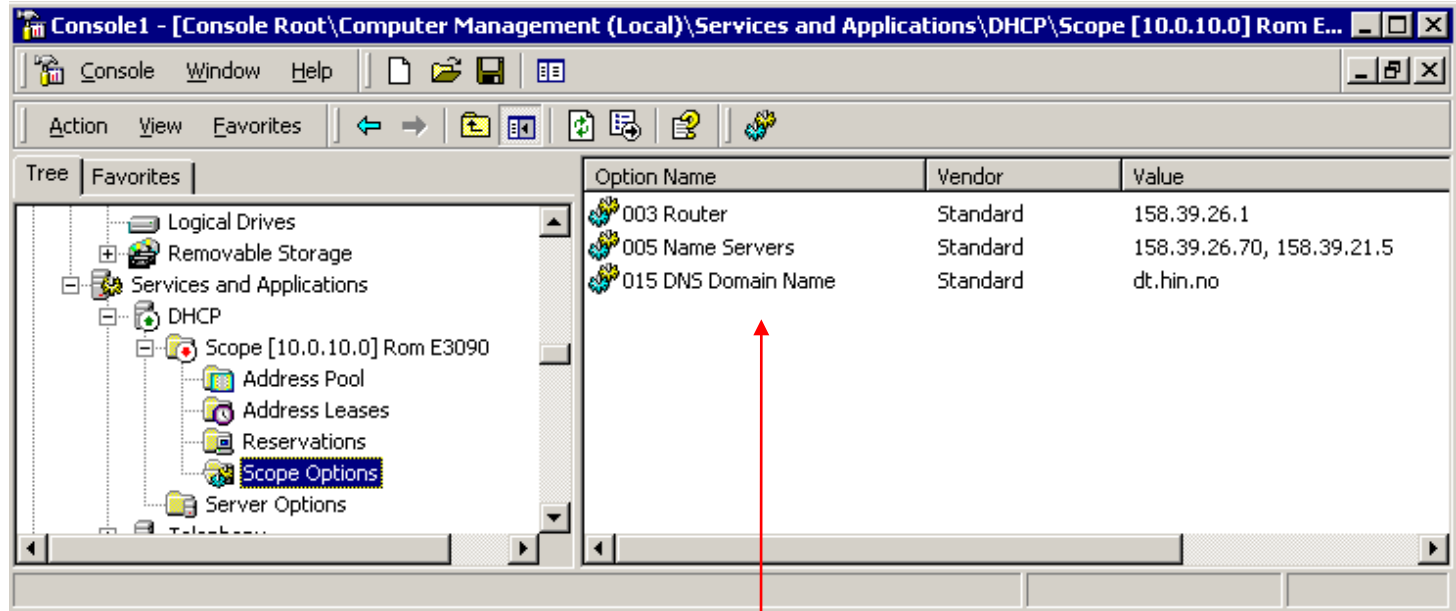
DHCP reserverasjoner

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



The screenshot shows the DHCP console window for a scope named 'Scope [10.0.10.0] Rom E3090'. The 'Scope Options' folder is selected in the tree view. The main pane displays a table of configured options:

Option Name	Vendor	Value
003 Router	Standard	158.39.26.1
005 Name Servers	Standard	158.39.26.70, 158.39.21.5
015 DNS Domain Name	Standard	dt.hin.no

A red arrow points to the table, indicating the configuration of these options.

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

DHCP admin fra webmin

The screenshot shows the Webmin interface for editing a DHCP subnet. The browser window title is "Edit Subnet - Mozilla" and the address bar shows "http://192.168.0.1:10000/dhcpd/edit_subnet.cgi?id=7". The Webmin navigation bar includes links for "Webmin", "System", "Servere", "Nettverk", "Maskinvare", "Cluster", and "Andre". The "Edit Subnet" page is titled "Edit Subnet" and contains the following configuration fields:

- Subnet description:** [Empty text field]
- Network address:** 192.168.0.0
- Netmask:** 255.255.0.0
- Address ranges:** 192.168.0.10 - 192.168.0.11
- Dynamic BOOTP ?:** Dynamic BOOTP ?
- Shared network:** <None>
- Default lease time:** Default secs
- Boot filename:** None
- Maximum lease time:** Default secs
- Boot file server:** This server
- Server name:** Default
- Lease length for BOOTP clients:** Forever secs
- Lease end for BOOTP clients:** Never
- Dynamic DNS enabled?:** Ja Nei Default
- Dynamic DNS domain name:** Default
- Dynamic DNS reverse domain:** Default
- Dynamic DNS hostname:** From client
- Allow unknown clients?:** Allow Deny Ignore Default
- Hosts directly in this subnet:** gandalf
- Groups directly in this subnet:** [Empty dropdown]

Buttons at the bottom of the form include "Lagre", "Edit Client Options", "List Leases", and "Slett". Below the form are links for "Add a new host" and "Add a new host group". The status bar at the bottom indicates "Transferring data from 192.168.0.1..."

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

