Universitetet i Sørøst-Norge

6105 Windows Server og datanett

Leksjon 11b Navnetjenesten DNS – Domain Name System

- Oppbyggingen av navnesystemet DNS
- Administrasjon og registreringsenheter
- DNS-klient, DNS-tjener og navneoppslag
- DNS-soner og DNS-databasen
- DNS-tjener i Windows Server

Pensum

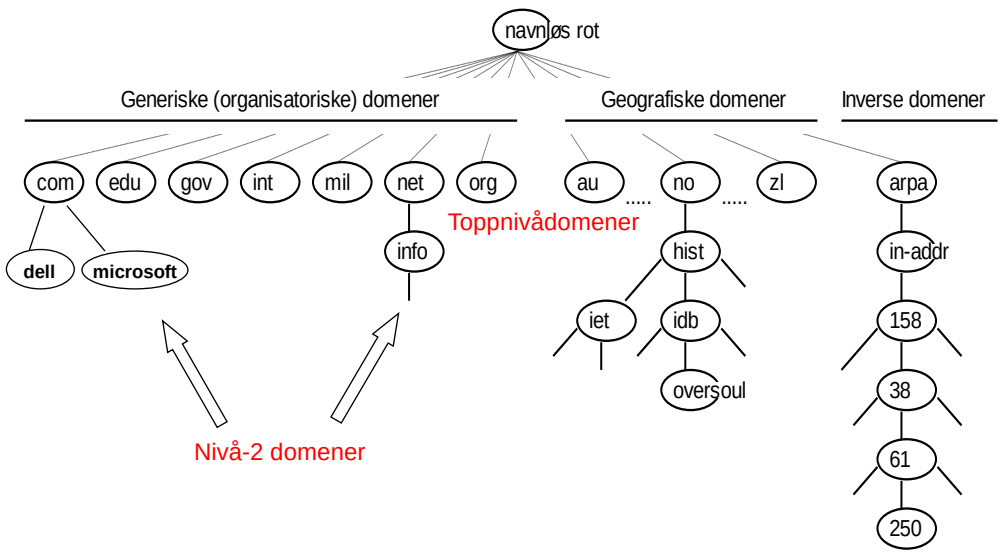
- Kvisli: *Windows Server og datanett*, Kapittel 15 DNS – Domain Name System

Relevante lenker

- Wikipedia: Domain Name System
- Microsoft Docs: Domain Name System (DNS)
- Microsoft Docs: DNS Resource Record Management

1

DNS - Domain Name System



2

DNS - Domain Name System

- **Hovedhensikt**
  - Tillate bruk av maskin-/domenenavn istedet for IP-adresser
- **DNS-domene (DNS *Domain*)**
  - DNS er en hierarkisk struktur av *domener* som utgjør *DNS-navneområdet* (DNS-namespace)
  - Eksempel på *domenenavn*: `sales.microsoft.com`
  - DNS-domener er ikke det samme som Windows/AD domener!
    - » Men Windows bruker DNS som navnetjeneste for AD domener
- **Vertsnavn (*Host Name*)**
  - Hver maskin gis et *vertsnavn* i domenet
  - Eksempel: `computer1`
- **Fullt kvalifisert domenenavn - FQDN (*Fully Qualified Domain Name)***
  - Identifiserer entydig hver node (maskin) i domenetreet
  - FQDN = vertsnavn + domenenavn
  - Eksempel: `computer1.sales.microsoft.com.`

Obs! Det siste punktumet hører med i FQDN !

3

DNS - Domain Name System

- **Rot-domenet**
  - Navnløst
- **Toppnivådomene (TDL)**
  - Generiske (organisatoriske) toppnivådomene (gTLD)
    - » Administreres av ICANN
    - » De fleste brukerorganisasjoner i USA tilhører ett av disse.
    - » Nye generiske toppnivådomener blir opprettet av og til
      - Usponsede domener som administreres av ICANN :.biz, .info, .name, .pro
      - Sponsede domener som administreres av andre:.aero, .coop, .museum
  - Geografiske toppnivådomener (ccTDL)
    - » To-bokstavs forkortelser for land eller andre geografiske områder
    - » Administreres av **nasjonale** DNS-administratorer
  - Inverse domener
    - » Brukes for *reverse-lookup* (finne vertsnavn fra IP-adresse)
- **Nivå-2 domener**
  - administreres av den som har fått tildelt domenenavnet.

Informasjon om nye generiske toppnivådomener:
https://newgtlds.icann.org/en/

Oppdatert liste over toppnivådomener (ICANNS rotsone database)
https://www.iana.org/domains/root/db

4

Administratorer / registreringsenheter

ICANN (icann.org) administrerer rotdomenet
- tildeler nye toppnivådomener (svært restriktivt)

NORID (norid.no) administrerer toppnivådomenet .no
- tildeler nivå-2 domener under .no
- vedlikeholder sentral database over alle norske domener
- bestemmer regelverket for norske domener:
  - **Bedrifter** og **organisasjoner** registrert i Enhetsregisteret: inntil 100 domenenavn direkte under *.no*
  - **Privatpersoner** over 18 år, registrert i Folkeregisteret: inntil 5 domenenavn direkte under *.no* + inntil 5 domenenavn direkte under *priv.no*
- Søknaden må sendes inn av en **registrar** som har avtale med Norid.

Kilde: NorID. Regelverk for norske domenenavn

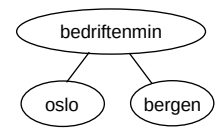
Registrarene "selger" og registrerer nivå-2 domener til sluttkunder
- ISP'er og webhotell-tilbydere er gjerne også registrarer
- Eks: domenetorget.no domene.shop
- Priseksempler: 125-140 kr. pr. år for .no domene, 90-95 kr. pr. år for .com domene

Administrerer sine egne domener på nivå-2.
- Kan fritt lage subdomener på egen DNS-tjener

5

Private navneområder i DNS

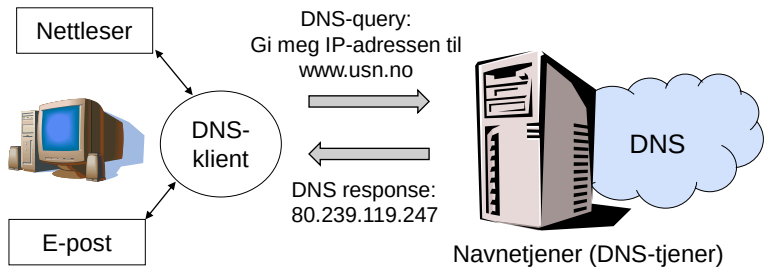
- **Private navneområder**
  - DNS-navnerom med domener som ikke er knyttet til Internett
  - Rotnivået administreres av en privat DNS-rot-tjener
  - Domenenavn kan velges fritt innenfor et privat navneområde
  - Kan opprettes av alle, men må holdes isolert fra DNS-tjenere i Internett
  - Beregnet for lukkede bedriftsinterne nett
  - Brukes lite i praksis fordi de fleste ønsker å ha et offisielt Internett domene



- **DNS-domener og AD domener**
  - AD bruker DNS som navnetjeneste
  - AD krever at DNS-tjener er tilgjengelig (f.eks. installert på domenekontroller)
  - AD kan brukes med offisielt Internett-domene eller privat navneområde

6

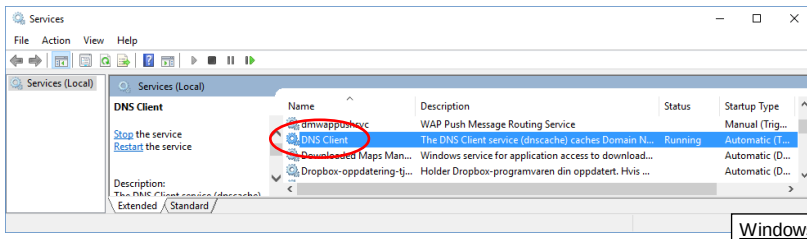
Navnetjenesten DNS



- **En HTTP forespørsel sendes alltid til webtjeneren IP-adresse**
- **Maskin/domenenavn i URL'en må først oversettes til IP-adresse**
- **Dette gjøres ved et DNS-oppslag (query) til en DNS-navnetjener**
  - Utføres av en DNS-klient (DNS-resolver) på klientmaskinen
- **De fleste Internett-applikasjoner benytter seg av DNS**

7

DNS-klient (resolver) i Windows



Windows kommandoer:

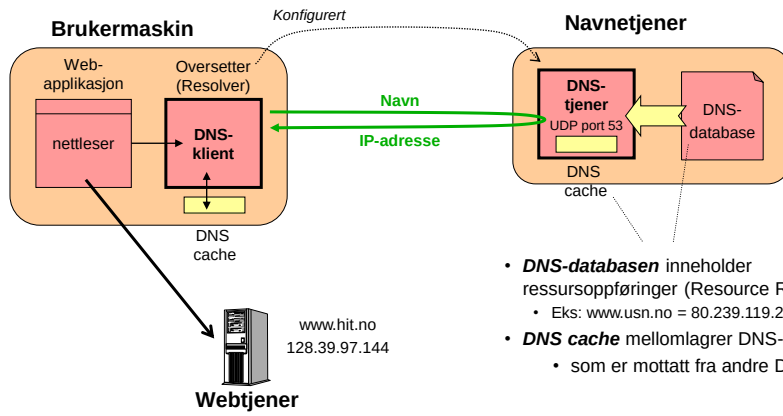
nslookup *navn / IP-adr*	- gjør DNS-oppslag
ipconfig /displaydns	- viser lokalt DNS cache
ipconfig /flushdns	- tømmer lokalt DNS cache

- **DNS-klient (DNS Resolver)**
  - Installert på hver maskin i nettet
  - Kjører som en tjeneste i Windows (*DNS Client*)
  - Applikasjoner bruker DNS-klienten for å gjøre DNS-oppslag mot DNS-tjener
- **DNS-buffer (DNS cache) på klient**
  - DNS-klienten lagrer IP-adresser den har funnet tidligere
  - Sjekker alltid sitt eget DNS-buffer (DNS cache) før den spør andre DNS-tjenere
- **DNS-tjeneren tilbyr to typer oppslag**
  - *Forward Lookup Query* Finner IP-adresse til oppgitt maskin/domenenavn
  - *Reverse Lookup Query* Finner domenenavn til oppgitt IP-adresse

8

DNS-klient og -tjener

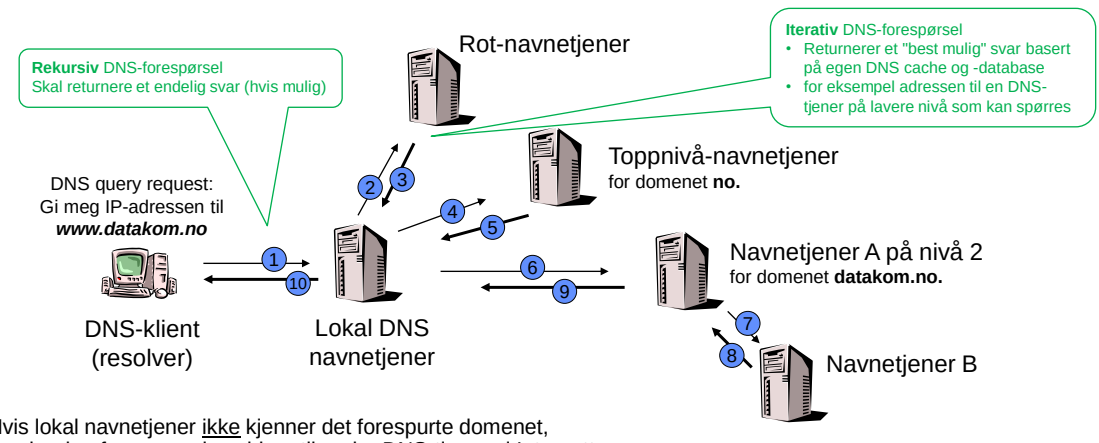
- **Et DNS-oppslag (lookup) består av to DNS-meldinger:**
  - Fra klient: *DNS query* med domenenavn
  - Fra tjener: *DNS response* med tilhørende IP-adresse



- ***DNS-databasen*** inneholder ressursoppføringer (Resource Records)
  - Eks: www.usn.no = 80.239.119.247
- ***DNS cache*** mellomlagrer DNS-data
  - som er mottatt fra andre DNS-tjenere

9

Navneoppslag med DNS



Hvis lokal navnetjener ikke kjenner det forespurte domenet,
sender den forespørselen videre til andre DNS-tjenere i Internett.

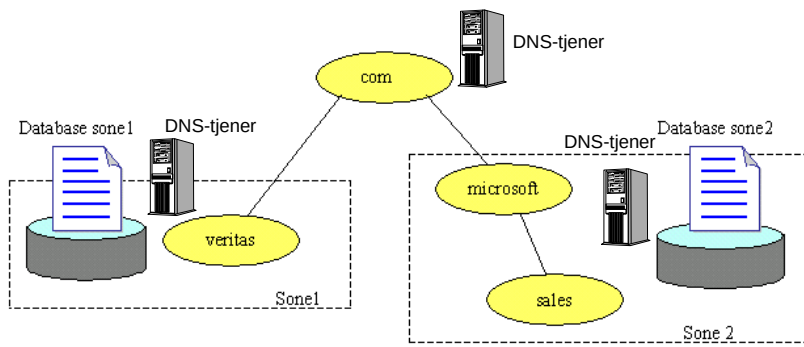
10

Navneoppslag med DNS

Hierarkisk navneoppslag i DNS

- **Klient sender FQDN til sin lokale navnetjener (1)**
  - som først sjekker sin egen DNS cache og navnedatabase
  - hvis IP-adressen finnes der, returneres denne til DNS-klienten
- **Lokal navnetjener spør rot-navnetjener (2)**
  - Alle DNS-tjenere kjenner IP-adressen til en håndfull rot-navnetjenere i Internett !
  - returnerer IP-adressen til navnetjener for toppnivådomènet (3)
- **Lokal navnetjener spør navnetjener for toppdomenet (4)**
  - returnerer IP-adressen til navnetjener for nivå2-domènet (5)
- **Lokal navnetjener spør navnetjener for nivå2-domènet (6)**
  - navnetjeneren **kan** videresende forespørsel til andre navnetjenere (7/8)
  - navnetjeneren som finner den endelig IP-adressen returnerer denne til lokal navnetjener (9)
- **Lokal navnetjener videresender IP-adressen til DNS-klienten (10)**
- **Klienten returnerer IP-adressen til applikasjonen, f.eks. nettleseren.**
  - Først nå kan klientapplikasjonen kontakte tjeneren

DNS-soner og tjenere



DNS-soner og -tjenere

- **DNS-sone (Namespace Zone)**
  - Område av sammenhengende domener
    - » f.eks. domenene microsoft.com og sales.microsoft.com
  - *Sonenavn* er navn på det høyeste domenet i sonen
    - » f.eks. microsoft.com
  - Administreres av én organisasjon
  - Må inneholde minst én DNS-tjener (*primær DNS-tjener*)
    - » denne lagrer den primære navnedatabasen for sonen
  - Kan inneholde flere DNS-tjenere (*sekundære DNS-tjenere*)
    - » disse har kopier av navnedatabasen på den primære DNS-tjeneren
- **DNS-tjener**
  - Maskin som kjører et DNS-tjenerprogram (f.eks. BIND i UNIX/Linux)
  - Lagrer en DNS-navnedatabase med informasjon om en DNS-sone
  - Lagrer vertsnavn og IP-adresse til alle maskiner i den lokale DNS-sonen
    - » Kalles *autorativ tjener* for denne informasjonen
  - Én DNS-tjener kan betjene flere soner, men vanligvis bare én.

13

DNS-databasen

- **Hver DNS-tjener har en DNS-"database"**
  - Inneholder data i form av *resource records* (*ressursrader* i DNS-databasen)
  - Hver resource record angir en ressurs (maskin eller tjeneste) i den lokale DNS-sonen
- **Flere typer ressursrader (resource records):**

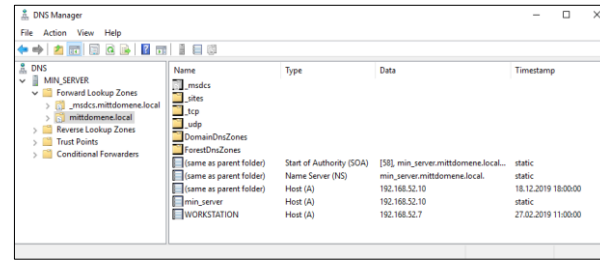
A	Address	IP adresse til fysisk maskin (IP v.4) Eksempel: min_server A 192.168.52.10
AAAA	IPv6 address	IP v.6 adresse til fysisk maskin Eksempel: min_server AAAA F800::0
CNAME	Alias	Aliasnavn for en fysisk maskin (f.eks. www) Eksempel: www CNAME min_server.mittdomene.local
MX	Mail Exchanger	Hostnavn til epost-tjener for et epost-domene Eksempel: @ MX 1 min_server.mittdomene.local
SRV	Service location	Hostnavn og portnr til tjenester, f.eks. LDAP Eksempel: _ldap._tcp SRV 0 0 389 min_server.mittdomene.local
NS	Name Server	IP adresse til DNS-navnetjeneren for ett domene Eksempel: @ NS min_server.mittdomene.local
SOA	Start of Autority	Opplysninger om DNS-domenet / administratoren
PTR	Pointer	Brukes i reverse lookup soner

14

DNS-tjener i Windows Server

- **Sonetyper i Windows**
  - *Active Directory-Integrated*
    - » Sonedata blir en del av AD og replikeres av AD
    - » DNS-tjener må være AD domenekontroller
  - *Standard Primary*
    - » Én primær DNS-tjener lagrer sonedata
    - » Disse kan replikeres til sekundære DNS-tjenere
  - *Standard Secondary*
    - » Sonedata er kopi av *Standard Primary* sone
- **To typer soner på en DNS Server**
  - *Forward Lookup Zones*
  - *Reverse Lookup Zones*

Server Manager → Tools → DNS



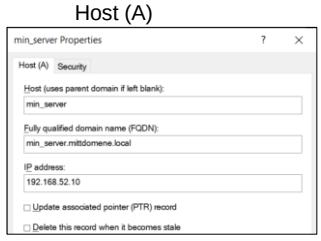
- **Dynamisk oppdatering av DNS**
  - DNS-databasen i Windows kan oppdateres automatisk fra andre programmer
  - DNS-klienten oppdaterer DNS-databasen automatisk når maskinen mottar IP-adresse fra DHCP
- **Replikering**
  - Endringer i DNS-databasen kan kopieres til andre navnetjenere i sonen
  - Benyttes for feiltoleranse og lastbalansering (spredning av belastning på flere tjenere)

DNS-tjener i Windows Server

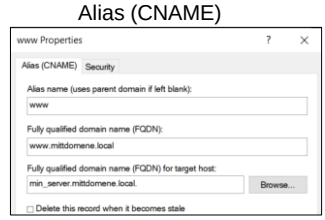
- **To *resource records* opprettes automatisk med DNS-tjeneren:**
  - Start of Authority (SOA) informasjon om DNS-sonen
  - Name Server (NS) navn (FQDN) på DNS-tjeneren for sonen

- **Manuellt registrerte resource records:**

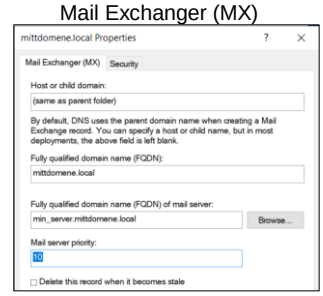
Host (A)



Alias (CNAME)

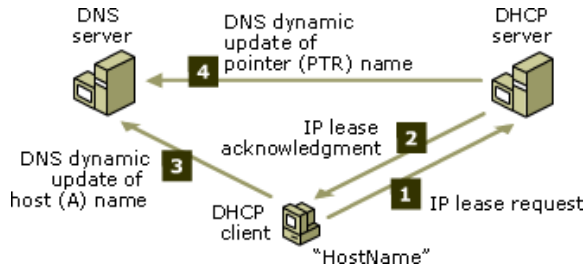


Mail Exchanger (MX)



- **Dynamisk DNS-tjener (DDNS)**
  - Resource records i DNS-tjeneren registreres/oppdateres automatisk fra andre programmer
  - Eks: DNS-klient registrerer Host (A) records i DNS Server

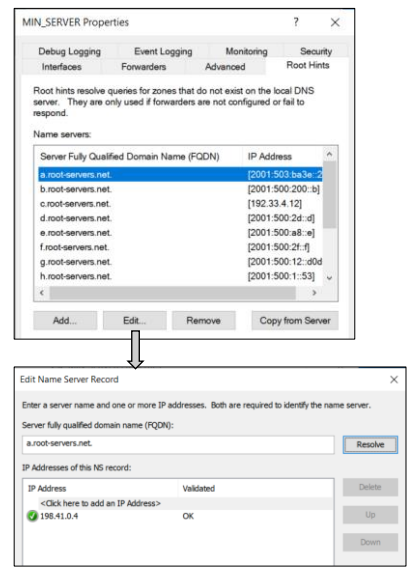
Dynamisk DNS-oppdatering



- **Hva er dynamisk DNS-oppdatering?**
  - DNS-databasen oppdateres automatisk når klienter får sin IP-adresse dynamisk fra DHCP-tjener
    - » DHCP-klienten legger inn A-record med eget hostnavn og den tildelte IP-adressen
    - » DHCP-tjeneren oppdaterer PTR-recorden (kobling IP-adresse til navn)

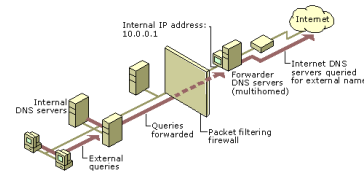
Rot-tjenere (root-hints)

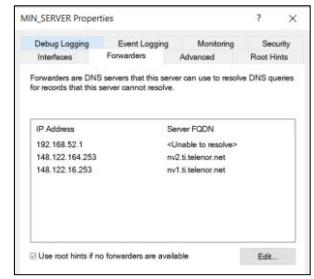
- **Bare på DNS-tjenere**
  - Ikke klienter
- **Fil med IP adresser til DNS-rot-tjenere på Internett**
  - Windows: C:\WINDOWS\system32\Dns\Cache.dns
  - UNIX/Linux: /var/named/root.hints
- **Innholdet leses inn i internminnet når DNS-tjeneren starter**
- **Listen kan oppdateres fra en rot-tjener (*Copy from server*)**



Videresending til andre DNS-tjenere (forwarding)

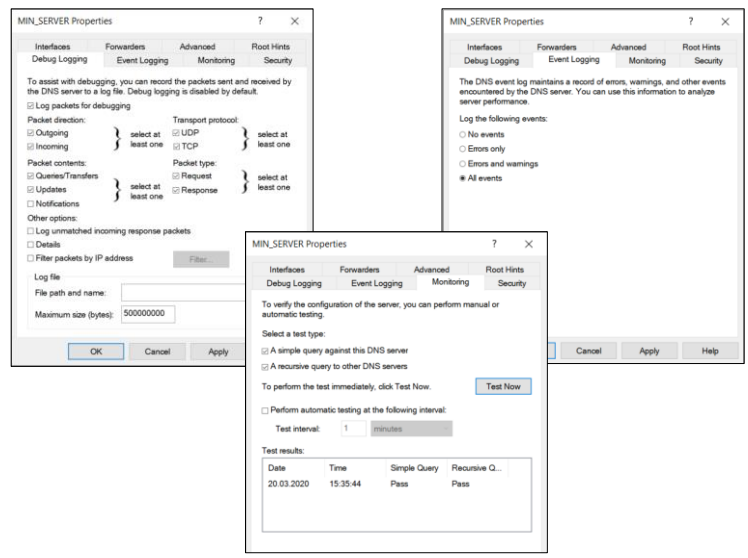
- **Forwarder**
  - En DNS-tjener utenfor eget nett som brukes for å gjøre oppslag av eksterne DNS-navn
- **Virkemåte**
  - Den interne DNS-tjeneren har DNS-navn for maskiner i eget domene
  - DNS-forespørsler om navn utenfor eget domene videresendes (forwardes) til en ekstern DNS-tjener (forwarder)
  - Hvis DNS-tjeneren ikke kjenner noen annen DNS-tjener, kan rot-tjenerne benyttes som forwardere





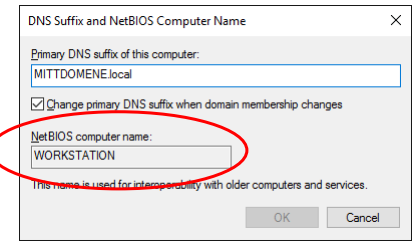
Testing og logging i DNS

- **Logging av DNS-pakker**
  - Kun for debugging!
- **Logging av hendelser**
- **Test av forespørsler**
  - Mot denne tjeneren
  - Mot andre DNS-tjenere



Andre navnesystemer i Windows (ikke pensum)

- **Windows vil alltid bruke først DNS hvis DNS er tilgjengelig !**



- **NetBIOS Name Service (NBNS)**
  - Navnesystem laget av Microsoft for eldre Windows versjoner uten DNS
  - Finnes fremdeles i Window Server 2012, og Windows 7/10 (!)
  - Muliggjør bruk av maskinnavn i små nett uten DNS-tjener
  - Flatt navnerom – kun maskinnavn – ingen domenenavn eller hierarkier
  - Tre ulike metoder for navneoppslag:
    - » **Broadcasts** over IPv4 - tjenerløst - ingen konfigurasjon av navnetjener – kun i lag-2 nett
    - » **Windows Internet Name Service (WINS)** – tjenerbasert – kan krysse lag-2 nett
    - » **LMHOST fil** – lokal fil på hver maskin som mapper maskinnavn til adresse (tilsv. host fil i DNS)

- **Link Local Multicast Name Resolution (LLMNR)**
  - Nytt "tjenerløst" navnesystem for IPv6 adresser (kan også brukes på IPv4)
  - Brukes i Windows 7/10 og 2008/2012/2016/2019 hvis DNS ikke er tilgjengelig
  - Aktiveres når du skrur på **Network Discovery** (og **IPv6**)
  - Gjør navneoppslag med *multicast* meldinger til alle maskiner i nettet
  - **Fungerer bare innenfor ett lag-2 nett (LAN) !**