

# Hur integrera Active Directory och DNS?

Rolf Åberg, Simplex System  
<mailto:rolf.aberg@simplex.se>  
<http://simplex.se>  
08-650 25 80

# Innehåll

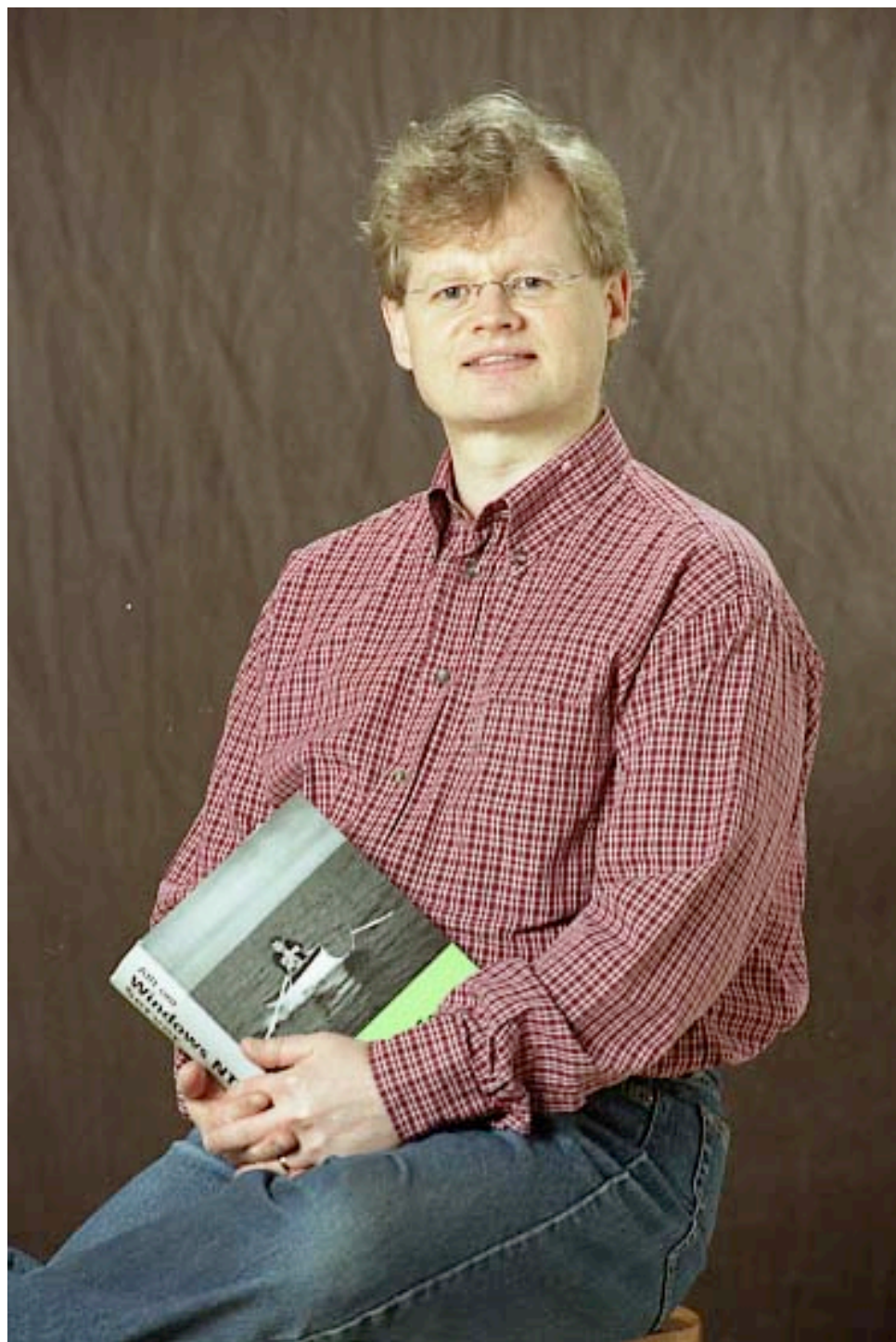
- ◆ Vad används DNS till i en AD-domän?
- ◆ Vad händer i en AD-domän utan DNS-stöd?
- ◆ Kan man använda BIND ihop med AD?
- ◆ Vilka friheter har Microsoft tagit sig med DNS?

# Rolf Åberg och tiden

|      |         |                             |                               |                          |
|------|---------|-----------------------------|-------------------------------|--------------------------|
| 2001 |         | Windows XP/<br>Server 2003  |                               |                          |
| 1999 |         | Windows 2000                |                               |                          |
| 1995 |         |                             | Utbildning, konsult,<br>hack  | Egen (mycket)            |
| 1993 |         | Windows NT                  |                               |                          |
| 1991 |         | Visual Basic,<br>SQL Server | Programutveckling<br>(i smyg) |                          |
| 1990 |         | LAN Manager                 |                               |                          |
| 1989 |         | 3+Open                      |                               |                          |
| 1988 |         | 3+Share                     | Support/Nätadmin.             | Microsoft AB             |
| 1984 | IBM PC  | Pascal                      | Programutveckling             | LKB-Produkter AB         |
| 1983 | ABC 800 | BASIC                       | Programutveckling             | Karolinska<br>Institutet |
| 1980 | ABC 80  | BASIC                       | Programutveckling<br>(exjobb) | KTH                      |

# Rolf Åberg

- ◆ Rolf Åberg har varit systemsupportchef på Microsoft AB och även utvecklat PC-program. Om Visual Basic säger han: »Det enda dataspel jag behöver«. Ett annat specialområde är SQL Server och han har gedigen erfarenhet av hur det är att administrera levande nätverk. Rolf är civilingenjör i grunden och har mångårig vana av utbildning och konsulting inom Windows NT/2000/XP/Server 2003, Visual Basic, C# och SQL Server. Rolfs senaste bok heter »Vägen till Active Directory och Windows 2000/XP/Server 2003«. Sedan en tid knåpar han på en med arbetsnamnet »Windows 2000/Server 2003 på bredden och djupet«. Rolf konsultar och utbildar i det egna företaget Simplex System.
  - <mailto:rolf.aberg@simplex.se>
  - <http://simplex.se>



Active Directory på sju bilder...

# Kungstanken: användare och alla »deras« resurser är samlade på en plats

Triangel = AD-domän



Det finns »inget« för användarna på andra platser. Det spelar ingen större roll när domänkontrollanter på andra platser uppdateras





# Active Directory-platser (AD-platser) avspeglar det fysiska nätverket

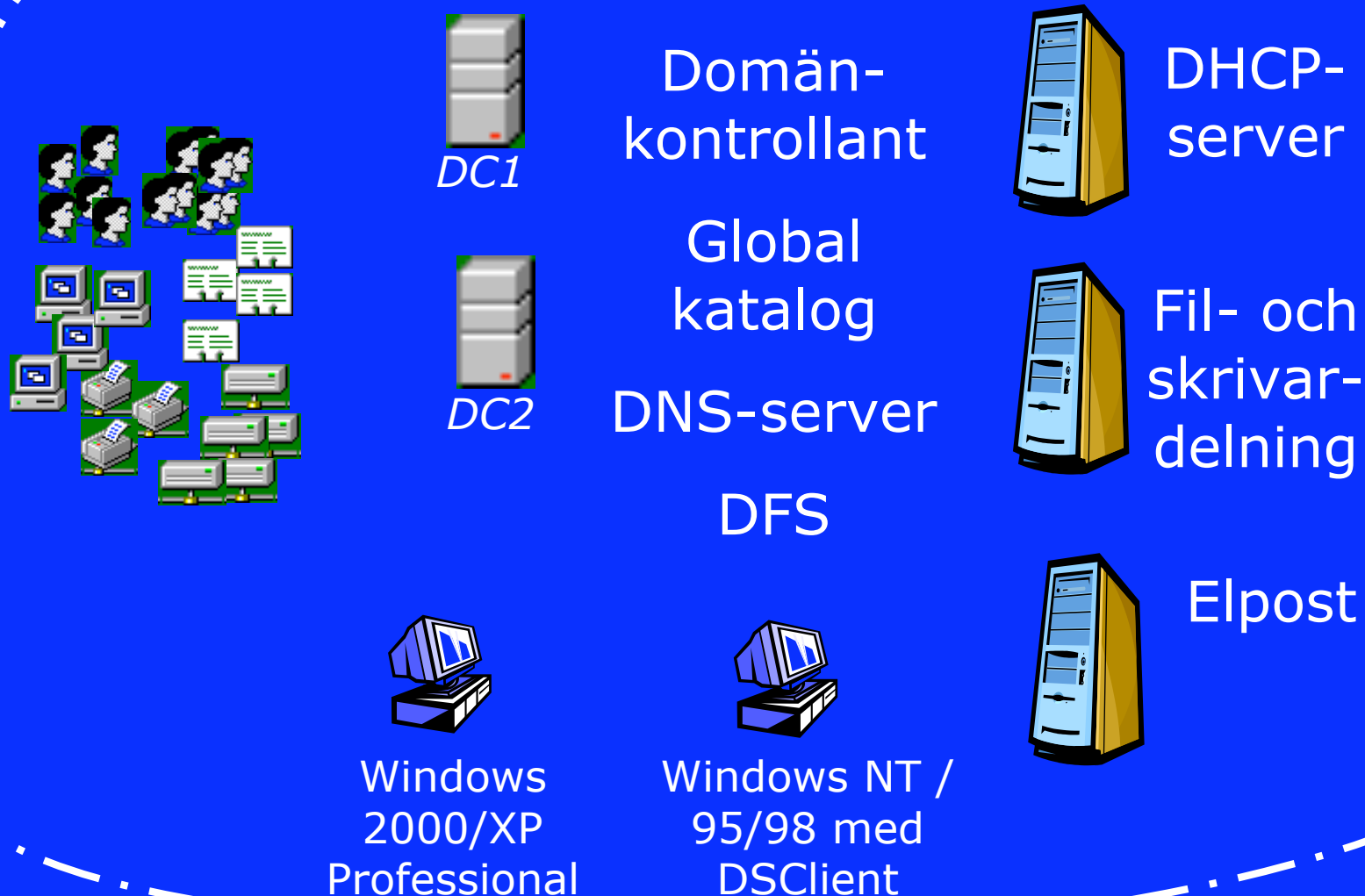
· — = A



Microsoft:  
plats//site

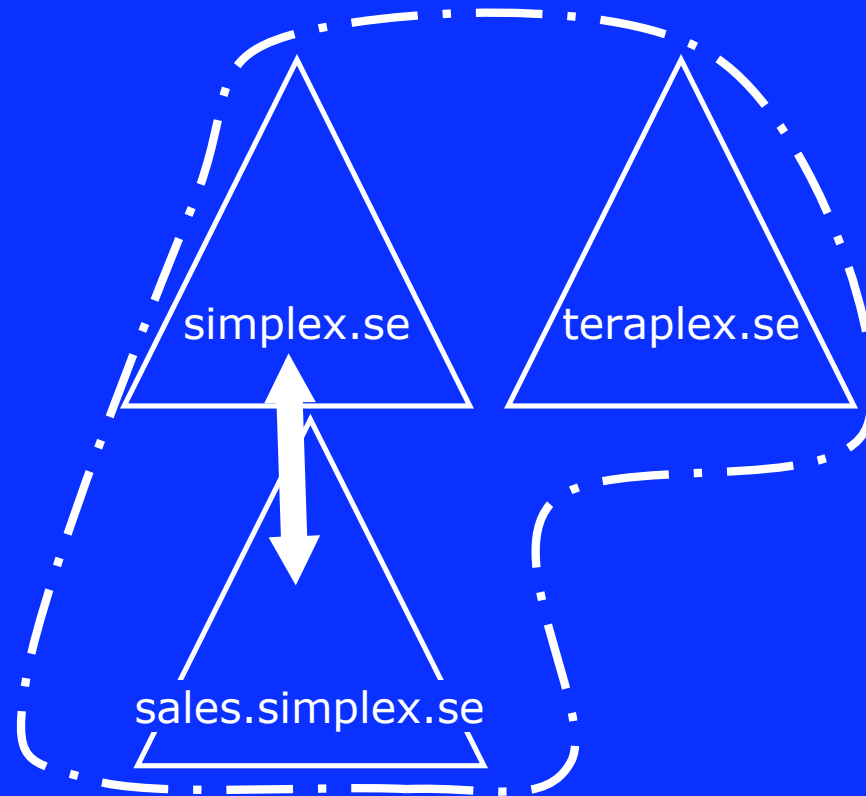


# En »ideal« AD-plats



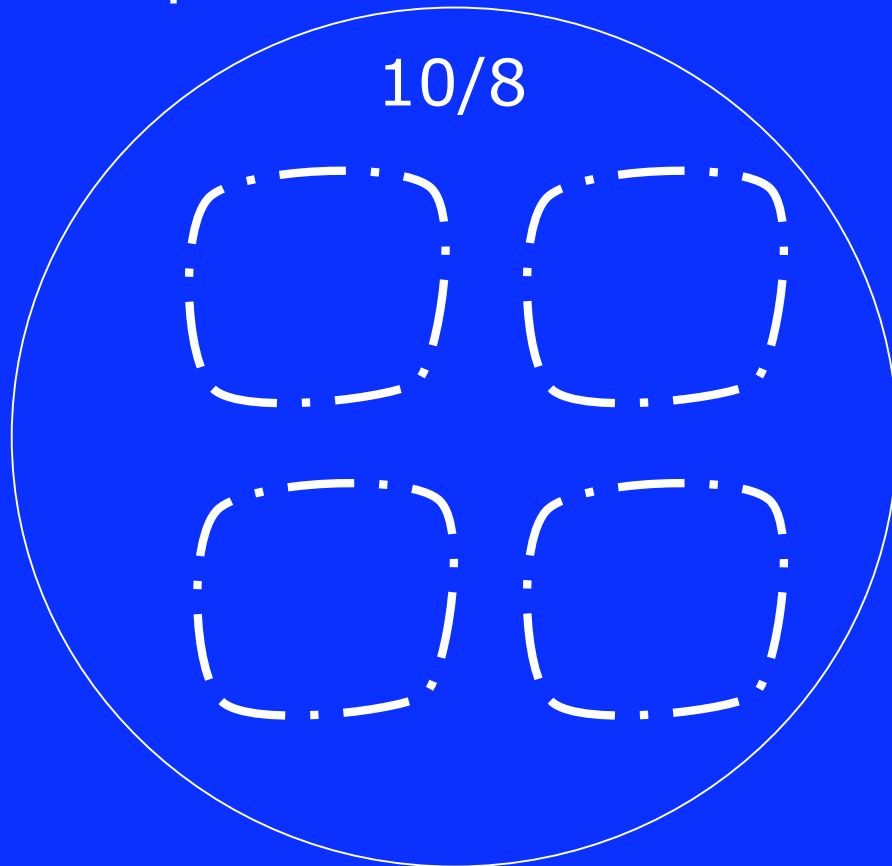
# Koppling mellan AD-plats och domäner

- ◆ En Active Directory-domän kan finnas på många AD-platser
- ◆ En AD-plats kan härbärgera många domäner

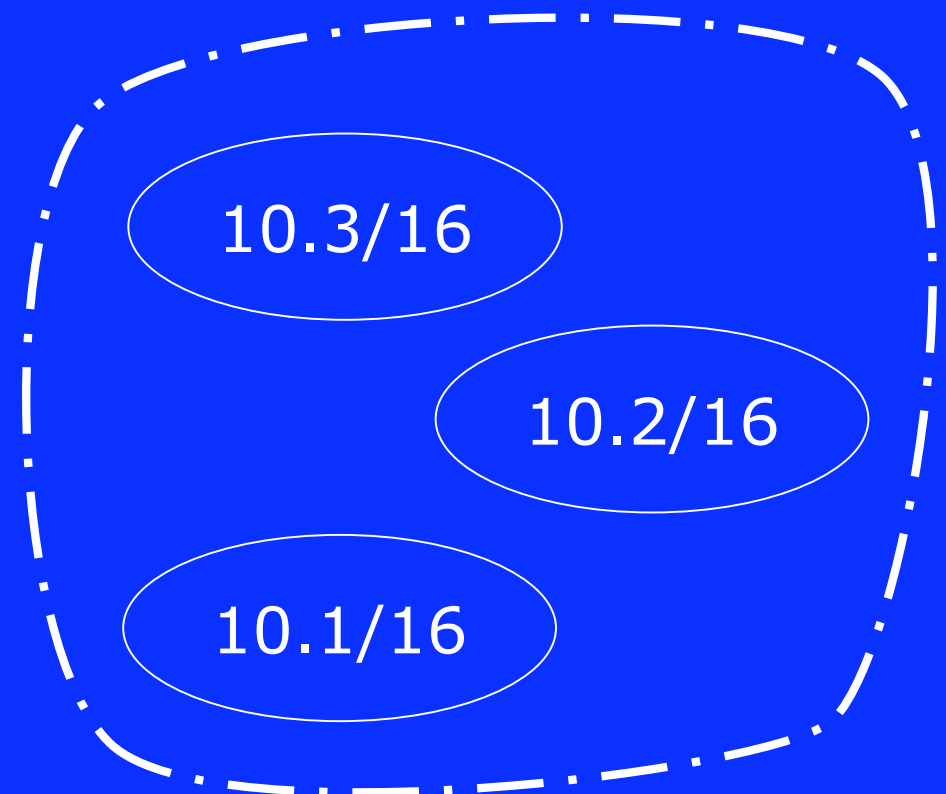


# Koppling AD-plats – IP-subnät

- ◆ Ett IP-subnät kan omfatta flera AD-platser

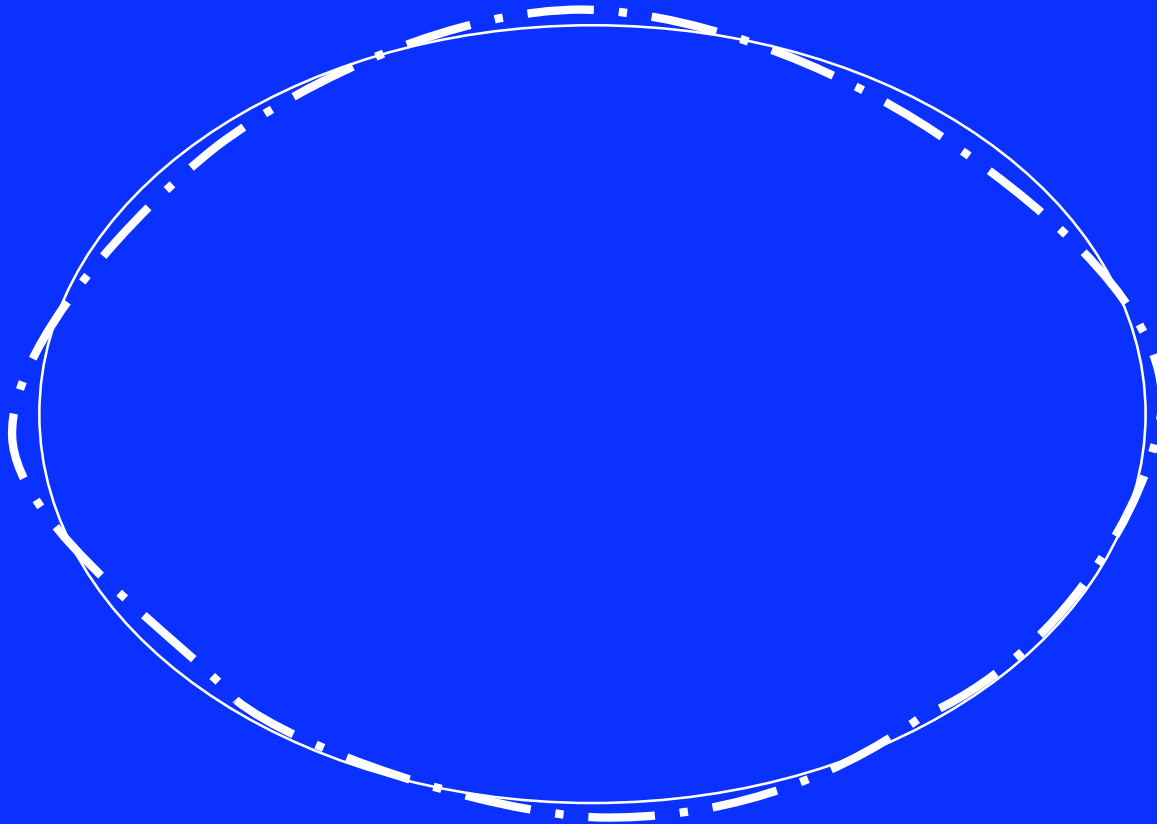


- ◆ En AD-plats kan omfatta många IP-subnät

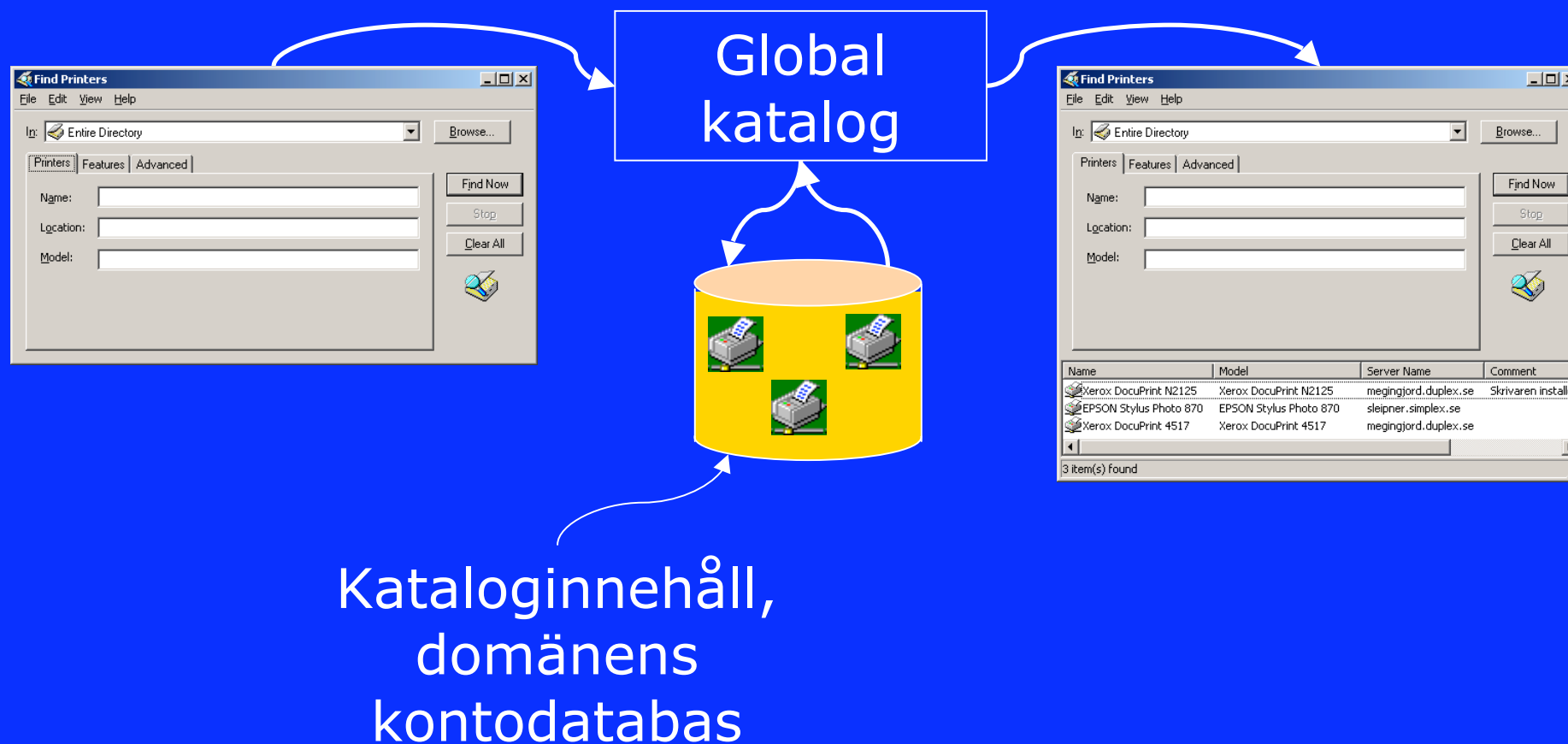


## Koppling AD-plats – IP-subnät, forts.

- ◆ Ett IP-subnät kan omfatta en AD-plats



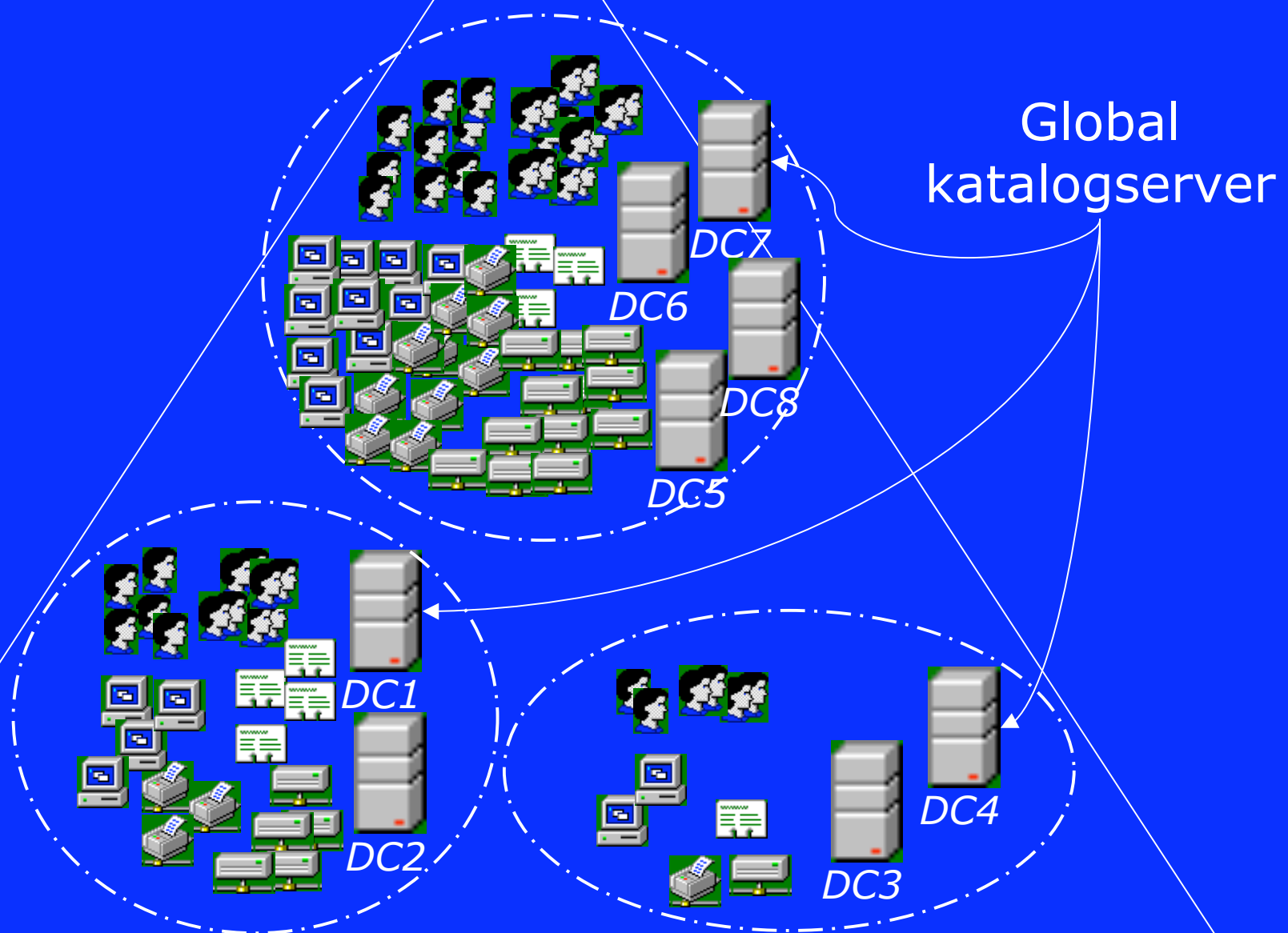
# Den globala katalogen används vid sökning i kataloginnehållet



# Global katalog//Global Catalogue

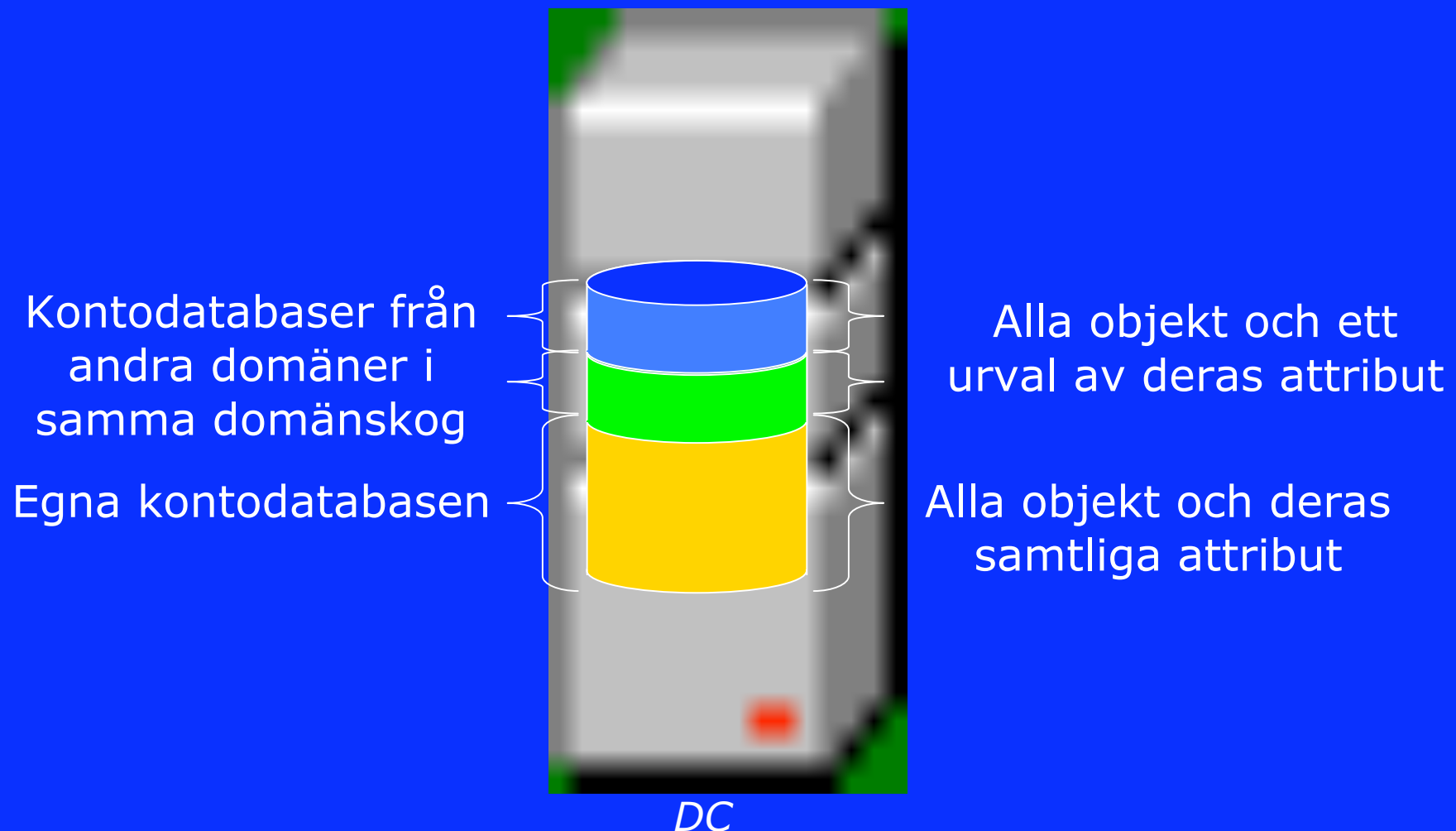
- ◆ En optimering – en GC innehåller en del av Active Directory-databasen
- ◆ En GC innehåller flera domäners AD-innehåll
  - alla objekt, inte alla attribut
  - Innehållsförteckning för en katalog
- ◆ Krävs för att användare skall kunna logga in, i enhetligt läge
  - Uppgift om medlemskap i universella grupper finns i den globala katalogen
- ◆ Placering bestäms av nätverksfysik
  - Nära användaren, räknat i nätverkshastighet

# Skall finnas nära användare





# Flera domäner i domänskogen



Vad används DNS till i en  
AD-domän?

# DNS **krävs** i Active Directory-domäner

- ◆ Windows 2000/XP/Server 2003 kan användas utan DNS-stöd i arbetsgrupp, i Windows NT-domän, i NetWare-nätverk, m.fl.
- ◆ DNS-stöd **krävs** när man använder Windows 2000/XP/Server 2003 i Active Directory-domän

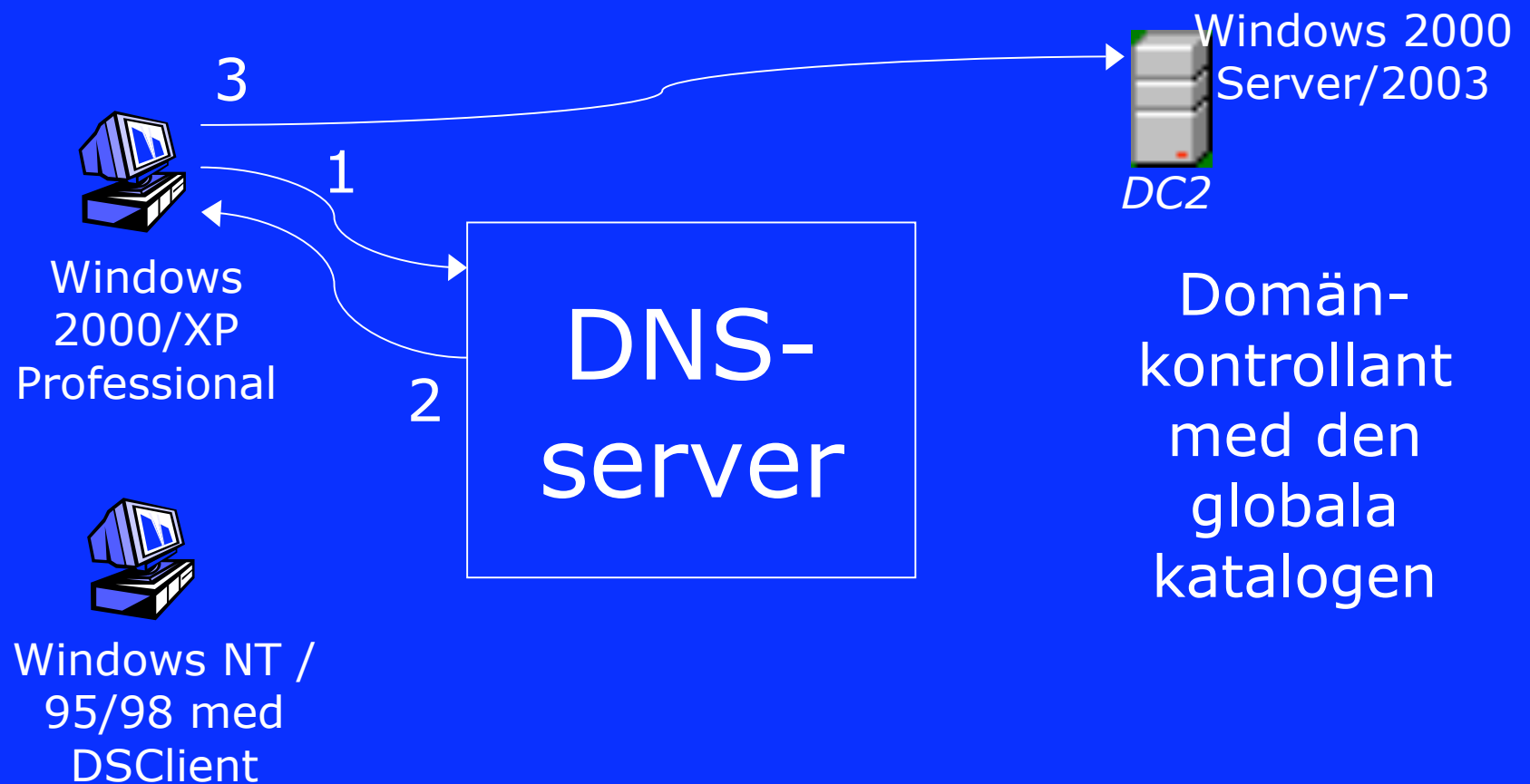
# DNS krävs för ... inloggning av Windows 2000/XP/Server 2003



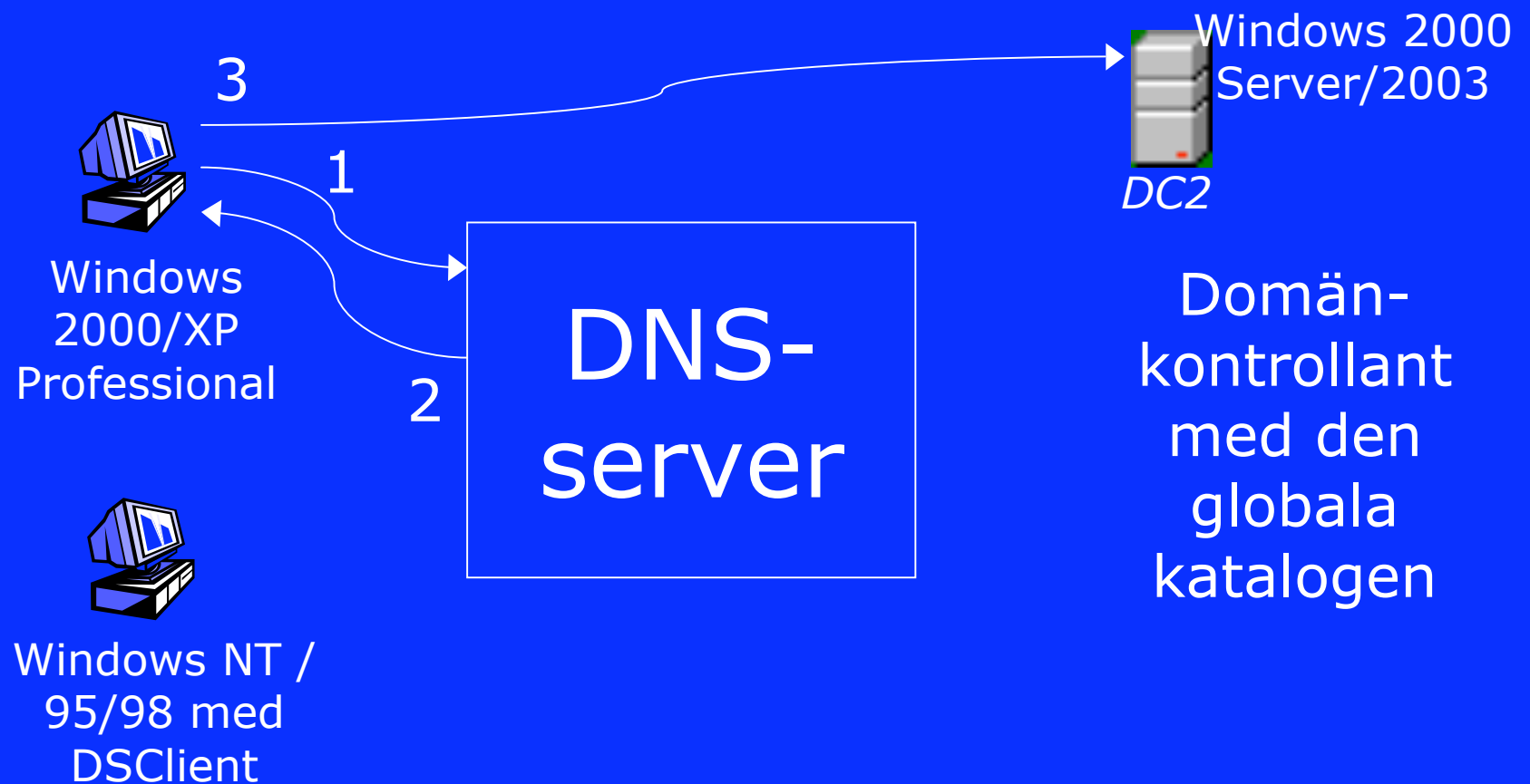
# DNS krävs för ... inloggning av Windows NT/95/98 med DSCClient



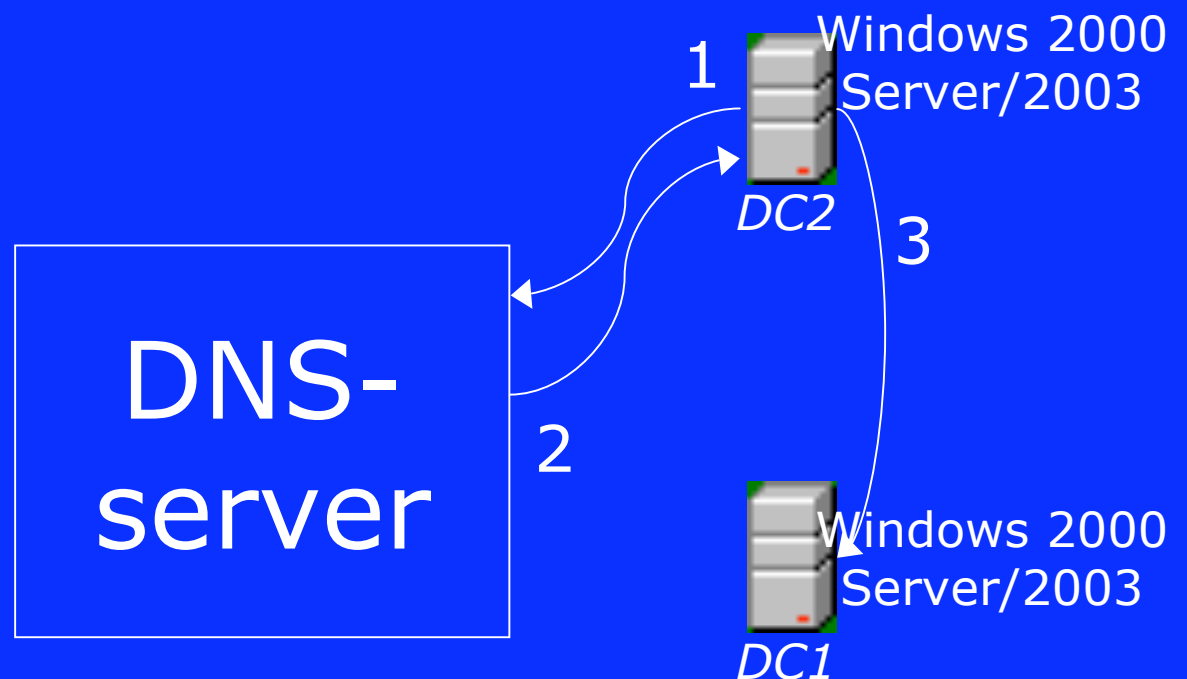
# DNS krävs för ... sökning i den globala katalogen



# DNS krävs för ... LDAP-program

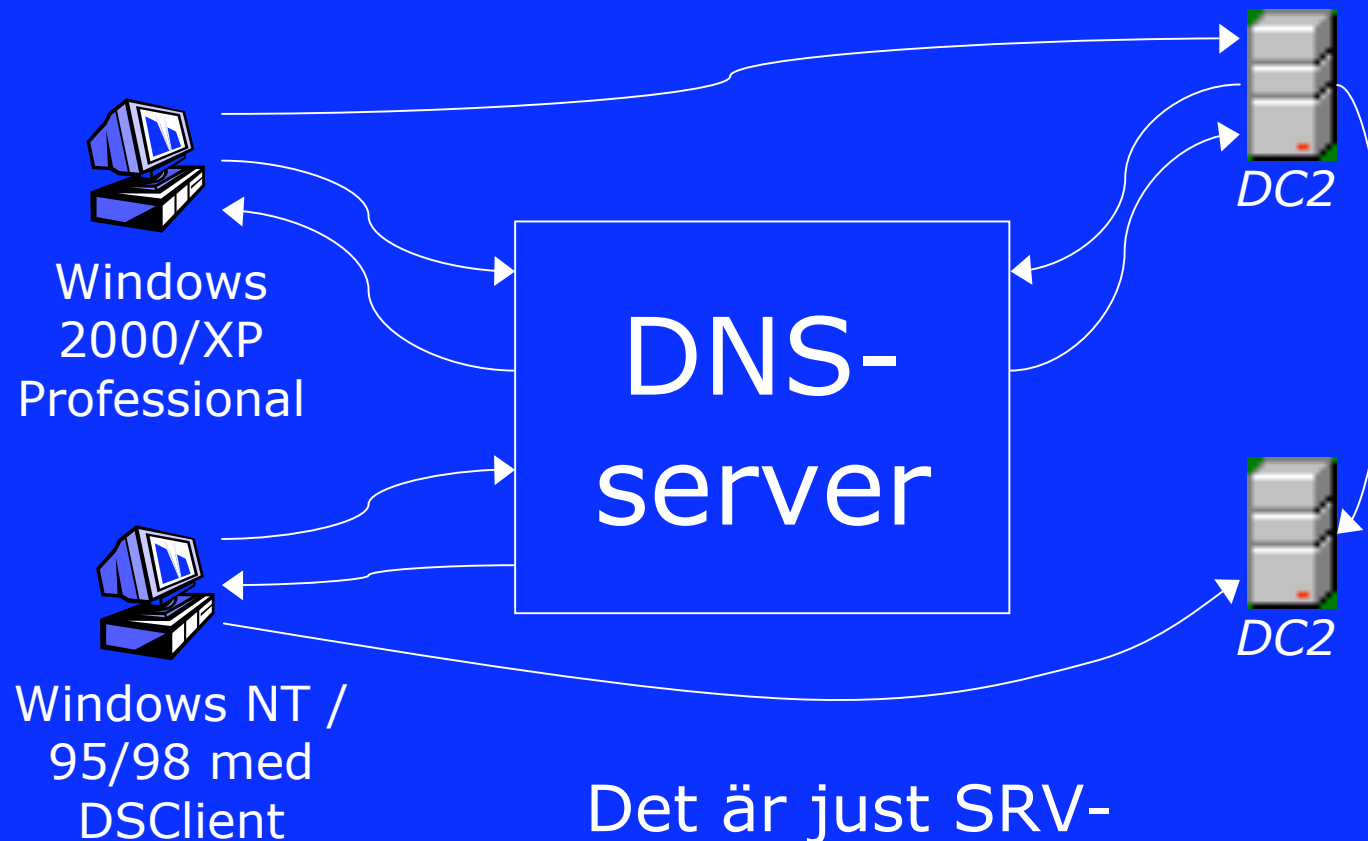


# DNS krävs för ... att domänkontrollanter skall hitta varandra





# SRV-poster



Det är just SRV-  
poster som pekar ut  
domänkontrollanterna

# Microsoft använder ett antal olika SRV-poster

- ◆ Kerberos, inloggning av Windows 2000/XP/Server 2003 och andra Kerberos-klienter
  - för hela domänen
  - alla AD-platser
- ◆ LDAP, för sökningar i katalogtjänsten
  - hela domänen
  - alla AD-platser
- ◆ kpasswd, för Unix-klienter, byte av lösenord
  - hela domänen
  - alla AD-platser

# SRV-poster för domänkontrollant (i AD-moderdomän) i/på AD-plats »HK«

|                                                |     |    |     |   |     |      |                        |
|------------------------------------------------|-----|----|-----|---|-----|------|------------------------|
| _ldap._tcp.simplex.se.                         | 600 | IN | SRV | 0 | 100 | 389  | mekingjord.simplex.se. |
| _gc._tcp.simplex.se.                           | 600 | IN | SRV | 0 | 100 | 3268 | mekingjord.simplex.se. |
| _kerberos._tcp.simplex.se.                     | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _kpasswd._tcp.simplex.se.                      | 600 | IN | SRV | 0 | 100 | 464  | mekingjord.simplex.se. |
| _kerberos._udp.simplex.se.                     | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _kpasswd._udp.simplex.se.                      | 600 | IN | SRV | 0 | 100 | 464  | mekingjord.simplex.se. |
| <i>GUID-för DC:n.</i> _msdcs.simplex.se.       | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _kerberos._tcp.dc._msdcs.simplex.se.           | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _ldap._tcp.dc._msdcs.simplex.se.               | 600 | IN | SRV | 0 | 100 | 389  | mekingjord.simplex.se. |
| _kerberos._tcp.HK._sites.dc._msdcs.simplex.se. | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _ldap._tcp.HK._sites.dc._msdcs.simplex.se.     | 600 | IN | SRV | 0 | 100 | 389  | mekingjord.simplex.se. |
| _ldap._tcp.gc._msdcs.simplex.se.               | 600 | IN | SRV | 0 | 100 | 3268 | mekingjord.simplex.se. |
| _ldap._tcp.HK._sites.gc._msdcs.simplex.se.     | 600 | IN | SRV | 0 | 100 | 3268 | mekingjord.simplex.se. |
| _ldap._tcp.pdc._msdcs.simplex.se.              | 600 | IN | SRV | 0 | 100 | 389  | mekingjord.simplex.se. |
| _ldap._tcp.HK._sites.simplex.se.               | 600 | IN | SRV | 0 | 100 | 389  | mekingjord.simplex.se. |
| _kerberos._tcp.HK._sites.simplex.se.           | 600 | IN | SRV | 0 | 100 | 88   | mekingjord.simplex.se. |
| _gc._tcp.HK._sites.simplex.se.                 | 600 | IN | SRV | 0 | 100 | 3268 | mekingjord.simplex.se. |

# Alla underdomäners DNS-servrar bör vara slavservrar till rotzonen

- ◆ Den globala katalogen används ofta
- ◆ DNS-poster för domänkontrollanter med den globala katalogen finns endast i rotzonen
- ◆ Alltså: alla underdomäner bör låta sina DNS-servrar vara slavservrar till rotdomänens zon

# Krav på DNS-servrar för Active Directory

## ◆ **Måste:**

- SRV-poster (RFC 2782)

## ◆ **Bra:**

- Dynamisk DNS (RFC 2136)
  - » RFC 2137, *Secure Domain Name System Dynamic Update*, används inte!
- Notify (RFC 1996)
- Inkrementella zon-överföringar (RFC 1995)

## ◆ **Vilka finns:**

- BIND 8 och senare
- Microsoft DNS-server i Windows 2000 / Server 2003

Vad händer i en AD-  
domän utan DNS-stöd?

Inte mycket...

Kan man använda  
BIND ihop med AD?



# BIND ihop med AD?

- ◆ Absolut!
- ◆ Problem:
  - Skyddad uppdatering! Microsoft använder RFC 2136, inte RFC 2137 eller RFC 3007
  - I Windows 2000 dokumenterade MS skyddad uppdatering, men gjorde inte som de skrev, osäker på Windows Server 2003

# Sätt att använda BIND

- ◆ »Ensam« DNS-tjänst
  - ex. simplex.se och alla underdomäner
- ◆ Delegera AD-subdomäner till Windows Server 2003
  - ex. simplex.se på BIND,  
\_msdcs.simplex.se, \_tcp.simplex.se,  
\_udp.simplex.se & \_sites.simplex.se på Windows

Vilka friheter har  
Microsoft tagit sig  
med DNS?

# Vilka friheter har Microsoft tagit sig med DNS?

- ◆ Kort svar: inte många!
- ◆ Något längre svar:
  - Man stödjer ännu inte RFC 3007 *Secure Domain Name System (DNS) Dynamic Update*, utan endast RFC 2136
  - Tack vare sin strävan att begränsa nätverkstrafik låter man närmaste DNS-server (om Windows) påstå sig vara Primary Master!

# DNS Security Extensions (RFC 2535)

- ◆ DNSSEC allows RR's and zones to have integrity and encryption.
- ◆ Zones and round robins (RR) are signed with a private key.
- ◆ Windows Server 2003 only provides basic support:
  - Can only act as secondary zone.
  - Cannot sign zones or resource records.
- ◆ DNS server sends both signed and unsigned records in response to a query.
- ◆ Windows Server 2003 client does not authenticate records; it simply passes them to the application.

# New DNSSEC Records

- ◆ KEY: Public key resource record
  - Contains the public key.
- ◆ SIG: Signature resource record
  - Contains the signature.
- ◆ NXT: Next resource record
  - Enables the DNS server to inform the client that a particular domain does not exist.

# DNS Extension Mechanism

- ◆ OPT Resource Record
- ◆ As described in RFC 2671, EDNS0 uses an OPT pseudo-RR that is added to the additional data section of either a DNS request or a DNS response to indicate the sender's ability to handle the extended DNS protocols.
- ◆ It is called a pseudo-RR because it pertains to a particular transport level message and not to any actual DNS data.
- ◆ OPT RR's are never cached, forwarded, stored in, or loaded from zone files.

# DNS Extension Mechanism

- ◆ Allows DNS server to send User Datagram Protocol (UDP) packets larger than 512 bytes.
- ◆ UDP length is defined in the OPT RR that is part of a DNS query.
- ◆ EDNS0 support is server-side, not client-side.
- ◆ EDNS0 cache: Caches support hosts for one month.



# Sammanfattning

- ◆ Vad används DNS till i en AD-domän?
- ◆ Vad händer i en AD-domän utan DNS-stöd?
- ◆ Kan man använda BIND ihop med AD?
- ◆ Vilka friheter har Microsoft tagit sig med DNS?

