Dynamisk DNS och varifrån det kommer...

Rolf Åberg
Duplex Datautbildning AB & Simplex System

Punkter

- DNS, bakgrund och nuläge
- Vad innebär dynamisk DNS
- DNS är från 1980-talet, varför blir det hela dynamiskt först nu?
- Vilka DNS-servrar kan hantera dynamisk uppdatering?
- Inte bara dynamisk uppdatering, utan även inkrementell zonöverföring
- Transaction Signatures, TSIG, löser säkerhets-problemet?
- Varför inte DNSSec för att lösa säkerhetsproblemet?

Punkter, forts.

- Active Directory kan inte användas utan DNS (men dynamisk DNS kan avvaras)
- Hur löser Microsoft säkerhetsproblemet i Windows 2000 Servers DNS-servertjänst?
- DNS-databasen som en del av Active Directory ger flera primära DNS-servrar för en zon

Mål

- Att förstå varifrån dynamisk DNS kommer och de problem och frågeställningar som måste lösas

Upplägg

- Del 1: DNS
- Del 2: Dynamisk DNS
- Del 3: Dynamisk DNS & Microsoft

När får man ställa frågor

Vi människor är olika så ställ frågor när ni vill…

Jag svarar kanske inte på en gång (svaret kan komma senare). Jag har också avsatt tio minuter i slutet till frågor.

Del 1: DNS

DNS, bakgrund och nuläge

Bakgrund

- Problem:
  - Datorer arbetar med siffror
  - Människor föredrar bokstäver, helst namn
  - TCP/IP-världen roterar runt IP-adress (och portnummer)
- Insikt:
  - Uppfinn ett sätt som låter människor använda namn och datorer IP-adresser

Bakgrund, forts.

- Lösning:
  - Datornamn för datorer
  - Tabell med översättning mellan datornamn och IP-adresser
  - Klientprogram som hanterar förfrågan från människa om datornamn, använder tabellen för att ta reda på vilken IP-adress som motsvarar detta namn och låter datorerna kontakta varandra m.h.a. IP-adressen

Begrepp: RFC

- Request For Comments, RFC
  - Den dokumentsamling som bl.a. omfattar Internetstandarder
  - Skrivs av intresserade
  - ”Godkänns” av Internet Engineering Steering Group, IESG, men egentligen av alla Internetanvändare
  - Olika krav om dokumentet beskriver en föreslagen standard eller endast är för information
  - Finns på http://www.rfc-editor.org
  - RFC 2026 The Internet Standards Process – Revision 3
  - Extra viktiga: de med 00 på slutet!

Begrepp: Internet Draft

- Innan en RFC godkänns kallas den Internet Draft och finns på http://www.ietf.org/ID.html
  - Förses med ett bäst-före-datum
  - Vissa leder aldrig till RFC:er
  - (”The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.”)

Standarddokument för DNS

- De standarder som erkänns av IETF (jmf. RFC 2700) för DNS-hantering är
  - RFC 1034 Domain Names – Concepts and Facilities, 1987
  - RFC 1035 Domain Names – Implementation and Specification, 1987
  - RFC 1123 Requirements for Internet Hosts – Application and Support, 1989

How the DNS came till…

I begynnelsen...

- Var Hosts.Txt:

```
NET : 10.0.0.0 : ARPANET :
NET : 128.10.0.0 : PURDUE-CS-NET :
GATEWAY : 10.0.0.77, 18.10.0.4 : MIT-GW.ARPA,MIT-GATEWAY : PDP-11 :
          MOS : IP/GW,EGP :
HOST : 26.0.0.73, 10.0.0.51 : SRI-NIC.ARPA,SRI-NIC,NIC : DEC-2060 :
  TOPS20 : TCP/TELNET,TCP/SMTP,TCP/TIME,TCP/FTP,TCP/ECHO,ICMP :
HOST : 10.2.0.11 : SU-TAC.ARPA,SU-TAC : C/30 : TAC : TCP :
```

- Fanns på 1 (en) dator till vilken alla andra ftp:ade
- Total bandbredd proportionell mot kvadraten på antalet poster (värdar)
- Spec. i RFC 952

Därnäst…

- Många tänkte hårt och länge
  - RFC 799 Internet name domains, 1981
  - RFC 819 Domain naming convention for Internet user applications, 1982
  - RFC 830 Distributed system for Internet name service, 1982
  - RFC 882 Domain Names – Concepts and Facilities, 1983
  - RFC 883 Domain Names – Implementation and Specification, 1983
  - RFC 973 Domain System Changes and Observations, 1986

Fulländning!?

- RFC 1034 Domain Names – Concepts and Facilities, 1987
- RFC 1035 Domain Names – Implementation and Specification, 1987
- Paul Mockapetris
- Mitt favoritcitat från RFC 1035: ”…future dynamic update facilities…”

Nåja, nästan fulländat…

- RFC 1123 Requirements for Internet Hosts – Application and Support, 1989
  - Tillåter domännanm med inledande siffra
- RFC 1886 DNS Extensions to support IP version 6, 1995
- RFC 1995 Incremental Zone Transfer in DNS (IXFER), 1996
- RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), 1996

Arbetet fortsätter

- RFC 2052 A DNS RR for specifying the location of services (DNS SRV), 1996
  - Ersatt av RFC 2782
- RFC 2065 Domain Name System Security Extensions (DNSSEC), 1997
  - Skyddar DNS-posterna på DNS-servrarna
  - Ersatt av RFC 2535

Nu kommer dynamisk uppdatering

- RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE), 1997
  - ”Therefore it is very strongly recommended that the protocols described in this document not be used without [RFC 2137] or other equivalently strong security measures, e.g. IPsec.”
- RFC 2137 Secure Domain Name System Dynamic Update, 1997

Förbättringarna fortsätter, DNSSec

- RFC 2181 Clarifications to the DNS Specification, 1997
- RFC 2308 Negative Caching of DNS Queries (DNS NCACHE), 1998
- RFC 2535 Domain Name System Security Extensions, 1999
  - RFC 2536 – 2539, RFC 2541
- RFC 2673 Binary Labels in the Domain Name System, 1999

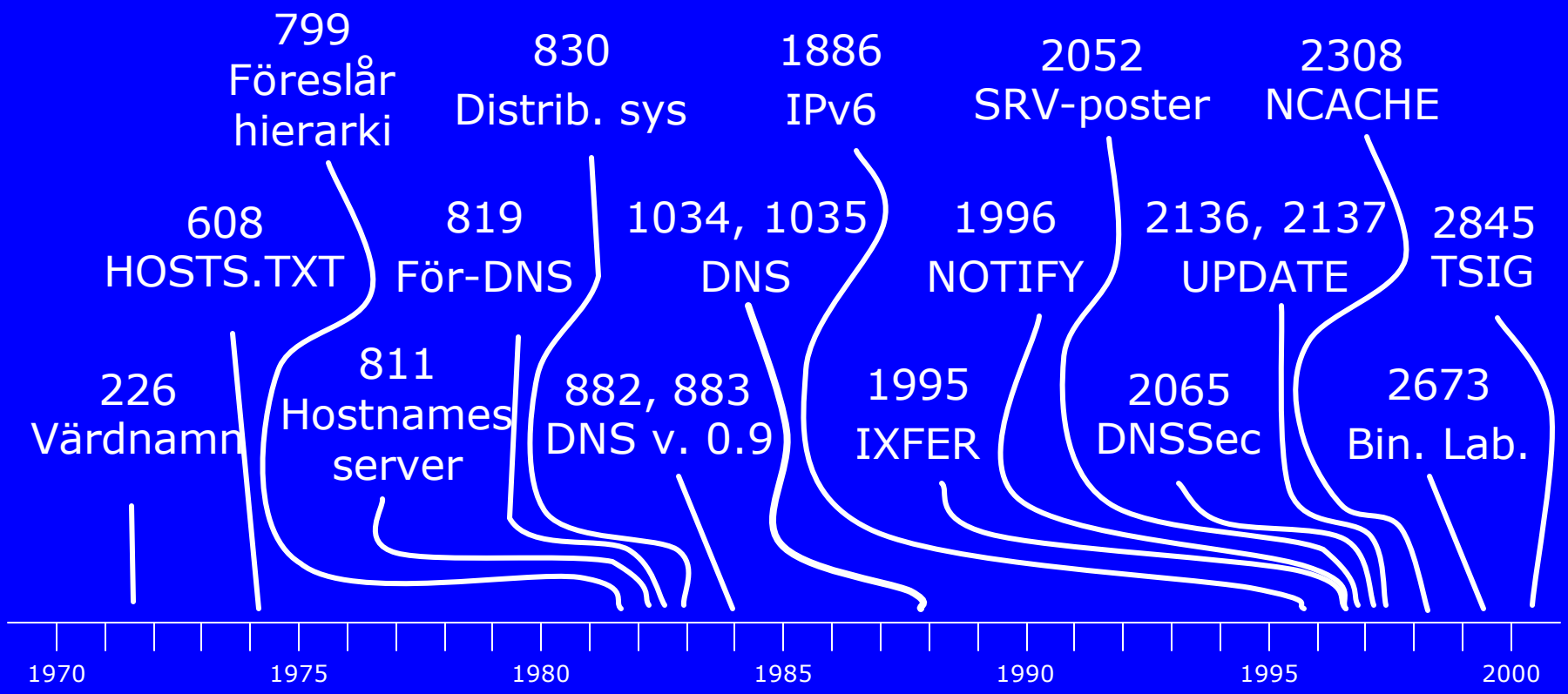
Årets bidrag (hittills)

- RFC 2782 A DNS RR for specifying the location of services (DNS SRV), 2000
  - Ersätter 2052
- RFC 2845 Secret Key Transaction Authentication for DNS (TSIG), 2000
- RFC 2930 Secret Key Establishment for DNS (TKEY RR), 2000
- RFC 2931 DNS Request and Transaction Signatures (SIG(0)s), 2000

Om hörnet…

- Draft: Domain Name System Security (DNSSEC) Signing Authority, 2000
  - Uppdaterar RFC 2535
- Draft: Secure Domain Name System (DNS) Dynamic Update, 2000
  - Uppdaterar RFC 2535, RFC 2136
  - Ersätter RFC 2137
- Draft: GSS Algorithm for TSIG (GSS-TSIG)
  - Microsofts hantering av säker uppdatering i Windows 2000

(Delar av) DNS-utvecklingen över tiden

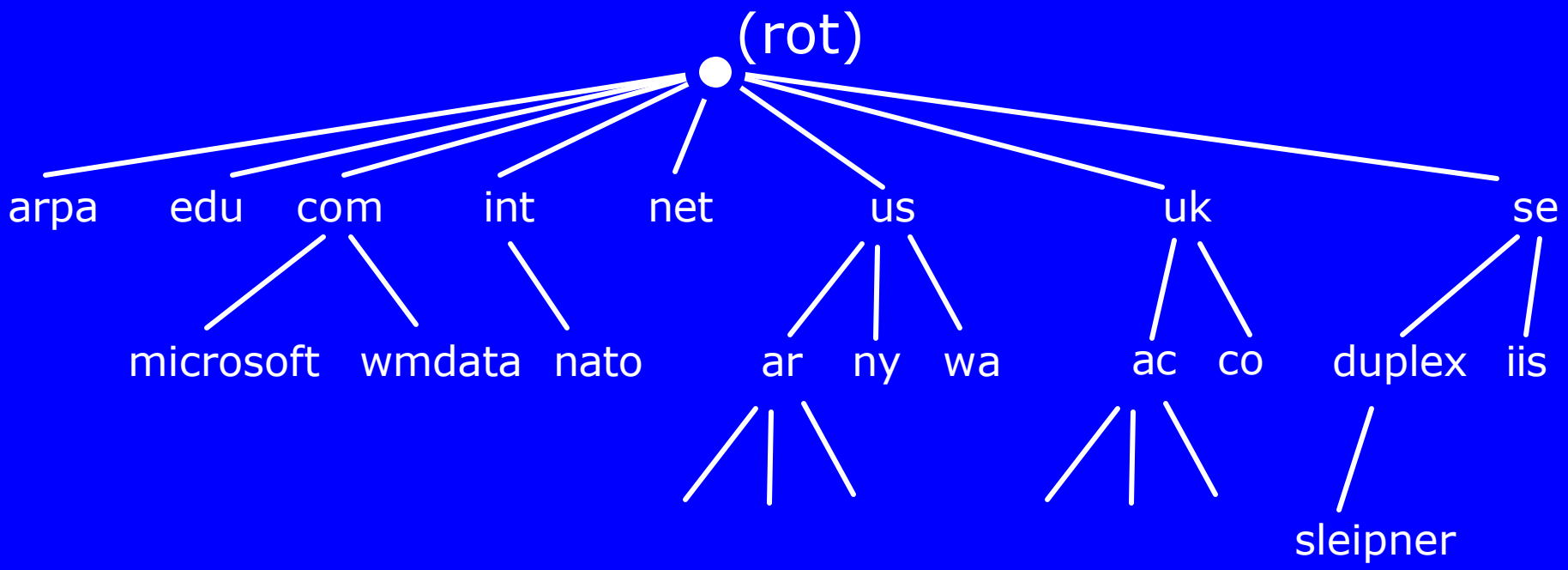


Uppbyggnad och indelning

- RFC 1034/1035 delar in DNS-systemet i tre delar
  - Domain Name Space och Resource Records
  - Name Servers
  - Resolvers
- Jag tycker det blir än lättare att dela upp den första i två:
  - Domain Name Space
  - Resource Records

Domain Name Space/-/DNS-namnrymden

DNS-namnrymden (en pytteliten del)



Några viktiga punkter

- DNS-namnrymden:
  - Är hierarkisk
  - Har distribuerad administration
  - Stor frihet nedåt
  - Är inte endast till för Internet-namn
  - Är idag begränsad till 255^{28} ($2{,}41 \cdot 10^{67}$) noder (man måste räkna bort de fall då två punkter kommer direkt efter varandra, säg hälften)
  - Varje delnamn (label) är begränsat till 63 oktetter
  - Ett helt DNS-namn, med alla delar, är begränsat till 255 oktetter

Resource Records/-/DNS-poster

Några viktiga punkter

- DNS-poster
  - Finns i en stor databas
- DNS-databasen är ett mycket lyckat exempel på en distribuerad databas
- DNS-databasen är aldrig (sic!) uppdaterad
- DNS-databasen finns på många olika operativsystem

DNS-poster: allmänna egenskaper

- DNS-poster har alltid (engelska benämningar):
  - **Owner** ex. sleipner.simplex.se
  - **Type** ex. A
  - **Class** ex. IN (Internet)
  - **Time To Live, TTL** ex. 60 min.
  - **RData** (olika för olika Class) ex. 19.55.11.17

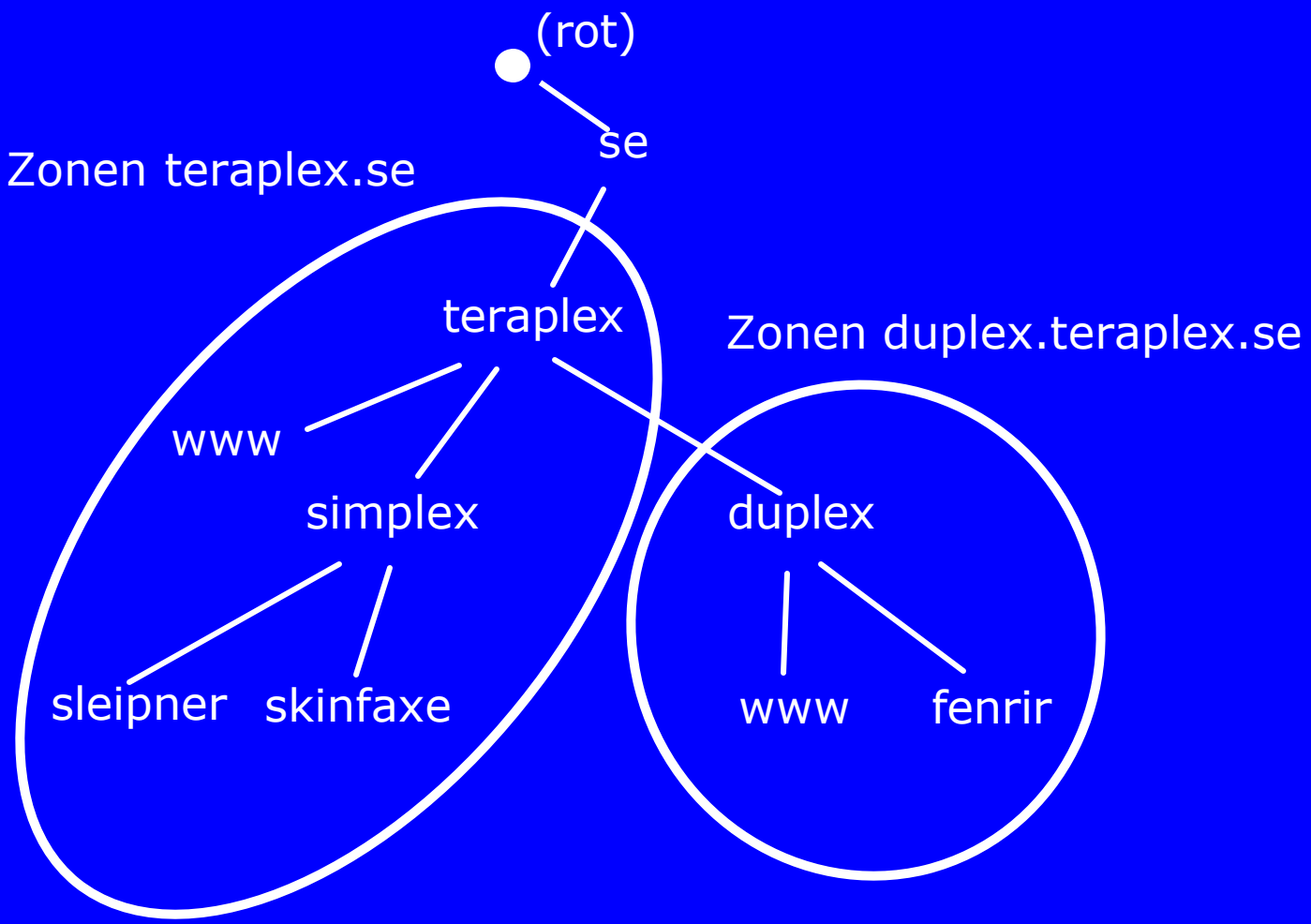
DNS-poster: SOA

- DNS-poster av av typen Start Of Authority används för att beskriva vilken del av DNS-rymden som den själv och de andra posterna handlar om
  - Den blir en slags metapost

DNS och zoner

- En zon är
  - en DNS-domän med underdomäner
  - del av en DNS-domän
- En zon är en fil på en DNS-server
- Ex. på zoner:
  - en fil som omfattar teraplex.se
  - en fil som omfattar duplex.teraplex.se

Zoner i DNS-rymden



DNS-zonen består av poster

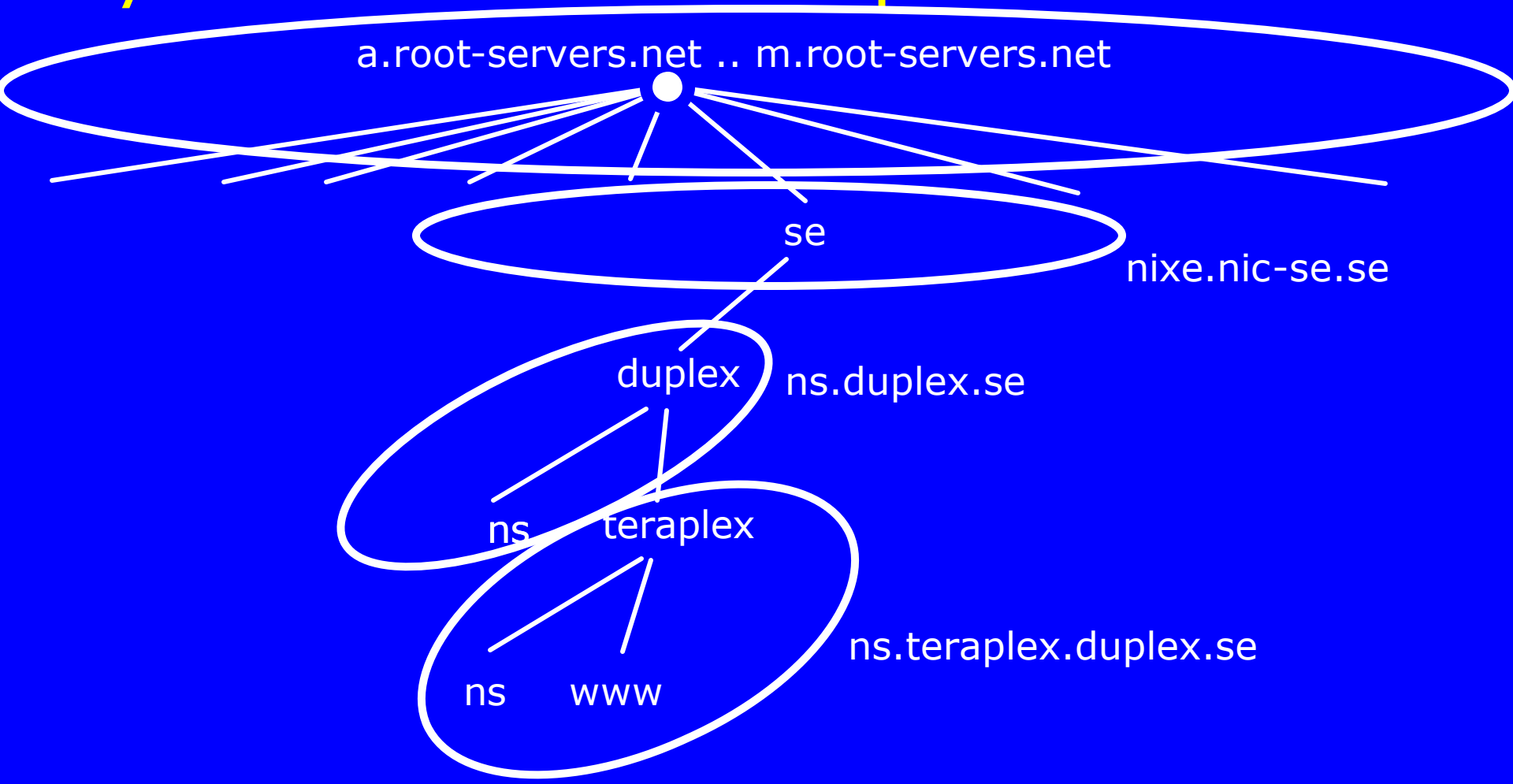
- En zon består av olika typer av poster. Det finns alltid en post som beskriver zonen och en post för DNS-servern.
  - Start of Authority, SOA
  - Name Server, NS
- Värdar har en A-post (Address)
- Alias anges med CNAME-poster
- MX-poster anger vart elbrev skall skickas
- Omvänd sökning använder PTR-poster

DNS-servrar

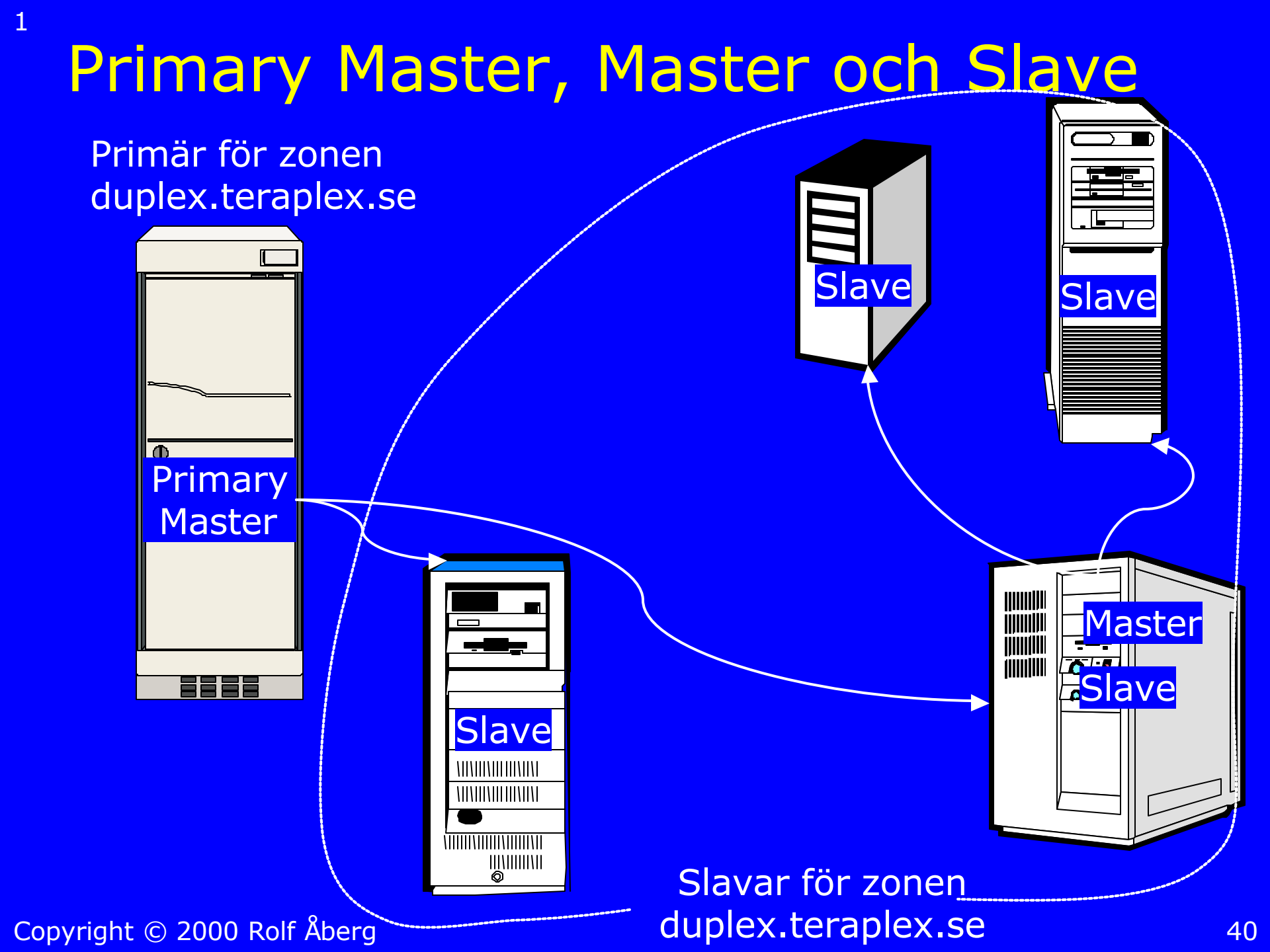
DNS-servrar har flera uppgifter

- DNS-servrar är hem och härbärge för DNS-posterna
- DNS-servrar härbärgerar DNS-poster indelade i zoner
- DNS-servrar kan samarbeta och dela zon-information mellan flera servrar
- DNS-servrar svarar på DNS-frågor från klientdatorer

DNS-servrarna bygger upp DNS-rymden m.h.a. DNS-poster



Primary Master, Master och Slave



DNS-servrar pekas ut av DNS-poster

- I SOA-posten för en zon står vilken DNS-server som är dess Primary Master
- I NS-poster står vilka övriga DNS-servrar som är slavar för zonen
- (Vilka DNS-servrar som är Master-servrar anges på annat ställe)

Start of Authority, SOA

- Namn på primära DNS-servern: **MName**
- Elpostadress till ansvarig person: **RName**
- Serienummer
  - Mycket viktigt för uppdatering mellan primär och sekundär server. Vanligt att man använder serie-nummer av typen ååååmmddnn, där nn går från 00 (eller 01) till 99. Ex. 2000111701.
- Refresh Interval
- Retry Interval
- Expire Time
- Minimum Default Time to Live – numera ändrad till Negative Cache

SOA-uppgifter för Master/Slave-hanteringen

- Refresh Interval
  - En slav skall fråga sin master om ”de’ vatt nå’t” med detta intervall
- Retry Interval
  - Får inte slaven kontakt skall den försöka igen efter denna tid
- Expire Time
  - Efter så här lång tid utan kontakt är inte zon-posterna giltiga längre

DNS-server

- DNS är idag statisk, servern måste förses med information om vilket DNS-namn som motsvarar en viss IP-adress
- En DNS-server kan vara Primary Master för godtyckligt antal zoner, Master för ett godtyckligt antal (även andra) zoner och Slave för ett godtyckligt antal (ytterligare andra) zoner
- Windows 2000 Server innehåller dynamisk DNS, DDNS
- BIND i senare versioner är också dynamisk
- Dynamisk DNS är ett säkerhetsproblem!

Grundantaganden om DNS-poster

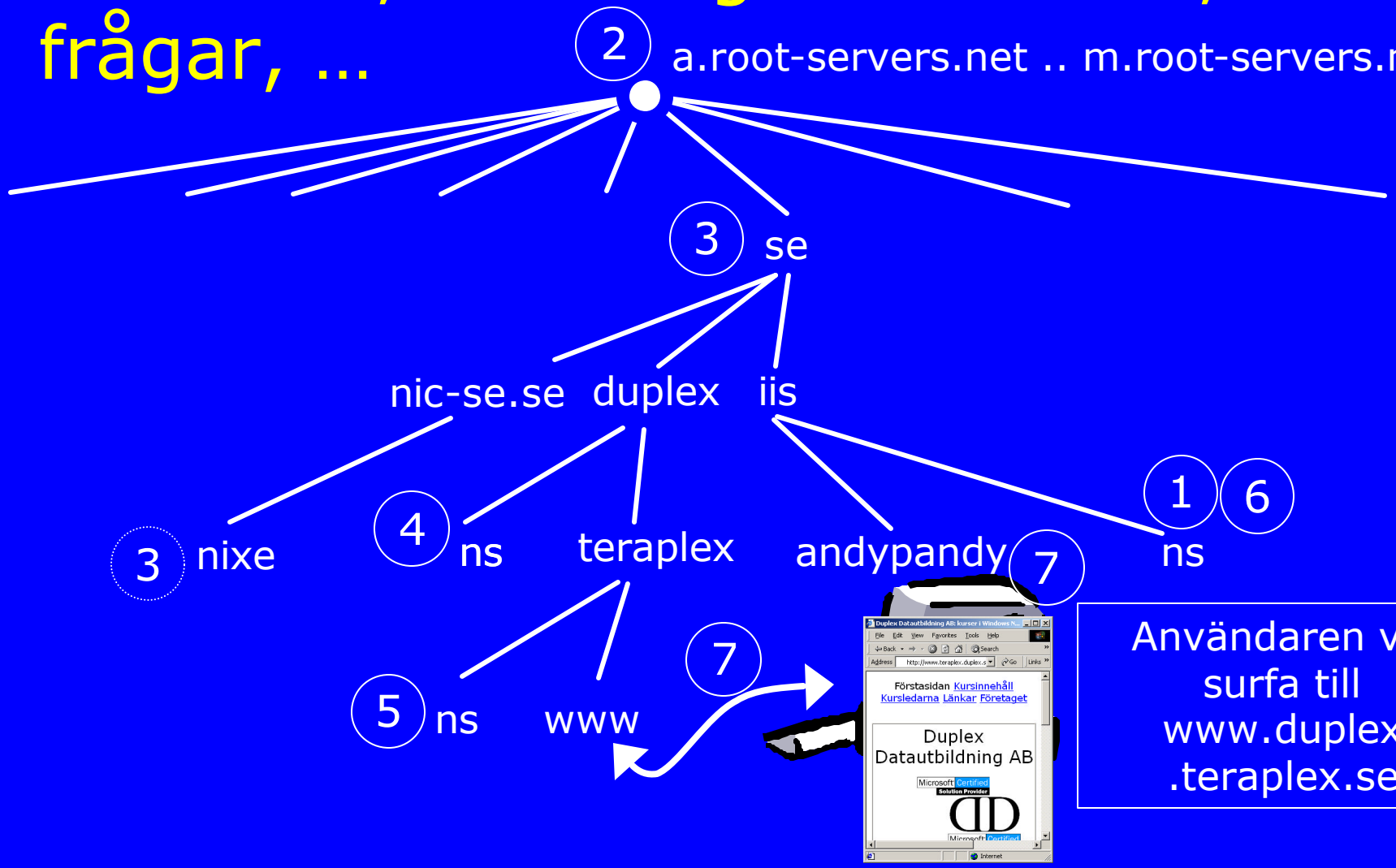
- DNS-posterna uppdateras statiskt
- Uppdateringar sker sällan
- Uppdateringar sker genom att ändra i Master-filen för zonen – utanför DNS-systemet
- (RFC 2136: ”The Domain Name System was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made as external edits to a zone’s Master File.”)

Resolvers/-/klientprogram

Namnuppslagning: har DNS-namn, söker IP-adress

- Rekursivt (recursive namn resolution)
  - En klient begär svar av **sin** DNS-server
  - Klientens utsedda DNS-server gör allt jobb för att klienten skall få svar
  - Vanligaste arbetssättet
- Iterativt (iterative name resolution)
  - Klienten blir hänvisad till olika DNS-servrar
- Klientprogrammet (DNS Resolver) bestämmer om det skall vara rekursivt eller iterativt – en server är dock fri att neka rekursion

”Din” DNS-server frågar en rotserver, som frågar en dotter, som frågar, ...



Användaren vill surfa till www.duplex.teraplex.se

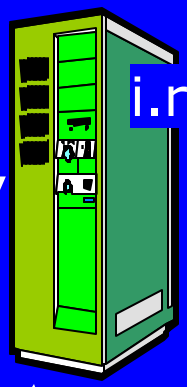
Vartefter DNS-servrarna får/ser svar lagras dessa

- De DNS-servrar som besvarar eller hjälper till med frågor mellanlagrar (cache:ar) information
  - När samma fråga kommer på nytt finns den redan på lagret
- Mellanlagringen i DNS-systemet är en mycket stor fördel sett ur nätverksbandbredds- och svarstidssynvinkel

Rotservrarna är ofta DNS-servrar även för nästa nivå

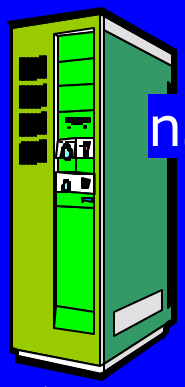
- Rotservern i.root-servers.net är namnserver även för .se
  - Den står i Sverige
- Rimligen är det den som svarar på frågor från Sverige
- Nästa bild antar att det är i.root-servers.net som besvarar frågan: den har alltså själv information om .se och behöver inte låta nixe.nic-se.se ”ta över”

Rekursiv namnuppslagning



i.root-servers.net

rotserver,
äger ”.”
och .se



ns.teraplex.se

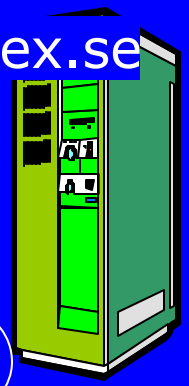
4 ?

5 Fråga ns.duplex.teraplex.se

3 Fråga ns.teraplex.se

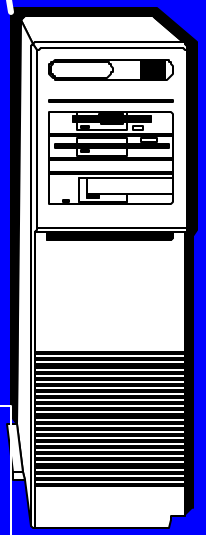
? 2

ns.duplex.teraplex.se

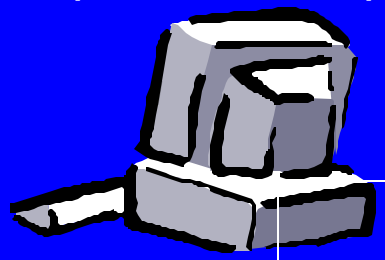


6 ?

7 Ja: 207.46.131.137



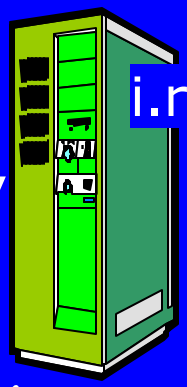
http://www.duplex.teraplex.se



207.46.131.137 8

IP-adress för 1
www.duplex.teraplex.se?

Iterativ namnuppslagning



i.root-servers.net

rotserver,
äger ”.”
och .se

ns.teraplex.se

?

3

Fråga ns.teraplex.se

4

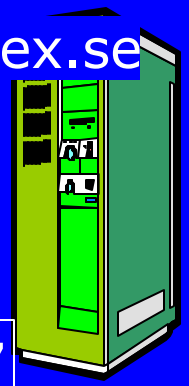
?

5

6

Fråga ns.duplex.teraplex.se

ns.duplex.teraplex.se

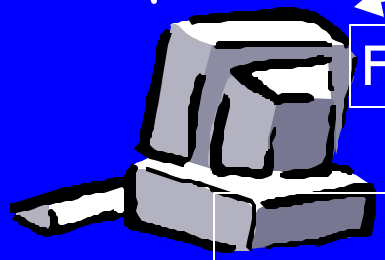


?

7

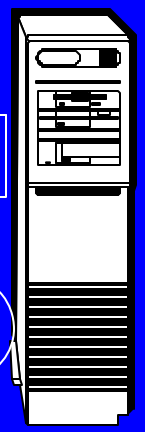
2

8



Fråga i.root-servers.net

Ja: 207.46.131.137



IP-adress för
www.duplex.teraplex.se?

1

Begreppen rekursiv och iterativ skall ses ur klientens synvinkel

- Rekursiv namnuppslagning är rekursiv för klienten, men iterativ för klientens DNS-server
- Det är artigt, mellan DNS-servrar, att **inte** be nästa göra en rekursiv namn-uppslagning (strängt taget är den första DNS-servern klient till den andra)

Omvänd namnuppslagning: har IP-adress, söker DNS-namn

- Omvänd (inverse name resolution)
  - IP-adressen är känd och DNS-namnet söks
  - Kräver poster i en bakåtsökningsdomän
    - *n*.*m*.in-addr.arpa
    - PTR-post för den dator vars DNS-namn vi söker i *n*.*m*.in-addr.arpa

Bakåtsökningsdomäner, in-addr.arpa

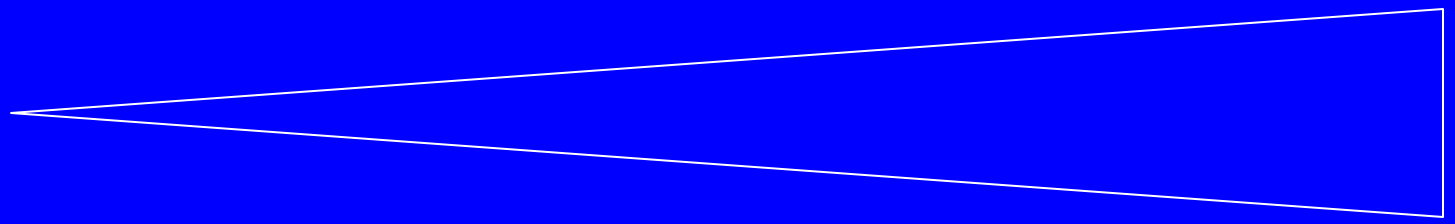
- För att kunna finna DNS-namn om man har IP-adressen måste DNS-servern innehålla en bakåtsökningsdomän
- Alla bakåtsökningsdomäner har gemensam sistadel: in-addr.arpa
- Domändelen in-addr.arpa används enbart för bakåtsökningsdomän

IP-nätadresser och bakåtsökningsdomäner

- Med känd IP-nätadress fås bakåtsöknings-domänen genom att vända på IP-nätadressen och häkta på in-addr.arpa
  - 17/8 ger 17.in-addr.arpa
  - 171.1/16 ger 1.17.in-addr.arpa
  - 195.51.11/24 ger 11.51.195.in-addr.arpa
  - 195.51.11.16/28 ger 11.51.195.in-addr.arpa
- Bakåtsökningsdomäner har alltid ett, två eller tre led före in-addr.arpa

Bakåtsökningsdomänen utseende är en följd av olika hierarkisystem

- DNS-namn avspeglar hierarkin i DNS-systemet:
  - värd.domän.domän.toppdomän



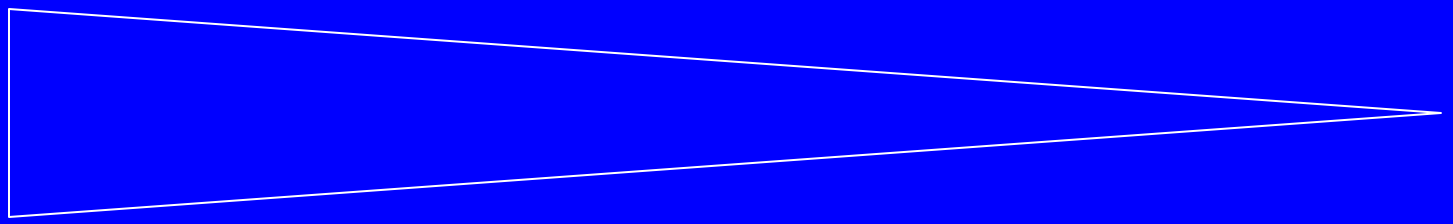
Mest unikt, minst allmänt

Minst unikt, mest allmänt

(det är många objekt som har samma slutdel)

Bakåtsökningsdomänen utseende är en följd av olika hierarkisystem

- IP-adresser avspeglar hierarkin i IP-adresssystemet:
  - IP-nät 1.IP-nät 2.IP-nät 3.IP-värd

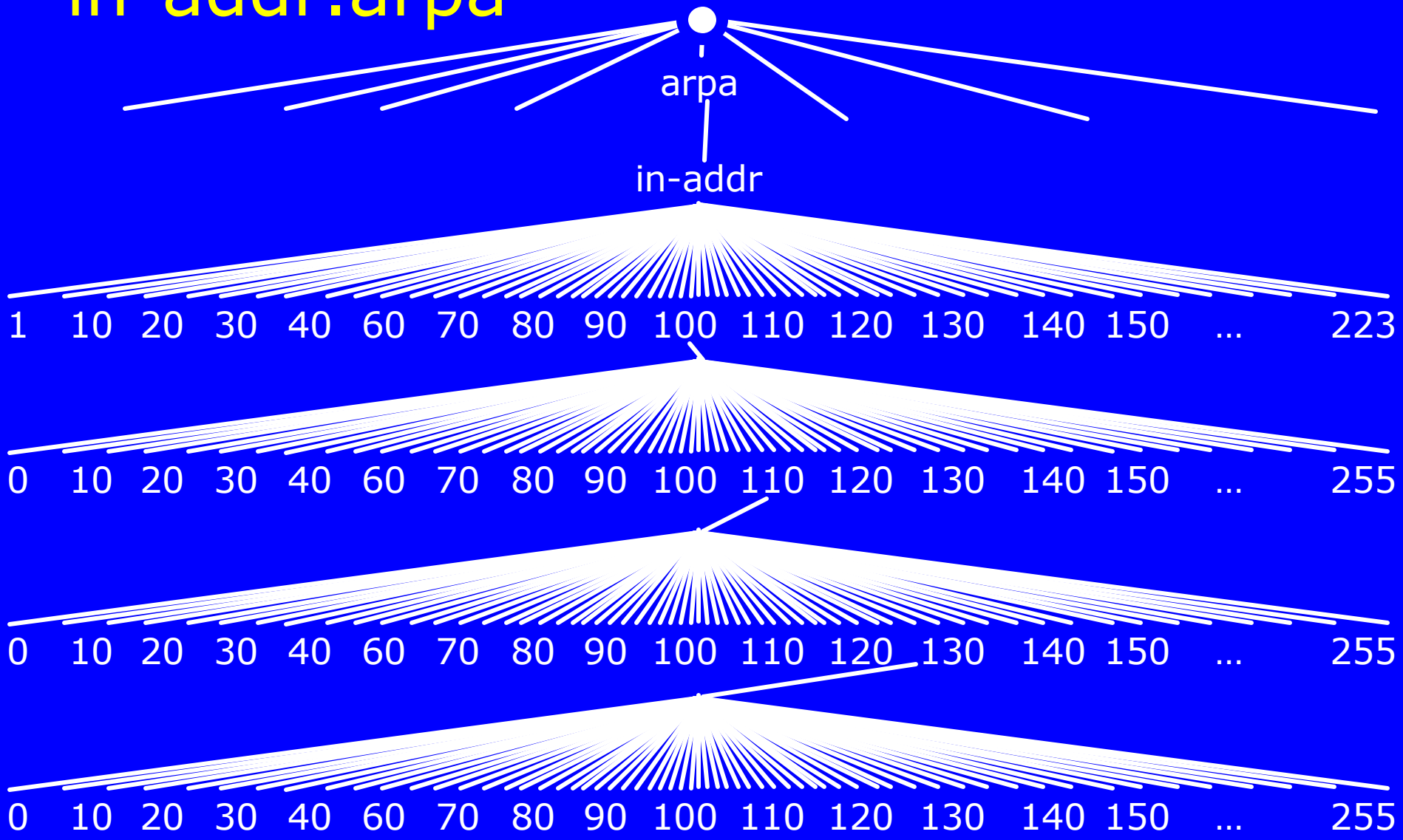


Minst unikt, mest allmänt

(det är många objekt som har samma första-led)

Mest unikt, minst allmänt

Toppdomänen arpa och dess dotter in-addr.arpa



Del 2: Dynamisk DNS

Hur kommer vi från dagens läge till dynamisk uppdatering

- DNS-systemet realiseras av DNS-servrar
- Med endast en DNS-server för en zon är dynamisk uppdatering ett ganska litet problem
  - Antal poster som uppdateras per sekund
  - Säkerställa att hela uppdateringen genomförs, eller backas tillbaka
  - Hantera frågor mot poster som är under uppdatering just nu (inga halva svar, tack!)
- Hur blir det med flera DNS-servrar för samma zon?
  - Kan man vänta på nästa Refresh?
  - Måste hela den uppdaterade zonen skickas, AXFR?

Med dynamisk uppdatering av DNS-poster följer ett antal frågor

- Skall datorer själva uppdatera ”sina” DNS-poster?
- Skall användare kunna beordra datorer att uppdatera ”sina” DNS-poster?
- Är det tillåtet att ändra DNS-namn och IP-adress eller endast IP-adress?
- Är det endast A-poster som får uppdateras?
- Får CNAME-poster uppdateras?

Flera spörsmål

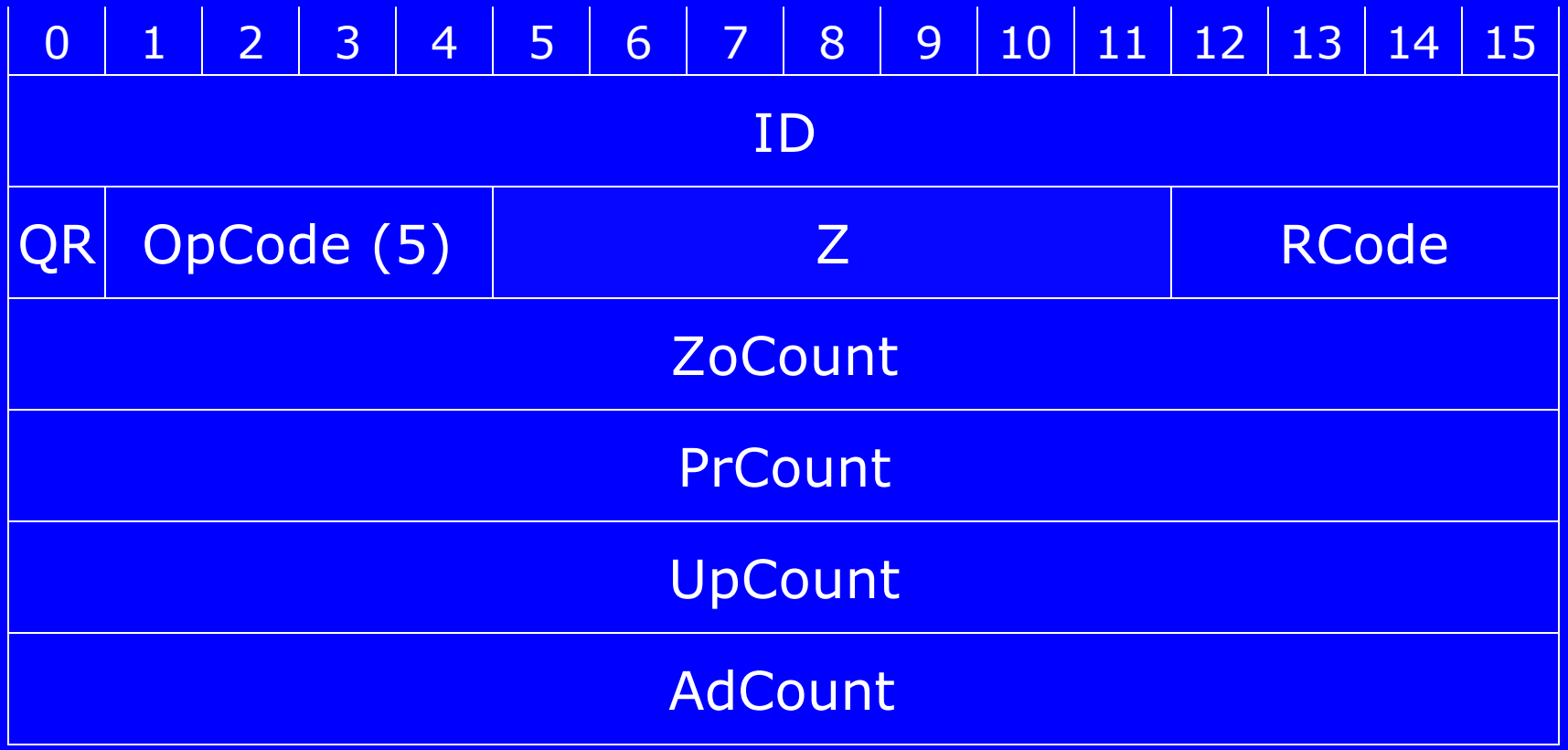
- Vilken DNS-server skall man uppdatera
  - Primary Master
- Hur hittar man Primary Master
  - ”Min” DNS-server skickar vidare
  - MName-uppgiften i SOA-posten
  - Inte alla har namnet på Primary Master i MName
- Inte alltid NS-post för Primary Master
- Uppdatering av befintlig post
  - Hur hittar man rätt post?
- Hur vet man att den som försöker uppdatera är behörig och vem det är?

RFC 2136 *Dynamic Updates in the Domain Name System (DNS UPDATE)*

DNS Update

- Medger uppdatering av enskild DNS-post (Resource Record, RR)
- Medger uppdatering av DNS-postmängd (RRset)
- Inför en ny OpCode: Update
- Använder DNS standardformat för meddelanden, med några tillägg (felkoder)
- Använder UDP eller TCP

Meddelandeformat: styrinformation (header)



Meddelandeformat: styrinformation (header), forts.

- ID: meddelande-ID
- QR: query (0)/response (1)
- OpCode: 5 (för Update)
- Z: alla bitar satta till 0 (även AA-, TC-, RA- och RD-bitarna)
- RCode: Response Code, helst NoError (0)
- ZoCount: antal DNS-poster (RR) i Zone-delen
- PrCount: antal DNS-poster i Prerequisite-delen
- UpCount: antal DNS-poster i Update-delen
- AdCount: antal DNS-poster i Additional Data-delen

Meddelandeformat: datadelar

- Zone-del
  - Innehåller namn på den (enda) zon i vilken aktuella DNS-poster finns
    - » Innehåller ZName, ZType (SOA) och ZClass (oftast IN för Internet)
- Prerequisite-del
  - Här anger man vilka villkor som skall vara uppfyllda för att uppdateringen skall genomföras, såsom befintlighet av poster, icke-befintlighet av poster, m.m.

Meddelandeformat: datadelar, forts.

- Update-del
  - Här anger man en av:
    - » Lägg till en DNS-post till en DNS-postmängd
    - » Ta bort en DNS-postmängd
    - » Ta bort alla DNS-postmängder för ett namn
    - » Ta bort en DNS-post från en DNS-postmängd
- Additional Data-del
  - Uppgifter som kan behövas, ex. klister-poster (glue RR) anges här

DNS-serverns del av arbetet (om den kan Update)

- DNS-servern undersöker/genomför detta:
  - Endast en zon angiven i meddelandet
  - Är angiven zon en av våra?
  - Skicka vidare om slav för en av våra zoner
  - Undersök Prerequisite-delen (är alla villkor uppfyllda)
  - Är uppdateraren behörig att uppdatera?
    - » Här anges utanförliggande mekanismer, ex. RFC 2137
- Om allt är i lag påbörjas uppdaterings-arbetet

DNS-serverns uppdateringsarbete

- Meddelandet går igenom ett tvättsteg (pre-scan):
  - Zontillhörighet för poster är samma i servern som uppges i meddelandet (ZName)
  - Type skall inte vara en av: AXfr, MailA, MailB
  - Genomför ändring (infogning, borttagning)

Säkra dynamisk uppdatering

Första försöket

- RFC 2137 Secure Domain Name System Dynamic Update
  - Bygger på DNSSec i RFC 2065
  - Använder SIG-poster (Signature RR)
  - I och med att RFC 2065 ersätts av RFC 2535 ”faller” RFC 2137

Andra försöket

- Draft: [Simple] Secure Domain Name System (DNS) Dynamic Update
  - Anger användning av TSIG [RFC 2845] eller SIG(0) [RFC 2931]

Säker uppdatering enl. nya metoden

- Klient och server förhandlar om metod för kryptering
  - De kan välja mellan TSIG och SIG (0)
    - » TSIG innebär symmetrisk kryptering och därmed måste man komma överens om hemlig nyckel
    - » SIG(0) är asymmetrisk kryptering och därmed enkel vad gäller den publika nyckeln, men resurskrävande
- Om TSIG skall användas så plockar de fram TKEY-protokollet
  - Det är detta de börjar med

RFC 2930 Secret Key Establish-ment for DNS (TKEY RR)

- TKEY är en pseudo-DNS-post, d.v.s. den är uppbyggd som en DNS-post, men sparas inte i någon DNS-server och mellanlagras inte heller (TTL=0)
  - Används endast i förhandling mellan klient och DNS-server
- Man kan ange en av flera olika nyckelutbytesmetoder
  - Diffie-Hellman **tvingande**
  - GSS-API
  - *Klienten bestämmer*
  - *Servern bestämmer*

RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)

- TSIG är en pseudo-DNS-post och kan varken lagras eller mellanlagras (TTL=0)
- Använder HMAC-MD5 för att kryptera ett textkondensat
  - Hashed Message Authentication Code, HMAC

Inte bara dynamisk uppdatering, utan även inkrementell zonöverföring och gärna bli upplyst om att det finns något nytt att hämta

Inkrementell zonöverföring

- RFC 1995 Incremental Zone Transfer in DNS (IXFR)
- Inkrementell zonöverföring bygger på att DNS-servrar har en journal/logg över genomförda ändringar
- I loggen sparas ändringar tillsammans med zonens serienummer (som alltså måste uppdateras för varje ändring)

Inkrementell zonöverföring, forts.

- När slavservrar begär en inkrementell zonöverföring uppger de sitt senaste serienummer för zonen
- Om master-servern har alla ändringar i loggen och det är lämpligt att endast skicka dessa genomförs en inkrementell zonöverföring, annars hela zonen (AXFR)
- Master-servern har möjlighet att spara ett begränsat antal ändringar
  - En slav med lägre serienummer får hela zonen (AXFR)

Upplysning om ändringar

- RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- Master-servrar skickar ett meddelande till slavservrarna med innebörd att zonens innehåll ändrats
- Detta meddelande innehåller den aktuella SOA-posten
  - Slavservern jämför med sin egen SOA-post och kan begära zonöverföring (AXFR eller IXFR)

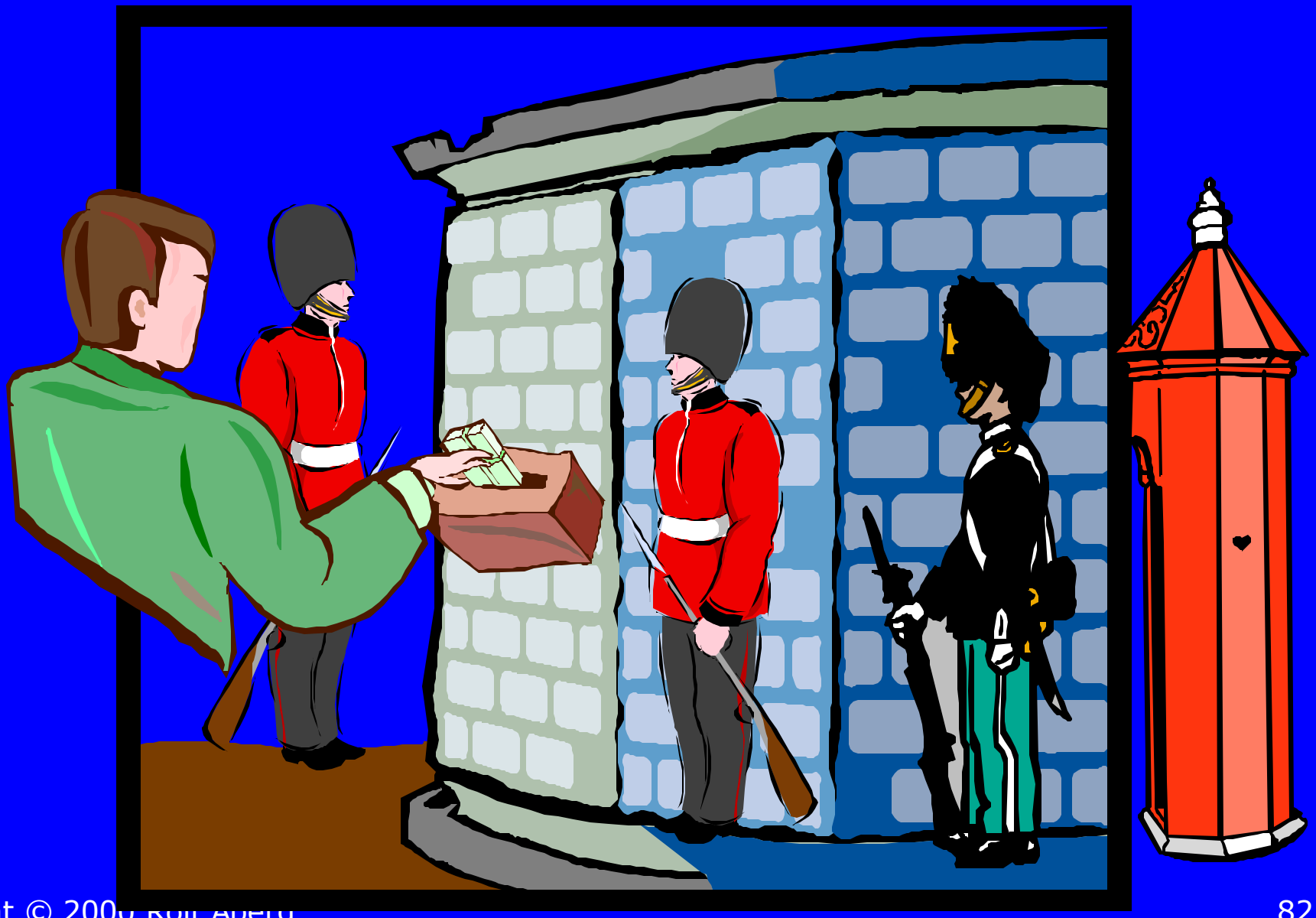
DNS-implementationer som kan allt detta

DNS-implementationer som kan dynamisk DNS, med IXFR och Notify

- BIND 8.1.2
- BIND 8.2
- BIND 9
- Windows 2000 Server

Vem (eller vad) skall få uppdatera?

Transaction Signatures, TSIG



Med Transaction Signatures säkrar man uppdateringar och zonöverföringar

- RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)
- TSIG bygger på kryptering av överföringen
  - RFC 2845 anger endast symmetrisk kryptering med hemlig nyckel

TSIG utan DNSSec (på baksidan)

DNSSec

- RFC 2535 Domain Name System Security Extensions
  - Ersätter RFC 2065
- System för att skydda DNS-poster mot olovlig påverkan

Del 3: Dynamisk DNS & Microsoft

Microsoft har en dynamisk DNS-server i Windows 2000 Server

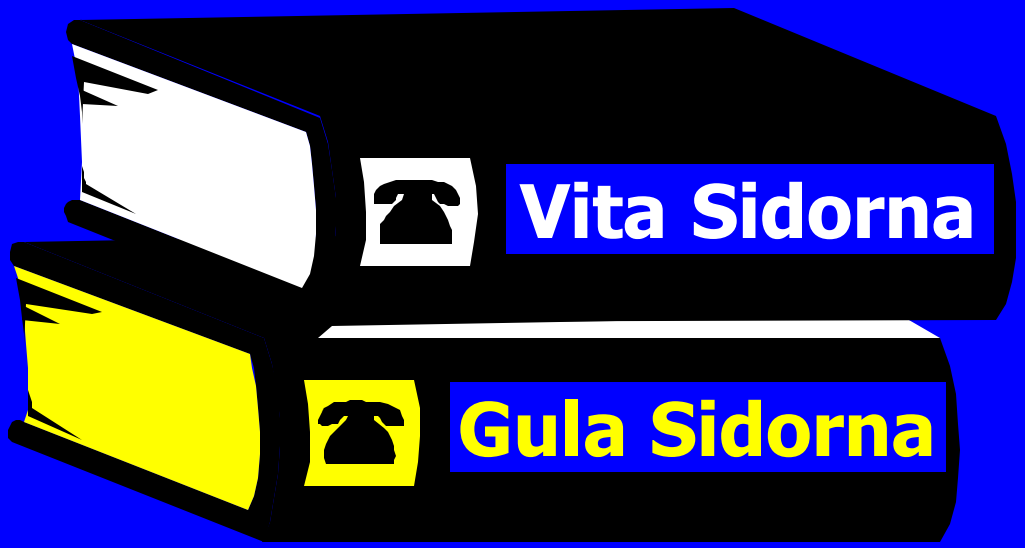
- DNS-servertjänsten i Windows 2000 Server följer RFC 2136, m.fl.
- Microsoft använder inte TSIG för att säker uppdatering/zonöverföring utan GSS-TSIG resp. MSRPC
  - Jämför GSS-API som angavs i RFC 2930 (TKEY)
  - Finns ett draft-dokument för GSS-TSIG
- Microsoft använder inte DNSSec för att säkra DNS-posterna
  - Endast om man låter DNS-posterna bli en del av Active Directory skyddas de (över huvudtaget!)

Active Directory är en katalogtjänst

- Active Directory är Microsofts nya katalogtjänst för Windows 2000
  - Jämför Novells NDS eller NIS/NIS+
- Active Directory använder DNS-namn
- Active Directory är en LDAP-katalogtjänst
- Active Directory bygger upp domäner, inte helt olika Kerberos realms

Vita och gula sidorna samtidigt, och mer ändå

- En katalogtjänst samlar information och tillhandahåller sedan denna information
- Vita och gula sidorna tillsammans: både människor och det som är deras samt tjänster



Hur en katalogtjänst **inte** är som telefonkatalogens vita sidor

- I en katalogtjänst finns lösenord
- I en katalogtjänst finns namn, avdelning, arbetsgivare
- En katalogtjänst innehåller beskrivning av vad som faktiskt kan finnas i katalogen – denna beskrivning kallas metadata eller databasschema

Hur en katalogtjänst är precis som gula sidorna

- I gula sidorna söker vi en tjänst och finner då en hänvisning till vem som tillhandahåller denna tjänst
- I gula sidorna finns det ofta flera likvärdiga tjänsteleverantörer att välja mellan, om en inte har möjlighet kontaktar man en annan

Active Directory kräver DNS-stöd

- Active Directory är Microsofts första nätverksprodukt som kräver DNS-stöd!
- Active Directory **kräver** stöd för SRV-poster (enligt RFC 2782, med under-strykningstecken)
  - BIND 4.9.7, 8.1.2, 8.2, Windows NT Server 4.0 SP4, Windows 2000 Server
- Active Directory samarbetar gärna med dynamisk DNS-server
  - BIND 8.1.2, 8.2, Windows 2000 Server

DNS-servern i Windows 2000 Server har tre körlägen

- DNS-servern i Windows 2000 Server kan användas på tre olika sätt:
  - Statisk DNS-server
  - Dynamisk DNS-server
  - Dynamisk DNS-server med DNS-posterna i Active Directory-databasen
- Gissa vilken som krävs för ”säker” användning?

Ingen säkerhet i statisk och ”vanlig” dynamisk DNS

- Om du använder DNS-servern i Windows 2000 Server som statisk eller dynamisk DNS-server, utan att låta DNS-posterna bli en del av Active Directory, så erbjuder Microsoft **inte** möjlighet att säkra DNS-posterna och inte heller uppdateringen av dem
  - Man *kan* betrakta statisk DNS som säker

Säker uppdatering endast med DNS-posterna i Active Directory

- Endast när du låter DNS-posterna bli en del av Active Directory erbjuder Microsoft säkerhet för DNS-posterna och även för uppdateringstrafiken
  - DNS-posterna i Active Directory förses med behörighetslista (Access Control List, ACL)
  - Uppdatering kräver genomförd Kerberos-inloggning, sedan används GSS-TSIG
    - » Endast Windows 2000-klienter
    - » Det är DHCP-klienten som uppdaterar

Zonöverföringar skyddas om DNS-poster en del av Active Directory

- Med DNS-posterna som en del av Active Directory överförs zonuppdateringar på samma sätt som andra ändringar i AD
  - MSRPC och TCP, ”krypterat”

Microsofts DHCP-server kan uppdatera åt sina klienter

- DHCP-servern i Windows 2000 Server kan ställas in att uppdatera DNS-poster åt sina klienter, både A- och PTR-poster
- Det finns inget enkelt sätt att ange att endast DHCP-servern får uppdatera DNS-poster (om man inte har DNS-posterna i Active Directory)
- DHCP-servern får inte köras på samma dator som DNS-servern (om domän-kontrollant och poster i AD)
  - Båda tjänsterna använder samma konto, System

DHCP-servern uppdaterar åt sina klienter

- När DHCP-servern upprättar en första post för sina klienter får denna post ingen säkerhet (Alla på Internet har tillgång till den)
  - Den första dator, som inte är DHCP-server, som uppdaterar posten kommer att bli dess ägare
- Klaras genom att DHCP-servrar är med i en särskild grupp: DnsUpdateProxy

DNS-poster i Active Directory för baklängesslagning

- DNS-poster i Active Directory för baklängesslagning kommer att registreras på den klient som först får IP-adressen
- Om avregistrering inte fungerar kommer nästa klient som får denna IP-adress att inte kunna uppdatera baklängesposten

Minst osäkra sättet att använda DDNS i Active Directory-domäner

- Förutsättning: DNS-poster i Active Directory
- DHCP-servrarna på egna Windows 2000-datorer
- DHCP-servrarna uppdaterar alltid åt sina klienter
  - Både A- och PTR-poster
- Windows 2000-klienter tillåts inte uppdatera DNS-posterna
  - Ändra i Registret

DNS-posterna i Active Directory-databasen

- Med DNS-posterna i Active Directory-databasen används Kerberos/GSS-TSIG för ”säker” uppdatering
- Varje Active Directory-domänkontrollant blir DNS-server
- Varje domänkontrollant blir primär DNS-server (Primary Master Server)
  - RFC 2136: ”There is by definition only one Primary Master Server per zone.”

Replikering av DNS-posterna i Active Directory-databasen

- DNS-posterna i Active Directory-databasen replikeras på samma sätt som andra poster i Active Directory-databasen
  - Fem minuter efter senaste ändring kontaktar domänkontrollanten sina grannar och replikerar ny information med dem
  - Tiden fem minuter är ändringsbar

Med DNS-poster i Active Directory fungerar ändå Notify

- När DNS-poster görs till en del av Active Directory fungerar fortfarande Notify-möjligheten
- Det går att slå av Notify, vilket gör att DNS-poster replikeras som andra poster i AD
  - Det finns en enda inställning för replikering, den styr alla poster i AD

Uppdatering av DNS-poster i Active Directory-databasen

1) Q: ”Jag tänkte behålla posterna intakta”
   R: 1/0
2) Q: ”Mina nya inställningar”
   R: 1/0, **vägras** om inställd för säker uppd.
3) Q/R: TKEY-förhandling, Kerberos blir resultatet, via GSS-API
4) Q/R: Uppdatering m.h.a. GSS-TSIG

När Windows 2000-klienter uppdaterar DNS-post kan de få ”riggad” information

- Windows 2000-klienten vet vilken domän den tillhör så den frågar sin DNS-server om namnet på den DNS-server som äger zonen (**MName**)
- Domänkontrollanten/DNS-servern stoppar in eget datornamn i SOA-posten så att klienten kontaktar den!
  - Används för att den DNS-server som är närmast servar klienten
- Klienten chansar på att dess DNS-post är OK och skickar ett kort meddelande med denna innebörd
- Fanns inte posten skickar klienten en nyregistrering

Uppdatering av DNS-poster, forts.

- Vägras klienten oskyddad uppdatering så går den över till GSS-TSIG
  - Klient och server förhandlar fram TKEY [RFC 2930] med hjälp av Kerberos
  - GSS-TSIG används under uppdateringen

Säker uppdateringar med andra DNS-servrar än Windows 2000

- Microsoft uppger sig har provat säker uppdatering från Windows 2000-klienter till ”andra GSS/Kerberos”-system
  - Det går dock inte att finna någon redogörelse för hur de kommer från GSS/Kerberos till säker uppdatering av DNS-poster
- Paul Leach har sagt:
  - ”None of the Microsoft extensions to Kerberos are needed to implement an interoperable BIND server using GSS-TSIG. An implementation that does standard Kerberos, that does not understand the extensions, can safely ignore them. We do such interoperability testing as part of our release process.”

? ? ¿ _ ! ! !

Win2k-request@sunet.se

Referenser

Referenser

- RFC 1034 Domain Names – Concepts and Facilities
- RFC 1035 Domain Names – Implementation and Specification
- RFC 1123 Requirements for Internet Hosts – Application and Support
- RFC 1886 DNS Extensions to support IP version 6
- RFC 1982 Serial Number Arithmetic
- RFC 1995 Incremental Zone Transfer in DNS (IXFER)
- RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- RFC 2065 Domain Name System Security Extensions

Referenser, forts.

- RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 2137 Secure Domain Name System Dynamic Update
- RFC 2181 Clarifications to the DNS Specification
- RFC 2308 Negative Caching of DNS Queries (DNS NCACHE)
- RFC 2316 Report of the IAB Security Architecture Workshop
- RFC 2535 Domain Name System Security Extensions
- RFC 2536 DSA KEYs and SIGs in the Domain Name System (DNS)

Referenser, forts. 2

- RFC 2537 RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
- RFC 2538 Storing Certificates in the Domain Name System (DNS)
- RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
- RFC 2541 DNS Security Operational Considerations
- RFC 2782 A DNS RR for Specifying the Location of Services (DNS SRV)
- RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)

Referenser, forts. 3

- RFC 2929 Domain Name System (DNS) IANA Considerations (BCP 42)
- RFC 2930 Secret Key Establishment for DNS (TKEY RR)
- RFC 2931 DNS Request and Transaction Signatures (SIG(0)s)
- Draft: Domain Name System Security (DNSSEC) Signing Authority
- Draft: Secure Domain Name System (DNS) Dynamic Update
- Draft: GSS Algorithm for TSIG (GSS-TSIG)

Referenser, forts. 4

- DNS i Windows 2000
  - http://www.eu.microsoft.com/windows2000/library/howitworks/communications/nameadrmgmt/w2kdns.asp
- Kerberossamverkan med andra
  - http://www.eu.microsoft.com/windows2000/library/howitworks/security/kerbint.asp
- Kerberossamverkan med CyberSafe
  - http://www.eu.microsoft.com/PressPass/press/2000/Jan00/CyberSafePR.asp

Referenser, fort. 5

- Stuart Kwan om säker DNS i Win2k
  - http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0002&L=NTBUGTRAQ&P=R6854
- Paul Leach om GSS-TSIG i andra system
  - http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0003&L=NTBUGTRAQ&D=0&P=3105

Måste läsas!

- ”Secrets and Lies”, Bruce Schneier
  - Du har inte en chans – ta den!

Uppdateringar, svar på frågor

- http://www.simplex.se/ddns
- mailto:rolfa@simplex.se

Rolf Åberg och tiden

1999		Windows 2000		
1995			Utbildning, konsult, hack	Egen (mycket)
1993		Windows NT		
1991		Visual Basic, SQL Server	Programutveckling (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 Institutet
1980	ABC 80	BASIC	Programutveckling (exjobb)	KTH

Rolf Åberg

- Rolf Åberg har varit systemsupportchef på Microsoft 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, Windows 95, Visual Basic och SQL Server. Rolfs senaste bok heter ”Allt om Windows NT Server” (ISBN 91-88590-12-7), och försöker på nästan 1400 sidor göra skäl för namnet. Sedan en tid knåpar han på en som troligtvis får titeln ”Vägen till Windows 2000 och Active Directory”. Förutom Duplex Datautbildning konsultar Rolf inom ramen för Simplex System.
- mailto:rolfa@duplex.se eller mailto:rolfa@simplex.se
- http://www.duplex.se eller http://www.simplex.se