Linux 2

ITINF 2021

Lektion 4

Idag

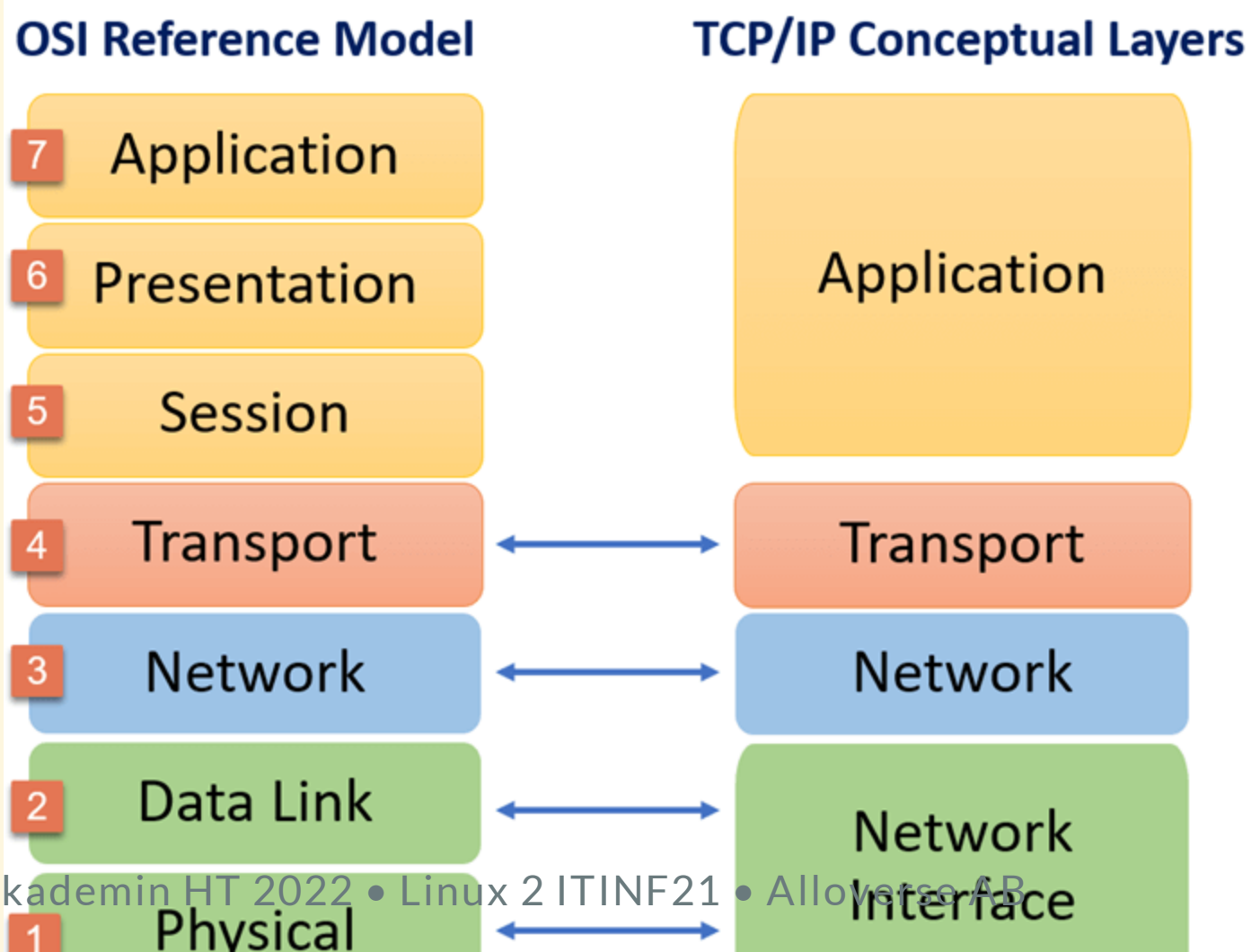
- Nätverk
- Nätverksinställningar
- Mailserver och SMTP
- DNS och DNS-records
- konfigurera DNS

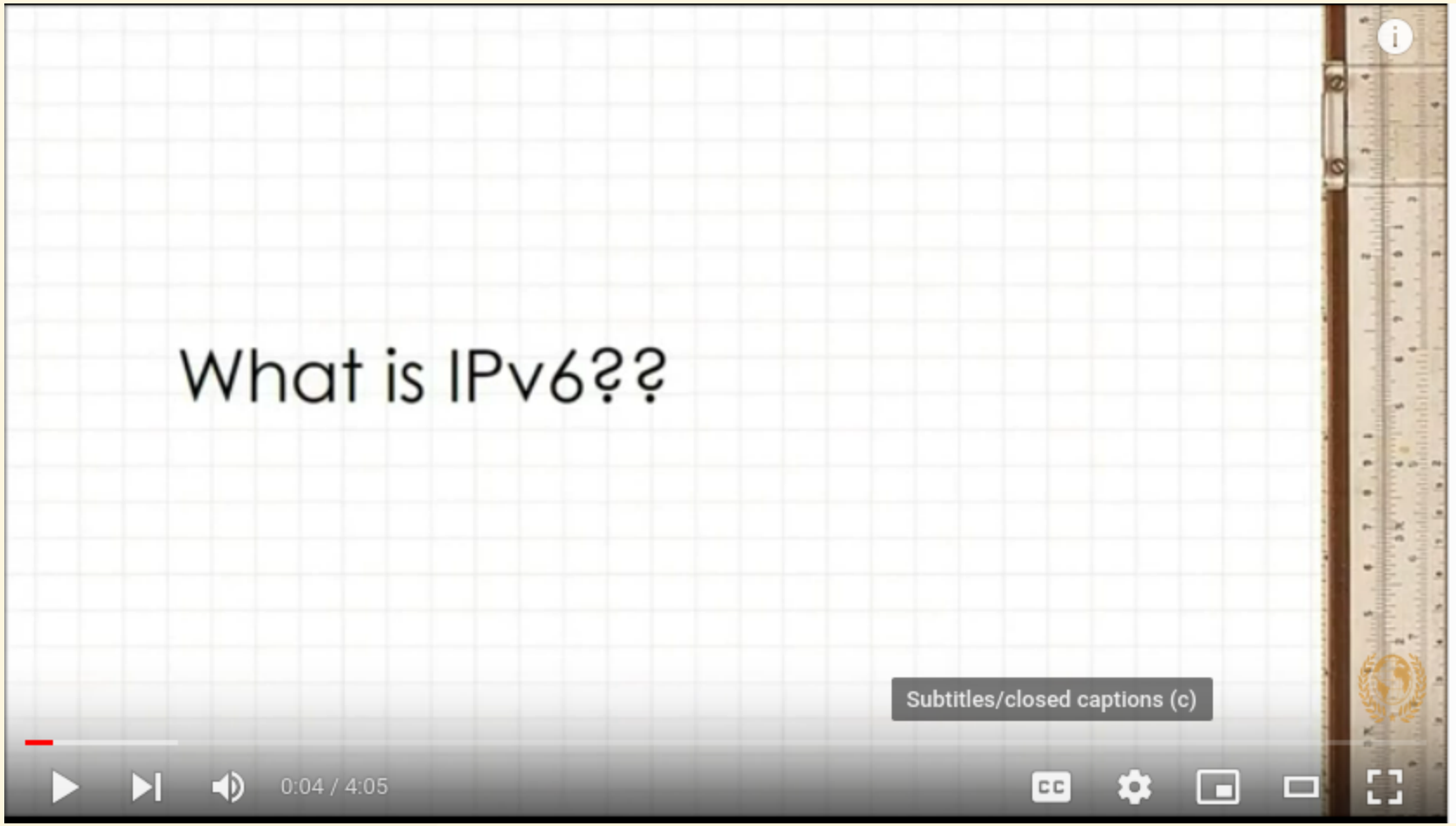
Nätverk

Nätverk

- Datorer pratar med varandra
  - Kommunikation på många protokoll, men måste alltid hitta varandra
- IP-adresser (Internet Protocol Address)
  - En numerisk bestämning som pekar ut nätverkskopplingen för en viss enhet
  - IPv4, IPv6

Nätverk


OSI Reference Model
TCP/IP Conceptual Layers
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface



https://www.youtube.com/watch?v=bNmnRvZW3HU

Nätverkskommandon i Linux

Kommando	Funktion
`ifconfig`	Visa/ändra nätverksinterface och konfiguration
`ip`	Nyare ersättare till `ifconfig`
`route`	Visa/ändra routingtabell
`ethtool`	Visa/ändra parametrar för ett nätverksinterface
`ping`	testa kontakt och latens till en adress
`traceroute`	Visa routen som ett paket tar till en adress

`route`

- Ange en default gateway:

```
route add default gw <ip>
```

```
route add default gw 192.168.1.1
```

Exempel

- `ifconfig`
- `ip addr show`
- `route`
- `ethtool <interface>`
- `ping <adress>`
- `traceroute <adress>`

Övning 1

Använd lämpliga nyss nämnda verktyg till att ta reda på hur din Linux-maskin är uppsatt nätverksmässigt.

- Ser du om den använder eth eller wlan?
- Ser du routingtabell?
- Kolla speciellt efter
  - din IP
  - ditt loopback-interface

Konfigurera din ip-adress manuellt

`ifconfig <interface> <ip> <netmask> up`

e g: `ifconfig eth1 192.168.1.5 netmask 255.255.255.0 up`

--

`ip addr add <ip>/<mask> dev <interface>`

`ip link set <network> up`

e g:

```
ip addr add 192.168.1.5/24 dev eth1
ip link set eth1 up
```

Övning 2

- Hur gör du för att sätta din Linux-maskins ip- adress till 10.1.1.101 med netmask /24?
  - Testa förslagsvis bara på ett nätverksinterface som inte är det du använder för din koppling till världen just nu.

Övning 2

```
$ sudo ifconfig eth0 10.1.1.101 netmask 255.255.255.0
```

```
nevyn@linmishi ~> ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.101  netmask 255.255.255.0  broadcast 10.1.1.255
        inet6 fe80::adfe:6442:b0a8:9b36  prefixlen 64  scopeid 0x20<link>
        ether 38:00:25:aa:58:89  txqueuelen 1000  (Ethernet)
        RX packets 20489326  bytes 20376802164 (20.3 GB)
        RX errors 0  dropped 239184  overruns 0  frame 0
        TX packets 11225179  bytes 6659493115 (6.6 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

nevyn@linmishi ~> sudo ifconfig wlp2s0 0.0.0.0
nevyn@linmishi ~> sudo ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.68.112  netmask 255.255.255.0  broadcast 192.168.68.255
        inet6 fe80::adfe:6442:b0a8:9b36  prefixlen 64  scopeid 0x20<link>
        ether 38:00:25:aa:58:89  txqueuelen 1000  (Ethernet)
        RX packets 20489582  bytes 20376868346 (20.3 GB)
        RX errors 0  dropped 239184  overruns 0  frame 0
        TX packets 11225433  bytes 6659544246 (6.6 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Se vilka interfaces som är igång?

- `ip addr` och söka efter "state UP"
- `ifconfig` och söka efter "RUNNING"

Övning 3

Implementera följande:

Två gånger i timmen kontrolleras ifall eth0 respektive wlan0 är uppe, och resultatet skrivs till en log-fil, med tidsstämpel

Övning 3

```
#!/bin/bash
logfile=/var/log/myiptest.log
timestamp=`date +%Y-%m-%d_%H-%M-%S`
ip addr | grep wlan0 | grep "state UP" >/dev/null

if [ $? -eq 0 ]; then
    echo $timestamp ": wlan0 UP" >> $logfile;
fi
```

Till crontab:

```
0,30 * * * * /var/scripts/iptest.sh
```

Email

SMTP, IMAP, POP

Vad finns det för mailservrar?

- Postfix, Sendmail, Qmail, etc etc etc...
- Översikt över de populäraste: https://www.ubuntupit.com/best-linux-mail-server-software-and-solutions/

Vad gör en mailserver?

- Tar emot e-post från klienter, och antingen lägger dem i en användares inbox eller skickar vidare (över **SMTP**)
- Tar emot e-post från andra mailservrar, och skickar mail till dem (över **SMTP**)
- Hanterar/levererar/listar/etc mail till klienter
  - POP *(gammalt, dåligt, port 110)*
  - IMAP *(modernt, snazzy, port 143)*

SMTP

"**Simple Mail Transfer Protocol**" (ps. "simple" är en lögn)

- "Pusha" mail till mailserver. Protokoll för utgående e-post
- Text-baserat protokoll; går att skriva för hand
- Anslutnings-baserat (koppla upp dig, autentsiera, skicka diverse kommandon, koppla ner. "SMTP-session")
- Port 25 plaintext, 465 över SSL

Snacka SMTP (kommandon)

- `HELO`: vem är du, vem är jag (modernare: `EHLO` för att be om "extended SMTP")
- `MAIL FROM`: skicka ett mail från angiven adress
- `RCPT TO`: ange mottagare
- `DATA`: Ange meddelandet som ska skickas
- `QUIT`: hejdå!

```
$ telnet example.org 25
S: 220 example.org ESMTP Sendmail 8.13.1/8.13.1; Wed, 30 Aug 2006 07:36:42 -0400
C: HELO mailout1.phrednet.com
S: 250 example.org Hello ip068.subnet71.gci-net.com [216.183.71.68], pleased to meet you
C: MAIL FROM:<xxxx@example.com>
S: 250 2.1.0 <xxxx@example.com>... Sender ok
C: RCPT TO:<yyyy@example.com>
S: 250 2.1.5 <yyyy@example.com>... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: From: Dave
To: Test Recipient
Subject: SPAM SPAM SPAM

This is message 1 from our test script.
.
S: 250 2.0.0 k7TKIBYb024731 Message accepted for delivery
C: QUIT
S: 221 2.0.0 example.org closing connection
Connection closed by foreign host.
```

Från https://en.citizendium.org/wiki/SMTP_example_sessions

Övning 4

- Testa att kontakta `mail.nackademin.se` med smtp-protokollet (t ex med `telnet`).

Övning 4 (om ni har tur...)

```
$ telnet mail.nackademin.se 25
Trying 192.71.164.33...
Connected to mail.nackademin.se.
220 shmail01.nackademin.local Microsoft ESMTP MAIL
Service ready at Sun, 16 Aug 2020 14:28:12 +0200
HELP
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT
HELP AUTH BDAT
QUIT
221 2.0.0 Service closing transmission channel
```

Mer sannolikt:

```
nevyn@linmishi ~> telnet mail.nackademin.se 25
Trying 52.98.151.82...
telnet: Unable to connect to remote host: Network is unreachable
```

Mer SMTP-exempel

Prata SMTP med hjälp av curl?! (exempel från https://ec.haxx.se/usingcurl/usingcurl-smtp):

```
curl smtp://mail.example.com --mail-from myself@example.com –
mail-rcpt receiver@example.com --upload-file email.txt
```

TLS

- **Transport Layer Security**
- Uppföljare till SSL ("Secure Sockets Layer")
- HTTP**S**
- Helt krypterad trafik
- SMTP kan köras över TLS

Prata SMTP+TLS

```
openssl s_client -connect mail.example.com:587 -starttls smtp
```

```
curl --ssl smtp://mail.example.com --mail-from myself@example.com
--mail-rcpt receiver@example.com --upload-file email.txt -- user
'user@your-account.com:your-account- password'
```

Hur du bäst kör din egen mail-server

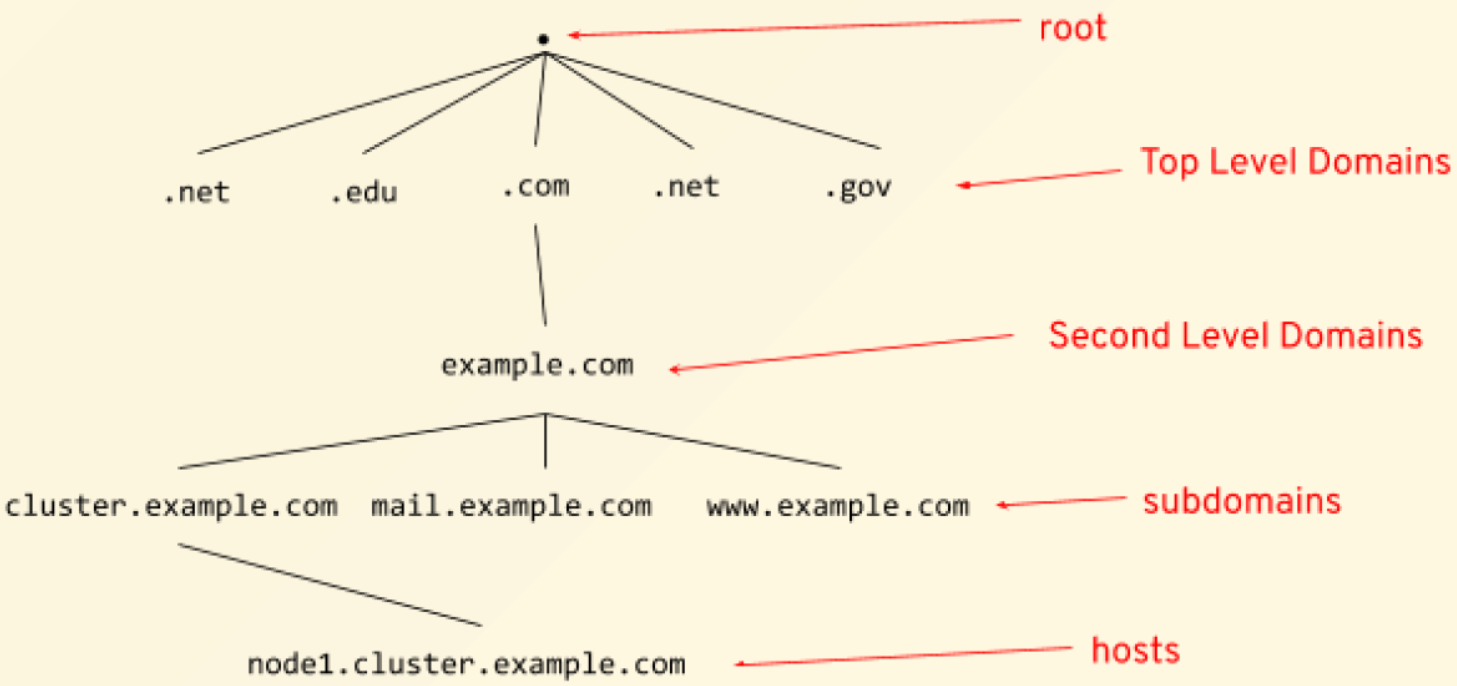
- inte (om du kan undvika det).
  - du kommer få otroliga mängder spam
  - din smtp-server kommer inte vara vitlistad hos världen så din mail kommer inte komma fram
  - du kommer bli hackad
  - tusen varianter på mail-klienter, hälften kommer bete sig buggigt
- Istället: sendgrid, din leverantörs SMTP-server (heroku, loopia, whatev), el dyl.

DNS

Domain Name System, DNS

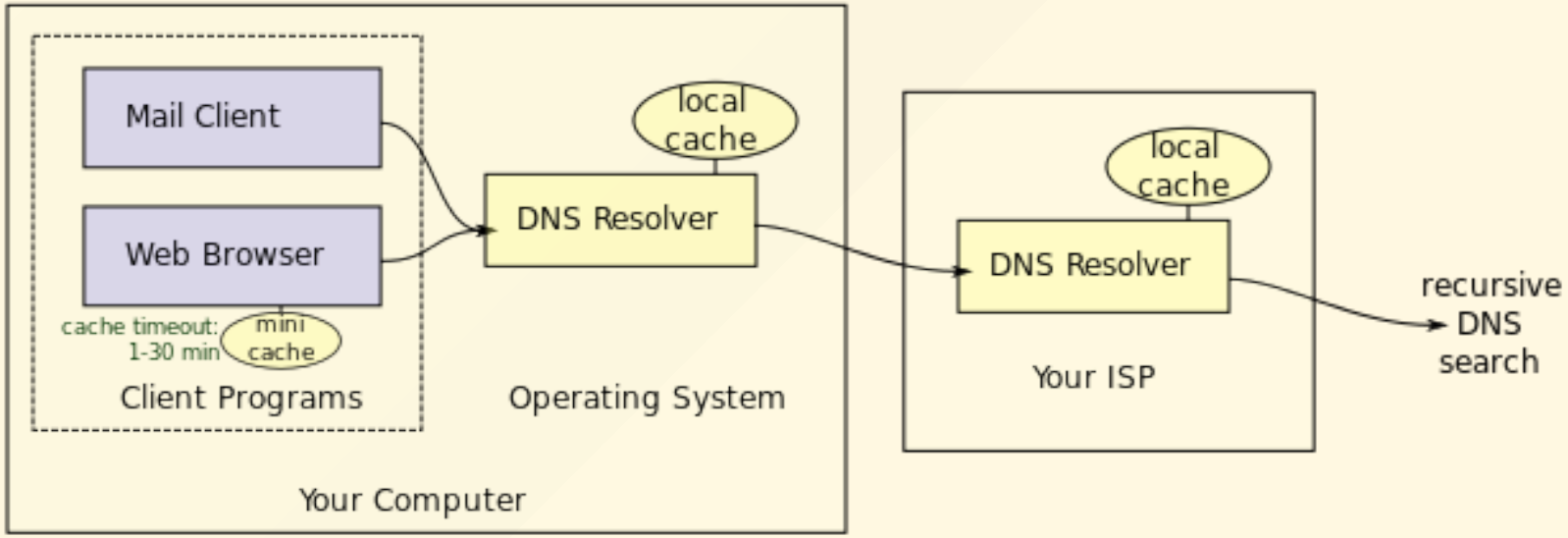
- Uppslagning av **namn** ➡️ **IP**
- Hierarkiskt: domäner (`google.com`) under toppdomäner (`.com`)
- "DNS records"

DNS



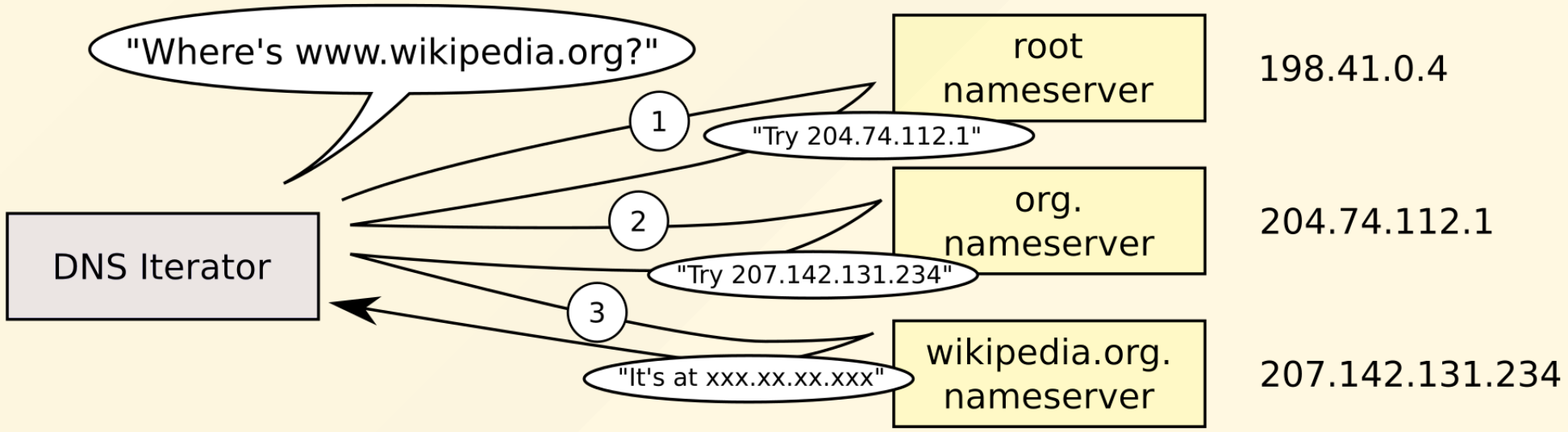
(redhat.com/sysadmin/dns-domain-name-servers)

DNS



(wikipedia.org/wiki/Domain_Name_System)

DNS



(wikipedia.org/wiki/Domain_Name_System)

DNS: två typer av servrar

- Authorative name server
  - Den som styr data för en eller flera specifika domäner
- Recursive resolver
  - Cachead data för uppslagning
  - Skickar frågan vidare vid behov

Verktyg för uppslagning

`dig <name> <type>`

e g `dig www.theverge.com`

e g `dig theverge.com MX`

`nslookup <name>`

e g `nslookup theverge.com`

DNS record types

typ	beskrivning
A	Mappa namn mot ipv4-adress
AAAA	Samma, fast ipv6
CNAME	Alias från ett namn till ett annat namn
MX	Peka ut mailserver för (sub)domänen
NS	Peka ut namnserver för domänen
TXT	Arbiträrt textfält; används ofta för app-specifik data, verifieringar, etc
PTR	Mappa IP-adress mot namn (motsats till A)

DNS records

```
<name>                  <ttl>    IN       <type>   <data>

t ex...

nackademin.se.          3600     IN       A        217.198.66.51
```

DNS records, exempel

```
> dig www.dnsimple.com
;; ANSWER SECTION:
www.dnsimple.com. 3600 IN CNAME dnsimple.com.
dnsimple.com. 60 IN A 104.245.210.170

> dig dnsimple.com mx
;; ANSWER SECTION:
dnsimple.com. 3600 IN MX 5 alt2.aspmx.l.google.com.
dnsimple.com. 3600 IN MX 5 alt1.aspmx.l.google.com.
dnsimple.com. 3600 IN MX 10 alt3.aspmx.l.google.com.
dnsimple.com. 3600 IN MX 10 alt4.aspmx.l.google.com.
dnsimple.com. 3600 IN MX 1 aspmx.l.google.com.
```

DNS records, exempel

```
> dig www.dnsimple.com ns
;; ANSWER SECTION:
dnsimple.com. 3600 IN NS ns4.dnsimple.com.
dnsimple.com. 3600 IN NS ns1.dnsimple.com.
dnsimple.com. 3600 IN NS ns3.dnsimple.com.
dnsimple.com. 3600 IN NS ns2.dnsimple.com.

> dig dnsimple.com txt
;; ANSWER SECTION:
dnsimple.com. 3600 IN TXT "MS=ms34502024"
dnsimple.com. 60 IN TXT "google-site-
verification=1LkF3IUYGELUtiSYhEtHI_UgDcpoKOvkD4LNrxSw7p0"
```

Övning 6

Vad kan ni utläsa av följande DNS records?

```
foobar.se.       3600  IN  A       5.150.254.28
mail.foobar.se.  3595  IN  A       5.150.254.28
www.foobar.se.   2842  IN  CNAME   foobar.se.
foobar.se.       3600  IN  MX   10 foobar-se.mx1.staysecuregroup.com.
foobar.se.       3600  IN  MX   20 foobar-se.mx2.staysecuregroup.net.
```

Övning 6

- Namnen `foobar.se`, `www.foobar.se` och `mail.foobar.se` pekar alla på samma server: `5.150.254.28`.
- Mail till `foobar.se` hanteras i första hand av `foobar-se.mx1.staysecuregroup.com` och i andra hand av `foobar-se.mx2.staysecuregroup.net`.

Konfigurera DNS

- `/etc/hosts` -- det som användes innan DNS fanns! nu, manuella namn-till-ip-mappningar.
- `/etc/resolv.conf`: peka ut namn-server för systemet. brukade vara massa meck med att filen skrevs över av dhcp, etc... sköts nuförtiden av systemd
- `/etc/host.conf`: i vilken ordning ska olika host name resolvers användas? hosts, bind, etc

Konfigurera DNS: bind

> BIND (/ˈbaɪnd/, or named (pronounced name-dee: /ˈneɪmdiː/, short for name daemon), is an implementation of the Domain Name System (DNS) of the Internet. It performs both of the main DNS server roles, acting as an authoritative name server for domains, and acting as a recursive resolver in the network.

- `apt install bind9 bind9utils bind9-doc`
- `named` är binds daemon
- `/etc/bind` -- bind9-inställningar, konfigurera din bind0-server
  - `./named.conf.options` för att konfigurera beteende
  - `/named.conf.local` för att lägga in dina enga zoner t ex

Konfigurera DNS: zoner

> A DNS zone is any distinct, contiguous portion of the domain name space in the Domain Name System (DNS) for which administrative responsibility has been delegated to a single manager.

Konfigurera DNS: egen bind-server!

Två potentiella resurser:

- https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04
- https://www.youtube.com/watch?v=EDBvowAOT4s

Övning 7

Gör din Linux-maskin till en DNS-server med named, och gör så den är auktorativ för `exempel.se` (eller valfri annan domän).

Fortsätt skicka alla andra förfrågningar till den name server du använder just nu.

- Lägg minst in ett A record och ett CNAME record
- Tänk på att backa upp relevanta filer innan du labbar, så att du enkelt kan gå tillbaka sedan

Övning 7: Lösning

1. `apt install bind9 bind9utils bind9-doc`
2. "Fortsätt skicka andra förfrågningar" => vi vill vara en "recursive resolver":
   - `pico /etc/bind/named.conf.options`
   - lägg till `forwarders { 1.1.1.1; };` för att säga att det är nästa hopp efter oss
   - lägg till `allow-recursion { any; };` -- tillåt vem som helst att använda oss som recursive resolver

Övning 7: Lösning

3. I `/etc/bind`, använd db.local som template för vår zon:
   `sudo cp db.local db.minzon`
4. Vi måste lägga zonen det i en conf-fil också!
   - `sudo pico named.conf.local`

```
zone "minzon" {
        type master;
        file "/etc/bind/db.minzon";
};
```

Övning 7: Lösning

pro-tip: `tail -f /var/log/syslog` i ett separat terminal-fönster för att hitta fel. Och/eller, använd `named-checkconf`.

5. Dags att editera vår zon. `pico /etc/bind/db.minzon`
6. Ändra `@TTL` och "negative cache ttl" till 500
7. Se till att lägga in rätt zon-namn i SOA:
   `@ IN SOA minzon. root.localhost. (`
8. Lägg in de A och CNAME records du vill ha

```
$TTL    500
@       IN      SOA     minzon.          root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         500 )          ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       172.20.140.75
nevyn   IN      A       172.20.140.75
hej     IN      CNAME   nevyn.itinf
```

9. `sudo systemctl restart bind9`

DNS misc

- Round robin -- flera A-records för samma domän
- Seriös setup: använd en gömd main-server, och sedan flera publika servrar som använder den gömda main som authority

Sätt "min" dator som din DNS:

- `sudo pico /etc/systemd/resolved.conf`
- `DNS=10.6.69.100`
- `sudo systemctl restart systemd-resolved`

Tillbakablick, reflektion, kommentarer...