

Kytkimet, reitittimet, palomuurit

- Kytkin (ja hubi): kaikki liikenne välitetään kaikille samaan kytkimeen kytketyille koneille suoraan, ei tarvitse omaa IP-osoitetta
- Reititin: ohjaa liikennettä verkkoalueiden välillä, useita omia IP-osoitteita
- Palomuuuri: suodattaa (valikoi) ja mahdollisesti muokkaa välitettäviä paketteja (vrt. myös ns. softapalomuuuri)
- Yleensä palomuuuri on myös reititin (poikkeuksena siltapalomuuuri (bridged tai bridging firewall))

Verkko-osoitteet ja -alueet

- Ipv4-osoite: 32 bittiä, xxx.xxx.xxx.xxx, xxx = 0...255
- Privaattiosoitteet 192.168.*.*, 172.{16...23}.*.*, 10.*.*.* eivät näy maailmalle
- Samassa aliverkossa oleviin pääsee suoraan, muihin yhdyskäytävän (gateway) kautta
- Netmask kertoo aliverkon koon (bittimaski); esim. 8-bittinen aliverkko 192.168.1.0/24 -> 255.255.255.0 (binäärinä 11111111.11111111.11111111.00000000), 10-bittinen 172.16.4.0/22 -> 255.255.252.0 (11111111.11111111.11111100.00000000)

Reititys

- Reitti (route) määrittää mitä kautta oman aliverkon ulkopuolelle päästään
- Esim. IP 192.168.1.3, netmask 255.255.255.0
- Aliverkko 192.168.1.0/24, osoitteisiin 192.168.1.* pääsee suoraan
- Oletusreitti: `route add default gw 192.168.1.1`
- Reititys aliverkkoon 172.16.0.0/16 eri yhdyskäytävällä:
`route add -net 172.16.0.0/16 gw 192.168.1.5`
- Reitin poisto: `route delete ...`

/etc/network/interfaces

```
auto lo
```

```
iface lo inet loopback
```

```
auto eth0
```

```
iface eth0 inet static
```

```
    address 172.20.209.6
```

```
    netmask 255.255.0.0
```

```
    network 172.20.0.0
```

```
    broadcast 172.20.255.255
```

```
    gateway 172.20.0.1
```

DNS: Domain Name Service

- Koneen nimi <-> osoite
- A-record = koneen oma IPv4 -osoite
- Muita: MX = Mail Exchanger, AAAA = IPv6-osoite, CNAME = alias, NS = name server, PTR = pointer (reverse), TXT = vapaa teksti, SOA = start of authority
- host [-t type] nimi [tai osoite]
- dig [paljon optioita]
- /etc/resolv.conf: nimipalvelimet, oletusdomain
- Vrt. /etc/hosts

Portit

- Portti = 16-bittinen numero, jota jokin palvelu (ohjelma) kuuntelee
- 0-1023 System (privileged, systeemiprosesseille) ja 1024-49151 User varattuja, 49152-65535 Dynamic/Private (sisäisiin/tilapäisiin tarpeisiin)
- Varattujen porttien luettelo:
<http://iana.org/assignments/port-numbers>
- Esim. 22 = ssh, 80 = http, 8080 = http_alt, 443 = https, 5900 = vnc
- /etc/services

Network Address Translation

- NAT: palomuuuri muuntaa osoitteen toiseksi (yleensä julkisen yksityiseksi)
- "Full NAT" (1-to-1 NAT): yhtä (julkista) osoitetta vastaa yksi (yksityinen) osoite
- "One-to-many NAT" (pNAT): monta (yksityistä) osoitetta -> yksi (julkinen) osoite; vaihtaa porttinumeroita julkisella puolella, ongelmallinen palvelinten kanssa

Kurssin verkkoalueet

- JY:n verkkoalue 130.234.0.0/16
- Sisäverkko 1-to-1 NATin takana: 172.20.0.0/16, 172.20.x.y
↔ 130.234.x.y (kun x=208,209)
- Alustakone lonka7.it.jyu.fi, 130.234.208.17, sisäverkossa
172.20.208.17
- Kurssin virtuaalikoneet 130.234.209.x, sisäverkossa
172.20.209.x
- Sisäverkon DNS-palvelin 172.20.0.2, gateway 172.20.0.1
- s001.vm.it.jyu.fi = 130.234.209.1 jne

Virtuaalikoneen asennus (virt-install)

Tarvittavat tiedot (virt-install optiot):

- Koneen nimi (--name / -n)
- Levyimagen paikka ja koko (--disk)
- Muistin (RAM) määrä (--ram / -r)
- Asennusmedia (--cdrom / -c tai --location / -l)
- Verkkoasetukset (--network / -w)
- --arch, --vcpus, --cpu, --import ...

Virtuaalikoneen asennus 2

Levyimage voi olla normaali tiedosto tai mikä tahansa "looginen levy" (fyysinenkin levy tai levyosio, tai LVM:n kanssa looginen volume). Myös levyohjaimen tyyppi voidaan valita, oletus on IDE, mutta yleensä "virtio" on parempi.

Tiedoston tapauksessa virt-install osaa luoda sen, kun kerrotaan polku ja koko (GB):

virt-install ...

--disk path=\$HOME/disk1.img,size=5,bus=virtio

Virtuaalikoneen asennus 3

Oletuksena virt-install tekee virtuaalikoneelle sisäisesti many-to-1 NATatun verkon 192.168.122.* -alueelle, jolloin siihen ei pääse käsiksi kuin alustakoneesta ilman eri säätöä.

Haluttaessa täydelliset yhteydet sisäänkinpään käytetään siltaverkkoa (bridged), jolloin VM näkyy suoraan isäntäkoneen verkkosegmentissä:

```
virt-install ... --network bridge=br0
```

IP-osoite jne asetetaan myöhemmin (kuten normaalisti konetta asennettaessa, dhcp:llä tai käsin)

Virtuaalikoneen asennus 4

Asennusmedia voi olla (virtuaalinen tai oikea) optinen media (cdrom image) tai URL:

```
virt-install ... --cdrom /srv/ftp/iso/image.iso
```

```
virt-install ... --location
```

```
http://archive.ubuntu.com/ubuntu/dists/trusty/main/installer-amd64/
```

Virtuaalikoneen asennus 5

Oletuksena käytettävissä on graafinen konsoli. Vaihtoehto on määritellä sarjaporttikonsoli:

```
virt-install ... --graphics none
```

```
--extra-args='console=ttyS0,115200n8 serial'
```

(toimii vain --location ... -asennuksella, cd-image on muokattava sarjaporttiasennusta varten)

Yhteyden konsoliin saa sitten komennolla

```
virsh --connect qemu:///system console kone
```

Virtuaalikoneen asennus 6

Esimerkki:

```
virt-install --name tt1 --ram 256 --disk  
path=$HOME/tt1.img,size=2 --network  
bridge=br0 --cdrom ubuntu.iso
```

IP-osoite, netmask, gateway jne annetaan normaaliin tapaan asennuksen yhteydessä.

Virtuaalikoneen hallinta

virsh start kone

virsh shutdown kone

virsh destroy kone

virsh suspend kone

virsh resume kone

virsh save kone

Virtuaalikoneen hallinta 2

virt-viewer kone

virsh connect ... kone

virsh edit kone

virsh dumpxml kone > kone.xml

virsh undefine kone

virsh define kone.xml

Käyttäjien hallinta

`useradd -u uid -U -m -s /bin/bash -c 'nimi' login`

`groupadd -g gid group`

`usermod ...`

`userdel -r login`

`groupdel group`

`vrt. adduser`

PAM

”Pluggable authentication modules”

Kerberos-autentikointi (JY:ssä):

```
sudo apt-get install libpam-krb5
```

```
realm: AD.JYU.FI
```