Linux-virtuaalipalvelimen ylläpito

Kevät 2018

Tapani Tarvainen
sekä Matias Kangas, Pyry Kotilainen ja Ilona Nurminen

Tarkoitus antaa riittävät valmiudet oman palvelimen ylläpitoon palvelinkäytön harjoittelua ja sovellusten kokeilua varten sekä perustiedot virtuaalikoneiden asentamisesta, hallinnasta ja erityispiirteistä.

Kotisivu: https://kurssit.it.jyu.fi/TIES478/


AN ENGINEER HELPING A DESIGNER
NO PROBLEM, WE CAN FIX THIS ON THE TERMINAL
CLACK
CLACK
WHOA, YOU'RE A HACKER!
NO, IT'S JUST THE TERMINAL.
WHERE ARE ALL THE BUTTONS, ICONS, AND DROPDOWN MENUS?
IS THIS... THE MATRIX?
YES.
PABLO STANLEY

Kurssin suoritus 1

- Demot: enimmäkseen ohjattua työskentelyä, kaikki tekevät kaiken itse
- Jokainen saa oman virtuaalikoneen (luodaan ensimmäisissä demoissa), myöhemmin useampiakin, joille tehdään sitä sun tätä ”asiakkaiden” ja ”esimiehen” pyynnöstä
- Koneisiin tulee vikoja, myös demojen välissä odottamattomina aikoina, ne pitää huomata ja korjata

Kurssin suoritus 2

- Demoista pidetään lokikirjaa, josta selviää, että demot on tehty itse ja josta voi itse tarkistaa miten
- Oma virtuaalikoneen asennuksen ja ylläpidon dokumentointi niin hyvin, että koneen tuhoutuessa sen pystyy asentamaan uusiksi lokin perusteella
- Tentti: mikroluokassa, jokainen saa oman (tenttiä varten tehdyn) virtuaalikoneen, jossa on jotain vikaa vikaa vikaa... Muistiinpanoja ja hakukoneitakin saa käyttää, vain avun kysyminen ja muu yhteistyö on kielletty

Demotehtävistä

- Demot tehtään tai ainakin aloitetaan ohjauksissa ja viimeistellään tarvittaessa omalla ajalla.
- Demot rakentuvat edellisten pohjalle, joten ne pitää tehdä järjestyksessä.
- Tehtävissä viitataan usein yliopiston käyttäjätunnukseesi merkkijonoilla TUNNUS tai $TUNNUS. Komennoissa nämä tulee aina korvata omalla tunnuksella!
- Tehtävänannoissa aina implisiittisenä lisänä ”ja hoida vastaantulevat odottamattomat ongelmat” (ja joskus varsinainen tehtävä onkin vasta siinä).

Linux

- Periaatteessa Linux on vain käyttöjärjestelmän ydin (kernel), yleisemmin myös ”Linux -pohjainen käyttöjärjestelmäjakelu”: Linux ydin, yleensä Gnu-varusohjelmisto, valikoima muuta ohjelmistoa, pakettivarasto asennusta ja päivitystä varten
- Enemmistö maailman www-palvelimista Linux-pohjaisia
- Edullinen (ei lisenssimaksuja) ja helposti kustomoitavissa (Open Source)
- Esim. Ubuntu, RHEL, CentOS, Debian, Fedora, (Open)SuSE, Gentoo, Arch, Slackware ... (ks. distrowatch.org)
- Tällä kurssilla ensisijaisena Ubuntu

Palvelin

- Fyysinen tai virtuaalinen kone tai ohjelma, joka tarjoaa jotain palvelua/palveluita
- Etäkäyttö (mitään fyysistä konsolia ei yleensä ole)
- Useita (samanaikaisiakin) käyttäjiä (ihmisiä, toisia koneita tai ohjelmia...)
- Päällä yleensä 24/7
- Tarjoaa palvelun tai palveluita, esim: www, ftp, levytila, sähköposti, tietokanta, laskenta, irc, jabber, suorakäyttö (shell), varmuuskopiointi, pelit, webcam, palomuuri, vpn, dns, dhcp, tftp, ntp ...

Virtuaali-

- Ei omaa, dedikoitua fyysistä konetta, vaan ohjelma, joka esittää sellaista toisen koneen sisällä (mahdollisesti liikkuen koneesta toiseen)
- Etuja: Hinta, ylläpidon (raudan/palvelun) ulkoistaminen, skaalattavuus, käyttöönoton ja resurssien lisäämisen nopeus
- Haittoja: jaettujen resurssien vaikea ennakoitavuus, tietoturvaongelmat (Spectre!), datan fyysinen sijainti, lainsäädäntö (GDPR!)

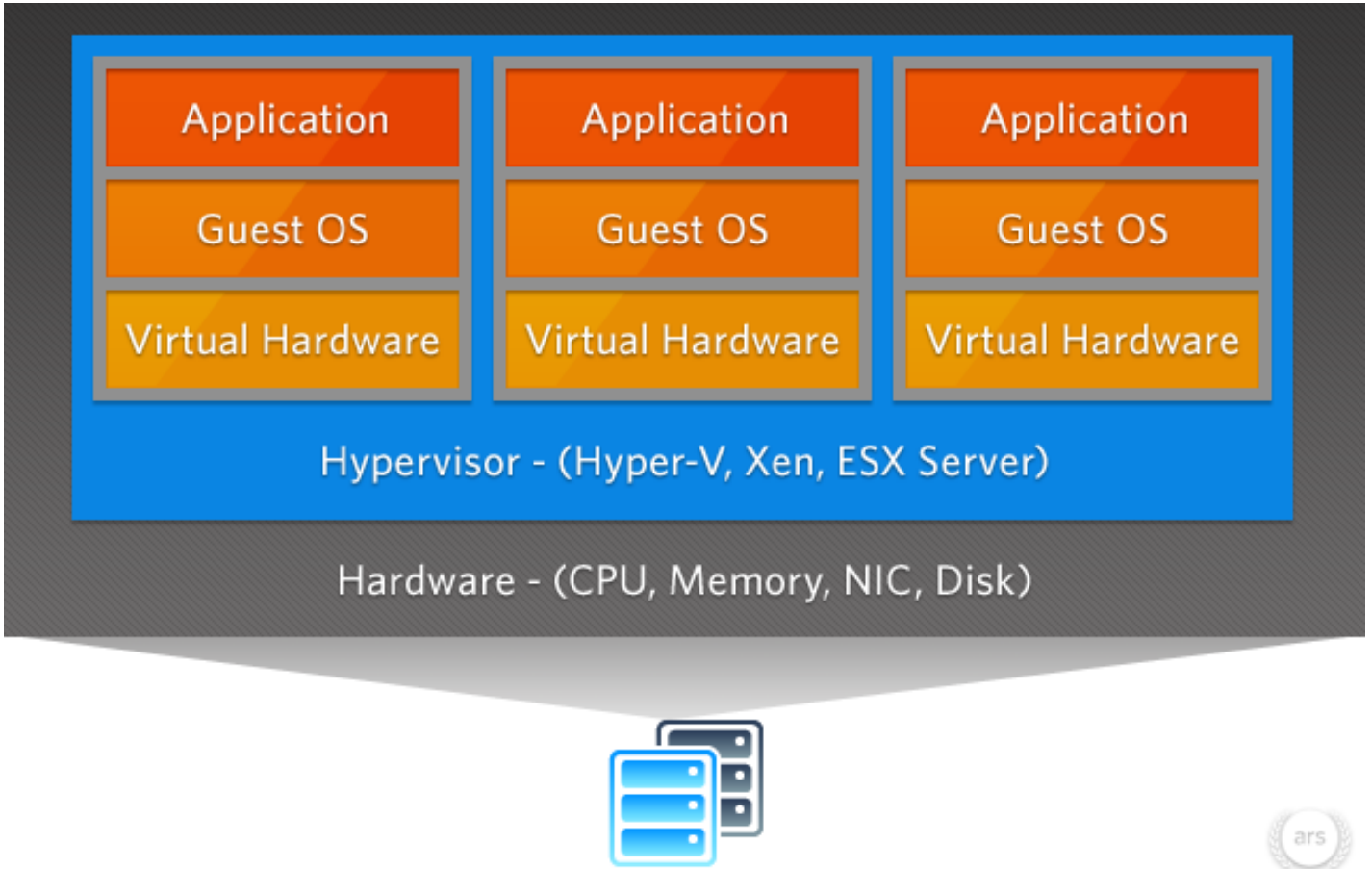
Monenlaista virtualisointia

- Virtuaalikoneet (full hardware virtualization)
  - Virtuaalikoneen sisältä kuin ”oikea” rautakone
- Kontit (containers, OS-level virtualization)
  - Alustakoneen käyttöjärjestelmä mutta omat kirjastot jne
- Ajoympäristöt (application virtualization)
  - Eristetty sovellusympäristö, usein palveluna (PaaS, Faas)
- Palvelun virtualisointi (virtual hosting)
  - Monta IP-osoitetta tai nimeä samalla koneella
- Virtuaaliverkot (VPN, VLAN), -levyt, -laitteet ...

Virtuaalikone

- Ei dedikoitua fyysistä konetta: samassa raudassa useita virtuaalikoneita, virtuaalikone voi siirtyä fyysisestä koneesta toiseen
- Hypervisor luo fyysistä konetta simuloivan ympäristön, johon voidaan asentaa käyttöjärjestelmä kuten suoraan rautaan; virtuaalikoneen käyttöjärjestelmä voi olla eri kuin alustakoneen
- Native (hypervisor ”suoraan raudassa”) vs. Hosted (hypervisor alustakoneen käyttöjärjestelmän päällä)
- Esim. VMWare, VirtualBox, XenServer, Hyper-V, Qemu...
- Tällä kurssilla käytössä KVM (sort-of native)

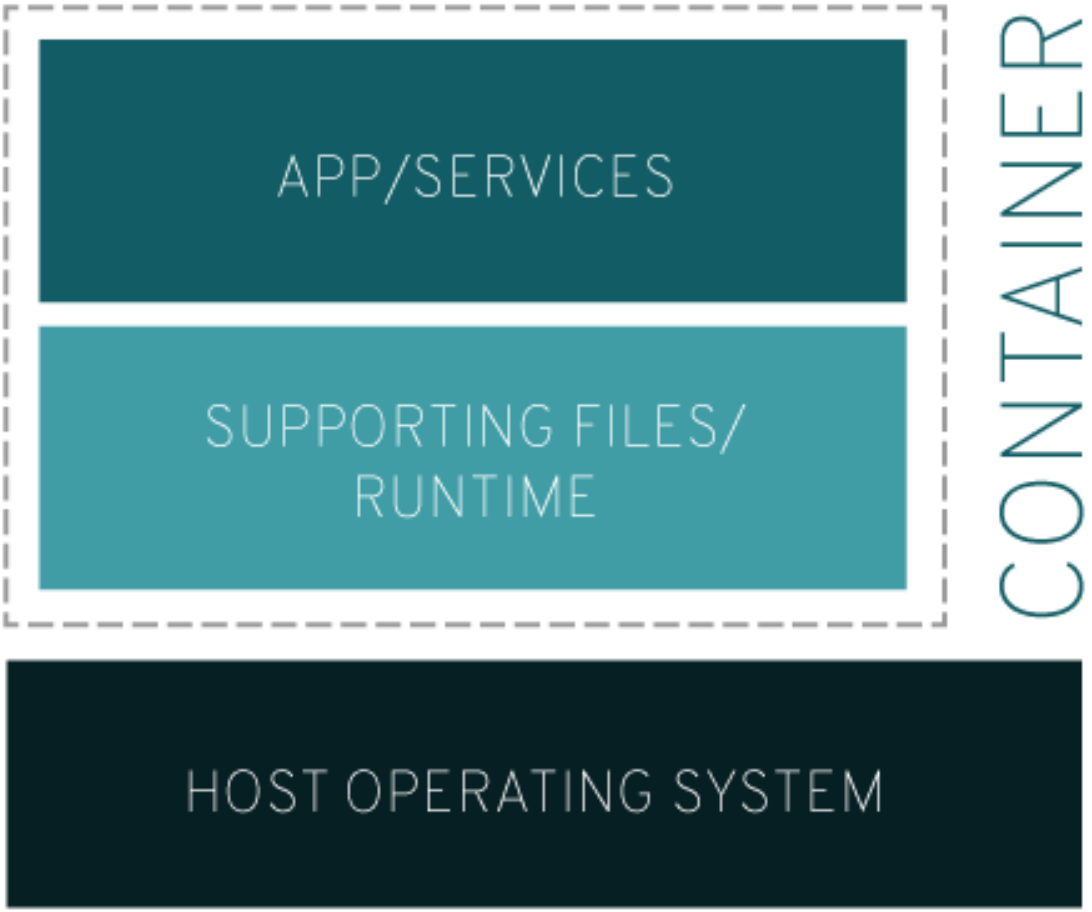
Virtuaalikone



Kontti (container)

- Sama käyttöjärjestelmä ja ydin kuin alustakoneessa
- Tiedostojärjestelmä (pääosin) oma kirjastoja myöten, laitetiedostot (osin) yleensä jaettuja alustakoneen kanssa
- Ei hypervisoria, prosessit samalla tasolla kuin alustakoneen omat mutta eristettynä (vrt. chroot)
- Kevyt (nopea käynnistää ja tuhota)
- Esim. Docker, LXC, OpenVZ

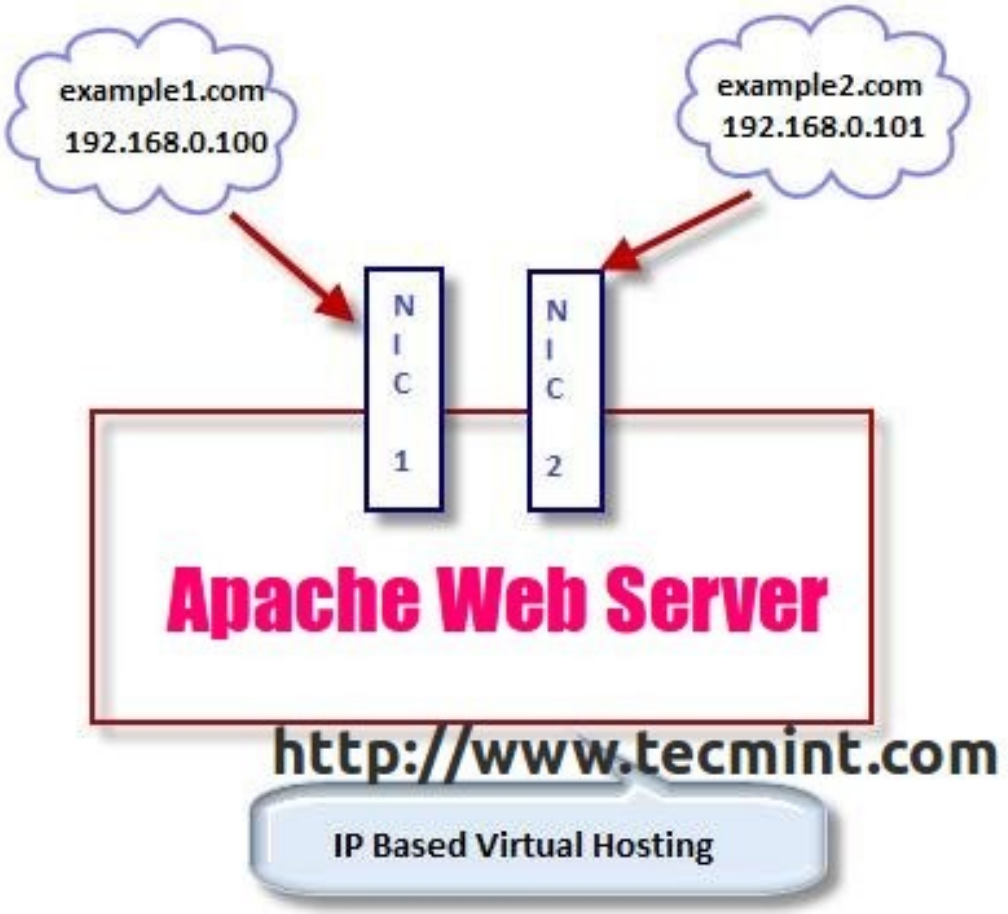
Kontti, container



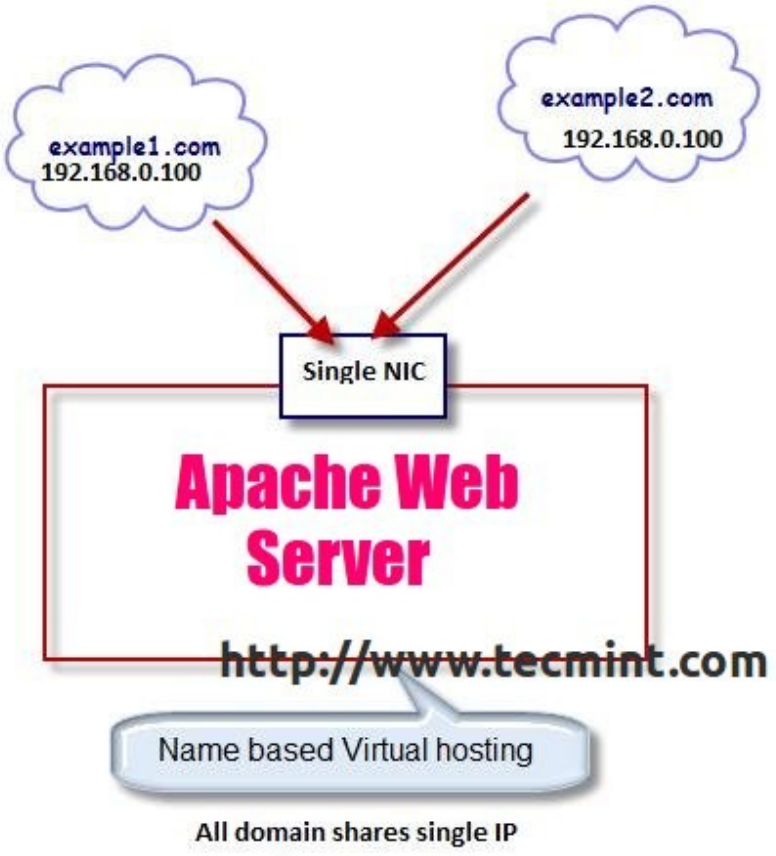
Virtual host

- Yksi (virtuaalinen tai fyysinen) kone, yksi käyttöjärjestelmä, yksi tiedostojärjestelmä
- Monta nimeä tai IP:tä
- Palvelinohjelma (esim. web server kuten Apache) tunnistaa millä osoitteella (IP:llä tai nimellä) sitä kutsutaan ja vastaa sen mukaan eri tavoin, tai eri IP:t voidaan ohjata eri palvelinohjelmille
- Monet protokollat eivät välitä nimeä jolloin sitä ei voi käyttää virtualisointiin, http kyllä

IP-pohjainen virtual host



Nimipohjainen virtual host



Sisäkkäistä virtualisointia

- Eritasoisia virtualisointeja voi olla käytössä yhtaikaa
- Esim. virtuaalikoneen sisällä kontti jonka sisällä virtual hosting
- Samantasoisia virtualisointeja ei yleensä voi olla sisäkkäin

Ylläpito 1

- Käyttöjärjestelmän ja muiden ohjelmien ja laitteiden asennus, konfigurointi ja päivittäminen
- Käyttäjien ja oikeuksien hallinta
- Resurssien hallinta (levytila, muisti, cpu jne)
- Tietoturva ja -suoja
- Varmuuskopiointi
- Dokumentointi

Ylläpito 2

Monitorointi ja ongelmien ratkaiseminen

https://xkcd.com/705

Sisältö 1

- Komentorivityöskentelyn perusteet, ssh
- Shell-ohjelmointi
- Oikeuksien hallinta, ryhmät, root, su, sudo
- Prosessit (&, ps, kill, bg, fg, jobs, top, lsof)
- Ohjelmapakettien etsiminen, asentaminen, poistaminen jne (apt-get, dpkg-reconfigure...)
- Levytilan hallinta (fdisk, parted, mkfs, mount, umount, /etc/fstab, LVM...)

Sisältö 2

- IP-osoitteet (IPv4), julkiset vs. privaattiosoitteet
- Kytkimet, reitittimet, palomuurit
- Reititys (routing, gateways, netmask)
- Portit
- NAT (network address translation)
- Nimipalvelu (DNS), host, dig, resolv.conf

Sisältö 3

- Käyttöjärjestelmän asennus
- KVM-virtuaalikoneen luonti ja hallinta: virt-install, virsh, virt-viewer, kvm, qemu-img
- WWW-palvelimen asennus ja konfigurointi
- ftp-palvelimen asennus ja konfigurointi
- Palomuurit, iptables
- (jatkuu...)

Komentorivityöskentelyn alkeet

- Bourne/POSIX -shellit, erityisesti bash
- Yleisiä komentoja: man ls cp mv ln rm df cat mkdir rmdir cd pwd echo grep sort
- Muuttujat: var=x; echo $var; export var
- Ulkoisten ohjelmien suoritus, $PATH
- stdin, stdout, stderr, uudelleensuuntaus (exec, <, >, |, >>, >|, <<)
- Erikoismerkit: & ; ( ) $ ` \ " ' * ? [# ~ = % !
- Alustustiedostot .bash_profile .bash_login .profile .bashrc .bash_logout $BASH_ENV

Etäkäyttö

- ssh [-X] [user@]kone
- Windowsista putty tms
- scp file[...] [user@]kone:[dir/file]
- ssh-keygen -t rsa ...
- ~/.ssh/authorized_keys
- ~/.ssh/config, /etc/ssh/{ssh_config,sshd_config}
- rsync [-av] file[...] [user@]kone:[dir/file]
- VPN (ks. ohjeet IT-palveluiden sivuilta)

Shell-ohjelmointi (scripting)

- ./file, sh file, sh -c 'komentoja', . file (source)
- #! /bin/bash -ex jne
- Komennon paluuarvo, $?
- if komento; then ... ; else ... ; fi
- while komento; do ...; done
- www.mit.jyu.fi/opiskelu/kurssit/unixshell01/

Omistajat ja oikeudet

- Unixin perusoikeusmalli: omistaja (user), ryhmä (group) ja muut (others), oikeuksia read(r), write(w), execute/search(x), suid(s), sticky(t)
- chmod ugo+rwx file; chmod 1777 dir
- ACL:t (Access Control Lists)
- /etc/passwd /etc/group /etc/shadow
- chown chgrp groupmod usermod newgrp
- Superuser (root), su, sudo (/etc/sudoers, visudo)

Prosessit

- Foreground vs background, parents and children, zombies
- ps, top, jobs
- & bg fg
- kill, killall
- lsof, fuser

Ohjelmapakettien hallinta

- dpkg & apt: Debian-pohjaisissa jakeluissa
- apt-cache search ...
- apt-get install remove purge update upgrade dist-upgrade clean autoremove
- dpkg -i -l --configure --remove --purge
- dpkg-reconfigure, dpkg-query
- /etc/apt/sources.list, /etc/apt/apt-conf.d ...
- /etc/update-manager

Levytila

- Partitiointi (ositus): fdisk, parted
- Tiedostojärjestelmätyypit (ext4, xfs, tmpfs...)
- Tiedostojärjestelmän luonti: mkfs
- Tiedostojärjestelmän tarkistus: fsck
- mount, umount, /etc/fstab
- /dev/...
- LVM, md, cryptsetup

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
- Palomuuri: suodattaa (valikoi) ja mahdollisesti muokkaa välitettäviä paketteja (vrt. myös ns. softapalomuuri)
- Yleensä palomuuri on myös reititin (poikkeuksena siltapalomuuri (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)
- IPv6-osoitteet 128-bittisiä, erottimena kaksoispiste, esim. 2001:4b98:dc0:45:216:3eff:fe5e:2e10

IP-osoite

”Koneella X on IP-osoite Y” tarkoittaa...

- jokin Ylempi Taho™ sanoo niin (DNS, reititys, IT-palvelut...)
- kone itse uskoo omistavansa IP:n
  - nähdessään paketin, jonka kohdeosoite on ko. IP, kone ottaa sen käsiteltäväkseen, ja lähettäessään paketteja käyttää ko. IP:tä lähettäjäosoitteena
- samalla koneella voi olla monta IP:tä (myös samalla interfacella), myös useita sekä IPv4- että IPv6-osoitteita
- monella koneella voi olla sama IP, myös samassa aliverkossa (tarkoituksella tai vahingossa)

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: ip route add default via 192.168.1.1
- Reititys aliverkkoon 172.16.0.0/16 eri yhdyskäytävällä: ip route add 172.16.0.0/16 via 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: palomuuri 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. Yleisin NAT, ensisijainen tarkoitus säästää julkisia IPv4-osoitteita
- Vain IPv4:n kanssa, IPv6:n kanssa tarpeeton