Data Networks

Janno Lamus
+372 504 7043
janno@gurud.ee

Tere tulemast!
Saame tuttavaks.

Kes oled?
Tööd?
Hobid?
Miks siin?
Kass / koer?
Õlu / vein?
Lumelaud / suusk?

Kodukord

* Reegel nr. 1: see kes teise seadme häkib, paneb selle ise üles
* Aita teisi
* Tarbi piisavalt vedelikke, sukrut ja valke
* Küsi julgelt

Küberleksikon
https://akit.cyber.ee
Kuutõrvaja võrgu osa
https://kuutorvaja.eenet.ee/wiki/V%C3%B5rgu_administreerimine

Suur pilt

Ajalugu
LAN - külapood
WAN - kõik maailma poed
Täna liigume pigem lihtsalt turvaliste ühenduste suunas, kõik ühes suures võrgus
Veatõrje, käideldavuse tagamine, paindlikkuse suurendamine link, liiasus
Bandwidth, BER, time delay, network security

Võrgud

Routing, rate, routers, gateways, switches, firewalls etc

Ethernet, optical fibre
e.g. LAN/MAN: CSMA/CD, Ethernet frame types,
VLAN tag (802.1q), FO cable qualities for SM
and MM, connectors, SFP module types,
wireless; WAN: MPLS, pdH, sdH networks

Võrgu(komponentide) elutsükkel

SLA 99,9% link
- SLA lepingu näidis, reaalsus on 97,5%

Võrgu kihid, ISO/OSI 7 kihti

väga mõistlik seletus on wikis

1. Füüsiline kiht (bitt)
kõik riistvara + eri tüüpi signaal n valgus, elekter erinevatel sagedustel
Näiteks: Kaabel, Wi-Fi raadiolained, fiiber
--> Praktikas on kihid kokku sulandunud, ainult raud on väga selgelt eristuv

2. Kanalikiht (kaader)
Füüsiline adresseerimine (MAC aadress)
Paketeerimine (bittidest moodustub kogum e. pakett)
Sünkroniseerimine
Vookontroll
Veaparandus
Pakettide/kaadrite märgistamine
Näiteks: Ethernet, ARP, VLAN
--> Kanali kihis lisatakse MAC aadress

3. Võrgukiht (pakett)
Protokollisisene adresseerimine (IP aadress)

IP aadresside haldus
Teekondade leidmine (üksik/kanal), ruutimine (marsruutimine)
Ummistuste lahendamine
Näiteks: Ruuterid
--> Võrgukihis lisatakse IP aadress

4. Transpordikiht (Segment)
andmevahetus rakenduste vahel, järjestab, saadab uuesti, vookontroll
Näiteks: protokolli valik, uuesti saatmine

Kuidas TCP segment töötab?
Suur andmemass jagatakse väiksemateks segmentideks.
Iga segment saadetakse oma päise info ja kontrollsummaga.
Vastuvõtja kasutab päises olevat järjestusnumbrit, et panna andmed õiges järjekorras kokku.
Vastuvõtja saadab saatjale kinnitusnumbri, mis tähendab, et segment on vastu võetud ja korras.
Kui segment kaduma läheb, saadetakse see uuesti.

5. Seansikiht (Andmed)
Loob, haldab, lõpetab ja jätkab loogilisi seansse
Näiteks: *cookie* haldus, *longpoll*, *websocket*

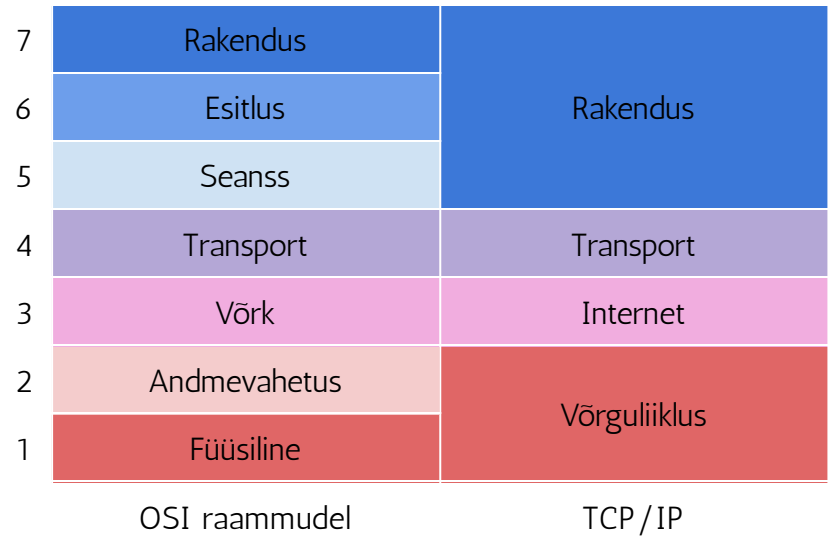
6. Esituskiht e süntaks (Andmed)
Andmete esituskujust sõltumatu tõlkekiht
Kokkuleppeline andmete esitlusviis
Andmete loetavaks muutmine
Andmete loetamatuks muutmine
Näiteks: kanali krüptimine (VPN, Wireguard), SFTP, JPG, JSON

7. Rakenduskiht (Andmed)
Kõik mida rakendused omavahel jutustavad
Lubatud on oma keel
Näiteks: HTTP, FTP, DNS, SMTP, IMAP

TCP 4 kihti

Kihid on veidi koomale tõmmatud. Link

TCP/IP mudeli kihid: 7 kihti versus 4 kihti



Protokollid

UDP
TCP/IPv4
TCP/IPv6
ICMP (ping protokoll)
NETBIOS :)
tegelikult on ka ftp, ppp, imap, smtp.... ka kõik ka protokollid, kuid seda siiski juba pigem TCP laiendusena

--> ära unusta NMAPi

Ruutimine

MAC aadress - seadme "füüsiline" tunnus ~kujul 00:EB:24:B2:05:AC
ARP tabel - MAC aadresside tabel - seob MAC aadressi IPga
DHCP - IPde jagamise teenus, kui arvuti läheb võrku
GW - GateWay ehk ruuter
DNS - Domain Name Service: annab domeeninimele IP aadressi
--> TEST: kirjuta mõni nimi + IP hosts faili ning pingi sisestatud nime

Teenused

Teenus sisaldab tihti ka oma protokolli laiendust
DNS - Domain Name Service - edastab domeeni vastu IP aadressi
FTP / SFTP - File Transfer Protocol - failiedastus
SSH - turvaline kanal kahe punkti vahel (LINUX all konsool, WIN PUTTY) "Secure Shell"
TELNET - kahesuunaline protokoll ja programm. Vanasti kasutati, eriti tore ka praegu

IMAP - meilide lugemine nii et meilid on serveris
POP3 - sikutab meilid alla (enam väga ei kasutata)
SMTP - meilide saatmine, võtab kirjad vastu saatjalt (esimene teenus)
HTTP - turvamata veeb reeglina port :80
HTTPS - turvatud veeb:443
IRC - suhtlusteenus
DHCP - jagab arvutitele ip aadresse
jms

Võrgu- ja leviaadress, TCP/IP mask

Lugemissoovitus (pilt on kohutav, aga sisu OK)
kahendsüsteemi kalulaator klassikaline kahendsüsteemis-arvutamine
Aadresside "cheat sheet" (kui see on ees, siis tegelikult pole rohkem midagi teada vaja)

```
255.255.255.0 = 11111111 11111111 11111111 00000000 = 3 baiti fikseeritud ehk “/24”
                3*8=24 ehk 24 ühte

255.255.254.0 = 11111111 11111111 11111110 00000000 ehk “/23”
                23 ühte jne

255.255.255.240 = 11111111 11111111 11111111 11110000 ehk “/28”
                  mitu ühte?
```

"255.255.255.255" - vorming kümnendsüsteemis
"/32" - CIDR-vorming (loe ühed kokku)
"11111111.11111111.11111111 11111111" - vorming kahendsüsteemis (binaarne) / bittides (iga bitt on 0 või 1)

võrguaadress - *netwok address* - esimene IP (ei saa kasutada IP aadressina)
leviaadress - *broadcast address* - viimane IP (ei saa kasutada IP aadressina)

Mitu hosti on võrgus, kui mask on..?

```
255.255.255.0   = 11111111.11111111.11111111.00000000 ehk /24 - 254 hosti (256 ip)
255.255.255.128 = 11111111.11111111.11111111.10000000 ehk /25 - 126 hosti (128 ip)
```

/-/

```
255.255.255.248 = 11111111.11111111.11111111.11111000 ehk /29 - 6 hosti
```

Loogika: väga lihtsustatult võime öelda et 254-248=6

```
255.255.255.252 = 11111111.11111111.11111111.11111100 ehk /30 - 2 hosti
```

254-252=2

```
NB! 255.255.255.255 /32 - 0 hosti, 1 ip aadress
```

255-255=0 aga matemaatiliselt on tegemist siiski võrguga
MITU IP AADRESSI ON VÕRGUS? MITU HOSTI ON VÕRGUS?
GW IP: 10.1.1.1 mask: /25
IP: 0001010 00000001 00000001 00000001
MASK: 11111111 11111111 11111111 10000000

TCP/IP aadress

konverter 1 - binaarseks
konverter 2 - kõik

IPv4 kasutab 32-bitiseid aadresse
127.0.0.1 = 01111111 00000000 00000000 00000001
192.168.0.1 = 11000000 10101000 00000000 00000001
192.0.2.1 = 11000000 00000000 00000010 00000001

Kahendkoodi arvutamise abitabel

Mis asendis on bitt	1	0	1	0	1	0	0	0
Vastav summa	128	64	32	16	8	4	2	1

saame:
128 + 32 + 8 =
ehk 10101000 = 168

127.0.0.1 - oma arvuti e localhost
0.0.0.0 - tähistab ruutingus kõiki hoste
* - reeglina sama mis 0.0.0.0 - sõltub interpretaatorist
10.0.0.x - LAN klass A
172.16.0.x - LAN klass B (ei kasutata väga)
192.168.0.x - LAN klass C

võrguaadress (network): klassi kõige väiksem IP-aadress
n 192.168.0.0.
leviaadress (broadcast): `leviaadress = võrguaadress + aadresside koguarv alamklassis - 1`
n 192.168.0.255

WILDCARD
Näiteks: 0.0.0.0:443 -> server kuulab kogu masinal kõigil IP-del porti 443
Näiteks2: pordisuunamisel sisenev piirang 0.0.0.0 aktsepteerib kõiki IP aadresse

Brains on

Mitu IPd on võrgus ja mitu reaalset hosti
võrgus maskiga: 255.255.255.128
ja mis on selle võrgu numbriline mask kujul /zz /00000000 00000000 00000000 00000000
zz IPd?
zz hosti?
Kuju1?
Kuju2?
Võrgumaski lihtne peast arvutamine

Olgu meil võrgumask 255.255.255.224 kujul, tahame teada bittide arvu ja seda, mitu hosti on antud võrgus (koos leviaadressidega). Arvutus on lihtsalt peast tehtav:
– 255 ja 0 väärtused on triviaalselt kõik 1-d või kõik 0-d, need saab baidi kaupa kokku arvutada
– Neist erinev maski bait 224
- 256-224=32
– Seega on antud võrgus 32 eri IP-d
- ruutjuur 32-st on 5, millegagi
– (32 = 2 astmes 5) seega on hostiosa pikkus 5 bitti
– Maskis jääb võrguosale seega sellest baidist 8-5=3 bitti
– Seega on numbriliseks maskiks /27
----> sest 8+8+8+3=27 (11111111 11111111 11111111 11100000) m.o.t.t.
Khmm, mis see nüüd siis oli?!

Hands on 1

Ubuntu MATE install ja edaspidi tööjaamaks
winbox nüüd ka linux
Käime läbi ruuteri menüüd ja automaatseadistused
Väike ruuter tööle - mobiiliga peab saama wifisse
WAN: DHCP
LAN: eth2/bridge
+ DHCP sisevõrgus IPsi jagama

Hands on 2

Monitoorimine ja mõõtmine
ping, telnet, tracert
Data analyser (sniffer), NetScout, Wireshark
host, arp, routes, ping, tracepath, portmap, terminal
TCP pakett
* installi wireshark ja jälgi oma võrgu liiklust 2-10 sekundit
* tee oma väikesesse ruuterisse wifi
  - WiFi nimi <sinueesnimisinuperenimi>, parool: 1234567890
  - pane admin kasutajale parool: 111

Nullimine

1. Tarkvaraline
 - system - reset configuration
2. Riistvaraline
   - voolujuhe välja
   - nupp sisse (suurel punasel pastakas/kruvikas)
   - voolu juhe külge (midagi võiks põlema hakata)
   - hoia 5 sekundit ja lase lahti (nupp/pastakas)

Hands on 3

*** oleme nii kaugel, et meil on olemas (väike) wifi purk, mis saab automaatselt WAN IP ja jagab DHCPga aadresse 192.168.x.x

T U B L I !
..tõsta parem käsi kõrgemale ja aseta vasakule õla. Patsuta, naerata. :)

*** Wifi purk täpselt selline, nagu ta praegu on

* kui midagi ei tööta, tuleb ära parandada :)

Nüüd tuleb seadistada suur ruuter internetti ilma automaatikata (WAN osa ilma DHCPta)
Vihjed:
Identity
DHCP Client: disable

WAN: IP: tabelist eth1
ROUTES: 0.0.0.0/0 -> 10.1.1.1/24
DNS: 10.1.1.1
LAN: (handson1, samamoodi kui väiksel purgil, aga IP on 10.x.x.1)
BRIDGE aadress
DHCP + POOL
NETWORK (10.x.x.0/24->10.x.x.1)

192.168.<väikse ruuteri LAN kolmas nr+1>.x/24

Hands on 4

* HTTPS admin väljast wifi purki
suur ruuter: pordi suunamine 14<oma-eilne-nr> -> wifi ruuteri WAN IP peale porti 443
--- firewall - nat - dstnat - dst-nat
* DHCP reservatsioon
  - et wifi purgil väline (WAN) IP ei muutuks
  - ip - dhcp server - leases (mine rea sisse ja nupp STATIC, siis muuda)
väike ruuter e wifi purk
* genereeri CA sert (see millega allkirjastame)
- allkirjasta
* sert tule lisada HTTPS teenusele
* avame WAN pordis ligipääsu porti 443
  - ip - firewall - add ... :)

https://192.168.77.169:14<oma-eilne-nr>
https://192.168.77.181:14<oma-eilne-nr>
https://192.168.77.190:1412
https://192.168.77.191:1411
https://192.168.77.186:1414
https://192.168.77.183:1415
https://192.168.77.182:1416
https://192.168.77.179:1443
https://192.168.77.205:1443

T U B L I !!

Hands on 5

* VPN väljast 100% tööle (kui jõuab)

1. suures ruuteris suuname pordi 1194 wifi purki (wan ip eth1)
2. wifi purgis peme tegema FW reegli, mis võimaldab väljast kuulata port 1194 (nagu tegime 443)
3. ~~lisa ppp -> ovpn server binding~~
4. lisa ppp - profile Local: 10.0.77.1 + vpn pool
5. lisa ppp - secret + VPN profiil
6. vpn pool 10.0.77.101-199
   - 10.0.<sinu-üleeilne-nr>.x (10.0.11.x/24)
7. CA cert, sign, export
8. OpenVPN serveri sert, sign (kasuta ca serti allkirjastamiseks), export
   - digital signature, key encipherment, tls server
9. kasutaja sert (samad linnukesed nagu serveril)
   - kindlasti vajame parooli (kamarajura)

10. ppp - (nupp) OVPN server - (linnuke) enable...
väidetavalt ongi server valmis :)

192.168.77.179:8080

Klient kui vaja:
https://openvpn.net/community-downloads/

Kliendi fail (pane nimeks minutoreveepeeenn.ovpn)
faili sisu (abiks notepad, IPd tuleb õigeks panna):

```
------------
client
dev tun
proto tcp
remote 192.168.77.1  1194     # väline IP aadress
resolv-retry infinite
nobind
persist-key
persist-tun
tls-client
remote-cert-tls server
ca ca.crt          #Change the name certificates you exported for CA
cert kasutaja2.crt         #Change the name certificates you exported For Remote user
key kasutaja2.key         #Change the name key you exported For Remote user

cipher AES-128-CBC
auth SHA1
pull
auth-user-pass
verb 3
route 192.168.77.0 255.255.255.0          # Publish your Network which you want to make reachable
#route 192.168.20.0 255.255.255.0        # Behind the Mikrotik Router


------------
```

Hand on 6

EoIP

Hands on boonus

* DHCP üle EoIP tunneli
* Repiiter
* Väljast hallatav AP

* VPN abilink1 abilink2 pesa

Hands on boonus 2

ipsec

Teooria boonus

Serverite ajalugu, põlvkonnad
- kast -> virtukas -> teenus

"Värskem" tehnoloogia
- letsencrypt, docker, AI, chatgpt?

kõik :)