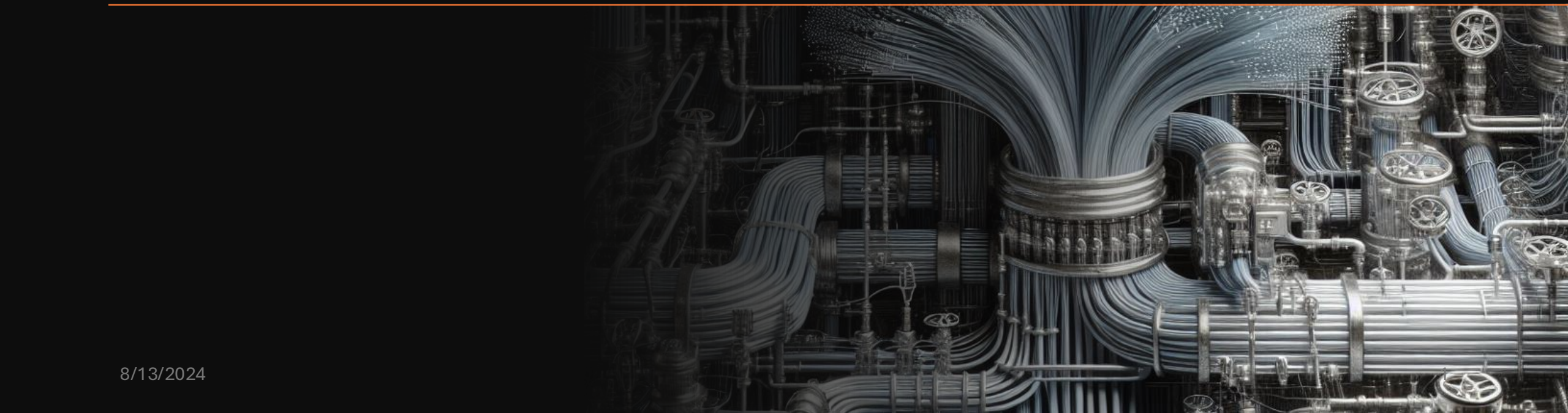
# Külmatehnika andmeside ja IT turvalisus

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks



8/13/2024

# I osa

# Andmeside

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks

# Andmete kogumine

## ANDMETE KOGUMISE OLULISUS

- **Süsteemide efektiivsus:** Täpsed andmed võimaldavad optimeerida külmasüsteemide tööd, säästa energiat ja vähendada kulusid.
- **Hooldus ja tõrkeotsing:** Kogutud andmed aitavad tuvastada ja ennetada võimalikke probleeme, võimaldades kiiret ja täpset tõrkeotsingut.
- **Regulatiivsed nõuded:** Andmete kogumine ja säilitamine on vajalik regulatiivsete nõuete täitmiseks ning kvaliteedi ja ohutuse tagamiseks.

# Andmete kogumise meetodid ja tehnoloogiad

**Andurid ja mõõteseadmed:** Kasutatakse erinevaid andureid, nagu temperatuuri, rõhu, niiskuse ja vooluandurid, et koguda vajalikku teavet külmasüsteemide toimimise kohta.

- **Näide:** Temperatuuriandur mõõdab külmaaine temperatuuri ja edastab andmed juhtsüsteemile, et tagada stabiilne temperatuur külmhoones.

**Andmekogumisseadmed:** Kasutatakse seadmeid, nagu andmelogerid, PLC-d (Programmeeritavad Loogikakontrollerid) ja SCADA (Järelevalve ja Andmete Kogumise Süsteemid), et koguda ja hallata andmeid.

- **Näide:** PLC kogub ja töötleb erinevatest anduritest pärinevaid andmeid ning juhib külmasüsteemi komponente vastavalt eelnevalt määratud loogikale.

# Andmeedastus ja olulisus

**Reaalajas jälgimine ja kontroll:**

- Andmete kiire ja täpne edastamine võimaldab reaalajas jälgida ja juhtida külmasüsteeme.

**Kaugjälgimine:**

- Võimaldab süsteeme jälgida ja hallata eemalt, vähendades vajadust kohapealsete külastuste järele.

# Andmeedastuse meetodid ja protokollid

**Juhtmega ühendused:**

- **Ethernet:** Pakub kiiret ja usaldusväärset andmeedastust.
- **Modbus:** Üks vanimaid ja laialdaselt kasutatavaid tööstuslikke protokolle, mis võimaldab lihtsat ja usaldusväärset andmevahetust.
- **BACnet:** Spetsiaalselt hooneautomaatika süsteemidele mõeldud protokoll, mis võimaldab erinevatel hooneautomaatika seadmetel omavahel suhelda.
- Modbus
- BACnet
- Ethernet

# Andmeedastuse meetodid ja protokollid

**Juhtmevabad ühendused:**

- **Wi-Fi:** Pakub kiiret andmeedastust ja paindlikkust.
- **Zigbee:** Madala energiatarbega traadita protokoll, sobib suurepäraselt sensorvõrkudesse.
- **LoRaWAN:** Pikkade vahemaade jaoks mõeldud traadita protokoll, mis sobib hästi suurte alade katmiseks.
- Wi-Fi
- Zigbee
- LoRaWAN

# Andmeedastuse meetodid ja protokollid

- **Tööstuslikud protokollid:**
- **Protokollide ühilduvus:** Kasutatakse standardseid tööstuslikke protokolle, et tagada ühilduvus erinevate seadmete ja süsteemide vahel.

# Andmeedastuse meetodid ja protokollid

Andmeedastus on kriitilise tähtsusega reaalajas jälgimise ja kontrolli võimaldamiseks, samuti kaugjälgimise võimaldamiseks, mis vähendab vajadust kohapealsete külastuste järele.

Juhtmega ühendused, nagu Ethernet, Modbus ja BACnet, tagavad usaldusväärse ja kiire andmeedastuse.

Samas kui juhtmevabad ühendused, nagu Wi-Fi, Zigbee ja LoRaWAN, pakuvad paindlikke ja lihtsaid paigaldusvõimalusi.

Tööstuslikud protokollid tagavad ühilduvuse erinevate seadmete ja süsteemide vahel, võimaldades sujuvat integreerimist ja töö.


# Iot integreerimine IOT (Asjade internet) olulisus külmatehnikas

- **Andmete kogumine ja analüüs:** IoT võimaldab koguda ja analüüsida andmeid suuremahuliste süsteemide kohta, parandades seeläbi süsteemide efektiivsust ja töökindlust.
- **Ennustav hooldus:** IoT seadmed võimaldavad ennustada ja ennetada probleeme enne nende tekkimist, vähendades seisakuid ja hoolduskulusid.

# Iot integreerimise meetodid ja tehnoloogiad

- **IoT platvormid:** Kasutatakse spetsiaalseid platvorme, nagu AWS IoT, Azure IoT ja ThingWorx, et hallata IoT seadmeid ja andmeid.
- **Sensorid ja seadmed:** Integreeritakse IoT-sensorid ja -seadmed külmasüsteemidesse, et koguda reaalajas andmeid.
- **Andmeanalüütika ja visualiseerimine:** Kasutatakse andmeanalüütika tööriistu ja armatuurlaudu andmete analüüsimiseks ja visualiseerimiseks, et teha informeeritud otsuseid.

# TÄIENDAVAD NÄITED JA DETAILID

**IoT platvormide kasutamine:**

- **Funktsioon:** IoT platvormid võimaldavad seadmete haldamist, andmete kogumist, analüüsi ja hoiatussüsteemide loomist.
- **Kasutus:** AWS IoT võimaldab jälgida ja juhtida külmasüsteeme eemalt, hallata tarkvaravärskendusi ja rakendada turvapoliitikaid.

**Sensorite ja seadmete Integreerimine:**

- **Funktsioon:** IoT-sensorid koguvad reaalajas andmeid temperatuuri, rõhu, niiskuse ja energiatarbimise kohta.
- **Kasutus:** IoT-sensorid paigaldatakse külmasüsteemidesse, et koguda pidevat andmevoogu ja edastada see juhtimissüsteemidesse.

**Ennustav hooldus:**

- **Funktsioon:** Ennustav hooldus kasutab IoT-andureid ja masinõppe algoritme, et ennustada ja ennetada süsteemirikkeid.
- **Kasutus:** IoT-süsteem tuvastab, kui kompressori töötsüklites esineb kõrvalekaldeid ja saadab hooldustiimile hoiatuse, et probleem enne rikke tekkimist lahendada.

**Andmeanalüütika tööriistad:**

- **Funktsioon:** Analüüsivad kogutud andmeid ja loovad visuaalseid aruandeid, et teha informeeritud otsuseid.
- **Kasutus:** Power BI või Tableau abil saavad insenerid luua visuaalseid armatuurlaudu, mis näitavad külmasüsteemi efektiivsust ja töökindlust reaalajas.

**Visualiseerimise armatuurlauad:**

- **Funktsioon:** Pakuvad visuaalset ülevaadet külmasüsteemi toimimisest ja võimaldavad kiiret tuvastamist ja reageerimist probleemidele.
- **Kasutus:** Armatuurlauad kuvavad olulisi süsteemiparameetreid, nagu temperatuur, rõhk ja energiatarbimine, võimaldades operatiivset juhtimist ja jälgimist.

# II osa
# Võrgu konfigureerimine ja andmeturve külmatehnikas

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks

# VÕRGU KONFIGUREERIMINE

# VÕRGU KONFIGUREERIMISE OLULISUS

**Süsteemide ühendamine:** Õigesti konfigureeritud võrk tagab erinevate seadmete ja süsteemide omavahelise ühendamise ja koostöö.

- **Näide:** Külmasüsteemide, andurite ja juhtimissüsteemide ühendamine ühtsesse võrku võimaldab tõrgeteta andmevahetust ja koostööd, tagades süsteemi sujuva toimimise. Näiteks võib külmhoone juhtimissüsteem saada andmeid temperatuurianduritelt ja rõhuanduritelt ning kohandada tööparameetreid vastavalt.

**Töökindlus ja efektiivsus:** Tagab sujuva andmevahetuse ja süsteemide töökindluse.

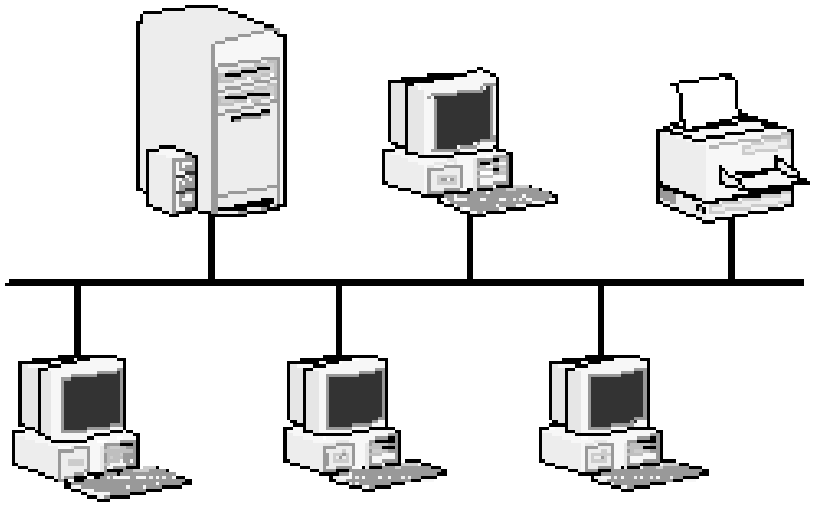
- **Näide:** Hea võrgu konfigureerimine aitab vältida andmete kadu ja võrguühenduse probleeme, tagades pideva ja usaldusväärse süsteemide toimimise. Näiteks, korralikult konfigureeritud kommutaatorid ja ruuterid tagavad, et andmed liiguvad kiiresti ja tõrgeteta külmhoone andurite ja juhtimissüsteemide vahel.

# VÕRGU KONFIGUREERIMISE SAMMUD

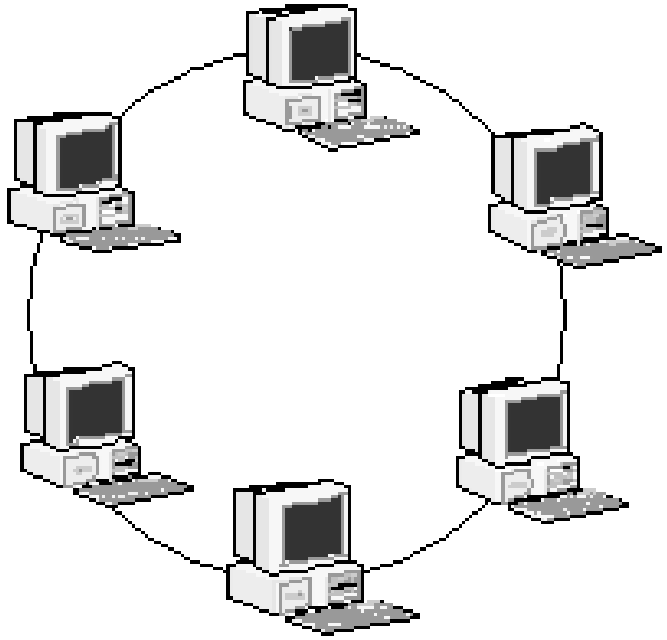
**Võrgu topoloogia planeerimine:** Määratletakse võrgu struktuur (tähtvõrk, hierarhiline, silmus jne) vastavalt vajadustele ja seadmete paigutusele.

**Täht- ja hierarhiline :**

- **Tähtvõrk:** Kõik seadmed on ühendatud keskse kommutaatoriga või ruuteriga. See struktuur on lihtne hallata ja vigu diagnoosida.
  - **Näide:** Külmhoones on kõik andurid ja kontrollerid ühendatud keskse juhtimissüsteemiga, mis võimaldab lihtsat haldust ja kiiret probleemide tuvastamist.
- **Hierarhiline (puu):** Hierarhiline struktuur, kus seadmed on ühendatud allüksustesse, mis on omakorda ühendatud keskse seadmega. See struktuur on sobiv suurematele ja keerukamatele võrkudele.
  - **Näide:** Suures jaotuskeskuses on erinevad külmhooned ühendatud alamvõrkudesse, mis on omakorda ühendatud keskse juhtimissüsteemiga.

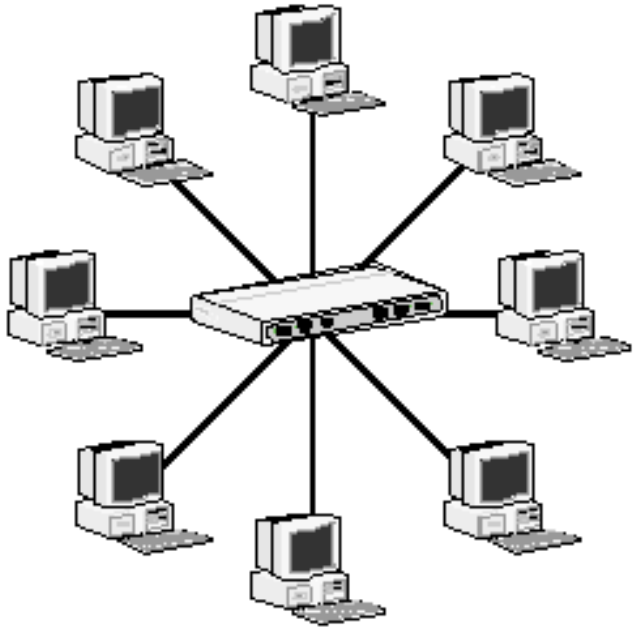


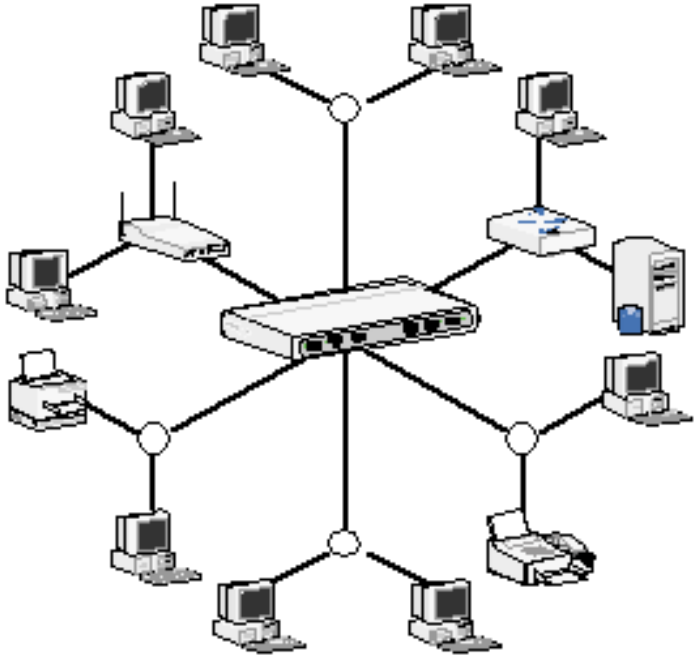
- **Siinitopoloogia**



**Ring-topoloogia**

# Võrgutopoloogiad ja mudelid

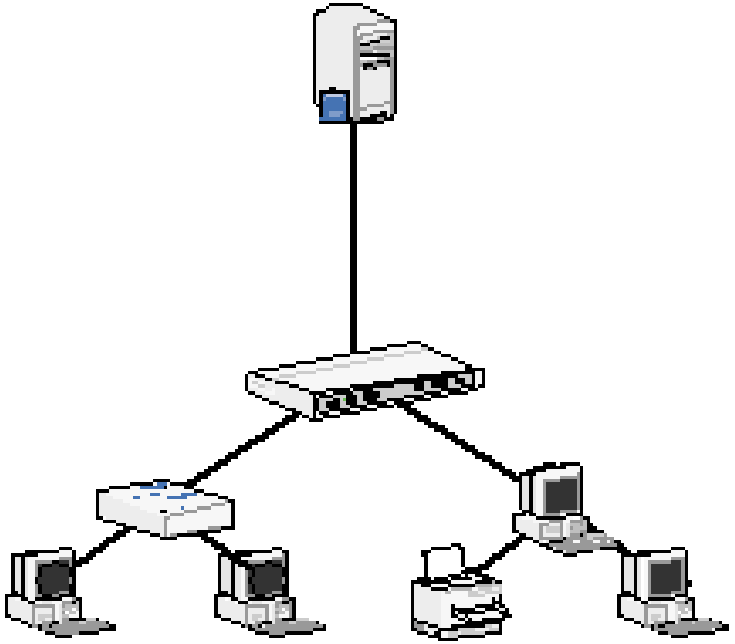


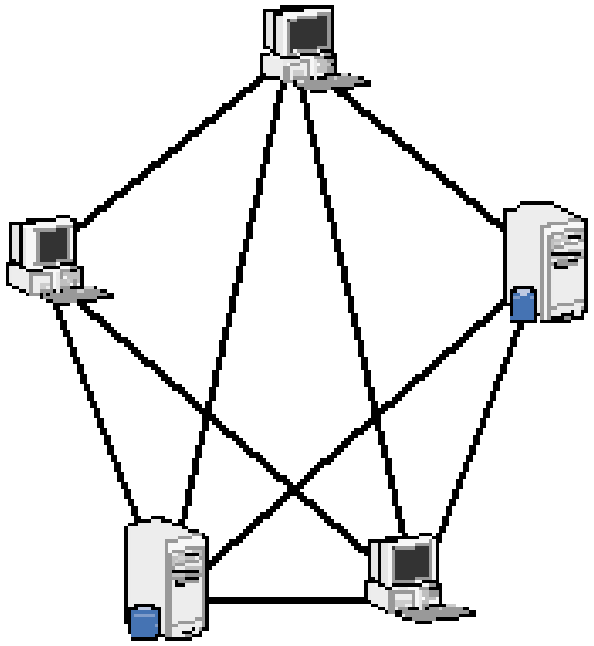


- **Tähttopoloogia**

**Laiendatud täht-topoloogia**

# Võrgutopoloogiad ja mudelid





- **Hierarhiline topoloogia**

**Silmus-topoloogia**

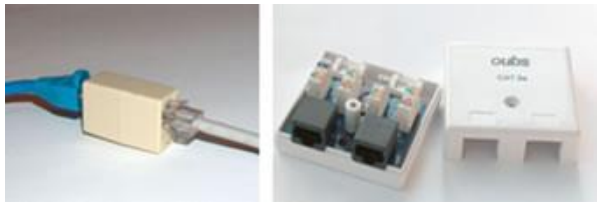
# Võrgutopoloogiad ja mudelid

# Arvutivõrgu seadmed ja nende seadistamine

- **Seadmete aadresside määramine:** Iga seadme IP-aadressi ja MAC-aadressi määramine, et tagada unikaalne identifitseerimine ja side.
- **Staatilised ja dünaamilised aadressid:**
- **Staatilised IP-aadressid:** Olulistele seadmetele, nagu serverid ja juhtimiskeskused, määratakse fikseeritud IP-aadressid, tagades nende pideva kättesaadavuse.
    - **Näide:** Juhtimissüsteemile ja peamistele anduritele määratakse staatilised IP-aadressid, et tagada nende püsiv ühendus ja lihtne haldamine.
- **Dünaamilised IP-aadressid:** Vähem kriitilised seadmed, nagu ajutised andurid või kasutajaseadmed, võivad kasutada DHCP serveri poolt määratud dünaamilisi IP-aadresse.
    - **Näide:** Hooldustehnikute sülearvutid saavad dünaamilised IP-aadressid, kui nad ühenduvad võrku, lihtsustades võrgu haldamist.
- **Võrgu Seadistamine:** Ruuterite, kommutaatorite ja võrguadapterite seadistamine vastavalt määratud topoloogiale ja aadressidele.

# Üksused füüsilise ja loogilise võrgu struktureerimiseks

- **Passiivsed üksused**
- Passiivsed üksused on sidevõrgu ühenduspunktid, mis ei muuda sisendisse saabuva signaali parameetreid. See üksuste grupp sisaldab:
- *Ühenduspistikud* (*Jack couplers)* on passiivsed üksused, mida kasutatakse võrgukaabli pikendamiseks.



# Üksused füüsilise ja loogilise võrgu struktureerimiseks

- *Juhtmepaneel (Patch panel)* on ühendus- ja jaotuspunkt kaablite korraldamiseks.
- *Passiivne kontsentraator/jaotur (passive concentrator/hub)* on keskne ühenduskolmik, mille abil luuakse ühendus hulga tööjaamade vahel. See ei sisalda elektroonilisi komponente ega vaja seega elektritoidet. Suvalisse porti saabuv sisendsignaal edastatakse kõigisse teistesse portidesse.

# Aktiivsed seadmed



- *repiiter*. See seade funktsioneerib füüsilisel tasandil, suurendab sidevõrgu kogupikkust. See taastab signaalitugevust ja parandab impulsi tugevust suurematel vahemaadel.

# Aktiivsed seadmed

*Hub (jaotur)*. See on mitme sisendiga repiiter, millega luuakse täht-ühendus. Seda iseloomustavad tehnilised spetsifikatsioonid ja omadused on järgmised

- Ühendab individuaalsed, võrgukaardiga varustatu tööjaamad ühtseks võrguks;
- Hubid võimaldavad lisada olemasolevasse võrku uusi füüsilisi tööjaamu;
- Kõik pordid on võrdse prioriteediga;
- Protsessi, mille käigus hub mõned pordid välja lülitab, kui tuvastatakse talitlushäire, nimetatakse segmentatsiooniks;
- See leiab rakendust võrkudes, mis kasutavad UTP kaableid;
- Vastu võetud andmepakette ei puhverdata, mistõttu on andmevahetuskiirus väike;
- See ei sünkroniseeri teistel kiirustel töötavaid porte.

# Aktiivsed seadmed

*Sild (bridge). See jagab võrgu loogilisteks segmentideks ja sõnumid edastatakse ühest segmendist teise üle silla pordi, kui vastuvõtja unikaalne võrguaadress (MAC [1]) kuulub vastavasse segmenti. See seade sisaldab mõlema segmendi üksuste aadressitabelit ja side käib järgnevate sammude jadana:*

- *Andmepaketi vastuvõtmisel algatatakse lähteaadressi ja sihtaadressi kontroll. Tabelis on esitatud igas segmendis oleva üksuse individuaalne aadress.*
- *Kui sihtaadressi ei ole kirjutatud tabelisse, tuleb pakett edastada kõikidesse segmentidesse. Sihtaadressi puudumisel tabelist lisatakse see võimalusel sinna automaatselt.*
- *Sild edastab paketi vastavale segmendile, kui sihtaadress on kirjutatud tabelisse.*
- *Kui lähteaadress ja sihtaadress on samas segmendis, ei edasta sild andmepaketti teise segmenti.*

# Aktiivsed seadmed

*Switch (kommutaator). See on uuema generatsiooni sild, mis kindlustab informatsiooni paralleelse töötlemise. Switchi kasutatakse kõige laialdasemalt tööjaamade ühendamiseks täht-topoloogia võrkudes:*

*See suurendab võrgu andmevahetuskiirust. Välimuselt sarnaneb see hubiga kuid siiski on kommutaator sellest oluliselt intelligentsem seade.*

*Hub edastab vastuvõetud signaali kõigisse portidesse, switch seevastu filtreerib informatsiooni ning edastab selle ainult sihtseadmetele.*

# Switchi spetsiifilised tunnused on järgmised:

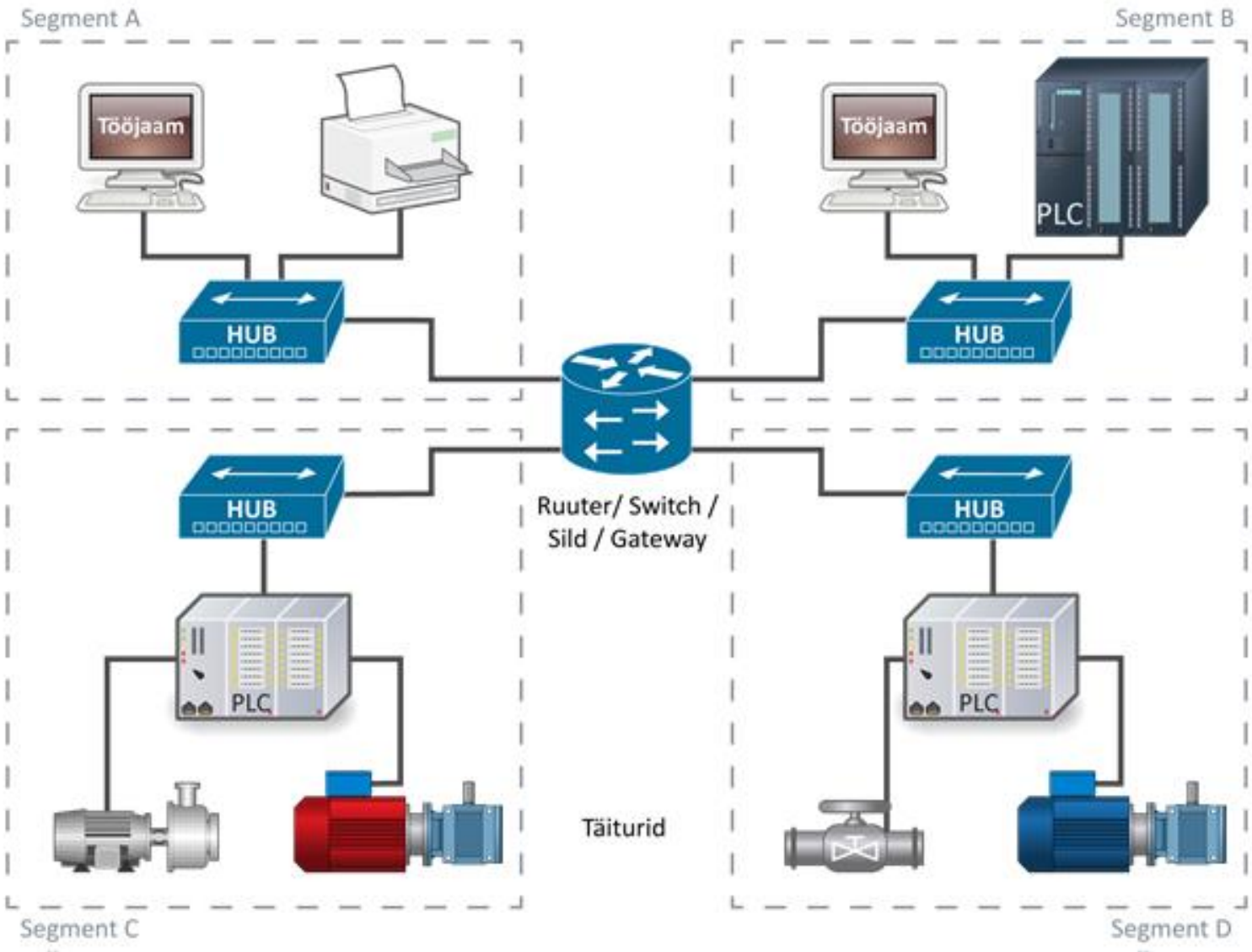
- Omab iga pordi jaoks spetsiaalset protsessorit, mis töötleb sissetulevaid andmepakette (kaadreid) ülejäänud portide protsessoritest eraldi;
- Võimaldab igal tööjaamal edastada andmeid üle ülekandemeediumi ilma teiste tööjaamadega konkureerimata;
- Kontrollib sellesse ühendatud seadmete MAC aadresse;
- Tõlgib andmepakette ühest standardist teise (näiteks Ethernetist FDDI-sse);
- Lingib mitmed eraldiseisvad seadmed ja võrgusegmendid, millest igaühel võib olla veel sellesse ühendatud terminale;
- Puhverdab andmed (salvesta-ja-edasta) enne vastuvõtja ühendusparameetrite tuvastamist;
- Kommutaatorid suhtlevad omavahel täisdupleks-režiimis, mis võimaldab andmeid edastada ja vastu võtta samaaegselt.

# Aktiivsed seadmed

*Ruuter on eraldiseisev seade, mida kasutatakse infopakettide jaotamiseks erinevate võrkude või võrgusegmentide vahel. Ruuterina saab kasutada ka tavalist arvutit. Erinevalt hubidest, sildadest ja madalama taseme switchidest töötab ruuter OSI võrgukihis IP aadressidega, mitte MAC aadressidega*



# Aktiivsed seadmed



# Võrguteenuste seadistamine

**Võrguteenuste seadistamine:** DHCP, DNS ja muude võrguteenuste konfigureerimine, et tagada sujuv ja efektiivne võrgu toimimine.

**DHCP ja DNS:**

- **DHCP:** Dünaamiliste IP-aadresside jaotamine seadmetele, et lihtsustada võrgu haldamist ja tagada, et kõik seadmed saavad automaatselt vajaliku võrguühenduse.
  - **Näide:** DHCP server jaotab IP-aadresse hooldustehnikute seadmetele, kui nad ühenduvad võrku, lihtsustades seadmete haldamist ja võrgu laiendamist.
- **DNS:** Nimelahenduse teenus, mis võimaldab seadmetel ja kasutajatel pääseda juurde ressurssidele lihtsamate nimede kaudu, mitte keerukate IP-aadresside kaudu.
  - **Näide:** DNS server võimaldab kasutajatel ja süsteemidel pääseda juurde juhtimiskeskuse ressurssidele lihtsate nimede, nagu “control-center.local”, kaudu.

# MIS ON IP-AADRESS?

- **IP-aadress (Internet Protocol Address)** on unikaalne numbriline identifikaator, mida kasutatakse seadmete tuvastamiseks ja nendega suhtlemiseks arvutivõrgus, mis kasutab Interneti Protokolli (IP). IP-aadressid tagavad, et andmed liiguvad ühelt arvutilt või seadmelt teisele õige sihtkohaga

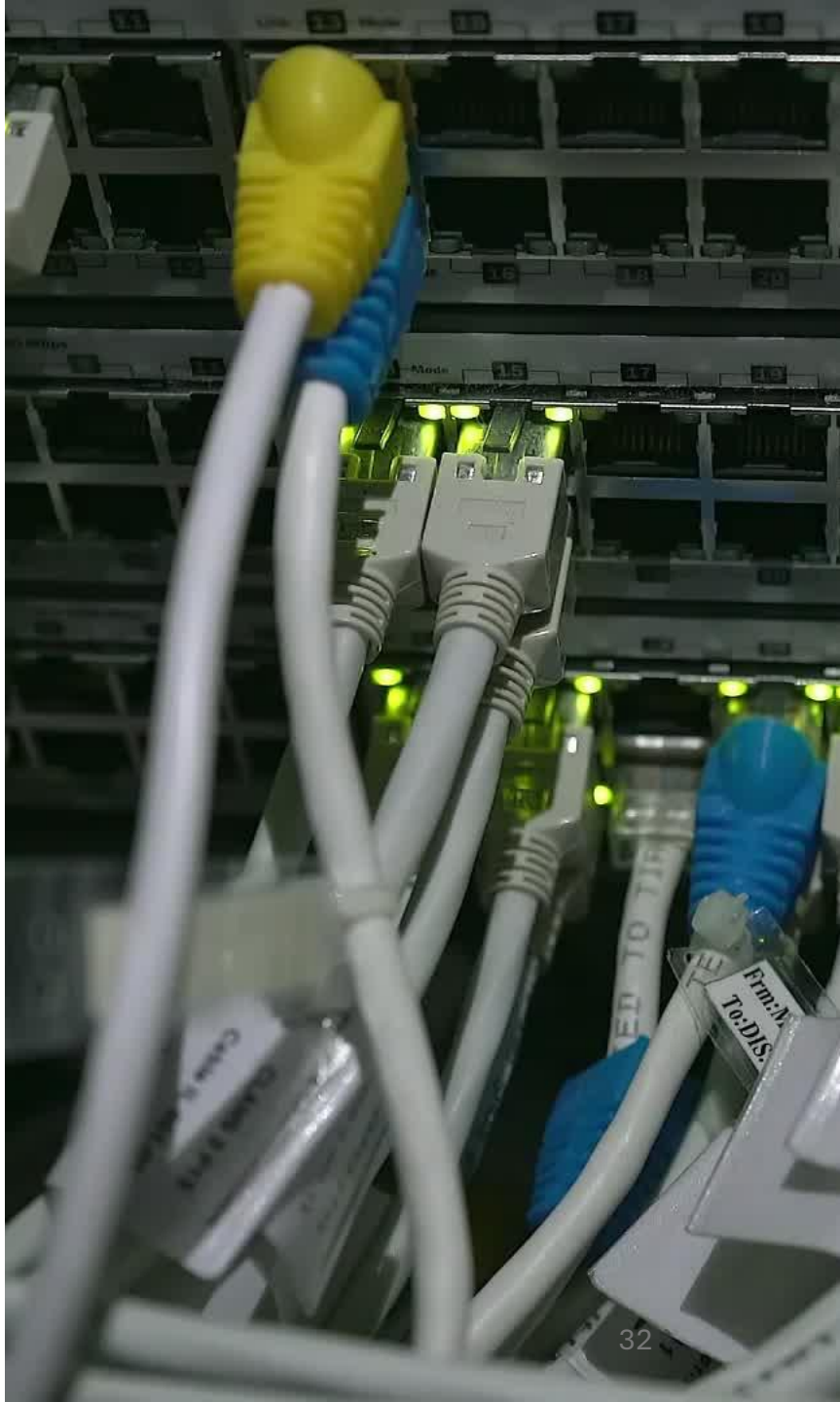
# IP-AADRESSIDE TÜÜBID

**IPV4**

- **IPv4 (Internet Protocol version 4)**: Kasutab 32-bitist aadressiruumi, mis võimaldab kokku umbes 4,3 miljardit unikaalset aadressi. IPv4 aadress koosneb neljast oktetist (8-bitised plokid), mis on eraldatud punktidega, näiteks 192.168.1.1.
- **Formaat**: 192.168.0.1

**IPV6**

- **IPv6 (Internet Protocol version 6)**: Kasutab 128-bitist aadressiruumi, pakkudes oluliselt suuremat aadressiruumi kui IPv4. IPv6 aadress koosneb kaheksast 16-bitiste segmentide rühmast, mis on eraldatud koolonitega, näiteks 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- **Formaat**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334



# IP-AADRESSI AJALUGU

- **1970ndad**: IP-aadresside kontseptsioon sai alguse ARPANETi arendamise käigus, mis oli USA Kaitseministeeriumi projekt. ARPANET oli esimene tõeline võrk, mis kasutas pakettkommutatsiooni ja võimaldas erinevatel arvutitel omavahel andmeid vahetada.
- **1980ndad**: 1981. aastal määratleti IPv4 standard RFC 791 kaudu. IPv4 oli esimene laialdaselt kasutatud IP-aadressi versioon, mis võimaldas seadmetel internetis suhelda.
- 1987 aastal loodi esimesed Interneti-teenuse pakkujad (ISP). Sel ajahetkel oli vaja saata interneti teenuse pakkujalekiri ja küsida oma võrgu jaoks IP-aadresside plokki. Tavaliselt määrati teile nii palju aadresse, kui olite palunud – või tõenäolisemalt veidi rohkem, sest aadressi arhitektuur nägi välja selline:

# IP-AADRESSIDE KLASSID

## IP address classes (pre 1993 mindset)

| | | |
|---|---|---|
| **Class A** | 1.0.0.1 to 126.255.255.254 | 16M hosts<br>127 networks |
| **Class B** | 128.1.0.1 to<br>191.255.255.254 | 64K hosts<br>16K networks |
| **Class C** | 192.0.1.1 to<br>223.255.254.254 | 254 hosts<br>2M networks |
| **Class D** | 224.0.0.0 to<br>239.255.255.255 | Multicast |
| **Class E** | 240.0.0.0 to<br>254.255.255.254 | R&D == wasted |

- Aadressid määrati 8-bitistel piiridel. Niisiis, saime mõned väga suured IP vahemikud (klass A), mõned keskmise suurusega IP vahemikud (klass B) ja paljud väikeseid IP vahemike (klass C).
- Lisaks sellele oli hulk aadresse (klass E), mis olid üsna kasutuskõlbmatud, kuna need olid reserveeritud uurimis- ja arendustegevuseks ning paljud operaatorid filtreerivad tänapäeval nendelt aadressidelt saadetud pakette.

# IP-AADRESSIDE KLASSID

**IPv4 aadressid** jagunevad viide klassi, mille eesmärk on pakkuda erineva suurusega võrkudele sobivaid aadressiruume:

- **Klass A**: Suured võrgud, millel on palju hoste. Aadressivahemik: 1.0.0.0 kuni 126.0.0.0
- **Klass B**: Keskmise suurusega võrgud. Aadressivahemik: 128.0.0.0 kuni 191.255.0.0
- **Klass C**: Väikesed võrgud. Aadressivahemik: 192.0.0.0 kuni 223.255.255.0
- **Klass D**: Kasutatakse mitmiksaateks (multicast). Aadressivahemik: 224.0.0.0 kuni 239.255.255.255
- **Klass E**: Eksperimentaalseks kasutamiseks. Aadressivahemik: 240.0.0.0 kuni 255.255.255.255

# IP aadress

- **1990 ndad**: Interneti plahvatuslik kasv tõi esile vajaduse suurema aadressiruumi järele, kuna IPv4 aadressid hakkasid otsa saama. See viis IPv6 arendamiseni, mis tutvustati 1998. aastal RFC 2460 kaudu.
- **21. sajand**: IPv6 kasutuselevõtt on olnud järk-järguline, kuna paljud süsteemid ja teenused töötavad endiselt IPv4 aadressidega. Siiski on IPv6 üha enam levinud tänu vajadusele suurema aadressiruumi ja paremate võrgufunktsioonide järele

# IP-AADRESSIDE TÖÖPÕHIMÕTE

- IP-aadressid määravad seadme asukoha võrgus ja võimaldavad seadmetel omavahel suhelda. Kui seade saadab andmeid teisele seadmele, lisatakse andmepakettidele sihtkoha ja saatja IP-aadressid. Ruuterid ja teised võrguseadmed kasutavad neid aadresse, et suunata pakette õigesse sihtkohta.

# PRIVAATSED JA AVALIKUD IP-AADRESSID

- **Privaatsed IP-aadressid**: Kasutatakse lokaalses võrgus ja ei ole internetis otse nähtavad. Privaatsed vahemikud on määratletud RFC 1918:
- 10.0.0.0 kuni 10.255.255.255
- 172.16.0.0 kuni 172.31.255.255
- 192.168.0.0 kuni 192.168.255.255
- **Avalikud IP-aadressid**: Kasutatakse internetis ja on unikaalsed globaalselt.

# IP-AADRESSIDE OLULISUS

- **IP-AADRESSIDE OLULISUS**
- IP-aadressid on kriitilise tähtsusega interneti toimimisel, võimaldades seadmetel omavahel suhelda ja tagades, et andmed jõuavad õigesse sihtkohta. Ilma IP-aadressideta ei oleks võimalik luua toimivaid võrke ega internetiühendusi.

# kommutaatorite (Switch) ja ruuterite konfigureerimine:

**Kommutaatorid:** VLAN-ide kasutamine, et segmenteerida võrku ja suurendada turvalisust.

- **Näide:** Erinevad VLAN-id eraldavad külmhoonete andurid, juhtimissüsteemid ja kasutajaseadmed, vähendades võrguliikluse ülekoormust ja turvariske.

**Ruuterid:** Marsruutimisreeglite seadistamine, et tagada andmete sujuv liikumine erinevate võrguosade vahel.

- **Näide:** Ruuterite konfigureerimine tagab, et andmed liiguvad tõhusalt juhtimiskeskuse, külmhoonete ja väliste serverite vahel.

# 2. JÄRELEVALVE JA SEIRE

JÄRELEVALVE JA SEIRE OLULISUS

**Süsteemide Töökindlus:** Tagab, et kõik süsteemid töötavad ootuspäraselt ja tuvastatakse kiiresti võimalikud probleemid.

- **Näide:** Järelevalvesüsteem tuvastab koheselt, kui külmasüsteemi temperatuuriandur hakkab näitama ebanormaalseid väärtusi, võimaldades operatiivset sekkumist ja probleemide ennetamist.

**Ennetav Hooldus:** Võimaldab tuvastada probleemid varakult ja võtta ennetavaid meetmeid.

- **Näide:** Järelevalvesüsteemide kaudu saadud andmete analüüs näitab, et teatud kompressor töötab liiga sageli, viidates võimalikule probleemile, mis vajab hooldust enne, kui see põhjustab tõsisemaid rikkeid.

# JÄRELEVALVE JA SEIRE MEETODID

**Järelevalvetarkvara:** Kasutatakse spetsiaalseid tarkvaralahendusi, nagu Nagios, Zabbix või PRTG, süsteemide ja seadmete jälgimiseks.

**Näide:** Zabbix jälgib reaalajas külmasüsteemi temperatuuri, niiskust ja rõhku ning saadab teateid, kui parameetrid ületavad määratud piirväärtused.

**Andmeanalüütika ja Raporteerimine:** Reaalajas andmete analüüsimine ja raporteerimine, et tuvastada mustrid ja anomaaliad.

**Näide:** Andmeanalüütika tööriistad koguvad ja analüüsivad külmasüsteemi andmeid, genereerides aruandeid, mis aitavad tuvastada ebatavalisi mustreid või trende, mis viitavad võimalikele probleemidele.

**Alarmsüsteemid:** Häirete ja hoiatuste seadistamine, et teavitada vastutavaid isikuid probleemidest viivitamatult.

**Näide:** PRTG seadistatakse nii, et kui külmasüsteemi temperatuur tõuseb üle määratud piirväärtuse, saadab see koheselt SMS-teate hooldustehnikule, et probleemiga saaks tegeleda viivitamatult.

# JÄRELEVALVE JA SEIRE NÄITED KÜLMASÜSTEEMIDES

1. **Temperatuuri seire:**

- **Näide:** Järelevalvetarkvara jälgib pidevalt külmasüsteemi temperatuuriandureid. Kui temperatuur ületab kriitilise taseme, saadetakse koheselt teade hooldustehnikule.

2. **Rõhu seire:**

- **Näide:** Rõhuandurid külmasüsteemis on ühendatud järelevalvetarkvaraga, mis jälgib ja analüüsib rõhutasemeid reaalajas. Kui rõhk langeb alla määratud piiri, teavitatakse viivitamatult vastutavaid isikuid.

3. **Niiskuse seire:**

- **Näide:** Niiskusandurid jälgivad külmhoone niiskustaset. Kui niiskus ületab ohutu piiri, saadab järelevalvesüsteem hoiatuse, et vältida toote kahjustusi.

4. **Energiatarbimise seire:**

- **Näide:** Energiatarbimise monitooring võimaldab tuvastada, kui külmasüsteem hakkab tarbima ebatavaliselt palju energiat, viidates võimalikele riketele või ebaefektiivsusele.

5. **Andmeanalüütika kasutamine:**

- **Näide:** Andmeanalüütika tööriistad analüüsivad pikaajalisi andmeid, et tuvastada mustreid ja trende, mis võivad viidata eelseisvatele probleemidele või hooldusvajadusele.

# VÕRGU TURVALISUS

## VÕRGU TURVALISUSE OLULISUS

**Andmete Kaitse:** Kaitseb tundlikku teavet volitamata juurdepääsu eest.

- **Näide:** Külmasüsteemi andurid ja juhtimissüsteemid koguvad ja edastavad tundlikku teavet, nagu temperatuuri, rõhu ja energiatarbimise andmed. Need andmed tuleb kaitsta volitamata juurdepääsu eest, et vältida andmete manipuleerimist või vargust.

**Süsteemide Töökindlus:** Ennetab küberrünnakuid ja tagab süsteemide katkematu töö.

- **Näide:** Külmasüsteemide võrgud võivad olla rünnaku all, kui turvameetmed on ebapiisavad. Küberrünnakute ennetamine ja süsteemide töökindluse tagamine on kriitilise tähtsusega, et vältida süsteemi seisakuid ja tagada pidev toimimine.

# VÕRGU TURVALISUSE MEETODID

**Krüptimine:** Andmete krüptimine, et tagada andmete konfidentsiaalsus ja terviklikkus.

- **Näide:** Külmasüsteemide andurid ja kontrollerid saadavad andmeid krüpteeritult, et vältida andmete pealtkuulamist ja manipuleerimist. Kõik andmed, mis liiguvad võrgus, peaksid olema krüpteeritud kasutades tugevaid krüpteerimisalgoritme nagu AES (Advanced Encryption Standard).

**Tulemüürid ja VPN:** Kasutamine tulemüüride ja VPN-ide (Virtuaalsed Privaatvõrgud) abil, et piirata juurdepääsu ja kaitsta võrku.

- **Näide:** Tulemüürid aitavad blokeerida volitamata juurdepääsu külmasüsteemide võrgule, samal ajal kui VPN-id võimaldavad turvalist kaugjuurdepääsu hooldustehnikutele, kes peavad süsteemi eemalt jälgima ja hooldama.

**Autentimine ja Autoriseerimine:** Tugevate autentimis- ja autoriseerimismeetodite rakendamine, sealhulgas paroolid, kahefaktoriline autentimine ja biomeetrilised andmed.

- **Näide:** Külmasüsteemide juhtimissüsteemid nõuavad kasutajatelt tugevaid paroole ja kahefaktorilist autentimist, et tagada, et ainult volitatud isikutel on juurdepääs tundlikele süsteemiandmetele ja juhtimisfunktsioonidele.

# HÄDAOLUKORRAPLAANID

HÄDAOLUKORRAPLAANIDE OLULISUS

**Valmidus ja reageerimine:** Tagab, et organisatsioon on valmis reageerima ootamatutele probleemidele ja kriisidele.

- **Näide:** Külmasüsteemi ootamatu rike võib põhjustada toote riknemise ja olulisi rahalisi kahjusid. Hädaolukorraplaan tagab, et meeskond teab täpselt, kuidas reageerida, et probleemi kiiresti lahendada ja kahjusid minimeerida.

**Minimeerib katkestusi:** Vähendab süsteemide tööseisakuid ja kahjusid hädaolukorra korral.

- **Näide:** Hädaolukorraplaan sisaldab meetmeid, mis aitavad kiiresti taastada külmasüsteemide töö pärast riket, minimeerides tööseisakuid ja tagades süsteemi kiire taastumise.

# HÄDAOLUKORRAPLAANIDE KOOSTAMINE

**Riskianalüüs:** Määratletakse potentsiaalsed ohud ja nende mõju.

- **Näide:** Külmasüsteemide puhul võib riskianalüüs hõlmata võimalikke ohte, nagu kompressori rike, elektrikatkestus, võrguühenduse kaotus ja küberrünnakud. Analüüsitakse nende ohtude mõju süsteemi toimimisele ja võimalikke kahjusid.

**Hädaolukorra protokollid:** Koostatakse detailne plaan probleemide lahendamiseks ja süsteemide taastamiseks.

- **Näide:** Hädaolukorra protokollid võivad sisaldada samme kompressori rikke korral, sealhulgas varuosade kättesaadavuse kontrollimist, hooldusmeeskonna teavitamist ja süsteemi alternatiivse töörežiimi käivitamist, et tagada külmaaine tsirkulatsioon.

**Koolitus ja testimine:** Korraldatakse regulaarseid koolitusi ja simulatsioone, et tagada personali valmisolek ja plaanide toimivus.

- **Näide:** Personalile korraldatakse koolitusi ja regulaarseid simulatsioone, kus harjutatakse hädaolukorra protokollide järgimist. Simulatsioonide käigus testitakse plaanide toimivust ja tehakse vajadusel parandusi.

# VÕRGU OPTIMEERIMINE

- VÕRGU OPTIMEERIMISE OLULISUS
- **Parandab efektiivsust:** Tagab võrgu sujuva ja kiire toimimise, vähendades viivitusi ja optimeerides ressursikasutust.
- **Näide:** Optimeeritud võrgu konfiguratsioon võimaldab külmasüsteemide andmetel liikuda kiiresti ja tõhusalt andurite, kontrollerite ja juhtimissüsteemide vahel, tagades, et süsteem töötab sujuvalt ja tõrgeteta.
- **Vähendab kulutusi:** Optimeerimine aitab vähendada energiatarbimist ja hoolduskulusid.
- **Näide:** Võrgu optimeerimine vähendab liigset andmeliiklust ja energiatarbimist, mis omakorda vähendab hoolduskulusid ja pikendab seadmete eluiga.

# VÕRGU OPTIMEERIMISE MEETODID

| | |
|---|---|
| **Võrgu läbilaskevõime analüüs:** Jälgitakse ja analüüsitakse võrgu läbilaskevõimet, et tuvastada kitsaskohad ja parandada jõudlust. | • **Näide:** Läbilaskevõime analüüs tuvastab, et teatud kommutaatori on ülekoormatud, mis põhjustab andmete viivitusi. Selleks võetakse kasutusele täiendavad kommutaatorid või suurendatakse olemasoleva kommutaatori läbilaskevõimet, et parandada andmevoogude sujuvust. |
| **Võrguliikluse Prioriseerimine (QoS):** Määratakse prioriteedid erinevatele andmetüüpidele, et tagada kriitiliste andmete kiire ja usaldusväärne edastamine. | • **Näide:** Võrguliikluse prioriseerimise abil tagatakse, et külmasüsteemi kriitilised juhtimisandmed saavad kõrgema prioriteedi ja edastatakse kiiremini kui vähemolulised andmed, nagu tarkvaravärskendused või kasutajate tegevuslogid. |
| **Liiklusvoogude optimeerimine:** Kasutatakse meetodeid, nagu load balancing ja VLAN-id, et optimeerida andmevoogusid ja vähendada ülekoormust. | • **Näide:** Load balancing jaotab andmeliikluse mitme serveri või seadme vahel, et vältida ülekoormust ja tagada võrgu sujuv toimimine. VLAN-ide kasutamine segmenteerib võrguliiklust, vähendades liigse liikluse mõju kriitilistele süsteemidele. |
| **Regulaarne seadmete uuendamine ja hooldus:** Tagatakse, et kõik võrgu seadmed on ajakohased ja töötavad optimaalselt. | • **Näide:** Võrgu seadmete regulaarne uuendamine ja hooldus aitab vältida rikkeid ja tagab, et seadmed töötavad optimaalselt. Näiteks kommutaatorite ja ruuterite püsivara uuendamine võib parandada nende jõudlust ja turvalisust. |
| **Võrguliikluse monitooring ja analüüs:** Kasutatakse tööriistu, nagu Wireshark ja NetFlow, et jälgida võrgu liiklust ja tuvastada optimeerimisvõimalusi. | • **Näide:** Wireshark aitab tuvastada liigse võrguliikluse allikaid ja NetFlow võimaldab analüüsida liikluse mustreid, et teha kindlaks, kus optimeerimist on vaja. |

# III osa

# Külmatehnika
# IT turvalisus

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks

# MÕISTE JA OLULISUS

- **Küberturvalisus** hõlmab tehnoloogiate, protsesside ja kontrollide kogumit, mis on mõeldud süsteemide, võrgu ja andmete kaitsmiseks küberrünnakute, kahjustuste ja volitamata juurdepääsu eest. Küberturvalisus on oluline kõigis organisatsioonides, et kaitsta tundlikku teavet ja tagada süsteemide usaldusväärne toimimine.
- **Tehnoloogiad:** Hõlmavad turvatarkvara ja -seadmeid, nagu tulemüürid, sissetungide tuvastamise süsteemid (IDS/IPS), krüptograafia ja viirusetõrjeprogrammid.
- **Protsessid:** Sisaldavad turvaprotokolle, riskihindamist ja intsidentide haldust.
- **Kontrollid:** Hõlmavad juurdepääsukontrolli, autentimist ja auditeerimist.

# PÕHIELEMENDID

KONFIDENTSIAALSUS

- **Konfidentsiaalsus** tähendab, et ainult volitatud isikud saavad juurdepääsu tundlikule teabele. See on üks küberturvalisuse põhielementidest, mis tagab andmete privaatsuse ja kaitse volitamata juurdepääsu eest.

TERVIKLIKKUS

- **Terviklikkus** tähendab, et andmed ja süsteemid on täpsed ja muutumatud volitamata isikute poolt. See element tagab, et andmed ei ole rikutud või muudetud ilma loata.

KÄTTESAADAVUS

- **Kättesaadavus** tagab, et volitatud isikutel on juurdepääs süsteemidele ja andmetele alati, kui see on vajalik. See element on kriitilise tähtsusega, et süsteemid oleksid töövalmis ja andmed kättesaadavad.

# ANDMESIDE TURVALISUS

**Andmete Kaitse:** Tagab, et andmeid edastatakse turvaliselt ja kaitstult, ennetades volitamata juurdepääsu ja andmepüügirünnakuid.

- **Näide:** Külmasüs teemide juhtimisandmed, nagu temperatuuri ja rõhu näidud, edastatakse turvaliselt, et vältida andmete manipuleerimist ja volitamata juurdepääsu.

# ANDMESIDE TURVALISUS

## ANDMESIDE TURVALISUSE MEETODID

**Krüpteerimine:** TLS/SSL ja VPN-tehnoloogiate kasutamine andmeside turvamiseks.

- **TLS/SSL Krüpteerimine:**
- **Funktsioon:** Tagab andmeside konfidentsiaalsuse ja terviklikkuse, krüpteerides andmed enne nende edastamist..

**VPN (Virtuaalsed Privaatvõrgud):**

- **Funktsioon:** Loob turvalise ja krüpteeritud ühenduse üle avaliku võrgu, kaitstes andmete konfidentsiaalsust ja terviklikkust.

**Tunneldamine:** Andmeliikluse tunneldamine läbi turvaliste kanalite, et vältida volitamata ligipääsu.

- **Funktsioon:** Edastab andmed turvalises tunnelis, kaitstes neid pealtkuulamise ja rünnakute eest.

# VÕRGUTURVALISUS

## VÕRGUTURVALISUSE OLULISUS

- **Kaitse Küberrünnakute Eest:** Kaitseb võrku küberrünnakute, pahavara ja volitamata juurdepääsu eest.

VÕRGUTURVALISUSE MEETODID

- **Tulemüürid ja IDS/IPS:** Tulemüüride ja sissetungide tuvastamise/sissetungide ennetamise süsteemide kasutamine.
- **Tulemüürid:**
- **Funktsioon:** Kontrollivad ja piiravad võrgu liiklust, lubades ainult volitatud ühendusi ja blokeerides kahtlase liikluse..
- **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):**
- **Funktsioon:** Tuvastavad ja ennetavad kahtlase tegevuse võrku sissetungimise, analüüsides liiklust ja rakendades turvapoliitikaid.
- **Segmenteerimine ja VLAN-id:** Võrgu segmentimine ja VLAN-ide (virtuaalsed kohtvõrgud) kasutamine turvalisuse parandamiseks.
- **Võrgu segmenteerimine:**
- **Funktsioon:** Jagab võrgu väiksemateks segmentideks, piirates liikluse levikut ja suurendades turvalisust.
- **VLAN-id:**
- **Funktsioon:** Loovad virtuaalsed kohtvõrgud, mis võimaldavad liikluse eraldamist ja paremat turvalisust.

# IOT TURVALISUS

## IOT TURVALISUSE OLULISUS

- **IoT seadmete kaitse:** Tagab, et kõik IoT-seadmed on turvalised ja ei kujuta endast turvariski.
- IOT TURVALISUSE MEETODID
- **Turvalised ühendused:** IoT-seadmete ühendamine turvaliste protokollide abil (nt MQTT üle TLS).
- **MQTT üle TLS:**
- **Funktsioon:** Kasutab krüpteeritud ühendust andmete edastamiseks, tagades andmete konfidentsiaalsuse ja terviklikkuse.
- **Regulaarne tarkvarauuendus:** IoT-seadmete regulaarne tarkvarauuendamine ja turvapaikade rakendamine.
- **Funktsioon:** Tagab, et kõik seadmed on ajakohased ja kaitstud tuntud turvahaavatavuste eest.

# FÜÜSILINE TURVALISUS

## FÜÜSILISE TURVALISUSE OLULISUS

- **Kaitse füüsiliste rünnakute eest:** Tagab, et seadmed ja andmekeskused on kaitstud füüsiliste rünnakute ja varguste eest.

FÜÜSILISE TURVALISUSE MEETODID

- **Lukustatud Kapslid ja Kapid:** Kasutamine lukustatud seadmekappe ja kapsleid seadmete kaitsmiseks.
- **Lukustatud kapslid ja kapid:**
- **Funktsioon:** Tagab, et ainult volitatud isikud saavad füüsiliselt juurde pääseda seadmetele, vähendades varguste ja kahjustuste riski.
- **Juurdepääsu Kontroll:** Füüsilise juurdepääsu kontroll läbi turvakaartide, biomeetriliste andurite ja valvekaamerate.
- **Turvakaardid ja biomeetrilised andurid:**
- **Funktsioon:** Tagab, et ainult volitatud isikud saavad juurde pääseda tundlikele aladele ja seadmetele.
- **Valvekaamerad:**
- **Funktsioon:** Tagab pideva jälgimise ja salvestamise, et tuvastada ja ennetada volitamata juurdepääsu ja füüsilisi rünnakuid.

# ANDMEKAITSE

## ANDMEKAITSE OLULISUS

- **Kaitse isikuandmete eest:** Tagab, et isikuandmed ja muud tundlikud andmed on kaitstud volitamata juurdepääsu ja lekkimise eest.

ANDMEKAITSE MEETODID

- **GDPR Järgimine:** Isikuandmete kaitse üldmääruse (GDPR) järgimine.
- **Funktsioon:** Tagab, et kõik andmete kogumise, töötlemise ja säilitamise protsessid vastavad GDPR-i nõuetele, kaitstes isikuandmeid volitamata juurdepääsu ja töötlemise eest.
- **Andmete Anonüümimine ja Pseudonüümimine:** Andmete anonüümimine ja pseudonüümimine, et vähendada andmete kuritarvitamise riski.
- **Anonüümimine:**
- **Funktsioon:** Eemaldab isikuandmed või muudab need selliselt, et andmete alusel ei ole võimalik tuvastada konkreetset isikut.
- **Pseudonüümimine:**
- **Funktsioon:** Asendab isikuandmed pseudonüümidega, mis muudab isiku tuvastamise keerulisemaks, kuid mitte võimatuks.

# JÄRELEVALVE JA LOGIMINE

## JÄRELEVALVE JA LOGIMISE OLULISUS

- **Jälgimine ja audit:** Tagab süsteemide pideva jälgimise ja võimaldab läbi viia auditeid turvalisuse tagamiseks.

JÄRELEVALVE JA LOGIMISE MEETODID

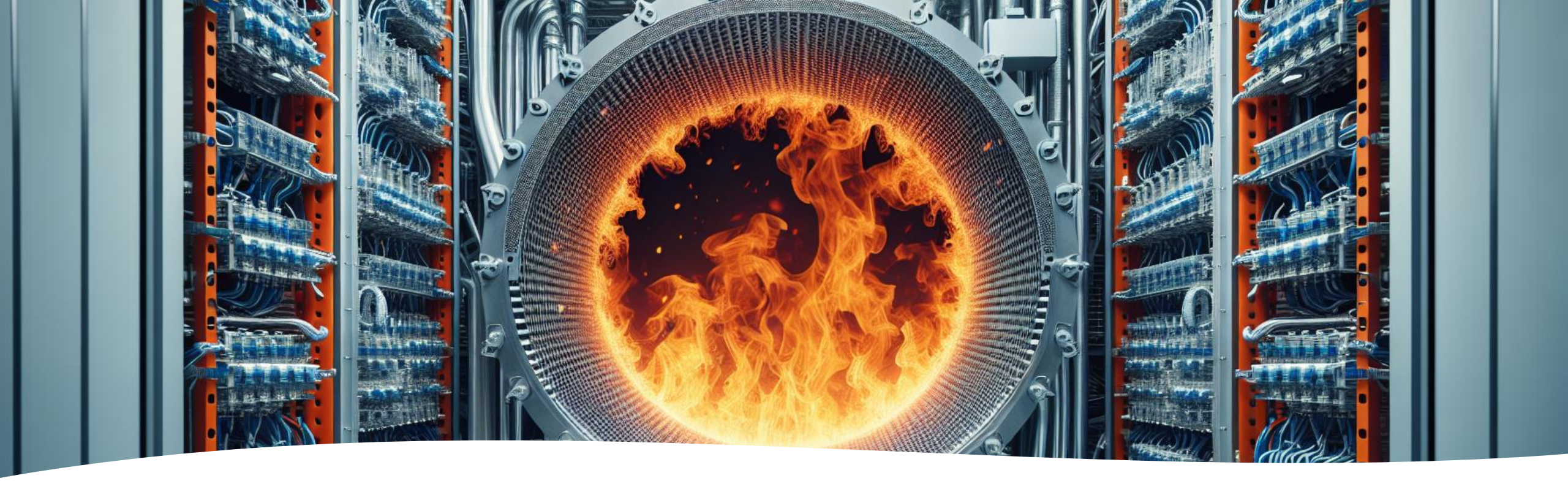
- **Logimissüsteemid:** Logimissüsteemide kasutamine, et jälgida ja salvestada kõikide süsteemide ja võrkude tegevused.
- **Funktsioon:** Salvestab süsteemide ja võrkude tegevuste logid, et tuvastada ebatavaline tegevus ja viia läbi auditeid.
- **SIEM (Security Information and Event Management):** SIEM-lahenduste kasutamine logide analüüsimiseks ja turvaintsidentide tuvastamiseks reaalajas.
- **Funktsioon:** Kogub, analüüsib ja korreleerib logisid erinevatest allikatest, et tuvastada ja reageerida turvaintsidentidele reaalajas.

# IV osa

# Tulemüüride kasutamine külmasü-steemides

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks



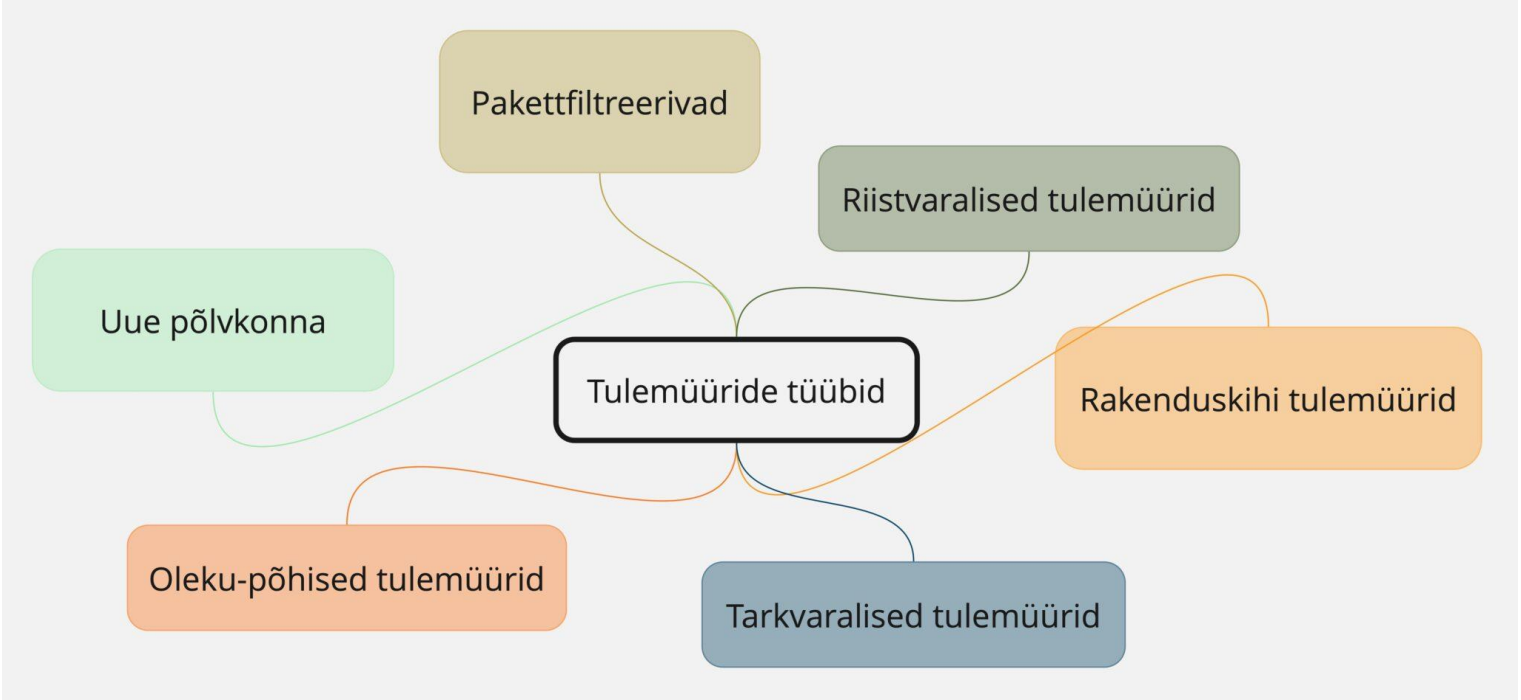
## TULEMÜÜRIDE KASUTAMINE KÜLMASÜSTEEMIDES

Külmasüsteemid, mis hõlmavad tööstuslikke jahutusseadmeid, kaubanduslikke külmutusseadmeid ja kliimaseadmeid, on olulised paljudes tööstusharudes alates toiduainete töötlemisest kuni farmaatsiasektorini. Nende süsteemide töökindlus ja tõhusus on kriitilise tähtsusega, kuid üha enam on tähelepanu pööratud ka nende turvalisusele. Tulemüürid on üks peamisi küberjulgeoleku vahendeid, mida kasutatakse andmeside kaitsmiseks ja süsteemide turvalisuse tagamiseks.

# Tööstuskeskkon na tulemüürid

- Tulemüürid mängivad kriitilist rolli tööstuslike infovõrkude kaitsmisel, pakkudes esmast kaitset volitamata juurdepääsu ja küberrünnakute vastu. Tööstuskeskkonnas, kus kasutatakse keerukaid süsteeme nagu SCADA (Supervisory Control and Data Acquisition) ja ICS (Industrial Control Systems), on tulemüürid hädavajalikud, et tagada pidev ja turvaline töö

# Mis on tulemüür?



# Tulemüüride Tüübid

1. Tulemüürid süsteemide järgi
    1. Riistvaralised tulemüürid
    2. Tarkvaralised tulemüürid
    3. Uue põlvkonna tulemüürid (NGFW)
2. Hostipõhised tulemüürid
    1. Serveripõhised tulemüürid
    2. Töötajate arvutite tulemüürid
3. Perimeetri tulemüürid
4. Jaotatud tulemüürid
5. Pakettfiltreerimise tulemüürid
6. Oleku põhised tulemüürid
7. Puhverserveri tulemüürid
8. Veebirakenduse tulemüürid (WAF)

# Tulemüüride tüübid

**Tulemüürid süsteemide järgi**

1. Riistvaralised tulemüürid
2. Tarkvaralised tulemüürid
3. Uue põlvkonna tulemüürid (NGFW)

**Hostipõhised tulemüürid**

1. Serveripõhised tulemüürid
2. Töötajate arvutite tulemüürid

**Perimeetri tulemüürid**

**Jaotatud tulemüürid**

**Pakettfiltreerimise tulemüürid**

**Oleku põhised tulemüürid**

**Puhverserveri tulemüürid**

**Veebirakenduse tulemüürid (WAF)**

# 1.Riistvaralised tulemüürid

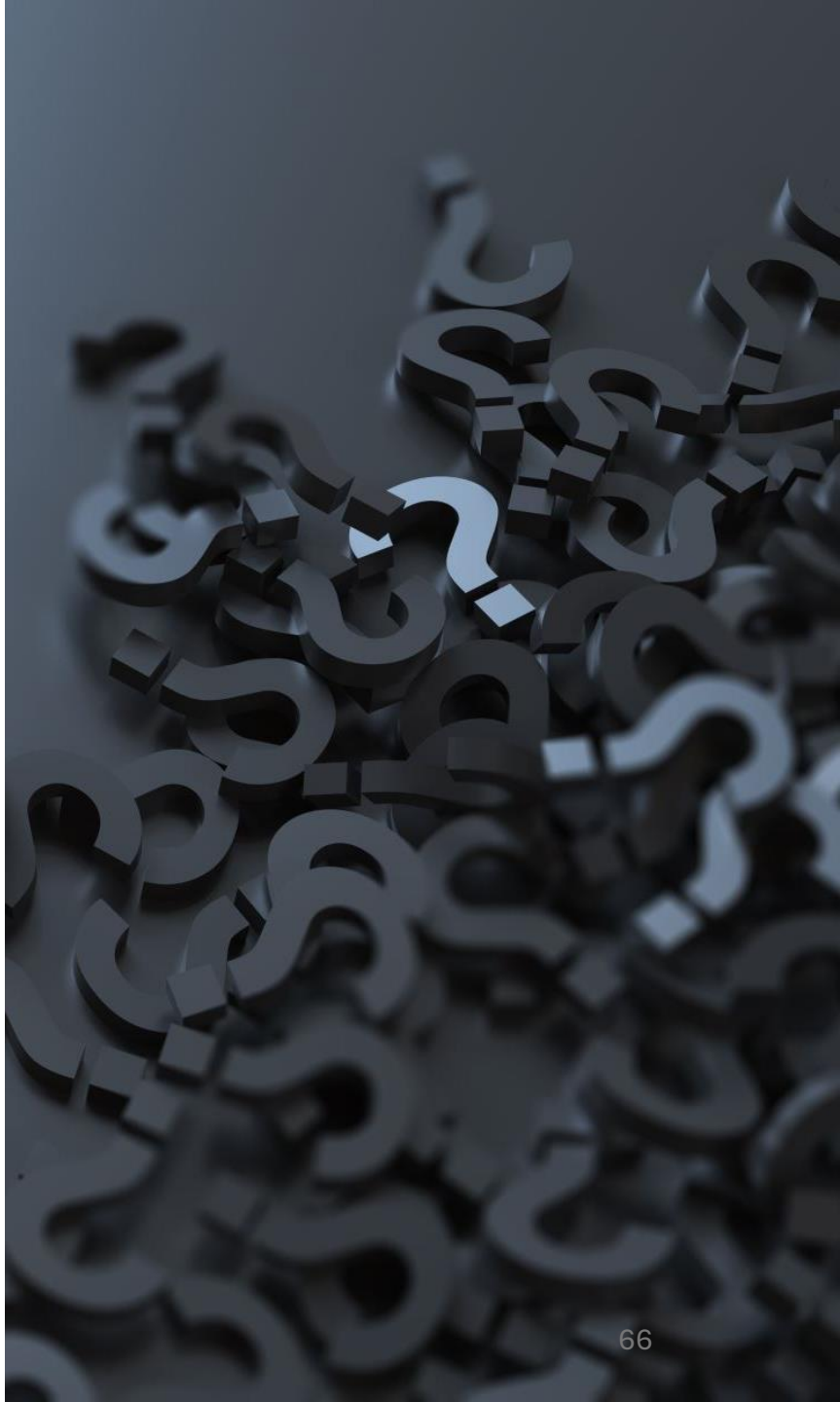
**Riistvaralised tulemüürid** on spetsiaalsed seadmed, mis paiknevad tavaliselt tööstusvõrkude ja väliste võrkude vahel. Need pakuvad võimsat ja usaldusväärset kaitset, mida on tööstuskeskkondades sageli vaja.

**Eelised**:

- **Kõrge jõudlus**: Suudavad töödelda suurt andmemahtu ilma võrgu jõudlust oluliselt mõjutamata.
- **Usaldusväärsus**: Eraldiseisvad seadmed, mis on vähem vastuvõtlikud viirustele ja tarkvaravigadele.

**Puudused**:

- **Kõrgem hind**: Võivad olla kulukamad nii ostmisel kui hooldamisel.
- **Paindlikkuse puudumine**: Võib olla raskem kohandada ja uuendada võrreldes tarkvaraliste tulemüüridega.



# Tarkvaralised tulemüürid

Tarkvaralised tulemüürid on programmipõhised lahendused, mis töötavad serverites või virtuaalmasinates. Need pakuvad sama turvalisust nagu riistvaralised tulemüürid, kuid on paindlikumad ja hõlpsamini kohandatavad.

**Eelised**:

- **Paindlikkus**: Hõlpsasti kohandatavad ja uuendatavad.
- **Madalam hind**: Tavaliselt odavamad ja võivad olla tasuta kättesaadavad.

**Puudused**:

- **Madalam jõudlus**: Võivad võrgu jõudlust vähendada, eriti suure liikluse korral.
- **Vähem turvalised**: Kuna töötavad samal süsteemil, mida kaitsevad, võivad olla vastuvõtlikumad rünnakutele.
- **Näiteks** Microsoft Azure ja AWS pakuvad tarkvaralisi tulemüüre pilvekeskkondade jaoks.

# Uue põlvkonna tulemüürid (NGFW)

Uue põlvkonna tulemüürid (Next-Generation Firewalls ehk NGFW) on võrguturbe seadmed, mis pakuvad täiustatud ja tänapäevast kaitset

**NGFW EELISED**

1. **Terviklik turvalisus**:.
2. **Parema nähtavuse ja kontrolli tagamine**:
3. **Proaktiivne turvajuhtimine**:
4. **Skaleeritavus ja paindlikkus**:

**PUUDUSED**:

- **Kõrgem hind**: Kallimad kui traditsioonilised tulemüürid.
- **Keerukus**: Keerulisem seadistada ja hallata.

# 2.Hostipõhised tulemüürid

Hostipõhised tulemüürid paigaldatakse individuaalsetele seadmetele, pakkudes kaitset konkreetsel masinal. Need on eriti kasulikud, kui seadmed töötavad tundlikke andmeid või on otseses kontaktis välise võrguga

**HOSTIPÕHISTE TULEMÜÜRIDE EELISED:**

1. **Individuaalne kaitse**:
2. **Sissetuleva ja väljamineva liikluse kontroll**.
3. **Lihtne konfigureerida**:
4. **Täiendav kaitse**

**Isiklikud arvutid**: Kodukasutajad paigaldavad hostipõhised tulemüürid, et kaitsta oma arvuteid ja andmeid internetis surfamise ajal.

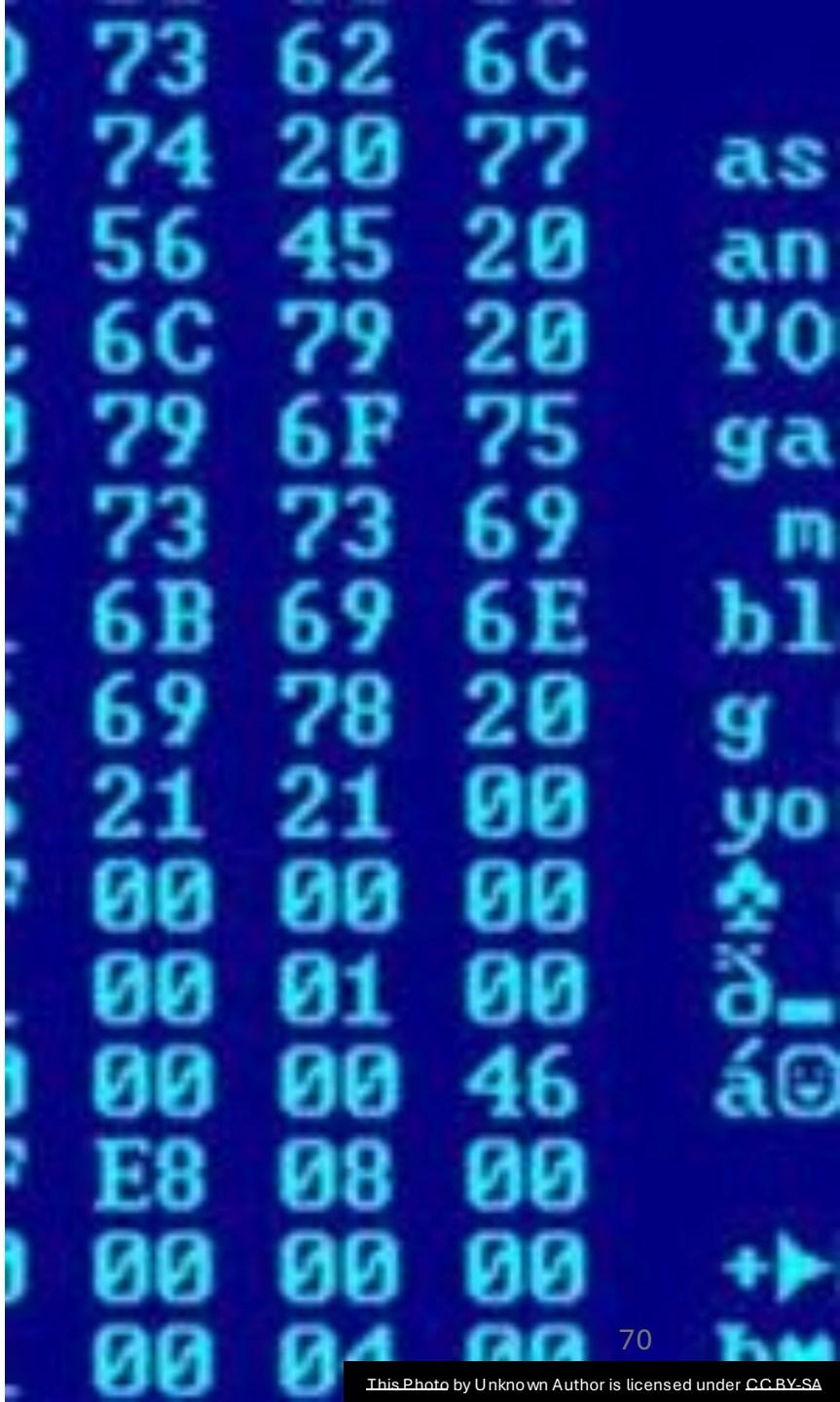
Jne.

# 3. Perimeetri tulemüürid

Perimeetri tulemüürid paiknevad ettevõtte sisevõrgu ja välise võrgu piiril, kontrollides kogu sissetulevat ja väljaminevat liiklust. Need pakuvad esmast kaitset väliste rünnakute eest, blokeerides volitamata juurdepääsu ja turvades ettevõtte sisevõrku.

NÄITED:

1. **SonicWall**: SonicWall pakub laia valikut perimeetri tulemüüre, mis on mõeldud väikestest ettevõtetest kuni suurte korporatsioonideni.
2. **Juniper Networks**: Juniper Networks pakub perimeetri tulemüüre, mis on loodud ettevõtete ja andmekeskuste turvamiseks.



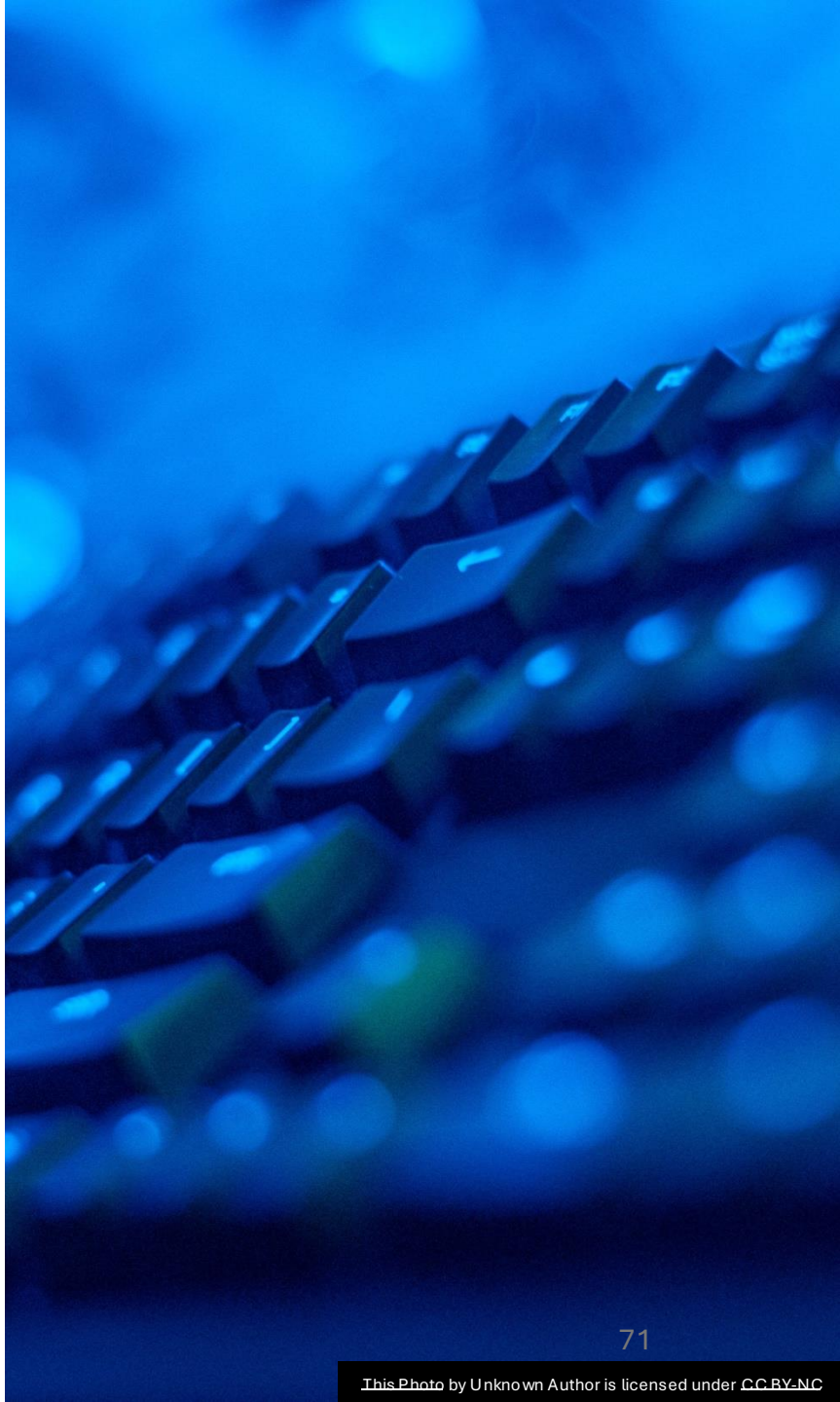
# 4. Jaotatud tulemüürid.

Jaotatud tulemüürid on võrguturbe mehhanismid, mis toimivad kogu ettevõtte infrastruktuuris, jälgides ja reguleerides liiklust mitme seadme vahel. Need tulemüürid pakuvad paremat kaitset sisemiste ohtude eest, kuna nad suudavad jälgida ja kontrollida liiklust otse seadmete tasemel, mitte ainult perimeetril.

NÄITED:

**VMware NSX**: VMware NSX on virtualiseeritud võrgulahendus, mis pakub jaotatud tulemüüri funktsioone.

**Cisco ACI**: Cisco Application Centric Infrastructure (ACI) on lahendus, mis ühendab võrgutöötluse ja turvalisuse.



# 5. Pakettfiltreerimise tulemüürid

Pakettfiltreerimise tulemüürid töötavad võrgukihi tasemel, kontrollides andmepakette eelnevalt määratletud reeglite alusel. Nad kontrollivad andmepakettide päiseid ja filtreerivad liiklust vastavalt määratud reeglitele. NÄITED:

**IPTables**: IPTables on populaarne pakettfiltreerimise tulemüür Linuxi süsteemides. See võimaldab kasutajatel määrata reegleid, mis kontrollivad, millised andmepaketid võivad võrgus liikuda.

**pfSense**: pfSense on avatud lähtekoodiga tulemüür, mis pakub pakettfiltreerimise ja NAT (Network Address Translation) funktsioone. pfSense on tuntud oma paindlikkuse ja konfigureeritavuse poolest.

# 6. Oleku (seisundi) põhised tulemüürid

Oleku-põhised tulemüürid (Stateful Inspection Firewalls) kuuluvad OSI (Open Systems Interconnection) mudeli järgi Layer 3 ja Layer 4 klassi tulemüüride alla. Oleku-põhised tulemüürid toimivad järgmiselt:

1. **Töötavad võrgu- ja transpordikihis**: Oleku-põhised tulemüürid analüüsivad ja filtreerivad liiklust võrgu- ja transpordikihi tasemel.
2. **Oleku jälgimine**: Erinevalt staatilistest tulemüüridest, mis kontrollivad iga paketti eraldi, jälgivad oleku-põhised tulemüürid kogu ühenduse olekut.
3. **Paketisisu analüüs**: Oleku-põhised tulemüürid analüüsivad pakette sügavamalt kui staatilised tulemüürid, kontrollides, kas pakett on osa kehtivast ja lubatud seansist.
4. **Tugev turvalisus**: Oleku-põhised tulemüürid pakuvad kõrgemat turvalisust võrreldes staatiliste tulemüüridega, kuna nad suudavad tuvastada ja blokeerida rünnakuid, mis püüavad ära kasutada üksikute pakettide lubamise loogikat.

# 7. Puhverserveri tulemüürid

Puhverserveri tulemüürid (proxy tulemüürid) Puhverserveri tulemüürid, tuntud ka kui rakenduskihi tulemüürid, toimivad vahendajatena klientide ja sihtserverite vahel. EELISED

1. **Sügav liikluse kontroll**: Puhverserveri tulemüürid saavad liiklust uurida detailsemalt, sealhulgas
2. **Kasutajapõhine turvalisus**: Need tulemüürid saavad autentida kasutajaid ja rakendada erinevaid turvapoliitikaid sõltuvalt kasutaja identiteedist.
3. **Logimine ja jälgimine**: Võimaldavad põhjalikku logimist ja kasutajate tegevuste jälgimist.
4. **Andmete kaitse**: Kaitsevad ettevõtte sisevõrku, filtreerides välja pahatahtliku liikluse ja ennetades tundliku teabe lekkimist.
5. **Vahemällu salvestamine (caching) -** Võimaldavad vahemällu salvestamist, mis parandab jõudlust.

# 8. Veebirakenduse (rakenduskihi) tulemüürid (waf)

Veebirakenduse tulemüürid kaitsevad veebirakendusi.

Rakenduskihi tulemüürid toimivad järgmiselt:

1. **Töötavad rakenduskihis**: Nad analüüsivad ja filtreerivad liiklust rakenduse tasemel. See võimaldab neil mõista ja kontrollida spetsiifilisi rakenduse protokolle, nagu HTTP, FTP, ja DNS.
2. **Paketisisu analüüs**: See võimaldab neil tuvastada ja blokeerida keerukamaid rünnakuid, nagu SQL injektsioonid ja XSS (cross-site scripting).
3. **Kasutavad proxy meetodit**: Samuti võtavad nad vastu serveri vastuse, kontrollivad seda, ja edastavad kliendile.
4. **Tugev turvalisus**: Nad suudavad tuvastada ja peatada spetsiifilisi rakenduse taseme rünnakuid.

# Tulemüüride integreerimine tööstuskeskkonda

Tööstuskeskkonnas on oluline integreerida tulemüürid nii võrgutasemel kui ka individuaalsetes seadmetes. See hõlmab tulemüüride paigaldamist SCADA süsteemidesse, PLC-dele ja muudele kriitilistele infrastruktuuridele, tagamaks, et kõik andmevood on turvalised ja kaitstud.

- **Näiteks** võib tööstusettevõte kasutada Fortineti või Palo Alto tulemüüre, et kaitsta oma tootmisliine ja andmevooge

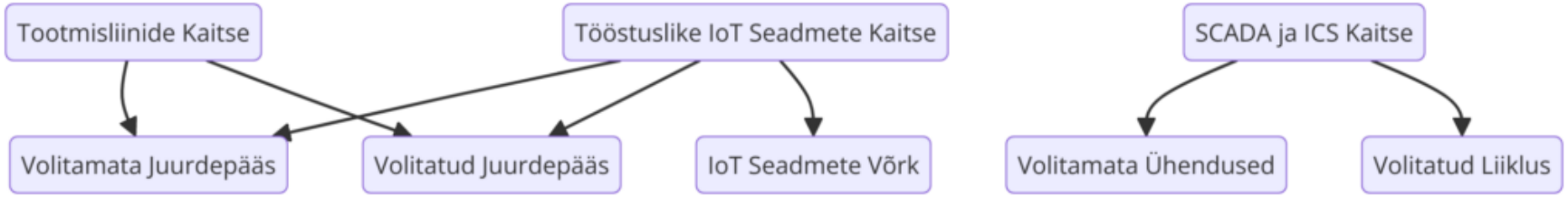
# Tulemüüride seadistamine ja halduse parimad tavad tööstuskeskkonnas

Reeglite defineerimine: Regulaarne audit.

Dokumente erimine.

Uuendused.

Koolitus.




**1. Tootmisliinide Kaitse**

- Tootmisliinide kaitsmine on kriitilise tähtsusega, kuna igasugune rünnak või volitamata juurdepääs võib põhjustada tootmise seiskumise ja märkimisväärseid rahalisi kahjusid. Tulemüürid aitavad piirata juurdepääsu ainult volitatud kasutajatele ja seadmetele.

**2. SCADA ja ICS Kaitse**

- SCADA ja ICS süsteemid on sageli küberrünnakute sihtmärgid, kuna need kontrollivad ja jälgivad olulisi tootmis- ja infrastruktuuriprotsesse. Tulemüürid kaitsevad neid süsteeme, võimaldades ainult volitatud liikluse ja blokeerides kõik volitamata ühendused.

**3. Tööstuslike IoT Seadmete Kaitse**

- Tööstuslikud IoT seadmed on üha sagedamini kasutusel, kuid nende turvalisus on sageli nõrk. Tulemüürid kaitsevad IoT seadmeid, filtreerides liiklust ja tagades, et ainult volitatud seadmed saavad võrku ühenduda.

# Tulemüüride rakendamine tööstuslikus kontekstis

# Tulemüüride juhtumiuuringud tööstuskeskkonnas

Tööstuskeskkondades on tulemüüride kasutamine kriitilise tähtsusega, kuna need kaitsevad olulisi süsteeme ja andmeid küberohtude eest. Järgnevalt on esitatud põhjalikud juhtumiuuringud tööstustulemüüride rakendamisest.

**Juhtumiuuring 1: Siemens Scalance S Tulemüürid**

- **Taust**
- Üks juhtiv autoosade tootja seisis silmitsi kasvavate küberohtudega. Ettevõtte tootmisliinid ja SCADA süsteemid olid ühendatud laiaulatusliku võrgu kaudu, mis muutis need haavatavaks volitamata juurdepääsu ja rünnakute suhtes. Tootmise peatamine või andmete vargus võinuks põhjustada märkimisväärseid rahalisi kahjusid ja mainekahju.
- **Lahendus**
- Ettevõte otsustas rakendada Siemens Scalance S seeria tulemüüre, et tagada oma tööstusvõrkude turvalisus. Scalance S seeria tulemüürid pakuvad tugevat kaitset ja võimaldavad võrgu segmentimist, mis on kriitilise tähtsusega, et piirata juurdepääsu ainult volitatud kasutajatele ja seadmetele.

# JUHTUMIUURING 2: ABB TÖÖSTUSLIKU IOT KAITSE

TAUST

ABB, juhtiv energia ja automaatikatehnoloogia ettevõte, seisis silmitsi vajadusega kaitsta oma tööstuslikke IoT seadmeid, mis olid ühendatud globaalse võrguga. IoT seadmed olid kriitilised erinevate tööstusprotsesside jälgimisel ja juhtimisel, kuid nende turvalisus oli sageli nõrk.

LAHENDUS

ABB rakendas oma võrkudes uue põlvkonna tulemüüre (NGFW), et tagada IoT seadmete turvalisus. NGFW-d ühendavad traditsiooniliste tulemüüride funktsioonid täiendavate turvafunktsioonidega nagu sissetungimise tuvastamise ja ennetamise süsteemid (IDS/IPS), rakenduste teadlikkus ja viirusetõrje.

# JUHTUMIUURING 3: ENERGIASEKTORI KAITSE

TAUST

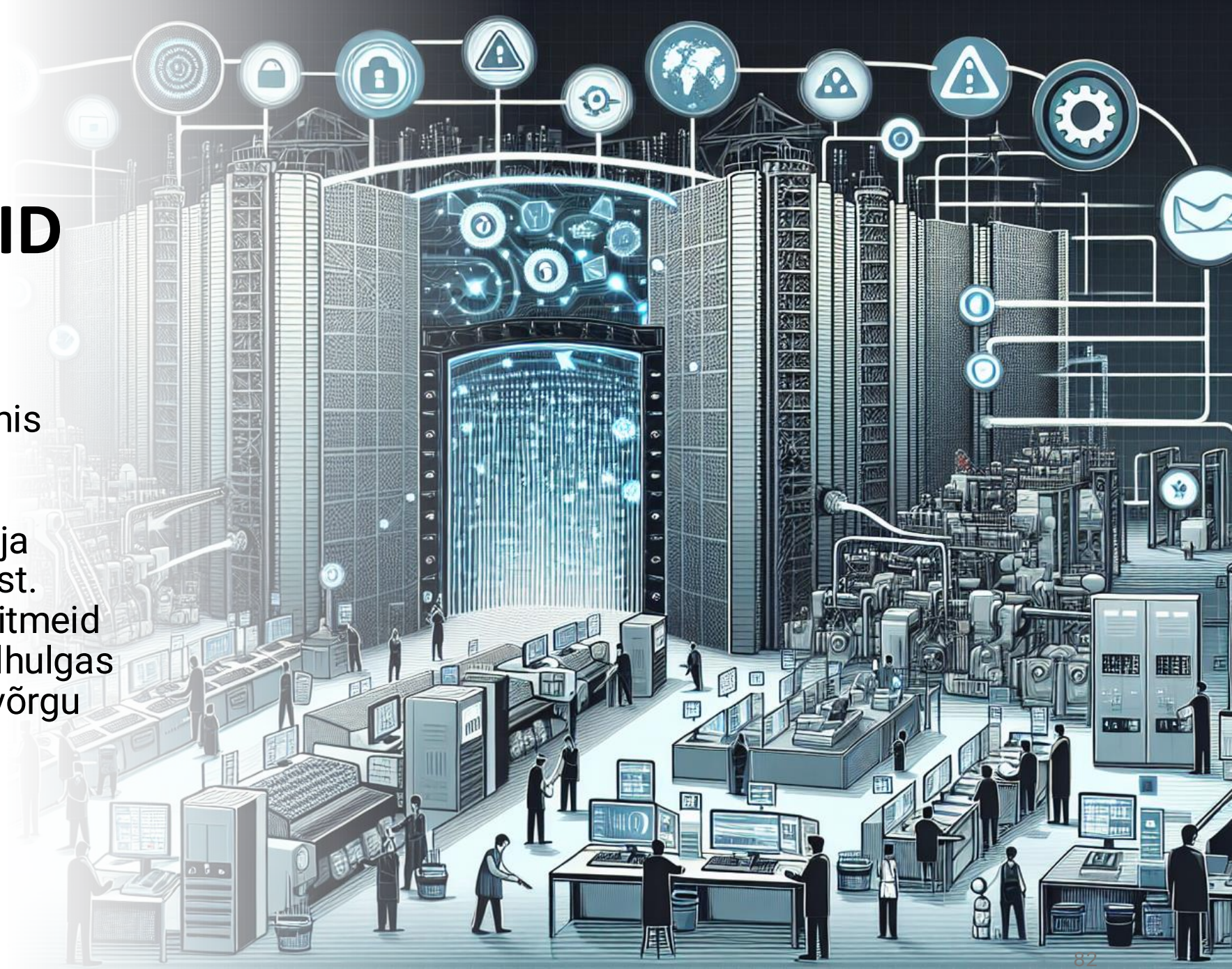
Energiasektoris tegutsev ettevõte, mis haldab suuri elektrivõrke ja jaotussüsteeme, seisab silmitsi suurenenud küberohtudega. Elektrivõrkude kaitse on kriitilise tähtsusega, kuna igasugune rünnak võib põhjustada ulatuslikke katkestusi ja kahjustada infrastruktuuri.

LAHENDUS

Ettevõte rakendas riistvaralisi tulemüüre, mis olid spetsiaalselt projekteeritud tööstuslike juhtimissüsteemide (ICS) kaitsmiseks. Need tulemüürid pakkusid tugevat kaitset ja võimaldasid keerukate turvameetmete rakendamist.

# TULEMÜÜRI FUNKTSIOONID

- Tulemüürid on kriitilise tähtsusega seadmed, mis aitavad kaitsta võrke ja süsteeme volitamata juurdepääsu, pahavara ja muude küberohtude eest. Tulemüürid täidavad mitmeid olulisi funktsioone, sealhulgas liikluse filtreerimine ja võrgu segmenteerimine.



# Liikluse filtreerimine

Tulemüürid filtreerivad võrguliiklust, otsustades, millised paketid lubatakse läbi ja millised blokeeritakse. See aitab kaitsta võrku volitamata juurdepääsu ja pahatahtliku tegevuse eest.

**Pakettfiltreerimine**

- **Pakettfiltreerimine** on tehnika, kus tulemüür kontrollib iga andmepaketi päiseid, et teha otsus selle lubamise või blokeerimise kohta. Pakettfiltreerimine toimub võrgukihi (Layer 3) tasandil.
- **Rakenduskihi** tehnika puhul kontrollib tulemüür rakenduste andmevahetust, et avastada ja blokeerida pahatahtlikku tegevust. Rakenduskiht-filtreerimine toimub rakenduskiht (Layer 7) tasandil ja võimaldab süvitsi vaadata rakenduste liiklust.

# Pakettfiltreerimine

| .IP-aadresside | Pordinumbrite | Protokolli kontroll: Tulemüür kontrollib, millist protokolli pakett kasutab (nt TCP, UDP, ICMP) ja teeb otsuse selle põhjal. |
|---|---|---|
| **kontroll:** Tulemüür kontrollib andmepaketi lähte- ja siht-IP-aadresse ning otsustab, kas lubada pakett läbi. | **kontroll:** Tulemüür kontrollib andmepaketi lähte- ja sihtpordi numbreid, et määrata, millised teenused on lubatud. | |
| • **Näide:** Lubada liiklus ainult usaldusväärsetest IP-aadressidest ja blokeerida kõik teised. | • **Näide:** Lubada liiklus ainult HTTP (port 80) ja HTTPS (port 443) portidest ning blokeerida kõik teised. | • **Näide:** Lubada ainult TCP-liiklus ja blokeerida kõik UDP-põhised päringud. |

**Pakettfiltreerimine** on tehnika, kus tulemüür kontrollib iga andmepaketi päiseid, et teha otsus selle lubamise või blokeerimise kohta. Pakettfiltreerimine toimub võrgukihi (Layer 3) tasandil

# Rakenduskihi tehnika

**.HTTP ja HTTPS Filtreerimine:** Kontrollib veebiliiklust, et tuvastada ja blokeerida pahatahtlikud veebilehed ja skriptid.

- **Näide:** Blokeerida juurdepääs tuntud pahatahtlikele veebilehtedele või filtreerida sisu, nagu pahatahtlik JavaScript.

**E-posti Filtreerimine:** Kontrollib e-posti liiklust (nt SMTP, IMAP), et avastada ja blokeerida rämpspost ja pahatahtlikud manused.

- **Näide:** Kasutada viirusetõrjet ja rämpsposti filtreid e-posti süsteemides.

**Rakenduste Spetsiifilised Reeglid:** Määrab reeglid konkreetsetele rakendustele ja protokollidele, et tagada, et ainult volitatud rakendused saavad võrguressursse kasutada.

- **Näide:** Lubada juurdepääs andmebaasiserverile ainult volitatud rakendustel

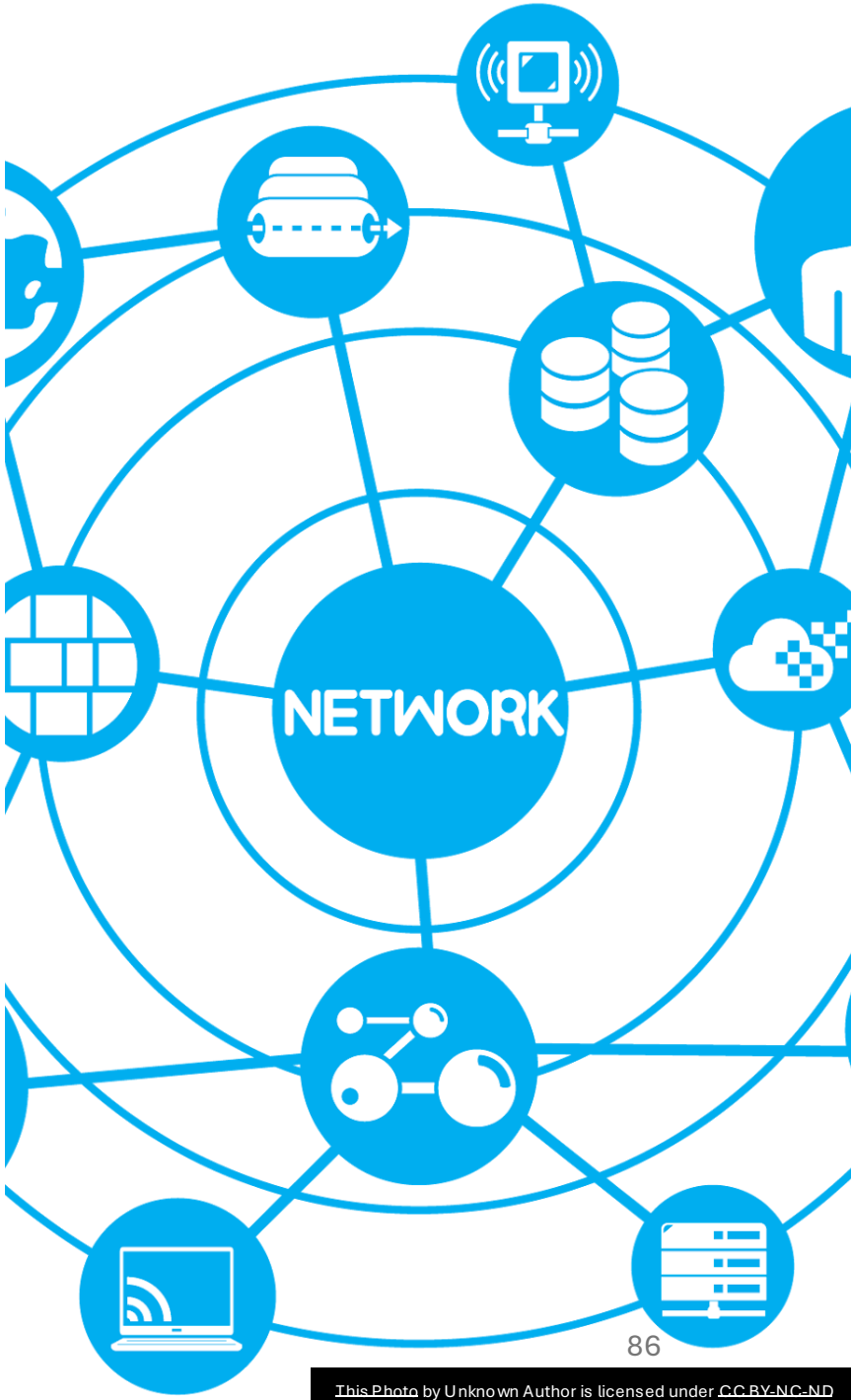
**Rakenduskihi** tehnika puhul kontrollib tulemüür rakenduste andmevahetust, et avastada ja blokeerida pahatahtlikku tegevust. Rakenduskiht-filtreerimine toimub rakenduskiht (Layer 7) tasandil ja võimaldab süvitsi vaadata rakenduste liiklust

# Võrgu segmenteerimine

Tulemüürid aitavad võrgu segmenteerimisel, eraldades erinevad võrgusegmendid ja tagades, et liiklus nende vahel on kontrollitud ja turvaline.

**Eraldavad võrgud**

- **Eraldavad Võrgud** on võrgusegmentide loomise meetod, kus kasutatakse VLAN-e ja alavõrke, et jagada suur võrk väiksemateks, eraldatud osadeks. See aitab piirata ründevektorite levikut ja suurendab üldist turvalisust.
- **VLAN-id (Virtual Local Area Networks):** VLAN-id võimaldavad loogiliselt jagada füüsilist võrku väiksemateks segmentideks, mis võivad olla eraldatud isegi füüsiliselt samas võrgus.
- **Alavõrgud (Subnets):** Alavõrgud jagavad IP-võrgu väiksemateks osadeks, mis võivad omada erinevaid turvapoliitikaid ja juurdepääsukontrolle.
- **DMZ (Demilitarized Zone):** DMZ on võrgu segment, mis eraldab avaliku võrgu ja privaatvõrgu, vähendades turvariske.



# IP Reeglid

IP reeglid on olulised komponendid tulemüürides, mis määravad, milline võrguliiklus on lubatud ja milline on blokeeritud. Need reeglid aitavad hallata ja kontrollida juurdepääsu võrgule ja selle ressurssidele, tagades võrgu turvalisuse ja töökindluse.

- **Reeglite Määratlemine**
- IP reeglite määratlemine on protsess, mille käigus määratakse kindlaks, milline liiklus on lubatud või blokeeritud. Reeglid võivad põhineda mitmetel parameetritel, sealhulgas lähte- ja siht-IP-aadressid, portnumbrid ja protokollid.

# Sissetuleva ja väljamineva liikluse reeglid

1

**Sissetuleva liikluse reeglid:** Määravad, milline sissetulev liiklus on lubatud võrku ja milline tuleb blokeerida. Need reeglid on olulised volitamata juurdepääsu ennetamiseks ja turvalisuse tagamiseks.

- **Näide:** Lubada ainult HTTP (port 80) ja HTTPS (port 443) liiklus veebiserverile ja blokeerida kõik teised sissetulevad päringud.
- **Näide:** Lubada SSH (port 22) ühendused ainult kindlate IP-aadresside vahemikust ja blokeerida kõik teised sissetulevad SSH ühendused.

2

**Väljamineva liikluse reeglid:** Määravad, milline väljaminev liiklus on lubatud võrku ja milline tuleb blokeerida. Need reeglid aitavad hallata võrguressursside kasutamist ja piirata volitamata ühendusi.

- **Näide:** Lubada töötajatel pääseda internetti ainult kindlate portide kaudu (nt HTTP, HTTPS) ja blokeerida kõik muud väljaminevad ühendused.
- **Näide:** Lubada serveritel suhelda andmebaasidega ainult kindlate IP-aadresside ja portide kaudu.

# Reeglite tüübid

IP reeglid võivad olla kas lubavad (allow) või keelavad (deny). Need kaks tüüpi reegleid võimaldavad tulemüüril täpselt määrata, milline liiklus on lubatud ja milline on blokeeritud.

- **Luba (Allow)**
- **Luba (Allow):** Reegel, mis määrab, et kindel liiklus on lubatud võrku läbima. Lubavad reeglid võimaldavad volitatud liiklusel jõuda oma sihtkohta ja kasutavad turvaliselt võrgu ressursse.
- **Näide:** Lubada kõik HTTPS liiklus (port 443) lähte- ja siht-IP-aadresside vahemikust.
- **Näide:** Lubada sissetulev ja väljaminev liiklus kindlast IP-aadressist andmebaasi serverile (port 3306).

**Keela (Deny)**

- **Keela (Deny):** Reegel, mis määrab, et kindel liiklus tuleb blokeerida ja see ei ole lubatud võrku läbima. Keelavad reeglid on olulised volitamata juurdepääsu ennetamiseks ja võrgu turvalisuse tagamiseks.
- **Näide:** Keelata kõik SSH (port 22) ühendused, välja arvatud need, mis pärinevad kindlast IP-aadresside vahemikust.
- **Näide:** Blokeerida kõik sissetulevad ICMP (ping) päringud, et vältida võrgu kaardistamist ja potentsiaalseid rünnakuid.

# Näited reeglitest

SISSETULEVA LIIKLUSE REEGLID

**Reegel:** Luba HTTPS liiklus (port 443) kõigilt IP-aadressidelt veebiserverile.

**Tüüp:** Allow

**Lähteaadress:** Kõik

**Sihtaadress:** Veebiserveri IP

**Protokoll:** TCP

**Port:** 443

**Reegel:** Keelata kõik sissetulevad SSH ühendused (port 22), välja arvatud need, mis pärinevad IT-osakonna IP-aadresside vahemikust.

**Tüüp:** Deny

**Lähteaadress:** Kõik (v.a IT-osakonna IP vahemik)

**Sihtaadress:** Kõik

**Protokoll:** TCP

**Port:** 22

VÄLJAMINEVA LIIKLUSE REEGLID

**Reegel:** Lubada kõik HTTP ja HTTPS liiklus (port 80 ja 443) töötajate tööarvutitest internetti.

**Tüüp:** Allow

**Lähteaadress:** Töötajate tööarvutite IP vahemik

**Sihtaadress:** Kõik

**Protokoll:** TCP

**Port:** 80, 443

**Reegel:** Keelata kõik väljaminevad ühendused andmebaasiserverilt, välja arvatud need, mis suunduvad varundusserverile.

- **Tüüp:** Deny
- **Lähteaadress:** Andmebaasiserveri IP
- **Sihtaadress:** Kõik (v.a varundusserveri IP)
- **Protokoll:** Kõik
- **Port:** Kõik



8/13/2024 90

# Hindamise järjekord

Tulemüüri reeglite hindamise järjekord määrab, kuidas ja millises järjekorras reegleid rakendatakse, et kontrollida võrguliiklust. Reeglite hindamise protsess ja prioriteetide seadmine on kriitilise tähtsusega, et tagada liikluse täpne ja turvaline kontroll.

- **REEGLITE HINDAMINE**
- Reeglite hindamine on protsess, mille käigus tulemüür kontrollib liikluse vastu määratud reegleid ja otsustab, milline reegel kehtib iga konkreetse paketi suhtes. Tulemüür hindab reegleid kindlas järjekorras, mis on oluline, et vältida konflikte ja tagada reeglite täpne rakendamine.

# Prioriteetide seadmine

**Prioriteetide seadmine:** Tulemüür hindab reegleid kindlas järjekorras, alustades kõige täpsematest. See tähendab, et kõige spetsiifilisemad reeglid, mis vastavad konkreetsetele kriteeriumidele, hindavad enne üldisemaid reegleid, mis võivad hõlmata suuremat liiklusmahtu.

- **Näide:** Kui on olemas spetsiifiline reegel, mis lubab ainult teatud IP-aadressilt tuleva liikluse, siis see reegel hindab enne üldist reeglit, mis võib lubada kogu sissetuleva HTTP liikluse.
- **Eelis:** Prioriteetide seadmine tagab, et kriitilised ja spetsiifilised reeglid rakenduvad esmalt, pakkudes täpsemat kontrolli liikluse üle.

# Esmatähtsad ja üldised reeglid

SPETSIIFILISED REEGLID

- **Spetsiifilised reeglid:** Need on reeglid, mis on määratletud konkreetsete kriteeriumide alusel, nagu kindel IP-aadress, port või protokoll. Spetsiifilised reeglid rakenduvad enne üldiseid reegleid, et tagada täpne kontroll ja suurem turvalisus.
- **Rakendamine:** Tulemüür kontrollib esimesena spetsiifilisi reegleid, et kindlaks teha, kas liiklus vastab täpselt määratletud tingimustele.
    - **Näide:** Reegel, mis lubab liikluse ainult teatud IP-aadressilt ja ainult kindlale portile.

# Esmatähtsad ja üldised reeglid

ÜLDISED REEGLID

- **Üldised reeglid:** Need on reeglid, mis katavad laiemat liiklusmahtu ja on vähem spetsiifilised. Üldised reeglid hindavad pärast spetsiifilisi reegleid ja neid kasutatakse üldise liikluse kontrollimiseks ja haldamiseks.
- **Rakendamine:** Pärast seda, kui kõik spetsiifilised reeglid on hinnatud ja ükski neist ei kehti, hindab tulemüür üldisi reegleid, et teha otsus liikluse kohta.
    - **Näide:** Reegel, mis lubab kõik sissetulevad HTTP ühendused sõltumata lähte-IP-aadressist.

# Näited hindamise järjekorrast

PRIORITEETIDE SEADMINE

**Reegel:** Lubada HTTPS liiklus (port 443) ainult IT-osakonna IP-aadressilt.

**Tüüp:** Allow

**Lähteaadress:** IT-osakonna IP

**Sihtaadress:** Veebiserveri IP

**Protokoll:** TCP

**Port:** 443

**Prioriteet:** Kõrge

**Reegel:** Keelata kõik sissetulevad SSH ühendused (port 22), välja arvatud need, mis pärinevad turvalisest VPN-i IP-aadressist.

**Tüüp:** Deny

**Lähteaadress:** Kõik (v.a VPN-i IP)

**Sihtaadress:** Kõik

**Protokoll:** TCP

**Port:** 22

**Prioriteet:** Kõrge

ESMATÄHTSAD JA ÜLDISED REEGLID

**Spetsiifiline reegel:** Lubada sissetulev liiklus veebiserverile ainult kindlalt IP-aadressilt (administraatori tööarvuti).

**Tüüp:** Allow

**Lähteaadress:** Administraatori tööarvuti IP

**Sihtaadress:** Veebiserveri IP

**Protokoll:** TCP

**Port:** 80, 443

**Prioriteet:** Kõrge

**Üldine reegel:** Lubada kõik sissetulevad HTTP ja HTTPS ühendused sõltumata lähte-IP-aadressist.

**Tüüp:** Allow

**Lähteaadress:** Kõik

**Sihtaadress:** Veebiserveri IP

**Protokoll:** TCP

**Port:** 80, 443

**Prioriteet:** Madal

# Eelnevalt kindlaks määratud reeglid

Tulemüürides kasutatakse sageli eelnevalt kindlaks määratud reegleid, mis on süsteemi tootjate poolt ette nähtud. Need reeglid pakuvad baaskaitset ja aitavad järgida parimaid turvapraktikaid. Lisaks tagavad need süsteemi esialgse turvalisuse, enne kui kohandatud reeglid rakendatakse.

# Tootjapoolsed reeglid

**Tootjapoolsed Reeglid** on süsteemi tootjate poolt määratud reeglid, mis on loodud tagama baasturvalisuse ja järgima parimaid praktikaid. Need reeglid on sageli eelkonfigureeritud ja integreeritud süsteemi osana.

SÜSTEEMI TOOTJATE POOLT MÄÄRATUD REEGLID

- Tootjapoolsed reeglid on ette nähtud, et pakkuda algset turvataset ja kaitset kohe pärast süsteemi paigaldamist.
- **Standardne konfiguratsioon:** Paljud tulemüürid tulevad eelkonfigureeritud reeglitega, mis pakuvad üldist kaitset levinud rünnakute ja ohtude vastu.
- **Parimad praktikad:** Need reeglid põhinevad parimatel praktikatel, mis on välja töötatud tootjate kogemuste ja teadusuuringute põhjal.
- **Üldine kaitse:** Eelnevalt määratud reeglid pakuvad laiapõhjalist kaitset ja võivad sisaldada reegleid, mis blokeerivad teadaolevaid pahatahtlikke IP-aadresse, kontrollivad teatud protokolle ja piiravad juurdepääsu tundlikele portidele

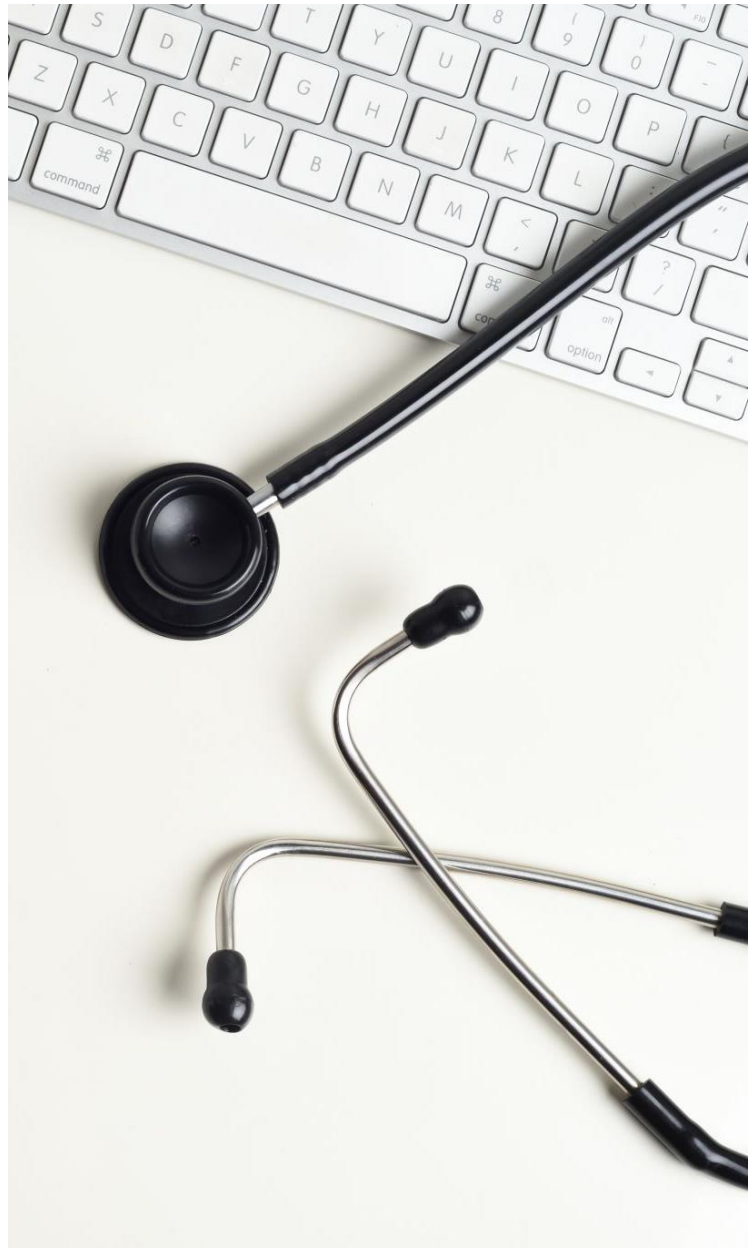
# Baasturvalisus

**Baasturvalisus** viitab süsteemi algsele kaitsetasemele, mida pakutakse eelnevalt määratud reeglite abil. Need reeglid tagavad, et süsteem on kaitstud kohe pärast paigaldamist, enne kui administreerijad saavad kohandatud reeglid rakendada.

EELNEVALT MÄÄRATUD REEGLITE ROLL

Eelnevalt kindlaks määratud reeglid mängivad olulist rolli süsteemi baasturvalisuse tagamisel.

- **Esialgne kaitse:** Pakuvad kohest kaitset ja turvalisust, ilma et oleks vaja keerulist konfiguratsiooni.
- **Minimaalne turvalisustase:** Tagavad, et süsteem vastab vähemalt miinimumtasemele turvanõuetest, kaitstes seda levinud ohtude ja rünnakute eest.
- **Kiire seadistamine:** Võimaldavad süsteemi kiiret kasutuselevõttu, kuna eelnevalt määratud reeglid on juba paigaldatud ja aktiveeritud.
- **Parandused ja uuendused:** Tootjad uuendavad regulaarselt eelnevalt määratud reegleid, et kohaneda uute ohtude ja turvaaukudega.



# Näited eelnevalt kindlaks määratud reeglitest

- NÄIDE 1: TOOTJAPOOLNE REEGEL

1. **Reegel:** Blokeerida kõik sissetulevad ühendused teadaolevatest pahatahtlikest IP-aadressidest.
- **Tüüp:** Deny
- **Lähteaadress:** Musta nimekirja kantud IP-aadressid
- **Sihtaadress:** Kõik
- **Protokoll:** Kõik
- **Port:** Kõik
- **Kirjeldus:** See reegel aitab kaitsta võrku levinud pahatahtlike IP-aadresside eest, mis on teadaolevalt seotud küberrünnakutega.

- NÄIDE 2: BAASTURVALISUSE REEGEL

2. **Reegel:** Lubada ainult HTTPS liiklus (port 443) veebiserverile ja blokeerida kõik muud ühendused.
- **Tüüp:** Allow
- **Lähteaadress:** Kõik
- **Sihtaadress:** Veebiserveri IP
- **Protokoll:** TCP
- **Port:** 443
- **Kirjeldus:** Tagab, et veebiserver saab vastu võtta ainult turvalisi HTTPS ühendusi, vähendades rünnakute pinda.

# Tulemüüri funktsionaalsed põhimõtted

Tulemüürid mängivad olulist rolli võrgu turvalisuse tagamisel ja erinevad funktsionaalsed põhimõtted määravad nende tööviisi ja tõhususe. Allpool on toodud peamised funktsionaalsed põhimõtted, mis hõlmavad staatilist ja dünaamilist filtreerimist, riistvaralisi ja tarkvaralisi tulemüüre, samuti läbilaskevõimet ja jõudlust.

- **STAATILINE JA DÜNAAMILINE FILTREERIMINE**
- Tulemüürid kasutavad liikluse filtreerimiseks kahte põhilist meetodit: staatilist ja dünaamilist filtreerimist. Mõlemal lähenemisel on oma eelised ja puudused ning neid kasutatakse erinevates olukordades.

# Staatiline ja dünaamiline filtreerimine

- STAATILINE FILTREERIMINE
- **Staatiline filtreerimine:** Kasutab eelnevalt määratud reegleid, mida administraator on konfigureerinud. Need reeglid jäävad muutumatuks, kuni neid käsitsi muudetakse.
- **Eelised:** Lihtne seadistada ja hallata, reeglid on selged ja ettearvatavad.
- **Puudused:** Ei kohandu automaatselt muutuvate turvaolukordadega, võib olla vähem tõhus uute ja ootamatute rünnakute vastu.
    - **Näide:** Reegel, mis lubab või blokeerib liikluse kindlatelt IP-aadressidelt ja portidelt, näiteks lubada ainult HTTPS liiklus (port 443).

- DÜNAAMILINE FILTREERIMINE
- **Dünaamiline filtreerimine:** Kohandub liikluse mustrite ja turvaolukorra järgi. Kasutab intelligentseid algoritme ja reaalajas analüüsi, et määrata liikluse lubatavus.
- **Eelised:** Võimaldab kiiret reageerimist muutuvatele turvaohtudele, suudab tuvastada ja blokeerida uusi ründevektoreid.
- **Puudused:** Võib olla keerulisem seadistada ja hallata, nõuab suuremat arvutusvõimsust ja võib põhjustada valepositiivseid tulemusi.
    - **Näide:** IDS/IPS süsteemid, mis analüüsivad reaalajas liiklust ja kohandavad reegleid, et blokeerida kahtlane tegevus.

# Tulemüüride läbilaskevõime ja jõudlus

## LÄBILASKEVÕIME

- **Läbilaskevõime:** Tulemüüri võime käsitleda teatud hulka liiklust ilma märkimisväärsete viivitusteta. Läbilaskevõime mõõdetakse tavaliselt andmemahtudes (Mbps või Gbps), mida tulemüür suudab töödelda.
- **Eelised:** Suur läbilaskevõime võimaldab tulemüüril hallata suurt liiklusmahtu ja tagada võrgu tõrgeteta toimimine.
- **Puudused:** Piiratud läbilaskevõime võib põhjustada kitsaskohti ja viivitusi, eriti kõrge liikluse korral.
  - **Näide:** Tulemüür, mis suudab töödelda 10 Gbps liiklust, sobib suure liiklusmahuga andmekeskustele.

# Tulemüüride läbilaskevõime ja jõudlus

JÕUDLUS

- **Jõudlus:** Mõõdetakse tulemüüri tõhusust ja kiirust liikluse töötlemisel. Jõudlust võivad mõjutada mitmed tegurid, sealhulgas riistvara spetsifikatsioonid, konfigureeritud reeglid ja süsteemi koormus.
- **Eelised:** Kõrge jõudlus tagab kiire ja tõhusa liikluse töötlemise, vähendades viivitusi ja suurendades turvalisust.
- **Puudused:** Madal jõudlus võib põhjustada liikluse aeglustumist ja süsteemi ülekoormust, vähendades turvalisust ja kasutajakogemust.
  - **Näide:** Tulemüür, mis suudab reaalajas töödelda ja analüüsida sadu tuhandeid pakette sekundis.
- .

# V osa

# VLAN-I tehnoloogia põhimõtted ja omadused

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks

# MIS ON VLAN?

VLAN ehk virtuaalne kohalik võrk (Virtual Local Area Network) on tehnoloogia, mis võimaldab jagada füüsilist võrku loogilisteks segmentideks. Iga segment ehk VLAN toimib nagu eraldi füüsiline võrk, kuigi kõik VLAN-id võivad eksisteerida sama füüsilise infrastruktuuri (näiteks samade kommutaatorite ja kaablite) peal. VLAN-ide abil saab võrgu liiklust loogiliselt eraldada ja hallata sõltumata füüsilisest asukohast.

# Vlan-i eesmärk ja eelised

## Turvalisus:

- VLAN-id eraldavad tundlikku liiklust, takistades volitamata juurdepääsu ja vähendades turvariske. Näiteks saab kontoritöötajate ja tootmisseadmete võrgu liikluse eraldada, et tagada kriitiliste süsteemide turvalisus.

## Liiklusjuhtimine:

- VLAN-id aitavad vähendada liiklusummikuid, suunates liikluse konkreetsetesse segmentidesse ja vähendades liikluskoormust kogu võrgus.

## Paindlikkus:

- VLAN-id võimaldavad seadmeid kergesti ümber konfigureerida ja ümber paigutada ilma füüsiliste kaablite muutmiseta. Näiteks saab uusi tööjaamu lisada olemasolevasse VLAN-i lihtsalt tarkvara kaudu.

## Jõudlus:

- Eraldades võrguliikluse VLAN-ideks, vähenevad kollisioonid ja suurendatakse võrgujõudlust.

# Näide:

*VLAN tehnika võimaldab ühel füüsilisel infrastruktuuril moodustada mitmeid loogilisi etherneti segmente, selliste võimalustega:*

- *lokaliseerida liiklust (on vaieldav kas tegu on ranges mõttes turvalisuse instrumendiga, vt nt VLAN Hopping)*
- *lahendada topoloogilisi küsimusi ISO level 2 kihis, st kiht allpool ruuterid*

*VLAN ilises andmevahetuses osalevatel ethernet frame'idel on lisaks juures spetsiaalne VLAN silt (ingl. k. tag), mis sisaldab andmeid selle kohta, millisesse VLANi frame kuulub. VLAN siltide abil saavad võrgus osalevad seadmed kontrollida kõnealuse frame'i liikumist. Kasutaja jaoks esinevad VLAN sildid positiivsete täisarvude kujul, mida nimetatakse VLAN ID'deks.*

# Näide:

*Tavaliselt kõneldaks VLAN võimest seoses switchidega, kahes tähenduses*

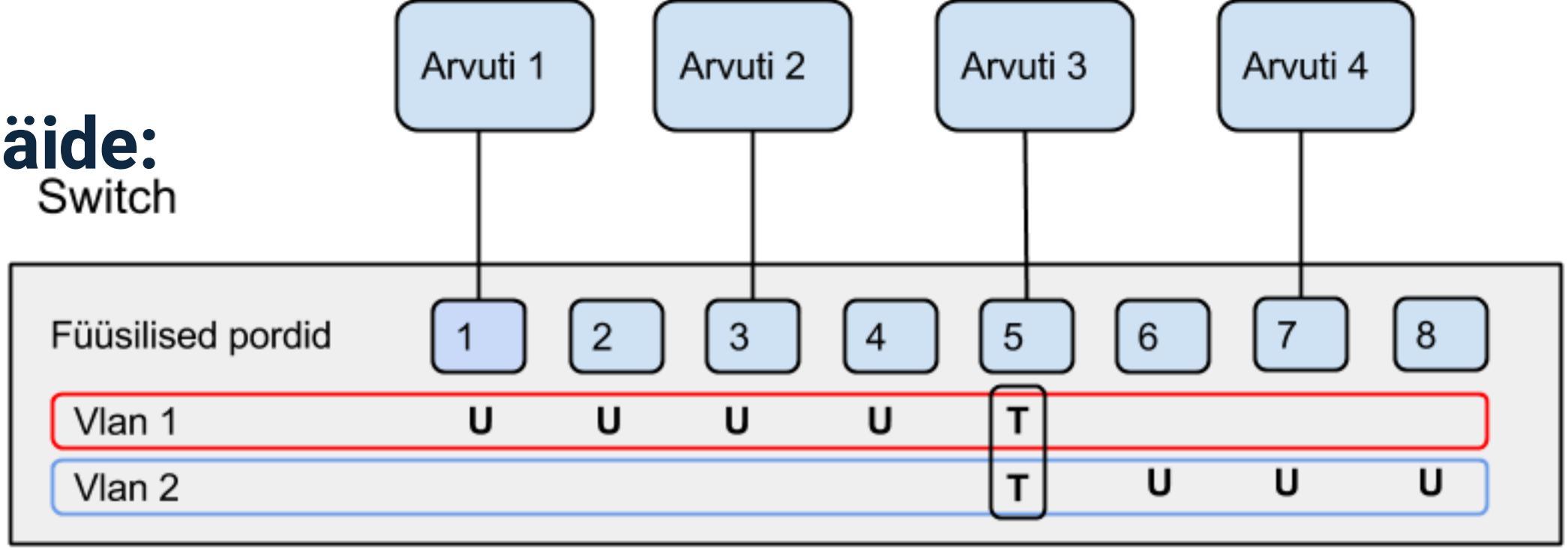
- *mode access - füüsilise switchi igale pordile on öeldud, millisesse VLANi ta kuulub ning ühendades selliselt seadistatud switchi portidesse arvutid nö näevad üksteist ethernetis ainult samasse VLANi kuuluvad arvutid.*
- *mode trunk - selleks, et mode access režiimis saaks kasutada sama VLANi nii, et see ulatub üle mitme switchi peab olema VLAN siltidega frame'idel võimalus liikuda switchide vahel nii, et need märgid säilivad.*

# Näide:

*Mode access või mode trunk režiimis olek on üksiku pordi mitte switchi omadus.*

- *Switchis ehk kommutaatoris on igal vlani paigutatud pordil kaks asendit taged ja untaged ehk märgitud ja mittemärgitu.*
- *Switchi(kommutaatori) poolselt näeb asi välja selline, et tekitatakse kaks Vlani. Sageli on esimene default vlan juba isegi olemas ja kõik pordid on sinna sisse untaged. Kui nüüd tekitada uus vlan ja lisada poole kommutaatori pordid sinna ümber ja untagida tekib meil virtuaalselt kaks teineteisest eraldatud kommutaatorit-võrku mis omavahel suhelda ei saa.*

# Näide:
Switch



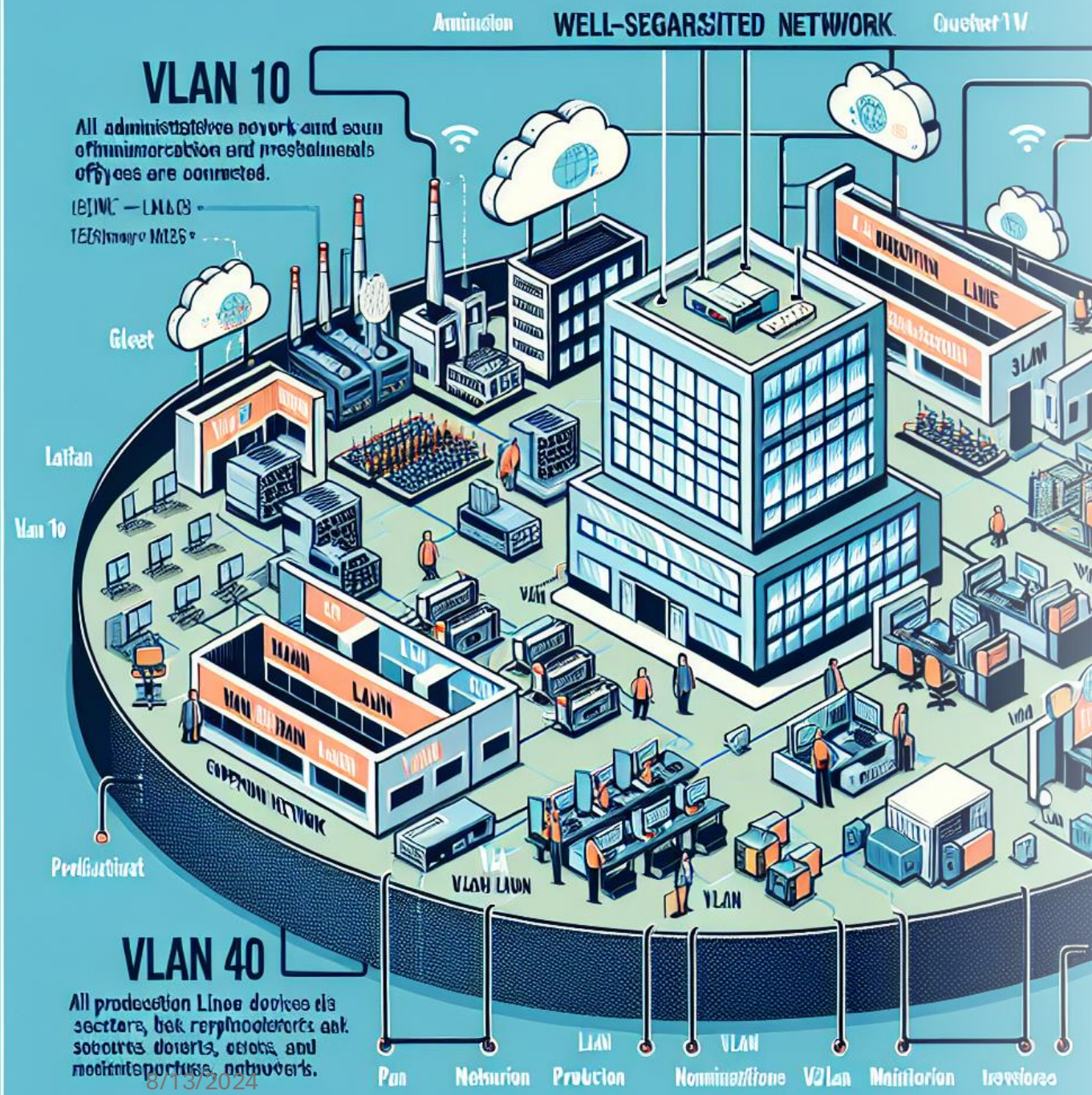

- *Juhul kui aga tahame, et üks kommutaatori port oleks nii vlanis 1 kui ka vlanis 2 tuleb see port tagida ehk märkida. Samuti tuleb vlani tagid lisada võrguseadmele Linuxi/Unixi poolselt siis eraldab juba võrgukaart tagide kaudu neid võrke edasi.*
- *Tagimine ehk märkimine toimub IEEE 802.1q standardi alusel, mille käigus lisatakse tagitavatele pakettidele lisainfot. Hiljem see info eemaldatakse võrgukaardi poolt.*

*Ülaloleval skeemil on pordid 1-4 untagitud vlani 1 ja 6-7 vlani 2. Port viis on aga tagitud mõlemasse vlani ning saab ligipääsu kõigile seal portidesse ühendatud seadmetele. Täpsemalt siis*
*•Arvuti üks omab ligipääsu masinale arvuti2 ja arvuti3 aga mitte masinale arvuti4.*
*•Arvuti4 pääseb ligi masinale arvuti3 aga mitte masinatele arvuti1 ja arvuti2.*
*•Arvuti3 pääseb ligi kõigile kolmele masinale.*
*Seejuures ei vaja arvutid 1, 2 ja 4 mitte mingit täiendavat võrguseadistust. Küll aga vajab seda arvuti3, kuhu on vaja tekitada samuti vlani seadistused*

# Kuidas VLAN-e kasutatakse tööstuses ja tootmises?

- Tööstuslikus keskkonnas kasutatakse VLAN-e mitmete oluliste ülesannete täitmiseks:

1. **Tootmisliinide segmentimine**:
    1. Tootmisettevõtetes on sageli vaja eraldada erinevate tootmisliinide ja masinate võrguliiklus. VLAN-id võimaldavad iga tootmisliini või osakonna jaoks eraldi võrgu, mis tagab stabiilse ja turvalise andmeedastuse.
2. **Kriitiliste süsteemide Kaitse**:
    1. Kriitilisi juhtimissüsteeme, nagu SCADA (Supervisory Control and Data Acquisition) ja PLC (Programmable Logic Controller) süsteemid, kaitstakse, eraldades nende võrguliikluse muudest võrgusegmentidest. See vähendab riski, et volitamata isikud pääsevad juurde tundlikule andmevoole.
3. **Külalisvõrgud ja kaugühendused**:
    1. Tööstusettevõtted võivad luua VLAN-e külalisvõrkude jaoks, kus ajutised töötajad või tarnijad saavad ligipääsu ilma, et see mõjutaks peavõrku. See tagab, et külaliste tegevus ei häiri tootmisvõrgu toimimist.
4. **Tootmisandmete kogumine ja jälgimine**:
    1. VLAN-id võimaldavad tõhusat andmete kogumist ja jälgimist erinevatest tootmisüksustest. Näiteks saab andureid ja jälgimisseadmeid ühendada spetsiaalsetesse VLAN-idesse, et kogutud andmed oleksid eraldatud ja turvaliselt hallatud.




# Näide VLAN-i kasutamisest tööstuskeskkonnas

KUJUTAGE ETTE TEHAST, KUS KASUTATAKSE VLAN-E JÄRGMISELT:

1. **VLAN 10: Administratiivvõrk**
    1. Kõik kontoritöötajad ja administratiivsed seadmed on ühendatud VLAN 10-sse. See hõlmab arvuteid, printereid ja muid kontoriseadmeid.
2. **VLAN 20: Tootmisliini võrk**
    1. Kõik tootmisliiniga seotud seadmed, nagu PLC-d, andurid ja robottöötajad, on ühendatud VLAN 20-sse. See eraldab tootmisliini liikluse kontorivõrgust, tagades stabiilse ja kiire andmevahetuse.
3. **VLAN 30: Külalisvõrk**
    1. Külalistele, tarnijatele ja ajutistele töötajatele luuakse VLAN 30, mis võimaldab neil ligipääsu Internetile ja teatud ressurssidele, kuid mitte tootmis- või administratiivvõrkudele.
4. **VLAN 40: Jälgimis- ja Kontrollvõrk**
    1. Turvakaamerad, jälgimisseadmed ja muud turvasüsteemid on ühendatud VLAN 40-sse. See tagab, et turvaseadmete andmed on eraldatud ja turvaliselt hallatud.

# VLAN-ide konfigureerimine

VLAN-ide seadistamine ja haldamine hõlmab mitmeid samme, sealhulgas:

**1. VLAN-ide Määramine**:

1. VLAN-id määratakse kommutaatoritele (switch) ja ruuteritele (router), kasutades nende haldustarkvara. Igal VLAN-il on unikaalne identifikaator (ID), mida kasutatakse liikluse eraldamiseks.

**2. Pordide Konfigureerimine**:

1. kommutaatori portide seadistamine VLAN-idesse. Näiteks võib port 1-10 kuuluda VLAN 10-sse, port 11-20 VLAN 20-sse jne.

**3. VLAN-i Liiklust Labeldamine (Tagging)**:

1. IEEE 802.1Q standardi järgi märgistatakse VLAN liiklus, et kommutaatorid ja ruuterid teaksid, millisele VLAN-ile konkreetne pakett kuulub.

**4. Trunk-portide Kasutamine**:

1. Trunk-pordid kannavad liiklust mitmest VLAN-ist ja neid kasutatakse kommutaatorite ja ruuterite vaheliseks ühendamiseks, võimaldades mitme VLAN-i liiklust ühe kaabli kaudu.

# VLAN-I TEHNOLOOGIA ALUSMEHHANISM

- VLAN-i tehnoloogia võimaldab võrkude loogilist segmentimist, eraldades võrgusegmendid loogiliselt, sõltumata nende füüsilisest paigutusest. See suurendab võrgu turvalisust ja tõhusust, võimaldades paremat haldamist ja liikluse suunamist.
- VLAN-id kasutavad sildamist ja marsruutimist liikluse eraldamiseks ja suunamiseks, pakkudes suuremat kontrolli ja paindlikkust võrgu arhitektuuris.

# Loogiline segmentimine

VIRTUAALSED KOHALIKUD VÕRGUD (VLAN-ID)

**Virtuaalsed kohalikud võrgud (VLAN-id)** on loogilised võrgusegmendid, mis eraldavad erinevad seadmed ja liikluse ühes füüsilises võrgus. VLAN-id võimaldavad hallata ja turvata võrku, jagades selle väiksemateks segmentideks.

- **Kasutusjuhud:** Võimaldavad eri osakondade, meeskondade või projektide liikluse eraldamist samas füüsilises võrgus.
    - **Näide:** Suures ettevõttes on erinevatel osakondadel, nagu turundus, IT ja finants, oma VLAN-id, mis tagavad, et nende liiklus on eraldatud ja turvaline.

VLAN-I KONFIGURATSIOON

**Pordi põhine VLAN:** Iga kommutaatori port on konfigureeritud kuuluma kindlasse VLAN-i.

- **Näide:** kommutaatori port 1-10 kuuluvad VLAN 10 (turundus), port 11-20 kuuluvad VLAN 20 (IT), port 21-30 kuuluvad VLAN 30 (finants).

**Tagimine (Tagging):** VLAN-i identifikaatori (VID) lisamine andmepaketi päisesse (IEEE 802.1Q standard), mis võimaldab VLAN-ide andmepakettide liikumist üle mitme kommutaatori ja ruuteri.

- **Näide:** Andmepakett, mis liigub VLAN 10 sees, on märgistatud VLAN 10 ID-ga, tagades, et see jääb samasse VLAN-i ka üle mitme kommutaatori liikudes.

# Sildamine ja marsruutimine

SILDAMINE (BRIDGING)

**Sildamine** võimaldab VLAN-i liiklusel liikuda sama VLAN-i sees ilma vajaduseta marsruutimise järele. Sildamine toimub kommutaatori tasandil ja tagab, et andmepaketid liiguvad VLAN-i sees kiiresti ja tõhusalt.

- **L2 sildamine:** kommutaatori kontrollib MAC-aadresside tabelit, et suunata liiklus õigele pordile sama VLAN-i sees.
    - **Näide:** Arvuti A (MAC 00:11:22:33:44:55) VLAN 10-s saadab andmepaketi arvutile B (MAC 00:66:77:88:99:AA) VLAN 10-s. kommutaatori kontrollib MAC-aadresside tabelit ja suunab paketi õigele pordile VLAN 10 sees

MARSRUUTIMINE (ROUTING)

**Marsruutimine** võimaldab liikluse suunamist erinevate VLAN-ide vahel. See toimub L3 kommutaatorite või ruuterite abil, mis suudavad teha otsuseid IP-aadresside alusel.

- **L3 marsruutimine:** Ruuter või L3 kommutaatori kontrollib IP-aadresside tabelit, et suunata liiklus erinevate VLAN-ide vahel.
    - **Näide:** Arvuti A VLAN 10-s (IP 192.168.10.2) saadab andmepaketi arvutile C VLAN 20-s (IP 192.168.20.2). Ruuter kontrollib IP-aadresside tabelit ja suunab paketi VLAN 20-le.

# Näide VLAN-i kasutamisest ettevõtte võrgus

**Ettevõtte Võrgustruktuur:**

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24, kommutaatori port 1-10
- **IT VLAN 20:** IP vahemik 192.168.20.0/24, kommutaatori port 11-20
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24, kommutaatori port 21-30

**Liikluse Suunamine:**

- **Sildamine VLAN-i Sees:** Turundus VLAN 10 sees liigub liiklus otse läbi L2 sildamise, näiteks arvuti A saadab paketi arvutile B, mis on sama VLAN-i sees.
- **Marsruutimine VLAN-ide Vahel:** IT VLAN 20 liiklus suunatakse finants VLAN 30-le läbi L3 marsruutimise, näiteks arvuti C (VLAN 20) saadab paketi serverile D (VLAN 30).

# VÕRGU ERALDAMISE KAITSEMEEDE

VLAN-id on tõhusad vahendid võrgu segmentimiseks, mis suurendab turvalisust ja jõudlust. Eraldades võrguliiklust, piiravad VLAN-id potentsiaalseid turvariske ja optimeerivad võrguressursside kasutamist. Allpool on põhjalik ülevaade VLAN-ide kasutamise eelistest turvalisuse ja jõudluse seisukohalt.

# Turvalisus ja jõudlus

**ERALDAB LIIKLUST**

**VLAN-id piiravad liikluse levikut ja vähendavad turvariske**. VLAN-id loovad eraldatud võrgusegmendid, mis tagavad, et andmed liiguvad ainult määratud segmentides ja ei saa suvaliselt levida üle kogu võrgu.

- **Liikluse eraldamine:** VLAN-id jagavad võrgu väiksemateks osadeks, kus iga osa võib sisaldada konkreetseid seadmeid ja kasutajaid. See eraldab tundliku teabe ja kriitilised süsteemid muudest võrgusegmentidest.
    - **Näide:** Ettevõtte võrgus on eraldatud VLAN-id, nagu turundus, IT ja finants. Iga VLAN sisaldab ainult vastavate osakondade seadmeid, tagades, et finantsandmed ei ole kättesaadavad turundusosakonna seadmetele.
- **Turvariskide vähendamine:** VLAN-id aitavad piirata ründajate liikumisvõimalusi võrgu sees. Kui ründaja saab juurdepääsu ühele VLAN-ile, ei tähenda see, et tal on automaatne juurdepääs teistele VLAN-idele.
    - **Näide:** Kui ründaja saab ligipääsu turundusosakonna VLAN-ile, jäävad IT- ja finantsosakonna VLAN-id turvaliseks ja ründaja ei pääse neile ligi ilma täiendavate turvameetmete rikkumiseta.

# Turvalisus ja jõudlus

**PARANDAB JÕUDLUST**

**VLAN-id vähendavad ülekoormust ja optimeerivad võrguliiklust**. Loogiline segmentimine aitab paremini hallata ja optimeerida võrguressursside kasutamist, mis omakorda suurendab võrgu üldist jõudlust.

- **Vähendatud ülekoormus:** VLAN-id piiravad ülekandevõimekuse kasutamist, vähendades vajadust kogu võrgu kaudu liikluse edastamiseks. See vähendab võrguliikluse ülekoormust ja suurendab töökindlust.
  - **Näide:** Kui kogu ettevõtte võrk oleks ühes VLAN-is, saaks kõikide osakondade liiklus liigelda läbi kogu võrgu, põhjustades suurema liikluskoormuse. VLAN-ide kasutamine jagab liikluse väiksemateks, hallatavateks osadeks.
- **Optimeeritud võrguliiklus:** VLAN-id suunavad liikluse optimaalselt, tagades, et andmed liiguvad ainult vajalike sihtkohtadeni. See optimeerib võrguressursside kasutamist ja vähendab tarbetut liiklust.
  - **Näide:** Turundusosakonna seadmete vaheline liiklus liigub ainult VLAN 10 sees, ilma et see mõjutaks IT- või finantsosakonna võrgu segmente.

# Näide VLAN-ide kasutamisest ettevõtte võrgus

### Ettevõtte Võrgustruktuur:

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24, kommutaatori port 1-10
- **IT VLAN 20:** IP vahemik 192.168.20.0/24, kommutaatori port 11-20
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24, kommutaatori port 21-30

### Turvalisuse Näide:

- **Turundus VLAN 10:** Kõik turundusosakonna seadmed asuvad VLAN 10-s. Kui seadmel tekib turvarikkumine, jäävad IT ja finants VLAN-id puutumata.
- **IT VLAN 20:** IT-osakond hoiab kriitilisi süsteeme ja servereid VLAN 20-s, mis on eraldatud muudest VLAN-idest, vähendades riske.

### Jõudluse Näide:

- **Turundus VLAN 10:** Turundusosakonna seadmete vaheline liiklus liigub ainult VLAN 10 sees, vähendades ülekoormust ja optimeerides liiklust.
- **Finants VLAN 30:** Finantsosakonna seadmete vaheline liiklus on optimeeritud VLAN 30 sees, tagades, et finantsandmed liiguvad tõhusalt ja turvaliselt.

# VLAN-i identifikaatori kodeerimine

- VLAN-i identifikaatori kodeerimine on oluline aspekt VLAN-i tehnoloogias, mis võimaldab andmepakettide liikumist määratud VLAN-ide sees. VLAN-i identifikaator (VID) on unikaalne number, mis määrab, millisesse VLAN-i andmepakett kuulub. Tagimine (tagging) on protsess, mille käigus lisatakse andmepaketi päisesse VLAN-i identifikaator, kasutades IEEE 802.1Q standardit. Allpool on põhjalik ülevaade VLAN-i identifikaatori kodeerimisest ja tagimise protsessist.

# VID (VLAN Identifier)

**UNIKAALNE IDENTIFIKAATOR**

**VLAN Identifier (VID)** on unikaalne number, mis määrab, millisesse VLAN-i andmepakett kuulub. Igal VLAN-il on oma unikaalne identifikaator, mis eristab seda teistest VLAN-idest samas füüsilises võrgus.

- **VID vahemik:** IEEE 802.1Q standard määrab VLAN-ID vahemikuks 0 kuni 4095. Praktikas kasutatakse VID-e vahemikus 1 kuni 4094, kus 0 ja 4095 on reserveeritud spetsiaalseteks eesmärkideks.
  - **Näide:** Turundus VLAN võib olla määratud VID-iga 10, IT VLAN VID-iga 20 ja finants VLAN VID-iga 30.
- **Kasutusjuhud:** VID võimaldab võrguseadmetel, nagu kommutaatorid ja ruuterid, eristada liiklust erinevate VLAN-ide vahel ja suunata see õigesti määratud sihtkohtadele.
  - **Näide:** Kui kommutaatori saab andmepaketi VID-iga 10, teab see, et pakett kuulub turundus VLAN-ile ja suunab selle vastavalt.

# Tagimine (TAGGING)

**VLAN-I IDENTIFIKAATORI LISAMINE ANDMEPAKETI PÄISESSE**

**Tagimine (Tagging)** on protsess, mille käigus lisatakse andmepaketi päisesse VLAN-i identifikaator (VID), kasutades IEEE 802.1Q standardit. See tagab, et andmepakett jääb samasse VLAN-i ka siis, kui see liigub läbi mitme kommutaatori või ruuteri.

- **IEEE 802.1Q standard:** See standard määrab VLAN-tagimise protsessi, lisades 4-baidise sildi (tag) andmepaketi päisesse. Silt sisaldab VLAN-i identifikaatorit (VID), prioriteedi informatsiooni ja muid olulisi parameetreid.
  - **Näide:** Andmepakett, mis liigub VLAN 10 sees, saab 802.1Q sildi, mis sisaldab VID 10 ja muid vajalikke parameetreid.
- **Tagitud ja mittetagitud liiklus:** VLAN-id toetavad nii tagitud kui ka mittetagitud liiklust. Mittetagitud liiklus kuulub tavaliselt vaikimisi VLAN-i (native VLAN), samas kui tagitud liiklus sisaldab VLAN-i identifikaatorit.
  - **Näide:** kommutaatoril võib port 1 kuuluda vaikimisi VLAN 1-le (mittetagitud liiklus), samas kui port 2 kasutab VLAN 10 (tagitud liiklus).

# Näide VLAN-I Identifikaatori kodeerimisest ja tagimisest

**Ettevõtte Võrgustruktuur:**

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24, VID 10
- **IT VLAN 20:** IP vahemik 192.168.20.0/24, VID 20
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24, VID 30

**Tagimise Näide:**

- **Andmepaketi liikumine:** Arvuti A (VID 10) turundus VLAN-is saadab andmepaketi kommutaatori kaudu arvutile B (VID 10). Andmepakett saab sildi, mis sisaldab VID 10, tagades, et pakett liigub ainult VLAN 10 sees.
- **802.1Q silt:** Andmepaketi päisesse lisatakse 4-baidine 802.1Q silt, mis sisaldab VID 10 ja muid vajalikke parameetreid. Kui pakett jõuab sihtkommutaatorile, eemaldatakse silt ja pakett suunatakse õigesse porti

# Pordi VID

- VLAN-ide konfiguratsioonis on oluline mõista, kuidas pordid on määratud erinevatele VLAN-idele. Pordi VLAN ID (PVID) määrab, millisesse VLAN-i port vaikimisi kuulub. PVID määramine ja haldamine on oluline osa VLAN-ide seadistamisest ja võrgu liikluse eraldamisest.

# PVID (PORT VLAN ID)

**VAIKIMISI VLAN**

**PVID (Port VLAN ID)** on identifikaator, mis määrab, millisesse VLAN-i port vaikimisi kuulub. PVID määrab, kuidas kommutaatori käsitleb sissetulevat liiklust konkreetsel pordil, kui liiklus ei ole märgistatud (untagged).

- **Vaikimisi VLAN:** Kui porti siseneb mittetagitud liiklus, määratakse sellele liiklusele PVID-i põhjal vastav VLAN. See tagab, et kõik seadmed, mis ei toeta VLAN-tagimist, saavad ikkagi õigesse VLAN-i määratud.
  - **Näide:** Kui PVID on määratud 10-ks, siis kõik mittetagitud pakettid, mis sisenevad sellesse porti, määratakse VLAN 10-le.

# VID (VLAN Identifier)

**PORDI SEADISTAMINE**

**Pordi seadistamine:** PVID määramine ja haldamine on oluline osa kommutaatori konfiguratsioonist. See võimaldab võrguadministraatoritel kontrollida, kuidas liiklus liigub läbi võrgu ja kuidas see on eraldatud erinevatesse VLAN-idesse.

- **PVID määramine:** Iga kommutaatori porti saab määrata PVID, mis määrab, millisesse VLAN-i mittetagitud liiklus kuulub.
  - **Näide:** kommutaatori port 1 võib olla määratud PVID 10-ks, mis tähendab, et kõik mittetagitud pakettid, mis sisenevad porti 1, kuuluvad VLAN 10-le.
- **PVID halduse tööriistad:** Kaasaegsed kommutaatorid võimaldavad administraatoritel konfigureerida PVID-i käsurealiidese (CLI), veebipõhise graafilise kasutajaliidese (GUI) või võrgu haldusprotokollide (nt SNMP) kaudu.
  - **Näide:** Administraator võib kasutada CLI-d, et määrata kommutaatori port 2 PVID 20-ks järgmise käsuga:
    plaintext switchport access vlan 20
- **PVID ja tagitud liiklus:** Kuigi PVID määrab, millisesse VLAN-i mittetagitud liiklus kuulub, võivad pordid ka käsitleda tagitud liiklust. See tähendab, et port võib samaaegselt käsitleda mitut VLAN-i liiklust, sõltuvalt pakettide siltidest.
  - **Näide:** Port võib olla määratud PVID 10-ks (vaikimisi VLAN), kuid see võib ka käsitleda tagitud liiklust VLAN 20 ja VLAN 30 jaoks.

# Näide PVID-I kasutamisest ettevõtte võrgus

**Ettevõtte võrgustruktuur:**

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24, PVID 10
- **IT VLAN 20:** IP vahemik 192.168.20.0/24, PVID 20
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24, PVID 30

**Pordi seadistamise näide:**

- **Port 1 (Turundus VLAN 10):** PVID määratud 10-ks. Kõik mittetagitud liiklus, mis sisenevad porti 1, määratakse VLAN 10-le.
- **Port 2 (IT VLAN 20):** PVID määratud 20-ks. Kõik mittetagatud liiklus, mis sisenevad porti 2, määratakse VLAN 20-le.
- **Port 3 (Trunk Port):** PVID määratud 30-ks, kuid see port käsitleb ka tagitud liiklust VLAN 10 ja VLAN 20 jaoks. Mittetagatud liiklus määratakse VLAN 30-le.

**Konfiguratsioon:**

```
interface ethernet 1
switchport access vlan 10

interface ethernet 2
switchport access vlan 20

interface ethernet 3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport access vlan 30
```

https://ikt.tthk.ee/vlan-i-tehnoloogia-pohimotted-ja-omadused-2/#CLI

# Staatilised ja õpitud VID-id

VLAN-i konfigureerimine hõlmab staatiliste ja õpitud VID-ide kasutamist. Staatilised VID-id on administraatori poolt käsitsi määratud, samas kui õpitud VID-id on dünaamiliselt määratud seadmete poolt, kasutades liikluse analüüsi ja protokolle, nagu GVRP (GARP VLAN Registration Protocol).

# Loogiline segmentimine

VIRTUAALSED KOHALIKUD VÕRGUD (VLAN-ID)

**Virtuaalsed kohalikud võrgud (VLAN-id)** on loogilised võrgusegmendid, mis eraldavad erinevad seadmed ja liikluse ühes füüsilises võrgus. VLAN-id võimaldavad hallata ja turvata võrku, jagades selle väiksemateks segmentideks.

- **Kasutusjuhud:** Võimaldavad eri osakondade, meeskondade või projektide liikluse eraldamist samas füüsilises võrgus.
    - **Näide:** Suures ettevõttes on erinevatel osakondadel, nagu turundus, IT ja finants, oma VLAN-id, mis tagavad, et nende liiklus on eraldatud ja turvaline.

VLAN-I KONFIGURATSIOON

**Pordi põhine VLAN:** Iga kommutaatori port on konfigureeritud kuuluma kindlasse VLAN-i.

- **Näide:** kommutaatori port 1-10 kuuluvad VLAN 10 (turundus), port 11-20 kuuluvad VLAN 20 (IT), port 21-30 kuuluvad VLAN 30 (finants).

**Tagimine (Tagging):** VLAN-i identifikaatori (VID) lisamine andmepaketi päisesse (IEEE 802.1Q standard), mis võimaldab VLAN-ide andmepakettide liikumist üle mitme kommutaatori ja ruuteri.

- **Näide:** Andmepakett, mis liigub VLAN 10 sees, on märgistatud VLAN 10 ID-ga, tagades, et see jääb samasse VLAN-i ka üle mitme kommutaatori liikudes.

# Sildamine ja marsruutimine

SILDAMINE (BRIDGING)

**Sildamine** võimaldab VLAN-i liiklusel liikuda sama VLAN-i sees ilma vajaduseta marsruutimise järele. Sildamine toimub kommutaatori tasandil ja tagab, et andmepaketid liiguvad VLAN-i sees kiiresti ja tõhusalt.

- **L2 sildamine:** kommutaatori kontrollib MAC-aadresside tabelit, et suunata liiklus õigele pordile sama VLAN-i sees.
    - **Näide:** Arvuti A (MAC 00:11:22:33:44:55) VLAN 10-s saadab andmepaketi arvutile B (MAC 00:66:77:88:99:AA) VLAN 10-s. kommutaatori kontrollib MAC-aadresside tabelit ja suunab paketi õigele pordile VLAN 10 sees

MARSRUUTIMINE (ROUTING)

**Marsruutimine** võimaldab liikluse suunamist erinevate VLAN-ide vahel. See toimub L3 kommutaatorite või ruuterite abil, mis suudavad teha otsuseid IP-aadresside alusel.

- **L3 marsruutimine:** Ruuter või L3 kommutaatori kontrollib IP-aadresside tabelit, et suunata liiklus erinevate VLAN-ide vahel.
    - **Näide:** Arvuti A VLAN 10-s (IP 192.168.10.2) saadab andmepaketi arvutile C VLAN 20-s (IP 192.168.20.2). Ruuter kontrollib IP-aadresside tabelit ja suunab paketi VLAN 20-le.

# Näide staatiliste ja õpitud VID-ide kasutamisest ettevõtte võrgus

**Ettevõtte võrgustruktuur:**

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24, staatiline VID 10
- **IT VLAN 20:** IP vahemik 192.168.20.0/24, staatiline VID 20
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24, staatiline VID 30

**Staatiliste VID-ide näide**

- **Port 1 (Turundus VLAN 10):** Administraator määrab port 1-le käsitsi VID 10, tagades, et kõik ühendused selle pordi kaudu kuuluvad turundus VLAN-i.
- **Port 2 (IT VLAN 20):** Administraator määrab port 2-le käsitsi VID 20, tagades, et kõik ühendused selle pordi kaudu kuuluvad IT VLAN-i.

**Õpitud VID-ide näide**

- **Uue seadme ühendamine:** Uus seade ühendub porti 4, mis ei ole staatiliselt konfigureeritud. kommutaatori kasutab GVRP-d, et määrata seadmele dünaamiliselt sobiv VID, vastavalt võrgu konfiguratsioonile ja liiklusele.
- **GVRP päring ja vastus:** Seade saadab GVRP päringu ja kommutaatori määrab seadmele dünaamiliselt VID 10, kuna see kuulub turundus VLAN-i.

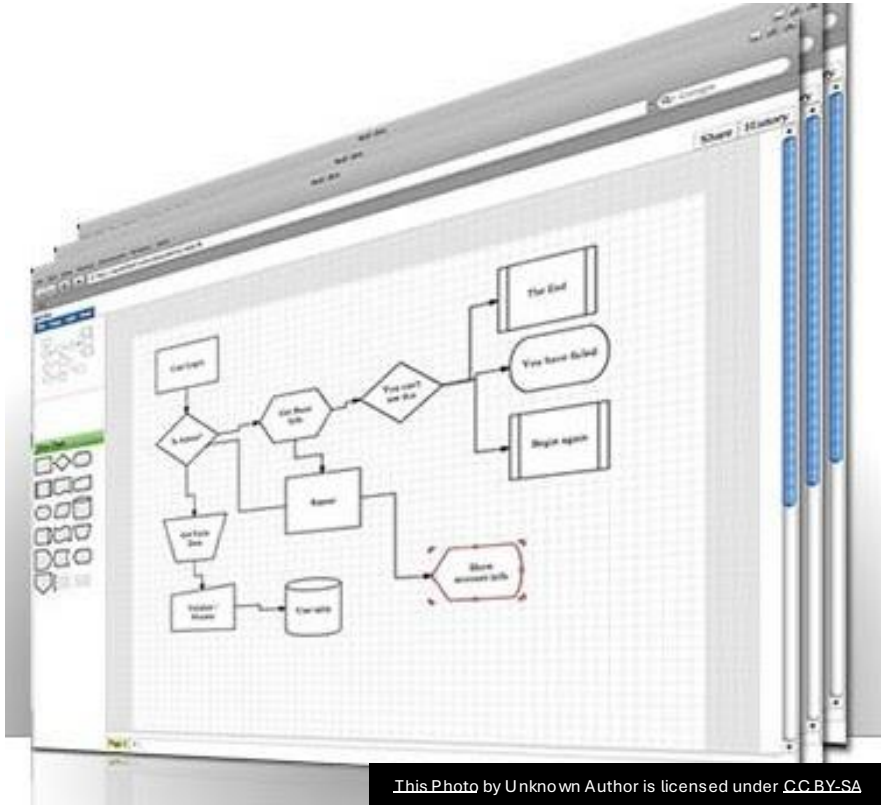
https://ikt.tthk.ee/vlan-i-tehnoloogia-pohimotted-ja-omadused-2/#CLI

# VLAN-ide graafiline kujutamine

- VLAN-ide graafiline kujutamine on oluline, et mõista võrgu struktuuri ja ühendusi visuaalselt. Diagrammid ja võrgukaardid aitavad võrguadministraatoritel ja inseneridel paremini planeerida, hallata ja tõrkeotsingut teha. Allpool on üksikasjalik ülevaade VLAN-ide graafilisest kujutamisest ja tööriistadest, mida saab selleks kasutada

# Diagrammid ja võrkude kaardid

- GRAAFILINE ESITAMINE
- **Graafiline esitamine** võimaldab võrgu struktuuri ja ühendusi visualiseerida, muutes keerulised võrgutopoloogiad hõlpsamini arusaadavaks. Diagrammid ja võrgukaardid võivad näidata erinevate VLAN-ide ühendusi, seadmeid ja nende vahelisi linke.
- **Topoloogia diagrammid:** Need näitavad võrgu struktuuri, sealhulgas lüliteid, ruutereid, servereid ja muid võrgu komponente, samuti nendevahelisi ühendusi.
  - **Näide:** Diagramm, mis näitab, kuidas turundus VLAN 10 on ühendatud erinevate kommutaatorite ja ruuteritega, samuti selle ühendust IT VLAN 20 ja finants VLAN 30-ga.
- **VLAN-i ühendused:** Diagrammid, mis näitavad, kuidas erinevad VLAN-id on ühendatud ja kuidas liiklus liigub nende vahel.
  - **Näide:** Diagramm, mis näitab, kuidas VLAN 10 ja VLAN 20 vaheline liiklus suunatakse läbi L3 ruuteri.



**Microsoft Visio**: Võimas tööriist, mis võimaldab luua üksikasjalikke võrgudiagramme ja topoloogia kaarte.

- **Eelised**: Lai valik kujundeid ja šabloone, mis on spetsiaalselt loodud võrkude ja IT-infrastruktuuride jaoks.
- **Link**: Microsoft Visio

**Lucidchart**: Veebipõhine diagrammitööriist, mis võimaldab koostööd ja jagamist reaalajas.

- **Eelised**: Lihtne kasutada, koostöövõimalused, integratsioonid teiste tööriistadega nagu Google Drive ja Confluence.
- **Link**: Lucidchart

**Draw.io**: Tasuta ja avatud lähtekoodiga diagrammitööriist, mis pakub laia valikut funktsioone ja šabloone võrgudiagrammide loomiseks.

- **Eelised**: Tasuta kasutamine, lihtne liides, integratsioonid mitme platvormiga.
- **Link**: Draw.io

**Ettevõtte võrgustruktuur:**

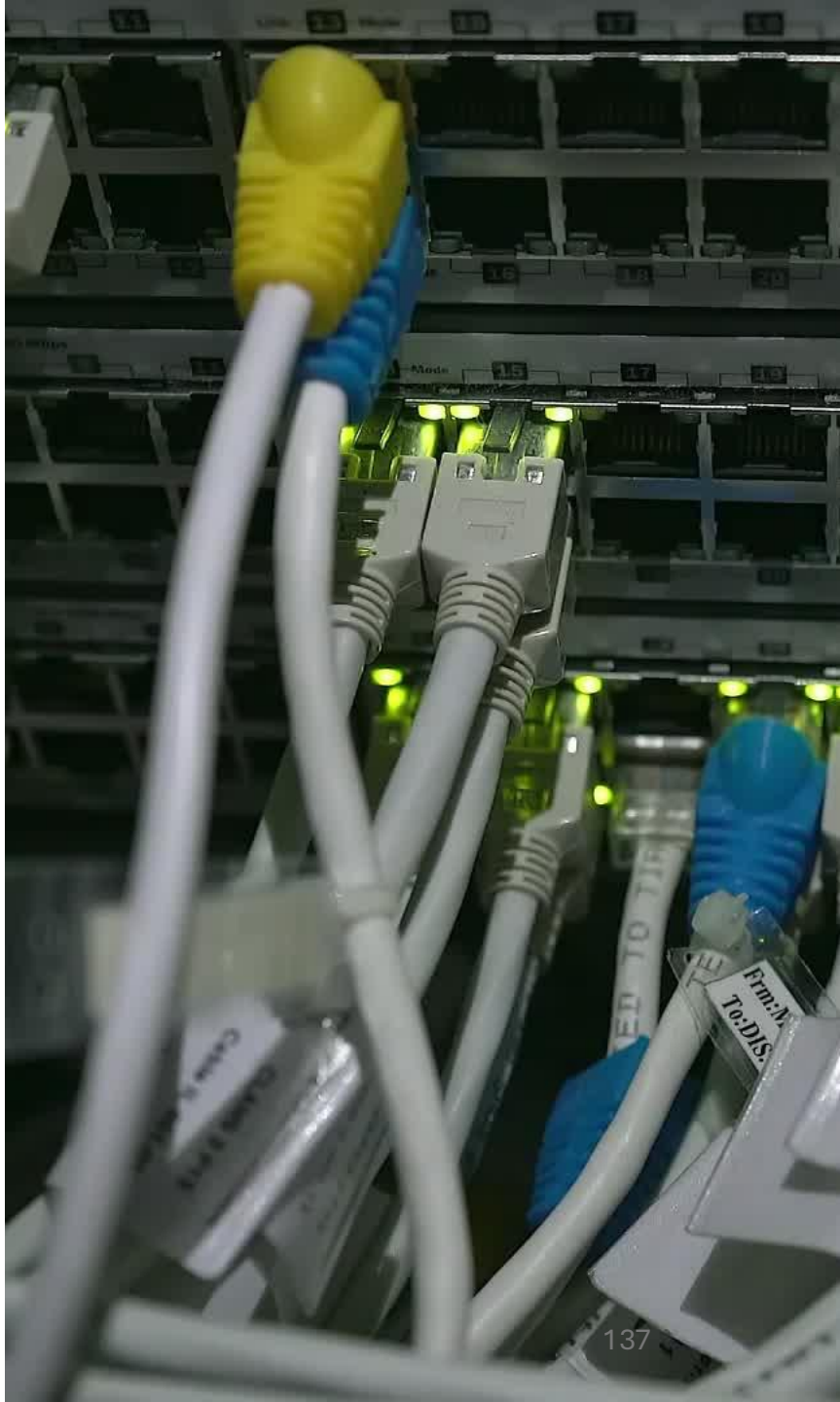
- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24
- **IT VLAN 20:** IP vahemik 192.168.20.0/24
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24
- **VLAN-ide diagrammi näide Microsoft Visio-s:**

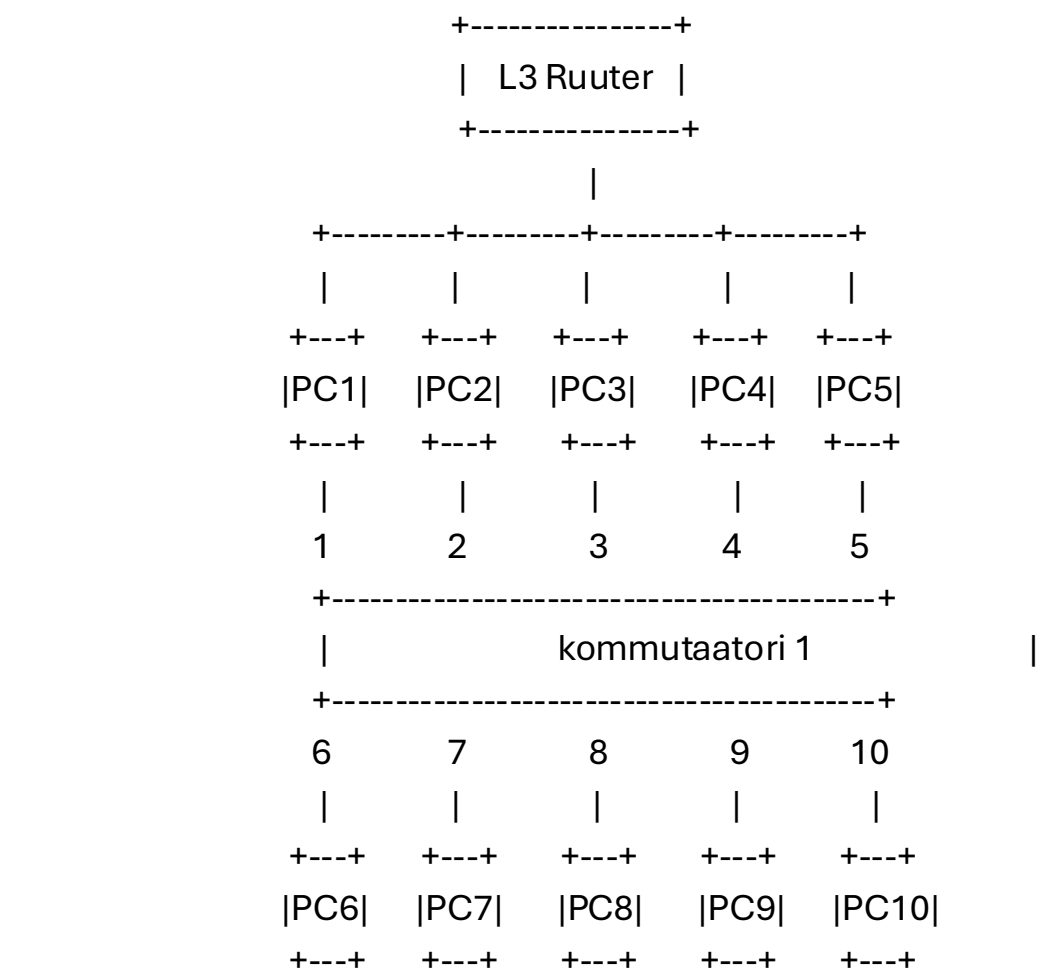
**kommutaatorid ja Ruuterid:**

- kommutaatori 1: Port 1-10 (VLAN 10), Port 11-20 (VLAN 20), Port 21-30 (VLAN 30)
- L3 Ruuter: Ühendab VLAN 10, VLAN 20 ja VLAN 30

**VLAN-ide Ühendused:**

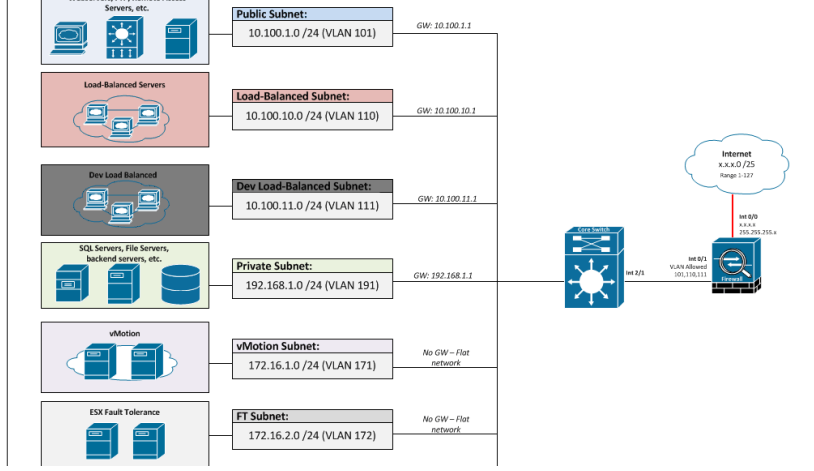
- Turundus VLAN 10 on ühendatud kommutaatori 1 portidega 1-10.
- IT VLAN 20 on ühendatud kommutaatori 1 portidega 11-20.
- Finants VLAN 30 on ühendatud kommutaatori 1 portidega 21-30.
- L3 Ruuter suunab liiklust VLAN 10, VLAN 20 ja VLAN 30 vahel.

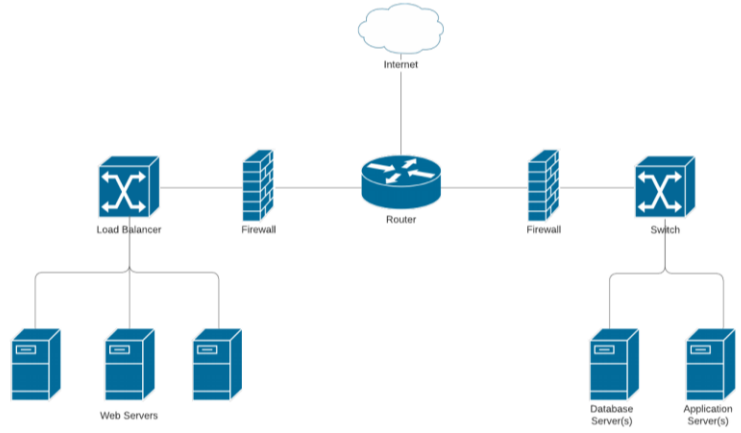


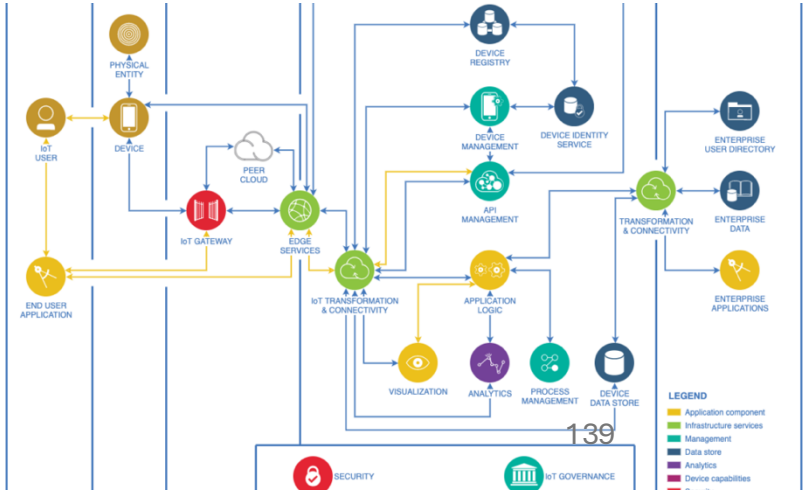



VLAN 10 - Ports 1-10 (Turundus)
VLAN 20 - Ports 11-20 (IT)
VLAN 30 - Ports 21-30 (Finants)

VLAN-ide graafiline kujutamine diagrammide ja võrgukaartide abil on oluline võrgu struktuuri ja ühenduste mõistmiseks. Graafiline esitamine aitab võrguadministraatoritel planeerida, hallata ja tõrkeotsingut teha. Tööriistad nagu Microsoft Visio, Lucidchart ja Draw.io pakuvad tõhusaid vahendeid VLAN-ide ning võrgutopoloogiate kujutamiseks. Näited VLAN-ide graafilisest kujutamisest ja tööriistade kasutamisest illustreerivad, kuidas loogilist segmentimist ja liikluse eraldamist saab visuaalselt esitada, parandades võrgu haldamist ja turvalisust.



# VLAN-sisene marsruutimine

- https://ikt.tthk.ee/vlan-i-tehnoloogia-pohimotted-ja-omadused-2/ - 8

## INTER-VLAN MARSRUUTIMINE

- **Inter-VLAN Marsruutimine** võimaldab liikluse liikumist erinevate VLAN-ide vahel, kasutades L3 ruutereid või L3 lüliteid. See protsess on vajalik, kuna VLAN-id töötavad L2 tasandil ja ilma L3 seadmeteta ei saa liiklus erinevate VLAN-ide vahel liikuda.
- **L3 marsruuterid:** Traditsioonilised ruuterid, mis toimivad L3 tasandil ja võimaldavad liikluse suunamist erinevate VLAN-ide vahel, kasutades alalisi marsruute ja marsruutimistabeleid.
  - **Näide:** Ettevõtte võrgus on VLAN 10 (turundus) ja VLAN 20 (IT). Liiklus nende vahel suunatakse läbi L3 ruuteri, mis ühendab need kaks VLAN-i.
- **L3 kommutaatorid:** kommutaatorid, mis sisaldavad L3 marsruutimisfunktsioone, võimaldades neil toimida nii L2 kui ka L3 tasandil. Need seadmed suudavad kiiresti ja tõhusalt suunata liiklust erinevate VLAN-ide vahel.
  - **Näide:** L3 kommutaatori suudab suunata liiklust VLAN 10 (turundus) ja VLAN 20 (IT) vahel ilma vajaduseta eraldi ruuteri järele.

# Näide VLAN-sisese marsruutimise kasutamisest ettevõtte võrgus

**Ettevõtte võrgustruktuur:**

- **Turundus VLAN 10:** IP vahemik 192.168.10.0/24
- **IT VLAN 20:** IP vahemik 192.168.20.0/24
- **Finants VLAN 30:** IP vahemik 192.168.30.0/24

**L3 Marsruuteri kasutamine:**

- **Alamliidesed VLAN 10 ja VLAN 20 jaoks:** L3 ruuteril on alamliidesed VLAN 10 ja VLAN 20 jaoks, mis võimaldavad liiklust nende VLAN-ide vahel.
- **Turundus ja IT suhtlus:** Kui turundusosakonna arvuti (IP 192.168.10.2) soovib suhelda IT osakonna serveriga (IP 192.168.20.2), suunab L3 ruuter liikluse vastavate alamliideste kaudu.

**L3 kommutaatori kasutamine:**

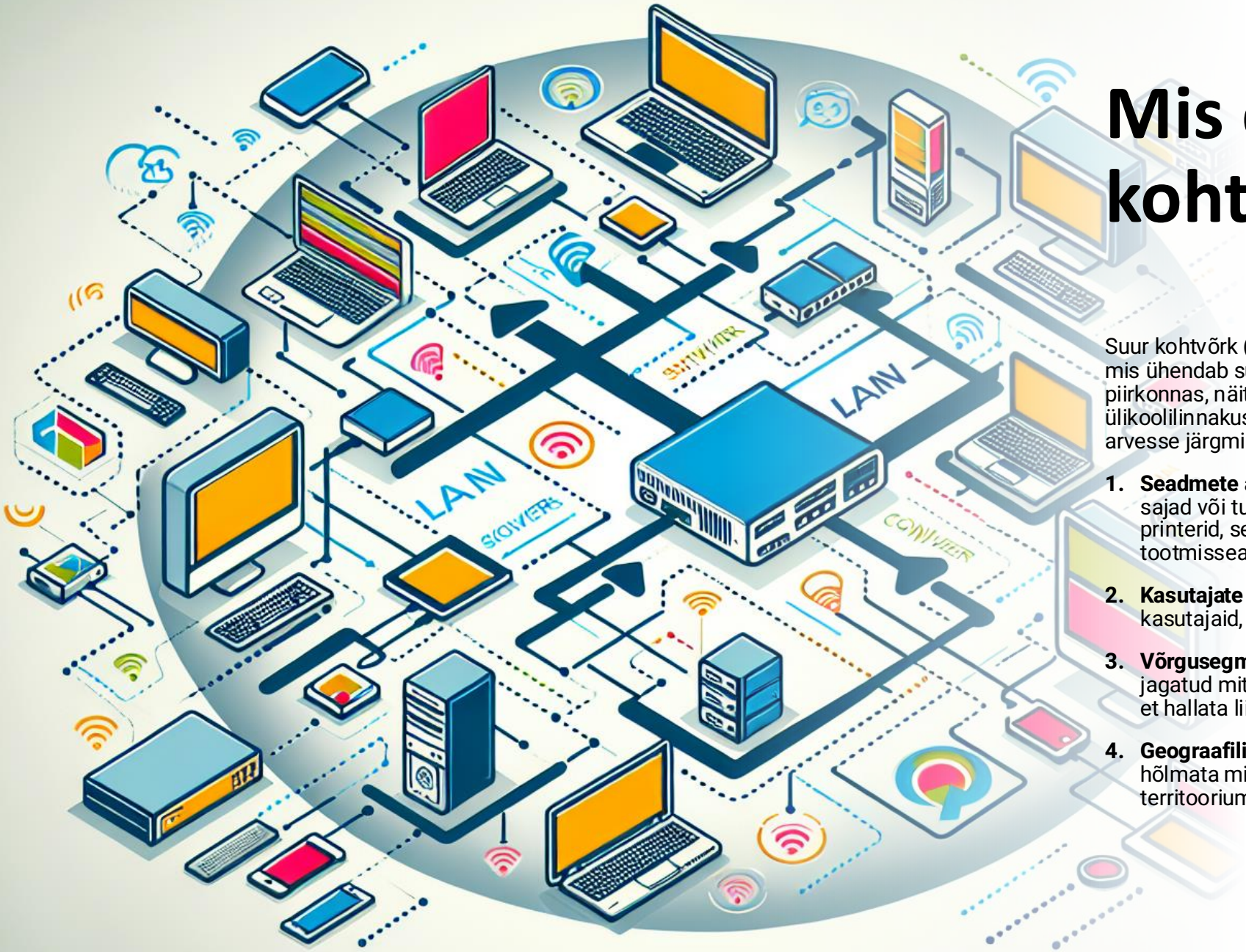
- **SVI VLAN 10 ja VLAN 20 jaoks:** L3 kommutaatoril on SVI-d VLAN 10 ja VLAN 20 jaoks, mis võimaldavad kiiret ja tõhusat liikluse suunamist VLAN-ide vahel.
- **Turundus ja IT suhtlus:** Kui turundusosakonna arvuti (IP 192.168.10.2) soovib suhelda IT osakonna serveriga (IP 192.168.20.2), suunab L3 kommutaatori liikluse otse SVI-de kaudu, ilma et oleks vaja eraldi ruuterit.

# VI osa

# Suurte kohtvõrkudega seotud probleemi

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks




# Mis on suur kohtvõrk?

Suur kohtvõrk (LAN – Local Area Network) viitab võrgule, mis ühendab suurt arvu seadmeid piiratud geograafilises piirkonnas, näiteks ettevõtte hoones, tehases või ülikoolilinnakus. Suure kohtvõrgu määratlemisel võetakse arvesse järgmisi tegureid:

1. **Seadmete arv**: Suure kohtvõrgu alla kuuluvad tavaliselt sajad või tuhanded seadmed, sealhulgas arvutid, printerid, serverid, turvakaamerad, nutiseadmed ja tootmisseadmed.
2. **Kasutajate arv**: Suure võrguga on ühendatud suur hulk kasutajaid, mis võib ulatuda sadadest tuhandeteni.
3. **Võrgusegmendid ja subnetid**: Suur kohtvõrk on sageli jagatud mitmeks segmendiks ja alavõrguks (subnet), et hallata liiklust ja parandada jõudlust.
4. **Geograafiline ulatus**: Suured kohtvõrgud võivad hõlmata mitut hoonet või osakonda ühe suure territooriumi piires.

# Segmendihaldus

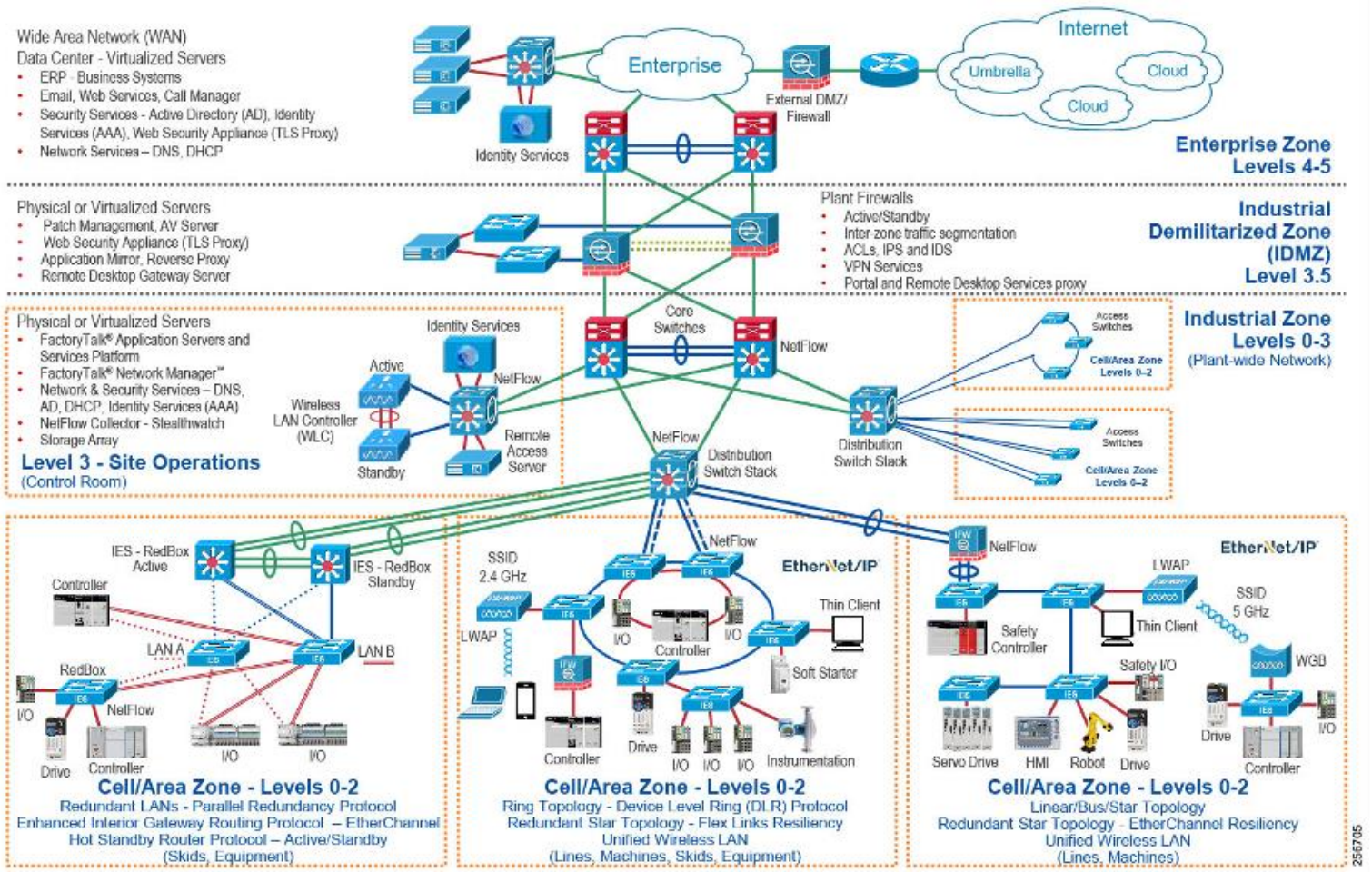
Suured kohtvõrgud (LAN-id) võivad olla keerulised ja nende haldamine nõuab hoolikat planeerimist ja haldusmeetodeid. Segmendihaldus on eriti oluline VLAN-ide puhul, kus võrgu segmenteerimine aitab suurendada turvalisust ja jõudlust. Allpool on üksikasjalik ülevaade segmendihaldusest, sealhulgas VLAN-ide haldamise keerukusest ja parimatest praktikatest.

# Vlan-ide haldamine - KEERUKUS

**VLAN-ide haldamine** suures võrgus võib olla keeruline, kuna see nõuab täpset konfiguratsiooni, pidevat järelevalvet ja kiiret reageerimist muutustele. Suure võrguga kaasnevad mitmed väljakutsed, sealhulgas konfiguratsiooni keerukus, vigade oht ja halduskulud.

| | |
|---|---|
| **Konfiguratsiooni keerukus:** Suurtes võrkudes on palju VLAN-e, seadmeid ja ühendusi, mis muudavad konfiguratsiooni keerukaks ja ajamahukaks. | • **Näide:** Ettevõttes, kus on sadu lüliteid ja tuhandeid porte, võib VLAN-ide konfiguratsioon ja haldamine nõuda palju aega ja ressursse. |
| **Vigade oht:** VLAN-ide vale konfiguratsioon võib põhjustada turvariske, jõudlusprobleeme ja võrguliikluse häireid. | • **Näide:** Vale VID-i määramine või unustatud konfiguratsioon võib põhjustada andmelekkeid või võrguliikluse suunamise probleeme. |
| **Halduskulud:** VLAN-ide haldamine nõuab pidevat järelevalvet ja auditit, mis võib suurendada halduskulusid. | • **Näide:** Regulaarne konfiguratsiooni kontrollimine ja uuendamine nõuab kvalifitseeritud personali ja ajakulu |

# VLAN-ide haldamine - KEERUKUS



# Näide VLAN-ide haldamisest suures võrgus

**Ettevõtte Võrgustruktuur:**

- **VLAN 10 (Turundus):** IP vahemik 192.168.10.0/24, VID 10
- **VLAN 20 (IT):** IP vahemik 192.168.20.0/24, VID 20
- **VLAN 30 (Finants):** IP vahemik 192.168.30.0/24, VID 30

**Dokumentatsioon:**

- **VLAN konfiguratsioon:** VLAN 10 on määratud portidele 1-10 kommutaatoril 1, VLAN 20 on määratud portidele 11-20 ja VLAN 30 on määratud portidele 21-30. Kõik need konfiguratsioonid on dokumenteeritud keskandmebaasis.
- **Seadmed:** Iga VLAN-i seadmed on loetletud koos vastavate IP-aadresside ja füüsiliste asukohtadega.

**Auditiprotsess:**

- **Regulaarsed kontrollid:** Iga kvartali järel teostatakse audit, et kontrollida VLAN-ide konfiguratsiooni ja turvalisust. Audit hõlmab konfiguratsioonifailide kontrollimist, seadmete ja ühenduste ülevaatamist ning turvavigade tuvastamist.
- **Automatiseerimine:** Kasutatakse võrgu haldustarkvara, mis toetab automaatset VLAN-ide konfigureerimist ja seiret. See vähendab manuaalse töö mahtu ja vigade ohtu.

# JÕUDLUS

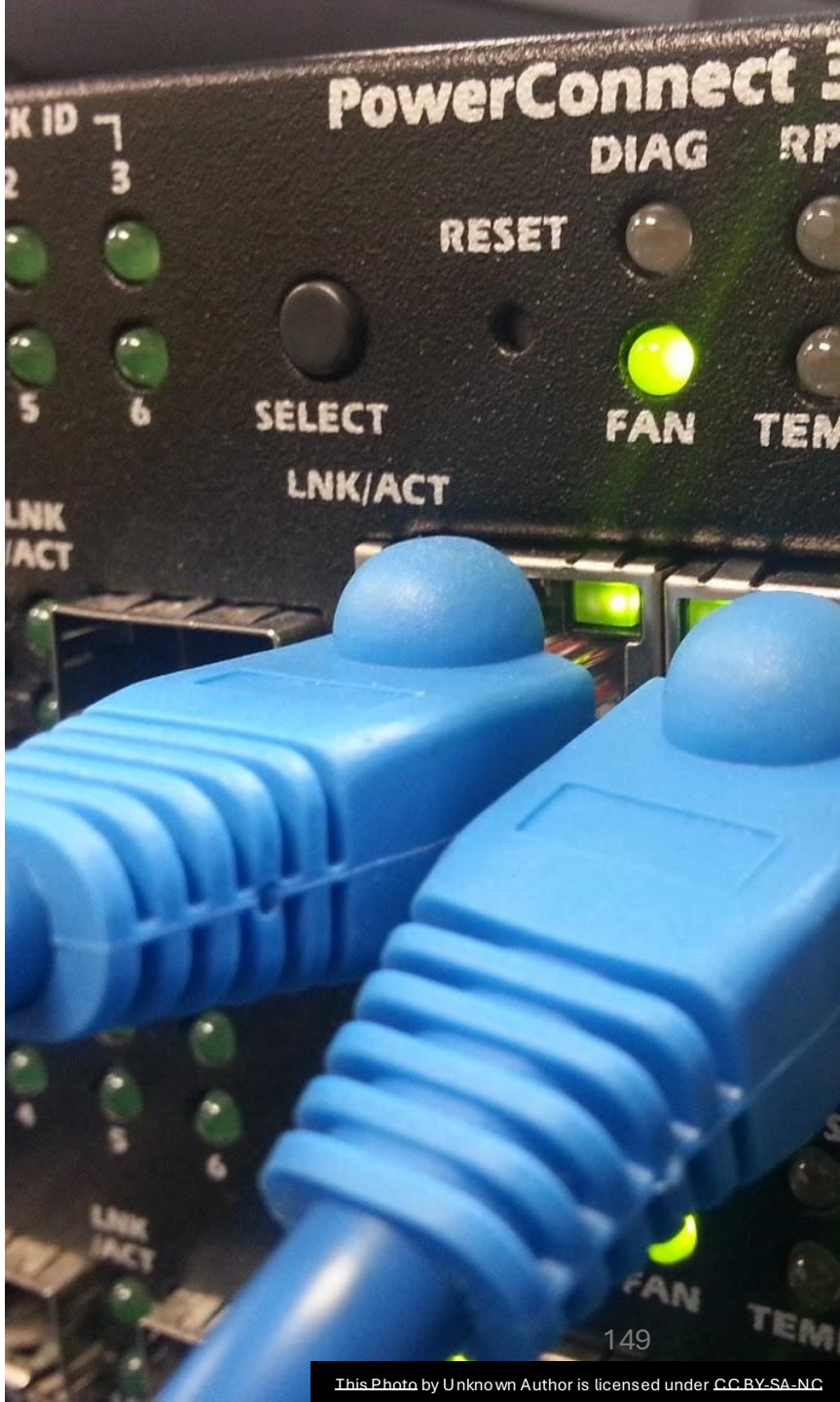
VLAN-id mängivad olulist rolli võrgu liikluse optimeerimisel ja ülekoormuse vähendamisel. Samas võivad VLAN-sisene marsruutimine ja suur võrgu segmentatsioon tekitada täiendavat koormust marsruuteritele ja kommutaatoritele. Allpool on üksikasjalik ülevaade jõudlusprobleemidest ja nende lahendamisest suurtes kohtvõrkudes.

# LIIKLUSE OPTIMEERIMINE

**VLAN-ID JA JÕUDLUS**

**VLAN-id aitavad optimeerida liiklust ja vähendada ülekoormust**, luues loogilisi võrgusegmente, mis piiravad liikluse levikut ja vähendavad ülekoormust. VLAN-ide abil saab võrguadministraatorid paremini hallata liikluse suunamist ja tagada, et liiklus liigub ainult vajalike sihtkohtadeni.

- **Piiratud liiklus:** VLAN-id piiravad liikluse levikut, võimaldades liikluse liikuda ainult määratud VLAN-i sees, vähendades nii kogu võrgu ülekoormust.
- **Vähendatud ülekoormus:** VLAN-id võimaldavad liikluse segmentatsiooni, mis vähendab kommutaatorite ja ruuterite ülekoormust.



# Marsruutimise koormus

**KOORMUS MARSRUUTERITELE JA KOMMUTAATORITELE**

**VLAN-sisene marsruutimine võib tekitada täiendavat koormust marsruuteritele ja kommutaatoritele**, eriti suurtes võrkudes, kus on palju VLAN-e ja seadmeid. Marsruuterid ja L3 kommutaatorid peavad suutma kiiresti ja tõhusalt suunata liiklust erinevate VLAN-ide vahel, säilitades samal ajal võrgu jõudluse ja usaldusväärsuse.

- **Marsruutimise koormus:** L3 marsruuterid ja kommutaatorid peavad töötlema suurtes võrkudes palju liiklust, mis võib tekitada täiendavat koormust ja vähendada jõudlust.
- **Optimeerimismeetodid:** VLAN-ide ja marsruutimise optimeerimiseks saab kasutada mitmeid meetodeid, sealhulgas liikluse prioriseerimist, koondamist ja jõudluse jälgimist.

# Näide vlan-ide jõudluse optimeerimisest suures võrgus

### Ettevõtte võrgustruktuur:

**VLAN 10 (Turundus):** IP vahemik 192.168.10.0/24, VID 10

**VLAN 20 (IT):** IP vahemik 192.168.20.0/24, VID 20

**VLAN 30 (Finants):** IP vahemik 192.168.30.0/24, VID 30

### Liikluse optimeerimine:

**Liikluse piiramine:** Turundusosakonna seadmete liiklus on piiratud VLAN 10 sees, vähendades kommutaatorite ja ruuterite ülekoormust.

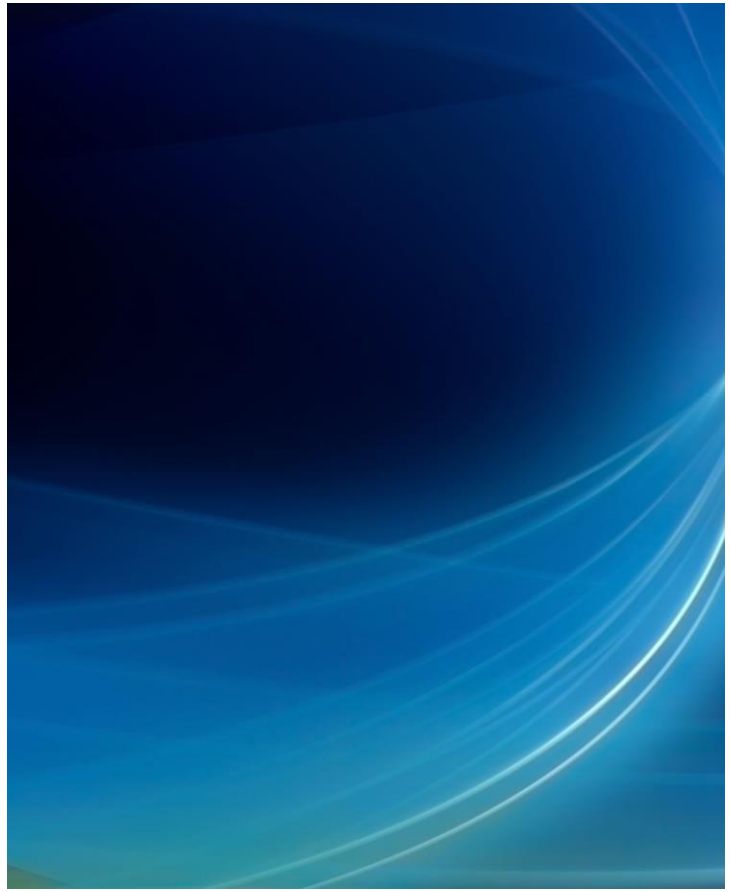
**Jõudluse parandamine:** Liiklus IT-osakonna ja finantsosakonna vahel suunatakse vastavalt vajadusele läbi L3 kommutaatori või marsruuteri, mis tagab kiire ning tõhusa suunamise.

### Marsruutimise koormuse halduse näide:

**QoS poliitikad:** Kasutades QoS poliitikaid, määratakse kriitiline liiklus (nt finantsandmed) kõrgema prioriteediga, tagades, et see liiklus saab vajalikud ressursid ja prioriteedi.

**Koondamine:** Kasutades kommutaatorite ja ruuterite koondamist (aggregation), saab vähendada üksikute seadmete koormust ning parandada üldist võrgu jõudlust.

**Jõudluse jälgimine:** Regulaarne jõudluse jälgimine ja analüüs aitab tuvastada võimalikke kitsaskohti ning optimeerida võrguressursse.



Abiks: *QoS (Quality of Service) Tööstuses*

# VII osa

# Võrguanalüsaator WIRESHARK

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks

# Sissejuhatus

- Wireshark on tasuta ja avatud lähtekoodiga võrguanalüüsitarkvara, mis võimaldab jälgida ja analüüsida võrgu liiklust. See on kasulik tööriist mehhatroonikutele, elektrikutele ja külmatehnika spetsialistidele, kes vajavad süvitsi mõistmist võrguühenduste ja andmeside protokollide toimimisest.
- Wireshark on vabavara, avatud lähtekoodiga ning üks parimaid täna saadaolevaid paketianalüsaatoreid.

# Miks Wireshark

Siin on mõned põhjused, miks inimesed Wiresharki kasutavad:

- Võrguadministraatorid kasutavad seda võrguprobleemide tõrkeotsinguks.
- Võrguturbeinsenerid kasutavad seda turvaprobleemide uurimiseks.
- QA insenerid kasutavad seda võrgurakenduste kontrollimiseks.
- Arendajad kasutavad seda protokolli rakenduste silumiseks.
- Õppurid kasutavad seda võrguprotokollide õppimiseks.
- Wireshark võib olla abiks ka paljudes muudes olukordades.

# Wiresharki funktsioonid:

- Saadaval UNIXi ja Windowsi jaoks.
- Jäädvustage reaalajas pakettandmeid võrguliidese kaudu.
- Avage failid, mis sisaldavad pakettandmeid, mis on jäädvustatud tcpdump/WinDump, Wiresharki ja paljude teiste pakettide püüdmise programmidega.
- Importige pakette tekstifailidest, mis sisaldavad pakettandmete hex dumps.
- Kuva paketid väga üksikasjaliku protokolliteabega.
- Salvestage jäädvustatud pakettandmed.
- Eksportige mõned või kõik paketid mitmes püüdmisfailivormingus.
- Filtreerige pakette paljude kriteeriumide alusel.
- Otsige pakette paljude kriteeriumide alusel.
- Värvige pakettkuva filtrite põhjal.
- Looge erinevat statistikat.
- … ja palju muud!

# Juhend Wiresharki paigaldamiseks ja esmaseks konfiguratsiooniks

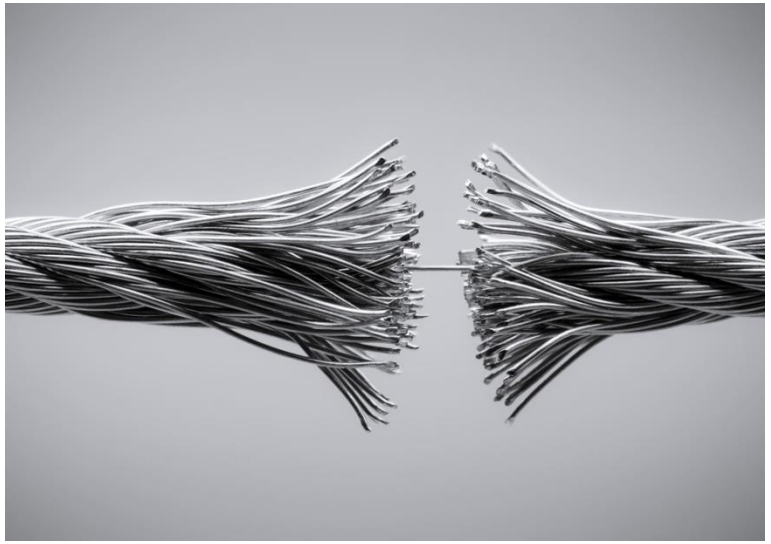
**1.1 Laadige alla Wireshark:**

- **Minge Wiresharki ametlikule veebisaidile:**
- Aadress: Wireshark Download
- **Valige oma operatsioonisüsteemile sobiv versioon:**
- **Windows:** Valige .exe fail.
- **macOS:** Valige .dmg fail.
- **Linux:** Valige sobiv pakett oma Linuxi distributsioonile (nt .deb Debian/Ubuntu jaoks, .rpm Fedora/Red Hat jaoks).

# Juhend Wiresharki paigaldamiseks ja esmaseks konfiguratsiooniks

**1.2 Installige Wireshark:**

- **Käivitage allalaaditud installatsioonifail ja järgige ekraanil kuvatavaid juhiseid:**
- **Windows:**
  - Käivitage .exe fail.
  - Järgige installiviisardi juhiseid.
  - Installi käigus küsitakse teilt WinPcap või NPCap paigaldamist. Need on vajalikud võrgupakettide püüdmiseks.
- **macOS:**
  - Käivitage .dmg fail.
  - Lohistage Wireshark rakenduste kausta.
- **Linux:**
  - Ubuntu/Debian: Avage terminal ja kasutage käsku sudo apt install wireshark.
  - Fedora: Avage terminal ja kasutage käsku sudo dnf install wireshark.



# Juhend Wiresharki esmaseks konfiguratsiooniks

**Käivitage Wireshark:**

- **Avage Wireshark pärast installatsiooni lõpetamist:**
- **Windows ja macOS:** Topeltklõpsake Wireshark ikoonil või avage see Start menüüst (Windows) või rakenduste kaustast (macOS).
- **Linux:** Käivitage Wireshark menüüst või kasutage terminalis käsku wireshark.

# Juhend Wiresharki esmaseks konfiguratsiooniks

**Käivitage Wireshark:**

- **Avage Wireshark pärast installatsiooni lõpetamist:**
- **Windows ja macOS:** Topeltklõpsake Wireshark ikoonil või avage see Start menüüst (Windows) või rakenduste kaustast (macOS).
- **Linux:** Käivitage Wireshark menüüst või kasutage terminalis käsku wireshark

**Valige võrguliides:**

- **Avakuval näete nimekirja võrguadapteritest:**
- Wiresharki avamisel kuvatakse teile nimekiri saadaolevatest võrguadapteritest.
- Iga adapteri kõrval on reaalajas graafik, mis näitab liikluse aktiivsust.
- **Valige adapter, mille kaudu soovite liiklust jälgida (nt Ethernet või Wi-Fi):**
- Klõpsake adapteril, mida soovite kasutada liikluse jälgimiseks.
- Kui te pole kindel, millist adapterit valida, vaadake, milline neist näitab aktiivset liiklust.

# Juhend Wiresharki esmaseks konfiguratsiooniks

**Jäädvustamise alustamine:**

- **Alustage liikluse jäädvustamist:**
- Klõpsake valitud adapteri kõrval asuvat sinist haakristi (Start capturing packets) või kasutage klaviatuuri otseteed Ctrl+E.
- Wireshark hakkab nüüd püüdma kõiki pakette, mis liiguvad läbi valitud adapteri.
- **Lõpetage liikluse jäädvustamine:**
- Jäädvustamise peatamiseks klõpsake punasel ruudul (Stop capturing packets) või kasutage klaviatuuri otseteed Ctrl+E uuesti.

- **Liikluse filtreerimine ja analüüs:**
- **Filtreerige püütud liiklust:**
- Kasutage Wiresharki ülemises osas asuvat filtri riba, et sisestada filtreerimiskriteeriumid (nt ip.addr == 192.168.1.1).
- Filtrid aitavad teil keskenduda konkreetsetele liiklusvoogudele või protokollidele.
- **Analüüsige püütud pakette:**
- Wireshark pakub väga detailset vaadet igale püütud paketile, võimaldades teil näha paketi sisu, päiseid ja muud.
- Kasutage Wiresharki tööriistu ja funktsioone, et uurida ja analüüsida võrguliiklust.

# Juhend Wiresharki esmaseks konfiguratsiooniks

**Pakettide salvestamine ja eksportimine:**

- **Salvestage püütud liiklus:**
- Wireshark võimaldab teil salvestada püütud pakette erinevates failivormingutes (nt .pcap).
- Pakettide salvestamiseks valige File > Save As ja määrake salvestuskoht ja failinimi.
- **Eksportige pakettandmed:**
- Wireshark võimaldab eksportida pakette erinevates formaatides (nt XML, CSV).
- Pakettide eksportimiseks valige File > Export Specified Packets ja määrake eksportimise valikud.

**Lisafunktsioonid:**

- **Statistika ja graafikud:**
- Wireshark pakub erinevaid statistika tööriistu, et analüüsida võrguliikluse mustreid ja mahtusid.
- Kasutage tööriistu nagu Protocol Hierarchy, Conversations ja Endpoints, et saada ülevaade võrguliiklusest.
- **Värvikoodide kasutamine:**
- Wireshark kasutab värvikoodide süsteemi, et aidata tuvastada erinevaid liiklustüüpe ja anomaaliaid.
- Kohandage värvikoodide reegleid vastavalt oma vajadustele, valides View > Coloring Rules.

# Esmased harjutused Wiresharki kasutamiseks:

**Pakettide Püük**

**1. Alustage püü**ki:

- Valige sobiv võrguliides ja klõpsake sinisel haakristil (shark fin icon) akna vasakus ülanurgas.
- Wireshark hakkab nüüd püüdma kõiki võrgu kaudu liiklevaid pakette.

**2. Peatage püük**:

- Kui olete piisavalt liiklust püüdnud, peatage püük punase ruudu ikooniga (stop button).

**Püütud Andmete Analüüs**

1. **Filtreerimine**:

- Wireshark võimaldab filtreerida konkreetseid pakette, kasutades filtrivälja akna ülaosas.
- Näited:
  - ip.addr == 192.168.1.1 (filtreerib kogu liikluse, mis on seotud konkreetse IP-aadressiga)
  - tcp.port == 80 (filtreerib kogu TCP liikluse, mis kasutab porti 80)

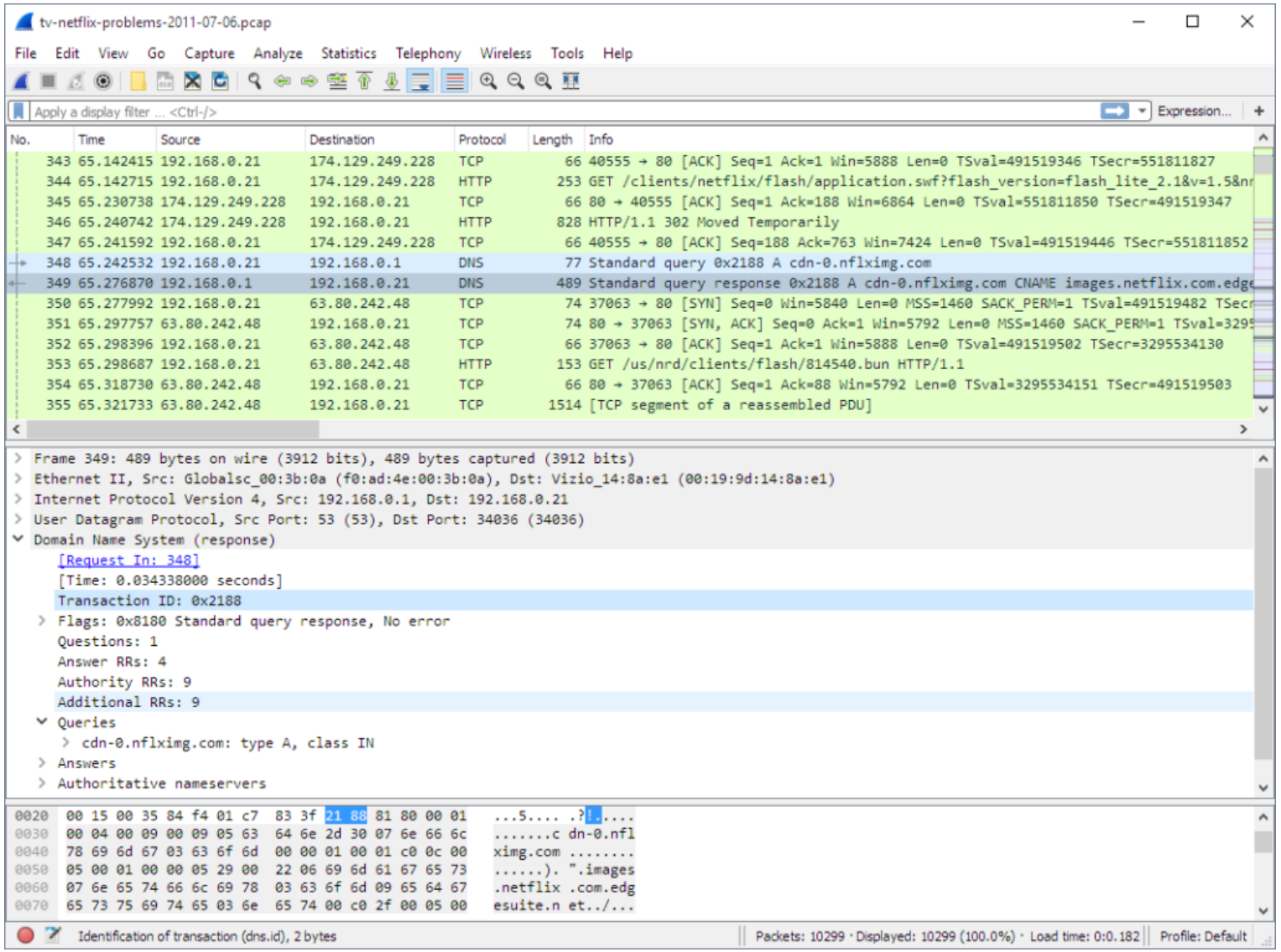
2. **Protokolli dekodeerimine**:

- Iga püüdmise ajal püütud pakett kuvatakse Wiresharki aknas koos üksikasjaliku protokollianalüüsiga.
- Klõpsake paketi peal, et näha selle üksikasju ja struktureeritud dekodeeringut.

3. **Statistika ja graafikud**:

- Wireshark pakub mitmeid tööriistu statistika ja graafikute loomiseks.
- Menüüst valige **Statistics** ja seejärel soovitud alammenüü (nt **Protocol Hierarchy**, **Conversations**, **IO Graphs**).

# Kuvafiltrid wiresharkile

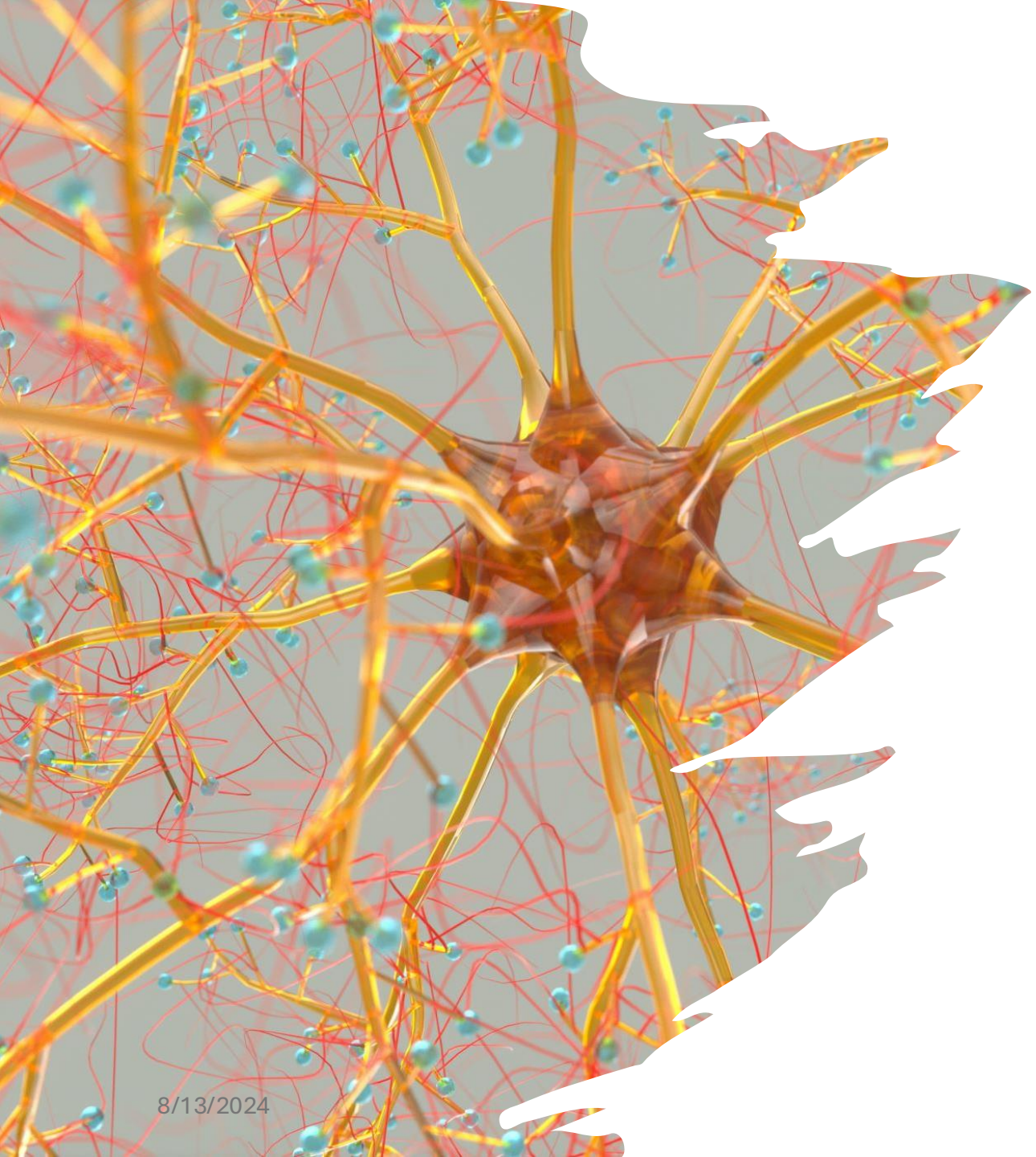


# IP-AADRESSI FILTREERIMINE

FILTREERIMINE IP-AADRESSI ALUSEL

**Filtreerimine IP-aadressi alusel** võimaldab kasutajatel jälgida ja analüüsida liiklust, mis on seotud konkreetsete IP-aadressidega. See on kasulik võrgutõrgete diagnoosimisel, turvalisuse jälgimisel ja võrguliikluse analüüsimisel.

- **IP-aadressi põhine filtreerimine:** Wireshark võimaldab filtreerida pakette, mis on saadetud kindlast IP-aadressist või saadud kindlale IP-aadressile.
- **Näide:** Jälgida kogu liiklust, mis on saadetud IP-aadressilt 192.168.1.1.
- **Filtrikäsud:**
  - ip.addr == 192.168.1.1 (filtreerib kõik paketid, kus lähte- või sihtaadress on 192.168.1.1)
  - ip.src == 192.168.1.1 (filtreerib paketid, kus lähteaadress on 192.168.1.1)
  - ip.dst == 192.168.1.1 (filtreerib paketid, kus sihtaadress on 192.168.1.1



# IP-AADRESSI FILTREERIMINE

- KUIDAS JÄLGIDA JA FILTREERIDA LIIKLUST KONKREETSETE IP-AADRESSIDE PÕHJAL
- **Lähte- ja sihtaadressi filtreerimine:** Wiresharkis saab määrata filtreid, mis põhinevad kas lähte- või sihtaadressil. See võimaldab jälgida, kuidas konkreetne seade suhtleb võrgus.
    - **Näide:** Kui soovite jälgida kõiki pakette, mis on saadetud IP-aadressilt 10.0.0.1 teisele IP-aadressile, võite kasutada filtrit ip.src == 10.0.0.1.
- **Mitme IP-aadressi filtreerimine:** Võimalik on ka jälgida liiklust mitme IP-aadressi vahel, kasutades loogilisi operaatorid nagu and ja or.
    - **Näide:** Filtreerimiseks, mis hõlmab pakette kahest IP-aadressist (192.168.1.1 ja 10.0.0.1), kasutage filtrit ip.addr == 192.168.1.1 or ip.addr == 10.0.0.1.

# NÄIDE IP-AADRESSI FILTREERIMISEST WIRESHARKIS

- **Ettevõtte Võrgustruktuur:**
- **Server:** 192.168.1.100
- **Tööjaam 1:** 192.168.1.101
- **Tööjaam 2:** 192.168.1.102
- **Jälgimine ja Filtreerimine:**
- **Serveri liiklus:** Jälgida kogu liiklust, mis läheb serverisse ja serverist (192.168.1.100).
- **Filtrikäsk:** ip.addr == 192.168.1.100
- **Tööjaamadevaheline liiklus:** Jälgida tööjaamadevahelist liiklust (192.168.1.101 ja 192.168.1.102).
- **Filtrikäsk:** ip.addr == 192.168.1.101 and ip.addr == 192.168.1.102

# KUIDAS LUUA JA KASUTADA KUVAFILTREID WIRESHARKIS

1. **Wiresharki avamine ja liikluse jälgimine:**
- Käivitage Wireshark ja valige võrguliides, mida soovite jälgida.
- Vajutage nuppu “Start” liikluse jälgimiseks.

2. **Filtri määramine:**
- Sisestage filtrikäsud Wiresharki filtripaneelile ja vajutage “Enter”.
- Näiteks, sisestage ip.addr == 192.168.1.1 kogu liikluse filtreerimiseks, mis on seotud IP-aadressiga 192.168.1.1.

3. **Filtri rrakendamine ja analüüs:**
- Wireshark kuvab ainult need paketid, mis vastavad määratud filtrile.
- Analüüsige filtreeritud liiklust, et tuvastada probleemid või jälgida võrguaktiivsust.

# PORTIDE FILTREERIMINE

- Wireshark võimaldab filtreerida võrgu liiklust mitte ainult IP-aadresside, vaid ka portide alusel. Portide filtreerimine on kasulik, et jälgida liiklust, mis on seotud konkreetsete rakenduste või teenustega, kuna paljud protokollid ja teenused kasutavad kindlaid portnumbrei

# FILTREERIMINE PORTNUMBRITE ALUSEL

**Filtreerimine portnumbrite alusel** võimaldab kasutajatel jälgida ja analüüsida liiklust, mis liigub kindlate portide kaudu. See on kasulik rakenduste ja teenuste analüüsimisel, turvalisuse jälgimisel ning võrgutõrgete diagnoosimisel.

- **Portide põhine filtreerimine:** Wireshark võimaldab filtreerida pakette, mis on seotud kindlate pordi numbritega. Seda saab teha nii lähte- kui ka sihtportide alusel.
- **Näide:** Jälgida kogu liiklust, mis kasutab porti 80 (HTTP).
- **Filtrikäsud:**
  - tcp.port == 80 (filtreerib kõik TCP paketid, mis kasutavad porti 80)
  - udp.port == 53 (filtreerib kõik UDP paketid, mis kasutavad porti 53)
  - tcp.srcport == 443 (filtreerib TCP paketid, kus lähteport on 443)
  - udp.dstport == 67 (filtreerib UDP paketid, kus sihtport on 67)

# KUIDAS JÄLGIDA JA FILTREERIDA LIIKLUST KINDLATE PORTIDE JÄRGI

- **Lähte- ja sihtportide filtreerimine:** Wiresharkis saab määrata filtreid, mis põhinevad kas lähte- või sihtportidel. See võimaldab jälgida, kuidas konkreetsed teenused või rakendused suhtlevad võrgus.
  - **Näide:** Kui soovite jälgida kõiki pakette, mis on saadetud lähteporti 22 kaudu (SSH), võite kasutada filtrit tcp.srcport == 22.
- **Mitme pordi filtreerimine:** Võimalik on ka jälgida liiklust mitme pordi vahel, kasutades loogilisi operaatorid nagu and ja or.
  - **Näide:** Filtreerimiseks, mis hõlmab liiklust portide 80 ja 443 vahel, kasutage filtrit tcp.port == 80 or tcp.port == 443.

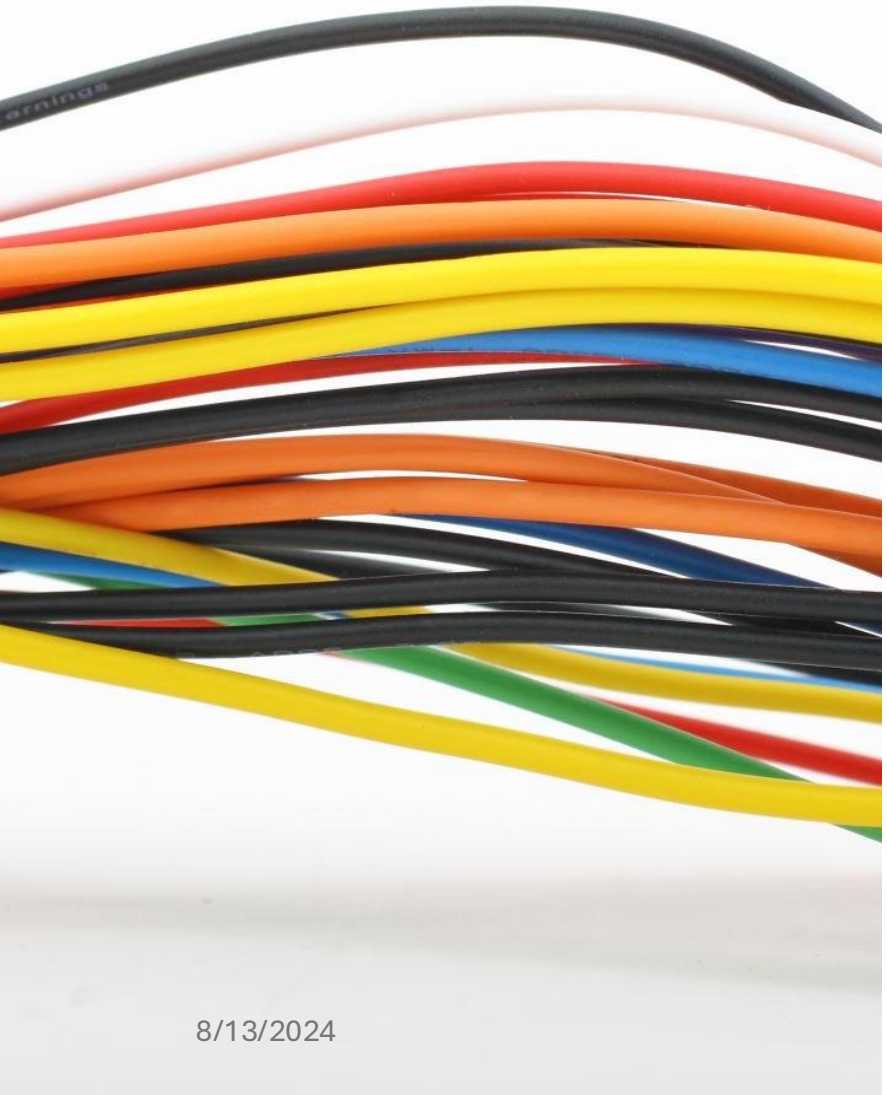
# NÄIDE PORTIDE FILTREERIMISEST WIRESHARKIS

**Ettevõtte võrgustruktuur:**

- **Veebiserver:** Port 80 (HTTP)
- **Turvaprotsess:** Port 443 (HTTPS)
- **DNS-server:** Port 53 (UDP)

**Jälgimine ja filtreerimine:**

- **Veebiliiklus:** Jälgida kogu liiklust, mis kasutab HTTP porti (80).
- **Filtrikäsk:** tcp.port == 80
- **Turvaline veebiliiklus:** Jälgida kogu liiklust, mis kasutab HTTPS porti (443).
- **Filtrikäsk:** tcp.port == 443
- **DNS Liiklus:** Jälgida kogu liiklust, mis kasutab DNS porti (53).
- **Filtrikäsk:** udp.port == 53



# KUIDAS LUUA JA KASUTADA KUVAFILTREID WIRESHARKIS

1. **Wiresharki avamine ja liikluse Jälgimine:**
- Käivitage Wireshark ja valige võrguliides, mida soovite jälgida.
- Vajutage nuppu “Start” liikluse jälgimiseks.
2. **Filtri määramine:**
- Sisestage filtrikäsud Wiresharki filtripaneelile ja vajutage “Enter”.
- Näiteks, sisestage tcp.port == 80 kogu liikluse filtreerimiseks, mis on seotud portiga 80.
3. **Filtri rakendamine ja analüüs:**
- Wireshark kuvab ainult need paketid, mis vastavad määratud filtrile.
- Analüüsige filtreeritud liiklust, et tuvastada probleemid või jälgida võrguaktiivsust.

# PROTOKOLLI FILTREERIMINE

Wireshark võimaldab filtreerida võrgu liiklust mitte ainult IP-aadresside ja portide, vaid ka protokollide alusel. Protokolli filtreerimine on kasulik, et jälgida ja analüüsida liiklust, mis kasutab kindlaid protokolle, nagu TCP, UDP või ICMP. See võimaldab sügavamat ülevaadet võrgu toimimisest ja aitab tõrkeotsingul ning turvalisuse jälgimisel.

# FILTREERIMINE PROTOKOLLIDE ALUSEL

- **Filtreerimine protokollide alusel** võimaldab kasutajatel jälgida ja analüüsida liiklust, mis kasutab kindlaid protokolle. See on kasulik võrgu toimimise mõistmiseks, turvalisuse jälgimiseks ja võrgutõrgete diagnoosimiseks.
- **Protokollipõhine filtreerimine:** Wireshark võimaldab filtreerida pakette, mis on seotud kindlate protokollidega, nagu TCP, UDP, ICMP jt.
  - **Näide:** Jälgida kogu liiklust, mis kasutab TCP protokolli.
  - **Filtrikäsud:**
    - tcp (filtreerib kõik TCP paketid)
    - udp (filtreerib kõik UDP paketid)
    - icmp (filtreerib kõik ICMP paketid)
    - http (filtreerib kõik HTTP paketid)
    - dns (filtreerib kõik DNS paketid)

# KUIDAS JÄLGIDA JA FILTREERIDA LIIKLUST KONKREETSETE PROTOKOLLIDE JÄRGI

- **TCP ja UDP filtreerimine:** Wiresharkis saab määrata filtreid, mis põhinevad TCP või UDP protokollidel. See võimaldab jälgida, kuidas andmeedastus toimub võrgu erinevate osade vahel.
  - **Näide:** Kui soovite jälgida kõiki pakette, mis kasutavad TCP protokolli, võite kasutada filtrit tcp.
- **ICMP filtreerimine:** ICMP protokolli filtreerimine on kasulik võrgudiagnostikas, näiteks ping-käskude ja vastuste jälgimisel.
  - **Näide:** Jälgida kõiki ping-päringuid ja vastuseid, kasutades filtrit icmp.

# NÄIDE PROTOKOLLI FILTREERIMISEST WIRESHARKIS

**Ettevõtte Võrgustruktuur:**

- **Veebiserver:** Kasutab HTTP (port 80) ja HTTPS (port 443) protokolle
- **DNS-server:** Kasutab DNS protokolli (port 53)
- **Tööjaamad:** Kasutavad erinevaid protokolle suhtlemiseks ja andmevahetuseks

**Jälgimine ja Filtreerimine:**

- **HTTP liiklus:** Jälgida kogu liiklust, mis kasutab HTTP protokolli.
- **Filtrikäsk:** http
- **DNS liiklus:** Jälgida kogu liiklust, mis kasutab DNS protokolli.
- **Filtrikäsk:** dns
- **ICMP liiklus:** Jälgida kogu liiklust, mis kasutab ICMP protokolli.
- **Filtrikäsk:** icmp

# KUIDAS LUUA JA KASUTADA KUVAFILTREID WIRESHARKIS

1. **Wiresharki avamine ja liikluse jälgimine:**
   - Käivitage Wireshark ja valige võrguliides, mida soovite jälgida.
   - Vajutage nuppu “Start” liikluse jälgimiseks.
2. **Filtri määramine:**
   - Sisestage filtrikäsud Wiresharki filtripaneelile ja vajutage “Enter”.
   - Näiteks, sisestage tcp kogu TCP liikluse filtreerimiseks.
3. **Filtri rakendamine ja analüüs:**
   - Wireshark kuvab ainult need paketid, mis vastavad määratud filtrile.
   - Analüüsige filtreeritud liiklust, et tuvastada probleemid või jälgida võrguaktiivsust.

# VOO FILTREERIMINE

Wireshark võimaldab mitte ainult IP-aadressi, pordi ja protokolli alusel filtreerida liiklust, vaid ka konkreetsete andmevoogude alusel. Voo filtreerimine on kasulik, et jälgida ja analüüsida konkreetseid andmevooge, mis liiguvad seadmete vahel, võimaldades detailset liikluse analüüsi ja tõrkeotsingut.

# VOO JÄLGIMINE JA FILTREERIMINE

**Voo jälgimine ja filtreerimine** võimaldab kasutajatel keskenduda konkreetsetele andmevoogudele, mis liiguvad seadmete vahel. Andmevoog koosneb seotud andmepakettidest, mis liiguvad lähteaadressilt sihtaadressile läbi kindla protokolli ja portide.

- **Voo põhine filtreerimine:** Wireshark võimaldab filtreerida konkreetseid andmevooge, kasutades erinevaid parameetreid, nagu IP-aadressid, portnumbrid ja protokollid.
- **Näide:** Jälgida kõiki pakette, mis liiguvad IP-aadressilt 192.168.1.1 IP-aadressile 192.168.1.2, kasutades TCP protokolli ja porti 80.
- **Filtrikäsud:**
  - ip.src == 192.168.1.1 and ip.dst == 192.168.1.2 and tcp.port == 80
  - tcp.stream eq 1 (filtreerib konkreetse TCP voo, mille voonumber on 1)

# KUIDAS JÄLGIDA JA FILTREERIDA KONKREETSEID ANDMEVOOGEKUIDAS JÄLGIDA JA FILTREERIDA KONKREETSEID ANDMEVOOGE

**Spetsiifiliste voogude filtreerimine:** Wireshark võimaldab filtreerida ja jälgida andmevooge, kasutades täpseid parameetreid, nagu lähteaadress, sihtaadress, portnumbrid ja protokollid.

**Näide:** Kui soovite jälgida kõiki pakette, mis liiguvad lähteaadressilt 10.0.0.1 sihtaadressile 10.0.0.2, kasutage filtrit ip.src == 10.0.0.1 and ip.dst == 10.0.0.2.

**Voonumbrite kasutamine:** Wireshark määrab igale TCP voole unikaalse voonumbri, mida saab kasutada konkreetse voo filtreerimiseks ja analüüsimiseks.

**Näide:** Konkreetse TCP voo jälgimiseks, mille voonumber on 5, kasutage filtrit tcp.stream eq 5.

# NÄIDE VOO FILTREERIMISEST WIRESHARKIS

**Ettevõtte võrgustruktuur:**

- **Veebiserver:** 192.168.1.100 (kasutab porti 80)
- **Tööjaam 1:** 192.168.1.101
- **Tööjaam 2:** 192.168.1.102
- **Jälgimine ja Filtreerimine:**
- **Tööjaam 1 ja veebiserver:** Jälgida kogu liiklust, mis liigub tööjaamast 1 (192.168.1.101) veebiserverisse (192.168.1.100) läbi TCP protokolli ja porti 80.
- **Filtrikäsk:** ip.src == 192.168.1.101 and ip.dst == 192.168.1.100 and tcp.port == 80
- **Konkreetne TCP voo jälgimine:** Jälgida konkreetset TCP voogu, mille voonumber on 3.
- **Filtrikäsk:** tcp.stream eq 3

# KUIDAS LUUA JA KASUTADA KUVAFILTREID WIRESHARKIS

1. **Wiresharki avamine ja liikluse jälgimine:**
- Käivitage Wireshark ja valige võrguliides, mida soovite jälgida.
- Vajutage nuppu “Start” liikluse jälgimiseks.
2. **Filtri määramine:**
- Sisestage filtrikäsud Wiresharki filtripaneelile ja vajutage “Enter”.
- Näiteks, sisestage ip.src == 192.168.1.101 and ip.dst == 192.168.1.100 and tcp.port == 80 konkreetse voo filtreerimiseks.
3. **Filtri rakendamine ja analüüs:**
- Wireshark kuvab ainult need paketid, mis vastavad määratud filtrile.
- Analüüsige filtreeritud liiklust, et tuvastada probleemid või jälgida võrguaktiivsust.

# HOSTINIME FILTREERIMINE

Wireshark võimaldab filtreerida võrgu liiklust ka hostinimede alusel, mis on eriti kasulik, kui soovite jälgida liiklust konkreetsete seadmete vahel ilma IP-aadresse meelde jätmata. Hostinime filtreerimine võib lihtsustada võrguadministraatorite ja analüütikute tööd, pakkudes lihtsamat ja intuitiivsemat viisi võrguliikluse jälgimiseks ja analüüsimiseks.

# FILTREERIMINE HOSTINIMEDE ALUSEL

**Filtreerimine hostinimede alusel** võimaldab kasutajatel jälgida ja analüüsida liiklust, kasutades seadmete hostinimesid. See on kasulik, kui IP-aadresse on raske meeles pidada või kui seadmete IP-aadressid võivad muutuda, kuid hostinimed jäävad samaks.

- **Hostinime põhine filtreerimine:** Wireshark võimaldab filtreerida pakette, mis on seotud kindlate hostinimedega. See toimub läbi DNS päringute, kus hostinimed tõlgitakse IP-aadressideks.
- **Näide:** Jälgida kogu liiklust, mis on seotud hostinimega “server.example.com”.
- **Filtrikäsud:**
  - host server.example.com (filtreerib kõik paketid, mis on seotud hostinimega “server.example.com”)

# KUIDAS KASUTADA HOSTINIMESID LIIKLUSE FILTREERIMISEKS

- **DNS päringud ja vastused:** Wireshark saab kasutada DNS päringuid ja vastuseid hostinimede tõlkimiseks IP-aadressideks, võimaldades filtreerida liiklust hostinimede alusel.
  - **Näide:** Kui soovite jälgida kogu liiklust hostinime “www.google.com” põhjal, teeb Wireshark DNS päringu, et tuvastada vastav IP-aadress, ja filtreerib liiklust selle IP-aadressi alusel.
- **Hostinime filtreerimise kombinatsioon:** Wireshark võimaldab kombineerida hostinime filtreid teiste filtritega, nagu portnumbrid ja protokollid, et saada täpsem ülevaade liiklusest.
  - **Näide:** Filtreerida kogu HTTPS liiklust, mis on seotud hostinimega “secure.example.com”.
    - **Filtrikäsk:** host secure.example.com and tcp.port == 443

# NÄIDE HOSTINIME FILTREERIMISEST WIRESHARKIS

**Ettevõtte Võrgustruktuur:**

- **Veebiserver:** Hostinimi “webserver.company.com”
- **Tööjaam 1:** Hostinimi “workstation1.company.com”
- **Tööjaam 2:** Hostinimi “workstation2.company.com”

**Jälgimine ja Filtreerimine:**

- **Veebiserveri liiklus:** Jälgida kogu liiklust, mis on seotud veebiserveri hostinimega “webserver.company.com”.
- **Filtrikäsk:** host webserver.company.com
- **Tööjaama liiklus:** Jälgida kogu liiklust, mis on seotud tööjaama 1 hostinimega “workstation1.company.com”.
- **Filtrikäsk:** host workstation1.company.com

# KUIDAS LUUA JA KASUTADA HOSTINIME KUVAFILTREID WIRESHARKIS

1. **Wiresharki avamine ja liikluse jälgimine:**
- Käivitage Wireshark ja valige võrguliides, mida soovite jälgida.
- Vajutage nuppu “Start” liikluse jälgimiseks.
2. **DNS päringud ja hostinime tuvastamine:**
- Veenduge, et Wireshark suudab lahendada DNS päringud ja vastused, et tuvastada hostinimed ja nende vastavad IP-aadressid.
3. **Filtri määramine:**
- Sisestage filtrikäsud Wiresharki filtripaneelile ja vajutage “Enter”.
- Näiteks, sisestage host webserver.company.com kogu liikluse filtreerimiseks, mis on seotud hostinimega “webserver.company.com”.
4. **Filtri rakendamine ja analüüs:**
- Wireshark kuvab ainult need paketid, mis vastavad määratud filtrile.
- Analüüsige filtreeritud liiklust, et tuvastada probleemid või jälgida võrguaktiivsust.

# Tööstus IT turvalisus

Rahastanud Euroopa Liit
NextGenerationEU

Eesti
tuleviku heaks