CASE VR

Työskentele junassa ;)


VR
FI EN SV
Kirjaudu sisään
Valikko
Kuvittele itsesi työmatkalle
Iltaa!
Minne olet matkalla?
Kajaani
Tikkurila
Meno
Paluu
Matkustajat ja alennukset
Pe 27.10.
-
1 aikuinen
Lisää
Lemmikki
Polkupyörä
Pyörätuoli
Saattaja
Ajoneuvo
Hae matkoja
Sarjaliput
Kausiliput
Yö- ja autojunat
Yrityspalvelut

Palvelut junassa

Minkälaisia tarpeita sinulla on junamatkallesi?

Lasten kanssa matkalle

Junassa lapset pääsevät leikkimään ja liikkumaan, eivätkä eväs- tai vessatauot hidasta matkaa. Myös lastenvaunut mahtuvat junaan.

→

Esteetön juna-matkustaminen

Onko sinulla tai läheiselläsi liikkumisesteitä tai vamma, joka vaatii erityistä huomiota?

→

Työskentely junassa

Enemmän työrauhaa Ekstra-luokassa, ravintolavaunun yläkerrassa tai 2-4 hengen hytissä.

→ Ilmainen, avoin Wi-Fi

1. Kuvittele itsesi junamatkalle Kajaani – Tikkurila
2. Mikä mainio hetki tehdä rauhassa töitä
3. Kirjaudut ilmaiseen VR:n tarjoamaan Wi-Fi-verkkoon

   SSID: VR junaverkko
4. Teet töitä avaten yritykselle kriittisiä dokumentteja, kirjautuen yrityksen järjestelmiin, välillä tilaat itsellesi uusia vaatteita, tavaroita, festarilippuja verkosta, aah mitä matkustamisen helppoutta

testphp.vulnweb.com/secured/newuser.php

Aloitussivu

ACUNETIX ART

You have been introduced to our database with the above informations:

- Username: Käärijä
- Password: salasana1234
- Name: Kalle Käärijä
- Address: lähiosoite 4c5
- E-Mail: kalle.kaarija@umk.fi
- Phone number: 0987654321
- Credit card: 12345678910

Now you can login from here.

HTTP

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Delta	Source	Destination	Protocol	TCP Segment Len	Info
3…	12.47…	0.000…	ec2-44-228-249-3.us-…	AHTA1-JUSSIAH-X…	HTTP	1102	HTTP/1.1 200 OK (text/css)
4…	20.50…	0.000…	ec2-44-228-249-3.us-…	AHTA1-JUSSIAH-X…	HTTP	1288	HTTP/1.1 200 OK (text/html)
5…	33.14…	0.000…	ec2-44-228-249-3.us-…	AHTA1-JUSSIAH-X…	HTTP	1460	HTTP/1.1 200 OK (text/html)
3…	12.24…	0.001…	ec2-44-228-249-3.us-…	AHTA1-JUSSIAH-X…	HTTP	812	HTTP/1.1 200 OK (text/html)
3…	12.30…	0.016…	AHTA1-JUSSIAH-X.frit…	ec2-44-228-249-…	HTTP	351	GET /secured/style.css HTTP/1.1
3…	12.06…	0.021…	AHTA1-JUSSIAH-X.frit…	ec2-44-228-249-…	HTTP	759	POST /secured/newuser.php HTTP/1.1 (appli
5…	32.96…	0.189…	AHTA1-JUSSIAH-X.frit…	ec2-44-228-249-…	HTTP	559	POST /userinfo.php HTTP/1.1 (application/
4…	20.33…	0.225…	AHTA1-JUSSIAH-X.frit…	ec2-44-228-249-…	HTTP	440	GET /login.php HTTP/1.1

```
POST /secured/newuser.php HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): POST /secured/newuser.php HTTP/1.1\r\n]
    [POST /secured/newuser.php HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Request Method: POST
  Request URI: /secured/newuser.php
  Request Version: HTTP/1.1
Host: testphp.vulnweb.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: fi,fi-FI;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 211\r\n
Origin: http://testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Referer: http://testphp.vulnweb.com/signup.php\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/secured/newuser.php]
[HTTP request 1/4]
[Response in frame: 317]
[Next request in frame: 319]
File Data: 211 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uuname" = "Käärijä"
  Form item: "upass" = "salasana1234"
  Form item: "upass2" = "salasana1234"
  Form item: "urname" = "Kalle Käärijä"
  Form item: "ucc" = "12345678910"
  Form item: "uemail" = "kalle.kaarija@umk.fi"
  Form item: "uphone" = "0987654321"
```

Hypertext Transfer Protocol: Protocol

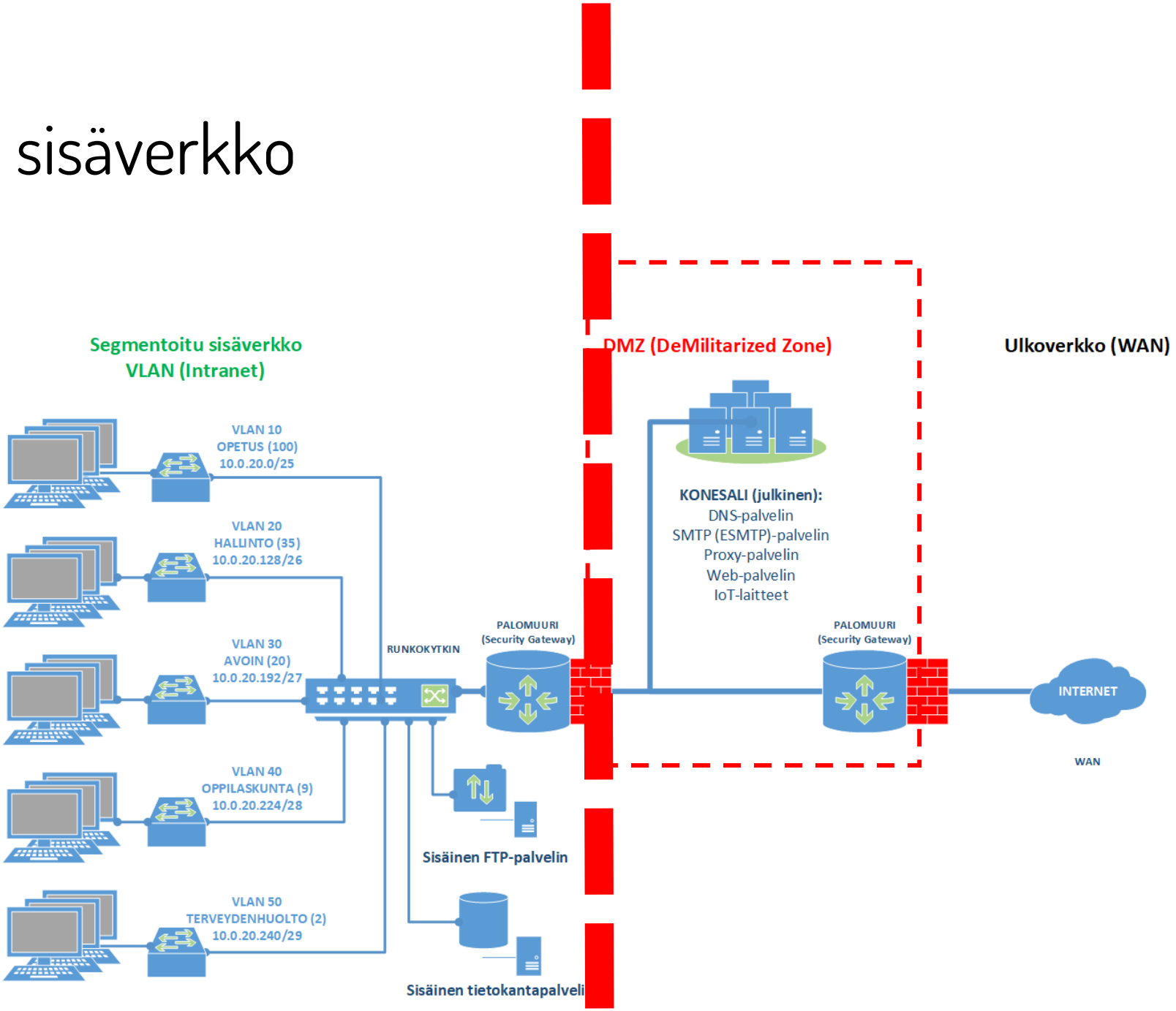
Mitä tapahtui?

KAMK • University of Applied Sciences

Lähiverkko eli sisäverkko

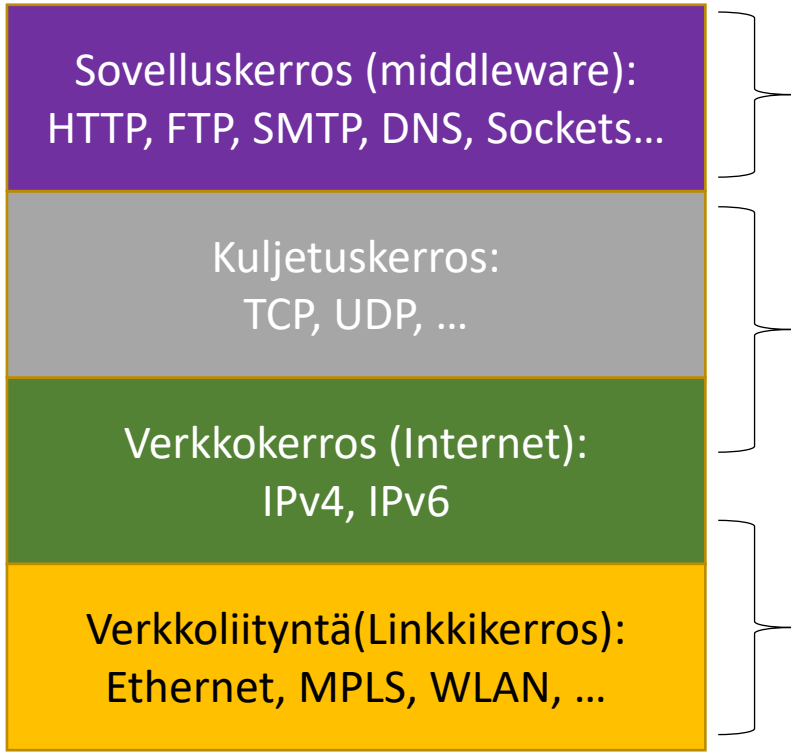
Mikäli päästään samaan lähiverkkoon (sisäverkkoon) olemme päässeet ohittamaan palomuurin eli keittiön kautta sisään

Millä TCP/IP-mallin kerroksella lähiverkko, LAN, Ethernet toimii?



KAMK • University of Applied Sciences

TCP/IP -malli



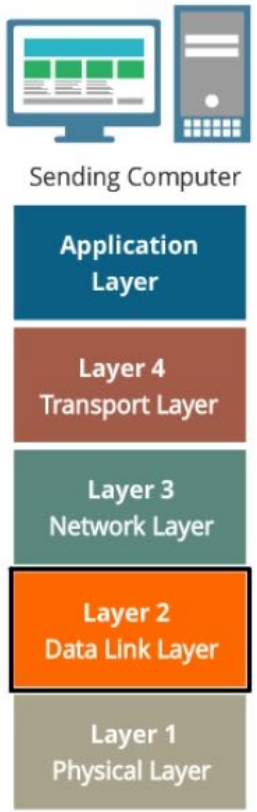
Asiakas/palvelinsovellukset,
palveluarkkitehtuurit

Tiedonsiirto päästä päähän (**IP-osoitteet**),
Internetin yli (end to end)

Tiedonsiirto yhden linkin yli (**MAC-osoitteet**)
Esim. lähiverkon tiedonsiirto

Ethernet-lähiverkko

Lähettävä pää



Layer 2

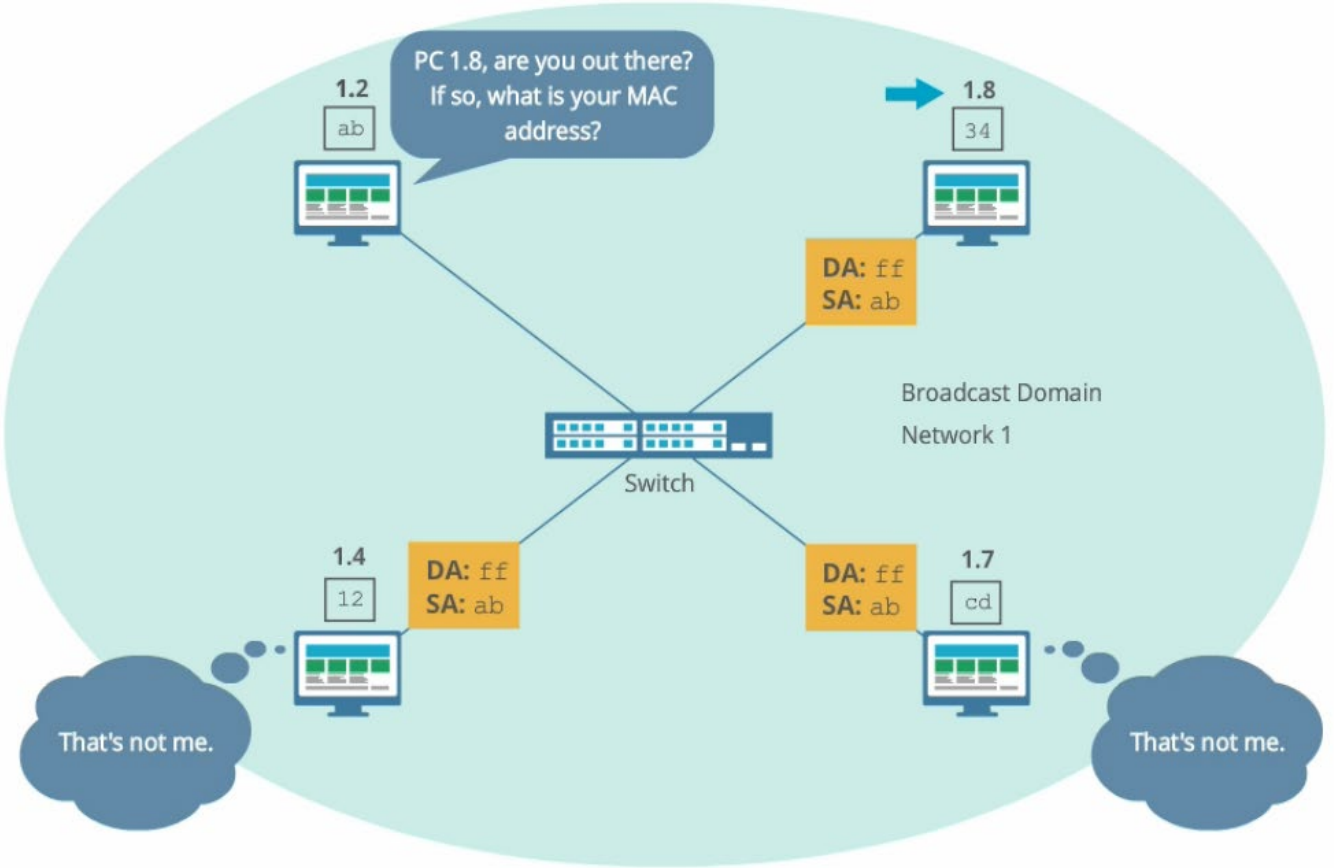
Data Link Layer – siirtoyhteyskerros

- **Kehystää** verkkokerroksesta (Network Layer) tulleen **paketin** kehykseen (Frame)
- Kehys pitää sisällään **lähettäjän ja vastaanottajan fyysisen osoitteen (MAC-osoite)**, joilla kehysten (frame) välitys lähiverkossa (Ethernet) tapahtuu.

KAMK • University of Applied Sciences

ARP – Address Resolution Protocol

- **Lähettävä tietokone tarvitsee** siis **vastaanottajan MAC-osoitteen** tietoonsa, jotta se voi kommunikoida vastaanottajan kanssa **lähiverkossa (LAN).**
- **Saadakseen MAC-osoitteen** tietoonsa se käyttää hyväkseen vastaanottajan IP-osoitetta lähettämässään **ARP-kysely**ssä



MITM hyökkäys ARP poisoning -menetelmällä

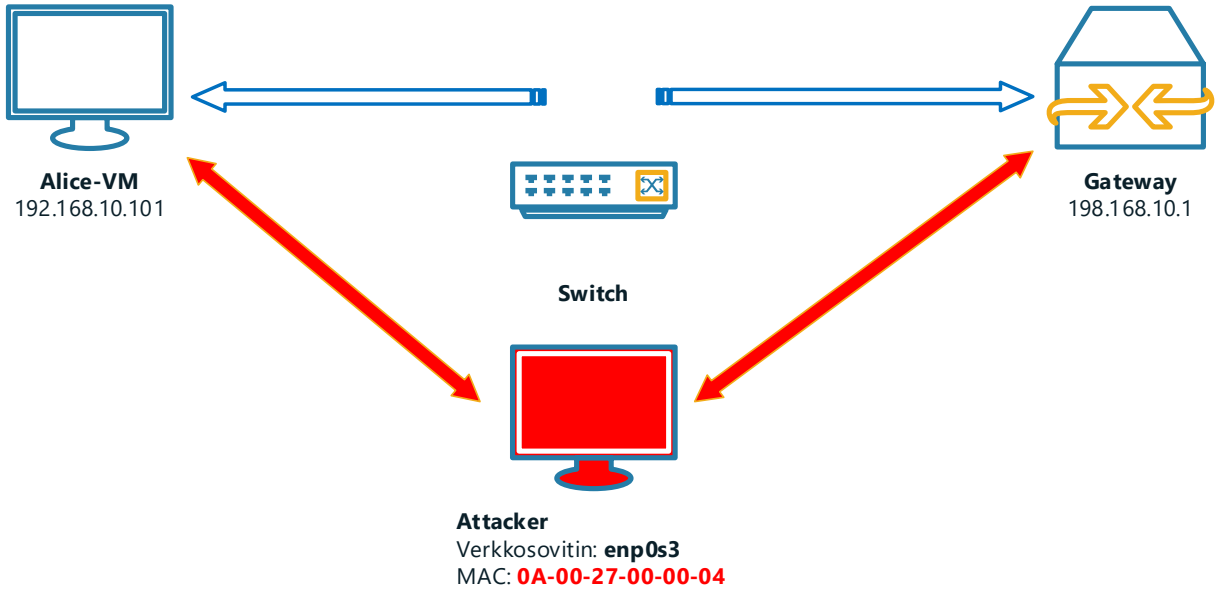
- ARP poisoning on mahdollinen, mikäli hyökkääjä pääsee käsiksi sisäverkkoon eli LAN:iin (Local Area Network)
- Hyökkääjä laittaa ip-forward komennolla pakettien välityksen päälle
- Hyökkääjä lähettää väärennettyjä ARP-vastauksia uhrilaitteille, jolloin niiden ARP-tauluihin päivittyy hyökkääjän verkkosovittimen MAC-osoite
- Kytkin välittää kehyksiä päivittyneiden MAC-osoitteiden perusteella hyökkääjän koneen kautta → **Man In The Middle**

Alicen ARP-taulu:
Interface: 192.168.10.101 --- 0x3

Internet Address	Physical Address	Type
192.168.10.255	ff-ff-ff-ff-ff-ff	static
192.168.10.1	**0A-00-27-00-00-04**	dynamic

Gatewayn ARP-taulu:
Interface: 192.168.10.1 --- 0x3

Internet Address	Physical Address	Type
192.168.10.255	ff-ff-ff-ff-ff-ff	static
192.168.10.101	**0A-00-27-00-00-04**	dynamic

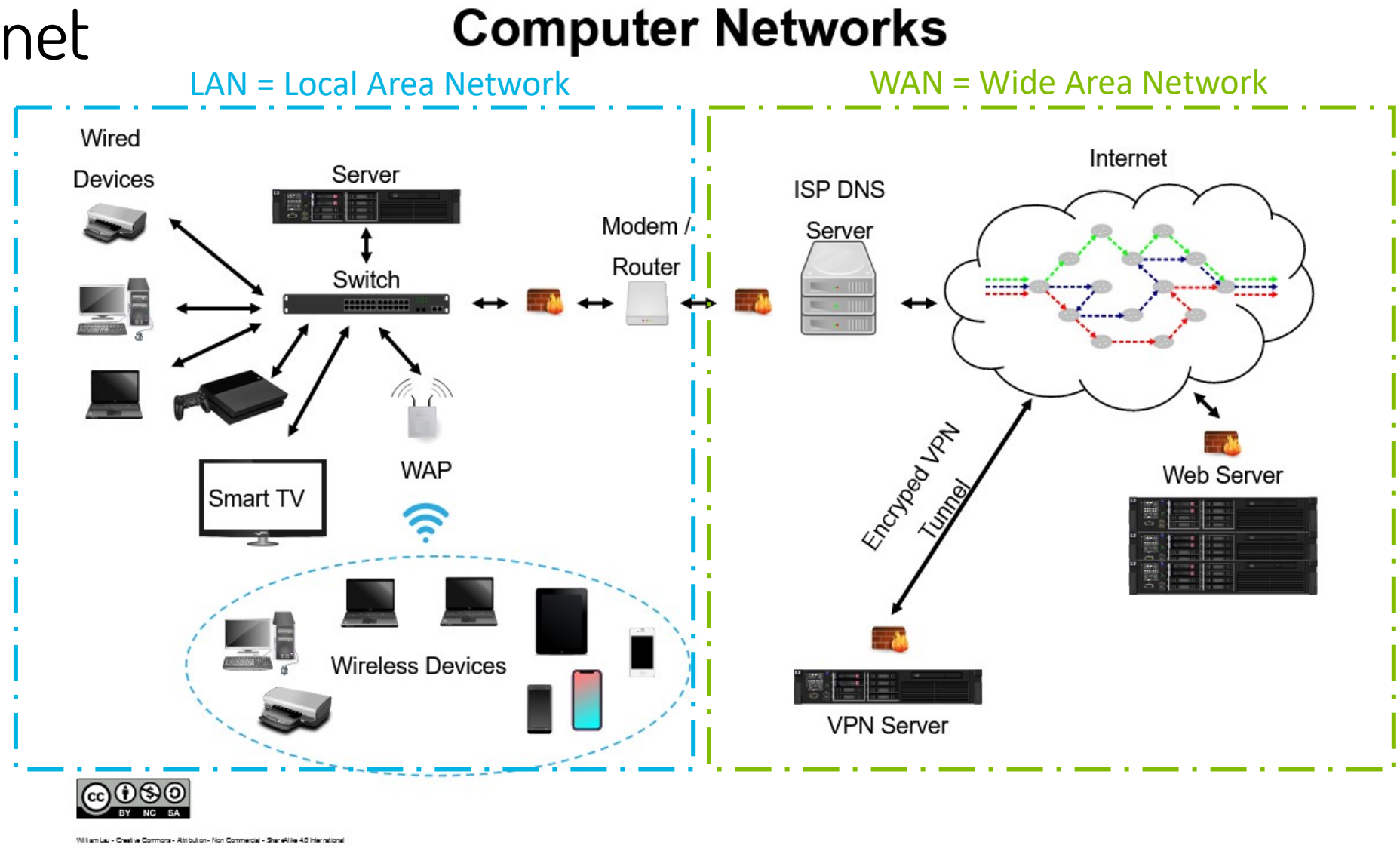


$ cat /proc/sys/net/ipv4/ip_forward

$ sudo arpspoof -i **enp0s3** -t 192.168.10.101 192.168.10.1
$ sudo arpspoof -i **enp0s3** -t 192.168.10.1 192.168.10.101

KAMK • University of Applied Sciences

Internet



KAMK • University of Applied Sciences

Lähteet

- https://learningportal.juniper.net/juniper/user_activity_info.aspx?id=769
- https://www.varonis.com/blog/arp-poisoning
- https://linuxhint.com/arp_spoofing_using_man_in_the_middle_attack/