KAMK • University of Applied Sciences

Yhteys- ja sovellusprotokollat

Layer 4 – Layer 7

Wireshark demot: Telnet ja HTTP

Jussi Ala-Hiiro

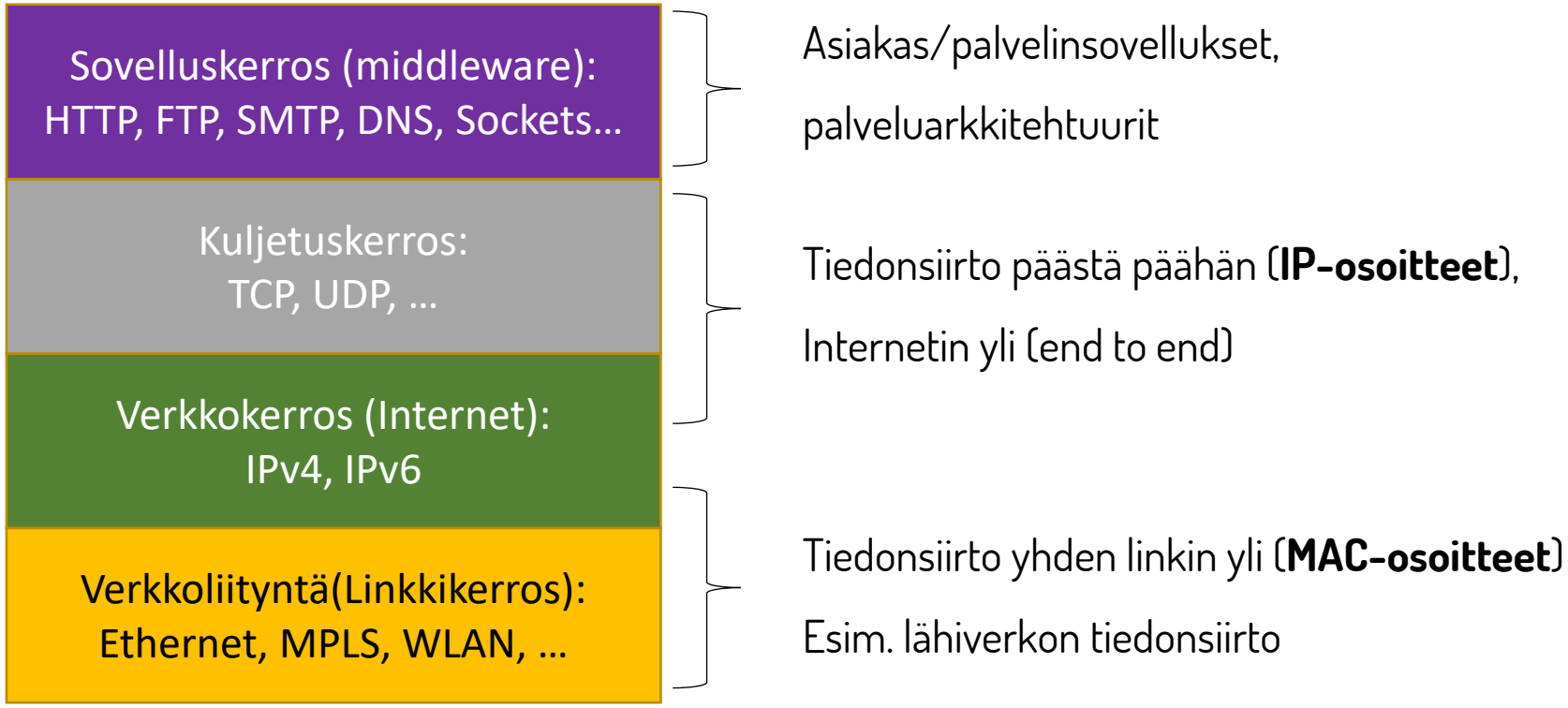
KAMK • University of Applied Sciences

Kertauksena: OSI-malli

Layer		Typical Use	Protocols
7	**Application**	End User Layer	HTTP, HTTPS, FTP, SSH, DNS
6	**Presentation**	Syntax Layer	TLS(SSL), SSH, IMAP, MPEG, JPEG
5	**Session**	Sync & Send Layer	APIs, Sockets
4	**Transport**	End-to-end Connections	TCP, UDP, QUIC
3	**Network**	Packets	IP, ICMP, IPSec, IGMP
2	**Data Link**	Frames	Ethernet, PPP, Switch
1	**Physical**	Physical Structure	Fiber, Access Points, Copper Cabling

KAMK • University of Applied Sciences

Kertauksena: TCP/IP -malli



KAMK • University of Applied Sciences

IETF – The Internet Engineering Task Force

https://www.ietf.org/

- **Perustettu 1986**

*The **overall goal** of the IETF is **to make the Internet work better.***
*Its **mission is to produce high quality, relevant technical** and **engineering documents** that **influence the way people design, use**, and **manage the Internet** in such a way as to make the Internet work better.*

*These documents include **protocol standards**, **best current practices**, and **informational documents** of various kinds.*

- **IETF**-työryhmät laativat **RFC-dokumentteja** (Request for Comments), jotka ovat ohjeistuksia, protokollia tai standardeja Internetin toimintaan liittyen

Internet Standardeja

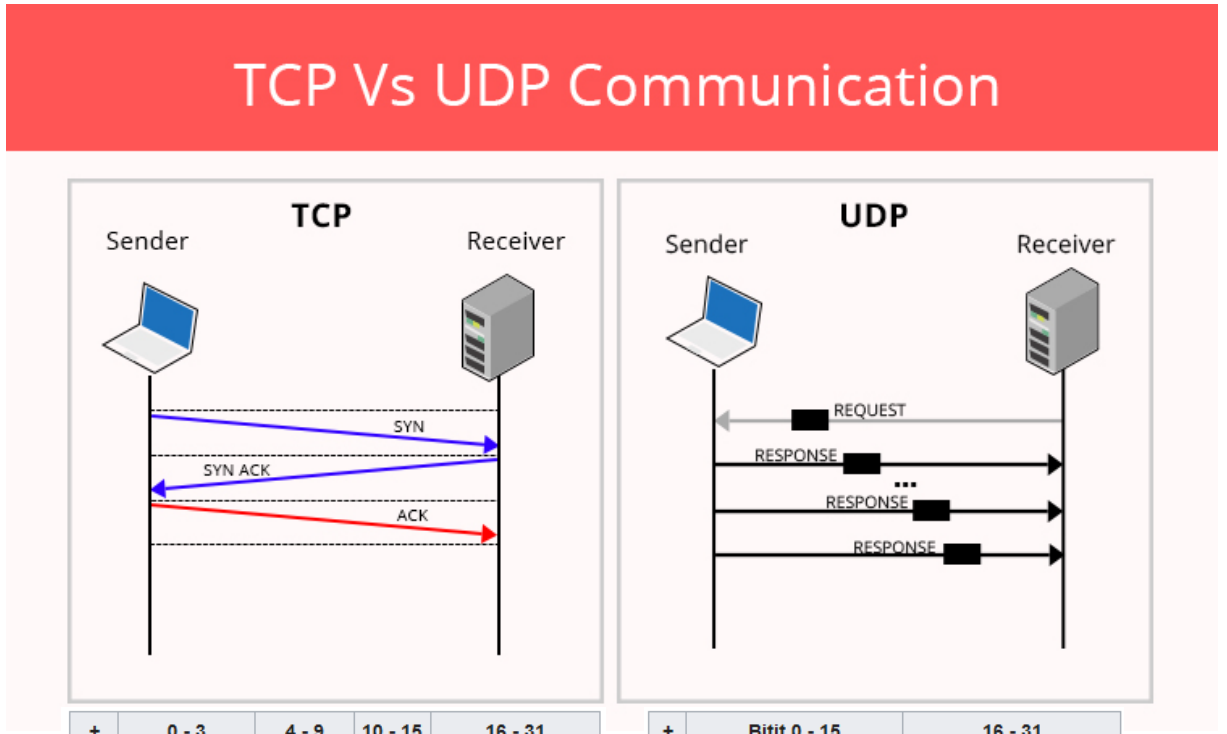
• RFC 1	IMP (Arpanet)	1969
• RFC 768	UDP	1980
• (RFC 793)	TCP	1981
• RFC 9293	TCP uudistettu	2022
• RFC 791	Internet Protocol	1981
• RFC 792	ICMP	1981
• RFC 854	Telnet	1983
• RFC 1034	DNS	1987
• RFC 2068	HTTP/1.1	1997
• RFC 8446	TLS 1.3	2020
• RFC 9000	QUIC	2021

KAMK • University of Applied Sciences

Layer 4, Transport Layer – kuljetuskerroksen käyttämät protokollat TCP ja UDP

TCP

- **Yhteydellinen** protokolla
- **Varmistaa** jokaisen **paketin perille menon kuittauksella**
- Jos **ei kuittausta**, **paketin uudelleen lähetys**
- **HUOM!** Paketin tippuessa **TCP-liikenne pysähtyy**, kunnes puuttuva paketti on tullut : **Head of Line Blocking**
- Järjestää saapuneet **paketit oikeaan järjestykseen**
- Käytetään, kun vaaditaan varmaa datan välitystä



+	0 - 3	4 - 9	10 - 15	16 - 31
0	Lähdeportti			Kohdeportti
32	Järjestysnumero			
64	Kuittausnumero			
96	Otsikon pituus	Reserved	Liput	Ikkunan koko
128	Tarkistussumma			Kiireellisyysosoitin
160	Optiot ja täyte			
192	Data			

+	Bitit 0 - 15	16 - 31
0	Lähdeosoitteen portti	Kohdeosoitteen portti
32	Datan koko	Tarkistussumma
64	Data	

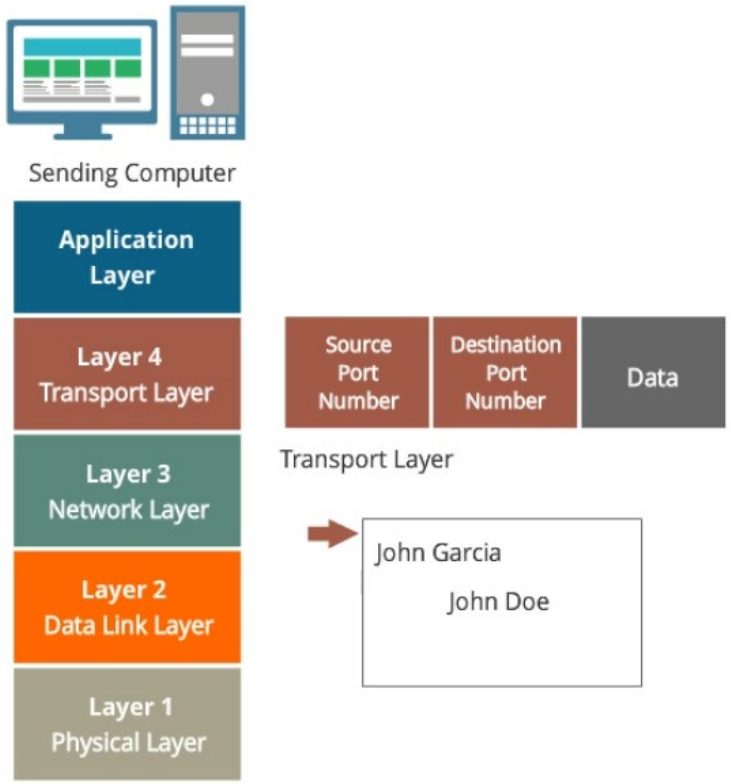
UDP

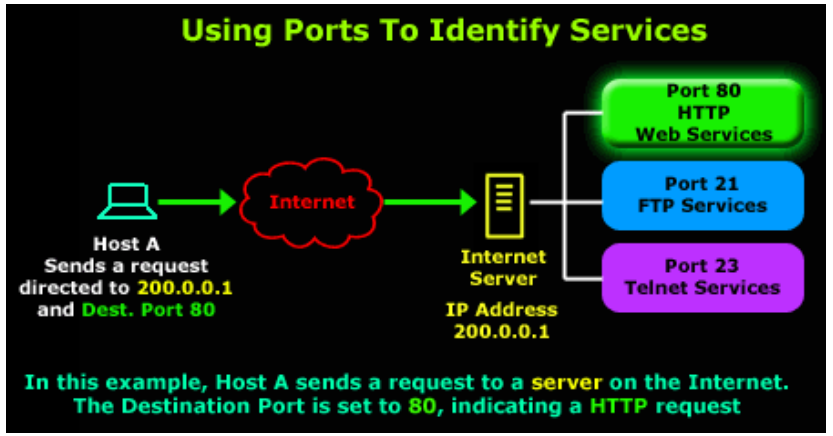
- **Yhteydetön** protokolla
- Ei kättelyitä, ei kuittauksia datan perille pääsystä.
- Kevyempi datagrammi
- käytössä **nopeaa datansiirtoa vaativissa sovelluksissa**, joissa datapakettien hukkumisesta matkalle ei ole suurta merkitystä.

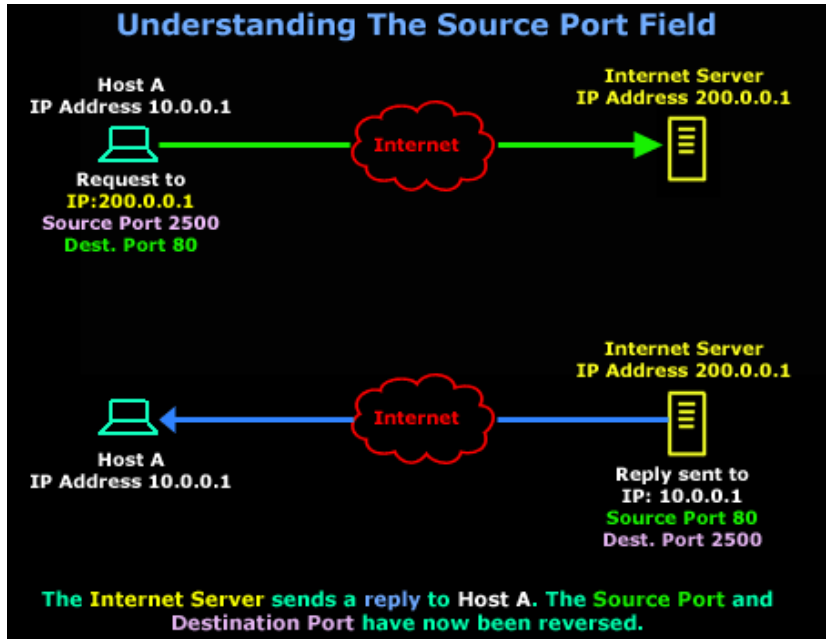
KAMK • University of Applied Sciences

Kuljetuskerroksen (Layer 4) portit

Lähettävä pää







https://www.firewall.cx/networking-topics/protocols/tcp/133-tcp-source-destination-ports.html

KAMK • University of Applied Sciences

Netstat (Network Statistics) -komento

- Komentokehote CMD (Command Prompt): **Netstat**
- Yksityiskohtainen tieto auki olevista TCP-yhteyksistä sekä kuuntelulla olevista UDP-porteista

  - **netstat** [**-a**] [**-b**] [**-e**] [**-f**] [**-n**] [**-o**] [**-p** *protocol*] [**-r**] [**-s**] [**-t**] [**-x**] [**-y**] [*time_interval*] [**/?**]

- https://www.lifewire.com/netstat-command-2618098

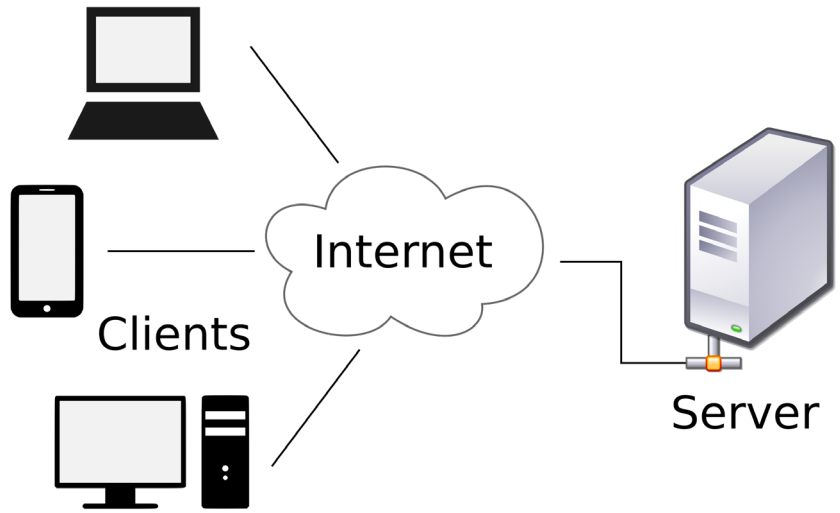
KAMK • University
of Applied Sciences

www.kamk.fi

KAMK • University of Applied Sciences

Telnet (**Tel**etype **Net**work)

- Internetin **Client – Server –rakenteen** johdosta jo aikojen alussa oli tarve etäyhteyden muodostamiseen palvelimelle – esim. konfigurointia varten
- Telnet (1969) oli pitkään ratkaisu etäyhteyden muodostamiseen
- Tietoturvattomuuden vuoksi korvautunut SSH:lla etäyhteyksien muodostamisessa
- Edelleenkin käytössä yksinkertaisena työkaluna yhteyksien tutkimisessa



Kuvan lähde: https://en.wikipedia.org/wiki/Client%E2%80%93server_model

KAMK • University of Applied Sciences

Telnet (**Tel**etype **Net**work)

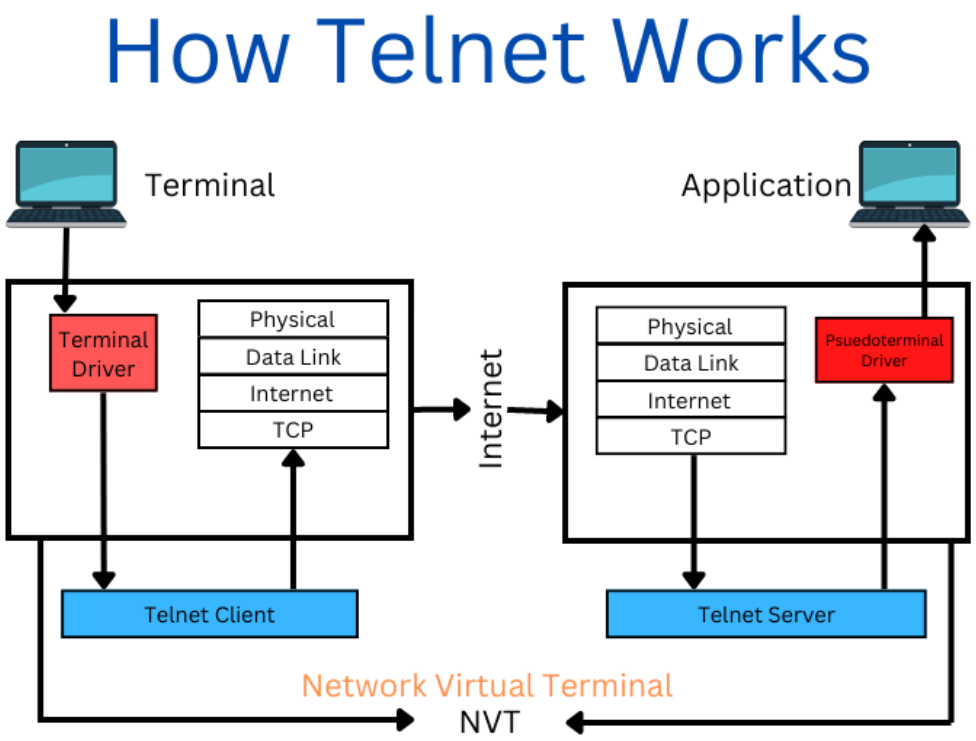
- Telnetillä voi
  - Tarkistaa avoimia portteja
  - Editoida tiedostoja, ajaa ohjelmia
  - Konfiguroida verkkolaitteita (kytkimet, reitittimet)

- Telnet syntaksi komentokehotteessa:

  telnet *hostname port*

  Esim: **telnet geekflare.com 80**

- https://geekflare.com/telnet-commands-to-troubleshoot-connection-issues/



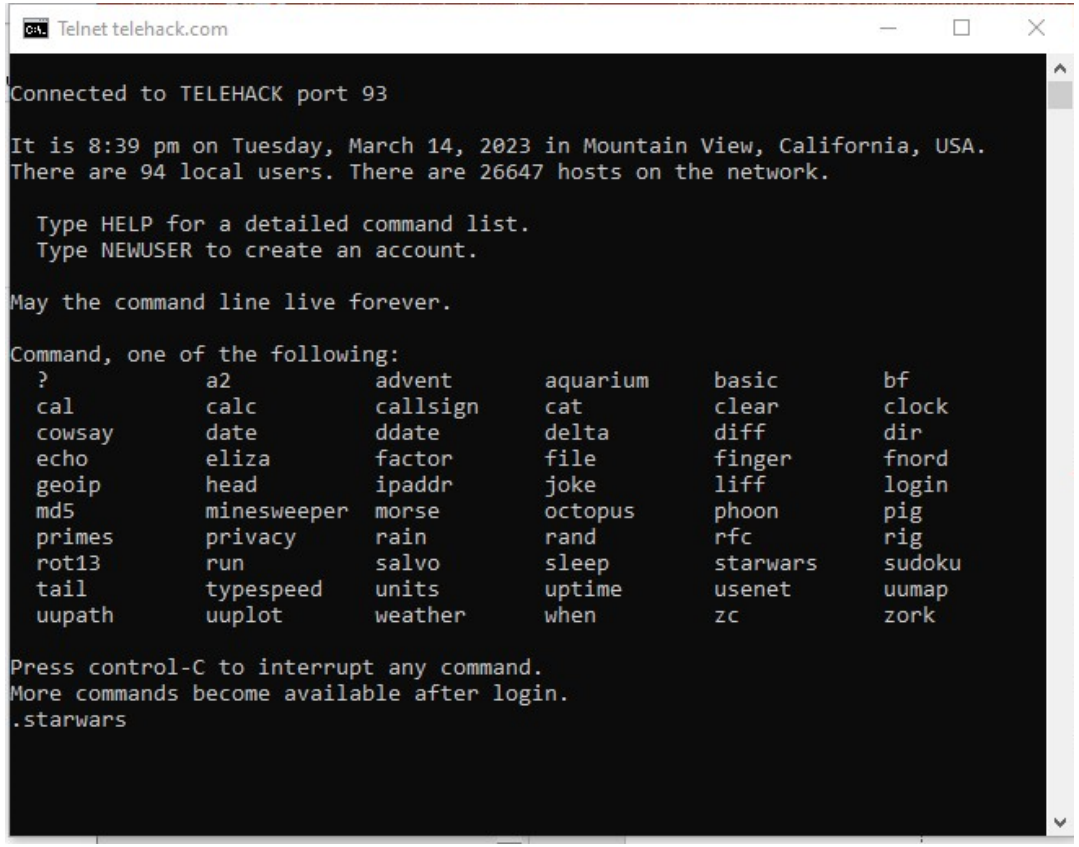
Kuvan lähde: https://geekflare.com/telnet-commands-to-troubleshoot-connection-issues/

KAMK • University of Applied Sciences

WIRESHARK DEMO 1: Telnet

Wireshark

1. Käynnistä Wireshark ja laita Capture päälle
2. Avaa komentokehote ja kirjoita: **telnet telehack.com**
3. Telnet yhteys avautuu, kirjoita **starwars** ja paina Enter

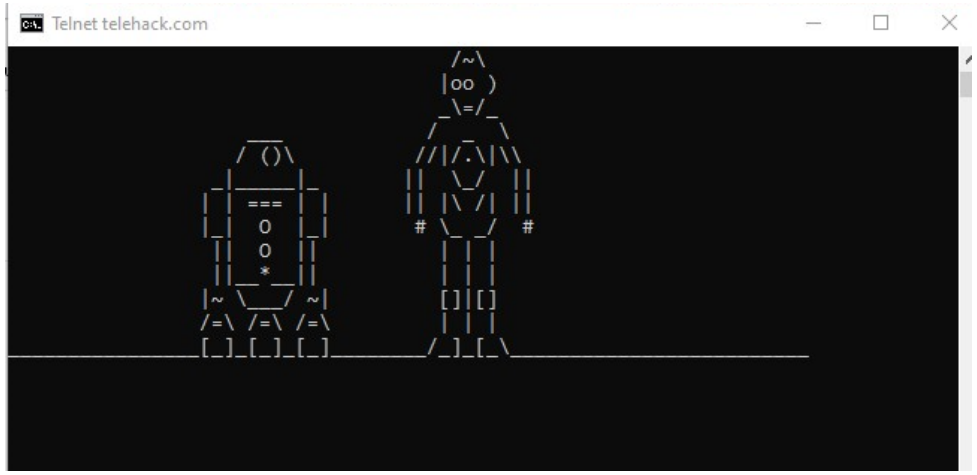


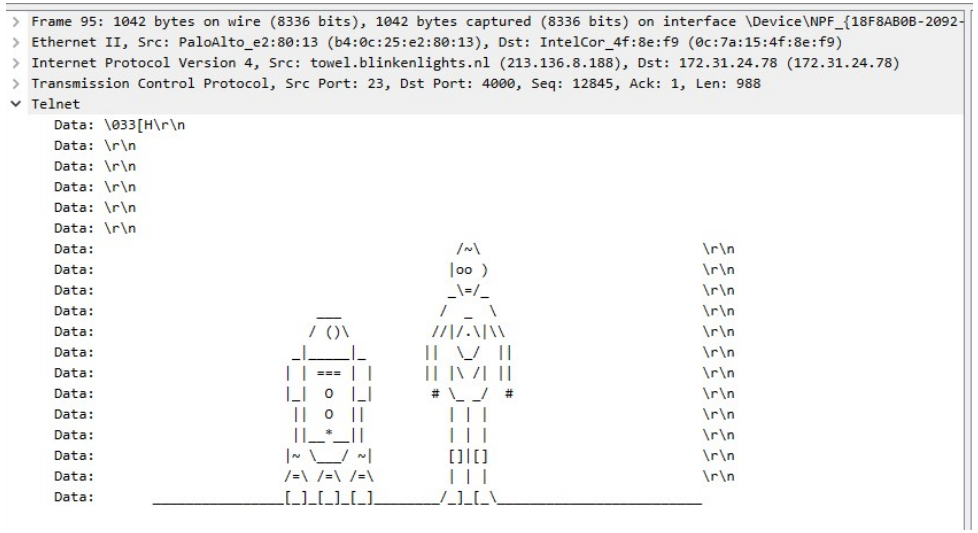
KAMK • University of Applied Sciences

WIRESHARK DEMO 1: Telnet

Wireshark

4. Kerää Wire Sharkilla sopiva määrä pakettiliikennettä ja pysäytä tallennus
5. Filteröi data kirjoittamalla kohtaan *Apply a display filter* **telnet**
6. Mitä voit päätellä telnetillä siirretyn datan tietoturvasta?

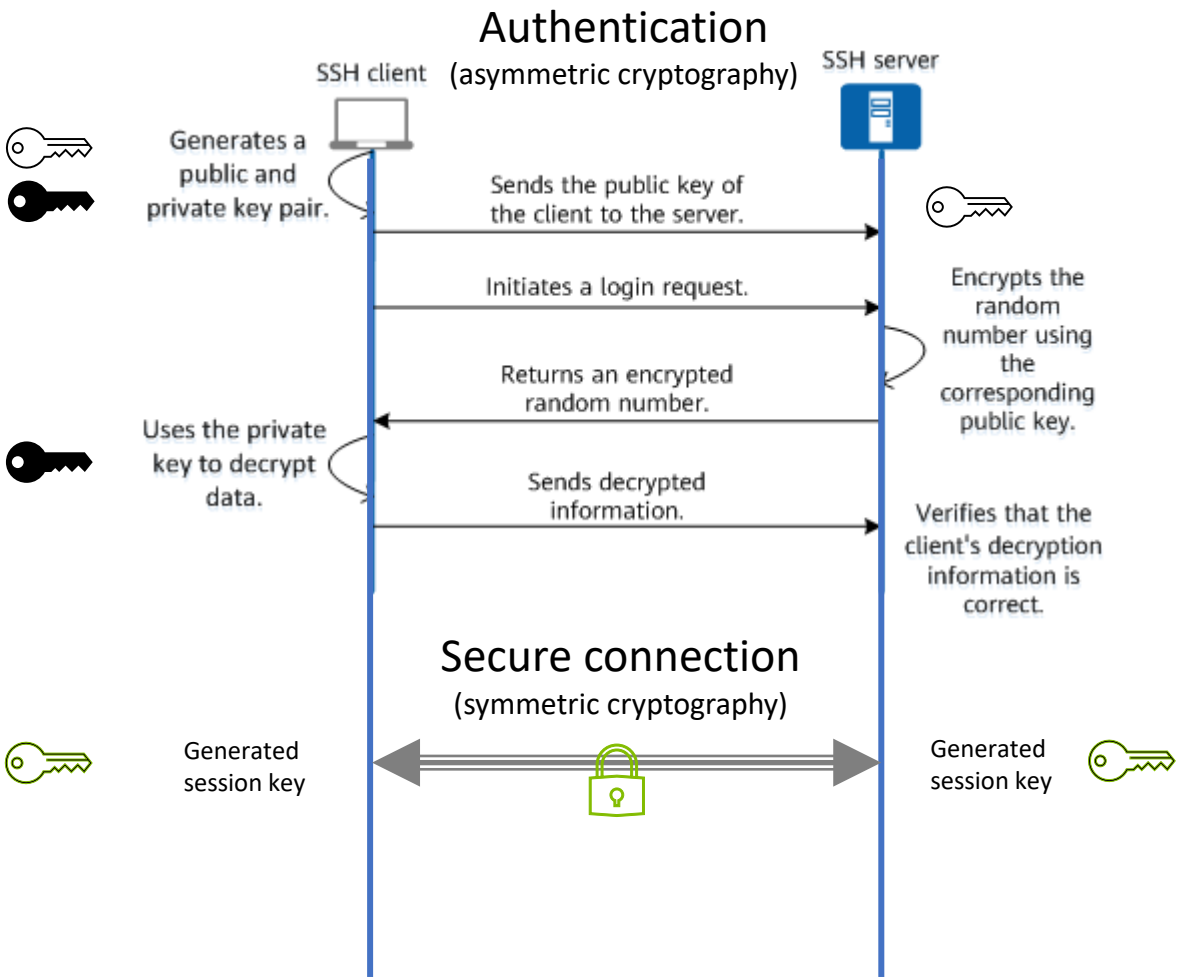




KAMK • University of Applied Sciences

SSH - Secure Shell

- Etäyhteyksiin aiemmin käytetyn Telnetin korvannut, tietoturvallinen tapa ottaa etäyhteys palvelimeen
- Ensimmäisen version (SSH-1) kehitti vuonna 1995 tekn.lis. Tatu Ylönen TKK
- Nykyisin käytössä SSH-2 versio
- **Tunnistautuminen suositellaan suoritettavaksi avainparin** (key authentication) **avulla** (epäsymmetrinen salaus)
- Siinä asiakaskoneella (SSH Client) luodaan avainpari (private key ja public key) , jonka yksityinen osa (private key) jätetään omalle koneelle, mutta julkinen osa (public key) siirretään palvelimille (SSH servers), joilla avainpari tunnistusta halutaan käyttää.
- Windows ympäristössä **Putty**
- Linux ympäristössä **Open SSH**

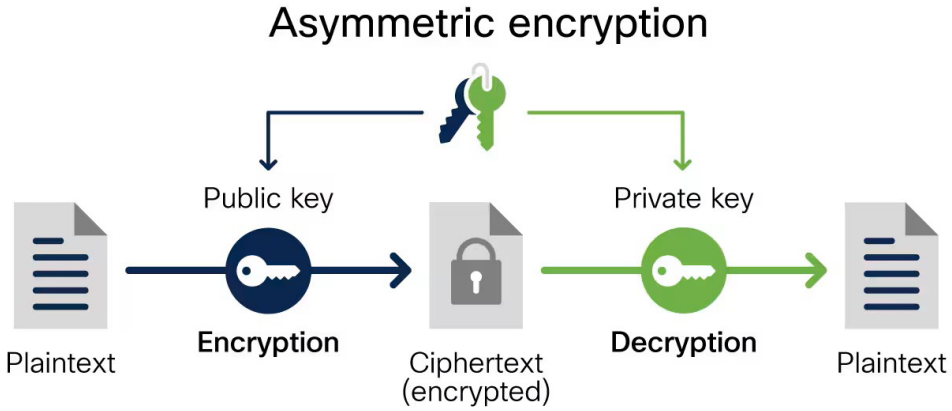


Kuva muokattu lähteestä:
https://info.support.huawei.com/info-finder/encyclopedia/en/SSH.html

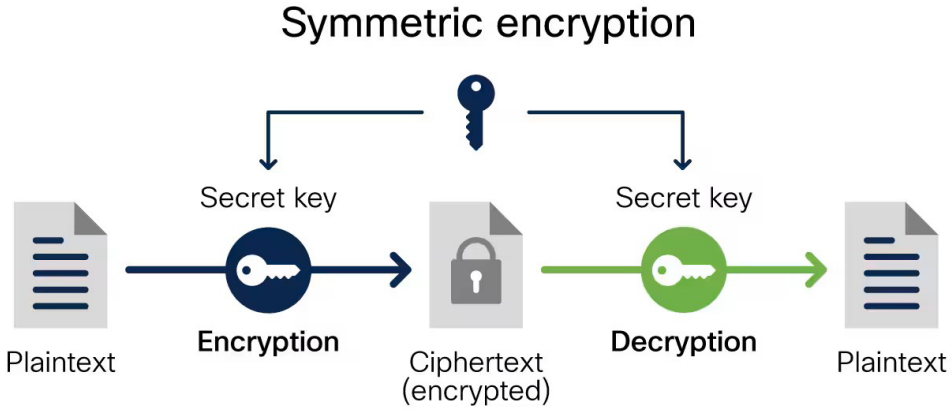
KAMK • University of Applied Sciences

Epäsymmetrinen ja symmetrinen salaus

- **Asymmetric encryption** uses two separate keys: a public key and a private key.
  - Often a public key is used to encrypt the data while a private key is required to decrypt the data.
  - The private key is only given to users with authorized access.
  - As a result, asymmetric encryption can be more effective, but it is also more costly.



- **Symmetric encryption** uses the same key for encryption and decryption.
  - Because it uses the same key, symmetric encryption can be more cost effective for the security it provides.
  - That said, it is important to invest more in securely storing data when using symmetric encryption.



Kuvien lähde: https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~encryption-algorithms

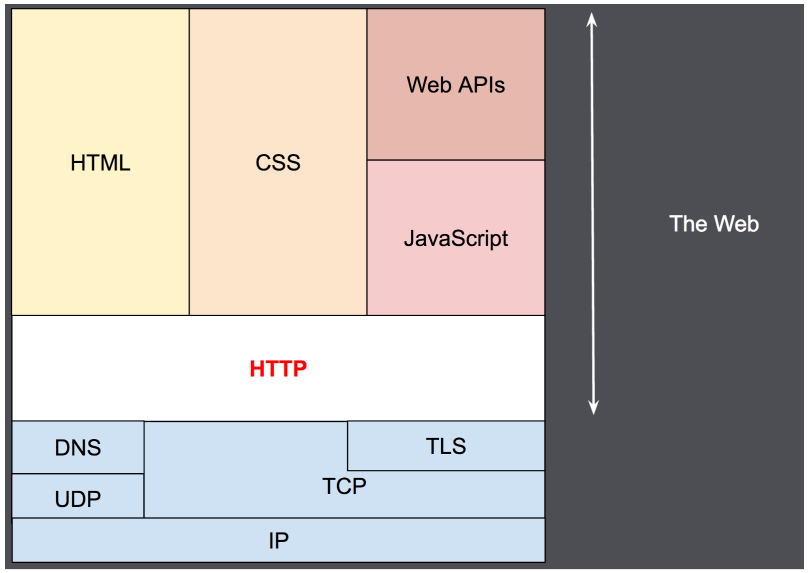
KAMK • University
of Applied Sciences

www.kamk.fi

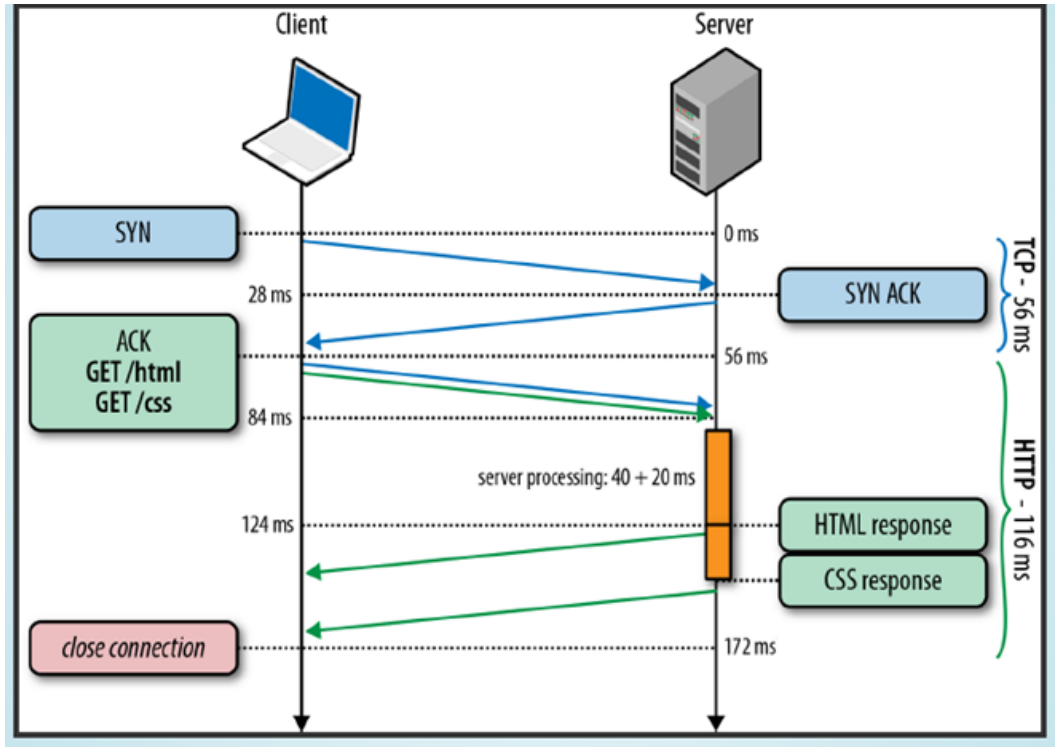
KAMK • University of Applied Sciences

HTTP Hyper Text Transfer Protocol

- Sovelluskerroksen **protokolla, jota selaimet** ja **WWW-palvelimet** käyttävät **tiedonsiirtoon**
  - HTTP/0.9 julkaistu 1989
  - HTTP/1.1 RFC 2068 julkaistu 1997
  - HTTP/2 RFC 7540 julkaistu 2015
  - HTTP/3 RFC 9114 julkaistu 2022



Kuvan lähde: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

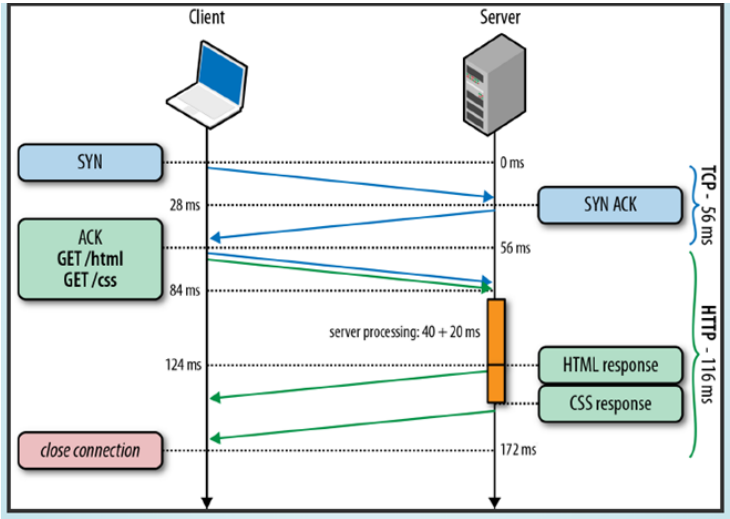


Kuvan lähde: https://www.concurrency.com/blog/june-2019/why-http-is-not-suitable-for-iot-applications

KAMK • University of Applied Sciences

HTTP/1.1 – Standardoitu protokolla

- HTTP/1.1 –versio oli ensimmäinen standardoitu http-protokolla
- Se tarjosi monia parannuksia aiempiin versioihin mm.
  - TCP-yhteyden ylläpito (Keep-Alive)
  - Pipelining
  - Chunked responses
  - Välimuistimekanismi (cache)
  - Ladattavan sisällön määritys (Content negotiation)
  - Host header – eri (ali)domainien lataaminen samasta IP-osoitteesta
  - Protocol Upgrade Header, jota käytetään mm. **websocketissa**
- HTTP/1.1 toimii pohjana monille web-sovelluksille (API)
- Lisätietoa HTTP-protokollasta https://developer.mozilla.org/en-US/docs/Web/HTTP



Kuvan lähde: https://www.concurrency.com/blog/june-2019/why-http-is-not-suitable-for-iot-applications

```
GET /index.html HTTP/1.1
Host: www.example.com
Connection: upgrade
Upgrade: example/1, foo/2
```

```
Connection: Upgrade
Upgrade: websocket
```

KAMK • University of Applied Sciences

HTTP Hyper Text Transfer Protocol

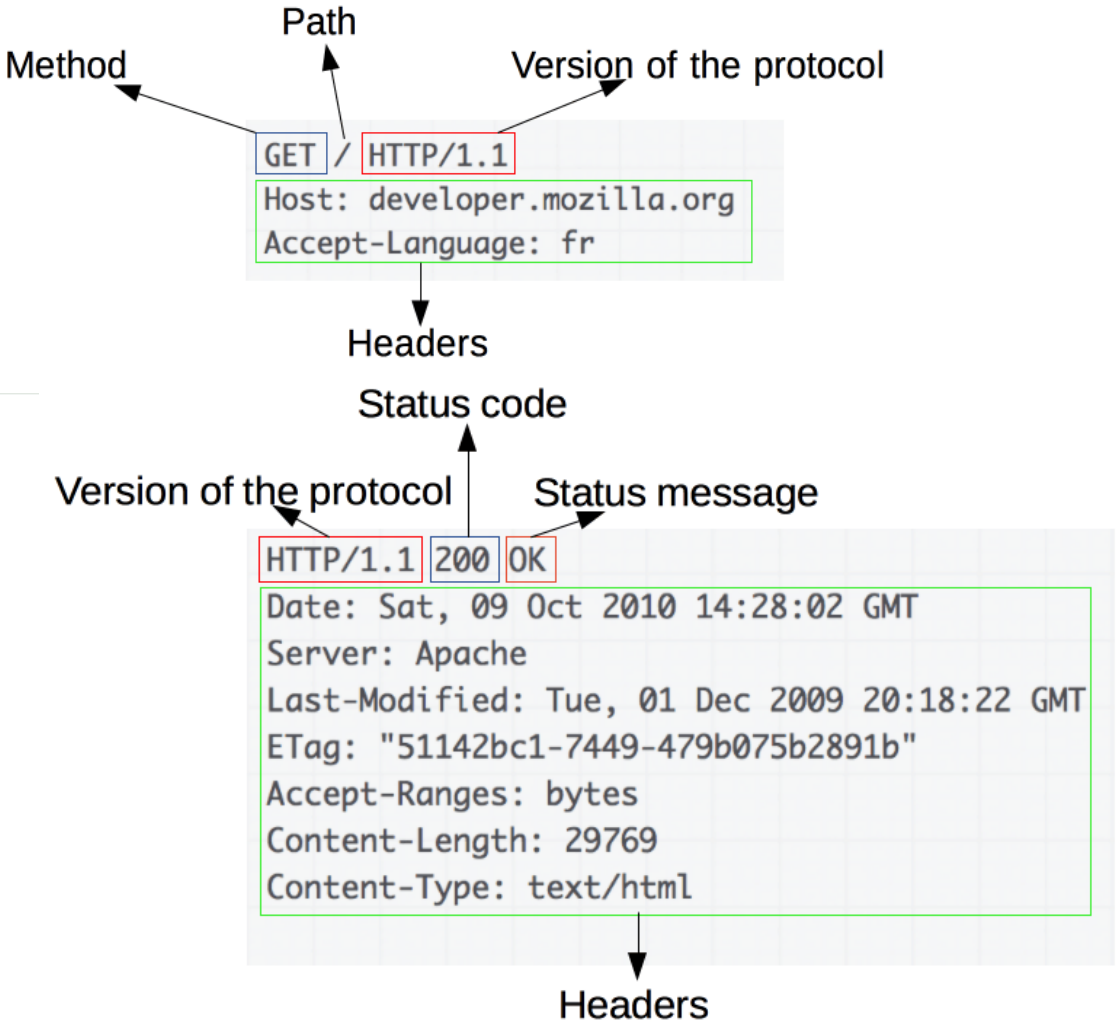
HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

Status codes indicate the result of the HTTP request.

STATUS CODE	EXPLANATION
200 - OK	The request succeeded.
204 - No Content	The document contains no data.
301 - Moved Permanently	The resource has permanently moved to a different URI.
401 - Not Authorized	The request needs user authentication.
403 - Forbidden	The server has refused to fulfill the request.
404 - Not Found	The requested resource does not exist on the server.
408 - Request Timeout	The client failed to send a request in the time allowed by the server.
500 - Server Error	Due to a malfunctioning script, server configuration error or similar.

Kuvien lähde: https://www.devopsschool.com/blog/understanding-rest-http-method-get-post-put-head-delete/



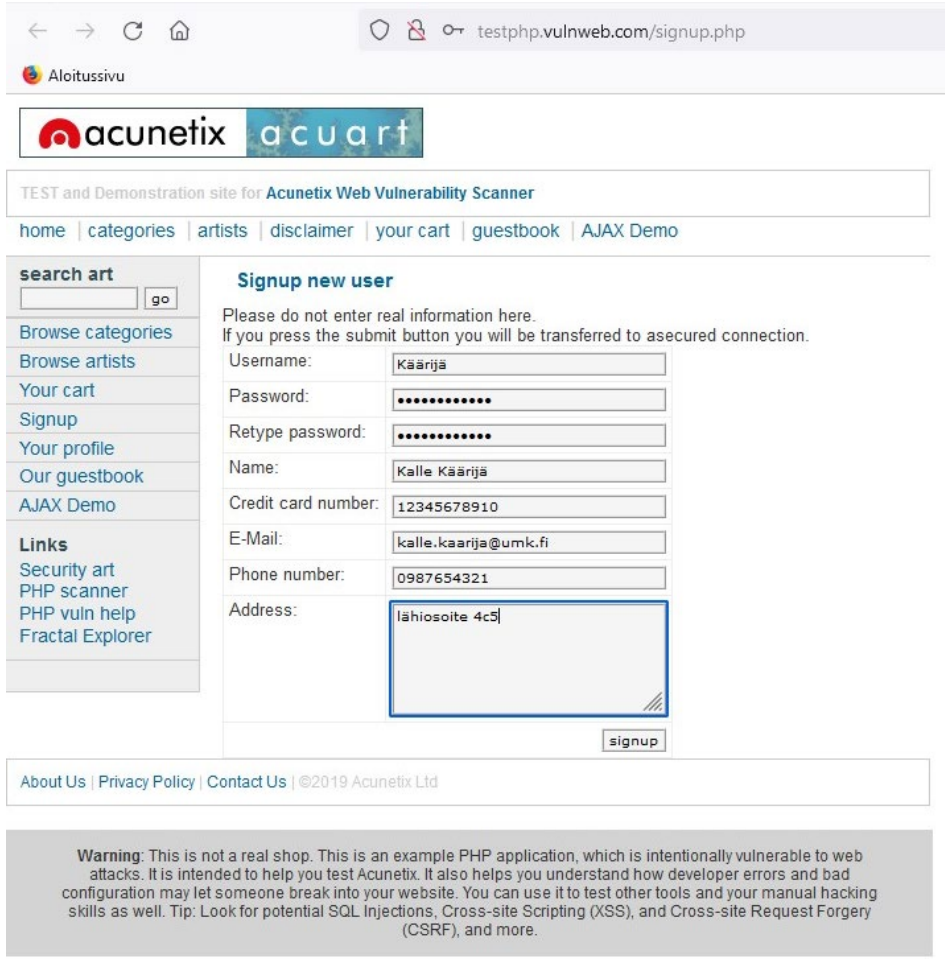
Kuvien lähde: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

KAMK • University of Applied Sciences

WIRESHARK DEMO 2: HTTP

Wireshark

1. Käynnistä Wireshark ja laita Capture päälle
2. Avaa selaimessa sivu http://testphp.vulnweb.com/signup.php
3. Kirjaa tiedot kenttiin ja paina signup-painiketta

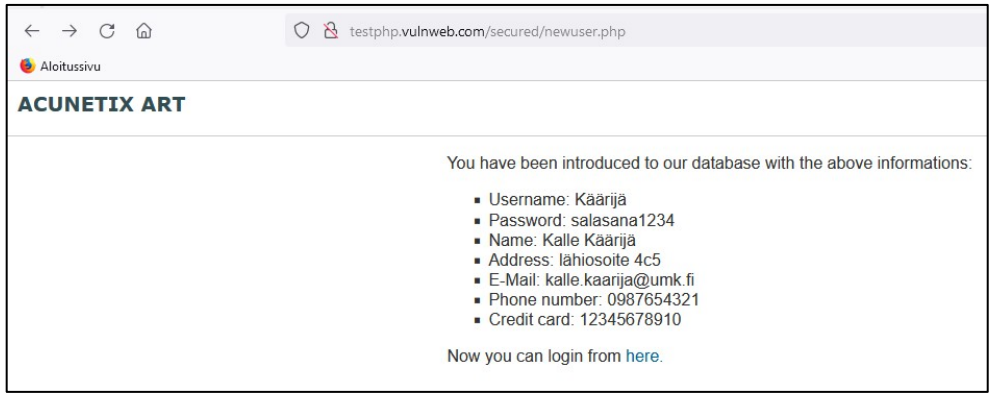


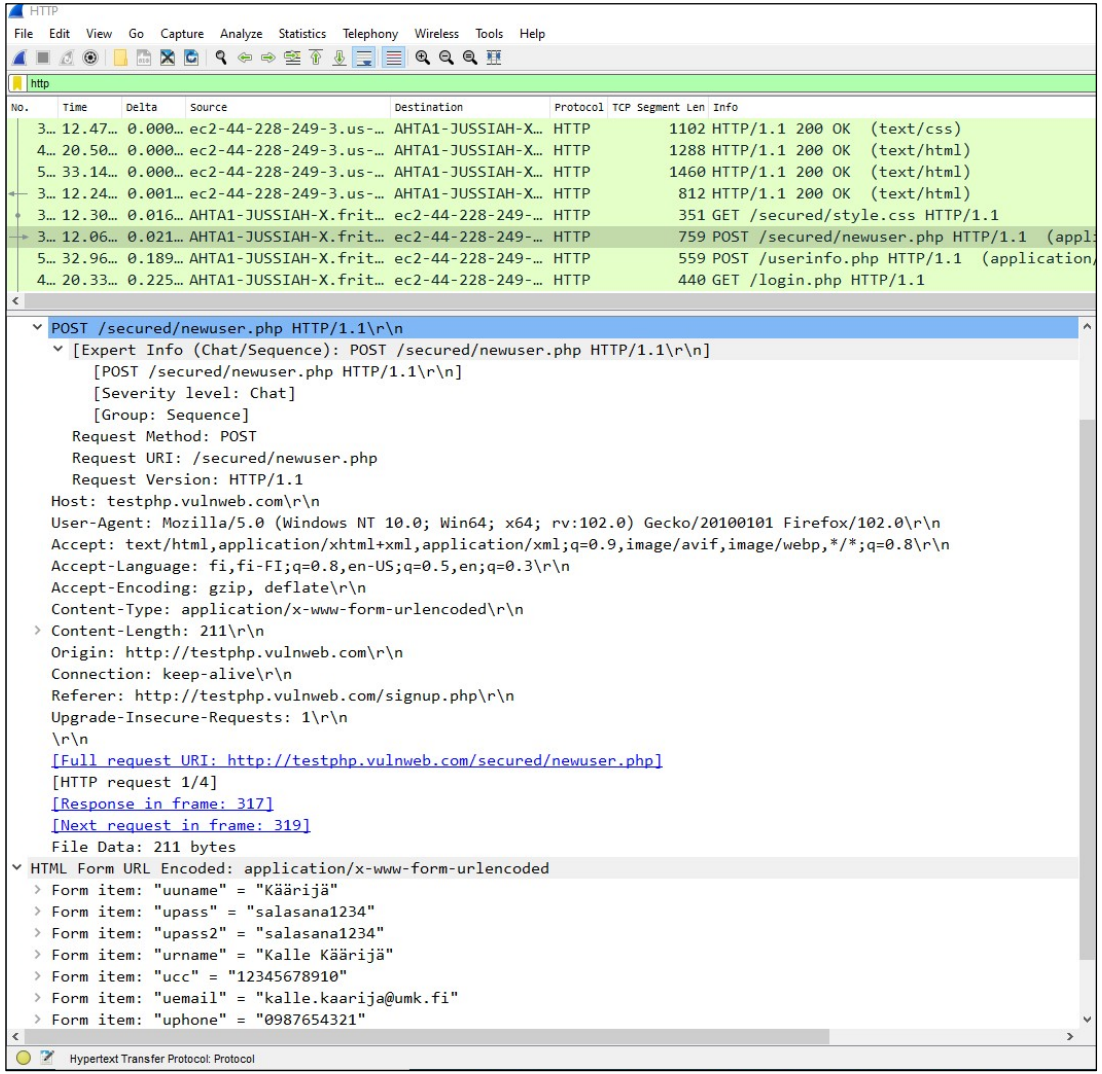
KAMK • University of Applied Sciences

WIRESHARK DEMO 2: HTTP

Wireshark

4. Pysäytä Wire Shark tallennus
5. Filteröi data kirjoittamalla kohtaan *Apply a display filter* **http** ja paina Enter
6. Etsi kaapatusta datasta, löydätkö lähettämäsi salasanan ja muut sensitiiviset tietosi?
7. Mitä voit päätellä HTTP-sivun tietoturvasta?

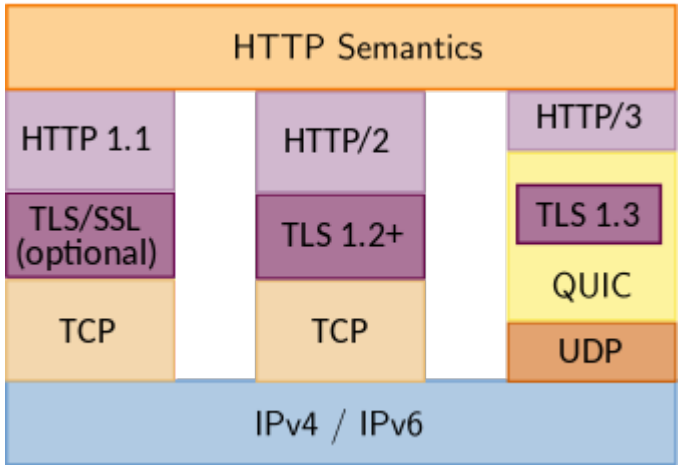


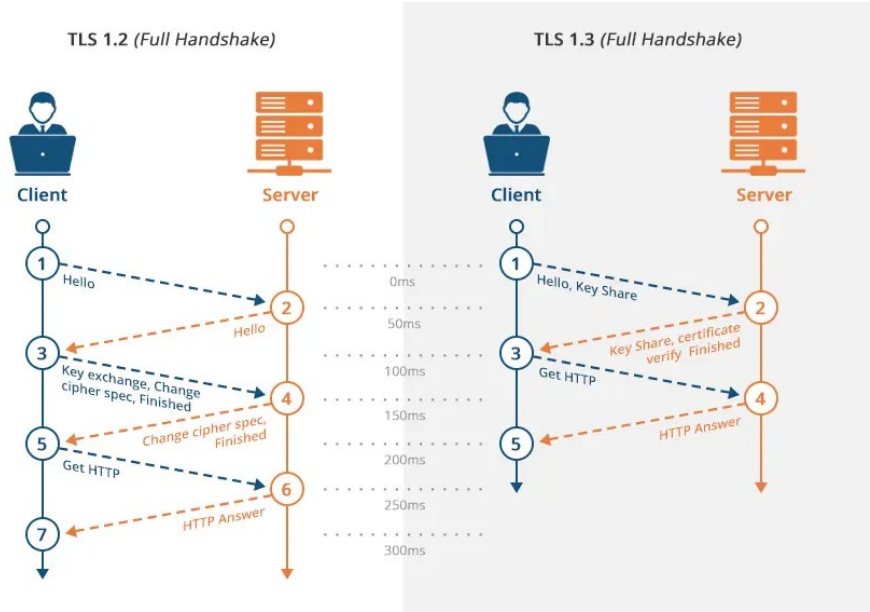


KAMK • University of Applied Sciences

HTTPS Hyper Text Transfer Protocol *Secured*

- **HTTP** protokolla ei ole tietoturvallinen, koska ei oletuksena tarjoa salausta siirrettävälle datalle
- Ratkaisun tarjosi SSL secure socket layer, joka lisättiin HTTP protokollaan → **HTTPS**
- SSL:n on korvannut TLS (Transport Layer Security), joskin SSL esiintyy edelleen nimissä esim. SSL VPN





KAMK • University of Applied Sciences

Kuinka SSL/TLS toimii

Step 1: A customer makes a connection to xyz.com on an SSL/TLS port, typically 443. This connection is denoted with **https** instead of http.

Step 2: xyz.com **(server) sends** back **its public key to the customer**. Once customer receives it, his/her **browser decides if it is alright to proceed.**

The xyz.com **public key must NOT be expired**

The xyz.com **public key must be for xyz.com only**

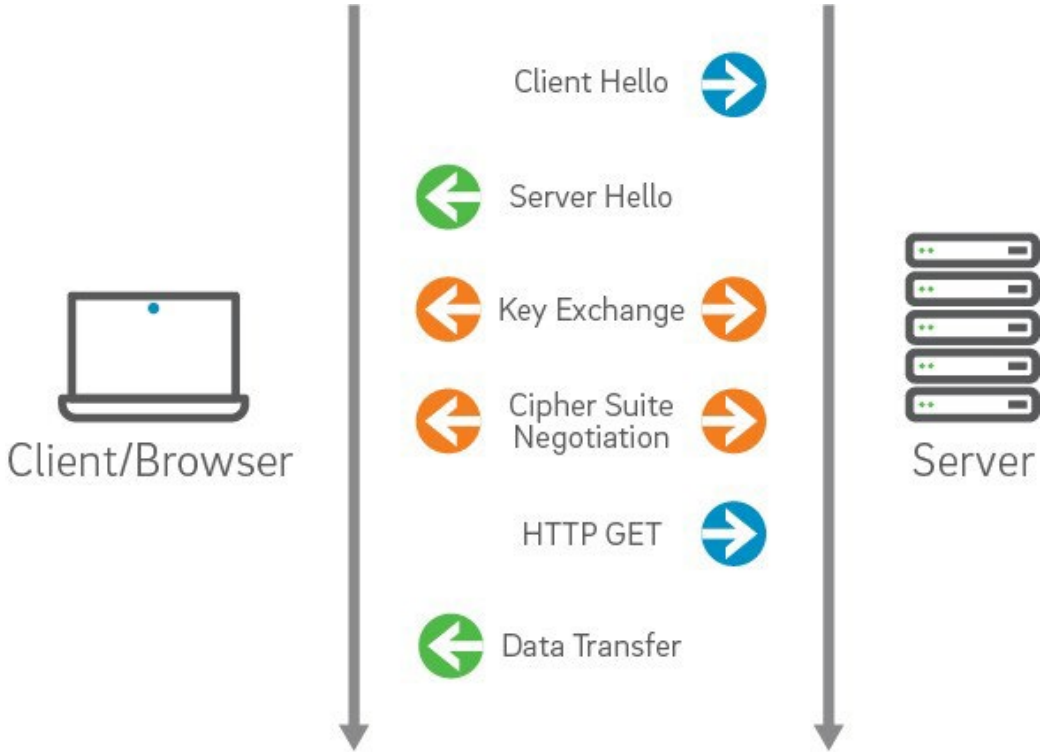
The **client must have the public key installed in their browser certificate store**. All modern browsers include the **SecureTrust root certificate**. If the customer has SecureTrust's trusted public key, then they can trust that they are really communicating with XYZ, Inc.

Step 3: **If the customer decides to trust the certificate**, then the **customer will be sent** to xyz.com his/her **public key**.

Step 4: xyz.com will next create **a unique hash and encrypt it using both the customer's public key and xyz.com's private key**, and **send** this back **to the client.**

Step 5: **Customer's browser will decrypt the hash**. This process shows that the xyz.com sent the hash and only the customer is able to read it.

Step 6: Customer and website **can now securely exchange information**.

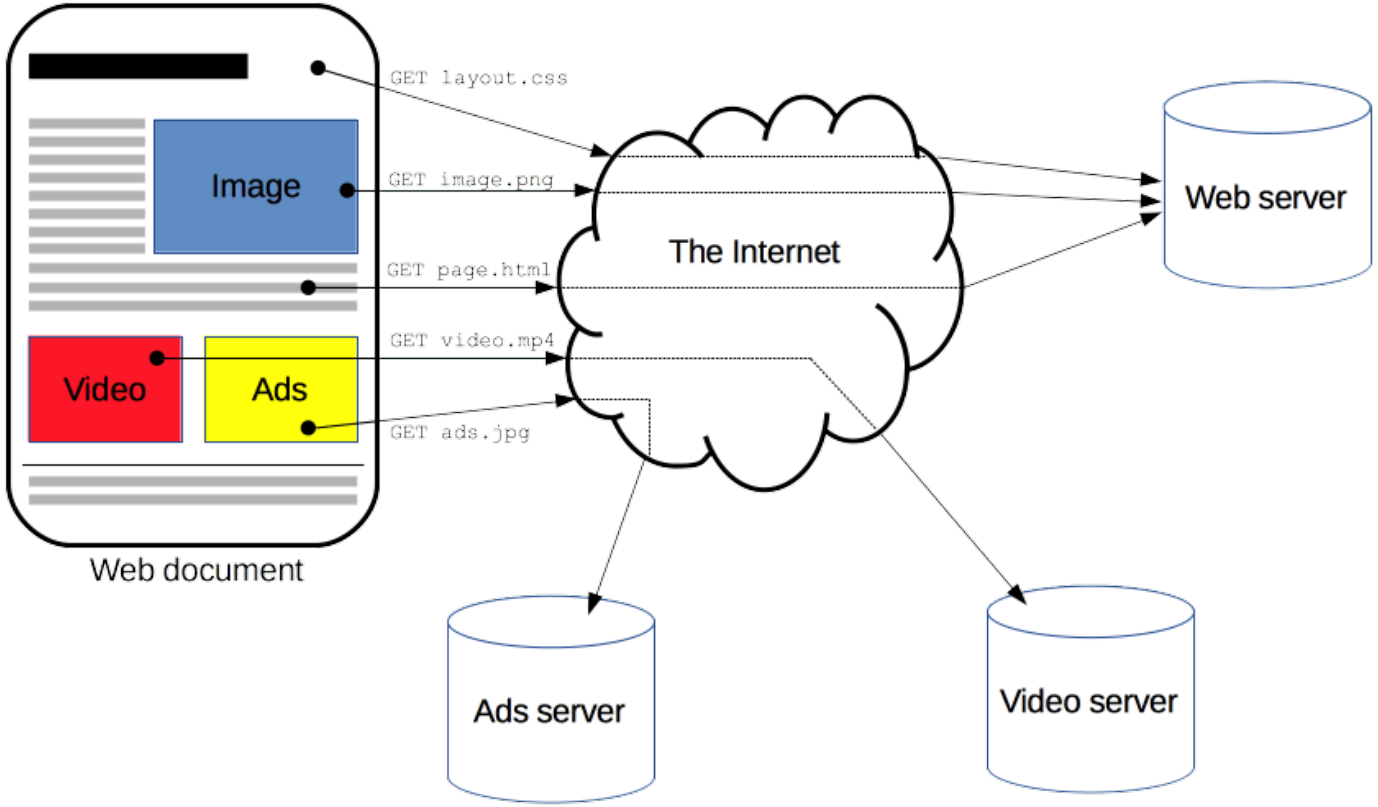


Kuvan lähde: https://certs.securetrust.com/support/support-how-ssl-works.php

KAMK • University of Applied Sciences

HTTP Hyper Text Transfer Protocol

- Selaimessa **F12** avaa web developer työkalun, jolla pääsee tutkimaan sivun lähdekoodia sekä mm. verkon yli tapahtuvaa kommunikointia

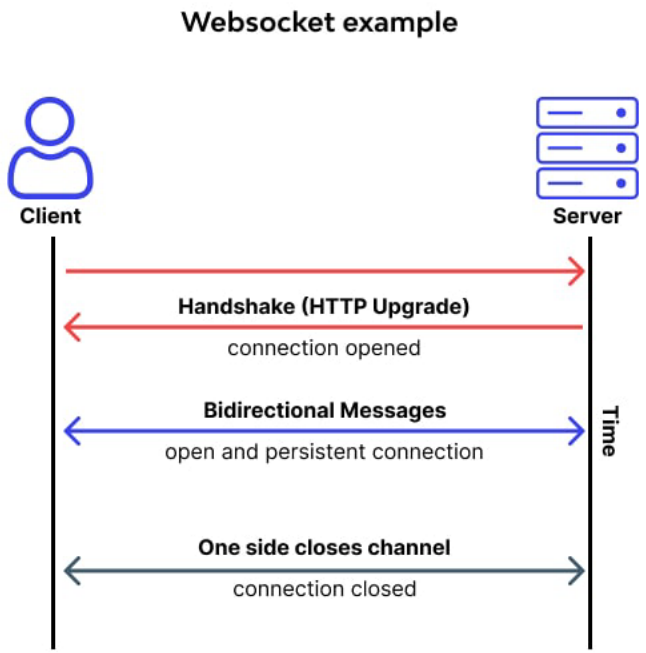


Kuvan lähde: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

KAMK • University of Applied Sciences

HTTP vs. Websocket

```
GET /chat
Host: javascript.info
Origin: https://javascript.info
Connection: Upgrade
Upgrade: websocket
Sec-WebSocket-Key: Iv8io/9s+lYFgZWcXczP8Q==
Sec-WebSocket-Version: 13
```



HTTP and WebSocket Connection (Table)

HTTP and WebSocket Connection

HTTP	WebSockets
It's unidirectional ensuring that only a request or a response is taking place at a time	The bidirectional nature of WebSocket makes to and from data transmission possible. Many responses for one request can be shared.
The connection isn't open for long	Connection can remain open for an indefinite time
The connection is terminated automatically as soon as a response is shared	Connection continues till the time client/server decides to end it.
It's perfect for stateless RESTful applications.	Preferred for the development of real-time, gaming, and chat applications.
As it used TCP, the connection tends to get slow	As the connection doesn't take a break, data delivery is quick.
It's not an event-driven protocol.	WebSocket is highly event-driven.

Comparison Table WebSocket vs HTTP

Comparison Table WebSocket vs HTTP

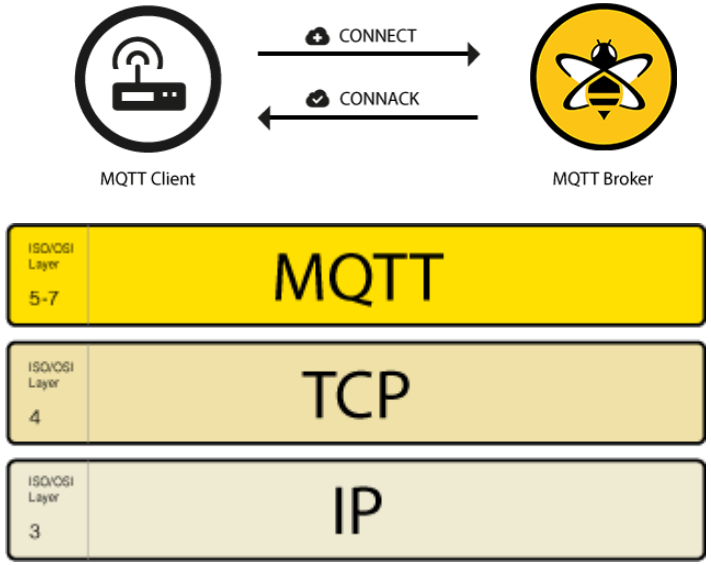
	HTTP	WebSockets
Technology used	Full duplex	Half duplex
Data type handled	Static and stagnant data	Real time and continuously updated data
Latency overheads	High	Low
Operational overheads	High as you need to generate fresh request for each unique/next response	Relatively low as one request can generate multiple responses as long as a connection is open
Speed	Slow as it takes time to establish a new connection for every request	Fast as connection remains open as long as it's not terminated by one party
Ability to handle frequent request	Frequent requests will reduce the performance of the connection	Frequent requests will have no impact on the connection they can be handled easily

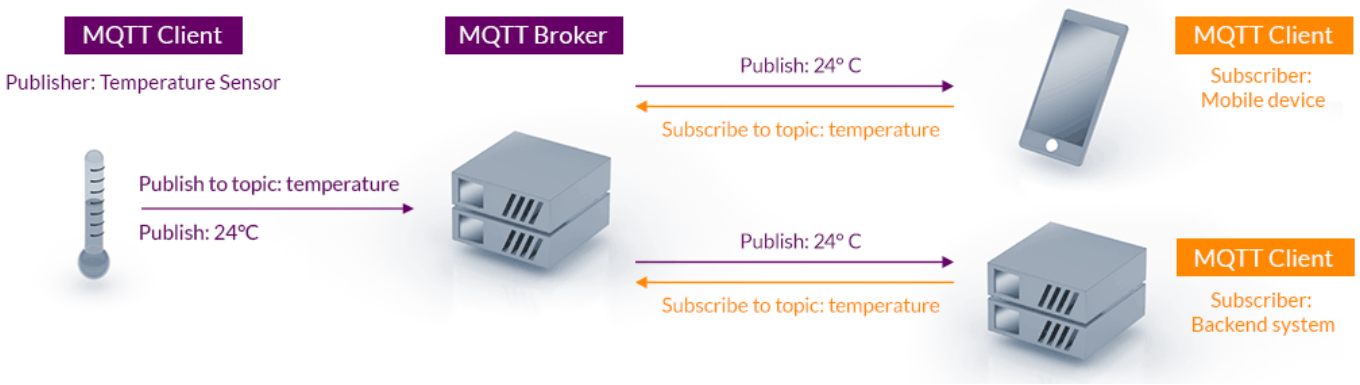
Kuvien lähde: https://www.wallarm.com/what/websocket-vs-http-how-are-these-2-different

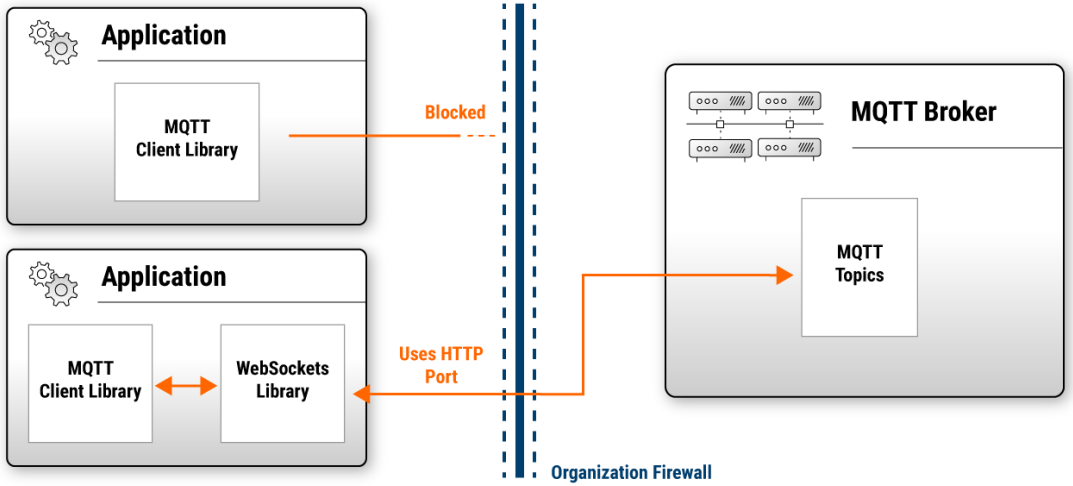
KAMK • University of Applied Sciences

MQTT: The Standard for IoT Messaging

- [Lisätietoa https://mqtt.org/](https://mqtt.org/)







Kuvien lähde: https://mqtt.org/

KAMK • University
of Applied Sciences

www.kamk.fi

KAMK • University of Applied Sciences

Lähteet

- https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml
- https://fi.wikipedia.org/wiki/OSI-malli
- http://bpastudio.csudh.edu/fac/lpress/471/hout/netech/tcpintro.htm
- https://fi.wikipedia.org/wiki/TCP/IP
- https://www.ietf.org/
- https://www.oodlestechnologies.com/blogs/Why-UDP-is-preferred-for-Live-Streaming
- https://fi.wikipedia.org/wiki/UDP
- https://fi.wikipedia.org/wiki/TCP
- https://www.lifewire.com/netstat-command-2618098
- https://en.wikipedia.org/wiki/Client%E2%80%93server_model
- https://geekflare.com/telnet-commands-to-troubleshoot-connection-issues/
- https://fi.wikipedia.org/wiki/SSH
- https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~encryption-algorithms
- https://www3.ntu.edu.sg/home/ehchua/programming/webprogramming/http_basics.html
- https://www.devopsschool.com/blog/understanding-rest-http-method-get-post-put-head-delete/
- https://www.concurrency.com/blog/june-2019/why-http-is-not-suitable-for-iot-applications
- https://en.wikipedia.org/wiki/WebSocket
- https://cyberhoot.com/cybrary/transport-layer-security-tls/
- https://certs.securetrust.com/support/support-how-ssl-works.php
- https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/129618/QUIC-authors-copy.pdf;jsessionid=FD68DE080D0AA9534A9A031CB3E15BF9?sequence=5

KAMK • University
of Applied Sciences

www.kamk.fi