

Protokolle und Standards

The Fundamentals of IoT – Nina Hecht

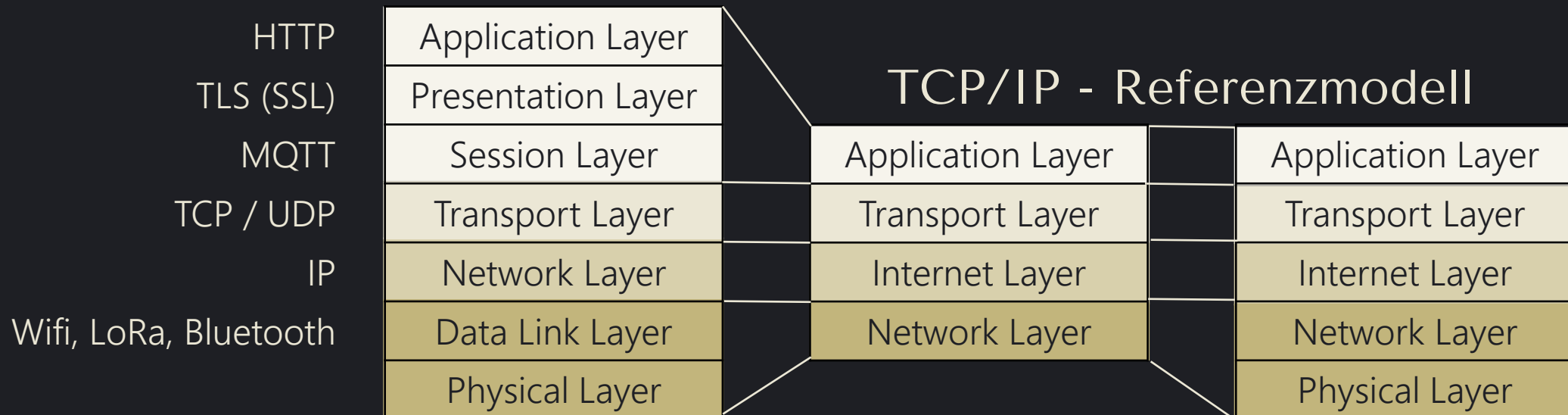
Protokolle

Formale Standards und Richtlinien bestehend aus Regeln, Prozeduren und Formaten, welche Kommunikation mehrerer Geräte über ein Netzwerk ermöglichen

Standards

Ermöglichen die Kommunikation zwischen verschiedenen Netzwerkkomponenten verschiedener „Hersteller“

ISO – OSI Referenzmodell



IP – Internet Protocol

einheitliches Adressierungsschema
→ einheitliche Datenkommunikation



Aufgaben:

1. Logische Adressierung von
 - Netzwerken
 - Netzwerkteilnehmern
2. Routing
 - Innerhalb autonomer Systeme (interne Routing Protokolle)
 - Zwischen autonomen Systemen (externe Routing Protokolle)

IP — Logische Adressierung

IPv4: Gepunktete Dezimalschreibweise

172 . 16 . 254 . 1

10101100 . 00010000 . 11111110 . 00000001

8 Bits

32 Bits = 4 Bytes

IPv6: Hexadezimalschreibweise

128 Bits = 16 Bytes

0123 : 4567 : 89ab : cdef : 0123 : 4567 : 89ab : cdef

Quartett: 16 Bits

0000 0001 0010 0011

IP – Logische Adressierung

Netzklassen

Klasse	Adressbereich	Netze	Knoten
A	001.xxx.xxx.xxx 126.xxx.xxx.xxx	1	16.777.214
B	128.000.xxx.xxx 191.255.xxx.xxx	16	65.534
C	192.000.000.xxx 223.255.255.xxx	256	254

┌──────────┐ ┌──────────┐
NetzID HostID

Subnetting

IP-Adresse (A)	10	217	123	7
Bitschreibweise	00001010	11011001	01111011	00000111
Subnetzmaske (Byteweise)	255	255	255	0
Subnetzmaske (Bitschreibweise)	11111111	11111111	11111111	00000000
Subnetz-ID	10	217	123	Host-IDs
Subnetzmaske (Bitweise – CIDR)	255	255	240	0
Subnetzmaske (Bitschreibweise)	11111111	11111111	11110000	00000000
Subnetz-ID	10	217	112	Host-IDs

Transportprotokolle

Software Abstraktion:
Adressierung von Diensten und deren
Kommunikationsverbindungen mittels
Ports

Transportprotokolle

TCP – Transmission Control Protocol

- Verbindungsauf- & abbau
 - Qualitäts- & Übertragungssicherheit
 - Quittungen (Acknowledge)
 - Checksum
 - Retransmission
 - Datenflusskontrolle
 - Window
- Zuverlässiger, gesicherter Transport

UDP – User Datagram Protocol

- Fokus auf Effizienz & Geschwindigkeit
 - Kein Verbindungsaufbau
 - Keine Übertragungssicherheit
 - Keine Flusskontrolle
 - Wenig Overhead
- Einfacher und schneller Kommunikationsdienst

TLS — Transport Security Layer

- Vertraulichkeit
 - Verschlüsselung
 - Datenintegrität (durch die Signatur)
 - Manipulation der Daten nicht möglich
 - Authentizität
 - Identität des Anbieters überprüfbar
- SSL-Zertifikat auf dem Server notwendig, zu dem abgesicherte Verbindung aufgebaut werden soll
- Aussteller des Zertifikats
 - Zertifikatinhaber
 - Öffentlichen Schlüssel

HTTP — Hypertext Transfer Protocol

- Einfaches, zustandsloses und daher schnelles Protokoll, das die Interaktion zwischen Client (Browser) und Server ermöglicht
- Zugriff auf die durch URIs gekennzeichneten Ressourcen des WWW
- Verschiedene Methoden zur Art des Abrufs
 - GET = Leseanforderung von Server-Daten
 - POST = Schreibanforderung zur Datenübertragung an den Server

1. Client: HTTP – Request

GET /iot-sose2021/beispiel.html HTTP/1.1
(Methode, Request-URI, HTTP Version)

2. Server: HTTP – Response

HTTP/1.1 404 Not found
(HTTP Version, Status-Code, Status-Nachricht)

HTTP — Hypertext Transfer Protocol

- Einfaches, zustandsloses und daher schnelles Protokoll, das die Interaktion zwischen Client (Browser) und Server ermöglicht
- Zugriff auf die durch URIs gekennzeichneten Ressourcen des WWW
- Verschiedene Methoden zur Art des Abrufs
 - GET = Leseanforderung von Server-Daten
 - POST = Schreibanforderung zur Datenübertragung an den Server

Zustandslos

- Keine Kenntnis vorhergehender Anfrage-Antwort-Zyklen
- Authentifikation und Autorisation müssen zustandslos geregelt werden
- Benutzernamen und Passwörter werden im Klartext übertragen
- HTTP + TLS = HTTPS

MQTT – MQ Telemetry Transport

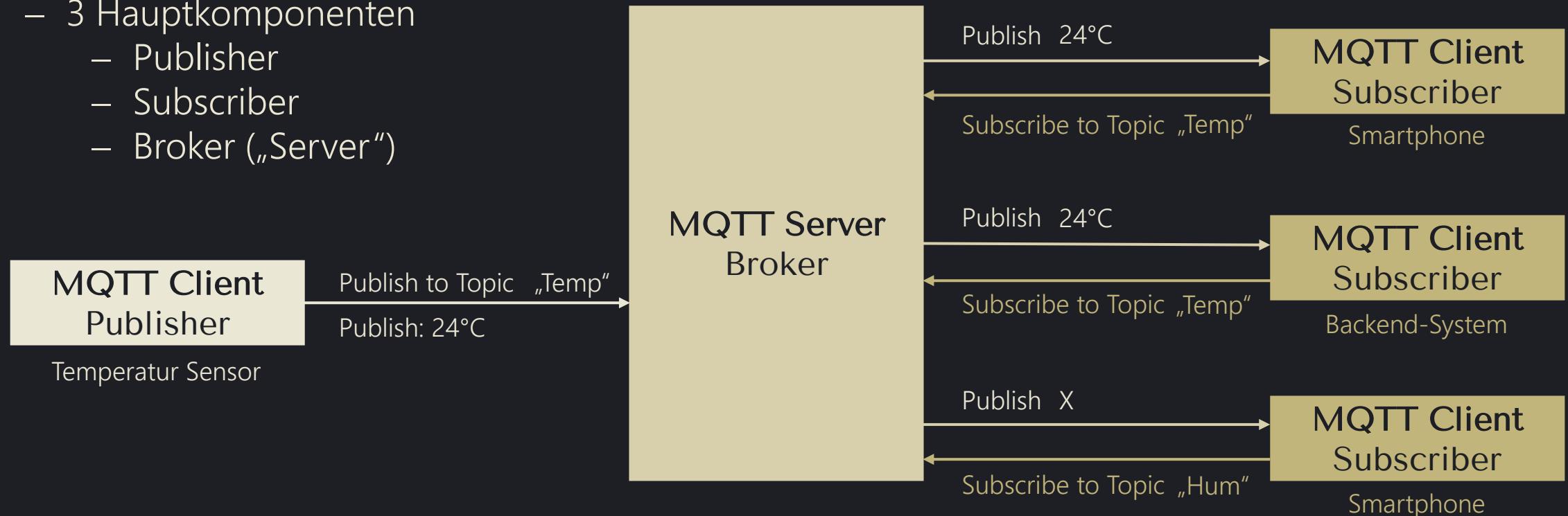
- Früher: Message Queue Telemetry Transport, heute werden Queues nicht mehr unterstützt
- 1999 von IBM entwickelt
- 2014 von OASIS als de-facto Standard Protokoll für Nachrichtenübermittlung in IoT standardisiert
- Eigenschaften
 - Machine 2 Machine Telemetrie
 - Publish-Subscribe Architektur
 - Super lightweight
 - Geringer Code Footprint
 - Geeignet für geringe Bandbreiten
 - Bidirektionelle Kommunikation
 - Broadcast an Gruppe
 - persistente Verbindungen
 - Unterstützt Verschlüsselung mit TLS und Client Authentifikationsprotokolle

MQTT – MQ Telemetry Transport

– Publish-Subscribe Architektur

– 3 Hauptkomponenten

- Publisher
- Subscriber
- Broker („Server“)



MQTT – MQ Telemetry Transport

- Clients haben keine Adressen sondern IDs oder Namen
- Nachrichten werden unter einem spezifischen Thema für den Broker veröffentlicht
- Der Broker filtert und verteilt die Nachrichten an Clients basierend auf deren Abos
 - Der Broker leitet die Nachrichten idR. nur weiter, speichert sie nicht
- Ein Client erhält Nachrichten wenn er die Themen beim Broker abonniert
- Es gibt keine direkte Verbindung zwischen Publisher & Client
- Alle Clients können abonnieren (Nachrichten erhalten) und veröffentlichen (Nachrichten broadcasten)

MQTT vs. HTTP (in IoT)

MQTT

- Data-centric
- Publish-Subscribe Architektur
- Nachrichten können zu Clients gepusht werden
- Geringer Bandbreitenverbrauch und wenig Overhead (kurze Spezifikationen und Header)
- 3 Qualities of Service

HTTP

- Document-centric
- Request-Response Architektur (Client-Server)
- Seit HTTP/2:
 - Server-Push
 - Binär statt textuell
 - Bidirektionale Kommunikation möglich
 - Multiplexing

Quellen

- <https://www.interserver.net/tips/kb/common-network-protocols-ports/>
- https://www.oreilly.com/library/view/networking-all-in-one-for/9781118381007/06_9781118381007-bk01ch02.html
- <https://www.elektronik-kompendium.de/sites/net/0606251.htm>
- <https://www.marcobeierer.de/wissen/ssl-tls-und-https-erklaert>
- <http://www.steves-internet-guide.com/mqtt/>
- <https://mqtt.org/>
- <http://www.steves-internet-guide.com/mqtt-works/>
- <https://youtu.be/2aHV2Fn0I60>
- <https://www.linkedin.com/pulse/internet-things-http-vs-websockets-mqtt-ronak-singh-cspo/>
- <https://medium.com/mqtt-buddy/mqtt-vs-http-which-one-is-the-best-for-iot-c868169b3105>
- <https://github.com/256dpi/arduino-mqtt>
- Unterlagen aus dem Modul „Webtechnologien“ (OMB 4, Prof. Dr. Anders)
- Unterlagen aus dem Modul „Streaming-Anwendungen“ (OMB 5, Prof. Hottong)