Technik des IoT

Protokolle und Technologien

Das Internet of Things (IoT) nutzt die Protokolle der IP-Welt, um neue Anwendungen zur Verfügung zu stellen und eine Vielzahl an Endgeräten zu vernetzen. Die klassischen Netzwerktechnologien und -protokolle bilden hierfür bestenfalls eine Ausgangsbasis. Für die großflächige Vernetzung im IoT sind neue Lösungen erforderlich. Diese Schulung vermittelt sowohl die technischen Grundlagen zur Vernetzung von Endgeräten mit IPv4 und IPv6 als auch die speziellen Anforderungen des IoT. Praxisnahe Übungen an einem Testnetz ermöglichen einen besseren Einblick in die typischen Protokolle und deren Umsetzung.

Kursinhalt

- Internet of Things – eine Definition
- Einsatzgebiete für IoT
- Kommunikationsmodelle
- Netzwerktechnologien (Ethernet, Wireless, Mobilfunk)
- Das Internet-Protokoll (IPv4 und IPv6)
- IP-Applikationen für das Internet of Things (HTTP, CoAP, MQTT, etc.)
- Endgeräte für IoT
- Kommunikationsbeziehungen und Skalierbarkeit
- QoS und Echtzeitfähigkeit
- Neue Protokolle im IoT (6LoWPAN ...)
- Security und Netzwerkmanagement
- Fehlersuche in verteilten Umgebungen
- Die Anbindung an das Data Center und Business-Applikationen

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Diese Schulung richtet sich an technische Mitarbeiter in der Netzplanung und im Betrieb, die grundlegende Protokollabläufe und Anwendungen zur Vernetzung des Internet of Things verstehen und umsetzen müssen. Die Kursinhalte werden durch Übungen an einem Testnetz vertieft.

Voraussetzungen

Grundlegende IT-Kenntnisse werden für eine erfolgreiche Teilnahme vorausgesetzt.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**IOTT**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**3 Tage**	**€ 1.995,-**
Online Training	**3 Tage**	**€ 1.995,-**

Termin/Kursort — Kurssprache Deutsch

23.06.-25.06.25	HY Frankfurt	01.12.-03.12.25	HY Online
23.06.-25.06.25	HY Online	08.06.-10.06.26	HY Frankfurt
01.12.-03.12.25	HY Frankfurt	08.06.-10.06.26	HY Online

Stand 23.05.2025

Technik des IoT

Inhaltsverzeichnis

Technik des IoT – Protokolle und Technologien

1 Definition und Motivation
1.1 Was ist IoT?
1.2 Anwendungsbereiche des IoT
1.3 Neue Technologie im IoT?
1.4 IoT Referenz-Modell
1.5 Schichtenmodelle für das IoT - Beispiel
1.6 Akteure und Standards im IoT

2 Übertragung und Vermittlung (OSI 1-2)
2.1 Verschiedene Technologien - eine Übersicht
2.1.1 ...Low-Rate WPAN - Standard IEEE 802.15.4
2.1.2 Low-Rate WPAN - Geräte und Topologien
2.1.3 IEEE 802.15.4 - Architektur
2.1.4 IEEE 802.15.4 - Modulation und Spreizung
2.1.5 IEEE 802.15.4 auf Mac-Layer (1) - CSMA/CA
2.1.6 IEEE 802.15.4 auf MAC-Layer (2)
2.2 Ethernet
2.3 Wireless LAN
2.4 Bluetooth (IEEE 802.15.1)
2.5 LoRaWAN
2.5.1 LoRa - Modulation
2.5.2 LoRaWAN - Sterntopologie
2.5.3 LoRaWAN - Security
2.6 Thread
2.6.1 Thread: Topologie und Anwendung
2.6.2 Thread: Security durch Commissioning
2.7 Sigfox
2.8 NB-IoT Überblick

3 Der Netzwerk-Layer: IP und Routing im IoT
3.1 Warum IP im IoT?
3.2 Echtzeitfähigkeit und QoS
3.3 IPv6 - Anforderungen an das neue IP
3.3.1 Das Header-Format in IPv6
3.3.2 Erweiterungen mit dem Next Header
3.3.3 Die IPv6-Adressen
3.3.4 Global Unicast Adressen
3.4 Adresszuweisung bei IPv6
3.5 IPv6 over IEEE 802.15.4 (RFC 4944)
3.5.1 6LoWPAN (RFC 4944) Überblick
3.5.2 6LoWPAN Dispatch Byte
3.5.3 6LoWPAN Header Übersicht
3.5.4 Mesh Type und Mesh Addressing Header
3.5.5 Fragmentation Type und Header
3.5.6 Adressierung mit 6LoWPAN
3.5.7 Header Compression in 6LoWPAN
3.6 Routing in LoWPANs
3.6.1 Routingprotokoll RPL
3.6.2 RPL Topologien
3.6.3 DODAG Aufbau
3.6.4 Mesh-Under vs. Route-Over
3.7 IPv6 über Bluetooth Low Energy (BLE)
3.8 ZigBee und IPv6
3.9 Thread

4 Protokolle der Applikationsschicht
4.1 Welches Transportprotokoll?
4.1.1 UDP – verbindungslos und ungesichert
4.1.2 TCP – anwendungsorientiert und gesichert
4.2 Datentransport ohne spezielles Applikationsprotokoll
4.3 MQTT
4.3.1 Das Protokoll
4.3.2 MQTT-Server/-Broker und Clients
4.3.3 Subscriptions, Topics, Topic Filter, Session
4.3.4 Datenformat in MQTT-Paketen
4.3.5 Flags im Fixed Header
4.3.6 Variabler Header CONNECT-Nachricht (1)
4.3.7 CONNACK (Acknowledge connection request)
4.3.8 MQTT Nachrichtentypen: CONNECT, CONNACK
4.3.9 CONNACK - Return Codes
4.3.10 MQTT PUBLISH Fixed Header
4.3.11 MQTT PUBLISH Variable Header
4.3.12 MQTT Nachrichtentypen PUBLISH, PUBACK, PUBREC, PUBREL und PUBCOMP
4.3.13 MQTT SUBSCRIBE
4.3.14 MQTT Nachrichtentypen SUBSCRIBE, SUBACK, UNSUBSCRIBE, UNSUBACK
4.3.15 MQTT Nachrichtentypen PINGREQ, PINGRESP, DISCONNECT
4.3.16 QoS in MQTT
4.3.17 Retained Messages
4.3.18 Last Will Messages
4.4 Constraint Application Protocol (CoAP)
4.4.1 CoAP - HTTP
4.4.2 CoAP Nachrichtenformat
4.4.3 CoAP Nachrichtenaustausch
4.4.4 CoAP Request/Response Model
4.4.5 CoAP - Umgang mit Nachrichtenverlust
4.4.6 CoAP - Proxy und Caching
4.4.7 CoAP Methoden
4.4.8 CoAP Methoden (Fortsetzung)

5 IoT-Plattformen und Anbindung an Cloud und Data Center
5.1 IoT-Modelle
5.2 IoT-Plattformen - Grundfunktionen
5.3 Cisco IoT Reference Model
5.4 Anbindung von „Dingen“ an die Cloud
5.4.1 Fog-/Edge-Computing
5.5 Schnittstellen von IoT-Plattformen
5.6 IoT-Netzwerkmanagement

6 Security und Troubleshooting im IoT
6.1 Die Bedrohungslage
6.1.1 Schutzziele: Security - Privacy - Safety
6.1.2 Sicherheit auch ohne Teppich: von IT zu OT
6.1.3 Privacy und Datenschutz
6.1.4 Neue Angriffsziele
6.1.5 Typologie der Angreifer
6.1.6 Ziele der Angreifer
6.2 Typische Angriffe
6.2.1 Sicherheit durch Design
6.2.2 Sicherheit durch Dokumentation und Support
6.2.3 RIPE und ATLAS-Netz
6.2.4 OWASP – IoT-Project
6.2.5 Ansatz Embedded Security
6.3 Klassische Security-Ansätze
6.4 Sicherheitscheckliste IoT
6.5 Troubleshooting und systematische Fehlersuche
6.5.1 Baselining

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de