

Wireless LAN I

Technologien, Zugriffsverfahren und Sicherheitskonzepte

Wireless LANs sind längst Kernbestandteil jedes Firmennetzes. In Heimnetzwerken und an Hot Spots ersetzen sie sogar fast vollständig das Ethernet, und ein Ende des WLAN-Booms ist nicht in Sicht. Dieser WLAN-Kurs führt in die Technik und den Einsatz der WLANs ein. Die Teilnehmer lernen die unterschiedlichen WLAN-Technologien und -Standards kennen, verstehen die Architektur von WLANs und können Planungs- und Dimensionierungsaufgaben lösen. Demonstrationen am Testnetz sorgen für den notwendigen Praxisbezug.

Kursinhalt

- Grundlagen, Funk- und Antennentechnik
- Topologien und Zugriffsverfahren
- Access Points und SSID
- IEEE 802.11a bis 11be: Die Übertragungs-Standards
- Bitraten und Reichweiten
- Einsatzgebiete von 802.11ax (Wi-Fi 6E)
- Ausblick 802.11be (Wi-Fi 7)
- Sicherheit im WLAN – Konsequenzen aus dem Shared Medium
- TKIP, AES, WPA, WPA2, WP3, IEEE 802.11i und Adressfilter
- Advanced Security: 802.1X, RADIUS, EAP
- Authentisierung mit Zertifikaten

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

Zielgruppe

Der Kurs bietet einen praxisnahen und umfassenden Einblick in die Wireless-LAN-Technologie für Netzwerkplaner, Administratoren und vertriebslich orientierte Mitarbeiterinnen und Mitarbeiter.

Voraussetzungen

Für die erfolgreiche Teilnahme an diesem Kurs sind neben grundlegendem Netzwerk- und IT-Wissen keine speziellen Vorkenntnisse erforderlich. Weitergehendes Wissen im LAN-Bereich ist zur Diskussion der praxisnahen Fallbeispiele von Vorteil.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/WLAN

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 CHF 1.975,-
Termine in Österreich	3 Tage CHF 1.975,-
Online Training	3 Tage CHF 1.975,-
Termin/Kursort	Kurssprache Deutsch
23.06.-25.06.25 Frankfurt	13.10.-15.10.25 Hamburg
23.06.-25.06.25 Online	13.10.-15.10.25 Online
21.07.-23.07.25 Hamburg	10.11.-12.11.25 Online
21.07.-23.07.25 Online	10.11.-12.11.25 Wien
25.08.-27.08.25 Düsseldorf	01.12.-03.12.25 München
25.08.-27.08.25 Online	01.12.-03.12.25 Online

Stand 07.05.2025



Inhaltsverzeichnis

Wireless LAN I – Technologien, Zugriffsverfahren und Sicherheitskonzepte

1	Wireless LANs im Überblick	2.8.5	802.11n: Wi-Fi 4	4.10	WPA3
1.1	LANs – drahtlos vs. drahtgebunden	2.8.6	802.11ac: Wi-Fi 5	4.10.1	WPA3 Enterprise: Krypto-Verfahren
1.1.1	Anforderungen an lokale Netze	2.8.7	IEEE 802.11ad-2012: 60 GHz	4.10.2	Simultaneous Authentication of Equals (SAE)
1.1.2	Einsatzszenarien für WLAN	2.8.8	802.11ax: Wi-Fi 6	4.10.3	Easy Connect und PMF
1.1.3	Fakten im Überblick	2.8.9	802.11be: Wi-Fi 7	4.10.4	Dragonblood
1.2	Aufbau und Struktur eines WLANs	3	Topologien, Zugriffsverfahren und Protokolle	A	Wireless LAN I – Architektur und Design
1.2.1	Ad-Hoc vs. Infrastructure	3.1	Aufbau eines WLANs		Übungen und Aufgaben zum Kurs
1.2.2	Basic Service Area (BSA)	3.1.1	Das Infrastruktur-Netz	A.1	WLAN Analyse mit Windows Bordmitteln
1.2.3	Distribution System	3.2	Anmeldung am Access Point	A.1.1	Erster Eindruck der Laborumgebung
1.2.4	Was ist ein Repeater (WDS)?	3.3	Zugriffsverfahren	A.2	Funkzellenanalyse mit inSSIDer und NetSpot
1.2.5	Bridge/Mesh	3.3.1	Distributed Coordination Function	A.2.1	Fragen zur WLAN-Umgebung
1.2.6	Controller-basierte Lösungen	3.3.2	Point Coordination Function	A.3	Wireless Frames mitlesen
1.3	WLAN im Schichtenmodell	3.4	Daten-Transport in WLAN Architekturen	A.3.1	Daten-, Management- und Control-Frames finden...
1.4	Troubleshooting in Layer 1	3.5	Typische Frame-Formate	A.3.2	Radio-Header inspizieren
1.4.1	Design Probleme	4	Sicherheit und Zugriffsschutz	A.3.3	MAC-Header untersuchen
1.5	Standardisierung und Regulierung	4.1	Ziele von Netzwerksicherheit	A.3.4	4-Way Handshake
1.5.1	Funkfrequenzen	4.1.1	Sicherheitsbausteine	A.4	Signal- und Übertragungsrate am WLAN-Client
1.5.2	IEEE 802.11-Standards	4.2	Vertraulichkeit		
2	Funktechnik und WLAN Generationen	4.2.1	Diffie-Hellman – Erzeugen symmetrischer Schlüssel		
2.1	Physikalische Grundlagen	4.2.2	RSA – Asymmetrische Verschlüsselung		
2.1.1	Dämpfung und Abstrahlung	4.3	Integrität		
2.1.2	Frequenzbereiche im WLAN	4.4	Authentizität		
2.1.3	Mögliche Störeinflüsse	4.4.1	Vorverteilte Schlüssel (Preshared Keys)		
2.1.4	Was zeigt ein Spektrometer an?	4.4.2	Digitale Unterschriften – Der moderne Fingerabdruck		
2.2	RF Interferenzen	4.4.3	Zertifikate		
2.2.1	Co-channel Interference	4.5	IEEE 802.1X		
2.2.2	Adjacency Channel Interference	4.5.1	IEEE 802.1X-Rahmenwerk		
2.2.3	Non-802.11 Interferenzen	4.5.2	EAP – Extensible Authentication Protocol		
2.2.4	Interference Device Report	4.5.3	Troubleshooting Client Authentication		
2.2.5	Monitor Radio Band Air Quality	4.5.4	EAP und Netzwerkbetriebssysteme		
2.3	Spektrum Analyse Tool MetaGeek	4.6	Verfügbarkeit		
2.4	Antennentechnik	4.7	Authentisierung im WLAN		
2.4.1	MIMO	4.7.1	MAC-Adress-Filter		
2.5	Header auf Layer 1 und 2	4.8	WPA: Wi-Fi Protected Access		
2.6	Frequenzspreizung	4.9	WPA2 und IEEE 802.11i		
2.6.1	Das OFDM-Verfahren	4.9.1	Schlüsselmanagement		
2.6.2	Das OFDMA-Verfahren	4.9.2	Datenintegrität mit AES-CCMP		
2.7	Modulationsverfahren	4.9.3	Verschlüsselung mit AES-CCMP		
2.7.1	Phasenmodulation	4.9.4	802.11i oder WPA2?		
2.7.2	Quadrature Amplitude Modulation	4.9.5	Hole 196		
2.8	WLAN Generationen	4.9.6	KRACK		
2.8.1	IEEE 802.11	4.9.7	Protected Management Frames		
2.8.2	IEEE 802.11b				
2.8.3	IEEE 802.11a				
2.8.4	IEEE 802.11g				

