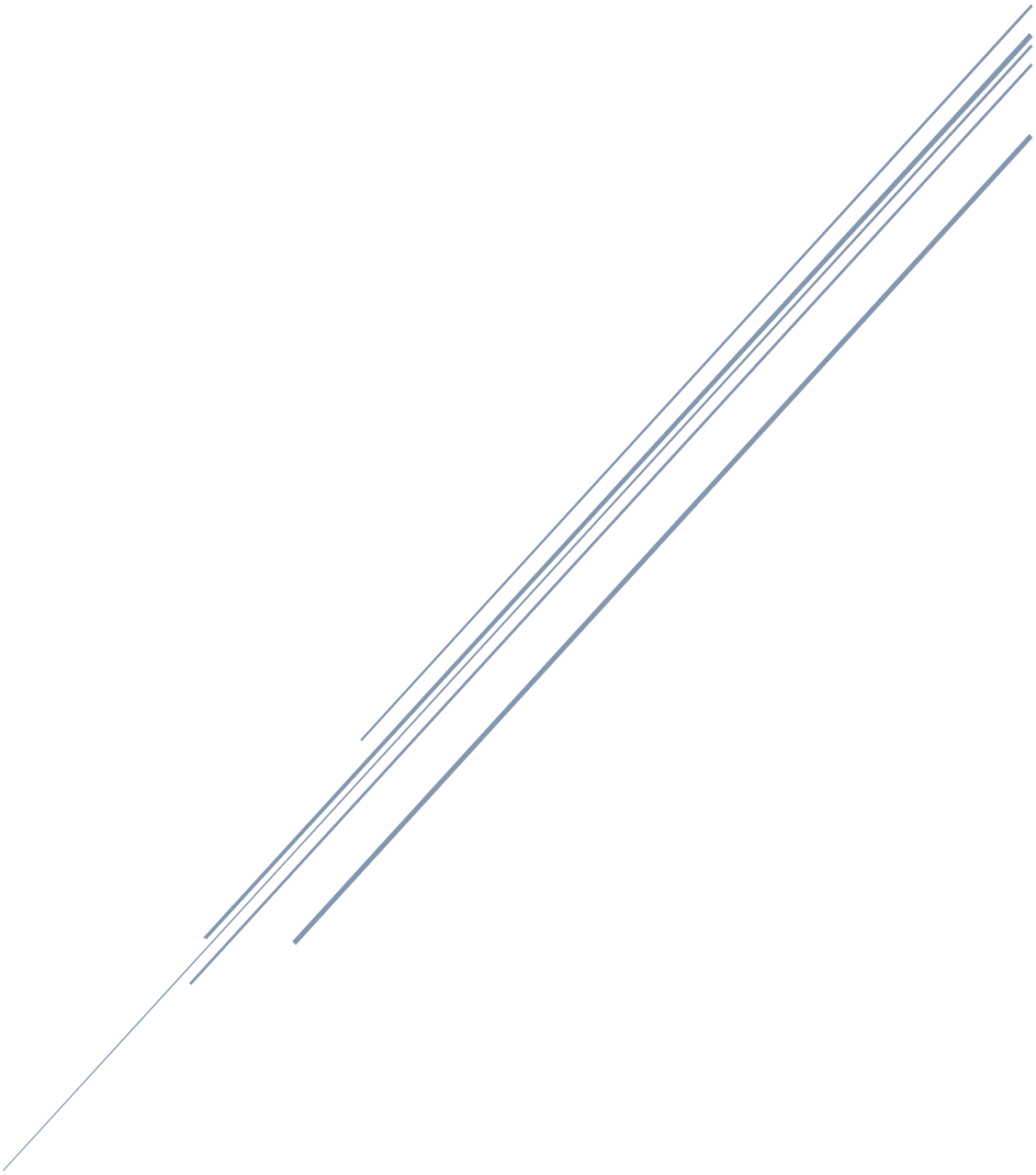
WLAN

ITS – LF11b



Short Summary CCNA SEM2 | V1.1

Inhaltsverzeichnis

Inhaltlicher Hinweis

Die gezeigten Inhalte sind zu großen Teilen eine Zusammenfassung des CISCO CCNA Switching, Routing und Wireless Essentials v7.0 (SRWE) und sollen als Kurzzusammenfassung für die Vorbereitung zur Abschlussprüfung dienen. Es lohnt sich zu dem einen oder anderen Thema noch weitergehend zu informieren (siehe zB Inhaltszusammenfassung Schulaufgabe). Wenn nicht anders angegeben, sind alle Inhalte als Quelle zugrundeliegend – CISCO Switching, Routing, and Wireless Essentials v7.0 (Netacad.com). Somit können auch alle Videos zu den Themen hier angesehen werden.

Einführung

Vorteile

Ein Wireless-LAN (WLAN) ist ein drahtloses Netzwerk, das häufig in Haushalten, Büros und Campusumgebungen verwendet wird. Netzwerke müssen Menschen unterstützen, die in Bewegung sind. Menschen verbinden sich über Computer, Laptops, Tablets und Smartphones. Es gibt viele verschiedene Netzwerkinfrastrukturen, die Netzwerkzugriff ermöglichen, z. B. kabelgebundene LANs, Dienstanbieter-Netzwerke und Mobilfunknetze. Aber es ist das WLAN, das Mobilität im privaten und geschäftlichen Umfeld ermöglicht.

In Unternehmen mit einer drahtlosen Infrastruktur kann es zu Kosteneinsparungen kommen, wenn sich die Ausstattung ändert oder wenn ein Mitarbeiter innerhalb eines Gebäudes umzieht, Ausrüstung oder Labor umorganisiert oder an temporäre Standorte oder Projektstandorte umgezogen wird. Eine drahtlose Infrastruktur kann sich an schnell ändernde Anforderungen und Technologien anpassen.

Nachteile

Durch Frequenzüberlagerungen kann es zu Störungen im eigenen WLAN Netz kommen. Die Folge sind Verbindungsabbrüche oder weitere Störungen. Besonders das 2,4 GHz Band ist hier sehr anfällig.

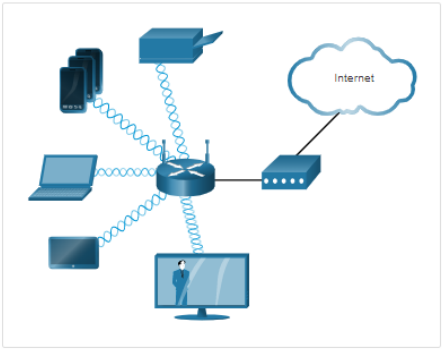
Arten von WLAN-Netzwerken

WPAN
WLAN
WMAN
WWAN

Wireless Personal-Area Networks (WPAN) - Verwendet Low Power-Sender für ein Nahbereichsnetzwerk, normalerweise 6 bis 9 Meter. Bluetooth- und ZigBee-basierte Geräte werden häufig in WPANs verwendet. WPANs basieren auf dem 802.15-Standard im 2,4-GHz-Frequenzband

WPAN
WLAN
WMAN
WWAN

Wireless LANs (WLAN) - Verwendet Sender, um ein mittelgroßes Netzwerk abzudecken, normalerweise bis zu 100 m. WLANs eignen sich für den Einsatz, im Home-Office und sogar in einer Campus-Umgebung. WLANs basieren auf dem 802.11-Standard im 2,4-GHz- oder 5-GHz-Frequenzband.



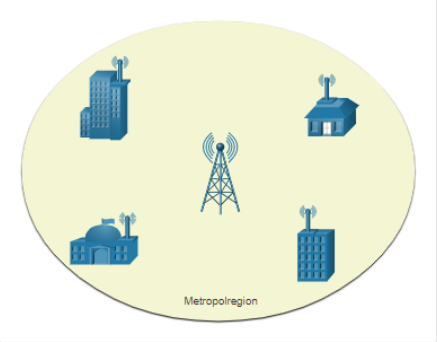
WPAN

WLAN

WMAN

WWAN

Wireless MANs (WMAN) - Verwendet Sender um drahtlose Dienste in einem größeren geografischen Gebiet bereitzustellen. WMANs eignen sich für den drahtlosen Zugang zu einer Metropolregion oder einem bestimmten Bezirk. WMANs verwenden spezielle staatlich lizenzierte Frequenzen.



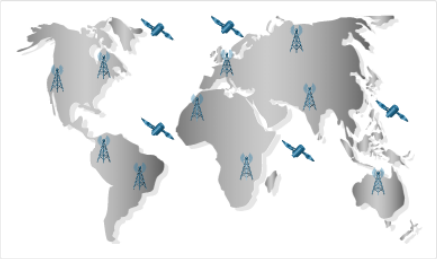
WPAN

WLAN

WMAN

WWAN

Wireless Wide-Area Networks (WWANs) - Verwendet Sender, um eine Abdeckung über ein weitläufiges geografisches Gebiet zu bieten. WWANs eignen sich für nationale und globale Kommunikation. WWANs verwenden auch spezielle staatlich lizenzierte Frequenzen.



Technologie für drahtlose Netzwerke

Bluetooth

WiMAX

Mobiles Breitband

Satelliten-Breitband

Bluetooth - Ein IEEE 802.15 WPAN-Standard, der ein Gerätepaarungsverfahren zur Kommunikation über Entfernungen von bis zu 100 m verwendet. Er findet sich in Smart-Home-Geräten, Audioverbindungen, Autos und anderen Geräten, die eine Kurzstreckenverbindung benötigen. Es gibt zwei Arten von Bluetooth-Funkgeräten

- **Bluetooth Low Energy (BLE)** - Unterstützt mehrere Netzwerktechnologien, einschließlich Mesh-Topologie für große Netzwerkgeräte.
- **Bluetooth Basic Rate/Enhanced Rate (BR/EDR)** - Dies unterstützt Punkt-zu-Punkt-Topologien und ist für Audio-Streaming optimiert.

Bluetooth

WiMAX

Mobiles Breitband

Satelliten-Breitband

WiMAX (Worldwide Interoperability for Microwave Access) - WiMAX ist eine Alternative zu Breitband-Internetverbindungen, die mit DSL und Kabel konkurrieren. Es wird jedoch in der Regel in Bereichen verwendet, die noch nicht an einen DSL- oder Kabelanbieter angeschlossen sind. Es handelt sich um einen IEEE 802.16 WWAN-Standard, der Hochgeschwindigkeits-Breitbandzugang mit einer Reichweite bis zu 50 km bietet. WiMAX arbeitet in ähnlicher Weise wie Wi-Fi, aber mit höheren Geschwindigkeiten, über größere Entfernungen und für eine größere Anzahl von Benutzern. Es verwendet ein Netzwerk von WiMAX-Sendemasten, die ähnlich wie Mobilfunkmasten sind. WiMAX-Sender und Mobilfunksender können den Platz auf demselben Mast teilen, wie in der Abbildung gezeigt.

Bluetooth

WiMAX

Mobiles Breitband

Satelliten-Breitband

Satelliten-Breitband - Bietet Netzwerkzugriff für abgelegene Standorte durch die Verwendung einer gerichteten Satellitenantenne, die auf einen bestimmten geostationären Satelliten ausgerichtet ist. Ist in der Regel teurer und erfordert eine freie Sicht zum Satelliten. Typischerweise wird es von ländlichen Hausbesitzern und Unternehmen verwendet, wo Kabel und DSL nicht verfügbar sind.

Bluetooth

WiMAX

Mobiles Breitband

Satelliten-Breitband

Mobiles Breitband - 4G/5G sind drahtlose Mobilfunknetze, die hauptsächlich von Mobiltelefonen verwendet werden, aber in Autos, Tablets und Laptops verwendet werden können. Mobilfunknetze sind Multi-Access-Netzwerke, die sowohl Daten- als auch Sprachkommunikation ermöglichen. Eine Zelle wird durch einen Mobilfunkmast erzeugt, der Funksignale in einem bestimmten Bereich sendet. Durch die Verbindung von Zellenstandorten wird das Mobilfunknetz gebildet. Die Arten von Mobilfunknetzen sind Global System for Mobile Communications (GSM), UMTS , LTE und 5 G und Code Division Multiple Access (CDMA). (Anmerkung: CDMA ist ein Mehrfachzugriffsverfahren und kein Mobilfunkstandartd. Die Bezeichung des Mobilfunkstandards ist CDMA2000) GSM ist international anerkannt, während CDMA2000 hauptsächlich in den USA verwendet wird.

Das Mobilfunk-Netz der 4. Generation (4G, LTE) ist das aktuelle Mobilfunknetz. 4G liefert Geschwindigkeiten, die das 10-fache der vorherigen 3G-Netzwerke sind. Der neue 5G verspricht, 100-mal schnellere Geschwindigkeiten als 4G zu liefern und mehr Geräte mit dem Netzwerk zu verbinden als je zuvor.

IEEE 802.11 (der WLAN Standard)

WLAN Organisationen

Standards gewährleisten die Interoperabilität zwischen Geräten, die von verschiedenen Herstellern hergestellt werden. International beeinflussen die drei Organisationen die WLAN-Standards ITU-R, IEEE und Wi-Fi Alliance.

ITU

IEEE

Wi-Fi Alliance

Die Internationale Telekommunikationsunion (ITU) regelt die Zuweisung des Funkfrequenzspektrums und der Satellitenbahnen über die ITU-R. ITU-R steht für den ITU Funkkommunikationssektor.

ITU

IEEE

Wi-Fi Alliance

IEEE legt fest, wie eine Funkfrequenz moduliert wird um Informationen zu übertragen. Er verwaltet die Standards für lokale und städtische Netze (MAN) mit der Normenfamilie IEEE 802 LAN/MAN. Die dominierenden Standards in der IEEE 802-Familie sind 802.3 Ethernet und 802.11 WLAN.

ITU

IEEE

Wi-Fi Alliance

Die Wi-Fi Alliance ist ein globaler, gemeinnütziger Branchenverband, der sich der Förderung des Wachstums und der Akzeptanz von WLANs verschrieben hat. Es handelt sich um eine Vereinigung von Anbietern, deren Ziel es ist, die Interoperabilität von Produkten, die auf dem 802.11-Standard basieren, zu verbessern, indem sie Anbieter für die Konformität mit Branchennormen und die Einhaltung von Standards zertifizieren.

WLAN-Generationen

Die Fähigkeit von WLANs mit unterschiedlichen Standards, Bezeichnungen und eventuelle Inkompatibilitäten ist für Normalnutzer unverständlich und kaum auseinanderzuhalten. Statt der kryptischen IEEE-Projektgruppennamen haben die WLAN-Standards zusätzlich eine fortlaufende Nummer. Offiziell beginnt die Bezeichnung mit „Wi-Fi 4“ für den Standard IEEE 802.11n.

- WLAN 1 / Wi-Fi 1: IEEE 802.11 (1999)
- WLAN 2 / Wi-Fi 2: IEEE 802.11b (1999)
- WLAN 3 / Wi-Fi 3: IEEE 802.11g (2003)
- **WLAN 4 / Wi-Fi 4:** IEEE 802.11n (2009)
- **WLAN 5 / Wi-Fi 5:** IEEE 802.11ac (2014)
- **WLAN 6 / Wi-Fi 6:** IEEE 802.11ax (2021)
- **WLAN 6E / Wi-Fi 6E**: IEEE 802.11ax im 6-GHz-Frequenzbereich
- **WLAN 7 / Wi-Fi 7:** IEEE 802.11be (?)

Leider ist diese Angabe völlig unzureichend. Denn der Standard allein ist nicht der einzige Parameter, der Einfluss auf die Geschwindigkeit und Leistungsfähigkeit der WLAN-Technik hat.

Quelle: in Anlehnung an https://www.elektronik-kompendium.de/sites/net/0610051.htm
Abgerufen am 12.04.2023

Aktuelle WLAN-Standards im Vergleich

WLAN-Generation	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6 / 6E

IEEE-Standard	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax
Maximale Übertragungsrate *	600 MBit/s	6.936 MBit/s	9.608 MBit/s
Theoretische Übertragungsrate **	300 MBit/s	867 MBit/s	1.200 MBit/s
Maximale Reichweite	100 m	50 m	50 m
Frequenzbereich	2,4 + 5 GHz	nur für 5 GHz	2,4 + 5 GHz + 6 GHz
Maximale Sende/Empfangseinheiten	4 x 4	8 x 8	8 x 8
Antennentechnik	MIMO	(MU-MIMO)	MU-MIMO
Maximale Kanalbreite	40 MHz	160 MHz	160 MHz
Modulationsverfahren	64QAM	256QAM	1024QAM

Quelle: in Anlehnung an https://www.elektronik-kompendium.de/sites/net/0610051.htm
Abgerufen am 12.04.2023

Nach CISCO

IEEE WLAN-Standard	Funkfrequenz	Beschreibung
802.11	2,4 GHz	• Geschwindigkeiten von bis zu 2 Mbit/s
802.11a	5 GHz	• Geschwindigkeiten von bis zu 54 Mbit/s • kleiner Abdeckungsbereich • weniger effektiv beim Durchdringenden von Gebäudestrukturen. (Funkversorgung in Gebäuden) • nicht interoperabel mit 802.11b und 802.11g
802.11b	2,4 GHz	• Geschwindigkeiten von bis zu 11 Mbit/s • größere Reichweite als 802.11a • besser in der Lage, Gebäudestrukturen zu durchdringen. (Funkversorgung in Gebäuden)
802.11g	2,4 GHz	• Geschwindigkeiten von bis zu 54 Mbit/s • abwärtskompatibel mit 802.11b mit reduzierter Bandbreitenkapazität
802.11n	2.4 GHz 5 GHz	• Datenraten reichen von 150 Mbit/s bis 600 Mbit/s mit einer Reichweite von bis zu 70 m (230 Fuß) • APs und Wireless-Clients benötigen mehrere Antennen mit MIMO Technologie • abwärtskompatibel mit 802.11a/b/g-Geräten mit begrenzten Daten Raten

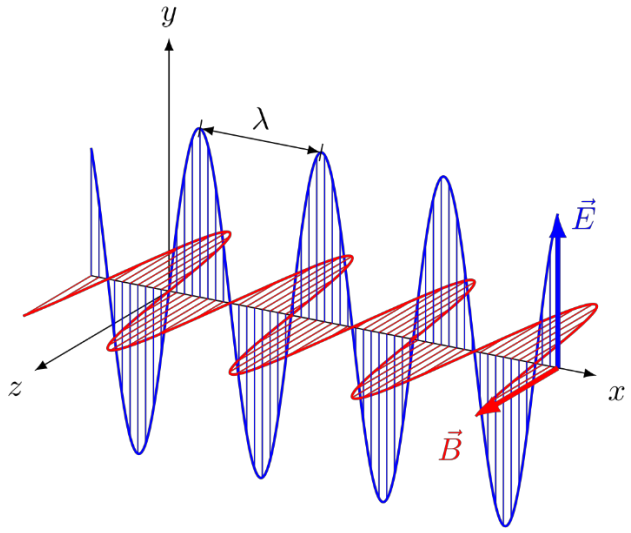
IEEE WLAN-Standard	Funkfrequenz	Beschreibung
802.11ac	5 GHz	• bietet Datenraten von 450 Mbit/s bis 1,3 Gbit/s (1300 Mbit/s) Verwendung von MIMO-Technologie • Bis zu acht Antennen können unterstützt werden • abwärtskompatibel mit 802.11a/n-Geräten mit begrenzter Datenrate
802.11ax	2.4 GHz 5 GHz	• eingeführt im Jahr 2019 - neuester Standard • auch bekannt als High-Efficiency Wireless (HEW) • höhere Datenraten • erhöhte Kapazität • kann viele angeschlossene Geräte handhaben • reduzierter Energieverbrauch • 1 GHz und 7 GHz fähig, wenn diese Frequenzen verfügbar werden • Suche im Internet nach Wi-Fi Generation 6 für weitere Informationen

Signalübertragung

Die Elektromagnetische Welle

Eine **elektromagnetische Welle**, auch **elektromagnetische Strahlung**, ist eine Welle aus gekoppelten elektrischen und magnetischen Feldern. Bisweilen wird auch kurz von **Strahlung** gesprochen, wobei hier Verwechslungsgefahr zu anderer Teilchenstrahlung besteht. Beispiele für elektromagnetische Wellen sind Radiowellen, Mikrowellen, Wärmestrahlung, Licht, Röntgenstrahlung und Gammastrahlung (Aufzählung nach aufsteigender Frequenz über 20 Größenordnungen hinweg). Elektromagnetische Wellen im Vakuum sind Transversalwellen. Die Wechselwirkung elektromagnetischer Wellen mit Materie hängt von ihrer Frequenz ab.

Quelle: in Anlehnung an https://de.wikipedia.org/wiki/Elektromagnetische_Welle
Abgerufen am 12.04.2023



Quelle: Von user And1mu - modified version of, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=59505315

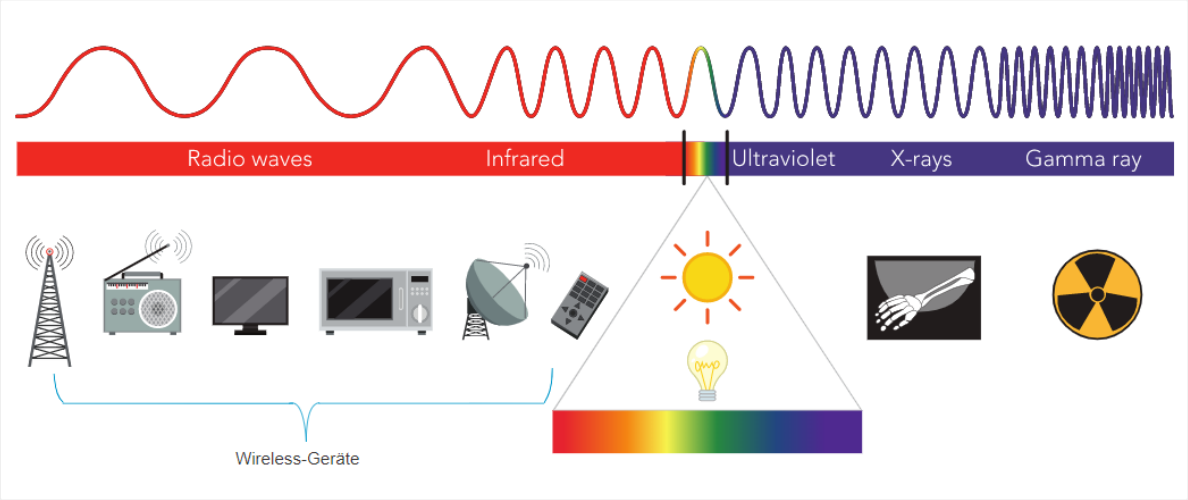
Anders als zum Beispiel Schallwellen benötigen elektromagnetische Wellen kein Medium, um sich auszubreiten.[1] Sie können sich daher auch über weiteste Entfernungen im Weltraum ausbreiten. Sie bewegen sich im Vakuum unabhängig von ihrer Frequenz mit Lichtgeschwindigkeit fort. Elektromagnetische Wellen können sich aber auch in Materie ausbreiten (etwa einem Gas oder einer Flüssigkeit), ihre Geschwindigkeit ist dabei allerdings verringert. Der Brechungsindex gibt das Verhältnis an, um das die Phasengeschwindigkeit von elektromagnetischen Wellen in Materie geringer als die Lichtgeschwindigkeit im Vakuum ist.

Quelle: in Anlehnung an https://de.wikipedia.org/wiki/Elektromagnetische_Welle
Abgerufen am 12.04.2023

Funkfrequenzen

Alle drahtlosen Geräte arbeiten im Radiowellen-Bereich des elektromagnetischen Spektrums. WLAN Netzwerke arbeiten im 2,4-GHz-Frequenzband und im 5-GHz-Band. Wireless LAN-Geräte haben Sender und Empfänger, die auf bestimmte Funkfrequenzen abgestimmt sind, wie in der Abbildung gezeigt. Insbesondere werden die folgenden Frequenzbänder 802.11-Wireless-LANs zugewiesen:

- 2,4 GHz (UHF) - 802.11b/g/n/ax
- 5 GHz (SHF) - 802.11a/n/ac/ax



Übersicht der Frequenzen mit Verwendung

Frequenzbereich	2,4 GHz	5 GHz	6 GHz	60 GHz
Frequenzen	2,3995 bis 2,4845 GHz	5,150 bis 5,350 GHz 5,470 bis 5,725 GHz	5,925 bis 6,425 GHz	57,0 bis 66,0 GHz
Reichweite	innerhalb eines Wohnhauses	begrenzt auf eine Wohnung oder Stockwerk	begrenzt auf eine Wohnung oder Stockwerk	begrenzt auf einen Raum
Kanalbreite	20 und 40 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160 MHz	2 GHz
Nutzung	stark überfüllt	gering	zukünftig	selten

Übersicht der Frequenz im 2,4 GHz Band

Kanal	Trägerfrequenz	Frequenzbereich	Europa	USA	Japan
1	2412 MHz	2399,5 - 2424,5 MHz	×	×	×
2	2417 MHz	2404,5 - 2429,5 MHz	×	×	×
3	2422 MHz	2409,5 - 2434,5 MHz	×	×	×
4	2427 MHz	2414,5 - 2439,5 MHz	×	×	×
5	2432 MHz	2419,5 - 2444,5 MHz	×	×	×
6	2437 MHz	2424,5 - 2449,5 MHz	×	×	×

7	2442 MHz	2429,5 - 2454,5 MHz	×	×	×
8	2447 MHz	2434,5 - 2459,5 MHz	×	×	×
9	2452 MHz	2439,5 - 2464,5 MHz	×	×	×
10	2457 MHz	2444,5 - 2469,5 MHz	×	×	×
11	2462 MHz	2449,5 - 2474,5 MHz	×	×	×
12	2467 MHz	2454,5 - 2479,5 MHz	×		×
13	2472 MHz	2459,5 - 2484,5 MHz	×		×
14	2484 MHz				**× (11b)**

Quelle: in Anlehnung an https://www.elektronik-kompendium.de/sites/net/1712061.htm
Abgerufen am 12.04.2023

Komponenten

Wireless-Netzwerkkarte

Für den Einsatz von WLAN sind mindestens zwei Geräte erforderlich, bei denen ein Funksender und ein Funkempfänger auf die gleichen Funkfrequenzen abgestimmt sind:

- Endgeräte mit Wireless-Netzwerkkarten
- Ein Netzwerkgerät, z. B. ein drahtloser Router oder ein drahtloser AP

Um drahtlos zu kommunizieren, verfügen Laptops, Tablets, Smartphones und sogar die neuesten Autos über integrierte drahtlose NICs, die einen Funksender/-empfänger enthalten. Wenn jedoch ein Gerät keine integrierte Wireless-Netzwerkkarte hat, kann ein USB-Wireless-Adapter verwendet werden, wie in der Abbildung gezeigt.

Hinweis: Viele drahtlose Geräte, die Sie kennen, haben keine sichtbaren Antennen. Sie sind in Smartphones, Laptops und Wireless-Home-Routern integriert.

Wireless Home Router

Der Typ von Infrastrukturgerät, mit dem sich ein Endgerät verknüpft und an dem es sich authentifiziert, variiert je nach Größe und Anforderung des WLAN.

Zum Beispiel verbindet ein Heimanwender normalerweise drahtlose Geräte über einen kleinen, drahtlosen Router, wie in der Abbildung gezeigt. Der Wireless-Router dient als:

- **Access Point** - Dieser bietet über 802.11a/b/g/n/ac drahtlosen Zugriff.
- **Switch** - Das ist ein Switch mit 4 Vollduplex-10/100/1000 Ethernet-Anschlüssen, um kabelgebundene Geräte zu verbinden.
- **Router** - Dieser stellt ein Standard-Gateway für die Verbindung mit anderen Netzwerkinfrastrukturen, wie dem Internet, bereit.

Ein Wireless-Router wird üblicherweise als drahtloses Zugangsgerät für kleine Unternehmen oder Wohnhäuser implementiert. Der Wireless-Router bietet seine drahtlosen Dienste an, indem er Beacons sendet, die seine Shared Service Set Identifier (SSID) enthalten. Geräte empfangen drahtlos die SSID und versuchen, sich mit ihr zu verbinden und zu authentifizieren, um auf das lokale Netzwerk und das Internet zuzugreifen.

Die meisten Wireless-Router bieten auch erweiterte Funktionen, wie High-Speed-Zugriff, Unterstützung für Video-Streaming, IPv6-Adressierung, QoS (Quality of Service), Konfigurationsprogramme und USB-Anschlüsse zum Anschluss von Druckern oder tragbaren Laufwerken.

Darüber hinaus können Heimanwender, die ihre Netzwerkabdeckung erweitern möchten, Wi-Fi-Range Extender einrichten. Ein Gerät kann eine drahtlose Verbindung mit dem Extender herstellen, wodurch sein Signal verstärkt und zum Wireless-Router weitergeleitet wird.

Wireless-Access-Points

Obwohl Range Extender einfach einzurichten und zu konfigurieren sind, wäre die beste Lösung, einen weiteren Wireless Access Point zu installieren, um orgniären drahtlosen Zugriff auf die Benutzergeräte zu ermöglichen. Wireless-Clients nutzen ihre Drahtlos-Netzwerkkarten, um APs in der Nähe zu entdecken, die ihre SSID aussenden. Clients versuchen dann, sich mit einem AP zu verbinden und sich an ihm zu authentifizieren. Nach der Authentifizierung haben Wireless-Benutzer Zugriff auf die Netzwerkressourcen. Die Cisco Meraki Go APs sind in der Abbildung dargestellt.

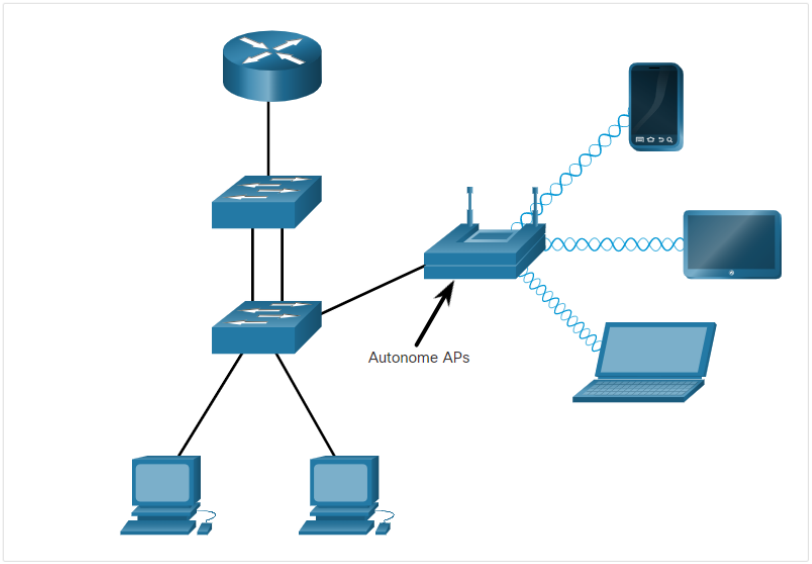
AP Arten

Autonome APs

Controller-basierte APs

Autonome APs

Dies sind eigenständige Geräte, die über die Befehlszeile oder eine GUI konfiguriert werden, wie in der Abbildung gezeigt. Autonome APs sind nützlich in Situationen, in denen nur ein paar APs in der Organisation benötigt werden. Ein Home-Router ist ein Beispiel für einen autonomen AP, da sich die gesamte AP-Konfiguration auf dem Gerät befindet. Wenn die Wireless-Anforderungen steigen, sind mehr APs erforderlich. Jeder AP würde unabhängig von anderen APs arbeiten und jeder AP würde eine manuelle Konfiguration und Verwaltung erfordern. Dies würde aufwändig werden, wenn viele APs benötigt würden.



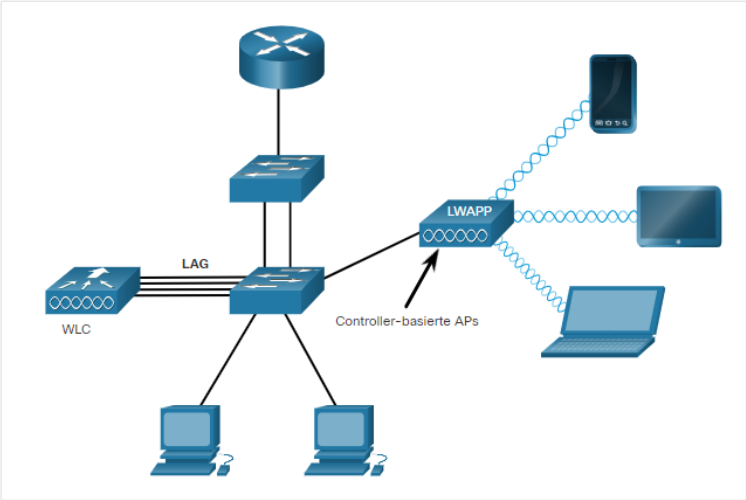
Autonome APs

Controller-basierte APs

Controller-basierte APs

Diese Geräte erfordern keine Erstkonfiguration und werden oft als Lightweight APs (LAPs) bezeichnet. LAPs verwenden das Lightweight Access Point Protocol (LWAPP), um mit einem WLAN-Controller (WLC) zu kommunizieren, wie in der nächsten Abbildung dargestellt. Controller-basierte APs sind nützlich in Situationen, in denen viele APs im Netzwerk benötigt werden. Wenn weitere APs hinzugefügt werden, wird jeder AP automatisch vom WLC konfiguriert und verwaltet.

Beachten Sie, dass der WLC in der Abbildung über vier Ports verfügt, die mit der Switching-Infrastruktur verbunden sind. Diese vier Ports sind als Link Aggregation Group (LAG) konfiguriert, um sie zu bündeln. Ähnlich wie die Funktionsweise von EtherChannel bietet LAG Redundanz und Lastausgleich. Alle Ports des Switches, die an den WLC angeschlossen sind, müssen Trunks sein und EtherChannel aktiviert haben. LAG funktioniert jedoch nicht exakt wie EtherChannel. Der WLC unterstützt weder Port Aggregation Protocol (PAGP) noch Link Aggregation Control Protocol (LACP).



Wireless Antennen

Rundstrahlantennen

Richtantenne

MIMO Antennen

Rundstrahlantennen, wie die in der Abbildung gezeigt, bieten 360-Grad-Abdeckung und eignen sich ideal für Häuser, offene Bürobereiche, Konferenzräume und Außenbereiche.

Rundstrahlantennen

Richtantenne

MIMO Antennen

Richtantennen fokussieren das Funksignal in eine bestimmte Richtung. Dies erhöht das Signal zum und vom AP in die Richtung, in die die Antenne zeigt. Dies bietet eine höhere Signalstärke in eine Richtung und reduziert die Signalstärke in alle anderen Richtungen. Beispiele für gerichtete Wi-Fi-Antennen sind Yagi und Parabolantennen.

Rundstrahlantennen

Richtantenne

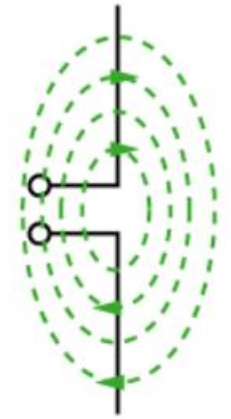
MIMO Antennen

Multiple Input Multiple Output (MIMO) verwendet mehrere Antennen, um die verfügbare Bandbreite für drahtlose IEEE 802.11n/ac/ax Netzwerke zu erhöhen. Bis zu acht Sende- und Empfangsantennen können verwendet werden, um den Durchsatz zu erhöhen.

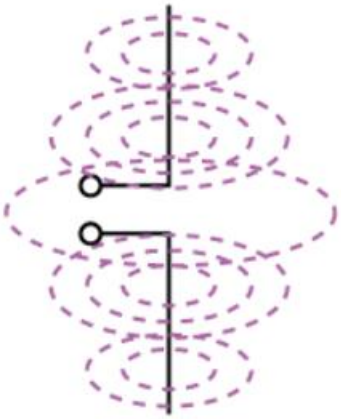
Die Antenne in der einfachsten Form

Per Definition ist eine Antenne eine Sende- und Empfangseinrichtung für elektromagnetische Wellen. Genau genommen ist eine Antenne ein metallischer Wandler für eine elektromagnetische Welle zwischen einer Leitung und dem freien Raum. Antennen empfangen elektromagnetische Wellen und senden bzw. strahlen sie ab. Angeschlossen wird die Antenne wie ein Zweipol. Der Prinzip-Aufbau ist aber ein Vierpol, wobei zwei Pole keine feste physikalische Verbindung haben. Stattdessen hängen sie im freien Raum.

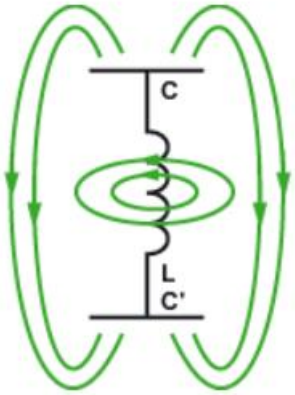
Die einfachste Antenne, der Dipol, besteht aus zwei Drähten. Häufig findet man diese Art der Antenne bei UKW-Tunern als Wurfantenne. Durch den ungeschirmten Draht fließt Strom. Dabei entsteht ein Magnetfeld. An den Spitzen der Drähte bauen sich Ladungen auf und erzeugen ein elektrisches Feld. Magnetisches und elektrisches Feld strahlen abwechselnd in den freien Raum.



Elektrisches Feld E

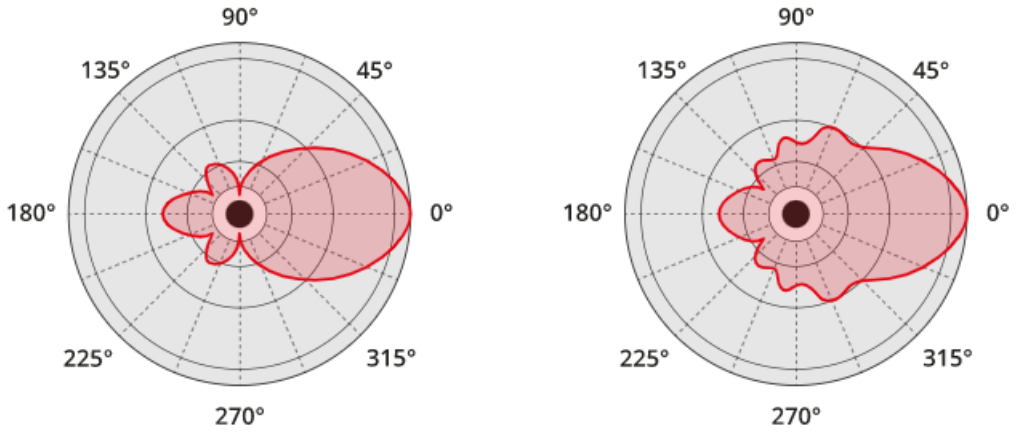


Magnetisches Feld H



Abstrahlung

Antennendiagramm einer Wandantenne. Diese Antenne hat deutliche Richtfunkeigenschaften und strahlt bei richtiger Montage zum Beispiel in Richtung der Büros oder zur Halle. Die zur Wand montierte Seite, im Schaubild links, ist stark gedämpft.



Quelle: in Anlehnung an https://www.kurthelectronic.de/fachwissen/wlan-antenne/
Abgerufen am 12.04.2023

Betrieb von WLAN Netzwerken

Topologien

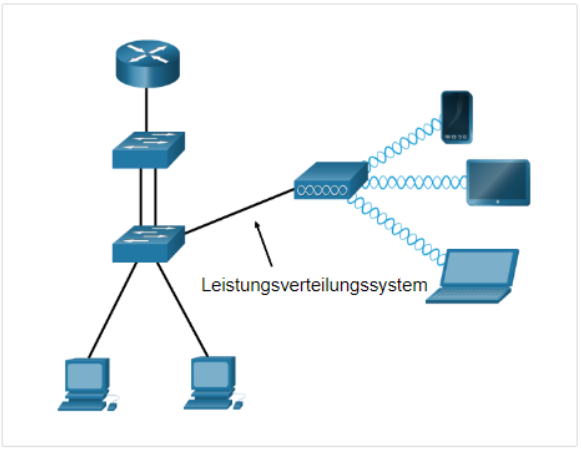
Wireless-LANs können verschiedene Netzwerktopologien annehmen. Der 802.11-Standard beinhaltet zwei Hauptmodi für drahtlose Topologie: Ad-hoc-Modus und Infrastrukturmodus. Tethering ist auch ein Modus, der manchmal verwendet wird, um schnellen drahtlosen Zugriff zu ermöglichen.

Ad-hoc-Modus | Infrastruktur-Modus | Tethering

Ad-hoc-Modus - Das ist, wenn sich zwei Geräte drahtlos in Peer-to-Peer (P2P) -Weise verbinden, ohne APs oder Wireless-Router zu verwenden. Beispiele hierfür sind drahtlose Clients, die sich über Bluetooth oder Wi-Fi Direct direkt miteinander verbinden. Der IEEE 802.11-Standard bezeichnet ein Ad-hoc-Netzwerk als unabhängiges Basic Service Set (IBSS).

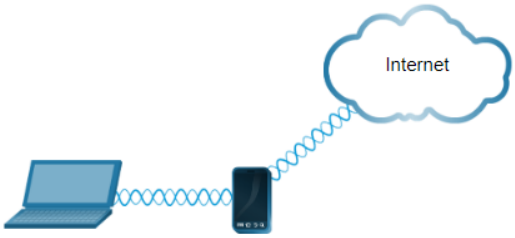
Ad-hoc-Modus | Infrastruktur-Modus | Tethering

Infrastruktur-Modus - Das ist, wenn drahtlose Clients über einen Wireless-Router oder AP (z. B. in WLANs) miteinander verbunden sind. APs stellen über das kabelgebundene Verteilungssystem wie Ethernet eine Verbindung zur Netzwerkinfrastruktur her.



Ad-hoc-Modus | Infrastruktur-Modus | Tethering

Tethering - Eine Variante der Ad-hoc-Topologie ist, wenn mit einem Smartphone oder Tablet bei dem Mobilfunk-Datenzugriff aktiviert ist, ein persönlicher Hotspot erstellt wird. Diese Funktion wird manchmal als Tethering bezeichnet. Ein Hotspot ist in der Regel eine temporäre schnelle Lösung, mit der ein Smartphone die drahtlosen Dienste eines WLAN-Routers bereitstellen kann. Andere Geräte können sich mit dem Smartphone verbinden und authentifizieren, um die Internetverbindung zu verwenden.



Bezeichnungen/Abdeckung

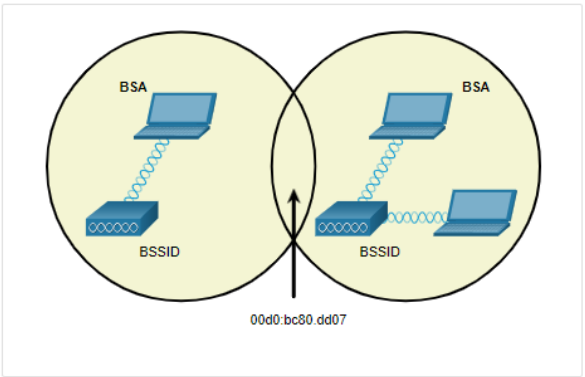
Der Infrastrukturmodus definiert zwei Topologiebausteine: Ein Basic Service Set (BSS) und ein Extended Service Set (ESS).

BBS | ESS

Basic Service Set

Ein BSS besteht aus einem einzigen AP, der alle zugehörigen Wireless-Clients verbindet. Zwei BSSs sind in der Abbildung dargestellt. Die Kreise stellen den Abdeckungsbereich für die BSS dar, der als Basic Service Area (BSA) bezeichnet wird. Wenn ein Wireless-Client seine BSA verlässt, kann er nicht mehr direkt mit anderen Wireless-Clients innerhalb des BSA kommunizieren.

Die Layer-2-MAC-Adresse des AP, die als Basic Service Set Identifier (BSSID) bezeichnet wird, wird verwendet, um jede BSS eindeutig zu identifizieren. Daher ist die BSSID der formale Name des BSS und ist immer nur einem AP zugeordnet.



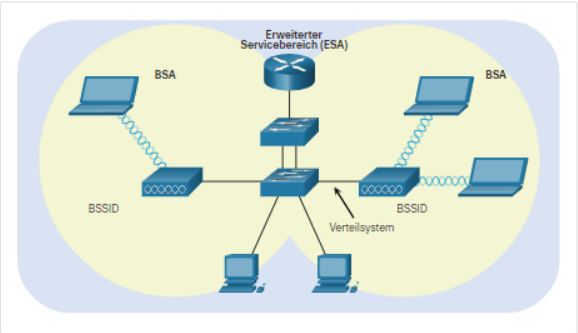
BBS | ESS

Extended Service Set

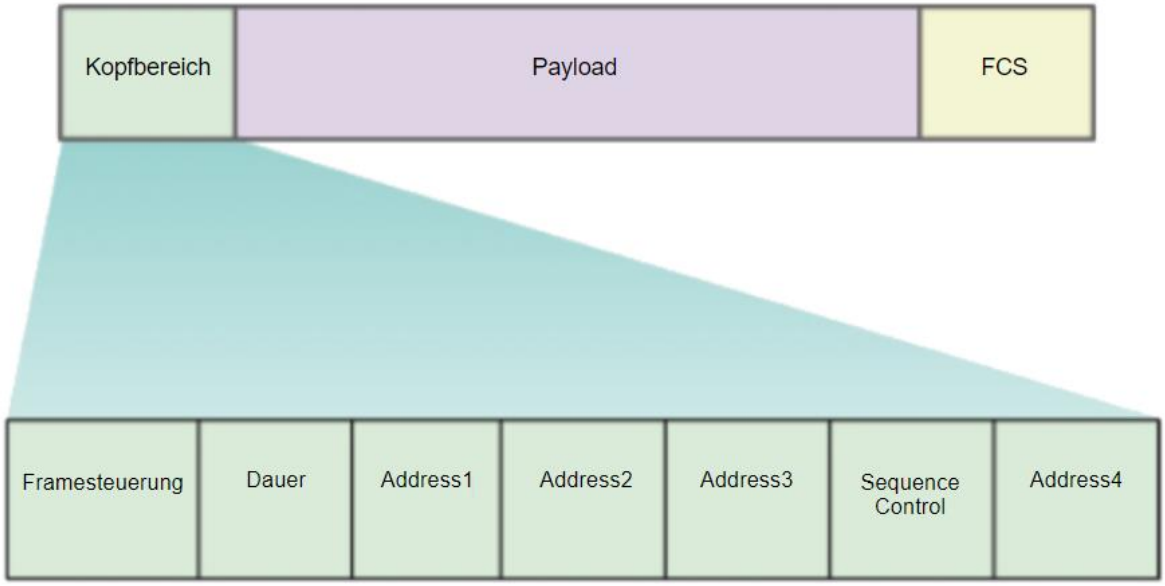
Wenn ein einzelnes BSS eine unzureichende Abdeckung bietet, können zwei oder mehr BSSs über ein Common Distribution System (DS) zu einem ESS zusammengeführt werden. Ein ESS ist die Vereinigung von zwei oder mehr BSSs, die durch einen kabelgebundenen DS miteinander verbunden sind. Jedes ESS wird durch eine SSID identifiziert und jedes BSS wird durch seine BSSID identifiziert.

Wireless-Clients in einem BSA können nun mit Wireless-Clients in einem anderen BSA innerhalb desselben ESS kommunizieren. Roaming: mobile Wireless-Clients können von einem BSA zu einem anderen wechseln (innerhalb desselben ESS) ohne Verbindungsunterbrechung.

Der rechteckige Bereich in der Abbildung zeigt den Abdeckungsbereich, in dem Mitglieder eines ESS kommunizieren können. Dieser Bereich wird als Extended Service Area (ESA) bezeichnet.



Protokollaufbau/Frame



Alle 802.11-Wireless-Frames enthalten die folgenden Felder:

- **Frame-Control** - Gibt den Typ des Wireless-Frames an und enthält Unterfelder für Protokollversion, Frame-Typ, Adresstyp, Energieverwaltung und Sicherheitseinstellungen.
- **Dauer** - Dies wird in der Regel verwendet, um die verbleibende Dauer anzugeben, bis die nächste Frame-Übertragung stattfinden kann.
- **Adresse1** - Dies enthält normalerweise die MAC-Adresse des empfangenden drahtlosen Geräts oder AP.
- **Adresse2** - Dies enthält in der Regel die MAC-Adresse des übertragenden drahtlosen Geräts oder AP.
- **Adresse3** - Diese enthält manchmal die MAC-Adresse des Ziels, z. B. die Router-Schnittstelle (Standard-Gateway), an die der AP angeschlossen ist.

- **Sequenzsteuerung** - Diese enthält Informationen zur Steuerung der Reihenfolge und fragmentierten Frames.
- **Adresse4** - Dies fehlt normalerweise, weil es nur im Ad-hoc-Modus verwendet wird.
- **Nutzlast** - Dies enthält die Daten für die Übertragung.
- **FCS** - Dies wird für Layer 2-Fehlerkontrolle verwendet.

CSMA/CA Verfahren

WLANs sind Halbduplex-Konfigurationen für freigegebene Medien. Halbduplex bedeutet, dass nur ein Client zu einem bestimmten Zeitpunkt senden oder empfangen kann, d.h. die Clients müssen abwechselnd senden. Gemeinsam genutzte Medien bedeutet, dass drahtlose Clients alle auf demselben Funkkanal senden und empfangen können. Dies führt zu einem Problem, da ein Wireless-Client nicht hören kann während er sendet, wodurch es unmöglich ist, eine Kollision zu erkennen.

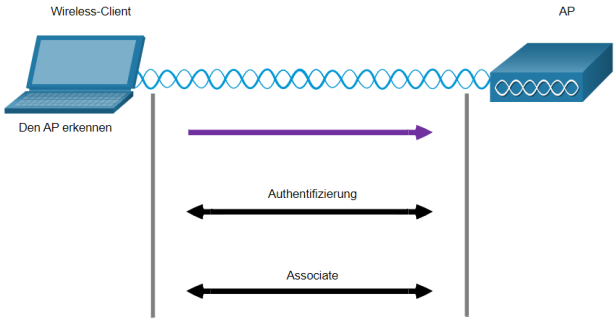
Um dieses Problem zu beheben, verwenden WLANs Carrier Sense Multiple Access (Mehrfachzugriff) mit Collision Avoidance (Kollisionsvermeidung) (CSMA/CA) als Methode, um zu bestimmen, wie und wann Daten im Netzwerk gesendet werden sollen. Ein Wireless-Client führt die folgenden Schritte aus:

1. Er hört den Kanal ab, um zu erkennen, ob dieser unbelegt ist, was bedeutet, dass er prüft, ob kein anderer Funkverkehr derzeit auf dem Kanal ist. Der Kanal wird auch Träger genannt.
2. Er sendet eine RTS-Nachricht (Ready to Send) an den AP, um einen dedizierten Zugriff auf das Netzwerk anzufordern. Dediziert heißt, er erhält einen Kanal zugewiesen, der nur von ihm genutzt wird.
3. Er erhält eine CTS (Clear to Send) -Nachricht vom AP, die den Sendezugriff gewährt.
4. Wenn der Wireless-Client keine CTS-Nachricht empfängt, wartet er eine zufällige Zeit, bevor der Prozess neu gestartet wird.
5. Nachdem er das CTS empfangen hat, überträgt er die Daten.
6. Alle Übertragungen werden quittiert. Wenn ein Wireless-Client keine Bestätigung (Acknowledge) erhält, nimmt er an, dass eine Kollision aufgetreten ist und startet den Prozess neu.

Wireless-Client- und AP-Zuordnung

Damit drahtlose Geräte über ein Netzwerk kommunizieren können, müssen sie sich zunächst einem AP oder einem Wireless-Router zuordnen. Ein wichtiger Teil des 802.11-Prozesses besteht darin, ein WLAN zu erkennen und anschließend eine Verbindung zu ihm herzustellen. Drahtlose Geräte durchlaufen den folgenden dreistufigen Prozess, wie in der Abbildung dargestellt:

- Erkennen eines drahtlosen AP
- Authentifizieren beim AP
- Mit AP verknüpfen



Um erfolgreiche eine Verbindung aufzubauen, müssen ein Wireless-Client und ein AP bestimmte Parameter vereinbaren. Die Parameter müssen dann auf dem AP und anschließend auf dem Client konfiguriert werden, um die Aushandlung einer erfolgreichen Zuordnung zu ermöglichen.

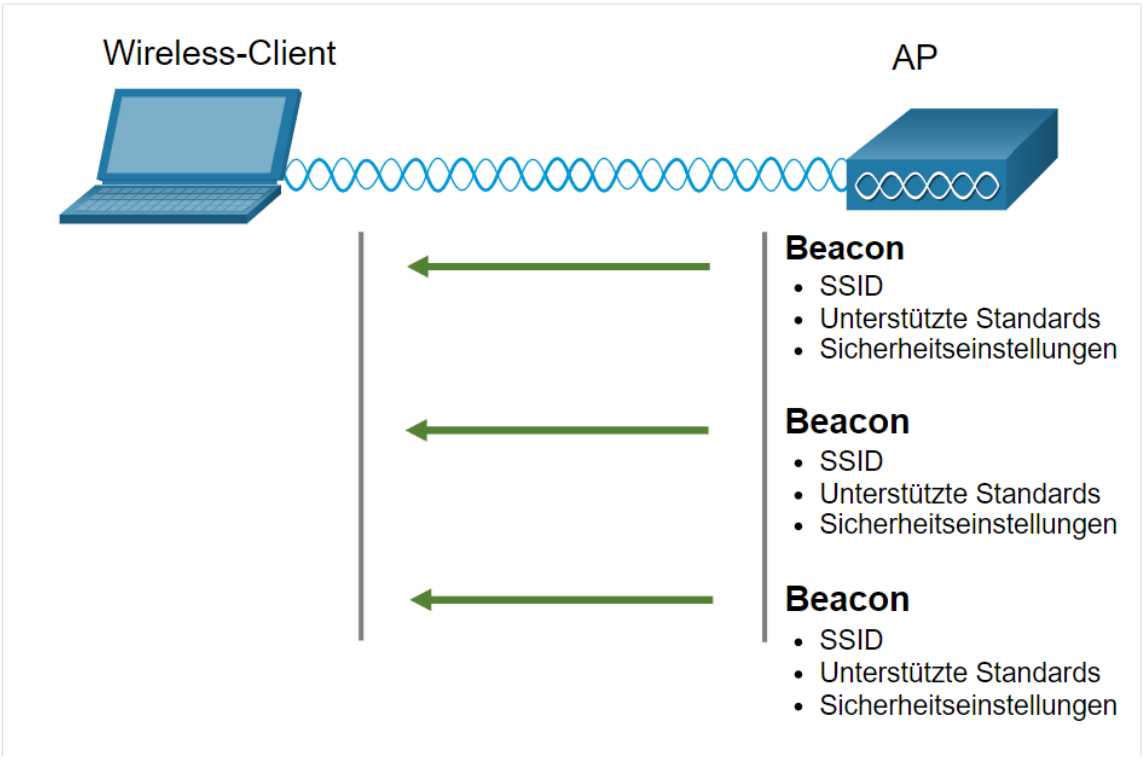
- **SSID** - Der SSID-Name wird in der Liste der verfügbaren drahtlosen Netzwerke auf einem Client angezeigt. In größeren Organisationen, die mehrere VLANs verwenden, um Datenverkehr zu segmentieren, wird jede SSID einem VLAN zugeordnet. Je nach Netzwerkkonfiguration können mehrere APs in einem Netzwerk eine gemeinsame SSID gemeinsam nutzen.
- **Kennwort** - Wird vom Wireless-Client gefordert, um sich beim AP zu authentifizieren.
- **Netzwerkmodus** - Bezieht sich auf die 802.11a/b/g/n/ac/ad WLAN-Standards. APs und Wireless-Router können im Mixed-Modus betrieben werden, was bedeutet, dass gleichzeitig Clients mit unterschiedlichen Standards mit ihnen verbunden sein können.
- **Sicherheitsmodus** - Dies bezieht sich auf die Sicherheitsparametereinstellungen, wie WEP, WPA oder WPA2. Aktivieren Sie immer die höchste unterstützte Sicherheitsstufe.
- **Kanaleinstellungen** - Dies bezieht sich auf die Frequenzbänder, die verwendet werden, um drahtlose Daten zu übertragen. Wireless-Router und APs können die Frequenzbänder scannen und automatisch geeignete Kanaleinstellungen auswählen. Der Kanal kann auch manuell eingestellt werden, wenn Interferenzen mit einem anderen AP oder Wireless-Gerät vorliegen.

Passiver und aktiver Erkennungsmodus

Drahtlose Geräte müssen einen AP oder einen Wireless-Router erkennen und eine Verbindung herstellen. Drahtlose Clients stellen eine Verbindung zum AP mithilfe eines Scanvorgangs (Prüfvorgang) her. Dieser Prozess kann passiv oder aktiv sein.

Passiver Modus | Aktiver Modus

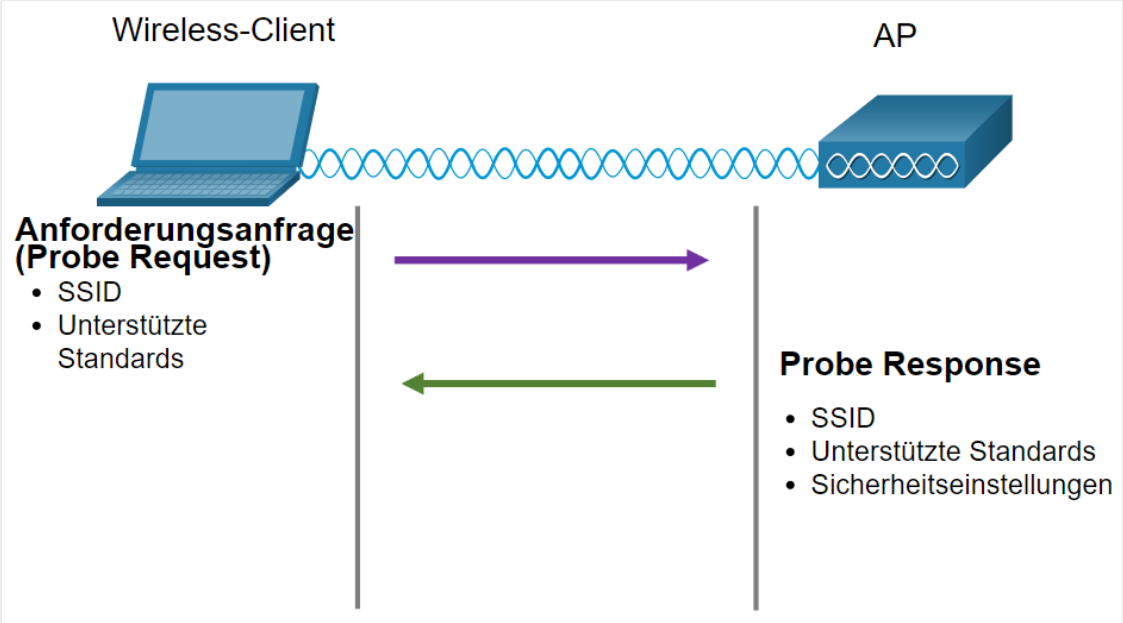
Im passiven Modus bietet der AP seinen Dienst offen an, indem er regelmäßig Broadcast-Beacon-Frames sendet, die die SSID, die unterstützten Standards und Sicherheitseinstellungen enthalten. Der primäre Zweck des Beacons besteht darin, drahtlosen Clients zu ermöglichen, zu erfahren, welche Netzwerke und APs in einem bestimmten Bereich verfügbar sind. Auf diese Weise können die Wireless-Clients auswählen, welches Netzwerk und AP verwendet werden sollen.



Passiver Modus | **Aktiver Modus**

Im aktiven Modus müssen drahtlose Clients den Namen der SSID kennen. Der Wireless-Client initiiert den Prozess, indem er einen Probe-Anforderungs-Frame auf mehreren Kanälen sendet. Die Prüfpunktanforderung enthält den SSID-Namen und die unterstützten Standards. APs, die mit der SSID konfiguriert wurden, senden eine Probe-Antwort, die die SSID, unterstützte Standards und Sicherheitseinstellungen enthält. Der aktive Modus ist möglicherweise erforderlich, wenn ein AP oder ein Wireless-Router so konfiguriert ist, dass er keine Beacon-Frames sendet.

Ein Wireless-Client kann auch eine Probe-Anfrage ohne SSID-Namen senden, um WLAN-Netzwerke in der Nähe zu erkennen. APs, die für einen Broadcast von Beacon-Frames konfiguriert wurden, reagieren auf den Wireless-Client mit einer Probe-Antwort und geben den SSID-Namen an. APs mit deaktivierter Broadcast-SSID-Funktion reagieren nicht.



CAP/WAP

CAPWAP ist ein IEEE-Standardprotokoll, das es einem WLC ermöglicht, mehrere APs und WLANs zu verwalten. CAPWAP ist auch für die Kapselung und Weiterleitung des WLAN-Client-Datenverkehrs zwischen einem AP und einem WLC verantwortlich.

CAPWAP basiert auf LWAPP, fügt jedoch zusätzliche Sicherheit mit Datagram Transport Layer Security (DTLS) hinzu. CAPWAP richtet Tunnel auf UDP-Ports (User Datagram Protocol) ein. CAPWAP kann entweder über IPv4 oder IPv6 betrieben werden, verwendet aber standardmäßig IPv4.

IPv4 und IPv6 können die UDP-Ports 5246 und 5247 verwenden. CAPWAP-Tunnel verwenden jedoch unterschiedliche IP-Protokolle im Frame-Header. IPv4 verwendet IP-Protokoll 17 und IPv6 verwendet IP-Protokoll 136.

Split MAC-Architektur

Eine Schlüsselkomponente von CAPWAP ist das Konzept einer Split Media Access Control (MAC). Das CAPWAP Split-MAC-Konzept übernimmt alle Funktionen, die normalerweise von einzelnen APs ausgeführt werden und verteilt sie auf zwei funktionale Komponenten:

- AP-MAC-Funktionen
- WLC MAC-Funktionen

Die Tabelle zeigt einige der MAC-Funktionen, die von jedem ausgeführt werden.

Tabellenüberschrift	
AP-MAC-Funktionen	**WLC MAC-Funktionen**
Beacons und Probe Responses	Authentifizierung
Paket-Acknowledgements und -Retransmission	Zuordnung und Neu-Zuordnung von Roaming-Clients
Frame-Warteschlange und Paketpriorisierung	Frame-Übersetzung in andere Protokolle
MAC-Layer-Datenverschlüsselung und -entschlüsselung	Weiterleitung des 802.11-Datenverkehrs an eine kabelgebundene Schnittstelle

DTLS-Verschlüsselung

DTLS ist ein Protokoll, das Sicherheit zwischen dem AP und dem WLC bietet. Es ermöglicht ihnen, verschlüsselt zu kommunizieren und verhindert Abhören oder Manipulation.

DTLS ist standardmäßig aktiviert, um den CAPWAP-Steuerungskanal zu sichern, ist aber standardmäßig für den Datenkanal deaktiviert, wie in der Abbildung dargestellt. Der gesamte CAPWAP-Verwaltungs- und Steuerungsverkehr, der zwischen einem AP und WLC ausgetauscht wird, ist verschlüsselt und gesichert, um den Schutz der Steuerungsebene zu gewährleisten und Man-in-the-Middle (MITM) Angriffe zu verhindern.

Die CAPWAP-Datenverschlüsselung ist optional und wird pro AP aktiviert. Für die Datenverschlüsselung muss eine DTLS-Lizenz auf dem WLC installiert sein, bevor sie auf einem AP aktiviert wird. Wenn aktiviert, wird der gesamte WLAN-Client-Datenverkehr vom AP verschlüsselt, bevor er an den WLC weitergeleitet wird und umgekehrt.

FlexConnect APs

FlexConnect ist eine Wireless-Lösung für die Bereitstellung in Zweig- und Außenstellen. Sie ermöglicht die Konfiguration und Steuerung von APs in einer Zweig- oder Außenstelle vom Unternehmenshauptsitz aus über eine WAN-Verbindung, ohne dass an jedem Standort ein Controller vorhanden sein muss.

Für den FlexConnect AP gibt es zwei Betriebsmodi.

- **Verbundener Modus** - Der WLC ist erreichbar. In diesem Modus verfügt der FlexConnect AP über CAPWAP-Konnektivität mit seinem WLC und kann Datenverkehr durch den CAPWAP-Tunnel senden, wie in der Abbildung gezeigt. Der WLC führt alle seine CAPWAP-Funktionen aus.
- **Standalone-Modus** - Der WLC ist nicht erreichbar. Der FlexConnect hat die CAPWAP-Konnektivität verloren oder konnte die mit seinem WLC nicht herstellen. In diesem Modus kann ein FlexConnect-AP einige der WLC-Funktionen übernehmen, z. B. das lokale Wechseln des Clientdatenverkehrs und das lokale Ausführen der Clientauthentifizierung.

Kanalverwaltung

Frequenzkanalsättigung

Wireless LAN-Geräte verfügen über Sender und Empfänger, die auf bestimmte Frequenzen von Funkwellen abgestimmt sind, um zu kommunizieren. Häufig ist es üblich, Frequenzen zu Bereichen zusammenzufassen. Solche Bereiche werden dann in kleinere Bereiche unterteilt, die Kanäle genannt werden.

Wenn die Auslastung eines Kanals zu hoch ist, wird dieser Kanal wahrscheinlich überlastet. Die Überlastung des drahtlosen Mediums beeinträchtigt die Qualität der Kommunikation. Im Laufe der Jahre wurden eine Reihe von Techniken entwickelt, um die drahtlose Kommunikation zu verbessern und die Überlastung zu lindern. Diese Techniken verringern die Kanalauslastung durch effizientere Nutzung der Kanäle.

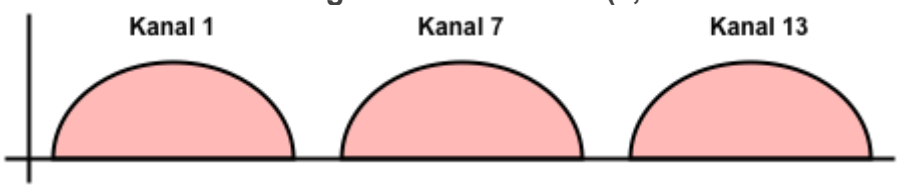
Kanalauswahl

Eine bewährte Vorgehensweise für WLANs, die mehrere APs erfordern, besteht darin, nicht überlappende Kanäle zu verwenden. Zum Beispiel arbeiten die 802.11b/g/n-Standards im 2,4-GHz- bis 2,5-GHz-Spektrum. Das 2,4-GHz-Band ist in mehrere Kanäle unterteilt. Jeder Kanal hat eine Bandbreite von 22 MHz und ist vom nächsten Kanal durch 5 MHz getrennt (Abstand der Trägerfrequenzen). Der 802.11b-Standard legt 11 Kanäle für Nordamerika fest, wie in der Abbildung gezeigt (13 in Europa und 14 in Japan).

Interferenz tritt auf, wenn ein Signal einen Kanal überlappt, der für ein anderes Signal reserviert ist, was zu einer möglichen Störung führt. Die beste Vorgehensweise für 2,4-GHz-WLANs, die mehrere APs erfordern, besteht darin, nicht überlappende Kanäle zu verwenden, wenngleich die meisten modernen APs dies automatisch tun. Wenn drei benachbarte APs vorhanden sind, verwenden Sie die Kanäle 1, 6 und 11, wie in der Abbildung gezeigt.

Für die 5 GHz-Standards 802.11a/n/ac gibt es 24 Kanäle. Das 5 GHz-Band ist in drei Abschnitte unterteilt. Jeder Kanal ist um 20 MHz vom nächsten Kanal getrennt. Die Abbildung zeigt den ersten Abschnitt von acht Kanälen für das 5 GHz-Band. Obwohl es eine leichte Überlappung gibt, stören die Kanäle einander nicht. 5 GHz Wireless kann aufgrund der großen Anzahl an nicht überlappenden Wireless-Kanälen eine schnellere Datenübertragung für Wireless-Clients in stark frequentierten Wireless-Netzwerken ermöglichen.

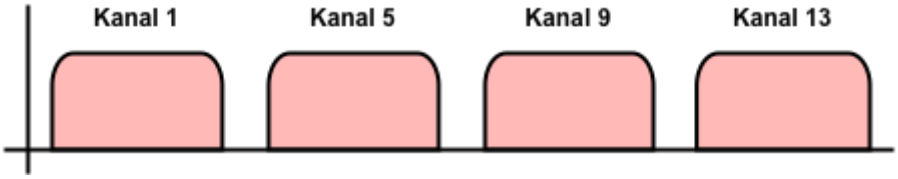
WLAN-Kanal-Verteilung bei IEEE 802.11b (2,4 GHz mit 22 MHz Kanalbreite)



Bei einem WLAN mit IEEE 802.11b empfiehlt es sich, die Kanäle 1, 7 oder 13 einzustellen. Hierbei handelt es sich, bei einer Kanalbreite von 22 MHZ (DSSS), um

die überlappungsfreien Kanäle, bei denen das Frequenzspektrum um 2,4 GHz optimal ausgenutzt wäre.

WLAN-Kanal-Verteilung bei IEEE 802.11g und 802.11n (2,4 GHz mit 20 MHz Kanalbreite)



Quelle: in Anlehnung an https://www.elektronik-kompendium.de/sites/net/1712061.htm
Abgerufen am 12.04.2023

Planen eines WLAN Netzwerks

Die Anzahl der von einem WLAN unterstützten Benutzer hängt vom räumlichen Layout des Netzes ab, einschließlich der Anzahl der Personen und Geräte, die in einen Raum passen, den Datenraten, die Benutzer erwarten, der Verwendung von nicht überlappenden Kanälen durch mehrere APs in einem ESS und der Übertragung von Energieeinstellungen.

Bei der Planung des Standortes von APs ist der ungefähre kreisförmige Abdeckungsbereich wichtig, wie in der Abbildung gezeigt. (Anmerkung: Dies ist aber nur ein grober Anhaltspunkt, da Wände die Ausbreitung stark beeinflussen), aber es gibt einige zusätzliche Empfehlungen:

- Wenn APs vorhandene Verkabelungen verwenden sollen oder wenn es Orte gibt, an denen keine APs platziert werden können, notieren Sie diese Positionen auf der Karte.
- Beachten Sie alle möglichen Störquellen, die Mikrowellenöfen, drahtlose Videokameras, Leuchtstofflampen, Bewegungsmelder oder jedes andere Gerät, das den 2,4-GHz-Bereich verwendet, umfassen können.
- Positionieren Sie APs oberhalb von Hindernissen.
- Positionieren Sie APs vertikal in der Nähe der Decke in der Mitte jedes Abdeckungsbereichs, wenn möglich.
- Positionieren Sie APs an Orten, an denen Benutzer erwartet werden. Beispielsweise sind Konferenzräume in der Regel ein besserer Standort für APs als ein Flur.
- Wenn ein IEEE 802.11-Netzwerk für den gemischten Modus konfiguriert wurde, können die Wireless-Clients langsamere als normale Geschwindigkeiten bekommen, um die älteren Wireless-Standards zu unterstützen.

Bei der Schätzung des erwarteten Abdeckungsbereichs eines AP ist zu beachten, dass dieser Wert in Abhängigkeit vom WLAN-Standard oder der Mischung von Standards, den Örtlichkeiten und der Sendeleistung variiert, für die der AP konfiguriert ist. Beachten Sie bei der Planung von Abdeckungsgebieten immer die Spezifikationen für den AP.

Bedrohungen

Wireless-Sicherheit Überblick

Ein Wireless-Netzwerk ist für alle Personen zugänglich, sie sich in Reichweite des Access-Points befinden und über die passenden Anmeldeinformationen für das Netzwerk verfügen. Mit einer Wireless-Netzwerkkarte und Kenntnissen über Cracking-Techniken muss ein Angreifer möglicherweise nicht physisch an den Arbeitsplatz gelangen, um Zugang zu einem WLAN zu erhalten.

Angriffe können von Außenstehenden, verärgerten Mitarbeitern und sogar unbeabsichtigt von Mitarbeitern ausgelöst werden. Drahtlose Netzwerke sind besonders anfällig für verschiedene Bedrohungen, darunter:

- **Abfangen von Daten** - Drahtlose Daten sollten verschlüsselt werden, um zu verhindern, dass sie abgehört werden.
- **Drahtlose Eindringlinge** - Nicht autorisierte Benutzer, die versuchen, auf Netzwerkressourcen zuzugreifen, können durch effektive Authentifizierungstechniken abgeschreckt werden.
- **Denial-of-Service-Angriffe (DoS)** - Der Zugriff auf WLAN-Dienste kann versehentlich oder in böswilliger Absicht gefährdet werden. Abhängig von der Quelle des DoS-Angriffs gibt es verschiedene Lösungen.
- **Rogue-APs** - Nicht autorisierte APs, die von einem gut meinenden Benutzer oder zu bösartigen Zwecken installiert wurden, können mithilfe von Managementsoftware erkannt werden.

DoS-Angriffe

Wireless-DoS-Angriffe können das Ergebnis sein von:

- **Unsachgemäß konfigurierten Geräte** - Konfigurationsfehler können das WLAN deaktivieren. Beispielsweise könnte ein Administrator versehentlich eine Konfiguration ändern und das Netzwerk deaktivieren, oder ein Eindringling mit Administratorrechten könnte ein WLAN absichtlich deaktivieren.
- **Ein bösartiger Benutzer, der absichtlich die drahtlose Kommunikation stört** - Ihr Ziel ist es, das drahtlose Netzwerk vollständig oder bis zu dem Punkt zu deaktivieren, wo kein berechtigtes Gerät mehr auf das Medium zugreifen kann.
- **Unabsichtliche Störungen** - WLANs sind anfällig für Störungen durch andere drahtlose Geräte, einschließlich Mikrowellenherde, Schnurlostelefone, Babymonitore und mehr, wie in der Abbildung gezeigt. Das 2,4-GHz-Band ist anfälliger für Störungen als das 5-GHz-Band.

Um das Risiko eines DoS-Angriffs durch falsch konfigurierte Geräte und bösartige Angriffe zu minimieren, sollten Sie alle Geräte schützen, Kennwörter sicher halten, Backups erstellen und sicherstellen, dass alle Konfigurationsänderungen außerhalb der Arbeitszeit eingespielt werden.

Überwachen Sie das WLAN auf unbeabsichtigte Störungen und beheben Sie diese, sobald sie auftreten. Da das 2,4-GHz-Band von anderen Gerätetypen verwendet wird, sollte das 5 GHz in Bereichen verwendet werden, die zu Störungen neigen.

Nicht autorisierte Access Points

Ein nicht autorisierter (rogue) AP ist ein AP oder ein Wireless-Router, der ohne ausdrückliche Autorisierung und gegen Unternehmensrichtlinien mit einem Unternehmensnetzwerk verbunden wurde. Jeder mit Zugang zu den Räumlichkeiten kann (böswillig oder nicht böswillig) einen preiswerten WLAN-Router installieren, der möglicherweise den Zugriff auf eine sichere Netzwerkressource ermöglichen kann.

Nach der Verbindung kann der Rogue-AP von einem Angreifer verwendet werden, um MAC-Adressen zu erfassen, Datenpakete zu erfassen, Zugriff auf Netzwerkressourcen zu erhalten oder einen Man-in-the-Middle-Angriff zu starten.

Ein privater Netzwerk-Hotspot könnte ebenso als nicht autorisierter AP verwendet werden. Beispielsweise aktiviert ein Benutzer mit sicherem Netzwerkzugriff seinen autorisierten Windows-Host als WLAN-AP. Dadurch werden die Sicherheitsmaßnahmen umgangen und andere nicht

autorisierte Geräte können nun als freigegebenes (shared) Gerät auf Netzwerkressourcen zugreifen.

Um die Installation nicht autorisierter APs zu verhindern, müssen Organisationen WLCs mit Richtlinien für nicht autorisierte APs konfigurieren, wie in der Abbildung dargestellt und Überwachungssoftware verwenden, um das Funkspektrum auf nicht autorisierte APs aktiv zu überwachen.

Man-in-the-Middle-Attack

Bei einer Man-in-the-Middle-Attack (MITM) wird der Hacker zwischen zwei legitimen Entitäten positioniert, um die Daten, die zwischen den beiden Teilnehmern ausgetauscht werden, zu lesen oder zu ändern. Es gibt viele Möglichkeiten, einen MITM-Angriff zu machen.

Ein beliebter drahtloser MITM-Angriff wird als „böser Twin AP“ -Angriff bezeichnet, bei dem ein Angreifer einen nicht authorisierten AP einführt und ihn mit der gleichen SSID wie einen legitimen AP konfiguriert, wie in der Abbildung gezeigt. Aufgrund der offenen Authentifizierung sind Orte, die kostenloses WLAN anbieten, wie Flughäfen, Cafés und Restaurants, besonders beliebte Orte für diese Art von Angriff.

Wireless-Clients, die versuchen, eine Verbindung zu einem WLAN herzustellen, sehen zwei APs mit derselben SSID, die drahtlosen Zugriff bieten. Diejenigen, die in der Nähe des Schurken-AP sind, empfangen von diesem das stärkere Signal und verbinden sich höchstwahrscheinlich damit. Der Benutzerverkehr wird nun an den nicht autorisierten AP gesendet, der wiederum die Daten erfasst und an den legitimen AP weiterleitet, wie in der Abbildung gezeigt. In umgekehrter Richtung wird der Verkehr vom legitimen AP an den nicht autorisierten AP gesendet, erfasst und dann an den ahnungslosen Benutzer weitergeleitet. Der Angreifer kann Passwörter und persönliche Informationen des Benutzers stehlen, Zugriff auf sein Gerät erhalten und das System gefährden.

Die Besiegbarkeit eines Angriffs wie ein MITM-Angriff hängt von der Raffinesse der WLAN-Infrastruktur und der Wachsamkeit bei der Überwachung der Aktivitäten im Netzwerk ab. Der Prozess beginnt mit der Identifizierung von legitimen Geräten im WLAN. Dazu müssen Benutzer authentifiziert werden. Nachdem alle legitimen Geräte bekannt sind, kann das Netzwerk auf abnormale Geräte oder Datenverkehr überwacht werden.

Sichere WLAN Netzwerke

SSID-Tarnung und MAC-Adressenfilterung

Drahtlose Signale können durch feste Materialien wie Decken, Böden, Wände, nach außerhalb des Gebäudes übertragen werden. Ohne strenge Sicherheitsmaßnahmen kann das Installieren von WLAN mit dem Installieren von Netzwerkdosen außerhalb des Gebäudes verglichen werden.

Um den Herausforderungen, drahtlose Eindringlinge fernzuhalten und Daten zu schützen, zu begegnen wurden zwei frühe Sicherheitsfunktionen verwendet, die auf den meisten Routern und APs noch verfügbar sind: SSID-Tarnung und MAC-Adressenfilterung.

SSID Cloaking

APs und einige Wireless-Router ermöglichen die Deaktivierung des SSID-Beacon-Frames, wie in der Abbildung gezeigt. Wireless-Clients müssen die SSID manuell konfigurieren, um eine Verbindung mit dem Netzwerk herzustellen.

MAC Addresses Filtering

Ein Administrator kann manuell Clients den drahtlosen Zugriff aufgrund der physischen MAC-Hardwareadresse erlauben oder verweigern. In der Abbildung ist der Router so konfiguriert, dass zwei MAC-Adressen zugelassen werden. Geräte mit anderen MAC-Adressen können sich nicht mit dem 2,4-GHz-WLAN verbinden.

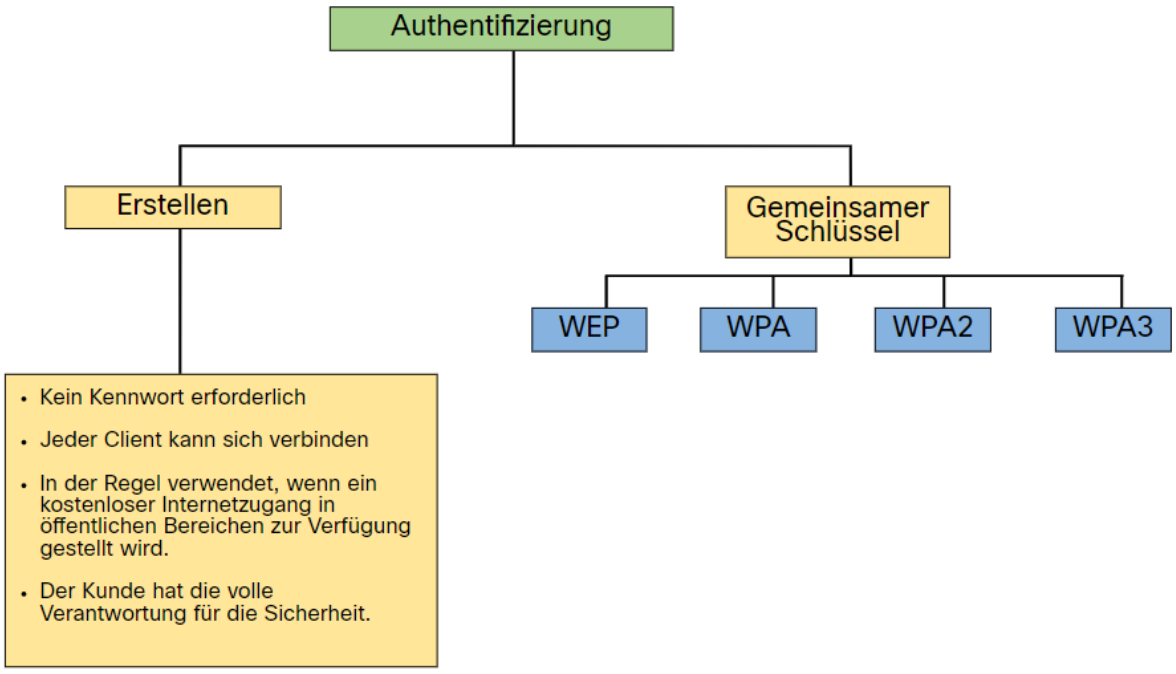
802.11 Authentifizierungsmethoden

Obwohl diese beiden Funktionen die meisten Benutzer abschrecken würden, ist die Realität, dass weder SSID-Tarnung noch MAC-Adressfilterung einen versierten Eindringling abschrecken würden. SSIDs werden leicht erkannt, selbst wenn APs sie nicht übertragen und MAC-Adressen können gefälscht werden. Der beste Weg, ein drahtloses Netzwerk zu sichern, ist der Einsatz von Authentifizierungs- und Verschlüsselungssystemen.

Mit dem ursprünglichen 802.11-Standard wurden zwei Authentifizierungsmethoden eingeführt.

- **Offene Systemauthentifizierung** - Jeder drahtlose Client sollte leicht in der Lage sein, eine Verbindung herzustellen und sollte nur in Situationen verwendet werden, in denen Sicherheit nicht wichtig ist, wie z. B. kostenlosen Internetzugang in Cafés, Hotels und in abgelegenen Gebieten. Der drahtlose Client ist für die Sicherheit verantwortlich, z. B. die Verwendung eines virtuellen privaten Netzwerks (VPN), um eine sichere Verbindung herzustellen. VPNs bieten Authentifizierungs- und Verschlüsselungsdienste. VPNs sind nicht Thema dieses Kapitels.
- **Shared Key-Authentifizierung** – Diese Methode stellt Mechanismen zum Authentifizieren und Verschlüsseln von Daten zwischen einem Wireless-Client und AP oder Wireless-Router bereit. Das sind z. B. WEP, WPA, WPA2, WPA3. Um eine Verbindung herzustellen, muss das Kennwort jedoch zwischen beiden Parteien vorab ausgetauscht werden.

In der folgenden Tabelle werden diese Authentifizierungsmethoden zusammengefasst.



Shared Key Authentifizierungsmethoden

Es stehen vier Methoden zur Authentifizierung mit shared Key zur Verfügung, wie in der Tabelle beschrieben. Bis die Verfügbarkeit von WPA3-Geräten allgemein verbreitet ist, sollten drahtlose Netzwerke den WPA2-Standard verwenden.

Tabellenüberschrift	
Authentifizierungsmethode	**Beschreibung**
Wired Equivalent Privacy (WEP)	Die ursprüngliche 802.11-Spezifikation, die entwickelt wurde, um die Daten zu sichern verwendet die Rivest Cipher 4 (RC4) Verschlüsselungsmethode mit einem statischen Schlüssel. Allerdings ändert sich der Schlüssel nie beim Austausch von Paketen. Dies macht es einfach ihn zu hacken. WEP wird nicht mehr empfohlen und sollte niemals verwendet werden.
Wi-Fi Protected Access (WPA)	Ein WIFI-Alliance-Standard, der WEP verwendet, aber die Daten mit dem viel stärkeren Temporal Key Integrity Protocol (TKIP) Algorithmus verschlüsselt. TKIP ändert den Schlüssel für jedes Paket, wodurch er deutlich schwerer zu hacken ist.
WPA2	WPA2 ist der aktuelle Industriestandard für die Sicherung drahtloser Netzwerke. Es verwendet Advanced Encryption Standard (AES) zur Verschlüsselung: AES gilt derzeit als das stärkste Verschlüsselungsprotokoll.
WPA3	Die nächste Generation der WLAN-Sicherheit. Alle WPA3-fähigen Geräte verwenden die neuesten Sicherheitsmethoden, verbieten veraltete Protokolle und erfordern die Verwendung von Protected Management Frames (PMF). Geräte mit WPA3 sind noch nicht weit verbreitet.

Authentifizieren von Benutzern

Home-Router haben in der Regel zwei Möglichkeiten für die Authentifizierung: WPA und WPA2. WPA2 ist der Stärkere der beiden. Die Abbildung zeigt die Möglichkeit, eine von zwei WPA2-Authentifizierungsmethoden auszuwählen:

- **Persönlich** - Für Heimnetzwerke oder kleine Büronetzwerke gedacht, Benutzer authentifizieren sich mit einem Pre-Shared Key (PSK). Wireless-Clients authentifizieren sich am Wireless-Router mit einem vorab mitgeteilten Kennwort. Es ist kein spezieller Authentifizierungsserver erforderlich.
- **Enterprise** - Für Unternehmensnetzwerke vorgesehen, erfordert jedoch einen RADIUS-Authentifizierungsserver (Remote Authentication Dial-In User Service). Obwohl es komplizierter einzurichten ist, bietet es zusätzliche Sicherheit. Das Gerät muss vom RADIUS-Server authentifiziert werden, dann müssen Benutzer sich mit dem 802.1X-Standard authentifizieren, der das EAP (Extensible Authentication Protocol) für die Authentifizierung verwendet.

Verschlüsselungsmethoden

Verschlüsselung wird zum Schutz von Daten eingesetzt. Wenn ein Eindringling verschlüsselte Daten erfasst hat, wäre er nicht in der Lage, diese in angemessener Zeit zu entziffern.

Die WPA- und WPA2-Standards verwenden die folgenden Verschlüsselungsprotokolle:

- **Temporal Key Integrity Protocol (TKIP)** - TKIP ist die von WPA verwendete Verschlüsselungsmethode. Es bietet Unterstützung für ältere WLAN-Geräte durch Behebung der ursprünglichen Fehler, die mit der 802.11 WEP-Verschlüsselungsmethode verbunden sind. Es verwendet WEP, verschlüsselt aber die Layer 2-Nutzlast mit TKIP und führt einen Message Integrity Check (MIC) im verschlüsselten Paket durch, um sicherzustellen, dass die Nachricht nicht geändert wurde.
- **Advanced Encryption Standard (AES)** - AES ist die von WPA2 verwendete Verschlüsselungsmethode. Es ist die bevorzugte Methode, weil es eine viel stärkere Methode der Verschlüsselung ist. Es verwendet den Counter Cipher Mode mit Block Chaining Message Authentication Code Protocol (CCMP), mit dem Zielhosts erkennen können, ob die verschlüsselten und die nicht verschlüsselten Bits geändert wurden.

Authentifizierung im Unternehmen

In Netzwerken mit strengeren Sicherheitsanforderungen ist eine zusätzliche Authentifizierung oder Anmeldung erforderlich, um Wireless-Clients den Zugriff zu gewähren. Für den Enterprise-Sicherheitsmodus ist ein AAA RADIUS-Server (Authentication, Authorization and Accounting) erforderlich.

- **RADIUS-Server IP Address** Das ist die erreichbare Adresse des RADIUS-Servers
- **UDP Port Nummers** - Offiziell zugewiesene UDP-Ports: 1812 für RADIUS-Authentifizierung und 1813 für RADIUS-Accounting. Kann aber auch mit den UDP-Ports 1645 und 1646 betrieben werden, wie in der Abbildung gezeigt.
- **Shared Key** - Wird verwendet, um den AP beim RADIUS-Server zu authentifizieren.

Der shared key ist kein Parameter, der auf einem Wireless-Client konfiguriert werden muss. Er ist nur auf dem AP erforderlich, um sich beim RADIUS-Server zu authentifizieren. Die Benutzerauthentifizierung und Autorisierung erfolgt durch den 802.1X-Standard, der eine zentralisierte, serverbasierte Authentifizierung von Endbenutzern ermöglicht.

Der 802.1X-Anmeldeprozess verwendet EAP, um mit dem AP- und RADIUS-Server zu kommunizieren. EAP ist ein Framework zur Authentifizierung des Netzwerkzugriffs. Es kann einen sicheren Authentifizierungsmechanismus bereitstellen und einen sicheren privaten Schlüssel aushandeln, der dann für eine drahtlose verschlüsselte Sitzung mit TKIP- oder AES-Verschlüsselung verwendet werden kann.

WPA3

Zum Zeitpunkt der Erstellung dieses Kurses waren Geräte, die die WPA3-Authentifizierung unterstützen, nicht weit verbreitet. WPA2 gilt jedoch nicht mehr als sicher. WPA3 ist, sofern verfügbar, die empfohlene 802.11-Authentifizierungsmethode. WPA3 umfasst vier Funktionen:

- WPA3-Personal
- WPA3-Enterprise
- Open Networks
- Internet of Things (IoT) Onboarding

WPA3-Personal

In WPA2-Personal können Bedrohungsakteure den „Handshake“ zwischen einem drahtlosen Client und dem AP abhören und einen Brute-Force-Angriff verwenden, um zu versuchen, die PSK zu erraten. WPA3-Personal vereitelt diesen Angriff, indem SAE (Simultaneous Authentication of Equals) verwendet wird, eine in IEEE 802.11-2016 spezifizierte Funktion. Der PSK wird nie öffentlich verwendet, was es dem Bedrohungsakteur unmöglich macht, ihn zu erraten.

WPA3-Enterprise

WPA3-Enterprise verwendet weiterhin 802.1X/EAP-Authentifizierung. Es erfordert jedoch die Verwendung einer 192-Bit-Kryptografie-Suite und eliminiert das Mischen von Sicherheitsprotokollen von früheren 802.11-Standards. WPA3-Enterprise hält sich an die Commercial National Security Algorithm (CNSA) Suite, die häufig in Hochsicherheits-Wi-Fi-Netzwerken verwendet wird.

Open Networks

Offene Netzwerke in WPA2 senden Benutzerdatenverkehr in nicht authentifiziertem, Klartext. In WPA3 verwenden offene oder öffentliche Wi-Fi-Netzwerke immer noch keine Authentifizierung. Sie verwenden jedoch Opportunistic Wireless Encryption (OWE), um den gesamten drahtlosen Datenverkehr zu verschlüsseln.

IoT Onboarding

Obwohl WPA2 Wi-Fi Protected Setup (WPS) enthielt, um Geräte schnell zu einzugliedern, ohne sie vorher zu konfigurieren, ist WPS anfällig für eine Vielzahl von Angriffen und wird nicht empfohlen. Darüber hinaus sind IoT-Geräte in der Regel headless, was bedeutet, dass sie keine integrierte GUI für die Konfiguration haben und eine einfache Möglichkeit brauchten, mit dem drahtlosen Netzwerk verbunden zu werden. Das Device Provisioning Protocol (DPP) wurde entwickelt, um diesem Bedarf zu begegnen. Jedes headless Gerät verfügt über einen fest codierten öffentlichen Schlüssel. Der Schlüssel wird normalerweise auf der Außenseite des Geräts oder seiner Verpackung als Quick Response (QR) -Code gestempelt. Der Netzwerkadministrator kann den QR-Code scannen und schnell das Gerät integrieren. Obwohl es nicht im engeren Sinn Teil des WPA3-Standards ist, wird DPP WPS im Laufe der Zeit ersetzen.

IEEE 802.1x / RADIUS

IEEE 802.1x ist ein sicheres Authentifizierungsverfahren für Zugangskontrollen in lokalen Netzwerken (LAN). Im Zusammenhang mit IEEE 802.1x werden auch häufig EAP und RADIUS genannt.
Das Protokoll EAP (Extensible Authentication Protocol), das ursprünglich als Erweiterung für PPP-Verbindungen entwickelt wurde, ist der Kern von IEEE 802.1x. IEEE 802.1x beschreibt die Einbettung von EAP-Datagrammen in Ethernet-Frames. Das ermöglicht den Austausch von Authentifizierungsnachrichten auf der Schicht 2 des OSI-Schichtenmodells.
EAP beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentifizierungsdaten vom Benutzer zum Authentifizierungs-Server und dessen Antworten ausgetauscht werden.
RADIUS kann bei der Anbindung einer zentralen Benutzerverwaltung eine wichtige Rolle spielen. Aber, IEEE 802.1x schreibt keinen RADIUS-Server vor. Doch in der Regel wird beim Einsatz einer Zugangskontrolle mit IEEE 802.1x auch ein RADIUS-Server eingesetzt.

Im Zusammenhang mit WLAN wird die Authentifizierungsmethode IEEE 802.1x auch als WPA2-Enterprise, WPA2-1x oder WPA2/802.1x bezeichnet.

Fehlersuche

In den vorangegangenen Themen haben Sie einiges über die WLAN-Konfiguration erfahren. Hier wird die Fehlerbehebung bei WLAN-Problemen diskutiert.

Netzwerkprobleme können einfach oder komplex sein und aus einer Kombination von Hardware-, Software- und Verbindungsproblemen entstehen. Techniker müssen in der Lage sein, das Problem zu analysieren und die Ursache des Fehlers zu ermitteln, bevor sie das Netzwerkproblem beheben können. Dieser Vorgang wird als Fehlerbehebung bezeichnet.

Die Fehlerbehebung jeglicher Art von Netzwerkproblemen sollte einem systematischen Ansatz folgen. Eine gängige und effiziente Fehlerbehebungsmethodik nutzt einen wissenschaftlichen Ansatz und kann in sechs Hauptschritte unterteilt werden, wie in der Abbildung gezeigt.

Schritt	Titel	Beschreibung
1	Identifizieren des Problems	Der erste Schritt bei der Fehlerbehebung besteht darin, das Problem zu identifizieren. Obwohl in diesem Schritt Werkzeuge verwendet werden können, ist ein Gespräch mit dem Benutzer oft hilfreich.
2	Aufstellen einer Theorie über die wahrscheinlichen Ursachen	Nach einem Gespräch mit dem Benutzer und dem Identifizieren des Problems können Sie versuchen, eine Theorie über die wahrscheinlichen Ursachen aufzustellen. Dieser Schritt führt oft zu mehr als einer Ursache.
3	Testen der Theorie zur Ermittlung der Ursache	Auf der Grundlage möglicher Ursachen prüfen Sie Ihre Theorien hinsichtlich der Ursache des Problems. Ein Techniker wird oft ein schnelles Verfahren zur Lösung des Problems bevorzugen. Sollte dies das Problem nicht behebt, müssen Sie möglicherweise das Problem weiter untersuchen, um die genaue Ursache zu ermitteln.
4	Erstellen eines Maßnahmenplans zur Behebung des Problems und Implementierung der Lösung	Nachdem Sie die genaue Ursache des Problems ermittelt haben, entwerfen Sie einen Aktionsplan, um das Problem zu lösen und die Lösung zu implementieren.
5	Überprüfen der ordnungsgemäßen Funktion des gesamten Systems und Implementieren von vorbeugenden Maßnahmen	Nachdem Sie das Problem behoben haben, prüfen Sie die volle Funktionalität und führen präventive Maßnahmen durch.
6	Dokumentieren von Erkenntnissen, Maßnahmen und Ergebnissen	Im letzten Schritt des Fehlerbehebungsverfahrens sollten Sie Ihre Erkenntnisse, Maßnahmen und Ergebnisse dokumentieren. Dies ist als zukünftige Referenz sehr wichtig.

Um das Problem zu beurteilen, ermitteln Sie, bei wie vielen Geräten im Netzwerk dieses auftritt. Wenn ein Problem bei einem Gerät im Netzwerk besteht, beginnen Sie mit dem Fehlerbehebungsverfahren auf diesem Gerät. Wenn ein Problem bei allen Geräten im Netzwerk besteht, beginnen Sie das Fehlerbehebungsverfahren auf dem Gerät, mit dem alle anderen Geräte verbunden sind. Sie sollten eine logische und konsequente Methode zur Diagnose von Netzwerkproblemen entwickeln, bei der Sie ein Problem nach dem anderen eliminieren.