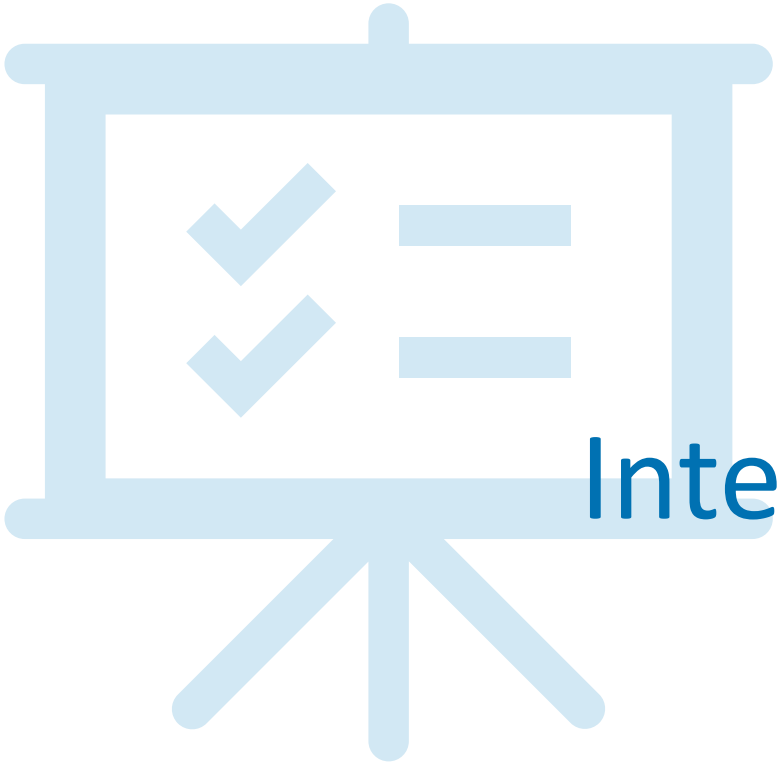

Netzwerke und Internettechnologien 2

WLAN
(Wireless Local Area Network)

Netzwerke und Internettechnologien 2

Lernziele

1

WLAN

Grundlagen

2

WLAN

Sicherheit

WLAN (Wireless Local Area Network)

- Ein WLAN ist ein Netzwerk, das für die Übertragung von Daten Funksignale statt Kabelverbindungen nutzt.
- WLAN arbeitet im GHz-Bereich und ermöglicht Datenübertragungsraten, die unter guten Bedingungen, an die eines verkabelten Netzwerkes heranreichen.
- WLAN-Anwendungen:
  - Kabellose Vernetzung in der Wohnung oder im Haus
  - Örtlich wechselnde Arbeitsplätze
  - Einfache Netzwerkanbindung in Besprechungsräumen
  - Alternative, wo keine Netzwerkverkabelung möglich oder zu teuer ist
  - Öffentliche Hot Spots

WLAN (Wireless Local Area Network)

Funkspektren und Regulierungsbehörde

- Der Ausdruck Spektrum bezieht sich auf den zusammenhängenden Frequenzbereich, über den Funkwellen übertragen werden.
- In Deutschland reguliert die Bundesnetzagentur, wie verschiedene Bereiche des Funkspektrums genutzt werden dürfen.
- Das Funkspektrum ist in viele kleine Bereiche unterteilt, die Frequenzbänder genannt werden und die für bestimmte Nutzungszwecke reserviert sind.
- Zwei der Bänder im Spektrum sind für WLAN vorgesehen, nämlich 2,4 bis 2,4835 GHz und 5,15 bis 5,725 GHz.

WLAN (Wireless Local Area Network)

Funkspektren und Regulierungsbehörde

- Hinweis:
  - Zu beachten gilt, dass diese Bänder nicht ausschließlich von WLANs genutzt werden.
  - Das 2,4-GHz-Band wird beispielsweise auch von Bluetooth genutzt.
  - Daher können entsprechende Geräte gelegentlich auch den WLAN-Betrieb stören.

- Drahtlose Netzwerke können ihre Daten über einen oder mehrere Kanäle übertragen. Diese Einstellung wird normalerweise am Access-Point erledigt.
- Moderne WLAN-Hardware, z.B. in Notebooks oder Smartphones, erkennt den genutzten Kanal automatisch.

WLAN (Wireless Local Area Network)

Netzwerkname

SSID - Service Set Identifier

- Drahtlose Netzwerke haben einen Namen, der als SSID bezeichnet wird.. Die SSID wird in der Regel am Accesspoint festgelegt. Über diese ist die Auswahl des korrekten Netzwerkes am Client (z.B. Notebook) möglich.

Multi SSID

- Ein Wireless Access Point kann u.U. mit mehrere SSIDs arbeiten. Solche multiplen SSID ermöglichen einem Wireless Access Point, mehrere Virtual Local Area Networks (VLAN) aufzubauen.
- Auf diese Weise können mehrere, voneinander strikt getrennte WLAN-Netzwerke angeboten werden. Der einfachste Anwendungsfall ist der WLAN-Gastzugang, den diverse Router anbieten.

WLAN (Wireless Local Area Network)

Topologie

- WLANs sind in Zelltopologie aufgebaut.
- In der Zelltopologie des WLANs agiert ein zentraler Access Point (AP) als Schaltstelle. Eine Funkzelle besteht zumindest aus einem Sender, dem Wireless Access Point (WAP), und einem Empfänger, z.B. einem Notebook.
- Die Anzahl der Clients in einem WLAN liegt bei modernen Standards theoretisch bei 255. In der Praxis begrenzen die Hersteller von Access Points diese auf einen deutlich geringeren Wert, meist unterhalb von 225.
- Die Funkzellengröße wird maßgeblich von der (zulässigen) Sendeleistung der Access Points bestimmt, aber auch von der Funkfrequenz und den physikalischen Bedingungen in der Funkzelle.

WLAN (Wireless Local Area Network)

Modi

Ad-hoc-Modus

- Lässt sich schnell und ohne größeren Aufwand einrichten.
- Alle Stationen sind gleichberechtigt und organisieren sich für die Kommunikation selbst.
- Alle Stationen verwenden dieselbe SSID.
- Eignet sich nur für eine begrenzte Anzahl an Stationen, die in Sendereichweite beieinander stehen müssen.
- Zur Vergrößerung der Reichweite können die teilnehmenden Stationen mit Routing-Fähigkeiten ausgestattet werden, um Daten zwischen Geräten weiterzuleiten, die sich außerhalb der Sendereichweite befinden.

Abbildung 1: WLAN_Ad-hoc (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Modi

Infrastruktur-Modus

- Die zentrale Komponente bildet der Wireless Access Point über den die gesamte Kommunikation zwischen den angeschlossenen Stationen und zu anderen Netzen läuft.
- Der Access Point übernimmt die Koordination der Clients und sendet kleine Datenpakete, engl. Beacons, an alle Stationen. Dadurch werden ein leichterer Verbindungsaufbau und eine Überwachung der Verbindungsqualität möglich.
- Die angeschlossenen Stationen kommunizieren miteinander mit derselben SSID.
- Der Access Point kann die Verbindung zum kabelgebundenen Netz herstellen.

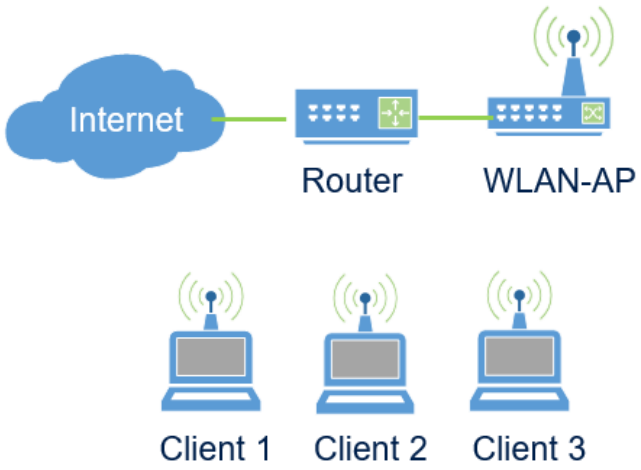

Abbildung 2: WLAN_Infrastruktur (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Wi-Fi-Direct

- Statt über Kabel werden die Daten zum Beispiel von einem Computer zu einem Smartphone oder von einer Digitalkamera zu einem Drucker übertragen.
- Für die Datenübertragung weder ein Access Point noch ein Hot Spot notwendig, die Wi-Fi-fähigen Geräte arbeiten selbst als Basisstation.

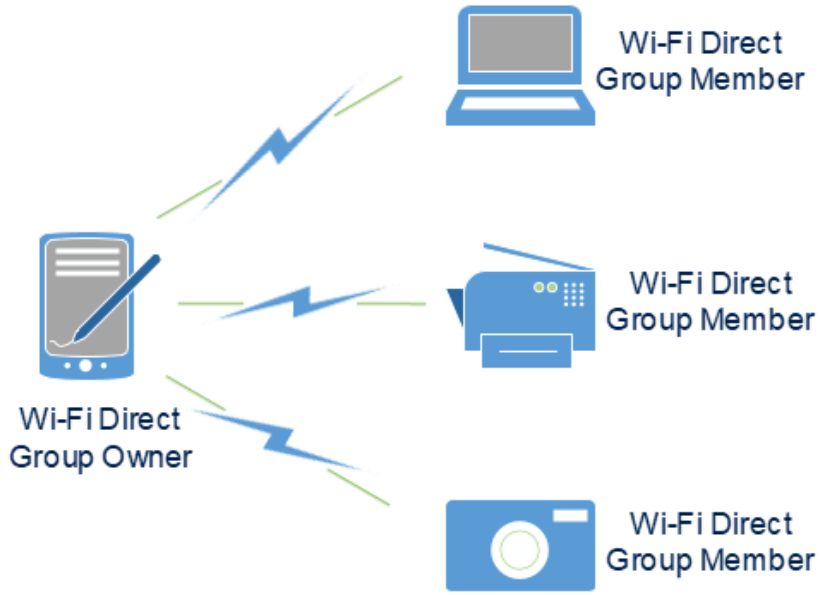

Abbildung 3: Wi-Fi-Direct_Ad-hoc (Eigene Darstellung)

WLAN (Wireless Local Area Network)

IEEE-802.11-Standards

Übertragungsgeschwindigkeiten

- "IEEE 802.11" definiert den Standard für die technischen Lösungen, die dem Aufbau eines Wireless LAN zugrunde liegt.
- Als Funkstandards kommen nur noch 802.11a/g/n/ac/ad zum Einsatz, während das veraltete 802.11b nicht mehr verwendet wird.
- IEEE 802.11ad funktioniert nur auf eine Entfernung von bis zu 10 m und im gleichen Raum.

Standard	Frequenzen	Streams	Datenrate (brutto)	Datenrate (typisch)	Datenrate (Praxis)
IEEE 802.11	2,4 GHz	1	2 Mbit/s	2 Mbit/s	0,5 - 1 Mbit/s
IEEE 802.11b	2,4 GHz	1	11 Mbit/s	11 Mbit/s	1 - 5 Mbit/s
IEEE 802.11a/h/j	5 GHz	1	54 Mbit/s	54 Mbit/s	bis 32Mbit/s
IEEE 802.11g	2,4 GHz	1	54 Mbit/s	54 Mbit/s	2 -16 Mbit/s
IEEE 802.11n	2,4 GHz	1 2 3 4	150 Mbit/s 300 Mbit/s 450 Mbit/s 600 Mbit/s	72 Mbit/s 144 Mbit/s 216 Mbit/s 288 Mbit/s	bis 50 Mbit/s bis 100 Mbit/s bis 150 Mbit/s bis 200 Mbit/s
	5 GHz	1 2 3 4	150 Mbit/s 300 Mbit/s 450 Mbit/s 600 Mbit/s		
IEEE 802.11ac	5 GHz	1 2 3 4 5…8	433 Mbit/s 867 Mbit/s 1.300 Mbit/s 1.733 Mbit/s bis 6936 Mbit/s	bis 400 Mbit/s bis 800 Mbit/s bis 1.200 Mbit/s bis 1.600 Mbit/s	
IEEE 802.11ad	60 GHz	1	4.620 Mbit/s 6.757 Mbit/s	4.620 Mbit/s 6.757 Mbit/s	2.500 Mbit/s

WLAN (Wireless Local Area Network)

MIMO - Multiple Input Multiple Output

- Bei dieser Technik sendet der Access Point mehrere unabhängige Datenströme.
- Jeder Datenstrom wird als Spatial Stream (SS) bezeichnet, weil er unterschiedliche Pfade durch den Raum benutzt und darüber Daten zum Receiver bzw. WLAN-Client transportiert.
- Je nach WLAN-Standard kann ein Transmitter zwei, vier oder sogar acht Spatial Streams unterstützen. Bei WLANs nach 802.11n sind es maximal vier Spatial Streams, bei 802.11ac acht.
- Die Zahl der gleichzeitig nutzbaren Streams hängt neben dem WLAN-Standard auch von der Zahl der vorhandenen Antennen am Access Point und am Client ab.

WLAN (Wireless Local Area Network)

Spatial Streams – Verschiedene Räumliche Streams

- Die Anzahl an Spatial Streams ist maßgeblich für die Datenrate.
- Mit Hilfe der MIMO-Technik sind beim Standard 802.11n Datendurchsatzraten bis zu 600 Mbit/s (brutto) möglich, aber nur im 5 GHz-Band und mit jeweils vier Antennen auf Sender- und Empfängerseite.
- Da z.B.: ein Notebooks höchstens drei, meist sogar nur zwei Antennen besitzt, ist das ein rein theoretischer Wert.

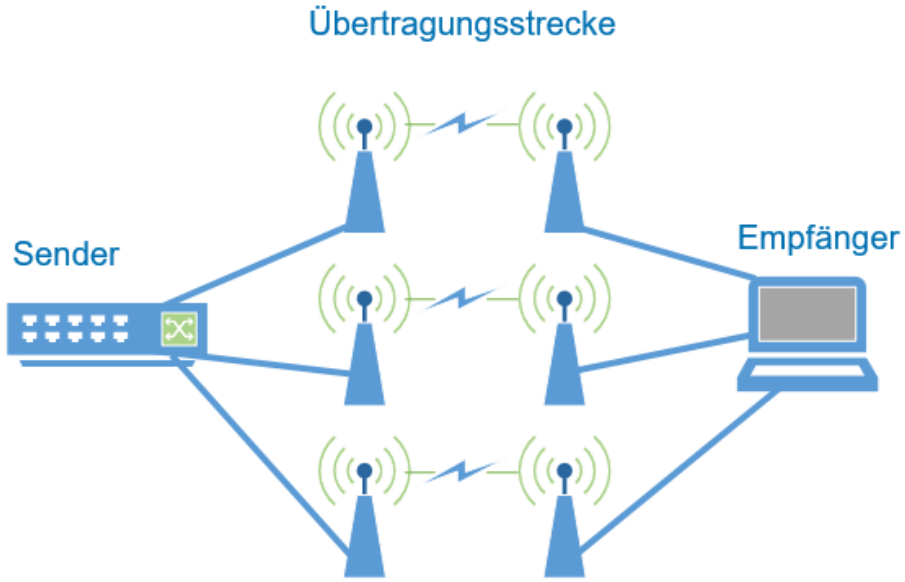

Abbildung 4: WLAN_Spatial_Streams (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Datenraten in der Praxis

- Schaut man sich die Angaben der Hersteller und Händler zur Bruttodatenrate ihrer Produkte an und vergleicht die Werte, die man damit in der Praxis erreicht, so stellt man fest, dass die Praxiswerte deutlich unter den Herstellerangaben liegen.
- Tatsache ist, dass die Bruttodatenraten, wie sie auf den Produktverpackungen und vom Standard angegeben sind, praktisch nie erreicht werden.
- In der Praxis haben hier viele Faktoren, z.B. örtliche Gegebenheiten, Entfernung und Antennen-Design einen maßgeblichen Einfluss.

WLAN (Wireless Local Area Network)

Störquellen

„aktive Störer“

- Sind eine häufige Störquelle, gemeint damit sind alle Geräte, die aus eigener Kraft Funkwellen erzeugen und abgeben. Das sind nicht nur andere WLAN-Sender.
- Zu diesen zählen auch (meist ältere) DECT-Telefone, Mikrowellengeräte, diverse Bluetooth-Geräte oder auch kabellose Überwachungskameras.
- Als Störquelle kommt auch die Stromversorgung in Betracht. Die WLAN-Geräte beziehen ihre Energie meist aus Steckernetzteilen. Je nach Qualität der Netzteile können Störungen aus dem Stromnetz durch das Netzteil bis in das WLAN-Gerät gelangen, besonders minderwertige Netzteile erzeugen u.U. selbst Störfrequenzen.

WLAN (Wireless Local Area Network)

Störquellen

Entfernung oder bauliche Begebenheiten

- Je weiter der Client vom Accesspoint entfernt ist, desto langsamer wird die Übertragung. Die tatsächliche Reichweite eines WLANs und der Bereich, in dem die Clients die maximale Übertragungsgeschwindigkeit erzielen, wird u.a. beeinflusst von:
  - Wände, geschlossenen Türen, Schränke und Glasflächen
  - Massive Möbel
  - Wände und Decken aus Stahlbeton
  - u.U. sogar ein größeres Aquarium
  - Heizungsanlagen, Rohrleitungen, Stromleitungen, sonstiges Metall

WLAN (Wireless Local Area Network)

Störquellen

Funkkanäle

- Damit sich in dicht bewohnten Gegenden die Funknetzwerke der einzelnen Parteien nicht gegenseitig blockieren, existieren im populären 2,4-Gigahertz-Frequenzband 13 Kanäle.
- Allerdings sind viele Router im Auslieferungszustand standardmäßig auf Kanal 1 eingestellt. Das sollte bei Bedarf geändert werden.
- Hinweis:
  - Bei einem geringen WLAN-Datendurchsatz kann versuchshalber auf einen anderen Kanal ausgewichen werden. Empfehlenswert ist ein Abstand von mindestens fünf Kanälen.
  - Manche Router bieten auch die Möglichkeit, bei Bedarf den Kanal automatisch zu wechseln.

WLAN (Wireless Local Area Network)

Repeater

WLAN – Repeater

- Der Repeater muss nicht vom selben Hersteller wie der WLAN-Router stammen.
- Wichtig: Nur Modelle mit Dual-Band-Modus oder Crossband-Repeating unterstützen gleichzeitig das 2,4- und das 5-GHz-Band.
- Zu bedenken ist allerdings, dass Repeater den Datendurchsatz halbieren, da sie das Signal von Access Point empfangen und das gleiche, aufgefrischte Signal wieder abstrahlen (Wiederholer nicht Verstärker!).

Abbildung 5: WLAN_Repeater (Quelle Amazon)

WLAN (Wireless Local Area Network)

Repeater

- Um Funklöcher in größeren Wohnungen zu vermeiden, lassen sich mehrere Repeater einsetzen.
- Die einzelnen Repeater müssen dabei so eingerichtet werden, dass sie jeweils das Signal des WLAN-Routers verstärken und nicht das eines anderen Repeaters.
- Der Repeater würde sonst die ohnehin schon halbierte WLAN-Geschwindigkeit weiter reduzieren.

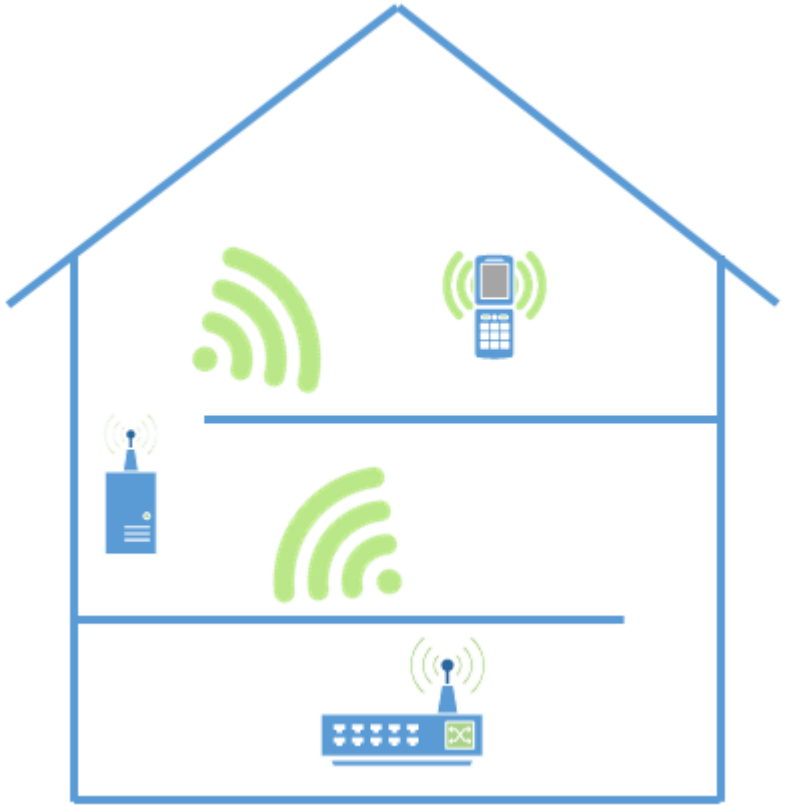

Abbildung 6: Repeater_Standort (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Mesh-WLAN

Mesh WLAN

- IEEE 802.11s ist der Standard für ein Wireless Mesh Network (WMN), in dem WLAN-fähige Geräte für andere Geräte als „Relaisstationen“ bis zum nächstgelegenen Access Point dienen.
- WLAN-Stationen bauen untereinander ein drahtlosen Backbone auf und leiten Frames an die Stationen, außerhalb der Reichweite des Access Points, weiter. Auf diese Weise wird die Flächenabdeckung der Funkzelle vergrößert.
- Theoretisch kann ein Mesh-WLAN eine beliebig große Funkzelle erzeugen. Dazu ist nur ein einziger Access Point nötig, der eine Verbindung ins Internet haben muss.
- Für eine volle Signalstärke und ein zuverlässig schnelles Netz im ganzen Haus kommen in letzter Zeit WLAN-Router mit Mesh-Technik auf den Markt.
- Sinnvoll ist ihr Einsatz zur Abdeckung größerer Flächen oder mehrerer Etagen.

WLAN (Wireless Local Area Network)

Mesh-WLAN

- Funktionsweise
  - Die Mesh-Router bauen im Verbund mit zwei, drei oder weiteren Geräten ein flächendeckendes Netzwerk unter Beibehaltung der WLAN-Geschwindigkeit auf.
  - Alle Geräte kommunizieren miteinander, erzeugen jeweils ein eigenes WLAN-Signal und tauschen direkt Daten miteinander aus. Sie sind somit nicht einfach Signalverstärker.
  - Das gesamte Mesh-Netzwerk läuft unter der gleichen (SSID).

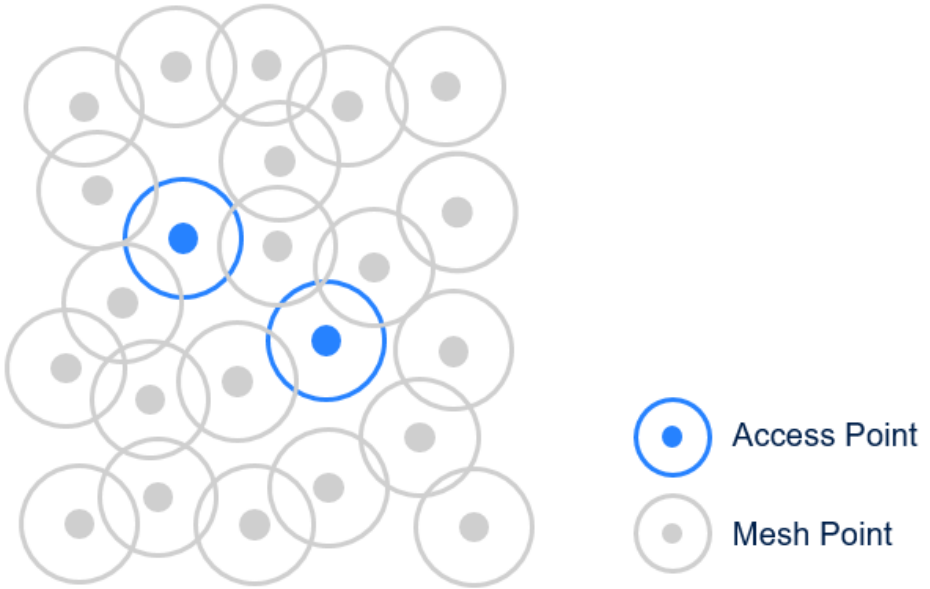

Abbildung 7:WLAN_Mesh (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Mesh-WLAN

- Hinweis
  - In der Praxis ist es aber so, dass auf dem Markt befindliche Mesh-Router die angestrebte Maschen-Struktur nur mit ausgewählter Hardware aus dem eigenen Haus realisieren.
  - Firmen wie AVM, Google und Netgear bieten z.Zt. eigene „Mesh“-Systeme an. Allen gemeinsam ist, dass die sogenannten „Mesh-Points“ zur Vergrößerung der Reichweite speziell zum Router passen müssen und aus der eigenen Produktion stammen. Mit Mesh nach IEEE 802.11s hat das nicht viel gemeinsam.
  - Gängige WLAN-Geräte wie Notebooks und Tablets sind aktuell nicht in der Lage, als Mesh-Point zu arbeiten.

WLAN - Sicherheit

WLAN (Wireless Local Area Network)

Sicherheit

Verbergen der WLAN-SSID

- Das Verstecken des WLAN-Namens in der Form "Hidden SSID aktivieren" oder "Broadcast SSID deaktivieren" ist scheinbar eine Maßnahme, um die Sicherheit eines WLANs zu erhöhen.
- Der Angreifer benötigt nicht nur das WLAN-Passwort, sondern auch den WLAN-Namen, um sich an einem WLAN authentifizieren zu können. Eine "Hidden SSID" ist mit recht einfachen Mitteln auszulesen und nicht standardkonform.
- Nachteilig ist für den Anwender, dass er beim ersten Verbinden mit dem versteckten WLAN die Verbindung manuell anlegen muß. Einige Geräte haben Probleme sich automatisch mit dem verborgenen WLAN zu verbinden.

WLAN (Wireless Local Area Network)

Sicherheit

MAC-Adress-Filter

- Ein MAC-Filter verhindert grundsätzlich, dass sich jemand mit einem WLAN verbinden kann, wenn die Hardware-Adresse des WLAN-Adapters nicht vorher im Wireless Access Point registriert wurde.
- Der Access Point wird dann den Verbindungsversuch ablehnen auch dann, wenn der betreffende Client das richtige WLAN-Passwort hat.
- Das Fälschen der übermittelten MAC-Adresse eines WLAN-Adapters ist verhältnismäßig simpel. Von daher erhöht ein MAC-Filter die Sicherheit nicht wirklich.

WLAN (Wireless Local Area Network)

Sicherheit

WEP - Wired Equivalent Privacy

- WEP ist ein veralteter Standard aus dem Jahr 1999 zur Authentifizierung und Verschlüsselung von WLANs, die dem Standard IEEE 802.11 entsprechen. WEP stellte Funktionen für die Authentifizierung, Verschlüsselung und Integritätsprüfung zur Verfügung.
- WEP enthält grundlegende Design-Schwächen und gilt seit 2001 als unsicher. Es ist mit relativ einfachen Mitteln möglich, in ein WEP-gesichertes WLAN einzudringen.
- Hinweis: WEP ist veraltet und sollte nicht mehr verwendet werden. Seit 2013 dürfen neue Access Points kein WEP mehr anbieten. Ab 2014 dürfen WLAN-Geräte, wie zum Beispiel Notebooks und WLAN-Sticks, kein WEP mehr unterstützen.

WLAN (Wireless Local Area Network)

Sicherheit

WPA - WiFi Protected Access

- WPA basierte ursprünglich auf WEP-Hardware, damit ein einfaches Software-Update einen Wireless Access Point von WEP auf WPA aktualisiert werden konnte.
- WPA verwendet für die Verschlüsselung TKIP (Temporal Key Integrity Protocol). TKIP bietet eine verbesserte Schlüsselberechnung (Fast Packet Keying, FPK). Im Vergleich zu WEP ist WPA nur wenig sicherer.
- Aus diesem Grund wurde WPA nur übergangsweise eingesetzt, heute wird durchgängig WPA2 empfohlen.

WLAN (Wireless Local Area Network)

Sicherheit

WPA2 (WiFi Protected Access 2) bzw. IEEE 802.11i

- ist ein Standard aus dem Jahr 2004 für die Authentifizierung und Verschlüsselung von WLANs, die auf IEEE 802.11 basieren und sollte die groben Sicherheitsmängel von WEP beseitigen.
- Nach der Verabschiedung von IEEE 802.11i erweiterte die Herstellervereinigung Wi-Fi Alliance den vorausgegangenen Standard WPA um eine zweite Version.
- Damit basiert WPA2 auf dem Standard IEEE 802.11i. Zu beachten ist, dass WPA2 mit IEEE 802.11i nicht identisch ist. WPA2 enthält nur einen Teil der IEEE 802.11i-Features.
- Der wesentliche Unterschied zwischen WPA und WPA2 ist die Verschlüsselungsmethode. Während WPA das weniger sichere TKIP verwendet, kommt in WPA2 das sichere AES zum Einsatz.

WLAN (Wireless Local Area Network)

Sicherheit

WPA2 Authentifizierungsverfahren

- WPA2 Enterprise
  - Verwendet einen RADIUS-Server (Remote Authentication Dial-In User Service) und ermöglicht so eine zentrale Benutzerverwaltung. Benutzer haben persönliche Zugangsdaten.
  - Die Authentifizierung erfolgt über Extensible Authentication Protocol (EAP).
- WPA Personal
  - Authentifizierung mit einem gemeinsamen Pre-Shared-Key.

WLAN (Wireless Local Area Network)

Sicherheit

IEEE 802.1x / RADIUS

- Bestandteile des Authentifizierungsverfahrens sind:
  - Supplicant (Antragsteller)
  - der Authenticator (Beglaubigter)
  - Authentication Server (Bestätigung)
- Der Authenticator schaltet den Zugang zum Netzwerk für den Supplicant frei oder verweigert ihn.

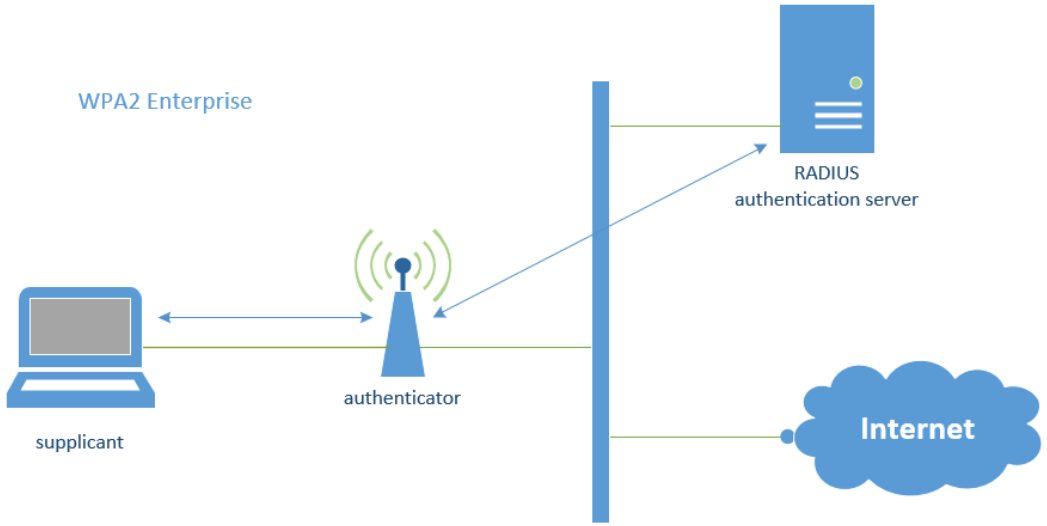

Abbildung 9: WLAN+RADIUS (Eigene Darstellung)

WLAN (Wireless Local Area Network)

Sicherheit

WPA3 (WiFi Protected Access 3)

- WPA3 enthält neue Funktionen, um die Authentifizierung zu vereinfachen und die Sicherheit der Authentifizierung und Verschlüsselung zu erhöhen.
  - robustere Authentifizierung und verbesserte Kryptografie
  - einfache Konfiguration für Geräte, die keine Bedienelemente haben
  - individuelle Verschlüsselung für jedes Gerät
  - Interoperabilität mit WPA2-Geräten
- Verwendet ebenfalls den Personal und den Enterprise Mode.
- WPA3 per Firmware- oder Treiber-Update in WLAN-Clients und Access Points einziehen.
- WPA3-Geräte müssen auf WPA2 zurückfallen können (WPA3-SAE Transition Mode).

WLAN (Wireless Local Area Network)

Sicherheit

WPS - Wi-Fi Protected Setup

- WPS ist eine Spezifikation der WiFi Alliance (WFA), hinter der sich eine Konfigurationsautomatik für den einfachen Aufbau eines WLANs mit Verschlüsselung verbirgt.
- Das Ziel von WPS war es, das Hinzufügen von Geräten in ein bestehendes Netzwerk zu vereinfachen. Die Hauptschwierigkeit bei der Konfiguration eines WLAN-Clients ist die Eingabe des WLAN-Passworts (Pre-Shared-Key), welches im Access Point hinterlegt ist.
- WPS vereinfacht und automatisiert diesen Vorgang. Die Konfiguration erfolgt entweder per Knopfdruck (WPS-PBC) oder Pin-Eingabe (WPS-PIN).
- WPS sollte nicht mehr verwendet werden, da es als unsicher angesehen wird.

WLAN (Wireless Local Area Network)

Sicherheit

Sicherheitsregeln für ein sicheres Funknetz:

- Bei neuen WLAN-Routern voreingestelltes Passwort ändern
- SSID ändern, Verschlüsselung auf WPA2 einstellen
- Sicheres Passwort verwenden
- WPS deaktivieren
- Ggf. Fernwartung deaktivieren
- Wenn Fremde das WLAN nutzen sollen, Gastzugang aktivieren und konfigurieren
- Regelmäßig Firmware auf Aktualität prüfen

Quellen

Buchquelle

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

VIELEN DANK!