Glossar
Wireless-LAN

Mit diesem Dokument finden Sie eine Sammlung an Erklärungen von Fachbegriffen und Abkürzungen zum Thema Wireless-LAN.

802.11
Hierbei handelt es sich um den IEEE (Haupt-)Standard für drahtlose lokale Netzwerke, so genannte Wireless Local Area Networks (WLANs).
IEEE 802.11 wurde 1997 verabschiedet und spezifizierte WLANs mit (Brutto-)Übertragungsraten von 2 Mbit/s.
Genutztes Frequenzband: 2,400 bis 2,485 GHz

802.11a
Nachfolger des ursprünglichen 802.11 Standards, der im Jahr 1999 verabschiedet wurde.
- (Brutto-)Datentransfer: 54 MBit/s
- Frequenzband: 5 GHz

802.11b
Weiterer Nachfolger des ursprünglichen 802.11 Standards von 1999.
- (Brutto-)Datentransfer: 11 MBit/s
- Frequenzband: 2,400 bis 2,4835 GHz

802.11g
Standard-Nachfolger aus dem Jahr 2003.
- (Brutto-)Datentransfer: 54 MBit/s
- Frequenzband: 2,400 bis 2,4835 GHz

802.11n
Zuletzt verabschiedeter Standard aus dem Jahr 2009.
- (Brutto-)Datentransfer: 600 MBit/s
- Frequenzband: 2,400 bis 2,4835 GHz , optional auch 5 GHz als zusätzliches Band

802.11ac
Geplanter Nachfolger des 802.11n-Standards.
- (Brutto-)Datentransfer: 1 GBit/s
- Frequenzband: < 6 GHz (geplant)

Access Point (AP)
Bei einem Access Point handelt es sich um ein Erweiterungsgerät für Funknetzwerke, der im Wesentlichen dazu dient das Funknetzwerk mit einem drahtgebundenen (Ethernet-)Netzwerk zu verbinden. Der Access Point dient hierbei als Brücke zwischen den Netzwerken und regelt deren Kommunikation untereinander.
Heutzutage werden Access Points (in der Regel) mit integrierter Firewall, Router und DSL-Modem ausgeliefert.

Ad-hoc (Netzwerk)
Ein Ad-hoc Netzwerk beschreibt die direkte Verbindung zweier Systeme über ein (privates) WLAN-Netz.
Hier werden in der Regel zwei Systeme über WLAN miteinander verbunden um die direkte Kommunikation zwischen den Teilnehmern zu ermöglichen. Diese Verbindungsvariante benötigt keine zusätzliche Hardware (z.B. Access Point) und hat nur eine sehr begrenzte Reichweite.

Bandbreite

Die Bandbreite beschreibt den Frequenzbereich (in MHz)i in dem Funksignale senden können.
Oft wird der Begriff („Bandbreite") fälschlicherweise für die Angabe der Übertragungsrate oder der „Geschwindigkeit" verwendet.

Datenrate

Beschreibt die „Geschwindigkeit" der Verbindung in der Anzahl binärer Daten (Bits), die pro Sekunde übertragen werden können (Einheit: Bit/s).
Die Datenrate wird oft auch als (Bit-)Übertragungsrate bezeichnet.
In Funkzellen/Drahtlosumgebungen hängt die Datenrate von mehreren Faktoren ab:

- Anzahl der Stationen (z.B. Verkettung mehrerer Access Points, Switches, etc.)
- Entfernung zum Access Point
- Qualität der Verbindung und Störeinflüsse (z.B. andere WLAN-Netzwerke oder –Geräte; Signal durch Wände/Stockwerke)
- Qualität der verwendeten Hardware (z.B. veraltete WLAN-Karten beim Client, Antenne/n)

Infrastruktur-Modus

Betriebsart von IEEE 802.11 WLANs bei dem ein Access Point (AP) erforderlich ist. Der Access Point stellt das WLAN unter vordefiniertem Namen („SSID") bereit, auf den sich verschiedene Clients verbinden können.
In dieser Betriebsart wird ein WLAN dann oft mit einem drahtgebundenen LAN über den Access Point verbunden.

Local Area Network

Ein auf ein Gebäude bzw. Gelände beschränktes Netzwerk (Ausdehnung ca. 2-5 km). Bekannte LAN Technologien sind bspw. Ethernet, Token Ring, aber auch WLANs.
LAN bzw. Ethernet ist u.a. die Schnittstelle zur Verbindung von Computern oder Netzwerken mit einem Router oder DSL-Modem.
Moderne Geräte wie Drucker oder Kopierer sind heute ebenfalls mit einer LAN-Schnittstelle ausgestattet und ermöglichen den direkten Zugriff auf bzw. über das Netzwerk.

MAC-Adresse

Die MAC-Adresse ist eine eindeutige, unverwechselbare Adresse aller Ethernet-Adapterkarten.
Jedes System mit einer Netzwerkkarte oder Geräte, die an einem Netzwerk angeschlossen sind, haben eine solche Adresse.
Eine MAC-Adresse besteht aus 6 Byte und wird hexadezimal geschrieben. Die ersten 3 Bytes kennzeichnen einen Hersteller und werden als ID gedeutet (z.B. 00-01-E3 für Siemens), die zweiten 3 Byte sind eine vom Hersteller vergebene eindeutige Nummer.
Die MAC-Adresse kann z.B. verwendet werden um die Zugangskontrolle der berechtigten User an einem Access Point zu steuern, indem man nur Bekannten MAC-Adressen den Zugang gewährt.

Remote Authentication Dial-In User Service (RADIUS)

Verfahren zur Authentifizierung von Nutzern anhand von Benutzernamen und Passwort über spezielle Server.
Um Zugang über einen RADIUS-Server zu erlangen muss der Client über einen entsprechenden Zugang inklusive gültigem Zertifikat verfügen.
Benutzer ohne Kennung oder Zertifikat werden vom RADIUS-Server ablehnt.

Roaming

Roaming ist die Definition des Vorgangs, bei dem eine mobile Station (z.B. Notebook) eines Netzwerkes ohne Unterbrechung der Mobilkommunikation zwischen mehreren Funkzellen wechseln kann.
Dies kommt z.B. vor, wenn sich mehrere Access Points mit gleicher SSID in einem WLAN-Netz befinden.
Wechselt man nun zwischen zwei Access Points, so sorgt das Roaming dafür, dass der Übergang für den Nutzer ohne Datenverlust abläuft.
Im GPRS/UMTS- Netz („Handy-Netz") spielt Roaming ebenfalls eine große Rolle.

Router

Ein Router ist ein Netzwerk-Gerät/-Element, das verschiedene Netzwerke verbindet bzw. koppelt.
Dabei analysiert der Router die ankommenden Datenpakete nach ihrer Zieladresse und leitet diese gezielt weiter, oder blockt diese gegebenenfalls.

Signal Strength
Stärke eines Signals (ausgedrückt in dbm).

Switch
Koppelelement in lokalen Netzwerken (LAN), der mehrere Ethernet-Geräte miteinander verbindet. Ein Switch baut selbständig eine MAC-Adressen-Tabelle anhand der Datenpakete auf, die von ihm weitergeleitet werden sollen und merkt sich dabei die Absender-Adresse und den zugehörigen Empfangsport.

Service Set Identifier (SSID)
Name einer Funkzelle, bzw. Name eines „WLAN-Netzwerks".
Die SSID wird normalerweise im Access Point konfiguriert und von diesem versendet.
Anhand der SSID kann man mehrere WLAN-Netze voneinander unterscheiden bzw. eindeutig zuordnen.

Temporal Key Integrity Protocol (TKIP)
TKIP ist ein Verschlüsselungsprotokoll und Teil des IEEE 802.11 Standards für WLANs. TKIP wurde entwickelt um eine höhere Sicherheit beim Verschlüsseln zu erlangen als beim „schwachen" Vorgänger WEP (Wired Equivalent Privacy).
TKIP ist die Verschlüsselungsmethode bei WPA (Wi-Fi Protected Access), welcher als Nachfolger/Ablöse von WEP gilt.

Wi-fi Protected Access (WPA)
Aufgrund der Schwachstellen von WEP wurde WPA als Zwischenlösung für Verschlüsslungen in WLANs entwickelt. WPA "erweiterte" WEP um eine dynamische Verschlüsselung (TKIP) und Port-basierte Benutzer-Authentifizierung. WPA gibt es mittlerweile in einer zweiten Generation (WPA2).

Wi-fi (Wireless Fidelity)
Die so genannte „Wi-Fi Alliance" ist eine Organisation aus über 300 Unternehmen, die Produkte verschiedener Hersteller auf der Basis des IEEE-802.11-Standards zertifiziert und so den Betrieb mit verschiedenen Wireless-Geräten (untereinander kompatibel) gewährleistet.
Hintergrund hierfür war, dass in vielen Produkten der 802.11-Standard nicht vollständig implementiert oder aber modifiziert/erweitert wurde. Dadurch ergaben sich häufig Inkompatibilitäten zwischen Produkten verschiedener Hersteller.
Die Wi-Fi-Alliance testet entsprechende Komponenten nach eigenen Richtlinien. Produkte, die die Prüfung bestehen, erhalten das Wi-Fi-Zertifikat und dürfen damit das Wi-Fi-Logo tragen. Dies führt dazu, dass beispielsweise ein „Wi-Fi" zertifiziertes Notebook mit jedem „Wi-Fi" zertifizierten Access Point kommunizieren können sollte. Ausnahmen und Restriktionen bei evtl. angepassten Einstellungen müssen allerdings berücksichtigt werden.

Wired Equivalent Privacy (WEP)
WEP ist ein Verschlüsselungsprotokoll das mit der Verabschiedung des ersten Standards IEEE 802.11 im Jahre 1997 spezifiziert wurde.
WEP sorgt zwar für eine Verschlüsselung und auch eine Benutzer-Authentifizierung, allerdings wird auf beiden Endpunkten (z.B. 2 Clients die miteinander kommunizieren) ein statischer Schlüssel eingetragen, was die Schwäche von WEP darstellt.
Die Verschlüsselung mit WEP gilt heutzutage als unsicher und überholt und sollte daher durch WPA/WPA2-Verschlüsselung ersetzt werden.

Wireless Local Area Network (WLAN)
Ein lokales Netzwerk bedeutet ein (örtlich,) auf ein Gebäude oder Gelände begrenztes Netzwerk. "Wireless" bedeutet dabei, wie der Name schon sagt, dass bei solchen lokalen Netzwerken keine Kabel verwendet werden. Statt elektrische oder optische Signale über geeignete Kabel zu übertragen, verwenden WLANs Funksignale und Luft als Medium zwischen Sender und Empfänger.
Hierfür wird jedoch eigene/zusätzliche Hardware benötigt (WLAN-Karten, Access Points, etc.). WLANs können mit entsprechender Hardware auch an lokale Ethernet-LANs gekoppelt werden.

WPA-PSK
Wi-fi Protected Access - Pre-Shared Key. Authentifizierungsvariante für WPA. Der „Pre-Shared Key" (oder „Kennwort") wird sowohl im Access Point als auch im Client gesetzt um eine Kommunikation zwischen beiden Punkten zu ermöglichen. Der Schlüssel besteht aus 6 bis 63 Zeichen und muss vorher bekannt und eingetragen sein um eine Verbindung aufzubauen, daher „Pre-Shared Key".
WPA-PSK ist vor allem in privatem Gebrauch die gängigste Variante um ein WLAN nach außen abzusichern bzw. um unerwünschte Zugriffe zu unterbinden.