Glossar

Dieses Glossar enthält Definitionen der Fachausdrücke, die in diesem Handbuch verwendet werden.

802.11 (Standard)
802.11 bzw. IEEE 802.11 ist eine Funktechnik, die in drahtlosen LANs (Wireless Local Area Networks, WLANs) eingesetzt wird. Es handelt sich dabei um einen Standard, der vom IEEE (Institute of Electrical and Electronic Engineers, *http://standards.ieee.org*) entwickelt wurde. Das IEEE ist eine internationale Organisation, die Standards für Hunderte von elektronischen und elektrischen Geräten entwickelt. Die Organisation verwendet zur Unterscheidung der unterschiedlichen Technologiefamilien Zahlen (ähnlich wie die Dewey-Dezimalklassifikation in Bibliotheken).
Die Untergruppe 802 (der IEEE) entwickelt Standards für LANs und WANs. Die Abteilung 802.11 ist dabei für die Überprüfung und Entwicklung von Standards für drahtlose LANs (WLANs) zuständig.
WiFi, 802.11, setzt sich aus mehreren Standards zusammen, die für unterschiedliche Frequenzen gelten: 802.11b ist der Standard für WLANs im 2,4-GHz-Spektrum mit einer Bandbreite von 11 MBit/s; 802.11a ist ein anderer WLAN-Standard und gehört zu Systemen, die im Frequenzbereich 5 GHz mit einer Bandbreite von 54 MBit/s arbeiten. Der Standard 802.11g gilt für WLANs, die im Frequenzbereich 2,4 GHz mit einer Bandbreite von 54 MBit/s arbeiten.

802.11a (Standard)
Ein IEEE-Standard für drahtlose Netzwerke im Frequenzbereich 5 GHz (5,15 GHz bis 5,85 GHz) mit einer maximalen Datenübertragungsrate von 54 MBit/s. Der 5-GHz-Frequenzbereich ist nicht so überfüllt wie der 2,4-GHz-Bereich, da der Standard 802.11a mehr Funkkanäle bietet als Standard 802.11b. Diese zusätzlichen Kanäle können helfen, Radio- und Mikrowellenstörungen zu vermeiden.

802.11b (Standard)
Ein internationaler Standard für drahtlose Netzwerke im Frequenzbereich 2,4 GHz (2,4 GHz bis 2,4835 GHz) mit einem Datendurchsatz von bis zu 11 MBit/s. Dieser Frequenzbereich wird sehr stark genutzt. Mikrowellengeräte, schnurlose Telefone, medizinische und wissenschaftliche Geräte sowie Bluetooth-Geräte verwenden allesamt das 2,4-GHz-Frequenzband.

802.11d (Standard)
802.11d ist eine Ergänzung des IEEE-Standards 802.11 zur MAC-Schicht (Media Access Control), die die weltweite Nutzung von 802.11-WLANs fördern soll. Dabei wird Access Points die Übermittlung von Daten über die zulässigen Funkkanäle mit akzeptabler Leistungsstärke für die Client-Geräte ermöglicht. Die Geräte werden dabei automatisch an die geografischen Anforderungen angepasst.
Der Standard 802.11d soll Funktionen und Einschränkungen festlegen, die den Betrieb von WLANs in den entsprechenden Ländern ermöglichen. Gerätehersteller möchten keine Vielzahl landesspezifischer Produkte herstellen und Benutzer, die viel reisen, möchten nicht für jedes Land eine eigene WLAN-PC-Card anschaffen. Dies wird langfristig zu landesspezifischen Firmware-Lösungen führen.

802.11e (Standard)
802.11e ist ein geplanter IEEE-Standard zur Definition von QoS-Mechanismen (Quality of Service) für drahtlose Geräte, der bandbreitenempfindliche Anwendungen wie Telefon und Video unterstützt.

802.11g (Standard)
Dieser Standard zur Erweiterung der Bitübertragungsschicht ist 802.11b sehr ähnlich, erlaubt jedoch einen Datendurchsatz von bis zu 54 MBit/s. Dieser Standard verwendet das 2,4-GHz-Frequenzband, setzt jedoch eine andere Funktechnik ein, um die Gesamtbandbreite zu vergrößern.

802.11i
Dieser Name bezeichnet die IEEE-Arbeitsgruppe, die sich mit der Standardisierung der WLAN-Sicherheit befasst. Das Sicherheitsrahmenwerk von 802.11i basiert auf RSN (Robust Security Network). RSN setzt sich aus zwei Teilen zusammen: 1.) einem Datensicherheitsmechanismus und 2.) der Verwaltung der Sicherheitsbeziehungen (Security Association Management).
Der Datensicherheitsmechanismus unterstützt zwei geplante Verschlüsselungsmethoden: TKIP and AES. TKIP (Temporal Key Integrity Protocol) ist eine Übergangslösung, die Software-Patches für WEP definiert, damit ein Mindestmaß an Datensicherheit gewährleistet ist. AES oder AES-OCB (Advanced Encryption Standard & Offset Codebook) ist ein leistungsstarkes Datensicherheitsschema, das als langfristige Lösung gedacht ist.
Die Verwaltung der Sicherheitsbeziehungen wird über drei Verfahren geregelt: a.) RSN-Abstimmungsverfahren, b.) IEEE-802.1x-Authentifizierung und c.) IEEE-802.1x-Schlüsselverwaltung.
Die Standards wurden so definiert, dass sie eine Koexistenz mit derzeit implementierten Netzwerken, die noch aus der Zeit vor RSN stammen, ermöglichen.

802.11n (Standard)
Eine im Oktober 2003 gebildete Arbeitsgruppe der IEEE, die als „802.11n“ oder „TGn“ bezeichnet wird. Sie ist zuständig für das 100 MBit/s-Standardprotokoll in der Bitübertragungsschicht. Als Veröffentlichungstermin ist derzeit Dezember 2005 geplant. Im Februar 2004 war noch kein Entwurf verfügbar. Es wird jedoch erwartet, dass das Protokoll sowohl die 2,4- als auch die 5-GHz-Frequenz verwendet.

AES (Advanced Encryption Standard)
Ein 128-Bit-Block-Datenverschlüsselungsverfahren, das von den belgischen Kryptographieexperten Joan Daemen und Vincent Rijmen entwickelt wurde. Die Regierung der Vereinigten Staaten übernahm im Oktober 2000 diesen Algorithmus als Verschlüsselungsverfahren anstelle der bisher verwendeten DES-Verschlüsselung. AES operiert auf mehreren Netzwerkschichten zugleich. Das National Institute of Standards and Technology (NIST) des US-Handelsministeriums wählte den Algorithmus „Rijndael“ aus einer Gruppe von fünf in die nähere Auswahl genommenen Algorithmen, darunter auch ein Algorithmus namens „MARS“ von einem großen Entwicklungsteam bei IBM. AES wird WEP voraussichtlich 2006 als WLAN-Verschlüsselungsmethode ablösen.

Access Point (auch Zugangspunkt)
Ein WLAN-Sende-/Empfangsgerät (oft auch als „Basisstation“ bezeichnet), über das ein oder mehrere drahtlose Geräte an ein kabelgebundenes LAN angeschlossen werden können. Über eine Funkbrücke können Access Points auch miteinander kommunizieren.
Es gibt unterschiedliche Typen von Access Points (Basisstationen), die sowohl in drahtlosen als auch in kabelgebundenen Netzwerken eingesetzt werden. Dazu gehören Bridges, Hubs, Switches, Router und Gateways. Die Unterschiede zwischen diesen Geräten sind nicht immer klar definiert, da bestimmte Funktionen, die einem dieser Geräte zugeordnet werden, auch in andere Geräte integriert werden können. So kann z. B. ein Router Funktionen einer Bridge übernehmen oder ein Hub auch als Switch eingesetzt werden. Alle diese Geräte dienen jedoch dazu, Daten von einem Ort an einen anderen zu übertragen.

Eine Bridge verbindet Geräte, die dasselbe Protokoll verwenden. Über einen Router können Netzwerke verbunden werden, in denen unterschiedliche Protokolle zum Einsatz kommen. Der Router liest zudem die in den Paketen enthaltenen Adressen und leitet die Pakete an die entsprechende Computerstation weiter. Dabei arbeitet er mit den anderen Routern im Netzwerk zusammen, um den besten Pfad zum Versand der Pakete zu finden. Ein drahtloser Hub oder Access Point verfügt neben anderen zusätzlichen Funktionen über Roaming und bietet eine Netzwerkverbindung zu einer Vielzahl von Clients. Er vergibt jedoch keine Bandbreite. Ein Switch ist ein Hub mit besonderen Fähigkeiten: Er kann die Adresse auf einem Paket lesen und dieses an die entsprechende Computerstation weiterleiten. Bei einem Wireless Gateway handelt es sich um einen Access Point, der zusätzliche Funktionen, wie NAT-Routing, DHCP, Firewalls und Sicherheit, bereitstellt.

Ad-hoc-Modus
Eine Client-Einstellung, die unabhängige Peer-to-Peer-Verbindungen über ein WLAN ermöglicht. Eine andere Einsatzmöglichkeit ist die Kommunikation von PCs untereinander über einen Access Point. Siehe Access Point und Infrastruktur-Modus.

Bandbreite
Die Übertragungskapazität, die in einem Netzwerk zur Verfügung steht. Die verfügbare Bandbreite hängt von mehreren Variablen ab, darunter die Datenübertragungsrate zwischen Geräten im Netzwerk, der Netzwerk-Overhead, die Benutzeranzahl und der Typ des Geräts, über das PCs an das Netzwerk angeschlossen werden. Die Bandbreite lässt sich gewissermaßen mit einem Rohr vergleichen, da bei beiden die Größe die Kapazität bestimmt: Je breiter das Rohr ist, desto mehr Wasser kann hindurchfließen, und je mehr Bandbreite ein Netzwerk zur Verfügung stellt, desto mehr Daten können hindurchfließen. Der Standard 802.11b bietet eine Bandbreite von 11 MBit/s; 802.11a und 802.11g dagegen 54 MBit/s.

Bit pro Sekunde (Bit/s)
Maßeinheit für die Datenübertragungsgeschwindigkeit über Kommunikationsleitungen, basierend auf der Anzahl von Bit, die pro Sekunde versendet oder empfangen werden können. Bit pro Sekunde (Bit/s) werden oft mit Bytes pro Sekunde (Bytes/s) verwechselt. Während Bits zum Messen der Übertragungsgeschwindigkeit verwendet werden, dienen Bytes zur Angabe der Speicherkapazität. 8 Bits ergeben ein Byte. Wenn ein drahtloses Netzwerk also mit einer Bandbreite von 11 Megabits pro Sekunde (11 MBit/s) arbeitet, versendet es pro Sekunde 1,375 Megabytes (1,375 Mbytes/s).

Bluetooth-Funktechnik
Eine technische Spezifikation zum Verbinden von tragbaren Computern, PDAs und Mobiltelefonen für die drahtlose Übertragung von Telefongesprächen und Daten über kurze Entfernungen mit Hilfe eines globalen Funkfrequenzbands. Bluetooth ist ein Frequenzsprungverfahren im Frequenzspektrum 2,4 GHz mit einer Reichweite von bis zu zehn Metern und einem Datendurchsatz von bis zu 1 MBit/s.

Bridge
Ein Gerät zum Verbinden eines LANs (Local Area Network) mit einem anderen LAN, das dasselbe Protokoll verwendet (z. B. drahtlos, Ethernet oder Token Ring). Wireless Bridges werden sehr häufig eingesetzt, um die unterschiedlichen Gebäude auf einem Universitätscampus zu verbinden.

Clients oder Client-Geräte
Jeder Computer in einem Netzwerk, der Dienste (Dateien, Druckfunktionen) von einem anderen Mitglied des Netzwerks bezieht. Clients sind Endbenutzer. Zu den WiFi-Client-Geräten gehören PC Cards für Laptop-Computer, Mini-PCI-Module in Laptop-Computern und mobilen Geräten sowie USB- und PCI-/ISA-Bus-WiFi-Radios. Client-Geräte kommunizieren in der Regel mit Hub-Geräten wie Access Points und Gateways.

Kollisionsvermeidung (Collision Avoidance)
Ein Netzwerkknotenmerkmal für die proaktive Entdeckung, ob ein Signal gesendet werden kann, ohne dabei eine Kollision zu riskieren.

Crossover-Kabel
Ein spezielles Kabel, mit dem zwei Computer ohne einen Hub vernetzt werden können. Crossover-Kabel werden zudem manchmal benötigt, um ein Kabel- oder DSL-Modem mit einem Wireless Gateway oder Access Point zu verbinden. Die Signale werden nicht parallel von einem Stecker zum nächsten geführt, sondern „gekreuzt“. Wird zum Beispiel ein Kabel mit acht Leitungen verwendet, geht das Signal am einen Ende des Kabels über Pin 1 ein und kommt am anderen Ende auf Pin 8 an. Die Signale wechseln von einer Seite auf die andere.

CSMA/CA (Carrier Sense Multiple Action/Collision Avoidance)
CSMA/CA ist die Hauptmethode für den Zugriff auf Medien in IEEE-802.11-WLANs. Diese Methode folgt dem Prinzip „Erst zuhören, dann reden“ und verringert die Anzahl von Kollisionen, die durch gleichzeitigen Datenversand verursacht werden. Ganz verhindert werden diese Kollisionen dadurch allerdings nicht. IEEE 802.11 legt fest, dass die Kollisionsvermeidungsmethode (und nicht Kollisionserkennung (Collision Detection)) verwendet werden soll, da der Standard Halbduplexbetrieb zu Grunde legt – d. h. es kann nur entweder gesendet oder empfangen werden, aber nicht beides gleichzeitig.
Im Gegensatz zu konventionellen kabelgebundenen Hosts kann eine WLAN-Station eine Kollision während des Sendens nicht erkennen. Wenn es zu einer Kollision kommt, erhält die Sendestation kein ACK-Paket (ACKnowledge) von der Empfängerstation. Aus diesem Grund haben ACK-Pakete die höchste Priorität im Netzwerk. Nach Abschluss einer Datenübertragung beginnt die Empfangsstation mit dem Senden des ACK-Pakets, bevor ein anderer Knoten den Versand eines neuen Datenpakets einleiten kann. Alle anderen Stationen müssen eine längere pseudo-zufällige Zeitspanne warten, bevor sie senden können. Wenn die Sendestation kein ACK-Paket erhält, wartet sie die nächste Gelegenheit für einen erneuten Übertragungsversuch ab.

CSMA/CD (Carrier Sense Multiple Action/Collision Detection)
Eine Methode zum Verwalten des Datenverkehrs und Verringern von Rauschen in kabelgebundenen Netzwerken. Ein Netzwerkgerät überträgt Daten, nachdem es einen verfügbaren Kanal entdeckt hat. Wenn jedoch zwei Geräte gleichzeitig Daten senden, entdecken die sendenden Geräte eine Kollision und senden die Daten nach Ablauf eines zufälligen Zeitraums erneut.

DHCP (Dynamic Host Configuration Protocol)
Ein Dienstprogramm, das Servern das dynamische Zuweisen von IP-Adressen aus einer vordefinierten Liste ermöglicht. Die Server können zudem die Nutzungszeit der Adressen begrenzen, damit diese erneut vergeben werden können. Ohne DHCP müssten IT-Administratoren die IP-Adressen auf allen Computern im gesamten Netzwerk manuell eingeben. Unter Verwendung von DHCP wird jedem Computer bei der Anmeldung am Netzwerk automatisch eine IP-Adresse zugewiesen.

Diversity-Antennen
Ein Antennensystem, das zwei Antennen einsetzt, um Empfangs- und Übertragungsqualität zu optimieren und Störungen zu minimieren.

DNS (Domain Name Service)
Ein Programm, das mit Hilfe einer auf mehreren Internetservern gespeicherten Datenbank URLs in IP-Adressen umwandelt. Das Programm läuft im Hintergrund und erleichtert das Surfen im Internet, da so statt numerischer alphabetische Adressen eingesetzt werden können. Ein DNS-Server wandelt einen Namen wie „mywebsite.com“ in eine Zahlenfolge wie „107.22.55.26“ um. Jede Website im Internet hat ihre eigene spezifische IP-Adresse.

Verschlüsselungscode
Eine alphanumerische (aus Buchstaben und Ziffern bestehende) Zeichenfolge, die die Verschlüsselung und Entschlüsselung von Daten für einen sicheren Datenaustausch unter den Mitgliedern eines Netzwerks ermöglicht. WEP verwendet einen Verschlüsselungscode, der ausgehende Daten im drahtlosen Netzwerk automatisch verschlüsselt. Auf der Empfängerseite kann der Computer die Informationen mit Hilfe desselben Verschlüsselungscodes automatisch entschlüsseln.

Verbesserte Datenverschlüsselung mit TKIP
Zur Verbesserung der Datenverschlüsselung setzt WPA (Wi-Fi Protected Access) TKIP (Temporal Key Integrity Protocol) ein. TKIP bietet wichtige Verbesserungen zur Datenverschlüsselung, darunter eine Funktion zum paketweisen Ändern von Schlüsseln, die Nachrichtenintegritätsprüfung Michael (Message Integrity Check, MIC), einen erweiterten Initialisierungsvektor (IV) mit Sequenzierungsregeln und einen Mechanismus zur Neuverschlüsselung. Mit diesen Verbesserungen berücksichtigt TKIP alle bekannten Schwächen von WEP.

Unternehmensnetzwerke: Benutzerauthentifizierung über 802.1x/EAP und RADIUS
WEP verfügt über nahezu keine Mechanismen zur Benutzerauthentifizierung. Zur Stärkung der Benutzerauthentifizierung implementiert WPA (Wi-Fi Protected Access) 802.1x und EAP (Extensible Authentication Protocol). Zusammengenommen bilden diese Verbesserungen das Gerüst für eine leistungsfähige Benutzerauthentifizierung. Dieses Gerüst verwendet einen zentralen Authentifzierungsserver, z. B. einen RADIUS-Server, um jeden Benutzer vor der Anmeldung am Netzwerk zu authentifizieren. Eine gegenseitige Authentifizierung verhindert zudem, dass der Benutzer sich versehentlich bei einem Spionagenetzwerk anmeldet, das seine Anmeldedaten stiehlt.

ESSID (häufig auch als „SSID“ – Service Set Identifier – bezeichnet)
Die Kennung eines drahtlosen 802.11-Netzwerks. Durch Angabe der richtigen ESSID beim Einrichten des Clients melden Sie sich an Ihrem drahtlosen Netzwerk an (statt bei einem anderen Netzwerk in Reichweite). (Siehe SSID.) Andere Bezeichnungen für die ESSID sind Netzwerkname, bevorzugtes Netzwerk, SSID oder Wireless LAN Service Area.

Ethernet
Internationaler Standard (Übertragungsprotokoll) für kabelgebundene Netzwerke. Einfache 10BaseT-Netzwerke bieten eine Bandbreite von ca. 10 MBit/s. Fast Ethernet (100 MBit/s) und Gigabit Ethernet (1000 MBit/s) werden immer beliebter.

Firewall
Ein System, das Netzwerke schützt und den Zugriff durch Unbefugte verhindert. Firewalls sind in Form von Software, Hardware oder einer Kombination aus beiden erhältlich. Firewalls können den Zugang zu einem Netzwerk regulieren sowie den Datenfluss nach außen einschränken.

Gateway
Üblicherweise ein Gerät, das eine Verbindung zu einem anderen Netzwerk, z. B. dem Internet, herstellt. Gateways können zudem VPN-Unterstützung, Firewalls, unterschiedliche Sicherheitsstufen und Wireless Access Points mit weiteren Funktionen beinhalten.

Hot-Spot
Hot-Spots bieten Zugang zu WiFi-Diensten. Dies kann kostenlos oder gebührenpflichtig sein. Hot-Spots sind in Cafés, Flughäfen, Bahnhöfen, Kongresszentren, Hotels und an anderen öffentlichen Orten zu finden. Unternehmen und Hochschulen richten ebenfalls Hot-Spots ein, um Besuchern und Gästen die Möglichkeit zum drahtlosen Internetzugang zu bieten. In manchen Ländern werden Hot-Spots als „Coolspots“ bezeichnet.

Hub
Ein Gerät mit mehreren Ports, über das PCs per Netzwerkkabel oder WiFi an ein Netzwerk angeschlossen werden können. Kabelgebundene Hubs können zahlreiche Ports haben und die Übertragungsgeschwindigkeit kann von 10 MBit/s bis zu mehreren Gigabyte pro Sekunde reichen. Ein Hub sendet die Pakete, die er empfängt, an alle angeschlossenen Ports. An einen kleinen kabelgebundenen Hub können nur 4 Computer angeschlossenen werden, an einen großen Hub 48 und mehr. An drahtlose Hubs (Access Points) können sogar Hunderte von Computern angeschlossen werden.

Hz (Hertz)
Die SI-Einheit für die Frequenz gibt die Anzahl der Schwingungen pro Sekunde an. Ein Megahertz (MHz) entspricht einer Million Hertz, ein Gigahertz (GHz) einer Milliarde Hertz. In den USA ist die Standardstromfrequenz 60 Hz, das Frequenzband für MW-Funk ist 535–1605 kHz, das Frequenzband für UKW-Funk ist 88–108 MHz und 802.11b-WLANs arbeiten bei 2,4 GHz.

IEEE (Institute of Electrical and Electronics Engineers)
Ein Berufsverband, zu dessen Mitgliedern Ingenieure, Wissenschaftler und Studenten der Elektrotechnik und verwandter Fachgebiete gehören (Website: *www.ieee.org*). Das IEEE hat über 300.000 Mitglieder und spielt eine wichtige Rolle bei der Entwicklung von Standards für Computer und Kommunikationstechnik.

IEEE 802.11
Eine Normenfamilie für LANs, herausgegeben vom IEEE (Institute of Electrical and Electronics Engineers). Die meisten kabelgebundenen Netzwerke entsprechen 802.3, dem Standard für CSMA/CD-basierte Ethernetnetzwerke, oder 802.5, dem Standard für Token-Ring-Netzwerke. 802.11 legt den Standard für drahtlose LANs (WLANs) fest und umfasst drei nicht miteinander kompatible Verfahren: FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) und Infrarot. Die WECA (Wireless Ethernet Compatibility Alliance, inzwischen Wi-Fi Alliance) konzentriert sich auf 802.11b, einen DSSS-Standard für drahtlose Netzwerke mit einer Übertragungsrate von 11 MBit/s.

Infrastruktur-Modus
Eine Client-Einstellung, die Verbindungen zu einem Access Point möglich macht. Im Gegensatz zum Ad-hoc-Modus, in dem PCs direkt miteinander kommunizieren, gehen im Infrastruktur-Modus alle von den Clients versendeten und empfangenen Daten durch einen Access Point. Der Access Point ist nicht nur für den drahtlosen Netzwerkdatenverkehr in der unmittelbaren Umgebung zuständig, sondern sorgt auch für die Kommunikation mit dem kabelgebundenen Netzwerk. Siehe Ad-hoc-Modus und Access Point.

IP-Adresse (Internet Protocol Address)
Eine 32-Bit-Nummer, die den Sender oder Empfänger jeglicher über das Internet versendeter Daten kennzeichnet. IP-Adressen setzen sich aus zwei Teilen zusammen: Der eine verweist auf ein bestimmtes Netzwerk innerhalb des Internets, der andere verweist auf das jeweilige Gerät (das ein Server oder eine Workstation sein kann) innerhalb dieses Netzwerks.

ISO-OSI-Referenzmodell
Ein von der ISO (International Standards Organization) entwickeltes Netzwerkmodell, das aus sieben Stufen oder Schichten besteht. Durch die Standardisierung dieser Schichten und der Schnittstellen zwischen ihnen können unterschiedliche Elemente eines bestehenden Protokolls angepasst oder geändert werden, um dem technischen Fortschritt und veränderten Systemanforderungen gerecht zu werden. Die sieben Schichten werden wie folgt bezeichnet:

- Bitübertragungsschicht (auch physikalische Schicht, engl. Physical Layer)

- Sicherungsschicht (auch Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene, engl. Data Link Layer)
- Netzwerk
- Transportschicht (auch Ende-zu-Ende-Kontrolle, Transport-Kontrolle, engl. Transport Layer)
- Kommunikationsschicht (auch Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsschicht, engl. Session Layer)
- Darstellungsschicht (auch Datendarstellungsschicht, Datenbereitstellungsebene, engl. Presentation Layer)
- Anwendungsschicht (auch Anwenderebene, Verarbeitungsschicht, engl. Application Layer)

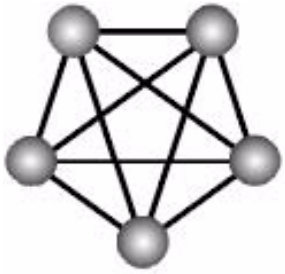
Der Standard IEEE 802.11 bezieht sich auf die Bitübertragungsschicht (physikalische Schicht, PHY) und den unteren Bereich der Sicherungsschicht. Der untere Bereich der Sicherungsschicht wird oft als MAC-Schicht (Media Access Control) bezeichnet.

MAC (Media Access Control)

Jedes drahtlose 802.11-Gerät hat seine eigene, unveränderbare MAC-Adresse. Diese eindeutige Kennzeichnung kann genutzt werden, um drahtlose Netzwerke sicherer zu machen. Wenn ein Netzwerk eine MAC-Tabelle einsetzt, erhalten nur diejenigen 802.11-Geräte, deren MAC-Adresse in der MAC-Tabelle dieses Netzwerks aufgelistet sind, Zugang zum Netzwerk.

Maschennetze

Maschennetze (oft auch als „Maschenstruktur“ bezeichnet) sind eine Netzwerktopologie, bei der Geräte über eine Vielzahl von Verbindungen zwischen den einzelnen Netzwerkknoten verbunden werden. In einer vollständigen Mesh Topologie ist jeder Knoten mit allen anderen Knoten im Netzwerk verbunden. Maschennetze können drahtlos oder kabelgebunden sein.



In der oben dargestellten Maschenstruktur entspricht jede Kugel einem Router. Server und Drucker können gemeinsam genutzt werden, indem sie mit jedem Router in der Masche verbunden werden. Für einen drahtlosen Zugang zum Maschennetz muss ein Access Point an einen der Router in diesem Netz angeschlossen werden.

MIMO (Multiple Input Multiple Output)

MIMO bezeichnet Funktechnologien, die zur Optimierung der drahtlosen Kommunikation mit mehreren Verbindungen zwischen Sender und Empfänger arbeiten. Hierzu werden mehrere Antennen benötigt.

NAT (Network Address Translation, Netzwerk-Adressumsetzung)

Eine Netzwerkfunktion, mit der mehrere Computer eine einzige Eingangs-IP-Adresse dynamisch zum gemeinsamen Zugriff auf das Internet über eine Einwähl-, Kabel- oder xDSL-Verbindung nutzen können. NAT verwendet die gemeinsame IP-Adresse und erstellt neue IP-Adressen für alle Client-Computer im Netzwerk.

Netzwerkname
Der Netzwerkname kennzeichnet das drahtlose Netzwerk für alle gemeinsam genutzten Geräte. Bei der Installation eines drahtlosen Netzwerks muss in der Regel ein Netzwerkname bzw. eine SSID eingegeben werden. Beim Einrichten eines einzelnen Computers, eines kabelgebundenen Netzwerks oder einer Arbeitsgruppe werden andere Netzwerknamen verwendet.

Netzwerkkarte (NIC, Network Interface Card)
Eine Steckkarte für PCs, die entweder drahtlos funktioniert oder über einen Anschluss für ein Netzwerkkabel verfügt. In beiden Fällen kann über die Karte eine bidirektionale Kommunikation zwischen dem Computer und Netzwerkgeräten wie einem Hub oder Switch hergestellt werden. Die meisten Netzwerkkarten in kabelgebundenen Büronetzwerken arbeiten mit 10 MBit/s (Ethernet), 100 MBit/s (Fast Ethernet) oder 10/100 MBit/s (Dual Speed). Daneben sind aber auch besonders schnelle Gigabit- und 10-Gigabit-Netzwerkkarten erhältlich. Oft werden Netzwerkkarten auch als Netzwerk-Adapter bezeichnet.

PC-Card
Oberbegriff für scheckkartengroße Erweiterungskarten in 16-Bit- (PCMCIA-) oder 32-Bit- (CardBus-) Technologie. PC-Cards werden vor allem in Notebooks eingesetzt. Zu den als PC-Cards erhältlichen Peripheriegeräten gehören u. a. WiFi-Karten, Speicherkarten, Modems, Netzwerkkarten und Festplatten.

PCI
PCI ist ein leistungsstarker E/A-Bus, mit dem die meisten Computer ausgestattet sind. Andere Bussysteme sind ISA und AGP. PCI und andere Busse ermöglichen den Einbau von internen Karten, die Dienste und Funktionen bieten, die von der Hauptplatine oder anderen Anschlüssen nicht unterstützt werden.

Peer-to-Peer-Netzwerk (bei WLANs auch Ad-hoc-Modus)
Ein kabelgebundenes oder drahtloses Computernetzwerk ohne Server, zentralen Hub oder Router. Alle vernetzten PCs können gleichrangig als Netzwerkserver oder Client agieren und jeder Client-Computer kann mit allen anderen drahtlosen Computern kommunizieren, ohne dabei über einen Access Point oder Hub gehen zu müssen. Da es keine zentrale Basisstation gibt, die den Datenverkehr überwacht oder den Internetzugang zur Verfügung stellt, kann es jedoch zu Kollisionen der einzelnen Signale und damit zu einer Beeinträchtigung der Leistung des Netzwerkes insgesamt kommen.

PHY (physikalische Schicht oder auch Bitübertragungsschicht)
Die unterste Schicht des ISO-OSI-Referenzmodells. Diese Schicht ist in erster Linie für die Übertragung der Bitströme über das PHYsikalische Übertragungsmedium zuständig. Bei drahtlosen Netzwerken ist das Übertragungsmedium der freie Raum. In der Bitübertragungsschicht werden Parameter wie Datenübertragungsrate, Modulationsmethode, Signalparameter, Sender-/Empfängersynchronisierung usw. festgelegt. In einer Funkimplementierung entspricht die Bitübertragungsschicht den Bereichen Funk-Front-End und Basisbandsignalverarbeitung.

Plug & Play
Eine Computersystemfunktion, die die automatische Konfiguration von Zusatz- und Peripheriegeräten wie PC-Cards, Druckern, Scannern und Multimediageräten ermöglicht.

Proxy-Server
Proxy-Server werden in größeren Unternehmen eingesetzt, um den Netzwerkbetrieb und die Sicherheit zu optimieren. Ein Proxy-Server kann die direkte Kommunikation zwischen zwei oder mehr Netzwerken verhindern. Der Proxy-Server leitet zulässige Datenanforderungen an entfernte Server weiter und/oder bearbeitet Datenanfragen direkt mit Hilfe von Daten auf entfernten Servern.

Reichweite
Die Entfernung, die ein drahtloses Netzwerk von einem Access Point aus abdecken kann. Die meisten WiFi-Systeme bieten eine Reichweite von 30 m oder mehr. Je nach Umgebung und der verwendeten Antenne können WiFi-Signale eine Reichweite von bis zu 1,6 km erreichen.

Residential Gateway (Heim-Gateway)
Ein drahtloses Gerät, über das in einem Heimnetzwerk mehrere PCs mit Peripheriegeräten und dem Internet verbunden werden können. Die meisten WiFi-Residential-Gateways bieten zudem auch DHCP und NAT.

RJ-45
Die Standardstecker in kabelgebundenen Netzwerken. RJ-45-Stecker sehen RJ-11-Telefonsteckern sehr ähnlich. RJ-45 können jedoch bis zu acht Leitungen haben, Telefonstecker haben dagegen nur vier.

Roaming
Der nahtlose Wechsel von der Funkzelle eines Access Points in die des nächsten mit einem Notebook oder Desktop-PC, ohne dass dabei die Verbindung unterbrochen wird.

Rogue Access Point
Als „Rogue Access Point“ bezeichnet man einen nicht autorisierten Access Point, der mit dem Heim- oder Unternehmensnetzwerk verbunden ist oder im Stand-Alone-Modus arbeitet (z. B. von einem Parkplatz oder benachbarten Gebäude aus). Rogue Access Points werden nicht von den Netzwerk-Administratoren verwaltet und erfüllen auch nicht die Sicherheitsrichtlinien des Netzwerks. Sie stellen ein beträchtliches Sicherheitsrisiko dar. Es ist zu empfehlen, ein WLAN-System einzusetzen, das das Hinzufügen von Rogue Access Points zu einem bestehenden WLAN so schwer wie möglich macht.

Router
Ein Gerät, das Datenpakete von einem LAN (Local Area Network) oder WAN (Wide Area Network) an ein anderes weiterleitet. Mit Hilfe von Routingtabellen und Routingprotokollen kann der Router die Netzwerkadresse jedes gesendeten Frames entziffern und entscheiden, welche die effizienteste Route für die Weiterleitung des Frames ist. Er berücksichtigt dabei u. a. die Auslastung, Leitungskosten, Geschwindigkeit und schlechte Verbindungen.

Satelliten-Breitband
Eine drahtlose Hochgeschwindigkeits-Internetverbindung über Satellit. Manche Satelliten-Breitbandverbindungen sind bidirektional (aufwärts und abwärts). Andere Verbindungen gehen nur in eine Richtung: Der Satellit bietet eine Hochgeschwindigkeitsverbindung für den Downstream (vom Internet zum Benutzer) an, für den Upstream (vom Benutzer zum Internet) wird dagegen eine Einwahlverbindung oder ein anderes terrestrisches System verwendet.

Server
Ein Computer, der seine Ressourcen für andere Computer und Geräte im Netzwerk verfügbar macht. Dazu gehören z. B. Printserver, Internet-Server und Datenserver. Ein Server kann auch mit einem Switch oder Router kombiniert werden.

Standortprüfung
Untersuchung eines Standorts vor der Installation eines drahtlosen Netzwerks. Bei einer Standortprüfung wird der Standort auf seine Funk- und Benutzereigenschaften hin untersucht, um eine optimale Positionierung der Access Points zu erreichen.

SSID (auch ESSID)
Eine eindeutige Kennzeichnung aus 32 Zeichen, die an den Header von über das WLAN versendeten Datenpaketen angehängt und als Passwort eingesetzt wird, wenn ein mobiles Gerät versucht, eine Verbindung zum BSS aufzubauen. (Siehe ESSID.) Die SSID dient dazu, ein WLAN von anderen zu unterscheiden. Deshalb müssen alle Access Points und sonstigen Geräte, die versuchen, eine Verbindung zu einem bestimmten WLAN aufzubauen, dieselbe SSID verwenden.
Geräten, die nicht über die eindeutige SSID verfügen, wird der Anschluss an das BSS verweigert. Da SSIDs jedoch den Paketen im Klartext zu entnehmen sind, bieten sie keinerlei Sicherheit für das Netzwerk. Die SSID wird auch als „Netzwerkname“ bezeichnet, da sie im Prinzip zur Kennzeichnung drahtloser Netzwerke dient.

SSL (Secure Sockets Layer)
Ein verbreitetes Verschlüsselungsprotokoll, das von vielen Online-Händlern und Online-Banking-Websites eingesetzt wird, um bei finanziellen Transaktionen Datensicherheit zu gewährleisten. Zu Beginn einer SSL-Sitzung sendet der Server seinen öffentlichen Schlüssel an den Browser. Der Browser sendet sodann einen nach dem Zufallsprinzip erstellten, geheimen Schlüssel zurück an den Server. Damit ist ein geheimer Schlüsselaustausch für diese Sitzung gewährleistet.

Subnetz
Diese kleineren Netzwerke werden in großen Netzwerken eingesetzt, um die Adressierung zwischen zahlreichen Computern zu erleichtern. Subnetze werden über einen Router, Switch oder ein Gateway mit dem zentralen Netzwerk verbunden. Ein WLAN verwendet in der Regel für alle lokalen Computer, mit denen es kommuniziert, dasselbe Subnetz.

Switch
Ein Hub-ähnlicher Netzwerkverteiler, der die Nutzung eines Netzwerkes durch unterschiedliche Geräte effizient steuert, damit alle Geräte optimale Leistung erbringen können. Switches übernehmen im Netzwerk die Rolle eines Datenverkehrspolizisten: Während ein Hub alle empfangenen Pakete an sämtliche Ports weiterleitet, sendet ein Switch die Pakete nur an den Port, für den sie bestimmt sind.

TCP (Transmission Control Protocol)
Ein Protokoll, das zusammen mit dem Internet Protocol (IP) verwendet wird, um Daten in Form von einzelnen Einheiten, den sog. Paketen, über das Internet zwischen Computern zu versenden. IP ist dabei für die Zustellung der Daten zuständig, TCP protokolliert die einzelnen Pakete, in die eine Nachricht für das effiziente Routing über das Internet zerlegt wird.
Wenn beispielsweise eine Webseite von einem Webserver heruntergeladen wird, teilt die TCP-Programmschicht auf diesem Server die Datei in Pakete, versieht sie mit einer Nummer und leitet sie dann einzeln an die

IP-Programmschicht weiter. Auch wenn alle Pakete dieselbe IP-Adresse als Ziel haben, können die einzelnen Pakete auf unterschiedlichen Wegen dorthin gelangen. Am anderen Ende fügt TCP die einzelnen Pakete wieder zusammen und wartet, bis alle angekommen sind, um sie dann als eine einzige Datei weiterzuleiten.

TCP/IP
TCP/IP ist das zugrunde liegende Protokoll, das die Kommunikation zwischen Computern im Internet und in einem Netzwerk ermöglicht. Der erste Teil, TCP, ist für die Übermittlung der Daten zuständig. TCP passt die Größe der Nachrichten an beiden Enden der Übertragung an und stellt sicher, dass die Nachricht richtig zugestellt wird. Der zweite Teil, IP, ist die Computeradresse eines Benutzers in einem Netzwerk. Jeder Computer in einem TCP/IP-Netzwerk hat eine eigene IP-Adresse, die ihm entweder dynamisch beim Systemstart oder aber permanent zugewiesen wird. Alle TCP/IP-Nachrichten enthalten die Adresse des Zielnetzwerks sowie die Adresse der Zielstation. So können TCP/IP-Nachrichten an mehrere Netzwerke (Subnetze) innerhalb eines Unternehmens oder in der ganzen Welt übermittelt werden.

TKIP (Temporal Key Integrity Protocol)
Eine Sicherheitsfunktion zur Verbesserung von WEP: TKIP und MIC (Message Integrity Check) sind Modifikationen von WEP zum Schutz gegen bekannte Angriffe (WEP und vier Patches für paketweises Ändern von Schlüsseln, Nachrichtenintegrität, Neuverschlüsselung und Initialisierungsvektorschutz).

Universal Plug and Play (UPnP)
UPnP vereinfacht die Vernetzung von Geräten aller Art, beispielsweise von Internet-Geräten und Computern. UPnP-fähige Geräte erkennen die von anderen registrierten UPnP-Geräten im Netzwerk angebotenen Dienste automatisch.

USB (Universal Serial Bus)
Eine bidirektionale, serielle Hochgeschwindigkeitsverbindung zwischen einem PC und einem Peripheriegerät, die Daten bei 12 MBit/s überträgt. Der neue Standard USB 2.0 bietet sogar eine Übertragungsrate von bis zu 480 MBit/s. IEEE 1394, FireWire und iLink bieten allesamt eine Bandbreite von bis zu 400 MBit/s.

Voice over IP (VoIP, auch als IP-Telefonie bekannt)
Sprachübertragung, bei der mit Hilfe von IP digitale Pakete zum Versand über das Internet erstellt werden. VoIP kann kostengünstiger sein als die Sprachübertragung in herkömmlichen analogen Paketen über POTS (Plain Old Telephone Service, ein international gebräuchliches Synonym für den analogen Telefondienst).

VPN (Virtual Private Network)
Ein Verfahren, das die Sicherheit bei der Datenübertragung über das Internet erhöhen soll. VPN kann bei kabelgebundenen und drahtlosen Netzwerken sowie bei Einwahlverbindungen über analoge Telefonleitungen eingesetzt werden. VPN richtet einen privaten, verschlüsselten Tunnel ein, der vom Computer des Endbenutzers durch das drahtlose Netzwerk und das Internet hindurch bis hin zu den Unternehmensservern und -datenbanken reicht.

Warchalking
Das Anbringen von Kreidemarkierungen an Mauern, Gehwegen, Gebäuden, Schildern, Bäumen usw., um das Bestehen eines offenen drahtlosen Netzwerks, in der Regel mit einer Internetverbindung, zu kennzeichnen. So können Eingeweihte erkennen, wo sie gratis eine drahtlose Verbindung nutzen können. Die offenen

Verbindungen stammen meist von den Access Points von drahtlosen Unternehmensnetzwerken in den Gebäuden. Die Kreidesymbole lassen erkennen, welche Art von Access Point an dieser spezifischen Stelle verfügbar ist. Derzeit werden drei Hauptzeichen verwendet: Zwei Rücken an Rücken positionierte Halbkreise verweisen auf einen offenen Knoten, ein geschlossener Kreis zeigt einen geschlossenen Knoten an und ein geschlossener Kreis mit einem „W“ in der Mitte steht für einen Knoten, bei dem WEP aktiviert ist. Warchalker geben zudem über den Symbolen oft das Passwort an, das zum Zugreifen auf den Knoten erforderlich ist. Dies kann mit Hilfe von Sniffer-Software leicht ermittelt werden.
Da Warchalking relativ neu ist, ist die Debatte über dessen Legalität noch nicht abgeschlossen.
Es geht zurück auf wandernde Arbeiter in den USA der dreißiger Jahre, die ähnliche Markierungen an Häusern hinterließen, um anderen Wanderern zu signalisieren, ob dieses Haus Reisenden gegenüber aufgeschlossen war oder nicht.

Wardriving
Wardriving ist das Aufspüren und unter Umständen auch Nutzen von Verbindungen zu WLANs in Städten oder anderen Umgebungen. Zum Wardriving benötigt man ein Fahrzeug, einen Computer (z. B. ein Notebook), eine drahtlose Netzwerkkarte im Mixmode und eine Antenne, die auf dem Dach oder im Inneren des Autos angebracht werden kann. Da die Reichweite eines drahtlosen LAN oft über das jeweilige Bürogebäude hinausgeht, können sich Eindringlinge von außen Zugang zum Netzwerk verschaffen, eine kostenlose Internetverbindung nutzen und vielleicht sogar auf Unternehmensunterlagen und andere Ressourcen zugreifen.
Manche Leute betreiben Wardriving als eine Art Sport, teilweise auch um aufzuzeigen, wie anfällig WLANs für derartige Angriffe sind. Mit Hilfe einer omnidirektionalen Antenne und eines Positionierungssystems (GPS) kann der Wardriver die Standorte der 802.11b-Wireless-Access-Points systematisch bestimmen.

WEP (Wired Equivalent Privacy)
Das durch WiFi bereitgestellte grundlegende Verschlüsselungsverfahren für drahtlose Netzwerke. In manchen Fällen reicht WEP vollkommen aus, um die Sicherheitsanforderungen von Heimanwendern und kleinen Unternehmen im drahtlosen Netzwerk zu erfüllen. Bei WEP sind Verschlüsselungsmodi mit 40 Bit (oft auch als 64-Bit-Verschlüsselung bezeichnet) oder 104 Bit (oft auch als 128-Bit-Verschlüsselung bezeichnet) verfügbar. Da bei der 104-Bit-Verschlüsselung ein längerer Algorithmus verwendet wird, der aufwendiger zu entschlüsseln ist, kann sie größeren Schutz bieten als die einfache 40-Bit- (64-Bit-)Verschlüsselung.

WiFi (Wireless Fidelity)
Eine andere Bezeichnung für den Standard IEEE 802.11b. Produkte mit WiFi-Zertifizierung sind vollständig miteinander kompatibel, selbst wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines WiFi-Produkts kann einen Access Point einer beliebigen Marke mit Client-Hardware jeder anderen Marke kombinieren, solange beide Geräte dem WiFi-Standard entsprechen.

Wi-Fi Alliance (früher WECA, Wireless Ethernet Compatibility Alliance)
Die Wi-Fi Alliance ist eine gemeinnützige internationale Vereinigung, die 1999 gegründet wurde, um die Kompatibilität von WLAN-Produkten des Standards IEEE 802.11 zu zertifizieren. Derzeit sind 193 Unternehmen aus aller Welt Mitglied der Wi-Fi Alliance und 509 Produkte haben seit Beginn der Zertifizierung im März 2000 die WiFi-Zertifizierung erhalten. Die Zielsetzung der Wi-Fi Alliance und ihrer Mitglieder ist eine Verbesserung der Benutzerfreundlichkeit durch Produktkompatibilität (*www.weca.net*).

WPA (Wi-Fi Protected Access)

WPA ist ein Verschlüsselungsverfahren für drahtlose Netzwerke, das die Authentifizierung und Verschlüsselung gegenüber WEP (Wired Equivalent Privacy) verbessert. WPA wurde von der Netzwerkbranche als Reaktion auf die Schwächen von WEP entwickelt.

Ein wichtiger Teil von WPA ist das Protokoll TKIP (Temporal Key Integrity Protocol). TKIP behebt die Verschlüsselungsschwächen von WEP. Eine weitere zentrale Komponente von WPA ist die integrierte Authentifizierung (die in WEP nicht enthalten ist). Dank dieser Funktion kann WPA ein Sicherheitsniveau erreichen, das sich in etwa mit dem eines VPN-Tunnels mit WEP vergleichen lässt, wobei WPA sich jedoch deutlich einfacher verwalten und benutzen lässt. WPA funktioniert ähnlich wie 802.1x-Unterstützung und erfordert einen RADIUS-Server für die Implementierung. Die Wi-Fi Alliance wird diese Form von WPA als „WPA-Enterprise“ bezeichnen.

Zu WPA gibt es auch eine Variante namens „WPA Pre-Shared Key“ (WPA-PSK). Diese bietet eine Authentifizierungsalternative zu einem teuren RADIUS-Server. WPA-PSK ist eine vereinfachte, aber immer noch sehr leistungsstarke Form von WPA, die besonders für drahtlose Heimnetzwerke geeignet ist. Zur Verwendung von WPA-PSK wird wie bei WEP ein statischer Schlüssel (auch als „Passphrase“ bezeichnet) festgelegt. Doch mit Hilfe von TKIP kann WPA-PSK diesen Schlüssel automatisch in bestimmten voreingestellten Zeitabständen ändern. So wird es sehr viel schwerer für Hacker, den Schlüssel zu finden und zu missbrauchen. Die Wi-Fi Alliance wird diese Form von WPA als „WPA-Personal“ bezeichnen.

WPA und IEEE 802.11i im Vergleich

WPA wird mit dem derzeit vom IEEE entwickelten Sicherheitsstandard IEEE 802.11i kompatibel sein. WPA ist eine Untergruppe des aktuellen 802.11i-Entwurfs, die einige der bereits einsatzreifen Elemente des 802.11i-Entwurfs umsetzt, darunter 802.1x und TKIP. Diese Funktionen können zudem bei den meisten vorhandenen Produkten mit Wi-Fi-Zertifizierung mit Hilfe eines Software-Upgrades aktiviert werden. Die wichtigsten Elemente des 802.11i-Entwurfs, die nicht in WPA enthalten sind, sind sicheres IBSS, Secure Fast Handoff, sichere Deauthentifizierung und Abmeldung sowie verbesserte Verschlüsselungsprotokolle wie AES-CCMP. Diese Funktionen sind entweder noch in der Entwicklung oder es sind Hardware-Upgrades für ihre Implementierung erforderlich.

WPA für Unternehmen

WPA erfüllt die WLAN-Sicherheitsanforderungen von Unternehmen auf effektive Weise und bietet eine leistungsstarke Verschlüsselungs- und Authentifizierungslösung bis zur Ratifizierung des Standards IEEE 802.11i. In einem Unternehmen mit einer eigenen EDV-Abteilung sollte WPA in Verbindung mit einem Authentifizierungsserver (z. B. RADIUS) eingesetzt werden, um eine zentrale Steuerung und Verwaltung des Netzwerkzugangs zu ermöglichen. Bei einer solchen Implementierung kann auf zusätzliche Lösungen wie VPNs verzichtet werden, vor allem, wenn es nur darum geht, die drahtlose Verbindung mit dem Netzwerk sicherer zu gestalten.

WPA für Klein- und Heimbüros

In einem Heimnetzwerk oder einer SOHO-Umgebung (Small Office/Home Office), wo es keine zentralen Authentifizierungsserver und keinen EAP-Rahmen gibt, wird WPA in einem speziellen Modus ausgeführt. Dieser Modus, der oft auch als „Pre-Shared Key“ (PSK) bezeichnet wird, ermöglicht die Benutzung von manuell eingegebenen Schlüsseln oder Passwörtern und wurde für die bequeme Einrichtung durch Privatbenutzer entwickelt. Der Privatbenutzer muss lediglich beim Access Point oder drahtlosen Heim-Gateway sowie auf jedem PC, der zum WiFi-Netzwerk gehört, ein Passwort (das auch als „Hauptschlüssel“ oder „Master Key“ bezeichnet wird) eingeben. Alles Weitere wird automatisch durch WPA geregelt. Erstens wird nur Geräten mit dem richtigen

Passwort der Zugang zum Netzwerk gestattet, so dass Lauscher und andere nicht autorisierte Personen ausgesperrt werden. Zweitens startet das Passwort automatisch die TKIP-Verschlüsselung (siehe weiter oben).

WPA für Public Access

Die in WPA festgelegten Verschlüsselungs- und Authentifizierungsmechanismen sind auch für Anbieter von drahtlosen Internetdiensten (Wireless Internet Service Provider, WISP) interessant, die so genannte „Hot-Spots“ – öffentlich zugängliche WiFi-Access-Points – betreiben. Da sich die Benutzer meist nicht gegenseitig kennen, sind sichere Datenübertragung und Authentifizierung dort von besonderer Bedeutung. Die in WPA definierte Authentifizierungsfunktion aktiviert einen sicheren Zugriffssteuerungsmechanismus für die Dienstanbieter und für mobile Benutzer, die keine VPN-Verbindungen verwenden.

WPA im „gemischten Modus“

In einem großen Netzwerk werden höchstwahrscheinlich die Access Points vor den WiFi-Clients ersetzt. Access Points können daher manchmal auch in einem „gemischten Modus“ betrieben werden, der sowohl WPA-Clients als auch die herkömmlichen WEP-Clients unterstützt. So nützlich dies für die Übergangszeit auch ist, hat die Unterstützung beider Arten von Client-Geräten doch sehr nachteilige Auswirkungen auf die Sicherheit, die so bei allen Geräten auf dem weniger sicheren WEP-Niveau liegt. Es lohnt sich daher für Unternehmen, den Wechsel zu WPA für alle WiFi-Clients und Access Points zu beschleunigen.

WiMAX

Eine IEEE 802.16-Arbeitsgruppe, die einen Standard für feste drahtlose Breitbandzugangssysteme auf Grundlage einer PMP-Architektur (Point-to-Multipoint) festlegt. Arbeitsgruppe 1 des Bereichs IEEE 802.16 hat einen Standard für den drahtlosen PMP-Breitbandzugang für Systeme im Frequenzbereich 10–66 GHz entwickelt. Der Standard gilt sowohl für die MAC- (Media Access Control) als auch für die Bitübertragungsschicht.

Wireless Multimedia (WMM)

WMM (Wireless Multimedia) ist eine Untergruppe des Standards 802.11e. Mit WMM kann drahtlos versendeten Daten je nach Datentyp eine unterschiedliche Priorität gegeben werden. Daten, bei denen Zeit eine wichtigere Rolle spielt (z. B. Video-, Audio- oder Sprachdaten) erhalten eine höhere Priorität als zeitlich unkritische Daten. WMM funktioniert jedoch nur, wenn die drahtlosen Clients WMM-fähig sind.

Drahtloses Netzwerk

Die Infrastruktur, die die drahtlose Übertragung von Signalen ermöglicht, wird als drahtloses Netzwerk bezeichnet. In einem Netzwerk sind unterschiedliche Geräte miteinander verbunden, und Ressourcen können von mehreren Teilnehmern gemeinsam genutzt werden.

WLAN (Wireless LAN)

Wird manchmal auch als „LAN“ bezeichnet. Ein LAN, das für die Kommunikation zwischen den einzelnen Knoten Hochfrequenzfunkwellen statt Kabeln verwendet.