„Beacons“ (engl. „Leuchtfeuer“), an alle Stationen im Empfangsbereich. Die Beacons enthalten u. a. folgende Informationen:

- Netzwerkname *(„Service Set Identifier“,* SSID)
- Liste unterstützter Übertragungsraten
- Art der Verschlüsselung

Dieses „Leuchtfeuer“ erleichtert den Verbindungsaufbau ganz erheblich, da die Clients lediglich den Netzwerknamen und optional einige Parameter für die Verschlüsselung kennen müssen. Gleichzeitig ermöglicht der ständige Versand der Beacon-Pakete die Überwachung der Empfangsqualität – auch dann, wenn keine Nutzdaten gesendet oder empfangen werden. Beacons werden immer mit der niedrigsten Übertragungsrate (1 MBit/s) gesendet, der erfolgreiche Empfang des „Leuchtfeuers“ garantiert also noch keine stabile Verbindung mit dem Netzwerk. Bild: Cisco Aironet AIR-AP1600 mit angeschraubten Antennen; Foto: Cisco

4.3.3 WLAN-Sicherheitsstandards

WLANs sind ohne zusätzliche Maßnahmen eine Sicherheits-Schwachstelle des gesamten Unternehmens. Deshalb haben sich im Laufe der Jahre eine ganze Reihe von Sicherheitsstandards entwickelt.

Man unterscheidet grundsätzlich drei Sicherheitsfunktionen, die voneinander unabhängig implementiert sein können:

- **Authentifizierung**: Computerauthentifizierung, Benutzerauthentifizierung
- **Verschlüsselung**: Die Daten zwischen Client und WLAN-Access Point werden verschlüsselt übertragen.
- **Datenintegrität**: Überprüfung, ob die Daten während der Übertragung nicht verändert wurden

Bei allen Sicherheitsstandards ist darauf zu achten, welche dieser drei Sicherheitsfunktionen implementiert wurden.

Der grundlegende Unterschied zwischen den "Personal" und "Enterprise"-Varianten von WPA und WPA2 ist die Art der Authentifizierung. Bei den "Personal"-Varianten wird ein *Pre-Shared Key* (PSK) verwendet, während bei den "Enterprise"-Varianten ein Authentifizierungsserver nötig ist.

4.3.4 IEEE 802.1X-Authentifizierung

EAP ist ein allgemeines, von der *Internet Engineering Task Force* (IETF) entwickeltes Authentifizierungsprotokoll, das verschiedene Authentifzierungsverfahren unterstützt. Mit EAP wird der eigentliche Authentifizierungsmechanimus nicht während der Herstellung der PPP-Verbindung gewählt, sondern erst nachher, in der Authentifizierungsphase. In dieser Phase handeln die Teilnehmer den sogenannten **EAP-Typ** aus.

	Verschlüsselung	Authentifizierung	Datenintegrität
WEP	RC4	Open System, Pre-Shared-Key	Keine
WPA-Personal	TKIP (RC4-basierend)	Pre-Shared Key	Michael
WPA-Enterprise	TKIP (RC4-basierend)	EAP, RADIUS (IEEE 802.1X)	Michael
WPA2-Personal	CCMP (AES-basierend)	Pre-Shared Key	AES-CBC-MAC
WPA2-Enterprise	CCMP (AES-basierend)	EAP, RADIUS (IEEE 802.1X)	AES-CBC-MAC

Von Microsoft unterstützte EAP-Typen	
EAP-MSCHAPv2 (Extensible Authentication Protocol – MSCHAPv2)	Computerauthentifizierung mit Zertifikat; Benutzerauthentifizierung mit Benutzername/Kennwort
EAP-TLS (EAP – Transport Layer Security)	RFC 5216. TLS ist ein Nachfolgestandard von SSL; zertifikatsbasierte Authentifizierung von Computern und Benutzern erforderlich (Smartcards)
EAP-IKEv2 (EAP – Internet Key Exchange v2)	RFC 5106. Authentifizierung mit Zertifikat.
PEAP/EAP-TLS	So wie EAP-TLS, allerdings mit verschlüssentem Kanal während des Verbindungsaufbaus
PEAP/EAP-MSCHAPv2	So wie EAP-MSCHAPv2, allerdings mit verschlüssentem Kanal während des Verbindungsaufbaus

Microsoft unterstützt folgende EAP-Typen:

Weitere EAP-Typen sind:

- **EAP-TTLS** *(Tunneled Transport Layer Security)*
- **LEAP** *(Lightweight Extensible Authentication Protocol, Cisco):* kann durch einfache Wörterbuch-Attacken geknackt werden.
- EAP-FAST *(Cisco, Flexible Authentication via Secure Tunneling):* Sowohl der Client als auch der Server generieren vor der Kommunikation einen Schlüssel

EAP ermöglicht zwar eine flexible Authentifizierung, jedoch wird die gesamte EAP-Konversation unverschlüsselt übertragen.

PEAP ist ein spezieller EAP-Typ, der zunächst für einen sicheren Kanal mit verschlüsselter Übertragung sorgt, dessen Unversehrtheit mit TLS gesichert wird. Anschließend findet eine neue EAP-Verhandlung mit einem anderen EAP-Typ statt. Vorteil der Verwendung von PEAP ist, dass bei WLAN-Authentifizierungen sogar kennwortbasierende Verfahren (PEAP-MSCHAPv2) genutzt werden können, die normalerweise anfällig für Wörterbuch-Angriffe sind.

4.4 PAN – Personal Area Networks („Bluetooth“)

Darunter versteht man einen Funk-LAN-Standard für Netze geringer Bandbreite mit kurzer Reichweite (< 10 m), genormt als IEEE 802.15.1.

1998 wurde von den Firmen IBM, Toshiba, Intel, Ericsson und Nokia die „Bluetooth Special Interest Group“ ins Leben gerufen, die sich seither mit der Weiterentwicklung und Anwendung dieses Standards beschäftigt. Der Name stammt von einem nordischen König mit dem Spitznamen „Blauzahn“.

Geräte, die Bluetooth unterstützen, werden mit dem Bluetooth-Logo gekennzeichnet (siehe Bild rechts).

Aktueller Standard: Bluetooth 4.2 (Dez. 2014)

Als Frequenzbereich wird der ISM-Bereich benützt (2,402 GHz bis 2,480 GHz). Eine spezielle Eigenschaft, das *„Frequency Hopping Spread Spectrum“* (FHSS) gewährleistet die Sicherheit der Datenübertragung: alle 625 µs wird die Trägerfrequenz geändert.

Mit Bluetooth ist eine Datenübertragungsrate von 64 kbit/s bei synchroner Sprachübertragung und 732,2 kbit/s Download/57,6 kbit/s Upload bei asynchronen Datenübertragungen erreichbar. Ab Bluetooth 2.0 + EDR *(Enhanced Data Rate)* sind Datenübertragungsraten bis ca. 2,1 Mbit/s möglich.

Die Geräte identifizieren einander automatisch, indem sie ihre 48 Bit-MAC-Adressen austauschen.