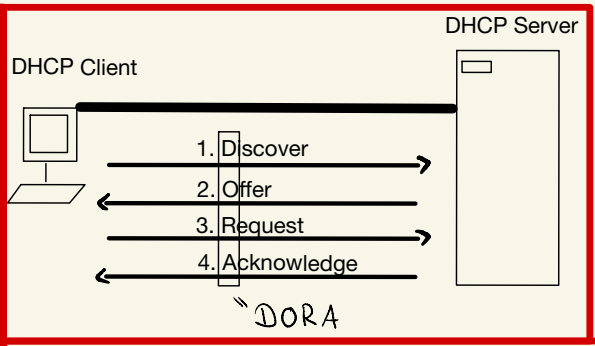
SCHICHT (ENGLISCH UND DEUTSCH)	FUNKTION
Anwendungsschicht (Application)	Führt Dienste für die Anwendung aus, die vom Endbenutzer verwendet werden. (HTTP, FTP, SMTP, DNS...)
Darstellungsschicht (Presentation)	Stellt der Anwendung Informationen zum Datenformat zur Verfügung. So gibt die Darstellungsschicht der Anwendungsschicht an, ob die Daten verschlüsselt sind, ob es sich um ein JPG-Bild handelt usw.
Sitzungsschicht (Session)	Verwaltet Sitzungen zwischen den Benutzern. Zum Beispiel synchronisiert die Sitzungsschicht mehrere Websitzungen in Webkonferenzen.
Transportschicht (Transport)	Definiert Datensegmente und nummeriert sie beim Absender, überträgt die Daten und setzt sie beim Empfänger wieder zusammen.
Vermittlungsschicht (Network)	Erstellt und adressiert Pakete zum Ende-zu-Ende-Transport in andere Netzwerke mithilfe von Vermittlungsgeräten (Routern).
Sicherungsschicht (Data Link)	Erstellt und adressiert Frames für die Host-zu-Host-Übertragung in lokalen Netzwerken (LANs) mithilfe von Netzzugangsgeräten (Switches).
Bitübertragungsschicht (Physical)	Überträgt binäre Daten über Medien zwischen Geräten.



WLAN Standards

IEEE 802.11 Standard	Theoretical Max Data Transfer Rate	Frequency
802.11	2Mbps	2.4GHz
802.11a	54Mbps	5GHz
802.11b	11Mbps	2.4GHz
802.11g	54Mbps	2.4GHz
802.11n	600Mbps	2.4GHz & 5GHz
802.11ac	866.7Mbps	5GHz
802.11ax	**4804 Mbits/s**	**2,5GHz & 5 GHz**

Aktueller WLAN Standard:
WiFi 6 = 802.11ax

4 Authentifizierungsmethoden

Open System

Bei einem „Open System" wird auf eine Authentifizierung durch den Access Point verzichtet. Voraussetzung ist nur, dass der WLAN-Client die richtige SSID (WLAN-Name) des Access Point kennt. Die WLAN-Verbindung ist dann aber in der Regel nicht verschlüsselt.

Pre-Shared Key

Bei der Authentifizierung mit einem Pre-Shared Key (PSK) ist im Access Point ein Passwort hinterlegt, mit dem sich alle WLAN-Clients authentifizieren müssen. Stimmt das Passwort mit dem eingestellten Passwort nicht überein, dann verweigert der Access Point die Authentifizierung des Clients. Erst wenn das Passwort korrekt ist, dann ist die Authentifizierung erfolgreich und eine Verbindung möglich.

WPS

Mit WPS kann man WLAN-Clients per Tastendruck, PIN-Eingabe oder NFC mit dem WLAN verbinden. WPS vereinfacht die Authentifizierung von Geräten ohne Anzeige- und Bedienelemente. In der Praxis wird WPS selten verwendet und viele Implementierungen sind leider nicht sicher, weshalb die Empfehlung gilt, WPS im WLAN-Router abzuschalten.

Eine Alternative ist das Device Provisionen Protocol (DPP), welche das WPS ergänzen soll. Hier werden alternative Identifikationsmerkmale, wie QR-Codes verwendet.

Captive Portal

Ein Captive Portal ist eine Webseite, auf die automatisch umgeleitet wird, wenn sich ein neuer WLAN-Gast an einem öffentlichen WLAN oder WLAN-Hotspot angemeldet hat. Über das Captive Portal werden die Gäste typischerweise auf Anwendungsebene authentifiziert. Zum Beispiel um die Nutzung zu begrenzen, abzurechnen oder zu protokollieren.

Verschlüsselungen

Bei WPA bzw. WPA2 erfolgt die Netzwerk-Authentifizierung mit einem Pre-Shared-Key (PSK) oder alternativ über einen zentralen 802.1x/Radius-Server (Enterprise Mode). Dabei wird ein Passwort mit 8 bis 63 Zeichen Länge verwendet.

WPA3 enthält eine Implementierung des sogenannten Dragonfly-Protokolls mit Simultaneous Authentication of Equals (SAE). Ziel dieser Implementierung ist es, die Sicherheit beim Schlüsselaustausch mit dem Handshake-Verfahren zu verbessern.

Sicherheitslücke: WPA2 mit Pre-Shared-Key gilt als einigermaßen sicher, wenn ein starkes Passwort (komplex und lang) verwendet oder noch besser ein zentraler Radius-Server für die Authentifizierung eingesetzt wird (Enterprise Mode). Der Key kann im 3. Oder 4. Schritt abgefangen und verändert werden. Somit kann sich Zugriff verschafft werden.