WLAN-Funktionalität und -Sicherheit (Nikita, Joel, Lukas)

1:

ad hoc mode:
-Komunikation direkt zwischen 2 Clients
-Kein Zentralle Controlle
infrastructure mode:
-Zentrallen Acces Point

2:

IEEE 802.11s ist ein Standard für ein Wireless Mesh Network (WMN) in dem WLAN-fähige Geräte für andere Geräte als Relaisstationen bis zum nächstgelegenen Access Point dienen.

Merkmale von IEEE 802.11s

- dynamisches Routing auf MAC-Ebene
- Änderungen am Kanalzugriff
- Ergänzungen zum Sicherheitskonzept

3:

QoS bezeichnet das Maß an erfüllten Anforderungen von dem Anwender an ein Kommunikationsnetzwerk und wird auch Dienstgüte genannt. Zu den Anforderungen gehören ein schneller und zuverlässiger Verbindungsaufbau, eine hohe Stabilität der bestehenden Verbindungen, eine hohe Übertragungsqualität, eine fehlerfreie und störungsfreie Übertragung und kurze Wartezeiten bei der Kommunikation.
Bei QoS werden bestimmte Datenpakete anderen bevorzugt, um Paketverluste zu entgehen. Dienste mit hoher Priorität sind z.B. VoIP oder Video Streams, da bei denen die Paketverluste und somit geringere Qualitäten schnell dem Anwender negativ auffallen.

4:

Die Abkürzung SSID steht für "Service Set Identifier". Über sie lässt sich das Netzwerk ansprechen und ist manuell wählbar. Auch können manche Geräte mehrere SSIDs gleichzeitig tragen, um großere Freiheiten in der Konfiguration zu lassen. Bei identischen SSIDs kann es passieren, dass Geräte nicht wissen, mit welchem Access Point sie sich verbinden sollen. Das kann zu Verbindungsproblemen führen. Eine SSID kann 32 Bytes lang sein.

5:

WEP: Nicht sicher, da veraltet und demnach gefährdet.
WPA: Nicht sicher, da veraltet und demnach gefährdet.
WPA2: Sicher genug. Aktuell meist verbreitete WLAN-Sicherheit.
WPS: Nicht sicher, da einfach (in relativ kurzer Zeit über Brute-Force) zu knacken.
WPA3: Sicher. Aktuell höchste WLAN-Sicherheit.

6:

PSK: Vorher Vereinbarter Schlüssel eines symmetrischen Kryptosystems, welcher allen Teilnehmern bekannt sein muss. Vorteil ist die Einfachheit der Zulassung neuer Teilnehmer,

Nachteil, dass der Schlüssel verteilt werden muss und jeder (auch ungewollte) Teilnehmer, welcher den Schlüssel besitzt Zugriff hat.
EAP: Erweiterbares Authentifizierungsprotokoll, das unterschiedliche Authentifizierungsverfahren wie z.B. Benutzername/Passwort, Digitale Zertifikate, SIM-Karte, etc. unterstützt. Vorteile: Mehrere Authentifizierungsmechanismen möglich, die nicht in der Verbindungsaufbauphase ausgehandelt werden müssen. Nachteile: Da der Authentifizierungsprozess noch ohne Verschlüsselung abläuft, wird der Nutzername im Klartext übertragen.