Klausur Lernzettel

Client mit Netzwerk verbinden

Aufgaben und Aufbau folgender Netzwerk-Einstellungen:

MAC-Adresse:

- Media Access Control
- die physische Adresse eines Geräts
- 48 bit lang (6 Byte: 6 x 8 bit)
- besteht aus
    - Herstellerkennung 24 bit (3 Byte)
    - Gerätekennung 24 bit (3 Byte)
- Byte werden in 2-stelligen Hexadezimalzahlen angegeben, bspw. 68-C6-AC-F9-25-4F
- werden unverschlüsselt übertragen und können mitgeschnitten werden --> keine Sicherheitsquelle

IP-Adresse:

- Zwei Versionen IPv4 und IPv6 (neuer, mehr Adressen)
- Die IP-Adresse ist die logische Adresse eines Clients in einem Netzwerk
- IPv4-Adressen bestehen aus 4 x 8 bit, auch Oktette genannt
- Es gibt einen privaten und einen öffentlichen IP-Adressbereich
- in einem normalen Heimnetzwerk hat nur der Router eine öffentliche IP-Adresse, die das Netzwerk identifiziert; alle Teilnehmer dahinter haben eine lokale, private IP-Adresse
- Die privaten IPv4-Adressbereiche lauten:
    - A-Klasse: 10.0.0.0 bis 10.255.255.255
    - B-Klasse: 172.16.00 bis 172.31.255.255
    - C-Klasse: 192.168.0.0 bis 192.168.255.255
- Spezielle IP-Addressen:
    - 127.0.0.0 /8 - Loopback-Adresse: wird verwendet, um Nachrichten an den eigenen Client zu senden
    - 169.254.0.0 /16 - APIPA-Adressbereich; wird die IP-Adresse weder durch DHCP noch manuell festgelegt, wird dem Client eine Adresse aus diesem Bereich zugeteilt
    - 192.0.2.0 /24 - Adressbereich zur Verwendung in Dokumentationen und Beispielen
- zwei feste IP-Adressen in einem jeden Netzwerk: Netzwerkadresse und Broadcastadresse --> Menge der Host-Adressen im Netzwerk immer 2^X -2 (wo X = Menge der 0en in Subnetzmaske); --> Menge der (möglichen) Subnetze immer 2^Y (wo Y Menge der variablen 1 im Netzwerkanteil der Subnetzmaske - je nach IP-Adressbereich)

IP-Adresskonflikte

- ARP: Address Resolution Protocol - soll die MAC-Adresse zu einer gegebenen IP-Adresse im eigenen Subnetz ermitteln
- Vorgehensweise:
    1. ARP-Request: Rechner stellt Frage per MAC-Broadcast (Adresse: FF:FF:FF:FF:FF:FF) an alle Teilnehmer: Wer hat IP-Adresse x.y.z.a?
    2. Rechner mi tder passenden IP-Adresse antwortet: Ich habe IP-Adresse xyz und meine MAC-Adresse lautet abc.
    3. Die Antwort wird im ARP-Cache zwischengespeichert
- Gratuitous ARP: ARP-Request nach der eigenen IP-Adresse; Zweck: andere von geänderter IP/MAC-Kombination unterrichten und Test ob anderer Rechner die gleiche IP verwendet

Subnetzmaske:

- Gibt Aufschluss über die Größe des Netzwerks, in dem sich der Client befindet
- Wird standardmäßig als Slash "/" hinter der IP-Adresse angegeben, CIDR-Notation
    - bspw. 192.168.2.0 /24

Standard-Gateway:

- die Adresse des Routers, über die Teilnehmer eines Netzwerks das Subnetz verlassen und mit außerhalb befindlichen Clients kommunizieren können
- die Vermittlung zu außerhalb befindlichen Teilnehmern wird *Routing* genannt

ICMP

- ping-Protokoll, mit dem Diagnose- und Fehlerdaten bei der Verbindung ermittelt werden können
- ggf. ist das Protokoll deaktiviert (durch Firewall etc.)

DHCP

- Protokoll, das die automatische Verteilung von IP-Adressen im lokalen Netzwerk übernimmt
- ist DHCP nicht verfügbar, müssen IP-Adressen manuell vergeben werden
- wird auch dies nicht gemacht, übernimmt das **APIPA**-Protokoll (Automatic Private IP Adressing) und verteilt eine Adresse aus dem APIPA-Adressbereich (169.254.0.0 /16)

Umrechnung Hexadezimal <-> Binär

- siehe SUD-Lernzettel

Dateneinheiten

Basis 10 (SI-Präfixe)

10^3 = Kilobyte 10^6 = Megabyte 10^9 = Gigabyte 10^{12} = Terabyte 10^{15} = Petabyte 10^{18} = Exabyte 10^{21} = Zettabyte 10^{24} = Yottabyte

Basis 2 (IEC-/Binärpräfixe)

2^{10} = Kibibyte 2^{20} = Mebibyte
2^{30} = Gibibyte 2^{40} = Tebibyte 2^{50} = Pebibyte 2^{60} = Exbibyte 2^{70} = Zebibyte 2^{80} = Yobibyte

WLAN

Access Point

- der Access Point ist Gerät, was die Verbindung mit kabelgebundene Verbindung mit einem Router in ein WLAN-Signal umwandelt
- Über die Verwendung mehrere Access Points kann die Reichweite eines WLAN-Netwerkes erweitert werden.
- Mobilgeräte mit WLAN-Adapter können sich mit dem Access Point verbinden

SSID

- Service Set Identifier
- Name des Access Points einer WLAN-Verbindung
- Wird benötigt, um eine Verbindung aufzubauen
- Multi-SSID: Über die Vergabe von SSIDs können bspw. auch in einem Router verschiedene Arten von Netzwerk- und Zugangsmöglichkeiten getrennt werden (bspw. 2,4 und 5 GHz Netze)

PEAP

- Protected Extensible Authentication Protocol
- Erweiterung des Extensible Authentication Protocol, welches ein Authentifizierungs-Framework ist
- Über sog. EAP-Methoden kann Zugriff auf ein Netzwerk geregelt sein (bspw. über Anmeldung)
- PEAP erweitert EAP um einen TLS-Tunnel

IEEE-Standards

- WLAN-Standards, folgende werden unterschieden

IEEE-Bezeichnung	Wi-Fi Name	Frequenzband
802.11n	Wi-Fi 4	2,4 GHz u. 5 GHz
802.11ac	Wi-Fi 5	5 GHz
802.11ax	Wi-Fi 6(E)	2,4 GHz, 5 GHz (und 6 GHz)
802.11be	Wi-Fi 7	2,4 GHz, 5 GHz und 6 GHz

- generell gilt: je neuer der Standard, desto besser die Übertragungsrate/Geschwindigkeit

Frequenzen

2,4 GHz

- operiert im Bereich von 2.400 MHz bis 2.500 MHz --> 100 MHz Bandbreite
- 14 Kanäle, in Europa nur 13
- Zur Übertragung wird eine Trägerfrequenz mit mindestens 20 bzw. 22 MHz Breite benötigt;

- Kanäle können sich überlappen, wenn Trägerfrequenzen direkt nebeneinander liegen
- Bspw. Kanal 1, 7, 13 (22 MHz Breite) oder 1, 5, 9, 13 (MHz Breite) für überlappungsfreie Kanäle

5 GHz

- 25 Kanäle bei einer 20 MHz Trägerfrequenz --> keine Überlappung
- Kanalbreiten von 20, 40, 80 oder 160 MHz überlappungsfrei möglich, mit entsprechend weniger Kanälen

Kanäle

- Die Frequenzbereiche der einzelnen Standards werden in Kanäle aufgeteilt
- 2,4 GHz = 13 Kanäle in Europa
- Die Kanäle sind jedoch eng aneinander und überlappen sich -> man kann nicht alle der 13 Kanäle gleichzeitig verwenden
- Es sind bspw. nur 3 nicht-überlappende Kanäle bei einer Kanalbreite von 20 MHz nutzbar
- Die optimale Belegung im 2,4 GHz Bereich für Europa wäre bspw. 1, 7, 13 (oder 1, 5, 9/13) bei einer Kanalbreite von 20 MHz
- Die Kanalbreite ist begrenzender Faktor dafür, wie viele Daten gesendet werden können
- Je höher die Kanalbreite, desto höher die Datenübertagungsrate, aber desto geringer die Reichweite und Störungsanfälligkeit
- Typische Kanalbreiten:
    - 2,4 GHz: 20, 40 MHz
    - 5 GHz: 20, 40, 80, 160 MHz
- Bei 20 MHz Kanälen:
    - 2,4 GHz: bis zu 4 überlappungsfreie Kanäle
    - 5 GHz: bis zu 25 überlappungsfreie Kanäle

Bandbreiten

- Die Frequenzbereiche 2,4 GHz und 5 GHz werden in Bereiche aufgeteilt, sogenannte Bandbreiten
- 2,4 GHz: 2,3995 bis 2,4845 GHz ~ ca. 85 MHz Bandbreite
- 5 GHz: 5,150 bis 5,350 GHz und 5,470 GHz bis 5,725 GHz ~ 200 bis 500 MHz
    - Das obere Frequenzband wird auch für Flug- und Wetterradar verwendet. Um Störungen zu vermeiden:
    - DFS: Dynamic Frequency Selection wechselt Frequenzen dynamisch, wenn Signale anderer Funksignale erkannt werden
    - TPC: Transmitter Power Control reduziert die Leistung, um Störungen zu vermeiden
    - Alternativ: Nur im Bereich 5,1 bis 5,3 GHz senden --> weniger Kanäle
- 6 GHz: 5,925 GHz bis 6,425 GHz ~ 500 MHz

Vor- und Nachteile der Frequenzbereiche

Vorteile

- 2,4 GHz:
    - Unterstützung von älteren Geräten
    - Bessere Durchdringungn von Wänden/abschirmender Materialien
- 5 GHz:
    - Nicht so störanfällig für Überlastung dank mehrerer Kanäle und geringerer Auslastung
    - Höhere Übertragungsrate
    - 19 nicht überlappende Kanäle

Nachteile

- 2,4 GHz
    - Viele störende Systeme im Frequenzband (bspw. Mikrowellen, Bluetooth, Babyphone etc.)
    - nur 3 überlappungsfreie Kanäle (1, 5, 9 und 13) --> Frequenzband und Kanäle sind schnell überlastet
- 5 GHz
    - Geräte müssen mindestens 802.11n unterstützen --> nicht kompatibel mit älteren Standards
    - schlechte Durchdringung von Wänden/abschirmenden Materialien

Ausbreitung der Funkwellen

- die physikalische Ausrichtung der Antenne kann Auswirkungen auf die Sendeleistung haben
- Richtantennen können eine höhere Distanzüberbrücken
- ansonsten breiten sich Funksignale im Wellen um die Spitze der Antenne aus

Hindernisse

- Decken/Wände/Fenster durch verbautes Metall
- Mikrowellenstrahlen
- Metall führt dazu, dass Magnet- bzw. elektrische Felder entstehen, die das WLAN hemmen

Heatmap

- grafische Darstellung der Signalabdeckung/Signalqualität eines WLAN-Netzwerks
- gut abgedeckte Bereiche werden mit grünen Bereichen, schlechte abgedeckte Bereiche mit roten Bereichen dargestellt
- eine Heatmap kann durch Messung erstellt werden

Signalstärke

- ist eine physikalische Größe

- wird in dBm (Dezibel-Miliwatt) angegeben
- die Signalstärke ist beim Empfänger immer geringer als beim Sender
- wird aus Sicht des Empfängers mit Werten unter 0 beschrieben
    - sehr gut: -30 bis -50 dBM
    - gut: -50 bis -60 dBm
    - ausreichend: -60 bis -70 dBm
    - schlecht: < -70 dBm
- die **Strahlungsleistung** wird in mW (Miliwatt) angegeben
- je höher die Strahlungsleistung einer Antenne, desto höher die Reichweite des WLAN-Signals
- gesetzliche Maximalwerte:
    - 2,4 GHz: 100 mW ~ 20 dBm
    - 5 GHz: zw. 200 ~ 23 dBm und 1000 mW ~ 30 dBm
- !! Formeln zur Umrechnung von dbm <-> mW

Sendeleistung

- logische Größe
- auch Datenrate genannt
- beschreibt die Geschwindigkeit mit der Daten übertragen werden
- Formel: Sendeleistung = Datenmenge / Zeit
- wird üblicherweise in bit/s angegeben
- die Sendeleistung eines Access Points ist unter anderem abhängig vom genutzen WLAN-Standard (sowohl Client als auch Access Point müssen den gleichen Standard unterstützen)

MIMO

- Drahtlose Datenübertragungstechnik, bei der die Übertragung über mehrere Frequenzbänder gleichzeitig erfolgt
- Mehrere Sendeantennen sind paarweise am Gerät angebracht (2x2, 3x3, 4x4)
- Jede Antennne empfängt und sendet gleichzeitig
- Verbessert die Datenübertragungsrate und verringert die Fehleranfälligkeit

Anmeldeverfahren

- z. B. über Protected Extensible Authentication Protocol (PEAP), eine sicherere Variante des Authentifizierungsframeworks EAP
- ermöglicht Anmeldung im WLAN über Benutzername und Passwort (wie bei uns im GSO)

Sicherheitsstandards

- alt: WEP
- WPA1 und WPA2
- ab WiFi 6 und 7: WPA3

AAA-Sicherheit

- *Autentification*: Benutzer stellt Infromationen bereit, wer er ist (Passwort/Benutzername), ein Identity Access Manager überprüft diese
- *Authorization*: Vergebung von Rechten an Benutzer
- *Accounting*: Überwachung der Benutzer während sie im Netzwerk angemeldet sind und sammelt benötigte Daten

VIVA-Prinzipg (auch CIA)

- *Vertraulichkeit/Confidentiality*: Daten dürfen nur berechtigen Personen zugänglich sein
- *Integrität/Integrity*: Daten dürfen nicht manipuliert worden sein (bspw. bei Übertragung)
- *Verfügbarkeit/Availability*: Daten müssen zu definierten Zeiten verfügbar und durch Backups gesichert sein
- *Authentizität/Authenticity*: Daten müssen aus einer glaubwürdigen Quelle stammen

Weitere Sicherheitskonzepte

- schriftliche Nutzerordnung, die festlegt wofür das Netz genutzt werden darf. Nutzende müssen ihr zustimmen, um das Netz benutzen zu können
- Zertifikate: WLAN-Netze können über Zertifikate ihre Echtheit sicherstellen --> Schutz vor Evil-Twin-Angriffen

Berechnung von Datenübertragungsrate und Übertragungsdauer

Subnetting

- Subnetz: Eingrenzung eines Netzwerks auf OSI-Schicht 3
- Nur Teilnehmer, die in einem gemeinsamen IP-Subnetz sind, können direkt miteinander kommunizieren
- Um Außerhalb eines Subnetztes zu kommunizieren, ist ein Gateway nötig
- Die Subnetzmaske gibt an, welcher Teil einer IP-Adresse zum Netzwerkteil gehört und welcher Teil die Hosts eines Netzwerks bestimmt
- Sie besteht immer aus einer Reihe von 1 gefolgt von 0.
- Beispiel: 255.255.0.0 => 11111111.11111111.00000000.00000000
- Mithilfe der CIDR-Notation kann die Subnetzmaske verkürzt hinter der IP-Adresse angegeben werden, bspw. 192.168.2.2 /24 (Menge an 1en der Subnetzmaske --> 255.255.255.0)

Aufteilung eines IP-Adressbereichs in Subnetze

- Dies geschieht mithilfe der Subnetzmaske, s. o.

Bestimmung der notwendigen Bitanzahl für Subnetze und Hosts

Beispiel:

- 10 Subnetze
- 100 Hosts pro Subnetz
- 10 Subnetze benötigen eine 4 bit Binärzahl
- 100 Hosts benötigen min. eine 7 bit Binärzahl

--> Netzwerkanteil muss mindestens 4 bit groß sein --> Hostanteil muss mindestens 7 bit Groß sein.

Netzwerkadresse

- Adresse eines Netzwerks, wo im Hostanteil der Adresse nur 0 stehen. (erste vergebbare Adresse in einem Subnetz)
- Identifiziert das Netzwerk

Broadcastadresse

- Adresse eines Netzwerkes, wo im Hostbereich nur 1 stehen (letzte vergebbare Adresse in einem Subnetz)
- Wenn an alle Teilnehmer eines Netzwerks gesendet werden soll, muss an diese Adresse gesendet werden

Subnetzmasken auf Oktettgrenze

- 10 Subnetze --> 4 bit
- 100 Hosts pro Subnetz --> 7 bit

Beispiel:

- Ausgangsadressbereich: 192.168.0.0 bis 192.168.255.255

Subnetzmaske auf Oktettgrenze: 255.255.255.0 --> 3. Oktett = Netzwerkanteil, 4. Oktett = Hostanteil

Adressverteilung:

	Netzwerkadresse	**Hostadressen**	**Broadcastadresse**
Spiel1	192.168.0.0	192.168.0.1 bis 192.168.0.254	192.168.0.255
...			
Spiel 100	192.168.99.0	192.168.99.1 bis 192.168.99.254	192.168.99.255

OSI-7-Schichtenmodell

Schichten 1-4 (Begriffe, Header- und Trailergröße, Adressierungen, Aufgaben der Schichten)

1. Schicht (Physical Layer / Bitübertragungsschicht)

- Aufgabe: Herstellen einer physikalischen Verbindung zwischen Clients und Aufbau eines Netzwerks
- Datenübertragung über physikalisches Medium --> Umwandlung von Binärcode (0 und 1) in physikalische Signale (bspw. Spannungpegel)

- Physikalische Regelung der Kommunikation (Richtung, Gleichzeitigkeit, Geschwindigkeit)

2. Schicht (Data Link Layer / Sicherungsschicht)

- Datentyp: Frame
- Aufgabe: Bilden von Frames und Anreichern/Verarbeiten von Informationen zur logischen Weiterleitung in einem Netzwerk
- wichtig: MAC(Media Access Control)-Adress
- Frame besteht aus:
    - Präambel (8 Byte),
    - **Frame-Header** (14 Byte):
        - Zieladresse (6 Byte)
        - Empfängeradresse (6 Byte)
        - Typfeld (2 Byte)
    - Payload/Datenbereich (min. 46 Byte bis zu 1.500 Byte)
    - **Frame-Trailer** (4 Byte)
- Über den Frame-Trailer wird eine per CRC-Verfahren eine sogenannte Frame Check Sequence gebildet, die die Korrektheit der Daten sicherstellt
- Layer 2 Geräte (bspw. Switches) können Daten des Headers und Trailers auslesen und verarbeiten
- Switches sind lernfähig und können über Broadcast-Sendungen die MAC-Adressen an ihren angeschlossenen Ports ermitteln

3. Schicht (Network Layer / Vermittlungsschicht)

- Datentyp: Paket
- Aufgabe: Routing und Verarbeitung von IP-Paketen
- das IP-Paket befindet sich in der Payload des Frames
- IP-Header: min. 20 Byte bis zu 60 Byte groß (40 Byte optionale Daten)
    - enthält Daten wie Sender- und Empfänger-IP-Adresse, IP-Version, Flags oder Fragment-Offsets

4. Schicht (Transport Layer / Transportschicht)

- Datentyp: Segment
- Aufgabe: sichere und vollständige Zustellung der IP-Pakete
- zwei Protokolle: TCP und UDP
- TCP:
    - Header: Informationen zu Quell- und Ziel-TCP-Port (bspw. 80 für HTTP)
    - Datenbereich: enthält jetzt die Daten, die übertragen werden sollen
    - Sequenznummer: kommen Daten nicht in der richtigen Reihenfolge an, können sie hierüber wieder zusammengesetzt werden
    - 3-Way-Handshake stellt einen sicheren Verbindungsaufbau zum Empfänger sicher
- UDP:
    - "send and forget" - erwartet keine Bestätigung vom Empfänger
    - schneller, aber fehleranfälliger
    - wird verwendet, wenn Übertragungsgeschwindigkeit wichtig ist
- Firewall: kontrolliert was über welche Ports eindringen darf

Switche (Funktionsweise)

- Switche sind lernfähig und können den Frame-Header auslesen.
- Anhand der Daten, die im Frame-Header stehen (Sender-Adresse), füllen Switche ihre MAC-Adresstabellen und ...
    - ... leiten Pakete aus den richtigen Ports, wenn sie die Empfänger-MAC-Adresse kennen
    - ... oder leiten den Frame aus allen Ports heraus
    - ist ein Empfänger identifizierbar, verarbeitet dieser den Frame, alle anderen falschen Empfänger verwerfen ihn

Begriffe:

- Store and Forward: Um Überlastung zu Vermeiden und zur Prüfung kann der Switch einen Frame Zwischenspeichern
- Buffer Memory: Speicher, der Store and Forwarding erlaubt
- Switching Capacity: Interne Geschwindigkeit mit der der Switch Frames bearbeitet (Geschwindigkeit: Geschwindikeit der Ports * Anzahl der Ports * 2)
- Packet Forwarding Rate: Maximale Anzahl an Paketen, die ein Switch verarbeiten kann (Einheit: Packets Per Second)
- Auto Negotiation: automatische Ermittlung und anpassung von Link-Speed, Datenrate und Duplexart der angeschlossenen Geräte
- MDI/MDI-X: Unterstützung von normalen sowie auch Crossover-Netzwerkkabel
- SFP/SFP+-Kombiports: Small Form Factor Pluggable-Ports, die es erlauben Module anzuschließen, die auch andere Netzwerktechnik (bspw. Glasfaser) unterstützen