

IT Netzwerke

Agenda

- 1 Netzwerk Definition

- 2 OSI-Schichtenmodell

- 3 Client-Server-Netzwerkmodell

- 4 IP-Adressen und CIDR

- 5 Domains

Netzwerk Definition

- Netzwerk: Ein Netzwerk besteht aus zwei oder mehr Computern oder Geräten, die miteinander verbunden sind, um Ressourcen wie Daten, Dateien oder Internetzugang gemeinsam zu nutzen.

Hauptkomponenten eines Netzwerks

- Knoten (Nodes): Computer, Server, Drucker oder andere Geräte
- Netzwerkgeräte: Router, Switcher, Hubs
- Übertragungsmedien: Kabel (Kupfer, Glasfaser), Funk (WLAN)
- Protokolle: Regeln zur Kommunikation zwischen Geräten (TCP/IP, HTTP, FTP)

Endgeräte (Hosts)

- Computer (Desktop, Laptop)
- Mobile Geräte (Smartphone, Tablets)
- Server (Datenbanken, Webserver)
- Endgeräte sind die Geräte, die Daten im Netzwerk erzeugen, senden und empfangen. Sie sind die "Knoten" eines Netzwerks und stellen die Verbindungen zu anderen Geräten her.

Netzwerkgeräte

- Netzwerkgeräte sind für die Vermittlung, Leitung und Verwaltung des Datenverkehrs im Netzwerk verantwortlich.
- Router
 - ◆ Verbindet Netzwerke und leitet den Datenverkehr zwischen verschiedenen Netzwerken.
 - ◆ Arbeitet auf der Netzwerkschicht (Schicht 3 des OSI-Modells).
 - ◆ Entscheidet anhand von IP-Adressen, welcher Weg für die Daten am besten geeignet ist.

Netzwerkgeräte

- Netzwerkgeräte sind für die Vermittlung, Leitung und Verwaltung des Datenverkehrs im Netzwerk verantwortlich.
- Switch
 - ◆ Verbindet mehrere Endgeräte innerhalb eines lokalen Netzwerks (LAN).
 - ◆ Arbeitet auf der Sicherungsschicht (Schicht 2 des OSI-Modells).
 - ◆ Leitet den Datenverkehr basierend auf MAC-Adressen.

Netzwerkgeräte

- Netzwerkgeräte sind für die Vermittlung, Leitung und Verwaltung des Datenverkehrs im Netzwerk verantwortlich.
- Access Point (WLAN Access Point)
 - ◆ Bietet drahtlosen Geräten Zugang zu einem kabelgebundenen Netzwerk.
 - ◆ Arbeitet als Brücke zwischen drahtlosen Geräten und kabelgebundenen Netzwerken.

Übertragungsmedien

- Das Medium, durch das Daten zwischen den Geräten übertragen werden. Es kann entweder kabelgebunden oder drahtlos sein.
- Kabelgebundene Medien
 - ◆ Twisted Pair Kabel (z. B. Ethernet-Kabel, Cat5/Cat6): Am häufigsten verwendetes kabelgebundenes Medium für LANs.
 - ◆ Koaxialkabel: Verwendet in älteren Netzwerken oder für Breitband-Internet.
 - ◆ Glasfaserkabel: Ermöglicht die Übertragung von Daten mit hoher Geschwindigkeit über große Entfernungen.

Übertragungsmedien

- Das Medium, durch das Daten zwischen den Geräten übertragen werden. Es kann entweder kabelgebunden oder drahtlos sein.
- Drahtlose Medien
 - ◆ WLAN (Wi-Fi): Drahtlose Verbindungstechnologie, die Funkwellen nutzt.
 - ◆ Bluetooth: Für Kurzstrecken-Datenübertragung zwischen Geräten.
 - ◆ Satellit: Für sehr weite Distanzen, z. B. in abgelegenen Regionen oder für globale Kommunikationssysteme.

Netzwerkprotokolle

- Regeln, die den Datenfluss in einem Netzwerk definieren. Sie bestimmen, wie Daten gesendet, empfangen und interpretiert werden
- Hauptkategorien:
 - ◆ Kommunikationsprotokolle: Definieren den Austausch von Nachrichten zwischen Endgeräten.
 - ◆ Sicherheitsprotokolle: Schützen die Datenintegrität und sorgen für Vertraulichkeit.
 - ◆ Routing-Protokolle: Leiten den Datenverkehr durch das Netzwerk.

Kommunikationsprotokolle

→ TCP (Transmission Control Protocol)

- ◆ Verwendung: Verbindungsorientiertes Protokoll, das in den meisten Internetdiensten verwendet wird, z. B. HTTP, FTP, E-Mail.
- ◆ Merkmale:
 - Stellt sicher, dass die Daten korrekt und vollständig beim Empfänger ankommen.
 - Verwendet eine Sequenznummer, um Datenpakete in der richtigen Reihenfolge zu setzen.
 - Bestätigt den Empfang von Datenpaketen.

Kommunikationsprotokolle

→ UDP (User Datagram Protocol)

- ◆ Verwendung: Verbindungslose Datenübertragung, oft verwendet in Echtzeitanwendungen wie Video-Streaming oder Online-Gaming.
- ◆ Merkmale:
 - Geringe Latenz, aber keine Garantie für die Zustellung von Datenpaketen.
 - Keine Paketwiederherstellung bei Verlust.

Kommunikationsprotokolle

→ HTTP (Hypertext Transfer Protocol)

- ◆ Verwendung: Überträgt Webseiten und Daten im World Wide Web.
- ◆ Merkmale:
 - Ein Protokoll der Anwendungsschicht, das auf TCP basiert.
 - Definiert, wie Nachrichten formatiert und übertragen werden.
 - HTTPS ist die sichere Version von HTTP, die durch SSL/TLS verschlüsselt wird.

Kommunikationsprotokolle

→ FTP (File Transfer Protocol)

- ◆ Verwendung: Überträgt Dateien zwischen Client und Server.
- ◆ Merkmale:
 - Ermöglicht die Übertragung großer Dateien.
 - Unterstützt Dateioperationen wie Hochladen, Herunterladen, Umbenennen und Löschen von Dateien.

Kommunikationsprotokolle

→ SMTP (Simple Mail Transfer Protocol)

- ◆ Verwendung: Versand von E-Mails über das Internet.
- ◆ Merkmale:
 - Funktioniert auf der Anwendungsschicht.
 - Leitet E-Mails vom Absender an den Empfänger-Server weiter.

Sicherheitsprotokolle

→ TLS (Transport Layer Security) / SSL (Secure Sockets Layer)

- ◆ Verwendung: Verschlüsselung von Datenübertragungen, um die Vertraulichkeit und Integrität zu gewährleisten.
- ◆ Merkmale:
 - Verwendet symmetrische Verschlüsselung für den Datenaustausch und asymmetrische Verschlüsselung für die Schlüsselverteilung.
 - Wird häufig für HTTPS (sichere Webverbindungen) verwendet.

Sicherheitsprotokolle

→ IPSec (Internet Protocol Security)

- ◆ Verwendung: Sicherung der IP-Kommunikation durch Verschlüsselung und Authentifizierung.
- ◆ Merkmale:
 - Arbeitet auf der Netzwerkschicht.
 - Schützt Datenpakete auf Netzwerkebene, indem es den Inhalt verschlüsselt und die Integrität der Pakete sicherstellt.

Sicherheitsprotokolle

→ SSH (Secure Shell)

- ◆ Verwendung: Sicherer Fernzugriff auf Geräte, häufig für die Verwaltung von Servern.
- ◆ Merkmale:
 - Verschlüsselt die Kommunikation zwischen zwei Computern.
 - Unterstützt passwortlose Anmeldung über öffentliche und private Schlüssel

Sicherheitsprotokolle

→ HTTPS (Hypertext Transfer Protocol Secure)

- ◆ Verwendung: Sichere Version des HTTP-Protokolls, das TLS/SSL für die Verschlüsselung verwendet.
- ◆ Merkmale:
 - Sicherer Zugriff auf Webseiten durch Verschlüsselung des Datenverkehrs.
 - Schützt sensible Daten wie Passwörter, Kreditkarteninformationen usw.

Vorteile von Netzwerken

- Daten- und Ressourcenfreigabe: Gemeinsame Nutzung von Dateien, Anwendungen und Geräten (z.B. Drucker)
- Kommunikation: Ermöglicht schnelle Kommunikation zwischen Benutzern
- Zentrale Verwaltung: Verwaltung von Sicherheitsrichtlinien und Benutzern über das Netzwerk

OSI-Schichtenmodell

- OSI (Open Systems Interconnection) Modell: Ein konzeptionelles Modell, das beschreibt, wie Daten zwischen Netzwerkkomponenten übertragen werden. Es besteht aus 7 Schichten.
- ◆ Schicht 1 – Physikalische Schicht (Physical Layer): Überträgt binäre Daten über physische Medien (z. B. Kabel, Funkwellen).
 - ◆ Schicht 2 – Sicherungsschicht (Data Link Layer): Verarbeitet die physikalische Adressierung (z. B. MAC-Adressen) und sorgt für fehlerfreie Übertragung zwischen Geräten.
 - ◆ Schicht 3 – Netzwerkschicht (Network Layer): Bestimmt den Pfad der Daten durch das Netzwerk (z. B. Routing, IP-Adressen).
 - ◆ Schicht 4 – Transportschicht (Transport Layer): Gewährleistet die zuverlässige Datenübertragung (z. B. TCP/UDP-Protokolle).
 - ◆ Schicht 5 – Sitzungsschicht (Session Layer): Verwalten von Sitzungen zwischen Anwendungen.
 - ◆ Schicht 6 – Darstellungsschicht (Presentation Layer): Datenumwandlung und -verschlüsselung (z. B. JPEG, SSL).
 - ◆ Schicht 7 – Anwendungsschicht (Application Layer): Schnittstelle zu Anwendungen und Diensten (z. B. HTTP, FTP).

Client-Server-Netzwerkmodell

- Client-Server-Modell: Ein Modell, bei dem mehrere Clients (Endbenutzergeräte) über ein Netzwerk mit einem zentralen Server verbunden sind, der Dienste bereitstellt.
- Hauptmerkmale:
 - ◆ Client: Fordert Dienste vom Server an (z. B. Datei-Download, Datenbankabfrage).
 - ◆ Server: Beantwortet Client-Anfragen und stellt Ressourcen bereit (z. B. Webserver, Datenbankserver).
- Beispiel: Webserver
 - ◆ Client: Der Webbrowser eines Benutzers.
 - ◆ Server: Der Webserver, der eine Website hostet.
 - ◆ Kommunikation: Über das HTTP-Protokoll.
- Vorteile des Client-Server-Modells:
 - ◆ Zentrale Verwaltung: Daten und Anwendungen werden zentral auf dem Server gespeichert und verwaltet.
 - ◆ Sicherheit: Zentrale Kontrolle ermöglicht besseren Schutz und Sicherheit.
 - ◆ Skalierbarkeit: Es ist einfach, neue Clients hinzuzufügen.

Andere Netzwerkarchitekturen

- Peer-to-Peer (P2P): Jeder Knoten agiert sowohl als Client als auch als Server (z. B. Torrents).
- Hybride Netzwerke: Kombination aus Client-Server und Peer-to-Peer-Modellen.

IP-Adressen

- Eine IP-Adresse (Internet Protocol Address) ist eine eindeutige numerische Kennung, die jedem Gerät in einem Netzwerk zugewiesen wird, das das Internet Protocol (IP) verwendet. IP-Adressen dienen dazu, Geräte zu identifizieren und die Zustellung von Datenpaketen zu ermöglichen.

Klassen von IP-Adressen

- Klasse A
 - ◆ Bereich: 0.0.0.0 bis 127.255.255.255
 - ◆ Netzwerk/Host-Aufteilung: Die ersten 8 Bits sind der Netzwerkanteil, die restlichen 24 Bits der Hostanteil.
 - ◆ Verwendung: Große Netzwerke mit bis zu 16 Millionen Hosts.
 - ◆ Beispiel: 10.0.0.0
- Klasse B:
 - ◆ Bereich: 128.0.0.0 bis 191.255.255.255
 - ◆ Netzwerk/Host-Aufteilung: Die ersten 16 Bits sind der Netzwerkanteil, die restlichen 16 Bits der Hostanteil.
 - ◆ Verwendung: Mittlere Netzwerke mit bis zu 65.536 Hosts.
 - ◆ Beispiel: 172.16.0.0
- Klasse C:
 - ◆ Bereich: 192.0.0.0 bis 223.255.255.255
 - ◆ Netzwerk/Host-Aufteilung: Die ersten 24 Bits sind der Netzwerkanteil, die restlichen 8 Bits der Hostanteil.
 - ◆ Verwendung: Kleine Netzwerke mit bis zu 254 Hosts.
 - ◆ Beispiel: 192.168.0.0
- Klasse D:
 - ◆ Bereich: 224.0.0.0 bis 239.255.255.255
 - ◆ Verwendung: Reserviert für Multicast-Gruppen (Daten an eine Gruppe von Hosts senden).
- Klasse E:
 - ◆ Bereich: 240.0.0.0 bis 255.255.255.255
 - ◆ Verwendung: Reserviert für experimentelle Zwecke.

IP-Adressen

→ Zwei Hauptversionen von IP-Adressen:

- ◆ IPv4: 32-Bit-Adressschema, das aus vier Oktetten besteht, die durch Punkte getrennt sind.
 - Beispiel: 192.168.1.1
 - Theoretisch gibt es etwa 4,3 Milliarden mögliche IPv4-Adressen.
- ◆ IPv6: 128-Bit-Adressschema, entwickelt, um das Problem der IPv4-Adressenerschöpfung zu lösen.
 - Beispiel: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 - Bietet theoretisch etwa 340 Undezillionen (3.4×10^{38}) mögliche Adressen.

→ Aufbau einer IPv4-Adresse:

- ◆ Hostanteil und Netzwerkanteil: Eine IP-Adresse besteht aus zwei Teilen:
- ◆ Netzwerkanteil: Gibt das Netzwerk an, zu dem das Gerät gehört.
- ◆ Hostanteil: Identifiziert das spezifische Gerät im Netzwerk.

Private IP-Adressen

- Klasse A: 10.0.0.0 bis 10.255.255.255
- Klasse B: 172.16.0.0 bis 172.31.255.255
- Klasse C: 192.168.0.0 bis 192.168.255.255
- Private IP-Adressen werden in lokalen Netzwerken verwendet und sind im öffentlichen Internet nicht routbar.

Mein Rechner hat welche IP-Adresse?

- Geräte im Heimnetzwerk bekommen eine private IP zugeordnet (Abfrage über ip a oder ipconfig) über DHCP vom Router
- Router hat eine öffentliche IP-Adresse vom Internetanbieter und NAT (Network Address Translation). NAT sorgt dafür, dass Datenverkehr von der privaten IP-Adresse vom lokalen Netzwerk ins Internet geroutet wird und Antworten wieder korrekt ankommen
- Unser Rechner ist von außen erstmal nicht erreichbar (nur private IP-Adresse). Um ihn erreichbar zu machen, brauchen wir ein Port-Forwarding, bei dem der Router Anfragen an den Rechner weiterleitet (oder VPN)
 - ◆ Wir haben einen Webserver auf dem Rechner. Wir könnten den Router so konfigurieren, dass er Anfragen auf Port 80 an den Webserver weiterleitet.

Meine VM hat welche IP-Adresse?

- Eine VM in einem lokalen Netzwerk erhält eine private IP-Adresse (genauso wie bei physischen Geräten im Netzwerk)
- Je nach Konfiguration der VM (NAT oder Bridge-Modus) kann VM eine IP vom Host oder direkt vom Router erhalten
 - ◆ NAT: VM erhält ihre IP vom Host-Rechner und ist für andere Geräte im Netzwerk nicht direkt sichtbar
 - ◆ Bridge-Modus: VM erhält eine IP vom Router und verhält sich wie ein eigenständiges Gerät im Netzwerk

Was macht also ein Router?

- Vergabe privater IP-Adressen: Der Router vergibt in einem Heimnetzwerk private IP-Adressen an Geräte (PCs, Smartphones, etc.).
- NAT (Network Address Translation): Der Router hat eine öffentliche IP-Adresse, die ihm vom Internetanbieter zugewiesen wird. Über NAT sorgt der Router dafür, dass Datenverkehr von den privaten IP-Adressen im lokalen Netzwerk ins Internet geroutet wird und die Antworten wieder an das richtige Gerät im lokalen Netzwerk zurückkommen.

Subnetting

- Wollen Netze bauen
- Direkte Kommunikation zwischen Abteilungen
- Mehr Sicherheit bei Angriffen

Subnetzmasken

- Eine Subnetzmaske teilt eine IP-Adresse in einen Netzwerk- und einen Hostanteil auf. Sie wird verwendet, um zu bestimmen, zu welchem Netzwerk eine IP-Adresse gehört.
- ◆ Beispiel einer Subnetzmaske: 255.255.255.0
 - ◆ Diese Subnetzmaske bedeutet, dass die ersten 24 Bits der IP-Adresse den Netzwerkanteil darstellen und die letzten 8 Bits für den Hostanteil reserviert sind.

CIDR

- CIDR ist eine Methode zur flexiblen Unterteilung und Adressierung von IP-Adressen. Anstelle von festen Klassen (A, B, C) ermöglicht CIDR die Verwendung von beliebigen Subnetzmasken, um Netzwerke in kleinere Subnetze zu unterteilen.
- ◆ CIDR-Notation: IP-Adresse gefolgt von einem Schrägstrich und der Anzahl der Bits, die für den Netzwerkanteil verwendet werden.
 - ◆ Beispiel: 192.168.1.0/24
 - ◆ Die ersten 24 Bits stellen das Netzwerk dar, die letzten 8 Bits sind für Hosts verfügbar.

CIDR

→ Beispiel 1: Netzmaske /24

- ◆ CIDR-Notation: 192.168.1.0/24
- ◆ Netzwerkanteil: 24 Bits (also die ersten 3 Oktette)
- ◆ Hostanteil: 8 Bits (letztes Oktett)
- ◆ Anzahl möglicher Hosts: $2^8 - 2 = 254$ Hosts
- ◆ Die Formel lautet: $2^{(\text{Anzahl der Host-Bits})} - 2$ (abzüglich 2, da eine Adresse für das Netzwerk und eine für die Broadcast-Adresse verwendet wird).

→ Beispiel 2: Netzmaske /16

- ◆ CIDR-Notation: 172.16.0.0/16
- ◆ Netzwerkanteil: 16 Bits
- ◆ Hostanteil: 16 Bits
- ◆ Anzahl möglicher Hosts: $2^{16} - 2 = 65.534$ Hosts

→ Beispiel 3: Netzmaske /30 (für Punkt-zu-Punkt-Verbindungen)

- ◆ CIDR-Notation: 192.168.1.0/30
- ◆ Netzwerkanteil: 30 Bits
- ◆ Hostanteil: 2 Bits
- ◆ Anzahl möglicher Hosts: $2^2 - 2 = 2$ Hosts
- ◆ Wird häufig für Punkt-zu-Punkt-Verbindungen verwendet, da nur zwei Hosts verbunden werden müssen.

CIDR

- Die Subnetzmaske kann auch in der CIDR-Notation dargestellt werden, indem man angibt, wie viele Bits für den Netzwerkanteil verwendet werden.
- CIDR und Subnetzmaske:
 - ◆ /8: 255.0.0.0 (Klasse A)
 - ◆ /16: 255.255.0.0 (Klasse B)
 - ◆ /24: 255.255.255.0 (Klasse C)
- Beispiel:
 - ◆ IP-Adresse: 192.168.1.0
 - ◆ Subnetzmaske: 255.255.255.0 oder /24
 - ◆ Bedeutet, dass die ersten 24 Bits der Adresse den Netzwerkanteil darstellen und die restlichen 8 Bits für Hosts verfügbar sind.

CIDR

→ Subnetzmaske /8 (Klasse A)

- ◆ Subnetzmaske: 255.0.0.0
 - In binär: 11111111.00000000.00000000.00000000
- ◆ Netzwerkanteil: Die ersten 8 Bits (1 Oktett) sind der Netzwerkanteil.
- ◆ Hostanteil: Die restlichen 24 Bits (3 Oktette) sind für Hosts verfügbar.
- ◆ Mögliche Hosts pro Netzwerk: $2^{24} - 2 = 16.777.214$

→ 2. Subnetzmaske /16 (Klasse B)

- ◆ Subnetzmaske: 255.255.0.0
 - In binär: 11111111.11111111.00000000.00000000
- ◆ Netzwerkanteil: Die ersten 16 Bits (2 Oktette) sind der Netzwerkanteil.
- ◆ Hostanteil: Die restlichen 16 Bits (2 Oktette) sind für Hosts verfügbar.
- ◆ Mögliche Hosts pro Netzwerk: $2^{16} - 2 = 65.534$

→ 3. Subnetzmaske /24 (Klasse C)

- ◆ Subnetzmaske: 255.255.255.0
 - In binär: 11111111.11111111.11111111.00000000
- ◆ Netzwerkanteil: Die ersten 24 Bits (3 Oktette) sind der Netzwerkanteil.
- ◆ Hostanteil: Die restlichen 8 Bits (1 Oktett) sind für Hosts verfügbar.
- ◆ Mögliche Hosts pro Netzwerk: $2^8 - 2 = 254$

Warum Subnetting?

- Effiziente IP-Nutzung: Subnetting ermöglicht es, den Adressraum effizienter zu nutzen, indem Adressen gezielt zugeteilt werden.
- Netzwerksegmentierung: Erhöht die Sicherheit und Leistung, indem Broadcast-Domänen getrennt werden.
- Leichtere Verwaltung: Kleinere Netzwerke sind leichter zu verwalten und zu überwachen.

Subnetting - Beispiel:

→ Ausgangs-IP-Bereich: 192.168.0.0/24

- ◆ Dies ist ein Standard-Subnetz, das Platz für 254 Hosts bietet.

→ Subnetting in kleinere Netzwerke:

- ◆ Wir können 192.168.0.0/24 in vier Subnetze aufteilen, indem wir die Subnetzmaske von /24 auf /26 ändern.

- ◆ Jedes Subnetz hat nun 64 Adressen ($2^6 - 2 = 62$ Hosts pro Subnetz).

→ Ergebnis:

- ◆ Subnetz 1: 192.168.0.0/26 (Hosts von 192.168.0.1 bis 192.168.0.62)

- ◆ Subnetz 2: 192.168.0.64/26 (Hosts von 192.168.0.65 bis 192.168.0.126)

- ◆ Subnetz 3: 192.168.0.128/26 (Hosts von 192.168.0.129 bis 192.168.0.190)

- ◆ Subnetz 4: 192.168.0.192/26 (Hosts von 192.168.0.193 bis 192.168.0.254)

Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = **11111111.11111111.11111111.00000000 = 255.255.255.0**
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also $11000000.10000000.00000000.00000000 \text{ AND } 11111111.11111111.11111111.00000000 = 11000000.10000000.00000000.00000000 = 192.128.0.0$ (Netzwerkanteil ist immer der Teil bis wohin die 1en gehen)
- Der Host-Anteil hat dann $2^{(32-(\text{Schrägerzahl}))}-2$ (hier $2^8 - 2 = 254$) viele Adressmöglichkeiten
 - ◆ 0 ist reserviert für Host
 - ◆ 255 ist reserviert für Broadcast-Adresse
 - ◆ Erste Möglichkeit wäre dann 192.128.0.1 usw.
- Was würde passieren wenn wir /10 als Subnetzmaske haben?

Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = **11111111.11111111.11111111.00000000 = 255.255.255.0**
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also $11000000.10000000.00000000.00000000 \text{ AND } 11111111.11111111.11111111.00000000 = 11000000.10000000.00000000.00000000 = 192.128.0.0$ (Netzwerkanteil ist immer der Teil bis wohin die 1en gehen)
- Der Host-Anteil hat dann $2^{(32-(\text{Schrägerzahl}))}-2$ (hier $2^8 - 2 = 254$) viele Adressmöglichkeiten
 - ◆ 0 ist reserviert für Host
 - ◆ 255 ist reserviert für Broadcast-Adresse
 - ◆ Erste Möglichkeit wäre dann 192.128.0.1 usw.
- Was würde passieren wenn wir /10 als Subnetzmaske haben?
 - ◆ Subnetzmaske → $11111111.11000000.00000000.00000000$ (255.192.0.0) && **$11000000.10000000.00000000.00000000 = 192.128.0.0$**
 - ◆ Anzahl der Hosts = $2^{(32-10)}-2 = 2^{10}-2 = 1022$

Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also
 $11000000.10000000.00000000.00000000 \text{ AND } 11111111.11111111.11111111.00000000 = 11000000.10000000.00000000.00000000 = 192.128.0.0$ (Netzwerkanteil ist immer der Teil bis wohin die 1en gehen)
- Der Host-Anteil hat dann $2^{(32-(\text{Schrägerzahl})) - 2}$ (hier $2^8 - 2 = 254$) viele Adressmöglichkeiten
 - ◆ 0 ist reserviert für Host
 - ◆ 255 ist reserviert für Broadcast-Adresse
 - ◆ Erste Möglichkeit wäre dann 192.128.0.1 usw.
- Wie teilen wir das nun auf?
 - ◆ Spendiere der Subnetzmaske noch 2 Einsen → Subnetzmaske ?
11111111.11111111.11111111.11000000 (255.255.255.192) ($2^2 = 4$ neue Netze spendieren..)



Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also

192.128.0.0/26

11000000.10000000.00000000.00111111

Subnetzadresse 192.128.0.0

Hostadressen 192.128.0.1 192.128.0.62

Broadcastadresse 192.128.0.63

00 HUMINT

192.128.0.0/26

HUMINT 00

10 OSINT

SIGINT 01

11 TECHINT

11111111.11111111.11111111.11000000

255. 255. 255. 192

Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also
11000000.10000000.00000000.00000000 AND 11111111.11111111.11111111.00000000
= 11000000.10000000.00000000.00000000 = 192.128.0.0 (Netzwerkanteil ist

→

→

→

192.128.0.0/26

11000000.10000000.00000000.01111111

Subnetzadresse 192.128.0.64

Hostadressen 192.128.0.65 192.128.0.126

Broadcastadresse 192.128.0.127

01 SIGINT

192.128.0.0/26

HUMINT 00

10 OSINT

SIGINT 01

11 TECHINT

11111111.11111111.11111111.11000000

255. 255. 255. 192


Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.
- Für Bestimmung des Netzanteils wird IP-Adresse des Netzwerks mit der Subnetzmaske mit AND-Operator verknüpft. Also

192.128.0.0/26

11000000.10000000.00000000.10111111

Subnetzadresse	192.128.0.128
Hostadressen	192.128.0.129 192.128.0.190
Broadcastadresse	192.128.0.191



192.128.0.0/26

**HUMINT 00**

**10 OSINT**

**SIGINT 01**



**11 TECHINT**

11111111.11111111.11111111.11000000

255. 255. 255. 192

Subnetting - Beispiel:

- Ausgangssituation: NSA hat 4 Teilbereiche HUMINT, SIGINT, OSINT und TECHINT
- Netzwerk hat IP-Adresse 192.128.0.0/24 → Subnetzmaske 24. Diese teilt Adresse in Netzanteil und Hostanteil auf. 24 = 1111111.1111111.1111111.00000000 = 255.255.255.0
- Netzanteil für die verschiedenen Bereiche und Hostanteil für die jeweiligen Endgeräte in den Bereichen.

192.128.0.0/26

11000000.10000000.00000000.11111111

Subnetzadresse	192.128.0.192
Hostadressen	192.128.0.193 192.128.0.254
Broadcastadresse	192.128.0.255

11 TECHINT

192.128.0.0/26

HUMINT 00

10 OSINT

SIGINT 01

11 TECHINT

11111111.11111111.11111111.11000000

255. 255. 255. 192

