Zusammenfassung Computernetzwerk

Inhalt

[1 3.Layer – Vermittlungsschicht 1](#_Toc433285354)

[1.1 Adressen 1](#_Toc433285355)

[1.1.1 Adressklassen 1](#_Toc433285356)

[1.2 Subnetze 1](#_Toc433285357)

[1.3 Segmentierung der Netze – Die Netzmaske 2](#_Toc433285358)

# 3.Layer – Vermittlungsschicht

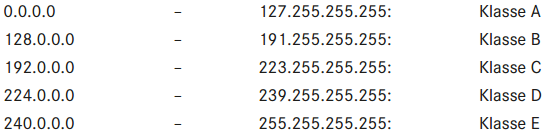
Kommunikation zwischen verschiedenen Netzwerken

## Adressen

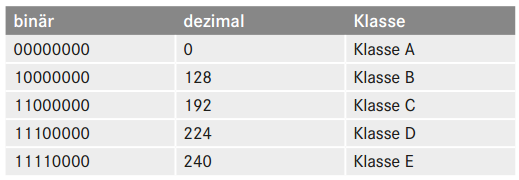
In Layer 3 gelten andere Adressen als in Layer 2 (physische Adressen, MAC-Adressen). Durchgesetzt hat sich das IP-Adressierungssystem. IP-Adressen sind weltweit gültig und werden deshalb zentral verwaltet. Die Koordination dabei übernimmt IANA – Internet Assigned Numbers Authority.

### Adressklassen

Man unterscheidet zwischen fünf Klassen von Adressen. Grosser Unterschied zwischen ihnen ist die Anzahl Hosts, welche adressiert werden können -> Grösse der möglichen Netze.



Die Aufteilung der Klassen ergibt sich aus dem ersten Byte.

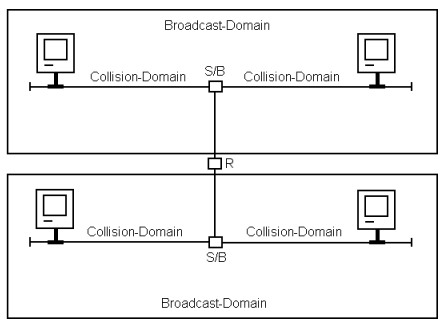


Den fixen, nicht veränderbaren Teil der IP-Adresse, nennt man Netzwerkteil



## Subnetze

Alle 65536 Hosts einer B-Klasse Adresse auf Layer 1 oder 2 zu kommunizieren zu lassen, macht keinen Sinn. Alleine die Rundsendungen (Broadcasts) würden das Netzwerk zum Erliegen bringen. Deshalb unterteilt man die Netze in so genannte Subnetze.



|  |  |
| --- | --- |
| **1.Layer** | Hubs und Mediumkonverter |
| **2.Layer** | Switches und Bridges -> Trennen Kollisionsdomänen |
| **3.Layer** | Router -> trennen Broadcast-Domänen |

Die Kommunikation erfolgt innerhalb von Broadcastdomänen auf Layer 2, zwischen ihnen auf Layer.

**Spezielle Adressen**

In Subnetzen gibt es auf Layer 3 (IP) fest reservierte Adressen, die keinem Host zugewiesen werden dürfen. Das sind:

|  |  |
| --- | --- |
| **Subnetzadresse** | Die kleinste Verfügbare Adresse ist die Bezeichnung des Subnetzes. |
| **Broadcast-Adresse** | Die grösste Verfügbare Adresse ist für die Rundspruchsendung.  Datenpakte für diese Adresse müssen von jedem Netzwerkgerät entgegen genommen werden. |

Wichtig: Durch die Segmentierung von Netzen gehen immer Minimum zwei Adressen für Endgeräte verloren. Beachtet man noch den benötigten Router für Netzwerk-Netzwerk Kommunikation, sind es sogar drei Adressen die „verloren“ gehen.

## Segmentierung der Netze – Die Netzmaske

Ein Router muss entscheiden können, zu welchem Teil eines Subnetzes welches Gerät gehört.

Ein Gerät möchte Daten an ein anderes Gerät schicken. Dafür muss es erst die Zieladresse auflösen. Innerhalb der Broadcast-Domäne (Layer 2) macht es deshalb einen Broadcast, einen ARP-Request. Ist die Zieladresse jedoch in einem anderen Netzwerk, macht ein ARP-Request keinen Sinn. Hier kommt die Netzmaske ins Spiel.

|  |  |
| --- | --- |
| **Sub-/Netzmaske** | Definiert den Host- und den Netzwerkteil der IP-Adresse. |

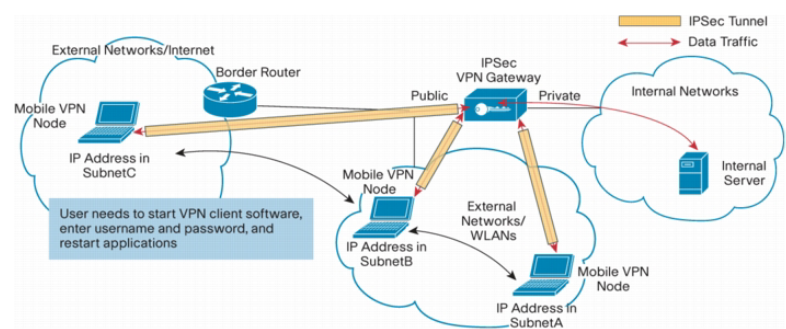
(Adressbereich der Klasse C: 220.1.10.0 hat 256 Adressen zur Verfügung. Der Administrator dieses Netzwerkes bemerkt, dass die Broadcasts zunehmen und das Netzwerk somit beeinträchtigen.

Lösung: Er segmentiert das Netz weiter in Subnetze.

Problem: Alle Router im Netzt müssen automatisch wissen, dass dies passiert ist.)

Beispiel

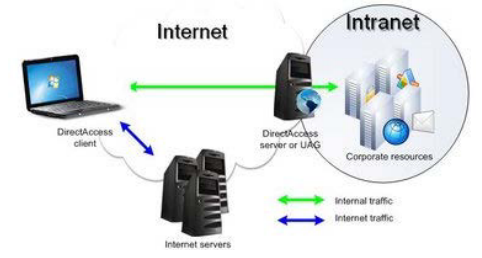
# VPN



VPN Gatewy (nicht Server) routet Subnetze A, B, C derClient.

Bei IP-Änderung bricht VPN-Verbindung zusammen.

## Split Tunnels



Diese geschossenen Tunnel verursachen viel Traffic.

Die Split Tunnels bieten Angriffspunkte für Angreifer aus dem Internet.

Der Client dient dabei als Hop-Node.

Als Gegenmassnahme ist nur eine Verbindung auf dem Client erlaubt.

## Verschlüsselung

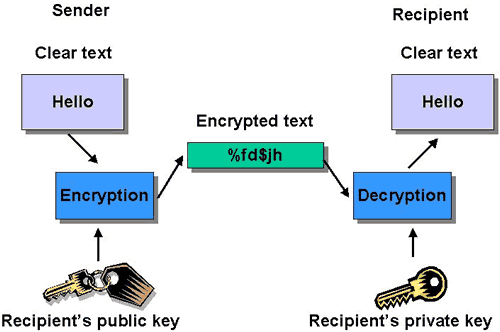
Verschüsselungsverfahren:

* DES
* 3DES
* IDEA
* AES -> aktueller Standard.

Symmetrisch:

Gleiche Schlüssel werden zum Verschlüsseln und Entschlüsseln verwendet. Problem dabei ist die Schlüsselverteilung, aso wir erhält mein Gegenüber den Schlüssel zur Entschlüsselung einer Nachricht auf sichere Art und Weise.

Asymmetrisch:



Mathematisch „verwandtes″ Schlüsselpaar (siehe Diffie-Helmann). Prinzip ist einfach, Nachrichten die mit dem öffentlichen Schlüssel verschlüsselt werden können nur mit dem Private-Key entschlüsselt werden. Verteilung des public Key ist daher unproblematisch, er kann veröffentlicht werden. Einzige Problematik ist die Frage der Authentizität (wirklich Bob’s Schlüssel?). Aus diesem Grund gibt es im Internet Certificate Authorities (CA).

Hybrid:

Mit asymmetrischem Verfahren einen symmetrischen Schlüssel für die gemeinsame Benutzung übertragen

Authentizität:

Sicherstellen, dass Gegenstelle authentisch ist, z.B. durch Prüfen der Kenntnis eines gemeinsamen Geheimnisses (PSK = Pre Shared Key)

Datenintegrität:

Den einzelnen Datenpaketen wird ein MAC (Message Authentication Code) angehängt, eine komplizierte Prüfzahl, die am Ziel erneut berechnet wird und den Originalwert ergeben muss. Ein HMAC kombiniert das Verfahren mit dem Hashwert eines gemeinsamen Geheimnisses (Authentizität)

## IPSec

IPSec kann in zwei verschienden Modis betrieben werden.

