TEM03 Zusammenfassung

Alexander Hauck

Wirtschaftsinformatik, Herbstsemester 2015

Inhalt

Geschichte von Netzwerken

- Zu Beginn: Lochkarten
- Terminalsysteme (Monitor + Tastatur) ohne Intelligenz wurden anschliessend an die Grossrechner angeschlossen.
- Mit der Entwicklung der PCs besitzten auch die eigenen Geräte genug Kapazität
- Da Drucker etc. sehr teuer waren, war die gemeinsame Nutzung von Ressourcen gefragt
- Dazu kamen dann noch Benutzerverwaltung, Datensicherung etc.

Netzwerk: Infrastruktur, die Datenendgeräten die Kommunikation, den Datenaustausch und die Nutzung gemeinsamer Ressourcen transparent ermöglicht.

- Transparent bedeutet dabei, dass sich der Nutzer nicht darum kümmern muss, WIE Informationen übertragen werden.
- Netzwerke verfolgen heute diverse Aufgaben, Ziele und Funktionen:
  - Datenverbund: gemeinsamer Zugriff auf Datenbestände
  - Funktionsverbund: gemeinsame Nutzung aufwändiger Datensicherungsverfahren, Webservices, Drucker
  - Verfügbarkeitsverbund: redundante Systeme (RAID, 2. Rechenzentrum)
  - Leistungsverbund: Parallele Verarbeitung
  - Lastverbund: Verteilen, Dispatching von Aufträgen

Das OSI Modell

- 1984 entwickelt durch die ISO
- Besteht aus sieben, jeweils in sich abgeschlossene Schichten (d.h. jede kann für sich weiterentwickelt werden)
- Sofern sich Hersteller an die Standards und die Schichtung halten, kann jeder den Layer nach seinen Vorstellungen implementieren; er bleibt weiterhin kommunikationsfähig.

Layer 7	Anwendungsschicht	Application	Verteilte Server-Client Lösungen, Kontroll- und User-Interfaces
Layer 6	Darstellungsschicht	Presentation	MPEG, TIFF, GIF etc.
Layer 5	Kommunikationsschicht	Session	„Serviceschicht“, SMB
Layer 4	Transportschicht	Transport	Kommunikation Netzwerk ←→Anwendung, TCP, UDP
Layer 3	Vermittlungsschicht	Netzwork	weltweite Adressierung, IP, Router
Layer 2	Sicherungsschicht	Data Link	Übertragung, Adressierung innerhalb eines Netzsegments (Hardwareadressen), Bridge, Switch
Layer 1	Physische Schicht*	Physical	Kabel, Anschlüsse, LAN, MAN, WAN, Repeater

Merksatz: Alle Priester saufen Tequila nach der Predigt.

***Achtung: Nicht physikalische!!**

- Kommunikation läuft von oben alle Layer nach unten und beim Empfänger wieder nach oben
- Dabei packt jede Schicht die Daten in ein zusätzliches Couvert
- Beim Auspacken öffnet die jeweilige Schicht nur ihr Couvert, der Rest interessiert sie nicht.

Layer I: Die Bitübertragungsschicht

- Definiert z.B. den Aufbau der Netzwerkkabel, die elektrischen Eckdaten, Spannungen, Frequenzen etc.
- Beinhaltet vor allem das Sichtbare eines Netzwerks

Thin-Wire Verkabelung (Koaxialkabel)

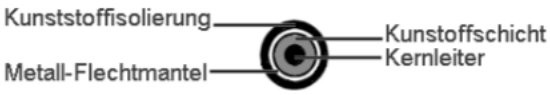


Bild 1: Aufbau des Koaxialkabels

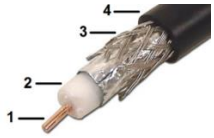


Bild 2 Aufbau

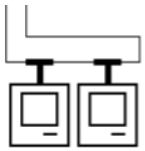


Bild 3 Verkabelung

- Lange und zuverlässig im Einsatz, hervorragende Abschirmung (Farady'scher Käfig).
- Allerdings keine hohen Übertragungsgeschwindigkeiten möglich (10 Mbit/s), Gefahr eines Totalausfalls des Netzwerks bei Fehlern. Deshalb heute bei Neuverkabelungen nicht mehr im Einsatz, ersetzt durch die Glasfaser.
- Die Kabel werden direkt an die Computer herangeführt (T-Stück); nicht benutzte Anschlussdosen müssen überbrückt werden. (siehe Bild 3)
- Zu beachten ist, dass die Kabel nicht zu stark gebogen werden. Dies führt zu Brüchen in der Ader der Schirmungsfolie mit gravierenden Auswirkungen auf die Performance bis hin zum Netzausfall, da der Wellenwiderstand beeinflusst wird und dadurch Reflexionen entstehen.
- An den beiden T-Stücken am Ende des Stranges müssen Widerstände aufgesetzt werden, welche genau den Widerstand des Mediums besitzen. Damit wird ein Signal zerstört. Wäre der Widerstand zu hoch, würde ein eintreffendes Signal reflektiert werden und sich selbst und andere Signale durch Überlagerung zerstören.

Die universelle Gebäudeverkabelung (UGV)

Bild 4: Western Modular Stecker

Bild 5: Twisted Pair, Typ S/UTP

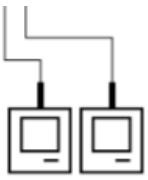


Bild 6: Verkabelung

- Ziel: Nur noch eine Sorte der Verkabelung mit dem höchsten Qualitätsstandard, um alle Dienste (Netzwerk, Telefonie, Fax) zu übertragen. Über die UGV ist es möglich, z.B. ISDN, Wechselsprechanlagen, Haustürklingeln etc. über diese Kabel zu führen und später zu variieren, welcher Dienst und welches Gerät wo angeschlossen ist.
- Heute: achtaderige Kabel und als Verbindung der Western-Modularstecker (siehe oben)
    - Vier der Kabel sind vom Netzwerk in Gebrauch. Es ist also möglich, mit speziell verkabelten Anschlussdosen zwei volle Geräteanschlüsse über ein Kabel zu erschliessen. Dies gilt jedoch nur bis 100 Mbit/s
    - Bei Gigabit-Ethernet wird heute mit allen acht adern gearbeitet
- Die Kabel sind verdrillt, deshalb der Name „Twisted Pair". Dadurch werden Störeinflüsse (elektromagnetische Abstrahlungen) minimiert. Dazu kommt, dass um jeden Leiter ein

Magnetfeld entsteht. Da die Kabel entgegengesetzt gerichtet sind, löschen sich diese jeweils gegenseitig aus.

- Es gibt verschiedene Kategorien, z.B. Unshielded Twisted Pair, Shielded/Shielded Twisted Pair (Adernpaar einzeln sowie das gesamte Kabel nochmal geschirmt).
- Übertragungsgeschwindigkeiten: 10 Mbit/s (Ethernet, kaum noch im Einsatz), 100 Mbit/s (Fast Ethernet, heutiger Standard). 1000 Mbit/s gewinnt immer mehr an Bedeutung.
- Verkabelung mittels Repeater, welche eingehende Signale verstärken, multiplizieren und durch alle anderen Ports wieder ausgeben.
- Maximal fünf Segmente mit vier Verstärken (hier die Repeater) in drei Kaskaden
- Nachteil gegenüber Koaxialverkabelung: Höherer Bedarf an Kabeln.
- Vorteile: bei einem Unterbruch ist nur das betroffene Endgerät vom Netzwerk isoliert und nicht alle. Nicht benutzte Anschlüsse müssen nicht überbrückt werden. Der Repeater erkennt, ob am Port ein Gerät angeschlossen ist oder nicht.
- Repeater müssen eine andere Pinbelegung der Stecker/Dosen besitzen als die Netzwerkadapter. Werden nun zwei Repeater direkt aneinander geschlossen, ist ein spezielles Kabel notwendig (Crossover-Kabel). Achtung bei Gigabit: Alle acht Adern in Gebrauch, hier wird ein „doppelt ausgekreuztes“ Crossover-Kabel benötigt. Gute Repeater haben einen Eingang, der Umschaltbar ist, ihn nennt man den „Uplink-Port“. Somit ist nur noch eine Sorte Kabel notwendig. Diese Technologie nennt man MDI-Autosensing. Problem: Werden zwei Ports eines Switches miteinander verbunden, entsteht so automatisch ein Link → Netzausfall.

Glasfaser

- Reichweite von 10-12km ohne, > 1‘000km mit Verstärker
- Übliche Übertragungsraten sind 100 Mbit/s und 1‘000 Mbit/s, möglich sind jedoch bereits 1‘000 Terabit/s!
- Sehr empfindlich bei Biegung und mechanischer Belastung
- Abhörsicher, da keine elektromagnetischen Emissionen vorhanden
- Keinerlei Empfindlichkeit auf elektromagnetische Störeinflüssen
- Galvanische Trennung: Wird ein Gerät im Netzwerk durch Überspannung (oder Blitzschlag etc.) beschädigt, wird dies nicht an andere Geräte weitergeleitet (im Gegensatz zur Kupferverkabelung)

Lichtwellenleiter

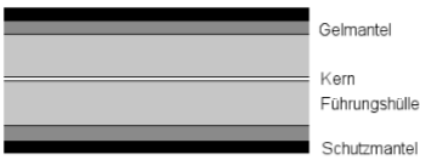


Bild 7: Aufbau Glasfaserkabel

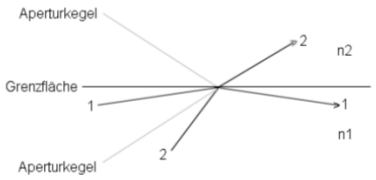


Bild 8: Gebrochenes und Reflektiertes Licht

- Von Interesse ist nur der Kern. Er ist sehr dünn, mit blossen Auge fast nicht zu sehen.
- Der Kern leitet das Licht. Der Lichtstrahl wird dabei jeweils vom Rand gebrochen. Ist der Winkel jedoch richtig gewählt, wird der Strahl nicht mehr gebrochen, sondern reflektiert.
- Aus diesem Grund ist der Faserkern aus zwei Schichten aufgebaut. Die äussere Schicht besitzt eine tiefere Brechzahl als der Mantel. Ist der Lichtstrahl nun richtig eingekoppelt, bewegt er sich in diesem durch Totalreflexion vorwärts.

- Das Kabel ist ziemlich empfindlich, so muss der Lichtwellenleiter und die Anschlussdosen mit Schutzkappen versehen werden, damit keine Luftfeuchtigkeit oder Staub eintreten kann. Ist das Kabel zu stark verbogen, wird die Reflexion gestört. Auch verliert der Lichtstrahl mit zunehmender Entfernung an Kraft.
- **Modendispersion:** Je nach Eingangswinkel benötigt der Lichtstrahl länger oder kürzer um zum Ziel zu gelangen. Hier kommt es zu einer Beeinflussung des Gesamtsignals, einer sogenannten Signalverbreiterung. Ab einer gewissen Länge fliessen die Signale ineinander und können folglich nicht mehr korrekt aufgelöst werden → Die Maximallänge ist erreicht.
- Lösung: Der Faserkern wurde mit Fremdatomen so verändert, dass der Brechungsindex von innen nach aussen immer kleiner wird. Das heisst: ein Strahl mit geringem Winkel hat mehr Widerstand, einer mit einem hohen Winkel ist schneller. Dadurch wird die oben genannte Verzögerung aufgehoben und damit die Signalverbreiterung minimiert.
- Unterschieden wird zwischen drei Standards: OM1, OM2 und OM3
- Ein Glasfaserkabel besteht i.d.R. aus zwei Fasern. Eine zum Senden, eine zum Empfangen.
- Auch hier müssen die Fasern überkreuzt werden, wenn zwei Endgeräte oder Netzwerkgeräte direkt miteinander verbunden werden.

Gesamtverkabelung

- Obige Verkabelungen sind im LAN anzutreffen
- Im Bereich MAN und WAN werden weitere Technologien eingesetzt: Satellit, Richtfunk, Laser.
- Die Glasfaser kommt bei allen drei Bereichen zum Einsatz
- Im Gebäude/Büro wird eine sternförmige Verkabelung eingesetzt, d.h. alle Anschlüsse werden an einer zentralen Stelle (Rack) zusammengeführt.

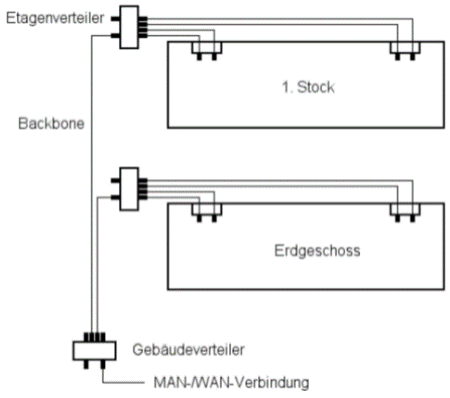


Bild 9: Übliche Gebäudeverkabelung

Backbone: Netzwerkleitungen, welche die Verbindung zwischen Stockwerken und Netzwerkgeräten vornehmen, an die jedoch normalerweise keine Endgeräte angeschlossen werden. Sollte die höchste Performance haben (heute 1 Gigabit oder 10GBit). Meistens Glasfaser.

- **Patchkabel:** Verbindung zwischen Netzwerkdose und der Netzwerkkarte des Geräts.
- Ein Gigabit-Anschluss bis zum Arbeitsplatz ist oft nicht sinnvoll, da die wenigsten Geräte dies ausnützen können. Der Lese-/Schreibzugriff auf die Harddisk ist noch zu wenig schnell. Wird sich jedoch in Zukunft noch ändern.
- Grundsätzlich sollte auf die Qualität der Hardware geachtet werden: Ein 48-Port Gigabit-Switch, der zu kleine Pufferspeicher hat und ein Backbone von 10 GBit, ist völlig überlastet. Hier ist u.U. ein 100 Mbit-Gerät mit genügend Kapazität besser!

- Basisbandübertragung (Baseband): Ein Dienst erhält eine gewisse Anzahl von Takten pro Sekunde. Man spricht in diesem Zusammenhang auch von „Bandbreite zuweisen“.
- Breitbandübertragung (Broadband): Mehrere Frequenzen werden gleichzeitig eingesetzt. Der Empfänger dekodiert dabei seine spezifische Frequenz.
- Beim Kabelfernsehen wird Breitband genutzt. Das Kabelmodem ist dabei zuständig, die entsprechende Frequenz abzufangen und zu decodieren und wieder als „normaler“ Ethernet-Anschluss zur Verfügung zu stellen. Hier sind wir wieder bei der Basisbandübertragung.
- Bei den Glasfasern muss auf die Wellenlänge, die Sorte (Multi- oder Singlemode) und den Durchmesser (Europa und Amerika haben unterschiedliche) geachtet werden.

Transceiver

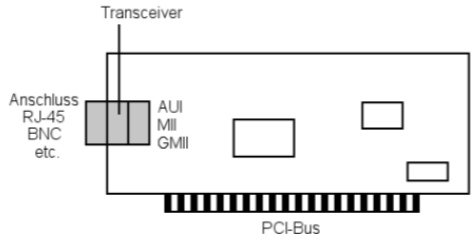


Bild 10: Schematischer Aufbau einer Netzwerkkarte

- Transceiver = Tramsitter + Receiver
- Der Sender und Empfänger, nimmt den direkten Zugriff auf das Medium vor.
- In den meisten Netzwerkadaptern fest eingebaut. Andernfalls ist ein externes Gerät anzuschliessen
- Wandelt die Daten um, um sie auf Layer I übertragen zu können
- MDI: Der Anschluss für das Kabel, z.B. RJ-45.

Zugriffsverfahren

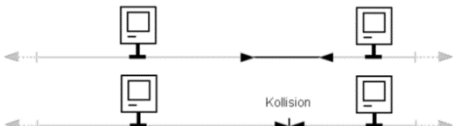


Bild 11: Kollision

Bild: Der Linke Rechner sendet. Der Rechte denkt, das Medium sei frei und sendet ebenfalls. Es kommt zur Kollision.

- Daher muss ein Rechner die doppelte Laufzeit des Signals auf der Länge des Stranges warten, bis er sich sicher sein kann, dass es keine Kollision geben kann.

CSMA/CD

- Der erste Netzwerkadapter, der eine Kollision bemerkt, generiert ein spezielles Signal. Dieses belegt das gesamte Medium und teilt allen anderen mit, dass es eine Kollision gegeben hat.
- Die Rechner können erst nach einer gewissen Zeit wieder senden. Dies soll verhindern, dass es direkt nach der Freigabe des Mediums wieder zu einer Kollision kommt.
- Die Implementierung der Regeln, die zur Teilung eines Mediums für viele Rechner definiert werden, nennt man Zugriffsverfahren. Hier beschrieben ist CSMA/CD.
    - Carrier Sense: Vor dem Senden prüfen, ob das Medium frei ist
    - Multiple Access: Viele Rechner teilen sich das Medium
    - Collision Detection: Kollision erkennen und darauf reagieren.
- Ist der heutige Standard in Ethernet-Netzwerken.
- Ein Datenpaket muss mindestens 64 Byte lang sein, um das gesamte Medium zu belegen.
- Late Collision: Ein (defekter) Adapter sendet, obwohl das Medium besetzt ist.

CSMA/CA

- Collision Avoidance
- Hier wird ein Request-to-Send-Signal (RTS) ins Medium gesendet. Gibt es keine Kollision mit einem anderen RTS-Signal, gehört das Medium dem Rechner. Alle anderen Geräte wissen, dass sie nun nicht senden dürfen.
- Nach der Sendung wird ein CTS (Clear to Send) Signal geschickt, der Rechner gibt das Medium also wieder frei.
- Ist im WLAN im Einsatz, beim „normalen“ Netzwerk konnte es sich nicht durchsetzen.

Layer II: Die Datensicherungsschicht

Adressen

- Physikalische Adresse (MAC): Für die Kommunikation innerhalb eines Netzwerksegmentes, gehören zum Layer II.
- Logische Adresse (z.B. IP): Für die Kommunikation weltweit
- MAC Adresse: 6 Byte lang, erste drei Bytes sind die Herstellerkennzeichnung
- Rundsendung auf Layer II an alle wird an die Adresse **ff:ff:ff:ff:ff:ff** adressiert. Dies ist die Broadcast-Adresse einer Broadcast-Domäne.

Adressermittlung (**ARP-Request**):

1. Rechner A schickt seine logische und seine physikalische Adresse, die logische von B und ein Fragezeichen an die Adresse ff:ff:ff:ff:ff:ff.
2. B, C, D, E, …. Schauen, ob ihre logische Adresse darin enthalten ist
    a. Wenn nein: Paket wird verworfen
    b. Wenn ja: Physikalische Adresse ins Fragefeld einfügen, Daten des Senders merken und Paket zurückschicken.

- **ARP-Cache**: Hier werden die Ergebnisse des ARP-Requests zwischengespeichert (ca. 300 Sek). Warum keine dauerhafte Speicherung? Falls ein Client seine logische oder physikalische (neue Netzwerkkarte) Adresse ändert.
- **RARP-Request:** Reverse ARP-Request, eine im Netzwerk angeschlossene, bootende Station ohne Festplatte erfragt ihre eigene, logische Adresse.

Trennung der Kollisionsbereiche. Bridge

- Immer mehr Geräte, der Repeater schickte alle Pakete immer zu allen Geräten → Überlastung der Übertragungsfähigkeit
- Lösung: Bridge. Hat zwei Anschlüsse und teilt das Medium somit in zwei Bereiche. Merkt sich, auf welcher Seite welche MAC-Adressen sind. Lässt nur die entsprechenden Pakete durch.
- Auch bei der Bridge wird der ARP-Cache nach ca. 300 Sek wieder geleert → wenn man einen Client von einer auf die andere Seite zügeln würde, wäre er nicht mehr erreichbar.
- **Store and Forward Bridging:** Auf jeder Seite der Bridge gibt ein eigenes CSMA/CD-Verfahren. D.h. wenn ein Paket auf die andere Seite muss, muss auch das Medium auf der anderen Seite frei sein. Die Bridge wartet, bis dies der Fall ist, dann erst kann sie senden.
- Die Bridge konnte die Layer I und Layer II Couverts verändern. So war es möglich, z.B. ein Token-Ring-Segment mit einem Ethernet-Segment zu verbinden.
- Zusätzlich konnten Netze mit unterschiedlichen Geschwindigkeiten verbunden werden
- Nun gab es aber auch Repeater, die das konnten. Wie ist das aber möglich, da sie nicht zwischenspeichern? Im Repeater wurde eine Bridge „versteckt“.
- **Cut-trough-Bridging:** Bridge sieht beim Empfangen von Daten sofort nach, ob das Medium frei ist. Wenn ja, wird direkt gesendet und gleichzeitig der Datenstrom dupliziert. Aufgrund der Längenbeschränkungen (Mindest-Paketgrösse von 64 Byte) weiss die Bridge, ab wann das Medium vollständig ihr gehört. Ab dann wird das Zwischenspeichern gestoppt und die Daten werden 1:1 weitergeleitet. Falls eine Kollision auftritt, liest sie den Rest in den Zwischenspeicher ein, um es später weiterzusenden (= Store and Forward). Hierdurch entstanden erhebliche Geschwindigkeitssteigerungen und effizientere Ausnutzung des Zwischenspeichers. Heute ist trotzdem „Store and Forward“ der Standard.

Der Switch (Meister der Bridges)

- Kann Netzwerke besser in viele Kollisionsdomänen (mit jeweils eigenem CSMA/CD-Verfahren) segmentieren als eine Bridge → massive Abnahme der Kollisionen.
- Allerdings mussten alle Broadcast-Anfragen (z.B. ARP-Request) transparent weitergeleitet werden → Dieser Broadcast-Verkehr wurde neu zur Beschränkung.
- Ist im Prinzip ein Repeater, der auf jedem Anschluss eine Bridge vorgeschaltet hat
- Die Bridge eines Ports muss sich lediglich die MAC-Adresse des angeschlossenen Geräts merken (oder wenn ein Repeater angeschlossen ist diejenigen der Endgeräte).
- Switches erhöhen die Security: Ein Paket wird nur noch an das entsprechende Gerät gesendet; mit Repeatern wurde jedes Paket an alle Clients geschickt.
- **Vollduplexmodus**: Ist das Gerät direkt an einen Switch angeschlossen, kann es die Collision Detection abschalten. Nun stehen alle vier Drähte für die Datenübertragung zur Verfügung; Senden und Empfangen ist gleichzeitig möglich. In einer Kollisionsumgebung kann entweder nur gesendet oder empfangen werden. Beschränkt auf UGV, Thin-Wire hat nur einen Draht.
- **Loop**: Eine Bridge erkennt, auf welcher Seite ein Gerät angeschlossen ist. Ein Broadcast muss nun von den Bridges im Switch transparent weitergeleitet werden. Gibt es eine Schleife, erscheint die MAC-Adresse auf beiden Seiten der Bridge. Sie weiss nicht mehr, auf welcher Seite das Gerät angeschlossen ist und sendet folglich in beide Richtungen weiter → Netzwerkzusammenbruch.

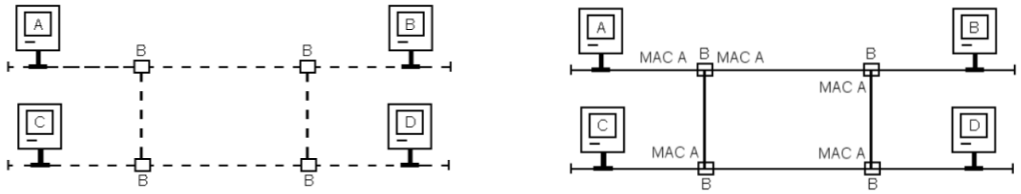


Bild 12: Layer II-Umgebung mit Loops: Mehrere Wege zum Ziel sind möglich, z.B. weil zwei Switches mit mehreren Patchkabeln untereinander verbunden sind. Client A führt z.B. einen ARP-Request durch.

- Gute Switches besitzen Mechanismen zur Vermeidung solcher Loops. Gefährlich sind kleine Büro-Mini-Switches.
- Später folgte die Idee, mittels der Verbindung von Switches redundante Systeme aufzubauen. Dies wäre jedoch wegen Loops nicht möglich. Man entwickelte ein Protokoll namens **Spanning Tree.** Ein Switch wird dabei zur Root-Bridge. Die Switches tauschen untereinander Infos zur Topologie des Netzwerks aus und blockieren so bewusst diejenigen Ports, die Loops verursachen würden. Fällt ein Switch aus, wird der Spaning Tree neu berechnet. Die Verbindung zur Root Bridge wird dabei stets gewährleistet. Sollte diese Root Bridge ausfallen, wird eine neue bestimmt. Für einen möglichst effizienten Tree sind Geräte höherer Preisklasse empfohlen, möglichst alle vom gleichen Hersteller.
- Managed Switch: Erlaubt Konfigurationen, z.B. des Spanning Trees, Zugriff auf die MAC-Tabelle, Zugriff via Telnet/SSH etc. Der unmanaged Switch dagegen „switcht vor sich hin“. Mindestens bei Backbones sollte nicht gespart werden.

Layer II-Pakete

- Pakete auf Layer II nennt man **Frames**

Präamble	SFD	DMAC	SMAC	Length	Data	Padding	FCS
Präamble	SFD	DMAC	SMAC	Type	Data	Padding	FCS
7 Byte	1 Byte	6 Byte	6 Byte	2 Byte	46–1500 Byte		4 Byte

Bild 13: Ethernet-Frames nach IEEE 802.3 (oben) und Digital, Intel und Xerox (unten)

- Präambel: Bitmuster zur Synchronisation. Wird von jedem Repeater oder Switch zur Sicherstellung der korrekten Versendung neu aufgebaut.
- SFD (Starting Frame Delimiter): Zeigt den Beginn eines Frames an
- DMAC/SMAC : Destination / Source MAC
- Type : Typ des Layer III-Protokolls, welcher transportiert wird
- Length: Länge des Frames
- Data: Nutzdaten des Frames und Kuverts höherer Layer (III – VII)
- Padding-Bits: Wenn Paket kleiner als 64 Byte wäre und damit nicht das gesamte Medium belegen könnte.
- FCS (Frame Check Sequence): Prüfsumme, um Fehler im Frame zu erkennen.

Layer III: Die Vermittlungsschicht

- Themen Layer III: Wie funktioniert die Kommunikation zwischen LANS und weltweit?
- Verwendet wird die **logische Adressierung mittels IP-Adressen**
- Zentrale Verwaltung und Vergabe durch die IANA
- IP-Adresse besteht aus vier Byte: 192.168.10.221

0.0.0.0	127.255.255.255	Klasse A
128.0.0.0	191.255.255.255	Klasse B
192.0.0.0	223.255.255.255	Klasse C
224.0.0.0	239.255.255.255	Klasse D
240.0.0.0	255.255.255.255	Klasse E

- Ein gewisser Teil, der Netzwerkteil, ist fix und darf nicht verändert werden.
  - Klasse A: Das erste Byte, z.B. 120.0.0.0 – 120.255.255.255 (16‘777‘216 Adressen)
  - Klasse B: Die ersten zwei Bytes, z.B. 160.1.0.0 – 160.1.255.255 (65‘535 Adressen)
  - Klasse C: Die ersten drei Bytes, z.B. 192.160.1.0 – 192.168.1.255 (256 Adressen)

Subnetze

- Es wäre nicht sinnvoll, z.B. die 65‘535 Adressen des Klasse B-Netzes miteinander zu verschalten. Die Broadcasts würden das Netzwerk zum Erliegen bringen. Lösung: Subnetze
- Subnetze bilden: Den Host-Teil der IP-Adresse weiter segmentieren. Als Beispiel steht ein B-Netz 172.16.x.x zur Verfügung. Dieses kann in 256 Subnetze mit Adressbereichen 172.16.0.y, 172.168.1.y, 172.168.2.y, … aufgeteilt werden.
- Router trennen Broadcast-Domänen
- Auch Subnetze können nochmals weiter segmentiert werden
- Dies kann vor allem Sicherheitsgründe haben. An Routern lassen sich Filter und Zugangsbeschränkungen konfigurieren.

Besondere Adressen

- Die kleinste und die höchste Adresse sind reserviert
  - Kleinste: Bezeichnung des (Sub-)Netzes
  - Grösste: Broadcast-Adresse. Ein Datenpaket an diese Adresse muss von jedem Netzwerkgerät im Subnetz beachtet werden.
- Bei der Teilung in Subnetze gehen somit für jedes Subnetz zwei Adressen verloren.

Subnetzmaske

- Ist der Adressraum nicht segmentiert, spricht man von der Netzmaske, sonst von der Subnetzmaske
- Trennt den Netzwerk- vom Host-Teil
- Wollen wir ein Klasse-B Netz in 256 Klasse-C Netze segmentieren, nehmen wir die Subnetzmaske 255.255.255.0.
- Das heisst anhand der IP-Adresse und der Subnetzmaske erkennen wir ob und wie segmentiert wurde.
- Zusätzlich sehen wir, ob sich ein anderer Computer im selben Netz (Broadcastdomäne) befindet oder nicht. D.h. es wird entschieden, ob ein ARP-Request durchgeführt wird oder ob der Weg über den Router gegangen werden muss.

Subnetzmaske binär	SNM dezimal	Kurzschreibweise (anz. Bits, hinter IP)	Netze x Adressen
11111111.11111111.11111111.00000000	255.255.255.0	/24	1 x 256
11111111.11111111.11111111.10000000	255.255.255.128	/25	2 x 128
11111111.11111111.11111111.11000000	255.255.255.192	/26	4 x 64
11111111.11111111.11111111.11100000	255.255.255.224	/27	8 x 32
11111111.11111111.11111111.11110000	255.255.255.240	/28	16 x 16
11111111.11111111.11111111.11111000	255.255.255.248	/29	32 x 8
11111111.11111111.11111111.11111100	255.255.255.252	/30	64 x 4
11111111.11111111.11111111.11111110	255.255.255.254	/31	128 x 2
11111111.11111111.11111111.11111111	255.255.255.255	/32	1 Host

- Obiges Beispiel ist für Klasse C; bei A-Klasse wäre es von /8 bis /16, bei B-Klasse /16 bis /24
- 10.12.16.14/25 bedeutet, wir haben eine IP-Adresse aus dem Subnetz 10.12.16.0 mit der Broadcast-Adresse von 10.12.16.127
- Zu beachten: Pro Subnetz gehen 2 Adressen verloren + meistens noch eine für den Router. Benötigen wir 7 Client-Adressen, müssen wir also mindestens /28 nehmen.
- Die Ermittlung des Netzwerks, in dem sich ein Gerät befindet, ist das Ergebnis der logischen Addition (AND) der Subnetzmaske und der Adresse des Geräts:

10010.00010000.00101000.10100000	Adresse, dezimal: 178.16.40.160
11111.11111111.11111111.10000000	Subnetzmaske, dezimal: 255.255.255.128
AND	
10010.00010000.00101000.10000000	Netz: 178.16.40.128

Der Router

- Die Router legen die Segmentierung fest. Sobald dies geschehen ist und kommuniziert wird, ist das neue Netz weltweit erreichbar.
- Der Router benötigt für jedes an ihm angeschlossene Subnetz je ein Interface (Adresse auf Layer II und III).

Ablauf

1. Anhand der eigenen IP-Adresse und Subnetzmaske sowie der IP-Adresse des Empfängers errechnen, ob der Empfänger im selben Netz ist.
2. Wenn nein, ARP-Request an den Default Gateway schicken um dessen Layer II-Adresse zu erhalten
3. Datenpakete an Router schicken
4. Router schaut, ob er eine Adresse im entsprechenden Subnetz des Empfängers hat
5. Wenn nein, schaut er, ob er den Weg zum Empfänger kennt (z.B. über Router2)
6. Wenn ja, löst er die MAC-Adresse von R2 mittels ARP-Request auf.
7. R1 entfernt die MAC-Adresse von Ethernet-Frame (SMAC / DMAC) und trägt seine eigene als Source und die von R2 als Destination ein. Dann gibt er das Frame an R2 weiter. Das heisst, der **Router verändert die Daten des Layer II-Couverts**.
8. R2 führt wieder einen ARP-Request für B durch, ändert wieder SMAC/DMAC und leitet das Frame weiter.
9. Die IP-Adresse des Senders (Computer A) ist immer noch im Couvert des Layers III, so dass der Empfänger diese bei sich hat und wieder danach suchen kann.

Vergleichbar mit Postverteilungszentrum: Adressen von Sender bleiben immer auf dem Couvert (=Layer III). In Postzentrum A gelangt der Brief jedoch in einen Container, der B als Ziel hat. Dort

angekommen, wird ein neues Ziel C auf den Container geschrieben und als Absender B. Dies Entspricht Layer II. Layer I wäre dann der Transport mit LKW, Zug, Schiff etc.

- Jeden „Sprung“ über einen Router nennt man einen Hop.

Reservierte und spezielle Adressen

- In der Klasse D befinden sich die **Multicast**-Adressen. Im Gegensatz zum Singlecast (direkte Sendung an eine Adresse) und dem Broadcast (Sendung an alle) ist ein Multicast eine Rundsendung an eine Gruppe von Adressen. Immer aktueller wegen Streaming von Audio- und Videodateien: Ein einziger Datenstrom für eine Multicast-Gruppe. Wer Interesse an den Daten hat, kann sich in den Strom einschalten.
- Pro Klasse gibt es einen Bereich, der nicht geroutet (d.h. nach aussen weitergeleitet) wird (für Tests, Adresstranslation etc.). Man nennt diese „**private Adressen**“.
  - Klasse A: 10.0.0.0 - 10.255.255.255
  - Klasse B: 172.16.0.0 - 172.31.0.0
  - Klasse C: 192.168.0.0 - 192.168.255.255
- Ist ein DHCP-Server nicht erreichbar, teilt sich die Netzwerkkarte selbst eine beliebige Adresse aus dem **APIPA-Bereich** zu (mittels Broadcast wird die erste freie Adresse gewählt). Damit soll gewährleistet werden, dass man innerhalb des Netzwerks trotzdem kommunizieren kann. Umfasst die Adressen 169.254.0.1 bis 169.254.255.255
- **Superprivate Adressen (auch Loopback-Adressen)** sind aus dem Bereich 127.0.0.0 bis 127.255.255.255. Jeder Netzwerkadapter hat eine solche. Ein Paket an diese Adresse wird nicht ins Netz weitergeleitet, sondern sofort wieder zurück. Somit erscheint es, als wäre es vom Netzwerk hereingekommen. 127.0.0.1 ist der „localhost“, als die eigene Netzwerkkarte.

Das IP-Paket

- Liegt im Datenteil des Frames (Layer II-Paket).

Version	IHL	TOS	Length
Ident	Flags		Offset
TTL	Protocol		Header-CS
Version	IHL	TOS	Length
Sender-IP-Address			
Destination-IP-Address			
Options/Padding			
Data			

- Version: Im Moment Version 4, Version 6 in Entwicklung
- IHL: Internet Header Length, Länge des Kopfes
- TOS: Type of Service, Priorität und Eigenschaften des Pakets. Selten genutzt, nur bei QoS
- Length: Gesamtlänge des IP-Pakets, maximal 65‘535 Byte.
- Ident: Nummerierung, so dass einzelne Pakete beim Empfänger sortiert werden können
- Flags: hier ist unter anderem die Fragmentierung kodiert
- Offset: Lage des Fragments im ursprünglichen IP-Paket
- Protocol: Hinweis auf das enthaltene Layer IV-Couvert
- Header-CS: Checksumme zur Prüfung der Integrität des IP-Headers
- Opt./Pad.: Daten zur Statistik, dem Routing, zu Diagnosezwecken, zum Auffüllen.
- Data: Transportierte Nutzdaten

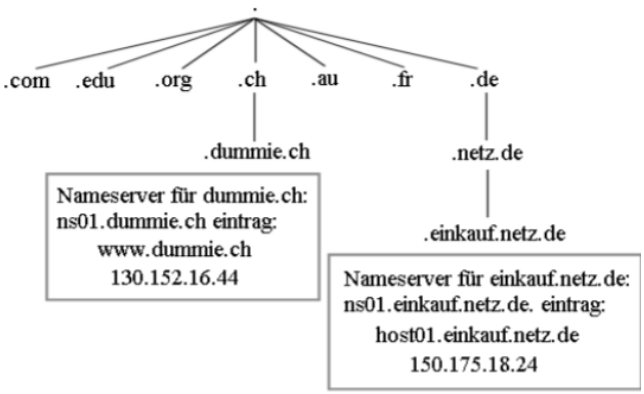
- Time to live wird in Anzahl Hops angegeben, d.h. wie viele Router noch übersprungen werden dürfen, bevor das Paket vernichtet wird.
- Bei der Fragmentierung wird das IP-Paket in kleinere Teilpakete zerlegt, je nachdem wie viele Daten im Netzwerk übertragen werden können (nur wenige Netzwerke können 65‘535 Byte übertragen, i.d.R. sind es 1‘500Byte).
- In den Flags des IP-Pakets kann auch angegeben werden, dass das Paket nicht fragmentiert werden darf. Ist das Paket zu gross für das Netzwerk, wird es verworfen. Erzeugt man nun Testpakete mit abnehmender Grösse und gesetztem Don’t fragment Bit- kann man so die maximale MTU (Maximum Transport Unit) einer Weiterverbindung ermitteln.

Routing – weltweite Wegfindung

- Ähnlich wie gute Switches im Layer II, befüllen auch die Router ihre Routing-Tabellen. Damit können sie sich mögliche Wege auf Layer III merken
- Zusätzlich können die Router jedoch alternative Wege finden und sogar über mehrere Wege gleichzeitig senden.
- Zwei grosse Klassen von Routing-Protokollen
    - Distance Vector-Protokoll: Router tauschen ihr eigenen Routing-Tabellen mit den direkten Nachbarn aus
    - Link-State-Protokoll: Router senden Informationen über ihre angeschlossenen Segmente zu allen Routern in einer definierten Routing-Domäne. Ist viel flexibler.
    - Moderne Routing-Protokolle bewerten neben den Anzahl Hops auch die Übertragungsgeschwindigkeit, Kosten etc.
- Router lernen Wege im Netzwerk entweder durch Kommunikation mit anderen Routern (=dynamisch, z.B. im Netzwerk zu Hause) oder durch Konfiguration (=statisch, z.B. von zu Hause zum Provider).
- Dial-on-Demand-Routing: Es existieren zwei mögliche Wege von A nach B. Durch Konfiguration (jeder Route werden Kosten zugewiesen) nimmt der Router wenn möglich die günstigere. Sollte jedoch die günstigere Störungen haben, wird die teurere benutzt.

Domain Name System

- Hosts besitzen oft nicht nur eine Adresse, sondern auch einen Namen, da einfacher merkbar
- Diese Namen sind ebenfalls streng hierarchisch organisiert wie die IP-Adressen.
- Beispiel: Firma reserviert zu Ihrer Adresse 132.150.0.0/16 den Namen „dummie.ch“. Dieses „dummie.ch“ ist fix, ansonsten kann der Name beliebig erweitert werden. Z.B. pc05.finanzen.dummie.ch
- Das DNS ist ein Verzeichnissystem mit verteilten Datenbanken.
- Jeder der Namen und IP-Adressbereiche registriert muss einen weltweit erreichbaren Nameserver führen.
- Weltweit gibt es 14 Root-Nameserver, die den weltweiten Aufbau kennen. Sie verweisen auf die NS der nächsten Ebene, an welche die Top-Level-Domains delegiert sind.



- Möchte ich nun von der Station host01.einkauf.netz.de die Website von www.dummie.ch erreichen, muss die IP-Adresse dieses Webservers ermittelt werden. Host01 fragt bei seinem Nameserver, einkauf.netz.de nach. Dieser kennt den Namen nicht und fragt bei netz.de nach. Diesem ist dieser Name ebenfalls unbekannt, er fragt bei einem Root-Server nach. Der kennt ihn ebenfalls nicht und leitet an den Zuständigen Server für „.ch“ weiter, welcher nun die IP-Adresse zurückliefern kann.
- Der korrekte, volle DNS-Name endet mit einem Punkt, da der oberste ein Root-Server ist (Kennzeichnung mit „.“).
- Das DNS-System erfüllt noch einen weiteren wichtigen Dienst. Durch spezielle Einträge in den Servern werden neben Adressen und Namen von Hosts auch Mail-Domains (MX-Records) geführt.
- **Forward Lookup:** Namen in IP-Adressen auflösen
- **Reverse Lookup:** IP-Adressen in Namen auflösen. Zuständig ist die in-addr.arpa-Domain, welche 256 Subdomänen hat. Jede dieser Domänen hat wiederum 256 Subdomänen. So geht es noch zwei Stufen weiter, womit der gesamte Range aller IP-Adressen abgebildet ist. Es gibt aber ein Problem: IP-Adressen werden von links nach rechts immer genauer, Namen umgekehrt. Hier wird einfach die IP-Adresse umgekehrt, aus 131.15.x.x/16 wird x.x.15.131-in-addr.arpa. Diese Adresse muss auf dem Nameserver geführt werden.

DHCP

- Konfiguration der Netzwerkparameter (IP-Adresse, Subnetzmaske, Default Gateway) durch einen Server
- Beim Starten schickt ein Computer einen DHCP-Request (Broadcast).
- Der DHCP-Server offeriert eine Adresse aus dem Pool → DHCP-Offer
- Client schickt einen DHCP-ACK (Acknowledge) zurück
- Die Adressen besitzen jeweils ein Verfallsdatum, damit sie wieder neu vergeben werden können.

Single-, Broad- und Multicast

- Singlecast: Senden von Daten an einzelne Adresse
- Broadcast: Senden von Daten an alle in der Broadcast-Domäne
- Multicast: Streaming von Video und Audio, es existiert ein Datenstrom, den sich interessierte „anzapfen“ können. Damit müssen z.B. in einem Schulungsraum mit 25 PCs (10 davon sind betroffen) nicht 10 Singlecasts durchgeführt werden. Auch werden die 15 nicht betroffenen nicht unnötig durch Broadcasts beschäftigt. Konkret sendet der Server an eine Multicast-Adresse (IP-Adressklasse D, 224.0.0.0 bis 239.255.255.255).

Layer IV: Die Transportschicht

Ports und Sockets

- Jeder Service ist an eine Portnummer gebunden
- Diese Nummer liegt zwischen 0 und 65‘535., 0-1023 sind „well knwon ports“.
  - FTP: 20/21 (20=Dateitransfer, 21=Dateitransfer-Control)
  - DNS: 53
  - http: 80
- Socket: Kombination aus IP-Adresse und Port, z.B. 192.168.17.4:80. Ein Sender sucht sich einen freien Port > 1‘024 aus und schickt diesen an den Port eines Empfängers, hinter dem ein Dienst läuft (z.B. Port 80 bei einem Webserver). Durch diese Kombination kann der Server einen Service vielen gleichzeitig anbieten, er kann sie leicht unterscheiden. Der Client kann mehrere Dienste gleichzeitig beanspruchen (**Multiplexing**)

TCP: Transmission Control Protocol

- TCP setzt beim Empfänger Pakete, die gespalten wurden, wieder in der richtigen Reihenfolge zusammen und reicht es nach oben an die Applikation weiter. Verlorene Pakete werden nachgefordert.
- Ist **verbindungsorientiert**, da eine virtuelle Verbindung zwischen Sender und Empfänger hergestellt wird.
- Sehr sicheres Protokoll, was aber mit einem gewissen Overhead bezahlt wird.

Senderport		Empfängerport	
Sequenznummer			
Bestätigungsnummer			
Header Length	unbenutzt	Flags	W-Size
Checksum		Urgent	
Options/Padding			
Data			

- Sequenz: Nummerierung der Datenpakete im Datenstrom
- Bestätigungsnummer: Jedes einzelne Paket wird vom Empfänger bestätigt
- Flags: z.B. Urgent-Pointer (Paket muss sofort bearbeitet werden), Acknowledgement
- Window-Size: Wie viele Bytes darf der Sender schicken, damit der Empfangpuffer nicht überläuft?
- Checksum: Querysumme zur Überprüfung der Integrität
- Opt./Pad.: Optionale Daten, wenn keine vorhanden wird bis 32Bit-Grenze mit Nullen gefüllt
- Data: Daten der höheren Layer

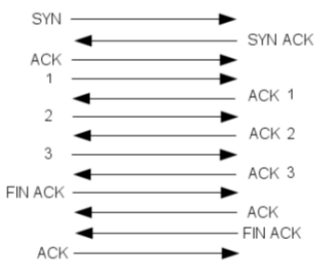


Bild 14: Ablauf TCP-Verbindung. Mehrfache gegenseitige Bestätigungen. Anhand der Sequenznummern erkennt TCP, ob alle Pakete eingetroffen sind und wenn ja, ob deren Reihenfolge auch stimmt..

UDP: User Datagram Protocol

- Keine Kontrolle, ob die Daten korrekt übermittelt wurden.
- Dadurch schlank und schnell
- Macht Sinn, wenn die Applikation hinter dem Port selbst für die korrekte Übertragung sorgt (z.B. SMB, das Protokoll für Windows-Freigaben und Drucker). TCP würde hier nur für unnötigen Overhead sorgen.
- Einsetzbar wenn eine Verbindung sinnlos wäre, z.B. bei der Anfrage eines DHCP Servers.

Senderport	Empfängerport
Länge	Checksum
Data	

Security: Router und Firewall

- Auf Layer III kann mit dem Router nach IP-Adressen gefiltert und diese blockiert werden
- Auf Layer IV kann feiner unterschieden werden. Webserver soll nur intern erreichbar sein → Alle Zugriffe von aussen auf den Port 80 unterbinden. Es kann sogar z.B. TCP einzeln gesperrt werden, UDP wird jedoch zugelassen.
- Eine Firewall ist im Prinzip ein Router, jedoch mit zusätzlichen Regeln.
  - Router = maximal offen, bestrebt so viele Daten wie möglich weiterzuleiten
  - Firewall = jeglicher Verkehr von vornherein verboten, explizite Freigabe erforderlich. Kontrolle der Pakete, blockieren des Verkehrs bei misstrauen, Protokollierung
- DMZ: Demilitarisierte Zone. Server, die von ausserhalb des Intranets erreichbar sein müssen (FTP, Webserver etc.) werden ausserhalb des Intranets angesiedelt. Somit besteht keine Möglichkeit z.B. über den FTP-Server auf das Intranet der Firma zuzugreifen.

NAT, PAT und Masquerading

- IPv4 Adressen wurden knapp und IPv6 war erst in der Entwicklung.
- Lösung: NAT (Network Address Translation).
- Hinter einem Router oder der Firewall wird ein eigenes Netz betrieben. Dabei werden nur die nötigen Geräte nach aussen in gültige Adressen umgesetzt. Damit ist die Sicherheit stark erhöht, nicht mehr jedes Gerät ist über das Internet erreichbar. Der Rest konnte aber intern miteinander kommunizieren, damit wurden Adressen gespart. Problem: So konnten nicht alle auf das Internet zugreifen.

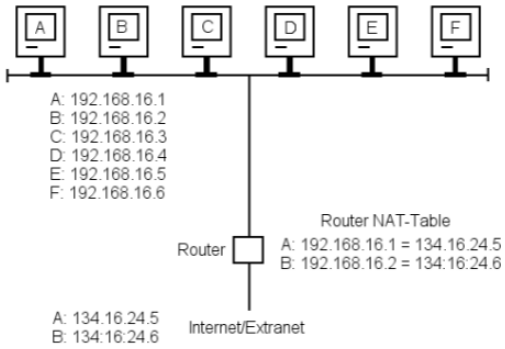


Bild 15: Router (möglich wäre auch eine Firewall) mit NAT-Tabelle

- Die Weiterentwicklung heisst PAT (Port and Address Translation), auch IP-Masquerading.
- Es werden nicht 1:1 private in offizielle Adressen übersetzt, sondern mehrere private Adressen laufen über eine offizielle. Dies ist durch das Beigeben der Portnummern möglich.

VLANs – virtuelle Netze

- Problem: Mehrstöckiges Firmengebäude, Abteilungen sind verstreut im Gebäude verteilt. Die einzelnen Abteilungen sollen jedoch nur auf ihren jeweiligen Server Zugriff haben.
- Theoretisch könnte man jedes Büro über Switches an eine Hauptfirewall hängen, wo auch die Server dran sind und dann mit Access-Listen arbeiten → sehr teuer und aufwendig
- Lösung: VLAN, Virtual Local Area Network. Am Switch wird dabei festgelegt, **welcher Port** in welchem Segment ist (mit Layer III-Adressen kann der Switch nichts anfangen). Computer sehen sich nur, wenn sie im selben Segment (VLAN) angesiedelt sind. Vorteil: Switches sind günstiger als Router/Firewalls und arbeiten auf Layer II, was einen Geschwindigkeitsvorteil mit sich bringt.

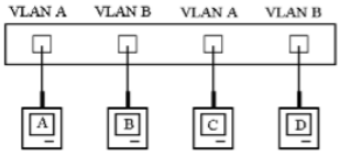


Bild 16: Switch mit VLAN

- Im Layer II-Paket ist im Feld „VLAN“ das entsprechende Segment eingetragen (das Paket ist dann „getaggt“). Für das Feld wurden extra 4 weitere Byte geschaffen. Dies kann bei älteren Switches und Repeatern für Verwirrung sorgen, da sie das noch nicht erkennen!
- Es gibt zwei Möglichkeiten:
  - Switch bekommt eine Tabelle mit MAC-Adressen und zugehörigen Kommunikationsbereichen (auf MAC Adressen basierende VLANs)
  - Admin teilt die Ports in VLANs (portbasierende VLANs) → verbreiteter.

Trunks

- Trunk: **Verbindung zwischen Switches, die VLANs (also getaggte Pakete) transportiert**
  - Kommen Frames zum Switch herein, werden sie mit einem VLAN-Tag versehen
  - Von Switch zu Switch werden die Pakete mit der VLAN-Kennung transportiert
  - Erst wenn sie den Switch zum Client verlassen, wird der Tag entfernt.

Verkehr zwischen VLANs

- VLAN wird auf Layer II organisiert
- Wird eine Kommunikation benötigt, wird ein Layer III Gerät benötigt: Ein **Router, der in jedem VLAN ein Interface besitzt (d.h. an zwei Ports des Switches angeschlossen ist)**.
- Für den Router sieht es aus, als ob er mit zwei Switches kommuniziert. Switch bekommt Frame, entfernt den Tag, schickt es zum Router. Dieser schaut sich die logische Adresse an, leitet in das andere Netz weiter und landet somit bei einem anderen Port des Switches. Dort wird wieder ein Tag hinzugefügt und das Frame weitergeschickt.
- Der Router sieht also nichts vom Tagging und der Switch nichts vom Routing.
- Moderne Router verstehen das Tagging auf Layer II, hier wird der Router einfach an einen Port des Switches angeschlossen. Diese Verbindung nennt man **Trunk-Links**. Der Router nimmt das Paket entgegen, ändert den Tag und gibt es zurück an den Switch.

Vorteile

- Verschiedene Subnetze können an verschiedenen Stellen in einem Gebäude konfiguriert werden.
- Access-Listen können an einem zentralen Ort geregelt werden und gelten für das gesamte VLAN
- Flexible Umzüge von Geräten oder ganzen Abteilungen
- Kostengünstigere Variante als viele Router zu kaufen.

Grenzen

- Durch Router (also auf Layer III) lassen sich keine Tags transportieren → Sind zwei Gebäude miteinander verbunden, können sie i.d.R. nicht dieselben VLANs benutzen.

Bemerkungen

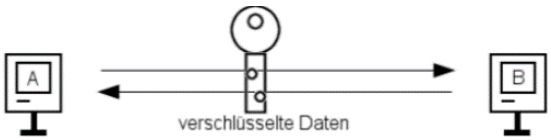
- Der Begriff VLAN wird oft verschiedenartig interpretiert:
    - VLAN-fähig bedeutet bei manchen Routern, dass sie die 4 Byte grösseren Ethernet-Pakete akzeptieren und weiterleiten (aber sie machen nix damit…)
    - Andere interpretieren VLAN so, dass alle an einem Switch angeschlossenen Geräte eine separate Verbindung zum ebenfalls am Switch angeschlossenen Router erhalten. Die angeschlossenen Clients können so nur noch mit dem Router, nicht mehr aber untereinander kommunizieren
- Mehr VLANs = theoretisch mehr Spanning Trees. Es ist zu entscheiden, ob für jedes VLAN ein einzelner Spanning-Tree definiert wird oder ein einziger über die gesamte Layer II-Umgebung.
- Pruning: Drei Switches, jeweils verbunden mit einem Trunk, einer hat kein „VLAN C“ konfiguriert. Pruning sorgt dafür, dass ein Broadcast im Subnetz C nicht zu diesem einen Switch gelangt.

VPN – virtuelle private Netzwerke

- VPN: Virtual Private Network
- Aufgrund Home-Offices, Zugriff für Reisende auf Firmendaten, sicherer Datenaustausch zwischen Filialen von Firmen
- VPN kann sich wie ein verschlüsselter Schlauch durch das Internet vorgestellt werden
- Client stellt über das Internet eine Verbindung mit dem VPN-Gateway der Firma her. Man spricht auch von **Host-to-Site VPN.**
- Client erhält durch den Tunnel eine Adresse aus dem Firmennetzwerk zugewiesen. Damit sieht es so aus, als ob er im Gebäude selbst angeschlossen wäre.
- Werden zwei Standorte miteinander verknüpft, arbeitet an jedem Ort ein VPN-Gateway, auch **Site-to-Site VPN** genannt.
- VPN-Protokolle: IPSec, PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol) uvm.
- Sicherheitsprotokolle: ESP (Encapsulating Security Payload), IKE (Internet Key Exchange)
- **Split Tunnel:** Beim Client wird lokaler Verkehr (z.B. mit dem Netzwerkdrucker, Faxserver etc.) weiterhin durch die Firewall erlaubt. Dies ist allerdings sicherheitstechnisch bedenklich, da ein Hacker den Client von aussen übernehmen könnte und somit im Intranet der Firma ist.
- **Closed Tunnel:** Kein lokaler Verkehr mehr beim Client, viel sicherer als Split Tunnel.
- **Transportmodus**: Nur der Datenteil des IP-Pakets wird beim Übertragen verschlüsselt
- **Tunnelmodus:** Das gesamte Paket wird beim Übertragen verschlüsselt und ein neuer IP-Header generiert.
- Firewalls bringen (ausser Performance-Einbussen) nichts in einer VPN-Verbindung. Diese läuft sowieso Point-to-Point. Sollte eine FW dazwischen sein, sind die jeweiligen Ports freizuhalten.
- Eine weitere, neuere Tunneltechnik ist SSL (Secure Socket Layer), bei dem der VPN-Gateway ein Webserver ist.

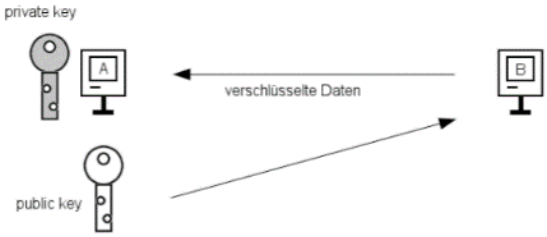
Verschlüsselung

Symmetrische Verschlüsselung



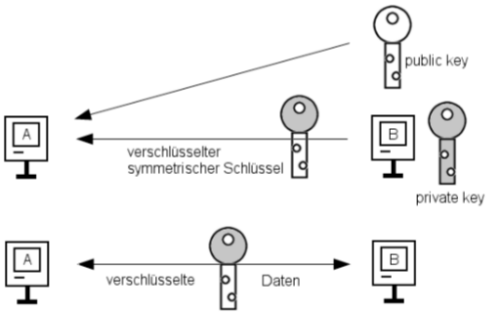
- Für das Ver- und Entschlüsseln wird derselbe Schlüssel benutzt
- Schnellste Methode der Verschlüsselung
- Schlüssel kann allerdings beim ersten Austausch „mitgelauscht“ werden
- Während der Übertragung wird i.d.R. immer derselbe Schlüssel verwendet. D.h.: Daten sammeln und in Ruhe versuchen zu knacken.

Asymmetrische Verschlüsselung



- B holt sich den öffentlichen Verschlüsselungsschlüssel von A, verschlüsselt damit die zu übertragenden Daten und schickt sie an A. Dieser hat einen passenden private Key zum Entschlüsseln der erhaltenen Daten.
- Auch RSA-Verfahren genannt.
- Benötigt viel Zeit und Prozessorleistung.

Hybrid-Verschlüsselung



- Zuerst wird ein symmetrischer Schlüssel generiert. Dies wird asymmetrisch verschlüsselt (jeweils über einen private Key) und an den Empfänger gesendet.
- Der Verkehr wird anschliessend mit dem gesichert übertragenen symmetrischen Schlüssel verschlüsselt, den nur der Empfänger wieder auspacken kann.
- Der symmetrische Schlüssel wird im Hintergrund beliebig oft gewechselt.
- Gilt als ebenso sicher wie die reine asymmetrische Verschlüsselung.

Wireless LAN, Funknetze, VoIP

- **Hotspot:** Öffentlich zugängliches Funknetz
- **Access Point:** Gerät, das die Verbindung zum physikalischen Netzwerk herstellt
- Störungen:
  - Durch andere WLANs auf der selben Frequenz
  - Signaldämpfung durch die Entfernung
  - Hindernisse, je nach Material
  - Mikrowellenherde (da selbe Frequenz)
- **Multipath-Effekt**: Durch Reflexionen sieht ein Empfänger das Signal mehrfach, das primäre und die reflektierten Signale stören sich.
- WLAN funktioniert (wie bei Thin-Wire) immer nur halbduplex, d.h. eine Antenne kann entweder nur senden oder empfangen. Das Zugriffsverfahren ist hier auch **CSMA/CD**. Gibt es zwei Clients, die jeweils das WLAN aber nicht sich gegenseitig sehen, muss der Access Point als Vermittler die Sendungen koordinieren (**Ready to Send / Clear to Send**). Zweiteres nennt man auch das „**Hidden-Node-Problem**“.
- **Roaming:** Übergabe eines Clients von einem Access-Point zum anderen beim örtlichen Wechsel des Clients.
- Nimmt die Geschwindigkeit des WLANs ab, kann es an einer niedrigen Qualität der Verbindung liegen. Lieber wenige, dafür alle Pakete senden anstatt viele senden und nur ein Bruchteil davon kommt an.
- **Ad-hoc Netzwerk:** Isolierter Peer-to-Peer Verbund von Netzwerkadaptern (z.B. 3 Laptops) unter sich ohne einen zentralen Access Point.
- **Infrastrukturmodus:** Alle kommunizieren über den zentralen Access Point.
- **Beacon:** Paket, das vom Access Point versendet wird und welches die Parameter des Netzw. enthält (SSID, Art der Verschlüsselung etc.). Den SSID-Broadcast kann man auch deaktivieren.
- **Verschlüsselung:**
  - Standardmässig WEP, ein symmetrischer Verschlüsselungsverfahren. Lässt sich allerdings relativ rasch knacken.
  - WPA-Verfahren: Wie WEP, ändert jedoch regelmässig die Keys im Hintergrund
  - Wenn möglich sollte WPA2 verwendet werden. Wer absolut sicher sein will, verbindet den Client über den Access Point über VPN.
- **Stromversorgung:**
  - Access Point direkt an Steckdose angeschlossen
  - PoE (Power over Ethernet): Strom über das Netzwerkkabel. Entweder gibt es einen Power-Injector der an der Steckdose angeschlossen ist und das Netzwerkkabel mit Strom speist, oder ein Switch speist den Strom direkt selbst ein.
- **Mesh (Netz, Masche):** Mehrere Access Points über einen Backbone miteinander verbunden, nur ein Access Point ist tatsächlich mit dem Internet verbunden. Bei öff. Plätzen sinnvoll.

VoIP

- (VoIP-)Server als Vermittler: Stellt Verbindung zwischen Anrufer und Empfänger her und klinkt sich dann aus, da die Verbindung zwischen diesen beiden direkt untereinander läuft.
- Die SIP-Adresse ermöglicht, am Dienst namentlich präsent zu sein, egal wo man ist und welche IP-Adresse man hat. SIP handelt die Verbindung aus, überträgt die nötigen Infos und die verwendeten Codecs. Die Datenübertragung wird vom RTP (Real-Time Transport Protocol) übernommen, welcher die Daten über UDP überträgt.

Powerline

- Signal wird durch die Stromleitung transportiert
- Das Signal wird dabei mittels sogenannten Powerline-Bridges aufmoduliert und ausgefiltert.
- Jeder der Zugriff zur selben Stromleitung hat, kann „mithören“.
- Zu beachten ist, dass Stromunternehmen eigene Stromzähler platzieren. Um die Fernwartung zu ermöglich, werden durch das Stromunternehmen meist alle Frequenzen herausgefiltert, die nicht vom Stromlieferanten sind.

Standards und Parameter

- WLAN ist ein eigener, 1997 von der IEEE entwickelter Standard
- Verwendet das 2.4-GHz-Band, Übertragungsgeschwindigkeit zu Beginn 1 oder 2 Mbit/s
- Kanalbandbreite: ca. 20 MHz
- 1999 kam das 5-GHz-Band dazu (Standard 802.11a), um das 2.4 zu entlasten.
- 802.11h: Neues Verfahren, welches für Sender und Empfänger den Kanal mit der besten Verfügbarkeit aussucht und die Sendeleistung auf das benötigte Minimum drosselt. Zusätzlich wurde durch ein zweites Verfahren der Kanal sofort gewechselt, wenn Verkehr von nicht-WLAN-Geräten erkannt wird (z.B. Radaranlagen, welche sog. Primärnutzer sind)
- 2003 kam 802.11g dazu, nun konnte mit bis zu 54 Mbit/s gesendet werden.
- 2009: 802.11n, welches mit mehreren Antennen arbeitet und damit in der Lage ist auf denselben Frequenzen (entweder 2.4GHz oder 5GHz) **parallel mehrere Datenströme** zu versenden und zu empfangen.
- 802.11n kennen drei Modi des Betriebs:
    - Legacy (802.11a/b/g):
    - Mixed Mode (802.11n und 802.11a/b/g)
    - Greenfield (nur 802.11n)

- Grundsätzlich wird zwischen Geschwindigkeit und Stabilität abgewogen. Ist das Signal robust und klar, werden die Verfahren auf Bandbreite optimiert. Ist es dagegen schwach und mit Störungen behaftet, wird die Geschwindigkeit zurückgeschaltet und mehr Wert auf Stabilität gelegt.

Netzzugang, Szenarien

- **ISDN** ist heute nur noch sehr selten anzutreffen. Es wird per analogem Telefon eingewählt. Die Übertragungsgeschwindigkeit ist 64 Kbit/s pro Kanal, meistens sind zwei Kanäle im Einsatz, selten auch mehrere. Vom Provider erhält man eine IP-Adresse, intern muss also NAT/PAT eingesetzt werden. Dies geschieht über einen Router, welcher eine entsprechende ISDN-/Telefonschnittstelle besitzt. Einzige Vorteile: ISDN kann als „Notfallleitung“ sehr gut verwendet werden, z.B. um auf spezielle Netzwerkgeräte zuzugreifen wenn das Netzwerk mal down ist.
- **DSL** ist heute quasi-Standard und ziemlich schnell.
    - Benutzt den Kupferdraht der Telefonleitung, aber mit eigenem Verfahren. Somit kann gleichzeitig gesurft und telefoniert werden.
    - Asymmetrisches DSL (ADSL) bedeutet, das Up- und Download verschiedene Geschwindigkeiten haben. Dies, weil für Download mehr benötigt wird als für Upload.
    - Das DSL Signal wird am Hausanschluss durch einen Splitter vom Telefonsignal getrennt und nach einem DSL-Modem als Ethernet weitergegeben.
- Das **Breitbandkabel** ist eine weitere Möglichkeit. Hier wird parallel zum Fernseher ein Kabelmodem angeschlossen, welches das Signal als Ethernet weitergibt.
- **Stand- oder Mietleitungen** sind eine direkte Verbindung zwischen einem Router und dem Provider. Sehr teuer, aber die beste Anbindung. So gibt es die Möglichkeit, Glasfaser- oder Kupferleitungen zu mieten, die Geräte jedoch selbst zu stellen und zu warten.
- Ein Internetzugang kann auch über **Satellit** realisiert werden. I.d.R. läuft der Download über den Satellit, der Upload über das Telefon.
- Auch das **Mobiltelefon** kann mittlerweile ohne Probleme ins Internet und auch als Hotspot dienen.
    - 1990 GSM (2G), 14.4 Kbit/s bis maximal 250 Kbit/s
    - 2000 UMTS (3G), 384 Kbit/s bis maximal 7.2 Mbit/s Download und 1.5 Mbit/s Upload
    - **LTE** ist der Nachfolger von UMTS und wird derzeit entwickelt. Der Fokus liegt auf dem mobilen Internet, Telefonie wird weiterhin problemlos mit UMTS möglich sein. Es sollen Datenmengen von 300 Mbit/s Downl. und 70 Mbit/s Upload möglich sein.
- **WiMax** wird zurzeit vorangetrieben und ist eine Weiterentwicklung von WLAN, ebenfalls ein Standard der IEEE. Gearbeitet wird mit gerichteten Antennen welche Bandbreiten von bis zu 100 Mbit/s erlauben sollen, über 50km Entfernung hinweg.
- Über **Richtfunkverbindungen** werden zwei Gebäude verbunden. Die Antennen senden scharf begrenzt in eine Richtung. Diese machen deshalb nur bei Sichtverbindungen Sinn. Ist ausserdem in den meisten Ländern genehmigungspflichtig.
- Eine Alternative zum Richtfunk sind **Richtlaser**. Sie sind viel schneller und sehr zuverlässig. Eine Sichtverbindung ist notwendig. Auch sie sind meistens genehmigungspflichtig.
- Server, die über das Internet erreichbar sein müssen, können auch **ausgelagert** werden, um so eine eigene schnelle Anbindung zu sparen.

IPv6

- Der Adressraum von IPv4 ist praktisch aufgebraucht (IPv4 = ca. 4.3 Milliarden Adressen)
- NAT / PAT konnten dieses Problem etwas entschärfen
- Es ist jedoch mit einer exponentiell wachsenden Nachfrage nach Adressen zu rechnen (Internet of everything).
- IPv6 Adressen bestehen aus 128 Bit, es gibt also 2^{128} Adressen, $3.4x10^{38}$
- Acht Blöcke à je 16 Bit. Hexadezimale Schreibweise, Trennung durch Doppelpunkte

fe80:0000:0000:0000:2ca8:00d4:3f58:0acf

- Führende Nullen können weggelassen werden, aufeinanderfolgende Blöcke mit Nullen können mit :: zusammengefasst werden. Zusammenfassung Null-Blöcke darf pro Adresse aber nur einmal erfolgen!

fe80::2ca8:d4:3f57:acf

- Die Adresse wird in mehrere Bereiche Unterteilt:

2001:0db8:0000:0001:2ca8:0000:0000:0acf		
2001:0db8:0000	:0001:	2ca8:0000:0000:0acf
Routing Präfix	Subnetz ID	Interface ID

- Bei einer URL wird anstelle der IPv4 Adresse die IPv6 Adresse in eckigen Klammern geschrieben. http://[2001:0db8:0000:0001:0000:0000:0000:0001]:80/
- Die Subnetzmaske, wie wir sie kennen, fällt weg

Adressierung

- In IPv6 wird nicht mehr der Host als solches adressiert, sondern seine Interfaces
- IPv6 kennt verschiedene Adressentypen: Unicast, Multicast und Anycast. Einen Broadcast gibt es in IPv6 nicht mehr.
- Jeder Host braucht für sein Interface in IPv6 eine Link-Local Adresse und eine Loopback-Adresse. Hören muss ein Host auf die „Alle-Hosts-Multicast-Adresse“. Jedes Interface benötigt noch eine Solicited-Node Multicast-Adresse. Für die Kommunikation aus dem eigenen Netz heraus wird eine Global Unicast Adresse benötigt.

Unicast

- **Link Local Unicast-Adresse**
  - Werden gebildet aus einem Präfix FE80::/10 und einer 65-Bit-Interface-ID
  - Jedes IPv6 Interface muss eine solche Adresse besitzen.
  - Sie werden nicht geroutet, sind also nur innerhalb eines Subnetzes erreichbar.
  - Entspricht ungefähr der APIPA Funktion bei IPv4.
- **Global Unicast Adresse:** Weltweit gültige, geroutete Adresse mit denen ein Host im Internet kommuniziert
- **Unique Local Unicast-Adresse**
  - Für diese ist der Bereich FC00::/7 vorgesehen
  - Entsprechen den privaten Adressen in IPv4, also für den internen Gebrauch

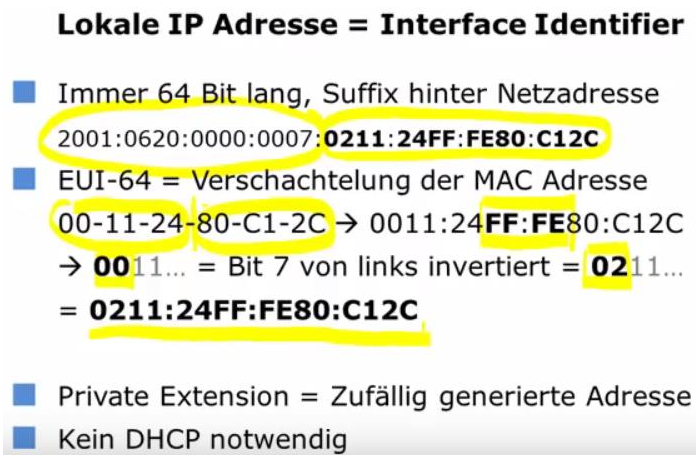
- **Unspecified Adresse**: Äquivalent zu 0.0.0.0/32 in IPv4. Hier gilt allerdings 0000:0000:0000:0000:0000:0000:0000/128 oder ::/128. Wird z.B. beim ersten DHCP Request versendet, wenn der Rechner noch keine Adresse bekommen hat.
- **Loopback:** Dasselbe wie bei IPv4. Aus 127.0.0.1 wird ::1/128
- **IPv4-kompatible Adressen**
  - Für die Kommunikation zwischen IPv4 und IPv6 Netzen müssen die Daten getunnelt werden. Dazu gibt es die Möglichkeit, eine IPv4 Adresse in einer IPv6 Adresse unterzubringen. Aus 131.152.2.150 wird 0000:0000:0000:0000:0000:0000:131.152.2.150 und in korrekter hexadezimaler Schreibweise ::8398:0296.
- IPv4 mapped Adressen: Dual Stack, d.h. Host kommuniziert sowohl mit IPv4 als auch IPv6. Die ersten 80 Bits der IPv6 Adresse sind Nullen, dann folgen 16 Bit FFF, dann die ins hexadezimale konvertierte IPv4-Adresse. Z.B. ::FFFF:8398:0296

Multicast

- Multicast-Adressen stammen aus dem Bereich FF00::/8

Interface-ID

- Die MAC-Adresse wird in die Interface-ID, einem Teil der IPv6-Adresse, integriert
- Dies hat jedoch Nachteile: Ein Gerät wird weltweit beobachtbar. Das Präfix ändert zwar, die Interface-ID bleibt jedoch gleich.
- Lösung: Privacy-Extension, welche die Interface-ID regelmässig ändert. Das ist jedoch der Horror für den Netzwerkadmin: Es wird praktisch unmöglich nachzuvollziehen wer wann welche Adresse hatte etc.



00-11-24-80-C1-2C ist die MAC-Adresse

0011 nehmen und ins binäre umwandeln: 0000 0000 0001 0001, dann 7. Bit von links invertieren: 0000 0010 0001 0001. Wieder in Hex zurückwandeln: 0211

Adressvergabe: Der Weg ins Internet

- Entweder feste Konfiguration durch den Administrator, DHCPV6 oder Autokonfiguration.
- Selbstvergabe einer lokalen Adresse
  - EUI-64 oder Private Extension
  - Link Local Unicast Adresse als Präfix
- Anschliessend Multicast zu allen Routern im LAN (Layer 2) → NDP (Neighbor Discovery Protocol)

- Routern senden ihre Präfixe, mehrere Präfixe möglich.

IPv6-Paket

- Header kann viel Grösser sein als bei IPv4
- Es ist eine Referenz auf einen nächsten Header möglich, dadurch lassen sich diese beliebig hintereinander reihen – so lange bis die Daten folgen.
- Es gibt gegenüber IPv4 keine Checksum mehr! Dies wurde an höhere Layer delegiert. Dadurch werden die Router entlastet.

Version	Traffic-Class			Flow-Label		
	Payload-Length		Next Header		Hop-Limit	
Source-Adress						
Destination-Address						
Extension-Header						
Data						

- Traffic Class: Die Priorität, ,für Quality of Service
- Flow Label: Labeling von Flows, Pakete aus Strömen mit gleicher Behandlung

Kommunikation beider Welten

- Dual-Stack: IPv4 und IPv6 werden parallel betrieben
- Kommunikation zwischen den beiden Protokollen erfordert Tunnels. Dafür gibt es einige Verfahren:

Encapsulierung

Um ein IPv6 Paket über ein IPv4 Netzwerk zu transportieren, wird es in den Payload eines IPv4 Pakets eingebaut.

Automatische Tunnel

6to4

- Kommunikation über Router, die für 6to4 und IPv6 konfiguriert sind.
- Der 6to4 Gateway encapsuliert das IPv6 Paket in IPv4. Es wird im IPv4 Netz ganz normal geroutet. Am Zielpunkt stellt der zweite Gateway das IPv6 Paket wieder her.

ISATAP

- ISATAP: Intra-Site Automatic Tunnel Adressing Protocol
- Kommt zum Einsatz wenn IPv6 Pakete zwischen Dual-Stack Knoten transportiert werden solche, die jedoch über ein IPv4-Netzwerk verbunden sind.
- Dafür wird die IPv6 Adresse aus der IPv4 Adresse gebildet. Die IPv4 Adresse wird dabei in der Interface ID der IPv6 Adresse eingebaut.

Teredo

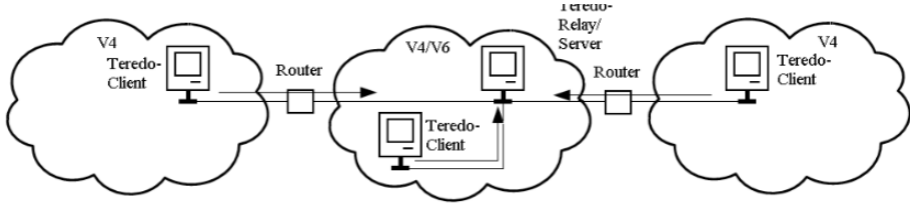


BILD 10.7 Im ersten Schritt nehmen die Teredo-Clients Kontakt zu einem Teredo-Server auf (UDP, IP V4). Dies kann auch über NAT erfolgen.

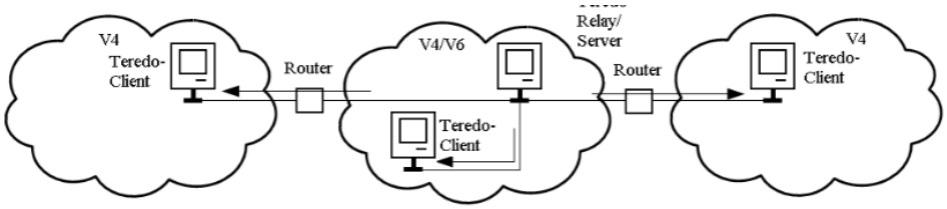


BILD 10.8 Der Teredo-Server sendet den Clients ein IP V6-Adresspräfix zu, aus dem sie sich eine IP V6-Adresse zusammensetzen.

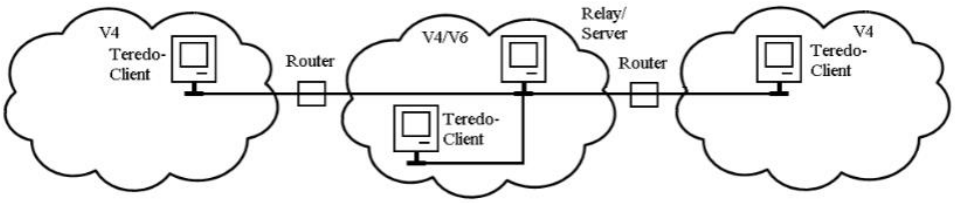


BILD 10.9 Ab diesem Zeitpunkt können die Teredo-Clients ihre IP V6-Pakete encapsuliert in IP V4 UDP an das Teredo-Relay senden. Dieses reicht sie weiter. So können Rechner in einem IP V4-Netz eine IP V6-Kommunikation aufbauen. Durch den Teredo-Server kann nicht nur mit anderen Teredo-Clients kommuniziert werden, sondern auch mit IP V6-Hosts. Da die Verbindungen der Clients „von innen nach außen" aufgebaut werden und der Teredo-Server als Relay fungiert, ist diese Kommunikation auch durch NAT und Firewalls möglich. Was die Sicherheit anbelangt, ist dies ein Albtraum.

Abkürzungen / Begriffe

- ISO: International Standardization Organisation
- OSI: Open Systems Interconnection
- LAN Local Area Network
- MAN Metropolitan Area Network
- WAN Wide Area Network
- Protokoll: Vereinbarung über die Rahmenbedingungen
- Konvergenz: Bei Störungen und Defekten an den Verkehrsverbindungen oder Netzwerkgeräten muss ein globales Netzwerk in der Lage sein, von selbst redundante Wege zu aktivieren und di Datenübertragung sicherzustellen.

Layer I

- Bussystem: Datenübertragungssystem, das aus einem durchgängigen Strang Medium besteht, den sich verschiedene Kommunikationsgeräte teilen)
- UGV Universelle Gebäudeverkabelung
- MDI: Media Dependent Interface → Erkennen, ob ein Netzwerkgerät oder ein Client angeschlossen ist und je nach dem die Pinbelegung umschalten.
- CSMA/CD: Carrier Sense Multiple Access / Collision Detection
- CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance
- DEEE: Datenendeinrichtung (z.B. Client)
- DÜE: Datenübertragungseinrichtung
- NTBA: Network Termination for ISDN Basic rate Acces
- NIC: Network interface card
- RTS: Ready to send
- CTS: Clear to send
- Bitrate: Anzahl Bits die pro Sekunde übertragen werden
- Baudrate: Anzahl Symbole die pro Zeiteinheit übertragen werden. Symbol benötigt 0.2 Sekunden zum Übertragen → 5 Baud.
- Bandbreite: Gesamter Frequenzbereich, der zum Senden zur Verfügung steht. In Hz, wobei 1 Hz = 1/s (1 Schwingung pro Sekunde)
- Übertragungsrate: Anzahl der pro Sekunde übertragbaren Bits -→ bit/s
- LWL: Lichtwellenleiter

Layer II

- MAC: Medium Access Control
- ARP: Address Resolution Protocol
- SFD: Starting Frame Delimiter
- DMAC: Destination MAC
- SMAC: Source MAC
- FCS: Frame Check Sequence
- Promiscuous Mode: Ein Modus der Netzwerkkarte, welcher es erlaub, alle Frames im Netzwerk entgegenzunehmen, nicht nur die welche an die eigene MAC adressiert sind.
- BPDU: Bridge Priority Data Units

Layer III

- IANA: Internet Assigned Numbers Authority
- APIPA: Automatic Private IP Adressing

- MTU: Maximum Transport Unit
- VLSM: Variable Length of Subnet Masks
- RIP: Router Information Protocol. Routing-Protokoll auf Basis des Distanzvektoralgorithmus (Kosten berechnen), das innerhalb eines autonomen Systems (z.B. LAN) eingesetzt wird, um die Routingtabellen von Routern automatisch zu erstellen.
- FQDN: Fully Qualified Domain Name
- DNS: Domain Namen System
- DHCP: Domain Host Configuration Protocol
- SMB: Server Message Block

Layer IV

- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- NAT: Network Address Translation
- PAT: Port and Address Translation

WLAN

- SSID: Service Set IDentifier
- WEP: Wired Equivalent Privacy
- WPA: Wi-Fi Protected Access
- PoE: Power over Ethernet
- WECA-Vereinigung: Wireless Ethernet Compatibility Alliance
- Wi-Fi: Wireless Fidelity (Marketing-Wort), vergeben das Wi-Fi Logo als Zertifizierung für WLAN-Geräte.
- VoIP: Voice over IP
- SIP: Session Initiation Protocol
- RTP: Real-Time Transport Protocol

Netzzugang, Szenarien

- ISDN: Integrated Services Digital Network
- DSL: Digital Subscriber Line
- ADSL: Asymmetric Digital Subscriber Line
- GSM: Global System for Mobile Communication (2G)
- UMT: Universal Mobile Telecommunication System (3G)
- LTE: Long Term Evolution
- WiMax: Worldwide Interoperability for Microwave Access
- ASIC: Application Specific Integrated Circuits (z.B. Hardware-Firewall oder Router, der Hardware En- und Decoder besitzt die viel schneller arbeiten als Software En- und Decoder)
- PPP: Point to Point Protocol
- PAP: Password Authentication Protocol
- CHAP: Challenge Handshake Authentication Protocol

ICMP: Internet Control Message Protocol. Gehört zum Internet Protocol. Es gibt 255 verschiedene ICMP-Pakete, die ID steht jeweils am Anfang des ICMP Headers. Bekannteste: Echo Request (ID 8), Echo Reply (ID 0)