**Kommunikation** 3
Definition Telematik 3
Kommunikationsarten 3
Verbindungsarten 3

**Übertragungsmedien** 4
Grafik Freier Raum 4
Grafik Leitergebunden 4
Koaxial 4
Twisted Pair 4
Lichtwellenleiter 4

**Übertragungsarten** 5
Datenbreite 5
Frequenzmultiplexen 5
Zeitmultiplexen 5
Wellenlängenmultiplexen 5
Datenstrom 5
Datenbasis 5

**Vernetzung** 6
Netzverbund 6
Vorteile Netzverbund 6
Netz-Ausdehnungen 6

**LAN-Topologien** 7
Definition Topologie 7
Bus 7
Ring 7
Stern 7
Maschennetz 7
Baum 7
UGV 7

**LAN-Technologien** 8
IEEE 8
Standard 802 8
802-Spezifikationen 8
Ethernet 8
Token Passing 8
FDDI 8

**LAN-Konzepte** 9
Geschichte der DV 9
Peer-to-Peer-Netze 9
Fileserver 9
Client/Server-Netze 9
Server-Funktionen 9
Client/Server-Architekturen 9
Client/Server-Modelle 9
Client/Server-Prinzipien 9

**WAN-Dienste** 10
Standleitung 10
Mietleitung 10
Wählverbindung 10
Drahtlose Verbindungen 10
WLAN 10

**Netzwerkkomponenten** 11
Hub 11
Repeater 11
Bridge 11
Switch 11
Router 11
Routing 11
Gateway 11

**Firewall** 12
Definition Firewall 12
Firewall-Techniken 12

Paketfilter 12
Stateful Inspection SIF 12
Circuit Level Gateway Proxy 12
Application Level Firewall ALF 12
Reverse Proxy 12

**Virtual Private Network VPN 13**
Verwendung VPN 13
Funktionsweise VPN 13
Firewalls bei VPN 13
Grafik VPN 13

**Kryptographie 14**
Definitionen 14
Symmetrische Verschlüsselung 14
Asymmetrische Verschlüsselung 14
Hybride Verschlüsselung 14
Digitale Signatur 14
Steganographie 14
Quantenkryptographie 14

**ISO/OSI-Modell 15**
Protokollschichten 15
Definition Protokoll 15
Kommunikationsverlauf 15
TCP/IP 15
TCP/IP-Protokolle 15
Requests for Comments RFC 15

**Physical Layer 16**
Aufgabe 16
Sublayers 16
Analoge Signale 16
Digitale Signale 16
Modulation 16
Störungen 16

**Data Link Layer 17**
Aufgaben 17
Sublayers 17
MAC-Adresse 17
Zugriffssteuerungs-Verfahren 17
Forward Error Control FEC 17
Feedback Error Control 17

**Network Layer 18**
Aufgaben 18
Vermittlung 18
IP-Adresse 18
IP-Adressklassen 18
Spezielle IP-Adressbereiche 18
Subnetz-Maske 18

**Transport Layer 19**
Aufgabe 19
Transport-Protokolle 19

**Session Layer 20**
Aufgabe 20

**Presentation Layer 21**
Aufgabe 21
Zeichensätze 21
Verschlüsselung 21
Komprimierung 21

**Application Layer 22**
Aufgabe 22

# Kommunikation

TECH

## Definition Telematik

Telematik: Übermittlung von Information über Distanz

- Telekommunikation: Kommunikation über Distanz
  - Tele: fern
  - Kommunikation: Datentransfer zwischen Sender und Empfänger über Übertragungsmedium
- Informatik: Eingabe, Verarbeitung und Ausgabe von Daten
  - Information: nutzbares Wissen mit Neuigkeitswert
  - Automatik: selbststeuernd

## Kommunikationsarten

- Point to Point:
  Punkt zu Punkt, z.B. Peer to Peer, Telefon
- Multicast:
  Punkt zu Gruppe, z.B. Client-Server
- Broadcast:
  Punkt zu allen, keine Adressierung, Teilnehmer unbekannt
  z.B. Radio

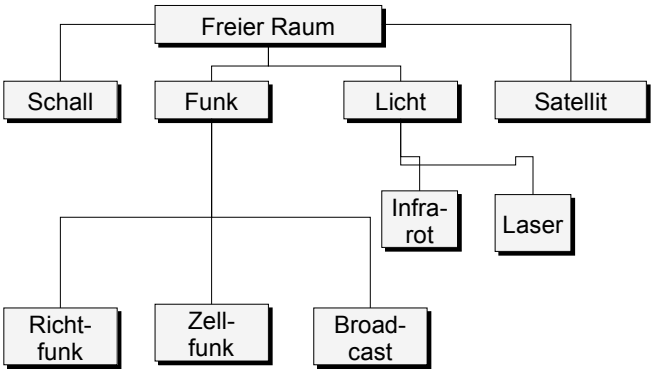
## Verbindungsarten

- SX (simplex):
  nur eine Richtung
  z.B. Radio, Fernsehen, Maussignal
- HDX (half duplex):
  abwechslungsweise, nur eine Frequenz / ein Kanal
  z.B. Funk
- FDX (full duplex):
  gleichzeitig senden und empfangen, zwei Frequenzen
  z.B. Mobiltelefon

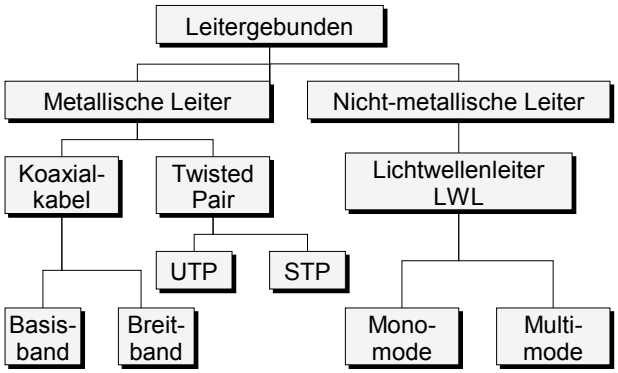
# Übertragungsmedien

TECH

## Grafik Freier Raum




## Grafik Leitergebunden




## Freier Raum

Schall: Ultraschall

Funk: Bluetooth, WLAN
Zellfunk: Mobiltelefon
Broadcast: Radiosender

Infrarot: TV-Fernbedienung

## Koaxial

Hochfrequenzkabel (HF)
für Neuinstallationen kaum noch eingesetzt

- Basisband:
  nur ein Kanal / Sender auf der ganzen Bandbreite
  Verwendung: Ethernet

- Breitband:
  Einteilung in Frequenzbänder für mehrere Kanäle / Sender
  Frequenzmultiplex: Hoch- / Zurückschieben der Frequenz
  Verwendung: Kabelfernsehen, Radioempfänger

## Twisted Pair

Niederfrequenzkabel (NF)
für kleine Übertragungsraten, kurze Kabellängen

verdrehte Paare von Kupferdrähten:
- kleiner Widerstand dank immer gleichem Abstand
- reduziert elektromagnetische Interferenzen

für LAN-Bereich
strukturierte Gebäudeverkabelung mit RJ-45-Stecker
(Registered Jack, genormter Stecker)

- unshielded: günstig, max. 100 m, Ethernet
- shielded: Abschirmungsfolie für jedes Drahtpaar

## Lichtwellenleiter

haardünner Glasfaden, leitet Licht

Vorteile:
- hohe Übertragungsgeschwindigkeiten
- grosse Reichweiten
- Resistenz gegenüber elektromagnetischen Störungen
- hohe Abhörsicherheit (strahlt nicht ab)

- monomode:
  MAN/WAN Standleitungen, teuer
  bis 100 km ohne Verstärkung
- multimode:
  LAN, bis 2 km ohne Verstärkung
  günstiger

# Übertragungsarten

TECH

## Datenbreite

Seriell:
- sequentiell, hintereinander bitweise
- z.B. Tastatur, Maus, USB Universal Serial Bus

Parallel:
- z.B. 1 Byte = 8 Bits gleichzeitig
- v.a. über kurze Strecken, z.B. Drucker

## Frequenzmultiplexen

Frequency Division Multiplexing FDM

- Zusammenführen von Kanälen
- Aufteilung der Frequenz-Bandbreiten
- Übertragungsrate vor und hinter Multiplexer gleich
- für Breitband-Kupferkabel

## Zeitmultiplexen

Time Division Multiplexing TDM

- Aufteilung in Zeitschlitze für Pakete mit Zieladresse
- Übertragungsrate hinter Multiplexer n mal grösser
- für Lichtimpulse in Glasfaserkabeln
- nur digitale Daten
- ca. 300 MB/s möglich

## Wellenlängenmultiplexen

Wavelength Division Multiplexing WDM
Dense Wavelength Division Multiplexing DWDM

- Aufteilung des Lichts nach Wellenlängen, Spektralfarben
- Prismen am Leitungsanfang und -ende
- Linsen im Kabel zur Verhinderung von Diffusion (früher alle 30 km elektrische Verstärker, brauchte Strom und ständige Umwandlung elektrische/optische Signale)
- halbdurchlässige lichtneutrale Spiegel für Verzweigungen
- für Transatlantik-Verbindungen
- 8 mal 3 GB-Kanäle (bzw. 32 mal für DWDM)

## Datenstrom

Asynchron:
- nur zeitweise Datenübertragung
- benötigt keine Taktgeberinformation
- benötigt Start- und Stopbits
- z.B. Tastatur

Synchron:
- kontinuierliche Datenübertragung
- benötigt Synchronisationsinformation
- für grössere Dateien oder Übertragungsraten

## Datenbasis

(Level 2)

Zeichenorientiert:
- anhand Code-Tabelle (z.B. ASCII)
- Steuerzeichen STX und ETX (start und end of text)
- Character stuffing zur Unterscheidung von Steuerzeichen
- z.B. Tastatur, einige Drucker

Bitorientiert:
- Strukturierung in Frames oder Cells
- Framebegrenzung mit opening und closing flags
- Bit stuffing zur Unterscheidung von Steuerflags

# Vernetzung

TECH

## Netzverbund

gemeinsame Nutzung von:
- Datenbeständen
- Peripheriegeräten
- Programmen

## Vorteile Netzverbund

- Kostenvorteile
- Arbeitsteilung
- Kommunikation
- bessere Verfügbarkeit durch Redundanz
- Lastenausgleich
- höhere Rechenleistung

## Netz-Ausdehnungen

- PAN Personal Area Network: Bluetooth, Infrarot
- LAN Local Area Network: Ethernet, WLAN
  gleiches Gebäude / Grundstück
  nicht über öffentlichen Grund
  vom Eigentümer betrieben und genutzt
- MAN Metropolitan Area Network: asynchronous tranfer mode ATM, gleiche Stadt
  öffentliches Netz, beliebig viele Benutzer
- WAN Wide Area Network: gleiches Land / Kontinent
  verbindet autonome Systeme
- GAN Global Area Network: auf der ganzen Erde

# LAN-Topologien

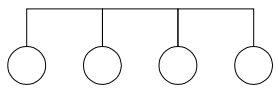
TECH

## Definition Topologie

Physikalischer Aufbau des Netzes, Verbindung der Netzwerkknoten untereinander.

- Knoten (node): Datenverarbeitungssystem für die Vermittlung und Übertragung von Daten
  z.B. Arbeitsstationen, Server, Grossrechner, Gateways, bzw. deren Netzwerkkarte
  - passiv: ohne Signalweiterleitung, z.B. Splitter
  - aktiv: mit Signalweiterleitung, z.B. Repeater, Bridge, Router, Hub
- Verbindung (connection): physikalische Verknüpfung zwischen Knoten in einem Netzwerk, Kabel oder drahtlos

## Bus

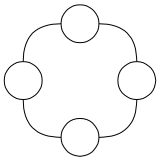


Verwendung:
- Zentralkabel mit Terminatoren
- Hub, Stromsteckdose
- Broadcast, z.B. Fernsehen, Radio

Vorteile:
- einfache Montage
- gute Erweiterbarkeit
- günstig (Koaxial)

Nachteile:
- keine Signalregenierung
- beschränkte Kabellänge
- unterbruchsanfällig
- Datenverlustrisiko

## Ring

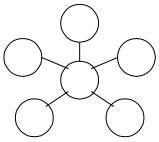


Verwendung:
- höchstens noch im Serverbereich
- früher Twisted Pair, heute Glasfaser

Lösungen:
- Token Ring: Ring wird bei Ausfall geschlossen, Token teilt Zeit ein
- doppelter Ring als Backup

Nachteile:
- Durchlauf bis zu n-2 Knoten
- Ausfallrisiko bei jedem Knoten

## Stern

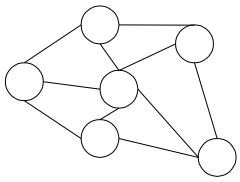


Verwendung:
- Hub als zentraler Knoten
- heute am üblichsten

Vorteile:
- Ausfall einzelner macht nichts
- relativ günstig (Twisted Pair)

Nachteile:
- Hub ist Flaschenhals
- schlechte Performance
  Lösung: Switch
- viele Leitungen
  Lösung: Segmentierung

## Maschennetz

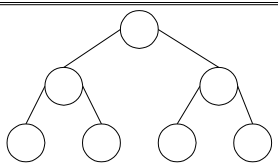


Verwendung:
- direkte Verbindungen
- Internet, WAN, Telefonnetz
- Weitverkehrsnetze

Vorteile:
- hohe Ausfallsicherheit
- flexibel, erweiterbar

Nachteile:
- viele Leitungen
- teuer

## Baum



Verwendung:
- hierarchische Struktur, Segmentierung mehrerer Sterne
- Grossrechnernetze
- komplexe Netze

Vorteile:
- Ausfall einzelner macht nichts
- relativ günstig (Twisted Pair)
- leicht erweiterbar

Nachteile:
- Ausfallrisiko

## UGV

Universelle / strukturierte Gebäudeverkabelung

Patchfeld mit RJ45-Steckdosen von dem aus alle Arbeitsplätze sternfömig verbunden werden.
Flexibel durch einfaches Umstecken der Kabel.

Transparente Verkabelungsstruktur:
- Primär-Verkabelung:
  Geländeverkabelung, Campus Backbone, LWL
- Sekundär-Verkabelung:
  Gebäudeverkabelung, Building Backbone, LWL
- Tertiär-Verkabelung:
  Etagenverkabelung, Horizontal Subsystem, UTP/STP

## IEEE

Institute of Electrical and Elektronics Engineers

- Organisation von Fachleuten und Experten aus der Elektrotechnik und dem Ingenieurwesen
- weltweit führende Organisation für die Standardisierung im Bereich Elektronik und Informationstechnik

## Standard 802

Projekt für die Standardisierung von Netzwerken, begann im Februar 1980.

- Spezifikationen für LAN-Technologien
- aufgeteilt in Arbeitsgruppen
- hauptsächlich für Übertragungsprotokolle auf Layer 1 / 2

## 802-Spezifikationen

802.1 LAN-Management
802.2 Logical Link Control
802.3 Ethernet, CSMA/CD, Fast Ethernet, Gigabit Ethernet
802.4 Token Passing Bus
802.5 Token Passing Ring, FDDI, Glasfaser
802.6 MAN
802.10 Security
802.11 Wireless LAN
802.15 Wireless PAN
802.16 Wireless MAN

## Ethernet

- Verwendung in Bus-Netzen
- carrier sense multiple access with collision detection CSMA/CD, Überprüfung der Netzwerkaktivität vor dem Senden, bei Kollision Jam-Signal
- carrier sense multiple acces with collision avoidance CSMA/CA

## Token Passing

- Token: übergibt Sendeberechtigung, besteht aus 3 Bytes: Starting Delimiter, Access Control Byte, Ending Delimiter
- braucht definierten Vorgänger und Nachfolger
- komplex, aber sicher

## FDDI

Fiber distributed data interface

- doppelter Ring mit LWL
- Sekundärring als Backup
- geeignet für Backbone

# LAN-Konzepte

TECH

## Geschichte der DV

| | |
|---|---|
| 60er Jahre: | isolierte Grossrechnerlösungen |
| 70er Jahre: | Terminals vom Grossrechner getrennt |
| 80er Jahre: | Einzelplatz-PCs mit eigener Software (Downsizing) |
| 90er Jahre: | Vernetzung der PCs |
| 2000er: | Client-Server-Architektur (Rightsizing)<br>Server: Dienstanbieter, Client: Dienstnutzer |

## Peer-to-Peer-Netze

- alle Stationen sind gleichzeitig Server und Client
- gemeinsame Nutzung verfügbarer Ressourcen
- Workgroup ohne Management
- geeignet für wenig Teilnehmer
- Variante: Server nur am Anfang als Vermittler
- Vorteil: kostengünstig
- Probleme: Integrität, Vertraulichkeit
- Beispiele: Windows 95, EasyLAN

## Fileserver

- Server ist verantwortlich für Datenspeicherung, Dateiverwaltung, Session Management
- Arbeitsplatzrechner liefern die Rechenleistung (Daten abladen, bearbeiten, zurückladen)
- Unterteilung in Netzsegmente mit Bridges für bessere Leistungsfähigkeit
- Probleme:
  - unterschiedliche Netzwerkbelastung
  - Datenintegrität, Lösung Daten-Replikation
  - Verfügbarkeit (File locking)
- Vorteile: leicht zu implementieren, preisgünstig

## Client/Server-Netze

- Back end: Server-Software, Grossteil der Rechenleistung
- Front end: Client-Software, Schnittstelle zum Benutzer
- Datenänderungen werden den anderen Clients sofort zur Verfügung gestellt (Render Service)
- geeignet für grosse Teilnehmerzahlen
- Nachteile: aufwändig, teuer
- Vorteile: schneller, stetige Netzwerkbelastung, Sicherheitskonzepte

## Server-Funktionen

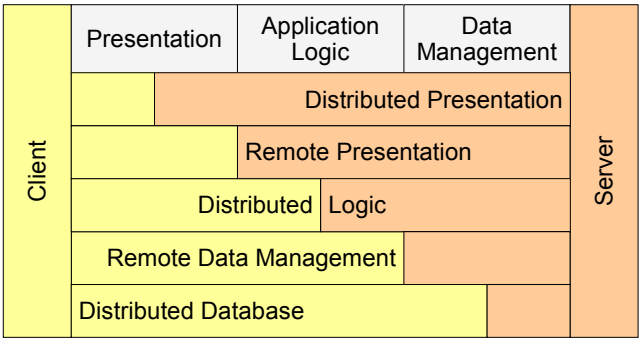
- Print Server (Druck-Server):
  Abarbeitung von Druckaufträgen über Print-Queue
  Vorteil: Jobs gehen nicht verloren
- Application Server (Anwendungsserver):
  Applikationen laufen ganz oder teilweise auf dem Server
- Communication Server (Kommunikationsserver):
  ermöglicht Kommunikation aus LAN heraus

## Client/Server-Architekturen

Funktionsbezogene Aufteilung durch n-tier (Knoten) Architekturen.

- 2tier: Client – Server
- 3tier: Client – Applikationsserver – DB-Server
  (der Appl.Server ist Client gegenüber dem DB-Server)
- 4tier: Client – Webserver – Appl.Server – DB-Server

## Client/Server-Modelle




## Client/Server-Prinzipien

- fat client / thin server:
  z.B. Lotus Notes
- thin client / fat server:
  z.B. Browser / Webserver, aber Javascript und Java sind Client Enhancements

# WAN-Dienste

TECH

## Standleitung

- dedicated line
- permante Verbindung über eine Zentrale
- exklusive Punkt-zu-Punkt-Verbindung
- Nahverkehr, max. 10 km
- Kosten übertragungsunabhängig
- Übertragung von Daten, Bildern und Sprache
- z.B. xDSL Digital Subscriber Line

## Mietleitung

- leased line
- permanente Verbindung über mehrere Zentralen
- Breitband-Verbindung für mehrere Benutzer
- für grosse Distanzen
- Kosten gemäss SLA, geschwindigkeits-, zeiten-, bandbreitenabhängig

## Wählverbindung

- Leitungsvermittlung
- Verrechnung für Verbindungszeit

z.B. PSTN Public Switched Telephone Network:
- POTS Plain Old Telephone System (analoge Telefonie)
- ISDN Integrated Services Digital Network

## Drahtlose Verbindungen

- Richtstrahl:
  gerichteter Funkstrahl, z.B. Elektrizitätswerke
  braucht direkte Sichtverbindung
  oder Relais-Funktionen auf dem Berg

- Laser:
  braucht Sichtverbindung
  Nebel macht das Licht diffus

- Satellit:
  Distanz 35-40'000 km, Signallaufzeit gegen 1 Sekunde
  z.B. Life-Schaltung im Fernsehen (leichte Verzögerung)

## WLAN

Wireless LAN

Verschlüsselungen:
- Wired Equivalent Privacy WEP: basiert auf RC4,
  64 / 128 bit, aber 40 bit Initialisierungsvektor, knackbar
- Wi-Fi Protected Access WPA: Nachfolger von WEP,
  basiert auf RC4, aber tauscht Schlüssel regelmässig aus
- WPA2: basiert auf AES

# Netzwerkkomponenten

TECH

## Hub

zentraler Knoten in Sternverbindung,
Bezeichnung für verschiedene Verteilerkomponenten,
sagt nichts über Funktion aus
Access Point: drahtloser Hub, kommuniziert über Funk

Grössenordnungen:
- Workgroup Hub: Repeater, Bridge, L2-Switch
- Departmental Hub: Bridge, Switch
- Enterprise Hub: Switch, Router

## Repeater

Layer 1
Signalverstärker, eigentlich physische Verbindung
nur für Segmente mit gleichem Netztyp
Kollisionen pflanzen sich in andere Segmente fort

## Bridge

Layer 2
Aufteilung in Subnetze zur Verminderung der Netzlast
Filter verhindert Fortpflanzung von Kollisionen
Weiterleitung an anderes Subnetz anhand MAC-Adresse
Verbindung unterschiedlicher Geschwindigkeiten, L2-Protokolle und Medien möglich
Verwaltung durch Selbstlernalgorhythmen

## Switch

Layer 2 (Frames) / 3 (Pakete)
Multiport-Bridge (Bridge auf jedem Port)
ermöglicht unterschiedliche Geschwindigkeiten und Zeitmultiplex pro Port
gezielte Verbindung zwischen zwei Stationen, abhörsicher

## Router

Layer 3
Verbindung geografisch getrennter Netzwerke
Übergang LAN-WAN
häufig kombiniert mit Modem, z.B. ADSL-Router

Network Address Translation NAT:
- setzt public IP-Adresse in private Netzwerkadresse um, z.B. 192.168.1.0, Netzwerk erscheint als einzelner Computer
- innerhalb des Subnetzes wird direkt geschickt, z.B. 192.168.1.2
- nach aussen an die Gateway-Adresse des Routers, z.B. 192.168.1.100

## Routing

- Adressanfrage über alle Knoten (Broadcast Storm)
- die schnellste Antwort bestimmt den Sendeweg
- default 30 Hops über Router, aber einstellbar
- Speicherung in Routing Tables
- automatisch anderer Weg bei Überlastung / Änderung (Pakete können sich überholen)
- Reset beim Ausschalten

## Gateway

Layer 7
Bezeichnung für verschiedene Netzwerkeinrichtungen, dient als Übergang, Implementation z.B. als Router oder Netzwerkkarte.

- Routing-Eintrag
- Übergang zwischen verschiedenen Applikations-Protokollen
- Verbindung unterschiedlicher Datenformate
  z.B. Windows NT – Novell, PC – Host – LAN

# Firewall

TECH

## Definition Firewall

Kombination Router / Gateway / Router.

Zugriffskontrollsystem zwischen zwei Netzen (intern / extern).

Gateway, einziger Durchgang zwischen geschütztem / vertrauenswürdigem Netz (LAN) und ungeschütztem / nicht vertrauenswürdigem Netz (Internet).

## Firewall-Techniken

- Paketfilter: Layer 3
- Stateful Inspection: Layer 3/4
- Circuit Level Gateway (Proxy): Layer 4
- Application Level Gateway: Layer 7
- Reverse Proxy: Layer 7

## Paketfilter

Filter-Regeln für Header-Informationen:
- Erlaubte Ports, d.h. Services (http, smtp, ftp etc.)
- Erlaubte Quelle (IP-Adresse, optional)
- Erlaubtes Ziel (IP-Adresse, optional)

Reaktionen:
- allow. Paket wird durchgelassen
- deny / drop: Paket wird verworfen, Sender bekommt Timeout oder keine Meldung
- reject: Paket wird zurückgewiesen, Sender bekommt eine Fehlermeldung

## Stateful Inspection SIF

- berücksichtigt aktuelle Status- und Kontextinformationen
- nimmt nur aus dem LAN initiierte Verbindungen an
- prüft Übereinstimmung mit den TCP/IP-Regeln
- Log-Files
- schützt vor DoS und manipulierten TCP/IP-Protokollen

## Circuit Level Gateway Proxy

Funktion eines Proxyservers, Verbindungs-Gateway zwischen Client und Server, hat zwei Netzwerkkarten.

- Address Translation:
  trennt die Verbindung zwischen LAN und Internet und handelt als Stellvertreter der jeweiligen Seite
- Authentisierung bei Zugriffen von ausserhalb
- Autorisierung
- Verschlüsselung
- Cache (Zwischenspeicher), spart Traffic

## Application Level Firewall ALF

- paketübergreifende, applikatorische Filterung
- Viren- und Contentfilterung
- Nutzungsprofile
- Alarmierung
- Nachteil: schlechtere Performance
- Lösung: Entlastung durch Router mit Paketfilter

## Reverse Proxy

- Session-Management und Mapping von IP-Adressen
- Content Rewriting in protokollkonformen Code, filtert Angriffe
- Entschlüsselung, entlastet Applikationsserver, ermöglicht dem IDS das Lesen
- für schützenswerte Systeme mit Zugriff von aussen (bei redundanter Datenhaltung im DMZ nicht relevant)
- geeignet für heterogene, verteilte, transaktionsorientierte und nicht webfähige Systeme
- z.B. für Internet-Shopping, E-Banking

# Virtual Private Network VPN

TECH

## Verwendung VPN

- Host-to-Net: Kopplung zweier Unternehmensstandorte
- Client-to-Net: Verbindung Aussendienstmitarbeiter mit LAN
- günstige Alternative zu klassischen Dial-In / Remote Access-Lösungen
- braucht Ipsec-Software auf Clients
- aufwändige Konfiguration

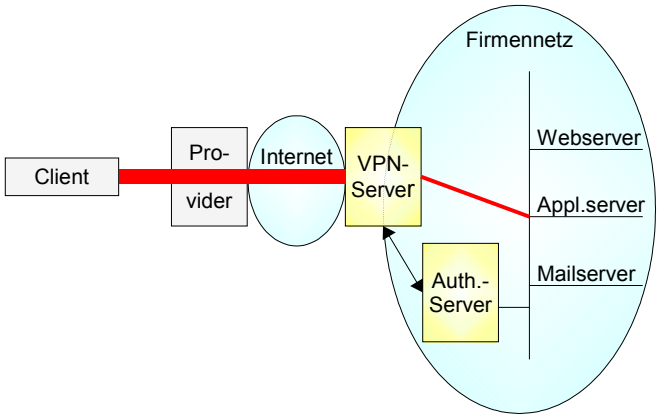
## Funktionsweise VPN

- Verbindung zum Internet über beliebigen Provider, z.B. mit Point-to-Point Protocol PPP
- Verbindung zwischen VPN-Client und VPN-Server, Anmeldung z.B. mit Token, Smart-Card, dig. Zertifikat
- Pakete werden verschlüsselt
- Authentisierungsprüfung beim VPN-Server
- sichere Datenverbindung (IPsec-Tunnel) zum VPN-Server
- gesicherte Verbindung zu beliebigem Rechner im Firmennetz

## Firewalls bei VPN

- Client:
  bekommt eine IP-Adresse aus dem Firmennetzwerk, vom Internet aus nicht mehr sichtbar, braucht deshalb keine Desktop-Firewall
- VPN-Server:
  hat keine offenen Ports ausser UDP 500 für den Schlüsselaustausch, sowieso kein Content-Check möglich, Firewall würde nur Performance reduzieren und Geld kosten
- Firmenseite:
  bei Bedarf Firewall, schützt aber Daten im Intranet nicht

## Grafik VPN



# Kryptographie

TECH

## Definitionen

Kryptographie: Verschlüsselungstechnologien
plaintext: Klartext
ciphertext: Chiffrat

Kryptoanalyse: Verfahren zur Entschlüsselung ohne Kenntnis des Schlüssels
Brute Force Attack: Durchprobieren aller Möglichkeiten

Algorithmen (Verschlüsselungsmethoden):
- Cäsar-Methode: Verschiebung im Alphabet
- Substitution: Zeichenaustausch
- Transposition: Reihenfolgenaustausch

## Symmetrische Verschlüsselung

- Verschlüsseln und Entschlüsseln mit gleichem Schlüssel
- Schlüssellänge 128 bit gilt heute als sicher ($2^{128}$ Kombinationen)
- Nachteile:
  - riskante Schlüsselverteilung
  - viele verschiedene Schlüssel
- Algorithmen: Data Encryption Standard DES (nur 56 bit), 3DES, AES, IDEA

## Asymmetrische Verschlüsselung

- Privater Schlüssel: 1024 – 4096 bit
- Öffentlicher Schlüssel: 128 bit, im Webbrowser integriert
- Nachteil: schlechte Performance
- Vorteil: nur ein Chiffrat für alle Empfänger
- Algorithmen: RSA

Funktionsweisen:
- Verschlüsselung mit öffentlichen Schlüssel(n): nur berechtige Personen können entschlüsseln (Vertraulichkeit)
- Verschlüsselung mit privatem Schlüssel: garantiert die Integrität des Absenders (Authentifikation)
- Fingerprint: Hashwert des Private Keys, zur raschen Überprüfung

## Hybride Verschlüsselung

- Generierung symmetrischer Session Key für die Daten
- asymmetrische Verschlüsselung des Session Keys mit Public Key des Empfängers
- Datenübertragung symmetrisch

## Digitale Signatur

Absender:
- bildet Hashcode: unumkehrbare, zufällige, eindeutige Prüfsumme des Texts mit fixer Länge
- verschlüsselt Hash-Wert mit privatem Schlüssel garantiert die Authentizität des Absenders
- oder message authentication code MAC: Einweg-Hashfunktion mit Schlüssel

Empfänger:
- bildet auch Hashcode des Texts
- vergleicht mit entschlüsseltem Hashcode: garantiert die Integrität des Textes

## Steganographie

Verschlüsselung in Bild / Ton.

## Quantenkryptographie

- Quantenbits können zwei Zustände gleichzeitig haben (Katze in Box ist tot und lebendig)
- beim Nachsehen / Messen wird der Zustand festgelegt und kann nicht mehr geändert werden
- wird der Quantenschlüssel unterwegs geöffnet, merkt das der Empfänger
- Problem: Widerstand in Leitungen festigt den Zustand bis ca. 100 km geht es

# ISO/OSI-Modell

TECH

## Protokollschichten

| | | |
|---|---|---|
| Application Layer | -------- 7 -------- | Anwendungsschicht |
| Presentation Layer | -------- 6 -------- | Darstellungsschicht |
| Session Layer | -------- 5 -------- | Sitzungsschicht |
| Transport Layer | -------- 4 -------- | Transportschicht |
| Network Layer | -------- 3 -------- | Vermittlungsschicht |
| Data Link Layer | -------- 2 -------- | Verbindungsschicht |
| Physical Layer | -------- 1 -------- | Bitübertragungssch. |
| Übertragungsmedium | | |

## Definition Protokoll

Kommunikationsvorschrift, definiert die Abläufe in den einzelnen Schichten, nach denen Programme dann eine Kommunikation aufbauen und durchführen.

OSI: open systems interconnection,
Referenzmodell für herstellerunabhängige Netzwerkprotokolle

Merkspruch: **A**ll **p**eople **s**eem **t**o **n**eed **d**ata **p**rocessing.

L5-7: anwendungsorientiert
L1-4: transportorientiert

www.protocols.com

## Kommunikationsverlauf

- Sendseite: von L7 über Schnittstellen zu L1
  jede Schicht fügt dem von oben erhaltenen Datenpaket eigene Protokollinformationen hinzu
- Übertragung: physisch mittels Übertragungsmedium
- Empfangsseite: von L1 über Schnittstellen zu L7
  jede Schicht verarbeitet die Protokollinformationen ihrer Ebene und entfernt sie vor der Weitergabe nach oben
- jede Schicht stellt der darüberliegenden Schicht Dienste zur Verfügung

## TCP/IP

Transmission Control Protocol / Internet Protocol
ist kein OSI-Protokoll

L7: Process / Application Layer
L6: fehlt, in L7 integriert, z.B. mit Secure Socket Layer
L5: fehlt, in L7 integriert, z.B. mit Cookies
L4: Host-to-Host Layer
L3: Internet / Gateway Layer
L2: Network Access Layer: kein MAC-Layer, nur Logical Layer
L1: fehlt

## TCP/IP-Protokolle

| | | |
|---|---|---|
| Process / Application | HTTP, DNS, SMTP, FTP, SNMP, POP3, Telnet | S/MIME, PGP, PEM, SSH, Kerberos, SET, S-HTTP |
| Host-to-Host | UDP, TCP | SSL, TLS |
| Internet / Gateway | IP, ICMP, ARP, RARP | IPsec |
| Network Access | Ethernet, FDDI, Token Ring, PPP | ECP, CHAP |

## Requests for Comments RFC

Technische und organisatorische Dokumente zum Internet.
Zuständig ursprünglich Stanford Research Institute SRI,
heute Internet Engineering Task Force IETF.

Beispiele:
- RFC 768: UDP
- RFC 791: IP
- RFC 793: TCP
- RFC 1034: DNS
- RFC 2616: HTTP

http://www.ietf.org/
http://www.faqs.org/rfcs/

# Physical Layer

TECH

## Aufgabe

Definiert die elektrische, mechanische und funktionale Schnittstelle zum Übertragungsmedium (hat keine Protokollinformationen).

## Sublayers

- Physical Medium Attachment PMA:
  - Definition der Schnittstellen zum Übertragungsmedium, z.B. Transceiver
- Physical Layer Signaling PLS:
  - Ankopplung an MAC-Sublayer im Endgerät
  - Zugriffssteuerung
  - Umsetzung des binären Datenstroms in elektrische, optische oder akustische Signale

## Analoge Signale

zeitgleich mit Original
z.B. Sonnenuhr

- Schwingung: Signalwelle
- Frequenz: Anzahl Schwingungen pro Sekunde, Hertz
- Amplitude: Schwingweite von Ruhelage zu Umkehrpunkt
- Bandbreite: Bereich der möglichen Schwingung
  z.B. menschliche Stimme von 100 bis 10000 Hz,
  Telefon von 300 bis 3400 Hz

## Digitale Signale

zählbare Werte
Zustände der Schwingung zu bestimmten Zeitpunkten
Genauigkeit hängt von Abtastrate und Auflösung ab

Vorteile:
keine Zwischenwerte
Störungen können korrigiert werden

## Modulation

Umwandlung in analoge Signale für die Übertragung.
Demodulation: Rückwandlung in digitale Signale.

Methoden zur Unterscheidung der binären Zustände 0 und 1:

- Amplitudenmodulation AM (amplitude shift keying ASK):
  unterschiedliche Amplituden, anfällig für Störungen und Dämpfung, nur für geringe Datenübertragungsraten geeignet
- Frequenzmodulation FM (frequency shift keying FSK):
  verschiedene Frequenzen, stabiler, höhere Übertragungsraten und Entfernungen
- Phasenmodulation PM (phase shift keying PSK):
  Phasenverschiebungen beim Übergang 0/1, höchste Übertragungsraten

## Störungen

- Dämpfung (Attenuation):
  Signalabschwächung bei der Übertragung, in Dezibel dB
- Wellenwiderstand, Kabelimpedanz:
  braucht Abschlusswiderstand zur Vermeidung von Reflektion
- Übersprechen:
  NEXT: Störung am empfängernahen Ende
  FEXT: Störung am empfängerfernen Ende

# Data Link Layer

TECH

## Aufgaben

L3-Daten + L2-Protokollinformationen = Frame

- Header: physische Source und Destination zur physischen Adressierung
- Trailer: Prüfsumme zur Fehlererkennung und Fehlerbehebung
- Datenflusskontrolle: zuverlässige Datenübertragung auf einer Teilstrecke zwischen zwei Netzknoten
- Zugriffssteuerung bei parallelem Versand
- Point-to-Point Protocol PPP: für analoge Leitungen

## Sublayers

- Media Access Control MAC:
  - Schnittstelle zum Physical Layer
  - Bildung von Frames beim Senden (Encapsulation)
  - Berechnung einer Prüfsumme, evtl. Fehlermeldung
  - Zugriffssteuerungs-Verfahren
  - Bearbeitung der empfangenen Frames (Decapsulation)
- Logical Link Control LLC:
  - Schnittstelle für höhere Schichten
  - Erkennen / Beheben von Übertragungsfehlern
  - Flusskontrolle, Verhinderung von Überlastung

## MAC-Adresse

- 48 Bits
- physische Adresse der Netzwerkkarte (Network Interface Card NIC)
- eindeutige Hardware-Identifikation

Funktionsweise:

- Frames mit MAC-Adresse kommen über das Kabel
- gehen an alle Netzwerkkarten im Netz
- Prozessor setzt Protokoll um
- Signal für 1 Bit ist 25 m lang
- Signale werden gespeichert bis die Adresse erkannt wird (Sicherheitsrisiko)

## Zugriffssteuerungs-Verfahren

Regelung, wer (bei Paketvermittlung) wann Daten senden oder empfangen darf.

- nichtdeterministische Verfahren:
  z.B. CSMA/CD, Zugriff nicht geregelt, bei zeitgleichen Übertragungsversuchen Wiederholung der Sendung, geeignet für kleine Netzwerke mit geringer Netzlast
- deterministische Verfahren:
  z.B. Token Passing, Zugriffssteuerung über Signalisierungsmechanismen, höherer Verwaltungsaufwand, komplexere Technik

## Forward Error Control FEC

- redundante Datenübermittlung:
  braucht mehr Bandbreite und/oder Zeit
- automatic repeat request ARQ
- Kontrolldaten / Prüfbit:
  Fehler wird nicht immer erkannt

## Feedback Error Control

Infos werden zurückgeschickt, braucht duplex

- nur Empfangsbestätigung
- Kontrolldaten / Prüfbit:
  Paritätsbit muss definiert werden
  (0/1 für gerade/ungerade)

# Network Layer

TECH

## Aufgaben

L4-Daten + L3-Protokollinfo = Datagramm

- Header: logische Source und Destination mit Netz und Knoten
- Internet Protocol IP: Routing, Vermittlung einer End-to-End-Verbindung, Wegfindung vom Sender zum Empfänger über mehrere Transitsysteme
- Internet Control Message Protocol ICMP: Austausch von Service-Meldungen
- Address Resolution Protocol ARP: Umsetzung der IP-Adresse in MAC-Adresse mit Tabelle
- Reverse ARP (RARP): Umsetzung MAC- in IP-Adresse
- korrekte Zustellung an den Empfänger

## Vermittlung

verbindungsorientiert:
- keine zeitliche Verzögerung
- Reihenfolge bleibt
- virtuelle exklusive End-to-End-Verbindung (Verbindungsauf- und -abbau)
- Leitungsvermittlung: z.B. Telefon
- geeignet für kurzzeitig hohen Datendurchsatz und zeitkritische Verbindungen (Sprach- und Bildübertragung)

verbindungslos:
- Reihenfolge egal, braucht Nummerierung
- Datagramm mit Quell- und Zieladresse
- Paketvermittlung: z.B. Post
- geeignet für wenige unregelmässige Nachrichten

## IP-Adresse

- 4 Bytes
- logische oder Software-Adresse
- eindeutig für alle erreichbaren Netzwerkknoten
- von bestimmten autorisierten Stellen vergeben
- Angabe dezimal mit Punkten, aufgeteilt in
  - Network: logische oder organisatorische Einheit von Rechnern, Domain
  - Host: einzelne Rechner des Netzwerks

## IP-Adressklassen

- Class-A:
  Bit 1 = 0, Network.Host.Host.Host
  0.x.x.x – 127.x.x.x, 126 Subnetze mit je 16'777'214 Hosts
- Class-B:
  Bit 1-2= 10, Network.Network.Host.Host
  128.0.x.x – 191.255.x.x, 16'384 Subn. mit je 65'534 Hosts
- Class-C:
  Bit 1-3 = 110, Network.Network.Network.Host
  192.0.0.x – 223.255.255.x, 2'097'152 Subn., je 254 Hosts
- Class-D:
  Network.Network.Network.Network
  224.0.0.0 – 239.255.255.255, Multicast
- Class-E:
  Experimental, Erweiterungen

## Spezielle IP-Adressbereiche

Private Netzwerke, werden nicht geroutet, brauchen deshalb Network Adress Translation NAT im Router.
Billiger, Netzwerk von aussen nicht einsehbar, aber interner Trojaner kann Backdoor öffnen.
Class A:
10.0.0.0 – 10.255.255.255, Subnetz mit 16'777'214 Hosts, für grosse Konzerne, Universitäten usw.
Class B:
172.16.0.0 – 172.31.255.255, 16 Subn. mit je 65'534 Hosts, für Betriebe mit verzweigten Liegenschaften
Class C:
192.168.0.0 – 192.168.255.255, 256 Subn. mit je 254 Hosts, für den Privatbereich
127.0.0.1: loop-back-Adresse, local host

## Subnetz-Maske

Host-Anteil kann weiter aufgeteilt werden in netzinternen Network- und Host-Anteil (Subclassing).

Beispiel:
Class-C-Adresse 255.255.255.240
Host-Anteil umsetzen auf binär = 11110000
1 = Network, 0 = Host
gibt 16 Subnetze mit je 16 Rechnern (je $2^4$ Möglichkeiten)

# Transport Layer

TECH

## Aufgabe

L5-Daten + L4-Protokollinformationen = Segment

- Header: Verbindungsnummer und Sequenznummer
- verbindungsorientierter Transport
- Sequenznummer gewährleistet Reihenfolge

## Transport-Protokolle

- Transmission Control Protocol TCP:
  Kontrolle der richtigen Reihenfolge und Vollständigkeit, Stauvermeidung (congestion control), braucht stehende offene Verbindung
- User Datagram Protocol UDP:
  keine Verbindungsgarantie, z.B. Ping, Antwort Pong, Option traceroute: Antwort von jedem Router

# Session Layer

TECH

## Aufgabe

- Header: Session-ID
- Session-Management: Eindeutigkeit mit IP-Adresse und Port-Nummer, bei Folgeverbindungen wird ein zufälliger Port gewählt
- Sessionkontrolle: Aufbau, Aufrechterhaltung und Abbau von Sessions
- Dialogverwaltung: An- und Abmeldefunktion
- Benutzerautorisierung

# Presentation Layer

TECH

## Aufgabe

- Header: Sessionkennung
- Darstellung auf den Endgeräten
- Datenteil wird modifiziert:
  - Zeichensatz-Anpassung, Kodierung
  - Verschlüsselung, Chiffrierung, Kryptographie
  - Komprimierung

## Zeichensätze

Ascii:
American Standard Code for Information Exchange
Verwendung im PC-Bereich
Standard: 7 Bits = 128 Zeichen
Zusatz: 8. Bit = +128 Zeichen für Spezialzeichen (Codepages)

Ebcdic:
Extended Binary Coded Decimal Information Code
Verwendung im Grossrechner-Bereich (IBM)

## Verschlüsselung

Mime:
Multipurpose Internet Mail Extensions
Umwandlung von 8bit-Binärdaten (z.B. Exe-Dateien, Textdokumente) in 7bit-Ascii-Code (z.B. E-Mail)

RSA:
asymmetrische kryptologische Verschlüsselung von Rivest, Shamir und Adelmann, beruht auf Primzahlen

## Komprimierung

verlustfreie Kompression:
vollständig reversibel

verlustreiche Kompression:
für grosse Mengen Nutzdaten mit geringem Anspruch an Informationsgehalt und Details

# Application Layer

TECH

## Aufgabe

- Schnittstellen zum Benutzer: Menüsystem, Kommandozeile
- Schnittstellen für Anwendungsentwickler: application programming interface API