Grundlagen der Netzwerktechnik

Dr. Holger Beck
GWDG
Holger.Beck@gwdg.de, http://www.gwdg.de/~hbeck

Februar 2003

Teil I: Kommunikation

Kursthema

- Themenkomplexe
  - Kommunikation
  - Elektronische Datenverarbeitung
- Thema
  - Kommunikation mit Hilfe von EDV und
  - EDV mit Hilfe von Kommunikationstechniken, also
  - Netzwerktechnik in der EDV
  - (z.B. nicht Telefonnetze)

Kursniveau

- Einführung
  - mit Schwerpunktsetzung bei Techniken, die im Bereich Universitäten / Forschungseinrichtungen gängig sind.
  - Kein Ersatz für praktische Erfahrungen
  - Grundlage für learning-by-doing unter Anleitung bzw. mit Unterstützung von Experten

Zielgruppe

- MitarbeiterInnen der Universität Göttingen und der MPG, die
  - in den Instituten
  - über einen längeren Zeitraum
  - mit Unterstützung der GWDG
  - Netzwerke betreuen

Kursinhalte

- Bestandteile moderner Netze
  - Verkabelungstechnik
  - Netzwerkverteiler
  - Protokolle und Normen
- Funktionsprinzipien lokaler Netze
  - Ethernet als Standardtechnik und Schwerpunkt
  - Token-Ring und FDDI als Alternativen
  - ATM als ganz anderer Lösungsansatz

Kursinhalte (Fortsetzung)

- Von kleinen Netzinseln zu großen Netzen
  - Repeater
  - Switches
  - Router
  - und ihre Funktion
- Netzwerkprotokolle
  - Strukturierung von Protokollen
  - Netzwerktechnologieabhängige Protokolle
  - Ausgewählte Internet-Protokolle als Beispiele

Kursinhalte (Schluss)

- Sicherheit in Datennetzen
- Netzwerkmanagement
  - Prinzipien
  - Netzwerkmanagement mit SNMP
  - Hilfsmittel zur Netzwerküberwachung und Störungsanalyse

Literatur

- *Als allgemeine Einführung in das Thema des Kurses (und darüber hinaus):*

  A. Badach, E. Hoffmann, O. Knauer
  High Speed Internetworking
  Addison-Wesley 1997
  ISBN 3-82731-232-9

- *Weitergehend:*

  Larry L. Peterson, Bruce S. Davie
  Computer Networks: A Systems Approach
  Morgan Kaufmann Publishers Inc. 1996
  ISBN 1-55860-368-9

- *Zu Ethernet:*

  Charles E. Spurgeon
  Ethernet: The Definitiv Guide
  O'Reilly & Associates Inc. 2000
  ISBN 1-56592-660-9

- *Zu TCP/IP-Protokollen:*

  Douglas Comer
  Internetworking with TCP/IP, Vol 1:
  Principles, Protocols and Architecture
  Prentice Hall PTR 2000
  ISBN 0-13018-380-6

- *Handzettel zum Kurs unter*

  http://www.gwdg.de/service/kurse/skripten

Kommunikation

- Verschiedene Betrachtungsweisen
  - Beschäftigung mit Inhalten und deren Vermittlung
    - Kommunikationswissenschaften / Sozialwissenschaften
    - Nicht unser Thema
  - Beschäftigung mit technischen Hilfsmitteln der Kommunikation
    - Informatik / Elektrotechnik / Nachrichtentechnik

Kommunikationtechnik im Rückblick

- Standardtechnik: Sprache
  - Hauptproblem: Ohne technische Hilfsmittel in der Reichweite stark begrenzt
- Einsatz technischer Hilfsmittel
  - Boten
  - optische Hilfsmittel
  - akustische Hilfsmittel
  - elektrische, elektronische oder elektomagnetische Hilfsmittel
- Beispiele:
  - Boten, Brieftauben, Post,
  - Leuchtfeuer, Rauchzeichen, Flaggensignale,
  - Buschtrommeln, Signalhörner, Lautsprecher,
  - Telegraphie, Telefonie, Funk, Radio, Fax

Kenngrößen von Kommunikationstechniken

- Reichweite
- Informationsumfang der übermittelten Nachricht
  - Ja/Nein-Botschaften
  - Komplexe Botschaften
- Zeitverhalten
  - Echtzeitkommunikation (synchron)
  - Zeitverzögerte Kommunikation (asynchron)

Kenngrößen von Kommunikationstechniken

- Übertragungsmedium
  - Luft (Schall)
  - Freier Raum (optische und elektromagnetische Übertragung)
  - Papier u.ä., menschliches Gedächtnis
  - Leitungsgebundene Übertragung
    - metallische Leiter (insbesondere Kupferkabel)
    - Glasfasern (Lichtwellenleiter, LWL)

Kenngrößen von Kommunikationstechniken

- Geschwindigkeit der Nachrichtenübermittlung
  - Verzögerung zwischen Absenden und Ankunft (als Zeit gemessen)
- Signalregeneration
- Signalcodierung
  - digital (stufenförmig, nur diskrete Werte annehmend)
  - analog (beliebige stufenlose Werte annehmend)

Entwicklung moderner Kommunikationsnetze

- Elektrizität und Leitungen als Voraussetzung
- Telegraphie
- Telefonie
- Richtfunk und Satelliten
- Datenübertragung über bestehende analoge Netze
- Computernetze

Entwicklung der Computernetze

- Anschluß von Peripheriegeräten (Kartenleser, Drucker) an Großrechnern
- Terminals an Großrechnern
- Informationsaustausch zwischen Großrechnern (Mail und kleinere Datenmengen)
- Datenübertragung zwischen lokalen „Mini-Computern“
- Ersatz der Großrechner durch vernetzte Kleincomputer: Netzwerkbetriebssysteme
- Sprach- und Bilddaten über Datennetze (Multimedia-Kommunikation)
- Internet als globales Netz
- Elektronische Geschäftsprozesse

Netzwerkanwendungen

- Kommunikation mit Hilfe von Computern
  - Elektronische Post / E-Mail
  - Informationssysteme
    - World Wide Web
    - NetNews
  - Telefonie und Videokonferenzen
  - Kommerzielle Anwendungen (E-Business)
- Kommunikation als Hilfsmittel der EDV
  - Kleinrechnernetze statt Großrechner
  - PCs statt Terminals
  - trotzdem gemeinsam nutzbare Daten und Programme (File-Server)
  - gemeinsam genutzte Peripherie (Print-Server, Backup-Server)
  - gemeinsame Ressourcenverwaltung

Netzwerkanwendungen und Anforderungen

- Unterschiedliche Netzwerkanwendungen stellen unterschiedliche Anforderungen an Netze
- Welche Charakteristika von Netzen sind zu betrachten?
- Beispiele:
  - Elektronische Post
  - WWW
  - NetNews
  - Telefonie und Videokonferenzen
  - File-Server

Vergleich

Anforderungen / Verhalten	Mail	WWW	News	Telefonie / Videokon.	File-Server
Interagierende Teilnehmer	mehrere	einer	mehrere	mehrere	einer
Synchronität	nein	ja	nein	ja	ja
Antwortzeiten	unkritisch (Minuten)	wichtig (Sekunden)	unkritisch (> Minuten)	kurz (<Sek.) konstant	wichtig bis kritisch
Netzbelastung	wechselnd	wechselnd	wechselnd	konstant	wechselnd
Datenmenge	meist gering	mittel – groß	Gering, groß zw. Servern	gering (Tel.) / groß (Vid.)	teils groß
Datenverlust / Verfälschung	inakzeptabel	inakzeptabel	inakzeptabel	begrenzt akzeptabel	inakzeptabel
Anonymität	persönliche Postfächer	meist anonym	Pseudonyme, Zugriffsrecht auf Server	nein	Benutzer-kennung
LAN /WAN	vor allem WAN	vor allem WAN	vor allem WAN	vor allem WAN	vor allem LAN

Charakterista von Netzen

- Kommunikationsmuster
  - Ein (WWW, File-Server), zwei (E-Mail), mehrere (NetNews, Videokonferenz) aktive interagierende Teilnehmer
  - symmetrische oder asymmetrische Übertragung
  - synchrone oder asynchrone Interaktion
- Art des Übertragungskanals
  - Request/Reply Channel
  - Message Stream

Bandbreite

- Pro Zeiteinheit übertragene Datenmenge
- Verfügbare Bandbreiten wachsen ständig
- Bandbreitenanforderungen
  - Dauer,
  - Quantität,
  - konstant oder
  - schwankend

Latenz und Antwortzeit

- Latenz: Zeit zwischen Absenden und Empfang einer Übertragungseinheit (latency oder delay)
- Antwortzeit: als Zeit zwischen Absenden einer Anfrage und Erhalt der Antwort (Round-Trip-Time, RTT)
- Abhängigkeit der Latenz
  - Latenz = Dauer des Sendevorgangs + Signalausbreitungszeit + Verzögerungen bei Zwischenstationen
  - Dauer des Sendevorgangs = Datenmenge / Bandbreite
  - Signalausbreitungszeit = Entfernung / Lichtgeschwindigkeit
  - Latenzen können nicht beliebig minimiert werden (Signalausbreitungsgeschwindigkeit ≤ Lichtgeschwindigkeit)

Auswirkungen von Bandbreite und Latenz

- Bandbreiten- oder Latenzabhängigkeit von Anwendungen
  - Bandbreitenabhängikeit bei Übertragung großer Datenmengen ohne zwischenzeitliche Bestätigung
  - Latenzabhängigkeit bei Übertragung kleiner Datenmengen mit zwischenzeitlichen Bestätigungen
- Latenzschwankungen
  - Jitter
  - für bestimmte Anwendungen kritisch (Telefonie, Video)

Rechnernetze

- Rechnernetze als Ersatz für Großrechner + Terminals
- Kommunikationsmodelle:
- Client-Server
  - Aufgabenteilung auf
    - Rechner, die Dienste anbieten: Server
    - Rechner, die Dienste nutzen: Clienten
  - Modell für größere Netze mit vielen Rechnern
  - Zusatzkosten für Server
  - Aufgabenteilung nicht immer 100%ig eingehalten
- Peer-to-Peer
  - Netz aus gleichberechtigten Rechner
  - Alle Rechner bieten Dienste an und nutzen Dienste anderer
  - Modell für Netze mit sehr wenigen Rechnern
  - Keine Zusatzkosten für Server
  - Höherer Probleme mit Betriebssicherheit

Netzwerkbetriebssysteme

- UNIX-Netze
  - Multi-User, Multi-Tasking Betriebssystem
  - Klassische Internet-Systeme
  - Netzwerkerweiterung eines bestehenden Betriebssystems
  - Strukturell gleiche Rechner
  - NFS für Dateisystem
  - LPD für Druckerzugriffe
  - NIS für Benutzerverwaltung
  - Rechteverwaltung mit deutlichen Mängeln (nur drei Stufen, Freigaben rechnerbezogen)
- Microsoft-Netze
  - Netzwerkerweiterung bzw. Integration im Betriebssystem
  - Client-Server-Struktur mit Windows-NT/2000-Server
  - Peer-to-Peer-Netz mit anderen Windows-Varianten (WfW, W9x, ME)
  - Managementstruktur nach Domänenkonzept (NT/2000/XP)
  - mit domänenweiter Benutzerverwaltung
  - Rechteverwaltung bei NT im wesentlichen ausreichend, ab 2000 stark erweiterte Möglichkeiten

Teil II: Physik

Physik

- Themen und Inhalte
  - Netzwerkstrukturen
  - Übertragungsmedien, insbesondere Kabel
  - Übertragungstechnik
- Warum muss man das wissen?
  - Planung von Netzen
    - Basis von Netzen sind die Übertragungswege
    - Netzwerktechnologien ändern sich, die Kabel bleiben
  - Problemanalyse
    - Mehrzahl aller Netzwerkprobleme auf der physikalischen Ebene

Netzelemente

- Basis von Datennetzen:
  - Physikalische Verbindung (engl. Link)
  - zwischen Geräten: Knoten (engl. Node)
  - über Netzwerkadapter
- Arten von Links
  - Punkt-zu-Punkt-Verbindung (engl. Point-to-Point Link)
    - dediziertes Medium (Kabel) zwischen zwei Knoten
  - gemeinsam genutzte Medien für mehrere Knoten (engl. Multiple Access Link)
    - mehrere Knoten an ein Medium angebunden (z.B. Funk)

Vom Link zum Netz

- Nur Punkt-zu-Punkt-Verbindung:
  - zu aufwendig
- Gemeinsam genutzte Medien:
  - in Ausdehnung und Bandbreite limitiert
- Lösung
  - Bildung von Teilnetzen,
  - Verbindung von Teilnetzen über ***Vermittlungssysteme*** (***Switching***, Switched Networks, vermittelte Netze),
  - ***Weiterleitung*** von Daten durch Vermittlungssysteme (***Forwarding***) zur
  - Kommunikation zwischen Endknoten innerhalb von (virtuellen) ***Übertragungskanälen***

LANs und WANs

- Local Area Networks (LANs)
  - begrenzte Ausdehnung,
  - private Netze,
  - daher gebührenfrei,
  - (früher immer) höhere Bandbreiten als WANs
  - Einsatzort von Netzwerkbetriebs-systemen
- Wide Area Networks (WANs)
  - Überbrückung größerer Entfernungen,
  - öffentliche Netze,
  - Nutzungsabhängige Gebühren und/oder Anschlussgebühren
  - aufwendigere Vermittlungsfunktionen,
  - Kommunikationsanwendungen

Leitungsvermittlung

- Realisierung von Übertragungskanälen durch Vermittlung von Leitungen
  - typische für Telefonie (früher Handvermittlung, heute automatische Vermittlungsanlagen),
  - Schaltung einer dedizierten Leitung,
  - Ineffiziente Nutzung durch anwendungsbedingte Übertragungspausen,
  - aber garantierte Übertragungskapazität
  - und Flexibilität bei Kommunikationsprotokollen.

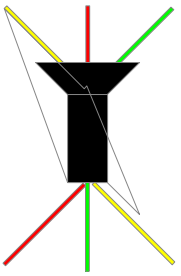
Vermittlungsstelle in Hamburg um 1900

Effizienz bei hohen Bandbreiten

- Moderne Kabel bieten hohe Bandbreiten,
- klassische Anwendungen benötigen wesentlich weniger Bandbreite (z.B. Telefonie) oder
- Leitungen zwischen Netzen bieten vielfache Kapazitäten der Leitungen innerhalb der Netze,
- Aufteilung von der Bandbreite auf verschiedene Kanäle auf einem Kabel:
- Multiplex-Techniken
  - Frequenzmultiplex (Frequency Domain Multiplexing, FDM, z.B. Radio, TV)
    - Aufteilung der Bandbreite in mehrere Kanäle verschiedener Frequenz
  - Zeitmultiplex (Time Division Multiplexing, TDM)
    - Aufteilung der Übertragungszeitpunkte

Zeitmultiplexverfahren

- Varianten des Zeitmultipexverfahren:
  - Synchones Zeitmultipexverfahren
    - Für jeden Kanal wird eine feste Zeitscheibe nach Dauer und Übertragungszeitpunkt vorab festgesetzt



Effizienz bei zeitweiser Nutzung

- Anwendungen nutzen Leitungen meist nur zeitweise,
- Anschluss mehrerer Knoten an eine Leitung (Multiple Access Link)
- mit Zugriff ähnlich TDM
- zur effizienten Nutzung der verfügbaren Bandbreite.
- Typisch für lokale Datennetze (LANs, Local Area Networks),
- Shared (Media) Networks,
- bis ca. zum Jahr 1995.
- Steigende Bandbreiten bedingen teilweise Abkehr von Shared (Media) Networks (Switched Networks, Switched LANs).

Pakete und Zellen

- Aufteilung der Bandbreite in LANs
- durch Übertragung der Daten in kleinen Blöcken.
- Varianten
  - Blöcke variabler Länge: Pakete (Frames)
    - an Bedarf anpassbar,
    - meist große Maximallänge (>1000 Byte),
    - überwiegend in LANs verwendet.
  - Blöcke konstanter Länge: Zellen (Cells)
    - bessere Eignung bei Anforderung nach konstanten Datenraten,
    - meist kleine Längen (50-100 Byte),
    - mehr in WANs üblich.

Paketvermittlung

- Paketübertragung und -vermittlung
  - effizientere Auslastung des Netzes durch
  - „gleichzeitige“ Nutzung der Übertragungswege durch mehrere Kommunikationen,
  - voneinander unabhängige Übertragung aller Pakete durch das Netz,
  - Overhead durch Adressinformation in jedem Paket
  - fehlende Garantie von Kapazitäten für einzelne Kanäle,
  - Zwischenspeicherung in Vermittlungssystemen bedingt
    - Verzögerungen,
    - aufwendigere Vermittlungssysteme
    - Möglichkeit von Datenverlusten bei Stauungen auf Teilstrecken,
  - Bindung an bestimmte Protokolle
- Problem: Garantierte Bandbreite oder effiziente Auslastung

Netzwerktopologien

- Netzwerktopologie:
  - Struktur der Anordnung der Knoten im Netz
  - Unterscheidung:
    - physikalische Struktur,
    - logischen Struktur (Softwarekonzeptionen oder Protokoll).
- WAN-Topologien
  - Punkt-zu-Punkt,
  - mit baumförmiger Struktur
  - oder vermaschten Struktur

LAN-Topologien

- Busförmige Topologie
  - Klassische Struktur früher Datennetze
- Ringförmige Topologie
  - Alternative Struktur früher Datennetze
- Sternförmige Topologie
  - Moderne Struktur
- Baumförmige Topologie
  - Hierachie von Sternstrukturen bei größeren Netzen
  - Strukturierte Netze
- Vermaschung
  - eher unüblich

Bustopologie

- Prinzip
  - Anschluß aller Stationen an gemeinsames Kabel,
  - Senden von Daten in alle Richtungen,
- Vor- und Nachteile
  - keine Verteilerfunktionen nötig,
  - geringer Platzbedarf für die Verkabelung, wenige Kabel,
  - jede Störung an Kabeln oder Endgeräten kann zu einem Totalausfall des Netzes führen.

Ringtopologie

- Prinzip
  - Verbindung aller Stationen in Form eines Ringes,
  - jede Station überträgt empfangene Daten an die nächste Station im Ring weiter,
- Vor- und Nachteile
  - geringfügig größere Kabelmengen als bei als bei Bustopologie,
  - Ausfall einer Kabelstrecke oder einer Station kann zu einem Totalausfall führen,
- Variante Doppelring
  - Kompensation des Ausfalls einer Verbindung oder einer Station

Sterntopologie

- Prinzip
  - Dedizierte Kabel von jeder Station zu einem zentralen Punkt,
- Vor- und Nachteile
  - hoher Aufwand bei Verkabelung
  - Notwendigkeit von Verteilern
    - mehr oder weniger intelligent
    - (ursprünglich) mehr Signalverstärker denn Vermittlungssystem,
    - Netzwerk-Managementfunktionen im Verteilers möglich,
  - Flexibilität in der Konfiguration,
    - zur Unterteilung
    - zum Einsatz verschiedener Technologien
  - geringe Anfälligkeit bei Defekten der Verkabelung oder der Endgeräte, (meist nur eine Station gestört).

Logische Topologien in LANs

- Bustopologie
  - dominante Struktur (Ethernet)
- Ringtopologie
  - Token-Ring und FDDI
- Stern- und Baumtopologien
  - Selten (ATM, VG-AnyLAN)
- Logische und physikalische Topologie
  - Verschaltung physikalischer Stern- oder Baumtopologien zu logischen Bussen oder Ringen

Kategorisierung der Netzelemente

- Hardware
  - Passive Komponenten:
    - keine Stromversorgung
    - Kabel
    - Stecker
    - Passive Ringleitungs-verteiler (im Token Ring)
  - Aktive Komponenten:
    - Stromversorgung vorhanden
    - Rechner
    - Signalverstärker und Vermittlungssysteme
- Architekturen und Normen
  - Modelle für Netzwerkverfahren
  - Normierungen von Netzwerktechnologien und Komponenten
- Software
  - Netzwerkbetriebssysteme
  - Netzwerkanwendungen

Übertragungsmedien

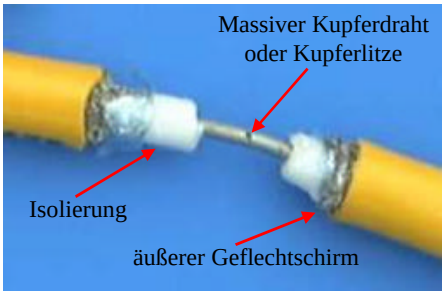
- Drahtlose Übertragungen
  - Funk
  - Licht/Laser
  - Infrarot
  - Probleme:
    - Wetterempfindlichkeit
    - Sichtverbindung nötig
- Leitungsgebundene Übertragungen
  - Elektrische Signale: Kupferkabel
  - Optische Signale: Glasfaserkabel

Kupferkabel

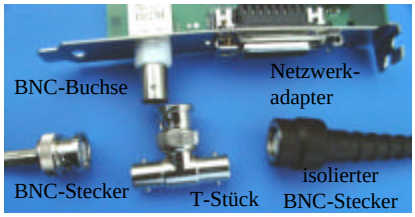
- Übertragung elektrischer Signale
  - als elektrische Impulse
  - über geschlossenen Schaltkreise
  - als Spannungsveränderungen
  - Übertragungsqualität steigt mit Kabeldurchmesser
- Kabeltypen
  - Asymmetrische Kabel
    - unterschiedliche Hin- und Rückleitungen,
    - Koaxialkabel
  - Symmetrische Kabel
    - gleiche Hin- und Rückleitungen,
    - paarweise verdrillte Kabel (Twisted Pair)

Asymmetrische Kupferkabel

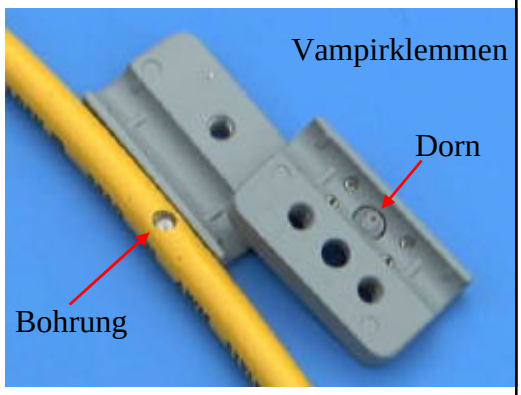
- Kabeleigenschaften
  - Koaxialkabel (gemeinsame Achse)
  - geringe elektromagnetische Abstrahlung bzw. Störanfälligkeit
- Einsatzbereiche
  - Breitband-Kabeltechnik
  - Frühe Ethernet-Netzwerke



Koaxialkabelanschlüsse

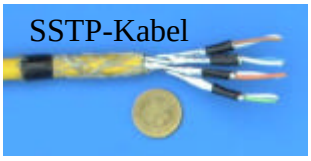


BNC-Anschluss



Symmetrische Kupferkabel

- Variationen
  - ungeschirmt (UTP)
  - mit äußerem Schirm (STP)
  - mit äußerem Schirm und einzeln geschirmten Adernpaaren (SSTP)
  - in Europa überwiegend SSTP, USA UTP
  - Varianten möglichst nicht mischen
- Einsatzbereiche
  - (fast) alle Netzwerktechnologien



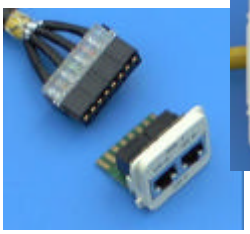
TP-Kabelanschlüsse

Geschirmte und ungeschirmte RJ45-Stecker

Acht Kontakte für 4 Adernpaare
Anschluss der Paare an Kontakte 1/2, 3/6 4/5 und 7/8

Geschirmte Doppeldose 2xRJ45

Variation: 2 Anwendungen über ein 4-paariges Kabel, jeweils Kontakte 1/2 und 3/6 belegt (Ethernet-Belegung)



Modulare Dose

Geschlossene Doppeldose

Steckersystem für höhere Frequenzen

IBM-Würfel-Stecksystem

Kabeleigenschaften

- Ausbreitungsgeschwindigkeit
  - ca. 50-75% der Vakuumlichtgeschwindigkeit je nach Kabeltyp
- Wellenwiderstand
  - Widerstand am Eingang einer unendlichen Leitung
  - 50 Ω(Koaxialkabel Ethernet), 75 Ω(Breitbandkabel), 100 Ω(Standard TP-Kabel), 150 Ω (IBM-Kabelsystem)
- Dämpfung
  - Signaldämpfung (in dB)
  - (Nah-) Nebensprechdämpfung Crosstalk (in dB)
  - Verhältnis Signal/Rauschen (SNR) und Attenuation / Crosstalk Loss Ratio (ACR)
  - frequenzabhängig
- Maximale Kabellänge
  - abhängig von Dämpfung
  - abhängig von Sendstärke und Empfängerempfindlichkeit
- Maximale Bitrate/Bandbreite
  - Abhängig von SNR- bzw. ACR-Wert
  - beeinflusst von Leitungskodierung

Lichtwellenleiter

- Übertragung optische Signale
  - Licht an oder Licht aus
  - Aufgrund der Dämpfungs- und Streuungs- und Absorptionseigenschaften von Lichtleitern drei Übertragungsfenster
    - 850 nm (teilweise sichtbar), 1300 nm (Infrarot), 1550 nm(Infrarot)
  - Sender
    - Lumineszenzdioden (LED)
    - Laserdioden
  - Empfänger
    - Photodioden
  - Getrennte Leitungen für Senden und Empfangen
- Teure elektro-optische Wandlungen

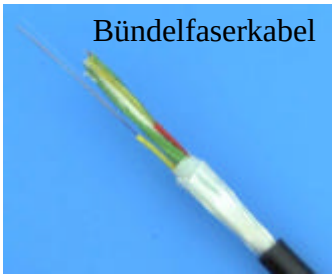
Lichtwellenleiter (Fortsetzung)

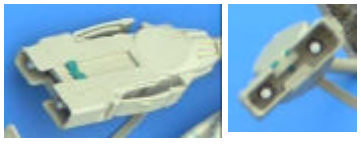
- Prinzip
  - Aufbau aus zwei Sorten Glas mit unterschiedlichem Brechungsindex: Kern und Mantel
  - Reflektion an Grenzfläche Kern/Mantel
- Dispersion
  - Unterschiedlich Strahlengänge je nach Einfallswinkel,
  - dadurch unterschiedliche Strecken
  - und unterschiedliche Laufzeiten
  - damit Verbreiterung des Signals

LWL-Typen

- Variationen zur Reduktion der Dispersion
  - Gradientenkabel statt Stufenindexkabel:
    - statt konstanter Brechzahl im Kern und Mantel
    - allmähliche Veringerung der Brechzahl von der Mitte des Kerns bis zum Mantel.
  - Monomode statt Multimode-Kabeln:
    - statt mehrerer Strahlen (Moden) bei verschiedenen Einfallswinkeln
    - Kern so klein, dass nur ein Strahl (Mode) einfallen kann
- Gängige Kabel für Datennetze
  - Multimode-Gradientenkabel (Multi Mode Fiber MMF)
    - 50/125 µm (in Europa)
    - 62,5/125 µm (in Nordamerika)
    - Größere Bandbreite bei 50/125 µm (ca. 500 MHz*km)
  - Monomode-Kabel (Single Mode Fiber SMF)
    - 9-10/125 µm (Bandbreiten-Längenprodukt ca. 10 GHz*km)

LWL-Kabel und -Stecker





MIC-Stecker

SC-Stecker

Auswahl von Übertragungsmedien

- Kriterien
  - Kosten
  - Bandbreite
  - Reichweite
  - Verfügbare Netztechnologien
- Praxis
  - Innerhalb von Gebäuden
    - meist Kupferkabel (Kosten, größere Angebotspallette bei Geräten),
    - selten LWL (Abhör- und Störsicherheit, Bandbreite, Reichweite, zentrale Konzepte)
  - Zwischen von Gebäuden
    - nur LWL
      - Potentialunterschiede
      - Störungen

Signalübertragung

- Übertragung von „Rechtecksignalen“
- Kenngrößen des Signalverlaufs
  - Minimal- und Maximalpegel
  - Flankensteilheit
  - Takt
- Rauschen

Anforderungen an Leitungskodierung

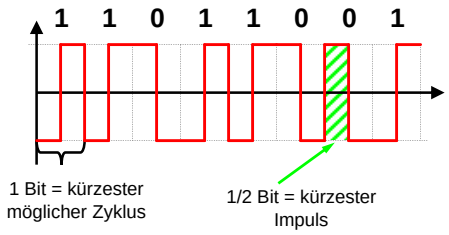
- Synchronisation
  - Sender und Empfänger müssen geringe Taktunterschiede ausgleichen
  - die Signale müssen daher immer wieder Pegelwechsel enthalten
  - auch wenn die Daten nur 0 oder nur 1 enhalten
  - Umwandlung der Bitfolgen in geeignete Leitungskodierungen
- Framing
  - Erkennung von Paketanfang und Paketende
    - durch spezielle Signalmuster,
      - die nicht in den Datenvorkommen oder
      - in den Daten entsprechend umkodiert werden
    - durch Sendepausen
- Gleichspannungsanteil
  - die Signale dürfen keinen Gleichspannungsanteil enthalten

Datenraten und Frequenzen

- Datenrate
  - Anzahl Bits pro Zeiteinheit (Mbit/s, Mbps)
- Bitrate
  - Anzahl übertragener Bits pro Zeiteinheit (Mbit/s, Mbps)
- Fundamentalfrequenz
  - 1 / Dauer des kürzest möglichen Signalzyklus (MHz)
- Baudrate oder Datentaktrate
  - 1 / Dauer des kürzesten Impulses einer Übertragung

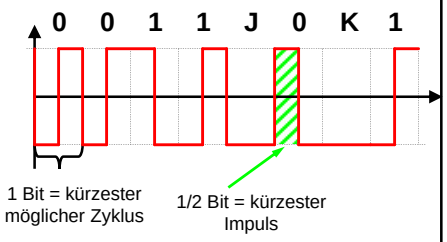
Manchester-Kodierung

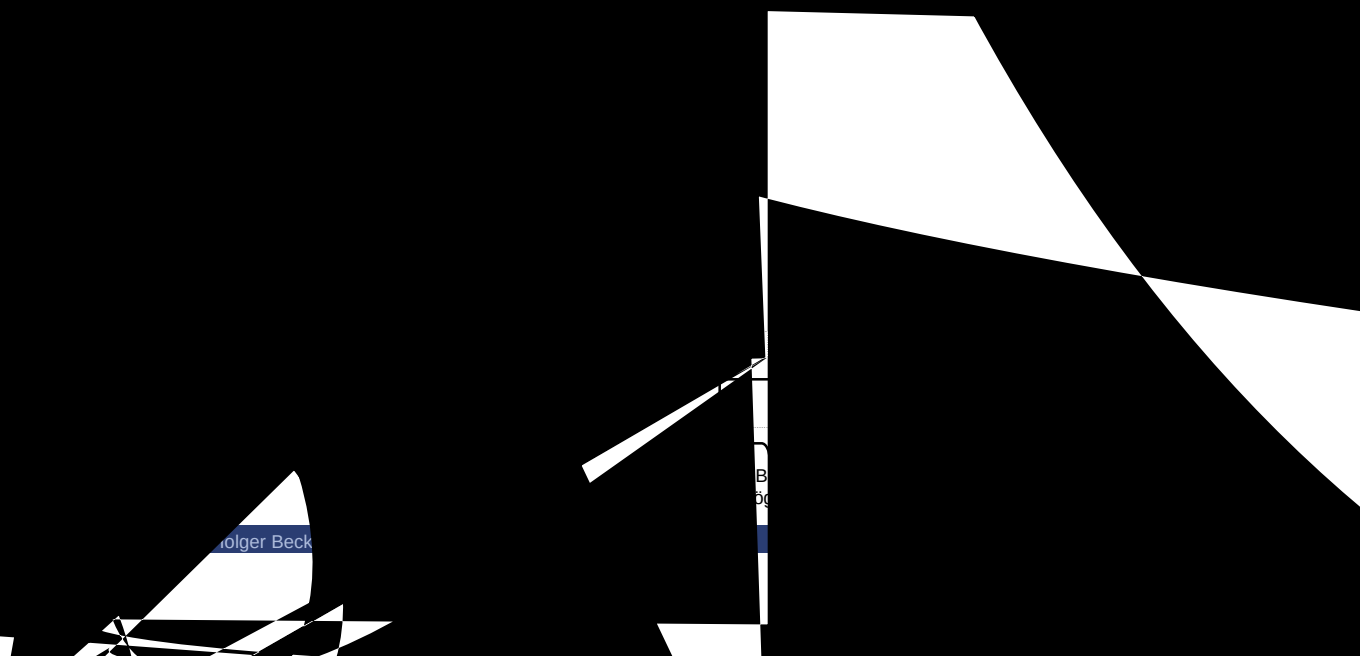
- Signale:
  - zwei Zustände (high und low)
  - Signalisierung durch Zustandswechsel in der Signalmitte
  - Übergang low -> high: 1
  - Übergang high -> low: 0
  - je nach Signalfolge ein zusätzlicher Zustandswechsel am Signalanfang
- Übertragungsraten
  - Datenrate = Bitrate = Fundamentalfrequenz
  - Datentaktrate = 200% der Datenrate
- Beispiel
  - Ethernet



Differential-Manchester

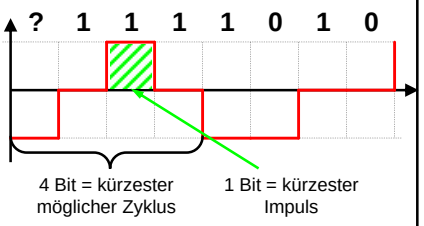
- Signale:
  - zwei Zustände (high und low)
  - Zustandwechsel in der Mitte jedes Signals zur Synchronisation
  - Signalisierung über Zustandswechsel am Signalanfang
  - Polaritätsumkehr: 0
  - keine Polaritätsumkehr : 1
  - zusätzliche Signale durch „Kodeverletzungen“: Signal ohne Polaritätswechsel in der Signalmitte (mit Wechsel am Anfang:„J“, sonst: „K“)
- Übertragungsraten
  - Datenrate = Bitrate = Fundamentalfrequenz
  - Datentaktrate = 200% der Datenrate
- Beispiel
  - Token-Ring




olger Beck

MLT-3

- MultiLevel Transition 3
  - Signale
    - drei Zustände (-,0,+)
    - keine Zustandswechsel in der Signalmitte
    - zyklische Zustandswechsel am Signalanfang
    - Zustandswechsel am Anfang: 1
    - kein Zustandswechsel am Anfang: 0
- Kombination mit 4B/5B-Kodierung
- Übertragungsraten (mit 4B/5B)
  - Bitrate = 125% der Datenrate
  - Fundamentalfrequenz = 31,25% der Datenrate
  - Datentaktrate = 125% der Datenrate
- Beispiel
  - FDDI, Fast-Ethernet über Kupferkabel



Teil III: Ethernet

Lokale Netze

- Entstanden in den 70er und 80er Jahren
- Kopplung von Mini-Computern
- Bandbreiten-Überschüsse
  - Mehr Bandbreite auf Übertragungsmedien verfügbar, als von einem Paar kommunizierender Rechner dauerhaft nutzbar
- Shared-Media Ansatz
  - Rundsendungsmöglichkeit (Broadcast)
  - Paket-Übertragung
- Verschiedene Netzwerktechnologien
  - Kernunterschiede in Regelungen für die Vergabe von Zugriffsberechtigungen (Media Access Control, MAC)

Media Access Control

- Modelle für MAC: Diskussionsregeln
  - jeder darf nach belieben reden
  - jeder darf reden, wenn nicht schon ein anderer redet
  - jeder bekommt in vordefinierter Reihefolge Redezeit zugeteilt
  - ein Diskussionsleiter verteilt Redezeit
- Diese Modelle werden von verschiedenen Netzwerktechnologien verwendet
- Gängigste Technologien
  - Ethernet
  - Token Ring
  - FDDI

Ethernet

- Geschichte
  - Vorläufer Aloha Network auf Hawai (Funk, CSMA ohne CD)
  - Beginn 1973
  - Version 1 von Xerox und Version 2 in 1980 von Digital, Intel und Xerox „standardisiert”
  - Von IEEE und ISO als Standard 802.3 in 1985 (geringfügige Abweichungen von Ethernet V.2, aber damit kompatibel)
  - Der Begriff Ethernet wird meist für beide Standards benutzt.
  - Übertragungsraten
    - Ethernet V.1: 2,94 MBit/s
    - Ethernet V.2/IEEE 802.3: 10 MBit/s
- Heutige Varianten:
  - Fast Ethernet (IEEE 802.3u) seit 1995
  - Gigabit Ethernet (IEEE 802.3z/IEEE 802.3ab) seit 1998/1999
  - 10G Ethernet (IEEE 802.3ae) seit 2002
  - Ethernet Switching statt Shared Ethernet seit 1990

Medienzugriffsverfahren

- Ethernet-Charakteristikum CSMA/CD
  - Carrier Sense, Multiple Access with Collision Detection
  - Gesprächsrunde ohne Diskussionsleiter.
- Bei einer solchen Diskussionsrunde gelten folgende Regeln:
  - Jeder Teilnehmer kann anfangen zu reden, wenn nicht schon ein anderer redet. (Carrier Sense)
  - Sollten mehrere Teilnehmer zufällig gleichzeitig in einer Gesprächspause anfangen zu reden (Multiple Access), so haben sie alle sofort ihren Beitrag abzubrechen (Collision Detection).
  - Durch zufällige Verzögerungen (oder Gesten) ergibt sich dann, wer als nächster reden darf.

CSMA/CD-Regel

- Carrier Sense
  - Sendewillige Stationen hören das Medium ab und warten bis es frei ist (Carrier Sense).
- Multiple Access
  - Ist das Medium frei, so kann jede sendewillige Station nach einer Pause von 96 Bit (12 Byte, 9,6µs [bei 10Mbit/s], ***Interframe Gap***) einen Sendevorgang beginnen.
- Collison Detection
  - Während des Sendens überprüft jede Station ob andere Stationen gleichzeitig senden, es also zu einer Kollision kommt.
  - Kollisionen werden an der Überlagerung von Signalen (überhöhte Signalpegel, Phasenverschiebung der Signale) erkannt.

Kollisionsbehandlung

- Alle Stationen müssen Kollisionszustand erkennen
  - Signalisierung des Kollisionszustand mit Jam Signal:
  - Nach dem Erkennen einer Kollision werden noch 4-6 weitere Byte (als 01-Bitmuster) gesendet.
- Interframe Gap
  - Nach dem Ende aller Übertragungen während eines Kollisionsvorgangs warten alle Stationen 9,6µs.
- Backoff-Algorithmus
  - Die kollisionserzeugenden Stationen warten zusätzlich ein Vielfaches i der „***Slot time***“ (512 Bit, 64 Byte, 51,2µs [bei 10 Mbit/s]),
  - wobei i eine Zufallszahl zwischen 0 und 2^k ist
  - und k die Nummer des Übertragungsversuchs für ein bestimmtes Paket (maximal 10) ist.
- Excessive Collision
  - Abruch nach 16maliger Kollision für ein Paket
  - Fehlermeldung an die Anwendung

Vor- und Nachteile von CSMA/CD

- Einfach zu Realisieren
- Keine Garantie für Medienzugriff
- Kollisionswahrscheinlichkeit steigt
  - mit Anzahl der Endstationen
  - Entfernung der Endstationen (Längere Übertragungswege, daher wird die gleichzeitige Nutzung im Durchschnitt später erkannt)
  - Netzlast
- Verschwendung von Übertragungsbandbreite bei hohen Kollisionsraten
  - effektive Datenrate < nominelle Datenrate
- Beschränkungen durch Notwendigkeit der Kollisionserkennung durch alle Beteiligten

Struktur einer Ethernet-Installation

- Einfachster Fall
  - Alle Stationen sind über ein Koaxialkabel in Reihe verbunden (Bus).
  - An den Enden des Kabel befindet sich je ein ***Abschlußwiderstand*** von 50 Ω.
- Problem der Dämpfung
  - Wegen der immer vorhanden Abschwächung der Signal mit der Kabellänge, haben Netzkabel eine maximal zulässige Länge (je nach Kabel und Datenrate 25-500m Kupfer, 260-5000m LWL).
  - Bei Überschreiten der maximalen Länge müssen Verstärker (***Repeater***) eingesetzt werden.
  - Die Kabelabschnitte, die über Repeater verbunden werden, werden ***Segmente*** genannt.

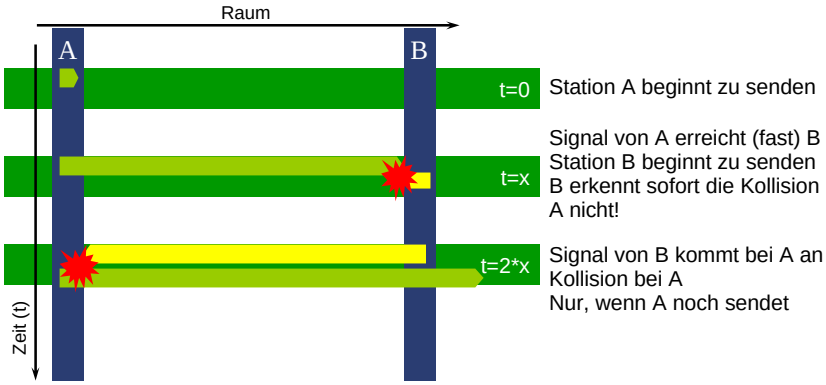
Repeater

- Verstärkerfunktion
  - Digitale Signalregeneration
  - Überwindung dämpfungsbedingter Längenrestriktionen
- Kollisionsdomäne
  - Alle durch Repeater verbunden Segmente bilden bezüglich des CSMA/CD-Algorithmus eine Einheit
- Durch Repeater darf kein Ringschluss entstehen
- Verzögerung der Signalübertragung
  - (Alte) Faustregel: Ein Repeater entspricht ungefähr einem 500m Segment (2µs, 20 Bit bei 10 Mbit/s).
- Zunächst zwei Ports, später Multiport-Repeater
- Verteiler bei sternförmiger Kabelstruktur

Repeater-Funktionalitäten

- Signalregeneration
- Auto-Partioning
  - automatische Abschaltung von gestörten Segmenten
- Repeater-Jam:
  - Signalisierung von Kollisionen von einem Segment in ein anderes
  - Auf allen Segmenten wird ein Paket mit einem 01-Muster gesendet, das aber kürzer als minimal vorgeschrieben (also fehlerhaft) ist.
- Übergang zwischen verschiedenen Kabelvarianten (bei gleicher Datenrate)

Kommunikation mit Kollision



Hätte Station A den Sendevorgang zum Zeitpunkt 2*x schon beendet, so hätte A die Kollision nicht erkannt, wodurch das CSMA/CD-Verfahren zusammenbrechen würde (CD!).

Kollisionserkennung und Folgen

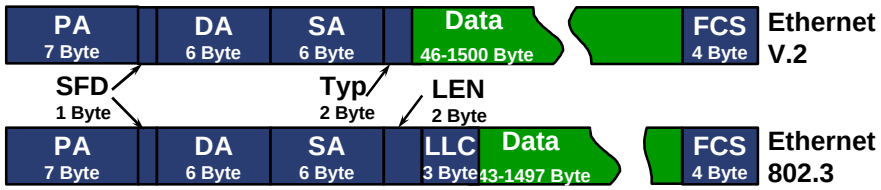
- Konsequenz des Kollisionserkennungsnotwendigkeit:
  - ***Maximale Round-Trip-Time*** zwischen zwei Stationen im Netz muss kleiner als
  - ***minimale Sendedauer (Paketlänge / Übertragungsrate)*** sein
- Ethernet-Grenzwerte:
  - 10 Mbit/s: RTT = 51,2µs (512 Bit, 64 Byte)
  - 100 Mbit/s: RTT = 5,12µs (512 Bit, 64 Byte)
  - 1000 Mbit/s: RTT = 4,096µs (4096 Bit, 512 Byte)
- Abhängigkeit der Round-Trip-Time
  - ***Kabellänge / Ausbreitungsgeschwindigkeit*** des Signals auf dem Medium
  - und den ***Verzögerungen*** durch die aktiven Komponenten im Netz
    - Sendern und Empfängern
    - Verstärkern (entscheidend!)
- Einhalten der Grenzen durch
  - Beschränkung in der Ausdehnung des Netzes
  - Beschränkung der Anzahl der Verstärker zwischen je zwei Stationen.

CSMA/CD und Übertragungsraten

- Abhängigkeit des CSMA/CD-Algorithmus von der Übertragungsrate
  - Sendedauer = Paketlänge / Übertragungsrate
  - Größere Übertragungsrate erzwingt kleiner RTT durch
    - Erhöhung der ***minimalen Paketlänge***
      - Verschwendung von Bandbreite bei kleinen Informationseinheiten oder Kollisionen
      - Bei 1000 Mbit/s verwendet
    - Verringerung der ***Netzwerkausdehnung***
      - kürzere Kabellänge
      - weniger Repeater
      - bei 100 Mbit/s verwendet

Paketformate

Ethernet-Kontrollinformation (Rahmen) **Übertragene Daten**



PA: Präambel zur Synchronisation des Empfängers auf den Takt des Senders mit einer Folge von 0 und 1

SFD: Start of Frame Delimiter, kennzeichnet den Beginn des eigentlichen Pakets und hat das Format 10101011.

DA Destination Address, Zieladresse

SA Source Address, Quelladresse

Typ: Typfeld zur Identifikation des Protokolls der übergeordneten Ebene

LEN: Länge des Pakets

LLC: "Logical Link Control"-Information (IEEE 802.2-Standard)

Data: Datenrahmen der übergeordneten Schichten

FCS: Frame Check Sequenz

Die Übertragung der Bits eines jeden Bytes erfolgt mit dem niederwertigste Bit zuerst (***lsb***, least significant bit)

Adressierung

- MAC-Adresse
  - Eindeutige Adresse, mit der Stationen angesprochen werden.
  - 48 Bit lang
- Adresstypen
  - Unicast-Adressen für einzelne Stationen
  - Gruppenadressen oder Funktionsadressen
    - Adresse für eine Gruppe von Rechnern
    - das erste Bit der Adresse eine 1,
    - Multicast-Adressen (an viele)
    - Broadcast-Adresse (an alle): binär 48 Einsen, hexadezimal FFFFFFFFFFFF
- Hardware-Adressen
  - von Netzwerkadapter-Herstellern von festgelegt,
  - 24 Bit Herstellerskode plus 24 Bit Seriennummer
  - keine Systematik bezogen auf die Netzstruktur oder Rechnereigenschaften
- lokale Adressen oder Software-Adressen
  - Von Rechnersoftware definiert
  - Möglichkeit höhere Systematik in die Adressen zu bringen
  - Adressen mit Wert 1 an Bitposition 2
  - universalen Adressen mit einer 0 an Bitposition 2.

Paketedefekte

- CRC-Fehler: Die Prüfsequenz ist falsch.
- Alignment-Fehler: Die Anzahl der Bits ist nicht durch 8 teilbar.
- Runt-Pakete: Pakete, die kürzer sind als die minimale Länge.
- Jabber- oder Giant-Pakete: Pakete mit Überlänge
- Late Collisions: Kollisionen, die nach mehr als 51,2 µs nach Beginn des Pakets auftreten.
- Excessive Collisions: 16 Kollisionen beim Versuch ein Paket zu senden.

Ethernet-Varianten

	Bezeichnung
• Unterscheidung nach	
– Datenrate	10, 100, 1000, 10G
– Übertragungsverfahren	
• eine Übertragungsfrequenz (Basisband-Übertragung)	Base
• mehrere Frequenzen (Broadband-Übertragung, bedeutungslos)	Broad
– Verkabelung	
• Koaxialkabel (zwei Varianten)	5, 2 (500 oder 200 m Kabel)
• Twisted-Pair-Kabel	T, TX, T4 (2 oder 4 Paare)
• LWL und Wellenlänge	FL, SX, LX
• Bezeichnungsschema	
– Datenrate + Übertragungsverfahren + Kabeltyp	10Base5, 10Base2, 10BaseT, 10BaseFL 100BaseTX, 100BaseFX, 100BaseT4 1000BaseSX, 1000BaseLX

Ethernet-Varianten (10 Mbit/s)

- Historisch
  - 10Base5 (Ethernet V.2, 1980 bzw. IEEE 802.3, 1985)
    - mit Koaxialkabeln (Yellow Cable)
    - auch Thickwire-Ethernet genannt,
  - 10Base2 (IEEE 802.3a, 1985)
    - oder Cheapernet, Thinwire-Ethernet (Basis 3Com)
    - als billigere und leichter zu installierende Variante,
  - 10BaseT (IEEE 802.3i, 1990)
    - als Variante über Twisted-Pair-Kabel
    - unter Verwendung vorhandener Kabel in USA und
  - FOIRL (IEEE 802.3d, 1987) und 10BaseF (IEEE 802.3j, 1993) für LWL

10 Base 5 und 10 Base 2

- Heute veraltet
- 500m / 185m maximale Segmentlänge
- Koaxialkabel mit
  - 50 Ω Wellenwiderstand
  - 0,77c / 0,65c Signalausbreitungsgeschwindigkeit (c = Lichtgeschwindigkeit = 300.000 km/s)
  - ca. 1cm / 0,5cm Durchmesser
  - 25cm / 5cm Biegeradius (beim Verlegen einzuhaltender minimaler Radius einer Biegung des Kabels)
- Maximale Anzahl Anschlüsse pro Segment: 100 / 30
- Anschluss:
  - 10 Base 5 über ***MAU***s (MAU=Media Access Unit, auch ***Transceiver*** (=***Trans***mitter/Re***ceiver*** genannt)
  - Anschluß von Stationen an MAUs über maximal 50 m lange „Dropkabel“
  - 10 Base 2 über T-Stücke, später unterbrechungsfreie Steckverbindungen / Dosen
- Maximal 1024 Stationen im Netz (genauer: innerhalb einer Kollisionsdomäne)
- Mindestabstand zwischen zwei Anschlüssen: genau 2,5m / mindestens 0,5m
- Maximal zwei Repeater zwischen zwei beliebigen Knoten

10 Base T

- Ethernet über Twisted-Pair-Kabel
  - moderne, strukturierte, sternförmige, standardisierte, diensteunabhängige Verkabelung
  - UTP, STP oder SSTP-Kabel mit 100 Ω Wellenwiderstand
  - verschiedene Standardkabel
    - Kategorie3 bis 20 MHz
    - Kategorie 5 bis 100 MHz (heutige Standardverkabelung)
    - Kategorie 6 und 7 bis 200 bzw. 600 MHz
  - Verwendung der Adernpaare auf Kontakten 1/2 und 3/6 des RJ45-Stecker
  - Maximale Kabellänge für einen Anschluß: 100 m
  - Maximal vier Repeater zwischen zwei beliebigen Knoten
- Kostenintensiver als Koaxialvarianten
  - da größere Kabelmengen zu installieren sind
  - und ein Repeaterport für jeden einzelnen Anschluß nötig ist,
  - aber zukunftsicherste Verkabelungsvariante (mit Kupferkabeln)

10 Base FL

- Ethernet über Lichtwellenleiter
  - moderne, strukturierte, sternförmige, standardisierte Verkabelung
- Glasfaserkabel
  - Gradientenkabel 50/125µm oder 62,5/125µ im 850 nm Fenster
  - Zwei Fasern pro Verbindung
  - 2000 m maximale Kabellänge für einen Anschluß:
  - Anschlußtechnik: ST-Steckerverbinder, neuerdings auch SC
  - Maximal vier Repeater zwischen zwei beliebigen Knoten
- Kostenintensivste Variante
  - Repeaterport für jeden einzelnen Anschluß
  - Verkabelung je nach Gebäudebedingungen meist etwas teuerer als TP
  - Aktive Komponenten deutlich teuerer als für Kupfertechnologie
  - Geringer Portdichten bei Repeatern und anderen aktiven Komponenten

Fast Ethernet

- Erhöhung der Datenrate auf 100 MBit/s
- 1995 standardisiert als IEEE 802.3u
- für strukturierte Verkabelungen:
  - keine physikalischen Busstrukturen vorgesehen,
  - keine Koaxialkabel vorgesehen,
  - 2 Varianten für TP-Kabel (100BaseTX, 100BaseT4)
  - Standard für LWL-Verkabelung (100BaseFX)
- Einschränkung der Netzwerkausdehnung gegenüber Standard-Ethernet zwecks Kollisionserkennung

100 Base TX und 100 Base T4

- Strukturierte Verkabelung
  - 100BaseTX für Kabel der Kategorie 5
    - Benutzung von 2 Adernpaaren wie 10BaseT
    - 31,25 MHz Übertragungsfrequenz mit 4B/5B- und MLT-3-Kodierung
  - 100BaseT4 für Kabel der Kategorie 3
    - Benutzung von 4 Adernpaaren
    - Halbierung der Übertragungsfrequenz durch Aufteilung der Übertragung
- Netzwerkausdehnung:
  - Maximale Kabellänge für einen Anschluß: 100 m
  - maximal 2 Repeater zwischen zwei beliebigen Knoten
  - maximal 5 m Verbindungskabel zwischen Repeatern

100 Base FX

- Glasfaserkabel
  - Gradientenkabel 50/125µm oder 62,5/125µm
  - Selten Monomodekabel 9/125µ
  - Zwei Fasern pro Verbindung
  - Anschlußtechnik: überwiegend SC-Steckerverbinder
  - Übertragung mit 1300 nm Wellenlänge
- Netzwerkausdehnung:
  - Maximale Kabellänge für einen Anschluß: 450 m (wegen RTT!)
  - maximale Kabellänge für einen Anschluß bei Vollduplex-Übertragung (kollisionsfrei!): 2000 m
  - maximal 2 Repeater zwischen zwei beliebigen Knoten
  - maximal 5 m Verbindungskabel zwischen Repeatern

Gigabit Ethernet

- Steigerung der Übertragungsrate auf 1000 MBit/s
- 1998 Standard IEEE 802.3z
  - Varianten für verschiedene LWL-Übertragungsfenster
    - 1000BaseSX bei 850nm
    - 1000BaseLX bei 1300nm
  - Varianten für verschiedene LWL-Kabeltypen
    - MMF 50/125µm (2-550m Kabellänge)
    - MMF 62,5/125µm (2-260m Kabellänge)
    - SMF 10/125µm (2-5000m Kabellänge)
  - für Twinax-Kabel (1000Base-CX, maximal 25m Kabel, unbedeutend)
- Standard für TP-Kabel (802.3.ab)
  - maximale Kabellänge 100m
  - über 4 Adernpaare gleichzeitig Senden und Empfangen
  - mit 31,25 MHz Frequenz
  - durch geeignete Kodierung
- Erhöhung der minimalen Paketgröße auf 512 Byte zwecks Kollisionserkennung (soweit nötig)
- Achtung: PC-Busse sind meist langsamer und können das Gigabit gar nicht umsetzen!

10 Gigabit Ethernet

- Steigerung der Übertragungsrate auf 10.000 Bit/s
- Standard IEEE 802.3ae für Glasfaserkabel in 2002
  - Über SMF (10 km bei 1310 nm, 40 km bei 1550 nm)
  - Über MMF (26-300m bei 850 bzw. 1310 nm je nach Kabelqualität)
  - Spezielle LAN (10 Gbit/s) und WAN-Varianten (9,.. GBit/s)
- Variante über Kupferkabel (Kategorie 5E) in Entwicklung (100m Kabellänge)
- Keine Repeater-Varianten mehr, nur noch Switches und Vollduplex
- Einsatzszenario bisher:
  - Weitverkehrsverbindungen
  - Zusammenschaltung von Gigabit-Ethernet-Switches
  - bisher keine Endgeräteanschlüsse

Vollduplex und Autonegotiation

- Halbduplex- / Vollduplex-Übertragung
  - TP- und LWL-Verkabelungen erlauben gleichzeitiges Senden und Empfangen (Vollduplexübertragung)
  - im Gegensatz zu Koaxialkabeln (Halbduplexverfahren)
  - Damit ist eine kollisionsfrei Übertragung möglich.
  - Bei 100BaseFX kann dadurch (bei Einsatz von Switches) die maximale Entfernung auf 2000 m erhöht werden.
- Autonegotiation
  - Standard zur automatischen Erkennung
    - der Übertragungsrate (10/100/1000 MBit/s) bei Kupferanschlüssen
    - Halbduplex- oder Vollduplexverfahren (IEEE 802.3x, 1997)
    - Flow-Control bei Vollduplex-Ethernet
    - bei Fast Ethernet (IEEE 802.3u, 1995) eingeführt
    - im Gigabit-Ethernet-Standard erweitert (IEEE 802.3z/ab)

Repeaterregel

- Maximale Signallaufzeit begrenzt Anzahl der Repeater zwischen zwei Stationen
- 10 Base 5 / 10 Base 2
  - maximal zwei Repeater zwischen zwei Stationen (drei Segmente) oder
  - maximal vier Repeater zwischen zwei Stationen (fünf Segmente), wenn zwei Segmente nur „Link-Segmente“ sind (keine Stationen angeschlossen).
- 10 Base T / 10 Base F
  - alle Segmente, über die Repeater gekoppelt werden, sind Link-Segmente: maximal 4 Repeater
- 100 Base T / 100 Base F
  - maximal 2 Repeater (mit einem 5m Verbindungskabel)

Ethernet-Parameter

Parameter	Bezeichnung / Formel	Einheit	10Base5	10Base2	10BaseT	10BaseFL
Übertragungsrate	v	bit/s	10.000.000			
Lichtgeschwindigkeit	c	m/s	299.792.458			
Ausbreitungskoeffizient	n		0,77	0,65	0,75	0,68
Maximale Segmentlänge	l_{max}	m	500	185	100	2000
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	µs	2,166	0,949	0,445	9,811
Dauer eines Bits	$t_{bit} = 1/v$	µs	0,1	0,1	0,1	0,1
Länge eines Bits	$l_{bit} = nc/t_{bit}$	m	23,08	19,49	22,48	20,39
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$		21,66	9,49	4,45	98,09
Dauer von 64 Bytes (RTT)	$t_{64Byte} = t_{bit} *8*64$	µs	51,2	51,2	51,2	51,2
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	m	11.817	9.979	11.510	10.440

Parameter	Bezeichnung / Formel	Einheit	100BaseTX	100BaseFX	1000BaseSX
Übertragungsrate	v	bit/s	100.000.000		1.000.000.000
Lichtgeschwindigkeit	c	m/s	299.792.458		
Ausbreitungskoeffizient	n		0,75	0,68	0,68
Maximale Segmentlänge	l_{max}	m	100	450	550
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	µs	0,445	2,21	2,70
Dauer eines Bits	$t_{bit} = 1/v$	µs	0,01	0,01	0,001
Länge eines Bits	$l_{bit} = nc/t_{bit}$	m	2,25	2,04	0,2
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$		44,44	220,59	2750
Dauer von 64 Bytes (RTT)	$t_{64Byte} = t_{bit} *8*64$	µs	5,12	5,12	0,51
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	m	1.152	1.044	102

Teil IV: LAN-Switching

Grenzen von Shared-LANs

- Anzahl anschließbarer Knoten ist begrenzt,
- Bandbreite ist begrenzt
- und muß geteilt werden,
- Ausdehnung ist begrenzt (z.B. Kollisionsdomänen im Ethernet),
- Fehlerhafte Pakete verbreiten sich im gesamten Netz,
- verschiedene Technologien können nicht gekoppelt werden (schon Ethernet und Fast Ethernet)

Überbrückung von LAN-Begrenzungen

- Bildung mehrere (zunächst) getrennter LANs
  - in der Summe beliebig viele Knoten anschließbar
  - n LANs haben die n-fache Bandbreite eines LANs
  - mehrere LANs können beliebig geographisch verteilt werden
  - Fehler bleiben lokal
  - Verteilung der inhaltlich am engsten zusammengehörigen Knoten in gleiche LANs
- Mikrosegmentierung
  - Optimierung von LANs zur Bewältigung ständig wachsender Bandbreitenanforderungen
  - Aufteilung in LANs mit sehr wenigen Knoten
  - bis zu Segmenten mit nur je einem Knoten
  - ***LAN-Switching***

LAN-Kopplung

- LAN-Kopplung
  - Kopplungsgeräte leiten selektiv Pakete zwischen LANs weiter
  - Verschiedene Varianten und Bezeichnungen
  - mit teilweise verschiedenen Funktionen:
    - Allgemein: Vermittlungssysteme
    - Speziell: Brücken/Bridges, Switches, Router, Gateways
- Prinzip der Kopplung
  - Vermittlungssysteme sind Knoten mit mehreren Netzadaptern,
  - Vermittlungssysteme empfangen Pakete von einem Netz
  - und senden diese in einem oder mehreren Netzen wieder aus,
  - mit getrennten Sende- und Empfangsvorgängen,
  - (meist) Zwischenspeicherung empfangener Pakete (Store&Forward-Prinzip)
  - und selektiver Weiterleitungsfunktion (Forwarding)

Paketweiterleitung

- Problem der Weiterleitung
  - Vermittlungssysteme müssen entscheiden,
  - welche Pakete weitergeleitet werden
  - und wohin Pakete weitergeleitet werden.
- Ansätze zur Problemlösung
  - Der Absender bestimmt explizit durch Angaben im Paket über die Wege eines Pakets durch das Netz (Source Routing)
    - Problem für den Absender
    - Lösung bei Token-Ring
  - Aufbau virtueller Leitungen über Vermittlungssysteme und Übertragung über diese Leitungen (verbindungsorientierte Kommunikation)
    - Problem beim Verbindungsaufbau
    - Lösung in WANs und bei ATM
  - Einzelvermittlung jedes Pakets bei autonomer Entscheidung der Vermittlungssysteme (verbindungslose Kommunikation)
    - Problem für die Vermittlungssysteme
    - Typische LAN-Lösung

Weiterleitung bei verbindungsloser Kommunikation

- Weiterleitung anhand Adresstabelle
  - Forwarding Table mit Information
    - Welche Adresse (im LAN: MAC-Adresse)
    - befindet sich an welchem Port.
  - Aufbau der Tabelle
    - manuell und statisch durch Administrator,
    - und/oder selbstlernend und dynamisch durch Vermittlungssystem
    - im LAN fast ausschließlich dynamisch
  - Lernfunktion
    - Tabellenaufbau durch Mitlesen der Absenderadressen ankommender Pakete
  - Alterungsfunktion
    - Löschen von Einträgen nach definierter (konfigurierbarer) Zeit

Bridges und Switches in LANs

- Direkte Kopplung von LANs
  - Vermittlungssysteme mit Anschlüssen an LANs gleicher MAC-Technologie
  - Verbindungslose Kommunikation
  - Forwarding-Tabelle mit MAC-Adressen
  - LAN-Pakete werden nicht verändert
- Ziele
  - Vorrangig: Lasttrennung / Erhöhung der Gesamtbandbreite
  - Nebenzweck: Isolation von Paketfehlern
  - Manchmal: Ausdehnung vergrößern
- Bezeichnung
  - Brücke / Bridge
    - Bezeichnung für frühe Systeme
    - mit meist nur zwei (oder wenig mehr) Ports
  - Switch
    - Bezeichnung für moderne Systeme
    - mit vielen Ports
    - im Zuge der zunehmenden Tendenz zur Mikrosegmentierung zur Bandbreitenerhöhung

Paketarten und Weiterleitung

- Unicast-Pakete
  - wenn Zieladresse in der Forwarding-Tabelle:
    - zum angegeben Port/Segment weiterleiten
  - wenn Zieladresse unbekannt:
    - meist weiterleiten in alle Segmente (Fluten)
    - oder (selten, Workgroup-Bridges) Paket wird nicht weitergeleitet (Verwerfen)
    - oder weiterleiten nur an einen bestimmten Port
      - eingesetzt bei Brücken zum Anschluß von Arbeitsgruppen an Backbone-Netze (Workgroup-Bridges)
      - insbesondere auch bei Switches zum Anschluss von je einer Station pro Port (Desktop-Switches)
- Broadcast- und Multicast-Pakete
  - weiterleiten an alle Segmente

Store & Forward

- Zwischenspeicherung von Paketen
  - Einlesen des gesamten Pakets vor Weiterleitung
    - Nachteil: Erhöhung der Latenz im Netzverkehr (100-1200 µs je nach Paketlänge)
    - Vorteil: Isolation von fehlerhaften Paketen
    - und Trennung von Kollisionsdomänen
- Alternative:
  - Weiterleitung nach Einlesen der Zieladresse (und Lookup in Forwarding-Tabelle)
    - Geringere Latenz (ca. 40 µs, ähnlich Repeater, unabhängig von Paketlänge)
    - Weiterleitung von defekten Paketen und Paketfragmenten
  - Bezeichnungen: cut through, on the fly
- Zwischenlösung
  - Weiterleitung nach Einlesen der minimalen Paketlänge
    - Konstante Latenz bei ca. 100 µs
    - Großer Teil der fehlerhaften Pakete aussortiert
  - Bezeichnung: Fragment free
- Mischlösung
  - Konfiguration der Varianten durch Administrator
  - Dynamische Umschaltung anhand Fehlerraten
- Alle Zahlen für 10 Mbit/s
  - Bei höheren Übertragungs-raten verkürzt sich die Zeit für das Speichern!
  - Latenz dann weitgehend von Lookup und interner Übertragung abhängig

Problem der Schleifenverhinderung

- Schleifen sind verboten,
  - da sie zu einer Vervielfachung von Paketen führen würden und
  - die Forwarding-Tabelle undefiniert wäre.
- Erste Lösung:
  - Brücken dürfen nicht so platziert werden, daß Schleifen entstehen könnten.
- Zweite Lösung (Spanning Tree):
  - Dynamische Abschaltung von Brücken, die zu einer Schleifenbildung beitragen würden.
  - Dazu tauschen Brücken untereinander Informationen aus, um Schleifenbildungen zu erkennen und zu verhindern (Spanning Tree Protokoll IEEE 802.1d / Rapid Spanning Tree IEEE 802.1w)
  - Vorteil: Ein redundanter Weg kann vorgehalten werden, der bei Ausfall einer Verbindung aktiviert werden kann.
  - Bei Ethernet und FDDI gängig, evtl. ein- und abschaltbar

Remote-Brücken

- Zur Kopplung von Netzen über andere Medien z.B.
  - Fernmeldeleitungen,
  - Funkstrecken
- Je Brücke ein oder mehrere Remote- und ein oder mehrere lokale Ports
- Einsatz immer paarweise (meist baugleiche Brücken)
- Ein Paar stellt funktional eine Brücke dar.
- Andere Brücken heißen korrekt „lokale Brücken”

Translation und Encapsulation

- Standardfall: Kopplung gleicher Netztechnologie (MAC)
  - Transparent-Bridges
  - bei unterschiedlicher Datenrate: Store&Forward zwingend
- Brücken zwischen verschiedenen Netzwerktechnologien
  - MAC-Protokollumsetzung bei verschiedener MAC-Teilschicht
    - Translation-Bridges
    - Anpassung der MAC-Adressen (lsb/msb)
    - Store&Forward zwingend
    - Unterschiedliche maximale Paketlängen
      - IP-Protokoll erlaubt Fragmentierung von Paketen durch Vermittlungssysteme,
      - sonst Datenverlust bei zu langen Paketen
      - oder Endstationen müssen maximale Paketlänge (MTU, Maximal Transmit Unit) aushandeln.
  - Alternativ
    - Originalpaket in MAC-Rahmen des anderen Netze einpacken
    - Encapsulation-Bridges
    - nur möglich, wenn das andere Netze nur als Durchgang benutzt wird

LAN-Switching

- Mikrosegmentierung
  - Ein Endgerät pro Segment
  - Dedizierte Bandbreite für jedes Endgerät
  - Vollduplex-Übertragung möglich
- Non-Blocking-Architektur
  - Verhinderung von Blockierungen beim Weg durch den Switch
  - soweit nicht einzelne Ausgangsports überlastet sind
  - schnellere Anschlüsse für stark belastete Ports (z.B. Server)
- Größere Netze
  - Kopplung mehrere Switches
  - Switches untereinander mit höheren Bandbreiten verbinden als zu Endgeräten
  - daher häufig einzelne Ports der nächst schnelleren Technologie
  - Problem Überbuchung oder ausreichende Backbonekapazität für alle lokalen Ports
- Link Aggregation (IEEE 802.3ad, 2000)
  - Bündelung von Ports für schnelle Switch-zu-Switch-Verbindungen
- Existent für Ethernet, Token Ring, FDDI (ATM sowieso)

Technische Realisierungsvarianten

- Vermittlung
  - Matrix / Crossbar
  - Schneller interner Bus mit Cell- oder Frame-Switching
  - Shared Memory
- Verschiedene Prozessorarchitekturen
  - Paketprozessoren (ASICs) an jedem Port (heute Standard)
  - Softwarelösung mit zentralen RISC-Prozessoren
- Zwischenspeicherungsvarianten
  - Pufferung bei belegtem Ausgang
  - Eingangspuffer (Problem bei Staus an einzelnen Ausgängen)
  - und/oder Ausgangspuffer
- Reaktion auf Überlastung von Ports
  - Flow-Control-Protokolle im Vollduplexmodus möglich
  - Bewusste Kollisionserzeugung bei vollem Puffer (Contention Management, Back Pressure) in Halbduplex-Varianten

Virtuelle LANs

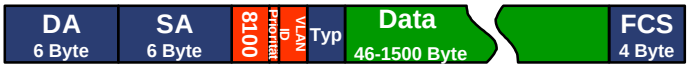
- Virtuelle LANs (VLANs):
  - Unterteilung eines physikalischen Netzwerks
  - auf Layer-2
  - in mehrere Layer-2-Netzwerke,
    - d.h. Broadcast-Domänen,
    - die voneinander unabhängig sind
    - durch Einsatz von speziellen LAN-Switches
- Kommunikation in und zwischen VLANs
  - In VLANs wie in einem normalen LANs
  - Zwischen VLANs nur über Routing-Funktionalitäten
    - in Form eines Routers
    - oder durch Routing-Funktionalität in Switches

Zuordnung zu VLANs

- Kriterien für die Zuordnung
  - Switch-Ports
  - MAC-Adressen
  - Layer-3-Adressen (insbesondere IP-Adressen)
  - Netzwerkprotokolle
- Konfiguration von VLANs
  - auf den einzelnen Switches
  - oder über einen speziellen VLAN-Server (Rechner mit spezieller Software)
  - Dynamisch über Protokolle
  - Dynamisch nach Anforderung der Endgeräte

Switchübergreifende VLANs

- Problem:
  - Mehrere VLANs auf den Verbindungen zwichen den Switches
  - Zuordnung von Paketen zu VLANs?
- Kennzeichnung der Pakete (Frame Tagging)
  - Modifikation des Pakets durch den ersten Switch: Einfügen einer Markierung (Tag)
  - Ein VLAN (Default oder Native VLAN) kann unmarkiert bleiben
  - Markierung durch „VLAN Tag Header“:
    - Tag Protocol Identifier (TPID): Wert 8100 (hexadezimal) statt Ethernet-Typfeld
    - Tag Control Incormation (TCI): 3 Bit Priorität, 12 Bit VLAN Identifier VID (also 1-4096)



  - letzter Switch erzeugt wieder das ursprüngliche Paket durch Entfernen der Markierung,
  - Abweichung vom Standard-Paketformat (4 Byte längere Pakete),
  - muss von allen beteiligten Switches verstanden werden,
  - Standard IEEE 802.1Q bzw. 802.3ac (1998)
- Alternativ: VLANs auf Basis von Layer-3-Kriterien
  - Normales Paket enthält dann Informationen, die die Zuordnung zu VLANs erlauben

Einsatz von VLANs

- In großen Netzen,
  - zur Begrenzung der Broadcast-Belastung
- Logische Trennung von Teilbereichen
  - z.B. Abteilungen einer Firma
  - über mehrere Verteilerstandorte ein Layer-2-Netz
- Zur Verringerung der Managementaufwands (?)
  - als Alternative zu router-basierten Lösungen zur Separierung
  - flexibler, weil Adressen nicht ortsabhängig sind.

Teil V: Ethernet-Alternativen

VG-AnyLAN

- Konkurrierende Entwicklung zu 100BaseFX/T-Standards
- Eigentlich kein Ethernet, da nicht CSMA/CD-Algorithmus
- Demand Priority Verfahren:
  - Vergabe der Zugriffsberechtigung durch den zentralen Verteiler
    - auf Anforderung
    - mit Möglichkeit von Prioritätenvergabe
    - in festgelegter Reihenfolge der Ports
- Standardisiert als IEEE 802.12 (nicht 802.3 wie alle Ethernet-Varianten)
- Vierpaarige Kupferkabel

Token Ring und FDDI

- Token Ring
  - von IBM entwickelt
  - von IEEE/ISO standardisiert (IEEE 802.5)
  - Übertragungsraten 4 oder 16 MBit/s
  - 100 MBit/s-Variante in Entwicklung
- FDDI
  - Fiber Distribute Data Interface
  - ANSI Standard (X3T9.5)
  - 100 MBit/s Übertragungsrate
  - ursprünglich für LWL-Leitungen definiert
  - später auch für Kupferkabel (CDDI=Koax-Kabel, TPDDI=TP-Kabel)
- Ähnliches Medienzugriffsverfahren (Token-Prinzip)
  - Vergabe des Medienzugriffs in vordefinierter Reihenfolge

Token-Prinzip

- Alle Knoten erhalten in vorgegebener Reihenfolge für eine begrenzte Zeit die Sendeberechtigung
- Wie erkennt ein Knoten, wann er senden darf?
  - Vergabe des Zugriffsrechtes durch ein spezielles Signal (Token)
  - Das Token wird spätestens nach Ablauf der maximalen Sendezeit an den nächsten Knoten weitergegeben.
  - Als Token dient ein spezielles, kleines Datenpaket.
- Probleme des Token-Prinzips
  - Im Netz muss zu jedem Zeitpunkt genau ein Token existieren
    - Überwachung des Token-Protokolls nötig
  - Im Netz muss eine Reihenfolge definiert werden
    - Einfachste Lösung: (Logische) Ringstruktur
    - (Token-Bus ist als Standard theoretisch vorhanden)

Initialisierung und Kontrolle der Token

- Am Beispiel IBM-Token-Ring (FDDI ähnlich)
- Claim-Prozeß zur Initialisierung
  - alle Stationen senden beim Start spezielle Pakete (Claim-Frames)
  - mit denen sie beantragen, die Token erzeugende und kontrollierende Station zu werden
  - eine Station gewinnt und wird aktiver Monitor
  - und sendet regelmäßige Statusmeldungen
- Kontrolle der Token-Existenz durch den aktiven Monitor
- Kontrolle der Existenz eines aktiven Monitors
  - Aktiver Monitor sendet alle 7s Statusmeldungen
  - Wenn Statusmeldungen ausbleiben, wird der Claim-Prozeß neugestartet

Management-Protokoll (1)

- Fehlendes Token
  - Alle 10ms muss spätestens ein neues Paket oder Token beim aktiven Monitor ankommen (10ms, maximale Paketlänge 4.096 bzw. 17.800 Byte)
- Mehrfachumlauf eines Paketes
  - Aktiver Monitor setzt „Monitor Bit“ im Access Control Feld jedes Pakets.
  - Wenn das Bit schon gesetzt ist, liegt ein Fehler vor.
- Senden ohne Berechtigung
  - die Station, die sendet muss ohne andere Daten zwischendurch zu empfangen das eigene Paket zurückbekommen
  - andere Daten bedeuten Fehler anderer Stationen oder mehrere Token
- Doppelte MAC-Adressen
  - Empfänger setzt Adress Recognized Bit
  - Darf beim Empfänger ankommend noch nicht gesetzt sein

Management-Protokoll (2)

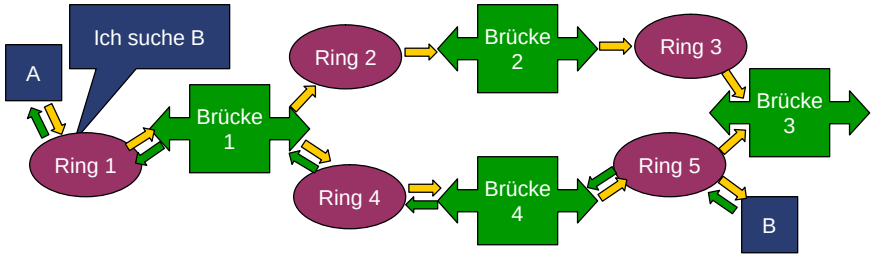
- Fehlerbehebung
  - aktiver Monitor leert den Ring
  - keine Daten weitergeben, dafür „Ring Purge“-Paket
- Minimale Speicherkapazität
  - von 24 Bit (Token-Länge) im Ring,
  - entspricht bei 4 MBit/s ca 1.200m bzw. bei 16 MBit/s 300m
  - daher ggf. Pufferung durch aktiven Monitor
- Takt wird vom Monitor vorgegeben
  - keine Präambel zur Synchronisation,
  - gegebenenfalls Aussenden von Idle-Signalen.
- Komplexität (und Kosten) des Token-Ring durch verschiedene Management-Funktionen, die von jeder Station aus ausführbar sein müssen.

Source Routing

- Im Token-Ring benutzt
- Explizite Festlegung des Weges eines Paketes durch den Sender
- Vorteil:
  - Redundante Wege
- Nachteile:
  - Overhead in Paketen
  - Problem der Routenfindung

Routenfindung

A sendet ein Explorer-Paket ⇨
Alle Brücken leiten das Paket an alle Netze weiter
Dabei werden die Brücken- und Ring-Nummern im Paket vermerkt



Pakete, in denen die eigene Nummer enthalten ist, gibt eine Brücke nicht weiter
Das Paket (oder die Pakete) kommt bei B an
⇦ B schickt das Paket mit entsprechenden Soure-Routing-Einträgen zurück
A kennt den Weg und kann Daten schicken

Es wird immer der aktuell schnellste Weg gewählt

Asynchronous Transfer Mode ATM

- Weiterentwicklung aus ISDN und Breitband-ISDN
- Standardisierung/Entwicklung durch ITU und ATM-Forum (Herstellervereinigung)
- Abwandlung des synchronen Zeitmultiplexing (STM):
  - feste Zellstruktur (alle Pakete sind 53 Byte groß) analog STM,
  - in jeder Zelle 5 Byte Header,
- verbindungsorientierte Kommunikation ähnlich Telekommunikationsdiensten
- Geschaltete Leitungen (Switched Circuits)
- Verbindung über ATM-Switches als Vermittlungsstellen
- Verschiedene Diensteklassen und Dienstgüten
- Zielsetzung: Integration von Sprach-, Bild und Datendiensten

Verbindungsmodell

- Verbindungsorientierte Kommunikation
- Schaltung von virtuellen Verbindung (Virtual Channel Connection, VCC):
  - Kennzeichnung der Verbindungen
    - durch eine Kombination von
    - virtuelle Pfadnummern (Virtual Path Identifier,VPI)
    - und virtuellen Kanalnummern (Virtual Channel Identifier, VCI).
  - Pfade und Kanäle bezeichnen
    - Verbindung zwischen zwei direkt verbundenen ATM-Knoten.
  - Die Knoten (ATM-Switches) haben eine Umsetzungstabelle VPI/VCI-Eingangsport zu VPI/VCI-Ausgangsport.
  - Ende-zu-Ende-Verbindung
    - durch viele verschiedene lokale VCCs
    - und Umsetzungstabellen der ATM-Switches
- Schwierige Phase ist der Verbindungsaufbau
  - Aufbau der Weiterleitungstabellen

Arten von VCCs

- Nach Art des Aufbaus der Kanäle:
  - PVC
    - Permanent Virtual Circuits,
    - feste definiert Kanäle,
    - vom Administrator permanent definiert.
  - SVC
    - Switched Virtual Circuits,
    - dynamisch aufgebaute Kanäle,
    - (durch Kommunikation der Endgeräte und ATM-Verteiler).
- Nach Art der Kommunikationsstruktur
  - Punkt-zu-Punkt-Verbindungen
  - Punkt-zu-Mehrpunkt-Verbindungen
  - keine Mehrpunkt-zu-Mehrpunkt-Verbindungen

Problem der Integration klassischer LANs

- Klassische LANs
  - („legacy LANs“)
  - kommunizieren verbindungslos,
  - basieren von ihren Protokollen her auf Broadcast/Multicast.
- Heutige Software
  - basiert auf klassischen LANs,
  - insbesondere Broadcasts
- ATM
  - arbeitet (schon auf Schicht 2) verbindungsorientiert,
  - unterstützt keine Broadcasts.
- Integration von legacy LANs über
  - Classical IP over ATM
  - LAN Emulation (LANE)
  - Multi Protocol over ATM (MPOA)

FunkLANs

- FunkLAN-Standard
  - IEEE 802.11b
  - Frequenzbereich: 2,4 GHz (13 cm Band, Mikrowelle), 13 Kanäle (22 MHz Abstand, teilweise überlappend, bis auf Kanal 1,7,13)
- Leistung
  - 0,035W an der Karte (teils auch regelbar),
  - 0,1W an der Antenne (erlaubt)
  - 1/10 – 1/60 eines Handy.
- Strukturen
  - Access Points (APs)
  - Rechner mit FunkLAN-Adaptern
  - evtl. zusätzliche Antennen
  - Shared Media Network wie das klassische Ethernet

Reichweiten

- Klassische Reichweiten
  - im Gebäude: stark abhängig vom Gebäude ca. 20-40 m
  - bei Antennen > 10dbi Gewinn bis zu 10 km
  - im freien Gelände: ca. 200-300 m
- Sende/Empfangsqualität wesentlich abhängig von
  - Gebäude
  - Antennen
  - Antennenkabel/Länge, Stecker etc.
  - Interferenzen mit anderen Funknetzen
  - frei Sicht (auf günstige Reflektionen kann man nicht hoffen)
- Übertragungsleistung:
  - brutto: 11 Mbit /shared
  - netto: 5-6 Mbit/s shared
  - neuere Systeme mit
    - brutto 22 Mbit/s (durch Kanalbündelung)
    - 54 Mbit/s (IEEE 802.11a- bzw. 802.11h-Standard bei 5 GHz oder IEEE 802.11g-Standard bei 2,4 GHz) bei geringerer Reichweite

Sicherheit im FunkLAN

- Abhören strukturbedingt leicht möglich
- Netz endet nicht an Gebäudegrenzen hinweg
- Verschlüsselung der Daten nötig
- Verschlüsselung in Funkkarten integriert
  - zwischen Adaptern und APs
  - ursprüngliches Verfahren WEP (Wired Equivalent Privacy) leicht zu knacken
  - WEP2 bietet Verbesserung
  - Problem des Schlüsselaustauschs wegen statischer (fester) Schlüssel bei vielen Teilnehmern
- Verschlüsselung zwischen Endgerät und zentralem Gateway
  - IP-SEC-Standard mit VPN-Gateway
  - spezieller VPN-Client auf Endgerät
  - Authentifizierung gegen RADIUS-Server mit Benutzername/Kennwort
- Angreifbarkeit von Endgeräten im FunkLAN wird leicht übersehen

Zugang zum FunkLAN

- Zugangsbeschränkung auf Basis von MAC-Adressen
  - APs können so konfiguriert werden, dass nur Verbindungen zu Adaptern mit registrierte MAC-Adressen aufgebaut werden
    - durch Eintragung aller Adressen in jedem AP (bei größeren Netzen kaum handhabbar)
    - oder durch Abgleich vom AP mit einem zentralen RADIUS-Server
  - MAC-Adressen sind im Kartentreiber konfigurierbar
    - unberechtigter Zugriff möglich durch Ausspähen der „gültigen“ MAC-Adressen
- Service Set Identifier (SSID)
  - Netzwerkname
  - nur nützlich, um nicht versehentlich in das falsche Netz zu geraten, falls mehrere parallel existieren
- Bei VPN-Lösung Authentifizierung über Benutzername und Kennwort

Teil VI: Globale Netze, Routing, Internet-Protokoll

GWDG

Überblick

- Globale Netze als Ziel
  - Verknüpfung lokaler Netze
  - beliebiger Netzwerktechnologie
  - zu einem (maximal) globalen Netz
  - mit sehr vielen angeschlossenen Teilnehmern
- Routing als Mittel
  - Finden von Wegen durch globale Netze
- Das Internet-Protokoll (IP)
  - als Beispiel
  - und de-facto-Standard für real existierende globale Netze

Rückblick auf Extented LANs

- Brücken und (LAN-) Switches
  - als Hilfsmittel zur Bildung von Extented LANs (Brücken)
  - oder als Hilfsmittel zur Mikrosegmentierung (LAN-Switches)
- Grenzen von Extented LANs
  - Mangelnde Skalierbarkeit
    - durch Weitergabe von Broadcasts/Multicasts,
    - Größe von Adresstabellen,
    - Redundante Wege und Spanning Tree
  - Begrenzte Heterogenität
    - Einsetzbar in Netzen gleicher (MAC-) Technologie
    - oder zumindest mit kompatiblem Adressformat
- Vorteile von Extented LANs
  - Transparenz von Brücken/Switches
    - Die Endgeräte müssen von der Existenz der Brücken nichts wissen,
    - d.h. es ist keine spezielle Software (Protokolle) nötig.
    - (Allerdings kann die Transparenz zu dem gefährlichen Trugschluss verleiten, dass Pakete nicht verloren gehen können und immer in der richtigen Reihenfolge ankommen)

Adressierung in globalen Netzen

- Adressen in Shared-Media-LANs
  - einheitliche Formate,
  - eindeutige (flache) Adresse
  - reichen zur Paketübertragung in einem Shared LAN,
  - weil jeder Teilnehmer jedes Paket „sieht“.
- In globalen Netzen trifft das alles nicht mehr zu
- Globale Netze
  - Zusammengesetzte Netze aus Netzen
  - Zusammengesetzte hierarchische Adressen:
    - Adressteil zur Bezeichnung des (Teil-) Netzes
    - Adressteil zur Bezeichnung der Rechner in den (Teil-) Netzen
    - Beispiele:
      - Telefonnumern mit Landes-, Ortsnetz- und Teilnehmernummer
      - Postleitzahlen

Routing und Forwarding

- Aufgaben von Paketvermittlungssystemen (Packet-Switch)
  - Forwarding
    - Gezielte Weiterleitung von Paketen zwischen Ein/Ausgängen (Ports)
    - Anhand von Informationen
      - in den empfangenen Paketen (Adressen, Kanalbezeichnungen)
      - und im Vermittlungssystem (Routing Table)
  - Routing
    - Aufbau von Informationen
      - im Packet-Switch
      - über Wege (Routen) durch das Netz
- Bezeichnung der Packet-Switches: Router

Grundkonzept des Internet-Protokolls

- Datagrammdienst
  - Übertragung einzelner, voneinander unabhängiger Paketen (verbindungslose Kommunikation)
  - Paketstruktur

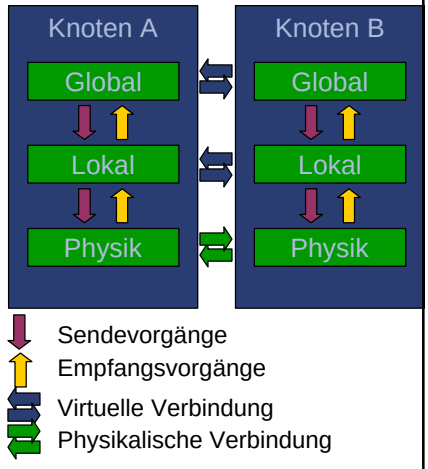
    - IP-Header mit Steuerinformation
    - IP-Datenteil
  - Einpacken der IP-Paketen in Pakete verschiedener Netztechnologien (z.B. Ethernet)
- Nutzung beliebiger Netzwerktechnologien
  - alle denkbaren Netze sollen an das Netz angeschlossen bzw. zum Zusammenschluß von Netzen genutzt werden können,
  - daher nur minimale Anforderungen an die Netze.
  - Der IP-Dienst übernimmt daher keine Garantie für Paketzustellung (Best Effort): unreliable network service

Exkurs über Protokollstrukturen

- Unterteilung der Kommunikation in Teilaufgaben, z.B.:
  - Physikalische Übertragungstechnik
  - Protokolle für lokale Übertragung über eine physikalische Verbindung
  - Protokolle zur Kommunikation in globalen Netzen
- Netzwerkarchitekturen
  - Abgestimmte Sätze von Teilprotokollen zur Realisierung eines Gesamtsystems
  - z.B.: TCP/IP, DECnet, Appletalk, SNA, OSI
- Grundprinzipien von Netzwerkarchitekturen
  - Schichtenstrukturierung
  - Encapsulation von Daten einer Schicht in „Rahmen“ (Frames) untergeordneter Schichten

Schichtenstrukturierung

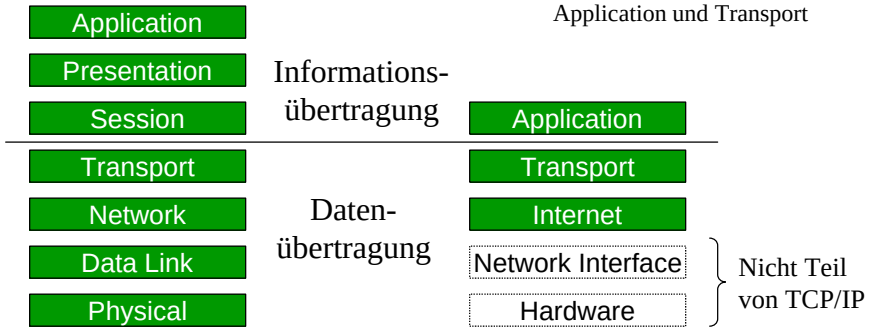
- Hierarchische Unterteilung in Schichten mit dedizierten Aufgaben
  - Austauschbarkeit
  - Alternativen für Teilschichten
  - Unabhängigkeit von Teilaufgaben
- Kommunikationsstruktur
  - Übergabe von Daten und Steuerinformationen zwischen benachbarten Schichten eines Knotens
  - (Virtuelle) Kommunikation zwischen gleichen Schichten verschiedener Knoten (Steuerinformation)



OSI- und TCP/IP-Schichtenstruktur

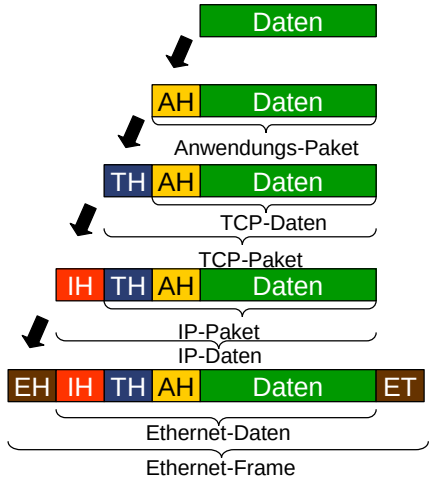
- OSI-Architektur
  - Open System Interconnection
  - ISO-Standard
  - OSI hat sich nicht durchgesetzt
- TCP/IP-Architektur

Ursprünglich keine weitere Unterteilung, in der Realität z.B. Remote Procedure Call als Schicht zwischen Application und Transport



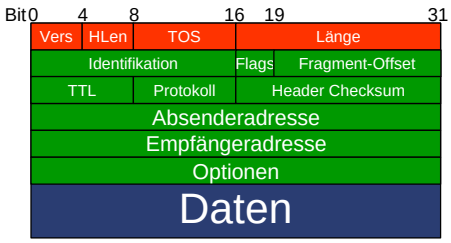
Encapsulation von Protokollen

- Beim Übergang von einer höheren Schicht zu einer darunterliegenden Schicht werden die Daten der höheren Schicht in einen Rahmen verpackt
  - meist wird ein Header vorangestellt
  - teilweise auch ein Trailer (z.B. CRC-Feld)
- Zusätzliche Netzbelastung zu den eigentlichen Daten (Protocol Overhead)



Ende des Exkurses

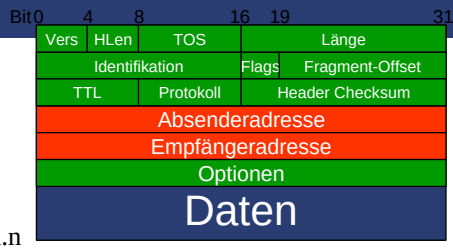
Internet-Packetformat



- Header-Länge:
  - Vielfaches von 4 Byte (mindestens 20 Byte)
- IP-Sprachgebrauch:
  - Oktett statt Byte

- Erläuterung der Felder
  - Vers: Versionsnummer (z.Z. 4)
  - HLen: Länge des Headers in 32-Bit-Worten
  - TOS: Type of Service: Prioritäten und Angabe, ob geringe Verzögerung, hoher Durchsatz oder hohe Zuverlässigkeit verlangt werden (meist unbenutzt)
  - Länge: Gesamtlänge in Byte (maximal 65.535)

IP-Adressen

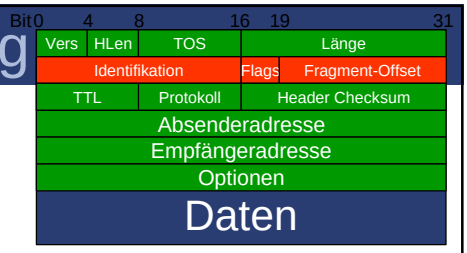


- Adressstruktur
  - 32-bit-Adressen
  - Dotted Decimal Notation:
    - Schreibweise als Quadrupel n.n.n.n
    - Jede Ziffer jeweils 8 Bit, also zwischen 0 und 255
- Unterteilung in Adresse in Netz- und Rechnerteil
  - Zuordnung von Adressbereichen zu physikalischen Netzen,
  - Adressen sind ortsabhängig,
  - Jedes Interface eines Netzknotens benötigt eine eigene Adresse,
  - so dass Rechner verschiedene Adressen haben
  - und der Weg eines Pakets zu einem Rechner von der Empfängeradresse abhängt.

Adressklassen

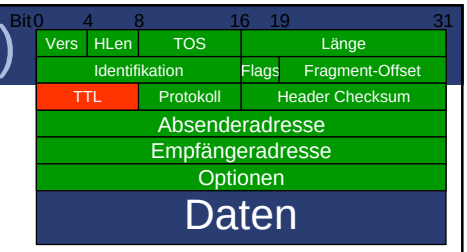
- Unterteilung der Adressen in Netz- und Rechnerteil (Net und Host)
- Class A Netze
  - Bit 1 = 0
  - Adressen 0.0.0.1 bis 127.255.255.254
  - 7 Bit Netzadresse, 24 Bit Hostadresse
  - 127 Netze
  - 2^{24} -2 = 16.777.214 Rechner pro Netz
- Class C Netze
  - Bit 1-3 = 110
  - Adressen 192.0.0.1 bis 223.255.255.254
  - 21 Bit Netzadresse, 8 Bit Rechneradresse
  - 2^{21} = 2.097.152 Netze
  - 2^{8}-2 = 254 Rechner pro Netz
- Class B Netze
  - Bit 1-2 = 10
  - Adressen 128.0.01 bis 191.255.255.254
  - 14 Bit Netzadresse, 16 Bit Rechneradresse
  - 2^{14} = 16.384 Netze
  - 2^{16} - 2 = 65.534 Rechner pro Netz
- Class D
  - Bit 1-4 = 1110
  - Adressen 224.0.0.0 bis 239.255.255.255
  - IP-Multicasts
- Class E
  - Bit 1-4 = 1111
  - Adressen 240.0.0.0 aufwärts
  - reserviert

Fragmentierung



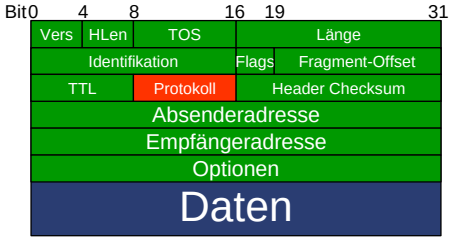
- Maximale Framegröße eines Netz
  - abhängig von Netztechnologien
  - ursprüngliche Größe kann für ein Transitnetz zu groß sein
  - IP-Router können Pakete fragmentieren
  - Mehrfache Fragmentierung möglich
  - Zusammenbau erst durch Empfänger
    - Empfänger startet bei Empfang des ersten Fragments eines Pakets einen Timer
    - Alle Fragmente werden verworfen, wenn ein Fragment nicht rechtzeitig ankommt
- Header-Felder
  - Identifikation: Eindeutige Nummer zwecks Zuordnung der Fragmente zu einem Paket
  - Fragment-Offset: Position des ersten Oktets im aktuellen Fragment im unfragmentierten Paket
  - Flags: Steuerung der Fragmentierung
    - 1. Bit unbenutzt
    - 2. Bit: don‘t fragment:
      - =1: das Paket darf nicht fragmentiert werden
    - 3. Bit: more fragments:
      - =1: weitere Fragmente folgen
      - =0: nicht fragmentiert oder letztes Fragment

Schleifen (TTL)



- Maßnahme gegen Schleifen
  - bei Fehlkonfigurationen möglich,
  - TTL-Feld (Time to live) verhindert Schleifen,
  - jeder Router dekrementiert TTL-Feld (meist um 1),
  - wird das Pakete mit TTL=0 werden verworfen,
  - der verwerfende Router sendet Fehlermeldung an den Absender
- Zusätzliche Anwendung
  - Ermitteln der Router auf einem Weg durch das Netz,
  - durch Test-Pakete mit TTLs 1,2,3,...
  - und warten auf Fehlermeldungen
  - Programm „traceroute“ (UNIX) bzw. „tracert.exe“ (Windows)

Multiplexing / Demultiplexing



- Übertragung verschiedener Protokolle über eine untergeordnete Protokollschicht
  - hier mehrere Transport-Protokolle über IP-Schicht

- Gängige Protokolle
  - ICMP (1)
    - Internet Control Message Protocol
    - Fehlermeldungen u.ä.
  - TCP (6)
    - Transmission Control Protocol
    - verbindungsorientierte Transport-Protokoll
  - UDP (17)
    - User Datagram Protocol
    - verbindungsloses Transport-Protokoll

Subnetze

- Problem: Netzwerk-Klassen A, B und C zu unflexibel
  - Option zur Aufteilung eines Netzes in Subnetze
  - die durch Router verbunden werden.
  - Unterteilung der Adressen in drei Teile: Netz, Subnetz, Host
  - (ähnlich Nebenstellenanlage beim Telefon)
- Beschreibung der Aufteilung durch „Subnetzmaske“
  - 32 Bit-Wert zu jeder Adresse
    - 1-Bit in Maske: Entsprechendes Adressbit beschreibt Netz oder Subnetz
    - 0-Bit in Maske: Entsprechendes Adressbit beschreibt Host
    - Fortlaufende Einsen am Anfang und Nullen am Ende der Maske
  - Anwendung:
    - Logische Und-Verknüpfung zwischen Adresse und Maske liefert Netz+Subnetz
    - Beispiel:
      - `134.76.11.125, binär:`
        `10000110.01001100.00001011.01111101`
      - `255.255.254.0, binär:`
        `11111111.11111111.11111110.00000000`
      - `Und-Operation, binär:`
        `10000110.01001100.00001010.00000000 = 134.76.10.0`
        `(Netz 134.76, Subnetz 10)`

Multinetting

- Einheitliche Subnetzmasken für ein Netz
  - von manche Routingprotokollen verlangt,
  - Problem bei unterschiedlich großen physikalischen Subnetzen
- Lösung Multinetting
  - Betrieb mehrerer logischer Subnetze auf einem physikalischen Netz,
  - durch Vergabe mehrerer Adressen für eine Schnittstelle
- im GÖNET häufig benutzt

Spezielle Adressen

- Spezielle Adressen
  - Alle Bits im Hostteil = 0:
    - das Netz, das im Netzteil angegeben ist
    - im Routing Table verwendet,
    - z.B. 134.76.0.0
  - Alle Bits im Hostteil = 1:
    - an alle Rechner in dem Netz, das durch den Netzteil angegeben ist
    - „Directed Broadcast“
    - z.B. 134.76.10.255, an alle Rechner im Netz 134.76.10.0
  - Alle Bits im Netzteil = 0:
    - Rechner mit der Adresse im Hostteil in diesem Netz
  - Alle Bits der gesamten Adresse = 1:
    - Broadcast an alle Rechner im lokalen Netz (255.255.255.255)
  - Alle Bits der gesamten Adresse = 0:
    - Default Netz/Route im Routing Table

ARP

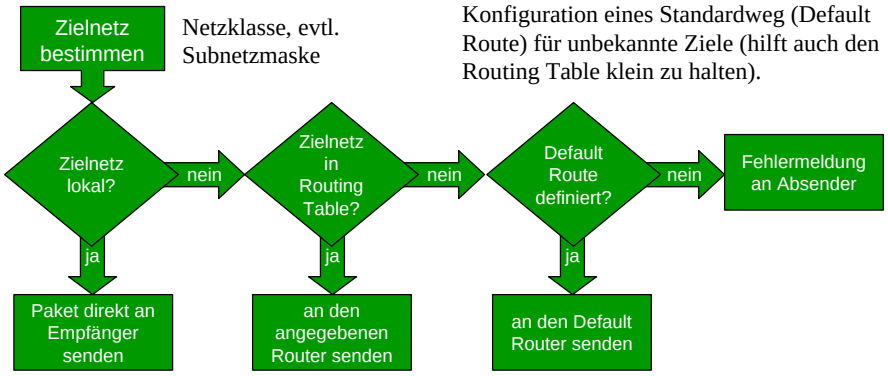
- Adress Resolution Protocol
- Finden der MAC-Adresse zu einer IP-Adresse
- Vorgehen:
  - Broadcast senden mit Inhalt
    - eigener IP-Adresse
    - eigener MAC-Adresse
    - Ziel-IP-Adresse
    - Dummy-MAC-Adresse
  - Antwort vom Zielrechner (oder einem Proxy-ARP-Server)mit Inhalt
    - eigener IP-Adresse
    - eigener MAC-Adresse
    - Quellen-IP-Adresse
    - Quellen-MAC-Adresse
- Speicherung einmal ermittelter Umsetzungen (ARP-Cache, mit Alterungsfunktion)
- RARP (Reverse ARP) für Auflösung von MAC-Adresse zu IP-Adresse (nicht sehr häufig benutzt)

ICMP

- Internet Control Message Protocol
- Funktionen
  - Tests der Netzfunktionalität
    - Echo Request
    - Echo Reply
    - Bei Anwendung „ping" verwendet.
  - Fehlermeldungen
    - Destination unreachable (vom Router)
    - Source quench (vom Router bei Überlastung)
    - Redirect (vom Router: anderen Router benutzen)
    - Time exceed (TTL war 0)
    - Parameter Problem (Formatfehler im Header)
  - Informationsdienste
    - Information request/reply (IP-Adresse für sich selbst anfordern)
    - Adress mask request/reply (Subnetzmaske erfragen)
    - Timestamp request/reply (Zeitmarkierung)

IP-Routingprozeß

- Entscheidungsablauf auf einem Rechner oder Router



Multinetting und Subnetzmasken

- Was ist lokal in einer Multinetting-Umgebung?
  - abhängig von Subnetzmaske
    - kleine Subnetzmaske (nur ein Subnetz) bedeutet: alle Pakete in andere logische Subnetze des gleichen physikalischen Subnetzes werden über den Router übertragen!
    - große Subnetzmaske (mehrere Subnetze umfassend):
      - Probleme bei mehreren Schnittstellen mit unterschiedlicher Subnetzgröße (oft vom Betriebssystem nicht erlaubt)
      - bei nicht zusammenhängenden Adressbereichen, können Rechner als lokal angesehen werden, die nur über einen Router erreicht werden können.
- Situation im GÖNET
  - Empfehlung: im Subnetzmaske für Class B benutzen
  - Ausnahme: Rechner mit mehreren Schnittstellen
  - GÖNET-Router fangen nicht lokale Pakete über Proxy-ARP ab
  - Broadcast-Adresse: 255.255.255.255 (oder 134.76.255.255)

Endgerätekonfiguration

- Routing-Einstellung
  - Unterscheidung nach
    - Anzahl der Schnittstellen
    - Anzahl der Router pro Netz
  - Geräte mit nur einer Schnittstelle und einem Router im Netz:
    - Statische Route zu einem Default-Router definieren
  - Andere Geräte
    - Übernahme von Informationen, die von Routern im Netz verteilt werden (über Protokoll RIP)
    - durch einen Routing-Prozeß im lokalen Rechner (UNIX: routed oder gated)

Metriken

- Bei Existenz alternativer Wege muß der „günstigste“ Weg ausgewählt werden.
- Routing-Metrik zur Bewertung von Wegen
  - Festgelegt für jede Router-Schnittstelle
- Mögliche Kriterien zur Bestimmung einer Metrik
  - 1. Anzahl von Vermittlungsstellen auf dem Weg (Hops),
  - 2. Übertragungskapazität auf dem Weg (Cost, Ticks)
  - 3. Verzögerungszeit auf dem Weg (lastabhängig!)
  - 4. Durchsatz (lastabhängig!)
  - 5. Kosten (bei gemieteten Leitungen)
  - Die Kriterien 3 und 4 sind zustandsabhängig (nützlich, aber schwer zu ermitteln)
  - Die Kriterien 1, 2 und 5 sind zustandsunabhängig
- Routing Table enthält mindestens:
  - Zielnetz, Metrik, nächster Router (oder lokal)

Routing

- Festlegung der Wege durch Aufbau des Routing Table
  - Methoden
    - Manuelle Konfiguration fester Routen (statisches Routing)
      - Insbesondere bei Endgeräten ohne Alternativen in der Wegewahl
    - Automatische Konfiguration durch Kommunikation zwischen Routern (dynamisches oder adaptives Routing)
    - Mischung von dynamischen und statischen Routen
  - Strukturen
    - Zentralisiertes Routing
      - Ein „Ober-Router“ bestimmt/errechnet zentral die Tabellen und verteilt sie.
    - Verteiltes Routing
      - Jeder Router entscheidet aufgrund einer selbst erstellten Tabelle.
      - Jeder Router kommuniziert mit jedem
      - Problem: relativ hohe Netzlast
    - Ganz anders: Hierarchisches Routing

Adaptives Routing

- Kommunikation zwischen Routern
  - jeder sendet die eigenen Information an alle
  - jeder sendet nur an ausgewählte Router (die dann die anderen informieren)
- Zeitverhalten des Informationsaustauschs
  - Periodisch, meist alle 10s bis 60s
  - Bedarfsorientiert
    - Routing-Information wird nur im Bedarfsfall ausgetauscht.
    - Zur Kontrolle werden periodisch kurze Hello-Pakete ausgetauscht.
- Inhalt des Informationsaustauschs
  - Quantität
    - Kompletter Routing-Table oder
    - nur Informationen über eigenen (sichere) Informationen
  - Qualität
    - Minimum: Netzwerkadressen und zugehörige Metrik
    - zusätzliche Informationen (z.B. Subnetzmasken bei IP)

Distance Vector Routing

- Verfahren
  - jeder Router sendet an alle direkten Nachbarn
  - seinen vollständigen Routing Table
  - mit eigenen (sicheren) Informationen
  - und von anderen gelernten Informationen
  - bezüglich Metrik (Distance) und Richtung (Vector)
- Vorteile
  - Übertragungen nur in direkt angeschlossene Netze
  - einfache Berechnung des neuen Routing Table (ersetzen eines alten Eintrags bei kleinere Metrik einer neuen Mitteilung)
- Nachteil
  - schlechte Konvergenz bei redundanten Wegen durch Weitergabe von gelernten (evtl. nicht mehr aktuellen) Informationen

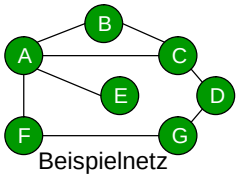
Link State Routing

- Verfahren
  - Jeder Router sendet an alle anderen Router (oder eine Zentralstelle)
  - Informationen über seine eigenen Schnittstellen (Link State)
  - also nur sichere Informationen.
  - Aus diesen Informationen berechnet jeder Router seinen Tabelle vollständig und eigenständig
- Vorteile
  - schnellere Konvergenz
- Nachteile
  - größerer Rechenaufwand zur Berechnung der Routing Table („Shortest Path“-Algorithmen aus der Graphentheorie)
  - Speicherung größerer Datenmengen in jedem Router

Routing Information Protocol (RIP)

- Distance-Vector-Verfahren
- Details
  - der vollständigen Routing-Tabellen
  - aus Netz- oder Subnetznummern und Metriken
  - Metrik meist Hopcount
    - Metrik maximal 15 (konfigurierbar, aber besser nicht ändern)
    - Metrik = 16 bedeutet unreachable/Netz nicht erreichbar
  - Paketformat
    - 14 Byte (!) lange Netznummer
    - 4 Byte Metrik
    - auch bei IPX-Protokoll fast identisch genutzt
  - Update-Intervall alle 30s oder bei Änderungen sofort.
  - Erfordert einheitlichen Subnetzmaske im gesamten Netz, da die Maske nicht übertragen wird.
- Unter UNIX von „routed“ und „gated“ benutzt.

Routing-Table-Aufbau (RIP)



Beispielnetz

Jeder lernt vom den Nachbarn

Erste Iteration

Von Knoten	Abstand zu Knoten						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	¥
C	1	1	0	1	2	2	2
D	2	2	1	0	¥	2	1
E	1	2	2	¥	0	2	¥
F	1	2	2	2	2	0	1
G	2	¥	2	1	¥	1	0

Startpunkt

Von Knoten	Abstand zu Knoten						
	A	B	C	D	E	F	G
A	0	1	1	¥	1	1	¥
B	1	0	1	¥	¥	¥	¥
C	1	1	0	1	¥	¥	¥
D	¥	¥	1	0	¥	¥	1
E	1	¥	¥	¥	0	¥	¥
F	1	¥	¥	¥	¥	0	1
G	¥	¥	¥	1	¥	1	0

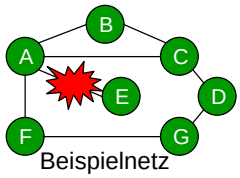
Jeder kennt seine direkten Nachbarn

Endpunkt

Von Knoten	Abstand zu Knoten						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Konvergenz von RIP

- Schlechte Konvergenz bei Ausfall einer Verbindung



Beispielnetz

Information (Metrik) zu E bei A und B

Zeitpunkt	bei A	bei B
0	1	2
1	3	2
2	3	4
3	5	4
4	5	6
..	..	..
13	15	14
14	15	15

Update von B nach A

Update von A nach B

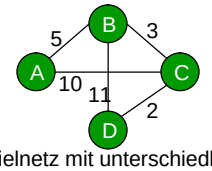
Vereinfachte Darstellung:
Das Problem tritt zwischen A und B nicht auf, da B weiss, das E über A erreichbar ist (Probleme erst bei größeren Abständen)

Open Shortest Path First (OSPF)

- Link-State-Verfahren
- Routing-Updates werden nur an zwei Router gesendet
  - Designated Router und Backup Designated Router,
  - die in der Initialisierungsphase bestimmt werden müssen,
  - Designated Router gibt den anderen Zusammenfassungen,
  - Metrik meist auf Basis der Übertragungskapazität der Netze,
  - Routing-Updates nur bei Änderungen,
  - Hello-Pakete alle 10s.
- Inhalt der Routing-Updates
  - Netznummern, Metrik und Subnetzmaske,
  - daher auch Unterstützung von variablen Subnetzmasken.
- Optionaler Password-Schutz
  - Klartext-Community bei Übertragung von Hello- und Routing-Update-Paketen zur Authentifikation.

Routing-Table-Aufbau (OSPF)

- Routenberechnung eines Knotens



Beispielnetz mit unterschiedlichen Interface-Metriken

Knoten D lernt Link States:
von A: (B,5), (C,10)
von B: (A,5), (C,3), (D,11)
von C: (A,10), (B,3), (D,2)
von D: (B,11), (C,2)

Open Shortest Path First:
immer den kürzesten, offenen (bekannten) Weg zu erst hinzufügen

Start: eigene Information
(D,0,-) (D mit Metrik 0 direkt)

Eigene Nachbarn: B und C ergeben als kürzeste Wege:
(B,11,B) und (C,2,C)

Davon wird der beste übernommen:
(D,0,-)
(C,2,C)

Mit den Nachbarn von C ergeben sich als kürzeste Wege:
(B,5,C) und (A,12,C)

Davon wird der beste übernommen:
(D,0,-)
(C,2,C)
(B,5,C)

Mit den Nachbarn von B ergeben sich als kürzeste Wege:
(A,10,C) (über C und B nach A!)

Davon wird der beste übernommen:
(D,0,-)
(C,2,C)
(B,5,C)
(A,10,C)

Fertig

Teil VII: Ende-zu-Ende-Kommunikation

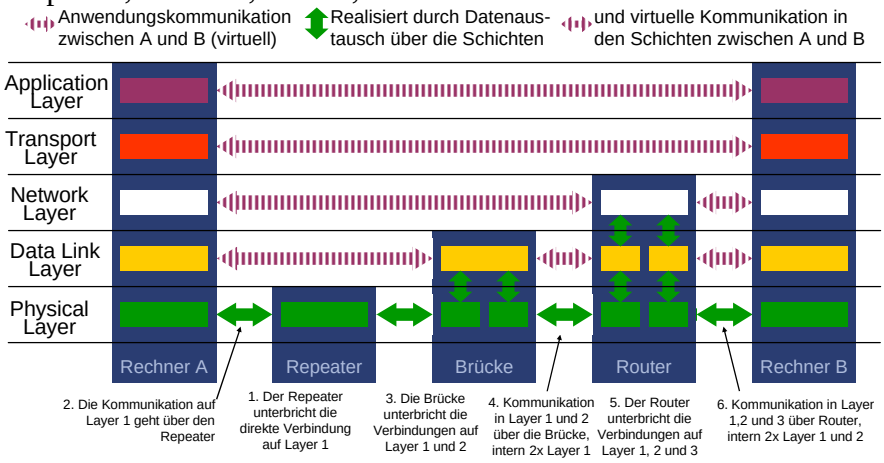
GWDG

Überblick

- Ende-zu-Ende-Kommunikation
  - Bisher betrachtet
    - Übertragung von Bits über Kabel
    - Übertragung von Frames zwischen lokalen Netzknoten
    - Übertragung von Paketen zwischen Rechnern in globalen Netzen
  - Sinn der Kommunikation ist aber
    - Austausch von Nachrichten zwischen Anwendungsprogrammen oder Prozessen auf den (End-) Rechnern
  - Aufgabenteilung
    - Inhalte der Nachrichten werden von Anwendungen und Anwendungsprotokollen verarbeitet
    - Vermittlung Nachrichten zwischen den Anwendungsprozessen über die Transportprotokolle

Internetworking und Schichten

- Repeater, Brücken, Router, Endstationen im Schichtmodell



Aufgaben der Transportprotokolle

- Multiplexing und Demultiplexing
  - Kennzeichnung abgehender Pakete zwecks Zuordnung zu Anwendungen/Prozessen (funktional)
  - Interpretation der Multiplex-Schlüssel bei eingehenden Paketen und Weitervermittlung zu den Anwendungen
- Segmentierung und Reassemblierung der Nachrichten
  - Aufteilung der Anwendungsdaten in netzwerkangepasste Portionen beim Senden
  - Zusammenfügen der Segmente beim Empfangen
  - Reihenfolgegarantie der Segmente

Transportprotokolle im Internet

- Zusätzliche Aufgaben
  - Virtuelle Verbindungen und Verlustsicherung
  - Flußkontrolle
  - Vermeidung gegen Überlastung/Netzverstopfung (Congestion Avoidance)
  - Solche Aufgaben können (und werden bei anderen Protokollen) auch in anderen Schichten implementiert werden.
  - Transportprotokolle erledigen diese Aufgaben zwischen Endsystemen einer Kommunikation
- Internet-Transportprotokolle
  - User Datagram Protocol (UDP)
    - als Minimalimplementation zum Multiplexing/Demultiplexing
    - für einfache Anfrage/Antwort-Kommunikationen
    - oder im lokalen Netz (geringe Verlustwahrscheinlichkeit)
  - Transmission Control Protocol (TCP)
    - als vollfunktionales Transportprotokoll

Protokoll-Multiplexing und Ports

- Kommunikation zwischen Prozessen über Netz
  - Spezifikation der an der Kommunikation beteiligten Prozesse ist nötig
  - und muss hinreichend abstrakt sein,
  - um nicht von Betriebssysteminterna abhängig zu sein.
- Spezifikation der Prozesse durch (Protokoll-) Ports
  - Bezeichnung durch Portnummern
  - Festdefinierte Nummern für Dienste auf Rechnern (z.B. Mail = 25)
    - Festdefiniert, um Server-Prozesse auffinden zu können.
  - Dynamisch gewählte Nummern für Clienten,
    - da diese die Kommunikation initieren und die Portnummer dem Server für Antworten mitteilen können.
  - Zuordnung der Portnummern zu tatsächlichen Prozessen über Mechanismen der Betriebssysteme

User Datagram Protocol (UDP)

- Eigenschaften
  - Multiplexing/Demultiplexing zwischen Prozessen
  - für einfache Abfrage/Antwort-Kommunikation,
    - z.B. Nameserver-Abfrage (ein Paket für die Frage, eins für die Antwort),
  - oder für schnelle lokale Kommunikationen
    - mit geringer Wahrscheinlichkeit von Datenverlusten (z.B. NFS für Fileserver), Segmentierung durch Anwendung,
    - daher ohne Segmentierung,
  - ohne Verlustsicherung,
  - bei verbindungloser Kommunikation.
- Paketformat
  - Portnummern der sendenden und empfangenen Prozesse
  - Länge von UDP-Header und Daten
  - Prüfsumme
  - jeweils 16 Bit lange Werte

Transmission Control Protocol (TCP)

- Reliable Stream Transport Service
  - Transport zwischen Prozessen (Multiplexing/Demultiplexing)
  - mit Segmentierung eines Datenstroms (Stream),
  - Einhaltung der Datenreihenfolge
  - und Verlustsicherung (reliable)
  - wozu eine definierte Verbindung zwischen Prozessen nötig ist,
  - sowie mit Vollduplex-Übertragung.
- Zusätzliche Algorithmen zur
  - Flußkontrolle (flow control)
    - zum Schutz vor Überlastung des Empfängers
  - Congestion Control
    - zur Vermeidung (oder wenigstens Minderung) von Überlastungen (Verstopfungen) des Netzes

Anwendungsschnittstelle

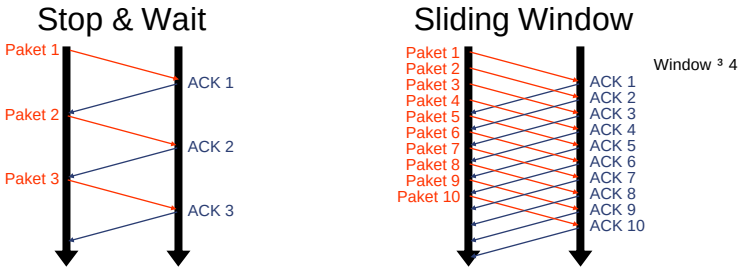
- Daten als Byte-Stream
  - Anwendungen übergeben eine (unstrukturierte) Folge von Bytes an TCP.
  - TCP überträgt Segmente von Bytes über das Netz.
  - Dabei sammelt TCP die Bytes in einem Sendepuffer
  - und sendet, wenn
    - die (konfigurierbare) maximale Größe eines Segments erreicht wird (MSS, Maximum Segment Size)
    - oder nach Ablauf eines Timers
    - oder auf Anforderung einer Anwendung (Push-Operation, z.B. für Dialogeingabe nötig).
  - Die empfangende Anwendung liest Daten aus dem Eingangspuffer des empfangenden TCP-Teils

Verlustsicherung

- Basis von Verlustsicherung
  - Rückmeldung des Empfängers über eingegangene Daten,
  - bei eindeutiger Kennzeichnung der Pakete,
  - zur Zuordnung der Rückmeldungen zu den gesendeten Paketen,
  - Zeitüberwachung: Retransmission nach Ablauf einer Wartezeit (Timeout).
- Einfache Lösung
  - Senden eines Pakets
  - und warten auf Bestätigung (Acknowledge, ACK) des Empfangs durch den Zielrechner.
  - Nachteil:
    - Starke Abhängigkeit des Durchsatzes von der Netzwerklatenz,
    - insbesondere in einem Internet mit vielen latenzerzeugenden Brücken und Routern.
  - „stop and wait“

Sliding Window

- Algorithmus zur effizienten Verlustsicherung
  - Übertragung mehrerer Pakete vor Warten auf Bestätigung,
  - Menge der unbestätigten Daten (Fenster) dynamisch vom Empfänger bestimmt,
  - dient gleichzeitig als Flußkontrolle,
  - ständig gefüllter Übertragungskanal möglich.



Sequenznummern

- Verlustsicherung durch Nummerierung
  - bei TCP (byte-orientiert) durch Nummerierung der Bytes
  - 32 Bit große Sequenznummern
  - Zählung beginnt bei einem Zufallswert (nicht 1)
- Empfangsbestätigung
  - durch Angabe der Nummers des ***nächsten*** erwarteten Bytes (Acknowledgement Number)
  - im Vollduplexbetrieb
    - jedes Segment enthält eine Sequenz- und eine Acknowlegment-Nummer
    - ein Acknowledgement-Bit in den „Code Bits“ des TCP-Headers besagt, dass die Acknowledgement-Nummer gültig ist.

Zeitüberwachung

- Wie groß muß der Timeout-Wert sein?
  - RTT-Werte sind im Internet entfernungsabhängig
  - und durch Lastwechsel zusätzlich auch für Einzelverbindungen kurzfristig variabel
- Lösung: Adaptive Retransmission
  - Sender misst RTT-Werte bereits bestätigter Segmente
  - und schätzt daraus zukünftige RTTs
  - ohne Berücksichtigung von RTTs bei Retransmissionen.
  - Ursprünglicher Algorithmus

    EstimatedRTT = α ´ EstimatedRTT (alt) + β ´ SampleRTT

    (mit $\alpha+\beta=1$, α = 0,8 bis 0,9)

    TimeOut = 2 ´ EstimatedRTT oder

    TimeOut = 2 ´ LastTimeOut (nach Retransmission)
  - Neuerer Algorithmus:
    - Berücksichtigung der Variation der RTTs

      TimeOut = EstimatedRTT + 4 ´ Deviation
  - (Wer implementiert was?)

Sliding Window und Retransmission

- Besonderer Effekt:
  - Nachdem mehrere Segmente übertragen wurden, muss eines der ersten wiederholt werden (entsprechendes ACK)
  - Werden sofort alle Segmente wiederholt?
    - Im Standard nicht festgelegt.
    - Alle wiederholen kann unnötige Netzlast bedeuten,
    - nur das offensichtlich fehlende wiederholen, ergibt „stop and wait“ und kann weitere Timeouts bedeuten (und damit stark sinkenden Durchsatz)
    - Vermutlich wird meist die zweite Variante benutzt.

Fast Retransmit

- TCP bestätigt jedes eingehende Paket
  - bei Verlust von Paketen wird das letzte in Reihenfolge angekommene Paket mehrmals bestätigt
  - neuere Implementationen reagieren auf doppelte ACKs
    - Vermutung des Datenverlustes (nicht nur falsche Reihenfolge)
    - Retransmission vor Ablauf des Timeouts
    - meist erst bei dreifachen ACKs

Flow Control

- Flußsteuerung über Windows-Size
  - der jeweilige Empfänger bestimmt die Größe des SlidingWindow
  - (die Window-Size kann in der Vollduplex-Verbindung assymetrisch sein).
  - Die Fenstergröße wird in jedem Segment-Header angegeben
  - und kann daher im Laufe der Übertragung variieren.
  - Setzen der Fenstergröße
    - nach Größe des Empfangspuffers
    - und Möglichkeit zur Anpassung an sich ändernde Bedürfnisse des Empfängers

Congestion Control

- Congestion:
  - Datenverluste durch Überlastung
  - führen zu Retransmissionen
  - und damit zu noch mehr Netzlast:
  - Congestion Collapse (zu manchen Zeiten in den USA-Verbindungen zu beobachten)
- Reaktion auf Datenverluste und Retransmissionen
  - durch Reduktion der Übertragungsrate im virtuellen Kanal
- Algorithmus
  - Zwei Fenstergrößen beim Sender:
    - vom Empfänger vorgegebenes Fenster
    - Congestion Window
  - Minimum von beiden wird benutzt
  - Congestion Window wird abhängig von Datenverlusten gesetzt

Congestion Window

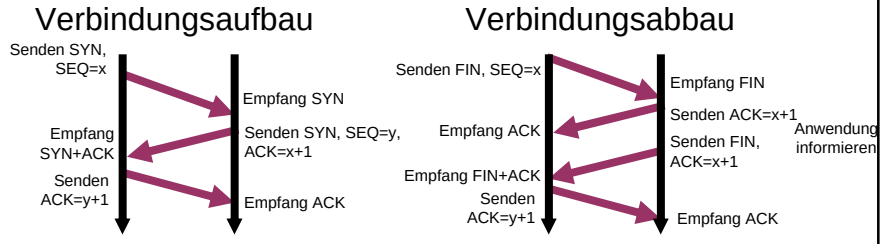
- Festlegung der Größe des Congestion Window
  - Slow Start / Additive Increase
    - Congestion Window mit der Größe eines Segment starten,
    - nach jeder verlustfreien Übertragen um ein Segment vergrößern.
  - Multiplicative Decrease
    - Bei Datenverlust Congestion Window halbieren
    - (mit einem Segment als Minimum)

Out of Band Data

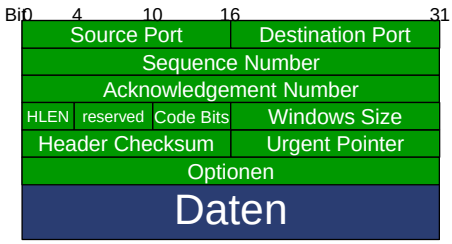
- Übermittlung dringender Daten
  - Behandlung außerhalb der Reihenfolge,
  - Sofortige Übermittlung beim Empfänger an die Anwendung,
  - (keine Priorisierung auf der Netzschicht)
- Nutzung durch Anwendungen
  - z.B. Unterbrechungen, Bildschirm anhalten bei Telnet u.ä.
- Kennzeichnung durch „Urgent Pointer“
  - Zeiger im Header
  - verweist auf den Beginn der normalen Daten
  - und das Setzen des Urgent-Bit (URG) in den „Code Bits“ des TCP-Header

Virtuelle Verbindungen

- Zweck
  - Verlustsicherung, Reihenfolgegarantie und Flußkontrolle ermöglichen
- Kennzeichnung einer Verbindung
  - durch IP-Adressen und Ports der Sender und Empfänger
  - Bezeichnung für ein Paar (IP-Adresse, Port): Socket
  - (der Port eines Services kann daher für alle Verbindungen gleich sein)
- Aufbau und Abbau der Verbindung
  - Durch speziell gekennzeichnete Segmente (Code Bits im Header)
  - SYN (Synchronize) beim Aufbau
  - FIN (Finish) beim normalen oder RST (Reset) beim „Not-“Abbau



TCP-Segmentformat



- Source- und Destination-Port
  - Multiplex-Keys
- Sequence Number
  - Nummer des ersten Byte
- Acknowledgement Number
  - Nummer des nächsten erwarteten Byte
- HLEN
  - Header-Länge in 32bit-Vielfachen
- reserved
  - reserviert aber unbenutzt
- Code Bits
  - URG (Urgent)
  - ACK (Acknowlegement)
  - PSH (Push)
  - RST (Reset, Abort Connection)
  - SYN (Start,Synchronize Sequence Numbers)
  - FIN (Finish, End of Data Stream)
- Window Size
  - Anzahl Bytes, die ohne Bestätigung gesendet werden dürfen.
- Header Checksum
  - Prüfsumme über den Header
- Urgent Pointer
  - Zeiger auf erstes Byte der normalen Daten im Segment
- Optionen
  - optionale Informationen, z.B. MSS

Lokale oder Ende-Ende-Kontrolle

- Verlustsicherung
  - Verlustsicherung kann auch auf anderen Schichten erfolgen
  - insbesondere im Data Link Layer
  - Standard für DLL: Logical Link Control LLC (IEEE 802.2)
  - Verlustsicherung auf allen Teilstrecken garantiert nicht Ende-zu-Ende-

Teil VIII: Anwendungsprotokolle, Adressen und Namen

GWDG

Netzwerkanwendungen

- Klassisches Dreigestirn
  - Dialogzugang / Remote Login
  - Dateitransfer
  - Electronic Mail
- Standard-Anwendungen
  - World Wide Web
  - Diskussionsforen
  - Netzwerkbetriebssysteme
- Schon Standard?
  - Video on demand
  - Videokonferenz
  - Internet-Telefonie / Voice over IP
  - Multi Media

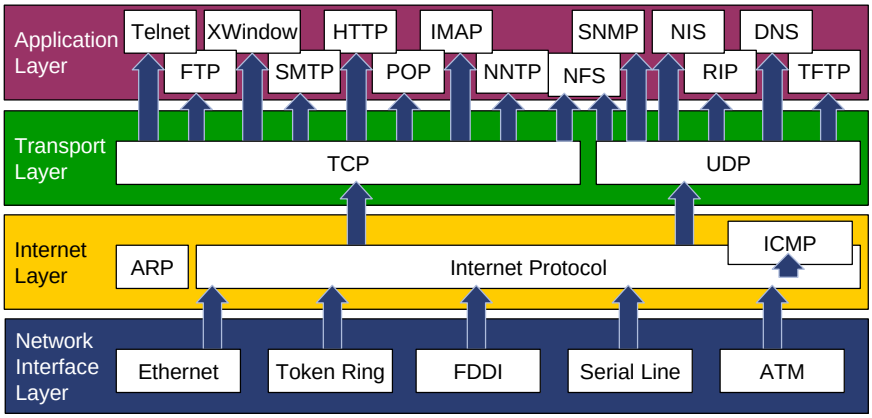
Anwendungen und Anwendungsschicht

- Netzwerkanwendungen
  - stellen Benutzern Dienste zur Verfügung,
  - insbesondere eine Benutzeroberfläche.
- Anwendungsprotokolle
  - realisieren Netzwerkanwendungen
  - durch Kommunikation zwischen Clienten- und Server-Prozessen
  - in einer formalisierten Sprache.
- Standards
  - gelten für die Anwendungsprotokolle,
  - in der Regel nicht für die Benutzerschnittstelle,
  - die daher für ein Protokoll unterschiedlich implementiert werden kann
  - (z.B. graphische Oberflächen statt kommandozeilengesteuerten Anwendungen für Mail oder Filetransfer).

Internet-Anwendungsprotokolle

- Anwendungsprotokolle im Internet (Auswahl)
  - Telnet (Dialogzugang)
  - SSH (Dialogzugang mit verschlüsselter Übertragung)
  - XWindow (Graphische Oberfläche)
  - FTP (File Transfer Protocol)
  - TFTP (Trivial File Transfer Protocol)
  - NFS (Network File System)
  - NIS (Network Information Service)
  - DNS (Domain Name System)
  - SMTP (Simple Mail Transfer Protocol)
  - POP (Post Office Protocol)
  - IMAP (Internet Message Access Protocol)
  - HTTP (Hypertext Transfer Protocol)
  - NNTP (NetNews Transfer Protocol)
  - SNMP (Simple Network Management Protocol)

Internet-Protokolle



(Auswahl von Protokollen verschiedener Schichten)

Electronic Mail

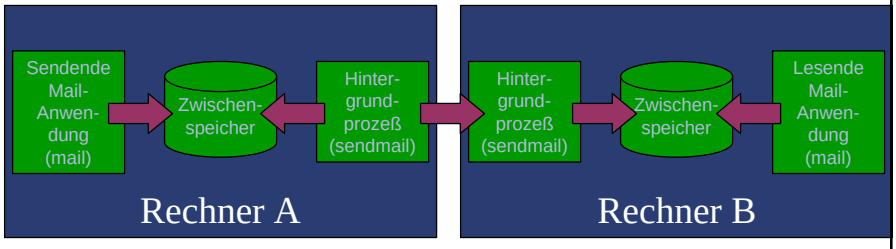
- Zweck
  - ursprünglich: Übertragung „kurzer“ Nachrichten in Textform
  - Dateiübertragung über E-Mail
  - Voice-Mail
- Mail-Adressen
  - Zweiteilung
    - Postfachname (Adressat, z.B. Holger.Beck)
    - und Mail-Server-Name (z.B. gwdg.de)
    - getrennt durch „@“.
  - Beispiel: Holger.Beck@gwdg.de
  - Zeichenumfang
    - „a-z“, „A-Z“, „0-9“, „.“, „-“, evtl. „_“ (im Adressaten),
    - insbesondere keine Umlaute oder „ß“,
    - keine Unterscheidung zwischen Groß- und Kleinschreibung

Mail-Inhalte

- Amerikanische Erfindung
  - Zeichensatz 7-Bit ASCII,
  - keine Umlaute, „ß“, usw.,
  - keine deutschen (oder gar kyrillische) Texte,
  - keine Übertragung binärer Inhalte (Dateien)
- Umgehung des 7-Bit-Zeichensatzes
  - Kodierung der Sonderzeichen oder binär Informationen
  - Abbildung auf 7-Bit-Zeichensatz
  - Varianten zur Kodierung von Dateien als „Attachement“
    - uuencode / uudecode (uu = Unix to Unix)
    - BinHex (Übertragung der hexadezimal Kodes der Zeichen, typisch für Apple Macintosh)
    - MIME (Multimedia Internet Message, Internet-Standard)
  - MIME zur Kodierung von Sonderzeichen im Text
  - Umwandlung durch Mail-Programme

Struktur von E-Mail-Übertragungen

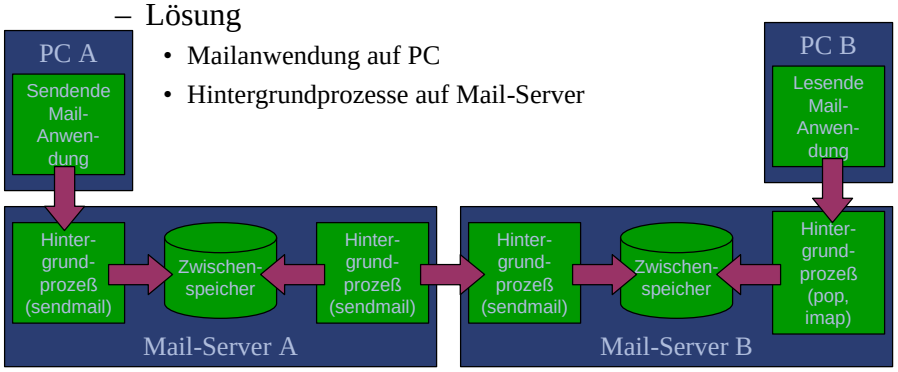
- Ursprüngliche Struktur
  - gedacht für Großrechner oder Multi-User-Systeme
  - also Rechner die im 24-Stunden-Einsatz sind:



Anwender schreibt eine Mail in einem Mail-Programm	Das Mail-Programm speichert die Mail lokal ab	Hintergrund-prozeß prüft regelmäßig den Spool-Bereich	Hintergrund-prozeß überträgt Mail über das Netz	Hintergrund-prozeß empfängt Mail	Hintergrund-prozeß speichert Mail im Postfach	Anwender liest Mail aus dem Postfach

Struktur für PCs

- PCs als Mail-Clienten
  - Probleme
    - PCs sind oft ausgeschaltet
    - PCs haben/hatten nicht genug Resourcen für Hintergrundprozesse
  - Lösung
    - Mailanwendung auf PC
    - Hintergrundprozesse auf Mail-Server

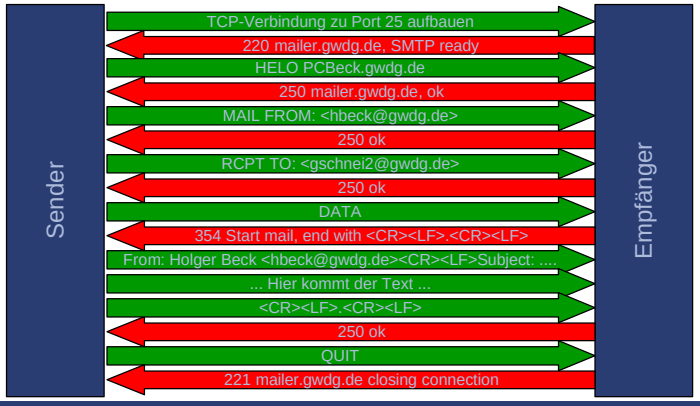


Mailprotokolle

- SMTP
  - Übertragung von Mail über das Internet
  - 7-Bit ASCII
  - ursprünglich ohne jegliche Authentifizierung (jetzt optional)
  - Einsatz
    - zum Senden allgemein (auch PCs)
    - Empfang auf Mail-Servern
- POP/POPS und IMAP/IMAP
  - Zugriff auf Postfächer über Netz (insbesondere PCs)
  - Authentifizierungsfunktion (PC-Programme authentifizieren meist vor dem Senden per SMTP über POP/IMAP)
  - Unterschiede
    - POP lädt Mail vom Server auf den Clienten
    - IMAP verwaltet Mail auf dem Server
  - Vor- und Nachteile
    - Konsistente Mail-Verwaltung bei Zugriff über verschiedene PCs mit IMAP gesichert
    - Offline-Lesen von Mail mit POP möglich

SMTP

- Protokollstruktur
  - Kodewörter für verschiedene Funktionen
  - Standardisierte Kodenummern mit (nicht standardisiertem) erläuternden Text als Antwort
- Ablauf



Sicherheit

- Datensicherheit
  - ohne Zusatzanwendungen werden Mails als Klartext übertragen
  - neuere Programme erlauben das Einbinden von Verschlüsselungstool wie PGP (Pretty Good Privacy) / GnuPP
- Authentifizierung
  - mit SMTP sind beliebige Absenderadressen vortäuschbar
  - die Header-Zeilen (auch From: und To:) sind Teil des Textes (nicht aus MAIL FROM: oder RCPT TO: übernommen)
  - Authentifizierung durch Angabe von Schlüsseln (PGP-Keys)
- Spam
  - Mail-Server-Betreiber sollten verhindern, dass Server von Werbe-Mailern missbraucht werden
    - Standard ist meist: alle eingehenden Mails werden bei Bedarf weitergeleitet
    - Nötig: Filtern (Ablehnen) von Mails mit nicht lokalen Empfängern **und** nicht lokalen Absendern
  - (Fast) jedes UNIX-System arbeitet automatisch als Mail-Server
    - ggf. sendmail nicht als Daemon starten
  - Klassifizierungssysteme (Spam Assasin) und Filterung durch Empfänger

Dateitransfer und File Sharing

- Unterschiedung
  - Dateitransfer: Kopieren von Dateien über Netz
  - File Sharing: Zugriff auf Dateien oder Teile davon über Netz
- Protokolle
  - Dateitransfer
    - FTP / SFTP
      - mit Authentifizierung
      - (optional) Fortsetzung nach Unterbrechung
      - über TCP
    - TFTP
      - ohne Authentifizierung
      - über UDP
      - für Dateiübertragung während Boot über Netz u.ä.
  - File Sharing
    - NFS
      - unter UNIX
      - Freigabe von Verzeichnissen an bestimmte Rechner
      - Authentifizierung durch UID des Clienten
    - SMB
      - MS-Windows (oder Nachbau auf anderen Systemen, SAMBA)
      - Freigabe von Verzeichnissen an bestimmte Benutzer
      - Authentifizierung bei Verbindungsaufbau

Namen und Adressen

- Verwendung von Namen und Adressen
  - IP verwendet Adresse zur Identifikation von Rechnern
  - Benutzer verwenden Rechnernamen
  - Umsetzung zwischen Namen und Adressen über spezielle Netzwerkprotokolle und -dienste
- Namen im Internet
  - hierarchische Struktur
    - Rechner.Unterorganisation. ... .Organisation.Domäne
    - maximal 255 Zeichen insgesamt
    - und 63 Zeichen pro Teil („Label“)
  - Top-Level-Domänen
    - ARPA Ursprüngliches ARPANET
    - EDU Educatianal Institutions
    - COM Commercial Organizations
    - GOV Government (USA)
    - MIL Militär (USA)
    - NET Network Provider
    - INT Internationale Organisationen
    - ORG Organisationen anderer Art (z.B. un.org)
    - Country Code (DE, UK, ...)

Domain Name System

- Hierachisches System von Name-Servern
  - Root-Name-Server
  - Delegation von Zonen an DNS-Server
  - beliebig tiefe Staffelung
- DNS-Server
  - Primärer Server: Originaldaten einer Domäne/Subdomäne
  - Sekundäre Server: Kopien der Originaldaten
  - Authoritative Server: Offiziell eingetragenen Server (Primär und sekundär)
- Ablauf
  - Client fragt (lokalen) Server nach Adresse zu einem Namen (oder umgekehrt)
  - Server gibt Namen zurück (oder einen weiteren Server, der zuständig ist, je nach Wunsch des Clienten)

DNS-Einträge

- Verschiedene Record-Typen
  - A-Record — Name -> Adresse
  - PTR-Record — Adresse -> Name
  - CNAME-Record — Aliasname -> („canonical“) Name
  - MX-Record — Mail-Exchanger
  - NS-Record — Name Server
  - SOA-Record — Start of Authority (Zonenparameter)
  - HINFO-Record — Hardware Informationen
  - MINFO-Record — Mail Informationen
  - TXT-Record — Beliebiger Text
  - SRV — Informationen über Dienste (Services)

Netzwerkbetriebssysteme und Namensdienste

- Prinzip
  - Zugriff auf freigegebene Ressourcen über Namen auf Benutzerebene
  - Zugriff über Adressen auf Protokollebene
  - Verwendung von Protokollen/Servern zur Umsetzung
- UNIX/NFS
  - über DNS
- Windows
  - über Anfrage via Broadcast
  - oder über WINS-Server
  - oder ab Windows 2000 über DNS
- Appletalk
  - Namensverwaltung über Router
  - Router als Name-Server
- Novell Netware
  - Verteilung der Namensliste (nur Server) über Router
  - per Broadcast an alle Server
  - Anfrage der Clienten an den nächsten Server

Windows und Namensdienste

- Aufgabenteilung
  - Umsetzung von Name zu Adresse
  - Auflistung aller Server (Browsing)
- Namensverteilung
  - Dynamische Namensregistrierung beim Booten
  - per Broadcast oder über WINS-Server
- Name-Server-Dienst
  - ursprünglich nur per Broadcast
    - Abfrage: suche Adresse zu Name, Zielrechner antwortet
    - unmöglich bei Einsatz von Routern
  - Alternative: Windows Internet Name Service (WINS)
    - zwei festkonfigurierte WINS-Server pro Client
    - WINS-Server synchronisiert
    - dynamische Namensverwaltung/Registrierung durch Clienten
- Browser-Dienst
  - Verwaltung einer Liste von Servern
  - durch einen Master-Browser und (ggf.) mehrere Backup-Browser
  - bei dynamischer Bestimmung der Browser-Server
  - nach Prioritäten (PDC vor BDC vor NT-Server vor NT-Workstation usw.),
  - mit Anmeldung via Broadcast (Probleme mit Routern)

Dynamische Konfigurationen

- BOOTP / DHCP
  - über Server-Tabelle
  - IP-Adresse
  - weitere Konfigurationsinformationen
- Appletalk
  - Zonen und Netznummern über Router
  - Hostnummern dynamisch per Trial-and-Error
- Novell Netware
  - Namen nur für Server (fest)
  - Netzadressen über Router/Server
  - Hostteil der Adresse: MAC-Adresse
- Standard Feature oder Add On
- router- oder broadcast-gesteuert

Teil IX: Sicherheit

Sicherheitsziele

- Sicherheit eines IT-System bedeutet
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
  - Nachvollziehbarkeit von Transaktionen

Risiken vernetzter Systeme

- Viren
  - sich selbst beim Aufruf durch Anwender vervielfältigenden Programme
  - teils mit weiteren Schadensfunktionen
  - früher auf Disketten oder über aus dem Netz kopierte Dateien
  - heute meist per Mail verschickt und automatisch weiterverteilt
- Würmer
  - virenähnlich, aber selbständige Verbreitung über Netz
- Trojaner
  - Programme mit versteckten Nebenwirkungen
  - Ausspähen von Rechnern
  - Hintertüren für Zugriff durch Fremde über das Netz
- Aktive Inhalte von Webseiten
  - JavaScript-, ActiveX-Programme können auf den Rechner ggf. voll zugreifen

Risiken vernetzter Systeme (2)

- Abhören von Daten
  - lokal oder im Intenet
- Hacker
  - Eindringen in Rechner
    - durch Ausnutzung von Softwarefehlern
    - Einschleusen von Trojanern
    - Abhören von Daten
    - Vortäuschen von IP-Adressen (IP Spoofing), Umleiten oder Übernehmen von Sitzungen (Session Hijacking), Erraten von Sequenznummern
  - Unterschiedliche Ziele
    - Nutzung von Massenspeicher und Netzkapazität
    - Ausspähen von Daten
    - Destruktive Maßnahmen
    - Basis für weitere Angriffe
  - fertige Programmpakete im Internet verfügbar („One Click Hacking“ ohne große Kenntnisse)
  - „Denial of Service“-Angriffe (DoS)
  - „Distributed Denial of Service“-Angriffe (DDoS)

Schutzmaßnahmen

- Verschlüsselung
  - von Kennwörtern bei Netzwerkanmeldungen
  - von Dateien
  - von Übertragungen
- Virenscanner
  - auf jedem Rechner,
  - auf Mail-Servern,
  - Signaturen (automatisch) aktualisieren
- Betriebssysteme und Anwendungen
  - Softwarekorrekturen implementieren
  - Sichere Konfiguration von Betriebssystemen und Anwendungen
  - Nicht benötigte Anwendungen/Dienste gar nicht erst installieren
- Firewalls
- Gefährdungs- und Sicherheitsbewusstsein
- http://www.gwdg.de/service/sicherheit

Kryptographieverfahren

- Symmetrische Verfahren: Secret Key
  - Ein – geheimzuhaltender – Schlüssel zum Ver- und Entschlüsseln
  - Algorithmen: DES, 3DES, IDEA, Blowfish, RC4, RC5, AES
- Asymmetrische Verfahren: Public Key
  - Korrespondierende Schlüsselpaare zum Verschlüsseln bzw. Entschlüsseln
  - Ein Teil des Paars bleibt geheim (privater Schlüssel, „private key“). d.h. ist nur dem Eigentümer bekannt.
  - Der andere Teil (öffentlicher Schlüssel, „public key“‘) wird veröffentlicht und steht jedem zur Verfügung.
  - Mit dem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem privaten entschlüsselt werden und umgekehrt.
  - Algorithmen: Diffie-Hellman, RSA, ElGamal
- Kryptographische Hash-Funktionen
  - Erzeugen eines Konzentrats einer Nachricht (kryptographische Prüfsequenz)
  - unumkehrbarer Algorithmus (Einbahnstraße)
  - extrem schwierig zwei Nachrichten zu finden, die den gleichen Hashwert ergeben
  - kleine Änderung der Nachricht ergibt große Änderung des Hashwerts
  - Algorithmen: MD4, MD5, SHA, HMAC

Vergleich der Verfahren

- Geschwindigkeit
  - Symmetrische Verfahren sind wesentlich schneller (im Sinne von verschlüsselten Bytes pro Sekunde)
- Schlüssellänge
  - Für eine sichere, nicht mit „Brute Force“ zu Verschlüsselung sind Mindestlängen von Schlüsseln nötig
  - Symmetrische Verfahren 128-256 Bit nötig
  - Asymmetrische Verfahren 1024-2048 Bit nötig
- Schlüsselverteilung
  - Bei asymmetrischen Verfahren einfacher (weil ja ein Schlüsselteil veröffentlicht werden kann)
- Kombination symmetrischer und asymmetrischer Verfahren
  - dynamische Erzeugung symmetrischer Schlüssel
  - Austausch der neu erzeugten Schlüssel mit asymetrischen Schlüsseln
  - Absender verschlüsselt mit seinem privaten Schlüssel
  - „Session Key“
  - schneller als reine Public-Key-Lösung

Ziele und Lösungsansätze

- Vertraulichkeit
  - Geheimhaltung von Daten oder Nachrichten
  - Komplette Daten/Nachricht verschlüsseln
  - mit symmetrischen Schlüsseln oder
  - öffentlichem Schlüssel des Empfängers oder
- Authentifizierung
  - Sichere Prüfung von Identitäten
  - durch Nachweis der Schlüsselkenntnis
  - Signieren der Nachricht
  - bei asymmetrischen Verfahren: Verschlüsselung mit privaten Schlüssel des Absenders
  - Verschlüsselung der ganzen Nachricht oder nur eines Hashwerts der Nachricht
- Datenintegrität
  - Verhindern bzw. Erkennen von Verfälschungen
  - Verschlüsselung der ganzen Nachricht oder nur eines Hashwerts
  - ggf. mit dem privaten Schlüssel des Absenders

Schlüsselaustausch

- Probleme
  - Sicherer Austausch geheimer Schlüssel (initial)
  - Glaubwürdigkeit öffentlicher Schlüssel
- Lösungen
  - persönliche Übergabe oder Übergabe auf „sicheren“ Wegen
  - Zertifizierung durch glaubwürdige Dritte
    - (Hierarchie von) Zertifizierungsstellen
    - insbesondere „Public Key Infrastructure“ PKI
    - Netz von Vertrauen Infrastructure

Verschlüsselung auf Anwendungsebene

- Spezielle Anwendungen
  - ssh statt Telnet
  - sftp/scp statt ftp (außer Anonymous-ftp)
  - https statt http (soweit Daten nicht öffentlich sein sollen)
  - imaps/pops statt imap/pop
- Umsteigen auf entsprechende Software (ist kostenlos verfügbar) dringend angeraten
- Problem der Zertifikate

Verschlüsselung auf Netzwerkebene

- IPsec-Standard
  - Geeignet zum Aufbau virtueller privater Netze (VPN) in beliebigen öffentlichen Netzen
  - Internet-Standard als Zusatzsoftware oder in IPv6 integriert
  - Varianten
    - Ende-zu-Ende (nur direkte Kommunikation zwischen zwei Geräten)
    - Ende-zu-Standort / End-to-Site (Anbindung externer Rechner an ein Intranet über ein VPN-Gateway)
    - Standort-zu-Standort / Site-to-Site (Tunnel zwischen zwei Netzen über zwei VPN-Gateways)
    - Schutz der Datenintegrität mit „Authentication Header“ (AH)
    - Schutz der Vertraulichkeit mit „Encapsulated Security Payload“ (ESP)
  - Problem: Schlüsselaustausch
    - Session Key mit Hilfe eines Benutzernamens und Kennwort erzeugen
    - nicht standardisiert, daher passende Clienten zum VPN-Gateway nötig
    - RADIUS-Server als Hilfsmittel
- Andere Lösung: PPTP
  - Point to Point Tunneling Protocol
  - weniger sicher
  - arbeitet auf Schicht 2

Firewallprinzipien

- Überwachung, Filterung, Einschränkung von Verkehr zwischen geschützten Netzen und dem Rest der Welt
- Trennung des Netzes in Zonen unterschiedlicher Sicherheit
  - sichere(s) Netz(e) / Intranet / LAN
  - unsicheres Netz / Internet / externes Netz / WAN
  - Demilitarisierte Zone(n) (DMZ) / Perimeter Network
    - Netz „zwischen“ Intranet und Internet
    - mit Rechnern die vom Intranet und Internet zugänglich sein müssen

Firewallvarianten

- nach Funktion
  - Einfache Paketfilter
  - Paketfilter mit Stateful Inspection
  - Application Level Gateways
  - etwas außer der Reihe: Personal Firewall
- nach Geräten
  - spezialisierte Hardware oder
  - „normale“ Rechner mit spezieller Software und spezieller „Härtung“
- Adressumsetzung
  - NAT: Network Address Translation
    - Umsetzung interner Adressen auf externe Adressen
  - PAT: Port Address Translation
    - NAT mit zusätzlicher Änderung der Portnummern
    - Möglichkeit ein ganzes Netz nach außen mit einer ÍP-Adresse erscheinen zu lassen

Paketfilter

- Im Prinzip ein filternder Router oder „Screening Router“
- Filterung nach Kriterien
  - IP-Adressen
  - IP-Protokollen (UDP, TCP, ICMP u.a.)
  - TCP/UDP-Ports, ICMP-Typen
  - TCP-Flags (z.B. Verbindungsaufbau nur in eine Richtung erlaubt)
  - Eingangs- und/oder Ausgangs-Interface
  - Fragmente
- Stateful Inspection (oder nicht)
  - einfache Paketfilter führen nicht über vorhandene Kommunikationen Buch,
  - lassen daher Pakete durch, die nur scheinbar zu einer bestehenden Verbindung gehören
  - Fragmente können so nicht wirklich behandelt werden
  - Dynamisch aufgebaute UDP-Kanäle (z.B. bei Videoübertragungen) können nicht sinnvoll gefiltert werden
  - Hier hilft nur eine Aufzeichnung des Zustands von Verbindungen und / oder detailierte Kenntnis von Protokollen
  - also: Stateful Inspection

Paketfilterbeispiele (1)

- Filter auf Cisco-Router
- Netz ohne Zugriff von außen

```
interface Vlan6
 ip address 134.76.7.254 255.255.254.0
 ip access-group 161 in
 ip access-group 163 out

access-list 161 permit ip 134.76.6.0 0.0.1.255 any
access-list 161 permit ip 224.0.0.0 31.255.255.255 any
access-list 161 deny   ip any any

access-list 163 deny ip 134.76.6.0 0.0.1.255 any
access-list 163 permit tcp any any established
access-list 163 permit ip 134.76.10.0 0.0.1.255 any
access-list 163 permit ip host 134.76.22.1 any
access-list 163 permit icmp any any echo
access-list 163 permit icmp any any echo-reply
access-list 163 permit icmp any any port-unreachable
access-list 163 permit icmp any any time-exceeded
access-list 163 deny   tcp any any eq www
access-list 163 deny   ip any any
```

Paketfilterbeispiele (2)

- Spezielle Regeln für einzelne Server

```
access-list 137 permit tcp any host 134.76.98.8 eq 1500
access-list 137 permit tcp any host 134.76.98.8 eq 1580
access-list 137 permit tcp any host 134.76.98.8 eq 3500
access-list 137 permit tcp any host 134.76.98.8 eq 3580
access-list 137 permit tcp any host 134.76.98.8 eq 1352
access-list 137 permit tcp any host 134.76.98.8 eq www
access-list 137 permit tcp any host 134.76.98.8 eq 443
access-list 137 permit tcp any host 134.76.98.8 eq 389
access-list 137 deny ip any host 134.76.98.8 log
```


Application-Level Gateways

- Prinzip
  - Statt direkter Kommunikation mit dem Internet Kommunikation mit einem Stellvertreter des Dienstes (Proxy Server)
- Realisierung
  - Verbindung geht erst zum Proxy, dann vom Proxy nach außen
  - der Proxy kann für den Benutzer transparent sein (optimaler Fall)
  - Simple Lösung: Benutzer verbindet sich explizit mit dem Proxy, dann vom Proxy weiter (z.B. ssh)
  - Vorteil: mehr Kontrollmöglichkeiten als bei Paketfilter, teils sogar benutzerabhängig
  - Nachteil: anwendungs- bzw. diensteabhängig
  - nur in Verbindung mit einem Paketfilter, um eine Umgehung des Proxy zu verhindern

Personal Firewall

- Filterung auf Endgeräten
  - ähnlich zu Paketfilter
- Probleme
  - Lernmodus
  - Standardregeln entweder zu unkomfortabel oder zu großzügig
  - Endbenutzer muss die Regeln aufstellen – verfügt er über die nötigen Kenntnisse?
  - Prozesse im Rechner – Angreifer können den einfach abschalten
- Was kann eine Personal Firewall (nicht)?
  - keine Filterung von aktiven Inhalten auf WWW-Seiten
  - keine Virenerkennung (auch nicht in Mails)
  - Kontrolle ausgehender Verbindungen
- Durchaus fragwürdiger Nutzen

Teil X: Netzwerkmanagement

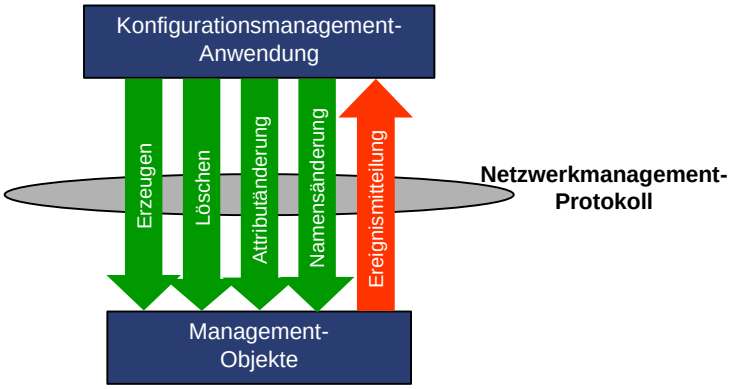
Ziele des Netzwerkmanagements

- Unterteilung in die Teilbereiche (nach OSI)
  - Konfigurationsmanagement (Configuration Management)
  - Fehlermanagement (Fault Management)
  - Leistungsmanagement (Performance Management)
  - Sicherheitsmanagement (Security Management)
  - Abrechnungsmanagement (Accounting Management)

Konfigurationsmanagement

- Aufgaben:
  - Bestandsaufnahme von Netzkomponenten
  - Bestandsführung von Netzkomponenten
  - Manipulation von Netzkomponenten
- Komponenten und deren Elemente als abstrakte Objekte
  - (nicht nur Hardware und Software)
  - Pflege von Datenbankobjekten
  - Zugänglichmachen von Datenbankobjekten
  - Präsentation von Datenbankobjekten

Schema



Fehlermanagement

- Unterteilung in
  - Störungsmanagement und
  - Problemmanagement
- Aufgaben:
  - Entdecken
  - Analysieren
  - Beheben von Fehlern
- Fehlerformen
  - (Total-) Ausfall von Komponenten
  - (Strukturelle) Fehler in der Netzsoftware
  - Minderung der Dienstqualität

Kausalgeflecht von Fehlern

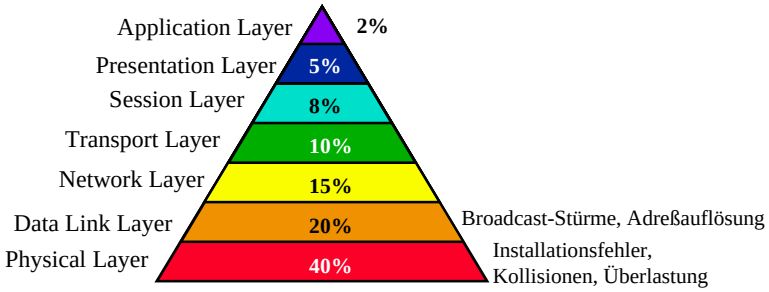
- Mensch
  - Durchführung schädlicher Handlung oder
  - Unterlassen nötiger Handlungen
  - aus
    - Unkenntnis,
    - Unvermögen oder
    - Absicht
- Umwelt, z.B.
  - elektromagnetische Strahlung,
  - Temperatur,
  - Feuchtigkeit,
  - Schmutz,
- Technik, z.B.
  - Konstruktion
  - Fertigungsqualität
  - Transport,
  - Installation,
  - Instandhaltung,
  - korrekte Bedienung,
  - Verschleiß.

Ablauf einer Fehleranalyse

- Ablauf
  - Protokollierung von Zuständen
  - Auswertung der Daten
  - Klassifizierung von Fehlern
  - Alarmmeldung
  - Analyse
  - Rekonfiguration
  - Beseitigung oder Umgehung
- dabei
  - Mitwirkung verschiedener Personen
  - Bedeutung des Benutzern nicht übersehen bei
    - Feststellung
    - Beseitigung
    - Informationspolitik

Fehlerverteilung

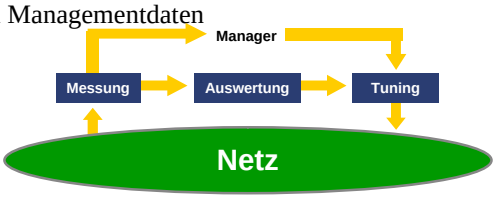
- Fehlerverteilung auf die Schichten des OSI-Referenzmodells (laut Literatur):



- Die Komplexität der Problematik der Fehleranalyse steigt mit der Schicht.

Leistungsmanagement

- Weiterführung des Fehlermanagements
- Sicherstellung der Effizienz und optimalen Funktion des Netzes durch
  - Überprüfung von Leistungskenngrößen
  - Überwachung von Leistungsengpässen
  - Messungen
  - Erfassung und Analyse von Managementdaten
  - Erstellen von Berichten
  - Tuning
- Schema:



- Problem der Belastung des Netzes durch die Messung
  - integrierte Messungen (SNMP)
    - über des Netz
    - automatisiert
  - isolierte Messungen (netzunabhängig, mit Analysator)
- Langfristige Messungen zur Trendanalyse

Sicherheitsmanagement

- Sicherstellung der Funktion des Netzes (Schutz)
- Aufgaben:
  - Überwachung und Erkennen von Angriffen auf die Sicherheit des Netzes,
  - Datenverschlüsselung,
  - Authentifizierung,
  - Ergreifen von Sicherheitsmaßnahmen.
- Unterteilung der Maßnahmen:
  - bau- und versorgungstechnische,
  - organisatorische,
  - technologische,
    - gerätetechnische,
    - programmtechnische.
- Gegensatz: sicheres und offenes Netz
- Dienste des Sicherheitsmanagements
  - Authentisierung (Identitätsprüfung)
  - Zugriffskontrolle (Prüfung von Rechten)
  - Vertraulichkeit (Schutz vor unauthorisiertem Zugriff)
  - Datenintegrität (Schutz vor unauthorisierter Modifikation)

Abrechnungsmanagement

- Kostenmanagement
- Aufgaben:
  - Erfassung von Leistungsdaten
  - Abrechnung von Leistungsdaten
  - Aufbereitung von Leistungsdaten
  - Kontrolle von Limitierungen
  - Speicherung von Abrechnungsdaten

Netzwerkmanagement-Werkzeuge

- Dokumentation
- Ausbildung
  - von Personal und Benutzern
  - zur effizienten und fehlerfreien Nutzung
- Kabelmessgeräte
- Netzwerkanalysatoren
- Netzwerkmanagement-Systeme

Dokumentation

- Verkabelungspläne
  - Kabelverlauf
  - Position von Anschlüssen
- Meßprotokolle
  - Korrekte Verlegung und korrekte Auflegung
    - Kurzschlüsse
    - Adernvertauschung
  - Dämpfung
  - Übersprechen
  - Schleifenwiderstand
  - Kapazität
  - TDR-Messung (Time-Domain-Reflektometer) / Oszilloskop
- Verteilerfelder
  - Übergang Verteilerfeld zum Endgerät
  - Übergang Verteilerfeld zum Verteiler
- Umgebungsbedingungen
  - Zugangsregelungen
  - Elektrische Sicherungen
- Aktive Komponenten
  - Netzverteiler,
  - Internetworking-Komponenten
  - Endgeräte
  - bezüglich
    - Aufstellung
      - Raum
      - Anschlußdose
    - Anschlüsse
      - Adaptertyp
    - Konfiguration
      - MAC-Adresse
      - Protokolladressen (IP, DECnet, usw.)
      - eingesetzte Software (Typ und Release)

Kabelmeßgeräte

- Kabeltester unterschiedlicher Güte
  - Von Spannungsmessungen bis zum
  - Autotest aller Kabelkenngrößen
- Messung mit TDR
  - Aussenden von kurzen Testimpulsen
  - Messung von Reflektionen mit Oszilloskop
  - Suche nach Störstellen im Kabel
- Spezialmeßgeräte zur Überprüfung der aktiven Stationen auf
  - Einhaltung des Takts
  - Signalformen
  - Signalpegel
  - Rauschen
- Aufgaben:
  - vorsorgliche Messung vor Inbetriebnahme
  - Hilfsmittel bei Fehlersuche auf Bitübertragungsschicht

Teil X: SNMP und Netzwerkmanagement-Systeme

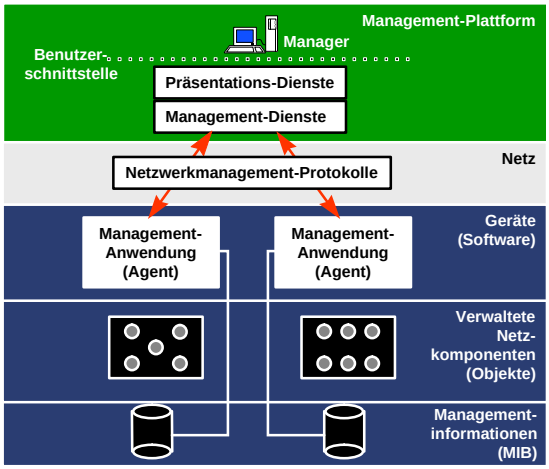
Einfache Managementhilfsmittel

- Vorhandene statistische Informationen
  - von Betriebssystem der Endgeräte
  - von managementfähigen Netzwerkkomponenten
- Einfache Testprogramme
  - ping
  - traceroute
  - netstat

Netzwerkmanagement-Systeme (NMS)

- Ziel
  - Realisierung der Managementaufgaben
  - insbesondere in größeren Netzen
- Prinzipien
  - Management von speziellen Managementstationen
    - zentrale Managementstation
    - mit zusätzlichen Konsolen
    - oder hierarchische Anordnung solcher Stationen und Konsolen
  - Nutzung verteilter Intelligenz im Netz
    - Managementagenten,
    - d.h. Software in Netzwerkkomponenten (auch Endgeräte),
    - sammeln und liefern Zustandsinformationen
    - oder reagieren auf Anweisungen.
  - Netzwerkmanagement-Protokolle
    - zur Kommunikation zwischen Managementstationen und Agenten

Allgemeine Struktur



Kommunikation

- Anweisungen vom Manager an Agenten
  - insbesondere zur Konfiguration von Netzkomponenten
- Abfrage vom Manager zum Agenten
  - „Polling“
  - explizite Abfrage vom Netzwerkmanagement-System zum Agenten
    - periodisch oder
    - bedarfsorientiert
  - Sammeln von Statusinformationen
  - insbesondere zum Fehler- und Leistungsmanagement
  - oder zur Konfigurationsprüfung
- Benachrichtigung vom Agenten an den Manager
  - „Traps“
  - selbständige Meldung des Agenten an das System
  - insbesondere zur Meldung kritischer Zustände

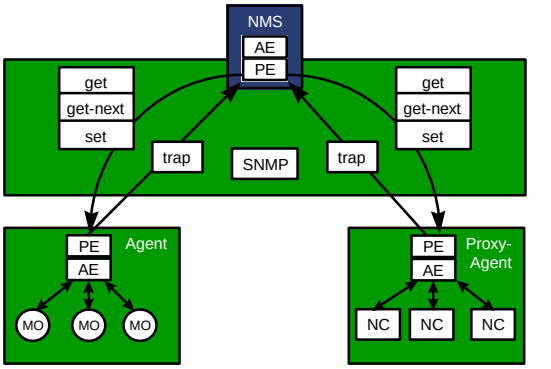
Eignung

- Im Prinzip alle Netzwerkmanagement-Funktionen
- Abhängigkeit von Funktionalität der Agenten
- Weniger für akute Fehler mit Totalausfall geeignet
- Konfigurationsmanagement
- Langfristige Analyse (Leistungsmanagement)
- Fehler in Anwendungsebene meist nicht erkennbar
- Problem: Analyse der Datenmengen

Internet-Standard SNMP

- Simple Network Management Protocol
- Dreiteilung
  - Management-Modell
    - Aufgabenverteilung
    - Kommunikationsstrukturen
  - Management-Informationsmodell
    - Darstellung von Informationen
  - Management-Kommunikationsprotokoll
    - Format des Nachrichtenaustauschs
- In der Praxis das dominierende Protokoll

Management-Modell



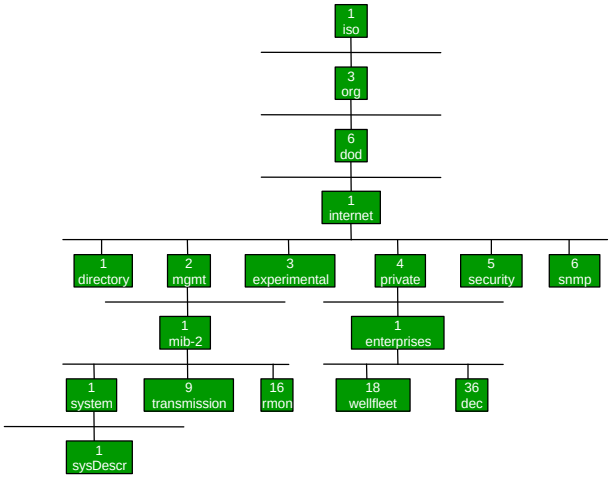
NMS: Network Management System
AE: Application Entity
PE: Protocol Entity
MO: Managed Object
NC: Network Component

- Elemente
  - Manager,
  - Agenten,
  - Managed Objects
  - Proxy Agenten
- Funktionen
  - set
  - get
  - get next
  - trap
- In der Praxis dominiert Polling statt Traps

Management-Informationsmodell

- Organisation der Informationen
  - „Management Information Base“ (MIB)
  - in einer Baumstruktur
  - Standardisierung der Inhalte des Baums
  - Möglichkeiten zur Erweiterung mit firmenspezifischen
  - oder hardwarespezifischen Ergänzungen
- Standardisierte Teile
  - Standard-MIB
    - Allgemeine Systeminformationen
    - Interface-Counter
    - ARP-Tabelle
    - Routing-Tabelle u.a.
  - Spezifische Erweiterungen, z.B.
    - für Brücken (Forwarding Table, Spanning Tree, Statistiken)
    - Ethernet-Geräte (Kollisionen, fehlerhafte Pakete)
- Bezeichnung der Objekte durch
  - Nummern und
  - Namen (in der Praxis optional, aber nach Möglichkeit benutzt)

Ausschnitt aus dem MIB-Baum



Ausblick zu SNMP

- Bewertung von SNMP
  - wenig Ansprüche an Agenten
  - weitverbreitet (der Quasi-Standard)
  - Sicherheitsschwächen
    - Authentifizierung nur durch im Klartext übertragenen „Community“
- SNMP Versionen 2 und 3
  - Verschiedene Varianten von Version 2
    - weitgehend nicht verwendet
  - zur Zeit neue Entwicklung von Version 3
  - Ziele
    - Behebung der Sicherheitsmängel
    - Erweiterung des Management-Modells um Manager-Manager-Kommunikation

Management-Systeme in der Praxis

- Unterteilung in
  - Managementplattformen
    - z.B. HP OpenView und Varianten, Sun NetManager, Cabletron Spektrum
    - Grundfunktionen (s.u.)
  - Elementmanager
    - Speziell angepasste Anwendungen für bestimmte Komponenten
      - Angepasst an herstellerspezifische MIBs
      - detailgetreue graphische Darstellungen
      - häufig in ein Plattformsystem integriert

NMS-Funktionen

- Zugriff auf MIB-Daten
  - Set und Get/Get Next
  - Integrationsmöglichkeit zusätzlicher MIBs (Standards oder Enterprise MIBs)
  - Erstellen von „Anwendungen“
    - als Tabellen oder
    - einfache Diagramme
- Graphische Darstellung der Netzwerktopologie
  - Strukturierung nach IP-Adressen
  - oder aus Brücken ausgelesenen MAC-Adressen
  - Automatische Ermittlung der Rechner und der Struktur
- Automatische Überwachungsfunktionen
  - Einfache Erreichbarkeitstest mit ICMP
    - periodisch
    - für Endgeräte ohne SNMP-Agenten
  - Überwachung von Schwellwerten (in MIBs der Agenten)

NMS-Funktionen (2)

- Ereignisverwaltung (Event Log)
  - Annahme und Interpretation von Traps
  - Aufzeichnung von Ergebnissen der Überwachungsfunktionen
- Konfigurierbare Reaktionen auf Änderung von Netzzuständen
  - Log
  - Mail
  - Pager
  - SNMP-Set
  - Beliebige Programme ausführen
  - Automatische Sammlung von Werten
- Integrationsplattform für zusätzliche Anwendungen (Elementmanager u.a.)

Teil XI: Analyse von Netzwerkproblemen

Zielsetzung und Inhalt

- Einführung in die Analyse von Netzwerkproblemen
- Überblick über die dazugehörigen Methoden und Hilfsmittel, insbesondere
  - Management mit SNMP
  - Überwachung von Netzen mit RMON
  - Einsatz von Protokollanalysatoren
- Vortrag und Vorführung

Arten von Netzwerkproblemen

- Ausfall des Netzes
  - Gesamtes Netz
  - für ein Teilbereich des Netzes
  - für ein einzelnes Gerät
- Leistungsengpässe des Netzes
  - in Form von zeitweisen Leistungseinbrüchen,
  - durch mangelnde Leistungsfähigkeit des Netzes,
  - durch fehlerhaften Einsatz.
- Fehler in Endgeräten

Komplexität von Netzproblemen

- *Problem können gruppiert werden*
  - nach Verursachern
    - Mensch
    - Technik
    - Umwelt
  - nach verursachender Komponente
    - Hardware
    - Software
  - nach Fehlerquelle
    - Kabel
    - Netzwerkverteiler
    - Endgeräte
  - nach Dauer
    - dauerhaft
    - sporadisch
  - nach Auswirkung
    - Totalausfall
    - Leistungsminderung
- *Komplexität erfordert*
  - Methodik,
  - Disziplin,
  - Erfahrung,
  - Intuition

Netzwerkprobleme und der Fortschritt

- Im Rückblick
  - Besondere Probleme durch Wildwuchs
  - Besondere Probleme der Koaxialverkabelung
- Aktuelle Entwicklung
  - Aufbau strukturierter Verkabelungen
  - Einführung von Switching-Technologie
  - Einführung virtueller LANs (VLAN)
  - Steigende Übertragungsraten und Volumina

Methoden der Netzwerkanalyse

- Präventive Maßnahmen
  - Dokumentation
  - Leistungsmessung
- Reaktive Analyse von Netzwerkproblemen
  - Fehler eingrenzen
  - Binary Search
  - Detailanalyse
- Abhängig von Hilfsmitteln

Hilfsmittel der Netzwerkanalyse

- professionell
  - Netzwerkmanagement mit SNMP
  - Remote Monitoring (RMON)
  - Protokollanalysatoren
  - sonstige Meßgeräte
- für den Hausgebrauch
  - Betriebssystemtools
  - Testen durch Benutzen
- nicht vergessen
  - Netzwerkdokumentation

Analyse von Netzwerkproblemen mit SNMP

- Erkennbarkeit von Totalausfällen
  - Relevant vor allem in größeren Netzen
- Störungsanalyse mit Hilfe intelligenter Netzkomponenten
  - Repeater,
  - Brücken,
  - Switches,
  - Router
- mit Management-Agenten
- Leistungsanalyse durch Abfrage geeigneter Netzkomponenten
- Langfristige Trendanalyse

Typische SNMP-zugängliche Betriebsdaten

- allgemein (RFC1213 / MIB-II)
- Netztechnologie-bezogenen Daten für z.B.
  - Ethernet (RFC1515)
  - Token-Ring (RFC1513)
  - FDDI (RFC1512)
- Komponenten-bezogene Daten für z.B.
  - Ethernet-Repeater (RFC1516)
  - Brücken (RFC1493 und RFC1525)
- Protokollbezogene Daten für z.B.
  - DECnet Phase IV (RFC1559)
  - Appletalk
  - DNS (RFC1611 und RFC1612)

MIB für Ethernet-Interfaces

- Informationen über z.B.
  - Alignment Errors: Anzahl Bits nicht Vielfaches von 8
  - FCS Errors: Falsche Prüfsequenz
  - Single Collisions: Anzahl gesendeter Pakete, bei denen einmal der Sendevorgang kollisionensbedingt abgebrochen wurde.
  - Multiple Collisions: Analog für mehrfache Kollisionen
  - Deferred Transmissions: Anzahl Pakete, die wegen Belegung des Mediums durch andere Stationen nicht sofort gesendet werden konnten.
  - Late Collisions: Anzahl Kollisionen, die nach Senden von mindestens 64 Bytes auftraten.
  - Excessive Collisions: Anzahl Pakete, die nach 16maliger Kollision nicht gesendet wurden.
  - Carrier Sense Errors: Fehler beim Abhören des Mediums
  - Frame Too Long
  - Collision Statistics: Verteilung der Kollisionen auf ein- bis 16malige Kollisionen für ein einzelnes gesendetes Paket.

MIB für Ethernet-Repeater

- Informationen zu allen Ports des Repeaters
- Informationen zu Portgruppen (z.B. Module in Hubs)
- Interessant für die Analyse von Netzwerkproblemen:
  - Fehlerfrei Pakete
  - Fehlerfrei Oktette
  - Kollisionen
  - FCS Errors: Falsche Prüfsequenz
  - Alignment Errors: Bitzahl nicht durch 8 teilbar
  - Frame Too Long: Paket zu lang (>1518 Oktette)
  - Very Long Events
  - Short Events: Paket kleiner 74-82 Bit (evtl. externe Einstrahlung, dadurch Erzeugung von Runts oder Late Events durch Repeater)
  - Runts: Paket kleiner 64 Byte (aber größer als Short Event), evtl. nach Kollisionen auf anderen Strängen von Repeatern erzeugt.
  - Late Events: Kollisonen nach Empfang von 64 oder mehr Oktetten (evtl. zu lange Signallaufzeiten oder Störeinstrahlung)
  - Data Rate Mismatches
  - Autopartitions: Anzahl von Portabschaltungen wegen Fehlern

MIB für Brücken / Switches

- Informationen über
  - Spanning Tree Protokoll
  - Transparent Bridges
  - Source Route Bridges
- Für Problemanalyse interessant
  - In Frames
  - Out Frames
  - In Discards
  - Nicht weitergeleitete Pakete, sollte ca. 80% von In Frames sein.
  - Delay Exceed Discards
  - MTU Exceed Discards
  - Spanning Tree Topology Change
  - Forward Transitions
  - Forwarding Database

Netzwerkproblemanalyse mit RMON

- Was ist RMON
  - Abkürzung für „Remote Monitoring“,
  - Standard zur erweiterten Überwachung von Ethernet- und Token-Ring-Netzsegmenten: RFC1757 „Remote Network Monitoring Management Information Base“und RFC1513 „Token Ring Extensions to the Remote Monitoring MIB“
  - erweitert in Version 2 (RMON2): RFC2021 „Remote Network Monitoring Management Information Base Version 2 using SMIv2“ und RFC2074 „Remote Network Monitoring MIB Protocol Identifiers“
  - unter Einsatz spezieller SNMP-Agenten und
  - spezieller RMON-Managerprogramme.
  - (von verschiedensten Herstellern, evtl. mit Erweiterungen für Agenten, die über den Standard hinausgehende Funktionalitäten beinhalten)
- Verfügbarkeit
  - als dedizierte RMON-Probes
  - integriert in Repeater, Ringleitungsverteiler, Switches usw.
  - Proprietäre Erweiterungen z.B. für FDDI oder Analyse höherer Protokollschichten

RMON Funktionalitäten

- Aufteilung in Gruppen
  - Allgemeine Statistik
  - Statistik über die Zeit
  - Rechner bezogenen Informationen auf Basis der MAC-Adressen
    - Host Group
    - Host Top N Group
    - Matrix Group
  - Überwachung und Alarmierung
    - Alarm Group
    - Event Group
  - Datenaufzeichnung einschließlich Filterung
  - Konfigurationsmöglichkeiten
  - Token-Ring-spezifische Parameter
  - Protokollverteilung
  - Adresstabellen
  - Rechnerbezogene Information auf der Netzwerkebenen
    - Network Layer Host Group:
    - Network Layer Matrix Group:
  - Rechnerbezogene Information auf der „Anwendungsebene“
    - Application Layer Host Group:
    - Application Layer Matrix Group:
  - Benutzerdefinierte, zeitabhängige Statistik über externe Datenquellen

Allgemeine Statistik

- Kumulative Statistik
  - für Ethernet- bzw.
  - Token-Ring-spezifische Parameter
  - bezüglich Last und
  - Fehlern.
- Statistik über die Zeit
  - realisiert in den Gruppen
    - History Control und
    - Ethernet History bzw.
    - Token Ring History,
  - erfaßt in konfigurierbaren Zeitintervallen
  - und über einen konfigurierbaren Zeitraum
  - mit den gleichen Inhalten wie zuvor.

Rechnerbezogene Informationen

- Host Group
  - kumulative Zähler pro Rechner (Pakete, Oktette, Fehler)
- Host Top N Group
  - als kurzzeitige Zähler pro Rechner für das letzte Zeitintervall
- Matrix Group
  - für kumulative Zähler über Sender-Empfänger-Paare
- auf Basis der MAC-Adressen

Überwachung und Alarmierung

- Alarm Group
  - Überwachung von Schwellwerten zur Erzeugung von Ereignissen
  - bei Über- und Unterschreitung von Schwellwerten
- Event Group
  - Konfigurierbare Reaktion auf Ereignisse
    - Log
    - SNMP-Trap
    - Log und SNMP-Trap
  - Verwaltung eines Event Log

Datenaufzeichnung mit Filterung

- Filter über Bitmasken
- Verknüpfung mehrere Filter
- Aufzeichnung gefilterter Daten
- Auslesen der gesammelten Daten über SNMP
- üblicherweise Datendekodierung auf Managementstation

Token-Ring-spezifische Parameter

- Ringordnung
- Endstationskonfiguration

Protokollverteilung

- Protocol Distribution Group:
- Zählung von Paketen und Okteten
- für verschiedene Protokolle der Netzwerkschicht oder
- für verschiedene Schichten oberhalb der Netzwerkschicht,
- RMON2-Erweiterung,
- Protokollauswahl Probe-Hersteller- und konfigurationsabhängig

Adresstabellen

- Address Mapping Group:
- Umsetzung MAC-Adressen zu Netzwerkadresse,
- für verschiedene Protokolle möglich,
- RMON2-Erweiterung,
- Protokollauswahl Probe-Hersteller- und konfigurationsabhängig

Information auf der Netzwerkebenen

- Network Layer Host Group:
  - Zählung von gesendeten Paketen und Okteten
  - für einzelne Rechner
  - auf Basis von Netzwerkadressen (Schicht 3)
  - als kumulative Tabelle oder
  - als Tabelle der Top-User im letzten Intervall.
- Network Layer Matrix Group:
  - Zählung von Paketen und Okteten
  - für Sender-Empfänger-Paare
  - auf Basis von Netzwerkadressen (Schicht 3)
  - als kumulative Tabelle oder
  - als Tabelle der Top-Paare im letzten Intervall.
- RMON2-Erweiterung,
- Protokollauswahl Probe-Hersteller- und konfigurations-abhängig

Information auf der „Anwendungsebene“

- Application Layer Host Group:
  - Zählung von gesendeten Paketen und Okteten
  - für einzelne Rechner
  - auf Basis von Anwendungsadressen (oberhalb Schicht 3)
  - als kumulative Tabelle oder
  - als Tabelle der Top-User im letzten Intervall.
- Application Layer Matrix Group:
  - Zählung von Paketen und Okteten
  - für Sender-Empfänger-Paare
  - auf Basis von Anwendungsadressen (oberhalb Schicht 3)
  - als kumulative Tabelle oder
  - als Tabelle der Top-Paare im letzten Intervall.
- RMON2-Erweiterung,
- Protokollauswahl Probe-Hersteller- und konfigurationsabhängig

Benutzerdefinierte, zeitabhängige Statistik

- Statistik über externe Datenquellen
- User History Collection Group:
- Zugriff auf SNMP-Zählerobjekte anderer Geräte,
- in konfigurierbaren Intervallen
- über eine konfigurierbare Zeit gespeichert,
- RMON2-Erweiterung.

Konfigurationsmöglichkeiten

- Protocol Directory Group
- Probe Configuration Group
- RMON2-Erweiterung.

RMON Einsatzmöglichkeiten

- Offline Überwachung
  - längerfristiger Einsatz
  - daher auch bei sporadisch auftretenden Problemen nützlich
  - Abfrage teilweise auch mit Verzögerung
- Proaktive Überwachung
- Alarmierung über Traps
- unter minimaler Netzlast Überwachung autonom durch Agent
- Probleme bei Inband-Zugriff

Funktionalitäten von Netzwerkanalysatoren

- Mitlesen von beliebigem Netzverkehr
- Statistische Auswertungen
  - auf MAC-Ebene
  - evtl. auf höheren Schichten
- Aufzeichnung von Datenpaketen
- Protokolldekodierung
  - Offline oder Online
  - Mit oder ohne weitere Analyse
- Lastgenerierung und Durchsatzmessung

Beispiele

- Softwarelösungen für Standardrechner
  - Etherload unter DOS
  - Etherreal
  - und mehr
- Spezialsysteme
  - Expert Sniffer von NAI
  - Observer von Network Instruments
  - Etherpeek von Wildpakets
  - Viele weiter, z.B. von Acterna, Hewlett Packard, …