# Module 2 – Networking Fundamentals

CCNA 1 version 3.0

# Objectives



Students completing this module should be able to:

- Briefly outline the history of networking.
- Identify devices used in networking.
- Understand the role of protocols in networking.
- Define LAN, WAN, MAN, and SAN.
- Explain VPNs and their advantages.
- Describe the differences between intranets and extranets
- Explain the importance of bandwidth in networking.
- Use an analogy from their experience to explain bandwidth.
- Identify bps, kbps, Mbps, and Gbps as units of bandwidth.
- Explain the difference between bandwidth and throughput.
- Calculate data transfer rates.
- Explain why layered models are used to describe data communication.
- Explain the development of the Open System Interconnection model (OSI).
- List the advantages of a layered approach.
- Identify each of the seven layers of the OSI model.
- Identify the four layers of the TCP/IP model.
- Describe the similarities and differences between the two models.

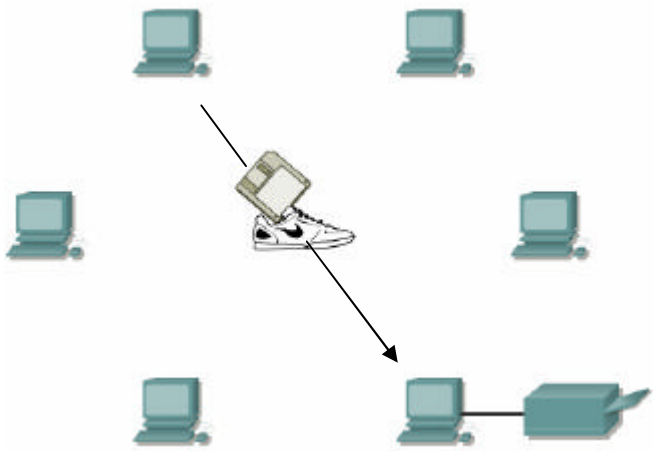
- Networking Terminology
- Network metrics
- Network and Protocol Layers

# Once upon the time



- The advent of the **microcomputer** brought data processing from the enterprise and departmental level to the desktop (***personal computer***).
- One of the difficulties of **decentralized computing** is that it isolates users from one another and from the data and applications they may need to use in common.
- The **early solution** to this was the so called **SneakerNet**: Put the file on **floppy disks** and hand carry them to the necessary destinations.

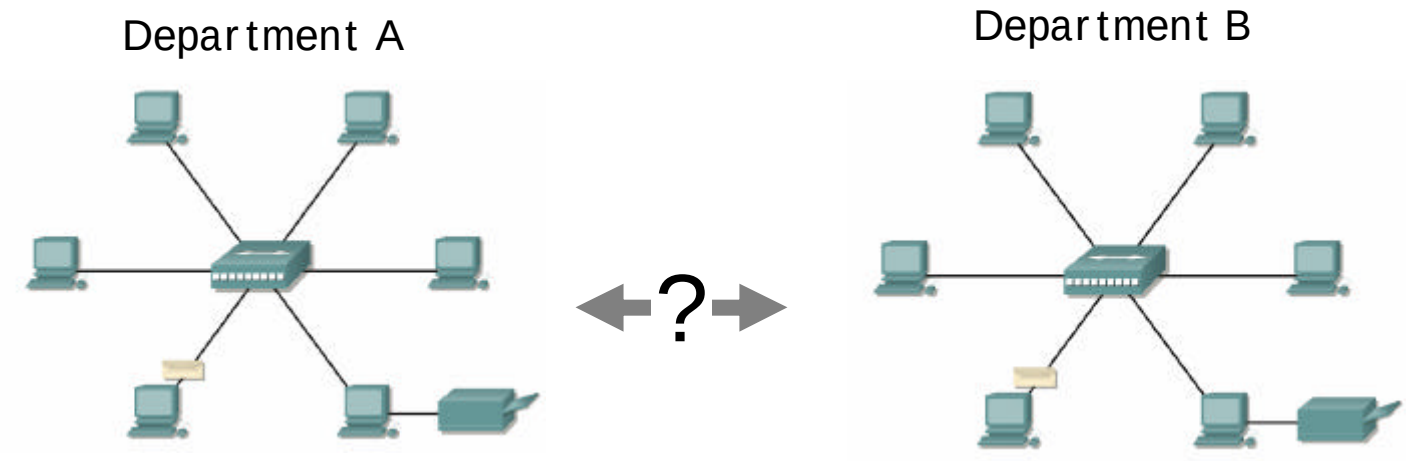
  - ineffective
  - not scalable



Stand-alone PCs
Stand-alone printers

# Data Networks

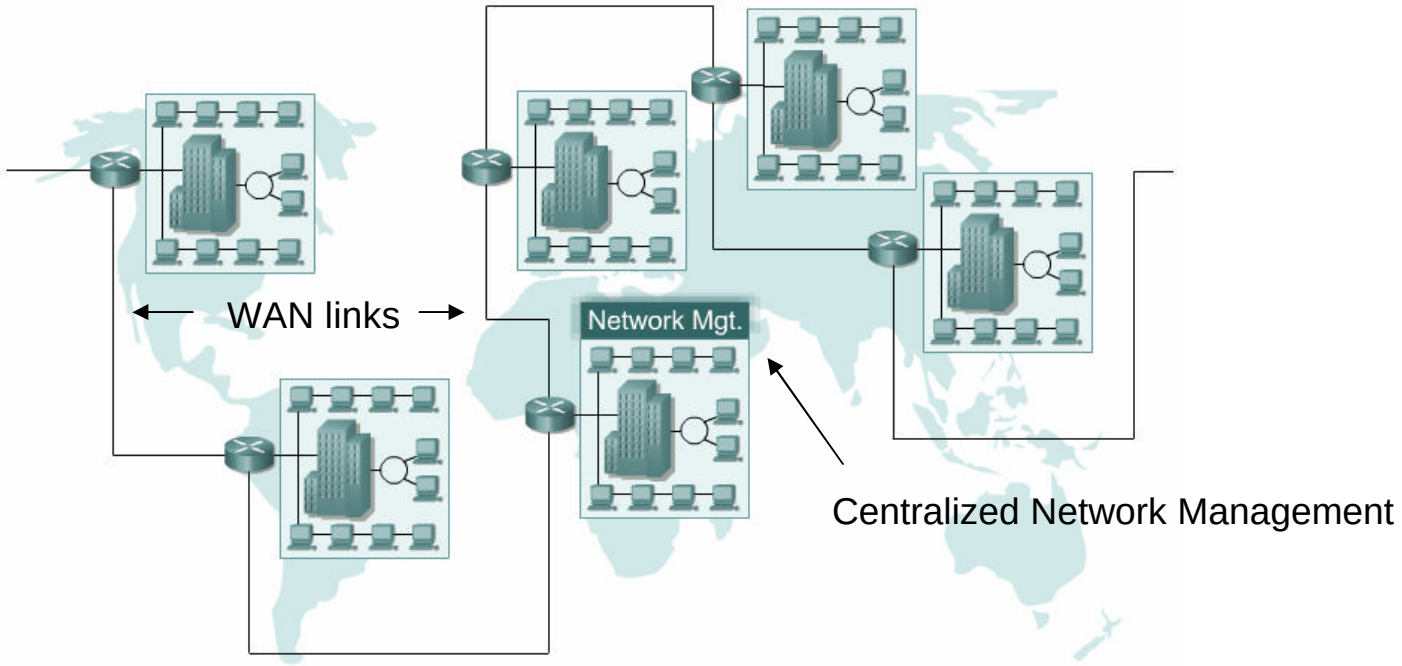





- In the 70s enterprise departments created standardized local-area network (LAN) to interconnect their computers within the departments.
- Standalone printers were replaces by powerful network printers
- **But**: In a LAN system, each department of the company is a kind of electronic island. There is no communication between the departments LAN.
- Consequences:
  - Still sneaker nets
  - Ineffective usage of resources
  - Lack of central network management
- As the use of computers in businesses grew, it soon became obvious that interconnection of LANs is necessary. Inter-LAN communication is also called internetworking.

# Data Networks






- Interconnected LANs of one enterprise were called an Intranet
- Soon it became obvious, that intranets needed to be interconnected with intranets of business partners such as suppliers, vendors or customers in order to share business's information. The resulting internetworks are also called Extranets.
- The solution was the creation of metropolitan-area networks (MANs) and wide-area networks (WANs).

# Network History



| Internet Timeline | |
|---|---|
| Pre-1900 | Long distance communications via messenger, rider, smoke signals, carrier pigeon, optical telegraph, electrical telegraph |
| 1890s | Bell invents the telephone; telephone service expands rapidly. |
| 1901 | Marconi's first transatlantic wireless transmission |
| 1920s | AM Radio |
| 1939 | FM Radio |
| 1940s | WWII spurs radio and microwave development. |
| 1947 | Shockley, Barden and Brittain invent the solid-state (semiconductor) transistor. |
| 1948 | Claude Shannon publishes "A Mathematical Theory of Communication". |
| 1950s | Invention of Integrated Circuits. |
| 1957 | ARPA is created by DoD. |
| 1960s | Mainframe Computing |
| 1962 | Paul Baran at RAND works on "packet switching" networks. |
| 1967 | Larry Roberts publishes first paper on ARPANET. |
| 1969 | ARPANET established at UCLA, UCSB, U-Utah, and Stanford. |
| 1970s | Widespread use of digital integrated circuits; advent of digital personal computers. |

# Network History



| Internet Timeline | |
|---|---|
| 1970 | ALOHANET is developed by University of Hawaii. |
| 1972 | Ray Tomlinson creates email program to send messages. |
| 1973 | Bob Kahn and Vint Cerf begin work on what later becomes TCP/IP.The ARPANET goes international with connections to University College in London, England and the Royal Radar Establishment in Norway. |
| 1974 | BBN opens Telnet, the first commercial version of the ARPANET. |
| 1980s | Widespread use of personal computers and Unix-based mini-computers. |
| 1981 | The term Internet is assigned to a connected set of networks. |
| 1982 | ISO releases OSI Model and protocols; the protocols die but the model is very influential. |
| 1983 | Transmission Control Protocol/Internet Protocol (TCP/IP) becomes the universal language of the Internet. ARPANET is split into ARPANET and MILNET. |
| 1984 | Cisco Systems founded; gateway and router development begins. Domain Name Service introduced. The number of Internet hosts exceeds 1000. |
| 1986 | NSFNET is created (with a backbone speed of 56 KBps). |
| 1987 | The number of Internet hosts exceeds 10,000. |
| 1988 | Computer Emergency Response Team (CERT) is formed by DARPA |

Ethernet

# Network History

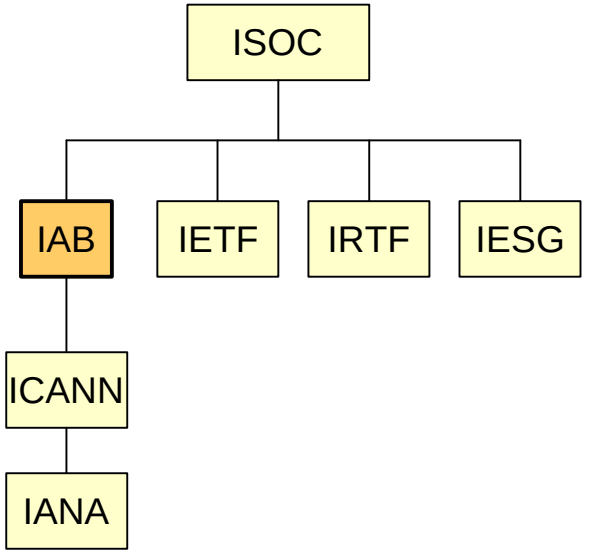


| Internet Timeline | |
|---|---|
| 1989 | The number of Internet hosts exceeds 100,000. |
| 1990 | ARPANET becomes the Internet. |
| 1991 | The World Wide Web (WWW) is born. Tim Berners-Lee develops code for WWW. |
| 1992 | Internet Society (ISOC) is chartered. Number of Internet hosts breaks 1,000,000. |
| 1993 | Mosaic, the first graphics-based Web browser, becomes available. |
| 1994 | Netscape Navigator introduced. |
| 1996 | The number of Internet hosts exceeds 10 million. The Internet covers the globe. |
| 1997 | The American Registry for Internet Numbers (ARIN) is established. Internet 2 comes online. |
| Late 1990's til present | Internet users doubling every 6 months (exponential growth.) |
| 1998 | Cisco hits 70% of sales via internet, Networking Academies launched. |
| 1999 | Internet 2 backbone network deploys IPv6. Major corporations race toward the video, voice and data convergence. |
| 2001 | The number of Internet host exceeds 110 million. |

# Development and Maintenance of the Internet



- **Internet Society** (www.isoc.org):
  - founded in 1992
  - Professional membership organisation with more than 150 member organizations and 16000 members in more than 180 countries
  - Responsible for the further development of the internet
  - Head organisation of IAB, IETF, IRTF, IESG
- **Internet Architecture Board** ( www.iab.org )
  - advises the ISOC
  - supervises the IETF activities (Process of standardisation, Protocol architectures,...)
  - mediates complaints about standardisation process
  - issues RFCs
  - administers IETF protocol parameters (RFC 1700)
  - responsible for further technical development. The IAB has two boards:
    - **Internet Engineering Task Force** (www.ietf.org) for short-term technical developments,
    - **IRTF** (Internet Research Task Force) for long-term technical developments.



# Development and Maintenance of the Internet



- **IESG** Internet Engineering Steering Group
- is responsible for technical management of IETF activities and the Internet standards process.
- **ICANN** Internet Corporation for Assigned Names and Numbers (ICANN)
  - is a technical coordination body for the Internet. Created in October 1998 by a broad coalition of the Internet's business, technical, academic, and user communities, ICANN is assuming responsibility for a set of technical functions previously performed under U.S. government contract by IANA and other groups.
  - coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:
    - Internet domain names IP address numbers (www.iana.org/assignments/ipv4-address-space)
    - protocol parameter and port numbers (http://www.iana.org/numbers.html)
  - coordinates the stable operation of the Internet's root server system.
  - **IANA** Internet Assigned Numbers Authority (www.iana.org)
  - serves ICANN as a bookkeeper in recording the assignments that are made (**registration service**): IP addresses, protocol numbers, other identifiers … (http://www.iana.org/numbers.html)
  - The IANA web page "Internet Protocol v4 Address Space" documents how the IPv4 address space is distributed among the (Regional Internet Registries (RIRs).
- **DENIC** (DE Network Information Center)

# Development and Maintenance of the Internet



- The Internet is a „anarchial“ network which is only regulated (in it's public part) but not controlled. Behavior codex: „Netiquette“ (RFC 1855)
- Technical recommendations are called **RFC**s (Request for Comment):
  - today about 6000 RFCs exist,
  - ~50 RFCs are Internet Standards.
  - RFC‘ s are open standards. Everybody can submit RFCs. The IAB checks them:
    - Meaningful RFCs become a proposed standard
    - If there exist at least 2 interworking implementations the RFCs become a Draft Standard
    - RFCs with noteworthy application become an Internet Standard

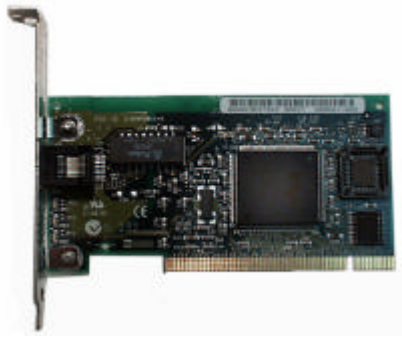
# Entwicklung und Betrieb des Internet - Standardisierung



- **1992** Gründung der **Internet Society** (www.isoc.org):
  - Verband mit mehr als 150 Mitglieds-Organisationen und 16000 Mitgliedern in mehr als 180 Ländern
  - Verantwortlich für die Weiterentwicklung des Internet
  - Dachverband des IAB, IETF, IRTF, IESG
- **Internet Architecture Board** (www.iab.org)
  - berät die ISOC
  - beaufsichtigt das IETF (Standardisierungsprozeß, Protokollarchitekturen,...)
  - schlichtet Beschwerden über Standardisierungsprozeß
  - Herausgeber der RFCs
  - verwaltet IETF Protokollparameter (RFC 1700)
  - für die technischeWeiterentwicklung zuständig. Im IAB gibt es zwei Gremien:
    - **Internet Engineering Task Force** (www.ietf.org) für kurzfristige technische Entwicklungen,
    - **IRTF** (Internet Research Task Force) für langfristige technische Entwicklungen.
- **IANA** Internet Assigned Numbers Authority
- **DENIC** (DE Network Information Center)
- Das Internet ist ein „anarchisches" Netz, es wird nur reguliert und (im öffentlichen Teil ) nicht reglementiert. Verhaltenskodex: „Netiquette".
- Technische Festlegungen werden als **RFC**s (Request for Comment) bezeichnet:
  - derzeit gibt es ca. 6000,
  - ~50 RFCs sind Internetstandards.
  - RFC' s sind frei verfügbar. Jeder kann RFC einreichen. Das IAB prüft.
    - Wenn sinnvoll: Proposed Standard
    - Liegen mindesten zwei unabhängige Implementierungen vor, die zusammenarbeiten: Draft Standard
    - Erfolgt nennenswerte Anwendung: Internetstandard

# Networking Devices



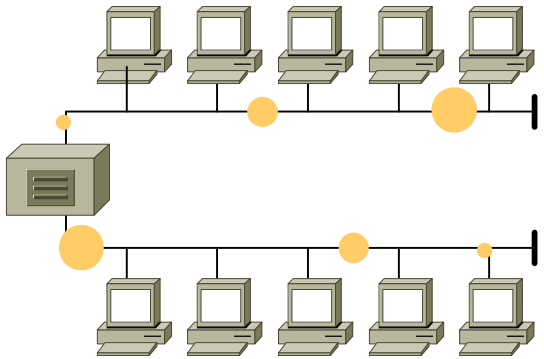


| Network Devices | |
|---|---|
| Repeater  | Bridge  |
| 10BASE-T Hub  | Workgroup Switch  |
| 100BASE-T Hub  | Router  |
| Hub  | Network Cloud  |

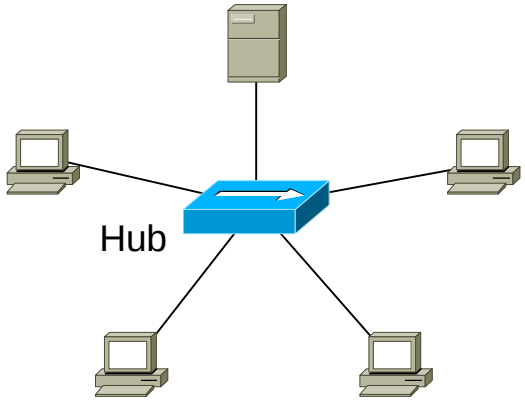
# Networking Devices - Repeater



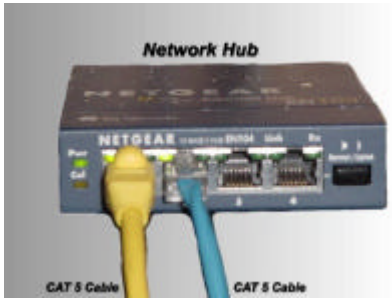
- **Repeaters** work at bit level. They regenerate ~~analog or~~ digital signals that are distorted by attenuation, by added noise or by media dispersion effects. This allows them to travel a longer distance.
- A repeater does not make intelligent decision concerning forwarding packets like a router or bridge .




- **Hubs** concentrate hosts.
- This is done passively, without any other effect on the data transmission (passive hubs).
- Active hubs concentrate hosts and also regenerate signals. They are also called multiport repeaters.
- Duties of a digital signal repeater are
  - signal equalization to reduce distortions introduced by imperfections of transmission media
  - amplification to compensate for attentuation
  - amplitude decision to recover the Bits
  - clock extraction from received signal for retiming of the Bits

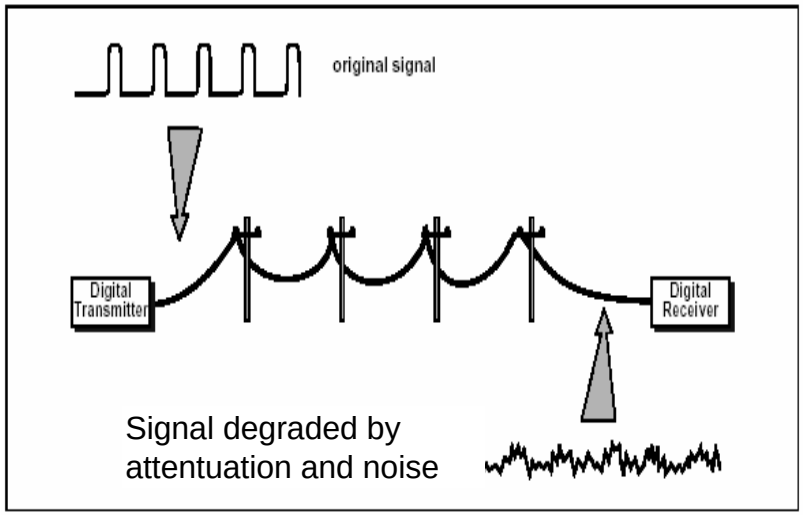



**Hub**: Only one device at a time can talk.

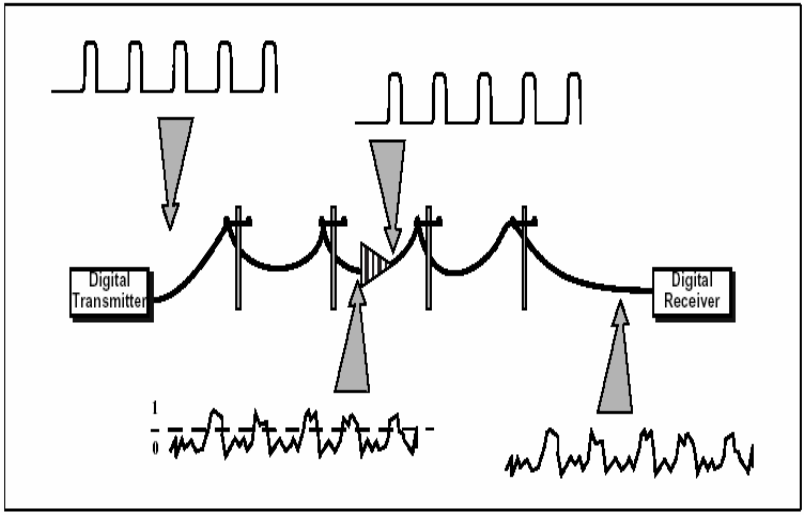


# Problems limiting Digital Signal Transmission

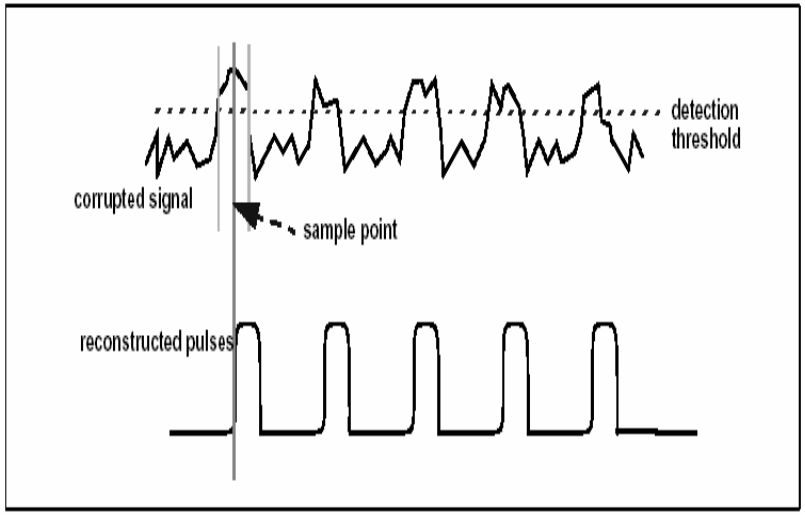




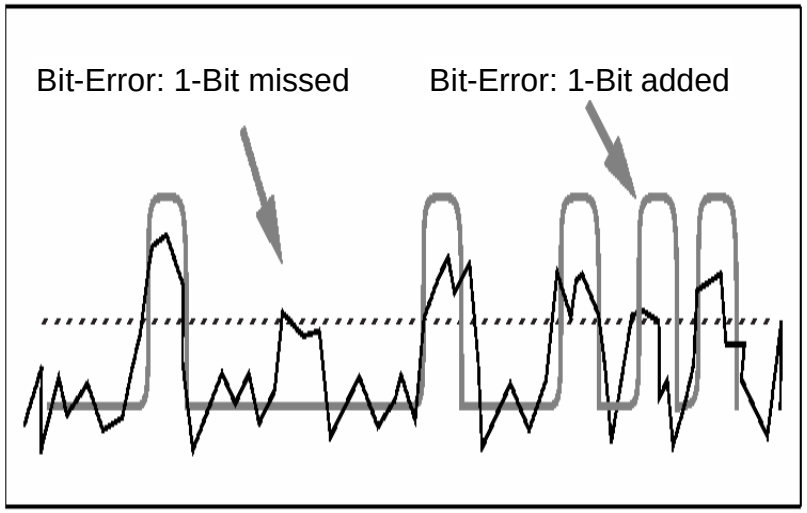

**Digital Signal Transmission**




**Digital Reapeater in Circuit**



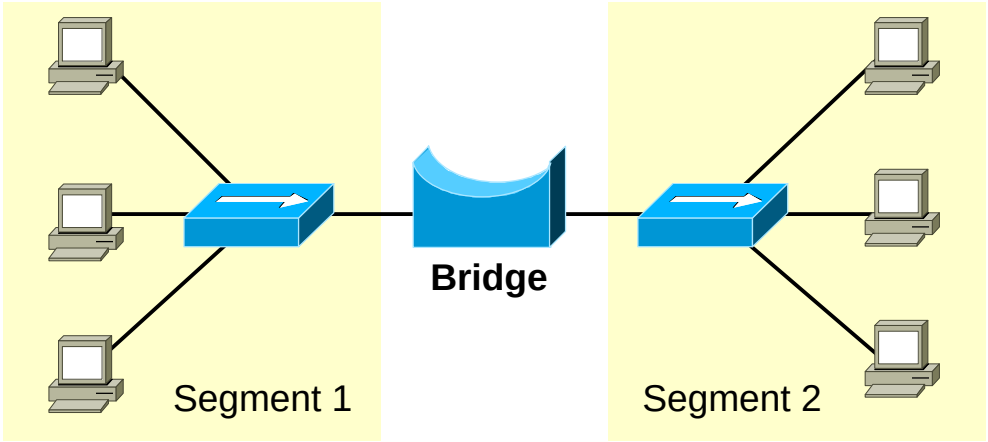

**Digital Signal Regeneration**




**Digital Signal Error Types**

# Networking Devices - Bridge



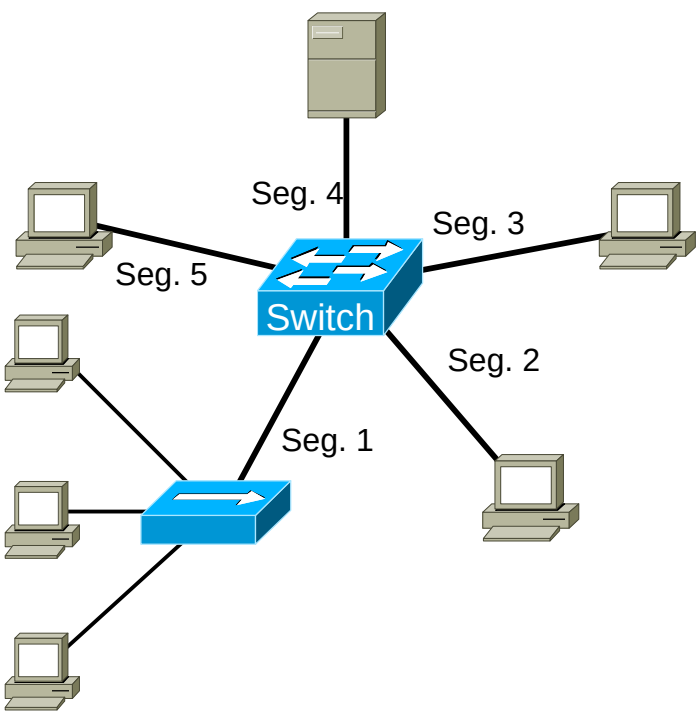



## Bridges

- Convert network data formats
- Perform basic data transmission management.
  - Provide connections between LAN segments.
  - Check data to determine if it should cross the bridge.
  - This makes each part of the network (Segment) more efficient.

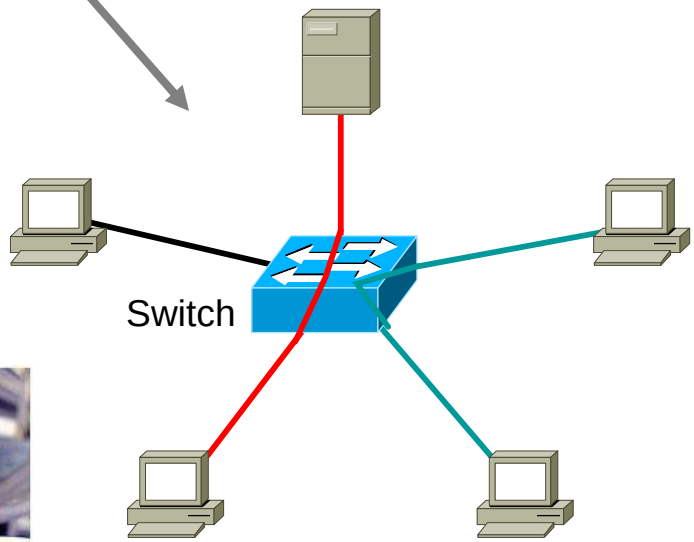
## Workgroup switches

- do not convert data transmission formats as a bridges can do.
- Segments a LAN into more and smaller segments (microsegmentation)
- Act like multiport bridges: They can determine if data should remain on a LAN segment and transfer data only to the connection that needs it.
- Add more intelligence to data transfer management. That means
  - multiple devices can talk at the same time.





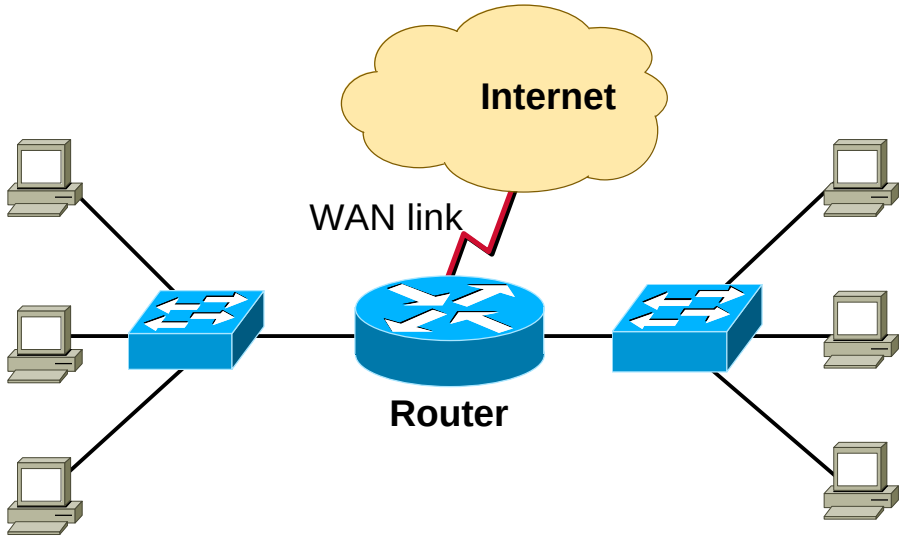
**Switch**



# Networking Devices - Routers



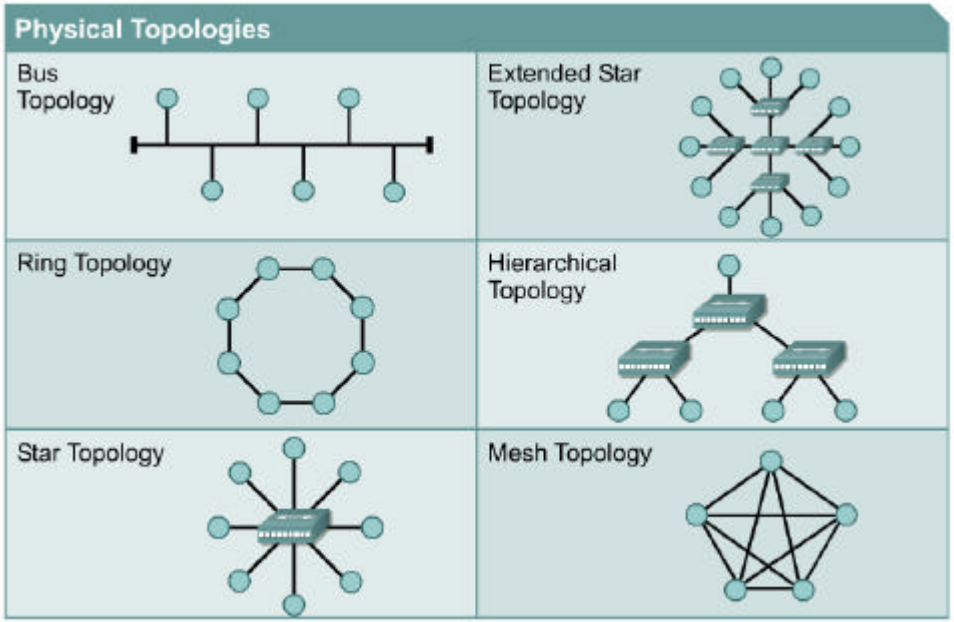
- **Routers** have all the capabilities listed above. Routers can
  - regenerate signals,
  - concentrate multiple connections,
  - convert data transmission formats,
  - manage data transfers.

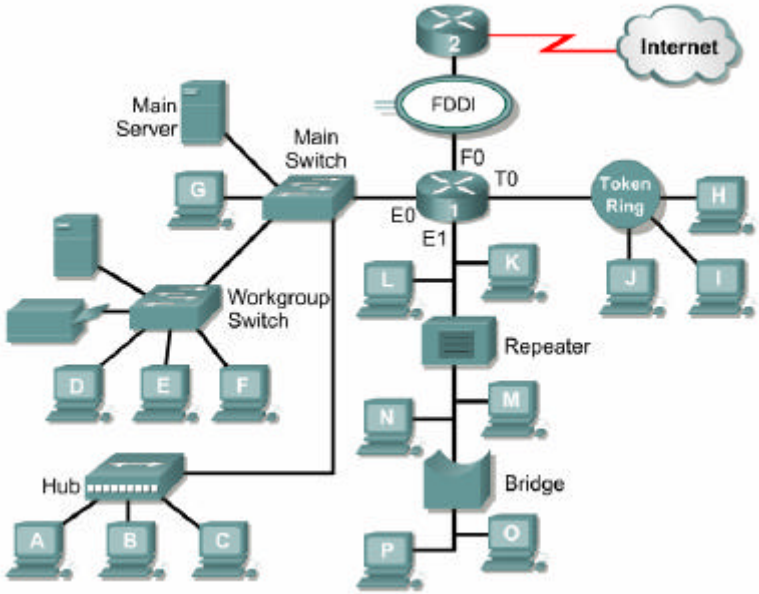



- They can also
  - connect to a WAN, which allows them to connect LANs that are separated by great distances. None of the other devices can provide this type of connection.

# Network Topology - Overview



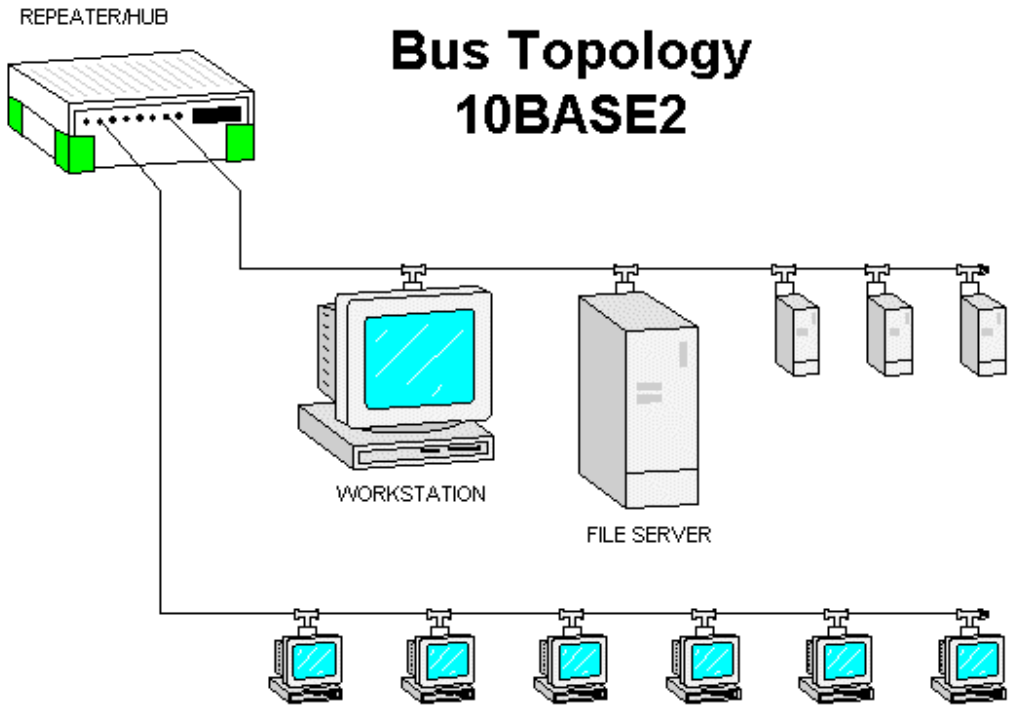



- Network topology defines the structure of the network.
  - Physical topology, which is the actual layout of the wire or media.
  - Logical topology, which defines how the media is accessed by the hosts for sending data and how the hosts communicate across the medium..
- The two most common types of logical topologies are broadcast and token passing.

# Physical Bus Topology



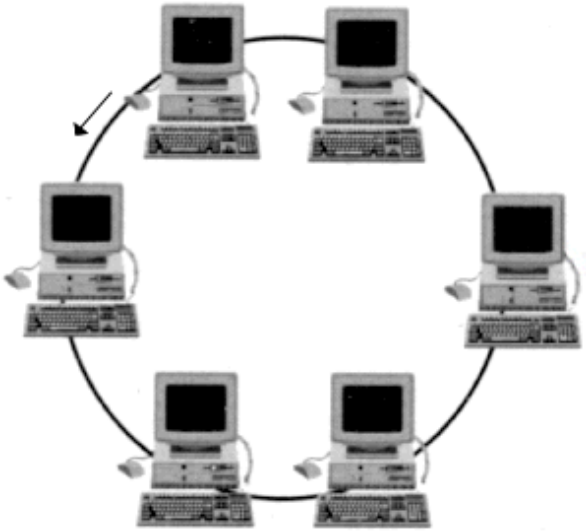


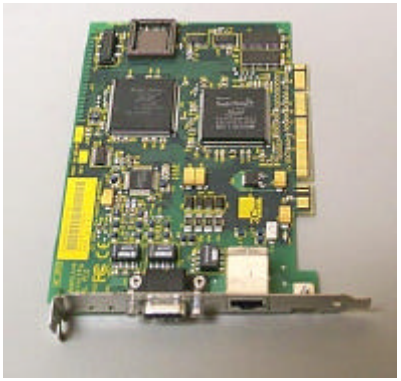

"A bus topology uses a single backbone segment (length of cable) that all the hosts connect to directly."

# Physical Ring Topology



"A ring topology connects one host to the next and the last host to the first. This creates a physical ring of cable."

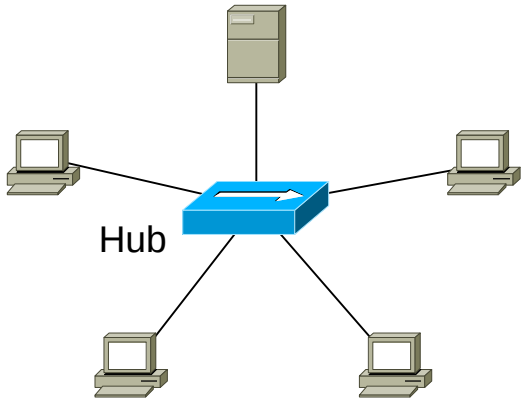


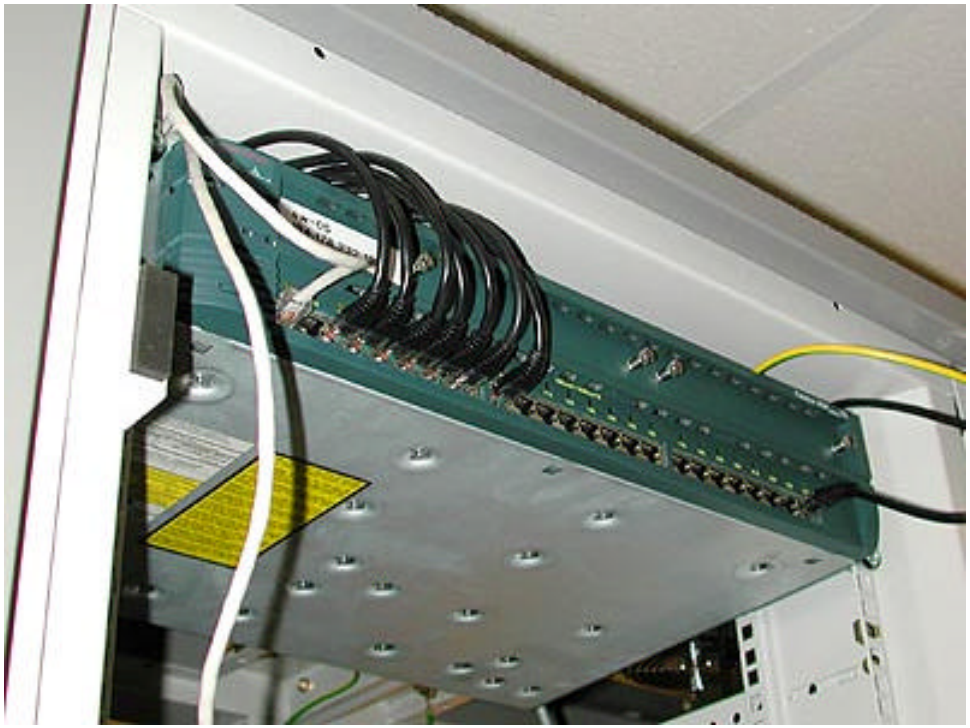


Physical ring topology

# Physical Star Topology



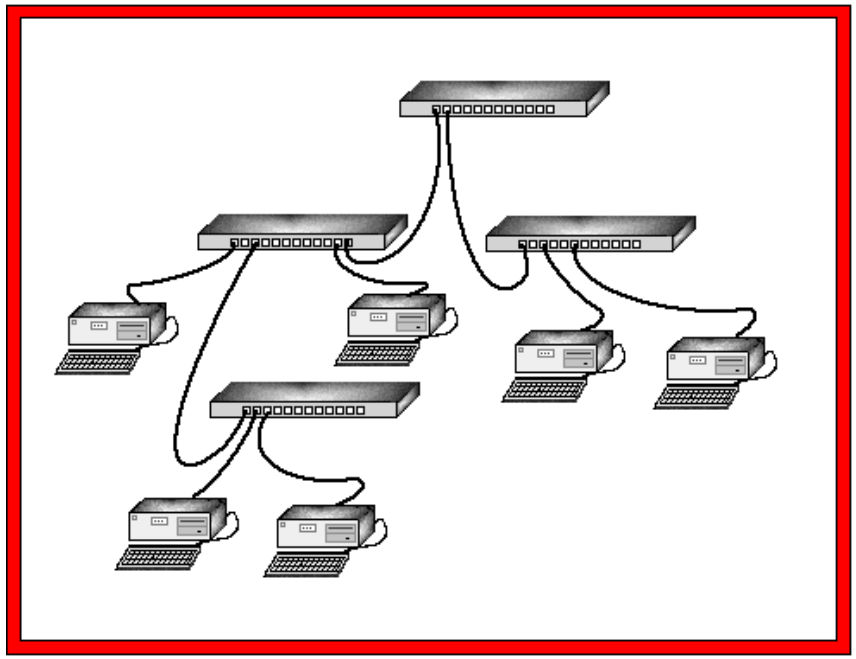


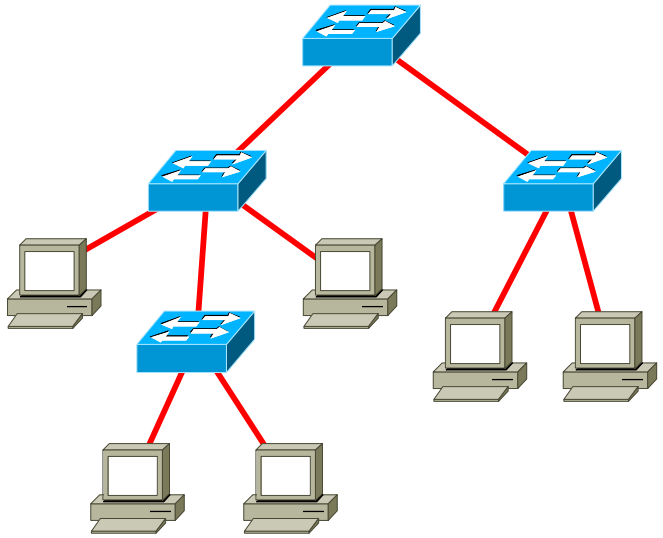



"A star topology connects all cables to a central point of concentration. This point is usually a hub or switch."

# Physical Extended Star Topology



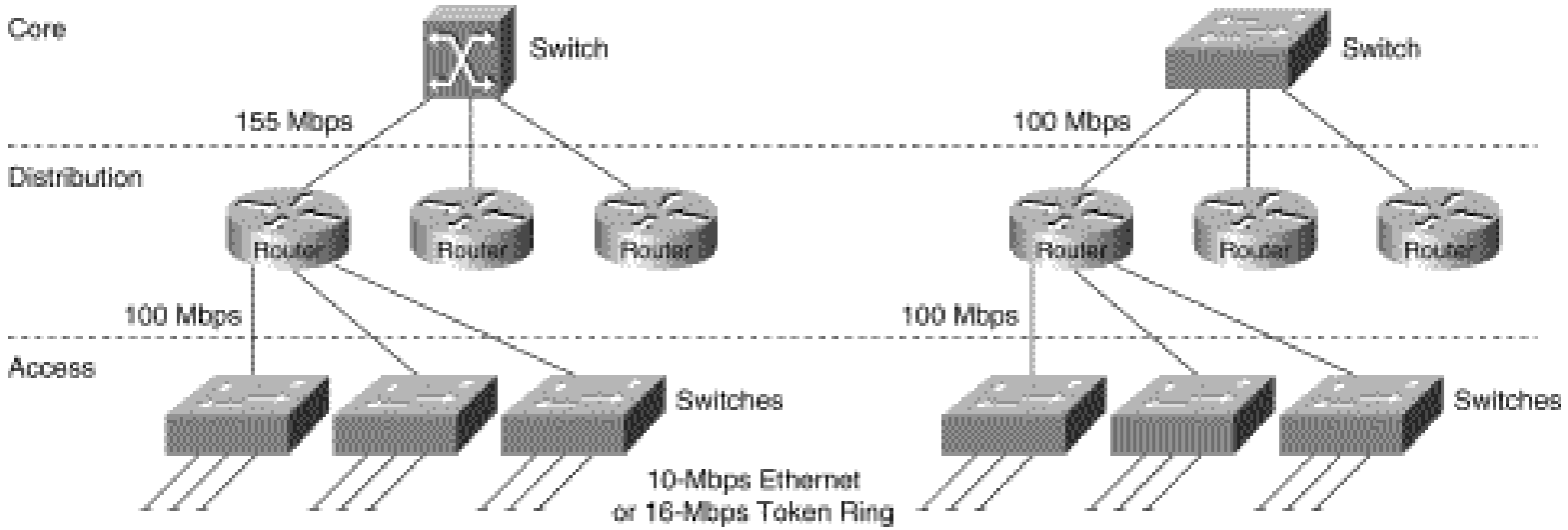




An extended star topology uses the star topology as it´s basis. It links individual stars together by linking the hubs/switches. This extends the length and size of the network. (coming soon)

# Hierarchical Topology

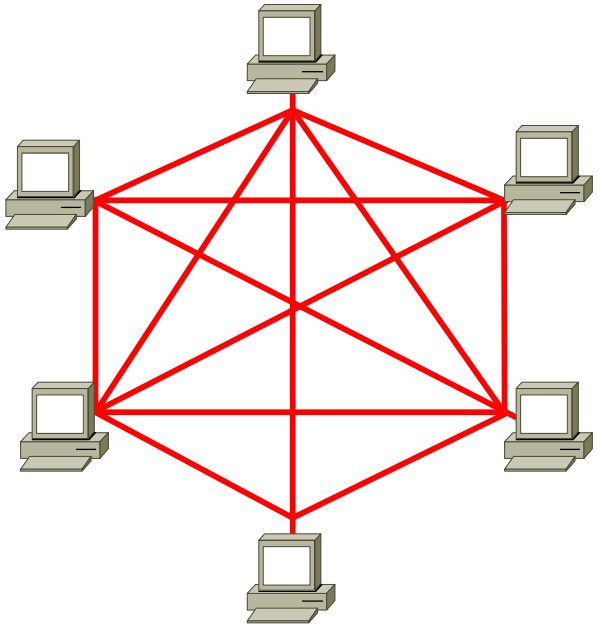





A hierarchical network design or model is one that implements a layered approach to networking.

# Physical Mesh Topology





- "A mesh topology is used when extremely reliable networks with no break in communications are needed, for example the control systems of a nuclear power plant. Each host has its own connections to all other hosts. This also reflects the design of the Internet, which has multiple paths to any one location."
- There are also full mesh and partial mesh topologies, both physical and logical.

# Logical Broadcast Topology



- Signals are transmitted like radio signals. One station transmits, all other listen. The sending stations signal can be heard by all receiving stations at (nearly) the same time.
- Simply means that each host sends its data to all other hosts on the network medium.
- There is no order that the stations must follow to use the network.
- It is first come, first serve.
- Ethernet works this way as will be explained later in the course.

# Logical Token Passing Topology



- Signals are transmitted like parcels by courier service provider who reaches each customer sequentially. Only if the courier is at the customer, customers have access to packets destined for them or they can hand over parcels for transport.
- Controls network access by passing an electronic token (=courier) sequentially to each host (customer).
- When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself.
- Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI).
- A variation of Token Ring and FDDI is Arcnet. Arcnet
  - is token passing on a physical bus topology
  - is an embedded networking technology that is frequently found in applications such as industrial control, building automation, transportation, robotics and gaming.
  - guarantees max. time to access the network. This feature is indispensable with real-time applications
  - see www.arcnet.de , http://www.arcnet.com/ for more details

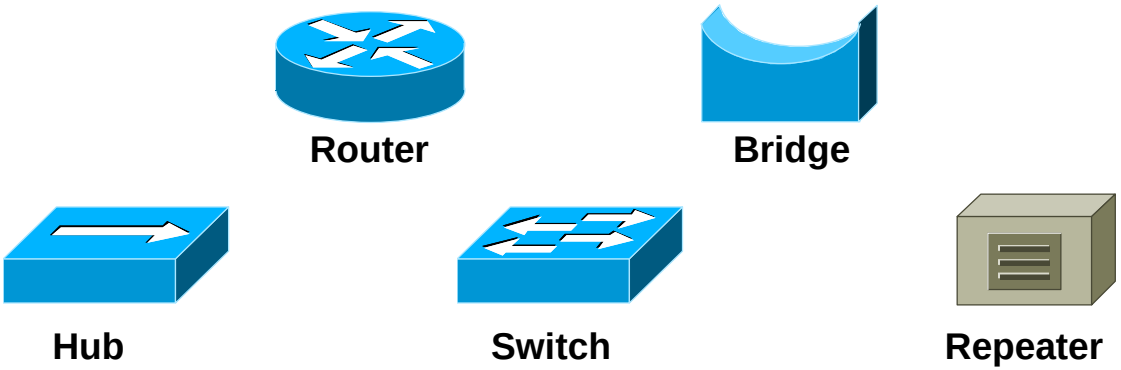
# Local-area networks (LANs)



LANs are designed to

- operate within a limited geographic area (about 2000 m diameter)
- allow multi-access to high bandwidth media
- control the network privately under local administration
- provide full-time connectivity to local services
- connect physically adjacent devices

using:




Some common LAN technologies are:

- Ethernet
- Token Ring
- FDDI
- ARCnet

# Wide-Area Networks (WANs)

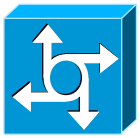


WANs are designed to:

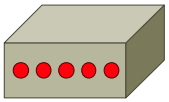
- operate over a large gegraphic area
- allow access over serial interfaces operating at lower speeds
- provide full-time and part-time connectivity
- connect devices separated over wide even global areas

using:

**Router**



**Communication Server**



**Modem CSU/DSU TA/NT1**

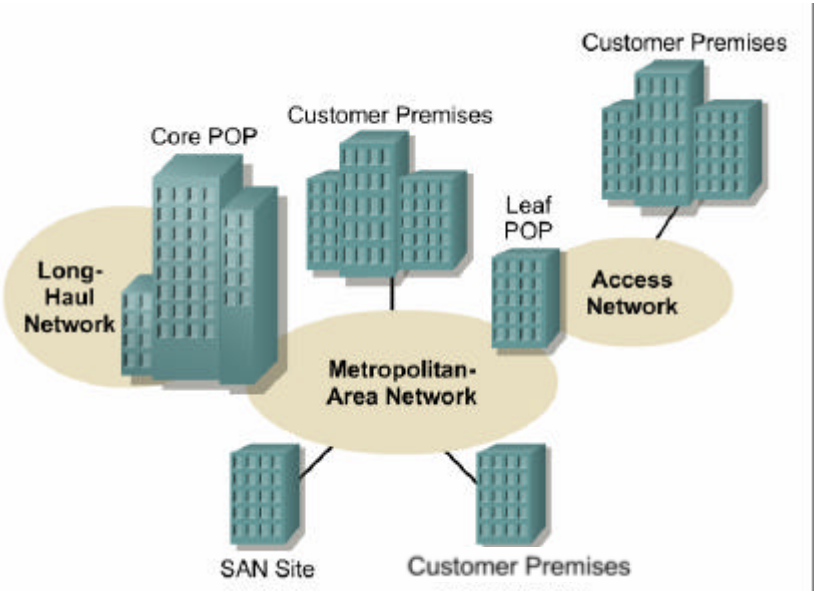
Some common WAN technologies are:

- Modems
- Integrated Services Digital Network (ISDN)
- Digital Subscriber Line (DSL)
- Frame Relay (FR)
- US (T) and Europe (E) Carrier Series – T1, E1, T3, E3
- Synchronous Optical Network (SONET)

# Metropolitan-Area Networks (MANs)



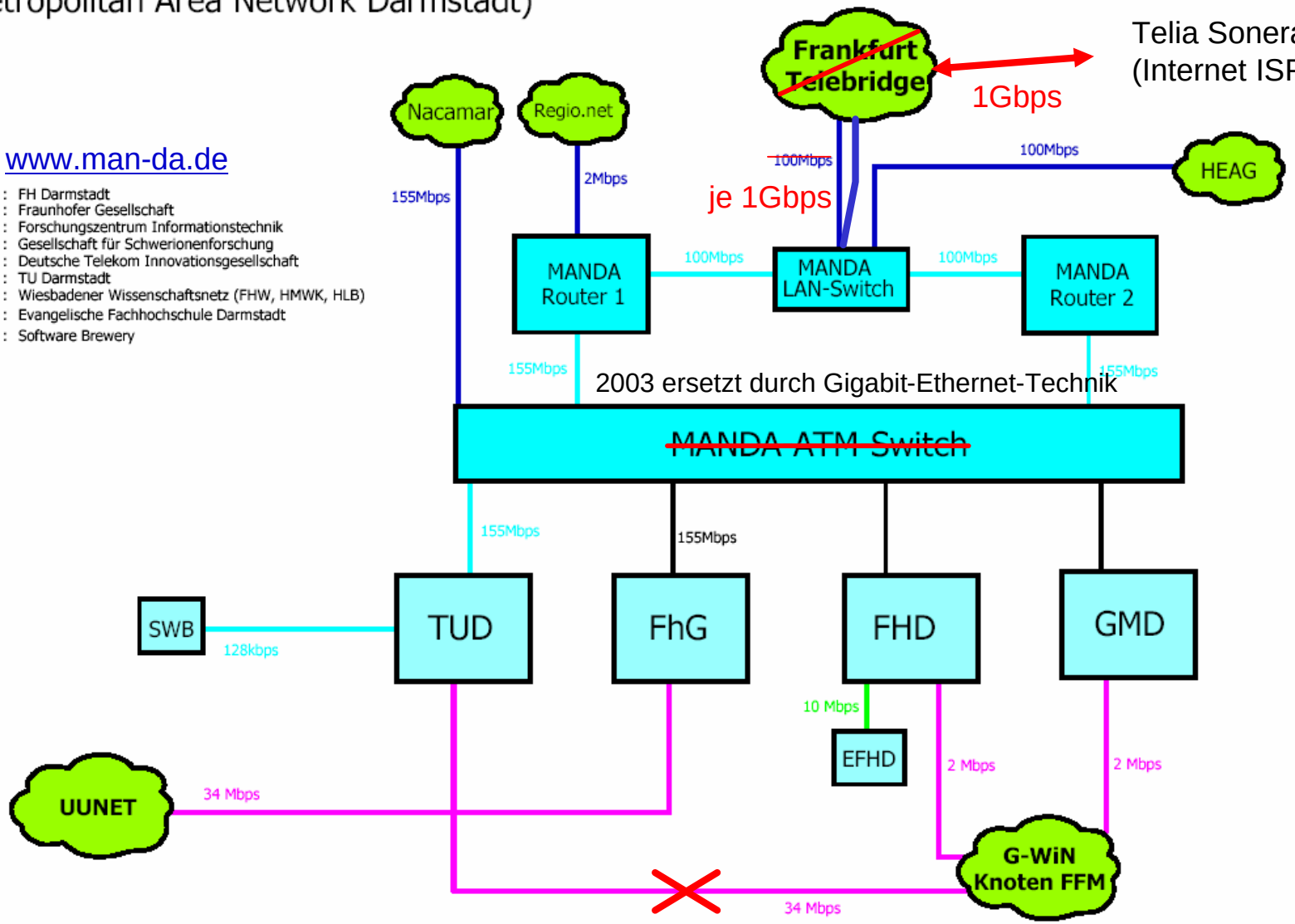
- A MAN is a network that spans a metropolitan area such as a city or suburban area.
- A MAN usually consists of two or more LANs in a common geographic area.
- For example, a bank with multiple branches may utilize a MAN.



# Darmstädter Stadtnetz: MANDA
(Metropolitan Area Network Darmstadt)

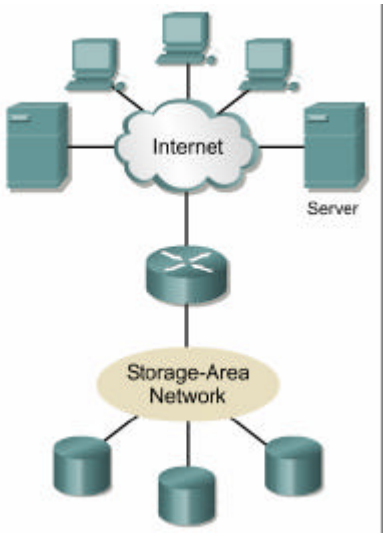
www.man-da.de

| | | |
|---|---|---|
| FHD | : | FH Darmstadt |
| FhG | : | Fraunhofer Gesellschaft |
| GMD | : | Forschungszentrum Informationstechnik |
| GSI | : | Gesellschaft für Schwerionenforschung |
| T-Nova | : | Deutsche Telekom Innovationsgesellschaft |
| TUD | : | TU Darmstadt |
| WWN | : | Wiesbadener Wissenschaftsnetz (FHW, HMWK, HLB) |
| EHFD | : | Evangelische Fachhochschule Darmstadt |
| SWB | : | Software Brewery |



# Storage-Area Networks (SANs)

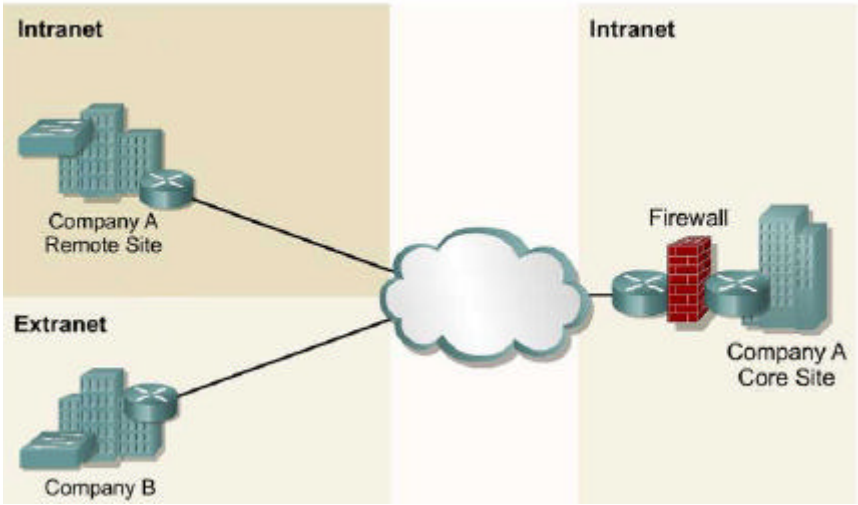





- A SAN is a dedicated, high-performance network used to move data between servers and storage resources.
- SANs offer the following features:
  - **Performance** – SANs enable concurrent access of disk or tape arrays by two or more servers at high speeds.
  - **Availability** – SANs have disaster tolerance built in, because data can be mirrored using a SAN up to 10 kilometers (km) away.
  - **Scalability** – Like a LAN/WAN, it can use a variety of technologies. This allows easy relocation of backup data, operations, file migration, and data replication between systems.

# Intranets and Extranets

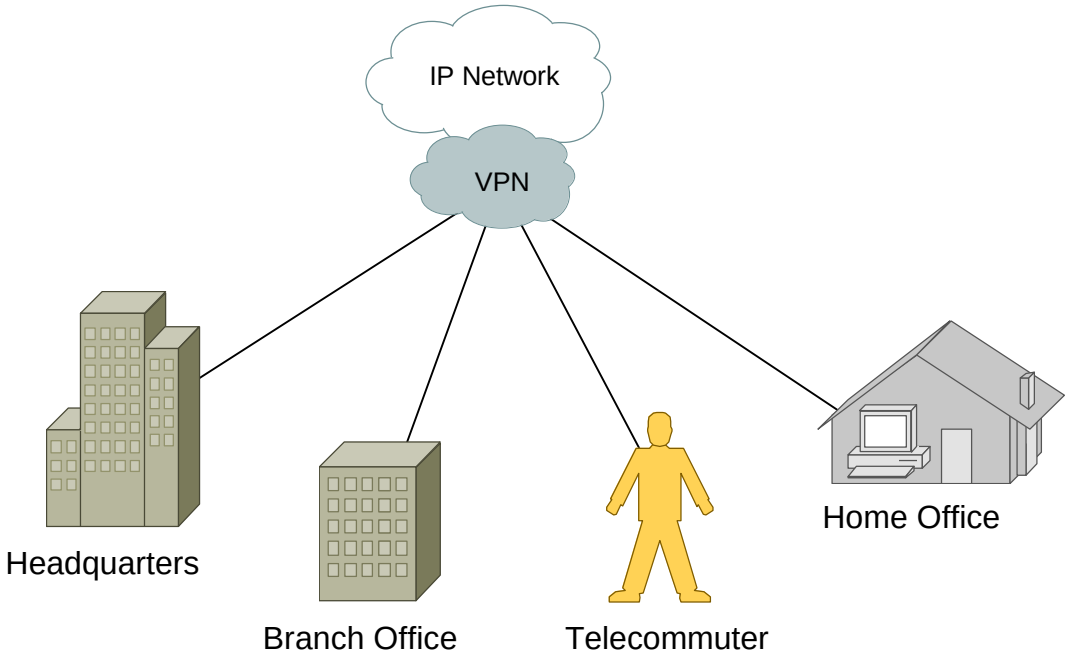





- **Intranets** are designed to permit access by users who have access privileges to the internal LAN of the organization.
- Within an Intranet, Web servers are installed in the network.
- Browser technology is used as the common front end to access information such as financial data or graphical, text-based data stored on those servers.
- **Extranets** refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises.
- This access is usually accomplished through passwords, user IDs, and other application-level security.

# Virtual Private Network (VPN)





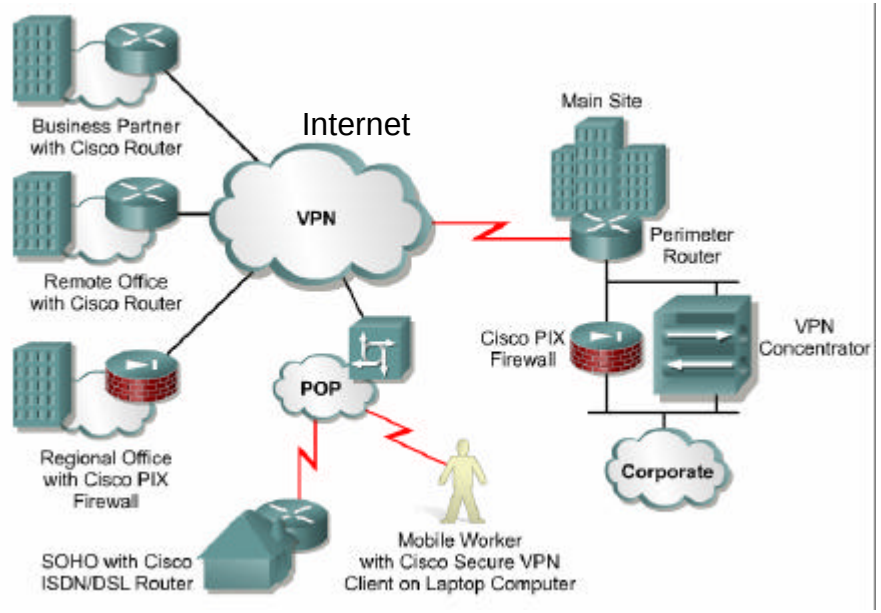

- VPN is a private network that is constructed within a public network infrastructure such as the global Internet.
- Using VPN, a telecommuter can access the network of the company headquarters through the Internet by building a secure tunnel between the telecommuter's PC and a VPN router in the headquarters.
- A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet.

# Types of VPNs



The following are the three main types of VPNs:

- **Access VPNs** – Access VPNs provide remote access to a mobile worker and small office/home office (SOHO) to the headquarters of the Intranet or Extranet over a shared infrastructure.
- **Intranet VPNs** – Intranet VPNs link regional and remote offices to the headquarters of the internal network over a shared infrastructure using dedicated connections. Allow access only to the employees of the enterprise.




- **Extranet VPNs** – Extranet VPNs link business partners to the headquarters of the network over a shared infrastructure using dedicated connections. Allow access to users outside the enterprise.
- Task: Identify the different VPN types in the figure!

- Networking Terminology
- Network metrics
- Network and Protocol Layers

# Nachricht, Daten, Signal



- Nachrichten sind Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen und die vorrangig zum Zweck der Weitergabe als zusammengehörig angesehen und deshalb als Einheit betrachtet werden (DIN 44300 Teil 2).
- Daten sind Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen, vorrangig zum Zweck der Verarbeitung oder als deren Ergebnis (DIN 44300 Teil 2).

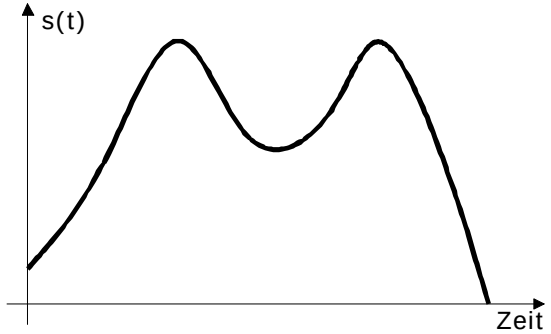
- Ein Signal ist eine Darstellung von Nachrichten oder Daten durch eine zeitveränderliche, physikalische Grösse. Information wird durch einen Parameter dieser Grösse kodiert.

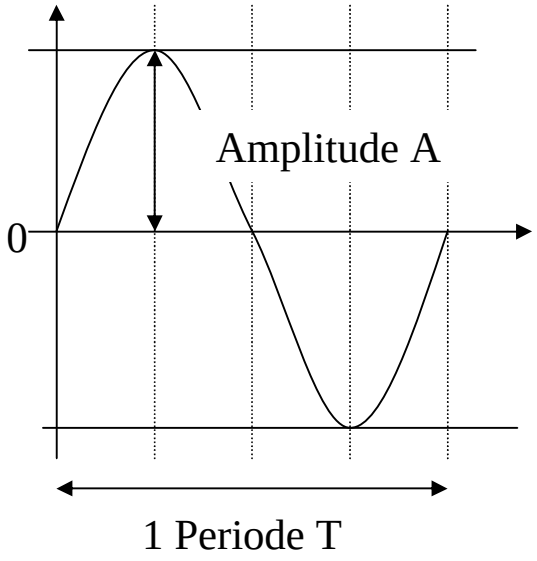
| physikalische Grösse | veränderbarer Parameter |
|---|---|
| Spannung, Strom | Amplitude, Frequenz, Phase |
| Widerstand | Widerstandswert |
| Licht | Intensität |
| ..... | ..... |

# Analoge Signale



- sind zeitkontinuierlich, d.h. sie haben zu jedem Zeitpunkt einen Wert
- sind wertkontinuierlich, d.h. sie können unendlich viele Werte annehmen.
- werden seit den Anfängen der elektrischen Telekommunikation bis heute benutzt
- sind meist wellig: im Bild rechts ist stellvertretend ein sinusförmiges Signal dargestellt. Dieses muss man sich periodisch fortgesetzt vorstellen.




*Frequenz* $f =$

*Anzahl Perioden pro Sekunde*

$$f = \frac{1}{Periode}$$

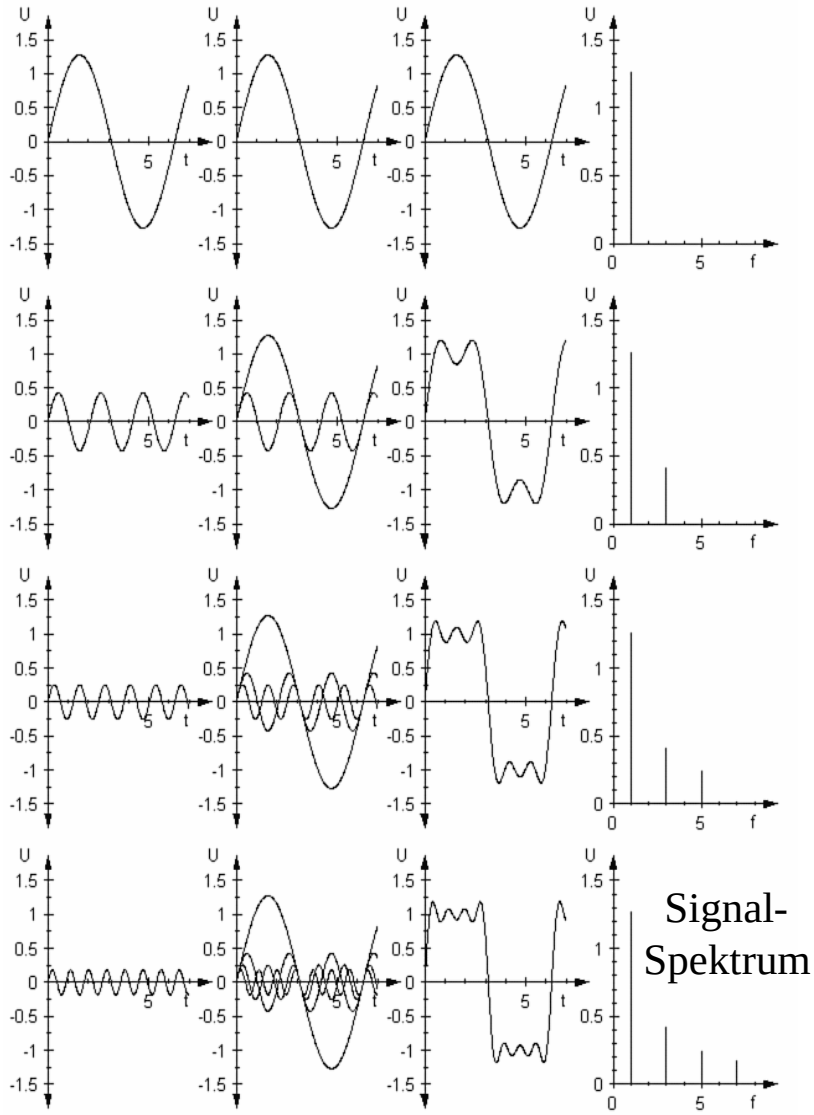
$$f = \frac{1}{T}$$

# Fequenzzusammensetzung von Signalen (Signalspektrum)



- Beliebige Signale bestehen aus summierten Sinussignalen bestimmter Frequenzen und Amplituden.
- Welche Frequenzen und Amplituden dies sind, stellt man durch Fourieranalyse (mathematisches Verfahren) oder mit Hilfe eines Spektrumanalysators (Meßgerät) fest
- Rechts ist dargestellt, wie ein periodisches Rechtecksignal der Frequenz $f_1$ sich aus Sinussignalen der Frequenzen $f_1$, $3f_1$, $5f_1$, $7f_1$, .... zusammensetzt.
- Die Differenz zwischen der höchsten und niedrigsten im Signal enthaltenen Sinus-Frequenz bezeichnet man als Signalbandbreite
- Signale mit Sprüngen (wie beim Rechtecksignal) haben theoretisch eine unendliche Bandbreite.
- Eine Demo in Form eines Java-Applet finden Sie bei

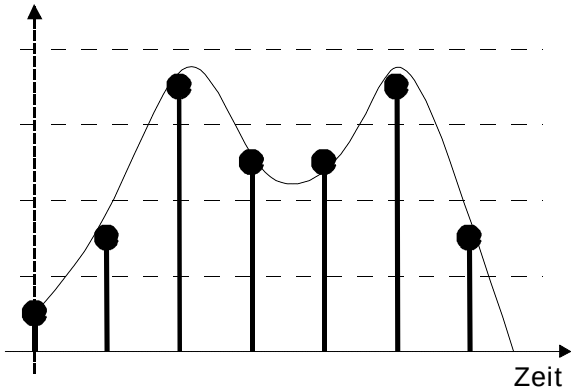
  http://www.fys.kuleuven.ac.be/pradem/laboproeven/sound.html



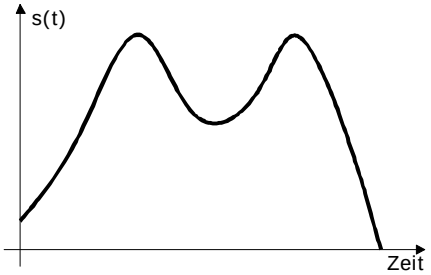
# Digitale Signale



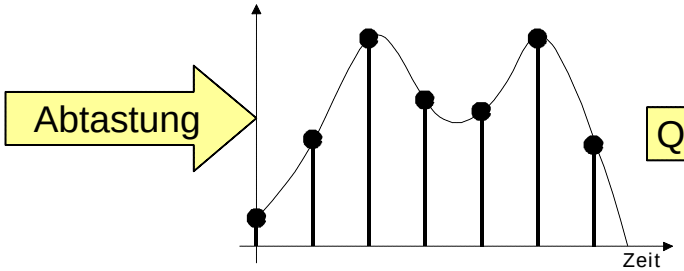
- Sind zeitdiskret, d.h. sie haben zu bestimmten Zeiten einen definierten Wert. Der Standard für Fernsprechsignale sieht 8000 Werte pro Sekunde vor (Audio-CD: 44100 pro Sekunde).
- Sind wertdiskret, d.h. sie können nur bestimmte (also endlich viele) Werte annehmen. Der Standard für Fernsprechsignale sieht 256 Intervalle vor.
- Digitale Signale können aus analogen Signalen entstehen durch Abtastung und Quantisierung. Diesen Vorgang nennt man auch Puls-Code-Modulation (PCM). Die Abtastung ist umkehrbar, wenn die Abtastfrequenz mehr als doppelt so groß wie die max. Signalfrequenz ist (Abtasttheorem von Shannon). Bei der Umkehrung der Quantisierung durch Glättung bleibt ein Quantisierungsgeräusch.



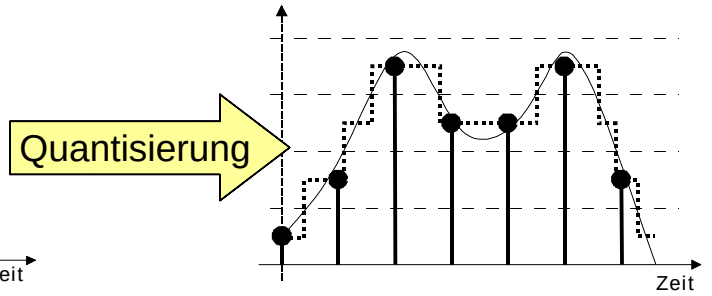

Digitales Signal




Analoges Signal




$f_A \geq 2 \times f_{Smax}$



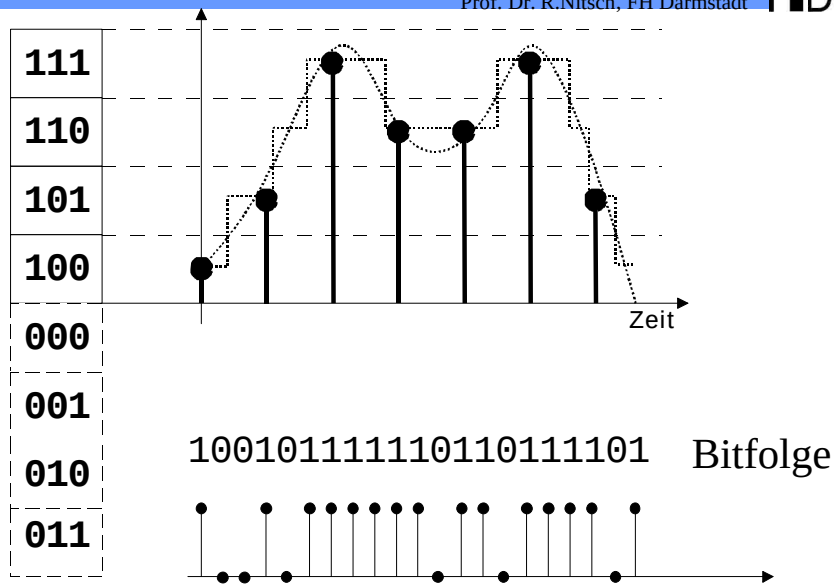

Digitales Signal
8-wertig

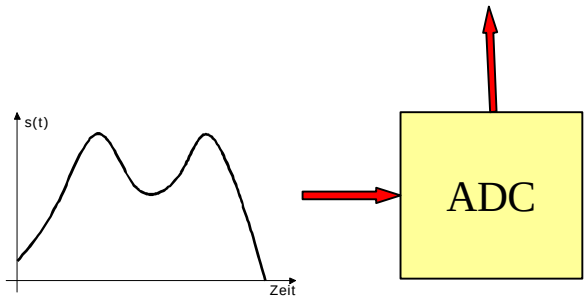
# Binäre Codierung analoger Signale



- Jedem Werteintervall eines m-wertigen Signals kann man binäre Codeworte zuordnen (Beispiel siehe Abbildung). Dadurch entsteht ein binäres Signal. Die Stellen eines binären Codewortes haben nur zwei Werte (0 oder 1; deshalb „binär“). Man bezeichnet sie als Bit. Mit 3-Bit-Codeworten können $m=2^3=8$ Quantisierungsintervalle codiert werden.
- Abtaster, Quantisierer und Codierer sind heute meist in einem Analog-Digital-Wandler (ADC) integriert. Den Vorgang der Analog-Digital-Wandlung bezeichnet man auch als Puls-Code-Modulation (PCM).
- **Fragen**:
  1. Wieviele Bits hat ein Codewort für die Codierung eines Fernsprechsignales?
  2. Wieviele Bits pro Sekunde liefert ein Codierer für ein Fernsprechsigal.

  (Fernsprechsignal: 0,3...3,4 kHz)

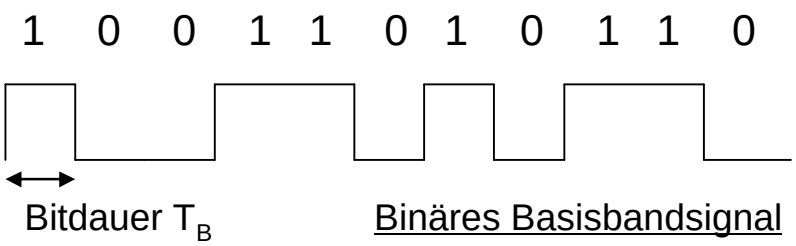


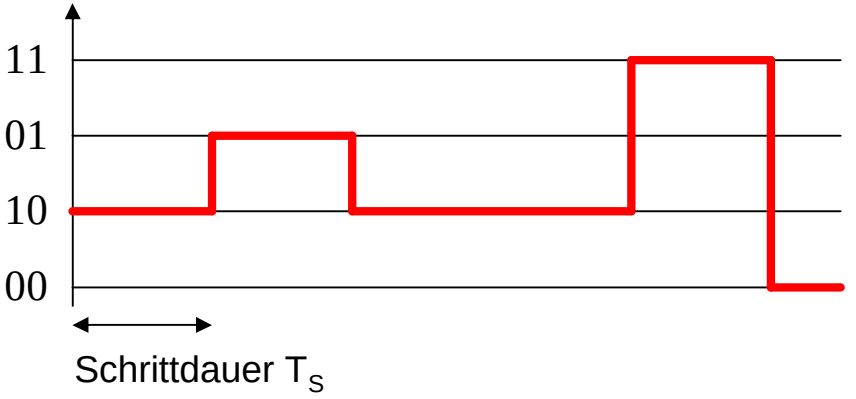
# Digitalsignalübertragung - Begriffe



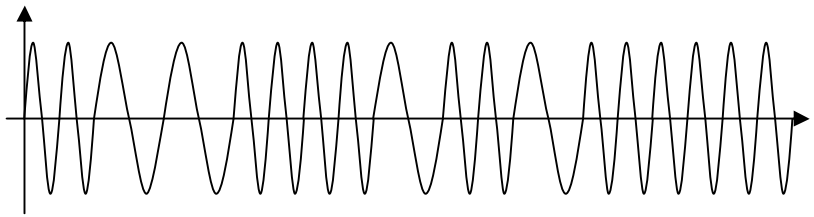
- In Datennetzen werden Bitfolgen (= binäre Digitalsignale) mit **Basisbandverfahren** oder **Bandpassverfahren** (=Breitbandverfahren) übertragen.
- Im **Basisbandverfahren** werden die Bitfolgen lediglich codiert (Leitungscodierung), um sie den Bandbreiteeigenschaften der Übertragungsleitung möglichst gut anzupassen (**Bandbreiteökonomie**) und gute Übertragungsergebnisse bei geringstem Aufwand im Empfänger zu erzielen.
- Im **Bandpassverfahren** wird zusätzlich eine **Modulation** verwendet, um die Sendesignale in den Übertagungsfrequenzbereich des Übertragungsweges zu verschieben (z.B. Funkstrecke)
- Die **Bitdauer** ist die Zeit, die für die Übertragung eines Bits benötigt wird.
- Die **Schrittdauer** ist die Zeit, während der sich die vom Signal getragene Information nicht ändert.




Binäres Basisbandsignal




Quaternäres Basisbandsignal




Bandpasssignal

# Digitalsignalübertragung - Begriffe



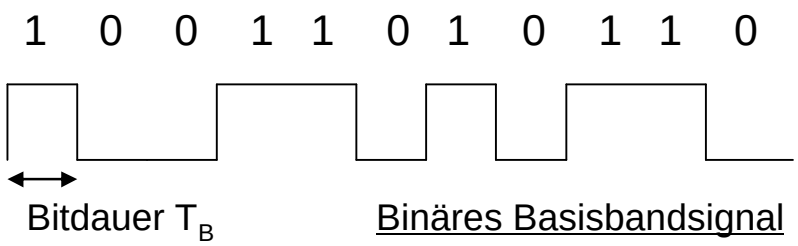
- **Schrittdauer** $T_S$ ist die Zeit, während der sich die vom Signal getragene Information nicht ändert. Ihr Kehrwert wird als **Schrittrate** bezeichnet und in Baud (Baudot: franz. Mathematiker) gemessen.

$$Schrittrate\ r_S = \frac{1}{Schrittdauer\ T_S}$$

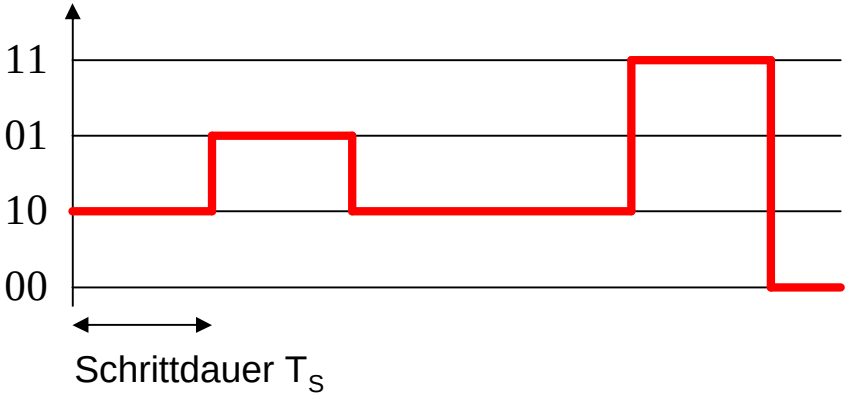
- **Bitdauer** ist die Zeit, die für die Übertragung eines Bits benötigt wird. Ihr Kehrwert wird als **Bitrate** bezeichnet und in bit/s gemessen.

$$Bitrate\ \ r_B = \frac{1}{Bitdauer\ \ T_B}$$

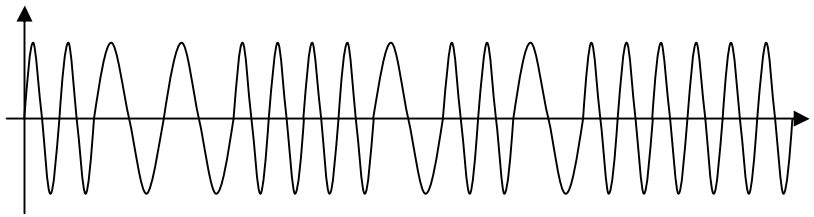
- Die Codierung der Bitfolge in ein m-wertiges Signal (m>2) reduziert die Schrittrate und damit die benötigte Frequenzbandbreite.




Binäres Basisbandsignal




Quaternäres Basisbandsignal



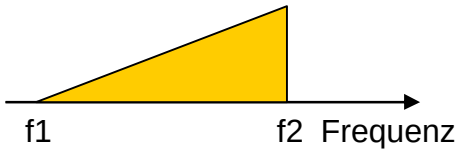

Bandpasssignal

# Leistungsmaße eines Netzwerks

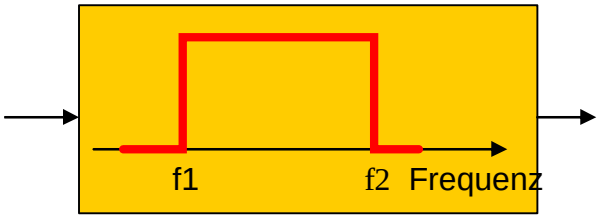


- Bandbreite (bandwidth)
- Latenz (latency)
- Latenz-Bandbreite-Produkt
- Durchsatz (throughput)
- Jitter (jitter)

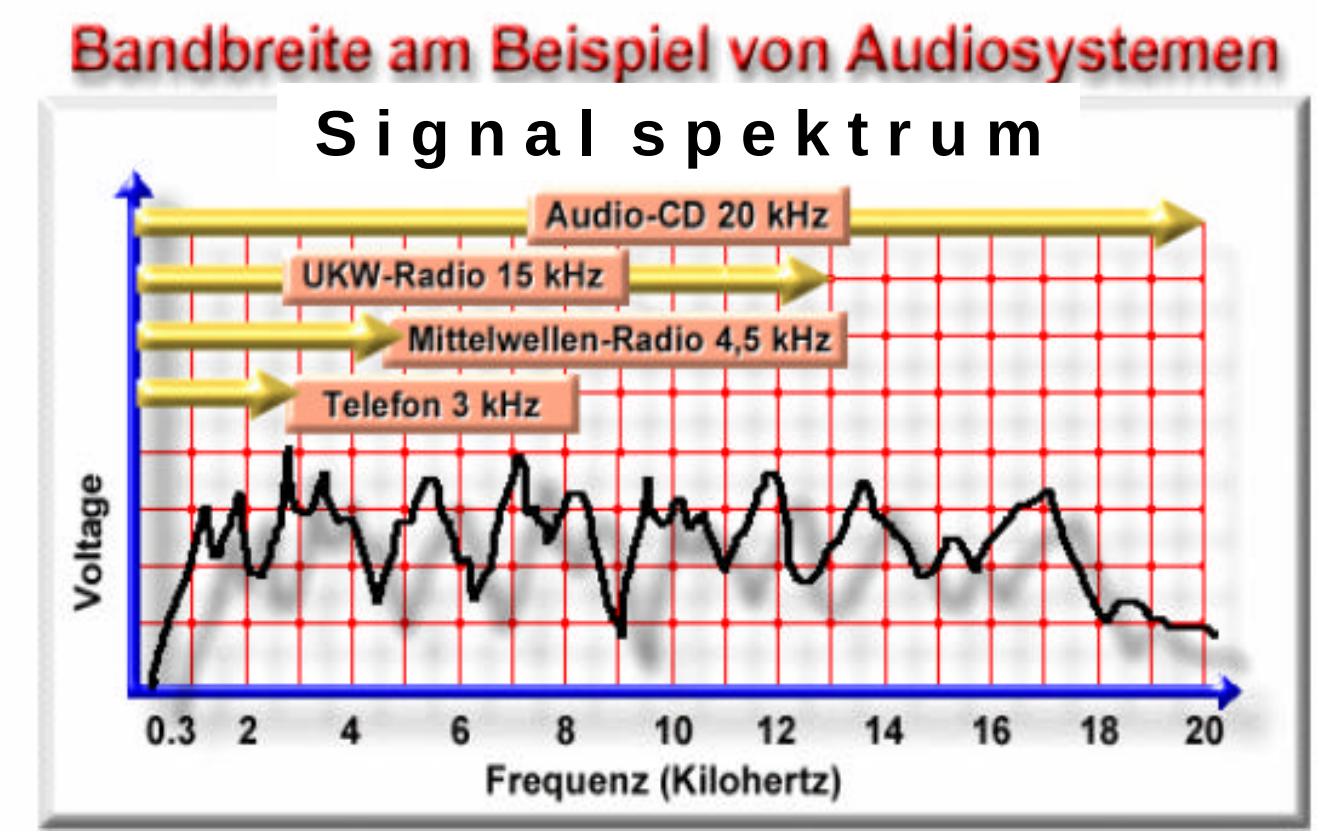
- Beim Signal:
  Bandbreite gibt die Breite des Frequenzbandes in Hertz (Hz) an, die das Frequenzgemisch eines Signals enthält (cycles per second, cps)
- Beim Übertragungskanal:
  Bandbreite gibt die Breite des Frequenzbandes in Hertz (Hz) an, das vom Kanal übertragen werden kann
- Beim Datenübertragungskanal:
  Bandbreite gibt die Anzahl der Bits pro Sekunde (bit/s) an, die der Kanal maximal übertragen kann (bits per second, bps)
  (Beispiel: 10 Mbit/s bei 10BaseT-Ethernet)
- Merkmale:
  - Bandbreite ist teuer
  - Bandbreite ist begrenzt durch Naturgesetze und die verwendete Technologie




Bandbreite = f2 – f1




Bandbreite = f2 – f1


Bandbreite am Beispiel von Audiosystemen
Signal spektrum
Audio-CD 20 kHz
UKW-Radio 15 kHz
Mittelwellen-Radio 4,5 kHz
Telefon 3 kHz
Voltage
0.3 2 4 6 8 10 12 14 16 18 20
Frequenz (Kilohertz)

# Leistungsmaße eines Netzwerks



- Bandbreite (bandwidth)
- Latenz (latency)
- Latenz-Bandbreite-Produkt
- Durchsatz (throughput)
- Jitter (jitter)

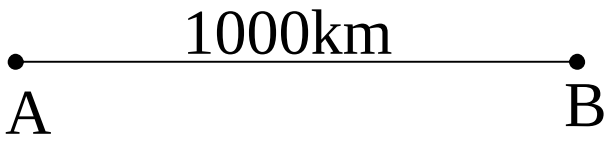
# Leistungsmaße eines Netzwerks - Latenz



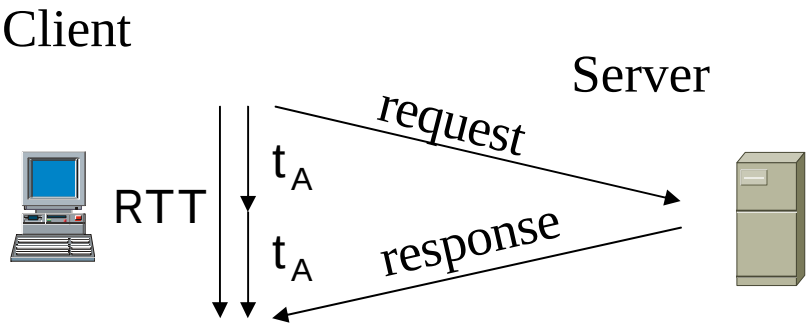
- Latenz (latency) ist die Zeitdauer, die ein Paket benötigt um von einem Ende des Netzwerks/Kanals zum anderen zu gelangen
- Latenz setzt sich aus 3 Komponenten zusammen

1. Ausbreitungsdauer: verursacht durch endliche Signalgeschwindigkeit

| c: Lichtgeschwindigkeit | |
|---|---|
| $c = 3 \cdot 10^8 m/s$ | im Vakuum |
| $c = 2{,}3 \cdot 10^8 m/s$ | im Kabel |
| $c = 2 \cdot 10^8 m/s$ | im LWL |




$$t_A = \frac{s}{c} = \frac{1000 \cdot 10^3 m}{2 \cdot 10^8 m/s} = 5ms$$




Round Trip Time (RTT):

$RTT = 2 \cdot t_A$

2. Übertragungsdauer: wird zum Senden des Pakets benötigt

**Beispiel:** Bandbreite B = 100 Mbit/s

1Bit wird gesendet in $\frac{1}{B} = \frac{1}{10^8} s = 10ns$

1Byte wird gesendet in $10ns \cdot 8 = 80ns$

1 Paket (1500 Byte) wird gesendet in $1500 \cdot 80ns = 120ms$

3. Wartezeit: ergibt sich als Summe aller Wartezeiten in den Sendepuffern aller Netzknoten

Zusammenfassung: $Latenz = Ausbreitungsdauer + Übertragungsdauer + Wartezeit$

$$Ausbreitungsdauer = \frac{Entfernung}{Ausbreitungsgeschwindigkeit}$$

$$Übertragungsdauer = \frac{Paketgröße\ in\ bit}{Bandbreite\ in\ bit/s}$$

**Konsequenz:** Auch bei Hochgeschwindigkeitsnetzen (Bandbreite $\rightarrow \infty$) ist die Latenz nie kürzer als die Ausbreitungsdauer.

## Relative Bedeutung von Ausbreitungs- und Übertragungsdauer

- Hängt ab von der Anwendung: Bei manchen Anwendungen ist Ausbreitungsdauer dominanter als Übertragungsdauer und umgekehrt
- **Beispiel:** Anfrage-Antwort-Kanal (1 Paket der Größe x wird übertragen (Anfrage) und danach vom Empfänger quittiert (Antwort))

| RTT (ms) | Paketgröße x | Bandbreite (Mbit/s) | Latenz | Bemerkung |
|---|---|---|---|---|
| 100 | 100 Byte | 10 | 50ms+80µs | Ausbreitungsdauer dominiert |
| 1 | 100 Byte | 10 | 0,5ms+80µs | |
| 100 | 100 Byte | 100 | 50ms+8µs | |
| 1 | 100 Byte | 100 | 0,5ms+8µs | |

| RTT (ms) | Paketgröße x | Bandbreite (Mbit/s) | Latenz | Bemerkung |
|---|---|---|---|---|
| 100 | 25 MByte | 10 | 50ms+20s | Bandbreite dominiert |
| 1 | 25 MByte | 10 | 0,5ms+ 20s | |
| 100 | 25 MByte | 100 | 50ms+ 2s | |
| 1 | 25 MByte | 100 | 0,5ms+ 2s | |

# Zusammenfassung

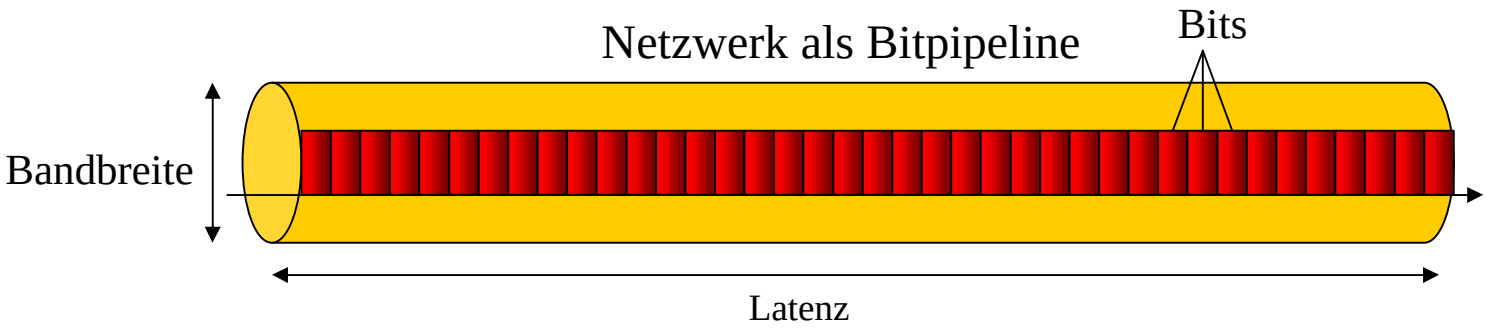
- Übertragung kleiner Pakete ist Entfernungs-bestimmt,
  die Übertragung großer Pakete ist Bandbreite-bestimmt.
- Bandbreite
  - Ist begrenzt
  - Ist bares Geld Wert
  - Ist ein wichtiger Maßstab für die Netzwerkleistung
  - Ist eine wichtige Größe für das Netzdesign
  - Jeder will mehr davon haben

# Leistungsmaße eines Netzwerks



- Bandbreite (bandwidth)
- Latenz (latency)
- Latenz-Bandbreite-Produkt
  Durchsatz (throughput)
- Jitter (jitter)

- Gibt an, wieviele Bits ein Sender senden muss, bevor das erste Bit den Empfänger erreicht
- Gibt auch an, wieviel Bit gleichzeitig im Übertragungskanal gespeichert sind




- **Beispiel:** 34-Mbit/s-Kanal mit RTT = 100 ms

  Latenz-Bandbreite-Produkt = $50 \cdot 10^{-3}$s · $34 \cdot 10^{6}$bit/s = 1,7 Mbit = 207,5 kByte

  **Konsequenz:** Wenn der Empfänger den Sender wegen Überlastung auffordert, das Senden einzustellen, muss der Empfänger noch mindestens ___ kByte empfangen!

- Der Durchsatz berücksichtigt, dass ein Datenpaket erst erfolgreich übertragen ist, wenn der Sender vom Empfänger eine Erfolgsmeldung erhält:

$$\text{Durchsatz } D = \frac{\text{Paketgröße } L}{\text{Pakettransferzeit}} = \frac{L}{RTT + L/B^{1)}}$$

Pakettransferzeit = RTT + Übertragungszeit + Wartezeit (≅ 2-Weg-Latenz)

- **Beispiel:** Hochgeschwindigkeitsnetz mit Bandbreite B=1 Gbit/s,
  RTT = 100ms, Datenpaketgröße 1 MByte, Wartezeit vernachlässigbar

$$Pakettransferzeit = 100ms + \frac{2^{20} \cdot 8\,\text{bit}}{10^9\,bit/s} = 100ms + 8{,}4ms = 108{,}4ms$$

$$Durchsatz = \frac{2^{20} \cdot 8\,\text{bit}}{0{,}1084\,s} = 77{,}4\,\frac{Mbit}{s} << 1Gbit/s$$

1) Wartezeit vernachlässigt

Konsequenzen:

- Die Bandbreite gibt die maximal übertragbaren, der Durchsatz die tatsächlich (im Mittel) auf der Verbindungsleitung übertragenen Bits pro Sekunde an

$$\text{Durchsatz} \leq \text{Bandbreite}$$

- Der Quotient Durchsatz/Bandbreite ist ein Maß für für die Effizienz, mit der die Bandbreite des Netzwerks genutzt wird:

$$Effizienz = \frac{D}{B} = \frac{L}{L + RTT \cdot B}$$

- Damit die Bandbreite von Hochgeschwindigkeitsnetzen auch tatsächlich effizient ausgenutzt werden kann, muss die Paketgröße ausreichend groß sein!

$$\lim_{L \to \infty} Effizienz = \lim_{L \to \infty} \frac{L}{RTT \cdot B + L} = 1$$

- ➢ Damit Hochgeschwindigkeitsnetze bandbreite-begrenzt sind müssen sie eine ausreichend bemessene Paketgröße haben.
- ➢ Aber: Bei Übertragungsfehlern müssen diese großen Pakete erneut übertragen werden.

# Leistungsmaße eines Netzwerks



- Gründe für Reduzierung des Durchsatzes
  - Anfrage-Antwort-Kanal
  - Andere Benutzer im LAN / Tageszeit
  - Routing innerhalb der Wolke
  - Aufbau (Topologie) aller beteiligten Netzwerke
  - Typ der übertragenen Daten

# Leistungsmaße eines Netzwerks

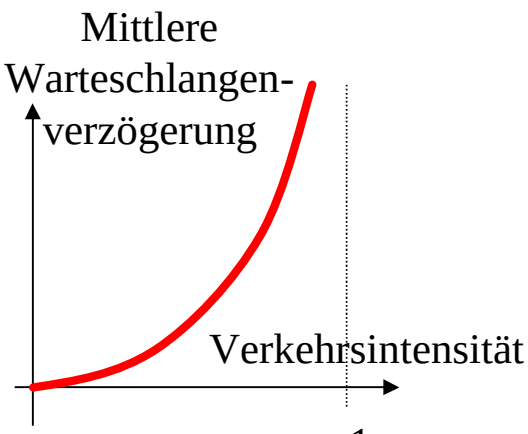


- Bandbreite (bandwidth)
- Latenz (latency)
- Latenz-Bandbreite-Produkt
  Durchsatz (throughput)
- Jitter (jitter)

# Leistungsmaße eines Netzwerks - Wartezeitverzögerung



- Ist die komplizierteste und interessanteste Komponente der Knotenverzögerung
- Sie kann im Gegensatz zu den anderen Verzögerungen stark schwanken (**Jitter**). Kommen z.B. fünf Pakete gleichzeitig in einen leeren Sendepuffer (Warteschlange), muss das erste Paket gar nicht, das letzte vier Übertragungszeiten warten.
- Werden deshalb durch **statistische Parameter** charakterisiert: Durchschnittliche Wartezeit, Abweichung vom Durchschnitt,...
- Die Bitrate **r** eines Links ist die Rate, mit der Bits aus seinem Sendepuffer entnommen werden. Wenn **a** Pakete pro Sekunde in den Puffer hineingeschoben werden und jedes Paket aus **L** Bit besteht so ist **L·a** die mittlere Empfangsbitrate. Die Größe **L·a/r** wird als **Verkehrsintensität** bezeichnet.
- Wenn **L·a/r > 1**: Die Warteschlange und mit ihr die Warteschlangenverzögerung wächst grenzenlos.
- Wenn der Puffer voll ist, werden weitere Pakete verworfen (**Datenverlust**). Der Vermittler bzw. das Netz ist überlastet. Verlorene Pakete müssen erneut übertragen werden. Durch **Überlastkontrolle** müssen solche Situationen möglichst erkannt und vermieden werden.




Wozu segmentieren? →

# Wartezeitverzögerung



Wenn die Verkehrsintensität **L·a/r ≤ 1** und

- die Pakete kommen periodisch an: → keine Wartezeitverzögerung
- die Pakete kommen zufällig an. → stark schwankende Wartezeitverzögerung

Designregel:
Systeme sollten so entworfen werden, dass die Verkehrsintensität nicht größer als eins ist.

- Wenn die Verkehrsintensität (temporär) > 1 ist liegt eine Überlastsituation (congestion) vor. Durch geeignete Abwehrmassnahmen (congestion control) kann man verhindern, dass Pakete verloren gehen.
- TCP verfügt über einen solchen Mechanismus, allerdings nur auf Ende-zu-Ende-Basis.

# What is Bandwidth?



**Why bandwidth is important:**

- Bandwidth is limited by physics and technology
- Bandwidth is not free
- Bandwidth requirements are growing at a rapid rate
- Bandwidth is critical to network performance

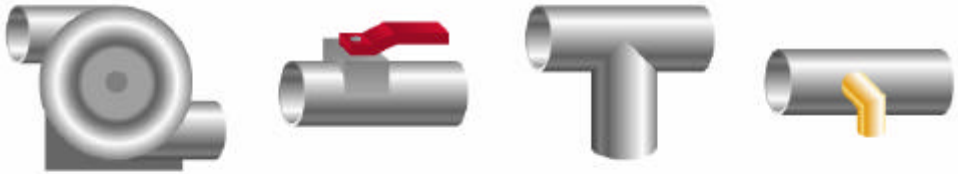
1. Analog bandwidth: A range within a band of frequencies or wavelengths.
   - For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).
2. Digital bandwidth: The amount of data that can be transmitted through a network connection in a fixed amount of time.
   - For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second.

# Analogies for Bandwidth



Bandwidth is like the width of a pipe.

Network devices are like pumps, valves, fittings, and taps.



Packets are like water.

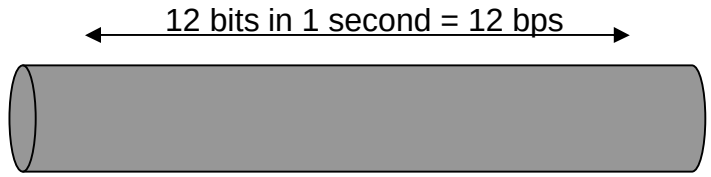
Bandwidth is like the number of lanes on a highway.

Network devices are like on-ramps, traffic signals, signs, and maps.


Packets are like vehicles.

# Measurement of Digital Bandwidth






- In digital systems, the basic unit of bandwidth is bits per second (bps).
- Bandwidths of standarydized data communication channels widely used all over the world
  - T-1 -> 1544 kbps
  - E-1 -> 2048 kbps

| Unit of Bandwidth | Abbreviation | Equivalence |
|---|---|---|
| Bits per second | bps | 1 bps = fundamental unit of bandwidth |
| Kilobits per second | kbps | 1 kbps = ~1,000 bps = $10^3$ bps |
| Megabits per second | Mbps | 1 Mbps = ~1,000,000 bps = $10^6$ bps |
| Gigabits per second | Gbps | 1 Gbps = ~1,000,000,000 bps = $10^9$ bps |
| Terabits per second | Tbps | 1 Tbps = ~1,000,000,000,000 bps = $10^{12}$ bps |

# Digital Bandwidth Limitations



| Typical Media<br>Ethernet | Maximum Theoretical Bandwidth | Maximum Theoretical Distance |
|---|---|---|
| 50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet) | 10 Mbps | 185 m |
| 50-Ohm Coaxial Cable (10BASE5 Ethernet; Thicknet) | 10 Mbps | 500 m |
| Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet) | 10 Mbps | 100 m |
| Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet) | 100 Mbps | 100 m |
| Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet) | 1000 Mbps | 100 m |
| Multimode Optical Fiber (62.5/125mm) (100BASE-FX Ethernet) | 100 Mbps | 2000 m |
| Multimode Optical Fiber (62.5/125mm) (1000BASE-SX Ethernet) | 1000 Mbps | 220 m |
| Multimode Optical Fiber (50/125mm) (1000BASE-SX Ethernet) | 1000 Mbps | 550 m |
| Singlemode Optical Fiber (9/125mm) (1000BASE-LX Ethernet) | 1000 Mbps | 5000 m |

| WAN Service | Typical User | Bandwidth |
|---|---|---|
| Modem | Individuals | 56 kbps = 0.056 Mbps |
| DSL | Individuals, telecommuters, and small businesses | 128 kbps to 6.1 Mbps = 0.128 Mbps to 6.1 Mbps |
| ISDN | Telecommuters and small businesses | 128 kbps = 0.128 Mbps |
| Frame Relay | Small institutions (schools) and reliable WANs | 56 kbps to 44.736 Mbps (U.S.) or 34.368 Mbps (Europe) = 0.056 Mbps to 44.736 Mbps (U.S.) or 34.368 Mbps (Europe) |
| T1 | Larger entities | 1.544 Mbps |
| E1 | Larger entities | 2.048 Mbps |
| T3 | Larger entities | 44.736 Mbps |
| E3 | Larger entities | 34.368 Mbps |
| STS-1 (OC-1) | Phone companies; Data-Comm company backbones | 51.840 Mbps |
| STM-1 | Phone companies; Data-Comm company backbones | 155.52 Mbps |
| STS-3 (OC-3) | Phone companies; Data-Comm company backbones | 155.251 Mbps |
| STM-3 | Phone companies; Data-Comm company backbones | 466.56 Mbps |
| STS-48 (OC-48) STM-16 | Phone companies; Data-Comm company backbones | 2.488320 Gbps |

- Bandwidth varies with the type of media as well as with the LAN and WAN technologies used.
- The physics of the media responsible for some of the difference.
- Common transmission media are twisted-pair copper wire, coaxial cable, optical fiber, and air.
- The actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for accessing the media and detecting network signals.

# Throughput and Digital Bandwidth



Throughput ≤ Digital Bandwidth of a Medium

- Throughput refers to actual measured bandwidth, at a specific time of day, using specific Internet routes, and while a specific set of data is transmitted on the network.
- Throughput is often far less than the maximum possible digital bandwidth of the medium that is being used.

The following are some of the factors that determine throughput:

- User computer
- Server computer
- Number of users on the network/time of day
- Communication rules (protocol)
- Type of data being transferred
- Network topology
- Power conditions

# Data Transfer Calculation



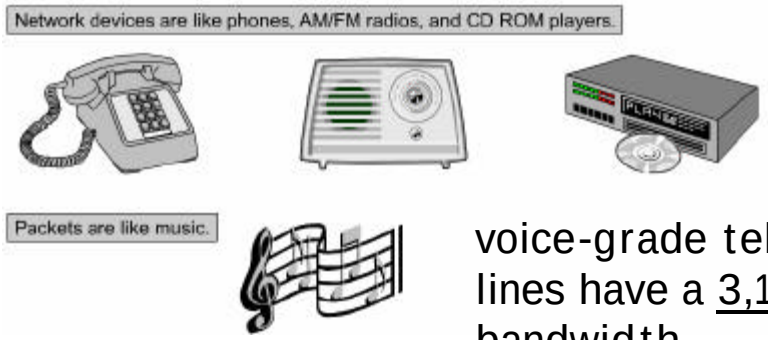
| Best Download | Typical Download |
|---|---|
| $T = \frac{S}{BW}$ | $T = \frac{S}{P}$ |

| | |
|---|---|
| BW | Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host bps |
| P | Actual throughput at the moment of transfer im bps |
| T | Time for file transfer to occur (in seconds) |
| S | File size in bits |

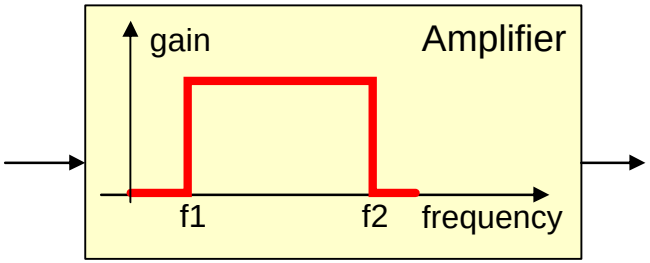
- Using the formula *transfer time = size of file / bandwidth (T=S/BW)* allows a network administrator to estimate the fastest time that the file can be transferred.
- Exercise: What time is needed to transfer a 5-GB-file with 768 kbps?

# Digital versus Analog






voice-grade telephone lines have a 3,100 Hz bandwidth

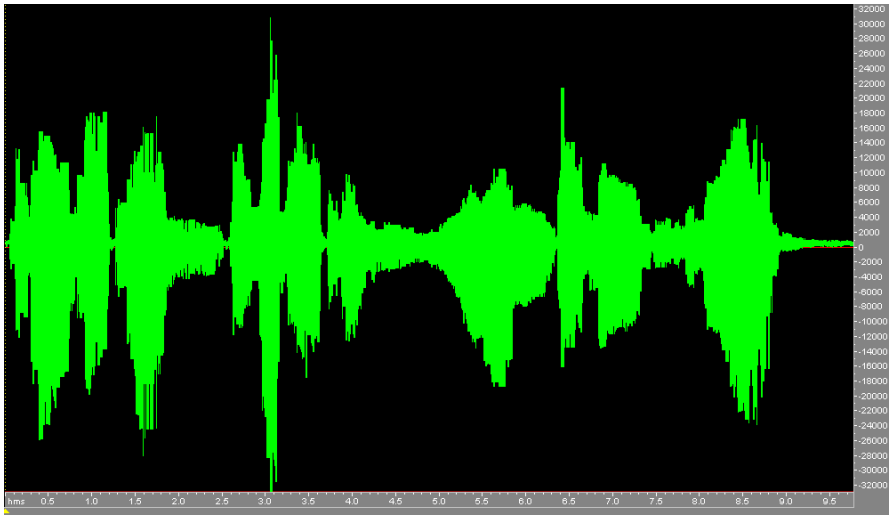



bandwidth = $f_2 - f_1$

- Analog bandwidth is measured by how much of the electromagnetic spectrum is occupied by each signal.
- The basic unit of analog bandwidth is hertz (Hz), or cycles per second.
- While analog signals are capable of carrying a variety of information, they have some significant disadvantages in comparison to digital signals:
  - Digital and analog signals are attenuated when traveling through a transmission media which means their amplitude decrease with increasing distance from the transmitter. Thereby the allways present noise on transmission media becomes a problem.
  - Analog signal must be amplified before their amplitude becomes too low but the accompanying noise is amplified too.
  - Digital signals need no amplification but a decision wether a "1" or a "0" was transmitted and the detected information can be transmitted further, freed from the received noise.

# Sound Waves



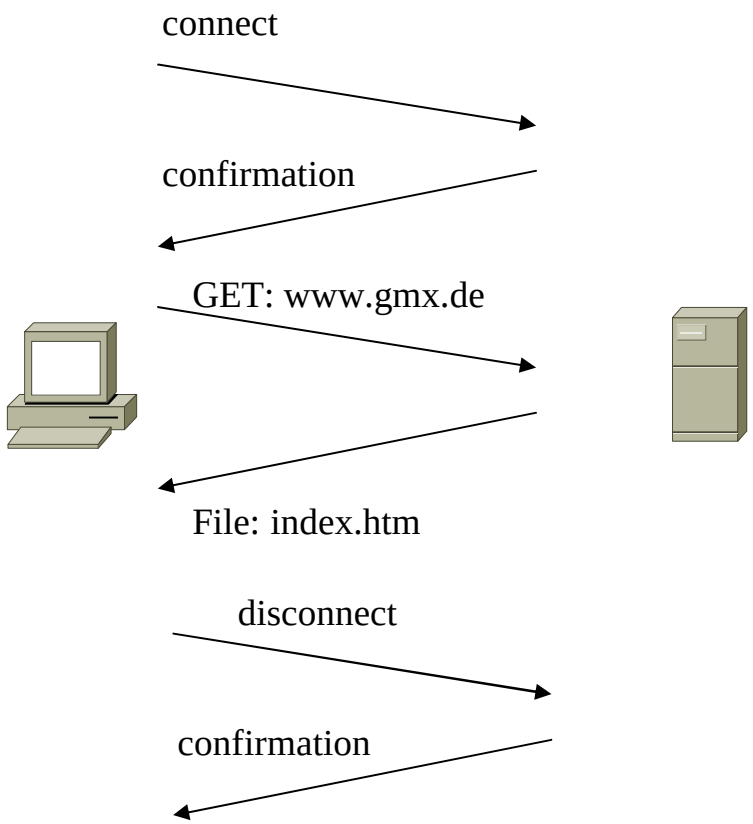

32000
30000
28000
26000
24000
22000
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
-2000
-4000
-6000
-8000
-10000
-12000
-14000
-16000
-18000
-20000
-22000
-24000
-26000
-28000
-30000
-32000
hms 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0 5.5 6.0 6.5 7.0 7.5 8.0 8.5 9.0 9.5

- Networking Terminology
- Network metrics
- Network and Protocol Layers

# Communication needs rules



- In order for data packets to travel from a source to a destination on a network, it is important that all the devices on the network speak the same language or protocol.
- A protocol is a set of rules and conventions that
  - make communication on a network possible and efficient.
  - govern a particular aspect of how devices on a network communicate.
  - determine the format, transmission, timing, sequencing, and error control of data
- Protocol suites are collections of protocols that enable network communication from one host through the network to another host.
- Without protocols, the computer cannot make or rebuild the stream of incoming bits from another computer into the original format.



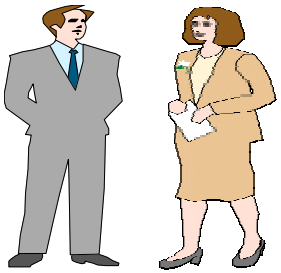
# Network Protocols

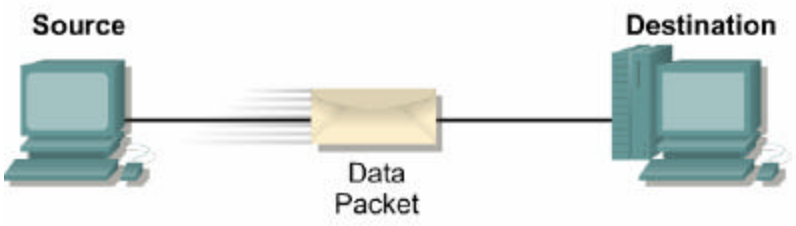


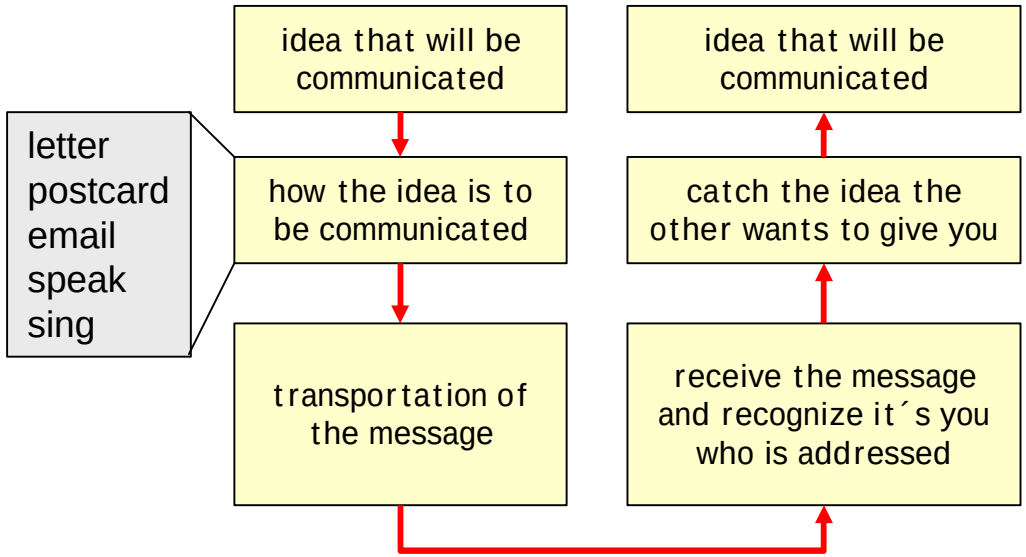
- Protocols control all aspects of data communication, which include the following:
  - How the physical network is built (Topology)
  - How computers connect to the network (Media Access)
  - How the data is formatted for transmission (PDU structures)
  - How that data is sent (Signal formats)
  - How to deal with errors (Error recovery)
- In order to fullfill it´s purpose protocols need standardization.
- Protocol standardization is done by a lot of international recognized standardization bodies. Important examples are
  - International Organization for Standardization (ISO, www.iso.ch )
  - International Telecommunications Union (ITU, www.itu.int ), formerly known as the Comité Consultatif International Téléphonique et Télégraphique (CCITT).
  - Institute of Electrical and Electronic Engineers (IEEE, www.ieee.org ),
  - European Telecommunications Standards Institute (ETSI, www.etsi.org )
  - American National Standards Institute (ANSI, www.ansi.org ),
  - Electronic Industries Alliance (EIA, www.eia.org )
  - Telecommunications Industry Association (TIA, www.tia.org ),

# Concept of Layers





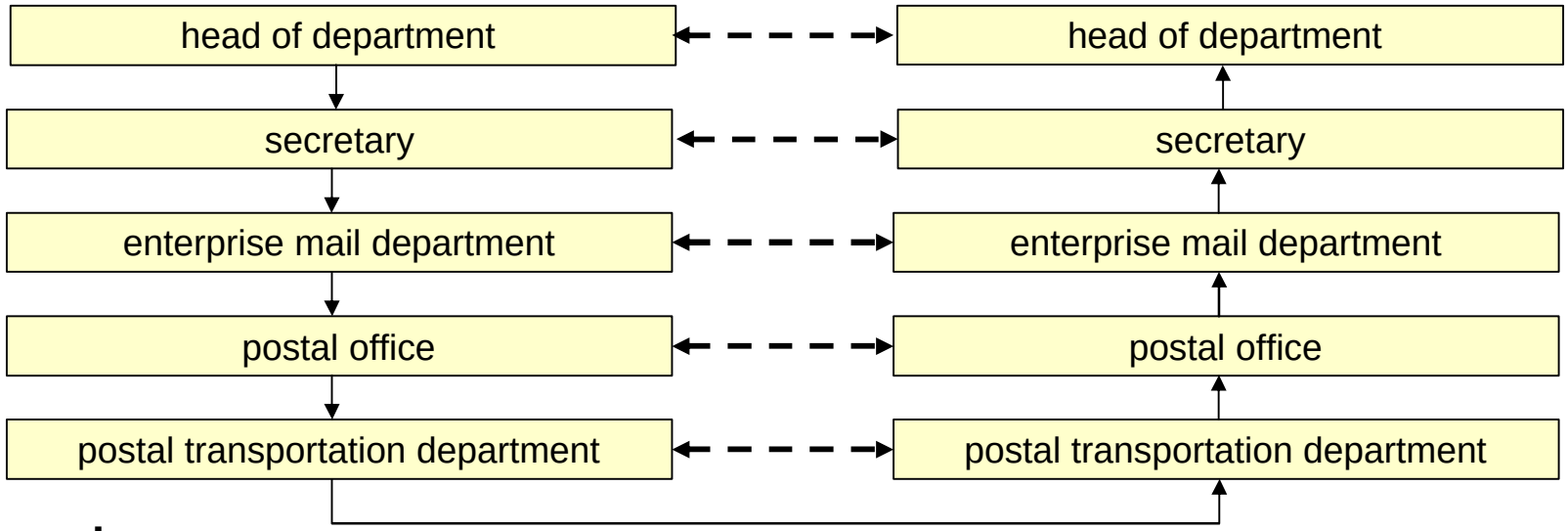



- The concept of layers is used to describe communication from one computer to another.
- The OSI and TCP/IP models have layers that explain how data is communicated from one computer to another.
- The models differ in the number and function of the layers.
- However, each model can be used to help describe and provide details about the flow of information from a source to a destination.

# Example: Layered Communication by Written Letter






**Remarks**:

- Each layer has it's own rules and activities
- Upper layers use and rely on the services of the lower layers
- Lower layers offer services to the upper layers
- Large and complex system is divided into well-defined decoupled parts
- Layer implementation may change as long as the offered/used services remain the same
- Source layers and equivalent dstination layers (peers) exchange special control information
  - Geschäftszeichen, Bearbeiterkürzel, Datum, Anlagenverzeichnis, Absender- und Empfängeradresse, PLZ
  - Briefmarke, Poststempel, Bearbeitungsvermerke (Einschreiben, Luftpost,...)

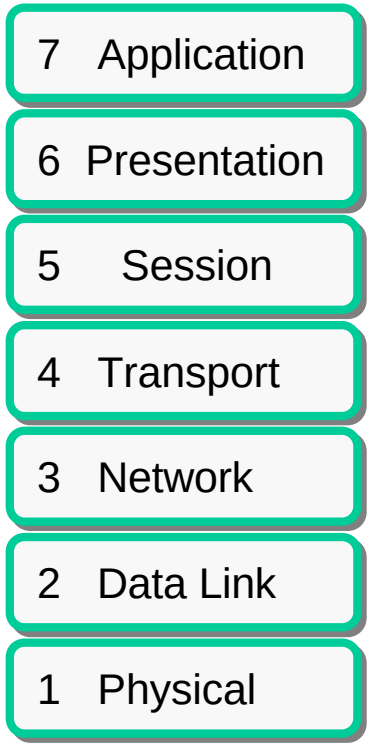
# 7-Layer OSI model



- Addresses the problem of network incompatibility
- Is structured into seven numbered layers, each of which illustrates a particular network function.

**History**

- Is the result of comparative research on network models like Digital Equipment Corporation net (DECnet), Systems Network Architecture (SNA), and TCP/IP in order to find a generally applicable set of rules for all networks.
- Using this research, the ISO created a network model that helps vendors create networks that are compatible with other networks.
- Released by the International Organization for Standardization (ISO) in 1984

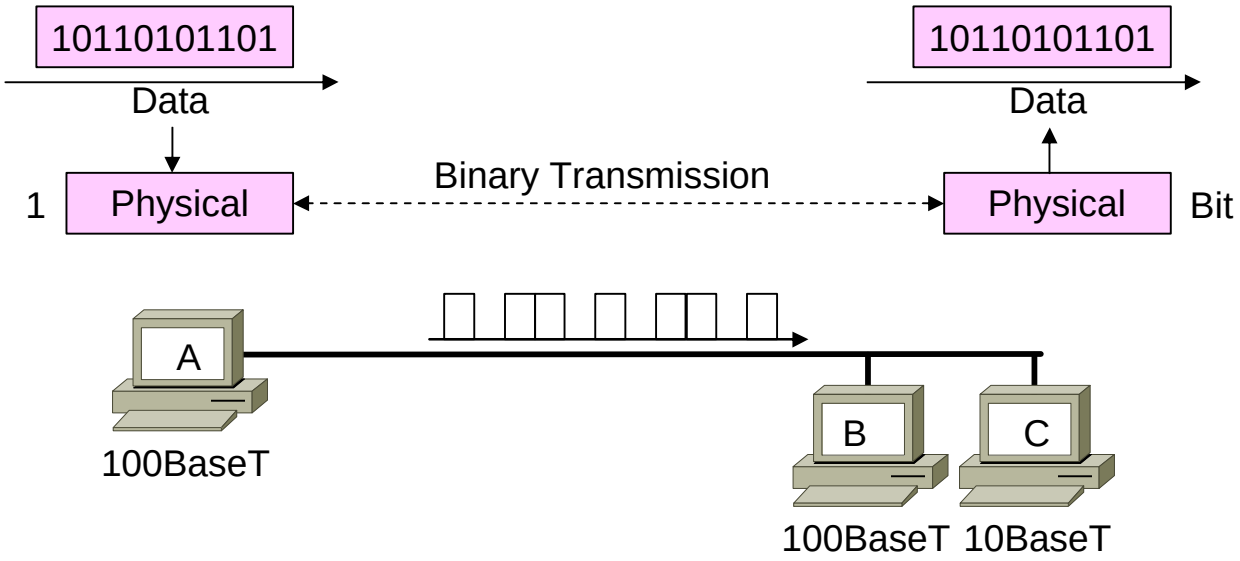


# Layer 1 - Physical (Physikalische Schicht)



**The Physical Layer is concerned with Binary Transmission:**

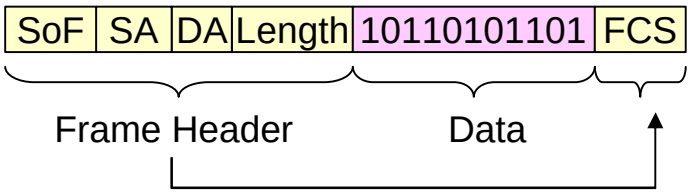
- connectors
- voltages
- data rates
- transmission media
- digital signal regeneration



# Layer 2 - Data Link (Sicherungsschicht)

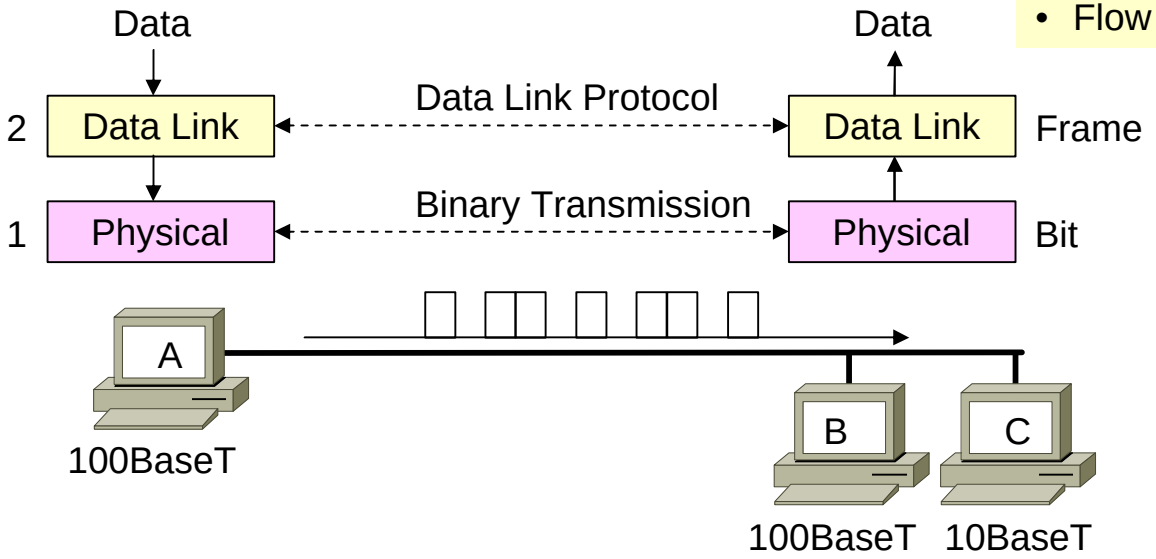


**Frame structure**




**Data Link Layer is concerned with:**

- Media Access
- Physical addressing (SA, DA)
- Put structure on bit stream (Frame format)
- Frame recognition (SoF)
- Reliable data transfer
- Network topology
- Error notification (FCS)
- Flow control




**Problems with growing LAN s**

- Physical distance
- Congestion
- Locality (limited distance)
- Scalability
- Laming broadcast traffic

- To manage broadcast traffic and other scaling challenges, another kind of boundary is necessary.
- A way to create populations of networks within a larger network (Internetwork) is also needed.
- The device that makes internetworks possible is a **router**.

**SA**: Source Address
**DA**: Destination Address
**SoF**: Start of Frame
**FCS**: frame Check Sequence
**IP**: Internet Protocol
**IPX**:
**ARP**: Address Resolution Protocol

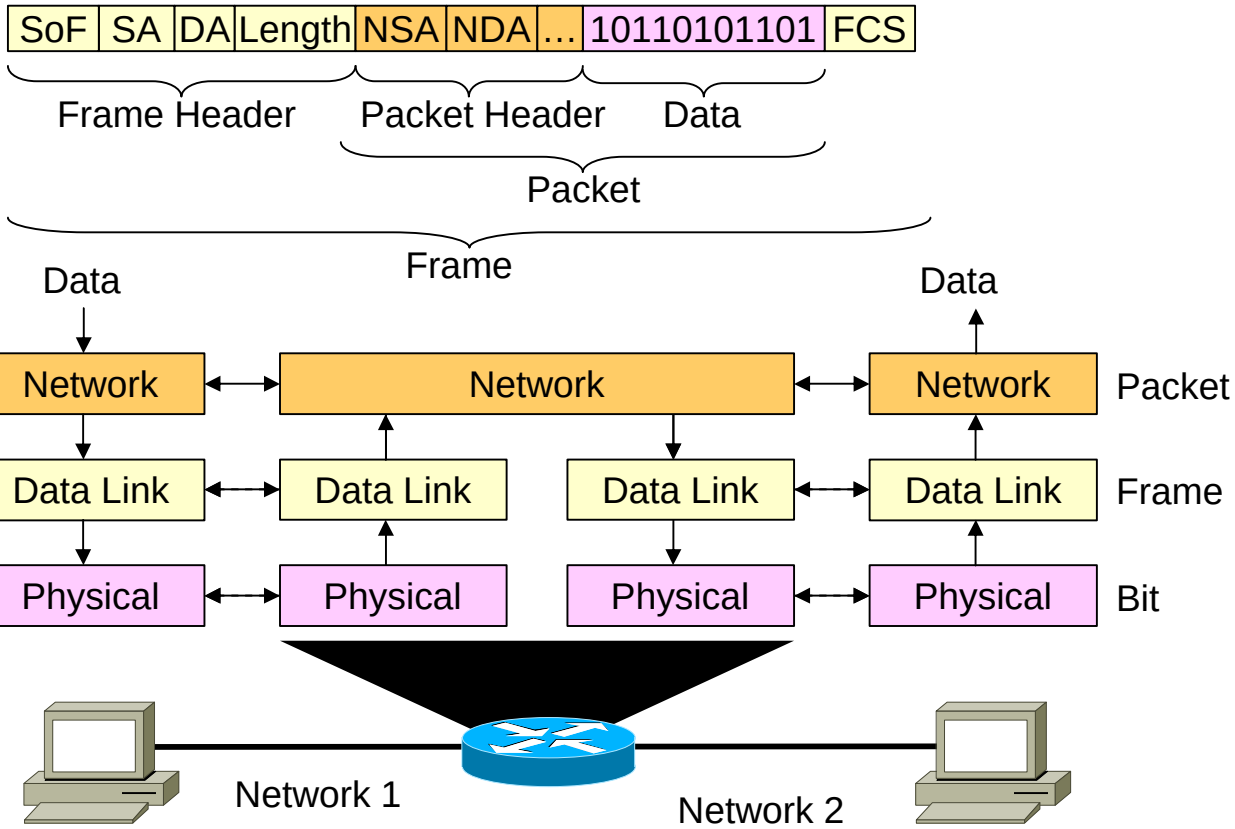
# Layer 3 - Network (Vermittlungsschicht)



**The network layer is concerned with**

- providing logical communication and path selection between 2 hosts
- network address
- best path determination (Routing protocols)
- packet forwarding between 2 networks (Routed protocols)

**Packet structure**

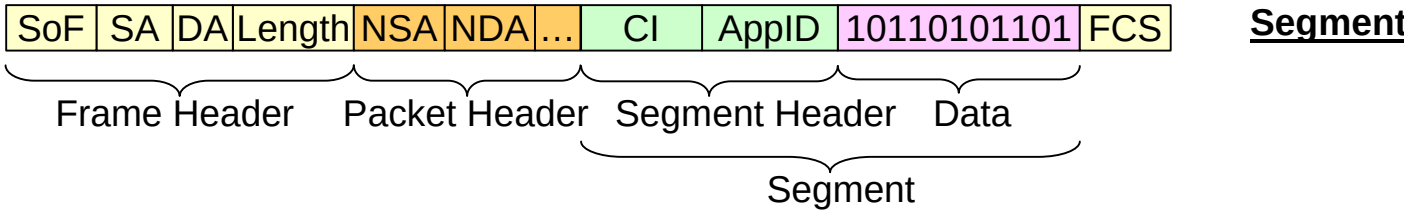


# Layer 4 - Transport

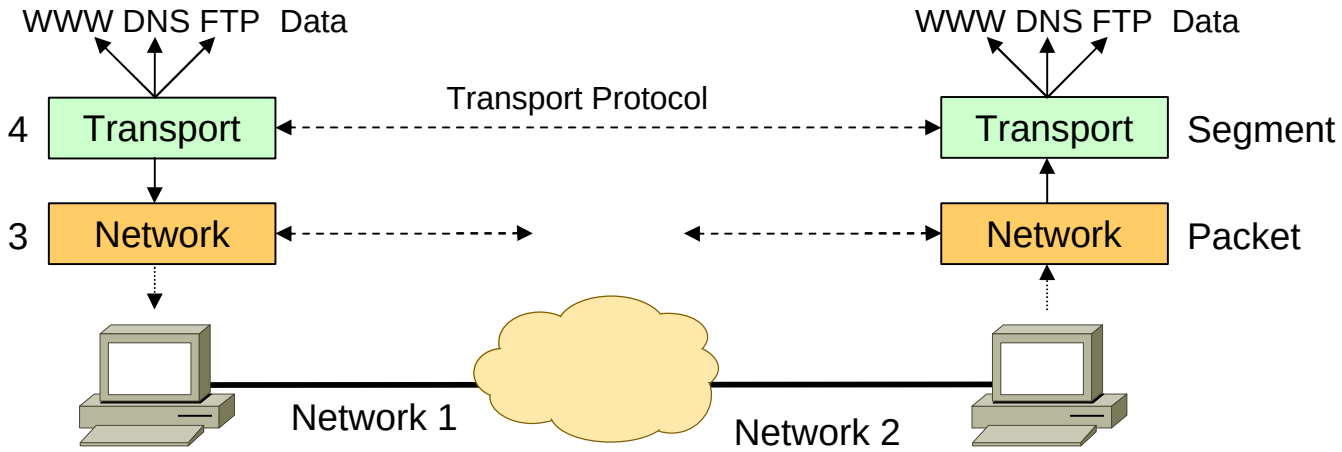


Transport layer protocols

- are implemented in end systems but not in intermediate systems such as routers
- provides for logical communication between application processes running on different hosts
- breaks the application messages into smaller chunks at the sending side and reassembles the messages at the receiving side (segmentation)
- adds information about the sending application in the 4-PDU and processes this infomation at the receiving endstation (Application multiplexing/demultiplexing)
- may implement an connection-oriented service if the lower network layer offers only best-effort service (reliable transmission).
- may implement end-to-end error detection, error recovery and flow control




**Segment structure**



# Layers 5 - 6 - 7



**Layer 5 - Session Layer** (Sitzungsschicht)

- establishes, manages and terminates sessions between applications
- tries to recover the connection in case of a connection loss
- may close down and re-open a connection for next use if it is not used for a longer period
- Organizes and manages one or more connections per application (Web-browser: html, jpg, .wav).
- manages buffer memories and memory swapping
- provides synchronization points in the stream of exchanged packets

**Layer 6 - Presentation Layer** (Darstellungsschicht)

- provides independence from differences in data representation by translating from application to network format, and vice versa.
- negotiates data transfer form that the application layer can accept to ensure that data is readable by receiving system
- negotiates data compression if demanded
- negotiates data encryption/decryption if demanded

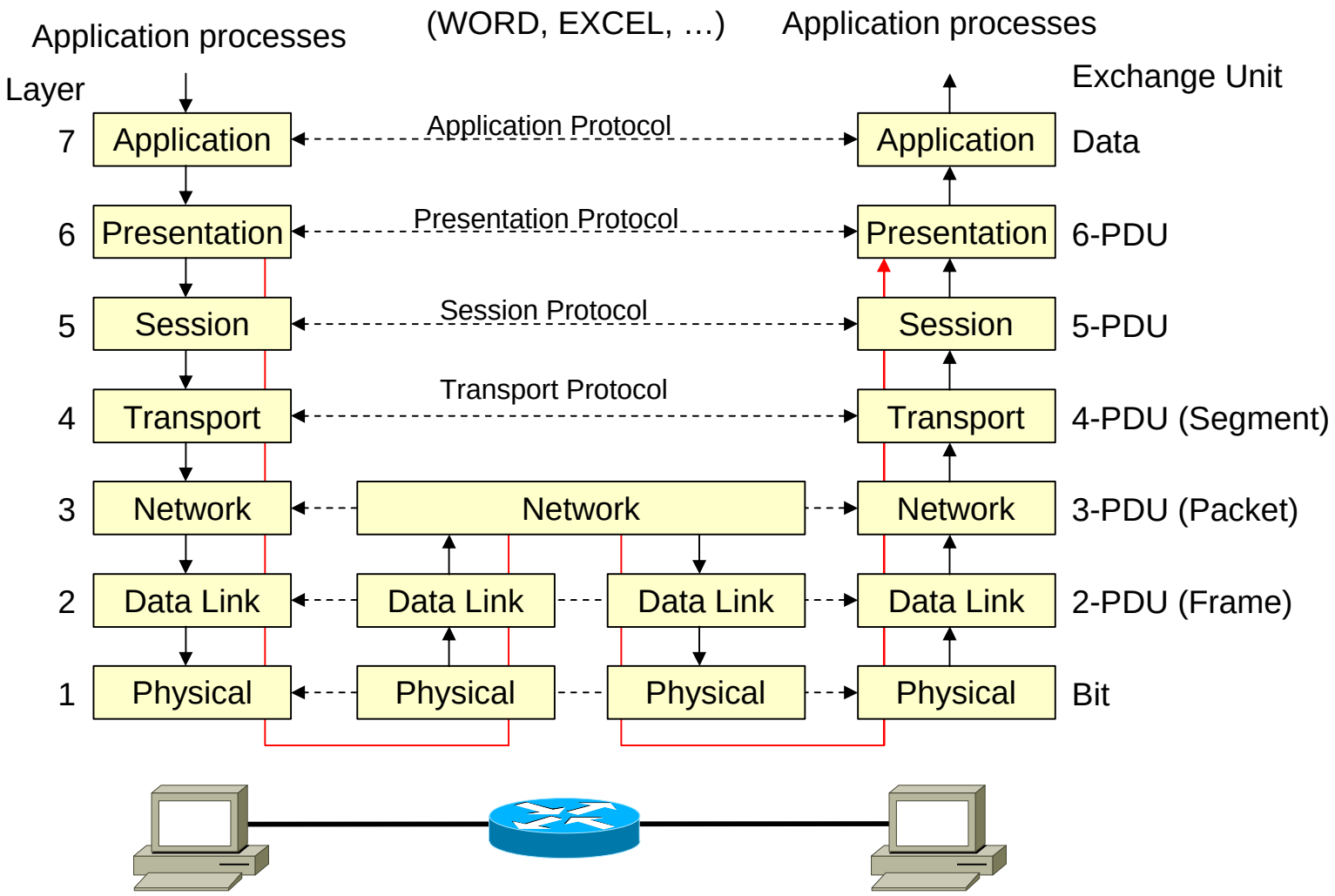
**Layer 7 - Application Layer** (Anwendungsschicht)

- provides network (Email, FTP, HTTP, DNS, Telnet, ...) services to application software
- identifies communication partners,
- identifies quality of service,
- considers user authentication and privacy.

In most modern Internet applications, the *session*, *presentation* and *application* layers are usually rolled together inside the application itself, thus, your web browser performs all functions of the *session*, *presentation* and *application* layers.

# OSI Model for Network Architecture






**PDU** - Protocol Data Unit

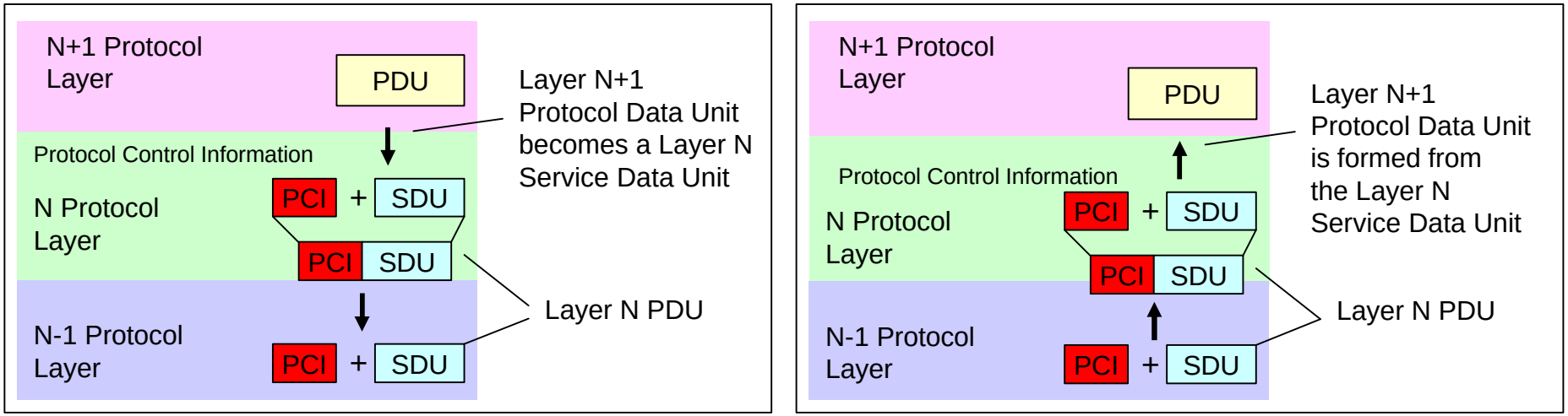
# Generic Layer Tasks



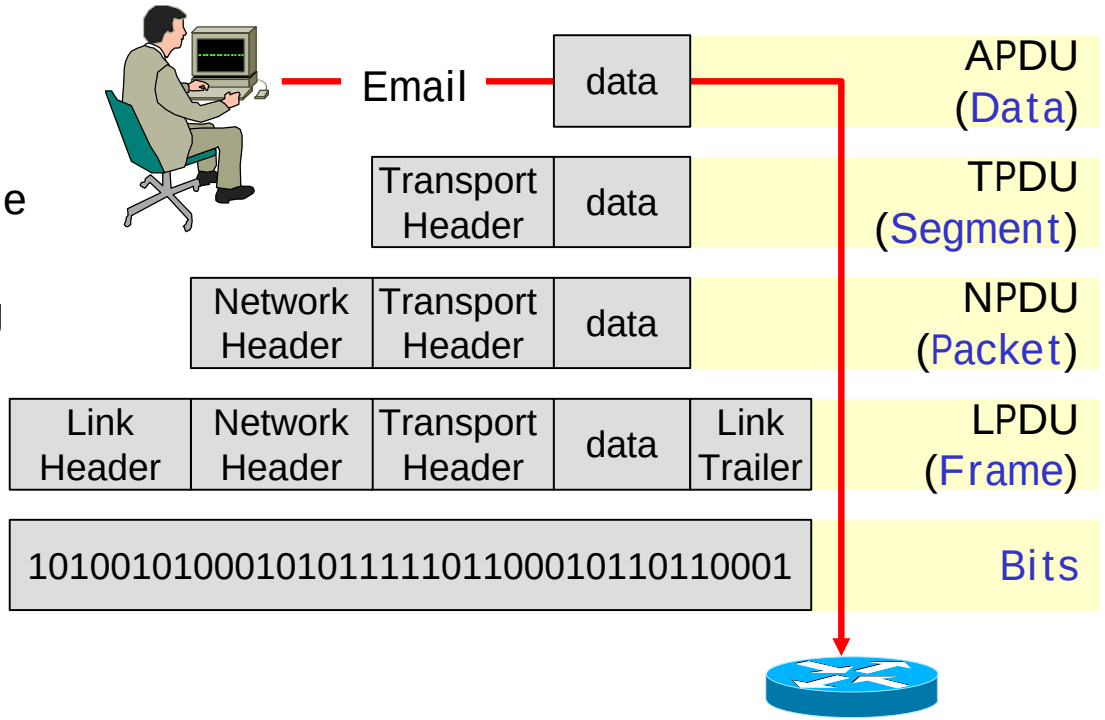
- In a layered networking model each layer may perform one or more of the following tasks
  - Peer-to-peer communication and communication with the layer above and below
  - Error control, which makes the logical channel between the layers in two peer network elements more reliable
  - Flow control, which avoids overwhelming a slower peer with PDUs
  - Segmentation and reassembly, which at the transmitting side divides large data chunk into smaller pieces and at the receiving side reassembles the smaller pieces into the original large chunk
  - Multiplexing, which allows several higher-level sessions to share a single lower level connection
  - Connection setup, which provides handshaking with a peer
  - Encapsulation, which takes the PDU of the higher layer as data and adds header with its own protocol control informationinformation

# Data Encapsulation






- Encapsulation by layer N means
  - put Layer-N+1 PDU as layer-N Service Data Unit (SDU) into the layer-N PDU´s data field
  - build the layer-N PDU by adding Layer-N Protocol Control Information (PCI) to the SDU in form of a header/trailer
- The PDUs of the different layers are also called Data, Segment, Packet and Frame



# Benefits and Drawbacks of the OSI Model



## Benefits

- The OSI reference model is a framework that is used to understand how information travels throughout a network.
- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- Interoperability: It allows different types of network hardware and software from different vendors to communicate with each other.
- Decouples layers: It prevents implementation changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

## Drawbacks

- One layer may duplicate lower-layer functionality
- One layer may need information that is present only in another layer. This violates the goal of decoupled layers

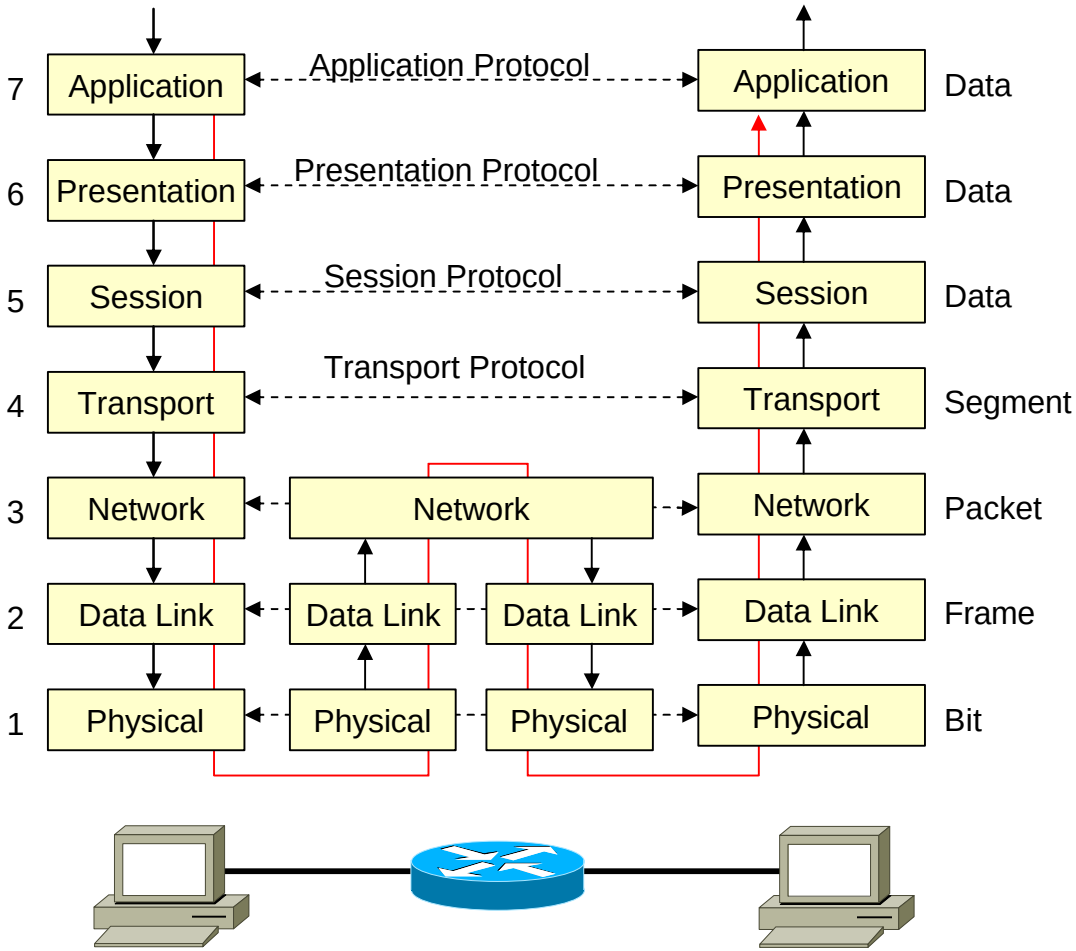
**Benefits of the OSI Model**

- Reduces complexity
- Standardizes interfaces
- Facilitates modular engineering
- Ensures interoperable technologies
- Accelerates evolution
- Simplifies teaching and learning

# Protocol Interaction during Transmission

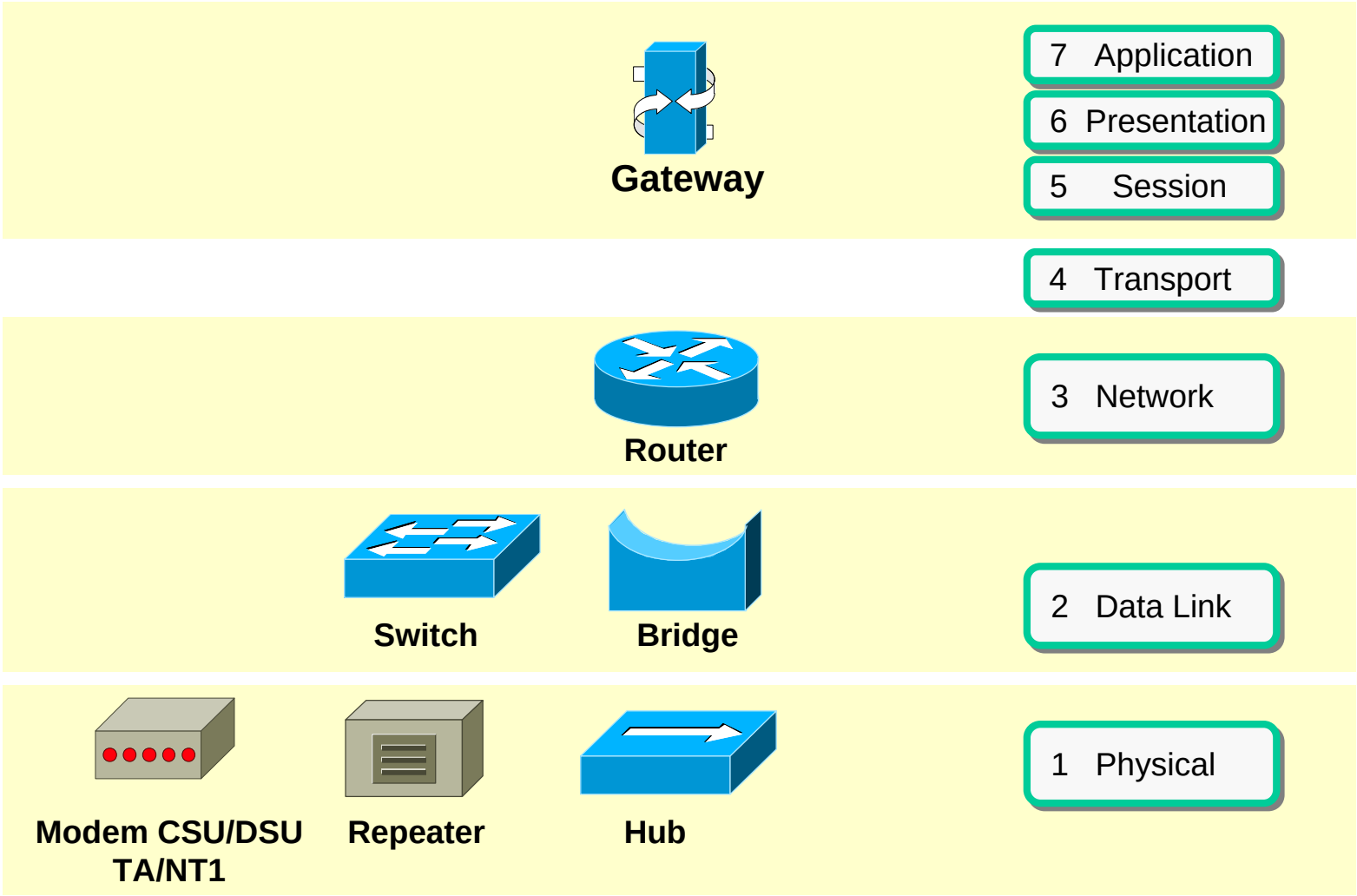


- Essentially networks must perform the following five conversion steps in order to encapsulate data:
  1. Build the data.
  2. Package the data for end-to-end transport.
  3. Add the network addresses of source and destination to the header.
  4. Add the data link layer header and trailer.
  5. Convert to bits for transmission.
- The inverse steps are necessary for decapsulation at the destination
- Only some of these steps are necessary at intermediate nodes



# Network Layers and Devices

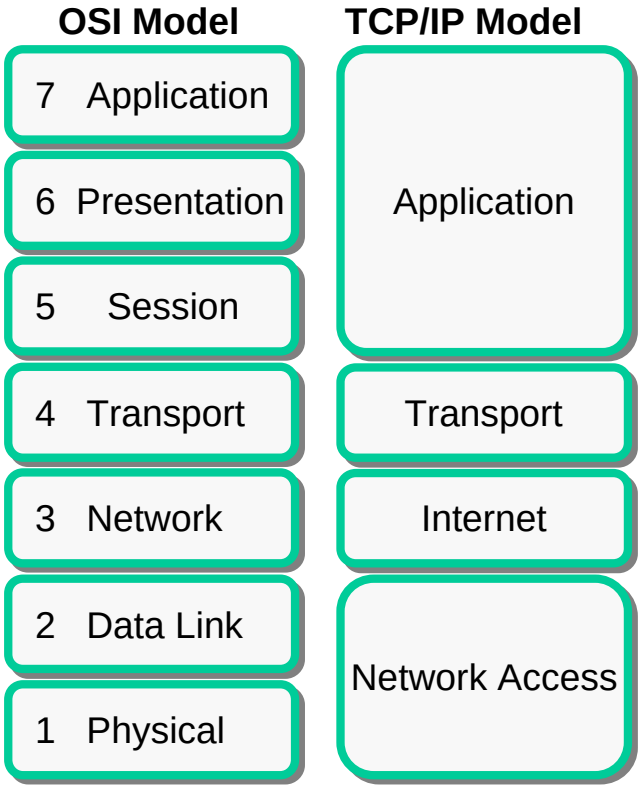




# TCP/IP model



- TCP/IP protocol has been used by most Unix workstation vendors.
- TCP/IP is designed around a simple four-layer scheme. It does omit some features found under the OSI model.
- It combines the features of some adjacent OSI layers and splits other layers apart.
- The four network layers defined by TCP/IP model are as follows.
- **Layer 1 - Link**
  - Defines the network hardware and device drivers.
- **Layer 2 - Network**
  - Is used for basic communication, addressing and routing. TCP/IP uses IP and ICMP protocols at the network layer.
- **Layer 3 - Transport**
  - Handles communication among End-user applications on a network. TCP and UDP falls within this layer.
- **Layer 4 - Application**
  - End-user applications reside at this layer. Commonly used applications include NFS, DNS, arp, rlogin, talk, ftp, ntp and traceroute.



# TCP/IP model and Protocol Suite



Some of the most commonly used application layer protocols include the following:

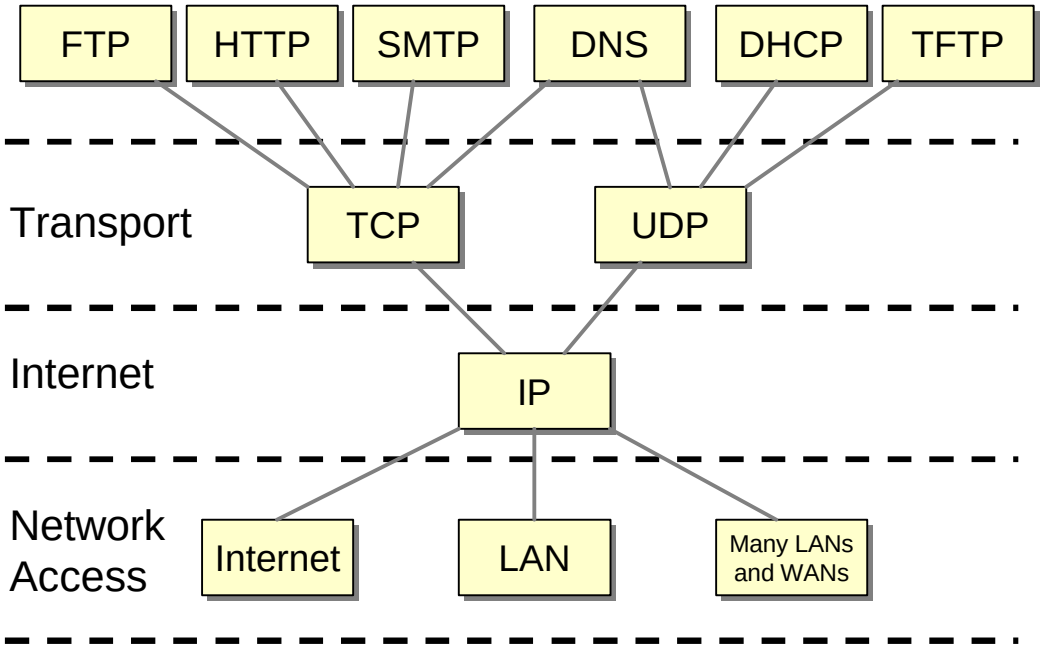
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Trivial File Transfer Protocol (TFTP)

The common transport layer protocols include:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

The primary protocol of the Internet layer is:

- Internet Protocol (IP)



# Lab Exercises



- 2.3.6 Lab Exercise: OSI Model and TCP/IP Model
  - In this lab, the student will learn the four layers of the TCP/IP model and the seven layers of the OSI model to the four layers of the TCP/IP model.
  - Homework

- 2.3.7 Lab Exercise: OSI Model Characteristics and Devices
  - In this lab, the student will learn the seven layers of the OSI model and the characteristics, functions and keywords relating to each layer.
  - Homework

# Summary (1)



An understanding of the following key points should have been achieved:

- Fundamental networking devices are hubs, bridges, switches, and routers
- The physical topology layouts include the bus, ring, star, extended star, hierarchical, and mesh
- LANs and WANs were developed in response to business and government computing needs
- A WAN consists of two or more LANs spanning a common geographic area
- A SAN provides enhanced system performance, is scalable, and has desaster tolerance built in
- A VPN is a private network that is constructed within a public network infrastructure
- Three main types of VPNs are access, Intranet, and Extranet VPNs
- Intranets are designed to be available to users who have access privileges to the internal network of an organization
- Extranets are designed to deliver applications and services that are Intranet based, using extended, secured access to external users or enterprises
- Understanding bandwidth is essential when studying networking
- Bandwidth is finite, costs money, and the demand for it increases daily
- Bandwidth is measured in bits per second, bps, kpbs, Mbps, or Gbps

# Summary (2)



- Limitations on bandwidth include type of media used, LAN and WAN technologies, and network equipment
- Throughput refers to actual measured bandwidth, which is affected by factors that include number of users on network, networking devices, type of data, user's computer and the server
- The formula T=S/BW (transfer time = size of file / bandwidth) can be used to calculate data transfer time
- Comparison of analog and digital bandwidth
- A layered approach is effective in analyzing problems
- Network communication is described by layered models
- The OSI and TCP/IP are the two most important models of network communication
- The International Organization for Standardization (ISO) developed the OSI model to address the problems of network incompatibility
- The seven layers of the OSI are application, presentation, session, transport, network, data link, and physical
- The four TCP/IP layers are application, transport, internet, and network access
- The TCP/IP application layer is equivalent to the OSI application, presentation, and session layers