Glossary
Network

This document is a collection of explanations of technical terms and abbreviations on the topic of Network.

802.3

Standard that describes the CSMA/CD transmission procedures.
These include:
The "original standard" (10Base5) which used a yellow coaxial cable ("yellow cable") as the medium (broadcast medium / bus). It is compatible with the already previously developed Ethernet and only differs slightly even as regards the technical specifications.

- 802.3a *(10Base2)* - the so-called "*cheapernet*". Uses black and red thin coaxial cable (broadcast medium / bus)
- 802.3i *(10Base-T)* - the so-called "*twisted pair*" (twisted copper cable), the most used transmission technology today, which permits so-called structured cabling
- 802.3u (100Base-T) - the so-called "fast Ethernet", which allows a 10 times higher transfer rate than "10Base-T"
- 802.3z, 802.3ab *(1000Base-T)* - the so-called "Gigabit Ethernet"
- 802.3ae - Ethernet with 10 Gb/s

ATM

ATM stands for Asynchronous Transfer Mode. The data is transferred to so-called cells with this transmission technology. ATM was designed to transfer voice and data on a medium. However, it has been sidelined by Voice Over IP and the fast 802.3 transmission technologies (e.g. Gigabit Ethernet).

Backbone

A network (segment) that is used to connect other networks with each other. Backbones are to be found e.g. in buildings or on a campus.

Bandwidth

Bandwidth in information technology means the most possible data quantity that can be transferred via a line (e.g. 10 MBit/s for Ethernet). Bandwidth in communications engineering is the difference between the lowest and highest transmission frequency (e.g. telephony: 300 Hz - 3400 Hz = 3.1 kHz)

BNC

BNC stands for Bayonet Neill Concelmann, Bayonet Nut Coupling (= threaded bayonet lock) The BNC plug-in connection is a bayonet lock for connecting two coaxial cables. BNC plug-in connections are designed for RG-58 cable (Ethernet and "cheapernet") and RG-59 cable (video). The BNC cable (RG58 cable) is equipped at both ends with a terminator. On each network card there is a connector that is directly fitted onto the network card.

Bridge

A bridge is a transit system (coupling element) between two (or more) network segments. Bridges work on the OSI layer 2a (MAC layer). Bridges are used to separate loads and errors between two segments. Based on a table with MAC addresses the bridge decides whether a packet is forwarded to the other segments - or whether it remains/can remain local.

Broadcast (Address)

Broadcast addresses (in short: broadcasts) are always received, and where applicable interpreted, by all the computers connected to a network. There are broadcast addresses both on layer 2 and on layer 3. See.

Bus Topology

The processors of a network are connected to a single cable ("bus cable") for bus topology, i.e. almost like pearls on a string Stars and rings are also topologies.

CRC

CRC stands for Cyclical Redundancy Check and is also called FCS (Frame Check Sequence). In the case of CRC/ FCS a checksum is formed by the sender according to a complex mathematical procedure over the data packet and attached to the packet (trailer). The receiver calculates on its part the checksum and compares it with the attached value. If the result is the same, error-free transmission can be assumed. If differences occur, transmission is faulty and the received packet is destroyed. If need be, a retransmit is also initiated.

DDNS (Dynamic DNS)

Normally, the DNS only works with static IP addresses - i.e. an IP address is firmly allocated to a name. Whoever makes Internet offers available via a dial-in line (e.g. ISDN, DSL), is confronted by the problem of dynamic IP addresses. Every time you dial-in to the Internet, the provider allocates a new address to the connection. However, it is possible with DDNS to always be present in the Internet under www.<meine_seite>.de present, although the corresponding IP address is continuously changing.

Decryption

Decryption is the opposite of encryption.

Default Gateway

A router that is permanently registered in an IP computer, to which this station sends all the packets that are not intended for its own network.

DHCP (Dynamic Host Configuration Protocol)

As a result of this protocol a DHCP server (frequently integrated in the router) automatically allocates its IP address to the computers in the LAN. Furthermore, the router also administers DNS and gateway information.

DNS (Domain Name Service)

The appropriate IP addresses are allocated to the computer names with help of the DNS. Every processor in the Internet has a unique IP address and generally always has one name (or more) - 216.239.55.100 stands for example for www.google.com and www.google.de.

Duplex

See Full duplex

Encryption

Encryption means specifically making data illegible during the transmission and saving of data. Encryption is done using a complicated mathematical rule - the so-called algorithm. Known algorithms include DES or AES. Encryption also requires one or two so-called keys (one for encryption and one for decryption).

Ethernet

Ethernet is the most frequently used transmission technology. Ethernet is based on bus technology and uses CSMA/CD as the access procedure. Ethernet was standardized as early as 1976. It is compatible with protocol 802.3 and also works in a very similar way.

Fragmenting

Breakdown of a data packet into several small parts (fragments). This becomes necessary e.g if a packet is larger than the MTU (maximum transmission unit) of the network. The fragmenting is generally done by the router.

Gateway

Transit system (coupling device) between two networks that normally works above the OSI layer 3, i.e. a protocol change is made. However, a router is also occasionally referred to as a (layer 3) gateway (e.g. default gateway) in literature and in standards.

Hub

See Repeater

IDS (Intrusion Detection System)

Computers in a network or a program on a server, which should detect an attempt at intrusion on the basis of behavior patterns. In a network this can in the simplest case be e.g. a sniffer / network analyzer. However, it can also be an interconnected computer (bridge, router, firewall).

IPSec

This protocol safeguards the data stream at packet level. The main area of application for IPSec is the setting-up of VPNs and the protection of dial-in connections.

Jitter

Jitters are phase shifts / fluctuations (time changes) of (digital) signals

Collision

Collisions occur in CSMA/CD networks if two or more stations want to transmit at the same time.

LAN

LAN is the abbreviation for Local Area Network and describes a network of low reach (a few 100 meters), but very high data transfer rates.

MAC Address

In order to communicate in a network it is necessary for the addresses to identify the destination and sender station. There are addresses on OSI layers 2 and 3.
The MAC address is the so-called hardware address (also known as the physical address). They are used for direct communication between a sender and its direct communications partner.
All routing-enabled protocols also have the so-called logical address on layer 3 (e.g. IP address). These addresses describe the route through a network (routing).

Multiplexer

A multiplexer (also: MUX) collects several data streams from different lines and transmits them via a common (faster) line.

NIC

NIC stands for *Network Interface Card* (network card) and refers to the network adapter in computers.

OSI Model

OSI stands for Open System Interconnection and refers to a reference model that was created by the International Standardization Organization (ISO) in 1977 as the basis for the formation of communications standards. The ISO/OSI model divides the transmission activities into seven function blocks, so-called layers.

Overhead

The overhead refers to all the data that is transmitted in addition to the actual usage data. This includes in particular headers and trailers.

Repeater

A repeater is a transit system that works on OSI layer 1 and is used there to strengthen and regenerate the electrical signals. In contrast to bridges and routers repeaters cannot separate loads or filter errors on account of the way they work. The term hub has in the meantime become widely accepted in colloquial speech.

Router

A router is a transit system that works on OSI layer 3. Routers are therefore specific to the protocol, i.e. they can only process (route) the packets of the one network protocol (e.g. IP). If support is to be provided for several network protocols, so-called multi-protocol routers are used. Due to the manner in which they work they route data packets through a network in the most suitable / fastest way. They are therefore also used to separate loads and errors. And they also take on additional tasks, such as fragmenting.

SSL (Secure Socket Layer)

Protocol / Procedure to safeguard communication between the client and the server (e.g. HTTPS). For more information see my SSL page.

TCP/IP Model vs. OSI Model

The TCP/IP protocol model differs from the OSI model in that it comprises less layers (only four). Thus, e.g. all the normal TCP/IP services, such as TELNET, FTP, etc. are accommodated on the OSI layers 5 - 7. And network access generally covers two OSI layers.

Twisted Pair

Twisted pair cable consists of twisted pairs of wire - e.g. telephone lines. Due to their symmetric structure such cables are insensitive to external (electromagnetic) interference. Twisted pair cable is available with a shield (Shielded Twisted Pair = STP) and without (Unshielded Twisted Pair = UTP). Coaxial cable is clearly better in terms of transmission properties

Encryption

See Encryption

VLAN (Virtual LAN)

A virtual LAN is a group of computers that have been put together at MAC level in an autonomous, secure domain (e.g. IP subnet). No multicast or broadcast traffic takes place into or out of the VLAN. The affiliation to a VLAN does not depend on the geographical situation of the network node. It is determined solely by the software configuration. It can be changed very quickly if a computer is to be allocated to a new working group.

Voice over IP (VoIP)

Voice over IP (VoIP) means the transmission of voice / telephone via an IP network. In the case of VoIP the analog (voice) signals are digitalized and packed into IP packets. It is important here that the packets are if possible not delayed on their way through the network / Internet, because voice quality can suffer significantly. Via gateways it is possible for the VoIP packets to be transmitted to the normal telephone network (and vice versa).

Full duplex

In the case of a full-duplex transmission (or also duplex transmission) the data channel between two terminals is permanently opened in both directions, i.e. both terminals can send and receive at the same time.

VPN - Virtual Private Network

A VPN is a network link, in which the data is transmitted through special tunneling protocols (e.g. IPSec) in a safe way (encrypted) via the Internet. VPNs are used to save the costs for a dedicated data line. Instead of connecting two lines with a rented line the Internet is simply used.

WAN

WAN stands for *Wide Area Network* and describes a spatially large network (reach > 50 km) with a comparably low data transfer rate.

WLAN (Wireless LAN)

WLANs are radio-based networks. They work according to the standard 802.11.
Communication here is generally always via a central node, the access point, which also establishes the connection to the wired network. WEP (Wired Equivalent Privacy) is used to make data interception more difficult. However, this procedure is only secure to a limited extent to the effect that VPN technology should also be used for real security.
WLANs should not be confused with VLANs.