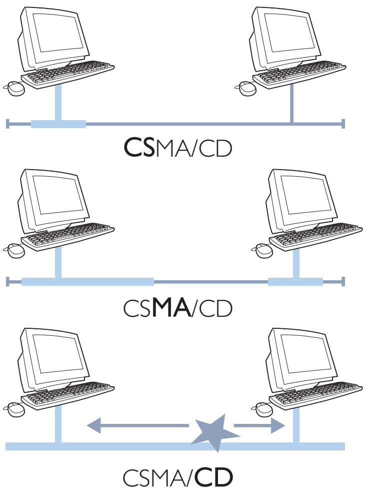
Industrial Ethernet

As a communication standard, Ethernet has existed for many years and today forms the basis of most networks throughout the world. Despite many claims over the years that Ethernet will be replaced, it continues to be developed and offers the properties that users have requested. In recent years Ethernet has also won approval in the industrial market.

IEEE 802.3 Ethernet

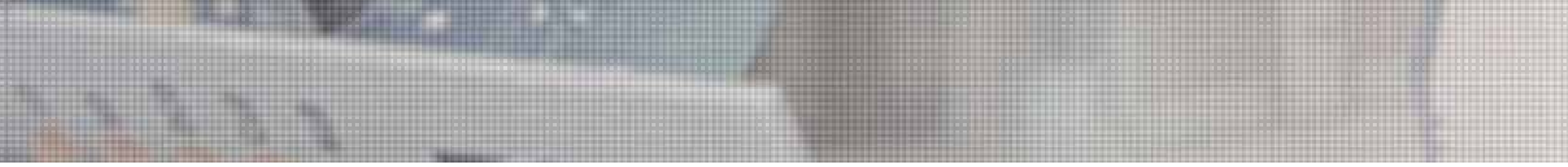
Access methods

In order for two or more parties to communicate requires a set of rules, this applies to everything, especially to data communication. How data is transmitted on to a line is known as the access method, the original method used by Ethernet was called CSMA/CD, which means: **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect. It is important to establish that Ethernet uses two access methods, constant access or CSMA/CD. CSMA/CD is referred to regularly in literature but is not so commonly used today. It has a historical background and for this reason we will give a brief description of the parts in CSMA/CD:

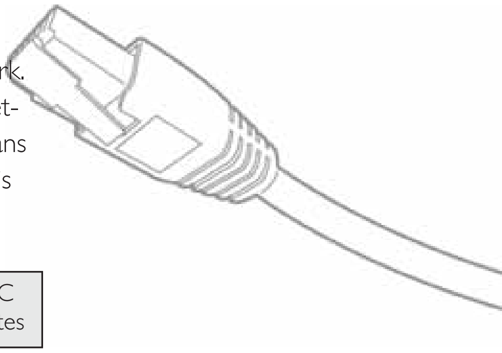


- **C**arrier **S**ense, which means that a single unit, before it sends, must detect whether someone is using the network. If so, the unit must wait before it transmits.
- **M**ultiple **A**ccess, means that everyone can use the network, but not simultaneously.
- **C**ollision **D**etect, means that when two or more units transmit simultaneously this should be detected. When a collision is detected, a collision signal is sent and all those concerned stop sending. All units then wait for a random period before new attempts are made, this minimises the risk of them starting to send at the same time. Naturally, collisions have the effect of slowing traffic in the system. A network with a high load results in many collisions, which leads to further network traffic, which in turn creates more collisions, etc. Some equipment has LEDs that indicate collisions, in doing so you can easily check the load on the network. The advantage of a CSMA/CD network is that all equipment can start transmitting at any time compared with a polled system or token ring where transmission is strictly controlled.

BACK



Ethernet Address & Packets



All Ethernet hardware has an address that uniquely identifies each node in a network. This address is programmed into the device by the manufacturer, for example, a network adapter card. This can not be changed by the user or by software, which means there is not (should not be) two network adapter cards with the same address. This address is often refered to as the MAC **M**edia **A**ccess **C**ontrol Address.

Preamble 8 bytes	Destination address 6 bytes	Source address 6 bytes	Type 2 bytes	Data 46 – 1500 bytes	CRC 4 bytes

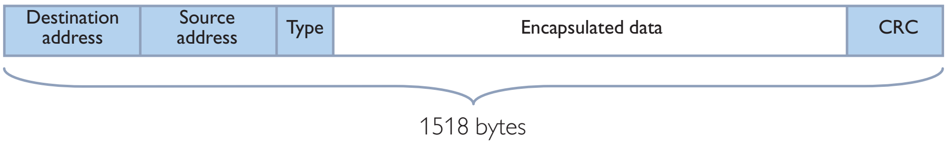
The Ethernet packet contains the following information:

- **Preamble.** The preamble is a 64-bit (8 byte) field that contains a synchronization pattern consisting of alternating ones and zeros and ending with two consecutive ones. After synchronization is established, the preamble is used to locate the first bit of the packet. The preamble is generated by the LAN interface card.
- **Destination Address.** The destination address field is a 48-bit (6 byte) field that specifies the station or stations to which the packet should be sent. Each station examines this field to determine whether it should accept the packet.
- **Source Address.** The source address field is a 48-bit (6 byte) field that contains the unique address of the station that is transmitting the packet.
- **Type field.** The type field is 16-bit (2 byte) field that identifies the higher-level protocol associated with the packet. It is interpreted at the data link level.
- **Data Field.** The data field contains 46 to 1500 bytes. Each octet (8-bit field) contains any arbitrary sequence of values. The data field is the information received from Layer 3 (Network Layer). The information, or packet, received from Layer 3 is broken into frames of information of 46 to 1500 bytes by Layer 2.
- **CRC Field.** The Cyclic Redundancy Check (CRC) field is a 32-bit error checking field. The CRC is generated based on the destination address, type and data fields.

BACK

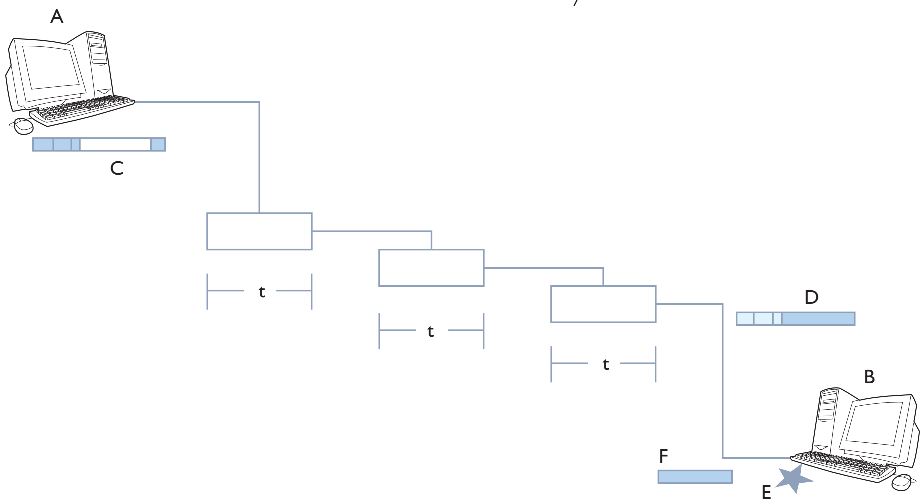
Collision domain

A collision domain is a segment where connected equipment must be capable of detecting and managing collisions (as several devices send simultaneously). Data that collides does not disappear automatically, but CSMA/CD neatly and tidily ensures the data is retransmitted. The number of retransmission attempts can be limited to 16, and it is not until then that data can be lost. On the other hand, it is only usual with so many retransmission attempts on a very heavily overloaded Ethernet network.

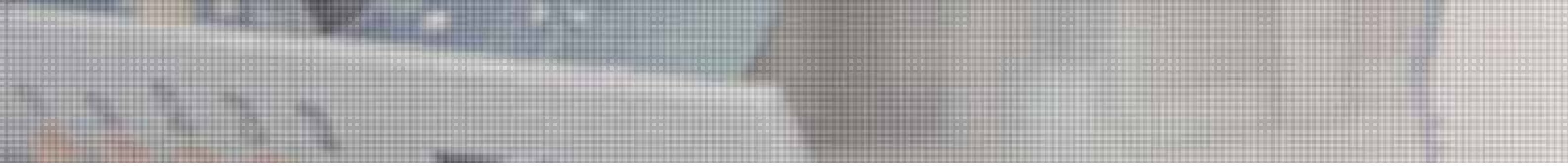


Destination address	Source address	Type	Encapsulated data	CRC

An Ethernet packet basically consists of 1518 bytes, if you use VLAN a further 4 bytes are added, which in total gives 1522 bytes. This, together with the speed of the network, gives the prerequisite for how quickly a message reaches the most remote devices on the network. Under no circumstances may a collision domain be constructed so that the sending device can not identify a collision before knowing in all certainty that the packet has reached the receiver. The network and installed equipment determine the maximum propagation on a collision domain as all equipment adds a delay, also known as latency.



BACK



- Assume that **A** intends to send a packet to **B**.
- The network includes a certain amount of equipment that has an internal delay (**t**).
- **A** continuously empties its send buffer, when no collision is discovered.
- A collision occurs on the outermost node on the network (**E**).
- All data (**D**) is not received, which results in (**B**) not being able to interpret it.
- The collision signal (**F**) is sent back to the transmitter (**A**).
- When the domain is too large, the collision signal does not reach (**A**) before the send buffer has been emptied. This makes it impossible to retransmit the packet.

IP Networks

Internet Protocol

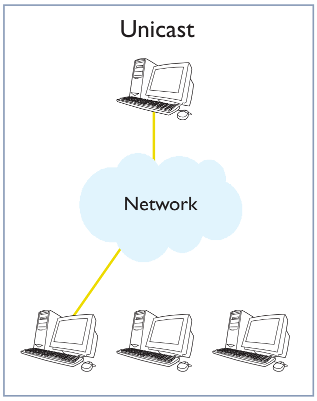
IP or Internet Protocol is designed for connections in a network or between several networks. When the specification was written it was understood that new technologies and new transfer methods would be continuously developed. This is why an open standard that is primarily independent of the underlying network and medium was developed. TCP/IP is a family of protocols that extends between many different layers in the OSI-model.

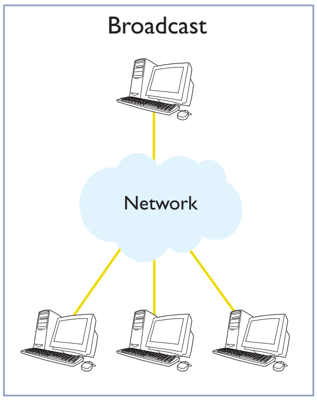
Addressing methods

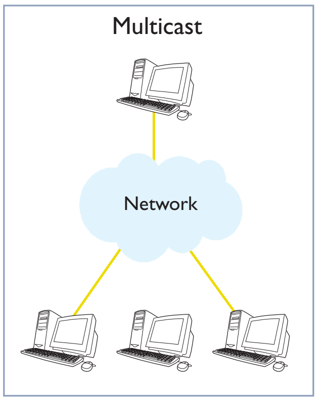
Much of the information in a network goes from single sender to a single receiver. This is completely natural in most cases, for example, a PLC communicating with an I/O device. This kind of transfer is usually called unicast.

The opposite to unicast is "broadcast", i.e. the way that radio and television are transmitted: one sender and many receivers. Broadcasting means that information is sent out to everyone, the technique is used in some closed computer networks, but broadcasting over the entire Internet is impossible as it would overload the network.

Multicast is a technique that fits in between unicast and broadcast. Information is not sent out indiscriminately to everyone as in broadcasting, but the same information can have numerous receivers unlike unicasting. Using multicast allows the building of distribution networks, which are suitable for video monitoring or television transmissions over the Internet, i.e. information with one sender and many receivers. Multicast will open up new possibilities for the Internet and prevent it from collapsing due to overloading.


Unicast


Broadcast


Multicast

BACK

Byte	1	2	3	4
	192.	168.	3.	23

Addressing in a network

Before we describe how an IP address is built up we need to explain a few concepts:

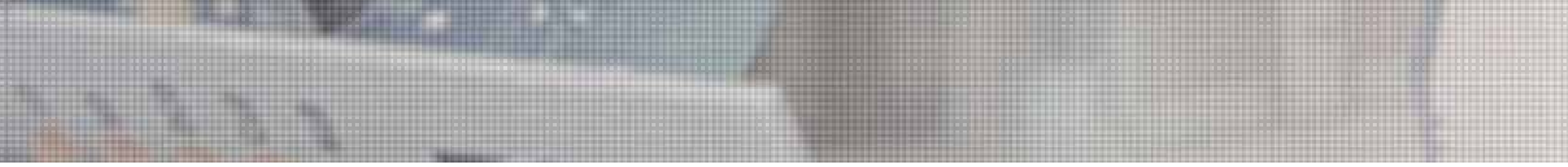
- An IP address consists of four bytes.
- One byte is 8 data bits, for example, 11000000, which corresponds to the decimal value 192, see byte 1 in the example opposite.
- In turn, addresses are allocated in different classes (A, B, C, D and E) where the class describes an address interval. There are currently five address classes, of these the first three are used (A-C) for different network types, where the IP address is divided into a network and computer part. There are also the groups D and E. A D address is a multicast-address while an E address has been saved for future use.
- IP addresses in class A, B and C networks are divided into two parts, a network part and a computer part.

Class	First byte	Address interval
A	0xxx xxxx	**0**.0.0.0 to **127**.255.255.255
B	10xx xxxx	**128**.0.0.0 to **191**.255.255.255
C	110x xxxx	**192**.0.0.0 to **223**.255.255.255
D	1110 xxxx	**224**.0.0.0 to **239**.255.255.255
E	1111 xxxx	**240**.0.0.0 to **247**.255.255.255

A, B or C networks differ in the number of bits utilised for network and device identity:
The A class network identity comprises 8 bits (1 byte), B class 16 bits and the C-class 24 bits. This makes it possible to address a different number of devices in respective networks, also see sub-network division below.

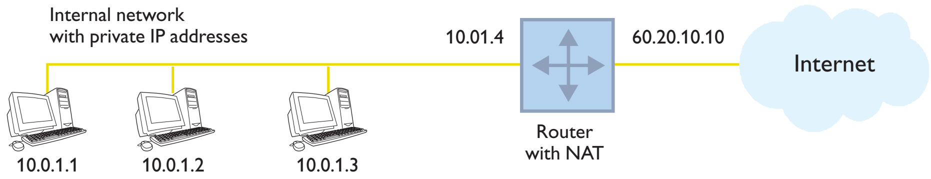
Class					Decimal value in octet 1	Max. number of devices in the network
A	Network	Computer	Computer	Computer	0 to 127	16 777 215
B	Network	Network	Computer	Computer	128 to 191	65 535
C	Network	Network	Network	Computer	192 to 223	255

BACK



Private and public addresses

There may be cases where you can not use or do not want to use public IP addresses on your internal network, instead you can use private IP addresses (RFC1918). These IP addresses will not work on an Internet connection, the solution is then to use NAT (**N**etwork **A**ddress **T**ranslation).



A router or "firewall" with support for NAT translates private addresses to public addresses:
When the computer with address 10.0.1.2 needs to access the Internet, 10.0.1.4 is addressed which is the "Default Gateway" or "way out". When data from address 10.0.1.2 passes through the router NAT translates the internal IP address 10.0.1.2 to 60.20.10.10 i.e. the IP address on the "outside". In this way an internal IP address can communicate with other computers on the Internet. It does not matter when another internal IP address communicates at the same time as the router manages which session belongs to which internal IP address and ensures the right traffic goes to the right computer on the internal network.

IANA (**I**nternet **A**ssigned **N**umbers **A**uthority) has reserved the following three address blocks for IP addresses in private networks:
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

BACK

Ipv4 and Ipv6

IPv6 is version 6 of the Internet-protocol, the new version was drawn up at the end of the 1990s to replace the current, IPv4 (version 4), mainly because the IP addresses are starting to come to an end. The greatest difference between IPv6 and IPv4 is that the address length has been increased from 32 bits to 128 bits. This means the number of possible addresses has been increased from 4 billion to a real astronomical number.

Ipv6 header

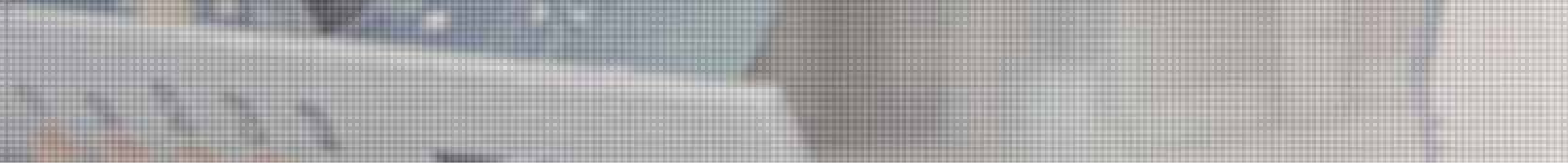
<table>
<tr><td colspan="3">128 bits source address</td></tr>
<tr><td>Payload length</td><td>Next header</td><td>Hop limit</td></tr>
<tr><td colspan="3">128 bits source address</td></tr>
<tr><td colspan="3">128 bits destination address</td></tr>
</table>

Subnetwork division

Local networks with more than a few hundred connected devices are unusual; allowing this kind of network to take up its own A or B Class (Over 16 million networks with 65000 devices possible on each network) is an immense waste of available addresses. Most of these classes are therefore divided into a **subnetwork**, where a part of the device identity is used as a type of network address. The division is made by utilising a part of the device identity, i.e. the "border" between the network address and the device identity is "moved" so that the number of available network identities is increased, at the same time as the number of devices in the subnetwork decreases. In order to achieve this a **netmask** is used where the bits that belong to the network part are set to one (and the computer bits are set to zero).

Smaller networks are easier to administrate, the data traffic in the subnetwork is less, the physical network becomes easier to set up and maintain (for example, you can utilise different subnetworks on different floors of a building), etc.

BACK



The following standard netmasks (i.e. a without subnetwork) apply to the address classes A, B and C:

Address class	Netmask	Binary value Byte 1	Binary value Byte 2	Binary value Byte 3	Binary value Byte 4
A	255.0.0.0	11111111	00000000	00000000	00000000
B	255.255.0.0	11111111	11111111	00000000	00000000
C	255.255.255.0	11111111	11111111	11111111	00000000

As described earlier, a Class B IP address consists of two equal sized address parts, 2 bytes each for the network and device identity, this can be written N.N.D.D, where N represents the octet belonging to the network identity and D the device identity, whereby the netmask becomes 255.255.0.0.

If the full 3rd octet is used to define the subnetwork instead of a device identity, the address can be interpreted as N.N.N.E, i.e. the netmask becomes 255.255.255.0. This means we have 254 C-like networks with 254 computers in each (first and last addresses in the network and computer parts are reserved).

In principle any of the bits in an octet can be used to define a subnetwork, normally the highest bits are reserved for this, as it significantly simplifies management. If, for example, the first three bits in a C address are used for subnetwork addresses, the C network would be divided into 6 subnetworks (see the possible combinations of networks as set out below). Two bit combinations of the device identity (11111 and 00000) are reserved for broadcast and network identity, which is why the number of available addresses will be 30 on each of these networks.

Netmask	C-like netmask	3 first bits in the C-like netmask	Other bits in the C-like netmask	Subnet work	Number of device identities
255.255.32.0	32	001	00000	1	30
255.255.64.0	64	010	00000	2	30
255.255.96.0	96	011	00000	3	30
255.255.128.0	128	100	00000	4	30
255.255.160.0	160	101	00000	5	30
255.255.192.0	192	110	00000	6	30

BACK

Ports

An application receives data on a special port number that identifies communication with this application.

For example, a computer can be both a web server, E-mail server and DNS server running at the same time. In order for the traffic to the different applications not to collide, it must be divided up, this is done by predefining the port number to the application. Port numbers between 1 and 1024 are known port numbers and must not be used by applications other than those specified.

Examples of known port numbers are:

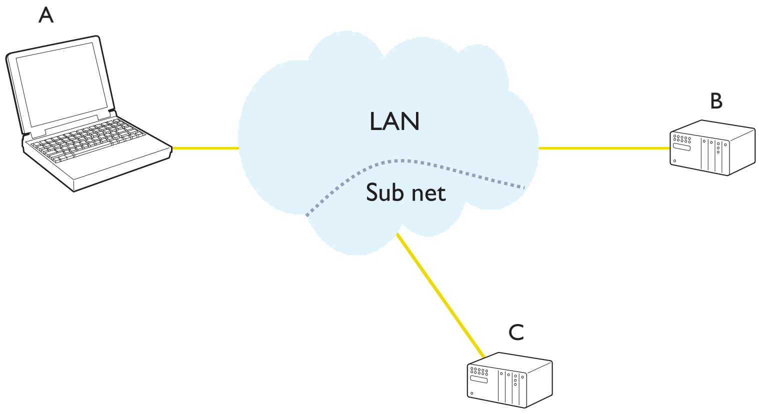
21	ftp	File transfer
23 Telnet	Telnet	
25	smtp	Mail, Simple Mail transfer
80	http	www

A complete list can be found at www.iana.org/assignments/port-numbers

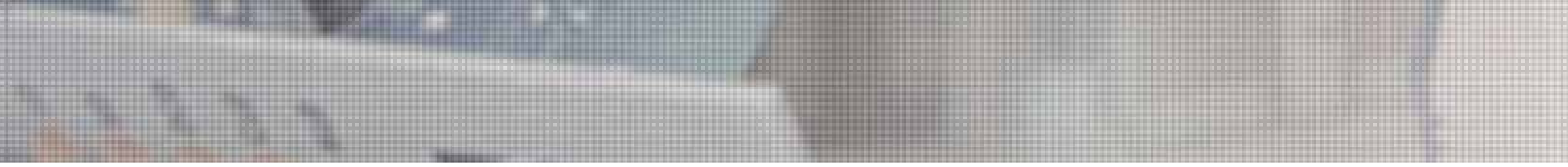
ARP

Computers, or other hardware, that are connected to a TCP/IP–network all have at least one IP address. The IP address is also known as the logical address as it is usually implemented in software and can be changed depending on where in the network the hardware is physically located. The devices also have a physical address which in an Ethernet network is called the MAC-address, this is unique for each piece of connected hardware.

When two pieces of equipment (A) and (B) utilises TCP/IP to communicate over Ethernet, they must keep track of each other's MAC-address, as all communication on an Ethernet is made to MAC-addresses.



BACK



This is why devices A and B have their own ARP-table of IP addresses and associated MAC-addresses.
ARP **A**ddress **R**esolution **P**rotocol, manages a dynamic update of the ARP-tables so that the association between IP and MAC-addresses is always known.

- Assume that computer (A) wants to communicate with the PLC (B). Computer (A) already knows (B's) IP address (can e.g. have been manually configured by an operator) but (B's) MAC address is unknown to (A). Communication can not begin until (A) knows (B's) MAC-address.
- A discovers that B is on the same network by comparing the destination's IP address and the network mask.
- A sends out an ARP request in the form of a broadcast message. The enquiry contains (A's) IP and MAC address as well as B's IP address.
- All units on the network understand the message, but only B recognises its IP address and sends an ARP reply in response, which contains B's MAC-address.
- A's ARP-table can now be updated so that it also contains B's MAC-address.

Point to Point (PPP)

There are also occasions when you need to connect and communicate using TCP/IP via a serial connection. This concerns connections to the Internet via a modem or when you need to connect to a local area network. How you communicate varies from application to application. On these occasions you use the PPP protocol (**P**oint to **P**oint **P**rotocol.) which is without doubt the most used link protocol for computers that remotely connect to a network. Examples of serial communications are: telecom modem, modem with own leased line, ISDN, GSM, radio or short-haul modems.

Security (CHAP and PAP)

The protocol PPP is frequently used for remote point to point connections, irrespective of whether it is a dial-up, ISDN or leased line. In general some form of security between the communicating parties is required. PPP supports two methods of user verification, PAP (**P**assword **A**uthentication **P**rotocol) and CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol) for this purpose. Authentication, verification of messages, is not compulsory in PPP, so the parties are free to communicate without identification or negotiating on which protocol to use. The principal rule is first and foremost to choose CHAP. PAP is generally only chosen when one of the parties does not support CHAP.

BACK

PAP works similarly to when a user logs in using a terminal, you state your user name and password. Authentication only takes place once when the connection is being established, never while communication is in progress.

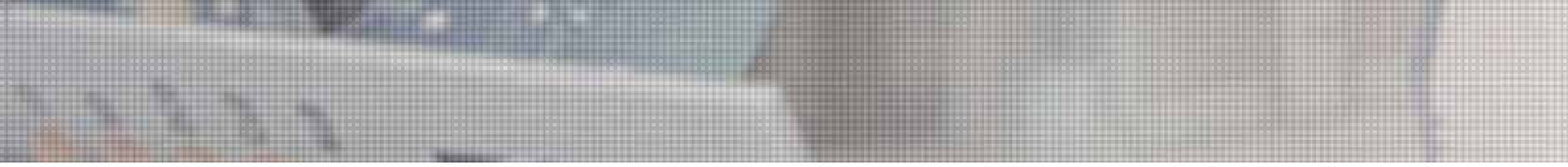
- The PAP-procedure starts by one of the parties sending an Authenticate-Request, containing name and password. This packet is repeated until the opposite party responds.
- When the name and password are accepted the recipient answers with an Authenticate-Ack. Otherwise an Authenticate-Nak is sent as the answer, and the recipient disconnects the connection.

The fact that the name and password are transmitted in plain text over the link makes PAP a relatively vulnerable authentication method. The password can be easily intercepted through tapping, and there is no protection against repeated trial-and-error-attacks.

CHAP involves significantly improved security compared to PAP.
CHAP uses an encrypted password in a three step procedure. Furthermore, authentication takes place partly when the link is established and this can then be repeated at anytime. The idea behind the periodic repetition is to limit the time that the system is open for an attack. It is always the authenticator (recipient) that determines how often authentication takes places. The three steps of authentication are:

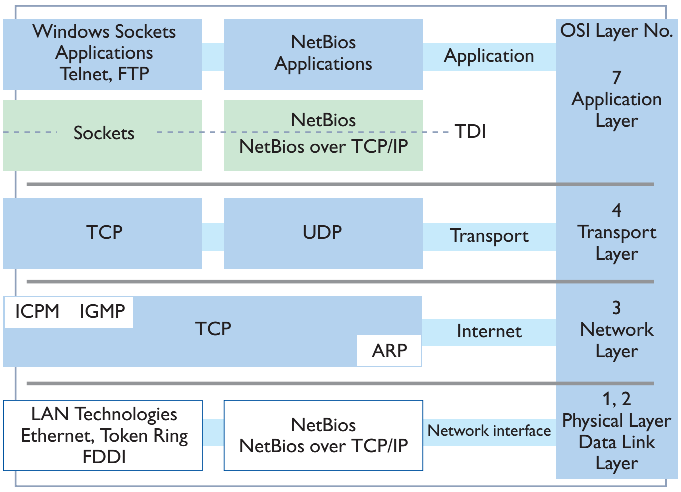
- When the link is established one of the parties (authenticator) sends a challenge to the peer.
- The peer calculates an encrypted value based on the challenge and its password. The encrypted value is returned to the authenticator.
- The authenticator makes an equivalent calculation (the challenge and the peer's password are known) and then compares the expected value with the value from the peer. When the value is identical authentication is confirmed, otherwise the connection is terminated.

BACK



TCP/IP and UDP/IP

In the OSI model each layer is responsible for the data that passes through it. The transport layer bears responsibility for the transfer of data and there are two alternative protocols available for this, TCP and UDP.



Windows Sockets Applications Telnet, FTP
NetBios Applications
Application
OSI Layer No.
7 Application Layer
Sockets
NetBios NetBios over TCP/IP
TDI
TCP
UDP
Transport
4 Transport Layer
ICPM
IGMP
TCP
ARP
Internet
3 Network Layer
LAN Technologies Ethernet, Token Ring FDDI
NetBios NetBios over TCP/IP
Network interface
1, 2 Physical Layer Data Link Layer

UDP

UDP (**U**ser **D**atagram **P**rotocol) is usually classified as a connectionless protocol. This means that data can be sent irrespective of whether the receiver exists or not. Neither will the receiver notify the sender whether the data was received or not. As data is transferred without an established connection, the transfer is more effective and usually faster. Consequently, UDP is used in applications that require effective use of the bandwidth and where the application supports the retransmission of lost data if necessary.

You can compare UDP to posting a letter, data is placed in an addressed envelope. Once you have posted the letter, you expect the post office to distribute the letter correctly. Another important function included in UDP is the possibility to send "broadcast" and "multicast", one message with many recipients. This is the primary reason for choosing UDP.

TCP

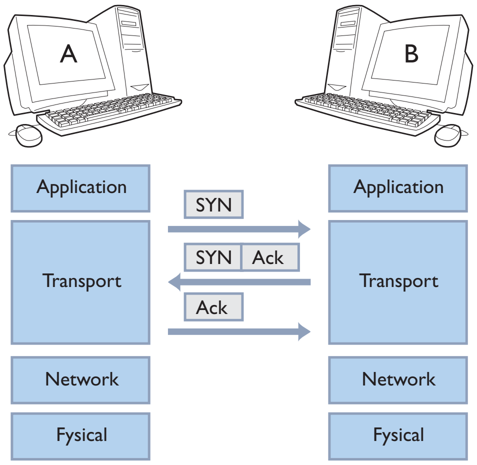
TCP (**T**ransmission **C**ontrol **P**rotocol) is a connection oriented protocol, this means a connection is established before the devices exchange data. TCP takes greater responsibility for the data transfer than UDP, as the transferred data is acknowledged by the recipient. The recipient must return an acknowledgement (ACK) for each sent data packet. When an ACK is not received, the packet is retransmitted, which guarantees that the data reaches the recipient.

Another function of TCP is that the protocol maintains sequence and flow control when large amounts of data are transferred. Several TCP-packets can reach the recipient in another order than the one they were sent in. TCP guarantees, that the packets are put together in the correct sequence, as they are assigned a sequence number. On account of the requirement to establish a session and acknowledge transfers, it takes longer for TCP to transfer data than UDP, in addition TCP uses more bandwidth.

BACK

Establishing a TCP connection

A connection is established using a handshaking procedure comprising of three steps:

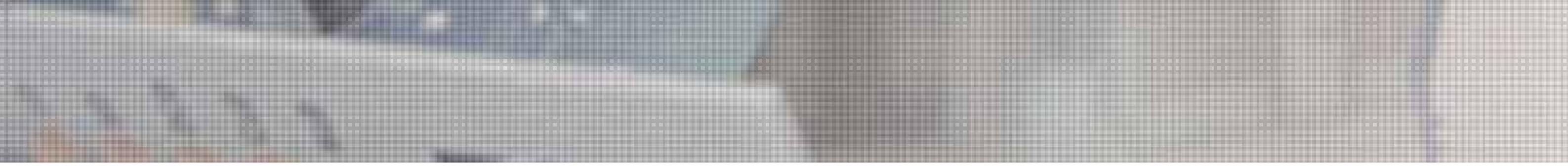


- The client A sends a connection request with the SYN-bit enabled. This allows the client to synchronise a sequence number with the Server (B).
- Server (B) acknowledges (ACK) the client with its SYN-bit enabled and with that the server has also synchronised its sequence number with the client.
- Finally the client acknowledges with (ACK).

The transfer takes place with one or more bytes, which are numbered and acknowledged.

A connection is terminated through the client (A) checking the local TCP-packet and through all information being transferred and acknowledged. A TCP-packet with the FIN-bit enabled is then sent. The server (B) acknowledges this, but continues to send data if the application so requires. Once this is complete the server (B) sends a TCP-packet with the FIN-bit enabled.

BACK



Building a network

Devices in a network

Repeaters

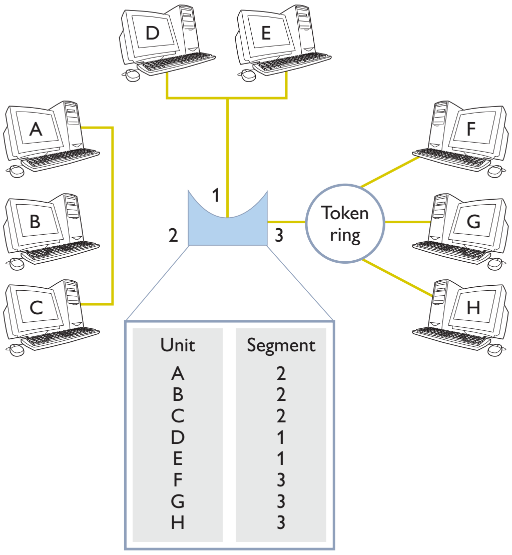
A repeater can be compared to an amplifier, it has no intelligence it only recreates signals. Signals are attenuated depending on the length of the medium and the frequency of the signal, which results in a network having a limited range. Using a repeater you can extend a medium by recreating the signal, thus the signal is identical to its initial state with regard to strength and appearance. A repeater acts within the same collision domain (HDPX CSMA/CD) and due to the added latency in each repeater, you can not install an unlimited number of repeaters in a segment.

Bridge

A bridge separates two or more collision domains and can be used to connect different topologies. The bridges listen and note which addresses belong to respective segments, and by doing so the bridge learns which segment respective devices are connected to.

A bridge is used, for example, when you want to join Ethernet with Token ring. Bridges usually work selectively, i.e. filters addresses so that data only reaches the destination address, for example, devices A and B only communicate on segment 2. In this way the network is divided up and internal traffic does not load other segments.

A bridge functions at the MAC layer routing traffic only based on its physical address. Whereas a router makes decisons based on the layer 3 addresses

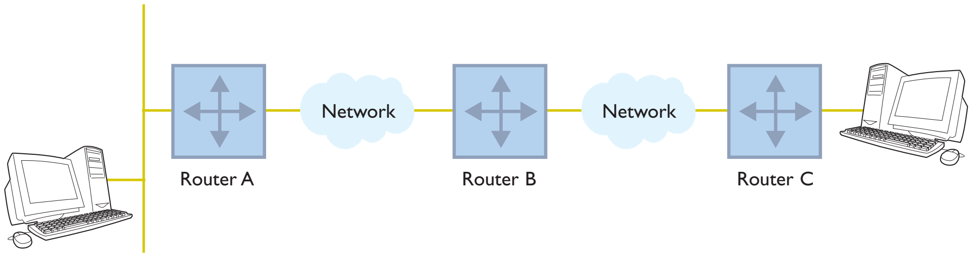


Unit	Segment
A	2
B	2
C	2
D	1
E	1
F	3
G	3
H	3

BACK

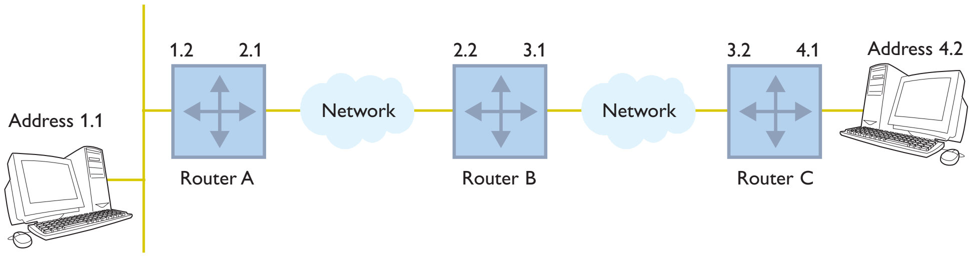
Router

The word route means to select or find the right path. A router is a device, or in some cases software in a computer, that determines where a packet should be sent on its way to the end destination (the router is the end destination from a LAN's perspective). Subsequently, the router is a network device that links together two or more logically separate networks. It does not connect networks blindly, but acts more as a packet switch for the interconnection of local networks over short or long distances. In addition to equipment being installed in separate networks, the network can also utilise different topologies and standards.



As all devices have a unique address, sending equipment can always address a special recipient in the same or in a different network. When a recipient in another network is addressed, the data is directed in an appropriate manner through a logical connection between the networks. This information is gathered in a routing table, which defines the routing and alternative connection options.

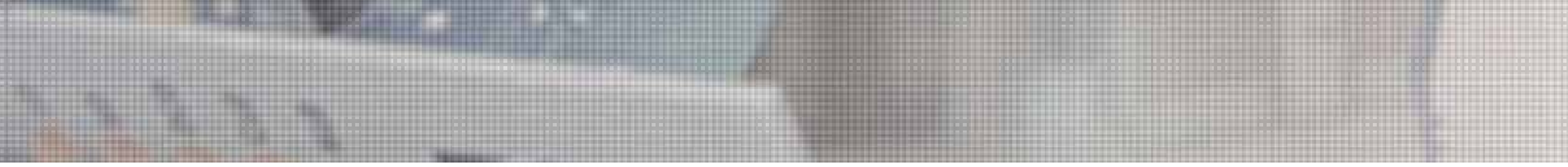
In the example opposite we adopt a simplified addressing technique. The network addresses are 1, 2, 3 or 4. Devices on the same network have the address 1.1, 1.2, etc.



Assume the computer with the address 1.1 wants to communicate with the computer at 4.2. Router A receives a packet addressed to 4.2, detects that the address belongs to another network, which results in the packet being routed forward, in this case to 2.1 and on to 2.2. The same procedure occurs between routers B and C. Finally the packet reaches router C and is transferred to network 4 to the computer with the address 4.2.

Besides routing traffic, there is usually the possibility to control and filter traffic. A routing table lists where different equipment and networks are located, a table can be

BACK



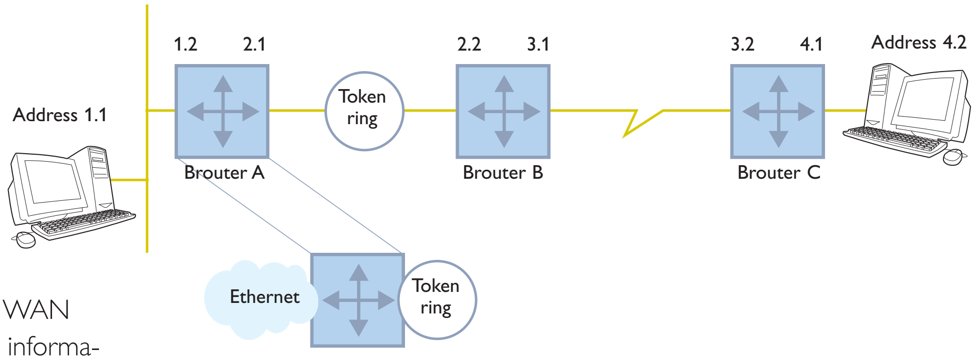
dynamic or static. A dynamic routing table is updated automatically based on the structure of the surroundings.

How the traffic should be routed is controlled by a routing protocol, e.g. RIP (**R**outing **I**nformation **P**rotocol) or OSPF (**O**pen **S**hortest **P**ath **F**irst).

Brouter

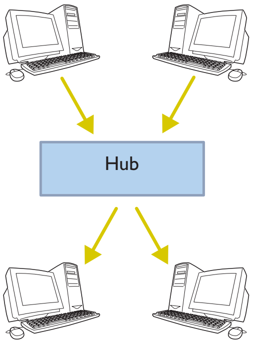
There are many standards on the market, the most common are Ethernet, Token ring and FDDI. All these use different communication techniques and formats, but addressing is common and standardised by IEEE.

A Brouter is a combination of a bridge and a router in the same device, many routers are really brouters. When the device needs to transfer the same protocol within a LAN, or to another LAN, the bridge function manages this. Alternatively, when a PC is connected to a WAN (**W**ide **A**rea **N**etwork), more information is needed about alternative connections so the device requires a routing table, in this way the brouter becomes a combination of a router and bridge.

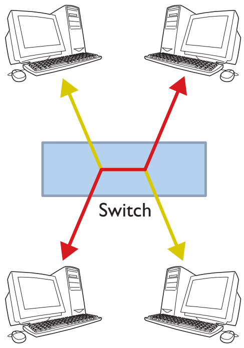


Hub

As the name implies this is a network device used as the central connection in a network. A hub works as a star coupler for network traffic. Data that comes in on one port, is sent to all others irrespective of who the recipient is. The hub was the network device that made 10baseT a success. It created completely new options for building networks, with centrally placed equipment and connection points at each workplace. There are two types of hubs, active and passive. A passive hub joins together network segments without amplifying the signal. An active hub acts in the same way as a passive hub, but also amplifies the signal.



BACK



Switch

A switch is similar to a hub in that it is the central connection point for the network. The difference is that the switch keeps track of which devices are connected to its respective ports. When data is sent to a device in the network, the recipient address is checked by the switch and data is only sent to the port where the device is connected (switched network). In this way the network is not overloaded with unnecessary traffic. Another advantage is an increase in security, as it is more difficult to access information that is not intended for the computer in question.

A layer 2 switch is a type of bridge.

A layer 3 switch is a type of router.

Consequently, in some contexts the terms switch, bridge and router are used synonymously.

Managed and unmanaged switches are other terms that are used regularly. The difference is that you can communicate with a managed (monitorable) switch, which normally takes place through SNMP, also refer to pages 138 to 143.

Gateway

A gateway connects together networks, but its main task is to convert data between different protocols, for example, between AppleTalk and TCP/IP. Apart from converting protocols, a gateway also supports different formats, character codes, addresses, etc.

Firewall

A firewall is special equipment or software that only forwards traffic when specific requirements have been met, other traffic is refused. This means that users in a network can be protected from prohibited traffic. Usually there is a firewall between a local network and the Internet. You can also have firewalls on internal networks or together with equipment that makes it possible to call into a network. Rules varying in degree of complexity are used to determine what the firewall allows to pass. When, where and how a firewall is used is controlled by the security requirements placed on the network. There are a large number of products on the market to choose between, from a combination of hardware and software solutions to firewalls that can be downloaded as "freeware" and used on your own computer.

BACK