

Manual

# TCP/IP-Ethernet



TCP/IP-Ethernet  
for Beginners

1<sup>st</sup> edition 11/1999 FT

This document is intended for anyone without expert knowledge of computer networks who wants to run Ethernet terminal devices under TCP/IP. It is divided into three sections.

- **Running TCP/IP-Ethernet**

Here the startup of TCP/IP Ethernet connections is explained step-by-step in the form of check lists. Anyone who conscientiously carries out each individual step will, even without background knowledge of PCs, be able to connect to a W&T Com Server under Windows (95/98 or NT).

- **Understanding TCP/IP-Ethernet**

Here you will find the essential background information on the subject of TCP/IP.

- **The little ABC book of networks**

Here we explain the key terms and abbreviations that you will encounter when working with networks.

All the important sequences and relationships are made easily understandable. If you would like to gain a more precise understanding of the steps described in the checklists, you are encouraged to first read the section *Understanding TCP/IP-Ethernet*.

Have no fear: We won't lose you in the details. We have intentionally limited ourselves to the things which are really important to understanding of the technologies in use here.

Just to start up TCP/IP network components it is after all unnecessary to know every protocol down to the last bit.

You can find additional reference material in the appendix to our DatenBuch and in our programming guide *Ready for Winsock in 1 Day*. This and other information sources can be ordered from us in printed versions or downloaded as a PDF file from our Web site at [www.WuT.de](http://www.WuT.de).

**© Copyright 11/1999 by Wiesemann & Theis GmbH**

All rights reserved.

Reprints, in whole or in part, is permitted if reference to the source, including Internet address ( W&T, *http://www.WuT.de*) is indicated.

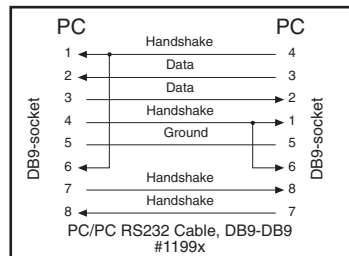
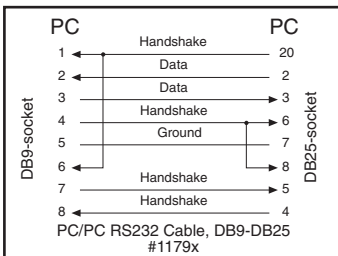
Microsoft, MS-DOS, Windows, Winsock and Visual Basic are registered trademarks of Microsoft Corporation.

In this section we will explain the startup of TCP/IP-Ethernet connections using several examples. If you work through the following checklists step-by-step, you will have no difficulty with startup.

## System prerequisites and needed components

You will always need:

- a PC running Windows 9x or Windows NT 4.0 with an installed Ethernet networking card and an available COM port
- a W&T Com-Server Model 58xxx
- a serial cable for connecting PC to PC
  - if 9-pin COM port
  - if 25-pin COM port



- Network connecting cable

If your PC is not yet connected in a network and the connection is to be made using coaxial BNC cable (10Base2), you need:

- 1 × BNC-BNC connecting cable 50 Ohm
- 2 × T-connectors 50 Ohm
- 2 × terminators 50 Ohm

If your PC is already connected in a network and the connection is to be made using coaxial BNC cable (10Base2), you need:

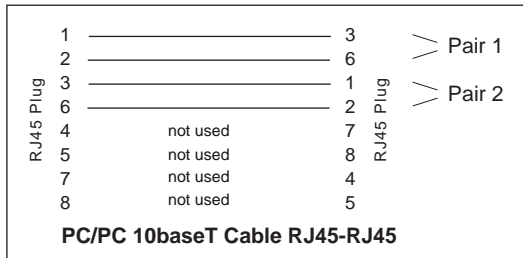
- a free BNC terminal, for example through an additional T-connector or an additional EAD cable. Check with your network administrator!

If your PC is not yet connected in a network and the connection is to be made using twisted-pair RS45 cable (10BaseT), you need:

- 2 × 10BaseT patch cables
- 1 × 10BaseT-HUB (star coupler)

or

- 1 × 10BaseT-Kabel „rotated“ with the following pin configuration:



If your PC is already connected in a network and the connection is to be made using twisted0pair RS45 cabale (10BaseT), you need:

- 1 × 10BaseT Patch cable
- a free 10BaseT port on a hub. Check with your network administrator!

### Determining/specifying IP addresses

The first thing to do is check whether the PC you are using is already configured for network operation under TCP/IP. If this is not the case, you must add TCP/IP support to the network properties.

If your PC is already connected in an Ethernet network, you should first find out whether applications are already being run in this network under TCP/IP. Here you should check with your network administrator to see whether an IP address has already been assigned for your PC or which IP addresses you can use for your PC and for the Com Server that you will be using.

If there are no TCP/IP components in your network, or your PC is not even networked, you can choose IP addresses as you desire, whereby the first three numbers should be the same (e.g. 172.16.232.23 for the PC and 172.16.232.49 for the Com Server). Use 255.255.0.0 for the subnet mask.

Please write down the values you are using:

IP address for PC: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_


IP address for Com-Server: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

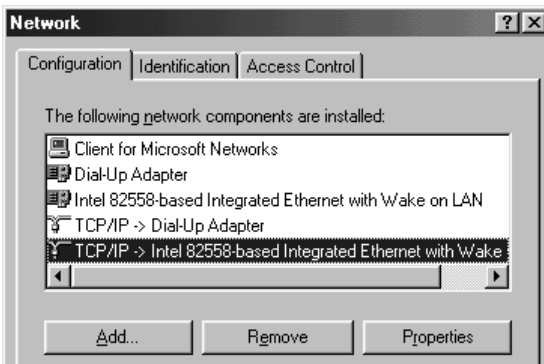
Subnet -Mask: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Gateway: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

## Installing and configuring TCP/IP under Windows 9x

You can skip this section if you are working under Windows NT.

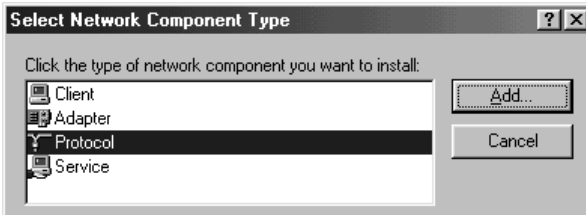
1. Click on *Start* and open the *Control Panel* under *Settings*.
2. Double click on the  network icon
3. Check to see whether *Network card* is listed in the *TCP/IP* configuration window.



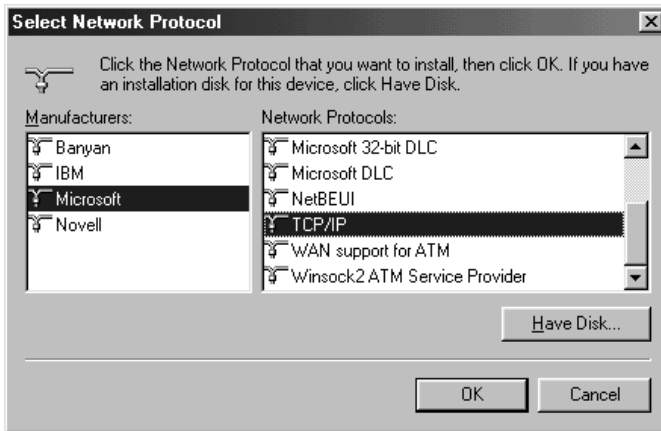
If the entry is there, skip to Point 5.

**Note:** *The entry TCP/IP->Dial-up Adapter is not sufficient to run Etghernet under TCP/IP!*

4. If the entry *TCP/IP-> „Network card“* is absent, click on *Add* and select *Protocol* in the following window.



Click on *Add* and in the following window select *Microsoft* as manufacturer and *TCP/IP* as the network protocol.

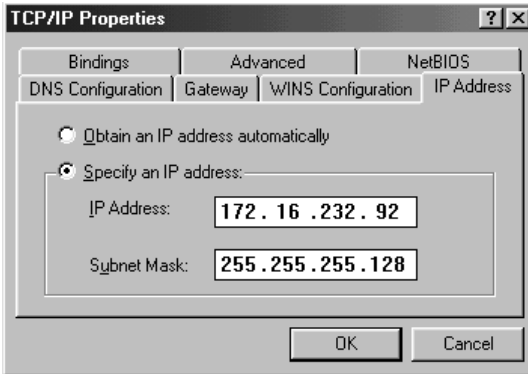


Confirm with *OK*.

**Note:** *To install the protocol you need the installation CD for your Windows version.*

5. Highlight *TCP/IP*-> “*Network card*“ and select *Properties*.

If there is already *TCP/IP* support, check the register *IP Address* to see whether the IP address and subnet-mask are correctly entered. Ask your network administrator whether the IP address is automatically obtained through *DHCP*. If not, enter the IP address and subnet-mask under *Properties* for the newly added *TCP/IP* address.




If there is already TCP/IP support, check under *Properties* in the *Gateway* register to see whether the gateway is correctly entered. For newly added TCP/IP support, enter the IP address of the gateway in the *New Gateway* field and click *Add*. Only if the entered gateway address appears in the lower window will it remain stored after confirming with *OK*.

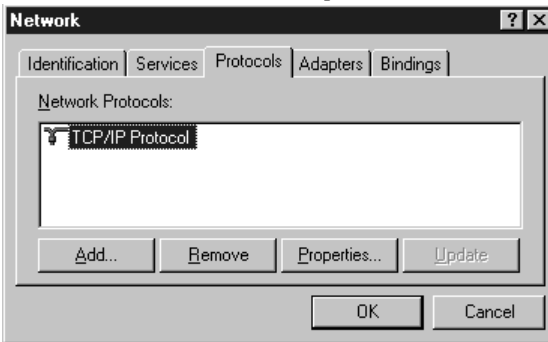


This concludes the installation of the TCP/IP support. To activate it you must first reboot the PC.

## Installing and configuring TCP/IP under Windows NT

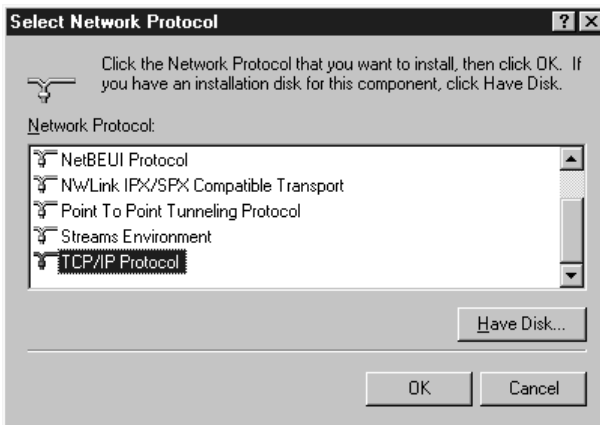
You can skip this section if you are working under Windows 9x.

1. Click on *Start* and open the *Control Panel* under *Settings*.
2. Double click on the  network icon
3. Check to see whether *TCP/IP protocol* is listed in the *Protocols* register.



If the entry *TCP/IP protocol* is present, skip to Step 5.

4. If the entry *TCP/IP->Protocol* is missing, click on *Add* and select *TCP/IP* in the following window.

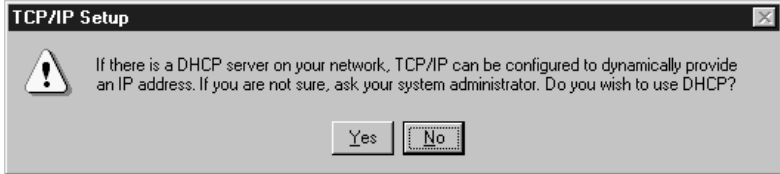


You now need the Windows NT installation CD.

After confirming with *OK*, the list of network protocols is expanded by the entry *TCP/IP Protocol*.

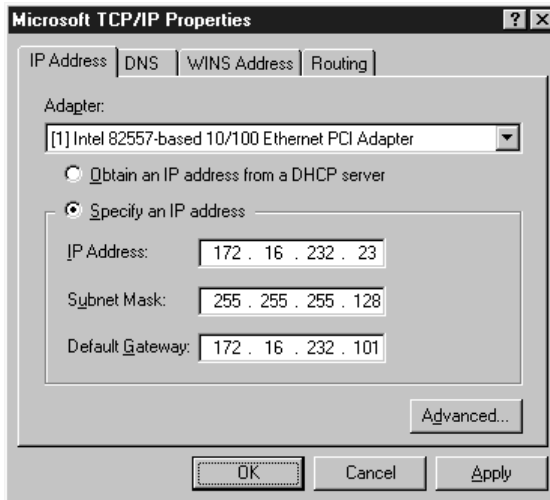
- For newly added TCP/IP support, click *OK* to configure the properties. If TCP/IP was already installed on your PC, highlight the entry *TCP/IP Protocol* and then click on *Properties*.

If you have newly installed TCP/IP support, the following message appears:



If your PC is already connected into a network, you need to check with your network administrator whether the DHCP service is supported. If not, click on *No*.

Enter the IP address, subnet-mask and gateway in the following window and confirm with *OK*. If the TCP/IP support was already present, you should now check whether the IP address, subnet-mask and gateway are correctly entered.



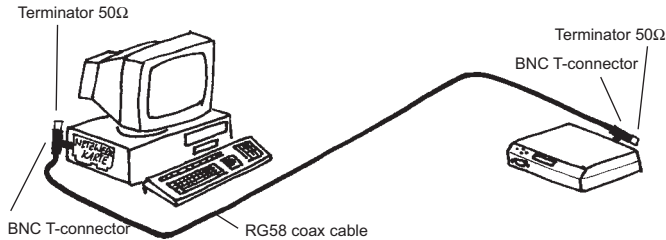
This concludes the installation of TCP/IP, and you are now prompted to reboot your PC.

## Connecting PC and Com Server to the network

**Caution:** All components must be turned off when connecting!

- Connecting PC <-> Com-Server without additional network linking using BNC cable (10Base2)

Connect as follows:



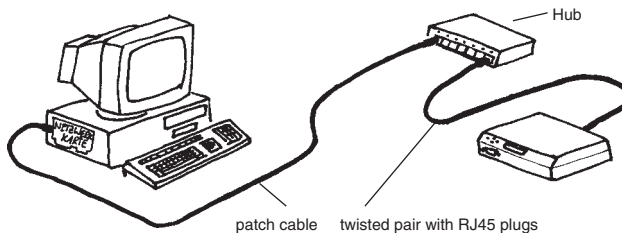
- Connecting PC <-> Com-Server using an existing 10Base2 network  
Connect the Com Server to an available BNC T-connector or EAD connecting cable. As you administrator!

**Caution:** Never simply disconnect the network in order to insert a BNC T-connector. Doing so will take down the entire network. Ask your administrator!

- Connecting PC <-> Com-Server without additional network linking using twisted-pair cable (10BaseT)

There are two ways to simply connect the PC to the Com Server:

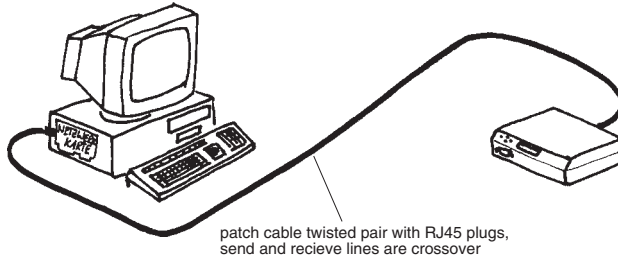
1. Connection through a hub. Connect as follows:



Both the PC and the Com Server are each connected to the hub through a patch cable.

## 2. Connecting through a crossed patch cable.

Connect the RJ45 terminals of the PC and Com Server using the crossed patch cable.



Using crossed patch cable creates a pure point-to-point connection which is not expandable.

- After the devices are connected, you may turn on the PC and Com Server. If you are using a Com Server with display, you should see *Mode Run* after a short time and also *Cable Coax* or *Cable TP* depending on the connection.

## Assigning the IP address to the Com Server

There are various ways to assign an IP address to the W&T COM Server.

### • Assigning the IP address using the display and keyboard

For Com Servers having a display it is advised to perform the entire configuration directly on the device using keyboard and display.

- Press the ↓ key until *SET TCPIP* appears on the display.
- Press the → key; *Box IP Number* appears in the display.
- Again press the → key and increment or decrement the individual digits of the IP address using the ↑↓ keys.
- After entering the complete IP address, hold down the OK key until *Saving* appears in the display.

The Com Server now has the specified address.

### • Assigning the IP address using a static entry in the ARP table

For Com Servers without a display but connected to an existing TCP/IP network, a static entry in the ARP table can be used to assign an IP address

to the Com Server. The stipulation is that the Com Server be connected in the same subnet as the PC. Check with your system administrator. In addition, you should ask your network administrator about the IP address for an additional network station.

The procedure described here for assigning an IP address only applies to assigning it for the first time. Changing the IP address later requires a different procedure.

- Open a DOS window on you PC.
- Enter

```
ARP -a
```

and confirm with Return..

If the ARP table does not contain any entries, such as

Internet Address	Physical Address	Type
172.16.232.92	00-80-48-9c-a3-62	dynamic
172.16.232.98	00-c0-3d-00-1b-26	dynamic

this message appears instead:

```
No ARP Entries Found
```

In this case it is absolutely necessary to „ping“ another network station in order to first create an entry in the ARP table.

- Type: ping <IP address of a different network station>

Example:

```
ping 172.16.232.92
```

The system responds:

```
Reply from 172.16.232.92 : . . . . .
```

Now you can continue with the assigning of the IP address.

- Type

```
ARP -s <new IP address> <Ethernet address of the Com Server>
```

Example:

```
arp -s 172.16.232.49 00-C0-3D-00-26-A1
```

**Note:** *The Ethernet address of the Com Server can be found on a sticker on the back of the housing.*

- Finally type:  
ping <IP address which the Com Server is to receive>

Example:

```
ping 172.16.232.49
```

The system responds:

```
Reply from 172.16.232.49 : .....
```

The Com Server now has the intended address.

- **Assigning the IP address through the serial port**

If your Com Server does not have a display, you can also use the serial (RS232) port to assign the IP address.

- Connect the serial (RS232) port on the Com Server to a free COM port on your PC using a serial PC-to-PC cable.
- Start a terminal program – such as Hyperterminal – on your PC which you can use to communicate through a COM port.
- In the terminal program select the COM port to which the Com Server is connected.
- Set the following parameters:  
9600 baud,8 bits,no parity, no handshake.
- Press the Reset button on the Com Server or momentarily interrupt power and type the letter *x* in the terminal program until the Com Server sends *IP no.+<Enter>*.
- Enter the desired IP address without leading zeros and confirm with Return. Your entries will not appear on the screen!
- The Com Server confirms that it has accepted the address by sending it out on the serial interface.

The Com Server now has the desired address.

## Entering subnet mask and gateway

To integrate Com Servers into an existing network, the subnet mask and gateway address also need to be entered.

- Open a DOS window and enter:

```
telnet <IP address of the Com Server> 1111
```

Example:

```
telnet 172.16.232.49 1111
```

- The following screen appears at the Telnet client:

```
*****
*           W&T - Com Server           *
*****

1. INFO System
2. SETUP System
3. SETUP Port 0 (Serial)
4. SAVE Setup
```

Press <No.+ ENTER> (q=quit):

- Enter 2 for *Setup System* and confirm with Enter.
- Enter 1 for *Set TCPIP* and confirm with Enter.
- Enter 2 for *Subnet-Mask* and confirm with Enter.
- Enter the desired subnet mask and confirm with Enter.
- Enter 3 for *Gateway* and confirm with Enter.
- Enter the desired gateway address and confirm with Enter.
- Press Enter twice to return to the Main Menu.
- Enter 4 for *Save Setup* and confirm with Enter to save the changes.
- Answer *Y* to the question *Save Changes?*.

The Com Server is now configured for use in the network.

**Note:** *The menu may be slightly different from model to model. You can still carry out the necessary steps with no problem by referring to the user's guide.*

## Establishing a telnet connection to the serial port of a Com Server

In this example we will create the connection between a Telnet application and a serial terminal application.

The connection path is such that a Telnet connection is made from the PC to the network side of a Com Server. The serial port of the Com Server is connected using a serial PC-PC cable to a free COM port on the PC.

Follow these steps in order:

- Connect the serial (RS232) port on the Com Server (Port A) to an available COM port on your PC using a PC-PC cable.
- Start a terminal program on your PC which can communicate through a COM port (such as Hyperterminal).
- Choose the COM port in the terminal program to which the Com Server is connected.
- Set the following parameters:
  - 9600 baud, 8 bits, no parity, no handshake.
- Open a DOS window and enter:  
telnet <IP address of the Com Server> 1111

Example:

```
telnet 172.16.232.49 1111
```

- When the configuration menu appears, select 3 for *Port 0* and then 2 for *UART Setup*. Both entries must be confirmed by pressing Enter.
- Compare the displayed transmission parameters with those in the terminal program. If these do not agree, follow the menu to adjust the parameters as needed.
- Press Enter until you are again in the starting menu.
- If everything is configured correctly, select 4 to save the entered transmission parameters in the Com Server.
- Quit the Telnet connection with *q*.
- Enter the following in the DOS window:  
telnet <IP address of the Com Server>

Example:

```
telnet 172.16.232.49
```

- The following then appears in the telnet window:

```
*****
*           W&T - COM SERVER           *
*****
```

- This means the telnet connection to the Com Server has been made.
- Now all the characters you enter in the telnet window appear in the window of the terminal program. All the characters you enter in the terminal program also appear in the telnet window.



- To end the telnet connection, select *Disconnect* in the *Connect* menu. If you are using a 4-port Com Server and also want to make telnet connections with the other ports, you must specify one of the following port numbers as additional parameters when opening the telnet application:

Port B = 6100  
Port C = 6200  
Port D = 6300

When calling up telnet enter the following in the DOS window:

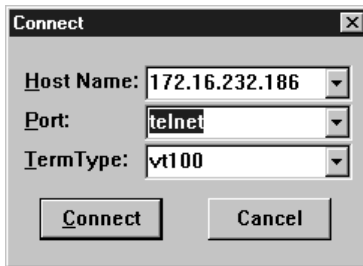
```
telnet <IP address of the Com Server> <Port no.>
```

Example for Port B:

```
telnet 172.16.232.49 6100
```

To change the port while in the already opened telnet application select *Network system...* in the *Connect* menu.

The following configuration window appears:



Instead of *telnet*, enter here under Connection the port number of the desired COM port; everything else works exactly the same as in the case of Port A.

**For additional application examples for connections using FTP, Berkley-Sockets etc., see the user's guide for the W&T COM Server.**

Just a few years ago the only places computer networks could be found were in banks, agencies and larger companies. The network components used were usually hardly affordable, and installation and administration required the services of specially trained technicians.

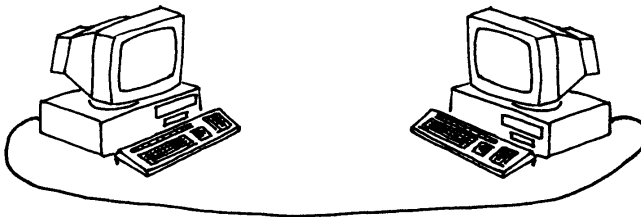
But since the 90's computers – especially PCs – have rapidly entered every area of daily life; a steadily growing volume of data contributed significantly to the spread and use of computer networks.

Parallel to this development was the explosive growth of the Internet, which today even private individuals have no trouble using.

All this has led to a situation where the possibility of accessing computer networks is a standard part of modern operating systems. There are two givens in this scenario: Ethernet as the physical basis and TCP/IP as the protocol.

## Requirements for a computer network

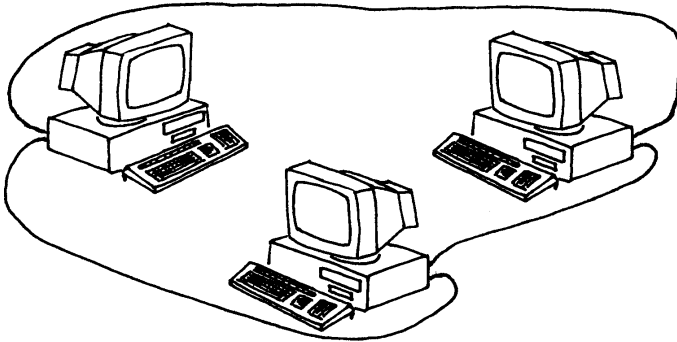
Every user of a computer has certainly had experience connecting two terminal devices together, such as PC and printer, PC and modem, or PC and PC. The connection is made using a cable specially designed for the application, through which data are sent back and forth between the two devices.



You can also imagine it this way: Two pen pals send letters to each other, and a messenger is always assigned the task of getting these letters to the respective mailboxes. In this simplified example neither an envelope nor the address of the sender is necessary.

The procedure is uncomplicated and functions without any hitches. Only the actual user data are sent. This type of connection is also called point-to-point connection. You could also use point-to-point connection to have

three PCs talk to each other. For this you would need a cable for connecting the two other PCs.



To send letters between three pen pals you would need three messengers for this procedure..

But when four PCs are involved you would already need six cables, and if you wanted to „network“ ten or more PCs this way, the result would be an impossible tangle of cables. Not to mention the fact that any change in such a network would result in an avalanche of changes in the cabling.

In other words: implementing such a network is hardly practical.

A computer network should, using the least possible materials and cables, employ existing resources (memory, databases, printers and other miscellaneous terminal devices) to make an indefinite number of connected users accessible. Plus you need the highest possible degree of data security and transmission speed.

The response to these requirements are the network standards which are in common usage today.

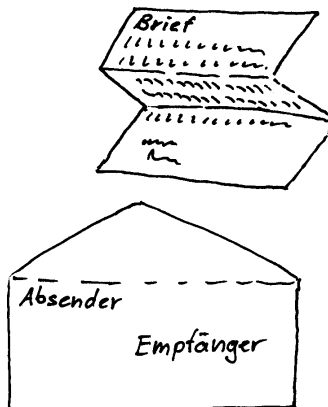
## Basic functions of networks

All network topologies have one basic thing in common:

Every network participant has its own address. The actual data are „packed“ into a frame of additional information (e.g. recipient address, sender address and checksum).

The address information in the resulting data packets can be used to get the actual data to the correct recipient over commonly used paths.

The example of a letter is not really different: You put the letter in an envelope with the sender and receiver address. The letter carrier then knows where to deliver the letter; and the recipient can tell where it came from and reply if needed.



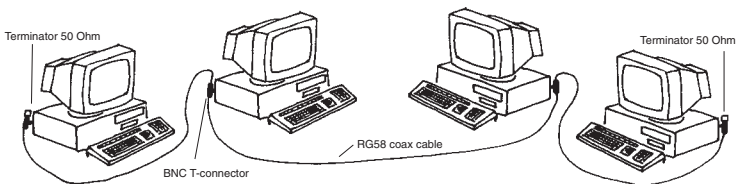
In data transfer within a network, the receiver has the additional option of verifying the contents of the data for completeness using a checksum.

## Ethernet and FastEthernet

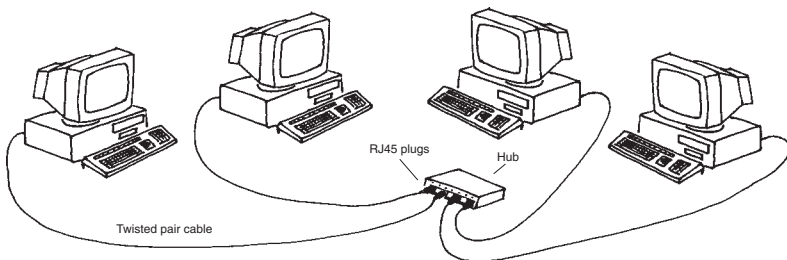
Ethernet is today the most widely used network standard. As early as 1996 around 86% of all existing networks were implemented using this technology.

Ethernet originally ran at a transmission speed of 10Mbit/s. There are three basic physical models:

**10Base2** Also known as Thin Ethernet, Cheapernet, or simply BNC network. All the stations are interconnected through a coax cable (RG58, 50 Ohm wave impedance). The cable must be terminated on both ends with a 50-Ohm terminator.



**10BaseT** Each participant is connected to a so-called hub (star distributor) which passes all data packets along equally to all stations. 10BaseT is thus star-shaped physically, but works logically like 10Base2 on a bus principle.



**10Base 5** Often referred to as „Yellow Cable“; was the original Ethernet standard and is hardly used today.

In response to increasingly large data quantities, the 90's saw the development of Fast Ethernet with a transmission speed of 100Mbit/s; here there are two basic physical models:

**100Base T4** Just as in 10BaseT each station is connected to a hub through its own twisted-pair cable, with the hub passing all data packets to all stations. 100BaseT4 is hardly ever used any more in new installations.

**100BaseTX** represents today's usual standard for 100Mbit networks. 100BaseT4 and 100BaseTX differ only on the physical level in the method of data transmission. In addition, 100BaseTX requires higher quality cable.

You can find more detailed specifications for Ethernet and the various physical topologies in the W&T Data Book.

Whichever basic physical model used, the logical structure of the data packets is the same for all Ethernet topologies. All stations in a local network receive all the data packets including those which are intended for the other stations (with the exception of *Switch*, cf. Appendix), but only process those packets which are actually addressed to them.

The Ethernet address – also called MAC-ID or node number – is „burned“ into the physical Ethernet adapter (network card, printer server, Com Server, router ...) by the manufacturer, so it is fixed for each terminal device and may not be changed. The Ethernet address is a 6-byte value which is generally expressed as a hex number.

e.g. 00-C0-3D-00-27-8B


The first three hex values represent the manufacturer's code, and the last three are numbered serially by the manufacturer..

**Every Ethernet address is unique in the world!**

There are four different types of Ethernet data packets, which are used depending on the application:

<i>Data packet type</i>	<i>Application</i>
Ethernet 802.2	Novell IPX/SPX
Ethernet 802.3	Novell IPX/SPX
Ethernet SNAP	APPLE TALK Phase II
Ethernet II	APPLE TALK Phase I, TCP/IP

In general, Ethernet data packets of the type Ethernet II are used in connection with TCP/IP. Here is how an Ethernet II data packet is constructed:

 ...	<b>00C03D00278B</b>	<b>03A055236544</b>	<b>0800</b>	<b>user data</b>	check-sum
Preamble	Destination	Source	Type	Data	FCS

**Preamble** The bit sequence with constant alternating between 0 and 1 is used for identifying the start of the packet and for synchronization. The end of the Preamble is indicated by the bit sequence 11.

**Destination** Ethernet address of the recipient.

**Source** Ethernet address of the sender..

**Type** Indicates the higher-order application (e.g. IP = Internet Protocol = 0800h).

**Data** User data.

**FCS** Checksum.

The structure of the other Ethernet packets differs only in the *Type* and *Data* fields, to which a different function is assigned according to the packet type. This means an Ethernet data packet possesses all the necessary properties for sending data in local networks from one station to another.

Ethernet alone is not however capable of addressing different networks. In addition, Ethernet works connectionless: the sender does not receive any confirmation from the recipient that the packet actually arrived.

Higher-order protocols such as TCP/IP need to be used in any case if an Ethernet network has to be connected with multiple networks.

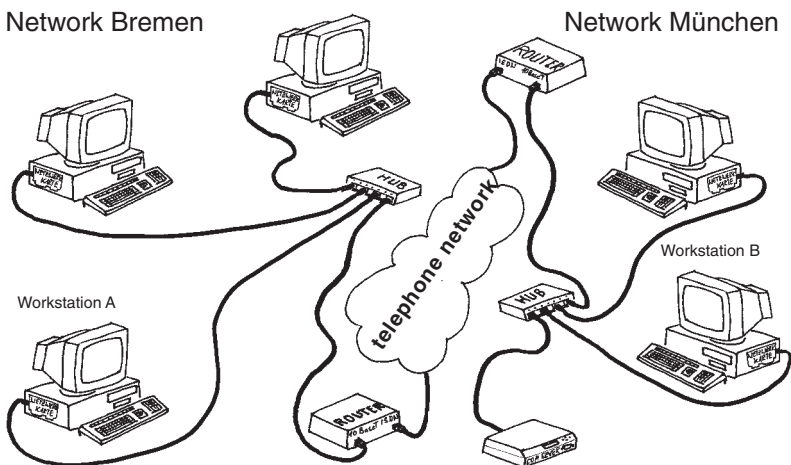
## TCP/IP – the most important protocols

As far back as the 1960's the American military gave out the assignment of creating a protocol which would enable a standardized exchange of information between any number of various networks regardless of the hard- and software used. The result of specification was TCP/IP protocol, which was introduced in 1974.

Although TCP and IP are always named together, they are really two complementary protocols. The Internet protocol IP takes over the actual addressing and delivery of the data packets, while the overlying Transport Control Protocol TCP is responsible for transporting the data and making it secure.

## IP – Internet Protocol

Internet Protocol makes it possible to assemble an indefinite number of individual networks into an overall network. This means it enables data exchange between any two network stations located respectively in any given individual network. The physical implementation of the networks and transmission paths (Ethernet, token ring, ISDN ...) is immaterial here. The data are sent to the recipient regardless of these differences.



## IP addresses

Under IP every network station has a unique Internet address, often referred to as an „IP No.“. This Internet address is a 32-bit value that for better readability is always expressed in the form of four decimal numbers (8-bit values) separated by decimal points (dot notation).

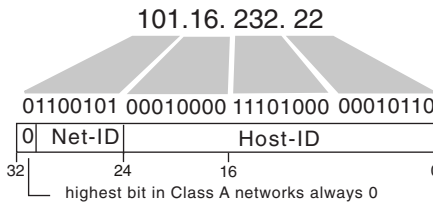
The Internet address is divided into Net ID and Host ID, whereby the Net ID is used for addressing the network and the Host ID for addressing the network station within a network.

Telephone numbers are constructed similarly. There also a distinction is made between the area code and the subscriber’s number.

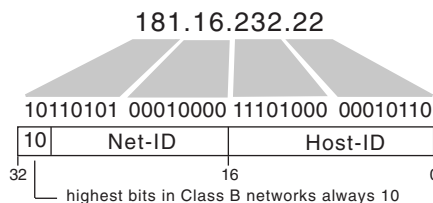
Which part of the IP address belongs to the Net ID and which to the Host ID depends on the size of the network.

Addressing normal networks involves one of three network classes:

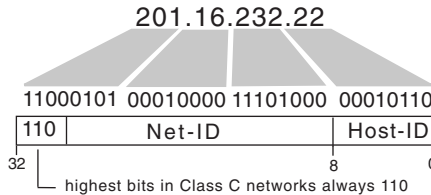
**Class A:** The first byte of the IP address is used for addressing the network, and the last three bytes address the network station.



**Class B:** The first two bytes of the IP address are used for addressing the network, and the last two bytes address the network station.



**Class C:** The first three bytes of the IP address are used for addressing the network, and the last byte for addressing the network station.



The following table lists the basic information for the different network classes:

	possible values of network addresses	possible number of networks	possible number of hosts/network
Class A	1.xxx.xxx.xxx–126.xxx.xxx.xxx	125 ( $2^7$ )	approx. 16 000 000 ( $2^{21}$ )
Class B	128.0.xxx.xxx–191.255.xxx.xxx	approx. 16 000 ( $2^{14}$ )	approx. 65 000 ( $2^{16}$ )
Class C	192.0.0.xxx–223.255.255.xxx	approx. 2 000 000 ( $2^{21}$ )	254 ( $2^8$ )

In addition to those listed above, there are also Class D and Class E networks whose address ranges lie above the Class C networks. Class D and Class E networks have little significance in practice, since they are used only for research purposes and special tasks. The normal Internet user will never come into contact with these classes.

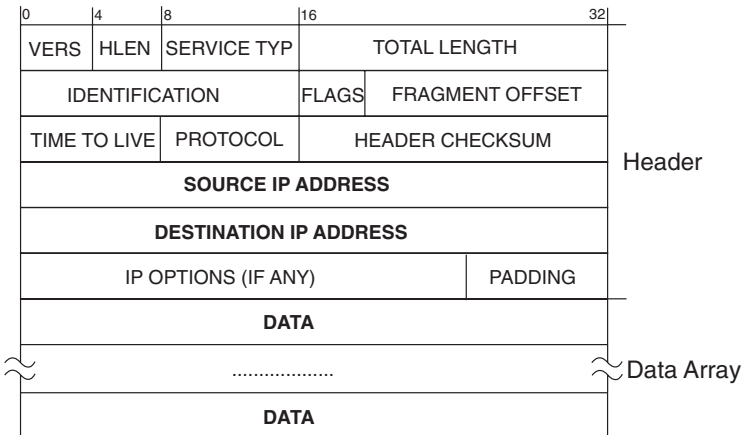
For networks which are to be directly linked with the Internet, a commission called InterNIC assigns an available Net ID and decides based on the intended network size which network class applies. The network operator (administrator) is free to select the assignment of the Host ID to the network station and the resulting IP address. He must however keep in mind that an IP address can be assigned only once at a time.

**Caution:** *An IP address must be unique within the entire interconnected network!*

## IP Data Packets

The user data are also packed into a frame of addressing information when data are sent over the Internet. IP data packets contain in addition to the user data a variety of address and additional information located in the so-called „header“.

Structure of an IP packet



We will restrict ourselves here to explaining the most important address information:

**source IP address:** IP address of the sender

**destination IP address:** IP address of the recipient

## TCP – Transport Control Protocol

Because IP is an unsecured, connectionless protocol, it generally works together with the overlaid TCP, which takes over security and handling of the user data.

TCP establishes a connection between two network stations for the duration of the data transmission. When establishing the connection, conditions such as the size of the data packets are specified, which then apply to the entire connection session.

TCP can be compared with a telephone connection. Participant A dials Participant B; Participant B accepts the connection by picking up the handset, and this connection remains until ended by one of the participants.

TCP works on the so-called **Client-Server principle**:

Whichever network participant establishes the connection (takes the initiative) is called the client. The client makes use of a service offered by the sever, whereby depending on the service one server can accomodate several clients at one time.

The participant to whom the connection is made is called the server. A server does nothing on his own, but just waits for a client to make contact with him.

In reference to TCP, the terms TCP Client and TCP Server are used.

TCP verifies the sent user data with a checksum and assigns a sequential number to each sent packet. The receiver of a TCP packet uses the checksum to verify correct receipt of the data. Once a TCP server has correctly received a packet, a predetermined algorithm is sued to calculate an acknowledgement number from the sequential number. The acknowledgement number is returned to the client with the next packet it sends as an acknowledgement. The server likewise assigns a sequential number to the packets it sends, which is then in turn acknowledged by the cilient with an acknowledgement number.

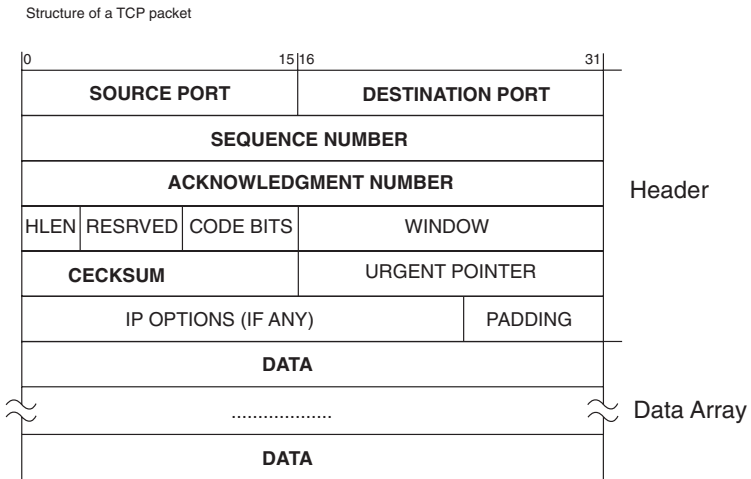
All of this ensures that any loss of TCP packets will be noticed, and that if needed they can be resent in the correct sequence.

In addition, TCP directs the user data on the destination computer to the correct application program by accessing various applications – also called services – through various port number. Thus telnet for example can be rea-

ched thorough Port 23, and FTP through Port 21.

If one compares a TCP packet with a letter to an official agency, the port number would correspond to the room number at the office building. If for example the Sanitation Department is located in Room 312 and you address a letter to this room, you are already indicating that you wish to use the services of the Sanitation Department.

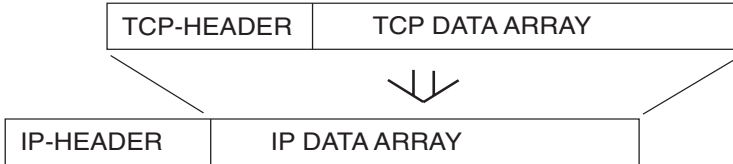
Like IP, TCP also packs the user data into a frame containing additional information. Such TCP packets are constructed as follows:



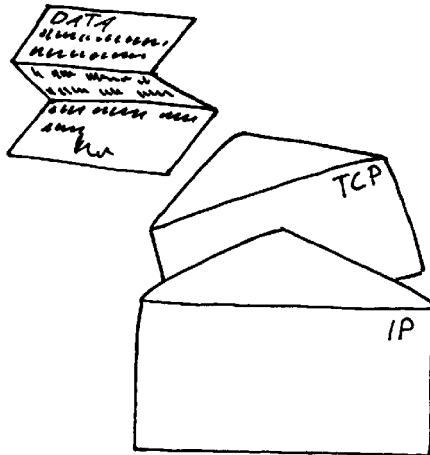
- Source Port:** Port number of the sender's application
- Destination Port:** Port number of the receiver's application
- Sequence No:** Offset of the first data byte relative to the start of the TCP flow (guarantees that the sequence is maintained)
- Acknowl. No:** Sequence No. expected in the next TCP packet
- Data:** User data

This TCP packet is inserted into the data array of the IP packet..

Construction of a TCP/IP data packet



The user data are placed in something like an envelope (TCP packet), which in turn is placed in another envelope (IP packet).



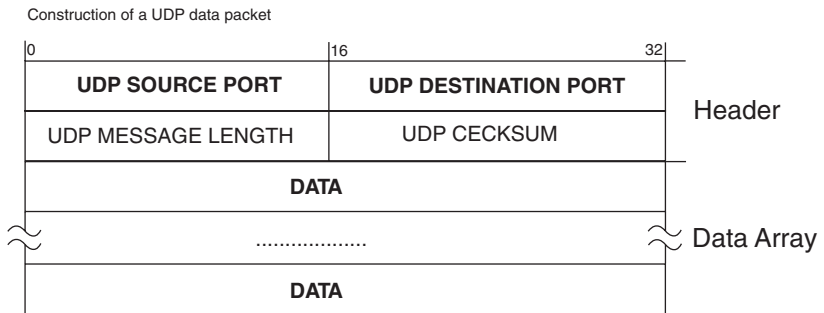
## UDP User Datagram Protocol

UDP is another transport protocol, which like TCP lives above IP.

But in contrast to TCP, UDP is connectionless. Each data packet is treated like a separate mailing, and there is no confirmation as to whether a packet was received.

Since UDP does not require connections to be established and broken off and therefore no timeout situations can arise, UDP can be faster than TCP: if a packet is lost, data transmission will continue unhindered as long as there is a higher protocol responsible for repetitions.

Data integrity under UDP should in any case be handled by the application program.



**Source Port:** Port No. of the sending application (reply port for receiver).

**Destination Port:** Target port at the receiver where the data should arrive.  
The rule of thumb is:

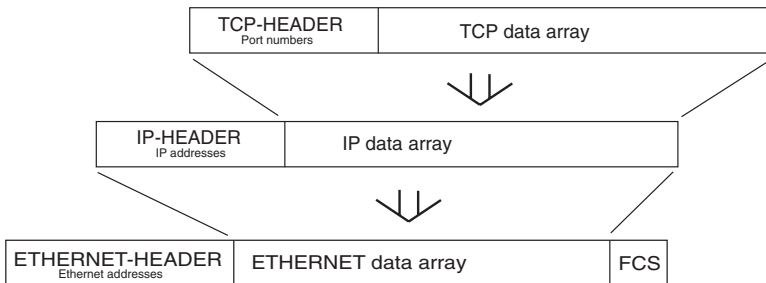
- TCP is generally used for continuous data streams or large quantities of data, as well as in situations where a high degree of data integrity is required.
- UDP makes sense when transmission parameters are changing frequently and when data integrity can be assured by a high-order protocol.

## TCP/IP Ethernet

TCP/IP is a purely logical protocol and always needs a physical foundation. As already mentioned earlier, Ethernet is the most widely used of the physical network topologies. This is also why you find Ethernet as the physical basis in most TCP/IP networks.

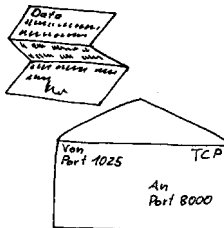
TCP/IP and Ethernet are merged by embedding each TCP/IP packet into the data array of an Ethernet packet.

Construction of a TCP/IP-Ethernet data packet

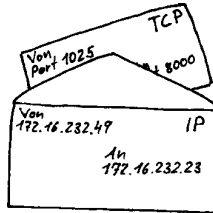


The user data pass through several driver levels on their way from the application on the PC into the network:

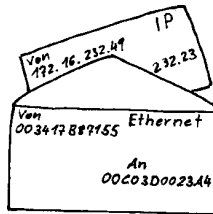
- The application program decides which other network stations should receive the data, and hands the IP address and TCP port number to the TCP/IP driver (also called the TCP/IP stack).
- The TCP/IP driver coordinates the organization of the TCP connection.
- The user data handed over by the application program are divided depending on size into smaller, transmittable blocks.
- Each data block is first packed by the TCP driver into a TCP packet.



- The TCP driver hands over the TCP packet and the IP address of the target to the IP driver.
- The IP driver packs the TCP packet into an IP packet.



- The IP driver looks up the Ethernet address of the target specified by the IP address (more on this later) in the so-called ARP table (Address Resolution Protocol) and hands the packet together with the determined Ethernet address to the Ethernet card driver.
- The Ethernet card driver packs the IP packet into an Ethernet packet and sends this packet to the network through the network card.



At the receiver end the procedure is carried out in reverse order:

- The Ethernet card recognizes from the destination Ethernet address that the packet is intended for the network station and passes it to the Ethernet driver.
- The Ethernet driver isolates the IP packet and passes it to the IP driver.
- The IP driver isolates the TCP packet and passes it to the TCP driver.
- The TCP driver checks the contents of the TCP packet for correctness and passes the data using the port number to the correct application.

This multi-layered transmission procedure may seem incredibly complicated at first glance. But only such strict separation of logical protocol (TCP/IP) and physical protocol (Ethernet) makes it possible to exchange data among networks and independent of hardware considerations.

## ARP – Address Resolution Protocol

As we have seen, the IP driver hands both the IP data packet and the physical Ethernet address to the Ethernet card driver. To determine the Ethernet address of the target, the IP driver uses Address Resolution Protocol (ARP).

Every TCP/IP-capable computer contains an ARP table. The ARP table is updated as needed by the TCP/IP driver and contains the relationship of IP addresses to Ethernet addresses.

Internet Address	Physical Address	Type
172.16.232.23	00-80-48-9c-ac-03	dynamic
172.16.232.49	00-c0-3d-00-26-a1	dynamic
172.16.232.92	00-80-48-9c-a3-62	dynamic
172.16.232.98	00-c0-3d-00-1b-26	dynamic
172.16.232.105	00-c0-3d-00-18-bb	dynamic

When an IP packet needs to be sent, the IP driver first looks to see whether the desired IP address is already contained in the ARP table. If yes, the IP driver passes the determined Ethernet address together with its IP packet to the Ethernet card driver.

If the desired IP address can't be found, the IP driver initiates an ARP request. An ARP request is an all-call (also referred to as a broadcast) to all the stations in the local network.

To make sure the broadcast is noticed by all the network stations, the IP driver uses FF FF FF FF FF FF as the Ethernet address. An Ethernet packet addressed with FF FF FF FF FF FF is always read by all network stations. The desired IP address is specified in the IP packet as the destination, and the identifier for ARP is indicated in the Protocol field of the IP header.

Whichever network station recognizes its own IP address in this ARP request confirms this with an ARP reply. The ARP reply is a data packet addressed to the ARP request sender on both the Ethernet level and the IP level, with the ARP identifier in the Protocol field.

The IP driver can now associate the Ethernet address obtained from the ARP reply with the desired IP address, and enters it in the ARP table.

In normal situations the entries do not remain permanently in the ARP table. If an entered network station is not contacted within a certain time (around

2 min. under Windows), the corresponding entry is deleted. This keeps the ARP table streamlined and allows exchange of hardware components while maintaining the IP address. These time-restricted entries are also referred to as dynamic entries.

In addition to dynamic entries there are also static entries, which the user himself creates in the ARP table. The static entries can be used for passing the desired IP address to new network components which do not yet have an IP address.

This type of IP address assigning is also supported by Com Servers:

If a Com Server which does not yet have its own IP address receives an IP data packet which was addressed to it on Ethernet, the IP address of this packet is processed and accepted as its own IP address.

**Caution:** *Not all network components have this capability. PCs for example are not configurable in this way!*

Now we know what information is needed for a TCP/IP Ethernet connection in the local network. What we don't have yet is the information for allowing an extra-network connection.

## Gateway and Subnet Mask

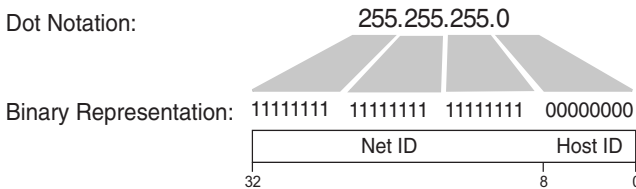
Whether a receiver to whom the connection is to be made is located in the same network as the sender is recognized from the Net ID - the part of the IP address which addresses the network. If this part of the IP address is the same for the sender and receiver, then both reside in the same network, and if there is no agreement, then the receiver can be found in a different network.

The various individual networks are connected to each other through gateways/routers, together forming the Internet.

For network classes A, B and C it is clearly defined which part of the IP address is the Net ID and which the Host ID.

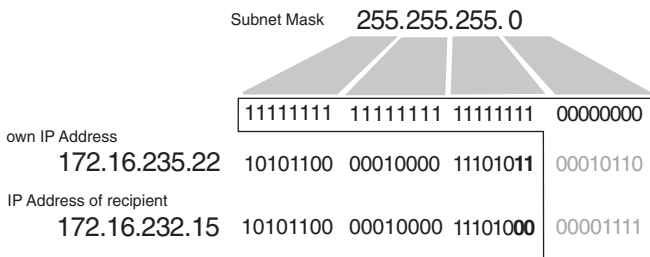
It is however possible to divide a network - regardless of which network class - into sub-networks. But the Net ID provided by the individual network classes is not sufficient for addressing such subnets; you must allocate a part of the Host ID for addressing the subnets. In plain English this means that the Net ID gets bigger and the Host ID correspondingly smaller.

Which part of the IP address is interpreted as the Net ID and which part as the Host ID is specified by the subnet mask. Just like the IP address, the subnet mask is a 32-bit value represented in dot notation. If you look at the subnet mask in binary format, the Net ID section is filled with 1's and the Host ID section with 0's.



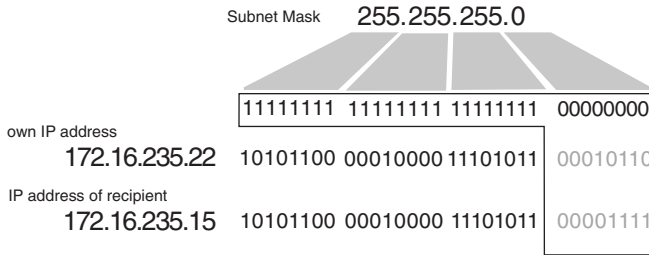
Before each data packet is sent, the IP driver compares its own IP address with that of the receiver. In this process the bits in the Host ID are masked over the part of the subnet mask which is filled with zeros.

If the interpreted bits are identical in both IP addresses, the selected network station is located in the same subnet.



In the example above the IP driver can determine the Ethernet address through the ARP and pass it to the network card driver for direct addressing.

But if even one of the processed bits is different, the selected network station does not live in the same subnet. In this case the IP packet must be passed for further transmission to the target network through the gateway or router.



The IP address of the desired network station is entered in the IP packet. The IP driver uses the ARP to determine not the Ethernet address of the desired network station, but rather the Ethernet address of the router.

Gateways and routers are basically nothing more than computers having two network cards. Ethernet data packets which are received at card A are unpacked by the Ethernet driver, and the received Ip packet is passed to the IP driver. This verifies whether the target IP address belongs to the subnet connected to card B and the packet can be delivered directly, or whether the IP packet needs to be passed to a different gateway.

In this way a data packet can pass through several gateways or routers on its way from one network station to another. Whereas on the IP level the IP address of the receiver is entered along the entire path, on the Ethernet level only the next gateway is addressed. The Ethernet address of the receiver is only inserted into the Ethernet packet on the link from the last gateway/router to the receiver.

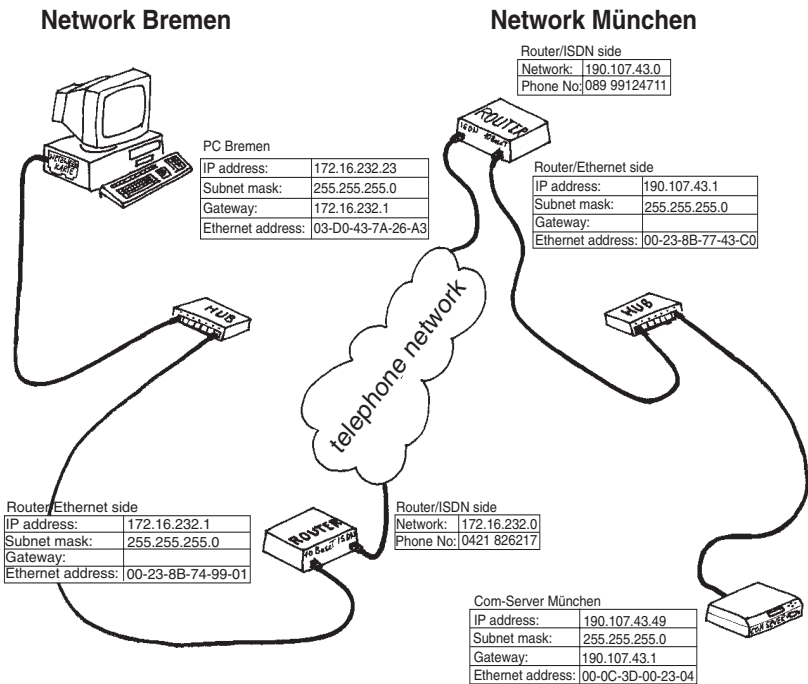
In addition to routers which connect one Ethernet subnet with another Ethernet subnet, there are routers which change the physical medium - for example from Ethernet to token ring or ISDN. While the IP addressing remains the same over the entire route, the physical addressing vom one router to another is adjusted to the physical conditions required on the links.

Telephone numbers may be used for example for addressing between two Ethernet-ISDN routers.

## Supra-network TCP/IP connection

In the following section we will use an existing telnet connection to describe the path of a character through a routed network connection.

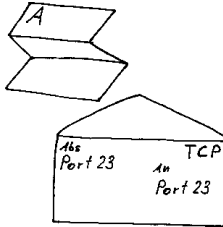
We assume in our example that a user in Bremen already has a telnet connection established to a W&T COM Server in Munich; the Bremen-Munich network connection exists in the form of a router connection over the ISDN network.



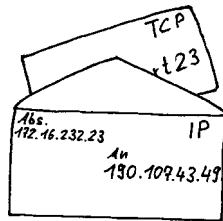
The user in Bremen enters the character „A“ in the telnet client application.

- The telnet client program on the PC hands the „A“ as user data to the TCP/IP stack. The IP address of the receiver (190.107.43.49) and Port No. 23 for telnet were already passed to the TCP/IP stack when the connection was established.

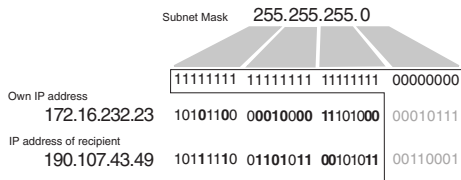
- The TCP driver writes the „A“ to the data array of a TCP packet and enters 23 as the destination port.



- The TCP driver hands the TCP packet and the IP address of the receiver to the IP driver.
- The IP driver packs the TCP packet into an IP packet.



- The IP driver compares the Net ID sections of its own IP address with the IP address of the receiver to determine whether the IP packet can be delivered in its own subnet or must be handed over to a router.

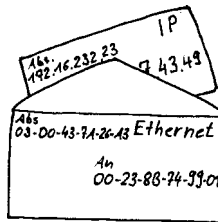


Here the Net ID sections of the two addresses are not the same; the IP packet must therefore be passed along to the specified router.

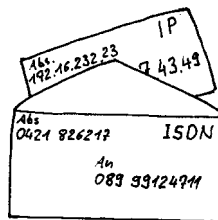
- The IP driver determines the Ethernet address of the router from the ARP. Since the TCP connection is already established, the IP address of the router will already be contained in the ARP table.

Internet Address	Physical Address	Type
→ 172.16.232.1	00-23-8B-74-99-01	dynamic
172.16.232.49	00-c0-3d-00-26-a1	dynamic
172.16.232.92	00-80-48-9c-a3-62	dynamic

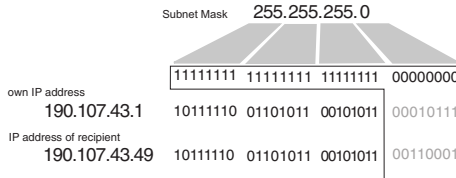
- The IP driver takes the Ethernet address of the router from the ARP table and passes it together with the IP packet to the Ethernet card driver.
- The Ethernet card driver packs the IP packet into an Ethernet packet and sends this packet through the network card to the network.



- The router removes the IP packet from the Ethernet packet it just received.
- The IP address of the receiver is compared against a so-called routing table. Based on this routing table the ISDN router decides which call number belongs to the network in question. Since the TCP connection already exists, the ISDN connection is also likely to be already established at this point. But if this is no longer the case, the router dials the number taken from the routing table and creates the ISDN connection to the counterpart router in the target network.
- In the ISDN network as well the IP packet is packed into a frame of address information. All that interests us here is that it goes unchanged in its address range into the ISDN packet.

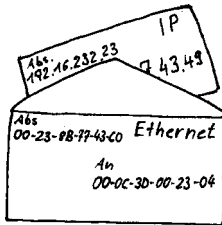


- The router in the destination network takes the IP packet from the ISDN packet. IP addresses and the subnet mask are used to determine whether the received IP packet can be delivered in the local subnet, or whether it has to be passed along to an additional router.



In our example the IP packet reached the destination network and can be addressed in the local network over the Ethernet.

- The router, which also maintains an ARP table, uses the ARP to determine the Ethernet address which is appropriate to the IP address and packs the IP packet - whose address range is still unchanged - into an Ethernet packet.



- The COM server recognizes from the destination Ethernet address that the packet belongs to it, and removes the IP packet.
- The IP driver in the COM server isolates the TCP packet and passes it along to the TCP driver.
- The TCP driver checks the contents of the TCP packet for integrity and passes the data - in this case the letter „A“ - to the serial driver.
- The serial driver sends the „A“ out on the serial port.

In a TCP connection the correct receipt of a data packet is confirmed by returning an Acknowledgement No. The acknowledgement packet travels over the entire transmission path and all the associated procedures in reverse. All this takes place within just a few milliseconds.

This summarizes the essential functionality of TCP/IP-Ethernet.

**We wish you much success in your future TCP/IP-Ethernet projects!**



## **10Base2 – 10Mbit/s BASEband 200 (185)m/Segment**

Ethernet topology using coaxial cable with a transmission rate of 10Mbps.

Other common designations for 10Base2 are Cheapernet or Thin Ethernet. Coaxial cable with 50 Ohm impedance in a thin and flexible construction is used to connect the individual stations together like a bus system. The beginning and end of a segment must be terminated with 50 Ohm resistors.

The transceivers are integrated on the network cards such that the bus must be routed to each workplace, where it is connected to the computers using BNC T-connectors. Cable attenuation as well as the sometimes large number of connectors limits a 10Base2 segment to max. 185m with max. 30 connections. No more than four repeaters are permitted between two stations.

The weak link in the physical bus topologies of Ethernet lies in the fact that a cable interruption - such as when a plug is pulled - shuts down the entire network segment.

## **10Base5 – 10Mbit/s BASEband 500m/Segment**

10Base5 is the original Ethernet specification. The cabling is based here on a coax bus cable with 50 Ohm impedance and a max. permissible length of 500m (Yellow Cable). Due to the coax 2-conductor technology (core and shield), both 10Base5 and 10Base2 only permit half-duplex operation. The network stations are connected through external transceivers which use vampire claws to get the signals directly off the bus cable without interrupting it with connectors etc. Divided into send, receive and collision information, the transceiver makes the data available on a 15-pin D-SUB connector. The terminal device is connected using an 8-pin TP cable max. 50m in length. No more than four repeaters are permitted between any two stations. This rule applies however only to „back-to-back“ repeaters - when implementing tree-type network structures a larger number of repeaters may be used.

The use of relatively high-quality cable without any interruptions in the form of connectors permits long segment lengths and a large number of possible tie-ins per segment (max. 100).

The thickness and non-flexibility of Yellow Cable as well as the additional cost due to external transceivers represent the main disadvantages of 10Base5, and are mainly responsible for the introduction of 10Base2.

**10BaseT – 10Mbit/s BASEband Twisted Pair**

In the 10BaseT definition, the physical topography is separated from the logical. The cabling is implemented in star-shape, originating from a hub as the central active component. A Category 3 cable having at least two pairs with 100 Ohm impedance is used, in which the send and receive data are transmitted on separate lines. The connectors are 8-pin RS45 types, in which the pairs are located on pins 1/2 and 3/6. The maximum length of a segment (= connection from hub to terminal device) is limited to 100m. 10BaseT topology originated in the United States, since it allowed normal telephone lines there to be used for network operation as well. This advantage was irrelevant in Germany, since star-shape 4-conductor cable is used for telephony, and this does not meet the requirements of Category 3.

Cable interruptions or removed plugs, which lead to a shutdown of the entire segment in all physical bus structures, only affect a single work station in 10BaseT.

**100BaseT4 – 100Mbit/s BASEband Twisted 4 Pairs**

100BaseT4 specifies an Ethernet transmission at 100Mbps. As in 10BaseT this is a physical star structure with a hub as the center. And here again a Category 3 cable with 100 Ohms of impedance, RJ45 connectors and a maximum length of 100m are specified. The use of all four wire pairs results in 10x the transmission speed (100Mbps) while still maintaining the Category 3 bandwidth of 25MHz. In 100BaseT4 three pairs are always used simultaneously for each data direction.

**100BaseTX – 100Mbit/s BASEband Twisted 2 Pairs**

100BaseTX specifies the 100Mbps transmission on 2 wire pairs through cabling implemented with Category 5 components. Cable, RJ45 wall sockets, patch panel etc. must be configured for a transmission frequency of at least 100MHz according to this category.

**Administrator**

A system manager who has unlimited access privileges in the local network and is responsible for administering and maintaining the network. The administrator assigns among other things the IP addresses in his network and must ensure the uniqueness of each IP address.

## **ARP – Address Resolution Protocol**

A Transmission Control Protocol/Internet Protocol (TCP/IP) process that maps IP addresses to Ethernet addresses. The determined assignments are administered in the ARP table of each individual computer. In Windows operating systems you can modify the ARP table using the ARP command.

Properties and parameters of the ARP command in the DOS window:

ARP -A lists the entries in the ARP table

ARP -S <IP address> <Ethernet address> adds a static entry to the ARP table

ARP -D <IP address> deletes an entry from the ARP table

ARP is defined in Internet Standard RFC-826.

*cf.* S. 12f, 35f

## **AUI – Attachment Unit Interface**

The cable (up to 50 meters in length) between the transceiver (mounted on the backbone Ethernet cable) and the network interface card in a PC or other network node.

Divided by send, receive and collision information, the data are provided by the transceiver on a 15-pin D-SUB connector. The terminal device is connected using an 8-wire TP cable.

Whereas the AUI interface used to be used mainly for connecting terminal devices to 10Base5 transceivers (Yellow Cable), they are used today more for connecting to fiber-optic transceivers.

## **BNC – Bayonet Neill Concelmann**

A bayonet-locking connector for miniature coax. BNC connectors are used in 10Base2 networks for mechanically connecting the RG58 cable (Cheapernet).

## **Bridge**

A device that connects two or more LANs (often called subnetworks) that are running the same protocols and cabling. This arrangement creates an extended network, in which any two workstations on the linked LANs can share data. Bridges use the Ethernet address to decide which packets may pass through the bridge and which may not. This information is obtained from the

bridge tables which must be entered by the administrator or dynamically created by the bridge itself, depending on the model.

*cf.* **Router**

### **Broadcast**

A broadcast is an all-call to all network stations. A typical broadcast application is the ARP request (see ARP). Other typical broadcast messages are RARP and RIP.

Broadcast messages are not sent through routers or bridges..

### **Bus system**

In a bus system several terminal devices share a single data line (bus line). Since only one terminal device may use the data line at any given time, bus systems require a protocol for controlling access privileges. Traditional bus systems include the Ethernet topologies 10Base2 and 10Base5.

### **Cheapernet**

An alternate name for Ethernet based on 10Base2.

### **Client**

Computers or applications which employ the services of so-called servers. Server services can include for example the preparation of a COM or printer port in the network, as well as telnet and FTP.

*cf.* p. 29

### **Client-Server architecture**

Systems having „distributed intelligence“, in which the client establishes a connection to a server in order to make use of the services provided by the server. Some server applications can serve multiple clients at the same time.

### **Com Server**

A terminal device in TCP/IP-Ethernet networks which uses the network to make ports available to serial devices and digital I/O points.

### **DHCP – Dynamic Host Configuration Protocol**

Dynamic, time-limited assigning of IP addresses from an address pool.

DHCP is used to automatically - without manual intervention - configure PCs in a TCP/IP network centrally and thus uniformly. The system admini-

strator determines how the IP addresses are to be assigned and specifies over what time period they are assigned.

This procedure has the basic result that each network station is assigned a different IP address each time a connection is established. This is why network components such as Com Servers or print servers, which are always accessed via a specified IP address, are excluded from IP address assigning using DHCP.

DHCP is defined in Internet Standards RFC 2131 (03/97) and RFC 2241 (11/97) .

## **DNS – Domain Name Service**

Network stations are accessed in the Internet through numerical IP addresses. But since names can be remembered better than numbers, DNS was introduced.

DNS is based on a hierarchical system: Each name address is identified by a top level domain („com“, „net“, „de“ etc.) and within this domain by a sub-level domain. Each sub-level domain can (but does not have to) contain further sub-domains. The individual parts of this name hierarchy are separated from each other by periods.

When the user enters a domain name for addressing, the TCP/IP stack queries the next DNS server for the associated IP address.

Network resources should logically contain a domain name which relates to the product or service provided by the company or to the company name. A relevant example would be „WuT.de“, which can be resolved into the top-level domain „de“ (=Deutschland) and the sub-level domain „WuT“ (=Wie-semann & Theis GmbH).

## **DNS Server**

DNS servers are used in the Internet to resolve a domain name into an IP address.

## **Ethernet**

Ethernet is the currently most frequently used technology for local networks. There are three different Ethernet topologies: 10Base2, 10Base5 and 10BaseT; the transmission rate is 10 Mbps.

*cf. p. 22ff*

**Ethernet Address**

The unchangeable, physical address of a network component in Ethernet.  
*cf. p. 23f, 35f*

**Fast Ethernet**

Fast Ethernet is basically an upgrade of 10BaseT topology from 10 Mbps to 100 Mbps.

*cf. 100BaseT4 and 100BaseTX*

**Firewall**

A firewall is defined as network components which similar to a router couple an internal network (Intranet) with a public network (e.g. Internet). Access to the other network can be limited or completely blocked depending on access direction, the service used as well as the authentication and identification of the network station.

An additional feature can be the encoding of data, when for example the public network is only used as a transit path between two spatially separated parts of an Intranet.

**FTP – File Transfer Protocol**

FTP is an upper-level TCP/IP service (protocol) that allows entire files to be sent between two network stations. FTP works like all other TCP protocols based on the client-server procedure. The FTP client take the initiative, and the user uses the FTp command to determine parameters, the type and direction of the data transmission.

After calling the FTP command from within the DOS window

```
FTP <IP-Adresse des FTP-Servers>
```

first the connection to the FTP server is established, which in turn asks for the user name and if appropriate a password.

Once the connection is established, entering additional commands and parameters allows access to the FTP server. Here are some key commands:

```
ascii          switches to transmission of text files,  
binary         switches to transmission of binary files,  
put <filename> sends the specified file to the FTP server,  
get <filename> reads the specified file from the FTP server.
```

In addition to the commands listed here, FTP under Windows offers a variety of other possibilities. For more details on this subject, check the Help functions under DOS (enter „?“ at the FTP prompt). Note that the syntax of FTP commands is different from one operating system to another.

FTP is described in RFC 959.

## Gateway

Gateways - like **Bridges** and **Routers** - connect various networks to each other. Whereas bridges and routers convert the physical type of the network (e.g. Ethernet - ISDN) while leaving the actual protocol (e.g. TCP/IP) intact, gateways provide a way of creating access to networks using different protocols (e.g. TCP/IP to Profibus). The job of a gateway is thus among other things translating the various communications protocols.

**Caution:** Network configuration in Windows operating systems also requires that a gateway be entered. This entry however refers to any router which may already be present in the network!

## Hub

A hub - also called a star coupler - offers the possibility of connecting multiple network stations to each other in a star configuration. Data packets which are received at a port are likewise sent to all the other ports.

In addition to hubs for 10BaseT (10Mbps) and 100BaseT (100Mbps), there are so-called autosensing hubs, which automatically detect whether the connected terminal device runs at 10 or 100Mbps. Autosensing hubs can be used to easily include older 10BaseT devices in new 100BaseT networks.

## ICMP – *Internet Control Message Protocol*

ICMP protocol is used to transmit status information and error messages between IP nodes. ICMP also allows echo requesting, to determine whether a destination is reachable.

*cf. Ping*

## Internet

The Internet is now the world's largest association of networks, providing connected stations with a virtually unlimited communications infrastructure. Through the use of TCP/IP the network stations can use the services provided by the Internet such as e-mail, FTP, browsers like HTTP etc. regardless of platform.

**Intranet**

A closed network (typically within a company) within whose borders the network stations enjoy Internet-typical services like e-mail, FTP or browser services such as HTTP.

An Intranet generally provides paths to the Internet through routers or firewalls.

**IP – Internet Protocol**

A protocol which allows connecting of stations which reside in different networks.

*cf. p. 25ff*

**IP Address**

The IP address is a 32-bit number that uniquely identifies each network station in the Internet or Intranet. It consists of a network section (Net ID) and a user section (Host ID).

*cf. p. 26f, 36ff*

**ISDN – Integrated Services Digital Network**

ISDN is the new standard in telecommunications and has completely replaced the analog telephone network in Germany. ISDN integrates telephone and telefax, video telephony and data transmission. ISDN thus allows speech, text, graphics and other data to be sent depending on the respective terminal devices.

ISDN uses the S0 port of a basic connection to provide two basic channels (B-channels) at 64Kbps each as well as a control channel (D-channel) at 16Kbps. The digital access channel thus has a maximum transmission speed of 144Kbps (2B+D). The two B-channels allow two different services to be operated at one time over a single line at a bit rate of 46Kbps.

**ISDN Router**

ISDN routers allow two local networks to be connected to each other over the ISDN network of a telephone network provider. In this way the ISDN routers take over both the normal functions of a router as well as the handling of the ISDN connection.

## **LAN – Local Area Network**

A local network within a defined area using a fast transmission medium such as Ethernet.

## **MAC-ID**

The unchangeable, physical address of a network component (MAC = Media Access Control).

*cf.* **Ethernet Address** and p. 23f, 35f

## **NAT – Network Address Translation**

The explosive growth of the Internet over the past several years has created a shortage of IP addresses, which are now given out only very sparingly. NAT is used when company networks are connected to the Internet. The company network is connected with the Internet through an NAT-capable router, but works internally with its own IP address array which is independent of the Internet. The network is only accessible from the outside over a single (or very few) IP addresses. The port number contained in the arriving TCP/IP packet is used to further route the packet to a particular internal network station.

## **Ping – Packet Internet Groper**

A program used in TCP/IP networks for diagnostics purposes, namely to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. If a network station issues an ICMP request by entering the ping command, the accessed station sends an ICMP reply back to the initiating station.

Invoking the command `PING <IP address>` in the DOS window requires the network station specified by the IP address to send a reply.

Various other parameters can also be specified:

- t Repeats the ping command in a loop until the user breaks it off with <Ctrl>C.
- n count Repeats the ping command „count“ times.
- l size „size“ specifies how many bytes the ICMP packet is filled with. The default setting for Com Servers is max. 512 bytes.
- w timeout „timeout“ specifies how long (in milliseconds) to wait for the reply.

Example:

PING 172.16.232.49 -n 50 repeats the ping command to station 172.16.232.49 fifty times.

If the station is there, the following reply is sent:

Reply from 172.16.232.49: bytes=32 time=10ms TTL=32

If there is no reply, the following message is returned:

Request timed out.

The ICMP packets used by ping are defined in Internet Standard RFC-792.

### **PPP – Point to Point Protocol**

PPP is an enhanced successor to **SLIP** and features among other things improved error correction.

Just like SLIP, PPP makes it possible to connect TCP/IP devices which have no LAN connection into TCP/IP networks over the serial interface.

### **Repeater**

A repeater is used in local networks to connect two Ethernet segments for the purpose of expanding the network by extending an individual segment. Repeaters pass data packets from one network segment to another by „refreshing“ the electrical signals in accordance with standards while leaving the contents of the data packets unchanged. If the repeater detects a physical error on one of the connected segments, the connection to this segment is separated („partitioned“). The partitioning is automatically lifted when the error has been remedied.

No more than four repeaters are permitted between two stations. This rule applies however only to „successive“ repeaters - a tree network structure does allow a larger number of repeaters to be used.

### **RIP – Routing Information Protocol**

Routing protocols such as RIP are used to exchange routing information between two networked systems, allowing dynamic changing of the routing tables.

RIP is defined in Internet Standard RFC-1058.

## Router

Routers connect two different networks, where in contrast to bridges, not the Ethernet address but rather the IP address is used to decide which data packets shall be passed on.

*cf. Bridge* and p. 38

## SLIP – *Serial Line Internet Protocol*

SLIP provides an easy means of transmitting TCP/IP data packets over serial point-to-point lines. This allows terminal devices which do not have a LAN connection to be integrated into the network through the serial port.

SLIP uses a very simple algorithm without its own data integrity checking procedure: A start character leads the actual IP data packet (decimal 192) and an end character (also decimal 192) is appended. To achieve binary transparency, start and end characters occurring in the data packet are first replaced by other sequences.

SLIP is described in RFC 1055.

## SLIP-Router

A SLIP router provides the hardware and functionality for integrating serial terminal devices which have a TCP/IP stack into a network.

Com Servers offer SLIP routing for example as a mode option.

## SNMP – *Simple Network Management Protocol*

SNMP lives over UDP and provides for central administration and monitoring of network components.

SNMP is specified in the following standards: RFC 1052, RFC 1155, RFC 1156, RFC 1157, RFC 1213 and RFC 1441.

## STP – *Shielded Twisted Pair*

Shielded cable made up of one or more twisted pairs. Twisted-pair cable is easier to install, less expensive, and easier to change than coaxial cable, but its bandwidth is usually smaller.

*cf. Twisted Pair*

## Subnet Mask

32-bit value which specifies which part of the IP address pertains to the network and which part to the network station.

*cf. p. 36ff*

## Switch

Like a hub, a switch makes it possible to connect multiple network stations together in a star configuration. Switches combine the functionality of a hub with that of a bridge: A switch „learns“ the Ethernet address of the network station connected to a port and sends it only those data packets which are addressed to this network station. One exception are broadcast messages, which are sent to all ports (here the switch differs in its functionality from a bridge, which in general does not forward broadcast messages).

In addition to switches for 100BaseT (100Mbps), there are so-called auto-sensing switches, which automatically detect whether the connected terminal device runs at 10 or 100Mbps. Autosensing hubs can be used to easily include older 10BaseT devices in new 100BaseT networks.

## TCP – *Transmission Control Protocol*

TCP lives over IP and takes responsibility not only for the station connection during data transmission, but also ensures data integrity and the correct sequence of data packets.

*cf. p. 29ff*

## TCP/IP Stack

Part of the operating system or a driver placed over the operating system which provides all the functions and drivers necessary for supporting IP protocol.

## Telnet – *Terminal over Network*

It used to be that telnet was used mainly for remote access to UNIX servers over the network. A telnet application (telnet client) can be used to give any computer in the network remote access to any other computer (telnet server). Today telnet is also used for configuring network components such as Com Servers. Under TCP/IP telnet is generally accessed through Port 23; but for special applications other port numbers may be used. Telnet lives over TCP/IP as a transmission and integrity protocol.

Properties and parameters of telnet in the DOS window:

```
TELNET <IP address>
```

establishes a telnet connection at Port 23 of the telnet server specified by the IP address.

```
TELNET <IP address> <Port No.>
```

establishes a telnet connection at the specified port of the addressed telnet server.

To establish a telnet connection on the configuration port (1111) of a W&T Com Server, for example, the command line might look like this:

```
TELNET 172.16.232.49 1111
```

In the Windows environment the addressing parameters for telnet connections are entered in the *Connect/Network systems* menu. Enter the IP address of the telnet server in the entry window under *Host name/Network systems*, and the desired port number under *Connection*. The already provided listing *telnet* corresponds to Port 23.

Telnet is defined in Internet Standard 854.

### **Terminating resistor**

In coax topologies such as 10Base5 or 10Base2 each network string must have a terminating resistor (terminator) at the beginning and end. The value of the terminator must correspond to the cable impedance, which for 10Base5 or 10Base2 is 50 Ohms.

### **TFTP – Trivial File Transfer Protocol**

Trivial File Transfer Protocol (TFTP) is another protocol for data transmission like FTP. TFTP offers only a minimum of commands, does not support any complex security mechanisms and uses UDP as the transmission protocol. Since UDP is an unsecured protocol, TFTP has its own minimal security mechanisms built in.

Trivial File Transfer Protocol is described in 783, 906, 1350 and 1782 to 1785 beschrieben.

### **Transceiver**

The word transceiver is a combination of transmitter and receiver. The transceiver implements the physical network access of a station to the Ethernet and is integrated on the network card for both modern Ethernet topologies 10Base2 and 10BaseT. Only in the case of 10Base5 (*cf. AUI Interface*) is the receiver fitted directly to the network cable as an external component.

### **Twisted Pair**

Data cable made up of one or more twisted pairs. Twisting the individual leads into pairs greatly reduces cross-talk between the double leads. A distinction is made between unshielded twisted-pair cables (UTP) and shielded STP cables (shielded twisted-pair).

Twisted-pair cables are used especially in network technology and are categorized according to their maximum transmission frequency; in practice, two types are used most commonly:

Category 3 cable allows a maximum transmission frequency of 25MHz, sufficient for use in 10BaseT, but also 100BaseT4 networks.

Category 5 cable allows a maximum transmission frequency of 100MHz, making it suitable for all current network topologies.

#### **UDP – *User Datagram Protocol***

UDP is a protocol which like TCP lives over IP, but in contrast to TCP is connection-less and provides no integrity mechanisms. The advantage of UDP over IP is the higher transmission speed.

*cf. p. 32*

#### **UTP – *Unshielded Twisted Pair***

Non-shielded data cable made up of one or more twisted pairs.

*cf. Twisted Pair*

In addition to the decimal number system (available characters: 0-9, new place starting at 10), computer technology often employs the binary number system (available characters 0-1, new place starting at 2) and the hexadecimal system (available characters 0-9 + A-f, new position starting at 16).

The following table contains some examples for representing common values in each of the three number systems:

Binary	Dec.	Hex.	Binary	Dec.	Hex.
0	0	0	11111	31	1F
1	1	1	100000	32	20
10	2	2	...	...	...
11	3	3	111111	63	3F
100	4	4	1000000	64	40
101	5	5	...	...	...
110	6	6			
111	7	7	...	...	...
1000	8	8	1111111	127	7F
1001	9	9	10000000	128	80
1010	10	A	11000000	192	C0
1011	11	B	11100000	224	E0
1100	12	C	11110000	240	F0
1101	13	D	11111000	248	F8
1110	14	E	11111100	252	FC
1111	15	F	11111110	254	FE
10000	16	10	11111111	255	FF