



Your connection to the world



OpenCom in Networks

Network basics

|

|

The network operation of OpenCom systems

OpenCom systems provide various network services for all of the PCs connected to them. You can configure these services in accordance with your own requirements. In some cases, in fact, configuration is a prerequisite. With few exceptions, it is immaterial whether the connection to the system is via Ethernet, USB or V.24. The OpenCom systems are designed for the creation of or integration in TCP/IP-based networks. Other network protocols such as Novell IPX/SPX, AppleTalk, IBM SNA, etc. are only supported in the OpenCom 31lan and 36lan bridging modes. However, the interference-free co-existence of several network protocols in the same network segment is possible.

General information on TCP/IP

The following information is based on IP V.4, which is currently the most widespread standard. Although the basic procedure also applies to IP V.6, the OpenCom systems do not support this standard.

In order for computers to transfer data to one another in a TCP/IP network, this data must first be divided into packets of a specified maximum size (Maximum Transmission Unit, MTU). The packets are then provided with the address of the sender (source) and the recipient (destination) and subsequently sent to the network. Here, various devices are responsible for forwarding the packets to the recipient. If desired, the address of the sender contained in the packet can then be used by the recipient to send a reply.

IP addresses

In order for a packet to reach the correct recipient, every device in a TCP/IP network must have a unique address - the so-called "IP address".

IP addresses consist of four numbers (bytes) lying between "0" and "255". The numbers are separated by dots, for example "192.168.70.254".

IP addresses are divided into a section that identifies the network as a whole (the network address), and a section that identifies a specific computer within this network (the host address). The network addresses are divided into different classes, depending on the highest possible number of hosts in that network.

General information on TCP/IP

Class A

Network address:

1.x.x.x to 127.x.x.x

Class B

Network address:

128.0.x.x to 191.255.x.x

Class C

Network address:

192.0.0.x to 223.255.255.x

The addresses in the range from 224.x.x.x to 254.x.x.x are reserved for special tasks ("multicast").

In addition, addresses whose binary representation consists completely of either "0" or "1" are also reserved. The latter are used to contact all of the hosts in a network ("broadcast"). Host addresses consisting solely of binary "0" are, in principle, permissible, but lead to incompatibility and should therefore be avoided.

RFC addresses

As mentioned above, every IP address on the Internet must be unique. For this reason, there is a central authority that assigns addresses for Class A, B and C networks for a fee. Addresses must be applied for in writing.

Clearly, there are not enough network addresses for every private user or small firm to have one, so address ranges have been reserved for the operation of local networks such as those you can create with OpenCom systems. These address ranges are:

Net-work-class	Max. no. of hosts	from	to
A	16.777.214	10.0.0.1	10.255.25.254
B	65.534	172.16.0.1	172.31.255.254
C	254	192.168.0.1	192.168.255.254

These address ranges are defined as being not valid in the Internet, which means that if the source or destination address of a data packet falls into any of these ranges, that packet will not be transferred in the Internet. However, these addresses can be used without restriction in local networks. The advantage of this is that even if there should be any accidental contact between a local network using reserved addresses and the Internet, no data can be transferred from the local network and there is no external access to the PCs in that network. The addresses can thus be used in more than one IP network

without any conflict arising, even when all these networks are connected to the Internet.

NAT / PAT

If a local network configured to use the addresses listed in the paragraph above has to contact the Internet, a special device or piece of software translates that address into an IP address that can be used in the Internet. This service is known as NAT (Network Address Translation). Whenever several local network addresses (i.e. RFC addresses) are translated simultaneously, the procedure is known as PAT (Port Address Translation). PAT is one of the many functions provided by the OpenCom systems. Normally your network will not be permanently connected to the Internet. The connection will be established by a DSL modem or by dialling in via ISDN when one of the computers in the network wants to contact the Internet. While the connection is being established, your Internet provider assigns the OpenCom system a valid IP address for use in the Internet. This address remains valid for the duration of the connection to the provider. The above-mentioned PAT translates the addresses of all the data packets from your local network to this address and sends them to the Internet. The addresses of reply packets from the Internet are translated back and sent to the corresponding computer in your local network. Please note

that even if you are using an ISDN or DSL flat rate, the IP address assigned to your OpenCom system will still change from time to time. This is because providers disconnect local networks from the Internet approximately once every 24 hours. Live TCP connections are terminated and therefore have to be re-established if required.

Network masks and default gateways

Whenever a computer wants to transfer a data packet to another computer, it first has to ascertain whether the target computer is within its own network or outside it. In order to do this, it analyses its own IP address and network mask. This information enables it to send packets in its own network directly to the destination, while packets destined for computers in other networks are sent to the default gateway. This is then responsible for forwarding the packet correctly.

The OpenCom system also takes over the function of the default gateway.

General information on TCP/IP

DNS

Computers manage IP addresses easily, but people find it difficult to remember series of numbers. For this reason, a network usually has a service that translates names, which are easier for people to remember, to the IP addresses suitable for machines. This service is called the Domain Name Service (DNS). For example, whenever you type "www.detewe.de" into your Web browser, your computer first contacts the DNS server to look up the IP address corresponding to this name. Then it sends a packet to that address requesting the page you wanted. The DNS server in your network may not be able to answer this request, as no computer in the world can store all the valid Internet names and corresponding IP addresses. However, the Internet provides a system enabling such requests to be relayed until they reach a server that can answer them.

The OpenCom systems include a DNS relay, which means that they can't answer DNS requests themselves, but can relay them and then forward the information supplied by the DNS server to the computer that sent the request.

Protocols

The **Transmission Control Protocol** (TCP) enables two hosts to transfer data packets to each other and acknowledge reception of that data. It ensures that data packets are not lost and that they arrive in the sequence in which they were sent; in the event of an error, the packet is sent again. In order to carry out these tasks, a large amount of information is transmitted in addition to the useful data.

The **User Datagram Protocol** (UDP) enables unacknowledged data transfer. When a UDP packet is sent, the sender cannot be sure that the packet has reached its destination. However, the packet requires very little additional information, which leads to a higher data throughput in a functioning network free of interference, such as a LAN.

The **Internet Control Message Protocol** (ICMP) transmits information about the network itself, e.g. whether certain paths within the network are available, whether certain hosts can be contacted, etc. For example, the widely used diagnostic tool known as "ping" sends an ICMP packet to the target host requesting that the packet be returned unaltered (ICMP echo request).

Besides the above, there are several other protocols for various other purposes (services). They exchange their protocol data packets in the hosts via the TCP and UDP transport protocols. Most services in the Internet are transported via TCP.

- The **HTTP protocol** (WWW) enables Web browsers (Microsoft Internet Explorer, Mozilla, Netscape, Opera, ...) to communicate with Web servers in a network. This is what makes Internet and intranet surfing possible.
- The **FTP protocol** (file transfer) enables files to be exchanged in a network. For this purpose, local FTP programs, e.g. WS-FTP, communicate with file servers (FTP servers).
- The **SMTP/POP3/IMAP protocols** enable the exchange of e-mail in a network. For this purpose, local mail programs (often integrated in Web browsers or office products) communicate with service providers' mail servers.
- The **DNS protocol** enables the resolution of logical names (e.g. t-online.de) in a network, locally and world-wide, to the IP addresses (194.25.134.146) used in all network elements. If a network element uses a logical host name, a DNS request is sent to the nearest known DNS server, which then attempts to either resolve this name or forward the request.

However, more simple services are transported in the network via UDP. These are often unidirectional or broadcasts.

- The **DHCP protocol** enables the unique assignment of network addresses (IP addresses) to hosts in local networks by means of a DHCP server.
- The **TFTP protocol** enables simple file exchange. It is often used to download binary data for software updates in the network elements.
- The **SNTP protocol** enables the synchronisation of the date and time in a system with timer servers in the network.
- The **SNMP protocol** enables the control and administration of systems in a network.
- **Voice over IP** (VoIP) also uses certain protocols over UDP. This is because telephony over IP has high requirements in terms of resources, while the voice data does not have such high requirements in terms of security.

This document does not provide detailed information or information on additional TCP and UDP protocols. If you require such information, please refer to the specialist literature.

General information on TCP/IP

Ports

A single computer can simultaneously establish several connections and provide several services for other computers. In order to distinguish between parallel connections, so-called ports are used: there are 65,535 ports each for TCP and UDP. By general agreement, hosts usually provide services on ports 1-1,023 while outgoing connections are usually established on ports 1,024 and above. However, this is merely a convention and not a technical necessity. There may be very good reasons for offering services on higher-numbered ports (i.e. ports higher than 1,023). Potentially risky services are traditionally assigned lower-numbered ports, which is why most firewalls are configured to only allow very restricted access to these ports. Normally, special rights (root or administrator rights) are required in order to assign services to ports lower than 1,024.

Static network configuration / DHCP

In the section on TCP/IP above, you will have seen that the computers in your network require various items of information in order to contact other computers in the network or in the Internet. These are:

- the computer's own IP address,
- the network mask,
- the address of the default gateway, and
- the address of the DNS server.

You can either save this information on every connected computer (static configuration) or have it assigned automatically by a central device (dynamic configuration). Such devices (or the software fulfilling this function) are known as DHCP servers (DHCP = Dynamic Host Configuration Protocol). The devices to which DHCP servers assign configurations are thus DHCP clients.

DHCP server mode

This is the default setting OpenCom systems have on delivery. If you have not changed the presettings, the integrated DHCP server assigns the following addresses:

OpenCom 31/31lan

LAN: 192.168.69.1 to 192.168.69.249

The address of the system itself is 192.168.69.254

OpenCom X32

LAN: 192.168.69.1 to 192.168.69.249

The address of the system itself is 192.168.69.254

OpenCom 36lan

LAN: 192.168.69.1 to 192.168.69.249

The address of the system itself is 192.168.69.254

OpenCom 40dsl

USB: 192.168.69.251

LAN: 192.168.69.1 to 192.168.69.249

The address of the system itself is 192.168.69.254

OpenCom 45dsl

USB: 192.168.70.253

RAS: 192.168.70.251 to 192.168.70.252

LAN: 192.168.70.1 to 192.168.70.250

The address of the system itself is 192.168.70.254

All devices are assigned the network mask 255.255.255.0, so that all the IP addresses in the ranges 192.168.69.x (for the OpenCom 31, 31lan, X32, 36lan and 40dsl) or 192.168.70.x (for the OpenCom 45dsl) are seen as local addresses, while all other addresses can only be contacted via the default gateway. Since the OpenCom system functions as the default gateway and as the DNS server, the address of the system is used for both.

Static network configuration / DHCP

DHCP client mode

This mode is only supported by OpenCom 31 / 31lan / 45dsl.

The OpenCom 45dsl starts in this mode of operation by searching the network for a DHCP server from which it can get its network configuration. This can take up to two minutes, during which the system is not operational. If no DHCP server is found, the system switches to "Static IP Mode".

When operating a PC connected to an OpenCom 45dsl via USB, you have to set the IP address given for the USB port in the network configuration. If you do not do so, the router integrated in the OpenCom 45dsl will not be able to forward data packets to this PC. Please also ensure that the IP address specified for the USB port is in the same sub-network as the address of the OpenCom 45dsl itself. Furthermore, the external DHCP server must be configured so that it does not assign the IP address configured for the USB port. You must therefore configure your DHCP server so that it always assigns the same IP address for the OpenCom 45dsl's MAC address. Exclude the USB port address from the list of addresses that can be assigned. Please ensure that your DNS resolves the name "opencom45" in the IP address assigned in the OpenCom 45dsl, as otherwise the system's Configurator will not be accessible at <http://opencom45/>.

If your DNS does not resolve the name, you will have to configure the IP address directly in order to start the

Configurator, e.g.

<http://192.168.123.234/>.

If you want to enable PCs to dial in to the OpenCom 45dsl in this mode, you must configure the IP addresses to be assigned to those PCs in accordance with the address range of your network. The OpenCom 45dsl cannot look these addresses up via DHCP because the DHCP protocol does not provide this function. Furthermore, the external DHCP server must be configured so that it does not assign any of the IP addresses used for dialling into the RAS.

Static IP mode

In this mode, the OpenCom system neither functions as a DHCP server nor does it attempt to find one. Instead, the system uses the network parameters you have configured.

If you connect a PC via USB or V.24, it must be configured with the IP address specified for the USB port in the network configuration. Otherwise, the router integrated in the OpenCom system will not be able to forward packets to this PC. Furthermore, please ensure that the IP address specified for the USB port is in the same sub-network as the address of the OpenCom system itself. Only OpenCom 45dsl:

Computers dialling into the system are assigned the addresses specified in the network configuration.

The OpenCom 45dsl runs a proxy ARP (Address Resolution Protocol) for the IP addresses assigned to the USB port and the RAS dial-in ports, even when these interfaces are not currently active.

Assigning IP addresses by code

This procedure is only supported by the OpenCom 45dsl.

If you assign the OpenCom 45dsl a new IP address by means of the code programming function, the addresses for the USB port, the RAS dial-in ports and the DHCP range are automatically adjusted accordingly. In addition, the system's integrated DHCP server is activated. The addresses are assigned according to the following scheme:

- The OpenCom 45dsl itself is assigned the address you entered
- The USB port is assigned the address entered - 1
- The RAS dial-in ports are assigned the entered addresses - 2 and - 3
- The larger of the two free ranges is assigned to the DHCP server.

Here is an example. Let's assume you assign the address 192.168.70.125, then the other addresses are 192.168.70.124 for the USB port, 192.168.70.123 for the first RAS dial-in port and 192.168.70.122 for the second RAS dial-in port.

The range of addresses from 192.168.70.126 to 192.168.70.254 contains more addresses than the range from 192.168.70.1 to 192.168.70.121 and is therefore assigned to the DHCP server.

This scheme of address assignment means that you cannot assign an IP address with a value of less than "4" as the last byte.

Please note that whenever you restart the DHCP server, the addresses you previously assigned become invalid and you will have to reboot the connected PCs.

Configuring the provider access

Your system can connect to the Internet via both DSL and ISDN. You only have to save your access data in the system and the integrated router will establish the connection to the Internet as required, disconnecting again after a configurable idle time.

The following additional notes apply to the DSL-capable systems (the OpenCom 31lan, the OpenCom X32, the OpenCom 36lanl, the OpenCom 40dsl and the OpenCom 45dsl).

If you often experience difficulty in establishing a connection, we recommend that you configure fallback access. The OpenCom system will first attempt to establish the connection to your default provider. If this is not successful, the fallback access will be used. Once established, the connection to the alternative provider remains active until it is disconnected on expiry of the idle time you configured. The next time the OpenCom tries to establish a connection, it again tries the default provider first before falling back on the alternative provider if this should prove necessary.

Thus, if you configure a short idle time, you will return to your usual provider more quickly because connections are established more frequently and in each case your usual provider is tried first. On the other hand, as long as only the alternative provider is accessible, this

leads to delays.

Specifying a longer idle time reduces the delay as connections do not need to be established so often, but in this case it will be longer before you return to your usual provider.

While the connection is being established, the configured user name and password are transmitted to the provider in order for access authorisation to be checked. The provider then returns an IP address to the OpenCom system to use when transferring packets to the Internet. The provider also transmits its DNS server address, to which the OpenCom system then forwards DNS queries. In addition, the provider specifies the network mask.

Some providers only transmit the IP address and expect the other parameters to be permanently configured in your system. Your provider will issue you with the necessary values, and you can store them using the Configurator.

Dialling into the OpenCom system

This is possible on the OpenCom X32 and 45dsl.

The OpenCom 45dsl can also function as an Internet provider and is able to serve up to two computers simultaneously. Whenever a computer dials into the system, the user name and password are checked. If the check is successful, the system assigns the computer an IP address previously configured in the Configurator (for default parameters, see above). The computer is also given the address of the OpenCom 45dsl as the DNS server and the correct network mask. Using this configuration, the computer that has dialled in can also access the local network, just as a locally connected computer can. The only difference is that the data transfer rate of approx. 7.5 Kbytes/s is much lower than via Ethernet or USB.

In case of OpenCom X32 dialling in is available for remote service / configuration. It can however also be used for accessing the LAN from remote.

Accessing the configuration (OpenCom 31/31lan, OpenCom X32, OpenCom 36lan, OpenCom 40dsl)

You can edit the configurations of the OpenCom 31lan, the OpenCom 36lan and the OpenCom 40dsl conveniently by means of the configuration program supplied. (In the case of the OpenCom 31, 31lan and OpenCom X32, this is only the Web Configurator. For access, see below). However, some settings, such as the configuration of the server services described below, can only be edited by means of the system's integrated Web server. To do this, you start a browser on any connected PC and key in the URL <http://opencom/> or <http://192.168.69.254/>. When prompted for a user name and password, leave the user name blank and key in the system PIN as the password. When using the OpenCom X32 it is possible in case of high security requirements, to assign an alpha numeric password for the web configurator.

Accessing the configuration (OpenCom 45dsl)

You can edit the OpenCom 45dsl configuration by means of any of the widely used browsers, such as Microsoft Internet Explorer, Netscape or Opera. Start the browser and key in the URL <http://opencom45>. The Web server integrated in the OpenCom 45dsl loads the configuration software to the browser and starts it. The software then contacts the system, thus enabling you to set all the parameters conveniently.

The Configurator is a JAVA program and thus requires the Java Runtime Environment (JRE), Version $\geq 1.3.1$. In the Windows version this is on the CD supplied and is installed on your PC as part of the driver installation. If you do not use a Windows operating system you will have to download the JRE for your operating system from SUN Microsystems (<http://java.sun.com>).

Running the Configurator on a computer in the local network gives you unrestricted access to all system parameters. For security reasons, however, computers that dial into the network are only granted restricted access. Firstly, access to the configuration must be explicitly permitted by the dial-in access configuration. If this is not the case, you will be able to load and start the Configurator using a browser, but the system will not permit its parameters to be read out or

changed. If access is permitted, you can change all the parameters except for the dial-in parameters themselves and the network filters. The reason for not permitting the dial-in parameters to be changed is so that a malicious hacker cannot open a door to your system. The network filters cannot be changed because if an incorrect setting were made here, you could prevent yourself from accessing the system.

If you have set your OpenCom 45dsl to DHCP client mode and transferred the configuration, there will be no contact between the Configurator and the system at first. This is because the Configurator assumes that the old IP address is valid, whereas the system has been assigned a new one by your DHCP server. If this occurs, simply close the Configurator and invoke the page again. Please also refer to the note on DNS in the section on DHCP client mode above.

Configuring server services

This feature is currently supported by the OpenCom 31lan, the OpenCom 40dsl, the OpenCom 45dsl and the OpenCom 36lan.

As described above, your OpenCom system uses PAT to translate your local network IP addresses to the address assigned to you by your provider. As a result of this translation, packets sent to the OpenCom system from the Internet can only be forwarded to a computer in the local network when NAT has the relevant reference information. This is always the case when the packet is a reply to a request sent by a local computer.

Unrequested packets sent to your OpenCom system from the Internet cannot be forwarded to a specific local computer as they lack reference information. Such packets are then dropped. This is an important element of the integrated firewall function and as such, makes a major contribution to the security of your local network. On the other hand, this mechanism makes it impossible for you to provide a service on your local computer in the Internet, as this would require desired but unrequested packets reaching that computer. In order to enable server operation, you can configure your system so that incoming packets without the reference information required for forwarding by PAT are routed directly to one of your

local computers in accordance with a defined set of rules. You configure this function by using the OpenCom system's integrated Web server to invoke the item called "Expert Configuration > Port Forwarding". In the OpenCom 45dsl you invoke "Expert Configuration > Port Routing". Here you can select the following settings:

Service name:

Here you can choose any name you find easy to remember.

Target IP service:

The IP address of the computer in the local network to which the packets are to be forwarded.

IP protocol:

Here you enter the desired protocol as a numerical value. These values are: 0 = any protocol, 6 = TCP, and 17 = UDP.

Port range:

The range of ports that can be accessed from the Internet. If only one port is to be released, then this port must be entered as both the first and last port in the range.

Active:

Tick to activate forwarding.

Important note: If you activate server services, you should operate your network in the static IP mode. In DHCP mode it is not possible to ensure that

Configuring server services

your server is always assigned the same IP address by the OpenCom system, which could lead to the incoming packets being forwarded to the wrong computer.

DeTeWe Systems GmbH • Zeughofstraße 1 • 10997 Berlin • www.detewe.de

Mat.-Nr.: 70148.028

Created in October 2005