# IT Knowledge

**Directory:**

## 1. Bits and bytes

A bit (short for "binary digit") is the smallest unit of measurement used to quantify computer data. It contains a single binary value of 0 or 1. A byte is a unit of measurement used to measure data. A byte contains eight binary bits. Therefore, each byte can be used to represent 2^8 or 256 different values.

## 2. What is an IP address and a subnet mask?

An Internet Protocol (IP) address is a numerical identifier associated with any device connected to a computer network. This protocol is the basis for sending data packets from one place to another. The main features are:

- Network Interface (Host) Identification
- Location Addressing

As an example, you could compare the IP address to a mailing address, so you can send a package from the sender to the recipient. There are two types of IP addresses: IPv4 and IPv6:

- IPv4 (version 4) defines an IP address as a 32-bit number.
- IPv6 (version 6) defines an IP address as a 128-bit number.

For the mBCA installation, you will only use the IPv4 standard.
IPv4 addresses have a size of 32 bits and are usually represented in point-decimal notation, consisting of four decimals, each ranging from 0 to 255, separated by periods (e.g., 192.168.2.1). Each of the four parts represents a group of 8 bits of the address.
Ranges of IP addresses in local networks are from 10.0.0.0 to 10.255.255.255, from 172.16.0.0 to 172.31.255.255, and from 192.168.0.0 to 192.168.255.255).

IP networks are divided into sub-networks. The subnet mask determines how the IP address is divided into network and host parts.

To take the example above, you need to imagine a street name + house number converted into numbers. The subnet mask defines the length of the network portion that corresponds to the street name, as well as the length of the host portion that corresponds to the house number.
A subnet mask is the same size as an IP address.
Example of a subnet mask: 255.255.255.0
In this example, the first three parts of the subnet mask define the network part, while the last part represents the host.
For example, if you have 2 devices (PC and mBCA) on the same subnet, the IP addresses could be 192.168.100.1 and 192.168.100.2
192.168.100. corresponds to the network part, which must be the same for both IP addresses. The last part of both IPs (XXX.XXX.XXX.1 and XXX.XXX.XXX.2) corresponds to the host part of the IP address. This must be individual for each device.

### 3. What is a port?

In the computer network, a port is an endpoint of communication. Physical and wireless connections end at ports of hardware devices. At the software level, within an operating system, a port is a logical construct that identifies a specific process or type of network service.
A computer/device can have one IP and multiple ports. Each port allows a different service to communicate with your device. Port 0 – 65535 can be used.

### 4. What is a router?

A router is a device that relays data packets between different computer networks. A router is connected to two or more networks, usually two local area networks (LAN) or one LAN and its ISP network.
Routers are also known as gateways, the point where two different networks are connected. Some routers include additional features such as DHCP services (see point 6), modem and firewall capabilities (see point 8) among others.

### 5. What is a standard gateway?

A standard gateway serves as an access point or IP router that a networked computer uses to send information to a computer on another network or to the Internet. Default simply means that this gateway is used by default unless an application specifies a different gateway.

### 6. What is a domain name server

A domain name server (DNS) is a database that links names, known as hosts, to IP addresses. For example, the computer name "seca-computer" is translated into an IP address.

### 7. What is DHCP and Dynamic IP Address

The Dynamic Host Configuration Protocol (DHCP) is a protocol that automatically assigns an Internet Protocol (IP) address to devices within the network.
As mentioned above, devices on a network need an IP address to communicate with each other. A DHCP server automatically provides IP addresses for each subscriber within a network and associates them with a device name, which is usually the "computer name" or "hostname" of the operating system.
A dynamic IP address can change every time a device is reconnected to a network. The DHCP server assigns an IP address, which can be different each time.

## 8. What is a static IP address?

A static IP is a fixed IP address assigned to a device within a network. Once a static IP address has been configured to a network participant, it remains in place until it is changed manually.

## 9. What are UDP and TCP?

UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) are communication protocols used to exchange data between two devices within a network.
In addition to the main data, a data packet contains the IP addresses of the sender and receiver as well as the port number.
TCP is used for:

- Establishing a Connection
- Data transmission
- Protection against transmission errors
- On the sender side: Distribution of data packets
- On the recipient side: merging the data packets

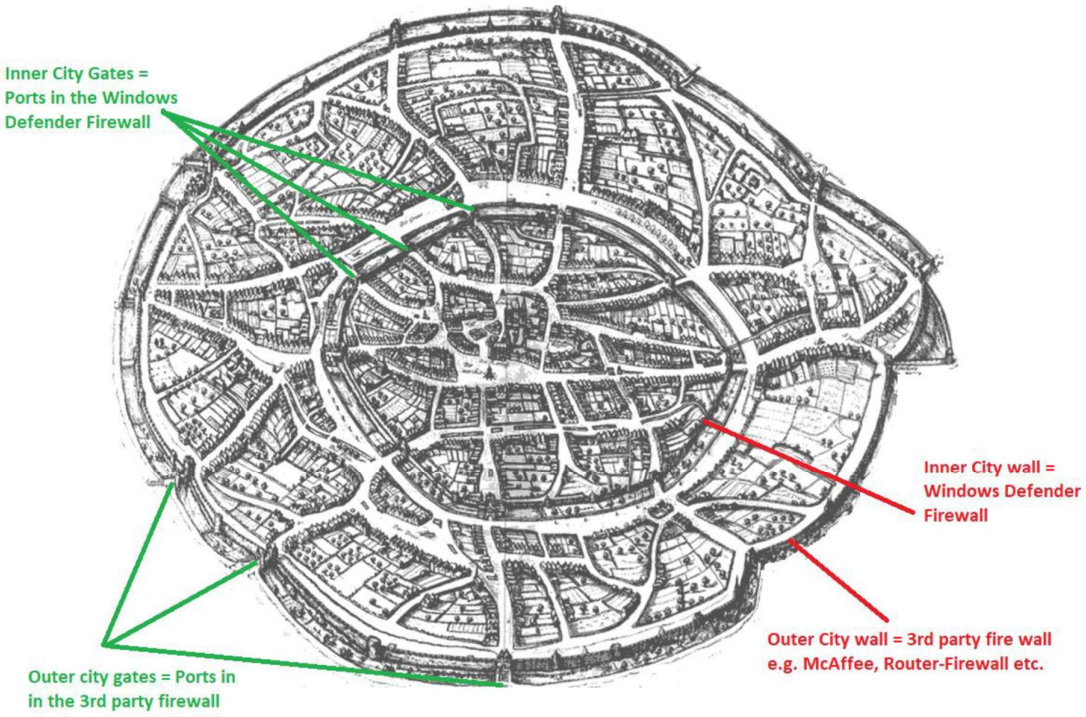
UDP is used for:

- Data transmission

UDP is a simplified form of a data transfer protocol. It does not check whether a data packet is incomplete, nor whether it has been received.

## 10. What is a firewall?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.
Basically, there are two different types of firewalls: network (hardware) and host-based (software) firewalls.
Network-based firewalls filter network traffic within your network to allow only legitimate traffic.
Host-based firewalls provide protection at the individual computer (host) level. Sometimes it is necessary to "whitelist" a desired application. This would allow traffic to enter your network that would otherwise have been filtered out.
As an example, a firewall can be compared to the city walls of a medieval city, which protects the city from unwanted access. Furthermore, the ports (see point 3) can be compared to the city gates that have to be passed through to get into the city. If a port (or city gate) is blocked, the message cannot reach its recipient.




### 11. What is the Command Prompt (cmd)

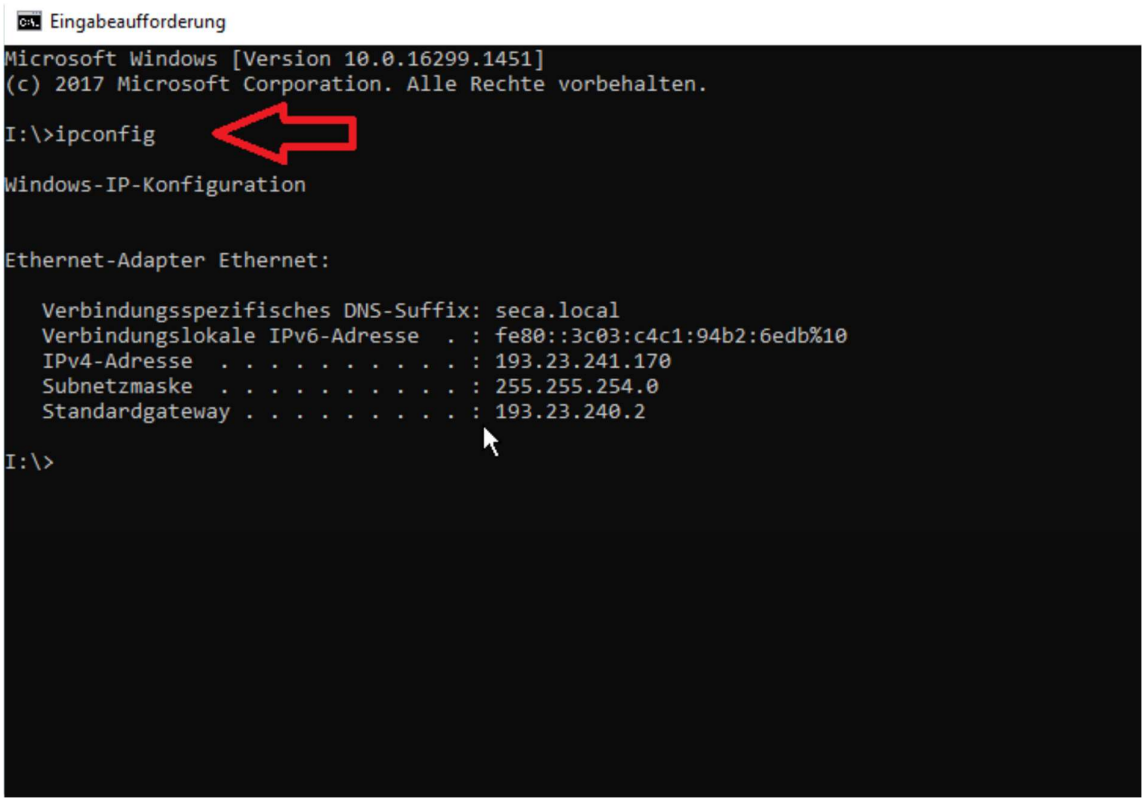
The Command Prompt is a command-line application available in most Windows operating systems. It is used to execute typed commands.

### 12. How to Open Command Prompt

You can open the Command Prompt from the Command Prompt shortcut, which is located in the Start menu or on the Apps screen, depending on your version of Windows. Another way to open the command prompt is via the cmd command in the Run dialog (type cmd in the search bar) or in its original location at C:\Windows\system32\cmd.exe.


### 13. How to Find Out the IP Address of a Windows Computer or Windows Server Network

Open the command prompt and type the ipconfig command.
You'll now see the IP address, subnet mask, and default gateway configured for your network adapters on that particular computer. Since more than one network may be displayed (e.g. another WIFI adapter), please double-check that you have retrieved the information for the correct network adapter.




### 14. How to Set Up a Static IP Address

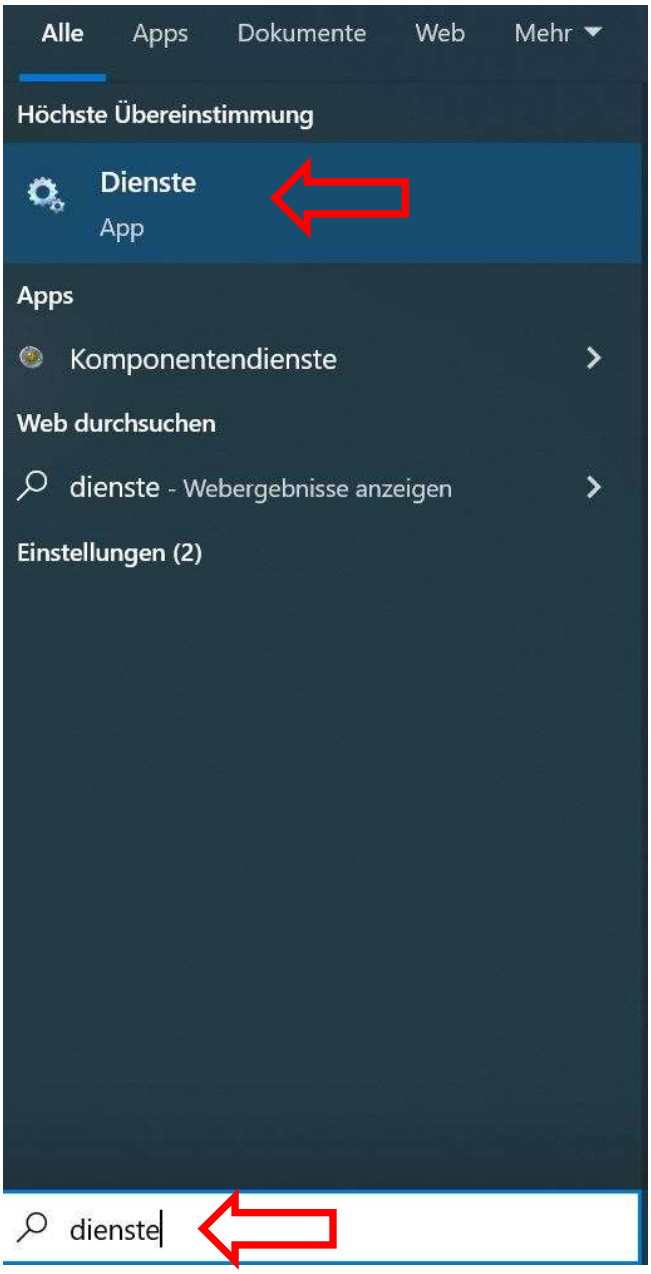
For the mBCA installation, the preferred option is to use a static IP address on the computer containing the seca analytics 115 installation. This may only be possible if the mBCA installation is a "complete installation" that is not implemented in a hospital network environment.

- Go to Windows Settings
- Click Network & Internet
- Click on "Change Adapter Options"
- Right-click on "Ethernet"
- Click on "Properties"
- Double-click Internet Protocol Version 4 (TCP/IPv4)
- Define Address and Subnet Mask

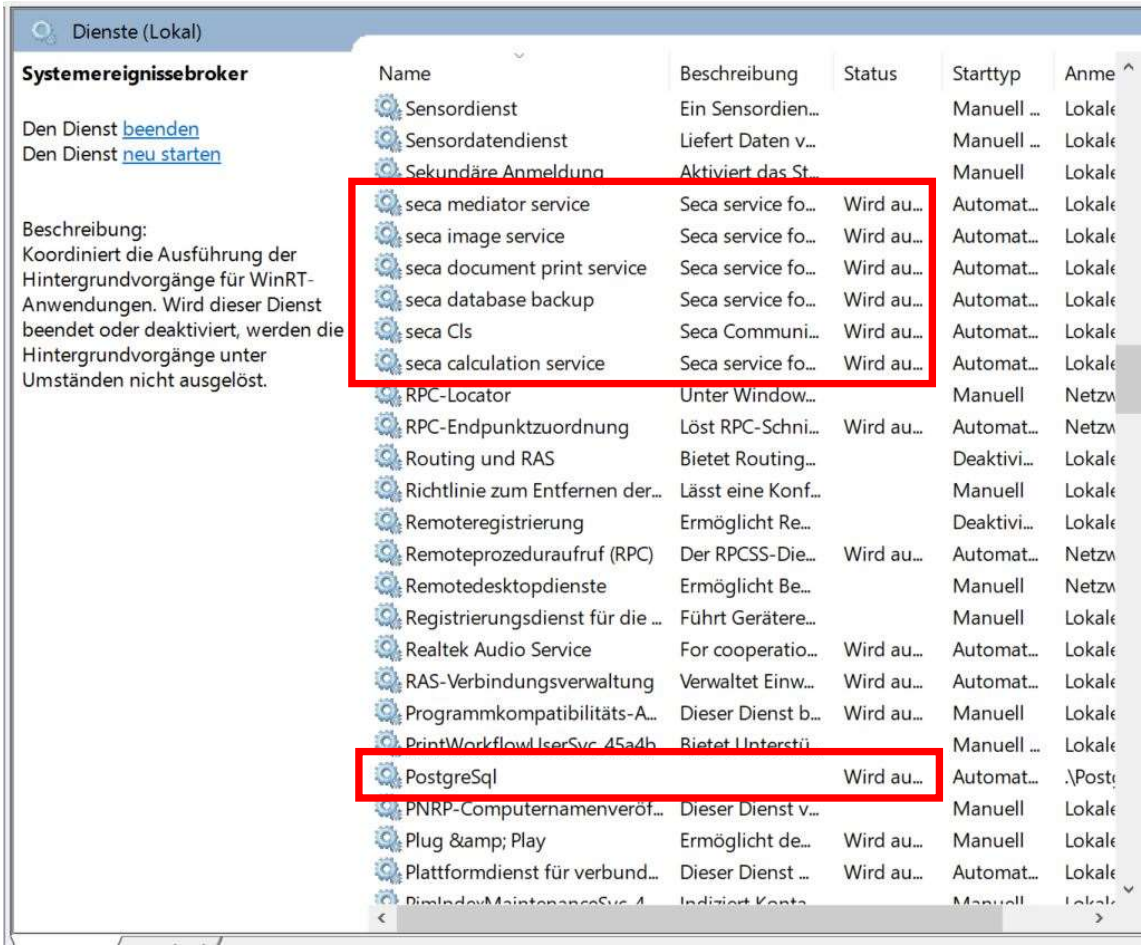
Example:
Subnetzmasks: 255.255.255.0
(Please note that the subnet mask must be set up in the same way on the device you want to connect.)
IP address: e.g. 10.10.10.10
(Please note that according to the subnet mask chosen above, the first three values of the IP address must be the same for both the PC and the device you are trying to connect. The fourth value must be different.)

## 15. How to check if services are running

To troubleshoot mBCA, it is often necessary to check whether the Windows services connected to seca are running or whether they are stopped and need to be restarted. Stopped services can have various causes, which are not described in detail here. Windows services are applications that typically start during Windows startup. Open Windows Services Manager by typing "Services" in the Windows search bar.



If you want to stop, start, or restart a service, highlight the service by clicking on it. Then select the required action from the menu that appears on the left side of the service overview. You can also right-click on the specific service and select the option you want.




The services marked in red are required to enable the operation of the seca analytics 115Software properly. If one or more services are not running, restart the service.