Automation by innovation.

KeContact M10

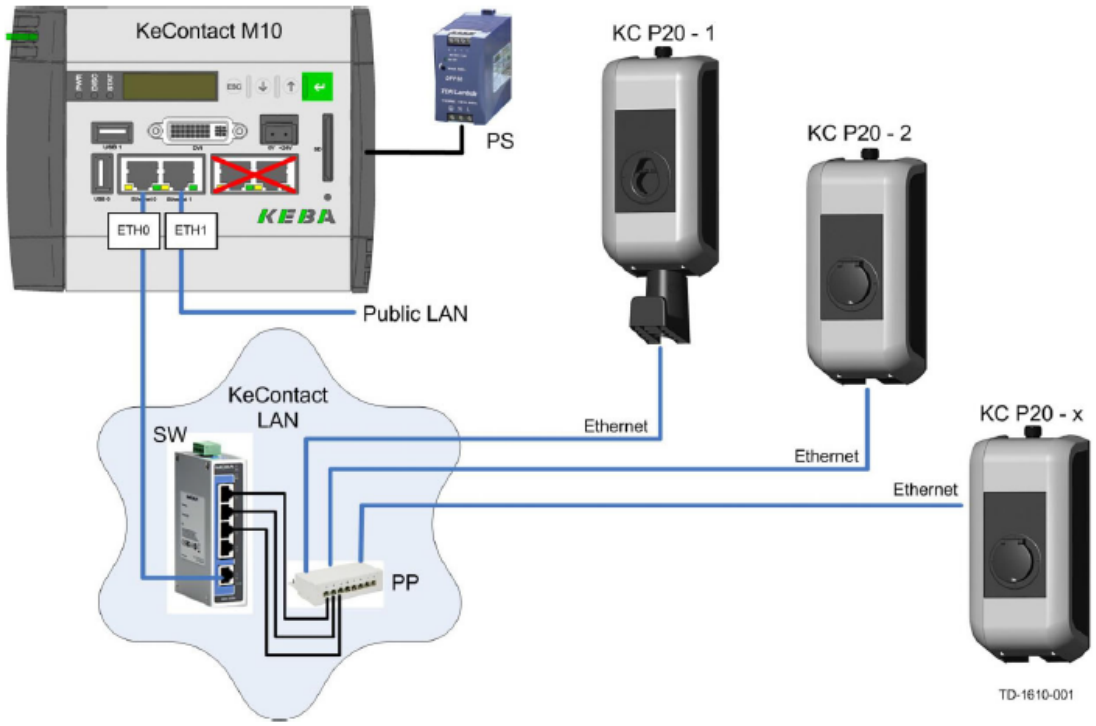
Network Basics

Note: *This document is intended to provide an overview of how the KeContact M10 is connected with KeContact P20 wall boxes and how it can be integrated into existing network structures. For more detailed information about installation, configuration and operation please refer to the KeContact M10 manual.*

The KeContact M10 features two functional Ethernet ports on its front side, ETH0 and ETH1. As shown in the picture below, these two ports have different functions. ETH0 is used to connect the P20 wall boxes to the M10. To do this, patch panel and network switches are required. We call the hereby created network the “KeContact LAN”.

ETH1 can be connected to any public/company LAN or even to the Internet directly.

Schematic overview (hardware)



[M10]… KeContact M10 fleet server	**[KC P20]**… KeContact P20 wallbox 1 to 15
[PS]… Power supply unit 24V	
[Eth0]…Ethernet port for Installation, configuration and monitoring	
[Eth1]…Ethernet port only for configuration and monitoring	
[SW]… Ethernet switch	
[PP]… Patch panel	

1 Why those two network ports?

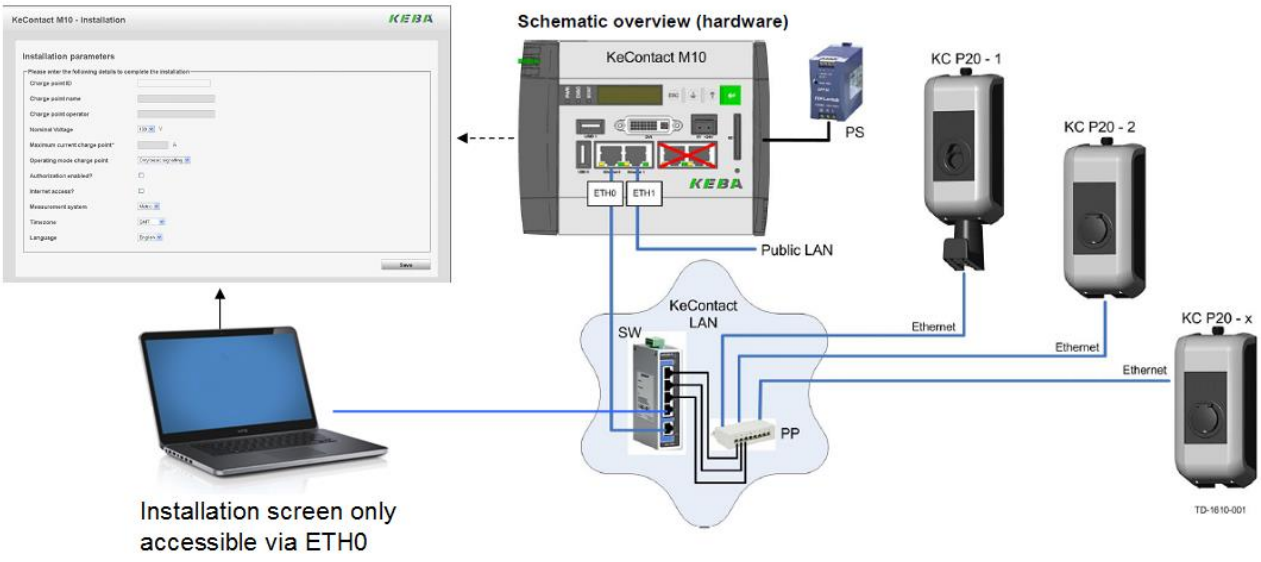
First and foremost it is important to highlight again that ETH0 and ETH1 are in two separated networks and have different functions. This is not only a security measure to prevent any outside attacks from the Internet, creating a sole “KeContact LAN” also makes life easier with addressing the single wall boxes. On ETH0, the M10 has a static IP address (192.168.25.1). The wall boxes in the KeContact LAN will be assigned another static IP address within the same network (192.168.25.xx). Wall box configuration by DIP switches can be found in the M10 manual in chapter 4.3 “DIP switch settings”.

We know that company network policies are sometimes quite strict and that IT departments are often suspicious towards unknown devices that need to be connected to their networks. Therefore, the M10 can principally work as a stand-alone, “zero-touch” device that does not need any attention or monitoring during operation. If a setup like this is required, it is important to know that no “public LAN” needs to be connected.

For installation, i.e. configuring basic parameters of the entire installation, a computer is simply plugged into the ETH0 network. Make sure that the computer obtains an IP address automatically and that no proxy and IEEE802.1X authentication is configured.

The web interface on ETH0 can be accessed by typing http://192.168.25.1:9091/admin into the address bar of the browser. In any case, for ETH0 there is no need to bother about subnet masks, proxies, gateways or anything of that sort.

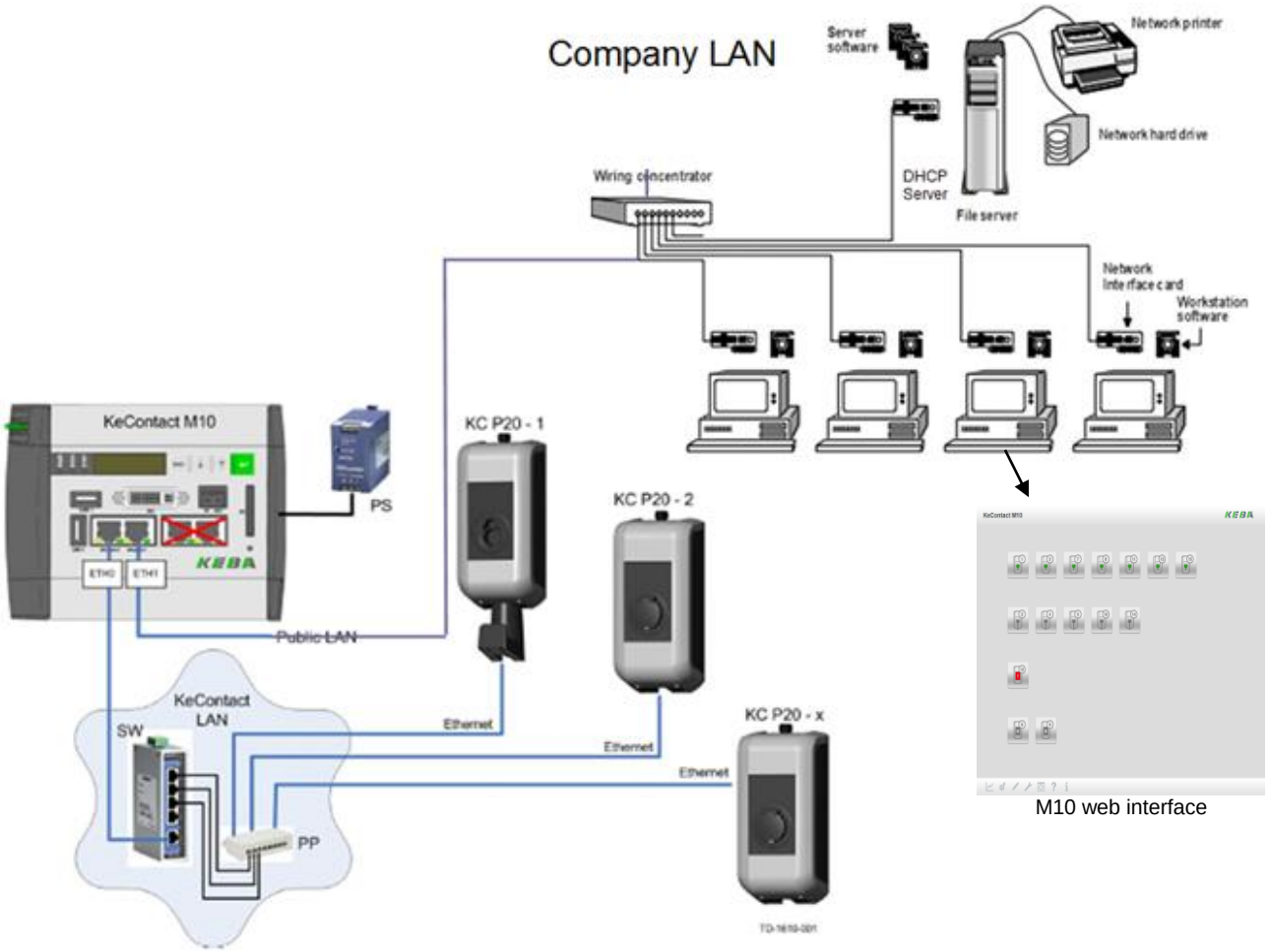
At this point it is important to understand that **configuration and monitoring is possible through a web interface on ETH1, but the installation and “home” screen containing basic information about the entire installation can only be accessed via ETH0**. Again, this is a security measure because basic settings should only be changeable for someone on site, someone who plugs directly into the KeContact LAN, knows the conditions and circumstances on site and, of course, has access to the M10 system (username + password).



The ETH1 port is the “public LAN” connection for remote control and/or monitoring. In contrast to ETH0, this port does not have a static IP address. ETH1 thus waits for an IP address to be assigned to the M10 by a DHCP Server within the network. Configuration and monitoring screens can be accessed from any computer within the “public LAN” by typing the M10’s IP address followed by :8443/admin into the address bar of a browser program (xxx.xxx.xxx.xxx:8443/admin).

2 Connecting the M10 to an existing LAN (Local Area Network)

The M10 is configured and operated through a browser-based web interface on ETH1 only. Hence, the DVI and USB ports on the front side of the device cannot be used. If desired, the M10 can work in “zero-touch” operation as soon as the system’s basic configuration is done.



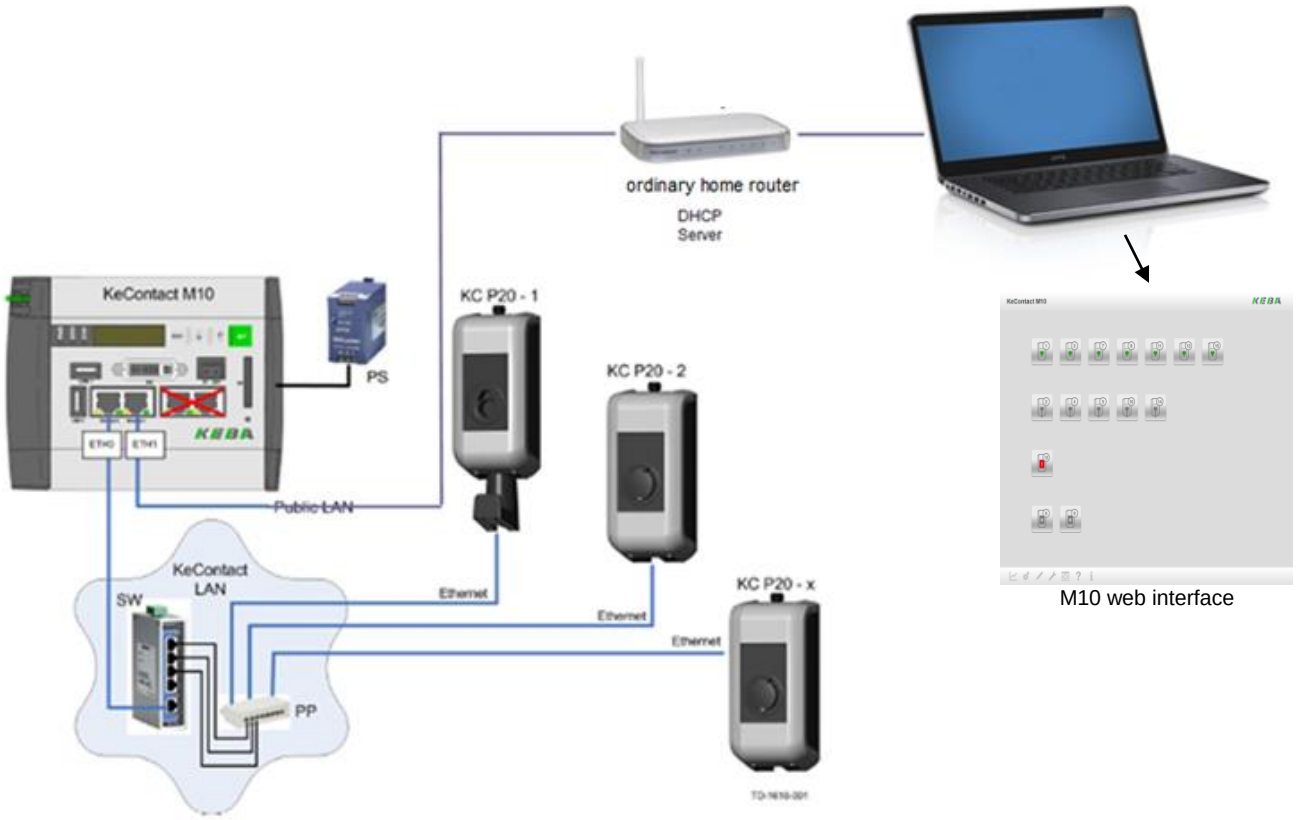
Example: M10 Connected to a company LAN

If the M10 is connected to a company LAN, for instance, it is up to the company network administrator to assign an IP address to the M10 within the respective network. As soon as an IP address is assigned to ETH1, the respective IP address will be displayed at the small LDC display at the front of the M10 device. In the picture above, you could monitor and control the M10 from any of those four depicted computers.

Currently the M10 uses HTTPS and port 8443 for its web interface on ETH1. So make sure that no network node within the public LAN (i.e. the company LAN in the picture above) blocks this protocol and this port. As HTTPS is a secured protocol for web contents, certificates are required. Ex works the M10 has insecure standard Keba certificates installed, which are valid for one year after first start-up. Please replace these with trusted certificates of your choice (further information about this procedure in the M10 system manual)

Please note that company LANs are almost always separated from the actual Internet. Although there are ways and options to connect to an M10 from anywhere around the world, it is not sufficient to simply know the IP address of ETH1 and thereby accessing the M10 through the Internet from somewhere else. Such solutions require the use of Dynamic Domain Name System software and it is up to the respective network administrator whether it is even allowed to access the M10 from outside the company LAN.

Another possibility would be to connect the M10 ETH1 to a simple home network router which mostly also run DHCP server. It is also possible to find out the M10's IP address by looking at the router webpage and see the list of "attached devices" (or similar). In any case, the important information to know is the IP address that has been assigned to ETH1.



Example: M10 connected to a home network router

The configuration and monitoring screens can again be accessed by typing the IP address of ETH1 IP into the address bar of a browser of any computer within the same network.

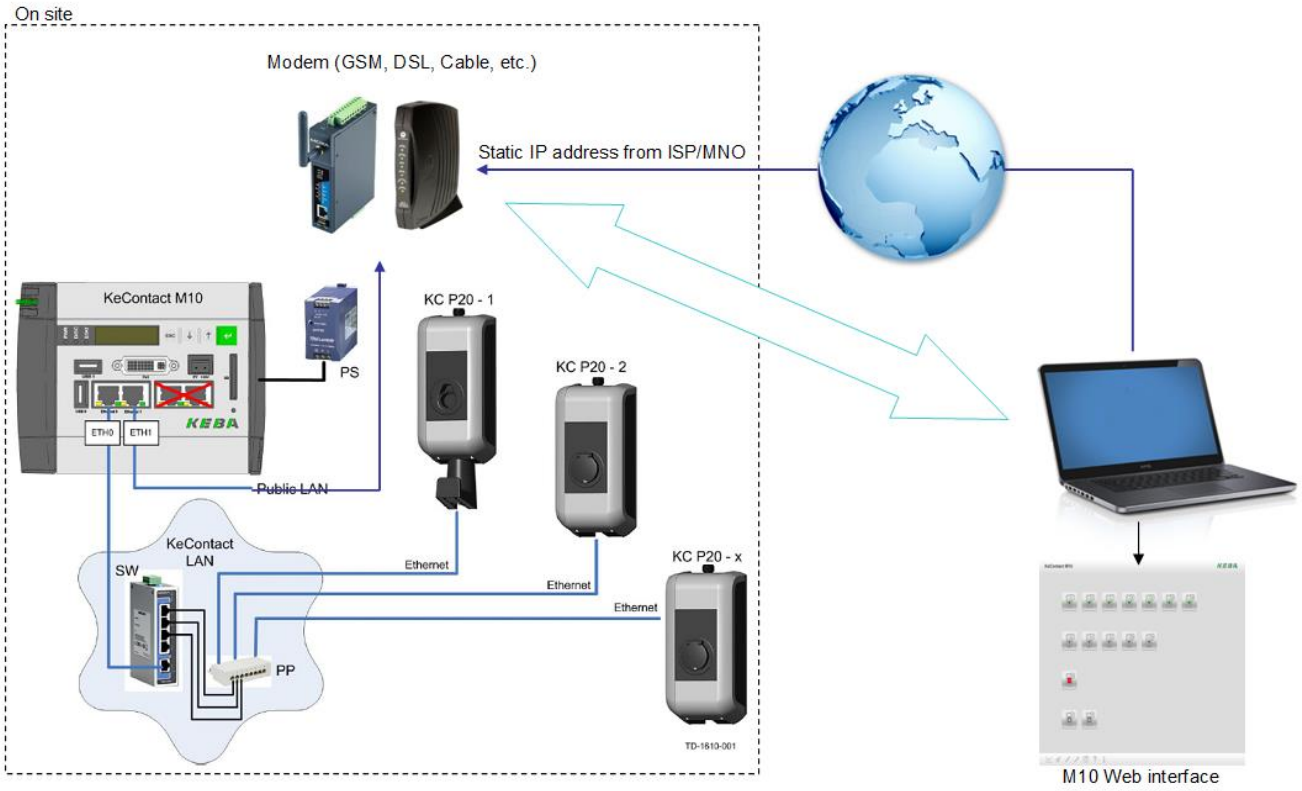
3 Connecting the M10 to the Internet directly (remote access)

In principal the M10 can be connected to the Internet/WAN too. Such a topology raises a number of questions on how to address the M10 remotely, though. If connected to the Internet/WAN directly, you would have to find out its IP address in order to access its web interface.

Connection with a static IP address

The first and most applicable solution is to connect to an internet connection with a static IP address, either hardwired (Cable/DSL modem, etc.) or mobile (GSM modem with SIM card). Suitable offers from Internet Service Providers (ISPs) and Mobile Network Operators (MNOs) are available to business customers in most countries. Please ask your preferred ISP/MNO for further information about static IP addresses.

If a static IP address is available, addressing the M10 remotely works just the same way as within a LAN by typing the IP address into the address bar of the browser.

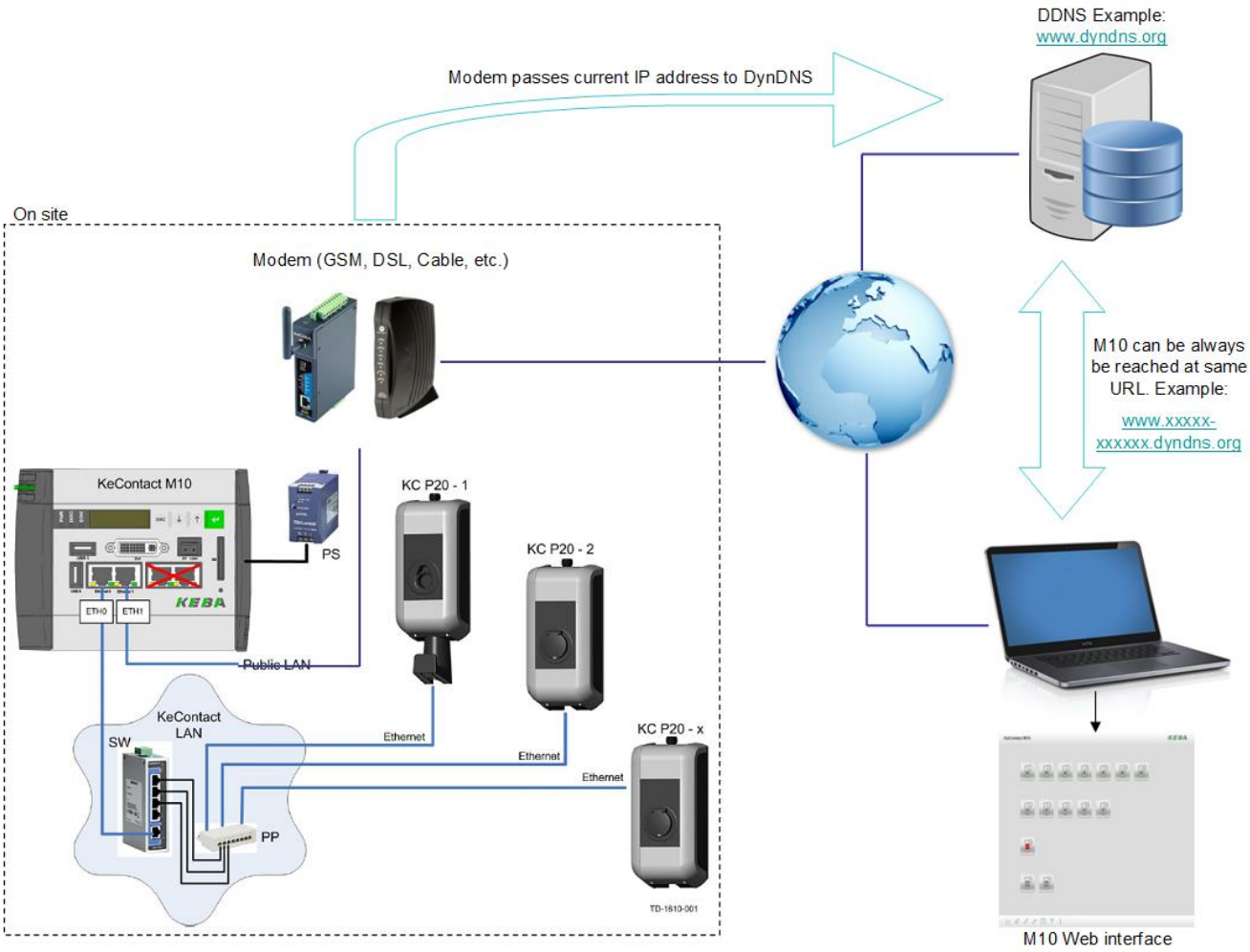


If the M10 is located in more remote areas and a mobile setup is required, we recommend the use of a Moxa G3100 series modem. For setups with dynamic IP addresses, this modem also features DynDNS (see next chapter).

Connection with dynamic IP addresses

As a matter of fact, in standard contracts most ISPs/MNOs dynamically assign IP addresses to their network clients. This is especially the case with most mobile contracts. This means that "finding" the M10 from a remote computer becomes more difficult. This is why we first and foremost see a typical installation of the M10 within an existing a company LAN, where an admin has a handle on connected devices and IP addresses.

However, addressing the M10 through the Internet is still possible. If an ISP assigns IP addresses dynamically, a system like DynDNS (or DDNS – Dynamic Domain Name System) comes into play (for example, www.dyndns.org). The idea of Dynamic DNS is to keep a host system up to date with the current IP address of a device. By using DDNS, the M10 can always be reached at the same domain name regardless of its current IP address. Many devices (modems, routers or even webcams) nowadays have DynDNS implemented and inform the DynDNS host continuously about their current IP address. The following picture provides an overview for such a setup.



With this system it is possible to connect to a M10 from any remote computer by typing the respective URL provided by the DynDNS host into the browser. DynDNS then automatically forwards to the M10.