Desigo™
Ethernet, TCP/IP, MS/TP and BACnet
Technical principles
## Contents

1. **About this manual**
   1.1 Introduction .................................................................6
   1.2 Target readers ............................................................6
   1.3 Product Security Disclaimer ...........................................6
   1.4 Additional literature ...................................................7

2. **Communications and network technologies**
   2.1 The ISO/OSI reference model .......................................8
   2.2 Protocols .................................................................9

3. **Ethernet principles**
   3.1 Standards ..................................................................11
   3.2 Topologies ..................................................................12
   3.2.1 Star/tree topology ....................................................12
   3.2.2 Ring topology .........................................................12
   3.2.3 Mash topology .......................................................13
   3.2.4 Additional topology types .........................................14
   3.2.5 Design and selection of suitable topology ..................14
   3.3 Cabling .....................................................................15
   3.3.1 Structured cabling ..................................................15
   3.3.2 Twisted pair for 100Base-TX and 1000Base-T ..........16
   3.3.3 Fiber optic cable for 100/1000Base-SX, 100/1000Base-LX ..17
   3.4 Addressing ................................................................18
   3.5 Network components ................................................19
   3.5.1 Media converters ...................................................19
   3.5.2 COM server, device server, gateways .......................19
   3.5.3 Time server ..........................................................20
   3.5.4 Switches ..............................................................20
   3.5.5 Router / Layer-3-Switch ..........................................22
   3.5.6 Firewall Layers 4 – 7 ...............................................23
   3.5.7 Wireless LAN (WLAN) ...........................................24
   3.5.8 LTE, UMTS, HSPA, GPRS, GSM cell communications .24
   3.5.9 Servers ..................................................................25
   3.6 Other Ethernet terms ..................................................25
   3.6.1 Power over Ethernet (PoE) ......................................25
   3.6.2 Network management systems ...............................26
   3.6.3 Network redundancy, high availability ....................27
   3.6.4 Auto-negotiation ....................................................27
   3.6.5 Link aggregation ...................................................27

4. **Principles of TCP/IP** .....................................................28
   4.1 Topology ..................................................................28
   4.2 TCP/IP protocol suite ................................................29
   4.2.1 ARP / RARP ..........................................................29
   4.2.2 IP .........................................................................29
   4.2.3 IPv6 .......................................................................32
   4.2.4 TCP .......................................................................35
   4.2.5 UDP .....................................................................35
   4.2.6 BOOTP / DHCP .....................................................35
   4.2.7 DNS / DDNS ..........................................................36
   4.2.8 SNMP ....................................................................37
## Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
<th>Section</th>
</tr>
</thead>
</table>
| V5      | 31.08.2012 | Additions:  
- Recommendation  
- Desigo MS/TP (Master-Slave/Token-Passing)                                                                                                                                  | 6.3     |
|         |          |                                                                                                                                                                                                    | 7, 8.3, 9.4 |
| V5.1    | 2013-03-30 | BACnet/IPv6 extensions  
- Various adjustments for IPv6  
- IPv6 (new Section)                                                                                                                                                    | Entire manual |
| V5.1 SP | 2013-11-30 | Updated to reflect Service Pack V5.1:  
- Various smaller updates  
- Power over Ethernet (PoE) (new section)  
- IT-Security (new section)                                                                                                                                         | Entire manual |
| V6.0    | 2015-10-21 | Revised for Desigo V6.0                                                                                                                                                                           | Entire manual |
| V6.0 SP | 2017-05-01 | Modified to reflect Service Pack V6.0:  
- Updated network graphics  
- Various modifications to MS/TP                                                                                                                                          | 6       |
|         |          |                                                                                                                                                                                                    | 7.3, 7.5 |
| V6.1    | 2017-05-01 | Desigo V6.1 revision:  
- Safety note supplemented  
- Various graphics updated  
- Appendix C (direct addressing of BACnet references…) supplemented                                                                 | 5.1     |
|         |          |                                                                                                                                                                                                    | 6       |
|         |          |                                                                                                                                                                                                    | 11      |
1 About this manual

1.1 Introduction

This manual is not an introduction to Ethernet, TCP/IP, MS/TP and BACnet. There are already enough books and courses on this subject. The aim here is to provide an overall view of communications technologies, specifically Ethernet, TCP/IP, MS/TP and BACnet. The emphasis here is on the "BACnet on IP" and "BACnet on MS/TP" combination. The manual explains the mechanisms involved and describes the systematic approach to troubleshooting. The principles are explained only where it is important to understand them in the context of the Desigo system. Rather than concentrating on the details, this manual focuses on the aspects relevant to Desigo.

1.2 Target readers

With the growing importance of Internet technologies for building automation and control systems, a deeper understanding of communications is required by all those involved. This is why this manual is addressed not only to readers with a technical background, but also to those with a commercial background. Depending on their needs, readers can concentrate on the principles, and skip the sections containing detailed information.

It is assumed that all readers have a basic technical understanding and a fundamental knowledge of communications and network technology.

1.3 Product Security Disclaimer

Siemens products and solutions provide IT-specific security functions to ensure the secure operation of building comfort, fire safety, security management and physical security systems. The security functions on these products and solutions are important components of a comprehensive security concept.

However, it is necessary to implement and maintain a comprehensive, state-of-the-art security concept that is customized to individual security needs. Such a security concept may result in additional site-specific preventive action to ensure that the building comfort, fire safety, security management or physical security systems for your site are operated in a secure manner. These measures may include, but are not limited to, separating networks, physically protecting system components, user awareness programs, in-depth security, and so on.

For additional information on building technology security and our offerings, contact your Siemens sales or project department. We strongly recommend signing up for our security advisories, which provide information on the latest security threats, patches and other mitigation measures.

## 1.4 Additional literature

<table>
<thead>
<tr>
<th>Ref. No.</th>
<th>Document</th>
<th>Document number</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>Network architecture</td>
<td>CM110664</td>
</tr>
<tr>
<td>[3]</td>
<td>System configuration</td>
<td>CM110664</td>
</tr>
<tr>
<td>[4]</td>
<td>Remote access</td>
<td>CM110664</td>
</tr>
<tr>
<td>[5]</td>
<td>Desigo Insight</td>
<td>CM110591</td>
</tr>
<tr>
<td>[7]</td>
<td>IT Security in Desigo Installations</td>
<td>CM110663</td>
</tr>
<tr>
<td>[8]</td>
<td>Desigo CC, System description version 2.1</td>
<td>A6V10415500</td>
</tr>
<tr>
<td>[9]</td>
<td>Desigo TRA Engineering, mounting and installation</td>
<td>CM111043</td>
</tr>
</tbody>
</table>
2 Communications and network technologies

It is impossible to maintain an overall mental picture of the world of communications today. Virtually every day a new protocol or protocol variant is published, and new terms and abbreviations are introduced. Usually, the best that home users can do is to hope that the default settings will suit their requirements. In business, however, with its increasingly complex IT structures, the default settings supplied by manufacturers are not good enough. This is where a better understanding of the principles is essential.

2.1 The ISO/OSI reference model

The ISO/OSI reference model (also known as the "seven-layer model") is an established way of describing communications between the nodes in a system. In this model, all communication functions are arranged in seven layers, known collectively as a "communications stack". When communicating, each layer uses only the services of the layer directly below it.

![Diagram of the ISO/OSI reference model]

Layer 7, like Layer 1, has a special position, in the sense that it represents a direct interface to the outside world. It provides the services required by the application.

In many systems, the functions of Layers 4, 5 and 6 are not shown separately, and are treated as part of the highest layer. These layers are thus not discussed in this document.

The third layers selects and manages the communications path. These services are not needed in simple systems with just one communications path, rendering the layer useless.

Layer 2 is where the procedure for access to the medium is defined, and where the security of the data is ensured (received data is checked for errors).

The lowest layer defines all the physical and mechanical parameters.

The assignment of a specific function to a given layer depends on the application or system under consideration. So, for example, the UDP service in the TCP/IP system is assigned to Layer 4, because it is a "Transport" service. From the BACnet perspective, however, it is only a simple service assigned to the Data Link Layer (refer to the Technical principles manual, Section 16).
2.2 Protocols

The discussion above relates to one node only. In this context, communication takes place between layers, by means of *services*. The purpose of communication however, is the exchange of data between two or more nodes. This communication, which takes place between two equal layers at opposite ends of a connection, is referred to as a *protocol*.

A specific layer may be implemented in various ways. BACnet uses various data link layers: UDP/IP, UDP/IPv6, Ethernet, ARCNET, MS/TP, PTP, and LonTalk. The criteria are firstly, that the selected technology must support the required services, and secondly that it must not exceed the technical limits. The following examples illustrate this aspect in relation to BACnet:

- The maximum length of a LonTalk datagram is limited to just 250 bytes. This leaves only 228 bytes for BACnet communications via the Network layer. Further, only 206 bytes are allowed for the Application layer. This limit is also a property of the device object (Max_ADPU_Length_Accepted).
- Similarly, MS/TP allows for a maximum of 501 bytes; IP allows for 1497 bytes.
- A BACnet broadcast must be distributed within a BACnet network via the Data Link Layer. If UDP/IP is used, the IP routers prevent the necessary distribution. For this reason, an additional intermediate layer must be provided (the BACnet Virtual Link Layer).
- When the BACnet protocol was defined, it was assumed that a fixed addressing scheme would be used (i.e. that the address in the Data Link Layer would not change). Although dynamic addressing (e.g. DHCP for UDP/IP) is possible, it leads to problems in conjunction with notifications (alarms/events and COV). DHCP is generally not allowed for devices with BBMD functionality (see Section 6.1.2).

BACnet over IP (or over IPv6) is based on the three protocol suites Ethernet, TCP/IP, and BACnet:

![Diagram of BACnet over IP protocol layers](image-url)

*Figure 2: BACnet over IP protocol layers*
The same principle applies for all other data links defined in the BACnet standard, including MS/TP as well:

![BACnet architecture](image)

As can be seen, BACnet/MSTP is based physically on EIA-485 (formerly known as "RS485").

The relevant aspects of the various protocol suites are introduced below and described within the context of a network.
3 Ethernet principles

3.1 Standards

Today, Ethernet is almost always used for the networking of computers within a local area (LAN). Both the American standards body, the Institute of Electrical and Electronic Engineers (IEEE) and the International Standard Organization (ISO) have standardized variants of Ethernet under 802.3 and ISO8802-3 respectively. Like Ethernet, the various standards for wireless LAN are located below the Logical Link Control layer.

<table>
<thead>
<tr>
<th>Protocol layers Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Link Control</strong></td>
</tr>
<tr>
<td>ISO8802-2 / IEEE802.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet variants</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10Base-T</strong></td>
</tr>
<tr>
<td>Ethernet via twisted pair copper cable, 10 Mbps</td>
</tr>
<tr>
<td><strong>100Base-TX</strong></td>
</tr>
<tr>
<td>Ethernet via twisted pair copper cable, 100 Mbps</td>
</tr>
<tr>
<td><strong>1000Base-T</strong></td>
</tr>
<tr>
<td>Gigabit Ethernet via twisted pair copper cable, 1000 Mbps</td>
</tr>
<tr>
<td><strong>10GBase-T</strong></td>
</tr>
<tr>
<td>10 Gigabit Ethernet via twisted pair copper cable at 10,000 Mbps</td>
</tr>
<tr>
<td><strong>100Base-FX/1000Base-SX</strong></td>
</tr>
<tr>
<td>Fast Ethernet via fiber optic cable (1300 nm/850 nm)</td>
</tr>
<tr>
<td><strong>1000Base-FX/1000Base-SX</strong></td>
</tr>
<tr>
<td>Gigabit Ethernet via fiber optic cable (1300 nm/850 nm)</td>
</tr>
<tr>
<td>(FX= Single mode, SX= Multi-mode)</td>
</tr>
</tbody>
</table>

Caution: Manufacturers often used different designations as well as different wavelengths.

Addition standards > 10 Gigabit Ethernet are generally found in fiber optics, but are not further described here.

10Base-T is still used with older equipment (PXG80-N and PXG80-WN), while all new products support **100Base-TX** with auto-negotiation. The auto-negotiation configuration protocol is used to negotiate a transmission mode (10 Mbps or 100 Mbps) before the data is actually transmitted.

Gigabit Ethernet and the fiber optic cable variants are not generally used for the automation level. They are used as a "backbone" in large networks, and (in the case of fiber optic cable only) to cover longer distances.

At the management level (server, management stations, or multimedia application), Gigabit technology is already the standard.
3.2 Topologies

Older topologies such as Token Ring, FDDI etc., but also older hardware such as repeaters and hubs are no longer pursued here.

3.2.1 Star/tree topology

In a star topology, the network participants are connected in a star over through a central switch. Star/tree topology has multiple star points in a network. Today, the star topology forms the basis for structured cabling and is commonly used. Communication fails when the central or core switch fails. Fiber optics and copper cabling can be combined in any manner here.

**Features**

- simple and smaller networks
- Less expensive installation
- Easy-to-understand
- No redundancy (back up against failures)
- managed or unmanaged switches can be selected
- Low operating costs

**Important!**

3.2.2 Ring topology

Special switches are connected on a ring topology in one or more rings. The ring can also be implemented using fiber optics or copper cabling. The current ring topology has nothing in common with the older token ring or FDDI. The various paths can be implements with fiber optics or copper cabling. In contrast to star topology, the central point is not decisive. Communication remains online even if a switch or connection fails. This type of topology is used if a plant must be highly reliable.
### Features
- Suitable for all large networks
- Specific planning is required
- High cabling expense
- Redundancy (back up against failures)
- Requires management switches capable of handling the ring
- Specialists recommended when planning and building larger networks and multiple rings
- Alarming and network management recommended
- Average operating costs (regular servicing, software, monitoring, etc.)

**Important!**

Switches with 2 voltage inputs are commonly offered to increase availability. Alarm messages can also be sent over hardware relay contacts (e.g. in the event a connection or power supply is lost, etc.).

**Note**

To learn more about the subject, please refer to the document "Practical Guide on IP Networks in Building Automation and Control Systems CM110668" [6].

#### 3.2.3 Mash topology

![Mash topology diagram](image)

Figure 7: Mash topology with root switch

Mash topology interconnects switches a number of times to significantly increase availability, and data transfer rates. Under the most extreme scenario, each switch is connected with all others (full mashed network). This form of topology is rather rare since it is extremely expensive to cable, plan, and commission.

**Features**
- for large networks with high availability
- Specific planning is required
- very high cabling expense
- Advanced redundancy (back up against failures)
- Only possible using "managed switches"
- Specialists for planning and building recommended
- Alarming and network management recommended
- Operating costs are high
3.2.4 Additional topology types

Another topology is the line topology or daisy chain. It can be compared to a bus system where the network devices are switched in series.

**Features**

- Low budget variant due to less cabling and fewer switch ports
- Availability is less solid compared to other topologies (probability of failure increase exponentially with the length of the chain)
- Only suitable for low data transfer rates (risk of bottleneck and delays during data transfer)

3.2.5 Design and selection of suitable topology

It is not always easy to select the proper topology. Plant or application requirements are always the decisive factor, however. Special attention should be directed at the network since it forms the backbone of automation communications.


**Rules**

- Decide in favor of one (1) topology and stick to it during construction as much as possible
- please remember that the selection of topology increases in importance for larger networks
- avoid linking switches (bus topology)
- use high-quality switches and cables (e.g. industrial standard)
- do not use outdated devices such as hubs and repeaters
- always use structured cabling (→ see cabling 3.3)
- We recommend using fiber optic cables for distances in excess of 100 meter between 2 switches.
3.3 Cabling

3.3.1 Structured cabling

Structured cabling, also referred to as UBC (Universal Building-Cabling) or UCC (Universal Communications-Cabling) describes the current standard on how to competently and correct install cabling.

The standard describes how to lay cables in ground (primary cabling), in the building (secondary cabling), and on floors (tertiary cabling).

The most important main rule to avoid faults on networks are:

**Rules**

- an installation cable (fiber optic or copper) always starts and ends at a plug or patch panel
- copper twisted part installation cables have a maximum length of 90 meters
- a patch cable (can be changed on site) never exceeds 1-5 meters
- the entire wire length for copper cables never exceeds 100 m between active components

**Benefits of structured cabling**

- the infrastructure is used for multiple applications/services
- simple troubleshooting thanks for easy-to-understand system
- measurements at the cables are possible
- a ground concept is possible
- modular and therefore easy to extend/change
- cabling is protected against dirt and unauthorized access since components are installed in rack or control cabinets

**Note**

TP installation cables include fixed copper wires, patch cables made of fine cores. A RJ-45 plug cannot be installed directly on an installation cable since the wires have different diameters. In addition, the patch cable is completely unsuitable for use on installation since it is not mechanically protected.

**Important!**

Incorrect or unclean cabling generally results in serious disturbances to data communication. And layer-1 errors are often very difficult to localize.
3.3.2 Twisted pair for 100Base-TX and 1000Base-T

Twisted pair cable technology (TP) is the current standard and consists of 4 twisted pairs each. The higher the category (Cat), the better the transmission characteristic and thus wiring reserves. Made possible at increasingly higher frequency. Design and execute cabling for ca. 20 years. As a result, we recommend using the newest category on new construction and renovation, but without overlooking general conditions such as various bending radius or cable types. Cable prices for the latest category is often less expensive than older categories.

The cable is available both unshielded (UTP – Unshielded Twisted Pair) and shielded (STP – Shielded Twisted Pair). UTP patch cables are suitable, for example, for interrupted shielding. Shielded installation cables are recommended in an industrial environment.

**RJ45 connector**

The classic RJ45 connector/plug are used up to and including Cat. 6a:

There are already various specifications that have changed over the years. The table below provides an overview:

<table>
<thead>
<tr>
<th>Category</th>
<th>Data transfer rate</th>
<th>max. length</th>
<th>Connector type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (UTP/STP)</td>
<td>100 Mbps</td>
<td>100 m</td>
<td>RJ-45</td>
</tr>
<tr>
<td>6 (UTP/STP)</td>
<td>1,000 Mbps</td>
<td>100 m</td>
<td>RJ-45</td>
</tr>
<tr>
<td>7 STP</td>
<td>10,000 Mbps</td>
<td>100 m</td>
<td>GG45 / TERA¹</td>
</tr>
</tbody>
</table>

*Note*  
Category 7 cables are often used in new construction but equipped with cat. 6 plugs and panels. This makes sense, however, since the cables are the cheapest and also permits upgrading the category on plugs or panels.

**Crossover cable**

The cable type in which the twisted pairs are crossed over is referred to as "crossover cable" or "link cable". This cable type is on the wane thanks to the increase in "Auto MDI/MDI-X" connections with automatic recognition of send and receive lines or their internal changeover. Only older generations of network device still require direct connection using a crossover cable.

*Note*  
When the two connectors of a crossover cable are placed side by side, it can be seen that the color sequence of the wires is not identical.

The different categories use a different number of core pairs. As a result, it does not make sense to split up TP cables that would not permit further category upgrades to the network.

---
¹A new connector system is required to use category 7 at 10GBit technology. At higher frequencies, the individual cores must have a larger distance to prevent crosstalk (NEXT).
3.3.3 Fiber optic cable for 100/1000Base-SX, 100/1000Base-LX

To cover long distances or in areas exposed to severe interference, fiber optic cables can be used instead of copper. The use of Ethernet switches is recommended with fiber optic cables.

With fiber optic cables, a distinction is made between single mode and multimode. With its very fine core (9 µm), single mode fiber is used primarily to span long distances (up to 180 km). Multimode fibers, with a larger diameter core (50 µm or previously 62.5 µm), are generally used for normal LAN connections (up to 2 km), as this type of fiber along with accessories is cheaper.

The fibers must be appropriate for the light source used (wavelength). The relevant data can be found in the switch/media converter specifications.

1000Base-LX is the commonly used standard for fiber optic LAN connections. The newer 1000Base-SX standard allows the use of lower-cost components, and is designed primarily for horizontal floor-by-floor cabling.

There are various types of fiber optic connector variants in use. Ready-made cables can be ordered in the required length from your dealer. Male-to-female adapter cables (patch cables) can also be purchased in various lengths. At the time of writing, LC connectors are particularly in favor.

![St connector, SC connector, LC connector, E2000 connector](image)

Figure 12: Common fiber optic connectors and couplers

The St connector was the first connector type used for LAN. Today, LC connectors have replaced SC connectors, which in turn have replaced ST connectors. All connector types are still in use (as per the applicable switch types) and can still be purchased, in particular, in the IT industrial range.

Additional practical information is available in the document "Practical Guide on IP Network in Building Automation and Control Systems CM110668" [6].
3.4 Addressing

During manufacture, every Ethernet device is assigned a globally unique address, which cannot be modified. This is referred to as the MAC (Medium Access Control) or hardware address. Since MAC addresses are also defined in other non-Ethernet-based systems, it is advisable to precede the address with the name of the system (e.g. Ethernet MAC address).

The Ethernet MAC address is 6 bytes long and expressed in hexadecimal notation. Examples:

- 00-30-05-6F-F5-98 Address of an Ethernet node
- FF-FF-FF-FF-FF-FF Broadcast address

The first 3 bytes identify the manufacturer based on IEEE assignment:

- 00-A0-03-

This 3 byte code can be helpful in troubleshooting the network. A complete list of all manufacturers is available on the Internet.
3.5 Network components

3.5.1 Media converters

Media converters are devices that connect network segments using different transmission media such as twisted pair cable or fiber optics and convert the transmitted data physically from one media to the other. There are also media converters that can convert, for example, fiber optics from multimode to signal mode.

The use of media converters is declining in general since most switches today can already be inexpensively equipped with optical ports. Switching fiber optic lines was an expensive affair just a few years ago. Moreover, one tremendous disadvantage of converters is that an additional network port, for example, a service port, is lacking.

![Figure 13 Media converter](image)

( red cable = fiber optics, grey cable = copper cable)

3.5.2 COM server, device server, gateways

Interfaces that are still common, such as RS-232, RS-422 and RS-485, are often rendered Ethernet capable in building automation and control using simple COM or device servers. The primary benefit is that it is possible to simply migrate older systems and avoid long serial cables.

It is also becoming increasingly difficult to find computers and servers with serial interfaces.

![Figure 14 COM server](image)

Devices with a similar function are called Gateways and are used to render building automation and control buses Ethernet capable.

For example: RTU/ASCII/TCP-to-EtherNet, PROFIBUS-to-PROFINET, PROFIBUS-to-Modbus-TCP and Serial-to-Ethernet Modbus-Gateways.
3.5.3 Time server

Technical networks often have no access to the Internet and are therefore lacking a time signal to synchronize system times on the network devices. This is important since computer internal clocks are imprecise, while different times cause all kinds of problems for alarms, time reactions, log messages, etc.

Time servers help here. They provide a time signal (e.g. RF clock) via Ethernet. Common time protocols include NTP (Network Time Protocol) and the older SNMP (Simple Network Time Protocol).

3.5.4 Switches

A switch can be regarded as a multiport bridge. Each port forms its own collision domain, to which only a small number of nodes are connected. Collisions are by-and-large avoided using micro segmenting and network capacity is also increased.

Switches can be classified into the following main categories:

![Switch categories](image)

Additional criteria
- Housing design, DIN rails (top hat), 19 inch, desktop
- modular or compact
- PoE ports (Power over Ethernet)
- Fiber optic connections
- Layer-2 and layer-3 functionality
- Stacking (connecting switches)
- 10-Gigabit uplinks

The differences between industrial and office switches are detailed in the document "Practical Guide to IP networks in Building Automation and Control Systems CM110668" [6].

The functions scope of the switches, which was once based solely on the hardware, is growing continuously:
Advantages

- **Layer 2 switches** (Ethernet switches) only take the Ethernet MAC address into account when transmitting a data packet. They do not require much configuration effort.
- **Layer 3 switches** also take account of details such as the IP addresses when forwarding data packets. In this way, they allow better structuring of the network and reduce the load from broadcast communications.

Another distinguishing feature is the scope for management. In this context, reference is made to **managed** and **unmanaged switches**. Managed switches normally have an IP address and can be managed using a Web browser or a CLI (Command Line Interface).

Virtual Local Area Network (VLAN)

Managed switches can be used to divide a network into several Virtual LANs. The grouping is based not on physical (geographical) criteria, but on logical associations. VLANs increase the security of information, because they enable user groups to be isolated from each other.

There are various mechanisms for the implementation of a VLAN. Normally each port is assigned to exactly one VLAN.

![Figure 16: VLAN example](image)

Note

The use of VLAN technology for the building automation and control system is particularly suitable for buildings with an existing IT infrastructure or if multiple applications are operated on the same network. The IT administrator can isolate ports for the building automation and control system in any location in the building. This method of grouping into logically separate networks increases the security and stability of the network, but without the need for additional cabling.

Notes on selecting suitable switches as well as other information and recommendations on the subject are available in the document "Practical Guide on IP Networks in Building Automation and Control Systems CM110668" [6].

---

2 In addition, so-called "tagged VLANs" as per IEEE 802.1q exist, where assignment is not by port but by additional information from internal data package information. This procedure is not generally applied in end device connections, and is thus not supported by Desigo.
3.5.5 Router / Layer-3-Switch

A router is used to connect one IP subnet with another. It operates at the Network Layer of the ISO/OSI reference model. It transmits IP packets to the correct subnets, and blocks limited broadcasts (255.255.255.255) or link-local multicasts von IPv6. If a packet is too large to transfer, the router divides it into fragments IP routers can be either IPv4 or IPv6 routers. IPv4 is incompatible with IPv6. For details on IPv6 see [4.2.3]

As an auxiliary function, most routers can also be used to filter specific TCP and UDP services.

However, the main task of a router is, and remains, the connection of IP subnets. Particularly when connecting a private network to the Internet, a router is indispensable. If IP addresses from the private range are used for the hosts within the private network, this address information must not be transmitted to the Internet. With Network Address Translation (NAT) the internal addresses of the hosts are mapped by the router to one or more external (official) addresses. NAT works well for communication connections initiated by a private network. In the case of requests from the Internet (e.g. HTTP requests to a Web server), NAT only accepts one host as the recipient.

NAT

However, when using NAT, certain limitations also have to be accepted.

- NAT looks only at the address information in the IP header. If applications transmit IP addresses as use data, NAT does not adapt them. The IP addresses are invalid outside the private network and communications thus interrupted.
- NAT modifies the IP header. Certain security protocols (e.g. IPSec) see this change, and discard the packet as "invalid".

Layer-3-Switch

Router functionality is fully covered today with Layer-3 switches. Layer-3 switches are multifunction devices representing a combination of router and switch. The Layer-3 switch can router various VLANs to one another. The VLANs remain autonomous but permit a network transition or common interfaces. Multiple Layer-3 switches can operate redundant routing depending on functionality. The somewhat more expensive switches, even permit to some extent layer-4 and higher functionality. As a result, certain restrictions can be implemented on TCP and UDP. ACL (Access Control List) is used to achieve this. Layer-3 switches are often used at the core. Managed layer-2 switches often suffice for distribution of the VLANs.

![Layer-3 switch with VLAN routing](image-url)
The following example illustrates a larger topology using two Layer-3 core switches designed to be redundant. In the event a switch fails, the distribution switches on ring A and B are taken over by the still operating system. So that routing continues to operate.

![High availability topology diagram](image)

3.5.6 Firewall Layers 4 – 7

A **firewall** is a system (or group of systems) that checks communications between two or more networks based on rules. The checking of a packet can cover the addresses, the type of packet and sometimes also the contents of the packet. Packets can be blocked or forwarded to a specified host. The firewall keeps a record of all actions, and generates alarms in the event of serious problems.

Firewalls are not only connected between the Internet and Intranet, but can also be used to protect critical areas within a corporate network. Different firewalls vary widely in their functional scope. In all cases the correct and effective use of a firewall depends on qualified specialists and constant checking of the system.

Additional, extended firewall rules must be adhered to for IPv6.

Firewalls are increasingly used on technical networks since they are tasked with executing an growing number of security related tasks (access control, video monitoring, etc.). A firewall must be implemented today for any remote access to a network.

**Note**

The document "IT security in installations with Desigo (CM110663)" [7] offers additional help on the topic.
3.5.7 Wireless LAN (WLAN)

Wireless networks (WLAN) are occasionally confused for VLANs, yet they do share some features. They are already different standards on the market since the technology behind wireless networks is subject to extremely fast development cycles. They are only used, due to RF transmission, if cabling is not possible or appears to be expensive.

Wireless transmission has a lot of overhead communication (data bits required for the secure transmission over the air) of up to 50%, not very efficient. In addition data transmission rates on wireless networks are considerably lower due to influence from other networks or other sources of disturbance (devices with RF frequencies) than for cabling with newer switches and end devices.

For example, a data transfer rate of up to 300 Mbps for newer standards can under best case scenario achieve 150 Mbps (no interference by third parties or barriers with a client and access point). For each additional wireless client, the 150 Mbps can be further divided by the total number of clients.

The only way to ensure stable 24 hour operation of wireless networks is to use the latest standards and a central WLAN controller. The WLAN controller are capable of reacting to changes in the RF range and thus able to provide coverage to a larger building.

3.5.8 LTE, UMTS, HSPA, GPRS, GSM cell communications

Developments in mobile data communication open up even more opportunities to connect with technical facilities. For example, remote access, alarming, and monitoring. Prices are sinking worldwide for what have been rather expensive services. The latest generations 3G/4G have download rates of up to 300 Mbps. Some manufacturers of industrial routers or modems are already working with cellular technology (SIM card required) to use technical networks.

It is primarily suited for use on the following applications and often only temporarily:

- Internet connections
- Alarming
- Remote access
- As backup line (secure)

Use of end devices and frequencies in the 800-2600 MHz range varies greatly by country. Public Internet address are in some cases no automatically used depending the provider subscription. So that direct access to such routers is limited.

Clarify with your ISP (Internet Service Provider) in advance.

A secure and proper configuration can take a number of hours!
3.5.9 Servers

The network infrastructure also includes the various servers which provide the hosts with the necessary services. This includes domain controllers, DNS, DHCP, web, file, terminal, and print server.

The server functions are frequently implemented on server hardware located in special server rooms. These servers are indispensable for the correct functioning of the network, which is why it is important to ensure that they are not accidentally switched off or disconnected from the network.

To increase server reliability, we recommend using a redundant power system and RAID (Redundant Array of Independent Disks). Depending on the configuration, these system can handle a hardware failure, for example, a disk crash, without stopping the services.

Plan to exchange server hardware after approximately 5-6 years to avoid longer downtimes.

3.6 Other Ethernet terms

3.6.1 Power over Ethernet (PoE)

Please consult the following standard to learn more about PoE:
http://standards.ieee.org/about/get/802/802.3.html

Standard IEEE 802.3af/at defines powering nodes (PoE) via Ethernet cabling. The target group are low powered unit units (IP telephones, WLAN Access Points, network cameras, etc.). Power (48 VDC, 350 mA in continuous operation) is provided via hubs or switches and is either provided through two free stand pairs on the Cat 5 cable to the end unit or directly, set up on the data line. The voltage source tests the nodes with a test current prior to supplying the full output. This prevents non-PoE compliant nodes from being damaged.

Depending on the application, switches with PoE support are used are special PoE adapters are inserted in a connection. A new standard has existed since 2009, IEEE 802.3at-2009 ("PoE+"), that increases the maximum power output from 15.4 to 25.5 Watts (or the maximum power consumption from 350 mA to 600 mA).

Which switch type to use?

Standard switches available on the market meet general requirements. Note primarily the following
- Required number of connection,
- Required power,
- Operating voltage required by the switch
  (for PoE, 48 VDC is needed, various switches can, however, be operated at, for example, 18...24 VDC and supply the 48 VDC for PoE using a step up).
- Installation location (due to degree of protection),

PoE topology

PoE requires cleanly structured cabling since the network cable is also used as the power cable. There now exist all kinds of combination devices that provide some or even all ports with PoE. Please attention however to overall power drawn by devices.
Ethernet connection
- Standard Ethernet cable min. category 5
- Shielded or unshielded STP / UTP
  STP (Shielded Twisted Pair) bzw.
  UTP (Unshielded Twisted Pair)
- Length between switch and end unit max. 100 m

Energy supply, energy transmission
The energy is supplied either directly by the PoE switch (end span) or via an intermediate electrical source (Midspan), e.g. via a PoE injector. Energy is transmitted dependent on the energy supply used as remote feed or via an unused strand pair.

Notes
- PoE ports can be specially configured on managed switches. For example, which how much a port can draw in power or which port to switch off if output is too high. It is for this reason that PoE is controversial in some circle since too many services burden the switch. As a result, the boot process for PoE switches can take from just a few seconds to a few minutes.
- For physical reasons, PoE power can only be provided over copper cable and not over fiber optics.

3.6.2 Network management systems

Network management systems, generally found on larger networks, proactively monitor networks and all their components. These systems permit the centralized output of faults including power outages, defective switches, or voltage sources, as well as output data on current load levels. The systems are mostly based on (Simple Network Management Protocol), which currently support a large percentage of management devices.

Passive outlets and patch panels are not included here for reasons of clarity.

Figure 19 Network management in a ring topology
3.6.3 Network redundancy, high availability

Network redundancy refers to building networks that are fail safe. A network must be as reliable as possible since an increasing number of services are run over the network. So that, for example, the loss of an Ethernet path or switch can be taken over by another component. There are various proprietary protocols depending on the manufacturer that initiate countermeasures within 0 - 500 ms. There are also generally applicable standards supported by various providers. More commonly recognized protocols include RSTP (Rapid Spanning Tree Protocol) or MRP (Media Redundancy Protocol). It is important to clarify in advance what the requirements are.

3.6.4 Auto-negotiation

A port that supports auto-negotiation negotiates with the port at the other end of the link to determine which bit rate (10, 100, or 1000 Mbps) and which transfer mode (full or half duplex) to use. Only switches capable of auto-negotiation should be used.

Auto Negotiation often results in fault on Gigabit technology of extremely slow communications. As a consequence, it is advantageous to set Gigabit uplinks for switches and server interfaces continuously to 1000 Mbps full duplex. Ensure that the settings are identical on both ends.

These settings are not possible on unmanaged switches.

3.6.5 Link aggregation

Link aggregation refers to multiple, parallel lines between two switches used as one link. This increases the data transmission rate on the network while also benefiting from redundant connections.

The managed switches must support these protocols, e.g. LACP (Link Aggregation Control Protocol) (IEEE 802.3ad) at both ends and must be specially configured. Pay special attention to avoid creating a loop on the network. This is particularly true when deleting an active configuration before removing the multiple lines.
4 Principles of TCP/IP

4.1 Topology

The TCP/IP protocol suite, which came into being around 1978, was first used to interconnect different proprietary networks. Very quickly, however, TCP/IP also became the established standard for local networks.

![Network Diagram]

Figure 20: The various network areas

**Definitions**

The various networks are referred to by different names:

- **Internet**
  
  The Internet is formed by the worldwide connection of individual networks on the basis of the Internet Protocol (IP). The means of access to the Internet by private individuals and companies is provided by an Internet Service Provider (ISP).

- **DMZ**
  
  The Internet is an uncontrollable medium, with all the associated risks for the networks connected to it. Special protection is therefore provided at the "point of entry" to the network of a company or organization. This area is referred to as a demilitarized zone (DMZ). All servers to which access is also required from the Internet (e.g. Web servers) are placed within the DMZ.

- **Intranet / Private Network**
  
  Private networks are connected to the Internet via a router. These private networks are also referred to as intranets.

- **IP subnet**
  
  Simple private networks normally consist of only one IP subnet. In larger networks, the Intranet is broken down into subnets by use of routers. So, for example, separate subnets can be created for the office applications and the building automation and control system network. Areas separated by routers are referred to as IP subnets.

Access to the Intranet from the Internet is only permitted via special security protocols (see Section 4.3 Remote access and Virtual Private Networks (VPN)).
4.2 TCP/IP protocol suite

The TCP/IP protocol suite consists of numerous protocols. They all share the Internet Protocol (IP) as a common base. The diagram shows the main protocols and how they are interrelated.

![TCP/IP protocol suite diagram](Ethernet)

4.2.1 ARP / RARP

IP nodes need to know the addresses of all other IP nodes in a network, in order that they can communicate. "Address resolution" is the process whereby the IP address of a node is mapped to its hardware address (Ethernet MAC address).

The Address Resolution Protocol (ARP) is the protocol responsible for address resolution in broadcast-based networks (e.g. Ethernet). An IP node requests the Ethernet MAC address for a given IP address by sending an ARP request. The request is broadcast on the network. Upon receipt, the IP address and the associated Ethernet MAC address are saved in the ARP cache. This avoids having to repeat the address resolution process with each transmission. Cache entries that are no longer used are deleted after a certain period of time.

Reverse Address Resolution Protocol (RARP) can be used by a node to obtain an IP address upon start-up of an address server. RARP has largely been replaced by DHCP.

For IPv6, ARP/RARP has been fully replaced by the Neighbor Discovery Protocol (NDP), which is based on ICMPv6.

4.2.2 IP

The Internet Protocol (IP) is the basis for TCP/IP architecture. All nodes in the Internet "understand" this protocol. The main tasks of IP include the addressing, fragmenting and routing of data packets.

IP provides "best effort" delivery, without any guarantee. An IP packet may get lost on the way from the sender to the recipient, or it may be delivered in the wrong order, duplicated or held up. No acknowledgement is required upon receipt of a packet. A higher transport layer (e.g. TCP) is responsible for acknowledging, sorting, and considering lost or duplicate packets.
IP addressing

The address of an IPv4 node is defined with a 32-bit value and represented as four
decimal numbers separated by periods (e.g. 172.16.87.12). Every address
includes a network identification (Net ID) and a host identification (Host ID). The
number of bits in the Net ID is determined by the subnet mask. The subnet mask is
the same length as the IP address, with all bits in the Net ID component set to 1
(e.g. 255.255.252.0).

Example of the breakdown into Net ID and Host ID for a given subnet mask:

IP Address: 172.16.87.12

10101100 00010000 01010111 00001100

Subnet Mask: 255.255.252.0

11111111 11111111 11111100 00000000

<table>
<thead>
<tr>
<th>31</th>
<th>24</th>
<th>23</th>
<th>16</th>
<th>15</th>
<th>8</th>
<th>7</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Net-ID Host-ID

Figure 22: IP addressing

To communicate with all the IP nodes on a given IP subnet, all bits of the Host ID
are set to 1 (in our example 172.16.87.255). When all 32 bits are set to 1
(255.255.255.255) this is referred to as a limited broadcast. This type of broadcast
is used by nodes in the start-up or configuration phases. Limited broadcasts should
not be used in normal operation.

The IP address ranges are allocated by the IANA (Internet Assigned Numbers
Authority, [www.iana.org](http://www.iana.org)). RFC1918 defines three specific address areas for
private networks. IP addresses within these ranges are not routed.

<table>
<thead>
<tr>
<th></th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>172.16.0.0</td>
<td>255.240.0.0</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

Fragmentation

Fragmentation refers to the breaking up of a large packet into several small
packets. Fragmentation is required when the original packet is too large for the
underlying network (for example: Ethernet allows from 1500 byte data).
Fragmentation can be used by both the sender and the IP routers. The recipient is
responsible for reassembling the fragments.

IP routing

The IP routers / Layer-3 switches are primarily responsible for packets transmitted
from the sender to the recipient across several networks. However, the sender has
to decide whether the recipient is in the same IP subnet or whether the IP packets
need to be transmitted to an IP router to then be routed to another IP subnet. For
this purpose, in addition to the IP address and subnet mask, a default gateway is
also configured for each IP node. The default gateway is the IP address of the next
IP router.

When sending a packet, the sender calculates its own Net ID via the subnet mask
and the destination Net ID via the destination IP address. If the Net IDs are
identical, the recipient is on the same IP subnet and the packet can be sent directly
to the recipient. If the Net IDs are different, the recipient is on another subnet, and
the packet is addressed to the default gateway. In both cases, the end recipient is
entered as the destination address in the IP packet. However, in the first case, the
sender uses the Ethernet MAC address of the recipient, and in the second case,
that of the router.
IP subnet routing

An IP subnet is designated with an IP address whose host bits are set to 0. The above example includes subnet links 192.168.111.0 the IP addresses in the range from 192.168.111.1 to 192.168.111.254. In the example to the right, subnet 192.168.112.0 includes IP addresses in the range of 192.168.112.1 to 192.168.112.254.

As a rule, an Ethernet segment only accommodates IP nodes of the same subnet. The packet is sent to the default route (192.168.111.1) if the station want to establish contact with the controller. The router provides the packet to the target address in the right subnet.

Among technicians, the first or last IP address on the subnet is now used as the default gateway.

Note on IPv4 ↔ IPv6
The information in this section relates to the IP version most commonly in use today (IPv4). The new protocol generation (IPv6) has only limited downward compatibility to IPv4. For IPv4, existing transmission media can physically continue to be used, but the new IPv6 networks add logically independent IP subnets to them. Connections between IPv4 and IPv6 subnets are not possible on the lower layers using simple means, and are thus carried out primarily by applications (OSI layer 7). This also applies to BACnet, which employs a corresponding BACnet router to implement BACnet/IPv4 and BACnet/IPv6.

Advantages of IPv6
IPv6 extends the IP address from 32 to 128 bits. The new addressing scheme allows a significantly greater number of IP nodes to be connected to the Internet. The bigger IPv6 addresses impact the data formats of the BACnet standard. As a result, changes to the BACnet standard will be required, likely to be introduced via Addendum in 2016.

ICMP: Error and control messages
The Internet Control Management Protocol (ICMP) sends error and control messages on behalf of IP. The most common and best-known use of ICMP is the transmission of an ICMP Echo Request to a given address, and the evaluation of the ICMP Echo Replies received. The "Ping" utility used for this purpose can be found on every PC.

In reality, PING is used primarily to located errors, check if individual IP network nodes can be reached; see Section 8.2.

IGMP: Multicasting
The Internet Group Management Protocol (IGMP) is used for multicasting. Unlike broadcasting, multicasting is addressed not to all nodes on a network, but only to a specified group. IGMP informs the routers which hosts in a network belong to a given multicast group.
4.2.3  IPv6

Internet Protocol (IPv6) succeeds Internet protocol IPv4. It was standardized in 1998 and, in addition to a larger address range and a simplified header format, contains a few more new features:

- More efficient routing
- Fixed header size
- No more fragmentation
- Security
- Integrated IPSec (optional), integrated QoS
- Other features: Auto-configuration, multicast, mobility extension, etc.
- ICMPv6: Very powerful, assumes ARP function

**Compatibility**
IPv6 is not compatible with IPv4. Parallel operation of IPv4 and IPv6, however, is still possible under the following modes:

"Dual stack mode"
Dual stack mode is supported by all large operating systems. Here, the application protocols (e.g. BACnet) must also be implemented at the application layer, as the network layer does not support it. As a result, IPv6 from the viewpoint of the BACnet user behaves toward IPv4 as differently as e.g. LonTalk, MS/TP or an other data link. The only difference is that IPv6 and IPv4 use the same physical medium (network cable) in parallel.

Furthermore, there are different ways to tunnel IPv6 via IPv4 for migration purposes (6to4, teredo, 6rd...) and vice-versa (4in6). Different mappers are also available (e.g. NAT64).

"Tunnel"
Tunnels emulate an IPv4 path through an IPv6 network (or vice-versa). Devices connected this way always only "speak" IPv4 or IPv6.

"Mapper"
Mappers are used for mixed scenarios by simultaneously connecting IPv4 and IPv6 devices. Here, a network infrastructure component (e.g. NAT64-Mapper) converts IPv4 addresses 1:1 into IPv6 addresses (and vice-versa).

**Restrictions**
Tunnels and mappers however can be recommended only within limits for the following reasons:

- Tunnels are end-to-end connections, required between each pair of the devices to be connected.
- Tunnels prevent true cross communications between BACnet/IPv6 with BACnet/IPv4 devices (or any other application protocol), and become useless at the latest when used in a mixed environment of both device types.
- Mappers apply the AT principle and thus also contain NAT-related issues. In particular, each device has two different addresses depending on the network side talking to the device.
- Both methods require high administrative efforts and close cooperation with the customer's IT department!


**IP addressing**
The IPv6 address is determined by a 128 bit value and is represented in a special notation defined for IPv6 (see below)).

Similar to IPv4, each address contains a network identification (network prefix) and a host identification (interface identifier). These normally are 64 bit long.

To form hierarchies and subnets, the network prefix can be subdivided into different lengths. The prefix length is used to determine the number of bits of a subnet, contrary to the subnet mask. /64 are 64 bit.
IPv6 address example

<table>
<thead>
<tr>
<th>Global Routing Prefix</th>
<th>Subnet</th>
<th>Interface Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>48 bits from provider (ISP)</td>
<td>16 bits local subnet</td>
<td>Identifies host e.g. from MAC addr</td>
</tr>
</tbody>
</table>

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

Figure 24  IP addressing

**IPv6 address notation:**
The IPv6 address is 128 bits long. It is represented in hexadecimal notation and divided into 8 16-bit blocks:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

To simplify the notation, the leading zeroes can be skipped for each block. In addition, sequential zeroes can once be replaced by a double colon "::".
The above address then has the following notation:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A or FF02:0:0:0:0:0:0:2 becomes to FF02::2

Literal IPv6 addresses (e.g. as URL in a web browser) are possible also. In this case, the address is packed into square brackets.

http://[2001:db8:100:f101:210:a4ff:fe01:2345]:8080/foo

**IPv6 address range and prefixes:**
The IP address range and prefixes are defined and assigned by IANA (Internet Assigned Numbers Authority, [www.iana.org](http://www.iana.org)).

**Global unicast addresses 2000::/3**
Equivalent to public IPv4 addresses (administered by IANA). They can be routed globally in the IPv6 portion of the Internet.

**Link-local addresses FE80::/64**
Equivalent to IPv4 link-local addresses (Auto IP 169.254.0.0/16). Cannot be routed.

**Unique local unicast addresses FC00::/7**
Identical to IPv4 private addresses. The uniqueness of the address is achieved by a random, global ID, therefore preventing routing conflicts.
The addresses can be routed globally and generated by the user.
The algorithm to calculate a global unique local identifier as described in RFC 4193.
For this purpose, the Internet contains a number of different tools (searches for "RFC4193 online calculator").
Multicast addresses FF00::/8
Equivalent to IPv4 multicast addresses with different spreading scopes. Replaces the traditional IPv4 broadcast.

Often required, special addresses:
- ::1 is the own address "loopback", comparable to the "127.0.0.1" local host address within IPv4
- :: (corresponds to a zeroes) is the unspecified address that indicates an address error similar to 0.0.0.0 within IPv4
- ff02::1 Multicast address for all devices on this subnet
- ff02::2 Multicast address for all routers on this subnet

Fragmentation
Designates the subdivision of a large packet into several small packets. Contrary to IPv4, fragmentation in IPv6 is possible only between end nodes and will no longer be executed by the routers.

IP routing
Designates the transmission of a packet from a sender to a recipient via several networks. Primarily carried out by the IP routers. For IPv6, transmission is carried out due to the changed header format of IPv6 routers.

IP configuration
IPv6 addresses can be configured similar to IPv4. A distinction is made between manual and automatic address assignment.

![Diagram of IPv6 configuration](image)

Conversely to IPv4, the final IPv6 address is generated in the host itself.

Normally, an IPv6 host has several IPv6 addresses per network interface.

The interface ID normally is based on the MAC address of the host. E.g. for link-local addresses.

For reasons of global retracability, the identifier can regularly be regenerated also based on a random number. (IPv6 "privacy extensions").

**Note**
As any automatic process that can change the address, this may result in application problems. For example, BACnet requires static addresses in the related BDT tables when using BBMD mechanisms, which in turn results in conflicts with dynamically changing IPv6 addresses.

For IPv6, DHCPv6 was completely remodeled and supplemented by a few additional functions. Operation is identical with the exception of the following variants:
- In *Stateful DHCPv6*, the network prefix is transmitted to the hosts by DHCPv6 (analogous to DHCP for IPv4).
- In *Stateless DHCPv6*, only additional information such as DNS server names etc. are transmitted to the hosts.
The host discovers its routers and other devices via the ICMPv6 Neighbor Discovery Protocol.

In IPv6 addressing, applications must be able to handle changing IP addresses. This can be prevented with manual addresses. For this reason, the importance of the domain name system (DNS) will grow (see Section 4.2.7).

### 4.2.4 TCP

*Transmission Control Protocol (TCP)* is responsible for the reliable transmission of data via the "unreliable" IP service. Before the actual data transmission can begin, a connection needs to be established. TCP is therefore described as a "connection-oriented" protocol. TCP is thus well suited for communicating over longer paths. In addition, TCP is broadly accepted in the IT world due to improved traceability. Typical applications that use TCP include http, https or smtp. Applications that use a TCP service are addressed by means of port numbers. The combination of IP address and port number for unique identification of each connection is referred to as a "socket". In the socket notation, the IP address is separated from the port number by a colon (e.g. 172.16.255.255:6301 or [0.0.0.0.0.0.0.0]:80 for IPv6)

### 4.2.5 UDP

*User Datagram Protocol (UDP)* is a simple connectionless transmission protocol. The processes or applications are addressed by port number, as with TCP. Since UDP is a "connectionless" protocol, the datagrams can be transmitted as broadcasts. For this reason, many management protocols (DHCP, DNS etc.) as well as the BACnet protocol are based on UDP.

### 4.2.6 BOOTP / DHCP

Each device requires initial data (IP address, subnet mask, gateway address) to communicate in an IP network. One of the following protocols to automatically assign these parameters can be used if the network has a protocol-capable server:

- The *Bootstrap Protocol (BOOTP)* is used by a host to retrieve its IP address settings from the network. Unlike RARP, BOOTP provides numerous other settings. For each host, a configuration file must be lodged with the BOOTP server. Today, BOOTP has largely been replaced by DHCP.

- Dynamic Host Configuration Protocol (DHCP) is an extension of BOOTP. DHCP permits the automatic configuration of the host. With DHCP, all the required address settings can be transmitted in one datagram. The DHCP server handles a pool of IP addresses, which it allocates to the DHCP clients. The allocation of the IP address is subject to a time limit and must be renewed by the client.

  The DHCP client can use a *DHCP Request* to send a "wish list" of all the required values to the DHCP server. The DHCP server replies with a *DHCP Acknowledge* packet containing the available values. Hence, the question of whether the client receives all the data required depends on the configuration and implementation of the server.

For IPv6, DHCPv6 was completely remodeled and supplemented by a few additional functions. Operation is identical with the exception of the following variants:
• In Stateful DHCPv6 the network prefix is transmitted to the hosts by DHCPv6 in place of the IPv6 r (analogous to DHCP for IPv4).
• In Stateless DHCPv6, only additional information such as DNS server names etc. are transmitted to the hosts.

Note

A lot of network participants from building automation and control, but in other technical environments as well, use static rather than dynamic IP addresses. This permits operation of the plant regardless of server services such as DHCP or DNS. One disadvantage is that each device must be manually switched for any change to IP configuration.

4.2.7 DNS / DDNS

The Domain Name System (DNS) allows the mapping of obscure IP addresses into easily understandable names. DNS is based on a hierarchical approach.

www.siemens.ch
www.siemens.com
intranet.sbt.siemens.com

The domain names are structured hierarchically from right to left. The individual elements are referred to as labels, and are separated by periods. The "top-level" domain is on the extreme right and denotes either a country (en, de, etc.) or a type of organization (com, org, net, etc.). The labels that directly follow the top-level domain must be unique for the domain.

The allocation of top level domains is the responsibility of the IANA (www.iana.org) which, in turn has delegated the administration of the subdomains (e.g. siemens.com).

The mapping of domain names to IP addresses (IPv4 A records) is handled by the DNS servers. A client can initiate a search for the required IP address by sending a DNS Query to a DNS server. The server either answers the request or forwards it to other known servers. The client therefore needs to know at least one DNS server as a starting point.

When DHCP is used, the IP address can change during operation. This means that the associated entry in the DNS server must also be adapted. The Dynamic Domain Name System (DDNS) allows a host to transmit a DNS update to the DNS server after a change of IP address, in order to update the change in the server too.

The DNS (domain name system) was extended by AAAA records to handle large addresses in IPv6. Furthermore, A and AAAA records can point to the same host. In this case, the client must receive a preference indicating the address to be preferred.
4.2.8 SNMP

Simple Network Management Protocol (SNMP) allows network nodes to exchange management information. It is an optional component of the TCP/IP protocol suite. SNMP allows the network administrator to identify and solve network problems, to manage the network capacity and to plan for network growth.

An SNMP system consists of an SNMP management station and SNMP-compatible network nodes (so called "SNMP-Agents"). The nodes contain a Management Information Base (MIB).

MIB is a hierarchically organized collection of information. There are various standardized MIBs. The best-known of these is the "Management Information Base for Network Management of TCP/IP-based Internets", or MIB-II for short (RFC1213). In addition to general node information, MIB-II also contains various protocol statistics. The majority of this information is read-only data. Write access is only possible with selected objects. Owing to the absence of security mechanisms in earlier versions of SNMP, many manufacturers have not implemented write access ("Set operation"), thereby reducing SNMP to a retrieval system only.

Three versions exist: SNMP V1, SNMP V2 and (since March 2002) SNMP V3. All versions incorporate the same basic range of functions. However, SNMP V3 is the only variant of the protocol with multiple security models. The older versions do not have any protection features, and IT managers therefore classify them as a security risk. (In the field of IT, even read-only access is viewed as a security breach, as it allows hostile users to obtain useful information about the network infrastructure).

For IPv6, there is:
- an IPv6 protocol support for transport as well as (and independent of)
- MIBs (Management Information Bases) for IPv6 configuration and host statistics.

4.2.9 Application protocols

A large number of applications can be implemented with the TCP and UDP services. The port numbers used for this purpose are assigned to one of three categories by the IANA (www.iana.org):

- **Well Known Ports (0…1023)**
  These port numbers are reserved for specific applications and must not be used by other applications. Examples: FTP (21), HTTP (80), SNMP (161)

- **Registered ports (1024…49151)**
  These port numbers are reserved for specific applications and must not be used by other applications. Example: BACnet (47808)

- **Dynamic/Private Ports (49152…65535)**
  These port numbers are not predefined and can be used as required.

A port in use on a host is referred to as an "open" port. Open ports are a security risk, as they allow attackers unauthorized network access. For this reason, routers and firewalls are configured to accept only packets or datagrams for configured and enabled ports and all others, block disabled ports (the "white-list" approach).

---

3 There are three sub-versions of SNMP V2; When spoken of "V2", the common "Community-Based" version V2c is usually meant.
4.3 Remote access and Virtual Private Networks (VPN)

The spread of the Internet throughout the world has resulted in changes in the field of remote access. Formerly, telephony was used for dialing into a corporate network, which meant that the company had to keep a pool of modems. Even branch networks were connected by leased line to the head office.

**Tunneling**

_Virtual Private Networks (VPN)_ make use of the Internet to connect geographically dispersed networks. Since the Internet is basically an open and unprotected network, there is a risk that messages can be intercepted or even manipulated. VPN is a means of creating a secure communications channel via the Intranet. The data packets of any protocol are encrypted and compressed. The data is transmitted across the Internet through a kind of virtual tunnel; hence the term _tunneling_.

**VPN categories**

There are various different categories of VPN:

- **Intranet VPN**[^4]: Two networks with _equal access rights_ are connected via a VPN tunnel. There are several hosts connected to each end of the link. The branch computers are connected via VPN to the intranet, similar to being at the site.
- **Extranet VPN**: A remote network with reduced access rights is connected to the primary network for limited access to data and services.
- **Remote Access VPN**[^5]: A single host has a secure data connection to the primary network.

![VPN Tunnels](image)

_Figure 25: VPN tunnels_

**Secure data exchange**

The criteria for the secure exchange of data are as follows:

- **Authentication**: Authentication involves checking the identity of the communications partner. The partner must identify itself, for example, with a password or key.
- **Authorization**: Authorization involves using an access list to check whether the communications partner is allowed access to the network, server(s) and data.
- **Encryption**: The communication must not be intercepted by third parties; this is why the entire data exchange is encrypted.
- **Integrity**: It must not be possible for third-parties to manipulate the communicated data. Alternatively, any such modification must be identified, and the packet must be discarded. The packets therefore include a checksum (seal).

[^4]: Also: "Site-to-site" VPN
[^5]: Also: "Site-to-end" VPN
Tunneling protocol

A VPN system comprises an Internet connection, a secure tunneling protocol, a VPN server and a VPN client on the remote network. With interconnected networks, the VPN client is normally integrated into a router. This creates a VPN tunnel between two routers. If there is only one remote host, the VPN client is downloaded to the host as a software component, thereby establishing a VPN tunnel between a PC and the VPN server.

The main tunneling protocols are PPTP and IPSec:

- **Point-to-Point Tunneling Protocol (PPTP)**
  This protocol was developed by Microsoft and other leading network companies. PPTP is provided as part of Windows 7, 8 and 10 and thus available at no additional expense.
  Note: PPTP is classified as not secure by specialists and should therefore be avoided. L2PT/IPsec has the same advantages and is much more secure.

- **Internet Protocol Security (IPSec)**
  This more recent technology is expected to replace PPTP as the VPN standard in the long term, as it can guarantee a higher degree of security than PPTP. Additional software needs to be installed on the VPN client. IPSec has two modes of operation: The transport layer is used between the client and the server, and only encrypts the data components of the IP packet. Tunnel mode between two gateways (router or server) encrypts the complete IP packet and adds a new IP header.

- **OpenVPN**
  OpenVPN is an open source technology. One of its major strengths is that works with SSL/TLS technologies. This makes its traffic impossible to distinguish from traffic using standard HTTP over SSL (https) and therefore causes little effort with IT firewalls. Despite needing third party software, it is becoming the most prominent cross-platform available VPN solution.

The port numbers used by the VPN tunnel must be opened in the firewalls of the system.

Point-to-Point Protocol (PPP / PPPoE)

Any telephone or xDSL connections between a remote client and an Internet Service Provider (ISP) are implemented by use of the Point-to-Point Protocol (PPP) or Point-to-Point Protocol over Ethernet (PPPoE). PPP / PPPoE comprises several protocols for establishing a connection, checking the connection, authentication and optional encryption. The subsequent path in the Internet is not protected by PPP. For this reason, either a VPN tunnel is connected to a network, or the communication is encrypted for each application/session (e.g. online banking). Secure Sockets Layer/Transport Layer Security (SSL/TLS) has become the established protocol for application-based encryption.
5 IT security
5.1 BACnet and IT security

Increased networking of building technology with IT systems as well as the extension of the BACnet standard toward IT standard, increases the risk of attacks from the outside against building-technical plants.

Security measures have been designed in the BACnet standard in Section 24 "Network Security" to counter the trend. It is, however, becoming increasingly irrelevant on the market since building technology has become closely networked with classical IT. BACnet systems will be increasingly viewed as part of the customer’s IT and integrated in the superposed corporate IT security accordingly.

Early consultation on security issues with IT managers at the customer ensure comprehensive and sustainable IT security on the project.

Note the following points, among others:

- Access to the plant: this includes, in particular, logical access to the plant via web server or other software access. The network of the building plant should be separated from the customer’s own IT network. Either physically through separate cabling or logically using VLANs or remote access through VPNs. Network ports not needed for communications, should be blocked after consultation with IT managers. Ports, that are explicitly needed should be enabled based on a "Whitelist".
- Avoid and disable outdated and non-secured protocols such as http, ftp, telnet etc. wherever possible.
- Customer plants can never be connected to the Internet unsecured. If, for example, a web server access point is made accessible in the customer DMZ, it must be secured through VPN tunneling (end-to-end)
- Password policy: Length and strength of plant passwords used, changing default passwords and user accounts.

Comply with the most important items for creating and using strong and secure passwords:

- Immediately change the preset Siemens default password to a strong password the first time you log onto the system.
- Use a different password for each project.
- Use different passwords for different users.
- Use only strong passwords consisting of a combination of:
  - Capital letters
  - Lowercase letters
  - Numbers and
  - Special characters
- Use at least 8 characters for a user account and at least 12 characters for privileged accounts.
- Check passwords at regular intervals, for example, every 45 days.
- Store the password at a secure location, protected against unauthorized access.
  Never save a password at an unsecured location, for example, on your monitor or keyboard.

As a rule, IT managers at the customer define or demand this type of security specifications.

The document "IT security in installations with Desigo (CM110663)" [7] offers additional help on the topic.
6 BACnet over IP

6.1 BACnet Virtual Link Layer BVLL (Annex J)

Annex J of the BACnet standard defines how BACnet NPDUs (Network Layer Protocol Units) are transmitted over IP networks. The UDP/IP combination does not satisfy all the requirements of a BACnet system, and for this reason, an additional protocol layer was defined. This is referred to as the BACnet Virtual Link Layer (BVLL) and it is an essential requirement on every BACnet/IP node.

6.1.1 BACnet/IP networks and addressing

A BACnet/IP network consists of one or more IP subnets assigned to the same BACnet network number. The limits of different transmission media in a system typically define the limits between different BACnet networks. A BACnet internetwork consists of two or more BACnet networks. These networks may either be BACnet/IP networks, or they may be implemented with other BACnet data link protocols (e.g. BACnet/LonTalk).

For BACnet/IP, the BACnet MAC address is 6 bytes long and consists of an IP address (4 bytes) and a UDP port number (2 bytes). The standard UDP port for BACnet communications is 0xBAC0 (in hexadecimal notation) or 47808 (in decimal notation). If two independent groups of BACnet devices are required to exist on one IP subnet, a different UDP port may be used for the second group. The range from 0xBAC1 to 0xBACF is not reserved, and should therefore be used with the appropriate Important.

![Figure 26: Various UDP ports with BACnet/IP define various BACnet internetworks](image)

The various UDP ports of the BACnet devices can be thought of logically as different "wires". Only BACnet devices "connected to the same wire" can communicate with each other.

![Figure 27: Several BACnet internetworks "on a single wire"](image)
By using different UDP ports, it is possible to create several independent BACnet internetworks based on the same IT infrastructure. A management station Desigo CC can communicate with several BACnet internetworks at the same time resulting in no system restrictions for operation.

The use of several BACnet internetworks can be helpful in very large projects, for migration, and to encapsulate sections of plant with different reliability criteria (e.g. pharmaceutical industry).

### 6.1.2 BACnet Broadcast Management Devices (BBMDs)

The BACnet standard requires the Data Link Layer to receive broadcast datagrams from all BACnet devices in the BACnet network.

In BACnet/IP networks consisting of only one IP subnet, this requirement is fulfilled without any additional work. The broadcast messages are transmitted as IP broadcasts (e.g. 172.16.255.255:0xBAC0).

If a BACnet/IP network is composed of several IP subnets, additional mechanisms are required to distribute the broadcasts. This is because IP broadcasts can only be transmitted to one IP subnet. For this purpose, BACnet defines the BACnet Broadcast Management Device (BBMD). This is not really a separate product but, rather, an additional function of the BACnet devices.

BBMDs forward received broadcasts via unicast to all other BBMDs in the BACnet network, and these, in turn, transfer the broadcast to the local subnet. The table of all the BBMDs in a BACnet network is known as the Broadcast Distribution Table (BDT). It consists of an entry for each IP subnet, comprising the IP address and UDP port of the BBMD, and a "Broadcast Distribution Mask". If the mask is 255.255.255.255, then the broadcast is transmitted to the relevant BBMD as a "unicast" message. The BBMD then places it on the local subnet. The procedure is referred to as "two-hop distribution" and is the "normal" case. If the IP routers are configured to forward broadcasts to remote subnets, the "one-hop distribution" method can be used. The BBMDs then send the broadcasts directly to the different IP subnets. In this process the subnet address is calculated on the basis of the Broadcast Distribution Mask. Message distribution to recipients within the target IP subnets is carried out by the IP router.
### Rules

- In a BACnet/IP network consisting of more than one IP subnet, one BBMD must be defined in each subnet.
- In a BACnet/IP network consisting of one IP subnet only, no BBMD is required. However, if a BBMD exists, this does not cause any problems.
- BBMDs are grouped by BACnet/IP network. BBMDs in different BACnet internetworks may not communicate with each other!
- Normally, the "two-hop distribution" method is used, as this works with all IP routers without the need for any further configuration.

A clear distinction must be made between the BBMD functions and those of the BACnet router.

- A BACnet router connects BACnet networks. All communication between the networks takes place exclusively via router.
- The BBMDs work within a BACnet/IP network, where they ensure the distribution of broadcast messages. The BBMDs are not relevant for the transmission of unicast messages.

#### 6.1.3 Foreign device

The way in which the BBMDs operate presupposes that all IP segments of the BACnet network are available at all times. All IP segments concerned carry the full BACnet broadcast load, even if there is only one BACnet device on an IP segment.

The **Foreign Device** is defined in BACnet to deal with this situation. As with the BBMD, this is not an actual product, but an additional function of an existing BACnet BBMD-device.

![Figure 30 Foreign device](image)
**Principle of operation**

1. The foreign device registers itself with (exactly) one BBMD for the receipt of broadcasts. The registration is accepted without any login mechanism, and must be renewed at regular intervals.

2. The BBMD enters the foreign device in the *Foreign Device table (FDT)*. The maximum size of the FDT depends on the BBMD in use, and must be determined by reference to the data sheet (PICS).

3. When it receives a broadcast, the local BBMD forwards it to all BBMDs in the BDT and to all foreign devices in the FDT.

4. Instead of transmitting broadcasts directly to the local subnet, the foreign device forwards the messages to the BBMD for distribution. Unicast messages, by contrast, are always delivered directly.

5. The foreign device de-registers from the BBMD and is removed from the FDT. If the foreign device fails to deregister, the entry is automatically deleted by the BBMD after a timeout, because the registration has not been renewed.

Registration with the BBMD involves the entry of an IP address and UDP port. A foreign device can therefore use any port number.

The registration process makes the foreign device a temporary member of the BACnet network. It is therefore required to comply with all the rules of the associated internetwork. In particular, the Device ID and Device Name of the foreign device must be unique within the internetwork.

---

**6.2 Restrictions of BACnet/IP**

In principle, the BACnet Virtual Link Layer (BVLL) allows the use of UDP/IP as the transmission protocol. However, since BACnet does not specify a login mechanism for foreign devices, this means that any BACnet device can obtain access the internetwork. In such cases, either special configurations must be used or combinations involving these components must not be used.

---

**6.2.1 IP version 6**

The BACnet standard also supports IP version 6 in the meantime.

This addendum primarily maps the functionality of BACnet IPv4 to IPv6 transport. To this end, a new BVLLv6 layer was defined.

- Rather than IPv4 broadcasts, IPv6 multicasts are used for BACnet broadcast telegrams.
- For reasons of compatibility, a virtual 3-byte address (VMAC) is used as BACnet address. This address is resolved into a correct IPv6 address in the BVLLv6 layer and saved temporarily in a table similar to ARP.
- All known BACnet IP features are found in similar form. For example, BBMD and foreign devices. They are required if communication is past an IPv6 multicast scope.
- In a BBMD, only two-hop distribution is allowed. A broadcast distribution mask no longer is required.
- In future, probably DNS names can be entered as BBMD addresses.

---

6 This statement only really applies to the "two-hop" distribution of the BBMD. Desigo (and nearly all other commercially available) BBMDs exclusively use this mode.
DNS names and IPv6 foreign devices are not supported at this time.

6.2.2 DHCP and DNS

The dynamic allocation of addresses with DHCP can have undesirable effects on the system:

- DHCP must never be used with BBMDs, as the IP addresses in the BDT are configured as static addresses, and must therefore not change during operation.
- As per the BACnet standard, alarm recipients can either be entered with the device object identifier, or BACnet address. The IP address is part of the BACnet address and must therefore not be changed for the alarm recipient. For this reason, dynamic IP addresses always must use the option involving the device object identifier.
- In the case of Change-of-Value reporting (SubscribeCOV, SubscribeCOVProperty) the subscription is always based on the BACnet address. Since the subscription is normally repeated at regular intervals and is monitored with a "Time-to-Live" parameter, the system is able to recover after any change of address.
- If access rights are assigned (e.g. for a firewall) on the basis of the IP address, this must be a static address.

In addition to the operational effects, dynamic address allocation also makes system fault diagnostics difficult.

We recommend to not use DHCP, especially not together with automation stations.

Network members are identified numerically (IP address) or by plain text names. In TCP/IP networks, the Domain Name System (DNS) is used. BACnet, by contrast, defines a mechanism that is independent of DNS (Who-Has, I-Have). In an automation station with BACnet and Web functions, DNS is therefore used exclusively for addressing the Web server.
6.2.3 Firewalls

BACnet communications are connectionless, and can take place between any devices. Even with operation as a foreign device, only the registration and exchange of broadcasts is required between the foreign device and the BBMD. Unicast messages are exchanged directly between devices.

In order to allow communication in such cases, the UDP port number in the firewall must be fully open. This produces a major breach in the security strategy and its suitability is therefore severely limited.

![Firewall Diagram](image)

The risk can be lessened by use of BACnet/IP to BACnet/IP router. All BACnet communications must then proceed via router. The access control defined in the firewall can now be limited so that it allows packets only to and from the router. However, since BACnet does not specify a login mechanism for foreign devices, this means that any BACnet device can obtain access the internetwork.

![Using a BACnet router with a firewall](image)

Note: The automation station variant shown in the example with integrated BACnet/IP to BACnet/IP router is not yet available in the Desigo system.

6.2.4 NAT

*Network Address Translation (NAT)* is used to map IP addresses from the private domain to official "Internet" addresses. Only address information in the IP protocol header is modified as described in Section 3.5.5.

With BACnet/IP, IP addresses are transferred as the UDP payload. These addresses are not modified by NAT. As a result, invalid address information reaches the Internet. Thus, communication between BACnet devices via NAT is not possible.

The BACnet standard in Annex J.7.8 describes the correct response of the BBMD in connection with NAT.
6.2.5 Prospects and workarounds

There is intensive discussion within the BACnet working groups about the requirements of BACnet/IP and the possible solutions. Topical themes:

- Impact of DHCP
- BACnet security (encryption and authentication)
- BACnet communication across firewalls and NAT routers

Projects to establish “BACnet Network Security” (previously: Addendum g) are not accepted today. The reason is the high effort that would be required from IT security.

For this reason, the ASHRAE BACnet working groups aim at basing IT security on existing IT standards and infrastructure.

Virtual Private Networks (VPN) are one way of getting round the firewall problem. The remote foreign device becomes a direct member of the internal network. The VPN “tunnels through” obstacles such as firewalls and NAT routers. Since authentication is required from the VPN client when creating the VPN tunnel, there is also some protection against unauthorized access to the BACnet internetwork.

Figure 33: Use of VPN in the context of NAT and firewall problems

6.3 The BACnet/IP network load

If it is planned to operate a BACnet internetwork via the existing IT infrastructure, the IT manager often raises the question of the required network capacity. If a separate network is used for the building automation and control system, this question is of secondary importance, because any network overload would not affect other applications (mail system, ERP system, Intranet etc.).

BACnet internetworks increasingly apply VLANS (virtual LANs), using the same physical transmission medium. In this case, common bandwidth must be distributed accordingly.

It is not possible to give a blanket statement on the incidence of BACnet/IP communications, especially in the case of Desigo. The communications load always depends on the specific design of the building automation and control system.

With new systems, e.g. Desigo CC and integration of camera surveillance (security), data transmission rates increase significantly. One full HD stream requires up to 20 Mbps, one 4K UHD stream up to 40 Mbps. Although BACnet data traffic, communications still takes place on the same network and is thus important for bandwidth calculations.
The following points must be observed:

- Automation stations are normally passive, i.e. they initiate very little data traffic. The data traffic is primarily caused by BACnet references to other automation stations and alarm and event messages.
- Management stations (Desigo CC) and operator units (PXM20) are responsible for most of the communications load. Especially when starting the BACnet client, a substantial amount of information has to be read from the BACnet internetwork, (including e.g. current alarms). During operation, the largest number of BACnet services is required when changing between operator views. This is the case above all with Desigo CC where one view may contain many data points: Numerous services are involved when refreshing or closing down views.
- From the system functions perspective, trend logging causes significant data traffic, as it involves the transfer of large volumes of data from the automation level to the management station.
- BACnet broadcasts can lead to bursts of communication, because in such cases a single service (e.g. WhoIs request) produces a response (e.g. IAm request) from many or all BACnet devices in the BACnet internetwork. If the network is overloaded, it is above all these broadcast-based functions (e.g. network scan with PXM20 unit) which cease to operate satisfactorily.

In summary, then, it can be said that the basic load on the BACnet internetwork is small, and that (short-term) communications loads are caused primarily by user actions. The communications strategy in the Desigo system (COV reporting instead of polling, phased transmission of IAm requests etc.) ensures efficient use of the communications media at all times.

From the Desigo perspective, there are no special demands on the IT infrastructure hardware. The commonly-used 100 Mbps Ethernet networks provide adequate capacity. Gigabit Ethernet recommended for redundant servers. Larger networks, moreover, have larger backbones (Gigabit-Ethernet or higher), so that bottlenecks can be avoided.

With BACnet internetworks extending over large areas, however, (e.g. within a town), a closer analysis of the IT infrastructure is required. In such cases, there is a high risk of intermittent downtime, increased delay times and hence a complete breakdown in the system performance. Note the system limits described in the section on system configurations in the technical principles [3].

Recommendations

We suggest to separate the technical IP network from the customer's network in large networks. There are two ways to do this:

- VLAN:
  A VLAN protects the Desigo IP network against disturbances from the customer network such as high-volume data traffic, port scans, defective devices, or misconfigured networks. The solution has the advantage that existing physical data networks can be used and no additional data lines must be installed. Nevertheless, verify that existing routers and switches can be used for a VLAN (or must be replaced accordingly).

- Separate network:
  For a separate network, separate Ethernet data lines must be installed for the Desigo system. This is the preferred solution when customers require total separation of their network from the Desigo network, or when customers are not willing to integrate VLAN-capable routers and switches.
Future extensions to the BACnet standard will increasingly use standard mechanisms from the IT universe (e.g. http(s) as transmission protocol).

- We can therefore anticipate new networks for building technology at higher data volumes. As a consequence, high reserves should be planned with regard to transmission capacities.
7 Principles of MS/TP

"MS/TP" stands for "Master-Slave/Token-Passing" and represents a data link protocol, which provides its services based upon EIA-485 as a physical layer. By this, it allows an easy wiring on site with 3-wires (possible also with 2-wires, but not recommended). MS/TP is described in detail in an own chapter (=clause 9) of the BACnet standard, so the following chapters will concentrate on the practically relevant parts instead.

7.1 MS/TP Basics

As BACnet/MSTP is physically based upon EIA-485, its relevant limits apply:
- max. total cabling of ~1200 m
- max. 32 "electrical full load" devices per MS/TP segment (more devices would thus require repeaters)
- max. 128 devices at all per MS/TP bus
- max. 115 kBaud transmission rate (typical other values 19.2 / 38.4 / 76.8 kBaud); note that all MS/TP devices connected to the same EIA-485 bus must use a common speed value

Note that these are maximum values; in reality, some interdependencies must be taken into account:
- max. transmission speed is a function of cable length: cabling longer than ~750 m might require to reduce speed to 76.8 kBaud
- MS/TP devices are typically ¼, ½, ¾ or "full load"; so 32 devices "full load" would translate into 64 MS/TP "half load" devices, etc. before a EIA-485 repeater would be required

Still, practical limitations might result from a bandwidth- (instead of an electrical load-) aspect (to be discussed later on).

7.2 MS/TP Master/Slave devices

As its name indicates, MS/TP’s logical working principle is based upon "token passing", that is: There is a "token" in the system which is passed from each device to the next on the EIA-485 bus. A device must wait for its communication until it receives that token.

MS/TP distinguishes between two types of devices:
- "master" devices
- "slave" devices

A BACnet slave can be read/written but never gets the token. The disadvantage of such "slave" devices therefore is, that they cannot initiate any messages on their own (but require a "MS/TP slave proxy" instead to help them to communicate). On the other hand, the advantage is that the more slaves are present on a EIA-485-bus, the fewer token passes, speeding up the overall communication.

However, as the disadvantage overweighs, most MS/TP-devices are realized as master devices.

As a slave device cannot announce itself to the network, adding new slave devices require to program at least one (1) master on the network to be used as "slave proxy" for that slave.
Adding a master device is different, however: Every master on the network periodically issues a "poll for master"; that is, it checks for its successor. This works in that each master queries between its own address and the next known master's address. For example, if the current master device's own address is 12 and the next known master address up to now is 22, then it will query addresses 13..21 every now and then to see if a new master device with an address in that range joined the network.

"Every now an then" translates into each N_poll times that the device receives the token (default = 50). Note that this gives rise to both:

- Avoid gaps in the address numbering scheme
- Avoid small values for N_poll unless the MS/TP network is frequently changing for whatever reason
- Avoid a "wrap-around" addressing gap from the largest used device address over 127 back to 0 by setting MAX_MASTER to the highest used master device address

Setting MAX_MASTER correctly is important, as it allows saving some bandwidth. But as no device with an MS/TP address larger than MAX_MASTER will be discovered, it also limits the discovery of new devices: A careful engineering is required thus.

### 7.3 MS/TP performance considerations

As described in 7.1, BACnet/MSTP has a far smaller bandwidth available than does BACnet/IP. Typically, a MS/TP network is operating with 76.8 kbaud whereas IP networks run at 100..1000 mbps.

So although MS/TP cannot act as a general purpose BACnet-backbone, MS/TP devices are a good choice for a range of applications where it can play off its strengths:

- Wiring is simple and cost-efficient, based upon proven EIA-485 technology
- MS/TP supports cabling lengths of up to 1200m without any additional network elements, thus supporting highly distributed controls
- BACnet/MSTP is an officially supported member of the BACnet standard, allowing a seamless BACnet system on all levels
- BACnet/MSTP devices are a cost efficient means for use-cases that do not require fast update rates (like VAV and heat pump controllers for instance) where BACnet/IP devices either do not exist at all or would be less cost-efficient

To play out its full strengths, it is important that MS/TP-networks are applied and installed appropriately. The following subsections describe aspects that should be taken into consideration to achieve an optimal system performance.

Still, the overall system performance of a MS/TP-network is a complex matter, determined by too much of a parameter to allow a fixed maximum number of devices to be stated as a general limit.

---

7 Note that as all MS/TP-devices must operate with the same baud rate, the slowest MS/TP-device will set the overall limit. Thus, for a good performance, make sure that you don't have single MS/TP-devices with slow down the system.
7.3.1 MS/TP bandwidth issues

As mentioned before, properly dimensioning the size of a MS/TP-network cannot be derived from bandwidth aspects alone; nonetheless, bandwidth considerations are a valuable help.

Due to its basic working principles, BACnet/MSTP has a different ratio on usable bandwidth, depending upon device types used:

- In a purely BACnet/MSTP Master device system, the bandwidth corresponds to just ca. 60% of the bandwidth of the effective load
- In a purely BACnet/MSTP Slave device system, with just one BACnet/MSTP master, corresponds to ca. 75% of the bandwidth of the effective load

These are the two extremes; the real use-case is typically something in between. Provided of course that the MS/TP parameters are set in an optimum manner, since otherwise dramatic drops in performance may occur due to incorrectly set timing values in the address range.

MS/TP knows of 8 different frame types of varying length (cf. chapter 9.5 of the BACnet standard), but typically, querying a BACnet property consists of ~30 bytes payload for the poll plus ~40 bytes payload for the answer.

At today’s typical data transmission rates of 76,800 baud, the best case on a network with the maximum of 32 BACnet/MSTP devices, i.e. optimally set timing parameters, is approximately 100...120 such short telegrams per second. Conversely, a maximum effective data transmission of 4.6 kByte/s can be expected for larger data transfers on longer telegrams.

Again, these are rough estimates, but should help as a rule of thumb.

Note that the usable bandwidth of BACnet/MSTP is some order of magnitudes lower than the one of a typical BACnet/IP network. BACnet-routers are transparently routing traffic back and forth between both types of networks without buffering. Still, both network sides belong to the same BACnet Internetwork (that is, to the same BACnet intercommunication domain). This requires careful planning not to overburden the slower MS/TP-subnet, e.g. not to use a MS/TP network segment as a backbone for BACnet/IP to BACnet/IP communication.

7.3.2 MS/TP timing issues

As discussed before, the BACnet Master-Slave/Token-Passing (MS/TP) protocol uses a token-passing scheme to control access to the EIA-485 bus network. A Master device that holds the token can initiate the transmission of a data frame. All other master and slave devices on the bus can respond to requests from this master by transmitting data in frames.

After a maximum number of data frames (N max_info_frames) sent (and awaiting any expected replies), a master node passes the token to the next master node.

The master device normally holds the token for just a few milliseconds. Of course processing or forwarding of the token can take up to 250 ms in a number of cases. Multiplied over the number of devices on a BACnet/MSTP network, this can quickly
result in cycles of multiple seconds, so that you must select very conservative time-out values.

In addition, MS/TP also uses a discovery mechanism, which ensures to adapt to find new devices on the EIA-485 bus (see next chapter), but this may further add upon overall latency-times.

This indicates that MS/TP:
- is a good choice for communicating with controls that do not require fast update rates,
- but should not be used for use-cases with near real-time requirements.

When MS/TP devices are involved in the communication the following timeouts must be configured:
- APDU timeout 6000 ms
- APDU segment timeout 5000 ms

This applies to MS/TP devices and IP based devices, especially Desigo management stations communicating with MS/TP devices.

For the router and large MS/TP networks Max-Info-Frames must be set to 50.

**Additional information**
- Desigo TRA Engineering, mounting and installation CM111043
- Section 10 MS/TP network [9]
- Customer Support Comfort: Knowledgebase article KB2556

### 7.3.3 MS/TP important addressing issues

**Important!** MS/TP uses a one-byte addressing scheme:
- Addresses 0 to 127 are valid for both master and slave nodes
- Addresses 128 to 254 are valid only for slave nodes
- Address 255 is reserved to denote the broadcast address

Note that the token passing principle is that each master device is handing on its token to the numerically next master device which it finds.

Therefore, two important things should be taken into consideration to avoid waste of reaction time in the network:
- Avoid gaps in the address numbering of the MS/TP master devices
- Set the MAX_MASTER parameter to be the highest used master address on the network

As 127 is the highest allowed master device address, it is also the default setting. However, as the device with the actual highest address will periodically "poll-for-master" till the MAX_MASTER limit, any gap in the numbering scheme will waste time.

Note also that address 0 is special in the sense that in the case of a network reset, the respective device with address 0 will be the first one to start the "poll for master" query. Therefore, a BACnet/IP to MS/TP router should be assigned the address 0 to achieve best performance.
7.3.4 MS/TP general performance issues

As described in 7.2 before, both a properly engineered addressing scheme and choosing the right master/slave devices are important to achieve a good system performance:

- Use sequential MS/TP device addresses for all your MS/TP master devices (=don't use gaps in addressing numbers)
- Start from zero, with the BACnet-router address = 0

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>discoverable devices &amp; -objects without any additional &quot;slave proxy&quot; functionality</td>
<td>token passing costs time</td>
</tr>
<tr>
<td>can initiate communication</td>
<td></td>
</tr>
<tr>
<td>- required for supervisory functions</td>
<td></td>
</tr>
<tr>
<td>- required for COV</td>
<td></td>
</tr>
</tbody>
</table>

Pros and cons of MS/TP master devices:

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>generally faster network communication with large number of non-COV capable devices</td>
<td>not discoverable, need a slave-proxy-capable BACnet-device in the MS/TP-network</td>
</tr>
<tr>
<td>larger address space</td>
<td>cannot initiate communication / COV / Alarming (=slave-proxy must poll regularly)</td>
</tr>
<tr>
<td></td>
<td>Polling scales very poorly and therefore is only usable on very small plants</td>
</tr>
<tr>
<td></td>
<td>No notification when devices restart</td>
</tr>
<tr>
<td></td>
<td>No BACnet segmenting</td>
</tr>
<tr>
<td></td>
<td>In summary: Overall, this massively restricts the practical benefits of MS/TP Slave devices!</td>
</tr>
</tbody>
</table>

So as a general rule of thumb...

- use COVs whenever the device allows to (but note that COV cannot be supported from slave devices)
- Avoid the use of MS/TP slave devices as much as possible

Note that future support of "MS/TP extended frames" (as of BACnet Addendum 135-2010an) will be another point to take into consideration:

- Support of large MS/TP frames requires end-to-end support of large frames between all participants along the communication path
- The usable data portion does increase, but only provides benefits where larger data volumes are actually transmitted (in other words, not typically the case for short commands)
- Conversely, the token circulation time (and with it system response times) increase and parameters such as Parameter wie Max_Info_Frames must be reduced to compensate
- We therefore recommend against using such extended MS/TP frames.
  If an MS/TP end-device supports large frames but does not support (de-) segmentation, end-to-end communication will not work at all, if on the way to the other end participant, a communications node in between cannot process the extended frames and no interim station can help using segmentation.
#### 7.4 MS/TP parameters

The BACnet standard defines a number of parameters (in chapter 9.5.3), which together describe the timely behavior of the MS/TP network:

- $N_{\text{max\_info\_frames}}$: Specifies the maximum number of information frames the master node may send before it must pass the token. $\text{Max\_Info\_Frames}$ may have different values on different nodes. This may be used to allocate more or less of the available link bandwidth to particular nodes. If $\text{Max\_Info\_Frames}$ is not writable in a node, its value shall be 1.

- $N_{\text{max\_master}}$: Specifies the highest allowable address for master nodes. The value of $\text{Max\_Master}$ shall be less than or equal to 127. If $\text{Max\_Master}$ is not writable in a node, its value shall be 127.
  
  **Note:** For optimum performance, set this value to the highest master device's address actually used in your MS/TP network.

- $N_{\text{poll}}$: The number of tokens received or used before a "Poll For Master" cycle is executed: Default by the BACnet standard is 50.

- $N_{\text{retry\_token}}$: The number of retries on sending Token: Default = 1.

- $N_{\text{min\_octets}}$: The minimum number of "DataAvailable" or "ReceiveError" events that must be seen by a receiving node in order to declare the line "active": Default = 4.

- $T_{\text{frame\_abort}}$: The minimum time without a "DataAvailable" or "ReceiveError" event within a frame before a receiving node may discard the frame: 60 bit times. (Implementations may use larger values for this timeout, not to exceed 100 milliseconds.)

- $T_{\text{frame\_gap}}$: The maximum idle time a sending node may allow to elapse between octets of a frame the node is transmitting: Default = 20 bit times.

- $T_{\text{no\_token}}$: The time without a "DataAvailable" or "ReceiveError" event before declaration of loss of token: Default = 500 milliseconds.

- $T_{\text{postdrive}}$: The maximum time after the end of the stop bit of the final octet of a transmitted frame before a node must disable its EIA-485 driver: Default = 15 bit times.

- $T_{\text{reply\_delay}}$: The maximum time a node may wait after reception of a frame that expects a reply before sending the first octet of a reply or Reply Postponed frame: Default = 250 milliseconds.

- $T_{\text{reply\_timeout}}$: The minimum time without a "DataAvailable" or "ReceiveError" event that a node must wait for a station to begin replying to a confirmed request: Default = 255 milliseconds. (Implementations may use larger values for this timeout, not to exceed 300 milliseconds.)

- $T_{\text{roff}}$: Repeater turnoff delay. The duration of a continuous logical one state at the active input port of an MS/TP repeater after which the repeater will enter the IDLE state: 29 bit times $< T_{\text{roff}} < 40$ bit times.

- $T_{\text{slot}}$: The width of the time slot within which a node may generate a token: Default = 10 milliseconds.
The minimum time after the end of the stop bit of the final octet of a received frame before a node may enable its EIA-485 driver: Default = 40 bit times.

The maximum time a node may wait after reception of the token or a "Poll For Master" frame before sending the first octet of a frame: Default = 15 milliseconds.

The minimum time without a "DataAvailable" or "ReceiveError" event that a node must wait for a remote node to begin using a token or replying to a Poll For Master frame: Default = 20 milliseconds. (Implementations may use larger values for this timeout, not to exceed 100 milliseconds.)

Boolean value, determining how to handle MS/TP-slave devices. If slave devices are to be used in the network, this value must be set to TRUE: As a slave is not able to respond to broadcast messages like "Who Is", a MS/TP-network requires a so-called "Slave Proxy"-device. If enabled, that (master) device (typically a BACnet-router) will act as a proxy on behalf of the slave devices(s) and respond to such messages.

7.5 MS/TP cabling and topology

Although the MS/TP-bus is logically a ring (due to its token passing principles), it is physically a line topology, that is: no T-connections, rings or other wiring schemes other than a simple multi-drop are allowed.

For cabling, Section 9.2.1 of the BACnet standard provides some minimum requirements, but they have not proven themselves in the real world. As a consequence, comply with TRA cable specifications when using Desigo devices for BACnet/MSTP.

See document "Desigo TRA Engineering, mounting and installation" CM111043, section 10 "MS/TP network" [9]
8 Dealing with problems

BACnet on IP involves the use of a large number of components, and this results in a high degree of complexity and a corresponding vulnerability to errors. If a problem arises in the system, it must be located in a step-by-step procedure. Analysis always starts with the "lowest" system. Once correct functioning is confirmed at this level, the system at the next level is checked.

A sketch of the topology is extremely helpful when attempting to locate problems. This should always be created first, if not already available.

8.1 Ethernet

Check: Is the link signal present?

With switches, the link signal is indicated by a continuous or flashing LED. In all devices in the Desigo system, the Service LED is continuously ON if no link signal is detected.

→ Is the extension module (PXC modular) plugged in firmly?
→ Are all connectors firmly in their sockets?
→ Is there a supply voltage for the switches?
→ Were the RX and TX connections mixed up on fiber optics?
→ Is the uplink port of the hub/router set correctly?

Check: Is communication on the PC slow?

→ Is the built-in Ethernet adapter set to auto detect (Speed and Duplex) or are manual settings active?
  Click > Start > Settings> Control Panel> Administrative Tools> Computer Management, click Device Manager in the tree view in the left pane, open Network adapters in the right pane, right-click the Ethernet adapter, select > Properties and click the Advanced tab.

Check: Are VLAN switches in use?

→ Are all BACnet devices configured on the same VLAN (see Section 3.5.4)?
→ A number of managed switches offer data on their own WEB interface on connected devices. This include, for example, port speed, VLAN association, and packet statistics. The latter can also provide references on insufficient cabling.
Check: Can the destination address of the IP node be accessed with Ping?

Command line (example): `ping 172.16.87.12`

Note: Ping can also be blocked by IT settings!

→ Are the IP address, subnet mask and default gateway settings correct?

Expected response: IP target node responds as shown below:

![Ping command output]

Check: Are communications stable?

The command "Ping –t": is suitable for testing communications over a longer period.

![Ping -t command output]

Check: Are IP routers used?

Command line: `tracert 172.16.87.12`

Note: TraceRt can also be blocked by IT settings!

→ Are the required ports open in the router (see Section 10)?

Expected response:

– All listed IP addresses to the target node are located in the same IP subnet (if no IP router is used).
– At least one IP address is located in an IP subnet different from the own IP address.
The own network ID is determined as described in Section 4.2.2 "IP" via Boolean operand\(^8\) using the network mask. To this end, first determine your own IP address and subnet mask by entering "ipconfig".

The address for the example is 139.16.77.31 and the subnet mask is 255.255.252.0. AND operation then results in your own IP network ID 139.16.76.0.

If the same procedure is applied to other IP addresses, the first station already is in another IP subnet\(^9\) – the network thus uses an IP router.

If TraceRt (or PING) cannot reach the target node, there is a basic issue with the IP level (e.g. firewall settings too restrictive, wrong IP parameter, faulty router settings, etc.). In this case, clarify first the issue with the ID department before proceeding on the BACnet level.

**Check: Are firewalls used (remote or in PC-software form)?**

The existence of a firewall cannot be detected. If in doubt, contact the IT manager.

→ Are the required ports open in the firewall (see Section 10)?

**Check: Are short packets transmitted correctly, and only long packets blocked?**

→ In a router or firewall, are fragmented packets being suppressed ("dropped")?

Command line: `ping -l [packet size] -f [target node]`

The PING command from above is used with special syntax. It indicates the length of the test packet and explicitly prohibits fragmentation: PING indicates a corresponding error if the packet cannot be transmitted due to size. This brings closer the max. supported MTU of overall transmission:

---

\(^8\) This is best carried out via the Windows Calculator and the AND-operation.

\(^9\) The first station uses IP address 139.16.75.252; although this address is similar to your own IP address, AND-operation and the subnet mask 255.255.252.0 shows that the network ID of the station is 139.16.72.0 – and thus does not match the previously calculated own network ID.
In the example, transmission of a test packet of 1472 bytes is successful; 1473 bytes is no longer transmitted. Knowing that the PING attaches 28 bytes to the packet\textsuperscript{10}, the path MTU of the transmission path is then 1500 bytes for the example.

**Check: Does the PC or Notebook have more than one IP port configured?**

**Command line:** `ipconfig [/all]`

→ Are the applications configured for one specific port?

→ Are the network connections in the correct order? You can check this by opening **Network Connections** in the **Control Panel**. Select **Advanced > Advanced Settings...** and click the **Adapters and Bindings** tab.

\textsuperscript{10} 8 byte ICMP header plus 20 byte header from IPv4 transmission layer (or 40 byte header on IPv6 transmission layer).
Check: On a PC or Notebook, are the required ports already in use?

Command line: `netstat -a -o`

→ Which applications or services are running?

→ Are any processes from crashed applications still active?
Check: Are the communications statistics on the PC or Notebook satisfactory?

Command line: `netstat -e -s`

→ What is the frequency of fragmentation, assembly and routing errors?

![Image of netstat output]

For additional tips on practical troubleshooting, see document "Practical Guide on IP Networks in Building Automation and Control CM110668" [6].

### 8.3 MS/TP

Check: Cabling correct?

→ Use 3-wire cabling wherever possible
→ Is the "common reference" wire terminated at (only) one end with a 100 ohms resistor to ground?
→ Are the "+" and "-" wires of the EIA-485 bus properly terminated with a 120 ohms resistor at both physical ends of the wires?
→ Note that some MS/TP devices have built-in terminating resistors; check that these are disabled (unless the respective device is actually the end of the EIA-485 bus)
→ In mixed mode 2-wire- and 3-wire-cabling environments, check that the cable shield is not misused as "common reference" connector to 3-wire type devices
→ Check installation against electrical noise impact:
→ Are all wiring, equipment controllers, and field panels at least 1.5 m away from power sources greater than 100 kVA?
  • Verify motor generator size. Direct on line (DOL) starters for motors greater than 25 hp generally exceed 100 kVA)
  • Switching DC signals (relays) are one of the worst noise source

Check: New device causing problems?

Electrically, EIA-485 devices must support some "idle" state to denote that they are currently not transceiving. Releasing the line would lead to a "floating" signal voltage, so pull up/down resistors are used to hold the device in a defined stage.

If a device floats to a value too high or too low, it might electrically represent a state that is either always transceiving (thus blocking the whole bus) or never transmitting (thus not working at all).

However, the proper pull up/down resistor choice is difficult, depending also upon
the electrical load of the EIA-485 network, the actual cabling resistance, noise impact, etc.
→ Does the network work without that newly introduced device?
→ Or does the device work alone, but no more when it is introduced into the EIA-485 network?
→ Both symptoms indicate a potential wrong use of pull up/down resistors

Check: New device’s settings correct?
→ If MS/TP device is a master device, check that for its address N
   • N ≤ 127
   • If M is the address of the MS/TP-master device with the next smaller used address (that is: M < N and there is no other MS/TP-master device with its address in between), then check that in device’s M settings, its MAX_MASTER ≥ N
→ If MS/TP device is a slave device, check that at least one master device is configured to know it

8.4 BACnet

Check: Are IP routers used?
→ Is NAT activated in the router? BACnet communications via NAT not possible without special NAT aware BACnet routers!
→ Is there a BBMD configured in every IP segment containing BACnet devices, or are the remote devices configured as foreign devices?
→ Are the BDTs of the BBMDs up to date?

Check: BACnet router or BACnet half router (for remote management)?
Both products incorporate full BACnet functionality, which is why it is particularly important to check the configuration.
→ Are the network numbers unique\(^{11}\), and are they configured correctly?
→ If remote management (BACnet/PTP) is applied to internetworks with BACnet/IP devices, the maximum APDU length for the remote PC (Desigo Insight or Desigo Toolset) must be limited to 480 bytes.
→ PXG3.L, PXG3.M, or PXG80-N run automatic network checks, and indicate errors with an illuminated Info-LED. Are the Info-LEDs off?

Check: Are automation stations configured for use of DHCP?
→ DHCP must NOT be used in conjunction with BBMDs!
→ The use of DHCP with automation stations is not recommended.
→ If the IP address of a BACnet device changes during operation, this change is gradually recognized by other system members. Temporary faults (alarming, COV reporting, primary/back-up response etc.) can result.

\(^{11}\) BACnet half-routers also connect different BACnet networks, thus requiring two different BACnet network numbers.
Check: Are the BACnet addresses unique?

The BACnet address information must be unique within each BACnet internetwork.

→ Is the same UDP port number configured for BACnet/IP in all devices?
→ Are the site no. and site name unique?
→ Are the device numbers and device names of the automation stations unique within each site?
→ Are the device numbers and device names of BACnet routers and management stations unique within each internetwork?

8.5 Data communications capture

If the various system component tests and checks fail to provide any insight into the source of the problem, the next step is the capture and analysis of the data communications. The analysis of the captured data, in particular, requires highly specialized protocol and system expertise, and support specialists should be called upon for assistance with this step. Section 0 describes the procedure in detail.
9 Appendix A – Capture of data communications

The capture and analysis of data communications is no light matter. The analysis of the captured data, in particular, requires highly specialized protocol and system expertise, and support specialists should be called upon for assistance with this step.

9.1 A note on data protection

If the building automation and control system is operated via a corporate network rather than a separate network, then local data protection guidelines must be observed. Discuss together with the IT staff who, when, and how long data traffic should be recorded.

9.2 Determination of capture points

The first hurdle with data capture and analysis is to select a suitable capture point within the system. Depending on the symptoms of the problem, the selected point will be close to the automation station or near the management station.

Where switches are used, a given port can receive only broadcasts and packets addressed directly to that node. Which generally does not provide the desired results. Managed switches therefore normally include a monitoring function. This enables them to mirror the traffic at one or more ports on one specific port. This is the port to which the sniffer is connected. The port is variously referred to as a monitor port, mirror port, SPAN (Switch Port Analyzer) port or maintenance port.

A final option is to install the sniffer software directly on the management station.

9.3 Tools for data capture and analysis of BACnet/IP

The data traffic is analyzed in two stages. In the first stage, the network analyzer or "sniffer" captures the Ethernet packets. Sniffers are available as self-contained devices or in the form of software for loading onto the PC. Normally, the software option is perfectly adequate. In the context of the Open Source License initiative, there are several sniffer programs available free of charge over the Internet (e.g. www.wireshark.org). Note the following when configuring the sniffer:

- If the PC/Notebook has several IP ports available, select the required port.
- The data should be captured in "promiscuous mode" in order to record all packets on the Ethernet segment.
- Adjust the data capture buffer according to requirements. When data capture is stopped, check whether all packets were captured or whether some were overwritten or discarded.
- If necessary, define a filter so that only BACnet communications are captured and saved.
• If the communication load is excessive, disable the real-time display of the packets.

Provided that only UDP port number 47808 (0xBAC0) is used for BACnet/IP, WireShark can decode the BACnet messages very simply\textsuperscript{12}. In all other cases, the captured data must be saved in Microsoft Network Monitor 2.x format (*.cap). The SBT BACnet Protocol Analyzer (BPA) can only import this file format. The BPA can be obtained from Field Support.

9.4 Tools for data capture and analysis of BACnet/MSTP & additional resources

The following third party tools are not free, but useful:

• Cimetrics BAS-O-Matic: This tool includes an MS/TP option for network sniffing: http://www.cimetrics.com/index.php/b5020-bacnet-protocol-analyzer.html


• Chipkin Automation Systems: Provides a number of BACnet-related tools (including, but not limited to BACnet/MSTP): http://www.chipkin.com/products/:
  – CAS BACnet Explorer: A utility for testing, debugging and discovering BACnet networks and devices (BACnet IP, BACnet Ethernet 802.3 and BACnet MS/TP)
  – CAS BACnet Watchdog: A utility which monitors and records BACnet packets and messages from certain Devices and Objects and allowing to set "traps" upon certain criteria
  – Other soft- and hardware

Chipkin Automation Systems also maintains a freely downloadable E-Book "BACnet for Field Technicians" at http://www.chipkin.com/files/pdf/Bacnet%20For%20Field%20Technicians.pdf; parts of this document were used by courtesy of Peter Chipkin / Chipkin Automation Systems.

• Wireshark is a free program for analyzing network communication connections (Sniffer). See: https://www.wireshark.org

\textsuperscript{12} If a port other than the above standard port is used for data capture, the port must first be entered via Edit/Preferences/BVLC under "Additional UDP Port" for decoding to work properly.
10 Appendix B – TCP/UDP port numbers used with Desigo

10.1 List of ports for online operation

To maintain reliable online operation of Desigo, the following ports must be opened in IP routers and any firewalls:

- **BACnet on Ethernet**
  - One UDP port per BACnet/IP network (range: 47808..47823, default: 47808).
  - A specific port (range: 47808..47823) or a dynamic port (range: 49152…65535) for BACnet devices working as foreign devices (register with BBMD).

- **Important!**
  - The port must be opened in an IP router (firewall) for all BACnet devices and not solely for the BBMD.
  - Open ports allow the interruption or hijacking of communication. Unauthorized access to customer sites may cause system malfunctions or system failures. This may result in high fixing costs and a loss of reputation.
  - Open only the ports in a firewall (i.e. external switch) that are required for operating the BACS. All other ports must be closed.
  - Only enable SNMP in the router if the function is used.

- **Web functionality**
  - HTTP (Port: 80) for normal web functions
  - HTTPS (Port: 443) for encrypted web functions (SSL)
  - SMTP (Port: 25) for e-mail service
  - FTP (Port: 21) for FTP service

10.2 List of opened ports for each product

Different products have certain ports which, in normal circumstances, only need to be accessible locally (i.e. within the IP subnet). The following lists the ports (TCP or UDP) for each product.

- **PXC3 / DXR2**
  - HTTP (Port: 80) for web server
  - HTTPS (Port: 443) for web server (SSL)
  - Port for diagnostics (Port: 2011)
  - UDP Port for knxnetip (Port: 3671)
  - Ports for commissioning (30000 and 30001) open
  - UDP Ports for BACnet (range: 47808…47823)
  - UDP Port for BACnet Broadcast (Port: 47874)

- **PXC with IP gateway**
  - UDP Port for BACnet (range: 47808..47823)
  - UDP port for commissioning (always 47808)
  - DHCP (Port: 68), if configured
  - HTTP (Port: 80) for web server
  - HTTPS (Port: 443) for web server
  - SMTP (Port: 25) for e-mail service
  - FTP (Port: 21) for FTP file download (graphics, languages etc.)
  - TCP port for firmware download (6301), temporarily open

- **PXM20-E**
  - UDP Port for BACnet (range: 47808..47823)

---

<sup>13</sup> For Desigo Insight, refer to the installation guide for details [5]
• UDP port for commissioning (always 47808)
• DHCP (Port: 68), if configured
• FTP (Port: 21) for FTP file download (graphics, languages etc.)
• TCP port for firmware download (6301), temporarily open

**PXG80-N**
- UDP Port for BACnet (range: 47808..47823)
- SNMP (Port: 161)
- Various ports for subcard configuration (1111, 888, etc.)
- RIP (Port 520) open but NOT active PXG80-WN

**PXG3.L/M**
- UDP Port for BACnet (range: 47808..47823)
- HTTP (Port: 80) for web server
- HTTPS (Port: 443) for web server
- SNMP (Port: 161)
- For commissioning: Port 30000, 30001

**PXG3.W100**
- UDP Port for BACnet (range: 47808..47823)
- HTTP (Port: 80) for web server
- HTTPS (Port: 443) for web server (SSL)
- Ports for commissioning (Ports: 30000, 30001)

**Desigo CC**
See Documentation "Desigo CC, System description Version 2.1 A6V10415500" [8]

**Desigo Xworks Plus**
- UDP port for BACnet (range: 47808..47823) or as foreign device (range: 49152...65535)
- UDP port for commissioning (always 47808)

**ABT (Automation Building Tool)**
- UDP Ports for BACnet (range: 47808...47823)
- UDP Ports for IP multicast (range: 30000...30001)
11 Appendix C – Direct addressing of BACnet references

As of Desigo V6.0 SP, BACnet references can also be defined with a BACnet address. It works both within an IP segment via various BACnet network ports as well as via different media. The benefit of this method is that you no longer need to broadcast for naming resolution and this optimizes network traffic. The referenced devices must have a fixed IP address for this to work.

Syntax:
B=[BACnet Network number (0=own network),
Communication path (IP, LON, ANY)
“Station address”][ObjectType, Object ID][Property ID]

Examples:

<table>
<thead>
<tr>
<th>IP/IP</th>
<th>B=[0,IP,&quot;10.170.173.11:0xBAC0&quot;][0,63]{85}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The own automation station has the IP address 10.170.173.10 and uses BAC0.</td>
</tr>
<tr>
<td></td>
<td>The present value of the analog input 63 from the device subscribes with IP address 10.170.173.11, used to communicate via BAC0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP/IP</th>
<th>B=[0,IP,&quot;10.170.3.11:0xBACF&quot;][0,63]{85}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The own automation station is on network 10.170.173.0 and uses BAC0.</td>
</tr>
<tr>
<td></td>
<td>The present value of the analog input 63 from the device subscribes with IP address 10.170.3.11, used to communicate via BACF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LON/IP</th>
<th>B=[1004,IP,&quot;10.170.3.11:0xBACF&quot;][0,63]{85}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The own automation station is on the LON network with address 1.2</td>
</tr>
<tr>
<td></td>
<td>The present value of the analog input 63 from the device on BACnet network 1004 subscribes with IP address 10.170.3.11, used to communicate via BACF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP/LON</th>
<th>B=[102,LON,&quot;1.1&quot;][1,6]{85}(P=2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The own automation station is on network 10.170.173.0.</td>
</tr>
<tr>
<td></td>
<td>The present value of the analog output 6 for LON device 1.1 is written at priority 2 on BACnet network 102.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP/MS/TP</th>
<th>B=[104,ANY,&quot;32&quot;][AI,73]{85}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The own automation station is on network 10.170.173.0.</td>
</tr>
<tr>
<td></td>
<td>The present value of analog input 73 for MSTP device 32 is subscribed to BACnet network 104.</td>
</tr>
</tbody>
</table>
12 Index

Address Resolution Protocol (ARP) ................................................. 29
Addressing ................................................................. 18
Application Layer ....................................................... 8
Application protocols .................................................. 37
ARP ................................................................. 29
Auto MDI/MDI-X .................................................... 16
Autonegotiation ......................................................... 27
Backbone ................................................................. 11
Backbone ................................................................. 11
BACnet Broadcast Management Device (BBMD) ................. 42
BACnet internetwork ................................................... 41
BACnet MAC address ................................................ 41
BACnet over IP .......................................................... 41
BACnet Protocol Analyzer (BPA) .................................. 66
BACnet Virtual Link Layer ............................................ 9
BACnet Virtual Link Layer (BVLL) ................................ 41
BACnet/IP
  Network .............................................................. 41
  Network load ......................................................... 47
BACnet/IP capture ..................................................... 65
BACnet/IP evaluation ................................................... 65
BACnet/IP restrictions ................................................ 44
BACnet/IP-BACnet/IP router ......................................... 46
Bootstrap Protocol (BOOTP) ......................................... 35
Broadcast Distribution Table (BDT) ................................ 42
Cabling ................................................................. 16
Cat 5 twisted pair ..................................................... 16
Collision domains ....................................................... 14
Data communications data capture ....................................... 64, 65
Data exchange
  Authorization ............................................................. 38
  Encryption ................................................................ 38
Data exchange authentication ........................................... 38
Data exchange integrity .................................................. 38
Data Link Layer ............................................................ 8
Data protection ........................................................... 65
DDNS ................................................................. 36
Demilitarized zone (DMZ) ................................................ 28
DHCP
  Limitations ............................................................. 45
  DHCP restrictions ..................................................... 45
DNS
  Limitations ............................................................. 45
Domain Name System (DNS) .............................................. 36
Dynamic Domain Name System (DDNS) ................................ 36
Dynamic Host Configuration Protocol (DHCP) .................... 35
Dynamic/Private Ports
  (49152...65535) ...................................................... 37
E2000 connector ......................................................... 17

Ethernet
  Variants ............................................................... 11
  Ethernet MAC address .............................................. 18
  Ethernet Standards .................................................. 11
  Ethernet switches ................................................... 21
  Fast Ethernet .......................................................... 11
  Firewall .................................................................. 46
  Firewalls .................................................................. 23
  Foreign device ......................................................... 43
  Foreign Device Table (FDT) ........................................ 44
  Gigabit Ethernet ...................................................... 11
  Gigabit Ethernet ...................................................... 11
  Hardware address ..................................................... 18
  ICMP / IGMP ............................................................ 31
  Internet .................................................................. 28
  Internet Assigned Numbers Authority .......................... 30
  Internet Group Management Protocol (IGMP) .............. 31
  Internet Service Provider (ISP) ................................ 28
  Intranet .................................................................. 28
  IP address ............................................................... 30, 31
  IP addressing .......................................................... 30
  IP broadcast ............................................................ 42
  IP packets ............................................................... 30
  IP protocol
    Fragmentation .......................................................... 30
    Routing ................................................................ 30
  IP protocol fragmentation ........................................... 34
  IP subnet .................................................................. 28, 30
  IP version 4 ............................................................. 31
  IP-Protocol Fragmentierung ......................................... 30
  IP-Protocol Routing ................................................... 30
  IPSec ....................................................................... 22
  IPv4 ....................................................................... 31
  ISO/OSI reference model
    presentation ............................................................ 8
  ISO/OSI reference model ............................................. 8
  Layer-2 switches ....................................................... 21
  LC connector ............................................................ 17
  Limits
    Datagram length ....................................................... 9
    MAC address .......................................................... 18
    MAC address Ethernet ............................................. 18
    Managed Switches ................................................... 21
    Management Information Base (MIB) ............................. 37
    MS/TP .................................................................. 50
    Multicasting ........................................................... 31
    NAT limitations ....................................................... 22
    NAT restrictions ...................................................... 46
    Net ID .................................................................. 30
    Network Address Translation (NAT) ............................... 22, 46
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network components</td>
<td>22</td>
</tr>
<tr>
<td>Network Layer</td>
<td>8</td>
</tr>
<tr>
<td>Network load</td>
<td>47</td>
</tr>
<tr>
<td>Network router</td>
<td>22</td>
</tr>
<tr>
<td>One-Hop Distribution</td>
<td>42</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>8</td>
</tr>
<tr>
<td>Point-to-Point Protocol (PPP)</td>
<td>39</td>
</tr>
<tr>
<td>Point-to-Point Tunneling Protocol (PPTP)</td>
<td>39</td>
</tr>
<tr>
<td>Ports for online operation</td>
<td>39</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>25</td>
</tr>
<tr>
<td>Presentation Layer</td>
<td>8</td>
</tr>
<tr>
<td>Protocols</td>
<td>9</td>
</tr>
<tr>
<td>Registered ports (1024...49151)</td>
<td>37</td>
</tr>
<tr>
<td>Remote Access</td>
<td>38</td>
</tr>
<tr>
<td>Reverse Address Resolution Protocol (RARP)</td>
<td>29</td>
</tr>
<tr>
<td>Router</td>
<td>22</td>
</tr>
<tr>
<td>Routing</td>
<td>30</td>
</tr>
<tr>
<td>SC connector</td>
<td>17</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>40</td>
</tr>
<tr>
<td>Servers</td>
<td>25</td>
</tr>
<tr>
<td>Services</td>
<td>9</td>
</tr>
<tr>
<td>Session Layer</td>
<td>9</td>
</tr>
<tr>
<td>Simple Network Management Protocol (SNMP)</td>
<td>37</td>
</tr>
<tr>
<td>SNMP V3</td>
<td>37</td>
</tr>
<tr>
<td>St connector</td>
<td>17</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>30</td>
</tr>
<tr>
<td>Switches</td>
<td>20</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>28, 29</td>
</tr>
<tr>
<td>Protocol suite</td>
<td>28, 29</td>
</tr>
<tr>
<td>TCP/UDP port numbers in Desigo</td>
<td>67</td>
</tr>
<tr>
<td>Tools</td>
<td>65</td>
</tr>
<tr>
<td>Transmission Control Protocol (TCP)</td>
<td>35</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>57</td>
</tr>
<tr>
<td>Troubleshooting BACnet</td>
<td>63</td>
</tr>
<tr>
<td>Troubleshooting data communications capture</td>
<td>64</td>
</tr>
<tr>
<td>Troubleshooting MS/TP</td>
<td>62</td>
</tr>
<tr>
<td>Tunneling</td>
<td>38</td>
</tr>
<tr>
<td>Tunneling protocol</td>
<td>39</td>
</tr>
<tr>
<td>IPSec</td>
<td>39</td>
</tr>
<tr>
<td>PPTP</td>
<td>39</td>
</tr>
<tr>
<td>Two-Hop Distribution</td>
<td>42</td>
</tr>
<tr>
<td>Unmanaged Switches</td>
<td>21</td>
</tr>
<tr>
<td>User Datagram Protocol (UDP)</td>
<td>35</td>
</tr>
<tr>
<td>Virtual Local Area Network (VLAN)</td>
<td>21</td>
</tr>
<tr>
<td>Virtual Private Networks (VPN)</td>
<td>38, 47</td>
</tr>
<tr>
<td>categories</td>
<td>38</td>
</tr>
<tr>
<td>VLAN</td>
<td>21</td>
</tr>
<tr>
<td>VPN categories</td>
<td>38</td>
</tr>
<tr>
<td>Well known ports (0…1023)</td>
<td>37</td>
</tr>
</tbody>
</table>
13 List of figures

Figure 1 The ISO/OSI reference model ................................................................. 8
Figure 2: BACnet over IP protocol layers ............................................................ 9
Figure 3 BACnet architecture ............................................................................ 10
Figure 4 Protocol layers Ethernet ..................................................................... 11
Figure 5 Simple tree topology .......................................................................... 12
Figure 6 Simple ring with ring master switch and client switch ....................... 12
Figure 7 Mash topoogy mit root switch ............................................................. 13
Figure 8 Line topology ...................................................................................... 14
Figure 9 Simple star/tree topology .................................................................. 14
Figure 10 Structured cabling ............................................................................ 15
Figure 11 Ethernet RJ45 connector (with pin layout) ....................................... 16
Figure 12: Common fiber optic connectors and couplers ................................. 17
Figure 13 Media converter ............................................................................... 19
Figure 14 COM server ...................................................................................... 19
Figure 15 Switch categories ............................................................................. 20
Figure 16: VLAN example ................................................................................ 21
Figure 17 Layer-3 switch with VLAN routing .................................................... 22
Figure 18 High availability topology .................................................................. 23
Figure 19 Network management in a ring topology .......................................... 26
Figure 20: The various network areas .............................................................. 28
Figure 21: TCP/IP protocol suite ..................................................................... 29
Figure 22: IP addressing .................................................................................. 30
Figure 23: IP routing ....................................................................................... 31
Figure 24 IP addressing ................................................................................... 33
Figure 25: VPN tunnels .................................................................................... 38
Figure 26: Various UDP ports with BACnet/IP define various BACnet internetworks ................................................................. 41
Figure 27: Several BACnet internetworks "on a single wire" .............................. 41
Figure 28: Broadcast on a BACnet/IP network ............................................... 42
Figure 29 BBMD: Broadcast on a BACnet/IP network with an IP router ......... 42
Figure 30 Foreign device .................................................................................. 43
Figure 31: Firewall ........................................................................................... 46
Figure 32: Using a BACnet router with a firewall ............................................. 46
Figure 33: Use of VPN in the context of NAT and firewall problems ............... 47
Figure 34: Ping -t (time) .................................................................................. 58