SIEMENS

DESIGO™
Ethernet TCP/IP and BACnet on Ethernet/IP
Basics

Building Technologies

DESIGO™

DESIGO™ Ethernet TCP/IP und BACnet on Ethernet/IP

Basics

CM110666en_03

28.02.2009

Table of contents

1 About this manual

1.1 Introduction

This manual is not an introduction to Ethernet, TCP/IP 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 and BACnet. The emphasis here is on the "BACnet on Ethernet/IP" 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 Ethernet/IP 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 Related documentation

Ref.Nr.	Dokument		Dokument-Nummer
[1]	Network architecture	Techn. principles Section 16	CM110664
[2]	BACnet Protocol Implementation Conformance Statement (PICS)	Technical principles	CM110665
[3]	System limits	Techn. principles, Section 18	CM110664
[4]	Remote management	Techn. principles, Section 14	CM110664
[5]	DESIGO INSIGHT	Installation and configuration	CM110591

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.

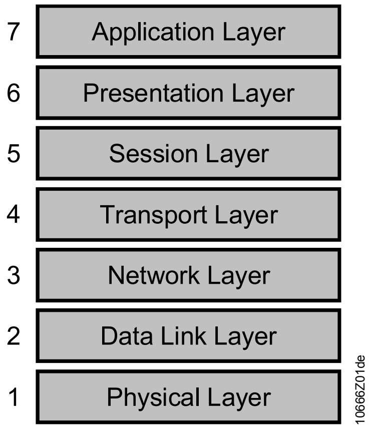


Figure 1: The ISO/OSI Reference Model

7	Application Layer	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.
6	Presentation Layer	In many systems, the functions of Layers 4, 5 and 6 are not shown separately, and are treated as part of the highest layer. For this reason, no further information on these layers is given here.
5	Session Layer	
4	Transport Layer	
3	Network Layer	The communications path is selected and managed in Layer 3. In simple systems with only one communications path, these services are not required and entire layer is therefore dispensed with.
2	Data Link Layer	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).
1	Physical Layer	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 [1]).

2.2 Protocols

Services
Protocol

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*.

Data Link Layer
for BACnet

A specific layer may be implemented in various ways. Hence, BACnet uses a wide range of different Data Link Layers: UDP/IP, 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).
- 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 5.1.2).

BACnet on Ethernet/IP is based on the three protocol suites Ethernet, TCP/IP and BACnet:

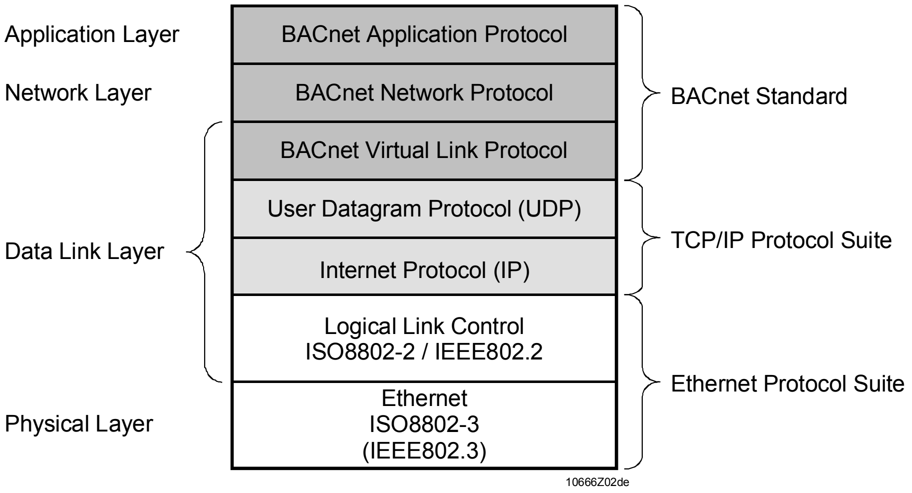


Figure 2: BACnet over Ethernet/IP protocol layers

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 Organisation (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

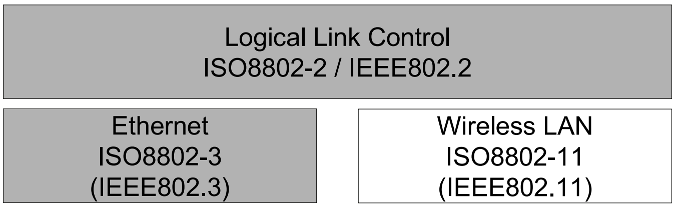


Figure 3: Ethernet protocol layers

Ethernet variants

In the field of building automation and control, the relevant variants of Ethernet are as follows:

- **10Base-T**
  Ethernet via twisted pair copper cable, 10 Mbps
- **100Base-TX**
  Ethernet via twisted pair copper cable, 100 Mbps
- **1000Base-TX**
  Gigabit Ethernet via twisted pair copper cable, 1000 Mbps
- **100Base-FX/100Base-SX**
  Fast Ethernet via fiber optic cable (1300 nm/850 nm)
- **1000Base-FX/1000Base-SX**
  Gigabit Ethernet via fiber optic cable (1300 nm/850 nm)

(FX= Single mode, SX= Multi-mode)

10Base-T is still used with older equipment (PXG80-N and PXG80-WN), while all new products support *100Base-TX* with autonegotiation. The autonegotiation 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 used directly. They are used as a "backbone" in large networks, and (in the case of fiber optic cable only) to cover longer distances.

3.2 Topologies

A star topology is used for both 10Base-T and 100Base-TX. Compared with the original bus topology, this makes for a more robust network. The extent and structure of the network is defined primarily by the maximum signal propagation times.

3.2.1 Small networks (with one collision domain only)

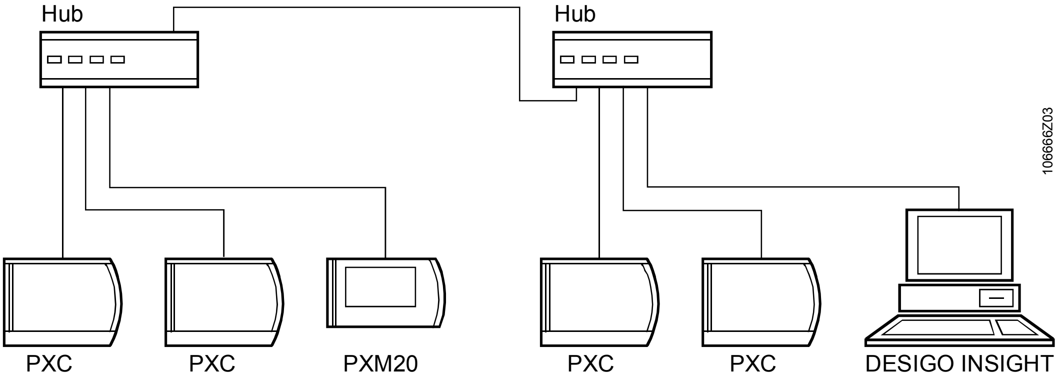


Figure 4: Small Ethernet networks (one collision domain)

Rules for 10Base-T

- Maximum 5 cable segments in succession
  i.e. max. 4 hubs in cascade
- Maximum cable length per segment: 100 m
- Maximum 1024 stations in a collision domain

STOP **Important!**

Do not use 10Base-T in new networks.

Rules for 100Base-TX

- Maximum one Class I hub, or two Class II hubs between network nodes, i.e. maximum 2 or 3 segments one after the other.
- Stackable hubs (stacked hubs with special connections) normally count as a Class II hub
- Maximum cable length per segment (hub network nodes): 100 m
  Maximum cable length per link segment (between two Class II hubs): 5 m
- Maximum 1024 stations in a collision domain

With fast Ethernet, the collision domains remain very small. Ethernet switches are used to interconnect several domains. Low-cost switches are already available on the market, and for this reason, hubs are often completely dispensed with, and switches are used instead. The difference between a hub and a switch is described in Section 3.5.

3.2.2 Large networks (with several collision domains)

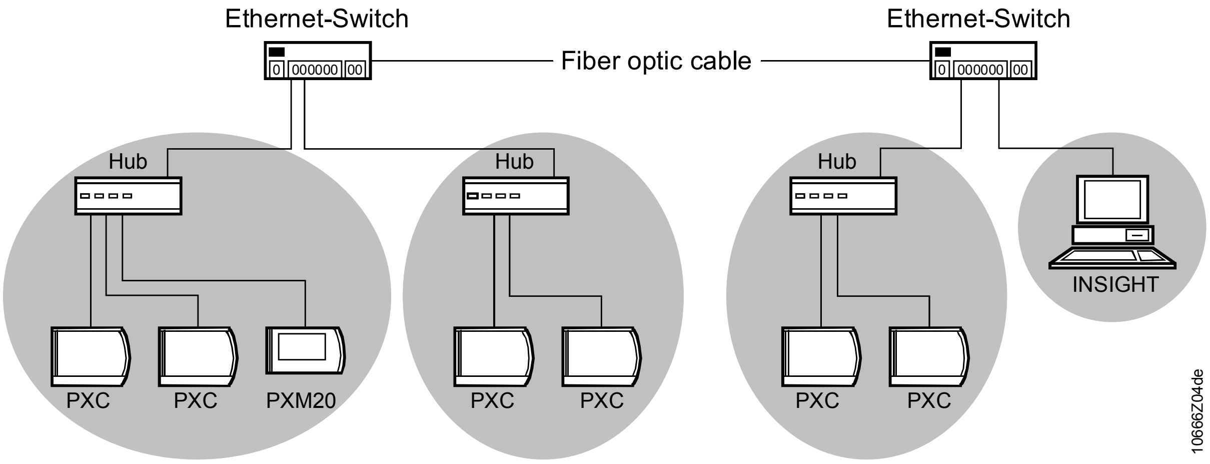


Figure 5: Large Ethernet networks (with several collision domains)

Switches connect different collision domains. The smaller the number of members in a domain, the fewer collisions occur, which means that the capacity of the network can be increased. The use of switches makes it simpler to design a network.

Rules

- Irrespective of the port speed, end devices can always be connected with copper cable of up to 100 m in length (Cat. 5 quality, or better still, Cat. 5e).
- The switch can be used as the central component for the connection of several hubs, where applicable. In this case, although the configuration rules described in Section 3.2.1 still apply, their validity ends at the port of the central switch.
- Within a local network, any number of switches may be connected in a cascade.
- If the distance between two switches is greater than 100 m, the use of fiber optic cables is recommended.

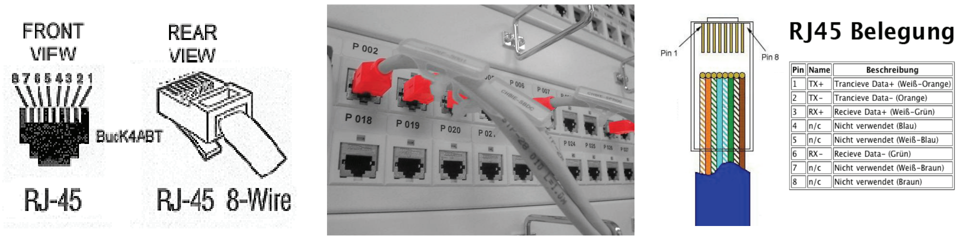
3.3 Cabling

3.3.1 Cat 5 Twisted Pair for 10Base-T and 100Base-TX

This is now standard cable technology, and consists of 4 pairs of twisted wires. The Cat 5e variant has better transmission properties and hence, more reserve capacity. The cable is available both unshielded (UTP – Unshielded Twisted Pair) and shielded (STP – Shielded Twisted Pair). Normally, unshielded cable is sufficient.

RJ45 connector

The plug-in connector is a conventional RJ45 connector.



RJ45 Belegung

Pin	Name	Beschreibung
1	TX+	Trancieve Data+ (Weiß-Orange)
2	TX-	Trancieve Data- (Orange)
3	RX+	Recieve Data+ (Weiß-Grün)
4	n/c	Nicht verwendet (Blau)
5	n/c	Nicht verwendet (Weiß-Blau)
6	RX-	Recieve Data- (Grün)
7	n/c	Nicht verwendet (Weiß-Braun)
8	n/c	Nicht verwendet (Braun)

Figure 6: Ethernet RJ45 connector (with pin layout)

Crossover cable

Two pairs of wires are used for transmission, and in normal circumstances these are not crossed. However, they must be transposed when connecting two end devices directly (i.e. without a hub). The same applies when connecting hubs and switches in cascade, unless any special uplink ports are available. Frequently, the pairs of wires can be transposed simply by pressing a button, while in other cases it is done by automatic detection (Auto MDI/MDI-X). The cable type in which the twisted pairs are crossed over is referred to as "crossover cable" or "link 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 two spare pairs of wires are not used for communications. With the new *Power over Ethernet* standard (IEEE 802.3af) (see Section 3.6), these wires are used to supply power (DC 48 V) to end devices. In this way, the supply is backed up via the hub or switch.

3.3.2 Fiber optic cable for 100Base-FX and 100Base-SX

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. This eliminates the necessity of complex calculations of length.

Single mode
Multimode

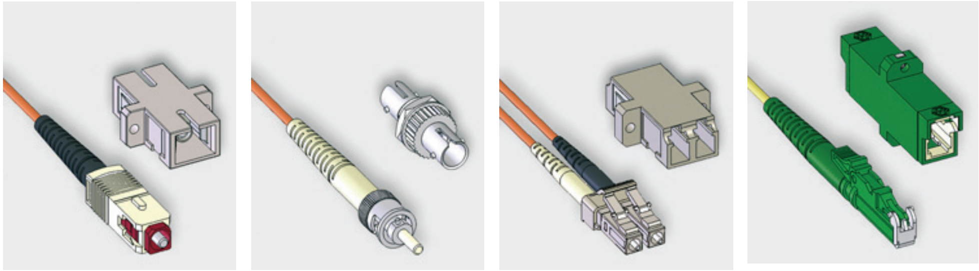
With fiber optic cables, a distinction is made between single mode and multimode. With its very fine core, single mode fiber is used primarily to span long distances (up to 30 km). Multimode fiber, with a larger diameter core, is generally used for normal LAN connections (up to 2 km).

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

100Base-FX is the commonly used standard for fiber optic LAN connections. The newer 100Base-SX standard allows the use of lower-cost components, and is designed primarily for horizontal floor-by-floor cabling.

There are various types of LWL connectors 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.

.



SX OPC connector ST connector LC connector E2000 connector

Figure 7: Common LWL connectors and couplers

3.4 Addressing

MAC address

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 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

3.5 Network components

3.5.1 Hubs or repeaters

The repeater is simply a signal amplifier, and in terms of the ISO/OSI Reference Model, it operates at the Physical layer. Since today's repeaters operate as star couplers, they are referred to as hubs. Due to the signal propagation times, only a small number of hubs may be connected together in a cascade. With 100Base-TX, there are two classes of hub. A Class I hub can be used to interconnect different media. This requires the repeated conversion of signals, which results in longer signal delays. A Class II hub, by contrast, can be used with one type of medium only. This makes it correspondingly easier to implement and the signal delay times are shorter.

Hubs are suitable for the interconnection of a geographically enclosed area (such as a room or control panel).

Note When monitoring data traffic at hubs with 10/100 Mbps auto sensing ports, note that ports with the same bit rate combine to form a domain. Hence, the local exchange of data at two 10 Mbps ports is not transferred to a 100 Mbps port.

In situations like this, the bit rate of the monitoring PC can be set manually.

3.5.2 Bridges

In the ISO/OSI Reference Model, bridge functions are assigned to the Data Link Layer. From the perspective of the Ethernet segment, this operates like a normal station, and it therefore forms the boundary of a collision domain. However, bridges are connected to two or more Ethernet segments. They receive all packets and if necessary, forward them to other segments on the basis of their destination address (Ethernet MAC address). This makes it possible to increase both the extent of a network and the number of nodes it contains.

The addresses available at the various ports are "learned" at runtime.

Bridges are no longer in common use. Their functions have been assumed by switches.

Router examples Switch examples

Figure 8: Examples of routers and switches

3.5.3 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. This micro-segmentation ensures that collisions are largely avoided, and increases the capacity of the network. Due to the collapse in the price of "simple" switches, it is increasingly possible to dispense with hubs and use switches only.

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. Configuration, if any, is minimal.
- *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 on the IP routers.

Unique, unambiguous assignment is not always possible. Layer 2 switches also evaluate some information from the IP protocol (e.g. Time-to-Live, TTL).

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.

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, a port provides access to only one VLAN.

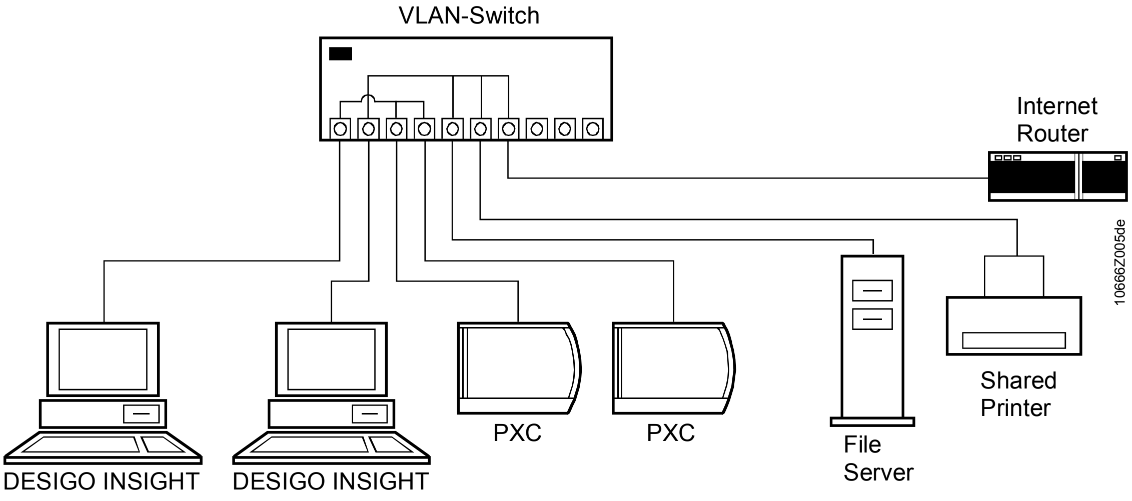


Figure 9: VLAN

Note The use of VLAN technology for the building automation and control system is particularly suitable for buildings with an existing IT infrastructure. The IT administrator can isolate ports for the building automation and control system in any location in the building. This method of grouping increases the security of the network, but without the need for additional cabling.

3.6 Other Ethernet terms

3.6.1 Power over Ethernet (PoE)

IEEE standard 802.3af defines the delivery of power to nodes (PoE) via Ethernet cables. The nodes concerned are end devices with low power consumption (IP telephones, WLAN access points, network cameras etc.). The voltage supplied (DC 48 V) is delivered via hubs or switches, and either connected to the end device via the two spare wire pairs of the Cat 5 cable, or routed directly into the data cable. Before delivering the full output, the voltage source tests the node with a test current. This prevents damage to nodes that are not PoE-compatible.

Depending on the application, either hubs/switches with PoE support can be used, or special PoE adapters can be connected into the circuit.

3.6.2 Autonegotiation

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

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.

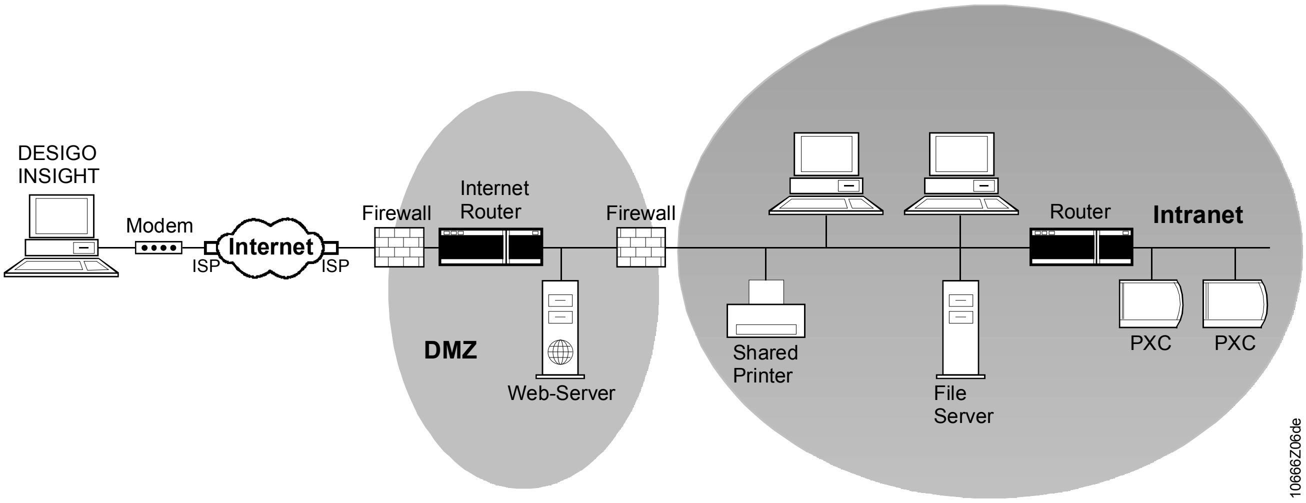


Figure 10: The various domains in a network

Definitions

The various domains of the network 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 4.4).

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.

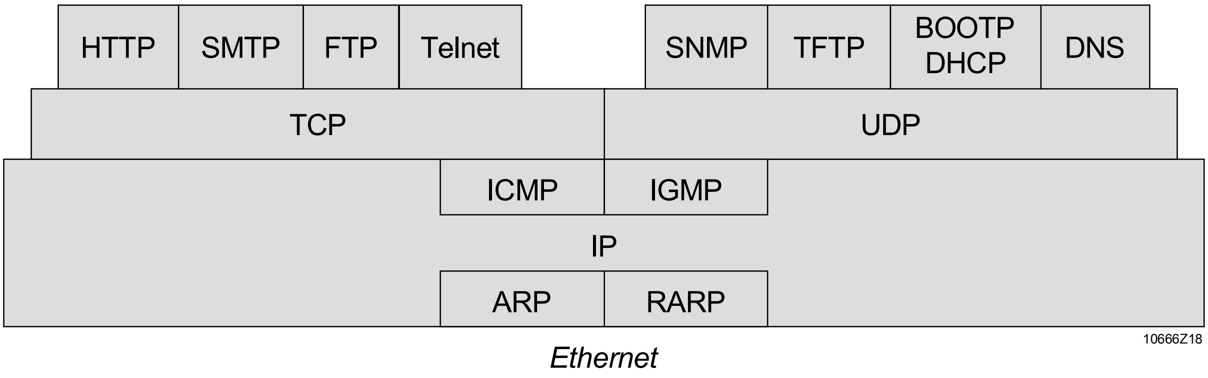


Figure 11: TCP/IP protocol suite

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.

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.

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 packets.

IP addressing

The address of an IP 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`

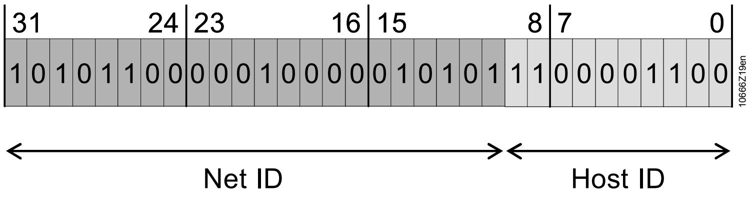


Figure 12: IP adressing

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). RFC1918 defines three specific address areas for private networks. IP addresses within these ranges are not routed.

10.0.0.0	-	10.255.255.255	Subnet mask: 255.0.0.0
172.16.0.0	-	172.31.255.255	Subnet mask: 255.255.0.0
192.168.0.0	-	192.168.255.255	Subnet mask: 255.255.255.0

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 a payload of 1500 bytes). Fragmentation can be used by both the sender and the IP routers. The recipient is responsible for re-assembling the fragments.

Routing

The IP routers 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. 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.

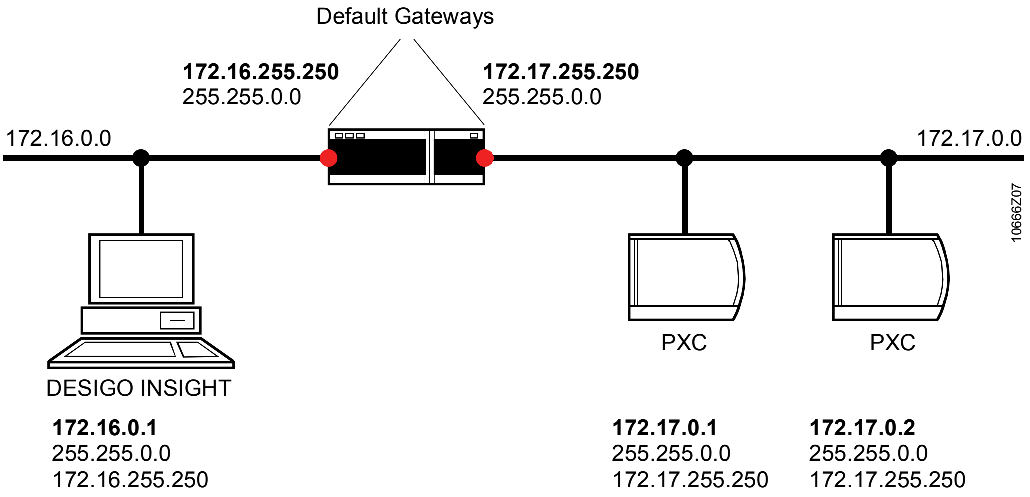


Figure 13: IP Routing

IP address

The IP subnet is identified by an IP address whose Host ID bits are set to 0. In the example shown, subnet 172.16.0.0 comprises IP addresses in the range 172.16.0.1 to 172.16.255.254.

As a rule, an Ethernet segment only accommodates IP nodes of the same subnet. However, it is also possible to operate several IP subnets on the same segment. Here too, an IP router is required for communications between the IP subnets. Only the router "knows" that the destination subnet is on the same segment, and it therefore sends the packet via the same port again. For this reason, each routed IP packet appears twice in an analysis of the data traffic.

Note The information in this section relates to the IP version most commonly in use today (IPv4). The new protocol generation (IPv6) is backward compatible with IPv4, so that the current IP version can continue to be used. The new functions of IPv6 eliminate the bottlenecks which occurred with the old IPv4 protocol. The main innovation of IPv6 relates to the extension of the IP addresses from 32 bits to 128 bits. The new addressing scheme allows a significantly greater number of IP nodes to be connected to the Internet.

4.2.3 ICMP/IGMP

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.

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.

4.2.4 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. The processes or 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

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.) are based on UDP.

4.2.6 BOOTP / DHCP

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. 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.

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 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.

Remarks on WINS

Microsoft Windows Internet Name Service (WINS) is used to register computer names and to resolve IP addresses. Whenever it is started, a WINS client registers its assigned "computer name/IP address" with the WINS server. When the need for communication arises, a WINS client can then retrieve the IP address associated with a given computer name from the WINS server. WINS is in widespread use in Microsoft-based IT networks.

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 operator station and SNMP-compatible network nodes. 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.

There are three versions available: 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.)

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 can be a security risk, as they unintentionally provide hackers with information, or act as the point of access for a hacker. For this reason, routers and firewalls are configured to accept only packets or datagrams for configured ports.

4.3 Network components

4.3.1 Routers

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). If a packet is too large to transfer, the router divides it into fragments.

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.

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

- NAT looks only at the address information in the IP header. If an application transmits IP addresses as the actual payload, these addresses are not modified by NAT. However, the IP addresses are no longer valid outside the private network, and the communication is terminated.
- NAT modifies the IP header. Certain security protocols (e.g. IPSec) see this change, and discard the packet as "invalid".

4.3.2 Firewalls

A *firewall* is a system (or group of systems) that checks communications between a secure, internal network and an insecure external network, on the basis of a set of 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.

4.3.3 Servers

The network infrastructure also includes the various servers which provide the hosts with the necessary services. These include the DNS and DHCP server.

The server functions are frequently implemented on PCs 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.

4.4 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:** Two networks with equal access rights are connected via a VPN tunnel. There are several hosts connected to each end of the link.
- **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:** A single host has a secure data connection to the primary network.

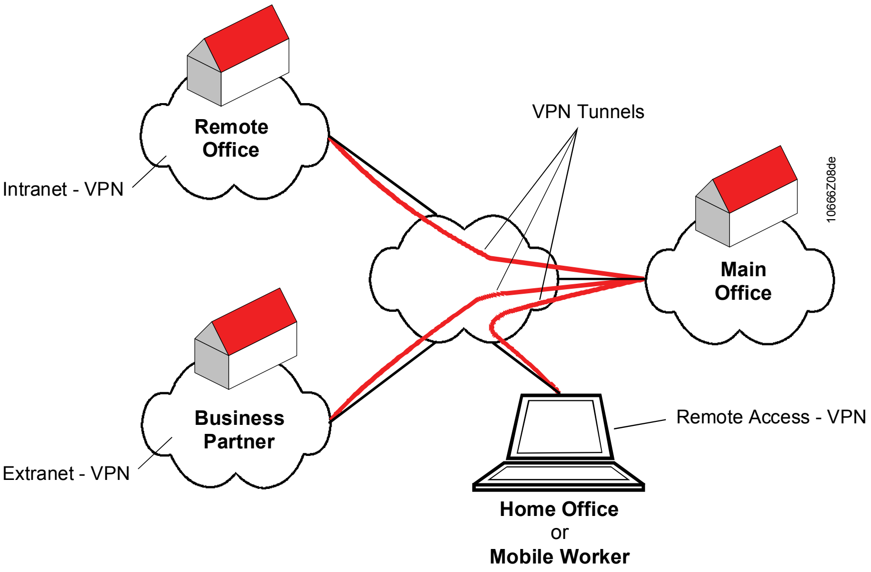


Figure 14: VPN tunnels

Secure exchange of data

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

- **Authenticity:** Authentication involves checking the identity of the communications partner. For example, communications partners must identify themselves 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.
- **Confidentiality:** 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. This is why the packets are "sealed" with a checksum.

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 companies working in the field of networking. PPTP is part of the standard Windows NT, 2000 and XP package, and is therefore available at no additional cost.
- *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.

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

Point-to-Point Protocol (PPP)

Any telephone connections between a remote client and an Internet Service Provider (ISP) are implemented by use of the *Point-to-Point Protocol (PPP).* PPP 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 (SSL) has become the established protocol for application-based encryption.

5 BACnet over Ethernet/IP

5.1 BACnet Virtual Link Layer BVLL (Annex J)

Annex J of the BACnet standard defines how BACnet NPDUs 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.

5.1.1 BACnet/IP networks and addressing

A *BACnet/IP network* consists of one or more IP subnets assigned to the same BACnet network number. 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.

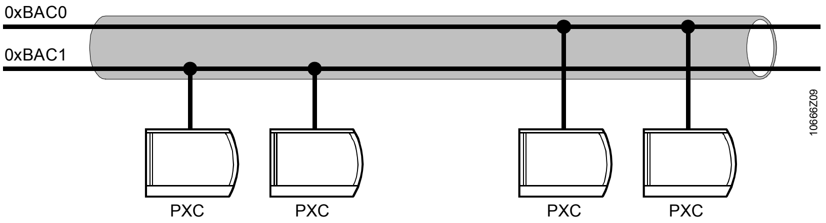


Figure 15: Various UDP ports with BACnet/IP

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.

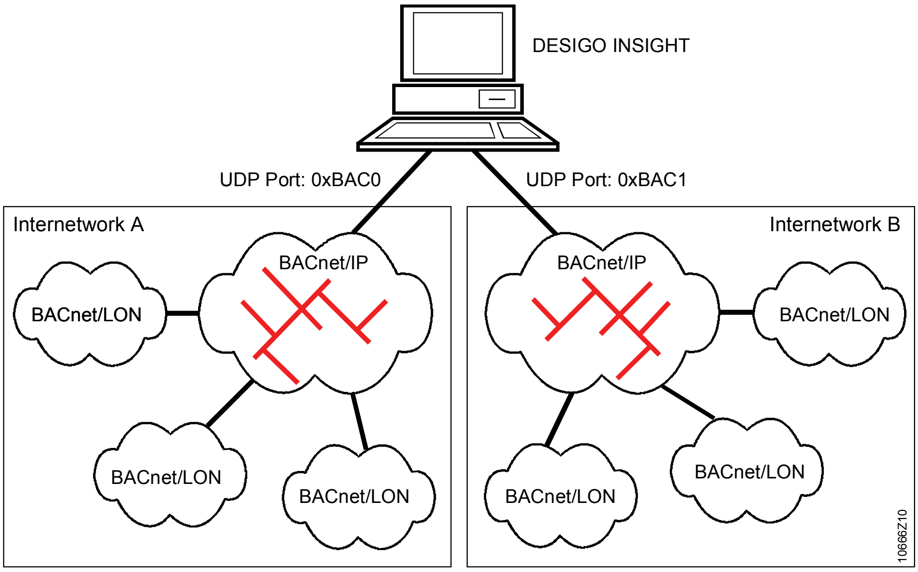


Figure 16: Several BACnet internetworks "on a single wire"

By using different UDP ports, it is possible to create several independent BACnet internetworks based on the same IT infrastructure. A DESIGO INSIGHT management station can communicate simultaneously with several BACnet internetworks, enabling the user to operate the system without restrictions.

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).

5.1.2 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).

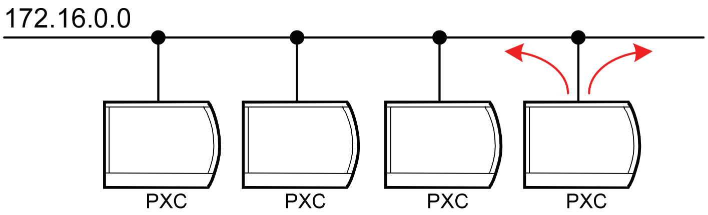


Figure 17: Broadcast on a BACnet/IP network

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 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.

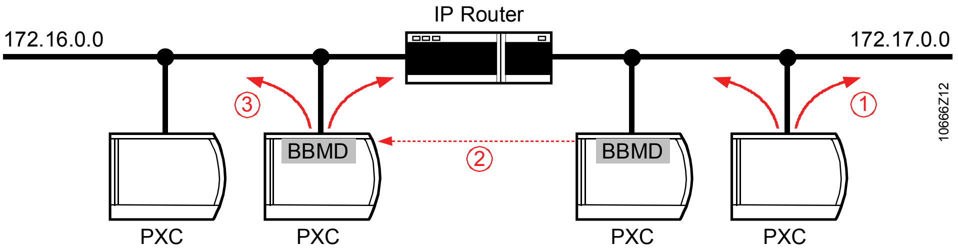


Figure 18: BBMD: Broadcast on a BACnet/IP network with an IP router

Broadcast Distribution Table (BDT)

BBMDs forward received broadcasts 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.

IP address	UDP port	Broadcast Distribution Mask	
172.16.0.1	0xBAC0	255.255.255.255	Two-hop distribution via BBMD → 172.16.0.1:0xBAC0
172.16.0.1	0xBAC0	255.255.0.0	One-hop distribution to IP subnet → 172.16.255.255:0xBAC0

The BDT is configured as a static table in the commissioning phase, and cannot be "learnt". It is identical for all the BBMDs of a BACnet/IP network. The maximum size of the BDT depends on the BBMD (product) in use, and must be determined by reference to the data sheet (PICS) see [2].

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. Communication between BBMDs in different BACnet networks is NOT permitted.
- 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.
-

5.1.3 Foreign devices

The way in which the BBMDs operate presupposes that all IP segments of the BACnet network are available at all times. The 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 device.

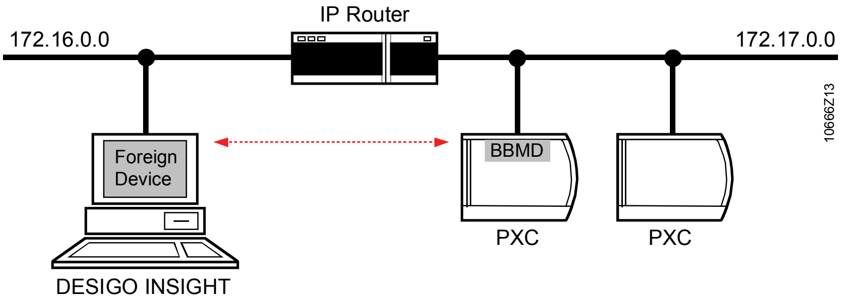


Figure 19: The "Foreign Device" function

Principle of operation

1. The foreign device registers itself with a 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.

5.2 Limitations of BACnet/IP

In principle, the BACnet Virtual Link Layer (BVLL) allows the use of UDP/IP as the transmission protocol. However, BACnet/IP is not compatible with all IT components. In such cases, either special configurations must be used or combinations involving these components must not be used.

5.2.1 IP Version 6

The BACnet standard currently supports only IP Version 4, which means that only IP nodes with a 32-bit address can be operated as BACnet/IP devices. The BACnet protocol does not yet handle the 128-bit addresses of IPv6.

5.2.2 DHCP and DNS

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

Rules

- 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.
- With BACnet, alarm recipients are entered with their 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, the option involving the device object identifier must always be used.
- 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. It is recommended that DHCP be used only with operator terminals/units (INSIGHT, DESIGO XWORKS Plus, PXM20 etc.), and that static IP addresses be assigned to 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.

5.2.3 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.

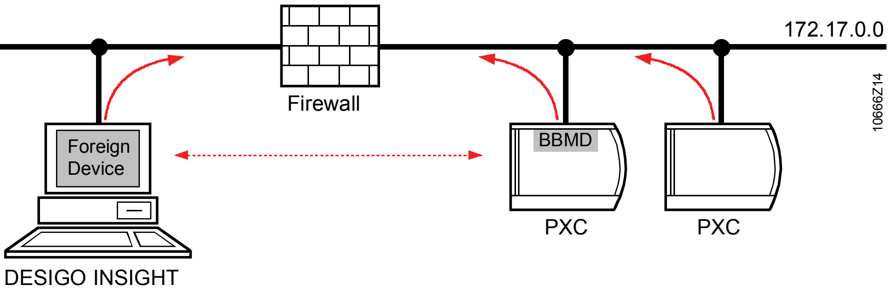


Figure 20: Firewall

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.

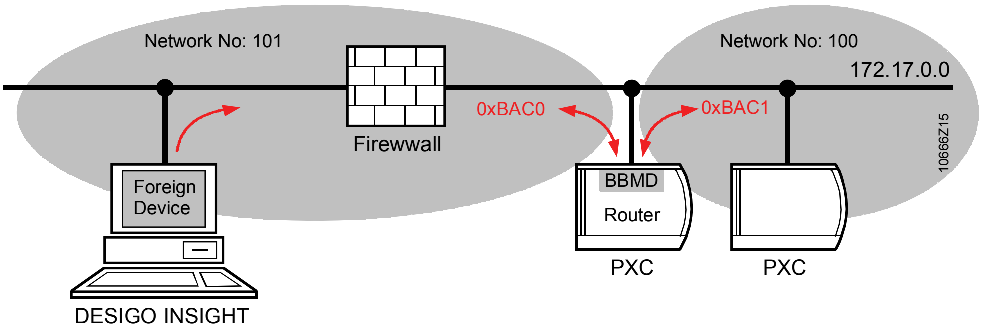


Figure 21: Using a BACnet router with a firewall

The automation station variant shown in the example, with BACnet/IP to BACnet/IP router is not yet available in the DESIGO system.

5.2.4 NAT

Network Address Translation (NAT) is used to map IP addresses from the private domain to official "Internet" addresses. In this process, the address information in the IP protocol header is modified, as described in Section 4.3.1.

With BACnet/IP, IP addresses are transferred as the UDP payload. These addresses are not modified by NAT. This results in the transmission of invalid address information to the Internet. Hence, BACnet devices cannot communicate via NAT.

There is no official BACnet standard solution available as yet. However, some suppliers have developed proprietary solutions for the NAT problem.

5.2.5 Prospects and workarounds

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

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

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.

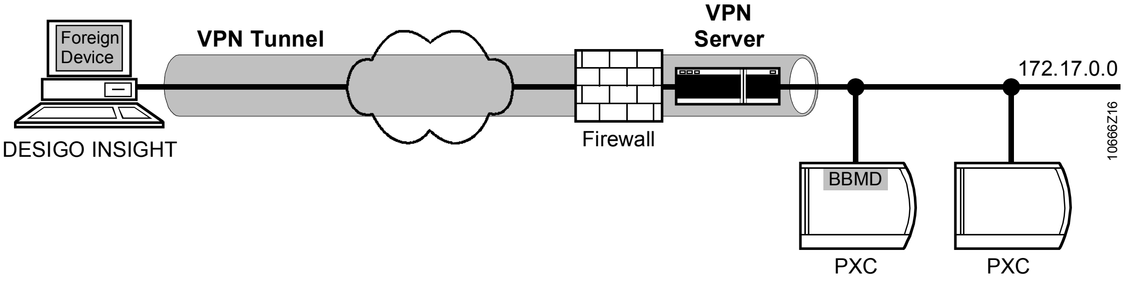


Figure 22: Use of VPN in the context of NAT and firewall problems

5.3 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.).

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.

Important!

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.
- Operator stations (DESIGO INSIGHT) 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 INSIGHT 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. Larger networks, moreover, have larger backbones (Gigabit-Ethernet), 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.

6 Dealing with problems

BACnet on Ethernet/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.

6.1 Ethernet

Check: Is the link signal present?

With hubs and 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.

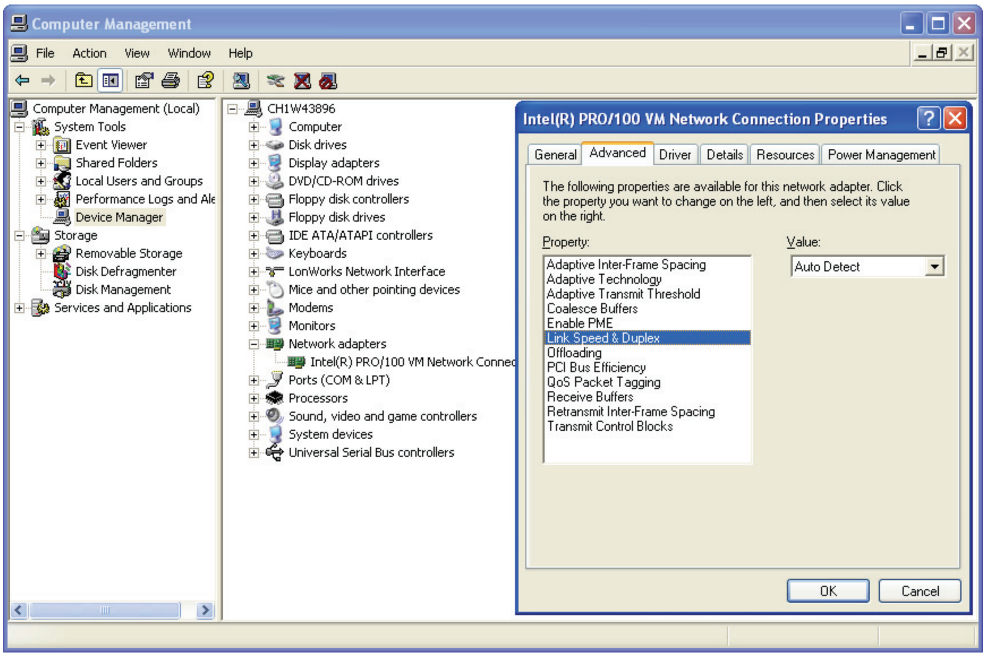
- Is the extension module (PXC modular) plugged in firmly?
- Are all connectors firmly in their sockets?
- Is there a supply voltage for the hubs/switches?
- Is a crossover cable in use?
- Is the uplink port of the hub/router set correctly?

Check: Is there a high collision rate? Is communication slow?

- Have the rules for the design of the collision domain been observed (see 3.2)?

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.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property: Link Speed & Duplex

Value: Auto Detect

Check: Are VLAN switches in use?

Are all BACnet devices configured on the same VLAN (see section 3.5.3)?

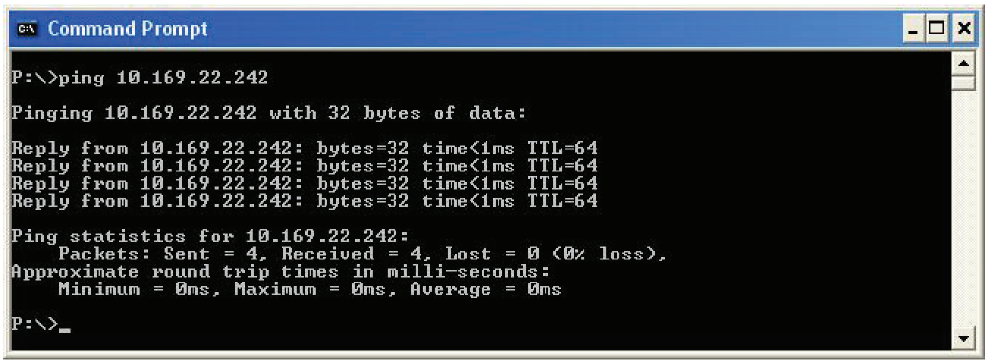
6.2 TCP/IP

Check: Can the destination address of the IP node be accessed with Ping?

Command line: `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?



```
P:\>ping 10.169.22.242

Pinging 10.169.22.242 with 32 bytes of data:

Reply from 10.169.22.242: bytes=32 time<1ms TTL=64
Reply from 10.169.22.242: bytes=32 time<1ms TTL=64
Reply from 10.169.22.242: bytes=32 time<1ms TTL=64
Reply from 10.169.22.242: bytes=32 time<1ms TTL=64

Ping statistics for 10.169.22.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

P:\>_
```

Is a PXG80-N or PXG80-WN with a date of manufacture prior to 1 March 2006 in use and is there a BOOTP server in the network?

These devices erroneously transmit BOOTP requests (address requests) and assume an error status if a BOOTP server answers.

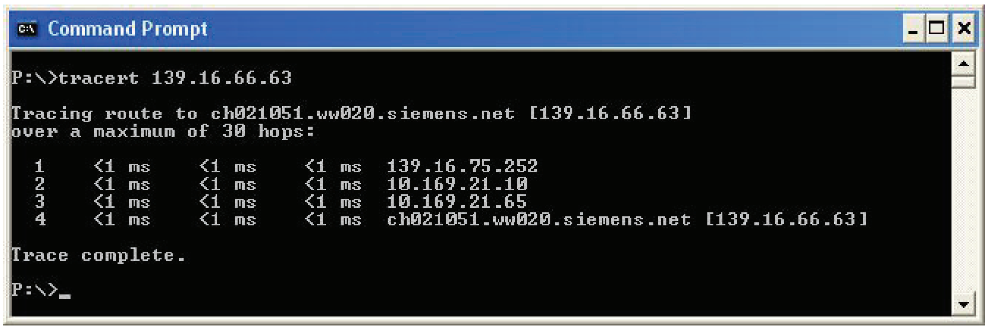
→ Disable the BOOTP request from PXG80-N and PXG80-WN. For the procedure, refer to Support Knowledge Base No. 496 Disable the BOOTP request from PXG80-N and PXG80-WN. For the procedure, refer to Support Knowledge Base No. 496: http://intranet.sbt.siemens.com/swanweb/en/kb/kbview.php?kb_no=496

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 8)?



```
P:\>tracert 139.16.66.63

Tracing route to ch021051.ww020.siemens.net [139.16.66.63]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  139.16.75.252
  2    <1 ms    <1 ms    <1 ms  10.169.21.10
  3    <1 ms    <1 ms    <1 ms  10.169.21.65
  4    <1 ms    <1 ms    <1 ms  ch021051.ww020.siemens.net [139.16.66.63]

Trace complete.

P:\>_
```

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.

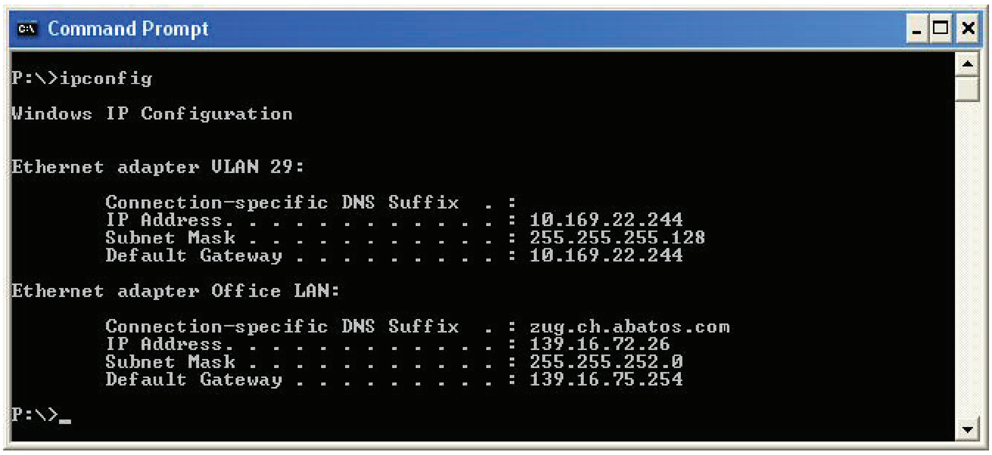
Are the required ports open in the firewall (see Section 8)?

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

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

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

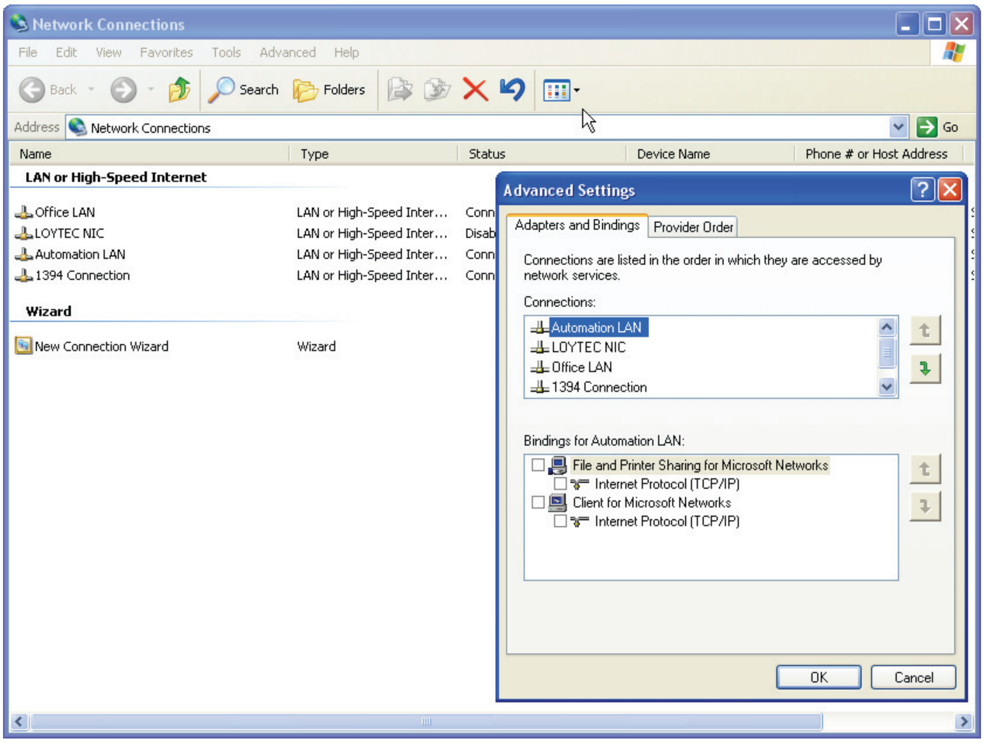
Command line: `ipconfig [/all]`



```
P:\>ipconfig

Windows IP Configuration


Ethernet adapter VLAN 29:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.169.22.244
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 10.169.22.244

Ethernet adapter Office LAN:

        Connection-specific DNS Suffix  . : zug.ch.abatos.com
        IP Address. . . . . . . . . . . . : 139.16.72.26
        Subnet Mask . . . . . . . . . . . : 255.255.252.0
        Default Gateway . . . . . . . . . : 139.16.75.254

P:\>_
```

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**. From the menu bar, select **Advanced > Advanced Settings...** and click the **Adapters and Bindings** tab. The network connection used must appear at the top of the list in the **Connections** field.



Name	Type	Status
LAN or High-Speed Internet		
Office LAN	LAN or High-Speed Inter…	Conn
LOYTEC NIC	LAN or High-Speed Inter…	Disab
Automation LAN	LAN or High-Speed Inter…	Conn
1394 Connection	LAN or High-Speed Inter…	Conn
Wizard		
New Connection Wizard	Wizard	

Device Name — Phone # or Host Address

Connections are listed in the order in which they are accessed by network services.

Connections:

- Automation LAN
- LOYTEC NIC
- Office LAN
- 1394 Connection

Bindings for Automation LAN:

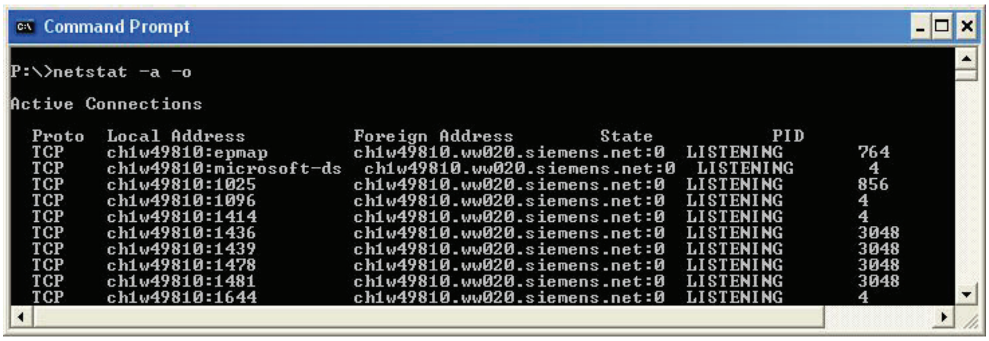
- □ File and Printer Sharing for Microsoft Networks
  - □ Internet Protocol (TCP/IP)
- □ Client for Microsoft Networks
  - □ Internet Protocol (TCP/IP)

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?

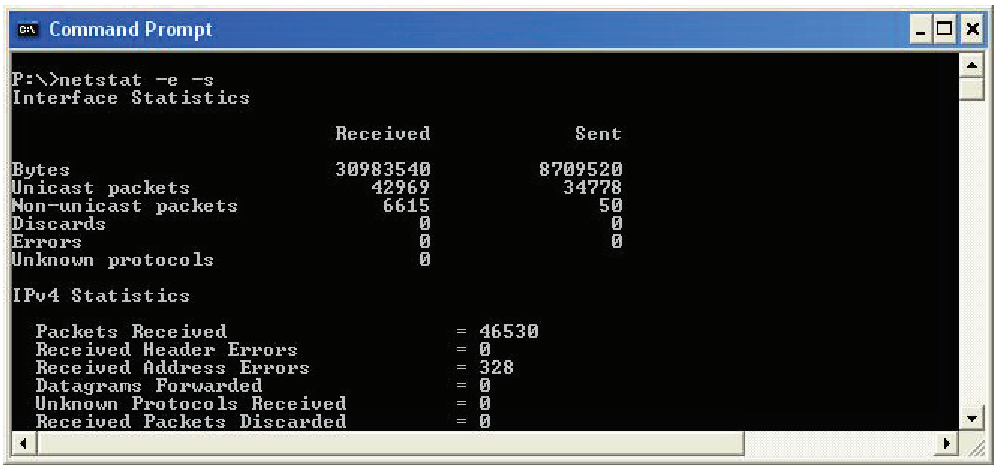


```
P:\>netstat -a -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    ch1w49810:epmap        ch1w49810.ww020.siemens.net:0  LISTENING       764
  TCP    ch1w49810:microsoft-ds  ch1w49810.ww020.siemens.net:0  LISTENING       4
  TCP    ch1w49810:1025         ch1w49810.ww020.siemens.net:0  LISTENING       856
  TCP    ch1w49810:1096         ch1w49810.ww020.siemens.net:0  LISTENING       4
  TCP    ch1w49810:1414         ch1w49810.ww020.siemens.net:0  LISTENING       4
  TCP    ch1w49810:1436         ch1w49810.ww020.siemens.net:0  LISTENING       3048
  TCP    ch1w49810:1439         ch1w49810.ww020.siemens.net:0  LISTENING       3048
  TCP    ch1w49810:1478         ch1w49810.ww020.siemens.net:0  LISTENING       3048
  TCP    ch1w49810:1481         ch1w49810.ww020.siemens.net:0  LISTENING       3048
  TCP    ch1w49810:1644         ch1w49810.ww020.siemens.net:0  LISTENING       4
```

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?



```
P:\>netstat -e -s
Interface Statistics

                           Received            Sent

Bytes                      30983540         8709520
Unicast packets               42969           34778
Non-unicast packets            6615              50
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                   = 46530
  Received Header Errors             = 0
  Received Address Errors            = 328
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
```

6.3 BACnet

Check: Are IP routers used?

Is NAT activated in the router? BACnet cannot communicate via NAT!

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? ("Update All BBMDs")

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, 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.

PXG80-N runs automatic network checks, and indicates 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.

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 operator stations unique within each internetwork?

6.4 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 7 describes the procedure in detail.

7 Appendix A – Capture and analysis 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.

7.1 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. The question of where, when and for how long the data traffic is monitored must be discussed with the IT manager.

7.2 Determining the capture point

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. If hubs are used, the packet analyzer ("sniffer") can be connected to the same hub as the potential source of the problem. In systems using 10/100 Mbps hubs, it is important to ensure that the local traffic between two 10 Mbps ports is not transferred to the 100 Mbps ports. In such cases, the bit rate of the sniffer must be reduced manually to 10 Mbps.

Where switches are used, a given port can receive only broadcasts and packets addressed directly to that node. The more expensive 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.

7.3 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.ethereal.com). Note the following when configuring the sniffer:

ℹ **Important!**

- If the PC/Notebook has several IP ports available, select the required port.
- The data should be captured in "promiscuous mode" in order to capture 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.

SBT BACnet Protocol Analyzer (BPA)

Provided that only UDP port number 47808 (0xBAC0) is used for BACnet/IP, Ethereal can decode the BACnet messages very simply. 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.

8 Appendix B – TCP/UDP port numbers used with DESIGO

8.1 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. In the case of DESIGO INSIGHT, the details should be taken from the installation guide.

BACnet on Ethernet/IP

- One UDP port per BACnet/IP network (range: 47808..47823, default: 47808)
- One specific port (range: 47808..47823) or a dynamic port (range: 49152…65535) for BACnet devices, operating 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.

Web functionality

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

8.2 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. For DESIGO INSIGHT, refer to the installation guide for details [5].

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 (SSL)
- SMTP (Port: 25) for e-mail
- 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)
- UDP port for commissioning (always 47808)
- DHCP (Port: 68), if configured
- FTP (Port: 21) for FTP file download (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

- All ports as for PXG80-N
- HTTP (Port: 80) for Web server
- SMTP (Port: 25) for e-mail

DESIGO INSIGHT

- UDP Port for BACnet (range: 47808..47823) or
  as foreign device (range: 49152…65535)
- Microsoft SQL server (Port: 1433)
- TCP port for license server (Port: 135)
- HTTP (Port: 80) for Web server
- HTTPS (Port: 443) for Web server (SSL)
- TCP Port for .NET Remoting between IIS and DI (Port: 11111)
- Various ports for IIS configuration (ports: 42424, 135, 1027)

DESIGO XWORKS Plus

- UDP Port for BACnet (range: 47808..47823) or as foreign device (range: 49152…65535)
- UDP port for commissioning (always 47808)

Index

Table of illustrations

Siemens Schweiz AG
Building Technologies Group
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41 724 24 24
Fax +41 41 724 35 22

Siemens Schweiz AG
Building Technologies
Sennweidstrasse 47
CH-6312 Steinhausen
Tel. +41 585-579 200
Fax +41 585-579 230
www.siemens.ch/sbt

The information in this document contains general descriptions of available technical options, which may not apply in all cases. As a consequence, required features should be specified on a case-by-case basis at the time the contract is concluded.

www.siemens.com/buildingtechnologies