Ethernet & IEC 61850

Concepts, Implementation, Commissioning

Manual

Table of Content

Release: 07.05.09

E50417-F1176-C361-A3

Information for Your Safety

This manual does not represent a complete listing of all the safety measures required to operate the equipment (module, device) since specific operating conditions may make further measures necessary. However, it contains information which you have to observe in order to ensure your personal safety and in order to avoid property damage. The information is highlighted by a warning triangle and, depending on the degree of danger, is shown as follows:

Warning

indicates that death, severe personal injury or substantial property damage can result if proper precautions are not taken.

Caution

indicates that minor personal injury or property damage can result if proper precautions are not taken.

Qualified personnel

Commissioning and operation of equipment (module, device) described in this manual may only be carried out by qualified personnel. Qualified personnel in the sense of the safety instructions in this manual are persons who are entitled to commission, enable, earth and identify devices, systems and circuits in accordance with the standards of safety technology.

Use as prescribed

The equipment (device, module) may only be used for the applications described in the catalogue and the technical specifications and only in combination with third party equipment recommended or approved by Siemens.

The successful and safe operation of this device is dependent on proper handling, storage, installation, operation, and maintenance.

Hazardous voltages are present in parts of this electrical equipment during operation. Severe personal injury or property damage can result if the device is not handled properly.

- The device is to be earthed to the protective-earth terminal before any other connections are made.
- Hazardous voltages can arise in all the circuit parts connected to the power supply.
- Hazardous voltages can be present in the equipment even after the power supply voltage has been removed, i.e. capacitors can still be charged.
- Equipment with current transformer circuits may not be operated openly.

The limits specified in this manual or in the operating instructions respectively may not be exceeded. This point must also observed during testing and commissioning.

Document version: 1.02.01

Table of Content

What You Can Expect 1

Computer and Co no longer have a monopoly on network functions. From their former refuge in the office world, they have started out and made their way to serve other applications in new locations. And maybe, you are one of those who already indulge in the comfort of a media server which provides pictures, videos and music. Isn't it obvious then to also go with the times, to go where the power comes from that drives everything.

All Aboard, please!

Ethernet is now also the motto for communication in the energy environment, at best in conjunction with IEC 61850. Many things stay the same as they always were but a lot is different with this new way to communicate. Anyone who doesn't want to leave things to chance in the conception and commissioning of his first IEC 61850 system, but also doesn't want to have to wade through a ton of literature, is well served with this book. You won't learn everything here but more than enough for a good start into the subject.

Trilogy

Basically, the book can be divided into three parts. In the first part, Chapters 2 to 4 explain the fundamentals of communication via Ethernet. It starts with an overview of possible topologies. It continues with a summary of network theory that should give you a better understanding of important basic concepts and procedures. With several important comments about the individual components that are necessary for Ethernet communication we leave this more abstract first section.

In the second part, we wake up to reality and present an application-oriented sample configuration in Chapter 5. In the following Chapters 6 to 10 we will always refer back to this configuration so as to explain to you all the preparations that are needed to arrive at a functioning communiation via Ethernet.

In the third and final part it is then: Connect, turn on and check. The three Chapters 11, 12 and 13 will be happy to answer all your questions.

Reading Tip

Are you already familiar with terms such as network mask, ring topology, MAC address and so on? If so, why don't you go directly to Chapter 5. If you don't already have this necessary basic knowledge, we recommend that you by all means read Chapters 2 to 4.

Call Me

Should you have additional questions, our Hotline would be more than happy to help you:

Tel.: 01 80 - 5 24 70 00
Fax: 01 80 - 5 24 24 71
e-mail: support.energy@siemens.com

Training

You can obtain the individual course offerings from our Training Center. There, Siemens offers you extensive courses on configuring and commissioning IEC 61850 systems and on DIGSI 4.

Siemens AG
Energy Sector
Power Distribution Division
Humboldtstr. 59
90459 Nuremberg, Germany
Tel.: +49 (0)9 11/4 33-70 05
Fax: +49 (0)9 11/4 33-79 29
Internet: www.siemens.com/power-academy-td

Beyond the Horizon It Continues

If you are interested in further information, here is a selection of order numbers on the topic of Ethernet and IEC 61850.

- **DIGSI 4 Start Up** Manual
  C50417-G1176-C152-A2
- **Ethernet & IEC 61850 Start Up** Manual
  E50417-F1176-C324-A1
- CD - **DISGI 4 YOU - Start Up**
  E50417-A1174-C329-A1
- CD - **SIPROTEC 4 YOU - Start Up**
  E50417-A1174-C215-A2
- CD - **SIPROTEC 4 YOU - Ethernet + IEC 61850**
  E50417-A1174-C314-A2

In particular, we strongly recommend - especially all Windows users - the book “Linux Network Administration” by Jens Banning. This book describes fundamental topics such as TCP/IP, connection to the network, routing, etc., very clearly. It is published by Addison-Wesley with the number ISBN 3-8273-1855-6.

Choosing the Right Topology

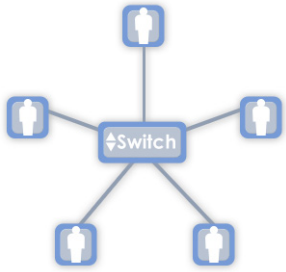
2

Before you begin to lay the first cable, the question of the physical topology must be clarified. What kind of connection structure of the individual devices is the right one for you? This will ultimately be influenced by many different factors. The desire for redundancy will play a role but also the physical dimensions of the required network will be an important factor in the selection of a configuration. Maybe you've already made the decision, then you can just skip this chapter.

Should you decide to read on, you will become familiar with our two favorites in the area of network topology: Star and Ring. From the pool of network topologies which also include the bus topology, the tree structure or the meshed network, these two topologies have materialized as the only ones which can serve our practical purposes.

Star Light - Star Bright

In the **star topology,** the connections of all devices meet at the same point - at least, in thought. Since we can't really interconnect the individual connections directly with one another, we need a distributor to do this job.



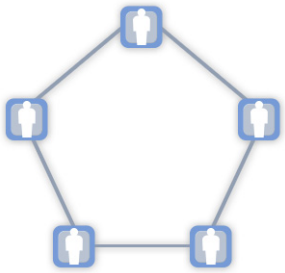
Switch in the middle: The star topology requires a distributor.

In Ethernet networks, the intelligent switch has established itself as the distributor of data and has pretty well forced the dumb hub to the offside as a result. The individual participants, on the other hand, lack any direct physical relationship with one another. The participants which we have symbolized as small figures can be PCs, but also devices of the protection and automation technology. With communication via Ethernet according to IEC 61850, even routers and time servers are considered to be participants.

The star topology permits high transmission rates, has a clear and understandable structure and can easily be expanded, although the cable installation is complicated. The failure of an end device has no effect on the rest of the network. On the other hand, a defective distributor will cripple the entire network.

Lord of the Rings

Whoever prefers (all)round things, grabs the **ring topology**. Here, each end device is connected to exactly two other devices so that a closed ring results.



Roundabout: The ring topology is a closed system.

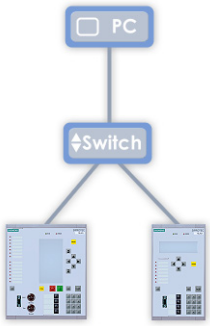
In this format, information is passed from participant to participant until it reaches its destination. Earlier, it would become critical if there was an interruption in the ring. This argument is no longer valid today: If the ring is interrupted in one spot, the system automatically changes over to line operation; communication can be continued almost without interruption. As we will see, switches also play an important role in this.

Star Topology

The star is probably the most frequently used topology for small networks. This may be due to its uncomplicated (hardware) installation which permits a fast and at times even tentative installation especially for small teams. A few cables and a distributor (switch or hub) are enough when security requirements don't play a role.

Small Beginnings

The picture below shows probably the simplest star structure of the world, reduced to the basics.



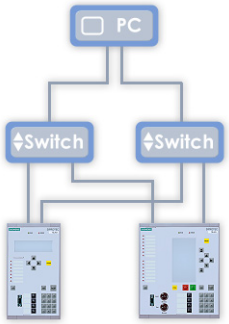
Star base: Simple structure, but then zero redundancy.

In such a topology, the minimum that is required is a so-called switch that connects the individual participants to one another. In our picture, that is only three (2 x SIPROTEC 4, 1 x PC). In actual fact, several devices can be connected to one switch.

How many depends on the number of ports the switch has. If one switch is not sufficient for all devices, or, the local situation requires it, then several switches can also be used. These are then linked together. In this way, larger structures can also be realized.

Double Take

The structure shown above may be simple but at the same time it is without any redundancy: If the PC's network card goes on strike, information can no longer be queried, commands can no longer be sent. If a device interface fails, the associated device is also not accessible. And, if the switch breaks down, then nothing works anymore. Still not the best, but the following configuration already looks a little bit better.



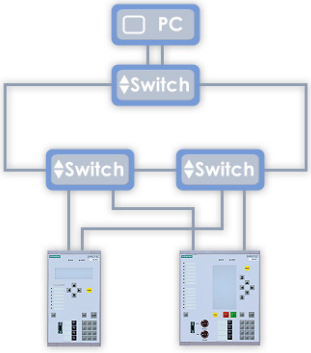
Basic expansion: Switches and network adapter exist twice on the PC.

With this structure we double the number of switches. Each device is connected via two switches each. This presumes, of course, that the connected devices can be equipped with redundant interfaces. In Chapter 4 we will learn that this works without a problem with the EN100 communication module for SIPROTEC 4 devices - not only for an electrical but also for an optical solution - because these modules have two interfaces through which two lines can be connected in parallel. Only one of the two interfaces is active at all times, however. The second communications channel always serves as a reserve and is automatically activated by the module as required. In this way, there is no interruption to the PC when a switch fails. In such a case, all devices that had actively built up a connection via the failed switch, change over to their second connection that is hooked up to another switch.

The PC has now also gotten two inputs and has gained security as a result. This becomes possible through a teaming-capable network card with two inputs (also see Chapter 4). The PC itself is not yet redundant; we'll present you with such a solution in a few hundred words.

Into the Ring

With several switches that are also doubled for redundancy reasons, the cabling effort between switches and higher level control centre (in our case - PC) increases dramatically. A more practical solution is to connect all switches with one another in the form of a ring.



Ring or star? The boundaries become blurred.

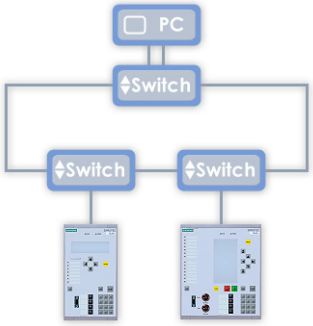
As a ring connection, you should give preference to a fiber-optic cable. When the switches work as amplifiers, you can easily realize connections over several kilometers. You then also connect the individual devices to the switches via fiber-optic or, for shorter distances, electric is also possible.

Ring Topology

Strictly speaking, the last shown structure is still a star even when the individual switches are connected together to form a ring. The switches are distributors, however, to which the individual devices are connected - and that corresponds to our definition of a star topology.

Bridging the Gap

To spite a bridge to the pure ring, let’s imagine that switches are connected together to form a ring to which only one device each is connected. In this way, we come to the following easy-to-understand structure.

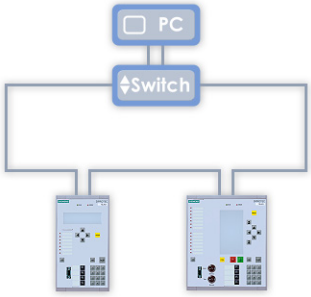


Transformation: This is how a star turns into a ring.

But we only have a pure ring structure when all devices are interconnected in one ring without having to use external switches to do this.

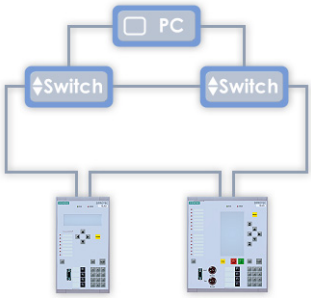
Savings Effect

It would therefore be perfect if we could drag each switch into the associated device. And, in fact, this is possible through the optic EN100 modules. The optic EN100 modules can, as an alternative to redundant operation, also actively transfer data through both ports simultaneously. Through this integrated switch functionality, you can (essentially) dispense with the external switches assigned to the devices.



Let there be light: In the optic EN100 modules, the switch is already integrated.

In this way, you can interconnect up to 30 SIPROTEC 4 devices to an optic ring. Because of the coupling to the PC (or to the control centre, in general), you will not, however, be able to dispense with at least one external switch. As a rule you will, for all that, implement this connection as redundant and will use two switches for this.



It takes two: Two switches guarantee redundancy for the PC interface.

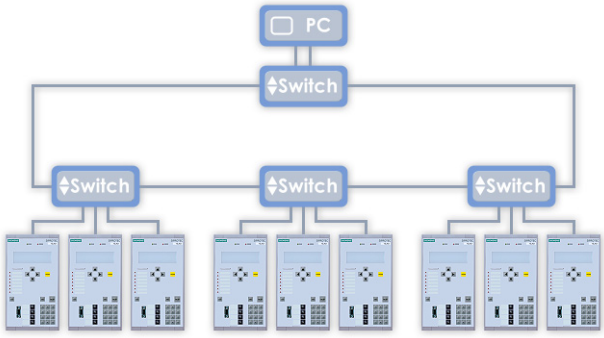
Talking about redundancy: Information is passed from device to device in the ring until it reaches its destination. If the ring structure shown is broken up in one spot it becomes a line. The communication still continues to function almost interruption-free. However, a second error in the line or in one of the devices can normally not be compensated. Since two switches are used in the configuration shown, it reduces the maximum possible number of SIPROTEC 4 devices in the ring to 27. Why this is so, and how you can calculate the permittable number of devices, you will learn in Chapter 4.

Commonly Used Configurations

To conclude this chapter, we will show you three commonly used configurations.

Configuration #1

In the first figure, you can see the probably most frequently occurring topology.

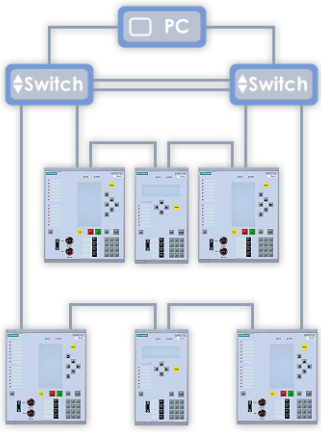


Popular combination of one ring and several stars

Several devices, arranged in stars, are connected to switches that are interconnected to one another via an optical ring, while copper cables produce the electrical connection between switches and devices. Whoever decides to use this concept cannot place great value on redundancy but, on the other hand, gets a cost-tolerable solution.

Configuration #2

Considerably more redundancy is offered by the second example. Two independent of one another rings are connected to two switches. A double line connects these switches with one another and even the PC is redundantly interconnected.

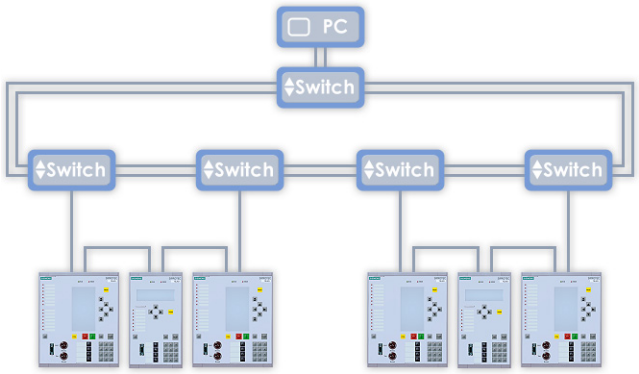


Two rings fitted into each other

The expansion possibilities of such a topology are considerable. You may install up to 27 devices to each ring. You can, at the same time, increase the number of rings if the switches used have sufficient ports.

Configuration #3

An alternative is shown in the third example. Each ring can call two swiches each its own. Even the PC is interconnected by its own switch. The ring has two optic lines.



Two rings connected via a double main ring

Here as well: A ring may connect a maximum of 27 devices with one another. The number of rings in this assignment are, indeed, theoretically unlimited.

A Little Bit of Network Theory

3

Our transmission path for IEC 61850 is called Ethernet. Why this is so, is explained by taking a short look into the past. Already in the year 1976, the first designs for an Ethernet system existed. Back then, printer sharing by several users stood in the foreground. Today Ethernet, with a wide-spread popularity of more than 90%, is the most commonly used connection type between computers and their peripherals in a local network - and with that the mainstream communications medium of our time.

Good Reasons

Reason enough to focus on this transmission technology as far as IEC 61850 is concerned, especially since you can already fall back on a cost-effective product line and often also on an already existing infrastructure. That Ethernet is simultaneously highly backwards and forewards compatible, makes it particularly interesting with regards to present and future investments. In that way, a 10-MBit network can easily be integrated into the usual 100-MBit network - and this on the other hand in the 1-GBit network of tomorrow.

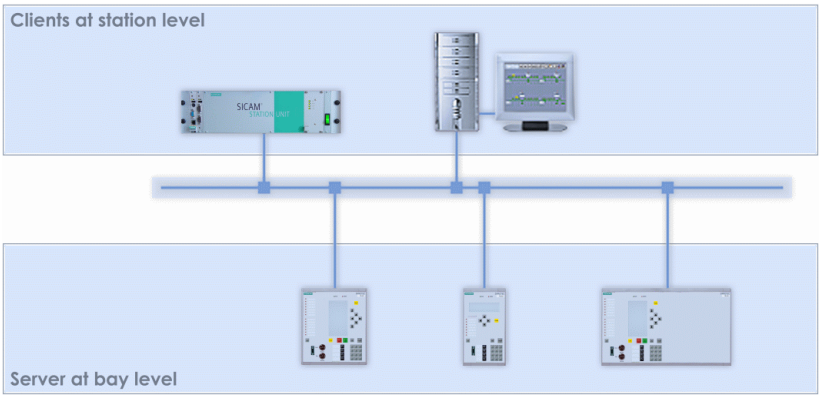
In this chapter, we will give you some insight into several topics which are inseparably linked to Ethernet and that serve as basis for understanding later chapters.

Types of Communication

As a rule, networks are classified by the role the individual participants take. And so it is, that Peer-to-Peer networks differentiate themselves from Client-Server networks.

Horizontal and Vertical

In the Peer-to-Peer version, devices communicate with others who find themselves on the same level hierarchically-speaking. For that reason, you also talk about horizontal communication. A Client-Server network, on the other hand, connects participants on different hierarchies. In this vertical communication, the client takes on the role of quizmaster and wants to know all sorts of information. The servers, as data suppliers, hopefully always have the correct answers.



Server and Clients - Peer-to-Peer: Everyone gets everything

Length and Breadth

With IEC 61850 both is possible, horizontal and vertical, and that simultaneously. Why don't you briefly take a look at our schematic drawing. The SIPROTEC devices on the field level collect data and pass it on. They are the servers. The automation system on the station level, here a SICAM PAS, wants the data, gets it and processes it. This is the client of which there can be several, by the way. But it gets even better: a client can demand data from all servers, vice-versa, a server can provide all clients with data. And: many tasks are handled directly between the servers. They communicate with one another, horizontally, without requiring the client. This so-called cross-communication is called GOOSE in IEC 61850: Generic object oriented substation event.

Data Transmission

Now that the jurisdictions of the communication devices have been clarified, we need to think about how data is transferred via the Ethernet. We're not talking so much about the physical sequence as the logical point of view.

Casting Show

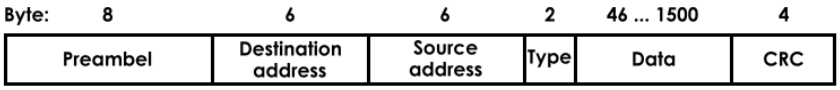
In its decision to whom a device sends its messages, technically "telegrams", the device has principally three possibilities: to one, to many or to all. In the language of telecommunication this is called Unicast, Multicast and Broadcast.

During unicast traffic, data packages are sent from one source to exactly one receiver. This type of transmission probably applies to most data that is sent. Broadcast data, on the other hand, is sent to all connected participants on the entire network in the form of a circular. A broadcast is primarily used when the address of the receiver of the message is still unknown. Each receiver of a broadcast must first of all accept the message in order to then decide whether the message is relevant to it.

Between the worlds of unicast and broadcast, there is occasional desire to send the same data package to several selected receivers. A clear case for multicast. It finds it use, for example, within the framework of IEC 61850 in horizontal communication between the individual participants. Here, multicast telegrams are used to cyclically transmit the state of information. When there is a spontaneous change, the new status of the information is immediately transmitted to all participants. The transmission is then repeated in millisecond intervals.

Dispatch Packaging

All data that is transmitted via Ethernet is packed in a so-called frame. The data is bundled up together with more information and is sent on its way. One such frame consists of a preamble, the destination and the source address, the type, a checksum - and of course the actual user data. A little picture makes it clearer.



It´s a frame: The user data is always accompanied on its trip. (Abb. vorl.)

The preamble identifies the beginning of a frame. The receivers can differentiate the individual frames from one another in this way. The type designates the protocol used, in our case, the IP protocol. By means of the checksum (CRC), the receiver can recognize possible transmission errors. Part of the frame is also the source and of course the destination address of the data. More on that in the next section.

Identification

As long as frames are sent within its own network, the sender addresses the packets with the MAC address of the receiver. As soon as the participant of another network is to be addressed, however, addressing is done via the IP address. None the less, in our case, we require the IP address even within a local network. Through the IP address we can then make contact with the communication module via a web browser. You do this, for example, in order to query important information. But let's first take a closer look at the individual addresses.

World-renowned

A good address has always been the most important thing for the start of a successful relationship. And who wouldn't like to be famous all over the world. Many a network component already has it easier in this respect because they are well-known right from the beginning. The **MAC address** makes this possible. This address, to prevent any possible misunderstandings, has nothing to do with the noted designer computers (and by all means not with something to eat). MAC stands for Media Access Control and regulates the unique access to communication hardware. This address is permanently stored in practically every network component and uniquely identifies it worldwide.

"Practically" because there is one exception: If a certain component is never actively involved in network communication, it doesn't need to have a MAC address. (That doesn't mean it's forbidden.) Examples of this are repeaters, hubs and simple switches, as long as they don't have any management or monitoring functions.

You cannot change MAC addresses (at least not easily). Officially, you only have a reading access to the MAC address because the manufacturer assigns this address to a component. And even he can't just produce any address out of the blue but must purchase a dedicated MAC address space. You will find out what important role the MAC address plays, when we talk about the individual components of a network communication in the next chapter.

Local Hero

The **IP address** is the identification of a device that takes part in communication via Ethernet. This identification must also be unique. However, this uniqueness is not as far reaching as with MAC addresses. Each IP address may only be assigned once within a network. Within two different networks which could also be networked with one another, the same IP addresses are definitely allowed.

The need for uniqueness within a network is true for all devices that actively take part in communication, which means to say, that have to be addressed in any way, shape or form, and be it only for diagnostic purposes. Otherwise, hard to localize network errors could occur and who needs that.

Unlike the MAC address, the Administrator himself must make sure that the IP address is unique. Unless of course there is a so-called DHCP Server on the network. This server automatically provides all participants with correct IP addresses. There's just one catch: networks according to IEC 61850 do not work with a DHCP Server. For that reason, we won't go into the topic in this book.

A Closer Look at the IP Address

We would now like to look at the structure of an IP address, more exactly, an IPv4 address. In other words, a fourth generation address.

Apartment Complex

IP addresses of the fourth generation are written in four blocks separated by decimals. An example: 207.142.131.235. Each block represents eight bits, whereby a value range from 0 to 255 exists for each block. An IPv4 address is therefore a 32-bit construction that can describe a maximum 4,294,967,296 unique addresses.

Semi-detached

If you look at it more closely, an IP address contains two addresses: one for the participant and one for the network in which this participant is. For example: in the IP address 197.255.255.89, the first three decimal blocks 197.255.255, could represent the network address.

The last decimal block, in our case, 89, would then be the address of the participant. A colleague in the same network could then have the IP address 197.255.255.13 for example. The network address is, of course, the same one; the 13 is the address portion of the participant.

Three Class Society

The example shown corresponds to a Class C address. In a network of this class, 2^8 = 256 participants can theoretically be addressed. In practise, though, it is only 254, since the address portion 0 identifies, along with the other three decimal blocks, the network itself. And, the address portion 255 is reserved for a so-called broadcast, as we already described earlier.

In a Class B network, the third and fourth decimal block are available for addressing a participant. As a value, this means 2^{16} - 2 = 65,534 maximum participants. For a Class A network in which the last three decimal blocks are used for participant addressing, this results in 16,777,214 different addresses following the same calculations.

The first decimal block reveals which class an address belongs to: If the address begins ...

- ... with 1-128, it is a Class A address,
- ... with 129-191, it is a Class B address,
- ... with 192-223, it is a Class C address.

The division into classes has an historical background. In the beginning of computer networking, the address room of 32 bits seemed to cover a vast space. To perform the search for the receiver of certain data within an acceptable period of time, a router first of all only evaluated an address based on the network portion - for the computer technology of the time quite a simplification.

If you take a look at the Internet today, it not only becomes apparent that the 32-bit address room is too small but also that the 3-Class scheme is too rigid. Today, network addresses for Internet traffic are allocated to Internet providers in consecutive address blocks. The subdivision into individual classes has become obsolete here.

Private Sphere

The class concept, however, is still a clear identifier in the configuration of local networks and can continue to be used without having a bad conscience. There’s a good reason for that because from each of the Classes A, B and C, an address area has been identified as a so-called private area. Addresses from such private areas are not procured from any router on the Internet. This means then that your local network can be connected to the Internet without provoking conflicts. Here are the facts:

- Private address range Class A: 10.0.0.0 - 10.255.255.255
- Private address range Class B: 172.16.0.0 - 172.31.255.255
- Private address range Class C: 192.168.0.0 - 192.168.255.255

Interesting for you are the areas in the Classes B and C with 65,534 and 254 addressable participants.

If you decide to make use of the Class C, it may at first be the more transparent version. This supposed advantage will, however, quickly become a disadvantage when, for example, an expansion is at hand. Then, the existing addresses will not be sufficient. The result then will be that you will have to set up a second network and interconnect the two networks via a router. If expansions are therefore on the horizon or the number of required addresses are already hitting the limits then you are better off to go straight to Class B.

But even if you couldn't in your wildest dreams imagine making use of this amount of available addresses, this class has its advantages. In this version, you can design the address structure much more transparently. For example, you could use the third decimal block to separate field and voltage levels in the participant's addressing from one another. Details to this in Chapter 5.

Interconnecting Several Networks

One thing that certainly doesn't count as a traditional entry-level task: the configuration of communication via several interconnected networks. Still, we would like to briefly tell you about this possibility and also to talk about some of the terms that are indispensible to it.

Dividing into Lots

You structure large networks according to topological as well as organizational aspects by splitting them up into smaller networks. These are sometimes also called subnets. These subnets are independently functioning units and are not necessarily technically different to larger networks. Reasons that justify this division are, on the one hand, better administration possibilities, but also the physical spread of participants and the resulting technical framework conditions.

Showing the Way

You use a router to connect different networks into a complete network. This router then decides into which network data has to be passed. The topology of the networks plays no role in this. Of course, you can only use a router to interconnect networks that use the same protocol. If the protocols on the individual subnets are different, a protocol conversion becomes necessary. In this case, you use a gateway instead of a router.

Masked

We've already explained that an IP address is divided into two parts. The leading bits identify the network, the remaining bits address the participant within the network. The net mask supplies the information which tells where in the IP address the separation takes place. With this bit code, which is exactly as long as the IP address, the router can extract the network section and so assign the incoming data to the correct target network.

The principle is actually quite simple: All bits of the net mask set to **1** let you know that the corresponding bit of the IP address is the part that specifies the network. Similarly, the bits set to **0** identify the part that addresses the individual participant.

If, for example, the first two decimal blocks of an IP address are to represent the network part, you must define 11111111.11111111.00000000.00000000 as the net mask. The way to write this in decimal is 255.255.0.0. If only the last decimal block is intended for the participant portion, the net mask 11111111.11111111.11111111.00000000 results, or decimal 255.255.255.0. The separation between net part and participant part can naturally take place anywhere. In this respect, net masks such as this one are also permitted: 11111111.11111111.11111000.00000000.

In the meantime, a dedicated way of writing IP addresses in networks has established itself for the benefit of better readibility. In this case, the number of set bits of the net mask is added to the IP address. From 198.200.133.17 and 11111111.11111111.00000000.00000000 you get 198.200.133.17/16.

Data Flow in Ring Structures

Ring structures present us with a high degree of redundancy. That is their clear advantage. But where there is an advantage, a disadvantage is not far behind. Since all participants are physically connected to one another as a ring, telegrams tend to endlessly circle it once they have entered the ring. This leads to a data overload and this cannot be. The solution is a logical gap from which telegrams can be taken out of the network during normal operation. In this way, a ring structure works like a line when you think of it logically. When there is a physical interruption, this gap is then closed. This results in a second task that a respectable ring control must take care of. After a network path fails, it must, if necessary, redirect the data onto another path to also get this to its destination - and that, of course, as quickly as possible.

Ring Control

Two different procedures are up for discussion.

- **OSM Control**
  A smart decision would be to choose OSM. Then you could skip the rest of this chapter without another thought after you have read this paragraph. But that is not the main reason, of course. Fact is, that this ring controller, developed by Siemens AG, can hardly be surpassed in its simple application. The only parameter you have to set is to identify one of the existing switches as the master, everything else takes care of itself. The bitter pill is, however, that this technology is still not widely established. In this respect, you will only have a chance if you (almost) exclusively use hardware from Siemens. And for that reason, you will have to continue reading after all.
- **RSTP Control**
  RSTP is in use worldwide and is supported by almost all switches with ring management functionality. It is far more complicated in its handling though. In RSTP, the data flow is controlled through the assignment of priorities to the individual switches. This task is your duty and turns out to be anything but trivial. Since most of you will end up deciding for this procedure, here a some more remarks on it.

The most important is: In the manual for the EN100 Ethernet module you will find very detailed information on RSTP. For that reason we will limit ourselves here to a summary of the fundamental features.

Setting Priorities

When using RSTP, you have to set priorities - for every switch. The switch with the highest priority (in other words, the lowest numeric value) is termed the root switch. As a rule, this is the switch to which the station master is connected. All other switches are termed designated switches. Important for normal operation is that two equally long chains exist from the root switch to our logical gap. The switch with the lowest priority, in other words, the highest numeric value always acts as the logical gap in the ring. If the root switch should now fail, another switch must take on its function. The priorities that have been set serve as the criterion in the search for a suitable replacement. The switch with the next lowest priority assigned to it will have to jump in. A switch in the ring operation is also called a bridge, by the way. The switch priority therefore also answers to the name of bridge priority, which will cross our path more often.

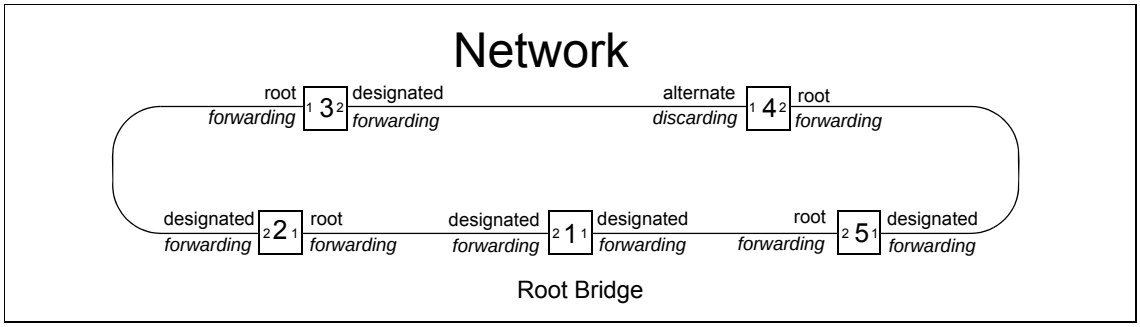
Three Procedures

Now before you begin to adjust the one or the other switch priority, we would like to present three fundamental procedures.

- **Procedure 1: Uniform priority for all switches**
  You read right, this is also possible. Because, if several switches within a ring have identically set priorities, the MAC addresses are used as the criterion. A low MAC address is then synonymous with a high priority and vice versa. And since you already learned a few pages ago that MAC addresses are unique worldwide, there can never be a priority fight. The benefit of this fast method is obvious. The configuration occurs almost by itself. If you want to add or remove switches, you don’t have to modify any settings. We shouldn’t, however, sweep the disadvantage under the carpet. Since you usually don’t know the MAC address of a switch, the assignment of root switch and logical separation point of the ring is more or less by chance.
- **Procedure 2: Define root switch (recommended method)**
  This method differs from the first in the way that you now set the priority of a switch to zero and thus define this one as the root switch. With that, you at least already have a limited control over the load distribution on the network but still not the complete control. Because, where the logical gap is located in the ring is still left up to chance.
- **Procedure 3: Set priority for (almost) every switch**
  The third method demands the most work from you, but also provides you with the possibility of realizing an elaborate redundancy concept. You define one switch each as root and as logical interruption. You set the priorities of the remaining switches according to your required redundancy. If, for example, there is a switch that is to take over the root function when there is a failure, then this switch receives the next lowest priority after the root switch. Of course, you can also define a double for the substitute. Its priority is then one lower, etc. The disadvantage of this method is obvious: when a change is made on the network, you have to reparameterize many network components.

Starring and Minor Role

The terms **root** and **designated** are not only used for the priority of the switches but also for their ports and describe which role each plays. Maybe its best to explain this with a small diagram.



The root bridge is the Number 1 in the ring.

Switch Number 1 is our root switch, also called root bridge. It is connected to Switches 2 and 3 which can jump in for Number 1 if there is an emergency. The ports of Switches 2 and 3 that are connected to the root switch are called Root Ports. Ports that are connected to the network but do not lead in the direction of the root switch are called Designated Ports. In that, the root switch itself only has designated ports, since it is not connected to another root switch (you know, there can only be one). Besides root and designated, there is still a third role, namely that of the Alternate Port. This port is nothing more than our logical gap in the ring.

Fine State of Affairs

Each port of a switch can, depending on its role, take on certain states. Of all the possible ones, two are of interest to us: Forwarding and Discarding. Root and designated ports take on the first of these two states - in other words, they forward incoming user data. The alternate port, on the other hand, finds itself in the discarding state and throws out incoming telegrams because this is its job.

The Components at a Glance

4

Our path to a successful communication is paved with a series of different components which we have more or less mentioned here and there. In this chapter, we will take a closer look at each of these required blocks. They are:

- The Switch
- The EN100 Communication Module
- The Time Server
- The Network Card

The Switch

While you can easily connect two participants directly to one another via a cross-connect cable, adding a third device will be rather cumbersome. So that this device doesn't feel like its quite superfluous, you require a distributor.

Mail Distribution

An intelligent approach is required when it comes to the distribution of data; fair distribution is always better than giving everything to just one while the others are left high and dry. For that reason, we don't choose terminal blocks or hubs but switches instead.

The switch is an intelligent data distributor to which several devices are connected in a type of star coupler. The connection of the devices to the switch is always a point-to-point connection.

The switch takes care of the management of incoming and outgoing messages. Unlike a hub which distributes the available bandwidth diplomatically in equal portions to the existing connections, a switch proceeds much more application-oriented. For that, all ports of the switch are connected to one another via an internal high-speed bus. True network professionals also call this a backplane. This bus is required so that the data packets to be received and to be sent can get quickly from one port to the next.

Good Times, Bad Times

What is also crucial is that the individual ports can receive and send data independently of one another. If the switch receives more data than it can pass on because of the current network load, it stores this data in a buffer and sends it on time-delayed.

If our switch receives data that is meant for several addresses, that is no problem either: it transmits this simultaneously via the individual ports to the different receivers.

But it can be even better: In the so-called full-duplex mode, the switch can send and receive data simultaneously to and from one and the same port. Then there are practically no more collisions for the affected port and the speed can theoretically be doubled. You should, however, keep in mind that the mode and therefore also the possible speed to each port can be 'negotiated' independently.

This all sounds pretty good. But as we don't want to pay homage to the secret weapon "Switch" indiscriminatingly, we have to mention one thing: where a hub mercilessly passes on an incoming telegram to all connected participants, the switch must first of all determine the receiver in order to precisely pass on the data. This may save bandwidth, but it costs time. For that reason, the switch makes use of one small management trick.

Management Trick

In Chapter 3 you learned that the MAC address is used to identify a participant within the local network.

Notes in the margin: There are participants which can receive but cannot send. Such participants would always stay outside following the principle given, since the switch would never register them. For these species, a MAC address can be entered in the switch and associated with a specific port.

As soon as a participant logs onto a port of the switch for the first time, its MAC address is (logically) associated with this port and this relation is stored in a table. When there are incoming data packets, the switch compares the target address with the stored relations and can, in this way, determine the required port.

Data is therefore passed on in this manner as quickly as possible and in the ideal case only to the port at which the receiver is actually located. Of course, it could happen, that no relation to a port is stored for a target address. The target address is therefore unknown. The data is then passed on to all ports with exception of the source port. This is true, naturally, also for broadcast data, for this behavior is desired in this case.

Return to Sender

What if the ideal situation is not the case? If, for example, the line is interrupted, the packets would continue to be given to a port even if there is no longer a receiver behind it. There are some mechanisms in place to deal with this situation.

First of all there is the so-called aging time (Maximum Aging Time), which, unlike that of a human, can easily be adjusted using software. With this time, you define how long the switch is to believe in a solid relationship between a MAC address and one of its ports. Or to put it another way: If the switch doesn't detect any connection and data activity for a stored MAC address within the aging time, it erases the address including its relation to a port from its internal table.

If a device is removed from a port and connected to another one, then this aging time disappears before the device is addressed on the new port. This may be sufficient for exactly this described case, but for a line break during normal operation, a faster change over is surely more desirable. For that reason, the aging time is superimposed by a further mechanism: Far End Fault Indication, in short, FEFI.

If this switch function is activated, the aging time is simply ignored when there is a line break. The associated MAC address falls victim to an immediate amnesia and the change over to an alternative path takes place in the shortest possible time.

Out of the Way, Here I come

A speciality of IEC 61850 is GOOSE telegrams. GOOSE stands for Generic Object Oriented Substation Event. With these telegrams, devices can communicate directly with one another. Usually they are time-critical messages that one device must send to another. Therefore, the switch must not act as a brake shoe but has to handle such telegrams with priority. The expert talks about a prioritization of GOOSE telegrams. For our purposes, we absolutely require switches that have this performance characteristic. Such switches have one processing path for telegrams that have a normal priority and one processing path for telegrams with a high priority. The switch evaluates the priority field of an incoming telegram and, depending on the priority recognized, pushes the data into the one or the other path. While the normal telegrams have to go to the back of the line from time to time, the privileged are processed into their path almost immediately.

Variations of the Game

For all, who are still interested in how a switch basically passes individual telegrams through, we will describe several variations that differ with regard to their delay time and error recovery.

- **Cut-Through**
  No new haircut, but the fastest of all methods although also the most trivial. The switch only takes a glance at the target MAC address of the incoming frame and sends the frame on accordingly. No sign of error check but therefore practically timeless.
- **Store-and-Forward**
  The purest of all methods is, at the same time, also the slowest. Within the framework of an initiative for a clean network, the switch checks each incoming packet for possible errors. Faulty frames don’t have a chance and are rejected without replacement.
- **Fragment-Free**
  If the truth is really somewhere in the middle, then this would be the method of choice: It is faster than Store-and-Forward, and more hostile than Cut-Through. It checks whether a packet has the minimum length of 64 bytes as required by the Ethernet standard. If yes, it immediately sends the packet to the target port. If no, they are obviously fragments of a collision that can be rejected without a thought.
- **Error-Free-Cut-Through / Adaptive Switching**
  A different opinion says: The correct mixture makes it. And that is why this one is probably the best method, although also the most complicated. The switch first of all works in the **Cut through** mode. It sends one frame on its long voyage via the correct port without looking at its origin and background. It does, however, keep a copy in the memory through which it calculates a checksum.

If this doesn't match the one in the frame, it cannot call the defective data back but, with the help of an internal counter, it makes note of the error that occurred. If too many errors occur within a certain, usually very shortly set timespan, the switch changes over to the **Store and Forward** mode. When the error rate once again falls below a permittable limit, the switch goes back to working in **Cut through**. Moreover, the switch can change over to the the **Fragment Free** mode from time to time when too many fragments with a length of less than 64 bytes arrive.

In Care Of

The described methods require, of course, different hardware designs that ultimately differ due to the number of buffers.

- **No buffer**
  In switches without buffer, only two ports can be logically connected directly to one another via the internal bus at any one time. Data that is present at a third port at the same time already delays the data transmission. This type of switch merely masters the cut through method and is not suitable for commercial purposes.
- **One buffer for all**
  Not exactly luxurious, but already better, is one common buffer for all ports. The participants place their data in the buffer while the switch prepares the connection to the other participants. This results in a decisive advantage: If several participants want to send data to the same port, these are first of all stored and then transmitted as a bundle.
- **One input and one output buffer for each port**
  The luxury solution offers you the maximum possible storage. This type of switch can intermediately store several telegrams and at the same time establish connections to several port pairs. In that way, participants A and B can communicate with one another while C and D are also gossiping.

It's a Tough Decission....

The question that we must ask ourselves is: Can ANY switch be used for communication via Ethernet? After all, switches come in a price range from 40 euros up to 2000 euros. As an answer to this there is only Yes and No.

For a simple connection between two PCs and a printer, a cheap solution from Company XYZ is more than sufficient. If, however, you would like to get a stable handle on time-critical procedures within the framework of IEC 61850, the demands are considerably higher. You have already become familiar with several distinctive characteristics. Here are some tips:

- Use switches with input and output memory for each port; this enables an almost delay-free passing through of telegrams and increases the speed during data exchange to a maximum.
- Make sure you have a stable voltage supply. The optimum would be the possibility to connect the switch to the existing auxiliary DC voltage that you also use to supply the protective devices.

- Very important: Switches that are used in electric power installations must comply with the applicable EMC regulations.
- Switches that you use in conjunction with IEC 61850 should, without fail, support the prioritization of GOOSE telegrams.
- The switches used in ring management must absolutely support FEFI.
- Insist on administrative comfort features such as the possibility of network monitoring through SNMP.

To sum it up: As a rule, you won't find the switch of your choice at your nearest IT discounter. Against communication problems, we recommend switches by RUGGEDCOM or Hirschmann. We have made many tests with these and have gathered positive results.

The Communication Module

We all know: Without the right contacts, nothing goes forward; that's true for life and rightly so for technology. With "right contact" we mean the system interface on which the EN100 module is mounted. The EN100 module makes sure that orderly communication according to IEC 61850 takes place via Ethernet

You will find an extensive description on the EN100 module in a separate manual. You can also download it as a PDF file from the **www.siprotec.com** website. Right here, we'll give you a short summary.

From 0 to EN100

The EN100 module not only provides us with the appropriate physical interfaces for a proven connection to the network. On it is also the complete logic and the protocol for the IEC 61850 standard. For you, this means that you are by no means on the outs if you've already had a SIPROTEC 4 device in your possession for a somewhat longer period of time. With a firmware update to Version 4.6 or greater, you can bring many a device up to par and mentally prepare it for installing an EN100 module. You can find out whether your device is suitable for this rejuvenation by contacting your Siemens partner directly. Right now, we will continue with an overview of the individual EN100 module versions.

Fraternal Twins

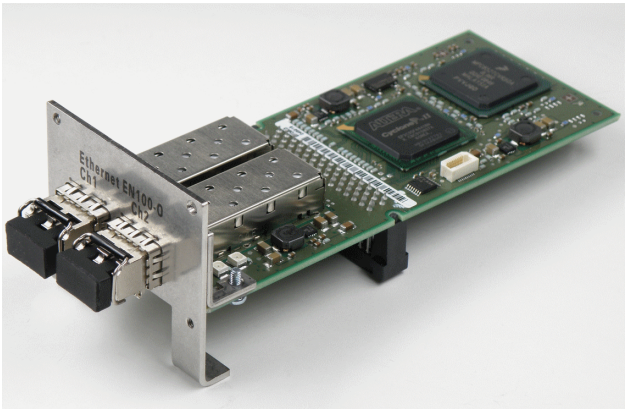
Siemens supplies you the EN100 module fitting to an electric-based or also an optic-based topology. The electrical connection version of the module is for built-in and surface-mounted housings. For devices in the built-in housing, an optic version is also available. To be sure, all versions are suitable for a 100 MBit network. Electrical signals are directed via RJ45 connectors; light clears its path via Duplex-LC connectors in professional metal design.

One thing is common in all designs, the physical interfaces exist twice. In the picture to the left this is easy to make out. Nevertheless, only one of the two interfaces is always active; the other is passively monitored. If the active interface is faulty, the change over to the interface that was passive up until now is automatically made within a few milliseconds. With this feature, which is officially termed **Line** mode, you can easily build up redundant structures in conjunction with external switches.

Double the pleasure: The physical interfaces of the EN100 are there twice

Both physical connections are monitored internally in the device. When there is an interruption, an appropriate indication is generated and stored in the event log buffer. Through parameterization you then easily route these, for example, to contacts, LEDs or CFC.

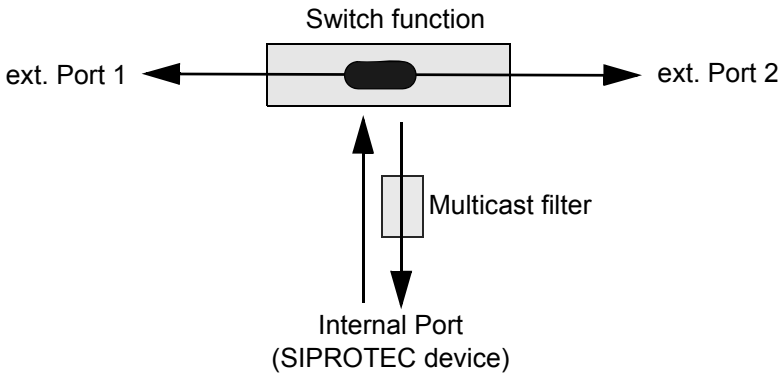
If you decide to use EN100 modules in the optic version, you kill two birds with one stone. For, this version has an additional switch on board, which allows you to use the two interfaces to also pass on signals. The **Switch** mode is then also the standard setting for the optic module. You only change this if the module is to operate in the line mode. The integrated switch is then automatically turned off.



Naturally is it an optical goody, too: The physical interfaces of the EN100-O are protected

Bosom Buddies

The switch function works as a link between the device and the two interfaces. In this way you can easily implement a ring topology, just as we described in Chapter 2 and save youself external switches, at least in the connection of SIPROTEC 4 devices amongst themselves.



Well integrated: The optic module has a switch function.

In principle, it is a switch with three ports. One is permanently connected to the MAC (Medium Access Controller) of the processor. Via the 2 other external ports, the device is integrated into the network. Since telegrams of all sorts hustle about on these, in other words, unicast, multicast or broadcast, each of these telegrams pass at least one external port and are then handled properly.

- **Unicast Telegrams ...**
  ... in other words, those that are meant for only a certain SIPROTEC 4 device, are only then passed on to the internal port if they are addressed exactly to the current device. And that's where it stays; it is removed from the telegram traffic. If the telegram, however, is not aimed at the current device, then the communication module is not further interested in it. It passes this telegram directly on to the respective other external port. The communication module inserts unicast telegrams that the device sends itself into the data flow via both ports.
- **Multicast Telegrams ...**
  ... are always meant for several receivers. In the cross-communication between the individual participants there is still another oddity. Multicast telegrams are repeatedly sent in the space of a few milliseconds to all participants when an event occurs. This means a high load for each receiver, even though the telegrams are quite possibly not meant for it. For that reason, a multicast filter is integrated in the receiving direction of the internal port. This actually only lets telegrams pass that have the address of the respective participant. Regardless of everything else, multicast telegrams are always passed on to the repective other external port of the communication module.
- **Broadcast Telegrams ...**
  ... are aimed at all participants. For that reason, the communication module passes these on to its internal port and also on to the respective other external port. Broadcast telegrams only occur in IEC 61850 networks if one or several other protocols are used on the same network. We strongly recommend not to do this.

PS

Two facts that we do not want to leave unmentioned here:

1. In conjunction with optic EN100 modules, you can set up rings with a maximum of 30 devices as long as you only use one external switch within a ring. With two external switches, the number drops to 27. The following formula lets you check whether the calculation works out in your specific case:

   Number of SIPROTEC 4 devices + 3*number of ext. switches < 34

2. The EN100 module should not be configured as the root switch if at all possible, since beyond the logical separation point the entire data traffic would otherwise run via this module. We recommend that you always use an external switch for this purpose. This is also the case for the replacement switch that is to fill in as the root switch in an emergency.

Time Server

Everything is a question of time; more accurately stated - the correct time. That the system time and date on your computer is incorrectly set, for example, can be easily recognized by different symptoms:

- According to the date, you haven't been born yet.
- Your e-mails arrive at the recipent earlier than when you sent them off.
- You leave your desk much too early every day.

While, as a rule, we're talking mostly about uncritical events in the above, a correct system time in all system structures is almost indispensible. As such all SIPROTEC 4 devices, just like IEDs of other manufacturers, have to synchronize on a uniform time basis in order to guarantee the recording and documenting of events at the correct time. For this we require two things: a) a reliable time source and b) a mechanism that makes this time available to each participant. As a trustworthy time source we make use of a time server and the mechanism is called NTP: Network Time Protocol.

It is Served

Let's first worry about the time server. We recommend an NTP-capable hardware time server such as the ones the Company Hopf and Meinberg, for example, offer in various versions. One such time server feeds in its UTC time at some point in the network. So that this time is always correct, it obtains a radio time signal, for example GPS, with which it can synchronize its own time.

Notes in the margin: To synchronize other devices to the same time, the time server itself doesn't necessarily have to be synchronized. Each participant can therefore only assume that its other colleagues use the same time; no participant can judge whether this is fundamentally correct.

In addition to NTP servers as a stand-alone device, you can also fall back on software solutions in conjunction with an industrial PC - or even get the time signal from the Internet. We categorically advise you against this second possibility, for it is safer to set the time according to your watch. Internet-based time information is completely beyond your control. You can neither judge the quality of the supplied information nor can you guarantee its constant availability. Even software solutions cannot be recommended without restrictions; at least systems that operate under Windows are not capable of supplying constantly correct results exactly to the millisecond.

Our summary: For those of you where an exact and stable time in a network plays an important role for safe and smooth execution, for you there is no alternative to your own time server.

Keeper of the Protocol

A time server alone is of no use. Only in conjunction with the Network Time Protocol do things start to roll. NTP is based on the Client/Server principle and has essentially two fundamental tasks:

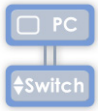
1. NTP must coordinate the distribution of time information from one or several time servers to the existing clients so that all clocks in the network always coincide with regards to a reference time.
2. NTP must synchronize the clock frequencies of server and clients so that these always tick rhythmically.

To make the principle of the NTP protocol clear, we once again reduce it to its basic method of operation. The client sends an NTP message to the server according to the motto "Have you got the time for me?". The server takes this telegram, exchanges some information here and there, and sends it back to the original sender, in other words, the client. The client

now has four time stamps available. From these four values, it calculates the difference between the reference time to its own time. This delta is then the value by which it must correct its own time.

Stand Pat

To synchronize the time-of-day, different procedures can be configured in DIGSI 4, even in conjunction with the EN100 module. This multitude of choice may have its justification for a “normal” communication via the office Ethernet. But, for communication according to IEC 61850, synchronization with the help of NTP is the only officially released method.



Notes in the margin:
A device can also be synchronized by supplying it with time telegrams via Port A. However, this requires additional wiring and that’s why NTP should be given preferential treatment.

For this, you must keep the following in mind: All absolute times stored in the log buffers of a SIPROTEC device are local times.

The EN100 module converts these local times into the UTC format (UTC = Universal Coordinated Time) required for IEC 61850. The greatest problem is the changeover between daylight saving time and standard time that is usual in most countries. As such, after the changeover from daylight saving time to standard time we have, for example, the time 2:10 twice.

So that the module can convert the two local times into the respective correct world time, it requires the information as to whether it is daylight saving time or standard time at this specific moment. Next to NTP, only DCF77 supplies this information; IRIG-B, internal time guidance, minute pulse and others don’t. So once again our emphatic tip: Stick to the type of time synchronization specified by IEC 61850, the NTP.

Network Card

Only a PC makes your network topology complete. Whether the handy Notebook, the office desktop for daily usage or a full-blown industrial PC, for the connection to the network, you require a network card in all cases. What shape this concretely takes is ultimately decided by the individual need for security through redundancy.

For the occasional remote querying of data from a SIPROTEC device, a standard card in the office PC may now and then be sufficient. But, the station automation, for example with SICAM PAS, can hardly afford to be absent from the network. That is why redundancy is also called for in network cards.

Team Spirit

In principle, you could also realize the required redundancy with two separate network cards in one PC. Much more elegant, however, is the use of a dual-port card, such as the Intel®PRO/1000 MT. Such a card has two independently working processors that are also accessible via separate ports and their own IP addresses. As such, they could also be connected with two different, independent networks.

Much more important insofar as redundancy is concerned, is for us however, that both adapters can be virtually united and can be addressed with a common IP address. This method is called **Teaming**, in other words, the network card is teaming-capable. Of all the possible operating modes of such a card, we want to talk about the two that are relevant for us.

More Tolerance

The picture to the right shows the connection version for the **Adapter Fault Tolerance Mode**. During normal operation, the communication flows over the first adapter of the network card. As soon as this, the cable to the switch or the switch port fails, the second adapter takes over the connection. The PC continues to be connected to the network. In the mode described above, however, the light goes out for the PC as soon as the switch fails. With the Switch Fault Tolerance Mode, you also get a handle on this problem. The picture to the left shows that the two adapters of the network card are connected to one switch each. Even the two switches are connected to one another. What is true for the Adapter Fault Tolerance Mode is also true here. In addition, the failure of a complete switch is now also redundantly secured. In such a failure, the network card automatically changes over to the other adapter.

Sample Configuration

5

In this book, we don’t want to hand over any phony numbers, but solid, concrete facts. For that reason, a simple, but completely application-oriented configuaration is to be the basis of our continued explanations.

In our example, we have tried to join the technologies and components shown until now to make a whole picture that makes sense. This example can therefore also form, with a few expansions here and there, the basis for your own first network structure.

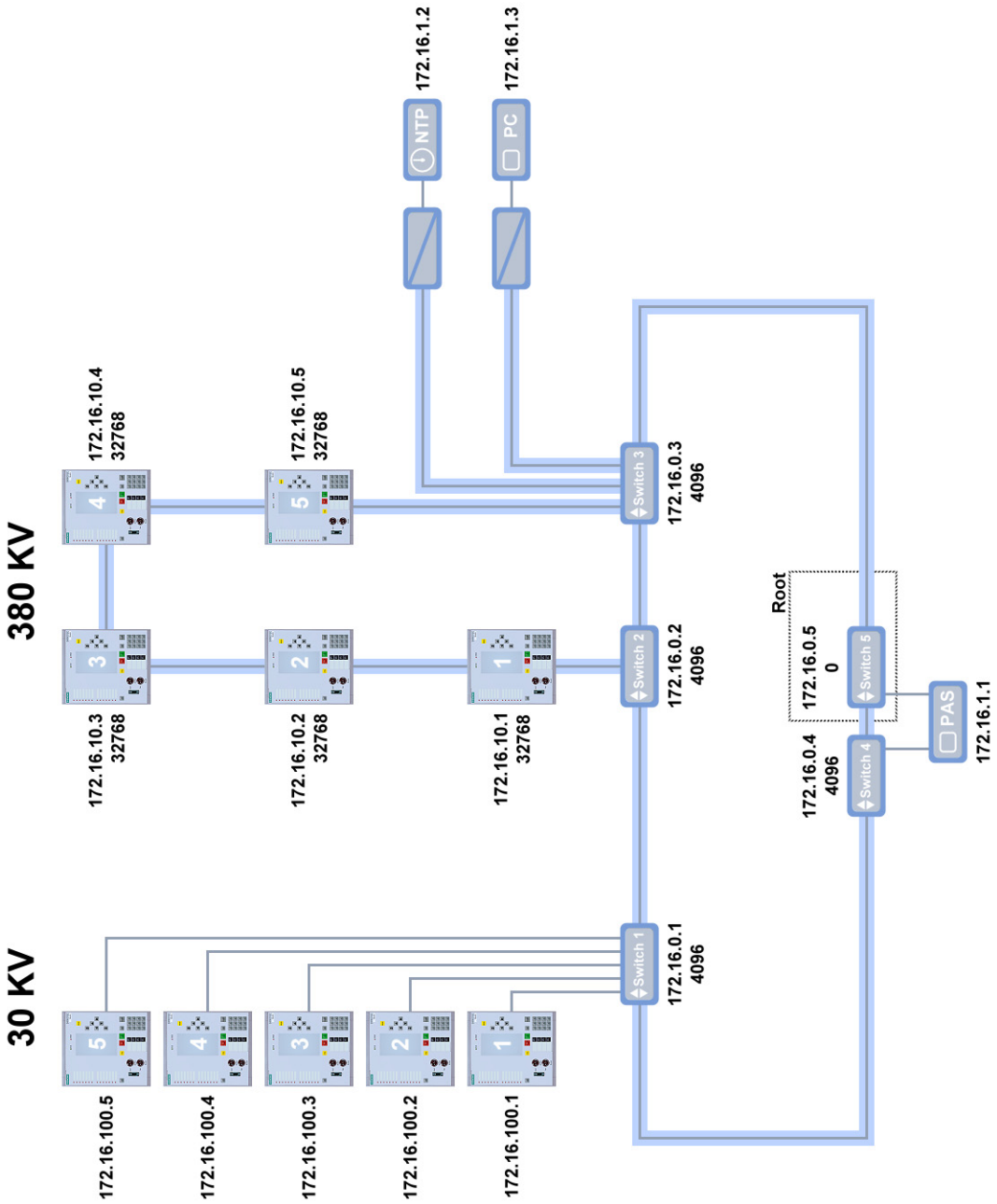
Topology

Let’s first look at the topology of our example. You’ll find a picture of this on the next page. On the left-hand side you’ll see five protection devices for the 30 KV level. These are connected to a switch in the form of a star. Since the devices are not to be located far apart from one another, cables of maximum 20 meters length are sufficient for the connection between device and switch. This is the upper limit of the cable length for an electrical connection and for that reason we decided to use it in this case. The SIPROTEC 4 devices are therefore equipped with electric Ethernet modules.

Another extension shows the 380 KV level. A fiber-optic cable connects five devices, that are equipped with optic modules, together to form a ring. The ring is closed through two switches and is not only redundant with regards to the connection of the devices amongst themselves but also the connection to the main ring is further secured should one of the two switches fail.

The main ring connects the star structure of the 30 KV level with the ring structure of the 380 KV level and also provides the interface to an automation system, in our case SICAM PAS, at the same time. Even this is redundantly designed with two switches and a teaming-capable network card in the industrial PC.

The NTP server also redundantly injects its time signal via Switches 2 and 3 - converters produce the transition from electrical signal to light information. We use one converter to connect a PC with DIGSI 4 on board to Switch 3. In the process we forego redundancy - the events are usually not time-critical so that it is possible to cope for a short time should the PC fail.



One of many possibilities: Sample configuration with electric and optic cabling.

Components

As switches, we recommond the products from Ruggedcom, which we are also using for our sample configuration. Switch Number 1 for the star-shaped connection is an RS 8000 T. This comes with six electrical and two fiber-optic connections. With it, it even provides an electrical port as a reserve for possible expansions and, through its two optic interfaces, it can easily be integrated into the main ring.

Switches 4 and 5 are also of the same type, by the way. Of the six electrical ports per switch, only one each is used however in order to connect the teaming-capable Intel PRO/1000 MT onto the network. This provides you with all sorts of leeway, in order to, for example, integrate a second industrial PC with installed SICAM PAS. With that, you would then achieve complete redundancy even on the automation level.

The IEDs of the 380 KV level connected as a ring are redundantly integrated into the main ring with two switches of the type RS 1600. This type only has optic ports and is predestined here for that reason.

The sign of the times expects, for example, a Hopf GPS System 7001 to be used. In the 19” rack of this modular system there is, next to the power supply and the LAN card, room for several time servers in the form of individual plug-in cards. Alternatively, the station control system, in our case a SICAM PAS, could also take on the function of time server.

IP Addresses

If we take a look at the number of protection devices, switches and other components, then two hands and two feet are enough to count them. The address space of a Class C network with its 254 addressible participants would be more than sufficient to uniquely identify each participant and beyond this would still offer ample room for expansions. Nevertheless, we have decided to make use of the private Class B network 172.16.x.x (Net mask 255.255.0.0).

The reason for this is simple: Through the additional third decimal block, that is available in the Class B network, considerably more opportunities for a structured addressing are presented. That way, we can assign IP addresses for protection devices based on voltage, for example. Even individual component types, such as switches, are immediately identifiable as such, based on their IP address when they are cleverly divided up.

Bridge Priorities

In the picture of our sample configuration, you will find in each case, the priority of a participant underneath the IP address. Should the individual numerical values be a mystery to you, here is the solution: The value 0 identifies the highest priority, all other priorities are graduated by the fixed value 4096. This results in a series of fixed priority values: 0, 4096, 8192, 12288, 16384, etc.

As root, we have chosen Switch 5. For that reason, it receives the highest priority, in other words, the value 0. Switch 4, right next door, is to take on the job of root switch if there is a failure. Its priority therefore lies one level lower and that corresponds to the value 4096. We will also give this priority to the rest of the switches in the main ring, by the way. The teaming-capable network card in the PAS will nevertheless make sure that Switch 4 takes over in case of an emergency.

As far as the logical separation point, the alternate port, is concerned, we will not commit ourselves further. We will simply assign the priority 32768 to all optic EN100 modules.

Creating and Structuring a Project

6

In spite of the expansion by IEC 61850, configuring with DIGSI 4 remains as easy as always, even if a few more moves are necessary here and there. We must assume at this point, that you are familiar with DIGSI 4. If this isn't the case, then we recommend that you go through **DIGSI 4 - Start Up**, an introductory course of a compact 60 pages. Of the same distinctive scope is **Ethernet & IEC 61850 - Start Up**. In it we describe, on the basis of a simple example, among other things, the cross communication between devices, also called GOOSE, that we will completely pass over at this point.

Sequence

In this chapter, we will explain the following steps as they are related to our sample configuration:

- Step 1: Create project
- Step 2: Insert SIPROTEC 4 devices
- Step 3: Insert IEC 61850 station
- Step 4: Enter devices as participants in the IEC 61850 station

Creating a Project and Inserting Devices

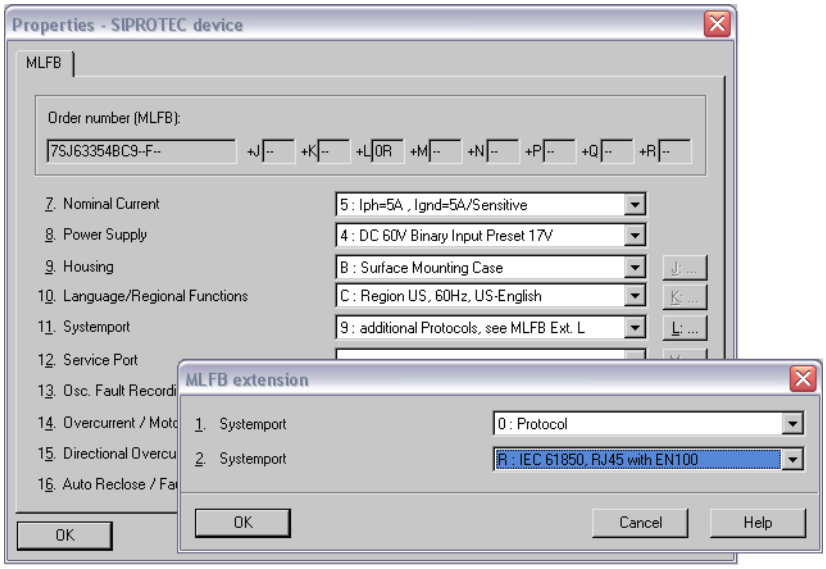
For our example, we will create a new project. This does not mean to say that you may not integrate an IEC 61850-conforming communication via Ethernet into an already existing project. It goes without saying that devices with different protocols or that use different transmission paths for communication can be included in the same project and thus in the same system. However, these devices simply cannot be integrated in the communication according to IEC 61850.

First You Take

In our freshly-baked project, the first thing we do is insert two folders so that we can differentiate between the two voltage levels 30 KV and 380 KV. These folders will then include the required devices. This division, though not necessary, creates order and clarity.

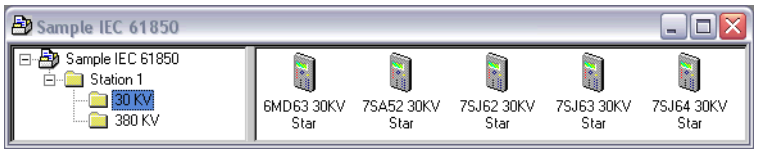
For communication via Ethernet and IEC 61850, SIPROTEC 4 devices version 4.6 and higher are suitable. Let's imagine you have purchased such a unit fresh from the production table and would now like to integrate it in an existing or even a new topology.

In DIGSI 4, you proceed as you always have: You insert this, just like all other SIPROTEC devices, using drag & drop from the Device Catalog into the project concerned. Before the SIPROTEC 4 device is placed in the project, you must define the device model in DIGSI 4. For this, the **MLFB** tab of the dialog box **Properties - SIPROTEC device** is displayed.

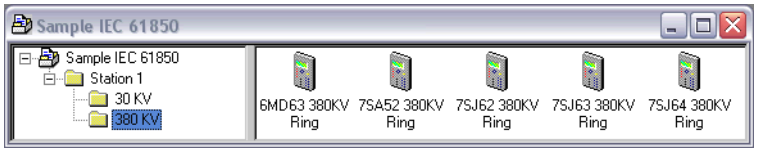


Important: Select the correct system port in the appropriate variant

From the possible settings, you select those that correspond to the MLFB of your device. For the system port, choose the setting **additional Protocols**. By selecting this, DIGSI 4 opens a second dialog with two listings. From the upper list, choose the setting **Protocol**. In the lower list select **IEC 61850** in the actual port variant - either optic or electric. As soon as you have closed both dialogs one after the other by clicking **OK**, DIGSI 4 inserts an icon for the device in the project. Once all devices have been inserted, the project should look like the following picture to the public.



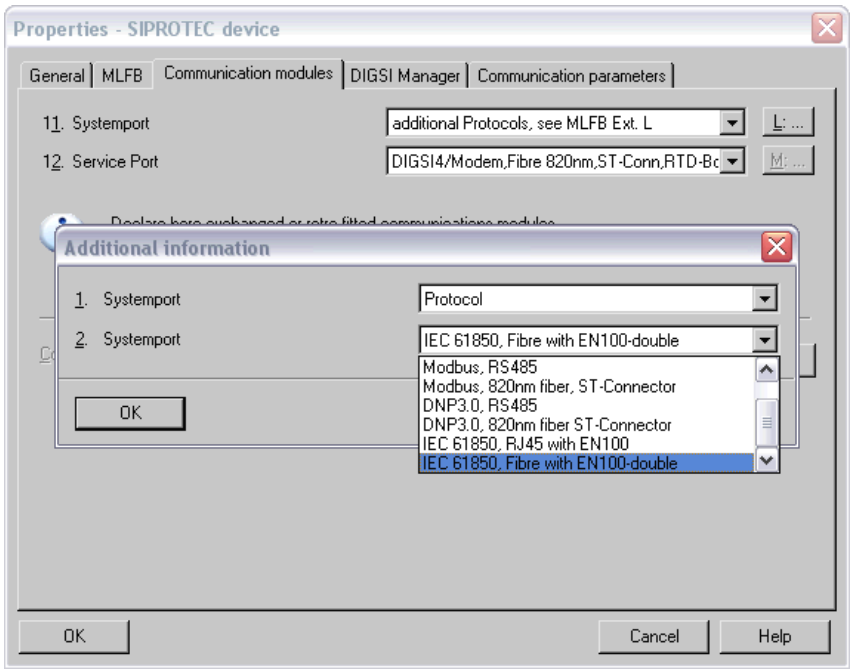
The devices on 30 KV level.



The devices on 380 KV level.

Plan B

A slightly different procedure is called for when you upgrade an existing device, have given it new firmware plus communication module. If you would like to integrate such a device in a new project, please always select the MLFB number that is stamped on your device. That is, you first select the identifying letter for the original system port. Once DIGSI 4 has inserted the device into the project, you open the Properties dialog of the device symbol and select the module **EN100** as port in the tab **Communication modules**.

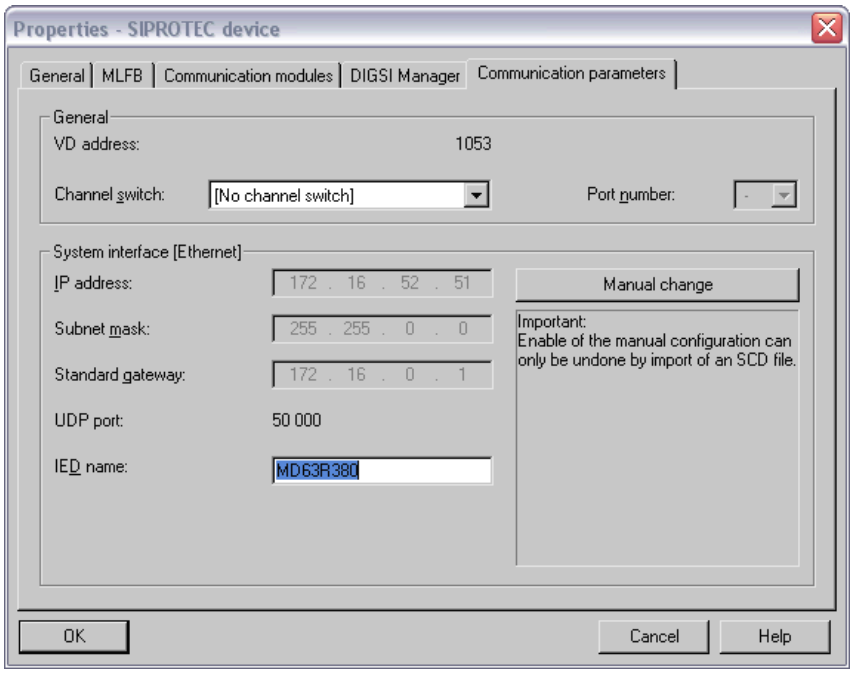


Subsequent operation: DIGSI 4 must be informed!

If the device is already part of a project, you can, of course, leave it where it is and so save yourself putting in the individual parameterizations once again. However, you must make sure that the device also has a base parameter set of Version 4.6 appropriate for the updated firmware. Otherwise, you won't even be able to select the required port variant. To do so, right-click on the device symbol. From the shortcut menu choose **Update parameter set**. If no more-current parameter sets are installed for the specific device type, you will get a message. Otherwise, the dialog box **Update parameter set** is opened. In the upper area, the version number of the currently used parameter set is displayed. With the help of the **New parameter set version** drop-down list, you select a version number 4.6 or higher and then click **OK**. Should the above-mentioned message have appeared because a more current parameter set did not exist, it is easy to get help by inserting the DIGSI Program-CD and installing the missing parameter set, that is, installing the respective device data after the fact. By the way, you will always find the most current data on the Internet under www.siprotec.com.

Name-Day

As you can see in the pictures of our project, we have given the devices informative names. Even within an IEC 61850 network, each participant requires a unique name. One such name may only consist of a maximum of eight letters or numbers, however. No 'umlauts' (modified vowels) or spaces are allowed and the first character must be a letter. Since we didn't want to restrict the considerably more permissive handling of the assignment of a device name within a project, there was only one solution: There had to be an additional name, the so-called IED name.



The IED name is part of the communication parameters of a SIPROTEC 4 device and is used in IEC 61850 as the device name

As you can see in the picture above, you define this IED name in the Properties dialog of the respective device. If, however, you're not fussy about the name, you don't have to rack your brains about it. The DIGSI Manager automatically defines a unique name. This consists of the prefix **IED_** and a four-digit consective number.

We do, however, recommend that you take the time to assign names that make sense. These will serve you well later on in uniquely identifying the participant. The IED names are not only displayed in the DIGSI Systemkonfigurator (which you will become familiar with shortly), but are also part of the telegram traffic in IEC 61850. If you plan to monitor these with diagnostic tools, names which can easily be associated are of great benefit.

For our sample configuration, we will craft names that give information on the device type, the topology (ring or star) and the voltage level. **MD63R380** tells us that we are dealing with a device of the type **MD63**, that is on **380** KV level integrated in a **R**ing.

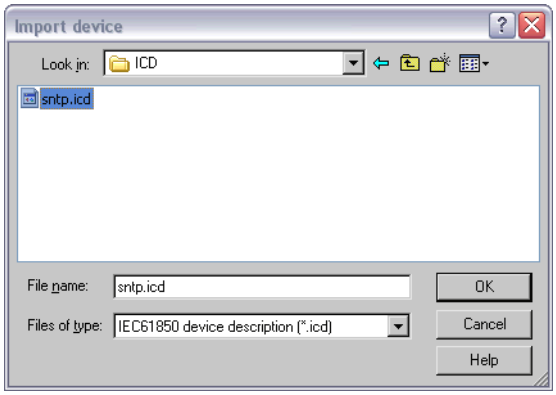
Adding a Station and Defining Participants

For a decent communication according to IEC 61850, you need a so-called IEC 61850 station.This new element in the DIGSI Manager represents a switchgear system in which all devices according to IEC 61850 communicate with one another via Ethernet. You choose which devices these specifically are, easily from a list and enter these as participants in the IEC 61850 station.

Notes in the margin:
You can basically insert as many time servers as you like in one project. However, DIGSI 4 currently only supports one time server per station. If several servers are configured, then only the one with the lowest IP address is ever addressed. The IP address is assigned to the time server later on during network configuration with the DIGSI Systemkonfigurator.

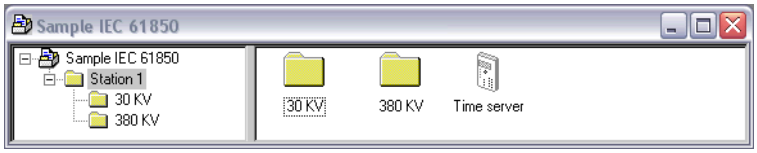
The participants are not limited to SIPROTEC 4 devices. DIGSI 4, of course, fulfills the requirements of the standard and gives you the opportunity to integrate IEC 61850-conforming devices with different functionality and from different vendors in one project. For this, you import the device description of the respective device and then add this device as a participant of the station - in the same way as you do for SIPROTEC 4 devices. We can do this right now for the required NTP server.

You will find the necessary file with the device describing data on the DIGSI Installation CD in the directory **..\Utility \IEC61850 \ICD**. In the DIGSI Manager, choose **Insert new object → Other IEC61850 Participant** from the shortcut menu. This opens a standard File dialog.



Selected ...

With the dialog shown, you select the device description **sntp.icd**. An icon for the participant is inserted in the project. This is not unlike a normal device icon, even if it is somewhat palefaced.

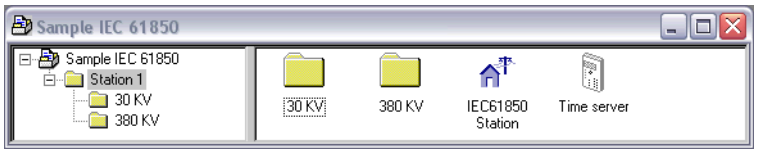


... and inserted. Inserting the time server takes hardly any time at all.

Housing

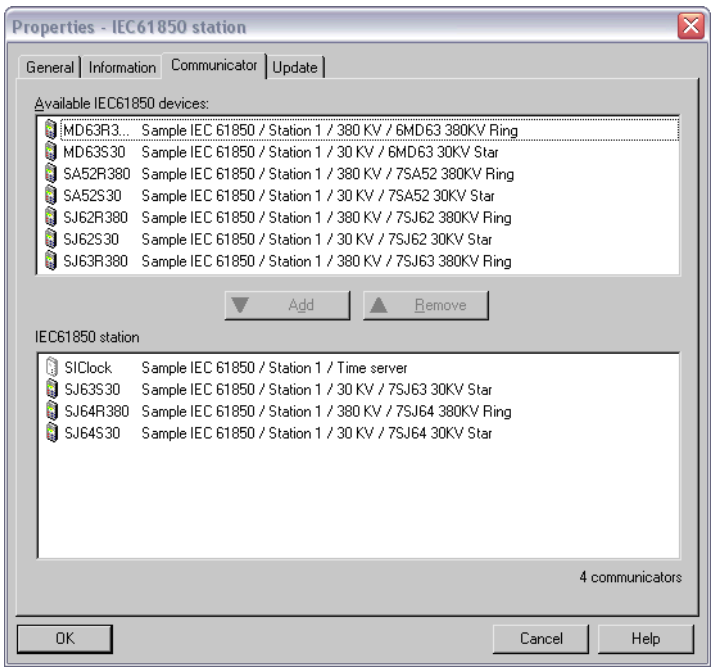
Now, we don’t want to leave our devices and the time server out in the rain any longer. Instead, we want to make sure that they finally have a roof over their heads. To do this, you have to insert an IEC 61850 station.

This is done once again with the shortcut menu, **Insert new object → IEC 61850 Station**. And voilà, a cute little house with its own powerline appears in the project.



The IEC station gives the participants a home.

This isn't enough though, for no one (except you and us) knows that the ten, in total, protection devices plus one time server are to communicate with one another within the station. Therefore, you still have to enter this hardware in the station as participants. Open the station's Properties dialog and select the **Communicator** tab.



Per selection list, you define the participants of an IEC 61850 station.

Since devices and NTP server fulfill all the requirements for an IEC 61850-conforming communication, they are already displayed as potential participants. Now you just have to accept these into the list of actual participants. This is done with a double-click on each desired name one after the other - or by multiple selection. To do this, you hold down the Alt or Ctrl key and with a mouse-click select consecutive name blocks or several individual names. You then ship the selected names to the lower list by clicking on **Add**. A quick click on **OK** and this step is also completed.

Please don't try to open the station with a double-click just yet - you won't succeed. So that this works, all participating SIPROTEC 4 devices have to have been opened once before. More on this in Chapter 8.

Parameterizing a SIPROTEC 4 Device

7

As usual, DIGSI 4 would really like to know about everything that's going on and depends on your support for this. In fact, the software requires information on the operating mode of the module, on the type of redundancy (OSM or RSTP) and on the type of time synchronization. And finally, there are still your own specific parameter settings, possibly also for communication between the individual devices. We won't go into any more detail in this book on the last two topics. On the one hand, your individual parameterization is for the most part independent of the selected communications form. On the other, there is the book **Ethernet & IEC 61850 - Start Up**. In it we describe extensively the communication between devices. About the rest - we are more than happy to give you information.

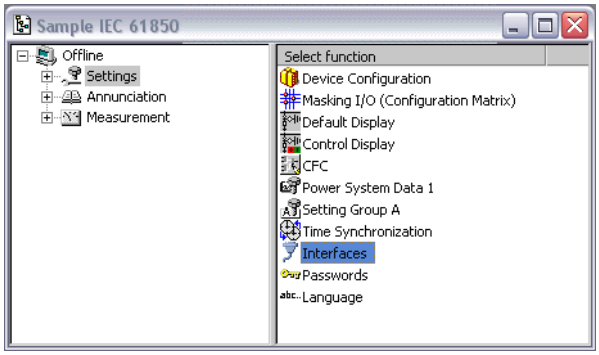
Open Says Me...

First of all open one of the devices for editing. The fastest way to do this is by double-clicking on the respective icon. We'll leave it up to you, which device you want to begin with. The first device we're going to start with is one from the 380 KV level, equipped with an optic EN100 module.

In the dialog for selecting the connection type, choose the option **Offline**. Now just click on **OK** and everything takes its course: The DIGSI Gerätebearbeitung is started, the device's data are loaded.

Setting the Interface Parameters

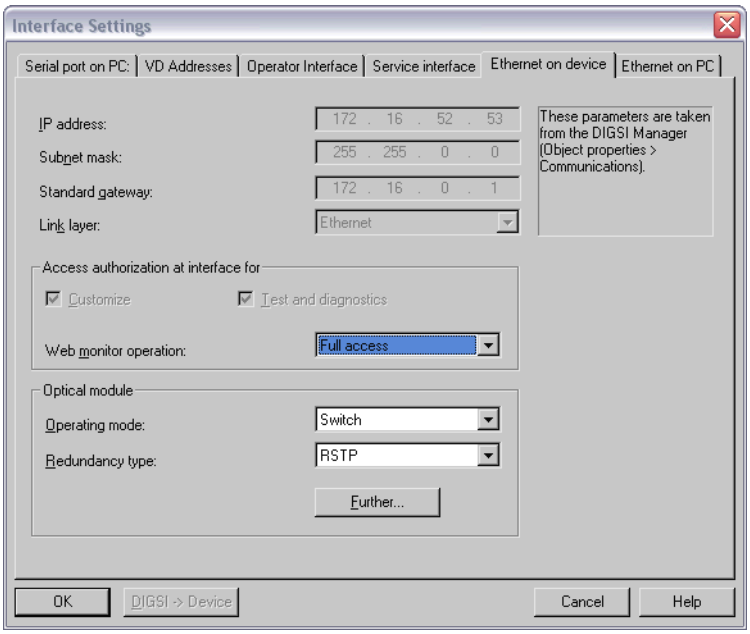
Let us begin with the Ethernet module. In the List View of the DIGSI Gerätebearbeitung, double-click on the **Interfaces** entry directly underneath **Time Synchronization** . DIGSI 4 then shows you the dialog **Interface Settings**. This dialog box contains, depending on how the computer and the SIPROTEC 4 device are equipped, varying numbers of tabs with setting possibilities for the respective interface parameters.



A double-click starts everything.

Viewing the Values

Of all of them, we are mainly interested in the parameters for the EN100 module that are summarized in the **Ethernet on device** tab. By the way, the tabs for the various module designs are all the same, but there are special parameters just for the optic interface.



Reading and writing: Not all parameter values can be changed.

The values for IP address, net mask and standard gateway merely have an informative character in the current location - you can only change these in the DIGSI Systemkonfigurator or (not fully recommended) in the DIGSI Manager. The Link layer, that describes the physical connection of the SIPROTEC 4 device to the other components is set to **Ethernet** and cannot be changed in any case.

With many of the current SIPROTEC 4 devices, you get support for commissioning, proofing and system management even without the use of DIGSI 4. The magic word is web monitoring. All you need is a web browser of your choice and you can then, for example also via Ethernet, fetch information from the device or even operate it. With the help of DIGSI 4 you define the degree of access for the web monitor operation. To do so, select one of the settings **No access**, **Reading**, **Changing** or **Full access** from the drop-down list. The last three named types of access are each protected with different passwords, by the way. Our tip: Set the access type for normal operation to **Reading**. For commissioning, we recommend **Full access**. That way, you can completely operate the device anytime from the commissioning PC.

Electrician or Optician?

With the electric Ethernet module on board, you have an easy time of it anyway because there are no other settings for it. This module only recognizes line operation and the selection of a special type of redundancy is not provided for. Things are different for the optic module.

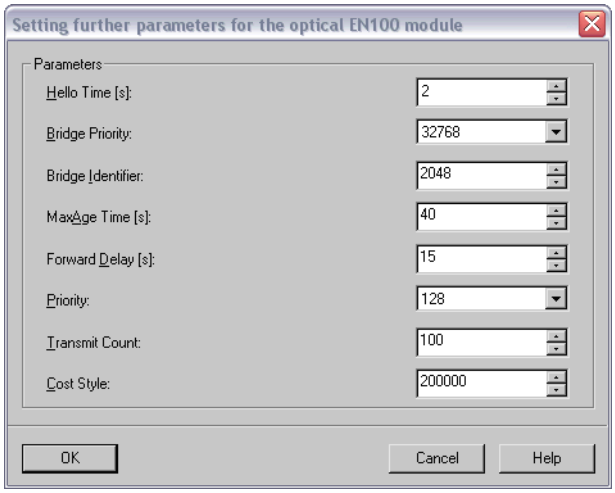
According to reliable sources (see Chapter 4), this module not only masters line operation, it can also be configured as a switch for operation in the ring.

You select the desired operating mode from the drop-down list of the same name. In conjunction with the **Line** setting**,** just as for the electric module, there is nothing more for you to do except to say “Good-bye” to the dialog box by clicking **OK**.

A Lof of Switch(ing)

For the use as switch and thus the operation in the ring, it becomes necessary for you to decide on a type of redundancy. RSTP and OSM are the two candidates. Your selection, of course, depends on which type of ring control you have already given preference to during the conception phase. For our sample configuration, it was RSTP.

For this type of redundancy a number of other settings are possible, however, they are only required in a few places. Put another way: Of the default values, you should only deviate from them selectively and on our recommendations. One click on **Further** gives you a look at the individual parameters and their settings.



Nothing for those who want to experiment: The specified RSTP settings should be retained, for the most part!

Some Good Advice

You should take the following advice to heart in order to ensure that the ring functions correctly:

- Set the **Hello Time** parameter to 2 seconds. If, within this given monitoring time, no test telegram is received 3 times running, then the connection is considered to be faulty.
- In Chapter 4, we advised you against configuring the EN100 module as a root-switch. For that reason, it’s best to leave the **Bridge Priority** at the default value of 32768. Merely set the module, that quite possibly is to serve as the Alternate Bridge, in other words, as logical gap, to the next lowest priority. At any rate, you should also try to shift this functionality to an external switch.

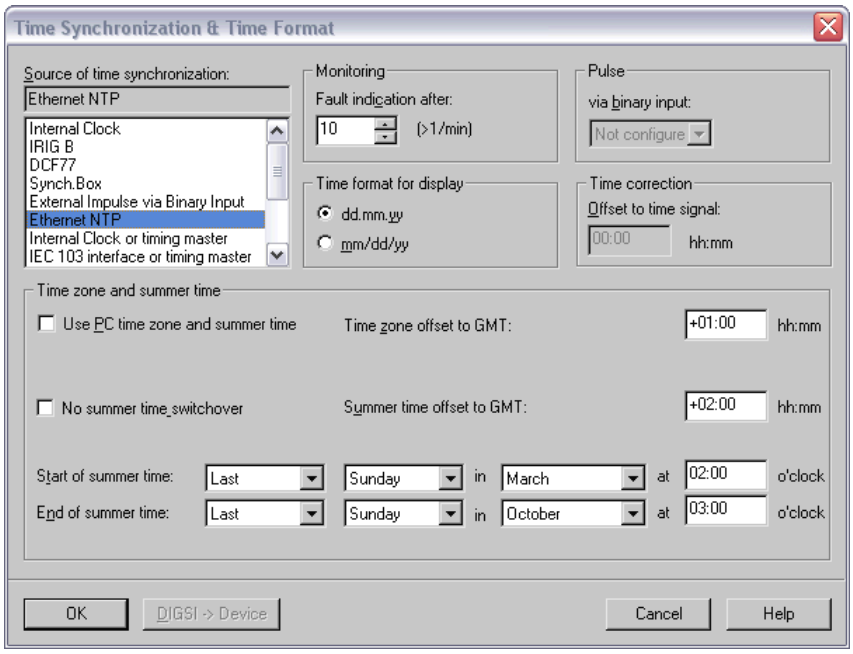
- In order to completely utilize the maximum number of 30 participants within a ring, as was addressed in Chapter 4, the **Max Age Time** must be 40 seconds. If this is not so, then the number of devices in a ring is limited to a maximum of 17.
- The **Transmit Count** parameter must be set to the value **100**. This parameter specifies the maximum number of configuration messages that are sent after a reconfiguration. The parameter's value should always be larger than the maximum number of switches within a ring.

Setting the Parameters for Time Synchronization

You have already learned that our design engineers (boys, you're really great!) have basically made DIGSI 4 capable of many procedures for time synchronization. As well, that for communication via Ethernet, Network Time Protocol (NTP) is the only sensible method to drill all participants on punctuality.

Great Expectations

Since DIGSI 4 leaves the selection of a particular type of time synchronization up to you, you must let the software know of your decision and, more importantly, you must do it separately for each participating device. To do so, double-click in the List View of the DIGSI Gerätebearbeitung on **Time synchronization** - and voilà, a dialog box appears with all the wonderful selection possibilities.



Going with the times: NTP should be selected for the time synchronization via Ethernet

Clear Decision

In the **Source of Time Synchronization** field, you will see **Ethernet NTP** as one of the possibilities you can choose. This possibility is not always selectable, by the way. It is only possible when you have configured an Ethernet module as the system port in the device's Properties. At any rate, there are no differences in the further parameterization of either of the two types, optic or electric.

If you would decide to use one of the other possibilities here, the time synchronization would not take place via the Ethernet network. The necessary time information for the IEC 61850 protocol itself would then be delivered from the device to the communication module. In our sample configuration we have integrated an NTP time server into the network. That is why we are selecting **Ethernet NTP**.

Waiting for Godot

The monitoring time defines the maximum allowed interval between two synchronization moments. A fault indication is generated as soon as two synchronization moments do not follow one another within the default time space. As of this point in time, all indications of the **Fault indication** status are set in the time stamp.

What period of time you select here is ultimately a question of your own system philosophy. Our tip: The SIPROTEC 4 devices query the time from the time server approximately every minute. In between, you work with the internal quarz clock which is very precise. Therefore, you can leave the default of 10 minutes.

The monitoring time is not a typical NTP parameter, by the way. It can be set for all forms of time synchronization. This is also true for the time format representation in the device display: The location of the device or possibly even only your taste are important here.

Four Seasons

In fact, we should direct our attention to the individual time zone and the differentiation between daylight saving time and standard time which we mentioned in Chapter 4. In the latter case, under no circumstances can you leave this change over up to the PC or heaven forbid deactivate it! As far as the concrete time specifications are concerned, our design engineers have already worked ahead. As long as the inofficial International Federal Supervisory Authority for time synchronization makes no new specifications, you can retain the values that DIGSI 4 provides and that are also shown in the figure above.

That´s it for now as far as the settings for time synchronization are concerned; you can exit the dialog by clicking **OK**. With the help of the DIGSI Systemkonfigurator, you carry through additional settings for the NTP server, and we will talk about that a little later. So stay tuned!

You should now save your settings and exit the device. Then, carry out the same procedure for all other devices that are integrated in the network.

Configuring a Network

8

Let’s take stock: We have decided on a topology and defined the IP addresses of the individual communication partners. The DIGSI 4 project has been created, all necessary devices have been inserted and duly entered as participants in an IEC 61850 station. Now it’s time to form relationships between the individual participants; to integrate them into a network with their valid IP addresses - everything still on a purely virtual level.

The access to information via communication connections and data linking between the participants is the station element. In keeping with the complete operating philosophy of DIGSI 4, according to which we open an object (device, control display, CFC chart) in order to edit the associated data, here as well, we will open the station – and thereby start the DIGSI System Configurator. With this, we define the network structure as well as the communication properties of the participants and networks and link the data objects of the individual participants.

Before you Start...

Now, before you let loose without restraint, we want to pass on a few hints. So that you can even start the DIGSI System Configurator, you must have previously opened each SIPROTEC 4 device that is entered as a participant at least once. Why? Quite simply: The DIGSI System Configurator gets its information about the individual participants from the respective device descriptions (ICD files) which we already introduced in Chapter 6. That’s why it is important that an ICD file exists for every participant when you open an IEC 61850 station. For other IEC 61850 participants, such as the time server, these ICD files are imported into the project. With SIPROTEC 4 devices they are generated as soon as you open the device to edit it. Since we are proceeding on the assumption that you have parameterized your SIPROTEC 4 devices as described in Chapter 7, you have already fulfilled this prerequisite.

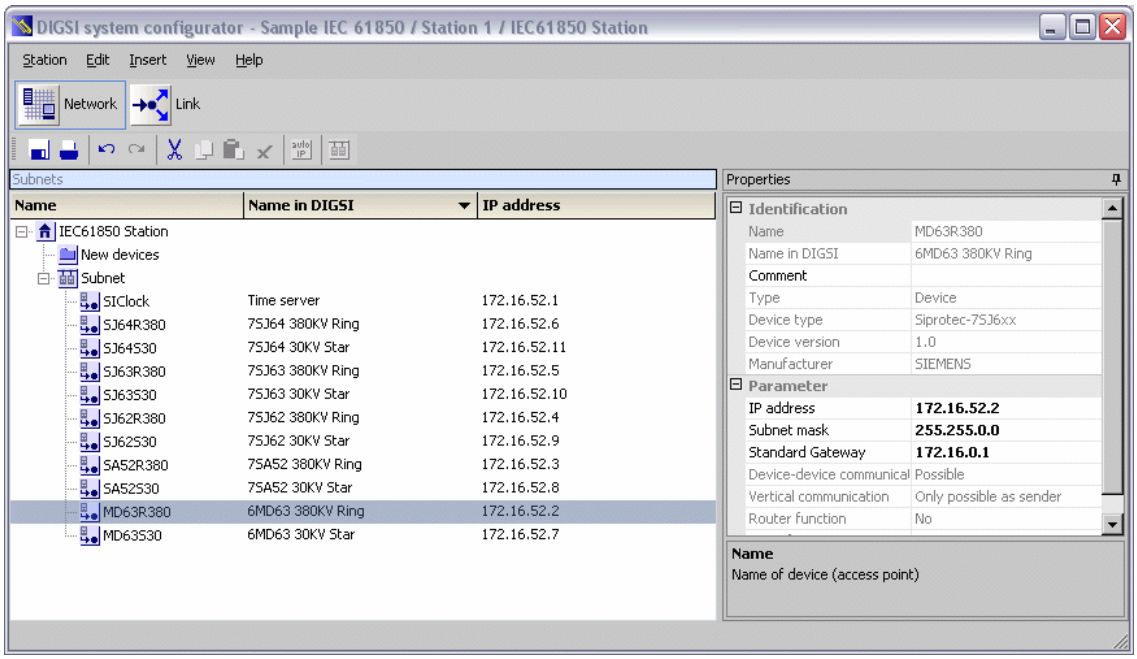
It is also important that the ICD file is current. If, for example, you change the IED name in the DIGSI Manager, you have to update the ICD file by once more opening up the device with the DIGSI device conditioning. You also have to make sure that none of the participating devices is being edited when you go to open the station. The DIGSI Manager will mercilessly stop you.

When all requirements are fulfilled, you can get started - with a double-click on the station icon. After a short dwelling time in which you can take a breather, the DIGSI System Configurator presents itself in a modern outfit. In the area of the menubar, you will immediately notice two amply dimensioned buttons. A mouse-click on either of these and you quickly switch between the work and task areas **Network** and **Link**.

Task Distribution

In the **Network** area**,** you structure the communication network of the IEC 61850 station as required. You do this by adding or deleting subnets. participants, that you previously selected for the station in the DIGSI Manager, you assign to these subnets. You define the addressing as well as other values for the relevant properties of the participants.

In the **Link** area, you define which participants are to exchange what data amongst themselves. To do this, you interconnect the data objects of individual participants. That is, you interconnect information between a source and a destination. So-called applications help you to structure these interconnections. An application is a group of interconnections for a specific application purpose, such as, for an interlock or a measured value task. You will find a nice and easy-to-understand example of this in our manual **Ethernet und IEC 61850 - Start Up**. For that reason, we don’t want to go into any more detail here. Rather, we have to take care of the special settings for the network.

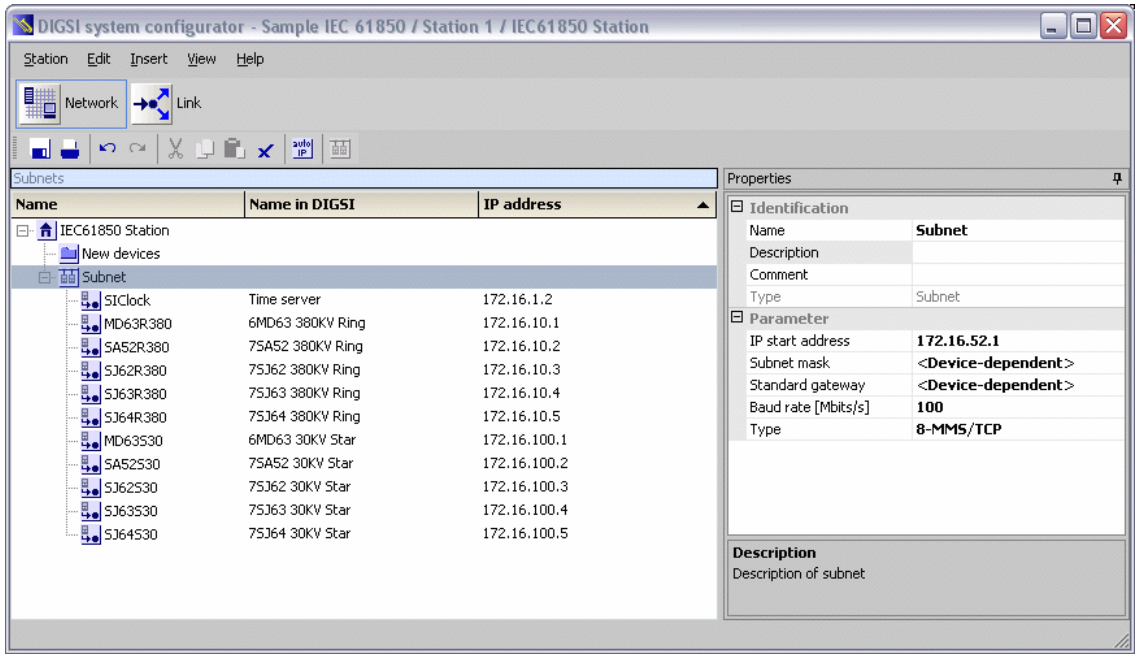


A question of perspective: The current network from the point of view of the DIGSI System Configurator

Back to the **Network** area**.** This shows you the current network structure on the left side. In our case, this consists of only one subnet. If you open this with a mouse-click, for example, you will get all important, basic information at a glance. In the **Name** column, you see the IED names of the time server as well as the ten protection devices that you or the DIGSI Manager assigned in the DIGSI Project. To the right of this you find the names of the devices as they are displayed in the project window of the DIGSI Manager. If you're interested in details, the Properties window on the right side helps you further. With the mouse, you select a particular element within the network structure and the Properties window immediately supplies you with the appropriate information. Why don't you select a participant in the **Subnets** window, **MD63R380,** for example. The Properties window then shows you, among other things, the device type or even the manufacturer in the **Identification** section.

Cleanliness is next to Godliness

A little lower you will see a series of parameters and their values. Very important is, of course, the IP address, for it establishes order in the network. We can't say it often enough: Invalid or doubly-assigned IP addresses are the beginning of the end for a functioning communication. That is why, as a precaution, the DIGSI System Configurator suggests a correct and unique IP address for every participant when you open a station for the first time. These are addresses in a private Class C network but they don't quite want to fit into our own address concept from Chapter 5. For that reason, we have improved on them just a little bit. This is done quite easily: You select the name of the participant in the **Subnets** window and edit the IP address in the **Properties** window. In this way, you work through one name after the other. When the whole thing is sorted according to IP address, the result should look like this:



New addresses: The participants with the IP addresses according to our concept.

Everything's Hunky Dory

Now almost everything has been said and done, at least, what is necessary for our task. For that reason, you can now close the DIGSI System Configurator. Your entries will automatically be checked for plausibility and then stored. Since you have made changes, a notice will pop up that the parameter sets of the individual station participants have to be updated. The parameter set update is done collectively for all devices. To do so, in the DIGSI Manager, open the Properties dialog of the IEC 61850 station and select the **Update** tab. Simply click on **Update all parameter sets** and let things take their course.

New Kids on the Block

A few words still on the assignment of IP addresses: Please note that only IEC 61850 participants of a DIGSI project are displayed in the DIGSI System Configurator and are taken into consideration when addresses are assigned. Other participants of the network, such as switches, serial hubs or PCs also need valid IP addresses to be sure. These, however, are not managed in the DIGSI System Configurator. You must therefore make absolutely sure that no IP address is assigned twice. Consistent planning and documenting of the network structure is the end all and be all for avoiding such errors.

Transferring Settings into the SIPROTEC 4 Device

9

The nice thing about DIGSI 4 is that you can carry out the complete parameterization without having a SIPROTEC device with you. If all preparations are completed, and we've almost reached this point, you simply transfer the results of your work into the device using a simple communication connection. Here, we are assuming that you possess a current SIPROTEC 4 device with the IEC 61850 option in which the EN100 module is already installed in the device and is ready-to-use, so to speak. If this is not the case, you still have a few other points to cover to prepare your SIPROTEC 4 device for its new task as networker. Everything that you have to do, you will find out about in Chapter 13 in the section **Swapping Modules**.

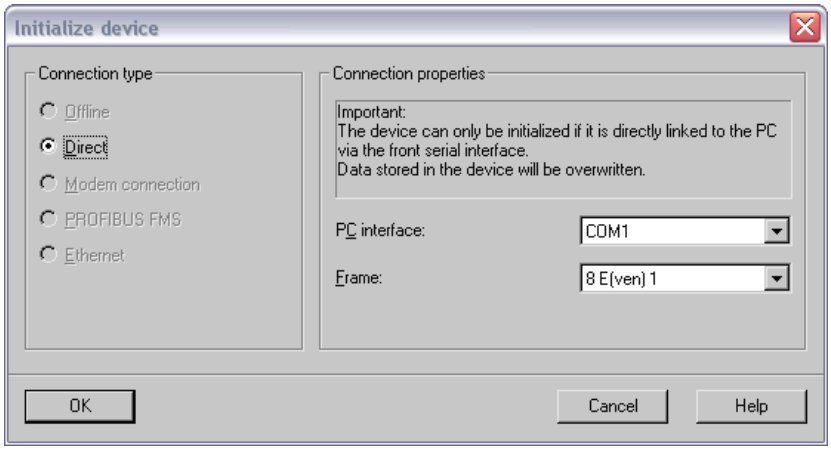
Notes in the margin: Through initialization, the network parameters in the device are set to valid values, so that the device can even be addressed via the network. If this is done once, the device can then be further parameterized much quicker via Ethernet later on. To do this, you select **Ethernet** as the connection type.

The settings that you have configured so far must now be transferred one after the other into the individual devices. Since, in our example, we had created these for the first time in our project, we must first initialize them. Initialization gives your SIPROTEC 4 device its own identity. Not only that the complete data set is transferred into the device in the process, during the initialization, the device is uniquely addressed.

We have extensively described the initialization of a device in the **DIGSI 4 Start Up** manual. For all of you who are not familiar with this, here's one simple rule to remember: As soon as you want to build up a connection between a newly created *virtual* device in the project structure and a *real* device, you must *initialize* the *real* device once with the data of the *virtual* device. After that, you can build up and disconnect a connection between the PC and the device as often as you like.

We have Ignition

Now connect any device you like with the PC. To do so, take the DIGSI 4 cable and plug it into a free serial PC interface (alias COM port). Plug the other end into the front interface on the SIPROTEC 4 device. In the project, select the icon for the relevant device and then choose the command **Device → Initialize device** from the menubar.



With the **Initialize device** dialog box you can check once more the current communication settings

The **Initialize device** dialog box displays the current settings for the PC interface (set according to the COM port chosen by you) and the Frame (please leave at **8E(ven)1**). Close this dialog box by clicking **OK**. A message will pop up that existing data in the SIPROTEC 4 device will be deleted by the initialization. If these values are not relevant for you or if they were already saved in files, then click on **Yes**.

The Right Words

After several intermediary messages you will be prompted to enter a password. As long as you haven't made any changes to the passwords, type in zero six times. Then click **OK**. By the way, you cannot only follow the transmission procedure on the monitor, you can also follow it on the SIPROTEC 4 device's display. Once the initialization is completed, the default display will again appear. The connection between the PC and the device was only of a temporary nature and once the intialization is completed, it is disconnected.

Assigning Parameters to the Switch and Time Server

10

When it comes to setting the switch and time server, we must ask you, for the most part, to refer to the respective manuals of these components. For one thing, many of the settings and even the way to get to them are very type-specific and you are utimately not bound to the recommendations that we make in this book. For another, a number of parameters are completely independent on the type of network topology; their setting is sooner determined by your personal system philosophy.

This affects the time server, in particular. So that our sample configuration functions correctly, the right IP address is the important thing, just like with all other participants. We ask you to please study the time server's operating instructions for all other possibilities for helpful or more exotic settings that your time server permits. The rest of this chapter is dedicated to the parameter assignment of the switches used - specifically those of the Ruggedcom company.

Regardless of whether you would now like to change any settings or would like to load new firmware into the switch, you need a communication connection between the switch and the PC to do so. An Ethernet connection is well suited for this. Alternatively, you can make use of a more traditional, but still usable method: the serial hyper terminal connection. We will describe both communications procedures, but we will put the emphasis on Ethernet.

By the way: We assume that your switches have the latest firmware version. If it wouldn't hurt to do a little firmware lifting, you can read about how it's done in Chapter 13.

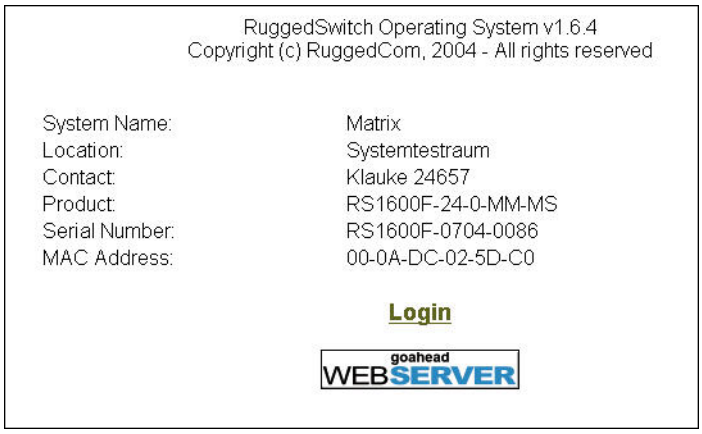
Addressing the Switch via Ethernet

Via an Ethernet connection, you can set all parameters of a switch from any location in the network - as long as the switch has its correct IP address on the network. You will first have to teach it this though. Each switch has a default IP address. This address and a direct Ethernet connection between switch and PC enable you to make a first contact. During this first contact, you can then set the IP address you have chosen. Everything else, you can take care of now if you like or later after commissioning - and then via the network.

First Connect ...

First thing, connect the PC's network card to the switch. Make sure that the cable used is wired straight through. Cross-over cable, like the ones used to connect two PCs are not suitable. Other than that, all you need for the first dialog is a web browser and you're off to the races.

In the browser's address field, enter the switch's default IP address in the format http://192.168.0.101 and confirm this by pressing the Enter key. The switch then responds in the browser with a first overview on the state of things.



Here comes the switch

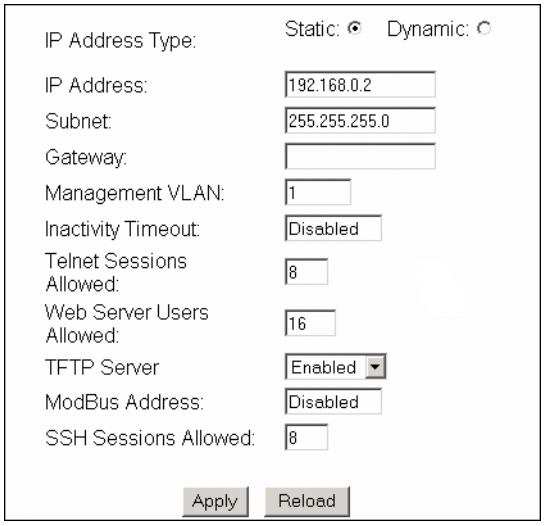
... then Login

You can only really take off after you have successfully logged on. To do so, you must enter the correct user name and the current codeword. The input dialog for the user data appears after you click **Login**. The first time both are **admin**. It is certainly most advisable to change at least the codeword into something less obvious later on. Now just click on **OK** and the switch clears the way to the main menu.

The main menu is the starting point to a multitude of configuration possibilities.

Setting the Network Parameters for the Switch

Before you can integrate a switch into the network operation, you must set several network parameters for it, the first one being the IP address. You will find this and other related parameters in the area **Administration** and from there under the menu entry **Configure IP-Services**.



You find the network parameters in the **IP Services menu**.

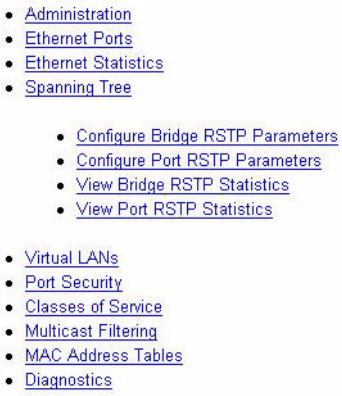
We enter the IP address for the switch according to our topology plan that we created earler. In any case, the address is of the **Static** type, since we are not using a DHCP server. The subnet for our Class B network is 255.255.0.0.

The **SNMP Get Community** parameter should be set to **public**. That way you can monitor the switch using SNMP. This can take place, on the one hand, through special software tools; on the other hand, functions are also implemented in SICAM PAS, for example, that make a diagnosis using SNMP possible.

Affer a click on **Apply,** the switch adopts the new settings. After that you can click on **Back** without a second thought in order to work your way back up in the menu structure.

Setting the Port Parameters

You can individually configure each single port of a switch. However, that doesn't make much sense, at least in our case. On the contrary, we will set the parameters for all ports identically. And this is how it's done: In the main menu, first click on **Port Configuration and Status**. Thereupon, a submenu will become visible which summarizes different port-specific settings and information.



The port parameters are accessible via a submenu.

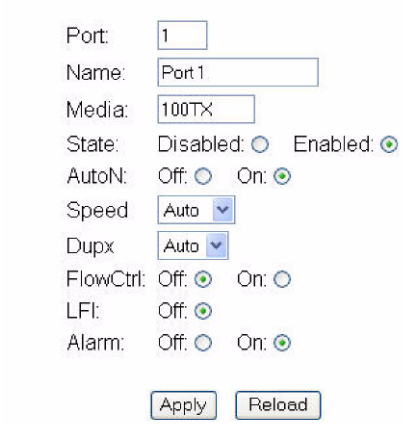
Port for Port

Above all, the port parameters as well as the port security are of interest to us. For that reason, please click on **Configure Port Parameters** in the submenu. The browser now shows you an overview of the current settings for all ports.

Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1	Port 1	100TX	Enabled	On	Auto	Auto	Off	Off	On
2	Port 2	100TX	Enabled	On	Auto	Auto	Off	Off	On
3	Port 3	100TX	Enabled	On	Auto	Auto	Off	Off	On
4	Port 4	100TX	Enabled	On	Auto	Auto	Off	Off	On
5	Port 5	100TX	Enabled	On	Auto	Auto	Off	Off	On
6	Port 6	100TX	Enabled	On	Auto	Auto	Off	Off	On
7	Port 7	100FX	Enabled	Off	100M	Full	Off	Off	On
8	Port 8	100FX	Enabled	Off	100M	Full	Off	Off	On

Everything at a glance: The table shows the current settings of the port parameters.

As you can see, the ports are consecutively numbered. With one click on the number of a port, you open the setting dialog for its parameters. The figure shows the settings as they should be. What we are about to explain as an example for one port, please do for all other ports.



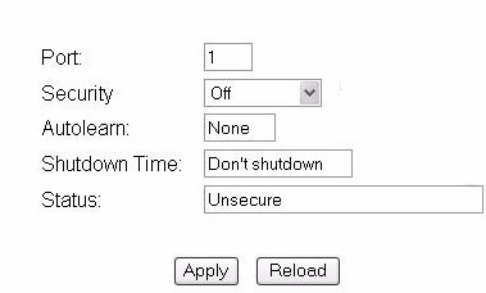
The port parameters are, for the most part, already familiar to you .

Notes in the margin:
As already explained in Chapter 3, the **FEFI** function superimposes the aging time of MAC addresses. When there is a connection failure, FEFI makes a significantly faster change over to a replacement channel possible.

Important, of course, is that a port that you would like to use is activated, that its status has the value **Enabled**. Transmission should occur in full duplex mode. For this, you must choose the **Full** setting for the **Media Type** parameter. And last but not least, the Far Error Fault Indication must be activated, therefore **FEFI** on **Enabled**! When all this is done, you assign the new settings to the switch by clicking **Apply**. After that, it means clicking once on **Back** and continuing with the next port. When you are through with all the necessary ports, a further click on **Back** gets you from the overview back to the submenu.

Without Security

In the submenu you click on **Configure Port Security**. Just as with the port parameters, the browser first of all shows you an overview of the current settings which gives you the opportunity to open the setting dialogs for the individual ports. The operating procedure is identical, only the dialog looks like this:



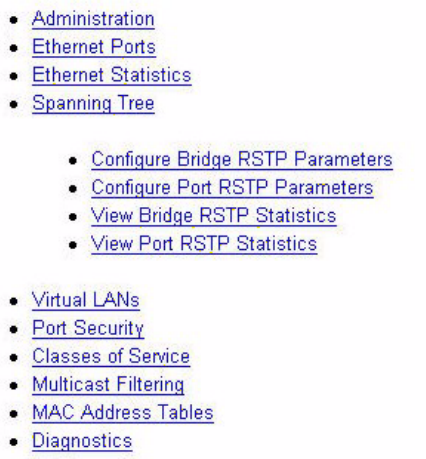
Unusual: Only when Port Security is deactivated, does everything run without a hitch.

You just have to set the **Security** parameter to **Off**, and for a good reason: An activated port security leads inevitably to conflicts with RSTP! As soon as you have deactivated the port security for all ports, go back to the main menu.

Setting the RSTP Properties

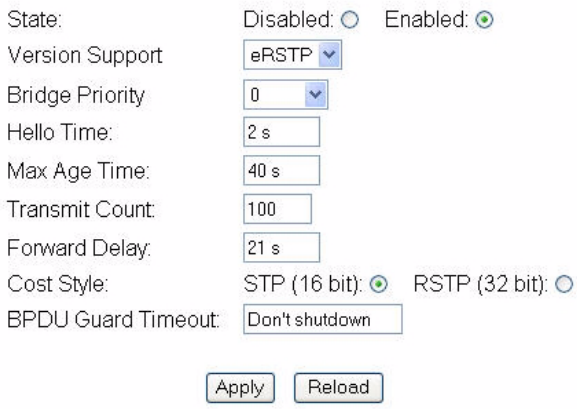
Even with the RSTP properties, there are those which you can set differently depending on the port, and, in most cases, you must. But we are naturally also considering the switch as a whole, namely in its function as RSTP Bridge, for which there are several cross-port settings, like for example, the RSTP priority.

A click on the entry **Spanning Tree** opens the way to both categories of parameters.



Still another menu: The RSTP Parameters.

Let’s begin with the parameters that refer to the switch as a whole. A corresponding setting dialog appears as soon as you click on **Configure Bridge RSTP Parameters** in the submenu.



Pay attention to the correct settings for the Bridge Parameters.

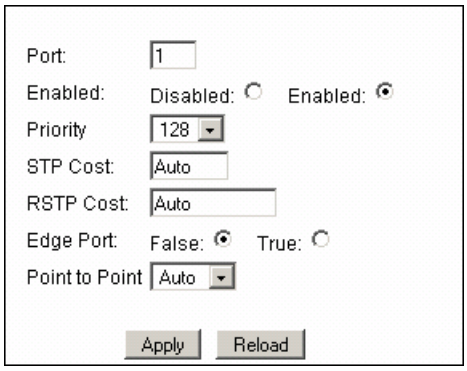
The figure shows settings that are important for flawless operation. For that reason, use them for all parameters - with the exception of the Bridge Priority. This must, of course, be set differently for several switches according to the topology. For our example, you would use the values as we defined them in Chapter 5.

All parameters correctly set? Then click once more on **Apply** and go back to the menu. Here, you then select **Configure Port RSTP Parameters**. Since we are once again dealing with port-specific settings, you will first of all get an overview of the current settings.

Port	Enabled	Priority	STP Cost	RSTP Cost	Edge Port	Point to Point
1	Enabled	128	Auto	Auto	False	Auto
2	Enabled	128	Auto	Auto	False	Auto
3	Enabled	128	Auto	Auto	True	Auto
4	Enabled	128	Auto	Auto	True	Auto
5	Enabled	128	Auto	Auto	False	Auto
6	Enabled	128	Auto	Auto	False	Auto
7	Enabled	128	Auto	Auto	True	Auto
8	Enabled	128	Auto	Auto	True	Auto
9	Enabled	128	Auto	Auto	True	Auto
10	Enabled	128	Auto	Auto	True	Auto
11	Enabled	128	Auto	Auto	True	Auto
12	Enabled	128	Auto	Auto	True	Auto
13	Enabled	128	Auto	Auto	True	Auto
14	Enabled	128	Auto	Auto	True	Auto
15	Enabled	128	Auto	Auto	True	Auto
16	Enabled	128	Auto	Auto	True	Auto

The RSTP port settings present themselves once more as a table.

As usual, click on the number of the port whose settings you want to edit and then get a dialog for it.



Now quickly set the RSTP parameters of the individual ports.

Edge Port or not Edge Port

Valid here as well: Use the values as you see them in the figure. The only exception is the **Edge Port** parameter. This one you have to look at individually for every port and set it to True if it is an Edge Port or to False if it is not an Edge Port. Put simply, classify a port as Edge Port if everything that is connected to it doesn't form a ring. Here are a few rules:

Select the setting **Edge Port = True** if ...

- ... a SIPROTEC device is connected to the port via an electric EN100 module.
- ... a SIPROTEC device is connected to the port via an optic EN100 module which is working in line operation.

Select the setting **Edge Port = False** if ...

- ... a SIPROTEC device is connected to the port via an optic EN100 module that is operated in switch mode.
- ... the port in question establishes the connection to a ring.
- ... the port in question is connected to the port of another switch.

If you have configured all ports, then your work here is done as well. By the way, you can also read out the settings in the form of a configuration file, edit them with an Editor and then reload them into the switch. We will divulge how this is done at the conclusion of this book in Chapter 13.

Addressing a Switch via Hyper Terminal

If, before the first commissioning of the network, you would rather operate a traditional but still usable method, then connect the serial RS232 interface of the switch with that of the PC and establish a hyper terminal connection between the two components. For this, you will require a so-called 1:1-modem-cable as connector cable. Such a cable is included with every DIGSI 4 for the communication between PC and SIPROTEC 4 device, by the way.

Window Opener

Directly via the Start menu with **Programs → Accessories → Communication → Hyper Terminal → <connectionname>,** you open the hyper terminal window. <connectionname> is used as a dummy for the individual hyper terminal connection between PC and switch that you must first configure yourself. A description on how you proceed has been placed in Chapter 13 along with various other supplementary topics.

Now all you have to do is activate the connection. To do so, select the command **Call** in the menu **Call**. This is no typing error, but is unfortunately really so. Alternatively, simply hit the key combination **Ctrl S**, it does the same thing. The connection between PC and switch is established. The switch now expects a formal registration for your part, in other words, a password.

The very first time this is, once again, simply **admin**. As soon as you enter the password and press **Enter** to send it to the switch, the terminal window shows a selection menu and you can get going. The selection menu, of course, contains the same entries as you had with communication via Ethernet using a web browser. And even for the necessary settings, there are no changes.

Connecting and Turning On

11

We could write several books on how you interconnect the mountains of sheet metal and plastic, filled with thousands of electronic parts, with one another - and for exactly that reason we will limit ourselves to a few paragraphs. The possibilities for your specific system configuration, the premises in which the hardware is accomodated and so forth... are too many-sided. If you're unsure of yourself, then place your trust in an experienced networker. So that you can have a say in things just the same, we'll pass on a few tips to keep you going.

If you want to go beyond a tentative test configuration and instead want to have a permanent connection between your devices, you must absolutely take into account the EN 50173. This standard defines the structured network cabling right up to the correct bundling of several cables with cable ties. If you would like to know more about EN 50173, any Internet search engine would be more than happy to spit out a multitude of articles on this topic. A subsection of this standard deals with the selection of the correct cable. For our sample configuration from Chapter 5, we need cables that are of an electrical and also optical design.

Under Power

At the local cable distributor around the corner you will find two very different kinds available in the electrical network cable department: Patch cables and installation cables. How much of which sort you buy should not be determined by what kind of a discount you will receive, but purely and simply for what purpose the cable is to used.

Patch cables are bendable because they are primarily designed for connecting devices that are placed close to one another. If, for example, you have mounted the protection devices of a field and the associated switch together in one rack, then patch cables are the predestined connection medium. The patches get their mechanical flexibility from the thinner wires that wind their way as strands through the plastic jacket. In most cases, strands are even used. And this unfortunately leads to poorer electrical values. For that reason, patch cables should not be used for longer stretches - five meters should be the upper limit.

If it has to be more, you are better off to grab installation cable. Choose shielded twisted pair, in short STP. With this type of cable, the data strands are surrounded by a shield that extensively eliminates outside electrical interference. With such STP cables you are sure to bridge up to twenty meters.

Quality Wares

With the selection of both patch cables and installation cables, you should pay attention to the electrical quality. This is defined by the classification into different categories. The most current state of things and sufficient for most applications is CAT5. If you are prepared to spend a few euros more, then take the CAT5e. With this cable quality, data will also be safely transported in distances of up to 100 meters in a gigabit Ethernet network. Compared to it, CAT6 or the up and coming CAT7 cable that can even transmit 10-gigabit Ethernet electrically are oversized for our application purposes.

Let there be Light

For greater distances and amounts of data, fiber-optic cables are the better choice. Multimode fiber cables are suitable for up to a cabling length of 2 km. Distances that go beyond that have to be bridged with single-mode fiber cables. With that, you can then also achieve up to 100 km without having to refresh the signal.

We will, however, remain very modestly underneath the 2-Km mark and use MMF cable that can transmit light with a wavelength of up to 1380 nm. What is important is a further characteristic value, namely the specification of core and outside diameters of the fibers. 50/125 µm or 65.5/125 µm are suitable types for our purposes.

Well Connected

We still need the correct connectors to match the cable. Our recommendation: As far as possible buy cable in a pre-assembled state. Considering the price of pre-assembled patches, it is not worth it to manually do the work with electrical patch cables. And to fit fiber-optic cables with connectors yourself usually doesn't lead to the desired results. Only with STP installation cable that is sold by the meter does it appear to make sense to do it yourself. But, whoever doesn't have the necessary tools or the experience is better of to let an expert do it.

As far as the connectors themselves are concerned: For electrical connections, only RJ45 comes into consideration. For fiber-optic, there are two separate camps, however. You make the connection to EN100 modules as well as to OSM switches with Duplex-LC connectors. Switches from Ruggedcom, on the other hand, prefer MTRJ connectors. You therefore need a mix of pre-assembled cables which you can purchase directly from Siemens, by the way.

Making the Right Choice

So that the perfect communication doesn't already fail because of a couple of defective cables, you should take the time to check them out before you install them. This makes particular sense for cables that are not new from the factory or ones you have assembled yourself. Simple testing equipment can already detect one wirebreak or simple wiring error and this equipment when compared to a SIPROTEC 4 device is very, very inexpensive to purchase. But it doesn't necessarily have to be an interrupted connection that leads to poor data transmission.

Cables that have been selected too long, not cleanly laid, or subject to other electrical interferences can also be the cause. A check by a professional is recommended especially when cables are permanently installed. He takes a close look at frequency response, damping and crosstalk and provides help in case of an emergency.

Plans and Lists

Our tip: A topological wiring plan and corresponding markings on cables (with felt-tip markers) and on the ports (with labels) considerably eases later troubleshooting. In addition, a list with several essential characteristic data of the participants provides clarity, even for colleagues and especially after a long time. Device type, MLFB number, BF number, firmware version of device and module, IP address, net mask, address of the standard gateway, MAC address and IED name under IEC 61850 is the minimum data for SIPROTEC 4 devices which should be documented by the list.

Notes in the margin:
For SIPROTEC 4 devices, you can read out the MAC addresses directly on the device display (key sequence Menu 5 5 Enter).

For devices such as switches and time servers, you should, as far as possible, include similar characteristic values in the list. When this is completed, make sure that no IP address appears twice. With MAC addresses, this should not be possible anyway because of their unique assignment.

Smoker or Non-smoker

If all preparations are finalized you can start to commission the system step by step. But first, you should physically interrupt the ring temporarily in one spot. This measure helps you to achieve a stable ring structure. First of all, switch on the time server and then the switches. After you have activated the last switch, wait for about 20 seconds and then begin to switch on the devices. We recommend that you apply voltage to the devices one after the other according to their assignment in the network. Give each device the time to completely power up before you switch on the next device. When all devices are operational, close the ring.

If you haven't registered any unpleasant burning smells so far, it's a positive sign and you can be happy for now. In the next chapter, you will find out what you still have to do.

Testing the Correct Functioning 12

In this chapter, we want to give you some information on how you can test your network and the integrated components for correct functioning. For all that, it is practical to first act as if everything is OK, since it's always only the other guy who has errors. We will therefore first try to make contact with each individual SIPROTEC 4 device on the network. Should there, contrary to our assumption, be a hitch here and there during our first attempt, we will take a closer look at the respective component.

Testing the Communications Capability

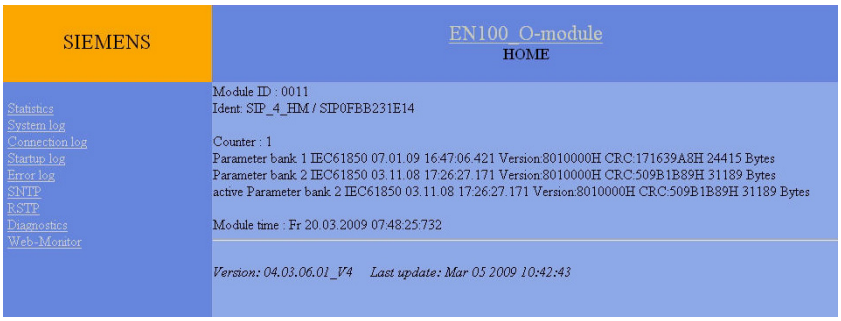
After you have set all parameters and transferred the values into the devices, they should be accessible on the network via their IP address. That is exactly what we want to check now.

Each EN100 module has the luxury of having its own homepage. This mainly serves for diagnostic purposes during commissioning or in cases when things are not going the way they are supposed to during operation. We use this homepage for a first attempt to determine whether we can even make contact with a device.

Off to Home

To activate the module homepage, use a PC to hook up to any switch on the network. This PC must, of course, be configured for the network. That is why it makes sense to use your DIGSI 4 PC for this task. It is already a component of the network anyway. DIGSI 4, itself, you don't need for this action. Instead, open your perferred web browser. In the address bar, enter the IP address of the target device and include the addition **/home**. Your entry then has the format **http://172.16.10.1/home** for example. With the Return key, you send your request on its way.

The browser should now display the module's homepage. If that's so, you can register several victories all at once: module and device are accessible, the connection cables from PC to the device are OK and even all switches connected in between appear to be working correctly. But let's have a closer look at the module's homepage.



Not pretty, but smart: The homepage of the EN100 module provides a lot of information.

The following is generally valid: Depending on the operating mode of the module, either line or switch, the homepage will be displayed differently with regard to the information it offers. In all cases, it will show the version and the manufacturing date of the software version that is currently located on the module. This information can be important when you correspond with our hotline.

That's not all, of course; you'll get to really indepth information via various links that are grouped in a menu on the lefthand side of the homepage. More on that in the section **Learning Even More Details with the Module Homepage**.

Naturally, not only the EN100 modules in the SIPROTEC 4 devices can be reached via the browser. This is normally also possible with time servers and switches of the higher priced segment. With Ruggedcom products you can, for example, access switches of the main firmware version 1.6 or higher with the help of a browser. All you have to do is enter the switch's IP address and then log in to the switch.

No Reply

It is possible that a device is not accessible and its module homepage remains hidden because of it. This can be be caused by several things:

- A SIPROTEC 4 device, that is connected to an external switch via a line connection, is turned off.
- A SIPROTEC 4 device, that is integrated in an optic ring, is turned off.
- A ring structure is interrupted in several locations; therefore, some of the devices can no longer be reached. The cause for the interruptions could be turned off devices or detached connections.

In principle, a malfunction of the EN100 module could also exist. More on that in the next section.

Testing the Correct Functioning of the EN100 Module

If there are problems reaching a device you should, in addition to the connection cables, also take a closer look at the respective built-in module. But even if the unit is operating impeccably, you can't get around a few tests directly on the device, such as, to check the ring functionality. The

module information page helps you for all examinations directly on the unit. So that this is shown on the device's display, press the following keys one after the other on the device: **Menu 5 5 1.**

Connection Display

Fantastic look: Information for an optic EN100 module

Lucky owners of devices with large displays can see the information of this module information page in all its splendor, just as it appears above. Devices with smaller displays only show four lines at a time. In order to see the other lines, you have to operate the vertical navigation keys.

1	Network Config
2	MAC 080006865116
3	IP 172.016.052.055
4	NM 255.255.000.000
5	GW 172.016.000.001
6	NTP 172.016.000.254
7	Chan1/2=Up/Up
8	Rx/TxCnt=23489/34403
9	Rx/TxErr=00000/00000
10	Rx/Tx10s=03221/02888
11	CPU load=68%
12	LRx1/LTx1=norm/norm
13	LRx2/LTx2=weak/----
14	Switch RSTP
15	Priority=32768
16	Bridge Id=172165255
17	Hello Time=3sec
18	Max Age Tm.=40sec
19	Forward Del=15sec
20	MaxTransmCnt=100
21	R/S1=A/D R/S2=R/F
22-26	...
27	******* END *******

The picture above shows the module information page for an EN100 module in optic version. Since the electric variant of the module does not have a switch functionality, its display has less lines. Which information is the same for both versions, which is only for the optic version and above all how you interpret the information is what we will clarify now.

Who am I and Where am I?

Lines 2 to 5 give you information about the framework conditions, as it were, for both module versions. From top to bottom these are the MAC address and the IP address of the module, the net mask, followed closely by the gateway address. Now it pays to have an overview diagram that shows the individual devices in conjunction with their IP addresses. That way, it's quick to check whether the originally defined addresses have really found the correct owners.

007

For now we will jump over Line 6 and take a look at the information in Line 7. This gives details about the state of the connection to the network. How this information is presented can depend on the type of EN100 module, namely then when the optic module is operated in switch mode. In this case, Line 7 supplies you the information for each of the two ports, whether it is active (up) or not active (down). The information **Chan1/2=Up/Up** is the best thing that can happen to you for both ports (or channels) are active. The ring is therefore at least intact at the currently
checked spot. You should now test whether the module recognizes a ring interruption correctly. For this, the first thing you do is to pull the connector from Port 1. This display must now show the appropriate information for this **Chan1/2=Down/Up**. Repeat the test with the other possible combinations.

In line operation, and this is the only mode for EN100 modules in electric version, the information in Line 7 is displayed a little differently. The message **Phy1 100 MBit Full-Duplex** wants to tell us that presently Port 1 is active and that it is working with a maximum transmission rate of 100 MBit in full duplex mode. Here, as well, you should simulate a line interruption by pulling a cable and checking the module's response.

Telegram Delivery

You learn something about the telegram traffic in Lines 8 to 10. Line 8 indicates the number of received and sent telegrams. In addition to an absolute number, this counter also provides information on whether the port can receive and send telegrams at all. Recognized telegram errors are also counted, the respective current value is displayed in Line 9. The value in Line 10 is a 10 second mean value derived from the number of received and sent telegrams.

Line 6 helps ...

We certainly hope that only positive indications for all modules can be read in the displays. Should this not be so, then systematic troubleshooting is called for. Since you've already got your eye focused on the display, please take a look at the contents of Line 6, the one that we jumped over earlier. This line is fully loaded; a multitude of information can be displayed here: The IP address of the NTP server, the amount of time that has passed since the last time synchronization, the indication of an inconsistent parameter assignment and the reference to another participant that has the same IP address as the currently examined device.

... in Relationship Conflicts

The last piece of information named is particularly critical because it means that no connection to the network is built up. It is therefore statically displayed in the form **!!MAC!!0007E908FCC8** and overlays the display of the other three pieces of information. The displayed MAC address clearly identifies the participant on the network that has an identical IP address. You now have to change the IP address of one of the two participants and in that way hopefully solve the original connection problem.

... in Different Points of View

A further cause of communication difficulties could be inconsistent parameters. Put bluntly: The module's parameter set doesn't really want to fit to that of the device's. Something like this can happen, for example, when modules are swapped between devices but the devices are not reinitialized. The text **Corrupt parameters** points to such a circumstance. Of course, this is not shown statically like with the double address assignment, but alternately with the two pieces of information on the NTP server.

... in Unpunctuality

To remember: We are still dealing with Line 6 and are now assuming that no indications are being displayed to signal faulty connections. In this spot between Line 5 and Line 7 you will then see the IP address of the NTP server displayed alternately, every ten seconds, with a time specification: **NTP last sync 0033s**. The time displayed is the time that has passed since the last time synchronization.

Immediately after the device starts up, until the first synchronization after about a half a minute, there is no valid time-of-day available in the device. Should you, of course, see the maximum possible value of 999 seconds in the display, then you can be sure that the NTP server has slept through its engagement. In such a case, you will have to search for the cause in the respective NTP server using the diagnostic tools.

Connection Analysis

If all checks and controls prove that the participants themselves cannot be the cause of the missing connection, you'll have to take another closer look at the connecting cables. Have you remembered that you aren't allowed to use cross-over cable between the protection device and the switch when you make the electrical connections? Are mechanical damages visible on the cables? Or is it possible that a connector doesn't have the necessary contact?

Let's assume, that the port of a module in an optic ring has the state **Down**. In this case, it is worth taking a look at the neighboring device that is interconnected with this port. If the corresponding port also indicates that it is sickly, then it is obvious that you should look for the error in the connecting cable.

Dampened Spirits

Actually, for the optic modules you get even more indications on the module information page that can be helpful during troubleshooting. As such you find information about the receiving performance LRx and the sending performance LTx of the individual ports in the Lines 12 (Port 1) and 13 (Port 2). The word **norm** signals that everything is hunky dory. **Weak** indicates an already too low performance and if all you can see are horizontal lines, then the damping is clearly too high. The cause does not have to, but could be faulty connecting cables.

Remote Connection

Let's briefly get away from the module page in the display and with that from the on-site control of the device. Even from a distance, you can learn with DIGSI 4 whether the module as well as the two ports are working correctly or whether there is a fault. For this there is a module failure indication and two link status indications that are protocolled in the event log buffer. The module failure indication signals a module that is not functional. The two link status indications give information about the physical state of the connection.

	Information				Source			
	Number	Display text	L	Type	BI	F	S	C
Device, General							×	×
EN100-Modul 1	009.0100.01	Failure Modul		IntSP				
	009.0101.01	Fail Ch1		IntSP				
	009.0102.01	Fail Ch2		IntSP				
CommTest		TestSignal		ExSP			X	

EN100 module indications in DIGSI 4

You can route these indications to different destinations in the device matrix, for example, to LEDs of the device. In our book **DIGSI 4 - Start Up,** you will find out how you basically go about this.

Testing the Ring Functionality

After extensive testing of the communication capabilities and of the EN100 module it is now time to do a gap test. We will check whether the logical gap opens in our optic ring where we wanted it. Here, as well, the module information page helps us further. On this page, the first thing you check is whether the values set in DIGSI 4 for the communications parameters have arrived correctly in the device.

Notes in the margin:
If you have decided to use OSM, Lines 15 to 21 are not visible.

Line 14 shows the redundancy mode set in the module. In our case it should be RSTP. The value for the priority in Line 15 must match the value you defined specifically for your topology.

Very important are the values of the parameters in Lines 17 to 20. These must be set exactly as we explained it in Chapter 7. Here, once more, an overview on the pertinent parameters and their imperative settings.

- **Hello Time**: 2 s
- **Max Age Time**: 40 s
- **Forward Delay**: 15 s
- **Max Transmit Count**: 100

With the information from Line 21, you check whether the module also has the desired ring functionality. For each of the two ports, the role and the status are displayed. Before we get into how you can evaluate the displayed information, here once more a short review of the possible roles and statuses of a port.

The following roles are defined for the ports:

- **Root Port** (R) Role:
  A root port is logically connected with the root switch. With the internal switch of the EN100 module, one of the two ports always has the role of root port.
- **Designated Port** (D) Role:
  A designated port can also establish a connection to the root switch, but in another way. As a rule, one of the two ports of the internal switch as the role of designated port.
- **Alternate Port** (A) Role:
  An alternate port can establish a logical connection when there is a failure. In stable operation there can only be exactly one alternate port in the ring. If no port with this role exists in the ring, then the redundancy cannot be ensured.

The following statuses are defined for the ports:

- **Forwarding** (F) Status:
  During normal operation, this status is the status of the ports that play the role of root or designated. In this state, user data telegrams are always transmitted.
- **Discarding** (D) Status:
  This status means that telegrams are not passed on or are discarded. During normal operation, only the alternate port has this status.

Back to Line 21. You recognize the logical separation point by the fact that a port has the role (R) **Alternate** and the status (S) **Designated**. If, for example, the information **R/S1=A/D R/S2=R/F** is displayed, then you've found it: Port 1 of this device is the logical separation in the ring, in other words, the alternate port.

The status of the port changes when the ring is physically separated. The logical separation point is then closed. For that, the port first of all takes on the status **Discarding**. In this state, only administration information is sent, for example, about the change of the role of the port. As soon as the port reaches the status **Forwarding** and taken on the role of **Root**, the logical reconfiguration of the network is completed. Then user data telegrams are sent once more.

You can and should also test this behavior. To do so, you merely have to separate the connection in one spot of the ring by pulling the network cable from a module. The display in Line 21 of the device that works as alternate bridge should then look like this: **R/S1=R/F R/S2=R/F**.

You can also do an automated search for the alternate port in a network. By means of batch file or script, you can search through the homepages of all EN100 modules. More on these possibilities in Chapter 13.

Learning Even More Details with the Module Homepage

Let's go back once more to our module homepage. You'll come to appreaciate how much varied information you can get from this page as soon as you click on a few items in the menu on the left-hand side.

Long Term Memory

There is, for example, the error buffer. By clicking on **Error Buffer,** you can bring its contents to the sceen. If the error buffer is empty, your mood will continue to be positive.

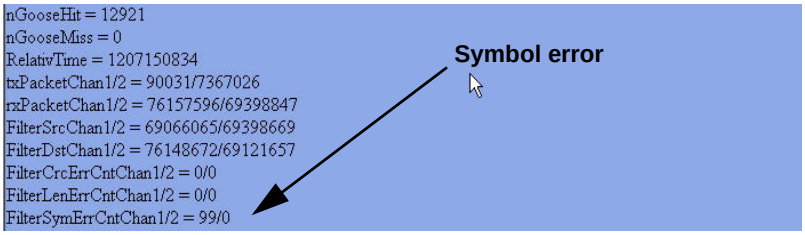
Another important memory is the printf Buffer, whose contents you get at by clicking on the link of the same name. To interpret the information that is displayed will be hard. It is there more to give our Hotline a base for targeted error diagnosis in those cases when you can't get any further yourself.

Without an abdomen: Excerpt from the Print Buffer

Statistic page

What will also come in handy here and there during commissioning is a targeted look in the so-called Statistic. This is a cross-section of information about the data transmission including the switches. A table at the end of this section shows you all information including a few explanations.

Some information deserves to be looked at a little more closely, however. Of particular significance is, for example, the number of faulty symbols that give a statement about the quality of the connection: The higher the value, the poorer the connection. This value is counted up during turn on and turn off or when the connection is interrupted. During running operation, however, the number cannot change.



Even symbols can make a mistake: A section of the Statistic shows the number of symbol errors.

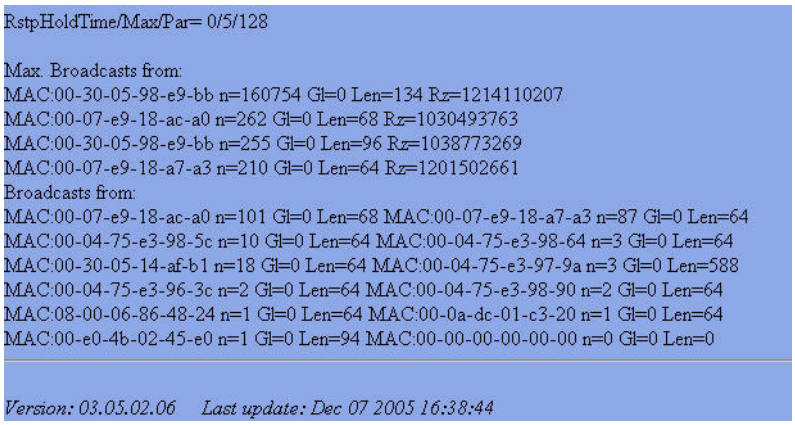
Free Additional Information

Some more interesting information:

- **RSTP Role Chan1/2 = Alternate/Root**
  If the SIPROTEC 4 devices are arranged in a ring and the ring is connected and linked with the external (turned on) switches, then the Statistic of one of the SIPROTEC 4 devices must include this indication. If this doesn't exist on any of the devices on the ring, then the ring is physically interrupted at least in one point in the ring.
- **FilterSymErrCntChan1/2 = 0/2753**
  If these two counters count up during stable operation of the device without one or both neighbor devices being turned off, then there is a poor fibre-optic connection. Cause can be an increased damping, for example, through bad cable.
- **Frames Loss = 0**
  A value unequal to zero signals circling multicast telegrams.
- **FNS queue overflow = 0**
  If the value of this information is unequal to zero, then it is an indication of circling broadcast telegrams.

Please note that you must manually update the web page display in order to be able to see changes in the variable values or counter statuses.

Those of you who are more interested in broadcast telegrams, by the way, will also find interesting information in the Statistic, as can be seen in the following figure.



The Statistic has quite a bit to offer the fans of broadcast telegrams.

- **Max Broadcasts from**
  Here, the four most frequent broadcasts since the start up of the module are listed. They are described by five individual pieces of information:
  - The MAC address of the broadcast sender
  - The number n of these broadcasts within the last four minutes
  - The number Gl of successive identical telegrams
  - The length Len of the telegrams
  - The relative time Rz

- **Broadcasts from**
  Here, the momentary broadcasts in the current 4-minute interval are listed. Each line contains two senders each with the following information:
  - The MAC address of the broadcast sender
  - The number n of broadcasts since the beginning of the interval
  - The number GI of successive identical telegrams
  - The length Len of the telegrams

Here now the complete overview of the individual information of the Statistic. The setpoints are only specified if they are static.

Name	Setpoint	Description
RxFrames		Counter for telegrams received which are forwarded to module applications and the TCP/IP stack.
BD out of sequence	0	Counter for receive buffer overflows in the communications processor. This value must always be zero.
Miss		Counter for telegrams received that do not match the MAC address of the device.
Broadcast		Counter for broadcast telegrams received
Multicast		Counter for multicast telegrams registered
More than 0x5f0 Bytes		Counter for telegrams (1520 bytes) that are too long. Such telegrams are discarded.
Non Octett	0	Counter for the number of bits which cannot be divided by 8. If this value is not equal to zero, there may be problems on the transmission link. This can also be the case if the link is physically broken.
CRC Error	0	Counter for telegrams received with a CRC-check error. Indicates possible problems on the transmission link.
Overrun	0	Counter for receive buffer overflow. Indicates possible performance problems of the Ethernet controller.
Truncated	0	MAC-internal counter. Counter for reduced telegrams received (> 2 kb)
TxFrames		Counter of telegrams transmitted.
no transmit buffer	0	Incrementing can only happen if the collision or retransmission volume is very high.
FNS queue overflow	0	Counts broadcast telegrams which were not evaluated because of a processor overload. Activation usually due to circulating telegrams.

Name	Setpoint	Description
Frames Loss	0	Counts of discarded received telegrams; if more than 1000 such telegrams have arrived per second. Can only occur with circulating telegrams.
MaxRxBDs		Max. level of the receiving buffer.
RxLoopMax	0	Counter for receiving buffer overrun.
RxOverload	0	Counter for receiving overload. Receiving telegrams are lost.
TxDef	0	Counts the 'defers' when sending frames. An incrementation of the counter indicates that half duplex mode is set.
TxHB	0	Heartbeat counter
TxLC	0	Late Collision counter
TxRL	0	Counts violations of the retransmission limit
TxRC	0	Counts retransmissions. Indicates collisions
TxUN	0	Counts 'Buffer underrun'
TxCSL	0	Counts 'Carrier sense lost'
MaxTxBD		Max. level of the transmitting buffer.
nGooseHit		Counts the GOOSE telegrams received
nGooseMiss		Counts the GOOSE telegrams which passed the multicast filter, but are not addressed to the device (e.g. by incorrect GOOSE-parameterization).
Relative time		Momentary value of the relative time counter. This is a 32 bit counter which is incremented once per millisecond. Starts at 120000 (is equal to appr. 49 days, after it reboot with 0).
Module CPU load		Efficiency CPU
txPacketChan1/2		Counts of data packages, which was sent by the port.
rxPacketChan1/2		Counts of all data packages, which was received by the port.
FilterSrcChan1/2		Counter of all received data packages, which doesn't agree with all received data packages of the source address with the own address.
FilterDstChan1/2		Counter of all received data packages, which doesn't agree with all received data packages of the destination address with the own address.

Name	Setpoint	Description
FilterCRCErrCnt Chan1/2	0	Counter of data packages with CRC error
FilterLenErrCnt Chan1/2	0	Counter of data packages, which are too long or too short. The acceptable length is 64 bytes to 1518 bytes.
FilterSymErrCnt Chan1/2	0	Counter of received symbol errors on the line (4b5b value is invalid). This monitoring is completed by the Phy.
overflowExtCnt Chan1/2	0	No counter for this value.
overflowIntCnt Chan1/2	0	No counter for this value.
overflowIntTraCnt	0	No counter for this value.
OptLevelChan1/2	> 2300	Level of the optical receiver in mV. Should not be less than 2300 when the cable is connected.
EPLD Version		Current EPLD version
Malloc Size		primary storage management
Data Size, Code Size, NORMAL pool, ENTRY pool, GOOSE pool, WEAK pool		primary storage management

What Else You Should Know

13

In this chapter we have put together some information that is useful and informative.

Setting Up a Hyper Terminal Connection

For all those who have never done it and even for those who can't remember we will describe how to set up a hyper terminal connection in this section.

You implement a hyper terminal connection exclusively with Windows standard tool facilities. The advantage: You don't need any additional software for it. The disadvantage: Depending on the operating system version, the procedures vary. We will now briefly describe how you set up and start a hyper terminal connection under Windows XP.

First connect PC and switch using the 1:1 modem cable and turn on both devices.

Off into Hyperspace

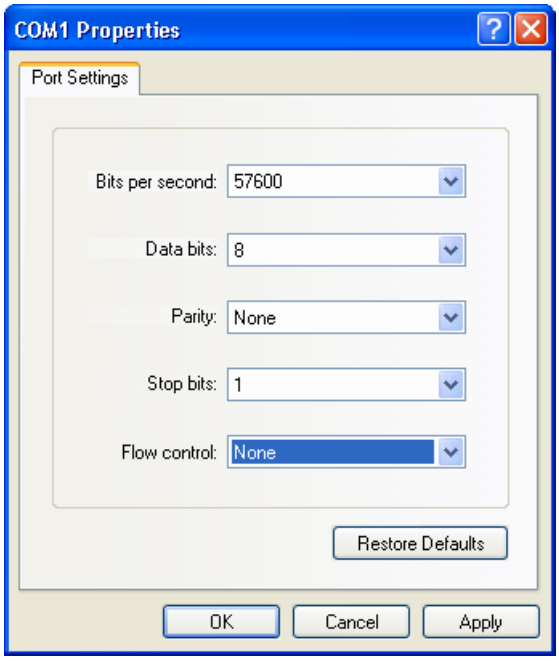
Click the Start menu and select **All Programs** → **Accessories** → **Communications** → **Hyper Terminal**. Windows goes into expectation mode with the following dialog:

Step-by-step to the finish: First the name, ...

Enter a name for the new hyper terminal connection here and select one of the suggested icons for it. After that click **OK** as usual. Windows doesn't let go yet and introduces a further dialog right after that.

... then the COM port, ...

From the **Connect using:** list select the PC's serial interface ID to which you have connected the 1:1 modem cable. In that way the rest of the input fields are deactivated and your initial shock about the supposed necessity for some telephone numbers is surely eased. However, Windows is still not appeased and demands additional data.



... and finally, define some parameter values.

The settings suggested as default by Windows don't really want to fit to our requirements. For that reason, please change these so that they coincide with the values shown above.

With a click on **OK** you complete setting up the hyper terminal connection. However, you still have to explicitly save this so that you can refer back to the defined settings at any time. A click on **Save** in the **File** menu of the terminal window suffices. We had already defined the name **Set Switch** at the beginning of the whole act. As of now, you can open the hyper terminal with the selected settings directly via the Start menu, so in our case with **All Programs → Accessories → Communications → Hyper Terminal → Set Switch**. (Here for once brevity is *not* the soul of wit.)

Saving and Loading Switch Configurations

Five switches, like in our sample configuration, are still easy to handle. With somewhat larger systems this could very quickly become fifty switches however. Then it comes in handy when you can save a switch configuration, change it a little as required, and then be able to push as many other switches as possible under it. Prerequisite for this, though, is that the switches are all of the same type.

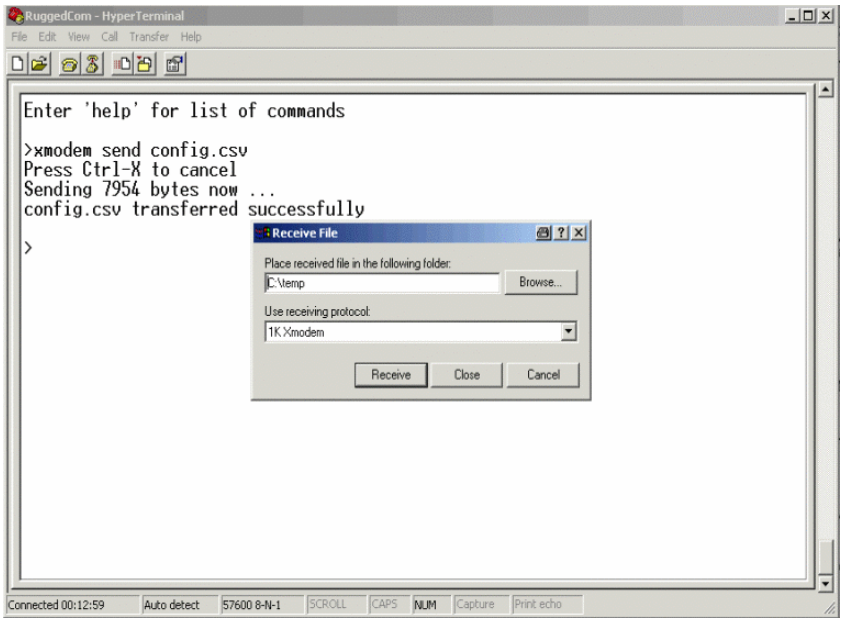
The configurations are stored as CSV files and therefore as text that can be edited. A simple text editor is completey sufficient for later editing; with which you then change the IP address, for example. By the way, the configuration files can also be read out and then read back in via batch file - nothing stands in the way of efficient working any longer.

Out ...

The configuration must be read out of the switch. To do so, you once more require an active hyper terminal connection to this. In the command area enter **xmodem send config.csv** and then select **Transfer → Receive File**, which will lead to the display of a dialog. For receiving information, we also use this protocol **1Kxmodem**. You can define the destination and name of the configuration file any way you like. Click **Receive**: The data is transferred from the switch into the PC and stored there.

... and In

To load an existing configuration in a switch you proceed exactly like you do for a firmware update, in principle. Type the command **xmodem receive config.csv** into the terminal window. Then, with the command **Send File**, that you find in the menu **Transfer**, open the dialog **Send File**. Once more select **1Kxmodem** as the send protocol and specify the name and path of the configuration file. After clicking **Send,** the PC transfers the data to the switch.



Time saving: Configurations can be saved and loaded.

In Larger DOSes

Wouldn't it be practical to be able to read out CSV files in larger quantities and then be able to load them back into the switch? That works very easily with batch files and a tftp connection. The Microsoft operating systems bring along a tftp-client that you use via the good old DOS command line. We'll show you first off how this basically works with just one individual file.

From the Start menu, select the command **Run** and then type **Command** in the input field. After clicking **OK,** Windows opens the DOS window. Here you now enter roughly the following:

```
tftp 172.16.0.1 get config.csv c:\Config\Switch_1.csv
```

As IP address enter that of the switch whose configuration file you want to read out. **C:\Config\Switch_1.csv** corresponds to the destination and the target name of the file. You have to adapt this information, of course.

As soon as you press the Enter key, the command is sent off and as an answer you get the desired file. Prerequisite, of course, is that the switch in question and the PC are able to communicate via the network.

Loading the configuration file into the switch works along the same principle:

```
tftp 172.16.0.1 put c:\Config\Switch_1.csv config.csv
```

To rationalize the reading out, we will now pack all get-commands into one batch filed called **get.bat**. This will then look like this for the five switches in our sample topology:

```
rem Read out all csv files
tftp 172.16.0.1 get config.csv C:\Config\Switch_1.csv
tftp 172.16.0.2 get config.csv C:\Config\Switch_2.csv
tftp 172.16.0.3 get config.csv C:\Config\Switch_3.csv
tftp 172.16.0.4 get config.csv C:\Config\Switch_4.csv
tftp 172.16.0.5 get config.csv C:\Config\Switch_5.csv
> get.txt
pause
rem end
```

Similarly, the file **put.bat** shows up for loading the configurations as follows:

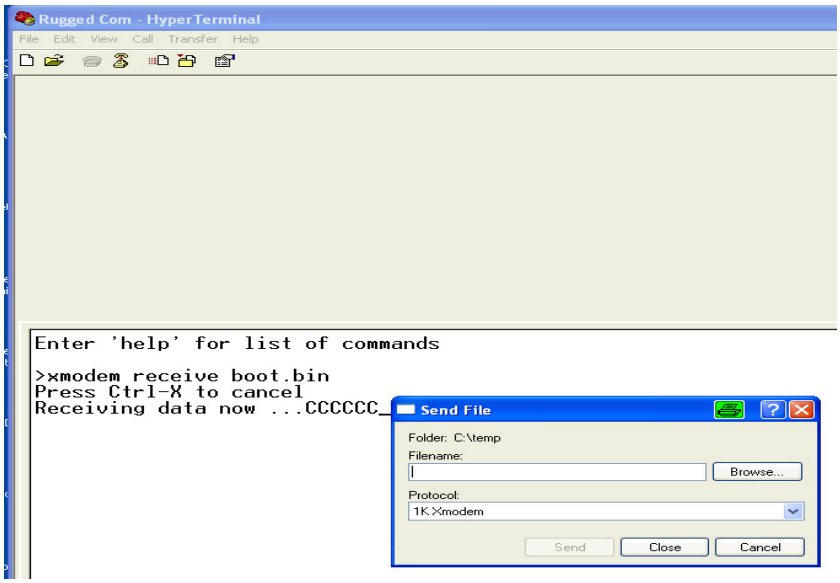
```
rem Load all csv files
tftp 172.16.0.1 put C:\Config\Switch_1.csv config.csv
tftp 172.16.0.2 put C:\Config\Switch_2.csv config.csv
tftp 172.16.0.3 put C:\Config\Switch_3.csv config.csv
tftp 172.16.0.4 put C:\Config\Switch_4.csv config.csv
tftp 172.16.0.5 put C:\Config\Switch_5.csv config.csv
> put.txt
pause
rem end
```

Loading New Firmware in the Switch

If we proceed on the notion of ideal conditions, then you have just stocked up on brand-new switches equipped, of course, with the most current firmware. Often, however, several days or even weeks go by before the newly purchased switches get put to use. While these are now lying around on the shelf waiting for their mission, it could quite possibly happen that the manufacturer gets some ideas on how to improve one or the other function. For you it means first finding out whether there is a more current firmware than the one loaded into the switch. And more than anything else, this becomes particularly true for switches that you have had in operation for a longer period of time. For the RS 8000 T and RS 1600 switches recommended by us, you will find possible firmware updates under www.ruggedcom.com. A complete patch consists of two files: boot.bin and main.bin.

Now One after the Other

The following is generally valid for a firmware update: First load the file **boot.bin** in the switch, then the file **main.bin**. Therefore, first type the command **xmodem receive boot.bin** in the display area of the terminal window. Then, using the command **Send File** that you will find in the menu **Transfer,** open the dialog **Send File**.



Rejuvenation: Per hyper terminal, you update the switch's firmware. (Abb. vorl.)

From the list of available send protocols, select **1Kxmodem**. In the input field above it, either enter the name **boot.bin** including the complete path directly or choose the file via the search dialog. With a click on **Send,** exactly this should happen. Prerequisite: There is a connection between PC and switch. This can easily be determined by the telephone icons in the toolbar.

If everything worked out OK, repeat the procedure, but this time with the file **main.bin**. Then interrupt the connection and carry out a reset on the switch.

Swapping Modules

If you would like to prepare your much loved longtime device for its new task as networker, then you can already lay out the tools. For it will be necessary in any case to swap the presently installed communication module for one of the type EN100. No matter what, you have to take the following sequence to heart:

1. Update the device firmware to Version 4.6.
2. Remove the existing module.
3. Insert the EN100 module.
4. Load the module firmware into the device.
5. Test the availability of the new module.

Should you mix up this sequence, it is quite possible that after the module is installed, the device can no longer be operated. Removing the module with the subsequent downgrade is then the consequence and, last but not least, the expense in considerably higher than necessary.

Psycho-analysis 1

The exact description, when and how you update the firmware of a device and what you have to pay attention to, fills about 30 pages with all its details. That is why there is an independent document for this which you can get under **www.siprotec.com**. Concealed behind the entry **Devices,** you will not only find the necessary information on procedures, you will also find current firmware updates and device drivers for DIGSI 4. We would like to give you a glimpse here and for that reason will briefly outline the fundamental stations on the path from an older to a newer firmware version.

- First check whether you even need a firmware update for the SIPROTEC 4 device in question and whether the device is suited for a firmware update. If yes, then download the update files from the SIPROTEC website.
- Check whether it will become necessary to supplement your DIGSI 4 installation because of the firmware update. This is always the case when the first digit after the decimal point of the firmware version's identification has changed. You can also obtain the necessary update files on the SIPROTEC website.
- Before the firmware update, use DIGSI 4 to save the parameter set that is currently in the device. Also read out all process data from the device.
- Install the firmware loading program onto your PC. You can download this as well from the SIPROTEC website.
- De-energize the device and connect it to your PC.
- Update the firmware.
- Commission the device and test the functionality.

If everything goes smoothly, you can then swap the communication module without a second thought.

Prepareing for Operation

First, the best thing to do is gather up all the tools you will need. They are ...

- ... a pad that is suitable for electrostatically-sensitive components,
- a flat-bladed screwdriver with a width of 5 mm to 6 mm,
- a crosstip screwdriver Pz size 1 and
- a socket wrench with a width of 4.5 mm.

While you're at it, unpack the new module and have it ready.

Before you open up the housing, you must disconnect all lines on the SIPROTEC 4 device from the power supply; you simply have to take the time! Also loosen any other possible connections to the device.

Turn-over the Patient

Next, start on the backside of the device. Using the crosstip screwdriver, remove all the screws with which the built-in communication module is secured. With the socket wrench, remove the two bolts of the DSUB socket.

Swing the device by 180 degrees and then remove the four screw covers on the front. With that, we mean the small rectangular plastic covers on the upper and lower edges, on the left and right-hand sides. Then loosen the slotted-head screws that are located underneath these covers.

The Operation Begins

Now slowly pull off the device's front plate and carefully turn it to the side. But not too far because the front plate and the board in the housing are still connected to one another through the ribbon cable. You have to loosen the ribbon cable's plug connector from the board. To do so, slightly flip the locking levers upward or downward until the plug connector is pushed out. And while you're at it, please do the same for the plug connector on the second ribbon cable that establishes the connection to the neighboring board.

Next, pull the board out of the housing and place it on the pad; the communication module that is installed in the unit must be facing down. Completely remove the communication module's two retaining screws. Then, turn over the board and lift off the module. Fit the new communication module onto the board by pressing lightly, turn the board over and fasten the module with the two screws.

Now slide the board back into the housing. Use the existing markings to orient yourself. Connect the board to the plug connectors. In the process, make sure that the locking levers snap in securely.

Operation Completed

The rest of the procedure is child's play:

- Mount the front plate giving slight pressure,
- Screw in the screws,
- Mount the covers,
- On the back, screw in the screws for the communication module.

If you would like to see what we have just explained to you in a small film, we have a tip for you: On the CD "SIPROTEC 4 You – Start Up", you will find an animated operating instruction that shows you the procedure for swapping communication modules. There is also a detailed description which you can download from **www.siprotec.com**. You will find it in the area **Devices > General Information**. Now apply voltage once more to the device.

Psycho-analysis 2

Modules are usually supplied with the module firmware already loaded. If for some reason you possess a module without firmware, you must load it after you have installed the module. More than likely, however, you would probably like to update the firmware of a module. You can get information about possible updates from the SIPROTEC website. By the way, the module firmware is the same for all module types as of Version 3.0. There is no difference for modules with electric and optic interface or for built-in and surface-mounted versions.

You load the firmware itself, similar to the update procedure of the device firmware, via the front interface into the device and thus onto the module. After that, switch off the protection device's auxiliary voltage for a few seconds and then switch it back on. This then completes the firmware and parameter update.

Reading Out and Saving the Printf.html and fecst.html

The module homepage of an EN100 module provides you with a series of useful information, among other things also the contents of the printf buffer and the Statistic. You can activate the homepages one after the other via the IP addresses of the SIPROTEC 4 devices and manually store the HTML pages named. But there's an easier way to do it. With a very helpful tool named Curl and a small batch file, you can complete this task in a lot less time. Curl is freeware that you can easily download from the Internet.

The syntax for activating Curl is anything but complicated:

```
curl -o printf_1_380.html http://172.16.10.1/printf
```

In this example, fetch the Printf page from the device with the IP address 172.16.10.1, and save this as printf_1_380.html. The batch file for all devices in our sample topology then looks like this:

```
rem Read out all printf and fecst pages
curl -o printf_1_380.html http://172.16.10.1/printf
curl -o fecst_1_380.html http://172.16.10.1/fecst
curl -o printf_2_380.html http://172.16.10.2/printf
curl -o fecst_2_380.html http://172.16.10.2/fecst
curl -o printf_3_380.html http://172.16.10.3/printf
curl -o fecst_3_380.html http://172.16.10.3/fecst
curl -o printf_4_380.html http://172.16.10.4/printf
curl -o fecst_4_380.html http://172.16.10.4/fecst
curl -o printf_5_380.html http://172.16.10.5/printf
curl -o fecst_5_380.html http://172.16.10.5/fecst
curl -o printf_1_30.html http://172.16.100.1/printf
curl -o fecst_1_30.html http://172.16.100.1/fecst
curl -o printf_2_30.html http://172.16.100.2/printf
curl -o fecst_2_30.html http://172.16.100.2/fecst
curl -o printf_3_30.html http://172.16.100.3/printf
curl -o fecst_3_30.html http://172.16.100.3/fecst
curl -o printf_4_30.html http://172.16.100.4/printf
curl -o fecst_4_30.html http://172.16.100.4/fecst
curl -o printf_5_30.html http://172.16.100.5/printf
curl -o fecst_5_30.html http://172.16.100.5/fecst
pause
rem End
```

Automated RSTP Status Check

In Chapter 12, we showed you how you can find out about the Alternate Port, for example. The methods described may pass for commissioning but for the running operation, they are not practical. We need a method that enables us to demand various information from several devices simultaneously and then to have it presented ready made.

This could then look like this: You start a file that in our case is called **scan.bat**, and in a blink of an eye, the PC spits out a file named **Data.dat**. Quickly open the file with an editor of your choice and it shows us information from its best side, filtered according to our requirements and clearly formated:

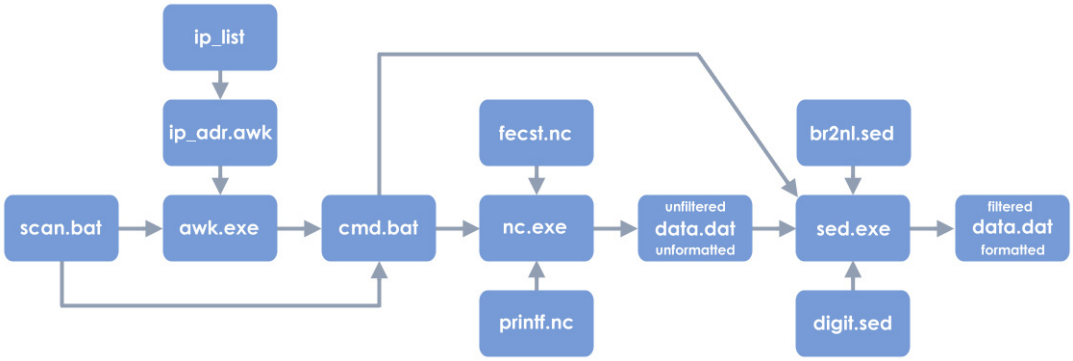
```
...
---------- 172.16.10.1 -------
IP = 172.16.10.1
MAC = 8-0-6-86-58-a7
nGooseHit = 12423
nGooseMiss = 0
RSTP-Role Chan1/2 = Designated/Root (Break 1<==2)
RSTP-State Chan1/2 = Forwarding/Forwarding
---------- 172.16.10.2 -------
IP = 172.16.10.2
MAC = 8-0-6-86-58-a9
nGooseHit = 52158
nGooseMiss = 0
****** --> RSTP-Role Chan1/2 = Alternate/Root <-- ******
RSTP-State Chan1/2 = Discarding/Forwarding
---------- 172.16.10.3 -------
IP = 172.16.10.3
MAC = 8-0-6-86-58-b4
nGooseHit = 18833
nGooseMiss = 0
RSTP-Role Chan1/2 = Root/Designated (1==>2 Break)
RSTP-State Chan1/2 = Forwarding/Forwarding
...
```

In our example you see which roles and states the individual ports momentarily have and you learn, with the counters **nGooseHit** and **nGooseMiss**, how it is with the hit rate for GOOSE telegrams. IP and MAC addresses make assigning information to the individual devices simple.

The way it works is actually quite simple. With Scan.bat, you start a procedure which reads out the Statistics and the printf buffer contents of all desired devices, gathers them up in a file and then filters and formats them. Filter criteria and format instructions can be adapted and in that way you determine the form and contents of the information to be supplied.

All that sounds good, and it is, but there is just one little hitch. That is, if the printf buffer of a device should have overflowed because of a multitude of indications, then it is quite possible that the information you are interested in is no longer available. We do think however that you can live with this little disadvantage.

A graphic should first of all illustrate which components play a role between Scan.bat and Data.dat. Three little programs take part: nc.exe, awk.exe and sed.exe - all freeware you download from the Internet.



Keep it going from left to right

Let's simply start in the middle and cast an eye on the file **nc.exe** alias NetCat. This is the actual tool that obtains the information from the individual devices. Everything to the left of it in the graphic makes our work easier so that NetCat queries all devices one after the other with just one double-click. Everything to the right of the middle removes the information from the superfluous ballast and presents it in a stately format. To motivate NetCat to work, this program expects a call according to the following structure:

```
nc hostadr port < script > file
```

As you can see, NetCat requires some information. The host address is the IP address of the device from which you need information. The port has nothing to do with a hardware port of an EN100 module, but identifies a software port. In conjunction with TCP/IP, always use the value 80 for this. A script defines exactly what NetCat is to do. (The contents of this script follows immediately.) And finally, NetCat still has to know where the new-found knowledge is to go. In our case it is the file **Data.dat**.

Since we want information from two different sources, namely fecst and printf, we also need two scripts for NetCat.

Script 1 for procuring the Statistic is:

```
GET /fecst HTTP/1.1
--- blank line ---
```

Script 2 for procuring printf is:

```
GET /printf HTTP/1.1
--- blank line ---
```

Please note that immediately after the command **GET ...** exactly one blank line must follow, otherwise the scripts don't work.

For each device, NetCat must be called twice. That can be quite a bit when you have an average network topology. Therefore, it makes sense to combine all calls in one batch file. This should be called cmd.bat and look like this, for example:

```
@REM
@echo Scanning 172.16.10.1 ...
@nc 172.16.10.1 80 < printf.nc > data.dat
@nc 172.16.10.1 80 < fecst.nc >> data.dat
@REM
@echo Scanning 172.16.10.2 ...
@nc 172.16.10.2 80 < printf.nc >> data.dat
@nc 172.16.10.2 80 < fecst.nc >> data.dat
@REM
@echo Scanning 172.16.10.3 ...
@nc 172.16.10.3 80 < printf.nc >> data.dat
@nc 172.16.10.3 80 < fecst.nc >> data.dat
@REM
@echo Scanning 172.16.10.4 ...
@nc 172.16.10.4 80 < printf.nc >> data.dat
@nc 172.16.10.4 80 < fecst.nc >> data.dat
@REM
@echo Scanning 172.16.10.5 ...
@nc 172.16.10.5 80 < printf.nc >> data.dat
@nc 172.16.10.5 80 < fecst.nc >> data.dat
@echo.
@echo ==================
@echo.
@sed -f br2nl.sed data.dat | sed -n -f digit.sed
```

The **cmd.bat** file shown initiates the successive scanning of five devices. After that, the command in the last line starts the stream editor **sed.exe**. More on that later.

By the way, you don't have to create the batch file manually. You can quite conveniently let the program **awk.exe** generate it. For this, the program must still receive structural information and it must know about the IP addresses of the devices that are to be scanned. The associated batch command for activating awk.exe then looks like this:

```
@awk -f ip_adr.awk ip_list
```

Behind ip_adr.awk there lies a script that instructs awk.exe as to which structure it should use to generate cmd.bat. You can accept this in the form it comes in and as far as that goes we don't want to go into more detail about the individual command sequences here. More important in this connection is the file **ip_list**. In it, you must enter line-by-line the IP addresses of all devices whose information you are interested in.

Here an example for ip_list:

```
#
# IP addresses of all devices
#
172.16.10.1
172.16.10.2
172.16.10.3
172.16.10.4
172.16.10.5
```

As you already know, you start the whole procedure with Scan.bat. One look in this file reveals that it initiates two things.

```
@REM
@REM Scan all addresses from “ip-list”
@REM
@awk -f ip_adr.awk ip_list
@call cmd.bat
```

Scan.bat first of all starts the program **awk.exe** and hands over the required files **ip_adr.awk** and **ip_list**. With the help of the information in these files, awk.exe generates the batch file **cmd.bat**. Scan.bat activates this file with a Call instruction. After that, NetCat contacts one device after the other, extracts the information from both the Statistic and the printf buffer and transfers these in turn into the file **Data.dat**.

After its work is done, NetCat leaves all the information in this file that could be gotten from the sources. We actually only need a very limited portion of it but in a reasonable visual quality. To first filter and then format the stored information is now the task of sed.exe. This streaming editor takes in data on the one side that it spits out on the other side by means of different patterns and criteria, then, however, in a usually reduced and orderly format.

Now let’s take a look at the call of sed.exe that you find as the last line in the batch file cmd.bat:

```
@sed -f br2nl.sed data.dat | sed -n -f digit.sed
```

Here as well, the actual instructions are not given directly but rather as reference to two script files: br2nl.sed and digit.sed. The first of these increases the readability of the information by generating a line-by-line representation. For that, all line separators in the original HTML format are simply replaced by a ↲-character. The script only needs an instruction line for this.

```
s/<BR>/\n/g
```

The second script is a little more complicated since it must filter and then format the information. This shouldn’t bother you though for you can adopt it 1:1 in principle.

Here the script:

```
1 /external IP/ {
2 h
3 s/.+\(IP=[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+\).+$/\1/
4 s/IP=\(.+\)/\nIP = \1/
5 p
6 g
7 s/.+\(MAC=[0-9a-fA-F]+-[0-9a-fA-F]+-[0-9a-fA-F]+-[0-9a-
fA-F]+-
8 [0-9a-fA-F]+-[0-9a-fA-F]+.+$/\1/
9 s/MAC=\(.+\)/MAC = \1/p
10 }
11 /RSTP-/ {
12 /Alternate/ {
13 s/\(.+$\)/\n**********\n\1\n**********/
14 }
15 p
16 }
17 s/nGooseHit[ \t]+=\(.+$\)/nGooseHit = \1/p
18 s/nGooseMiss[ \t]+=\(.+$\)/nGooseMiss = \1/p
19 s/\(^-------.+$\)/\n\1/p
```

If further information is relevant for you, then supplement the script after Line 18 with additional instructions which you formulate like those out of Lines 17 and 18.