Ethernet & IEC 61850

Konzepte, Umsetzung, IBS

Handbuch

Inhaltsverzeichnis

Ausgabe: 16.09.2011

E50417-F1100-C361-A4

Hinweise zu Ihrer Sicherheit

Dieses Handbuch stellt kein vollständiges Verzeichnis aller für einen Betrieb des Betriebsmittels (Baugruppe, Gerät) erforderlichen Sicherheitsmaßnahmen dar, weil besondere Betriebsbedingungen weitere Maßnahmen erforderlich machen können. Es enthält jedoch Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise sind durch ein Warndreieck hervorgehoben und je nach Gefährdungsgrad wie folgt dargestellt:

Warnung

bedeutet, dass Tod, schwere Körperverletzung oder erheblicher Sachschaden eintreten können, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

bedeutet, dass eine leichte Körperverletzung oder ein Sachschaden eintreten können, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Qualifiziertes Personal

Inbetriebsetzung und Betrieb eines in diesem Handbuch beschriebenen Betriebsmittels (Baugruppe, Gerät) dürfen nur von qualifiziertem Personal vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieses Handbuches sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, freizuschalten, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch

Das Betriebsmittel (Gerät, Baugruppe) darf nur für die im Katalog und der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und -komponenten verwendet werden.

Der einwandfreie und sichere Betrieb des Produktes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie Bedienung und Instandhaltung voraus.

Beim Betrieb elektrischer Betriebsmittel stehen zwangsläufig bestimmte Teile dieser Betriebsmittel unter gefährlicher Spannung. Es können deshalb schwere Körperverletzung oder Sachschäden auftreten, wenn nicht fachgerecht gehandelt wird:

- Vor Anschluß irgendwelcher Verbindungen ist das Betriebsmittel am Schutzleiteranschluß zu erden.
- Gefährliche Spannungen können in allen mit der Spannungsversorgung verbundenen Schaltungsteilen anstehen.
- Auch nach Abtrennen der Versorgungsspannung können gefährliche Spannungen im Betriebsmittel vorhanden sein (Kondensatorspeicher).
- Betriebsmittel mit Stromwandlerkreisen dürfen nicht offen betrieben werden.

Die im Handbuch bzw. in der Betriebsanleitung genannten Grenzwerte dürfen nicht überschritten werden; dies ist auch bei der Prüfung und der Inbetriebnahme zu beachten.

Dokumentenversion: V01.03.00

Inhaltsverzeichnis

Was Sie erwartet

1

Rechner und Co haben längst nicht mehr das Monopol auf Netzwerkfunktionen. Vom früher einzigen Refugium Büro haben sich diese aufgemacht, um in neuen Räumen anderen Anwendungen dienlich zu sein. Und möglicherweise gehören Sie selber bereits zu denen, die sich zuhause den Komfort eines Medienservers gönnen, der Bilder, Videos und Musik bereit hält. Da liegt es doch nahe, auch dort wieder mit der Zeit zu gehen, woher die Power kommt, die alles antreibt.

Alles einsteigen, bitte!

Ethernet heißt nun also auch für die Kommunikation im Energiebereich die Devise, am besten in Verbindung mit IEC 61850. Manches bleibt dabei so, wie es schon immer war, doch vieles ist anders an dieser neuen Art zu kommunizieren. Wer sich also bei der Konzeption und Inbetriebnahme seiner ersten IEC 61850-Anlage nicht auf den Zufall verlassen, aber dennoch nicht vorab Kilos von Literatur verschlingen will, ist mit diesem Buch gut beraten. Sie erfahren hier nicht alles, aber vieles, was Ihnen zu einem vernünftigen Einstieg in die Thematik verhelfen wird.

Trilogie

Im Grunde genommen lässt sich das Buch inhaltlich betrachtet in drei Teile zerlegen. Im ersten Teil erläutern die Kapitel 2 bis 4 die Grundlagen der Kommunikation über Ethernet. Dabei steht eine Übersicht zu möglichen Topologien an erster Stelle. Weiter geht es mit kompakter Netzwerktheorie, die Ihnen wichtige Grundbegriffe und -verfahren näher bringen soll. Mit einigen wichtigen Bemerkungen zu den einzelnen Komponenten, die für eine Ethernet-Kommunikation benötigt werden, verlassen wir den eher abstrakten ersten Teil.

Im zweiten Teil wenden wir uns dem Realismus zu und stellen Ihnen in Kapitel 5 eine praxisgerechte Beispielkonfiguration vor. In den weiteren Kapitel 6 bis 10 beziehen wir uns immer wieder auf diese, um Ihnen alle Vorbereitungen zu erläutern, die auf dem Weg zu einer funktionierenden Kommunikation via Ethernet notwendig sind.

Im letzten und dritten Teil heißt es dann: Anschließen, einschalten und prüfen. Die drei Kapitel 11, 12 und 13 haben sich freundlicherweise bereit erklärt, Ihnen dazu Rede und Antwort zu stehen.

Lesetipp

Sind Sie bereits vertraut mit Begriffen wie Netzmaske, Ringtopologie, MAC-Adresse und so weiter, dann steigen Sie doch gleich bei Kapitel 5 ein. Verfügen Sie jedoch noch nicht über dieses nötige Basiswissen, dann empfehlen wir Ihnen in jedem Fall die Lektüre der Kapitel 2 bis 4.

Ruf mich an

Falls Sie weitere Fragen zur Thematik haben, erhalten Sie Unterstützung bei unserer Hotline:

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

Bildungs-maßnahmen

Das individuelle Kursangebot erfragen Sie bei unserem Trainingcenter. Dort bietet Siemens Ihnen ausführliche Kurse zur Projektierung und Inbetriebsetzung von IEC 61850-Anlagen und zu DIGSI 4.

Siemens AG
Energy Sector
Power Distribution Division
Humboldtstr. 59
90459 Nürnberg
Tel.: 09 11/4 33-70 05
Fax: 09 11/4 33-79 29
Internet www.siemens.com/power-academy-td

Hinterm Horizont geht´s weiter

Wenn Sie an weiteren Informationen interessiert sind, hier eine Auswahl an Bestellnummern zum Thema Ethernet und IEC 61850.

- Handbuch **DIGSI 4 Start Up**
  C50417-G1100-C152-A2
- Handbuch **Ethernet & IEC 61850 Start Up**
  E50417-F1100-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

Ganz besonders ans Herz legen möchten wir Ihnen das Buch Linux-Netzwerkadministration von Jens Banning - und zwar ausdrücklich auch allen Windows-Benutzern. Denn dieses Buch beschreibt sehr verständlich grundlegende Themen wie TCP/IP, Anbindung ans Netzwerk, Routing, etc. Erschienen ist dieses Buch im Verlag Addison-Wesley unter der ISBN 3-8273-1855-6.

Die geeignete Topologie wählen

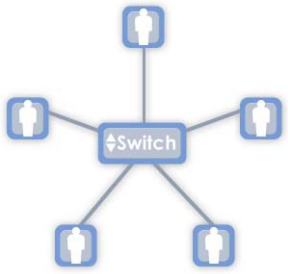
2

Bevor Sie beginnen, die ersten Strippen zu verlegen, muss die Frage der physischen Topologie geklärt sein. Welche Verbindungsstruktur der einzelnen Geräte untereinander dabei für Sie geeignet ist, wird letztlich von unterschiedlichen Faktoren beeinflusst sein. So spielt der Wunsch nach Redundanz eine Rolle, aber auch die räumliche Ausdehnung des benötigten Netzwerkes wird bei der Wahl einer Konfiguration mitbestimmend sein. Vielleicht ist die Entscheidung für Sie auch längst gefallen, dann können Sie dieses Kapitel überspringen.

Falls Sie jedoch weiterlesen, werden Sie unsere beiden Favoriten aus dem Bereich der Netzwerktopologie kennen lernen: Stern und Ring. Aus dem Pool der Netzwerktopologien, zu denen auch die Bustopologie, die Baumstruktur oder das vermaschte Netz gehören, haben sich diese beiden Topologien als einzig brauchbare Vertreter für unsere praktischen Zwecke herauskristallisiert.

Sternstunde

Bei der **Sterntopologie** treffen sich die Anschlüsse aller Teilnehmer im selben Punkt - zumindest gedanklich. Da wir die einzelnen Anschlüsse schlecht direkt miteinander verbinden können, benötigen wir in der Praxis einen Verteiler.



Switch der Mitte: Die Sterntopologie benötigt einen Verteiler.

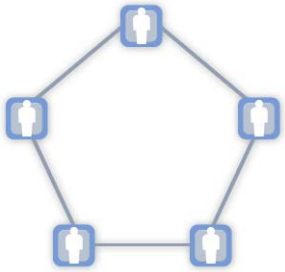
In Ethernetnetzwerken hat sich der intelligente Switch zum Verteilen der Daten etabliert und hat damit den dumpen Hub ziemlich ins Aus gedrängt. Die einzelnen Teilnehmer untereinander entbehren dagegen jeglicher direkter physischer Beziehung.

Die einzelnen Kommunikationsteilnehmer haben wir zunächst als kleine Figuren stilisiert. Es kann sich dabei um PCs, aber auch um Geräte der Sekundär- und Automatisierungstechnik handeln. Bei der Kommunikation über Ethernet nach IEC 61850 werden sogar Router und Zeit-Server als Teilnehmer bezeichnet.

Die Sterntopologie lässt hohe Übertragungsraten zu, besitzt eine klare und verständliche Struktur und kann leicht erweitert werden, wenngleich auch verbunden mit einer aufwändigen Verkabelung. Der Ausfall eines Endgerätes hat keine Auswirkung auf den Rest des Netzes. Dagegen legt ein defekter Verteiler das gesamte Netzwerk lahm.

Herr der Ringe

Wer eher auf runde Sachen steht, greift zur **Ringtopologie**. Hier ist jedes Endgerät mit genau zwei anderen verbunden, sodass ein geschlossener Ring entsteht.



Kreisverkehr: Die Ringtopologie ist ein geschlossenes System.

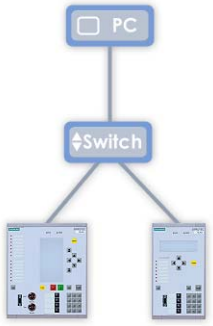
Informationen werden in diesem von Teilnehmer zu Teilnehmer weitergeleitet, bis sie ihr Ziel erreicht haben. Dabei wurde es früher kritisch, wenn es im Ring zu einer Unterbrechung kam. Dieser Einwand gilt heute jedoch nicht mehr: Wird der Ring an einer Stelle unterbrochen, wird automatisch auf Linienbetrieb umgeschaltet, die Kommunikation kann nahezu unterbrechungsfrei fortgeführt werden. Wie wir noch sehen werden, spielen auch dabei Switches eine wesentliche Rolle.

Sterntopologie

Der Stern ist wohl die für kleine Netzwerke am häufigsten verwendete Topologie. Das mag an seiner unkomplizierten (Hardware-)Installation liegen, die gerade für kleine Teams einen schnellen und bisweilen auch fliegenden Aufbau zulässt. Ein paar Kabel und ein Verteiler (Switch oder Hub) genügen, wenn Sicherheitsanforderungen keine Rolle spielen.

Klein anfangen

Das Bild auf der nächsten Seite zeigt dann auch die wohl einfachste Sternstruktur der Welt, auf das Nötigste reduziert. In einer solchen Topologie ist mindestens ein so genannter Switch erforderlich, der die einzelnen Kommunikationsteilnehmer miteinander verbindet. In unserem Bild sind das nur drei (2 x SIPROTEC 4, 1 x PC), tatsächlich können an einen Switch mehrere Teilnehmer angeschlossen werden. Wie viele, hängt von der Anzahl der Schnittstellen (= Ports) des Switches ab.

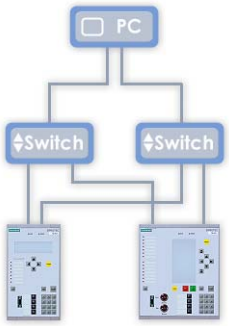


Sternenbasis: Simple Struktur, dafür aber null Redundanz.

Reicht ein Switch nicht für alle Teilnehmer aus oder erfordern es die lokalen Gegebenheiten, können auch mehrere Switches verwendet werden. Diese werden dann untereinander verbunden. So lassen sich auch größere Strukturen realisieren.

Doppelt gemoppelt

Die oben gezeigte Struktur ist zwar simple, aber gleichzeitig auch bar jeglicher Redundanz: Streikt die Netzkarte des PCs, können Informationen nicht mehr abgefragt, Befehle nicht mehr gesendet werden. Fällt eine Geräteschnittstelle aus, ist auch das zugehörige Gerät unerreichbar. Und versagt der Switch, dann geht gar nichts mehr. Noch nicht optimal, aber bereits ein wenig besser sieht es da mit der folgenden Konfiguration aus.



Basiserweiterung: Switches und Netzwerkadapter am PC sind doppelt vorhanden.

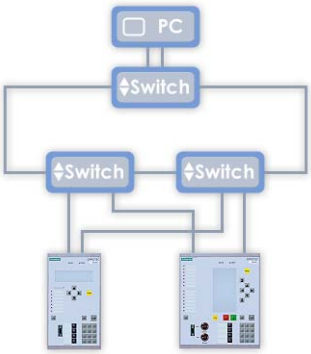
Bei dieser Struktur verdoppeln wir die Anzahl der Switches. Jedes Gerät wird mit je zwei Switches verbunden. Das setzt natürlich voraus, dass die angeschlossenen Geräte mit redundanten Schnittstellen ausgestattet werden können. In Kapitel 4 werden Sie erfahren, dass das mit dem EN100-Kommunikationsmodul für SIPROTEC 4 Geräte problemlos funktioniert - sowohl bei einer elektrischen als auch einer optischen Lösung. Denn diese Module besitzen zwei Schnittstellen, über die parallel zwei Leitungen angeschlossen werden können. Aktiv dagegen ist stets nur eine der beiden Schnittstellen.

Der zweite Kommunikationskanal dient immer als Reserve und wird vom Modul bei Bedarf automatisch aktiviert. So führt auch der Ausfall eines Switches nicht zu einer Verbindungsunterbrechung zum PC. In einem solchen Fall wechseln alle Geräte, die aktiv über den ausgefallenen Switch eine Verbindung aufgebaut hatten, auf ihre zweite Verbindung, die an einem anderen Switch angeschlossen ist.

Der PC hat nun auch zwei Eingänge abbekommen und gewinnt dadurch an Sicherheit. Möglich wird das durch eine teamingfähige Netzwerkkarte mit zwei Eingängen (siehe auch Kapitel 4). Der PC selbst ist noch nicht redundant ausgeführt; eine solche Lösung präsentieren wir Ihnen ein paar hundert Wörter später.

Auf in den Ring

Bei mehreren Switches, die aus Redundanzgründen auch noch gedoppelt werden, steigt der Verkabelungsaufwand zwischen Switches und übergeordneter Zentrale (in unserem Fall PC) drastisch an. Praktischer ist es da schon, sämtliche Switches ringförmig miteinander zu verbinden.



Ring oder Stern? Die Grenzen verwischen.

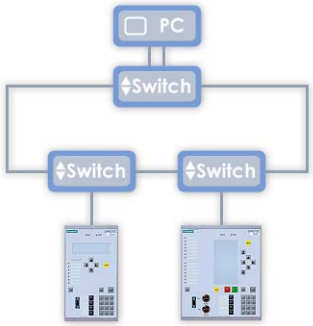
Als Ringverbindung sollte man einem Lichtwellenleiter den Vorzug geben. Arbeiten die Switches als Verstärker, kann man damit problemlos Verbindungen über mehrere Kilometer realisieren. Die einzelnen Geräte schließen Sie dann ebenfalls über LWL oder bei kürzeren Entfernungen auch elektrisch an die Switches.

Ringtopologie

Genau genommen handelt es sich bei der zuletzt gezeigten Struktur noch um einen Stern, auch wenn die einzelnen Switches ringförmig verbunden sind. Die Switches aber sind Verteiler, an denen die einzelnen Teilnehmer angeschlossen sind - und das entspricht unserer Definition der Sterntopologie.

Eselsbrücke

Um eine Brücke zum puren Ring zu schlagen, stellen wir uns ringförmig verbundene Switches vor, an denen jeweils nur ein Teilnehmer angeschlossen ist. Damit erhalten wir die folgende überschaubare Struktur.

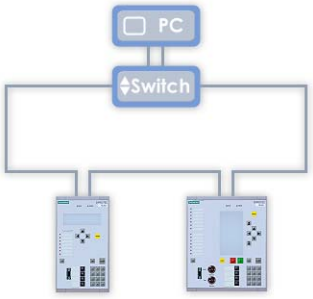


Verwandlung: So wird aus dem Stern ein Ring.

Eine reinrassige Ringstruktur erhalten wir aber erst dann, wenn alle Geräte in einem Ring zusammengeschaltet sind, ohne dafür die externen Switches zu verwenden.

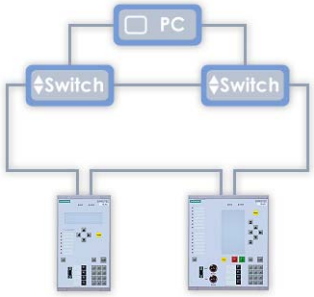
Einspareffekt

Es wäre also optimal, wenn wir jeden Switch in das zugehörige Gerät hineinziehen könnten. Und tatsächlich ist das durch die optischen EN100-Module möglich. Die optischen EN100-Module können nämlich alternativ zur redundanten Betriebsweise auch über beide Ports gleichzeitig aktiv Daten übertragen. Durch diese integrierte Switch-Funktionalität können Sie auf die externen, den Geräten zugeordneten Switches (weitestgehend) verzichten.



Lichtblick: Bei den optischen EN100-Modulen ist der Switch bereits integriert.

Bis zu 30 SIPROTEC 4 Geräte können Sie so zu einem optischen Ring verschalten. Wegen der Kopplung zum PC (oder zur Zentrale allgemein) können Sie auf mindestens einen externen Switch jedoch nicht verzichten. In der Regel werden Sie diese Verbindung jedoch redundant ausführen und dazu zwei Switches verwenden.



Doppeltes Lottchen: Zwei Switches garantieren Redundanz für die PC-Ankopplung.

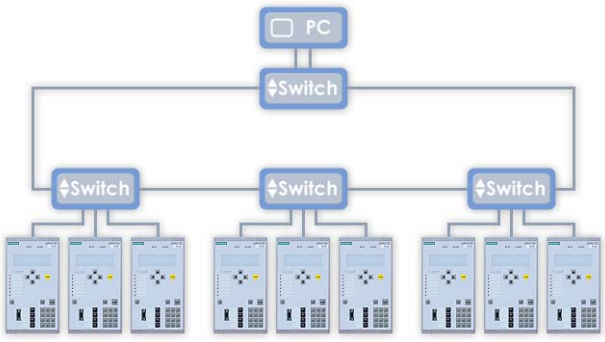
Apropos Redundanz: Informationen werden im Ring von Teilnehmer zu Teilnehmer weitergeleitet, bis sie ihren Bestimmungsort erreichen. Wird die gezeigte Ringstruktur an einer Stelle aufgetrennt, so wird daraus eine Linie. Die Kommunikation funktioniert dabei noch nahezu unterbrechungsfrei weiter. Ein zweiter Fehler auf der Leitung oder in einem der Teilnehmer lässt sich aber in der Regel nicht mehr auffangen. Da in der gezeigten Konfiguration zwei Switches verwendet werden, reduziert sich die maximal mögliche Anzahl von SIPROTEC 4 Geräten im Ring auf 27. Warum das so ist und wie Sie zulässige Anzahl von Geräten berechnen können, erfahren Sie in Kapitel 4.

Gängige Konfigurationen

Zum Abschluss dieses Kapitels zeigen wir Ihnen noch drei gängige Konfigurationen.

Konfiguration 1

In der ersten Abbildung sehen Sie die wohl am häufigsten vorkommende Topologie.



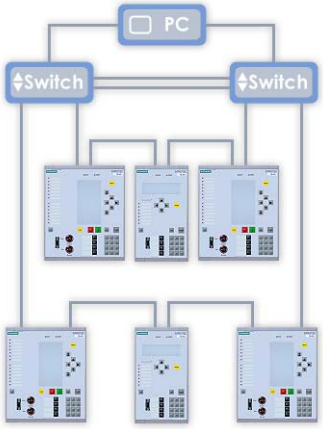
Beliebte Kombination aus einem Ring und mehreren Sternen.

Mehrere Geräte sind sternförmig an Switches angeschlossen, die über einen Ring miteinander verbunden sind. Dieser ist in der Regel optisch ausgeführt, während Kupferleitungen die elektrische Verbindung zwischen Switches und Geräten schaffen.

Wer sich für dieses Konzept entscheidet, darf keinen großen Wert auf Redundanz legen, erhält aber auf der anderen Seite eine kostenverträgliche Lösung.

Konfiguration 2

Deutlich mehr Redundanz bietet da schon das zweite Beispiel. Zwei voneinander unabhängige Ringe sind an zwei Switches angeschlossen. Eine Doppelleitung verbindet diese Switches untereinander und auch der PC ist redundant angekoppelt.

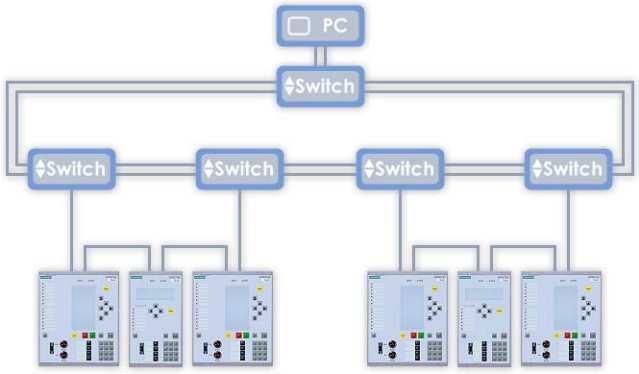


Zwei Ringe sind ineinander gelegt.

Die Ausbaumöglichkeiten einer solchen Topologie sind beachtlich. Sie dürfen bis zu 27 Geräte je Ring installieren. Dabei können Sie auch gleichzeitig die Anzahl der Ringe erhöhen, wenn die verwendeten Switches über ausreichend Ports verfügen.

Konfiguration 3

Eine Alternative zeigt das dritte Beispiel. Jeder Ring darf je zwei Switches sein Eigen nennen. Auch der PC ist über einen eigenen Switch angekoppelt. Der Ring ist mit einer doppelten optischen Leitung ausgeführt.



Zwei Ringe sind über einen doppelten Hauptring verbunden.

Ein Ring darf wieder maximal 27 Geräte miteinander verbinden. Die Anzahl der Ringe selbst ist hier allerdings theoretisch unbegrenzt.

Ein wenig Netzwerktheorie

3

Unser Übertragungsweg für IEC 61850 heißt Ethernet. Warum das so ist, erklärt ein Blick zurück. Bereits im Jahr 1976 gab es die ersten Entwürfe für ein Ethernet-System. Damals stand vor allem das Druckersharing durch mehrere Benutzer im Vordergrund. Heute ist Ethernet mit einem Verbreitungsgrad von mehr als 90% der gängigste Verbindungstyp zwischen Rechnern und deren Peripherie in einem lokalen Netzwerk - und damit das Mainstream-Kommunikationsmedium unserer Zeit.

Gute Gründe

Grund genug, sich auch in Hinsicht auf IEC 61850 auf diese Übertragungstechnologie zu fokussieren, zumal bereits auf eine kostengünstige Produktpalette und oft auch auf eine vorhandene Infrastruktur zurückgegriffen werden kann. Dass Ethernet zugleich in hohem Maße rückwärts- und vorwärtskompatibel ist, macht es besonders in Hinsicht auf bisherige und zukünftige Investitionen interessant. So kann ein 10-MBit-Netzwerk ohne weiteres in ein heute gängiges 100-MBit-Netzwerk integriert werden - und dieses wiederum in das 1-GBit-Netz von morgen.

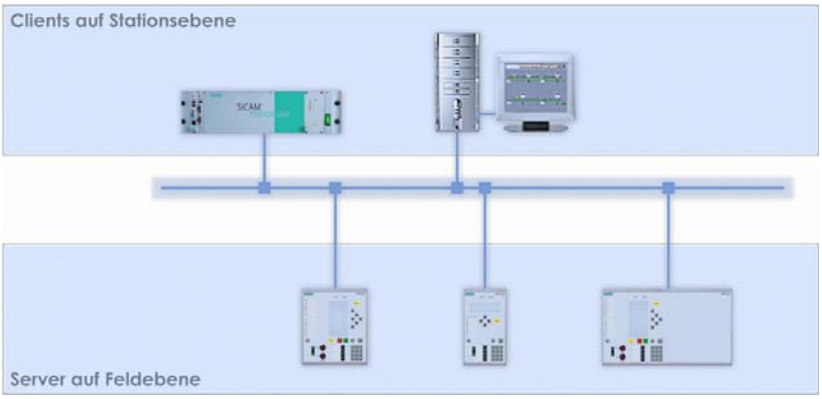
Mit diesem Kapitel werden wir Ihnen einen Einblick in einige Themen geben, die untrennbar mit Ethernet verbunden sind und die Ihnen als Basis für das Verständnis der weiteren Kapitel dienen werden.

Kommunikationsformen

In der Regel werden Netzwerke durch die Rolle der einzelnen Teilnehmer klassifiziert. Peer-to-Peer-Netzwerke unterscheiden sich so von Client-Server-Netzwerken.

Horizontal und vertikal

Bei der Peer-to-Peer-Variante kommunizieren Teilnehmer miteinander, die sich hierarchisch auf einer Ebene befinden. Deshalb spricht man auch von horizontaler Kommunikation. Ein Client-Server-Netzwerk dagegen verbindet hierarchisch unterschiedliche Teilnehmer. Bei dieser vertikalen Kommunikation übernimmt der Client die Rolle des Quizmasters und will alles Mögliche wissen. Die Server als Datenlieferanten haben dann hoffentlich immer die passenden Antworten.



Server und Clients - Peer-to-Peer: Jeder bekommt alles

Kreuz und quer

Bei IEC 61850 ist beides möglich, horizontal und vertikal, und das auch noch gleichzeitig. Betrachten Sie einfach kurz unsere Schema-Abbildung. Die SIPROTEC-Geräte auf Feldebene erfassen Daten und liefern diese. Sie sind die Server. Das Automatisierungssystem auf Stationsebene, hier eine SICAM PAS, will die Daten, bekommt diese und verarbeitet sie. Das ist der Client, von denen es übrigens mehrere gegeben kann. Aber es kommt noch besser: Ein Client kann von allen Servern Daten anfordern, umgekehrt kann ein Server allen Clients Daten zur Verfügung stellen. Und: Viele Aufgaben werden direkt zwischen den Servern erledigt. Sie verständigen sich, horizontal, ohne dafür den Client zu benötigen. Diese so genannte Querkommunikation wird bei IEC 61850 als GOOSE bezeichnet: Generic Object Oriented Substation Event.

Datenübertragung

Nachdem die Zuständigkeiten der Teilnehmer geklärt sind, geht es nun darum, wie Daten über das Medium Ethernet übertragen werden. Damit meinen wir weniger den physischen und physikalischen Ablauf, sondern vielmehr die logische Sicht der Dinge.

Casting-Show

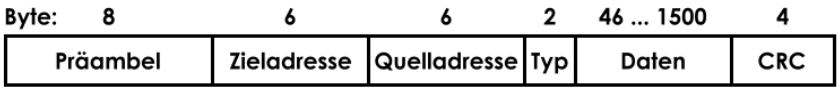
Bei der Entscheidung, an wen ein Teilnehmer seine Botschaften, technisch “Telegramme”, richtet, hat dieser prinzipiell drei Möglichkeiten: An einen, an viele oder an alle. In der Sprache der Telekommunikation heißt das dann Unicast, Multicast und Broadcast.

Beim Unicast-Verkehr werden Datenpakete von einer Quelle an exakt einen Empfänger gerichtet. Diese Art der Übertragung trifft sicher bei den meisten der gesendeten Daten zu. Broadcast-Daten werden dagegen in Form eines Broadcasts an alle angeschlossenen Teilnehmer im gesamten Netzwerk gesendet. Ein Broadcast wird vorwiegend dann verwendet, wenn die Adresse des Empfängers der Nachricht noch unbekannt ist. Jeder Empfänger eines Broadcasts muss die Nachricht zunächst entgegennehmen, um anschließend zu entscheiden, ob die Nachricht für ihn relevant ist.

Zwischen den Welten Unicast und Broadcast gibt es gelegentlich den Wunsch, dasselbe Datenpaket an mehrere ausgewählte Empfänger zu schicken. Ein eindeutiger Fall für Multicast. Anwendung findet dieses zum Beispiel im Rahmen der IEC 61850 bei der horizontalen Kommunikation zwischen den einzelnen Teilnehmern. Hier werden Multicasttelegramme verwendet, um zyklisch den Zustand von Informationen zu übertragen. Bei einer spontanen Änderung wird der neue Status der Information sofort an alle Teilnehmer übertragen. Die Übertragung wird dann im Millisekundenabstand wiederholt.

Versand-verpackung

Alle Daten, die über das Ethernet übertragen werden, sind in einen so genannten Frame verpackt. Die Daten werden also gebündelt mit weiteren Informationen auf den Weg geschickt. Ein solcher Frame besteht aus einer Präambel, der Ziel- und der Absenderadresse, dem Typ, einer Prüfsumme - und natürlich aus den eigentlichen Nutzdaten. Ein kleines Bildchen macht es deutlicher.



It´s a frame: Die Nutzdaten gehen immer in Begleitung auf die Reise.

Die Präambel kennzeichnet den Beginn eines Frames. Die Empfänger können so die einzelnen Frames voneinander unterscheiden. Der Typ benennt das verwendete Protokoll, in unserem Fall das IP-Protokoll. Anhand einer Prüfsumme (CRC) kann der Empfänger eventuelle Übertragungsfehler erkennen. Teil des Frames sind auch die Quell- und natürlich die Zieladresse der Daten. Dazu mehr im nächsten Abschnitt.

Identifikation

Solange Frames innerhalb des eigenen Netzwerks verschickt werden, adressiert der Versender die Pakete mit der MAC-Adresse des Empfängers. Sobald jedoch ein Teilnehmer eines anderen Netzwerks angesprochen werden soll, erfolgt die Adressierung über die IP-Adresse. Nichtsdestotrotz benötigen wir in unserem Fall die IP-Adresse auch innerhalb eines lokalen Netzes. Denn über die IP-Adresse nehmen Sie beispielsweise über einen Web-Browser Kontakt mit dem Kommunikationsmodul auf, um wichtige Informationen abzufragen. Aber lassen Sie uns doch zunächst auf die einzelnen Adressen näher eingehen.

Weltbekannt

Eine gute Adresse war schon immer das A und O für den Beginn einer Erfolg versprechenden Beziehung. Und wer wäre nicht gerne auf der ganzen Welt bekannt. Da haben es so mache Netzwerkkomponenten schon leichter, die sind es nämlich von Geburt an. Möglich macht das die **MAC-Adresse**. Diese hat, um möglichen Missverständnissen vorzubeugen, nichts mit den bekannten Designer-Rechnern zu tun (und schon gar nicht mit irgendetwas Essbarem). MAC bedeutet Media Access Control und regelt den eindeutigen Zugriff auf Kommunikationshardware.

Diese Adresse ist fest in praktisch jeder Netzwerkkomponente hinterlegt und identifiziert diese weltweit eindeutig. “Praktisch” deswegen, da es doch eine Ausnahme gibt: Ist eine bestimmte Komponente grundsätzlich nie aktiv an der Netzwerkkommunikation beteiligt, muss diese auch keine MAC-Adresse besitzen. (Verboten ist es indes natürlich nicht.) Beispiele dafür sind Repeater, Hubs und einfache Switches, sofern sie keine Management- oder Monitoring-Funktionen besitzen.

MAC-Adressen können nicht von Ihnen verändert werden (zumindest nicht so ohne weiteres). Offiziell haben Sie also nur einen lesenden Zugriff auf die MAC-Adresse. Denn diese wird einer Komponente von ihrem Hersteller zugewiesen. Und auch dieser kann sich eine solche Adresse nicht beliebig aus den Fingern saugen, sondern muss sich einen eigenen MAC-Adressenraum gegen Bares erwerben. Welche wichtige Rolle die MAC-Adresse spielt, werden Sie erfahren, wenn wir uns im nächsten Kapitel über die einzelnen Komponenten einer Netzwerkkommunikation unterhalten.

Local hero

Die **IP-Adresse** ist die Kennzeichnung eines Gerätes, das an einer Kommunikation über Ethernet teilnimmt. Diese Kennzeichnung muss ebenfalls eindeutig sein. Allerdings ist die Eindeutigkeit nicht so weit gefasst wie bei MAC-Adressen. Jede IP-Adresse darf innerhalb eines Netzwerks nur ein einziges Mal vergeben werden. Innerhalb zweier verschiedener Netzwerke, die sogar miteinander verbunden sein können, sind gleiche IP-Adressen durchaus erlaubt.

Der Zwang zur Eindeutigkeit innerhalb eines Netzwerkes gilt übrigens für alle Geräte, die aktiv an der Kommunikation teilnehmen, soll heißen, in irgendeiner Form angesprochen werden müssen, und sei es nur zu Diagnosezwecken. Ansonsten können schwer lokalisierbare Netzwerkfehler auftreten und wer braucht das schon.

Für die Eindeutigkeit einer IP-Adresse muss, ganz im Gegensatz zur MAC-Adresse, der Administrator selbst sorgen. Außer es befindet sich ein so genannter DHCP-Server im Netzwerk. Dieser versorgt nämlich alle Teilnehmer automatisch mit korrekten IP-Adresse. Das Ganze hat nur einen Haken: Netzwerke nach IEC 61850 arbeiten nicht mit einem DHCP - Server. Deshalb werden wir dieses Thema nicht behandeln.

Die IP-Adresse genauer betrachtet

Wir wollen uns nun einmal die Struktur einer IP-Adresse ansehen, genau genommen, einer IPv4-Adresse, also einer solchen der vierten Generation.

Wohnblock

IP-Adressen der vierten Generation werden dezimal in vier Blöcken geschrieben. Ein Beispiel: 207.142.131.235. Jeder Block repräsentiert acht Bit, wodurch sich ein Wertebereich von 0 bis 255 für jeden Block ergibt. Bei einer IPv4-Adresse handelt es sich also um ein 32-Bit-Konstrukt, das maximal 4.294.967.296 eindeutige Adressen beschreiben kann.

Doppelhaus

Eine IP-Adresse enthält genau betrachtet zwei Adressen: Eine für den Teilnehmer und eine für das Netzwerk, in welchem sich dieser befindet. Beispiel: Von der IP-Adresse 197.255.255.89 könnten die ersten drei Dezimalblöcke, also 197.255.255, die Netzwerkadresse darstellen. Der Letzte Dezimalblock, in unserem Fall die 89, wäre dann die Adresse des Teilnehmers. Ein Kollege im selben Netzwerk könnte dann beispielsweise die IP-Adresse 197.255.255.13 besitzen. Die Netzwerkadresse ist dabei natürlich die gleiche, die 13 ist der Adressteil des Teilnehmers.

Drei-Klassen-Gesellschaft

Das gezeigte Beispiel entspricht einer Adresse der Klasse C. In einem Netz dieser Klasse können theoretisch 2^8 = 256 Teilnehmer adressiert werden. Praktisch sind es nur 254, denn der Adressteil 0 kennzeichnet zusammen mit den übrigen drei Dezimalblöcken das Netz selbst. Und der Adressteil 255 ist für einen so genannten Broadcast reserviert, also einem Rundumschlag, wie wir ihn bereits in einem Abschnitt vorher beschrieben hatten.

In einem Klasse-B-Netz stehen der dritte und vierte Dezimalblock zur Adressierung eines Teilnehmers zur Verfügung. Als Wert bedeutet das 2^{16} - 2 = 65.534 maximale Teilnehmer. Für ein Klasse-A-Netz, bei welchem die letzten drei Dezimalblöcke zur Teilnehmeradressierung verwendet werden, ergeben sich nach dem gleichen Rechenschema 16.777.214 unterscheidbare Adressen.

Welcher Klasse eine Adresse angehört, verrät uns der erste Dezimalblock: Beginnt die Adresse ...

- ... mit 1-128, so handelt es sich um eine Klasse-A-Adresse,
- ... mit 129-191, so handelt es sich um eine Klasse-B-Adresse,
- ... mit 192-223, so handelt es sich um eine Klasse-C-Adresse.

Die Einteilung in Klassen ist historisch bedingt. Zu Beginn der Rechnervernetzung erschien der Adressraum von 32 Bit als unendliche Weite. Um die Suche nach dem Empfänger bestimmter Daten innerhalb eines vertretbaren Zeitraums zu realisieren, bewertete ein Router eine Adresse zunächst nur anhand des Netzwerkteils - bei dem damaligen Stand der Rechnertechnik eine deutliche Erleichterung.

Betrachtet man das heutige Internetaufkommen, erweist sich nicht nur der 32-Bit-Adressraum als zu klein, sondern auch das 3-Klassen-Schema als zu starr. Netzwerkadressen für den Internetverkehr werden heute in zusammenhängenden Adressblöcken an Internet Provider vergeben. Die Unterteilung in einzelne Klassen ist hier mittlerweile obsolet.

Privatsphäre

Bei der Projektierung lokaler Netzwerke ist der Klassenbegriff aber immer noch eine griffige Kennzeichnung und darf ohne schlechtes Gewissen weiterverwendet werden. Das hat auch einen guten Grund, denn aus jeder der Klassen A, B und C ist ein Adressbereich als so genannter privater Bereich ausgewiesen. Adressen aus solchen privaten Bereichen werden von keinem Router im Internet vermittelt. Das heißt also, dass ihr lokales Netz durchaus mit dem Internet verbunden sein kann, ohne Konflikte heraufzubeschwören.

Hier die Fakten:

- Privater Adressenbereich Klasse A: 10.0.0.0 - 10.255.255.255
- Privater Adressenbereich Klasse B: 172.16.0.0 - 172.31.255.255
- Privater Adressenbereich Klasse C: 192.168.0.0 - 192.168.255.255

Interessant für Sie sind dabei die Bereiche aus den Klassen B und C mit 65.534 bzw. 254 adressierbaren Teilnehmern.

Entscheiden Sie sich für die Klasse C, mag das zunächst die übersichtlichere Variante sein. Dieser vermeintliche Vorteil wird aber schnell zum Nachteil, wenn beispielsweise eine Erweiterung ins Haus steht. Dann nämlich reichen die vorhandenen Adressen mitunter nicht aus. In Folge müssen Sie ein zweites Netzwerk anlegen und beide Netze über einen Router verbinden. Sind also Erweiterungen bereits geplant oder ist die Anzahl der benötigten Adressen von vornherein schon grenzwertig, dann greifen Sie lieber gleich zur Klasse B.

Aber auch wenn Sie die Menge der verfügbaren Adressen nie im Leben auszunutzen gedenken, hat diese Klasse ihre Vorteile. Bei dieser Variante können Sie die Adressenstruktur viel übersichtlicher gestalten. Zum Beispiel können Sie den dritten Dezimalblock dazu nutzen, Feld- und Spannungsebenen in der Teilnehmeradressierung voneinander zu trennen. Details dazu erfahren Sie in Kapitel 5.

Mehrere Netze verbinden

Zu einer klassischen Einstiegsaufgabe zählt sicherlich eines nicht: Die Projektierung einer Kommunikation über mehrere miteinander verbundene Netze. Dennoch möchten wir Sie kurz über diese Möglichkeit und einige davon untrennbare Begriffe informieren.

Parzellierung

Sie strukturieren große Netzwerke nach topologischen, aber auch organisatorischen Aspekten, indem Sie diese in kleinere Netze zerlegen. Diese werden bisweilen auch als Subnetze bezeichnet, sind aber eigenständig funktionierende Einheiten und unterscheiden sich technisch nicht zwangsläufig von größeren Netzen. Gründe, die das Aufteilen rechtfertigen, sind zum einen bessere Administrationsmöglichkeiten, aber auch die gegebene räumliche Ausdehnung der Teilnehmer und damit verbundene technische Rahmenbedingungen.

Richtungsweisend

Unterschiedliche Netze verbinden Sie mit einem Router zu einem Gesamtnetzwerk. Dieser Router entscheidet dann, in welches Netz Daten weitergeleitet werden müssen. Die Topologie der Netze spielt dabei übrigens keine Rolle. Allerdings können Sie mit einem Router nur Netzwerke verbinden, auf denen dasselbe Protokoll verwendet wird. Unterscheiden sich die Protokolle auf den einzelnen Subnetzen, dann wird eine Protokollumsetzung nötig. Für diesen Fall verwenden Sie statt eines Routers ein Gateway.

Maskiert

Wir haben Ihnen bereits erläutert, dass sich eine IP-Adresse in zwei Teile gliedert. Die führenden Bits kennzeichnen das Netz, die verbleibenden Bits adressieren den Teilnehmer innerhalb des Netzes. Die Information, an welcher Stelle der IP-Adresse die Teilung liegt, liefert die Netzmaske. Mit diesem Bitschlüssel, der genauso lang ist wie die IP-Adresse, kann der Router den Netzteil extrahieren und so die eingehenden Daten dem richtigen Zielnetz zuordnen.

Das Prinzip dabei ist eigentlich ziemlich simpel: Alle auf **1** gesetzten Bits der Netzmaske outen das entsprechende Bit der IP-Adresse als den Teil, der das Netz spezifiziert. Analog kennzeichnen die auf **0** gesetzten Bits den Teil, der die einzelnen Teilnehmer adressiert. Sollen beispielsweise die ersten beiden Dezimalblöcke einer IP-Adresse den Netzteil darstellen, müssen Sie 11111111.11111111.00000000.00000000 als Netzmaske definieren. Die Dezimalschreibweise dazu ist 255.255.0.0. Ist nur der letzte Dezimalblock als Teilnehmeranteil vorgesehen, folgt daraus die Netzmaske 11111111.11111111.11111111.00000000 oder dezimal 255.255.255.0. Die Trennung zwischen Netzteil und Teilnehmerteil kann natürlich an jeder beliebigen Stelle erfolgen. Insofern sind auch Netzmasken wie diese zulässig: 11111111.11111111.11111000.00000000.

Mittlerweile hat sich zugunsten einer besseren Lesbarkeit eine eigene Schreibweise für IP-Adressen in Netzwerken etabliert. Bei dieser wird die Anzahl der gesetzten Bits der Netzmaske an die IP-Adresse angefügt. Aus 198.200.133.17 und 11111111.11111111.00000000.00000000 wird damit 198.200.133.17/16.

Datenfluss in Ringstrukturen

Ringstrukturen bescheren uns ein höheres Maß an Redundanz, das ist ihr eindeutiger Vorteil. Wo ein Vorteil ist, ist der Nachteil meist nicht weit. Da alle Teilnehmer physisch als Ring miteinander verbunden sind, pflegen Telegramme endlos darin zu kreisen, nachdem sie erst einmal eingespeist wurden. Das führt zu einer Datenüberlast und darf daher nicht sein. Die Lösung ist eine logische Lücke, an der Telegramme im Normalbetrieb wieder aus dem Netz genommen werden. So arbeitet eine Ringstruktur logisch betrachtet als Linie. Bei einer physischen Unterbrechung wird diese Lücke dann geschlossen. Daraus ergibt sich sogleich die zweite Aufgabe, die eine ordentliche Ringsteuerung erledigen muss. Nach dem Ausfall eines Netzwerkpfades muss sie die Daten gegebenenfalls auf einen anderen Pfad umleiten, der dann ebenso zum Ziel führt - und das natürlich möglichst schnell.

Ringsteuer

Zwei unterschiedliche Verfahren stehen zur Diskussion.

- **OSM-Steuerung**
  Eine sicher kluge Entscheidung wäre, OSM zu wählen. Dann dürften Sie nach diesem Absatz den Rest des Kapitels getrost überspringen. Aber das ist natürlich nicht der wesentliche Grund. Fakt ist, dass diese von SIEMENS entwickelte Ringsteuerung in ihrer einfachen Anwendung wohl kaum zu übertreffen ist. Als einzigen Parameter müssen Sie einen der vorhandenen Switches als Master kennzeichnen, alles andere erledigt sich dann wie von selbst. Der Wermutstropfen ist jedoch, dass sich diese Technologie noch nicht weit genug etabliert hat. Insofern werden Sie damit nur Chancen haben, wenn Sie (fast) ausschließlich Hardware von Siemens verwenden. Und deshalb werden Sie nun wohl doch weiterlesen müssen.
- **RSTP-Steuerung**
  RSTP ist weltweit im Einsatz und wird von nahezu allen Switches mit Ringmanagement-Funktionalität unterstützt, ist in der Handhabung aber weitaus komplizierter. Bei RSTP wird der Datenfluss über die Vergabe von Prioritäten an die einzelnen Switches gelenkt. Diese Aufgabe obliegt Ihnen und stellt sich mitunter als alles andere als trivial heraus. Da sich sie meisten von Ihnen aber dennoch für dieses Verfahren entscheiden werden, gibt es hier noch einige weitere Hinweise dazu.

Der wichtigste davon: Im Handbuch zum Ethernetmodul EN100 erhalten Sie ganz ausführliche Informationen zu RSTP, hinab bis in mathematische Untiefen. Deshalb beschränken wir uns hier auf eine Zusammenfassung der wesentlichen Merkmale, die RSTP charakterisieren.

Prioritäten setzen

Beim Einsatz von RSTP müssen Sie Prioritäten setzen, und zwar für jeden Switch. Der Switch mit der höchsten Priorität (also dem niedrigsten Zahlenwert) wird als Root-Switch bezeichnet. In der Regel wird dazu der Switch gewählt, an den der Stationsmaster angeschlossen ist. Alle anderen Switches werden als Designated Switches bezeichnet.

Wichtig für den Normalbetrieb ist, dass vom Root-Switch ausgehend hin zu unserer logischen Lücke möglichst zwei gleich lange Ketten entstehen. Als logische Lücke im Ring wirkt immer der Switch mit der niedrigsten Priorität, also dem höchsten Zahlenwert. Fällt nun im Fehlerfall der Root-Switch aus, muss ein anderer Switch dessen Funktion übernehmen. Auf der Suche nach einem geeigneten Ersatz dient die eingestellte Priorität als Kriterium. Es wird also der Switch einspringen müssen, dem die nächstniedrigere Priorität zugewiesen wurde.

Ein Switch im Ringbetrieb wird nebenbei bemerkt auch als Bridge bezeichnet. Die Switch-Priorität hört daher auch auf den Namen Bridge Priority, der noch häufiger unseren Weg kreuzen wird.

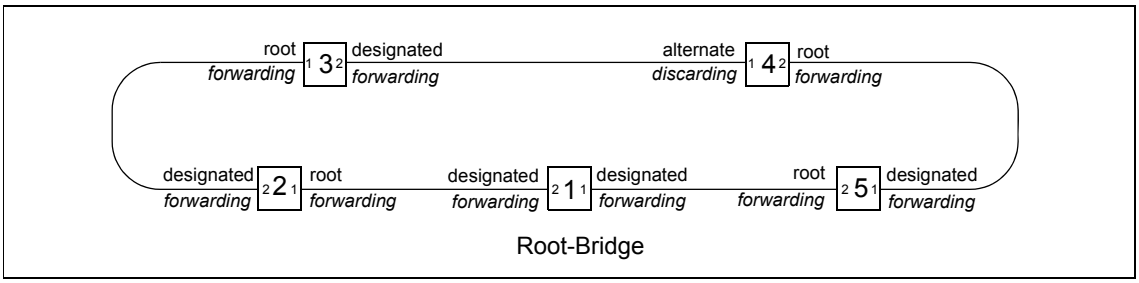
Mit Methode

Bevor Sie nun loslegen, schon mal die eine oder andere Switch-Priorität zu verstellen, wollen wir Ihnen drei grundsätzliche Vorgehensweisen vorstellen.

- **Methode 1: Einheitliche Priorität für alle Switches**
  Sie haben richtig gelesen, auch das ist möglich. Denn besitzen mehrere Switches innerhalb eines Rings identisch eingestellte Prioritäten, werden die MAC-Adressen als Kriterium herangezogen. Eine niedrige MAC-Adresse ist dann gleichbedeutend mit einer hohen Priorität und umgekehrt. Und da Sie bereits vor einigen Seiten erfahren haben, dass MAC-Adressen weltweit eindeutig sind, gibt es in keinem Fall einen Prioritätenstreit. Der Vorteil dieser schnellen Methode liegt auf der Hand. Die Konfiguration erfolgt praktisch wie von selbst. Wollen Sie Switches hinzufügen oder entfernen, müssen Sie dazu keine Einstellungen ändern. Den Nachteil sollte man allerdings nicht unter den Tisch kehren. Da Ihnen die MAC-Adresse eines Switches meist nicht bekannt ist, ist die Anordnung von Root-Switch und logischer Trennstelle des Rings eher zufälliger Natur. Es ergeben sich mit hoher Wahrscheinlichkeit unterschiedlich lange Ketten, die auf dem längeren Stück zu einer höheren Netzwerklast führen.
- **Methode 2: Root-Switch festlegen (Empfohlene Methode)**
  Diese Methode unterscheidet sich von der Ersten in der Art, dass Sie nun die Priorität eines Switches auf Null setzen und diesen damit als Root-Switch definieren. Damit haben Sie zumindest schon eine eingeschränkte Kontrolle über die Lastverteilung im Netzwerk, aber noch nicht die Vollständige. Denn an welcher Stelle im Ring sich die logische Lücke befindet, entscheidet nach wie vor Meister Zufall.
- **Methode 3: Priorität für (fast) jeden Switch einstellen**
  Die dritte Methode fordert Ihnen die meiste Arbeit ab, bietet aber auch die Möglichkeit, ein ausgefeiltes Redundanzkonzept umzusetzen. Sie legen je einen Switch als Root und als logische Unterbrechung fest. Die Prioritäten der übrigen Switches stellen Sie entsprechend der benötigten Redundanz ein. Gibt es beispielsweise einen Switch, der im Fehlerfall die Root-Funktion übernehmen soll, erhält dieser die nächstniedrigere Priorität nach dem Root-Switch. Natürlich können Sie auch für den Ersatzmann ein Double festlegen. Dessen Priorität ist dann nochmals niedriger, usw. Der Nachteil dieser Methode liegt auf der Hand: Bei einer Änderung im Netzwerk müssen viele Netzwerkkomponenten neu parametriert werden.

Haupt- und Nebenrollen

Die Begriffe **root** und **designated** werden nicht nur für die Priorität der Switches verwendet, sondern auch für deren Ports, und beschreiben, welche Rolle ein solcher spielt. Am besten, wir erläutern das an einem kleinen Bildchen.



Die Root Bridge ist die Nummer 1 im Ring.

Switch Nummer 1 ist unser Root-Switch. Er ist mit den Switches 2 und 5 verbunden, die im Notfall für Nummer 1 einspringen können. Die Ports der Switches 2 und 5, die mit dem Root-Switch verbunden sind, werden als Root-Ports bezeichnet. Ports, die mit dem Netzwerk verbunden sind, aber nicht in Richtung Root-Switch führen, werden als Designated Port bezeichnet. Insofern besitzt der Root-Switch selbst ausschließlich Designated Ports, da er nicht mit einem anderen Root-Switch verbunden ist (Sie wissen ja, es kann nur einen geben). Neben Root und Designated gibt es noch eine dritte Rolle, nämlich die des Alternate Ports. Dieser Port ist nichts anderes als unsere logische Lücke im Ring.

Schöne Zustände

Jeder Port eines Switches kann, abhängig von seiner Rolle, bestimmte Zustände annehmen. Von den insgesamt Möglichen interessieren uns vor allem 2: Forwarding und Discarding. Root und Designated Ports nehmen den ersten dieser beiden Zustände an, sie leiten eingehende Nutzdaten also weiter. Der Alternate Port dagegen befindet sich im Zustand Discarding und verwirft eingehende Telegramme, denn genau das ist sein Job.

Die Komponenten im Überblick

4

Unser Weg zu einer erfolgreichen Kommunikation ist gepflastert mit einer Reihe unterschiedlicher Komponenten, die wir hier und da schon mehr oder weniger erwähnt haben. In diesem Kapitel werden wir auf jeden dieser benötigten Bausteine näher eingehen, als da sind:

- Der Switch
- Das EN100-Kommunikationsmodul
- Der Zeitserver
- Die Netzwerkkarte

Der Switch

Verbinden Sie zwei Teilnehmer ohne weiteres noch über ein Cross-Connect-Kabel direkt miteinander, wird es ab dem dritten Gerät bereits kompliziert. Damit sich dieses dann nicht als fünftes Rad am Wagen fühlt, benötigen wir einen Verteiler.

Postverteiler

Auch beim Verteilen von Daten hat es sich als geschickt erwiesen, intelligent vorzugehen; gerechtes Verteilen ist allemal besser, statt einem alles zu geben, während die anderen in die Röhre gucken. Wir entscheiden uns daher weder für Lüsterklemmen noch für Hubs, sondern wählen Switches.

Der Switch ist ein intelligenter Datenverteiler, an den in der Art eines Sternkopplers mehrere Geräte angeschlossen werden. Bei der Verbindung der Geräte zum Switch handelt es sich immer um eine Punkt-zu-Punkt-Verbindung.

Der Switch kümmert sich um die Verwaltung der eingehenden und ausgehenden Nachrichten. Im Gegensatz zu einem Hub, der die verfügbare Bandbreite diplomatisch stets zu gleichen Teilen auf die vorhandenen Anschlüsse verteilt, geht ein Switch dabei erheblich praxisgerechter vor. Dazu sind alle Ports des Switch über einen internen Hochgeschwindigkeitsbus miteinander verbunden. Wahre Netzwerkprofis nennen diesen auch Backplane. Dieser Bus ist die Voraussetzung, dass die empfangenen und zu sendenden Datenpakete auch zügig von einem Port zum nächsten gelangen.

Gute Zeiten, schlechte Zeiten

Entscheidend ist jedoch auch, dass die einzelnen Ports Daten unabhängig voneinander empfangen und senden können. Erhält der Switch mehr Daten, als er aufgrund der aktuellen Netzauslastung weitersenden kann, legt er diese in einem Zwischenspeicher ab und sendet sie zeitverzögert. Empfängt unser Switch Daten, die für mehrere Adressaten bestimmt sind, ist das für ihn sowieso kein Problem: Er übermittelt diese dann gleichzeitig über die einzelnen Ports an die unterschiedlichen Empfänger.

Aber es geht sogar noch effektiver: Im so genannten Vollduplex-Modus kann der Switch an ein und demselben Port gleichzeitig Daten senden und empfangen. Kollisionen gibt es dann für den betreffenden Port praktisch keine mehr und die Geschwindigkeit kann theoretisch verdoppelt werden. Man sollte allerdings beachten, dass der Modus und damit auch die mögliche Geschwindigkeit an jedem Port unabhängig ausgehandelt werden kann.

Das alles klingt ziemlich gut. Wir wollen aber nicht kritiklos der Wunderwaffe “Switch” huldigen, sondern auch eines nicht verheimlichen: Wo ein Hub ein eingehendes Telegramm gnadenlos an alle angeschlossenen Teilnehmer weitergeleitet wird, muss der Switch zunächst den Empfänger ermitteln, um die Daten gezielt weiterzuleiten. Das spart zwar Bandbreite, kostet aber Zeit. Deshalb bedient sich der Switch eines kleinen Management-Tricks.

Management-Tricks

In Kapitel 3 haben Sie erfahren, dass zur Identifikation eines Teilnehmers innerhalb des lokalen Netzwerks die MAC-Adresse verwendet wird.

Hinweis am Rande:
Es gibt Teilnehmer, die zwar empfangen, aber nicht senden können. Solche Teilnehmer wären nach dem geschilderten Prinzip immer außen vor, da sie der Switch niemals registrieren würde. Für diese Spezies kann im Switch eine MAC-Adresse eingetragen und fest in Beziehung zu einem Port gebracht werden.

Sobald sich an einem Port des Switches ein Teilnehmer zum ersten Mal meldet, wird dessen MAC-Adresse mit diesem Port logisch verknüpft und diese Relation in einer Tabelle gespeichert. Bei eingehenden Datenpaketen vergleicht der Switch die Zieladresse mit den gespeicherten Relationen und kann so den benötigten Port ermitteln.

Daten werden also auf diese Weise möglichst zügig und im Idealfall nur an den Port weitergeleitet, an welchem sich tatsächlich der Empfänger befindet. Allerdings kann es vorkommen, dass für eine Zieladresse keine Relation zu einem Port gespeichert ist. Die Zieladresse ist also unbekannt. Die Daten werden dann an alle Ports weitergeleitet, den Quellport ausgenommen. Dies gilt natürlich ebenso für Broadcast-Daten, denn da ist dieses Verhalten ja sogar gewollt.

Unbekannt verzogen

Was aber, wenn nicht der Idealfall vorliegt? Wird beispielsweise die Leitung unterbrochen, so würden die Pakete weiterhin an einen Port vermittelt, auch wenn dahinter längst kein Empfänger mehr zu finden ist. Einige Mechanismen sollen dem entgegentreten.

Da ist zunächst einmal die so genannte Alterungszeit (Maximum Aging Time), die sich, im Gegensatz zu der des Menschen, per Software leicht einstellen lässt. Mit dieser Zeit legen Sie fest, wie lange der Switch an eine feste Beziehung zwischen einer MAC-Adresse und einem seiner Ports glauben soll.

Oder mit anderen Worten ausgedrückt: Erkennt der Switch innerhalb der Alterungszeit für eine gespeicherte MAC-Adresse keine Verbindungs- und Datenaktivitäten, löscht er die Adresse samt ihrer Relation zu einem Port aus seiner internen Tabelle.

Wird also ein Gerät von einem Port abgezogen und mit einem anderen verbunden, dann vergeht diese Alterungszeit, ehe das Gerät auf dem neuen Port angesprochen wird. Für exakt den beschriebenen Fall mag das ausreichend sein. Bei einem Leitungsbruch während des normalen Betriebs aber ist mit Sicherheit eine schnellere Umschaltung wünschenswert. Deshalb wird die Alterungszeit durch einen weiteren Mechanismus überlagert: Far End Fault Indication, kurz FEFI. Ist diese Switch-Funktion aktiviert, wird bei einem Leitungsbruch die Alterungszeit schlichtweg ignoriert. Die zugehörige MAC-Adresse fällt einem sofortigen Gedächtnisverlust zum Opfer und die Umschaltung auf einen alternativen Pfad erfolgt in kürzestmöglicher Zeit.

Weg da, jetzt komm ich

Eine Spezialität von IEC 61850 sind GOOSE-Telegramme. GOOSE steht für Generic Object Oriented Substation Event. Mit diesen Telegrammen können Geräte direkt miteinander kommunizieren. Meistens handelt es sich dabei um zeitkritische Nachrichten, die ein Gerät einem anderen mitteilen muss. Der Switch darf sich daher nicht als Bremsklotz erweisen, sondern muss solche Telegramme bevorzugt behandeln. Der Fachmann spricht auch von einer Priorisierung der GOOSE-Telegramme. Wir benötigen für unsere Zwecke also unbedingt Switches, die dieses Leistungsmerkmal besitzen. Solche Switches haben je einen Bearbeitungspfad für Telegramme mit normaler und für solche mit hoher Priorität. Der Switch wertet bei einem eingehenden Telegramm dessen Priority Field aus und schiebt anhand der erkannten Priorität die Daten in den einen oder den anderen Pfad. Müssen sich dann die normalen Telegramme schon mal hinten anstellen, werden die privilegierten in ihrem Pfad möglichst sofort bearbeitet.

Spielarten

Für alle, die sich noch dafür interessieren, wie ein Switch grundsätzlich einzelne Telegramme durch sich hindurch leitet, beschreiben wir noch einige Spielarten, die sich hinsichtlich ihrer Verzögerungszeit und der Fehlerkorrektur unterscheiden.

- **Cut-Through**
  Kein neuer Haarschnitt, sondern die schnellste aller Methoden, wenngleich auch die trivialste. Der Switch wirft beim eingetroffenen Frame nur einen Blick auf die Ziel-MAC-Adresse und schickt den Frame entsprechend weiter. Von Fehlerprüfung also keine Spur, dafür praktisch zeitlos.
- **Store-and-Forward**
  Die reinlichste aller Methoden ist zugleich die langsamste. Im Rahmen der Initiative für ein sauberes Netz prüft der Switch dabei jedes eingehende Paket auf mögliche Fehler. Fehlerbehaftete Frames haben keine Chance und werden ersatzlos verworfen.

- **Fragment-Free**
  Liegt die Wahrheit wirklich irgendwo dazwischen, dann wäre dieses die Methode der Wahl: Sie ist schneller als Store-and-Forward, und fehlerfeindlicher als Cut-Through. Sie prüft, ob ein Paket die im Ethernet-Standard geforderte minimale Länge von 64 Bytes erreicht. Falls ja, schickt es das Paket sofort auf den Zielport. Falls nein, handelt es sich offensichtlich um Fragmente einer Kollision, die guten Gewissens verworfen werden dürfen.
- **Error-Free-Cut-Through / Adaptive Switching**
  Eine andere Meinung besagt: Die richtige Mischung macht´s. Und deshalb ist dieses wohl die optimale Methode, wenngleich auch die aufwändigste. Der Switch arbeitet zunächst im Modus **Cut through**. Einen Frame schickt er ohne Ansehen von Herkunft und Werdegang über den korrekten Port auf die weitere Reise. Er behält sich jedoch eine Kopie im Speicher, über die er eine Prüfsumme berechnet. Stimmt diese nicht mit der im Frame überein, so kann er die defekten Daten zwar nicht mehr zurückpfeifen. Mithilfe eines internen Zählers merkt er sich jedoch den aufgetretenen Fehler. Treten innerhalb einer bestimmten, meist knapp angelegten Zeitspanne zu viele Fehler auf, wechselt der Switch in den Modus **Store and Forward**. Fällt die Fehlerrate wieder unterhalb eines zugelassenen Grenzwertes, arbeitet er wieder mit **Cut through**. Überdies kann der Switch zeitweise in den Modus **Fragment Free** wechseln, wenn zuviele Fragmente mit weniger als 64 Byte Länge ankommen.

Postlagernd

Die beschriebenen Methoden erfordern natürlich verschiedene Hardwareausführungen, die sich letztendlich durch die Anzahl der Zwischenspeicher unterscheiden.

- **Kein Zwischenspeicher**
  In Switches ohne Zwischenspeicher können immer nur zwei Ports direkt über den internen Bus logisch miteinander verbunden sein. Daten, die gleichzeitig an einem dritten Port anstehen, verzögern bereits die Datenübermittlung. Diese Art von Switches beherrschen lediglich die Cut-Through-Methode und sind für kommerzielle Zwecke nicht geeignet.
- **Ein Zwischenspeicher für alle**
  Nicht gerade üppig, aber schon besser ist da ein gemeinsamer Zwischenspeicher für alle Ports. Die Teilnehmer legen ihre Daten in den Zwischenspeicher, während der Switch die Verbindung zu den anderen Teilnehmern vorbereitet. Daraus ergibt sich ein entscheidender Vorteil: Wollen mehrere Teilnehmer an den gleichen Port Daten senden, werden diese zunächst gespeichert und anschließend gesammelt übertragen.
- **Ein Eingangs- und ein Ausgangsspeicher je Port**
  Die Luxuslösung bietet Ihnen die maximal mögliche Verspeicherung. Diese Art von Switch kann mehrere Telegramme zwischenlagern und zeitgleiche Verbindungen mehrerer Portpaare herstellen. So können die Teilnehmer A und B miteinander kommunizieren, während auch C und D am Tratschen sind.

Die Qual der Wahl

Die Frage, die wir uns natürlich stellen müssen, lautet: Kann jeder beliebige Switch für die Kommunikation über Ethernet genutzt werden? Schließlich gibt es Switches von 40 Euro bis zu 2000 Euro. Als Antwort darauf gibt es nur ein eindeutiges Jein.

Für eine einfache Verbindung zwischen zwei PCs und einem Drucker tut es allemal die Billiglösung von Ildi und Ladl. Wollen Sie jedoch im Rahmen der IEC 61850 zeitkritische Vorgänge stabil in den Griff bekommen, liegen die Anforderungen deutlich höher. Sie haben bereits einige Unterscheidungsmerkmale kennen gelernt. Hier noch einige Tipps:

- Nehmen Sie Switches mit Ein- und Ausgangsspeicher je Port; das ermöglicht das nahezu verzögerungsfreie Durchleiten von Telegrammen und steigert die Geschwindigkeit beim Datenaustausch auf ein Maximum.
- Achten Sie auf eine stabile Spannungsversorgung. Optimal ist die Möglichkeit, den Switch an die vorhandene Hilfsgleichspannung anschließen zu können, die Sie auch zur Versorgung der Schutzgeräte verwenden.
- Ganz wichtig: Switches, die in Energieanlagen installiert sind, müssen den geltenden EMV-Bestimmungen genügen.
- Switches, die Sie in Verbindung mit IEC 61850 einsetzen, sollten unbedingt die Priorisierung von GOOSE-Telegrammen unterstützen.
- Die im Ringmanagement eingesetzten Switches müssen unbedingt FEFI unterstützen.
- Legen Sie Wert auf administrative Komfortmerkmale wie die Möglichkeit zur Netzwerküberwachung durch SNMP.

Fazit: Den Switch Ihrer Wahl werden Sie in der Regel nicht beim IT-Discounter finden. Wir empfehlen Ihnen gegen Kommunikationsprobleme Switches von RuggedCom. Mit diesen haben wir in einer Vielzahl von Tests positive Erfahrungen gesammelt.

Das Kommunikationsmodul

Wir wissen alle: Ohne die richtigen Kontakte geht gar nichts, das gilt für´s Leben und erst recht für die Technik. Wenn wir im Leben von “Vitamin B” sprechen, meinen wir damit in unserem technischen Fall Port B, also die Systemschnittstelle. Denn auf dieser wird das Modul EN100 montiert, das für eine ordentliche Kommunikation nach IEC 61850 über Ethernet sorgt.

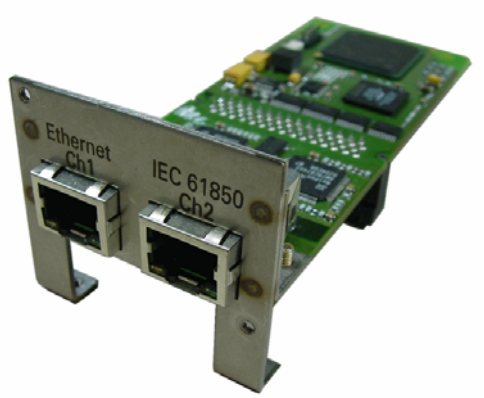
Eine ausführliche Beschreibung zum EN100-Modul erhalten Sie in einem separaten Handbuch. Dieses können Sie sich als PDF-Dokument von der Website **www.siprotec.de** herunterladen. Wir geben Ihnen an dieser Stelle einen kurzen Abriss.

Von 0 auf EN100

Das Modul EN100 stellt uns nicht nur die passenden physischen Schnittstellen für einen probaten Anschluss ans Netz zur Verfügung. Auf ihm ist auch die komplette Logik und das Protokoll für die Norm IEC 61850 implementiert. Das heißt für Sie, dass Sie keinesfalls außen vor sind, falls sich ein SIPROTEC 4 Gerät bereits etwas länger in Ihrem Besitz befindet. Mit einem Firmware-Update auf die Version 4.6 oder höher lässt sich so manches Gerät auf Trapp bringen und auf den Einbau eines Moduls EN100 seelisch vorbereiten. Ob Ihr Gerät für diese Verjüngungskur geeignet ist, erfahren Sie direkt von Ihrem SIEMENS-Ansprechpartner. Hier geht es jetzt erst einmal weiter mit einer Übersicht zu den einzelnen Varianten des Moduls EN100.

Zweieiige Zwillinge

Siemens liefert Ihnen das Modul EN100 passend zu einer elektrisch oder auch optisch ausgeführten Topologie. Die elektrische Anschlussvariante des Moduls gibt es für Einbau- und Aufbaugehäuse. Für Geräte im Einbaugehäuse ist zusätzlich eine optische Variante lieferbar. Natürlich sind alle Varianten für ein 100 MBit-Netzwerk geeignet. Elektrische Signale werden über RJ45-Stecker geführt, das Licht bahnt sich über Duplex-LC-Steckverbinder seinen Weg.



Mit dem zweiten fährt man besser: Die physischen Schnittstellen des EN100 sind doppelt ausgeführt

Allen Ausführungen ist gemeinsam, dass die physischen Schnittstellen doppelt vorhanden sind. In den Bildern links ist das gut zu erkennen. Dabei ist immer nur eine der beiden Schnittstellen aktiv, die andere wird passiv überwacht. Ist die aktive Schnittstelle gestört, wird automatisch innerhalb weniger Millisekunden auf die bis dato passive umgeschaltet. Mit diesem Feature, das amtlich als Betriebsart **Linie** bezeichnet wird, lassen sich in Verbindung mit externen Switches also leicht redundante Strukturen aufbauen.

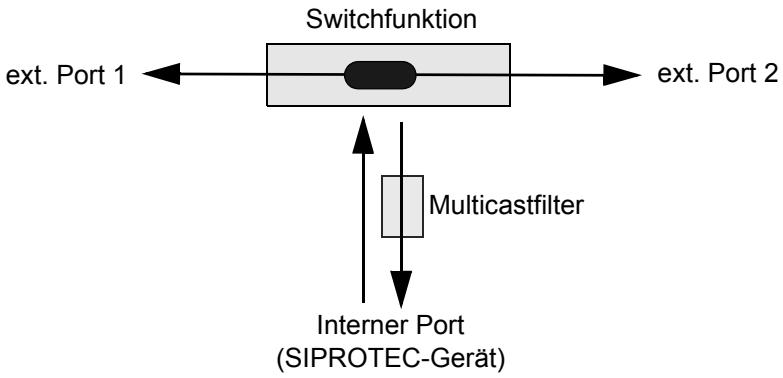
Beide physischen Verbindungen werden geräteintern überwacht. Bei einer Unterbrechung wird eine entsprechende Meldung generiert und im Betriebsmeldepuffer gespeichert. Per Parametrierung rangieren Sie diese dann leicht beispielsweise auf Kontakte, LED oder CFC.

Falls Sie sich für EN100-Module in der optischen Variante entscheiden, schlagen Sie gleich zwei Fliegen mit einer Klappe. Denn diese Modulvariante hat zusätzlich einen Switch mit an Bord. Sie können die beiden Schnittstellen also alternativ dazu nutzen, Signale weiterzuleiten. Die Betriebsart **Switch** ist dann auch die Standardeinstellung beim optischen Modul. Sie ändern diese nur, wenn das Modul im Linienbetrieb eingesetzt werden soll. Der integrierte Switch wird dann automatisch abgeschaltet.

Natürlich ist es auch optisch ein Leckerbissen: Die physischen Schnittstellen des EN100-O sind geschützt

Enge Bande

Die Switchfunktion arbeitet als Bindeglied zwischen Gerät und den beiden Schnittstellen. So realisieren Sie leicht eine Ringtopologie, wie wir diese in Kapitel 2 beschrieben haben und sparen sich zumindest bei der Verbindung der SIPROTEC 4 Geräte untereinander externe Switches.



Gekonnt integriert: Das optische Modul besitzt eine Switchfunktion.

Prinzipiell handelt es sich um einen Switch mit drei Ports. Einer ist fest mit dem MAC (Medium Access Controller) des Prozessors verbunden. Über die beiden anderen, externen Ports ist das Gerät in das Netzwerk integriert. Da sich auf diesem alle Arten von Telegrammen tummeln, also Unicast, Multicast oder Broadcast, passiert jedes dieser Telegramme mindestens einen externe Port und wird dann artgerecht behandelt:

- **Unicast-Telegramme ...**
  ... also solche, die nur für ein bestimmtes SIPROTEC 4 Gerät bestimmt sind, werden nur dann an den internen Port weitergeleitet, wenn sie genau an das aktuelle Gerät adressiert sind. Und dort bleibt es dann auch, sprich: Es wird aus dem Telegrammverkehr entfernt. Ist das Telegramm jedoch nicht an das aktuelle Gerät gerichtet, interessiert sich das Kommunikationsmodul auch gar nicht weiter dafür: Es leitet dieses Telegramm direkt an den jeweils anderen externen Port weiter. Unicast-Telegramme, die das Gerät selbst sendet, fügt das Kommunikationsmodul über beide Ports in den Datenstrom ein.
- **Multicast-Telegramme ...**
  ... sind immer für mehrere Empfänger bestimmt. Bei der Querkommunikation zwischen den einzelnen Teilnehmern gibt es noch eine weitere Eigenheit. Multicast-Telegramme werden dabei nach Eintreten eines Ereignisses wiederholt im Abstand von wenigen Millisekunden an alle Teilnehmer gesendet. Dies bedeutet eine hohe Belastung jedes Empfängers, obwohl die Telegramme möglicherweise nicht für ihn bestimmt sind. Deshalb ist in Empfangsrichtung des internen Ports ein Multicastfilter integriert. Dieses lässt tatsächlich nur Telegramme passieren, welche die Adresse des jeweiligen Teilnehmers enthalten. Unabhängig davon werden Multicast-Telegramme immer an den jeweils anderen externen Port des Kommunikationsmoduls weitergeleitet.
- **Broadcast-Telegramme ...**
  ... sind an sämtliche Teilnehmer gerichtet. Deshalb leitet das Kommu-

nikationsmodul diese auf seinen internen Port weiter und ebenso auf den jeweils anderen externen Port. Broadcast-Telegramme treten in IEC 61850 Netzen nur auf, wenn auf demselben Netzwerk ein oder mehrere andere Protokolle verwendet werden. Davon raten wir aber dringend ab.

PS

Zwei Fakten möchten wir an dieser Stelle nicht unerwähnt lassen:

1. In Verbindung mit optischen EN100-Modulen lassen sich Ringe mit maximal 30 Geräten aufbauen, sofern Sie innerhalb eines Rings nur einen externen Switch verwenden. Bei zwei externen Switches sinkt die Anzahl auf 27. Mit folgender Formel prüfen Sie leicht, ob die Rechnung in Ihrem speziellen Fall aufgeht:

   Anzahl SIPROTEC 4 Geräte + 3*Anzahl ext. Switches < 34

2. Das EN100-Modul sollte möglichst nicht als Root-Switch konfiguriert werden, da sonst der gesamte Datenverkehr ab der logischen Trennstelle über dieses Modul laufen würde. Wir empfehlen Ihnen, für diesen Zweck immer einen externen Switch zu verwenden. Das gilt auch für den Ersatz-Switch, der im Notfall für den Root-Switch einspringen soll.

Zeitserver

Alles ist eine Frage der Zeit, genauer gesagt der richtigen Zeit. Dass beispielsweise Systemzeit und -datum Ihres Rechners falsch eingestellt sind, können Sie leicht an unterschiedlichen Symptomen erkennen:

- Dem Datum nach sind Sie noch gar nicht geboren.
- Ihre eMails kommen beim Empfänger stets früher an, als Sie diese abgeschickt haben.
- Sie verlassen jeden Tag deutlich zu früh Ihren Arbeitsplatz.

Reden wir oben von in der Regel meist unkritischen Ereignissen, ist in praktisch allen Anlagenstrukturen eine korrekte Systemzeit unverzichtbar. So müssen sich alle SIPROTEC 4-Geräte, wie natürlich IEDs anderer Hersteller ebenso, auf eine einheitliche Zeitbasis synchronisieren, um das zeitlich korrekte Erfassen und Dokumentieren von Ereignissen gewährleisten zu können. Wir benötigen dazu zwei Dinge: a) Eine verlässliche Zeitquelle und b) einen Mechanismus, der jedem Teilnehmer diese Zeit zur Verfügung stellt. Als vertrauenswürdige Zeitquelle bedienen wir uns eines Zeitservers und der Mechanismus heißt NTP: Network Time Protocol.

Es ist serviert

Kümmern wir uns zunächst um den Zeitserver. Wir empfehlen Ihnen dazu einen NTP-fähigen Hardware-Zeitserver, wie ihn beispielsweise die Firmen Hopf und Meinberg in unterschiedlichsten Ausführungen anbieten. Ein solcher Zeitserver speist seine UTC-Zeit an irgendeiner Stelle ins Netz ein. Damit diese auch immer korrekt ist, bezieht er per Funk ein Zeitzeichensignal, zum Beispiel GPS, anhand dessen er seine eigene Uhrzeit synchronisiert.

Hinweis am Rande:
Um andere Geräte auf dieselbe Zeit zu synchronisieren, muss der Zeitserver selbst nicht unbedingt synchronisiert sein. Jeder Teilnehmer kann also nur davon ausgehen, dass seine anderen Kollegen dieselbe Uhrzeit verwenden; ob diese jedoch grundsätzlich korrekt ist, kann kein Teilnehmer beurteilen.

Neben NTP-Servern als eigenständigem Gerät können Sie auch auf Softwarelösungen in Verbindung mit einem Industrie-PC zurückgreifen - oder gar das Zeitsignal aus dem Internet beziehen. Von zweiter Möglichkeit raten wir Ihnen jedoch mit aller Entschiedenheit ab, da ist es noch sicherer, die Zeit nach Ihrer Armbanduhr zu stellen. Internetbasierte Zeitinformationen liegen vollkommen außerhalb Ihrer Kontrolle. Sie können weder die Qualität der gelieferten Information beurteilen noch die dauerhafte Verfügbarkeit garantieren. Auch Softwarelösungen sind nicht uneingeschränkt zu empfehlen; zumindest Systeme, die unter Windows laufen, sind nicht in der Lage, dauerhaft korrekte Ergebnisse millisekundengenau zu liefern.

Unser Resümee: Für wen die genaue und stabile Zeit in einem Netzwerk eine wichtige Rolle für den sicheren und reibungslosen Ablauf spielt, für den gibt es keine Alternative zu einem eigenen Zeitserver.

Protokollführer

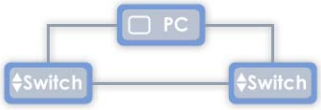
Ein Zeitserver allein nutzt jedoch noch nichts. Erst in Verbindung mit dem Network Time Protocol kommt die Sache zum Laufen. NTP basiert auf dem Client/Server-Prinzip und hat im Wesentlichen zwei grundlegende Aufgaben:

1. NTP muss das Verteilen der Zeitinformation eines oder auch mehrerer Zeitserver an die vorhandenen Clients koordinieren, sodass alle Uhren im Netzwerk immer bezüglich einer Referenzuhrzeit übereinstimmen.
2. NTP muss die Uhren-Frequenzen von Server und Clients synchronisieren, damit diese stets gleichmäßig ticken.

Um das Prinzip des NTP-Protokolls verständlich zu machen, reduzieren wir es einfach wieder auf seine grundlegende Wirkungsweise. Der Client schickt an den Server eine NTP-Message nach dem Motto “Haste mal die Zeit für mich?”. Der Server nimmt dieses Telegramm, tauscht hier und da einige Informationen und schickt es an den ursprünglichen Absender, also den Client, zurück. Dieser hat nun vier Zeitstempel zur Verfügung. aus diesen vier Werten berechnet er sich die Differenz der Referenzzeit zu seiner eigenen Zeit. Dieses Delta ist dann der Wert, um welchen er seine eigene Zeit korrigieren muss.

Standhaft bleiben

Zum Synchronisieren der Uhrzeit lassen sich in DIGSI 4 unterschiedliche Verfahren projektieren, auch in Verbindung mit dem EN100-Modul. Für eine “normale” Kommunikation über das Office-Ethernet mag diese Vielfalt ihre Berechtigung haben. Für die Kommunikation nach IEC 61850 ist jedoch die Synchronisierung mithilfe von NTP die einzig offiziell freigegebene Methode.



Hinweis am Rande:
Ein Gerät lässt sich ebenfalls synchronisieren, indem man es über Port A mit Zeittelegrammen versorgt. Dies erfordert aber zusätzliche Verdrahtung, weshalb NTP eindeutig der Vorzug zu geben ist.

Dazu muss man sich Folgendes vor Augen halten: Alle in den Meldepuffern eines SIPROTEC-Gerätes gespeicherten Absolutzeiten sind Ortszeiten. Das EN100-Modul wandelt diese Ortszeiten in das für die IEC 61850 benötigte UTC-Format um (UTC = Universal Coordinated Time). Das größte Problem ist dabei die in den meisten Ländern übliche Umstellung zwischen Sommer- und Winterzeit. So haben wir nach dem Umstellen der Uhr von Sommer- auf Winterzeit beispielsweise die Zeit 2:10 Uhr zwei Mal.

Damit das Modul die beiden Ortszeiten in die jeweils richtige Weltzeit umwandeln kann, benötigt es also die Information, ob es sich zum jeweiligen Zeitpunkt um die Sommerzeit oder die Winterzeit handelt. Neben NTP liefert einzig DCF77 diese Information, IRIG-B, interne Uhrzeitführung, Minutenimpuls und weitere aber nicht. Also nochmals unser eindringlicher Tipp: Halten Sie sich an die von der IEC 61850 vorgeschriebene Art der Zeitsynchronisierung, also NTP.

Netzwerkkarte

Erst ein PC macht Ihre Netzwerktopologie komplett. Ob nun das handliche Notebook, der Büro-Desktop für den täglichen Bedarf oder ein ausgewachsener Industrie-PC, für die Anbindung an das Netzwerk benötigen Sie in allen Fällen eine Netzwerkkarte. Wie diese allerdings konkret aussieht, entscheidet letztendlich der individuelle Bedarf an Sicherheit durch Redundanz. Für das gelegentliche Fernabfragen von Daten aus einem SIPROTEC-Gerät mag mitunter eine Standardkarte im Büro-PC genügen. Die Stationsautomatisierung, beispielsweise mit SICAM PAS, kann sich Abwesenheit vom Netz dagegen kaum leisten. Deshalb ist Redundanz auch bei den Netzwerkkarten angesagt.

Teamgeist

Prinzipiell könnten Sie die geforderte Redundanz auch mit zwei getrennten Netzwerkkarten in einem PC realisieren. Erheblich eleganter aber ist der Einsatz einer Dual-Port-Karte, wie beispielsweise der Intel® PRO/1000 MT. Eine solche Karte hat zwei unabhängig voneinander arbeitende Prozessoren, die auch über getrennte Ports und jeweils eigene IP-Adressen zugänglich sind. So könnten diese also auch grundsätzlich mit zwei unterschiedlichen, voneinander unabhängigen Netzwerken verbunden werden. Viel wichtiger ist für uns jedoch, dass sich beide Adapter mit einer gemeinsamen IP-Adresse ansprechen lassen. Diese Methode wird **Teaming** genannt, die Netzwerkkarte ist teamingfähig. Aus den möglichen Betriebsmodi wollen wir die beiden für uns relevanten erläutern.

Toleranzgrad

Das Bild rechts zeigt die Anschlussvariante für den **Adapter Fault Tolerance Modus**. Im Normalbetrieb läuft die Kommunikation über den ersten Adapter der Netzwerkkarte. Sobald dieser, das Kabel zum Switch oder der Switchport ausfällt, übernimmt der zweite Adapter die Verbindung. Der PC bleibt also weiterhin mit dem Netzwerk verbunden. Im oben Modus geht für den PC jedoch das Licht aus, sobald der Switch versagt. Mit dem **Switch Fault Tolerance Modus** bekommen Sie jedoch

auch diese Problematik in den Griff. Das Bild links zeigt, dass die beiden Adapter der Netzwerkkarte an je einem Switch angeschlossen sind. Auch die beiden Switches sind miteinander verbunden. Was für den Adapter Fault Tolerance Modus gilt, ist auch hier gültig. Zusätzlich ist nun aber auch der Ausfall eines kompletten Switches redundant abgesichert. Die Netzwerkkarte schaltet in einem solchen Fehlerfall selbsttätig auf den jeweils anderen Adapter um.

Beispielkonfiguration

5

Wir wollen in diesem Buch natürlich keine Luftnummern abliefern, sondern handfeste, nachvollziehbare Fakten. Deshalb soll eine einfache, aber durchaus praxisgerechte Konfiguration die Basis für unsere weiteren Erläuterungen sein.

In unserem Beispiel haben wir versucht, die bisher gezeigten Technologien und Komponenten zu einem sinnvollen Ganzen zu verbinden. Dieses Beispiel kann deshalb auch, mit einigen Erweiterungen hier und da, den Grundstock für Ihre eigene erste Netzwerkstruktur bilden.

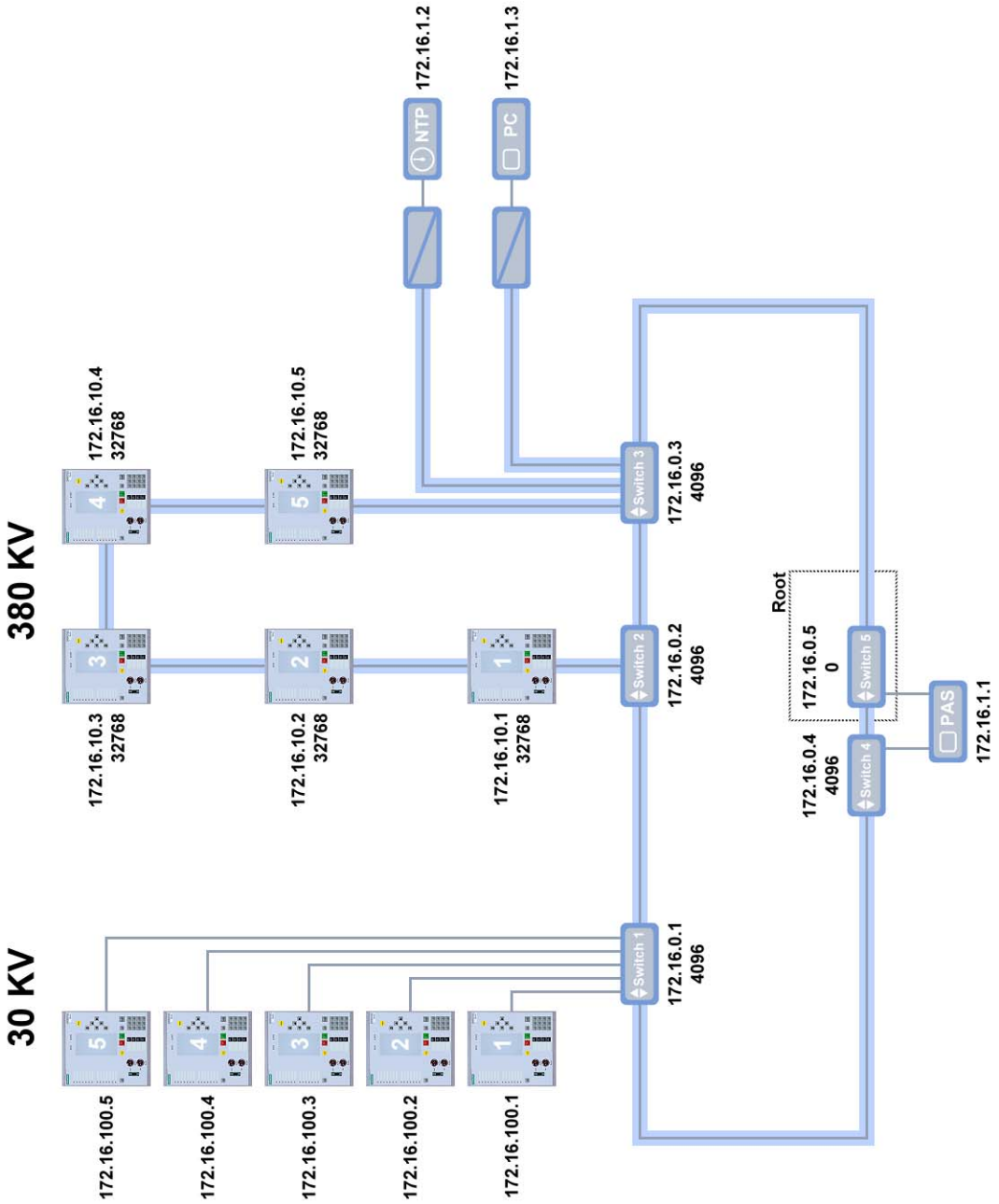
Topologie

Betrachten wir zunächst die Topologie unseres Beispiels. Ein Bild dazu finden Sie auf der nächsten Seite. Im linken Bereich sehen Sie fünf Schutzgeräte für die 30 KV Ebene. Diese sind sternförmig an einen Switch angeschlossen. Da die Geräte nicht weit voneinander entfernt stehen sollen, reichen Kabel von maximal 20 Metern Länge für die Verbindung zwischen Gerät und Switch. Das ist nämlich die Obergrenze für die Kabellänge bei einer elektrischen Verbindung, für die wir uns in diesem Fall dann auch entschieden haben. Die SIPROTEC 4 Geräte sind in diesem Fall also mit elektrischen Ethernet-Modulen ausgerüstet.

Einen anderen Ansatz zeigt die 380 KV Ebene. Ein Lichtwellenleiter verbindet fünf Geräte, die mit optischen Modulen ausgestattet sind, ringförmig miteinander. Der Ring wird durch zwei Switches geschlossen und ist damit nicht nur redundant hinsichtlich der Verbindung der Geräte untereinander. Auch der Anschluss an den Hauptring ist bei Ausfall eines der beiden Switches weiterhin gesichert.

Der Hauptring verbindet die Sternstruktur der 30 KV-Ebene mit der Ringstruktur der 380 KV-Ebene und schafft gleichzeitig die Anbindung an ein Automatisierungssystem, in unserem Fall SICAM PAS. Auch diese ist durch zwei Switches und eine teamingfähige Netzwerkkarte im Industrie-PC redundant ausgelegt.

Der NTP-Server koppelt sein Zeitzeichen ebenfalls redundant über die Switches 2 und 3 ein - Umsetzer schaffen dabei den Übergang von elektrischem Signal zur Lichtinformation. Einen PC mit DIGSI 4 an Bord schließen wir über einen Umsetzer an Switch 3 an. Auf Redundanz verzichten wir dabei - die Vorgänge sind in der Regel nicht zeitkritisch, sodass der Ausfall des PCs für kurze Zeit zu verkraften ist.



Eine Möglichkeit von vielen: Beispielkonfiguration mit elektrischer und optischer Verkabelung.

Komponenten

Als Switches empfehlen wir Produkte von RuggedCom, die wir auch für unsere Beispielkonfiguration einsetzen. Switch Nummer 1 für die sternförmige Verbindung ist ein RS 8000 T. Dieser kommt mit sechs elektrischen und zwei LWL-Anschlüssen daher. Er bietet damit sogar noch einen elektrischen Reserveport für eventuelle Erweiterungen und lässt sich über seine beiden optischen Schnittstellen leicht in den Hauptring einbinden.

Vom selben Typ sind übrigens auch die Switches 4 und 5. Von den sechs elektrischen Ports pro Switch werden allerdings nur jeweils einer genutzt, um die teamingfähige Intel PRO/1000 MT ans Netz zu hängen. Hier bleibt Ihnen also noch genügend Freiraum, um beispielsweise einen zweiten Industrie-PC mit installiertem SICAM PAS einzubinden. Damit erreichen Sie dann vollständige Redundanz auch auf der Automatisierungsebene.

Die ringförmig verbundenen IEDs der 380KV-Ebene binden wir über zwei Switches des Typs RS 1600 redundant in den Hauptring ein. Dieser Typ besitzt ausschließlich optische Ports und ist deshalb an dieser Stelle prädestiniert.

Die Zeichen der Zeit gehen beispielsweise von einem Hopf GPS System 7001 aus. Im 19”-Rack dieses modularen Systems ist neben dem Netzteil und der LAN-Karte Platz für mehrere Zeit-Server in Form einzelner Steckkarten. Alternativ könnte auch das Stationsleitsystem, in unserem Fall eine SICAM PAS, die Funktion des Zeit-Servers übernehmen.

IP-Adressen

Betrachten wir die Anzahl der Schutzgeräte, Switches und sonstiger Komponenten, genügen noch zwei Hände und zwei Füße zum Zählen. Der Adressraum eines Klasse-C-Netzes mit seinen 254 adressierbaren Teilnehmern würde also locker ausreichen, jeden Mitstreiter eindeutig zu identifizieren und böte überdies noch hinreichend Spielraum für Erweiterungen. Dennoch haben wir uns für das private Klasse-B-Netz 172.16.x.x (Netzmaske 255.255.0.0) entschieden.

Der Grund dafür ist einfach: Durch den zusätzlichen dritten Dezimalblock, der beim Klasse-B-Netz zur Verfügung steht, bieten sich erheblich mehr Möglichkeiten für eine strukturierte Adressierung. So können wir IP-Adressen für Schutzgeräte beispielsweise spannungsbezogen vergeben. Auch einzelne Komponententypen wie Switches sind bei geschickter Aufteilung sofort als solche nur anhand der IP-Adresse identifizierbar.

Switch-Prioritäten

Im Bild zu unserer Beispielkonfiguration finden Sie jeweils unterhalb der IP-Adresse die Priorität eines Teilnehmers. Falls Ihnen die einzelnen Zahlenwerte Rätsel aufgeben sollten, hier die Auflösung: Der Wert 0 kennzeichnet die höchste Priorität, alle weiteren Prioritäten sind um den festgelegten Wert 4096 abgestuft. So ergibt sich eine Reihe von festen Prioritätswerte: 0, 4096, 8192, 12288, 16384, usw.

Als Root haben wir Switch 5 auserkoren. Deshalb erhält dieser die höchste Priorität, also den Wert 0. Switch 4 gleich nebenan soll bei Ausfall des Root-Switches übernehmen. Seine Priorität liegt daher eine Stufe niedriger und das entspricht dem Wert 4096. Diese Priorität vergeben wir übrigens auch an die übrigen Switches im Hauptring. Die teamingfähige Netzwerkkarte in der PAS wird dennoch dafür sorgen, dass Switch 4 im Notfall übernimmt.

Bei der logischen Trennstelle, also dem Alternate Port, legen wir uns nicht weiter fest. Wir weisen einfach allen optischen EN100-Modulen die Priorität 32768 zu.

Projekt anlegen und strukturieren

6

Trotz der Erweiterung um IEC 61850 bleibt das Projektieren mit DIGSI 4 gewohnt einfach, auch wenn an der einen oder anderen Stelle ein paar Handgriffe mehr nötig sind. Dass Sie mit DIGSI 4 vertraut sind, müssen wir an dieser Stelle voraussetzen. Falls dem nicht so ist, dann empfehlen wir Ihnen unseren Leitfaden **DIGSI 4 - Start Up**, ein Schnupperkurs auf kompakten 60 Seiten. Von ebenso übersichtlichem Umfang ist das Pendant **Ethernet & IEC 61850 - Start Up**. Darin beschreiben wir anhand eines einfachen Beispiels unter anderem die Querkommunikation zwischen den Geräten, auch GOOSE genannt, die wir an dieser Stelle allerdings völlig ausklammern.

Schrittfolge

In diesem Kapitel werden wir Ihnen bezogen auf unsere Beispielkonfiguration folgende Schritte erläutern:

- Schritt 1: Projekt anlegen
- Schritt 2: SIPROTEC 4 Geräte einfügen
- Schritt 3: IEC 61850-Station einfügen
- Schritt 4: Geräte als Teilnehmer in der IEC 61850-Station eintragen

Projekt anlegen und Geräte einfügen

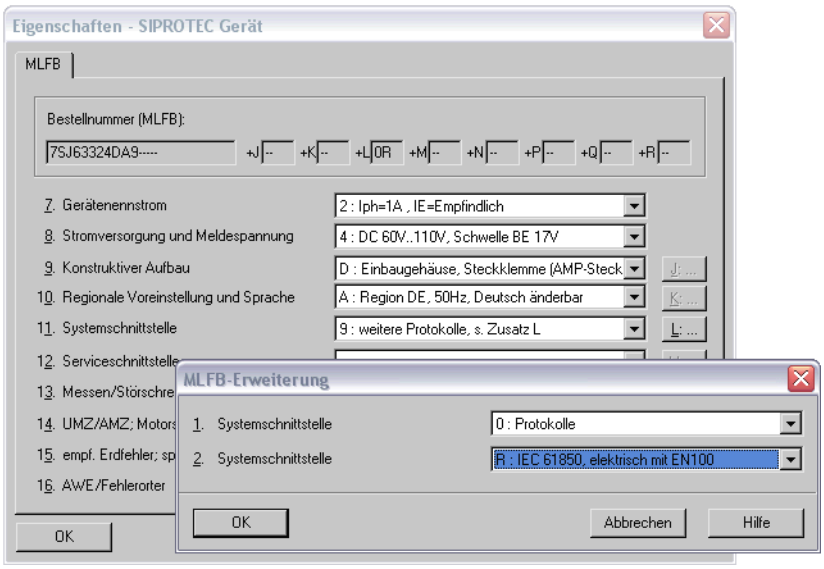
Für unser Beispiel werden wir ein neues Projekt anlegen. Das soll aber nicht heißen, dass Sie eine IEC 61850-konforme Kommunikation über Ethernet nicht auch in ein bestehendes Projekt integrieren dürften. Selbstverständlich können im selben Projekt und damit in derselben Anlage auch Geräte enthalten sein, die andere Protokolle oder andere Übertragungswege zur Kommunikation verwenden. Allerdings lassen sich diese nicht in die Kommunikation nach IEC 61850 einbinden.

Man nehme

In unser frisch gebackenes Projekt fügen wir als erstes 2 Ordner ein, mit denen wir die beiden Spannungsebenen 30 KV und 380 KV voneinander unterscheiden. Diese Ordner nehmen anschließend die benötigten Geräte auf. Diese Unterteilung wäre zwar nicht nötig, schafft aber Ordnung und Übersicht.

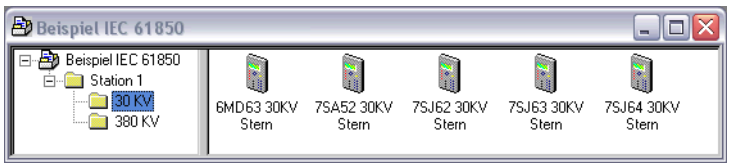
Für eine Kommunikation via Ethernet und IEC 61850 sind SIPROTEC 4 Geräte ab Version 4.6 geeignet. Stellen wir uns vor, Sie haben ein solches frisch vom Produktionstisch erworben und wollen es nun in eine bestehende oder auch neue Topologie integrieren.

In DIGSI 4 gehen Sie dazu vor wie Sie es von je her gewohnt sind: Sie fügen diese wie auch alle anderen SIPROTEC-Geräte per Drag & Drop aus dem Gerätekatalog in das betreffende Projekt ein. Bevor das SIPROTEC 4 Gerät im Projekt platziert wird, müssen Sie die Geräteausführung in DIGSI 4 festlegen. Dazu wird die Registerkarte **MLFB** im Dialog **Eigenschaften SIPROTEC-Gerät** angezeigt.



Wichtig: Stellen Sie die korrekte Systemschnittstelle in der passenden Variante ein

Sie wählen also aus den möglichen Einstellungen diejenigen aus, die der MLFB Ihres Gerätes entsprechen. Für die System-Schnittstelle wählen Sie die Einstellung **weitere Protokolle**. Durch diese Auswahl öffnet DIGSI 4 einen zweiten Dialog mit zwei Listenfeldern. Wählen Sie in der oberen Auswahlliste die Einstellung **Protokolle**. In der unteren Auswahlliste wählen Sie **IEC 61850** in der tatsächlichen Schnittstellenvariante - also optisch oder elektrisch. Sobald Sie beide Dialoge nacheinander mit einem Klick auf **OK** geschlossen haben, fügt DIGSI 4 ein Symbol für das Gerät ins Projekt ein. Sind alle Geräte eingefügt, sollte das Projekt so aussehen, wie es sich im folgenden Bild der Öffentlichkeit zeigt.

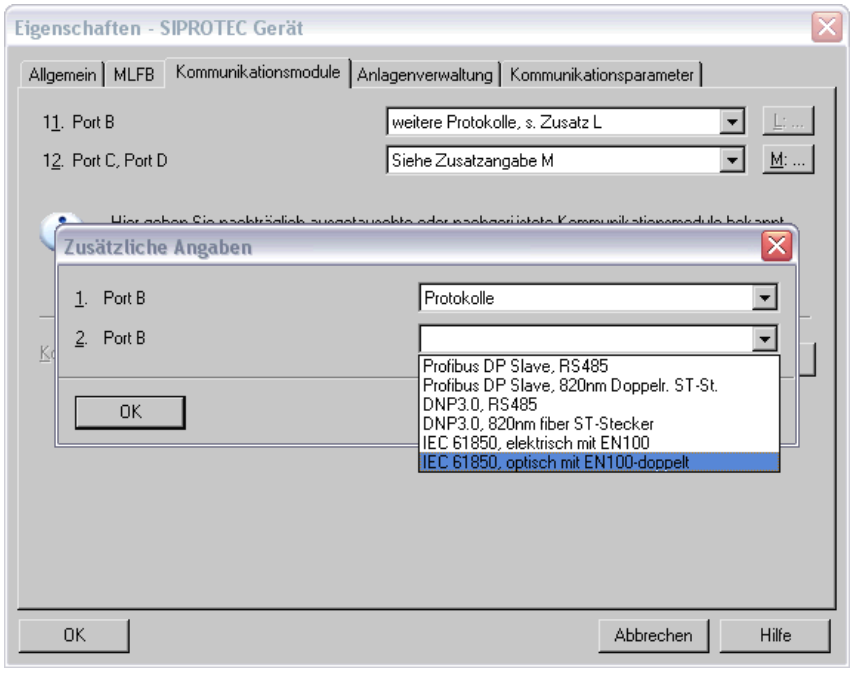


Die Geräte auf 30 KV-Ebene.

Die Geräte auf 380 KV-Ebene.

Plan B

Eine leicht veränderte Vorgehensweise ist dann angesagt, wenn Sie ein vorhandenes Gerät aufgerüstet, diesem also neue Firmware plus Kommunikationsmodul spendiert haben. Möchten Sie ein solches Gerät in ein neues Projekt integrieren, stellen Sie bitte immer die MLFB-Nummer ein, die auf Ihrem Gerät aufgedruckt ist. Das heißt, Sie wählen zunächst den Kennbuchstaben für die ursprüngliche System-Schnittstelle. Hat DIGSI 4 das Gerät in das Projekt eingefügt, öffnen Sie den Eigenschaftendialog des Gerätesymbols und wählen in der Registerkarte **Kommunikationsmodule** als Schnittstelle das Modul **EN100**.

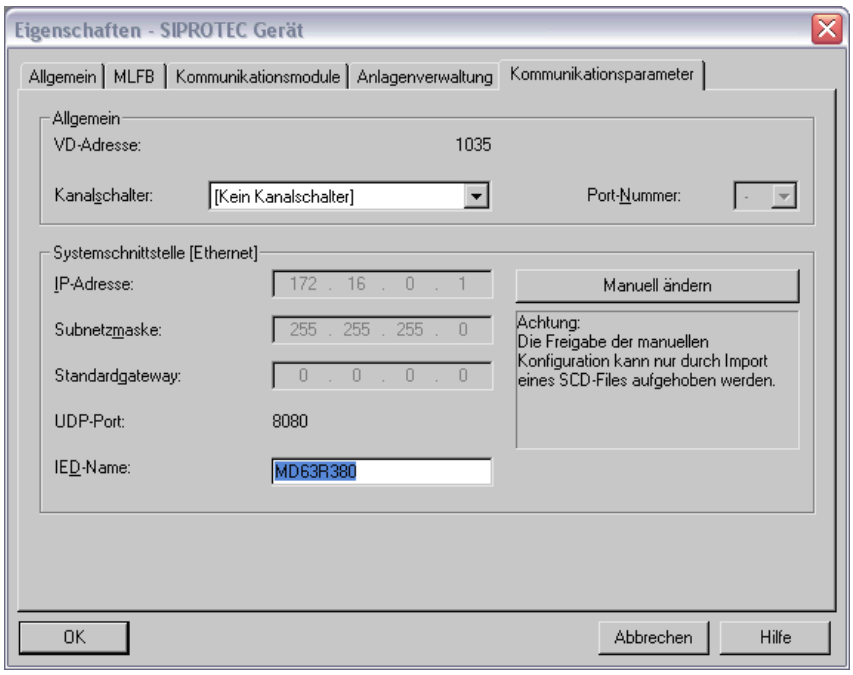


Nachträglicher Eingriff: DIGSI 4 muss unbedingt Bescheid wissen!

Ist das Gerät bereits Bestandteil eines Projekts, können Sie dieses selbstverständlich an Ort und Stelle belassen und sich so die erneute Eingabe der individuellen Parametrierung sparen. Allerdings müssen Sie dafür sorgen, dass das Gerät passend zur aktualisierten Firmware auch einen Basisparametersatz der Version 4.6 erhält. Ansonsten steht Ihnen die benötigte Schnittstellenvariante erst gar nicht zur Auswahl. Klicken Sie dazu mit der rechten Maustaste auf das Gerätesymbol. Aus dem Kontextmenü wählen Sie **Parametersatz aktualisieren**. Falls keine aktuelleren Parametersätze zum betreffenden Gerätetyp installiert sind, erhalten Sie dazu eine Meldung. Ansonsten wird der Dialog **Parametersatz aktualisieren** geöffnet. Im oberen Bereich wird Ihnen die Versionsnummer des derzeitig verwendeten Parametersatzes angezeigt. Mit Hilfe der Auswahlliste **Neue Parametersatzversion** wählen Sie eine Versionsnummer ab 4.6 und klicken danach auf **OK**. Falls Sie die erwähnte Meldung mangels aktuellerem Parametersatz zu Gesicht bekommen haben, schaffen Sie leicht Abhilfe, indem Sie die DIGSI-Programm-CD einlegen und den fehlenden Parametersatz, das heißt also die jeweiligen Gerätedaten nachinstallieren. Die aktuellen Daten finden Sie übrigens immer im Internet unter www.siprotec.de.

Namenstag

Wie Sie in den Bildern unseres Projekts sehen können, haben wir die Geräte mit aussagekräftigen Namen versehen. Auch innerhalb eines IEC 61850-Netzes benötigt jeder Teilnehmer einen eindeutigen Namen. Ein solcher Name darf jedoch maximal aus acht Buchstaben oder Zahlen bestehen. Dabei sind keine Umlaute oder Leerzeichen erlaubt und das erste Zeichen muss zudem noch ein Buchstabe sein. Da wir die wesentlich freizügigere Handhabung bei der Vergabe eines Gerätenamens innerhalb des Projektes nicht einschränken wollten, gab es nur eine Lösung: Ein zusätzlicher Name musste her, der so genannte IED-Name.



Der IED-Name ist Teil der Kommunikationsparameter eines SIPROTEC 4 Gerätes und wird bei IEC 61850 als Gerätename verwendet

Wie Sie im Bild oben sehen, legen Sie diesen IED-Namen im Eigenschaftendialog des jeweiligen Gerätes fest. Wenn Sie keine besonderen Ansprüche an die Namensgestaltung stellen, müssen Sie sich nicht weiter darum kümmern. Der DIGSI Manager legt nämlich automatisch einen eindeutigen Namen fest. Dieser besteht aus dem Präfix **IED_** und einer vierstelligen fortlaufenden Zahl.

Wir empfehlen Ihnen jedoch, sich die Zeit zu nehmen, sinnvolle Namen zu vergeben, die Ihnen im weiteren Verlauf zur eindeutigen Identifizierung der Teilnehmer dienen können. Die IED-Namen werden nicht nur im DIGSI Systemkonfigurator angezeigt (den Sie in Kürze kennen lernen werden), sondern sind bei IEC 61850 auch Bestandteil des Telegrammverkehrs. Haben Sie vor, diesen mit Diagnosetools zu überwachen, sind leicht zuordenbare Namen ein nicht zu unterschätzender Vorteil.

Für unsere Beispielkonfiguration basteln wir Namen, die Auskunft geben über den Gerätetyp, die Topologie (Ring oder Stern) und die Spannungsebene. **MD63R380** sagt uns daher, dass es sich um ein Gerät des Typs 6**MD63** handelt, das auf **380** KV-Ebene in einen **R**ing eingebunden ist.

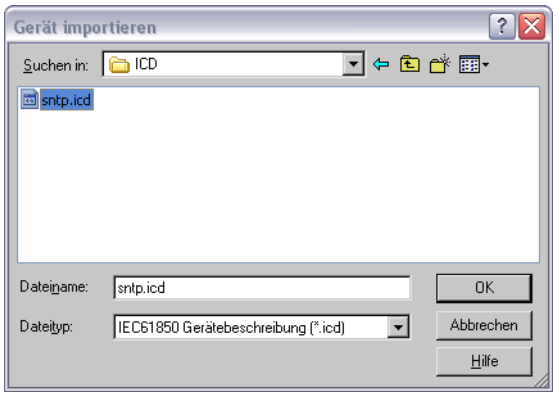
Station hinzufügen und Teilnehmer festlegen

Zu einer ordentlichen Kommunikation nach IEC 61850 bedarf es einer so genannten IEC 61850-Station. Dieses neue Element im DIGSI Manager repräsentiert eine Schaltanlage, in welcher alle Geräte nach IEC 61850 über Ethernet miteinander kommunizieren. Welche Geräte das im Speziellen sind, wählen Sie, wie Sie gleich noch detailliert erfahren werden, bequem aus einer Liste aus und tragen diese als Teilnehmer in der IEC 61850-Station ein.

Hinweis am Rande:
Sie können grundsätzlich beliebig viele Zeit-Server in ein Projekt einfügen. Von DIGSI 4 unterstützt wird zurzeit jedoch nur ein Zeit-Server je Station. Sind mehrere Server projektiert so wird immer der mit der niedrigsten IP-Adresse angesprochen. Die IP-Adresse wird dem Zeit-Server erst später während der Netzwerkkonfiguration mit dem DIGSI Systemkonfigurator zugeteilt.

Die Teilnehmer sind dabei nicht auf SIPROTEC 4 Geräte beschränkt. DIGSI 4 erfüllt natürlich die Anforderungen der Norm und gibt Ihnen die Möglichkeit, IEC 61850-konforme Geräte anderer Funktionalität und von anderen Herstellern in ein Projekt einzubinden. Dazu importieren Sie die Gerätebeschreibung des jeweiligen Gerätes und fügen dieses anschließend als Teilnehmer der Station hinzu - auf die gleiche Weise wie auch bei SIPROTEC 4 Geräten. Das können wir gleich einmal für den benötigten NTP-Server erledigen.

Die benötigte Datei mit den gerätebeschreibenden Daten finden Sie auf der DIGSI-Installations-CD, und zwar im Verzeichnis **..\Utility \IEC61850 \ICD**. Wählen Sie im DIGSI Manager aus dem Kontextmenü **Neues Objekt einfügen → Anderer IEC61850-Teilnehmer**. Daraufhin wird ein üblicher Datei-Dialog geöffnet.



Ausgewählt ...

Mit dem gezeigten Dialog selektieren Sie die Gerätebeschreibung **sntp.icd**. Schon wird ein Symbol für den Teilnehmer in das Projekt eingefügt. Dieses ist einem normalen Gerätesymbol nicht unähnlich, wenngleich auch etwas bleichgesichtiger.

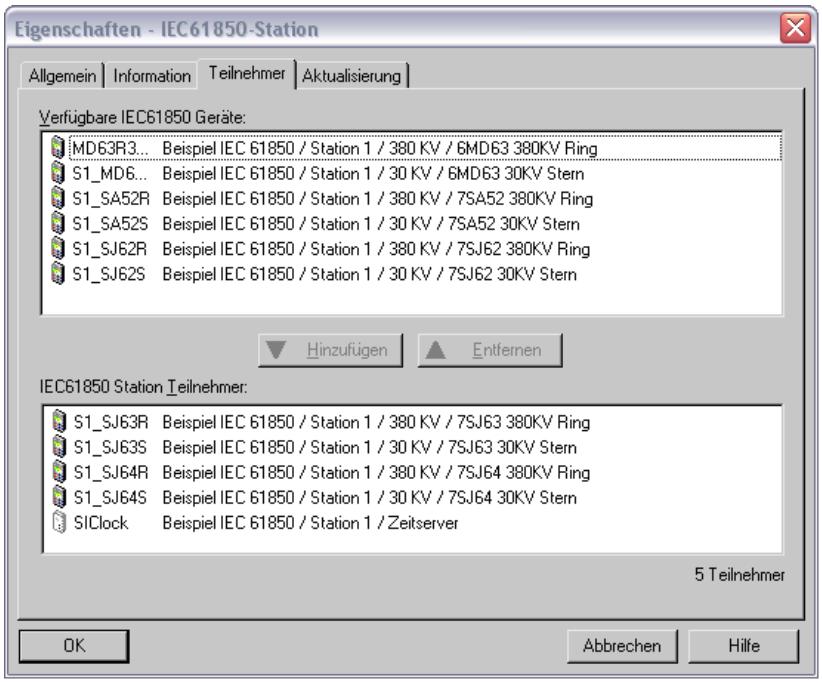
... und eingefügt. Das Einfügen des Zeit-Servers kostet Sie kaum Zeit.

Behausung

Nun wollen wir unsere Geräte und den Zeit-Server aber nicht länger im Regen stehen lassen, sondern dafür sorgen, dass diese endlich ein Dach über dem Kopf bekommen. Dazu fügen Sie eine IEC 61850-Station ein. Das erledigen Sie wieder per Kontextmenü, also **Neues Objekt einfügen → IEC61850-Station**. Schon erscheint innerhalb des Projektes ein schmuckes kleines Häuschen mit eigenem Strommast.

Dazwischengedrängelt: Die IEC-Station gibt den Teilnehmern ein Zuhause.

Das alleine genügt aber nicht, denn bisher weiß noch niemand (außer Ihnen und uns), dass die insgesamt zehn Schutzgeräte plus der Zeit-Server innerhalb der Station miteinander kommunizieren sollen. Deshalb müssen Sie diese Hardware noch als Teilnehmer in der Station eintragen. Öffnen Sie den Eigenschaftendialog der Station und wählen Sie die Registerkarte **Teilnehmer**.



Übersichtlich: Per Auswahlliste legen Sie die Teilnehmer einer IEC 61850-Station fest

Da Geräte und NTP-Server alle Voraussetzungen für eine IEC 61850-konforme Kommunikation erfüllen, werden Ihnen diese bereits als potenzielle Teilnehmer angezeigt. Jetzt müssen Sie diese noch in die Liste der tatsächlichen Teilnehmer übernehmen. Das funktioniert mit einem Doppelklick auf jeden gewünschten Namen nacheinander - oder per Mehrfachselektion. Dazu halten Sie die Umschalt- oder Steuertaste gedrückt und selektieren per Mausklick zusammenhängende Namensblöcke bzw. mehrere einzelne Namen. Die ausgewählten Namen befördern Sie nun mit einem Klick auf **Hinzufügen** in die untere Liste. Jetzt noch schnell auf **OK** geklickt und schon ist auch diese Arbeitsetappe geschafft.

Nur net hudle

Bitte versuchen Sie jetzt noch nicht, die Station per Doppelklick zu öffnen - es wird Ihnen noch nicht gelingen. Damit das funktioniert, müssen alle teilnehmenden SIPROTEC 4 Geräte vorher einmal geöffnet worden sein. Mehr dazu in Kapitel 8.

SIPROTEC 4 Gerät parametrieren

7

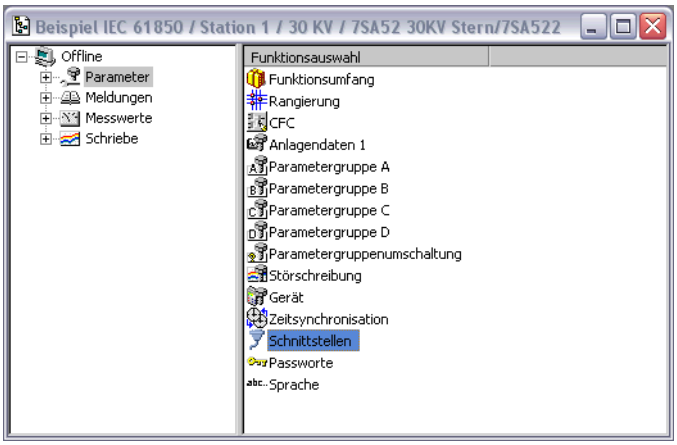
Wie immer möchte DIGSI 4 gerne über alles Bescheid wissen und ist dabei auf Ihre Unterstützung angewiesen. Im konkreten Fall benötigt die Software Informationen zum Modus der Schnittstelle, zur Redundanzart (OSM oder RSTP) und zur Art der Zeitsynchronisation. Und schließlich sind da noch Ihre eigenen spezifischen Parametereinstellungen, möglicherweise auch für die Kommunikation zwischen den einzelnen Geräten. Die beiden letzten Themen werden wir in diesem Buch nicht weiter besprechen. Zum einen ist Ihre individuelle Parametrierung weitestgehend unabhängig von der gewählten Kommunikationsform. Zum anderen gibt es das Buch **Ethernet & IEC 61850 - Start Up**. Und darin beschreiben wir ausführlich die Kommunikation zwischen den Geräten. Über den Rest allerdings geben wir Ihnen gerne Auskunft.

Offenlegen

Öffnen Sie zunächst eines der Geräte zur Bearbeitung. Am schnellsten erledigen Sie das mit einem Doppelklick auf das jeweilige Symbol. Mit welchem Gerät Sie dabei beginnen, bleibt Ihnen überlassen. Wir knöpfen uns als Erstes eines der Geräte aus der 380 KV-Ebene vor, ausgestattet mit einem optischen EN100-Modul.

Im Dialog zur Auswahl der Verbindungsart markieren Sie die Option **Offline**. Klicken Sie jetzt noch auf **OK** und schon nimmt alles seinen Lauf: Die DIGSI Gerätebearbeitung wird gestartet, die Daten des Geräts werden geladen.

Schnittstellenparameter einstellen

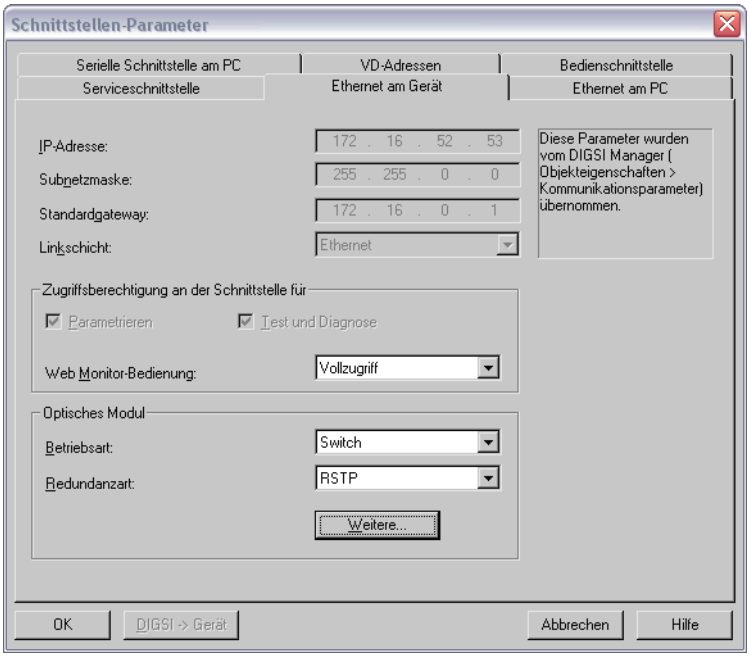


Mit einem Doppelklick fängt alles an.

Zu Beginn werden wir uns um das Ethernet-Modul kümmern. Dazu doppelklicken Sie in der Listenansicht der Gerätebearbeitung auf den Eintrag **Schnittstellen**, direkt unterhalb von **Zeitsynchronisation**. DIGSI 4 zeigt Ihnen daraufhin den Dialog **Schnittstellen-Parameter**. Dieser Dialog enthält je nach Ausstattung des Rechners und des SIPROTEC 4 Gerätes eine unterschiedliche Anzahl Registerkarten mit Einstellmöglichkeiten für die jeweiligen Schnittstellenparameter.

Wertebetrachtung

Uns interessieren davon vor allem die Parameter für das EN100-Modul, die in der Registerkarte **Ethernet am Gerät** zusammengefasst sind. Es gibt übrigens keine unterschiedlichen Registerkarten für die verschiedenen Modulbauweisen, wohl aber spezielle Parameter nur für die optische Schnittstelle.



Lesen und schreiben: Nicht alle Parameterwerte können verändert werden.

Die Werte für IP-Adresse, Subnetzmaske und Standardgateway haben an der aktuellen Stelle lediglich informativen Charakter - verändern können Sie diese nur im DIGSI Systemkonfigurator oder (eingeschränkt empfehlenswert) im DIGSI Manager. Die Sicherungsschicht, die die physische Verbindung des SIPROTEC 4 Gerätes mit anderen Komponenten beschreibt, ist sowieso unveränderbar auf **Ethernet** eingestellt.

Bei vielen aktuellen SIPROTEC 4 Geräten erhalten Sie Unterstützung bei der Inbetriebnahme, Prüfung und Betriebsführung auch ohne den Einsatz von DIGSI 4. Das Zauberwort heißt Webmonitoring. Dabei benötigen Sie lediglich einen beliebigen Web-Browser und können dann, beispielsweise auch über Ethernet, Informationen aus dem Gerät abrufen oder dieses sogar bedienen. Mit Hilfe von DIGSI 4 legen Sie den Grad des Zugriffs für die Webmonitor-Bedienung fest. Wählen Sie dazu aus der Auswahlliste eine der Einstellungen **Kein Zugriff**, **Lesen**, **Ändern** oder **Vollzugriff**. Die drei zuletzt genannten Zugriffsarten sind übrigens mit jeweils unterschiedlichen Passwörtern geschützt. Unser Tipp: Stellen Sie die Zugriffsart für den Normalbetrieb auf **Lesen** ein. Für die Inbetriebnahme empfehlen wir dagegen **Vollzugriff**. So können Sie jederzeit vom IBS-PC aus das Gerät vollständig bedienen.

Elektriker oder Optiker?

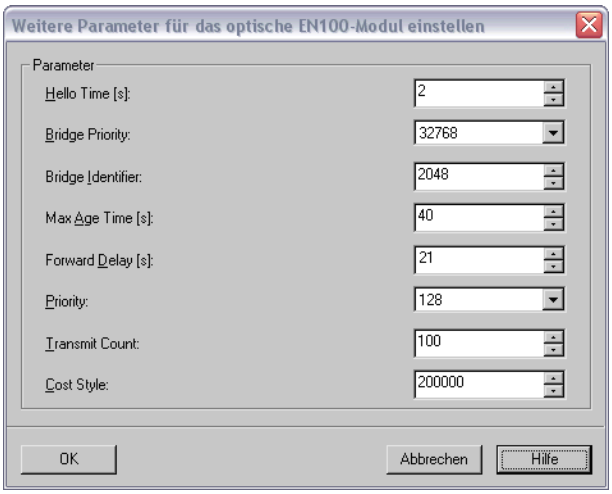
Mit dem elektrischen Ethernet-Modul an Bord haben Sie ansonsten ein leichtes Spiel, denn weitere Einstellungen gibt es dafür nicht. Schließlich kennt dieses Modul nur den Linienbetrieb und die Wahl einer speziellen Redundanzart ist dafür eben nicht vorgesehen.

Anders verhält es sich da schon mit dem optischen Modul. Verlässlichen Quellen zufolge (siehe Kapitel 4) beherrscht dieses nicht nur den Linienbetrieb, sondern lässt sich auch als Switch für einen Betrieb im Ring konfigurieren. Die gewünschte Betriebsart wählen Sie aus der gleichnamigen Auswahlliste. In Verbindung mit der Einstellung **Linie** gibt es wie bereits beim elektrischen Modul nichts weiter zu tun für Sie, außer mit einem Klick auf **OK** dem Dialog “Auf Wiedersehen” zu sagen.

Viel Geswitscher

Für den Einsatz als Switch und damit dem Betrieb im Ring wird es nötig, sich für eine Redundanzart zu entscheiden. RSTP und OSM heißen die beiden Kandidaten. Ihre Wahl ist natürlich abhängig davon, welcher Art der Ringsteuerung Sie bereits während der Konzeptionsphase den Vorzug gegeben haben. Für unsere Beispielkonfiguration war das RSTP.

Für diese Redundanzart sind noch eine Reihe weiterer Einstellungen möglich, allerdings nur an wenigen Stellen nötig. Anders ausgedrückt: Von den voreingestellten Werten sollten Sie nur gezielt und auf unsere Empfehlungen abweichen. Ein Klick auf **Weitere** gestattet Ihnen einen Blick auf die einzelnen Parameter und deren Einstellungen.



Nichts für Experimentierfreudige: Die vorgegebenen RSTP-Einstellungen sollten größtenteils beibehalten werden!

Rat schlagen

Folgende Ratschläge sollten Sie beherzigen, um eine korrekte Ringfunktionalität sicherzustellen:

- Stellen Sie den Parameter **Hello Time** auf 2 Sekunden ein. Wird innerhalb dieser eingegebenen Überwachungszeit 3 Mal hintereinander kein Testtelegramm empfangen, dann gilt die Verbindung als gestört.
- In Kapitel 4 haben wir Ihnen davon abgeraten, das EN100-Modul als Root-Switch zu konfigurieren. Belassen Sie deshalb am besten die

Bridge Priority auf dem voreingestellten Wert von 32768. Lediglich für das Modul, das möglicherweise als Alternate Bridge, also als logische Lücke dienen soll, stellen Sie die nächstniedrigere Priorität ein. Allerdings sollten Sie auch dabei versuchen, diese Funktionalität auf einen externen Switch zu verlagern.

- Um die in Kapitel 4 angesprochene maximale Anzahl von 30 Teilnehmern innerhalb eines Rings voll auszuschöpfen, muss die **Max Age Time** 40 Sekunden betragen. Tut sie das nicht, ist die Zahl der Geräte in einem Ring auf maximal 17 beschränkt.
- Der Parameter **Transmit Count** muss auf den Wert **100** eingestellt werden. Dieser Parameter gibt an, wie viele Konfigurationsnachrichten maximal nach einer Umkonfigurierung gesendet werden. Der Wert des Parameters sollte immer größer sein als die maximale Anzahl an Switches innerhalb eines Rings.

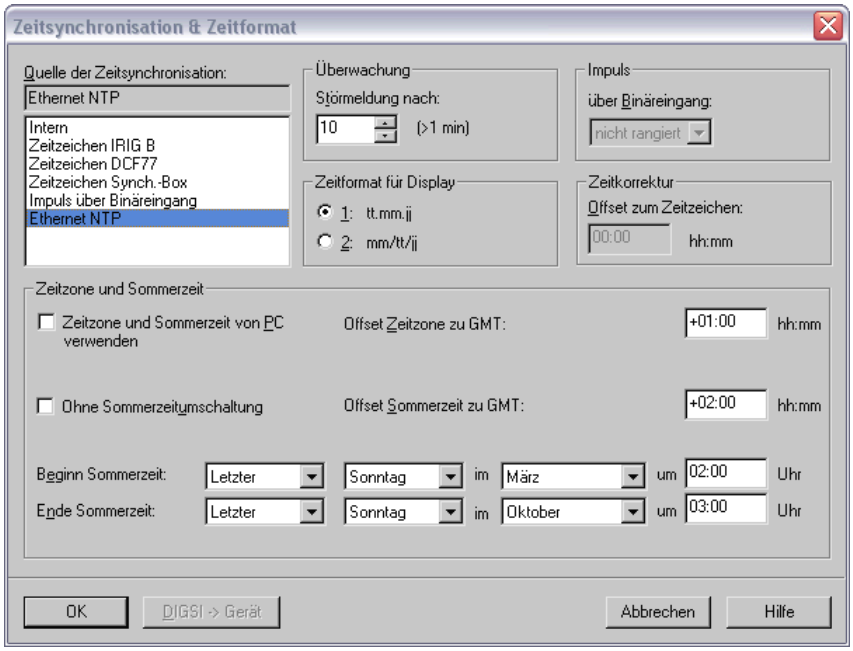
Die Werte aller weiteren Parameter belassen Sie bitte in der voreingestellten Form.

Parameter für Zeitsynchronisation einstellen

Dass unsere Entwickler (Jungs, ihr seid echt prima!) DIGSI 4 grundsätzlich für viele Verfahren zur Zeitsynchronisation fit gemacht haben, durften Sie bereits erfahren. Ebenso, dass für die Kommunikation über Ethernet das Network Time Protocol (NTP) die einzig vernünftige Methode ist, alle Teilnehmer auf Pünktlichkeit zu trimmen.

Erwartungshaltung

Da DIGSI 4 die Auswahl für eine bestimmte Art der Zeitsynchronisation Ihnen überlässt, müssen Sie der Software Ihre Entscheidung mitteilen, und zwar getrennt für jedes teilnehmende Gerät. Dazu doppelklicken Sie in der Listenansicht der Gerätebearbeitung auf **Zeitsynchronisation** und schon präsentiert sich Ihnen ein Dialog mit all den herrlichen Auswahlmöglichkeiten.



Mit der Zeit gehen: Für die Zeitsynchronisation über Ethernet sollte NTP gewählt werden

Klare Entscheidung

Im Feld **Quelle der Zeitsynchronisation** sehen Sie als eine der Auswahlmöglichkeiten **Ethernet NTP**. Diese Möglichkeit ist übrigens nicht immer wählbar, sondern nur dann, wenn Sie in den Eigenschaften des Gerätes ein Ethernet-Modul als System-Schnittstelle projektiert haben. Allerdings gibt es für keine der beiden Bauarten, optisch oder elektrisch, Unterschiede in der weiteren Parametrierung.

Würden Sie sich hier für eine der anderen Möglichkeiten entscheiden, erfolgte die Zeitsynchronisation nicht über das Ethernet-Netzwerk. Die notwendige Zeitinformation für das IEC 61850-Protokoll selbst würde dann vom Gerät an das Kommunikationsmodul geliefert. In unserer Beispielkonfiguration haben wir einen NTP-Zeitserver im Netz integriert. Deshalb markieren wir auch **Ethernet NTP**.

Warten auf Godot

Die Überwachungszeit gibt den maximal zulässigen zeitlichen Abstand zwischen zwei Synchronisationszeitpunkten an. Eine Störmeldung wird abgesetzt, sobald innerhalb des eingestellten Zeitraumes keine zwei Synchronisationszeitpunkte aufeinander folgen. Ab diesem Zeitpunkt wird im Zeitstempel aller Meldungen der Status **Uhrzeitstörung** gesetzt.

Welche Zeitdauer Sie hier wählen, ist letztlich eine Frage Ihrer Anlagenphilosophie. Unser Tipp: Die SIPROTEC 4 Geräte fragen die Uhrzeit annähernd jede Minute beim Zeit-Server ab. Dazwischen arbeiten sie mit der internen Quarzuhr, die sehr präzise ist. Daher können Sie die Voreinstellung von 10 Minuten belassen.

Die Überwachungszeit ist übrigens kein typischer NTP-Parameter, sondern kann bei allen Formen der Zeitsynchronisation eingestellt werden. Das gilt auch für die Darstellung des Zeitformats im Gerätedisplay: Der Standort des Gerätes oder möglicherweise auch nur Ihr Geschmack sind hier entscheidend.

Vier Jahreszeiten

Vielmehr sollten wir noch ein Augenmerk auf die individuelle Zeitzone und die Unterscheidung zwischen Sommer- und Standardzeit legen, auf die wir in Kapitel 4 eingegangen waren. Bei Letzterem dürfen Sie die Umschaltung in keinem Fall dem PC überlassen oder gar deaktivieren! Bei den konkreten Zeitangaben sind unsere Entwickler bereits in Vorleistung gegangen. Solange also das inoffizielle Bundesaufsichtsamt für Zeitsynchronisation keine neuen Vorgaben macht, können Sie die Werte, die Ihnen DIGSI 4 vorgibt und die auch in der Abbildung oben gezeigt werden, beibehalten.

Das war´s auch vorerst mit den Einstellungen zur Zeitsynchronisation, Sie dürfen den Dialog mit einem Klick auf **OK** schließen. Weitere Einstellungen für den NTP-Server selbst erledigen Sie mit Hilfe des DIGSI Systemkonfigurators und das besprechen wir ein wenig später. Also dran bleiben!

Sie sollten nun Ihre Einstellungen speichern und das Gerät schließen. Anschließend führen Sie die beschriebene Prozedur für alle weiteren Geräte durch, die in das Netzwerk eingebunden sind.

Netzwerk konfigurieren

8

Lassen Sie uns doch kurz Zwischenbilanz ziehen: Wir haben uns für eine Topologie entschieden und die IP-Adressen der einzelnen Kommunikationspartner festgelegt. Das DIGSI 4-Projekt ist angelegt, alle benötigten Geräte sind eingefügt und ordnungsgemäß als Teilnehmer in einer IEC 61850-Station eingetragen. Jetzt ist es an der Zeit, Beziehungen zwischen den einzelnen Teilnehmern zu knüpfen, diese also mit ihren gültigen IP-Adressen in ein Netzwerk einzubinden - alles immer noch auf rein virtueller Ebene.

Der Zugang zu Informationen über Kommunikationsverbindungen und Datenverknüpfungen zwischen den Teilnehmern ist das Stationselement. Konsequent zur gesamten Bedienphilosophie von DIGSI 4, nach der wir ein Objekt (Gerät, Abzweigsteuerbild, Logikbaustein-Plan) öffnen, um die zugehörigen Daten zu bearbeiten, öffnen wir also auch hier die Station – und starten damit den DIGSI Systemkonfigurator. Mit diesem legen Sie die Netzwerkstruktur sowie die Kommunikationseigenschaften der Teilnehmer und Netze fest und verknüpfen Datenobjekte einzelner Teilnehmer.

Mach keine Netzchen!

Bevor Sie nun aber ungezügelt loslegen, wollen wir Ihnen noch einige Hinweise mit auf den Weg geben. Damit sich der DIGSI Systemkonfigurator überhaupt starten lässt, müssen Sie jedes SIPROTEC 4 Gerät, das als Teilnehmer eingetragen ist, vorher wenigstens einmal geöffnet haben. Warum? Ganz einfach: Der DIGSI Systemkonfigurator bezieht seine Informationen über die einzelnen Teilnehmer aus den jeweiligen Gerätebeschreibungen (ICD-Dateien), die wir bereits in Kapitel 6 vorgestellt hatten. Deshalb ist es nötig, dass beim Öffnen einer IEC 61850-Station für jeden Teilnehmer eine ICD-Datei vorliegt. Bei anderen IEC 61850-Teilnehmern, zum Beispiel dem Zeit-Server, werden diese ICD-Dateien in das Projekt importiert. Bei SIPROTEC 4 Geräten werden sie dagegen erzeugt, sobald Sie das Gerät zur Bearbeitung öffnen. Da wir aber davon ausgehen, dass Sie, wie in Kapitel 7 beschrieben, Ihre SIPROTEC 4 Geräte parametriert haben, haben Sie damit diese Voraussetzung bereits erfüllt.

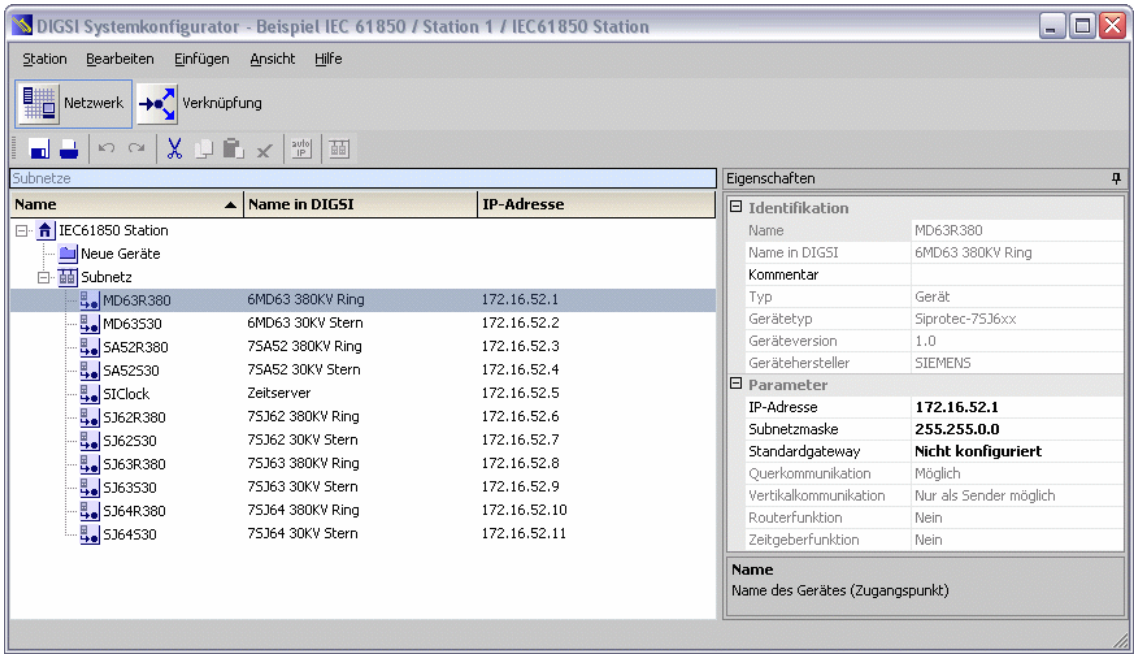
Wichtig ist auch, dass die ICD-Datei aktuell ist. Ändern Sie beispielsweise im DIGSI Manager den IED-Namen, müssen Sie durch erneutes Öffnen des Gerätes mit der DIGSI Gerätebearbeitung die ICD-Datei aktualisieren. Sie müssen außerdem darauf achten, dass keines der teilnehmenden Geräte bearbeitet wird, wenn Sie die Station öffnen wollen. Auch dann schiebt Ihnen der DIGSI Manager gnadenlos einen Riegel vor.

Sind alle Voraussetzungen erfüllt, dann legen Sie los - mit einem Doppelklick auf das Stationssymbol. Nach einer kurzen Verweildauer, in der Sie in sich ruhen können, präsentiert sich Ihnen der DIGSI Systemkonfigurator in modernem Outfit. Im Bereich der Menüleiste fallen Ihnen sofort zwei reichlich dimensionierte Schaltflächen auf. Mit diesen wechseln Sie schnell per Mausklick zwischen den Arbeits- und Aufgabenbereichen **Netzwerk** und **Verknüpfung**.

Arbeitsteilung

Im Arbeitsbereich **Netzwerk** strukturieren Sie bei Bedarf das Kommunikationsnetz der IEC 61850-Station, indem Sie Subnetze hinzufügen oder löschen. Diesen Subnetzen ordnen Sie Teilnehmer zu, die Sie vorher im DIGSI Manager für die Station ausgewählt haben. Sie legen die Adressierung sowie weitere Werte relevanter Eigenschaften der Teilnehmer fest.

Im Arbeitsbereich **Verknüpfung** definieren Sie, welche Teilnehmer welche Daten untereinander austauschen. Dazu verknüpfen Sie Datenobjekte einzelner Teilnehmer. Das heißt, Sie verknüpfen Informationen zwischen einer Quelle und einem Ziel. So genannte Anwendungen helfen dabei, Verknüpfungen zu strukturieren. Eine Anwendung ist eine Gruppe von Verknüpfungen zu einem bestimmten Anwendungszweck, zum Beispiel für eine Verriegelung oder eine Messwertaufgabe. Ein schönes und leicht verständliches Beispiel dafür finden Sie in unserem Handbuch **Ethernet und IEC 61850 - Start Up**. Deshalb wollen wir uns an dieser Stelle nicht weiter damit auseinandersetzen. Vielmehr müssen wir uns um die speziellen Einstellungen für das Netzwerk kümmern.

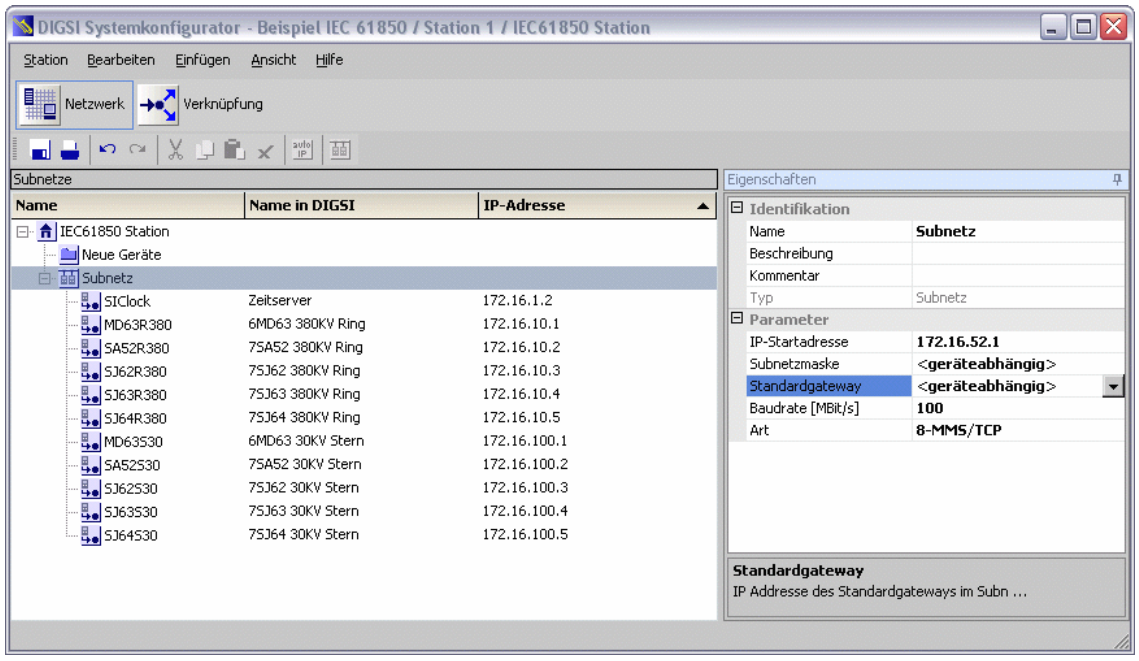


Frage der Perspektive: Das aktuelle Netzwerk aus der Sicht des DIGSI Systemkonfigurators

Zurück zum Arbeitsbereich **Netzwerk.** Dieser zeigt Ihnen im linken Bereich die aktuelle Netzwerkstruktur. Diese besteht in unserem Fall aus nur einem Subnetz. Wenn Sie dieses z.B. per Mausklick öffnen, erhalten Sie alle wichtigen Basisinformationen direkt auf einen Blick. In der Spalte **Name** sehen Sie die IED-Namen des Zeit-Servers sowie der 10 Schutzgeräte, die Sie oder der DIGSI Manager im DIGSI Projekt vergeben haben. Rechts daneben finden Sie die Namen der Geräte, so wie diese auch im Projektfenster des DIGSI Managers angezeigt werden. Interessieren Sie sich für Details, hilft Ihnen das Eigenschaftenfenster auf der rechten Seite weiter. Sie selektieren mit der Maus ein bestimmtes Element innerhalb der Netzwerkstruktur und das Eigenschaftenfenster liefert sofort die passenden Informationen dazu. Markieren Sie doch einmal im Fenster **Subnetze** einen Teilnehmer, beispielsweise **MD63R380**. Das Eigenschaftenfenster zeigt Ihnen nun im Abschnitt **Identifikation** unter anderem den Typ des Gerätes an oder auch den Hersteller.

Ordnung muss sein

Ein Stückchen tiefer finden Sie eine Reihe von Parametern und deren Werte. Ganz wichtig ist die IP-Adresse, denn diese schafft Ordnung im Netzwerk. Wir können es nicht oft genug betonen: Ungültige oder doppelt vergebene IP-Adressen sind der Anfang vom Ende einer funktionierenden Kommunikation. Der DIGSI Systemkonfigurator schlägt Ihnen deshalb vorsichtshalber beim erstmaligen Öffnen einer Station für jeden Teilnehmer eine korrekte und eindeutige IP-Adresse vor. Es handelt sich dabei zwar um Adressen aus einem privaten Klasse-C-Netz, aber so ganz wollen diese noch nicht zu unserem eigenen Adressenkonzept aus Kapitel 5 passen. Deshalb müssen wir ein wenig nachbessern. Das geht eigentlich ganz einfach: Sie markieren den Namen eines Teilnehmers im Fenster **Subnetze** und editieren die IP-Adresse im Fenster **Eigenschaften**. So arbeiten Sie einen Namen nach dem anderen ab. Nach den IP-Adressen sortiert sollte das Ergebnis dann so aussehen:



Neue Anschriften: Die Teilnehmer mit den IP-Adressen entsprechend unseres Konzepts.

Alles paletti

Nun ist eigentlich fast alles gesagt und getan, zumindest, was für unsere Aufgabenstellung nötig ist. Deshalb schließen Sie jetzt den DIGSI Systemkonfigurator. Ihre Eingaben werden automatisch auf Plausibilität geprüft und anschließend gespeichert. Da Sie Veränderungen vorgenommen haben, erhalten Sie noch einen Hinweis darauf, dass die Parametersätze der einzelnen Stationsteilnehmer aktualisiert werden müssen. Das Aktualisieren der Parametersätze funktioniert übrigens für alle Geräte gemeinsam. Öffnen Sie dazu im DIGSI Manager den Eigenschaftendialog der IEC 61850-Station und wählen Sie die Registerkarte **Aktualisierung**. Klicken Sie einfach auf **Alle Parametersätze aktualisieren** und die Dinge nehmen Ihren Lauf.

Zugereiste

Noch einige Worte zur Vergabe der IP-Adressen: Bitte beachten Sie, dass im DIGSI Systemkonfigurator nur IEC 61850-Teilnehmer eines DIGSI-Projekts angezeigt und bei der Adressvergabe berücksichtigt werden. Andere Teilnehmer des Netzwerks wie beispielsweise Switches, Serial Hubs oder PCs benötigen natürlich ebenfalls gültige IP-Adressen. Diese werden jedoch nicht im DIGSI Systemkonfigurator verwaltet. Sie müssen daher unbedingt darauf achten, dass IP-Adressen nicht doppelt vergeben werden. Ein konsequentes Planen und Dokumentieren der Netzwerkstruktur ist das A und O, um solche Fehler zu vermeiden.

Einstellungen ins Schutzgerät übertragen 9

Das Schöne an DIGSI 4 ist ja, dass Sie die gesamte Parametrierung durchführen können, ohne ein SIPROTEC-Gerät bei sich zu haben. Sind alle Vorbereitungen abgeschlossen, und an diesem Punkt sind wir nun fast angelangt, übertragen Sie das Resultat Ihrer Arbeit per einfacher Kommunikationsverbindung in das Gerät. Dabei gehen wir davon aus, dass Sie ein aktuelles SIPROTEC 4 Gerät mit der Option IEC 61850 besitzen, in das das EN100-Modul bereits im Gerät eingebaut und sozusagen gebrauchsfertig installiert ist. Ist das nicht der Fall, müssen Sie Ihr SIPROTEC 4 Gerät noch in einigen anderen Punkten auf seine neue Aufgabe als Netzwerker vorbereiten. Was für Sie dabei alles zu tun ist, erfahren Sie in Kapitel 13 im Abschnitt **Kommunikationsmodul im SIPROTEC 4 Gerät tauschen**.

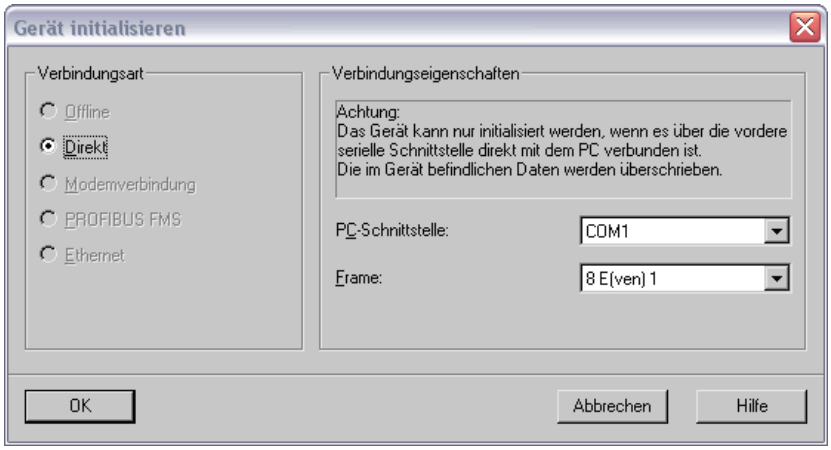
Hinweis am Rand:
Durch das Initialisieren werden im Gerät die Netzwerkparameter auf gültige Werte gesetzt, sodass das Gerät überhaupt über das Netzwerk angesprochen werden kann. Ist dies einmal geschehen, kann das Gerät im Weiteren deutlich schneller über Ethernet parametriert werden. Dazu wählen Sie **Ethernet** als Verbindunsart.

Die bisher projektierten Einstellungen müssen Sie nun nacheinander in die einzelnen Geräte übertragen. Da wir diese in unserem Beispiel neu im Projekt angelegt hatten, müssen wir sie zunächst initialisieren. Das Initialisieren verleiht Ihrem SIPROTEC 4 Gerät eine eigene Identität. Nicht nur, dass dabei der komplette Parametersatz in das Gerät übertragen wird, während der Initialisierung wird das Gerät vor allem eindeutig adressiert.

Wie Sie ein Gerät initialisieren, haben wir ausführlich im Handbuch **DIGSI 4 Start Up** beschrieben. Für alle, die dieses noch nicht kennen, hier noch eine einfache Merkregel: Sobald Sie mit einem in der Projektstruktur neu angelegten *virtuellen* Gerät eine Verbindung zu einem *realen* Gerät aufbauen wollen, müssen Sie das *reale* Gerät einmalig mit den Daten des *virtuellen* Gerätes *initialisieren*. Danach können Sie beliebig oft zwischen PC und Gerät eine Verbindung auf- und abbauen.

Initialzündung

Verbinden Sie jetzt ein beliebiges Gerät mit dem PC. Dazu nehmen Sie das DIGSI 4-Kabel und stöpseln es auf eine freie serielle Schnittstelle (alias COM-Port) des PCs. Das andere Ende stecken Sie auf die vordere Schnittstelle am SIPROTEC 4 Gerät. Im Projekt markieren Sie das Symbol für das betreffende Gerät und wählen dann in der Menüleiste den Befehl **Gerät** → **Initialisieren**.



Mit dem Dialog **Gerät initialisieren** prüfen Sie noch einmal die aktuellen Kommunikationseinstellungen

Der Dialog **Gerät initialisieren** zeigt Ihnen die aktuellen Einstellungen für die PC-Schnittstelle (entsprechend des von Ihnen gewählten COM-Ports einstellen) und den Frame (bitte auf **8E(ven)1** belassen). Schließen Sie diesen Dialog mit Klick auf **OK**. Sie erhalten einen Hinweis, dass vorhandene Daten im SIPROTEC 4 Gerät durch das Initialisieren gelöscht werden. Sind diese Werte für Sie nicht relevant oder wurden diese bereits in Dateien gesichert, klicken Sie hier auf **Ja**.

Die passenden Worte

Nach einigen Zwischenmeldungen werden Sie aufgefordert, ein Passwort einzugeben. Sofern Sie keine Änderungen an den Passwörtern vorgenommen haben, tippen Sie sechsmal die Null ein. Klicken Sie anschließend auf **OK**. Den Übertragungsvorgang können Sie übrigens nicht nur am Bildschirm, sondern auch am Display des SIPROTEC 4 Gerätes verfolgen. Ist die Initialisierung beendet, wird im Display des Gerätes wieder das Grundbild angezeigt. Die Verbindung zwischen PC und Gerät war allerdings nur temporärer Natur und wird nach Abschluss der Initialisierung wieder abgebaut.

Switch und Zeit-Server parametrieren 10

Wenn es um das Einstellen von Switches und Zeit-Server geht, müssen wir Sie im Großen und Ganzen auf die jeweiligen Handbücher zu diesen Komponenten verweisen. Zum einen sind viele Einstellungen und auch der Weg zu diesen sehr typspezifisch und Sie sind schließlich nicht gebunden an die Empfehlungen, die wir in diesem Buch geben. Zum anderen sind eine Reihe von Parametern völlig unabhängig von der Art der Netzwerktopologie; deren Einstellung wird eher bestimmt durch Ihre persönliche Anlagenphilosophie.

Das betrifft insbesondere den Zeit-Server. Für die korrekte Funktionsweise unserer Beispielkonfiguration ist zunächst vor allem dessen richtige IP-Adresse wichtig, genau wie bei allen anderen Teilnehmern auch. Alle weiteren Möglichkeiten für hilfreiche oder eher exotische Einstellungen, die Ihr Zeit-Server zulässt, studieren Sie bitte in dessen Bedienungsanleitung. Der Rest dieses Kapitels ist denn also dem Parametrieren der verwendeten Switches gewidmet - im Speziellen solchen der Firma RuggedCom.

Egal ob Sie nun irgendwelche Einstellungen ändern oder neue Firmware in den Switch laden möchten, Sie benötigen dazu eine Kommunikationsverbindung zwischen Switch und PC. Hier bietet sich ganz nahe liegend eine Ethernetverbindung an. Alternativ bedienen Sie sich einer eher klassischen, aber immer noch brauchbaren Methode: Die serielle Hyperterminalverbindung. Wir werden Ihnen beide Kommunikationsverfahren beschreiben, allerdings mit Schwerpunkt auf Ethernet.

Übrigens: Wir gehen davon aus, dass Ihre Switches auf dem neuesten Stand der Firmware sind. Sollte dagegen ein kleines Firmware-Lifting nicht schaden können, dann lesen Sie in Kapitel 13 wie es geht.

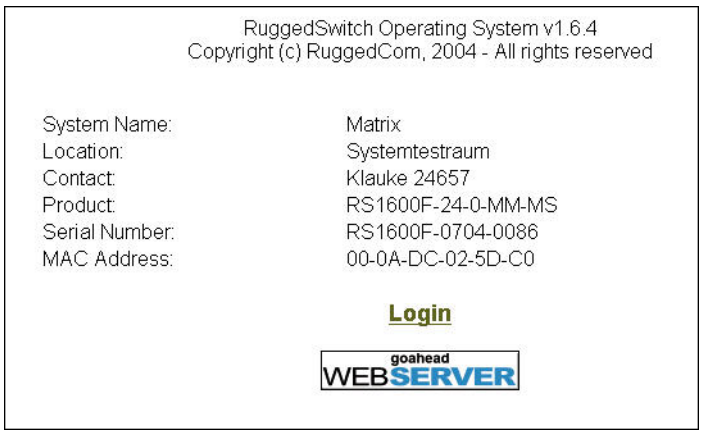
Switch über Ethernet ansprechen

Über eine Ethernetverbindung können Sie von jeder Stelle des Netzwerkes aus alle Parameter eines Switches einstellen - sofern dieser seine korrekte IP-Adresse im Netz besitzt. Diese müssen Sie ihm jedoch erst beibringen. Jeder Switch hat dazu eine voreingestellte IP-Adresse. Diese und eine direkte Ethernetverbindung zwischen Switch und PC ermöglichen Ihnen eine erste Kontaktaufnahme. Während dieser stellen Sie dann die von Ihnen vorgesehene IP-Adresse ein. Alles Weitere können Sie je nach Belieben gleich oder erst nach der Inbetriebnahme - und dann über das Netzwerk - erledigen.

Erst anbandeln ...

Verbinden Sie als Erstes die Netzwerkkarte des PCs mit dem Switch. Achten Sie darauf, dass das verwendete Kabel 1:1 verdrahtet ist. Cross-over-Kabel, wie sie beim Verbinden zweier PC zum Einsatz kommen, sind nicht geeignet. Ansonsten benötigen Sie für das erste Zwiegespräch nur noch einen Web-Browser und schon kann es los gehen.

In das Adressfeld des Browsers geben Sie die im Switch voreingestellte IP-Adresse in der Form http://192.168.0.101 ein und bestätigen diese mit der Enter-Taste. Der Switch meldet sich daraufhin im Browser mit einer ersten Übersicht zum Stand der Dinge.



Hier kommt der Switch

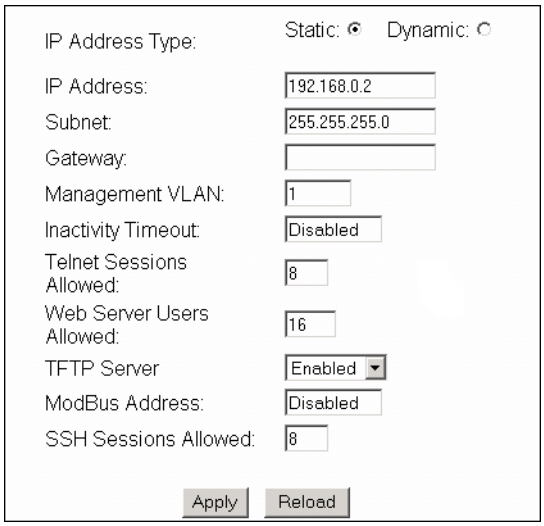
... dann anmelden

Richtig loslegen können Sie aber erst nach einer erfolgreichen Anmeldung. Dazu müssen Sie den korrekten Benutzernamen und das aktuelle Passwort eingeben. Der Eingabedialog für die Benutzerdaten erscheint nach einem Klick auf **Login**. Beim 1. Kontakt lautet beides **admin**. Es ist aber sicherlich ratsam, später vor allem das Passwort in eine etwas weniger leicht durchschaubare Variante zu ändern. Jetzt noch ein Klick auf **OK** und der Switch gibt den Weg frei zum Hauptmenü.

Das Hauptmenü ist der Einstieg in eine Vielzahl von Konfigurationsmöglichkeiten.

Netzparameter für Switch einstellen

Bevor Sie einen Switch in den Netzwerkbetrieb integrieren, müssen Sie für diesen in jedem Fall einige Netzparameter einstellen, an erster Stelle die IP-Adresse. Sie finden diese und auch weitere verwandte Parameter im Bereich **Administration** und dort wiederum unter dem Menüeintrag **Configure IP-Services**.



Die Netzwerkparameter finden Sie im Menü IP-Services.

Die IP-Adresse für den Switch tragen wir entsprechend unseres Topologieplanes ein, den wir uns vorher erstellt haben. In jedem Fall ist die Adresse vom Typ **Static**, da wir keinen DHCP-Server verwenden. Die Netzmaske für unser Klasse-B-Netz ist 255.255.0.0.

Der Parameter **SNMP Get Community** sollte auf **public** stehen. Damit ermöglichen Sie die Überwachung des Switches per SNMP. Das kann zum einen durch spezielle Softwaretools erfolgen, zum anderen sind auch beispielsweise in SICAM PAS Funktionen implementiert, die eine Diagnose per SNMP möglich machen.

Nach einem Klick auf **Apply** übernimmt der Switch die neuen Einstellungen. Danach können Sie guten Gewissens auf **Back** klicken, um sich in der Menüstruktur wieder nach oben zu hangeln.

Portparameter einstellen

Sie können jeden einzelnen Port eines Switches individuell konfigurieren. Allerdings hat das, zumindest in unserem Fall, wenig Sinn. Vielmehr stellen wir die Parameter für alle Ports identisch ein. Und das geht so: Im Hauptmenü klicken Sie zuerst auf **Ethernet Ports**. Daraufhin bekommen Sie ein Untermenü zu Gesicht, das unterschiedliche portspezifische Einstellungen und Informationen zusammenfasst.

Die Portparameter sind über ein Untermenü zugänglich.

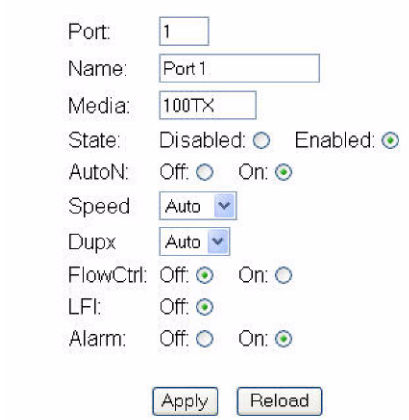
Port für Port

Uns interessieren dabei in erster Linie die Portparameter sowie die Portsicherheit. Klicken Sie daher bitte im Untermenü auf **Configure Port Parameters**. Der Browser zeigt Ihnen nun eine Übersicht der aktuellen Einstellungen für alle 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

Alles auf einen Blick: Die Tabelle zeigt die aktuellen Einstellungen der Port Parameter.

Wie Sie sehen können, sind die Ports fortlaufend nummeriert. Mit einem Klick auf die Nummer eines Ports öffnen Sie den Einstelldialog für dessen Parameter. Die Abbildung zeigt die Einstellungen, so wie diese sein sollten. Was wir Ihnen hier nun beispielhaft für einen Port erläutern, führen Sie bitte für alle Ports durch.

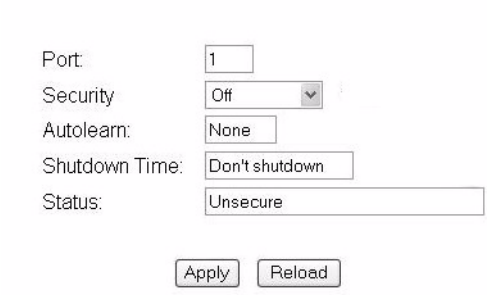


Die Port Parameter sind Ihnen bereits größtenteils bekannt.

Wichtig ist natürlich, dass ein Port, den Sie nutzen wollen, überhaupt aktiviert ist, sein Status also den Wert **Enabled** besitzt. Die Übertragung sollte stets im Vollduplex-Modus erfolgen. Dazu müssen Sie für den Parameter **Media** die Einstellung **100TX** eintragen. Und zu guter Letzt muss der Alarm unbedingt aktiviert sein, also **Alarm** auf **Enabled**! Ist das alles erledigt, weisen Sie dem Switch mit einem Klick auf **Apply** die neuen Einstellungen zu. Danach heißt es für Sie, einmal auf **Back** klikken und mit dem nächsten Port fortfahren.

Ohne Sicherheiten

Sind Sie mit allen benötigten Ports durch, gelangen Sie mit einem weiteren Klick auf **Back** von der Übersicht zurück zum Untermenü. Dort klikken Sie auf Configure Port Security. Wie bereits bei den Portparametern zeigt Ihnen der Browser auch hier zunächst eine Übersicht der aktuellen Einstellungen, die Ihnen wieder als Möglichkeit dient, die Einstelldialoge für die einzelnen Ports zu öffnen. Das Bedienverfahren ist also identisch, der Dialog hingegen sieht so aus:



Ungewohnt: Nur mit deaktivierter Port Security läuft es problemlos.

Sie müssen lediglich den Parameter **Security** auf **Off** stellen, das aber verbindlich und aus gutem Grund: Eine aktivierte Portsecurity führt unweigerlich zu Konflikten mit RSTP! Sobald Sie die Portsecurity für alle Ports deaktiviert haben, kehren Sie zum Hauptmenü zurück.

RSTP-Eigenschaften einstellen

Auch bei den RSTP-Eigenschaften gibt es solche, die Sie portbezogen unterschiedlich einstellen können und in den meisten Fällen auch müssen. Aber wir betrachten den Switch natürlich auch als Ganzes, nämlich in seiner Funktion als RSTP-Bridge, für die es einige portübergreifende Einstellungen gibt wie beispielsweise die RSTP-Priorität.

Ein Klick auf den Eintrag **Spanning Tree** gibt den Weg frei zu beiden Kategorien von Parametern.

Noch ein Menü: Die RSTP-Parameter.

Beginnen wir mit den Parametern, die sich auf den Switch als Ganzes beziehen. Ein entsprechender Einstelldialog zeigt sich, sobald Sie im Untermenü auf **Configure Bridge RSTP-Parameters** klicken.

Achten Sie auf die korrekten Einstellungen für die Bridge-Parameter.

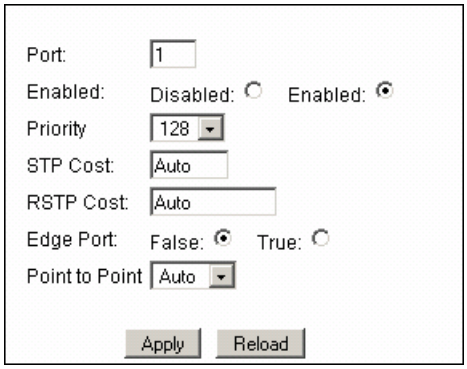
Die Abbildung zeigt Ihnen Einstellungen, die für einen einwandfreien Betrieb wichtig sind. Übernehmen Sie diese daher für alle Parameter - mit Ausnahme der Bridge Priority. Diese muss natürlich passend zur Topologie für einige Switches unterschiedlich eingestellt werden. Für unser Beispiel würden Sie also die Werte übernehmen, so wie wir diese in Kapitel 5 festgelegt haben.

Alle Parameter richtig eingestellt? Dann klicken Sie wieder auf **Apply** und wechseln zurück zum Menü. Hier wählen Sie dann **Configure Port RSTP-Parameters**. Da es nun wieder um portspezifische Einstellungen geht, erhalten Sie zunächst eine Übersicht der aktuellen Einstellungen.

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

Die RSTP-Porteinstellungen präsentieren sich wieder als Tabellenwerk.

Wie gewohnt klicken Sie in auf die Nummer des Ports, dessen Einstellungen Sie bearbeiten wollen und erhalten dann dazu einen Dialog.



Jetzt noch schnell die RSTP-Parameter der einzelnen Ports einstellen.

Edge Port oder nicht Edge Port

Übernehmen Sie die Werte so, wie Sie diese in der Abbildung sehen. Einzige Ausnahme ist der Parameter **Edge Port**. Diesen müssen Sie für jeden Port individuell betrachten. Hier ein paar Regeln:

Sie wählen die Einstellung **Edge Port = True**, wenn ...

- ... ein SIPROTEC-Gerät über ein elektrisches EN100-Modul an den Port angeschlossen ist.
- ... ein SIPROTEC-Gerät über ein optisches EN100-Modul an den Port angeschlossen ist, welches im Linienbetrieb arbeitet.

Sie wählen die Einstellung **Edge Port = False**, wenn ...

- ... ein SIPROTEC-Gerät über ein optisches EN100-Modul, das im Switchmodus betrieben wird, an den Port angeschlossen ist.
- ... der Port die Verbindung zu einem Ring herstellt.

- ... der Port mit dem eines anderen Switches verbunden ist.

Vereinfacht ausgedrückt stufen Sie einen Port als Edge Port ein, wenn alles, was daran angeschlossen ist, keinen Ring bildet.

Haben Sie alle Ports konfiguriert, ist auch Ihre Arbeit an dieser Stelle getan. Übrigens können Sie die Einstellungen auch in Form einer Konfigurationsdatei auslesen, mit einem Editor bearbeiten und anschließend wieder in den Switch laden. Wie das geht, verraten wir Ihnen am Schluss dieses Buchs in Kapitel 13.

Switch über Hyperterminal ansprechen

Falls Sie sich vor der ersten Inbetriebnahme des Netzwerks lieber einer klassischen, aber dennoch brauchbaren Methode bedienen wollen, dann verbinden die serielle RS232-Schnittstelle des Switches mit der des PCs und bauen eine Hyperterminalverbindung zwischen beiden Komponenten auf. Dazu benötigen Sie ein so genanntes 1:1-Kabel als Verbindungsleitung. Ein solches ist übrigens jedem DIGSI 4 für die Kommunikation zwischen PC und SIPROTEC 4 Gerät beigepackt.

Fensteröffner

Direkt über das Startmenü mit **Programme** → **Zubehör** → **Kommunikation** → **Hyperterminal** → **<Verbindungsname>** öffnen Sie das Hyperterminalfenster. <Verbindungsname> steht dabei als Platzhalter für die individuelle Hyperterminalverbindung zwischen PC und Switch, die Sie selbst erst konfigurieren müssen. Eine Beschreibung, wie Sie dabei vorgehen, haben wir zusammen mit weiteren ergänzenden Themen in das Kapitel 13 ausgelagert.

Jetzt müssen Sie die Verbindung noch aktivieren. Dazu wählen Sie im Menü **Anrufen** den Befehl **Anrufen**. Das ist kein Schreibfehler, sondern leider wirklich so. Menschen, die sich Zeugnissen solcher sprachlichen Gewandtheit lieber nicht aussetzen möchten, greifen zum Tastaturkurzbefehl **Strg S**, die dasselbe bewirkt: Die Verbindung zwischen PC und Switch wird hergestellt. Der Switch erwartet nun eine förmliche Anmeldung Ihrerseits, also ein Passwort.

Beim ersten Kontakt heißt dieses auch hier schlicht und einfach **admin**. Sobald Sie das Passwort eingegeben und mit einen Druck auf **Enter** an den Switch abgeschickt haben, zeigt das Terminalfenster ein Auswahlmenü an und es kann losgehen. Das Auswahlmenü enthält natürlich die gleichen Einträge wie dies bei der Kommunikation über Ethernet mit einem Web-Browser der Fall ist. Und auch an den notwendigen Einstellungen ändert sich nichts.

Anschließen und einschalten

11

Darüber, wie Sie die Berge aus Blech und Kunststoff, gefüllt mit tausenden Elektronikteilen, miteinander verbinden, könnten wir mehrere Bücher schreiben - und beschränken uns genau deswegen auf wenige Absätze. Zu vielseitig sind die Möglichkeiten Ihrer speziellen Anlagenkonfiguration, der Räumlichkeiten, in denen die Hardware untergebracht wird, und so weiter ... Fühlen Sie sich unsicher, vertrauen Sie gegebenenfalls einem erfahrenen Netzwerker. Damit Sie in jedem Fall mitreden können, geben wir Ihnen noch einige Tipps mit auf den Weg.

Wenn Sie Geräte über einen fliegenden Testaufbau hinaus als dauerhafte Einrichtung miteinander verkabeln wollen, sollten Sie unbedingt die EN 50173 berücksichtigen. Diese Norm definiert die strukturierte Netzwerkverkabelung bis hin zum korrekten Bündeln von mehreren Leitungen mit Kabelbindern. Falls Sie mehr zur EN 50173 wissen möchten, spuckt Ihnen jede Internetsuchmaschine eine Vielzahl von Aufsätzen zu dieser Thematik aus. Ein Teilbereich daraus ist die Wahl der richtigen Kabel. Für unsere Beispielkonfiguration aus Kapitel 5 benötigen wir solche in elektrischer und auch in optischer Ausführung.

Unter Strom

Beim Kabelgemischtwarenhändler finden Sie in der Abteilung für elektrische Netzwerkkabel zwei grundsätzlich unterschiedliche Sorten im Angebot: Patch-Leitung und Verlegekabel. Wie viel Sie von welcher Sorte kaufen, sollte nicht von einem in Aussicht gestellten Mengenrabatt bestimmt werden, sondern einzig allein vom Einsatzzweck des Kabels.

Patch-Leitungen sind biegsam, denn sie sind vor allem für das Verbinden von Geräten konzipiert, die nahe beieinander aufgestellt sind. Haben Sie also beispielsweise die Schutzgeräte eines Feldes und den zugehörigen Switch in ein gemeinsames Rack montiert, sind Patch-Leitungen das prädestinierte Verbindungsmedium. Ihre mechanische Flexibilität erhalten die Patches durch dünnere Drähte, die sich als Adern durch den Kunststoffmantel schlängeln. Meistens wird dabei sogar Litze verwendet. Und das führt leider zu schlechteren elektrischen Werten. Patch-Leitungen sollte man deshalb nicht für längere Strecken verwenden - fünf Meter sollte die Obergrenze sein.

Muss es mehr sein, greifen Sie besser zu Verlegekabel. Wählen Sie Shielded Twisted Pair, kurz STP. Bei diesem sind die Datenadern von einem Schirm umgeben, der äußere Störeinflüsse weitestgehend eliminiert. Mit solchen STP-Kabeln überbrücken Sie sicher bis zu zwanzig Meter.

Qualitätsware

Bei der Auswahl sowohl von Patch-Leitung als auch Verlegekabel sollten Sie auf die elektrische Qualität achten. Diese ist durch die Einteilung in verschiedene Kategorien definiert. Aktueller Stand der Dinge und für die meisten Anwendungen ausreichend ist CAT5. Wenn Sie bereit sind, ein paar Euro mehr springen zu lassen, dann entscheiden Sie sich für CAT5e. Mit dieser Kabelqualität werden auch in einem Gigabit-Ethernet-Netzwerk Daten auf Strecken bis zu 100 Metern sicher transportiert. Dagegen sind CAT6- oder derzeit auf den Markt kommende CAT7-Kabel, die sogar 10-Gigabit-Ethernet elektrisch übertragen können, für unsere Anwendungszwecke überdimensioniert.

Es werde Licht

Für größere Distanzen und Datenmengen stehen überdies Lichtwellenleiter höher im Kurs. Bis zu einer Verbindungslänge von 2 km sind Multimodefaserkabel geeignet. Entfernungen, die darüber hinaus gehen, müssen mit Singlemodefaserkabel überbrückt werden. Damit schaffen Sie dann aber auch bis zu 100 km, ohne das Signal auffrischen zu müssen.

Wir bleiben allerdings ganz bescheiden unterhalb der 2-Km-Marke und verwenden MMF-Kabel, das Licht mit einer Wellenlänge bis zu 1380 nm übertragen kann. Wichtig ist eine weitere Kenngröße, nämlich die Angabe von Kern- und äußerem Durchmesser der Faser. 50/125 µm oder 65,5/125 µm sind für unsere Zwecke geeignete Ausführungen.

Ozapft iis

Passend zum Kabel benötigen Sie noch die richtigen Stecker. Unsere Empfehlung: Kaufen Sie Kabel soweit möglich in konfektioniertem Zustand. Bei elektrischen Patch-Leitungen selbst Hand anzulegen, lohnt angesichts der Preise für fertig konfektionierte Patches ohnehin nicht. Und LWL-Kabel in Eigenregie mit Steckern zu versehen, führt meistens nicht zum gewünschten Ergebnis. Allein beim als Meterware gekauften STP-Verlegekabel erscheint es sinnvoll, in Heimarbeit ans Werk zugehen. Wer jedoch nicht über das nötige Werkzeug und die Erfahrung verfügt, sollte besser den Fachmann ran lassen.

Was die Stecker selbst betrifft: Für elektrische Verbindungen kommt nur noch RJ45 in Frage. Beim Licht gibt es allerdings zwei getrennte Lager. Anschluss zu EN100-Modulen sowie zu OSM-Switches finden Sie mit Duplex-LC-Steckern. Switches von RuggedCom stehen dagegen mehr auf MTRJ-Stecker. Sie benötigen daher gemischt konfektionierte Kabel, die Sie übrigens auch direkt bei Siemens erwerben können.

Drum prüfe, wer sich ewig bindet

Damit die einwandfreie Kommunikation nicht bereits an ein paar defekten Kabeln scheitert, sollte man sich die Zeit nehmen, diese vor dem Einsatz zu prüfen. Besonders sinnvoll ist das bei Kabeln, die nicht fabrikneu sind oder bei selbst konfektionierten Leitungen. Einen Drahtbruch oder simple Verdrahtungsfehler erkennen bereits einfache Prüfgeräte, die es, im Vergleich zu einem SIPROTEC 4 Gerät für sehr, sehr wenig Geld zu kaufen gibt. Aber es muss nicht unbedingt eine unterbrochene Verbindung sein, die zu einer schlechten Datenübertragung führt.

Zu lang gewählte Kabel, unsauber verlegt oder sonstigen Störeinflüssen ausgesetzt, können ebenfalls die Ursache sein. Besonders bei fest verlegten Leitungen empfiehlt sich ein Check durch den Profi. Dieser nimmt Frequenzgang, Dämpfung und Übersprechen unter die Lupe und sorgt im Notfall für Abhilfe.

Pläne und Listen

Unser Tipp: Ein topologischer Verdrahtungsplan und korrespondierende Bezeichnungen auf Kabeln (mit Filzschreiber) und an den Ports (mit Aufklebern) erleichtert eine spätere Fehlersuche erheblich. Zusätzlich schafft eine Liste mit einigen wesentlichen Kenndaten der Teilnehmer Klarheit, auch für Kollegen und vor allem auch noch nach längerer Zeit. Gerätetyp, MLFB-Nummer, Seriennummer, Firmwareversion von Gerät und Modul, IP-Adresse, Netzmaske, Adresse des Standardgateways, MAC-Adresse und IED-Name unter IEC 61850 sind die Mindestdaten für SIPROTEC 4 Geräte, welche die Liste dokumentieren sollte.

Hinweis am Rande
Die MAC-Adressen können Sie bei SIPROTEC 4 Geräten übrigens direkt am Gerätedisplay ablesen (Tastenfolge: Menü 5 5 Enter).

Für Geräte wie Switches und Zeit-Server sollten Sie, soweit möglich, analoge Kennwerte in das Verzeichnis aufnehmen. Ist die Liste vollständig, stellen Sie sicher, dass keine IP-Adresse doppelt vorkommt. Bei MAC-Adressen sollte das aufgrund ihrer eindeutigen Vergabe grundsätzlich ausgeschlossen sein.

Raucher oder Nichtraucher

Sind alle Vorbereitungen abgeschlossen, können Sie die Anlage stufenweise in Betrieb nehmen. Zuvor sollten Sie den Ring temporär an einer Stelle physisch auftrennen. Diese Maßnahme hilft Ihnen, eine stabile Ringstruktur zu erreichen. Schalten Sie als Erstes den Zeit-Server ein und danach die Switches. Nachdem Sie den letzten Switch aktiviert haben, warten Sie noch etwa 20 Sekunden und beginnen dann, die Geräte zuzuschalten. Wir empfehlen Ihnen, die Geräte nacheinander entsprechend ihrer Anordnung im Netzwerk an Spannung zu legen. Geben Sie jedem Gerät die Zeit, vollständig hochzulaufen, bevor Sie das nächste Gerät einschalten. Sind alle Geräte in Betrieb, schließen Sie den Ring.

Haben Sie bislang keinerlei unangenehme Schmorgerüche registriert, ist das bereits ein positives Zeichen und Sie dürfen sich zunächst einmal freuen. Was Sie danach noch tun sollten, erfahren Sie im nächsten Kapitel.

Funktionsfähigkeit testen

12

In diesem Kapitel wollen wir Ihnen noch einige Informationen darüber geben, wie Sie Ihr Netzwerk und die integrierten Komponenten auf Funktionsfähigkeit testen. Dabei ist es nützlich, erst einmal so zu tun, als wäre alles in Ordnung, denn Fehler treten sowieso nur bei den anderen auf. Wir werden also zunächst versuchen, mit jedem einzelnen SIPROTEC 4 Gerät im Netz Kontakt aufzunehmen. Sollte es unserer ersten Annahme entgegen doch an der einen oder anderen Stelle hapern, sehen wir uns die entsprechende Komponente eben ein wenig genauer an.

Die Kommunikationsfähigkeit testen

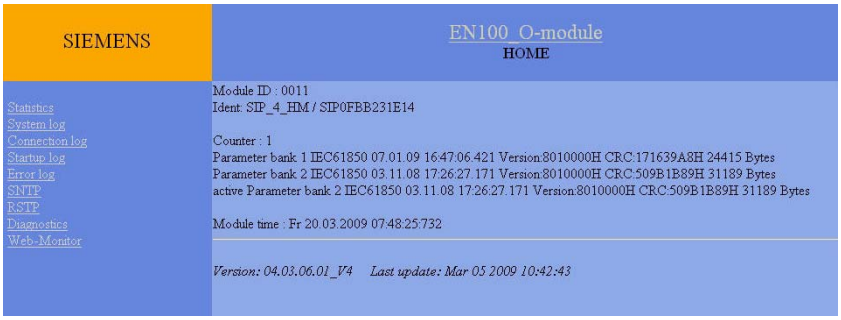
Nachdem Sie alle Parameter eingestellt und die Werte in die Geräte übertragen haben, müssten diese über ihre IP-Adresse im Netz erreichbar sein. Genau das wollen wir nun überprüfen.

Jedes EN100-Modul leistet sich den Luxus einer eigenen Homepage. Diese dient vor allem der Diagnose während der Inbetriebsetzung oder in Fällen, wenn es während des Betriebs nicht so klappt, wie es eigentlich klappen sollte. Wir verwenden diese Homepage nun als erste Möglichkeit, um festzustellen, ob wir überhaupt Kontakt mit einem Gerät aufnehmen können.

Ab nach Hause

Um die Modulhomepage aufzurufen, klinken Sie sich mit einem PC an einen beliebigen Switch des Netzwerks. Dieser muss natürlich für das Netzwerk konfiguriert sein. Deshalb bietet es sich an, dass Sie für diese Aufgabe Ihren DIGSI 4 PC verwenden, der sowieso bereits Bestandteil des Netzes ist. DIGSI 4 selbst benötigen Sie jedoch nicht für diese Aktion. Stattdessen öffnen Sie Ihren bevorzugten Web-Browser. In die Adressleiste geben Sie die IP-Adresse des Zielgerätes mit dem Zusatz **/home** ein. Ihre Eingabe hat also beispielsweise die Form **http://172.16.10.1/home**. Mit der Eingabetaste schicken Sie die Anforderung auf den Weg.

Der Browser sollte nun die Heimatseite des Moduls anzeigen. Ist dem so, können Sie auf einen Schlag mehrere Erfolge verbuchen: Modul und Gerät sind erreichbar, die Verbindungsleitungen vom PC bis hin zum Gerät sind in Ordnung und auch sämtliche zwischengeschaltete Switches scheinen korrekt zu arbeiten. Aber sehen wir uns doch die Modulhomepage etwas genauer an.



Nicht schön, aber klug: Die Homepage des EN100-Moduls liefert viele Informationen.

Grundsätzlich gilt: Abhängig von der Betriebsart des Moduls, also Linie oder Switch, zeigt sich auch die Homepage hinsichtlich ihres Informationsangebots von unterschiedlichen Seiten. In allen Fällen zeigt sie jedoch die Version und das Erzeugungsdatum der Softwareversion, die sich aktuell auf dem Modul befindet. Diese Information kann wichtig sein, wenn Sie mit unserer Hotline korrespondieren.

Das ist natürlich beileibe nicht alles; wirklich tiefgehende Informationen erreichen Sie über verschiedene Links, die sich am linken Rand der Homepage zu einem Menü gruppieren. Mehr dazu im Abschnitt **Noch mehr Details erfahren mit der Modulhomepage**.

Alle machen mit

Natürlich sind nicht nur die EN100-Module in den SIPROTEC 4 Geräten via Browser erreichbar. In der Regel bieten auch Zeitserver und Switches der gehobenen Preisklasse diese Möglichkeit. Bei RuggedCom-Produkten kann beispielsweise ab der Main-Firmwareversion 1.6 mit Hilfe eines Browsers auf den Switch zugegriffen werden. Sie geben dazu nur die IP-Adresse des Switches ein und melden sich anschließend am Switch an.

Kein Anschluss

Es kann durchaus passieren, dass ein Gerät nicht erreichbar ist und seine Modulhomepage daher im Verborgenen bleibt. Das kann verschiedene Ursachen haben:

- Ein SIPROTEC 4 Gerät, das über eine Linienverbindung an einen externen Switch angeschlossen ist, ist ausgeschaltet.
- Ein SIPROTEC 4 Gerät, das in einen optischen Ring integriert ist, ist ausgeschaltet.
- Eine Ringstruktur ist an mehreren Stellen aufgetrennt; damit ist ein Teil der Geräte nicht mehr erreichbar. Die Trennstellen können ausgeschaltete Geräte oder gelöste Verbindungen sein.

Prinzipiell kann auch eine Fehlfunktion des EN100-Moduls vorliegen. Mehr dazu im nächsten Abschnitt.

Funktionsfähigkeit der EN100-Module testen

Gibt es Probleme mit der Erreichbarkeit eines Gerätes, sollte man neben den Verbindungsleitungen auch das jeweils eingebaute Modul unter die Lupe nehmen. Aber auch bei einwandfreiem Betrieb sind einige Tests direkt am Gerät unabwendbar, so zum Beispiel, um die Ringfunktionalität zu prüfen. Bei allen Untersuchungen direkt am Objekt hilft Ihnen die Modulinformationsseite. Damit diese im Display des Gerätes angezeigt wird, drücken Sie am Gerät nacheinander die Tasten **Menü 5 5 1.**

Verbindungs-anzeige

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 *******

Tolle Optik: Informationen für ein optisches EN100-Modul (Abb. vorl.)

Glückliche Besitzer von Geräten mit großem Display sehen die Informationen dieser Modulinformationsseite in voller Pracht, so wie oben gezeigt. Geräte mit kleinem Display stellen nur vier Zeilen gleichzeitig dar. Um die weiteren Zeilen sehen zu können, müssen Sie sich in diesem Fall der vertikalen Navigationstasten bedienen.

Das Bild oben zeigt die Modulinformationsseite für ein EN100-Modul in optischer Ausführung. Da die elektrische Variante des Moduls keine Switch-Funktionalität besitzt, kommt dessen Anzeige mit weniger Zeilen aus. Welche Informationen für beide Varianten gleich sind, welche nur der optischen Variante vorbehalten bleiben und vor allem, wie Sie die Informationen interpretieren, klären wir jetzt.

Wer und wo bin ich?

Die Zeilen 2 bis 5 informieren Sie bei beiden Modulvarianten quasi über die Rahmenbedingungen. Von oben nach unten sind das die MAC-Adresse und die IP-Adresse des Moduls, danach die Netzmaske, dicht gefolgt von der Gatewayadresse. Jetzt lohnt es sich, einen Übersichtsplan zu besitzen, der die einzelnen Geräte in Verbindung mit ihren IP-Adressen zeigt. Damit lässt sich schnell überprüfen, ob die ursprünglich festgelegten Adressen auch die richtigen Besitzer gefunden haben.

007

Die Zeile 6 überspringen wir vorerst und sehen uns zunächst die Informationen in Zeile 7 an. Diese geben Auskunft über den Zustand der Verbindung zum Netzwerk. Die Präsentation dieser Information kann abhängig sein von der Ausführung des EN100-Moduls, nämlich dann, wenn Sie das optische Modul im Switch-Modus betreiben. In diesem Fall liefert Ihnen die Zeile 7 die Information für jede der beiden Ports, ob sie aktiv (up) oder nicht aktiv (down) ist. Die Information **Chan1/2=Up/Up** ist also das Beste, was Ihnen passieren kann, denn beide Ports (oder auch Kanäle = Channels) sind aktiv. Der Ring ist also zumindest an der aktuell überprüften Stelle intakt. Sie sollten nun testen, ob das Modul eine Ringunterbrechung korrekt erkennt. Dazu ziehen Sie als Erstes den Stecker von Port 1 ab. Die Anzeige muss nun die dazu passende Information **Chan1/2=Down/Up** liefern. Wiederholen Sie den Test auch mit den übrigen möglichen Kombinationen.

Im Linienbetrieb und das ist für EN100-Module in elektrischer Ausführung die einzige Betriebsart, stellt sich die Information in Zeile 7 ein wenig anders dar. Die Meldung **Phy1 100 MBit Full-Duplex** will uns sagen, dass gegenwärtig Port 1 aktiv ist und mit einer maximalen Übertragungsrate von 100 MBit im Vollduplexmodus arbeitet. Auch hier sollten Sie durch Abziehen eines Kabels eine Leitungsunterbrechung simulieren und die Reaktion des Moduls überprüfen.

Telegrammzustellung

Einiges über den Telegrammverkehr erfahren Sie in den Zeilen 8 bis 10. Zeile 8 zeigt die Zahl der empfangenen und gesendeten Telegramme an. Dieser Zähler informiert Sie neben einer absoluten Zahl also auch darüber, ob die Schnittstelle grundsätzlich Telegramme empfangen und senden kann. Erkannte Telegrammfehler werden ebenfalls gezählt, der jeweils aktuelle Wert wird in Zeile 9 angezeigt. Der Wert in Zeile 10 ist ein 10-Sekunden Mittelwert aus der Anzahl der empfangenen und gesendeten Telegramme.

Sechs hilft ...

Wir wollen natürlich hoffen, dass für alle Module nur positive Meldungen in den Displays zu lesen sind. Sollte dem nicht so sein, ist systematische Fehlersuche angesagt. Da Sie nun schon Ihren Blick auf das Display gerichtet haben, sehen Sie sich bitte den Inhalt der Zeile 6 an, die wir vorhin in der Betrachtung übergangen hatten. Diese Zeile hat es in sich, können hier doch eine Vielzahl von Informationen angezeigt werden: Die IP-Adresse des NTP-Servers, der vergangene Zeitraum seit der letzten Zeitsynchronisation, der Hinweis auf eine inkonsistente Parametrierung und der Verweis auf einen anderen Teilnehmer, der dieselbe IP-Adresse besitzt wie das aktuell untersuchte Gerät.

... bei Beziehungskonflikten

Die zuletzt genannte Information ist besonders kritisch, denn sie führt dazu, dass keinerlei Verbindung zum Netzwerk aufgebaut wird. Sie wird daher statisch in der Form **!!MAC!!0007E908FCC8** angezeigt und überlagert die Anzeige der anderen drei Informationen. Die angezeigte MAC-Adresse identifiziert eindeutig den Teilnehmer im Netz, der eine identische IP-Adresse besitzt. Sie müssen nun die IP-Adresse eines der beiden Teilnehmer ändern und lösen damit hoffentlich das ursprüngliche Verbindungsproblem.

... bei unterschiedlichen Ansichten

Eine weitere Ursache für Verständigungsschwierigkeiten können inkonsistente Parameter sein. Auf gut Deutsch: Der Parametersatz des Moduls will nicht so recht zu dem des Gerätes passen. So etwas kann beispielsweise vorkommen, wenn Module zwischen Geräten getauscht, die Geräte aber nicht neu initialisiert wurden. Der Text **Corrupt parameters** weist Sie auf einen solchen Umstand hin. Allerdings nicht statisch wie bei der doppelten Adressenvergabe, sondern im Wechsel mit den beiden Informationen zum NTP-Server.

... bei Unpünktlichkeit

Zur Erinnerung: Wir sind noch immer bei Zeile 6 und gehen jetzt einmal davon aus, dass keine Meldungen zu fehlerhaften Verbindungen angezeigt werden. Dann sehen Sie an dieser Stelle zwischen Zeile 5 und Zeile 7 die IP-Adresse des NTP-Servers im zehnsekündlichen Wechsel mit einer Zeitangabe: **NTP last sync 0033s**. Die angezeigte Zeit ist also vergangenen seit der letzten Zeitsynchronisation.

Unmittelbar nach dem Anlauf des Gerätes bis zur ersten Synchronisierung nach ca. einer halben Minute ist im Gerät keine gültige Uhrzeit verfügbar. Sollten Sie allerdings den maximal möglichen Wert von 999 Sekunden in der Anzeige zu Gesicht bekommen, können Sie davon ausgehen, dass der NTP-Server seinen Einsatz verschlafen hat. In einem solchen Fall müssen Sie also mit den Diagnosewerkzeugen des jeweiligen NTP-Servers nach der Ursache fahnden.

Verbindungsanalyse

Haben alle Überprüfungen ergeben, dass die Teilnehmer an sich nicht die Ursache der fehlenden Verbindung sein können, nehmen Sie sich noch einmal die Verbindungsleitungen zur Brust. Haben Sie bedacht, dass Sie bei den elektrischen Verbindungen zwischen Schutzgerät und Switch keine Crossover-Kabel verwenden dürfen? Sind mechanische Schäden an den Kabeln sichtbar? Oder liefert ein Stecker möglicherweise nicht den nötigen Kontakt?

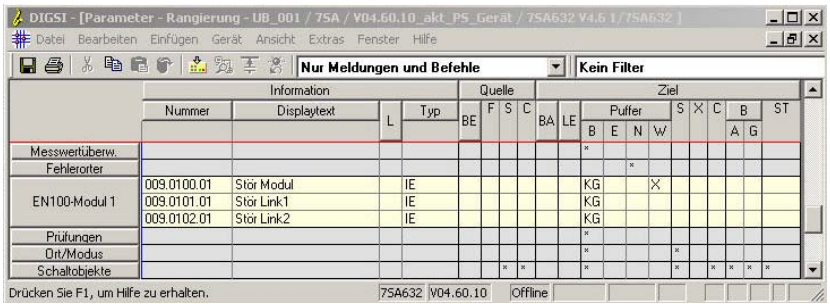
Nehmen wir an, dass in einem optischen Ring der Port eines Moduls den Zustand **Down** besitzt. In diesem Fall lohnt ein Blick auf das benachbarte Gerät, das mit diesem Port verbunden ist. Zeigt sich auch hier der korrespondierende Port kränklich, dann liegt es nahe, den Fehler bei der Verbindungsleitung zu suchen.

Gedämpfte Stimmung

Überhaupt erhalten Sie für die optischen Module auf der Modulinformationsseite noch weitere Hinweise, die Ihnen bei der Fehlersuche behilflich sein können. So finden Sie Informationen zur Empfangsleistung LRx und zur Sendeleistung LTx der einzelnen Ports in den Zeilen 12 (Port 1) und 13 (Port 2). Der Wert **norm** signalisiert, dass alles im grünen Bereich ist. **Weak** bezeichnet eine bereits zu niedrige Leistung und sehen Sie nur noch waagrechte Striche, ist die Dämpfung eindeutig zu hoch. Die Ursache dafür muss nicht, kann aber in mangelhaften Verbindungsleitungen liegen.

Fernverbindung

Lösen wir uns einmal kurz von der Modulseite im Display und damit von der Kontrolle vor Ort am Gerät selbst. Auch über die Ferne hinweg können Sie mit DIGSI 4 erfahren, ob das Modul sowie die beiden Schnittstellen korrekt arbeiten oder ob eine Störung vorliegt. Dazu gibt es eine Modulstörungsmeldung bzw. zwei Linkstatusmeldungen, die im Betriebsmeldepuffer protokolliert werden. Die Modulstörungsmeldung zeigt ein funktionsunfähiges Modul an. Die beiden Linkstatusmeldungen informieren über den physischen Zustand der Verbindung.



Meldungen des EN100 Moduls in DIGSI 4

Sie können diese Meldungen in der Gerätematrix auf verschiedene Ziele rangieren, beispielsweise auf LEDs des Gerätes. Wie Sie dabei grundsätzlich vorgehen, erfahren Sie in unserer Lektüre **DIGSI 4 - Start Up**.

Ringfunktionalität testen

Nach eingehendem Test der Kommunikationsfähigkeit und des EN100-Moduls folgt nun ein Lückentest. Wir werden also prüfen, ob sich in unserem optischen Ring die logische Lücke da auftut, wo wir diese haben wollten. Auch dabei hilft uns die Modulinformationsseite weiter. Auf dieser kontrollieren Sie als erstes, ob die in DIGSI 4 für die Kommunikationsparameter eingestellten Werte korrekt im Gerät angekommen sind.

Hinweis am Rand:
Falls Sie sich für OSM entschieden haben, dann sind die Zeilen 15 bis 21 nicht sichtbar.

Zeile 14 zeigt die im Modul eingestellte Redundanzbetriebsart. In unserem Fall sollte das RSTP sein. Der Wert für die Priorität in Zeile 15 muss übereinstimmen mit dem von Ihnen speziell für Ihre Topologie festgelegten Wert.

Ganz wichtig sind die Werte der Parameter in den Zeilen 17 bis 20. Diese müssen unbedingt so eingestellt sein, wie wir es in Kapitel 7 erläutert hatten. Hier noch einmal eine Übersicht zu den betreffenden Parametern und deren zwingend notwendigen Einstellungen.

- **Hello Time**: 2 s
- **Max Age Time**: 40 s
- **Forward Delay**: 21 s
- **Max Transmit Count**: 100

Mit den Informationen aus Zeile 21 überprüfen Sie, ob das Modul auch die gewünschte Ringfunktionalität besitzt. Für jeden der beiden Ports werden die Rolle und der Zustand (= Status) angezeigt. Bevor wir darauf eingehen, wie Sie die angezeigten Informationen auswerten, hier noch einmal eine kurze Wiederholung zu den möglichen Rollen und Zuständen eines Ports.

Folgende Rollen sind für die Ports definiert:

- Rolle **Root-Port** (R):
  Ein Root-Port ist logisch mit dem Root-Switch verbunden. Beim internen Switch des EN100-Moduls hat immer einer der beiden Ports die Rolle eines Root-Ports.
- Rolle **Designated-Port** (D):
  Ein Designated-Port kann ebenfalls eine Verbindung zum Root-Switch herstellen, aber auf einem anderen Weg. In der Regel hat einer der beiden Ports des internen Switches die Rolle eine Designated-Ports.
- Rolle **Alternate-Port** (A):
  Ein Alternate-Port kann im Fehlerfall eine logische Verbindung herstellen. Im stabilen Betrieb darf es im Ring nur exakt einen Alternate-Port geben. Existiert im Ring kein Port mit dieser Rolle, dann ist die Redundanz nicht gewährleistet.

Folgende Zustände sind für die Ports definiert:

- Zustand **Forwarding** (F):
  Dieser Zustand ist im Normalbetrieb der Zustand der Ports, die die Rolle Root oder Designated spielen. In diesem Zustand werden Nutzdatentelegramme immer übertragen.
- Zustand **Discarding** (D)
  Dieser Zustand bedeutet, dass Telegramme nicht weitergeleitet oder verworfen werden. Im Normalbetrieb besitzt nur der Alternate-Port diesen Zustand.

Zurück zu Zeile 21. Sie erkennen die logische Trennstelle daran, dass ein Port die Rolle (R) **Alternate** und den Zustand (S) **Designated** besitzt. Wird also beispielsweise die Information **R/S1=A/D R/S2=R/F** angezeigt, dann sind Sie fündig geworden: Port 1 dieses Gerätes ist die logische Trennung im Ring, also der Alternate Port.

Der Zustand des Ports ändert sich, wenn der Ring physisch aufgetrennt wird. Die logische Trennstelle wird dann geschlossen. Dazu nimmt der Port zunächst den Zustand **Discarding** an. In diesem Zustand werden nur Verwaltungsinformationen versendet, z.B. zur Änderung der Rolle des Ports. Sobald der Port den Zustand **Forwarding** erreicht und die Rolle **Root** angenommen hat, ist die logische Umkonfigurierung des Netzes abgeschlossen. Nun werden wieder Nutzdatentelegramme gesendet.

Sie können und sollten dieses Verhalten auch testen. Dazu müssen Sie lediglich an einer Stelle des Rings die Verbindung auftrennen, indem Sie an einem Modul das Netzwerkkabel abziehen. Die Displayanzeige in Zeile 21 des Gerätes, das als Alternate Bridge arbeitet, sollte danach so aussehen: **R/S1=R/F R/S2=R/F**.

Sie können nach dem Alternate-Port in einem Netz auch automatisiert suchen. Per Batch-Datei beziehungsweise Skript lassen Sie die Homepages aller EN100-Module durchsuchen. Mehr zu diesen Möglichkeiten erfahren Sie in Kapitel 13.

Noch mehr Details erfahren mit der Modulhomepage

Kommen wir doch noch einmal zurück auf unsere Modulhomepage. Welche vielfältigen Auskünfte diese Ihnen geben kann, erkennen Sie, sobald Sie ein paar Klicks im Menü am linken Rand spendieren.

Langzeitgedächtnis

Da ist zum Beispiel der Fehlerspeicher. Dessen Inhalt bringen Sie mit einem Klick auf **Error-Buffer** auf den Schirm. Ist der Fehlerspeicher leer, bleibt die Stimmung auch weiterhin positiv.

Ein weiterer wichtiger Speicher ist der Print-Puffer, dessen Inhalt Sie über den gleichnamigen Link zu Tage bringen. Die angezeigten Informationen zu deuten, wird Ihnen allerdings schwer fallen.

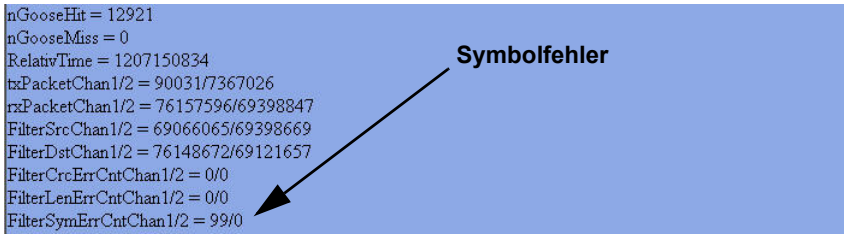
Vielmehr dienen diese unserer Hotline als Basis für eine gezielte Fehlerdiagnose in Fällen, wo Sie selbst nicht mehr weiterkommen.

Ohne Unterleib: Auszug aus dem Print-Buffer

Statistics-Seite

Was Ihnen bei der Inbetriebnahme hier und da weiterhelfen kann, ist ein gezielter Blick in die so genannte Statistics-Seite. Diese ist ein Querschnitt an Informationen über die Datenübertragung inklusive der Switches. Eine Tabelle am Ende dieses Abschnitts zeigt Ihnen sämtliche Informationen einschließlich einiger Erläuterungen.

Einige Informationen verdienen jedoch eine individuelle Betrachtung. Von besonderer Bedeutung ist beispielsweise die Anzahl der fehlerhaften Symbole, die eine Aussage über die Verbindungsqualität trifft: Je höher der Wert, desto schlechter die Verbindung. Dieser Wert wird beim Ein- und Ausschalten oder einer Verbindungsunterbrechung hochgezählt. Im laufenden Betrieb darf sich die Zahl dagegen nicht ändern.



Sogar Symbole können irren: Ein Ausschnitt der Statistics-Seite zeigt die Anzahl der Symbolfehler.

Kostenlose Zusatzinfos

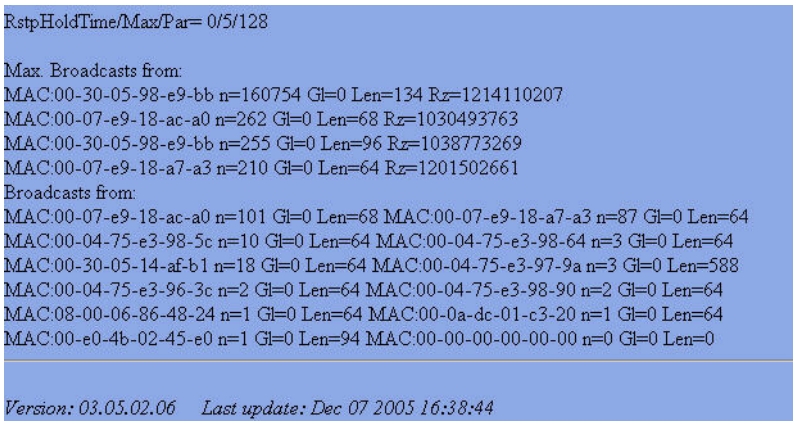
Hier noch einige weitere interessante Informationen:

- **RSTP-Role Chan1/2 = Alternate/Root**
  Sind die SIPROTEC 4 Geräte im Ring angeordnet, der Ring geschlossen und mit den externen (eingeschalteten) Switches verbunden, dann muss die FEC-Statistik eines der SIPROTEC 4 Geräte diese Anzeige enthalten. Ist diese auf keinem Gerät des Ringes vorhanden, ist der Ring an mindestens einer Stelle physisch unterbrochen.
- **FilterSymErrCntChan1/2 = 0/2753**
  Wenn diese beiden Zähler im stabilen Betrieb des Gerätes hochlaufen, ohne dass eines oder beide Nachbargeräte ausgeschaltet sind, liegt ein schlechte LWL-Verbindung vor. Ursache kann eine erhöhte Dämpfung zum Beispiel durch schlechte Kabel sein.
- **Frames Loss = 0**
  Ein Wert ungleich Null signalisiert kreisende Multicasttelegramme.
- **FNS queue overflow = 0**
  Ist der Wert dieser Information ungleich Null, dann ist das ein Indiz für kreisende Broadcasttelegramme.

Beachten Sie bitte, dass Sie die Anzeige der Webseite manuell aktualisieren müssen, um Änderungen bei Variablenwerten oder Zählerständen sehen zu können.

Breitenfunk

Wer sich übrigens näher für Broadcasttelegramme interessiert, wird ebenfalls in der Statistics-Seite fündig, wie die folgende Abbildung zeigt.



Für Fans von Broadcasttelegrammen hat die Statistics-Seite einiges zu bieten.

- **Max Broadcasts from**
  Hier sind die 4 häufigsten Broadcasts seit dem Anlauf des Moduls aufgeführt. Sie werden durch 5 Einzelinformationen beschrieben:
  - Die MAC-Adresse des Broadcastsenders
  - Die Anzahl n dieser Broadcasts innerhalb der letzten 4 Minuten
  - Die Anzahl Gl der aufeinanderfolgenden identischen Telegramme
  - Die Länge Len der Telegramme
  - Die Relativzeit Rz

- **Broadcasts from**
  Hier sind die aktuellen Broadcasts im laufenden 4-Minuten-Intervall aufgelistet. Pro Zeile sind jeweils 2 Sender mit folgenden Angaben enthalten:
  - Die MAC-Adresse des Broadcastsenders
  - Die Anzahl n der Broadcasts seit dem Beginn des Intervalls
  - Die Anzahl GI der aufeinanderfolgenden identischen Telegramme
  - Die Länge Len der Telegramme

Alles auf einmal

Hier nun die vollständige Übersicht zu den einzelnen Informationen der Statistics Seite. Die Sollwerte sind nur angegeben, wenn sie statisch sind.

Name	Soll	Beschreibung
RxFrames		Zähler für empfangene Telegramme, die an Modulapplikationen und TCP/IP-Stack weitergeleitet werden.
BD out of sequence	0	Zähler für Empfangspufferüberläufe im Kommunikationsprozessor. Der Wert muss immer Null sein.
Miss		Zähler für empfangene Telegramme, die nicht der MAC-Adresse des Gerätes entsprechen.
Broadcast		Zähler für empfangene Broadcasttelegramme
Multicast		Zähler für empfangene Multicasttelegramme
More than 0x5f0 Bytes		Zähler für zu lange Telegramme (1520 Bytes), die verworfen werden.
Non Octett	0	Zähler für die Anzahl der Bits, die nicht durch 8 teilbar sind. Ist dieser Wert ungleich Null, dann können Problem mit der Übertragungsstrecke vorliegen. Das kann auch der Fall beim physikalischen Unterbrechen einer Verbindung sein.
CRC-Error	0	Zähler für empfangene Telegramme mit fehlerhafter CRC-Prüfung. Hinweis auf Probleme mit der Übertragungsstrecke.
Overrun	0	Zähler für Empfängerüberlauf. Deutet auf Performanceprobleme des Ethernet-Controllers hin.
Truncated	0	MAC-interner Zähler. Zähler für gekürzte Empfangstelegramme (größer 2 kB).
TxFrames		Zähler der gesendeten Telegramme.
no transmit buffer	0	Inkrementieren kann nur bei vielen Kollisionen oder Retransmissions auftreten.

Name	Soll	Beschreibung
FNS queue overflow	0	Zählt nicht ausgewertete Broadcasttelegramme, weil der Prozessor überlastet ist. Wird i.d.R. durch kreisende Telegramme ausgelöst.
Frames Loss	0	Anzahl der verworfenen Empfangstelegramme, wenn mehr als 1000 solcher Telegramme pro Sekunde aufgetreten. Kann nur bei kreisenden Telegrammen auftreten.
TxDef	0	Zählt die 'Defers' beim Senden von Frames. Läuft der Zähler hoch, deutet das auf eingestellten Halbduplexbetrieb hin.
TxHB	0	Heartbeat Zähler
TxLC	0	Late Collision Zähler
TxRL	0	Zählt Überschreitungen des 'Retransmission Limits'
TxRC	0	Zählt Retransmissions. Hinweis auf Kollisionen
TxUN	0	Zählt 'Buffer underrun'
TxCSL	0	Zählt 'Carrier sense lost'
MaxTxBD		Maximaler Füllstand des Sendepuffers
nGooseHit		Zählt die empfangenen GOOSE-Telegramme
nGooseMiss		Zählt die GOOSE-Telegramme, die den Multicastfilter passiert haben, aber für das Gerät nicht plausibel sind (z.B. durch fehlerhafte GOOSE-Parametrierung).
Relative time		Momentaner Stand des Relativzeitzählers. Ist ein jede Millisekunde inkrementierter 32-Bit Zähler. Startet bei 120000 (entspricht etwa 49 Tage, danach Neustart bei 0).
Module CPU load		Auslastung CPU
txPacketChan1/2		Anzahl aller Datenpakete, die der Port gesendet hat.
rxPacketChan1/2		Anzahl aller Datenpakete, die der Port empfangen hat.
FilterSrcChan1/2		Anzahl aller empfangenen Datenpakete, bei der die Source Adresse nicht mit der eigenen Adresse übereinstimmt.
FilterDstChan1/2		Anzahl aller empfangenen Datenpakete, bei der die Destination Adresse nicht mit der eigenen Adresse übereinstimmt.
FilterCRCErrCnt Chan1/2	0	Anzahl der Datenpakete mit CRC Fehler.

Name	Soll	Beschreibung
FilterLenErrCnt Chan1/2	0	Anzahl der Datenpakete die zu lang oder zu kurz sind. Die zulässige Länge beträgt 64 Byte bis 1518 Byte.
FilterSymErrCnt Chan1/2	0	Anzahl der empfangen Symbolfehler (ungültige 4b5b Werte) auf der Leitung. Diese Überwachung liegt im Phy.
overflowExtCnt Chan1/2	0	Für diesen Wert gibt es im FPGA keinen Zähler.
overflowIntCnt Chan1/2	0	Für diesen Wert gibt es im FPGA keinen Zähler.
overflowIntTraCnt	0	Für diesen Wert gibt es im FPGA keinen Zähler.
OptLevelChan1/2	> 2300	Pegel des opt. Empfängers in mV. Sollte bei verbundenen Kabel nicht kleiner als 2300 sein.
EPLD-Version		Aktuelle Version des EPLDs
Data Size, Code Size, NORMAL pool, ENTRY pool, GOOSE pool, WEAK pool		interne Speicherverwaltung
Malloc Size		interne Speicherverwaltung

Was Sie sonst noch wissen sollten 13

In diesem Kapitel haben wir Ihnen noch Nützliches und Informatives zusammengestellt.

Hyperterminalverbindung einrichten

Für alle, die es noch nie gemacht haben und auch für die, die sich nicht mehr darin erinnern können, beschreiben wir in diesem Abschnitt, wie Sie eine Hyperterminalverbindung einrichten.

Eine Hyperterminalverbindung realisieren Sie ausschließlich mit Windows-Bordmitteln. Der Vorteil: Weitere Software benötigen Sie dazu nicht. Der Nachteil: Abhängig von der Betriebssystemvariante unterscheidet sich die Vorgehensweise. Wir beschreiben Ihnen nun kurz, wie Sie eine Hyperterminalverbindung unter Windows XP einrichten und starten.

Verbinden Sie zunächst PC und Switch mit dem 1:1-Kabel und schalten Sie beide Geräte ein.

Ab in den Hyperspace

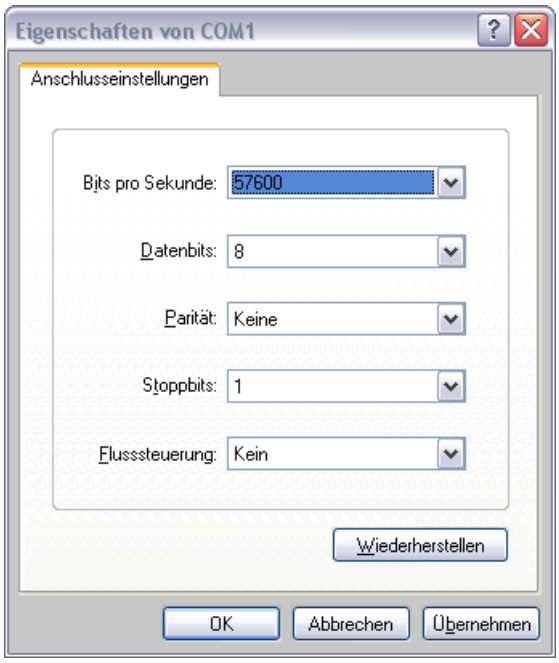
Öffnen Sie das Startmenü und wählen Sie **Programme** → **Zubehör** → **Kommunikation** → **Hyperterminal**. Windows geht mit dem folgenden Dialog in Erwartungshaltung:

Schrittweise ans Ziel: Zuerst den Namen, ...

Geben Sie hier einen Namen für die neue Hyperterminalverbindung ein und wählen Sie eines der angebotenen Icons dafür aus. Danach klicken Sie wie üblich auf **OK**. Windows lässt noch nicht locker und schiebt gleich ein weiteren Dialog nach.

... dann den COM-Port, ...

Aus der Liste **Verbindung herstellen über** wählen Sie die Bezeichnung der seriellen Schnittstelle des PCs, an welcher Sie das 1:1-Kabel angeschlossen haben. Die übrigen Texteingabefelder werden dadurch deaktiviert und Ihr anfänglicher Schock über die vermeintliche Notwendigkeit irgendwelcher Rufnummern sicherlich gelindert. Allerdings hat Windows noch immer nicht genug und fordert zusätzliche Daten an.



... und schließlich noch einige Parameterwerte festlegen.

Die von Windows als Standard vorgeschlagenen Einstellungen wollen nicht so recht zu unseren Anforderungen passen. Deshalb ändern Sie diese bitte so, dass diese mit den oben gezeigten Werten übereinstimmen.

Mit einem Klick auf **OK** beenden Sie das Einrichten der Hyperterminalverbindung. Allerdings müssen Sie diese noch explizit speichern, um jederzeit auf die festgelegten Einstellungen zurückgreifen zu können. Ein Klick auf **Speichern** im Menü **Datei** des Terminalfensters genügt dazu. Den Namen **Switch einstellen** hatten wir ja bereits zu Beginn der ganzen Aktion festgelegt. Sie können ab sofort das Hyperterminal mit den gewählten Einstellungen direkt über das Startmenü öffnen, also in unserem Fall mit **Programme** → **Zubehör** → **Kommunikation** → **Hyperterminal** → **Switch einstellen**. (Hier liegt ausnahmsweise einmal die Würze nicht in der Kürze.)

Switch-Konfigurationen speichern und laden

Fünf Switches, wie in unserer Beispielkonfiguration, sind eine noch durchaus überschaubare Angelegenheit. Bei etwas größeren Anlagen können daraus allerdings schnell auch fünfzig Switches werden. Da kommt es einem gelegen, wenn man die Konfiguration eines Switches speichern, bei Bedarf ein wenig ändern und möglichst vielen anderen Switches wieder unterschieben kann. Voraussetzung ist, dass es sich um Switches desselben Typs handelt.

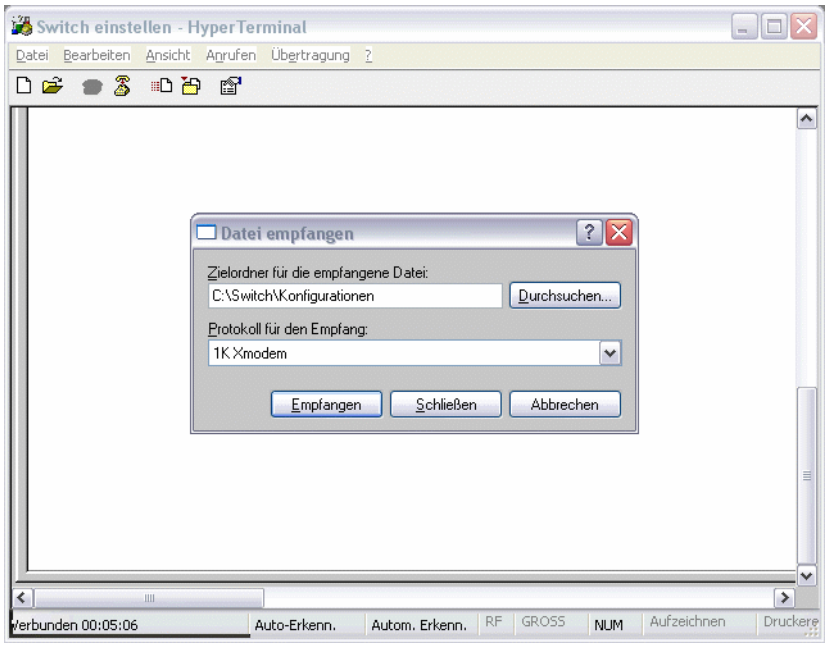
Die Konfigurationen werden als CSV-Dateien und damit als bearbeitbarer Text gespeichert. Ein schlichter Texteditor reicht zur Nachbearbeitung also völlig aus, mit dem Sie dann beispielsweise die IP-Adresse ändern. Übrigens lassen sich die Konfigurationsdateien auch per Batch-Datei aus- und wieder einlesen - rationellem Arbeiten steht also nichts mehr im Wege.

Raus ...

Die Konfiguration muss aus dem Switch ausgelesen werden. Dazu benötigen Sie wieder eine aktive Hyperterminal-Verbindung zu diesem. Im Befehlsbereich geben Sie **xmodem send config.csv ein** und wählen dann **Transfer** → **Receive File**, was zur Anzeige eines Dialogs führt. Auch für das Empfangen von Informationen verwenden wir das Protokoll **1Kxmodem**. Zielort und Name der Konfigurationsdatei legen Sie nach Belieben fest. Klicken Sie auf **Empfangen**: Die Daten werden aus dem Switch in den PC übertragen und dort gespeichert.

... und rein

Um eine vorhandene Konfiguration in einen Switch zu laden, gehen Sie prinzipiell genauso vor wie beim Update der Firmware. Tippen Sie das Befehl **xmodem receive config.csv** im Terminalfenster ein. Danach öffnen Sie mit dem Befehl **Datei senden**, den Sie im Menü **Übertragung** finden, den Dialog **Datei senden**. Wählen Sie erneut **1Kxmodem** als Sendeprotokoll und geben Sie Namen und Pfad der Konfigurationsdatei an. Nach einem Klick auf **Senden** überträgt der PC die Daten in den Switch.



Zeitersparnis: Konfigurationen können gespeichert und geladen werden.

In größeren DOSen

Wäre es nicht praktisch, CSV-Dateien in größeren Mengen auszulesen und anschließend wieder in den Switch zu laden? Das klappt ganz einfach mit Batch-Dateien und einer tftp-Verbindung. Die Microsoft-Betriebssysteme bringen von Haus aus einen tftp-Client mit, den Sie über die gute alte DOS-Kommandozeile nutzen. Wir zeigen Ihnen erst einmal, wie es grundsätzlich mit einer einzelnen Datei funktioniert.

Wählen Sie aus dem Startmenü den Befehl **Ausführen** und tippen Sie dann in das Texteingabefeld **Command** ein. Nach einem Klick auf **OK** öffnet Windows das DOS-Fenster. Hier geben Sie nun in etwa Folgendes ein:

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

Als IP-Adresse setzen Sie die des Switches ein, dessen Konfigurationsdatei ausgelesen werden soll. **C:\Config\Switch_1.csv** entspricht dem Zielort und dem Zielnamen der Datei. Diese Angaben müssen Sie natürlich anpassen.

Sobald Sie die Eingabetaste drücken, wird der Befehl abgesetzt und Sie erhalten als Antwort die gewünschte Datei zurück. Voraussetzung ist natürlich, dass der betreffende Switch und der PC grundsätzlich über das Netz kommunizieren können.

Das Laden der Konfigurationsdatei in den Switch funktioniert nach demselben Muster:

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

Um das Auslesen zu rationalisieren, packen wir nun alle get-Befehle in eine Batch-Datei namens **get.bat**. Diese sieht dann für die 5 Switches unserer Beispieltopologie so aus:

```
rem Auslesen aller csv-Dateien
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 ende
```

Analog dazu präsentiert sich die Datei **put.bat** zum Laden der Konfigurationen folgendermaßen:

```
rem Laden aller csv-Dateien
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 ende
```

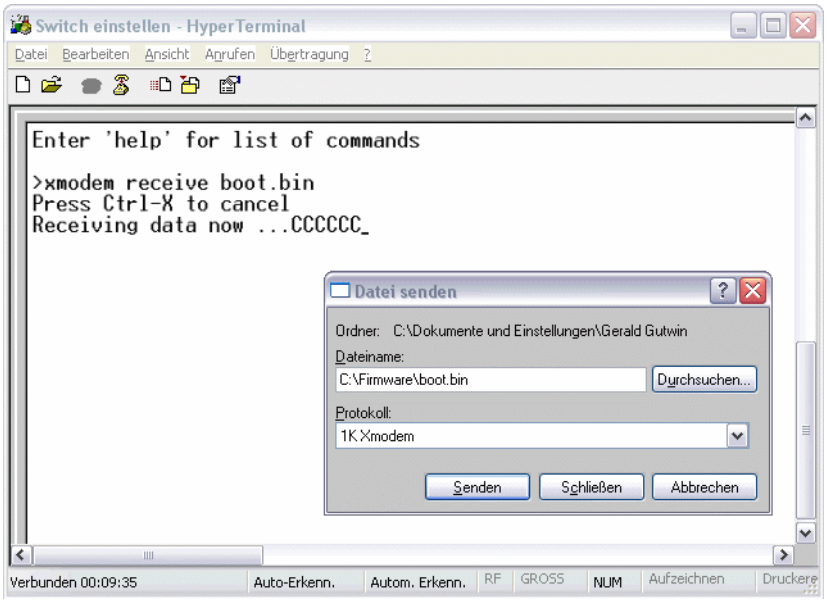
Neue Firmware in den Switch laden

Gehen wir vom Idealfall aus, dann haben Sie sich soeben mit fabrikneuen Switches eingedeckt, ausgestattet natürlich mit der aktuellsten Firmware. Oft vergehen aber doch einige Tage oder gar Wochen, bis die neu erworbenen Switches zum Zuge kommen. Während diese nun im Regal liegend auf ihren Einsatz warten, kann es durchaus vorkommen, dass dem Hersteller noch einige Ideen zur Verbesserung der einen oder anderen Funktion in den Sinn kommt. Für Sie heißt das, sich zunächst einmal zu informieren, ob es bereits eine aktuellere Firmware als die im Switch geladene gibt. Und das gilt natürlich erst recht für Switches, die Sie schon längere Zeit in Betrieb haben. Für die von uns empfohlenen Switches RS 8000 T und RS 1600 finden Sie mögliche Firmwareupdates unter www.ruggedcom.com. Ein kompletter Patch besteht dabei aus zwei Dateien: boot.bin und main.bin.

Schön der Reihe nach

Grundsätzlich gilt für ein Update der Firmware: Erst die Datei **boot.bin** in den Switch laden, danach die Datei **main.bin**. Deshalb tippen Sie als erstes das Befehl **xmodem receive boot.bin** im Anzeigebereich des Terminalfensters ein. Danach öffnen Sie mit dem Befehl **Datei senden**, den Sie im Menü **Übertragung** finden, den Dialog **Datei senden**.

Aus der Liste der verfügbaren Sendeprotokolle wählen Sie **1Kxmodem**. Im Texteingabefeld darüber tragen Sie entweder direkt den Namen **boot.bin** einschließlich des gesamten Pfades ein oder wählen die Datei über den Durchsuchen-Dialog. Mit einem Klick auf **Senden** sollte genau dieses passieren. Voraussetzung: Es besteht nach wie vor eine Verbindung zwischen PC und Switch. Das erkennen Sie leicht an den Telefon-Symbolen in der Symbolleiste.



Runderneuerung: Per Hyperterminal aktualisieren Sie die Firmware des Switches.

Hat alles geklappt, wiederholen Sie den Vorgang, dieses Mal jedoch mit der Datei **main.bin**. Anschließend trennen Sie die Verbindung und führen am Switch einen Reset durch.

Kommunikationsmodul im SIPROTEC 4 Gerät tauschen

Falls Sie ihr bereits über Jahre liebgewonnenes Gerät für seine neue Aufgabe als Netzwerker vorbereiten möchten, dann können Sie schon Mal das Werkzeug bereit legen. Denn es wird in jedem Fall nötig sein, das gegenwärtig installierte Kommunikationsmodul gegen eines vom Typ EN100 auszutauschen. Dabei müssen Sie in jedem Fall folgende Reihenfolge beherzigen:

1. Aktualisieren Sie die Gerätefirmware auf Versionsstand 4.6.
2. Bauen Sie das bisherige Modul aus.
3. Setzen Sie das EN100-Modul ein.
4. Laden Sie bei Bedarf die Modulfirmware in das Gerät.
5. Testen Sie die Verfügbarkeit des neuen Moduls.

Sollten Sie diese Reihenfolge durcheinander würfeln, wird nach dem Einbau des Moduls das Gerät möglicherweise nicht mehr bedienbar sein; der Ausbau des Moduls mit nachfolgendem Downgrade ist dann die Folge und der Arbeitsaufwand letztlich erheblich höher als nötig.

Seelenanalyse 1

Die genaue Beschreibung, wann Sie wie die Firmware eines Gerätes aktualisieren und was dabei zu beachten ist, füllt mit allen Detailangaben rund 30 Seiten.

Diese können Sie sich wieder unter **www.siprotec.de** besorgen. Dort verbergen sich hinter dem Eintrag **Geräte** nicht nur die nötigen Informationen zur Vorgehensweise, sondern auch aktuelle Firmware-Updates und Gerätetreiber für DIGSI 4. Wir skizzieren deshalb nur die grundsätzlichen Stationen auf dem Weg von einer älteren zu einer neueren Firmwareversion.

- Prüfen Sie zunächst, ob Sie überhaupt ein Firmware-Update für das betreffende SIPROTEC 4 Gerät benötigen und ob das Gerät für ein Firmwareupdate geeignet ist. Falls ja, dann laden Sie die Updatedateien von der SIPROTEC-Website herunter.
- Prüfen Sie, ob es durch das Firmwareupdate nötig wird, Ihre DIGSI 4-Installation zu ergänzen. Das ist immer dann der Fall, wenn sich die Firmwareversionsbezeichnung auf der 1. Stelle hinter dem Dezimalpunkt geändert hat. Die benötigten Update-Dateien erhalten Sie ebenfalls auf der SIPROTEC-Website.
- Sichern Sie mit DIGSI 4 vor dem Firmwareupdate den Parametersatz, der sich aktuell im Gerät befindet. Lesen Sie ebenfalls alle Prozessdaten aus dem Gerät aus.
- Installieren Sie das Firmwareladeprogramm auf Ihrem PC. Auch dieses können Sie von der SIPROTEC-Website herunterladen.
- Schalten Sie das Gerät spannungslos, verbinden Sie es mit dem PC.
- Aktualisieren Sie die Firmware.
- Nehmen Sie das Gerät in Betrieb und testen Sie die Funktionalität.

Hat alles geklappt, dann können Sie guten Gewissens das Kommunikationsmodul tauschen.

OP vorbereiten

Legen Sie am besten zunächst das benötigte Werkzeug zurecht. Sie brauchen ...

- ... eine Unterlage, die für elektrostatisch gefährdete Bauelemente geeignet ist,
- einen Schlitzschraubendreher mit 5 mm bis 6 mm Klingenbreite,
- einen Kreuzschlitz-Schraubendreher Pz Größe 1 und
- einen Steckschlüssel mit einer Schlüsselweite von 4,5 mm.

Packen Sie auch gleich das neue Modul aus und legen Sie dieses ebenfalls bereit.

Bevor Sie das Gehäuse öffnen, müssen Sie in jedem Fall das SIPROTEC 4 Gerät allpolig von der Versorgungsspannung trennen, so viel Zeit muss sein! Lösen Sie auch alle sonstigen möglicherweise vorhandenen Verbindungen zum Gerät.

Patient umdrehen

Nehmen Sie sich als Erstes die Rückseite des Gerätes zur Brust. Drehen Sie mit dem Kreuzschlitz-Schraubendreher alle Schrauben heraus, mit welchen die eingebauten Kommunikationsmodule fixiert sind. Mit dem Steckschlüssel drehen Sie die beiden Schraubbolzen der D-Sub-Buchse heraus.

Schwenken Sie das Gerät um 180 Grad und entfernen Sie dann an der Frontseite die vier Schraubenabdeckungen. Damit meinen wir die schmalen rechteckigen Plastikklappen am oberen und unteren Rand, jeweils links und rechts. Lösen Sie anschließend die Schlitzschrauben, die sich unter diesen Abdeckungen befinden.

Operation beginnt

Ziehen Sie nun die Frontabdeckung des Gerätes langsam ab und klappen Sie diese vorsichtig zur Seite. Allerdings bitte nicht zu weit, denn Frontabdeckung und Leiterplatte im Gehäuse sind noch über ein Flachbandkabel verbunden. Den Steckverbinder dieses Flachbandkabels müssen Sie von der Leiterplatte lösen. Dazu klappen Sie die Verriegelungshebel leicht nach oben bzw. nach unten, bis der Steckverbinder herausgedrückt wird. Und wenn Sie schon gerade dabei sind, dann machen Sie das Gleiche bitte auch noch für den Steckverbinder des zweiten Flachbandkabels, das die Verbindung zur benachbarten Leiterplatte herstellt.

Ziehen Sie jetzt die Leiterplatte aus dem Gehäuse und legen Sie diese auf die vorbereitete Unterlage; das bisher installierte Kommunikationsmodul muss dabei nach unten zeigen. Drehen Sie die beiden Befestigungsschrauben des Kommunikationsmoduls komplett heraus. Wenden Sie anschließend die Leiterplatte und ziehen Sie das Modul nach oben ab. Das neue Kommunikationsmodul setzen Sie mit leichtem Druck ein, drehen die Leiterplatte und befestigen es mit den beiden Schrauben.

Nun schieben Sie die Leiterplatte wieder in das Gehäuse. Orientieren Sie sich dabei an den vorhandenen Markierungen. Verbinden Sie die Leiterplatte mit den Steckverbindern. Dabei achten Sie darauf, dass die Verriegelungshebel sicher einschnappen.

Operation beendet

Der restliche Ablauf ist denkbar einfach:

- Frontabdeckung mit leichtem Druck aufsetzen,
- Schrauben eindrehen,
- Abdeckungen aufsetzen,
- auf der Rückseite Schrauben für Kommunikationsmodule eindrehen.

Wenn Sie das, was wir Ihnen soeben erläutert haben, als kleinen Film sehen möchten, haben wir einen Tipp für Sie: Auf der CD „SIPROTEC 4 You – Start Up“ finden Sie eine animierte Anleitung, die Ihnen die grundsätzliche Vorgehensweise beim Austauschen von Kommunikationsmodulen zeigt. Eine ausführliche Beschreibung zum Herunterladen gibt es wieder unter **www.siprotec.de** im Bereich **Geräte > Allgemeine Informationen**. Legen Sie jetzt wieder Spannung an das Gerät.

Seelenanalyse 2

Module werden in der Regel mit geladener Modulfirmware ausgeliefert. Sollten Sie dennoch im Besitz eines Moduls ohne Firmware sein, müssen Sie diese nach dem Einbauen in das Modul laden. Wahrscheinlicher ist da allerdings der Fall, dass Sie die Firmware eines Moduls aktualisieren möchten. Über mögliche Updates informieren Sie sich wieder auf der SIPROTEC-Website.

Die Modulfirmware ist übrigens ab Version 3.0 für alle Modulbauformen gleich, es gibt also keinen Unterschied für Module mit elektrischer und optischer Schnittstelle bzw. Ein- und Aufbauausführung. Die Firmware selbst laden Sie vergleichbar zur Update-Prozedur der Gerätefirmware über die Frontschnittstelle in das Gerät und damit auf das Modul. Schalten Sie die Hilfsspannung des Schutzgerätes für einige Sekunden aus und dann wieder ein. Damit ist das Firmware- und Parameter-Update beendet.

Printf.html und fecst.html auslesen und speichern

Die Modulhomepage eines EN100-Moduls liefert Ihnen eine Reihe nützlicher Informationen, darunter auch den Inhalt des printf-Puffers und die Statistics-Seite. Sie können die Homepages nacheinander über die IP-Adressen der SIPROTEC 4 Geräte aufrufen und die genannten HTML-Seiten manuell speichern.

Aber es geht auch komfortabler. Mit einem hilfreichen Tool namens Curl und einer kleinen Batch-Datei erledigen Sie diese Aufgabe in weitaus weniger Zeit. Curl können Sie sich als Freeware bequem und kostenlos über das Internet besorgen.

Die Syntax für den Aufruf von Curl ist alles andere als kompliziert:

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

Im Beispiel holen Sie sich aus dem Gerät mit der IP-Adresse 172.16.10.1 die Printf-Seite und speichern diese als printf_1_380.html ab. Hier die Batch-Datei für alle Geräte in unserer Beispieltopologie:

```
rem Auslesen aller printf- und fecst-Seiten

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 Ende
```

Automatisierte RSTP-Statusabfrage

In Kapitel 12 haben wir Ihnen gezeigt, wie Sie zum Beispiel den Alternate-Port ausfindig machen können. Die beschriebenen Methoden mögen für die Inbetriebnahme durchgehen, für den laufenden Betrieb sind diese jedoch nicht praktikabel. Wir benötigen eine Methode, die es ermöglicht, verschiedene Informationen aus mehreren Geräten gleichzeitig anfordern zu können und diese dann mundgerecht präsentiert zu bekommen. Das könnte dann praktisch so aussehen:

Sie starten eine Datei, die in unserem Fall **scan.bat** heißt, und mir nichts dir nichts liefert Ihnen der PC eine Datei namens **Data.dat** zurück. Flugs die Datei mit einem x-beliebigen Editor geöffnet, zeigt uns diese Informationen von ihrer schönsten Seite, nach unseren Anforderungen gefiltert und übersichtlich formatiert:

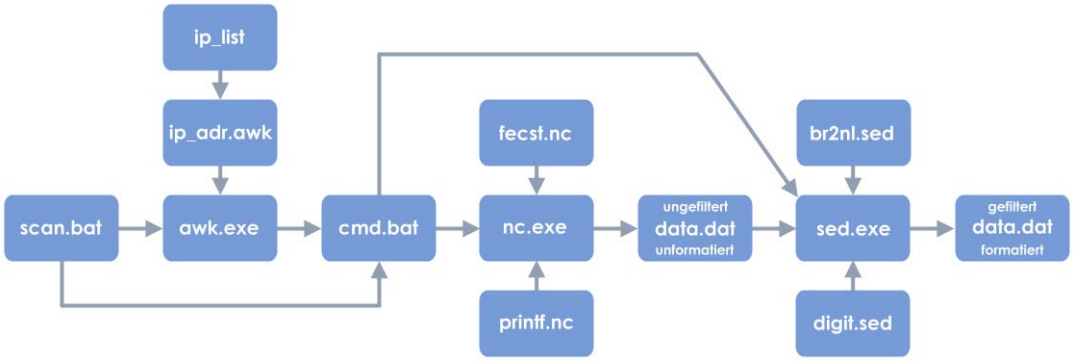
```
...
---------- 172.16.10.1 -------
IP = 172.16.10.1
MAC = 8-0-6-86-58-a7
nGooseHit = 12423
nGooseMiss = 0
RSTP-Role Chan1/2 = Designated/Root (Break 1<==2)
RSTP-State Chan1/2 = Forwarding/Forwarding
---------- 172.16.10.2 -------
IP = 172.16.10.2
MAC = 8-0-6-86-58-a9
nGooseHit = 52158
nGooseMiss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

Sie sehen in unserem Beispiel, welche Rollen und Zustände die einzelnen Ports momentan besitzen und Sie erfahren mit den Zählern **nGooseHit** und **nGooseMiss**, wie es um die Trefferquote bei GOOSE-Telegrammen steht. IP- und MAC-Adressen machen die Zuordnung der Informationen zu den einzelnen Geräten einfach.

Die Funktionsweise ist eigentlich ganz simpel. Mit Scan.bat starten Sie eine Prozedur, welche die Statistics-Seite und die printf-Pufferinhalte aller gewünschten Geräte ausliest, in einer Datei sammelt und anschließend filtert und formatiert. Filterkriterien und Formatanweisungen lassen sich anpassen und somit bestimmen Sie selbst über Form und Inhalt der zu liefernden Information.

Das klingt alles gut, ist es auch, aber dennoch gibt es einen kleinen Haken. Falls nämlich durch eine Vielzahl von Meldungen der printf-Puffer eines Gerätes übergelaufen sein sollte, sind möglicherweise genau jene Informationen, die Sie interessieren, nicht mehr verfügbar. Wir meinen allerdings, dass dieser kleine Nachteil verschmerzt werden kann.

Eine Grafik soll Ihnen zunächst verdeutlichen, welche Komponenten zwischen Scan.bat und Data.dat eine Rolle spielen. Drei kleine Programme wirken mit: nc.exe, awk.exe und sed.exe - alles Freeware, die Sie über das Internet herunterladen.



Immer schön von links nach rechts

Beginnen wir doch einfach mitten drin und richten unser Augenmerk auf die Datei **nc.exe** alias NetCat. Dieses ist das eigentliche Werkzeug, das die Informationen aus den einzelnen Geräten beschafft. Alles in der Grafik links davon erleichtert uns die Arbeit, sodass NetCat mit nur einem Doppelklick alle Geräte nacheinander befragt. Alles rechts der Mitte entschlackt die Informationen von überflüssigem Ballast und bringt diese in eine ansehnliche Form. Um NetCat zur Arbeit zu bewegen, erwartet dieses Programm einen Aufruf nach folgender Struktur:

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

Wie Sie sehen, benötigt NetCat einige Informationen. Die Hostadresse ist die IP-Adresse des Gerätes, von dem Sie Informationen benötigen. Der Port hat nichts mit einem Hardware-Port eines EN100-Moduls zu tun, sondern bezeichnet einen Softwareport. In Verbindung mit TCP/IP verwenden Sie dafür stets den Wert 80.

Ein Skript definiert, was NetCat genau zu tun hat. (Den Inhalt dieses Skripts gibt es gleich im Anschluss.) Und schließlich muss NetCat noch wissen, wohin mit den gewonnen Erkenntnissen. In unserem Fall ist das die Datei **Data.dat**. Da wir Informationen aus zwei unterschiedlichen Quellen wollen, nämlich aus fecst und printf, benötigen wir auch zwei Skripte für NetCat.

Skript 1 zur Beschaffung der Statistics lautet:

```
GET /fecst HTTP/1.1
--- Leerzeile ---
```

Skript 2 zur Beschaffung von printf lautet:

```
GET /printf HTTP/1.1
--- Leerzeile ---
```

Bitte beachten Sie, dass unmittelbar nach dem Befehl **GET ...** genau eine Leerzeile folgen muss, ansonsten funktionieren die Skripte nicht.

Für jedes Gerät muss NetCat zwei Mal aufgerufen werden. Da kommt bei einer durchschnittlichen Netztopologie schon einiges zusammen. Es bietet sich also an, alle Aufrufe in einer Batch-Datei zusammenzufassen. Diese soll cmd.bat heißen und beispielsweise so aussehen:

```
@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
```

Die gezeigte Datei **cmd.bat** bewirkt das sukzessive Scanning von fünf Geräten. Danach startet der Befehl in der letzten Zeile den Streameditor **sed.exe**. Dazu später mehr.

Sie müssen die Batch-Datei übrigens keineswegs per Hand erstellen. Ganz bequem lassen Sie sich diese vom Programm **awk.exe** generieren. Dazu muss dieses Programm noch strukturelle Informationen erhalten und es muss über die IP-Adressen der Geräte Bescheid wissen, die gescannt werden sollen. Der zugehörige Batch-Befehl für den Aufruf von awk.exe sieht dann so aus:

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

Hinter ip_adr.awk verbirgt sich ein Skript, das awk.exe anweist, mit welcher Struktur es cmd.bat generieren soll. Sie können dieses in der gegebenen Form übernehmen, insofern wollen wir hier auch nicht näher auf die einzelne Befehlabfolge eingehen. Viel wichtiger ist in diesem Zusammenhang die Datei **ip_list**. In diese müssen Sie zeilenweise die IP-Adressen sämtlicher Geräte eintragen, an deren Informationen Sie interessiert sind.

Hier ein Beispiel für ip_list:

```
#
# IP-Adressen aller Geräte
#
172.16.10.1
172.16.10.2
172.16.10.3
172.16.10.4
172.16.10.5
```

Wie Sie bereits wissen, starten Sie die gesamte Prozedur mit Scan.bat. Ein Blick in diese Datei verrät uns, dass sie zwei Dinge bewirkt.

```
@REM
@REM Scanne alle Adressen aus “ip-List”
@REM
@awk -f ip_adr.awk ip_list
@call cmd.bat
```

Scan.bat startet zunächst das Programm **awk.exe** und übergibt diesem die benötigten Dateien **ip_adr.awk** und **ip_list**. Awk.exe generiert anhand der Informationen in diesen Dateien die Batch-Datei **cmd.bat**. Scan.bat ruft diese Datei mit einer Call-Anweisung auf. Daraufhin wendet sich NetCat an ein Gerät nach dem anderen, extrahiert dabei jeweils die Informationen aus der Statistics-Seite und aus dem printf-Puffer und überträgt diese der Reihe nach in die Datei **Data.dat**.

Nach getaner Arbeit hinterlässt NetCat in dieser Datei alles, was aus den Quellen an Informationen zu bekommen war. Nur einen geringen Teil davon benötigen wir tatsächlich, den aber in vernünftiger visueller Qualität. Die gespeicherten Informationen erst zu filtern und anschließend zu formatieren, ist nun die Aufgabe von sed.exe. Dieser Streamingeditor nimmt auf der einen Seite Daten auf, die er anhand unterschiedlicher Muster und Kriterien auf der anderen Seite wieder ausspuckt, dann allerdings in meist reduzierter und geordneter Form.

Betrachten wir uns jetzt den Aufruf von sed.exe, den Sie als letzte Zeile in der Batch-Datei cmd.bat finden:

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

Auch hier werden die eigentlichen Anweisungen nicht direkt, sondern als Referenz auf zwei Skriptdateien gegeben: br2nl.sed und digit.sed. Die erste davon erhöht die Lesbarkeit der Informationen, indem es eine zeilenweise Darstellung erzeugt. Dazu werden einfach alle Zeilentrenner im ursprünglichen HTML-Format gegen ein ↵-Zeichen ersetzt. Das Skript benötigt dafür nur eine Befehlszeile.

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

Das zweite Skript ist da schon ein wenig komplizierter, da es die Informationen filtern und anschließend formatieren muss. Das sollte Sie aber nicht weiter stören, denn Sie können es prinzipiell 1:1 übernehmen.

Hier das Skript:

```
1 /extern 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
```

Sind für Sie weitere Informationen relevant, dann ergänzen Sie nach der Zeile 18 das Skript um weitere Anweisungen, die Sie wie die aus den Zeilen 17 und 18 formulieren.