

18 Ethernet-TCP/IP

18.1 Grundlagen

18.1.1 Übersicht

Ethernet-TCP/IP ist ein weltweit erprobter und akzeptierter Standard für lokale Netze im Büro-Umfeld mit Zugang zu ISDN und Internet geworden. Der Datenverkehr in den lokalen Netzen unterscheidet sich wesentlich von dem in Feldbussystemen. Die räumlich eng begrenzten Feldbusse dienen hauptsächlich der zyklischen (wiederholenden) Übertragung von Prozesswerten, um immer deren aktuellen Stand auswerten zu können. Dabei kann die Länge der Datentelegramme als sehr kurz bei AS-i-Bus bis kurz bei PROFIBUS bezeichnet werden. Die in den räumlich ausgedehnteren lokalen Netzen zu übertragenden Datensätze sind dagegen in der Regel umfangreicher und nur einmalig zu übertragen. Ein weiterer wesentlicher Unterschied zwischen den Feldbussystemen und den lokalen Netzen liegt in der zulässigen Übertragungszeit zwischen den Endgeräten. Feldbusse müssen hier die wesentlich schärfere Echtzeitbedingung erfüllen, wenn es z. B. um Steuerungsprozesse schnell laufender Maschinen geht.

Obwohl große Unterschiede zwischen den Feldbussen und lokalen Netzen bestehen, vollzieht sich in der Automatisierungstechnik ein deutlicher Wandel hin zu einer vertikalen Datendurchlässigkeit zwischen Fabrik- und Bürowelt im Sinne einer integrierten Betriebsführung. Damit verbunden ist eine Annäherung beider Systeme bis hin zu einer Systemintegration, wie im nachfolgenden Kapitel 19 bei PROFINET gezeigt wird. Vielfach wird sogar gefordert, die lokalen Netze der Bürowelt so zu erweitern, dass die Feldbusse überflüssig werden.

Aus allem folgt, dass sich eine Ausbildung in Automatisierungstechnik dem Thema Ethernet-TCP/IP stellen muss. Hier zunächst einige wichtige Begriffe in Kurzbeschreibung:

- Lokale Netze (Local Area Network = LAN, Verbund räumlich verteilter Rechner, die untereinander Daten austauschen; Richtwert der räumlichen Ausdehnung: maximal 5 km);
- Ethernet ist die zur Zeit bei lokalen Netzwerken am häufigsten angewandte Übertragungstechnik. Ethernet als Übertragungsmedien verwendet Kupferkabel und Lichtwellenleiter. Ethernet als Übertragungsverfahren beruht auf einem festgelegten Protokoll für den Aufbau der Datentelegramme und der Anwendung eines bestimmten Buszugriffsverfahren, bei dem alle angeschlossenen Teilnehmerstationen gleichberechtigt sind. Zur Unterscheidung erhält jede Netzwerkstation eine weltweit eindeutige Geräteadresse. Zu Ethernet gehören auch Netzwerkkomponenten wie Hubs und Switches für den Zusammenschluss der Geräte zu Subnetzen. Die Ethernetkomponenten wie Kabel, Stecksysteme und Switches müssen den rauerer Betriebsbedingungen in der Fabrik angepasst werden, bei SIMATIC z. B. in der Ausführung *Industrial Ethernet*.
- TCP/IP ist die Bezeichnung eines Netzwerkprotokolls für den Datenaustausch zwischen Rechnern über Netzwerkgrenzen hinaus. Für den Datentransfer werden die Gesamtdaten in Teilmengen zerlegt und in Datenpaketen bestimmter Größe übertragen. Um einen Rechner in den weltweiten Netzwerken gezielt finden zu können, wird ein logisches Adressensystem verwendet. Da die Datenübertragung auch gesichert erfolgen soll, muss ein übergeordnetes Kontrollverfahren gewährleisten, dass beispielsweise auch alle Datenpakete angekommen sind.

- Internet (Gesamtheit aller Netzwerke und Computer, die über TCP/IP-Verbindungen erreichbar sind. Dazu zählen u. a. die firmeninternen Netzwerke, die auch Internettechnologien anwenden und Intranets genannt werden);
- ISDN (Integrated Service Digital Network = Dienste-integrierendes digitales Telekommunikationsnetz für Sprach-, Bild- und Datenübertragung auf einer Leitung, weltweit);

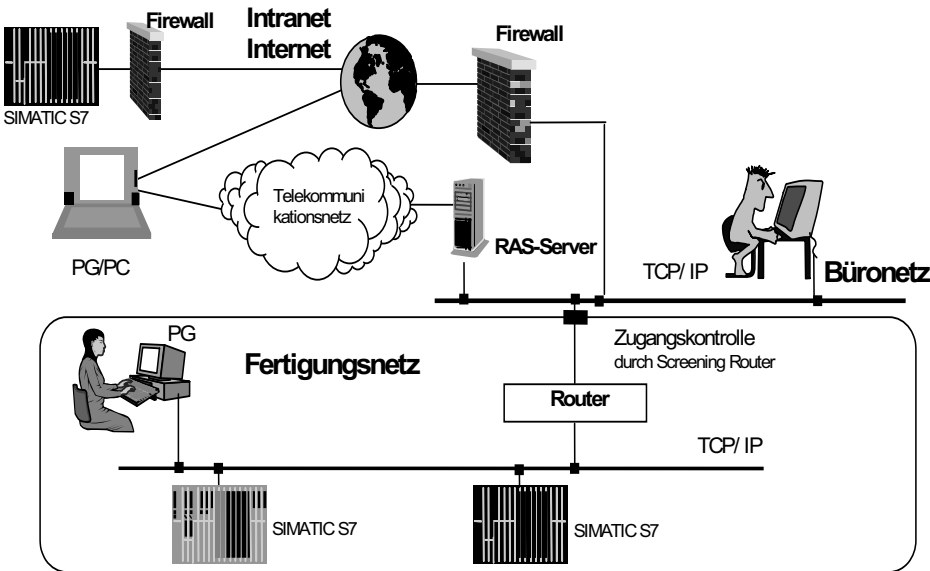


Bild 18.1: Typisches Ethernet-TCP/IP-Netz in der Automatisierungstechnik
(RAS = Remote-Access-Server)

18.1.2 Ethernet-Netzwerke

18.1.2.1 Standard 10 BASE-T

Die Ethernet-Standards unterliegen seit Abfassung des Ursprungsstandards im Jahre 1985 der fortlaufenden technischen Entwicklung. Die Bezeichnungweise folgt einem Schema:

Die erste Zahl gibt die Übertragungsrates in MBit/s (Megabit pro Sekunde) an.

BASE bzw. BROAD steht für Basis- bzw. Breitband.

Die letzte Zahl bzw. Buchstabe steht für die maximale räumliche Ausdehnung pro Segment in Hundert Meter bzw. für eine Kennzeichnung des verwendeten Mediums, z. B.

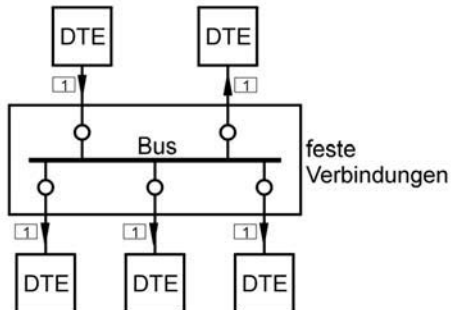
„T“ für Twisted Pair und „F“ für Fiber-Optic (Lichtwellenleiter).

Unter 10Base-T versteht man das Standard-Ethernet-Verfahren mit dem CSMA/CD-Buszugriffsverfahren und einer Übertragungsgeschwindigkeit von 10 MBit/s auf Twisted Pair-Kabeln, bei der die Arbeitsstationen (PCs) so an Verteiler angeschlossen werden, dass eine sternförmige Netzstruktur entsteht (siehe Bild 18.4). Jeder Verteiler kann wiederum Teil einer sternförmigen Oberverteilung sein. Für den Verteiler gibt es zwei verschiedene Konstruktionen, die den internen Datenverkehr regeln:

Hub, auch Sternkoppler genannt, bietet die Möglichkeit, mehrere Teilnehmerstationen sternförmig miteinander zu verbinden. Datenpakete, die auf einem Port empfangen werden, werden ungefiltert an allen anderen Ports verstärkt (regeneriert) ausgegeben.

Switch, vorstellbar als ein äußerst schnell und parallel arbeitendes Datenpaket-Vermittlungssystem, bietet wie schon der Hub die Möglichkeit zur sternförmigen Vernetzung der Teilnehmer. Der Switch „lernt“ die Ethernet-Adressen der angeschlossenen Teilnehmer und leitet ankommende Datenpakete adressorientiert nur an den betreffenden Netzteilnehmer weiter, so dass die anderen Netzwerksegmente mit diesem Datenverkehr nicht belastet werden.

Datenverkehr im Hub-Verteiler



Datenverkehr im Switch-Verteiler

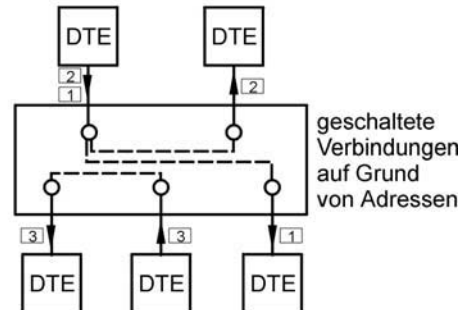


Bild 18.2: Verteilertypen: Hub und Switch

18.1.2.2 Fast Ethernet (100 MBit/s)

Fast Ethernet ist kein neuer Standard sondern nur die kompatible Erweiterung von 10 BASE-T und wird derzeit in der Automatisierungstechnik überwiegend eingesetzt.

Die Bezeichnungen für Fast Ethernet können lauten:

- 100 BASE-TX, d. h. 100 MBit/s über zweipaariges Kategorie-5-Kabel,
- 100 BASE-FX, d. h. 100 MBit/s über Kabel mit zwei optischen Fasern.

Der Standard 100 BASE-TX definiert bestimmte Eigenschaften des Netzwerkes, bestehend aus den aktiven Netzwerkkomponenten und den Kabeln:

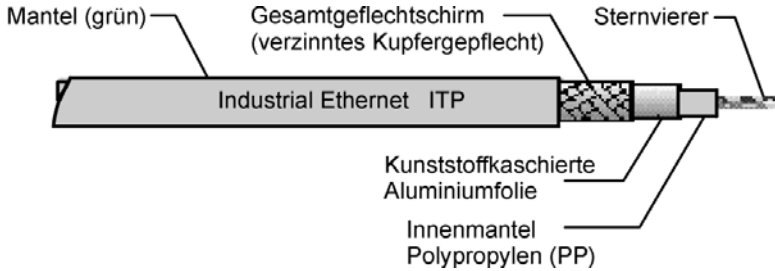
- 100 MBit/s Übertragungsrate,
- Full Duplex Betrieb (FDX), gleichzeitiges Senden und Empfangen
- Stern-Topologie mit Switch-Verteilern,
- Kabellänge 100 m,
- Buszugriffsverfahren CSMA/CD (siehe Kapitel 18.1.4.1),
- RJ 45-Stecker.

18.1.3 Industrielle Installation

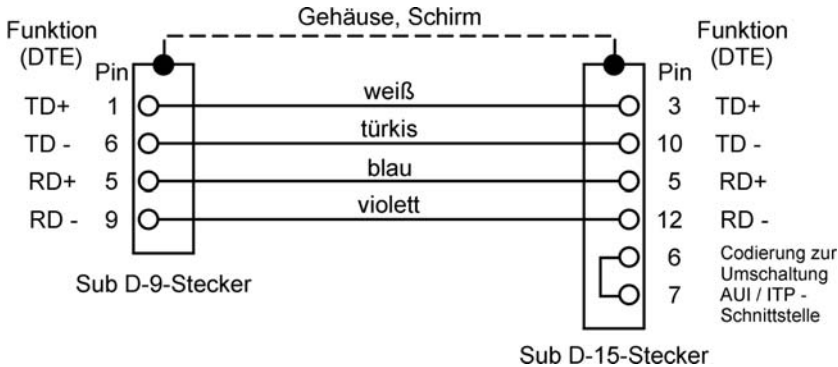
Im Unterschied zum Büro-EDV-Umfeld müssen in der Industrie-Automatisierungs-Umgebung zusätzliche Bedingungen zur Sicherung eines störungsfreien Ethernet-Netzbetriebes vorgesehen werden. Am Beispiel von „Industrial Ethernet“ (Siemens) soll nachfolgend der physikalische Aufbau eines „Industrial-Twisted-Pair-Netzes“ dargestellt werden.

18.1.3.1 Industrial-Twisted-Pair-Leitung ITP

Beim Twisted-Pair-Kabel ist jedes Kupfer-Adernpaar verdreht und einzeln abgeschirmt sowie kunststoffummantelt. Das äußere Schirmgeflecht um 4 Paare besteht aus verzinnnten Kupferdrähten. Das Industrial-Twisted-Pair-Kabel (ITP) für einen sternförmigen Netzaufbau erfüllt die Anforderungen 10BASE-T nach IEEE 802.3-Standard für Frequenzen bis 100 MHz und darf bis zu einer Leitungslänge bis 100 m verlegt werden. Der Wellenwiderstand des ITP-Kabels beträgt 100 Ω.



In konfektionierter Ausführung als Anschlusskabel wird es mit zwei Sub-D-Steckern geliefert. Der 15-polige Stecker kommt an den Industrial-Ethernet-Kommunikationsprozessor der SPS und der 9-polige Stecker zum Electrical Link Modul (ELM), das die Verteilerfunktion ausübt.



18.1.3.2 Strukturierte Verkabelung nach EN 50173

Industrial Ethernet wendet die Vorschriften der *strukturierten Verkabelung* nach EN 50173 an:

- Die Realisierung der hierarchischen Sternstruktur besteht bei einem vollen Ausbau aus drei Verkabelungsbereichen, die in Primärbereich, Sekundärbereich und Tertiärbereich unterschieden werden.
- Die Primärverkabelung, das ist die Verbindung von verschiedenen Gebäuden, beginnt im Standortverteiler (SV) und reicht bis zum Gebäudeverteiler (GV) mit einer maximalen Leitungslänge von 1500 m (vorzugsweise Lichtwellenleiter LWL mit Potenzialtrennung).
- Die Gebäudeverteiler sind das Bindeglied zwischen Primär- und Sekundärbereich, in denen sich die Etagenverteiler (EV) befinden mit einem Abstand von maximal 500 m (vorzugsweise Lichtwellenleiter LWL).

Der Tertiärbereich liegt zwischen den Etagenverteilern und den Endgeräte-Anschlussdosen (TA). Die Gesamtlänge einer Leitung im Tertiärbereich beträgt maximal 100 m (Twisted Pair-Kabel oder Lichtwellenleiter LWL). Optional kann den TAs ein Kabelverzweiger (KV) vorge-schaltet werden, der mehrpaarige Leitungen bzw. mehrfaserige LWL verzweigt und auf Anschlussdosen führt.

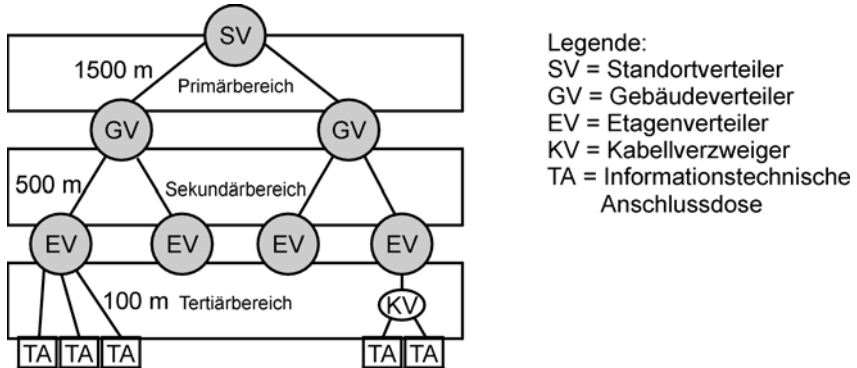


Bild 18.3: Hierarchische Sternstruktur nach EN 50173

18.1.3.3 Sterntopologie

Bei Industrial Ethernet werden einfache Netze mit den Verteilerkomponenten ELM (Electrical Link Modul) aufgebaut, die auch als Sternverteiler bezeichnet werden und bessere Hubs sind.

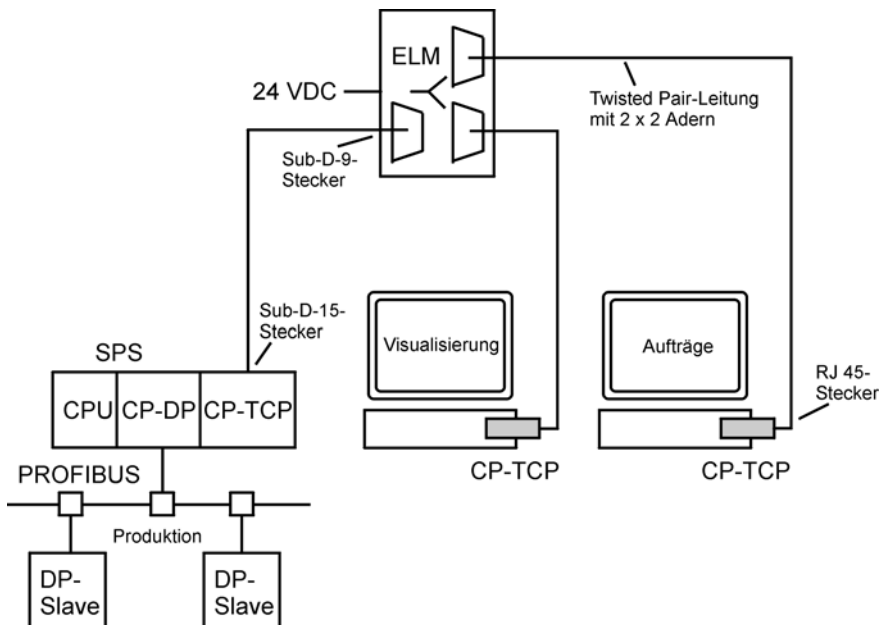


Bild 18.4: Einfaches sternförmiges Ethernet-Netz in der Automatisierungstechnik

18.1.3.4 Linientopologie

In der Automatisierungstechnik kann mit den Link Modulen (ELM, OLM) auch eine linienförmige Netztopologie größerer Ausdehnung realisiert werden, z. B. in Tunnelanlagen. Man koppelt die Link Module zu einer Linienstruktur zusammen. Der maximale Abstand zweier ELMs darf nur 100 m, der Abstand bei den OLMs (Optical Link Modul) kann 2600 m betragen (abhängig von LWL-Typ).

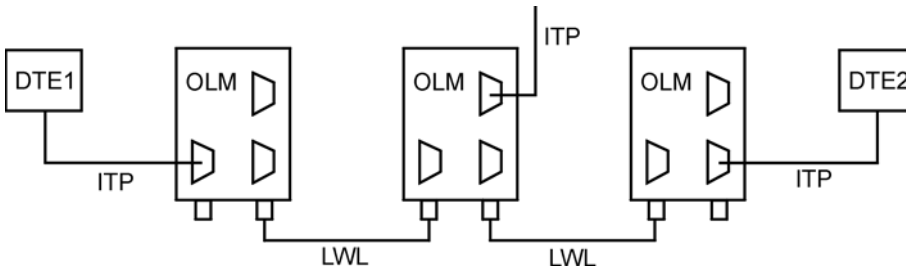


Bild 18.5: Linienförmiges Netz in der Automatisierungstechnik

18.1.4 Datenübertragung über Ethernet

18.1.4.1 Buszugriffsverfahren

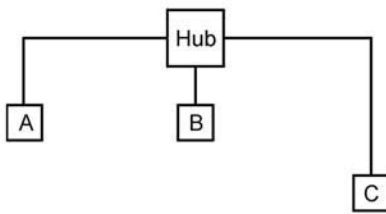
Im (Industrial) Ethernet Netz gibt es keine Master- bzw. Slave-Stationen sondern alle Teilnehmer haben das Buszugriffsrecht. Der Buszugriff muss aber geregelt sein; es wird das *CSMA/CD-Verfahren* angewendet (Carrier Sense with Multiple Access and Collision Detection = Mehrfachzugriff mit Signalabtastung und Kollisionserkennung). Das Verfahren sieht für jede sendewillige Station folgende Prinzipien vor:

- Listen bevor Talking: Vor dem Senden überprüft jede Station, ob die Leitung frei ist, oder ob gerade eine andere Station sendet. Ist die Leitung frei, kann die Station sofort senden. Bei belegter Leitung muss später ein neuer Sendeversuch gestartet werden.
- Listen while Talking: Die Sendestation hört die Leitung ab. Dies ist aus technischen Gründen nur bei einer kabelgebundenen Übertragungstechniken möglich.
- Abbruch der Sendung bei Datenkollision: Tritt der Fall ein, dass zwei Stationen gleichzeitig senden wollen, die Leitung als frei erkennen und unabhängig von einander mit dem Senden beginnen, kommt es zu einer Überlagerung der Signalverläufe und dabei zu einer Zerstörung der Daten. Man bezeichnet dieses Geschehen als eine Kollision. Die nach dem CSMA/CD-Verfahren arbeitenden Sender erkennen den Fehler, da sie etwas anderes hören als sie selber senden und brechen ihre Sendungen ab. Nach einer stochastisch (zufällig) bestimmten Wartezeit versucht jeder Sender einen erneuten Buszugriff zur Wiederholung.

Um die ordnungsgemäße Funktion des Buszugriffsverfahrens bei CSMS/CD sicherzustellen, ist die Ausdehnung eines Ethernet-Netzes durch zwei Einflüsse begrenzt:

- Durch die Leitungsdämpfung (das Kollisionssignal muss noch erkennbar sein).
- Durch das Signallaufzeitenproblem, das in Bild 18.6 vereinfacht dargestellt wird.

Die maximale Netzausdehnung wird eine *Kollisionsdomäne* genannt, sie beträgt 512 Bitzeiten, das sind $51,2 \mu\text{s}$ ($\hat{=}$ ca. 4000 m) bei 10 MBit/s oder $5,12 \mu\text{s}$ ($\hat{=}$ ca. 400 m) bei 100 MBit/s.



1. Station A sendet Daten zur Station B.
2. Station C hat auf Grund der Signallaufzeit noch nicht erkannt, dass die Leitung belegt ist, und beginnt ebenfalls zu senden.
3. Im ungünstigsten Fall empfängt Station B gestörte, unbrauchbare Daten und Station A hat die Sendung bereits beendet, bevor sie bemerken kann, dass eine Datenkollision stattgefunden hat und eine Wiederholungssendung aus ihrer Sicht nicht notwendig ist.

Bild 18.6: Zum Begriff der Kollisionsdomäne

Zur sternförmigen Verbindung von Netzteilnehmern wurden bisher meistens Hubs (Industrial Ethernet ELMs bzw. OLMs) mit Signalregenerierung verwendet, die als Verteilstationen arbeiten (siehe Bild 18.2). Bei dieser Technologie müssen sich die Teilnehmerstationen das Netzwerk zur Benutzung teilen, woraus sich die Bezeichnung *Shared LAN* (to share = teilen) herleitet.

Kennzeichen von Shared LANs sind:

- Die von einer Verteilstation empfangenen Datenpakete werden allen Teilnehmern einer Kollisionsdomäne zugestellt. Alle Datenpakete gehen durch alle Segmente (Punkt-zu-Punkt-Verbindung zwischen Teilnehmerstation und Verteiler), es besteht Kollisionsgefahr.
- Zu einem Zeitpunkt darf nur ein Datenpaket im Netz bleiben.
- Alle Netzteilnehmer teilen sich die Netzressourcen, d. h. die nominale Datenrate.
- Die räumliche Ausdehnung eines shared LANs ist begrenzt durch die Signallaufzeit in den Kabeln und den zusätzlichen Signalverzögerungen in den Hubs oder Repeatern (Verstärker und Koppler von Ethernet Segmenten, die auch aus verschiedenen Kabeltypen bestehen können). Die Signalverzögerungen in den Netzwerkkomponenten werden nicht in Zeitwerten sondern in Längen angegeben (so genannte Laufzeitäquivalente). Die Summe aller Laufzeitäquivalente einer Punkt-zu-Punkt-Verbindung zwischen den am weitesten von einander entfernten Teilnehmern muss von dem zur Verfügung stehenden Gesamtbudget abgezogen werden. Der Rest steht für die Verkabelung der Komponenten zur Verfügung.

Eine entscheidende Vereinfachung und Verbesserung beim Aufbau der Netzwerke bringt die Einführung der *Switching-Technologie*. Ein Switch ist eine Verteilstation, mit der sich Datenpakete anhand von Adressen gezielt durchschalten lassen. Dabei kann ein Switch mehrere Paare von Teilnehmern gleichzeitig verbinden (siehe Bild 18.2) und für den Fall, dass eine Zieladresse gerade besetzt ist, auch kurze Zwischenspeicherungen der Datenpakete vornehmen.

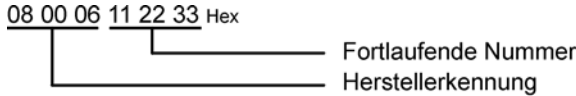
Kennzeichen von *Switched LANs* sind:

- Jedem einzelnen Segment steht die nominale Datenrate zur Verfügung.
- Es ist gleichzeitiger Datenverkehr in mehreren Segmenten möglich ohne Kollisionsgefahr.
- Nur die Daten für Endgeräte in anderen Subnetzen werden dorthin durchgeleitet, dadurch bleibt lokaler Datenverkehr lokal begrenzt und damit auch die Fehlerausbreitung.
- Bei Industrial Ethernet kommen ESM (Electrical Switching Modul) und OSM (Optical Switching Modul) zu Einsatz.

18.1.4.2 Aufbau einer Ethernet-Nachricht

Jede Ethernet-Netzwerkkarte in einem PC bzw. Ethernet-CP in einer SPS hat eine weltweit eindeutige „physikalische Adresse“, die im ROM-Speicher fest abgelegt ist und die MAC-Adresse (Media Access Control) genannt wird. Netzwerkkarten können nur über ihre MAC-Adresse angesprochen werden, diese ist 6 Bytes lang und nach einem festgelegten Schema aufgebaut, wie nachfolgendes Beispiel zeigt:

MAC-Adressenformat nach IEEE 802.1:



Unter der Adresse FF FF FF FF FF FF Hex fühlen sich alle Netzwerkkarten im lokalen Netz angesprochen, sog. MAC-Broadcast-Adresse.

Das nachfolgende Bild zeigt den Aufbau einer Ethernet-Nachricht oder eines Ethernet-Frames (MAC-Datenpaket) mit einer vereinfacht dargestellten Übersicht für den mehrfach untergliederten Daten-Bereich, dessen Einzelheiten erst im folgenden Kapitel erklärt werden.

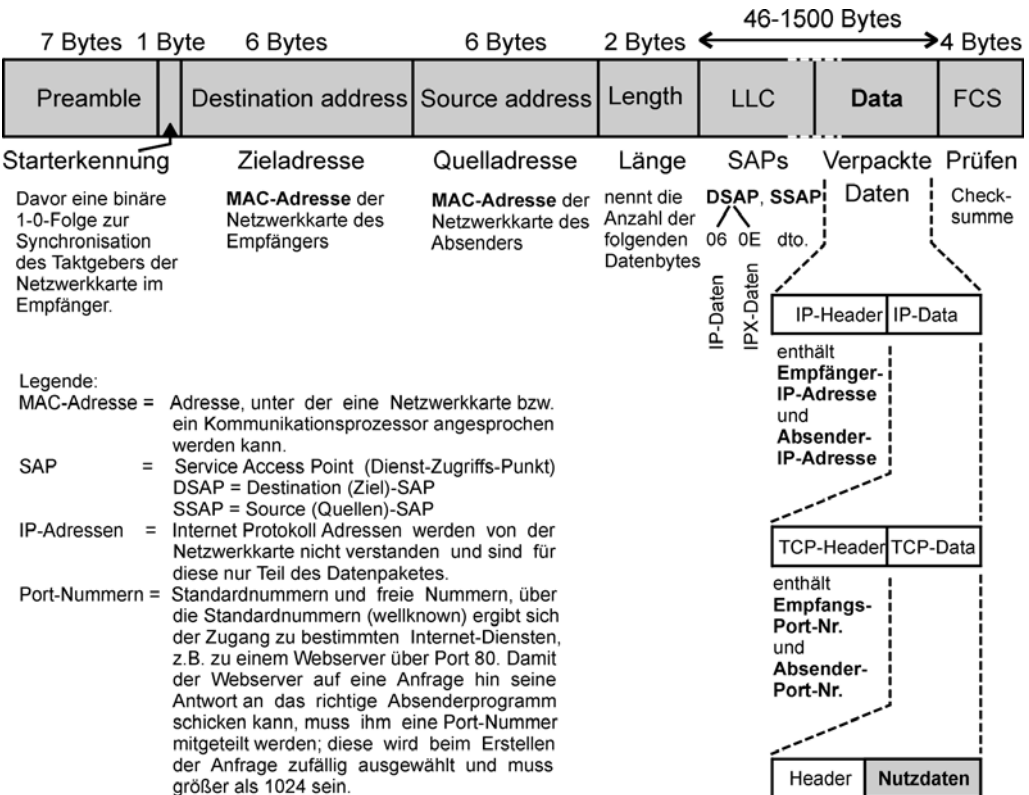


Bild 18.7: Aufbau eines Ethernet-Frames

Damit die Datenpakete ihr Ziel finden, muss die Zieladresse (Destination) angegeben sein. Auch die Absenderadresse (Quelladresse oder Source) wird mitgeliefert, damit der Empfänger weiß, wo er die Antwort hinschicken hat.

Im Telegramm sind auch 2 Bytes zur Längenangabe des folgenden Datenbereiches vorgesehen, d. h., es wird die Anzahl der folgenden Datenbytes angekündigt. Das Datenfeld beginnt mit einer LLC-Typinformation (Logical Link Control). Aus dieser so genannten Frametyp-Information kann die Netzwerkkarten-Treibersoftware entnehmen, wie sie die MAC-Datenpakete richtig weiterzuleiten hat. Bei den Datenpaketen kann es sich nämlich um TCP/IP-Datenpakete (z. B. von einem Kommunikationsserver mit Daten aus dem Internet) oder um SPX/IPX-Datenpakete (z. B. von einem Novell-Fileserver mit Daten aus einer Textdatei) handeln, die von dem auf der Arbeitsstation laufendem Browserprogramm und Textverarbeitungsprogramm quasi-parallel angefordert werden.

Das Datenfeld kann Daten im Umfang von 46 Bytes bis maximal 1500 Bytes enthalten (wenn ein sehr viel größeres Datenpaket zu übertragen ist, z. B. eine große Datei, dann wird vom System eine Segmentierung vorgenommen mit Nummerierung der Einzeldatenpakete und Setzen eines bestimmten Bits, aus dem die Zielstation erkennen kann, ob alle Segmente angekommen sind). Die vorgeschriebene Mindestdatenmenge hängt mit der Kollisionserkennung zusammen. Bei kürzeren Telegrammen müssten die Kollisionsdomänen entsprechend verringert werden. Liegen keine echten Daten von 46 Bytes vor, werden Füllbytes übertragen.

Zum Abschluss des Datenpaketes werden 4 Bytes CRC-Checksumme angehängt (Cyclic Redundancy Check), die es dem auf der Netzwerkkarte befindlichen Spezialprozessor nach einem festgelegten Rechenverfahren ermöglicht, in begrenztem Umfang Übertragungsfehler zu erkennen und zu korrigieren oder aber die empfangenen Daten als verfälscht einzustufen und deshalb zu ignorieren (keine Weitergabe). Die Prüfbyte-Information wird auch mit FCS (Frame Check Sequence) oder als Blocksicherung bezeichnet.

Die Datenpakete, die auch *Ethernet-Frames* (engl. frame = Rahmen) genannt werden, beginnen mit einer Starterkennung von 8 Bytes Umfang, die im wesentlichen der Synchronisation (Gleichlauf) der Netzwerkkartenoszillatoren dienen.

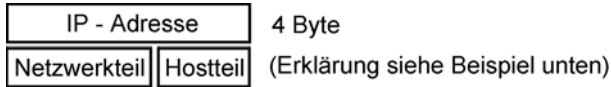
18.1.5 Internet Protokoll (IP)

18.1.5.1 IP-Adressen

Aus den MAC-Adressen der Ethernetkarten kann man kein weltweites Adressierungssystem herleiten, da diese Kartenadressen je nach Hersteller und Kaufdatum zufällig verteilt sind. Das ist eine Festlegung, die man nicht mehr abändern kann oder will. Auch der einfache Austausch einer Netzwerkkarte würde zu einer Adressenänderung führen. Man ist daher gezwungen, ein System übergeordneter *logischer Adressen* der so genannten *IP-Adressen* (Internet Protokoll Adressen) einzuführen. Diese bestehen beim Internet Protokoll Version 4 (IPv4) aus 4 Bytes, die meist als vierstellige Dezimalzahlen (0 ... 255) dargestellt werden und durch Punkte getrennt sind. Offizielle, d. h. weltweit gültige IP-Adressen werden nur von so genannten Providern fest oder auch nur dynamisch (für die Zeit einer Datenübertragung) vergeben. In privaten IP-Netzen, z. B. innerhalb des Intranets einer Firma, ist die Zuweisung von IP-Adressen für die Computer völlig frei.

Die Internetadresse unterteilt sich in die Net-ID und Host-ID, wobei die Net-ID zur Adressierung des Netzes und die Host-ID zur Adressierung des Netzteilnehmers innerhalb eines Netzes dient.

Alle Rechner, die an einem gemeinsamen Ethernet-Segment angeschlossen sind, müssen eine gemeinsame IP-Adresse haben, deren Netzwerkteil gleich ist. Der Benutzerteil oder Hostteil der IP-Adresse kann zum Durchnummerieren der Rechner innerhalb des Ethernet-Segments verwendet werden.



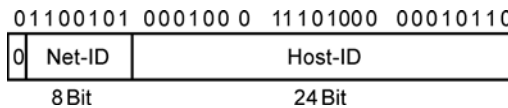
Bei der Adressierung von Netzen unterscheidet man drei Netzwerkklassen:

Class A: wenige Netze mit vielen Teilnehmern

Das erste Byte der IP-Adresse dient der Adressierung des Netzes, die folgenden drei Byte adressieren den Netzteilnehmer.

IP-Adresse: z. B.: 101.16.232.22

Subnetzmaske: 255.0.0.0

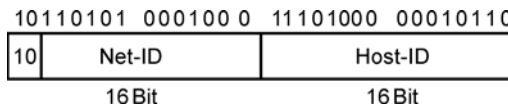


Class B:

Die beiden ersten Byte der IP-Adresse dienen der Adressierung des Netzes und die beiden folgenden Byte adressieren den Netzteilnehmer.

IP-Adresse: z. B.: 181.16.232.22

Subnetzmaske: 255.255.0.0

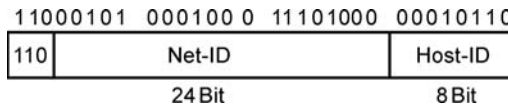


Class C: viele Netze mit wenigen Teilnehmern

Die ersten drei Byte der IP-Adresse dienen der Adressierung des Netzes und das letzte Byte adressiert den Netzteilnehmer.

IP-Adresse: z. B.: 197.16.232.22

Subnetzmaske: 255.255.255.0



Es gibt besondere IP-Adressen für nur internen und nicht weltweiten Gebrauch. Datenpakete mit diesen IP-Adressen werden von den Routern nicht weiter geleitet.

Class A: 10.x.x.x

Class B: 172.16.x.x bis 172.31.x.x

Class C: 192.168.x.x

Für Telegramme, die sich an alle Teilnehmer eines Subnetzes richten sollen, ist die Host-ID mit dem Wert 255 je Byte zu verwenden.

Subnetzmaske: Die Subnetzmaske ist wie die IP-Adresse eine 4 Byte-Zahl, mit der festgelegt wird, welcher Teil der IP-Adresse der Netzwerkteil und welcher der Hostteil ist. Diejenigen Bits, die bei der IP-Adresse den Netzwerkteil kodieren, sind in der Subnetzmaske von links beginnend auf „1“ zu setzen.

Zur Ermittlung der Netzwerkteil-Adresse aus einer IP-Adresse führt der Computer eine UND-Verknüpfung der Binärstellen von IP-Adresse und Subnetzmaske durch. Das Ergebnis der UND-Verknüpfung ist die Netzwerkteil-Adresse.

Beispiel:

Gegeben sind die IP-Adresse eines Rechners (130.80.45.9) und die Subnetzmaske (255.255.255.0). Wie lautet die Subnetz-Adresse des Netzwerkteils, in dem sich der Rechner befindet? Wie viele Rechner könnten sich insgesamt in diesem Subnetz befinden?

Lösung:

IP-Adresse 130.80.45.9 als Dualzahl:	1000 0010. 0101 0000. 0010 1101. 0000 1001
Subnetzmaske 255.255.255.0 als:	1111 1111. 1111 1111. 1111 1111. 0000 0000
UND-Verknüpfung ergibt:	1000 0010. 0101 0000. 0010 1101. 0000 0000
Gesuchte Subnetzadresse:	130. 80. 45. 0

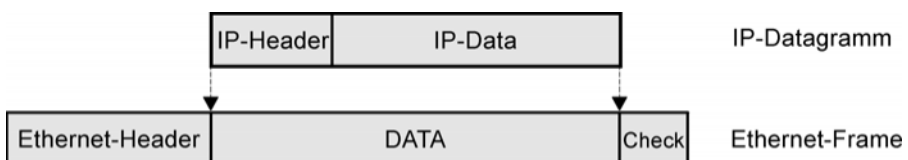
Für die Rechner des Subnetzes stehen die IP-Adressen 130.80.45.1 ... 130.80.45.254 zur Verfügung. Das sind 254 Host-Adressen für mögliche Rechner in Subnetz. Die Adresse 130.80.45.255 ist die IP-Broadcast-Adresse für einen Rundruf an alle Rechner im Subnetz.

18.1.5.2 IP-Datenpakete

Das Internet Protokoll IP spezifiziert den Aufbau von Internet-Datenpaketen, den so genannten Datagramms. Man geht davon aus, dass ein zu übertragender Datensatz sehr groß sein kann und es daher zweckmäßig ist, ihn in abgegrenzte Datenpakete zu zerlegen und diese nacheinander durch das Netzwerk an den Empfänger zu übertragen. Das Internet-Protokoll sieht dafür einen **verbindungslosen Dienst** vor, d. h., es wird kein durchgehender, fester Verbindungsweg geschaltet, über den alle Datenpakete nacheinander übertragen werden könnten. Die Datenpakete können auf unterschiedlichen, möglichst günstigen Wegen an das Ziel befördert werden. Mit dieser Konzeption wird Rücksicht genommen auf die ständig wechselnde Netz-Auslastung.

- Das Internet Protokoll sorgt nur dafür, dass der Weg zum Zielteilnehmer gefunden werden kann. Das Ankommen vollständiger Datenpakete in der richtigen Reihenfolge wird jedoch nicht garantiert. IP bietet nur einen verbindungslosen Dienst, also keinen gesicherten Datentransfer, keine Quittung, kein Fehler-Behebungsverfahren.

Die Bildung der Datenpakete erfolgt nach den Vorschriften des schon erwähnten IP-Standards (IP = Internet Protocol Version 4). Die IP-Datagramme oder IP-Pakete sind aus zwei Teilen zusammen gesetzt, dem Bereich IP-Header und dem Bereich IP-Daten, in dem die zu übertragenden Daten untergebracht sind. Das IP-Datagramm wird zur Übertragung im Ethernet-Netz in ein Ethernet-Frame eingefügt.



Der IP-Header enthält als wichtigste Angaben:

- die IP-Absenderadresse und die IP-Zieladresse, um einen Weg durch das Netz zu finden;
- die Life-Time für das Datagramm im Netz. Diese vom Sender eingetragene Verweilzeit im Netz, wird von jedem Router, den das Datenpaket durchläuft, reduziert. Sobald der Wert = 0 ist, wird das Paket eliminiert. Man verhindert damit, dass eventuelle Irrläufer ewig im Netz herumgeschickt werden und die „Daten-Autobahnen“ verstopfen;
- die Protokoll-Kennung mit der angegeben wird, welches nächst höhere Protokoll im Empfänger das IP-Datagramm weiterverarbeiten soll;
- die Header-Prüfsumme zur Kontrolle, ob der IP-Header korrekt empfangen wurde. Für die eigentlichen Datenbytes verlässt man sich auf die Ethernet-Prüfsumme (CRC).

18.1.5.3 Routing (Wege finden) durch das Netz

Bei der Beschreibung von Kommunikationsvorgängen zwischen Computern, die mit ihrer MAC-Adresse und IP-Adresse in einem komplexen Netz eindeutig identifizierbar sind, ist davon auszugehen, dass kein Teilnehmer Kenntnisse über die Konfiguration des Gesamtsystems haben kann. Zu überlegen ist, welche Bedingungen erfüllt sein müssen, damit trotzdem „Wege durch das Netz“ gefunden werden.

Der physikalische Aufbau von Transportverbindungen zur Übertragung von Daten zwischen den Rechnern A, B und C sieht im allgemeinen Fall so aus, dass sich zwei Rechner innerhalb eines lokalen Netzes befinden (LAN 1) und der dritte Rechner in einem davon getrennten anderen lokalen (entfernten) Netz (LAN n) angeschlossen ist. In den Netzen sind weitere Rechner vorhanden, die im Bild 18.8 aber nicht dargestellt sind.

Die lokalen Netze sind im allgemeinen Fall durch Router an ein globales Netz angeschlossen. Router sind Vermittlungskomponenten im Netz und stellen die Verbindung zwischen Subnetzen her. Dabei leiten sie Daten anhand von Netzwerk-Adressen zu den Empfängern weiter (oder zu anderen Routern auf dem Wege dorthin). Einige Router haben sogar die Aufgabe unterschiedliche Übertragungssysteme zu koppeln, wie z. B. Ethernet-ISDN-Router, die eine Verbindung zwischen einem Ethernet-LAN und dem ISDN-Telefonnetz ermöglichen.

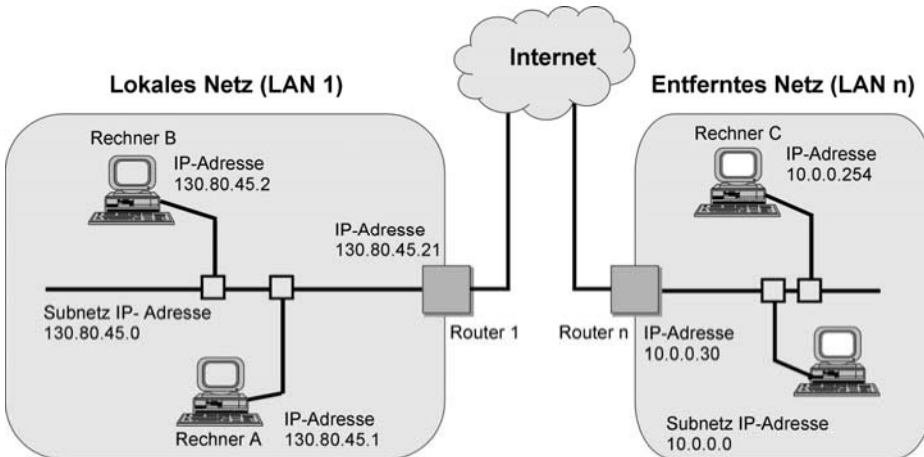


Bild 18.8: Wege finden durch das Netz

Welche Einzelprobleme müssen nun beim „Wege durchschalten“ im Ethernet-IP-System gelöst werden?

- Problem 1: Der sendende Rechner A in LAN 1 (siehe oben Bild) muss wissen, welche Zieladresse er in die Datenpakete (Telegramme) einsetzen muss, damit die Nutzdaten tatsächlich beim richtigen Rechner ankommen. So müssen z. B. Datenpakete an Rechner B, der sich in dem selben LAN befindet wie Rechner A, mit der MAC-Adresse von Rechner B als Zieladresse versehen werden. Dagegen müssen Datenpakete, die für Rechner C bestimmt sind, mit der MAC-Adresse des Routers 1 abgeschickt werden und nicht etwa mit der MAC-Adresse des Rechners C.
- Problem 2: Router 1 muss wissen, an welche anderen Router er die ihm zugestellten Datenpakete für Rechner C weiterreichen könnte und welcher Weg dabei für jedes Datenpaket aktuell der günstigste ist, weil die Wegeauslastung im Netz sich ständig ändert.
- Problem 3: Router n muss wissen, wie er den Endrechner C erreicht, dazu muss er die MAC-Adresse von Rechner C in Erfahrung bringen und als Zieladresse in die Datenpakete einsetzen.

Insgesamt liegt also das Problem vor, wie ein Ethernet-Sender die benötigte MAC-Zieladresse erfährt, und zwar unter der Bedingung einer fehlenden gemeinsamen Verbindungsprojektierung zwischen den Teilnehmern, die es in einem weltweiten und sich ständig ändernden System nicht geben kann. Die Durchführung der nachfolgend beschriebenen Abläufe wird von dem *IP-Standard* (*IP = Internet Protocol Version 4*) auf den Rechnern gesteuert. Als Protokoll wird eine Verfahrensvorschrift für die Übermittlung von Daten verstanden. Standard bedeutet hier so viel wie „praktisch weltweit durchgesetzt“ oder genormt zu sein.

Vor dem Hintergrund des IP-Adressen/Subnetzmasken-Systems und der Tatsache, dass Netzwerkkarten nur die MAC-Adresse erkennen, wird das Problem „Rechner A will Daten an Rechner B schicken“ wie folgt gelöst:

1. Rechner A muss seine eigene IP-Adresse kennen,
2. Rechner A muss die IP-Adresse von Rechner B kennen,
3. Rechner A muss die Subnetzmaske seines eigenen Subnetzes (LAN 1) kennen,
4. Rechner A ermittelt aus seiner IP-Adresse und der Subnetzmaske die Subnetzadresse des Netzes, in dem er sich befindet. Das gleiche Verfahren wendet er auf Rechner B an und stellt fest, dass dieser sich im gleichen Subnetz befindet wie er selbst.
5. Rechner A wendet dann das so genannte Address Resolution Protocol (ARP) an, um die MAC-Adresse von Rechner B zu erfahren. Dazu sendet er einen Rundruf (Broadcast) auf der Ethernet-Ebene an alle Rechner im LAN 1 mit dem sinngemäßen Inhalt: „Ich möchte dem Rechner, dessen IP-Adresse 130.80.45.2 lautet, Daten senden. Dazu brauche ich seine MAC-Adresse, bitte um Antwort.“ Damit alle Netzwerkkarten und damit alle Rechner im LAN 1 den Ruf „hören“, verwendet Rechner A die Ethernet-Broadcastadresse FF FF FF FF FF FF als Zieladresse in seinem Sendetelegramm. Alle Netzwerkkarten haben „mitgehört“ und melden die genannte IP-Adresse an ihren Rechner. Nur der Rechner, dessen IP-Adresse mit der genannten IP-Adresse übereinstimmt, antwortet mit einem ARP-Datenpaket, das die gewünschte MAC-Adresse enthält.
6. Rechner A kann nun sein Datenpaket zusammenstellen, und zwar mit der MAC-Adresse von Rechner B als Zieladresse.

Lösung des Problems „Rechner A will Daten an Rechner C schicken“:

1. Rechner A muss zusätzlich noch die IP-Adresse seines Standard-Gateways kennen.
2. Rechner A führt dieselben Schritte durch wie oben beschrieben und kommt dabei aber zu dem Ergebnis, dass sich Rechner C nicht im gleichen Subnetz befindet wie er selbst. Daraus schließt Rechner A, dass er eine ARP-Rundruf mit der Zieladresse FF FF FF FF FF FF abschicken muss, jedoch mit der IP-Adresse 130.80.45.21 des Routers.
3. Der Router antwortet mit einem ARP-Datenpaket, das seine MAC-Adresse enthält.
4. Rechner A kann nun das Datenpaket an Rechner C zusammenstellen, und zwar mit der IP-Adresse von Rechner C und setzt dabei als Zielfeldadresse im Ethernet-Frame die MAC-Adresse von Router 1 ein.
5. Lösung des Problems „Router 1 muss die von Rechner A erhaltenen Daten weiterleiten“. Hier müssen zwei Fälle unterschieden werden:
6. Wenn es sich bei den Routern um so genannte Ethernet-ISDN-Router handelt, das globale Netz also ein Telefonnetz ist, ruft der Router 1 auf Grund der IP-Subnetzadresse des fernen Netzwerkes die bei der Projektierung eingetragene Telefonnummer von Router n an.
7. Bei einem Routing im Internet muss Router 1 in einer auf IP-Netzadressen beruhenden so genannten Routing-Tabelle nachsehen, ob sich dort eine Adresse findet, an die er das Datenpaket schicken kann. Die Beschaffung und Aktualisierung der Routing-Tabellen ist ein Spezialproblem des Routingverfahrens überhaupt: Die Router erkennen Veränderungen in der Netztopologie und informieren sich untereinander!

Lösung des Problems „Router n muss die MAC-Zieladresse von Rechner C ermitteln“:

1. Router n sendet einen Rundruf (Broadcast) mit der MAC-Adresse FF FF FF FF FF FF an alle Teilnehmer seines Subnetzes unter Angabe der IP-Adresse von Rechner C. Dieser wird seine MAC-Adresse mit einem ARP-Datenpaket zurückschicken.
2. Router n bildet ein Datenpaket mit der MAC-Adresse von Rechner C als Zieladresse.

Die Übertragung der Daten erfolgt in Datenpaketen. Das hat den Vorteil der freien Wegewahl zwischen Sender und Empfänger durch die Router, wie im nachfolgenden Bild gezeigt wird. Man bezeichnet dies als *paketvermittelte Kommunikation* oder *Datagramm-Dienst*.

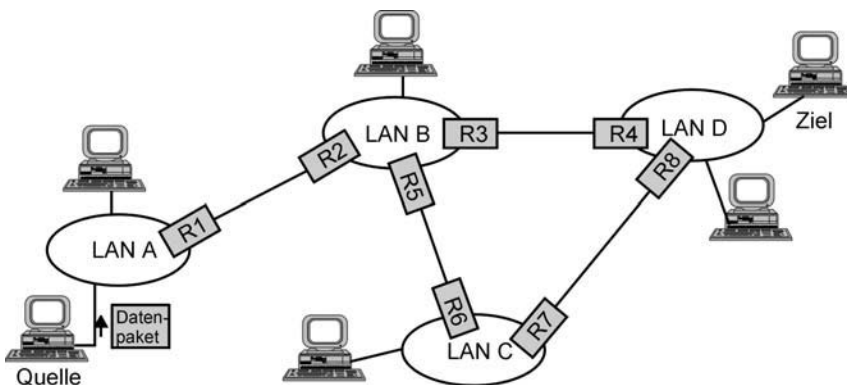


Bild 18.9: Router (R) verbinden LANs untereinander zum Internet. Ob ein entfernter Rechner erreichbar ist, lässt sich mit dem **Ping-Kommando** über Start > Eingabeaufforderung > C:\>ping IP-Adresse prüfen.

18.1.6 Transport-Protokolle (TCP, UDP)

18.1.6.1 Verbindungsorientierter Transportdienst: TCP-Standard

Das angewendete IP-Protokoll garantiert in Zusammenarbeit mit dem Ethernet-Protokoll nur, dass die **tatsächlich** beim Empfänger eingetroffenen IP-Pakete fehlerfrei sind. Nicht sicher ist dagegen, dass alle IP-Pakete auch angekommen sind, denn Router können im Überlastungsfall eintreffende IP-Pakete verwerfen. Das IP-Protokoll hat keine Möglichkeit fehlende IP-Pakete zu entdecken. Ferner bietet das IP-Protokoll auch keine Möglichkeit, die falsche Reihenfolge angekommener Datenpakete zu erkennen. Deshalb ist ein dem Internet Protokoll IP übergeordnetes Transport Protokoll TCP in den Rechnern erforderlich, um die Schwächen des IP-Standards auszugleichen. Dazu soll der übergeordnete TCP-Standard einen **fehlerfreien Softwarekanal** zwischen **zwei Programmen** auf zwei Endrechnern herstellen, der die Übertragungssicherheit einer fest verdrahteten Verbindung aufweist.

Der *TCP-Standard (Transmission Control Protocol)* hat drei Aufgaben zu übernehmen:

1. TCP muss eine Verbindung zwischen dem Datentransportkanal und dem jeweiligen Anwenderprogramm in beiden Rechnern herstellen. Das erfolgt über so genannte Ports.

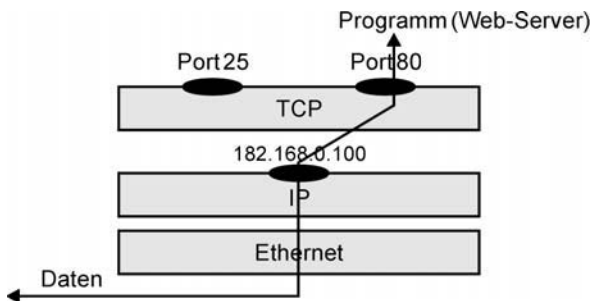


Bild 18.10:
Socket = Port-Nr.+ IP-Adresse

TCP-Ports

TCP stellt die Verbindung eines Anwenderprogramms mit dem Transportkanal über so genannte Ports her. Die Ports sind die Anfangs- und Endpunkte des Kommunikationsweges. Jeder TCP-Kommunikationsteilnehmer ist ein *Endpoint* und wird durch eine besondere Adressangabe gekennzeichnet:

Host-IP-Adresse, Port-Nummer, z. B. 182.168.0.100, 80

Die Host-IP-Adresse steht für den Rechner im Netz. Die Port-Nummer ist die lokal bekannte Adresse für ein bestimmtes Anwenderprogramm, das auf diesem Rechner läuft. Für bekannte Internetprogramme wie HTTP und E-MAIL sind die Port-Nummern standardisiert und als *well known Portnumbers* bekannt. Im SimatcNET-System werden für Automatisierungsprogramme Port-Nummern >2000 verwendet.

Die Kombination von IP-Adresse und Port-Nummer kennzeichnet weltweit eindeutig ein bestimmtes Programm auf einem bestimmten Rechner und wird als Socket (= Stecker) bezeichnet, daher auch der Name „winsock.dll“ für die Windows TCP/IP-Treibersoftware.

Die Inanspruchnahme eines Anwenderprogramms durch ein anderes Programm beruht auf dem *Client-Server-Prinzip*. Der Client (Kunde) ist z. B. ein Browser-Programm. Der Server (Dienstbringer) ist dann ein Web-Server-Programm, das eine Webseite anbietet.

2. Es muss ein bidirektionaler Softwarekanal zwischen den zwei Programmen auf den zwei Rechnern hergestellt werden. Das dazu erforderliche Verfahren nennt man einen **verbindungsorientierten Dienst**. Typisch für einen verbindungsorientierten Dienst ist es, dass vor Beginn der Datübertragung der Softwarekanal zu öffnen ist (Verbindungsaufbau durch „Open“) und am Ende des Datentransfers wieder geschlossen werden muss (Verbindungsabbau durch „Close“). Die Datübertragung selbst erfolgt durch Anwendung von „Send“- und „Receive“-Funktionen.

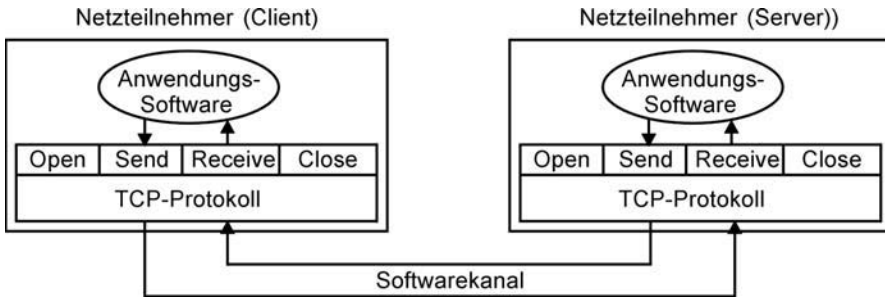


Bild 18.11: Modell einer TCP-Verbindung

3. Zwischen den zwei Programmen muss der bidirektionale **Softwarekanal fehlerfrei** gehalten werden. Als übergeordnete Instanz ist TCP Lieferant bzw. Empfänger von Daten gegenüber IP und beansprucht die Überwachung des Datentransfers. Das schließt ein, dass TCP über Mittel verfügen muss, aufgetretene Fehler zu erkennen und deren Beseitigung veranlassen zu können, z. B.:

- Erkennen von Übertragungsfehlern durch Prüfsummen-Kontrolle,
- Wiederholte Übertragung von Datenblöcken (TCP-Segmenten) im Fehlerfall,
- Automatische Sendewiederholung bei ausbleibender Bestätigung im Zeitfenster,
- Anwendung eines Sequenz-Nummern-Verfahrens auf die Nutzdaten.

TCP-Segmente

Der Aufbau eines TCP-Segments gliedert sich in den TCP-Header und das Nutz-Datensegment. Im TCP-Header sind u. a. die Port-Nummern von Datenquelle und Datenziel untergebracht.

Das nachfolgende Bild zeigt wie im Prinzip die Nutzdatenübertragung bei Ethernet-TCP/IP durch Mehrfachverpackung der Daten gesichert erfolgt. Die Nutzdaten werden beim sendenden Teilnehmer gleichsam in mehrere Briefumschläge gesteckt und beim Empfänger in umgekehrter Reihenfolge wieder geöffnet.

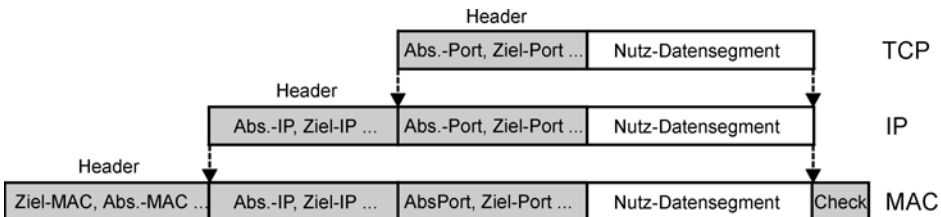


Bild 18.12: Protokollaufbau bei Ethernet-TCP/IP

18.1.6.2 Verbindungsloser Transportdienst: UDP-Standard

Der Transportdienst *UDP (User Datagram Protocol)* bietet an sich nur einen ungesicherten Datagramm-Dienst mit den Port-Nummern, wie bei TCP beschrieben, um die Datenpakete an das richtige Anwenderprogramm weiterzuleiten. Es bleibt dem Anwenderprogramm überlassen, auf Fehler zu reagieren.

Für die Automatisierungstechnik ist UDP trotzdem von Bedeutung, weil dieses einfachere Protokoll schneller ausführbar ist und daher die Echtzeitbedingung im Feldbereich besser erfüllt als TCP. Die dem Anwenderprogramm selbst überlassene Fehlerkorrektur kann entfallen, wenn es sich um eine zyklische Prozessdatenübertragung handelt. Ein fehlerhaft übertragener Prozesswert wird durch den sofort folgenden aktualisierten Prozesswert überschrieben also automatisch korrigiert.

18.1.7 TCP/IP-Kommunikation bei Industrial Ethernet

18.1.7.1 Leistungsmerkmale

Industrial Ethernet (abgekürzt IE) ist die Siemens-Bezeichnung für ein sehr leistungsfähiges offenes industrielles Kommunikationssystem, das oberhalb der Feldbussysteme AS-Interface und Profibus DP positioniert ist. Es ermöglicht die Vernetzung von SPS- und PC-Stationen in einem Automatisierungssystem mit Anbindungsmöglichkeit über Router an übergeordnete Firmennetze (LAN, Intranet) des Bürobereichs.

- Physikalisch ist Industrial Ethernet ein Netz der 100 MBit/s Fast Ethernet und Switching-Technologie in industrieller Ausführung, wie unter 18.1.3 beschrieben.
- Kommunikationstechnisch ist Industrial Ethernet ein Multi-Protokoll-Netz für TCP/IP, ISO, SEND-RECEIVE und S7-FUNKTIONEN.
- Informationstechnisch ist Industrial Ethernet in erster Linie ein Netz zur Übertragung großer Datenmengen und zur Nutzung von Internetdiensten wie HTTP, E-MAIL, FTP.
- Automatisierungstechnisch ist Industrial Ethernet zur Vernetzung verteilter Anlagen mit eigenständig arbeitenden Steuerungen vorgesehen, die von einem übergeordneten Leitsystem koordiniert werden. Nicht geeignet ist Industrial Ethernet für die zyklische Prozess-Datenübertragung im Feldbereich. Hier wird zukünftig das neue Kommunikationssystem PROFINET IO positioniert sein (siehe Kapitel 19), mit dem gleichen Übertragungssystem wie IE.

18.1.7.2 Zugang zu TCP/IP

Für die Kommunikation zwischen zwei Endteilnehmern (SPS- oder PC-Stationen) benötigt man in vereinfachter Betrachtung:

1. Ein Übertragungssystem mit einer vollduplexfähigen Verbindung zwischen den zwei Endteilnehmern, also z. B. Ethernet-TCP/IP. Das Übertragungssystem beginnt und endet in den Kommunikationsbaugruppen des Systemanschlusses (siehe Kapitel 15.3).
2. Kommunikationsdienste, um einen Zugang von den Datenbereichen der CPU (E/A-Prozessabbild, Datenbausteine) zum TCP/IP-Übertragungssystem zu erhalten. Industrial Ethernet verwendet hierzu SEND/RECEIVE-Funktionen aus der Baustein-Bibliothek (AG_SEND, AG_RECV).
3. Eine Verbindungsstelle, in der das TCP/IP-Übertragungssystem mit den Kommunikationsdiensten zusammenkommt. Das ist die Socket-Schnittstelle von Industrial Ethernet.

18.1.7.3 Socket-Schnittstelle

Das Socket-Prinzip (siehe Kapitel 18.1.6.1) kann auch auf eine ausgewählte Industrial Ethernet Verbindung angewendet werden. Die IP-Adresse einer SPS-Station und eine projektierte Portnummer bilden zusammen einen „Socket“, dem die Betriebsart SEND/RECEIVE zugewiesen ist (Default-Einstellung). Die Transport-ID der Verbindung und die Baugruppen-Anfangsadresse sind bei der Programmierung der SEND/RECEIVE-Bausteine zu verwenden, sie stellen den inneren Zusammenhang zwischen dem „Socket“ und der S/R-Schnittstelle im Steuerungsprogramm her.

Die Projektierung der Socket-Schnittstelle verläuft in folgenden Schritten:

- Anlegen einer Kommunikationsverbindung unter Auswahl eines geeigneten Verbindungstyps (siehe Kapitel 18.2.4),
- Adressierung der Verbindungsendpunkte durch deren IP-Adressen und einer übereinstimmenden Port- bzw. TSAP-Nummer,
- Bestätigung der Betriebsart SEND/RECEIVE und Beachtung der vergebenen Transport-ID und Baugruppen-Anfangsadresse für die Baustein-Programmierung. Die Betriebsart SEND/RECEIVE dient der Datenübertragung bei Datenpuffern wie E/A-Prozessabbild oder Datenbausteinen.

18.1.7.4 Verbindungstypen

Unter einer Verbindung (Kommunikationsverbindung) wird bei SimaticNET eine logische Zuordnung zweier Kommunikationspartner zur Ausführung von Kommunikationsdiensten auf der Grundlage eines vorhandenen Subnetzes verstanden.

Verbindungstypen für TCP/IP-Subnetze sind:

- TCP/IP native, das ist Original TCP/IP.
- ISO-on-TCP, das ist Original TCP/IP ergänzt mit RFC 1006 zur Übertragung von Datenblöcken variabler Länge. Anstelle von Port-Nummern sind TSAP-Nummern anzugeben (SAP = Service Access Point, T = TCP-Protokoll), RFC = Request For Comment.
- UDP, das ist Original Datagrammdienst für schnelleren aber ungesicherten Datentransfer, anwendbar bei zyklischer Datenübertragung, bei der eventuelle Fehler sofort wieder überschrieben werden.
- E-MAIL, nur zum Senden von E-Mails mit Prozess-Nachrichten an einen Mail-Server, nicht für Empfang. Das Versenden von E-Mails aus dem Steuerungsprogramm geschieht mit AG_LSEND Baustein und einem Datenbaustein als Datenquelle.

Bei der Projektierung einer Kommunikationsverbindung zwischen zwei Teilnehmern in getrennten Projekten, muss für den fernen Teilnehmer zuerst ein „Stellvertreterobjekt“ angelegt werden (so genannte „Andere Station“ oder PC-Station). Danach ist ein Verbindungstyp auszuwählen und mit den Angaben zur Adressierung der Partnerstation zu ergänzen (IP-Adresse und Port-Nummer bei TCP/IP native bzw. IP-Adresse und TSAP bei ISO-on-TCP). Eine entsprechende Projektierung ist auch bei der Partnerstation durchzuführen und ins jeweilige Zielsystem zu laden. Es besteht dann zwischen den Partnerstationen eine logische (virtuelle) Verbindung, wie in Bild 18.13 eingezeichnet. In Wirklichkeit besteht die Verbindung natürlich über die Protokoll-Ausführung von TCP, IP und Ethernet sowie dem Signaltransport im Übertragungsmedium.

Die Verbindungen bei SimaticNET sind *statisch*, d. h., sie werden beim System-Hochlauf aufgebaut und bleiben dauerhaft bestehen, auch wenn zeitweilig keine Nutzdaten übertragen werden.

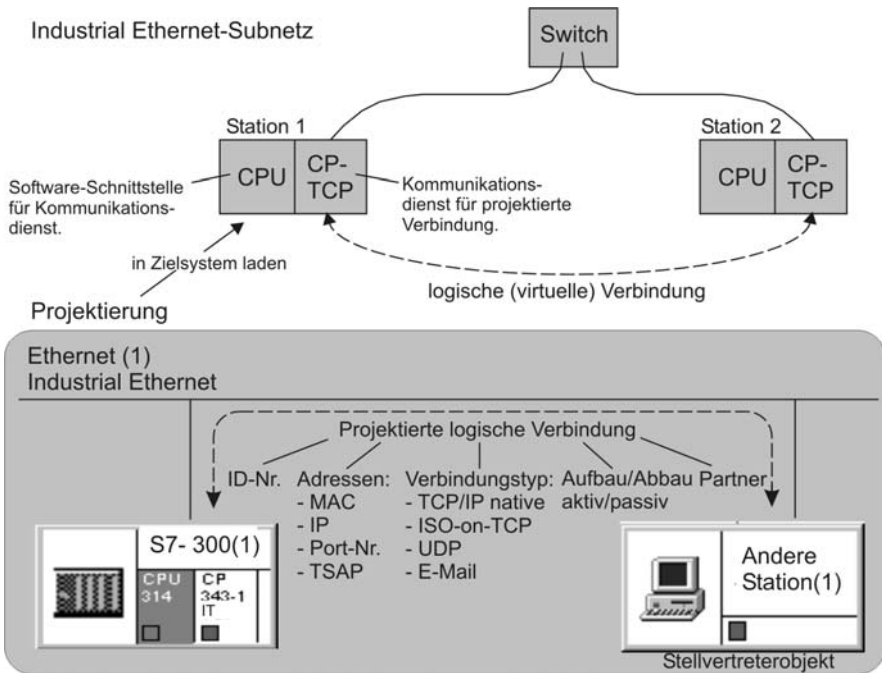


Bild 18.13: Projektieren einer Verbindung für Industrial Ethernet aus Sicht der Station 1

18.1.7.5 SEND-RECEIVE-Schnittstelle

Mit dieser Schnittstelle kann eine CPU-CPU-Verbindung zwischen zwei S7-SPSen zum Zwecke eines Datenaustausches über eine projektierte ISO-on-TCP-Verbindungen bei Industrial Ethernet hergestellt werden.

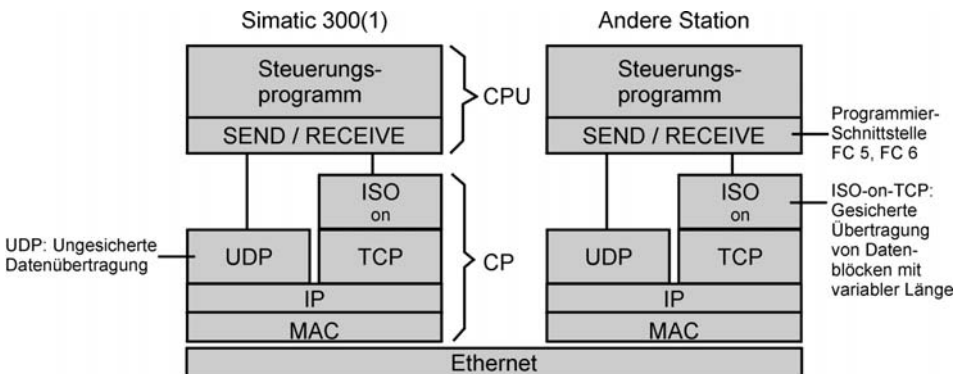
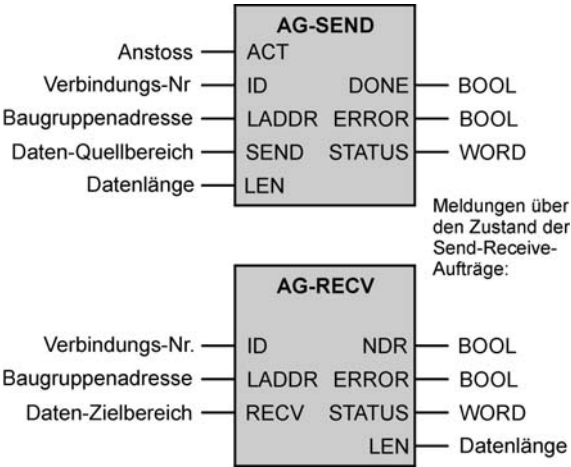


Bild 18.14: Zugang zum Ethernet-TCP/IP-Übertragungssystem über SEND/RECEIVE-Bausteine

Im nachfolgenden Bild werden Hinweise für den Einsatz der SEND/RECEIVE-Bausteine im Steuerungsprogramm gegeben. Als Datenziel- und Daten-Quellbereich kommen das E-A-Prozessabbild, ein Merkerbereich oder ein Datenbausteinbereich der SPS in Frage.



Im Sendebaustein AG-SEND kann mit einem Pointer ein Daten-Quellbereich angegeben werden, aus dem heraus Daten nach einem Auftragsanstoß über eine projektierte und durch ihre ID-Nr. aufgerufene Verbindung an den Sendepuffer des CPs zum Transfer übergeben werden.

Durch zyklische Bausteinaufrufe des AG-RECV kann veranlasst werden, dass über die projektierte und mit ihrer ID-Nr. aufgerufene Verbindung neue Daten aus dem Empfangspuffer des CPs geholt und dem angegebenen Daten-Zielbereich der SPS übergeben werden.

18.1.7.6 Bedeutung der S7-Funktionen im SIMATIC-System

Im gesamten SIMATIC-System gibt es ein durchgängiges Kommunikationsprotokoll, das alle Steuerungskomponenten „verstehen“: die so genannten **S7-Funktionen** als Kommunikationsdienste.

Bei PC-Systemanschlüssen sind die S7-Funktionen in den Kommunikationsbaugruppen bereits integriert oder werden mit der Kommunikations-Software mitgeliefert.

Die S7-Funktionen sind **in allen Subnetz einsetzbar**: MPI, PROFIBUS, Industrial Ethernet, jedoch muss eine logische Verbindung zur Partnerstation projektiert werden.

Die S7-Funktionen sind zwar Siemens-spezifisch, bieten jedoch in den allermeisten Fällen die **einfachste Kommunikationslösung**.

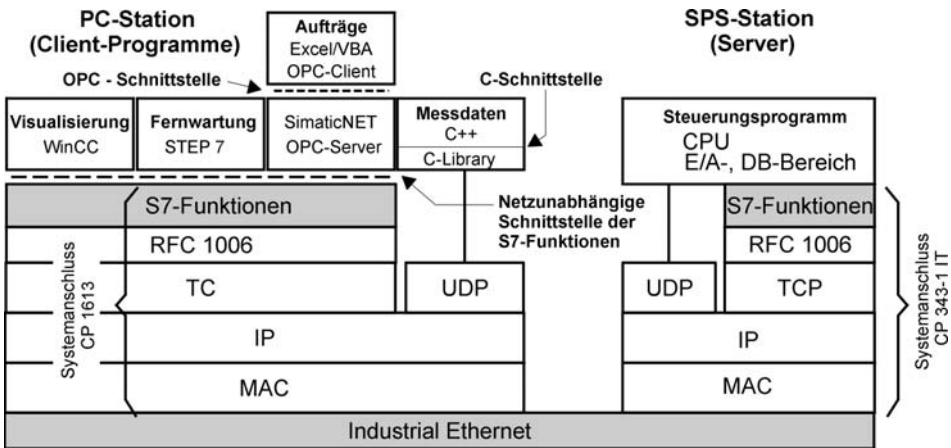


Bild 18.15: Kommunikation zwischen PC-Anwenderprogrammen und S7-SPS über S7-Funktionen. Kommunikationsbaugruppen CP 1613 (PC-Karte mit eigenem Prozessor zur Abarbeitung der Protokolle), Kommunikationsbaugruppe CP 343-1 IT der SPS

18.2 Projektierung Industrial Ethernet

18.2.1 Übersicht

Im Prinzip erfordert die Projektierung eines Industrial Ethernet-Systems mit STEP 7 Arbeitsschritte, die sehr ähnlich sind wie eine Projektierung mit PROFIBUS-DP. Größere Unterschiede bestehen eigentlich nur darin, dass eine Transportverbindung aus mehreren möglichen auszuwählen ist und anstelle von Profibus-Adressen jetzt MAC- und IP-Adressen sowie TSAPs zu verwenden sind.

Arbeitsschritte in der Übersicht:

1. Hardware-Projektierung
 - 1.1 Station 1 mit CPU und CP projektieren
 - 1.2 Netzanschluss für „Andere Station“ einrichten
2. Verbindungsprojektierung zur fernen Station
 - 2.1 ISO-on-TCP-Verbindung auswählen
 - 2.2 Eigenschaften der ISO-on-TCP-Verbindung festlegen
 - 2.3 Kommunikationsdienste Send/Receive auswählen
3. Datenschnittstelle im Anwenderprogramm einrichten
 - 3.1 AG-SEND-, AG_RECV-Bausteine projektieren
 - 3.2 Hinweise zur Inbetriebnahme

18.2.2 Aufgabenstellung: AG-AG-Kopplung in zwei STEP 7 Projekten

Es wird angenommen, dass ein Datenaustausch zwischen zwei selbstständigen Anlageteilen nachträglich eingerichtet werden soll. Jede Anlage verfüge über ein Profibus-Netz. Der Datentransfer soll über ein vorhandenes Ethernet-TC/IP Netz erfolgen. Zu diesem Zweck erhalten die beiden SPS-Stationen einen zusätzlichen Bussystemanschluss für Industrial Ethernet. Eingesetzt werden die Kommunikationsbaugruppen CP 343-1 TCP.

Zur Aufgabenlösung sollen getrennte Projekte angelegt werden, d. h. selbstständige Projekte für die „Station 1“ und für die „Andere Station“.

Die Aufgabenlösung wird nur für ein Projekt und ohne den Profibus-Anteil dargestellt. Zur Versuchsausführung ist auch das zweite Projekt erforderlich, dass sich im Prinzip nur in der überkreuzten Angabe der IP-Adressen vom ersten Projekt unterscheidet.

Technologieschema:

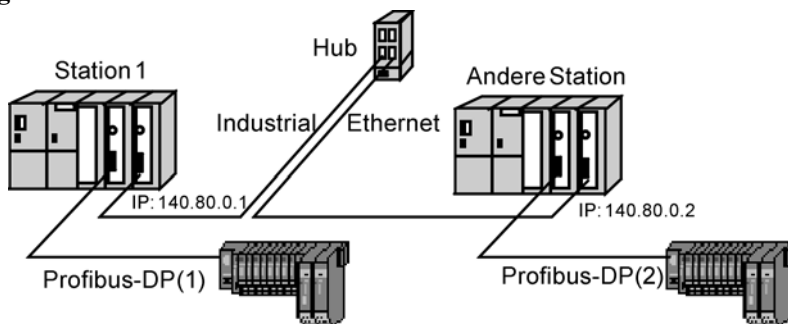


Bild 18.16: Datentransfer zwischen SPS-Stationen über Industrial Ethernet mit SEND-RECEIVE

18.2.3 Arbeitsschritt (1): Hardware-Projektierung

Die Projektierung wird in zwei getrennten Projekten durchgeführt. Es wird nur die Projektierung der Ethernet-TCP/IP-Verbindung beschrieben.

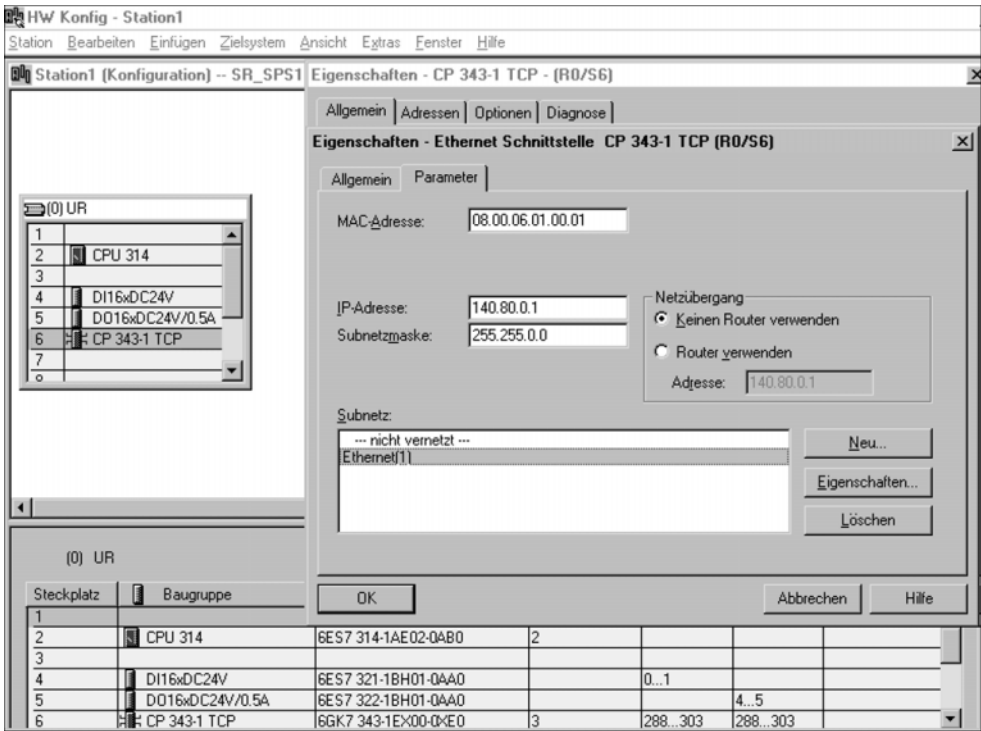
18.2.3.1 Station 1 mit CPU und CP projektieren

- CPU 314

Die S7-Station soll aus einer CPU 314 und 16 Bit zentralen Digitaleingängen sowie 16 Bit zentralen Digitalausgängen bestehen. Es wird eine externe 24 V DC-Stromversorgung eingesetzt, die in der Projektierung nicht erscheint.

- Ethernet-CP 343-1 TCP

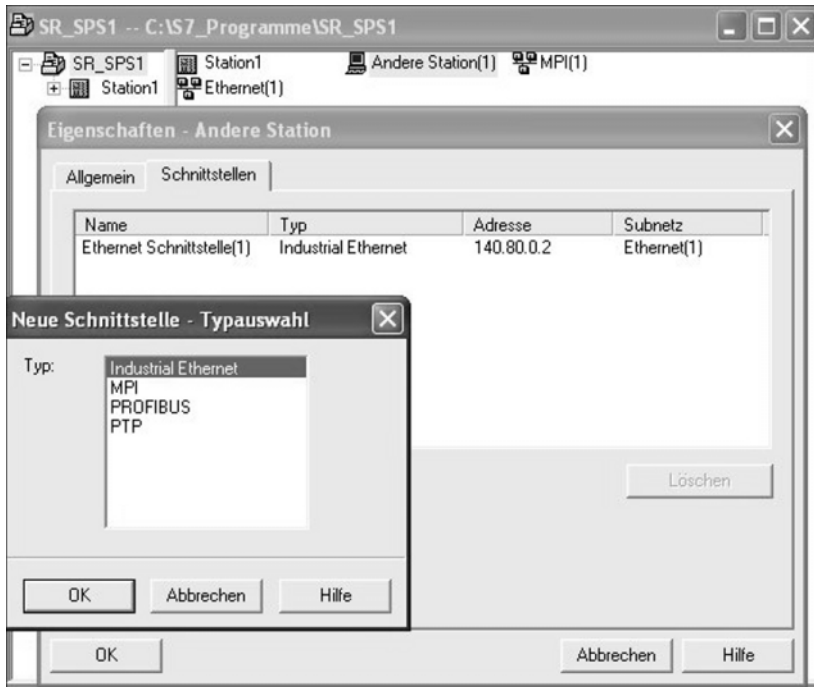
Als Kommunikationsprozessor wird der CP 343-1 TCP verwendet. Zu seinen projektierbaren Objekteigenschaften gehören die 6 Byte-MAC-Adresse und die 4-stellige IP-Adresse.



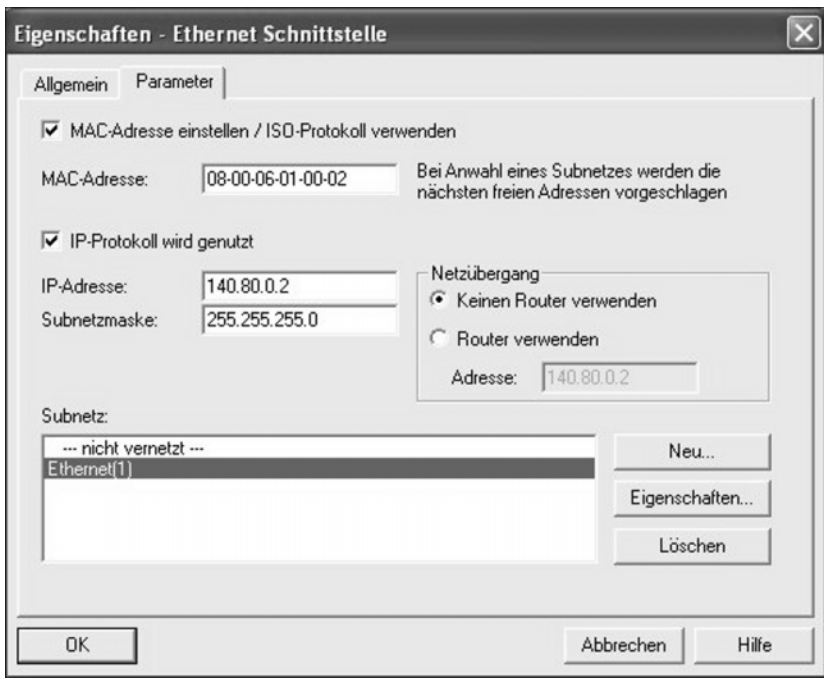
18.2.3.2 Netzanschluss für „Andere Station“

Für die Partnerstation muss in das Projekt ein Stellvertreterobjekt als „Andere Station“ (Station 2) eingefügt und ihre Schnittstelle als IP-Schnittstelle angegeben und bestätigt werden, wie im nachfolgenden Bild gezeigt. Der Eigenschaftsdialog wird dann in einem weiteren Bild fortgeführt. Hier ist die MAC-Adresse der Station 2 einzutragen und anzugeben, ob ein Router im Netzübergang liegt oder nicht. In diesem Dialogfenster muss ferner die IP-Adresse der Station 2 eingegeben werden. Die vorgeschlagene Subnetzmaske kann man bestätigen.

Industrial Ethernet Anschluss für „Andere Station“:



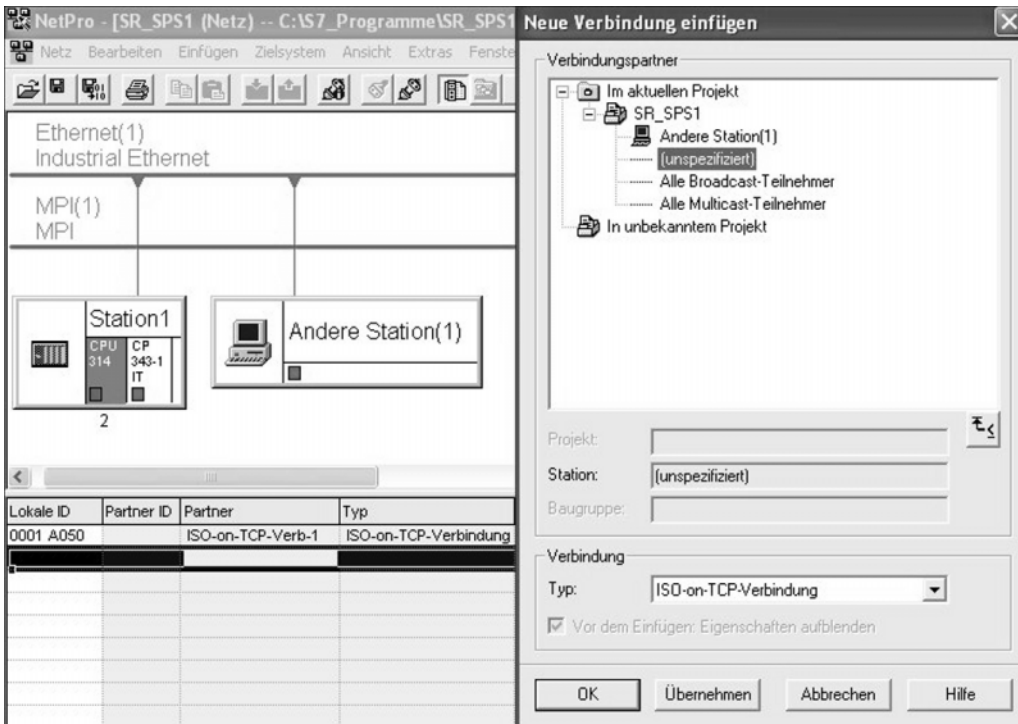
Adressen für „Andere Station“:



18.2.4 Arbeitsschritt (2): Verbindungsprojektierung zur fernen Station

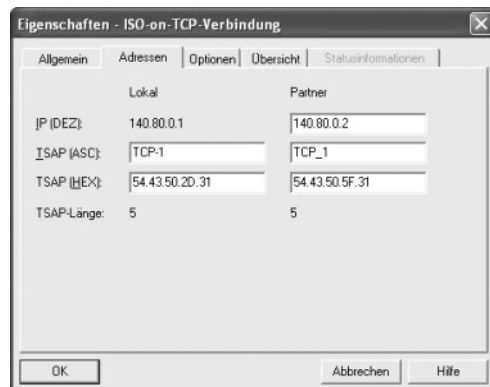
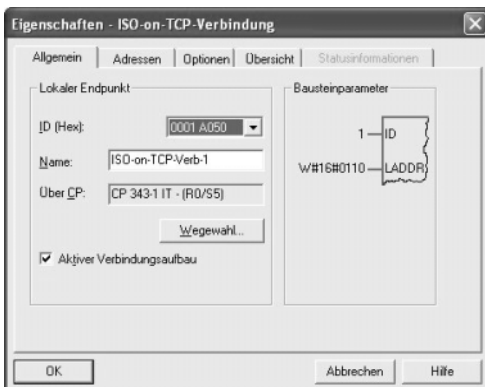
18.2.4.1 ISO-on-TCP-Verbindung auswählen

Der gewählte Verbindungstyp ISO-on-TCP hat dieselben Eigenschaften wie TCP/IP, benutzt jedoch zusätzlich den Standard RFC1006 für eine Datenblockung.



18.2.4.2 Eigenschaften der ISO-on-TCP-Verbindung festlegen

Nach Auswählen des Verbindungstyps ISO-on-TCP öffnet sich ein Eigenschaftsfenster (links), dem nur die beiden Bausteinparameter zu entnehmen sind. Unter Adressen ist die IP-Adresse für die „Andere Station“ einzutragen. Die TSAPs sind die „Port-Nummern“ bei ISO-on-TCP.



18.2.4.3 Kommunikationsdienste Send/Receive anmelden



Es darf nicht übersehen werden, dass Ethernet-TCP/IP nur für die gesicherte Datenübertragung zwischen den beiden Endpunkten eines Kommunikationsweges sorgt. Im Anlagenbeispiel liegen diese Kommunikations-Endpunkte innerhalb der Kommunikationsbaugruppen CP 343-1 TCP der SPS-Stationen. Die zu überragenden Daten selbst befinden sich aber im E/A-Prozessabbild bzw. in Datenbausteinen der jeweiligen CPU. Es muss also noch ein Kommunikationsdienst in Anspruch genommen werden, der die Daten zu TCP/IP bringt oder dort abholt: Send/Receive wird mit FC-Bausteinen im Programm realisiert.

18.2.5 Arbeitsschritt (3): Datenschnittstelle im Anwenderprogramm einrichten

18.2.5.1 AG_SEND-, AG_RECV-Bausteine projektieren

Die Sendedaten stehen im Eingangsbyte EB 1 des AG-SEND bereit. Zur Aufnahme der Empfangsdaten ist bei AG_RECV das Ausgangsbyte AB 5 vorgesehen. Der Sendevorgang wird durch Signal E 0.0 angestoßen. Der Empfangsbaustein ist immer empfangsbereit. **Für den Kommunikationsbetrieb muss die „Andere Station“ entsprechend eingerichtet sein.**

Netzwerk 1: Senden von 1 Byte Daten ab Adressbereich E 1.0

... — EN	
E0.0 — ACT	
1 — ID	
W#16#120 — LADDR	DONE — M100.0
P#E 1.0 BY	ERROR — M100.1
TE 1 — SEND	STATUS — MW102
1 — LEN	ENO —

Netzwerk 2: Empfangsdaten in Adressbereich ab A5.0 ablegen.

... — EN	NDR — M100.2
1 — ID	ERROR — M100.3
W#16#120 — LADDR	STATUS — MW104
P#A 5.0 BY	LEN — MW106
TE 1 — RECV	ENO —

Programmelemente

- GRAPH7
- Standard Library
- Welle
- SIMATIC_NET_CP
 - CP 300 V51
 - FB2 IDENT
 - FB3 READ
 - FB4 REPORT
 - FB5 STATUS
 - FB6 WRITE
 - FC1 DP_SEND
 - FC2 DP_RECV
 - FC3 DP_DIAG
 - FC4 DP_CTRL
 - FC5 AG_SEND
 - FC6 AG_RECV

AG_RECV / CP_300

18.2.5.2 Hinweise zur Inbetriebnahme

Jede TCP/IP oder ISO-on-TCP-Verbindung stellt einen gesicherten bidirektionalen Softwarekanal bereit, d. h., es muss nur eine Verbindung zwischen den beiden SPS-Stationen vorhanden sein, über die in beiden Richtungen gesendet und empfangen werden kann.

Die Projektierung der „Anderen Station“ in einem eigenen Projekt kann auf dem gleichen PC erfolgen, auf dem sich das Projekt für „Station 1“ befindet. Die Projektierung verläuft in den gleichen Schritten wie bei Station 1.

Die Projektierungen müssen in die SPS-Stationen heruntergeladen werden.

Die Formalparameter der Bausteine haben die in den nachfolgenden Tabellen angegebenen Bedeutungen. Die Überwachungs-Ausgangsparameter DONE, ERROR, STATUS werden hier nicht erläutert und der Einfachheit halber nicht ausgewertet.

Erklärung der Baustein-Eingangs-Parameter:

Tabelle für FC-SEND

INPUT-Parameter	Bedeutung	Datentyp/Wertebereich
ACT	Bei ACT = 1 werden Daten-Byte aus dem unter SEND angegebenen Datenbereich gesendet, und zwar solange in Wiederholung wie ACT = 1 ist. Der Eingang verfügt nicht über eine Flankenauswertung, diese muss im Anwenderprogramm für azyklische Datenübertragung ggf. selbst erzeugt werden.	BOOL // FALSE,TRUE
ID	Nummer der Transportverbindung (Siehe Bild bei TSAPs: Lokale ID war dort 0001 A050.)	INT // 1 bis z. B. 16 je nach CP-Ressourcen
LADDR	Baugruppen-Anfangsadresse	WORD // z. B.: W#16#120
SEND	Angabe von Adresse und Länge des Sende-Datenbereichs	ANY//z. B.: P#A5.0 Byte 1
LEN	Anzahl der Bytes aus dem angegebenen Datenbereich, die gesendet werden sollen	INT // z. B. 1, wenn von den bei SEND angegebenen Bytes nur das 1. Byte gesendet werden soll

Tabelle für FC-RECEIVE (Auszug)

INPUT-Parameter RECV	Angabe von Adresse und Länge des Empfangs-Datenbereichs	ANY//z. B. P#E1.0 Byte 1
Output-Parameter LEN	Anzahl der Bytes, die in den angegebenen Datenbereich übernommen wurden	INT // z. B. in MW106 abgelegt, um ggf. ausgewertet zu werden