Ausbildungsunterlage für die durchgängige Automatisierungslösung Totally Integrated Automation (T I A)

ANHANG V

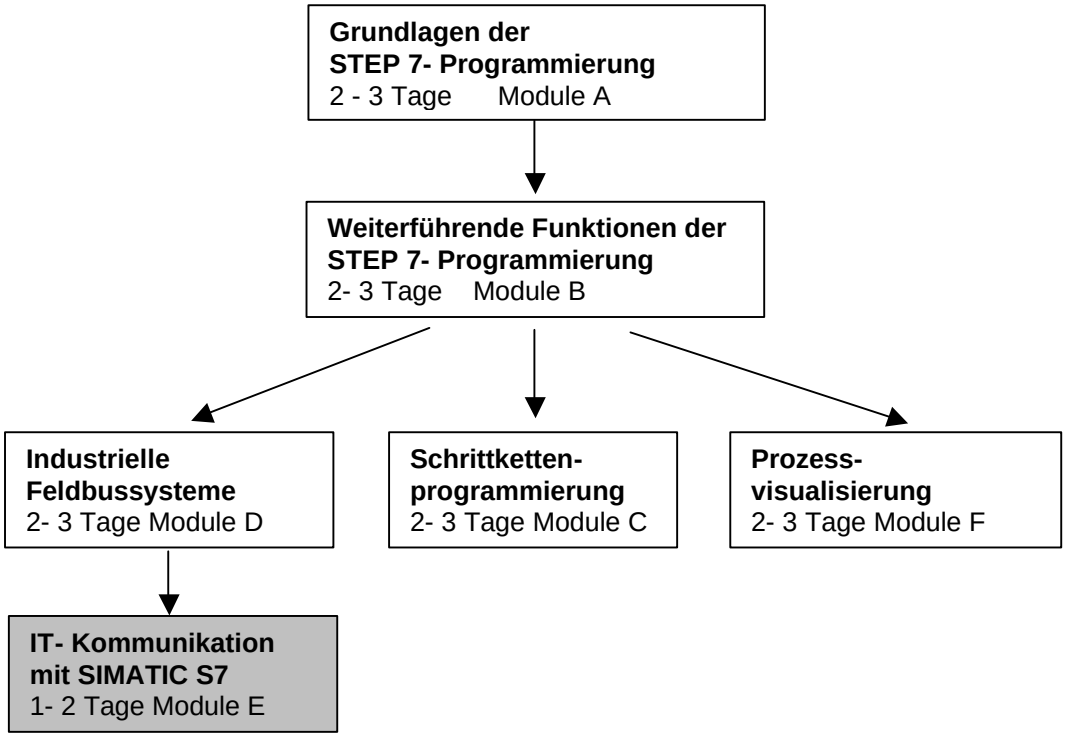
Grundlagen der Netzwerktechnik

Autoren: Fachhochschule Köln - Prof. Dr. Frithjof Klasen,
Dipl.-Ing. Dirk Gebert

SEITE:

1. VORWORT

Anhang V ist die Voraussetzung für die Bearbeitung der Module zum Thema **‚IT-Kommunikation mit SIMATIC S7'**.



Lernziel:

Der Leser erhält mit diesem Anhang eine Einführung in die Ethernet- bzw. Internet-Technologien die für das Verständnis der SCE-Module E benötigt werden.
Dazu gehören unter anderem:

- Kommunikation im Ethernet
- TCP/IP- Protokoll
- Typen von Netzwerkgeräten
- Technologien im World Wide Web

Voraussetzungen:
Da in diesem Anhang die Grundlagen erläutert werden, sind hierfür auch keine speziellen Voraussetzungen erforderlich.

2. EINLEITUNG

Diese Lernmodul dient dazu, die Grundlagen für den Bereich Ethernet und Internet-Technologien zu vermitteln. Dazu wird auf eine Schichten-Aufteilung der Kommunikationsmechanismen zurückgegriffen und anhand dieser die relevanten Technologien erläutert.

Zu Beginn werden zunächst diese Kommunikationsschichten (ISO-OSI-Schichtenmodell) vorgestellt. Anschließend werden auf dieser Basis die Mechanismen und Technologien des Ethernet erläutert und die relevanten Netzwerkkomponenten vorgestellt.

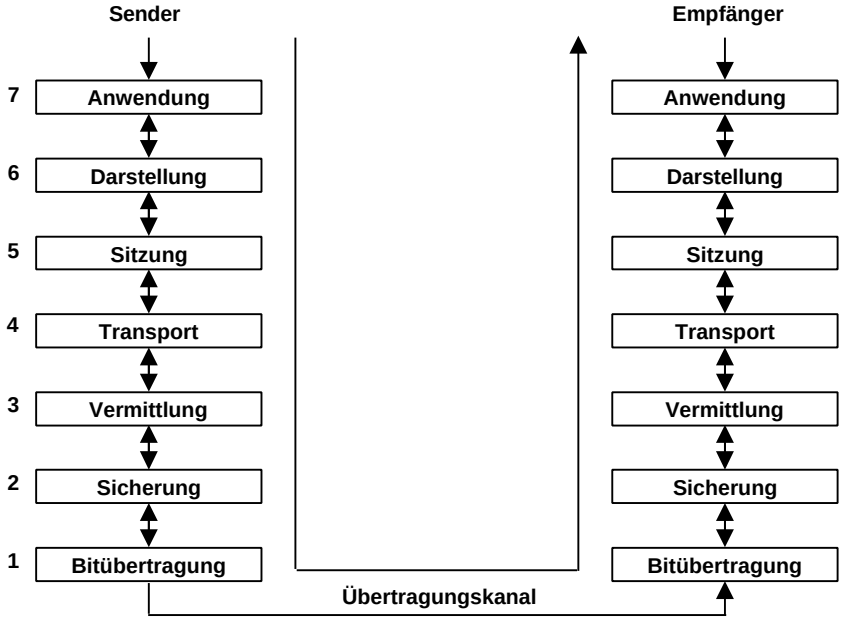
Die nachfolgenden Kapitel befassen sich mit den wichtigsten Mechanismen und Technologien des Internets bzw. Intranets, wie zum Beispiel welche Protokolle verwendet werden oder welche Dienste angeboten werden.

Abschließend werden neben den Kommunikationsmechanismen auch die eigentlichen Inhalte (bzw. deren Technologien), die im Internet Verwendung finden, dargestellt.

3. SCHICHTENMODELL FÜR KOMMUNIKATIONSNETZE

Die Kommunikationsmechanismen zwischen unterschiedlichen Systemen sind in der Regel sehr komplex und unübersichtlich. Daher wurden einzelne logische Bereiche der Kommunikation in überschaubare Teilsysteme aufgeteilt. Diese Aufteilung erfolgte in einzelne hierarchisch angeordnete Schichten mit klar definierten Aufgaben. Dabei stützt sich eine Schicht auf die Funktionalität der jeweils darunter liegenden Schicht.

Die folgende Abbildung stellt das ISO-OSI-Schichtenmodell dar, welches durch die „International Standards Organisation“ definiert wurde. OSI steht dabei für „Open Systems Interconnection”



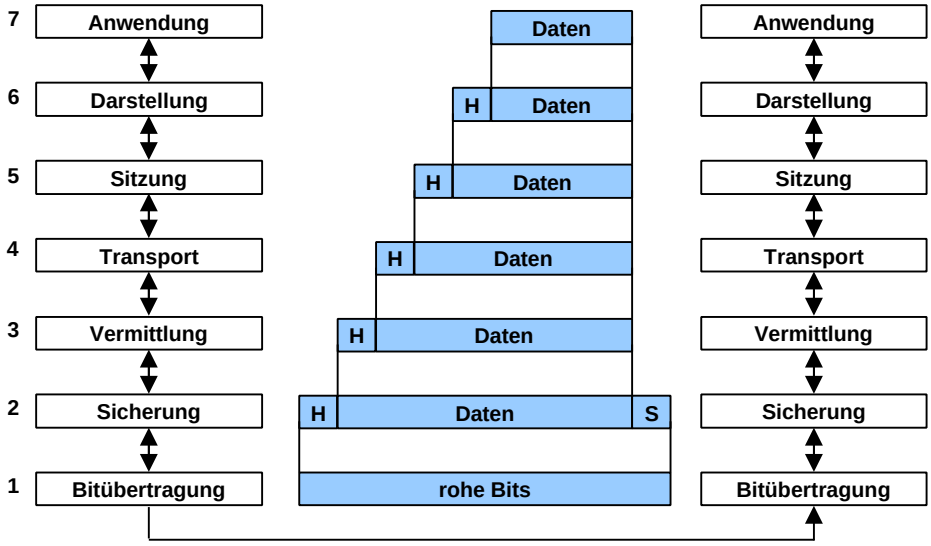
Wie in der Abbildung zu sehen ist, sind die einzelnen Schichten symmetrisch angelegt, d.h. zu jeder Schicht beim Sender gibt es eine korrespondierende Schicht beim Empfänger.

Die einzelnen Schichten bieten dabei die folgende Funktionalität:

- Schicht 1: Bitübertragung (physical layer)
  Diese Schicht dient dazu die rohen Bitdaten der Kommunikation über den entsprechenden Kanal zu übertragen. Dazu werden unter anderem Übertragungsmedien, Signalpegel oder auch Kommunikationsrichtungen festgelegt.
- Schicht 2: Sicherungsschicht (data link layer)
  Diese Schicht bietet Sicherungsmechanismen um fehlerhaft übertragene Daten durch Koderedundanz zu erkennen und entsprechend darauf zu reagieren. Im Fehlerfall könnten beispielsweise die übertragenen Daten erneut angefordert werden.
- Schicht 3: Vermittlungsschicht (network layer)
  Die Aufgabe dieser Schicht ist es, einen Weg vom Ursprungs- zum Bestimmungsort zu ermitteln und auszuwählen.

- Schicht 4: Transportschicht (transport layer)
  In dieser Schicht werden die Daten für die Vermittlungsschicht aufbereitet. Im wesentlichen werden die zu übertragenen Daten in kleine Pakete aufgeteilt bzw. auf der anderen Seite wieder zusammengesetzt.
- Schicht 5: Sitzungsschicht (session layer)
  Diese Schicht stellt gehobenere Dienste für die Datenkommunikation bereit. Dazu zählen zum Beispiel die Zugangsmechanismen oder Zugriffssynchronisation.
- Schicht 6: Darstellungsschicht (presentation layer)
  In dieser Schicht werden die Datenstrukturen entsprechend dem Protokoll oder Zielsystem umgewandelt. Dies können beispielsweise Konvertierungen von Zeichensätzen oder auch kryptographische Verschlüsselungen sein.
- Schicht 7: Anwendungsschicht (application layer)
  Diese Schicht stellt dem Anwender die entsprechende Dienste bereit. Dazu zählen unter anderem Dateiübertragung / -verwaltung oder auch E-Mail. In der Anwendungsschicht wird das eigentliche Ziel des Systems erfüllt.

Die folgende Abbildung zeigt, wie die Daten gemeinsam mit einer Kopfinformation (Header... H) in eine sogenannte Protokoll-Daten-Einheit (Protocol Data Unit...PDU) verpackt werden, um sie der jeweils darunter liegenden Schicht zu übergeben. Der Dateninhalt interessiert dabei die jeweils tiefere Schicht nicht, sondern diese entnimmt ihre Steuerinformation der Kopfinformation. Die Information wird so immer weiter verpackt und auf der Empfängerseite wieder ausgepackt. So kommt jede Schicht wieder zu der für sie bestimmten Kopfinformation. Es ist dann so, als ob die Schichten miteinander kommunizieren würden.



In der Sicherungsschicht wird noch eine Sicherungsinformation, z.B. eine Prüfsumme angehängt, um beim Empfänger eine Prüfung zu ermöglichen, ob die rohen Bits auch richtig über das Kommunikationsmedium übertragen wurden.

In den folgenden Kapiteln werden die jeweiligen Netzwerkgeräte bzw. -protokolle auf das ISO-OSI-Schichtenmodell abgebildet.

4. ETHERNET

Das Ethernet ist eine weit verbreitete, herstellerneutrale Technologie mit der im **L**okal **A**rea **N**etwork (LAN) Daten mit einer Geschwindigkeit von 10, 100 oder 1000 Millionen Bit pro Sekunde (MBps) übertragen werden können.

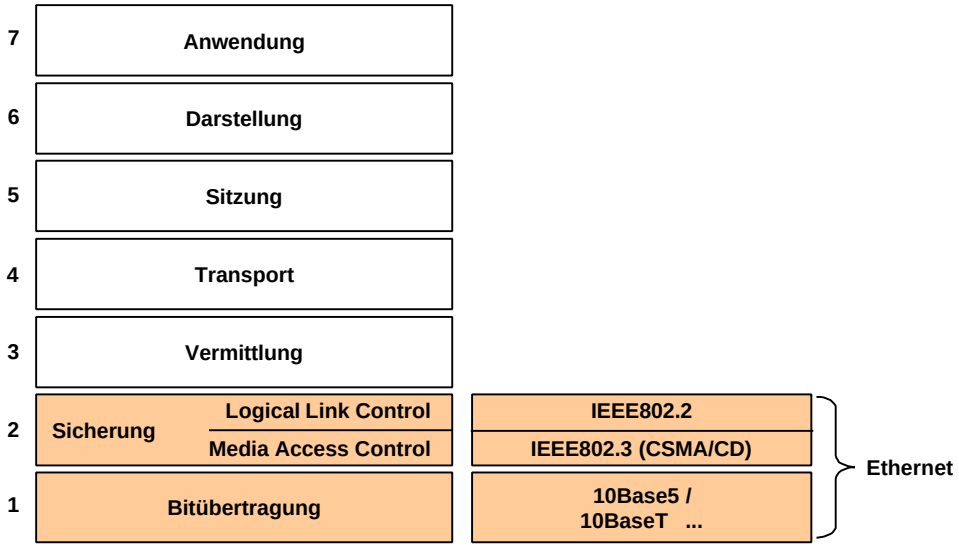
LANs sind in IEEE 802 spezifiziert und unterscheiden sich von anderen Netzwerktypen unter anderem durch:

- die Gesamtlänge der Kabel bzw. die Netzausdehnung (10-1000m),
- die Übertragungstechnik (Koaxialkabel, Twisted Pair und Glasfaser- Kabelsyteme) und
- die Netzwerktopologie (Bus-, Ring-, Stern- und Baumstruktur).

Ethernet ist ein Teil dieser Spezifikation und wird in IEEE 802.3 bzw. für Fast Ethernet in IEEE 802.3u. definiert.

In Bezug auf das ISO-OSI-Schichtenmodell umfasst das Ethernet die Schichten 1 und 2. Dabei wird die Schicht 2 (Sicherungsschicht) in zwei weitere Schichten unterteilt:

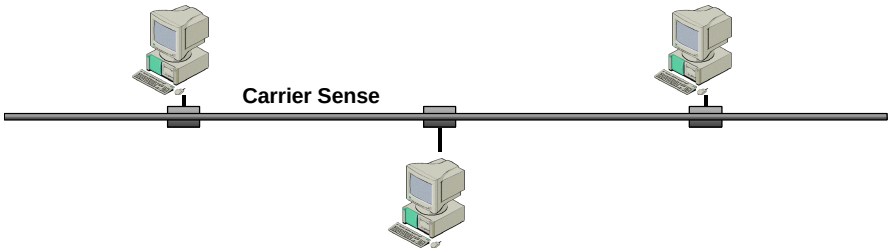
- Zugriffsschicht: Media Access Control MAC
  Die untere Schicht bietet Zugriffsmechanismen für die Bitübertragung. Darin wird koordiniert, wer, zu welchem Zeitpunkt auf die Bitübertragungsschicht zugreifen darf. Dabei kommt beim Ethernet das CSMA/CD-Verfahren zum Einsatz, welches im folgenden Kapitel 4.1 erläutert wird.
- Sicherungsschicht: Logical Link Control LLC
  Die zweite, darüber liegende Sicherungsschicht entspricht der eigentlichen Schicht 2-Funktionalität des ISO-OSI-Modells. Diese dient der Datensicherung durch Prüfsummen. Wie diese Datensicherung aufgebaut ist, ist in Kapitel 4.2 dargestellt.



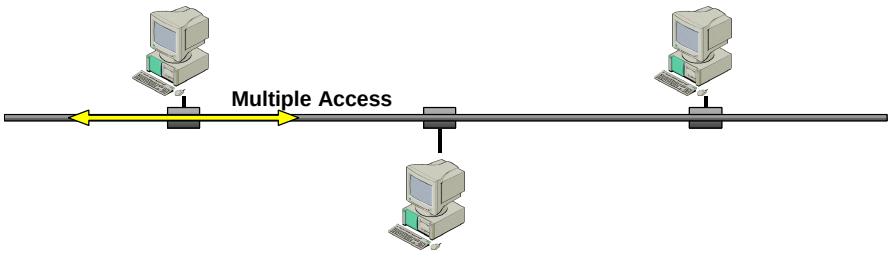
4.1 BUSZUGRIFFSVERFAHREN

Beim Ethernet-Netzwerk gibt es keine Einteilung in Master- bzw. Slave-Stationen, sondern alle Teilnehmer haben das Recht auf den Bus zuzugreifen. Um den Zugriff auf den Bus zu koordinieren, wird das CSMA/CD-Protokoll eingesetzt. (***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess with* ***C****ollision* ***D****etection)*. Dieses Protokoll ist Teil der MAC-Ebene und beschreibt, wann Daten über das Netzwerkinterface auf das Netz gestellt und wie Datenkollisionen auf diesem behandelt werden.

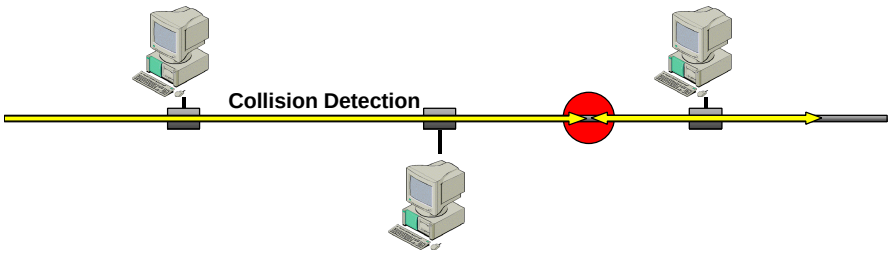
Wenn ein Teilnehmer, der mit dem LAN verbunden ist, etwas senden möchte, wartet er zunächst, bis es auf dem Verbindungsmedium „still“ ist, d.h. keine Daten versendet werden (carrier sense).



Wird festgestellt, dass keine Daten mehr übertragen werden, beginnt der Teilnehmer selbst mit dem Senden seiner Daten. Bei diesem Verfahren kann es jedoch dazu kommen, dass mehrere Teilnehmer gleichzeitig auf eine Pause in der Datenübertragung warten und anschließend in dieser Pause gemeinsam anfangen zu senden (Multiple Access).



Tritt dieser Fall ein, so spricht man von einer Kollision. Die Ethernet-Kommunikation ist so aufgebaut, dass solche Kollisionen erkannt werden.

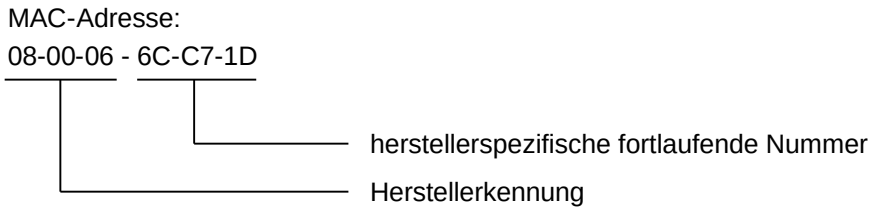


Stellt das CSMA/CD-Protokoll des Netzwerkgeräts eine Kollision fest, so wird die Übertragung abgebrochen und die beschädigten Pakete gelöscht. Nach einer zufällig gewählten Zeitspanne beginnt das Netzwerkgerät den Übertragungszyklus wieder von vorne.

4.2 ETHERNET-PAKETFORMAT

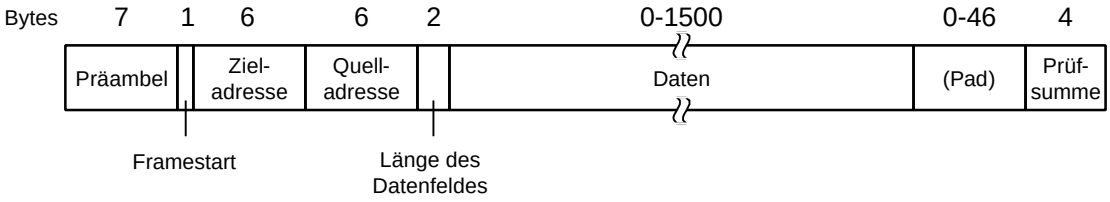
MAC-Adresse

Jede Netzwerkschnittstelle eines Gerätes, das am Ethernet-Netzwerk betrieben wird, wie zum Beispiel Netzwerkkarten im PC oder Ethernet-CP-Baugruppen in einer SPS, haben eine weltweit eindeutige Ethernet-Adresse. Diese Adresse wird im allgemeinen MAC-Adresse (**M**edia **A**ccess **C**ontrol) genannt und dient dazu, die einzelnen Teilnehmer im Ethernet-Netzwerk zu identifizieren bzw. anzusprechen.
Die MAC-Adresse besteht aus insgesamt 6 Bytes, wobei die erste drei Bytes eine Herstellerkennung darstellen. Die letzten drei Bytes kann der jeweilige Hersteller frei vergeben. Allerdings darf jede Adresse nur einmal vergeben werden.



Paketformat

Das Format des Ethernet-Datenpakets ist ein wesentlicher Bestandteil des Ethernet-Standards. Alle Daten, die über das Ethernet-Netzwerk ausgetauscht werden, werden in diesen Paketen übertragen. Von der Funktionsweise her, lässt sich dieses Paket mit einem Brief vergleichen, der zu einer anderen Station übermittelt wird. Dabei werden die eigentlichen Daten (Briefpapier) mit entsprechenden Zusatzinformationen (Briefumschlag) versehen, damit die Daten sicher versendet werden können. Die Aufgaben und Eigenschaften der einzelnen Elemente wird nun im folgenden dargestellt:



Präambel und Framestart

Die Präambel ist eine Folge von 7 Bytes, welche zur Taktsynchronisation der Kommunikationsteilnehmer benötigt werden. Diese stellt mit dem, Framestart-Byte eine Startkennung des Ethernet-Datenpakets dar.

Zieladresse

Dies ist die bereits zuvor beschriebene MAC-Adresse des anzusprechenden Netzwerkgerätes (Empfängeradresse).

Quelladresse

Bei der Quelladresse handelt es um die MAC-Adresse des sendenden Netzwerkgerätes. (Absenderadresse)

Läge des Datenfeldes
Dieses Feld gibt die genaue Länge des Datensegments im Ethernet-Paket an. Die Länge kann zwischen 0 und 1500 Bytes liegen.

Daten und Pad
Dieser Bereich beinhaltet die eigentlichen Daten. Dies sind in der Regel Daten von höheren Protokollen, wie dem Internet Protokoll (IP). Das Datensegment kann eine Größe zwischen 0 und 1500 Bytes besitzen. Um nach dem CSMA/CD-Verfahren die Kollisionserkennung zu gewährleisten, muss ein Ethernet-Datenpaket mindestens 64 Bytes lang sein. Um das zu erreichen, werden dem Pad-Feld so viele Daten hinzugefügt, bis diese Mindetslänge erreicht ist.

Prüfsumme
Dieses Feld beinhaltet eine Prüfsumme über den Datenbereich des Ethernet-Paketes. Sollte ein Fehler in der Übertragung erkannt werden, wird das entsprechende Paket verworfen und nicht an die nächsthöhere Protokollschicht weitergegeben.

4.3 NETZWERKKOMPONENTEN

Ethernetkabel:
Für ein Ethernet-Netzwerk sind unterschiedlichste Kabel- und Steckertypen vorgesehen. Die am häufigsten verwendeten Kabeltypen sind:

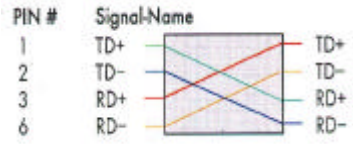
- Koaxialkabel
- Twisted Pair-Kabel
- Glasfaserkabel

Während Koaxialkabel hauptsächlich früher eingesetzt wurden, wird heute hauptsächlich das sogenannte Twisted-Pair-Kabel verwendet. Dieses Kabel besteht aus zwei Kupfer-Adernpaaren, die jeweils miteinander verdrillt sind. Beide Adernpaare werden zusätzlich von einem Schirmgeflecht sowie einer Ummantelung umgeben.

Glasfaserkabel finden hauptsächlich bei längeren Übertragungswegen bzw. höheren Übertragungsgeschwindigkeiten Verwendung.

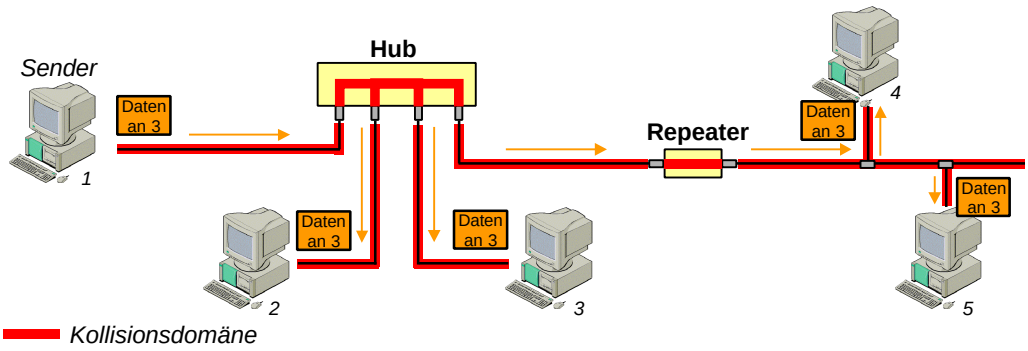
Passend zu den einzelnen Kabeltypen gibt es auch unterschiedliche Steckervarianten. Allerdings sei an dieser Stelle nur der RJ45-Stecker des Twisted-Pair-Kabels dargestellt:

Im Allgemeinen werden TwistedPair-Kabel verwendet, bei denen die einzelnen Adern 1:1 miteinander verbunden sind. Das heißt, die Sende- (TD) und Empfangsadern (RD) sind jeweils mit einander verbunden. Diese Kabel werden dazu verwendet, um Netzwerkteilnehmer wie zum Beispiel PCs oder Ethernet-CPs mit entsprechenden Netzwerkgeräten (siehe nachfolgende Kapitel) zu verbinden.
Sollen jedoch zwei dieser Netzwerkteilnehmer direkt miteinander verbunden werden, z.B. ein PC direkt mit einem Ethernet-CP, so ist ein spezielles Netzwerkkabel erforderlich. Bei diesem sogenannten Crossover-Kabel sind die Sende- (TD) und Empfangsadern (RD) jeweils miteinander verbunden. Eine schematische Darstellung dieser Kabelkreuzung ist in der folgenden Abbildung zu erkennen.



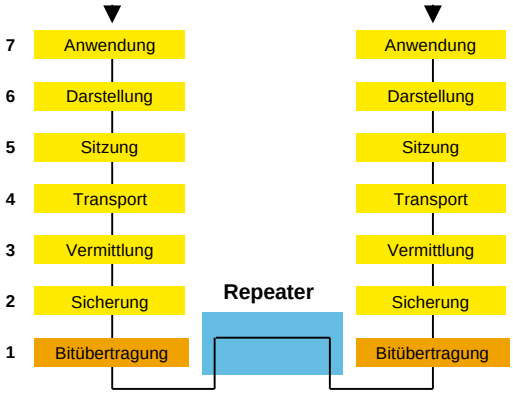
Repeater / Hub

Ein Repeater wird zur Kopplung von Netzwerksegmenten verwendet und kann damit die Ausdehnung und Topologie eines Netzwerks beeinflussen. Ein Hub bietet die selbe Funktionalität wie ein Repeater, besitzt allerdings mehrere Anschlüsse (sogen. Ports) und wird daher auch als Multiport-Repeater bezeichnet.



Von der Funktionalität her sind Repeater bzw. Hubs, der Schicht 1 des ISO-OSI-Modells zugeordnet. Alle auf der Bitübertragungsschicht (Schicht 1) arbeitenden Netzwerkkomponenten leiten empfangene Daten transparent weiter und verhalten sich damit, logisch gesehen wie ein Stück Netzwerkkabel. D.h. eine Kollisionsdomäne erstreckt sich auch über mehrere, durch Repeater bzw. Hubs getrennte Netzwerksegmente hinweg.

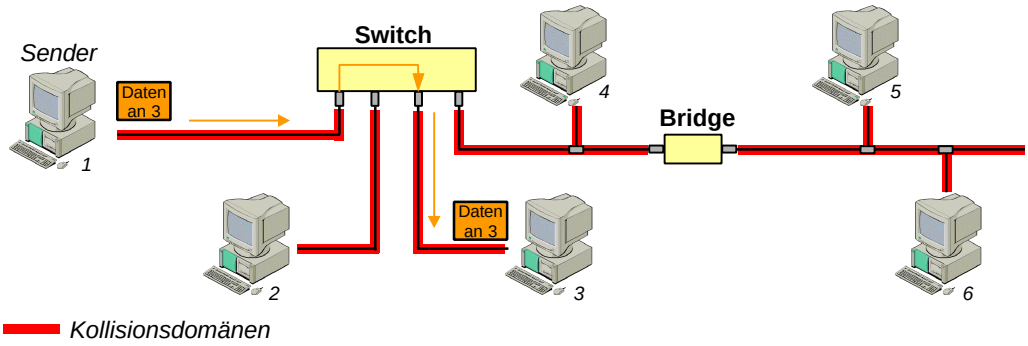
Repeater werden daher dazu eingesetzt um unterschiedliche Kabeltypen (z.B. Koaxial- und Twisted-Pair-Kabel) miteinander zu verbinden. Hubs dienen in der Regel dazu, mehrere Netzwerkteilnehmer logisch miteinander zu verbinden.



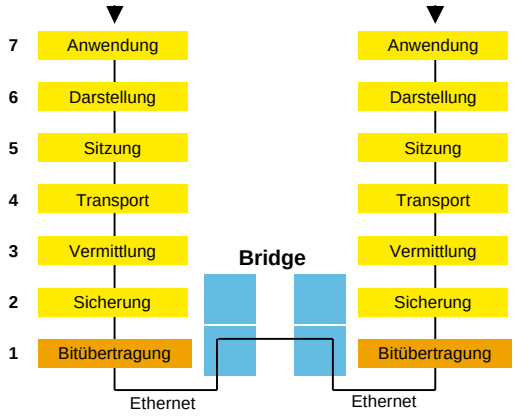
Switch / Bridge

Im Gegensatz zum Repeater leitet eine Bridge die Ethernetpakete nicht einfach weiter, sondern macht die Weiterleitung vom entsprechenden Ethernetpaket abhängig. Eine Bridge teilt dabei ein Netzwerk in zwei getrennte Kollisionsdomänen. Ein Switch arbeitet wie eine Bridge, jedoch mit mehr als nur zwei Kollisionsdomänen. Dabei ist jedem Anschluss (sogen. Port) des Switch eine eigene Kollisionsdomäne zugeordnet.

Bridges bzw. Switches interpretieren die Adressfelder (MAC-Adressen) der einzelnen Ethernetpakete und leiten diese dann gezielt vom Sender an den entsprechenden Empfänger weiter. Dadurch kommt es zu einer Filterung des Datenverkehrs in der Form, dass die Ethernetpakete nur in den Netzwerksegmenten des Senders und des Empfängers übertragen werden. Befinden sich sowohl Sender als auch Empfänger im gleichen Netzwerksegment, werden die Daten überhaupt nicht durchgeleitet. Dieser Filtermechanismus hat auch eine große Bedeutung beim Einsatz von Ethernet in der Automatisierungstechnik, welcher in Kapitel 4.4 noch ausführlicher dargestellt wird.

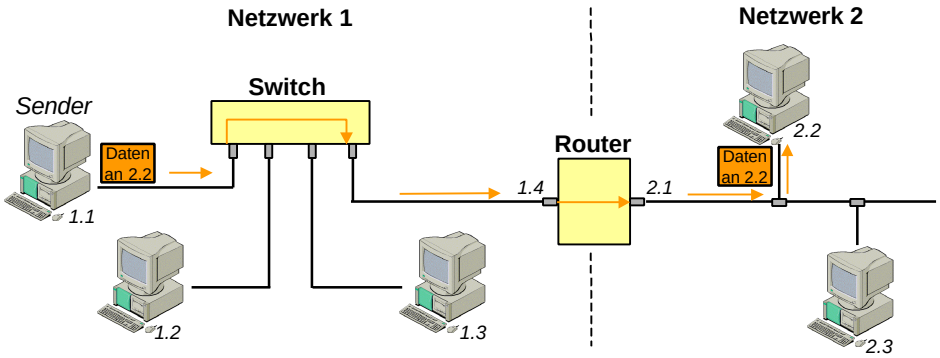


Im Bezug auf das ISO-OSI-Schichtenmodell, arbeiten Bridges und Switches auf der 2. Schicht. Somit lassen sich mit diesen Geräten Netzwerksegmente koppeln, bei denen die Schicht 1 unterschiedlich sind. D.h. es lassen sich damit beispielsweise Ethernetsegmente mit unterschiedlichen Übertragungsgeschwindigkeiten (z.B. 10Mbit/s ←→ 100Mbit/s) verbinden, ohne dass das gesamte Netzwerk auf die niedrigere Übertragungsgeschwindigkeit herabgestuft werden muss.

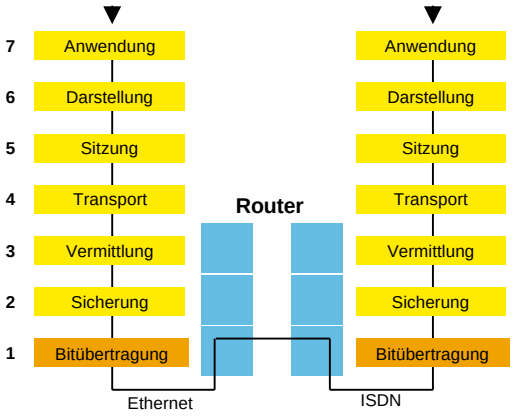


Router / Gateway

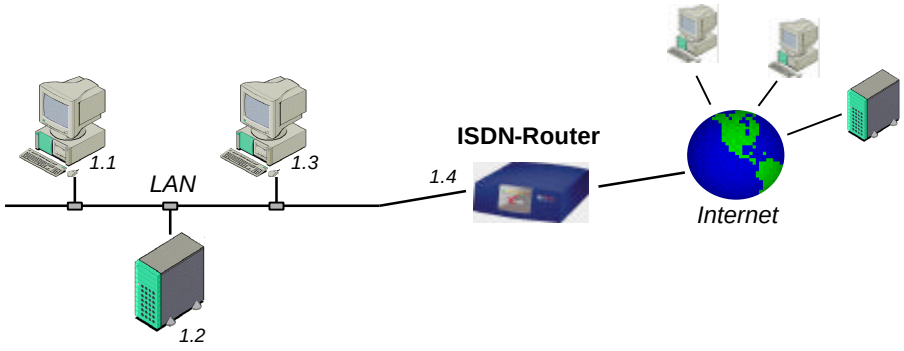
Noch einen Schritt weiter als eine Bridge bzw. ein Switch geht die Funktionalität eines Routers. Ein Router interpretiert nicht nur die einzelnen Ethernetpakete, sondern zusätzlich auch deren Inhalt d.h. den Datenbereich des Ethernetpaketes.
Wie bereits zuvor dargestellt, besteht der Datenbereich aus Daten der überlagerten Protokollschichten. Diese beinhalten in der Regel auch wieder Adressierungsinformationen (siehe TCP/IP-Protokoll in Kapitel 5) welche der Router auswertet und die Datenpakete entsprechend weiterleitet. Router werden in der Regel eingesetzt, um eine Verbindung zwischen eigenständigen Netzwerken zu ermöglichen.



Im ISO-OSI-Modell arbeitet ein Router auf der 3 Ebene. Daraus ergibt sich, dass man mit einen Router Netzwerke koppeln kann, bei denen die Schichten 1 und 2 verschieden sind.



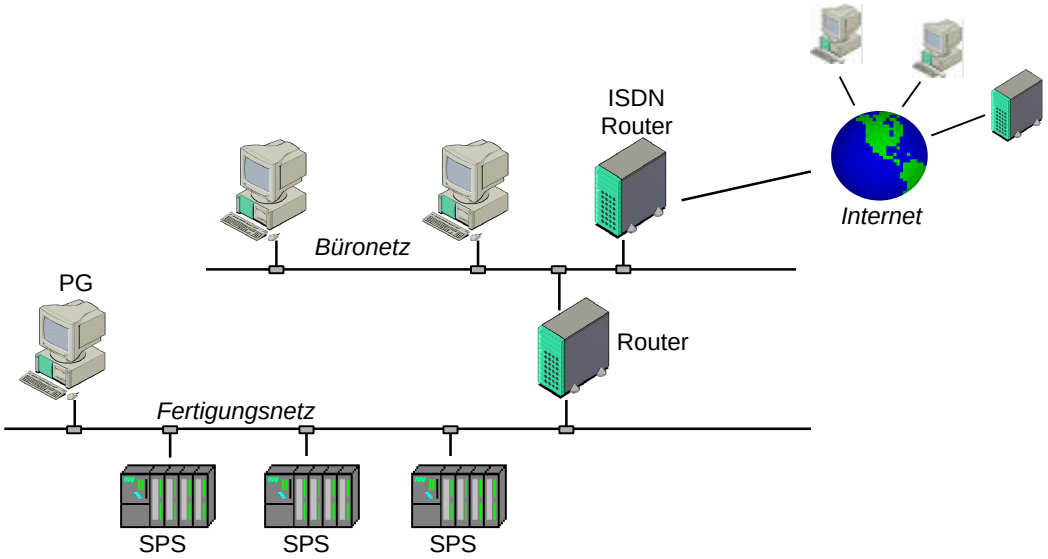
Ein Beispiel für einen Router mit unterschiedlichen Schichten 1 und 2 ist ein Ethernet-ISDN-Router (kurz: ISDN-Router). Dieser Router koppelt ein Ethernet-Netzwerk mit einem ISDN-Telefonnetz.



4.4 ETHERNET IN DER AUTOMATISIERUNGTECHNIK

Nachdem sich die Ethernet-Technologie im Büro-Bereich seit längerer Zeit als Standard etabliert hat, findet sie seit ein paar Jahren auch zunehmend in der Automatisierungstechnik Verwendung. Die folgende Abbildung zeigt einen beispielhaften Einsatz der Ethernet-Technologie in der Automatisierungstechnik.

Der Einsatz der Ethernet-Technologie im industriellen Umfeld, der mit dem Begriff ‚Industrial Ethernet' bezeichnet wird, umfasst im wesentlichen die Funktionalitäten des Ethernet-Standards wie er im Büro-Bereich verwendet wird. Jedoch gibt es beim ‚Industrial Ethernet' Besonderheiten in der Ausführung der Komponenten, um den höheren mechanischen und EMV-Beanspruchungen zu widerstehen.



Bei der Verkabelung kommt neben einem höher belastbaren Twisted-Pair-Kabel, ein Sub-D-Stecker zum Einsatz. Dieser Sub-D-Stecker ersetzt den aus dem Büro-Bereich stammenden RJ45-Stecker.

Weiterhin kommen statt Netzwerkkarten spezielle Kommunikationsprozessoren (CP-Baugruppen, **C**ommunication **P**rocessor) zum Einsatz. Diese können dazu verwendet werden, um eine SPS mit dem Ethernet-Netzwerk zu verbinden. Die folgende Abbildung zeigt eine solche CP-Baugruppe:

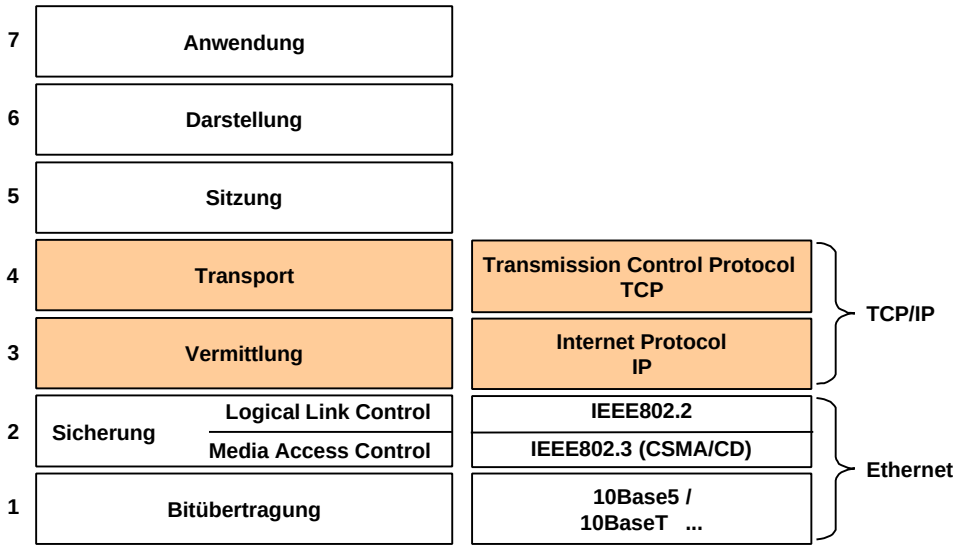
Solche Kommunikationsprozessoren gibt es auch in Form von speziellen Einsteckkarten für den PC. Prinzipiell funktionieren diese aber wie normale Ethernet-Netzwerkkarten, bieten jedoch zusätzliche Protokollfunktionalität auf höheren OSI-Schichten.

Ein weiterer Unterschied zum Einsatz im Büro-Bereich besteht darin, dass gewisse Übertragungszeiten eingehalten werden müssen. Diese Sicherstellung einer maximalen Nachrichtenübertragungsdauer wird als Deterministik bezeichnet. Beim herkömmlichen Ethernet gibt es eine solche Deterministik nicht, da jeder Netzwerkteilnehmer zu jedem beliebigen Zeitpunkt Daten übertragen kann, sofern er sich an das CSMA/CD-Verfahren hält. Daher kann es, insbesondere bei einer hohen Teilnehmerzahl, zu häufigen Kollisionen kommen, mit dem Effekt, dass die Übertragungszeiten deutlich höher werden. Im Büro-Umfeld ist eine solche Verzögerung zwar unschön, aber nicht kritisch. Im Produktionsbereich können dadurch jedoch Inkonsistenzen im Produktionsablauf auftreten und damit Produkte oder gar Produktionsanlagen zerstört werden. Daher ist in diesem Bereich eine Deterministik erforderlich. Um bei der Ethernet-Kommunikation dennoch Deterministik zu erreichen, verwendet man die bereits zuvor vorgestellten Switches. Dadurch lassen sich die Kollisionsdomänen im Netzwerk soweit verkleinern, dass die Wahrscheinlichkeit einer Kollision sehr klein ist.

5. INTERNET PROTOKOLL TCP/IP

Nachdem im vorausgegangenen Kapitel die Ethernet-Kommunikation auf den OSI-Schichten 1 und 2 betrachtet wurden, werden in diesem Kapitel die TCP/IP-Protokolle, auf den höheren Schichten behandelt.

Unter dem Begriff TCP/IP versteht man eigentlich zwei verschiedene Protokolle. Das IP-Protokoll (**I**nternet **P**rotocol) ist das Basisprotokoll des Internet. In Bezug auf das ISO-OSI-Modell liegt das IP-Protokoll auf der 3. Schicht und implementiert damit die Vermittlung von Datenpaketen über die verschiedenen Netze des Internets. Das TCP-Protokoll (**T**ransmission **C**ontrol **P**rotocol) hingegen basiert auf dem IP-Protokoll und befindet sich auf der 4. OSI-Schicht, wie in der folgenden Darstellung zu erkennen ist.



Das Internet ist ein Zusammenschluss unterschiedlichster Netzwerke, die auch andere als Ethernet-Netzwerke sein können. Um eine Abstraktion des eigentlichen Netzwerkes zu erreichen, wurde das IP-Protokoll entwickelt, welches die Grundlage für eine netzwerkübergreifende Kommunikation bereitstellt. Dazu wurden im wesentlichen folgende Aspekte definiert, die in den nächsten Kapiteln im Detail dargestellt werden:

- ein weltweit eindeutiger Adressierungsmechanismus
- ein Konzept für den Transport der Datenpakete über Netzwerkgrenzen hinweg

5.1 ADDRESSIERUNG

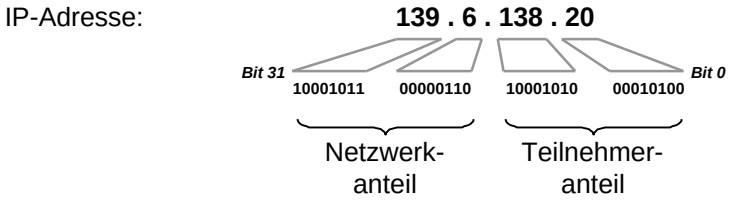
Um die einzelnen Teilnehmer im Internet eindeutig identifizieren zu können definiert das IP-Protokoll ein Adressierungsschema, welches dem der MAC-Adressen des Ethernet übergeordnet ist. Eine solche sogenannte IP-Adresse besteht aus insgesamt 32 Bits, die meist als vierstellige Dezimalzahlen dargestellt und durch Punkte getrennt wird (z.B.: 139.6.138.20).

Die meisten dieser IP-Adressen sind öffentlich, d.h. weltweit eindeutig. Diese Adressen werden von zentraler Stelle, unter anderem an Internet-Provider oder größere Unternehmen vergeben.
Neben diesen öffentlichen Adressen gibt es noch private, nicht offiziell vergebene IP-Adressen.

Reservierte private IP-Adressen	10.0.0.1	-	10.255.255.254
	172.16.0.1	-	172.31.255.254
	192.168.0.1	-	192.168.255.254

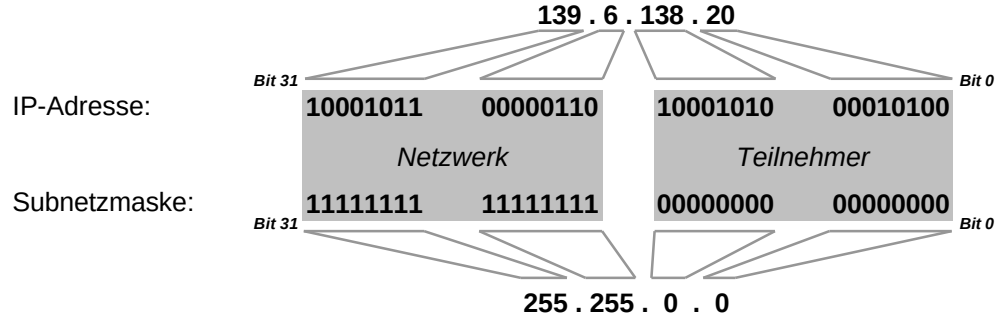
Diese privaten IP-Adressen dienen dazu, lokale Netzwerke aufzubauen, ohne für jeden Teilnehmer eine offentliche IP-Adresse zu verwenden. Da diese IP-Adressen weltweit mehrfach verwendet werden, können diese im Internet nicht zugeordnet werden und werden daher von den Routern verworfen.

Während die MAC-Adressen der Ethernetkarten wahllos zugewiesen werden, werden die IP-Adressen nach der logischen Topologie des Netzwerks vergeben. Dazu ist die IP-Adresse in zwei Bereiche aufgeteilt:



Dadurch ergibt sich, dass alle Teilnehmer in einem Ethernet-Netzwerk, den selben Netzwerkanteil besitzen müssen. Der Teilnehmeranteil kann dann zur Durchnummerierung der einzelnen Netzwerkteilnehmer verwendet werden.

Welcher Teil der IP-Adresse nun als Netzwerk- bzw. Teilnehmeranteil definiert ist, bestimmt die sogenannte Subnetzmaske. Diese Subnetzmaske besteht, ebenso wie die IP-Adresse aus insgesamt 32 Bits und wird meist ebenso in Form von 4 Dezimalzahlen dargestellt. Für jedes Bit, des Netzwerkanteils, enthält das Bit der Subnetzmaske eine 1. Die folgende Darstellung zeigt das Prinzip der Subnetzmaske:



Die Zuordnung der einzelnen IP-Adressen zu den jeweiligen MAC-Adressen des Ethernet geschieht über ein weiteres Protokoll des Internets, dem ARP-Protokoll (**A**dress **R**esolution **P**rotocol).
Möchte ein Netzwerkteilnehmer beispielsweise ein Datenpaket ein an die IP-Adresse eines anderen Teilnehmer im selben Netzwerk schicken, so kennt dieser zunächst nicht dessen MAC-Adresse. Um diese herauszufinden, wird ein spezielles Datenpaket an alle Teilnehmer im lokalen Netzwerk gesendet. Der Teilnehmer, der sich angesprochen fühlt, d.h. dessen IP-Adresse angefragt wurde, antwortet auf diesen Aufruf und der anfragende Teilnehmer kann die gewünschten Daten senden.

Praktisches Beispiel:
Dieses Beispiel zeigt, wie die ARP-Tabelle (Zuordnung IP- / MAC-Adresse) des Computers über das „*arp*"-Kommando ausgelesen werden kann. Damit zunächst ein Eintrag in dieser Tabelle erstellt wird, muss der entsprechende Netzwerkteilnehmer mindestens einmal angesprochen werden. Dazu wird das „*ping*"-Kommando eingesetzt, das hauptsächlich dazu verwendet wird, um die Erreichbarkeit eines Teilnehmers zu testen. Geben Sie hinter dem „*ping*"-Kommando den gewünschten Zielrechner an.

```
C:\>ping 192.168.0.1

Ping wird ausgeführt für 192.168.0.1 mit 32 Bytes Daten:

Antwort von 192.168.0.1: Bytes=32 Zeit<10ms TTL=255
Antwort von 192.168.0.1: Bytes=32 Zeit<10ms TTL=255
Antwort von 192.168.0.1: Bytes=32 Zeit<10ms TTL=255
Antwort von 192.168.0.1: Bytes=32 Zeit<10ms TTL=255

Ping-Statistik für 192.168.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum =  0ms, Mittelwert =  0ms


C:\>arp -a

Schnittstelle: 192.168.0.2 on Interface 0x1000003
  Internetadresse       Physikal. Adresse     Typ
  192.168.0.1           00-e0-7d-93-a3-6c     dynamisch

C:\>
```

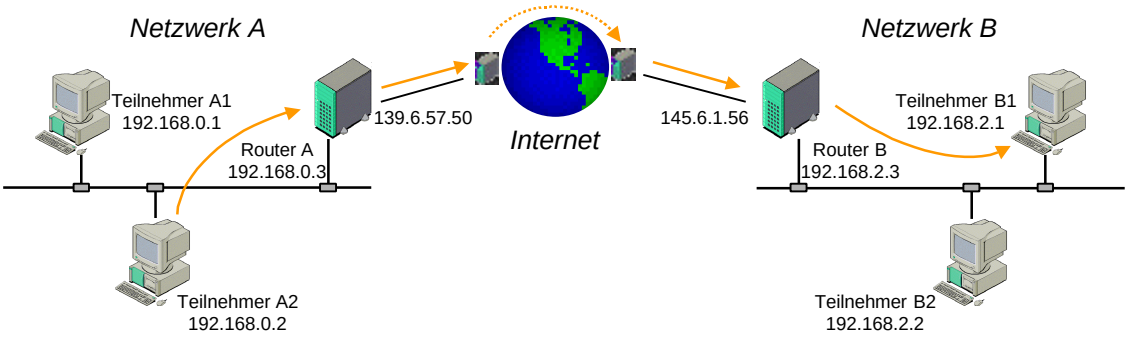
5.2 IP-KOMMUNIKATION

Neben der Adressierung ist die Datenübertragung über Netzwerkgrenzen hinaus ein wesentlicher Bestandteil des IP-Protokolls.

Da die Topologie des Internet sehr komplex ist, ist es nicht möglich jedem Teilnehmer mitzuteilen, über welche Wege er welchen Teilnehmer erreichen kann. Daher wurden spezielle Routing-Verfahren entwickelt, bei denen ein Teilnehmer lediglich seine angrenzenden Kommunikations-partner kennen muss und trotzdem auch weit entfernte Teilnehmer erreichen kann.

Möchte beispielsweise Teilnehmer A2, wie in der folgenden Abbildung dargestellt, Daten zu Teilnehmer B1 verschicken, so weis er zunächst nicht, wie er ihn erreichen kann.

Über den Vergleich der IP-Adresse von Teilnehmer B1 mit dem Netzwerkanteil seiner eigenen IP-Adresse kann er feststellen, dass sich Teilnehmer B1 nicht in Netzwerk A befindet.
In den Netzwerkeinstellungen des Teilnehmer A2 befindet sich neben der eigenen IP-Adresse sowie der dazugehörigen Subnetzmaske noch eine Router-Adresse (bei Windows-Betriebssystemen als ‚Standardgateway' bezeichnet). Diese Router-Adresse ist bei Teilnehmer A2 die IP-Adresse von Router A. Da Teilnehmer A2 festgestellt hat, dass sich die gewünschte Zieladresse außerhalb des eigenen Netzwerks befindet, also hinter dem Router A, schickt Teilnehmer A2 die zu sendenden Daten an den entsprechenden Standard-Router A.



Dieser Router kennt Teilnehmer B1 auch nicht direkt, kennt aber einen weiteren Router, an den er die Daten weiterleiten kann. Über entsprechende Routing-Tabellen der einzelnen Internet-Router gelangt das Datenpaket schließlich bei Router B an. Dieser Router kennt jetzt den gewünschten Zielteilnehmer B2 und kann das Datenpaket direkt zustellen.

Praktisches Beispiel:

Den Weg, den ein IP-Paket vom Sender zum Empfänger durchläuft, kann mit dem Programm „*tracert*" dargestellt werden. Dazu geben Sie hinter dem Befehl den gewünschten Empfänger an. In diesem Beispiel sehen Sie, dass das Paket zunächst über den eigenen ISDN-Router verschickt wird. Nachdem das Paket von mehreren Routern weitergeleitet wurde, wird zum Schluss der eigentliche Server erreicht.

```
C:\>tracert www.denic.de

Routenverfolgung zu www.denic.de [194.246.96.76]  über maximal 30 Abschnitte:

  1    10 ms   <10 ms   <10 ms  isdnrouter [192.168.0.1]
  2    30 ms    31 ms    30 ms  isdn01.nz.FH-Koeln.DE [139.6.14.10]
  3    30 ms    40 ms    30 ms  139.6.240.8
  4    30 ms    40 ms    40 ms  ar-koeln1.g-win.dfn.de [188.1.43.1]
  5    30 ms    40 ms    40 ms  cr-koeln1.g-win.dfn.de [188.1.84.1]
  6    40 ms    40 ms    40 ms  cr-frankfurt1.g-win.dfn.de [188.1.18.85]
  7    40 ms    40 ms    40 ms  ir-frankfurt2.g-win.dfn.de [188.1.80.38]
  8    40 ms    40 ms    40 ms  decix.Space.NET [80.81.192.105]
  9    70 ms   251 ms   240 ms  Cisco-F-V-Fa6-0-0.Space.Net [195.30.3.25]
 10   261 ms   310 ms   291 ms  spacenet-gw.denic.de [193.149.44.17]
 11    40 ms    50 ms    50 ms  www.denic.de [194.246.96.76]

Ablaufverfolgung beendet.

C:\>
```

5.3 TCP-PROTOKOLL

Über das IP-Protokoll gelangen die einzelnen Datenpakete nun vom Sender zum gewünschten Empfänger, auch wenn sich dieser in einem ganz anderen Netzwerk befindet. Wenn allerdings Daten auf mehrere kleiner Datenpakete aufgeteilt werden müssen (z.B. bei Übertragung einer Datei), ist bei dem IP-Protokoll nicht sichergestellt, dass alle Pakete in der richtigen Reihenfolge beim Empfänger ankommen. Dazu dient das dem IP-Protokoll überlagerte TCP-Protokoll, welches entsprechende Transport- und Sicherungsmechanismen bereitstellt.

Der TCP-Protokoll baut eine Kommunikationsverbindung zwischen dem Sender und dem Empfänger auf, indem in den ersten Datenpaketen entsprechende Kommandos zum Verbindungsaufbau gesendet werden. Anschließend werden die eigentlichen Daten in einzelnen, durchnummerierten Paketen übertragen. Nachdem alle relevanten Daten übertragen wurde, wird eine solche Verbindung auch wieder durch entsprechende Kommandos abgebaut. Dadurch ist sichergestellt, dass alle Datenpakete übertragen werden und anschließend in der richtigen Reihenfolge wieder zusammengesetzt werden können.

Das TCP-Protokoll bietet noch eine weitere Funktionalität, um mehrere gleichzeitige Verbindungen zwischen zwei Netzwerk-Teilnehmern zu ermöglichen. Dazu werden sogenannte ‚Ports' definiert, die eine Zuordnung der Datenpakete zu bestimmten Applikationen ermöglichen. Diese Ports bestehen aus einem 16-Bit-Wert d.h. sie liegen zwischen 0 und 65535. Die Bereich der Ports von 0 bis 1023 ist fest vergeben und bestimmten Applikationsprotokollen zugeordnet.

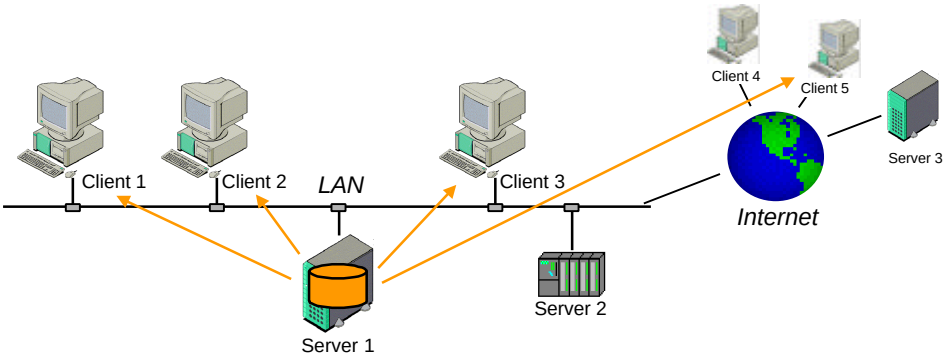
Im folgenden sind einige der bekannteren Port-Adressen mit den dazugehörigen Diensten aufgeführt.
Auf die wichtigsten Dienste wird im Kapitel 6 noch detailliert eingegangen.

Port-Nummer	**Dienst / Protokoll**
20 / 21	FTP – File Transfer Protocol (Kapitel 6.2) Übertragung von Dateien zwischen den Netzwerkteilnehmern
23	Telnet - Terminalzugriff auf ein entferntes System
25	SMTP – Simple Mail Transfer Protocol (Kapitel 6.3) Versand von elektronischer Post (E-Mail)
80	HTTP – Hypertext Transfer Protocol (Kapitel 6.1) Übertragung von HTML-Dateien (Webseiten)

Eine vollständige Liste der Port-Adressen wird von der IANA (Internet Assigned Number Authority, www.iana.org) bereitgestellt.

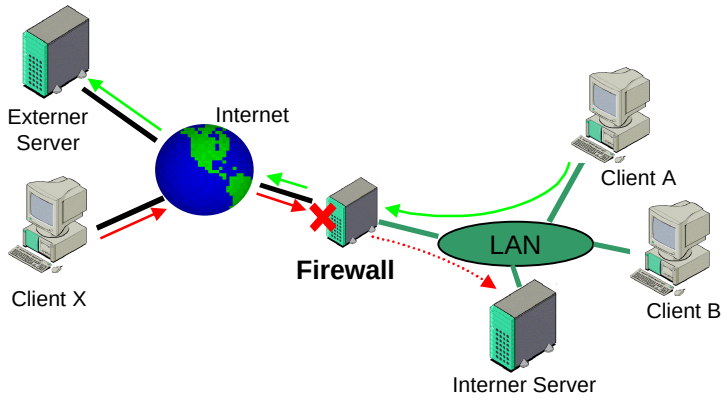
5.4 CLIENT-SERVER-STRUKTUR

Im bisherigen Verlauf dieses Dokuments war immer davon ausgegangen, dass sich im Netzwerk bzw. im Internet nur gleiche Teilnehmer befinden, die Daten miteinander austauschen. In der Praxis findet man jedoch häufig eine Aufteilung der Netzwerkteilnehmer in Systeme die Daten bereitstellen bzw. liefern und solchen, die Daten abfragen bzw. empfangen. Aus diesem Grund spricht man bei den Systemen auch von Servern bzw. Clients.



5.5 FIREWALL-SYSTEME

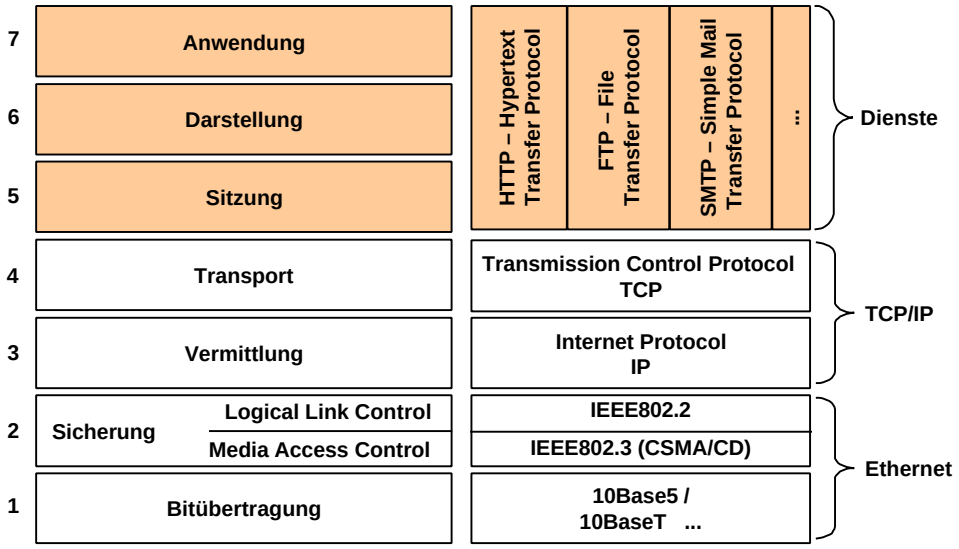
In den letzten Kapiteln wurde dargestellt, wie Daten von einem Server geholt bzw. zu einem Client übertragen werden können, auch wenn diese sich in unterschiedlichen Netzwerken befinden. Allerdings ist es nicht immer erwünscht, dass jemand auf bestimmte Netzwerke zugreifen kann. Daher kommen in den letzen Jahren immer mehr entsprechende Sicherungsmaßnahmen zum Einsatz, die man im allgemeinen unter dem Begriff Firewall zusammenfasst.
Unter einer Firewall versteht man einen Router, der mit entsprechenden Netzwerkfiltern ausgestattet ist, weswegen man in diesem Zusammenhang auch von Paketfilter-Firewalls spricht. Diese speziellen Router leiten die ankommenden Datenpakete nicht einfach weiter, sondern prüfen diese gegen bestimmte Filterregeln. Je nach Ergebnis dieser Prüfung werden die Datenpakete dann weitergeleitet, abgelehnt oder einfach verworfen.
In dem folgenden Szenario könnten die Filter beispielsweise so definiert sein, dass Zugriffe auf das interne Netz (LAN) generell untersagt sind, jedoch Zugriffe vom internen Netz nach außen möglich sind.



Neben der Ziel-IP-Adresse lassen sich noch weitere Kriterien wie z.B. Quell-IP-Adresse oder Portnummern für die Filter verwenden. Neben Paketfiltern bieten viele Firewalls noch weiterführende Sicherungsmechanismen, die jedoch hier nicht weiter betrachtet werden.

6. INTERNET DIENSTE

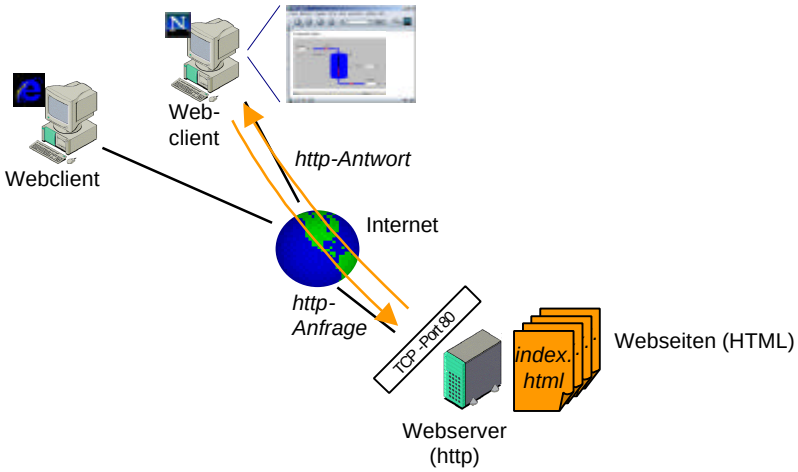
Nachdem in den vorherigen Kapiteln bereits die Schichten 1 bis 4 des ISO-OSI-Modells behandelt wurden, werden in diesem Kapitel die letzen Schichten betrachtet. Wie in der Abbildung zu erkennen ist, gibt es für die Schichten 5 bis 7 keine weitere Unterteilung. Stattdessen übernehmen die einzelnen Internet-Dienste die Funktionalität dieser drei Schichten in jeweils einem Protokoll.



Im Internet bzw. im LAN bei Verwendung der Internet-Technologien finden sich zahlreiche Dienste die auf Basis des TCP/IP-Protokolls arbeiten. An dieser Stelle sei jedoch nur auf die wichtigsten Dienste eingegangen.

6.1 WORLD WIDE WEB - HTTP

Die wohl bekannteste Anwendung des Internet ist das sogenannte World Wide Web. Dabei werden Webseiten (HTML-Dokumente, siehe Kapitel 7.1) und darin eingebettete Elemente wie Grafiken oder Java-Applets (siehe Kapitel 7.2) von speziellen Anwendungsprogrammen geladen. Diese Anwendungsprogramme werden im Allgemeinen als Web-Browser bezeichnet, von denen die bekanntesten wohl der Microsoft Internet Explorer und der Netscape Navigator sind.



Die Grundlage für die Kommunikation in diesem ‚World Wide Web' bietet das HTTP-Protokoll (**H**yper**T**ext **T**ransfer **P**rotocol). Dieses Protokoll arbeitet nach dem Client/Server-Prinzip, indem von einem Web-Browser (Client) Kommandos an einen Web-Server geschickt werden. Der Server bearbeitet die Kommandos und liefert gegebenenfalls die entsprechenden Daten an den Web-Browser zurück. Für Anfragen an den Webserver stehen dem Client die folgenden Kommandos zur Verfügung:

- *GET* fordert ein bestimmtes Dokument vom Webserver an
- *HEAD* fordert allgemeine Informationen über ein Dokument an
- *PUT* sendet Daten für eine weitere Bearbeitung zum Server (z.B. Daten aus einem ausgefüllten Formular)

Damit dem Webserver auch mitgeteilt werden kann, welche Daten angefordert werden, gibt es eine spezielle Adressierungssyntax, die unter der Bezeichnung URL (Uniform Resource Locator) bekannt ist. Korrekt ist eine HTTP-URL wie folgt aufgebaut:

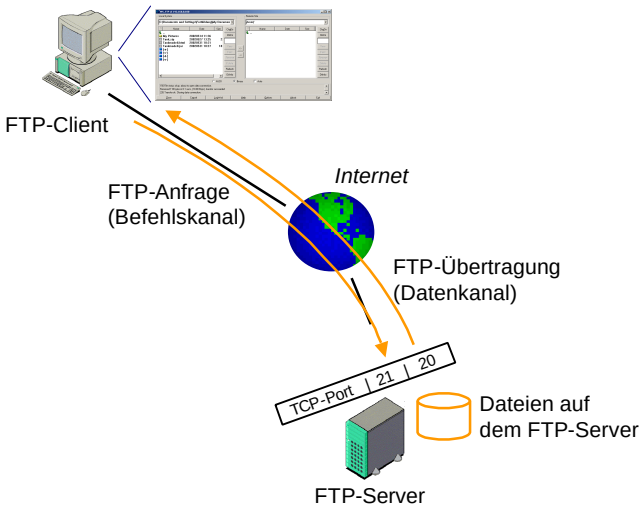
Syntax: http://<host>:<port>/<pfad>?<parameter>
Beispiel: http://www.siemens.de/sce

Das Präfix *http://* identifiziert den URL dabei als HTTP-Verweis und unterscheidet ihn damit von anderen Verweisen wie *ftp://* oder *mailto://*. Dahinter folgt der Host- oder Domainname des anzusprechenden Webservers. Getrennt durch einen Doppelpunkt kann noch eine Port-Angabe folgen, die jedoch meist weggelassen wird. In diesem Fall wird der TCP-Port 80 des http-Protokolls verwendet (siehe Kapitel 5.3). Hinter dem Port folgt noch der Pfad der Ressource, der bei http aus einem Verzeichnis und / oder einem Dateinamen bestehen kann. Im Beispiel oben wird zum Beispiel auf das Verzeichnis */sce* verwiesen. Wenn ein solches Verzeichnis angegeben wird, gibt es im Allgemeinen eine Standard-HTML-Datei (index.html, default.htm, o.ä.), die in diesem Fall zurückgeliefert wird.

Im Bereich der Automatisierungstechnik kommt der HTTP-Dienst zunehmend zum Einsatz, um aktuelle Informationen aus dem Prozess über einen Standard-Web-Browser abrufen zu können. Dazu wird in die SPS-Steuerungen entsprechende Web-Server-Funktionalität integriert, so dass man direkt auf die Web-Seiten in der SPS-Steuerung zugreifen kann.

6.2 DATEITRANSFER - FTP

Ein weiterer wichtiger Dienst des Internet ist das FTP-Protokoll (File Transfer Protocol), welcher die Möglichkeit bietet, Daten in Form von Dateien zu übertragen.
Auch dieses Protokoll arbeitet nach dem Client/Server-Prinzip, in der Form, dass ein FTP-Client-Programm bestimmte Kommandos an einen FTP-Server schickt. Dabei können Dateien, ähnlich wie auf eine lokale Festplatte gespeichert bzw. von dort geladen werden. Auch die Darstellung bzw. Organisation der Daten ähnelt dem einer lokalen Festplatte, da die Dateien ebenfalls in entsprechenden Verzeichnissen abgelegt werden können.



Während bei anderen Internet-Protokollen nur jeweils ein Kommunikationskanal benötigt wird, verwendet das FTP-Protokoll zum einen ein Befehlskanal (TCP-Port 21) und zum anderen einen Datenkanal (TCP-Port 20). Ein FTP-Client-Programm baut zunächst die Verbindung über den Befehlskanal zum FTP-Server auf und sendet anschließend die entsprechenden FTP-Kommandos. Fordert der Client eine Datei an, baut der FTP-Server eine neue Verbindung zum anfordernden Client auf und überträgt über diesen Datenkanal die entsprechende Datei.

Diese FTP-Kommunikation wird jedoch oft von Firewalls abgeblockt, da Verbindungen von außen in das interne Netzwerk meist nicht erlaubt werden. Das heißt, der FTP-Server kann den Datenkanal nicht zum FTP-Client aufbauen, da dies als externer Zugriff gewertet wird.
Aus diesem Grund wurde das FTP-Protokoll erweitert und bietet auch einen sogenannten ‚passiv Modus'. Bei dieser FTP-Kommunikation teilt der FTP-Server dem Client beim Verbindungsaufbau einen bestimmten TCP-Port mit, über den sich der FTP-Client mit dem Server verbinden kann. Über diesen Datenkanal werden dann wie zuvor die eigentlichen Daten ausgetauscht. Allerdings werden nun beide Kommunikationskanäle vom FTP-Client aufgebaut und es kommt nicht mehr zu Komplikationen mit einer zwischengeschalteten Firewall.

Neben speziellen FTP-Client-Programmen besteht auch die Möglichkeit mit Web-Browsern auf FTP-Dienste zuzugreifen. Dazu gibt es, ähnlich wie beim HTTP-Protokoll, auch eine entsprechende Adressierungssyntax, die im Adressfeld des Web-Browsers angegeben werden kann:

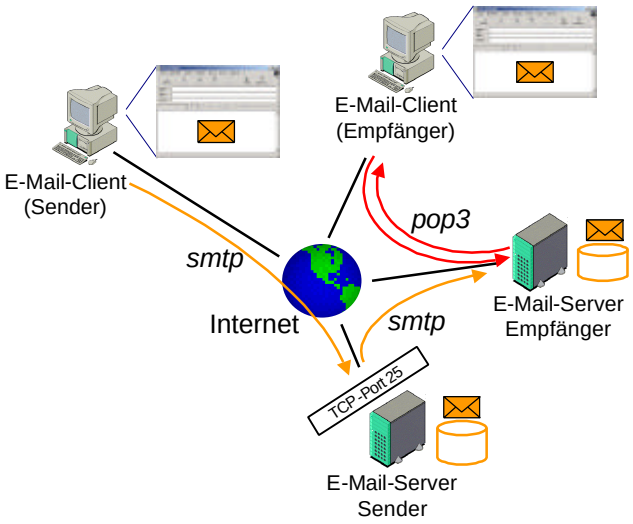
Syntax: ftp://[Benutzername[:Passwort]@]Servername[:Port][/Pfad]
Beispiel: ftp://anwender:geheim@ftp.server.net/

Die optional anzugebenen Daten Benutzername und Passwort dienen einer möglichen Anmeldeprozedur am FTP-Server. Sollten diese nicht angegeben werden, meldet sich der Web-Browser unter dem Pseudonym ‚anonymous' an. Als Passwort wird in diesem Fall die eigene E-Mail-Adresse übergeben. Der übrige Teil der Adressierungssyntax entspricht weitgehend dem des HTTP-Protokolls. Auch hier lässt sich optional wieder eine andere Port-Adresse als der Standard-FTP-Port 21 angeben. In den meisten Fällen wird dies aber nicht benötigt.

Im Bereich der Automatisierungtechnik wird das FTP-Protokoll zum einen eingesetzt, um Daten wie Web-Seiten oder Java-Applets auf die SPS-Steuerung zu übertragen, um anschließend über einen Web-Browser aktuelle Prozessdaten abfragen zu können (siehe Kapitel 6.1).

6.3 E-MAIL - SMTP

Ein weiteres wichtiges Internet-Protokoll, welches ebenfalls im Bereich der Automatisierungtechnik zum Einsatz kommt, ist das SMTP-Protokoll (**S**imple **M**ail **T**ransfer **P**rotocol). Dieses Protokoll dient dazu, elektronische Post (E-Mail) zu versenden bzw. zu übertragen.



Im allgemeinen werden zu versendende E-Mails an einen bestimmten Mail-Server des eigenen Internet- oder Mail-Providers geschickt. Dazu baut der E-Mail-Client über den TCP-Port 25 eine Verbindung zum Mail-Server auf und überträgt die zu verschickende Nachricht. Der Mail-Server schickt die E-Mail dann an den entsprechenden Mail-Server des Empfängers weiter. Für diese beiden Kommunikationsverbindungen wird jeweils das SMTP-Protokoll verwendet. Für das Abholen der eigenen E-Mails vom Mail-Server kommt hingegen andere Protokolle zum Einsatz (POP3 oder IMAP) die hier aber nicht weiter betrachtet werden.

Im Bereich der Automatisierungtechnik wird dieser Dienst beispielsweise dazu eingesetzt um durch eine SPS im Bedarfsfall eine Mitteilung an bestimmte Personen zu verschicken.

6.4 DOMAIN NAME SYSTEM DNS

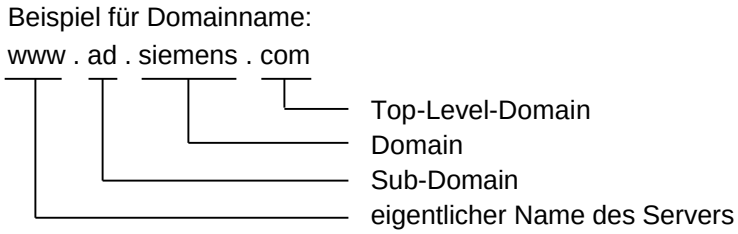
Ein sehr hilfreicher Dienst im Internet, der aber eigentlich kaum wahrgenommen wird, ist der DNS-Dienst (**D**omain **N**ame **S**ervice). Dieser Dienst stellt vereinfacht gesehen das Adressbuch des Internet dar. D.h. es handelt sich um eine verteilte Datenbank mit den Namen und den dazugehörigen IP-Adressen aller Hosts im Internet. Erst durch diesen Dienst ist es möglich, beispielsweise statt der IP-Adresse ‚194.138.38.99' den Domain-Namen ‚www.ad.siemens.de' im Adressfeld des Web-Browsers einzugeben.

Der zur Verfügung stehende Adressraum wurde dazu unabhängige Bereiche, die sogenannten Domains (Domänen) unterteilt. Ein solcher Domainname besteht aus verschiedenen Einheiten, die jeweils durch einen Punkt voneinander getrennt sind. Organisatorisch gesehen werden die Einheiten von rechts nach links immer kleiner. Dementsprechend befindet sich ganz links der eigentliche Name des Servers. Ganz rechts, also als höchste organisatorische Einheit, befindet sich die sogenannte Top Level Domain, die von einer zentralen Stelle, dem InterNIC festgelegt wird.

Derzeit gibt zwei Kategorien für die Top Level Domains:

- Domains nach Betreibern / Inhalt: .com / .net / .edu / .gov / .mil / .org / (.info)
- Länderdomains: .de / .uk / .fr / .it / ...

Zu jeder Top Level Domain existiert eine Körperschaft, die für die Namensvergabe innerhalb ihrer Domain verantwortlich ist. Für die deutsche Länder-Domain ‚.de' ist dies beispielsweise das DeNIC.



Zu jeder Domain gibt es auch die Möglichkeit weitere Sub-Domains hinzuzufügen. Auf diese Art und Weise können dann leicht Host-Namen zustande, die vier oder fünf Domains enthalten.

Praktisches Beispiel:
Um zu einem bestimmten Domainnamen die zugehörige IP-Adresse zu ermittelt, kann das „*nslookup*"-Kommando verwendet werden. Dazu geben Sie hinter dem Kommando den gewünschten Domainnamen an. Statt dem Domainnamen können Sie auch eine IP-Adresse angeben, wenn Sie den entsprechenden Domainnamen suchen.

```
C:\>nslookup www.ad.siemens.de
Server:  nets1.gm.fh-koeln.de
Address:  139.6.57.5

Nicht autorisierte Antwort:
Name:    www.ad.siemens.de
Address:  194.138.38.99

C:\>
```

7. INHALTE DES WORLD WIDE WEB

Nachdem in den letzten Kapiteln die wichtigsten Kommunikations- und Transportmechanismen dargestellt wurden, werden in diesem Kapitel die eigentlichen Inhalte vorgestellt. Allerdings beschränkt sich die Betrachtung im wesentlichen auf die Inhalte, die im Bereich der Automatisierungstechnik zum Einsatz kommen.

7.1 WEBSEITEN – HTML

Die wichtigsten Elemente des World Wide Web sind eindeutig die sogenannten Webseiten. Diese Seiten, die der Web-Browser vom Webserver anfragt und anschließend anzeigt, bestehen aus Elementen einer eigenen Sprache. Diese Sprache wird als HTML bezeichnet, was für Hypertext Markup Language steht - also eine Beschreibungssprache für Hypertext-Dokumente.

HTML besteht aus einer relativ einfachen Sprachsyntax zur Strukturierung von Texten zum Beispiel in Form von Überschriften, Textabsätzen, Listen oder Tabellen. Zusätzliche Elemente wie Grafiken oder andere multimediale Inhalte werden durch Referenzen in das HTML-Dokument eingebunden. Diese Elemente werden also, anders als beispielsweise bei einem Dokument einer Textverarbeitung, nicht direkt in das HTML-Dokument eingebettet.

Eine der wichtigsten Eigenschaften von HTML ist jedoch die Möglichkeit, Verweise (sogenannte Hyperlinks) zu definieren. Diese Verweise können zu anderen Stellen innerhalb des eigenen Web-Projektes führen, aber auch zu beliebigen anderen Adressen im World Wide Web. Ein Anwender kann diesen Verweisen über einen einfachen Mausklick folgen.

Um eigene HTML-Dokumente zu erstellen reicht im Grunde bereits ein einfacher Text-Editor. Für die Erstellung von umfangreicheren Webseiten ist allerdings ein spezialisierter HTML-Editor empfehlenswert. Für erste Schritte ist jedoch ein Text-Editor ausreichend.

Zur Strukturierung der einzelnen Elemente des Web-Dokumentes sind in HTML Deklarierungselemente, sogenannte HTML-Tags, verfügbar. Diese HTML-Tags bestehen aus bestimmten Schlüsselwörtern, die in spitze Klammern eingefasst sind. Weiterhin besteht ein solches Strukturierungselement aus einem öffnenden und einem schließenden HTML-Tag, wobei das schließende HTML-Tag dadurch gekennzeichnet ist, dass dem Schlüsselwort ein Schrägstrich (/) vorangestellt ist. Das folgende Beispiel zeigt die Deklaration einer Überschrift im HTML-Format:

Beispiel für ein HTML-Tag: <h1>Hauptüberschrift</h1>

Jedes HTML-Dokument besitzt eine grundsätzliche Hauptstruktur, die im folgenden abgebildet ist. Daraus ist zu erkennen, dass die einzelnen HTML-Tags auch ineinander verschachtelt sein können.

```
<html>
   <head>
    ... <!-- allgemeine Informationen zum HTML-Dokument -->
   </head>
   <body>
    ... <!-- eigentlicher Inhalt des HTML-Dokuemts -->
   </body>
</html>
```

Das gesamte HTML-Dokument gliedert sich in einen <head>- und einen <body>-Bereich. Der <head>-Bereich beinhaltet allgemeine Informationen zu dem jeweiligen HTML-Dokument, wie beispielsweise Dokumententitel, Autor oder Schlüsselwörter.
Der <body>-Bereich beinhaltet dann das eigentliche Dokument, so wie es auch später in einem Web-Browser angezeigt wird. Neben diesen beiden Bereichen gibt es keine weitern Vorgaben für eine grundsätzliche Dokumentenstruktur.

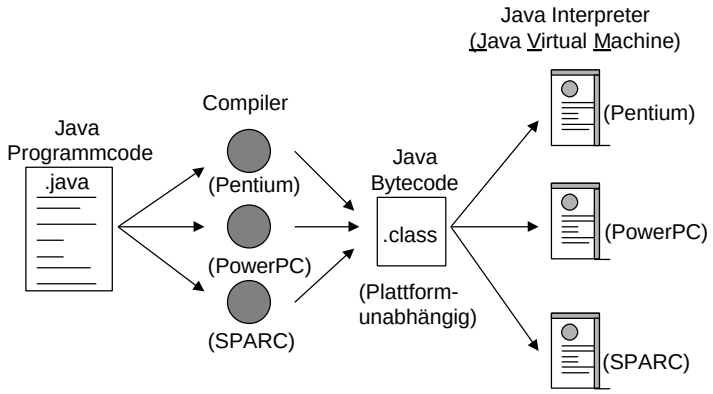
Im folgenden sind ein paar der häufig verwendeten HTML-Tags dargestellt. Für eine ausführlicher Darstellung sei an dieser Stelle auf entsprechende Literatur verwiesen.

HTML-Tag	**Bedeutung**
<title>Dokumententitel</title>	Deklaration eines Dokumententitels im <head>-Bereich
Überschrift 1	Überschrift der höchsten Gliederungsebene
Überschrift 2	Überschrift der 2 Gliederungsebene
Absatz	Deklaration eines Absatzes
<img href="logo.gif">	Einbindung einer Grafik in die Webseite
weiter	Verweis (Hyperlink) auf eine weitere Webseite
<!-- Kommentar -->	Kommentar, der vom Web-Browser nicht angezeigt wird.

7.2 JAVA-APPLETS

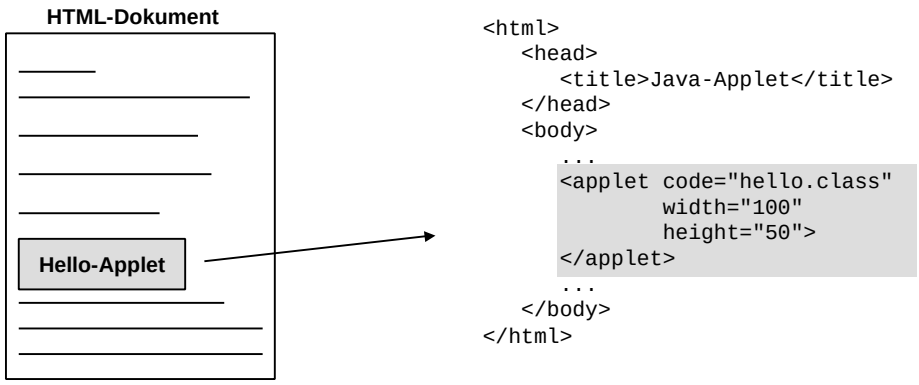
Java ist eine von Sun Microsystems entwickelte, plattformunabhängige Programmiersprache. In Aufbau und Syntax lehnt sich die Sprache an C/C++ an.

Die Plattformunabhängigkeit wird dadurch erreicht, dass der Java-Programmcode nicht, wie sonst üblich entsprechend dem jeweiligen Prozessor und Betriebssystem übersetzt (kompiliert) wird, sondern in einen eigenen ausführbaren Code. Dieser als Bytecode bezeichnete Programmcode ist auf keinem Prozessor bzw. Betriebssystem direkt ausführbar, sondern wird von einem virtuellen Prozessor ausgeführt, der diesen Bytecode interpretieren kann. Ein solcher virtueller Prozessor wird ‚Virtual Machine' genannt und setzt den Java-Bytecode in die jeweiligen plattformspezifischen Betriebssystem- und Prozessorcodes um.
Dies hat den Vorteil, dass ein Java-Programm, welches auf einem System entwickelt und übersetzt (kompiliert) wurde, direkt auf einem anderen System (auch mit anderem Prozessortyp / Betriebssystem) ausgeführt werden kann.



Java-Programme, die für den Einsatz im Internet ausgelegt sind, werden Applets genannt. Diese werden dazu in HTML-Dokumente eingebunden und erscheinen dann innerhalb der entsprechenden Web-Seite. Applets sind besondere Java-Programme, die in ihren Möglichkeiten eingeschränkt sind, so dass diese auf dem Client keine unerlaubten Aktionen durchführen können (z.B. Dateien löschen oder verändern). Um das zu gewährleisten laufen die Applets in einer speziellen Sicherheitsumgebung, der sogenannten Sandbox.

In HTML-Dateien werden zusätzliche Elemente, wie zum Beispiel Grafiken, über Verweise eingebettet. Auch für Java-Applets gibt es ein speziellen HTML-Tag (<APPLET>), der einen Verweis auf eine entsprechende CLASS-Datei bereitstellt, in der sich das gewünschte Java-Applet befindet. Die folgende Grafik zeigt die Einbindung eines Applets (hello.class) in eine HTML-Datei:



Da das <APPLET>-Tag noch über weitere Attribute verfügt, sind hier die wichtigsten aufgeführt:

- code = ... Dieses Attribut verweist auf das einzubindende Java-Applet. Hier darf nur die CLASS-Datei angegeben werden, auch wenn diese sich in einem anderen Verzeichnis befindet.
- codebase = ... Falls sich die CLASS-Datei in einem anderen Verzeichnis als die HTML-Datei befindet, kann hier das entsprechende Verzeichnis angegeben werden
- width = ... Dieses Attribut bestimmt die Anzeigebreite des Java-Applets
- height = ... Dieses Attribut bestimmt die Anzeigehöhe des Java-Applets

Um selbst Java-Applets erstellen zu können, benötigen Sie einen Texteditor um den Java-Quellcode zu erstellen sowie das Software-Entwickler-Kit von Sun (SDK). Eine komfortablere Entwicklung von Java-Applets bieten die zahlreichen Java-Entwicklungsumgebungen.
Beispiele für diese Entwicklungsumgebungen sind:

- Borland JBuilder
- IBM VisualAge for Java
- Sun Microsystems Forte for Java