TCP/IP-Ethernet bis Web-IO

Dieses Buch ist für alle gemacht, die ohne Spezialwissen über Computernetzwerke Ethernet-Endgeräte unter TCP/IP in Betrieb nehmen wollen. Es ist in drei Teile gegliedert:

- TCP/IP-Ethernet verstehen
  Hier finden Sie die wichtigsten Grundlageninformationen zum Thema TCP/IP und zu den Basisprotokollen.

- TCP/IP-Ethernet einrichten
  Hier wird Schritt für Schritt die Einrichtung von TCP/IP-Ethernet auf PCs mit den gängigen Betriebssystemen aufgezeigt.

- Kleines Netzwerk-ABC
  Hier erläutern wir die wichtigsten Begriffe und Abkürzungen, die Ihnen beim Umgang mit Netzwerken begegnen können.

Alle wichtigen Abläufe und Zusammenhänge werden leicht verständlich erklärt.

Keine Angst: Wir werden uns dort nicht bis ins letzte Detail verlaufen. Wir haben uns ganz bewusst auf die Dinge beschränkt, die zum Verständnis der beschriebenen Technologien wirklich wichtig sind.

Zur reinen Inbetriebnahme von TCP/IP-Netzwerkkomponenten ist es schließlich auch gar nicht nötig, jedes Protokoll bis ins letzte Bit zu kennen.

W&T liegt uns am Herzen

Wir entwickeln und produzieren seit über 30 Jahren Mikrocomputer als Schnittstellenwandler. Wir beschäftigen uns seit über 20 Jahren mit Netzwerktechnik. Seit 10 Jahren versuchen wir, mit diesem Grundlagenbuch technische Orientierung in der weiten Welt der TCP/IP-Netze zu geben.

Dies tun wir, um Sie zu ermutigen, auch für Ihre Datenverbindungen diese Netze zu nutzen. Dazu braucht es neben dem Wissen auch häufig kleine Umsetzer, die Ihre Endpunkte und Geräte tatsächlich mit dem Netzwerk verbinden. Solche Interfaces finden Sie unter **http://www.wut.de**.

Und nicht nur sichere und robuste Datenverbindungen liegen uns am Herzen. Es ist auch immer die Verbindung von Mensch zu Mensch, welche das gelingende technische Funktionieren herstellt und begleitet. Darum sind unsere Techniker unter 0202/2680-110 gerne für ihre aktuellen Fragen zu sprechen.

Während Geräte einfach durch neu produzierte ersetzt werden können, wenn sie das Ende ihrer Lebensdauer erreicht haben, müssen Menschen den langen Weg vom hilflosen Säugling bis zur technischen Ausbildung erfolgreich gegangen sein, bis sie gelernt haben, die komplexen Techniken unserer Tage zu beherrschen.

Obwohl wir dabei die hohe Bedeutung der frühen Kindheit allzu leicht vergessen - auch weil wir uns selbst an diese Zeit gar nicht erinnern können - möchten wir die Gelegenheit nutzen und Sie auf die eng mit uns verbundene Winzig-Stiftung hinweisen: **http://www.winzig-stiftung.de**.

Mit den besten Wünschen für die Lektüre des Büchleins,
für das Gelingen Ihrer Projekte und
für noch viele gute gemeinsame Jahre

Ihr Rüdiger Theis, Frank Thiel
und alle WuTler


R.Theis


F.Thiel

Inhalt

TCP/IP-Ethernet verstehen 7

TCP/IP-Ethernet verstehen

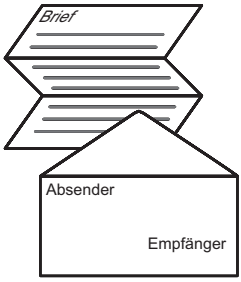
Grundsätzlich haben alle Netzwerktopologien eines gemeinsam:

Jeder Netzteilnehmer erhält (mindestens) eine eigene und eindeutige Adresse.

Die zu übertragenden Nutzdaten werden in einen Rahmen aus z. B. Adresse des Empfängers, Adresse des Absenders und Checksumme in ein „Datenpaket“ verpackt.

Mit Hilfe der Adressinformationen können die Nutzdaten in den so entstandenen Datenpaketen über gemeinsam benutzte Leitungswege an den richtigen Empfänger übermittelt werden.

Bei einem Brief ist es nicht anders: Man steckt den Brief in einen Umschlag, auf dem Empfänger und Absender notiert sind. Der Postbote weiß dann, wem er den Brief zustellen soll; der Empfänger kann ablesen, woher er kommt und wem er bei Bedarf zu antworten hat.



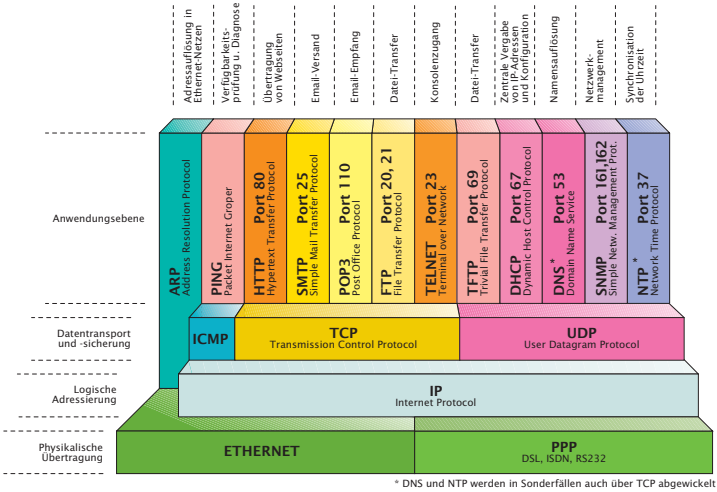
Beim Datentransfer innerhalb eines Netzwerkes hat der Empfänger zusätzlich die Möglichkeit, mit Hilfe der mit versandten Checksumme die Vollständigkeit und Fehlerfreiheit der empfangenen Nutzdaten zu überprüfen.

Auf ihrem Weg von einer Anwendung zur anderen durchlaufen die Daten verschiedene „Schichten“. Jede dieser Schichten übernimmt dabei eine andere Funktion, auf die die nächst höhere Schicht wiederum aufbaut.

Die unterste Schicht ist der physikalische Netzzugangs. In lokalen Netzen ist sind hier die verschiedenen Ethernet-Standard üblich. Wir werden später noch sehen, wie in den Datenpaketen der untersten Schicht tatsächlich auch alle Informationen für die höheren Schichten mit übermittelt werden.

Soll das Ethernet-Datenpaket in ein fremdes Netz versandt werden, wird es sodann von übergeordneten Protokollen, z.B. TCP/IP, adressiert und transportiert.

TCP/IP liefert das Datenpaket schließlich nicht nur beim richtigen Empfänger, sondern auch bei der richtigen Applikation ab, nämlich einem weiteren übergeordneten Protokoll, welches mit einem Anwendungsprogramm zusammenarbeitet. Sie erhalten z.B. eine E-Mail über das Protokoll POP3 und können diese mit Ihrem E-Mail-Programm abrufen.



* DNS und NTP werden in Sonderfällen auch über TCP abgewickelt

1. Physikalische Übertragung

Je nach Anwendungsbereich stehen verschiedene physikalische Vernetzungstechnologien zur Verfügung. Bei lokalen Netzwerken ist Ethernet der heute am meisten verbreitete Netzwerkstandard; bereits 1996 waren ca. 86% aller bestehenden Netzwerke in dieser Technologie realisiert. Der Weg ins Internet wird dagegen mit Hilfe des öffentlichen Telefonnetzes oder des Kabelfernsehnetzes und PPP realisiert.

1.1 Lokale Netze mit Ethernet und Fast-Ethernet

Ethernet ist in der IEEE-Norm 802.3 standardisiert. Vereinfacht gesagt überträgt Ethernet mit Hilfe verschiedener Algorithmen Daten in Paketen über ein Medium an die Teilnehmer des Netzes, die sich jeweils durch eine eindeutige Adresse auszeichnen.

Ethernet-Standards

Im Laufe der Zeit haben sich verschiedene Ethernet-Varianten herausgebildet, die sich maßgeblich anhand von Übertragungsgeschwindigkeit und verwendeten Kabeltypen unterscheiden lassen. Ethernet wurde ursprünglich mit einer Übertragungsgeschwindigkeit von 10 Mbit/s betrieben; hierbei gab es drei verschiedene Grundmodelle:

10Base5

Auch oft als „Yellow Cable“ bezeichnet; stellt den ursprünglichen Ethernet-Standard dar und hat heute keine Bedeutung mehr. Verwendet wurde ein Koaxialkabel; die Reichweite betrug 500m.

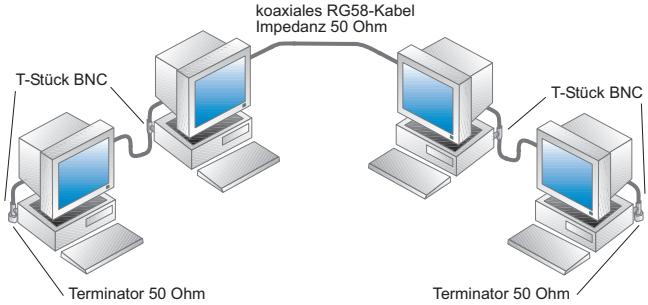
10Base2

wird heute bei Neuinstallationen nicht mehr verwendet und ist nur noch selten in älteren Netzwerkinstallationen zu finden.

10Base2 ist auch bekannt als Thin Ethernet, Cheapernet oder schlicht als BNC-Netzwerk.

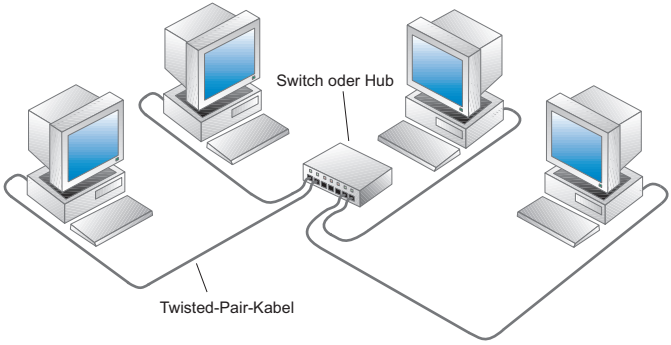
Alle Netzteilnehmer werden parallel auf ein Koaxialkabel (RG58, 50 Ohm Wellenwiderstand) aufgeschaltet. Das Kabel muss an beiden Enden mit einem 50-Ohm-Terminator (Endwiderstand) abgeschlossen sein.

Teilen sich mehrere Geräte einen gemeinsamen Leitungsweg, spricht man auch von einer Bustopologie. Der Nachteil dieser Technik liegt in der hohen Störanfälligkeit. Wird die RG58-Verkabelung an einer beliebigen Stelle unterbrochen, ist der Netzwerkzugriff für alle angeschlossenen Netzteilnehmer gestört.



10BaseT

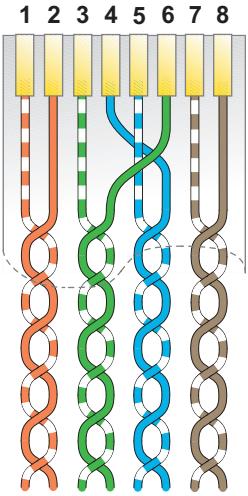
Jeder Netzteilnehmer wird über ein eigenes Twisted-Pair-Kabel an einen sogenannten Hub (Sternverteiler) angeschlossen, der alle Datenpakete gleichermaßen an alle Netzteilnehmer weitergibt.

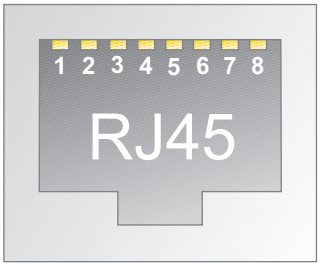


Auch wenn 10BaseT physikalisch sternförmig arbeitet, bleibt von der Logik her das Busprinzip erhalten, da alle angeschlossenen Netzwerkteilnehmer den gesamten Netzwerkver-

kehr empfangen.

Die für 10BaseT verwendeten Twisted-Pair Kabel kommen ursprünglich aus der US-amerikanischen Telefontechnik. Twisted-Pair bedeutet, dass die jeweils für ein Signal verwendeten Kabelpaare miteinander verdrillt sind. Gebräuchlich sind Kabel mit 4 Adernpaaren.





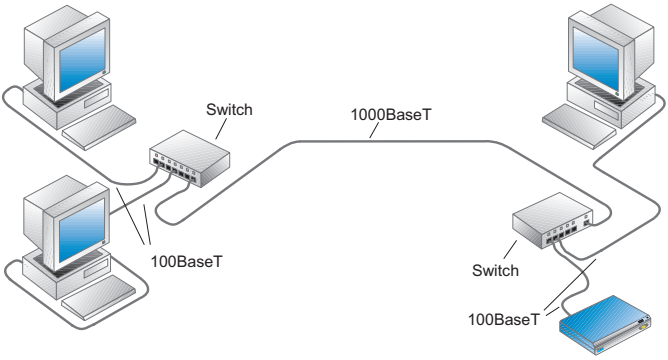
Auch die verwendeten RJ45 Steckverbinder entstammen der amerikanischen Telefontechnik. Die zunächst etwas merkwürdig anmutende Aufteilung der einzelnen Paare und deren Farbgebung ist im AT&T Standard 258 festgeschrieben. 10BaseT benutzt nur die Pins 1 und 2, sowie 3 und 6.

Mit zunehmend größeren Datenmengen wurde in den 90er Jahren Fast Ethernet mit einer Übertragungsgeschwindigkeit von 100Mbit/s eingeführt.

100BaseT

Genau wie bei 10BaseT wird jeder Netzteilnehmer über ein eigenes Twisted-Pair-Kabel an einen Hub oder Switch angeschlossen, der alle Datenpakete an alle Netzteilnehmer weitergibt. Allerdings müssen die Kabel und Komponenten wie Hubs für die höhere Übertragungsrate ausgelegt sein.

1000BaseT - Gigabit Ethernet
ist der nächste Ethernet Standard, mit dem Übertragungsgeschwindigkeiten von einem Gigabit (1000 Megabit) pro Sekunde möglich sind. Um diese hohe Bitrate zu erreichen arbeitet 1000BaseT mit einem speziellen Datenkodierungsverfahren. Die Anforderungen an die Verkabelung sind die gleichen wie bei 100BaseT. Es werden allerdings alle vier Adernpaare der Twisted-Pair-Kabel parallel genutzt.



HUB und Switch
Als sich 10BaseT und 100BaseT als physikalischer Standard für Ethernet-Netzwerke durchgesetzt haben, wurden zunächst nur HUBs als Sternverteiler eingesetzt. HUBs leiten, wie bereits beschrieben, den gesamten Datenverkehr des Netzwerkes an alle angeschlossenen Netzwerkteilnehmer weiter.

Inzwischen werden an Stelle von Hubs ausschließlich Switches eingesetzt. Switches leiten nicht mehr den gesamten Ethernet-Datenverkehr an alle angeschlossenen Netzwerkteilnehmer weiter. Stattdessen filtern Switches den Datenstrom so, dass am entsprechenden Port nur noch die Daten ausgegeben werden, die für den dort angeschlossenen Netzteilnehmer bestimmt sind.

Der Vorteil dieser Technik liegt darin, dass den einzelnen Netzwerkteilnehmern die volle Bandbreite des Anschlusses allein zur Verfügung steht, was vor allem dann zur Geltung kommt, wenn sowohl die übergeordnete Verkabelung als auch der Switch selbst über eine entsprechend höhere Band-

breite verfügen.

Spezielle physikalische Ethernet-Standards

Neben den bis hierhin vorgestellten herkömmlichen Verkabelungsvarianten, gibt es inzwischen weitere Möglichkeiten, Teilnehmer an ein Netzwerk anzuschließen.

PoE - Power over Ethernet

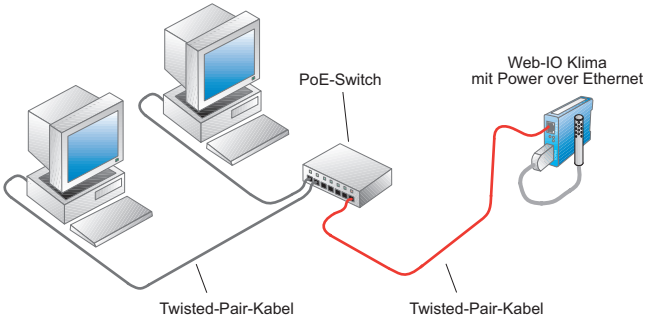
Wenn von Netzwerkteilnehmern gesprochen wird, denken die meisten zunächst an einen PC. Jeder stationäre PC benötigt neben dem Netzwerkkabel zumindest ein weiteres Kabel zur Stromversorgung - meist 230V. Es gibt aber auch Netzwerkteilnehmer, die zum einen deutlich kleiner sind als ein PC und zum anderen mit relativ wenig Versorgungsenergie auskommen.

Mit PoE lassen sich solche Geräte über die ganz normale Ethernet-Verkabelung zusätzlich mit Strom versorgen. Damit das funktionieren kann, wurde die Ethernet-Schnittstelle dieser Geräte entsprechend technisch erweitert. Zum Betrieb sind außerdem spezielle Switches oder PoE-Injektoren nötig, welche die benötigte Energie in das Netzwerkkabel einspeisen.

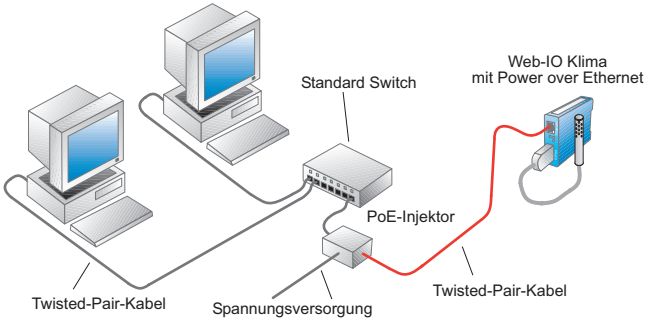
PoE versorgt die Endgeräte mit 48V und kennt z.Zt. 5 verschiedene Leistungsklassen, die sich durch die max. aufgenommene Leistung unterscheiden. Durch ein besonderes Kodierungsverfahren erkennt der PoE-Switch, ob ein angesteckte Gerät PoE-fähig ist oder nicht und schaltet die Versorgung nur bei Bedarf und wenn die benötigte Leistung auch zur Verfügung gestellt werden kann ein.

Klasse	Max. Speiseleistung	Entnahmeleistung	Beispiele für Endgeräte
0	15,4 W	0,44 W - 12,95 W	
1	4,0 W	0,44 W - 3,84 W	W&T Web-IO u. Com-Server
2	7,0 W	3,84 W - 6,49 W	IP-Telefone
3	15,4 W	6,49 W - 12,95 W	Panal PCs
4	15,4 W	wird z.Zt. nicht genutzt	

So können am selben Switch normale Ethernet-Komponenten und PoE-Geräte gemischt betrieben werden.



Wenn die PoE-Versorgung aus einem Switch kommt, spricht man von einer EndSpan-Lösung. In bestehenden Netzwerken können PoE-Geräte aber auch mittels eines zwischengeschalteten PoE-Injektoren mit Strom versorgt werden.



Diesen Fall nennt man MidSpan-Lösung.

100BaseFX - Ethernet über Glasfaser

Bei Kabellängen über 100 Metern oder stark elektromagnetisch gestörtem Umfeld stößt die Übertragungstechnik von 10/100BaseT an ihre Grenzen.

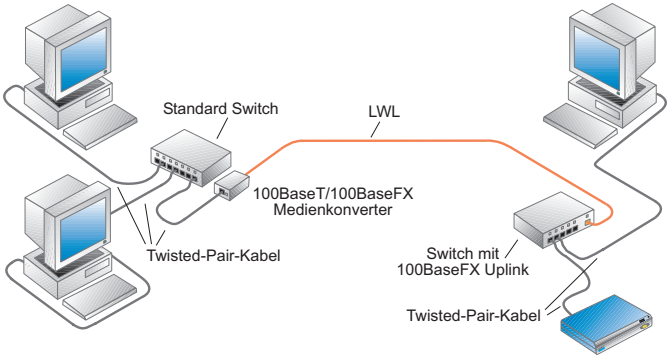
Bei 100BaseFX werden die Ethernet-Daten in Lichtsignale umgesetzt, die über einen Lichtwellenleiter oder kurz LWL weitergeleitet werden. Verwendet werden Glasfaserleitungen mit einem Kerndurchmesser von 50µm oder 62,5µm, wobei für jede Richtung eine einzelne Faser benutzt wird. Auf diese Weise können Distanzen bis 2km überbrückt werden.

Leider gibt es bei der mechanischen Ausführung der LWL-Ste-

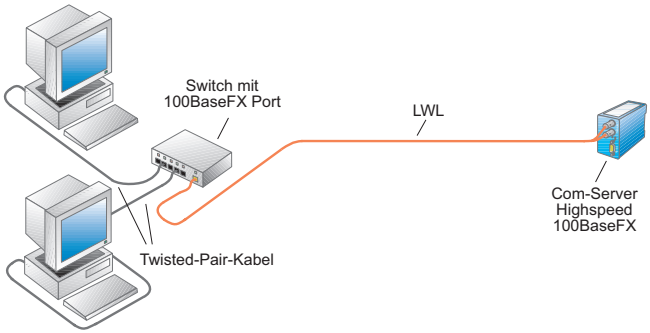
cker verschiedene Standards. Es sollte also bereits bei der Planung von 100BaseFX Netzen oder Netzbereichen geprüft werden, mit welchen Anschlussmöglichkeiten die eingesetzten Komponenten ausgestattet sind

Hochwertige Switches lassen sich optional mit 100BaseFX Ports ausstatten. Alternativ kann ein 100BaseT/100BaseFX-Medienkonverter eingesetzt werden.

Da die Kosten für eine 100BaseFX Installation deutlich über denen von 100BaseT liegen, werden meist nur bestimmte Teile eines Netzwerkes als LWL ausgeführt.



Es gibt aber auch Endgeräte, die bereits von Hause aus mit einem 100BaseFx Port ausgestattet sind. So zum Beispiel der W&T Com-Server Highspeed 100BaseFX.



Solche Lösungen bezeichnet man als „Fiber to the Desk“

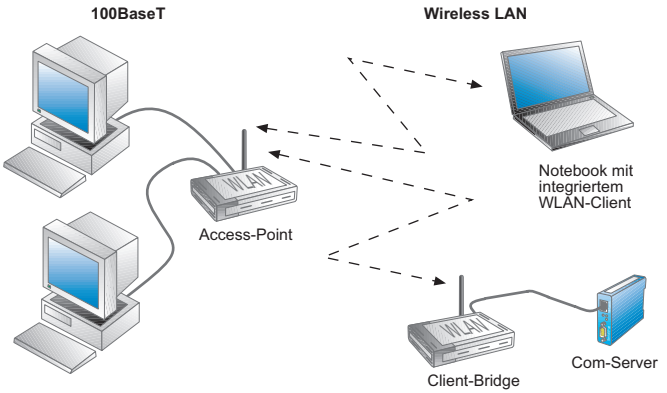
Mehr Details zu 100BaseFX und LWL im Kapitel kleines Netzwerk ABC

Wireless LAN

WLAN realisiert die Netzwerkanbindung über Funk und verschafft dem Nutzer damit Unabhängigkeit vom Kabel und somit Mobilität.

Im Allgemeinen besteht ein WLAN aus mindestens einem Access Point und einem WLAN-Client.

Der Access Point übernimmt die Rolle eines Sternverteilers. WLAN-Clients können sich beim Access Point anmelden und danach über Funk mit dem restlichen Netzwerk kommunizieren.



In den meisten Fällen sind Access Points in DSL-Routern oder Switches integriert und fungieren als Anbindung an ein kabelgebundenes Netzwerk.

Netzteilnehmer, die kein integriertes Wireless LAN Interface haben, können über eine WLAN Client-Bridge Zugang zum WLAN bekommen. Die Client-Bridge fungiert als Medienkonverter zwischen funk- und drahtgebundenem Netzwerk.

Die Reichweite eines WLAN kann je nach Umgebung und eingesetzten Komponenten theoretisch bis zu 300 Meter betragen. Innerhalb von Gebäuden werden typische Werte von 25m angegeben, wobei Geschossdecken und Wände die

Reichweite zusätzlich einschränken können.

Da sich die örtlichen Ausdehnungen von Funknetzwerken überschneiden können, gibt es mehrere mögliche Kanäle (Übertragungsfrequenzen). Bei mehreren WLAN an einem Standort (in Mehrfamilienhäusern oder Geschäftsgebäuden keine Seltenheit) sollte, wenn möglich zwischen 2 benutzten Kanälen ein ungenutzter Kanal liegen, damit es nicht zu gegenseitigen Störungen kommt.

Ein weiterer Aspekt bei WLAN ist die Datensicherheit. Funksignale sind bei entsprechender technischer Ausstattung für jeden, der sich in Reichweite des WLAN befindet empfangbar.

Um Funknetzwerke vor Fremdnutzung und „Mithören“ zu schützen, werden die Daten verschlüsselt. Ein regulärer WLAN Teilnehmer muss sowohl das benutzte Verschlüsselungsverfahren, als auch den richtige Schlüssel anwenden um Zugang zum Funknetz zu bekommen.

Mehr Informationen zum Einrichten von WLAN-Komponenten finden Sie im Kapitel **TCP/IP-Ethernet einrichten**.

Ethernet-Standards im Überblick

Ethernet Standard	Übertragungsmedium	max. Distanz	Datenrate	
10Base2	50Ohm Koaxialkabel	185m	10MBit/s	*
10Base5	50Ohm Koaxialkabel	500m	10MBit/s	*
10BaseT	100Ohm TP-Kabel Kat.3	100m	10MBit/s	
100BaseT	100Ohm TP-Kabel Kat.5	100m	100MBit/s	
1000BaseT/Gigabit	100Ohm TP-Kabel Kat.5	100m	1000MBit/s	
100BaseT-PoE	100Ohm TP-Kabel Kat.5	100m	100MBit/s	
100BaseFX	Multimode LWL	2000m	100MBit/s	
1000BaseSX	Multimode LWL	550m	1000MBit/s	
1000BaseLX	Multimode LWL	550m	1000MBit/s	
1000BaseLX	Monomode LWL	10km	1000MBit/s	
WLAN 802.11a	Funk 5GHz	typisch 25m	max. 54Mbit/s	*
WLAN 802.11b	Funk 2,4GHz	typisch 25m	max. 11Mbit/s	*
WLAN 802.11g	Funk 2,4GHz	typisch 25m	max. 54Mbit/s	*

* Hier müssen sich die Netzwerkteilnehmer die maximale Datenrate teilen.

Bei den anderen Standards steht die angegebene Datenrate jedem Netzteilnehmer zur Verfügung, wenn dieser über einen Switch mit dem Netzwerk verbunden ist.

Verschiedene Ethernet-Standards kombinieren

Alle Ethernet-Standards lassen sich mit Hilfe entsprechender Infrastrukturkomponenten kombinieren bzw. mischen.

So können z.B. verschiedene Gebäudeteile über eine Glasfa-

serverkabelung miteinander verbunden werden. Entsprechende Switches übernehmen die Umsetzung auf 100BaseT oder Gigabit und können bei Bedarf sogar die PoE-Versorgung liefern. WLAN-fähige Geräte können über Einen Access Point oder WLAN-Router an das Netzwerk angebunden werden.

Das Ethernet-Datenformat

Welches physikalische Grundmodell auch genutzt wird – der logische Aufbau der verwendeten Datenpakete ist bei allen Ethernet-Topologien gleich. Die Netzteilnehmer verarbeiten aber nur diejenigen Pakete weiter, die tatsächlich an sie selbst adressiert sind.

Die Ethernet-Adresse

Die Ethernet-Adresse – auch MAC-ID oder Node-Number genannt – wird vom Hersteller in den physikalischen Ethernetadapter (Netzwerkkarte, Printserver, Com-Server, Router ...) fest „eingebrannt“, steht also für jedes Endgerät fest und kann nicht geändert werden. Die Ethernet-Adresse ist ein 6-Byte-Wert, der üblicherweise in hexadezimaler Schreibweise angegeben wird. Eine Ethernet-Adresse sieht typischerweise so aus: 00-C0-3D-00-27-8B.

Jede Ethernet-Adresse ist weltweit einmalig!

Die ersten drei Hex-Werte bezeichnen dabei den Herstellercode, die letzten drei Hex-Werte werden vom Hersteller vergeben.

Das Ethernet-Datenpaket

Es gibt vier verschiedene Typen von Ethernet-Datenpaketen, die je nach Anwendung eingesetzt werden:

Datenpakettyp	*Anwendung*
Ethernet 802.2	Novell IPX/SPX
Ethernet 802.3	Novell IPX/SPX
Ethernet SNAP	APPLE TALK Phase II
Ethernet II	TCP/IP, APPLE TALK Phase I

In Verbindung mit TCP/IP werden in aller Regel Ethernet-Datenpakete vom Typ Ethernet II verwendet

Hier der Aufbau eines Ethernet-II-Datenpakets:

Aufbau eines Ethernet-Datenpakets

⎍⎍⎍...	00C03D00278B	03A055236544	0800	Nutzdaten	Check-summe
Preamble	Destination	Source	Type	Data	FCS

Preamble Die Bitfolge mit stetigem Wechsel zwischen 0 und 1 dient zur Erkennung des Paketanfangs bzw. der Synchronisation. Auch Kollision (überschneidendes Senden zweier Teilnehmer) kann ggf. an der Preamble erkannt werden. Das Ende der Preamble wird durch die Bitfolge „11“ gekennzeichnet.

Destination Ethernet-Adresse des Empfängers

Source Ethernet-Adresse des Absenders

Type Gibt den übergeordneten Verwendungszweck an (z.B. IP = Internet Protocol = 0800h)

Data Nutzdaten

FCS Checksumme

Der Aufbau der anderen Ethernet-Pakete unterscheidet sich nur in den Feldern *Type* und *Data*, denen je nach Pakettyp eine andere Funktion zukommt.

2. Logische Adressierung und Datentransport

Weder Ethernet, noch die gängigen DFÜ-Techniken allein verfügen über die Möglichkeit, verschiedene Netze zu adressieren.

Darüber hinaus arbeitet Ethernet z.B. verbindungslos: Der Absender erhält vom Empfänger keine Bestätigung, ob ein Paket angekommen ist.

Spätestens wenn ein Ethernet-Netzwerk mit mehreren Netzen verbunden werden soll, muss also mit übergeordneten Protokollen – etwa mit TCP/IP – gearbeitet werden.

Bereits in den 60er Jahren vergab das amerikanische Militär den Auftrag, ein Protokoll zu schaffen, das unabhängig von der verwendeten Hard- und Software einen standardisierten Informationsaustausch zwischen einer beliebigen Zahl verschiedener Netzwerke möglich machen sollte. Aus dieser Vorgabe entstand im Jahr 1974 das Protokoll TCP/IP.

Obwohl TCP und IP immer in einem Wort genannt werden, handelt es sich hier um zwei aufeinander aufsetzende Protokolle. Das Internet Protocol IP übernimmt die richtige Adressierung und Zustellung der Datenpakete, während das darauf aufsetzende Transport Control Protocol TCP für den Transport und die Sicherung der Daten zuständig ist.

2.1 TCP/IP im lokalen Netz

Der besseren Übersichtlichkeit halber wollen wir zunächst den Datentransport und die logische Adressierung mit TCP/IP innerhalb eines lokalen Netzes näher beleuchten.

IP - Internet Protocol

Für das Verständnis der Adressierung innerhalb eines lokalen Netzes reicht uns zunächst ein Blick auf die grundsätzliche Struktur des Internet Protocols IP und auf das Address Resolution Protocol ARP, welches die Zuordnung von IP-Adressen zu Ethernet-Adressen ermöglicht.

IP-Adressen

Unter IP hat jeder Netzteilnehmer eine einmalige IP-Adresse, die oft auch als „IP-Nummer“ bezeichnet wird. Diese Internet-Adresse ist ein 32-Bit-Wert, der zur besseren Lesbarkeit immer in Form von vier durch Punkte getrennte Dezimalzahlen (8-Bit-Werten) angegeben wird (Dot-Notation).

192.168. 1. 22

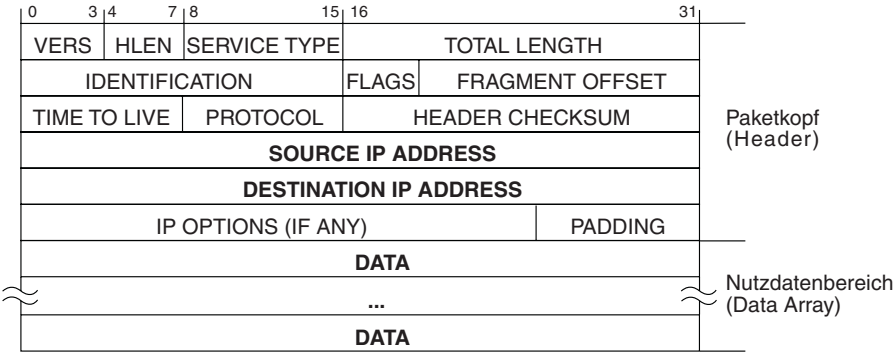
11000000 10101000 00000001 00010110

Eine IP-Adresse muss im gesamten verbundenen Netzwerk einmalig sein!

IP-Datenpakete

Auch bei der Datenübertragung mit IP werden die Nutzdaten in einen Rahmen von Adressierungsinformationen gepackt. IP-Datenpakete enthalten neben den zu transportierenden Nutzdaten eine Fülle von Adress- und Zusatzinformationen, die im sogenannten „Paketkopf“ stehen. Wir beschränken uns hier auf die Erklärung der wichtigsten Adressinformationen.

Aufbau eines IP-Datenpakets



source IP address: IP-Adresse des Absenders
destination IP address: IP-Adresse des Empfängers

ARP – Address Resolution Protocol

Der IP-Treiber übergibt neben dem IP-Datenpaket auch die physikalische Ethernet-Adresse an den Ethernet-Kartentreiber. Zur Ermittlung der Ethernet-Adresse des Empfängers bedient sich der IP-Treiber des Address Resolution Protocol ARP.

In jedem TCP/IP-fähigen Rechner gibt es eine ARP-Tabelle. Die ARP-Tabelle wird vom TCP/IP-Treiber bei Bedarf aktualisiert und enthält die Zuordnung von IP-Adressen zu Ethernet-Adressen.

Internet Address	Physical Address	Type
172.16.232.23	00-80-48-9c-ac-03	dynamic
172.16.232.49	00-c0-3d-00-26-a1	dynamic
172.16.232.92	00-80-48-9c-a3-62	dynamic
172.16.232.98	00-c0-3d-00-1b-26	dynamic
172.16.232.105	00-c0-3d-00-18-bb	dynamic

Soll ein IP-Paket verschickt werden, sieht der IP-Treiber zunächst nach, ob die gewünschte IP-Adresse bereits in der ARP-Tabelle vorhanden ist. Ist dies der Fall, gibt der IP-Treiber die ermittelte Ethernet-Adresse zusammen mit seinem IP-Paket an den Ethernet-Kartentreiber weiter.

Kann die gewünschte IP-Adresse nicht gefunden werden, startet der IP-Treiber einen ARP-Request. Ein ARP-Request ist ein Rundruf (auch Broadcast genannt) an alle Teilnehmer im lokalen Netz.

Damit der Rundruf von allen Netzteilnehmern zur Kenntnis genommen wird, gibt der IP-Treiber als Ethernet-Adresse FF-FF-FF-FF-FF-FF an. Ein mit FF-FF-FF-FF-FF-FF adressiertes Ethernet-Paket wird grundsätzlich von allen Netzteilnehmern gelesen. Als Destination wird die gewünschte IP-Adresse angegeben und im Feld Protocol des Ethernet-Headers die Kennung für ARP ausgewiesen.

Derjenige Netzteilnehmer, der in diesem ARP-Request seine eigene IP-Adresse wiedererkennt, bestätigt das mit einem ARP-Reply. Der ARP-Reply ist ein auf Ethernet-Ebene an

den ARP-Request-Absender adressiertes Datenpaket mit der ARP-Kennung im Protocol-Feld. Im Datenbereich des ARP-Paketes sind außerdem die IP-Adressen von Sender und Empfänger des ARP-Reply eingetragen.

Der IP-Treiber kann nun die dem ARP-Reply entnommene Ethernet-Adresse der gewünschten IP-Adresse zuordnen und trägt sie in die ARP-Tabelle ein.

Im Normalfall bleiben die Einträge in der ARP-Tabelle nicht dauerhaft bestehen. Wird ein eingetragener Netzwerkteilnehmer über eine bestimmte Zeit (unter Windows ca. 2 Min.) nicht kontaktiert, wird der entsprechende Eintrag gelöscht. Das hält die ARP-Tabelle schlank und ermöglicht den Austausch von Hardwarekomponenten unter Beibehaltung der IP-Adresse. Man nennt diese zeitlich begrenzten Einträge auch dynamische Einträge.

Neben den dynamischen Einträgen gibt es auch statische Einträge, die der Benutzer selbst in der ARP-Tabelle ablegt. Die statischen Einträge können genutzt werden, um an neue Netzwerkkomponenten, die noch keine IP-Adresse haben, die gewünschte IP-Adresse zu übergeben.

Diese Art der Vergabe von IP-Adressen lassen auch Com-Server zu: Empfängt ein Com-Server, der noch keine eigene IP-Adresse hat, ein IP-Datenpaket, das auf Ethernet-Ebene an ihn adressiert ist, wird die IP-Adresse dieses Pakets ausgewertet und als eigene IP-Adresse übernommen.

Achtung: Nicht alle Netzwerkkomponenten besitzen diese Fähigkeit. PCs lassen sich auf diese Weise z.B. nicht konfigurieren!

Die Transportprotokolle TCP und UDP

Die Frage, auf welche Art und Weise Daten transportiert werden sollen, lösen Transportprotokolle, die jeweils verschiedenen Anforderungen gerecht werden.

TCP - Transport Control Protocol

Weil IP ein ungesichertes, verbindungsloses Protokoll ist, arbeitet es oft mit dem aufgesetzten TCP zusammen, das die gesicherte Zustellung der Nutzdaten übernimmt. TCP stellt außerdem für die Dauer der Datenübertragung eine Verbindung zwischen zwei Netzteilnehmern her. Beim Verbindungsaufbau werden Bedingungen wie z.B. die Größe der Datenpakete festgelegt, die für die gesamte Verbindungsdauer gelten.

TCP kann man mit einer Telefonverbindung vergleichen. Teilnehmer A wählt Teilnehmer B an; Teilnehmer B akzeptiert mit dem Abheben des Hörers die Verbindung, die dann bestehen bleibt, bis einer der beiden sie beendet.

TCP arbeitet nach dem sogenannten *Client-Server-Prinzip*:

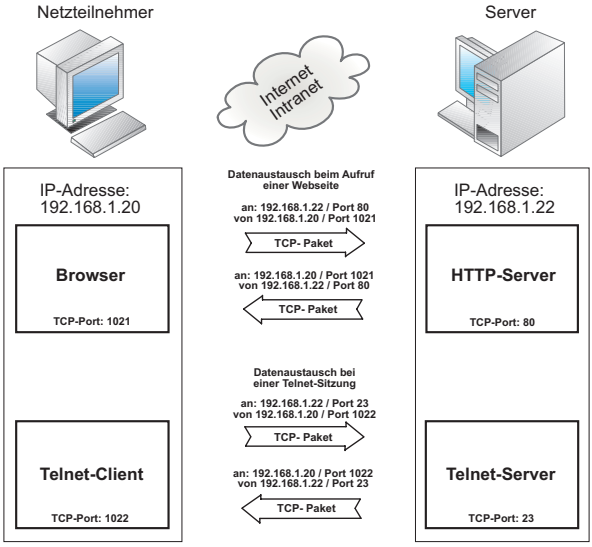
Denjenigen Netzteilnehmer, der eine Verbindung aufbaut (der also die Initiative ergreift), bezeichnet man als Client. Der Client nimmt einen vom Server angebotenen Dienst in Anspruch, wobei je nach Dienst ein Server auch mehrere Clients gleichzeitig bedienen kann.

Derjenige Netzteilnehmer, zu dem die Verbindung aufgebaut wird, wird als Server bezeichnet. Ein Server tut von sich aus nichts, sondern wartet auf einen Client, der eine Verbindung zu ihm aufbaut. Im Zusammenhang mit TCP spricht man von TCP-Client und TCP-Server.

TCP sichert die übertragenen Nutzdaten mit einer Checksumme und versieht jedes gesendete Datenpaket mit einer Sequenznummer. Der Empfänger eines TCP-Pakets prüft anhand der Checksumme den korrekten Empfang der Daten. Hat ein TCP-Server ein Paket korrekt empfangen, wird über einen vorgegebenen Algorithmus aus der Sequenznummer eine Acknowledgement-Nummer errechnet.

Die Acknowledgement-Nummer wird dem Client mit dem nächsten selbst gesendeten Paket als Quittung zurückgegeben. Der Server versieht seine gesendeten Pakete ebenfalls mit einer eigenen Sequenznummer, die wiederum vom Client mit einer Acknowledgement-Nummer quittiert wird. Dadurch ist gewährleistet, dass der Verlust von TCP-Paketen bemerkt wird, und diese im Bedarfsfall in korrekter Abfolge erneut gesendet werden können.

Darüber hinaus leitet TCP die Nutzdaten auf dem Zielrechner an das richtige Anwendungsprogramm weiter, indem es unterschiedliche Anwendungsprogramme – auch Dienste genannt – über unterschiedliche Portnummern anspricht. So ist Telnet z.B. über Port 23, HTTP, der Dienst über den Webseiten aufgerufen werden, über Port 80 zu erreichen. Vergleicht man ein TCP-Paket mit einem Brief an eine Behörde, kann man die Portnummer mit der Raumnummer der adressierten Dienststelle vergleichen. Befindet sich z.B. das Straßenverkehrsamt in Raum 312 und man adressiert einen Brief an eben diesen Raum, dann gibt man damit zugleich auch an, dass man die Dienste des Straßenverkehrsamts in Anspruch nehmen möchte.

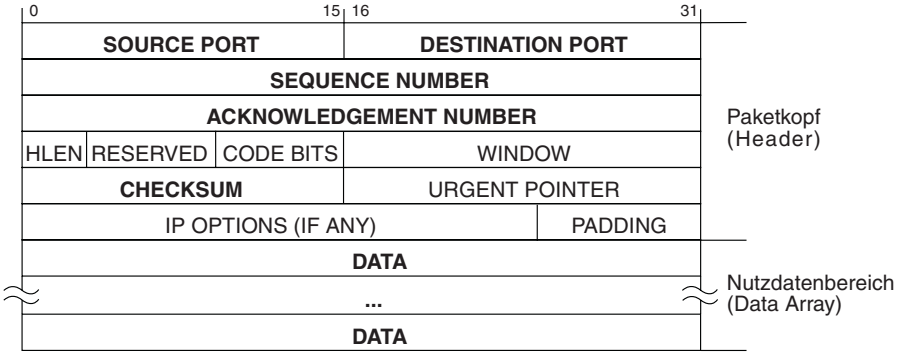


Damit die Antwort des Zielrechners wieder an der richtigen

Stelle ankommt, hat auch die Client-Anwendung eine Portnummer. Bei PC-Anwendungen werden die Portnummern der Client-Anwendungen dynamisch und unabhängig von der Art der Anwendung vergeben.

Auch TCP verpackt die Nutzdaten in einen Rahmen von Zusatzinformationen. Solche TCP-Pakete sind wie folgt aufgebaut:

Aufbau eines TCP-Datenpakets



Source Port: Portnummer der Applikation des Absenders

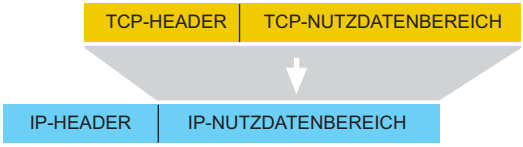
Destination Port: Portnummer der Applikation des Empfängers

Sequence No: Offset des ersten Datenbytes relativ zum Anfang des TCP-Stroms (garantiert die Einhaltung der Reihenfolge)

Acknowl. No: im nächsten TCP-Paket erwartete Sequence No.

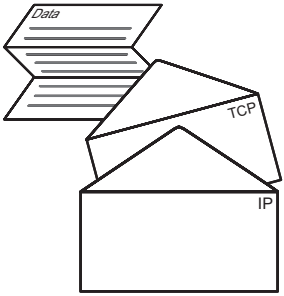
Data: Nutzdaten

Das so entstandene TCP-Paket wird in den Nutzdatenbereich eines IP-Pakets eingesetzt.



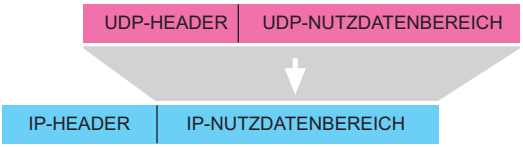
Das IP-Paket hat anschließend folgenden Aufbau:

Die Nutzdaten werden quasi in einen Briefumschlag (TCP-Paket) gesteckt, der wiederum in einen Briefumschlag (IP-Paket) gesteckt wird.



UDP – User Datagramm Protocol

UDP ist ein weiteres Transportprotokoll, das genau wie TCP auf IP aufsetzt.



Das IP-Paket hat anschließend folgenden Aufbau:

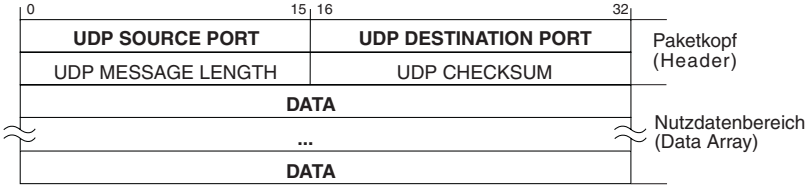
Im Gegensatz zu TCP arbeitet UDP verbindungslos. Jedes Datenpaket wird als Einzelsendung behandelt, und es gibt keine Rückmeldung darüber, ob ein Paket beim Empfänger angekommen ist.

Weil unter UDP aber keine Verbindungen auf- und abgebaut werden müssen und somit keine Timeout-Situationen entste-

hen können, kann UDP jedoch schneller als TCP sein: Wenn ein Paket verlorengeht, wird die Datenübertragung hier eben ungehindert fortgesetzt, sofern nicht ein höheres Protokoll für Wiederholungen sorgt.

Die Datensicherheit ist unter UDP also in jedem Fall durch das Anwendungsprogramm zu gewährleisten.

Aufbau eines UDP-Datenpakets



Source Port: Portnummer der sendenden Anwendung (Rücksende-Port für Empfänger)

Destination Port: Zielport, an den die Daten beim Empfänger übertragen werden sollen

Als Faustregel kann man sagen:

- Für kontinuierliche Datenströme oder große Datenmengen sowie in Situationen, in denen ein hohes Maß an Datensicherheit gefordert ist, wird in aller Regel TCP eingesetzt.
- Bei häufig wechselnden Übertragungspartnern sowie einer Gewährleistung der Datensicherheit durch übergeordnete Protokolle macht der Einsatz von UDP Sinn.

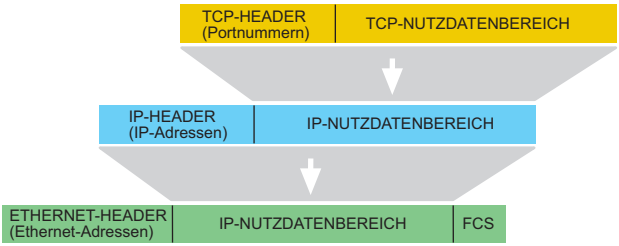
Der Weg eines Zeichens durch das Ethernet

Wir haben nun mit TCP/IP (bzw. UDP/IP) das Handwerkszeug kennengelernt, mit dem Daten adressiert und transportiert werden. Zusammenfassend wird im Folgenden noch einmal der Weg eines Zeichens in einem lokalen Netz aufgezeigt.

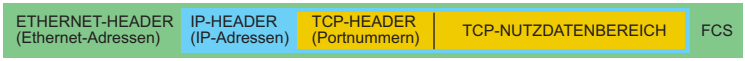
TCP/IP ist ein rein logisches Protokoll und benötigt immer eine physikalische Grundlage. Wie bereits anfänglich er-

wähnt, genießt Ethernet heute die größte Verbreitung bei den physikalischen Netzwerktopologien. So findet man auch in den meisten TCP/IP-Netzwerken Ethernet als physikalische Grundlage.

TCP/IP und Ethernet werden zusammengeführt, indem jedes TCP/IP-Paket in den Nutzdatenbereich eines Ethernet-Paketes eingebettet wird.

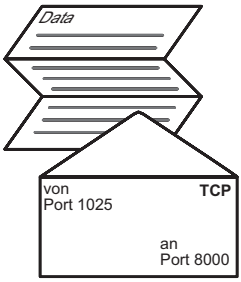


Das komplette Paket sieht dann so aus:

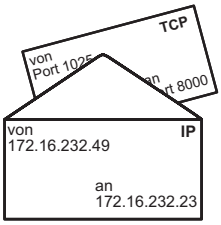


Die Nutzdaten passieren auf ihrem Weg von der Applikation auf dem PC bis ins Netzwerk mehrere Treiberebenen:

- Das Anwendungsprogramm entscheidet, an welchen anderen Netzteilnehmer die Daten gesendet werden sollen, und übergibt IP-Adresse und TCP-Port dem TCP/IP-Treiber (oft auch TCP/IP-Stack genannt).
- Der TCP/IP-Treiber koordiniert den Aufbau der TCP-Verbindung.
- Die vom Anwendungsprogramm übergebenen Nutzdaten werden vom TCP-Treiber je nach Größe in kleinere, übertragbare Blöcke geteilt.
- Jeder Datenblock wird zunächst vom TCP-Treiber in ein TCP-Paket verpackt.

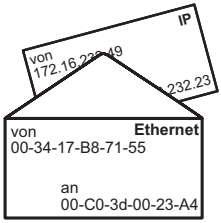


- Der TCP-Treiber übergibt das TCP-Paket und die IP-Adresse des Empfängers an den IP-Treiber.
- Der IP-Treiber verpackt das TCP-Paket in ein IP-Paket.



- Der IP-Treiber sucht in der ARP-Tabelle (Address Resolution Protocol) nach der Ethernet-Adresse des durch die IP-Adresse angegebenen Empfängers (wenn kein Eintrag vorhanden ist, wird zunächst ein ARP-Request ausgelöst) und übergibt das IP-Paket zusammen mit der ermittelten Ethernet-Adresse an den Ethernet-Kartentreiber.

- Der Ethernet-Kartentreiber verpackt das IP-Paket in ein Ethernet-Paket und gibt dieses Paket über die Netzwerkkarte auf das Netzwerk aus.



Beim Empfänger findet die Prozedur in umgekehrter Reihenfolge statt:

- Die Ethernet-Karte erkennt an der Destination-Ethernet-Adresse, dass das Paket für den Netzteilnehmer bestimmt ist und gibt es an den Ethernet-Treiber weiter.

- Der Ethernet-Treiber isoliert das IP-Paket und gibt es an den IP-Treiber weiter.

- Der IP-Treiber isoliert das TCP-Paket und gibt es an den TCP-Treiber weiter.

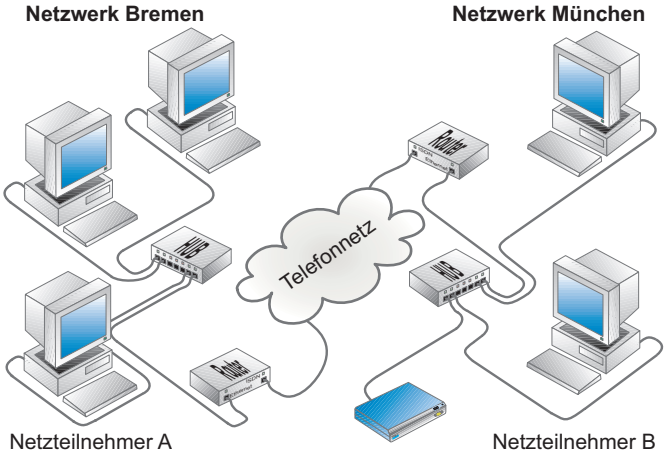
- Der TCP-Treiber überprüft den Inhalt des TCP-Paketes auf Richtigkeit und übergibt die Daten anhand der Portnummer an die richtige Applikation.

Das Beispiel zeigt das Zusammenspiel von logischer Adressierung (TCP/IP) und tatsächlicher physikalischer Adressierung (Ethernet).

Erst dieses Zusammenspiel macht es möglich, netzübergreifend und hardwareunabhängig Daten auszutauschen.

2.2 TCP/IP bei netzübergreifender Verbindung

Das Internet-Protokoll macht es möglich, eine unbestimmte Anzahl von Einzelnetzen zu einem Gesamtnetzwerk zusammenzufügen. Es ermöglicht also den Datenaustausch zwischen zwei beliebigen Netzteilnehmern, die jeweils in beliebigen Einzelnetzen positioniert sind. Die physikalische Ausführung der Netze bzw. Übertragungswege (Ethernet, Token Ring, ISDN....) spielen hierbei keine Rolle.



Die verschiedenen Einzelnetze werden über Gateways/Router miteinander verbunden und fügen sich so zum Internet bzw. Intranet zusammen. Die Adressierung erfolgt nach wie vor über die IP-Adresse, die wir uns nun einmal genauer ansehen werden.

Netzklassen

Die IP-Adresse unterteilt sich in 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. An der Net-ID erkennt man, ob der Empfänger, zu dem die Verbindung aufgebaut werden soll, im gleichen Netzwerk wie der Sender zu finden ist. Stimmt dieser Teil der IP-Adresse bei Sender und Empfänger überein, befinden sich beide im selben Netzwerk; stimmt er nicht überein, ist der Empfänger in einem anderen Netzwerk zu finden.

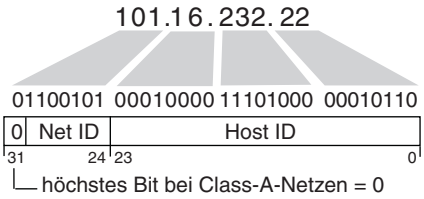
Ähnlich sind auch Telefonnummern aufgebaut. Hier unterscheidet man ebenfalls zwischen Vorwahl und Teilnehmerrufnummer.

Je nachdem, wie groß der Anteil der Net-ID an einer IP-Adresse ist, sind wenige große Netze mit jeweils vielen Teilnehmern und viele kleine Netze mit jeweils wenigen Teilnehmern denkbar. In den Anfängen des Internets hat man den IP-Adressraum anhand der Größe der möglichen Netzwerke in Klassen unterschieden.

Klasse	Adresse	mögliche Netze	mögliche Hosts
Class A	1.xxx.xxx.xxx - 126.xxx.xxx.xxx	127 (2^7)	ca. 16 Millionen (2^{24})
Class B	128.0.xxx.xxx - 191.255.0.0	ca. 16000 (2^{14})	ca. 65000 (2^{16})
Class C	192.0.0.xxx - 223.255.255.xxx	ca. 2 Millionen (2^{21})	253 (2^8)

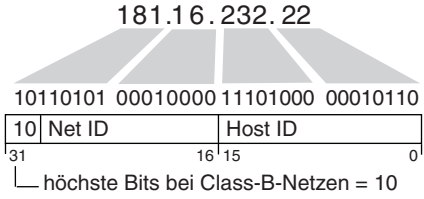
Class A

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



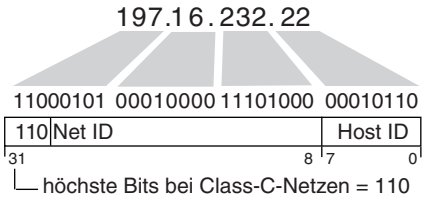
Class B

Die ersten zwei Byte der IP-Adresse dienen der Adressierung des Netzes, die letzten zwei Byte adressieren den Netzteilnehmer.



Class C

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

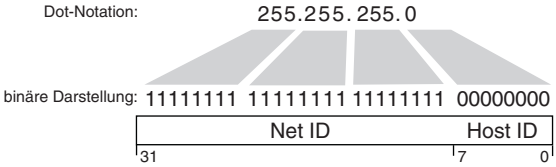


Neben den hier aufgeführten Netzen, gibt es auch noch Class-D- und Class-E-Netze, deren Adressbereiche oberhalb der Class-C-Netze liegen. Class-D-Netze und Class-E-Netze haben in der Praxis wenig Bedeutung, da sie nur zu Forschungszwecken und für Sonderaufgaben verwendet werden. Der normale Internetbenutzer kommt mit diesen Netzwerkklassen nicht in Berührung.

Subnet-Mask

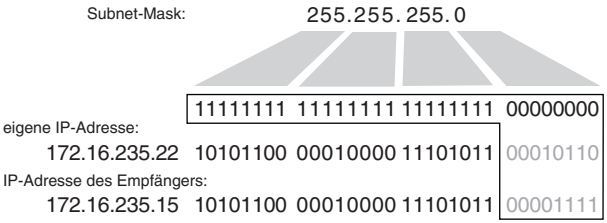
Nun ist es allerdings möglich, ein Netzwerk – egal welcher Netzwerkklasse – in weitere Unternetzwerke zu unterteilen. Zur Adressierung solcher Subnets reicht die von den einzelnen Netzwerkklassen vorgegebene Net-ID allerdings nicht aus; man muss einen Teil der Host-ID zur Adressierung der Unternetze abzweigen. Im Klartext bedeutet dies, dass die Net-ID sich vergrößert und die Host-ID entsprechend kleiner wird.

Welcher Teil der IP-Adresse als Net-ID und welcher als Host-ID ausgewertet wird, gibt die Subnet-Mask vor. Die Subnet-Mask ist genau wie die IP-Adresse ein 32-Bit-Wert, der in Dot-Notation dargestellt wird. Betrachtet man die Subnet-Mask in binärer Schreibweise, ist der Anteil der Net-ID mit Einsen, der Anteil der Host-ID mit Nullen aufgefüllt.



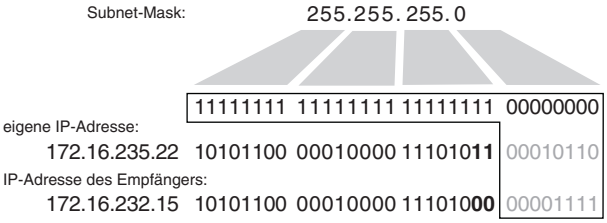
Bei jedem zu verschickenden Datenpaket vergleicht der IP-Treiber die eigene IP-Adresse mit der des Empfängers. Hierbei werden die Bits der Host-ID über den mit Nullen aufgefüllten Teil der Subnet-Mask ausgeblendet.

Sind die ausgewerteten Bits beider IP-Adressen identisch, befindet sich der gewählte Netzteilnehmer im selben Subnet.



Im oben dargestellten Beispiel kann der IP-Treiber die Ethernet-Adresse über ARP ermitteln und diese dem Netzwerkkarten-Treiber zur direkten Adressierung übergeben.

Unterscheidet sich auch nur ein einziges der ausgewerteten Bits, befindet sich der gewählte Netzteilnehmer nicht im selben Subnet.



In diesem Fall muss das IP-Paket zur weiteren Vermittlung ins Zielnetzwerk einem Gateway bzw. Router übergeben werden. Zu diesem Zweck ermittelt der IP-Treiber über ARP die Ethernet Adresse des Routers, auch wenn im IP-Paket selbst nach wie vor die IP-Adresse des gewünschten Netzteilnehmers ein-

getragen ist.

Gateways und Router

Gateways bzw. Router sind im Prinzip nichts anderes als Computer mit zwei Netzwerkkarten. Ethernet-Datenpakete, die auf Karte A empfangen werden, werden vom Ethernet-Treiber entpackt und das enthaltene IP-Paket wird an den IP-Treiber weitergegeben. Dieser prüft, ob die Ziel-IP-Adresse zum an Karte B angeschlossenen Subnet gehört und das Paket direkt zugestellt werden kann, oder ob das IP-Paket an ein weiteres Gateway übergeben wird.

So kann ein Datenpaket auf seinem Weg von einem Netzteilnehmer zum anderen mehrere Gateways/Router passieren. Während auf IP-Ebene auf der gesamten Strecke die IP-Adresse des Empfängers eingetragen ist, wird auf Ethernet-Ebene immer nur das nächste Gateway adressiert. Erst auf dem Teilstück vom letzten Gateway/Router zum Empfänger wird in das Ethernet-Paket die Ethernet-Adresse des Empfängers eingesetzt.

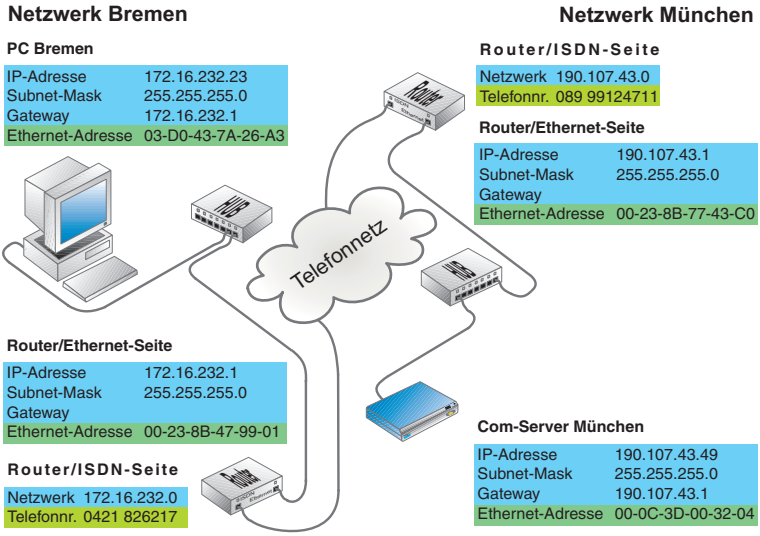
Neben Routern, die ein Ethernet-Subnet mit einem anderen Ethernet-Subnet verbinden, gibt es auch Router, die das physikalische Medium wechseln –z.B. von Ethernet auf Token Ring oder ISDN. Während auch hier die IP-Adressierung über die gesamte Strecke gleich bleibt, ist die physikalische Adressierung von einem Router zum anderen den auf den Teilstrecken geforderten physikalischen Gegebenheiten angepasst.

Zwischen zwei Ethernet-ISDN-Routern wird zum Beispiel über Telefonnummern adressiert.

Der Weg von Daten durch mehrere Netze

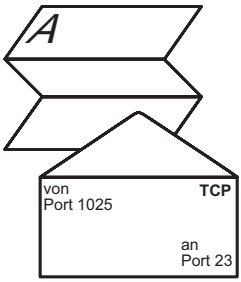
Im folgenden Abschnitt wird anhand einer bestehenden Telnet-Verbindung der Weg eines Zeichens über eine geroutete Netzwerkverbindung beschrieben.

Wir gehen in unserem Beispiel davon aus, dass ein Anwender in Bremen bereits eine Telnet-Verbindung zu einem W&T Com-Server in München aufgebaut hat; die Verbindung der Netze Bremen und München besteht in Form einer Router-Verbindung über das ISDN-Netz.



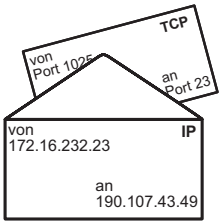
Der Anwender in Bremen gibt in der Telnet-Client-Anwendung das Zeichen „A“ ein.

- Das Telnet-Client-Programm auf dem PC übergibt dem TCP/IP-Stack das „A“ als Nutzdatum. Die IP-Adresse des Empfängers (190.107.43.49) und die Portnummer 23 für Telnet wurden dem TCP/IP-Stack bereits bei Aufbau der Verbindung übergeben.
- Der TCP-Treiber schreibt das „A“ in den Nutzdatenbereich eines TCP-Pakets und trägt als Destination-Port die 23 ein.

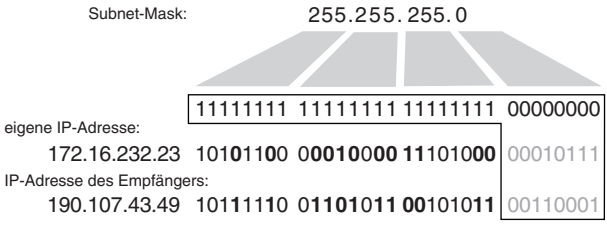


- Der TCP-Treiber übergibt das TCP-Paket und die IP-Adresse des Empfängers an den IP-Treiber.

- Der IP-Treiber verpackt das TCP-Paket in ein IP-Paket.



- Der IP-Treiber ermittelt über den Vergleich der Net-ID-Anteile von eigener IP-Adresse und IP-Adresse des Empfängers, ob das IP-Paket im eigenen Subnet zugestellt werden kann oder einem Router übergeben wird.



Hier sind die Net-ID-Anteile der beiden Adressen nicht gleich; das IP-Paket muss folglich an den eingetragenen Router übergeben werden.

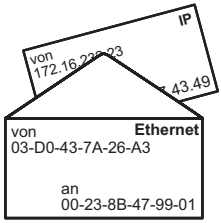
- Der IP-Treiber ermittelt über ARP die Ethernet-Adresse des Routers. Da die TCP-Verbindung bereits aufgebaut ist,

wird die IP-Adresse des Routers bereits in der ARP-Tabelle aufgelöst sein.

```
Internet Address   Physical Address     Type
→ 172.16.232.1     00-23-8B-74-99-01    dynamic
  172.16.232.49    00-c0-3d-00-26-a1    dynamic
  172.16.232.92    00-80-48-9c-a3-62    dynamic
```

- Der IP-Treiber entnimmt der ARP-Tabelle die Ethernet-Adresse des Routers und übergibt sie zusammen mit dem IP-Paket dem Ethernet-Kartentreiber.

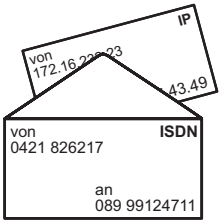
- Der Ethernet-Kartentreiber verpackt das IP-Paket in ein Ethernet-Paket und gibt dieses Paket über die Netzwerkkarte auf das Netzwerk aus.



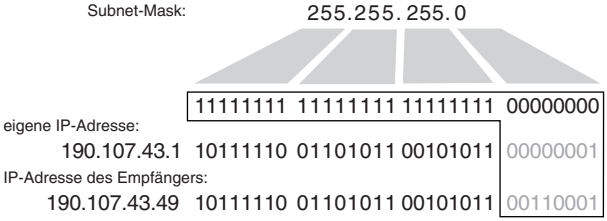
- Der Router entnimmt dem empfangenen Ethernet-Paket das IP-Paket.

- Die IP-Adresse des Empfängers wird mit einer sogenannten Routing-Tabelle verglichen. Anhand dieser Routing-Tabelle entscheidet der ISDN-Router, über welche Rufnummer das gesuchte Netzwerk zu finden ist. Da die TCP-Verbindung bereits besteht, ist vermutlich auch die ISDN-Verbindung zu diesem Zeitpunkt schon aufgebaut. Sollte dies nicht mehr der Fall sein, wählt der Router die der Routing-Tabelle entnommene Rufnummer und stellt die ISDN-Verbindung zum Gegen-Router im Zielnetzwerk wieder her.

- Auch im ISDN-Netz wird das IP-Paket in einen Rahmen von Adressinformationen eingepackt. Für uns ist nur wichtig, dass es in seinem Adressierungsbereich unverändert in das ISDN-Paket übernommen wird.

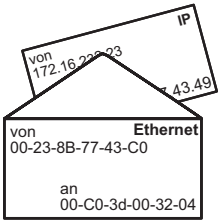


- Der Router im Zielnetz entnimmt dem empfangenen ISDN-Paket das IP-Paket. Über IP-Adressen und Subnet-Mask wird festgestellt, ob das empfangene IP-Paket im lokalen Subnet zugestellt werden kann oder einem weiteren Router übergeben werden muss.



In unserem Beispiel hat das IP-Paket das Zielnetzwerk erreicht und kann im lokalen Netz über Ethernet adressiert werden.

- Der Router, der intern ebenfalls eine ARP-Tabelle führt, ermittelt über ARP die zur IP-Adresse passende Ethernet-Adresse und verpackt das im Adressierungsbereich immer noch unveränderte IP-Paket in ein Ethernet-Paket.



- Der Com-Server erkennt an der Destination-Ethernet-Adresse, dass das Paket für ihn bestimmt ist, und entnimmt das IP-Paket.

- Der IP-Treiber des Com-Servers isoliert das TCP-Paket und gibt es an den TCP-Treiber weiter.

- Der TCP-Treiber überprüft den Inhalt des TCP-Paketes auf Richtigkeit und übergibt die Daten – in diesem Fall das „A“ – an den seriellen Treiber.

- Der serielle Treiber gibt das „A“ auf der seriellen Schnittstelle aus.

Bei einer TCP-Verbindung wird der korrekte Empfang eines Datenpaketes mit dem Rücksenden einer Acknowledgement-Nummer quittiert. Das Quittungspaket durchläuft den gesamten Übertragungsweg und alle damit verbundenen Prozeduren in Gegenrichtung. All dies spielt sich innerhalb weniger Millisekunden ab.

2.3 Exkurs: NAT - Network Address Translation

Möchte man über einen normalen Router ein Netzwerk mit 10 Endgeräten z.B. mittels PPP mit dem Internet verbinden, so würde jedes dieser Endgeräte eine eigene, einmalige IP-Adresse benötigen.

Wie bereits mehrfach angesprochen, sind öffentliche IP-Adressen, d.h. solche, die von der IANA einmalig vergeben werden und daher mit dem Internet verbunden werden können, inzwischen knapp.

Neben diesen öffentlichen IP-Adressen gibt es jedoch noch einen Adressraum für private Netze. Die Bezeichnung „privat“ steht hier für „nicht öffentlich“ und schließt auch Firmennetze mit ein. Je nach Netzwerkgröße sind für private Netze die Adressbereiche vorgesehen.

10.0.0.1 bis 10.255.255.254 für Class A Netze
172.16.0.1 bis 172.31.255.254 für Class B Netze
192.168.0.1 bis 192.255.255.254 für Class C Netze

In diesen Adressbereichen können sich Anwender bei der Einrichtung ihres privaten Netzwerks frei bedienen. Da ein und die gleiche Adresse in mehreren Netzwerken vorkommen kann, sind Adressen aus diesen Bereichen nur innerhalb des eigenen Netzwerkes eindeutig. Somit ist auch kein normales Routing zu diesen Adressen möglich. Genau hier schafft NAT-Routing Abhilfe.

Mit NAT (Network Address Translation) wurde nun eine Art des Routings geschaffen, die es erlaubt, eine Vielzahl von Teilnehmern in einem privaten Netzwerk zum Internet hin mit nur einer öffentlichen IP-Adresse zu repräsentieren.

Zur Erinnerung: Bei normalem TCP/IP-Datenverkehr adressiert die IP-Adresse den Netzwerkteilnehmer, die Portnummer die Anwendung im Gerät.

Beim NAT-Routing wird auch die Portnummer als zusätzliche Adressinformation für das Endgerät selbst mitgenutzt.

Client im privaten Netzwerk

Die Arbeitsweise von NAT-Routing soll hier anhand eines kleinen Beispiels erläutert werden.

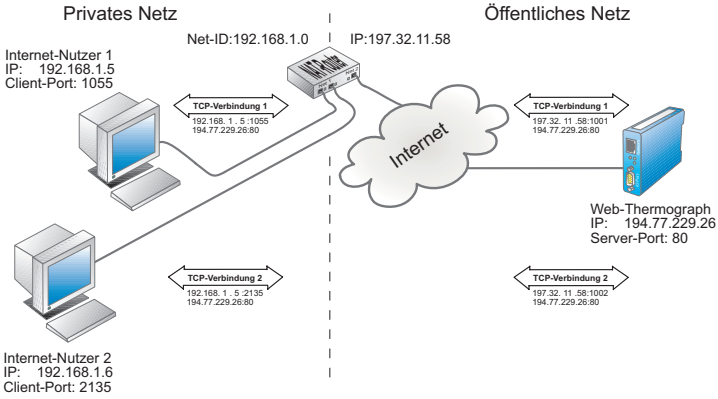
In einem privaten Class C Netzwerk wird im Adressraum 192.168.1.x gearbeitet. Als Übergang zum Internet ist ein NAT-Router im Einsatz, der nach außen mit der IP-Adresse 197.32.11.58 arbeitet.

Der PC mit der netzinternen IP-Adresse 192.168.1.5 baut eine TCP-Verbindung zum W&T Web-Thermographen (IP 194.77.229.26, Port 80) im Internet auf und benutzt dazu den lokalen Port 1055.

Ein zweiter PC mit der IP-Adresse 192.168.1.6 baut ebenfalls eine TCP-Verbindung zum Web-Thermographen auf und benutzt dazu den lokalen Port 2135.

Um mit dem Web-Thermographen verbunden zu werden, wenden sich die PCs zunächst an den NAT-Router.

Der NAT-Router wechselt in den TCP/IP-Datenpaketen, die zum Web-Thermographen weitergesendet werden, die IP-Adresse des jeweiligen PCs gegen seine eigene aus. Auch die vom PC vorgegebene Port-Nr. kann gegen eine vom NAT Router verwaltete Port-Nr. ausgetauscht werden.



Die vergebenen Port-Nr. verwaltet der NAT-Router in einer Tabelle, die folgendermaßen aufgebaut ist:

nach außen Port-Nr.	im privaten Netz zugehörige IP	zugehörige Port-Nr.
1001	192.168.1.5	1055
1002	192.168.1.6	2135

Der Web-Thermograph empfängt also für beide Verbindungen Datenpakete, in denen der NAT-Router als Absender eingetragen ist. Dabei wird aber für jede Verbindung jeweils eine eigene Port-Nr. verwendet.

In alle Datenpakete in Richtung der beiden PCs setzt der Web-Thermograph diese „verbogenen“ Adressinformationen ein. Das bedeutet die TCP/IP-Pakete werden so aufgebaut, dass der NAT-Router der Empfänger ist.

Empfängt der NAT-Router ein solches an ihn adressiertes Datenpaket, stellt er mit Hilfe der Zuordnungstabelle fest, wer der tatsächliche Empfänger ist und ersetzt die empfangenen Adressdaten durch die ursprünglichen netzinternen Verbindungsparameter.

Die Zuordnungstabelle für ausgehende Verbindungen (Client im privaten Netz, Server außerhalb) wird dynamisch verwaltet und kann natürlich deutlich mehr als zwei Verbindungen beinhalten. So können beliebig viele Verbindungen nach außen geroutet werden.

Server im privaten Netzwerk

Die andere Richtung (Server im privaten Netz, Client außerhalb) kann natürlich genauso über NAT abgewickelt werden.

Auch hier wird mit Hilfe einer Zuordnungstabelle bestimmt, zu welchem Endgerät und auf welchen Port eingehende Verbindungsanforderungen bzw. Datenpakete geroutet werden sollen.

Im Gegensatz zu der Zuordnungsliste für ausgehende Verbindung ist die Serverzuordnungsliste aber statisch und muss vom Administrator angelegt und gepflegt werden.

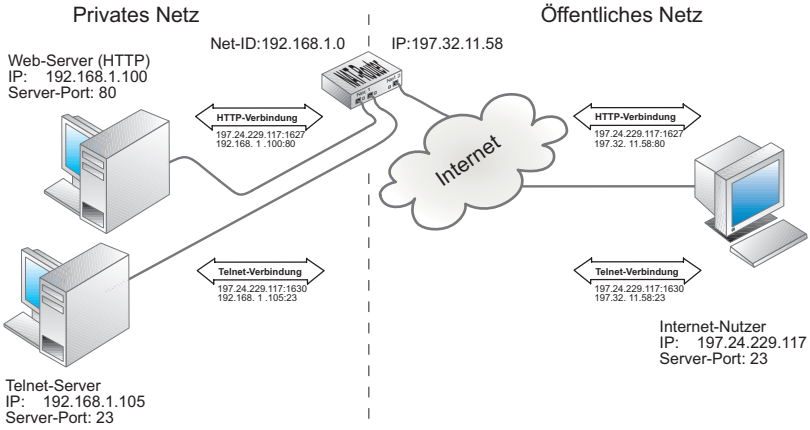
Für jeden Serverdienst, der aus dem öffentlichen Netz zu-

gänglich sein soll, ist ein Eintrag in der Serverliste nötig.

Sollen von außen z.B. ein Web-Server (HTTP = Port 80) und ein Telnet-Server (Telnet = Port 23) erreichbar sein, könnte die Servertabelle so aussehen:

nach außen	im privaten Netz	
Server Port	zugehörige IP	zugehörige Port-Nr
80	192.168.1.100	80
23	192.168.1.105	23

Detaillierte Informationen zu den Protokollen Telnet und HTTP folgen im weiteren Verlauf dieses Buches.



Den Austausch der Verbindungsparameter nimmt der NAT-Router genauso vor, wie bei den im vorhergehenden Abschnitt gezeigten Verbindungen.

In einem privaten Netzwerk, das über einen NAT-Router mit nur einer IP-Adresse zum Internet abgebildet wird, darf natürlich jeder Server-Port nur einmal in der Servertabelle vorkommen. Das bedeutet, dass ein spezieller Serverdienst mit einer spezifischen Port-Nr. nur von einem internen Endgerät angeboten werden kann.

Port Forwarding

Port Forwarding kann als eine erweiterte Form des Nat Routing betrachtet werden. Während beim Nat Routing der nach

außen repräsentierte Port im privaten Netzwerk beibehalten wird, ändert Port Forwarding auch die Portnummer.

Beispiel: Im privaten Netzwerk sind zwei Server mit den IP-Adressen 192.168.1.100 und 192.168.1.105 in Betrieb. Beide Server sind innerhalb des privaten Netzwerks über Port 80 als HTTP-Server erreichbar.

Zusätzlich sollen beide Server auch aus dem Internet erreichbar sein. Das geht natürlich nicht über den gleichen Port. Der Router muss also mindestens einen der Server nach außen über einen abweichenden Port repräsentieren.

nach außen	im privaten Netz	
Server Port	zugehörige IP	zugehörige Port-Nr
80	192.168.1.100	80
81	192.168.1.105	80

Port Forwarding wird allerdings nicht von allen Routern unterstützt.

2.4 VPN - Virtual Private Network

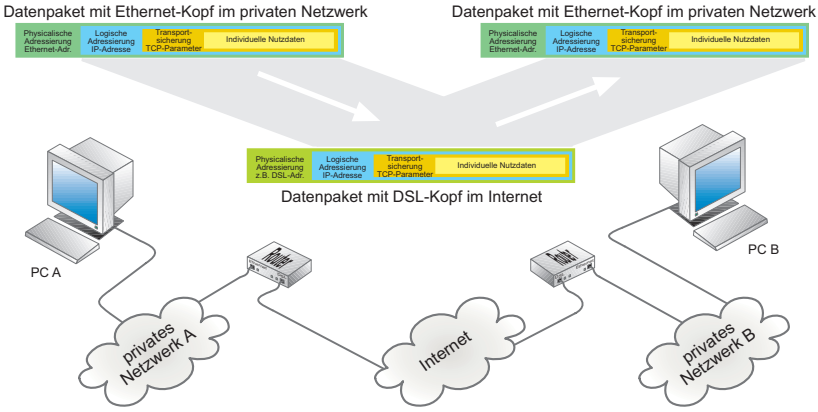
VPN beschreibt die Technik, vertrauliche Netzwerkteile an verschiedenen Standorten über das Internet, also ein öffentliches Netz, miteinander zu verbinden.

Vorweg sei gesagt: Der Einsatz und die Realisierung von VPN erlaubt diverse Varianten. Alle Details von VPN zu beleuchten, bietet genug Stoff für ein eigenes Buch und würde den Rahmen dieses Kapitels sprengen.

An dieser Stelle soll deshalb nur die globale Funktion und die wichtigsten Grundbegriffe von VPN vorgestellt werden.

Exkurs: normales Routing
Zur Erinnerung: Beim normalen Routing haben Quell- und Zielnetzwerk verschiedene Net-IDs. Die Net-IDs sind Bestandteil der IP-Adressen und dienen als Routing-Information. Die Adressen innerhalb des IP-Datenpaketes bleiben über die gesamte Strecke unverändert.

Die physikalischen Adressdaten hingegen wechseln von Teilabschnitt zu Teilabschnitt.



Innerhalb der lokalen Netzwerke erfolgen die Adressierung und der Datentransport über Ethernet, auf Internet-Ebene über DSL und andere physikalische Übertragungsmethoden. Das IP-Paket bleibt dabei über die gesamte, zu überbrücken-

de Strecke unverändert.

Datensicherheit

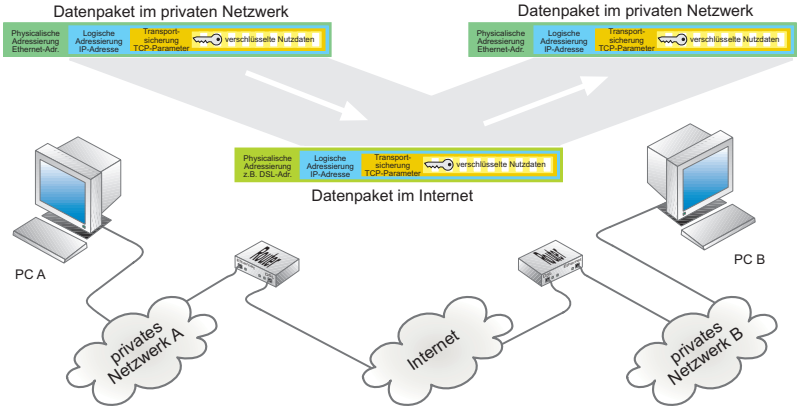
Solange die Übertragungswege durchgängig sind, gelangen die Daten auch mit herkömmlichem Routing zuverlässig von Netzwerk A zu Netzwerk B.

Ein Nachteil bei normaler Netzwerkkommunikation besteht darin, dass die Daten von jedem gelesen werden können, der physikalischen Zugang zu den Übertragungswegen hat. Nicht nur bei z.B. Bankdaten ist also ein erhebliches Sicherheitsrisiko gegeben.

Datenverschlüsselung

Eine Möglichkeit, Daten vor Aushorchen oder Manipulation zu schützen, ist die Verschlüsselung. Beim Verschlüsseln von Daten wird der Datenstrom blockweise, durch mathematische Verknüpfung mit einem Datenschlüssel inhaltlich verändert.

Der vom Versender verwendete Datenschlüssel muss natürlich auch dem Empfänger bekannt sein. So können nach der Übertragung die Originaldaten wieder hergestellt werden. Bei besonders sicherheitsrelevanten Daten wird oft sogar mit mehreren Schlüsseln gearbeitet.



Dritte, die den oder die verwendeten Schlüssel nicht kennen, können den verschlüsselten Datenstrom nicht ohne weiteres lesen bzw. auswerten.

Lesbar sind allerdings die IP und TCP Adressierungsparameter. Dritte die sich Zugriff auf fremde Daten oder ein fremdes Netzwerk verschaffen möchten, sehen anhand dieser Daten zumindest wo das Zielnetzwerk im Inneren ggf. angreifbar ist.

VPN statt normalem Routing

Wie anfänglich bereits gesagt, können mittels VPN zwei Netzwerkteile an verschiedenen Standorten über das Internet bzw. ein öffentliches Netz verbunden werden.

Auch wenn VPN auf die ganz normalen IP-Netzwerkmechanismen aufsetzt, gibt es hinter den Kulissen ganz erhebliche Unterschiede.

Anforderungen an ein VPN

Im Gegensatz zum normalen Routing muss VPN einige zusätzliche Anforderungen erfüllen:

- Authentifizierung
  Für den Zugriff auf den entfernten Netzwerkteil muss die Zugriffsberechtigung nachgewiesen werden.
- Datenintegrität
  Beim Empfang von Daten muss sichergestellt werden, das diese auf dem Transportweg nicht verändert wurden.
- Datensicherheit
  Die übertragenen Daten müssen auf dem Transportweg vor Verfälschung oder Abhorchen durch unberechtigte Dritte geschützt sein.

VPN - Mögliche Topologien

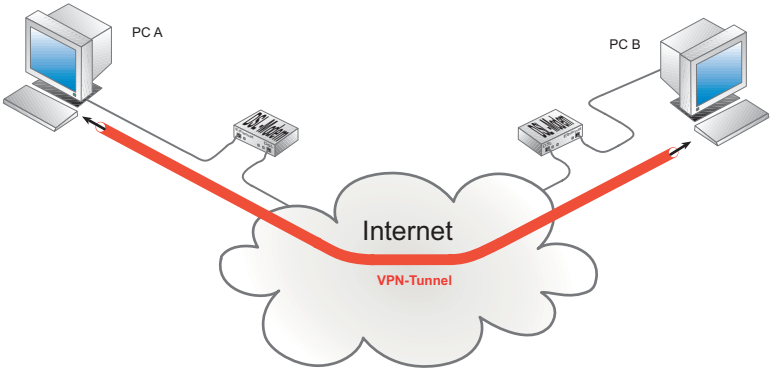
Es gibt drei grundlegende Topologien bei VPN-Lösungen:

- End-to-End
- Site-to-Site
- End-to-Site

Welche Variante zum Einsatz kommt, hängt letztlich davon ab, wie die VPN-Anbindung genutzt werden soll.

VPN - End-to-End

Bei End-to-End Lösungen werden zwei Netzwerkendgeräte über ein öffentliches Netz - z.B. das Internet - so miteinander verbunden, dass sie uneingeschränkt Netzwerkpakete miteinander austauschen können. Die Übertragungsstrecke durch das öffentliche Netz bezeichnet man auch als Tunnel, da der Datenverkehr zwischen den Endgeräten abgegrenzt zum restlichen Netzwerkverkehr abgewickelt wird.

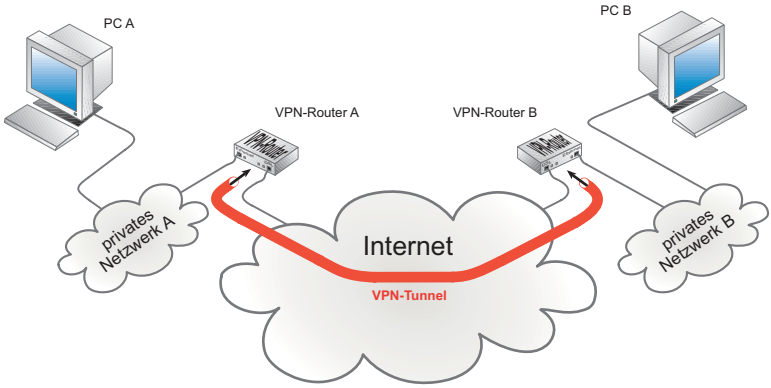


Ein klassisches Beispiel für End-to-End VPN-Anbindung ist das Home-Office. Der heimatliche PC eines Mitarbeiters ist per VPN mit dem Datenbank Server in der Firma verbunden. Der Mitarbeiter kann auf diese Weise zu Hause genauso arbeiten wie im Firmenbüro.

Damit das Ganze funktioniert, muss allerdings auf beiden PCs eine spezielle VPN-Software installiert sein. Ferner muss der PC speziell für den VPN-Zugriff konfiguriert werden.

VPN - Site-to-Site

Mit der VPN-Site-to-Site Technik werden zwei einzelne Netzwerke z.B. über das Internet miteinander verbunden.



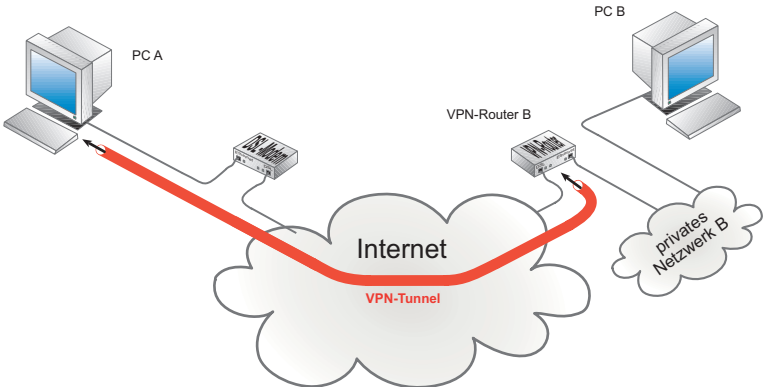
Der VPN-Tunnel wird zwischen zwei speziellen VPN-Routern aufgebaut. Die gesamte VPN-Konfiguration erfolgt in den Routern.

Die einzelnen Teilnehmer im Netzwerk benötigen keine spezielle Software und müssen auch nicht gesondert konfiguriert werden.

Site-to-Site Lösungen werden hauptsächlich zur Verbindung verschiedener Firmenstandorte eingesetzt.

VPN - End-to-Site

Die End-to-Site Lösung bietet einzelnen Endgeräten bzw. PCs Zugang zu einem gesamten Netzwerk am entfernten Standort.



Diese Lösung bietet sich noch besser für die Anbindung von Home-Office-Arbeitsplätzen an. Der Mitarbeiter kann von zu Hause die gesamte Infrastruktur des Firmennetzes nutzen.

VPN - Protokolle

Für die technische Umsetzung von VPN kommen in der Praxis wahlweise drei Protokolle zum Einsatz:

- PPTP - Point-to-Point Tunneling Protocol
- IPsec - IP Security Protocol
- L2TP - Layer 2 Tunneling Protocol

Welches Protokoll zum Einsatz kommt, hängt von der VPN-Topologie und der verwendeten Hard- und Software ab.

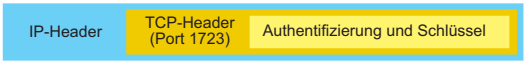
PPTP - Point-to-Point Tunneling Protocol

Ursprünglich wurde PPTP von Microsoft und 3COM entwickelt um abgesetzten PCs über Einwahlleitung Zugriff auf zentrale Server zu ermöglichen. Da PPTP von Hause aus in Windows-Betriebssystemen implementiert ist, erfreut es sich immer noch großer Verbreitung, um End-to-End VPNs zu realisieren. Die Verschlüsselung von PPTP wurde 2012 allerdings gehackt und gilt seit dem nicht mehr als sicher.

Technische Grundlage von PPTP ist das PPP-Protokoll, das unter anderem um eine Datenverschlüsselung und zusätzliche Authentifizierung erweitert wurde.

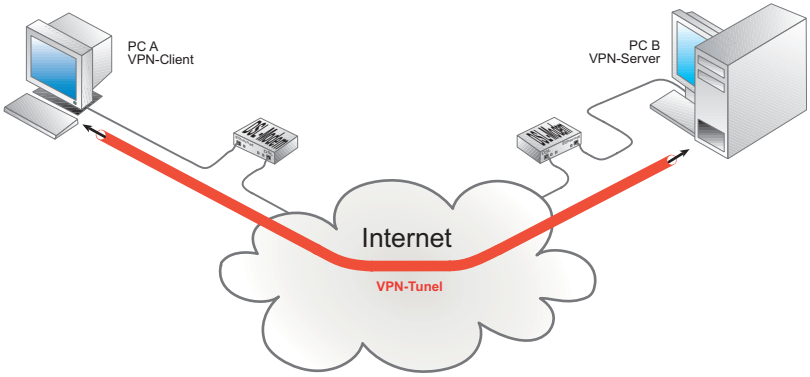
Durch die PPP-Implementierung hat PPTP den Vorteil, neben IP auch andere Protokolle wie z.B IPX (ehemals von Novell und Windows genutzt) übertragen zu können.

PPTP arbeitet zweistufig: Zunächst werden über eine Steuerverbindung auf TCP Port 1723 Authentifizierungs- und Schlüsseldaten ausgetauscht.



Anschließend werden über einen IP-Tunnel die PPP-Daten ausgetauscht. Die PPP-Daten sind dabei im GRE-Protokoll (Generic Route Encapsulation) gekapselt und somit geschützt.

GRE hat den Charakter eines Transportprotokolls und wird direkt in ein IP-Paket eingebettet.



PPTP arbeitet nach dem Client-Server Verfahren. Der VPN-Client meldet sich also mit Aufbau der Steuerverbindung bei einem VPN-Server an.

IPsec - Internet Security Protocol

Im Gegensatz zu PPTP wurde IPsec speziell für die gesicherte Datenübertragung von IP-Datenverkehr über öffentliche Netze bzw. das Internet konzipiert.

Anders als bei PPTP wird bei IPsec nicht der Umweg über PPP-gegangen. Anstelle dessen werden die zu übertragenen Daten in einen IPsec-Rahmen eingebunden. Innerhalb des IPsec-Headers werden mittels AH und ESP (Autentification Header und Encapsulation Security Payload) Informationen zu Autenthifizierung- und Verschlüsselung weitergegeben.

Auch wenn AH und ESP hier der Vollständigkeit halber erwähnt sind, wollen wir die Funktion dieser Techniken hier nicht weiter beleuchten.

Um am Ende des VPN-Tunnels die ursprünglichen Daten wieder herstellen zu können, muss beiden Seiten der entsprechende Schlüssel bekannt sein

Es werden zwei Modi von IPsec unterschieden:

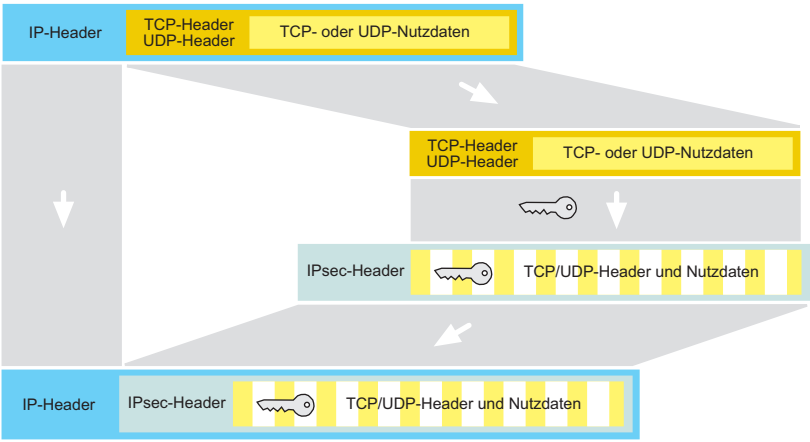
- IPsec-Transportation
  Der Transport von Daten erfolgt über normales Routing, wobei innerhalb des öffentlichen Netzes alle Daten bis auf die IP-Header gegen Fremdzugriff geschützt sind
- IPsec-Tunneling
  Der durch VPN-Tunneling entstandene Netzwerkverbund stellt sich für die Netzwerkbenutzer so dar, wie ein lokales Netzwerk. Der gesamte Datenstrom inklusive IP-Header ist geschützt.

IPsec-Transportation
Der IPsec-Transportation Modus wird bevorzugt bei End-to-End VPN-Lösungen eingesetzt. Damit das funktionieren kann, muss auf den beteiligten PCs eine Software installiert sein, welche das IPsec-Prozedere abwickelt.

Um die Daten gesichert über das öffentliche Netz zu bekommen, entnimmt der IPsec-Treiber den gesendeten TCP/IP-Paketen alle Inhalte, die protokolltechnisch oberhalb des IP-Teils liegen.

Der gesamte TCP- bzw. UDP Teil - also Header und Nutzdaten werden zusammen verschlüsselt und in einen IPsec-Rahmen verpackt.

Der IPsec-Rahmen wird dann in ein IP-Paket eingebaut, wobei die ursprünglichen IP-Adressinformationen erhalten bleiben.

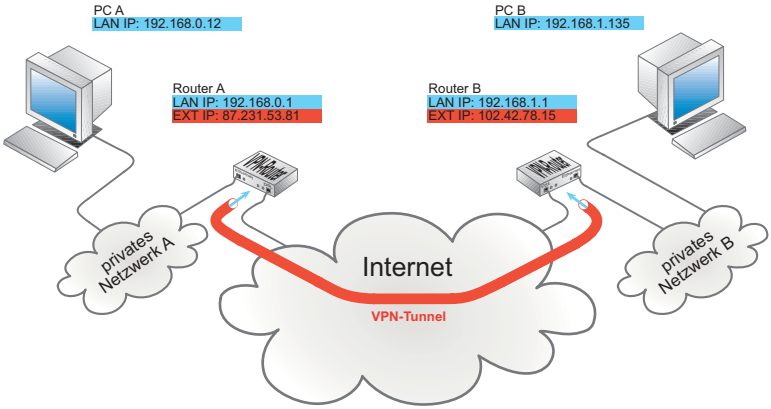


Der Datentransport wird also mittels ganz normalem Routing bewerkstelligt, wobei die transportierten Daten und Port-Informationen geschützt sind.

IPsec-Tunneling

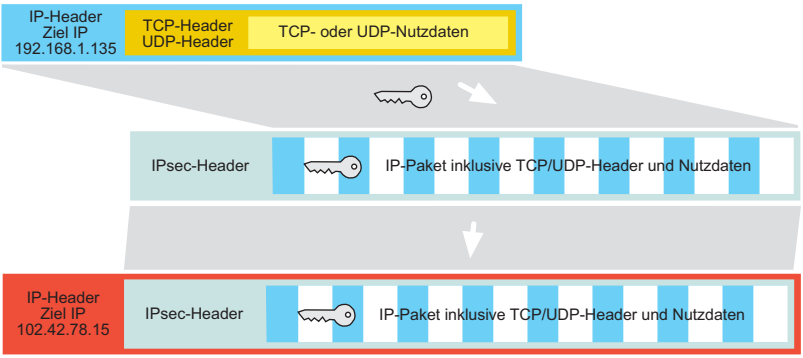
Wie anfänglich bereits gesagt, können mittels IPsec-Tunneling zwei Teilnetzwerke an verschiedenen Standorten über das Internet so verbunden werden, als würden Daten zwischen zwei lokalen Sub-Netzen ausgetauscht (Site-to-Site Lösung).

Die Abwicklung von IPsec übernehmen beim IPsec-Tunneling spezielle Router. Der Vorteil von IPsec-Tunneling gegenüber IPsec-Transportation liegt unter anderem in der Entlastung der beteiligten Endgeräte. Spezielle Treiber sind nicht nötig.



Sendet PC A ein Datenpaket an PC B, wird dieses zunächst von Router A entgegengenommen.

Router A verschlüsselt den gesamten IP-Paketanteil so wie er ist und verpackt ihn in einen IPsec-Rahmen. Der IPsec-Rahmen wird dann in ein neues IP-Datenpaket eingebaut, das an Router B adressiert ist.



Router B entschlüsselt das ursprüngliche IP-Paket und sendet es an PC B.

Für die PCs stellt sich die Datenübertragung so dar als würde der Datenverkehr ganz normal geroutet.

Das Routing innerhalb des Internet erfolgt aber ausschließlich zwischen den beiden VPN-Routern.

Bei Bedarf kann so jedes Endgerät in Netzwerk A Daten mit jedem Endgerät in Netzwerk B Daten austauschen; sicher und so als wäre die Gegenstelle im selben lokalen Netzwerk.

L2TP - Layer 2 Tunneling Protocol

L2TP ist ein reines Tunneling-Protokoll.

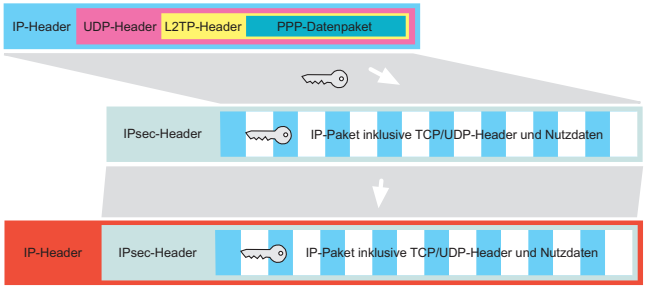
Zur Datenübertragung benutzt L2TP, so wie auch PPTP das PPP-Protokoll. Die PPP-Daten werden mit einem L2TP-Header versehen und in ein UDP-Paket eingebettet.

L2TP übernimmt dabei folgende Aufgaben:

- Auf- und Abbau eines Datentunnels
- Kontrolle ob Daten ihren Empfänger korrekt erreicht haben
- Nummerierung der Datenpakete um beim Empfänger die Daten in die richtige Reihenfolge zu bringen

Allerdings arbeitet L2TP völlig unverschlüsselt. Unbefugte Dritte, die Zugang zu den Übertragungswegen haben, könnten alle Informationen ungehindert lesen. Damit ist L2TP allein für die Realisierung eines VPN-Tunneln nicht geeignet.

Um die nötige Sicherheit zu gewinnen wird L2TP meist zusammen mit IPsec eingesetzt.



Nun könnte man natürlich fragen: Wenn L2TP allein ohnehin nicht sicher ist, warum nicht gleich IPsec nutzen?

- Zum einen gibt es Anwendungen, bei denen innerhalb eines vertraulichen Netzwerkes Daten getunnelt werden sollen - hier bietet L2PT ja alles was benötigt wird.
- Zum anderen kann IPsec nur IP-Pakete tunneln. L2TP hingegen kann wegen des verwendeten PPP-Protokolls auch andere Pakettypen transportieren - mittels IPsec auch verschlüsselt.

3. Protokolle auf Anwendungsebene

Nachdem im vorangegangenen Kapitel die grundlegenden Protokolle der TCP/IP-Datenübertragung erklärt wurden, soll im Folgenden auf die Anwendungsprotokolle eingegangen werden, die auf diese Basisprotokolle aufsetzen.

Bei den Anwendungsprotokollen unterscheidet man zwischen Hilfsprotokollen und tatsächlichen Anwendungsprotokollen.

Hilfsprotokolle werden für Management- und Diagnosezwecke genutzt und laufen oft für den Anwender unsichtbar im Hintergrund ab.

Zu den Hilfsprotokollen zählen:

- DHCP
- DNS
- DDNS
- DynDNS
- ICMP-Ping
- SNMP
- SYSLOG

Anwendungsprotokolle verrichten eine für den Anwender sofort erkennbare Aufgabe oder können direkt durch den Anwender benutzt werden, schaffen also eine Schnittstelle zum Nutzer.

Im Anschluss an die oben genannten Hilfsprotokolle gehen wir in diesem Kapitel noch auf die folgenden Anwendungsprotokolle näher ein:

- Telnet
- FTP
- TFTP
- HTTP
- SMTP
- POP3

3.1 DHCP - Dynamic Host Configuration Protocol

Zur Erinnerung: Jedes Ethernet-Endgerät hat eine weltweit einmalige Ethernet-Adresse (MAC-Adresse), die vom Hersteller unveränderbar vorgegeben wird. Für den Einsatz in TCP/IP-Netzen vergibt der Netzwerkadministrator dem Endgerät zusätzlich eine zum Netzwerk passende IP-Adresse.

Wird kein DHCP benutzt, werden die IP-Adressen „klassisch" vergeben:

- Bei Geräten, die direkte User-Eingaben erlauben (z.B. PCs), kann die IP-Nummer direkt in ein entsprechendes Konfigurationsmenü eingegeben werden.
- Bei „Black-Box-Geräten" (z.B. Com-Servern) gibt es zum einen das ARP-Verfahren über das Netzwerk, zum anderen besteht die Möglichkeit, die Konfigurationsinformation über eine serielle Schnittstelle einzugeben. Darüber hinaus stellen einige Hersteller Tools (z.B. das WuTility-Tool von W&T) zur Verfügung um Embedded Geräte direkt vom PC aus zu konfigurieren

Neben der IP-Adresse müssen als weitere Parameter noch Subnet-Mask und Gateway sowie ggf. ein DNS-Server (mehr dazu im nächsten Kapitel) konfiguriert werden. Bei großen Netzen mit vielen unterschiedlichen Endgeräten bringt das allerdings schnell ein hohes Maß an Konfigurations- und Verwaltungsaufwand mit sich.

Mit DHCP wird dem Netzwerkadministrator ein Werkzeug angeboten, mit dem die Netzwerkeinstellungen der einzelnen Endgeräte automatisch, einheitlich und zentral konfigurierbar sind.

Für die Nutzung von DHCP wird im Netzwerk mindestens ein DHCP-Server benötigt, der die Konfigurationsdaten für einen vorgegebenen IP-Adressbereich verwaltet. DHCP-fähige Endgeräte erfragen beim Booten von diesem Server ihre IP-Adresse und die zugehörigen Parameter wie Subnet-Mask und Gateway. DHCP-Server sehen drei grundsätzliche Möglichkeiten der IP-Adresszuteilung und Konfiguration vor:

Vergabe der IP-Adresse aus einem Adresspool
Auf dem DHCP-Server wird ein Bereich von IP-Adressen festgelegt, aus dem einem anfragenden Netzteilnehmer eine zur Zeit nicht benutzte Adresse zugeteilt wird. Die Zuteilung ist bei diesem Verfahren in aller Regel zeitlich begrenzt, wobei die Nutzungsdauer (Lease-Time) vom Netzwerkadministrator festgelegt oder ganz deaktiviert werden kann. Darüber hinaus lassen sich wichtige Daten (Lease-Time, Subnet-Mask, Gateway, DNS-Server usw.) in einem Konfigurationsprofil hinterlegen, das für alle Endgeräte gilt, die aus dem Adresspool bedient werden.

Vorteile
Geringer Administrationsaufwand;
Anwender können mit demselben Endgerät ohne Konfigurationsaufwand an verschiedenen Standorten ins Netzwerk.

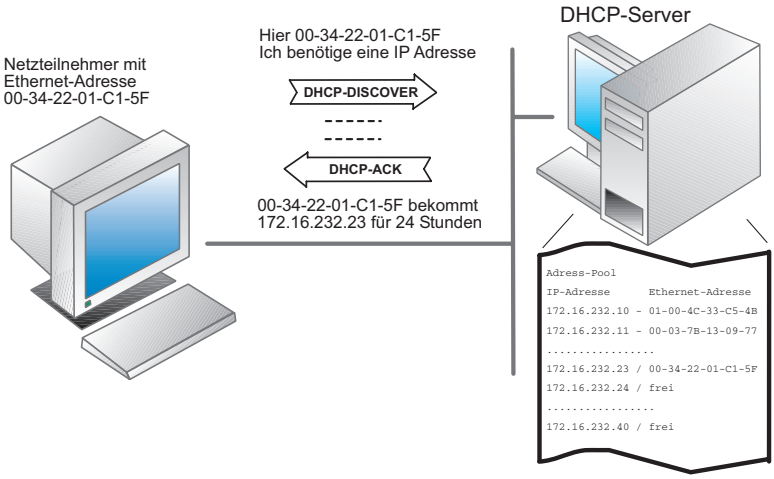
Sofern nicht alle Endgeräte gleichzeitig im Netzwerk aktiv sind, kann die Anzahl der möglichen Endgeräte größer sein als die Zahl der verfügbaren IP-Adressen.

Nachteile
Ein Netzteilnehmer kann nicht anhand seiner IP-Adresse identifiziert werden, da nicht vorhersehbar ist, welche IP-Adresse ein Endgerät beim Start zugewiesen bekommt.

Beispiel: Typische Fälle für die Vergabe von IP-Adressen aus einem Adresspool sind Universitätsnetzwerke. Hier gibt es Netze mit einer fast unbegrenzten Zahl potentieller Anwender, von denen aber nur jeweils wenige tatsächlich im Netzwerk arbeiten. Dank DHCP haben die Studenten die Möglichkeit, ihr Notebook ohne Konfigurationsänderung von einem Labor ins andere mitzunehmen und im Netzwerk zu betreiben.

Um den Administrations- bzw. Konfigurationsaufwand gering zu halten, arbeiten aber auch die meisten Heimnetzwerke (ein DSL-Router, wenige PCs, Drucker und Smartphones) mit DHCP. Die Aufgabe des DHCP-Servers übernimmt hier der

DSL-Router.



Vergabe einer reservierten IP-Adresse

Der Netzwerkadministrator hat die Möglichkeit, einzelne IP-Adressen für bestimmte Endgeräte zu reservieren. Auf dem DHCP-Server wird dazu der IP-Adresse die Ethernet-Adresse des Endgeräts zugeordnet; für jede reservierte IP-Adresse kann außerdem ein individuelles Konfigurationsprofil angelegt werden. Die Angabe einer Lease-Time ist in diesem Fall nicht sinnvoll (aber trotzdem möglich), da die IP-Adresse ohnehin nur vom zugeordneten Endgerät benutzt wird.

Vorteile: Trotz individueller Konfiguration lassen sich alle Netzwerkeinstellungen an zentraler Stelle erledigen und müssen nicht am Endgerät selbst vorgenommen werden.

Endgeräte können gezielt über ihre IP-Adresse angesprochen werden.

Nachteile: Da für jedes Endgerät spezifische Einstellungen angegeben werden müssen, steigt der Administrationsaufwand.

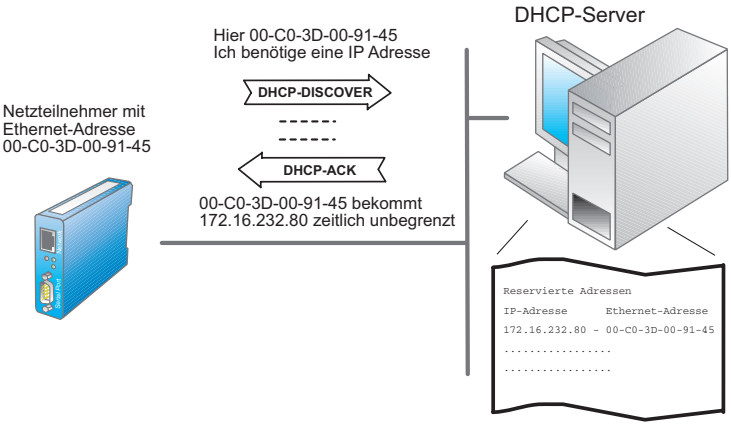
Beim Austausch von Endgeräten muss auf dem DHCP-Server im Konfigurationsprofil

mindestens die Ethernet-Adresse neu eingetragen werden.

Beispiel: Konfiguration von DHCP-fähigen Endgeräten wie Printservern oder Com-Servern, bei denen je nach Einsatzfall eine Adressierung über IP-Adresse benötigt wird. Im DHCP-Manager wird bei der reservierten IP-Adresse die Ethernet-Adresse des zugehörigen Endgerätes eingetragen; die Lease-Time sollte deaktiviert sein. Beim Com-Server können als zusätzliche Parameter Subnet-Mask, Gateway (Router) und DNS-Server angegeben werden.

DHCP-Server unter Windows 2000 vergeben auch auf BootP-Anfragen hin IP-Adressen aus dem normalen Adress-Pool. Diese Eigenschaft lässt sich aber deaktivieren, was Ihr Netzwerkadministrator unbedingt tun sollte!

Hierzu muss ergänzend gesagt werden, dass einige Endgeräte auch das ältere BootP-Protokoll nutzen, um ihre Konfiguration zu erfragen. BootP ist ein Vorläufer von DHCP und wird ebenfalls von DHCP-Servern unterstützt. Allerdings kann BootP nur mit reservierten IP-Adressen arbeiten.



Bei „Black-Box-Geräten“ wie dem Com-Server kann das BootP-Protokoll eingesetzt werden, um in jedem Fall die Übergabe einer reservierten IP-Adresse zu erzwingen. Ist beim DHCP-Server kein zur Ethernet-Adresse des Com-Server passender Eintrag vorhanden, sollte die BootP-Anfrage ignoriert werden und der Com-Server behält die aktuell eingestellte IP-Adresse. Leider handhaben das nicht alle DHCP-Server so und vergeben auch auf einen BootP-Request hin eine IP-Adresse aus dem Adress-Pool.

Ausschluss bestimmter IP-Adressen aus der DHCP-Konfiguration

Für Endgeräte, die weder DHCP- noch BootP-fähig sind, hat der Netzwerkadministrator die Möglichkeit, einzelne IP-Adressen oder auch ganze Adressbereiche von der Vergabe durch DHCP auszuschließen.

Die Konfiguration muss in diesem Fall entweder am Endgerät selbst vorgenommen werden oder durch den Einsatz mitgelieferter Tools erfolgen.

Nachteil: Uneinheitliche und ggf. dezentrale Konfiguration; höherer Administrationsaufwand ist erforderlich.

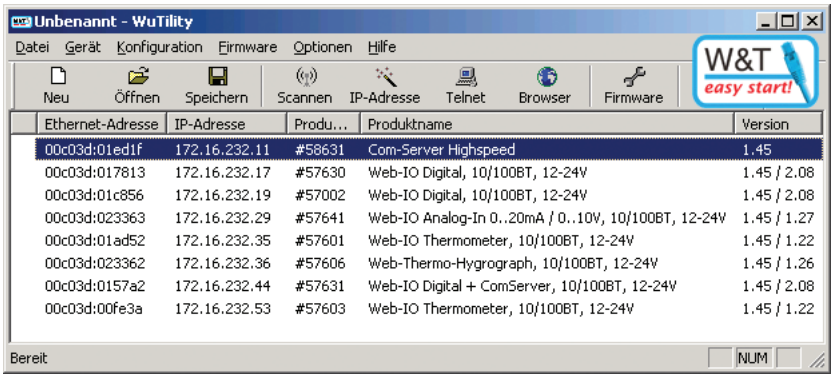
Beispiel: PCs mit älteren DOS-Versionen oder ältere Printserver sind nicht DHCP-fähig und müssen auf jeden Fall „von Hand“ konfiguriert werden.

Alle drei Verfahren können in Netzwerken mit DHCP-Unterstützung nebeneinander angewandt werden.

Natürlich gibt es auch Sonderfälle, in denen es sinnvoll ist, auf DHCP zur Adressvergabe zu verzichten. In technischen Anwendungen gilt es oft neben der Vergabe der IP-Adressdaten noch weitere gerätespezifische Einstellungen vorzunehmen, die ohnehin nicht von DHCP unterstützt werden.

Hier bieten die vom Hersteller mitgelieferten Softwarewerkzeuge in vielen Fällen mehr Komfort als DHCP.

W&T bietet dem Anwender zum Beispiel mit dem *Wutility* Tool ein Werkzeug zur einfachen Inbetriebnahme, Inventarisierung, Wartung und Verwaltung von W&T Geräten wie Com-Servern, USB-Servern, Web-IO Boxen, sowie Mother- und PureBoxen.



Natürlich können auch solche W&T Endgeräte, die ihre IP-Adresse über DHCP bekommen haben, mit Wutility verwaltet werden.

DHCP und Router

Der Informationsaustausch zwischen Endgeräten und DHCP-Servern erfolgt auf physikalischer Ebene in Form von UDP-Broadcasts (Rundrufen ins Netz). Erstreckt sich die DHCP-Konfiguration über mehrere Subnetze gibt es zwei Möglichkeiten:

- Der eingesetzte Router sollte als DHCP-Relay-Agent arbeiten, also das Subnetz-übergreifende Weiterleiten von DHCP-Requests unterstützen.
- Es sollte in jedem Subnetz ein eigener DHCP-Router arbeiten.

3.2 DNS – das Domain Name System

Das Domain Name System ist das Adressbuch des Internet. Obwohl es vom Anwender nur im Hintergrund genutzt wird, ist es doch einer der wichtigsten Internetdienste.

Auf IP-Ebene werden die Millionen von Teilnehmern im Internet über IP-Adressen angesprochen. Für den Nutzer wäre der Umgang mit IP-Adressen aber schwierig: Wer kann sich schon merken, dass das Web-Thermometer von W&T unter der IP-Adresse 194.77.229.26 zu erreichen ist? Einen aussagekräftigen Namen, wie *klima.wut.de,* kann man sich dagegen viel leichter merken.

Schon in den Anfängen des Internet trug man dem Bedürfnis Rechnung, IP-Adressen symbolische Namen zuzuordnen: auf jedem lokalen Rechner wurde eine *Hosts*-Tabelle gepflegt, in der die entsprechenden Zuordnungen hinterlegt waren. Der Nachteil bestand jedoch darin, dass eben nur diejenigen Netzwerkteilnehmer erreichbar waren, deren Namen in der lokalen Liste standen. Zudem nahmen diese lokalen Listen mit dem rapiden Wachstum des Internet bald eine nicht mehr handhabbare Größe an. Man stand also vor der Notwendigkeit, ein einheitliches System zur Namensauflösung zu schaffen. Aus diesem Grund wurde 1984 der DNS-Standard verabschiedet, an dem sich bis heute kaum etwas geändert hat.

Das Prinzip ist einfach. Die Zuordnung von IP-Adressen und Domainnamen wird auf sogenannten DNS-Servern hinterlegt und dort bei Bedarf „angefragt“. Doch ehe wir hier in die Details gehen, noch einige Anmerkungen zum Aufbau von Domain-Namen:

Domainnamen
Das DNS sieht eine einheitliche Namensvergabe vor, bei der jeder einzelne Host (Teilnehmer im Netz) Teil mindestens einer übergeordneten „Top-Level-Domain“ ist.

Als Top-Level-Domain bietet sich ein länderspezifischer Domainname an:

- *.de* für Deutschland
- *.at* für Österreich
- *.ch* für Schweiz usw.

Die Domain kann aber auch nach Inhalt bzw. Betreiber gewählt werden:

- *.com* für kommerzielle Angebote
- *.net* für Netzbetreiber
- *.edu* für Bildungseinrichtungen
- *.gov* ist der US-Regierung vorbehalten
- *.mil* ist dem US-Militär vorbehalten
- *.org* für Organisationen

Alle untergeordneten (Sub-Level-) Domainnamen können vom Betreiber selbst gewählt werden, müssen in der übergeordneten Domain aber einmalig sein. Für jede Top-Level-Domain gibt es eine selbst verwaltende Institution, bei der die Sub-Level-Domains beantragt werden müssen und die damit eine Mehrfachvergabe ausschließt. Für die *de*-Domain ist in solchen Fragen die DENIC (*De*utsches *N*etwork *I*nformation *C*enter; *http://www.denic.de*) zuständig.

Ein Beispiel: *klima.wut.de* setzt sich zusammen aus:

- *de* für Deutschland als Top-Level-Domain
- *wut* für Wiesemann und Theis als Sub-Level-Domain
- *klima* für das Web-Thermometer in der Domain *wut.de*

Der gesamte Domainname darf maximal 255 Zeichen lang sein, wobei jeder Subdomainname höchstens 63 Zeichen umfassen darf. Die einzelnen Subdomainnamen werden mit Punkten getrennt. Eine Unterscheidung zwischen Groß- und Kleinschreibung gibt es nicht. *WWW.WUT.DE* führt Sie genauso auf die Homepage von W&T wie *www.wut.de* oder *www.WuT.de*.

Namensauflösung im DNS

Wie bereits angesprochen, werden auf DNS-Servern (auch Nameserver genannt) Listen mit der Zuordnung von Domain-Namen und IP-Adresse geführt. Gäbe es bei den heutigen Aus-

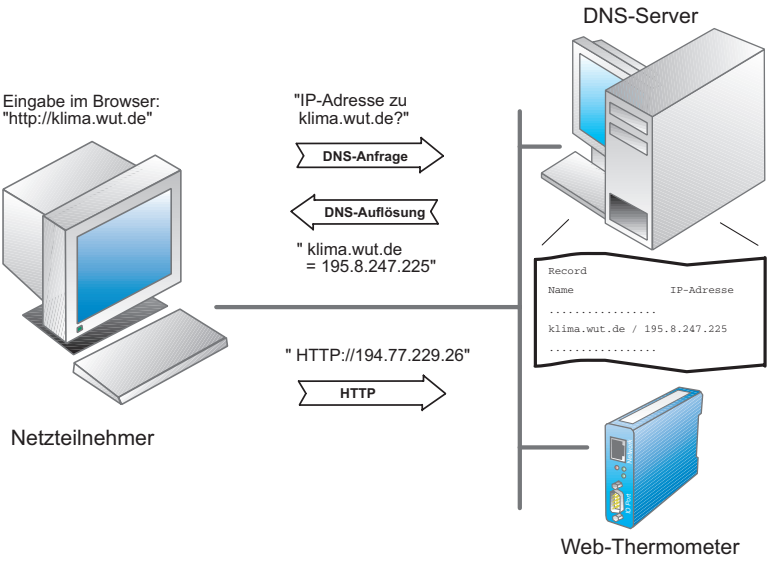
dehnungen des Internets nur einen einzigen DNS-Server, wäre dieser vermutlich mit der immensen Zahl der DNS-Anfragen hoffnungslos überfordert. Aus diesem Grund wird das Internet in Zonen aufgeteilt, für die ein bzw. mehrere DNS-Server zuständig sind.

Netzteilnehmer, die das DNS nutzen möchten, müssen in ihrem TCP/IP-Stack die IP-Adresse eines in Ihrer Zone liegenden DNS-Servers angeben. Um auch bei Ausfall dieses Servers arbeiten zu können, verlangen die üblichen TCP/IP-Stacks sogar die Angabe eines zweiten DNS-Servers.

Welcher DNS-Server für den jeweiligen Netzteilnehmer zuständig ist, erfährt man beim Provider bzw. beim Netzwerk Administrator.

Um Domainnamen in IP-Adressen auflösen zu können, verfügen heutige TCP/IP-Stacks über ein Resolver-Programm. Gibt der Anwender anstatt einer IP-Adresse einen Domainnamen an, startet das Resolver-Programm eine Anfrage beim eingetragenen DNS-Server. Liegt dort kein Eintrag für den gesuchten Domainnamen vor, wird die Anfrage an den in der Hierarchie nächsthöheren DNS-Server weitergegeben. Dies geschieht so lange, bis die Anfrage entweder aufgelöst ist oder festgestellt wird, dass es den angefragten Domainnamen nicht gibt.

Die zum Domainnamen gehörende IP-Adresse wird von DNS-Server zu DNS-Server zurückgereicht und schließlich wieder dem Resolver–Programm übergeben. Der TCP/IP-Stack kann nun die Adressierung des Zielteilnehmers ganz normal über dessen IP-Adresse vornehmen.



Die Zuordnung von IP-Adresse und Domainnamen wird vom TCP/IP-Stack in einem Cache hinterlegt. Diese Cache-Einträge sind dynamisch: Wird der hinterlegte Netzteilnehmer für bestimmte Zeit nicht angesprochen, löscht der Stack den Eintrag wieder. Das hält den Cache schlank und macht es möglich, die zu einem Domainnamen gehörende IP-Adresse bei Bedarf auszutauschen.

DNS in Embedded-Systemen

Nicht alle Embedded-Systeme bieten die Möglichkeit, am Gerät selbst einen Domainnamen einzugeben.

Das ist auch gar nicht nötig, denn das Endgerät muss seinen eigenen Namen gar nicht wissen. Vielmehr wird die Zuordnung von Name und IP-Adresse auch hier auf dem DNS-Server festgehalten. Soll z.B. von einem Client eine Verbindung auf ein als Server arbeitendes Embedded-System aufgebaut werden, erfragt der Client die zum Namen gehörende IP-Adresse wie gehabt beim DNS-Server.

Da Embedded-Systeme aber häufiger in „Maschine-Maschine-Verbindungen“ als in „Mensch-Maschine-Verbindungen“ arbeiten, ist eine direkte Adressierung über IP-Adresse hier

effizienter, da die Zeit für die DNS-Auflösung entfällt.

Die Adressierung über Namen ist bei Embedded-Systemen nur dann sinnvoll, wenn entweder nur der Name bekannt ist (z.B. E-Mail-Adressen) oder mit einem „Umzug“ eines Servers (Name bleibt, IP-Adresse ändert sich) gerechnet werden muss (z.B. Webserver).

DDNS - dynamisches DNS in Verbindung mit DHCP

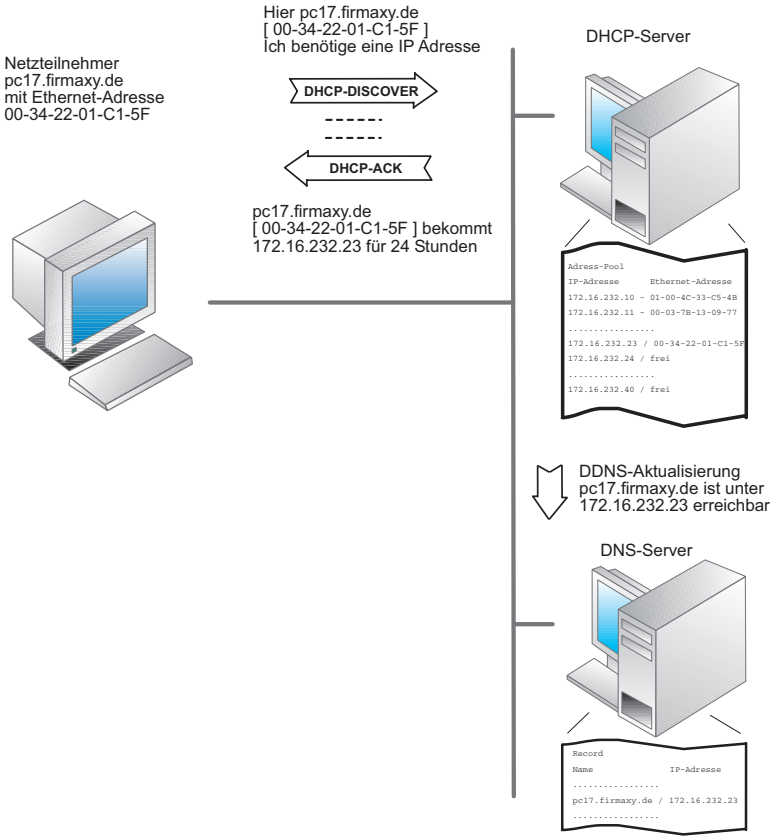
Zusammengefasst kann man sagen: DNS ist eine Art Telefonbuch fürs Netzwerk. Nun hat DNS in seiner Urform die gleichen Nachteile wie ein Telefonbuch. Ändert sich die Telefonnummer eines Teilnehmers, nachdem das Buch gedruckt wurde, kann der Teilnehmer mit Hilfe dieses nun veralteten Telefonbuches nicht mehr erreicht werden.

Die Zuordnungen in DNS-Servern werden natürlich regelmäßig aktualisiert und nicht nur einmal pro Jahr erneuert. Wird aber mit dynamischen IP-Adressen gearbeitet, die mittels DHCP vergeben werden, macht DNS nur Sinn, wenn eine ständige Korrektur der DNS-Listen betrieben wird.

Die Technik des automatischen Abgleiches zwischen DHCP-Server und DNS-Server wird als DDNS - dynamisches DNS bezeichnet.

DDNS ist kein Standard TCP/IP Dienst.

Auf welchem Weg und in welcher Form die Synchronisation zwischen DHCP-Server und DNS-Server erfolgt, hängt davon ab, unter welchem Betriebssystem die Server laufen.



Der prinzipielle DDNS-Ablauf bei Vergabe einer IP-Adresse via DHCP verläuft folgendermaßen:

1. Das Endgerät versucht vom DHCP-Server eine IP-Adresse zu beziehen. Dabei ist der Host-Name des Gerätes (hier pc17.firmaxy.de) im Endgerät fest konfiguriert.
2. Der DHCP-Server vergibt eine IP-Adresse aus seinem Address-Pool an das Endgerät und trägt die Zuordnung zur Ethernet-Adresse in die Adressverwaltung ein.
3. Zusätzlich übergibt der DHCP-Server dem DNS-Server IP-Adresse und Host-Namen des Endgerätes.
4. Der DNS-Server aktualisiert die Namensverwaltung mit dem neuen Eintrag.

Bei dem gezeigten Ablauf spielt es keine Rolle, ob DNS-Server

und DHCP-Server auf zwei getrennten Rechnern oder auf einer gemeinsamen Hardware laufen.

Da die DDNS-Kopplung vom Netzwerkadministrator eingerichtet werden muss, kommt DDNS nur in abgeschlossenen Netzen wie z.B. Firmen-Netzen zum Einsatz.

Dynamisches DNS

Nicht nur in lokalen Netzen, in denen die IP-Adressvergabe der DHCP -Server abwickelt, wird mit dynamischen IP-Adressen gearbeitet.

Zur Erinnerung: In Netzen, die miteinander verbunden sind, man spricht auch von WAN (Wide Area Network), muss jedes angeschlossene Endgerät eine einmalige IP-Adresse haben.

Diese Regel gilt auch für das Internet, welches den mit Abstand größten Netzwerkverbund darstellt.

Der größte Teil der Internet-Nutzer ist nur zeitweise über einen Zugang bei einem Provider mit dem Internet verbunden. Ähnlich wie bei DHCP teilt der Provider dem verbundenen Endgerät für die Dauer der Nutzung eine IP-Adresse zu. Diese IP-Adresse wird voraussichtlich bei jeder Internet-Nutzung eine andere sein.

Da die meisten Internet-Nutzer nur Server-Dienste (E-Mail, Abruf von Webseiten, ...) in Anspruch nehmen, also Verbindungen zu diesen Servern aufnehmen, ist das kein Problem.

Soll aber das Endgerät des Internet-Nutzers (meist ein PC) auch für andere Internet-Nutzer erreichbar sein, ist die dynamische IP-Adresse ein Problem, da die aktuell zugeteilte IP-Adresse ja nur dem Provider und dem dort angekoppelten Endgerät bekannt ist.

Um dieses Problem zu umgehen gibt es zwei Möglichkeiten:

1. Permanenter Anschluss an das Internet

Feste Internet-Zugänge mit einer festen IP-Adresse sind aber ungleich teurer als z.B. normale DSL- oder Modem-Zugänge.

Diese Lösung bietet sich deshalb nur für größere Firmen an.

2. Verwendung von Dynamischem DNS

Einer der ersten Anbieter für dynamisches DNS war die Organisation DynDNS. In der Vergangenheit konnte man bei DynDNS nach einmaliger Anmeldung kostenlos einen weltweit einmaligen Hostnamen registrieren lassen.

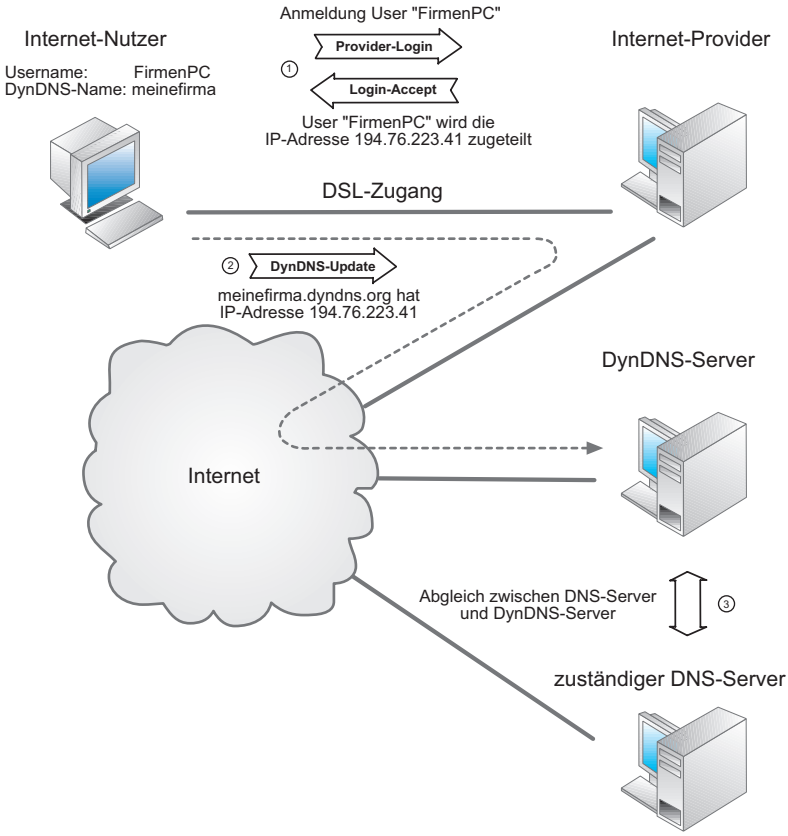
Heute ist dieser Dienst leider kostenpflichtig.

Eine detaillierte Beschreibung der Vorgehensweise ist auf den Webseiten von DynDNS unter *http://www.dyndns.org* verfügbar.

Die Abwicklung der Adressauflösung mittels DynDNS erfolgt in drei Schritten.

1.) Der Internet-User stellt z.B. via DSL eine Verbindung zu seinem Internet-Provider her und bekommt nach erfolgreichem Login eine IP-Adresse zugeteilt.
2.) Im Gegensatz zu DDNS muss der Anwender bzw. sein Endgerät dafür sorgen, dass DynDNS weiß, unter welcher IP-Adresse das Endgerät erreichbar ist. Dazu nutzt das Endgerät den DynDNS-Update-Client. Für PC gibt es entsprechende Programme, die diese Aufgabe übernehmen. Andere Endgeräte müssen spezielle Funktionen integriert haben. Bei Zugang zum Internet über einen Router, übernimmt dieser meist auch das DynDNS-Update.
3.) Erfolgt nun bei einem DNS-Server die Anfrage nach dem vom Internet-User benutzten DynDNS-Namen und der zugehörigen IP-Adresse, fragt der zuständige DNS-Server diese beim DynDNS-Server an und gleicht seine Daten ab.

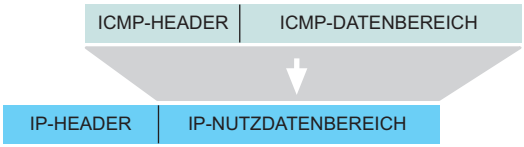
Damit ist das Endgerät unter dem gewählten Namen weltweit ansprechbar, kann also auch Server-Dienste anbieten.


Anmeldung User "FirmenPC"
Internet-Nutzer
Provider-Login
Internet-Provider
Username: FirmenPC
DynDNS-Name: meinefirma
1
Login-Accept
User "FirmenPC" wird die
IP-Adresse 194.76.223.41 zugeteilt
DSL-Zugang
2
DynDNS-Update
meinefirma.dyndns.org hat
IP-Adresse 194.76.223.41
DynDNS-Server
Internet
Abgleich zwischen DNS-Server
und DynDNS-Server
3
zuständiger DNS-Server

3.3 Ping – Erreichbarkeit prüfen

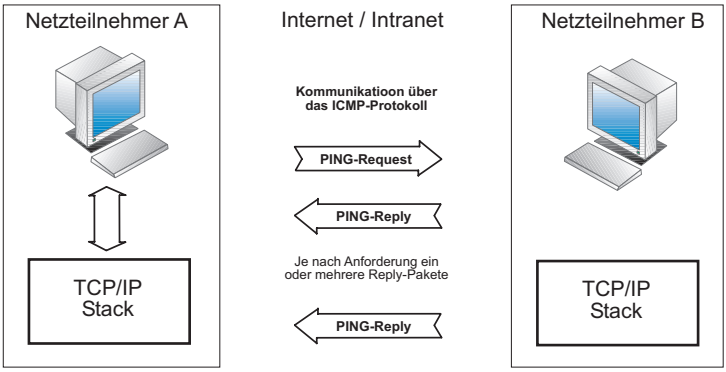
Die Ping-Funktion dient in TCP/IP-Netzen zu Diagnosezwecken. Mit Hilfe von Ping lässt sich überprüfen, ob ein bestimmter Teilnehmer im Netz existiert und tatsächlich ansprechbar ist.

Ping arbeitet mit dem ICMP-Protokoll, welches auf das IP-Protokoll aufsetzt.



Das Paket sieht dann so aus:

Setzt ein Netzteilnehmer durch Eingabe des Ping-Kommandos einen ICMP-Request ab, gibt die angesprochene Station einen ICMP-Reply an den Absender zurück.



Der Aufruf des Kommandos *PING <IP-Adresse>* in der DOS-Box fordert den durch die IP-Adresse angegeben Netzteilnehmer auf, eine Rückmeldung zu geben.

Zusätzlich können unter Windows noch diverse Parameter angegeben werden:

-t
Wiederholt das Ping-Kommando in Dauerschleife, bis der Anwender mit <Strg> C unterbricht.

-n count
Wiederholt das Ping-Kommando „count“ mal.

-l size
„size“ gibt an, mit wieviel Byte das ICMP-Packet aufgefüllt wird. Bei Com-Servern in Default-Einstellung sind dies maximal 560 Byte.

-w timeout
„timeout“ spezifiziert, wie lange (in Millisekunden) auf die Rückmeldung gewartet wird.

Ein Beispiel:

```
PING 172.16.232.49 -n 50
```

sendet 50 Ping-Kommandos an die Station 172.16.232.49.
Ist der Netzteilnehmer vorhanden, erscheint folgende Rückmeldung:

```
Reply from 172.16.232.49: bytes=32 time=10ms TTL=32
```

Bleibt die Rückmeldung aus, wird folgende Meldung zurückgegeben:

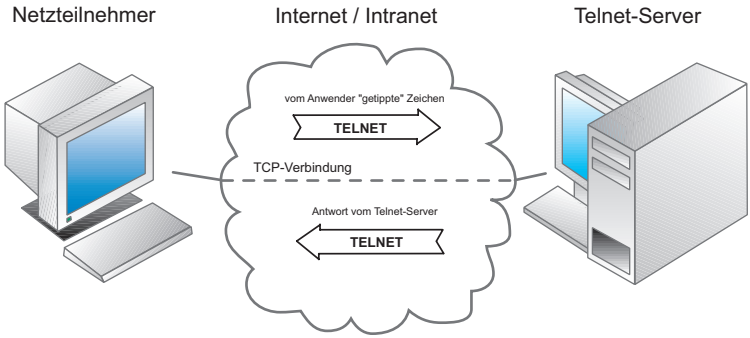
```
Request timed out.
```

Anstelle der IP-Adresse kann natürlich auch ein Host-Name eingegeben werden. Die Voraussetzung hierzu ist der Zugang zu einem DNS-Server.

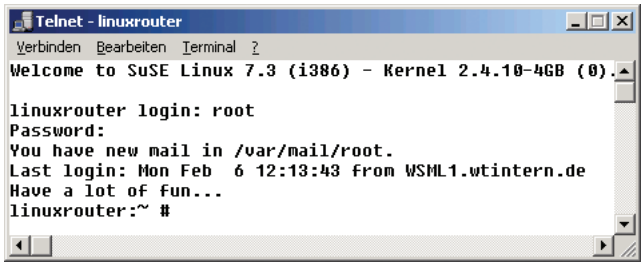
Die von Ping verwendeten ICMP-Pakete sind im Internet-Standard RFC-792 definiert.

3.4 Telnet - Terminal over Network

Einfach ausgedrückt ist Telnet ein Textfenster bzw. textorientiertes Programm, über das ein anderer Rechner (Host) im Netzwerk vom Anwender fernbedient werden kann.



Eine Telnet-Sitzung kann man sich vorstellen wie eine DOS-Box, allerdings werden die eingetippten Befehle auf dem entfernten Rechner ausgeführt.



Dafür werden mehrere Elemente benötigt.

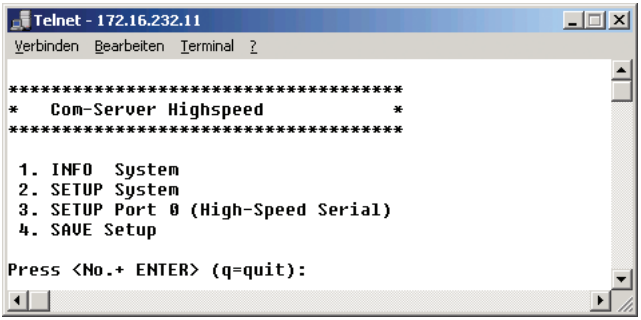
Der Telnet Client

Alle modernen Betriebssysteme verfügen heute über ein Telnet-Clientprogramm. Bei Windows7 muss der Telnet Client allerdings erst aktiviert werden. Das erfolgt in der Systemsteuerung über *Programme und Funktionen >> Windows-Funktionen aktivieren oder deaktivieren >> Telnet-Client.*

Der Telnet-Client baut eine TCP-Verbindung zu einem Telnetserver auf, nimmt Tastatureingaben vom Anwender entge-

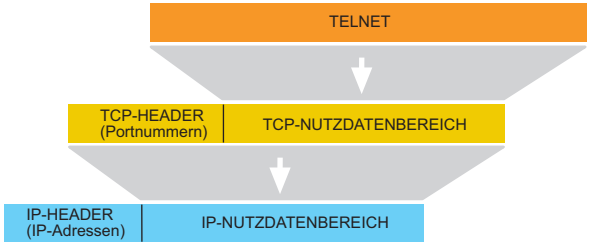
gen, gibt sie an den Telnetserver weiter und stellt die vom Server gesendeten Zeichen auf dem Bildschirm dar.

Der Telnet-Server
ist auf dem entfernten Rechner aktiv und gibt einem oder ggf. mehreren Nutzern die Gelegenheit sich dort „einzuloggen“. Damit ist der Telnet-Server (in Unix Systemen auch oft als Telnet-Daemon bezeichnet) das Bindeglied zwischen Netzwerkzugang via Telnet-Client und dem zu bedienenden Prozess. In seinem Ursprung wurde Telnet eingesetzt, um einen Remote-Zugang zu UNIX-Betriebssystemen zu schaffen. Es verfügen auch viele Embedded-Systeme wie Com-Server oder Printer-Server, Switches, Hubs und Router über einen Telnet-Server, der als Konfigurationszugang dient.



3.4.3 Das Telnet Protokoll

Auch Telnet setzt auf TCP als Basisprotokoll auf.



Das Telnet-Datenpaket sieht dann so aus:

Hierbei wird, wenn vom Anwender nicht anders vorgegeben,

der Port 23 genutzt. Es kann aber auch jeder beliebige andere Port angegeben werden. Wichtig ist, dass auf dem gewählten Port ein Telnet-Server aktiv ist.

Das Telnet Protokoll übernimmt im Wesentlichen drei Aufgaben:

1. Festlegung benutzter Zeichensätze und Steuercodes zur Cursor-Positionierung

   Als gemeinsame Basis für Client und Server wird hierzu der NVT-Standard „Network Virtual Terminal“ eingesetzt. NVT benutzt den 7Bit ASCII Zeichensatz und legt fest, welche Zeichen dargestellt werden und welche zur Steuerung und Positionierung genutzt werden.

2. Aushandeln und Einstellen von Verbindungsoptionen

   Über die Festlegungen im NTV hinaus kann Telnet von einer Vielzahl spezieller Funktionen Gebrauch machen. Das Telnet-Protokoll gibt Client und Server die Möglichkeit Verbindungsoptionen auszuhandeln. Zum Beispiel: ob der Server alle vom Client empfangenen Zeichen als Echo zurückgeben soll.

   Hierzu werden Steuerzeichen benutzt, bei denen das 8. Bit gesetzt ist, also Zeichen oberhalb 127 und damit außerhalb des NTV-Zeichensatzes.

3. Transport der Zeichen, die zwischen Client und Server ausgetauscht werden

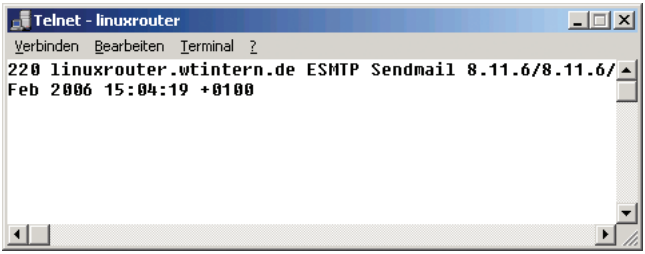
   Alle vom Anwender eingegebenen oder vom Server gesendeten Zeichen des NTV Zeichensatzes werden 1:1 in den Nutzdatenbereich eines TCP-Paketes gepackt und übers Netzwerk transportiert.

Die Einfachheit des Telnet-Protokolls sowie die Transparenz bei der Zeichenübertragung, haben Telnet auch zu einem beliebten Diagnosetool gemacht. So lassen sich Verbindungen zu http, SMTP oder POP3 Servern herstellen.

Es lässt sich zum Beispiel durch Eingabe der folgende Zeile in einer Dosbox überprüfen, ob der SMTP-Server (Port25) arbeitet:

```
telnet <IP-Adresse eines Mail-Servers> 25
```

Ist der SMTP-Server aktiv, wird eine Begrüßungsmeldung zurückgegeben.



Durch konsequentes Eintippen des SMTP-Protokolls könnte man nun theoretisch per Telnet-Client E-Mails verschicken.

3.5 FTP - File Transfer Protocol

In einfachen Worten ausgedrückt, erlaubt FTP einem Anwender im Netzwerk den Zugriff auf das Datei-System, bzw. die Festplatte eines entfernten Rechners.

Eine der Hauptanwendungen für FTP ist heute das Aufspielen von HTML-Seiten auf WWW-Server, die zu diesem Zweck auch immer einen FTP-Zugang haben.

FTP kann aber auch genutzt werden, um über embedded FTP-Clients, wie zum Beispiel den W&T Com-Server, serielle Daten von Endgeräten in eine Datei auf dem Server zu speichern.

Ein weiteres Anwendungsfeld ist das Data-Logging (zyklisches Abspeichern von Datensätzen) via FTP. Auf diesem Weg kann z.B. ein Web-Thermograph die Werte für Temperatur und Luftfeuchte in vorgegebenen Abständen mit Zeitstempel in eine Datei auf dem FTP-Server schreiben.

Der FTP-Client

FTP arbeitet nach dem Client/Server Prinzip. Ein FTP-Client ist heute Bestandteil jedes Betriebssystems. Unter Windows z.B. wird durch Eingabe des FTP-Befehls in einer Dosbox der FTP-Client gestartet.

Mit dem OPEN-Kommando, gefolgt von der IP-Adresse bzw. dem Hostnamen des FTP-Servers, wird die FTP Verbindung geöffnet und der Nutzer muss seinen Login-Namen und ein Passwort eingeben. Nach erfolgreichem Login, sind je nach Zugriffsrecht unter anderem folgende Dateioperationen möglich:

	FTP Befehl
Speicher von Dateien auf dem Server	PUT
Laden von Dateien vom Server	GET
Daten an eine bestehende Datei anhängen	APPEND
Löschen von Dateien auf dem Server	DELETE

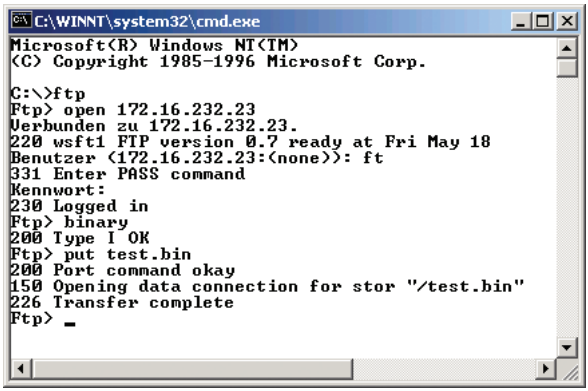
Anzeigen des Verzeichnisinhaltes	DIR

Eine Auflistung aller unterstützten Kommandos erhält man mit der Eingabe eines "?" hinter dem FTP-Prompt. Eine kurze Beschreibung der einzelnen Kommandos kann mit „? Kommando" abgerufen werden.

Eine wichtige Eigenschaft von FTP ist die unterschiedliche Handhabung von Text- und Binärdateien. Um die gewünschte Betriebsart auszuwählen, stellt FTP zwei weitere Kommandos zur Verfügung:

	FTP Befehl
für die Übertragung von Textdateien	ASCII
für die Übertragung von Binärdateien (z.B. ausführbare Programmdateien)	BINARY

Nach der Eingabe von FTP findet die Bedienung in einer Art Dialog statt, wie hier beispielhaft für das Speichern der Datei „test.bin" auf dem Server „172.16.232.23" gezeigt.



Je nach Betriebssystem können sowohl die Bedienung als auch die Kommandos des FTP-Client variieren.

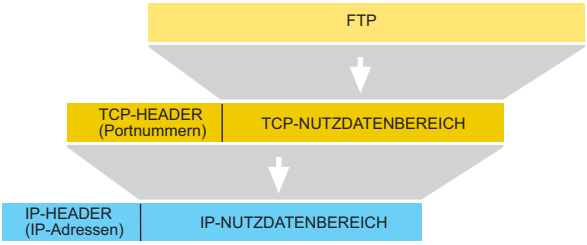
In Unix-Betriebssystemen ist außerdem strikt auf Groß- und Kleinschreibung zu achten.

Eine komfortablere Handhabung von FTP lässt sich durch den Einsatz von zugekauften FTP-Client Programmen mit grafi-

scher Benutzeroberfläche erreichen.

Das FTP-Protokoll

Als Basis-Protokoll setzt FTP auf das verbindungsorientierte und gesicherte TCP auf.



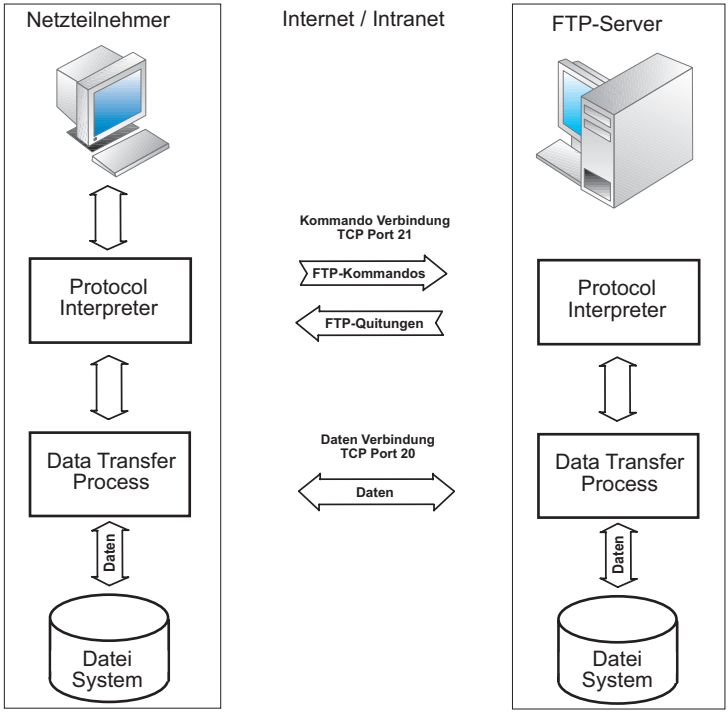
Das FTP-Datenpaket sieht dann so aus:

Im Gegensatz zu anderen Internetdiensten nutzt FTP aber zwei TCP-Verbindungen und damit zwei TCP-Ports:

- Port 21 als Kommando-Verbindung
- der zweite Port wird für die Übertragung der Dateien benutzt. Die verwendete Portnummer wird ausgehandelt.

Die Steuerung des Datei-Transfers zwischen Client und Server wird über einen Kommandodialog gesteuert. Diesen Part wickeln die Protocol-Interpreter über die Kommando-Verbindung ab. Die Kommando-Verbindung bleibt für die gesamte Dauer der FTP-Sitzung bestehen.

Der eigentliche Datei-Transfer erfolgt über die Daten-Verbindung, die vom Data Transfer Prozess für jede Dateioperation neu geöffnet wird. Der Data Transfer Prozess ist dabei das Bindeglied zwischen Netzwerk und Dateisystem und wird vom Protocol-Interpreter gesteuert.



Der FTP-Server

Ein FTP-Server steht in der Regel nur bei Server-Betriebssystemen zur Verfügung und muss ggf. erst gestartet werden.

FTP-Server bieten zwei Zugriffsmöglichkeiten:

1. Nur eingetragene Nutzer haben Zugriff und können, je nach in einer User-Liste festgehaltenem Zugriffsrecht, Dateioperationen ausführen.
2. Jeder Nutzer kann auf den Server zugreifen. Ein Login findet entweder gar nicht statt oder es wird der Username „anonymous“ angegeben. Man spricht dann von Anonymous-FTP.

3.6 TFTP - Trivial File Transfer Protocol

Neben FTP ist TFTP ein weiterer Dienst, um übers Netzwerk auf die Dateien eines entfernten Rechners zugreifen zu können.

TFTP ist allerdings sowohl vom Funktionsumfang als auch von der Größe des Programmcodes deutlich „schlanker“ als FTP.

Ein TFTP-Client ist nicht unbedingt Bestandteil des Betriebssystems.

TFTP-Server kommen im Officebereich selten zum Einsatz.

Besonders geeignet ist TFTP für den Einsatz in Embedded Systemen, in denen nur ein begrenzter Speicherplatz für Betriebssystemkomponenten zur Verfügung steht. TFTP bietet hier bei minimalem Programmcode ein hohes Maß an Effizienz.

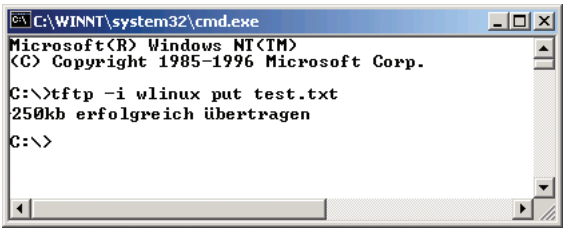
In Com-Servern, Printerservern und Miniterminals wird beispielsweise TFTP genutzt, um Konfigurations- und Firmware-Dateien zu übertragen.

TFTP stellt nur zwei Dateioperationen zur Verfügung:

	TFTP Befehl
Speicher von Dateien auf dem Server	PUT
Laden von Dateien vom Server	GET

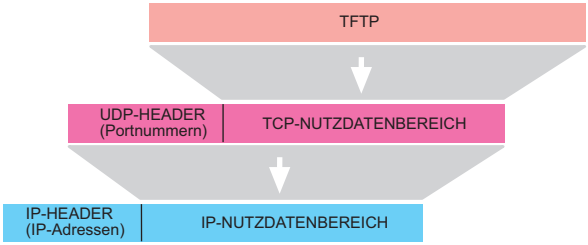
Wie auch FTP unterscheidet TFTP zwischen der Übertragung von Text- und Binär-Dateien. Sollen Binär-Dateien übertragen werden, wird dies durch den zusätzlichen Parameter „-i“ angegeben.

Hier als kurzes Beispiel: Die binäre Datei „test.txt“ wird von einem Windows NT Rechner auf den Server wlinux gespeichert.



Auf eine Authentifizierung, also ein Login mit Passwortabfrage wie bei FTP, wird verzichtet.

Im Gegensatz zu FTP verwendet TFTP als Basis Protokoll UDP, wobei der Port 69 genutzt wird.



Das TFTP-Datenpaket sieht dann so aus:

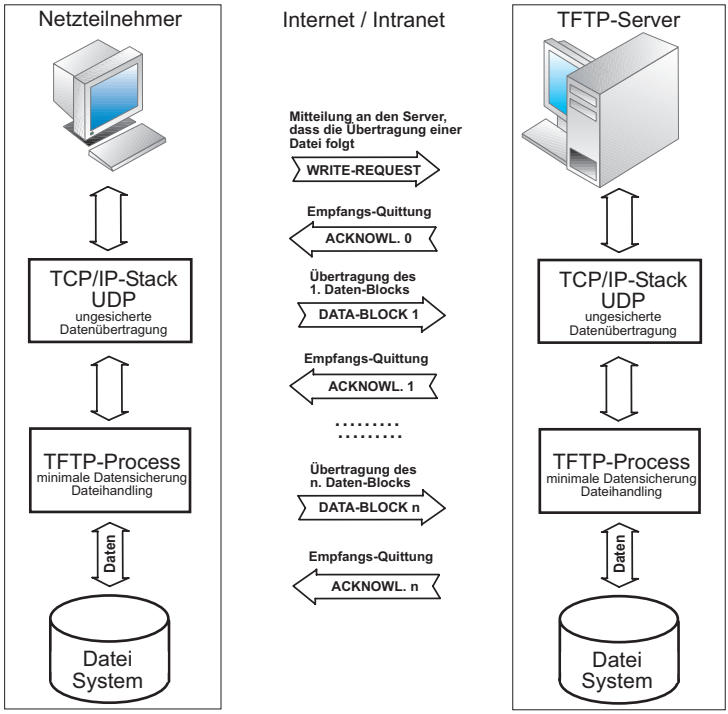
Zur Erinnerung:

UDP arbeitet verbindungslos. Man spricht bei UDP-Paketen auch von Datagrammen, wobei jedes Paket als eigenständige Datensendung behandelt wird. Auf UDP-Ebene werden empfangene Pakete nicht quittiert. Der Sender erhält keine Rückmeldung, ob ein gesendetes Paket wirklich beim Empfänger angekommen ist. UDP-Pakete bekommen keine Sequenz-Nummer. Ein Empfänger, der mehrere UDP-Pakete erhält, hat keine Möglichkeit festzustellen, ob die Pakete in der richtigen Reihenfolge empfangen wurden.

Aus diesem Grund übernimmt TFTP die Sicherung der übertragenen Daten selbst.

Die Übertragung von Dateien geschieht in Blöcken von je

512Bytes, wobei die Blöcke mit einer laufenden Nummer versehen werden. Jeder empfangene Block wird von der Gegenseite quittiert. Erst nach Empfang der Quittung wird der nächste Block gesendet.



TFTP erkennt, ob die empfangenen Datenblöcke in Ordnung sind; eine Fehlerkorrektur gibt es aber nicht. Geht bei der Übertragung etwas schief, stimmt etwa die Paketlänge nicht oder ein komplettes Paket geht verloren, wird das Paket von der Gegenseite nicht quittiert. Bei ausbleibender Quittierung wird das Datenpaket einige male erneut versandt. Bleibt die Quittierung dauerhaft aus, wird die Übertragung abgebrochen. In diesem Fall kann der Anwender oder eine intelligente Anwendungssoftware den Vorgang erneut starten.

3.7 SNMP – Simple Network Management Protocol

Gerade in technischen Anwendungen verbindet das Netzwerk eine Vielzahl verschiedener Endgeräte unterschiedlicher Hersteller. Jeder Hersteller hat dabei seine ganz eigene Methodik, auf welche Weise die Geräte parametriert und überwacht werden.

So stellen einige Hersteller spezielle Managementprogramme für ihre Endgeräte zur Verfügung, andere bieten dem Benutzer bzw. Administrator eine Web-Oberfläche an, über die sich die Komponenten im Browser überwachen und konfigurieren lassen.

Kleinere Netzwerke lassen sich mit diesen Mitteln bequem einrichten, überwachen und warten.

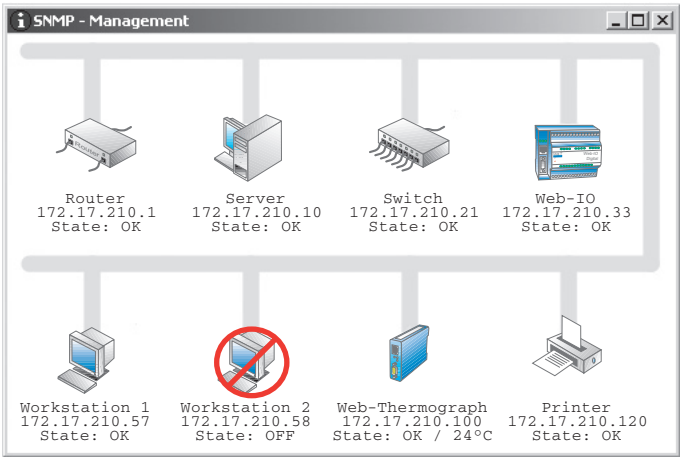
In größeren Netzwerken, mit zum Teil mehreren 100 Netzwerkteilnehmern, wäre es allerdings sehr mühsam, jedes Gerät mit anderen Mitteln zu konfigurieren und zu überwachen. Hier bietet SNMP die Grundlage für ein einheitliches und überschaubares Netzwerkmanagement.

SNMP-Agent
Bedingung für den Einsatz von SNMP ist, dass alle beteiligten Endgeräte einen SNMP-Agenten besitzen. Der SNMP-Agent ist eine Software-Schnittstelle, die das Endgerät mit allen betriebswichtigen Parametern repräsentiert. SNMP-fähige Endgeräte werden auch als Netzwerkknoten bzw. Nodes bezeichnet. Nodes können Workstation-PC, Server, Switches, Router, Web-IO, also eigentlich alles sein, was über eine eigene IP-Adresse im Netzwerk ansprechbar ist.

SNMP-Manager
Neben den Nodes gibt es in SNMP-Systemen mindestens einen SNMP-Manager. Der SNMP-Manager ist eine Software-Anwendung, die auf einer Workstation oder einem Server arbeitet.

Während SNMP-Manager früher kommandozeilengesteuerte Anwendungen waren, in denen die Nodes in Listen verwaltet wurden, stellen moderne SNMP-Systeme dem Administrator

mächtige Visualisierungsfunktionen zur Verfügung. Die gesamte Netzwerkinfrastruktur kann in Form von Plänen dargestellt und somit sehr übersichtlich verwaltet werden.



Zu den Aufgaben eines SNMP-Managers zählen: Konfiguration, Verwalten von Zugriffsrechten, Überwachen, Fehlermanagement und Netzwerksicherheit.

SNMP-MIB

Die Abkürzung MIB steht für Management Information Base. Zu jedem Netzwerkknoten gehört eine spezifische MIB, d.h. eine Liste aus abrufbaren Variablen, in denen die Eigenschaften und Zustände des Netzteilnehmers beschrieben sind.

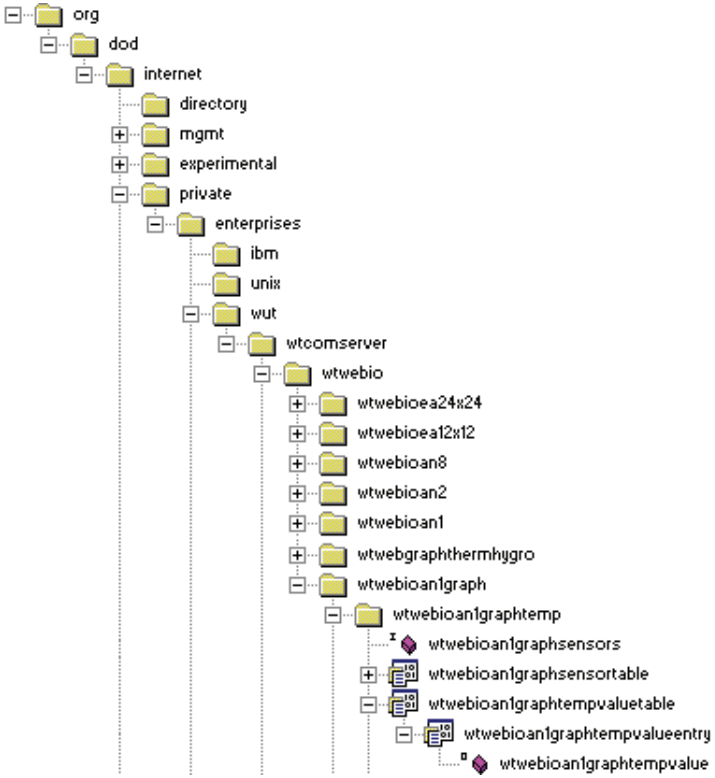
Im Normalfall muss der Anwender sich nicht im Detail mit dem Aufbau der MIB beschäftigen. Moderne Managementsysteme verfügen über einen MIB-Compiler, der die MIB-Daten ins System integriert und dem Nutzer in einer gut handhabbaren Form zur Verfügung stellt.

Um das Verständnis für die Abläufe bei SNMP zu erhöhen, möchten wir hier dennoch einen groben Überblick über den Aufbau vermitteln.

Die MIB besteht aus zwei grundsätzlichen Teilen: der Standard MIB, in der System-Variablen verwaltet werden, die für

alle Knoten benötigt werden, und der Private-MIB, in der die gerätespezifischen Variablen untergebracht sind und auf die wir hier näher eingehen.

Die Datenstruktur der MIB hat einen baumartigen Aufbau, ähnlich der Verzeichnisstruktur auf einer Festplatte. Die einzelnen Variablen sind in Gruppen, Untergruppen usw. gegliedert, so wie einzelne Dateien auf einem Datenträger in Ordnern und Unterordnern gespeichert werden.



Die Abbildung zeigt in der Darstellungsweise eines Verzeichnisbaumes, an welcher Stelle zum Beispiel bei einem Web-Thermographen die gemessene Temperatur per SNMP abgerufen werden kann.

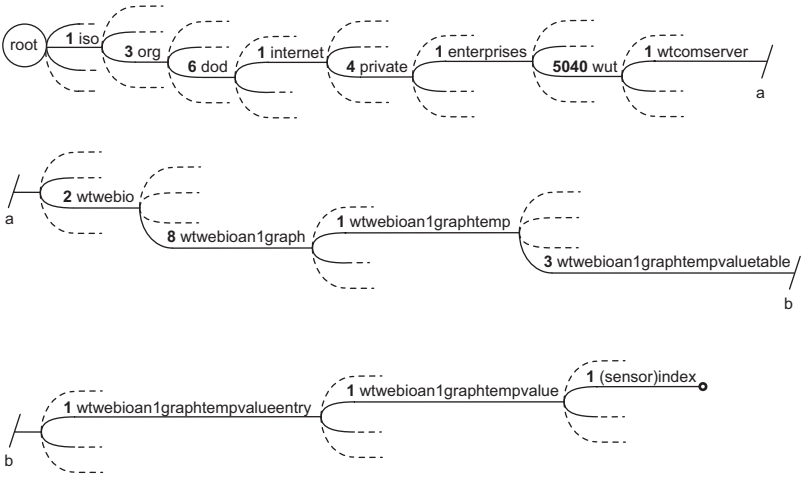
Bei den MIB-Variablen spricht man auch von Objekten. Zu jedem Objekt einer MIB gehört die MIB-OID. OID steht für Ob-

ject Identifier. Die OID ist eine durch Punkte getrennte Kette von Zahlen, wobei jede Zahl für einen Abzweig im MIB-Baum angibt, wohin verzweigt wird.

Die OID für die Sensortemperatur des Wiesemann & Theis Web-Thermographen sieht z.B. so aus:

1.3.6.1.4.1.5040.1.2.8.1.3.1.1.1

Da solche Datenketten für den Anwender nicht überschaubar sind, kann man die OID auch als MIB-Diagramm darstellen:



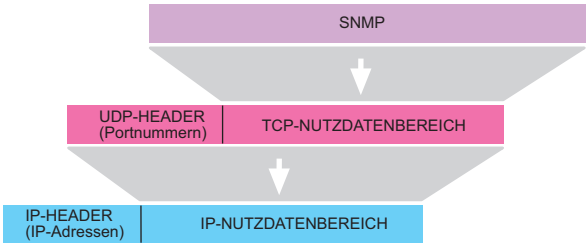
Die von den Herstellern der verschiedenen Netzwerkknoten mitgelieferten MIB-Dateien beschreiben die OID-Struktur im ASN1-Format (Abstract Syntax Notification).

ASN1 Dateien sind zwar lesbar, eine Entschlüsselung durch den Anwender ist aber kompliziert und nicht vorgesehen.

Wie bereits angesprochen, verfügen SNMP-Managementsysteme über einen ASN.1 MIB-Compiler. Dieser Compiler wertet das ASN.1 Format aus und vermittelt dem Manager, welche Variablen eines Netzwerkknotens an welcher Stelle zu finden sind.

SNMP-Kommunikation

Die Kommunikation zwischen SNMP Managementsystem und SNMP-Netzknoten wird über das UDP-Protokoll abgewickelt.



Das SNMP-Datenpaket sieht dann so aus:

Hierbei empfängt der Netzwerkknoten die Datensendungen vom SNMP-Managementsystem auf Port 161.

Die normale Kommunikation geht immer vom Managementsystem aus. Dieses sendet ein GET-Kommando mit der OID des gewünschten Wertes an den Netzwerkknoten. Der Netzwerkknoten sendet darauf hin ein RESPONSE-Paket zurück, welches ebenfalls die OID und zusätzlich den zugehörigen Wert enthält.

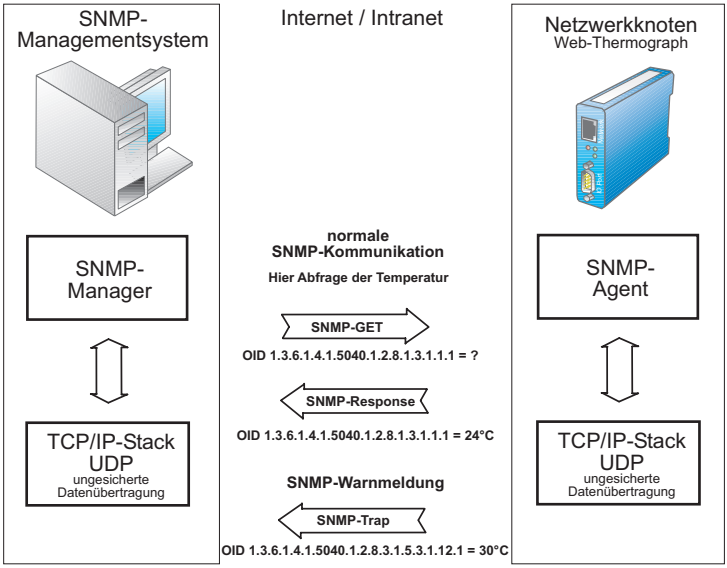
SNMP-Trap

Neben der normalen Kommunikation gibt SNMP den Netzwerkknoten die Möglichkeit, unaufgefordert Meldungen an den SNMP-Manager zu senden.

Diese SNMP-Traps werden als Status- oder Warnmeldungen genutzt. So kann z.B. ein Switch auf diesem Weg melden, wenn ein Port seinen Link verliert.

SNMP-Traps werden an Port 162 gesendet.

Beim Web-Thermographen können z.B. Alarme definiert werden, die bei Temperaturüberschreitung (z.B. im Serverraum) einen SNMP-Trap senden.



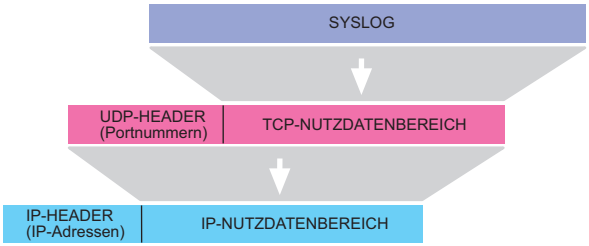
SNMP Traps haben eigene OIDs, die in einem gesonderten Teil der MIB untergebracht sind, auch wenn der gleiche Wert in einem anderen Teil der MIB ggf. noch einmal auftaucht.

Für Administratoren ausgedehnter Netze mit vielen Netzwerkteilnehmern bietet SNMP alle Voraussetzungen, die Wartung und Überwachung aller beteiligten Geräte einheitlich und übersichtlich abzuwickeln.

3.8 Syslog - Der Systemlogger

Syslog ist ähnlich dem SNMP ein Protokoll um Systemmeldungen an zentraler Stelle zu überwachen. Im Gegensatz zu SNMP ist Syslog aber eine Einbahnstraße. Das heißt mit Syslog können Netzwerkgeräte wie PCs, Router, Switches, Hubs, aber auch embedded Geräte wie Web-IO und Web-Thermographen, Systemmeldungen an einen zentralen Server senden; Datensendungen vom Server zu den Endgeräten sind jedoch nicht vorgesehen.

Auf Netzwerkebene werden Syslog-Meldungen über das UDP-Protokoll auf Port 514 übertragen.



Das SYSLOG-Datenpaket sieht dann so aus:

Syslog-Meldungen können normale Statusinformationen, Warnmeldungen und Fehlermeldungen sein.

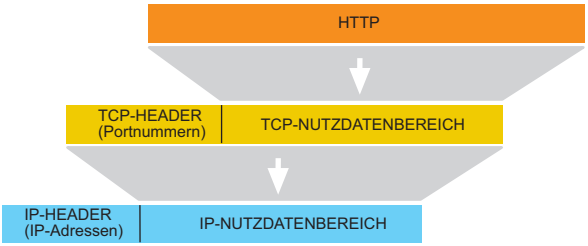
Je nach Dringlichkeit werden den Syslog-Meldungen vom Absender Prioritäten zugeordnet. Auf diese Weise kann beeinflusst werden, welche Meldungen bevorzugt bearbeitet werden. Ferner enthält jede Syslog-Meldung einen Zeitstempel mit Uhrzeit und Datum.

Der Prozess, der auf dem Server die Syslog-Meldungen entgegennimmt und weiterverarbeitet, wird als Syslog-Daemon bezeichnet.

Syslog stammt im Ursprung aus der Unix- bzw. Linux-Welt, wird heute aber auch im Windows-Umfeld eingesetzt.

3.9 HTTP – Hypertext Transfer Protocol

Durch die rasante Zunahme von WWW-Nutzern ist HTTP heute das mit Abstand meist genutzte Protokoll im Internet. HTTP setzt auf TCP als Basisprotokoll auf, wobei in aller Regel der TCP-Port 80 genutzt wird (abweichende Ports sind möglich, müssen aber explizit im URL angegeben werden).



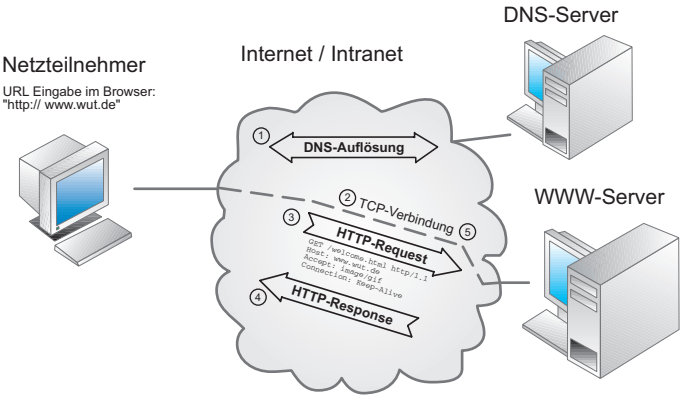
Das HTTP-Datenpaket hat somit folgenden Aufbau:

Die Anforderung und Übertragung einer Webseite erfolgt in vier Schritten:

1. Auflösen des angegebenen Host- und Domainnamens in eine IP-Adresse
   Der TCP/IP-Stack startet eine DNS-Anfrage, um die IP-Adresse des gewünschten Servers zu ermitteln.
2. Aufbau der TCP-Verbindung
   Zur Erinnerung: Bei einer TCP-Verbindung gilt das Client-Server-Prinzip. Bei HTTP übernimmt der Browser die Rolle des Client und stellt die TCP-Verbindung zum angegebenen HTTP-Server her.
3. Senden der HTTP-Anforderung
   Nach erfolgreichem Aufbau der TCP-Verbindung fordert der Browser die gewünschte Webseite beim WWW-Server an. An dieser Stelle beginnt das eigentliche HTTP-Protokoll: Der Browser sendet das *GET*-Kommando mit den erforderlichen Parametern zum WWW-Server.
4. Senden der angeforderten Webseite
   Der WWW-Server sendet erst eine HTTP-Bestätigung und dann die Webseite selbst.

5. Beenden der TCP-Verbindung durch den WWW-Server
   Eine Besonderheit bei HTTP ist, dass die TCP-Verbindung nicht wie sonst üblich durch den Client, sondern durch den Server abgebaut wird. Dafür gibt es zwei Gründe:

   - Der WWW-Server signalisiert dem Browser auf einfache Art und Weise, dass die Übertragung abgeschlossen ist. Eine empfangene Webseite wird im Browser deshalb auch erst dann angezeigt, wenn die TCP-Verbindung beendet ist.
   - WWW-Server müssen eine Vielzahl von TCP-Verbindungen gleichzeitig bedienen. Dabei verlangt jede offene Verbindung dem Server ein gewisses Maß an Leistung ab. Um die Verbindungszeiten so kurz wie möglich zu halten, baut der Server die Verbindung einfach ab, sobald alle angeforderten Daten übertragen wurden.



Die wichtigsten HTTP-Kommandos und Parameter

Wie bereits angesprochen basiert auch HTTP auf dem Client-Server-Prinzip: Der Browser als Client kann durch das Senden bestimmter Kommandos die Kommunikation steuern.

Das GET-Kommando

Das mit Abstand am häufigsten verwendete Kommando ist die GET-Anfrage, die jeden Aufruf einer Webseite einleitet. GET fordert den HTTP-Server auf, ein Dokument oder Element zu senden und ist damit das wichtigste Kommando.

Für den Einsatz von GET sind einige Parameter nötig; man spricht auch von einer Kommandozeile (engl. Request Line).

```
GET /pfadname/filename http-Version
```

Weitere Parameter können jeweils als neue Zeile mitgesendet werden. Diese angehängten Parameter werden auch als „Header“ bezeichnet.

Host	Hostname (nur bei HTTP1.1 nötig).
Accept	gibt an, welche Dateiformate der Browser verarbeiten kann Mit *Accept: image/gif* gibt der Browser z.B. bekannt, dass er Bilder im GIF-Format anzeigen kann.
Connection	über diesen Parameter *(Connection: Keep-Alive)* kann vom Browser vorgegeben werden, ob die TCP-Verbindung zum Nachladen anderer Elemente offengehalten wird.

Eine Vielzahl weiterer Parameter sind in der RFC2616 beschrieben, die unter *http://www.w3.org/Protocols/rfc2616/rfc2616.html* eingesehen werden kann.

Ein typisches GET-Kommando könnte etwa so aussehen:

```
GET /welcome.html http/1.1
Host: www.wut.de
Accept: image/gif
Connection: Keep-Alive
```

Als Antwort sendet der HTTP-Server eine Statuszeile, auf die ein Header (diesmal mit Parametern des Servers) folgt. Getrennt durch eine Leerzeile <CR LF CR LF> wird das angeforderte Element übermittelt.

```
HTTP/1.1 200 OK                              | Statuszeile
Date: Thu, 15 Mar 2001 11:33:41GMT           |
Server: Apache/1.3.4 (Unix) PHP/3.0.6        |
Last-Modified: Thu 15 Mar 2001 11:32:32 GMT  |
```

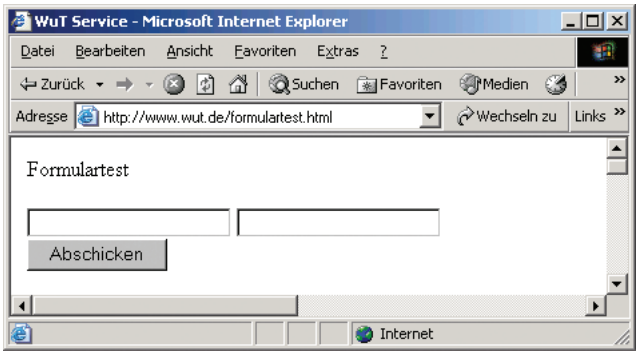
```
...                              |
...                              | Header
Keep-Alive: timeout=15           |
Connection: Keep-Alive           |
Content-Type: text/html          |
<html>                           |
  ...                            | HTML-Seite
</html>                          |
```

Die Statuszeile umfasst die vom Server unterstütze HTTP-Version, eine Fehlercode-Nummer und einen Kommentar. Im Header zeigt der Server unterstützte Verbindungseigenschaften und Daten an.

Das POST-Kommando

Das Gegenstück zu GET ist das POST-Kommando. POST erlaubt dem Browser, Informationen an den HTTP-Server zu übergeben.

Der klassische Einsatz für das POST-Kommando ist die Übergabe von Formulareinträgen aus einer HTML-Seite. Im Kern ist der Aufbau der POST-Anforderung identisch mit der von GET. Nach den Parametern steht eine Leerzeile <CR LF CR LF>, der die zu übergebenden Informationen folgen. Enthält eine POST-Anforderung mehrere Einzelinformationen, werden diese durch ein „&“ voneinander getrennt. Als *filename* muss in der ersten Zeile der POST-Anforderung ein auf dem Server verfügbarer Prozess angegeben werden, der die Informationen entgegennehmen und verarbeiten kann.



Für dieses Formulartest-Formular könnte die POST-Anforderung folgendermaßen aussehen; der bislang nicht besprochene Parameter *Referer* stellt hier einen Bezug zu der ursprünglich geladenen Formular-Seite her:

```
POST /Formularauswertung.cgi HTTP/1.1
Accept: image/gif, image/jpeg
Referer: http://172.16.232.145/formulartest.html
Host: 172.16.232.145
Connection: Keep-Alive

EINGABEFELD1=test1&EINGABEFELD2=test2&submit=Abschicken
```

Tipp: Die meisten Internet Provider bieten sogenannte „CGI-Scripts“ (Programme auf dem HTTP-Server) an, die Formularangaben entgegennehmen und als E-Mail an eine beliebige Adresse weiterleiten. So kann man seinen Kunden z.B. die Gelegenheit geben, direkt von einer Webseite aus eine Bestellung oder Anfrage zu verschicken.

Das HEAD-Kommando

Als drittes Kommando sei hier der Vollständigkeit halber noch eine Variante von GET genannt. Das HEAD-Kommando arbeitet wie das GET-Kommando, doch der HTTP-Server gibt nur die Statuszeile und den Header, nicht aber das angeforderte Element selbst zurück.

Es wird fast ausschließlich zu Testzwecken und von Suchmaschinen genutzt, die über die resultierende Meldung (Fehlercode) die Existenz einer Seite überprüfen können.

HTTP-Versionen

HTTP wurde seit der Einführung des WWW mehrfach weiterentwickelt und kommt heute in drei Versionen vor:

HTTP 0.9	in 1989 erstmalig vorgestellt und seitdem genutzt, aber nie spezifiziert
HTTP 1.0	erst 1996 wurde HTTP in der Version 1.0 durch die RFC 1945 spezifiziert, die weitestgehend mit HTTP0.9 identisch ist
HTTP 1.1	wurde 1997 (RFC 2068) eingeführt und ist

seit 1999 (RCF 2616) in überarbeiteter Form im Einsatz.

Alle heute erhältlichen Browser unterstützen standardmäßig HTTP1.1 , können aber auch problemlos mit Servern zusammenarbeiten, die HTTP0.9 oder HTTP1.0 verwenden.

Die wohl grundlegendste Änderung in HTTP1.1 liegt darin, dass die für die Übertragung des HTML-Dokuments aufgebaute TCP Verbindung auch für das Nachladen weiterer Elemente weitergenutzt wird. HTTP1.0 bzw. 0.9 haben für jedes Element eine separate TCP-Verbindung aufgebaut.

Eine persistente Verbindung wie in 1.1 erhöht den Datendurchsatz, da die Zeiten für Verbindungsaufbau und -abbau entfallen.

Der Browser öffnet die TCP-Verbindung und sendet das GET-Kommando. Um auf einem HTTP-Server die Internet-Auftritte mehrerer Anbieter verwalten zu können, wurde mit *Host* ein zusätzlicher Parameter zum GET-Kommando eingeführt, der dem Server zusammen mit einer GET-Anfrage auch den Hostnamen übermittelt (z.B *Host: http://www.wut.de*). Dank dieses zusätzlichen Parameters kann der HTTP-Server über die GET-Anfrage erkennen, welchem Host die TCP-Verbindung gilt.

3.10 E-Mail

Die Möglichkeit, elektronische Post in wenigen Sekunden von einem Ende der Welt zum anderen verschicken zu können, ist sicherlich einer der Hauptgründe für die rasante Ausbreitung des Internets.

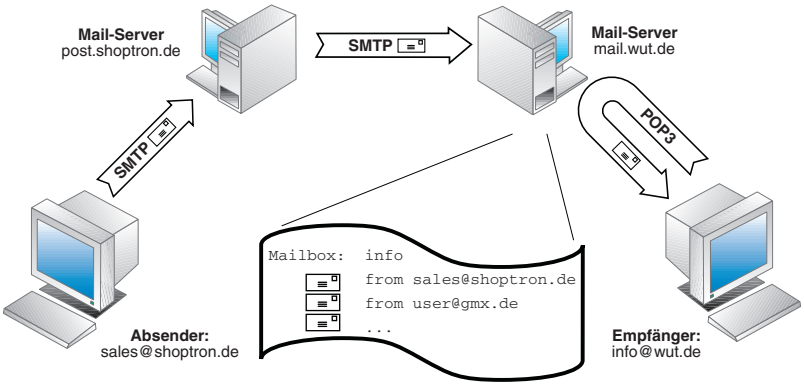
Im Gegensatz zu den meisten anderen Anwendungen im Internet ist das Versenden von E-Mail ein Dienst, bei dem keine direkte Verbindung zwischen Sender und Empfänger besteht. Das klingt zunächst verwirrend, ist aber sinnvoll, da sonst der Austausch von E-Mail nur möglich wäre, wenn Versender und Empfänger gleichzeitig im Netz aktiv sind.

Um eine zeitliche Unabhängigkeit zu gewährleisten, benötigt der E-Mail-Empfänger eine Mailbox (Postfach) auf einem Mail -Server, in der eingehende Nachrichten zunächst abgelegt werden.

Eine E-Mail-Adresse setzt sich immer aus dem Postfachnamen und der Zieldomain zusammen; als Trennzeichen steht das „@“ (engl. „at“, gesprochen „ätt“) zwischen diesen beiden Bestandteilen. Ein Beispiel: *info@wut.de* bezeichnet das Info-Postfach auf dem Mailserver von Wiesemann & Theis.

Der Weg einer E-Mail vom Versender zum Empfänger besteht aus zwei Teilabschnitten, auf denen der Transport über unterschiedliche Protokolle geregelt wird:

- vom Rechner des Absenders bis zum Postfach des Empfängers wird das SMTP-Protokoll benutzt,
- vom Postfach des Empfängers bis zum Rechner des Empfängers wird das POP3-Protokoll benutzt.



Aufbau einer E-Mail

Eine E-Mail setzt sich aus dem Nachrichtenkopf und der eigentlichen Nachricht zusammen. Diesen Kopf kann man mit einem Briefumschlag vergleichen, der Felder für Absender, Empfänger, Datum, Betreff und einige weitere Informationen enthält.

Hier die wichtigsten Felder im Überblick:

Die folgenden vier Felder bilden einen Minimalkopf und müssen auf jeden Fall enthalten sein.

Feld	Funktion
FROM	E-Mail-Adresse des Verfassers
TO	E-Mail-Adresse des Empfängers
DATE	Datum und Uhrzeit Hinweis: Die Uhrzeit kann willkürlich eingetragen werden und ist in aller Regel die Ortszeit des Absenders.
SUBJECT	Text der Betreffzeile
RECEIVED	Das Feld RECEIVED stellt eine Besonderheit dar, denn es wird nicht bei Erstellung der E-Mail angelegt. Jeder auf dem Weg der E-Mail liegende Mail-Router fügt ein RECEIVED-Feld ein und hinterlässt auf diese Weise einen "Durchgangsstempel" mit Datum und Uhrzeit.

Die Verwendung der im Folgenden genannten Felder ist optional.

Feld	Funktion
SENDER	E-Mail-Adresse des Absenders (in aller Regel identisch mit Eintrag unter FROM)
REPLY-TO	E-Mail-Adresse, an die der Empfänger im Bedarfsfall antworten soll. Wichtig, wenn E-Mails von einem Embedded-System wie dem W&T IO-Mailer automatisiert verschickt werden. Als Antwortadresse könnte in diesem Fall z.B die E-Mail-Adresse des Administrators eingetragen sein.
CC	E-Mail-Adresse eines weiteren Empfängers, der einen "Durchschlag" (CC = "Carbon Copy") der Nachricht erhält.
BCC	E-Mail-Adresse eines weiteren Empfängers, die für alle anderen Empfänger aber unsichtbar bleibt (BCC = "Blind Carbon Copy").
MESSAGE-ID	Eindeutige Identifikation einer E-Mail, die von der Mailsoftware willkürlich vergeben wird.
X-"MEINFELD"	Durch Voranstellen von "X-" können eigene Felder erzeugt werden.

Bei einigen Feldern ist eine RESENT-Variante möglich, die dann zum Tragen kommt, wenn es sich um eine vom ursprünglichen Empfänger weitergeleitete E-Mail handelt.

Der formale Aufbau von Nachrichtenkopf und Feldern muss den folgenden Konventionen genügen:

- Nach dem Feldnamen steht ein Doppelpunkt; danach folgt der jeweilige Parameter.
- Jedes Feld steht in einer eigenen Zeile, die mit <CR LF> (Carriage Return Line Feed; hex 0D 0A) endet.
- Nachrichtenkopf und Körper werden durch eine zusätzliche Leerzeile <CR LF> getrennt.
- Der Nachrichtenkörper selbst enthält nur den zu übermittelnden Text bzw. weitere eingefügte Dateien. Das Ende der Nachricht wird durch <CR LF . CR LF> (hex 0D 0A 2E 0D 0A) gekennzeichnet.
- Sowohl Kopf als auch Nachrichtenkörper bestehen ausschließlich aus 7-Bit-ASCII-Zeichen. Deshalb können auch alle Steuerinformationen als Klartext übertragen werden.

MIME – Multipurpose Internet Mail Extensions

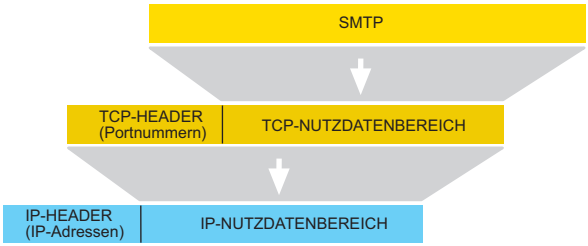
Um auch binäre Daten (8-Bit-Format) via E-Mail verschicken zu können, werden diese vor dem Einbinden in den Nachrichtenkörper nach dem „MIME-Standard“ in das 7-Bit-Format codiert und beim Empfänger wieder decodiert. Da die Verarbei-

tung binärer Daten von heutigen E-Mail-Programmen automatisch übernommen wird, verzichten wir an dieser Stelle auf eine detaillierte Erklärung der „MIME-Codierung“.

SMTP – Simple Mail Transfer Protocol

SMTP regelt den Versand von E-Mails vom Mail-Client zum Mailserver (SMTP-Server). Der Mail-Client kann dabei entweder der ursprüngliche Versender oder ein auf dem Weg liegender Mail-Router sein. Mail-Router kommen zum Einsatz, wenn die E-Mail auf ihrem Weg über mehrere Domains weitergereicht wird. Häufig findet man für Mail-Router auch die Bezeichnung *MTA* (Mail-Transfer-Agent).

Für jedes Teilstück, das eine E-Mail zurücklegt, wird eine eigene TCP-Verbindung aufgebaut. SMTP setzt auf diese TCP-Verbindung auf, wobei der TCP-Port 25 genutzt wird.



Der Aufbau des SMTP-Datenpaketes sieht somit aus wie folgt:

SMTP stellt einige Kommandos (z.B Angabe des Absenders, Angabe des Empfängers ...) zur Verfügung. Jedes SMTP-Kommando wird einzeln vom SMTP-Server quittiert. Die eigentliche E-Mail wird komplett mit Kopf und Körper gesendet und dann erst vom SMTP-Server quittiert. Wenn keine weiteren E-Mails zum Versand anstehen, wird auch die TCP-Verbindung wieder abgebaut.

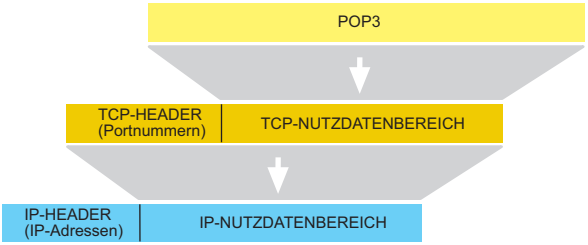
Hat die E-Mail den Ziel-Mailserver erreicht, wird sie im Postfach des Empfängers abgelegt und bleibt dort so lange liegen, bis sie vom Empfänger abgeholt wird.

POP3 – Post Office Protocol Version 3

Um eingegangene E-Mails aus dem Postfach auf dem Mailserver abzuholen, wird in den meisten Fällen das POP3-Protokoll benutzt. Der Empfänger wird über eingehende E-Mails nicht informiert. Er muss sein Postfach selbständig auf eingegangene E-Mails überprüfen und kann diese zu einem beliebigen Zeitpunkt abholen.

Die meisten der heute genutzten E-Mail-Programme überprüfen bei Start zunächst automatisch das Postfach des Nutzers auf eingegangene Mail. Viele E-Mail-Programme bieten darüber hinaus die Möglichkeit, ein Intervall vorzugeben, in dem das Postfach zyklisch geprüft wird. Typische Nutzer, die die meiste Zeit des Tages „offline“ sind, erhalten ihre E-Mails ohnehin nur dann, wenn sie sich beim Provider eingewählt haben. Doch bei Computern mit permanentem Internetzugang ist die zyklische Abfrage durchaus sinnvoll: Der Nutzer ist hier ständig online und erhält seine E-Mails mit nur geringer Verzögerung – quasi in Echtzeit.

Auch das POP3-Protokoll setzt auf eine TCP-Verbindung auf und ist nichts anderes als ein Klartextdialog.



Der Aufbau des POP3-Datenpaketes sieht somit wie folgt aus:

POP3 nutzt die TCP-Portnummer 110. Wie bei SMTP beginnt der Dialog auch hier mit einem Login. Bei POP3 muss sich der Empfänger allerdings in zwei Schritten anmelden: mit Nutzernamen und mit Passwort. Nach erfolgreichem Login stellt POP3 einige Kommandos zur Verfügung, mit denen eingegangene Nachrichten aufgelistet, abgeholt oder gelöscht wer-

den können.

Heute wird der Nutzer mit SMTP und POP3 nur noch in geringem Maße konfrontiert: Er muss lediglich beim Einrichten der Mailsoftware den Namen des POP3- und SMTP-Servers angeben – das Abwickeln der Protokolle selbst wird unsichtbar im Hintergrund vom Mailprogramm übernommen.

Der Vollständigkeit halber sei noch erwähnt, dass es neben dem POP3-Protokoll noch die Protokolle POP2 und POP1 (beides Vorläufer von POP3) gibt, die ebenfalls zum Abholen von E-Mails entwickelt wurden. Diese Protokolle konnten sich in der Praxis aber noch nicht durchsetzen oder wurden von POP3 verdrängt.

IMAP - Internet Message Access Protocol

Genau wie POP3 setzt IMAP auf TCP als Basisprotokoll auf und dient dazu, empfangene Emails in die Client-Anwendung zu transportieren. Im Gegensatz zu POP3 belässt IMAP empfangene Emails auf dem Server und holt nur eine Kopie der Email zur Ansicht in die Client-Anwendung.

Für den Anwender hat das den Vorteil, dass ein Email-Konto von verschiedenen Endgeräten wie PC, Notebook, Smartphone oder Tablet genutzt werden kann und alle Geräte den gleichen Empfangsstand sehen.

Eine weitere Neuerung von IMAP ist die Möglichkeit auf dem Mailserver die empfangenen Emails in Ordnern abzulegen und zu verwalten.

E-Mail per SMTP über gesicherte Server versenden

SMTP in seiner ursprünglichen Form sieht nicht vor, dass der Benutzer, der E-Mails versenden möchte, sich in irgendeiner Form authentifizieren, also seine Berechtigung nachweisen muss.

Das bedeutet: jeder, der Zugang zu dem Netzwerk hat, in welchem der SMTP Server platziert ist, kann von dort aus E-Mails versenden.

Im Zeitalter von Internet, Spam (unerwünschte Werbe-E-Mail) und Computerviren ist das natürlich ein nicht tragbarer Zustand.

Deshalb wurden Authentifizierungsverfahren entwickelt, die nur dem berechtigten Benutzer erlauben, E-Mails über den Server zu verschicken.

Die zwei gängigsten Verfahren möchten wir hier kurz vorstellen.

SMTP after POP3
Diese Methode ist denkbar einfach. Nur solche User, die auf dem Mail-Server ein POP3 Postfach haben, sind berechtigt über diesen Server E-Mails zu versenden.

Bevor das Senden von E-Mails zugelassen wird, muss ein Login in das POP3-Postfach erfolgen.

Der Vorteil dieser Methode ist, dass jedes normale Mailprogramm nach dem Start zunächst das POP3-Postfach nach neuem Posteingang durchsucht und über den damit verbundenen POP3-Login automatisch die Voraussetzung zum Versenden von E-Mails schafft.

Der Anwender muss also keine besondere Konfiguration an seinem Mailprogramm vornehmen.

Nur bei Embedded Endgeräten wie z.B. Web-IO oder Web-Thermographen sollte darauf geachtet werden, dass bei SMTP Authentification *SMTP after POP3* eingestellt wird.

ESMTP
Wird ESMTP benutzt, können E-Mails unabhängig vom POP3-Zugang versendet werden.

Nachdem die TCP-Verbindung zum SMTP-Server zustandegekommen ist, fragt dieser zunächst nach einem Usernamen und dem zugehörigen Passwort.

Erst wenn beides richtig übergeben wurde, können E-Mails

versendet werden.

Für den Betrieb von Embedded Geräten hat diese Methode den Vorteil, dass zum Versenden von E-Mails nur eine TCP-Verbindung nötig ist.

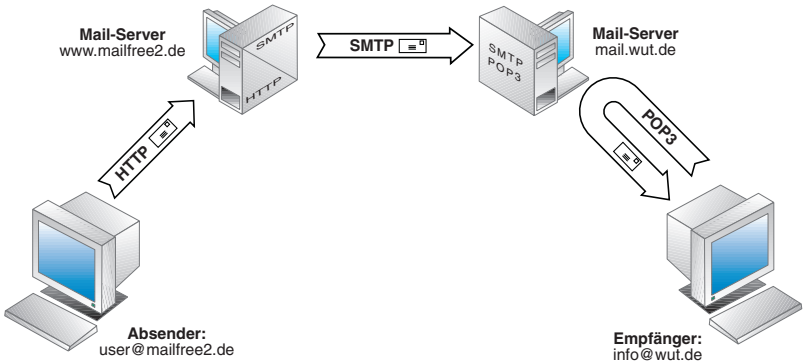
Normale Mailprogramme müssen für den ESMTP-Betrieb speziell konfiguriert werden.

E-Mail über HTTP senden und empfangen

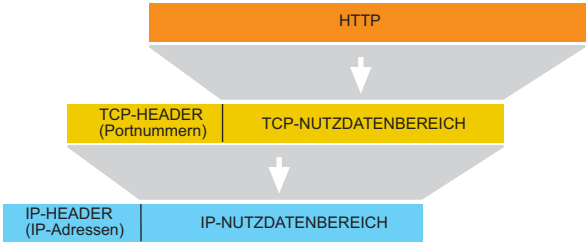
Mit der zunehmenden Nutzung von E-Mail gibt es immer mehr Freemail-Anbieter, die auf ihrem Mailserver kostenlos Postfächer zur Verfügung stellen. Diese Dienstleistung, die jeder nutzen kann, wird in aller Regel über Werbung finanziert.

Um Raum zur Einblendung von Werbung zu schaffen, geben die meisten Freemail-Anbieter dem Nutzer die Möglichkeit, das Senden und Abrufen von E-Mails bequem über HTTP im Browser abzuwickeln, der selbstverständlich durch Werbebanner bereichert ist. Hierzu stehen dem Nutzer entsprechende HTML-Formulare zur Verfügung.

Um die E-Mail-Abwicklung über HTTP zu ermöglichen, muss der Freemail-Anbieter eine spezielle Mailserver-Kombination betreiben, die zur Nutzerseite als Webserver, zur anderen Seite als SMTP-Server arbeitet. Der Weg einer E-Mail sieht hier folgendermaßen aus:



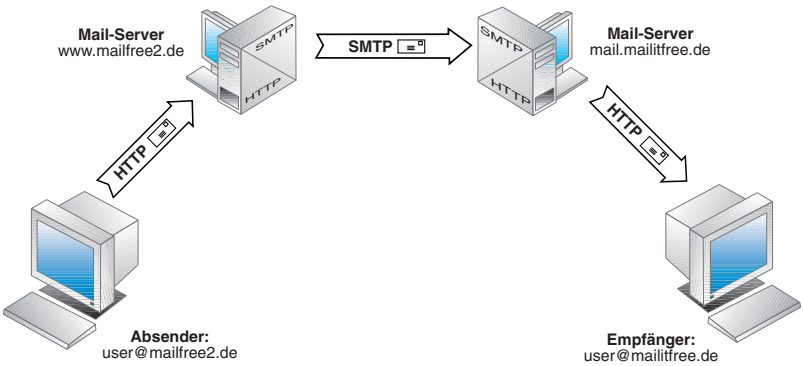
Zwischen dem Rechner des Absenders und dem Server des Freemail-Anbieters wird das HTTP-Protokoll verwendet. Wie bei anderen HTTP-Anwendungen auch, wird auch hier die TCP-Portnummer 80 genutzt.



Zwischen den Mailservern selbst ändert sich nichts. Sie kommunizieren miteinander über das SMTP-Protokoll.

Zwischen dem Ziel-Mailserver und dem Rechner des Empfängers können zwei unterschiedliche Varianten zum Einsatz kommen:

- Hat der Empfänger ein Standard-Mailkonto, werden eingegangene Mails über POP3 abgeholt.
- Nutzt auch der Empfänger die Dienste eines Freemail-Anbieters, kommt hier ebenfalls HTTP zum Einsatz.



Wer seine E-Mail lieber über SMTP und POP3 versenden möchte, sollte bei der Wahl des Freemail-Anbieters unbedingt darauf achten, dass auch Zugangsmöglichkeiten über einen SMTP- bzw. POP3-Server vorhanden sind.

E-Mail und DNS

Auch beim Versenden von E-Mails wird auf IP-Ebene mit IP-Adressen gearbeitet. Die Namensauflösung bei E-Mail Adressen funktioniert vom Prinzip genauso wie bei normalen Netzteilnehmern auch. Natürlich wird dabei nicht die Adresse des E-Mail-Empfängers selbst aufgelöst, sondern lediglich die des Mailservers, auf dem der Empfänger sein Postfach hat.

Zur Erinnerung: Um Namen in Adressen aufzulösen, bedient sich der TCP/IP-Stack eines Resolver-Programms, das beim DNS-Server eine entsprechende Anfrage stellt.

Nun ist der Hostname des Ziel-Mailservers aber nicht bekannt. Bekannt ist lediglich die Ziel-Domain, die ja in der E-Mail-Adresse hinter dem @-Zeichen steht. Um auch DNS-Anfragen nach Mailservern auflösen zu können, gibt es auf DNS-Servern spezielle Datensätze, in denen die zu einer Domain gehörenden Mailserver samt der zugehörigen IP-Adressen verzeichnet sind.

Das Resolver-Programm gibt also bei der Anfrage nur den Ziel-Domainnamen an und teilt zudem mit, dass es sich bei dem gesuchten Netzteilnehmer um einen Mailserver handelt. Der DNS-Server ermittelt die gesuchte IP-Adresse und gibt sie an das Resolver-Programm zurück.

Der Postfachname selbst wird für die DNS-Anfrage gar nicht benötigt. Er wird erst bei Eintreffen der Nachricht auf dem Ziel-Mailserver ausgewertet, damit diese im richtigen Postfach abgelegt werden kann.

4. Der Weg ins Internet

Eine entscheidende Einschränkung der heute üblichen Ethernet -Technik ist die maximale Distanz von 100m. Zwar können mit Hilfe entsprechender Komponenten wie Hubs, Switches und Routern auch größere Entfernungen erreicht werden, aber auch damit ist die Ausdehnung eines Ethernet-Netzwerkes auf das Grundstück einer Firma bzw. die Wohnung eines privaten Nutzers begrenzt.

Geht es z.B. darum, eine Verbindung zum Internet herzustellen (Datenfernübertragung, kurz DFÜ), sind oft mehrere Kilometer zu überbrücken. Internet Zugänge werden deshalb bis auf wenige Ausnahmen über das öffentliche Telefon- oder Kabelfernsehnetz abgewickelt.

4.1 Physikalische Grundlagen

Vier DFÜ-Zugangsarten haben sich durchgesetzt:

- Analoges Modem
- ISDN
- DSL
- GPRS/UMTS/EDGE
- HSPA
- LTE

Analoge Modem
Der Zugang über analoge Modem ist die ursprüngliche Art des Internet-Zugangs und wird heute nur noch dort eingesetzt, wo eine Anbindung per DSL oder einer anderen Highspeed-Technik nicht verfügbar ist.

Für den analogen Modem-Zugang wird ein normaler, analoger Telefonanschluss (kein ISDN) benutzt.

Zwischen das Endgerät, meist ein PC, und den Telefonanschluss wird ein Modem (Modulator-Demodulator) geschaltet. Als Schnittstelle zwischen z.B. PC und Modem wird meist die

serielle Schnittstelle (COM-Port / RS232) oder USB verwendet. Alternativ zu den externen Modems gibt es PC-Einsteckkarten, welche die Modem-Funktionen innerhalb des PC abwickeln.

Wird für die Übertragung das öffentliche Telefonnetz benutzt, ist es zunächst nötig, eine Einwahlverbindung zum Internet-Provider herzustellen. Auch diese Aufgabe übernimmt der Modem.

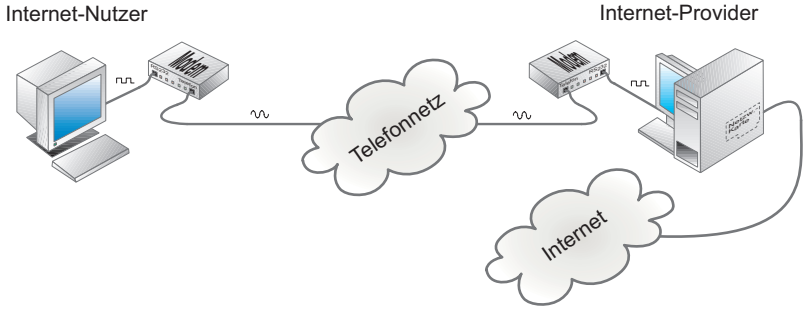
Wenn die Telefonverbindung zu Stande gekommen ist, werden die digitalen Informationen auf eine Trägerfrequenz aufmoduliert.

Wir wollen an dieser Stelle nicht näher auf die angewendeten Modulationsverfahren eingehen, sondern nur eine beispielhafte Erklärung dieser Technik geben.

Die Trägerfrequenz kann man sich vorstellen wie einen bestimmten hörbaren Ton aus dem Frequenzbereich der Sprache (300 Hz – 3.400 Hz).

Der zu übertragende Datenstrom wird in einige Bits große Blöcke zerteilt. Je nachdem welches Bitmuster vorliegt, wird der Ton in einer für dieses Bitmuster vorgegebenen Art verändert.

Am anderen Ende der Verbindungsstrecke übernimmt ein zweiter Modem die umgekehrte Aufgabe (Demodulation). Aus den empfangenen Tönen wird wieder ein Datenstrom zurückgewonnen.



Durch den eingeschränkten Frequenzbereich von analogen Telefonanschlüssen liegt die maximale Datenübertragungsrate bei 33kBit/s vom Teilnehmer in Richtung Vermittlungsstelle (Upstream). Von der Vermittlungsstelle in Richtung Teilnehmer (Downstream) sind maximal 56kBit/s möglich.

Ein großer Nachteil von DFÜ über den analogen Telefonanschluss ist neben der geringen Übertragungsrate die Tatsache, dass parallel zu DFÜ nicht telefoniert werden kann.

ISDN

Der wesentliche Unterschied zum analogen Telefonanschluss besteht darin, dass bei ISDN selbst analoge Sprachdaten bereits am Standort des Teilnehmers in digitale vermittlungstechnische Daten umgewandelt werden.

Vom Teilnehmer zur Vermittlungsstelle werden also ausschließlich digitale Daten in Form von ISDN-Netzwerkpaketen ausgetauscht.

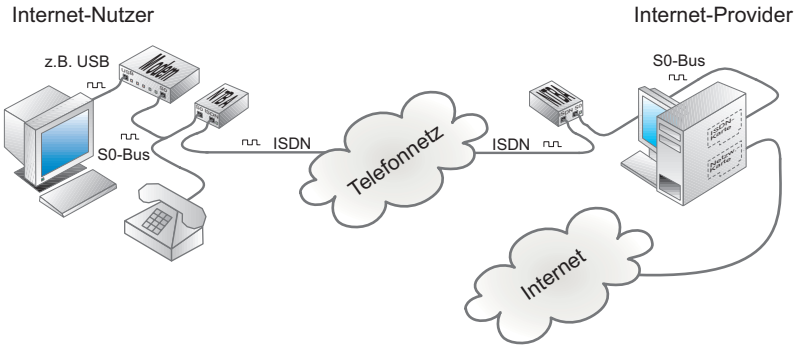
ISDN steht für Integrated Services Digital Network, was locker übersetzt so viel bedeutet wie: Integriertes digitales Netzwerk für verschiedene Dienste.

Neben der Übertragung von Sprache erlaubt ISDN von Hause aus den Austausch von digitalen Daten z.B. für Fax und DFÜ.

Eine Modulation von DFÜ-Daten ist bei ISDN im eigentlichen Sinne nicht nötig. Statt dessen werden die zu übertragenden Daten in ISDN-Pakete verpackt und versendet, wobei auch hier zunächst eine Wahlverbindung nötig ist.

Trotz dem spricht man bei externen ISDN <-> DFÜ-Daten Umsetzern gemeinhin von ISDN-Modems.

Zwischen ISDN-Modem und dem Telefonnetz bereitet der NTBA die ISDN-Daten physikalisch so auf, dass sie zur Vermittlungsstelle übertragen werden können. Die Schnittstelle zwischen den ISDN-Endgeräten und dem NTBA wird als S0-Bus bezeichnet.



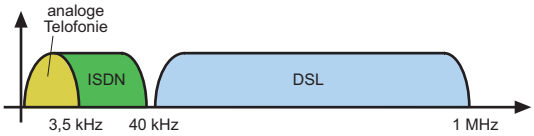
ISDN stellt dem Teilnehmer zwei Kanäle (Bereiche im ISDN-Paket) zur Verfügung, die auch für unterschiedliche Dienste, z.B. Telefonieren und DFÜ, genutzt werden können.

Pro Kanal können 64kBit/s übertragen werden. Bei paralleler Nutzung beider Kanäle (Kanalbündelung) erhöht sich die Transferrate auf 128kBit/s.

DSL

Digital Subscriber Line (deutsch: Digitale Teilnehmeranschlussleitung) bietet zur Zeit die attraktivste Möglichkeit, sich mit dem Internet zu verbinden.

Analoge Anschlüsse arbeiten auf dem Kabel mit Frequenzen bis max. 3,5 kHz. Bei ISDN liegt die Obergrenze bei ca. 40 kHz. DSL nutzt ausschließlich Frequenzen, die oberhalb 40kHz bis ca. 1MHz angesiedelt sind. Damit kann DSL parallel zu analogen oder ISDN-Anschlüssen über das selbe Kabel betrieben werden. Am Standort des Teilnehmeranschlusses wird über einen Splitter (eine Frequenzweiche) das DSL-Signal von den Telefonsignalen getrennt.



Die Übertragung der DSL-Daten funktioniert ähnlich wie beim

analogen Modem, nur dass gleichzeitig mit mehreren, deutlich höheren Trägerfrequenzen gearbeitet wird.

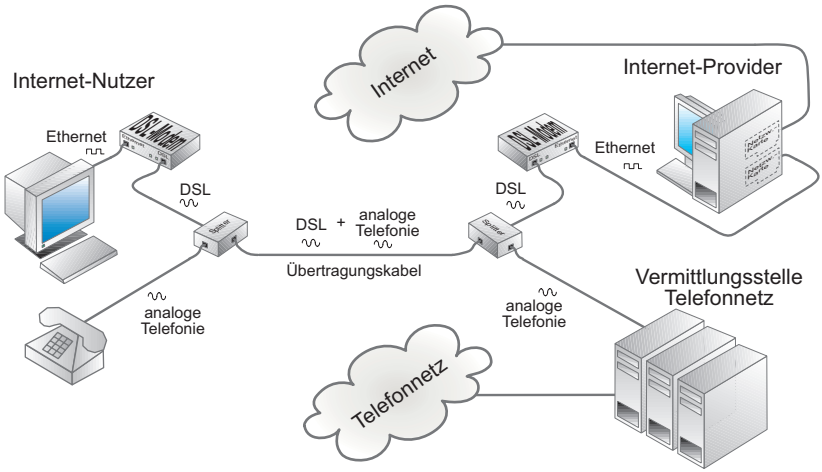
DSL gibt es in verschiedenen Varianten:

ADSL - Asymmetric Digital Subscriber Line
ADSL-Zugänge werden meist von Privatkunden genutzt und lassen beim Download Übertragungsraten von max. 16MBit/s zu. Da die Upstream-Geschwindigkeit nur ca. ein Achtel der Downstream-Geschwindigkeit beträgt, spricht man auch von asymetrischer Datenübertragung.

SDSL- Symmetric Digital Subscriber Line
Bei SDSL wird in beide Richtungen mit der gleichen Übertragungsgeschwindigkeit von max. 2MBit/s gearbeitet. SDSL-Zugänge werden bevorzugt von gewerblichen Kunden genutzt - z.B. um zwei Firmenstandorte netzwerktechnisch miteinander zu verbinden.

VDSL - Very Highspeed Digital Subscriber Line
Da immer mehr Dienste wie z.B. Fernsehen oder Telefonie das Internet als Übertragungsweg nutzen, steigt zunehmend der Bedarf an sehr schnellen Internet-Zugängen. VDSL arbeitet ähnlich wie ADSL, aber mit deutlich höheren Übertragungsraten von über 50MBit/s im Downstream und 11MBit/s im Upstream.

Für alle DSL-Standards gilt: Je größer die Entfernung zur Vermittlungsstelle, desto geringer die mögliche Übertragungsgeschwindigkeit.



Auf Grund der hohen Übertragungsgeschwindigkeit tauschen DSL-Modems die Daten mit dem PC über USB oder direkt über Ethernet aus. Eine häufige Variante ist ein Ethernet Router mit DSL-Anschluss.

Kabel-Modem

Der Internet-Zugang über ein Kabel-Modem ist inzwischen eine echte Alternative zum DSL-Anschluss. Der Zugang erfolgt über das Kabelfernsehnetz. In den 80er Jahren wurde das Kabelfernsehnetz für die Verteilung von Fernseh - und Radiokanälen aufgebaut und war nur dazu bestimmt Signale vom Anbieter zum Kunden zu transportieren. Nachdem die Netzbetreiber den zunehmenden Bedarf an Internet-Zugängen erkannten, wurde der notwendige Rückkanal vom Kunden Richtung Anbieter nachgerüstet.

Physikalisch sind die Bestandsnetze mit Koaxialkabeln aufgebaut. Für Netzerweiterungen und neue Netze kommen Lichtwellenleiter zum Einsatz.

Die Verbindung zwischen Kabelfernsehnetz und lokalem Netzwerk bildet das Kabel-Modem bzw. ein spezieller dazu ausgestatteter Router.

Die mögliche Übertragungsgeschwindigkeit liegt bei

32MBit/s und mehr.

GPRS/EDGE und UMTS
Eine Alternative zu den vorangegangenen Festnetzvarianten ist die Verbindung mit dem Internet über die Mobilfunknetze.

Eine detaillierte Beschreibung der Mobilfunktechnik würde den Rahmen des Buches sprengen. Deshalb wollen wir an dieser Stelle nur einen sehr oberflächlichen Überblick vermitteln.

Aktuell gibt es drei technische Mobilfunkvarianten:

- GSM - Global System for Mobile Communications
- UMTS - Universal Mobile Telecommunications System
- LTE - Long Term Evolution

GSM - Global System for Mobile Communications
ist der ursprüngliche und erste Standard der digitalen Mobilfunktelefonie und technische Grundlage der D- und E-Netze. GSM arbeitet in einem Frequenzbereich zwischen 890MHz und 960MHz. Innerhalb dieses Bereiches gibt es je 124 Kanäle je Übertragungsrichtung. Innerhalb jeder Einzelfrequenz teilen sich 8 Kanäle die Übertragungszeit. Durch Datenkompressionsverfahren können so 8 Teilnehmer gleichzeitig über die selbe Sende- bzw. Empfangsfrequenz telefonieren.

GPRS - General Packet Radio Service
Obwohl der Focus bei GSM auf die Übertragung von Sprachdaten gelegt wurde, bietet GSM die Möglichkeit mittels GPRS Daten zu übertragen. Auch für die Datenübertragung stehen pro Frequenz 8 Kanäle zur Verfügung.

Bei der Telefonie wird für die Dauer eines Gespräches eine Verbindung aufgebaut, die in jede Richtung einen Kanal blockiert.

Bei der Datenübertragung mit GPRS wird ein Kanal nur dann blockiert, wenn wirklich Daten gesendet werden und kann so zeitversetzt von mehreren Teilnehmern genutzt werden. Auch die parallele Nutzung mehrerer Kanäle durch einen Teilnehmer ist zulässig. So können Übertragungsraten von bis zu

55,6kbits/s erreicht werden, was in etwa der Übertragungsgeschwindigkeit analoger Modem entspricht.

EDGE - Enhanced Data Rates for GSM Evolution
EDGE ist eine Weiterentwicklung der GSM-Technik und basiert auf effizienteren Datenmodulations- bzw. Kompressionsverfahren. GPRS wird mit EDGE zu E-GPRS (Enhanced GPRS) und erlaubt Datenraten bis zu 220kbit/s (Download) bzw. 110kbit/s (Upload).

Da EDGE nur eine Erweiterung von GSM ist, können im gleichen Netz, Endgeräte beider Techniken betrieben werden.

UMTS - Universal Mobile Telecommunications System
Mit UMTS entstand nach der Analogen Mobiltelefonie und GSM die dritte Generation der Mobilfunktechnik. Bei UMTS steht nicht mehr die Telefonie im Vordergrund. Vielmehr wurde UMTS bereits bei der Entwicklung auf die Nutzung vielfältiger multimedialer Dienste ausgerichtet.

UMTS-Endgeräte senden über ein Frequenzband von 1920MHz bis 1980MHz und empfangen bei 2110MHz bis 2170MHz. Die benutzbaren Einzelfrequenzen liegen jeweils 5MHz auseinander. Auf einer Einzelfrequenz können mehrere hundert Kanäle betrieben werden. Diese gleichzeitige Nutzung einer Frequenz wird nicht, wie bei GSM über feste zeitliche Zuordnung geregelt. Bei UMTS regelt ein spezielles Protokoll die Nutzung. So können wenige Nutzer auf einer Frequenz große Datenmengen übertragen oder die Frequenz kann von vielen Nutzern zur Übertragung geringerer Datenmengen in Anspruch genommen werden.

Auf diese Weise lassen sich Übertragungsraten von bis zu 384kbit/s erreichen.

HSPA, HSDPA/HSUPA - High Speed Packet Access
HSPA ist eine Weiterentwicklung von UMTS. Es wird das gleiche Frequenzband und die gleiche Sendetechnik auf Provider-Seite verwendet. Dabei kommt allerdings ein deutlich verbessertes Modulations- und Kodierungsverfahren zum Einsatz. Um ein Maximum an Effizienz zu erreichen, wird beim

Download (HSDPA) anders gearbeitet, als beim Upload (HSUPA). Der Grund hierfür liegt darin, dass die Sendeeinrichtung auf Provider-Seite deutlich mehr Sendeleistung zur Verfügung hat, als das Mobile Endgerät des Kunden.

Beim Download mit HSDPA können bis zu 42MBit/s erreicht werden. Beim Upload sind bis zu 5,8MBit/s möglich.

LTE - Long Term Evolution

In Verbindung mit LTE wird oft von der vierten Mobilfunkgeneration gesprochen, Das ist nicht ganz richtig. LTE ist ein reines, IP-basierendes Datennetz. Für die Telefonie nutzen LTE-fähige Endgeräte z.Zt. immer noch das ganz normale GSM/UMTS-Netz.

Mit LTE soll erstmals ein international einheitlicher Mobilfunkstandard geschaffen werden. Deshalb ist LTE, was die benutzten Funkfrequenzen angeht flexibel. In Deutschland werden zwei Frequenzbereiche genutzt:

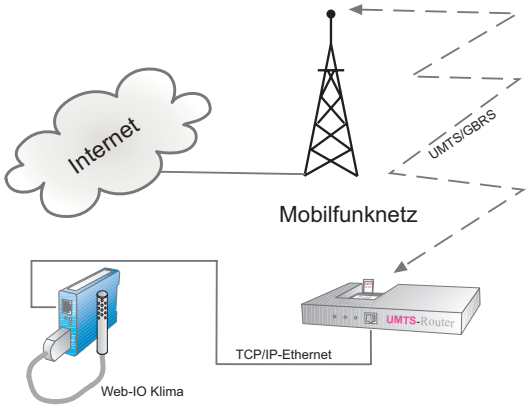
- 800MHz
- 2,6GHz

Das 800MHz Frequenzband wurde ehemals für die Übertragung analoger Fernsehkanäle genutzt und ist mit dem Wegfall dieser Technik freigeworden. Ein großer Vorteil dieses Frequenzbandes ist die große Reichweite von bis zu 30km. Damit können auch ländliche Gebiete gut mit LTE abgedeckt werden. Das 2,6GHz Frequenzband kommt vorrangig in Ballungsgebieten mit räumlich kleineren Funkzellen zum Einsatz. Ein effizienteres Kodierungsverfahren und eine deutlich verbesserte Technik auf Provider-Seite erlauben Übertragungsraten von bis zu 100MBit/s (theoretisch sogar 300MBit/s) beim Download und 50MBit/s (theoretisch sogar 100MBit/s) beim Upload.

Durch die hohen Übertragungsgeschwindigkeiten, bietet sich LTE als Alternative zum DSL-Anschluss an. Allerdings teilt sich die gesamte in einer Funkzelle verfügbare Bandbreite, wie bei den anderen Mobilfunktechniken auch, auf die Anzahl der aktiven Nutzer auf.

Technische Voraussetzungen

Um sich als Einzel-User über das Mobilfunknetz mit dem Internet zu verbinden, benötigt man entweder ein Smartphone (Tablet), einen Surf-USB-Stick ober eine entsprechende PCMCIA Karte für den PC.



Um beliebige Ethernet-Endgeräte über Mobilfunk mit dem Internet zu verbinden, können Router mit dem entsprechenden Mobilfunkzugang eingesetzt werden.

4.2 Übertragungsprotokolle

Die im vorigen Abschnitt beschriebenen Übertragungsverfahren analoge Modemübertragung, ISDN, DSL und die verschiedenen Mobilfunkzugänge sind für sich betrachtet nur physikalische Standards, die aber nichts darüber aussagen, in welcher Form der Datenstrom transportiert wird.

Um Daten per DFÜ zwischen zwei Netzwerkstandorten auszutauschen, ist ein übergeordnetes Protokoll nötig, welches folgende Aufgaben übernimmt:

- Aufbau einer logischen Verbindung zwischen beiden Standorten
- Authentifizierung (Prüfen der Zugangsberechtigung)
- Aufbereitung des eingehenden Datenverkehrs für die Übertragung und Wiederherstellen des ursprünglichen Da-

tenformates am Ende der Übertragungsstrecke
- Datensicherung
- Verschlüsselung der Übertragungsdaten
- Abbau der logischen Verbindung nach Abschluss der Datenübertragung

SLIP - Serial Line IP Protocol

Ein erster Ansatz für die Übertragung von DFÜ-Daten war SLIP. SLIP ist ein sehr einfaches Protokoll, das ausschließlich für den Transport von IP-Datenverkehr geeignet ist und nicht alle oben aufgeführten Anforderungen erfüllt.

Die kompletten IP-Datenpakete werden bei SLIP einfach um ein festgelegtes Start- und Endezeichen erweitert. Zufällig im IP-Paket vorkommende Zeichen dieses Typs ersetzt der Sender durch eine Kombination aus Ersatzzeichen.

So präpariert wird Paket für Paket auf die Leitung gegeben.

An den Start-/Ende-Zeichen eines Pakets erkennt der Empfänger wo das eigentliche IP-Paket beginnt bzw. endet. Die Ersatzzeichen werden vom Empfänger wieder gegen das Original ausgetauscht und die Start-/Endezeichen entfernt.

Durch die Beschränkung auf IP-Datenübertragung und fehlende Sicherheitsmechanismen wird SLIP heute für normale Internetzugänge nicht mehr benutzt. Dort wo räumlich abgesetzte Netzwerksegmente über Distanzen verbunden werden sollen, die mit einer normalen Ethernet-Verkabelung nicht mehr möglich sind, ist Slip aber nach wie vor eine zweckmäßige Lösung.

Die W&T Com-Server können z.B. als SLIP-Router konfiguriert werden und somit TCP/IP-Daten über eine RS232 oder RS422 Verkabelung übertragen.

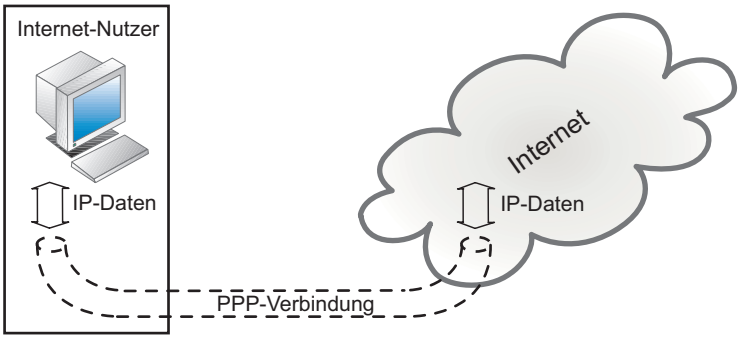
PPP - Point-to-Point Protocol

Um allen Anforderungen für eine Datentunnelung zwischen zwei Netzwerkstandorten gerecht zu werden, wurde PPP ent-

wickelt.

Sowohl für den Zugang ins Internet als auch zur Verbindung mit einem entfernten nicht öffentlichen Netzwerk sorgt PPP für eine gesicherte Datenübertragung.

Dazu stellt PPP sozusagen einen Tunnel durch die netzwerkfremde Umgebung her.



Der Aufbau einer PPP-Verbindung findet in mehreren Schritten statt und bedingt eine bestehende physikalische Verbindung wie z.B. DSL oder ISDN:

1. Aushandeln der Verbindungsoptionen
   Um festzulegen, mit welchen Optionen PPP arbeiten soll, wird das LCP-Protokoll - Link Control Protocol benutzt.
   Verhandelbar sind unter anderem:
   - Art der Authentifizierung
   - Blockgröße der Übertragungsdaten
   - Datenkompression
   - Art der zu übertragenden Daten (IP, IPX, ...)

2. Authentifizierung
   Hierbei werden User-ID und ein Passwort übergeben. Es gibt zwei Arten der Passwortübergabe:
   - PAP - Password Authentication Protocol
     Passwortübergabe lesbar im Klartext
   - CHAP - Challenge Handshake
     verschlüsselte Passwortübergabe

3. Konfiguration übergeordneter Netzwerkprotokolle

Soll über PPP eine Verbindung in Netze mit übergeordneten Protokollen (z.B. Internetprotokoll) hergestellt werden, ist es erforderlich bestimmte, das entsprechende Protokoll betreffende Einstellungen vorzunehmen.
Die nötigen Informationen werden mittels des NCP - Network Control Protocol übergeben. Im Falle eines Internetzugangs über PPP wird als NCP das Internet-spezifische IPCP - Internet Protocol Control Protocol verwendet. IPCP erlaubt z.B. für die Dauer der PPP-Verbindung die Vergabe einer IP-Adresse (mehr zum Internet Protokoll im nächsten Abschnitt).

4. Übertragung der Nutzdaten
   Sobald alle Verbindungsoptionen festgelegt sind und der Nutzer seine Zugangsberechtigung nachgewiesen hat, beginnt der eigentliche Austausch von Nutzdaten.
   Im Fall einer Verbindung zum Internet können das Daten in Form aller IP-basierenden Protokolle sein (UDP, TCP, Telnet, FTP, HTTP...).

5. Abbau der PPP-Verbindung
   Auch der Verbindungsabbau wird über LCP abgewickelt.

Ähnlich wie Ethernet bettet PPP die zu transportierenden Daten in eine festgelegte Paketstruktur:

Flag	Address	Control	Protocol	Information	FCS	Flag
1 Byte	1 Byte	1 Byte	1 oder 2 Byte	n Byte	2 Byte	1 Byte

Flag (1 Byte)
Startzeichen zur Paketsynchronisation bzw. Paketerkennung

Address (1 Byte)
Eine Punkt- zu- Punkt-Verbindung erfordert keine Adressierung.

Trotzdem ist dieses Feld aus Kompatibilitätsgründen zu anderen Netzwerkprotokollen vorhanden, wird aber von PPP nicht benutzt und ist willkürlich mit dem Wert 255 gefüllt.

Control (1 Byte)
Dieses Feld war ursprünglich zur Nummerierung der Pakete vorgesehen, hat bei PPP aber immer den Wert 3, da ohne Paketnummerierung gearbeitet wird.

Protocol (1 oder 2 Byte)
Der Inhalt dieses Feldes gibt an, wie das aktuelle PPP-Paket genutzt wird: Verbindungsaufbau, Steuerinformation, Authentifizierung, Datentransport, Verbindungsabbau, ...

Information (n Byte)
An dieser Stelle wird die eigentliche Information (z.B. IP-Daten) übertragen. Bei Steuerpaketen stehen hier die Steueroptionen im LCP-Format.

Die Größe dieses Feldes ist per LCP verhandelbar, beträgt in aller Regel aber 1500 Byte. Ist die zu transportierende Information kleiner, werden Füllzeichen aufgefüllt.

FCS (2 Byte)
Checksumme zur Kontrolle der empfangenen Daten

Flag (1 Byte)
Endezeichen zur Paketsynchronisation

Durch die Möglichkeit, über eine PPP-Verbindung verschiedene unabhängige IP-Dienste und Protokolle gleichzeitig zu betreiben, können durch Einsatz geeigneter Router auch ganze Netzwerke über PPP verbunden werden.

5. Web-IO - Der Browser als Bedienoberfläche

In den ersten 20 Jahren seines Daseins war die Nutzung des Internets für normale Menschen kaum interessant. Eine für heutige Verhältnisse kleine Gruppe von Insidern musste kryptische Befehlszeilen eintippen, um Informationen austauschen zu können. Erst mit der Entwicklung des WWW-Standards, eines über das Internet abrufbaren Hypertext-Systems (World Wide Web), erschloss sich das Internet einem immer breiter werdenden Publikum.

Um die Möglichkeiten des WWW nutzen zu können, benötigt der Anwender einen Internetbrowser – ein Client-Programm, das über eine graphische Oberfläche die Inhalte von Webseiten anzeigt, die auf WWW-Servern hinterlegt sind.

Mit der Eingabe eines URL (Uniform Resource Locator) teilt der Anwender dem Browser mit, wie und wohin die Verbindung hergestellt werden soll. Er gibt zunächst vor, welches Protokoll genutzt wird; für den Zugriff auf Webseiten z.B. HTTP. Auf das Protokoll folgt dann die Angabe auf welchem Webserver die gewünschte Webseite liegt und wo diese dort genau zu finden ist.

```
protokoll://hostname [:tcp-port] [/pfadname][/filename][?weitere parameter]
```

http://www.wut.de/pdf/e-wwwww-12-prde-000.pdf

öffnet z.B. die Produktübersicht von W&T.

Die meisten Browser unterstützen noch weitere Protokolle, wie FTP zur Dateiübertragung (ftp://www.wut.de/download/e-58www-19-swde-000zip startet z.B. den Download der Programmbeispiele zu diesem Buch) oder Telnet. Telnet wird häufig genutzt, um Embedded Systeme via Netzwerk zu konfigurieren (Mit telnet://<IP-Adresse eines W&T Com-Servers>:1111 wird z.B. der Zugriff auf den Konfigurationsport eines W&T Com-Servers eingeleitet.)

Webseiten liegen als Hypertext vor und können neben Textinformationen auch Verweise auf Bilder, Graphiken und weite-

re multimediale Inhalte enthalten. Wie all diese Elemente im Browser angezeigt werden sollen, ist ebenfalls im Hypertext hinterlegt.

Neben der statischen Anzeige von Informationen können über Webseiten jedoch auch Aktionen ausgelöst und Elemente dynamisch dargestellt werden. Das Grundgerüst einer Webseite kann mit HTML realisiert werden; für die Einbindung von interaktiven bzw. dynamischen Elementen stehen verschiedene Techniken zur Verfügung. Den Aufbau einer solchen Webseite werden wir Ihnen im Folgenden erläutern und anhand einiger Beispiele darlegen.

5.1 HTML – Hypertext Markup Language

Eines der Probleme im WWW war zunächst die Vielzahl unterschiedlicher Rechner und Betriebssysteme. Eine einheitliche Softwareschnittstelle auf Anwenderebene gab es nicht. Aus dem Bedürfnis heraus, eine auch für den Laien einfach zu bedienende Oberfläche zu schaffen, die sich auf verschiedensten Rechnern gleich darstellt, wurde HTML entwickelt.

HTML ist eine Auszeichnungssprache (Markup Language) die sich aus Schlüsselwörtern – auch Tags genannt – und den darzustellenden Inhalten zusammensetzt. Die Tags geben an, in welcher Art und Weise der nachfolgende Text darzustellen ist. So lassen sich z.B. Schriftgröße, -art und -ausrichtung vorgeben, Inhalte können in Tabellen oder in Form einer numerischen Aufzählung dargestellt werden, die Farbe von Text und Hintergrund kann festgelegt werden usw. Der Browser interpretiert diese Angaben und stellt sie dar.

Neben Text können mit Hilfe von HTML auch Grafiken angezeigt werden, und sogar multimediale Inhalte wie Musik, Sprache oder Filmsequenzen lassen sich per HTML einbinden. Das HTML-Dokument selbst transportiert dabei ausschließlich Textinhalte. Für jedes andere darzustellende Element wird via HTML angegeben, von wo es geladen werden kann, wo es auf dem Bildschirm erscheinen soll und in welcher Größe es dargestellt werden soll.

Die wohl wichtigste Eigenschaft von HTML liegt darin, dass alle Elemente mit einem Verweis – auch *Hyperlink* oder kurz *Link* genannt – versehen werden können. Klickt der Anwender ein solches Element mit der Maus an, wird er automatisch auf eine weitere Website weitergeleitet, bekommt eine Grafik angezeigt oder startet einen Download.

Mit der Erklärung der von HTML bereitgestellten Tags lassen sich ganze Bücher füllen. Deshalb beschränken wir uns hier auf die elementaren Tags und Eigenschaften von HTML.

Für HTML-Tags gilt ein festes Schema:

- Einzelne Tags sind in spitze Klammern „eingepackt". *<HTML-Tag>*
- Das eigentliche Tag kann durch Angabe von Attributen erweitert werden. *<HTML-Tag Attribut="xy">*
- Überwiegend wird durch die paarweise Verwendung von Tags der Anfang und das Ende ihres Gültigkeitsbereichs festgelegt; die definierten Eigenschaften gelten dann für alles was zwischen den Tags steht. Das schließende Tag wiederholt das öffnende Tag mit einem vorangestellten Schrägstrich. Beispiel: <title>Willkommen</title>
- Bei HTML-Tags wird nicht zwischen Groß- und Kleinschreibung unterschieden. *<HTML>* ist gleichbedeutend mit *<html>.*

Grundsätzlicher Aufbau einer HTML-Datei

Jede HTML-Datei wird mit *<HTML>* eingeleitet und endet mit *</HTML>.* Man unterscheidet beim weiteren Aufbau einer Seite zwischen Kopf und Körper.

Alle Angaben im Kopf bleiben für den Betrachter unsichtbar und enthalten Eigenschaften der Seite, die nicht direkt die Darstellung betreffen. Einzige Ausnahme ist der Titel, der in der Titelleiste des Browserfensters angezeigt wird. Die Kopfinformationen stehen zwischen den Tags *<head>* und *</head>*

Auf den Kopf folgt der Seitenkörper, der mit dem *<body>*-Tag

eingeleitet wird. Im Körper der HTML-Seite sind alle Angaben zu finden, die den eigentlichen Inhalt der Seite und dessen Darstellung betreffen. Das Ende des Körpers wird mit dem *</body>* Tag gekennzeichnet.

Hier ein einfaches Beispiel:

```
<html>
  <head>
    <title>WuT Service</title>
  </head>
  <body bgcolor="#FFFFFF">
    Willkommen bei WuT.de
  </body>
</html>
```

Bitte beachten Sie, dass beim *<body>*-Tag das Attribut *bgcolor="#FFFFFF"* für einen weißen Hintergrund angegeben wurde. Im Browser sieht das dann so aus:

Hyperlinks

Einer der großen Vorteile von HTML liegt in der Möglichkeit, einzelne Inhaltselemente mit einem Hyperlink zu versehen. Klickt der Anwender auf ein solches verlinktes Element, wird er auf eine andere Webseite weitergeleitet.

Wir erweitern unseren HTML-Code um einen Hyperlink:

```
  <body bgcolor="#FFFFFF">
    Willkommen bei <a href="http://www.wut.de/index.html">WuT.de</a>
```

```
</body>
```

Bei einem Mausklick auf „WuT.de“ werden wir nun auf die Homepage von W&T gelenkt.

Das Pfadattribut des Tags *<a href=“Pfadangabe“>* kann die Pfadangabe entweder in absoluter oder in relativer Form enthalten.

- Absolut: es wird der komplette URL angegeben, auf den der Hyperlink verweisen soll.
- Relativ: es wird nur der Name der Datei angegeben auf die zugegriffen werden soll. Die Datei wird dann im gleichen Verzeichnis gesucht, in dem sich auch die aktuelle HTML-Datei befindet.

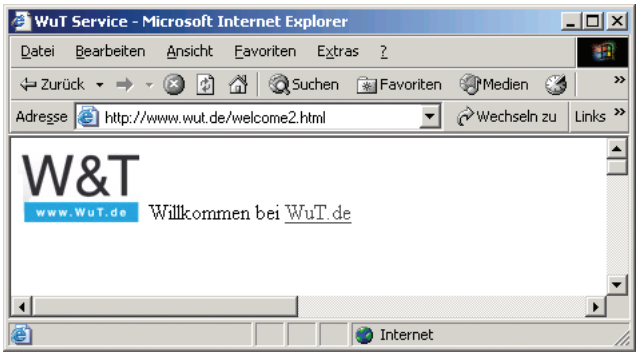
Darstellung von multimedialen Inhalten
Wie bereits angesprochen, erlaubt HTML die Darstellung von Inhalten, die nicht Bestandteil des HTML-Dokuments sind, sondern von anderer Stelle nachgeladen werden.

Bilder
Zur Einbindung von Bilddateien stellt HTML z.B. das *<img>*-Tag (*img* für Image) zur Verfügung, wobei über das Attribut *src* Namen und Quelle der Bilddatei angegeben werden.

Wir erweitern unser HTML-Dokument um eine Grafik:

```
<body bgcolor="#FFFFFF">
  <img src="http://www.wut.de/kpcs/logo5.gif">
  Willkommen bei <a href="http://www.wut.de/index.html">WuT.de</a>
</body>
```

Nun wird neben dem Text ein Logo im GIF-Format dargestellt, das aus dem Verzeichnis *kpics* auf dem Webserver von W&T geladen wird. Der Pfad der Bilddatei kann wie auch beim Hyperlink absolut oder relativ angegeben werden.

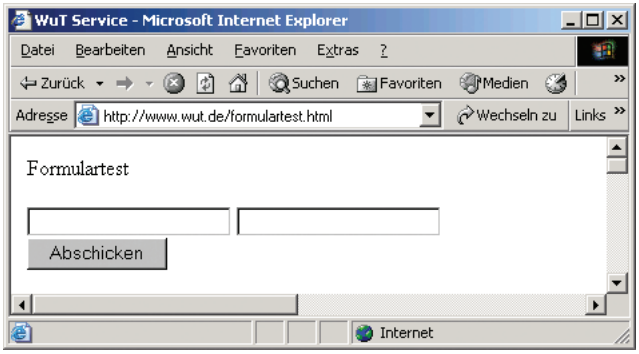


Formulare

HTML ist eine reine Darstellungssprache, die eine statische Anzeige im Browser generiert. Aber wie sieht es aus, wenn der Anwender Informationen an den WWW-Server zurückgeben möchte?

Als Lösung bietet HTML die Möglichkeit, Formulare anzuzeigen, die vom Anwender ausgefüllt werden können. Die so eingegebenen Informationen können durch Anklicken eines sogenannten „Submit-Buttons“ vom Browser zum WWW-Server gesendet werden.

Hier ein kurzes Beispiel:



Im HTML-Code sieht das so aus:

```
<html>
  <head>
    <title>WuT Service</title>
```

```
  </head>
  <body bgcolor="#FFFFFF">
    Formulartest
    <form method="post" action="Formularauswertung.cgi" name="FORMULAR1">
      <input type="text" name="EINGABEFELD1">
      <input type="text" name="EINGABEFELD2">
      <input type="submit" name="submit" value="Abschicken">
    </form>
  </body>
</html>
```

Sämtliche zum Formular gehörenden Elemente sind zwischen dem einleitenden *<form>*-Tag und dem abschließenden *</form>*-Tag zu finden.

Die Attribute des Form-Tags sind:

method	gibt an, wie HTTP die Eingaben an den WWW-Server übergibt.
action	legt fest, an welchen Prozess auf dem Server die Eingaben übergeben werden.
name	kann willkürlich vergeben werden und zeigt dem Prozess auf dem Server, von welchem Formular die Eingaben stammen (ein Prozess kann ggf. mehrere Formulare auswerten).

Die Eingabeelemente selbst werden über das *<input>*-Tag festgelegt, wobei das Attribut *type* angibt, um welche Art von Eingabeelement es sich jeweils handelt. Mögliche Attribute sind hier:

text	Texteingabefeld
checkbox	Ankreuzkästchen
radio	Optionsbutton
submit	Button zum Abschicken oder Zurücksetzen des Formulars

Über das Attribut *name* kann dem Element ein eindeutiger Name (vergleichbar mit einem Variablennamen) gegeben werden; mit dem Attribut *value* kann ihm ein Anfangswert zuge-

teilt werden.

Die Angabe *<"input type="text" name="EINGABEFELD1" value="test1">* würde z.B. dazu führen, dass beim Öffnen des Formulars im Browser schon der Text *test1* im ersten Eingabefeld stehen würde.

Was mit den per Formular übergebenen Informationen geschieht – ob der Anwender eine Rückmeldung erhält und wie diese aussieht –, bestimmt allein der Prozess auf dem WWW-Server, der die Informationen entgegennimmt und auswertet.

Wie bereits angesprochen, möchten wir hier nicht bis auf das letzte Detail von HTML eingehen. Wer Webseiten erstellen möchte, sollte sich auf jeden Fall eingehender mit diesem Thema beschäftigen. Eine hervorragende Quelle für weitere Informationen zu HTML findet man unter *http://www.selfhtml.org;* sehr nützlich ist selbstverständlich auch die Website des W3-Konsortiums (*http://www.w3.org*), das in Sachen HTML als normierende Körperschaft fungiert.

5.2 Interaktive bzw. dynamische Elemente

Es gibt verschiedene Möglichkeiten, über im Browser angezeigte Webseiten Aktionen auszulösen und Elemente dynamisch darzustellen.

Dazu ist auf jeden Fall ein Programm, bzw. ein Prozess nötig, der z.B. Eingaben vom Anwender entgegennimmt und entsprechende Reaktionen auslöst. In technischen Anwendungen ist es sinnvoll, dass sich angezeigte Werte und Prozessabbilder selbstständig aktualisieren.

Unterschieden wird zwischen Programmen, die auf dem WWW-Server aktiv sind und solchen die im Browser, also auf dem lokalen Rechner ablaufen. Auch eine Kombination von beidem ist oft zu finden.

Serverseitige Programme

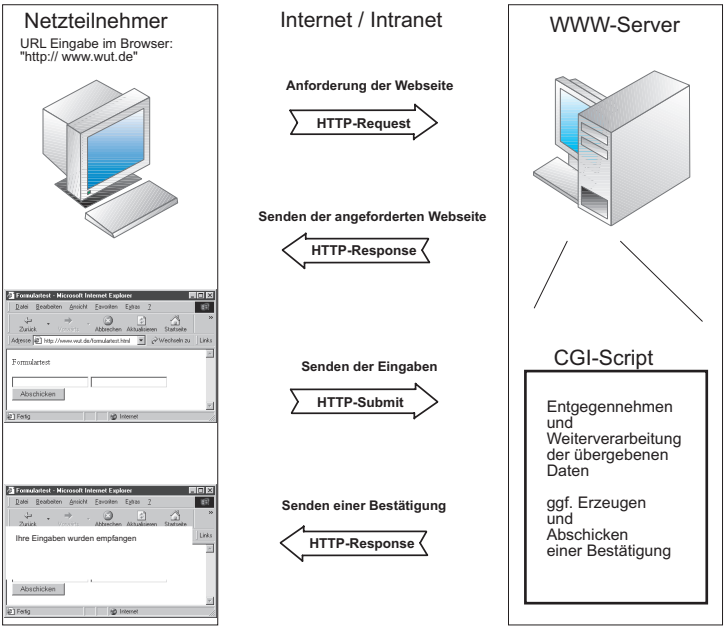
CGI - Common Gateway Interface

Der Einsatz von CGI-Scripten war lange Zeit das meistgenutzte Verfahren, im Browser interaktive Inhalte anzuzeigen bzw. Aktionen auszulösen.

Über CGI können vom Browser aus Programme auf dem WWW-Server ausgeführt werden.

Über einen Hyperlink, einen Submit-Button oder direkte Eingabe des URL wird das entsprechende Programm aufgerufen und es werden ggf. die nötigen Parameter übergeben.

Ein klassisches Beispiel sind HTML-Formulare, die vom Anwender ausgefüllt werden. Klickt der Anwender den Submit-Button (Abschicken) werden die Eingaben via http mit Hilfe des POST-Kommandos an den WWW-Server übergeben. Das angegebene CGI-Script wird gestartet und verarbeitet die Eingaben weiter.



Weitere mögliche Anwendungen sind Besucherzähler, Gäste-

bücher, Diskussionsforen, Datenbankzugriffe oder Suchmaschinen.

CGI-Scripte können grundsätzlich in allen gängigen Programmiersprachen erstellt werden. Wichtig ist, dass der WWW-Server die gewählte Sprache unterstützt.

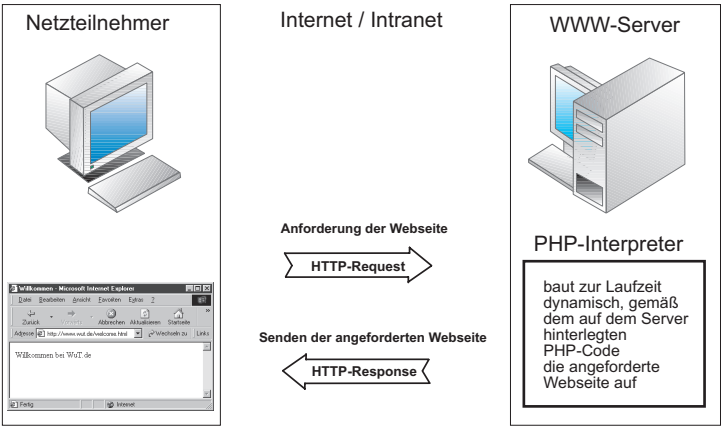
In der Praxis hat sich Perl für die Erstellung von CGI-Scripts durchgesetzt.

PHP

PHP hat CGI heute als meistgenutztes Verfahren für die Darstellung interaktiver Inhalte abgelöst und wird z.Zt. in den Versionen PHP3, PHP4 und PHP5 verwendet.

Auch PHP erlaubt das Ausführen von Programmen auf einem WWW-Server. PHP ist eine Interpretersprache, deren Quelltext in eine HTML-Seite eingebunden ist, die auf dem WWW-Server liegt. Dabei können statische Inhalte der Seite im HTML-Format definiert werden, wogegen veränderbare Inhalte durch PHP-Quellcode eingebracht werden. PHP kann auch auf andere Resourcen auf dem Server, wie z.B. Datenbanken zugreifen.

Bei Anforderung der entsprechenden Seite durch den Browser wird der in der Seite integrierte PHP-Code auf dem Server vom PHP-Interpreter ausgewertet. Der PHP-Interpreter erzeugt individuell eine Seite in HTML-Code. Die so entstandene Webseite wird dann vom Server via http zum Browser gesendet. Der PHP-Quellcode bleibt für den Anwender unsichtbar.



Beim Onlineshopping könnte man zum Beispiel zu den offerierten Artikeln dynamisch Lagerstückzahlen, Lieferzeiten und Preise aus einer Warenwirtschaftsanwendung via PHP in die Webseite einbringen. Das bedingt natürlich, dass auf dem Server ein PHP-Interpreter aktiv ist.

ASP - Active Server Pages

ASP ist eine von Microsoft ins Leben gerufene Art, Webseiten dynamisch anzuzeigen. ASP-basierende Webseiten bestehen wie auch bei der PHP-Technik aus klassischen HTML-Anteilen und Scripten, die bei Aufruf der Webseite serverseitig ausgeführt werden. Ein Interpreter auf dem WWW-Server generiert, gesteuert durch diese Scripte, Webseiten in normalem HTML-Format.

Als Scriptsprachen werden zumeist VBScript (Visual Basic Syntax) oder JScript (Java Syntax) verwendet.

Ein Vorteil dieser Technik besteht darin, auf dem Server installierte DLLs und AktivX-Komponenten nutzen zu können. Dynamic Link Libraries und AktivX-Komponenten sind fertige, ausgelagerte Programmfunktionen, die dem Programmierer Arbeit abnehmen, da entsprechende, oft komplexe Funktionalitäten nicht selbst programmiert werden müssen.

Der Nachteil von ASP liegt in den Server-Betriebssystemvoraussetzungen. Im Ursprung gab es ASP-Unterstützung nur

auf Microsoft Serversystemen. Von Drittherstellern gibt es seit einiger Zeit aber auch ASP-Varianten für Linux-Server.

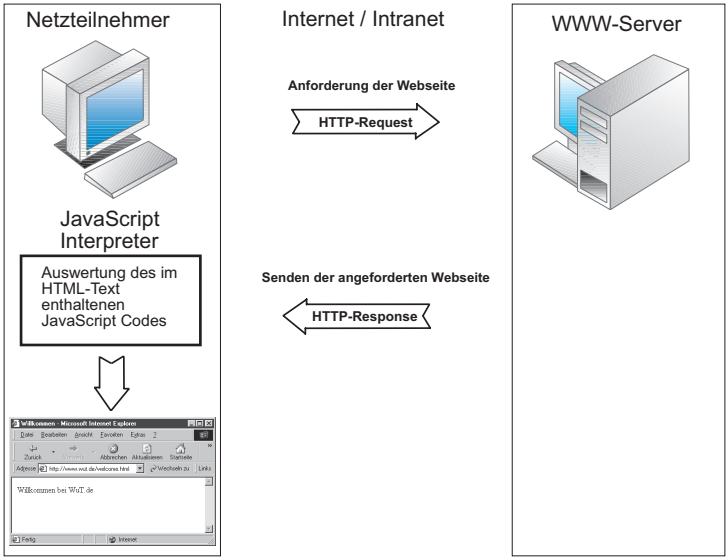
ASP-basierende Webseiten erkennt man an der Endung „.asp“ im Dateinamen.

Das klassische ASP wurde von Microsoft inzwischen durch ASP.NET abgelöst.

Browserseitige Programme

JavaScript

Bei JavaScript wird der Quellcode in den HTML-Text der Seite eingebunden. Der JavaScript Code wird mit dem <SCRIPT language="JavaScript"> Tag gekennzeichnet und beim Laden einer Webseite vom Browser erkannt, interpretiert und ausgeführt.



Mit JavaScript können z.B. individuelle Anpassungen der angezeigten Inhalte einer Webseite vorgenommen werden, indem Variablen angelegt werden. In Abhängigkeit des Wertes einer Variablen kann dann entschieden werden, wie bestimmte Dinge dargestellt werden. Auch Benutzereingaben lassen

sich überprüfen, bevor sie zum WWW-Server weitergeleitet werden.

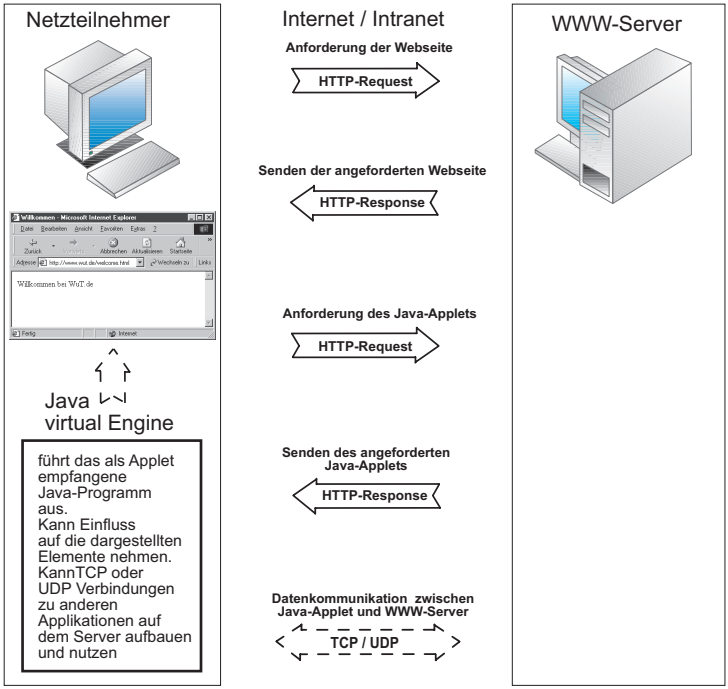
Ein Beispiel:
Wie bereits in den vorangegangenen Kapiteln beschrieben, werden öffentliche Webauftritte über Domainnamen repräsentiert. Dabei kann ein und die selbe Webseite über mehrere Domainnamen erreichbar sein. Zum Beispiel über eine „de“ Domain und eine „com“ Domain. Der folgende Code wertet aus, ob eine Webseite über die „com“ Domain oder die „de“ Domain aufgerufen wurde und stellt sich entsprechend englisch oder deutsch dar.

```
<HTML>
  <HEAD>
   <TITLE>urltest</TITLE>
   <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
  </HEAD>
  <BODY>
   <SCRIPT LANGUAGE="JavaScript"><!—
   if (location.hostname == "www.web-io.com") document.write("welcome at WuT");
   else document.write("willkommen bei WuT");
   //—></SCRIPT>
  </BODY>
</HTML>
```

Java Applets
Hier handelt es sich um kompilierte Programme, die in der Programmiersprache Java erstellt wurden. Java Applets werden, ähnlich wie grafische Elemente, zusätzlich zum HTML-Text geladen und im Browser ausgeführt.

Nicht alle Browser unterstützen von Hause aus die Ausführung von Java-Applets. Für alle gängigen Browser kann die Java-Unterstützung nachinstalliert werden (kostenloser Download unter java.com).

Mit Java Applets können auch komplexere Aktionen, wie Netzwerkzugriffe auf TCP- und UDP-Ebene realisiert werden.



Aus Sicherheitsgründen ist allerdings nur die Kommunikation mit dem Server möglich, von dem das Applet geladen wurde. Auch auf dem lokalen Rechner des Anwenders ist der Zugriff auf Elemente und Funktionen des Browsers beschränkt. Ein Zugriff auf die Festplatte des eigenen Rechners ist zum Beispiel nicht möglich.

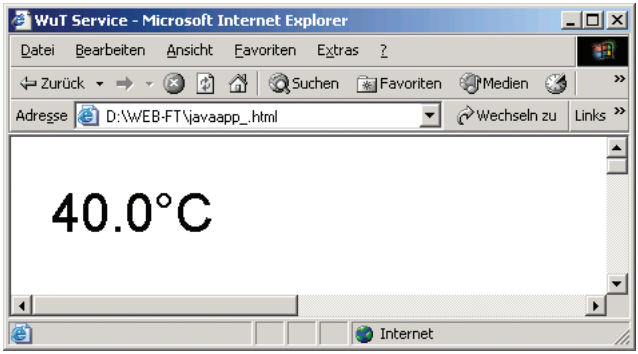
Ein Beispiel für den Einsatz von Java Applets ist der W&T Web-Thermograph. Vom Web-Thermograph wird ein Applet zur Verfügung gestellt, das, einmal im Browser gestartet, in regelmäßigen Abständen die aktuelle Temperatur abfragt und in der Webseite darstellt, von der es aufgerufen wurde.

Im HTML Code werden Applets über das Applet-Tag eingebunden, wobei mit *code=* der Name des Applets und mit *archiv=* der Name des Archivs innerhalb des Applets angegeben wird. Unter *codebase=* wird festgelegt, von welchem Host das Applet geladen wird.

Zwischen den Applet-Tags werden zusätzliche Parameter übergeben; im folgenden Quelltext z.B. welcher Sensor al Quelle für die gezeigte Temperatur ausgewählt wird.

```
<html>
  <head>
    <title>Schaltschranktemperatur</title>
  </head>
  <body bgcolor="#FFFFFF">
    <applet archive="A.jar" code="A.class" codebase = "http://172.16.232.152/" >
      <param name="sensor" value="1">
    </applet>
  </body>
</html>
```

Im Browser sieht das dann so aus:



Java und Javascript als zuverlässiges Team

Mit Java und Javascript können zuverlässig dynamische Webseiten auch für technische Anwendungen realisiert werden.

HTML stellt dabei das visuelle Grundgerüst der Webseite. HTML ist jedoch lediglich eine Beschreibungssprache, in der ausschließlich festgelegt wird, in welcher Form die Inhalte im Browser angezeigt werden.

Mit JavaScript können hingegen bestimmte Inhalte der Webseite zustandsabhängig, d.h. je nach Wert der Variablen angezeigt werden. Der Wert einer Variablen wird jedoch zum Zeitpunkt des Ladens der Webseite festgelegt.

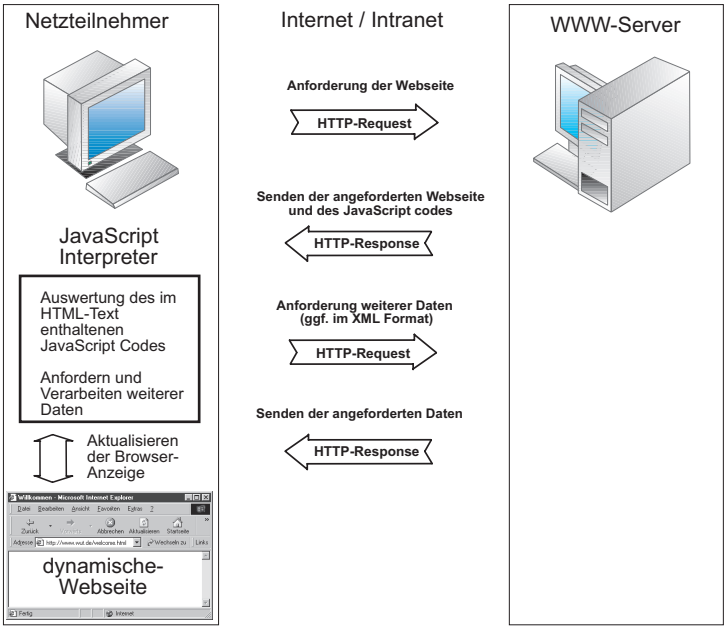
Den kontinuierlichen Abgleich mit einer technischen Anwendung übernimmt schließlich Java in Form eines Applets. Ein Java-Applet kann nicht nur in einem vorgegebenen Format Werte anzeigen, sondern auch eine Benutzeroberfläche oder eine Software-Schnittstelle zu JavaScript bilden, die zum Datenabgleich bzw. zur Kommunikation genutzt wird. So wird die dynamische Anzeige von Werten im Browser möglich, ohne dass die zugrundeliegende Webseite neu geladen werden muss.

AJAX - Asynchronus JavaScript and XML

AJAX gewinnt bei der Gestaltung dynamische Webseiten zunehmend mehr Popularität. Das Kernstück von AJAX ist die in aktuellen Versionen von JavaScript angebotene HTTP-Request Methode. Hiermit kann JavaScript auch nach dem Laden und Anzeigen einer Webseite Daten vom Web-Server anfordern. Daten können, wenn es der Server unterstützt im XML-Format angefordert werden. Alternativ wird aber auch die Übertragung von Textformaten unterstützt.

Im Gegensatz zur im vorangegangenen Abschnitt beschriebenen Java-Applet-Technik, kommt AJAX also ohne das Laden zusätzlicher Applets aus. JavaScript übernimmt sowohl das nachträgliche Holen der Daten, als auch die Aktualisierung der Browser-Anzeige.

Allerdings kann JavaScript keine dauerhafte Verbindung zum Web-Server aufrechterhalten. Es kann aber durch zyklisches Nachladen von Prozessdaten eine selbstaktualisierende Prozessvisualisierung im Browser realisiert werden.



Das Nachladen von Daten ist nur von dem Web-Server erlaubt, von dem auch die ursprüngliche Webseite geladen wurde.

Konkrete Programmierbeispiele zu den hier beschriebenen Techniken finden Sie unter www.WuT.de im Applikationsbereich der Web-IO Produkte.

6. OPC – Der Prozessdaten Dolmetscher

In der Automatisierungstechnik werden meist Hardware-Komponenten verschiedenster Hersteller zu einer Anlage zusammengesetzt. Hierbei verfolgt jeder Hersteller einen eigenen Weg, Prozessdaten an die Softwareebene weiterzugeben. Das betrifft sowohl den physikalischen Kommunikationsweg als auch das Datenformat.

Um diesem Prozessdaten-Babylon zu entgehen, wurde der OPC-Standard eingeführt .

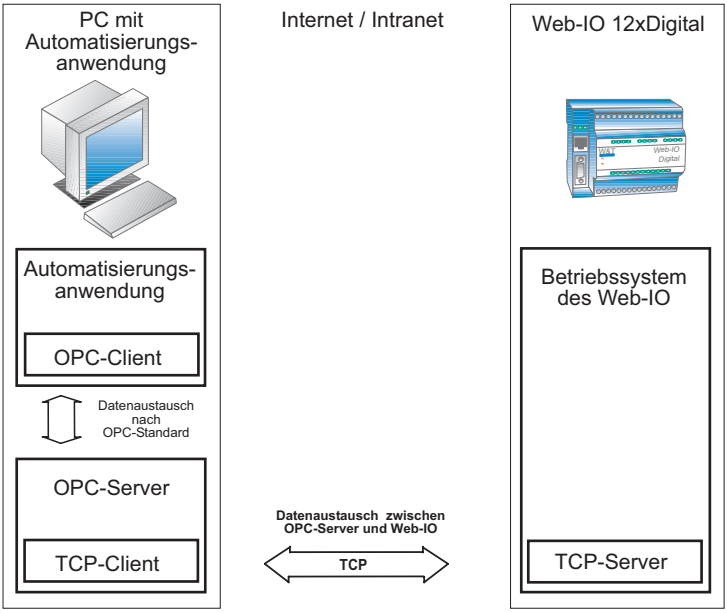
OPC steht für OLE for Process Control, wobei OLE die Abkürzung für Object Linking and Embedding ist. Die Grundidee von OLE ist die geregelte Einbettung von Dokumenten anderer Anwendungen in die eigene Anwendung. Zum Beispiel das Einfügen eines EXCEL Dokuments in eine Word Datei.

Sowohl OLE als auch OPC wurden speziell für PCs mit Windows-Betriebssystem konzipiert.

OPC gestützte Anwendungen kommunizieren nicht auf direktem Weg mit den angesprochenen Endgeräten. Stattdessen wird für das entsprechende Endgerät ein OPC-Server installiert. Der OPC-Server ist ein Softwareprozess, der im Hintergrund die herstellerspezifische Kommunikation mit dem Endgerät abwickelt. Die so gewonnenen Prozessdaten werden nach dem OPC-Standard aufgearbeitet und der Anwendung in einer standardisierten Form übergeben.

Der Teil der Anwendung, der mit dem OPC-Server kommuniziert, wird als OPC-Client bezeichnet.

Das folgende Beispiel zeigt den Zugriff auf ein Wiesemann & Theis Web-IO 12xDigital mittels OPC-Server:



6.1 Der Zugriff über OPC

Bei der OPC-Schnittstelle unterscheidet man zwischen vier Hauptaufgaben:

Data Access: kurz DA beschreibt den Austausch von Echtzeitdaten über OPC.

Alarm & Events: kurz AE dient zur Alarm- und Ereignisbehandlung.

Historical Data Access: kurz HDA erlaubt gespeicherte, historische Werte und Werteverläufe zugänglich zu machen.

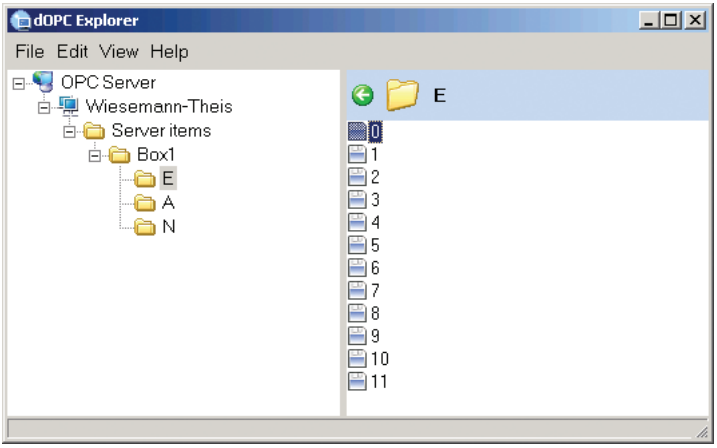
Data Exchange: Kurz DX erlaubt es OPC-Servern untereinander Daten auszutauschen.

Prozessdaten werden vom OPC-Server in Form von Items bereitgestellt. Alle Items haben eine Item-ID, eine innerhalb des OPC-Servers einmalige also eindeutige Adresse. Jedes Item hat eine unbestimmte Anzahl von Properties bzw. Item-Eigen-

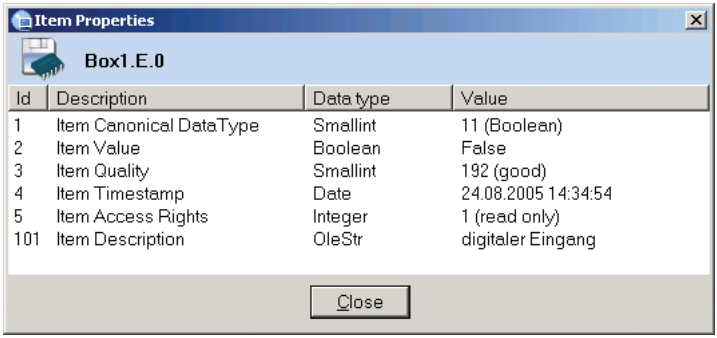
schaften, wie z.B. Wert, Qualität, Zeitstempel, usw.

Die Items werden vom OPC-Server meist in Gruppen zusammengefasst. Daraus ergibt sich dann eine Art Hierarchie (OPC-Server > OPC-Group > OPC Item).

Um dem OPC-Client einen einfachen Zugang zu allen verfügbaren Items zu ermöglichen, erlauben viele OPC-Server dem OPC-Client das OPC-Browsing.



Der OPC-Client kann darüber alle Items in einer Art Verzeichnisbaumstruktur abfragen. Hier als Beispiel die Struktur der Items eines W&T Web-IO 12xDigital.



6.2 Kommunikation zwischen OPC-Client und OPC-Server

Der OPC-Client kann aus allen vom OPC-Server angebotenen Items eine Teilmenge (oder auch alle) auswählen und seinerseits zu einer oder mehreren Gruppen zusammenfassen. Diese Gruppen müssen nicht identisch mit den vom OPC-Server gebildeten Gruppen sein. Die ausgewählten Items werden dann gruppenweise vom OPC-Client abonniert. Das bedeutet, der OPC-Client muss nicht ständig den Zustand der Items abfragen, sondern wird vom OPC-Server automatisch informiert, wenn sich eine der Eigenschaften eines Items ändert. Auf diese Weise entlastet der OPC-Server den OPC-Client, und somit die Anwendung.

6.3 Wann macht es Sinn mit OPC zu arbeiten?

Immer dann, wenn eine flexible Anwendung entstehen soll, die ohne großen Aufwand mit der Hardware verschiedenster Hersteller Daten austauschen muss, ist OPC die ideale Lösung.

In Applikationen der Prozessleittechnik und der Prozess- und Messdatenvisualisierung ist OPC vor allem für den Anwender eine feine Sache.

Bei allen Vorteilen der OPC-Technik soll hier aber nicht verschwiegen werden, dass die Programmierung einer universellen OPC-Client Anwendung eine komplexe Aufgabe ist, die ein hohes Maß an Programmierkompetenz voraussetzt.

Wenn es also darum geht, eine spezielle Anwendung für ein spezielles Endgerät eines Herstellers zu erstellen, sollte man abwägen, ob es nicht einfacher ist den direkten, vom Hersteller vorgesehenen Kommunikationsweg zu gehen.

TCP/IP -Ethernet einrichten

Sowohl die aktuellen Betriebssysteme, als auch die PC-Hardware sind heute für den Betrieb in TCP/IP Ethernet Netzwerke vorbereitet.

Wie aufwändig die Konfiguration des PC ist, hängt davon ab, wie im Netzwerk die IP-Adressen verwaltet werden. Erfolgt der physikalische Netzwerkzugang über RJ45-Anschluss und Patchkabel oder über WLAN?

Bei verwendetem WLAN-Zugang benötigen Sie SSID, Verschlüsselungsverfahren und Password

Des weiteren müssen Sie in Erfahrung bringen, ob die IP-Adressvergabe per DHCP erfolgt oder ob mit fest vergebenen IP-Adressen gearbeitet wird.

Wie der Netzwerkzugriff über TCP/IP-Ethernet auf den gängigen Microsoft Windows Systemen eingerichtet und konfiguriert wird, soll auf den folgenden Seiten Schritt für Schritt beschrieben werden.

IP-Adresse	_____._____._____._____
Subnet-Mask	_____._____._____._____
Gateway	_____._____._____._____
DNS-Server	_____._____._____._____

7. TCP/IP unter Win XP installieren und konfigurieren

7.1 WLAN unter Windows XP einrichten

Wenn die Netzwerkanbindung nicht über WLAN erfolgt, können Sie diesen Abschnitt überspringen.

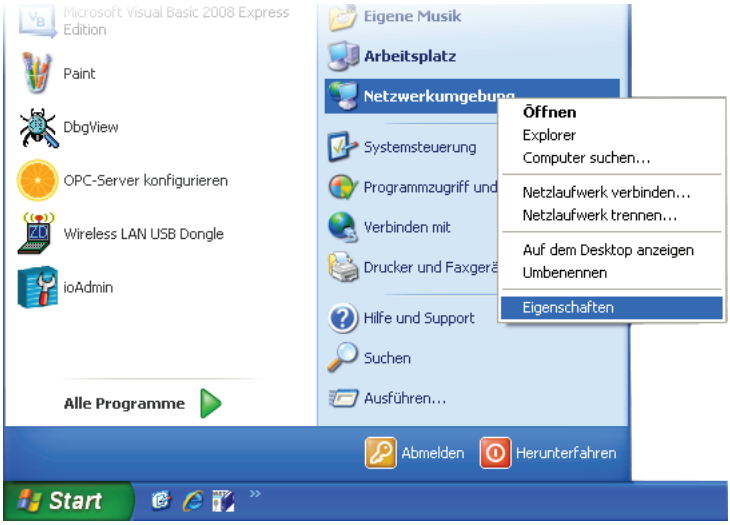
Für die PC seitige WLAN Hardware gibt es vier Varianten:

- bereits integrierter WLAN Anschluss
- nachgerüstete WLAN-Netzwerkkarte
- PCMCIA WLAN-Karte (nur bei Notebooks)
- WLAN USB Stick

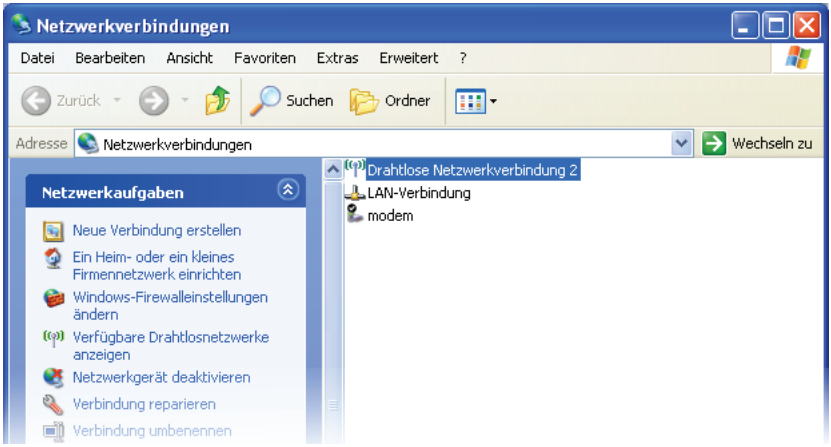
Bei der Nachrüstung von WLAN-Komponenten müssen zunächst die Hardware-Treiber des Herstellers installiert werden

Bei Windows XP ist die Netzwerkanbindung mittels WLAN bereits Bestandteil des Betriebssystems. Wenn die WLAN-Hardware nicht zu exotisch ist stellt Windows XP zur Konfiguration eine einheitliche Oberfläche zur Verfügung.

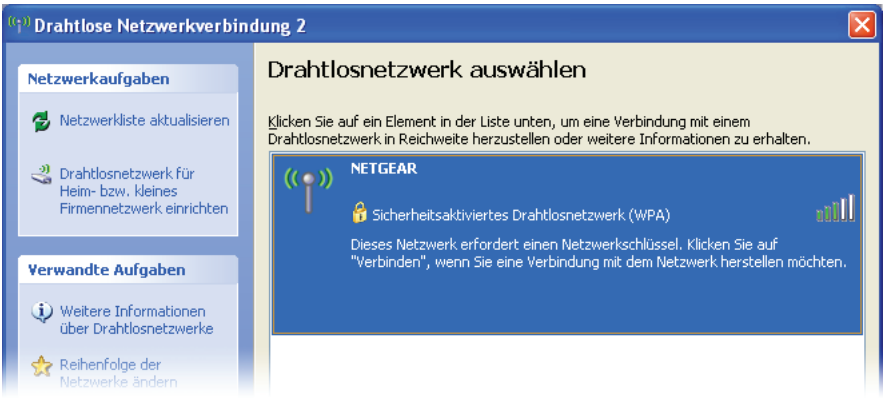
Klicken Sie auf *Start* und dann mit der rechten Maustaste auf *Netzwerkumgebung* und wählen Sie dann *Eigenschaften*



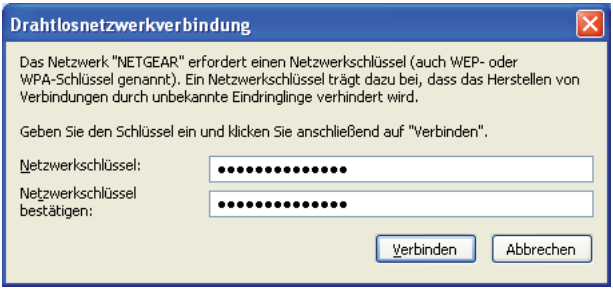
Markieren Sie *Drahtlose Netzwerkverbindung* und klicken auf *verfügbare Drahtlos Netzwerke anzeigen*.



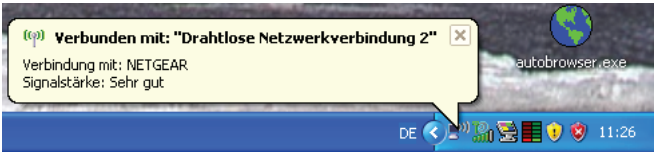
Es erscheint eine Liste mit den verfügbaren WLAN-Netzwerken.



Markieren Sie den Eintrag für das gewünschte Netzwerk und klicken Sie auf den *Verbinden*-Button



Wenn das gewählte WLAN mit einer Verschlüsselung arbeitet, werden Sie aufgefordert, den vom Administrator festgelegten Schlüssel einzugeben.



Nun kann mit der Konfiguration von TCP/IP begonnen werden.

Näheres dazu am Anfang des Kapitels TCP/IP unter Win XP installieren.

7.2 TCP/IP Parameter konfigurieren

1. Klicken Sie auf *Start* und öffnen unter *Einstellungen* die *Systemsteuerung.*

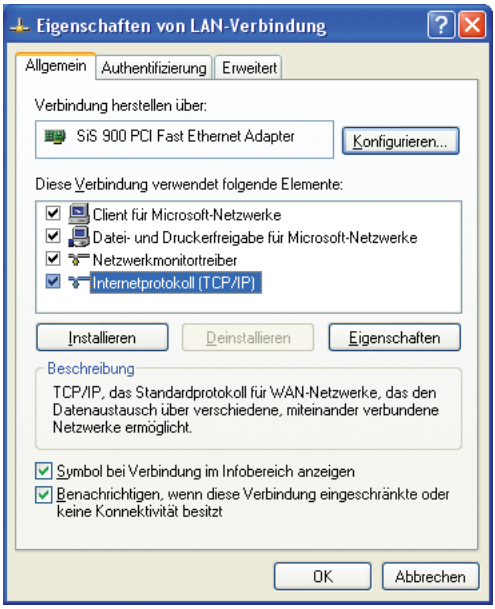
2. Doppelklicken Sie auf das Icon:

und im nächsten Fenster auf:

Anschließend klicken Sie mit der rechten Maustaste auf:

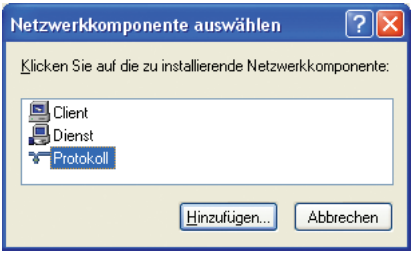
Sollte der PC mehrere LAN-Verbindungen anbieten - z.B. einen normalen Ethernet-Anschluss oder einen WLAN Adapter wählen Sie, welcher Zugang konfiguriert werden soll.

3 Kontrollieren Sie, ob *Internetprotokoll (TCP/IP)* aufgelistet ist.

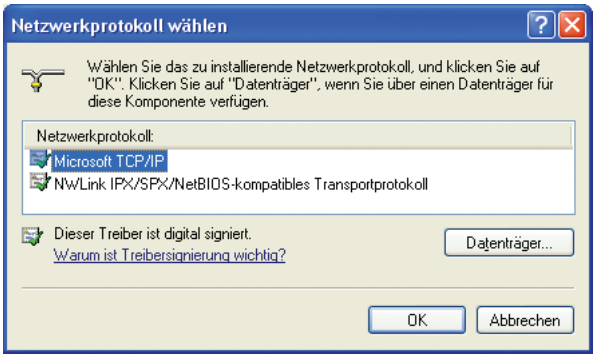


Wenn der Eintrag *Internetprotokoll (TCP/IP)* vorhanden ist, fahren Sie mit Punkt 5 fort.

4. Bei fehlendem Eintrag *Internetprotokoll (TCP/IP)* klicken Sie auf *Installieren* und wählen im folgenden Fenster *Protokoll* und *Hinzufügen*.



Wählen Sie *Microsoft TCP/IP*.

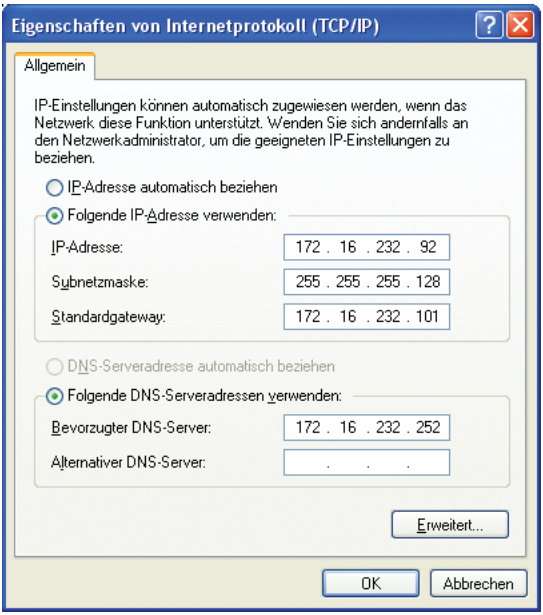


Sie benötigen nun die Windows XP Installations-CD. Nach Bestätigung mit *OK* ist die Liste der Netzwerkprotokolle um den Eintrag *Microsoft TCP/IP* erweitert.

5. Es erscheint nun wieder das Fenster *Eigenschaften von LAN-Verbindung*. Markieren Sie den Eintrag *Internetprotokoll (TCP/IP)* und klicken Sie anschließend auf *Eigenschaften*.

   Wenn Ihr PC bereits in ein Netzwerk eingebunden ist, sollten Sie sich bei Ihrem Netzwerkadministrator erkundigen, ob der DHCP-Dienst unterstützt wird.

   Ist das der Fall, wählen Sie *IP-Adresse automatisch beziehen*.



Sonst tragen Sie im folgenden Fenster IP-Adresse, Subnet-Mask und Gateway ein. Arbeitet Ihr Netzwerk mit DNS-Unterstützung, sollte auch die IP-Adresse des DNS-Servers eingetragen werden. Bestätigen Sie mit *OK*.

Damit ist die Installation von TCP/IP abgeschlossen, und Sie werden jetzt aufgefordert, Ihren PC neu zu starten.

8. TCP/IP unter Windows Vista / 7 / 8 konfigurieren

8.1 WLAN einrichten

Wenn die Netzwerkanbindung nicht über WLAN erfolgt, können Sie diesen Abschnitt überspringen.

Für die PC seitige WLAN Hardware gibt es vier Varianten:

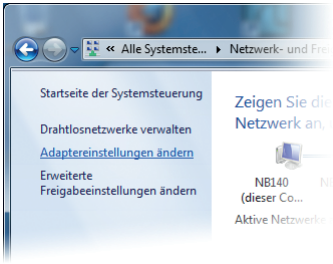
- bereits integrierter WLAN Anschluss
- nachgerüstete WLAN-Netzwerkkarte
- PCMCIA WLAN-Karte (nur bei Notebooks)
- WLAN USB Stick

Bei der Nachrüstung von WLAN-Komponenten müssen zunächst die Hardware-Treiber des Herstellers installiert werden

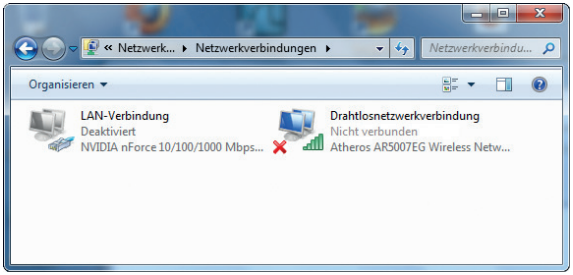
Ab Windows Vista ist die Netzwerkanbindung mittels WLAN Bestandteil des Betriebssystems.

Drücken Sie bei gehaltener Windows-Taste die E-Taste. Klicken Sie mit rechts auf Netzwerk und wählen Sie Eigenschaften.

Es öffnet sich das Netzwerk- und Freigabecenter.



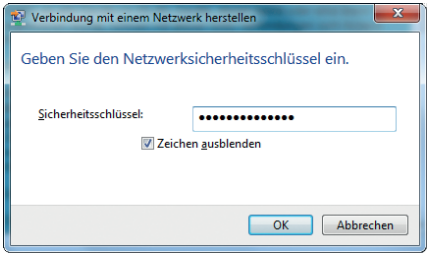
Wählen Sie hier auf der linken Seite *Adaptereinstellungen ändern* bzw. bei Vista *Netzwerkverbindungen verwalten.*



Klicken Sie mit der Rechten Maustaste auf *Drahtlosnetzwerkverbindung* und wählen Sie dann *Verbindung herstellen/trennen.*

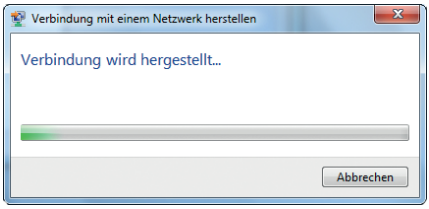
Es erscheint eine Liste der verfügbaren WLAN-Netze

Markieren Sie das Netzwerk, mit dem der PC verbunden werde soll und klicken Sie auf den *Verbindung herstellen* Button.

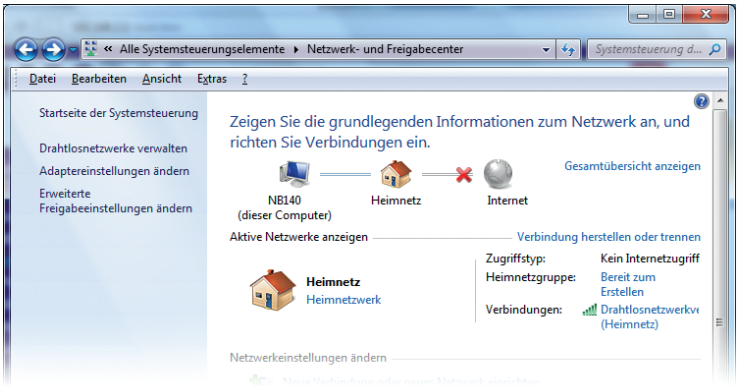


Wenn das gewählte WLAN mit einer Verschlüsselung arbeitet werden Sie aufgefordert, den vom Administrator festgelegten Schlüssel einzugeben.

Nach einem Klick auf den *Verbinden*-Button wird die WLAN-Verbindung hergestellt



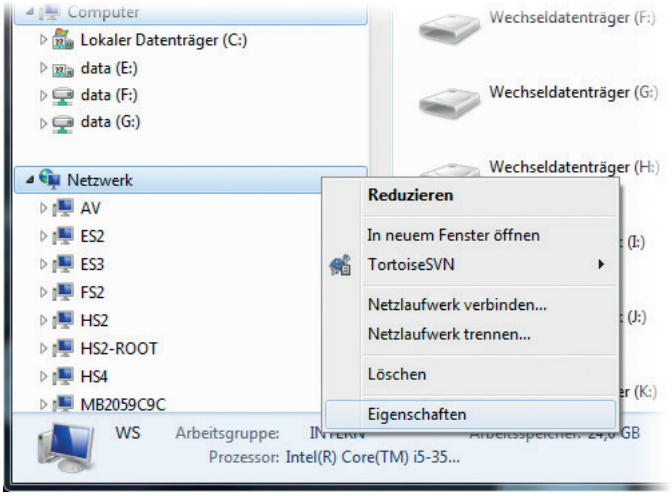
Sobald die Verbindung hergestellt ist, wird das von Windows bestätigt



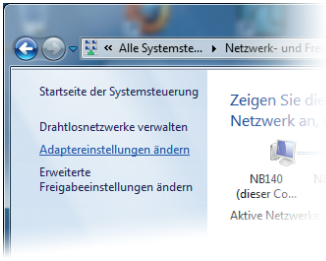
8.2 TCP/IP Parameter konfigurieren

Nun kann mit der Konfiguration von TCP/IP begonnen werden.

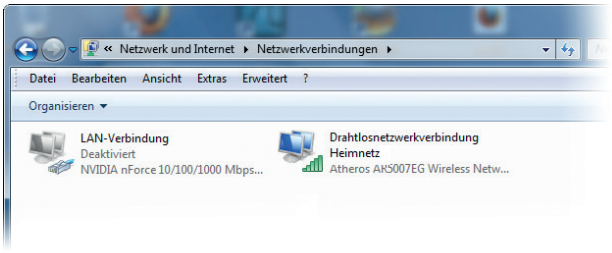
1. Drücken Sie bei gehaltener Windows-Taste die E-Taste. Klicken Sie mit rechts auf Netzwerk und wählen Sie Eigenschaften.



Es öffnet sich das Netzwerk- *und Freigabecenter.*

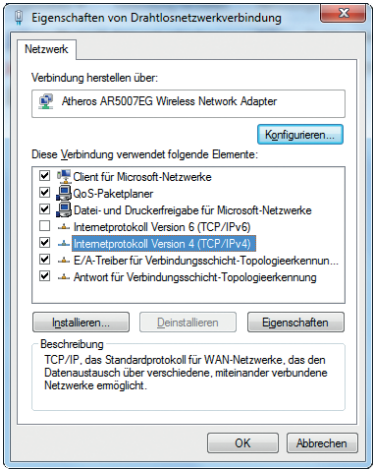


Es öffnet sich ein Fenster mit dem *Netzwerk- und Freigabecenter*. Wählen Sie hier auf der linken Seite *Adaptereinstellungen ändern* bzw. bei Vista *Netzwerkverbindungen verwalten.*

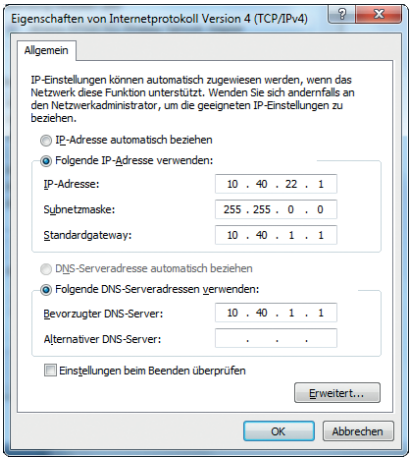


3. Klicken Sie mit der rechten Maustaste auf die Netzwerk-Verbindung, die Sie einrichten möchten. Windows zeigt nun ggf. eine Benutzerkonten-Warnmeldung. Quittieren Sie diese durch Klick auf *Fortsetzen*.

   Es öffnet sich das Eigenschaftsfenster für die ausgewählte Lan-Verbindung



4. Markieren Sie den Punkt *Internet Protokoll Version 4 (TCP/IPv4)* und klicken Sie auf *Eigenschaften*.

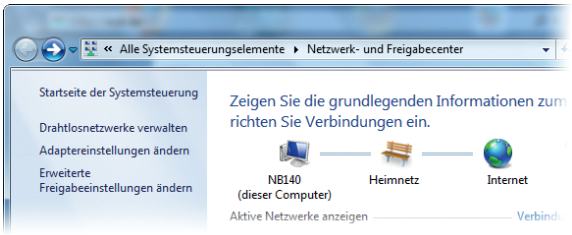


Wenn Ihr PC bereits in ein Netzwerk eingebunden ist, sollten Sie sich bei Ihrem Netzwerkadministrator erkundigen, ob der DHCP-Dienst unterstützt wird.

Ist das der Fall, wählen Sie *IP-Adresse automatisch beziehen*.

Sonst tragen Sie im folgenden Fenster IP-Adresse, Subnet-Mask und Gateway, sowie IP-Adresse des DNS-Servers ein. Bestätigen Sie mit *OK*.

Im *Netzwerk- und Freigabecenter* sollte die eingerichtete Verbindung nun angezeigt werden.



Damit ist die Installation von TCP/IP abgeschlossen.

Kleines Netzwerk-ABC

10Base2 – 10Mbit/s BASEband 200 (185)m/Segment
Ethernet-Topologie auf koaxialer Basis mit einer Übertragungsrate von 10Mbit/s.
Weitere geläufige Bezeichnungen für 10Base2 sind auch Cheapernet oder Thin-Ethernet. Es wird Koax-Kabel mit 50 Ohm Impedanz in einer dünnen und flexiblen Ausführung verwendet, um die einzelnen Stationen busförmig miteinander zu verbinden. Anfang und Ende eines Segments müssen mit Abschlusswiderständen von 50 Ohm abgeschlossen werden.
Die Transceiver sind auf den Netzwerkkarten integriert, so dass der Bus direkt bis an jeden Arbeitsplatz geführt werden muss, wo er über BNC-T-Stücke an den Rechner angeschlossen wird. Die Dämpfung des Kabels, sowie die teilweise hohe Anzahl von Steckverbindern beschränken ein 10Base2 Segment auf max. 185m mit max. 30 Anbindungen. Zwischen zwei Stationen dürfen nicht mehr als vier Repeater liegen.
Die Schwachstelle der physikalischen Bus-Topologien von Ethernet liegt in der Tatsache, dass eine Unterbrechung des Kabels – z.B. durch Abziehen eines Steckverbinders – den Stillstand des gesamten Netzsegmentes zur Folge hat.

10Base5 – 10Mbit/s BASEband 500m/Segment
10Base5 ist die ursprüngliche Ethernet-Spezifikation. Die Verkabelung beruht hier auf einem koaxialen Buskabel mit 50 Ohm Impedanz und einer max. zulässigen Länge von 500m (Yellow Cable). Bedingt durch die koaxiale Zwei-Leiter-Technik (Seele und Schirm) lassen sowohl 10Base5 als auch 10Base2 lediglich einen Halbduplex-Betrieb zu. Die Netzwerkteilnehmer werden über externe Transceiver angeschlossen, die über Vampir-Krallen die Signale direkt vom Buskabel abgreifen, ohne dieses durch Steckverbinder o. ä. zu unterbrechen. Getrennt nach Sende-, Empfangs- und Kollisions-Information werden die Daten vom Transceiver auf einem 15-poligen D-SUB-Steckverbinder zur Verfügung gestellt. Der Anschluss des Endgerätes erfolgt über ein 8adriges TP-Kabel von max. 50m Länge. Zwischen zwei beliebigen Stationen dürfen nicht

mehr als vier Repeater liegen. Diese Regel betrifft allerdings nur „hintereinander“ liegende Repeater – bei der Realisierung baumartiger Netzwerkstrukturen kann also durchaus eine Vielzahl von Repeatern eingesetzt werden.
Durch die Verwendung von relativ hochwertigem Kabel ohne jegliche Unterbrechungen durch Steckverbinder ergeben sich die Vorteile der großen Segmentlänge und der hohen Anzahl möglicher Anbindungen pro Segment (max. 100).
Die Dicke und Unflexibilität des Yellow Cable sowie die durch externe Transceiver zusätzlich entstehenden Kosten sind die Hauptnachteile von 10Base5 und haben wohl entscheidend zur Einführung von 10Base2 beigetragen.

10BaseT – 10Mbit/s BASEband Twisted Pair

Mit der Definition von 10BaseT wird die physikalische Topologie von der logischen getrennt. Die Verkabelung ist, ausgehend von einem Hub als zentraler aktiver Komponente, sternförmig ausgeführt. Es wird ein mindestens zweipaariges Kabel der Kategorie 3 mit 100 Ohm Impedanz verwendet, in dem die Daten getrennt nach Sende- und Empfangsrichtung übertragen werden. Als Steckverbinder werden 8-polige RJ45-Typen eingesetzt, in denen die Paare auf den Pins 1/2 und 3/6 aufgelegt sind. Die max. Länge eines Segments (= Verbindung vom Hub zum Endgerät) ist auf 100m begrenzt. Ihren Ursprung hat die 10BaseT-Topologie in den USA, weil sie ermöglichte, die dort üblichen Telefonverdrahtungen auch für den Netzwerkbetrieb zu nutzen. Für Deutschland entfiel dieser Vorteil, da hier für die Telefonie Stern-4er-Kabel verlegt wurden, die den Anforderungen der Kategorie 3 nicht entsprachen.
Kabelunterbrechungen oder abgezogene Stecker, die bei allen physikalischen Busstrukturen einen Stillstand des gesamten Segmentes bedeuten, beschränken sich bei 10BaseT lediglich auf einen Arbeitsplatz. *vgl. a.* 10ff

100BaseFX – 100Mbit/s BASEband Fiber Exchange

Ethernet-Standard für die sternförmige Glasfaserverkabelung mit einer Übertragungsgeschwindigkeit von 100Mbit/s. Zur

Übertragung des Ethernet-Signals werden Lichtimpulse mit einer Wellenlänge von 1300nm in eine 50µm oder 62,5µm Multimodefaser eingespeist. Die maximale Segmentlänge beträgt 2km.
vgl. a. 14ff

100BaseT4 – 100Mbit/s BASEband Twisted 4 Pairs
100BaseT4 spezifiziert eine Ethernet-Übertragung mit 100Mbit/s. Wie bei 10BaseT handelt es sich um eine physikalische Sternstruktur mit einem Hub als Zentrum. Es wird ebenfalls ein Kabel der Kategorie 3 mit 100 Ohm Impedanz, RJ45 Steckverbindern und einer max. Länge von 100m eingesetzt. Die zehnfache Übertragungsgeschwindigkeit von 100Mbit/s bei gleichzeitiger Einhaltung der Kategorie-3-Bandbreite von 25MHz wird u.a. auch durch die Verwendung aller vier Aderpaare erzielt. Für jede Datenrichtung werden bei 100BaseT4 immer 3 Paare gleichzeitig verwendet.
vgl. a. 11ff

100BaseTX – 100Mbit/s BASEband Twisted 2 Pairs
100BaseTX spezifiziert die 100Mbit/s-Übertragung auf 2 Aderpaaren über eine mit Komponenten der Kategorie 5 realisierte Verkabelung. Kabel, RJ45-Wanddosen, Patchpanel usw. müssen gemäß dieser Kategorie für eine Übertragungsfrequenz von mindestens 100MHz ausgelegt sein.

ABAP - Advanced Business Application Programming
ABAP ist eine Programmiersprache, die von SAP entwickelt wurde, um die SAP-Softwareumgebung individuell zu programmieren.

Abschlusswiderstand
Bei koaxialen Netzwerktopologien wie 10Base5 oder 10Base2 muss jeder Netzwerkstrang am Anfang und am Ende mit einem Abschlusswiderstand (Terminator) abgeschlossen werden. Der Wert des Abschlusswiderstandes muss der Kabelimpedanz entsprechen; bei 10Base5 oder 10Base2 sind dies 50 Ohm.

Administrator
Systemverwalter, der im lokalen Netzwerk uneingeschränkte Zugriffsrechte hat und für die Verwaltung und Betreuung des Netzwerks zuständig ist. Der Administrator vergibt unter anderem die IP-Adressen in seinem Netzwerk und muss die Einmaligkeit jeder IP-Adresse gewährleisten.

AJAX - Asynchronous JavaScript and XML
AJAX ist eine JavaScript-Programmiertechnik, die es erlaubt, Inhalte einer Webseite durch Nachladen von Daten dynamisch zu aktualisieren.
vgl. a. 140ff

ARP – Address Resolution Protocol
Über ARP wird die zu einer IP-Adresse gehörende Ethernet-Adresse eines Netzwerkteilnehmers ermittelt. Die ermittelten Zuordnungen werden auf jedem einzelnen Rechner in der ARP-Tabelle verwaltet. In Windows-Betriebssystemen kann man auf die ARP-Tabelle mit Hilfe des ARP-Befehls Einfluss nehmen. Eigenschaften und Parameter des ARP Kommandos in der DOS-Box:

- ARP -A listet die Einträge der ARP-Tabelle auf
- ARP -S <IP-Adresse> <Ethernet-Adresse> fügt der ARP-Tabelle einen statischen Eintrag hinzu
- ARP -D <IP-Adresse> löscht einen Eintrag aus der ARP-Tabelle

ARP ist im Internet-Standard RFC-826 definiert.
vgl. a. 22ff.

AUI – Attachment Unit Interface

Schnittstelle zur Anbindung eines externen Ethernet-Transceivers.

Getrennt nach Sende-, Empfangs- und Kollisions-Information werden die Daten vom Transceiver auf einem 15-poligen D-SUB-Steckverbinder zur Verfügung gestellt. Der Anschluss des Endgerätes erfolgt über ein 8-adriges TP-Kabel von max. 50m Länge.

Während die AUI-Schnittstelle in der Vergangenheit hauptsächlich zur Ankopplung von Endgeräten an 10Base5-Transceiver (Yellow-Cable) genutzt wurde, verwendet man sie heute eher zur Anbindung an LWL-Transceiver (Glasfaser) o.ä.

BNC – Bayonet Neill Concelmann

Bei der BNC-Steckverbindung handelt es sich um einen Bajonettverschluss zum Verbinden zweier Koaxialkabel. BNC-Steckverbindungen werden in 10Base2-Netzwerken zur mechanischen Verbindung der RG-58-Kabel (Cheapernet) verwendet.

BootP – Boot Protocol

Dieses ältere Protokoll zum Booten von PCs ohne Festplatte über das Netzwerk ist der Vorläufer von DHCP. Auch moderne DHCP-Server unterstützen immer noch BootP-Anfragen. Heute wird BootP in erster Linie eingesetzt, um Embedded-Systemen eine IP-Adresse zuzuteilen. Dazu muss auf dem DHCP-Server ein reservierter Eintrag hinterlegt werden, in dem der MAC-Adresse des Embedded-Systems eine feste IP-Adresse zugeordnet ist.

vgl. a. 63ff

Bridge
Bridges verbinden Teilnetze miteinander und entscheiden anhand der Ethernet-Adresse, welche Pakete die Bridge passieren dürfen und welche nicht. Die dazu notwendigen Informationen entnimmt die Bridge Tabellen, die je nach Modell vom Administrator eingegeben werden müssen oder von der Bridge dynamisch selbst erstellt werden; *vgl. a.* Router

Broadcast
Als Broadcast bezeichnet man einen Rundruf an alle Netzteilehmer. Eine typische Broadcast-Anwendung ist der ARP-Request (siehe ARP). Auch andere Protokolle – etwa RIP oder DHCP – nutzen Broadcast-Meldungen.
Broadcast-Meldungen werden nicht über Router oder Bridges weitergegeben.

Browser
Client-Programm mit grafischer Benutzeroberfläche, das dem Anwender die Möglichkeit gibt, Webseiten anzuzeigen und andere Dienste im Internet zu nutzen.
vgl. a. 125.

Bus-System
Bei einem Bus-System teilen sich mehrere Endgeräte eine einzige Datenleitung (Busleitung). Da zu einer gegebenen Zeit jeweils nur ein Endgerät die Datenleitung benutzen darf, erfordern Bus-Systeme immer ein Protokoll zur Regelung der Zugriffsrechte. Klassische Bus-Systeme sind die Ethernet-Topologien 10Base2 und 10Base5.

Cheapernet
Andere Bezeichnung für Ethernet auf der Basis von 10Base2.

Client
Computer oder Anwendungen, die Dienste von sogenannten Servern in Anspruch nehmen. Server-Dienste können zum Beispiel die Bereitstellung einer COM- oder Drucker-Schnittstelle im Netzwerk, aber auch Telnet und FTP sein.
vgl. a. 24.

Client-Server-Architektur
System der „verteilten Intelligenz", bei dem der Client Verbindung zu einem Server aufbaut, um vom Server angebotene Dienste in Anspruch zu nehmen. Manche Server-Anwendungen können mehrere Clients gleichzeitig bedienen.
vgl. a. 24.

Com-Server
Endgerät in TCP/IP-Ethernet Netzwerken, das Schnittstellen für serielle Geräte über das Netzwerk zur Verfügung stellt.

DHCP – Dynamic Host Configuration Protocol
Dynamische Zuteilung von IP-Adressen aus einem Adressenpool.
DHCP wird benutzt, um PCs in einem TCP/IP-Netz automatisch – also ohne manuellen Eingriff – zentral und somit einheitlich zu konfigurieren. Der Systemadministrator bestimmt, wie die IP-Adressen zu vergeben sind und legt fest, über welchen Zeitraum sie vergeben werden.
DHCP ist in den Internet-Standards RFC 2131 (03/97) und RFC 2241 (11/97) definiert.
vgl. a. 60ff.

DDNS – Dynamic Domain Name Service
DNS-Dienst, der auch die Namensauflösung für solche Netzteilnehmer unterstützt, die ihre IP-Adresse dynamisch über DHCP beziehen
vgl. a. 70ff.

DNS – Domain Name Service

Netzteilnehmer werden im Internet über numerische IP-Adressen angesprochen. Doch weil man sich Namen eben besser merken kann als Nummern, wurde der DNS eingeführt.
DNS beruht auf einem hierarchisch aufgebauten System: Jede Namensadresse wird über eine Top-Level-Domain („de“, „com“, „net“ usw.) und innerhalb dieser über eine Sub-Level-Domain identifiziert. Jede Sub-Level-Domain kann (muss aber nicht) nochmals untergeordnete Domains enthalten. Die einzelnen Teile dieser Namenshierarchie sind durch Punkte voneinander getrennt.
Wird vom Anwender zur Adressierung ein Domain-Name angegeben, erfragt der TCP/IP-Stack beim nächsten DNS-Server die zugehörige IP-Adresse.
Netzwerkressourcen sollten sinnvollerweise einen Domain-Namen erhalten, der im Kontext zu der angeboten Dienstleistung oder dem Firmennamen des Anbieters steht. So lässt sich z.B. *wut.de* in die Top-Level-Domain *de* (= Deutschland) und die Sub-Level-Domain *wut* (= Wiesemann & Theis GmbH) auflösen; *vgl. a.* 66ff.

DNS-Server

DNS-Server stellen im Internet die Dienstleistung zur Verfügung, einen Domain-Namen in eine IP-Adresse aufzulösen.

DynDNS

Bei den meisten Internetzugängen bekommt das angeschlossene Endgerät zum Zeitpunkt der Einwahl eine IP-Adresse aus dem Adresspool des Internetproviders. Da diese temporäre IP-Adresse nach außen nicht bekannt ist, sind solche Endgeräte normalerweise vom Internet aus nicht adressierbar. Über DynDNS kann einem solchen Internetteilnehmer ein Name gegeben werden. DynDNS aktualisiert die Zuordnung zwischen Namen und temporärer IP-Adresse, sobald der Teilnehmer online geht, so dass eine Erreichbarkeit über den Namen möglich wird.
vgl. a. 72ff.

EDGE - Enhanced Data Rates for GSM Evolution
EDGE ist eine Weiterentwicklung der GSM-Mobilfunktechnik und basiert auf effizienteren Datenmodulations- bzw Kompressionsverfahren. GPRS wird mit EDGE zu E-GPRS (Enhanced GPRS) und erlaubt Datenraten bis zu 220kbit/s (Download) bzw. 110kbit/s (Upload).
vgl. a. 117ff.

E-Mail
Elektronische Post über Internet und Intranet.
vgl. a. 101ff.

E-Mail-Adresse
Eine E-Mail-Adresse wird benötigt, um einem Anwender elektronische Post senden zu können und setzt sich immer aus dem Mailbox-Namen des Anwenders und der Ziel-Domain, getrennt durch das @-Zeichen zusammen. Ein Beispiel: *info@wut.de* bezeichnet das Info-Postfach auf dem Mailserver von W&T.
vgl. a. 101ff.

Embedded System
Als Embedded System bezeichnet man eine mikroprozessorgesteuerte Baugruppe, die als eingebetteter Teil eines Gerätes oder einer Maschine im Hintergrund Daten verarbeitet und ggf. Prozesse steuert.

ERP-System
Enterprise Resource Planning System - darunter versteht man eine Software-Lösung, die Unternehmen hilft, Kapital, Betriebsmittel und Personal möglichst effizient zu nutzen. Bekanntester Anbieter auf diesem Gebiet ist SAP.

Ethernet
Ethernet ist die zur Zeit bei lokalen Netzen am häufigsten angewandte Technologie. *vgl. auch* 7ff.

Ethernet-Adresse
Die unveränderbare, physikalische Adresse einer Netzwerkkomponente im Ethernet.
vgl. a. 18.

Fast-Ethernet
Fast-Ethernet ist quasi ein Upgrade der 10BaseT-Topologie von 10MBits/s auf 100 Mbit/s. *vgl. hierzu* 100BaseT4 und 100BaseTX

Firewall
Unter Firewall versteht man Netzwerkkomponenten, die ähnlich einem Router ein internes Netzwerk (Intranet) an ein öffentliches Netzwerk (z.B. Internet) ankoppeln. Hierbei lassen sich die Zugriffe ins jeweils andere Netz abhängig von der Zugriffsrichtung, dem benutzten Dienst sowie der Authentifizierung und Identifikation des Netzteilnehmers begrenzen oder komplett sperren.
Ein weiteres Leistungsmerkmal kann die Verschlüsselung von Daten sein, wenn z.B. das öffentliche Netz nur als Transitweg zwischen zwei räumlich getrennten Teilen eines Intranet genutzt wird.

FTP – File Transfer Protocol
FTP ist ein auf TCP/IP aufsetzendes Protokoll, das es ermöglicht, ganze Dateien zwischen zwei Netzwerkteilnehmern zu übertragen.
vgl. a. 81ff.

Gateway
Gateways verbinden – wie auch Bridges und Router – verschiedene Netze miteinander. Während Bridge und Router zwar ggf. die physikalische Art des Netzes umsetzen (z.B. Ethernet/ ISDN), das eigentliche Protokoll (z.B. TCP/ IP) aber unberührt lassen, bieten Gateways die Möglichkeit, einen Zugang zu protokollfremden Netzen zu schaffen (z.B. TCP/IP auf Profibus). Ein Gateway hat also unter anderem auch die Aufgabe, unterschiedliche Kommunikationsprotokolle zu übersetzen.
Achtung: bei der Netzwerkkonfiguration in Windows-Betriebssystemen wird auch die Eingabe eines Gateways gefordert. Diese Angabe bezieht sich allerdings auf einen ggf. im Netzwerk vorhandenen Router!

GPRS - General Packet Radio Service
bietet die Möglichkeit basierend auf dem GSM-Mobilfunkstandard Daten zu übertragen. Die maximale Übertragungsgeschwindigkeit liegt bei 55,6kbits/s.
vgl. a. 117ff.

GSM - Global System for Mobile Communications
ist der ursprüngliche und erste Standard der digitalen Mobilfunktelefonie und technische Grundlage der D- und E-Netze.
vgl. a. 117ff.

HTML – Hypertext-Markup-Language
Auszeichnungssprache, die über Schlüsselwörter vorgibt, wie die Inhalte im Browser angezeigt werden, wo Multimedia-Elemente zu finden sind und welche Elemente wie verlinkt sind;
vgl. a. 126ff.

HTTP – Hypertext Transfer Protocol
Das HTTP-Protokoll setzt auf TCP auf und regelt die Anforderung und Übertragung von Webinhalten zwischen HTTP-Server und Browser.
vgl. a. 95ff.

Hyperlink
Verweis auf andere Webseiten oder Inhalte innerhalb einer Webseite. Durch einfaches Anklicken des verlinkten Elements gelangt der Anwender auf die gewünschte Webseite. 128ff.

Hub
Ein Hub – oft auch als Sternkoppler bezeichnet – bietet die Möglichkeit, mehrere Netzteilnehmer sternförmig miteinander zu verbinden. Datenpakete, die auf einem Port empfangen werden, werden gleichermaßen auf allen anderen Ports ausgegeben.
Neben Hubs für 10BaseT (10Mbit/s) und 100BaseT (100Mbit/s) gibt es sogenannte Autosensing-Hubs, die automatisch erkennen, ob das angeschlossene Endgerät mit 10 oder 100Mbit/s arbeitet. Über Autosensing-Hubs können problemlos ältere 10BaseT-Geräte in neue 100BaseT-Netzwerke eingebunden werden.
vgl. a. 12ff.

ICMP – Internet Control Message Protocol
Das ICMP-Protokoll dient der Übertragung von Statusinformationen und Fehlermeldungen zwischen IP-Netzknoten. ICMP bietet außerdem die Möglichkeit einer Echo-Anforderung (*siehe auch Ping*); auf diese Weise lässt sich feststellen, ob ein Bestimmungsort erreichbar ist.
vgl. a. 75ff.

Internet
Das Internet ist der derzeit weltweit größte Netzverbund, der den angeschlossenen Netzteilnehmern eine nahezu grenzenlose Kommunikationsinfrastruktur zur Verfügung stellt. Durch Einsatz von TCP/IP können die Netzteilnehmer plattformunabhängig im Internet angebotenen Dienste wie E-Mail, FTP, HTTP usw. in Anspruch nehmen.

Intranet
Ein abgeschlossenes Netzwerk (etwa innerhalb eines Unternehmens), in dessen Grenzen die Netzteilnehmer Internet-

typische Dienste wie E-Mail, FTP, HTTP usw. in Anspruch nehmen können. In aller Regel gibt es von einem Intranet über Router bzw. Firewalls auch Übergänge in das Internet.

IP – Internet Protocol
Protokoll, das die Verbindung von Teilnehmern ermöglicht, die in unterschiedlichen Netzwerken positioniert sind.
vgl. a. 21ff.

IP-Adresse
Die IP-Adresse ist eine 32-Bit-Zahl, die jeden Netzteilnehmer im Internet bzw. Intranet eindeutig identifiziert. Sie besteht aus einem Netzwerkteil (Net-ID) und einem Benutzerteil (Host-ID).
vgl. a. 21ff.

IPSec
IPSec ist ein Protokoll um lokale Netzwerke gesichert und verschlüsselt über öffentliche Netzwerke wie das Internet zu verbinden. IPSec wird beim Aufbau von VPNs (Virtual Private Networks) eingesetzt.
vgl. a. 54ff.

ISDN – Integrated Services Digital Network
ISDN wurde in den 1980er Jahren als neuer Standard in der Fernmeldetechnik eingeführt. Bei ISDN werden Telefon und Telefax, aber auch Bildtelefonie und Datenübermittlung integriert. Über ISDN können also abhängig von den jeweiligen Endgeräten Sprache, Texte, Grafiken und andere Daten übertragen werden.
ISDN stellt über die S0 Schnittstelle eines Basisanschlusses zwei Basiskanäle (B-Kanäle) mit je 64 kbit/s sowie einen Steuerkanal (D-Kanal) mit 16 kbit/s zur Verfügung. Der digitale Teilnehmeranschluss hat zusammengefasst eine maximale Übertragungsgeschwindigkeit von 144 kbit/s (2B+D). In den beiden B-Kanälen können gleichzeitig zwei unterschiedliche Dienste mit einer

Bitrate von 64 kbit/s über eine Leitung bedient werden.
vgl. a. 113ff.

ISDN-Router
ISDN-Router gestatten es, zwei lokale Netzwerke über das ISDN-Netz eines Telefonnetz-Providers miteinander zu verbinden. Dabei übernehmen ISDN-Router neben den normalen Funktionen eines Routers auch das Handling der ISDN-Verbindung.

L2TP - Layer 2 Tunneling Protocol
Mit dem L2TP-Protokoll können Daten zwischen zwei Netzwerken unverschlüsselt getunnelt werden.
vgl. a. 57ff.

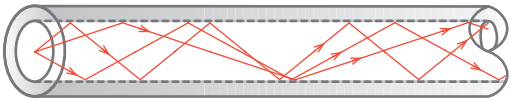
LAN – Local Area Network
Lokales Netz innerhalb eines begrenzten Gebiets unter Anwendung eines schnellen Übertragungsmediums wie z.B. Ethernet.

LWL - Lichtwellenleiter
In der Netzwerk- und Nachrichtentechnik wird zunehmend Lichtwellenleiter - kurz LWL - als Kommunikationsmedium eingesetzt. Vor allem in der Netzwerktechnik lassen sich mit LWL deutlich größere Distanzen überbrücken, als mit herkömmlicher Kupferverkabelung. Darüber hinaus ist die Datenübertragung über LWL resistent gegen elektrische Einflüsse wie z.B. Blitzschlag und Einkoppelung von Fremd- und Störsignalen.

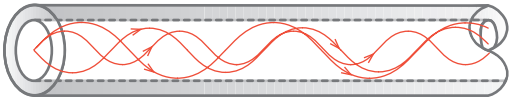
Elektrische Signale werden in Lichtsignale gewandelt und über LWL-Transmitter in den Lichtwellenleiter eingespeist. Als Übertragungsmedium werden meist Glasfasern eingesetzt, es gibt aber auch Systeme die mit Kunststofffasern arbeiten.

Bei den Glasfasern unterscheidet man zwei physikalische LWL-Typen: Multimodefasern und Monomodefasern

Multimodefasern haben einen Faserdurchmesser von 62,5µm oder 50 µm. Da sich Licht, wenn möglich, in alle Richtungen ausbreitet, nimmt es innerhalb der Faser verschiedene Signalwege (deshalb Multimode). Durch die unterschiedlichen Reflexionswinkel legt das Licht kürzere und längere Wege zurück, bis es beim Empfänger ankommt.



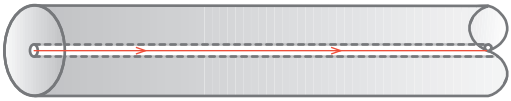
Solche Multimode-LWL werden auch als Stufenindexfasern bezeichnet. Neben den Stufenindexfasern gibt es Gradientenindexfasern. Auch bei diesen Fasern breitet sich das Licht in verschiedene Richtungen aus. Durch eine besondere optische Beschaffenheit werden die Lichtstrahlen aber sanft abgelenkt und nicht wie bei der Stufenindexfaser vom Rand reflektiert.



Gradientenindexfasern haben eine höhere Bandbreite als Stufenindexfasern und erlauben deshalb höhere Signalgeschwindigkeiten.

Mit beiden Multimodefasertypen können abhängig vom zu übertragenen Signal, Distanzen von bis zu mehreren Kilometern überbrücken (bei 100BaseFX z.B. max. 2km).

Monomodefasern - oft auch als Singlemodefasern bezeichnet - haben einen Faserdurchmesser von 3-9µm. Bedingt durch den geringen Faserdurchmesser kann sich das Licht nur auf einem Signalweg ausbreiten (deshalb Monomode).

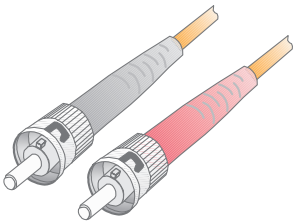


Monomodefasern erlauben je nach zu übertragendem Signal Distanzen von bis zu 50km.

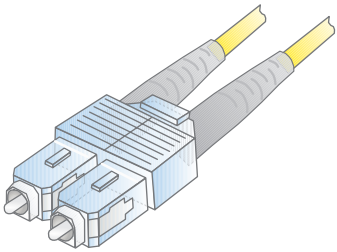
Durch den geringen Faserdurchmesser von max. 9µm (ein menschliches Haar hat ca. 100µm Durchmesser) ist die Ver-

arbeitung von Monomodefasern deutlich aufwändiger als bei Multimode-LWL.

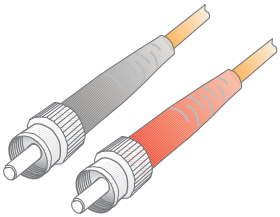
Eine weitere Varianz gibt es bei den LWL-Steckverbindungen. Hier gibt es drei grundsätzliche Verfahren:
Steckverbindungen mit Bajonet-Verriegelung, Steckverbindungen mit Überwurfmutter und Push/Pull-Steckverbinder mit Federarretierung.

	**ST-Stecker**
LWL-Type:	Multimode, Monomode
Verrieglung:	Bajonet
Einsatzgebiet:	LAN, WAN, Serielle Signale
Verbreitung:	hoch

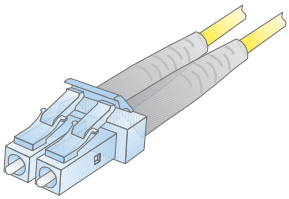
Über lange Zeit war der ST-Steckverbindung im Netzwerk- und Industriebereich der meist genutzte. Verdrehschutz und Bajonetverschluss verleihen dem ST-Stecker eine sichere und einfache Handhabung.

	**SC-Stecker**
LWL-Type:	Multimode, Monomode
Verrieglung:	Push/Pull
Einsatzgebiet:	LAN, WAN, Serielle Signale
Verbreitung:	sehr hoch

Bedingt durch seine einfache Push/Pull-Handhabung und die Duplexfähigkeit hat der SC-Steckverbinder heute die ST-Technik als meist verbreitetste abgelöst.

	**SMA-Stecker**
LWL-Type:	Multimode, Monomode
Verrieglung:	Überwurfmutter
Einsatzgebiet:	LAN
Verbreitung:	Hoch

Der SMA-Steckverbinder wurde in den Anfangszeiten der LWL-Technik eingesetzt. Der fehlende Verdrehschutz und die Gefahr des zu festen Anziehens führten oft zu Beschädigungen der Faser, weshalb die SMA-Technik heute kaum noch Bedeutung hat.

	**LC-Stecker**
LWL-Type:	Multimode, Monomode
Verrieglung:	Push/Pull
Einsatzgebiet:	LAN, WAN
Verbreitung:	Hoch

Wegen seiner kompakten Bauform wird der LC-Steckverbinder vorwiegend zur Konnektierung an Switches und anderen aktiven Netzwerkkomponenten eingesetzt.

An dieser Stelle haben wir nur die vier meistgenutzten

Stecksysteme vorgestellt. Eine vollständige Liste aller LWL-Steckervarianten würde den Rahmen sprengen.

Neben den Glasfasern gibt es, wie bereits angesprochen, Systeme die mit Kunststoff-LWL bzw. Polymerfasern arbeiten. Der Faserdurchmesser beträgt bei Kunststoff-LWL 1mm. Da Kunststoff das eingestrahlte Licht deutlich höher dämpft als Glas, reduziert sich die max. Distanz auf 100m. Der bei Polimerfasern noch ausgeprägtere Multimodeeffekt erlaubt zudem nur geringe Übertragungsgeschwindigkeiten. Der Haupteinsatz für Kunststoff-LWL ist deshalb die Übertragung von seriellen Signalen wie z.B. RS232 oder RS422/485.

MAC-ID
Die unveränderbare, physikalische Adresse einer Netzwerkkomponente (MAC = Media Access Control); *vgl. a.* Ethernet-Adresse

Monomode-LWL
siehe LWL

Multimode-LWL
siehe LWL

NAT – Network Address Translation
Durch die explosionsartige Ausweitung des Internets in den letzten Jahren sind freie IP-Adressen knapp geworden und werden nur noch sehr sparsam vergeben. NAT kommt dort zum Einsatz, wo Firmennetze ans Internet angebunden werden. Das Firmennetz ist über einen NAT-fähigen Router mit dem Internet verbunden, arbeitet intern allerdings mit einem eigenen, vom Internet unabhängigen IP-Adressraum. Von außen ist das Netz nur über eine einzige (oder einige wenige) IP-Adresse(n) ansprechbar. Anhand der Portnummer im empfangenen TCP/IP-Paket wird dieses an einen bestimmten internen Netzteilnehmer weitergeroutet.
vgl. a. 42ff.

Ping – Packet Internet Groper
Ping dient in TCP/IP-Netzen zu Diagnosezwecken; mit Hilfe dieser Funktion lässt sich überprüfen, ob ein bestimmter Teilnehmer im Netz existiert und tatsächlich ansprechbar ist. Die von Ping verwendeten ICMP-Pakete sind im Internet-Standard RFC-792 definiert.
vgl. a. 75ff.

PoE - Power over Ethernet
Mit PoE können Ethernet-Endgeräte die Versorgungsenergie aus dem Netzwerkkabel beziehen und so auf eine zusätzliche Stromversorgung verzichten. Die Versorgungsspannung wird von speziellen PoE-Switches oder speziellen Zwischenadaptern in das Netzwerkkabel eingespeist.
vgl. a. 13ff.

POP3 – Post Office Protocol Version 3
Um eingegangene E-Mails aus dem Postfach auf dem Mailserver abzuholen, wird in den meisten Fällen das POP3-Protokoll benutzt. Auch POP3 setzt auf TCP auf.
vgl. a. 105ff.

PPP – Point to Point Protocol
PPP ist ein erweiterter Nachfolger von SLIP und weist u.a. eine verbesserte Fehlerkorrektur auf.
Genau wie SLIP bietet PPP die Möglichkeit, TCP/IP-Geräte, die keinen LAN-Anschluss haben, über die serielle Schnittstelle in TCP/IP-Netze einzubinden.
vgl. a. 121ff.

PPS-System - Produktionsplanungs- u. Steuerungssystem
Software-Lösung zur Produktionsplanung mit dem Ziel Produktionszeiten zu verkürzen, Bestands- und Lagermengen zu optimieren und Termine einzuhalten. Bekanntester Anbieter von PPS-Systemen ist SAP.

PPTP - Point-to-Point Tunneling Protocol
PPTP wurde ursprünglich von Microsoft, 3COM und anderen Firmen entwickelt, um PCs über öffentliche Netzwerke netztwerktechnisch mit Servern zu verbinden. Da PPTP Bestandteil von Windows Betriebssystemen ist, wird es auch heute noch für den Aufbau von VPN genutzt
vgl. a. 57ff.

Repeater
In 10Base2 Netzen dienen Repeater zur Verbindung zweier Ethernet-Segmente, um das Netz über die Ausdehnung eines einzelnen Segmentes hinaus zu erweitern. Repeater geben Datenpakete von einem Netzwerksegment zum anderen weiter, indem sie zwar die elektrischen Signale normgerecht „auffrischen“, den Inhalt der Datenpakete dabei aber unverändert lassen. Erkennt der Repeater auf einem der angeschlossenen Segmente einen physikalischen Fehler, wird die Verbindung

zu diesem Segment abgetrennt („partitioniert“). Die Partitionierung wird automatisch aufgehoben, wenn der Fehler nicht mehr vorhanden ist.
Zwischen zwei Stationen dürfen nicht mehr als vier Repeater liegen. Diese Regel betrifft allerdings lediglich „hintereinander“ liegende Repeater – bei der Realisierung baumartiger Netzwerkstrukturen kann also durchaus eine Vielzahl von Repeatern eingesetzt werden.

RIP – Routing Information Protocol
Routingprotokolle wie RIP dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routingtabellen zu ermöglichen. RIP ist im Internet-Standard RFC-1058 definiert.

Router
Router verbinden zwei unterschiedliche Netze, wobei im Gegensatz zu Bridges nicht anhand der Ethernet-Adresse, sondern in Abhängigkeit von der IP-Adresse entschieden wird, welche Datenpakete weiterzuleiten sind.
vgl. a. Bridge und 36.

Singlemode-LWL
siehe LWL

SLIP – Serial Line Internet Protocol
SLIP bietet eine einfache Möglichkeit zur Übertragung von TCP/IP-Datenpaketen über serielle Punkt-zu-Punkt-Verbindungen. Damit können Endgeräte, die nicht über einen LAN-Anschluss verfügen, auch über die serielle Schnittstelle ins Netzwerk eingebunden werden.
SLIP arbeitet nach einem sehr einfachen Algorithmus ohne eigene Datensicherungsverfahren: Dem eigentlichen IP-Datenpaket wird ein Startzeichen (dezimal 192) vorangestellt und ein Endzeichen (ebenfalls dezimal 192) angehängt. Um die binäre Transparenz zu erhalten, werden im Datenpaket vorkom-

mende Start- und Endzeichen zuvor durch andere Sequenzen ersetzt. SLIP ist in RFC 1055 beschrieben.

SLIP-Router
Ein SLIP-Router stellt die Hardware und Funktionalität zur Verfügung, um serielle Endgeräte, die über einen TCP/IP-Stack verfügen, in ein Netztwerk einzubinden.
Com-Server stellen z.B. SLIP-Routing als Betriebsart zur Verfügung.

SMTP – Simple Mail Transfer Protocol
SMTP regelt den Versand von E-Mails vom Mail-Client zum Mailserver (SMTP-Server) und zwischen den Mailservern und setzt auf TCP auf.
vgl. a. 104ff.

SNMP – Simple Network Management Protocol
SNMP setzt auf UDP auf und ermöglicht die zentrale Administration und Überwachung von Netzwerkkomponenten.
SNMP ist in folgenden Standards spezifiziert: RFC 1052, RFC 1155, RFC 1156, RFC 1157, RFC 1213 und RFC 1441.
vgl. a. 88ff.

STP – Shielded Twisted Pair
Abgeschirmtes Datenkabel, bei dem jeweils 2 Kabeladern miteinander verdrillt sind; *vgl. a.* Twisted Pair

Subnet-Mask
32-Bit-Wert, der festlegt, welcher Teil der IP-Adresse das Netzwerk und welcher den Netzwerkteilnehmer adressiert.
vgl. a. 34ff.

Switch
Ein Switch bietet wie ein Hub die Möglichkeit, mehrere Netzteilnehmer sternförmig miteinander zu verbinden. Switches

vereinigen die Funktionalität eines Hub mit denen einer Bridge: Ein Switch „lernt" die Ethernet-Adresse des an einem Port angeschlossenen Netzteilnehmers und leitet dorthin nur noch diejenigen Datenpakete weiter, die an diesen Netzteilnehmer adressiert sind. Eine Ausnahme bilden dabei Broadcast-Meldungen, die an alle Ports weitergegeben werden (hier unterscheidet sich der Switch in seiner Funktion von einer Bridge, die Broadcast-Meldungen generell nicht weitergibt).
vgl. a. 12ff.

TCP – Transmission Control Protocol
TCP setzt auf IP auf und sorgt nicht nur für die Verbindung der Teilnehmer während der Datenübertragung, sondern stellt auch die korrekte Zustellung der Daten und die richtige Abfolge der Datenpakete sicher;
vgl. a. 24ff.

TCP/IP-Stack
Teil des Betriebssystems oder ein auf das Betriebssystem aufgesetzter Treiber, der alle für die Unterstützung des IP-Protokolls benötigten Funktionen und Treiber zur Verfügung stellt.

Telnet – Terminal over Network
In der Vergangenheit kam Telnet vor allem für den Fernzugriff über das Netzwerk auf UNIX-Server zum Einsatz. Über eine Telnet-Anwendung (Telnet-Client) kann von einem beliebigen Rechner im Netz ein Fernzugriff auf einen anderen Rechner (Telnet-Server) erfolgen. Heute wird Telnet auch zur Konfiguration von Netzwerkkomponenten wie z.B. Com-Servern benutzt. Telnet wird unter TCP/IP normalerweise über Portnummer 23 angesprochen; für spezielle Anwendungen können aber auch andere Portnummern verwendet werden. Telnet setzt auf TCP/IP als Übertragungs- und Sicherungsprotokoll auf.
Telnet ist im Internet-Standard RFC 854 definiert.
vgl. a. 77ff.

TFTP – Trivial File Transfer Protocol

Das Trivial File Transfer Protocol (TFTP) ist neben FTP ein weiteres Protokoll zur Übertragung ganzer Dateien. TFTP bietet nur ein Minimum an Kommandos, unterstützt keine aufwendigen Sicherheitsmechanismen und benutzt UDP als Übertragungsprotokoll. Da UDP ein ungesichertes Protokoll ist, wurden in TFTP eigene minimale Sicherungsmechanismen implementiert. *vgl. a.* 85ff.
Das Trivial File Transfer Protocol ist in den Standards 783, 906, 1350 und 1782 bis 1785 beschrieben.

Transceiver

Das Wort Transceiver ist eine Zusammensetzung aus Transmitter (Sender) und Receiver (Empfänger). Der Transceiver realisiert den physikalischen Netzzugang einer Station an das Ethernet und ist bei den modernen Ethernet-Topologien 10Base2 und 10BaseT auf der Netzwerkkarte integriert. Nur bei 10Base5 (*vgl. auch* AUI-Anschluss) ist der Transceiver als externe Komponente direkt am Netzwerkkabel angebracht.

Twisted Pair

Datenkabel, bei dem jeweils zwei Kabeladern miteinander verdrillt sind. Hierdurch wird ein deutlich reduziertes Übersprechverhalten zwischen den Doppeladern in einem Kabel erreicht. Man unterscheidet bei Twisted-Pair-Kabeln zwischen ungeschirmten UTP-Kabeln (Unshielded Twisted Pair) und geschirmten STP-Kabeln (Shielded Twisted Pair).
TP-Kabel werden vor allem in der Netzwerktechnik eingesetzt und sind nach ihren maximalen Übertragungsfrequenzen kategorisiert; in der Praxis kommen heute meist zwei Typen zum Einsatz:

- Kategorie-3-Kabel erlauben eine maximale Übertragungsfrequenz von 25MHz, ausreichend für den Einsatz in 10BaseT-, aber auch 100BaseT4-Netzen.
- Kategorie-5-Kabel erlauben eine maximale Übertragungsfrequenz von 100MHz und reichen damit für alle heutigen Netzwerktopologien aus.

UDP – User Datagram Protocol
UDP ist ein Protokoll, das wie TCP auf IP aufsetzt, im Gegensatz dazu aber verbindungslos arbeitet und über keine Sicherheitsmechanismen verfügt. Der Vorteil von UDP gegenüber IP ist die höhere Übertragungsgeschwindigkeit.
vgl. a. 27.

UMTS - Universal Mobile Telecommunications System
UMTS beschreibt die dritte Generation der Mobilfunktechnik. Bei UMTS steht nicht mehr die Telefonie im Vordergrund. Vielmehr wurde UMTS bereits bei der Entwicklung auf die Nutzung vielfältiger multimedialer Dienste ausgerichtet.
vgl. a. 118ff.

URL – Uniform Resource Locator
Adress- und Protokollinformation für den Browser. Über den URL gibt der Anwender dem Browser vor, welches Protokoll genutzt wird, auf welchem Webserver die Seite liegt, und wo diese auf dem Webserver zu finden ist.

UTP – Unshielded Twisted Pair
Im Gegensatz zu Shielded Twisted Pair ein nicht abgeschirmtes Datenkabel, bei dem jeweils zwei Kabeladern miteinander verdrillt sind.

VPN - Virtual Private Network
VPN beschreibt die Technik, vertrauliche Netzwerkteile an verschiedenen Standorten, über das Internet, also ein öffentliches Netz, miteinander zu Verbinden.
vgl. a. 47ff.

Web-Based Management
Unter Web-Based Management versteht man die Möglichkeit, ohne spezielle Software Endgeräte übers Netzwerk direkt im Browserfenster zu konfigurieren.

Web-IO
Kleine zigarettenschachtelgroße Boxen mit Ethernet-Anschluss und integriertem Webserver. Web-IO können digitale oder analoge Signale über TCP/IP-Ethernet zugänglich machen, bzw. im Browser visuallisieren bzw. steuerbar machen.

Wireless LAN
WLAN realisiert die Netzwerkanbindung über Funk.
vgl. a. 16ff.

WWW – World Wide Web
WWW wird häufig mit dem Internet gleichgesetzt. Das stimmt nicht ganz: Während das Internet die physikalischen Verbindungswege beschreibt, definiert das WWW die Gesamtheit der über das Internet verlinkten Webseiten bzw. Dokumente, die über das HTTP-Protokoll vom Browser geladen und angezeigt werden können.
vgl. a. 125ff.

Zahlensysteme

Neben dem dezimalen Zahlensystem (Zeichenvorrat: 0–9, neue Stelle bei 10) werden in der Computertechnik auch oft das binäre Zahlensystem (Zeichenvorrat 0–1, Stellensprung bei 2) und das hexadezimale Zahlensystem (Zeichenvorrat: 0–9 + A–F, neue Stelle bei 16) verwendet.

In der folgenden Tabelle finden Sie einige Beispiele für die Darstellung gebräuchlicher Werte in den drei Zahlensystemen:

Bin r	Dez.	Hex.	Bin r	Dez.	Hex.
0	0	0	11111	31	1F
1	1	1	100000	32	20
10	2	2	...	...	...
11	3	3	111111	63	3F
100	4	4	1000000	64	40
101	5	5	...	...	...
110	6	6			
111	7	7	...	...	...
1000	8	8	1111111	127	7F
1001	9	9	10000000	128	80
1010	10	A	11000000	192	C0
1011	11	B	11100000	224	E0
1100	12	C	11110000	240	F0
1101	13	D	11111000	248	F8
1110	14	E	11111100	252	FC
1111	15	F	11111110	254	FE
10000	16	10	11111111	255	FF

Index

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z