Industrielle Datenkommunikation

Theoretische und Allgemeine Anwendungen

WESTERMO

Westermo Handbuch

5.0

Ausgabe 1 erschienen im Dezember 1994, © Westermo, Schweden 1994
Zweite Ausgabe 1996 © Westermo, Schweden 1996
Ausgabe 2.1 erschienen 1997, © Westermo, Schweden 1997
Ausgabe 3.0 erschienen 1998, © Westermo, Schweden 1998
Ausgabe 4.0 erschienen 2001, © Westermo, Schweden 2001
Ausgabe 5.0 erschienen 2005, © Westermo, Schweden 2004
Produktion: Westermo Teleindustri AB, Schweden
Illustrationen: Visual Information AB, Eskilstuna, Schweden
Fotos: bildN, Västerås, Schweden
Björn Fröberg, Jordnära bildform, Eskilstuna, Schweden
futureimagebank.com
Repros: Ågerups Repro AB, Eskilstuna, Schweden
Druck: Eskilstuna Offset AB, Eskilstuna, Schweden

Sehr geehrter Leser,
Sie halten die 5. Auflage des Westermo Handbuchs in den Händen. Die erste Auflage dieses Handbuchs wurde 1994 herausgegeben und wurde mit den Jahren zu einem wertvollen Hilfsmittel von Ingenieuren und allen an der Datenkommunikation Interessierten.

Wie in den vorigen Ausgaben ist es auch diesmal unser Ziel, Sie nicht nur eingehend über die Westermo-Produktpalette zu informieren, sondern Ihnen auch einen zusammenfassenden Überblick über den theoretischen Hintergrund der Datenkommunikation zu geben. Die Abschnitte über Theorie und Anwendungsbereiche wurden mit jeder neuen Ausgabe des Handbuchs erweitert und die fünfte Ausgabe macht dabei keine Ausnahme.

Diese Auflage des Handbuchs weicht jedoch von den vorhergehenden ab. Aufgrund der enormen Erweiterung unseres Produktangebotes wurde das Handbuch für einen einfacheren Gebrauch in Abschnitte unterteilt.

Die einzelnen Abschnitte sind:

- Theoretische und allgemeine Anwendungen
- Fernverbindungen
- Industrielle Ethernet-Anwendungen
- Lokale Datenkommunikation

Wir hoffen, dass Ihnen dieses Westermo-Handbuch zu einer nützlichen Arbeitshilfe wird, es Ihre täglichen Aufgaben erleichtert und eine wertvolle Unterstützung für unsere engagierten Mitarbeiter weltweit darstellt.

Inhalt

Datenkommunikation – nicht nur Kabel und Anschlüsse

Industrielle Datenkommunikation

Die industrielle IT-Revolution

Durch die Schaffung neuer und effizienterer Kommunikationswege für die Informationen der Firmenprozesse können Wettbewerbsvorteile erreicht werden. Kürzere Lieferzeiten, schnellere Produktentwicklung, kundenorientierte Produktion und kürzere Rüstzeiten sind nur einige der Schlagworte, die mit fortschrittlicher industrieller IT-Entwicklung verbunden werden. Dazu gehören auch der schnelle Zugang zu Informationen sowie die Möglichkeit, Prozesse optimal zu steuern. Die Industrie entwickelt IT-Werkzeuge, die eine verstärkte Integration in sämtliche Phasen der Arbeitsprozesse erfordern, vom Einkauf über die Produktion bis zum Vermarkten. Die Qualität der Informationspfade und Informationsflüsse ist heutzutage eine der wichtigsten Voraussetzungen für gesteigerte Effizienz und Wettbewerbsfähigkeit in der Industrie.

Unterschiedliche Standards

Neue Ideen, neue Systeme und neue Lösungen für die Schaffung dieser IT-Werkzeuge enstehen.
Trotz vieler Ansätze ergaben sich für lange Zeit als negative Konsequenz dieser dynamischen Vielfalt fehlende, allgemein akzeptierte Standards. Jeder Entwickler schuf seine eigenen Lösungen. Das Problem unzulänglicher Standards zeigt sich besonders, wenn Computer, Maschinen und andere Ausrüstungsteile miteinander kommunizieren müssen. Die Frage des Standards stellt sich auf vielen Ebenen, nicht nur bei Kabeln und Anschlüssen. Hier geht es um die Art und Weise, wie Daten erstellt, gespeichert, komprimiert, adressiert und übertragen werden, wie das Medium (zum Beispiel ein Kabel) Informationen überträgt, empfängt und entkomprimiert und wie sie vom Empfänger gelesen werden. Wenn all das funktioniert, hat Datenübertragung stattgefunden. Dies ist Voraussetzung für die IT-Entwicklung in der Industrie.

Industrielle Datenkommunikation

Die größten Fortschritte in der Standardisierung der Datenübertragung fanden im Bürobereich statt, in den integrierten Netzwerken für Personal Computer, Mainframes, Druckern, Servern, Telefon-Modems usw. Lokale Datenübertragung in der Industrie stand nicht so sehr im Blickfeld, ebenso aufgrund fehlender Standards wie auch durch die noch größere Vielfalt, da die Datenkommunikation zum Beispiel zwischen Computern, Drehbänken, Messeinrichtungen, Waagen, Robotern, Transportsystemen sowie unterschiedlichen Alarmsystemen stattfindet. Die Ansprüche an Betriebssicherheit und Unempfindlichkeit gegen störende Einflüsse sind bedeutend höher. Hierin liegt die Aufgabe dieses Buches, Bezeichnungen und Arbeitsweisen sollen erklärt werden und es soll ein praktischer Führer bei der Problemlösung industrieller Datenübertragung sein. Falls Sie noch mehr wissen möchten, zögern Sie bitte nicht, sich an Westermo zu wenden.

Was bedeutet industrielle Datenkommunikation für uns?

Keine Ausfallzeiten

Sämtliche Anlagenteile müssen so ausgelegt sein, dass Übertragungsfehler und Ausfallzeiten eliminiert werden. Wir erreichen dies durch den Einsatz hochwertiger Komponenten, wie langlebige Kondensatoren und durch Überprüfung unserer Anlagen unter schwierigsten Umweltbedingungen mit hohem Störfaktor.

Keine Wartung

Unsere Produkte wurden entwickelt, um diesen schwierigsten Umweltbedingungen ohne Wartung und Service standzuhalten. Zusätzlich zu ihrer robusten Bauart enthalten sie niemals Komponenten, die ersetzt werden müssen, wie z. B. Batterien.

Extreme Umweltbedingungen

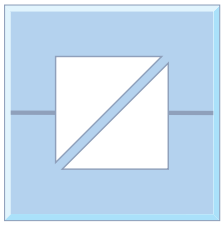
Industrieanlagen werden normalerweise gemeinsam mit oder in direkter Nähe anderer Anlagen installiert, die Störungen verursachen können, z. B. Schweißanlagen oder große Maschinen. Wir haben über 30 Jahre Erfahrung in Konstruktion und Herstellung von Datenübertragungsanlagen für die Industrie und wir nutzen unser gesamtes Wissen für die Weiterentwicklung dieser industriellen Anlagen.

Erweiterter Temperaturbereich

Bei industriellen Anlagen ist häufig ein erweiterter Temperaturbereich notwendig. Wir garantieren eine einwandfreie Funktionalität durch den Einsatz hochwertiger Komponenten mit erweitertem Temperaturbereich, zum Beispiel bei Hardware wie Anschlüssen.

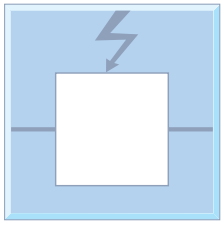
Mechanische Eigenschaften

Bei industriellen Anwendungen werden Ausrüstungsteile häufig an Maschinen montiert, die sich bewegen oder vibrieren. Unsere sämtlichen Produkte sind dafür ausgelegt, hohen mechanischen Beanspruchungen zu widerstehen. Ebenso wichtig wie die mechanische Zuverlässigkeit ist die Befestigungsmethode, daher umfasst unsere Produktpalette ebenso Einschubgeräte wie Geräte mit DIN-Befestigung sowie Tisch- oder Mini-Modem-Geräte.



Galvanische Trennung
Eine der häufigsten Störursachen bei Übertragungsfehlern ist ein Potentialunterschied zwischen miteinander verbundenen Anlagenteilen. Dies eliminieren wir durch galvanische Trennung der Schnittstelle, eines der Standardmerkmale sämtlicher Westermo-Produkte.

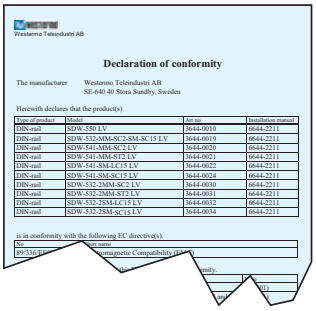
Unterdrückung von Spannungsspitzen
Industrieanlagen sind häufig starken Interferenzen ausgesetzt, die z. B. durch Hochspannungsleitungen, Blindlasten oder unterschiedliche Formen von elektromagnetischen Wellen erzeugt werden. Die Produkte von Westermo sind so konstruiert, dass sie diesen Interferenzen widerstehen.



Stromversorgung
Für industrielle Anlagen ist eine zuverlässige Stromversorgung besonders wichtig, daher wird häufig Gleichstrom in Verbindung mit Akkus eingesetzt, um Ausfallzeiten zu eliminieren. Bei der Akkuladung wird eine höhere Spannung eingesetzt als bei Batterien, daher müssen sämtliche Anlagenteile für diese Bedingungen ausgelegt sein. Manchmal ist der Einsatz einer redundanten Stromversorgung zu einer doppelten Sicherheit notwendig, diese Möglichkeit bieten viele unserer Produkte.

Determinierung

Beim Einsatz von Anlagen in Real-Time-Anwendungen ist es wichtig, unterschiedliche Ebenen der Priorität festlegen zu können. Unser Angebot an Switches bietet integrierte Funktionen und Warteschleifen, die die Übertragung von Daten mit Priorität sicherstellen.



Westermo Teleindustri AB

Declaration of conformity

The manufacturer Westermo Teleindustri AB
SE-640 40 Stora Sandby, Sweden

Herewith declares that the product(s)

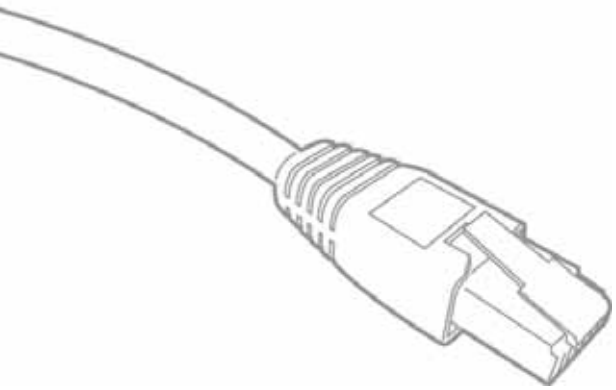
Type of product	Model	Art.no	Installation manual
DIN-rail	SDW-550 LV	3644-0010	6644-2211
DIN-rail	SDW-532-MM-SC2-SM-SC15 LV	3644-0019	6644-2211
DIN-rail	SDW-541-MM-SC2 LV	3644-0020	6644-2211
DIN-rail	SDW-541-MM-ST2 LV	3644-0021	6644-2211
DIN-rail	SDW-541-SM-LC15 LV	3644-0022	6644-2211
DIN-rail	SDW-541-SM-SC15 LV	3644-0024	6644-2211
DIN-rail	SDW-532-2MM-SC2 LV	3644-0030	6644-2211
DIN-rail	SDW-532-2MM-ST2 LV	3644-0031	6644-2211
DIN-rail	SDW-532-2SM-LC15 LV	3644-0032	6644-2211
DIN-rail	SDW-532-2SM-SC15 LV	3644-0034	6644-2211

is in conformity with the following EC directive(s).

No.	EC name
89/336/EEC	Electromagnetic Compatibility (EMC)

Anerkannte Standards

Unsere Anlagen sind weltweit in den unterschiedlichsten Anwendungsbereichen installiert. Um örtlichen Sicherheitsbestimmungen zu entsprechen, die elektrische Störsicherheit, Emissionen und mechanische Eigenschaften festlegen, konstruieren und fertigen wir auf der Grundlage internationaler Standards
und Anforderungen.



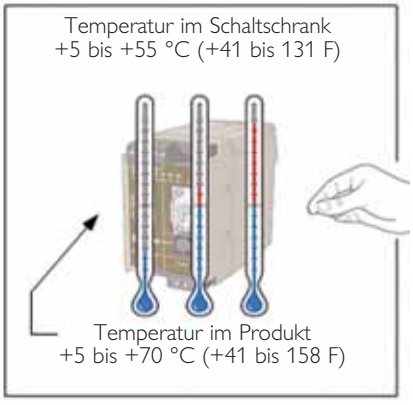
Allgemeine technische Daten

Umwelt- und mechanische Bedingungen

	Anforderung		
Faktor	**Beanspruchung**	**Standard**	**Hinweise**
Temperatur Betrieb	+ 5° bis + 55° C – 25 bis + 70° C* (–13 bis 158° F *)	IEC 721-3-3	
Temperatur Lagerung und Transport	– 25 bis + 70° C (–13 bis 158° F)	IEC 721-3-1/2	
Relative Luftfeuchtigkeit Betrieb	5 bis 95 %, nicht-kondensierend	IEC 721-3-3	Erst einsetzen, wenn sich Temperatur und Feuchtigkeit stabilisiert haben.
Relative Luftfeuchtigkeit Lagerung und Transport	5 bis 95 %, Kondensation zulässig unverpackt	IEC 721-3-1/2	Produkt in der Verpackung
Luftverschmutzung Belastungsniveau	G2 (1000 Å = 0,1 µm) Mittleres	ISA 71.04	Produkt in Gehäuse IP 21 installiert, oder vorteilhafter, mit begrenzter Luftzufuhr (kein Lüfter)

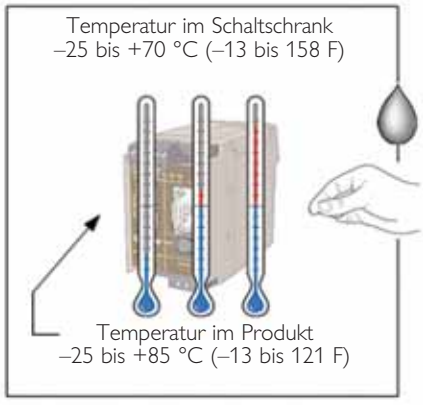
* Erweiterter Temperaturbereich

Industrieumgebung
Zulässige Betriebstemperatur +5 bis +40 °C
(+41 bis 104 F)



IP20
- Schutz vor dem Zugreifen auf gefährliche Spannungen mit den Fingern
- Schutz vor dem Eindringen von festen Fremdkörpern ≥12,5 mm

Außenumgebung
Zulässige Betriebstemperatur –25 bis +55 °C
(–13 bis 131 F)



IP21
- Schutz vor dem Zugreifen auf gefährliche Spannungen mit den Fingern
- Schutz vor dem Eindringen von festen Fremdkörpern ≥12,5 mm
- Schutz vor Beschädigung durch das Eindringen von senkrecht fallendem Tropfwasser.

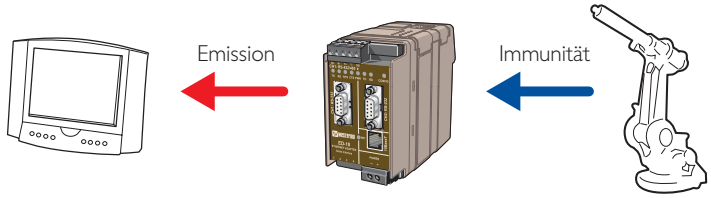
Anforderungen an Temperaturbereiche und IP-Klassifizierung bestehen auf unterschiedlichen Ebenen, wir unterscheiden zwischen industriellen Umgebungsbedingungen und Außeninstallationen. Die Komponenten für die jeweiligen Anwendungsbereiche müssen den Umgebungstemperaturen standhalten sowie der zusätzlichen Hitze unter Abdeckungen oder in Schaltschränken. Im allgemeinen rechnet man, dass jede Abdeckung für einen Temperaturanstieg von 15°C (59 F) sorgt, z. B. wählen wir Komponenten, die +85°C widerstehen (+121 F), damit wir (außerhalb des Schaltschrankes) eine Umgebungstemperatur von +55°C (+131 F) garantieren können.

Elektrische Bedingungen

	Anforderung			
Faktor	**Beanspruchung**	**Standard**	**Hinweise**	**Referenz**
Emission	EN 61000-6-3 Wohnbereich	EN 55022 Klasse B		**Siehe 1.1 und 1.2**
Immunität	EN 61000-6-2 Industriebereich	EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8 EN 61000-4-11		**Siehe 1.1 und 1.2**
	Informationstechnik Geräte	EN 55024		**Siehe 1.3**
Stromversorgung (LV) Spannungsbereich	 12 bis 48 VDC			**Siehe 2.1**
Betriebsspannungsbereich	9,6 bis 57,6 VDC			
Stromversorgung (HV) Spannungsbereich	 95 – 240 VAC 110 – 250 VDC			**Siehe 2.2**
Betriebsspannungsbereich	85,5 – 264 VAC 88 – 300 VDC			
Frequenzbereich der Stromversorgung	48 – 62 Hz			
Schutz gegen falsche Polarität	Ja			
Schutz gegen Kurzschluss	Teil der Gebäude- -installation			
TNV-3	Maximum 70,7 V Spitzenwert / 120 VDC		PSTN oder ähnlich	**Siehe 2.5**
TNV-1	Maximum 42,4 V Spitzenwert / 60 VDC		RS-422/485, Ethernet oder ähnlich	**Siehe 2.4**
SELV	Maximum 42.4 V Spitzenwert / 60 VDC		RS-232 oder ähnlich	**Siehe 2.3**

1.1 Allgemeine Emissionen

EN 61000-6-3 EMC – Allgemeine Standards – Emissionsstandard für Wohnbereiche, Geschäfts- und einfache Industrieumgebungen.



Immunität = Toleranz gegen Umwelteinflüsse.
Emission = Einfluss auf die Umwelt (Energiestrahlung).

Auf der Ebene der Toleranz gegen Umwelteinflüsse ist das Emissionsniveau ungefähr 100 000-fach geringer als die Auslegung unserer Geräte arbeitstechnisch vertragen.

Maximalwerte für Funkstörungen, die durch Anlagen verursacht werden, die an öffentliche Netze oder Wechselstromquellen angeschlossen sind. Diese Emissionswerte werden so festgelegt, dass Störabstrahlungen durch Anlagen im Normalbetrieb in Wohnbereichen, Büros, Geschäftsräumen und ähnlichen Umgebungen keine anderen Anlagen (z. B. Radioempfänger) in ihrer Funktion beeinträchtigen.

1.2 ITE-Emissionen

EN 55022 Information Technology Equipment (ITE) – Funkstörungs-eigenschaften – Grenzen und Messmethoden.

- Messmethoden und Grenzwerte für Funkstörungen durch ITE.
- Klasse B, ITE gilt für Wohnbereiche, Büros, Geschäftsräume und ähnliche Umgebungen. Keine Garantie für Schutz gegen Einflüsse bei Radio- und Fernsehempfang, wenn ITE-Anlagen in weniger als 10 m Entfernung der Empfangsantenne betrieben werden.
- Klasse A, ITE gilt für alle anderen Umgebungen (z. B. in der Industrie). Keine Garantie für Schutz gegen Einflüsse bei Radio- und Fernsehempfang, wenn ITE-Anlagen in weniger als 30 m Entfernung der Empfangsantenne betrieben werden.

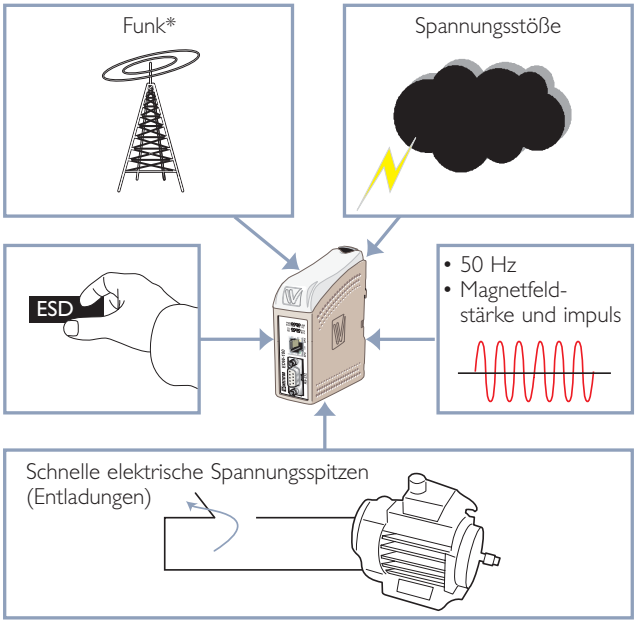
1.3 ITE-Immunität

EN 55024 Information Technology Equipment (ITE) – Immunitätseigenschaften – Grenzen und Messmethoden.

- Testanforderungen bei ITE-Anlagen für Immunität gegen kontinuierliche oder temporäre Spannungsspitzen und übertragene und abgestrahlte Störfrequenzen, einschließlich elektrostatischer Entladungen. Immunitätsanforderungen sorgen für eine ausreichende Immunität, damit die Anlagen in ihrem vorgesehenen Einsatzgebiet entsprechend funktionieren.

1.4 Allgemeine Immunität

EN 61000-6-2 Elektromagnetische Kompatibilität (EMC) Allgemeine Standards Immunitätsstandard für industrielle Umgebungen.



* Abgestrahlte Feldimmunität Übertragene Funk-frequenzfelder

Testanforderungen bei Anlagen, die an Netzwerke in industriellen Umgebungen angeschlossen sind, für Immunität gegen kontinuierliche oder temporäre Spannungsspitzen und übertragene und abgestrahlte Störfrequenzen (einschließlich elektrostatischer Entladungen). Immunitätsanforderungen sorgen für eine ausreichende Immunität bei Anlagen in industriellen Umgebungen.

1.5 EMC-Testmethode

EN 61000-4-2 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunitätstest gegen elektrostatische Entladungen.

- Testmethode für die Immunität elektrischer Anlagen gegen elektrostatische Entladungen, entweder direkt oder über Fremdobjekte. Führt einige Testverfahren für unterschiedliche Installations- und Umweltbedingungen auf.

EMC-Belastungsniveaus in unterschiedlichen Umgebungen

Wohnbereich
Wohnbereich, Geschäfts- und einfache Industrieumgebungen

Industrie
Immunität in industriellen Umgebungen

Eisenbahn
Eisenbahn — Signal- und Telekommunikationsanlagen

Nebenstation
Kommunikationsnetzwerke und — systeme in Elektro-Nebenstationen

Westermo
Eine Kombination von Anwendungsbereichen: Wohnen, Industrie, Eisenbahn, dazu die Erfahrungen bereits installierter Westermo-Produkte.

Merkmale, damit werden Leistungen eingeordnet

Merkmal A: Normale Leistung innerhalb festgelegter Grenzen (wie in den Testanforderungen festgelegt).

Merkmal B: Zeitlich begrenzter Funktions- oder Leistungsverlust, der mit dem Ende der Störung ebenfalls beendet ist, die getestete Anlage nimmt ohne Einflussnahme des Bedienungspersonals ihre normale Arbeitstätigkeit wieder auf.

Merkmal C: Zeitlich begrenzter Funktions- oder Leistungsverlust, die Fehlerkorrektur erfordert die Einflussnahme des Bedienungspersonals.

Test	Port	Westermo	
		Niveau	Merkmale
Emission			
Abgestrahlt	Gehäuse	30/37 dB (µV/m)	Klasse B
Übertragen	Wechselstrom	66-56/56/60 Qp dB (µV)	Klasse B
	Gleichstrom	66-56/56/60 Qp dB (µV)	Klasse B
Immunität			
ESD	Einschl. Kontakt	± 6 kV	B
	Einschl. Luft	± 8 kV	B
Abgestrahlte Feld-Immunität	Gehäuse	20 V/m 1 kHz 80 % AM 20 V/m 200 Hz Impuls	A A
Schnelle elektrische Spannungssp.	Signal	± 2,0 kV	A
	Wechselstrom	± 2,0 kV	A
	Gleichstrom	± 2,0 kV	A
Spannungs-stöße	Signal L-E Signal L-L	± 2,0 kV ± 2,0 kV	B B
	Wechselstr. L-E Wechselstr. L-L	± 2,0 kV ± 2,0 kV	B B
	Gleichstr. L-E Wechselstr. L-L	± 2,0 kV ± 2,0 kV	B B
Übertragenes Funk-frequenzfeld	Signal	10 V 1 kHz 80 % AM	A
	Stromversorgung	10 V 1 kHz 80 % AM	A
Stromversorgung Magnetfeld	Gehäuse	100 A/m 50 Hz	A
Impuls Magnetfeld	Gehäuse	300 A/m 6,4/16 µs	–
Wechselstr.*	Stromversorgung	30 % 10/500 ms 60 % 100/1000 ms Interrupt 10/5 ms	B B B
Gleichstrom	Stromversorgung	30 % 10 ms 60 % 10 ms Interrupt 10/100 ms 20 % über/unter Spannungsbereich	B B
Oszillierendes Wellen	Signal L-E Signal L-L	– –	– –
	Stromvers. L-E Stromves. L-L	– –	– –
50 Hz Stör-ungen**	Signal L-E Signal L-L	10/100 V 250 V	A A

* Spannungsabfälle, kurze Stromunterbrechungen und Spannungsschwankungen

** Übertragener gewöhnlicher Modus und Differentialmodus

Test	Port	Wohnbereich		Industrie		Eisenbahn		Nebenstation	
		Niveau	Merkmale	Niveau	Merkmale	Niveau	Merkmale	Niveau	Merkmale
Emission									
Abgestrahlt	Gehäuse	30/37 dB (µV/m)	Klasse B	40/47 dB(µV/m)	Klasse A	40/47 dB(µV/m)	Klasse A	30/37 dB(µV/m)	Klasse A&B
Übertragen	Wechselstrom	66-56/56/60 Qp dB(µV)	Klasse B	79/73 Qp dB (µV)	Klasse A	79/73 Qp dB (µV)	Klasse A	66-56/56/60 Qp dB (µV)	Class A&B
	Gleichstrom	–	–	–	–	79/73 Qp dB(µV)	Klasse A	–	–
Immunität									
ESD	Einschl. Kontakt	± 4 kV	B	± 4 kV	B	± 6 kV	B	± 6 kV	A***
	Einschl. Luft	± 8 kV	B	± 8 kV	B	± 8 kV	B	± 8 kV	A***
Abgestrahlte Feld-Immunität	Gehäuse	3 V/m 1 kHz 80 % AM	A	10 V/m 1 kHz 80 % AM	A	20 V/m 1 kHz 80 % AM	A	10 V/m 1 kHz 80 % AM	A
						20 V/m 200 Hz Impuls	A		
Schnelle elektrische Spannungssp.	Signal	± 0,5 kV	B	± 1,0 kV	B	± 2,0 kV	A	± 2,0 kV	A***
	Wechselstrom	± 1,0 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
	Gleichstrom	± 0,5 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
Spannungs-stöße	Signal L-E Signal L-L	± 0,5 kV –	B	± 1,0 kV –	B –	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Wechselstr. L-E Wechselstr. L-L	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Gleichstrom L-E Gleichstrom L-L	± 0,5 kV ± 0,5 kV	B B	± 0,5 kV ± 0,5 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
Übertragenes Funk-frequenzfeld	Signal	3 V 1 kHz 80 % AM	A	10 V 1 kHz 80 % Wechselstr.	A	10 V 1 kHz 80 % Wechselstr.	A	10 V 1 kHz 80 % Wechselstr.	A
	Strom-versorgung	3 V 1 kHz 80 % AM	A	10 V 1 kHz 80 % Wechselstr.	A	10 V 1 kHz 80 % Wechselstr.	A	10 V 1 kHz 80 % Wechselstr.	A
Stromver. Magnetfeld	Gehäuse	3 A/m 50 Hz	A	30 A/m 50 Hz	A	100 A/m 50 Hz	A	100 A/m 50 Hz	A
Impuls Magnetfeld	Gehäuse	– 6,4/16 µs	–	–	–	300 A/m	B	–	–
Wechselstr.*	Stromver.	30 % 0,5 s 60 % 100 ms Interrupt 5 s	B C C	30 % 10 ms 60 % 0,1/1 s Interrupt 5 s	B C C	–	–		
Gleichstrom	Stromver-sorgung	–	–	–	–	–	–	Interrupt 10 ms	A
								Interrupt willkürlich	C
Oszillierendes Wellen	Signal L-E Signal L-L	– –	– –	– –	– –	– –	– –	2,5 kV 1,0 kV	A*** A***
	Stromver. L-E Stromver. L-L	– –	– –	– –	– –	– –	– –	2,5 kV 1,0 kV	A*** A***
50 Hz Stör-ungen**	Signal L-E Signal L-L	– –	– –	– –	– –	– –	– –	30 V Gleichstr. 300 V 1 s 250 V	A A

* Spannungsabfälle, kurze Stromunterbrechungen und Spannungsschwankungen

** Übertragener gewöhnlicher Modus und Differentialmodus

*** Akzeptierter Fehler bei Übertragungsstörungen, falls keine Verzögerungen oder kein Datenverlust für wichtige Funktionen auftritt. Statusveränderungen der elektrischen, mechanischen oder Datenübertragungsausgänge sind nicht zulässig, dies gilt auch für Alarm- und Statusausgänge.

EN 61000-4-3 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunitätstest für abgestrahlte Funkfrequenzen und elektromagnetische Felder.

- Testmethode für die Immunität elektrischer Anlagen gegen abgestrahlte Funkfrequenzen und elektromagnetische Felder. Führt unterschiedliche Testanforderungen und —verfahren auf.

EN 61000-4-4 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunitätstest für schnelle elektrische Spannungsspitzen/Entladungen

- Testmethode für die Immunität elektrischer Anlagen gegen schnelle Spannungsspitzen und Entladungen. Führt unterschiedliche Testanforderungen und —verfahren auf.

EN 61000-4-5 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunitätstest für Spannungsstöße

- Testmethode für die Immunität von Anlagen gegen Spannungsstöße durch Blitzeinschläge oder das Schalten hoher Lasten. Führt einige Testverfahren für unterschiedliche Installations- und Umweltbedingungen auf.

EN 61000-4-6 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunität gegen Übertragungsstörungen durch Funkfrequenzfelder.

- Testmethode für die Immunität elektrischer Anlagen gegen Übertragungsstörungen durch Funkfrequenzfelder innerhalb des Frquenzbereiches von 9 kHz bis 80 MHz. Führt unterschiedliche Testanforderungen und —verfahren auf.

EN 61000-4-8 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Immunitätstest für Magnetfelder der Stromfrequenz.

- Testmethode für die Immunität elektrischer Anlagen gegen Magnetfelder der Stromfrequenz. Führt einige Testverfahren für unterschiedliche Installations- und Umweltbedingungen auf.

EN 61000-4-11 Elektromagnetische Kompatibilität (EMC) Test- und Messtechniken Test- und Messtechniken Immunitätstest gegen Spannungsabfälle, kurze Stromunterbrechungen und Spannungsschwankungen.

- Testmethode für die Immunität elektrischer Anlagen gegen Spannungsabfälle, kurze Stromunterbrechungen und Spannungsschwankungen. Führt unterschiedliche Testanforderungen und —verfahren auf.

Sicherheitsbedingungen

	Anforderung			
Faktor	**Beanspruchung**	**Standard**	**Hinweise**	**Referenz**
Elektrische Sicherheit	Informationstechnologie Geräte	EN 60.950		**Siehe 1.6**
Lebensdauer	10 Jahre			
Versorgungsanschluss	Fest angeschlossen			
Zugänglichkeit	Begrenzter Zugang		Zugang durch Service-Mitarbeiter und mit Werkzeugen	
Wartung	keine			
Isolation Verbindung	 An Schaltkreis(e)		 Stromstärke	
Versorgung Versorgung HV SELV TNV-1 TNV-1 TNV-3	Alle anderen Alle anderen TNV-1, TNV-3 TNV-3 TNV-1 TNV-3		≥1 kV AC 3 kV Wechselstrom 1 kV AC 1 kV AC 1 kV Wechselstrom 1 kV Wechselstrom	 **Siehe 2.3** **Siehe 2.4** **Siehe 2.5**

Installationsbedingungen

Installation	**Kategorie**	**Kabeltyp**	**Port**	**Hinweise**
Stromversorgung	II		Stromversorgung	
Stromversorgung (HV)	II		Stromversorgung	
TNV-3 (<70,7 Vp 120 V DC)	I	nicht abgeschirmt	Signal abgeglichen	PSTN oder ähnlich
TNV-1 (<42,4 Vp 60 V DC)	I	Paarverdrillt, nicht abgeschirmt	Signal abgeglichen	RS-422/485, Ethernet oder ähnlich
SELV (<42,4 Vp 60 V DC)	I	nicht abgeschirmt	Signal	RS-232 oder ähnlich

1.6 Elektrische Sicherheit

EN 60950 Information Technology Equipment. Sicherheit. Allgemeine Anforderungen.

- ITE-Sicherheitsstandard, der die Anforderungen an die Vermeidung von Feuergefahr, elektrischen Schlägen oder Verletzungen für das mit den Geräten in Kontakt kommenden Personen oder Bedienungspersonal festlegt. Dies gilt für Netzstrom- oder batteriebetriebene ITE ebenso wie für ITE, das direkt an Telefonnetze angeschlossen wird, unabhängig von der Stromversorgung.

Gehäuse

Faktor	Beanspruchung	Standard	Hinweise	Referenz
Maße (B x H x T) mm	55 x 100 x 128 (2.17 x3.94 x 5.04 in) 35 x 121 x 119 (1.43 x 4.76 x 4.69 in)		2 card DIN-Hutschiene 1 card DIN-Hutschiene	
Gewicht kg (pounds)	< 0.6 (<1.3)			
Montage	35 mm DIN-Hutschiene	EN 60715 (EN 50022)	Klick-Anschluss	
Schutzgrad	IP 20	IEC 529		**Siehe 1,7**
Kühlung	Konvektion, Abstand: 10 mm (0,4 in) (links/rechts) 25 mm (1.0 in) (oben/unten)		Abstand (links/rechts) empfohlen für volle Betriebsfähigkeit Temperaturbereich	
Gehäusematerial	PC / ABS			
Brandschutzklasse	Entflammbarkeitsklasse V-0	UL 94		**Siehe 1.8**

1.7 Schutzgrad

IEC 529 Schutzgrad durch Gehäuse (IP Code)

- Klassifizierung des Schutzgrades durch elektrische Gehäuse. Schutz von:
- Personen, gegen gefährliche Spannungen innerhalb der Anlage
- Innerhalb der Anlage gegen das Eindringen von festen Fremdkörpern
- Innerhalb der Anlage gegen Schäden durch eindringendes Wasser.

Zum Beispiel IP 21:

- Schutz vor dem Zugreifen auf gefährliche Spannungen mit den Fingern
- Schutz vor dem Eindringen von festen Fremdkörpern ≥12,5 mm
- Schutz vor Beschädigung durch das Eindringen von senkrecht fallendem Tropfwasser.

1.8 Entflammbarkeit

UL 94 Der Standard für die Entflammbarkeit von Anlagenkomponenten aus Kunststoffmaterialien

- Mess- und Darstellungsmethoden der Verhaltenseigenschaften bestimmter Materialien in Bezug auf Entflammbarkeit, wenn sie unter kontrollierten Laborbedingungen Hitze und Flammen ausgesetzt werden.

2 Definitionen

2.1 Spannungsbereich

- Vom Hersteller angegebener Spannungsbereich.

2.2 Betriebsspannungsbereich

- Spannungsbereich, in dem das Gerät, unter den angegebenen Bedingungen, seiner vorgesehenen Funktion entsprechend arbeitet. Spannungsbereich und obere sowie untere Toleranzen.

2.3 SELV

- Ein zweiter Schaltkreis, der so ausgelegt und abgesichert ist, dass seine Spannung unter normalen und Single-fault-Bedingungen einen Sicherheitswert nicht übersteigt.

2.4 TNV-1

- Ein zweiter Schaltkreis, dessen normale Betriebsspannung unter normalen Betriebsbedingungen die Grenzen eines SELV-Schaltkreises nicht übersteigt und in dem Überspannungen aus Telefonnetzwerken auftreten können.

2.5 TNV-3

- Ein zweiter Schaltkreis, dessen normale Betriebsspannung unter normalen Betriebsbedingungen die Grenzen eines SELV-Schaltkreises übersteigt und in dem Überspannungen aus Telefonnetzwerken auftreten können.

Datenkommunikation...

...ist besonders wichtig, um die Produktivität zu erhöhen

Fortschritte in der Automatisierung stellen verstärkte Anforderungen an eine zuverlässige Datenübertragung zwischen den Steuersystemen und den Anlagenteilen, die produzieren und messen. Datenübertragung ist das Nervensystem, das die Grundlage für eine gesteigerte Effizienz und Wettbewerbsfähigkeit bildet. Dies gilt ebenso für die Produktion wie für Installation, Transport und Gesundheitswesen.

Schnittstelle (Interface)

Vereinbarungen, die nur die Datensignale betreffen und wie sie konvertiert und übertragen werden, sind nicht ausreichend. Es sind auch Vereinbarungen notwendig, die die zu unterstützenden Anschlusstypen und Spannungsbereiche betreffen, mit anderen Worten, die physischen und elektrischen Schnittstellen. Und es gibt auch eine logische Schnittstelle, die die Wichtigkeit des Signals festlegt.
Ein Protokoll steuert den Signalaufbau, wie die Übertragungen eingeleitet werden und wie sie beendet werden, die Reihenfolge von Übertragung und Sendung, wie eine Meldung bestätigt wird, usw. Es gibt viele verschiedene Protokolle, zum Beispiel PROFIBUS, Comli, Modbus, usw.

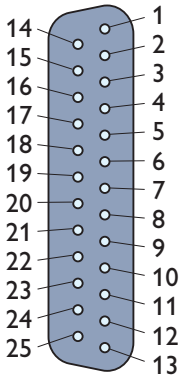
Die physische Schnittstelle	definiert, wie die Anlage angeschlossen ist und wie der Anschlusstyp aussieht.
Die elektrische Schnittstelle	definiert die elektrischen Potentiale und was sie bedeuten (Null oder Eins).
Die logische Schnittstelle	definiert, was die Signale bedeuten.

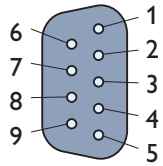
Die gebräuchlichsten Schnittstellen

Die gebräuchlichste Schnittstelle für die Datenübertragung über den seriellen Port von Computeranlagen ist RS-232/V.24, die normalerweise mit einem 9-/25-pol. Sub-D-Anschluss arbeitet. Gemäß den Empfehlungen für RS-232/V.24 sollte das Kabel zwischen angeschlossenen Anlagen nicht länger als 15 Meter sein. Um größere Übertragungsentfernungen zu erreichen, können unterschiedliche Modems je nach dem vorhandenen Übertragungsmedium verwendet werden (z. B. Glasfaser, Kupfer, Telekommunikationsnetz). V.24 (Europäischer CCITT-Standard) oder RS-232-C (Amerikanischer ITU-T-Standard) sind zwei im Prinzip identische Standards, siehe Tabelle Seite 25. V.24 beschreibt den physischen Standard und bei V.28 handelt es sich um den elektrischen Standard. Daher wird die Schnittstelle häufig als V.24/V.28 bezeichnet.
Die Schnittstelle beschreibt und definiert die Anschlusspins sowie die unterstützten Signale und Spannungsbereiche.

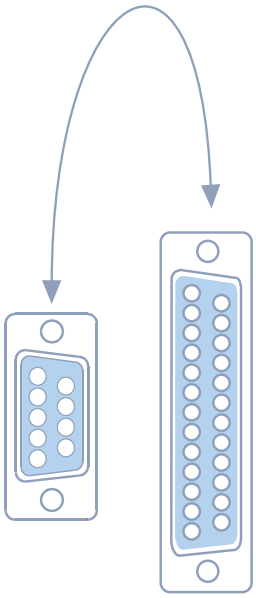
Signale in V.24/RS-232-C

Stift 9/25	Bezeichnung V.24	Bezeichnung RS-232	Stift	Signalname	Richtung DCE
1	**101**	**AA**	**GND**	**Protective Ground**	–
3 2	**103**	**BA**	**TD**	**Transmitted data**	**I**
2 3	**104**	**BB**	**RD**	**Received data**	**O**
7 4	**105**	**CA**	**RTS**	**Request To Send**	**I**
8 5	**106**	**CB**	**CTS**	**Clear To Send**	**O**
6 6	**107**	**CC**	**DSR**	**Data Set Ready**	**O**
5 7	**102**	**AB**	**SG**	**Signal Ground**	–
1 8	**109**	**CF**	**DCD**	**Data Carrier Detector**	**O**
9	–	–		can be + 12 V	–
10	–	–		can be – 12 V	–
11	126	SCF	STF	Select Transmit Frequency	**I**
12	122	SCB		Secondary DCD	**O**
13	121	SBA		Secondary CTS	**O**
14	118	SBA		Secondary TD	**I**
15	**114**	**DB**	**TC**	**Transmit Clock**	**O**
16	119	SBB		Secondary RD	**O**
17	**115**	**DD**	**RC**	**Receive Clock**	**O**
18	–	–		–	–
19	120	SCA		Secondary RTS	**I**
4 20	**108/2**	**CD**	**DTR**	**Data Terminal Ready**	**I**
21	110	CG	SQD	Signal Quality Detect	**O**
9 22	**125**	**CE**	**RI**	**Ring Indicator**	**O**
23	111	CH/CI		Data Signal Rate Selector	**O**
24	**113**	**DA**	**EC**	**External Clock**	**I**
25	133	–	RFR	Ready For Receiving	**I**





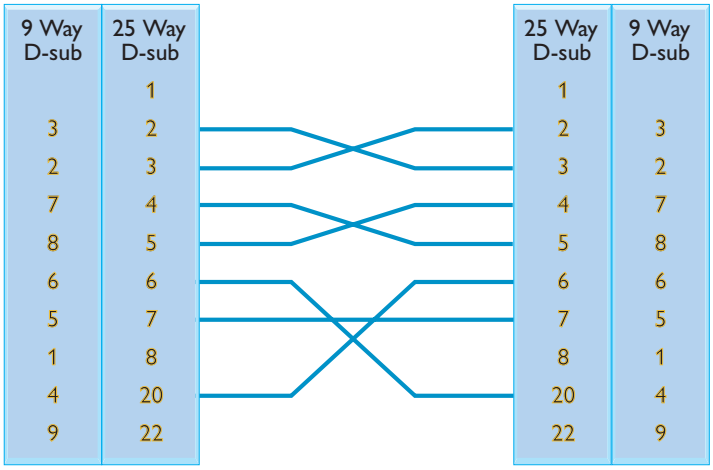
Fettdruck bezeichnet die gebräuchlichsten Signale bei der lokalen Kommunikation mit Kurzstreckenmodems. Richtung **I/O** bezeichnet die Richtung zum/vom Modem (DCE), wobei es sich bei **I** um einen Input und **bei O** um einen Output handelt. Dementsprechend ist das TD (Transmit Data) Signal in einem DTE ein Output und in einem DCE ein Input. Die Definition von DCE und DTE ist eine der häufigsten Fehlerquellen, falls diese mit RS-232-Anlagen verlinkt sind, siehe Seite 26.



Leitungskonfiguration

Unten wird gezeigt, wie der Anschluss zwischen 9-/25-pol. Sub-D-Anschlüssen für sämtliche Kombinationen von DTE- und DCE-Geräten hergestellt wird.

DTE an DTE oder DCE an DCE



DTE an DCE

Schlüssel zu den wichtigsten Signalen

Erklärung der wichtigsten Signale

GND	**Schutzerde**	Pin Nr. 1 ist für den Schutzleiter zwischen den Geräten reserviert.
SG	**Signalmasse Erde**	Signalmasse Erde ist eine Signalreferenz und muss immer an Pin 7 (25-pol) oder Pin 5 (9-pol) bei V.24 angeschlossen werden.
TD	**Übertragene Daten**	Dieses Signal übermittelt Daten von einem DTE an ein DCE.
RD	**Empfangene Daten**	Dieses Signal sind die Daten, die ein Modem oder ein DCE an ein DTE übermittelt.
RTS	**Sendeanfrage**	Dieses Signal ist eine Anfrage, Daten von einem DTE zu senden. Das Gerät wartet auf das CTS-Antwortsignal.
CTS	**Sendebereit**	Das Antwortsignal von DCE, dass dem DTE mitteilt, dass es Daten senden kann.
DSR	**Datensatz bereit**	Das Signal von einem DCE, das anzeigt, dass das Gerät eingeschaltet, angeschlossen und bereit ist.
DTR	**Datenterminal bereit**	Das gleiche wie DSR, aber von einem DTE.
DCD	**Erkennung des Datenträgers**	Das Ausgangssignal von einem DCE, das anzeigt, dass ein Träger zwischen den DCEs vorhanden ist und dass die Verbindung zur Datenübertragung bereit ist.
EC	**Externe Uhr**	Dieses Signal wird in synchronen Übertragungen verwendet, bei denen Daten ein Zeitimpuls beigegeben wird. Das Signal ist das Eingangssignal in ein DCE.
TC	**Zeitsignal übertragen**	Überträgt das DCE-Zeitsignal in synchronen Systemen.
RC	**Zeitsignal empfangen**	Zeitsignal im DTE zur Decodierung der Daten empfangen.
RI	**Ring-Indikator**	Ausgangssignal von einem Modem, das anzeigt, dass ein Ringsignal empfangen wurde.

ASCII

ASCII ist eine Abkürzung für American Standard Code for Information Interchange. Unterschiedliche ASCII-Codes sind für unterschiedliche Sprachen vorhanden, ebenso ein Extended (erweiterter) ASCII-Code, bei dem das achte Datenbit verwendet wird.

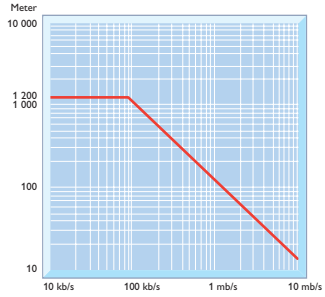
BINARY				b_6	0	0	0	0	1	1	1	1
				b_5	0	0	1	1	0	0	1	1
				b_4	0	1	0	1	0	1	0	1
b_3	b_2	b_1	b_0	**HEX**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	**0**	NUL	DLE	SP	0	@ / É	P	` / é	p
0	0	0	1	**1**	SOH	DC_1	!	1	A	Q	a	q
0	0	1	0	**2**	STX	DC_2	"	2	B	R	b	r
0	0	1	1	**3**	ETX	DC_3	#	3	C	S	c	s
0	1	0	0	**4**	EOT	DC_4	$ / €	4	D	T	d	t
0	1	0	1	**5**	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	**6**	ACK	SYN	&	6	F	V	f	v
0	1	1	1	**7**	BEL	ETB	'	7	G	W	g	w
1	0	0	0	**8**	BS	CAN	(	8	H	X	h	x
1	0	0	1	**9**	HT	EM	)	9	I	Y	i	y
1	0	1	0	**A**	LF	SUB	*	:	J	Z	j	z
1	0	1	1	**B**	VT	ESC	+	;	K	[/ Ä	k	{ / ä
1	1	0	0	**C**	FF	FS	,	<	L	\ / Ö	l	| / ö
1	1	0	1	**D**	CR	GS	-	=	M	] / Å	m	} / å
1	1	1	0	**E**	SO	RS	.	>	N	^ / Ü	n	~ / ü
1	1	1	1	**F**	SI	US	/	?	O	_	o	DEL

Industrielle Schnittstellen

RS-422

RS-422 ist ein idealer Standard für die Industrie, da die Schnittstelle dafür ausgelegt ist, Datenbusse, normalerweise Multidrop, zwischen Zentralrechnern und verschiedenen nachgeordneten Stationen aufzubauen. Die Schnittstelle arbeitet symmetrisch und relativ unempfindlich gegen äußere Störungen . Die Schnittstelle wechselt die Polarität auf dem Kabelpaar, je nachdem ob eine Eins oder eine Null übertragen wird. Ursprünglich war RS-422 nur dafür ausgelegt, von einem Mastergerät an 10 Slavegeräte zu übertragen, die die Daten auch nur abhören konnten. Wir setzen die "drive circuits" für RS-485 ein, wobei der Sender mit 32 Geräten kommunizieren kann und auch im Tri-state-Modus arbeiten kann, d.h. wir können Anwendungen mit Multidrop entwickeln, die ebenso mit 4-adrigen wie mit 2-adrigen Leitungen arbeiten.

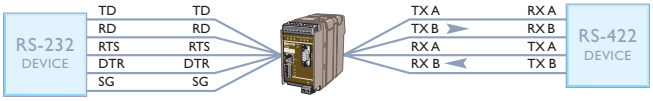
Die empfohlene Maximalentfernung beträgt 1200 m bei einer Übertragungsrate von 100 kbit/s. Die "drive circuits" unterstützen Datenraten bis zu 10 Mbit/s, aber der Übertragungsabstand verringert sich dann auf 20 m. RS-422 kann über einen Wandler in RS-485, RS-232/V.24 integriert werden.



RS-485 Übertragungs-reichweite

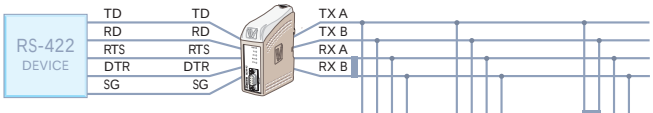
RS-422, 4-adrig

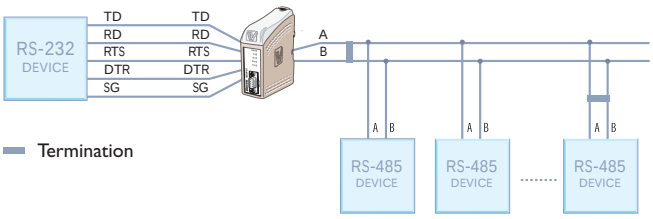
In einem 4-adrigen RS-422-System kann der Master-Sender immer aktiv/eingeschaltet sein, Der Standard ermöglicht vollduplex Verbindungen.

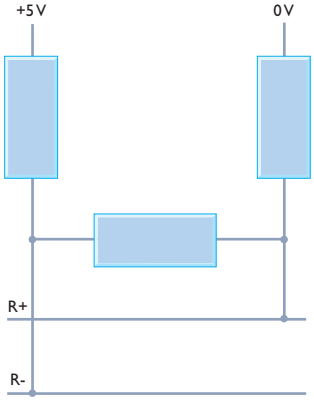


RS-485

RS-485 ist eine Weiterentwicklung von RS-422 und wird verstärkt als Standard bei unterschiedlichen Anlagen eingesetzt. Der größte Vorteil von RS-485 ist die Unterstützung von 2-adrigem Datenaustausch, d.h. Sender und Empfänger der Anlage können die Richtung der Datenübertragung umkehren. Sie ist für Datenbusse für bis zu 32 Geräte ausgelegt und für Multidrop-Netzwerke mit Master/Slave-Verbindungen geeignet. Die empfohlene Maximalentfernung beträgt 1200 m bei einer Übertragungsrate von 100 kbit/s. Es gibt viele verschiedene Standard-Schnittstellen, die RS-485 als physisches Medium verwenden, z.B. PROFIBUS, Interbus-S und Bitbus.





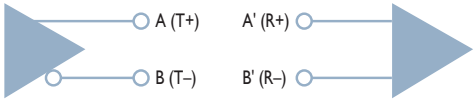


Termination und Fail-Safe

Die Leitung sollte eine Termination haben, die den gleichen Widerstandswert besitzt, wie der Impedanzwert der Leitung. Der Widerstandswert sollte etwa 120 Ohm betragen. Endanschlüsse sollten so ausgeführt werden, wie im Diagramm auf Seite 29 gezeigt. Das Wort Endanschluss bitte in Termination ändern! Endanschlüsse verhindern Reflektionen im Kabel. "Fail-safe" ist ein Widerstand von jedem Draht auf der Plus-Versorgungsleitung sowie auf der 0V Seite. Dies bedeutet, dass die Leitung mit einer vorbestimmten passiven Ebene verlegt wird, anderenfalls läuft die Leitung Gefahr, durch Störungen als Daten erkannt zu werden.

Polarität

Die Verbindung zwischen Sender und Empfänger muss mit der korrekten Polarität im Verhältnis zueinander erfolgen. Durch den Anschluss von Geräten unterschiedlicher Hersteller wissen wir aus Erfahrung, dass Standards verschieden interpretiert werden können. Ein Polaritätsfehler in Verbindung mit anderen Geräten bedeutet, dass dieses Gerät die Daten nicht korrekt interpretiert. Gemäß dem Standard wird der Sender mit A und B bezeichnet, diese werden an A´ und B´ angeschlossen. Wir haben uns entschlossen, diese Bezeichnungen durch T+, T–, R+ and R- besser zu kennzeichnen (transmit/receive + und –).

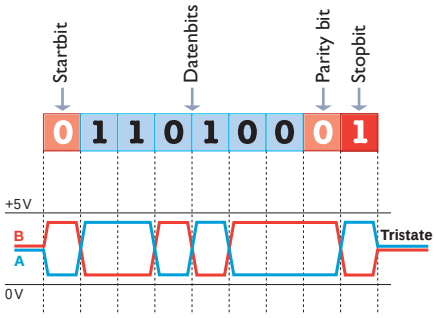


RS-232/V.24 zu RS-422/485 Wandler – RTS-Unterstützung

Systeme mit RS-422/485 Wandlern in einem Multidrop-Netzwerk ermöglichen es zu einem bestimmten Zeitpunkt nur einem Sender auf dem Bus aktiv zu sein. Die Sender anderer Geräte müssen sich im "Tri-state"-Modus befinden, d.h. passiv sein. Dafür muss die Möglichkeit bestehen, angeschlossene Geräte über ein Hardware-Signal zu steuern. Dazu werden normalerweise RTS- oder DTR-Signale verwendet. Wenn ein Gerät auf dem Bus senden möchte, muss es zuerst sein RTS- oder DTR-Signal hochsetzen, damit der Wandler seinen Sender so schaltet, dass er daraufhin die Daten senden kann. Falls kein Hardware-Signal zur Verfügung steht, kann ein spezieller Wandler eingesetzt werden, der seinen Sender sofort einschaltet, wenn Daten über RS-232 gesendet werden und ihn sofort abschaltet, wenn der Datenfluss stoppt.

Installation von RS-422 und RS-485

Allgemeine Empfehlungen für die Installation

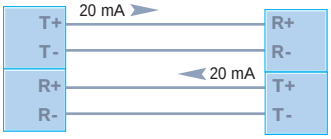


- Paarverseilte Vierdrahtleitungen sollten verwendet werden.
- Stern-Netzwerke sind nicht zulässig und der Abstand vom Bus zum Gerät darf maximal 30 cm betragen.
- Empfänger am Ende des Busses müssen mit einem 120-Ohm Widerstand versehen werden.
- Die RS-232/V.24 Verbindung sollte nicht länger als 15 Meter sein.
- RS-422/485 unterstützt Übertragungsentfernungen bis zu 1200 m bei 100 kbit/s. Bei einer verringerten Übertragungsrate können bedeutend größere Reichweiten erzielt werden.

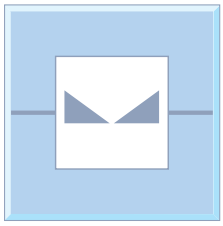
Übertragungsabstände und Kurzstreckenmodems

Wie bereits erwähnt, wird der Standard RS-232/V.24 nicht für Leitungen empfohlen, die länger als etwa 15 Meter sind. Mit Kurzstreckenmodems können längere Verbindungen eingerichtet werden. Diese wandeln RS-232/V.24 Signale in definierte elektrische oder optische Signale um, die dann über mehrere Kilometer z. B. mit Standleitungen per Glasfaserkabel oder paarverseilten Vierdrahtleitungen übertragen werden. Das Kurzstreckenmodem auf der Empfangsseite wandelt dann die Signale wieder in RS-232/V.24 Signale um. Das Modem muss für die Datenübertragung per Kabel einen gemeinsamen Standard und eine identische Schnittstelle verwenden.

20 mA Stromschleife (TTY)



Die älteste Technik ist die Stromschleife. RS-232/V.24 Signale werden in einer 20 mA-Stromschleife als Anwesenheit oder Abwesenheit von Spannung im Leitungspaar kodiert.
Um jedes Leitungspaar mit Spannung zu versorgen, ist entweder der Sender aktiv angeschlossen und der Empfänger passiv oder umgekehrt. Die Stromschleife ermöglicht zuverlässige Übertragungen, ist aber verhältnismäßig empfindlich gegen Störungen, da sie nicht symmetrisch ist (siehe Seite 40). Zusätzlich können Probleme mit den Geräten auftreten, da es für die Stromschleife keinen anerkannten Standard gibt.

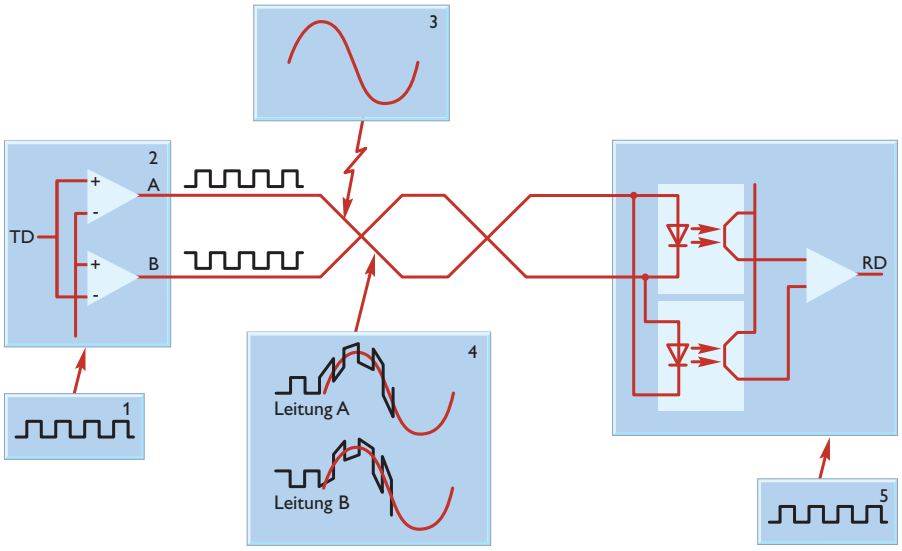


10 mA symmetrische Stromschleife (W1)

Westermo hat für Kurzstreckenmodems eine eigene Übertragungstechnik entwickelt, die Übertragungen über größere Distanzen und unter Umweltbedingungen mit hohem Störpotential sicherstellt. Bei dieser Technologie werden die Signale in eine ±10 mA symmetrische Stromschleife konvertiert, wobei die Stromrichtung auf dem Leitungspaar verändert wird, je nachdem, ob ein hohes oder niedriges Signal von RS-232/V.24 ausgegeben wird. Die Leitung des Senders wird mit ±10 mA gespeist und auf der Empfangsseite erkennt ein Optokoppler das Signal. Die Optokoppler bewirken eine komplette galvanische Trennung zwischen den Modems. Der Strom fließt immer nur in eine Richtung, auch wenn keine Geräte an die RS-232/V.24 Schnittstellenseite angeschlossen sind. Eine Ausnahme ist die Steuerung/Aktivierung des Senders über ein Handshake-Signal. In langen Jahren hat sich diese Technik als sehr zuverlässig und störungsfrei erwiesen und sie ermöglicht Datenübertragungen über Distanzen bis zu 18 km.

Daher ist die 10 mA symmetrische Stromschleife weniger anfällig für externe Störquellen.

Im Vergleich mit einer unsymmetrischen Stromschleife ist die symmetrische Stromschleife bedeutend unempfindlicher gegen externe Störungen, da der Potentialunterschied auch bei Störungen der Leitung erhalten bleibt. Siehe Abbildung unten.



1. Daten werden an den Sender übertragen.
2. Die Datensignale der Leitung A sind umgekehrt zu den Datensignalen der Leitung B .
3. Die Leitung ist Störungen ausgesetzt.
4. Übertragene Daten überlagern die Störung.
5. Die auf der Empfangsseite ankommenden Datensignale sind unverändert von den vom Sender ausgesendeten Datensignalen (1).

Netzwerk

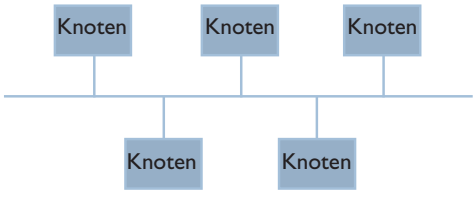
Der Durchbruch lokaler Netzwerke erfolgte in den achtziger Jahren, zuerst über zentralisierte Großrechner, aber auch bei Minicomputern mit sternförmig angeschlossenen Terminals. Die Einführung dieser Netzwerke zeigte gleichzeitig den Bedarf nach einer sicheren und zuverlässigen Ddatenübertragung.

Datenübertragung erfordert: Einen Sender, einen Empfänger, ein Übertragungsmedium sowie Informationen und ein Protokoll. Sender, Empfänger und Medium brauchen bestimmte Spezifikationen für die physischen Geräte (wie sie an ein Netzwerk angeschlossen werden, usw.). Das Protokoll regelt, wie die Datenübertragung erfolgt, dies wird in einem späteren Kapitel erklärt.

Ein lokales Netzwerk kann ebenso Daten für ein Büro übertragen, wie für Industrie, Krankenhäuser, Minenanlagen oder die Verkehrsüberwachung. Ein leistungsstarkes Netzwerk mit einer zuverlässigen Datenübertragung ist eine der Grundlagen, auf denen Unternehmen oder Organisationen sich weiterentwickeln können:

- *Informationen sind für alle verfügbar,* gemeinsame Datenbanken können genutzt werden, E-mail und File-sharing erhöhen ebenfalls die Arbeitseffektivität.
- *Gemeinsame Ressourcen,* mehrere Anwender teilen sich wichtige Ressourcen des Netzwerkes, z. B. Farbdrucker oder gemeinsame Programme eines Servers.
- *Sicherheit,* durch Zugangsprivilegien zum Netzwerk für individuelle Anwender oder Gruppen von Anwendern kann der Zugriff auf individuelle Anwendungen kontrolliert werden. Dadurch kann die Verwaltungseffektivität zentral gesteigert werden.

Wenn von Netzwerken gesprochen wird, werden auch regelmäßig Knoten erwähnt. Ein Knoten ist z. B. ein Computer, ein Drucker oder eine Datenübertragungsanlage. Da sehr viele verschiedene Knotentypen mit einer Vielzahl von Funktionen existieren, ist es ausgesprochen wichtig, dass es Regeln gibt, wie sie miteinander kommunizieren sollen.



Genauso, wie sich nur Menschen mit der gleichen Sprache untereinander verstehen, müssen die Netzwerk-Geräte die gleiche Sprache sprechen. Dies wird über ein Protokoll geregelt, das festlegt, wie die Kommunikation ablaufen soll, was gesagt werden kann, von wem und wann und wie. Diese Protokolle müssen aufeinander abgestimmt sein, damit alle Hersteller sich an die gleichen Regeln halten. Standards können von einzelnen Unternehmen entwickelt werden (De-facto-Standards) oder von allgemein anerkannten, übergeordneten offiziellen Stellen wie ISO, ANSI or IEEE.

Unter anderem hängt die Qualität eines Netzwerkes ab von der:

- Geschwindigkeit, die wiederum von der Anzahl der gleichzeitigen Anwender abhängt, sowie vom Medium, von der Hardware und Software.
- Art der Übertragung, ob der richtige Empfänger erreicht wird, und ausschließlich nur er.
- Qualität der Daten sowie der Minimierung von Übertragungsstörungen.
- Geschwindigkeit des Netzwerkes.
- Zuverlässigkeit, d.h. wie gut das Netzwerk gegen Spannungsspitzen, Erdströme und andere die Datenübertragung störende Einflüsse abgesichert ist.
- Sicherheit, d.h. wie sicher das Netzwerk gegen Angriffe und Viren ist.

Mit der Zeit ergab sich ein steigender Bedarf nach der Vernetzung verschiedener lokaler Netzwerke, so dass Daten zwischen Unternehmen ausgetauscht werden können oder auch innerhalb eines nationalen oder internationalen Unternehmens. Wie kommunizieren die verschiedenen Computersysteme und Datenbanken eines Unternehmens miteinander, wenn sie weltweit verstreut sind? Es gibt viele Möglichkeiten:

- LAN (**L**ocal **A**rea **N**etwok), ein schnelles Netzwerk für lokale Datenübertragung, z. B. Ethernet.
- MAN (**M**etropolitan **A**rea **N**etwork), ein schnelles Netzwerk, das eine größere geographische Fläche abdeckt.
- WAN (**W**ide **A**rea **N**etwork), ein Netzwerk mit sehr großer geographischer Verbreitung, landesweit oder sogar weltweit.
- VAN (**V**alue **A**dded **N**etwork), ist ein Netzwerk, dass noch weitere Leistungen bietet, als nur Datenübertragung.
- GAN (**G**lobal **A**rea **N**etwork), ist ein Netzwerk, das mehrere lokale Netzwerke umfasst, die entweder über MAN und schnelles WAN zusammengeschlossen werden können.
- AAN (**A**ll **A**rea **N**etwork), ein Netzwerk, das ebenso in lokalen wie auch in geographisch weiter verbreiteten Netzwerken eingesetzt werden kann.

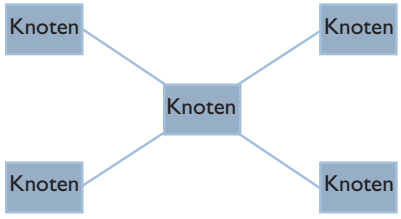
Topologie

Die Bezeichnung Topologie bezieht sich auf die Struktur des Netzwerkes, auf die physische oder logische Lage der Knoten. Es gibt fünf grundlegende Topologien: Punkt-zu-Punkt, Ring, Stern, Bus und kombiniertes Netzwerk. Die Auswahl der Topologie ist wichtig, da es sich um eine langfristige Infrastrukturentscheidung handelt, die für Bearbeitung und Transport wichtiger Daten ohne Zeitverlust und Ausfall verantwortlich ist. Zusätzlich muss die Möglichkeit bestehen, das Netzwerk an sich eventuell verändernde Bedingungen anzupassen und zu erweitern.

Serielle Punkt-zu-Punkt-Verbindungen

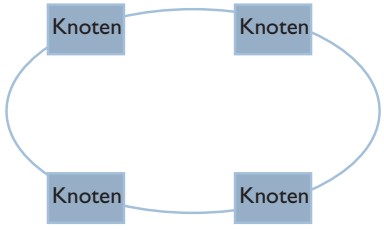
Punkt-zu-Punkt Datenübertragung, d.h. zwischen zwei kommunizierenden Geräten, ist eine der häufigsten Anwendungen. Das gilt ebenso für einfache Anwendungen, wie Computer zu Drucker, als auch bei anspruchsvolleren Lösungen, bei denen jeder Anwender aus Sicherheitsgründen mit einer eigenen Leitung arbeitet. Die Standardschnittstelle RS-232/V.24 ist für Übertragungsdistanzen über 15 Metern nicht empfehlenswert. Aus diesem Grund wird ein Modem verwendet, um die Leitung zu erweitern, um Störungen zu unterbinden und um die Distanz auf bis zu 18 km zu erhöhen.

Stern-Netzwerk



Ein Netzwerk mit mehreren angeschlossenen Punkt-zu-Punkt-Anwendern wird als Stern-Netzwerk bezeichnet. Jedes Gerät kommuniziert mit dem zentralen Gerät in der Mitte auf einer eigenen Leitung. Das Stern-Netzwerk bietet den Vorteil einer sehr hohen Zuverlässigkeit. Falls eine Leitung ausfällt, werden die anderen Leitungen davon nicht beeinträchtigt. Nachteile sind der höhere Leitungsbedarf und eine damit verbundene Kostenerhöhung sowie die Tatsache, dass alle Datenströme über das zentrale Gerät laufen müssen.

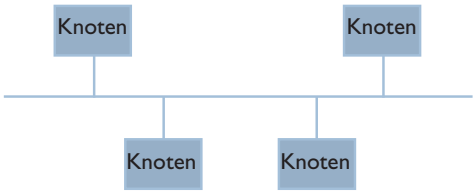
Ring-Netzwerk



Ein Ring-Netzwerk verbindet alle Geräte einer Serie hintereinander in einem geschlossenen Ring. Dies bedeutet, dass alle Datenflüsse "durch" sämtliche Geräte des Rings fließen müssen, um den Endempfänger zu erreichen. Ein "empty slot" (freie Stelle) wird um das Netzwerk geschickt, um Kollisionen zu vermeiden. Der Sendeknoten überprüft ob der Slot frei ist, markiert seine Adresse und hängt seine Dateninformationen an. Der nächste Knoten überprüft, ob die Daten im Slot für ihn bestimmt sind, ist das nicht der Fall, werden sie weitergeleitet. Wenn der Slot den korrekten Empfänger erreicht, leert dieser den Inhalt, fügt eine Empfangsbestätigung ein und sendet diese wieder in das Netzwerk. Das Sendegerät überprüft, ob die Nachricht erhalten und bestätigt wurde, danach wird der jetzt wieder freie Slot für eine neue Datenübertragung weitergeschickt. Token Ring ist ein Beispiel für ein Ring-Netzwerk aus Signalsicht, das physisch wie ein Stern-Netzwerk verbunden ist. Ring-Netzwerke bieten eine hohe Leistungsfähigkeit, sind aber, im Vergleich mit einem Bus-Netzwerk, schwieriger aufzubauen und anzupassen.

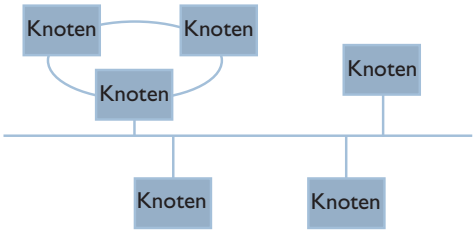
Bus-Netzwerk

Prinzipiell besteht ein Bus-Netzwerk aus einer Hauptleitung, an die alle Geräte als Knoten angeschlossen werden. Der gesamte Datenverkehr wird über den Bus zu den Empfängern geleitet. Ein Bus-Netzwerk muss Regelmöglichkeiten bieten, dass die Datensender erkennen können, ob die Leitung frei ist und wie sie reagieren müssen, falls es während einer Übertragung zu Datenkollisionen kommt, z. B. durch eine verzögerte Übertragung. Ein Bus-Netzwerk ist einfach zu installieren, zu vergrößern und zu erweitern. Ethernet und AppleTalk sind bekannte Beispiele für Bus-Netzwerke. Einer der Nachteile ist ein langsamer Datenverkehr, wenn viele Geräte im Netzwerk kommunizieren. Das Bus-Netzwerk kann jedoch in mehrere kurze Busse unterteilt werden, die das Netzwerk segmentieren.



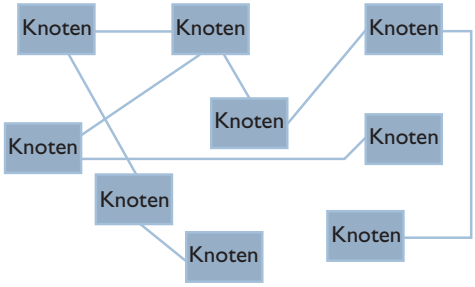
Kombiniertes Netzwerk

Der Einsatz von verschiedenen Kommunikationsgeräten ermöglicht den Aufbau sehr individueller Netzwerklösungen, die die Vorteile unterschiedlicher Topologien zusammenfassen, einschließlich Leistungsfähigkeit und Zuverlässigkeit. Zum Beispiel ein Bus-Netzwerk mit verteilten Stern-Netzen, eine Lösung, die mehrere Stern-Netzwerke verbindet. Wichtig dabei ist, dass jedes Netzwerk über ein arbeitsfähiges Regulierungssystem verfügt, das Datenverkehr und Kommunikation steuert.



Maschen-Netzwerk

Netzwerke, die ohne Struktur miteinander verbunden sind, werden als Maschen-Netzwerke bezeichnet. In einem schlecht dokumentierten Netzwerk ohne Struktur ist die Gefahr von Kommunikationsstörungen durch Fehler verhältnismäßig groß. Falls zum Beispiel ein weiterer Knoten angeschlossen und dadurch eine Schleife geschaffen wird, kann eine Datensendung im Netzwerk zirkulieren, weitere Sendungen erhöhen den Datenverkehr und das kann eventuell zu einem Datenwirrwarr im Netzwerk führen.

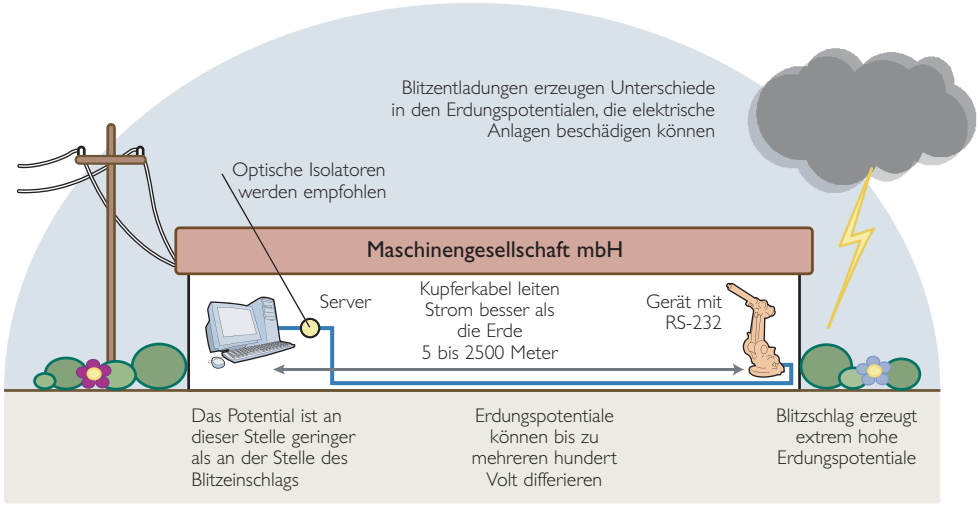


Das Problem der Interferenz

Leider sind noch nicht alle Probleme gelöst, auch wenn wir bei der Suche nach der richtigen Übertragungsmethode und der richtigen Schnittstelle erfolgreich waren. Den meisten Ärger in der Datenübertragung verursachen immer noch Interferenzen. Äußere Störungen, die zu Datenverlust und Übertragungsstörungen führen und im schlimmsten Fall zum Ausfall der Anlagen. Die Weiterentwicklung der Computer führte zu kleineren Anlagen sowie zu Komponenten, die weniger Strom verbrauchen. Vom Energiestandpunkt gesehen, ist das ideal, aber leider wurden die Komponenten dadurch empfindlicher und anfälliger für Überspannungen. Untersuchungen zeigen, dass bis zu 70 % aller Datenstörungen auf Installationsfehler oder Umgebungseinflüsse von benachbarten Maschinen, Einrichtungen oder Kabeln zurückzuführen sind. Nur 20 % der Ausfälle werden von Hard- oder Software verursacht. Daher finden sich die meisten Fehlerquellen innerhalb der eigenen Gebäude oder in direkter Nähe. Die anderen kommen von außerhalb. Wie ein Blitz aus heiterem Himmel. Die größte Fehlergruppe sind Spannungsspitzen. Kurze aber hohe Spannungsimpulse im Netzwerk. Computeranlagen, die Spannungsspitzen von 1000 V und bis zu 10 kV für einige Millisekunden ausgesetzt sind, sind stark gefährdet.

Gewitter-, Maschinen- und Leuchtstoffröhren-Einflüsse

Es ist bekannt, dass ein direkter Blitzschlag sehr hohe Spannungen freisetzt, dass diese weitergeleitet werden und Elektro- und Telefonleitungen beschädigen können, im schlimmsten Fall können sie auch Feuer verursachen. Selbst bei nicht direktem Blitzeinschlag, können die Spannungsimpulse über große Entfernungen in Leitungsnetzwerken oder durch Unterschiede im Erdungspotential zwischen zwei Punkten, übertragen werden. Daher können Lampen flackern, selbst wenn das Gewitter weit entfernt zu sein scheint.



Aber nicht nur Gewitter erzeugen externe Spannungsspitzen. Lampen können ebenfalls flackern, wenn naheliegende Industrieanlagen an- oder abgeschaltet werden und damit Einschaltstöße und Spannungsspitzen im Netzwerk erzeugen.

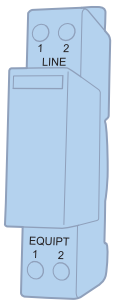
Als Regel kann man aber annehmen, dass die meisten Spannungsspitzen ihre Ursache innerhalb des eigenen Werksgeländes haben. Maschinen, Anlagen und Leuchtstoffröhren verursachen Spannungsimpulse im Netzwerk. Eine Leuchtstoffröhre, die abgeschaltet wird, kann z. B. gespeicherte Energie in Form einer Spannungsspitze von bis zu 3000 V abgeben. Ein Blitzeinschlg in der Nähe einer elektrischen Leitung kann einen Spannungsstoß zwischen 6 – 10 kV erzeugen. Eine Standard-Netzkarte in einem Computer ist für ±12 V ausgelegt. Spannungsspitzen sind normalerweise die Ursache für unerklärliche Computerausfälle oder zeitlich begrenzte Übertragungsstörungen. Sie sind ebenfalls die häufigste Ursache für Störungen. Nur in etwa 10 % aller Fälle sind die Störungen auf Stromanschlussfehler zurückzuführen, d.h. auf langfristig zu niedrige oder zu hohe Spannung oder auf Stromausfall.

Schutz gegen Überspannungen und Gewitter

Da Überspannungen und Blitzeinschläge Datenübertragungseinrichtungen beschädigen können, werden wir häufig nach dem effektivsten Schutz gefragt.

Ein völliger Schutz vor Blitzschlägen ist extrem schwierig, aber viele Probleme können durch entsprechende Schutzmaßnahmen vermieden werden. Bei der Diskussion von Blitzschutz müssen zwei Bereiche betrachtet werden, direkte Einschläge und erzeugte Überspannungen.

Der Schutz vor direkten Einschlägen erfordert die Möglichkeit, mehrere hunderttausend Ampère abzuleiten. Einfacher ist es, sich gegen erzeugte Spannungsstöße zu schützen, da diese keine so schnelle Übertragungsgeschwindigkeit haben und der dabei abzuleitende Strom bei weitem nicht so hoch ist. Induzierte Überspannungen werden, wie der Name bereits sagt, durch Induktion übertragen, d.h. es ist kein Kontakt mit dem Blitz notwendig. Diese Spannungsstöße sind die häufigsten, da sie im Zusammenhang mit jedem Blitzschlag auftreten.



Beispiele für Überspannungsschutz

Schnittstelle (Interface)	Spannungsbereich
RS-232	12 V
RS-422/RS-485	12 V
W1	24 V
4-20 mA	24 V
Standleitung Telefonmodem	24 V
Telefonmodem angewählt	170 V

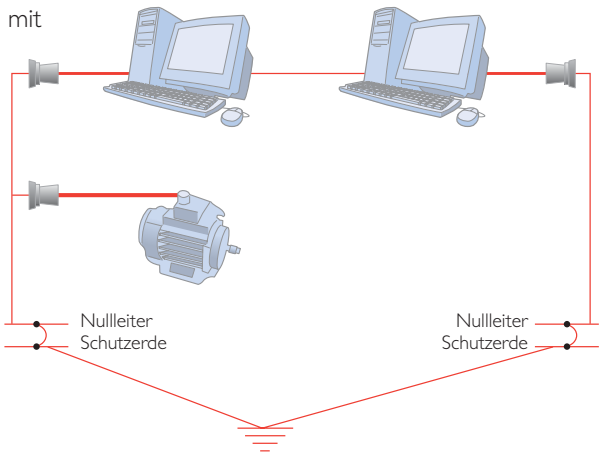
Eine Vielzahl von Schutzeinrichtungen gegen Spannungsstöße in Signal-/Telefonleitungen sind auf dem Markt erhältlich, ebenso für Telefon-Modems, RS-232, 4–20 mA, RS-485 und weitere typische Signaleinrichtungen. Der Schutz besteht aus Primärschutz und Sekundärschutz, wobei der Sekundärschutz an die Übertragungsmethode angepasst ist. Der Schutz ist normalerweise wartungsfrei, nachdem ein Spannungsstoß verarbeitet wurde, kehrt die Schutzeinrichtung in ihre Ausgangsposition zurück. Ist das nicht der Fall, hat der Spannungsschutz normalerweise aus einem der folgenden Gründe versagt:

- Die Energie der Spannungsspitze war größer, als die Kapazität des Schutzes verarbeiten konnte (da der Blitzeinschlag sehr nah an der Installation erfolgte).
- Schäden durch dauernde Überspannung, z. B. durch einen Direktanschluss an 230 V.

Erdschleifen

Eine weitere verbreitete Ursache für Datenübertragungsfehler sind unterschiedliche Erdungspotentiale oder *Erdschleifen*. Dies ist besonders der Fall, wenn Netzwerk-Einrichtungen von unterschiedlichen Stromverteilern mit gegenüber Erde unterschiedlichem Erdungspotential versorgt werden. Jedem Kriechstrom stehen zwei Wege zur Masse zur Verfügung, entweder der korrekte Weg über die Erdung des Stromanschlusses oder über die Signalmasse des seriellen Ports zur Erdung an einem anderen Stromanschluss. Erdungsströme, die im Netzwerk fließen, können ebenso Störungen verursachen wie die Schaltkreise beschädigen, die die Leitungen mit Strom versorgen. Ein Datenübertragungsnetzwerk besteht aus vielen Metern von physischen Leitungen. Häufig sind diese gemeinsam mit Elektrizitäts- und Telefonleitungen verlegt. Jede stromführende Leitung erzeugt ein elektromagnetisches Feld, das anliegende oder kreuzende Leitungen beeinflusst. Gemeinsam bilden sie lange *Antennen,* die unterschiedliche Störpotentiale einfangen können. Es gibt Empfehlungen, wie die Verlegung unterschiedlicher Leitungstypen erfolgen muss, um elektromagnetische Interferenzen zu minimieren. Die einfachste Lösung, um Probleme mit Spannungsspitzen und unterschiedlichen Erdungspotentialen zu vermeiden, ist der Einsatz eines Modems mit *galvanischer Trennung,* das Leitungen und Geräte voneinander elektrisch trennt, aber die Signale nicht beeinflusst. Dadurch wird verhindert, dass Spannungsspitzen, Blitzschläge und Erdungsströme die Geräte erreichen.

Im unteren Beispiel können die Erdungsströme den falschen Weg über die Signalmasse des Computer-Netzwerkes zu einer Sicherungstafel nehmen und damit Störungen verursachen

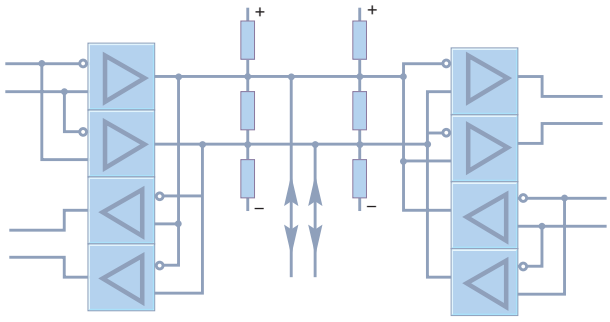


Reduzierung von Störeinflüssen

Elektronische Signale sind in jedem System Störeinflüssen ausgesetzt. Analoge Signale sind dafür anfälliger, da alle Punkte des Signals Dateninformationen übertragen, d.h. Amplitude und Frequenz. Geringe Störungen des Signals lassen den Empfänger das Signal unterschiedlich interpretieren als es ursprünglich ausgesendet wurde und verfälschen die Ausgabe. Digitale Signale sind für Störungen weniger anfällig, da es nur zwei Basiszustände gibt, hoch oder niedrig. Trotzdem kann durch das Zusammenwirken von Kapazität, Widerstand und Induktivität der Leitungen, die das digitale Signal übertragen sowie durch äußere Geräusche die vom Signal übertragene Information so verändert werden, dass das Signal nicht mehr erkennbar ist.

Abgeglichene Signale

Abgeglichene Signale werden für die Übertragung von Impulssignalen über große Entfernungen mit Differential-Schnittstellen wie RS-422/485 oder W1 verwendet.



Schnelle abgeglichene Kommunikation

Wenn bei paarverseilten Vierdrahtleitungen abgeglichene Protokolle eingesetzt werden, löscht sich der Austausch zwischen den Paaren durch die entgegengesetzten induzierten Felder des Stromflusses aus.
Nicht abgeglichene Systeme haben diesen Effekt nicht.

Isolation

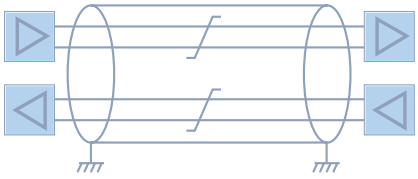
Um Übertragungsstörungen und Schäden an der Anlage durch Spannungsspitzen und andere Störungen zu vermeiden, ist es bei sämtlichen Datenübertragungen wichtig, Geräte und Netzwerk voneinander galvanisch zu trennen.

Für die Isolierung von Relais, Tranformatoren, Verstärkern und Optokopplern stehen verschiedene Methoden zur Verfügung. Ankommende Spannungsspitzen können auch durch Schutzeinrichtungen wie Varistoren, Kondensatoren, RC-Filter und Zener-Dioden beseitigt werden.

Westermo verwendet in seinen Empfängern Optokoppler für die Isolierung. Optokoppler bieten eine bessere Leistung als zum Beispiel Differential-Verstärker. Transformatoren bieten eine Isolierung an der Stromquelle und Varistoren und Zener-Dioden werden dazu eingesetzt, Spannungsspitzen zu unterdrücken.

Geerdete Netzwerke

Die beste Methode, Störungen in einem System zu minimieren, ist eine Auslegung mit Potentialausgleich. Dies bedeutet, dass Gebäude, Elektronikeinrichtungen, Feldbusse und Feldanlagen alle das gleiche Erdungspotential besitzen. In der Praxis ist das sehr schwer zu erreichen, hilfreich für ein gleichmäßiges Potential sind spezielle Erdleiter und geerdete Leitungsnetzwerke. Dabei ist es wichtig, dass das geerdete Leitungsnetzwerk und die Schutzerdung miteinander verbunden sind und so nah beieinander wie möglich liegen.

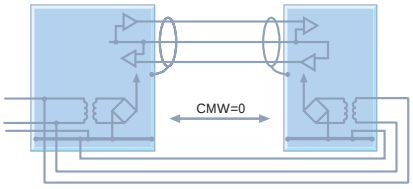


Datenübertragung an RS-422 für 10 Mbit

Abschirmung

Um die Resistenz gegen äußere Einflüsse zu erhöhen, können abgeschirmte oder auch doppelt abgeschirmte Leitungen verwendet werden. Unter normalen Bedingungen sollte die Leitungsabschirmung nur an einem Ende geerdet sein.

Unter einigen extremen Bedingungen, bei denen hochfrequente Geräusche problematisch sind, kann die Leitung auch an beiden Enden geerdet werden. Diese Methode zieht möglicherweise ein größeres Problem nach sich, falls an den Enden ein Potentialunterschied besteht. Sollte dies der Fall sein, fließt ein Strom durch die Abschirmung der Kabel und leitet die Geräusche auf dem Erdleiter weiter.



Datenübertragung an RS-232/V.24

Alternativ kann manchmal eine Seite der Abschirmung an Erde angeschlossen werden und die andere Seite über einen kleinen Hochspannungskondensator geerdet werden.

Kurze Verbindungen ohne Modem

Direkte Datenübertragung mit RS232/V.24 ohne Modem ist nur über sehr kurze Entfernungen möglich. Die Leitungen müssen von anderen Leitungen getrennt verlegt werden, trotzdem aber so nah wie möglich am Erdkabel liegen. Die Anlagengehäuse sollten ebenfalls durch Kupferkabel miteinander verbunden werden, um Geräuschprobleme durch CMV (**C**ommon **M**ode **V**oltages) zu vermeiden. RS-232/V.24 bietet eine langsame Übertragung über einen Entfernungsbereich von bis zu 15 m. Für Distanzen über 15 m sollte ein Leitungstreiber oder ein Modem eingesetzt werden.

RS-422 bietet einen besseren Schutz, da ebenso der Sender wie der Empfänger abgeglichen sind. Abgeschirmte paarverseilte Vierdrahtleitungen können eingesetzt werden und die Anlagengehäuse müssen miteinander verbunden und möglichst von der gleichen Stromquelle gespeist werden, falls sie separat aufgestellt sind.

Telefon-Modems und Störeinflüsse

Beim Einsatz von Telefon-Modems in der Industrie muss beachtet werden, dass sie trotz Isolierung und Verwendung von Signalcodes besonders sensibel auf Störungen reagieren. Falls die Leitungen nicht sorgfältig geschützt werden, können die Übertragung gestört werden und Komponenten fehlerhaft arbeiten. Die Verkabelung von Telefonanlagen muss von der Anlagenverkabelung getrennt verlegt werden. Unter besonders ungünstigen Industriebedingungen können kombinierte Schutzeinrichtungen für einen gesteigerten Schutz sorgen.

Glasfaserkabel

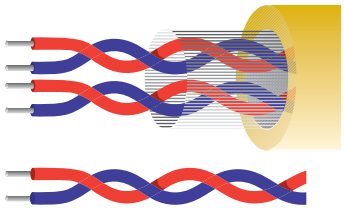
Datenübertragungen über Glasfaserkabel sind in diesem Zusammenhang völlig unempfindlich gegen elektrische Störeinflüsse. Trotzdem können Störungen durch den Kabeltyp und durch Dämpfung an der Verbindungsstelle verursacht werden.

Arten von Kupferkabeln

Die physische Leitung ist häufig die Schwachstelle in der Datenübertragung. Es ist die Leitung, die das störempfindliche Analogsignal überträgt. Und es ist die Leitung, die durch Auslegung, Installation und Länge in Verbindung mit den elektrischen Umgebungseinflüssen, die Übertragungsrate und -qualität bestimmt.

Paarverseilte Drahtleitungen

Die paarverseilte Leitung ist die einfachste, billigste und verbreiteteste Leitung. Normalerweise ist es eine vieradrige paarverseilte Leitung. Es handelt sich um einen Standard-Kupferdraht mit Kunststoffumhüllung, mit oder ohne Metallabschirmung. Es sind verschiedene Marken und Typen erhältlich, mit unterschiedlichen Eigenschaften, die bei der Installation zu berücksichtigen sind. Es werden unterschiedliche Isolationsmaterialien eingesetzt, die den verschieden Installationsbedingungen angepasst sind. Drei wichtige Eigenschaften beeinflussen die Übertragungsqualität: Widerstand, Kapazität und Dämpfung.



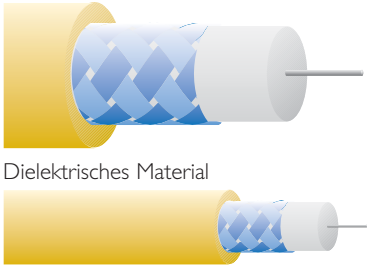
Widerstand bezeichnet den elektrischen Widerstand der Leitung. Er wird in ohm/km gemessen und variiert mit Leitungsmaterial und Querschnitt. Der Widerstand des Kabels ist für jede Leitung dem Datenblatt zu entnehmen. Für Leitungen mit einer einzigen Ader sollte der Querschnitt nicht unter 0,26 mm^2 liegen und für mehradrige Leitungen nicht unter 0,2 mm^2. Bei einer niedrigen Übertragungsrate ist es der Widerstand, der die Grenzen setzt.

Kapazität da die Leiter im Kabel voneinander isoliert sind, erzeugen sie untereinander einen Kapazitätseffekt. Die Paarverseilung, das Leitermaterial und eventuelle Abschirmungen haben ebenfalls Auswirkungen. Die Kapazität dämpft das Signal unterschiedlich bei verschiedenen Frequenzen und der Wert wird normalerweise bei 800 Hz angegeben. Die Kapazität wird in pF/m und ein Richtwert für ein gutes Datenübertragungskabel ist etwa 50–70 pF/m. Bei hohen Übertragungsraten ist es die Kapazität, die die Grenzen setzt.

Dämpfung bezeichnet die gesamte Dämpfungswirkung des Kabels auf das Signal vom Sender zum Empfänger. Kabeldämpfung wird in dB/km angegeben und verstärkt sich mit steigender Frequenz. Eine Steigerung der Dämpfung von 3 dB bedeutet eine Halbierung der Leistung.

Dämpfung (Beispiele)

150 kHz	8 dB/km
1 MHz	20 dB/km
4 MHz	40 dB/km
10 MHz	65 dB/km
16 MHz	82 dB/km
25 MHz	105 dB/km



Koaxialkabel

Koaxialkabel bestehen aus einem einzigen Kupferleiter, der von einer Abschirmung umgeben ist. Um den Abstand konstant zu halten, wird der Zwischenraum von einer isolierenden dielektrischen Kunststoffschicht ausgefüllt. Die Abschirmung dient dem Schutz und wird für das Bestätigungssignal verwendet. Koaxialkabel besitzen hervorragende elektrische Eigenschaften und sind für Kommunikationen mit einer hohen Übertragungsrate geeignet. Ursprünglich arbeitete das Ethernet nur mit Koaxialkabeln, und zwar mit zwei Ausführungen, einer stärkeren (10Base5) und einer leichteren (10Base2). Heutzutage verwendet das Ethernet verstärkt eine spezielle paarverseilte Vierdrahtleitung (10BaseT). Koaxialkabel bieten den Vorteil Breitbandkabel zu sein, d.h. es kann auf mehreren Kanälen gleichzeitig gesendet werden (z. B. Kabel-TV).

Entfernung und Auslegung

Es ist nicht immer einfach, Brücken für die Datenübertragung zu schlagen. Es müssen nicht nur unterschiedliche Orte mit einem Übertragungsmedium verbunden werden, sondern das Medium muss auch so ausgelegt sein, dass es den momentanen und zukünftigen Datenverkehr bewältigen kann. Es muss in der Lage sein, bestimmte Übertragungsgeschwindigkeiten effektiv zu bewältigen, darf nur wenig Wartungsaufwand erfordern und es muss den Umweltbedingungen standhalten.

Da es sich hierbei immer um die passende Lösung einer bestimmten Anwendung unter ganz besonderen Bedingungen handelt, kann es niemals eine Universallösung geben, die für alle Fälle passt. Der beste Ansatz, eine optimale Lösung zu erreichen, ist die Diskussion unterschiedlicher Alternativen mit einem oder mehreren Experten.

Übertragungsentfernung bei unterschiedlichen Kabelarten und Datenübertragungsraten

Das folgende Diagramm zeigt die Übertragungsentfernung, die mit unterschiedlichen Kabelarten und Übertragungsraten erreicht werden kann. Die Linien mit den Farben schwarz, blau und grün zeigen eine paarverseilte Leitung mit 0,3 mm^2 und 42 pF/m. Da Qualität und Abmessungen von Telefonleitungen unterschiedlich sind, zeigen wir ein Kabel des schwedischen Telefonnetzes mit einem Querschnitt von 0,2 mm^2 und einer Dämpfung von etwa 1,1 dB/km.

Widerstandsberechnung

Falls der Widerstand eines Kabels nicht bekannt ist, kann mit folgender Formel gearbeitet werden:

Q = R x A/l

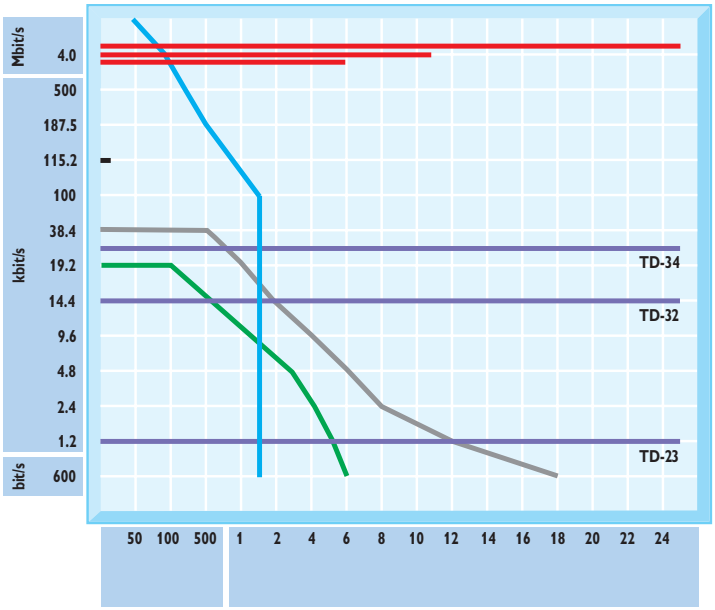
Wobei Q = spezifischer Widerstand des verwendeten Materials ist. Für Kupfer gilt der Wert 0,017 µ Ωm, oder 0,017 x 10^{-6}. R = Widerstand im Kabel, A = Kabelquerschnitt und l = Länge.

Die Formel kann einfach bei Leitungen mit einer Ader angewendet werden. Bei mehreren Adern muss der Querschnitt einer Leitung mit der Anzahl der Leitungen multipliziert werden.

Querschnitt = Radius x Radius x pi.

Zwei Symbole für Kapazität

Es gibt zwei unterschiedliche Bezeichnungen, nF/km oder pF/m, die beide die gleiche Einheit bezeichnen. nF steht für Nanofarad, d.h. 10^{-9} Farad pro 1000 Meter. pF steht für Picofarad, d.h. 10^{-12} Farad pro Meter.



- Telefon-Standleitung
- 10 mA symmetrische Stromschleife (W1)
- Glasfaserkabel
- RS-422/485
- 20 mA Stromschleife
- RS-232/V.24

Anmerkung: Sämtliche Geschwindigkeiten und Entfernungen basieren auf Berechnungen mit Standardwerten der Kabel für Widerstand und Impedanz. Bei Außeninstallationen kann die Übertragungsdistanz je nach Leitungsqualität und örtlichen Umweltbedingungen variieren.

Farbkodierung

DIN 47100 für LiYY und LiYCY Datenkabel Leiter-Nr. und Farbe:

1	□	31	■■
2	■	32	■■
3	■	33	■■
4	■	34	■■
5	■	35	■■
6	■	36	■■
7	■	37	■■
8	■	38	■■
9	■	39	■■
10	■	40	■■
11	■■	41	■■
12	■■	42	■■
13	□■	43	■■
14	■■	44	■■
15	□■	45	□■■
16	■■	46	■■■
17	□■	47	■■■
18	■■	48	■■■
19	□■	49	□■■
20	■■	50	■■■
21	□■	51	□■■
22	■■	52	■■■
23	□■	53	□■■
24	■■	54	■■■
25	□■	55	□■■
26	■■	56	■■■
27	■■	57	□■■
28	■■	58	■■■
29	■■	59	□■■
30	■■	60	■■■
		61	■□

Kabelkodierung

Der schwedische Standard for Kabelmarkierungen heißt SEN 241701 und ein weiterer internationaler Standard ist CENELEC. Das Kabel wird mit zwei bis fünf Buchstaben bezeichnet, sie stehen für:

Leiter — E D C K P — *Sonstiges*

Isolierung — *Hülle* — *Eigenschaften*

1. Buchstabe
A *Kupfer, einadrig*
B *Kupfer, mehrere Leiter*
K *Koaxialleiter*
M *Kupfer, mehradrig*
R *Kupfer, extra mehradrig*
S *Kupfer, feinadrig*
T *Kupfer, extra feinadrig*

2. Buchstabe
D *Gummi, äußerer Gummischlauch*
E *Ethylen-Propylen-Gummi*
F *Fluorcarbon-Gummi*
H *Silikon-Gummi*
I *Polyurethan*
K *PVC*
L*Polythen Kunststoff*
M *Polypropylen Kunststoff*
N *Polyamid*
T *Polytetrafluor-Ethylen (PTFE)*
U *Zellularer Polythen Kunststoff*
V *Gummi, ohne Gummi-außenschlauch*

2. und 3. Buchstaben
O *Öl- und wetterbeständiger Gummi (Chloropren-Gummi)*
S *Chlorsulphaniertem Polyethylen*

3. Buchstabe
C *Runder Kupferleiter*
H *Hitzebeständiger Webstoff*
I *Polyurethan*
J *mit Stahlband armiert*
K *PVC-Hülle mit rundem Querschnitt*
L *Polythen Kunststoff*
N *Polyamid*
T *mit galvanisiertem Stahldraht armiert*
U *ohne Abdeckung*
V *Gummi*
Y *mit einfacher Isolierung und Hülle*

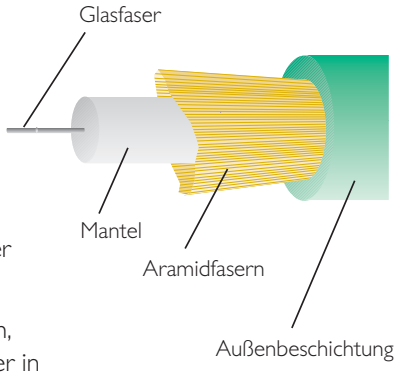
3. und 4. Buchstaben
A *Abschirmung mit Aluminiumband*
F *metallabgeschirmte s Kabel*
P *mit galvanisiertem Stahldraht armiert*

4. Buchstabe
B *Anschluss oder Kabel für Fahrzeuge*
D *Hülle mit eingearbeiteter Verstärkung und losen Leitern*
H *isolierte Leiter, Kabel um Verstärkung*
K *PVC-Hülle*
L *PE-Hülle*
N *PA-Hülle*
O *Öl- und wetterbeständige Gummihülle (Chloropren-Gummi)*
T *starke Anschlussleitung*
V *Kabel für Unterwasser-Verlegung*

5. Buchstabe
H *separat abgeschirmte Leiter*
K *PVC-Hülle*
L *PE-Hülle*
N *PA-Hülle*
P *separat umhüllte Leiterpaare*

4. und 5. Buchstabe
C *Kabel mit in der Hülle integrierter Verstärkung*
E *verstärkte Ausführung*
J *Kabel für Bodenverlegung oder Stahlbandarmierung mit Metall-beschichtung*
R *Steuer- oder Signalkabel*
X *PSTN-Leitung*
Y *wetterbeständige PSTN-Leitung*

Glasfaser-Datenübertragung

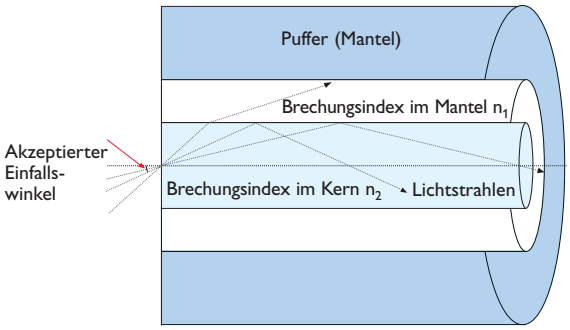


Der größte Vorteil der Glasfaserkabel liegt in ihrer völligen Unempfindlichkeit gegen elektrische und magnetische Störungen. Sie sind daher ideal für besonders ungünstige Industriebedingungen geeignet. Sie bieten eine zuverlässige Übertragung mit einer hohen Datenübertragungskapazität. Glasfaserkabel können in besonders sensiblen Bereichen des Netzwerks eingesetzt werden und z. B. gemeinsam über ein Modem mit vieradrigen Leitungen kombiniert werden. Die Investitionen für ein Glasfaser-Netzwerk sind immer noch etwas höher als für ein Netzwerk mit Kupferleitungen, aber es bietet viele Vorteile und der Markt wächst und damit fallen die Preise.

Das Westermo-Angebot an Glasfaserprodukten wandelt elektrische Signale in Licht um, das dann mit einer Leuchtdiode oder einem Laser über einen glasfaseroptischen Sender in das Glasfaserkabel eingeleitet werden. Beim Einsatz eines Lasers können Daten mit größerer Geschwindigkeit über größere Distanzen übertragen werden. Laserdioden sind jedoch teure Komponenten, daher sind Leuchtdioden weit verbreitet im Einsatz. Im Empfänger sitzt eine Photodiode, die die Lichtsignale wieder zurück in elektrische Signale umwandelt.

Glasfaserkabel

Prinzipiell besteht ein Glasfaserkabel aus zwei Glasarten mit unterschiedlichem Brechungsindex. Die Mitte wird Kern genannt und der umhüllende Teil Mantel. Wenn ein Lichtimpuls in das Glasfaserkabel eintritt, wird der Impuls durch das Kabel reflektiert, da die Grenze zwischen den beiden Schichten wie ein Spiegel wirkt, der Einfallswinkel des Lichts darf allerdings nicht zu groß sein. Kern und Mantel des Glasfaserkabels sind von einer Außenhülle umgeben, deren einzige Aufgabe der Schutz vor äußeren Einflüssen ist.



Die Wahl eines Kabels ist abhängig von Faktoren wie:

- Material
- Single- oder Multimode
- Schritt- oder Grad-Index
- Wellenlänge des Senders

Material

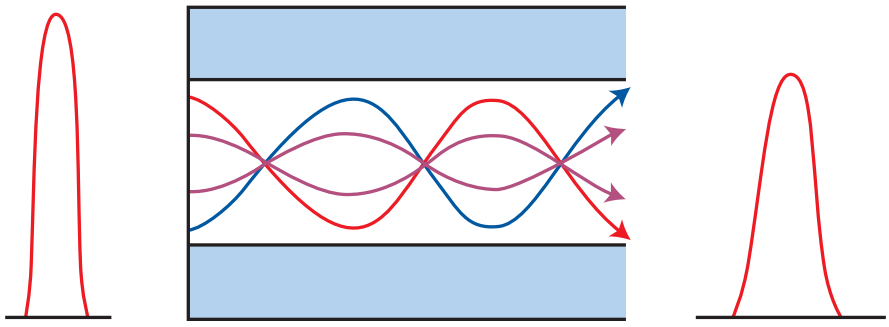
Das für den Kern und den Mantel verwendete Material ist für die verschiedenen Arten von Glasfaserkabeln unterschiedlich. Das am meisten verwendete Material ist Glas. Das verwendete Glas ist extrem reines Silikon-Dioxid-Glas (Silica). Weitere Arten von Kabeln sind PCS (Plastic-Clad Silica) mit einem Kern aus Glas und einem Mantel aus Kunststoff oder ein Kunststoffkabel bei dem Kern und Mantel aus Kunststoff sind.
Glasfaserkabel haben eine höhere bessere Leistungsfähigkeit, die Endanschlüsse sind aber schwieriger herzustellen. Kunststoffkabel sind einfacher anzuschließen, bieten aber eine geringere Leistung.

Dämpfung in Multi-Mode-Kabeln

Eine unterschiedliche Stärke des Kernmaterials kennzeichnet verschiedene Typen von Glasfaserkabeln aus. Es gibt zwei Hauptarten von Kabeln, Multi-Mode- und Single-Mode-Kabel.

Die verbreitetste Kabeldimension für Multi-Mode ist 62,5 µm Kern und 125 µm Mantel (das Kabel wird dann mit 62,5/125 bezeichnet).

Die verbreitetste Kabeldimension für Single-Mode ist 9 µm Kern und 125 µm Mantel (9/125).



Gesendeter Lichtimpuls

Lichtweg in Multi-Mode-Glasfasern (gradierter Index)

Empfangener Lichtimpuls

Multi-Mode

Multi-Mode-Glasfaserkabel haben Dimensionen, die in einem Kern für mehr als einen Modus Platz lassen. Multi-Mode-Kabel sind in zwei Kategorien lieferbar, Graded-index-Glasfasern (fließender Index) und Step-index-Glasfasern (abgestufter Index). Bei Step-index-Glasfasern müssen manche Lichtreflexionen im Kabel einen weiteren Weg zurücklegen als andere und dadurch wird der Lichtimpuls gestreut. Dies ist ein Nachteil und bedeutet, dass das Glasfaserkabel eine geringere Bandbreite hat. Eine Lösung für dieses Problem sind Graded-index-Glasfaserkabel. In diesen Kabeln reduziert sich der Brechungsindex fließend vom Kerninneren zum Mantel. Dies bedeutet, dass ein hauptsächlich im Zentrum des Kabels übertragener Lichtstrahl sich langsamer fortpflanzt als ein Strahl weiter außen. Als Gesamteffekt wird der Lichtimpuls zusammengehalten.

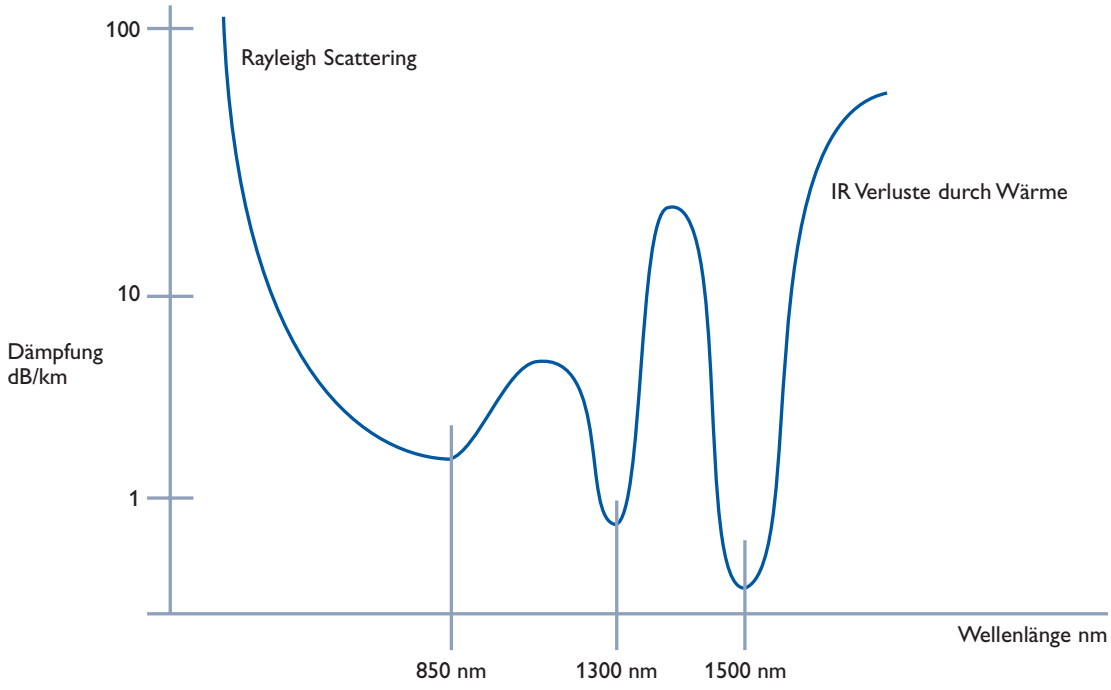
Dämpfung in Single-Mode-Kabeln

Ein Single-Mode-Kabel hat einen so feinen Kern, dass es nur einen Modus unterstützen kann, d.h. dass der übertragene Lichtimpuls bei seinem Weg durch das Kabel nicht beeinträchtigt werden kann.

Wellenlänge

Die Dämpfung in einem Glasfaserkabel ist auch von der Wellenlänge des Lichts abhängig, das der Sender ausstrahlt. Wellenlängen mit geringer Dämpfung sind 820 nm, 1300 nm und 1550 nm. Single-Mode-Glasfasern übertragen nur die höheren Frequenzen effektiv.

Lichtdämpfung in Glasfaserkabeln bei unterschiedlichen Wellenlängen

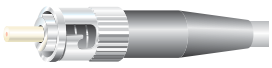


Zusammenfassung der Glasfasertypen

Material	Typ	Kern/Mantel	Dämpfung (dB/km)	Anwendungsbereich
Kunststoff	Multi-Mode Step-index	200-600/450-1000 um	330-1000	Einfache Installation Kurze Entfernungen
Glass (Silikon) Kunststoff-Kern	Multi-Mode Step-index	200-600/350-900 um	4-15	Geringe Kosten, Kurze Entfernungen
Glas	Multi-Mode Step-index	50-400/125-440 um	4-15	Geringe Kosten, Kurze Entfernungen
Glas	Multi-Mode Graded-index	30-100/100-140 um	2-10	Mittlere Kosten, Mittlere Entfernungen
Glas	Single-Mode	3-10/50-125 um	0,4-5	Hohe Kosten Weite Entfernungen

Glasfaser Anschlussstecker

Es gibt viele Arten von Glasfaserstecker für Glasfaserkabel. Die einfachste Art für Glasfasern ist der Anschluss von Multi-Mode-Kabeln. Eine einfache Methode heißt "crimpen und kleben", d.h. der Anschluss wird mit einer speziellen Zange auf die Glasfaser gecrimpt und dann werden die Fasern sorgfältig verklebt. Bei einer zuverlässigeren Methode werden die Glasfasern mit Epoxy in den Anschluss geklebt, es gibt Anschlüsse, die bereits mit Epoxy versehen sind. Mit einem besonderen Ofen wird der Anschluss für etwa 1 Minute erhitzt, das Glasfaserkabel wird in den Anschluss eingeführt und er kühlt wieder ab. Beide Abschlussarten erfordern eine besondere Ausrüstung zur Vorbereitung der Glasfasern vor der Montage des Anschlusses sowie eine Politur der Fasern nach der Fertigstellung. In Systemen, in denen die Anschlüsse häufig gewechselt werden, sind mit Epoxy geklebte Verbindungen besser, da sie haltbarer sind. Es sind viele verschiedene Anschlusstypen für Glasfaser auf dem Markt, es werden aber hauptsächlich nur die folgenden vier Anschlüsse in der Industrie eingesetzt:



ST Simplex-Anschluss für Multi-Mode 2,00 km.

MTRJ Duplex-Anschluss für Multi-Mode 2,00 km oder Single-Mode 15/40 km.

SC Simplex-Anschluss für Multi-Mode 2,00 km oder Single-Mode 15/40 km.

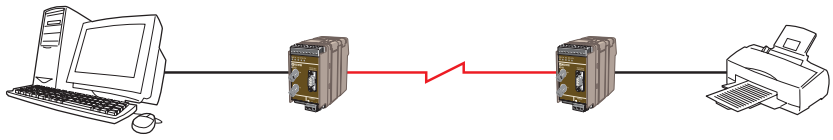
LC Duplex-Anschluss für Single-Mode 15/40/85 km.

Verlustrechnungen

Die Übertragungsreichweite eines Systems hängt von der Sendeleistung und der Empfindlichkeit des Empfängers ab sowie von den Verlusten, die in Kabelverbindungen und Endabschlüssen entstehen. Um diese Verlustwerte zu berechnen, wird ein Wert festgelegt, der dem Unterschied zwischen der gesendeten Ausgangsleistung und der Empfängerempfindlichkeit entspricht, für beide Werte gibt es typische und minimale Größen. Wir haben uns dafür entschieden, für die meisten unserer Produkte beide Werte anzugeben. Der Grund sind die großen Unterschiede in den Herstellerangaben, dies gilt hauptsächlich für Single-Mode-Glasfasern.

Beispiel

Wir verbinden zwei Geräte mit zwei MD-62s. Sollen wir Multi-Mode- oder Single-Mode-Glasfasern verwenden? Multi-Mode-Glasfaserkabel haben eine Dämpfung von 3,2 dB/km bei 820 nm und Single-Mode-Kabel eine Dämpfung von 0,5 dB/km bei 1300 nm. Die Entfernung beträgt in unserem Beispiel 6 km mit zwei Verbindungsspleißen, die jeweils eine Dämpfung von 0,2 dB ergeben.



Option 1, Multi-Mode-Kabel
3,2 dB/km x 6 + 2 x 0,2 dB = 19,6 dB

Option 2, Single-Mode-Kabel
0,5 dB/km x 6 + 2 x 0,2 dB = 3,4 dB

Gemäß dem Handbuch für das MD-62 sollte für Glasfaser der Minimalwert sein:
Multi-Mode-Kabel 62,5/125 bei einer Wellenlänge von 820 nm 14,5 dB
Single-Mode-Kabel 9/125 bei einer Wellenlänge von 1300 nm 6,3 dB

In diesem Beispiel sollte ein Single-Mode-Kabel gewählt werde.
Dies war ein Beispiel dafür, wie mit dem Glasfaserwert die Übertragungsentfernung berechnet wurde, der Glasfaserwert wurde dem Handbuch entnommen.

Das OSI-Modell

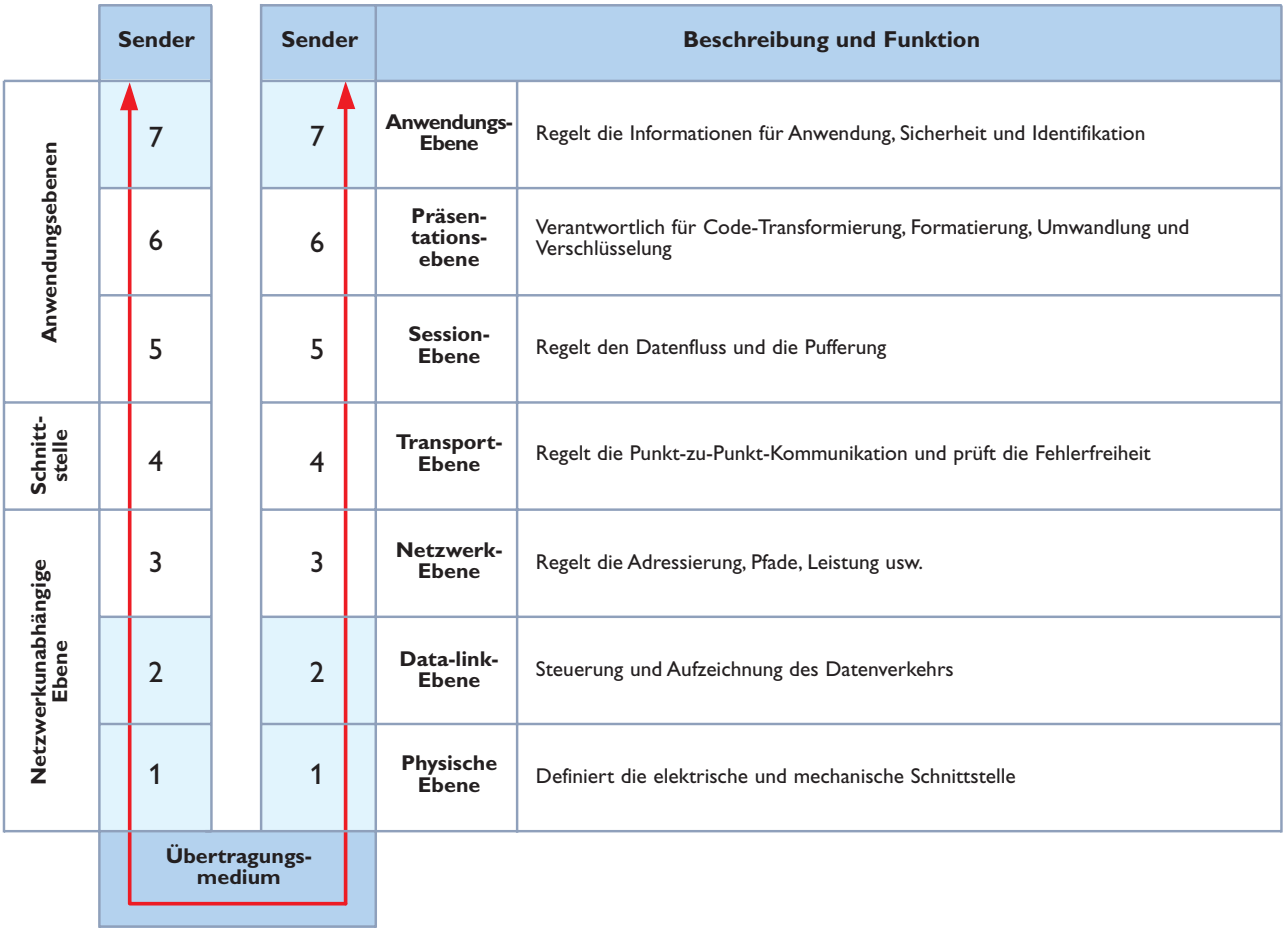
Damit Systeme untereinander kommunizieren können, muss ein strukturierter Rahmen vorhanden sein, der es ermöglicht, Lösungen unterschiedlicher Hersteller gemeinsam zu betreiben. Dies war der Grund zur Schaffung des OSI-Modells (**O**pen **S**ystem **I**nterconnection). Das OSI-Modell wurde von ISO entwickelt und zeigt, wie die Kommunikation zwischen zwei unterschiedlichen Systemen funktionieren kann. Wie der Name schon sagt, war es das Ziel, Systeme offen zu gestalten und damit herstellerunabhängig zu machen. Herstellerspezifische Systeme verhindern es, mit den Anlagen von anderen Herstellern kommunizieren zu können, diese Nachteile werden mit einem standardisierten Protokoll aufgehoben. Es ist zu beachten, dass es sich um ein Modell handelt und nicht um ein Protokoll, sein Zweck ist die Erklärung und Konzeption von flexiblen Netzwerken, die robust und vor allem offen sind.

Struktur des OSI-Modells

1983 hat die **I**nternational **S**tandards **O**rganization (ISO) genau dafür das Modell OSI (**O**pen **S**ystem **I**nterconnection Reference Model) entwickelt. Hier werden sämtliche Komponenten, Strukturen und Funktionen definiert, die für eine Kommunikation notwendig sind und sie werden in 7 Schichten oder Ebenen (layers) geordnet, gemäß den unterschiedlichen Phasen des Kommunikationsprozesses.

Vereinfacht könnte man sagen, dass jede Ebene (ausgenommen die Anwendungsebene) so arbeitet, dass sie mit der angrenzenden Ebene kommunizieren kann. Weitere Informationen, der Header, werden hinzugefügt, um den Austausch zwischen den Ebenen zu ermöglichen. Dies ist notwendig, damit die nächstniedrigere Ebene die Daten interpretieren und verarbeiten kann. Wenn die Daten den Empfänger erreichen, entfernt jede Ebene die hinzugefügten Informationen (Header), die sie benötigt. Die Informationen werden dann zur nächsthöheren Ebene weitergeschickt. Wenn die Informationen zuletzt die oberste Ebene erreichen, sind sämtliche Zusatzinformationen entfernt. Das bedeutet, dass jede Ebene mit der entsprechenden Ebene des anderen Computers kommuniziert.

Beim europäischen V.24-Standard zum Beispiel handelt es sich um eine logische Spezifikation, die durch die physische Ebene definiert wird. Sie definiert nur die Aufgabe der Leitung: Daten und mögliche Übertragungsraten zu steuern. Daher wird der V.24-Standard durch eine elektronische Spezifikation ergänzt, V.28, die ebenfalls einer physischen Ebene zugeordnet ist.



V.24 und V.28 entsprechen dem amerikanischen Standard RS-232, der ebenso die physische wie die elektrische Schnittstelle definiert.

Ein Vergleich

Um ISO etwas klarer zu machen, können wir es mit einem normalen Telefonanruf vergleichen.

- Die physische Ebene ist das Telefon-Netzwerk sowie die Definitionen der übertragenen Signale.
- Die "Logical Link Control" (LLC) der Data-link-Ebene entspricht dem Telefonlautsprecher und —mikrofon. "Media Access Control" (MAC) der Data-link-Ebene entspricht den Telefon-Komponenten, die die Mikrophonsignale so umwandeln, dass das Telefon sie im Netzwerk senden kann und entsprechend umgekehrt für den Lautsprecher.
- Die Netzwerk-Ebene entspricht den Schlüsselimpulsen des Tefefons.
- Die Transport-Ebene entspricht dem Anwählen des anderen Teilnehmers und dem Verbinden, d.h. in der Transport-Ebene wird der Kontakt mit der Gegenstelle hergestellt.
- Die Session-Ebene entspricht dem eigentlichen Anruf.
- Das Gespräch findet seinen Gegenpart in der Präsentationsebene.
- Der Anwendungsebene entspricht das gesamte Telefongespräch.

Lokale Kommunikation

Feldbusse

Heute muss jedes Teil eines modernen Automatisierungssystems kommunikationsfähig sein und universale Informationspfade haben. Die Anforderungen an die Datenkommunikation nehmen beständig zu, sowohl horizontal im Feld als auch vertikal durch weitere Hierarchiestufen. Eine hochintegrierte Datenkommunikationslösung für industrielle Anwendung muss dazu Lösungen bieten. Dies gilt für alle Gebiete: Sensorsignale, Instrumente, Ventile, Motoren u.s.w.. Diese Systemkomponenten kommunizieren mit dem Hauptsteuersystem oder mit industriellen Computern, auf denen eine Anwendung läuft.

Dies ist die Grundlage des Feldbus-Konzeptes, aber was ist ein Feldbus nun wirklich? Ganz einfach könnte man sagen, Feldbusse sind so etwas wie das Internet, aber für die Industrie. Grundsätzlich ermöglichen sie Maschinen und anderen Anlagenkomponenten miteinander in einem Netzwerk verbunden zu werden. Damit wird den Anlagen ermöglicht, Daten miteinander und mit anderen Systemen auszutauschen. Als die Idee Ende der achtziger Jahre auftauchte, war der auslösende Gedanke der Wunsch nach einer verkürzten Installationszeit und kürzeren Kabelverbindungen, mit anderen Worten Kostenreduzierungen. Dieser Aspekt hat über die Jahre an Bedeutung verloren und heute geht es mehr um den Austausch von Informationsdaten. Man könnte sagen, dass der Feldbus von morgen mehr und mehr dem Internet gleichen und eventuell auch auf derselben Technologie basieren wird.

Die internationale Standardisierung der Feldbussysteme ist für ihre Einführung und Akzeptanz absolut notwendig. IEC 61158 ist ein Standard, der Feldbusse beschreibt, der Standard hat den Titel: "Digitale Datenkommunikation für Messungen und Steuerungen, Feldbusse für den Einsatz in industriellen Steuersystemen" und ist in 6 Abschnitte unterteilt.

IEC 61158 Dokument	Inhalt	OSI-Ebenen
61158-1	Einleitung	
61158-2	Spezifikationen und Definitionen des Dienstes	Ebene 1 Physisch
61158-3	Definition des Dienstes	Ebene 2 Data-link
61158-4	Protokoll-Spezifikation	Ebene 2 Data-link
61158-5	Definition des Dienstes	Ebene 7 Anwendung
61158-6	Protokoll-Spezifikation	Ebene 7 Anwendung

Unterschiedliche Feldbusse

In der industriellen Kommunikation wird eine Anzahl unterschiedlicher Medien eingesetzt: Kupferkabel, Glasfaserkabel, Infrarot-Übertragung oder Funktechnik. Die Feldbus-Technologie wurde mit dem Ziel entwickelt, die früheren Systeme durch standardisierte Lösungen zu ersetzen. Im Moment sind durch unterschiedliche Anforderungen, verschiedene Anwendungsbereiche und herstellereigene Lösungen mehrere Bussysteme mit unterschiedlichen Eigenschaften erhältlich, die alle mehr oder weniger offen sind. Ein zusammenfassender Vergleich der verbreitetsten Feldbusse ist unten zu sehen.

Feldbus	Entwickelt von	Standard	Topologie	Medium	Max. Entfernung	Kommunikations-methode
PROFIBUS DP/PA	Siemens	EN 50170/ IEC 1158-2	Bus, Stern, Ring	Paarverseilt oder Glasfaser	100 m bei 12 Mbit/s	Master/Slave Peer-to-Peer
INTERBUS-S	Phoenix Contact, Interbus club	DIN19258 EN 50254	Ring	Paarverseilt oder Glasfaser	400 m/ Segment 128 km total	Master/Slave
DeviceNet	Allen-Bradley ODVA	ISO 11898 ISO 11519	Bus	Paarverseilt	500 m (geschwindigkeitsabhängig)	Master/Slave Multimaster Peer-to-Peer
LonWorks®	Echelon Corp.		Bus, Ring, Schleife, Stern	Paarverseilt oder Glasfaser	2.000 m (2,00 km) @ 78 kbit/s	Master/Slave Peer-to-Peer
CAN open	CAN In. Automation	CiA	Bus	Paarverseilt (geschwindigkeitsabhängig)	25 – 1.000 m (82 – 3283 ft)	Master/Slave Peer-to-Peer Multicast Multimaster
Ethernet Xerox	DEC, Intel,	IEEE 802.3	Bus, Stern oder Glasfaser	Paarverseilt 100 Meter	10/100 Base T	Peer-to-Peer
Modbus Plus	Modicon		Bus	Paarverseilt pro Segment	450 Meter	Peer-to-Peer
Modbus RTU/ASCII	Modicon	EN 1434-3 ICE870-5	Bus	Paarverseilt	1000 Meter	Master/Slave
Data Highway Plus (DH+)	Allen-Bradley		Bus	Paarverseilt	3.000 m	Multimaster Peer-to-Peer

PROFIBUS

PROFIBUS ist ein offenes, universales digitales Kommunikationssystem für einen breiten Anwendungsbereich, besonders im Maschinenbau und der Prozessautomatisierung. PROFIBUS ist ebenso gut für zeitempfindliche Anwendungsbereiche wie für komplexe Kommunikationsanwendungen geeignet. Die PROFIBUS-Kommunikation basiert auf den internationalen Standards IEC 61158 und IEC 61784 und erfüllt damit die Anforderungen von Feldbus-Anwendern an ein offenes und herstellerunabhängiges System. Die Kommunikation zwischen Produkten unterschiedlicher Hersteller kann ohne Anpassungen oder spezielle Software erfolgen.

Geschichte

Die Geschichte des PROFIBUS reicht bis ins Jahr 1987 zurück, als ein europäisches Konsortium von Unternehmen und Institutionen eine Strategie für einen Feldbus entwickelte. Das Konsortium bestand aus 21 Mitgliedern, Unternehmen, Universitäten, anderen Institutionen und unterschiedlichen öffentliche Einrichtungen. Ziel war die Entwicklung und allgemeine Durchsetzung eines seriellen Feldbusses. Ein wichtiges Zwischenziel war die Standardisierung einer Schnittstelle für die Feldgeräte. Mit der Absicht, einen weit verbreiteten Standard zu setzen, unterstützten die betroffenen Mitglieder von ZVEI (Central Association for the Electrical Industry) ein gemeinsames technisches Konzept für Maschinenbau und Prozessautomatisierung. Ein erster Schritt war die Spezifizierung des komplexen Übertragungsprotokolls PROFIBUS FMS (**F**ieldbus **M**essage **S**pecification), das so ausgelegt wurde, dass es sehr anspruchsvolle Kommunikationsanforderungen erfüllte. Ein weiterer Schritt war 1993 die erste Spezifikation für das einfachere und damit bedeutend schnellere Profibus DP Protokoll,
DP steht für **D**ecentralized **P**eripherals. Dieses Protokoll unterlag fortlaufender Weiterentwicklung und ist jetzt in drei Versionen mit unterschiedlichem Funktionsumfang erhältlich: DP-V0, DP-V1 und DP-V2. DP übergeordnet ist der PROFIBUS PA (**P**rocess **A**utomation), der für spezielle Anforderungen der weiterverarbeitenden Industrie entwickelt wurde. Motion Control ist eine Version für Antriebseinheiten und PROFIsafe ist eine Version für Sicherheitsanwendungen. In diesem Handbuch werden nur Anwendungen für DP beschrieben.

PROFIBUS-Kommunikation

Profibus basiert auf der wahrscheinlich verbreitetsten industriellen Übertragungstechnik RS-485. Er verwendet abgeschirmte paarverseilte Vierdrahtleitungen und kann Übertragungsraten bis zu 12 Mbit/s unterstützen. Die Version RS-485-IS wurde kürzlich als 4-adriges Übertragungsmedium für die Schutzklasse E in explosionsgefährdeten Umgebungen spezifiziert. Die Übertragungstechnik MBP (**M**anchester coded, **B**us **P**owered) wird für Anwendungen in der Prozessautomatisierung eingesetzt, die eine Stromversorgung über den Bus zu Geräten in eigensicheren Bereichen erforderlich machen. Die Übertragung von PROFIBUS-Daten mit Glasfaserkabeln wird für Anwendungen empfohlen, die

Datenübertragungsrate (kbit/s)	Max. Segmentlänge (m)
9.6	1200
19.2	1200
45.45	1200
93.75	1200
187.5	1000
500	400
1500	200
3000	100
6000	100
12000	100

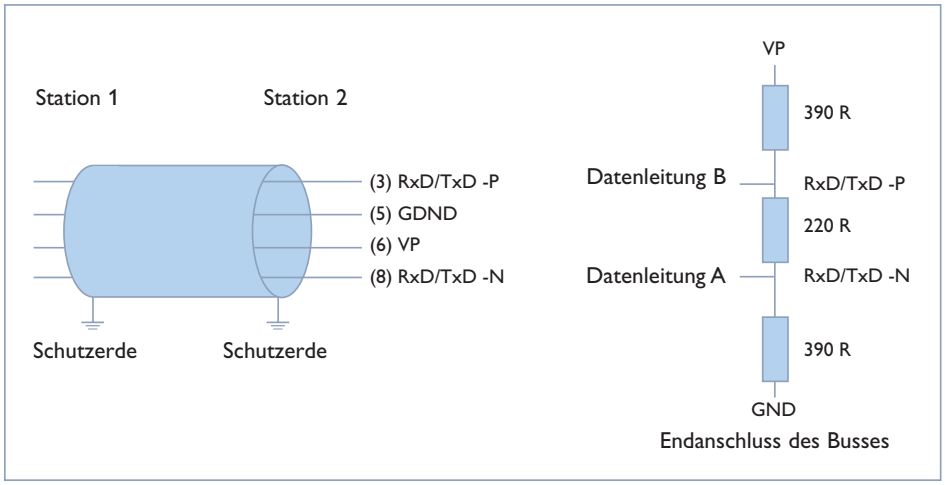
Die Werte beziehen sich auf **Kabeltyp A** mit folgenden Eigenschaften:

Spannungsstöße Impedanz	135–165 Ω
Kapazität	<30 pf/m
Schleifenwiderstand	110 Ω/km
Kerndurchmesser	0,64 mm
Kabelquerschnitt	>0,34 mm²

elektromagnetischen Störfeldern ausgesetzt sind, zwischen Installationen mit unterschiedlichen Erdungspotentialen und um große Entfernungen zu überbrücken.

PROFIBUS Netzwerk-Topologie

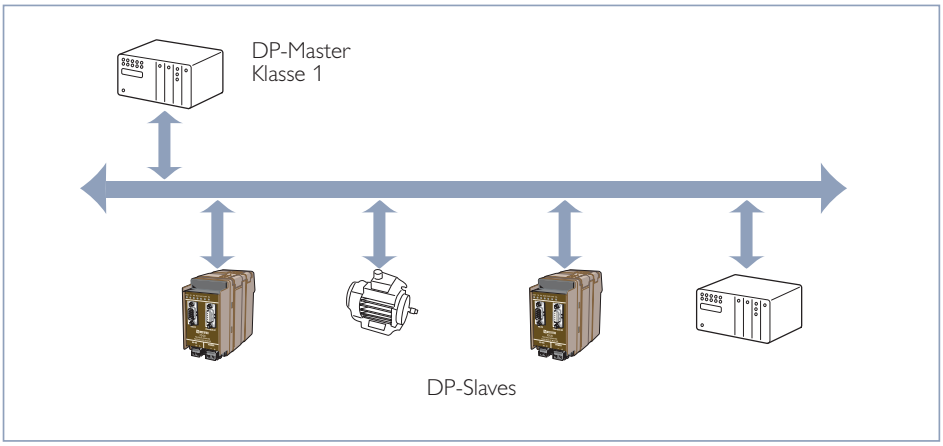
Da die Basisschnittstelle RS-485 ist, sollten die Geräte in einer Busstruktur angeschlossen werden. An ein Segment können bis zu 32 Stationen angeschlossen werden. Wie in der Abbildung unten gezeigt, wird am Beginn und am Ende jedes Segments ein aktiver Busanschluss angebracht. Beide Busanschlüsse müssen über eine permanente Spannungszufuhr verfügen, um eine fehlerfreie Übertragung zu gewährleisten. Die Busanschlüsse sind normalerweise in den Kabelanschluss integriert und werden über einen Switch aktiviert. Ein Repeater wird für den Anschluss von mehr als 32 Stationen an das gleiche Netzwerk eingesetzt oder wenn das Netzwerk größere Übertragungsdistanzen zu bewältigen hat, als in der Tabelle auf Seite 51 angegeben. Es ist zu beachten, dass ein Repeater als elektrische Last im Netzwerk wirkt, so dass mit einem Repeater nur 31 Stationen pro Segment angeschlossen werden können. Bis zu 10 Segmente können in Reihe geschaltet werden, wenn regenerierende Repeater verwendet werden.



PROFIBUS DP

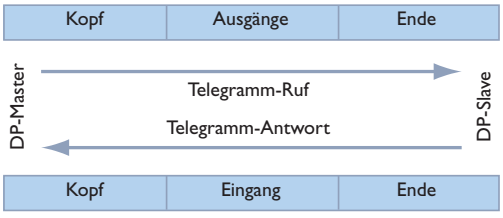
Hierbei handelt es sich um einen grundlegenden, schnellen, zyklischen und determinierend arbeitenden Datenaustausch zwischen einem Bus-Master und seinen zugeordneten Slaves. Die Kommunikation zwischen Master und Slaves wird vom Master reguliert und gesteuert. Der Master ist normalerweise das zentral zu programmierende Steuersystem, PLC oder Industrie-PC.

Master und Slave



Ein Slave ist ein industrielles Gerät (I/O-Terminal, Antriebseinheit, HMI-Station, Ventil, Sender, Analyseinstrument oder ähnlich), das Informationen über den Arbeitsprozess liest und/oder Informationen von außen verarbeitet, um den Prozess zu steuern. Es gibt auch Geräte, die nur Eingangs- oder Ausgangsinformationen verarbeiten, ohne den Prozess zu beeinflussen. Vom Übertragungsstandpunkt aus gesehen, sind Slaves nur passive Systemkomponenten, die auf eine direkte Anfrage reagieren.

Zyklische Datenkommunikation zwischen DPM1 und den Slaves

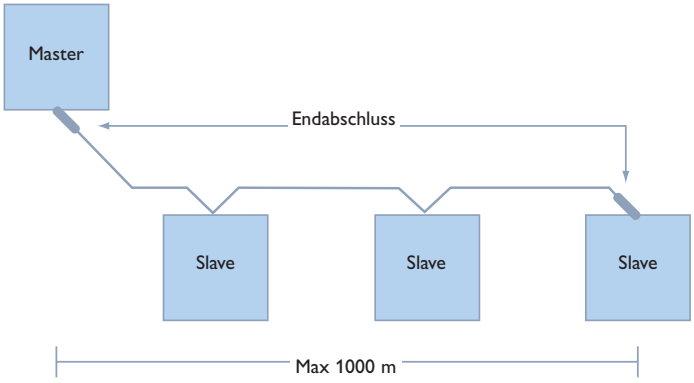


Die Datenübertragung zwischen DPM1 (DP Master Class 1) und seinen zugeordneten Slaves geschieht automatisch gemäß einer definierten wiederholten Sequenz. Der Anwender ordnet bei der Konfiguration des Bussystems die Slaves zu und entscheidet zum gleichen Zeitpunkt, welche Slaves in die zyklische Übertragung eingeschlossen oder nicht eingeschlossen sind.

Modbus

Modbus ASCII und Modbus RTU

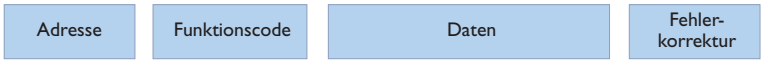
Modbus ASCII und Modbus RTU sind Protokolle, die de facto in vielen Anwendungsbereichen zum Industriestandard wurden. Das Protokoll wurde Ende der siebziger Jahre von Modicon entwickelt. Die Datenübertragung basiert auf Multidrop mit Master und Slaves. Modbus war nicht nur für industrielle Anwendungen vorgesehen. Es wird universell in Situationen eingesetzt, in denen Prozesse oder Informationsflüsse gesteuert werden müssen.



Die an Modbus ASCII und Modbus RTU angeschlossenen Geräte kommunizieren seriell über RS-232 oder RS-485. Der Hauptunterschied zwischen ihnen besteht darin, dass bei RTU jedes 8–bit-Byte einer Nachricht zwei 4–bit-hexadezimal-Zeichen enthält, während bei ASCII jedes 8-bit-Byte der Nachricht als zwei ASCII-Zeichen gesendet wird. Dies bedeutet, dass RTU effizienter ist und mehr Daten übertragen kann, nachteilig ist aber, dass die Datenpakete während der Übertragung nicht aufgeteilt werden können. Modbus ASCII andererseits kann Übertragungslücken tolerieren und wurde damit zum bevorzugten Protokoll moderner Datenübertragung.

Die maximale Übertragungsrate ist normalerweise auf 19,2 kbit/s begrenzt. Die Übertragung wird von einem Master kontrolliert und kann nur halbduplex erfolgen, eine Übertragung zwischen den Slaves ist nicht möglich.

Das Basis-Protokoll für Modbus zwischen einem Master und einem Slave besteht aus:

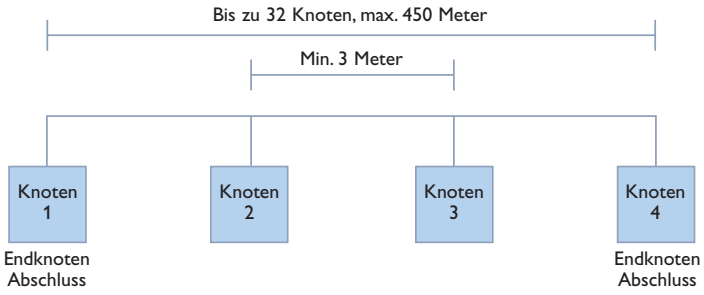


Modbus Plus

Modbus Plus ist ein industrielles Anwendungsnetzwerk, das mit Token Exchange, Peer-to-Peer- Übertragung arbeitet. Token Exchange und Peer-to-Peer arbeitet bei der Datenübertragung mit einem logischen Ring, in dem alle Knoten den Austausch initiieren können, aber ein Knoten kann erst senden, wenn er den Token (Markierung) erhalten hat. Die Übertragungsrate beträgt 1 Mbit/s über abgeschirmte, paarverseilte Vierdrahtleitung. Modbus Plus ist ein offenes Netzwerk für den Informationsaustausch zwischen Netzwerk-Knoten, mit der Möglichkeit, industrielle Prozesse zu steuern und zu überwachen.

Das Netzwerk ist transparent, d.h. es besteht die Möglichkeit, sämtliche Systemgeräte über den Anschlusspunkt zu erreichen.

Die Schnittstelle basiert auf RS-485 und besteht aus Sektionen, wobei pro Sektion bis zu 64 Knoten angeschlossen werden können. Bis zu 32 Knoten können direkt an jedes Leitungssegment angeschlossen werden, die maximale Übertragungsreichweite für ein Segment beträgt 450 Meter. Muss über größere Strecken übertragen werden, kann ein Repeater installiert werden, ebenfalls wenn mehr als 32 Knoten an ein Segment angeschlossen werden sollen. Die maximale Sektionslänge beträgt 1800 Meter, für längere Strecken können Glasfaserkabel eingesetzt werden.

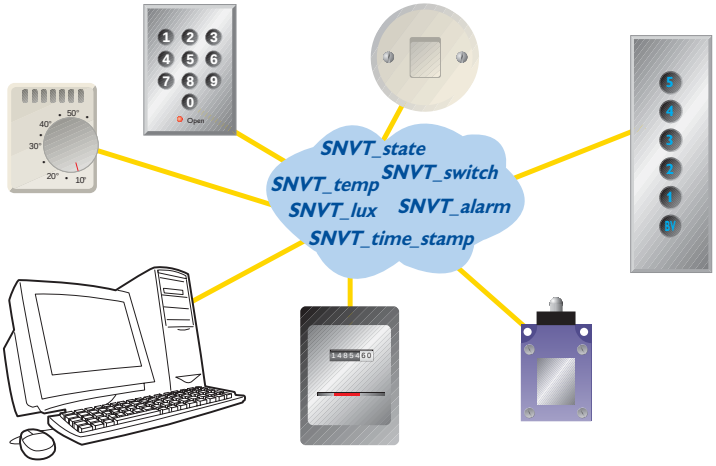


MODBUS/TCP

MODBUS/TCP ist eine Variante von MODBUS, ein unkompliziertes, herstellerunabhängiges Übertragungsprotokoll für Steuerung und Überwachung von automatisierten Anlagen. Das Protokoll arbeitet mit den Eigenschaften des MODBUS, wobei das Übertragungsmedium das TCP/IP-Protokoll ist, das auch in Intranets und dem Internet arbeitet. Es besteht die Möglichkeit, ein Modbus-ASCII- oder Modbus-RTU-Paket in ein TCP- oder UDP-Paket über einen seriellen Server einzubetten, das ist aber nicht das gleiche wie ModbusTCP. Im Modbus TCP kennt jeder Knoten seine IP-Adresse und kommuniziert auf TCP-Port 502.

LON®WORKS

Die Echelon® Corporation bietet mit der LONWORKS®-Technologie eine komplette Plattform zur Entwicklung offener Steuersysteme auf der Basis einer intelligenten Netzwerkarchitektur. Ein LONWORKS®-System besteht normalerweise aus mehreren intelligenten Geräten, auch Knoten genannt, wobei jeder Knotenpunkt für eine spezielle Aufgabe zuständig ist, beispielsweise eine Temperaturmessung oder das Steuern eines Ventils. Die Knoten tauschen untereinander wichtige Informationen über das Netzwerk aus. Ein Steuerungsnetzwerk, das mit dieser intelligenten Lösung arbeitet, wird auch als Peer-to-Peer-Architektur bezeichnet. Die Knoten senden normalerweise keine Befehle zueinander, sondern tauschen Datenpakete mit Informationen, beispielsweise über



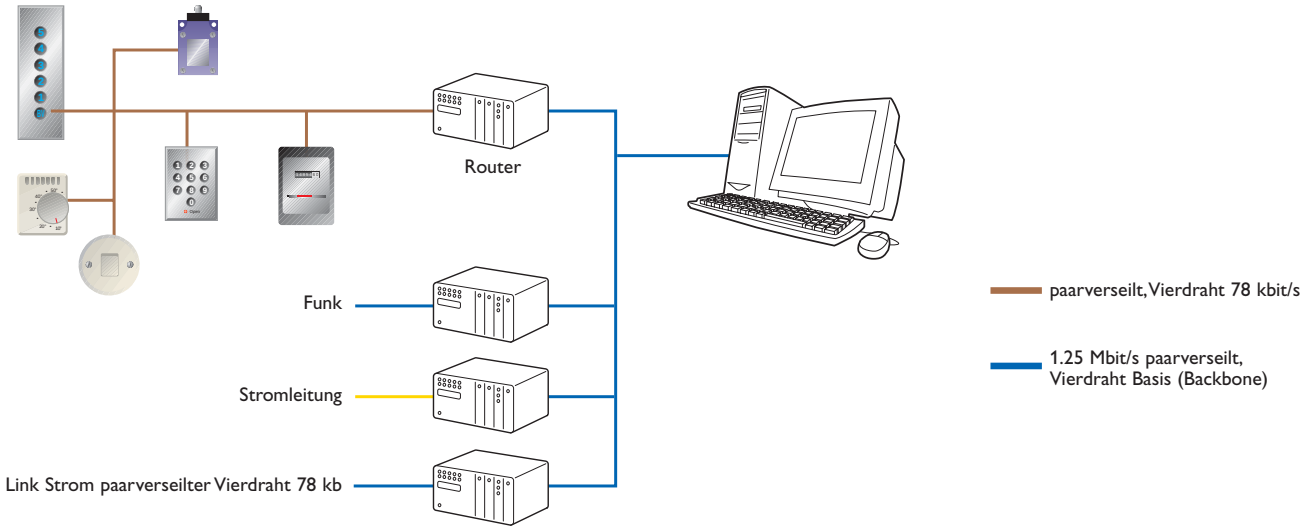
LONWORKS® – ein datenorientiertes Netzwerk

Temperatur, Druck, Status, Datum und Uhrzeit, miteinander aus. Die Knoten können die Informationen in den Datenpaketen dann in verschiedener Weise je nach ihrer speziellen Funktion nutzen. Innerhalb von LONWORKS® können diese Datenpakete als allgemein im Netzwerk verfügbare Variable betrachtet werden und sie erhielten daher die Bezeichnung Netzwerkvariable. Wenn ein Knoten eine Netzwerkvariable aktualisiert, wird diese Information automatisch an das Netzwerk weitergegeben, so dass die anderen Knoten den neuen Wert ebenfalls kennen. Zusammenarbeit ist ein Schlüsselwort der LONWORKS®-Technologie. Eine der Bedingungen für die Zusammenarbeit ist, dass die Knoten verschiedener Hersteller Daten austauschen und verstehen können, ohne dass spezielle Adaptionen der Software oder Hardware nötig sind. Um so arbeiten zu können, reicht es nicht, an das gleiche Netzwerk angeschlossen zu sein, den gleichen Typ von Sender-Empfänger zu nutzen und in der Lage zu sein, die Netzwerkvariablen zu senden. Die

Knoten müssen auch den Inhalt der Netzwerkvariablen verstehen können. Die Knoten müssen zum Beispiel wissen, ob eine Temperaturangabe in Fahrenheit oder Celsius erfolgt oder ob eine Durchflussmenge in Litern/s oder Milliliter/s angegeben wird. Daher sind Standards notwendig, wie der Inhalt dieser Datenpakete zu interpretieren ist. Innerhalb von LonWorks® wird die Standardisierung von einer Organisation bearbeitet, die LonMark® Association heißt. Dies ist eine unabhängige Gesellschaft, in der Hersteller von LonWorks®-Knoten, System-Integrators und Endverbraucher zusammengeschlossen sind. Sie haben eine Typenliste von standardisierten Netzwerkvariablen zusammengestellt. Diese Typen heißen SNVT (ausgesprochen snivit), das für "**S**tandard **N**etwork **V**ariable **T**ypes" steht. Diese Typen enthalten Informationen über das Gerät, die Auflösung und welche Werte der Typ enthalten kann. Wird zum Beispiel der Typ SNVT_speed (Geschwindigkeit) verwendet, wissen alle LonWorks®-Knoten, dass die Einheit Meter/s beträgt, die Auflösung ist 0,1 Meter/s und es kann sich um Werte zwischen 0 und 6553,5 Meter/s handeln.

Der am häufigsten eingesetzte Sender/Empfänger ist der FTT-10A mit freier Topologie. Er überträgt mit einer Rate von 78 kbit/s über eine paarverseilte Vierdrahtleitung. Freie Topologie bedeutet, dass er mit Stern-Netzwerken, Ring-Netzwerken, Bus-Netzwerken oder mit Kombinationen davon arbeiten kann. Echelon® bietet ebenfalls einen Sender/Empfänger mit freier Topologie, LPT-10 LinkPower genannt. Er arbeitet auf dem gleichen Signalniveau wie der FTT-10A und kann gemeinsam mit ihm betrieben werden. Das Besondere am LPT-10 ist, dass es sich um ein "echtes 2-adriges" Gerät handelt, d.h. die Leitung überträgt ebenso die Stromversorgung wie auch die Daten. Der Vorteil dieser Sender/Empfänger mit ihrer freien Wahl der Topologie macht sie in modernen Steuernetzwerken besonders vorteilhaft, in die häufig neue Geräte integriert werden müssen. Ein weiterer Vorteil dieser Sender/Empfänger ist ihr polaritätsneutraler Anschluss, der die Installation erleichtert und das Risiko eines falschen Anschlusses vermeidet. Weitere Sender/Empfänger von Echelon® sind ein Sender/Empfänger mit 1250 kbit/s und Bustechnologie für paarverseilte Vierdrahtleitung und ein Sender/Empfänger für elektrische Netzwerk-Kommunikation. Mit der Möglichkeit zwischen zwei Frequenzbändern zu wechseln sowie einer fortschrittlichen Signalverarbeitung und Fehlerkorrektur bietet der Sender/Empfänger für elektrische Netzwerke eine hervorragende Störunempfindlichkeit gegen Motoren-, Dimmer-, PC- und Fernseheinflüsse.

Der Sender/Empfänger PLT-22 kann entweder so konfiguriert werden, dass er über das Strom-Netzwerk im öffentlichen Cenelec-C-Band kommuniziert oder über das Frequenzband Cenelec-A, das Stromversorgungsunternehmen vorbehalten ist. Das C-Band wird normalerweise für Anwendungen in industriellen und gewerblichen Bereichen eingesetzt, während das A-Band häufig für die Ablesung von elektrischen Zählern genutzt wird. Auf dem Markt sind auch Sender/Empfänger für Glasfaser-, Funk- und IR-Übertragung von Drittanbietern erhältlich. Unterschiedliche Medien werden häufig in einem LonWorks® Netzwerk gemeinsam eingesetzt. Echelon® bietet Router an, die LonTalk®-



Daten auf unterschiedliche Art von einem Medium in das andere übertragen können. Es ist durchaus normal, wenn Kanäle mit einem langsamen Medium an eine Basis mit einem schnelleren Medium angeschlossen werden. Das Ergebnis ist eine logische und physische Trennung des Netzwerks, die eine gesteigerte Leistung bei größerer Sicherheit nach sich zieht.

Hinweise zu großen LonTalk®-Netzwerken

Eine Vergrößerung der Übertragungsdistanz zwischen zwei oder mehr TP/FT-Segmenten mit einem Glasfaser-Kabel resultiert in einer leichten Verzögerung der Übertragung zwischen den verschiedenen Segmenten. Dies verursacht Datenkollisionen, die wiederum ein erneutes Senden des Datenpakets hervorrufen und damit zu einer Leistungseinbuße des Nertzwerkes führen. Daher empfehlen wir, dass die Gesamtlänge des Glasfaserkabels 25 km nicht übersteigt. Gemäß dem Standard EIA-709.3 ist eine maximale Verzögerung von 36 ms zulässig, die eine Übertragungsdistanz von 6,8 km ermöglichen sollte. Wir empfehlen den Einsatz des Router LR-11, um größere Übertragungsentfernungen sicherzustellen, mehrere Netzwerk-Segmente oder mehr Knoten mit 1250 kbit/s. In jedem Fall empfehlen wir, die Datenübertragung mit einem LonWorks®-Protokoll-Analyzer zu analysieren.

Fernverbindungen

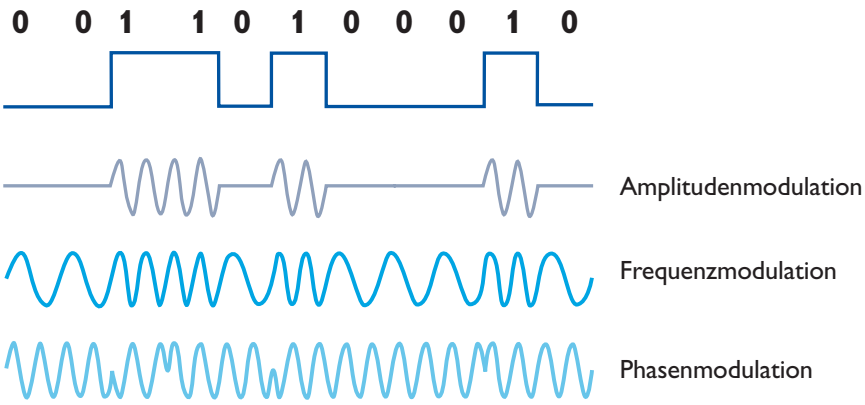
PSTN Wählverbindungen

Datenübertragung über das Telefon-Netzwerk

Datenaustausch über Fernverbindungen ist eine wichtige Ergänzung der lokalen Datenübertragung. Das bedeutet die Möglichkeit, sich mit weit entfernten Datenquellen zu verbinden und dort nach Informationen zum Beispiel über Märkte, Preisangeboten im Aktienhandel oder in öffentlichen Datenbanken zu suchen. Die Anzahl der Datenquellen hat beträchtlich zugenommen und sie sind häufig über globale Netzwerke verbunden. Obwohl die Verbindung mit einer Datenquelle im eigenen Land hergestellt wurde, endet man leicht in einer internationalen Finanzdatenbank in New York. Es gibt viele Gründe Datenfernverbindungen zu schaffen, unter anderem zur Verbindung über eine Telefonleitung mit dem eigenen Computerarbeitsplatz im Unternehmen, wenn man unterwegs ist. Heutzutage sind in einem einzigen tragbaren Gerät bereits Computer, Modem, GSM-Telefon und Fax vereint.

Wählverbindung

Das Prinzip der Fernverbindung über das Telefonnetz basiert auf einem Anruf am Empfängermodem, das antwortet und beide Modems bauen über die Telefonleitung eine Trägerverbindung auf. Der Träger ist ein Signal, auf das das Modem hört. Können beide Modems ihre Trägersignale hören, dann verbinden sie sich oder synchronisieren sich mit dem Signal. Die Übertragungsraten über die Telefonleitung haben sich beständig erhöht und heutzutage sind 2400 – 56000 bit/s die Regel. Es ist nicht nur das Modem, das die Übertragungsraten begrenzt, sondern auch die Telefonleitung. Die Entfernung, die Anzahl der Verbindungen und Relais beeinflussen bedeutend die Leitungsqualität. Die meisten modernen Hochgeschwindigkeitsmodems besitzen die Möglichkeit, sich automatisch anzupassen, um eine gute Übertragungsqualität aufrecht zu erhalten. In der Telefonkommunikation ist es besonders wichtig, Standards einzuhalten, da Sender und Empfänger häufig von unterschiedlichen Herstellern sind. In der Tabelle auf Seite 69 werden die Bitraten der verschiedenen Standards aufgeführt.



Modulation

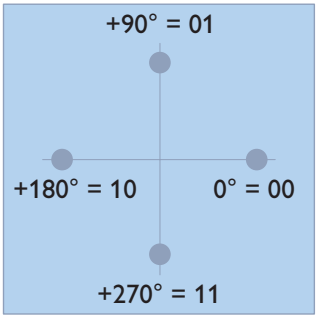
Das Wort Modem ist zusammengesetzt aus dem Wort **Mo**dulation, also Signalumwandlung und **Dem**odulation, das ist die Wiederherstellung des Originalsignals. Damit Datensignale über unterschiedliche Leitungstypen übertragen werden können, müssen sie konvertiert und adaptiert werden. Die digitalen Signalpegel (Einsen und Nullen) werden in für das jeweilige Kabel lesbare Signale transformiert. Es gibt drei Hauptarten von Modulation. Frequenzmodulation, bei der unterschiedliche Frequenzen die Nullen und Einsen repräsentieren. Phasenmodulation, bei der die Phasenunterschiede des Trägers die Nullen und Einsen repräsentieren. Amplitudenmodulation, bei der der Signalpegel oder die Amplitudenspitzen eingesetzt werden, um lesbare Nullen und Einsen darzustellen. Komplexere Modulationsarten entstehen aus Kombinationen der drei Basistypen.

Ist bit/s das gleiche wie Baud?

Die Übertragungsrate eines Telefonmodems wird ebenso in bit/s (Bitrate) und in Baud (Baudrate) angegeben. Daraus ergaben sich Missverständnisse, daher hier eine Erklärung.

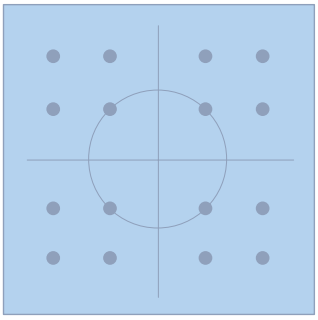
Bitrate = Die Anzahl der über die serielle Schnittstelle übertragenen Bits pro Sekunde; Einheit bit/s

Baudrate = Die Anzahl der über die Leitungsschnittstelle gesendeten Signalkombinationen pro Sekunde; Einheit Baud



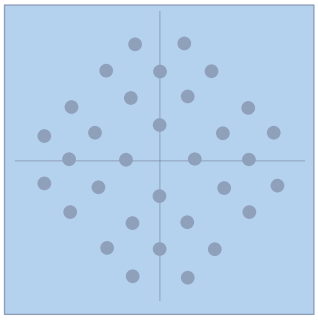
Um die Übertragungsrate eines Telefonmodems zu erhöhen, werden mehr Bits gemeinsam moduliert und über das Telefonnetz übertragen. Im nebenstehenden Beispiel wird die Technik der Phasenmodulation gezeigt, bei der zwei Bits durch die Phasenverschiebung des Leitungssignals definiert werden (V.22).

Im nebenstehenden Beispiel beträgt die Bitrate 1200 bit/s und die Baudrate 600 Baud.



Wenn zusätzliche Signale gemeinsam moduliert werden, erreicht man eine höhere Übertragungsgeschwindigkeit. In einigen Standards, z. B. in V.22bis, werden Amplituden- und die Phasenmodulation kombiniert (auch QAM **Q**uadrature **A**mplitude **M**odulation genannt), dabei werden 4 Bits auf jeder Modulation übertragen.

Im nebenstehenden Beispiel beträgt die Bitrate 9600 bit/s und die Baudrate 2400 Baud.



In Standards wie V.32 wird die Leitung mit einer Technik moduliert, die man TCM (**T**rellis **C**ode **M**odulation) nennt, sie entspricht QAM, aber mit einem zusätzlichen Extrabit für die Fehlerkorrektur. Dies ist erforderlich, da sich der Abstand zwischen den übertragenen Bit-Kombinationen verringert und eine zusätzliche Fehlerkorrektur erfordert.

Im nebenstehenden Beispiel beträgt die Bitrate 9600 bit/s und die Baudrate 2400 Baud.

Einige Standards

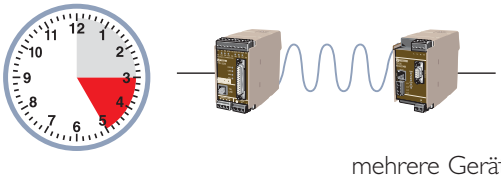
Standard	Bitrate	Halb/Voll	Baudrate	Anz. der bits	Modulation
V.21	300 bit/s	FDX	300 Baud	1 bit/Baud	FSK
V.22	1200 bit/s	FDX	600 Baud	2 bit/Baud	DPSK
V.22bis	2400 bit/s	FDX	600 Baud	4 bit/Baud	QAM
V.23	1200 bit/s	FDX	1200 Baud	1 bit/Baud	FSK
V.32	9600 bit/s	FDX	2400 Baud	4 bit/Baud	TCM
V.32bis	14400 bit/s	FDX	2400 Baud	7 bit/Baud	TCM
V.34	Bis zu 33600 bit/s	FDX	Bis zu 3429 Baud	*)	TCM
V.90	Bis zu 56000 bit/s	FDX FDX	Bis zu 8000 Baud	*)	PCM

*) Die Rate wird während der Quittierung (Handshaking) bestimmt

V.90

V.90 ist ein interessanter Modem-Standard, da mit ihm hohe Datenübertragungsraten möglich sind. Dies erreicht man durch den Einsatz des teilweise digitalen Übertragungsstandards PCM (**P**ulse **C**ode **M**odulation). Dieser Standard wurde besonders für das Einwählen von Nutzern in das Internet entwickelt und er ist daher kein symmetrischer Datenaustausch. Obwohl unter günstigen Bedingungen Download-Geschwindigkeiten von 56.0 kbit/s möglich sind, beträgt die Upload-Geschwindigkeit nur 9600 bit/s. Eine weitere Komplikation ist der Umstand, dass die Internet-Serviceprovider mit speziellen Modems arbeiten müssen, um den V.90-Modems die Einwahl zu ermöglichen. Dies bedeutet, dass zwei verbundene Standard-V.90-Modems nicht mit V.90 verbunden sind, sondern eher mit V.34bis, und damit bieten sie nur eine Verbindung mit 33,6 kbit/s in beiden Richtungen.

Verbindungsaufbau



Beim Aufbau einer Modemverbindung erfolgt ein Handshaking-Prozess (Quittierung)), bei dem Datenübertragungsrate und Fehlerkorrektur aufeinander abgestimmt werden. Die nebenstehende Liste zeigt die Verbindungszeiten von zwei Modems für unterschiedliche Protokolleinstellungen.
Diese Messwerte zeigen, dass die schnellste Datenrate nicht immer die effektivste ist. Die Verbindungszeit ist der entscheidende Faktor, wenn mehrere Geräte angewählt werden und nur geringe Datenmengen zu übertragen sind.

Protokoll	Verbindungs-zeit
V.32 bis fehlerkorrigiert	16 s
V.32 bis	13 s
V.22 bis fehlerkorrigiert	12 s
V.22 bis	7 s
V.23	6 s
V.21	7 s

'Sprache' der Telefonmodems

Um eine Verbindung, einen Computer oder ein Endgerät mit Software zu konfigurieren, die den seriellen Port des Computers nutzt, müssen sie in der Lage sein, mit dem Modem zu kommunizieren. Es sind Anweisungen notwendig, wie das Telefonmodem zu steuern ist. Hayes Microcomputer Products entwickelte einen Befehlssatz, der zum Standard wurde, die Befehle werden Hayes®-Befehle genannt. Dies ist ein Befehlssatz für Telefonmodems, der entweder manuell über die Tastatur von einem Computer gesendet werden kann oder automatisch von einem angeschlossenen Gerät, um die erforderlichen Einstellungen vorzunehmen.

Fehlerkorrektur und Komprimierung

Die meisten Telefonmodems übertragen untereinander synchron, selbst wenn die Verbindung zwischen dem Computer und dem seriellen Port asynchron ist und liefern damit eine einfache Datenkomprimierung. Um die Zuverlässigkeit zu überwachen, können die Daten in Blöcke unterteilt werden, wobei jedem Block eine Prüfsumme (checksum) zugeteilt wird. Bei Übertragungsunterbrechung oder nicht passender Prüfsumme veranlasst der Empfänger das erneute Senden des Blocks. Dieser Prozess wird ARQ (**A**utomatic **R**epeat re**Q**uest) genannt und arbeitet gemäß ITU-T, V.42 mit den beiden bekanntesten Methoden zur Fehlerkorrektur MNP (**M**icrocom **N**etworking **P**rotocol) und LAPM (**L**ink **A**ccess **P**rocedure for **M**odems).

ARQ und MNP

MNP Niveau 1:
Asynchrones Protokoll, halbduplex

MNP Niveau 2:
Asynchrones Protokoll, vollduplex, Daten in Blocks unterteilt. Eigentliche Übertragungsgeschwindigkeit etwas geringer als normal.

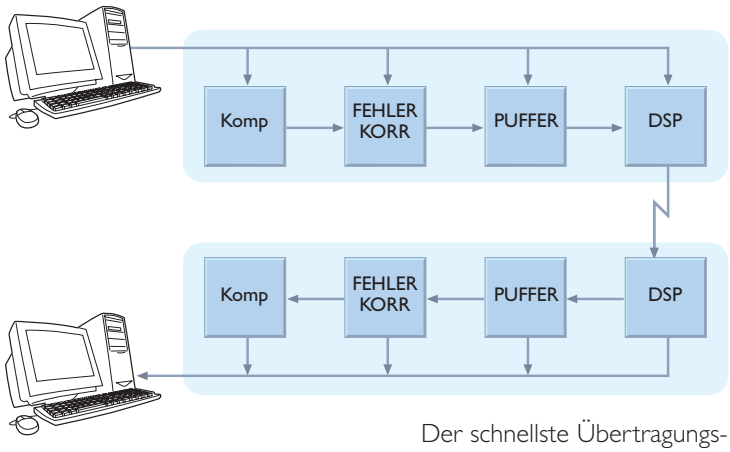
MNP Niveau 3:
Synchrones Protokoll, vollduplex, Daten in Blocks, 10 % höhere Geschwindigkeit mit fehlerfreier Übertragung.

Abfrage und Dateiübertragung

Über eine Telefonmodem-Verbindung kann man, direkt oder indirekt über ein Netzwerk, andere Computer erreichen. In kürzester Zeit hat sich das Internet zum größten weltweiten Netzwerk mit bis zu 250 Millionen Anwendern entwickelt. Auf der Grundlage des TCP/IP-Protokolls bietet das Internet E-mail, Diskussionsgruppen, das World Wide Web (Datenbanken, Informationen und Marketingangebote), das Herunter- und Hochladen von Dateien, Telefonie, Videokonferenzen, Chatangebote usw. Darüber hinaus gibt es weitere Netzwerke und Serviceangebote, die über Modems erreichbar sind, z. B. MEMO, Lotus Notes, Compuserve usw. Das Telefonmodem ermöglicht ebenso die Heimarbeit wie auch die Verbindung der Unternehmenscomputer über mobiles GSM.

Datenautobahn von morgen

Es wird intensiv an der Erstellung internationaler Standards gearbeitet und damit wird eine Entwicklung vorangetrieben, die man allgemein die "Datenautobahnen von morgen" nennt. Das sind schnelle Hochgeschwindigkeitsnetzwerke wie Broadband, die riesige Mengen von Informationen, einschließlich Daten, Audio- und Videosignalen über Kontinente übertragen. Die großen Kapazitäten der Netzwerke für Kabelfernsehen können sich ebenfalls zu einer neuen Quelle für schnelle Datenübertragung entwickeln. Wir sind davon überzeugt, dass auch schnelle Autobahnen in Ihren eigenen vier Wänden beginnen, mit einer hochleistungsfähigen, schnellen lokalen Datenübertragung. Auf dieser wichtigen Infrastruktur können dann Datenverbindungen zu nationalen oder weltweiten Netzwerken aufgebaut werden.



Der schnellste Übertragungsweg ist immer der direkte Modus (Direct Mode). Jede Komprimierungsstufe, Fehlerkorrektur und Pufferung bedeutet eine Zeitverzögerung.

Standleitungen

Hierbei handelt es sich um eine permanent angeschlossene Telefonverbindung, die von einer einer Telefongesellschaft bereitgestellt wird und Punkt-zu-Punkt- oder Multidrop-Verbindungen (V.23) über große Entfernungen ermöglicht. Anders als eine immer wieder neu zu wählende Verbindung, besteht hier eine Standleitung zwischen zwei Punkten. Diese Verbindung kann über Vermittlungsstellen geroutet oder eine direkte Kabelverbindung sein. Selbstverständlich können Telefonmodems mit Standleitungsfunktion auch über Standard-Datenleitungen eingesetzt werden. Eine Vollduplex-Übertragung kann ebenso mit 2-adrigen wie mit 4-adrigen Leitungen erfolgen. Modems von Westermo bieten mehrere Standards bis zu V.90, der Übertragungsraten bis zu 56,0 kbit/s unterstützt. Ein Modem wird als Anwahlmodem konfiguriert und das andere als Antwortmodem, sobald die Verbindung hergestellt ist, können Daten kontinuierlich übertragen werden.

MNP Niveau 4:
Daten in Blocks, Blockgröße entsprechend der Leitungsqualität, Kleinere Blocks als in Niveau 3, daraus resultiert eine um 20 % schnellere Übertragungsrate, wenn frei von Umgebungseinflüssen.

MNP Niveau 5:
Wie in Niveau 4, aber mit Datenkompression, daher bis zu doppelte Geschwindigkeit.

MNP Niveau 10:
Eine Weiterentwicklung von MNP 5, die Leitung wird dynamisch überwacht und garantiert eine fehlerfreie Übertragung.

V.23 bei einer Standleitung

V.23 ist ein alter Standard der ursprünglich für Standleitungen entwickelt wurde. Datenübetragungsraten sind mit 600 und 1200 Baud standardisiert.. Modems für den V.23-Standard bieten mindestens die folgenden Funktionen:

- Modulationsgeschwindigkeiten bis zu 600 oder 1200 Baud
- Frequenzmodulation (FSK)

Zwei unterschiedliche Frequenzmodulationsverfahren werden wie folgt eingesetzt:

- Modus 1: 600 Baud, 1300 Hz–1700 Hz
- Modus 2: 1200 Baud, 1300 Hz–2100 Hz

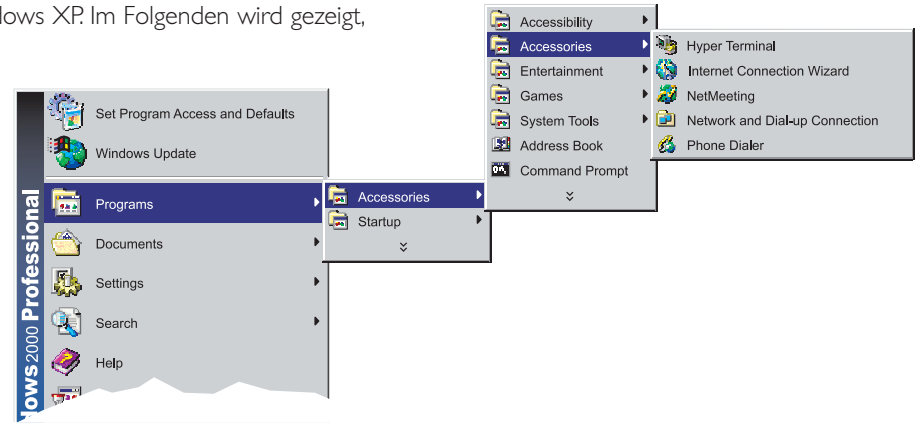
V.23 ermöglicht normalerweise bis zu 6 Anschlusspunkte bei einer 2-adrigen Leitung. Die maximale
Anzahl von Modems an einer Leitung hängt jedoch davon ab, wie die Modems installiert werden, da häufig Impedanzprobleme auftreten. Die Leitungsimpedanz für V.23 sollte 600 Ohm brtragen.

Westermo V.23-Modem

Das Westermo V.23-Modem (TD-23) unterstützt alle Übertragungsgeschwindigkeiten bis zu 1200 Baud. Die Leitung kann als Endabschluss mit einem 600 Ohm Leitungswiderstand ausgestattet werden. Alle Ebenen wie Träger-, Übertragungs- und Empfangsebene sind einstellbar.

Der Einsatz des HyperTerminal

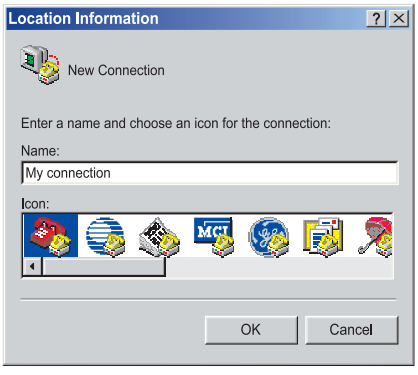
Zur Konfiguration eines Modems ist häufig eine serielle Emulationssoftware notwendig, eine der am meisten eingesetzten Anwendungen ist HyperTerminal in Windows, dieses Beispiel zeigt Windows XP. Im Folgenden wird gezeigt, wie HyperTerminal zur Kommunikation mit einem Modem verwendet wird:

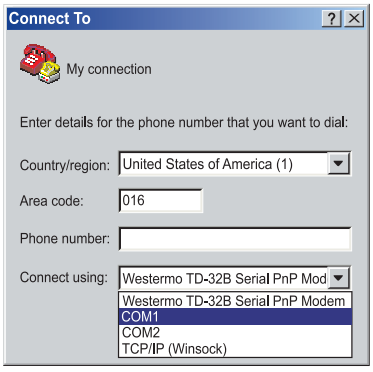


1. Modem mit einem modernen Kabel an den seriellen Anschluss des Computers anschließen, in diesem Beispiel Com 1. Ein direktes 9-pol. Kabel wird verwendet, da der Computer DTE ist und das Modem DCE (siehe Seite 26).

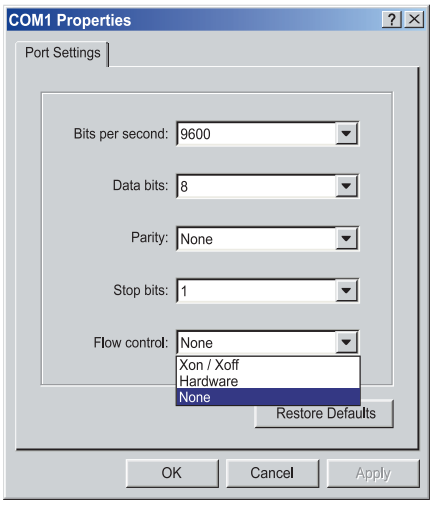
2. HyperTerminal starten, die Anwendung liegt normalerweise unter Zubehör/Kommunikation.

3. Einen Namen für die Verbindung eingeben, z. B. Com 1 9600 8N1 (für Com 19,6 kbit/s 8-Datenbits, Parität keine (N) und 1 Stopbit).





4. Aus der Drop-down-Liste wird der Übertragungsport gewählt, der mit dem Modem verbunden ist.
   - In diesem Beispiel wird COM1 gewählt
   - Wenn COM1 gewählt wird, sind die Felder für Land, Ortsvorwahl und Telefonnummer deaktiviert (gedimmt).
   - Auf OK klicken.

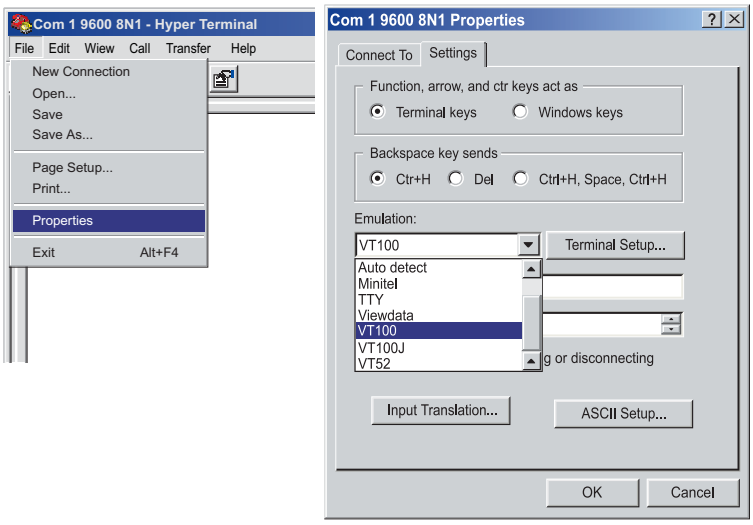


5. Hier werden die Eigenschaften des Übertragungsports eingeben, z.B. Übertragungsrate, Anzahl der Datenbits, Parität, Anzahl der Stopbits und Datenflusssteuerung. In diesem Beispiel werden gewählt:
   - Bits pro Sekunde 9600
   - Datenbits 8
   - Parität Keine (N)
   - Stopbit 1

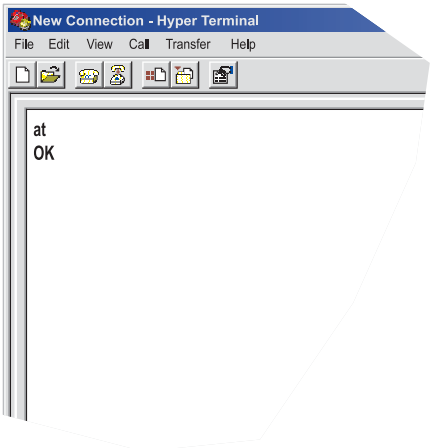
Die Einstellungen für die Datenflusssteuerung geben an, wie das Handshaking zwischen
Modem und PC ausgeführt werden soll.

- Xon/Xoff, wird von der Software gesteuert
- Hardware, bedeutet die Signalgebung mit RTS/CTS
- Kein, bedeutet, dass Handshaking abgeschaltet ist

6. Nachdem diese Einstellungen erfolgt sind, ist HyperTerminal konfiguriert. Weitere Einstellungen können unter Datei/Eigenschaften vorgenommen werden. Hier kann unter anderem gewählt werden, ob unterschiedliche Terminals emuliert werden sollen, z. B. VT100. Mit der Taste für die ASCII-Einstellungen können die Werte für Zeichen, Zeilenabstände und lokales Echo verändert werden.



7. HyperTerminal ist jetzt einsatzbereit, da das Telefonmodem mit AT-Befehlen für die Konfigurierung arbeitet, kann das Bestehen der Verbindung überprüft werden, indem eingegeben wird:
   - AT, gefolgt von <Return>
   - Das Modem muss mit OK antworten.

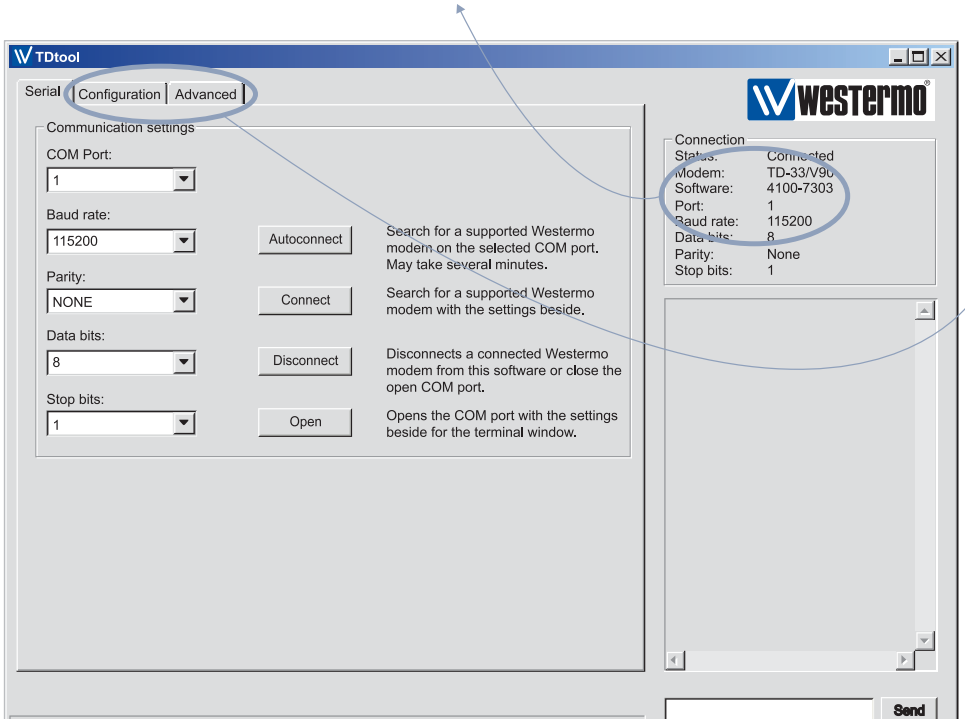


OK ist der Bestätigungscode des Modems, der anzeigt, dass der Befehl ausgeführt wurde, der Befehl stellt am Modem auch automatisch die Werte für Geschwindigkeit, Parität und Stopbit ein.

Da jetzt eine Verbindung zwischen HyperTerminal und dem Modem hergestellt wurde, kann jetzt auch das Modem konfiguriert werden. Es sollte dabei auch an die Eigenschaften gedacht werden, die das Modem in der Endanwendung übertragen soll.

TD-Tool

Eine der Konfigurationsmöglichkeiten für unsere Modems ist die Software TD-Tool, eine Anwendung die automatisch das angeschlossene Modem erkennt und seine Konfiguration erleichtert.



Die Anwendung liest die Konfigurationsparameter für das angeschlossene Modem. Dies gilt ebenso für die aktuellen Einstellungen wie für eventuelle Konfigurationsmöglichkeiten. Diese befinden sich unter Konfiguration und Fortgeschritten.

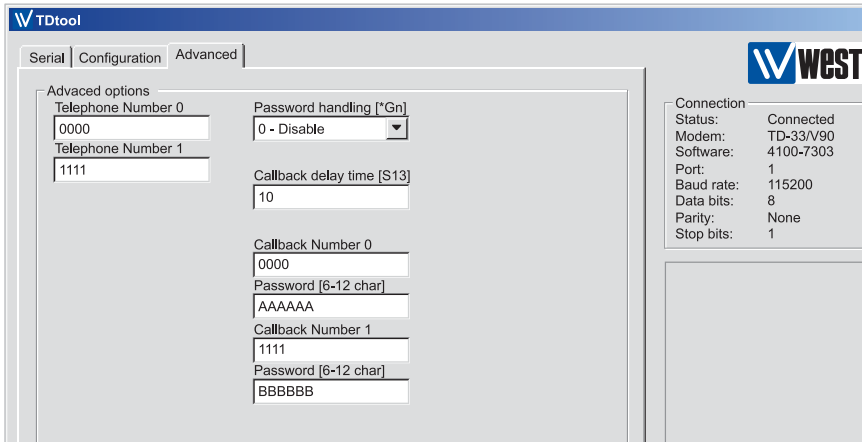
TD-Tool kann von unserer Website heruntergeladen werden.

In diesen Beispielen haben wir TDtool an zwei alternative Modems angeschlossen, die Bildschirmabbildungen zeigen, wie die Anwendung sich je nach Modem verhält.

Option 1) A TD-33

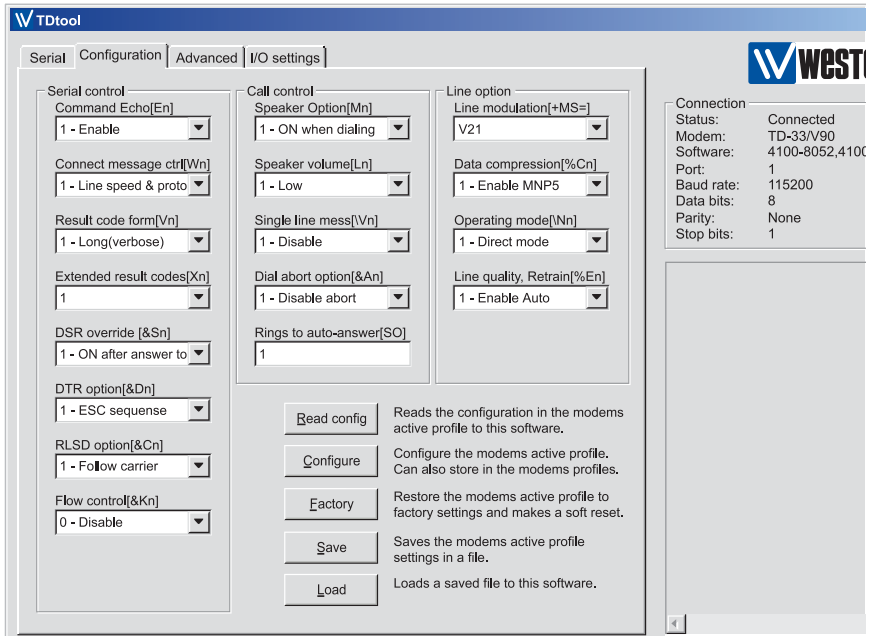
Option 2) A TD-34, ein Modem, das unter anderem SMS-Meldungen versenden kann

Unter der Karteikarte Fortgeschritten für das TD-33, kann die Telefonnummer für den Rückruf eingetragen werden und das verwendete Passwort.



Option 1 TD-33

Unter der Karteikarte Fortgeschritten des TD-34 finden sich weitere Konfigurationsoptionen, hier können die erforderlichen SMS-Einstellungen usw. vorgenommen werden.



Option 2 TD-34

TDtool ist eine ausgezeichnete Ergänzung zu Anwendungen wie HyperTerminal, da es die Konfiguration der Telefonmodems erleichtert. Sind alle Einstellungen erfolgt, werden sie entweder zum Modem heruntergeladen oder in einer Textdatei gespeichert.

AT-Befehle

Ein Telefonmodem arbeitet auf zwei Arten, im:

- Befehlsmodus
- und im Übertragungsmodus

Im Befehlsmodus kann das Modem so konfiguriert werden, dass es mit den Anwendungen arbeiten kann. Im Übertragungsmodus ist das Modem mit einem anderen Modem verbunden und tauscht mit ihm Daten aus.

Wie bereits erwähnt, wurde von Hayes Microcomputer Products ein Befehlssatz entwickelt, der zum De-facto-Standard wurde, die Befehle werden Hayes®-Befehle genannt. Diese Befehle werden einerseits dafür verwendet, das Modem zu konfigurieren und andererseits zum Aufbau einer Verbindung.

Da die AT-Befehle zum Standard für Telefonmodems wurde, bestehen große Ähnlichkeiten in ihrem Einsatz. In jedem Fall muss aber beachtet werden, dass Unterschiede bestehen, je nachdem wie fortschrittlich ein Modem im Gegensatz zu einem anderen ist. Einige der wichtigsten Befehle werden im Folgenden vorgestellt, genaue Beschreibungen finden sich in den entsprechenden Installationshandbüchern.

ATA – **A**nswer (Antwort)

Befiehlt einem Modem im Befehlsmodus einen aktuellen ankommenden Ruf zu beantworten. Das Modem führt ein Handshaking aus, um eine Verbindung herzustellen. Nachdem die Verbindung hergestellt wurde, wechselt das Modem in den Übertragungsmodus.

ATDn – **D**ial (Wählen)

Befiehlt einem Modem im Befehlsmodus einen Anruf zu initiieren. Bei (n) handelt es sich normalerweise um die Telefonnummer, aber es gibt auch andere Codes, z. B. um eine Pause während des Wählvorgangs einzulegen, falls das Modem auf einen Rufton der Verbindungsstelle warten muss. Nachdem die Verbindung hergestellt wurde, wechselt das Modem in den Übertragungsmodus.

ATH – **H**ang-Up (Auflegen)

Das Modem beendet die Verbindung und legt auf. Um diesen Befehl verwenden zu können, muss das Modem vom Übertragungsmodus in den Befehlsmodus geschaltet werden, normalerweise mit dem Code +++.

AT&Fn – Restore **F**actory Configuration (Auslieferungszustand wiederherstellen)

Setzt das Modem wieder auf die Grundeinstellungen des Herstellers zurück, oder auf das Konfigurationsprofil 0 oder 1.

ATQn – **Q**uiet Result Code Control (Ergebniscode abschalten)

Die vom Modem gesendeten Ergebniscodes können hier an- oder abgeschaltet werden, bei einigen Anwendungen muss das Modem so eingestellt sein, dass keine Zeichen gesendet werden.

ATEn – Echo on/off (Echo ein/aus)

Schaltet für ein angeschlossenes Terminal das Echo ein oder aus. Dies ist bei einigen Anwendungen erforderlich, kann aber beim Versuch Befehle einzugeben Störungen hervorrufen.

AT&V – Display Current configuration and Stored Profiles (Aktuelle Konfiguration und gespeicherte Profile anzeigen)

Der Befehl listet die Inhalte der im Modem gespeicherten Profil- und S-Register auf, die für die Funktionskonfiguration eingesetzt werden, siehe Beispiel auf Seite 80.

AT&Wn – Store Current Configuration (Aktuelle Konfiguration speichern)

Speichert die aktuelle Konfiguration des Modems in Profil 0 oder 1.

ATZn – Soft Reset and Restore Profile (Software-Reset mit Profilwiederherstellung)

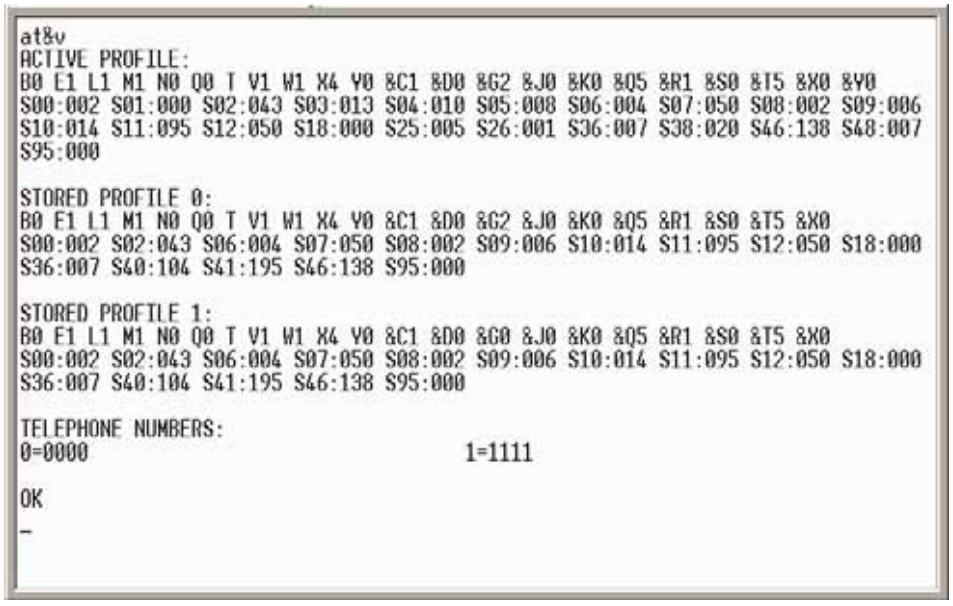
Am Modem findet ein Software-Reset statt und das konfigurierte Profil wird wiederhergestellt.

ATO – On Line Data Mode (Online-Datenmodus)

Das Modem schaltet in den Datenmodus.

+++ Schaltet vom On-Line-Data-Mode in den Befehlsmodus.

Die Bildschirmabbildung zeigt die Inhalte der Modemregister, eine genaue Auflistung und Beschreibung der Register findet sich im Handbuch des Modems. Das untere Beispiel beschreibt einige der Funktionen der S-Register.



Register	Funktion
S00	Der Inhalt des Registers sagt dem Modem, nach wieviel Rufsignalen es antworten soll. Bei diesem Beispiel antwortet das Modem nach dem zweiten Rufsignal, da der Wert auf 002 gesetzt ist.
S01	Zählt die Anzahl der ankommenden Rufsignale.
S02	Beschreibt, welcher Buchstabe für die Escape-Sequenz verwendet werden soll.
S03	Beschreibt, welcher Buchstabe für Zeilenwechsel verwendet werden soll.
S04	Beschreibt, welcher Buchstabe für die Zeilenweiterschaltung verwendet werden soll.
S05	Beschreibt, welcher Buchstabe für die Rücktaste verwendet werden soll.
S07	Beschreibt, wieviel Sekunden das Modem auf den Träger warten soll, bevor es auflegt.
S10	Beschreibt, wie viele Sekunden das Modem warten soll, bevor es auflegt wenn das Trägersignal verloren wurde.

Höhere Geschwindigkeiten

xDSL

Der Name xDSL gilt für eine ganze Technologiefamilie, bei der digitale Modems mit Standard-Telefonleitungen oder festen Leitungen eingesetzt werden. Die Art der digitalen Übertragung wird mit dem Buchstaben bezeichnet, der das x ersetzt. Einige Beispiele für Bezeichnungen sind: ADSL, SDSL, SHDSL und VDSL. Diese Technologien passen für unterschiedliche Anwendungsbereiche. VDSL zum Beispiel erreicht Übertragungsraten von bis zu 52 Mbit, aber nur über etwa 300 m , SHDSL unterstützt ein Maximum von 2,3 Mbit bis zu 3 km und 192 kbit/s bis zu etwa 6 km.

HDSL

HDSL, High Speed Digital Subscriber Line, Duplex-Übertragung mit Geschwindigkeiten von 2,3 Mbit/s in jeder Richtung.

ADSL

ADSL, Asymmetric Digital Subscriber Line, Duplex-Übertragung bis zu Geschwindigkeiten von 8 Mbit/s zum Teilnehmer (Downstream) und 640 kbit/s vom Teilnehmer (Upstream). Die Datenübertragung nutzt simultan die gleiche Leitung wie der normale Telefonverkehr. Der Anwender installiert einen Filter an der ersten Dose um die Sprachqualität zu verbessern, der Filter wird Splitter genannt und normalerweise mit dem ADSL-Produkt geliefert. ADSL ist eine populäre Lösung für Privatanwender, da die Technologie eine höhere Downstream-Übertragungsrate ermöglicht als Upstream. Downloadzeiten sind für einen Privatanwender normalerweise wichtiger, da der Upload nur für E-mails eingesetzt wird.

VDSL

VDSL, Very high speed Digital Subscriber Line, Duplex-Übertragung bis zu Geschwindigkeiten von 52 Mbit/s zum Teilnehmer (Downstream) und 6,4 Mbit/s vom Teilnehmer (Upstream). Die Übertragung nutzt ein Leitungspaar.

VDSL ist die zur Zeit schnellste Technologie zur Datenübertragung über das Standard-Telefonnetz. Es ist eine Alternative zu ADSL, wenn besonders hohe Übertragungsraten erforderlich sind, wie zum Beispiel für:

- Video-Streaming
- Video-Konferenzen
- Kombinationen von Video und Daten über die gleiche Verbindung
- Hohe Anforderungen an den Datenzugang

SDSL

SDSL (Symmetric Digital Subscriber Loop) und G.SHDSL sind symmetrische xDSL-Technologien.
Eine ihrer herausragenden Eigenschaften sind die gleich hohen Upload- und Downloadraten, daher die Bezeichnung symmetrisch. Beim Einsatz von SDSL erreicht der Anwender eine Datenrate von maximal 2,3 Mbit/s in beiden Richtungen. Symmetrisches SDSL kann im Back-to-Back-Modus eingesetzt werden, der zwei Modems mit einem Kupferkabel verbindet. SDSL ist eine herstellereigene Lösung, die hauptsächlich in Nordamerika installiert wird. Industrielle Anwender wechseln verstärkt zum internationalen Standard SHDSL, siehe unten.

SHDSL

SHDSL steht für Symmetric High-Bitrate Digital Subscriber Loop, der erste internationale Standard for Multi-Rate symmetrisches DSL. SHDSL wurde für die Übertragung über eine oder mehrere paarverseilte Vierdrahtleitungen entwickelt. Mit einem Leitungspaar erreicht man Übertragungsraten zwischen 192 kbit/s und 2,3 Mbit/s, zwei Leitungspaare ermöglichen Raten zwischen 384 kbit/s and 4,6 Mbit/s. SHDSL arbeitet mit einem fortschrittlichen Algorithmuscode, TC-PAM, der im Vergleich mit anderen DSL-Technologien zu verbesserten Übertragungsraten und/oder Übertragungsdistanzen führt.

Beispiele für Übertragungsentfernungen mit SHDSL

	Geschwindigkeit	Entfernung
Kommunikation über ein Leitungspaar		
AWG 26	192 kbit/s	6 km
Kommunikation über ein Leitungspaar		
AWG 26	2,3 Mbit/s	3 km
Kommunikation über zwei Paare		
AWG 26	2,3 Mbit/s	5 km

Sind größere Übertragungsentfernungen erforderlich, kann ein Repeater zwischen den Geräten eingesetzt werden.

Detaillierte Informationen finden sich in den Standards:

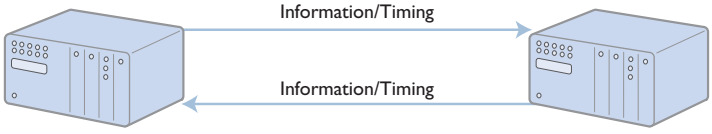
- ANSI (T1E1.4/2001-174) für Nordamerika
- ETSI (TS 101524) für Europa
- ITU-T (G.991.2) weltweit

G.703

Der ITU-Standard G.703 beschreibt elektrische und physische Eigenschaften und einige Übertragungsraten.
Es gibt drei grundlegend verschiedene Arten von Schnittstellen, kodirektionale, kontradirektionale and zentrale Schnittstellen.
Der Standard beschreibt Geschwindigkeiten von 64 kbit/s bis 155 520 kbit/s. Ursprünglich wurde der Standard entwickelt, um Sprache über einen PCM-Link zu übertragen.
Das Übertragungsmedium kann entweder ein abgeglichenes Leitungspaar von 120 Ohm sein oder ein nicht abgeglichenes Koaxialkabel von 75 Ohm.

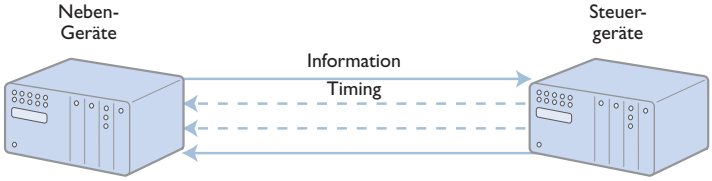
Kodirektionale Schnittstelle

Die Übertragung erfolgt über Leitungspaar für jede Richtung. Daten und Timing-Informationen sind überlagert. Daten und Timing-Informationen laufen in die gleiche Richtung, es ist Aufgabe des Empfängers, diese Daten- und Zeitinformationen zu synchronisieren.



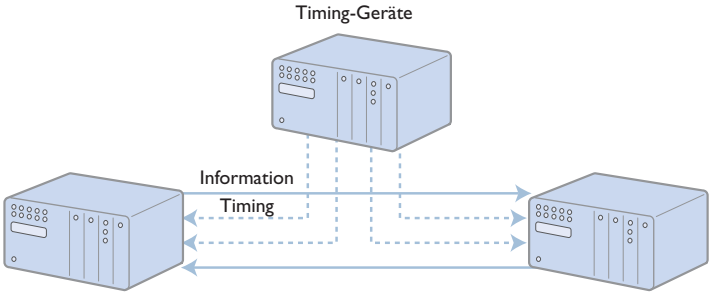
Kontradirektionale Schnittstelle

Diese Art der Übertragung arbeitet mit 4 Leitungspaaren, die Timing-Informationen werden vom Steuergerät geliefert.



Zentrale Uhren-Schnittstelle

Diese Variante der Schnittstelle arbeitet mit 3 bis 4 Leitungspaaren, die Timing-Informationen werden von der Zentraleinheit geliefert. Bei 3 Leitungspaaren wird ein gemeinsames Timing an Sender und Empfänger geliefert. Bei 4 Leitungspaaren erfolgt das Timing individuell für Sender und Empfänger.



GSM

Was bedeuten Abkürzungen wie GSM, GPRS, UMTS und welche Möglichkeiten bieten sie für die Datenkommunikation?

Technische Bezeichnungen enthalten häufig Abkürzungen und Initialwörter. Wir haben uns dafür entschieden, diese technischen Bezeichnungen und Abkürzungen beizubehalten, da sie zum Industriestandard geworden sind, obwohl sie häufig in englischer Sprache sind.

Die Geschichte von GSM

Zu Beginn der achtziger Jahre waren unzählige analoge Systeme mit unterschiedlicher Qualität in Europa im Einsatz. Es war jedoch schnell ersichtlich, dass die analoge Technik zukünftige Anforderungen an eine effiziente Datenübertragung nicht erfüllen kann. Daher wurde die **G**roupe **S**péciale **M**obile (GSM) 1982 in Wien gegründet.
Die Gruppe erhielt den Auftrag, ein mobiles System zu entwickeln, das eine hohe Audioqualität bietet und das zu geringen Kosten.

1989 übernahm das **E**uropean **T**elecommunication **S**tandards **I**nstitute (ETSI) die Verantwortung für die Weiterentwicklung von GSM. Die Abkürzung GSM erhielt eine neue Bedeutung, **G**lobal **S**ystem for **M**obile communications.

GSM ermöglicht den drahtlosen Transfer von Sprache, Text und Bildern zwischen verschiedenen Gerätetypen, allerdings nur, wenn sich die Geräte im Empfangsbereich einer Funkbasisstation eines Netzwerkbetreibers befinden. Die Anzahl der Benutzer von GSM-Geräten ist nach der Standardisierung explosionsartig angestiegen, hauptsächlich mit Sprachdiensten. Anfang 1994 gab es 1,3 Millionen Teilnehmer, diese Zahl ist weltweit auf 1024 Millionen angestiegen (Februar 2004).

Ein starker Anstieg ist jedoch auch bei industriellen M2M-Anwendungen (**M**achine **to M**achine) zu beobachten. Hierbei kann es sich zum Beispiel um die Daten- oder Alarmübertragung von einem Basisgerät (Slave) an ein Steuersystem handeln oder um die Übertragung von Daten zu/von Parkuhren. Das Feld dieser Anwendungen ist nahezu unbegrenzt und es wird zur Abdeckung zukünftiger Bedürfnisse eine schnelle Entwicklung verschiedener Typen von GSM-Geräten erwartet.

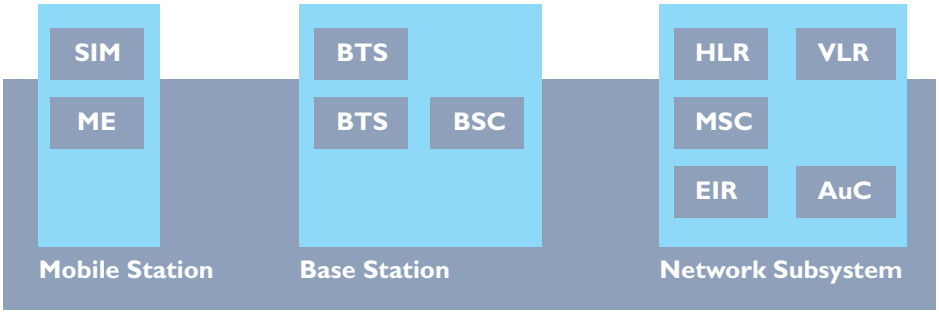
Die digitale Übertragung bietet im Gegensatz zur Analogtechnik für mobile Netzwerke viele Vorteile, z. B.:

- Verbesserte Qualität der Telefonverbindung
- Höhere Übertragungsraten
- Verbesserte Ausnutzung der Bandbreite, das ermöglicht eine Erhöhung der Teilnehmerzahlen im Netzwerk
- Neue Service- und Funktionsangebote wie Datentransfer, Texte und Fax.
- Möglichkeit der Datenverschlüsselung für eine verbesserte Sicherheit
- Geringeren Stromverbrauch, d.h. längere Stand-by- und Übertragungszeiten bei batteriebetriebenen Geräten

Architektur

In einem GSM-Netzwerk können drei unterschiedliche Bereiche betrachtet werden:

- **M**obile **S**tation (MS)
- **B**ase **S**tation **S**ystem (BSS)
- **N**etwork **S**ubsystem, mit Verbindungen zu externen Netzwerken, z. B. ISDN- oder PSTN-Netzwerken



Die Bauteile des Netzwerks

ME Bedeutet **M**obile **E**quipment, das sind Geräte, die für den Einsatz im GSM-Netzwerk ausgelegt sind. Jedes ME-Gerät besitzt eine einmalige Identifikation (IMEI-Nummer), International Mobile Equipment Identity. Dies ermöglicht dem Netzwerkbetreiber die Nutzung eines Gerätes zu blockieren, z. B. wenn ein ME gestohlen wurde.

SIM Steht für **S**ubscriber **I**dentity **M**odule, dies ist eine Karte, die gemeinsam mit einem ME-Gerät genutzt wird. Die SIM-Karte wird vom Netzwerkbetreiber geliefert und enthält Daten wie: Telefonnummer, PIN-Code, Adressbuch, usw. Die SIM-Karte kann zwischen unterschiedlichen ME-Geräten getauscht werden.

BTS Steht für **B**ase **T**ransceiver **S**tation, eine Funkbasisstation, d. h. ein Sender und Empfänger, der es ermöglicht, mit ME-Geräten zu kommunizieren.

BSC Steht für **B**ase **S**tation **C**ontroller; und bezeichnet eine Nebenstation, die mit der Funkbasisstation kommuniziert. Die Nebenstation kann mit mehreren Funkbasisstationen kommunizieren.

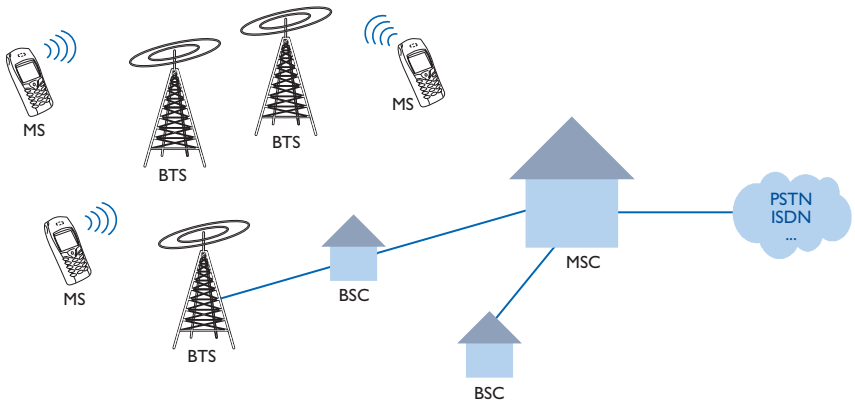
MSC Steht für **M**obile **S**witching **C**entre, eine Station, die die Weiterleitung an ein analoges PSTN (**P**ublic **S**witched **T**elephone **N**etwork) oder an ein digitales ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork) Netzwerk ermöglicht.

HLR Steht für **H**ome **L**ocation **R**egister, eine Datenbank, die unter anderem Basisinformationen über den Teilnehmer enthält, z. B. wie der Vertrag gestaltet ist.

VLR Steht für **V**isitor **L**ocation **R**egister, eine Datenbank, die Informationen über ein ME speichert, das sich in einer Zelle befindet, die nicht durch das HLR kontrolliert wird.

EIR Steht für **E**quipment, **I**dentity **R**egister, ein Register sämtlicher Nutzer des Netzwerks. Die Identifikation erfolgt über die IMEI-Nummer des ME.

AuC Steht für **Au**thentication **C**entre, eine Datenbank, die Informationen über den Netzwerkbetreiber enthält und über die Vertragsart des Nutzers.

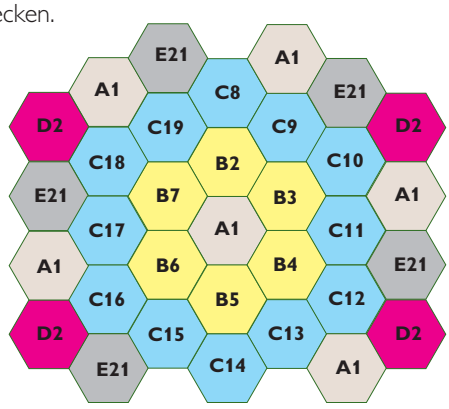


Zellenstrukturen

Funkbasisstationen werden so positioniert, dass sie einen maximalen Bereich abdecken. Der von einer Funkbasisstation abgedeckte Bereich wird Zelle genannt.

Das gesamte GSM-Netzwerk setzt sich aus Zellen unterschiedlicher Größe zusammen. Eine Zelle kann einen Bereich mit einem Radius von 200 Metern bis zu einem Radius von ~ 30 km umfassen. Das ist von der Lage der Funkbasisstation abhängig sowie von den Umgebungsbedingungen.

Weitere Faktoren, die die Installation beeinflussen, sind unter anderem die Sendeleistung und ob die Funkbasisstation in einer Umgebung liegt, die für den Funkverkehr problematisch ist. Die Zellenstruktur ermöglicht die Wiederverwendbarkeit von Frequenzen in der Funkbasisstation. In der nebenstehenden Abbildung kann die Frequenz A1 im dritten Ring wieder eingesetzt werden, ohne Gefahr einer Funküberlagerung zwischen Zellen der gleichen Frequenz.



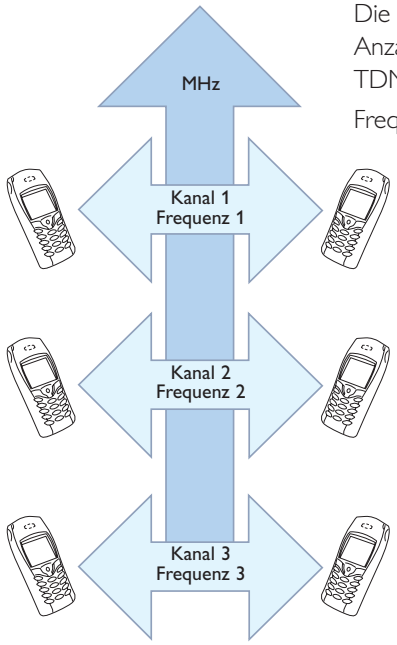
Bei Reisen über längere Strecken wird es notwendig, zwischen den Zellen zu wechseln, durch die man fährt. Dieser Prozess wird Handover genannt.

Funkübertragungen zwischen MS und BSS

Als in den achtziger Jahren die GSM-Eigenschaften festgelegt wurden, hat die ITU (International Telecommunication Union) zwei Frequenzbänder von 25 MHz für GSM-Funkübertragungen reserviert:

- 880–915 MHz "Uplink"-Übertragung von MS zu BSS
- 925–960 MHz "Downlink"-Übertragung von BSS zu MS

Die Nachfrageentwicklung der Mobilkommunikation erforderte die Nutzung weiterer Frequenzen. Heute werden fünf standardisierte Frequenzen genutzt 400, 850, 900, 1800 und 1900 MHz. Die letzte Frequenz wird hauptsächlich in den USA und in einigen Ländern Asiens genutzt, während 900 und 1800 weltweit eingesetzt werden.



Frequenzaufteilung

Die Grenzen der Bandbreite haben zum Einsatz von Techniken geführt, die eine maximale Anzahl von gleichzeitigen Nutzern ermöglichen. Dies wird mit einer Kombination aus TDM, *Time Division Multiplexing* und FDM, *Frequency Division Multiplexing* erreicht.

Frequency division (Frequenzaufteilung) bedeutet, dass das vorhandene 25 MHz-Band in 200 KHz-Bänder aufgeteilt wird. Im oberen Beispiel sind die Frequenznutzungen zwischen den Zellen A1, B2, B3, usw. Beispiele für Frequenzaufteilungen.

Zeitscheibenverfahren

Beim TDM (Time Division Multiplexing) nutzen alle Sender dieselbe Frequenz, jedoch zu unterschiedlichen Zeitpunkten. Die Ausrüstung muss synchronisiert sein, damit sich die verschiedenen Sender nicht gegenseitig stören.

Zusammenstellung

Frequenz für die Übertragung vom ME zur Funkbasisstation	880-915	MHz
Frequenz für die Übertragung von der Funkbasisstation	925-960	MHz
Bandbreite	35+35	MHz
Zugangsmethode	TDMA/FDMA	
Frequenz pro Funkkanal	200	KHz
Frequenzabstand zwischen Downlink/Uplink	45	MHz
Maximaler Radius für eine Zelle	30	km
Minimaler Radius für eine Zelle (Mikrozelle)	30	m
Maximale Sendeleistung vom mobilen Endgerät	2	W @ 900 MHz

Dienste im GSM-Netzwerk

Im GSM-Netz stehen eine Anzahl von Diensten zur Verfügung, wie:

- Telefon
- CSD (**C**ircuit **S**witched **D**ata, Datenübertragung)
- SMS (**S**hort **M**essage **S**ervice, Kurznachrichten)
- MMS (**M**ultimedia **M**essage **S**ervice, Multimedia-Kurznachrichten)
- FAX
- GPRS (**G**eneral **P**acket **R**adio **S**ervice)

Telefon

Der bekannteste GSM-Dienst, der zu seiner universellen Verbreitung beigetragen hat. Die Algorithmen, die den Datenverkehr kodieren und dekodieren sind kontinuierlich weiterentwickelt worden und führten zu einer stetigen Verringerung der Bandbreite für das Telefonieren ohne Verlust in der Übertragungsqualität.

Circuit Switched Data

Die Übertragung von Daten, Geschwindigkeiten von 2400 bit/s bis zu 14,4 kbit/s sind möglich. Die nebenstehende Tabelle zeigt die möglichen Geschwindigkeiten und Protokolle.

Datenübertragung kann für transparente oder nicht-transparente Datenübertragung eingerichtet werden. RLP (**R**adio **L**ink **P**rotocol) wird in nicht-transparenten Übertragungen eingesetzt, ein fehlerkorrigiertes GSM-Protokoll. Dieses Protokoll bietet eine zuverlässigere Übertragung, es sorgt allerdings auch für Verzögerungen in der Übertragung. Eine Nutzung dieses Dienstes erfordert ebenso die Unterstützung des Service wie der angeschlossenen Geräte.

Geschwindigkeit	Protokoll
2400 bit/s	V.22 bis
4800 bit/s	V.32
9600 bit/s	V.32
14400 bit/s	V.32 bis
2400 bit/s	V.110
4800 bit/s	V.110
9600 bit/s	V.110
14400 bit/s	V.110

SMS

Der am meisten genutzte Dienst nach dem Telefonieren. Eine SMS-Nachricht nutzt den Signalkanal, um eine Textmeldung zu übertragen. Durch seine Einfachheit ist SMS ebenso privat wie beruflich populär geworden. Zusammengefasst bietet der Dienst folgende Merkmale:

- Eine Nachricht kann bis zu 160 Zeichen umfassen.
- Eine Übertragung kann nicht garantiert werden, da der Empfänger abgeschaltet sein oder sich außerhalb des Sendebereichs befinden kann. Die Nachricht kann mit unterschiedlichen Einstellungen gesendet werden:
- Wie lange die Nachricht vor dem Löschen im Netzwerk aufbewahrt werden soll (bis zu einer Woche), wenn sie nicht gleich zugestellt werden kann.
- Empfangsbestätigung, d. h. der Sender erhält eine Bestätigung, dass die Nachricht angekommen ist.
- Es erfolgt eine Bestätigung, dass die Nachricht gesendet wurde.
- Sendung und Empfang kann während eines Telefongesprächs erfolgen.
- Übertragungen können individuell an Einzelpersonen erfolgen oder an eine Empfängergruppe.

MMS

MMS steht für **M**ultimedia **M**essaging **S**ervice und funktioniert genauso wie der SMS-Service, aber mit der Möglichkeit:

- Bilder und Animationen zu senden
- Musik zu senden
- Eigene Nachrichten aufzuzeichnen und zu senden
- Lange Textmeldungen zu senden
- Eine MMS kann aus Tausenden von Zeichen bestehen, je nach eingesetztem Mobiltelefon.

Fax

Für Klasse 1 und Klasse 2 Faxe möglich

GPRS

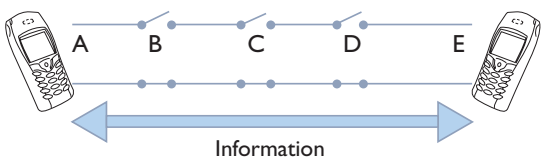
GPRS ist eine Erweiterung des GSM-Netzes, die paketorientierten Datenverkehr ermöglicht. Dieser unterscheidet sich vom CSD-Datenverkehr, der in GSM unterstützt wird Bei GPRS ist jeder Kanal, der nicht mit Telefonverkehr belegt ist, für paketorientierten Datenverkehr frei. Pakete mehrerer unterschiedlicher Nutzer können im selben Kanal gemischt werden, daraus ergibt sich eine effiziente Ausnutzung der verfügbaren Netzwerkressourcen.

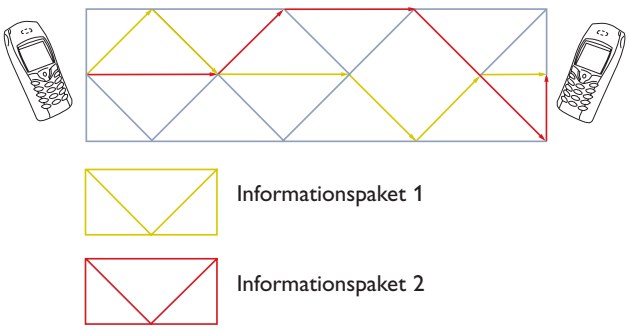
GPRS ermöglicht noch höhere Übertragungsraten, da es mit mehreren Zeitfenstern (time slots) für die Übertragung arbeitet. Theoretisch können bis zu 115,2 kbit/s erreicht werden, in der Praxis sind Übertragungsraten von 20 - 50 kbit/s üblich. Im Vergleich dazu bietet das von einigen Anbietern alternativ zu CSD angebotene HSCSD, *High Speed Circuit Switched Data*, eine Rate von 9,6 - 43,2 kbit/s. Trotzdem hängen die Übertragungsraten von verschiedenen Faktoren ab: Betreiber, Endgerät, Nutzeranzahl in derselben Zelle, der Distanz zur Funkbasisstation, der Bewegung der Geräte, da die Übergabe zwischen Funkbasisstationen die Übertragungsrate reduziert, usw.

Die Übertragungsrate ist ebenfalls davon abhängig, wieviele Zeitfenster eingesetzt werden und mit welchem Kodierungsschema die Übertragungsverbindung arbeitet. Es gibt 4 **C**oding **S**chemes (CS) in GPRS, wobei CS1 das sicherste und zuverlässigste ist, aber auch das mit der langsamsten Übertragungsrate (9,05 kbit/s) während CS4 keine so strenge Fehlerkorrektur und Neuübertragungen bietet, dabei aber Geschwindigkeiten von 21,4 kbit/s erreicht. Die oben genannten Geschwindigkeiten hängen von der Anzahl der Zeitfenster und vom CS ab, d. h. vier Zeitfenster bei CS4 ergeben 4 x 21,4 = 85,6 kbit/s. Es ist ebenfalls zu beachten, dass der GSM-Standard zwar 4 CS definiert, aber nur die ersten beiden CS1 und CS2 (13,4 kbit/s/Zeitfenster) zur Zeit im aktiven GPRS-Netzwerk implementiert sind.

Der Unterschied zwischen "Circuit Switching"- und "Packet Switching"-Netzwerken wird kurz erläutert:

Im **Circuit Switching** -Netzwerk basiert die Anschlussverbindung auf einer physischen Verbindung von zwei Parteien. Diese bleibt konstant erhalten und wird nicht abgebrochen, bis sich eine Partei dazu entschließt, genauso wie bei einem Telefonanruf. Das bietet ebenso Vor- wie Nachteile. Die Kommunikationsgeräte haben eine ständige Verbindung miteinander, sie suchen eine freie Leitung und wissen, dass diese nicht von anderen verwendet wird. Andererseits ist es eine Verschwendung von Ressourcen, wenn die Parteien keine Daten austauschen, da die Verbindung besteht und niemand sie sonst nutzen kann. Dementsprechend sollten die Parteien auflegen, wenn die Verbindung nicht weiter genutzt wird.





Ein **Packet Switching** -Netzwerk ist ein Netzwerk, in dem der Datenverkehr in kleine Pakete aufgeteilt wird, die über das Netz gesendet werden. Deshalb können auch andere Parteien das Netzwerk gleichzeitig nutzen. Wenn man das "Circuit Switching"-Netzwerk mit einem Telefonanruf vergleicht, könnte man das "Packet Switching"-Netzwerk mit einem Spediteur oder dem Postamt vergleichen. Mehrere Personen können gleichzeitig viele Pakete aufgeben. Die Post oder die Spedition sorgen dafür, dass alle Pakete den Empfänger erreichen. Die Pakete teilen sich Transportfahrzeuge und —wege.

Im Februar 2004 boten 172 Anbieter in vielen Ländern die GPRS-Option an. Die Anzahl der Mobiltelefone mit GPRS soll erwartungsgemäß von 10 Millionen im Jahre 2001 auf 280 Millionen 2005 steigen.

Netzwerk-Sicherheit

GSM

Die wichtigsten Sicherheitsmaßnamen im GSM-Netzwerk sind:

- Strenge Authentisierung des Nutzers (das Netzwerk authentisiert die SIM-Karte, die SIM-Karte authentisiert den Nutzer mit dem PIN-Code)
- Schutz gegen Datenanzapfung an der Funkschnittstelle
- Schutz gegen Signalanzapfung an der Funkschnittstelle
- Überprüfung der Geräteidentität, kann bei Diebstahl blockiert werden

Verschlüsselung der Daten über die Funkverbindung, d. h. zwischen dem Gerät und der Funkbasisstation. Die geheime Verschlüsselung jedes Nutzers ist auf seiner SIM-Karte gespeichert, die Authentifizierung des Betreibers erfolgt zentral.

GPRS

Arbeitet prinzipiell mit den gleichen Sicherheitsmaßnahmen wie GSM. Die Authentifizierung erfolgt auf gleiche Art, es werden die gleiche Authentifizierungstechnologie und SIM-Karte eingesetzt. Trotzdem ist die generierte Verschlüsselung für GPRS immer verschieden von GSM. Für GPRS werden spezielle Verschlüsselungsalgorithmen verwendet, die mit 64-bit-Schlüsseln arbeiten.

Unterschiede zwischen GSM und GPRS

CSD
Circuit Switched Data
TDM
Time Division Multiplexing

1	2	3	4	5	6	7	8

Ein Zeitfenster wird verwendet, das ergibt einen maximalen Datendurchsatz von 14,4 kbit/s.

Die laufenden Kosten berechnen sich nach der Verbindungsdauer, egal welche Datenmenge gesendet wurde.

GPRS
General Packet Radio Service
TDM
Time Division Multiplexing

1	2	3	4	5	6	7	8

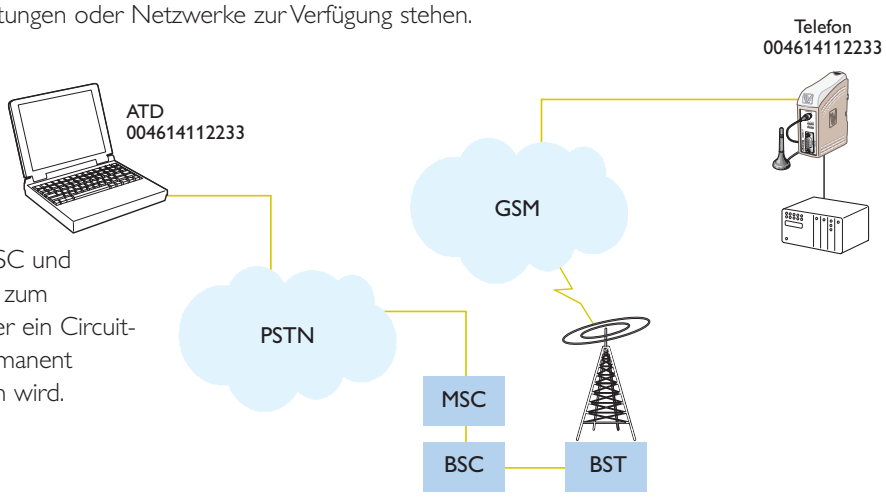
Durch die Verwendung von vier Zeitfenstern und Kodierungsschema (CS) 4 beträgt der maximale Datendurchsatz 85,6 kbit/s.

Die laufenden Kosten basieren auf der gesendeten Datenmenge (Anzahl der Pakete) unabhängig von der Verbindungszeit.

Anwendungsbereiche von GSM und GPRS

Die Einsatzmöglichkeiten von GSM und GPRS in der Datenübertragung sind eine Alternative zu Funkübertragungen. Drahtlose Anwendungen werden zumeist dort für die Übertragung genutzt, wo keine Standleitungen oder Netzwerke zur Verfügung stehen. Trotzdem erfordert die Kommunikation über ein GSM- oder GPRS-Modem einige grundlegende Voraussetzungen.

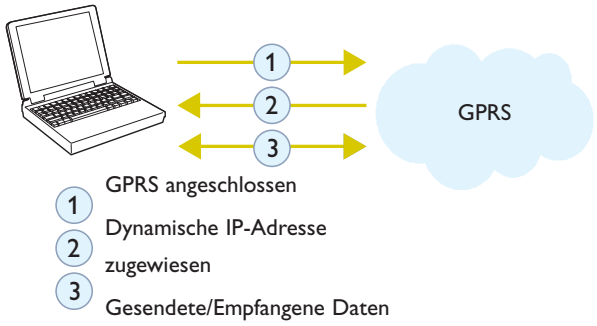
Das GSM-Modem stellt die Verbindung zu einem GSM-Netzwerk her. Eine Verbindung erfolgt über das MSC und BSC und dann über eine PSTN-Leitung zum Computer. Da die GSM-Verbindung über ein Circuit-Switched-Netzwerk erfolgt, ist man permanent verbunden, bis die Leitung unterbrochen wird.



GPRS-Kommunikation arbeitet mit einer anderen Methode. GPRS basiert auf IP-Kommunikation und das angeschlossene Gerät muss eine IP-Adresse nennen, bevor eine Verbindung hergestellt werden kann.

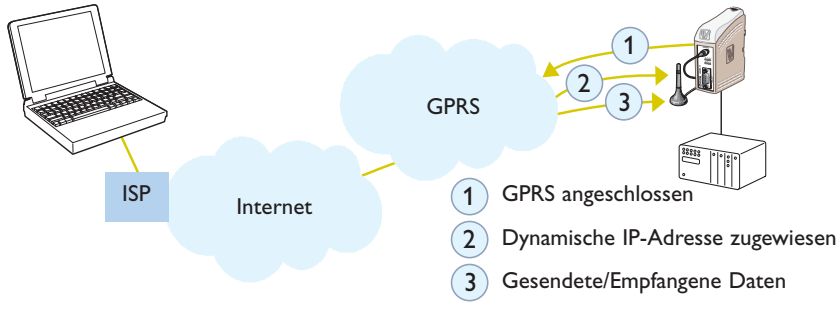
Dies geschieht folgendermaßen:

- Eine Verbindung mit dem GPRS-Netzwerk wird hergestellt
- Eine dynamische Adresse wird zugewiesen
- Der Datenaustausch kann erfolgen

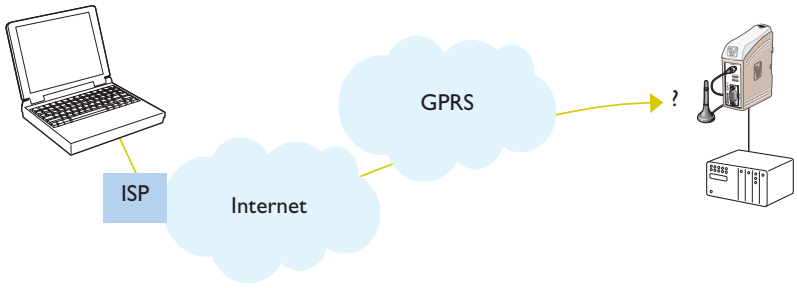


Im Moment bieten nicht alle Dienstanbieter Verträge mit einer festen Zuweisung der Adresse. Bei der dynamischen Zuweisung weiß man nicht, welche Adresse der Gegenseite im Moment gerade zugewiesen wurde.

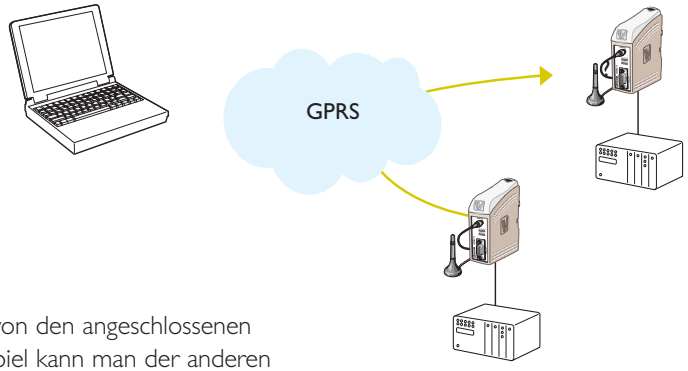
Das ist kein Problem, wenn das GPRS-Modem an den Master angeschlossen ist. Der Master leitet die Verbindung ein und das Modem bekommt seine IP-Adresse zugewiesen. Das bedeutet, dass eine Verbindung mit Geräten hergestellt werden kann, die über eine feste IP-Adresse verfügen, Z. B. ein Computer.



Das Problem tritt auf, wenn ein Gerät, z. B. ein Computer, mit Peripheriegeräten kommunizieren will und der Computer die Verbindung herstellt. Niemand kennt die IP-Adresse, mit der sich der Computer verbinden kann, da sie dynamisch zugewiesen werden.

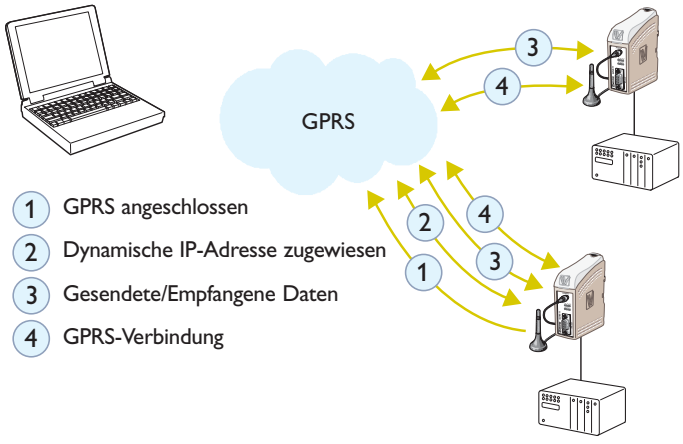


Das gleiche Problem tritt bei einem anderen Anwendungsbereich auf, wenn zwei Geräte Daten austauschen müssen und kein Gerät der Master ist. Das Modem kann die IP-Übertragung nicht beginnen, da es nicht weiß, welche Adresse zugewiesen wird.



Für dieses Problem gibt es Lösungen, die aber von den angeschlossenen Geräten unterstützt werden müssen. Zum Beispiel kann man der anderen Seite die zugewiesene IP-Adresse per SMS zusenden.

Es muss aber dabei beachtet werden, dass im Falle eines Stromausfalls eines der angeschlossenen Geräte der Vorgang wiederholt werden muss, da die IP-Adresse dabei verloren geht.



GPRS-Klassen

GPRS-Geräte sind in drei Kategorien erhältlich, die als Klasse A, B und C bezeichnet werden.

Klasse A	Unterstützt gleichzeitig GSM- und GPRS-Funktionen
Klasse B	Unterstützt GSM- and GPRS-Funktionen, aber nicht gleichzeitig
Klasse C	Die Verbindung unterstützt nur GPRS- oder GSM-Daten Wenn zwischen GPRS und GSM gewechselt werden muss, ist eine neue Verbindung erforderlich.

Multislot-Klassen mit 1 bis 5 Zeitfenster

	Maximale Fensterzahl (slots)		
GPRS Multislot-Klasse	RX "Downlink"	TX "Uplink"	Max
Klasse 1	1	1	2
Klasse 2	2	1	3
Klasse 4	3	1	4
Klasse 6	3	2	4
Klasse 8	4	1	5
Klasse 10	4	2	5
Klasse 11	4	3	5
Klasse 12	4	4	5

RX: Maximale Anzahl der empfangenen Zeitfenster, die vom MS über den GSM TDMA-Frame unterstützt werden können.

RX: Maximale Anzahl der Zeitfenster, die das MS über den GSM TDMA-Frame senden kann.

Max: Gesamtzahl der Zeitfenster im Uplink und Downlink, die gleichzeitig vom MS im TDMA-Frame genutzt werden können.

UMTS (3G)

Die Abkürzung 3G ist in vielen Ländern der geläufige Ausdruck für den Standard UMTS (**U**niversal **M**obile **T**elecommunications **S**ystem), der die Technologie hinter der dritten Generation von Telefonsystemen beschreibt. In einigen Ländern könnte 3G andere Standards bezeichnen. Der Ausdruck 3G kommt daher, dass es sich hier um die dritte Generation der Mobiltelefonie handelt, die erste Generation war analog, ihr folgte GSM, das heutzutage verbreitetste System und jetzt wurde 3G lanciert.

Der Hauptunterschied zwischen 3G und GSM ist die Übertragungskapazität, d. h. wie schnell Daten vom Telefon gesendet oder empfangen werden können. Je höher die Übertragungsrate, desto universeller kann das Mobilnetz eingesetzt werden. 3G ist etwa 40 Mal schneller, das bedeutet, es können zusätzlich fortschrittliche Dienste eingesetzt werden, wie: Senden und Empfangen von Bildern, Filme übertragen und Dienste nutzen, die auf der Position des Nutzers basieren. Daher ist 3G bei vielen auch als mobiles Breitband bekannt.

ISDN

Was ist ISDN?

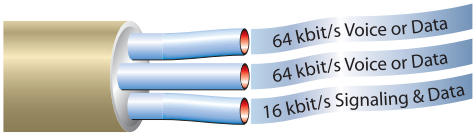
ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork) ist die digitale Entsprechung des Standard-PSTN-Telefonnetzwerkes (**P**ublic **S**witched **T**elephone **N**etwork). Die ISDN-Technologie wurde gemäß den Empfehlungen der **I**nternational **T**elecommunications **U**nion (ITU) standardisiert.

Signalisierung

Anstelle der Aktivierung des Klingelsignals durch die Telefongesellschaft im Telefon (In-Band-Signal) wird ein digitales Paket auf einem separaten Kanal (Out-of-Band-Signal) gesendet. Das Out-of-Band-Signal stört den gerade erfolgenden Anruf nicht und hat eine kurze Verbindungszeit. Das Signal enthält Informationen über den Anrufer, den Anruftyp (Sprache/Daten) und die anrufende Nummer. Das angeschlossen ISDN-Gerät entscheidet dann über den Umgang mit dem Anruf.

Anschlüsse

Eine ISDN-Verbindung setzt sich aus einer Anzahl von B-Kanälen hauptsächlich zum Datentransfer und einem D-Kanal zusammen, der vor allem Steuersignale übermittelt. Die Transferrate eines B-Kanals beträgt 64 kbit/s, mehrere Kanäle können zusammengeschlossen werden, um die Übertragungsrate zu erhöhen. Normalerweise wird ISDN den Kunden in zwei Vertragsformen angeboten: Basisanschluss, der den Zugriff auf zwei B-Kanäle und einen 16 kbit/s-D-Kanal erlaubt (2B+D). Das ermöglicht eine Maximalgeschwindigkeit von zweimal 64 kbit/s, d. h. 128 kbit/s, günstig für Kunden, die eine höhere Datenübertragungsrate wünschen, die Telefon, Fax und Datenübertragung kombinieren oder ein kleines lokales Netzwerk einrichten möchten. An der gleichen Leitung können bis zu acht ISDN-Geräte angeschlossen werden. Das ist ein großer Vorteil, wenn sich unterschiedliche Geräte an einem ISDN-Anschluss befinden.



Die Geräte erhalten ihre eigenen Nummern, als ob sie einen eigenen Anschluss an des Netz hätten. Primärmultiplexanschluss, der den Zugriff auf 30 B-Kanäle und einen 64 kbit/s-D-Kanal erlaubt (30B+D). Die maximale Kapazität bei Nutzung aller 30 B-Kanäle beträgt dann 2 Mbit/s. ISDN mit Primärmultiplexanschluss eignet sich für die Verbindung von Computern, bei denen hohe Übertragungsraten erforderlich sind (z. B. für Videokonferenzen), für große lokale Netzwerke, für Digital-Switches und Bridges zwischen großen regionalen Netzwerken.

Die größten Vorteile von ISDN sind eine Übertragungsrate von 64–128 kbit/s, Verbindungsaufbauzeiten von unter 2 Sekunden, stabilere, störunanfällige Verbindungen und die Flexibilität, mehrere unterschiedliche Geräte an der selben Leitung anzuschließen (z. B. Telefon, Fax oder Computer).

ISDN-Komponenten/-Schnittstellen

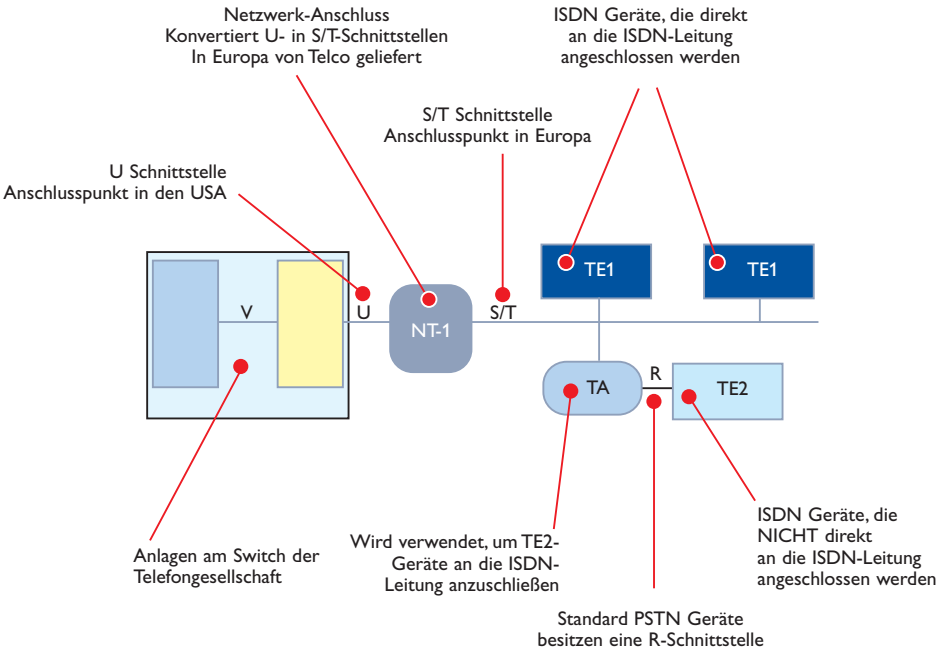
ISDN-Komponenten sind u. a. Endgeräte (terminals), Terminal-Adapter TA, Netzwerk-Termination-Geräte NT, Leitungs-Termination-Geräte LT und Exchange-Termination-Geräte CLA. Zwei Terminal-Typen werden mit ISDN eingesetzt. Spezielle ISDN-Terminals mit einer ISDN-Schnittstelle, Terminal-Geräte Typ 1 TE1 und Terminals mit einer anderen Schnittstelle als ISDN, Geräte mit V.24-Schnittstelle. Diese werden Terminal-Geräte Typ 2 TE2 genannt. TE1 wird an ISDN mit einer digitalen Schnittstelle und paarverseilter Vierdrahtleitung angeschlossen, während TE2 über einen TA an das ISDN-Netzwerk angeschlossen werden. Der Terminal-Adapter kann entweder ein freistehendes Gerät sein oder eine Schnittstellenkarte im TE2-Gerät. Sind TE2 und TA freistehende Geräte, wird normalerweise eine standardisierte Schnittstelle wie RS-232/V.24 oder V11/RS-485 verwendet.

Die nächste Schnittstelle Upstream ist das Netzwerk-Terminal, diese arbeitet als Schnittstelle zwischen der 4-adrigen Schnittstelle des Kundengerätes und dem konventionellen 2-adrigen Kupferkabel des Telefonbetreibers.

Netzwerk-Terminals sind ebenfalls in zwei Typen erhältlich, NT1 und NT2, wobei NT2 das komplexere Gerät ist und Ebene 2 und 3, Protokollfunktionen und Konzentration bietet. NT2-Geräte befinden sich z. B. in Büro-Verbindungsstellen. In den meisten Ländern gehören die Netzwerk-Terminals der Telefongesellschaft.

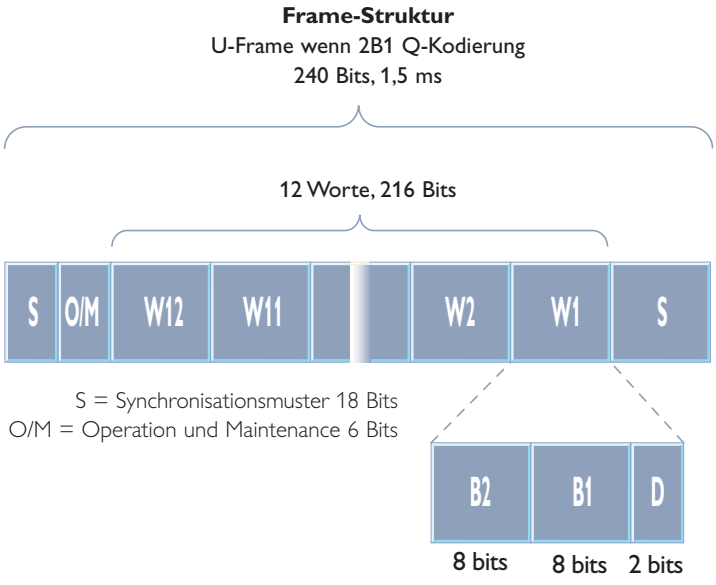
Im Referenzmodell für ISDN wurden eine Anzahl von Referenzpunkten festgelegt, die die Schnittstellen zwischen den Geräten/Terminals des Referenzmodells wie folgt bilden:

- R --- Referenzpunkt, der die Schnittstelle zwischen Nicht-ISDN-Geräten und dem Terminal Adapter TA Standard RS-232/V.24 bildet
- S --- Referenzpunkt, der die Schnittstelle zwischen TE/TA und NT1 bildet
- T --- Referenzpunkt, der die Schnittstelle zwischen NT1 und NT2 bildet
- U --- Referenzpunkt, der die Schnittstelle zwischen NT und dem LT Leitungs-terminal bildet.



Physische Ebene

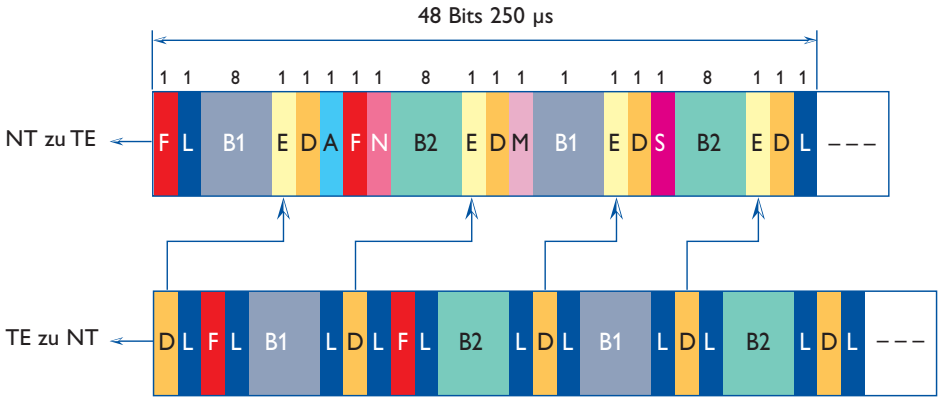
Die Signalgebung zwischen dem Leitungsterminal (LT) der Telefongesellschaft und dem Netzwerk-Terminal des Nutzers (NT) erfolgt über die U-Schnittstelle, während die Signalgebung beim Nutzer zwischen NT und Terminal-Adapter TA über die S-Schnittstelle erfolgt. In der U-Schnittstelle werden Frames mit einer Länge von 240 Bits verwendet, die mit einer Rate von 160 kbit/s übertragen werden. Die Frames der U-Schnittstelle sind so strukturiert, wie es auf der folgenden Abbildung gezeigt wird.



Frame-Format der S-Schnittstelle

Die Frames der S-Schnittstelle arbeiten mit 48 Bits, von denen 36 für die Datenübertragung verwendet werden, die Bitrate in der S-Schnittstelle beträgt 192 kbit/s. Die innere Struktur der Frames ist etwas unterschiedlich, je nachdem in welche Richtung sie gesendet wurden. Die untere Abbildung zeigt, wie die verschiedenen Bits eingesetzt werden.

A = Activation bit
B1 = B1 Kanal (2 x 8 Bits / Frame)
B2 = B2 Kanal (2 x 8 Bits / Frame)
D = D Kanal (4 x 1 Bit / Frame)
E = Echo des Vorigen D-Bit
F = Framing-Bit
L = DC Abgleich
S = S-Kanal
N = Invertierte F von NT an TE
M = Multiframing-Bit



Ebene 2 - Data-link-Ebene

Die Data-link-Ebene für ISDN wird in den ITU-Standards Q.920 bis Q.923 festgelegt. Die Signalgebung des D-Kanals wird in Q.921definiert. Link Access Procedure – D-Kanal (LAP-D) ist das in der Data-link-Ebene verwendete Protokoll. LAP-D ist mit X.25 LAP-B fast identisch, beide basieren auf HDLC. Die von LAP-D verwendete Frame-Struktur wird hier gezeigt:

Flag	Adresse	Steuer-	information	CRC	Flag

Flag (1 Oktett)
Start-Flag ist immer 7E16 (0111 11102).

Adresse (2 Oktetts)

8	7	6	5	4	3	2	1
SAPI (6 Bits)						C/R	EA0
TEI (7 Bits)							EA1

SAPI (**S**ervice **A**ccess **P**oint **I**dentifier), 6-Bits
C/R (**C**ommand/**R**esponse) Bit, das anzeigt, ob der Frame ein Befehl oder eine Antwort ist
EA0 (**A**ddress **E**xtension) Bit, das das letzte Byte einer Adresse bezeichnet
TEI (**T**erminal **E**ndpoint **I**dentifier) 7-Bits Geräte-Identifizierer (siehe Seite 102)
EA1 (Address Extension) Bit, dieselbe Funktion wie EA0

Steuerung (2 Bytes)
Das Steuerungsfeld zeigt den Frametyp und den Befehl. Es gibt drei unterschiedliche Frame-Typen: Information, Steuerung/Überwachung und nichtnummerierte Frames, wobei die ersten beiden ebenfalls die Sequenznummern (N[r] and N[s]) enthalten.

information
Informationen für die darüberliegende Netzwerk-Ebene und Nutzerdaten.

CRC (2 Bytes)
Prüfsumme für die zyklische Redundanz (16-Bits) um Bitfehler in der Übertragung zu erkennen.

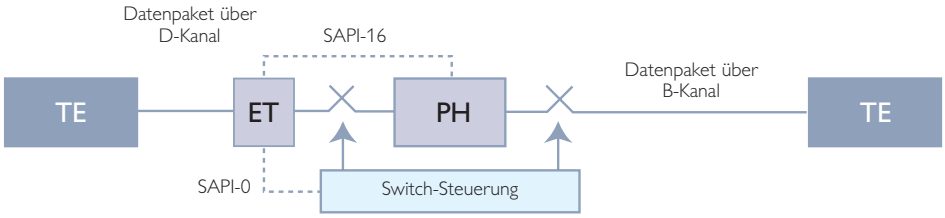
Flag (1 Oktett)
End-Flag ist immer 7E16 (0111 11102).

SAPI

Der Service Access Point Identifier (SAPI) ist ein 6-Bit-Feld, das die Definition von bis zu 64 unterschiedlichen Servicefunktionen ermöglicht, die von Ebene 2 an Ebene 3 weitergegeben werden.

SAPI-Wert	Ebene-3-bezogen oder Management-bezogen
0	Ruft Steuerprozesse auf
1–11	Für spätere Standardisierung reserviert
12	Teleaktion — Kommunikation
13–15	Für spätere Standardisierung reserviert
16	Paket-Übertragung gemäß X.25 Ebene 3 Prozessen
17–31	Für spätere Standardisierung reserviert
63	Ebene 2 Management-Prozesse
Alle anderen	Für Q.921 Prozesse nicht verfügbar

Die Abbildung zeigt den Einsatz eines SAPI-Feldes, wobei SAPI = 0 für die Switch-Steuerung verwendet wird und SAPI = 16 für das Paket-Routing, wenn X.31, X.25 über den D-Kanal verwendet wird.



TEI

Terminal Endpoint Identifiers (TEI) ist eine eindeitige ID, die jedem TA/TE des ISDN-S/T-Busses zugewiesen wird. Der Identifier kann dynamisch beim Gerätestart zugewiesen werden oder statisch während der Installation.

TEI-Wert	Nutzertyp
0–63	Nicht-automatische TEI-Zuweisung Nutzergeräte
64–126	Automatische TEI-Zuweisung Nutzergeräte
127	An alle Geräte senden

Ebene 3 – Netzwerk-Ebene

Die Netzwerk-Ebene für ISDN wird in den ITU-Standards Q0.930 bis Q0.939 festgelegt. Ebene 3 bietet Funktionen, die eine logische Verbindung zwischen zwei Geräten aufbauen, aufrechterhalten und beenden. Die Struktur des Informationsfeldes auf Ebene 3 hat eine variable Länge und die unterschiedlichen Felder werden in Q.931 spezifiziert:

Informationsfeld							
8	7	6	5	4	3	2	1
Protocol Discriminator							
0	0	0	0	Länge des CRV			
Call Reference Value (1 oder 2 Octets)							
0	Nachrichtentyp						
Pflicht- & freiwillige Informationselemente (veränderlich)							

Das Informationsfeld im Nachrichten-Header sieht folgendermaßen aus:

Protocol Discriminator (1 Octet)

Das Feld identifiziert den Protokolltyp, mit dem Eben-3-Nachrichten verarbeitet werden. Wenn Q.931 verwendet wird enthält das Feld 0816.

Länge (1 Octet)

Länge des nachfolgenden Feldes.

Call Reference Value (CRV) (1 oder 2 Bytes)

Das Feld dient der Identifizierung des/der Anrufers/Verbindung, zu der die Signalmeldung gehört. Der Wert wird solange für alle Signalisierungen verwendet, wie der laufende Anruf dauert.

Nachrichtentyp (1 Octet)

Das Feld nennt den gesendeten Nachrichtentyp. Vier Gruppen von Nachrichten können unterschieden werden: Verbindungsaufbau, Information, Verbindungsende und andere Nachrichten. SETUP und CONNECT gehören zur ersten Gruppe. Informationselemente (variable Länge)

Dieses Feld enthält unterschiedliche Informationselemente. Die Art der gesendeten Informationselemente hängt vom Nachrichtentyp des vorigen Feldes ab. Elemente für die B-Nummmerninformation, zusätzliche Dienste und Übertragungsanforderungen an das Netzwerk, usw. sind hier zu finden.

CAPI

COMMON-ISDN-API (CAPI) liefert eine standardisierte Schnittstelle für die Softwareentwicklung von Anwendungen für ISDN.
Für den CAPI-Standard entwickelte Anwendungen können über ISDN kommunizieren, ohne Rücksicht auf herstellerspezifische ISDN-Eigenheiten zu nehmen.
Zur Zeit ist die Arbeit mit diesem Standard fast zum Stillstand gekommen und die meisten Telefonnetzbetreiber liefern ISDN basierend auf Q931/**ETSI 300 102**, CAPI-Version 2.0 wurde entwickelt, um das Protokoll auf Basis von Q 931zu unterstützen. CAPI wurde als Plattform für viele unterschiedliche Protokollstacks entwickelt, u.a. für Netzwerke, Telefon und Datentransfer.
CAPI wurde kürzlich in den Europäischen Standard ETS 300 838 "**I**ntegrated **S**ervice **D**igital **N**etwork (ISDN); Harmonized Programmable Communication Interface (HPCI) für ISDN" übernommen.

Funk

Funkkommunikation

Die drahtlose Datenkommunikation über ein Funkmodem bietet die Möglichkeit zur Kommunikation mit:

- entfernten Geräten
- Messstationen
- externen Gebäuden und unbemannten Stationen
- temporären oder mobilen Einsatzorten.

Diese Kommunikationsform wird beispielsweise genutzt, um Testergebnisse abzurufen, Anlagen zu steuern oder zu regeln sowie um verschiedene Arten von Fehlermeldungen aufzuzeichnen.

Technologie, Planung, Dimensionierung sowie die Bewältigung von Störungen und Interferenzen bei der Funkkommunikation unterscheiden sich wesentlich von der lokalen Kommunikation in einem Datennetzwerk.

Arbeitsweise

Zu den Kommunikationsausrüstungen gehört ein Funkmodem, das die Datensignale in Funkwellen für einen bestimmten Kanal mit einer bestimmten Bandbreite konvertiert. Es kann dabei erforderlich sein, das Datensignal vor der Übertragung auf dem Funkkanal zu bearbeiten oder zu filtern. Außerdem wird das Signal (von einem Modem) auf eine korrekte Trägerfrequenz aufmoduliert, die über eine Funkverbindung zum Empfänger übertragen wird. Unabhängig davon, ob die Quelle analog oder digital ist, erfolgt die Übertragung fast immer analog. Der Empfänger decodiert und rekonstruiert das Originalsignal.

Der verfügbare Frequenzbereich für Funkkommunikationen wird durch ein internationales Abkommen (ITU) begrenzt und geregelt.

Funkwellen breiten sich in der Atmosphäre in der Schicht zwischen der Ionosphäre und der Erdoberfläche aus. Die Kommunikationsbedingungen unterschieden sich sehr stark in Abhängigkeit von dem Frequenzband, das im ELF-Band von den längsten Wellenlängen bis 1.000 Metern (0,63 mi) bis zu den kürzesten von 10 mm (0,34 in) im EHF-Band reicht. Funkmodems arbeiten im UHF-Band bei etwa 440 mHz. Im UHF-Band zwischen 300 und 3 000 mHz senden außerdem Radar, Radio, TV, NMT mobile Telefonie, Mobilfunk, Satellitenkommunikation, Amateurfunk sowie GSM und schnurlose Telefone.

Frequenzband	
ELF	300 – 3000 Hz
VLF	3–30 kHz
LF	30–300 kHz
MF	300–3000 kHz
HF	3–30 MHz
VHF	30–300 MHz
UHF	300–3000 MHz
SHF	3–30 GHz
EHF	30–300 GHz

Dämpfung und Rauschen

Eine ausgesendete Funkwelle wird sowohl vom Boden als auch von den Luftschichten beeinflusst, die sie durchquert. In den Frequenzbändern, in denen Funkmodems arbeiten, also mit Wellenlängen von etwa 1 Meter (3.28 ft), befinden sich viele Objekte wie beispielsweise Hügel und Gebäude, die einen Funkschatten hervorrufen können (betrifft mobile Telefonie). Hinzu kommen sich überlagernde Interferenzen von anderen Ausrüstungen. Diese von Objekten verursachten Interferenzen und Funkschatten führen zu Signaldämpfungen oder Störungen.

Das am Empfänger ankommende Signal ist im Verhältnis zum ausgesendeten Signal oft sehr schwach, doch diese Tatsache an sich bewirkt noch keine Qualitätsverschlechterung der Kommunikation. Störungen und Rauschen, die dem Signal hinzugefügt werden und die nicht steuerbar sind, können Probleme verursachen. Dieses Problem tritt nicht nur in der Empfängerausrüstung auf, sondern existiert auch in Form von thermischen Störungen (thermische Bewegung von Partikeln), atmosphärischen Störungen (elektrische Phänomene wie Blitze), kosmischen Störungen (Funkfrequenzstrahlung von der Sonne oder das so genannte galaktische Rauschen) sowie von vor Ort erzeugten Störungen (elektrische Ausrüstungen in der Nähe des Empfängers).

Antennen

Terminologie

Zum besseren Verständnis von Funkkommunikation und Antennen wollen wir einige Fachbegriffe näher erläutern. Die erste wichtige Formel, die wir kennen müssen, definiert in der folgenden Gleichung das Verhältnis von Frequenz (f) zur Wellenlänge (l):
l [m] = 300 / f [MHz].

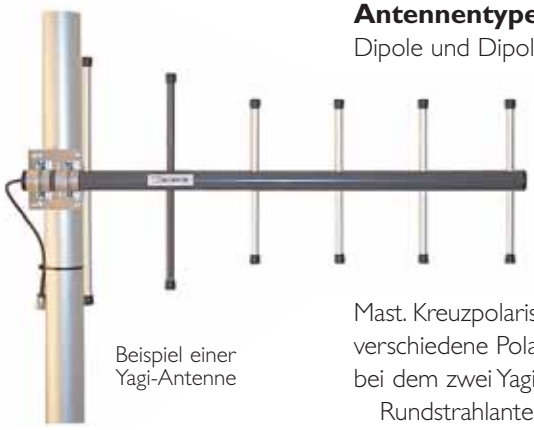
Das Strahlungsmuster ist die dreidimensionale Strahlungscharakteristik einer Antenne in zwei Ebenen, dem elektrischen Feld (E) und dem magnetischen Feld (H). Der Vorteil der Antenne besteht in ihrer Fähigkeit, die Strahlung in einer bestimmten Richtung auszusenden. Die Verstärkung wird in dB im Verhältnis zu Referenzwerten angegeben: so bezieht sich dBi auf eine Verstärkung im Vergleich zu einer Isotrop-Antenne und dBd auf eine Dipol-Antenne. Die Polarisation wird durch die Form des elektrischen Felds E der Antenne bestimmt, die vertikal, horizontal, schräg oder kreisförmig sein kann. Normalerweise entspricht die physikalische Ausrichtung der Antenne ihrer Polarisation. Rechtwinklige Polarisationen haben einen Kreuzpolarisationsverlust von 21 dB. In der Praxis sollten alle Antennen in einem System die gleiche Polarisation verwenden.

Die Impedanz einer Antenne ist ihr AC-Widerstand und ihre Reaktanz innerhalb des Frequenzbandes. Normalerweise beträgt die Impedanz 50 Ohm. Die Bandbreite ist der Frequenzbereich, in dem die Charakteristika der Antenne wie Impedanz, Verstärkung und Strahlungsmuster innerhalb der Spezifikationen liegen. Der häufig verwendete Begriff Dämpfung bezieht sich meist auf die Versorgungsleitungen sowie Funkverbreitung und wird ebenfalls in dB ausgedrückt.

Die Antenne und ihre Bauteile

Eine Antenne ist ein elektromechanisches Bauteil, dessen Aufgabe darin besteht, Signale möglichst wirkungsvoll auf eine bestimmte Art auszustrahlen.

Ein Leistungssplitter koordiniert und kombiniert mehrere Lasten oder Quellen und verteilt die Leistungen unter ihnen, ohne die charakteristische Impedanz des Systems zu verändern. Splitters werden in Antenneninstallationen zur Kombination mehrerer Antennen oder in Funkfrequenzverteilern eingesetzt. Zwischen der Funkausrüstung und der Antenne befindet sich ein Zuführkabel. In Versorgungsleitungen können erhebliche Verluste auftreten, daher muss man den Leitungstyp sorgfältig je nach benötigter Länge und genutzter Frequenz wählen. Zwischen der Funkausrüstung und der Versorgungsleitung können Blitzableiter installiert werden, um die Funkausrüstung vor Schäden durch Blitzeinschlag zu schützen. Ein Blitzschutz besteht typischerweise aus einem kurzgeschlossenen Schwingungsdämpfer. Bei der Verbindung der Bauteile des Antennenschaltkreises ist darauf zu achten, dass die Impedanz unverändert bleibt, um zusätzliche Leistungsverluste durch Reflexionen auszuschließen. Die Impedanzübereinstimmung wird normalerweise als VSWR (**V**oltage **S**tanding **W**ave **R**atio) gemessen, wobei ein VSWR von 1:1 ideal ist, aber 1:1,5 in der Praxis zumeist erzielt wird.



Beispiel einer Yagi-Antenne

Antennentypen

Dipole und Dipol-Antennen bestehen aus einer oder mehreren Dipol-Antennen und Splittern für die Kombination der Antennen. Dies sind typische rundstrahlende oder verzweigende Antennen.

Yagi und Yagi-Antennen bestehen aus einer oder mehreren Yagi-Antennen und Splittern für die Kombination der Antennen. Dies sind immer Richtantennen. Kreuzpolarisierte Yagi-Antennen sind eine Kombination aus zwei unabhängig versorgten, rechtwinklig polarisierten und physikalisch abgestimmten Viertelwellen-Yagi-Antennen am gleichen Mast. Kreuzpolarisierte Yagi-Antennen werden in Anwendungen eingesetzt, in denen verschiedene Polarisationen erforderlich sind oder im kreisförmigen Polarisationsmodus, bei dem zwei Yagi-Antennen mit einem Power-Splitter kombiniert werden.

Rundstrahlantennen können endgespeiste Halbwellenantennen, kollineare Antennen oder Erdantennen sein. Diese Antennen strahlen gleichmäßig in alle Richtungen ab.

Portable Antennen sind typischerweise flexible Viertelwellenantennen mit besonderen Versorgungsmethoden für eine korrekte Impedanzübereinstimmung mit kleinen tragbaren Funkgeräten.

Beispiel einer Dipolantenne

Signalausbreitung

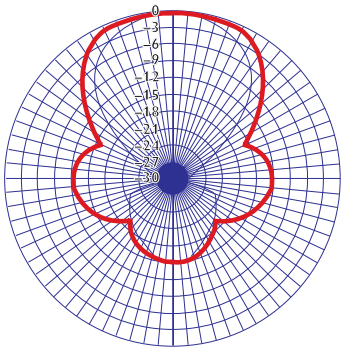
Funkwellen breiten sich hauptsächlich entlang der Landschaft aus, es kommt aber auch zu Krümmungen, Reflexionen und Beugungen. Typischerweise verbreiten sich Funkwellen gleichzeitig in verschiedenen Modi und Richtungen. Diese mehrfache Ausbreitung führt zu einer gewissen Signalinstabilität als einer Funktion der Zeit, da mehrere Signale mit unterschiedlichen Phasen gleichzeitig eintreffen. Dies erklärt auch, warum eine kleine physikalische Verschiebung der Antenne Auswirkungen auf die angezeigte Signalstärke haben kann.

Da Funkwellen zur Krümmung neigen, ist der Funkhorizont etwa 15 % weiter als der optische Horizont.

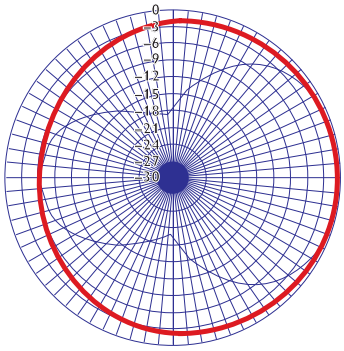
Funk-Netzwerk

Um zu ermitteln, ob auf der Empfängerseite genügend Leistung nach Ausstrahlung der Funksignale empfangen wird, sollte eine Kostenkalkulation der Funkverbindung erfolgen. Bei den Berechnungen einer Funkverbindung werden alle Parameter in dB ausgedrückt (plus oder minus) und zusammen addiert. Zu den bei der Berechnung einer Funkverbindung zu berücksichtigen Parametern zählen Entfernung, Frequenz, Terrain, Antennenhöhe, Empfängerempfindlichkeit, Speisekabelverluste, Antennenverstärkung und Ausstrahlungsverluste. Die Kostenberechnung einer Funkverbindung ergibt in beiden Richtungen das gleiche Resultat.

Die Reichweite eines Funknetzwerks kann durch den Einsatz von Relaissendern erhöht werden, die an geeigneten Positionen errichtet werden..



Yagi-
Dämpfungsdiagramm



Dipol-
Dämpfungsdiagramm

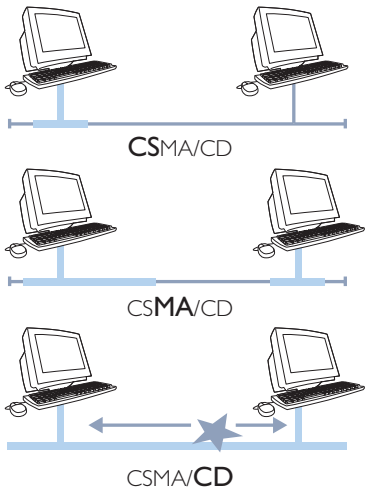
Das Ethernet in der Industrie

Ethernet existiert als Kommunikationsstandard seit vielen Jahren und bildet heute die Basis der meisten weltweiten Netzwerke. Obwohl im Lauf der Jahre oft gefordert wurde, Ethernet zu ersetzen, wird es ständig weiterentwickelt und bietet daher die Eigenschaften, die die Nutzer verlangen. In den letzten Jahren hat das Ethernet auch verstärkt in industriellen Anwendungen Akzeptanz gefunden.

IEEE 802.3 Ethernet

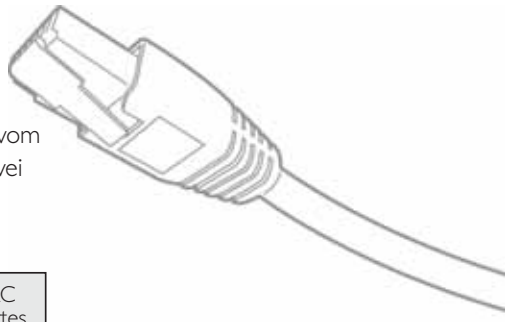
Zugangsmethoden

Damit zwei oder mehr Parteien miteinander kommunizieren können, ist ein Regelwerk erforderlich, dies gilt für alle Situationen, insbesondere jedoch für die Datenkommunikation. Wie die Daten auf eine Leitung übertragen werden, wird als Zugangsmethode bezeichnet. Die ursprüngliche Methode im Ethernet wurde als CSMA/CD bezeichnet. Dies bedeutet: **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect. Es ist wichtig festzuhalten, dass Ethernet zwei Zugangsmethoden verwendet, konstanter Zugang oder CSMA/CD. Auf CSMA/CD wird in der Fachliteratur regelmäßig verwiesen, wird heute jedoch nicht so häufig eingesetzt. Es hat jedoch eine gewisse historische Bedeutung, deshalb folgt hier eine kurze Beschreibung von CSMA/CD:



- **C**arrier **S**ense bedeutet, dass ein Einzelgerät vor dem Senden prüfen muss, ob jemand das Netzwerk nutzt. Falls dies der Fall sein sollte, muss das Gerät mit dem Senden warten.
- **M**ultiple **A**ccess bedeutet, dass jeder das Netzwerk nutzen kann, jedoch nicht simultan.
- **C**ollision **D**etect bedeutet, dass festgestellt werden muss, wenn zwei oder mehr Geräte gleichzeitig Daten übertragen. Bei Vorliegen einer Kollision wird ein Kollisionssignal gesendet und alle betroffenen Geräte stoppen den Sendevorgang. Alle Geräte warten dann eine nach dem Zufallsprinzip bestimmte Zeitspanne, bevor neue Versuche unternommen werden. Hierdurch wird verhindert, dass alle Geräte gleichzeitig versuchen, wieder zu senden. Diese Kollisionen führen selbstverständlich zu einer Verlangsamung des Datenverkehrs im System. In einem Netzwerk mit einer starken Auslastung gibt es viele Kollisionen, die wiederum zu mehr Datenverkehr im Netzwerk führen, die ebenfalls den Verkehr verstärken usw. Einige Anlagen sind mit LEDs zur Anzeige von Kollisionen ausgestattet, so dass man die Auslastung des Netzwerks leicht prüfen kann. Der Vorteil eines CSMA/CD-Netzwerks besteht darin, dass alle angeschlossenen Geräte jederzeit mit der Übertragung starten können, während die Übertragungen in einem Abfragesystem oder Token-Ring-Netzwerk strikt geregelt sind.

Ethernet-Adressen & Pakete



Jede Ethernet-Hardware hat eine Adresse, die jeden Knoten im Netzwerk eindeutig identifiziert. Diese Adresse wird normalerweise vom Hersteller bei der Produktion im Gerät, beispielsweise einer Netzwerkkarte, programmiert. Diese Adresse kann weder vom Nutzer noch mithilfe einer Software geändert werden. Dies bedeutet, dass es keine zwei Netzwerkkarten mit der gleichen Adresse geben kann bzw. geben darf. Diese Adresse wird meist als MAC **M**edia **A**ccess **C**ontrol Address bezeichnet.

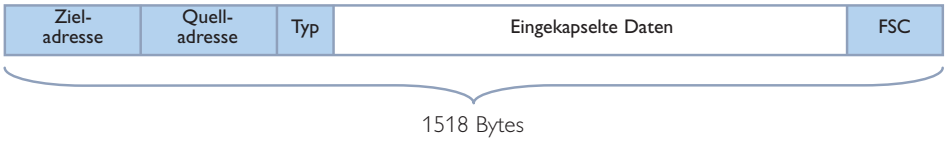
Präambel 8 Bytes	Zieladresse 6 Bytes	Quelladresse 6 Bytes	Typ 2 Bytes	Daten 46 – 1500 Bytes	CRC 4 Bytes

Das Ethernet-Paket besteht aus folgenden Informationen:

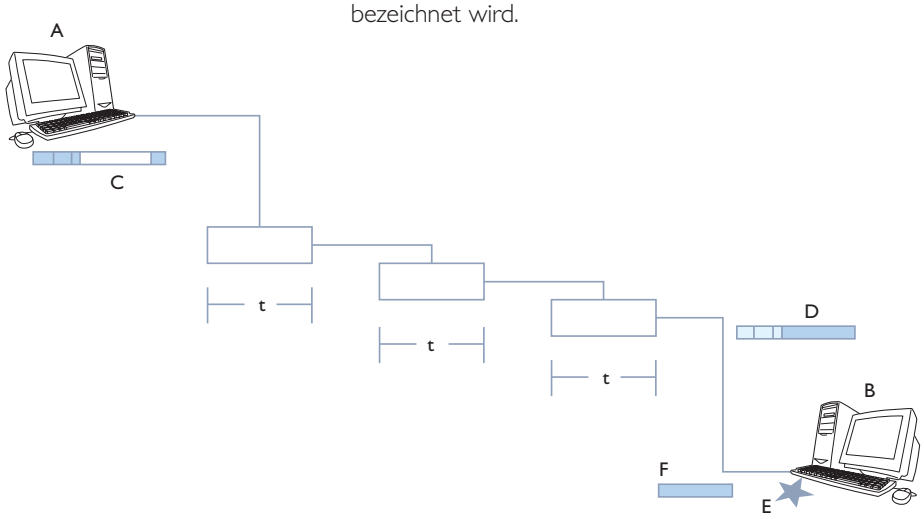
- **Präambel.** Die Präambel ist ein 64-Bit (8 Byte) Feld mit einem Synchronisationsmuster, das abwechselnd aus Einsen und Nullen und aus zwei aufeinanderfolgenden Einsen am Ende besteht. Nach Herstellung der Synchronisation wird die Präambel genutzt, um das erste Bit des Pakets zu lokalisieren. Die Präambel wird von der LAN-Schnittstellenkarte erzeugt.
- **Zieladresse.** Das Zieladressenfeld ist ein 48-Bit (6 Byte) Feld, das die Station oder die Stationen angibt, zu denen das Paket gesendet werden soll. Jede Station prüft dieses Feld, um zu ermitteln, ob sie das Paket akzeptieren soll.
- **Quelladresse.** Das Quelladressenfeld ist ein 48-Bit (6 Byte) Feld, das die eindeutige Adresse der Station enthält, die das Paket sendet.
- **Typenfeld.** Das Typenfeld ist ein 16-Bit (2 Byte) Feld, welches das dem Datenpaket zugewiesene höhere Protokoll identifiziert. Es wird auf der Data-Link-Ebene interpretiert.
- **Datenfeld.** Das Datenfeld enthält 46 bis 1500 Bytes. Jedes Oktett (8-Bit-Feld) enthält eine beliebige Sequenz von Werten. Das Datenfeld ist die Information, die vom Layer 3 (Netzwerk-Layer) empfangen wird. Die Information (oder das Paket), die vom Layer 3 empfangen wird, wird von Layer 2 in Informationsblöcke mit 46 bis 1500 Bytes zerlegt.
- **CRC-Feld.** Das Cyclic Redundancy Check (CRC) Feld ist ein 32-Bit Fehlerprüffeld. Das CRC wird in Abhängigkeit von Zieladresse, Typ und Datenfeldern erzeugt.

Collision Domain

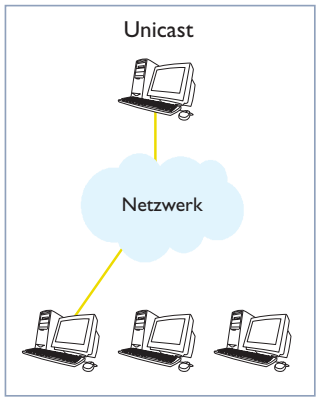
Eine Collision Domain ist ein Segment, in dem die angeschlossenen Geräte in der Lage sein müssen, Kollisionen (beispielsweise wenn mehrere Geräte simultan senden) zu erkennen und zu handhaben. Kollidierende Daten verschwinden nicht automatisch, sondern CSMA/CD stellt nahtlos und sorgfältig sicher, dass die Daten erneut übertragen werden. Die Anzahl der erneuten Übertragungsversuche kann auf 16 begrenzt werden und erst dann können Daten verloren gehen. Derartig viele erneute Übertragungsversuche gibt es jedoch nur in einem sehr stark überlasteten Ethernet-Netzwerk.



Ein Ethernet-Paket besteht aus 1518 Bytes, bei einem VLAN kommen weitere 4 Bytes hinzu, was insgesamt 1522 Bytes ergibt. Dies zusammen mit der Geschwindigkeit des Netzwerks entscheidet darüber, wie schnell die Mitteilung das am weitesten entfernte Gerät im Netzwerk erreicht. Unter keinen Umständen dürfen Kollisionsbereiche entstehen, bei denen das sendende Gerät eine Kollision nicht erkennen kann, bevor mit Sicherheit feststeht, dass das Datenpaket den Empfänger erreicht hat. Das Netzwerk und die installierten Ausrüstungen entscheiden über die maximale Ausbreitung von Kollisionsbereichen, da jedes Gerät eine Verzögerung produziert, die auch als Latenz bezeichnet wird.



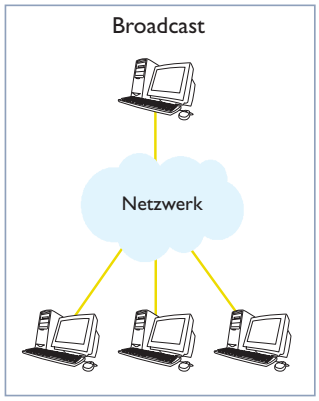
- Nehmen wir an, dass **A** ein Paket nach **B** senden möchte.
- Das Netzwerk enthält eine bestimmte Anzahl von Ausrüstungen mit der internen Verzögerung (**t**).
- **A** entleert kontinuierlich seinen Sendepuffer, wenn keine Kollision festgestellt wird.
- Am äußersten Knoten des Netzwerks (**E**) entsteht eine Kollision.
- Es werden nicht alle Daten (**D**) empfangen, was dazu führt, dass (**B**) sie nicht interpretieren kann.
- Das Kollisionssignal (**F**) wird an den Sender (**A**) zurückgesendet.
- Wenn die Domain zu groß ist, erreicht das Kollisionssignal (**A**) nicht rechtzeitig, und der Sendepuffer wurde bereits geleert. Damit ist es unmöglich, das Paket erneut zu senden.



IP-Netzwerke

Internet-Protokoll

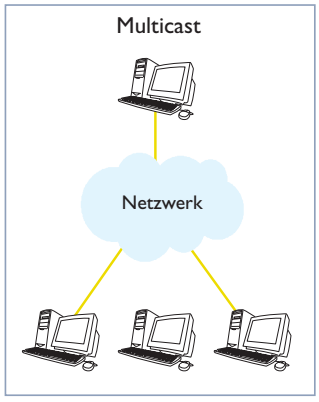
Das IP oder Internet-Protokoll ist für Verbindungen in einem Netzwerk oder zwischen mehreren Netzwerken bestimmt. Als die Spezifikation festgelegt wurde, war klar, dass kontinuierlich neue Technologien und neue Übertragungsmethoden entwickelt werden würden. Daher wurde ein offener Standard entwickelt, der primär von dem darunter liegenden Netzwerk und Medium unabhängig ist. TCP/IP ist die Protokollfamilie, die sich zwischen den vielen verschiedenen Ebenen im OSI-Modell ausbreitet.



Adressmethoden

Viele der Informationen in einem Netzwerk gehen von einem einzelnen Sender an einen einzelnen Empfänger. Dies ist in den meisten Fällen völlig selbstverständlich, beispielsweise wenn ein PLC mit einem I/O-Gerät kommuniziert. Diese Art der Übertragung wird normalerweise Unicast genannt.

Das Gegenteil von Unicast ist „Broadcast", also beispielsweise die Art, wie Radio und Fernsehen übertragen werden: ein Sender und viele Empfänger. Beim Broadcasting werden die Informationen an alle gesendet. Diese Technik wird auch in einigen geschlossenen Computernetzwerken verwendet. Broadcasting über das gesamte Internet ist jedoch unmöglich, da es das Netzwerk überlasten würde.



Multicast ist eine Technik, die zwischen Unicast und Broadcast liegt. Informationen werden nicht unterschiedslos an jeden wie beim Broadcasting gesendet und auch nicht an nur einen Empfänger wie beim Unicast, sondern an mehrere. Mit Multicast lassen sich Vertriebsnetzwerke errichten, die sich für die Videoüberwachung oder die Fernsehübertragung über das Internet eignen. Es handelt sich also um Informationen, die von einem Sender an mehrere Empfänger gehen. Multicasting eröffnet neue Möglichkeiten für das Internet und verhindert, dass es wegen Überlastung zusammenbricht.

Byte	1	2	3	4
	192	168	3	23

Adressen in einem Netzwerk

Bevor wir beschreiben, wie eine IP-Adresse aufgebaut ist, wollen wir einige Grundlagen erläutern:

- Eine IP-Adresse besteht aus vier Bytes.
- Ein Byte sind acht 8 Datenbits, beispielsweise 11000000, dies entspricht dem Dezimalwert 192, siehe Byte 1 in dem gegenüberliegenden Beispiel.
- Der Reihe nach werden die Adressen verschiedenen Klassen zugewiesen (A, B, C, D und E), wobei die Klasse ein Adressintervall beschreibt. Zurzeit gibt es fünf Adressklassen, von denen die ersten drei (A-C) für verschiedene Netzwerktypen verwendet werden, wobei die IP-Adresse in einen Netzwerkbereich und einen Computerbereich unterteilt ist. Es gibt also die Gruppen D und E. Eine D-Adresse ist eine Multicast-Adresse, und eine E-Adresse wurde für die zukünftige Nutzung reserviert.
- IP-Adressen in den Netzwerkklassen A, B und C sind in zwei Bereiche unterteilt, einen Netzwerkbereich und einen Computerbereich.

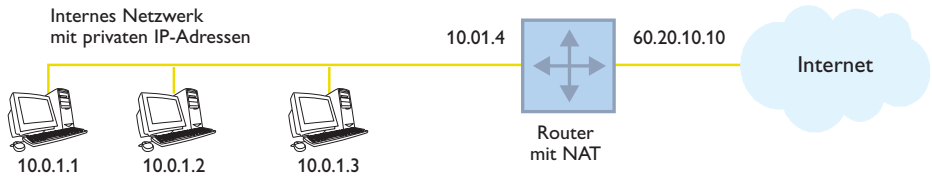
Klasse	Erstes Byte	Adress-Intervall
A	**0**xxx xxxx	**0**.0.0.0 to **127**.255.255.255
B	**10**xx xxxx	**128**.0.0.0 bis **191**.255.255.255
C	**110**x xxxx	**192**.0.0.0 bis **223**.255.255.255
D	**1110** xxxx	**224**.0.0.0 bis **239**.255.255.255
E	**1111** xxxx	**240**.0.0.0 bis **247**.255.255.255

A-, B- und C-Netzwerke unterscheiden sich in der Anzahl von Bits, die für die Netzwerk- und Geräteidentität verwendet werden:
Netzwerke der A-Klasse verwenden hierfür 8 Bits (1 Byte), die der B-Klasse verwenden 16 Bits und die C-Klasse nutzt 24 Bits. Dies ermöglicht die Adressierung verschiedener Geräte in den jeweiligen Netzwerken, siehe auch den Abschnitt Sub-Netzwerk weiter unten.

Klasse					Dezimal-Wert im Oktett 1	Max. Anzahl von Geräten im Netzwerk
A	Netzwerk	Computer	Computer	Computer	0 bis 127	16 777 215
B	Netzwerk	Netzwerk	Computer	Computer	128 bis 191	65 535
C	Netzwerk	Netzwerk	Netzwerk	Computer	192 bis 223	255

Private und öffentliche Adressen

Es gibt Situationen, in denen Sie die öffentlichen Adressen in Ihrem internen Netzwerk nicht nutzen können oder wollen. In diesen Fällen können Sie private IP-Adressen benutzen (RFC1918). Diese IP-Adressen funktionieren nicht bei einer Internetverbindung. Die Lösung lautet dann NAT (**N**etwork **A**ddress **T**ranslation).



Ein Router oder eine „Firewall" mit Unterstützung für NAT übersetzt private Adressen in öffentliche Adressen:
Wenn ein Computer mit der Adresse 10.0.1.2 auf das Internet zugreifen möchte, wird 10.0.1.4 adressiert. Dies ist die „vorgegebene Einfahrt" oder „way out". Wenn Daten von der Adresse 10.0.1.2 durch den Router passieren, übersetzt NAT die interne IP-Adresse 10.0.1.2 in 60.20.10.10, also eine IP-Adresse auf der „Außenseite". Dadurch kann eine interne IP-Adresse mit anderen Computern im Internet kommunizieren. Es spielt keine Rolle, wenn eine andere interne IP-Adresse zur gleichen Zeit kommuniziert, da der Router weiß, welche Sitzung zu welcher internen IP-Adresse gehört und sicher stellt, dass die Daten an den richtigen Computer im internen Netzwerk gelangen.

IANA (**I**nternet **A**ssigned **N**umbers **A**uthority) hat die folgenden drei Adressblöcke für IP-Adressen in privaten Netzwerken reserviert:
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Ipv4 und Ipv6

IPv6 ist die Version 6 des Internet-Protokolls, die neue Version wurde Ende der 1990er Jahre entwickelt, um IPv4 (Version 4) zu ersetzen, primär weil die IP-Adressen knapp wurden. Der größte Unterschied zwischen IPv6 und IPv4 besteht darin, dass die Adressenlänge von 32 Bits auf 128 Bits erweitert wurde. Dies bedeutet, dass die Anzahl der verfügbaren Adressen von vier Milliarden auf eine astronomische Anzahl erhöht wurde.

Ipv6 Kopfzeile

128 Bits-Quelladresse		
Nutzlastlänge	Nächste Kopfzeile	Sprunggrenze
128 Bits-Quelladresse		
128 Bits-Zieladresse		

Subnetzwerk-Unterteilung

Lokale Netzwerke mit mehreren hundert angeschlossenen Geräten sind selten. Wenn diese Art von Netzwerk seine eigene A- oder B-Klasse einrichtet (über 16 Millionen Netzwerke mit bis zu 65000 Geräten in jedem Netzwerk) wäre dies eine enorme Verschwendung von verfügbaren Adressen. Die meisten dieser Klassen werden daher in ein **Subnetzwerk** unterteilt, in dem ein Teil der Geräteidentität als Netzwerkadresse verwendet wird. Die Unterteilung erfolgt durch Nutzung eines Teils der Geräteidentität. Die „Grenze" zwischen der Netzwerkadresse und der Geräteidentität wird „verschoben", so dass die Nummer des verfügbaren Netzwerks erweitert und gleichzeitig die Anzahl von Geräten im Subnetzwerk abnimmt. Um dies zu erreichen, wird eine **Netzmaske** verwendet, in der die zum Netzwerkteil gehörigen Bits auf Eins (und die Computer-Bits auf Null) gesetzt werden.

Kleinere Netzwerke sind einfacher zu verwalten, der Datenverkehr im Subnetzwerk ist geringer, das physikalische Netzwerk lässt sich leichter einrichten und unterhalten (so kann man beispielsweise unterschiedliche Subnetzwerke auf verschiedenen Etagen in einem Gebäude nutzen) usw.

Die folgende Standard-Netzmaske (also ohne Subnetzwerk) gilt für die Adressen-Klassen A, B und C:

Adresse Klasse	Netzmaske	Binär-Wert Byte 1	Binär-Wert Byte 2	Binär-Wert Byte 3	Binär-Wert Byte 4
A	255.0.0.0	11111111	00000000	00000000	00000000
B	255.255.0.0	11111111	11111111	00000000	00000000
C	255.255.255.0	11111111	11111111	11111111	00000000

Wie bereits oben erläutert, besteht eine IP-Adresse der Klasse B aus zwei gleichgroßen Adressteilen, zwei Bytes für die Netzwerk- und Geräteidentität. Dies kann als N.N.G.G dargestellt werden, wobei N für das zur Netzwerkidentität gehörige Oktett steht und G die Geräteidentität darstellt, wodurch die Netzmaske 255.255.0.0. lautet.

Wenn das gesamte dritte Oktett für die Definition des Subnetzwerks statt für die Geräteidentität verwendet wird, kann die Adresse interpretiert werden als N.N.N.E, das heißt die Netzmaske lautet 255.255.255.0.
Dies bedeutet, wir haben 254 C-ähnliche Netzwerke mit jeweils 254 Computern in jedem Netzwerk (die erste und die letzte Adresse in den Netzwerk- und Computerbereichen sind reserviert).

Im Prinzip kann jedes Bit in einem Oktett zur Definition eines Subnetzwerks verwendet werden, normalerweise werden die höheren Bits dafür reserviert, da dies die Verwaltung erleichtert.
Wenn beispielsweise die ersten drei Bits in einer C-Adresse für die Subnetzwerk-Adressen verwendet werden, würde das C-Netzwerk in sechs Subnetzwerke unterteilt werden (siehe folgende mögliche Kombinationen von Netzwerken). Zwei Bit-Kombinationen der Geräteidentität (11111 und 00000) sind für Broadcast- und Netzwerkidentität reserviert. Daher beträgt die Anzahl der verfügbaren Adressen in jedem dieser Netzwerke 30.

Netzmaske	C- ähnliche Netzmaske	3 erste Bits in der C-ähnlichen Netzmaske	Andere Bits in der C-ähnlichen Netzmaske	Subnetz Arbeit	Anzahl von Geräte identitäten
255.255.32.0	32	001	00000	1	30
255.255.64.0	64	010	00000	2	30
255.255.96.0	96	011	00000	3	30
255.255.128.0	128	100	00000	4	30
255.255.160.0	160	101	00000	5	30
255.255.192.0	192	110	00000	6	30

Ports

Eine Anwendung empfängt Daten auf einer speziellen Portnummer, die die Kommunikation mit dieser Anwendung identifiziert.

So kann zum Beispiel ein Computer gleichzeitig ein Web-Server, E-Mail-Server und DNS-Server sein. Damit der Datentransfer zu den einzelnen Anwendungen nicht kollidiert, muss er aufgeteilt werden. Dies geschieht durch Zuweisung der Portnummer an die Anwendung. Die Portnummern zwischen 1 und 1024 sind bekannte Portnummern und dürfen ausschließlich von spezifizierten Anwendungen verwendet werden.

Beispiele für bekannte Portnummern sind:

21	ftp	Dateitransfer
23	Telnet	Telnet
25	smtp	Mail, Simple Mail Transfer
80	http	www

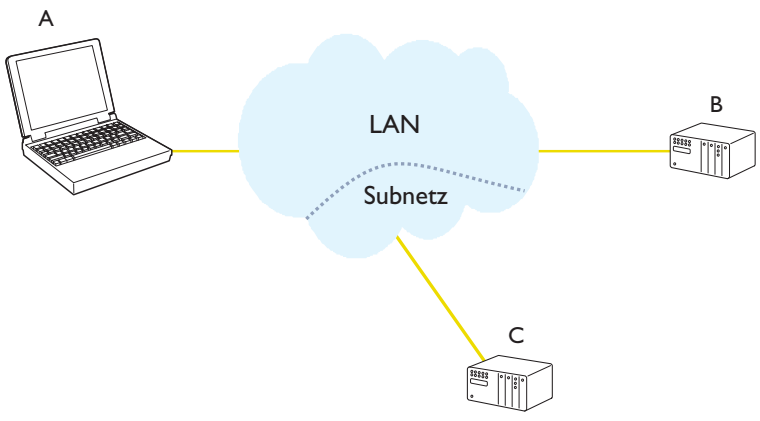
Eine komplette Liste finden Sie unter www.iana.org/assignments/port-numbers

MAC-Adresse

Dies ist die Abkürzung für Media Access Control-Adresse und bezeichnet eine Hardware-Adresse, die jeden Knoten in einem Ethernet-Netzwerk eindeutig identifiziert. Diese Adresse wird normalerweise vom Hersteller bei der Produktion im Gerät, beispielsweise einer Netzwerkkarte, programmiert. Diese Adresse kann weder vom Nutzer noch mithilfe einer Software geändert werden. Dies bedeutet, dass es keine zwei Netzwerkkarten mit der gleichen MAC-Adresse geben kann bzw. geben darf.

ARP

Computer oder andere Hardware, die mit einem TCP/IP–Netzwerk verbunden sind, haben mindestens eine IP-Adresse. Die IP-Adresse ist auch bekannt als die logische



Adresse, wird normalerweise in Software implementiert und kann je nachdem, wo sich die Hardware im Netzwerk physikalisch befindet, geändert werden. Die Geräte haben außerdem eine physikalische Adresse, die in einem Ethernet-Netzwerk MAC-Adresse genannt wird und bei jeder angeschlossenen Hardware einzigartig ist.

Wenn zwei Geräte (A) und (B) TCP/IP zur Kommunikation über das Ethernet nutzen, müssen sie die MAC-Adresse des jeweils anderen Geräts kennen, da sämtliche Kommunikation in einem Ethernet über die MAC-Adressen erfolgt.
Daher haben die Geräte A und B ihre eigene ARP-Tabelle mit IP-Adressen und entsprechenden MAC-Adressen.
Das ARP **A**ddress **R**esolution **P**rotocol managt eine dynamische Aktualisierung der ARP-Tabellen, so dass die Zuordnung zwischen IP- und MAC-Adressen immer bekannt ist.

- Nehmen wir an, dass Computer (A) mit dem PLC (B) kommunizieren will. Computer (A) kennt bereits die IP-Adresse von (B) (sie kann beispielsweise manuell von einem Administrator konfiguriert worden sein), aber (A) kennt die MAC-Adresse von (B) nicht. Kommunikation kann erst dann stattfinden, wenn (A) die MAC-Adresse von (B) kennt.
- Durch Vergleich der IP-Adresse des Ziels mit der Netzwerk-Maske erkennt (A), dass (B) sich im gleichen Netzwerk befindet.
- (A) sendet eine ARP-Anfrage in Form einer Broadcast-Mitteilung. Die Anfrage enthält die IP- und MAC-Adresse von (A) sowie die IP-Adresse von (B).
- Alle Einheiten im Netzwerk verstehen die Mitteilung, aber nur (B) erkennt seine IP-Adresse und sendet eine ARP-Antwort mit der MAC-Adresse von (B) zurück.
- Die ARP-Tabelle von (A) kann jetzt mit der MAC-Adresse von (B) aktulisiert werden.

Point-to-Point (PPP)

Es gibt auch Situationen, in denen man TCP/IP über einen seriellen Anschluss zur Verbindung und Kommunikation nutzt. Dies betrifft Verbindungen ins Internet über ein Modem oder den Anschluss an ein LAN (local area network). Die Art der Kommunikation variiert von Anwendung zu Anwendung. In diesen Fällen benutzt man das PPP-Protokoll (**P**oint to **P**oint **P**rotocol), dies ist zweifellos das am häufigsten verwendete Verbindungsprotokoll für Computer, die sich an ein entfernt liegendes Netzwerk anschließen. Beispiele der seriellen Kommunikation sind: Telefonmodem, Modem mit eigener Standleitung, ISDN, GSM, Funk- oder Kurzstreckenmodems.

Sicherheit (CHAP und PAP)

Das PPP-Protokoll wird häufig für entfernte Punkt-zu-Punkt-Verbindungen genutzt, unabhängig davon, ob es sich um eine Telefon-, ISDN- oder gemietete Standleitung handelt. Grundsätzlich ist eine Form von Sicherheit zwischen den Kommunikationspartnern erforderlich. PPP unterstützt zu diesem Zweck zwei Methoden der Nutzerprüfung, PAP (**P**assword **A**uthentication **P**rotocol) und CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol). Authentifikation und die Prüfung von Mitteilungen sind im PPP nicht zwangsläufig, die Parteien können daher ohne Identifizierung oder Verhandlung darüber, welches Protokoll verwendet werden soll, frei miteinander kommunizieren.
Als grundsätzliche Regel wird CHAP zuerst gewählt. PAP wird grundsätzlich nur dann gewählt, wenn eine der Parteien CHAP nicht unterstützt.
PAP arbeitet ähnlich wie das Einloggen eines Nutzers an einem Terminal, man gibt Nutzernamen und Passwort ein. Die Authentifikation findet nur beim Verbindungsaufbau statt und niemals bei laufender Kommunikation.

- Das PAP-Procedere wird von einer der Parteien durch Senden einer Authentifikationsanfrage mit Name und Passwort gestartet. Dieses Paket wird wiederholt gesendet, bis die Gegenpartei antwortet.
- Wenn Name und Passwort akzeptiert werden, antwortet der Empfänger mit einer Authentifikationsbestätigung. Anderenfalls wird eine Authentifikations-Verneinung gesendet und der Empfänger unterbricht die Verbindung.

Da Name und Passwort im Klartext über die Verbindung gesendet werden, ist PAP eine ziemlich ungeschützte Authentifikationsmethode. Das Passwort kann einfach durch Anzapfen ermittelt werden, und es gibt keinen Schutz gegen wiederholte Angriffsversuche.

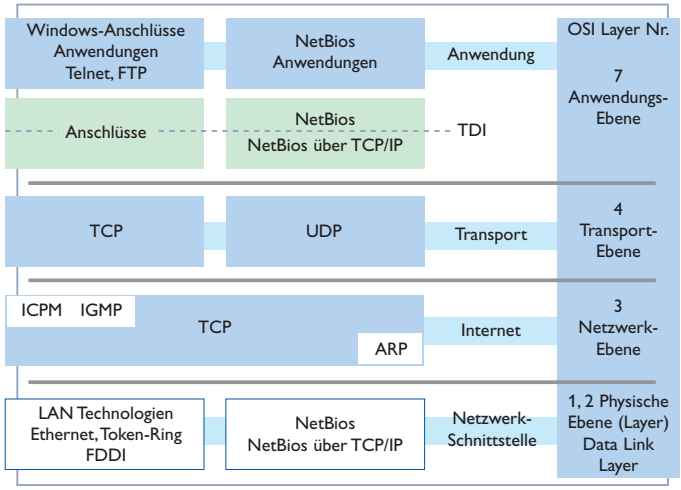
CHAP bietet im Vergleich mit PAP eine bedeutend verbesserte Sicherheit

CHAP nutzt ein verschlüsseltes Passwort in einem dreistufigen Verfahren. Außerdem findet die Authentifikation teilweise statt, wenn die Verbindung aufgebaut ist und kann daher jederzeit wiederholt werden. Durch die periodische Wiederholung reduziert man den Zeitraum, in dem das System offen für Angriffe ist. Der Empfänger, der die Authentifikation vornimmt, bestimmt dabei immer, wie oft die Authentifikation erfolgt. Die drei Stufen der Authentifikation sind:

- Wenn die Verbindung hergestellt ist, sendet eine der Parteien (die die Authentifikation vornimmt) eine Anfrage an die andere.
- Die andere Partei berechnet einen verschlüsselten Wert auf der Basis der Anfrage und seinem Passwort und sendet den verschlüsselten Wert zurück.
- Die die Authentifikation vornehmende Partei nimmt eine entsprechende Berechnung vor (die Anfrage und das Passwort der anderen Partei sind bekannt) und vergleicht die beiden Werte. Wenn die Werte identisch sind, wird die Authentifikation bestätigt, anderenfalls wird die Verbindung unterbrochen.

TCP/IP und UDP/IP

Im OSI-Modell ist jede Ebene für die Daten verantwortlich, die durch sie hindurchgeleitet werden. Die Transportebene trägt die Verantwortung für den Datentransfer. Hierfür gibt es zwei alternative Protokolle, TCP und UDP.



UDP

Das UDP (**U**ser **D**atagram **P**rotocol) wird normalerweise als verbindungsloses Protokoll bezeichnet. Dies bedeutet, dass die Daten gesendet werden können, unabhängig davon, ob der Empfänger existiert oder nicht. Der Empfänger sendet keine Bestätigung zum Sender, dass die Daten empfangen wurden. Da die Daten ohne hergestellte Verbindung übertragen werden, ist der Transfer effektiver und oft auch schneller. UDP wird daher in Anwendungen eingesetzt, die eine effiziente Nutzung der Bandbreite erfordern und in denen eine Anwendung die erneute Übertragung bei Datenverlusten unterstützen.

Man kann UDP mit einem Brief vergleichen, die Daten werden in einen adressierten Umschlag gelegt. Nachdem Sie den Brief in den Briefkasten geworfen haben, erwarten Sie, dass die Post den Brief korrekt zustellt. Eine weitere wichtige Funktion von UDP ist die Möglichkeit, „Broadcast"- und „Multicast"-Sendungen zu verschicken, also eine Nachricht an mehrere Empfänger. Dies ist der wichtigste Grund für die Wahl von UDP.

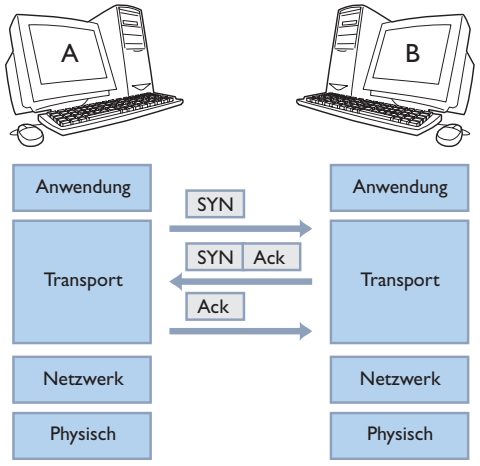
TCP

TCP (**T**ransmission **C**ontrol **P**rotocol) ist ein verbindungsorientiertes Protokoll, das heißt, es wird eine Verbindung hergestellt, bevor die Geräte Daten austauschen. TCP übernimmt eine größere Verantwortung für den Datentransfer als UDP, da der Empfang der übertragenen Daten vom Empfänger bestätigt wird. Für jedes gesendete Datenpaket muss der Empfänger eine Bestätigung (acknowledgement – ACK) zurücksenden. Wird kein ACK empfangen, werden die Daten erneut übertragen. Dies gewährleistet, dass der Empfänger die Daten auch wirklich erhält.

Eine weitere Funktion von TCP ist die Sequenz- und Flusssteuerung des Protokolls bei der Übertragung von großen Datenmengen. Mehrere TCP-Pakete können den Empfänger in einer anderen Reihenfolge erreichen, als sie abgeschickt wurden. TCP gewährleistet, dass die Pakete in der korrekten Sequenz zusammengesetzt werden, da sie eine Sequenznummer enthalten. Wegen der Notwendigkeit, eine Verbindung herzustellen und eine Bestätigung des Transfers abzuwarten, benötigt TCP mehr Zeit für die Datenübertragung als UDP, außerdem nutzt TCP eine größere Bandbreite.

Aufbau einer TCP-Verbindung

Mithilfe einer Handshake-Prozedur wird in drei Schritten eine Verbindung aufgebaut:



- Der Client A sendet eine Verbindungsanfrage mit dem SYN-Bit. Dies ermöglicht es dem Client, eine Sequenznummer mit dem Server (B) zu synchronisieren.
- Server (B) bestätigt (ACK) den Client mit seinem SYN-Bit, und damit hat der Server ebenfalls seine Sequenznummer mit dem Client synchronisiert.
- Schließlich bestätigt der Client mit (ACK).

Der Transfer erfolgt mit einem oder mehreren Bytes, die nummeriert und bestätigt werden.

Eine Verbindung wird beendet, wenn der Client (A) das lokale TCP-Paket prüft und alle Informationen gesendet und bestätigt wurden. Dann wird ein TCP-Paket mit dem FIN-Bit gesendet. Der Server (B) bestätigt dies, sendet aber weiterhin Daten, wenn die Anwendung dies verlangt. Wenn dies beendet ist, sendet der Server (B) ein TCP-Paket mit dem FIN-Bit.

Aufbau eines Netzwerks

Geräte in einem Netzwerk

Repeater

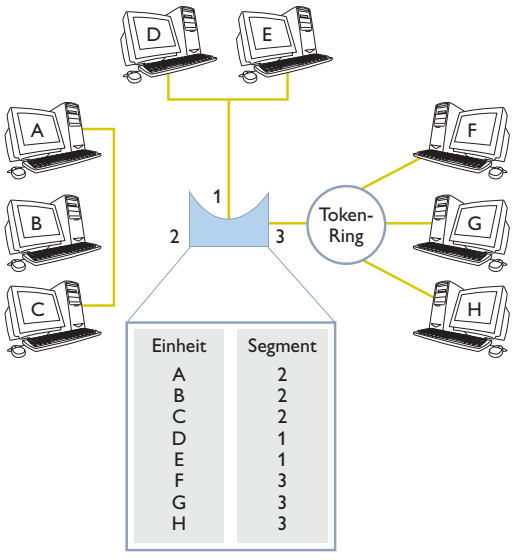
Ein Repeater kann mit einem Verstärker verglichen werden, er verfügt über keine intelligenten Funktionen sondern wiederholt nur Signale. Signale werden abhängig von der Länge des Übertragungsmediums und der Signalfrequenz gedämpft. Deshalb haben Netzwerke nur eine begrenzte Reichweite. Mit einem Repeater kann man ein Übertragungsmedium verlängern, indem man das Signal wiederholt, wobei jedoch genau darauf zu achten ist, dass seine Stärke und Form dabei nicht verändert werden. Ein Repeater arbeitet im gleichen Kollisionsbereich (HDPX CSMA/CD), und aufgrund der zusätzlichen Latenz in jedem Repeater kann in einem Segment nur eine begrenzte Anzahl von Repeatern installiert werden.

Bridge

Eine Bridge trennt zwei oder mehr separate Kollisionsbereiche und kann verwendet werden, um verschiedene Topologien miteinander zu verbinden. Die Bridges ermitteln und speichern, welche Adressen zu den jeweiligen Bereichen gehören. Daher lernen sie, welche Bereiche bzw. Geräte angeschlossen sind.

Eine Bridge wird beispielsweise genutzt, um Ethernet mit Token-Ring-Netzwerken zu verbinden. Bridges arbeiten normalerweise selektiv, das heißt sie filtern Adressen, so dass die Daten nur die Zieladresse erreichen. Wenn zum Beispiel die Geräte A und B nur im Bereich 2 kommunizieren, wird das Netzwerk aufgeteilt und der interne Datenverkehr belastet die anderen Bereiche nicht.

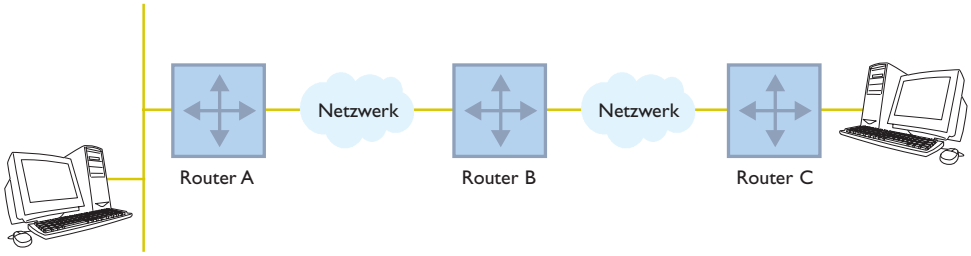
Eine Bridge funktioniert auf der Ebene des MAC-Verkehrs, die nur mit physikalischen Adressen arbeitet. Ein Router hingegen trifft seine Entscheidungen auf der Basis der Layer-3-Adressen.



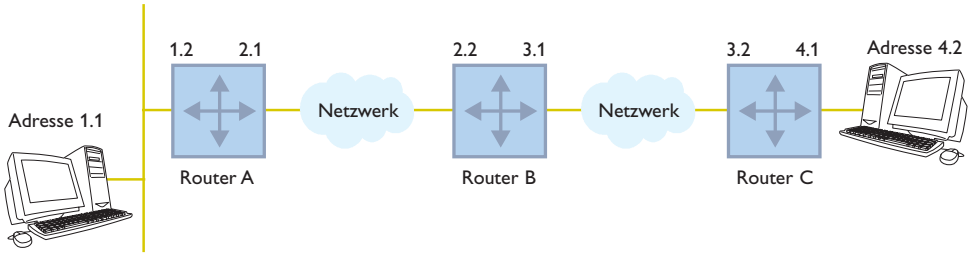
Einheit	Segment
A	2
B	2
C	2
D	1
E	1
F	3
G	3
H	3

Router

Das englische Verb ‚route' bedeutet so viel wie den richtigen Weg wählen oder finden. Ein Router ist ein Gerät, oder in einigen Fällen eine Software in einem Computer, das entscheidet, wohin ein Datenpaket auf seinem Weg zum Empfänger geschickt werden soll (aus der Perspektive eines LAN ist der Router die Endstation). Daher ist ein Router ein Netzwerkgerät, das zwei oder mehr logisch getrennte Netzwerke verbindet. Er verbindet die Netzwerke nicht blind, sondern funktioniert eher wie ein Paketschalter für die Verbindung lokaler Netzwerke über kurze oder lange Entfernungen. Je nach den in den separaten Netzwerken installierten Ausrüstungen kann das Netzwerk auch verschiedene Topologien und Standards nutzen.



Da alle Geräte eine eindeutige Adresse haben, kann die sendende Ausrüstung immer einen speziellen Empfänger im eigenen oder fremden Netzwerk adressieren. Wenn ein Empfänger in einem anderen Netzwerk adressiert ist, werden die Daten in geeigneter Weise durch die logische Verbindung zwischen den Netzwerken geleitet. Diese Information wird in einer Routing-Tabelle gesammelt, die die Route sowie alternative Verbindungsmöglichkeiten definiert.



Im nebenstehenden Beispiel zeigen wir eine vereinfachte Adressiertechnik. Die Netzwerkadressen lauten 1, 2, 3 oder 4. Die Geräte im gleichen Netzwerk haben die Adressen 1.1, 1.2 usw.

Nehmen wir an, dass der Computer mit der Adresse 1.1 mit dem Computer bei 4.2 kommunizieren will. Router A empfängt ein Paket, das an 4.2 adressiert ist und erkennt, dass die Adresse zu einem anderen Netzwerk gehört. Daher leitet er das Paket weiter, in diesem Fall an 2.1 und an 2.2. Die gleiche Prozedur erfolgt zwischen den Routern B und C. Schließlich erreicht das Paket Router C und wird an das Netzwerk 4 an den Computer mit der Adresse 4.2 geleitet.

Neben dem Verteilen des Datenverkehrs besteht auch die Möglichkeit, den Verkehr zu kontrollieren und zu filtern. In einer Routing-Tabelle ist aufgelistet, wo sich die

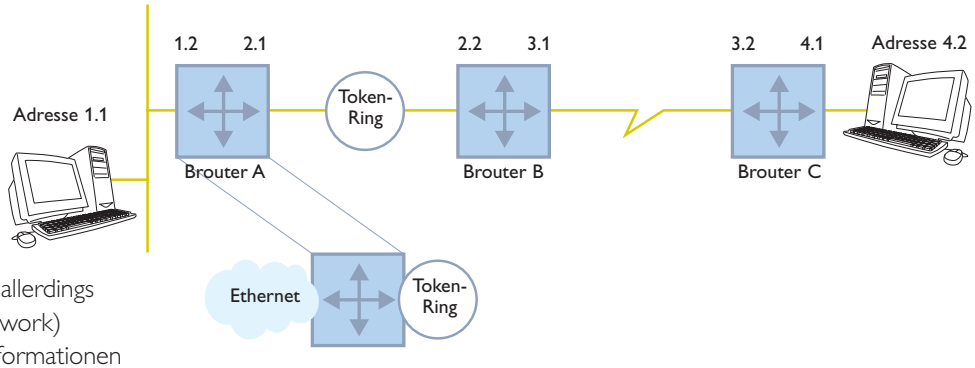
verschiedenen Geräte und Netzwerke befinden. Eine derartige Tabelle kann dynamisch oder statisch sein. Eine dynamische Tabelle wird automatisch auf Basis der Umgebungsstrukturen aktualisiert.

Die Weiterleitung des Datenverkehrs wird durch ein Routing-Protokoll gesteuert, z. B. durch RIP (**R**outing **I**nformation **P**rotocol) oder OSPF (**O**pen **S**hortest **P**ath **F**irst).

Brouter

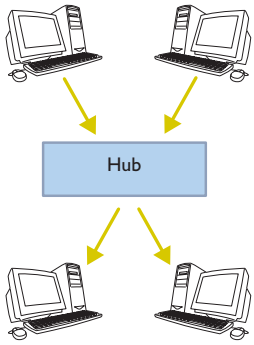
Es gibt zahlreiche Standards auf dem Markt, zu den verbreitetsten gehören Ethernet, Token-Ring und FDDI. Diese Standards nutzen verschiedene Kommunikationstechniken und Formate, wobei die Adressierung jedoch gleich und durch IEEE standardisiert ist.

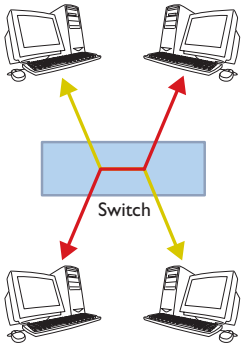
Ein Brouter ist eine Kombination aus Bridge und Router in einem Gerät, wobei viele Router eigentlich Brouter sind. Wenn das Gerät das gleiche Protokoll innerhalb eines LAN oder an ein anderes LAN übertragen muss, erfolgt dies mit der Bridge-Funktion. Wenn ein PC allerdings an ein WAN (**W**ide **A**rea **N**etwork) angeschlossen ist, sind mehr Informationen über alternative Verbindungen erforderlich. Das Gerät benötigt also eine Routing-Tabelle, und in diesem Fall wird der Brouter zu einer Kombination aus Router und Bridge.



Hub

Wie der Name andeutet, handelt es sich hierbei um ein Netzwerkgerät, das als zentrale Verbindung zu einem Netzwerk dient. Ein Hub arbeitet als sternförmiges Kupplungslied für den Netzwerkverkehr. An einem Port eingehende Daten werden unabhängig davon, wer der Empfänger ist, an alle anderen gesendet. Der Hub ist das Netzwerkgerät, das 10baseT zum Erfolg verhalf. Er eröffnete völlig neue Optionen für den Aufbau von Netzwerken mit zentral angeordneten Ausrüstungen und Anschlusspunkten an jedem Arbeitsplatz. Es gibt zwei Typen von Hubs, aktive und passive. Ein passiver Hub verbindet Netzwerksegmente oder Verstärkung des Signals. Ein aktiver Hub funktioniert ebenso, verstärkt aber das Signal.





Switch

Ein Switch arbeitet ähnlich wie ein Hub als zentraler Anschlusspunkt des Netzwerks. Der Unterschied zwischen den beiden besteht darin, dass ein Switch ermittelt, welche Geräte an seine jeweiligen Ports angeschlossen sind. Wenn Daten an ein Gerät in einem Netzwerk gesendet werden, wird die Empfängeradresse vom Switch geprüft, und die Daten werden nur an den Port gesendet, an dem das Gerät angeschlossen ist (switches network). Dadurch wird das Netzwerk nicht mit unnötigem Datenverkehr überlastet. Ein weiterer Vorteil ist die erhöhte Sicherheit, da es schwieriger ist an Informationen zu gelangen, die nicht für den betreffenden Computer bestimmt sind.

Ein Layer 2 Switch ist eine Art Bridge.

Ein Layer 3 Switch ist eine Art Router.

Konsequenterweise werden die Begriffe Switch, Bridge und Router in einigen Zusammenhängen als Synonyme verwendet.

"Managed" und "unmanaged" Switches sind andere, häufig verwendete Begriffe. Der Unterschied besteht darin, dass man mit einem managed (überwachbaren) Switch kommunizieren kann, was normalerweise mit SNMP erfolg, siehe auch die Seiten 138 bis 143.

Gateway

Ein Gateway verbindet Netzwerke miteinander, aber seine Hauptaufgabe besteht darin, Daten zwischen verschiedenen Protokollen zu konvertieren, beispielsweise zwischen AppleTalk und TCP/IP. Neben dem Konvertieren von Protokollen unterstützt ein Gateway außerdem verschiedene Formate, Zeichencodes, Adressen usw.

Firewall

Eine Firewall ist eine Spezialausrüstung oder Software, die Daten nur dann weiterleitet, wenn bestimmte Anforderungen erfüllt wurden, anderer Datenverkehr wird zurückgewiesen. Damit können Nutzer in einem Netzwerk vor unerlaubten Zugriffen geschützt werden. Normalerweise befindet sich eine Firewall zwischen einem lokalen Netzwerk und dem Internet. Man kann Firewalls auch in einem internen Netzwerk oder zusammen mit Geräten installieren, die den Zugang zu einem Netzwerk ermöglichen. Es gibt eine Vielzahl von komplexen Regeln, die festlegen, welche Daten die Firewall durchlässt. Wann, wo und wie eine Firewall eingesetzt wird, ist abhängig von den an ein Netzwerk gestellten Sicherheitsanforderungen. Es gibt eine Vielzahl von Produkten auf dem Markt: Kombinationen von Hardware und Softwarelösungen sowie Firewalls die kostenlos im Internet heruntergeladen werden können.

Hub oder Switch

Warum ist ein Switch deutlich besser als ein Hub und worin besteht der Unterschied zwischen den beiden Produkten? Wir haben bereits erläutert, dass der Hub die Installation von sternförmigen Netzwerken ermöglichte und zusammen mit dem Ethernet strukturierte Kabelsysteme populär machte. Ein Hub hat keine aufwändige Konstruktion, alle an einen Port gesendeten Daten werden an die anderen Ports geleitet. Die bedeutet, dass jeder hört, was jeder sendet und dass sich alle im gleichen Kollisionsbereich befinden.

Ein Switch mit seinen Prozessoren und maßgeschneiderten integrierten Schaltkarten ist deutlich intelligenter. Dies ermöglicht die Kontrolle und Verarbeitung von Daten, die an einem Port empfangen werden. Ein Switch lernt, welche Geräte an welchem Port angeschlossen sind und speichert dies im eigenen MAC-Adressenspeicher. Es gibt zwei Switch-Typen: „Cut-through" und „Store-and-forward". Der Cut-through-Switch prüft die Empfängeradresse und sendet die Daten an den Empfangsport. Dies führt zu einer Kollision, wenn der Port von anderem Datenverkehr genutzt wird, wobei das letzte Datenpaket verloren geht. Die Switches sind sehr schnell. Der Store-and-forward-Switch kopiert das erhaltene Paket und stellt es in einen Puffer, bevor er den Empfangsport lokalisiert und sendet erst dann, wenn der Port frei ist. Folglich geht kein Paket verloren. Daten können auch vorgezogen werden, das Netzwerk kann in virtuelle LANs unterteilt werden usw.

Die folgende Liste beleuchtet einige Unterschiede zwischen Hub und Switch.

Hub	Switch
Halbduplex-Kommunikation.	Halbduplex oder Vollduplex (HDX/FDX).
Erweitert den Kollionsbereich.	Segmentiert das Netzwerk.
Das gesamte Netzwerk teilt sich die Bandbreite.	Bandbreite wie erforderlich (selbstlernendes System).
Geringe Bandbreitennutzung wegen CSMA/CD.	Speichern und weiterleiten (Kontrolle des Pakets vor dem Weiterleiten).
Schneller als ein Switch (geringere Latenz).	Lernt MAC-Adressen (wer ist wo angeschlossen).
	Alte Adressen sind vergessen (Time-out im MACAdressenspeicher).
	Flusssteuerung für FDX und HDX.
	Paketpuffer auf Portebene.
	QoS, Prioritätensetzung von Daten (Daten mit hoher Priorität stehen am Pufferspeicher).
	Virtuelles Netzwerk VLAN (verbindet spezielle Ports virtuell).
	Gbit-Switches (leistungsstarke Switches mit hoher Kapazität).

Der Vorteil, den wir normalerweise hervorheben, besteht darin, dass ein Switch das Netzwerk segmentiert (switched Ethernet), wodurch Kollisionen verhindert werden.

Unterschiedliche Arten von Switches

Je nach den Anforderungen von Anwendung und Installation gibt es zahlreiche unterschiedliche Switches. Zuerst unterscheiden wir nach den Schnittstellen, es gibt TX (Kupfer) und FX (Glasfaser). Andere Varianten sind managed/unmanaged Switches, dies bedeutet, es gibt die Möglichkeit der Kommunikation und Überwachung des Switch mit SNMP oder es gibt sie nicht. Schließlich unterscheiden wir zwischen Ringswitches und zeitsynchronisierten Switches, die beim Aufbau eines Ringnetzwerks mit Redundanz oder für ein Netzwerk mit der Erfordernis von Zeitsynchronisation verwendet werden.

FRNT und Spanning Tree

Komplexe Netzwerke mit hohen Anforderungen an die Redundanz müssen bei Auftreten eines Netzwerkfehlers die Möglichkeit zur Rekonfiguration haben.

Die Rekonfiguration wird vom Switch ausgeführt, das heißt, der Switch muss erkennen, dass ein Verbindungsfehler aufgetreten ist. Dies kann auf unterschiedliche Weise erfolgen, standardisierte Lösungen sind beispielsweise IEEE **S**panning **T**ree **P**rotocol (STP) oder **R**apid **S**panning **T**ree **P**rotocol (RSTP). Das Spanning Tree Protocol erzeugt eine Verbindung durch das Netzwerk und eliminiert gleichzeitig unerwünschte Schleifen im Netzwerk. Redundanz wird erzielt, indem das Protokoll der Baumstruktur innerhalb des Netzwerks aufrechterhält, wobei einige Verbindungen blockiert werden (in den Stand-by-Modus versetzt werden). Wenn ein Segment nicht gelesen werden kann, wird das Netzwerk mit Hilfe des Spanning Tree Algorithmus rekonfiguriert, wodurch die im Stand-by stehenden Verbindungen aktiviert werden. Die Rekonfiguration eines STP-Netzwerks kann bis zu 30 Sekunden dauern, da neue Bedingungen berechnet und die Switches aktualisiert werden müssen. Diese Berechnung ist komplex, da das Netzwerk keine festgelegte Topologie hat. RSTP ist eine Weiterentwicklung von STP mit schnellerer Rekonfiguration, die statt 30 Sekunden nur noch 5 Sekunden dauert.

Außerdem gibt es speziell entwickelte Lösungen wie **F**ast **R**ecovery **N**etwork **T**opology (FRNT), die in unserem Ringswitch R200 sowie dem zeitsynchronisierten Switch T200 verwendet werden. FRNT ist eine patentierte Lösung, die ein Netzwerk im extreme kurzen Zeitraum von 30 ms rekonfiguriert. Dies ist möglich, da die Switches die Netzwerkkonfiguration kennen, die ebenfalls eine Ringtopologie hat. Außerdem ist die Rekonfiguration ereignisgesteuert, „Leerlauf-Verkehr" wird zwischen jedem Gerät im Ring hin- und hergeschickt, um zu ermitteln, ob die Verbindung besteht. Wenn ein Fehler erkannt wird, erhält der Brennpunkt (Ringmaster) sofort eine Information, der daraufhin das Netzwerk rekonfiguriert.

Ringswitch

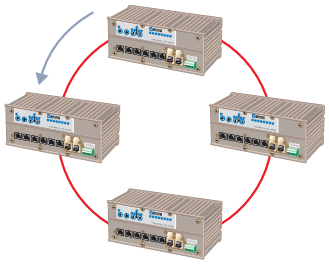
Unsere Ringswitches sind in zwei Ausführungen erhältlich, für Basis-Ringnetzwerke und für Ringnetzwerke mit Bridges. Die Modelle haben unterschiedliche Software für die Rekonfiguration, FRNT0 und FRNT1.

FRNT0

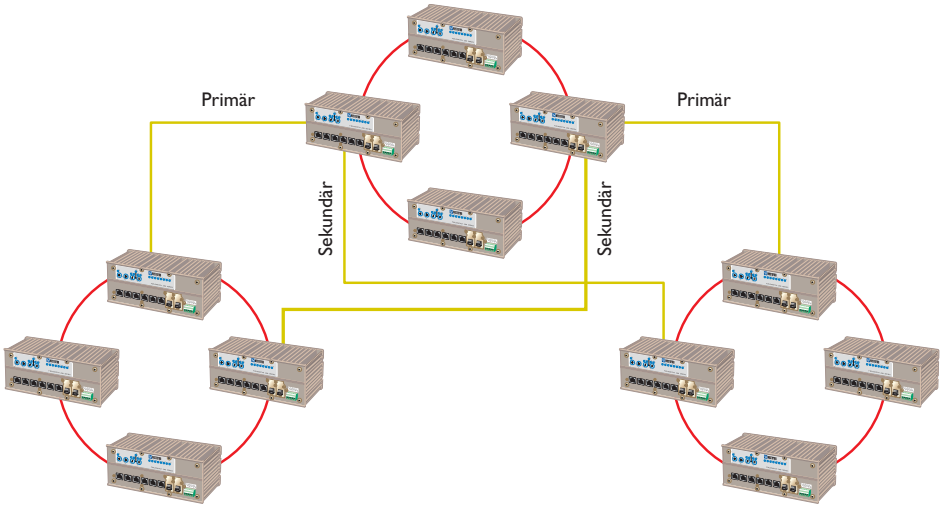
Es gibt immer zwei alternative Richtungen für den Verkehr in einem Ring: rechts herum oder links herum. Ein Ringswitch nutzt diese Möglichkeit und verhindert dadurch Netzwerkfehler. Wenn ein Fehler auftritt, wird der Switch, der als Brennpunkt konfiguriert ist, informiert. Er rekonfiguriert darauf hin das Netzwerk, so dass jeder mit jedem kommunizieren kann.

FRNT1

Einige Switches haben die Fähigkeit, mehrere Ringe miteinander zu verbinden, wodurch eine noch höhere Zuverlässigkeit erzielt wird. Die Ringe mit Bridges verwenden eine primäre und eine sekundäre Verbindung zu anderen Ringen im Netzwerk. Wenn ein Fehler in der primären Verbindung auftritt, wird der Switch, der als Brennpunkt konfiguriert ist, informiert. Dieser rekonfiguriert das Netzwerk und verbindet die sekundäre Verbindung mit dem darunter liegenden Ring. Wenn ein Kabelfehler auftritt, muss dieser behoben werden. Bei einer redundanten Verbindung wird dieser Fehler jedoch nicht bemerkt, es sei denn, es wird gleichzeitig ein Alarm ausgelöst.



FRNT0



FRNT1

Time-Switch

Ethernet ist durch seine Konstruktion nicht deterministisch, das bedeutet, man kann keine Garantie für die Übertragungszeit eines Datenpakets von einer Situation zur nächsten übernehmen. Dies machte es früher unmöglich, Ethernet für Echtzeit-Anwendungen wie die Überwachung von Umspannstationen oder die Steuerung komplexer Maschinen zu nutzen, doch diese Beschränkungen gelten nicht mehr. In einem Echtzeitsystem müssen alle Verbindungen mit Vollduplex kommunizieren, wobei die Flusssteuerung (auf der Ethernet-Ebene) ausgeschaltet sein muss und es muss möglich sein, Daten Priorität einzuräumen. Alle Daten mit einer hohen Priorität kommen an die Spitze der Warteschlange und werden mit Priorität an den Empfänger gesendet. In Kombination mit der Zeitsynchronisierung eröffnet dies Möglichkeiten für Echtzeit-Anwendungen mit dem Ethernet, siehe auch die Seiten 136 bis 137.

Was kann bei Echtzeit-Anwendungen in einem geschalteten Netzwerk Probleme verursachen?

In einem geschalteten Netzwerk kommt es in Abhängigkeit von Netzwerklast, Geschwindigkeit der Verbindung, Datenpaketgröße, Switch-Architektur und der Anzahl der Switches zwischen Server und Client zu Verzögerungen. Eine Verzögerung kann zwischen zehn µs bis zu mehreren ms betragen. Die meisten Switches basieren auf der „store-and-forward"-Technologie, die das gesamte Paket empfängt und vor dem Weiterschicken prüft. Wenn wir annehmen, dass der Switch eine Verbindungsgeschwindigkeit (drop link speed) von 10 Mbit/s (Eingangsport am Switch) hat und die Paketgröße 1522 Bytes beträgt, führt dies zu einer maximalen Verzögerung 1,2 ms aufgrund der "store-and-forward"-Technik. Wenn man jedoch 100 Mbit/s zur Verfügung hat, beträgt die maximale Verzögerung 1,2 µs. Die richtige Technologie mit Zeitsynchronisation bildet also die Grundvoraussetzung für die Nutzung des Ethernet für Echtzeit-Anwendungen.

Switch-Funktionen

Prioritäten setzen (QoS, Quality of Service)

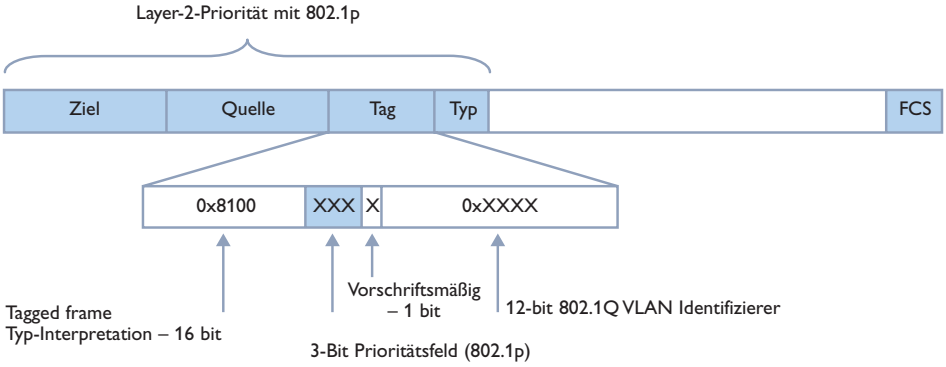
Switches, die das Setzen von Prioritäten unterstützen, haben zwei oder mehr Warteschlangen, die mit den entsprechenden Ports zum Handling der Daten verbunden sind (QoS). Das Setzen von Prioritäten kann auf verschiedenen ebenen mit unterschiedlichen Techniken erfolgen.

Es gibt zahlreiche Techniken, der Switch kann eine vorbestimmte Anzahl von Datenpaketen aus einer Warteschleife mit höherer Priorität vor einem Paket mit niedrigerer Priorität senden (Round-robin). Oder er kann mit einer strikten Prioritätenfolge Verkehr mit hoher Priorität immer Verkehr mit niedrigerer Priorität vorziehen.

Layer-2-Priorität

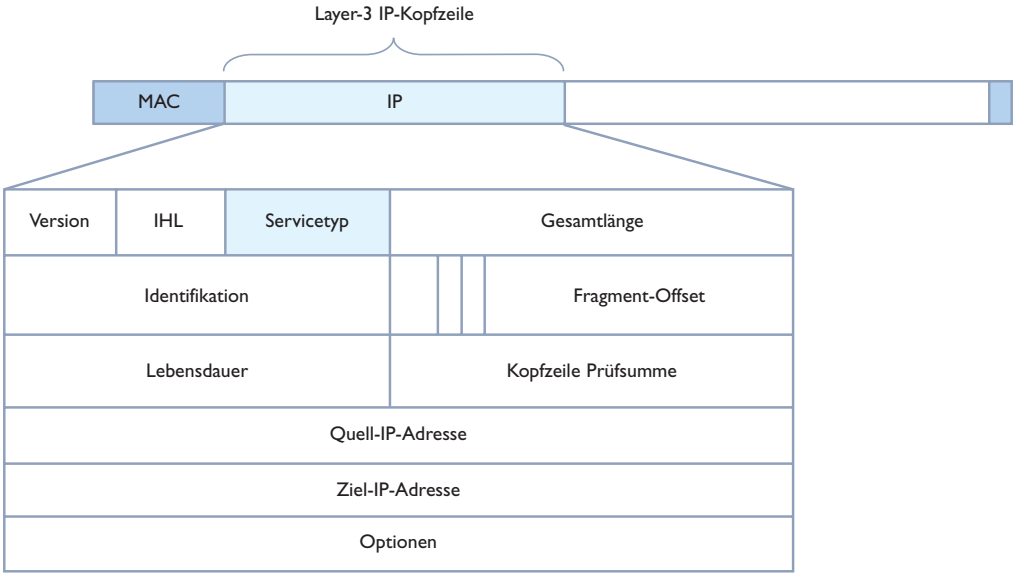
Ein Layer-2-Switch kann Daten auf einer MAC-Ebene aufgrund folgender Gegebenheiten Priorität einräumen:

- **MAC-Adresse** sowohl die Zieladresse als auch die Quelladresse können zum Setzen von Prioritäten genutzt werden. Der Switch muss gemanagd sind, um dies zu nutzen, damit er die Prioritäten der MAC-Adressen setzen kann.
- **Ethernet-Port (Layer 1)** ein Port oder mehrere Ports können für hohe Datenpriorität konfiguriert werden. Jeder Datenverkehr zu diesen Ports wird mit hoher Priorität behandelt.
- **Priorität setzen mit Tags** IEEE 802.1 p (und 802.1Q) dem Ethernet-Paket wird zusätzlich ein Feld mit der Bezeichnung „Tag Control Info" (TCI) hinzugefügt. Dieses Feld wird zwischen der Quelladresse und dem Typfeld eingefügt. Die Länge des Pakets erweitert sich damit von 1518 Byte auf 1522 Byte. Drei Bits werden für die „Tag-Information" verwendet, um die Priorität zu setzen. Dadurch wird es möglich, Prioritäten auf acht verschiedenen Ebenen zu setzen.



Layer-3-Priorität

Mit einem Layer-3-Switch können teilweise wie oben beschrieben Daten auf der MAC-Ebene (Layer 2) gesetzt werden oder zusammen mit einer IP „Kopfzeile", also wie bei einem Router. Jedem Paket wird basierend auf dem Inhalt des Felds, "Type of Service" (ToS), Priorität eingeräumt.

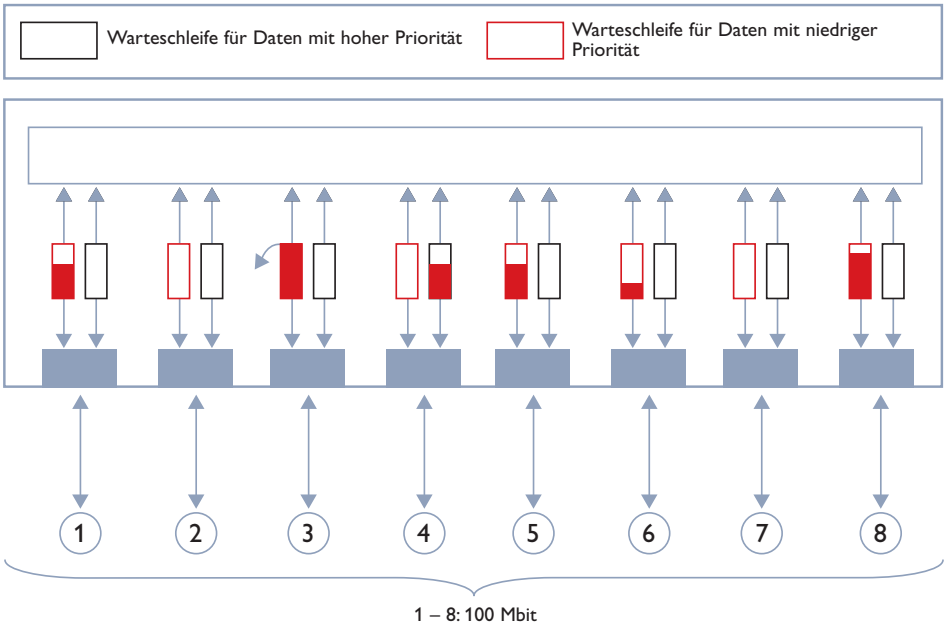


Head of Line blocking prevention

Eingehende und ausgehende Daten werden in einem Switch gepuffert (Warteschleife), dies geschieht normalerweise nach dem Prinzip FIFO (first in - first out). Wenn die empfangenen Daten an mehrere Ports gesendet werden müssen und einer von diesen überlastet ist, muss gewartet werden, bis der überlastete Speicher wieder Daten empfangen kann. Diese Funktion nennt man „Head of Line (HoL) blocking".

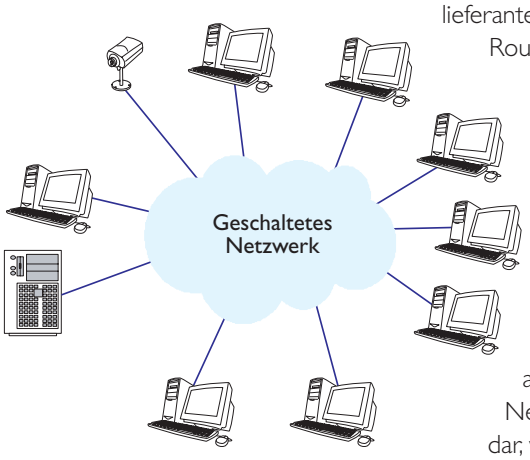
Wenn ein Switch mehrere Warteschleifen für Daten mit hoher und niedriger Priorität hat, kann ein Paket mit hoher Priorität wegen HoL verzögert werden.

Mit "Head of Line blocking prevention" kann man diese Situation bewältigen. Es wird geprüft, ob dem Paket eine Priorität zugewiesen ist und wenn ja wird dieses Paket in eine separate Warteschleife gestellt. Wenn keine hohe Priorität zugewiesen ist, wird dies ignoriert (Port 3 in der Abbildung). Die Daten mit niedriger Priorität werden abgelegt, da Anwendungen wie das TCP-Protokoll prüfen, ob eine erneute Übertragung notwendig ist oder nicht.



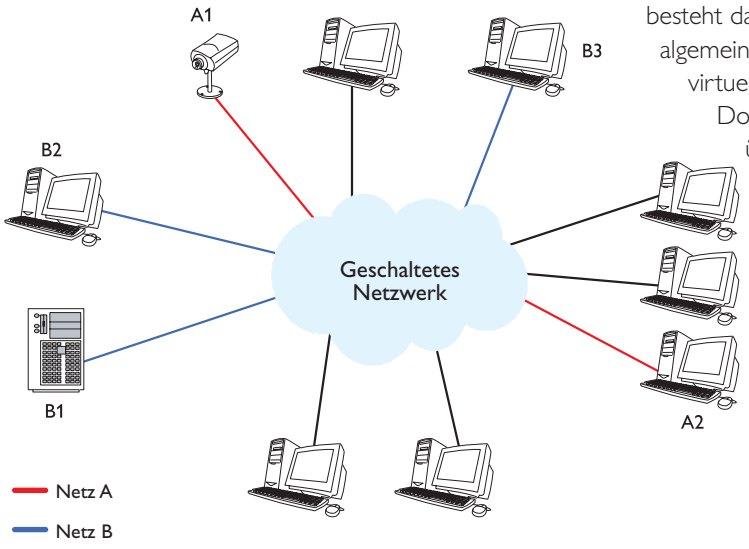
VLAN

VLAN oder Virtual LAN ist eine Technik, mit der Ausrüstungen in einem allgemeinen Netzwerk zu Gruppen zusammengefasst werden können. Hierfür gibt es mehrere Optionen, auf einer Portebene oder auf einer MAC-Adressen-Ebene. Außerdem gibt es lieferantenspezifische Lösungen. Früher haben Unternehmen und Organisationen Router zum Segmentieren großer Netzwerke verwendet. Diese Segmentierung kann auch mit VLAN erfolgen.



Ein Netzwerk mit installierter Ausrüstung bildet eine allgemeine "Broadcast"-Domain für alle angeschlossenen Geräte. Wenn ein Netzwerk erweitert werden soll, muss aufgrund der Geschwindigkeit und wegen der leichteren Verwaltung in der Regel eine Form von Segmentierung erfolgen. Dies geschieht meist mit einem oder mehreren Routern.

In einem Netzwerk ist jeder Anschluss ein separater Kollisionsbereich, aber alle Ausrüstungen gehören zur gleichen Broadcast-Domain, weshalb alle Broadcast-Sendungen an alle Geräte geleitet werden. Wenn das Netzwerk erweitert wird, stellen weitere Broadcast-Sendungen ein Risiko dar, weil weitere Geräte angeschlossen werden und dadurch die Netzwerkleistung abnimmt. Einige Ausrüstungen können auch Multicast nutzen und Daten an eine bestimmte Anzahl von Empfängern senden. Es kann daher erforderlich sein, diesen Datenverkehr zu begrenzen. Dies kann mit Routern oder mit einem VLAN (**V**irtual **LAN**) erfolgen.



Das Nutzungsprinzip eines Switch mit VLAN-Unterstützung besteht darin, jene Geräte anzugeben, die zu einem algemeinen virtuellen Netzwerk gehören sollen. Dieses virtuelle Netzwerk erzeugt eine separate Broadcast-Domain, die den unerwünschten Datenverkehr zu den übrigen Geräten verhindert. In dem Beispiel kommunizieren B1, B2 und B3 in einem virtuellen Netzwerk miteinander. Die Videokamera A1 sendet konstant Informationen, aber nur zu A2. Die anderen Geräte kommunizieren gemäß des Standards für geschaltete Netzwerke.

IGMP/IGMP Erkennung

Internet **G**roup **M**anagement **P**rotocol (IGMP) ist ein Protokoll, das von IP-Hosts verwendet wird, um die naheliegendsten Router über die Mitgliedschaft in Multicast-Gruppen zu informieren. Multicast-Router senden periodisch eine "Host Membership Query message" (Anfrage zur Hostmitgliedschaft), um sich über die aktuelle Zusammensetzung der Gruppe in dem lokalen Netzwerk zu informieren. Die Hosts im lokalen Netzwerk antworten dann mit einem Berichtsdatengramm. Die Hosts regieren nur auf Anfragen für die Gruppen, zu denen sie gehören. Wenn nach einer bestimmten Anzahl von Anfragen keine Berichte für eine spezielle Gruppe eingehen, geht der Router davon aus, dass in dem lokalen Netzwerk keine Gruppenmitglieder mehr vorhanden sind. Daher werden für diese Gruppe von anderen Netzwerken keine Datenaufstellungen mehr für das lokale Netzwerk weitergeleitet.

Grundsätzlich unterstützen Layer-2-Switches IP Multicast-Datenverkehr auf die gleiche Weise wie eine Broadcast-Sendung, also Daten an alle Ports. Dies kann zu einer starken Belastung führen und die Netzwerkleistung beeinträchtigen. Mit IGMP Erkennung kann ein Switch den Verkehr filtern und dadurch unnötigen Verkehr verhindern. Dies geschieht, indem der Switch den IGMP-Verkehr zwischen Host und Router abhört. Der Switch erkennt, ob ein Host ein Gruppenmitglied wird, oder ob seine Mitgliedschaft endet. Daher weiß er, welche Geräte zu einer Multicast-Gruppe gehören. Zurzeit sind drei Ebenen von IGMP definiert:

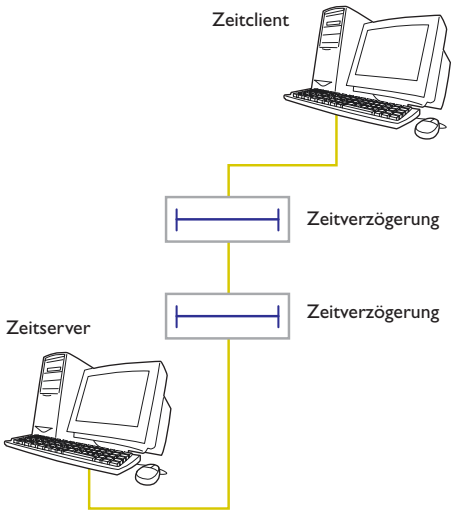
- IGMPv1 (REF 1112) die Originalversion von IGMP, hierzu gehört wie ein Host die Mitgliedschaft in einer Gruppe abfragt. Allerdings gibt es in der Version 1 keine Methode, die Mitgliedschaft zu beenden, hierfür benötigt ein Router einen Timer.
- IGMPv2 (REF2236), diese Version beinhaltet die Beendigung einer Mitgliedschaft.
- IGMPv3 (REF3376), allgemeine Überarbeitung von IGMP.

Zeitsynchronisierte Netzwerke

Bisher vertriebene Echtzeitsysteme basierten normalerweise auf Feldbussen, aber geschaltete Ethernet-Systeme sind jetzt eine weitere Option. Möglich wird dies durch Leistungsmerkmale wie: Bandbreite, Einräumen von Prioritäten und industrielle Spezifikationen von Netzwerkausrüstungen. Und nicht zuletzt, weil die Preise für Ethernet-Ausrüstungen gefallen sind.

Latenz (variable Verzögerungen) in einen geschalteten Netzwerk bedeutet, dass von Knoten gesendete Daten von verschiedenen Verzögerungen betroffen sein können. Dies ist neben anderen Faktoren auf die aktuelle Belastung eines Netzwerks zurückzuführen. Die Genauigkeit von zeitsynchronisiertem Datenverkehr ist vor allem von folgenden Faktoren abhängig:

1. Variable Netzwerkverzögerungen beruhen auf: Netzwerkauslastung, Geschwindigkeit, Paketgröße und der in den Switches verwendeten Architektur.
2. Das verwendete Protokoll hat im Vergleich zu den oberen Bedingungen eine untergeordnete Bedeutung, wir empfehlen jedoch SNTP/NTP, da dies die Standards mit geringeren Begrenzungen sind.
3. Die Zeitstemplung der eingehenden und ausgehenden Datenpakete erfolgt so dicht an der Hardware wie möglich, also auf der niedrigsten Ebene des OSI-Modells.



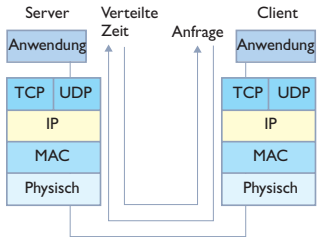
SNTP/NTP

RFC 2030 **S**imple **N**etwork **T**ime **P**rotocol (SNTP), RFC 1305 **N**etwork **T**ime **P**rotocol (NTP) und P1588 sind bewährte Protokolle für zeitsynchronisierten IP-Datenverkehr. SNTP ist ein Subset von NTP. Der SNTP/NTP-Server regelt die System-Uhr, die entweder auf der internen Uhr oder GPS basiert. Die Zeitinformation wird dann entweder über Unicast oder Multicast übertragen.

1. Aktualisieren über Unicast, das Update wird vom Client initiiert, der Server sendet dann eine Antwort. Die Zeitreferenz wird dann allen Kommunikationen zwischen Client und Server hinzugefügt, dies dient der Berechnung einer maximalen Genauigkeit.
2. Aktualisierung über Multicast, die Zeit wird vom Server an eine Client-Gruppe (Multicast-Gruppe) in festgelegten Intervallen gesendet. Es ist für den Client nicht möglich, die Verzögerung im Netzwerk zu berechnen.

Zeitstempelung über Anwendungen

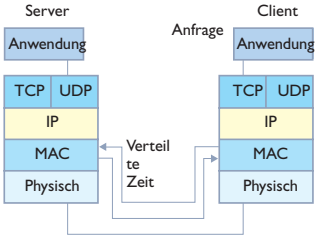
Die meisten SNTP/NTP Anwendungen erzeugen die Zeitstempelung der Daten auf der Anwendungsebene, die Genauigkeit ist dann von der Verzögerung/der Instabilität durch den gesamten IP-Stapel abhängig. Die typische Genauigkeit für diese Technik beträgt eine bis zwei Millisekunden.



Zeitstemplung über Anwendungen

Zeitstempelung über Ethernet-Treiber

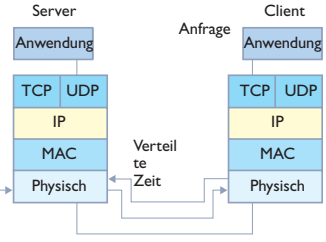
Die Genauigkeit kann bedeutend erhöht werden, wenn die Zeitstempelung mit der Ethernet Interrupt Service Routine erfolgt, die Zeitstempelung erfolgt, wenn die Daten zwischen Server und Client gesendet werden. Die Anfrage wird vom Client ausgelöst, die Genauigkeit hängt in diesem Fall von der Instabilität ab, vom Interrupt und vom Handling beim Server und Client. Die Genauigkeit in dieser Anwendung variiert zwischen 10 µs bis etwa 100 µs.



Zeitstemplung über Ethernet-Treiber

Zeitstempelung auf der physischen Ebene

Die Verzögerung im IP-Stapel kann vermieden werden, wenn die Zeitstempelung auf der physischen Ebene stattfindet, d. h. über die Hardware. In diesem Fall kann die Zeitstempelung extrem genau sein, d. h. besser als 1 µs. Diese Genauigkeit erfordert eine Direktverbindung zwischen Server und Client, da weitere Geräte zur Verzögerung beitragen würden. Aus diesem Grund ist der Zeitserver im Switch integriert. Zusätzlich besteht die Möglichkeit, den Switch von der Referenzuhr über GPS oder den internen Oszillator zu synchronisieren.



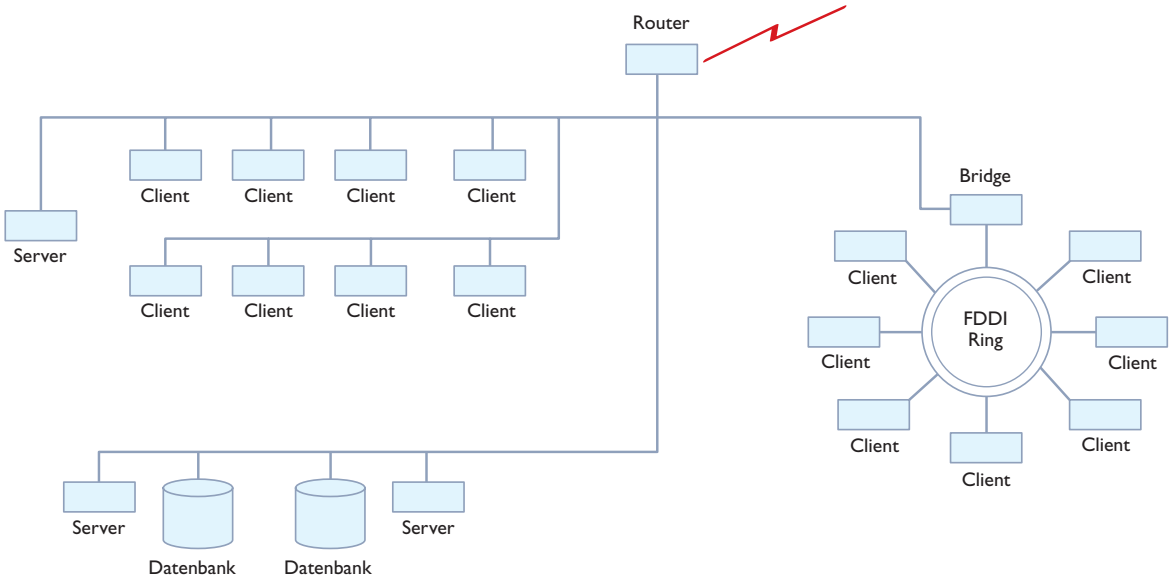
Zeitstemplung auf der physischen Ebene

SNMP

SNMP steht für **S**imple **N**etwork **M**anagement **P**rotocol. Mit SNMP können Geräte in einem Netzwerk verwaltet werden. Ein Gerät, das überwacht werden kann, heißt Agent. Ein Master-System sendet eine Anfrage an die Agenten und fordert Daten an, dies kann mit speziellen Anwendungen oder über Telnet erfolgen.

Mit SNMP kann man:

- Trends Aufzeichnen
- Abläufe zur Analyse aufzeichnen
- Geräte im Netzwerk und ihren Status überwachen
- Eine besonders wichtige Verbindung überwachen
- Zur Schadensvermeidung kann der Datenverkehr eines oder mehrerer Netzwerk-Geräte überprüft werden
- Geräte können konfiguriert werden

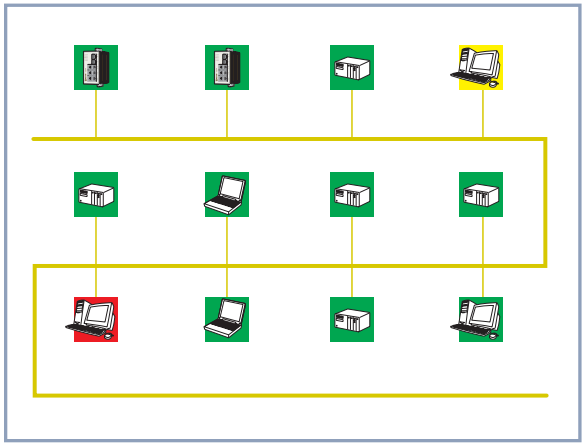


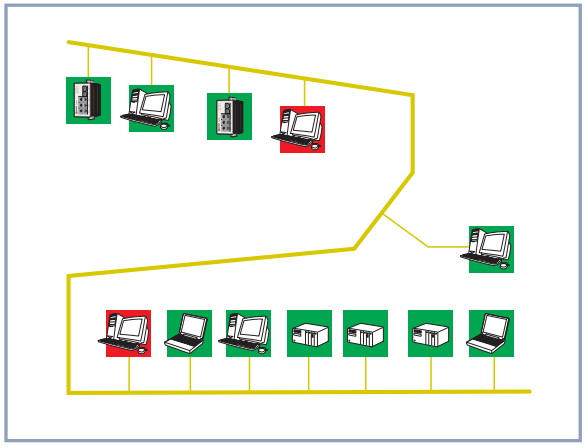
Software für SNMP

Die Software, die für die Kommunikation mit den Agenten eingesetzt wird, heißt **N**etwork **M**anagement **S**olution (NMS). Der Datenaustausch mit den Agenten erfolgt ähnlich wie die Kommmunikation zwischen Master und Slaves, d. h. die Kommunikation mit den untergeordneten Geräten erfolgt durch Abfragen (polling). Der Netzwerkadministrator kann von einem Agenten Informationen anfordern oder eine Aktion durchführen, der Agent antwortet auf die Anfrage oder reagiert auf die Aktion. Eine weitere Möglichkeit, ist das Setzen eines Sperrkreises (trap), d.h. einer unter bestimmten Bedingungen ausgelösten Funktion. Bei der Auslösung sendet der Agent bestimmte Daten an den Administrator.

Hier ein Beispiel:

In einem großen Netzwerk sind kritische Geräte integriert, die mit UPS als Stand-by-Stromversorgung arbeiten. Im Fall eines Stromausfalls werden die UPS-Geräte automatisch angeschlossen und die Geräte arbeiten weiter. Dieser Fehlerzustand muss nun dem Netzwerk-Administrator mitgeteilt werden, dies kann über eine Sperrschaltung erfolgen, die feststellt, dass die UPS-Geräte angeschlossen sind. Die Information wird an ein SCADA-System (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) weitergeleitet, wo der Netzwerk-Administrator einen Alarm über ein blinkendes Icon am UPS-Gerät empfängt (durch die SNMP-Sperrschaltung aktiviert).





SNMP, SNMPv2 und SNMPv3

Von SNMP gibt es drei Versionen. Die Originalversion von SNMPv1 besitzt ein Multisicherheitssystem, dass aus einem Passwort besteht. In Version 1 kann der Sender einer Nachricht nicht mit aller Sicherheit identifiziert werden. Dies macht SNMP offen, dadurch können Geräte im Netzwerk rekonfiguriert werden. Als Konsequenz haben viele Gerätehersteller sich dafür entschieden, nicht alle Funktionen in den Standard zu implementieren. Diese Nachteile wurden von Beginn an erkannt und es wurde eine bedeutend verbesserte Version geplant, SNMPv2. Diese arbeitet mit einem Verschlüsselungsalgorithmus für die Authentifizierung von Übertragungen zwischen SNMP-Servern und Agenten. SNMPv2 kann auch die Übertragung verschlüsseln. SNMPv2, als Verbesserung geplant, wurde aber als Standard nie akzeptiert. Ein dazu beitragender Faktor war die Uneinigkeit darüber, wie die Sicherheitsmaßnahmen implementiert werden sollten. SNMPv2 ist aber ein wichtiges Bindeglied in der Entwicklung der nächsten Version, SNMPv3.

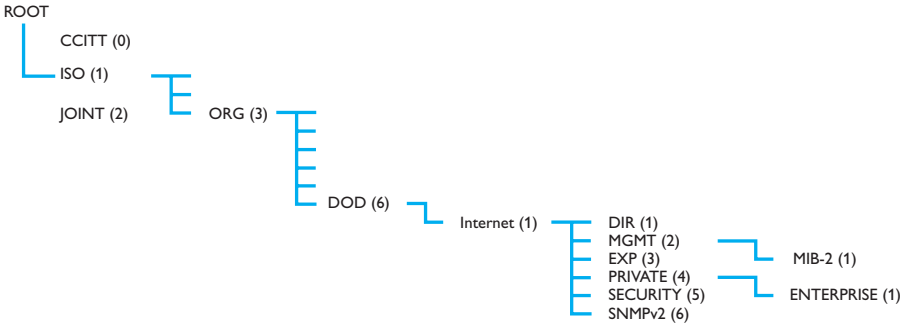
Die SNMPv3-Arbeitsgruppe wurde im März 1997 gegründet, mit der Aufgabe, die vorliegenden Sicherheits- und Verwaltungsvorschläge zu prüfen und eine gemeinsame Lösung für das Problem zu finden. Der Fokus der Arbeit war, so weit wie möglich die eingegangenen Vorschläge zu prüfen, und nicht noch weitere neue Ideen zu entwickeln. Der Vorschlag für SNMPv3 war 1998 fertiggestellt. Es basiert auf Version 2, sowie auf einem Sicherheits- und Verwaltungskonzept, das auf unterschiedlichen Modulen basiert, die je nach dem zu erreichenden Sicherheitsniveau ausgetauscht werden können.

SNMPv3, der aktuelle Standard, bietet bedeutend mehr Möglichkeiten Netzwerk-Geräte sicher zu machen, trotzdem erfolgt die Einführung sehr langsam. Die meisten installierten Geräte arbeiten immer noch mit SNMPv1.

MIB

Jeder Agent im Netzwerk besitzt einen Satz von MIBs (**M**anagement **I**nformation **B**ase), ein MIB ist ein Objekt, das von einem Administrator angesprochen werden kann. Bei den Informationen kann es sich entweder um Standardinformationen wie z. B. Port-Status handeln oder um herstellerspezifische (private) MIBs, z. B. die Temperatur innerhalb des Gerätes.

MIBs sind strukturierte Tabellen, die die verschiedenen Objekte auflisten, die angesprochen werden können. Die Struktur kann mit einem Baum verglichen werden, seiner Wurzel und den darunterliegenden Directories. Auf der niedrigsten Ebene finden sich die Directories für das Standard-MIB und für private MIBs.



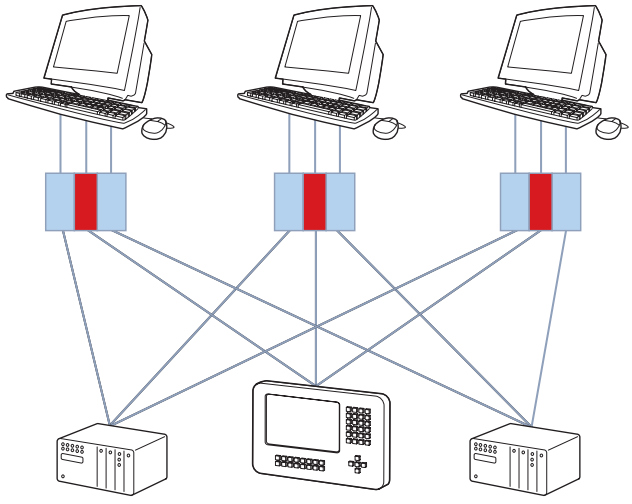
OPC

Eine Alternative zu SNMP ist OPC, eine Abkürzung für OLE for Process Control. Dies ist eine Serie von Standards speziell für den Informationsaustausch in der industriellen Automatisierung. Eine der Hauptaufgaben dieser Standards ist die Verbesserung der Effizienz und die Verringerung des Bedarfs an herstellerspezifischen Treibern. Viele verschiedene Treiber führen normalerweise zu einer komplexen Implementierung, da mehrere Anwendungen zusammenarbeiten und Dateninformationen untereinander austauschen müssen.

Die OPC-Funktionen beinhalten Funktionen für:

- **OPC D**ata **A**ccess oder (OPC DA), Zugang zu Daten zwischen Anwendungen, Austausch von Informationen zwischen Systemen in Echtzeit
- **OPC H**istorical **D**ata **A**ccess (OPC HDA), wird für alte Datenbestände und zur Trendanalyse eingesetzt
- **OPC A**larm and **E**vents (OPC A&E), Steuerung von Alarmen und Abläufen
- **OPC D**ata e**X**change (OPC DX), definiert wie der Datenaustausch zwischen verschiedenen OPC-Servern erfolgen soll.

- **OPC** e**X**tensible **M**arkup **L**anguage (normalerweise OPC XML genannt), HTML-basierte Sprache für den Informationsaustausch zwischen Anwendungen.

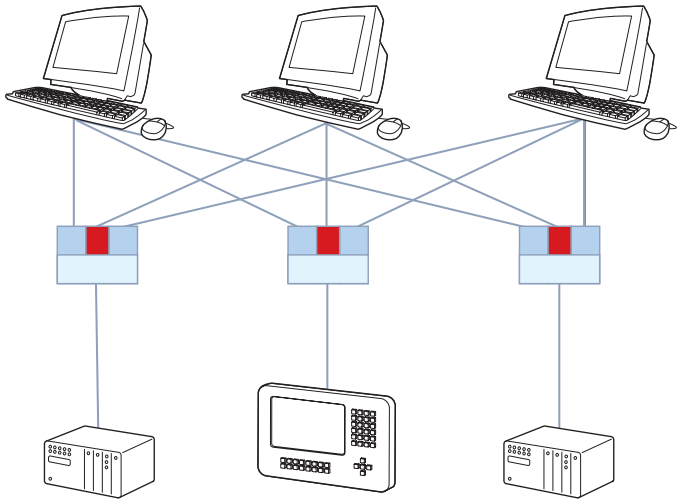


Um die Probleme dabei zu verdeutlichen, kann man sich vorstellen, dass zwischen drei Anwendungen Informationen ausgetauscht werden sollen, zwischen zwei PLCs und einen Bedienungspult (HMI).

Jeder Lieferant hat seine eigene Anwendung mit ihren eigenen Treibern. Die Treiber müssen die Daten von den entsprechenden PLCs und der HMI herunterladen,in unserem Beispiel führt das zu neun Integrationspunkten.

OPC vereinfacht das unter Einsatz von Standard-Tools. Die Entwicklung von OPC ist das Ergebnis der Zusammenarbeit von führenden Herstellern von Automatisierungsanlagen und Microsoft. Von der Technik her werden Microsofts COM (**C**omponent **O**bject **M**odel) und DCOM (**D**istributed **C**omponent **O**bject **M**odel) für die Kommunikation zwischen den Anwendungen eingesetzt. So hat in diesem Beispiel jeder PLC und HMI nur einen Anschlusspunkt, das führt zu einer einfacheren und kostengünstigeren Implementierung des gesamten Systems.

Diese Möglichkeiten und Vorteile haben dazu geführt, dass Systemanlagenhersteller bereits die Unterstützung von OPC in ihre Geräte integrieren.



Ethernet mit Kabel

10 Mbit/s Ethernet

Signale, die über alle 10 Mbit/s Mediasysteme gesendet werden, verwenden Manchester-Codierung. Die Manchester-Codierung kombiniert Daten und Uhr in Bit-Symbolen, die ein Uhrsignal in der Mitte jedes Bits ermöglichen. Eine logische Null (0) ist definiert als ein Signal, das in der ersten Hälfte der Bitperiode hoch und in der zweiten Hälfte niedrig ist, d. h. ein negativer Signalübergang. Eine logische Eins (1) ist definiert als ein positiver Signalübergang in der Mitte einer Bitperiode.

Der Signalübergang erleichtert dem Empfänger die Synchronisation mit dem eingehenden Signal sowie die Extraktion der Daten aus dem Signal. Ein Nachteil ist, dass die Worst-case-Signalrate doppelt so groß ist wie die Datenrate. Wenn keine Daten zum Senden vorhanden sind, wird ein Verbindungstestsignal gesendet.

Fast Ethernet

100Base-T Mediasysteme nutzen 4B/5B Blockcodierung. Blöcke von 4-Bit Daten werden in 5-Bit Codesymbole für die Übertragung über das Mediasystem übersetzt. Das 5-Bit Codiersystem ermöglich die Übertragung von 32 5-Bit-Symbolen inklusive 16 Symbolen, die die 4-Bit Daten sowie 16 Symbole für die Steuerung tragen. Das IDLE Kontrollsymbol wird kontinuierlich gesendet, wenn keine anderen Daten vorhanden sind. Aus diesem Grund ist Fast Ethernet permanent aktiv und sendet 5-Bit IDLE-Symbole bei 125 Mbit/s wenn nicht anderes gesendet werden muss. Jedes 100 Mbit/s (Fast Ethernet) System nutzt verschiedene Mediasignalisierungsverfahren.

100Base-TX verwendet "scrambling and multilevel threshold-3" (MLT-3) Signalisierung. Das Signal auf dem Kabel kann eine von drei Ebenen haben. Ein Wechsel von einer Ebene zur nächsten markiert eine logische Eins (1). Eine konstante Einzelebene zeigt eine logische Null (0) an.

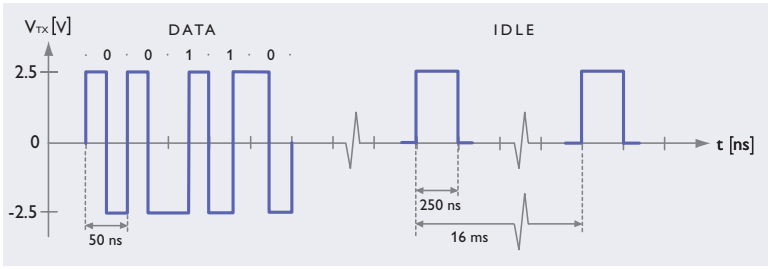
Um die elektromagnetische Emission zu reduzieren, erfolgt ein Zerhacken bevor das Signal MLT-3 moduliert wird. Der Zerhacker produziert eine sich nicht wiederholende Bitsequenz der zu übertragenden Bits.

Ein 100Base-FX Glasfasersystem nutzt NRZI-Codierung. Dieses System macht keinen Unterschied der Signalebene beim Senden einer logischen Null, invertiert die Ebene jedoch bei logischen Einsen.

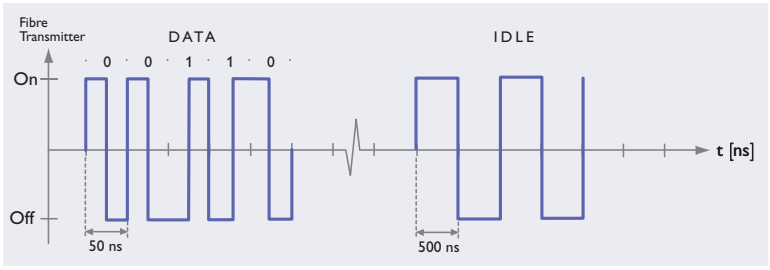
Gigabit Ethernet

1000Base-T (Kupfer) verwendet 4D-PAM5-Codierung. Das System überträgt und empfängt Daten gleichzeitig auf vier Drahtpaaren (4D) mithilfe von fünf Voltniveaus (PAM5) auf jedem Paarseil.

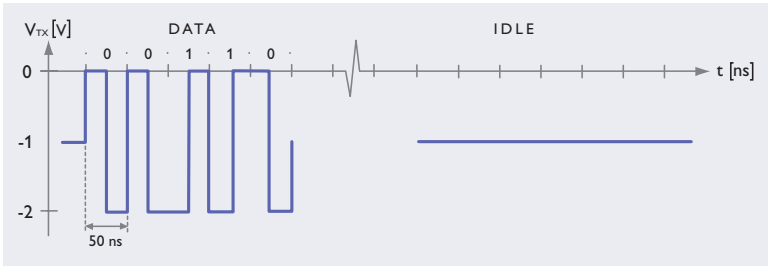
1000Base-T (Glasfaser) verwendet 8B/10B-Codierung. Daten und Steuersymbole werden mit einer Rate von 1250 Mbit/s übertragen. Die hohe Signalrate erfordert den Einsatz von Laser-Sende-Empfangsgeräten.



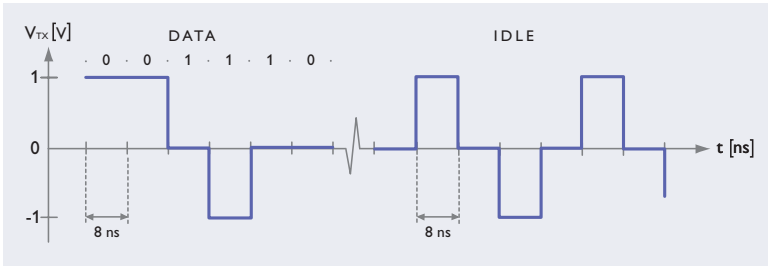
10Base-T



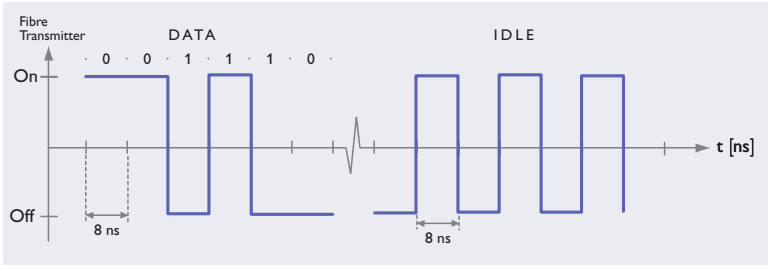
10Base-FL



10Base2



100Base-TX



100Base-FX

Glossary

10Base2	Eine Ethernet-Verkabelung mit dünnen Koaxialkabeln als Netzwerkmedium. Pro Netzwerksegment ist eine Kabellänge von 185 Metern (616 ft) möglich. Die einzelnen Geräte können direkt in Reihe an das LAN angeschlossen werden.
10Base5	Eine Ethernet-Verkabelung mit dicken, doppelt abgeschirmten Koaxialkabeln als Netzwerkmedium. Pro Netzwerksegment ist eine Kabellänge von 500 Metern (1.666 ft) möglich. Am Kabel wird ein MAU befestigt, damit Geräte über den AUI-Port am Ethernet-Gerät kommunizieren können.
10BaseFL	Eine Ethernet-Verkabelung mit Glasfaserkabeln als Netzwerkmedium. 10BaseFL arbeitet mit 10 Mbit/s.
10BaseT	Eine Ethernet-Verkabelung mit zwei paarverseilten Vierdrahtleitungen aus Kupferdraht. Zwischen den Geräten oder einem Verteiler bzw. Switch ist eine maximale Entfernung von 100 Metern möglich. Als Verbindung zwischen den Ethernet-Geräten wird ein RJ-45-Anschluss verwendet. 10BaseT arbeitet mit 10 Mbit/s, 100BaseT mit 100 Mbit/s.
AC	**A**lternating **C**urrent, ‚Wechselstrom'.
Amplitude	‚Amplitudenmodulation'; die Übermittlung von Informationen über Änderungen der Amplitude bzw. der Signalstärke der Trägerwelle.
Anwahl-Netzwerk	Eine andere Bezeichnung für das öffentliche Telefonnetz (PSTN).
ARP	Das **A**ddress **R**esolution **P**rotocol wird verwendet, um IP-Adressen an MAC-Adressen zu übertragen. Als TCP/IP-Werkzeug wird es dazu benutzt, MAC oder IP-Adresseninformationen hinzuzufügen oder zu löschen.
ARQ	**A**utomatic **R**epeat re**Q**uest, ‚automatische Wiederholungsauff-orderung'.
ASCII	Kodierungssystem für Binärdaten, das 128 druckbare Zeichen mit Zahlenkombinationen mit Nullen und Einsen darstellt. ASCII = **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange, ‚Amerikanischer Standardcode zum Informationsaustausch'.
Asynchronous	"asynchrone" Datenübertragung mit einzeln übermittelten Zeichen, die von Start- und Stopbits eingerahmt werden. Ungefähr 90–95 % aller seriellen Datenkommunikation sind asynchron.
Attenuation	‚Dämpfung'; Datensignale werden durch Kabellänge und bei Lichtwellenleitern durch die Anzahl der Spleißverbindungen abgedämpft.
AUI	**A**ttachment **U**nit **I**nterface Port. Die Verbindung zwischen Netzwerkgerät und MAU erfolgt über ein Standard 15 Pin D-Typ Ethernetkabel.

Auto-Negotiate Der IEEE802.3u-Standard bestimmt eine MAC-Subschicht für die Erkennung von Geschwindigkeit und Duplex-Modus der Verbindung, die von einem Gerät unterstützt wird. Dieser Standard wird nur auf Wunsch unterstützt.

Auto-Sense Die Fähigkeit eines 10/100 Ethernet-Geräts zur Erkennung von Geschwindigkeit und Duplex-Modus des angeschlossenen Geräts. Es findet eine automatische Konfiguration an die Vorgabe statt.

Baud Definiert die Geschwindigkeit der per Sekunde übermittelten Anzahl von "Paketen". Bei lokaler Datenkommunikation entspricht Baud bit/s. In der Telekommunikation können mehr Bits in einem Paket sein.

Binary "Binär"-Zahlen können nur einen von zwei Werten annehmen, null oder eins, die von den beiden möglichen Halbleiterzuständen im Computer repräsentiert werden, nämlich der An- oder Abwesenheit von elektrischer Spannung.

Bit Ein Datenbit ist eine binäre Ziffer, also null oder eins.

Bit/s Datentransferrate, gemessen in der Anzahl von Datenbits pro Sekunde.

BOOTP Das BOOTP-Protokoll ermöglicht es Netzwerkgeräten von einem BOOTP-Server Konfigurationsinformationen abzurufen.

BRI **B**asic **R**ate **I**nterface, ‚Basisanschluss'; ISDN-Dienst, der den Zugriff auf zwei B-Kanäle und einen 16 kbit/s-D-Kanal erlaubt.

Broadband "Breitband"; eine Technologie, die simultane Übermittlung verschiedener Kanäle in verschiedenen Frequenzen von Daten und Audio- und Videoinformationen ermöglicht.

BSC **B**ase **S**tation **C**ontroller, ‚Funkbasissteuerung'; eine Schaltstation im GSM-Netz, die einerseits zwischen Funkbasisstation und andererseits dem Kernnetz kommuniziert.

BTS **B**ase **T**ransceiver **S**tation, ‚Funkbasisstation'; Funkstation im GSM-Netz, die einerseits mit Mobilgeräten und andererseits mit einer BSC; Funkbasissteuerung, kommuniziert.

Buffer ‚Puffer'; Speicherbereich zur kurzeitigen Datenspeicherung, z. B. während der Wartezeit auf das Fertigsignal eines Empfängers.

Byte Ein mit acht Bits als Binärzahl dargestellter Buchstabe, z. B. korrespondiert ein Ascii-Wert 65 mit dem Buchstaben ‚A'.

Capacitance ‚Kapazität', Fähigkeit zur Absorbierung einer elektrischen Ladung.

Gemessen in	Microfarad	$= 10^{6}$	F = 1 µF
	nanofarad	$= 10^{-9}$	F = 1 nF
	picofarad	$= 10^{-12}$	F = 1 pF

CAT5	Eine paarverseilte Vierdrahtleitung aus Kupfer, die Bandbreiten bis zu 100 MHz oder bei Nutzung aller vier Paare 1000 MHz ermöglicht. Normale Datenübertragungsraten sind 100 Mbit/s oder 1000 Mbit/s.
CAT5e	Erweiterter Cat5-Standard mit Störgeräuschunempfindlichkeit. Dies ist der häufigste Standard in den neuen Installationen.
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol ist deutlich sicherer als PAP. Passwörter werden nicht nur beim Einloggen abgefragt, sondern auch beim Abfragemodus. Die Verbindung wird beendet, wenn keine identischen Buchstaben oder Passwörter gesendet werden.
Checksum	‚Prüfsumme'; Ergebnis einer mathematischen Berechnung zur Kontrolle der Korrektheit von Datenübertragungen.
Client Server	'Kunde/Diener', Problemlösung in Netzwerken, bei der Datenverarbeitung und Software auf einem zentralen Server von vielen Personalcomputern (Clients) genutzt werden.
Clock	‚Uhr', Bezeichnung einer von einer Signalquelle (clock pulse generator, ‚Uhrtaktgeber') gesandten regelmäßigem Frequenz, die unter anderem zum Setzen der Datenflussgeschwindigkeit bei serieller Übertragung dient.
CMV	**C**ommon **M**ode **V**oltage, ‚Funkspannung' bzw. ‚Längsspannung', normalerweise induktiv erzeugt.
Coaxial cable	"Koaxialkabel"; Kabel mit abschirmender äußerer Hülle und darin einem geschützten Leiter zur schnellen und von Interferenzen ungestörten Datenübertragung.
CSD	**C**ircuit **S**witched **D**ata, ‚leitungsvermittelte Daten'; gebräuchlichste Form des Datentransports im GSM-Netz.
CSMA/CD	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect. Dies ist die Zugangsmethode im Ethernet, bei der sämtliche Geräte gleichberechtigt versuchen, Zugang zum Netzwerk zu erhalten, um Daten zu übertragen. Wenn ein Gerät bei dem Versuch, Daten zu übertragen, das Signal eines anderen Gerätes erkennt, wird die Übertragung abgebrochen und nach einer gewissen Verzögerung erneut aufgenommen.
Current Loop	‚Spannungsschleife'; serielle Übermittlungsmethode, die mit der An- und Abwesenheit elektrischer Spannung in einem Kabelpaar arbeitet.
Data bits	Siehe Bit.
Databus	‚Datenbus', eine Reihe paralleler Kabel für geräteinternen Datentransport.

Datagram	Ein vollständiges Datenpaket, das ausreichende Informationen umfasst, um es von der Quelle zum Ziel zu leiten, ohne dass ein zusätzlicher oder vorheriger Abgleich zwischen den beiden Geräten stattfinden muss. Diese Art der Verbindung wird normalerweise als verbindungslose Kommunikation bezeichnet.
DC	**D**irect **C**urrent, ‚gerichtete Spannung', Gleichstrom.
DCE	**D**ata **C**ommunication **E**quipment, Datenendgeräte.
DDS1	Europäischer Standard für ISDN-Verbindungen.
Dedicated line	‚dezidierte Leitungsverbindung'; „betriebseigene Leitung,"; private, nicht im Besitz eines Netzbetreibers befindliche Kommunikationsleitung.
DHCP	The **D**ynamic **H**ost **C**onfiguration **P**rotocol ermöglicht es, dass Netzwerkgeräte IP-Adressen von einem DHCP-Server im LAN abfragen und sie ihnen dann zugeordnet werden können. Wenn ein DHCP-Server nicht verfügbar ist, werden die IP-Adressen bei der Konfiguration des Ethernet-Geräts fest eingegeben.
DIN rail	**D**eutsche **I**ndustri **N**orm, DIN-Schiene, ‚Hutschiene'; Montagestandard für Geräte in Schaltschränken.
DTE	**D**ata **T**erminal **E**quipment, Datenendgeräte.
Duplex	definiert Kommunikation in zwei Richtungen. Im Halbduplexbetrieb senden und empfangen die Seiten abwechselnd, im Vollduplexbetrieb geschieht dies gleichzeitig.
Eine Verbindung	zu entfernten Geräten aufzubauen.
EMC	**E**lectro **M**agneti **C**ompatibility, ‚elektromagnetische Kompatibilität', Produktauslegung in einer Art und Weise, dass keine Beeinflussung mit anderen elektronischen Geräten passiert.
EMI	**E**lectro **M**agnetic **I**nterference, elektromagnetische Beeinflussung.
Ethernet	verbreiteter Standard für lokale Netzwerke (LAN) für Büroanwendungen, der mit vieradrigem Kabel und mit Koaxialkabeln realisiert werden kann.
Euro-ISDN	auf europäische Standards basierendes ISDN.
Fading	Abschwächung und Dämpfung der Signale in Kabeln, Luft usw. mit zunehmender Entfernung.
Faxmodem	Modem, das zum Senden und Empfangen von Text- und Bilddaten im Faxformat in der Lage ist.
FDDI	**F**ibre **D**istributed **D**ata **I**nterface: Standard für Lichtwellenleiternetze.
Fibre optics	'Glasfaseroptik'; moduliertes Laserlicht bzw. Laserstrahlen aus lichtemittierenden Dioden in normalerweise zwischen 800-1300 Nanometer dünnen Fiberglas- oder Plastikfasern. Glasfaserbündel können sehr umfangreiche Informationsmengen transportieren.

Fieldbus	'Feldbus'; definierter Standard industrieller Datennetze, z. B. PROFIBUS.
Firewall	Ein Router, mit dem IP-Adressen überprüft werden können.
Four wire	twisted pair 4-wire cable, ‚vieradriges paarweise verdrilltes Kabel'.
FP	A **F**ibre Optic Ethernet **P**ort.
Frame	Ein **Frame** ist ein Datenpaket, das zwischen zwei Ethernet-Geräten als komplette Einheit mit Adress- und Protokollinformationen gesendet wird. Die Information wird seriell Bit-für-Bit übertragen.
Frequency	‚Frequenzmodulation', Technologie zum Informationstransport mittels variierender Frequenz einer Trägerwelle.
FRNT	**F**ast **R**e-Configuration **N**etwork **T**opology. Hier werden Ethernet-Switches in mehrfachen, redundanten Ringen angeordnet. Durch die Verlinkung unterschiedlicher Ringe mit Backup-Pfaden wird eine verbesserte Redundanz erzielt.
FTP	**F**ile **T**ransfer **P**rotocol. Dies ist eine der einfachsten Möglichkeiten, Daten über das Internet zu übertragen. Es arbeitet mit TCP/IP-Protokollen, um Datenübertragungen zu ermöglichen.
Full Duplex	Bidirektionale Kommunikation, bei der Signale in beiden Richtungen simultan übertragen werden.
Galvanic isolation	"Galvanische Trennung"; Mittel zur elektrischen Isolation ohne metallischen bzw. elektrischen Kontakt.
GPRS	**G**eneral **P**acket **R**adio **S**ervice, ‚Dienstqualität'. GSM-Dienst zum Datentransport von in Paketen zerlegten Datenströmen.
GPRS Attach	'GPRS-Anbindung'; einleitende Anfrage eines GSM-Geräts zur Erlaubnis zur Verbindungsaufnahme mit einem GPRS-Netzwerk.
GPS	**G**lobal **P**osition **S**ystem. Ein Satellitennavigationssystem, das sich auf 24 Satelliten stützt, die im Weltall positioniert sind. Jeder Satellit arbeitet mit einer Atomuhr, deren Genauigkeit bei einer milliardstel Sekunde liegt.
Ground currents	‚Erdungsströme', Ströme, die zwischen den Massekontakten zweier Systeme mit unterschiedlichem Erdungspotential fließen.
GSM	**G**lobal **S**ystem for **M**obile communication, ein Standard zur digitalen drahtlosen Datenübertragung.
Half Duplex	Zweiwegkommunikation.
Handover	'von Hand zu Hand geben', Bezeichnung für den Wechsel zwischen Funkbasisstationen während der Kommunikation in einem GSM-Netzwerk.
Handshaking	‚Hand schütteln'; zwischen Kommunikationsgeräten gesendete Bestätigungs- und Statussignale zur Datenflusskontrolle.

Hayes commands	'Hayes-Kommandos', "AT-Befehle", Befehlssatz zur technischen Kommunikation mit Telefonmodems (zur Einstellung des Modems, nicht zur Nutzdatenübermittlung).
Hub	Dieser zentrale Verteiler ermöglicht die Verbindung von Netzwerksegmenten. Wenn ein Datenpaket an einem Port eingeht, wird es an alle am Verteiler angeschlossene Ports gesendet.
IEEE802.1d	STP-Standard (Spanning Tree Protocol). Eine Basismethode der Netzwerkredundanz.
IEEE802.1p	PPS (Packet prioritization standard). Bei diesem Standard wird Datenpaketen ein Prioritätskennzeichen verliehen. Dadurch kann das Datenpaket vorrangig vor anderem Datenverkehr behandelt werden.
IEEE802.3	Die Standardspezifikation für das Ethernet
IEEE802.3x	Ein Standard zur Datenflusssteuerung im Ethernet. Damit kann die Geschwindigkeit eines Switch gedrosselt werden, bevor der Puffer überläuft. Der sendende Switch erhält ein Signal, das ihn auffordert, für eine bestimmte Zeit keine Datenpakete mehr zu senden.
Interface	"Schnittstelle", definierter Standard für Signale, elektrische Potentiale und Verbindungen.
Interface	‚Schnittstellenumsetzer'; Modem, das Signale zwischen zwei verschiedenen. Schnittstellen konvertiert, z. B. von RS-232 nach RS-422/485.
IP	Das IP (**I**nternet **P**rotocol) ist ohne Berücksichtigung des Inhalts von Datenpaketen für deren Übertragung von Knoten zu Knoten verantwortlich. IP befördert jedes Paket auf der Basis einer vier Bytes umfassenden Zieladresse (die IP-Adresse).
IP-Adresse	Die IP-Adresse ist eine 32-Bit-Nummer, die ein Netzwerkgerät identifiziert. Die IP-Adresse besteht aus zwei Teilen. Der erste Teil identifiziert ein spezielles Netzwerk und der zweite Teil ein spezielles Gerät in diesem Netzwerk. Wegen der begrenzten Anzahl von IP-Adressen mit einer 32-Bit-Nummer wird jetzt eine neue IPv6 Adressmethode eingeführt.
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork, ‚integriertes digitales Dienstnetz', Standard für digitale Netzwerke für Telekommunikation, Daten, Fax, Video und Videotelefonie.
Isolator	sorgt für die galvanische (elektrische) Trennung verbundener Geräten.
ISP	**I**nternet **S**ervice, ‚Dienstqualität'. **P**rovider, Internetdienstanbieter; Dienstleister, der eine Verbindung ins Internet bereitstellt.

Kollision	Kollisionen entstehen, wenn zwei oder mehr Geräte im gleichen Netzwerk zur gleichen Zeit versuchen, Daten zu übertragen. Die Datenübertragungen sind in diesem Fall fehlerhaft.
LAN	Ein Local Area Network ist eine Gruppe von Computern oder Ethernet-Geräten, die eine gemeinsame Kommunikationsstruktur teilen. Ein LAN kann einige wenige bis zu mehrere hundert Geräte umfassen.
LAPM	**L**ink **A**ccess **P**rocedure for **M**odems, ‚Verbindungsprocedere für Modems'; Methode zur Fehlerkorrektur bei der Datenübertragung mit Telefonmodems.
LCD	**L**iquid **C**rystal **D**isplay, Flüssigkristallanzeige.
Leased line	‚Mietleitung'; „Standleitung", eine zwei- oder vieradrige Drahtverbindung, die von einer Telefongesellschaft gemietet wird. Eine Standleitung kann eine Punkt-zu-Punkt-Verbindung oder eine Multidrop-Verbindung sein.
LED	**L**ight **E**mitting **D**iode, ‚Leuchtdiode'; Halbleiter, der bei angelegter Spannung Licht emittiert bzw. leuchtet.
Line sharer	‚Leitungsteiler', teilt eine Datenleitung in mehrere auf, wenn z. B. mehrere Computer einzelne Geräte gemeinsam nutzen müssen.
Local modem	‚Lokales Modem', siehe auch short-haul modem, ‚Kurzstreckenmodem'.
M2M	**M**achine-**to**-**M**achine, Abkürzung für ‚Kommunikation von Maschine zu Maschine'.
MAC-Adresse	The **M**edia **A**ccess **C**ontrol Adresse ist die eindeutige Hardwarenummer, die dem Ethernet-Gerät während der Herstellung zugeordnet wird. Normalerweise kann die MAC-Adresse nicht geändert werden.
MAN	**M**etropolitan **A**rea **N**etworks. Bezeichnung für von mehreren interessierten Gruppen genutzte Netzwerke, die in der gleichen Gegend oder der gleichen Stadt lokalisiert sind.
Manchester	‚Manchesterkodierung'; Modulationsmethode, die die Zeitsynchronisation (zur synchronen Datenübertragung) vereinfacht.
Master	‚Meister', Hauptgerät, das ‚Sklaven' genannte, nachrangige Geräte ‚polled' bzw. abfragt
MAU	**M**edia **A**ttachment **U**nit. Ermöglicht es einem Gerät, an das Lan-Medium anzudocken. Normalerweise wird für diesen Schnittstellentyp als LAN-Medium ein Koaxialkabel verwendet. Dieser Kabeltyp wird als "Thicknet" oder "Thinnet" bezeichnet.

MDI	**M**edium **D**ependant **I**nterface. Ein Ethernet-Port, der den Anschluss an andere Datenübertragungsausrüstungen (Switches, Hubs etc.) ermöglicht, ohne dass ein Nullmodem-Koaxialkabel oder eine gekreuzte Kabelverbindung erforderlich ist. Sie werden auch als Uplink-Ports bezeichnet.
MDI/MDI-X auto	Ein Ethernet-Port, der erkennt, ob der Endport ein MDI oder MDI-X Gerät ist und den Port automatisch entsprechend konfiguriert.
MDI-X	**M**edium **D**ependant **I**nterface – **C**rossover. Ein Ethernet-Port, der den Anschluss an andere Datenverarbeitungsgeräte (PCs, PLCs etc.) ermöglicht.
MIB	**M**anagement **I**nformation **B**ase. Eine Datenbank von Objekten, die von einem Managementsystem mit Hilfe von SNMP abgefragt werden kann.
MNP	**M**icrocom **N**etworking **P**rotocol, ‚Netzwerkprotokoll für Mikrocomputer', mehrere Methoden für Fehlerkorrektur und Datenkompression in Telefonmodems.
Modem	zusammengesetztes Wort aus**Mo**dulator und **Dem**odulator. Modems modulieren bzw. konvertieren Signale aus Computern in zur Übertragung geeignete elektrische Signale. Empfängerseitig existiert ein korrespondierendes Modem zur Rückkonvertierung bzw. zur Demodulation.
MSC	**M**obile **S**witching **C**enter, Übergangsstelle zu externen Netzen aus GSM-Netzwerken zu z. B. ISDN oder PSTN.
Multidrop	eine der am meisten verbreiteten Netzwerktopologien für industrielle Datennetze.
Multimode	Technologie zur optischen Datenübertragung, bei der Lichtwellen in einem Glasfaserkern reflektiert werden.
Multiplexer	eine Art "Leitungssparer", der zwei oder mehr Leitungen mit Modems an einer Einzelleitung ersetzt, in der unabhängige logische Kanäle etabliert werden.
Netzwerk	allgemeine Bezeichnung für Kommunikationsverbindungen zwischen zwei oder mehr Geräten.
NMT	**N**ordic **M**obile **T**elephony, ‚Nordische Mobiltelefonie', ein früheres analoges Mobilfunknetz.
NTP	**N**etwork **T**ime **P**rotocol. Ein Internet-Standard, der eine präzise Zeitsynchronisation der in Ethernet-Geräten vorhandenen Uhren in Millisekunden gewährleistet. Das Protokoll basiert auf TCP/IP.
OPC	**O**pen **P**rocess **C**ontrol. Formal OLE Process Control). Ein offener Standard, der die freie Kommunikation zwischen verschiedenen Geräten unabhängig von deren Hersteller ermöglicht.

Optocoupler ''Optokoppler'', optische Signalübertragungsstrecke, z. B. aus lichtemittierenden Dioden und Fototransistoren. Optokoppler übertragen keinen elektrischen Strom und sorgen so für galvanische Trennung.

Optoplexor Multiplexer für Glasfaserkabel. Siehe auch Multiplexer.

OSI **O**pen **S**ystem **I**nterconnection, ‚Offene Systemverbindung', Referenzmodell zur Definition der Handhabung von Daten in verschiedenen Kommunikationsebenen.

Paket Dies ist die Einheit von Daten, die im Internet von einer Quelle zu einem Ziel gesendet wird. Wenn Daten von einem Gerät angefordert werden, teilt der TCP-Layer der TCP/IP-Geräte die Datei in größere Einzelteile. Jedes dieser Pakete wird mit TCP/IP numeriert. Daher können alle Pakete am Zielort wieder korrekt zusammengefügt werden, obwohl sie verschiedene Routen genommen haben. Die Paketgröße reicht von 48 Bytes bis 1518 Bytes (1522 Bytes, wenn eine Prioritätskennzeichnung erfolgt).

PAP Die **P**assword **A**uthentication **P**rocedure. Ein Passwort wird als Klartext zur Überprüfung zum Server gesendet.

Parallel transfer ''Parallelübertragung'', simultane Datenübertragung in einer Schar paralleler Leitungen.
Ein Zeichen von acht Bit bzw. einem Byte benötigt acht parallele Leitungen. 32-Bit-Kommunikation überträgt gleichzeitig vier Bytes über 32 parallele Leitungen. Parallelübertragung wird vor allem innerhalb von Geräten und über sehr kurze Distanzen eingesetzt.

Parity bit ''Paritätsbit'', mathematisch errechnetes Kontrollbit, das vom Sender einer transportierten Datensequenz zugefügt wird. Der Empfänger prüft die Parität und erkennt so mögliche Übertragungsfehler.

PDP Context **P**acket **D**ata **P**rotocol Context, ‚Funkverbindungsprotokoll-Umgebung', ''Datenpaketprotokoll-Umgebung'', Information über eine GPRS-Verbindung zwischen einer MS (**M**obile **S**tation, Mobilgerät) und einem GPRS-Netz. Die Umgebung definiert Aspekte wie z.B. Routing, QoS (**Q**uality **o**f **S**ervice), Sicherheit, Tarife usw.

PDS **P**remises **D**istributed **S**ystem, 'räumlich verteilte Systeme', bezeichnet die verschiedenen Ebenen integrierter Systeme zur Daten- und Telekommunikation, Heizung, Belüftung, Überwachung usw.

Phase Modulation nutzt die Positionierung des Signals innerhalb der Wechselstromperiode bzw. im Phasenwinkel zur Kodierung von Daten. Phasenmodulation wird hauptsächlich bei digitaler Übertragung eingesetzt.

Pin 'Kontaktstift', Anschlusskontakte an z. B. einem Sub-D-Stecker oder Montage- und Lötkontakte an Bauelementen.

PLC	**P**rogrammable **L**ogic **C**ontroller, ‚speicherprogrammierbare Steuerung'.
Polling	‚Abfragen', angeschlossene Geräte werden von einem zentralen Rechner befragt, ob Informationen zur Übertragung anstehen.
POTS	**P**lain **O**ld **T**elephone **S**ystem, ‚einfaches altes Telefonsystem', identisch mit PSTN.
PPP	**P**oint to **P**oint **P**rotocol. Ein Kommunikationsprotokoll, das es einem PC ermöglicht, über eine serielle Verbindung mit einem weiteren Ethernet-Anschluss zu kommunizieren.
PRI	**P**rimary **R**ate **I**nterface , ‚Primärmultiplexanschluss', ISDN-Dienst (in Europa), der Zugriff auf zwei B-Kanäle und einen 64 kbit/s-D-Kanal bietet.
Prioritätskennung	Die Fähigkeit, eines Geräts in einem Ethernet-Netzwerk, ein Ethernet-Paket mit einem Kennzeichen zu versehen, das dem Paket vor anderen Paketen im gleichen Netzwerk eine höhere Priorität einräumt.
PROFIBUS	Industrieller Netzwerkstandard
Protocol	‚Protokoll', gibt Regeln zur Datenkommunikation vor, z. B. über die Art des Sendens und Empfangens, Signalfolgen, Beginn und Ende von Übertragungen, die Handhabung von Datenstaus und Blockaden usw.
PSTN	**P**ublic **S**witched **T**elephone **N**etwork, ‚öffentlich geschaltetes Telefonnetz', das gewohnte analoge Telefonsystem.
PTT-modem	Modem zur Datenkommunikation über das öffentliche Telefonnetz.
QoS	**Q**uality **o**f **S**ervice, ‚Dienstqualität'. Definierbares Dienst- und Qualitätsniveau in Netzwerkdiensten, z. B. für Echo, Rauschen, Fehlerhäufigkeit, Verbindungsaufbauzeit usw.
Rack modem	Modem zur Montage in einem 19" Einschubrack.
Remote	Möglichkeit, mittels eines Kommunikationsmediums wie GSM, ISDN
Repeater	'Wiederholer', Signalverstärker zum erneuten Senden von Signalen, der damit den Anschluss weiterer Netzsegmente ermöglicht.
Resistance	„Widerstand", der elektrische Widerstand eines Kabels pro Kilometer.
Ring network	‚Ringnetzwerk', zu einem geschlossenem Ring verbundene Reihe von Netzwerken, in dem alle Kommunikation durch alle Einheiten läuft.
RJ-45	Achtpoliger Stecker nach dem Standard ISO 8877.

RLP	**R**adio **L**ink **P**rotocol Context, ‚Funkverbindungsprotokoll-Umgebung', in GSM genutztes Protokoll zur Fehlerkorrektur.
RMON	**R**emote **Mon**itoring. Ein Standard MIB, das diagnostische Daten für Netzwerke liefert.
Roaming	Möglichkeit zum Einsatz von GSM-Geräten in Netzen verschiedener Betreiber.
Router	Ein Router ist ein Gerät (normalerweise ein PC), das an mindestens zwei Netzwerke angeschlossen ist und den nächsten Netzwerkpunkt festlegt, an den ein Paket gesendet werden soll. In der Regel wird ein Paket über zahlreiche Router gesendet, bevor es seinen Bestimmungspunkt erreicht. Komplexere Router haben Nachschlagetabellen, mit denen sie die schnellste oder effektivste Route ermitteln können, über die das Paket gesendet werden soll.
RS-232	aus den USA stammender Standard für serielle Datenübertragung.
Segment	Abgegrenzter Bereich eines Netzes.
Serial transfer	'serielle Übertragung', bezeichnet den aufeinanderfolgenden Versand von Einzeldaten, im Unterschied zur parallelen Übertragung.
Short-haul	moduliert das Signal und passt es an verschiedene Kabel und Schnittstellen an modems Das Modem erlaubt sichere Übertragung über große Entfernungen. Nahbereichsmodems oder lokale Modems werden in lokaler Datenkommunikation eingesetzt.
Short-range	moduliert das Signal und passt es an verschiedene Kabel und Schnittstellen an modem Das Modem erlaubt sichere Übertragung über große Entfernungen. Nahbereichsmodems oder lokale Modems werden in lokaler Datenkommunikation eingesetzt.
Simplex	Einwegkommunikation.
Singlemode	Technologie zur Übertragung optischer Signale in Glasfaserkabeln. Singlemode wird üblicherweise beim Lasertransfer in sehr dünnen Glasfasern eingesetzt.
Slave	‚Sklave', abgefragtes Gerät in einem ‚polled system', ‚einem Abfragesystem', im Gegensatz zum Master, siehe dort.
SMS	**S**hort **M**essage **S**ervice, '"Kurznachrichtendienst', Dienst zum Senden und Empfangen kurzer Textmitteilungen im GSM-Netz.
Start bit	Markiert den Beginn eines Datentransfers. Bei asynchroner Übertragung wird jeder Buchstabe bzw. jedes Byte von einem Startbit eingeleitet.

Status signal	signalisiert den Status des angeschlossenen Geräts, z.B. eingeschaltet, empfangsbereit oder sendebereit.
Stern-Netzwerk	'Sternnetz', ein um eine zentrale Einheit angeordnetes Netzwerk mit direkten Leitungen zwischen Zentrale und den angeschlossenen Geräten.
Stop bit	Ein oder mehrere Stopbits signalisieren das Ende eines übertragenen Buchstabens.
Switch	'Schalter', per Hand oder per Software gesteuertes Geräts zur Kanalisierung von Datenverkehr.
Synchronous	synchrone Übertragung, bei der Daten in einer Sequenz in konstanter Geschwindigkeit gesendet und empfangen werden. Die Übertragungsgeschwindigkeit wird von Zeitsignalen gesteuert.
TCP	**T**ransmission **C**ontrol **P**rotocol ist verantwortlich für Transport und Überprüfung von Daten von einem Gerät zu einem anderen. Das Protokoll entdeckt Fehler oder verlorene Daten und kann auch erneute Übertragungen auslösen, bis die Daten korrekt und vollständig empfangen wurden.
TCP/IP	**T**ransmission and **C**ontrol **P**rotocol/**I**nternet **P**rotocol, ‚Übertragungs- und Kontrollprotokoll/Internetprotokoll', für das Internet entwickelte Verfahren zum Zusammenschluss verschiedener LANs in ein WAN, das den Datenaustausch unter anderem unabhängig von der Quelle mithilfe eines Routingprotokolls erlaubt. Das ursprünglich UNIX-basierte Netzwerkwerkprotokoll TCP/IP hat sich auch in anderen Umgebungen fest etablieren können.
TDM	**T**ime **D**ivision **M**ultiplexing, ‚Zeitscheibenverteilung'; Multiplexverfahren, bei dem ein Kanal in Zeitabschnitte geteilt wird, die unterschiedlichen Unterkanälen zugeteilt werden. Siehe auch Multiplexer.
Telephone modem	Modem zur Kommunikation über das Telefonnetz.
Terminal	Untergeordnetes Bedienungsgerät eines Computers oder Großrechners ohne eigene Rechenkapazität. Ein PC mit eigener Rechenkapazität kann in bestimmten Anwendungen auch als Terminal agieren.
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol. Eine noch einfachere Art zur Übertragung von Dateien. Dieses Protokoll arbeitet mit dem UDP/IP-Protokoll zur Dateiübertragung.
Topology	„Topologie"; Netzwerkkonfiguration.
TP	A Copper **T**wisted **P**air Port (Port mit paarverseilter Vierdrahtleitung).
Transients	„Spannungsspitzen"; führen zu Änderungen und Störungen im Netzwerk.

UDP	**U**ser **D**atagram **P**rotocol verantwortlich für die Lieferung von Daten von einem Gerät zu einem anderen. UDP verwendet normalerweise IP, um Daten zu befördern, aber im Gegensatz zu TCP kann die Mitteilung nicht in Pakete unterteilt werden, die sich am Zielort wieder korrekt zusammensetzen lassen. Daher muss eine Anwendung mit UDP die Fähigkeit haben zu erkennen, dass die Mitteilung oder die Daten korrekt empfangen wurden. UDP bietet jedoch den Vorteil, dass die Daten im Vergleich zu TCP schneller transportiert und mit weniger Overheads beladen werden. UDP ist die ideale Anwendung zum schnellen Transport kleiner Datenmengen.
Unintelligent	Geräte, die keine Daten über sich selbst speichern können, z. B. nicht die eigene Netzwerkadresse. Beispiele unintelligenter Geräte sind einfache Ein- u. Ausgabegeräte, Messwertgeber, Sensoren, Messinstrumente usw.
Unix	Mehrbenutzersystem für Großrechner und Minicomputer, das viele Prozesse gleichzeitig handhaben kann.
V.24	aus den USA stammender Standard für serielle Datenübertragung.
WAN	A **W**ide **A**rea **N**etwork ist ein geographisch verteiltes Kommunikationsnetzwerk.
Watchdog	Überwachungsschaltung, Schaltkreis zu Überwachung und automatischen Reset von Modemfunktionen.
VN4	Französischer Standard für ISDN-Verbindungen.