
# Ethernet Basics

Rev. 02

PHOENIX CONTACT
INSPIRING INNOVATIONS

# Inhaltsverzeichnis

# Kapitel 1

# Einleitung

## 1.1 Das OSI-Modell

Die Internationale Organisation für Normung (International Organization for Standardization, ISO) hat 1979 ein Modell entwickelt, um die Welt der Datenkommunikation und Netzwerke zu strukturieren und zu standardisieren. Dieses Modell ist das OSI-Referenzmodell (Open Systems Interconnection). Ziel der ISO war es, ein Referenzmodell für die Kommunikation zwischen zwei Systemen (z. B. Computern) zu entwickeln.

Nach dem ISO/OSI-Modell (auch 7-Schichten-Modell genannt) kann ein System A mit einem System B kommunizieren (zwei Systeme zweier verschiedener Hersteller). Zwischen diesen Systemen können verschiedene Netzwerke bestehen, sowohl öffentliche, als auch private.

Ein öffentliches Netzwerk ist ein Netzwerk, das für jeden unter den für das betreffende Netzwerk geltenden Bedingungen zugänglich ist. Private Netzwerke sind häufig firmenintern.

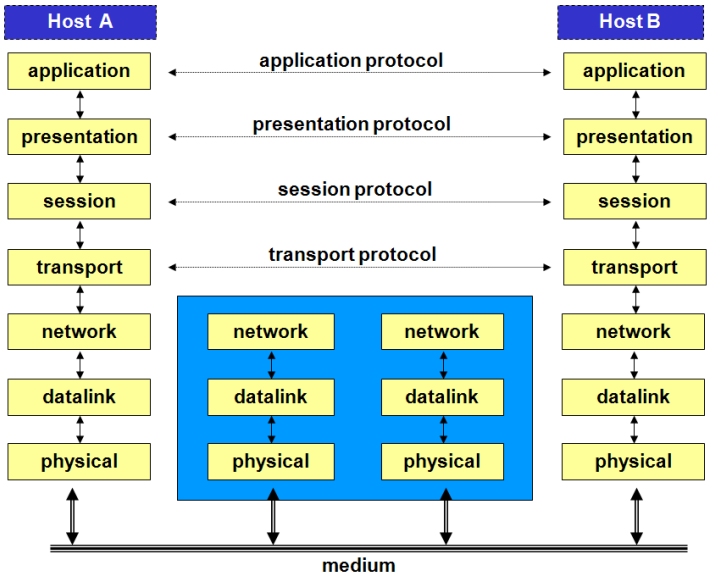


**Abbildung 1.1:** Das OSI-Modell

Das OSI-Modell besteht aus sieben funktionellen Schichten. Für jede dieser Schichten sind bestimmte Funktionen definiert. Im Folgenden wird eine knappe Übersicht über die verschiedenen Schichten gegeben:

**BIT-ÜBERTRAGUNGSSCHICHT (Schicht 1)**
Diese Schicht sorgt für die Verbindung mit dem Medium, über das die Informationen zwischen zwei Punkten im Netzwerk verschickt werden. Dies bedeutet, dass diese Schicht die mechanischen, elektrischen und/oder optischen Einheiten zur Verfügung stellt, die für das Zustandekommen, das Aufrechterhalten und das Unterbrechen der physischen Verbindung nötig sind.

**SICHERUNGSSCHICHT (Schicht 2)**
Die Protokolle der 2. Schicht geben an, wie die Frames letztlich über das Netzwerk verschickt werden. Schicht 2 weist einen Mechanismus zur Fehlererkennung und -korrektur auf, um sicherzustellen, dass Übertragungsfehler ausgeschlossen sind und die Daten an der Empfängerseite fehlerfrei empfangen werden.

**VERMITTLUNGSSCHICHT (Schicht 3)**
Auf dieser Ebene findet die Adressierung statt, also das Suchen eines Pfads durch das Netzwerk. Außerdem werden hier Maßnahmen ergriffen, um Blockaden im Netzwerk zu verhindern. Die Vermittlungsschicht sorgt auf dem Weg vom Sender zum Empfänger für die Übertragung von Nachrichten von einem Knotenpunkt zum nächsten.

**TRANSPORTSCHICHT (Schicht 4)**
Die Transportschicht ist für eine verlässliche Übertragung der Daten verantwortlich. Sie sorgt für eine logische Verbindung zwischen den beiden Endsystemen des Netzwerks (logische Punkt-zu-Punkt-Verbindung). Hierdurch wird ein fehlerfreier Datentransport sichergestellt, bei dem die Daten in der richtigen Reihenfolge beim Empfänger ankommen.

**SITZUNGSSCHICHT (Schicht 5)**
Diese Schicht sorgt für die Steuerungsstruktur des Dialogs (der Sitzung) zwischen zwei Anwendungen über das Netzwerk sowie das Öffnen und Beenden solcher Sitzungen.

**DARSTELLUNGSSCHICHT (Schicht 6)**
Die Protokolle in Schicht 6 legen fest, auf welche Weise Daten dargestellt werden. Dies ist nötig, da in verschiedenen Computersystemen Zahlen und Zeichen unterschiedlich interpretiert werden. Diese Schicht sorgt daher unter anderem für die Übersetzung zwischen verschiedenen Codierungen, z. B. von ASCII nach EBCDID.

**ANWENDUNGSSCHICHT (Schicht 7)**
Diese Schicht stellt den Anwendungen, die der Benutzer auf den Systemen des Netzwerks laufen lässt, Dienste zur Verfügung.

Nachrichten, die der Sender verschickt, müssen im Referenzmodell alle sieben Schichten durchlaufen. Jede Schicht des Modells fügt der Nachricht einen Kopf (Header) hinzu, beginnend bei Schicht 7 und absteigend bis Schicht 1 (siehe Abb. 1.2). Im Header ist verzeichnet, welche Datenkommunikationsfunktionen ausgeführt werden müssen.
Für das ordnungsgemäße Funktionieren der Kommunikationsprotokolle tauscht jede Schicht losgelöst von den Nutzdaten, die die Anwender einander über die Verbindung zuschicken, Informationen mit der korrespondierenden Schicht auf der anderen Seite der Verbindung

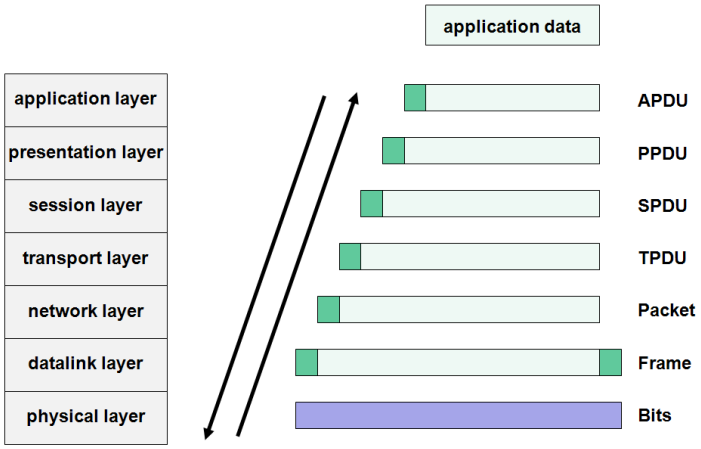


**Abbildung 1.2:** Protokoll-Overhead im OSI-Modell

aus. Im OSI-Modell fügt jede Schicht den Nutzdaten des Senders einige Informationen hinzu (den Header), die die entsprechende Schicht auf der Empfängerseite wieder entnimmt. Die Sicherungsschicht fügt gewöhnlich nicht nur am Kopf der zu übertragenden Daten, sondern auch an deren Ende Informationen hinzu. Die dem Header hinzugefügten Daten beinhalten eine Prüfsumme zur Erkennung möglicher Übertragungsfehler.
Lediglich die Bit-Übertragungsschicht fügt keine Daten hinzu.

## 1.2 LAN

Ein lokales Netzwerk (Local Area Network, LAN) dient zur Kommunikation zwischen Computern, Workstations und Peripheriegeräten in einem Gebiet mit sehr begrenztem geographischem Umfang.
In einem LAN sind die angeschlossenen Stationen autonom, es gibt also keine primären und sekundären Stationen. Jede Station kann Verbindungen mit einer anderen Station aufbauen, aufrechterhalten und beenden. Für öffentliche LANs ist für die vier unteren Schichten des OSI-Modells eine etwas andere Herangehensweise nötig.
Die Kommission 802 des Institute for Electrical and Electronic Engineers (IEEE) hat für LANs einige Standards festgelegt.
Abb. 1.3 zeigt die Umsetzung der Schichten 1 und 2 des OSI-Modells durch den IEEE802-Standard. Das allgemeine Konzept des LAN ist in der IEEE802.1-Norm zu finden.

Innerhalb der IEEE802-Kommision sind gegenwärtig die folgenden Arbeitsgruppen tätig:

- IEEE802.1 Bridging (networking) and Network Management
- IEEE802.2 Logical Link Control
- IEEE802.3 CSMA/CD (Ethernet)
- IEEE802.5 Token Ring
- IEEE802.11 Wireless LAN & Mesh (Wi-Fi certification)
- IEEE802.15 Wireless PAN

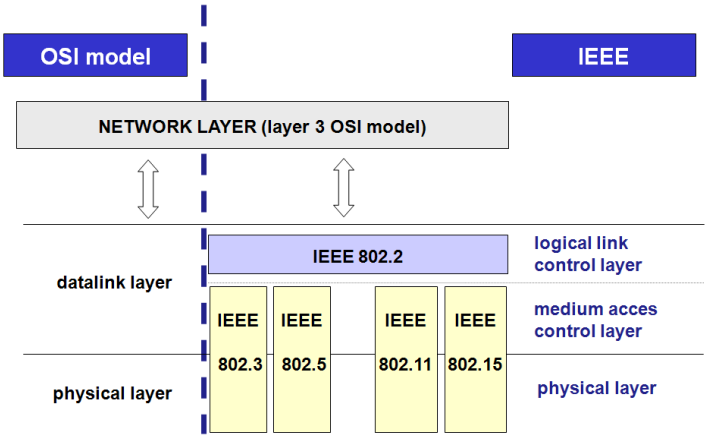


**Abbildung 1.3:** LAN im OSI-Modell

  - IEEE802.15.1 (Bluetooth certification)
  - IEEE802.15.4 (ZigBee certification)
- IEEE802.16 Broadband Wireless Access (WiMAX certification)
- IEEE802.16e (Mobile) Broadband Wireless Access
- IEEE802.16.1 Local Multipoint Distribution Service
- IEEE802.17 Resilient packet ring
- IEEE802.18 Radio Regulatory TAG
- IEEE802.19 Coexistence TAG
- IEEE802.20 Mobile Broadband Wireless Access
- IEEE802.21 Media Independent Handoff
- IEEE802.22 Wireless Regional Area Network

# Kapitel 2

# Ethernet

## 2.1 Einleitung

Basis von LANs ist das Ethernet. Der heutige LAN-Markt ist durch ein bisher unerreichtes Maß an Standardisierung auf das Ethernet gekennzeichnet. Durch seinen enormen Marktanteil verbannt der Ethernet-Standard trotz einiger Nachteile alle alternativen Technologien in Nischenanwendungen.

Eine kurze historische Übersicht:

- 1980: Digital Equipment Corporation, Intel und Xerox veröffentlichen unter dem Namen *Ethernet Blue Book* oder DIX-Standard den ersten Ethernet-Standard, Version 1.0. Dieser definiert *Thick Ethernet* als CSMA/CD mit 10 Mbit/s. Die ersten auf dem DIX-Standard basierenden Ethernet-Controller waren ab 1982 verfügbar. Die zweite und endgültige Version des DIX-Standards, Version 2.0, wurde im November 1982 veröffentlicht: *Ethernet II*.
- 1983: Das Institute of Electrical and Electronic Engineers (IEEE) veröffentlicht den ersten IEEE-Standard für Ethernet-Technologie. Dieser wurde von der 802.3-Gruppe der IEEE802-Kommission unter dem Namen *IEEE802.3 Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications* veröffentlicht. Das IEEE überarbeitete einige Teile des DIX-Standards, besonders hinsichtlich der Definition der Frames.
- 1985: IEEE802.3a; Definition von Thin Ethernet, Cheapernet oder 10Base2
- 1987: IEEE802.3d; Fiber Optic Inter Repeater Link (FOIRL): Einsatz von zwei Glasfaserkabeln, um den möglichen Abstand zwischen 10-Mbps-Repeatern bis auf 1000 m zu erhöhen.
- 1987: IEEE802.3e; 1 Mbit/s über Twisted-Pair-Kabel
- 1990: IEEE802.3i; Einführung des verbreiteten 10Base-T; 10 Mbit/s über UTP Kat. 3
- 1993: IEEE802.3j; 10Base-F, Abstände von mehr als 2 km über Glasfaserkabel
- 1995: IEEE802.3u; 100Base-T und 100Base-F
- 1997: IEEE802.3x: Vollduplex-Ethernet

- 1997: IEEE802.3y; 100Base-T2
- 1998: IEEE802.3z; 1000Base-X-Standard, allgemein bekannt unter dem Namen Gigabit-Ethernet
- 1999: IEEE802.3ab; Gigabit-Ethernet über Twisted-Pair-Kabel
- 1999: IEEE802.3ac; 802.1Q: Definition des Q-Tags mit VLAN und Prioritätsinformation
- 2003: IEEE802.3af; Power over Ethernet
- 2006: IEEE802.3an; 10GBase-T
- 2006: IEEE802.3aq; 10GBase-LRM, Ethernet over multimode fiber

Ethernet ist nichts anderes als eine Spezifizierung der Schichten 1 und 2 des OSI-Modells. Es handelt sich dabei also nicht um ein vollständiges Netzwerkprotokoll, sondern ein Subnetz, in dem andere Protokolle arbeiten können, etwa TCP/IP.

Die wichtigsten Funktionen des ETHERNET sind:

- Zurverfügungstellen der Bit-Übertragungsschicht
  - Versenden und Empfangen serieller Bitströme über das Medium
  - Detektieren von Kollisionen
- Zurverfügungstellen der Sicherungsschicht
  - MAC-Subschicht:
    - Mechanismus für den Zugang zum Netzwerk (CSMA/CD)
    - Aufbau der Daten-Frames
  - LLC-Subschicht:
    - Datenzuverlässigkeit
    - Bereitstellen von Datenkanälen für darüberliegende Anwendungen

## 2.2 Die physischen Implementierungen

Die wichtigsten Implementierungen in den vergangenen Jahren waren:

- Thick Ethernet (10Base5)
- Thin Ethernet (10Base2)
- Broadband-Ethernet (10Broad36)
- Ethernet über Twisted-Pair-Kabel (10Base-T)
- Ethernet über Glasfaserkabel (10Base-F)
- Fast Ethernet (100Base-T / 100Base-F)
- Gigabit-Ethernet (1000Base-T)
- Wireless Ethernet

### 2.2.1 Implementierungen auf Basis von Koaxialkabeln

Das ursprüngliche Ethernet wurde für eine Bustopologie entworfen. Die ersten Implementierungen des Ethernet (Thick Ethernet oder 10Base5 genannt) verwendeten ein dickes gelbes Koaxialkabel.

Merkmale des ursprünglichen Ethernets:

- 10 Mbit/s
- Baseband (Basisbandübertragung)
- max. 5 x 100 = 500 m
- max. 100 Transceiver pro Segment

Koaxialkabel für das Thick Ethernet weisen alle 2,5 m eine Markierung auf, um die korrekte Positionierung der 10Base5-Transceiver (oder MAUs) sicherzustellen. Diese Transceiver werden benötigt, um Stationen an das Netzwerk anzuschließen. Sie dürfen nur alle 2,5 m angebracht werden, um Signalreflexionen zu verhindern, die zu einer Verschlechterung der Übertragungsqualität führen.

Diese Implementationsform war schnell überholt. Nach kurzer Zeit wurde das starre und dicke gelbe Koaxkabel durch ein schwarzes, flexibleres ersetzt, was zur Implementierung des Thin Ethernet (10Base2) führte. Der Anschluss der verschiedenen Stationen geschieht durch T-förmige BNC-Anschlussstücke, wodurch eine maximale Segmentlänge von etwa 200 m möglich wird.

Bei vielen Bustechnologien ist für die Verkabelung ein wichtiges Detail zu beachten: Der Abschlusswiderstand (Terminator) - ein kleines und kostengünstiges Bauteil, das an allen Enden der im Ethernet verwendeten Koaxkabel montiert werden muss. Ein Abschlusswiderstand besteht aus einem Widerstand, über den der zentrale Leiter des Kabels mit der Abschirmung verbunden wird. Wenn ein elektrisches Signal den Abschlusswiderstand erreicht, wird es neutralisiert. Für die korrekte Funktion eines Netzwerks ist der Abschlusswiderstand unentbehrlich, da elektrische Signale an den Enden eines nicht abgeschlossenen Kabels wie Licht an einem Spiegel reflektiert werden. Wenn eine Station versucht, ein Signal über ein nicht abgeschlossenes Kabel zu senden, wird das Signal am offenen Kabelende reflektiert. Erreicht dieses reflektierte Signal den Sender, tritt Interferenz auf.

### 2.2.2 Implementierungen auf Basis von Twisted-Pair-Kabeln

Das große Problem bei Koaxkabeln ist, dass die Kommunikation nur im Halbduplexverfahren möglich ist. Auch die verwendete Busstruktur ist nicht ideal, wenn bestimmte Probleme auftreten. Um die Beschränkung der Bustopologie zu durchbrechen, ist Ethernet zu einer Topologie übergegangen, bei der auch Twisted-Pair-Kabel verwendet werden können: Dabei sind alle Stationen mit einem oder mehreren zentralen Hubs verbunden. Auf diese Weise kann eine Sterntopologie erstellt werden. Das Netzwerk kann so leichter erweitert und kontrolliert werden, auch die Fehlersuche wird erleichtert. Die maximale Segmentlänge zwischen Teilnehmer und Hub beträgt 100 m.

Die Twisted-Pair-Varianten sind von 10Base-T (10 Mbit/s) über 100Base-T (100 Mbit/s) bis 1000Base-T (1000 Mbit/s) weiterentwickelt worden.

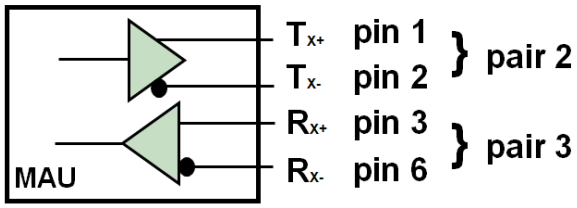


**Abbildung 2.1:** Die MAU für 10/100Base-T

Die MAU wurde für Twisted-Pair-Kabel entwickelt und verfügt über 4 Datenpins: 2 für das Senden, 2 für den Empfang auf. Dies ist die Basis für Vollduplexethernet. Grundsätzlich ist nur eine Punkt-zu-Punkt-Kommunikation möglich, da jeder Host direkt mit einem Strukturelement verbunden werden muss: einem Hub oder einem Switch.

### Fast Ethernet

UTP[1]-Kabel, z. B. CAT5[2]-UTP unterstützt Übertragungsgeschwindigkeiten bis 100 Mbit/s. Das Kabel besteht aus 8 Leitern, die zu 4 Paaren geordnet sind. Die 4 Paare können daran erkannt werden, dass der eine Leiter stets vollständig gefärbt ist, während der andere Leiter des Paares dieselbe Farbe mit weißen Unterbrechungen aufweist. Von den 4 Paaren werden bei 10/100Base-T lediglich 2 verwendet (Paar 2: orange/weiß und orange sowie Paar 3: grün/weiß und grün).

Die IEEE-Spezifikation für 10/100Base-T-Ethernet legt fest, dass das eine verwendete Paar an Pin 1 und Pin 2 des Steckers angeschlossen werden, während das zweite Paar mit den Pins 3 und 6 verbunden wird. Die verbleibenden, ungenutzten Paare werden an die Pins 4 und 5 bzw. 7 und 8 angeschlossen.

**Tabelle 2.1:** Pinbelegung für Fast Ethernet

| Pin | Farbe | Funktion |
|---|---|---|
| 1 | grün/weiß | +TD |
| 2 | grün | -TD |
| 3 | orange/weiß | +RD |
| 4 | blau | ungenutzt |
| 5 | blau/weiß | ungenutzt |
| 6 | orange | -RD |
| 7 | braun/weiß | ungenutzt |
| 8 | braun | ungenutzt |

Tabelle 2.1 zeigt die Pinbelegung für 10/100Base-T. TD steht für Transmitted Data, RD für Received Data. Die Plus- und Minuszeichen geben an, dass das Signal vorzeichenverkehrt über die zwei Datenleitungen geschickt wird, siehe Abb. 2.2.

[1] Unshielded Twisted Pair
[2] Category 5

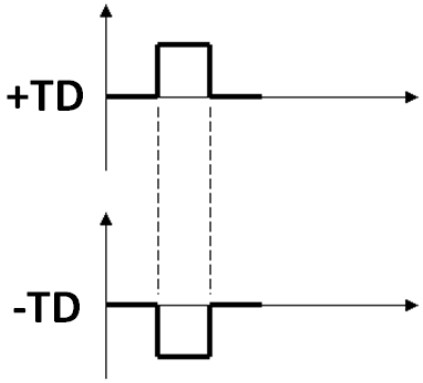


**Abbildung 2.2:** Übertragungstechnologie für 10/100Base-T

Gerade Kabel, auch Patchkabel genannt, sind solche, bei denen an beiden Kabelenden Paar 2 mit Pin 1 und 2 und Paar 3 mit Pins 3 und 6 verbunden ist. Diese Kabel können verwendet werden, um Verbindungen zwischen einem Patchfeld oder einem PC und einem Hub/Switch, oder zwischen PC und der Wandanschlussdose herzustellen. Allgemein werden diese Kabel für die Verbindung zwischen einem Strukturelement und einem Endgerät verwendet.

Ein Kreuzkabel wird benötigt, um Verbindungen zwischen zwei PCs (Verbindung zweier Anschlussgeräte) sowie zwischen einem Hub/Switch und einem weiteren Hub/Switch (Verbindung zweier Strukturelemente) herzustellen. Zur Herstellung eines Kreuzkabels müssen die verwendeten Paare miteinander vertauscht werden: An einem Kabelende wird Paar 2 mit den Pins 3 und 6 sowie Paar 3 mit den Pins 1 und 2 verbunden.

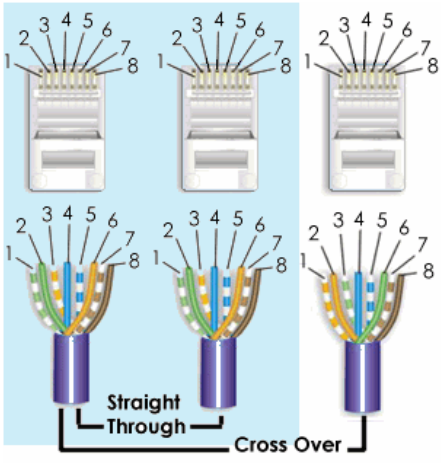


**Abbildung 2.3:** Twisted-Pair-Verkabelung, 10/100Base-T

Aktuelle Ethernet-Ports beherrschen das sogenannte Autocrossing. Dabei wird automatisch erkannt, welches Kabel verwendet wird, und ggf. die Kreuzung intern vorgenommen.

Als Erweiterung des 10-BaseT-Standards hat das IEEE das Fast Ethernet (100Base-T) definiert.

Merkmale des Fast Ethernet sind:

- Datenübertragung mit einer Geschwindigkeit von 100 Mbit/s
- Vollduplexbetrieb
- Switched Ethernet

Das Fast Ethernet verfügt über einen Autonegotiation-Mechanismus. Dieser macht Ethernetschnittstellen möglich, die automatisch zwischen 10 und 100 Mbit/s umschalten.

Beim 10Base-T-Standard wird jedes Daten-Bit in ein physisches Bit abgebildet. Für eine Gruppe von acht Daten-Bits werden also acht Signale über das Kabel gesendet. Die Datenrate von 10 Mbit/s bedeutet eine Taktfrequenz von 10 MHz. Bei jedem Taktimpuls wird ein einzelnes Bit gesendet.

100Base-T verwendet die sogenannte 4B5B-Codierung, bei der jede Gruppe von je vier Bits in ein 5-Bit-Signal umgewandelt wird. Die einzelnen Bits werden also nicht eins zu eins in Signale umgewandelt.

| | |
|---|---|
| Datenstrom: | 0111010000100000 |
| 4-Bit-Muster: | 0111 0100 0010 0000 |
| 5-Bit-Code: | 01111 01010 10100 11110 |

Die verwendete Taktfrequenz beträgt 125 MHz (5/4 x 100). Cat5-Kabel sind für Übertragungsgeschwindigkeiten bis 125 MHz zugelassen.

**Gigabit-Ethernet**

Gigabit-Ethernet strebt eine Datenrate von 1000 Mbit/s an. Falls hierfür z. B. CAT5-Ethernet-Kabel verwendet werden sollen, gibt es ein Problem, da diese nur eine Taktfrequenz bis 125 MHz unterstützen. Deshalb muss die Technologie angepasst werden.

Zunächst werden bei 1000Base-T zwei Bits pro Taktimpuls (00, 01, 10 und 11) codiert, wozu vier Spannungspegel verwendet werden.

Außerdem werden bei 1000Base-T alle vier Datenleitungspaare des Ethernet-Kabels verwendet. Die vier Paare werden dabei bidirektional verwendet: auf allen vier Paaren werden Daten gesendet und empfangen.

Gigabit-Ethernet verwendet also immer noch die 100Base-T/Cat-5-Taktrate von 125 MHz. Da bei jedem Taktsignal über jedes der vier Datenleitungspaare 2 Bits verarbeitet werden, wird insgesamt eine Datenübertragungsrate von 1000 Mbit/s erreicht. Dieses Modulationsverfahren wird 4D-PAM5 genannt und verwendet gegenwärtig fünf verschiedene Spannungspegel. Der fünfte Pegel wird für den Fehlermechanismus verwendet. Tabelle 2.2 zeigt die Pinbelegung für das Gigabit-Ethernet. Dabei steht BI für bidirektional; DA, DB, DC und DD jeweils für Data A, Data B, Data C und Data D.

**Tabelle 2.2:** Pinbelegung für Gigabit-Ethernet

| Pin | Farbe | Funktion |
|---|---|---|
| 1 | grün/weiß | +BI_DA |
| 2 | grün | -BI_DA |
| 3 | orange/weiß | +BI_DB |
| 4 | blau | -BI_DB |
| 5 | blau/weiß | +BI_DC |
| 6 | orange | -BI_DC |
| 7 | braun/weiß | +BI_DD |
| 8 | braun | -BI_DC |

### 2.2.3 Implementierungen auf Basis von Glasfaserkabeln

Um längere Segmentabstände zu ermöglichen, wurde das Glasfaserkabel als mögliche Schnittstelle integriert. Die ersten Glasfaservarianten sind unter den Namen 10Base-F und 100Base-F bekannt. Bei beiden werden für das Senden und Empfangen von Daten getrennte Lichtleiter verwendet.

Gigabit-Ethernet über Glasfaser wurde für den Vollduplexbetrieb mit einer Datenübertragungsrate von 1000 Mbit/s entwickelt. Es gibt zwei verschiedene Varianten des Gigabit-Ethernets: 1000Base-SX und 1000Base-LX.

1000Base-SX verwendet Lichtpulse mit einer kleinen Wellenlänge, die über eine Multimode-Glasfaser übertragen werden. Bei 1000Base-LX werden Lichtpulse mit einer großen Wellenlänge über eine Multi- oder Monomode-Glasfaser übertragen.
Seit Kurzem gibt es auch 10-Gigabit-Ethernet über Glasfaser in verschiedenen Varianten.

### 2.2.4 Wireless LAN

#### IEEE802.11

Das IEEE definiert unter IEEE802.11 verschiedene Standards für Wireless LAN. Die Funkverbindungen in einem Wireless LAN finden im 2,4-GHz-Band (dem sogenannten ISM[3]-Band) oder dem 5-GHz-Band statt. Hierfür sind keine Lizenzen erforderlich. Ein Wireless LAN verwendete die sogenannte Frequenzspreizung (Spread Spectrum). Diese Technik ist speziell für störungsanfällige Übertragungskanäle ausgelegt. Dies ist besonders deshalb von Bedeutung, weil die verwendeten Frequenzbänder (besonders 2,4 GHz) auch von zahlreichen anderen Systemen, z. B. Bluetooth, verwendet werden.

Ein drahtloses Netzwerk ist im Allgemeinen etwas langsamer als ein fest verdrahtetes. Sein großer Vorteil ist die Flexibilität.

Als physische Implementierung sieht IEEE802.11 die Infrastruktur- und die Ad-hoc-Konfiguration vor.

[3] Industrial, Scientific and Medical

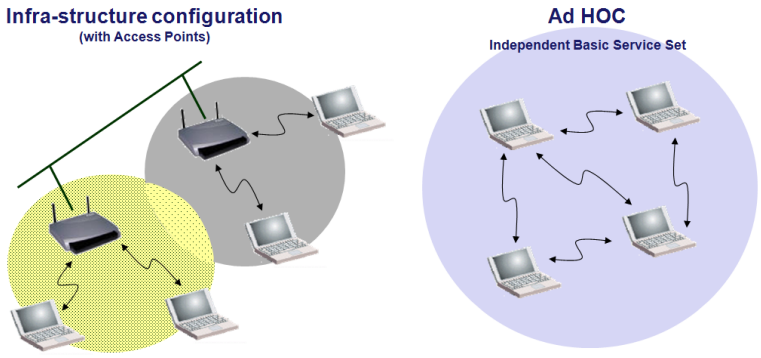


**Abbildung 2.4:** Physische Implementierung des WLAN-Standards

Bei der Infrastrukturkonfiguration wird ein Wireless Access Point verwendet, um ein drahtloses LAN mit einem verkabelten zu verbinden. Der Wireless Access Point fungiert als Zentrale für das Routen allen drahtlosen Datenverkehrs. Drahtlos arbeitende Computer, die in einen Infrastrukturmodus aufgenommen werden, bilden eine Basic Service Set (BSS) genannte Gruppe. Es können jeweils höchstens 64 individuelle Computer zum gleichen Zeitpunkt Teil eines BSS sein, da die Kapazität des Wireless Access Points auf 64 Clients begrenzt ist. Das gesamte drahtlose Netzwerk hat eine einmalige SSID (Service Set Identifier), auch Netzwerkname genannt. Dieser Name bezieht sich ausschließlich auf das drahtlose Netzwerk.

Unter Ad-hoc oder Peer-to-Peer wird eine drahtlose Konfiguration verstanden, bei der jeder Teilnehmer direkt mit anderen kommuniziert. Eine echte Organisation des Netzwerks ist hier daher nicht möglich. Ein drahtloses Ad-hoc-Netzwerk besteht aus einer Anzahl Geräten, die jeweils mit einem drahtlosen Adapter ausgestattet sind. Diese sind über Funksignale direkt miteinander verbunden und bilden so ein unabhängiges drahtloses LAN.

### WLAN-Standards

Im Rahmen der IEEE802.11 sind verschiedene Standards definiert. Diese Standards verwenden verschiedene Modulationstechniken, um die Übertragungsgeschwindigkeiten zu optimieren. Tabelle 2.3 zeigt eine Übersicht der verschiedenen Standards.

**Tabelle 2.3:** WLAN-Standards gemäß IEEE802.11

| Standard | Frequenzband | Übertragungsrate |
|---|---|---|
| IEEE802.11b | 2,4 GHz | 11 Mbit/s |
| IEEE802.11g | 2,4 GHz | 54 Mbit/s |
| IEEE802.11a | 5 GHz | 54 Mbit/s |
| IEEE802.11h | 5 GHz | 54 Mbit/s |
| IEEE802.11n | 5 GHz und/oder 2,4 GHz | 600 Mbit/s |

### IEEE802.11b/g

IEEE802.11b/g verwendet den 72 MHz breiten Teil des 2,4-GHz-Bandes. Gemäß den Vorschriften der FCC sind darin 11 Kanäle mit einer Breite von je 22 MHz definiert. Theoretisch wäre so eine Bandbreite über diese 11 Kanäle von 242 Mbit/s (11x22 Mbit/s) möglich. In der Praxis wird dieser Wert jedoch bei Weitem nicht erreicht, da die Kanäle einander stark überlappen. Abb. 2.5 zeigt, dass lediglich drei Kanäle einander nicht gegenseitig überlappen: Kanal 1, 6 und 11.

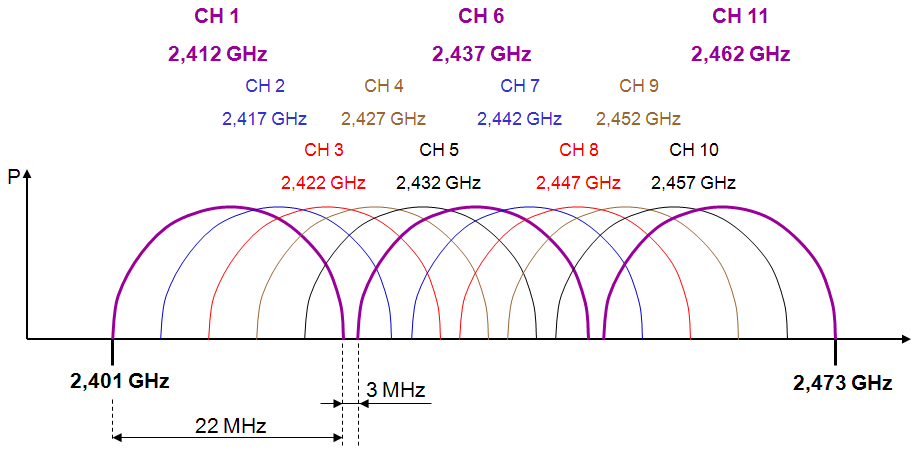


**Abbildung 2.5:** Das 2,4-GHz-Band für WLAN

Für Europa hat die ETSI ein etwas größeres Frequenzband mit 13 Kanälen zu je 22 MHz Bandbreite definiert. Deshalb können in Europa grundsätzlich 4 einander kaum überlappende Kanäle (nämlich 1, 5, 9 und 13) verwendet werden.

IEEE802.11b unterstützt eine maximale Geschwindigkeit von 11 Mbit/s. Mit IEEE802.11b ist eine maximale Geschwindigkeit von 54 Mbit/s möglich. Bei einer schlechten Verbindung oder großem Abstand zum Access Point wird die Geschwindigkeit dynamisch reduziert.

### IEEE802.11a/h

IEEE802.11a verwendet das komplette 5-GHz-Band. Durch Anwendung des OFDM (Orthogonal Frequency Division Multiplexing) erreicht IEEE802.11a eine (theoretische) Höchstgeschwindigkeit von 54 Mbit/s. Abb. 2.6 zeigt die verschiedenen Kanäle im 5-GHz-Band. Für Europa bedeutet dies, dass auf den zwei niedrigsten Bändern des 5-GHz-UNII-Bandes 8 einander nicht überlappende Kanäle mit einer Bandbreite von 20 MHz zur Verfügung stehen.

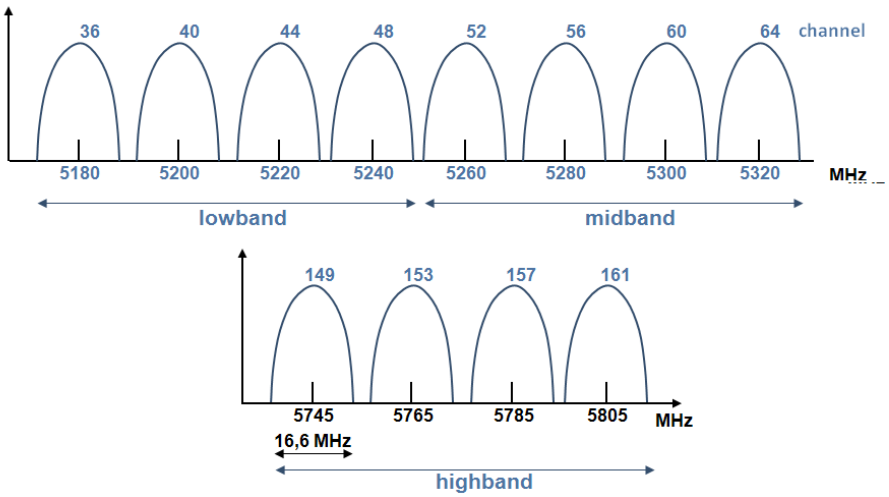


**Abbildung 2.6:** Das 5-GHz-Band für WLAN

Der Einsatz des 5-GHz-Bandes ist in Europa im Vergleich zu den USA zahlreichen Beschränkungen unterworfen. Deshalb wurde IEEE802.11a angepasst, was zu IEEE802.11h führte. Um den in Europa geltenden Vorschriften zu genügen, wurden zwei wichtige Protokolle hinzugefügt:

- DCS (Dynamic Channel Selection): Der AP sucht automatisch einen anderen Kanal, wenn er feststellt, dass ein bestimmter Kanal bereits von einer anderen Anwendung benutzt wird.
- TPC (Transmit Power Control): Die Sendeleistung ist nicht größer als nötig: Wenn zwei Teilnehmer Kontakt zueinander haben, regelt der AP die Sendeleistung auf den kleinsten ausreichenden Wert ab.

#### IEEE802.11n

Dieser neue Standard verwendet das MIMO-Verfahren (Multiple Input - Multiple Output), mit dem durch Einsatz mehrerer Sende- und Empfangsantennen Daten drahtlos mit einer Geschwindigkeit von bis zu 600 Mbit/s übertragen werden können, sofern 4 Kanäle mit einer Bandbreite von je 40 MHz verwendet werden.

### 2.2.5 Bluetooth

Der Standard für die Basistechnologie (die beiden untersten Schichten des OSI-Modells) ist in der IEEE802.15.1 festgelegt. Ergänzend definiert die Bluetooth-SIG (Special Interest Group) verschiedene Anwendungsprofile, u. a. für die serielle Kommunikation und die Übertragung von Ethernet-Daten-Frames.

Bluetooth verwendet das lizenzfreie 2,4-GHz-ISM-Band. Im Gegensatz zum WLAN werden die zu sendenden Daten nicht über ein breiteres Frequenzband gespreizt, sondern es wird das sogenannte FHSS (Frequency Hopping Spread Spectrum) angewendet. Hierbei wird das 2,4-GHz-Band in 79 Kanäle zu je 1 MHz aufgeteilt. Abb. 2.16 zeigt die Funktionsweise von FHSS. Es werden 1600 Frequenzsprünge pro Sekunde ausgeführt. Jeder Daten-Frame wird jeweils

auf einer anderen Frequenz gesendet. Auf diese Weise können verschiedene logische Kanäle nebeneinander aktiv sein.

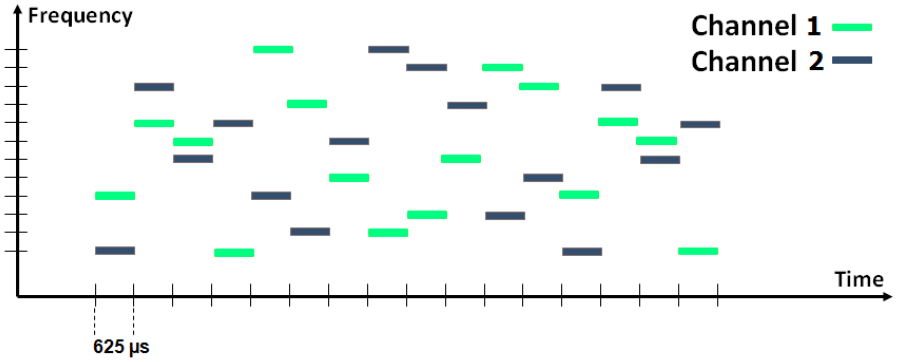


**Abbildung 2.7:** FHHS-Technologie

Ein großer Vorteil beim Einsatz von Bluetooth in der Industrie liegt in der problemlosen Koexistenz mit WLAN. Falls auf einer Bluetooth-Frequenz Interferenz durch einen WLAN-Kanal auf derselben Frequenz auftritt, kann Bluetooth diese Frequenz(en) meiden. Da dieses Phänomen häufig auftritt, verfügt Bluetooth über einen automatischen Koexistenzmechanismus: Adaptive Frequency Hopping (AFH).

Dieser Mechanismus erlaubt es Bluetooth, bestimmte ßchlechteFrequenzen zeitweilig aus der Liste der Frequenzen zu streichen, die für das Hopping verwendet werden. Abb. 2.8 zeigt, dass bei einem voll besetzten 2,4-GHz-Band mit drei aktiven und einander nicht überlappenden WLAN-Kanälen genug Platz für Bluetooth ist. Der WLAN-Kanal verwendet ein statisches Frequenzband, Bluetooth hingegen kann sich anpassen und hat die Wahl aus ausreichend vielen Frequenzen, um Interferenzen zu vermeiden.

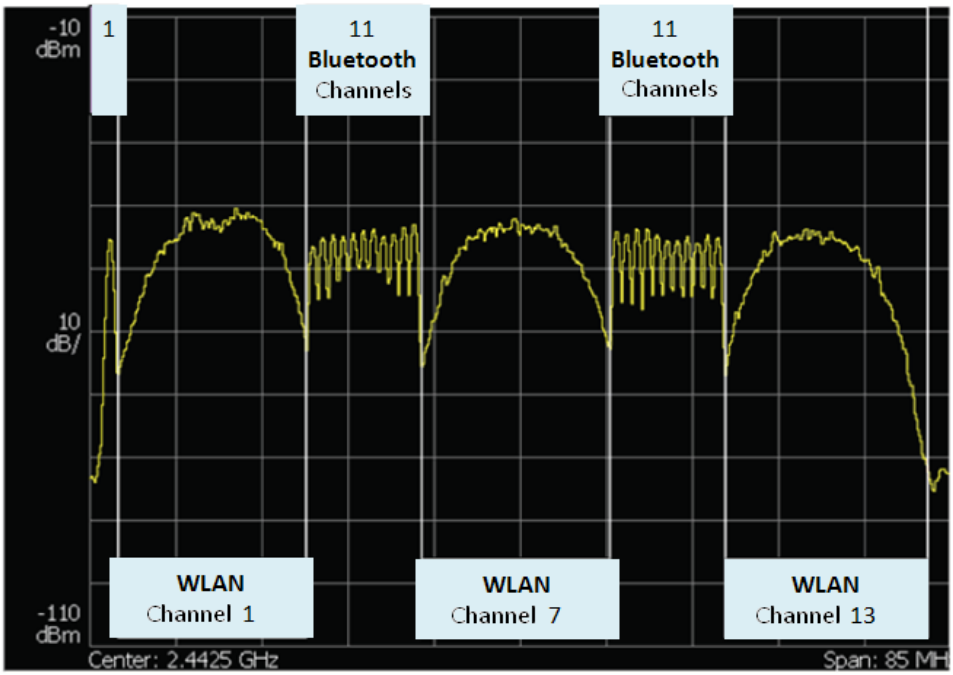


**Abbildung 2.8:** Koexistenz von Bluetooth und WLAN

## 2.3 Die Sicherungsschicht

### 2.3.1 Einleitung

Nachrichten werden nach dem Paketvermittlungsverfahren versendet. Paketvermittlung wird vor allem bei der Kommunikation von Computer zu Computer angewendet. In Computernetzwerken werden Daten nicht in einem kontinuierlichen Strom übertragen. Stattdessen teilt das Netzwerksystem die Daten in kleine Blöcke, die sogenannten Pakete auf, die einzeln übertragen werden. Computernetzwerke werden aus diesem Grunde auch Paketvermittlungsnetzwerke (Packet Switching Networks) genannt.

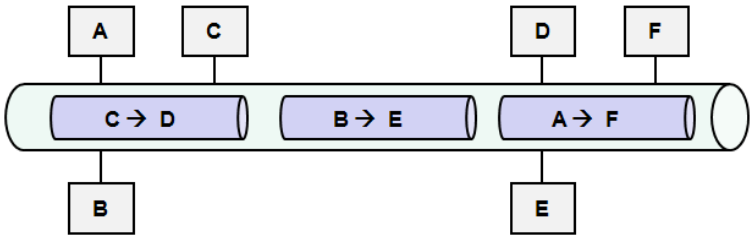


**Abbildung 2.9:** Paketvermittlung

Die Verwendung von Paketen hat zwei Gründe:

- Sender und Empfänger müssen die Übertragung koordinieren. Im Falle von Übertragungsfehlern kann viel Information verloren gehen. Werden die Daten in kleinere Blöcke

aufgeteilt, so können Sender und Empfänger leichter feststellen, welche Blöcke korrekt empfangen wurden und welche nicht.

- Mehrere Computer nutzen die darunterliegende Verbindung und Hardware gemeinsam. Ein Netzwerk muss dafür sorgen, dass alle Computer gleichwertigen direkten Zugang zu einem gemeinsam genutzten Übertragungsweg haben. Ein Computer darf eine gemeinsam genutzte Ressource nicht länger in Beschlag nehmen, als es für das Versenden eines einzigen Pakets nötig ist.

### 2.3.2 MAC-Adresse

Auf einem gemeinsamen Übertragungsmedium eines LAN muss jede Station über eine eindeutige Adresse verfügen. Jeder Teilnehmer hat eine Ethernet-Adresse, eine physikalische Adresse, die der Netzwerkkarte zugeordnet ist: die MAC-Adresse (Medium Access Control Address). Jeder Hersteller von Netzwerkkarten gibt jeder Karte eine einzigartige Adressnummer, die im ROM der Karte gespeichert wird.

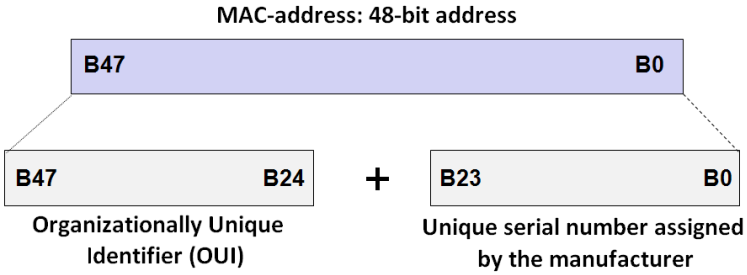


**Abbildung 2.10:** Die MAC-Adresse

Die MAC-Adresse setzt sich aus 48 Bits (6 Bytes) und ist in zwei Gruppen zu je drei Bytes aufgeteilt. Die höherwertigen 24 Bits bilden eine Herstellernummer, die von XEROX vergeben wird. Es gibt 4194302 mögliche Herstellernummern, Phoenix Contact hat die Nummer 00A045h.

Die niederwertigsten 24 Bits bilden eine Seriennummer. Jede MAC-Adresse darf nur einmal vergeben werden.

### 2.3.3 Der Ethernet-Daten-Frame

Ein Ethernet-Frame besteht aus mindestens 46 effektiven Datenbytes und einer konstanten Anzahl von 26 Protokollbytes (Overhead). Diese Mindestanzahl an Datenbytes ist aufgrund der Definition der Slotzeit nötig.

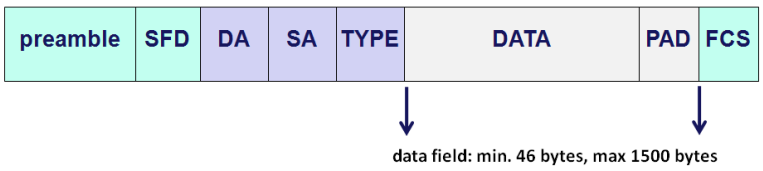


**Abbildung 2.11:** Aufbau eines Ethernet-Daten-Frames

In einem Ethernet-Daten-Frame sind die folgenden Felder definiert:

- Präambel: Die Präambel ist eine Folge von 56 Bits, jeweils abwechselnd 1 und 0. Diese Bits werden für die Synchronisation verwendet und verschaffen jedem Teilnehmer die nötige Zeit, um die Aktivität auf dem Bus wahrzunehmen, bevor die Nutzdaten übertragen werden.
- SFD: Der Start of Frame Delimiter (10101011) ist das letzte Byte der Präambel und signalisiert dem Empfänger, dass als nächstes die Nutzdaten folgen.
- DA: Die Zieladresse (Destination Address). Die Ziel-MAC-Adresse identifiziert die Station oder die Stationen, für die die Nachricht bestimmt ist. Das Feld ist 6 Bytes lang. Die Zieladresse kann eine individuelle, eine Multicast- oder eine Broadcast-Adresse sein. Die MAC-Broadcast-Adresse lautet FF FF FF FF FF FF.
- SA: Die Quelladresse (Source Address). Die Quell-MAC-Adresse identifiziert die Station, von der die Nachricht stammt. Das Feld ist 6 Bytes lang.
- TYPE: Das Typfeld (Type) ist beim Ethernet II (DIX-Standard) anders als bei IEEE802.3. Bei Ethernet II verweist das Typfeld auf das darüberliegende Protokoll, das einen Ethernet-Frame verwendet, um Daten zu verschicken. Xerox weist jedem Protokoll, das für das Ethernet entwickelt wurde, einen 2 Byte langen Code zu. Einige Beispiele:

  | | |
  |---|---|
  | 0600h | XNS |
  | 0800h | IP (Internet Protocol) |
  | 0806h | ARP protocol |
  | 0835h | Reverse ARP protocol |
  | 8100h | IEEE802 1.q tag frame (VLAN) |

  IEEE802.3 definiert das Feld TYPE als LENGTH-Feld, um die effektive Anzahl der Datenbytes mitsenden zu können.

  Da Xerox keine Typnummern unterhalb 1500 verwendet und die maximale Länge eines Daten-Frames 1500 beträgt, ist keine Überlappung möglich, und beide Definitionen können gemischt verwendet werden.
- DATA: Das Datenfeld enthält die zu versendenden Daten. Das Datenfeld ist transparent, das heißt, dass der Inhalt des Felds im Ethernet vollständig frei gewählt werden kann. Die einzige Beschränkung liegt in der Länge: Sie muss mindestens 46 und darf höchstens 1500 Bytes betragen.
- PAD: Die Padding-Bits sind willkürliche Daten-Bits, die ggf. den Daten hinzugefügt werden, um die erforderliche Mindestlänge von 46 Datenbytes zu erreichen.
- FCS: Dies ist eine 4 Byte lange CRC-Prüfsumme, die vom Sender errechnet und mitgesendet wird. Anhand dieser Prüfsumme kann der Empfänger die Integrität der empfangenen Daten überprüfen.

### 2.3.4 CSMA/CD

Ethernet verwendet das CSMA/CD-Protokoll (Carrier Sense Multiple Access / Collision Detect). Mit CSMA/CD können zwei oder mehr Stationen ein gemeinsames Übertragungsmedium nutzen. Um einen Daten-Frame zu senden, muss eine Station auf eine Ïdle Period"warten: die Inaktivität des Busses, bei der kein Teilnehmer Daten versendet. Es wird dann eine Nachricht versendet, die alle anderen Teilnehmer empfangen. Wenn ein zweiter Teilnehmer gleichzeitig eine Nachricht verschicken möchte, wird eine Kollision detektiert. Der Teilnehmer, der als erster eine Kollision erkennt, sendet einen Error-Frame (Fehler-Frame).

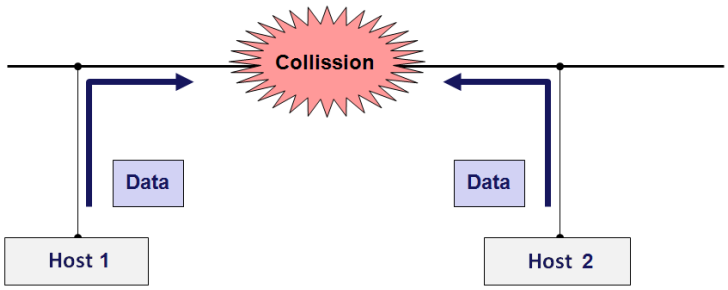


**Abbildung 2.12:** Kollision in einem Ethernet-Segment

Eine Kollisionsdomäne ist eine Mehrsegmentkonfiguration im CSMA/CD-Protokoll, bei der eine Kollision entsteht, sobald zwei Teilnehmer im Segment zum selben Zeitpunkt einen Daten-Frame senden.

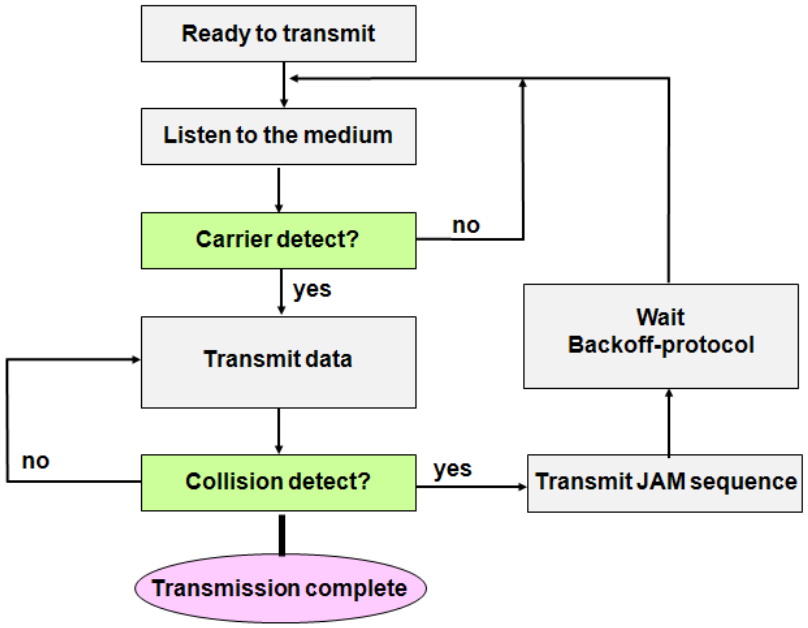


**Abbildung 2.13:** CSMA/CD-Flussdiagramm

Abb. 2.13 zeigt ein CSMA/CD-Flussdiagramm. Ein Teilnehmer, der Daten senden will, muss

zunächst das Netzwerk auf das Vorhandensein eines *Trägers* oder einer Station, die gegenwärtig Daten sendet, überprüfen. Falls ein aktiver Träger erkannt wird, wird mit dem Versenden der Daten gewartet.

Wird über einen Zeitraum, der größer oder gleich dem Interframe Gap ist, kein aktiver Träger erkannt, so kann die Station mit dem Senden der Nachricht beginnen. Während des Sendens der Nachricht muss der Teilnehmer das Medium weiterhin auf Kollisionen überprüfen. Eine Netzwerkschnittstelle muss daher gleichzeitig Daten versenden und das Medium abhören. Falls eine Kollision erkannt wird, wird die Übertragung sofort unterbrochen und ein 32 Bit langes Jam-Signal gesendet. Falls die Kollision sehr frühzeitig erkannt wird, wird zunächst die Präambel des Frames vollständig gesendet, bevor das Jam-Signal übertragen wird. Dieses Jam-Signal ist nötig, um sicherzustellen, dass die Länge der Kollision ausreichend groß ist, dass alle Teilnehmer sie erkennen können. Nach dem Senden des Jam-Signals wartet der Teilnehmer eine zufällige Zeitspanne, bevor ein neuer Versuch unternommen wird. Dies wird Backoff genannt.

Einige weitere wichtige Definitionen:

- Interframe Gap: Ethernet-Teilnehmer müssen zwischen dem Versenden zweier Frames eine gewisse inaktive Mindestzeit, die Ïdle Periodëinhalten. Der Interframe Gap dauert so lange wie die Übertragung von 96 Bits (9,6 $\mu$s bei 10 Mbit/s, 960 ns bei 100 Mbit/s und 96 ns beim Gigabit-Ethernet.).
- Slot-Zeit: Dieser Parameter ist definiert als 512 Bitzeiten für 10 und 100 Mbit/s, beim Gigabit-Ethernet beträgt er 4096 Bit-Zeiten. Die Übertragungszeit für einen vollständigen Daten-Frame muss mindestens eine Slot-Zeit betragen. Die Zeit, die benötigt wird, bis alle Teilnehmer eine Kollision erkennen, darf höchstens eine Slot-Zeit betragen.

  Die Slot-Zeit ist ein wichtiger Parameter:

  - Sie legt die Mindestlänge eines Daten-Frames fest (64 Bytes für 10 und 100 Mbit/s). Jeder Frame, der kleiner als 64 Bytes ist, wird als Kollisionsfragment betrachtet.
  - Sie bestimmt die maximale Länge einer Kollisionsdomäne, um späte Kollisionen zu vermeiden.
  - Sie stellt sicher, dass auftretende Kollisionen innerhalb der 512 Bitzeiten der Übertragungszeit des Frames stattfinden.

### 2.3.5 CSMA/CA

Beim drahtlosen Ethernet kann die CSMA/CD-Technologie des drahtgebundenen Ethernets nicht angewendet werden. Dieser Standard beschreibt Halbduplex-Funksignale: Während Daten gesendet werden, kann nicht kontrolliert werden, ob evtl. Kollisionen vorliegen. Abhilfe schafft eine andere Technologie: CSMA/CA. Anstatt Kollisionen zu erkennen, werden sie vermieden: CA steht für Collision Avoidance.

Die Wahrscheinlichkeit von Kollisionen ist am größten, kurz nachdem ein Medium besetzt war. Es werden deshalb Wartezeiten und eine Zugriffsphase definiert. Abb. 2.14 zeigt einige wichtige Parameter im Zusammenhang mit den Wartezeiten für den Zugang zum Medium. Alle Parameter sind von der Slot-Zeit abhängig, die wiederum von der durch das Medium verursachten Ausbreitungsverzögerung abgeleitet ist. Diese Parameter sind:

- SIFS (Short Interframe Spacing): Dies ist die kürzeste Wartezeit für den Zugang zum Medium (also die höchste Priorität). Der Access Point verwendet diese Wartezeit für das Versenden von ACK-Nachrichten.
- PIFS (PCF Interframe Spacing): Diese Zeit wird für das Polling eines Access Points verwendet (mittlere Priorität).
- DIFS (DCF Interframe Spacing): Dies ist die niedrigste Priorität für den Zugang zum Medium und gilt für normale Teilnehmer im drahtlosen Segment.

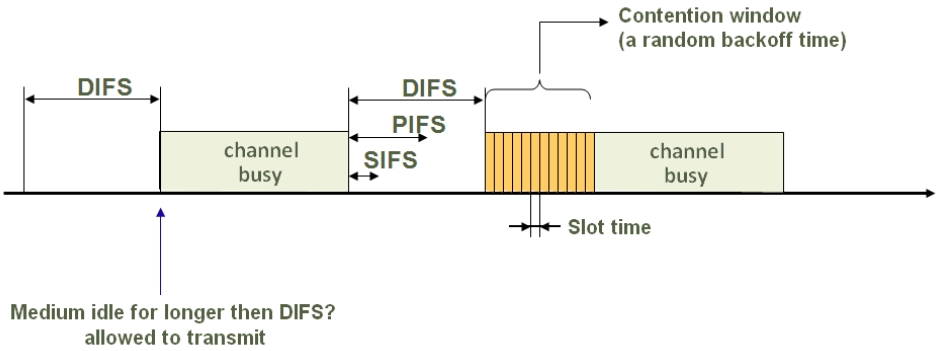


**Abbildung 2.14:** CSMA/CA

Wenn ein Host eine Nachricht senden möchte, muss er zunächst "horchen". Wenn das Medium länger als die DIFS-Zeit frei ist, kann der Teilnehmer die Initiative ergreifen und die Nachricht senden.

Ist das Medium besetzt, wird gewartet, bis der sendende Teilnehmer den Sendevorgang abgeschlossen hat. Danach muss die Wartezeit DIFS eingehalten werden. Der Access Point hat eine höhere Priorität und muss daher nur die Wartezeit SIFS einhalten. Wenn nach Ablauf des DIFS das Medium immer noch frei ist, beginnt die Zugriffsphase, bei der jeder Host, der Daten senden möchte, einen zufälligen Backoff-Timer startet. Der Teilnehmer, dessen Backoff-Timer als erster abläuft, kann die Initiative ergreifen und Daten über das Medium versenden.

## 2.4 Strukturelemente des Ethernet

### 2.4.1 Der Hub

Die maximale Segmentlänge eines LAN wird durch das verwendete Medium und den verwendeten Zugangsmechanismus bestimmt. Um die Beschränkung der Länge aufzuheben, wurde bereits nach kurzer Zeit mit der Suche nach Methoden zur Kopplung mehrerer Segmente aneinander begonnen. Die erste und einfachste Methode ist hierbei der Einsatz eines Repeaters. Ein Repeater ist ein Signalverstärker, der Pakete unabhängig von deren Inhalt transparent weitergibt. Mit einem Repeater lassen sich zwei oder mehr Ethernet-Segmente miteinander verbinden. Wie auf der Abbildung zu sehen ist, findet eine Repeater-Kopplung gemäß ISO/OSI-Definitionen auf der Bit-Übertragungsschicht statt.

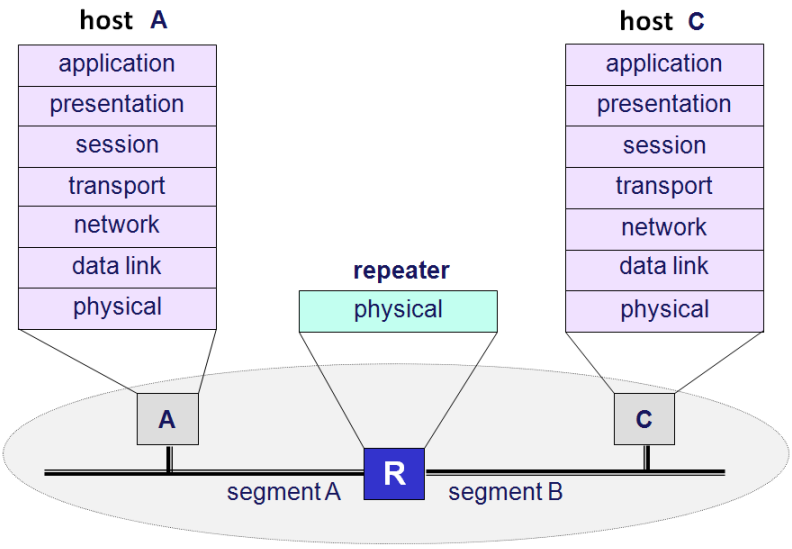


**Abbildung 2.15:** Der Repeater im OSI-Modell

Die Übertragungsmedien der Segmente können unterschiedlich sein. So kann z. B. ein 10Base-T-Segment mittels eines Repeaters an ein Glasfasersegment gekoppelt werden. Eine andere wichtige Eigenschaft einer Kopplung mit einem Repeater ist, dass nicht nur die Daten-Bits, sondern auch eventuelle Kollisionen und Signalfehler weitergegeben werden. Netzwerksegmente, die über einen Repeater miteinander verbunden sind, sind daher empfindlich für Fehlersituationen: Ein in einem der Segmente auftretender Fehler setzt sich auch in alle anderen Segmente fort. In modernen lokalen Netzwerken auf Ethernet-Basis werden Repeater hauptsächlich verwendet, um Segmente mit unterschiedlichen Medien miteinander zu verbinden. So werden z. B. Backbone-Segmente (Glasfaser) stets über optische Repeater an Abteilungssegmente mit Twisted-Pair-Verkabelung angeschlossen.

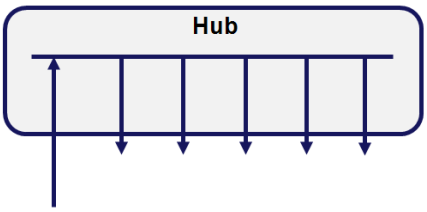


**Abbildung 2.16:** Der Hub

Ein Hub ist eigentlich ein Multiport-Repeater: Er gibt ein eingehendes Signal an alle anderen Ports weiter, wie in Abb. 2.16 zu sehen. Alle über einen Hub miteinander verbundenen Segmente bilden eine Kollisionsdomäne.

Hubs sind in zahlreichen verschiedenen Ausführungen erhältlich. Sie unterscheiden sich in der Anzahl der Ports, den unterstützten Medientypen und der Erweiterbarkeit.

Eine wichtige Funktionalität moderner Hubs ist die Fähigkeit zum Netzwerkmanagement. Hubs können mindestens Ports an- oder ausschalten und Störungen erkennen. Um diese

Möglichkeiten zur Verfügung stellen zu können, sind moderne Hubs mit einem SNMP-Agenten ausgestattet, der von einer Managementstation verwaltet wird.

### 2.4.2 Der Switch

Eine der Möglichkeiten, LAN-Segmente mit einer höheren Intelligenz miteinander zu verbinden, ist die Verwendung einer Bridge. Eine Bridge ist mehr als nur ein Medium für das Weitergeben von Daten wie beim Repeater. Eine Bridge untersucht vor dem Weitergeben eines Pakets von einem Segment zum anderen die MAC-Adresse und entscheidet in Abhängigkeit davon, ob der Transport in das andere Segment stattfindet oder nicht.

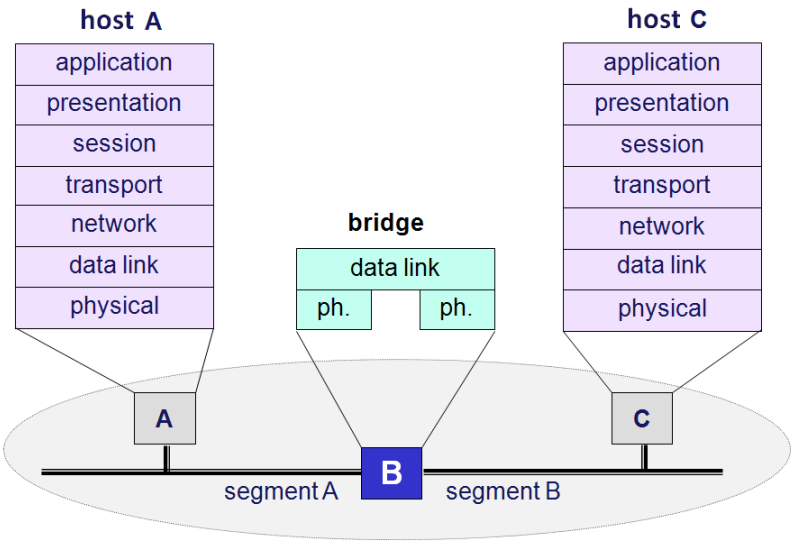


**Abbildung 2.17:** Die Bridge im OSI-Modell

Eine Bridge kann mehr als zwei Netzwerkports aufweisen. In diesem Fall wird die Bezeichnung Switch gebraucht. Für jeden Port wird softwareseitig eine MAC-Adresstabelle geführt. Diese Tabelle wird ausgefüllt, in dem der Switch die MAC-Adressen, die die Teilnehmer als Absenderadressen verwenden, registriert. Jede Adresse wird eine begrenzte Zeit in der Tabelle gehalten und wieder gelöscht, wenn eine bestimmte Zeit, die Aging-Time, verstrichen ist. Auf diese Weise wird verhindert, dass Stationen nicht mehr erkannt oder inaktive Stationen adressiert werden.

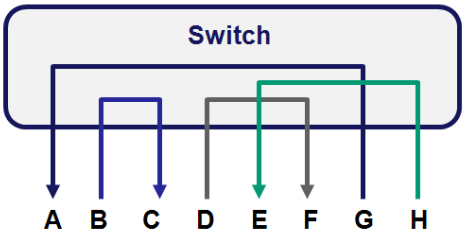


**Abbildung 2.18:** Der Switch

Der Einsatz eines Switches zur Kopplung von Segmenten in einem lokalen Netzwerk hat gegenüber der Verwendung eines Repeaters oder Hubs einige Vorteile. So werden z. B. beim Einsatz eines Switches Segmente nicht mit Frames belastet, die für andere Segmente adressiert sind. Die Belastung pro Segment wird durch diese Funktion der Bridge also reduziert. Ebenso werden Fehlersituationen nicht weitergegeben, da der Switch auch den korrekten Aufbau des Frames überprüft. Schließlich wird durch die Bridge auch verhindert, dass Kollisionen zwischen Frames von einem Segment in ein anderes weitergegeben werden. Jeder Port eines Switches schließt also eine Kollisionsdomäne ab. Wenn jeder Teilnehmer direkt an den Port eines Switches angeschlossen wird, entstehen zwar viele Kollisionsdomänen, doch enthält jede von ihnen nur einen einzigen Teilnehmer, weshalb keine Kollisionen auftreten können. Es wird an anderer Stelle noch detaillierter auf den Switch eingegangen.

## 2.5 IEEE802.1Q Tagged Frame

IEEE801.1Q beschreibt 4 zusätzliche Bytes, aufgeteilt in zwei weitere Felder im Ethernetframe, um neue Anwendungen zu ermöglichen. Eine dieser Anwendungen ist das VLAN (siehe weiter unten in diesem Kapitel).

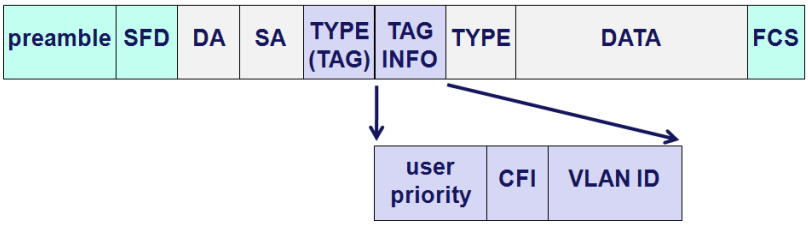


**Abbildung 2.19:** Aufbau eines Tagged Frame

Beschreibung der zusätzlichen Felder:

- TYPE(TAG), 2 Bytes: erhält den Wert 8100h, um anzugeben, dass das betreffende Frame ein Tagged Frame ist und daher ein zusätzliches Informationsfeld enthält
- VLAN TPID, 2 Bytes: VLAN Tag Protocol Identifier
  - User Priority, 3 Bits: hier wird die Priorität des Frames mitgesendet, der Prioritätscode (eine Zahl zwischen 0 und 7) ist in IEEE802.1p beschrieben
  - CFI: Canonical Format Indicator. IEEE802.1Q wurde ausschließlich für Ethernet- oder Token-Ring-Netzwerke entwickelt. Dieses Bit hat den Wert 0 für Ethernet und 1 für Token Ring.
  - VLAN ID: Identifikation des VLAN, 4094 Möglichkeiten

| | |
|---|---|
| FFFFh | reserviert |
| 0000h | kein VLAN, Frames mit Priorität (Profinet IO) |

## 2.6 Power over Ethernet

IEEE802.3af *(Power over Ethernet)* bietet seit Juni 2003 die Möglichkeit zur gleichzeitigen Übertragung von Daten und Energie über dasselbe Ethernet-Kabel.

PoE wurde für WLAN-Access-Points, Bluetooth-Access-Points, IP-Telefone (Voice over IP), IP-Kameras, RFID-Lesegeräte, Touchscreens etc. entwickelt. Bereits vor Einführung dieses Standards wurden nicht genormte Systeme verwendet, die über die ungenutzten Adern des Ethernet-Kabels eine Versorgungsspannung von 24 oder 48 V übertragen. Über den IEEE802.3af-Standard kann der zu den Geräten geführte Strom begrenzt und gesteuert werden. Durch den Einsatz von PoE wird ein gesondertes Netzteil überflüssig. Dies ist besonders nützlich, wenn das Netzwerkgerät an einem Ort eingesetzt werden soll, wo die Stromversorgung über eine Steckdose schwierig zu verwirklichen ist.

Das Protokoll definiert zwei Basiskomponenten: Das PSE (Power Sourcing Equipment) und das PD (Powered Device).

### 2.6.1 PSE

Das Gerät, das die Versorgungsspannung für das PoE zur Verfügung stellt, wird PSE (Power Sourcing Equipment) genannt. Die vom PSE zur Verfügung gestellte Nennspannung beträgt 48 V (zwischen 44 und 57 V). Jeder Port eines PSE muss an 44 V einen Strom von 350 mA zur Verfügung stellen können (15,4 W).

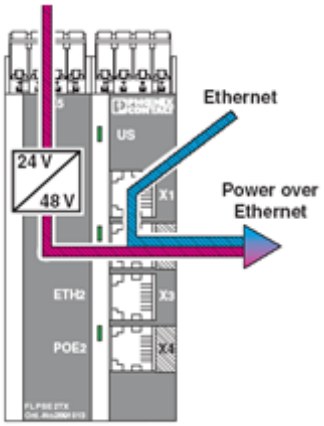


**Abbildung 2.20:** Aufbau eines PSE

Es werden zwei verschiedene Typen unterschieden:

- End Point PSE: der Standard-Ethernetswitch wird durch einen PoE-Switch ersetzt
- Mid Span PSE: dieses Gerät wird zwischen dem konventionellen Switch und dem Netzwerkteilnehmer eingefügt (nur mit Alternative B möglich, s. u.)

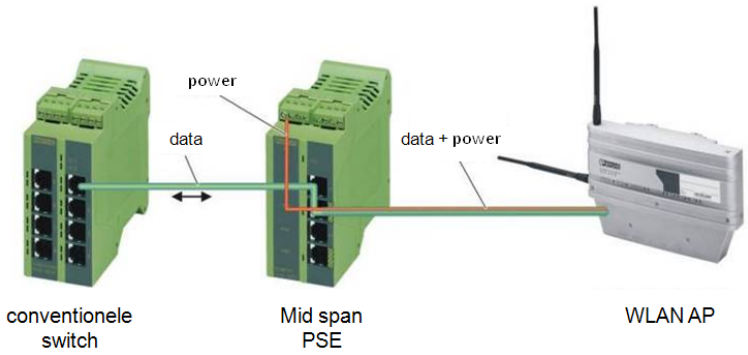


**Abbildung 2.21:** Einsatz eines Mid Span PSE

Abb. 2.21 zeigt die Integration eines Mid Span PSE. Es ist also nur ein zusätzliches Modul nötig, um PoE zu ermöglichen.

### 2.6.2 PD

Netzwerkteilnehmer, die ihre Versorgungsspannung über das Ethernet-Kabel erhalten, werden PD (Powered Device) genannt. Um Beschädigungen durch Verpolung zu verhindern, sind PDs mit einem Verpolungsschutz ausgestattet. Ein PD muss gemäß der Norm Alternative A oder B unterstützten (siehe unten).

In der Norm ist festgelegt, dass ein PSE mindestens 15,4 W leisten und ein PD höchstens 12,95 W aufnehmen darf. Die Differenz ist nötig, um Verluste im Twisted-Pair-Kabel auszugleichen. Ein 100 m langes Kabel hat einen elektrischen Widerstand, der für einen Spannungsfall entlang der leitung sorgt.
Um Geräte gegen unerwartete Spannungen zu schützen, wird beim Herstellen der Verbindung ein Identifikationsprozess durchgeführt:

- Wenn nichts mit dem PSE verbunden ist, ist der Port spannungslos.
- Ein Gerät meldet sich mit einem Widerstand von 25 k$\Omega$ an.
- Das PSE legt eine Spannung von 10,1 V an und misst den Strom. Wenn der Stromfluss kleiner als der Mindeststrom ist, wird die Spannungszufuhr unterbrochen.
- Um im Einzelnen die Klasse (0 bis 3) festzustellen, legt das PSE eine Spannung von 20,5 V an. Nach dem Bestimmen der Klasse legt das PSE eine Spannung von 48 V an. Es werden die folgenden Leistungsklassen unterschieden:

| | |
|---|---|
| Klasse 0 | 0,44 W bis 12,95 W |
| Klasse 1 | 0,44 W bis 3,84 W |
| Klasse 2 | 3,84 W bis 6,49 W |
| Klasse 3 | 6,49 W bis 12,95 W |

### 2.6.3 Alternative A

Hierbei wird die Spannung über die Datenleitungen übertragen. Die Spannung wird über Transformatoren mit Mittenanzapfung zur Verfügung gestellt und an die Pins 1-2 und 3-6

angeschlossen, sodass sie für den Datenstrom unsichtbar ist. Dieses Verfahren eignet sich für 10/100/1000Base-T.

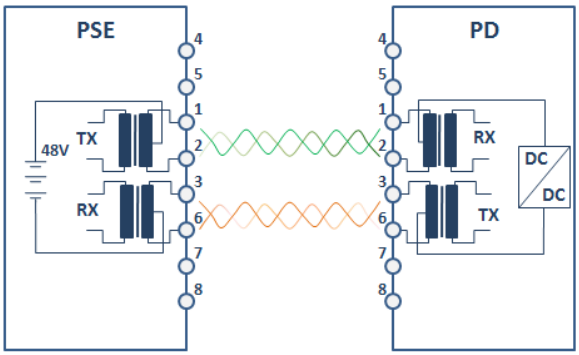


**Abbildung 2.22:** PoE, Alternative A

### 2.6.4 Alternative B

Hierbei wird die Energie über die in einem UTP-Kabel nicht für die Datenübermittlung verwendeten Adern übertragen. Die Paare 4-5 und 7-8 werden parallel verwendet, um den Spannungsfall entlang der Leitung zu minimieren. Plus liegt dabei an Pins 4 und 5, Minus an Pins 7 und 8.

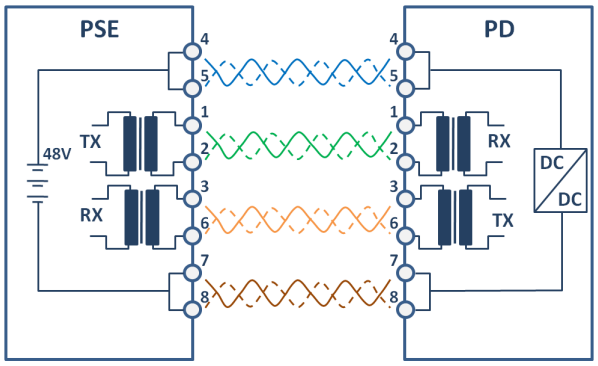


**Abbildung 2.23:** PoE, Alternative B

Dieses Verfahren kann nur Anwendung finden, wenn die Paare 1 und 4 zur Verfügung stehen (bestimmte industrielle Ethernet-Kabel enthalten nur die Paare 2 und 3) und sie nicht verwendet werden (bei 1000Base-T ist die Anwendung daher nicht möglich).

## 2.7 VLAN

Ein VLAN oder Virtual Local Area Network besteht aus einer Gruppe Teilnehmern in einem größeren Netzwerk, die auf logische Weise ein gesondertes Netzwerk bilden. Auf diese Weise können in einem größeren physikalischen Netzwerk mehrere logische Gruppen geschaffen werden. Ein VLAN bilden eine eigene Broadcast-Domäne. Datenpakete werden nur innerhalb

eines VLAN weitergeschickt. Alle Teilnehmer müssen sich physikalisch in einem gemeinsamen Netzwerk befinden, mit Hilfe von VLANs lässt sich dieses Netzwerk dann in logische Segmente unterteilen. Einige Beispiele für die Aufteilung in ein Netzwerk:

- nach Abteilungen: ein VLAN für die Verkaufsabteilung, ein anderes für das Engineering und ein weiteres für die Automation
- nach Hierarchien: ein VLAN für die Direktion, ein anderes für die Manager und ein weiteres für die Arbeitnehmer
- nach Nutzung: ein VLAN für Anwender, die E-Mail-Dienste verwenden, ein anderes für Multimedia-Anwender

### 2.7.1 Vorteile von VLANs

Der größte Vorteil von VLANs ist die Segmentierung des Netzwerks. Weitere Vorteile sind die verbesserte Sicherheit sowie die Möglichkeit der Netzlastverteilung.

- Mobilität von Geräten: Geräte können innerhalb des Netzwerks leichter umgesetzt werden. In einem traditionellen Netzwerk muss die Verkabelung angepasst werden, wenn ein Anwender von einem Subnetz in ein anderes umzieht. Der Umzug von einem VLAN in ein anderes hingegen bedarf keinerlei Veränderungen der Verkabelung: Es muss lediglich eine Einstellung am Switch vorgenommen werden. So kann eine Station der Salesabteilung an einen Netzwerkanschluss des Engineering umgesetzt werden. Dazu muss der Port als Mitglied des Engineering-VLANs konfiguriert werden, eine neue Verkabelung ist hingegen unnötig.
- zusätzliche Sicherheit: Geräte eines VLAN können ausschließlich mit anderen Geräten desselben VLANs kommunizieren. Wenn ein Gerät des Sales-VLANs mit dem Automations-VLAN kommunizieren will, so muss diese Verbindung in einem Router eingestellt werden.
- Beschränkung des Datenverkehrs im Netzwerk: Bei einem traditionellen Netzwerk können Broadcasts für eine Überlastung des Netzwerks sorgen. Geräte erhalten oft Broadcast-Nachrichten, die sie nicht benötigen. VLANs beschränken dieses Problem, da VLANs eigene Broadcast-Domänen bilden.

### 2.7.2 Trunking

Trunking (Bündelung) ist eine Methode, um Daten verschiedener VLANs zwischen zwei Switches auszutauschen. Hierfür ist pro Gerät lediglich ein Port nötig. Es gibt verschiedene Methoden zur Durchführung des Trunkings:

- ISL: InterSwitch Link, ein häufig verwendetes proprietäres Protokoll von Cisco
- IEEE802.1Q: ein von zahlreichen Switch-Herstellern unterstützter Standard

Beim Trunking wird ein kleines Stück Code (ein Tag) hinzugefügt, in dem verzeichnet ist, aus welchem VLAN das gesendete Paket stammt. Durch dieses System bleiben die Vorteile von VLAN erhalten. Die VLANs bleiben voneinander getrennt, selbst wenn sie sich über verschiedene Switches ausbreiten. Um dennoch Datenverkehr zwischen den verschiedenen VLANs zuzulassen, wird ein Router benötigt.

### 2.7.3 Typen von VLANs

VLANs lassen sich in zwei Typen einteilen: statische und dynamische VLANs.

- Statische VLANs sind Port-basiert. Der Anwender gehört je nach dem Port, an den er sein Gerät anschließt, zum einen oder anderen VLAN.

  Vorteile:

  - leicht zu konfigurieren
  - Alles geschieht im Switch, der Anwender merkt kaum etwas davon

  Nachteile:

  - Wenn ein Anwender seinen PC am falschen Port anschließt, muss vom Administrator eine Neukonfiguration durchgeführt werden.
  - Wenn an einem zu einem gegebenen VLAN gehörenden Port ein zweiter Switch angeschlossen wird, so gehören alle Computer, die an diesem Switch angeschlossen werden, automatisch zu diesem VLAN.

- Dynamische VLANs: Diese basieren nicht auf den Ports eines Switches, sondern auf der Adresse des Anwenders oder dem verwendeten Protokoll.

  Vorteil: Egal an welchem Port ein Computer angeschlossen wird, gehört er stets zum korrekten VLAN.

  Nachteil: Die Kosten dieses VLAN-Typs sind höher, da spezielle Hardware benötigt wird.

## 2.8 Netzwerkredundanz

### 2.8.1 Einleitung

Unter Netzwerkredundanz wird die Integration von Hard- und Software verstanden, die dafür sorgen, dass bei Ausfall eines Single Point of Failure Netzes erhalten bleibt. Das Kommunikationssystem, das Netzwerk, ist das Herz jedes modernen Automationsprojekts. Um Netzwerkfehler aufzufangen, können verschiedene Protokolle in die Strukturelemente integriert werden. Es werden drei wesentliche Gruppen unterschieden:

- STP/RSTP: (Rapid) Spanning Tree Protocol. Dieses kann in vermaschten Topologien verwendet werden, siehe weiter unten in diesem Kapitel.
- MRP: Media Redundancy Protocol, ausschließlich für Ringtopologien.
- PRP: Parallel Redundancy Protocol

### 2.8.2 Das Spanning Tree Protocol

Das in IEEE802.1d beschriebene Spanning Tree Protocol (STP) ist ein offenes Protokoll. Das STP ist ein Schicht-2-Protokoll, das ein geschlossenes und schleifenfreies LAN gewährleistet. Es basiert auf einem von Radia Perlman (Mitarbeiter der Digital Equipment Corporation) entwickelten Algorithmus. Mit Spanning Trees ist es möglich, Netzwerke mit redundanten Pfaden

aufzubauen. Auf diese Weise kann ein automatischer Backup-Netzpfad bereitgehalten werden, wenn ein aktiver Pfad aus irgendeinem Grunde ausfällt, ohne dass dafür geschlossene Schleifen im Netzwerk nötig sind.

Um dieses Protokoll einsetzen zu können, muss es von den verwendeten Switches unterstützt werden. Nach einer Unterbrechung eines Segments kann es bis zu 30 oder 50 Sekunden dauern, bis der alternative Pfad verfügbar ist. Für Steuerungsanwendungen kann diese diese Verzögerungszeit inakzeptabel sein, und selbst für Überwachungsaufgaben sind 30 Sekunden sehr lang. Ein Vorteil des STP ist es, dass es nicht ausschließlich für redundante Ringstrukturen eingesetzt werden kann.

### 2.8.3 Das Rapid Spanning Tree Protocol

Als Antwort auf die Unzulänglichkeiten des Spanning Tree Protocols formulierte die IEEE 2001 das Rapid Spanning Tree Protocol (RSTP). Dieses ist im IEEE802.1w beschrieben. Seit 2004 ist das STP in der IEEE802.1d als überflüssig beschrieben, und es wird empfohlen, stattdessen RSTP einzusetzen. Daher ist auch IEEE802.1w in die 802.1d-Norm aufgenommen wurden.

Die Umschaltzeit des RSTP ist kleiner als die des STP (daher auch der Name), sie beträgt nur 1 bis 10 Sekunden statt 30 bis 50. Je nach Anwendung kann diese Umschaltzeit bereits schnell genug sein.

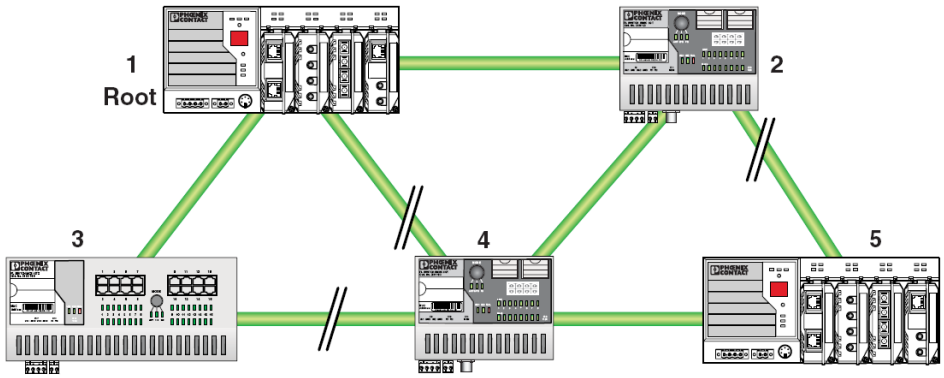


**Abbildung 2.24:** Beispiel einer (R)STP-Baumstruktur

Abb. 2.24 zeigt ein Netzwerk mit fünf verschiedenen Strukturelementen. Es werden verschiedene redundante Verbindungen geschaffen, wodurch unzulässige Schleifen entstehen, die das Netzwerk schnell in den Sättigungsbereich bringen. Das RSTP wandelt diese Topologie durch Abschalten einiger Ports in eine Baumstruktur um. Hierbei wird eines der Strukturelemente als Root konfiguriert. Von dieser Root aus sind alle Switches über einen einzigen Pfad erreichbar. Wenn ein Netzwerkfehler auftritt, wird ein neuer aktiver Pfad geschaffen.

#### Erweiterungen des RSTP

Um den Bedürfnissen der Automation nachzukommen, nutzen einige Hersteller proprietäre Erweiterungen des RSTP, um Umschaltzeiten unter einer Sekunde zu erzielen. Auf diese Weise wird die QoS für den redundanten Aufbau von Automationsnetzwerken erreicht.

**Fast Ring Detection** ist eine RSTP-Erweiterung von Phoenix Contact. Beim Ausfall eines Netzwerk-Switches werden Umschaltzeiten von 100 bis 500 ms erreicht. Umschaltzeiten von max. 500 ms lassen sich für umfangreiche Automationsnetzwerke mit 1000 Adresseinträgen in den Switches erreichen. Bei weniger Endgeräten im Netzwerk verkürzen sich die Zeiten. Dieses Protokoll ist jedoch nur bei 10 oder 100 Mbit/s verwendbar.

### 2.8.4 Bridge Protocol Data Units (BPDUs)

Anhand eines bestimmten Algorithmus wird die Baumstruktur berechnet, wobei ein Switch als Root konfiguriert wird. Jeder Switch muss dabei über alle nötigen Informationen verfügen, um die korrekten Portregeln festlegen zu können. Um zu gewährleisten, dass jeder Switch über ausreichende und korrekte Informationen verfügt, tauschen die Switches untereinander Informationen aus. Zu diesem Zweck werden spezielle Frames, die sogenannten Bridge Protocol Data Units (BPDUs) verwendet.

Eine Bridge schickt eine BPDU, wobei sie als SA die individuelle MAC-Adresse des Ports selbst und als DA die STP-Multicastadresse 01:80:C2:00:00:00 verwendet. Es gibt verschiedene Arten von BPDUs:

- Configuration BPDU (CBPDU): für die Berechnung des Spannbaums
- Topology Change Notification BPDU (TCN): zur Bekanntmachung von Veränderungen im Netzwerk
- Topology Change Notification Acknowledgement (TCA)

Um ein schleifenfreies Netzwerk zu schaffen, wird jedem Port eines Switches ein Status zugewiesen. Im Einzelnen sind dies:

- ROOT: Port, der den Pfad zum Root Switch bildet
- DESIGNATED: aktiver Port, der einen Pfad zu einem in der Hierarchie der Baumstruktur weiter unten liegenden Switch bildet
- ALTERNATE: ein Port mit einer niedrigeren Priorität, ein alternativer Pfad zur Root

### 2.8.5 Multiple Spanning Tree Protocol (MSTP)

In einer Ethernetumgebung mit Virtual Local Area Networks (VLAN) kann das Spanning Tree Protocol ebenfalls angewendet werden.

Das ursprünglich in IEEE 802.1s definierte und später in IEEE 802.1q 2003 aufgenommene MSTP definiert eine Erweiterung des RSTP in Kombination mit VLANs. Dabei werden die Vorzüge des PVST (Per-VLAN Spanning Tree), bei dem jedes VLAN seinen eigenen Spannbaum definiert, und dem ursprünglichen IEEE 802.1q, bei dem lediglich ein einziger Spannbaum über das gesamte Netzwerk aufgebaut wird, miteinander kombiniert.

Beim MSTP werden verschiedene VLANs in logische Instanzen (VLAN-Gruppen mit derselben Spanning-Tree-Topologie) aufgeteilt. Beim MSTP werden alle Spannbauminformationen in einer einzigen BPDU zusammengefasst, um so die Anzahl der BPDUs zu beschränken. Die Kompatibilität zu RSTP-Switches ist vollständig gewährleistet.

### 2.8.6 Media Redundancy Protocol

MRP ist Teil des PROFINET-Standards. Bei MRP blockiert ein Ringmanager einen Port, um so eine aktive Busstruktur zu erhalten. Bei einem Netzwerkfehler zerfällt das Netzwerk in zwei isolierte Netzwerksegmente, die durch Freigabe des blockierten Ports wieder aneinandergekoppelt werden. Die garantierten maximalen Umschaltzeiten liegen bei 200 ms.

### 2.8.7 Parallel Redundancy Protocol

Im Gegensatz zu den obengenannten Technologien sieht PRP bei einem Netzwerkfehler keine Änderung der aktiven Topologie vor. Dieses Protokoll arbeitet auf zwei parallelen Netzwerken. Jedes Daten-Frame wird über beide Netzwerke verschickt. Der Empfangsknoten verarbeitet die zuerst eingehende Nachricht und verwirft die später eingehende Kopie. PRP sorgt dabei für das Kopieren und Verwerfen der Nachrichten. Auch macht PRP das zweite Netzwerk für die höheren Schichten im Kommunikations-Stack unsichtbar.

## 2.9 Wichtige Ergänzungen

### 2.9.1 LLDP

Das Protokoll IEEE802.1ab (Link Layer Discovery Protocol, LLDP) ist ein Standard, mit dem sich Konfigurationsprobleme bei umfangreichen LAN-Strukturen lösen lassen. Das Protokoll definiert eine Standardmethode für Switches, Router, WLAN-Access-Points etc., um Informationen über sich selbst an andere Netzwerkteilnehmer zu übertragen und Informationen über benachbarte Teilnehmer zu speichern. LLDP ist mit allen 802-Medien möglich. Es arbeitet auf der Sicherungsschicht.

Ein Switch, der LLDP unterstützt, kann über andere Teilnehmer, die dieses Protokoll ebenfalls unterstützen, Topologiedetektion durchführen. Vorteile:

- verbesserte Erkennung von Netzwerkfehlern
- Hilfsmittel beim Austausch von Modulen
- bessere Netzwerkkonfiguration und besseres Netzwerkmanagement

LLDP-Informationen werden in Engineeringtools verwendet, um Netzwerktopologien grafisch darzustellen.

### 2.9.2 EEE 802.1x

IEEE802.1X ist ein Sicherheitsstandard für die Authentifizierung an jedem einzelnen Port eines Switches. Die Authentifizierung findet statt, bevor der Teilnehmer Zugang zum Netzwerk erhält. Die Erkennung eines berechtigten Teilnehmers geschieht also auf Schicht 2 des OSI-Modells, und zwar - je nach verwendeter Hardware - sowohl in drahtlosen als auch in drahtgebundenen Netzwerken.

IEEE802.1X verwendet ein Protokoll zum Austausch von Informationen mit einem Teilnehmer/Gerät, um eine Erlaubnis zum Zugriff auf das Netzwerk über einen Port anzufordern. Die

Nachrichten enthalten einen Benutzernamen und ein Passwort. Der Switch führt die Authentifizierung nicht selbst aus, sondern richtet seinerseits eine Anforderung an einen RADIUS-Authentifizierungsserver im Netzwerk. Dieser Server bearbeitet die Anforderung und teilt dem Switch mit, welchen Port er für den Teilnehmer öffnen soll.

Im Rahmen des Protokolls gibt es drei wichtige Mitspieler:

- den Anwender oder Client, dieser wird im Protokoll als SSupplicant"bezeichnet;
- die Zugangshardware (Switch oder Access Point) fungiert als Äuthenticator";
- die RADIUS-Infrastruktur ist die kontrollierende Instanz: der Äuthentication Server".

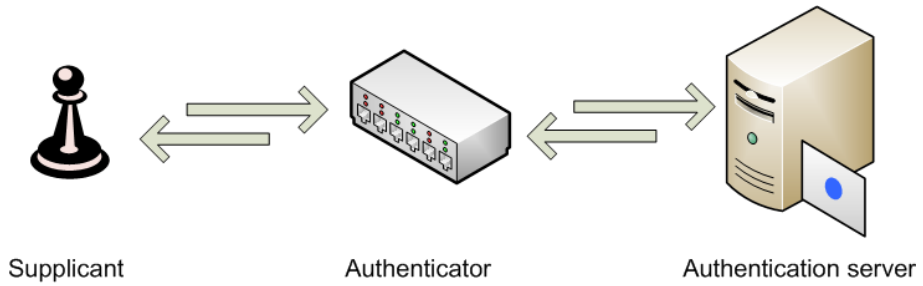


**Abbildung 2.25:** Im Rahmen des Protokolls gibt es drei wichtige Mitspieler

Die 802-1X-Authentifizierung geschieht über einen flexiblen Mechanismus: das Extensible Authentication Protocol (EAP), mit dem verschiedene Formen der Authentifizierung möglich sind. So können je nach Anwendertyp unterschiedliche Arten der Authentifizierung vorgeschrieben werden: eine starke oder eine schwache. Beispielsweise kann für Studenten die Verwendung einer Kombination aus Benutzername und Passwort vorgeschrieben werden, während Mitarbeiter ein Zertifikat verwenden. In den Kapiteln über Sicherheit wird auf diesen Punkt näher eingegangen.
Aggregation mit LACP nach IEEE 802.3ad Link Aggregation (auch Trunking oder Bündelung genannt) ist die englische Bezeichnung für ein Verfahren zur Zusammenfassung mehrerer physikalischer Netzwerkverbindungen, um eine höhere Übermittlungsgeschwindigkeit zu erzielen. Durch Link Aggregation kann auch ein redundanter Pfad zur Verfügung gestellt werden, wodurch empfindlichen Systemen eine zusätzliche Fehlertoleranz hinzugefügt wird. Die Technik wird in Switches und Netzwerkkarten (NICs) eingesetzt.

Die Link Aggregation wird gegenwärtig durch den IEEE 802.3ad-Standard beschrieben. Sie bietet die folgenden Vorteile:

- höhere Verfügbarkeit der Pfade
- Erhöhung der Kapazität eines Pfades
- höhere Leistung mit bestehender Hardware

Die gegenwärtigen LAN-Technologien sehen Datenraten von 10, 100 und 1000 Mbps vor. Durch Link Aggregation können ggf. Zwischenwerte erzielt werden. Durch das Bündeln mehrerer 1000-Mbps-Pfade können auch Hochgeschwindigkeitsverbindungen hergestellt werden.

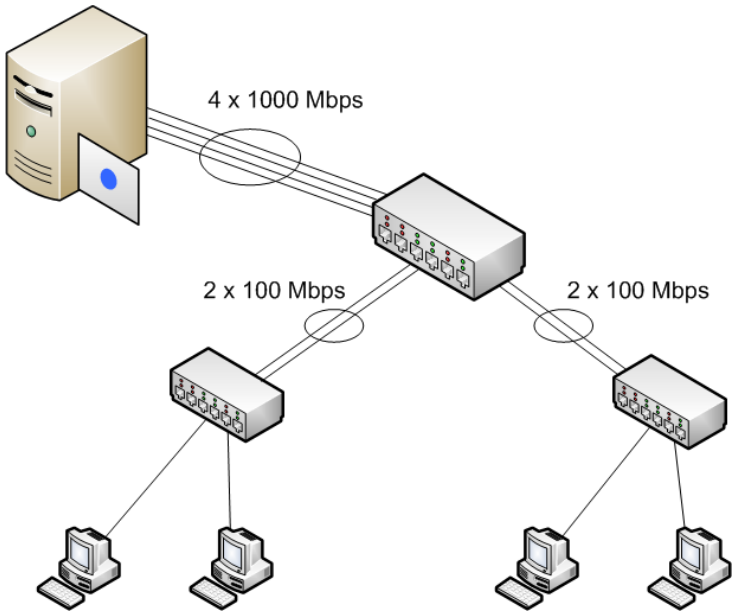


**Abbildung 2.26:** Link Aggregation

Link Aggregation ist auf verschiedene Weisen möglich:

- Verbindung zwischen zwei Switches
- Verbindung zwischen Switch und Endgerät
- Verbindung zwischen zwei Endgeräten

Abb. 2.26 zeigt, wie Switches über zwei 100-Mbps-Leitungen miteinander verbunden sind. Wenn eine dieser Verbindungen wegfällt, übernimmt die jeweils andere der Link Aggregation Group.

Die Link Aggregation wird gegenwärtig durch den IEEE 802.3ad-Standard beschrieben. Bei diesem Verfahren können eine oder mehrere Verbindungen zu einer sogenannten Link Aggregation Group gebündelt werden. Ein MAC-Client kann dann diese Gruppe nutzen, als ob es sich um eine einzelne Verbindung handeln würde (IEEE Standard 802.3, Edition 2000).

Der IEEE802.3ad-Standard beschreibt auch die Nutzung des LACP (Link Aggregation Control Protocol), um auf einfache Weise Konfigurationsinformationen zwischen den verschiedenen Systemen auszutauschen. Auf diese Weise ist eine automatische Konfiguration ebenso möglich wie eine Überwachung aller Link Aggregation Groups. Der Austausch dieser Informationen geschieht über die im Standard beschriebenen LACP-Frames.

## 2.10 Industrial Ethernet

In den vergangenen Jahren wird das Ethernet immer mehr in industrieller Umgebung angewendet. Die Unterschiede zwischen Büro- und industrieller Umgebung sind groß. Der Begriff Industrial Ethernet verweist auf den Gebrauch industrieller Produkte, um den spezifischen Anforderungen der Industrie zu genügen. In den folgenden Tabellen werden einige wichtige Gesichtspunkte aufgezählt:

**Tabelle 2.4:** Gesichtspunkte für die Ethernet-Installation

| **Büroumgebung** | **industrielle Umgebung** |
|---|---|
| Feste Basisinstallation im Gebäude | Systemspezifische Anwendungen |
| Variable Netzwerkverbindung für Workstations | Verbindungspunkte mit dem Netzwerk werden selten oder nie geändert |
| Kabel liegen in eingehängten Decken | |
| vorkonfigurierte Kabel | Stecker, die vor Ort zusammengebaut werden können |
| Standardworkstations mit RJ45 | RJ45 im Schaltschrank, extern M12 |
| | Regelmäßiger Einsatz von Glasfaserkabeln |
| | Verkabelung ist für den Einsatz in beweglichen Kabelführungen vorgesehen |
| | Sorgfältige Erdung |
| Spannungsversorgung: 230 V AC | Spannungsversorgung mit 24 V DC oder Power over Ethernet |
| Sterntopologie | regelmäßiger Einsatz von Bus- oder Ringtopologien |
| | Redundanz ist eine häufig gestellte Anforderung |
| Lebensdauer: ca. 5 Jahre | Lebensdauer: ca. 10 Jahre |
| | Terminals geeignet für Montage auf DIN-Schienen |
| Geräte mit aktiver Kühlung (Lüfter) | Passive Kühlung (keine beweglichen Teile) |
| | Meldekontakt für Fehleranzeige |

**Tabelle 2.5:** Umgebungseinflüsse

| **Büroumgebung** | **industrielle Umgebung** |
|---|---|
| Klimatisierte Umgebung | Extreme und stark schwankende Temperaturen |
| Kaum Staubbelastung | Hohe Staubbelastung |
| Kaum Feuchtigkeit oder Wasser | Feuchtigkeit oder Wasser können auftreten |
| Kaum Erschütterungen und Vibrationen | Erschütterungen und Vibrationen möglich |
| Niedriges EMV-Niveau | Hohes EMV-Niveau |
| Geringe mechanische Belastung oder Gefährdung | hohe mechanische Belastung oder Gefährdung |
| Keine Gefährdung durch Chemikalien | Chemische Belastung durch ölige oder aggressive Umgebungen |
| Keine Beeinträchtigung durch EMV-Strahlung | Hohe UV-Exposition in Außenanwendungen |

# Kapitel 3

# TCP/IP

## 3.1 Einleitung

Transmission Control Protocol / Internet Protocol (TCP/IP) ist eine Sammlung Standardprotokolle, die für die Kommunikation über große Netzwerke, die aus verschiedenen über Router miteinander verbundenen Netzwerksegmenten bestehen, entwickelt wurde.

TCP/IP ist z. B. gebräuchlich im Internet, einer Ansammlung tausender, weltweit verteilter Netzwerke, die Forschungszentren, Universitäten, Bibliotheken, Betriebe, Privatpersonen etc. miteinander verbinden.

Dagegen ist Intranet ein sehr allgemeiner Begriff. Ein Intranet ist in seiner Größe nicht beschränkt: Es gibt Intranet, die einige wenige, aber auch solche, die hunderte von Netzwerken umfassen. Mit dem Begriff Internet wird hingegen das weltweite oder auch öffentliche Internet bezeichnet.

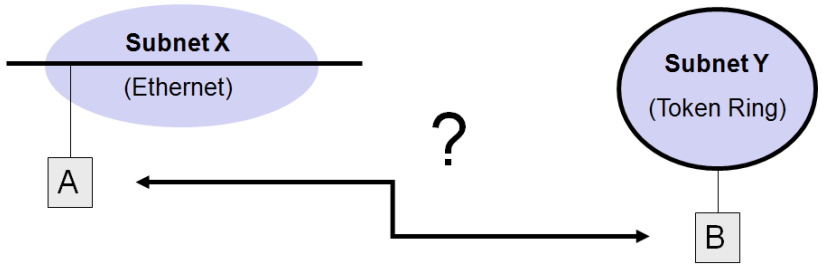


**Abbildung 3.1:** Wie kann Kommunikation über ein Intranet stattfinden?

Hier stellt sich die Frage, wie zwei verschiedene Hosts, die an verschiedenen Netzwerke mit großem Abstand voneinander angeschlossen sind, miteinander kommunizieren können. Die Antwort auf diese Frage ist zweigeteilt.

Der erste Teil der Antwort betrifft einen Hardware-Aspekt: Ein Intranet besteht aus verschiedenen Netzwerken, die über Router miteinander verbunden sind. Ein Router ist ein Strukturelement, dessen spezielle Aufgabe das Verbinden von Netzwerken miteinander ist. Jeder Router verfügt über einen Prozessor, einen Speicher und eine gesonderte Schnittstelle für jedes mit dem Router verbundene Netzwerk.

Der zweite Teil der Antwort ist ein Software-Aspekt: Auf jedem Host muss ein universeller Kommunikationsdienst aktiv sein. Obwohl es zahlreiche Software-Protokolle für Intranet gibt, ragt eine Familie unter ihnen besonders heraus. Dies ist die sogenannte TCP/IP-Familie.

Die TCP/IP-Familie kann perfekt im OSI-Modell lokalisiert werden. Zur Vorstellung der TCP/IP-Familie wird jedoch meistens ein vereinfachtes, vierschichtiges Modell verwendet: Das DoD[1]-Modell, auch ARPANET-Referenzmodell oder meistens einfach TCP/IP-Modell genannt.

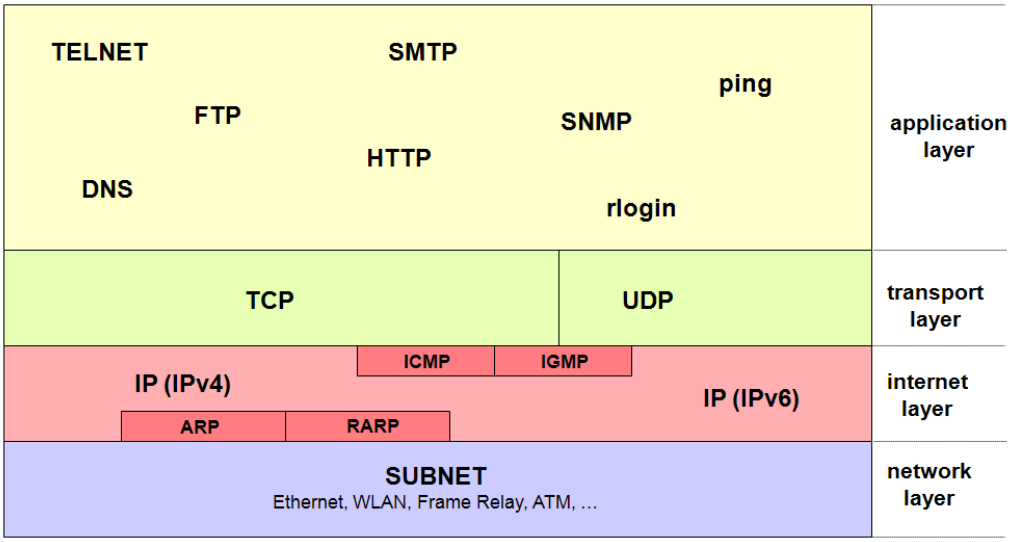


**Abbildung 3.2:** Die TCP/IP-Familie

In diesem Modell stehen die Internet-Schicht und die Transportschicht im Zentrum und werden in diesem Kapitel detailliert behandelt. Die Anwendungsschicht versammelt und beschreibt alle Protokolle, die das TCP/IP-Protokoll verwenden. Dazu gehört z. B. das HTTP-Protokoll, das zum Surfen im Internet dient. Das TCP/IP-Protokoll stellt dabei einen universellen Kommunikationsdienst zur Verfügung, mit dem der Surfauftrag über das ganze Internet ermöglicht wird. Die Netzwerkschicht sorgt dann für die Kommunikation zwischen Host und Router oder zwischen zwei Routern im lokalen Netzwerk.

## 3.2 Das Internet Protocol (IP)

### 3.2.1 Einleitung

Die wichtigsten Merkmale und Funktionen des IP-Protokolls sind:

- Das Protokoll übernimmt das Routing durch das Internet. Jeder Host wird dabei durch eine 32 Bit lange IP-Adresse identifiziert.
- Das IP-Protokoll ist ein verbindungsloses Protokoll. Jedes einzelne IP-Paket kann auf seinem Weg zum Ziel-Host einen anderen Weg nehmen, es wird keine feste physikalische Verbindung aufgebaut.

[1] Department of Defence

- Es wird ein universelles Datenpaket aufgebaut, das aus einem Header und einem Datenfeld besteht. Der Header enthält unter anderem die Absender- und die Empfängeradresse. Das Datenpaket ist hardware-unabhängig und wird im lokalen Netzwerk vor dem Transport nochmals eingekapselt.
- Das IP-Protokoll überprüft nicht, ob Daten korrekt gesendet wurden, und verfügt auch über keine Bestätigungs- oder Korrekturmechanismen: senden und hoffen.
- Der IP-Header hat eine Länge von mindestens 20 Bytes. Bei Verwendung des Options-Felds kann der Header bis zu 60 Bytes groß sein. Das Protokoll generiert eine Header-Prüfsumme.

Das Internet Protocol (IP) wird auf der Vermittlungsschicht (Schicht 3 des OSI-Modells) angewendet. Diese Schicht ist verantwortlich für das Zurverfügungstellen und Transportieren von Informationen über verschiedene Netzwerke. Zu diesem Zweck ist eine einheitliche Adressierung nötig: die IP-Adresse.

Solange die Informationsübertragung sich innerhalb desselben Netzwerks abspielt, kann diese Funktion unberücksichtigt bleiben. Die Verbindung verschiedener Netzwerke miteinander geschieht durch Router. Wenn verschiedene Netzwerke zu einem großen Ganzen verbunden werden, dann muss auch jedes Netzwerk an einer eindeutigen Adresse identifizierbar sein. Deshalb erhält jedes Netzwerk eine eindeutige Netzwerkadresse. Ausgehend von dieser Netzwerkadresse wird nun jedem Teilnehmer des Netzwerks eine eindeutige Adresse innerhalb dieses Netzwerkadressraums zugeteilt. Die einheitliche Adressierung basiert auf diesem Prinzip. Die Adresse wird auf der IP-Schicht definiert und IP-Adresse genannt.

### 3.2.2 Die IP-Adresse

#### Allgemein

Eine IP-Adresse besteht aus 32 Bits oder 4 Bytes, die durch 4 durch einen Punkt getrennte Dezimalzahlen dargestellt werden.

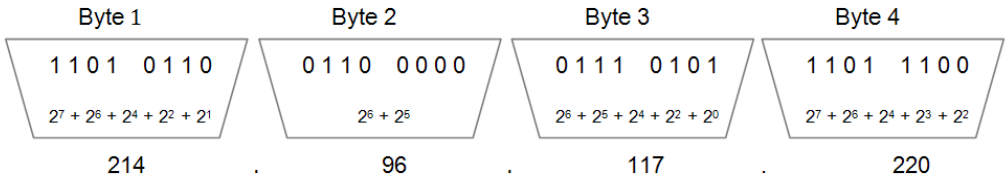


**Abbildung 3.3:** Die IP-Adresse

Jedes Netzwerk erhält einen Namen (Net-ID), und jedem Netzwerkteilnehmer wird innerhalb dieses Netzes eine eindeutige Nummer (die Host-ID) zugewiesen. Net-ID und Host-ID bilden zusammen die IP-Adresse. Der Netzwerkname ist dann die IP-Adresse, bei der die Host-ID Null ist.

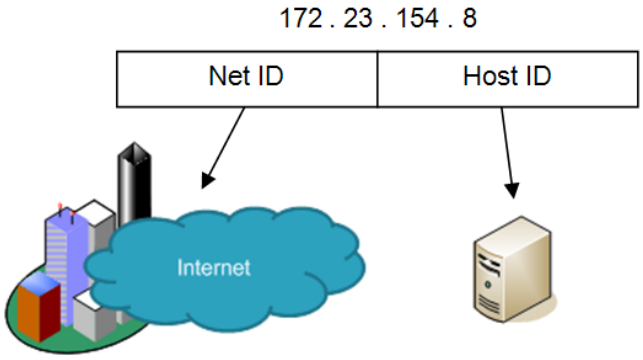


**Abbildung 3.4:** Aufbau der IP-Adresse

### Klasseneinteilung von IP-Adressen

IP-Adressen werden in verschiedene Klassen eingeteilt. Abb. 3.5 zeigt eine Übersicht.

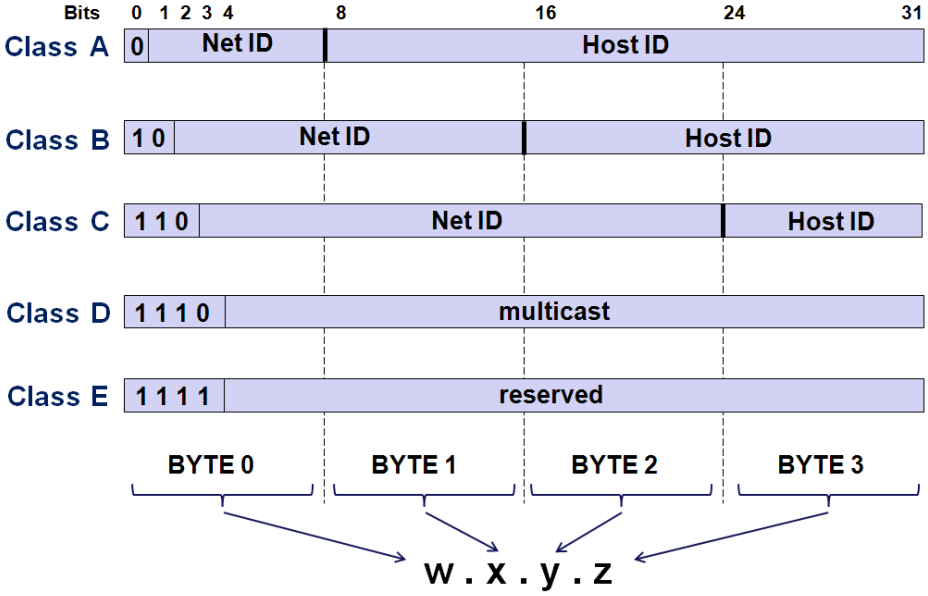


**Abbildung 3.5:** Die verschiedenen Klassen der IP-Adressierung

Tabelle 3.1 zeigt die Merkmale der Klassen A, B und C. Klasse D wurde hinzugefügt, um auf einfache Weise Multicast-Nachrichten versenden zu können. Klasse E ist zum gegenwärtigen Zeitpunkt noch ungenutzt.

Die Klassen A, B und C unterscheiden sich durch die Anzahl an Bytes, die jeweils für die Net-ID einerseits und die Host-ID andererseits verwendet werden. Die höchstwertigen Bits der IP-Adresse legen fest, zu welcher Klasse eine IP-Adresse gehört. Tabelle 3.1 fasst alle Merkmale der drei verschiedenen Klassen zusammen.

**Tabelle 3.1:** Merkmale der verschiedenen Klassen

| | | |
|---|---|---|
| **Klasse A** | Net-ID | Byte 1, erstes Bit ist 0, (0 x x x x x x x)<br>126 mögliche Netzwerkadressen |
| | Host-ID | Byte 2 + Byte 3 + Byte 4<br>16777214 mögliche Hosts pro Netzwerk |
| | Bereich | 1 . n . n . n → 126 . n . n . n |
| | Beispiel | 90.15.167.2 (Netzwerkname 90.0.0.0) |
| **Klasse B** | Net-ID | Byte 1, die ersten Bits sind 1 0, (1 0 x x x x x x) + Byte 2<br>16383 mögliche Netzwerkadressen |
| | Host-ID | Byte 3 + Byte 4<br>65534 mögliche Hosts pro Netzwerk |
| | Bereich | 128 . 0 . n . n → 191 . 255 . n . n |
| | Beispiel | 128.19.205.132 (Netzwerkname 128.19.0.0) |
| **Klasse C** | Net-ID | Byte 1, die ersten Bits sind 1 1 0, (1 0 0 x x x x x) + Byte 2 + Byte 3<br>2097152 mögliche Netzwerkadressen |
| | Host-ID | Byte 4<br>254 mögliche Hosts pro Netzwerk |
| | Bereich | 192 . 0 . 0 . n → 223 . 255 . 255 . n |
| | Beispiel | 192.147.25.112 (Netzwerkname 192.147.25.0) |

Die Vergabe der IP-Adressen wird von der IANA (Internet Assigned Number Authority) verwaltet.

### IP-Adressen für private Netzwerke

Bei der Adressvergabe werden öffentliche und private (betriebliche) Netzwerke unterschieden. Im Internet (der Summe aller öffentlichen Netzwerke) muss jede IP-Adresse eindeutig sein. Firmennetzwerke werden über Router mit dem Internet verbunden. Um Konflikte zwischen privaten und öffentlichen Netzwerken zu verhindern, ist innerhalb jeder Klasse eine Reihe IP-Adressen definiert, die im Internet nicht verwendet werden. Diese sind in unter RFC 1597 (Reserved Address Space) beschrieben. Ein Firmennetzwerk erhält vorzugsweise einen Wert aus dieser Reihe als Netzwerkadresse zugeteilt, siehe Tabelle 3.2.

**Tabelle 3.2:** IP-Adressen für private Netzwerke

| | |
|---|---|
| Klasse-A-Netzwerke | 10.0.0.0 → 10.255.255.255 |
| Klasse-B-Netzwerke | 172.16.0.0 → 172.31.255.255 |
| Klasse-C-Netzwerke | 192.168.0.0 → 192.168.255.255 |

### Spezielle IP-Adressen

Tabelle 3.3 zeigt eine Übersicht der speziellen IP-Adressen.

**Tabelle 3.3:** Einige wichtige spezielle IP-Adressen

| Net-ID | Host-ID | Beschreibung |
|---|---|---|
| nur Nullen | nur Nullen | IP-Adresse des jeweiligen Computers, wird beim Hochfahren verwendet |
| Net-ID | nur Nullen | Netzwerkadresse, identifiziert ein vollständiges Netzwerk |
| Net-ID | nur Einsen | Broadcast-Adresse im Netzwerk |
| 127 | beliebig | IP-Adresse zum Testen von Netzwerkanwendungen |

In einem Netzwerk können Broadcast-Nachrichten verschickt werden. Eine IP-Broadcast-Adresse für ein bestimmtes Segment erhält man, indem man alle Bits der Host-ID auf 1 setzt. Die IP-Adresse 131.107.255.255 ist eine Netzwerk-Broadcast-Adresse des Subnetzes mit der Netzwerkadresse 131.107.0.0.

## 3.2.3 Router und Subnetzmaske

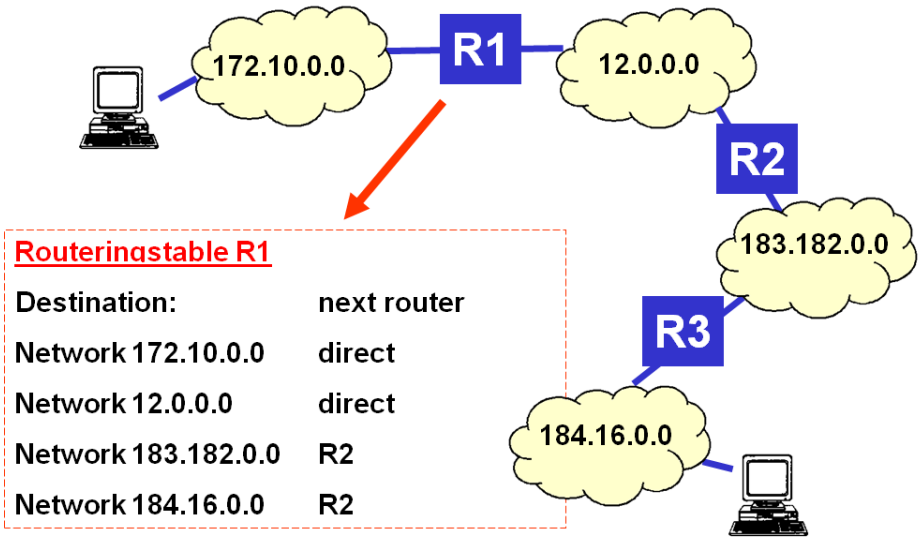


**Abbildung 3.6:** Funktion des Routers

Obwohl man vom Internet im Singular spricht, besteht es doch aus einer großen Anzahl von IP-Netzwerken. Jeder ISP (Internet Service Provider) verbindet sein Netzwerk mit mindestens einem anderen Netzwerk. Da jedes Netzwerk über eine eindeutige Identifikation verfügt, kann die Information von einer Station zur anderen gesendet werden. Dabei sorgen Router dafür, dass die Information ordnungsgemäß durch das Internet geroutet wird. Diese Router führen sogenannte Routingtabellen, in denen verzeichnet ist, wo bestimmte IP-Adressen sich befinden. Empfängt der Router ein IP-Paket, vergleicht er die Zieladresse mit seinen Routingtabellen. Wird eine Übereinstimmung gefunden, weiß der Router so, an welchen Port das betreffende Paket weitergeschickt werden muss.

Um das Routing zu vereinfachen und die bestehenden Klassen noch besser auszunutzen wurde 1985 mit RFC 950 eine Möglichkeit geschaffen, um innerhalb der Klassen A, B und C Adressgruppen zu schaffen. Um innerhalb einer Klasse mehrere Subnetze zu schaffen, wird das Präfix (Net-ID) um einige Bits erweitert, es entsteht ein Extended Network Prefix. Durch die Verwendung von Subnetzen ändert sich an der IP-Adresse per se nichts. Für die Router ist jedoch die Information wichtig, welche Bits die Net-ID bilden. Zu diesem Zweck setzt der Router eine Subnetzmaske ein. Mit dieser Maske filtert der Router den Netzwerkanteil aus der IP-Adresse.

Wie wird die Subnetzmaske zusammengesetzt?
Die den Netzwerkanteil repräsentierenden Bits erhalten den Wert 1.
Die den Hostanteil repräsentierenden Bits erhalten den Wert 0.
Danach wird in das Dezimalsystem umgewandelt.

Beispiel: Eine Adresse der Klasse C wird um vier Netzwerk-Bits erweitert. Dann ist die Subnetzmaske:

11111111 . 11111111 . 11111111 . 11110000
255 . 255 . 255 . 240

### 3.2.4 Subnetting

Unter Subnetting wird das Generieren mehrerer Subnetze aus einer gegebenen IP-Adresse verstanden.
Beispiel: Ein Betrieb arbeitet mit der Netzwerk-Adresse 172.23.0.0 (Klasse B).
Die Subnetzmaske ist 255.255.0.0 oder 1111 1111 1111 1111 0000 0000 0000 0000

Der gesamte Betrieb soll in zehn verschiedene Subnetze aufgeteilt werden. Alle diese Subnetze lassen sich über Router miteinander verbinden.

Mit 4 Bits sind 16 verschiedene Kombinationen möglich. Durch Hinzufügen von 4 Bits zur Net-ID lassen sich also die gewünschten 10 Subnetze generieren.
Subnetzmaske 1111 1111 1111 1111 **1111** 0000 0000 0000 oder 255 . 255 . 240 . 0

Auf diese Weise können die folgenden, in Tabelle 3.4 gezeigten zehn Subnetze generiert werden.

**Tabelle 3.4:** Subnetting und Subnetzmasken

| Byte 3 (binär) | Byte 3 (dezimal) | Subnetz | Subnetzmaske |
|---|---|---|---|
| 0000 0000 | 0 | 172.23.0.0 | 255.255.240.0 |
| 0001 0000 | 16 | 172.23.16.0 | 255.255.240.0 |
| 0010 0000 | 32 | 172.23.32.0 | 255.255.240.0 |
| 0011 0000 | 48 | 172.23.48.0 | 255.255.240.0 |
| 0100 0000 | 64 | 172.23.64.0 | 255.255.240.0 |
| 0101 0000 | 80 | 172.23.80.0 | 255.255.240.0 |
| 0110 0000 | 96 | 172.23.96.0 | 255.255.240.0 |
| 0111 0000 | 112 | 172.23.112.0 | 255.255.240.0 |
| 1000 0000 | 128 | 172.23.128.0 | 255.255.240.0 |
| 1001 0000 | 144 | 172.23.144.0 | 255.255.240.0 |

### 3.2.5 Classless Inter-Domain Routing

Durch den Erfolg des Internets droht ein Mangel an IP-Adressen. Die zunehmende Anzahl von Netzwerken sorgt für eine stark steigende Zahl von Routen, was zu einem Problem für die globalen Routing-Tabellen wird.

Die Lösung für dieses Problem besteht aus zwei Schritten:

- Neustrukturierung der IP-Adressen
- Steigerung der Routing-Effizienz durch eine hierarchische Routen-Struktur

CIDR (Classless Inter-Domain Routing) ist eine neue Form der Adressierung für das Internet, die die IP-Adressen im Vergleich zu den Klassen A, B und C effizienter einsetzt. Es ist eine Weiterentwicklung des Subnettings.

Die Net-ID wird hierbei nicht mehr auf 8, 16 oder 24 Bits beschränkt. Eine CIDR-Adresse umfasst die 32 Bit lange IP-Adresse und zusätzliche Informationen über die Anzahl an Bits, die die Net-ID ausmachen. So bezeichnet z. B. in der Adresse 206.13.01.48/25 das Suffix "/25", dass die ersten 25 Bits den Netzwerknamen festlegen, während die restlichen Bits den einzelnen Teilnehmer im Netzwerk identifizieren.

**Tabelle 3.5:** Classless Inter-Domain Routing

| CIDR-Code | Subnetzmaske | binär | Anzahl der Hosts |
|---|---|---|---|
| /28 | 255.255.255.240 | 11111111 11111111 11111111 11110000 | 16 |
| /27 | 255.255.255.224 | 11111111 11111111 11111111 11100000 | 32 |
| /26 | 255.255.255.192 | 11111111 11111111 11111111 11000000 | 64 |
| /25 | 255.255.255.128 | 11111111 11111111 11111111 10000000 | 128 |
| /24 | 255.255.255.0 | 11111111 11111111 11111111 00000000 | 256 |
| /23 | 255.255.254.0 | 11111111 11111111 11111110 00000000 | 512 |
| /22 | 255.255.252.0 | 11111111 11111111 11111100 00000000 | 1024 |
| /21 | 255.255.248.0 | 11111111 11111111 11111000 00000000 | 2048 |
| /20 | 255.255.240.0 | 11111111 11111111 11110000 00000000 | 4096 |
| /19 | 255.255.224.0 | 11111111 11111111 11100000 00000000 | 8192 |
| /18 | 255.255.192.0 | 11111111 11111111 11000000 00000000 | 16384 |
| /17 | 255.255.128.0 | 11111111 11111111 10000000 00000000 | 32768 |
| /16 | 255.255.0.0 | 11111111 11111111 00000000 00000000 | 65536 |
| /15 | 255.254.0.0 | 11111111 11111110 00000000 00000000 | 131072 |
| /14 | 255.252.0.0 | 11111111 11111100 00000000 00000000 | 262144 |
| /13 | 255.248.0.0 | 11111111 11111000 00000000 00000000 | 524288 |

Die CIDR-Adressierung ermöglicht auch die Routen-Zusammenfassung (Route Aggregation"). Dabei kann eine übergeordnete Route zahlreiche untergeordnete Routen in einer globalen Routing-Tabelle repräsentieren. Auf diese Weise kann eine vollständige hierarchische Struktur erstellt werden, die mit der Aufteilung der Telefonnummern in Ortsnetze verglichen werden kann.

### 3.2.6 Beispiele

- Zeigen Sie, dass die Server mit den IP-Adressen 203.125.72.28/28 bzw. 203.125.72.34/28 nicht zum selben Netzwerk gehören.
- Die IP-Adresse eines Hosts ist 192.168.100.102/27.
  - Zeigen Sie, dass dieser Host zum Netzwerk mit der Adresse 192.168.100.96/27 gehört.
  - Zeigen Sie, dass die Broadcast-Adresse dieses Netzwerks 192.168.100.127 ist.
  - Zeigen Sie, dass die IP-Adresse aller Teilnehmer dieses Netzwerks zwischen 192.168.100.97 und 192.168.100.126 liegt.
- Ein Firmennetzwerk setzt sich aus verschiedenen Subnetzen zusammen.
  Die Teilnehmer mit den folgenden IP-Adressen gehören jeweils zu verschiedenen Subnetzen: 172.23.136.45, 172.23.139.78 und 172.23.140.197.

Die Teilnehmer mit den IP-Adressen 172.23.126.120 und 172.23.127.92 gehören hingegen zum selben Subnetz.

Zeigen Sie, dass das CIDR-Suffix innerhalb des Firmennetzwerks /23 ist.

### 3.2.7 Das IP-Paket

Die zu versendenden Informationen werden von der Transportschicht an die Internetschicht weitergegeben. Die Internetschicht packt die Informationen in das Datenfeld und fügt dann den IP-Header hinzu. Dieses IP-Paket wird dann zur weiteren Bearbeitung an die Vermittlungsschicht übergeben. Das Versenden von Daten mit dem IP-Protokoll geschieht auf Basis von IP-Paketen.

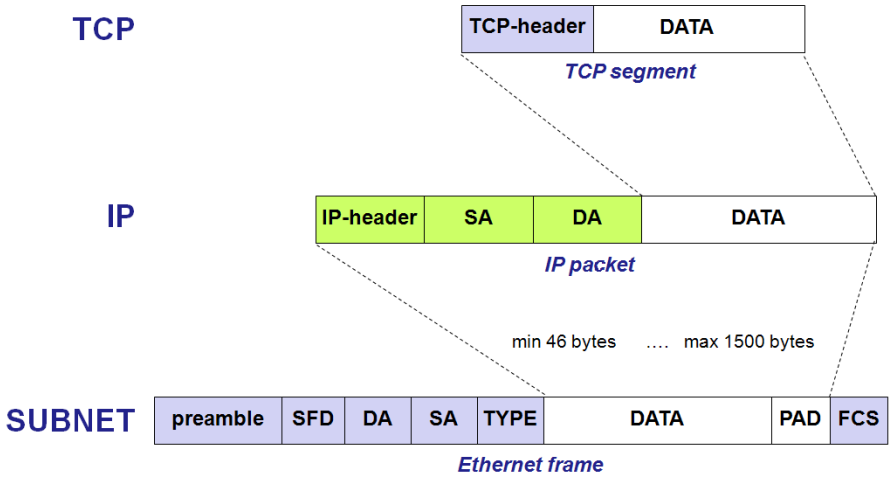


**Abbildung 3.7:** Das IP-Paket

Erhält ein Router ein IPv4-Paket, das für das Netz zu groß ist, in welches das Paket weitergeschickt werden soll, so trennt der Router das Paket in mehrere kleinere Pakete auf, die in die Daten-Frames des betreffenden Subnetzes passen. Wenn diese Pakete ihr Endziel erreichen, so setzt das IPv4-Protokoll des Ziel-Hosts diese Pakete wieder in der ursprünglichen Reihenfolge zusammen. Beim Aufteilen eines Pakets geschieht Folgendes:

- Jedes Paket erhält einen eigenen IP-Header.
- Alle Teilnachrichten, die zu derselben ursprünglichen Nachricht gehören, erhalten das originale Identifikation-Feld. Das Flag *more fragments flag* zeigt an, dass noch weitere Fragmente folgen. Beim letzten Fragment wird dieses Flag nicht gesetzt.
- Das *fragment offset field* gibt an, an welcher Stelle das betreffende Fragment in der ursprünglichen Nachricht steht.

Um eine klare Vorstellung der Funktionen des IP-Protokolls zu vermitteln, wird im Folgenden der IP-Header näher erläutert. Abb. 3.8 zeigt die verschiedenen Felder im IP-Header. Der Header besteht aus mindestens 20 Bytes.

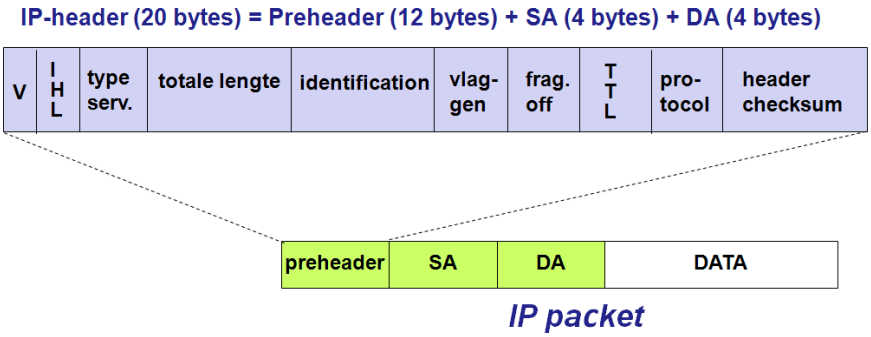


**Abbildung 3.8:** Der IP-Header

- Version (V): 4 Bit großes Feld, das die IP-Version wiedergibt.
- IHL: 4 Bit großes Feld, das die Länge des Headers in Bytes angibt.
- Type of Service: reserviert / Priorität des gewünschten Dienstes
- Gesamtlänge: Gesamtlänge des vollständigen IP-Pakets in Bytes.
- Identifikation: Wenn ein IP-Paket aufgeteilt werden muss, so erhält jedes Teilpaket eine eindeutige Identifikation, damit beim Empfänger alle Pakete korrekt wieder zusammengefügt werden können.
- Flags: Die Flags werden verwendet, um die Fragmentierung der Pakete zu überwachen.
- Fragment Offset : Wenn ein Datenpaket aufgeteilt wird, so wird die Position des Fragments innerhalb des ursprünglichen Pakets hier in einer 8-Bit-Einheit verzeichnet.
- Time to Live (TTL): Jedes Mal, wenn ein IP-Paket einen Router passiert, wird dieser Wert um 1 vermindert. Wenn der Wert Null erreicht wird, so verwirft der Router das betreffende Paket. Auf diese Weise wird verhindert, dass eine Nachricht unendlich lange bestehen bleibt.
- Protokoll: Hier wird auf das nächsthöhere Protokoll verwiesen.

  01h ICMP
  06h TCP
  11h UDP

- Header Checksum: Diese Prüfsumme für den IP-Header wird von jedem Router erneut berechnet.
- Source IP Address: IP-Adresse des sendenden Teilnehmers.
- Destination IP Address: IP-Adresse des empfangenden Teilnehmers.
- Options: Hier können weitere Netzwerkinformationen in den IP-Header aufgenommen werden. Wenn die Optionsdaten nicht mit einem 32-Bit-Wort enden, wird der Rest mit Nullen aufgefüllt.

### 3.2.8 IPv6

#### Allgemein

Das aktuellste in diesem Kapitel bisher behandelte IP-Protokoll hat die Versionsnummer 4 (IPv4). Durch den großen Erfolg des IP-Protokolls wird jedoch eine neue Version nötig. Es besteht ein deutlicher Mangel an IP-Adressen, außerdem ist es wichtig, neue Funktionen einfach integrieren zu können. Ferner muss eine neue Version des IP-Protokolls auch eine höhere Performance gewährleisten können.

Die Einführung von IPv6 bringt auch ein praktisches Problem mit sich: Wie kann das öffentlich zugängliche Internet, das bisher auf Grundlage von IPv4 arbeitet, auf IPv6 umschalten? Die einfachste Weise ist die sogenannte Dual-Stack-Herangehensweise. Dabei wird in Knoten sowohl IPv6 als auch IPv4 implementiert. Diese Knoten können daher sowohl IPv4- als auch IPv6-Datagramme verarbeiten.

Im Bereich der industriellen Automatisierung wird zur Zeit nicht an der Integration von IPv6 gearbeitet.

Im Folgenden werden kurz einige Eigenschaften von IPv6 erläutert. Es werden jedoch soweit möglich die Eigenschaften, die IPv4 so erfolgreich gemacht haben, berücksichtigt.

#### IP-Adresse

IPv6 sieht IP-Adressen mit einer Länge von 128 Bits vor. Hierdurch entstehen umfangreiche Adressierungsmöglichkeiten. Die 128 Bits langen Adressen werden in 8 durch Doppelpunkte voneinander getrennte Gruppen zu je 4 Hexadezimalziffern notiert:

2000:0000:0000:0FED:CBA9:8765:4321
2000::FED:CBA9:8765:4321
IPv4-Adressen: 192.32.20.46

Die neue Art der Adressierung soll für kleinere Routing-Tabellen sorgen.

#### IPv6-Header

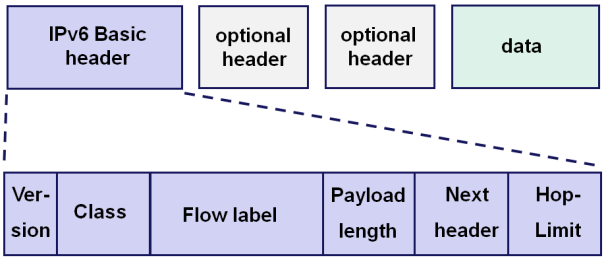


**Abbildung 3.9:** IPv6-Header

Bei IPv6 wurde der Header umfangreich geändert. Es wird nun ein einfacherer Basisheader verwendet, der die Möglichkeit zur Integration optionaler Header bietet und so für eine deutliche Reduktion der Header-Verarbeitungszeit für den Router sorgt. Einige IPv4-Felder gibt es nicht mehr oder sind nur noch als Option verfügbar. Die Felder im IPv6-Header:

- Flow Label: Eine 20 Bit lange Identifikationsnummer, um ein Paket in einem Datenstrom zu kennzeichnen.
- Hop Limit: Die Höchstzahl an Routern, die ein bestimmtes Paket durchlaufen kann.
- Next Header: Definiert den Typ des ersten optionalen Headers.
- Versionsfeld: Dieses 4-Bit-Feld gibt die IP-Versionsnummer an. Für IPv6 liegt dieser Wert bei 6.
- Payload-Länge: Diese 16 Bit lange Zahl ist eine vorzeichenloser Integer-Wert, die im IPv6-Datagramm die Anzahl der Bytes angibt, die nach dem 40 Byte langen Standard-Header folgen.

Da die Protokolle von Transportschicht (TCP und UDP) und Sicherungsschicht (z. B. Ethernet) im Internet Prüfsummen berechnen, waren die IPv6-Entwickler der Ansicht, dass in der Internet-Schicht keine Prüfsummenberechnung mehr notwendig ist.

## 3.3 Transmission Control Protocol (TCP)

### 3.3.1 Einleitung

IP ist ein verbindungsloses Paketübermittlungsprotokoll. TCP hat also eine schwierige Aufgabe: Über die unzuverlässigen IP-Paketdienste muss den verschiedenen Anwendungsprogrammen ein zuverlässiger Datenübermittlungsdienst zur Verfügung gestellt werden. Für viele Anwendungen ist die Zuverlässigkeit eines Übertragungssystems eine essentielle Eigenschaft: Das System muss gewährleisten, dass keine Daten verlorengehen, dupliziert werden oder in der falschen Reihenfolge ankommen.

### 3.3.2 Ende-zu-Ende-Transportdienst

Das TCP-Protokoll ist verantwortlich dafür, Informationen korrekt über ein oder mehrere Netzwerke zu übertragen. Der Datenaustausch unter TCP wird als *connection oriented* bezeichnet: Es wird eine logische Verbindung aufgebaut, verwendet und danach wieder beendet. TCP ist daher ein *Ende-zu-Ende-Protokoll*. Abb. 3.10 erläutert diesen Zusammenhang. TCP sieht IP als einen Mechanismus, mit dem das TCP auf einem bestimmten Host Daten mit einem TCP auf einem zweiten, entfernten Host austauschen kann.

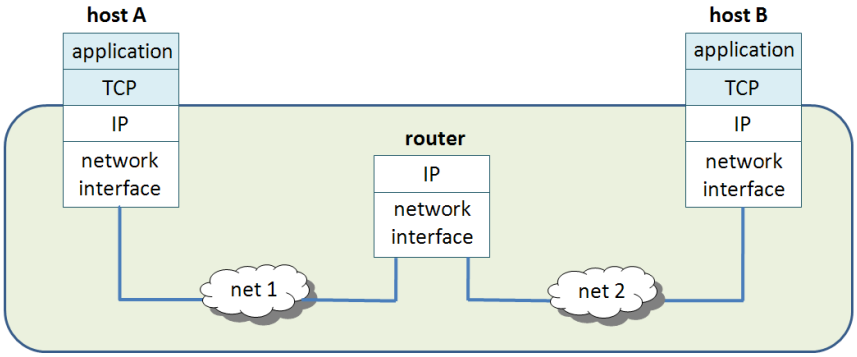


**Abbildung 3.10:** TCP als Ende-zu-Ende-Transportprotokoll

Aus der Sicht des TCP ist das gesamte Internet ein Kommunikationssystem, das Nachrichten senden und empfangen kann, ohne deren Inhalt zu verändern oder zu interpretieren.

### 3.3.3 Wie Zuverlässigkeit gewährleistet wird

TCP ist eine Bibliothek von Routinen, die von Anwendungen benutzt werden können, wenn sie eine zuverlässige Kommunikation mit einem anderen Teilnehmer oder Host aufnehmen wollen.
Um vollständige Zuverlässigkeit zu gewährleisten, setzt TCP verschiedene Techniken ein.

**Erneutes Senden von Datagrammen:** Wenn das TCP Daten empfängt, sendet es eine Bestätigung (Äcknowledgement") zurück an den Absender. Jedes Mal, wenn das TCP Daten versendet, wird ein Timer gestartet. Läuft der Timer ab, bevor die Bestätigung empfangen wird, werden die Daten erneut gesendet (siehe auch Abb. 3.11).

**Window-Mechanismus** zur Datenstromsteuerung: Wenn eine Verbindung aufgebaut ist, reserviert jeder der beiden Kommunikationspartner der Verbindung einen Puffer für die ein- und ausgehenden Daten und teilt dem jeweils anderen Ende die Größe dieses Puffers mit. Die verfügbare Puffergröße zu einem bestimmten Zeitpunkt wird *Window* genannt, das Mitteilen der Window-Größe heißt *Window Advertisement*. Der Empfänger sendet zusammen mit jeder Empfangsbestätigung ein Window Advertisement. Wenn die empfangende Anwendung die Daten so schnell lesen kann, wie sie eingehen, überträgt sie zusammen mit jeder Bestätigung ein positives Window Advertisement. Werden die Daten jedoch schneller gesendet, als die Empfängerseite sie auslesen kann, ist der Empfängerpuffer irgendwann voll. Der Empfänger meldet dann eine Window-Größe von Null (SZero Window"). Ein Sender, der ein Zero Window Advertisement empfängt, muss das Senden unterbrechen, bis der Empfänger wieder ein positives Window Advertisement sendet.

**Three-Way-Handshake**: Um zu gewährleisten, dass Verbindungen auf zuverlässige Weise aufgebaut und wieder beendet werden, verwendet das TCP ein Three-Way-Handshake, bei dem drei Nachrichten ausgetauscht werden. TCP benutzt die Bezeichnung Synchronisationssegment (SYN-Segment) für Nachrichten in einem dreifachen Handshake, die für den Verbindungsaufbau verwendet werden. Mit der Bezeichnung FIN-Segment werden Nachrichten für das Beenden einer Verbindung in einem dreifachen Handshake benannt.

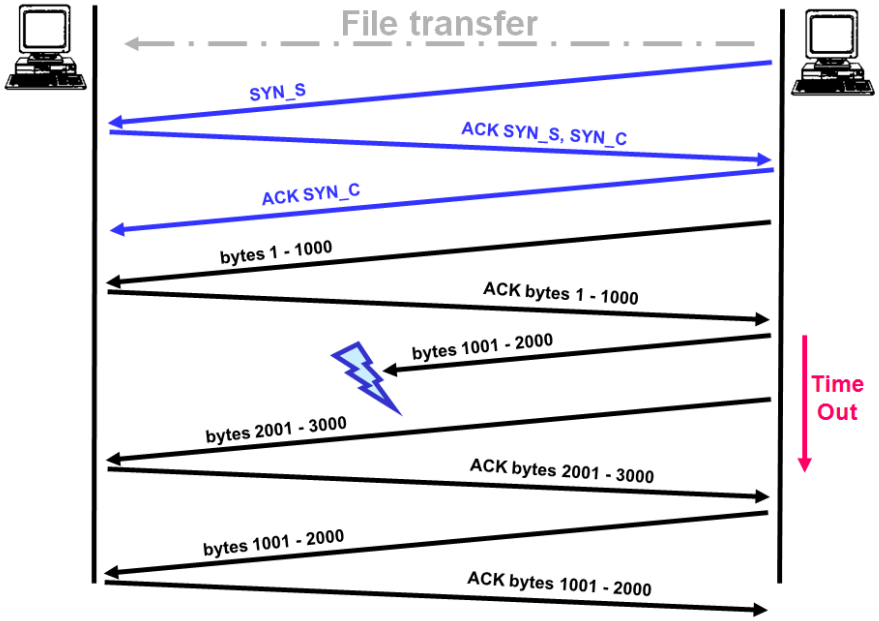


**Abbildung 3.11:** Three-Way-Handshake

### 3.3.4 Das TCP-Segment

Die zu versendenden Informationen werden von der Anwendungsschicht an die Transportschicht weitergegeben. Die Transportschicht packt die Informationen in das Datenfeld und fügt dann den TCP-Header hinzu. Dieses Paket wird dann zur weiteren Bearbeitung an die Internet-Schicht übergeben. Das Versenden von Daten mit dem TCP-Protokoll geschieht auf Basis von TCP-Segmenten.

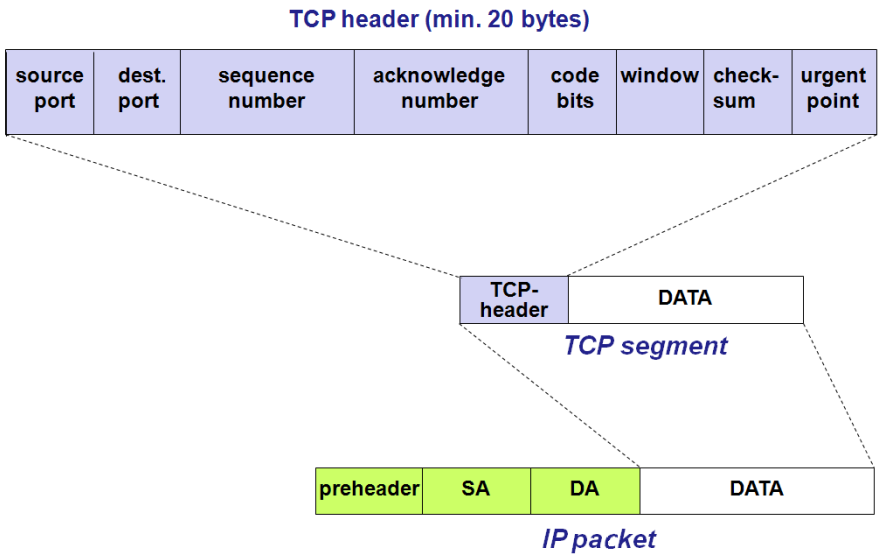


**Abbildung 3.12:** Three-Way-Handshake

Um eine klare Vorstellung der Funktionen des TCP-Protokolls zu vermitteln, wird im Folgenden der TCP-Header näher erläutert. Abb. 3.12 zeigt die verschiedenen Felder im TCP-Header. Der Header besteht aus 20 Bytes.

- Source Port und Destination Port: TCP ist über unterschiedliche Port-Nummern für die Anwendungen in übergeordneten Schichten zugänglich. *Ports* sind eindeutige 16-Bit-Adressen. Die Kombination eines Ports mit einer Internet-Adresse wird gemäß der ursprünglichen ARPA-Definition von 1971 *Socket* genannt. Die Verwendung von Port-Nummern ist wichtig für den Kommunikationsaufbau zwischen verschiedenen Anwendungen. Es wird weiter unten in diesem Kapitel noch näher darauf eingegangen. Tabelle 3.6 weiter unten vermittelt eine Übersicht über in der Automation häufig verwendete Ports.
- Sequence Number: Im TCP erhält jedes Byte eine Nummer. Die Sequenznummer (SSequence Number") ist die Nummer der ersten Daten-Bytes im TCP-Segment nach dem TCP-Header.
- Acknowledgement-Nummer: Dieses Feld enthält die nächste vom Kommunikationspartner erwartete Sequenznummer.
- Header Length: Länge des TCP-Headers in 32-Bit-Wörtern.
- Code Bits: Verschiedene Bits, mit denen einige Status mitgeteilt werden können.
  - das RST-Bit, mit dem die Kommunikation neu initialisiert werden kann;
  - das SYN-Bit, mit dem die Kommunikation neu gestartet werden kann;
  - das FIN-Bit, das anzeigt, dass die Kommunikation beendet werden kann.
- Window: Das Window-Feld gibt die maximale Menge an Daten-Bytes wieder, die vor dem Versenden und Empfangen einer Bestätigung gesendet werden kann.
- Checksum: eine Prüfsumme des TCP-Pakets;
- Urgent Pointer: Dieser Wert gibt an, wo im Datenfeld die Dringlichkeitsinformation beginnt. Um dringliche Informationen mit einem TCP-Paket zu verschicken, muss das URG-Codebit gesetzt werden.

## 3.4 UDP

Die Protokoll-Suite des Internets umfasst auch ein verbindungsloses Transportprotokoll, nämlich das UDP (User Data Protokoll). Mit dem UDP können Anwendungen IP-Pakete senden, ohne eine Verbindung aufbauen zu müssen. Zahlreiche Client-Server-Anwendungen, die eine Anfrage und eine Antwort umfassen, verwenden UDP, anstatt eine Verbindung aufbauen und später wieder beenden zu müssen. UDP wird in RFC 768 beschrieben.
UDP ist nahezu ein Null-Protokoll: Die einzigen Dienste, die es zur Verfügung stellt, sind eine Prüfsumme für die Daten und das Multiplexen von Anwendungen über Port-Nummern. Der UDP-Header ist daher auch um einiges einfacher als der des TCP.

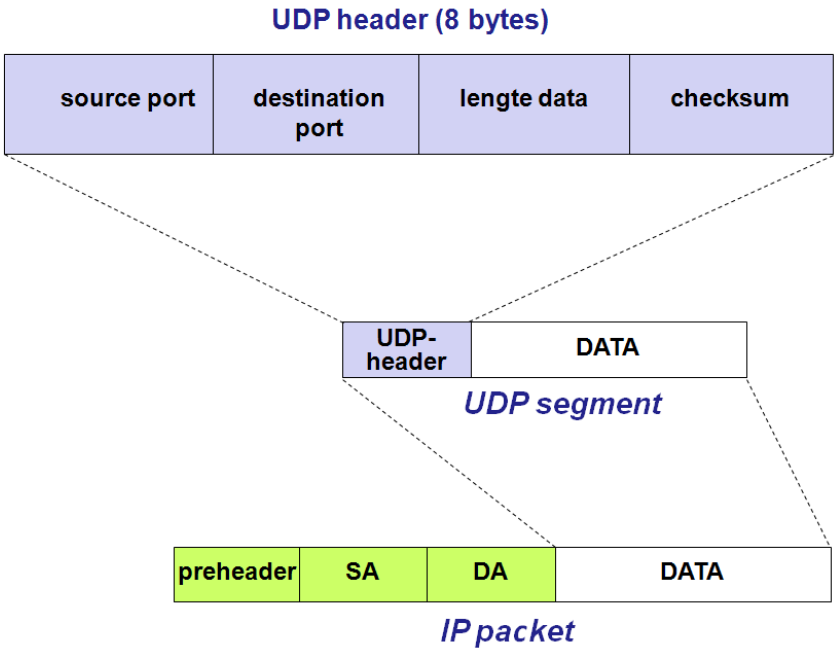


**Abbildung 3.13:** Das UDP-Segment

Ein UDP-Segment besteht aus einem Header mit einer Größe von acht Bytes, gefolgt von den Daten.
Der Header besteht aus:

- Source-Port (2 Bytes): Port-Nummer des Senders, wenn kein Port verwendet wird, ist der Wert Null.
- Destination-Port (2 Bytes): Port der Anwendung, für die die Nachricht bestimmt ist.
- Length (2 Bytes): Die Länge des UDP-Headers und der eingekapselten Daten in Bytes.
- Checksum (2 Bytes)

Ein typisches Beispiel für UDP ist Real-Time-Audio. Falls dabei Datenpakete verlorengehen, ist das bedauerlich, hat aber keinen Einfluss auf das weitere Funktionieren der Anwendung.

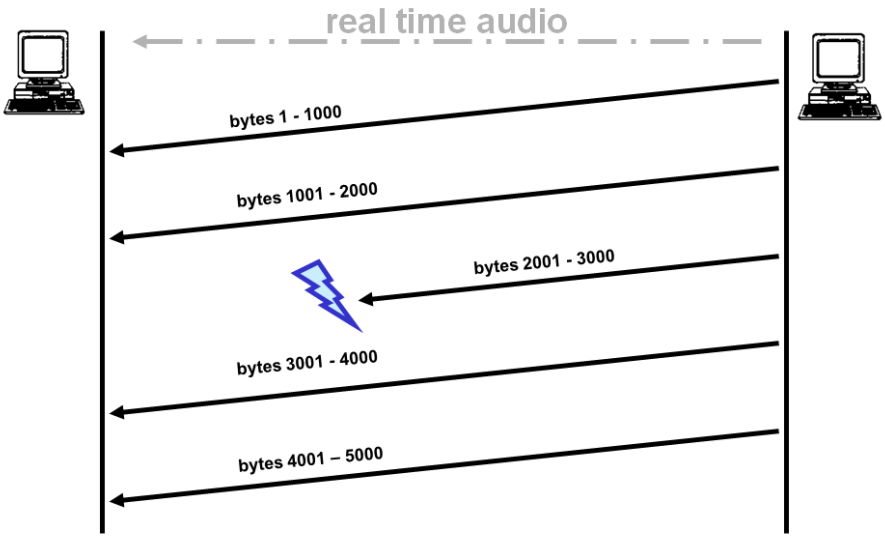


**Abbildung 3.14:** Real-Time-Audio als UDP-Anwendung

## 3.5 TCP- und UDP-Ports in der Automation

In dieser Liste geben wir eine Übersicht über einige häufig in der Automation gebrauchte Port-Nummern.

**Tabelle 3.6:** häufig verwendete TCP- und UDP-Port-Nummern

| **Anwendung** | **Port-Nummer / Protokoll** |
|---|---|
| FTP-Data (File Transfer Protocol) | 20 / TCP |
| FTP-Control (File Transfer Protocol) | 21 / TCP |
| SSH (Secure Shell) | 22 / TCP, UDP |
| Telnet-Protokol | 23 / TCP |
| BootP-Server | 67 / UDP |
| DHCP-Server | 67 / UDP |
| BootP-Client | 68 / UDP |
| DHCP-Client | 68 / UDP |
| TFTP (Trivial File Transfer Protocol) | 69 / UDP |
| HTTP (Hypertext Transfer Protocol) | 80 / TCP |
| NTP (Network Time Protocol) | 123 / UDP |
| SNMP (Simple Network Management Protocol) | 161 / TCP, UDP |
| SNMPTRAP (Simple Network Management Protocol Trap) | 162 / TCP, UDP |
| HTTPS (Hypertext Transfer Protocol Secure) | 443 / TCP |
| ISAKMP (Internet Security Association And Key Management Protocol) | 500 / UDP |
| MODBUS | 502 / TCP; UDP |
| IPsec NAT traversal | 4500 / UDP |
| EtherNet/IP | 2222 / TCP; UDP |
| PROFINET, etwa Verbindungsherstellung | 0x8892 (34962) / UDP<br>0x8893 (34963) / UDP<br>0x8894 (34964) / UDP |
| IANA, freie Ports reserviert für dynamische und/oder private Ports (Profinet-Service) | 0xC000 - 0xFFFF |
| DDI Device Driver Interface (speziell für Diagnosefunktionen verwendetes Protokoll) | 1962 / TCP |
| SOCOMM-Interface (Engineering-Kanal für Steuerungskommunikation) | 20547 / TCP |

## 3.6 Kommunikation über TCP(UDP)/IP

### 3.6.1 Client-Server-Modell

Ein Netzwerk (TCP/IP) sorgt für eine allgemeine Kommunikationsinfrastruktur, ohne dabei anzugeben, welche Dienste verwendet werden können. TCP/IP stellt einen Basiskommunikationsdienst zur Verfügung, aber die Protokoll-Software ist nicht in der Lage, den Kontakt mit einem entfernten Teilnehmer auf- oder entgegenzunehmen. Daher müssen bei jeder Kommunikation zwei Anwendungsprogramme gleichzeitig benutzt werden: das eine startet die Kommunikation, das andere akzeptiert sie.

Ein bedeutsames Problem: Die Protokoll-Software hat keine Möglichkeit, einem Anwendungsprogramm mitzuteilen, dass versucht wird, eine Kommunikation aufzunehmen. Daher basiert die Kommunikation zwischen zwei Teilnehmern auf einem Modell, bei dem die eine Anwendung aktiv ist (anfordern der Interaktion), während die andere passiv ist (horchen und ggf. akzeptieren). Ein solches Modell wird momentan im Allgemeinen bei der Kommunikation zwischen zwei Hosts über TCP/IP angewendet und heißt *Client-Server-Modell*. Eine Server-Anwendung wartet passiv auf Kontaktaufnahme, die Client-Anwendung startet die Kommunikation aktiv.

Merkmale der Client-Software:

- Client-Software ist ein Anwendungsprogramm, das vorübergehend zum Client wird, wenn der Zugang zu einem entfernten Computer benötigt wird, das aber auch lokal Berechnungen und Bearbeitungen vornimmt.
- Sie wird direkt vom Anwender gestartet und nur für eine einzige Sitzung ausgeführt.
- Sie läuft lokal auf dem PC eines Anwenders.
- Sie nimmt aktiv Kontakt zum Server auf.
- Kann ggf. Zugang zu mehreren Servern erhalten, nimmt aber zu einem gegebenen Zeitpunkt jeweils nur zu einem Server Kontakt auf.
- Benötigt keine spezielle Hardware oder ein aufwendiges Steuerungssystem.

Merkmale der Server-Software:

- Server-Software ist ein spezielles Anwendungsprogramm, das genau einen bestimmten Dienst zur Verfügung stellt, aber gleichzeitig mehrere Clients abhandeln kann.
- Sie wird beim Systemstart automatisch gestartet und bleibt über zahlreiche Sitzungen aktiv.
- Sie wartet passiv auf die Kontaktaufnahme durch beliebige Clients.
- Sie benötigt oft leistungsfähige Hardware und ein aufwendiges Steuerungssystem (je nach Art der Anwendung).

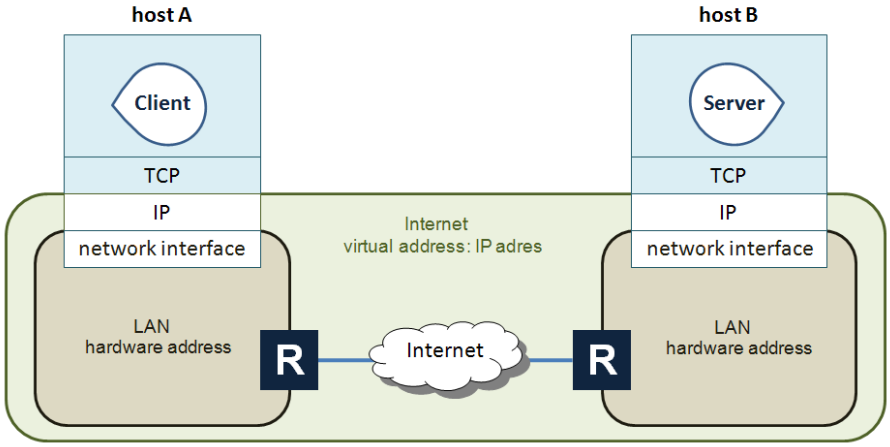


**Abbildung 3.15:** Client-Server-Modell über TCP/IP

### 3.6.2 Endpunkt und Internetsocket

Abb. 3.15 zeigt eine Client-Server-Kommunikation über den TCP/IP-Stack. Auf einem Computer-System können gleichzeitig mehrere Clients und Server aktiv sein. Hierbei ist es wichtig, dass jede Anwendung eindeutig identifizierbar ist, und dass ein Computer, auf dem mehrere Anwendungen laufen, nur eine einzige physische Verbindung zum Internet hat.

Zu diesem Zweck geben Transportprotokolle jedem Kommunikationsdienst einen eindeutigen Namen. TCP verwendet dazu ProtokollPort-Nummern. Jedem Server wird eine spezifische Protokollportnummer zugewiesen. Über diese Portnummer wartet der Server passiv auf Kommunikationsanforderungen. Beim Versenden einer Anforderung meldet der Client die Portnummer des gewünschten Diensts. Die TCP-Software auf dem Servercomputer verwendet die Destination-Port-Nummer in einer eingehenden Nachricht, um zu bestimmten, welcher Server die Anforderung bearbeiten muss.

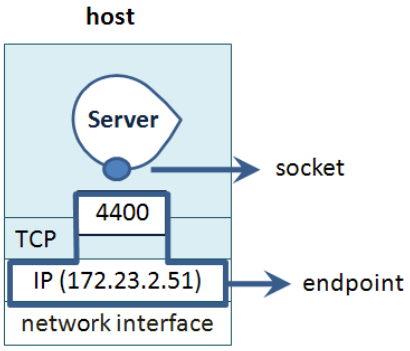


**Abbildung 3.16:** Endpunkt und Socket

**Endpunkt**

Der Begriff Endpunkt führt manchmal zur Verwechslung mit dem Begriff Socket. Laut ursprünglicher Definition gemäß ARPANET ist der Socket die Kombination einer IP-Adresse mit der Port-Nnummer. Diese Kombination wird heute Endpunkt genannt. Ein Endpunkt beschreibt, über welchen logischen Weg eine Anwendung in einem Netzwerk erreichbar ist.

**Internetsocket**

Der Begriff Socket ist heutzutage ein reiner Software-Begriff. Ein Socket sorgt für das Mapping, das Verknüpfen einer Anwendung mit einem Endpunkt. So entsteht der Begriff Internetsocket, auch Netzwerk-Socket genannt. Ein Internet-Socket oder auch kurz Socket ist ein bidirektionaler Kommunikationsendpunkt für eine Prozess-zu-Prozess-Verbindung und wird bestimmt durch:

- das Protokoll
  - UDP: Datagrammsockets oder verbindungslose Sockets
  - TCP: Streamsockets oder verbindungsorientierte Sockets
  - Basis-IP-Paket (z. B. ICMP): Rawsockets
- lokale IP-Adresse
- lokale Protokoll-Port-Nummer
- Remote-IP-Adresse
- Remote-Protokoll-Port-Nummer

### 3.6.3 Dynamische Server

Können auf einem Computer-System mehrere Anwendungsprogramme gleichzeitig arbeiten, sagt man, es unterstützt *Multitask*. Ein Programm mit mehr als einem Steuer-Thread (oder kurz Thread), Prozess oder Task wird ein *konkurrierendes* Programm genannt.

# Kapitel 4

# Erweiterungsprotokolle und Netzwerkanwendungen

## 4.1 ARP

### 4.1.1 Einleitung

Die IP-Adresse ist eine virtuelle Adresse, die durch eine Software verarbeitet wird. LAN- oder WAN-Hardware ist nicht in der Lage, eine Verbindung zwischen der Net-ID einer IP-Adresse und einem Netzwerk oder zwischen der Host-ID einer IP-Adresse und einem Host zu erkennen. Um ein IP-Paket zu transportieren, müssen die Daten in einen Frame eingekapselt werden, der von der lokalen Hardware beim Empfänger abgeliefert werden kann. Dieser Frame muss daher auch die Hardware-Adresse von Sender und Empfänger enthalten.

### 4.1.2 Address Resolution Protocol (ARP)

Wenn das IP-Protokoll eine Nachricht über das Ethernet senden möchte, so muss neben der IP-Adresse des Empfängers auch dessen MAC-Adresse bekannt sein. Zu diesem Zweck enthält die TCP/IP-Protokoll-Suite ein Address Resolution Protocol (ARP). Das ARP definiert zwei Basiskomponenten: eine Anfrage und eine Antwort. Eine Anfragenachricht enthält eine IP-Adresse und fragt die korrespondierende Hardware-Adresse (die MAC-Adresse) ab. Die Antwort enthält die entsprechende Hardware-Adresse und die IP-Adresse, für die die Anfrage gestellt wurde.

Um nicht für jedes zu sendende Paket zuerst eine ARP-Anfrage stellen zu müssen, speichert das ARP-Protokoll alle bereits bekannten Informationen zeitweise in einer Tabelle.

```
H:\PIH\personeel\henk.capoen>arp -a

Interface: 192.168.1.2 --- 0x3
  Internet-adres        Fysiek adres          Type
  192.168.1.1           00-12-bf-fa-0b-4e     dynamisch
  192.168.1.4           00-0c-41-62-8b-14     dynamisch

H:\PIH\personeel\henk.capoen>
```

**Abbildung 4.1:** Der ARP-Cache

ARP führt diese Tabelle wie einen Cache: eine kleine Tabelle mit einigen zusammen gehörigen Informationen, die jeweils wieder überschrieben oder nach einem gewissen Zeitraum (einige Minuten) wieder gelöscht werden. Abb. 4.1 zeigt, wie mit dem DOS-Befehl `arp -a` eine aktuelle Übersicht des ARP-Cache angezeigt werden kann.

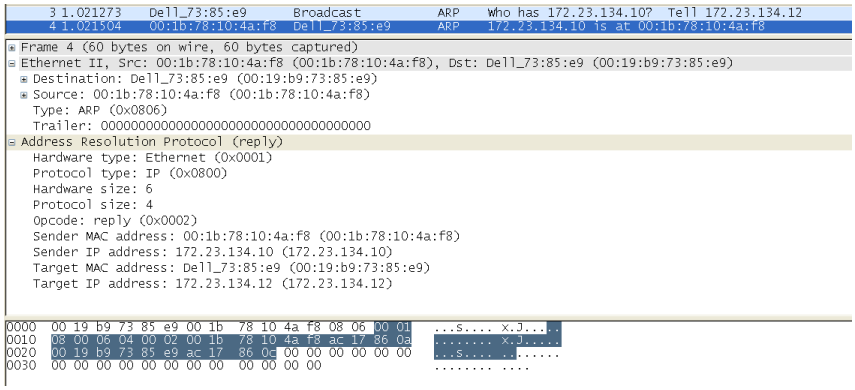


**Abbildung 4.2:** ARP-Ausgabe in Wireshark

Abb. 4.2 zeigt den Einsatz von ARP in Wireshark. Wireshark ist ein Packet Sniffer und Protokoll-Analysierer, ein Programm zum Auffangen und Analysieren von Daten in einem Computer-Netzwerk.
Das RARP-Protokoll funktioniert genau andersherum: Es sendet einen Request, eine Anfrage mit einer Hardware-Adresse. Daraufhin wird ein Reply, eine Antwort mit der gesuchten IP-Adresse gesendet.

## 4.2 BootP und DHCP

### 4.2.1 Einleitung

Beim Starten eines Hosts müssen einige Konfigurationen vorgenommen werden, bevor der Host aktiv am Netzwerkverkehr teilnehmen kann. Jeder Host muss eine IP-Adresse, die angewendete Subnetzmaske, die IP-Adresse des Standardgateways (dies ist der Router, der das lokale Netzwerk mit anderen Netzwerken, dem Internet etc. verbindet) und ggf. Daten über den DNS-Server (siehe weiter unten in diesem Kapitel) erhalten. Diese Daten können statisch in einem Host festgelegt oder ihm dynamisch zugewiesen werden. In diesem Abschnitt geht es darum, wie bestimmte Einstellungen beim Starten automatisch vorgenommen werden können. Dieser Startvorgang ist auch unter dem Namen Bootstrapping bekannt.

### 4.2.2 BootP

Das Bootstrap-Protokoll wurde der TCP/IP-Suite hinzugefügt, um einige dynamische Konfigurationsschritte in einem einzigen Schritt zu vereinen. Das BootP-Protokoll sendet einen Request-Broadcast aus, um Konfigurationsinformationen zu erhalten. Ein BootP-Server erkennt diese Nachricht und antwortet mit einem BootP-Reply, der alle nötigen Informationen enthält. BootP verwendet ein IP-Pakete, obwohl die Teilnehmer noch nicht über IP-Adressen verfügen. Als Zieladresse wird eine Broadcast-Adresse verwendet, die ausschließlich aus Einsen besteht, die Quelladresse besteht nur aus Nullen. Der BootP-Server kann die Hardware-Adresse verwenden, um seine Antwort zu senden.

Durch BootP wird die Konfiguration vereinfacht, doch bleibt das Problem bestehen, dass ein BootP-Server seine Informationen aus einer Datenbank erhält, die nach wie vor von einem Administrator von Hand geführt werden muss.

### 4.2.3 DHCP

Für die weitere automatische Konfiguration hat die IEFT das Dynamic Host Configuration Protocol (DHCP) entwickelt. DHCP ist ein Protokoll, mit dem ein Host einem neuen Netzwerk ohne manuelle Eingriffe durch einen Administrator beitreten kann. Abb. 4.3 zeigt die verschiedenen Schritte bei der automatischen Konfiguration eines Hosts. DHCP ist ein Client-Server-Protokoll. Der Client ist ein neuer Host, der IP-Informationen anfragt. Pro Netzwerk können einer oder mehrere DHCP-Server bestehen, die diese Daten zuweisen können.

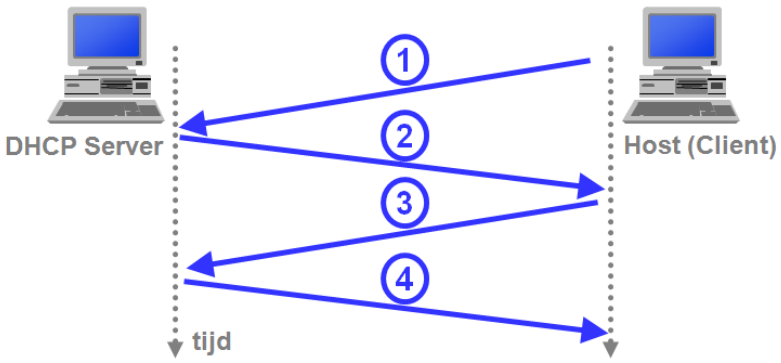


**Abbildung 4.3:** DHCP

Für einen neuen Host besteht das DHCP-Protokoll aus vier Schritten:

- DHCP-Discover: Ein Client sendet eine in ein IP-Paket gekapselte UDP-Nachricht über Port 67, um nach einem DHCP-Server zu suchen. Dazu wird eine Broadcast-Zieladresse (255.255.255.255) und die Quelladresse (0.0.0.0) verwendet.
- DHCP-Offer: die Antwort eines DHCP-Servers an den Client. Diese Antwort enthält eine IP-Adresse, eine Subnetzmaske und eine Lease-Zeit für die IP-Adresse.
- DHCP-Request: Der Host wählt aus den verschiedenen Adressangeboten und antwortet dem gewählten Server mit einem Request, der die Konfigurationsparameter enthält.
- DHCP ACK: Der Server antwortet mit einer Bestätigung.

### 4.2.4 DHCP Relay Agent - DHCP-Option 82

Der DHCP Relay Agent ist ein Bootstrap-Protokoll, welches DHCP-Pakete zwischen DHCP-Clients und -Servern an verschiedene IP-Netzwerke weiterleiten kann. Mit anderen Worten: Ein DHCP-Server kann über DHCP Relay Agent auch ein Netzwerk bedienen, mit dem er nicht direkt verbunden ist.

Ein DHCP Relay Agent horcht über den bekannten Bootpc des Clientports (67) nach Broadcastpaketen von DHCP-Clients im Netzwerk. Diese Pakete werden in Unicastpakete umgewandelt und an den konfigurierten DHCP-Server weitergeleitet. Dabei trägt der DHCP Relay Agent seine eigene IP-Adresse in das giaddr-Feld dieser Pakete ein. Der DHCP-Server kann die Antwort somit als Unicastpaket an den Relay Agent schicken. Der Relay Agent leitet die Antwort dann entweder als Broadcast- oder Unicastpaket im Netzwerk an den Client weiter.

Die DHCP-Option 82 ist eine Informationsoption des DHCP Relay Agents. Sie wurde entwickelt, damit ein DHCP Relay Agent einem Paket, das er an einen DHCP-Server weiterleitet, netzwerkspezifische Informationen hinzufügen kann. Die Option verwendet dabei zwei zusätzliche Informationen: Circuit ID und Remote ID. Über diese Informationen erhält der DHCP-Server Angaben über das Netz, in dem der sendende Host sich befindet. Die Informationen hängen sehr stark vom DHCP Relay Agent ab und bestehen bei ethernetbasierten Netzwerken aus den MAC-Adressen der Ports des Relay Agents, die den Pfad zum Endhost formen. Mit diesen Informationen kann angegeben werden, wo eine zugewiesen IP-Adresse sich physisch im Netzwerk befindet. Der DHCP-Server kann außerdem diese Angaben beim Treffen von Entscheidungen über das Zuweisen einer bestimmten IP-Adresse nutzen.

## 4.3 ICMP

### 4.3.1 Einleitung

Beim IP-Kommunikationsdienst können Datenpakete verlorengehen, ihre Zustellung kann stark verzögert werden, oder sie können in der falschen Reihenfolge abgeliefert werden. IP ist kein zuverlässiger Kommunikationsdienst, versucht aber, Fehler zu vermeiden und ggf. das Auftreten von Problemen zu melden. Ein typisches Beispiel für die Fehlererkennung ist die Header-Prüfsumme. Immer, wenn ein Datenpaket empfangen wird, wird die Prüfsumme kontrolliert, um zu gewährleisten, dass der Header unbeschädigt ist. Wenn ein Prüfsummenfehler festgestellt wird, wird die Nachricht sofort gelöscht. Dies kann nicht gemeldet werden, da zusammen mit der Nachricht auch die Quelladresse gelöscht wird. Andere, weniger wichtige Probleme können jedoch gemeldet werden.

### 4.3.2 Internet Control Message Protocol

Die TCP/IP-Protokoll-Suite enthält ein Protokoll zum Versand von Fehlermeldungen: das Internet Control Message Protocol (ICMP). Damit kann gemeldet werden, wenn eine bestimmte Netzwerkeinrichtung nicht verfügbar ist, oder dass ein bestimmter Host oder Router nicht erreichbar ist. Der Computer-Anwender kommt manchmal auch direkt in Kontakt mit dem ICMP, besonders beim Einsatz der Netzwerkdiagnosebefehle `ping` und `traceroute`.

ICMP kennt fünf Fehlermeldungen und vier informative Nachrichten. Die fünf Fehlermeldungen des ICMP sind:

- Source Quench (Quelle stoppen): wird von einem Router gesendet, wenn dieser vorübergehend nicht genug freien Puffer hat und deshalb eingehende IP-Pakete verwerfen muss. Diese Nachricht wird an den Host geschickt, der das IP-Paket erstellt hat. Der sendende Host muss seine Übertragungsgeschwindigkeit anpassen.
- Time Exceeded: wird von einem Router gesendet, wenn das *Time to Live*-Feld den Wert Null erreicht hat.

- Destination Unreachable: wird von einem Router gesendet, wenn er feststellt, dass ein IP-Paket sein Ziel nicht erreichen kann. Die Fehlermeldung unterscheidet dabei zwischen einer Situation, in der ein ganzes Netzwerk vorübergehend nicht mit dem Internet verbunden ist (weil ein bestimmter Router nicht ordnungsgemäß funktioniert), und dem Fall, dass ein bestimmter Host zeitweise offline ist.
- Redirect: wird von einem Router gesendet, wenn er feststellt, dass das IP-Paket eigentlich an einen anderen Router hätte geschickt werden müssen, um sein Ziel erreichen zu können.
- Fragmentation Required: wird von einem Router gesendet, wenn er feststellt, dass ein IP-Paket größer als die MTU (Maximum Transmission Unit) des Netzwerks ist, über welches das IP-Paket geschickt werden muss.

Im ICMP sind auch vier informative Nachrichten definiert:

- Echo Request/Reply: Ein Echo Request kann an jeden beliebigen Host gesendet werden. Als Antwort wird ein Echo Reply gesendet, dieses enthält dieselben Daten wie die Anfrage.
- Address Mask Request/Reply: ein Host sendet beim Start eine Adressmaskenanfrage. Ein Router antwortet mit einer Nachricht, die die korrekte im betreffenden Netzwerk verwendete Subnetzmaske enthält.

### 4.3.3 ICMP-Nachricht

Das ICMP-Protokoll dient zur Unterstützung des IP-Protokolls. Es verwendet daher ebenfalls IP-Pakete zum Versand von Nachrichten. Abb. 4.4 zeigt, wie eine ICMP-Nachricht in einem Daten-Frame eingekapselt ist.
Eine ICMP-Fehlermeldung wird stets als Antwort auf ein bestimmtes IP-Paket verarbeitet und an dessen Quelle zurückgesendet.

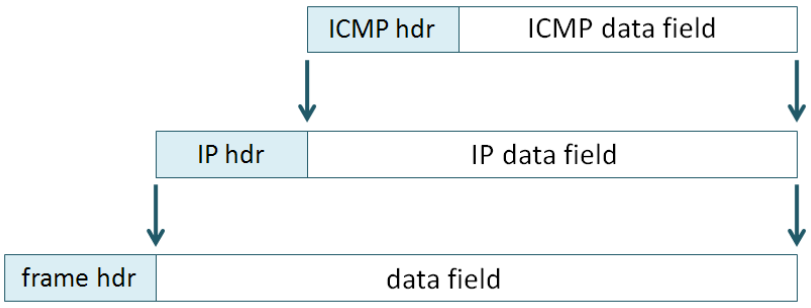


**Abbildung 4.4:** Einkapselung einer ICMP-Nachricht

Die verschiedenen Felder im ICMP-Header sind:

- TYPE:
- Code:
- Checksum:

- Identifier:
- Sequence Number:

### 4.3.4 Überprüfen der Erreichbarkeit eines Hosts

Viele Tools sammeln Informationen über ein Netzwerk, indem sie Testnachrichten senden und auf die ICMP-Antworten warten. Eines der wichtigsten Diagnosewerkzeuge ist der Ping-Befehl. Dieser sendet, nach Aufruf auf DOS-Ebene, über ICMP IP-Pakete an einen anderen Teilnehmer, um zu überprüfen, ob dieser Host über das Netzwerk erreichbar ist. Der angepingte Host sendet die Pakete sofort als Echo zurück. Ferner gibt der Befehl die Reaktionsgeschwindigkeit und eine statische Zusammenfassung des prozentualen Anteils an Paketen, auf die nicht reagiert wurde, aus. Es können sowohl die IP-Adresse als auch der Hostname verwendet werden.

ping www.google.be
ping 134.16.85.9

Eine Übersicht über die zahlreichen Optionen wird nach Eingabe des Befehls `ping` ohne Argumente angezeigt.

```
H:\PIH\personeel\henk.capoen>ping 192.168.1.1

Pingen naar 192.168.1.1 met 32 byte gegevens:

Antwoord van 192.168.1.1: bytes=32 tijd=3 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=4 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=3 ms TTL=64
Antwoord van 192.168.1.1: bytes=32 tijd=4 ms TTL=64

Ping-statistieken voor 192.168.1.1:
    Pakketten: verzonden = 4, ontvangen = 4, verloren = 0
    (0% verlies).De gemiddelde tijd voor het uitvoeren van één bewerking in mill
iseconden:
    Minimum = 3ms, Maximum = 4ms, Gemiddelde = 3ms
```

**Abbildung 4.5:** Ping-Befehl

### 4.3.5 Verfolgen von Routen

Während der Befehl Ping lediglich überprüft, ob ein bestimmter Host erreichbar ist, macht der Befehl `tracert` die Route zu einem bestimmten Host sichtbar. Abb. 4.6 zeigt, wie der Befehl `tracert` alle IP-Adressen der Router, die das Testpaket empfangen und weitersenden, ausgibt.

```
H:\PIH\personeel\henk.capoen>tracert www.google.be

Bezig met het traceren van de route naar www.l.google.com [74.125.79.104]
via maximaal 30 hops:

  1     1 ms     1 ms     1 ms  . [192.168.1.1]
  2     9 ms     7 ms     8 ms  86-39-8-1.customer.fulladsl.be [86.39.8.1]
  3     9 ms     9 ms     9 ms  83.217.77.30
  4     9 ms     9 ms     9 ms  ge-5-2-11.bb1.bru1.be.gbxs.net [193.27.64.161]
  5    17 ms    14 ms    14 ms  pos-6-0.bb1.bru2.be.gbxs.net [193.27.64.34]
  6    16 ms    13 ms    15 ms  so-7-0-0-0.bb1.ams3.nl.gbxs.net [83.143.243.18]

  7    16 ms    15 ms    14 ms  xe-3-1-0-26.bb1.ams1.nl.gbxs.net [193.27.64.178]

  8    17 ms    15 ms    15 ms  core2.ams.net.google.com [195.69.145.100]
  9    16 ms    15 ms    40 ms  209.85.254.90
 10    20 ms    18 ms    18 ms  209.85.248.79
 11    23 ms    19 ms    19 ms  209.85.255.20
 12    21 ms    23 ms    26 ms  209.85.255.122
 13    21 ms    19 ms    20 ms  ey-in-f104.google.com [74.125.79.104]

De trace is voltooid.
```

**Abbildung 4.6:** Tracert-Befehl

Tracert sendet zunächst ein Testpaket mit einem Time-to-Live-Wert von 1. Der erste Router verringert diesen Wert auf 0, verwirft die Nachricht und sendet die ICMP-Fehlermeldung Time Exceededßurück. Auf diese Weise kann die IP-Adresse des ersten Routers ermittelt werden. Nun wird ein Testpaket mit einem Time-to-Live-Wert von 2 gesendet. Der erste Router verringert diesen Wert um 1 und sendet die Nachricht weiter. Der zweite Router setzt den TTL-Wert nun auf 0, verwirft wiederum die Nachricht und sendet die ICMP-Fehlermeldung. Auf diese Weise kann die IP-Adresse des zweiten Routers ermittelt werden. Dieses Verfahren wird nun solange fortgesetzt, bis der letzte Host erreicht wird.

## 4.4 IGMP

### 4.4.1 Einleitung

Das IGMP (Internet Group Management Protocol) ist das Protokoll für IP-Multicast-Anwendungen in TCP/IP-Netzwerken. Dieser Standard wird in RFC 1112 definiert. Neben einer Definition von Adress- und Host-Erweiterungen für die Unterstützung von Multicasting durch IP-Hosts enthält dieser RFC auch eine Definition der Version 1 von IGMP. Die Version 2 des IGMP ist in RFC 2236 definiert. Beide IGMP-Versionen stellen ein Protokoll zur Verfügung, mit dem Informationen über die Zugehörigkeit eines Hosts zu spezifischen Multicast-Gruppen ausgetauscht und bearbeitet werden können.

Multicast-Nachrichten werden an eine einzige Adresse gesendet (die Multicast-IP-Adresse), aber von mehreren Hosts verarbeitet. Die Gruppe von Teilnehmern, die auf eine bestimmte Multicast-IP-Adresse reagieren, wird eine Multicast-Gruppe genannt. Einige wichtige Merkmale des Multicasting:

- Die Zugehörigkeit zu einer Gruppe ist dynamisch: Hosts können jederzeit eine Gruppe verlassen oder einer Gruppe beitreten.
- Hosts können sich durch das Senden von IGMP-Nachrichten Multicast-Gruppen anschließen.

- Die Gruppengröße ist nicht beschränkt. Die verschiedenen Teilnehmer können über mehrere Netzwerke verteilt sein, sofern die dazwischenliegenden Router IGMP unterstützen.
- Hosts können auch dann IP-Nachrichten an eine bestimmte Gruppe senden, wenn sie selbst nicht Teil dieser Gruppe sind.

### 4.4.2 IGMP-Nachrichten

IGMP beschreibt, wie die Informationen über den Zugehörigkeitsstatus zwischen Routern und den verschiedenen Teilnehmern von Multicast-Gruppen ausgetauscht werden. Beispiele für IGMP-Nachrichten:

- Host-Mitgliedschaftsbericht: Wenn ein Host Mitglied einer Multicast-Gruppe wird, versendet er einen Host-Mitgliedschaftsbericht und informiert damit alle anderen Mitglieder der Gruppe. Ein Router speichert diese Berichte und gewährleistet so die Verwaltung der Multicast-Gruppe.
- Host-Mitgliedschaftsabfrage: wird von Routern versendet, um periodisch Informationen über Gruppenmitglieder in einem Netzwerk zu sammeln. Alle Mitglieder einer Gruppe antworten erneut mit einem Mitgliedschaftsbericht. Router speichern alle Informationen und sorgen dafür, dass Multicast-Nachrichten nicht in Netzwerke gesendet werden, in denen sich keine Gruppenmitglieder befinden.
- Gruppe verlassen: wird vom letzten Host, der eine Gruppe in einem bestimmten Netzwerksegment verlässt, gesendet.

Das IGMP-Protokoll dient zur Unterstützung des IP-Protokolls. Es verwendet daher ebenfalls IP-Pakete zum Versand Nachrichten. Abb. 4.7 zeigt, wie eine IGMP-Nachricht in einem Daten-Frame eingekapselt ist.

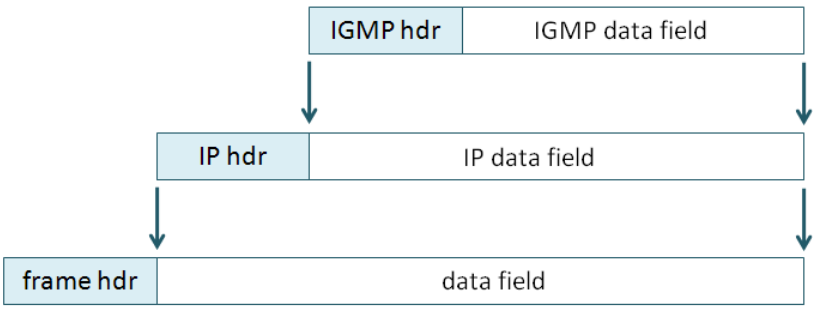


**Abbildung 4.7:** Einkapselung einer IGMP-Nachricht

### 4.4.3 IGMP-Snooping

Ein Switch, der ein Mitglied einer Multicast-Gruppe mit einem Router verbindet, kann mit Hilfe des IGMP-Snooping IGMP-Nachrichten lesen und auswerten. IGMP-Snooping übersetzt Multicast-IP-Adressen in Multicast-MAC-Adressen. Auf diese Weise kann ein Switch Multicast-MAC-Adressen in seiner Multicast-Filtertabelle speichern und so Multicast-Nachrichten nur an die korrekten Ports schicken. Dadurch wird verhindert, dass Multicast-Nachrichten ein

Netzwerk unnötig belasten. Dieses Verfahren ist bei Switches unter dem Namen dynamisches Multicasting bekannt, im Gegensatz zum statischen Multicasting, bei dem die Gruppen in allen Switches und für alle Ports manuell konfiguriert werden müssen.

### 4.4.4 Multicast-Adressen

Multicast-IP-Adressen sind Adressen im Bereich zwischen 224.0.0.0 und 239.255.255.255 (der Klasse D). Für private Netzwerke wird im Allgemeinen empfohlen, für Multicast-IP-Adressen den Bereich 239.x.x.x zu verwenden.

Die Adressen im Bereich von 224.0.0.1 bis einschließlich 224.0.0.255 sind für Multicast-Anwendungen innerhalb eines Netzwerks reserviert. Der Time-to-Live-Wert derartiger IP-Pakete wird auf 1 gesetzt, sodass sie das Netzwerk nicht verlassen können.

Es sind auch Multicast-MAC-Adressen reserviert. Alle Adressen, deren erstes Byte 01h ist, stehen für das Multicasting zur Verfügung. Adressen, die mit 01:00:5E:0 beginnen, sind Multicast-MAC-Adressen, die für das IP-Multicasting verwendet werden.

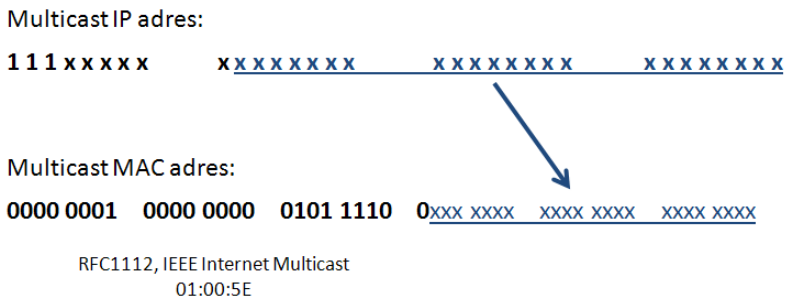


**Abbildung 4.8:** Umwandlung einer Multicast-IP-Adresse in eine Multicast-MAC-Adresse

Diese Umwandlung ist erläuterungsbedürftig. Das höchstwertige Bit des zweiten Bytes gehört zum Identifizierungs-Code einer Multicast-Adresse und wird daher nicht *mitgemappt*. So wird die Multicast-IP-Adresse 228.30.117.216 in die Multicast-MAC-Adresse 01:00:5E:1E:75:D8 umgewandelt. Die Multicast-IP-Adresse 228.158.117.216 wird hingegen in die Multicast-MAC-Adresse 01:00:5E:1E:75:D8 umgewandelt.

## 4.5 GMRP

### 4.5.1 IEEE 802.1p

Firmennetzwerke werden immer größer und komplexer. Es ist daher wichtig, dass der wachsende Datenverkehr effizient verwaltet werden kann. Hierbei stellt die "Quality of Serviceëin wichtiges Werkzeug dar, mit dem gewährleistet werden kann, dass die am meisten kritischen Daten auf vorhersagbare Weise übermittelt werden. Mit Hilfe des IEEE 802.1p-Protokoll können Switches Daten im Netzwerk bevorzugt übermittelt werden. Dadurch werden Vorhersagbarkeit und Zuverlässigkeit des Datenverkehrs verbessert.

IEEE 802.1p definiert innerhalb eines getaggten Ethernetframes ein 3-Bit-Feld, mit dem den zu übertragenden Daten eine Priorität von 0 bis 7 zugewiesen werden kann.

Der IEEE 802.1P-Standard sieht auch Maßnahmen zur Filterung von Multicastpaketen vor, damit diese sich nicht unnötig über Schicht-2-Netzwerke verbreiten. Eine dieser Maßnahmen ist das GMRP (GARP Multicast Registration Protocol). GMRP und GARP sind vom IEEE 802.1P definierte industrielle Protokolle.

### 4.5.2 Funktion des GMRP

GMRP verarbeitet Multicast-Gruppenadressen auf Schicht 2 (MAC-Schicht). GMRP arbeitet sowohl bei den Switches als auch bei den Hosts. Beim Host wird GMRP zusammen mit IGMP eingesetzt. Dort bildet es aus den IGMP-Paketen der Schicht 3 Datenframes auf Schicht 2.

Ein Switch empfängt sowohl die GMRP-Pakete auf Schicht 2, als auch die IGMP-Pakete auf Schicht 3. Mit den GMRP-Paketen begrenzt der Switch den Datenverkehr in der VLAN-Gruppe, zu der der sendende Host gehört. Wenn der Switch die "GMRP Join Messageëmpfängt, wird der Port, über den sie empfangen wurde, der betreffenden Multicastgruppe hinzugefügt. Der Switch leitet die Teilnahmeanforderung an alle anderen Teilnehmer des VLANs weiter, worunter sich auch die Multicastquelle befindet. Wenn die Quelle eine Multicastnachricht an die Gruppe schickt, leitet der Switch diese nur an die Mitglieder der entsprechenden Gruppe weiter.

Der Switch sendet regelmäßig GMRP-Queries. Wenn ein Teilnehmer in einer Gruppe bleiben will, muss er diese Queries beantworten. Möchte ein Teilnehmer nicht mehr zu der Gruppe gehören, kann er eine Leave-Nachricht schicken oder einfach nicht mehr antworten. Wenn der Switch von einem bestimmten Host keine Antwort oder eine Leave-Nachricht erhält, streicht er den betreffenden Teilnehmer aus der Liste.

## 4.6 DNS

### 4.6.1 Einleitung

Es gibt zwei wesentliche Arten, einen Host im Internet zu identifizieren: Neben der bereits dargestellten IP-Adresse gibt es auch die Möglichkeit, einem Teilnehmer einen Host-Namen (einen Klartextnamen) zuzuweisen, der im Allgemeinen die Verwendung erleichtert.
Host-Namen, wie etwa www.google.be (Suchmaschine) oder www.phoenixcontact.com lassen sich leichter merken und sind daher anwenderfreundlicher. Ein Host-Name enthält jedoch nicht genügend Informationen, um den Host im Internet auffinden zu können. Da Anwender den Host-Namen bevorzugen, die TCP/IP-Protokolle jedoch auf IP-Adressierung basieren, muss eine Zuordnung zwischen Host-Namen und IP-Adressen vorgenommen werden. Dies geschieht durch das Domain Name System (DNS), das von Dr. Paul V. Mockapetris und Jon Postel erfunden wurde. 1983 stellten sie die DNS-Architektur in RFC882 und 883 vor.

Zusammenfassend steht DNS für:

- eine verteilte Datenbank, die in einer Hierarchie von DNS-Servern implementiert ist;

- ein Protokoll auf der Anwendungsschicht, mit dem Hosts und DNS-Server miteinander kommunizieren können, um die Umwandlung von IP-Adressen in Host-Namen und umgekehrt vornehmen zu können.

Die DNS-Server sind häufig Unix-Maschinen, auf denen Software wie Berkeley Internet Name Domain (BIND) oder Microsoft DNS läuft. Das DNS-Protokoll arbeitet mit UDP und verwendet Port 53.

### 4.6.2 Die Struktur von Host-Namen

Hinsichtlich der Syntax bestehen Host-Namen stets aus einer Reihe alphanumerischer Segmente, die durch Punkte voneinander getrennt sind. Domain-Namen haben eine hierarchische Struktur, wobei der signifikanteste Teil des Namens rechts steht. Das am weitesten links stehende Segment ist der Name des individuellen Hosts. Andere Segmente in einem Domain-Namen identifizieren die Gruppe, die Eigner des Namens ist. DNS legt nicht fest, aus wie vielen Segmenten ein Domain-Name besteht, gibt aber Werte für das signifikanteste Segment vor. Tabelle 4.1 zeigt eine Übersicht der verschiedenen Werte des signifikantesten Segments.

**Tabelle 4.1:** Werte für das signifikanteste Segment eines Domain-Namens

| Domain-Name | zugewiesen an |
|---|---|
| com | kommerzielle Organisationen |
| edu | Bildungseinrichtungen |
| gov | öffentliche Organe |
| mil | Militär |
| net | Netzwerkverwaltungseinrichtungen |
| org | sonstige Organisationen |
| int | internationale Organisationen |
| Länder-Codes | Staaten, z. B. be für Belgien |

### 4.6.3 Funktionsweise des DNS-Protokolls

#### Einleitung

Wenn eine Anwendung (z. B. ein Webbrowser) auf dem Host eines Anwenders einen Host-Namen in eine IP-Adresse umwandeln muss, ruft diese Anwendung die Clientkomponente des DNS unter Angabe des umzuwandelnden Host-Namens an. Die Client-Komponente des DNS auf dem Host des Anwenders übernimmt dann und sendet eine Anfrage über das Netzwerk. Alle Anfrage- und Antwortnachrichten des DNS werden in UDP-Segmente an Port 53 gesendet.
Nach einer Zeit von einigen Millisekunden bis zu einigen Sekunden empfängt die Client-Komponente auf dem Anwender-Host die DNS-Antwortnachricht mit der gesuchten Auflösung. Diese Auflösung wird dann an die Anwendung übergeben. Auf diese Weise stellt das DNS aus Sicht der Anwendung auf dem Host des Benutzers eine Blackbox dar, die eine einfache und unkomplizierte Umwandlung erlaubt. In Wirklichkeit ist der von dieser Blackbox zur Verfügung gestellte Dienst jedoch sehr komplex und besteht aus einer großen Anzahl von über die ganze Welt verteilten DNS-Servern sowie einem Protokoll auf der Anwendungs-

schicht, welches festlegt, wie die DNS-Server und die anfragenden Hosts miteinander kommunizieren.
Ein einfacher DNS-Entwurf bestünde aus einem einzigen DNS-Server, auf dem alle Verweise gespeichert sind. In einem solchen zentralisierten Entwurf müssten alle Clients ihre Anfragen nur an diesen einen DNS-Server senden, der alle diese Anfragen abarbeitet. Ihre Einfachheit lässt eine solche Struktur zwar sehr attraktiv erscheinen, doch ist diese Lösung für das gegenwärtige Internet mit seiner enormen (und weiterhin schnell steigenden) Anzahl von Hosts ungeeignet.

Das DNS-System verwendet daher eine große Anzahl über die ganze Welt verteilte DNS-Server, die in einer hierarchischen Struktur organisiert sind. Es gibt nicht einen einzelnen DNS-Server, der alle Verweise für alle Hosts im Internet enthält, sondern sie sind über viele verschiedene DNS-Server verteilt.
In erster Instanz gibt es drei Klassen von DNS-Servern:

- Root-Nameserver;
- Top-Level-Domain-Nameserver (TLD-Nameserver);
- Autoritative DNS-Nameserver

**Eine verteilte, hierarchische Datenbank**

Zunächst nimmt ein DNS-Client Kontakt zu einem der Rootserver auf, der die IP-Adressen von TLD-Servern für die TLD comßurückgibt. Dann nimmt der Client Kontakt zu einem dieser TLD-Server auf, der dann die IP-Adresse eines autoritativen Servers zurückgibt. Schließlich nimmt der Client Kontakt zu einem dieser autoritativen Server auf, der dann die IP-Adresse des Host-Namen zurückgibt.

**DNS-Rootserver**
Im Internet gibt es lediglich 13 DNS-Rootserver (die mit den Buchstaben A bis M bezeichnet werden). Die meisten von ihnen befinden sich in Nordamerika. Obwohl die 13 DNS-Rootserver als jeweils ein einziger Server bezeichnet werden, so besteht doch jeder *Server* aus Gründen der Sicherheit und Zuverlässigkeit in Wirklichkeit aus einem Cluster replizierter Server.

**Top-Level-Domain-Server (TLD-Server)**
Diese Server sind für die Top-Level-Domains (z. B. com, org, net, edu) sowie alle länderspezifischen Top-Level-Domains (z. B. nl, fr, jp etc.) verantwortlich.

**Autoritative DNS-Server**
Jede Organisation mit öffentlich zugänglichen Hosts im Internet (wie Webservern und Mailservern) muss DNS-Daten öffentlich zugänglich machen, mit denen die Übersetzung der Host-Namen in IP-Adressen möglich wird. Der autoritative DNS-Server einer Organisation hält diese DNS-Datensätze bereit. Eine Organisation kann ihren eigenen autoritativen DNS-Server installieren, um diese Daten zu speichern; alternativ kann die Organisation dafür zahlen, diese Aufzeichnungen auf einem autoritativen DNS-Server eines Dienstanbieters speichern zu lassen. Die meisten Universitäten und großen Unternehmen installieren und verwalten ihre eigenen primären und sekundären (aus Backup-Gründen) autoritativen DNS-Server.
Die Root-, TLD- und autoritativen DNS-Server zählen alle zur Hierarchie der DNS-Server. Es gibt außerdem noch einen weiteren wichtigen Typ von DNS-Servern, der als lokaler DNS-Server bezeichnet wird. Ein lokaler DNS-Server gehört streng genommen nicht zur Hierarchie

der Server, ist aber dennoch ein wesentlicher Bestandteil der DNS-Architektur. Jeder ISP (Inter Service Provider) - z. B. eine Universität, eine Firma oder ein ISP für Privatanwender - besitzt einen lokalen DNS-Server (der auch als Default Name Server bezeichnet wird). Wenn ein Host eine Verbindung zu einem ISP aufnimmt, liefert dieser dem Host die IP-Adressen eines oder mehrerer seiner lokalen DNS-Server (normalerweise mittels DHCP).

## 4.7 SNMP

### 4.7.1 Einleitung

**SNMPv1:** Das SNMP-Protokoll wurde 1990 in RFC 1157 definiert. SNMP steht für *Simple Network Management Protocol.* Dieses Protokoll beschreibt eine strukturierte Methode für die Überwachung und Verwaltung einer bestimmten Netzwerkinfrastruktur. Es wurde schnell in großem Umfang in kommerziellen Produkten angewendet und wurde der de-facto-Standard für die Netzwerkverwaltung. SNMP ist ein einfaches Protokoll.

**SNMPv2:** Die Erfahrungen mit dem Protokoll führten 1993 zu einer verbesserten Version des SNMP, die in RFC 1441 und RFC 1452 (Koexistenz von v1 und v2) beschrieben und schließlich zum Standard im Internet wurde.

**SNMPv3:** Die dritte Version des Standard Management Framework (SNMPv3) basiert auf den Vorgängerversionen SNMPv1 und SNMPv2. SNMPv3 ist im Prinzip SNMPv2, ergänzt um Sicherheit und Administration. Zu den wichtigsten Eigenschaften von SNMPv3 zählen:

- Sicherheit
  - Authentifizierung und Datenschutz
  - Zugangskontrolle
- Administration
  - Management von Benutzernamen und Schlüsseln
  - Benennung von Teilnehmern
  - Policies

In einem Netzwerk sind zahlreiche interessante Teilnehmer aktiv, die über wichtige Statusinformationen für die Verwaltung eines Netzwerks verfügen können. Solche Teilnehmer können Hubs, Switches, Router, Drucker oder PCs sein. Um direkt durch SNMP verwaltet werden zu können, muss auf einem Knoten ein SNMP-Managementprozess - ein sog. SNMP-Agent - laufen können. Alle Computer sind dazu in der Lage, ebenso zahlreiche Hubs, Switches, Router und Peripheriegeräte, die für den Einsatz im Netzwerk vorgesehen sind. Jeder Agent führt eine lokale Datenbank, in der sein Zustand in Gegenwart und Vergangenheit in Variablen festgehalten ist, die seine Arbeit beeinflussen.

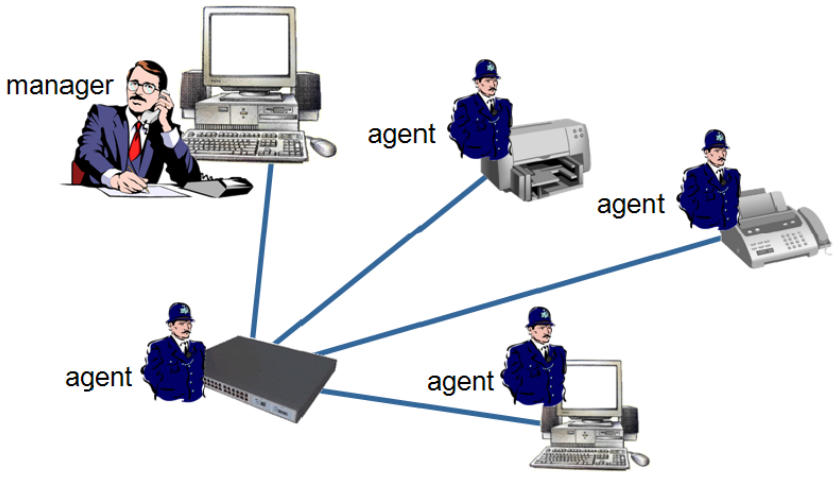


**Abbildung 4.9:** Manager und Agenten in einem Netzwerk

Das Netzwerkmanagement findet in Managementstationen statt: in der Praxis normale Computer, auf denen eine spezielle Management-Software läuft. Auf diesen Stationen laufen einer oder mehrere Prozesse, die über das Netzwerk mit Agenten kommunizieren, indem Sie Aufträge erteilen und Antworten erhalten. In diesem Aufbau sitzt alle Intelligenz in den Managementstationen, um die Agenten so einfach wie möglich zu halten und ihren Einfluss auf die Geräte, auf denen sie laufen, zu minimieren. Zahlreiche Managementstationen weisen eine graphische Benutzeroberfläche auf, sodass der Netzwerkadministrator den Zustand des Netzwerks inspizieren und ggf. Maßnahmen ergreifen kann.

### 4.7.2 Struktur des SNMP

Das SNMP besteht aus drei wesentlichen Teilen:

- MIB (Management Information Base (RFC1213)): Beschreibung aller Variablen eines bestimmten Netzwerkelements;
- SMI (Structure of Management Information (RFC 1155)): Struktur für die Speicherung der Netzwerkinformationen;
- SNMP: Protokoll für die Kommunikation zwischen Manager und einem Netzwerkteilnehmer (RFC1157).

Die meisten bestehenden Netzwerke bestehen aus Elementen verschiedener Hersteller - Hosts von einem oder mehreren Herstellern, Switches und Routern von anderen Firmen, und Drucker von wiederum anderen Fabrikaten. Um zu gewährleisten, dass eine Managementstation (die u. U. wiederum von einem anderen Hersteller stammt) mit all diesen verschiedenen Komponenten kommunizieren kann, muss die Art der von diesen Geräten gesammelten Informationen strikt spezifiziert werden. Es ergibt keinen Sinn, wenn eine Managementstation einen Router nach der Häufigkeit des Auftretens von verlorengegangenen Paketen fragt, wenn der Router diese Information nicht registriert. Deshalb beschreibt SNMP genau die Informationen, die jede Art von Agenten zur Verfügung stellen muss, sowie das Format, das der Agent dazu zu verwenden hat. Der größte Teil des SNMP-Modells besteht darin, zu definieren, wer welche Informationen führen muss und wie diese zu übermitteln sind. Kurz gefasst

läuft es darauf hinaus, dass jedes Gerät eine oder mehrere Variablen (Objekte) führt, die den Zustand des Geräts beschreiben. Die Gesamtheit aller möglichen Objekte in einem Netzwerk steht in einer Datenstruktur, die MIB (Management Information Base) genannt wird.
Das SNMP-Protokoll selbst beschreibt nun, wie die Interaktion zwischen der Managementstation und Agenten zustande kommt. Zu diesem Zweck werden fünf verschiedene Nachrichtentypen definiert.

### 4.7.3 MIB und SMI

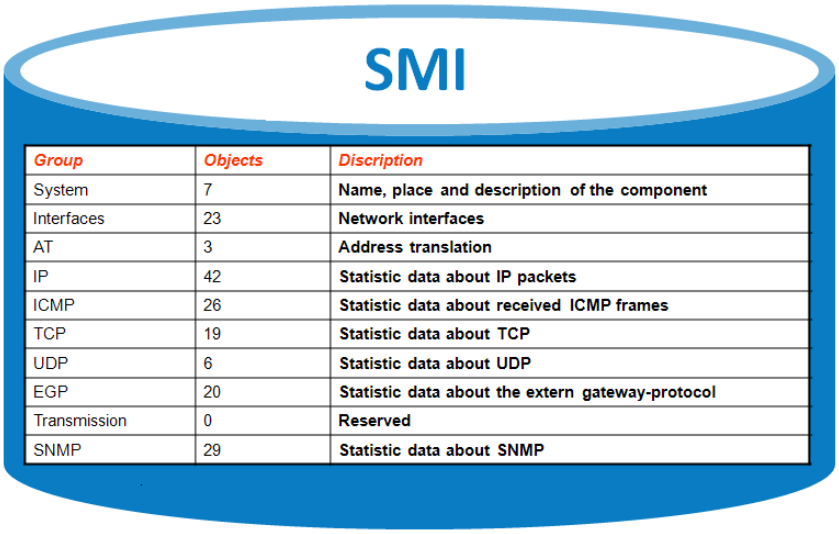


**Abbildung 4.10:** Die MIB ist eine Datenbank, die alle Variablen für das Netzwerkmanagement enthält

Die vom SNMP verwalteten Objekte werden in der MIB definiert und sind in Abb. 4.10 zu finden. Der Einfachheit halber werden diese Objekte in verschiedene Gruppen aufgeteilt. Diese Kategorien bilden eine Grundlage dafür, welche Informationen eine Managementstation verarbeiten können muss.

- Das Gruppensystem bietet dem Manager die Gelegenheit herauszufinden, wie ein Gerät heißt, wer es hergestellt hat, welche Hard- und Software es enthält, wo es sich befindet und was seine Aufgabe ist. Auch der Zeitpunkt des letzten Boot-Vorgangs wird angegeben.
- In der Interfaces-Gruppe geht es um die Netzwerkadapter. Die Gruppe registriert, wie viele Pakete und Bytes im Netzwerk gesendet und empfangen und verworfen werden, wie viele Broadcasts es gibt, und wie groß die Ausführungswarteschlange ist.
- Die Gruppe IP beschäftigt sich mit dem IP-Verkehr von und zum Knoten. Hier gibt es vor allem Zähler, die registrieren, wie viele Pakete aus verschiedenen Gründen verworfen wurden. Auch gibt es statische Daten über das Fragmentieren und Wiederzusammensetzen von Datagrammen. All diese Informationen sind vor allem für die Verwaltung von Routern von Bedeutung.
- In der ICMP-Gruppe geht es um IP-Fehlermeldungen. Hier gibt es für jede ICMP-Meldung einen Zähler, der die Anzahl des jeweiligen Meldungstyps registriert.

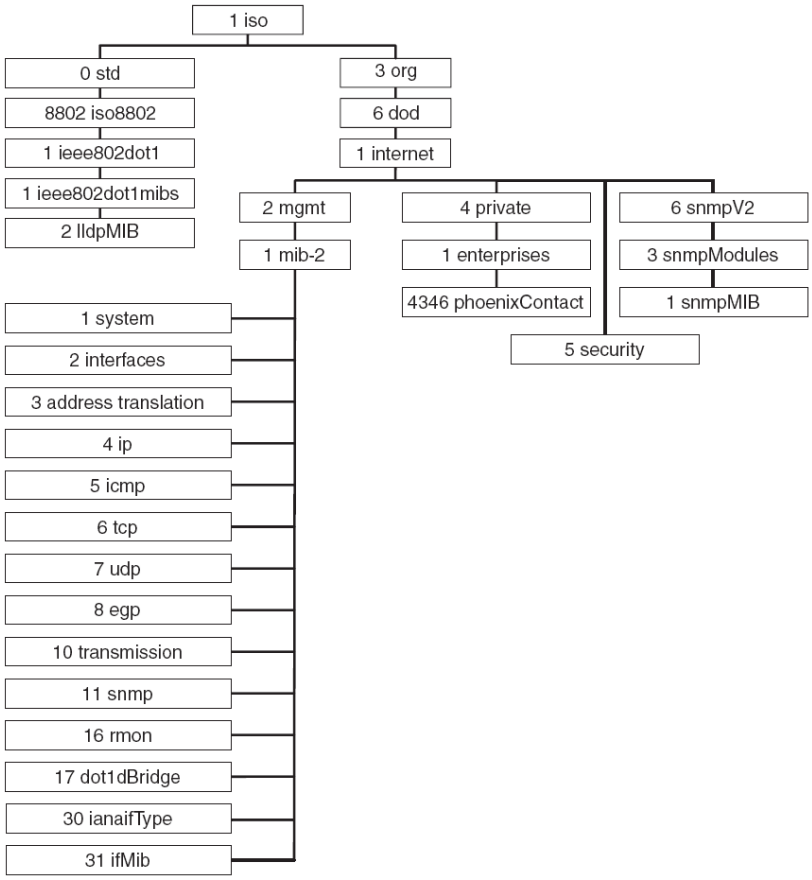


**Abbildung 4.11:** Baumstruktur der MIB

- Die TCP-Gruppe zeichnet die aktuelle Anzahl der geöffneten Verbindungen und der gesendeten und empfangenen Segmente sowie verschiedene statistische Daten über Fehler auf.
- Die UDP-Gruppe zählt die gesendeten und empfangenen UDP-Datagramme und registriert, wie viele davon auf Grund eines unbekannten Ports oder aus anderen Gründen unzustellbar waren.
- Die letzte Gruppe dient dazu, statistische Daten über die Arbeit des SNMP selbst zu sammeln: Wie viele Nachrichten wurden gesendet, um was für Nachrichten handelte es sich usw.

Jede Variable, jedes Objekt in der MIB wird durch einen Object Identifier (OID) und dessen Typ gekennzeichnet:

- Der OID beschreibt einen Pfad in der MIB-Baumstruktur. Abb. 4.11 zeigt die Struktur der im SNMP gebrauchten MIB. Das Objekt *sysObjectID*, welches zur Gruppe *System* gehört, ist über den OID 1.3.6.1.2.1.1.2.0 erreichbar.
- Objekttypen werden mit Hilfe von grundlegenden Typen aufgebaut, die in der SMI definiert sind.

Es stehen verschiedene MIBs zur Verfügung. Zunächst wurden die globalen MIBs in den RFCs beschrieben (z. B. MIB2 in RFC1213). Diese MIBs müssen von allen SNMP-kompatiblen Geräten unterstützt werden. Ferner gibt es auch noch herstellerspezifische MIB-Objekte.

### 4.7.4 SNMP-Protokoll

Das SNMP arbeitet normalerweise so, dass die Managementstation eine Anfrage an einen Agenten sendet, in dem sie Informationen anfordert oder ihn auffordert, seinen Zustand auf eine bestimmte Art und Weise zu ändern. Im Idealfall antwortet der Agent nur mit der angeforderten Information oder bestätigt, dass er seinen Zustand wie gewünscht geändert hat. SNMP definiert die verschiedenen Nachrichten, die verschickt werden können.

**Tabelle 4.2:** SNMP-Nachrichten vom Manager an den Agenten

| Nachricht | Beschreibung |
|---|---|
| Get request | Fragt den Wert einer oder mehrerer Variablen ab |
| Get next request | Ffragt die der gegenwärtigen folgende Variable ab |
| Get bulk request | Fragt eine große Gruppe Informationen ab |
| Set request | Ändert eine oder mehrere Variablen |
| Inform request | Nachricht zwischen verschiedenen Managern zur Beschreibung der lokalen MIB |

In einem bestimmten Fall kann der Agent selbst die Initiative ergreifen und eine Nachricht verschicken, nämlich wenn er das Auftreten eines kritischen Ereignisses feststellt. Verwaltete Knoten können ausfallen und neustarten, Netzwerksegmente können ausfallen und wieder in Betrieb gehen usw. Jedes relevante Ereignis wird in einem MIB-Modul definiert. Wenn ein Agent feststellt, dass ein relevantes Ereignis eingetreten ist, meldet er dies unmittelbar allen Managementstationen in seiner Konfigurationsliste. Diese Meldung wird *SNMP-Trap* genannt. Sie zeigt jedoch in der Regel lediglich das Auftreten eines Ereignisses an. Es ist die Aufgabe der Managementstation, Requests auszuführen, um die Details in Erfahrung zu bringen.

**Tabelle 4.3:** SNMP-Nachrichten vom Agenten an den Manager

| Nachricht | Beschreibung |
|---|---|
| SNMP-Trap | Agent meldet dem Manager ein Ereignis |

Abb. 4.12 zeigt, dass SNMP-Nachrichten das UDP-Protokoll verwenden, und welche Ports hierfür benutzt werden.

## 4.8 HTTP und HTTPS

### 4.8.1 TLS/SSL

Das Transport Layer Security (TLS), Nachfolger des Secure Sockets Layer (SSL), ist ein Verschlüsselungsprotokoll, mit dem ein sicherer Datenkanal in einem ungesicherten Netzwerk wie dem Internet geschaffen wird.

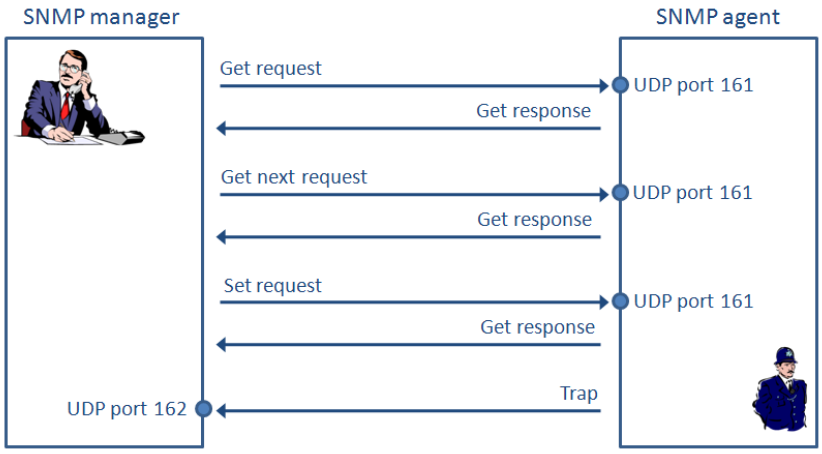


**Abbildung 4.12:** SNMP-Kommunikation

Beide Protokolle arbeiten eine Schicht tiefer als die Anwendungsprotokolle, wie etwa HTTP, SMTP, FTP etc., aber oberhalb des Transportprotokolls TCP. Sie sind ein Teil der Protokollfamilie TCP/IP. Eines ihrer wichtigsten Ziele ist das Sichern von Client/Serverapplikationen.

Senderseitig verschlüsselt die TLS-Schicht Daten der Applikation und übermittelt sie an den richtigen TCP-Port. An der Empfängerseite liest TLS die Daten aus dem korrekten TCP-Port aus, entschlüsselt sie und leitet sie an die Anwendung weiter. Das Durchschleusen der Daten ist Aufgabe der Record-Schicht.

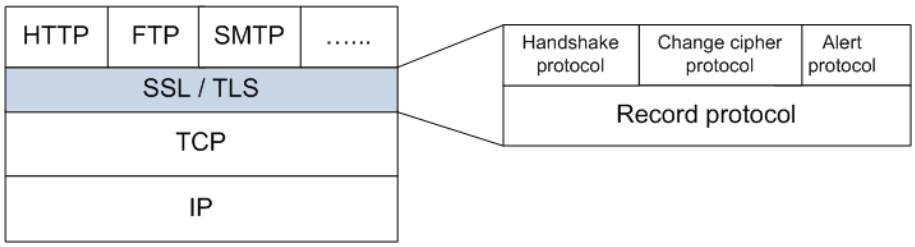


**Abbildung 4.13:** TLS/SSL protocol

TLS bietet die folgenden Sicherheitsfunktionen für Client/Serverapplikationen über TCP/IP:

- Authentifikation: Diese ermöglicht einer Applikation die Überprüfung der Identität einer anderen Applikation, mit der sie kommuniziert.
- Datenschutz: Zwischen den Applikationen übermittelte Daten sind vor Einsicht oder Missbrauch geschützt.
- Integrität: Anwendungen können feststellen, wenn Daten bei der Übertragung geändert wurden.

Die eingesetzten Techniken basieren auf Konzepten wie öffentlichen Schlüsseln und Zertifikaten (siehe Abschnitt SSicherheit").

Wenn eine Applikation SSL/TLS einsetzt, wird zunächst ein Handshakeverfahren gestartet, bei dem der Verschlüsselungsalgorithmus und die zu verwendenden Schlüssel vereinbart und der Server vom Client verifiziert werden. Nach Abschluss dieses Verfahrens werden alle Anwendungsdaten verschlüsselt. Die Durchführung und Überwachung des Handshakeverfahrens wird von den obersten Teilschichten des Protokolls übernommen (siehe Abb. 4.13 ).

### 4.8.2 HTTP

HTTP (HyperText Transfer Protocol) ist das Protokoll für die Kommunikation zwischen einem Webclient (einem Webbrowser) und einem Webserver. Dieses Protokoll wird nicht nur im World Wide Web, sondern auch in lokalen Netzwerken verwendet. Es definiert das genaue Format der Anfragen (Requests) eines Webbrowsers an den Server sowie das Format der Antworten (Responses), die der Webserver darauf geben kann. Jede Anfrage enthält eine URL, die auf eine Netzkomponente oder ein statisches Objekt (z. B. eine Webseite) verweist. Das HTTP-Protokoll verwendet Port 80.

Jede HTTP-URL beginnt mit "http://".

HTTP ist unsicher und anfällig gegenüber Man-in-the-middle-Angriffen und Abhörpraktiken.

### 4.8.3 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) ist eine Erweiterung des HTTP-Protokolls, das zum sicheren Austausch von Daten dient. Bei Verwendung von HTTPS werden die Daten verschlüsselt, wodurch es für einen Außenstehenden unmöglich wird, die Daten abzufangen. HTTPS ist im Prinzip HTTP, wobei zusätzlich SSL/TLS genutzt wird, um die Daten zu verschlüsseln und den Server zu verifizieren.

Jede HTTPS-URL beginnt mit "https://".

Das Protokoll verwendet TCP-Port 443.

## 4.9 Übersicht über einige andere wichtige Anwendungen

### 4.9.1 FTP

FTP (File Transfer Protocol) ist ein Protokoll, mit dem der Austausch von Dateien zwischen verschiedenen Hosts vereinfacht wird. Es gestattet die Übertragung beliebiger Dateien und das Anlegen von Verzeichnissen sowie das Umbennen oder Löschen von Verzeichnissen und Dateien. Das Protokoll verbirgt die Details eines individuellen Computer-Systems vor dem Anwender und eignet sich daher für heterogene Situationen. Das Protokoll kann Dateien zwischen beliebigen Systemen übertragen.

### 4.9.2 TFTP

TFTP (Trivial File Transfer Protocol) ist eine vereinfachte FTP-Version, die häufig verwendet wird, um Geräte wie Router, Switches etc. mit Firmware und Konfigurationen zu versehen.

### 4.9.3 NTP

NTP (Network Time Protocol) ist ein Protokoll, mit dem Computer in einem Netzwerk ihre interne Uhr mit der anderer Computer synchronisieren können. NTP basiert auf der Vorhersagbarkeit der vom Netzwerk verursachten Verzögerung. Das Computer-Netzwerk wird dabei hierarchisch aufgeteilt, wobei der Computer mit der genauesten Zeit als SStratum 0"bezeichnet wird. Die Computer-Systeme, die über NTP direkt von dort ihre Zeit holen, sind laut Definition SStratum 1". Das Protokoll verfügt über einige intelligente Funktionen. So kann z. B. ein NTP-Client Gebrauch von mehreren NTP-Servern machen und dabei selbst entscheiden, welcher der Server am besten arbeitet. Anhand einiger Entscheidungskriterien wählt ein NTP-Client einen Server aus und synchronisiert sich mit ihm. Kleine Zeitunterschiede zwischen Server und Client werden vom Client behoben, in dem er seine Uhr etwas schneller oder langsamer laufen lässt. Auf diese Weise kann die Zeitdifferenz ohne Zeitsprünge ausgeglichen werden.

### 4.9.4 SSH

Secure Shell ist auf der Anwendungsschicht des TCP/IP-Protokolls angesiedelt. SSH ersetzt ältere Protokolle wie Telnet und Rlogin durch eine gesicherte Variante. Das Protokoll verwendet TCP-Port 22.

Mit SSH ist ein sicheres Login an einem anderen Computer sowie die Ausführung von Befehlen auf einem Computer an einem anderen Ort über eine Shell möglich. Die eingesetzte Verschlüsselung erschwert es Fremden, die Originalbefehle zu lesen.

Ein wesentlicher Vorteil von SSH ist die Möglichkeit zur Authentifizierung mit einem asymmetrischen Verschlüsselungsverfahren. Dadurch können SSH-Anwendungen automatisiert eingesetzt werden, ohne dass im Code ein Kennwort hinterlegt sein muss. Durch den privaten Schlüssel ist eine Anmeldung an jedem System, das den entsprechenden öffentlichen Schlüssel verwendet, möglich.

### 4.9.5 CLI (Command Line Interface)

Betriebssystemen mit einem Command Line Interface (Kommandozeilenoberfläche) kann der Anwender über Textbefehle Aufträge erteilen. Ist die Ausführung eines Befehls abgeschlossen, kann der Anwender weitere Befehle eingeben. Ein Befehl wird in der Regel mit der <Enter>-Taste abgeschlossen.

Bekannte CLIs sind command.com (DOS) oder Bash (UNIX).

Neben Betriebssystemen gibt es noch weitere Softwareprogramme, die mit einem CLI bedient werden können, z. B. der FTP-Client und der Telnet-Client von Microsoft. Auch industrielle Switches sind häufig über ein CLI bedienbar.

# Kapitel 5

# Der Switch

## 5.1 Allgemein

Der Switch ist die Basiskomponente für den Aufbau eines lokalen ethernetbasierten Netzwerks. Mit Hilfe von Switches werden die verschiedenen Teilnehmer eines LANs auf intelligente Weise miteinander verbunden. Ein Switch hat mehrere Ports. An jedem dieser Ports kann ein Host (ein Netzwerkteilnehmer) oder ein anderer Switch angeschlossen werden. Auf diese Weise kann ein Netzwerk mit einer Sterntopologie aufgebaut werden. An jedem Port beginnt ein Netzwerksegment (eine Kollisionsdomäne).

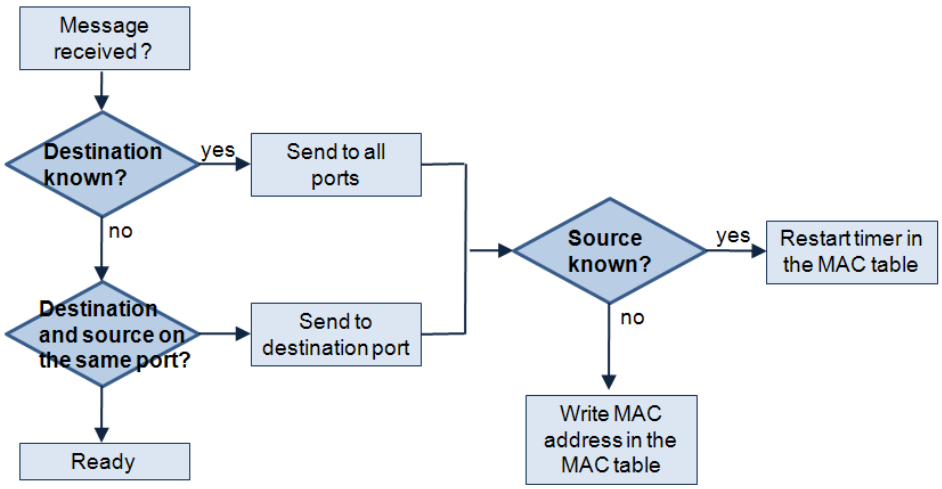


**Abbildung 5.1:** Der Switch lernt anhand der eingehenden Nachrichten

Für jeden Port wird software-seitig eine MAC-Adresstabelle geführt. Der Switch ist selbstlernend: Die MAC-Adresstabelle wird durch Analyse aller in dem betreffenden Segment eingehenden Nachrichten gefüllt. Die Quelladresse jeder eingehenden Nachricht an einem bestimmten Port wird in die Tabelle kopiert. Jede Adresse wird eine begrenzte Zeit in der Tabelle gehalten und wieder gelöscht, wenn eine bestimmte Zeit, die Aging-time, verstrichen ist. Auf diese Weise wird verhindert, dass Stationen nicht mehr erkannt oder inaktive Stationen adressiert werden.

Ein Switch untersucht vor der Weiterleitung eines Datenpakets von einem Segment zum anderen die MAC-Adresse und entscheidet in Abhängigkeit davon, ob der Transport in das andere Segment stattfindet oder nicht. Switches arbeiten nach der Store-and-Forward-Methode.

Ein Store-and-Forward-Switch nimmt zunächst das gesamte Daten-Frame entgegen, überprüft es auf Fehler, und sendet es dann über den korrekten Port weiter. Die Latenz ist daher von der Nachrichtengröße abhängig.
Am Beginn einer Nachricht steht die Präambel. Zwischen der Präambel und dem liegt ein bestimmter Zeitraum: der Interframe-Gap. Diese Zeit entspricht derjenigen Zeitdauer, die für das Übertragen von 96 Bits über das Netzwerk nötig ist. Sie beträgt bei 100 Mbit/s also 0,96 $\mu$s.
Die theoretische Latenz eines Store-and-Forward-Switches für das Weitersenden einer Nachricht mit der Mindestlänge (64 Bytes) lässt sich gemäß folgender Gleichung bestimmen: TL = TIG (Dauer des Interframe-Gap) + (64 $*$ 8 $*$ TBT) [$\mu$s].
TL = 0,960 + (64 $*$ 8 $*$ 0,01) = 6,08 $\mu$s.
Die maximale Nachrichtenlänge beträgt 1518 Bytes. Darauf ergibt sich die folgende Latenz:
TL = 0,960 + (1518 $*$ 8 $*$ 0,01) = 122,4 $\mu$s

## 5.2 Industrielle Switches

### 5.2.1 Allgemein

Industrielle Switches können zunächst in zwei verschiedene Kategorien eingeteilt werden:

- Unmanaged Switches
- Managed Switches

Bei der ersten Gruppe von Switches können keine Konfigurationen vorgenommen werden. Dies ist für die allgemeine Funktion eines Switches auch nicht nötig.

Die zweite Gruppe Switches kann z.B über einen Webserver konfiguriert werden. Eine solche Herangehensweise ist interessant für die Diagnose des Netzwerks.

**Abbildung 5.2:** Der FL SWITCH SFN 8GT

Abb. 5.2 zeigt den industriellen Switch FL SWITCH SFN 8GT Gigabit Switch von Phoenix Contact. Einige typische technische Merkmale derartiger Switches sind:

- 10/100/1000 TX, Auto-Negotiation, Auto-Crossing

- Unmanaged, keine Konfiguration
- Montage auf DIN-Schienen, Alarmkontakt, redundante Stromversorgung
- Temperaturbereich: -25°C bis +60°C

### 5.2.2 Technische Beschreibung eines industriellen Switches

Anhand der technischen Beschreibung eines Geräts aus der Reihe *Factory Line* von Phoenix Contact werden alle möglichen Eigenschaften eines Switches dargestellt.

**Abbildung 5.3:** Der FL SWITCH SMCS 8GT

SMCS steht für Smart Managed Compact Switch. Dieser Switch entspricht der Norm IEEE802.3 und dient zum Aufbau von Automationsnetzwerken auf Ethernet-Basis. Er weist acht RJ45-Ports zum Anschluss von Twisted-Pair-Kabeln auf. Alle Ports unterstützen 10/100/1000 Mbit/s sowie Autonegotiation und Autocrossing.

Der Switch eignet sich neben dem Einsatz als Standard-Ethernet-Switch besonders für Anwendungen im Bereich Profinet RT und Ethernet/IP und unterstützt die hierfür nötigen Management-Funktionen. Ferner unterstützt der Switch IGMP-Snooping für Ethernet/IP.

Redundante Netzwerkstrukturen können gemäß dem (Rapid) Spanning Tree Protocol oder dem Media Redundancy Protocol aufgebaut werden. Hierdurch wird unabhängig von der verwendeten Topologie eine optimale Funktion des Netzwerks gewährleistet.

Innerhalb vollständiger Netzwerksysteme können Informationen aus dem Switch über SNMP abgefragt werden. Konfiguration und Diagnose sind über Webserver, SNMP, Telnet oder eine V.24-Schnittstelle (RS232) möglich.

Der FL SWITCH SMCS 8GT ist ein Store-and-Forward-Switch. Alle Datentelegramme, die den Switch an einem Port erreichen, werden zunächst in einem Puffer gespeichert und auf ihre Gültigkeit überprüft. Korrupte Datenpakete, also solche mit einer Größe von mehr als 1522 oder weniger als 64 Bytes oder Pakete, bei denen ein Prüfsummenfehler auftritt, müssen verworfen werden. Gültige Datenpakete werden sodann umgehend über den korrekten Port weitergeschickt. Die Übertragungsgeschwindigkeit wird für jeden Port durch das angeschlossene Netzwerksegment festgelegt.

Der Switch lernt dynamisch alle Adressen der verschiedenen Netzwerkteilnehmer, indem er jeder eingehenden Nachricht die Quelladresse entnimmt. Es kann bis zu 8000 Adressen in

seiner Adresstabelle speichern. Die Aging Time beträgt 40 Sekunden (Default) und ist veränderbar. Diese Zeit kann per SNMP oder über eine webbasierte Verwaltung auf einen Wert zwischen 10 und 825 s eingestellt werden. Alle Adressen, die nach Ablauf dieser Zeit nicht mehr benötigt wurden, werden automatisch aus der MAC-Adresstabelle gelöscht.

Der Switch verfügt über einen Meldekontakt. Dieser Meldekontakt ist potentialfrei und bei ordnungsgemäßer Funktion des Switches geschlossen. Mit seiner Hilfe wird die Funktion des Switches überwacht, er wird unter den im Folgenden beschriebenen Umständen geöffnet. Bei einem Neustart führt der Switch einen Hardware-Selbsttest durch. Wenn dabei ein Fehler erkannt wird, wird der Meldekontakt geöffnet. Während des normalen Betriebs überwacht eine Watchdog-Einrichtung die zyklische Ausführung des Software-Programms. Wird diese Watchdog-Einrichtung nicht zyklisch von der Software getriggert, so wird der Meldekontakt geöffnet.

Der Anwender wird mit Hilfe verschiedener Status-LEDs über den Status des Switches informiert. Auf diese Weise ist eine lokale Diagnose ohne Einsatz zusätzlicher Tools möglich.

Der SMCS-Switch unterstützt Autocrossing. Dadurch ist es nicht mehr erforderlich, zwischen gekreuzten und ungekreuzten Twisted-Pair-Ethernet-Kabeln zu unterscheiden.

Der SMCS-Switch unterstützt Autonegotiation. Dabei erkennt der Switch automatisch die Parameter eines bestimmten Subnetzes an jedem Port und konfiguriert den jeweiligen RJ45-Port dementsprechend. Die erkannten Parameter sind: Übertragungsgeschwindigkeit (10, 100 oder 1000 Mbit/s) und Übertragungsmodus (Halb- oder Vollduplex). Diese automatische Erkennung macht manuelle Eingriffe durch den Anwender überflüssig. Die Autonegotiation-Funktion kann über die webbasierte Verwaltung ein- oder ausgeschaltet werden.

Bei Verwendung von Twisted-Pair-Kabeln mit der falschen Polarität (wenn also RD+ und RD- vertauscht sind), kehrt der Switch die Polarität automatisch intern um. Diese Eigenschaft ist unter dem Namen *Auto Polarity Exchange* bekannt.

Der Switch überprüft zu vorgegebenen Zeitpunkten die an jedem Port angeschlossenen Subnetze. Er verwendet Link-Testsignale wie in IEEE 802.3 beschrieben, um die angeschlossenen TP/TX-Kabel auf Kurzschluss und Unterbrechung zu überprüfen.

Der Switch kann auf zwei verschiedene Arten eine IP-Adresse erhalten: entweder über das BootP-Protokoll, oder über die serielle V.24-Schnittstelle. Werkseitig ist die Zuweisung der IP-Adresse auf BootP eingestellt. Es steht eine Konfigurations-Software zur Verfügung, um ggf. dem Switch auf einfache Weise eine IP-Adresse zuweisen zu können. Der Mechanismus zur Zuweisung einer IP-Adresse kann über die web-basierte Verwaltung oder die V.24-Schnittstelle eingestellt werden.

Über die MODE-Taste an der Vorderseite des Moduls kann der Switch in den Smart-Modus versetzt werden. Im Smart-Modus kann der Switch in einen anderen Modus versetzt werden, ohne die Management-Interfaces zu verwenden. Außerdem können im Smart-Modus die Werkseinstellungen wiederhergestellt werden.
Der Switch kann als Profinet-IO-Device konfiguriert werden. Über die Web-based Management oder im Smart-Modus kann zwischen den Betriebsmodi Default (Standard Ethernet-Switch) und Profinet-IO oder Ethernet/IP gewählt werden. Wird der Switch als Profinet-IO-Device konfiguriert, so kann er als ein solches in die Profinet-Engineeringsoftware aufgenom-

men werden. Auf diese Weise wird in der Engineeringsoftware pro Eingang des Switches ein Byte mit Diagnoseinformationen zur Verfügung gestellt.

Der SMCS-Switch unterstützt das LLDP-Protokoll gemäß IEEE802.1ab. Der Switch sendet und empfängt Verwaltungs- und Verbindungsinformationen an/von benachbarte(n) Geräte(n). So können über verfügbare Tools Netzwerkarchitekturen visuell dargestellt und überwacht werden. Die Profinet-Engineeringsoftware verwendet diese Informationen, um eine Netzwerkdiagnose visuell darzustellen.

Der Switch unterscheidet nach Priorität zwei verschiedene Warteschlangen (Traffic Classes gemäß IEEE802.1D). Empfangene Datenpakete werden je nach ihrer Priorität einer dieser Warteschlangen zugewiesen. Die Priorität ist im VLAN-Tag des Ethernetframes angegeben. So wird vermieden, dass die Übertragung von Daten mit hoher Priorität nicht durch große Datenmengen mit niedriger Priorität behindert wird. Im Fall einer Überlastung werden Daten mit einer niedrigen Priorität nicht mehr angenommen. Dieses Prinzip wird u. a. von Profinet RT angewendet und heißt dort Quality of Service.

Der Switch kann ein VLAN-Tag gemäß IEEE802.1Q verarbeiten. Dieses Tag besteht aus vier Bytes und steht im Ethernetframe zwischen Quelladressen und Typfeld. Drei Bits dieser vier Bytes stehen für die Priorität. Über das Web-Based Management können verschiedene VLANs pro Port am Switch eingestellt werden. Auf diese Weise lassen sich innerhalb einer Netzwerkstruktur mit derartigen Switches verschiedene VLANs aufbauen. Innerhalb eines physischen Netzwerks können so verschiedene logische Netzwerke geschaffen werden.

Der Switch unterstützt das Spanning Tree Protocol (STP) und das Rapid Spanning Tree Protocol (RSTP). STP ist in der IEEE802.1d beschrieben und ermöglicht die Bildung von Ring- oder Maschenstrukturen in der Topologie eines Netzwerks. Durch die Maschenstruktur können mehrere Verbindungspfade zwischen zwei Geräten bestehen. Um unendliche Schleifen und Broadcast-Fluten zu verhindern, unterbricht der Switch einige der Verbindungen. Im Falle eines Kabelbruchs stellt das Netzwerk nach einer bestimmten Zeit (20 bis 50 s) die Verbindung durch Wiedereinschalten der ausgeschalteten Ports wieder her. Ausgeschaltete Ports können noch Daten empfangen, aber keine mehr senden. Alle eingeschalteten Ports senden Daten.

RSTP ist eine neuere Version des STP und ermöglich Umschaltzeiten von 1 bis 10 s. Auch das RSTP unterstützt Ring- und Maschenstrukturen. Bei der RSTP-Konfiguration kann die RSTP Fast Ring Detection aktiviert werden.

Der SMCS unterstützt das Media Redundancy Protocol (MRP). Damit wird in einer Ringtopologie nach Auftreten eines Fehlers eine Wiederherstellzeit von maximal 200 ms ermöglicht.

Über SNMP (Simple Network Management Protocol) kann das Gerät über das Netzwerk überwacht werden. Ein SNMP-Managementsystem bietet die Möglichkeit, Konfigurationsdaten des Geräts auszulesen, zu diagnostizieren und zu verändern. Es werden die SNMP-Versionen 1 und 2c unterstützt. Die folgenden MIBs werden unterstützt: RFC1213, RMON-MIB, Bridge-MIB, If-MIB, Etherlike MIB, Iana-Address-Family-MIB, IANAifType-MIB,P-Bridge-MIB, Q-Bridge-MIB, SNMPv2-MIB, SNMP-FRAMEWORK-MIB, sowie die eigenen SNMP-Objekte von Phoenix Contact (FL-SWITCH-M-MIB).

Eine seriellen Verbindung mit dem Switch kann über eine V.24-Schnittstelle (RS232) hergestellt werden. Das Kabel wird am COM-Port des PCs und am Switch an einen Mini-DIN-Anschluss angeschlossen. Bei dieser seriellen Verbindung geschieht die Kommunikation über ein Programm, z. B. HyperTerminal. Über diese Schnittstelle können IP-Adresse, Subnetzmaske und Standardgateway eingestellt werden. Das für die automatische Zuweisung einer IP-Adresse verwendete BootP kann ein- oder ausgeschaltet werden. Die Parameter lassen sich über diese Schnittstelle speichern, und es kann ein Neustart des Geräts durchgeführt werden. Auch das Zurücksetzen des Geräts auf die Werkseinstellungen ist möglich.

Eine weitere Schnittstelle bietet das Web-based Management. Diese Schnittstelle bietet Diagnose- und Konfigurationsmöglichkeiten beim Starten und während des Betriebs des Geräts sowie bei Auftreten von Fehlern. Über die Web-based Management lassen sich auch Netzwerk- und Geräteinformationen abfragen. Mit dem Web-based Management lassen sich über eine allseits bekannte Weise (nämlich auf Basis eines Webbrowsers) alle Informationen vom Gerät abfragen. Technische Daten, Installationsdaten, lokale Diagnoseangaben können abgefragt werden. Ferner können alle Konfigurationsparameter (IP-Konfiguration, SNMP-Konfiguration, Softwareupdates, Passwörter) kontrolliert und geändert werden. Unter dem Punkt SSwitch Station"können verschiedene Diagnoseinformationen über die verschiedenen Ports und den Meldekontakt überwacht werden. Jeder Port kann individuell aktiviert oder deaktiviert werden. Für jeden Port können alle Übertragungsparameter angepasst werden, und über das Web-based Management lassen sich statische Informationen über die Daten selbst abfragen. Auch das Port Mirroring"kann aktiviert werden. Mit dieser Funktion ist es möglich, alle Daten, die über einen bestimmten Port versendet oder empfangen werden, auch an einen anderen Port zu schicken. Dies ist wichtig für die Fehlererkennung mithilfe eines Netzwerk-Sniffers.

Der SMCS-Switch ist mit einem steckbaren Konfigurationsspeicher (FL MEM PLUG) ausgestattet.

Einige allgemeine technische Daten:

- Das Gerät wird auf einer DIN-Schiene montiert.
- Die Schutzart ist IP20 (geschützt gegen Fremdkörper mit einer Größe von mehr als 12 mm; kein Schutz vor Wasser); DIN40050, IEC60529.
- Schutzklasse 3 gemäß VDE 0106, IEC60536.
- Stromversorgung: 24 V DC (18,5 V - 30,5 V), Leitungsquerschnitt max. 2,5 $mm^2$.
- Das Gerät kann redundant mit Strom versorgt werden.
- Die Erdung geschieht über die DIN-Schiene, auf der das Gerät montiert ist.
- Stromaufnahme: 600 mA (15 W)
- Abmessungen ohne Konfigurationsspeicher: 128 mm (B) x 110 mm (H) und 69 mm (T); Gewicht 650 g
- Betriebstemperatur: 0 °C bis 55 °C; Lagertemperatur: -40 °C bis 85 °C
- Luftfeuchtigkeit: zwischen 10 und 95 % (kondensationsfrei)
- Luftdruck: im Betrieb 80 bis 108 kPa bei 2000 mu. N.N.; bei Lagerung 70 bis 108 kPa bei 3000p. N.N.

# Kapitel 6

# Der Router

## 6.1 Einleitung

Ein Router ist ein Gerät, der zwei oder mehr verschiedene Computer-Netzwerke miteinander verbindet, z. B. ein Firmennetzwerk mit dem Internet. Abb. 6.1 zeigt, dass ein Router als eine Vermittlungsstelle für Datenpakete gesehen werden kann, die auf Schicht 3 des OSI-Modells arbeitet.

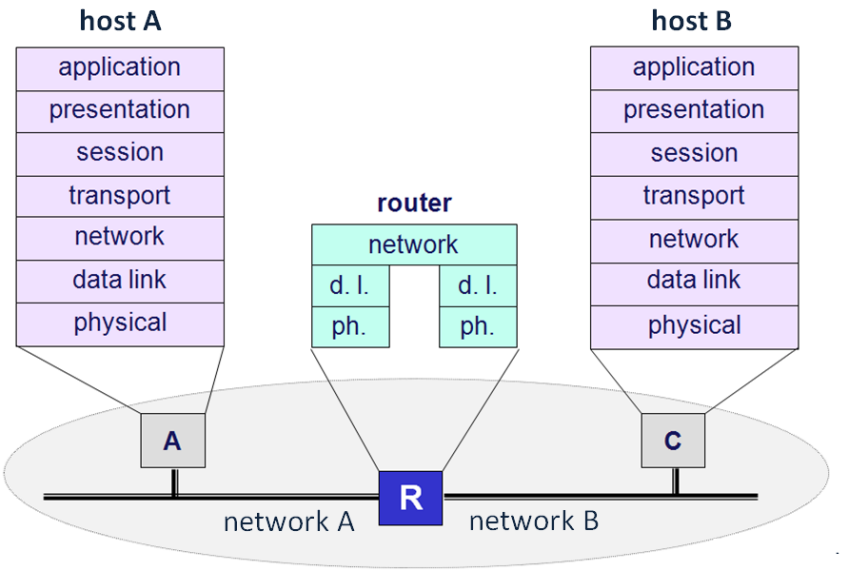


**Abbildung 6.1:** Der Router im OSI-Modell

## 6.2 Das Routen von Nachrichten

Eine Nachricht, die von einem Computer an einen anderen über ein Netzwerk gesendet werden soll, muss von verschiedenen Routern verarbeitet werden. Zunächst schickt ein Sender das IP-Paket an einen ersten Router. Zu diesem Zwecke kapselt der Sender das IP-Paket in einen Frame ein und fügt einen Header hinzu, wie er vom physischen Netzwerk, in dem Sender und Router sich befinden, vorgegeben wird.

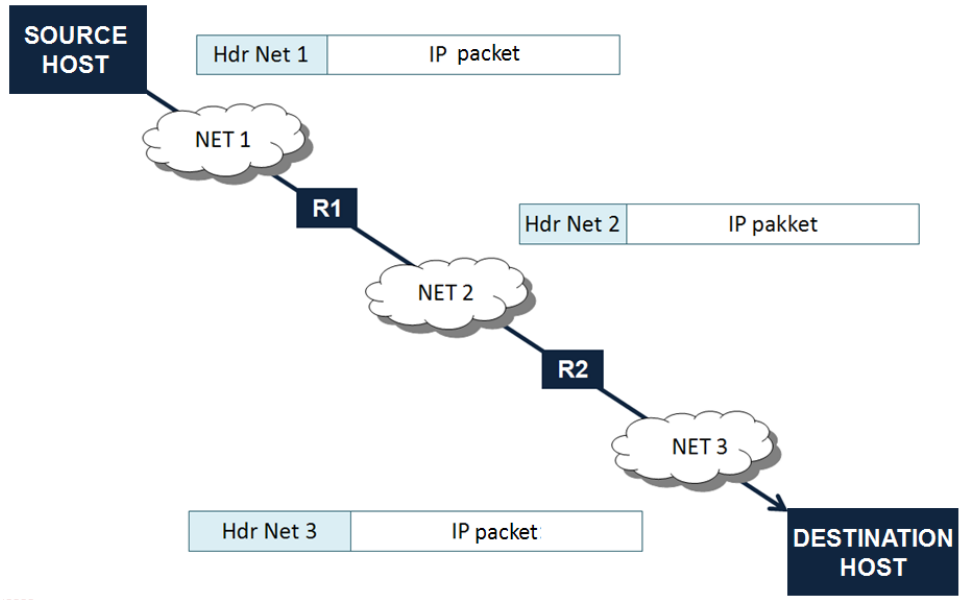


**Abbildung 6.2:** Die verschiedenen Schritte eines IP-Pakets auf der Route in einem Netzwerk

Wenn der Frame den Router erreicht, entnimmt dieser den Inhalt und untersucht das IP-Paket. Der Router benötigt nun die Information, über welchen Port er die Nachricht weitersenden muss. Um den korrekten Ausgangsport zu bestimmen, schlägt der Router die Zieladresse des zu routenden Pakets in der Routing-Tabelle nach. Beim TCP/IP-Protokoll besteht eine Routingtabelle aus einer Tabelle mit IP-Adressen und gruppierten IP-Adressen (Subnetz) und den jeweiligen nächsten Knotenpunkten (Next Hop).

Wenn die Zieladresse in der Routing-Tabelle gefunden wird und daher geroutet werden kann, legt der Router den Ausgangs-Port anhand des so gefundenen Knotenpunkts fest. Das empfangene IP-Paket wird nun an den Ausgangs-Port geschickt. Der Router kapselt dazu das IP-Paket erneut ein und fügt wiederum einen Header hinzu, wie er vom physischen Netzwerk, über das die beiden Router miteinander verbunden sind, vorgegeben wird. Abb. 6.2 zeigt, dass ein IP-Paket immer in einen Frame eingekapselt wird, der zum jeweiligen physischen Netzwerk passt.

Es ist klar, dass ein Router für jeden Port eine IP-Adresse hat, die zum Bereich der Net-ID des Netzes gehört, mit dem der Router verbunden ist. Jeder Port verfügt über eine eigene MAC-Adresse.

Ein Router wird als Ausgabegerät betrachtet. Ein Datenpaket darf normalerweise nur eine durch den TTL-Wert (Time to Live) des Pakets begrenzte Anzahl von Routern passieren, bevor es sein Endziel erreicht.

## 6.3 Routertypen

Es gibt zahlreiche verschiedene Typen von Routern. Sie lassen sich anhand ihrer Form, der Anschlüsse und der gebotenen zusätzlichen Funktionen (z.B. Modem, Firewall oder Switch) unterscheiden.

Ferner lassen sich Software- und Hardwarerouter unterscheiden. Mithilfe spezieller Software kann ein herkömmlicher, mit zwei Netzwerkschnittstellen ausgerüsteter PC als Router eingesetzt werden. Ein Hardwarerouter hingegen ist ein gesondertes Gerät, eigentlich ein kleiner, einfacher Computer, der speziell für das Routing entwickelt wurde.

Kommerzielle Router für den Heimgebrauch sind oft mit einem Switch kombiniert, haben ein Modem und einen Wireless-AP, sodass nur ein einziges Gerät benötigt wird, um ein kleines Heimnetzwerk mit dem Internet zu verbinden.

Auch gibt es Switches mir Router-Funktion auf dem Markt. Für diese Geräte wird häufig der Name Layer-3-Switch"benutzt.

Im weiteren Verlauf dieses Kapitels liegt der Schwerpunkt auf industriellen Routern. In seiner einfachsten Form weist ein solcher Router eine LAN- und eine WAN-Schnittstelle auf. Hiermit kann ein industrielles Netzwerk mit einem Firmennetzwerk oder dem Internet verbunden werden. Industrielle Router können auch optional eine Firewall enthalten, damit sie als vollwertiges Sicherheitsmodul für die Kopplung von industriellen an Firmennetzwerke eingesetzt werden können.

## 6.4 Layer-3-Switch

Wie bereits dargestellt arbeiten Switches auf Schicht 2 des OSI-Modells, während Router auf Schicht 3 arbeiten. Ein Layer-3-Switch hingegen ist ein leistungsfähiges Gerät für das Routing im Netzwerk.

Layer-3-Switches unterscheiden sich nur wenig von gewöhnlichen Netzwerkroutern. Beide verarbeiten eingehende Pakete und entscheiden anhand der in diesen genannten Adressen dynamisch über die Weiterleitung dieser Pakete (Routing). Ihren Ursprung haben sie in der Nachfrage nach Routern, die sich leicht in umfangreichen Netzwerken, z. B. Firmenintranets, einsetzen lassen.

Der wesentlichste Unterschied zwischen einem Layer-3-Switch und einem gewöhnlichen Router ist der Aufbau der Hardware. Bei einem Layer-3-Switch wird die Hardware eines Switches mit der eines Routers kombiniert, um so eine bessere Leistung beim Routing in großen LAN-Infrastrukturen zu gewährleisten. Die typischerweise für Intranets verwendeten Layer-3-Switches haben üblicherweise keine WAN-Ports und unterstützen in der Regel auch keine typischen WAN-Anwendungen.

## 6.5 Verbindung eines privaten Netzwerks mit dem Internet

Ein Automationsnetzwerk kann mit einem industriellen Router mit einem Firmennetzwerk oder dem Internet verbunden werden. Für das Ethernet-basierte Automationsnetzwerk muss eine Net-ID gewählt werden, die vorzugsweise der RFC 1597 entspricht.

Abb. 6.3 zeigt ein Beispiel. Der Router erhält auf der LAN-Seite eine IP-Adresse, die zum Adressraum der gewählten Net-ID gehört. In der Regel ist dies die erste oder letzte freie IP-Adresse des Netzwerks. Das Netzwerk-Interface hat andererseits auf der LAN-Seite auch eine MAC-Adresse. Der Router fungiert im Netzwerk als Standardgateway.

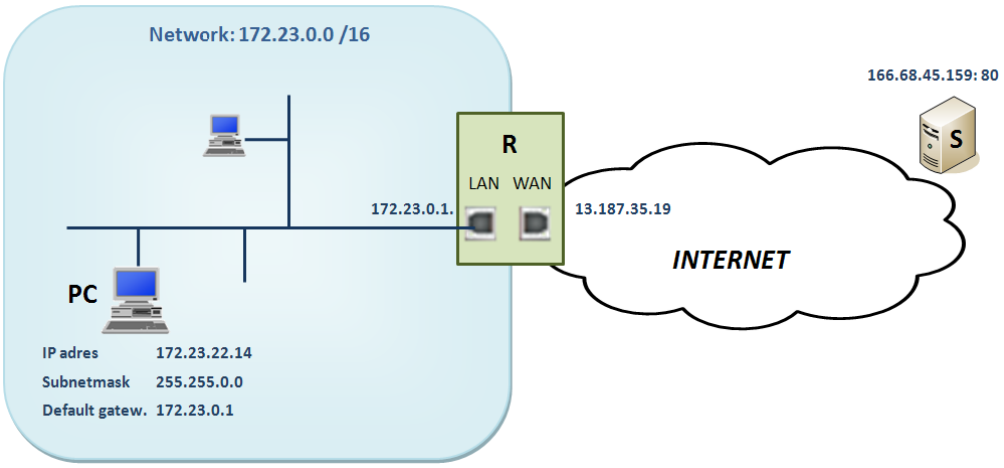


**Abbildung 6.3:** Verbindung eines privaten Netzwerks mit dem Internet über einen Router

Über die WAN-Schnittstelle des Routers kann das Netzwerk mit dem Internet verbunden werden. Hierfür bekommt der Router, üblicherweise über DHCP, vom ISP (Internet Service Provider) eine eindeutige IP-Adresse im Internet zugewiesen.

Jedes Gerät im Netzwerk kann nun wie folgt konfiguriert werden:

| | |
|---|---|
| IP-Adresse | 172.23.22.14 |
| Subnetzmaske | 255.255.0.0 |
| Standardgateway | 172.23.0.1 |

Hierbei bekommt jeder Teilnehmer eine IP-Adresse, wobei die Net-ID für alle Teilnehmer gleich, aber die Host-ID für jeden Teilnehmer unterschiedlich ist.

Wenn eine auf einem PC im Netzwerk laufende Anwendung die Kommunikation mit einem Server im Internet aufnehmen möchte, muss der PC zunächst ein IP-Paket erstellen, um die Verbindung anzufordern. Dieses IP-Paket wird über das Standardgateway in das Internet geschickt. Zu diesem Zweck kapselt der PC das IP-Paket in einen Ethernetframe ein. Abb. 6.4 zeigt die für die Erstellung des Ethernetframes benötigten Daten. Die MAC-Adresse des Routers wird über das ARP-Protokoll erfragt.

Sobald der ARP-Reply beim Router angekommen ist, schickt dieser das IP-Paket über die WAN-Schnittstelle zu einem anderen Router im Internet weiter. Da das private Netzwerk vom Internet getrennt ist, ersetzt der Router die Quell-IP-Adresse des PCs durch seine eigene Adresse auf der WAN-Seite. Das private Netzwerk ist ausschließlich über diese externe IP-Adresse des Routers über das Internet erreichbar.

Der Server kann nun eine Antwort an die externe IP-Adresse des Routers schicken. Der Router steht nun vor der Aufgabe zu ermitteln, an welchen PC diese Antwort weitergeschickt werden muss. In der Antwort des Servers stehen Angaben über den ursprünglichen Absender. Zur Lösung dieses Problems wurde IP-NAT entwickelt.

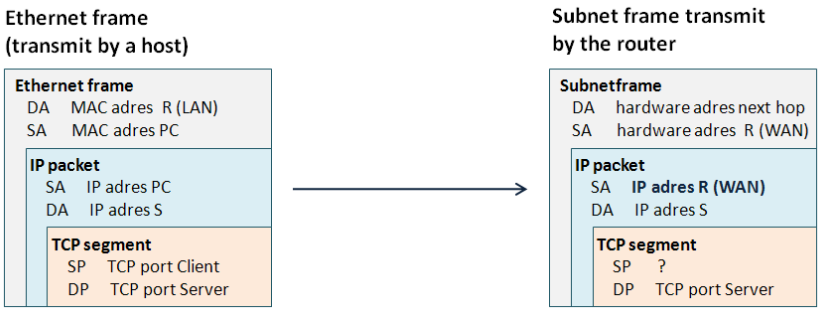


**Abbildung 6.4:** Verbindung eines privaten Netzwerks mit dem Internet über einen Router

## 6.6 IP-NAT

### 6.6.1 NAT: IP-Maskierung

Network Address Translation (NAT) ist ein Protokoll, mit dem Netzwerke mit unregistrierten IP-Adressen (private Netzwerke, die RFC 1597 entsprechen) mit dem Internet verbunden werden können. Wie weiter oben beschrieben vermerkt der Router in jeder Nachricht, die aus dem privaten Netzwerk in das Internet geschickt wird, stets seine externe IP-Adresse als Quell-Adresse. Konsequenterweise richten sich alle Antworten nun an die externe IP-Adresse des Routers.

Das NAT-Protokoll ermöglicht es dem Router, das TCP-Source-Port-Feld zu ändern. In einer NAT-Tabelle werden alle neuen Portnummern einem internen Endpunkt zugeordnet. Jede Antwort, die aus dem Internet an einen PC im privaten Netzwerk gerichtet ist, geht an die externe IP-Adresse des Routers, enthält aber als TCP-Destination-Port eine Portnummer aus der NAT-Tabelle des Routers. Auf diese Weise weiß der Router, für welchen Endpunkt die jeweilige Nachricht bestimmt ist.

Praktisch gesehen ist NAT ein Protokoll, das eine IP-Adresse des einen Netzwerks in eine in einem anderen Netzwerk gültige IP-Adresse übersetzt. Das eine Netzwerk wird *Inside* genannt, das andere *Outside*. Typischerweise übersetzt ein Betrieb seine lokalen Inside-IP-Adressen in eine oder mehrere globale Outside-IP-Adressen, und die globalen IP-Adressen eingehender Nachrichten umgekehrt wieder in Inside-IP-Adressen. NAT macht es also möglich, dass ein Betrieb lediglich eine einzige globale IP-Adresse für seine Kommunikation mit der Außenwelt, dem Internet verwendet. Dies trägt zum Sicherheitskonzept bei, da alle aus- und eingehenden Nachrichten einer Adressübersetzung unterworfen sind.

Abb. 6.5 zeigt die Arbeitsweise des NAT-Protokolls. Hier wird das NAT-Protokoll dynamisch eingesetzt. Diese Verwendung heißt auch dynamisches NAT.

### 6.6.2 Port Forwarding

Der statische Gebrauch des NAT-Protokolls ist unter dem Namen Port-Weiterleitung oder Port Forwarding bekannt. Wenn im privaten Netzwerk Server vorhanden sind, die direkt aus dem Internet erreichbar sein müssen, können den Endpunkten dieser Server statisch Portnummern in der NAT-Tabelle des Routers zugeordnet werden. Um diese Server aus dem Internet

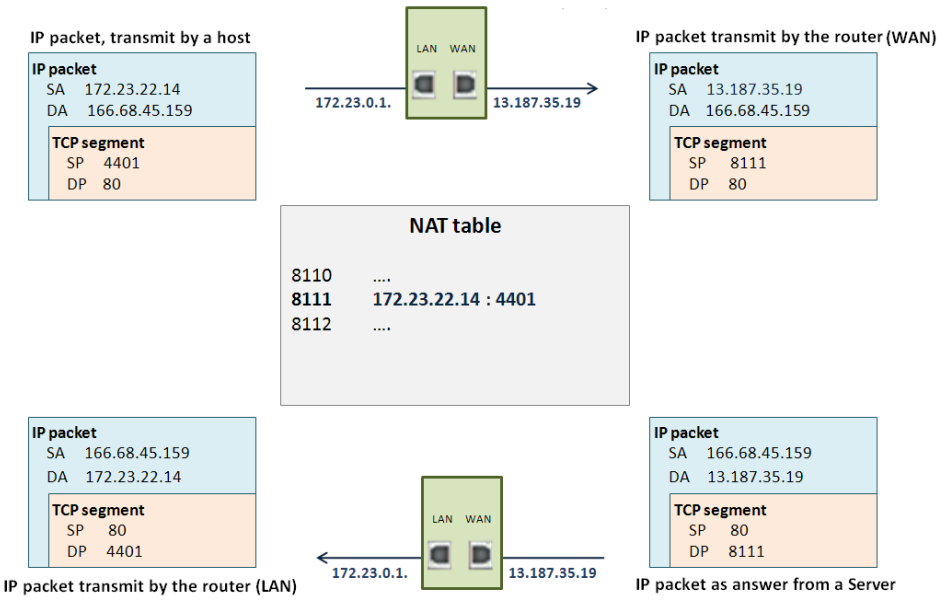


**Abbildung 6.5:** Funktionsweise des NAT-Protokolls: auf einem PC mit der IP-Adresse 172.23.22.14 wird Befehl *http://166.68.45.159: 80* gegeben

zu erreichen, muss als Endpunkt die externe IP-Adresse des Routers mit der Portnummer aus der NAT-Tabelle verbunden werden. Der Router übersetzt bei für den speziellen Server eingehenden Nachrichten den Endpunkt in den korrekten Endpunkt des Servers. Dies ist eine zusätzliche Form der Sicherheit. Die exakten IP-Daten des Servers müssen nicht veröffentlicht werden, und eventuelle Hacker erfahren nichts über die Architektur des Netzwerks, in dem sich die Server befinden. Abb. 6.6 zeigt die Konfiguration für das Port Forwarding oder Port-Weiterleitung.

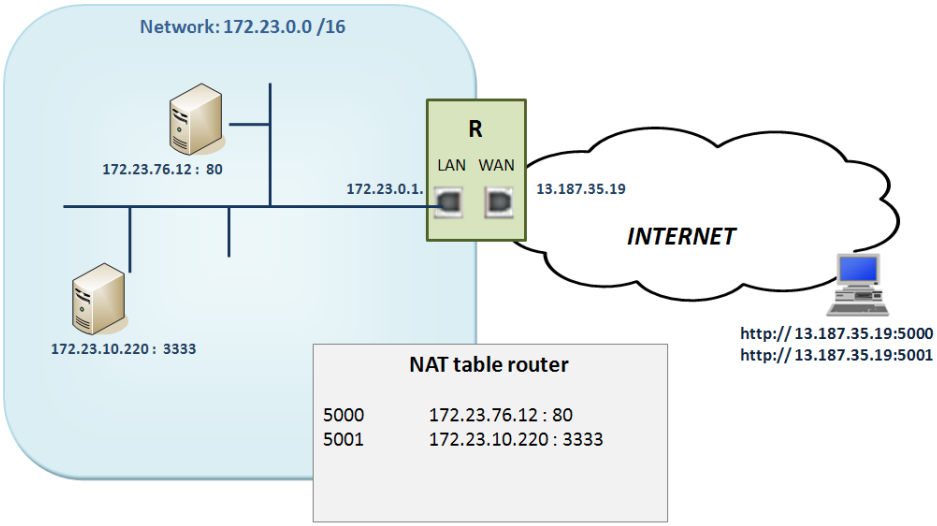


**Abbildung 6.6:** Port Forwarding

## 6.7 1:1-NAT

Beim 1:1-NAT wird eine IP-Adresse in eine andere übersetzt, ohne dabei die verwendeten TCP/UDP-Ports zu ändern.

Wenn ein Router auf der LAN-Seite mit dem Netzwerk 192.168.1.0/24 sowie über den WAN-Port mit dem Netzwerk 10.1.0.0/16 verbunden ist und als externe IP-Adresse 10.1.1.0/16 hat, dann ist mit Hilfe des 1:1-NAT der LAN-Teilnehmer mit der IP-Adresse 192.168.1.100 auf der WAN-Seite über die IP-Adresse 10.1.1.100 erreichbar.

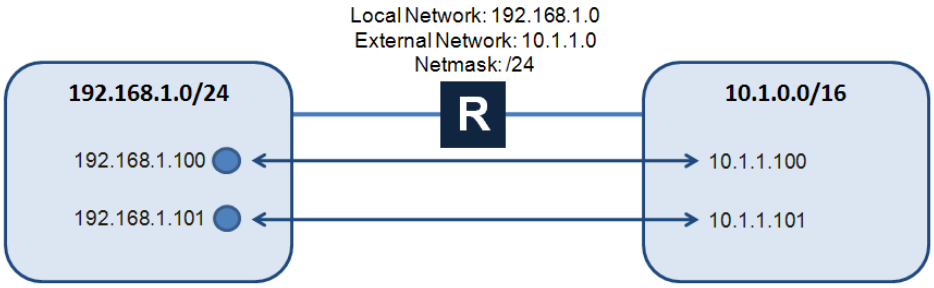


**Abbildung 6.7:** Mapping der IP-Adressen beim 1:1-NAT

1:1-NAT bietet interessante Möglichkeiten für die Automationswelt:

- Verschiedene Subnetze können miteinander verbunden werden, wobei in allen Subnetzen dieselbe IP-Adressierung verwendet wird.
- Es müssen keine zusätzlichen Routen im Firmennetzwerk definiert werden.

- Ein ARP-Dämon auf dem mGuard verarbeitet die ARP-Request aus dem externen Netzwerk.
- Systeme in Subnetzen können durch das IP-Mapping direkt aus dem Firmennetzwerk angesprochen werden. Bei diesem Mapping wird die Host-ID beibehalten, nur die Net-ID wird angepasst.

Abb. 6.8 zeigt die Funktionsweise von 1:1-NAT.

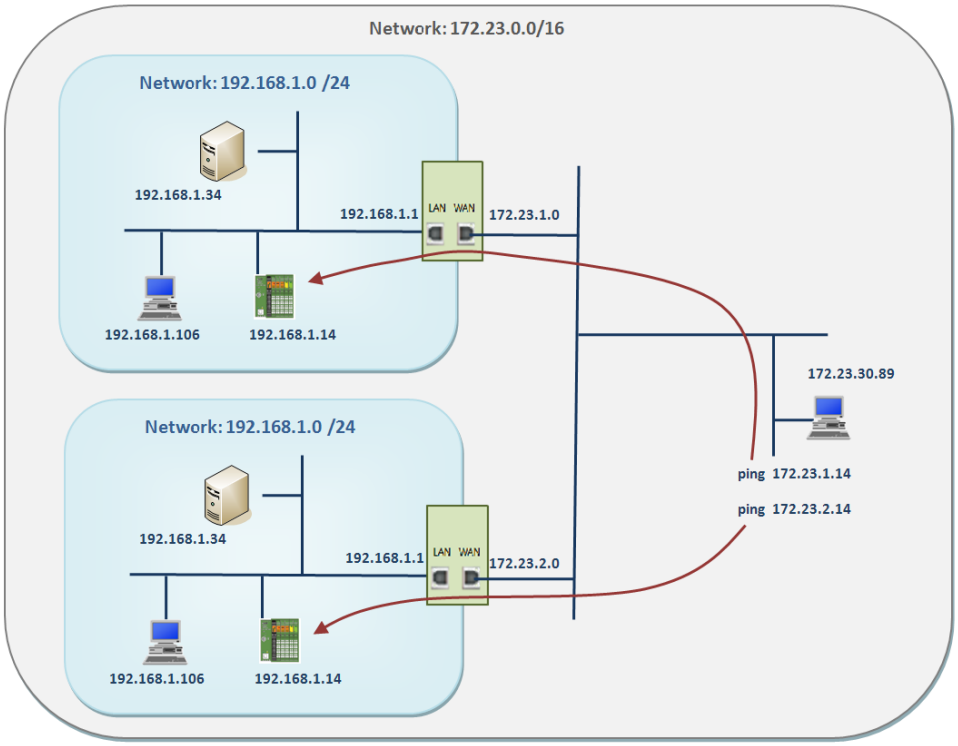


**Abbildung 6.8:** Prinzip des 1:1-NAT

# Kapitel 7

# Die Firewall

## 7.1 Einleitung

Eine Firewall ist eine Anwendung, die den Datenzugang zum Netzwerk regelt. Er unterbindet jeglichen Datenverkehr mit Ausnahme desjenigen, der ausdrücklich zugelassen ist.

Bisweilen werden Firewall und Router miteinander verwechselt, obwohl sie grundlegend verschieden sind. Ein Router ist ein Netzwerkstrukturelement, das dazu dient, Daten so schnell und effizient wie möglich durchzuleiten, es ist sicher nicht seine Aufgabe, Datenverkehr zu blockieren.

Die Verwendung von Firewalls ist nicht auf Internetverbindungen beschränkt. Sie können auch innerhalb von kleineren Netzwerken eingesetzt werden, um verschiedene Bereiche gesondert zu sichern. Firewalls können in der Regel auch so konfiguriert werden, dass sie allen Verkehr in einem Logbuch aufzeichnen und zentralisierte Managementfunktionen ausführen.

## 7.2 Firewall-Typen

Es gibt zwei Arten von Firewalls: Hard- und Softwarefirewalls. Eine Softwarefirewall ist ein Software-Programm, das auf einem Computer installiert wird. Eine Hardwarefirewall ist ein gesondertes Gerät, z. B. ein Router mit integrierter Firewall. Beide Arten von Firewalls arbeiten auf die gleiche Weise. Die verwendete Terminologie ist bei beiden identisch.

Ferner können Firewalls anhand ihrer Funktionsweise unterschieden werden. Unterscheidungskriterium ist dabei die Art und Weise, wie entschieden wird, ob Daten durchgelassen werden oder nicht.

- Paketfilter: Die Firewall bestimmt anhand einiger Regeln, ob ein IP-Paket durchgelassen werden soll oder nicht. Solche Regeln werden anhand von IP-Adressen, Domainnamen, Protokolle (http, ftp, telnet etc.) und Portnummern aufgestellt. Diese Art von Firewalls arbeitet einfach und schnell. Der Paketfilter arbeitet im Grunde wie ein Pförtner: Er überprüft passierende Nachrichten eher oberflächlich: Sind es eingehende (*inbound*), ausgehende (*outbound*) oder passierende (*route*) Nachrichten? Es wird die angegebene, aber leicht zu fälschende (Spoofing) Herkunft und Bestimmung (IP-Adresse und Portnummer) kontrolliert. In der Transportschicht werden die Angaben über Typ und Art der Nachricht kontrolliert. Der eigentliche Inhalt der Nachricht wird jedoch nicht betrachtet.

Paketfilter werden als *stateless* bezeichnet: Sie überprüfen Herkunft und Ziel, sind jedoch nicht in der Lage, verdächtige Muster in einer bestimmten Sitzung zu erkennen. So merkt er z. B. nicht, wenn plötzlich verdächtig viele Datenpakete zwischen bestimmten Anwendung ausgetauscht werden.

- Stateful Inspection: Neben den verschiedenen Regeln für die Paketfilterung kann eine solche Firewall zwischenzeitlich Informationen über den Zustand aller über die Firewall laufenden Verbindungen registrieren. Stateful Packet Inspection (SPI) bedeutet, dass der Inhalt jedes Pakets ab der Anmeldung und des darauf folgenden Handshaking zwischen den kommunizierenden Hosts untersucht wird. Die Stateful Inspection kann so während der gesamten Sitzung überprüfen, was gemäß der Verbindungsanfrage zulässig ist. Zunächst wird wie bei einem Stateless-Paketfilter überprüft, ob die Verbindung zwischen Quelle und Ziel generell zulässig ist. Ist dies nicht der Fall, wird die Synchronisationsanfrage verworfen. Ist die Verbindung zulässig, werden die Informationen aus dem ersten Datagramm, welches die Sitzung aufbaut (SYN) während der Sitzung in einer Zustandstabelle gespeichert. Falls im Zusammenhang mit der Verbindung etwas Unerwartetes geschieht (Host verändert plötzlich seine IP-Adresse oder den Zielport), so wird die Sitzung unterbrochen.

Die meisten aktuellen Firewalls sind Stateful-Inspection-Firewalls.

# Kapitel 8

# VPN

## 8.1 Einleitung

Datenpakete werden in der Regel vollständig ungeschützt über das Internet gesendet. Dadurch gibt es:

- keine Geheimhaltung der Daten (Verschlüsselung),
- keine Identitätsgarantie des Absenders (Authentifizierung), und
- keine Überprüfung, ob die Daten korrupt sind (Integrität).

Ein Virtual Private Network (VPN) ist ein privater Kommunikationskanal, der auf die öffentliche Infrastruktur (in der Regel das Internet) aufgesetzt ist. Die zu versendenden Daten werden über diesen Dienst so gesichert, dass die Integrität, Autorisierung und Authentizität gewährleistet bleibt. Der Endanwender merkt im Prinzip nicht, dass ein VPN eingesetzt wird. Dieser Dienst wird von verschiedenen Protokollen verfügbar gemacht.

## 8.2 Internet Protocol Security, IPsec

IPsec (Internet Protocol Security) ist das verbreitetste VPN-Protokoll. Es ermöglicht die Verschlüsselung von Daten, die zwischen zwei Kommunikationspartnern ausgetauscht werden. IPsec kann transparent in einer Netzwerkinfrastruktur implementiert werden. Es handelt sich bei IPsec um eine Protokoll-Suite, die dafür sorgt, dass IP-Pakete sicher über ein IP-Netzwerk versendet werden können. Internetnutzer können mit IPsec Daten auf eine sichere Weise versenden. Die Protokoll-Suite stellt dafür die folgenden Dienste zur Verfügung, die während des Sendens eines IP-Datenpakets aktiv sind:

- Integrität: Das Protokoll gewährleistet, dass das gesendete Paket während des Transports nicht von Dritten verändert wird.
- Authentifizierung: Das Protokoll legt die Identität der Kommunikationspartner fest. Beim gesicherten Datentransport muss gewährleistet werden, dass das Datenpaket tatsächlich den vorgesehenen Empfänger erreicht.
- Empfangsbestätigung: Das Protokoll weist nach, dass der Empfänger die Daten empfangen hat.

- Vertraulichkeit: Das Protokoll sorgt für den tatsächlichen Schutz der Daten und gewährleistet dem Absender, dass ausschließlich der Empfänger die Nachricht lesen kann.

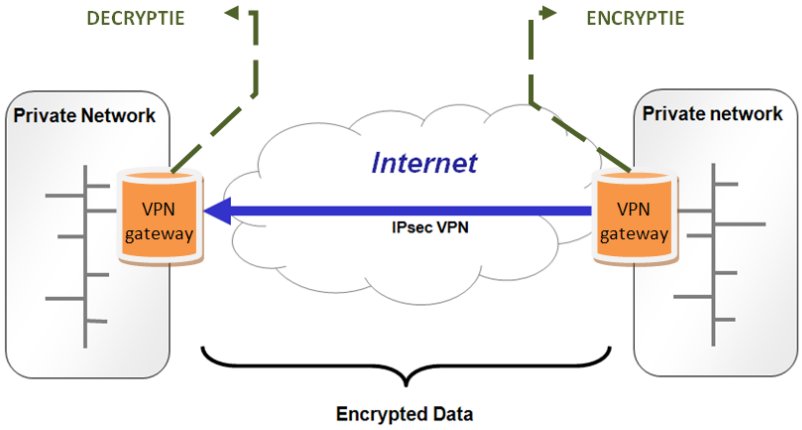


**Abbildung 8.1:** Verschlüsselte Datenübertragung

Das Protokoll wird vor allem für den Versand von Informationen über öffentliche Verbindungen eingesetzt und verhindert sogenannte *Man-in-the-Middle-Angriffe* (auch *Janusangriffe* genannt) und *Spoofing*. Zu diesem Zweck verwendet es das sogenannte IKE-Protokoll (Internet Key Exchange), mit dem die Parteien identifiziert werden, die eine Verbindung aufbauen wollen. Danach wird eine Verbindung aufgebaut und die zu versendenden Daten verschlüsselt.

Verschlüsselung wird bei zahlreichen Protokollen verwendet, um eine Geheimhaltung der Daten zu gewährleisten. Bei der Verschlüsselung werden die Daten in eine unlesbare Form, den sogenannten Schlüsseltext übertragen. Mit Hilfe eines Schlüssels kann der Empfänger dann die Umkehrtransformation (Entschlüsselung) durchführen, wodurch der Text wieder in lesbaren Klartext umgewandelt wird. Die leistungsfähigsten Verschlüsselungstechniken heutzutage sind 3DES und AES. Dabei ist AES aufgrund seiner stärkeren Verschlüsselung gegenüber 3DES vorzuziehen.

IPsec unterstützt den Schutz ab der dritten Schicht des OSI-Modells, also der Vermittlungsschicht. Hierdurch können TCP und UDP verwendet werden, es besteht aber noch genügend Spielraum z. B. für SSL, das auf höheren OSI-Ebenen arbeitet (und UDP nicht schützen kann). Der Standard wurde durch die IETF in den RFCs 2401-2412 festgelegt, und zwar optional für IPv4 und obligatorisch für IPv6.

Das Protokoll ist wie folgt aufgebaut:

- Authentication Header (AH): Prüfsumme für das gesamte IP-Paket.
- Encapsulating Security Payload (ESP): schützt vor Man-in-the-Middle-Angriffen.
- IP Payload Compression (IPcomp): Kompression der Nutzdaten des IP-Pakets vor der Verschlüsselung.
- Internet Key Exchange (IKE): unterstützt beim Verbindungsaufbau durch sichere Übertragung der Schlüssel/Zertifikate.

IPsec gibt es in zwei Varianten:

- Transport: Dabei werden die Nutzdaten (Payload) des IP-Pakets verschlüsselt, nicht jedoch der Header. In diesem Modus muss kein neues IP-Paket erstellt werden, sondern die Header (AH, ESP, oder beide) in das IP-Paket integriert. Quell- und Zieladressen bleiben unverändert.
- Tunnel: In diesem Modus werden sowohl der Inhalt des IP-Pakets als auch der Header verschlüsselt. Das komplette IP-Paket wird dabei in ein ganz neues IP-Paket verpackt. Quell- und Zieladresse dieses IP-Pakets ist der Start- bzw. Endpunkt des Tunnels.

## 8.3 VPN: Implementierungen

VPN kann auf drei verschiedene Arten implementiert werden:

1. Security-Gateway-to-Security-Gateway


**Abbildung 8.2:** Security-Gateway-to-Security-Gateway

2. Host-to-Security-Gateway


**Abbildung 8.3:** Host-to-Security-Gateway

3. Host-to-Host-Gateway


**Abbildung 8.4:** Host-to-Host-Gateway

# Kapitel 9

# Automationsnetzwerke & Sicherheit

## 9.1 Firmennetzwerk

Ein Firmennetzwerk ist die Gesamtheit von Servern, Computern und Systemen allgemein, die das Funktionieren des Betriebs auf IT-Ebene zu ermöglichen. Ethernet-TCP/IP ist schon seit Jahren der Standard für den Aufbau von IT-Netzwerken in Büros und Betrieben. Ein Firmennetzwerk ist in seiner einfachsten Form über einen Router und eine Firewall mit dem Internet verbunden. Größere Firmennetzwerke weisen zusätzlich eine DMZ auf. Dabei handelt es sich um einen Teil des Netzwerks, in den öffentliche Server stehen (Mailserver, Webserver, DNS-Server etc.)

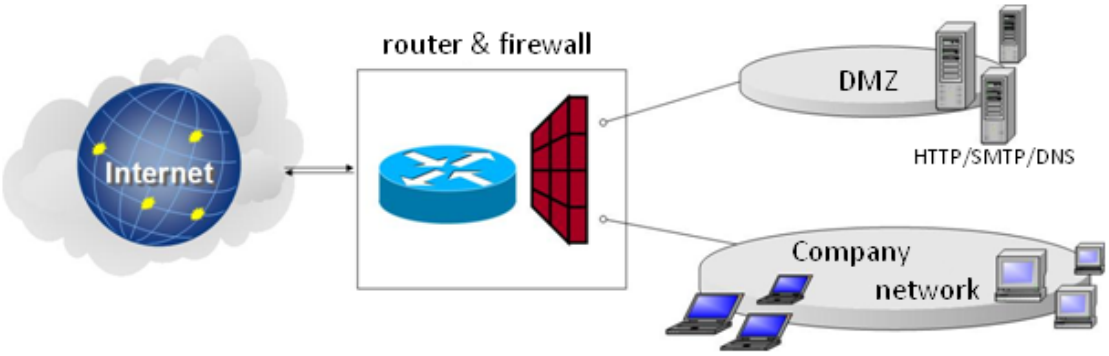


**Abbildung 9.1:** Firmennetzwerk

Ein Router ist in seiner einfachsten Form ein Gerät, das die Kommunikation zwischen zwei Netzwerken ermöglicht, in diesem konkreten Fall das Firmennetzwerk auf der einen Seite (LAN), das Internet auf der anderen Seite (WAN). Firewalls werden verwendet, um unerwünschte Kommunikation zu unterbinden. Dabei werden IP-Pakete gemäß vom Anwender festgelegter Regeln gefiltert. Dabei kann sowohl ein- als auch ausgehende Kommunikation blockiert werden. Die Filterkriterien können IP-Adressen, Portnummern oder bestimmte Protokolle sein, die jeweils blockiert oder freigegeben werden können.

## 9.2 Automationsnetzwerke

### 9.2.1 Automationszelle

Eine Automationszelle ist die Gesamtheit von PCs, Datenservern, Controllern, Ein-/Ausgabegeräte, Sensoren und Aktoren, die nötig sind, um die verschiedenen Funktionalitäten eines Automationskonzepts auszuführen.

Ein Automationsprojekt ist die Summe von

- Produktionslinien und Prozessanlagen
- SPS-Systemen (Speicherprogrammierbare Steuerungen)
- ESD-Systemen (Emergency Shut Down and Safety Controllers)
- DCS-Systemen (Process and distributed Control Systems)
- SCADA-Systemen (Supervisory Control and Data Acquisition)

Switches sind diejenigen Strukturelemente, mit denen eine vollständige Automationszelle weiter ausgebaut wird. Durch die Kombination verschiedener Topologien und Medien wird ein flexibles, sicheres und beherrschbares Netzwerk auf Grundlage von Ethernet-TCP/IP im industriellen Arbeitsbereich aufgebaut.

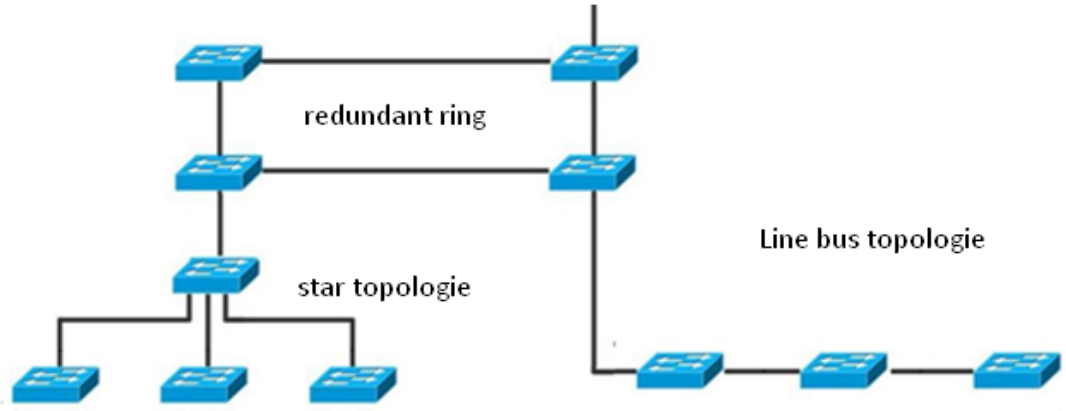


**Abbildung 9.2:** Verschiedene Topologien in einer Automationszelle

Wichtige Segmente werden über Switches in einem redundanten Ring miteinander verbunden. In bestimmten Teilsegmenten werden Netzwerkteilnehmer sternförmig über Switches miteinander verbunden (so wie im normalen IT-Netzwerken). Womöglich wird eine Busstruktur verwendet, um Teilnehmer miteinander zu verbinden. Dazu ist es notwendig, dass alle Ein-/Ausgabegeräte standardmäßig mit einem integrierten Switch ausgestattet sind.

### 9.2.2 Automationsnetzwerk

Ein Automationsnetzwerk besteht aus einer oder mehrerer Automationszellen. Jede Zelle ist dabei durch einen Router abgetrennt.

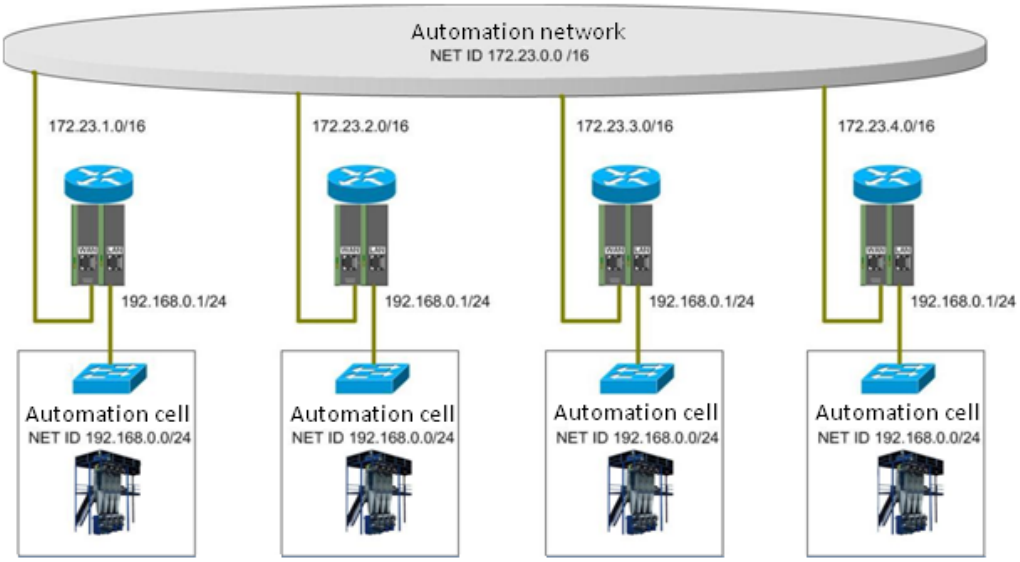


**Abbildung 9.3:** Automationsnetzwerk

### Verkabelung und Anschlüsse in einem Automationsnetzwerk

Aufbau und Verkabelung, wie sie aus der Büroumgebung bekannt sind, lassen sich nicht uneingeschränkt in rauen industriellen Umgebungen anwenden.

Kabel, Anschlüsse und Infrastrukturelemente müssen auf die Fertigungsumgebung abgestimmt sein, in denen Belastungen wie Feuchtigkeit, große Temperaturunterschiede, Stöße oder Vibrationen auftreten können. Diese Teile, Stecker und Kabel, müssen den Qualitätsanforderungen der Industrie genügen. Dies ist der erste Schritt zu einem zuverlässigen Automationsnetzwerk.

Es ist wichtig, dass alle Ethernet-Kabel auf eine einfache Weise vor Ort konfiguriert werden können. Es wird empfohlen, zunächst die Verkabelung auszuführen, und erst im Anschluss die Ethernet-Stecker anzubringen.

### Einsatz von Switches

Als Strukturelemente werden ausschließlich Switches verwendet. Der Aufbau des Netzwerks ist entscheidend, um die Netzwerkbelastung zu optimieren. Diese darf nicht mehr als 60% der gesamten Netzwerkkapazität betragen.

Für den Aufbau einer redundanten Ringstruktur müssen die Switches RSTP unterstützen. Ferner müssen die Switches innerhalb der verschiedenen Automationszellen für die Verwaltung und Diagnose des Netzwerks folgende Protokolle unterstützen:

- Web-based Management für eine schnelle und klare Konfiguration
- SNMP für die Gerätediagnose
- LLDP für die Kontrolle und Diagnose der Netzwerktopologie

- VLAN für eine strukturierte Aufteilung des Netzwerks

Switches müssen die Möglichkeit bieten, bei verschiedenen Ereignissen SNMP-Traps zusenden oder einen Meldekontakt einzuschalten. Für die einfache Konfiguration neuer Geräte wird ein steckbarer Konfigurationsspeicher verwendet. Ein weiterer wichtiger Schritt auf dem Weg zu einem sicheren Netzwerk ist die Verwendung von VLAN.

### 9.2.3 Verwendung eines Automationsnetzwerks mit einem Firmennetzwerk

Die Verwendung eines Automationsnetzwerks mit dem Firmennetzwerk geschieht mit Hilfe eines Routers. Dieser Router sorgt für die ideale Trennung zwischen den beiden Netzwerken, die völlig verschiedene Anforderungen aufweisen. Dieser Router muss eine offene, aber dennoch stark gesicherte Kommunikationsstruktur zwischen dem Firmennetzwerk und dem Automationsnetzwerk ermöglichen.

## 9.3 Sicherheitsbedarf

### 9.3.1 Einleitung

Automationsnetzwerke sind auch heute noch in der Regel isolierte Netzwerke mit Controllern und auf proprietären Protokollen basierenden Netzwerkprotokollen. In der Regel ist die Fertigungsabteilung selbst verantwortlich für die industrielle Kommunikation. Sicherheit spielt dabei selten eine Rolle.

Moderne Automationsprojekte sind durch offene Systeme und Kommunikationsnetzwerke gekennzeichnet, die auf Ethernet-TCP/IP basieren. Hierdurch wird die IT-Abteilung mitverantwortlich für die industrielle Kommunikation, und Sicherheit wird zu einem wichtigen Thema.

Die Eroberung der Produktionshallen durch Windows und Ethernet ist eine interessante Entwicklung. In zunehmendem Maße wird jedoch auch klar, dass nun auch Viren und Hacker Zugriff auf Maschinenparks und industrielle Anlagen erhalten. Es wird daher immer wichtiger, die Automationswelt gegen die in der IT-Welt seit langem bekannten Gefahren zu schützen.

### 9.3.2 Bewusstsein schaffen

Das Bewusstsein, Büronetzwerke schützen zu müssen, ist bereits heute vorhanden. Auch bestehen entsprechende Kenntnisse. Die Platzierung einer Firewall zwischen dem Büronetzwerk und dem Internet ist zum Standard geworden, ebenso die Anwendung einiger zusätzlicher Sicherungsmaßnahmen. Damit sind Büronetzwerke gut geschützt.

Auf Ebene der Produktion sind dieses Bewusstsein und die entsprechenden Kenntnisse noch nicht im gleichen Maß vorhanden. Die folgenden Fragen drängen sich auf:

- Ist die IT der Produktion so anfällig, dass ein Schutz nötig ist?
- Wenn das Firmennetzwerk gut geschützt ist, kann doch eigentlich nichts schiefgehen?
- Welche nicht autorisierte Person interessiert sich schon für das Hacken der Produktionsmaschinen und das Stilllegen der Fabrik?

- Außerdem laufen doch auf den Systemen der industriellen IT ganz andere Protokolle als die bekannten Microsoft-Protokolle. Sind dadurch nicht die Produktionsnetzwerke weniger empfindlich gegenüber Angriffen aus der Außenwelt?

Der letzte Punkt traf früher zu, doch gibt es eine Weiterentwicklung hin zum Gebrauch offener Systeme, zum Beispiel Windows-basierte Software-Anwendungen und Protokolle wie HTTP, FTP, DCOM (wird in OPC verwendet) bis auf SPS-Ebene. Diese offenen Systeme sind empfindlich gegenüber Angriffen durch Viren und können die SPS blockieren.

Die Probleme in der industriellen Produktionsumgebung konzentrieren sich jedoch nicht nur auf die Gefahr durch Hacker. Noch wichtiger sind zufällige Fehler innerhalb der Produktion, zum Beispiel Kabel, die herausgezogen oder falsch eingesteckt werden. Wird ein USB-Stick, der einen Virus enthält, in einen mit einer Maschine verbundenen PC gesteckt, so kann dies zum Produktionsstillstand führen. Datenverkehr aus dem Büronetzwerk kann zu Verzögerungen im Produktionsnetzwerk führen.

Andererseits kann nicht ausgeschlossen werden, dass *gehackte* Daten missbraucht werden. Der Betrieb kann erpresst werden. Neuere Untersuchungen deuten auf eine Evolution auf dem Gebiet der Sicherheitszwischenfälle in der Industrie hin. Zusätzlich zu den eher zufälligen Ereignissen kommen immer mehr externe Zwischenfälle wie Viren, Trojaner, Hacker, Sabotage etc. . Hacker kennen sich immer besser mit Steuersystemen und SCADA-Anwendungen aus. Ihre Motivation ist heutzutage immer weniger der Spaß, sondern immer mehr das organisierte Verbrechen, um einen bestimmten Betrieb zu erpressen.

Schützen wird zu einem *Muss*.

### 9.3.3 Sicherheitsaufgaben

Es gibt drei Hauptziele der Sicherheit:

- Zuverlässigkeit (Vertraulichkeit): die Sicherheit, dass Dritte nicht an Daten kommen.
- Korrektheit der Daten (Integrität): Schutz der Daten vor unerwünschten Änderungen und Löschung.
- Verfügbarkeit (Availability): Ressourcen müssen verfügbar sein und zum richtigen Zeitpunkt korrekt funktionieren.

Sicherheit ist also: verhindern, dass jemand unberechtigten Zugang zum System erhält; dafür sorgen, dass das System zu jeder Zeit normal funktioniert, und gewährleisten, dass alle Daten im System auf eine zuverlässige Weise bearbeitet werden können.

### 9.3.4 Sicherheit in der Bürowelt gegenüber der in der Automationswelt

#### Einleitung

Durch die Integration offener Systeme kann der Eindruck entstehen, dass die Sicherheitsprobleme in der Produktionswelt auf dieselbe Weise gelöst werden können wie in der Bürowelt. Es gibt jedoch einige bedeutsame Unterschiede zwischen den beiden Bereichen: Die IT im Büro ist nicht dieselbe wie in der Produktion. Es muss überprüft werden, welche Elemente der Büro-IT in der Produktion verwendet werden können, und welche nicht. Es wird gegenwärtig eine Norm entwickelt (ANSI/ISA99), die das Was, Wie und Warum der Sicherheit in der Automationswelt vollständig beschreibt.

### Hauptziele der Sicherheit

Zunächst gibt es einen wichtigen Unterschied, was die Hauptziele der Sicherheit betrifft.
In der Bürowelt ist es die Hauptaufgabe der Sicherheit stets, die Daten und Informationen auf eine vertrauliche Art und Weise zu behandeln.
In der Automationswelt hingegen ist es das Hauptziel der Sicherheit, stets die Verfügbarkeit des Produktionssystems zu gewährleisten.

### Netzwerkleistung

Beide Bereiche stellen völlig unterschiedliche Anforderungen an das Netzwerk.
Hier eine Übersicht:

| Automationsnetzwerk | Büronetzwerk |
|---|---|
| Echtzeit | keine Echtzeit |
| Antwort ist zeitkritisch | Antwort muss zuverlässig sein |
| mäßiger Durchsatz akzeptabel | hoher Durchsatz erwünscht |
| große Verzögerungen problematisch | große Verzögerungen und Jitter unproblematisch |

Es ist daher wichtig, den Einfluss von Sicherheitstechnologien auf die Leistung des Systems gut einschätzen zu können, bevor diese implementiert werden. So werden zum Beispiel in der Bürowelt häufig Verschlüsselungstechniken angewandt. Verschlüsselung stellt jedoch für Echtzeitanwendungen ein Problem dar.

### Zuverlässigkeit eines Netzwerks

Auch die Anforderungen hinsichtlich der Zuverlässigkeit sind für beide Bereiche unterschiedlich.
Hier eine Übersicht:

| Automationsnetzwerk | Büronetzwerk |
|---|---|
| kontinuierlicher Betrieb | geplanter Betrieb |
| Unterbrechungen der Stromversorgung unzulässig | Unterbrechungen zulässig |
| Test vor der Implementierung vorausgesetzt | Betatest vor Ort zulässig |
| bei Änderungen sind formelle Zertifikate nötig | geringer Verwaltungsaufwand bei Änderungen |

Ein gutes Beispiel hierfür ist die Installation eines neuen Servicepacks. In der Bürowelt ist dies ein ganz normaler Vorgang, in der Fertigungswelt hingegen eher unüblich und in bestimmten Bereichen sogar unzulässig.

### Unterschiedliche Risikoauffassung

| Automationsnetzwerk | Büronetzwerk |
|---|---|
| Sicherheit für Menschen | Datenintegrität |
| Gefahr: Verlust von Leben, Produkt oder Maschine | Gefahr: Verlust von Daten, betrieblichen Vorgänge |
| Fehlertoleranz ist unabdingbar | Neustart über Reboot |

Ferner gibt es in Automationsnetzwerken kritische Reaktionszeiten für Eingriffe durch Menschen: Das Bedienen eines Not-Aus-Schalters darf nicht durch einen Passwortschutz behindert werden.

#### Unterschiedliche Risikoarchitektur

Die für den Schutz kritischsten Geräte in der Büro-IT sind die zentralen Server.
In der Produktions-IT ist es hingegen das Endgerät, etwa die SPS, und nicht der zentrale Datenserver mit den zurückliegenden Daten des Prozesses.

#### Schlussfolgerung

Die klassische Firewall bietet einen Schutz vor Hackern, Würmern und Spyware. Firewall-Software schützt das Netzwerk oder den spezifischen Computer vor der Außenwelt und lässt nur vertrauenswürdige Nachrichten durch. Eine der Aufgaben ist es, alle verdächtigen Programme, die vom eigenen Rechner aus eine Verbindung mit dem Internet aufnehmen wollen, zu blockieren. Ergänzend werden in der Büro-IT sogenannte Antiviren-, Anti-Spyware- und Anti-Adware-Programme eingesetzt, die jede eingehende Datei aufhalten und auf die Anwesenheit von in Datenbanken gespeichertem gefährlichem Code überprüfen. Die Datei kann gegebenenfalls für unbedenklich erklärt oder in die Quarantäne verschoben werden. Solche Programme prüfen auch alle geöffneten Dateien auf die Anwesenheit von in der Datenbank gespeicherten Gefährdungen (Viren, Spyware, Adware). Das Prinzip des IT-Schutzes ist es, dass die Firewall allen ein- und ausgehenden Datenverkehr, alle Daten-Files, Programme etc. betrachtet und analysiert. Derartige Firewalls führen zu Verzögerungen im System und behindern falls nötig die Funktion des Programms.

Für die Verwirklichung einer Firewall, die stärker auf die Bedürfnisse der Industrie abgestimmt ist, müssen zunächst Techniken verwendet werden, um Verzögerungen zu vermeiden und dennoch die Sicherheit und Zuverlässigkeit der Daten zu gewährleisten. Dabei können beispielsweise sichere Kommunikationskanäle zwischen SPS und dem Bediencomputer oder den Datenservern verwendet werden. Um die Arbeit in Echtzeit zu gewährleisten, dürfen bei der Kontrolle von Daten, die die Firewall passieren, keine Verzögerungen auftreten. Daher müssen andere Technologien angewendet werden. Eine Möglichkeit besteht darin, nicht die eigentlichen Daten, sondern stattdessen die angewendeten Protokolle zu kontrollieren.

### 9.3.5 Standardisierung in der Automationsnetzwerksicherheit

#### Einleitung

ANSI/ISA 99 bietet Richtlinien für die Ausführung einer Risikoermittlung, die Erstellung einer sogenannten Cyber-Security-Politik und die Ausführung dieser Politik. Die Norm wurde in Zusammenarbeit mit den Anwendern, Systemintegratoren und Lieferanten erstellt. Sie befindet sich gegenwärtig in der Entwicklung, es sind aktuell zwei Teile verfügbar.
Abb. 9.4 zeigt eine Übersicht der ISA 99. Teil 1 bildet den Rahmen für alle anderen Teile. Gegenwärtig sind nur die Teile 1 und 2.01 verfügbar.

#### Teil 1 (ANSI/ISA report TR99.00.01- 2007)

Dieser erste Teil trägt den Titel: SSecurity for Industrial Automation and Control Systems", die letzte Version stammt vom 29. Oktober 2007. Hier werden Sicherheitstechnologien beschrieben, die gegenwärtig für industrielle Produktions- und Kontrollsysteme zur Verfügung stehen. Es werden Technologien wie etwa die Authentifizierung und die Automation, Firewalls, VPN etc. behandelt.


**Abbildung 9.4:** Der ANSI/ISA99-Standard

Authentifizierung ist das Verfahren, um Anwender, Geräte, Anwendungen und Ressourcen sicher identifizieren zu können. Authentifizierung kann anhand verschiedener Merkmale geschehen: einer Information (Pincode, Passwort etc.), einem Gegenstand (Schlüssel, Zugangskarte, Dongle etc.), ein physisches Merkmal (Fingerabdruck etc.) Hierbei sind zwei verschiedene Formen der Authentifizierung zu unterscheiden: Benutzerauthentifizierung und Netzwerkauthentifizierung.

#### Teil 2 (ANSI/ISA report TR99.00.02- 2004)

Ursprünglich war dem zweiten Teil der folgende Titel zugedacht: *Integrating Electronic Security into the Manufacturing and Control Systems Environment*. Letztendlich werden jedoch jetzt der ursprüngliche Teil 2 und Teil 3 in einem einzigen Teil 2 vereint, der dann aus zwei Abschnitten besteht. Der erste Teil (ISA 99 part 2.01) ist fertig und trägt den Titel Ëstablishing an Industrial Automation and Control Systems Security Program". Er dient dazu, den Anwendern bei der Erstellung eines Security-Management-Plans zu unterstützen. Zweck eines solchen Plans ist es, alle möglichen Risiken aufzuzählen und einige Lösungen zu formulieren. ISA 99 part 2.02 beschreibt dann, wie ein derartiger Plan auszuführen ist.

#### Teil 4

In Teil 4 sollen die an Geräte und Systeme für die Einhaltung des ISA-99-Standards gestellten Anforderungen beschrieben werden.

### 9.3.6 Ein Sicherheitsprogramm

Die Ausarbeitung eines Sicherheitsplans bedeutet mehr, als nur technische Lösungen (Firewalls, Datenverschlüsselung) aufzuzählen. Auch verschiedene menschliche Faktoren können zu einer erfolgreichen Implementation eines CSMS (Cyber Security Management System) beitragen. Einige Schwerpunkte, die zu einer erfolgreichen Integration führen können:

- eine Sicherheitspolitik muss vollständig zur Firmenpolitik passen

- das Sicherheitsprogramm muss zur Firmenkultur passen
- Unterstützung durch ein engagiertes Management
- klare Budgetierung der Maßnahmen des Sicherheitsmanagements
- Trennung der Funktionalitäten: Ist ein Produktverantwortlicher gleichzeitig auch für die Sicherheit verantwortlich, so steht die Sicherheit häufig erst an zweiter Stelle.
- Organisieren von Aktivitäten und Schulungen für alle Arbeitnehmer
- Bekanntmachen von Richtlinien unter allen Arbeitnehmern

## 9.4 Sicherheit in der Praxis

Sicherheit bedeutet, die Maschine, die Produktion oder das Verfahren gegen bestimmte menschliche Aktivitäten zu schützen. Menschliche Aktivitäten können unbewusst oder absichtlich zu einem Produktionsstillstand führen.

Es gibt nicht eine einzige Regel, mit deren Hilfe Sicherheit gewährleistet werden kann, sondern verschiedene Konzepte müssen dazu führen, dass menschliche Fehler minimiert werden und dass Personen mit schlechten Absichten davon abgehalten werden, die verfügbaren Daten zu missbrauchen.

Sicherheit im industriellen Umfeld kann auf verschiedenen Ebenen integriert werden:

### 9.4.1 Sicherheitsebene 1

Ein erster Schritt auf dem Weg zu einem gut geschützten Netzwerk ist die mechanische Sicherung der Netzwerkkabel. Mithilfe sicherer Clips kann verhindert werden, das Netzwerkkabel einfach aus einem Netzwerk-Port gezogen werden können. Auch der Zugang zu freien RJ45-Ports der verschiedenen Switches muss mechanisch erschwert werden, um den Zugang für Unbefugte zu verhindern.

Abb. 9.5 stellt die Möglichkeiten dar, ungenutzte Ports zu blockieren und Ethernet-Stecker zu befestigen.

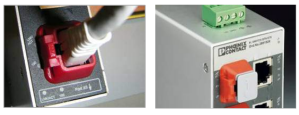

**Abbildung 9.5:** Sicherheitsebene 1

### 9.4.2 Sicherheitsebene 2

Ein zweiter Schritt zur Sicherung eines Netzwerks ist die Verwendung von verfügbarer Software für das Management von Switches.

Switches müssen einige wichtige Sicherheitsmerkmale aufweisen:

- Das Web-based Management muss passwortgeschützt sein.
- es muss die Möglichkeit bestehen, auf Basis von IP-Adressen verschiedene Rechte zuzuweisen (Read-only oder Read-Write).
- Switches müssen bestimmte Sicherungen pro Port einstellen können. So muss z. B. pro Port eine Liste der zugelassenen MAC-Adressen eingestellt werden können.

### 9.4.3 Sicherheitsebene 3

Der wichtigste Schritt bei der Sicherung eines Automationsnetzwerks ist die Trennung von verschiedenen Segmenten durch ein Sicherheitsmodul. Ein Sicherheitsmodul ist ein Router mit den folgenden Möglichkeiten:

- NAT und 1:1-NAT: Die Anwendung von NAT sorgt bereits für eine Übersetzung der IP-Adressen. Dadurch ist es für einen Außenstehenden bereits schwieriger, die im Netzwerk verwendete IP-Adressierung in Erfahrung zu bringen.
- Integrierte Stateful-Inspection-Firewall.
- User-Firewall: individuelle Regeln für verschiedene Anwender.
- Unterstützung der VPN-Technologie.