

Wendell Odom

Übersetzung: Uwe Ring, Cosmos Consulting GmbH

# CCNA INTRO Prüfungshandbuch

Die offizielle Vorbereitung zum  
Cisco-Examen CCNA INTRO Nr. 640–821

## Grundlagen zu Ethernet-LANs

Im vorigen Kapitel haben Sie gelernt, dass die beiden OSI-Layer 1 und 2 dem Netzwerkinterface-Layer von TCP/IP sehr ähnlich sind. In diesem Kapitel werden Sie mehr über die Funktionen der beiden unteren Layer des OSI-Referenzmodells erfahren. Dabei wird besonders auf Ethernet-LANs eingegangen.

Es wurde im Einführungskapitel erwähnt, dass das INTRO-Examen einige Themen nur andeutet und andere dagegen ausführlich behandelt. Wie der Titel verrät, geht es in diesem Kapitel um die Grundlagen von Ethernet. Damit wird der Weg vorbereitet, der zu einem tieferen Verständnis der später folgenden Themen führt. In Kapitel 9, »Cisco LAN Switching«, und Kapitel 10, »Virtuelle LANs und Trunking«, folgt eine gründliche Darstellung von LAN Switches und virtuellen LANs. In Kapitel 11, »LAN-Verkabelung, Standards und Topologien« wird Ihr Verständnis von Ethernet vertieft. Es enthält eine Menge Details über Ethernet-Standards, Verkabelung und Topologien – alles Themen, die für Ihr Examen relevant sein können.

### 3.1 »Weiß ich's schon?«-Quiz

Ziel des Quiz ist es, Ihnen bei der Entscheidung darüber zu helfen, welche Abschnitte eines Kapitels Sie lesen müssen. Wenn Sie ohnehin das ganze Kapitel lesen wollen, brauchen Sie die Fragen an dieser Stelle nicht zu beantworten.

Mit dem 10-Fragen-Quiz können Sie, bezogen auf das Grundlagen-Kapitel, Ihre begrenzte Studienzeit sinnvoll einteilen.

Tabelle 3.1 stellt die Hauptthemen des Kapitels und die dazu passenden Fragen aus dem Quiz dar.

Tabelle 3.1: »Weiß ich's schon?«- Übersicht zum Grundlagen-Kapitel

Grundlagen-Kapitel	Fragen zu diesem Abschnitt
LANs aus der Perspektive des OSI	1, 5
Frühe Ethernet Standards	3, 7, 8
Ethernet Datenverbindungs-Protokolle	2, 4, 6, 9
Neuere Ethernet Standards	10

**ACHTUNG**

Das Ziel dieser Selbsteinschätzung soll sein, dass Sie Ihren Wissensstand zu den Themen richtig bewerten. Wenn Sie eine Frage nicht beantworten können oder sich auch nur unsicher fühlen, sollten Sie sie als falsch einstufen und markieren. Jeder Sympathiepunkt, den Sie sich selbst geben, verfälscht Ihr Ergebnis und wiegt Sie in trügerischer Sicherheit.

1. Welche der folgenden Lösungen beschreibt am besten die Hauptfunktionen eines Protokolls auf OSI-Layer 1?
  - a) Framing
  - b) Übertragung von Bits von einem Gerät zum anderen
  - c) Adressierung
  - d) CSMA/CD
  - e) Festlegung von Größe und Form von Ethernet-Karten
2. Welche der folgenden Lösungen gehört zu den Funktionen von OSI-Layer 2-Protokollen?
  - a) Framing
  - b) Übertragung von Bits von einem Gerät zum anderen
  - c) Adressierung
  - d) Fehlererkennung
  - e) Festlegung von Größe und Form von Ethernet-Karten
3. Welche der folgenden Antworten trifft auf Ethernet-Crossover-Kabel zu?
  - a) Die Kontakte 1 und 2 sind am anderen Ende des Kabels umgekehrt belegt.
  - b) Die Kontakte 1 und 2 sind am anderen Ende des Kabels mit den Kontakten 3 und 6 verbunden.
  - c) Die Kontakte 1 und 2 sind am anderen Ende des Kabels mit den Kontakten 3 und 4 verbunden.

- d) Das Kabel kann bis zu 1000 m Länge haben und Gebäude verbinden.  
 e) Keine der genannten Antworten
4. Welche der folgenden Lösungen gilt für das Format von Ethernet-Adressen?
- a) Jeder Hersteller verwendet einen einmaligen Code für die ersten 2 Bytes der Adresse.  
 b) Jeder Hersteller verwendet einen einmaligen Code für die ersten 3 Bytes der Adresse.  
 c) Jeder Hersteller verwendet einen einmaligen Code in der ersten Hälfte der Adresse.  
 d) Der Teil der Adresse, der diesen Herstellercode enthält, wird MC genannt.  
 e) Der Teil der Adresse, der diesen Herstellercode enthält, heißt OUI.  
 f) Der Teil der Adresse, der diesen Herstellercode enthält, hat keinen spezifischen Namen.
5. Welche der folgenden Antworten trifft auf das Ethernet-FCS-Feld zu?
- a) Es wird für die Fehlerbeseitigung genutzt.  
 b) Es ist 2 Bytes lang.  
 c) Es befindet sich im Ethernet-Trailer, nicht im Ethernet-Header.  
 d) Es wird für die Verschlüsselung verwendet.  
 e) Keine der genannten Antworten
6. Welches der folgenden Felder kann von Ethernet als »Typen«-Feld genutzt werden, um den im Datenteil des Ethernet-Frames enthaltenen Datentyp zu bestimmen?
- a) Das DIX-Ethernet-DSAP-Feld  
 b) Das IEEE-802.2-Ethernet-Typenfeld  
 c) Das IEEE-802.2-Ethernet-DSAP-Feld  
 d) Das SNAP-Header-Protokoll-Typenfeld  
 e) Keine der genannten Lösungen
7. Welche der folgenden Lösungen trifft auf das CSMA/CD-Verfahren zu?
- a) Das Verfahren verhindert, dass Kollisionen stattfinden können.  
 b) Kollisionen können stattfinden, das Verfahren bestimmt jedoch, wie die Rechner eine Kollision erkennen und beseitigen.  
 c) Das Verfahren funktioniert nur, wenn mindestens zwei Geräte im selben Ethernet-Netzwerk liegen.  
 d) Keine der genannten Lösungen

8. Bei welcher der folgenden Situationen handelt es sich um eine Kollisionsdomäne?
  - a) Alle Geräte sind an einen Ethernet-Hub angeschlossen.
  - b) Alle Geräte sind an einen Ethernet-Switch angeschlossen.
  - c) Zwei PCs sind über ein Crossover-Kabel miteinander verbunden.
  - d) Bei keiner der genannten Situationen
9. Welcher Begriff trifft am besten auf Ethernet-Adressen zu, die gleichzeitig mit mehreren Geräten kommunizieren können?
  - a) Eingebrennte Adresse
  - b) Unicast-Adresse
  - c) Broadcast-Adresse
  - d) Multicast-Adresse
  - e) Keine der genannten Lösungen
10. Auf einer 10/100-Karte ist Autonegotiation eingestellt. Welche Verbindungseigenschaften werden vereinbart, wenn das Gerät am anderen Ende überhaupt keine Negotiation ausführt?
  - a) 100 Mbit/s, Halb-Duplex
  - b) 100 Mbit/s, Voll-Duplex
  - c) 10 Mbit/s, Halb-Duplex
  - d) 10 Mbit/s, Voll-Duplex

Die Antworten zum »Weiß ich's schon?«-Quiz stehen in Anhang A. Unser Vorschlag für Ihr weiteres Vorgehen sieht wie folgt aus:

- **8 oder weniger Gesamtpunkte** – Lesen Sie das gesamte Kapitel. Es enthält die »Grundlagen«, die »Grundlagen-Zusammenfassung« und den »Q&A«-Abschnitt.
- **9 oder 10 Gesamtpunkte** – Wenn Sie einen größeren Überblick über diese Themen bekommen möchten, springen Sie zur »Grundlagen-Zusammenfassung« und dann zum »Q&A«-Abschnitt. Andernfalls gehen Sie sofort zum nächsten Kapitel.

## Grundlagen

Ethernet ist der unangefochtene Spitzenreiter unter den heutigen LAN-Standards. Vor fünfzehn Jahren war noch nicht entschieden, ob Ethernet oder Token Ring den Wettkampf um die erfolgreichste LAN-Technologie gewinnen würde. Und vor acht Jahren sah es so aus, als ob Ethernet diesen Kampf

gegen Token Ring gewinnen, ihn aber gegen den Newcomer ATM (Asynchronous Transfer Mode) verlieren könnte. Denkt man heute an LANs, so steht außer Frage, um welchen Typ es sich handelt – es ist Ethernet.

Ethernet konnte seine Position seit so vielen Jahren behaupten, da es sich den Marktanforderungen anpassen konnte, ohne die Haupteigenschaften der Originalprotokolle zu verlieren. Die ursprüngliche Übertragungsrate von 10 Mbit/s (Megabits pro Sekunde) wurde bis hin zu einer heutigen Geschwindigkeit von 10 Gbit/s (Gigabits pro Sekunde) verbessert und Ethernet sicherte sich seinen Platz als das am weitesten verbreitete LAN-Protokoll aller Zeiten.

Ethernet bestimmt sowohl Layer 1-, als auch Layer 2-Funktionen. Deshalb beginnt dieses Kapitel mit einigen Grundlagen zu den OSI-Layern 1 und 2. Es folgt eine Darstellung der drei frühesten Ethernet-Standards, wobei das Augenmerk hier besonders auf die Eigenschaften des physikalischen Layers gerichtet wird. Anschließend werden jene Funktionen auf der Datenverbindungsebene vorgestellt, die sowohl bei früheren Ethernet-Standards galten als auch noch bei heutigen Standards üblich sind. Schließlich werden zwei jüngere Standardtypen, Fast Ethernet und Gigabit Ethernet, eingeführt.

## 3.2 LANs aus der Perspektive des OSI

Der physikalische OSI-Layer und das OSI-Datenverbindungs-Protokoll erfüllen gemeinsam die Funktion der Datenübertragung über eine Vielzahl unterschiedlicher physikalischer Netzwerke. Damit eine Kommunikation stattfinden kann, müssen naturgemäß einige physikalische Übereinstimmungen erfüllt sein, etwa die Verkabelung, die Steckverbindungen an den Kabelenden, die Stromspannung und die aktuellen Übertragungsmodi der Binärcodes.

Der Datenverbindungslayer erfüllt üblicherweise Funktionen, die nicht auf den ersten Blick zu erkennen sind. So legt er beispielsweise die Regeln (Protokolle) fest, nach denen einem Computer der Gebrauch des physikalischen Netzwerks erlaubt ist, wann er nicht auf das Netzwerk zugreifen darf, und wie Fehler erkannt werden können, die während einer Datenübertragung entstanden sind. Die Teile II und III, »Die Bedienung von Cisco-Geräten« und »LAN-Switching«, enthalten weitere Details zu den Ethernet-Layern 1 und 2.

### 3.2.1 Typische LAN-Eigenschaften des OSI 1-Layers

Der physikalische Layer des OSI-Modells, Layer 1, bestimmt die Einzelheiten dafür, wie Daten von einem Gerät zum anderen übertragen werden. Tatsächlich denken viele, dass der OSI-Layer 1 »Bits sendet«. Es sind jedoch die

höheren Layer, die Daten inkapseln und entscheiden, wann und was gesendet wird. Möglicherweise muss der Sender die Daten aber zu einem anderen Gerät schicken. Der physikalische Layer des OSI-Modells legt die Standards zum Senden und Empfangen von Bits über ein physikalisches Netzwerk fest.

Um das eigentliche Ziel im Auge zu behalten, sehen wir uns in einem Beispiel an, wie ein Webbrowser bei einem Server eine Internetseite abrufen. Bild 3.1 führt Ihnen den Zeitpunkt vor Augen, zu dem Bob die HTTP-, TCP-, IP- und Ethernet-Header fertig gestellt hat und die Daten an R2 senden möchte.

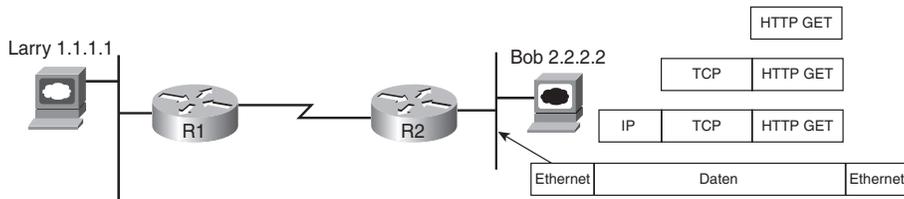


Bild 3.1: Datenverbindungs-Frames, gesendet über den physikalischen Layer

In der Abbildung sehen Sie, wie Bobs Ethernet-Karte die Ethernet-Eigenschaften des physikalischen Layers nutzt, um die im Ethernet-Frame dargestellten Bits über das physikalische Ethernet zu übertragen. Der physikalische OSI-Layer und die Protokolle, die ihm unter TCP/IP entsprechen, legen alle Einzelheiten für die Übertragung von Bits von einem Gerät zum nächsten fest. Der physikalische Layer bestimmt zum Beispiel die Einzelheiten bei der Verkabelung – die maximale Länge für einen Kabeltyp, die Anzahl der Drähte im Inneren des Kabels, die Form des Verbindungssteckers am Kabelende und andere Details. Die meisten Kabel enthalten mehrere Leiter (Drähte). Die Enden dieser Drähte, die im Verbindungsstecker ankommen, werden *Kontakte* (oder *Pins*) genannt. Der physikalische Layer muss also den Zweck für jeden Kontakt oder Draht definieren. Nehmen wir als Beispiel ein un abgeschirmtes paarweise-verdrilltes (twisted-pair) Kabel für Ethernet (UTP), das der Kategorie 5 (CAT5) entspricht. Hier werden die Kontakte 1 und 2 für die Datenübertragung verwendet, indem elektrische Signale über die anliegenden Drähte gesendet werden. Auf den Kontakten 3 und 6 werden hingegen Daten empfangen. Bild 3.2 zeigt ein Ethernetkabel mit RJ-45 Stecker aus mehreren Perspektiven.

Das Bild auf der linken Seite zeigt eine RJ-45-Steckerverbindung (Regulated Jack 45), wie sie für eine Ethernet-Verkabelung heutzutage typisch ist. Auf der rechten Seite sieht man die Kontakte, die auf den gängigen Ethernet-Standard-Kabeln verwendet werden. Ein Drahtpaar wird zur Datenübertragung genutzt, wobei die Kontakte 1 und 2 verwendet werden, ein weiteres

Drahtpaar ist unter Benutzung der Kontakte 3 und 6 für den Datenempfang zuständig. Das in Bild 3.1 gezeigte Ethernet zwischen Bob und R2 könnte sich aus Kabeln mit RJ-45-Steckern, Hubs und Switches zusammensetzen. (Hubs und Switches werden an späterer Stelle erklärt.)

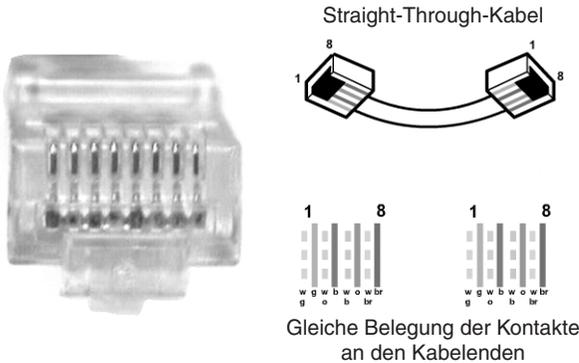


Bild 3.2: UTP-Kabel (CAT5) mit RJ-45 Stecker

Das in Bild 3.2 dargestellte Kabel heißt *Straight-Through-Kabel*. Ein Straight-Through-Kabel verbindet Kontakt 1 an einem Ende mit Kontakt 1 am anderen Ende des Kabels, Kontakt 2 an einem Ende mit Kontakt 2 am anderen Ende des Kabels und so weiter. Wenn Sie das Kabel so in der Hand halten, dass beide Stecker mit der gleichen Ausrichtung Seite an Seite liegen, dann sehen Sie die gleichen Drähte – erkennbar an ihrer Farbe – für jeden Stecker mit einem Straight-Through-Kabel.

Einige Leute, die sich noch nie mit dem Thema Netzwerkverkabelung auseinandergesetzt haben, sind erstaunt darüber, dass viele Kabel zwei Drähte zur Datenübertragung enthalten, und dass diese Drähte umeinander herumgedrillt sind. Wenn zwei Drähte innerhalb des Kabels miteinander verdrillt sind, werden Sie *twisted pair* genannt (genialer Name, oder?). Durch das Drehen der Drähte wird die beim Stromfluss erzeugte elektromagnetische Interferenz um einiges reduziert. Deshalb werden in den meisten LANs zwei *Twisted pair*-Kabel verwendet – ein Paar zur Datenübertragung und eines zum Datenempfang.

Der physikalische OSI-Layer und die Protokolle, die ihm unter TCP/IP entsprechen, legen alle Einzelheiten für die Übertragung von Bits von einem Gerät zum nächsten fest. Sie werden in späteren Abschnitten dieses Kapitels mehr über die spezifischen Standards des physikalischen Layers für Ethernet erfahren. Tabelle 3.2 enthält eine Auflistung der typischen Einzelheiten, die von physikalischen Layer-Protokollen festgelegt werden.

Tabelle 3.2: Typische Funktionen des physikalischen Layers

Funktion	Beschreibung
Verkabelung	Bestimmt die Anzahl der Drähte und die Art der Abschirmung (falls gegeben).
Stecker	Legt die Form des Steckers und die Anzahl der Kontakte fest.
Kontakte	Bestimmt den Zweck der Kontakte. Ein Kontakt kann einem anderen Gerät zum Beispiel signalisieren, ob es senden darf.
Spannung und Strom	Definiert die elektrischen Eigenschaften der Endgeräte, die ein Kabel verwenden.
Verschlüsselung/ Kodierung	Legt fest, auf welche Weise ein Gerät einem oder mehreren Übertragungskontakt(en) Binärzahlen signalisiert. 5V kann beispielsweise 1 bedeuten, während +5V eine 0 bedeutet. (Es existieren viele Verschlüsselungsschemata, die weit über die Relevanz für die CCNA-Prüfung hinausgehen.)

### 3.2.2 Typische LAN-Eigenschaften für OSI-Layer 2

OSI-Layer 2, der Datenverbindungslayer, legt die Standards und Protokolle fest, die die Datenübertragung über einen physikalischen Layer kontrollieren. Wenn Sie bei Layer 1 an einen Layer denken, der »Bits sendet«, so können Sie sich im Falle von Layer 2 vorstellen, dass dieser »weiß, wann Bits gesendet werden müssen, bemerkt, wenn beim Senden der Bits Fehler auftauchen, und den Computer erkennt, der die Bits bekommen soll.«

Ähnlich wie in dem Abschnitt über den physikalischen Layer, werden in diesem Abschnitt die Grundfunktionen des Datenverbindungslayers beschrieben. An späterer Stelle werden Sie mehr über die spezifischen Standards und Protokolle für Ethernet erfahren.

Datenverbindungs-Protokolle erfüllen viele Funktionen und enthalten vielfältige Ausführungsdetails. Da jedes Datenverbindungs-Protokoll einen bestimmten Typus des physikalischen Layers »kontrolliert«, müssen bei der Beschreibung seiner Funktionen auch einige Eigenheiten des physikalischen Netzwerks berücksichtigt werden. Unabhängig vom Typ des physikalischen Layers erfüllen die meisten Datenverbindungs-Protokolle jedoch folgende Funktionen:

- **Arbitration** – Legt fest, wann es bewilligt ist, ein physikalisches Medium zu benutzen
- **Adressierung** – Stellt sicher, dass der richtige Empfänger die gesendeten Daten erhält und weiterleitet

- **Fehlererkennung** – Prüft, ob die Daten ihren Weg über den physikalischen Layer erfolgreich zurückgelegt haben
- **Identifizierung der eingekapselten Daten** – Findet den Header-Typ, der dem Datenverbindungs-Header folgt, heraus

### Datenverbindungs-Funktion 1: Arbitration

Stellen Sie sich vor, Sie wollen eine Straßenkreuzung passieren, aber die Ampeln sind abgeschaltet – natürlich wollen auch alle anderen Autofahrer in diesem Moment die Kreuzung durchfahren, tun aber gut daran, dies nacheinander zu tun. Sie werden die Ampel schließlich passieren, nach Abwägung einer Vielzahl von Überlegungen – darüber, wie vorsichtig Sie sind, wie groß die anderen Autos sind, ob ihr Wagen neu oder alt ist und wie viel Ihr Leben Ihnen wert ist! Ganz gleich wie Sie sich verhalten, wenn Sie mit mehreren Autos aus verschiedenen Richtungen gleichzeitig losfahren, wird es mit großer Wahrscheinlichkeit zu ernstesten Zusammenstößen kommen.

Daten-Frames können auf einigen Typen von physikalischen Netzwerken kollidieren, wenn Geräte zu jeder beliebigen Zeit senden dürfen. Wenn Frames in einem LAN kollidieren, werden die Daten in jedem Frame zerstört und das LAN ist für einen kurzen Moment außer Betrieb gesetzt – diese Situation unterscheidet sich nicht allzu sehr von einem Verkehrsunfall auf einer Kreuzung. Die Spezifikationen für diese Datenverbindungs-Protokolle bestimmen, wie die Nutzung des physikalischen Mediums aufgeteilt wird, um Kollisionen zu vermeiden oder zumindest die Fehler zu beheben, die durch Kollisionen entstanden sind.

Ethernet verwendet *CSMA/CD (Carrier Sense Multiple Access Collision Detect)*, ein Verfahren zur Arbitration. Das CSMA/CD-Verfahren wird im nächsten Abschnitt besprochen, der sich mit Ethernet beschäftigt.

### Datenverbindungs-funktion 2: Adressierung

Wenn ich mit meinem Freund Gary zu Mittag esse – und zwar nur mit Gary – weiß er, dass ich mit ihm spreche. Ich muss nicht jeden Satz mit »Hey, Gary!« beginnen. Aber stellen Sie sich vor, ein paar Leute würden sich zu uns an den Tisch gesellen – jetzt könnte es notwendig werden, einen Satz mit »Hey, Gary!« zu beginnen, damit er weiß, dass ich ihn meine.

Datenverbindungs-Protokolle legen Adressen aus den gleichen Gründen fest. Bei vielen physikalischen Netzwerken können mehr als zwei Geräte angeschlossen sein. Ein Datenverbindungs-Protokoll bestimmt also Adressen, damit sichergestellt wird, dass das richtige Gerät zuhört und die gesendeten Daten empfängt. Indem die richtige Adresse in den Datenverbindungs-Header eingefügt wird, kann der Sender eines Frames ziemlich sicher sein,

dass der korrekte Empfänger die Daten erhalten wird. Das ist absolut übertragbar auf die Situation mit Gary am Mittagstisch. Damit er weiß, dass er und nicht jemand anders angesprochen wird, muss der Satz mit »Hey Gary!« beginnen.

Jedes Datenverbindungs-Protokoll entwickelt seine eigene Adresstruktur. Ethernet verwendet beispielsweise MAC-Adressen (Media Access Control), die mehr als 6 Bytes lang sind und als 12-stellige Hexadezimalzahl dargestellt werden. Frame Relay benutzt die typischen 10-Bit-Adressen namens DLCI (Data-Link Connection Identifier) – beachten Sie, dass der Name sogar den Begriff *data link* enthält. Dieses Kapitel behandelt die Einzelheiten der Ethernet-Adressierung. Über die Frame Relay-Adressierung erfahren Sie mehr im *CCNA ICND Prüfungshandbuch*.

### Datenverbindungsfunktion 3: Fehlererkennung

Das Feature »Error *detection*«, Fehler**beseitigung** erkennt, ob während der Übertragung des Frames Bitfehler entstanden sind. Für diese Funktion enthalten die meisten Datenverbindungs-Protokolle ein FCS-Feld (*frame check sequence*) oder ein CRC-Feld (*cyclical redundancy check*) im Datenverbindungs-Trailer. Dieses Feld enthält einen Wert. Er ist das Ergebnis einer mathematischen Formel, die auf die Daten im Frame angewendet wird.

Ein Fehler wird dadurch entdeckt, dass der Empfänger eine spezielle mathematische Formel auf den Inhalt des empfangenen Frames anwendet. Sowohl der Sender als auch der Empfänger führen die gleiche mathematische Kalkulation durch, wobei der Sender das Ergebnis vor dem Lossenden in das FCS-Feld einfügt. Wenn dieses Ergebnis mit dem des Empfängers übereinstimmt, hat der Frame während der Übertragung keinen Schaden erlitten.

Die Fehlererkennung schließt keine Fehlerbeseitigung, Error *Recovery* ein. Die meisten Datenverbindungen, darunter auch IEEE 802.5 Token Ring und 802.3 Ethernet, bieten keine Fehlerbeseitigungsfunktion. Das FCS-Feld erlaubt dem Empfangsgerät, Fehler zu bemerken und den Datenframe zu löschen. Für die Fehlerbeseitigung und das dazu gehörende Neuversenden der Daten ist ein anderes Protokoll zuständig. Zum Beispiel bietet TCP eine Fehlerbeseitigung. Seine Funktion wird in Kapitel 6, »Grundlagen von TCP und UDP« beschrieben.

### Datenverbindungsfunktion 4: Identifizierung der eingekapselten Daten

Der vierte Teil der Datenverbindung identifiziert schließlich den Inhalt des Datenfelds im Frame. Bild 3.3 verdeutlicht, wie nützlich diese Eigenschaft ist. Es wird ein PC dargestellt, der sowohl TCP/IP als auch Novell IPX nutzt.

Das erste Protokoll dient zur Kommunikation mit einem Webserver, das andere ermöglicht eine Kommunikation mit einem Novell NetWare-Server.

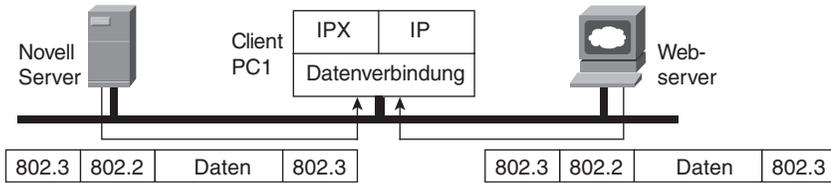


Bild 3.3: Multiplexing unter Verwendung von Datenverbindungstypen und Protokollfeldern

Wenn PC1 Daten empfängt, sollte er sie dann an die TCP/IP Software oder an die Software des NetWare-Kunden senden? Das hängt natürlich davon ab, was sich im Datenfeld befindet. Kommen die Daten vom Novell-Server, reicht sie PC1 an den NetWare Client-Code weiter. Wenn die Daten vom Webserver kommen, leitet er sie an den TCP/IP-Code weiter. Aber auf welcher Grundlage trifft PC1 diese Entscheidung? Nun, IEEE Ethernet 802.2 LLC verwendet ein Feld im Header zur Erkennung des Datentyps im Datenfeld. PC1 prüft das Feld im ankommenden Frame, um zu entscheiden, ob es sich bei dem Paket um ein IP-Paket oder um ein IPX-Paket handelt.

Jeder Datenverbindungs-Header hat ein Feld, um den Protokolltypen, der im Datenfeld des Frames vorkommt, zu identifizieren. Der Name dieses Feldes enthält im Allgemeinen das Wort *Type*. In jedem Fall enthält das Typenfeld einen Code, der IP, IPX oder eine andere Kennzeichnung bedeutet und den Typen des folgenden Protokoll-Headers festlegt.

### 3.3 Frühe Ethernet-Standards

Jetzt wissen Sie schon Einiges über die Funktionen von physischen und Datenverbindungs-Standards. Im nächsten Abschnitt werden Sie mehr Einzelheiten über Ethernet erfahren. Während in diesem Kapitel die Grundfunktionen erläutert werden, sind die Kapitel 9 bis 11 den Feinheiten gewidmet.

In diesem Abschnitt lernen Sie etwas über die frühesten Ethernet-Netzwerke. Der Begriff *Ethernet* bezieht sich auf eine Familie von Protokollen und Standards. Sie bestimmen zusammen den physikalischen und den Datenverbindungs-Layer des weltweit bekanntesten LAN-Typs. Es gibt viele Variationen von Ethernet. Dieser Abschnitt beschäftigt sich mit den Funktionen und Protokollspezifikationen der populärsten Ethernet-Typen, darunter 10BASE-T, Fast Ethernet und Gigabit Ethernet. Damit Sie die Funktion bestimmter

Eigenschaften von Ethernet richtig einordnen können, werden in diesem Abschnitt ein paar historische Informationen über zwei ältere Ethernet-Typen, 10BASE2- und 10BASE5-Ethernet gegeben.

### 3.3.1 Übersicht über die Standards

Wie die meisten Protokolle, entstand Ethernet innerhalb eines Unternehmens, das versuchte, ein bestimmtes Problem zu lösen. Xerox brauchte ein gutes Verfahren, um die damals neue Erfindung Personalcomputer in seinen Büroräumen zu verbinden. Dies war die Geburtsstunde von Ethernet. (Falls Sie mehr interessante historische Einzelheiten dazu erfahren wollen, können Sie im Internet unter der Adresse [inventors.about.com/library/weekly/aa111598.htm](http://inventors.about.com/library/weekly/aa111598.htm) nachlesen.) Schließlich wurde Ethernet von einem Team von Xerox, Intel und DEC (Digital Equipment Corp.) weiterentwickelt, daher der ursprüngliche Name von Ethernet: *DIX Ethernet* (eine Gemeinschaftsarbeit von DEC, Intel und Xerox).

Die IEEE begann im Februar 1980 mit der Entwicklung einer standardisierten Version von Ethernet, aufbauend auf der Arbeit von DEC, Intel und Xerox. Die IEEE Ethernet-Spezifikationen, die sich auf OSI-Layer 2 beziehen, wurden in zwei Unterlayer aufgeteilt: den MAC-Sublayer (*Media Access Control*) und den LLC-Sublayer (*Logical Link Control*). Die IEEE bildete ein Komitee, das damit beauftragt war, diese beiden Teile auszuarbeiten – das 802.3-Komitee sollte den MAC-Sublayer weiterentwickeln und das 802.2-Komitee den LLC-Sublayer.

In Tabelle 3.3 sehen Sie eine Auflistung der verschiedenen Protokollspezifikationen von den drei ursprünglichen IEEE LAN-Standards, außerdem die originalen Vorläuferversionen von Ethernet.

Tabelle 3.3: MAC- und LLC-Standards für drei LAN-Typen

Name	MAC-Sublayer-Spezifikationen	LLC-Sublayer-Spezifikationen
Ethernet-Version 2 (DIX-Ethernet)	Ethernet	–
IEEE-Ethernet	IEEE 802.3	IEEE 802.2
IEEE-Token Ring	IEEE 802.5	IEEE 802.2
ANSI FDDI	ANSI X3T9.5	IEEE 802.2

### 3.3.2 Die ursprünglichen Ethernet-Standards: 10BASE2 und 10BASE5

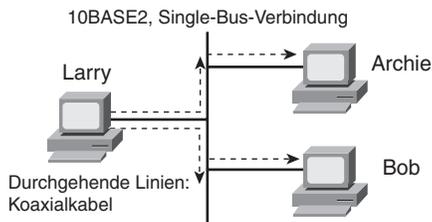
Man versteht Ethernet am besten, indem man zunächst einen Blick auf die frühen DIX-Ethernet-Spezifikationen wirft. Sie heißen *10BASE5* und *10BASE2*. Diese beiden Ethernet-Spezifikationen bestimmen die Details des physikalischen Layers von frühen Ethernet-Netzwerken. (10BASE2 und 10BASE5 weisen geringe Unterschiede in der Verkabelung auf, aber für unsere Zwecke können Sie sie als identisch betrachten.) Mit diesen beiden Spezifikationen installiert ein Netzwerktechniker eine Serie von Koaxialkabeln und verbindet jedes Gerät in dem Ethernet-Netzwerk – ohne Hub, Switch oder Verkabelungs-Frontplatte. Das Ethernet besteht lediglich aus den versammelten Ethernet-Karten der Computer und den Kabeln.

Die ganze Serie von Kabeln bildet einen elektrischen Bus, den sich alle an das Ethernet angeschlossenen Geräte teilen. Wenn ein Computer auf dem Bus Bits zu einem anderen Computer senden will, sendet er ein elektrisches Signal, und die Elektrizität verbreitet sich unter allen Geräten in dem Ethernet.

Da es sich um einen einzigen Bus handelt, tauchen Probleme auf, sobald zwei oder mehr Geräte zur gleichen Zeit Signale senden. Die Folge wäre eine Überlappung und Kollision der Signale, die dadurch letztendlich unverständlich würden. So überrascht es nicht, dass Ethernet auch eine Spezifikation definierte, mit der sichergestellt wurde, dass zu einem Zeitpunkt immer nur ein Gerät Datenverkehr senden konnte – Ethernet wäre sonst unbrauchbar gewesen. Das Verfahren, bekannt als CSMA/CD-Verfahren (*Carrier Sense Multiple Access Collision Detect*), legt den Zugang zum Bus fest. Auf eine menschliche Situation übertragen, entspricht das CSMA/CD-Verfahren ungefähr der Gesprächssituation in einem Meeting mit vielen Teilnehmern. Einige der Anwesenden beanspruchen viel Redezeit. Andere äußern sich gar nicht, hören aber zu. Wieder andere tragen gelegentlich etwas zur Diskussion bei. Es ist schwierig für Menschen, etwas zu verstehen, wenn zwei Personen gleichzeitig reden. Aus diesem Grund gibt es die Regel, dass nur einer spricht, während der Rest zuhört. Nun stellen Sie sich vor, dass sich Bob und Larry beide gleichzeitig zu Wort melden. Bei der ersten sich bietenden Gelegenheit versuchen beide, ihren Beitrag zu bringen. Es könnte der Fall eintreten, dass Larry Bobs Stimme wahrnimmt, noch bevor er einen Mucks tun konnte, und sich daraufhin zurücknimmt. Vielleicht reden sie aber auch beide zur gleichen Zeit los, so dass sie durcheinander reden und viele der im Raum Anwesenden nicht verstehen können, was sie sagen. Für einen solchen Fall könnte der Spruch »Entschuldigung, nach Ihnen.« zur Anwendung kommen, woraufhin nur noch einer das Wort hat, Larry oder Bob. In anderen Fällen kann es passieren, dass eine dritte Person sich einschaltet und

Larry und Bob beide verstummen. Die »Regeln« hängen von Ihrer Kultur ab. Das CSMA/CD-Verfahren basiert auf Ethernet-Protokoll-Spezifikationen und dient dem gleichen Ziel.

Bild 3.4 stellt die logische Grundlage eines alten Ethernet-10BASE2-Netzwerks dar. Es nutzte buchstäblich einen einzigen elektrischen Bus und bestand lediglich aus Koaxialkabeln und Ethernet-Karten.



*Bild 3.4: Kleines Ethernet-10BASE2-Netzwerk*

Die durchgezogenen Linien in der Abbildung stellen die physikalische Netzwerkverkabelung dar, die gestrichelten Linien mit den Pfeilen bezeichnen den Pfad, den Larrys gesendeter Frame verfolgt. Larry sendet über seine Ethernet-Karte ein Signal an das Kabel aus, das sowohl Bob als auch Archie empfangen. Die Verkabelung bildet einen physikalischen Bus, das heißt, dass alle gesendeten Signale von allen Stationen auf dem LAN empfangen werden. Genau wie ein Schulbus, der auf seiner Fahrtroute an jedem Haus hält, wird das elektrische Signal in einem 10BASE2- oder 10BASE5-Netzwerk an jeder Station des LANs empfangen.

Da das elektrische Signal auf der gesamten Länge des Busses entlang reist, kann es zu einer Kollision kommen, wenn zwei Stationen gleichzeitig senden. CSMA/CD beugt Kollisionen vor und bestimmt die Regeln für das Verhalten im Falle eines Zusammenstoßes. Das CSMA/CD-Verfahren folgt folgenden Prinzipien:

1. Ein sendungsbereites Gerät lauscht, bis das Ethernet frei ist.
2. Wenn das Ethernet frei ist, beginnt das Gerät mit der Sendung des Frames.
3. Der Sender hört zu, um sicher zu gehen, dass keine Kollision erfolgt ist.
4. Falls eine Kollision stattgefunden hat, senden alle Stationen, die einen Frame gesandt haben, ein Störsignal, so dass alle Stationen den Vorfall bemerken.
5. Nach der Störungsmeldung aktiviert jeder Sender einen Timer und wartet die entsprechende Zeit ab.

6. Nachdem alle Timer abgelaufen sind, beginnt der Prozess erneut mit Schritt 1.

Es ist also notwendig, dass alle Geräte auf dem Ethernet das CSMA/CD-Verfahren verwenden, damit Kollisionen verhindert und gegebenenfalls beseitigt werden können.

### Repeater (Hubs)

Wie bei jedem anderen Netzwerk auch, war die maximale Kabellänge bei 10BASE5 und 10BASE2 begrenzt. Im Fall von 10BASE5 lag das Limit bei 500 Metern; bei 10BASE2 betrug die Maximallänge 185 mMeter. Interessanterweise geht der Name dieser beiden Ethernet-Typen auf die Maximallänge ihrer Segmente zurück – die letzte Ziffer im Namen 10BASE2, die 2, steht für die 185 Meter, da es sich fast um 200 Meter handelt. Auf diese Weise kommen die 5 und die 2 am Ende der beiden Namen zustande (die Ziffer multipliziert mit dem Faktor 100 ergibt die jeweilige Maximallänge).

In einigen Fällen reichten diese Längen nicht aus. Aus diesem Grund wurde ein Gerät namens *Repeater* entwickelt. Ein Problem bei der Verwendung längerer Segmente war, dass ein gesendetes Signal bei einem Kabelnetz von mehr als 500 beziehungsweise 185 Metern Länge zu schwach werden konnte. *Attenuation*, Abschwächung bedeutet, dass elektrische Signale, die einen Draht passieren, im Verlauf des zurückgelegten Wegs immer schwächer werden. Dahinter verbirgt sich das gleiche Prinzip wie in folgender Situation: Wenn jemand direkt neben Ihnen steht, können Sie gut verstehen, was diese Person sagt. Spricht diese Person aber in der gleichen Lautstärke vom anderen Ende des Raums zu Ihnen, haben Sie möglicherweise Probleme, sie zu verstehen. Der Grund dafür ist auch hier, dass die Schallwellen auf ihrem Weg vom Sprecher bis zu Ihrem Ohr schwächer geworden sind.

Repeater machen es möglich, dass mehrere Segmente verbunden werden, indem ein ankommendes Signal empfangen wird, die Bits als Nullen und Einsen interpretiert werden und daraufhin ein ganz neues, klares Signal erzeugt wird. Die Aufgabe des Repeaters ist es also nicht, das Signal einfach zu *verstärken*, denn das würde bedeuten, dass auch alle auf dem Weg entstandenen Störgeräusche verstärkt werden.

### ANMERKUNG

Da der Repeater nicht für die Deutung der Bits zuständig ist, sondern sie lediglich untersucht und elektrische Signale wiederholt, wird die Funktion des Repeaters dem Layer 1 zugeordnet.

Sie stellen sich möglicherweise jetzt die Frage, wozu Sie alle diese Vertiefungen zu Ethernet-Standards brauchen, wenn Sie doch niemals damit arbeiten werden? Ganz einfach, diese älteren Standards liefern einen guten Vergleich zu den heutigen und viele Eigenschaften dieser beiden älteren Netzwerkstandards haben sich bis heute erhalten. Erfahren Sie nun mehr über einen Ethernet-Standard, der heute noch gelegentlich in Produktionsnetzwerken vorkommt – 10BASE-T.

### 3.3.3 10BASE-T Ethernet

10BASE-T löste mehrere Probleme früherer Ethernet-Spezifikationen. 10BASE-T machte es möglich, die bereits installierten Telefonkabel oder – falls eine neue Verkabelung notwendig war – noch billigere und einfacher zu installierende Kabel zu benutzen. 10BASE-T-Netzwerke verwenden Geräte namens *Hubs*, wie in Bild 3.5 dargestellt.

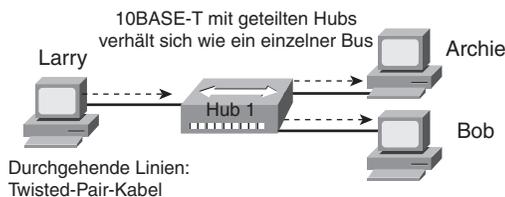


Bild 3.5: Kleines Ethernet-10BASE-T-Netzwerk

Das physikalische 10BASE-T-Ethernet verwendet Ethernet-Karten in den Computern, Kabel und einen Hub. Die Hubs, die zum Erstellen eines 10BASE-T-Ethernets benutzt werden, sind im Wesentlichen Repeater mit mehreren Ports. Das heißt, dass der Hub das in einem Port ankommende Signal einfach erneut generiert und dieses über jeden der anderen Ports wieder aussendet. Durch dieses Verfahren erzeugt 10BASE-T einen elektrischen Bus, genau wie 10BASE2 und 10BASE5. Darum kann es immer noch zu Zusammenstößen kommen, so dass CSMA/CD weiterhin notwendig ist.

Durch den Einsatz von 10BASE-T-*Hubs* erhält Ethernet eine weit größere Erreichbarkeit, verglichen mit 10BASE2 und 10BASE5, denn bei diesen beiden LAN-Typen konnte schon ein einfaches Kabelproblem ausreichen, um das ganze Netzwerk lahm zu legen. Beim 10BASE-T-Netzwerk wird von jedem Gerät ein Kabel zum Hub gelegt. Dadurch ist im Falle eines einfachen Kabelfehlers nur ein Gerät betroffen.

Das Konzept, jedes einzelne Gerät mit einem zentralen Hub zu verkabeln, der den gleichen elektrischen Bus wie bei älteren Ethernet-Typen erzeugte, war eines der Hauptmerkmale von 10BASE-T-Ethernet. Dadurch, dass das Konzept und die physikalische Realität eines einzelnen elektrischen Pfads

weitergeführt werden, der von allen Geräten geteilt wird, spricht man heute von einem geteilten Ethernet, einem *Shared Ethernet*: Sämtliche Geräte teilen sich einen einzigen 10-Mbit/s-Bus.

Es gibt eine Vielzahl von Begriffen, um die Topologie von Netzwerken zu beschreiben. Der Begriff *Star* (Stern) bezieht sich auf ein Netzwerk mit einem Zentrum, von dem sternförmig Verzweigungen abgehen – man muss sich das ungefähr wie bei einer Kinderzeichnung es Sterns vorstellen. Die Verkabelung eines 10BASE-T-Netzwerks folgt dem Prinzip dieser Sterntopologie, wie in Bild 3.5 dargestellt. Da der Hub das elektrische Signal über jeden Port wiederholt und aussendet, ist der Effekt jedoch, dass das Netzwerk wie bei einer Bus-Topologie arbeitet. 10BASE-T-Netzwerke haben also auf der physischen Ebene ein *sternförmiges* Netzwerk-Design, aber ebenso, auf der logischen Ebene, ein *Bus*-Netzwerk-Design. (Kapitel 11 vertieft die unterschiedlichen Netzwerk-Topologien und ihre Bedeutungen.)

### Die Verkabelung von Ethernet 10BASE-T

Die PCs und der Hub, die in Bild 3.5 dargestellt werden, sind mit den typischen UTP-Kabeln der Kategorie 5 mit RJ-45-Steckern ausgestattet. Letztere wurden bereits in Bild 3.2 dargestellt. Die Ethernet-Karten in jedem PC haben einen RJ-45-Stecker, genau wie der Hub. Bei diesen Steckern handelt es sich um eine verlängerte Version der Telefonstecker, die in den Vereinigten Staaten üblich sind, also jene, die das Telefon mit der Wandvorrichtung verbinden. Ethernet-Kabel zu verbinden, ist also genauso einfach wie ein neues Telefon anzuschließen.

Die Details, die sich hinter den spezifischen Kabeln der Hubverbindung verbergen, sind im realen Leben ebenso wichtig wie in Bezug auf das INTRO-Examen. Die Feinheiten der Spezifikationen werden in Kapitel 11 behandelt und die meisten typischen Standards an dieser Stelle. Sie können sich vielleicht noch daran erinnern, dass eine Besonderheit von Ethernet darin besteht, Drahtpaare mit den Kontakten 1 und 2 zum Datenempfang zu verwenden. Die PC-Ethernet-Karten verwenden die gleichen Stecker auf genau die gleiche Art.

Das Kabel, das die PCs mit dem Hub verbindet, wird *straight-through* genannt, wie in Bild 3.2 gezeigt. Bei einem Straight-Through-Kabel ist der auf der einen Seite mit Stecker 1 verbundene Draht auch auf der gegenüber liegenden Seite mit Stecker 1 verbunden, Stecker 2 ist über einen Draht auf der anderen Seite mit Stecker 2 verbunden und so weiter. Wenn Larry also Daten über die Stecker 1 und 2 sendet, empfängt der Hub die elektrischen Signale über das Straight-Through-Kabel auf den Steckern 1 und 2. Damit der Hub die Daten korrekt empfängt, muss er entsprechend gegensätzlich denken, genau wie ein PC. Anders gesagt: Der Hub empfängt Daten auf den

Steckern 1 und 2 und überträgt auf den Steckern 3 und 4. In Bild 3.6 wird dieses Prinzip verdeutlicht.

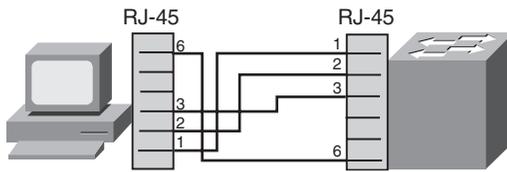


Bild 3.6: Straight-Through-Ethernet-Kabel

Larry sendet beispielsweise Daten über Stecker 1 und 2, und der Hub empfängt das Signal auf den Steckern 1 und 2. Der Hub wiederholt daraufhin das elektrische Signal und sendet es über alle ausgehenden Ports. Das Signal wird somit an Archie und Bob weitergesendet. Der Hub überträgt dabei das Signal über die Stecker 3 und 6 an das Kabel, das zu Archie und Bob führt, da Archie und Bob Daten auf Stecker 3 und 6 erwarten.

In einigen Fällen ist es notwendig, zwei Geräte direkt mit Ethernet zu verkabeln, wobei beide Geräte das gleiche Paar zur Datenübertragung nutzen. Sie wollen zum Beispiel zwei Hubs verbinden, aber beide Hubs senden über Stecker 3 und 6. Oder Sie wollen ein kleines Ethernet zwischen zwei PCs einrichten, einfach indem Sie die beiden PCs über ein Kabel verbinden – allerdings nutzen beide PCs die Stecker 1 und 2 zur Datenübertragung. Um dieses Problem zu lösen, brauchen Sie ein spezielles Kabel, ein so genanntes *Crossover*-Kabel. Dadurch hat Stecker 1 auf der einen Seite des Kabels nicht mehr Stecker 1 auf der anderen Seite als Gegenüber, sondern ist jetzt mit Stecker 3 verbunden. Stecker 2 ist nun statt mit Stecker 2 auf der anderen Seite mit Stecker 6 verbunden, Stecker 3 mit Stecker 1 und Stecker 6 mit Stecker 2. Bild 3.7 zeigt ein Beispiel für zwei PCs, die über ein Crossover-Kabel miteinander verbunden sind.

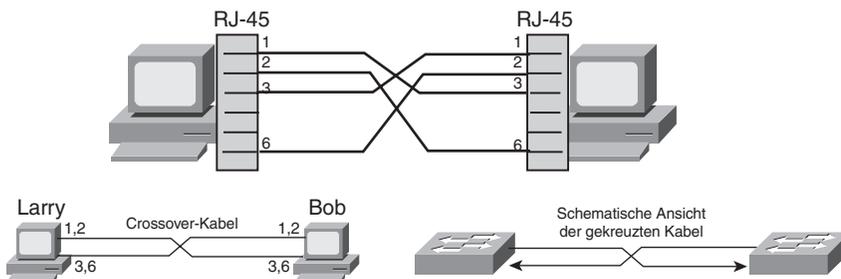


Bild 3.7: Crossover-Ethernet-Kabel

Sowohl Bob als auch Larry können über die Stecker 1 und 2 übertragen – gut so, denn das ist das Einzige, was eine Ethernet-Karte für einen Endcomputer tun kann. Da die Stecker 1 und 2 von Larry mit den Steckern 3 und 6 von Bob verbunden sind und da Bob auf den Steckern 3 und 6 Frames empfängt, verläuft der Empfang einwandfrei. Das Gleiche gilt für Frames, die Bob an Larry sendet – er sendet über die Stecker 1 und 2 und Larry empfängt über die Stecker 3 und 6.

Sie werden eher selten zwei Computer direkt mit einer Ethernet-Karte verbinden. Sie werden jedoch Crossover-Kabel für die Verbindungen von Switches mit Hubs verwenden. Ein Ethernet-Kabel zwischen zwei Hubs oder Switches nennt man *Trunk*. Bild 3.8 zeigt ein typisches Netzwerk mit zwei Switches in jedem Gebäude und den für jede Verbindung gebräuchlichen Kabeltypen.

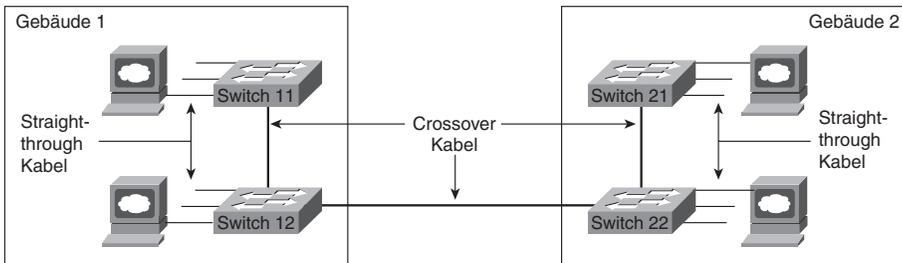


Bild 3.8: Typische Verwendungen von Straight-Through- und Crossover-Ethernet-Kabeln

### 10BASE-T Hubs

Im Vergleich zu 10BASE2- und 10BASE5-Netzwerken konnten einige Probleme der Verfügbarkeit durch den Einsatz von Hubs gelöst werden. Die Hubs bewirkten jedenfalls eine Reduktion der Netzwerkperformance bei erhöhter Belastung, so als ob 10BASE2 oder 10BASE5 benutzt würden, da 10BASE-T immer noch nur einen einzigen elektrischen Bus verwendete, der von allen Geräten auf dem LAN geteilt wurde. Ethernets, die einen Bus verwenden, können nicht die 100%-ige Leistung erbringen. Das liegt an Kollisionen und dem CSMA/CD-Arbitrationsverfahren. Um diese Leistungsschwächen auszuräumen, bestand der nächste Schritt darin, den Hub so intelligent zu machen, dass Kollisionen ganz vermieden werden – CSMA/CD wurde dadurch überflüssig.

Sie benötigen zunächst ein tiefgehendes Verständnis von 10BASE-T-Hubs, damit die Lösung dieses Stauproblems klarer wird. Bild 3.9 zeigt die Funktionsweise von Halbduplex-10BASE-T mit Hubs.

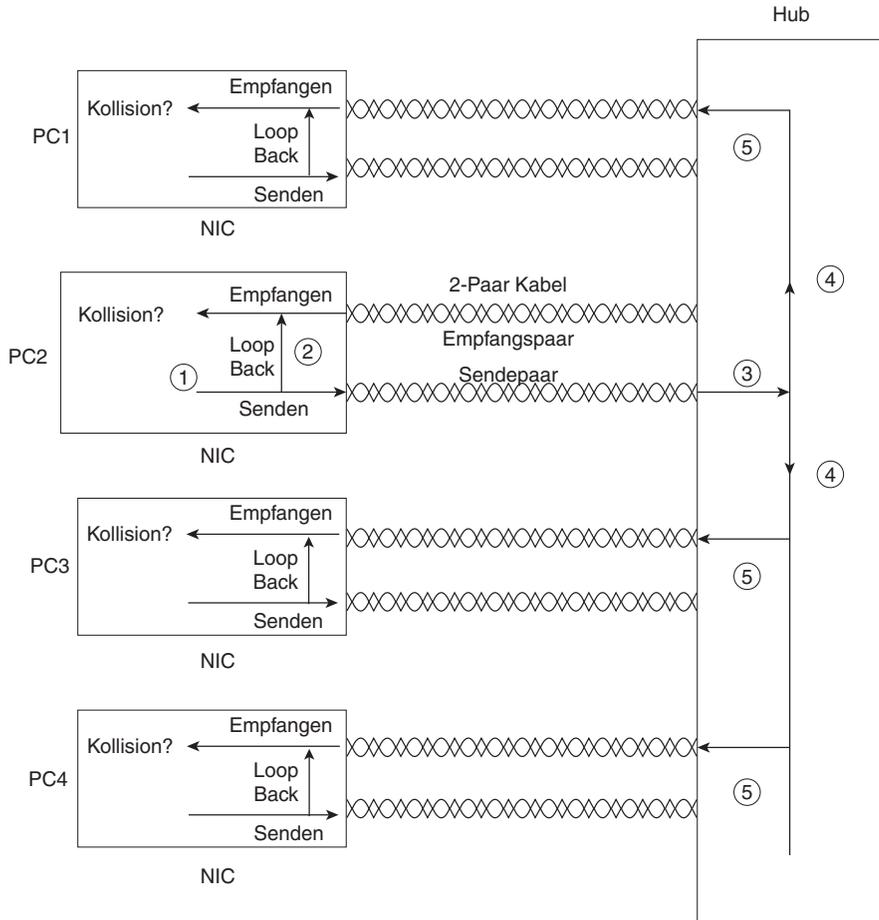


Bild 3.9: 10BASE-T Hub erzeugt einen elektrischen Bus, genau wie 10BASE2

In der Zeichnung können Sie sehen, wie ein 10BASE-T-Hub einen elektrischen Bus erzeugt. Die in Bild 3.9 illustrierten Schritte folgen chronologisch aufeinander:

1. Die NIC-Karte (Netzwerk-Interface-Karte) sendet einen Frame.
2. Die NIC sendet den gesandten Frame als Loop intern auf ihr Empfangspaar.
3. Der Hub empfängt den Frame.
4. Die Drähte im Hub senden das Signal an alle anderen Ports weiter, jedoch nicht zurück zu dem Port, der das Signal empfangen hat.
5. Der Hub wiederholt das Signal für jedes Empfangspaar der anderen Geräte.

In der Abbildung sehen Sie die Funktionsweise des Hubs im Einzelnen. Ein Gerät sendet und es gibt keine Kollision. Wenn PC1 und PC2 gleichzeitig einen Frame schicken, würde normalerweise ein Zusammenstoß erfolgen. Gemäß den Schritten 4 und 5 würde der Hub beide elektrischen Signale weiterleiten. Das hätte zur Folge, dass die überlappenden Signale an alle NICs gesendet werden würden. Da also Kollisionen auftauchen können, ist die CSMA/CD-Logik immer noch notwendig, damit PC1 und PC2 abwarten und es bei Gelegenheit wieder versuchen.

#### ANMERKUNG

PC2 würde auf Grund seines Loopback-Schaltkreises auf der NIC eine Kollision wahrnehmen. Der Hub sendet das Signal, das PC2 ihm gesandt hat, nicht an PC2 zurück. Statt dessen loopt jede NIC den gesendeten Frame, der auf ihr eigenes Empfangspaar zurückgeschickt wird, wie in Schritt 2 der Abbildung dargestellt. Weil PC2 und PC1 zur gleichen Zeit einen Frame senden, wird das Signal von PC1 vom Hub an PC2 weitergeleitet, an das Empfangspaar von PC2. Das aus der Richtung des Hubs kommende Signal und das Loopback-Signal der NIC von PC2 signalisieren PC2, dass es eine Kollision gibt. Wen interessiert das? Nun, um die Vollduplex-LAN-Funktion einschätzen zu lernen, müssen Sie etwas über die Loopback-Eigenschaft der NICs wissen.

### 3.3.4 Performance-Fragen bei Kollisions- und Duplex-Anordnungen

10BASE2, 10BASE5, und 10BASE-T-Ethernet könnten ohne CSMA/CD nicht funktionieren. Dennoch wird Ethernet bei starker Auslastung immer leistungsschwächer. Das ist auf das CSMA/CD-Verfahren zurückzuführen. In den Jahren, bevor LAN-Switches diesem Phänomen ein Ende setzten, galt die Faustregel, dass ein Ethernet-Netz merklich abbaute, sobald mehr als 30 Prozent des Netzwerks in Betrieb war.

Im folgenden Abschnitt werden Sie von zwei Dingen erfahren, die entscheidend zur Verbesserung der Netzwerkleistung beigetragen haben. Beide verfolgten die gleiche Absicht, nämlich die Reduktion oder, möglichst, die Verhinderung von Kollisionen: LAN Switching and Vollduplex-Ethernet.

#### Reduktion von Kollisionen durch LAN-Switching

Der Begriff *Kollisionsdomäne* bezeichnet alle Geräte, die für mögliche Kollisionen von Frames verantwortlich werden könnten. Alle Geräte auf einem 10BASE2-, 10BASE5- oder 10BASE-T-Netzwerk, die einen Hub benutzen,

stellen ein Kollisionsrisiko für Frames dar, die sie senden. Alle Geräte in Bild 3.9 liegen zum Beispiel in der gleichen Kollisionsdomäne.

LAN-Switches lösen das Problem der Kollisionen und des CSMA/CD-Verfahrens. Switches erzeugen im Gegensatz zu einem Hub keinen einfachen Bus, der von allen Geräten geteilt wird, sondern betrachten jeden physikalischen Port als einen eigenständigen Bus. Switches benutzen Pufferspeicher, um ankommende Frames zwischenspeichern. Wenn also zwei angeschlossene Geräte gleichzeitig einen Frame senden, kann der Switch einen Frame weiterleiten und den anderen so lange im Zwischenspeicher halten, bis der Weg wieder frei ist. Sie sehen in Bild 3.10, wie Kollisionen verhindert werden können.

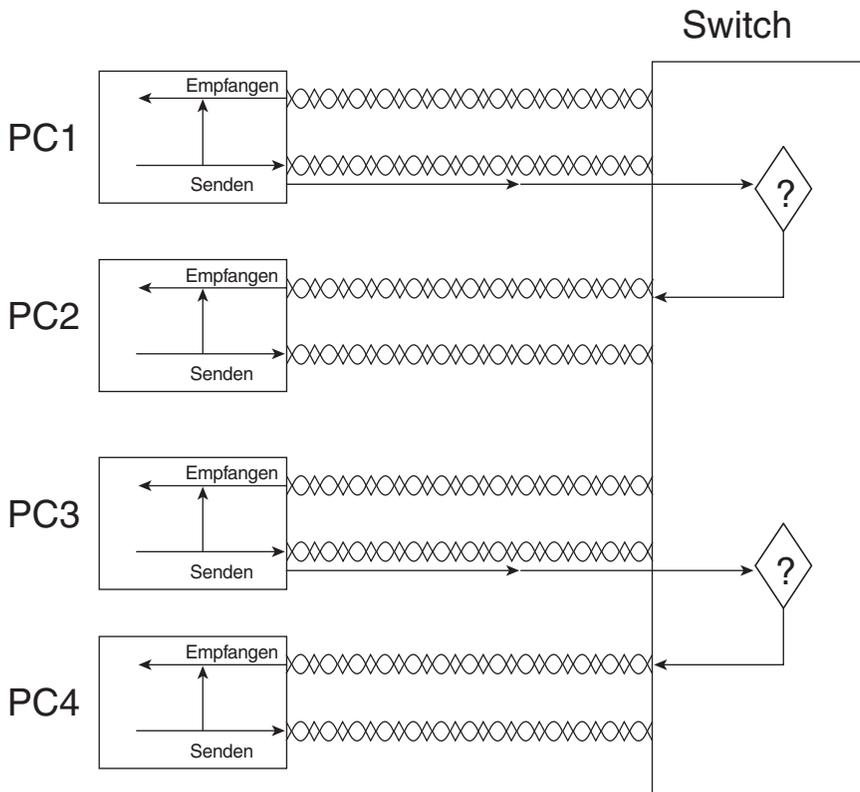


Bild 3.10: Grundlegende Switch-Funktionen

In Bild 3.10 senden PC1 und PC3 zur selben Zeit. Der Switch sieht sich die Ethernet-Zieladresse an und sendet im gleichen Moment einen Frame von PC1 an PC2 und einen Frame von PC3 an PC4. Der große Unterschied zwischen dem Hub und dem Switch besteht darin, dass der Switch das elektri-

sche Signal als einen Ethernet-Frame interpretiert und ihn verarbeitet, um eine Entscheidung zu treffen. (Die Einzelheiten der Ethernet-Adressierung und des Ethernet-Framings werden in den nächsten beiden Abschnitten behandelt.) Ein Hub wiederholt einfach das elektrische Signal (Layer 1), aber versucht nicht, es als LAN-Frame zu deuten (Layer 2). Ein Hub führt also genau genommen eine Funktion von OSI-Layer 1 aus, wenn er lediglich ein elektrisches Signal wiederholt. Ein Switch arbeitet dagegen auf OSI-Layer 2. Er interpretiert die Informationen in den Ethernet-Headern, insbesondere die Adressen, um die richtige Entscheidung für die Weiterleitung eines Datenpaketes zu treffen.

Das Buffering (die Zwischenspeicherung im Pufferspeicher) hilft ebenfalls, Kollisionen zu vermeiden. Stellen Sie sich vor, dass sowohl PC1 als auch PC3 zur gleichen Zeit einen Frame an PC4 senden. Der Switch weiß, dass ein Weiterleiten beider Frames an PC4 einen Zusammenstoß verursachen würde und hält deshalb einen Frame zurück (Buffering), bis die Weiterleitung des ersten Frames an PC4 vollständig abgeschlossen ist.

Zwei Eigenheiten des Switching bescheren dem Ethernet große Leistungsverbesserungen, verglichen mit Hubs:

- Wenn nur ein Gerät mit jedem Port eines Switches verkabelt ist, können keine Kollisionen erfolgen. Wenn keine Kollisionen erfolgen können, kann CSMA/CD ausgeschaltet werden, was das Ethernet-Problem löst.
- Es muss nicht jeder Switch-Port die Bandbreite teilen, sondern er hat seine eigene separate Bandbreite. Das bedeutet, dass ein Switch mit 10 Mbit/s-Ports eine Bandbreite von 10 Mbit/s *pro Port* hat.

LAN-Switching bedeutet also eine beachtliche Leistungssteigerung für Ethernet-LANs. Der nächste Abschnitt behandelt ein anderes Thema, das die Ethernet-Leistung real verdoppelt.

### Ausschluss von Kollisionen, um Vollduplex-Ethernet zu ermöglichen

Die ursprünglichen Ethernet-Spezifikationen benutzten einen geteilten Bus, über welchen lediglich ein Frame zu einer gegebenen Zeit gesendet werden konnte. Somit war es unmöglich, dass ein einzelnes Gerät einen Frame senden und gleichzeitig einen Frame empfangen konnte, denn dies führte zu einem Zusammenstoß. Die Geräte entschlossen sich also, einfach keinen Frame zu senden, wenn sie gerade einen Frame empfangen. Man nennt dieses Verfahren *Halbduplex*-Logik.

Ethernet-Switches ermöglichen, dass mehrere Frames über verschiedene Ports gleichzeitig gesendet werden können. Ist nur ein Gerät an einen Switch-Port angeschlossen, kann außerdem unmöglich eine Kollision erfol-

gen. Mit anderen Worten: LAN-Switches mit nur einem Gerät an jedem ihrer Ports machen *Vollduplex*-Übertragungen möglich. Das bedeutet, dass eine Ethernet-Karte gleichzeitig senden und empfangen kann. Betrachten Sie Bild 3.11. Es stellt eine Vollduplex-Schaltung dar, mit einem einzigen PC, der an einen LAN-Switch angeschlossen ist.

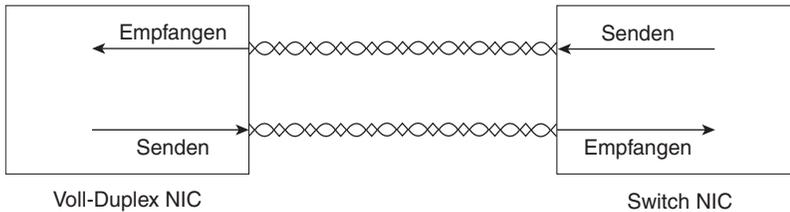


Bild 3.11: 10BASE-T-Vollduplex-Setting mit einem Switch

In einer Vollduplex-Situation können Daten mit voller Geschwindigkeit simultan in beide Richtungen fließen – in diesem Fall 10 Mbit/s. Um dies zu ermöglichen, muss die NIC-Karte ihre Loopback-Funktion deaktivieren.

Sie haben jetzt wesentliche Grundlagen der zwölfjährigen Entwicklung von Ethernet kennen gelernt. Tabelle 3.4 fasst die Schlüsselfunktionen zusammen, die in diesem Kapitel dargestellt wurden.

Tabelle 3.4: Zusammenfassung wichtiger Ethernet-Funktionen

Ethernet-Umgebung	Beschreibung
10BASE2, 10BASE5	Einzelner Bus, der seriell zwischen Geräten mit Koaxialkabeln liegt. Wird heute kaum verwendet.
10BASE-T mit einem Hub	Ein elektrischer Bus wird unter mehreren Geräten aufgeteilt, wobei eine Kollisionsdomäne entsteht. Die verdrehten Twisted-Pair-Kabel sind in einer Stern-Topologie angeordnet.
10BASE-T mit einem Switch	Ein elektrischer Bus pro Switch-Port erzeugt mehrere Kollisionsdomänen. Die Anordnung der Kabel folgt physisch der Stern-Topologie, logisch handelt es sich aber um eine Bus-Topologie mit Twisted-Pair-Verkabelung.
Halbduplex	Logik, die von einer Karte verlangt, zu einem gegebenen Zeitpunkt entweder nur zu senden oder nur zu empfangen. Wird zur Vermeidung von Kollisionen eingesetzt.
Vollduplex	Logik, bei der gleichzeitiges Senden und Empfangen möglich ist. Funktioniert, wenn ein Gerät mit einem Switch-Port verbunden ist und dadurch sichergestellt wird, dass keine Kollisionen entstehen können.

## 3.4 Ethernet Datenverbindungs-Protokolle

Eine der bedeutendsten Stärken der Protokolle aus der Ethernet-Familie liegt darin, dass diese Protokolle das gleiche kleine Set von Datenverbindungs-Protokollen nutzen. Ethernet-Adressierung verläuft beispielsweise auf allen Ethernet-Variationen gleich, sogar auf einem 10BASE5-Ethernet. In diesem Abschnitt erfahren Sie die meisten Details der Ethernet-Datenverbindungs-Protokolle.

### 3.4.1 Ethernet-Adressierung

Bei der Ethernet-LAN-Adressierung wird entweder ein individuelles Gerät oder Gruppen von Geräten auf einem LAN-Netzwerk identifiziert. *Unicast* Ethernet-Adressen identifizieren eine einzelne LAN-Karte. Jede Adresse hat eine Länge von 6 Bytes, wird normalerweise in Hexadezimalzahlen geschrieben und bei Cisco-Geräten typischerweise durch Punkte unterteilt, so dass vier Stellen der Hexadezimalzahlen zusammengefasst sind. 0000.0C12.3456 ist zum Beispiel eine gültige Ethernet-Adresse. Die Begriffe *Unicast-Adressen* oder *individuelle Adressen* werden benutzt, um eine individuelle LAN-Interface-Karte zu identifizieren. (Der Begriff *Unicast* wurde hauptsächlich gewählt, um einen Kontrast zu den Begriffen *Broadcast*, *Multicast* und *Gruppenadressen* herzustellen.)

Computer benutzen diese Adressen, um den Sender oder Empfänger eines Ethernet-Frames zu identifizieren. Stellen Sie sich beispielsweise vor, dass Fred und Barney sich auf dem gleichen Ethernet befinden und Fred an Barney einen Frame sendet. Fred fügt seine eigene Ethernet-MAC-Adresse als Quelladresse in den Ethernet-Header und benutzt Barneys Ethernet-MAC-Adresse als Zieladresse. Wenn Barney den Frame empfängt, bemerkt er, dass die Zieladresse seine eigene MAC-Adresse ist. Also weiß er, dass er den Frame weiterleiten soll. Wenn Barney einen Frame mit der Unicast-Adresse eines anderen Gerätes als Bestimmungsadresse erhält, leitet er den Frame einfach nicht weiter.

Die IEEE ist für das Format und die Zuweisung von LAN-Adressen zuständig. Sie verlangt allgemein einheitliche Unicast-MAC-Adressen auf allen LAN-Interface-Karten. (Die IEEE nennt sie MAC-Adressen, da die MAC-Protokolle wie zum Beispiel IEEE 802.3 die Details der Adressen festlegen.) Um eine einheitliche MAC-Adresse zu haben, versehen die Hersteller von Ethernet-Karten die MAC-Adresse mit einem Code auf der Karte, gewöhnlich in einem ROM-Chip. In der ersten Hälfte der Adresse wird der Hersteller der Karte angegeben. Dieser Code, der jedem Hersteller durch die IEEE zugewiesen wird, wird *OUI* (*organizationally unique identifier*) genannt.

Jeder Hersteller fügt in die erste Hälfte einer MAC-Adresse seinen eigenen OUI-Code ein. In der zweiten Hälfte der Adresse fügt er eine einmalig verwendete Nummer ein, so dass Überschneidungen mit anderen Karten ausgeschlossen sind.

Für Unicast-LAN-Adressen existieren viele Begriffe. Jede LAN-Karte wird mit einer *BIA* (*burned-in address*) geliefert. Die Bezeichnung für diese Adresse stammt daher, dass sie in den ROM-Chip auf der Karte eingebrannt ist. Die BIAs werden manchmal auch *UAAs* (*universally administered addresses*) genannt, da die IEEE die Zuweisung der Adressen universell (naja, zumindest weltweit) verwaltet. Unabhängig davon, ob die BIA verwendet oder eine andere Adresse konfiguriert wird, denken viele Leute bei Unicast-Adresse entweder an LAN-Adressen, Ethernet-Adressen oder MAC-Adressen.

*Gruppen-Adressen* identifizieren mehrere LAN-Interface-Karten. Die IEEE legt allgemein zwei Kategorien von Gruppen-Adressen für Ethernet fest:

- **Broadcast-Adressen** – Die am häufigsten verwendete der IEEE-MAC-Adressen-Gruppen. Ihr Wert ist FFFF.FFFF.FFFF (Hexadezimal-Schreibweise). Die Broadcast-Adresse impliziert, dass alle Geräte auf dem LAN den Frame weiterleiten.
- **Multicast-Adressen** – Durch Verwendung von Multicast-Adressen kann ein bestimmter Teil der Geräte auf dem LAN miteinander kommunizieren. Einige Anwendungen müssen mit einer Vielzahl anderer Geräte kommunizieren. Wenn eine Anwendung einen Frame sendet, können alle Geräte, die bestimmt sind, die Daten zu empfangen, diese weiterleiten, während der Rest sie einfach ignorieren kann. Das IP-Protokoll unterstützt Multicasting. Wenn IP über das Ethernet multicasted, folgen die von IP verwendeten Multicast-MAC-Adressen folgendem Format: 0100.5exx.xxxx, wobei x für einen beliebigen Wert steht.

Tabelle 3.5 fasst die meisten Details zu den MAC-Adressen zusammen.

*Tabelle 3.5: LAN-MAC-Adresen: Terminologie und Eigenschaften*

LAN-Adressen-Bezeichnungen und Eigenschaften	Beschreibung
MAC	Media Access Control. 802.3 (Ethernet) und 802.5 (Token Ring) sind die MAC-Unterslayer für diese beiden LAN-Datenverbindungs-Protokolle.
Ethernet-Adresse, NIC-Adresse, LAN-Adresse, Token Ring-Adresse, Kartenadresse	Weitere Bezeichnungen, die oft für <i>MAC-Adressen</i> verwendet werden. Diese Begriffe beschreiben die 6-Byte-Adresse auf der LAN-Interface-Karte.

Tabelle 3.5: LAN-MAC-Adresen: Terminologie und Eigenschaften (Forts.)

LAN-Adressen-Bezeichnungen und Eigenschaften	Beschreibung
BIA (Burned-in address)	Die vom Hersteller der Karte bezeichnete 6-Byte-Adresse. Sie wird normalerweise in einen ROM- oder EEPROM-Chip auf der LAN-Karte eingebrannt und beginnt mit einem 3 Bytes langen OUI (organizationally unique identifier), der von der IEEE zugewiesen wird.
Unicast-Adresse	Modebegriff für eine MAC-Adresse, die ein einzelnes LAN-Interface repräsentiert.
Broadcast-Adresse	Eine Adresse, die »alle Geräte, die auf diesem LAN jetzt gerade existieren« bezeichnet.
Multicast-Adressen	Nicht gültig für Token Ring. Auf Ethernet impliziert eine Multicast-Adresse eine Unterkategorie von allen aktuellen Geräten auf dem LAN.

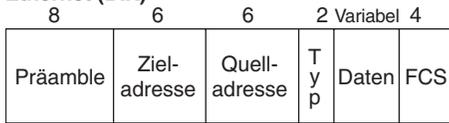
### 3.4.2 Ethernet-Framing

Beim *Framing* wird festgelegt, wie eine Folge von binären Zahlen interpretiert wird. Mit anderen Worten: Framing legt die Bedeutungen fest, die sich hinter den über das Netz gesendeten Bits verbergen. Mit Hilfe des physikalischen Layers können Sie eine Bitkette von einem Gerät zum anderen übertragen. Aber wie soll diese am Empfangsgerät interpretiert werden? Der Begriff *Framing* geht auf die Definition der Felder zurück, die in den empfangenden Daten enthalten sind. Framing bestimmt also die Bedeutung der Bits, die über ein Netzwerk übertragen und empfangen werden.

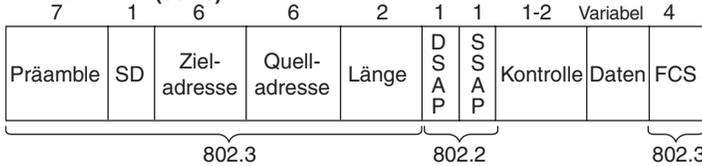
Sie erinnern sich an die Situation, dass Fred über ein Ethernet Daten an Barney sendet? Fred fügt Barneys Ethernet-Adresse in den Ethernet-Header ein, damit dieser weiß, dass der Frame für ihn bestimmt ist. Der IEEE 802.3 Standard legt fest, wo das Feld für die Zieladresse innerhalb der über das Ethernet laufenden Bitkette liegt. Bild 3.12 zeigt die Details von verschiedenen Typen von LAN-Frames.

Es ist vielleicht nicht jedes kleine Feld in diesen Frames von Interesse, aber Sie sollten sich zumindest an einige Details der Header- und Trailer-Inhalte erinnern. Vor allem die Adressen und ihre Standorte in den Headern sind wichtig, genau wie die Namen der Felder, die den Datentyp innerhalb des Ethernet-Frames bezeichnen – es handelt sich hauptsächlich um die Felder Typ, DSAP, und SNAP. Auch die Tatsache, dass ein FCS-Feld im Trailer vorkommt, ist bedeutend.

**Ethernet (DIX)**



**IEEE Ethernet (802.3)**



**IEEE 802.3 mit SNAP-Header**

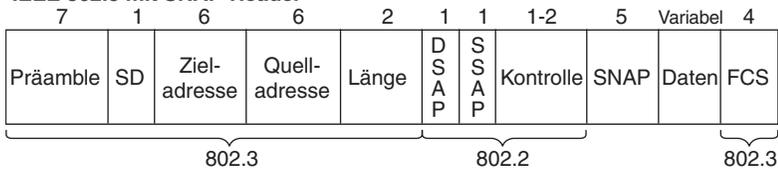


Bild 3.12: Formate von LAN-Headern

Die IEEE 802.3-Spezifikation begrenzt die Datenmenge für einen 802.3-Frame auf ein Maximum von 1500 Bytes. Das Datenfeld wurde entwickelt, um Layer 3-Pakete zu beinhalten. Der Begriff *MTU (maximum transmission unit)* legt die maximale Größe der Layer 3-Pakete fest, die über ein Medium gesendet werden können. Da das Layer 3-Paket immer innerhalb des Datenfelds eines Ethernet-Frames bleibt, ist ein IP-Paket mit 1500 Bytes das größte erlaubte Paket auf einem Ethernet.

### 3.4.3 Daten-Identifizierung innerhalb eines Ethernet-Frames

Jeder Datenverbindungs-Header hat ein Feld mit einem Code in seinem Header, welcher den Typen des folgenden Protokoll-Headers festlegt. Das DSAP-Feld (Destination Service Access Point) im ersten Frame in Bild 3.13 hat zum Beispiel einen Wert von E0. Das bedeutet, dass der folgende Header ein Novell-IPX-Header sein wird. Warum das so ist? Nun, die IEEE kreierte 802.2. Man erkannte den Bedarf an einem Protokolltypen-Feld. Es sollte die innerhalb des Feldes enthaltenen so genannten »Daten« in einem IEEE-Ethernet-Frame identifizieren können.

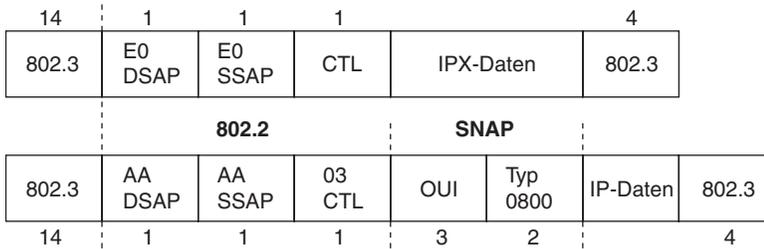


Bild 3.13: 802.2 SAP- und SNAP-Typenfelder

Die IEEE nannte ihr Typenfeld DSAP (*destination service access point*). Als sie erstmals den 802.2-Standard entwickelte, konnte jeder, der über die nötigen Mittel verfügte, seine Lieblingsprotokolle bei der IEEE registrieren lassen und einen reservierten Wert erhalten, um das DSAP-Feld zu identifizieren. So registrierte Novell beispielsweise IPX, worauf ihr durch die IEEE »E0« (hexadezimal) zugewiesen wurde. Die IEEE hatte jedoch keine große Anzahl von Protokollen im Sinn – sie täuschte sich. Es stellte sich heraus, dass das 1 Byte lange DSAP-Feld nicht groß genug ist, um die Bezeichnungen für alle Protokolle unterzubringen.

Um sich der erhöhten Anzahl von Protokollen anzupassen, erlaubte die IEEE, einen Extra-Header zu verwenden, einen SNAP-Header (*Subnetwork Access Protocol*). Beim zweiten Frame in Bild 3.13 sehen Sie ein DSAP-Feld mit dem Wert AA. Daraus geht hervor, dass dem 802.2-Header ein SNAP-Header folgt. Der SNAP-Header hat ein 2 Bytes langes Protokoll-Typenfeld. Das SNAP-Protokolltypen-Feld erfüllt den gleichen Zweck wie das DSAP-Feld, aber da es 2 Bytes lang ist, können alle Protokolle identifiziert werden. In Bild 3.13 hat das SNAP-Typenfeld zum Beispiel einen Wert von 0800, was bedeutet, dass es sich bei dem nächsten Header um einen IP-Header gemäß RFC 1700 handelt. Im Bereich »Assigned Numbers« – zugewiesene Nummern – ([www.isi.edu/in-notes/rfc1700.txt](http://www.isi.edu/in-notes/rfc1700.txt)) werden die Werte der SAP- und SNAP-Typenfelder und die Protokolltypen, die sie enthalten, aufgelistet.

Tabelle 3.6 fasst die Felder zusammen, die zur Identifizierung der im Frame enthaltenen Daten genutzt werden.

Tabelle 3.6: Protokoll-Typenfelder in LAN-Headern

Feldname	Länge	LAN-Typ
Ethernet-Typ	2 Bytes	DIX Ethernet
802.2 DSAP und SSAP	jeweils 1 Byte	IEEE Ethernet, IEEE Token Ring, ANSI FDDI
SNAP-Protokoll	2 Bytes	IEEE Ethernet, IEEE Token Ring, ANSI FDDI

Zwei mögliche Werte im Ethernet-Typfeld und im SNAP-Protokollfeld sind 0800 für IP und 8137 für NetWare. Beispiele für IEEE-SAP-Werte sind E0 für NetWare, 04 für SNA und AA für SNAP. Interessanterweise hat die IEEE keinen DSAP-Wert für TCP/IP reserviert. Um TCP/IP über IEEE-Ethernet zu unterstützen, müssen SNAP-Header verwendet werden.

### 3.4.4 Zusammenfassung zum Layer 2-Ethernet

Wie an früherer Stelle in diesem Kapitel bereits erwähnt, bestimmen Protokolle auf dem physikalischen Layer, wie Daten über ein physikalisches Medium gesendet werden. Datenverbindungs-Protokolle machen ein physikalisches Netzwerk nutzbar, indem sie festlegen, wie und wann das physikalische Netzwerk verwendet wird. Ethernet bestimmt Funktionen von OSI-Layer 1. Dazu zählen die Verkabelung, die Steckverbindungen, die Stromstärken, die Festlegung darüber, wie lang die Entfernungen der Kabel sein dürfen und einige wichtige Funktionen von OSI-Layer 2. In diesem Abschnitt wurden vier der Eigenschaften auf der Daten Verbindungsebene hervorgehoben, wie Tabelle 3.7 verdeutlicht.

*Tabelle 3.7: Zusammenfassung der OSI-Layer 2-Eigenschaften: Ethernet*

OSI Layer 2-Funktionen	Ethernet-Implementierung
Arbitration	CSMA/CD-Verfahren
Adressierung	6 Bytes lange MAC-Adressen
Fehlererkennung	FCS im Ethernet-Trailer
Identifizierung des Pakettypen innerhalb eines Frames	Protokoll-Typ (2 Bytes) – DIX Ethernet DSAP (1 Byte) – IEEE 802.2 SNAP Protokoll-Typ (2 Bytes) – IEEE 802.2 mit SNAP-Header

## 3.5 Jüngste Ethernet-Standards

In den meisten modernen Netzwerken würden Sie 10BASE2 oder 10BASE5 nicht einsetzen – tatsächlich hätten Sie wahrscheinlich noch nicht einmal mehr viele 10BASE-T-Hubs in Ihrem Netzwerk. Jüngere Alternativen wie Fast Ethernet und Gigabit Ethernet bieten schnellere Ethernet-Versionen zu vernünftigen Preisen an. Beide haben heutzutage eine hohe Akzeptanz in Netzwerklösungen, wobei Fast Ethernet meistens auf dem Schreibtisch und Gigabit Ethernet zwischen Netzwerkgeräten oder auf Servern zum Einsatz kommt. Zudem bedeuten 10 Gigabyte noch eine beachtliche Steigerung von Geschwindigkeit und Leistung. Auf den letzten Aspekt wird in Kapitel 11 kurz eingegangen.

### 3.5.1 Fast Ethernet

Fast Ethernet, in IEEE 802.3u festgelegt, enthält viele vertraute Eigenschaften von 10 Mbit/s schnellen IEEE 802.3 Ethernet-Varianten. Die uralte CSMA/CD-Logik existiert immer noch, kann jedoch in Vollduplex-Punkt-zu-Punkt-Topologien, bei denen keine Kollisionen stattfinden können, ausgeschaltet werden. Die Spezifikation 802.3u verlangt die Verwendung der alten IEEE-802.3-MAC- und 802.2-LLC-Framing-Regeln für LAN-Header und Trailer. Es ist eine Vielzahl von Kabel-Optionen erlaubt – nicht abgeschirmte und abgeschirmte Kupferkabel genauso wie verschiedene Glasfaserkabel. Unter Fast Ethernet können sowohl geteilte Hubs als auch Switches verwendet werden.

Zwei Haupteigenschaften, die Fast Ethernet von einem 10 Mbit/s Ethernet unterscheiden, sind höhere Bandbreite und Autonegotiation. Fast Ethernet arbeitet mit 100 Mbit/s – mehr muss nicht gesagt werden. Der andere Hauptunterschied, Autonegotiation, ermöglicht einer Ethernet-Karte oder einem Ethernet-Switch, dynamisch Verbindungseigenschaften auszuhandeln. Dadurch wird vereinbart, ob mit 10 oder 100 Mbit/s gesendet wird. Aus diesem Grund werden viele Ethernet-Karten und Switch-Ports 10/100-Karten genannt, da sie die Geschwindigkeit aushandeln können. Die Endpunkte vereinbaren selbstständig, ob Halb-Duplex oder Voll-Duplex eingesetzt wird. Wenn die Autonegotiation versagt, wird automatisch Halb-Duplex mit 10 Mbit/s gewählt.

Der Autonegotiations-Prozess ist bekannt für seine Ausfälle. Cisco empfiehlt bei Geräten, die selten bewegt werden – wie Server und Switches – die LAN-Switches und die damit verbundenen Geräte fest mit den gewünschten Werten zu konfigurieren. Hier sollte man sich nicht auf die Autonegotiation verlassen. Autonegotiation wird von Cisco für Switch-Ports empfohlen, die mit Endgeräten auf der Benutzerseite verbunden sind, so dass sich daher häufig Veränderungen ergeben, zumindest im Vergleich zu Servern und anderen Netzwerkgeräten, wie zum Beispiel Routern.

### 3.5.2 Gigabit Ethernet

IEEE definiert Gigabit Ethernet in den Standards 802.3z für die optische und 802.3ab für die elektrische Verkabelung. Wie Fast Ethernet enthält Gigabit Ethernet noch viele vertraute Eigenschaften von langsameren Ethernet-Varianten. CSMA/CD wird immer noch benutzt und kann zur Vollduplex-Unterstützung deaktiviert werden. Die Spezifikationen 802.3z und 802.3ab verlangen die Verwendung der alten IEEE-802.3-MAC- und 802.2-LLC-Framing-Regeln für LAN-Header und Trailer. Der wahrscheinlichste Einsatzort für Gigabit ist zwischen Switches, zwischen Switches und einem Router und zwischen einem Switch und einem Server.

Gigabit Ethernet ähnelt seinen langsameren Cousins unter mehreren Gesichtspunkten. Die größte Ähnlichkeit ist, dass die gleichen Header und Trailer verwendet werden, unabhängig davon, ob die Daten mit 10 Mbit/s, 100 Mbit/s, oder 1000 Mbit/s fließen. Wenn Sie verstehen, wie Ethernet bei 10 und 100 Mbit/s funktioniert, kennen Sie schon das meiste, was Sie über Gigabit Ethernet wissen müssen.

Gigabit Ethernet unterscheidet sich von langsameren Ethernet-Spezifikationen darin, wie es die Signale kodiert auf das Kabel schickt. Gigabit Ethernet ist offensichtlich schneller, mit einer Geschwindigkeit von 1000 Mbit/s, oder 1 Gbit/s.

## Grundlagen-Zusammenfassung

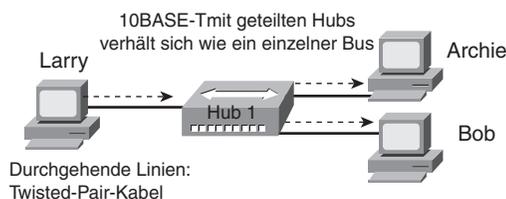
Die »Grundlagen-Zusammenfassung« fasst immer die wichtigsten Inhalte jedes Kapitels zusammen. Obwohl dieser Abschnitt nicht alles auflistet, was in Ihrem CCNA-Examen vorkommen kann, sollte ein gut vorbereiteter Prüfungskandidat ein Minimum an Details von jeder »Grundlagen-Zusammenfassung« kennen, bevor er sich zum Examen anmeldet.

Tabelle 3.8 listet die verschiedenen Protokollspezifikationen für die drei ursprünglichen IEEE LAN-Standards auf.

*Tabelle 3.8: MAC- und LLC-Details für drei Typen von LANs*

Name	Spezifikation MAC-Sublayer	Spezifikation LLC-Sublayer
Ethernet Version 2 (DIX Ethernet)	Ethernet	–
IEEE Ethernet	IEEE 802.3	IEEE 802.2
IEEE Token Ring	IEEE 802.5	IEEE 802.2
ANSI FDDI	ANSI X3T9.5	IEEE 802.2

Bild 3.14 stellt Verkabelung und Grundfunktion eines Ethernet-Netzwerks dar, das aus 10BASE-T-Verkabelung und einem Ethernet-Hub besteht.



*Bild 3.14: Kleines Ethernet 10BASE-T Netzwerk*

In den Bildern 3.15 und 3.16 werden Ethernet-Straight-Through- und Crossover-Kabel dargestellt.

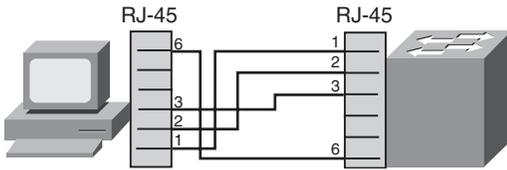


Bild 3.15: Straight-Through-Ethernet-Kabel

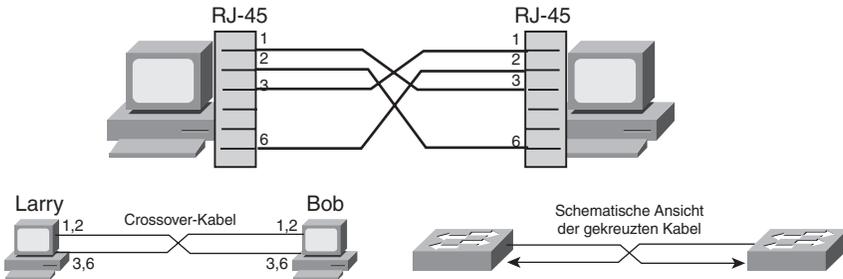


Bild 3.16: Crossover-Ethernet-Kabel

Vollduplex-Ethernet-Karten können zeitgleich senden und empfangen. Bild 3.17 zeigt die Vollduplex-Schaltung, die einen einzelnen PC mit einem LAN-Switch verbindet.



Bild 3.17: 10BASE-T Vollduplex-Schaltung

Tabelle 3.9 fasst einige Hauptpunkte zusammen. Sie beziehen sich auf die Themen, die am Anfang des Kapitels behandelt wurden.

Tabelle 3.9: Zusammenfassung wichtiger Ethernet-Eigenschaften

Ethernet-Umgebung	Beschreibung
10BASE2, 10BASE5	Einzelner Bus, der seriell zwischen Geräten mit Koaxialkabeln liegt. Wird heute kaum verwendet.
10BASE-T mit einem Hub	Ein elektrischer Bus wird unter mehreren Geräten aufgeteilt, wobei eine Kollisionsdomäne entsteht. Die verdrehten Twisted-Pair-Kabel sind in einer Stern-Topologie angeordnet.
10BASE-T mit einem Switch	Ein elektrischer Bus pro Switch-Port erzeugt mehrere Kollisionsdomänen. Die Anordnung der Kabel folgt physisch der Stern-Topologie, logisch handelt es sich aber um eine Bus-Topologie mit Twisted-Pair-Verkabelung.
Halb-Duplex	Logik, die von einer Karte verlangt, zu einem gegebenen Zeitpunkt entweder nur zu senden oder nur zu empfangen. Wird zur Vermeidung von Kollisionen eingesetzt.
Voll-Duplex	Logik, bei der gleichzeitiges Senden und Empfangen möglich ist. Funktioniert, wenn ein Gerät mit einem Switch-Port verbunden ist und dadurch sichergestellt wird, dass keine Kollisionen entstehen können.

Bild 3.18 zeigt die Einzelheiten von mehreren Typen von LAN-Frames.

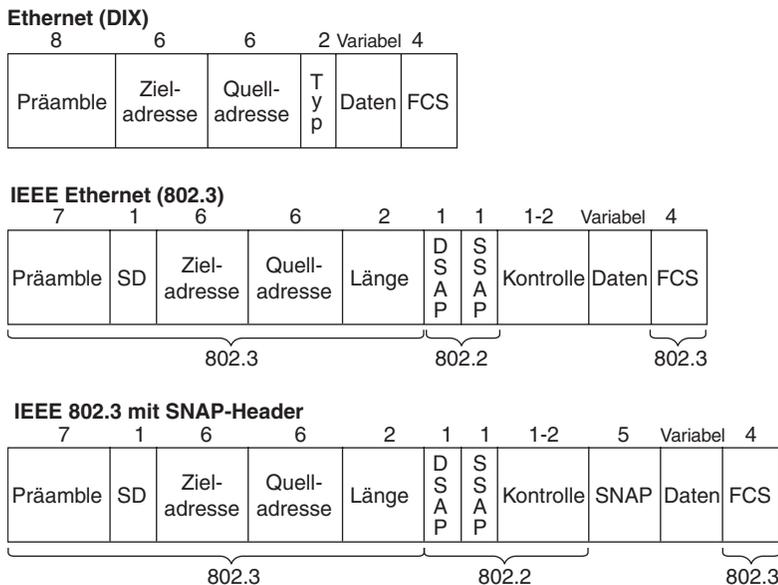


Bild 3.18: LAN-Header-Formate

Tabelle 3.10 fasst die Felder zusammen, die zur Identifizierung der in einem Frame enthaltenen Datentypen verwendet werden.

*Tabelle 3.10: Protokolltypen-Felder in LAN-Headern*

Feldname	Länge	LAN-Typ
Ethernet-Typ	2 Bytes	DIX Ethernet
802.2 DSAP und SSAP	jeweils 1 Byte	IEEE Ethernet, IEEE Token Ring, ANSI FDDI
SNAP-Protocol	2 Bytes	IEEE Ethernet, IEEE Token Ring, ANSI FDDI

Ethernet definiert auch viele wichtige OSI-Layer 2-Funktionen. In diesem Kapitel wurden vier dieser Eigenschaften hervorgehoben, wie in Tabelle 3.11 noch einmal zusammengefasst wird.

*Tabelle 3.11: Zusammenfassung der OSI-Layer 2-Eigenschaften: Ethernet*

OSI Layer 2-Funktionen	Ethernet-Implementierung
Arbitration	CSMA/CD-Verfahren
Adressierung	6 Bytes lange MAC-Adressen
Fehlererkennung	FCS im Ethernet-Trailer
Identifizierung des Pakettypen innerhalb eines Frames	Protokoll-Typ (2 Bytes) – DIX Ethernet DSAP (1 Byte) – IEEE 802.2 SNAP Protokoll-Typ (2 Bytes) – IEEE 802.2 mit SNAP-Header

## Q&A

Wie in der Einleitung erwähnt, haben Sie zwei Möglichkeiten, die folgenden Fragen zu beantworten. Diese stellen eine größere Herausforderung für Sie dar, als das Examen selbst. Die Lösung ist nicht so eindeutig festgelegt wie bei den Examensfragen. Durch diese offeneren, schwierigeren Fragen werden Sie mit der Thematik des Kapitels noch besser vertraut. Die Antworten zu den Fragen finden Sie in Anhang A.

Wenn Sie Fragen bearbeiten möchten, wie sie im Examen auf Sie zukommen, können Sie sich auf der Prüfungs-CD mit den Multiple-Choice-Fragen und dem Router-Simulator beschäftigen.

1. Welchen Zweck oder welche Zwecke erfüllt Layer 2 hauptsächlich?
2. Welchen Zweck oder welche Zwecke erfüllt Layer 1 hauptsächlich?

3. Wofür steht das Kürzel MAC?
4. Nennen Sie drei Begriffe, die gerne als Synonyme für MAC-Adressen verwendet werden.
5. In welchem Teil der MAC-Adresse befindet sich ein Code, an dem der Kartenhersteller zu erkennen ist?
6. Werden MAC-Adressen durch ein Layer 2 oder ein Layer 3 Protokoll definiert?
7. Wieviele Bits enthält eine MAC-Adresse?
8. Nennen Sie die beiden Hauptteile einer MAC-Adresse. An welchem Teil ist abzulesen, zu welcher »Gruppe« die Adresse gehört?
9. Welcher OSI-Layer ist unter Verwendung von einem Header und einem Trailer typischerweise für Einkapselungen zuständig?
10. Kann eine NIC-Karte in einem Fast Ethernet zeitgleich einen Frame empfangen und senden?
11. Worin bestehen die beiden Hauptunterschiede zwischen einer 10-Mbit/s-NIC-Karte und einer 10/100-NIC-Karte?
12. Welche Länge darf ein einzelnes Kabel unter 10BASE-T höchstens haben? Welche unter 100 BASE-TX?
13. Wie schnell ist Fast Ethernet?
14. Wieviele Bytes ist eine MAC-Adresse lang?
15. Definieren Sie den Unterschied zwischen Broadcast- und Multicast-MAC-Adressen.
16. Erklären Sie, welche Funktion die Features Loopback und Kollisionserkennung auf einer Ethernet-NIC-Karte in Bezug auf Halb- und Voll-duplex-Schaltungen haben.