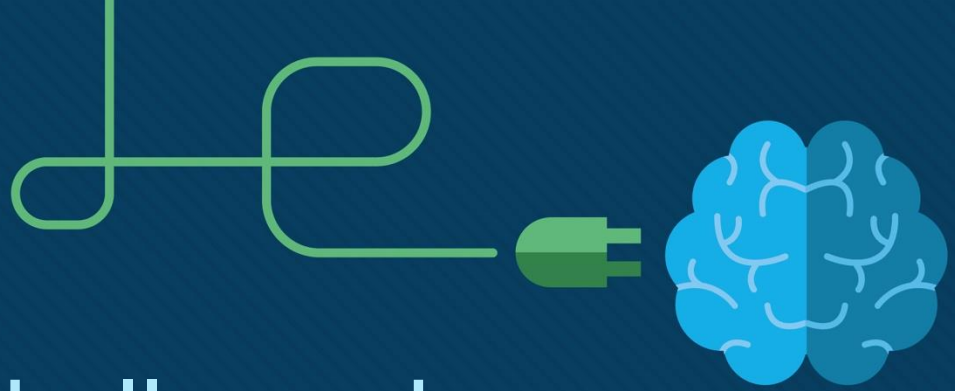
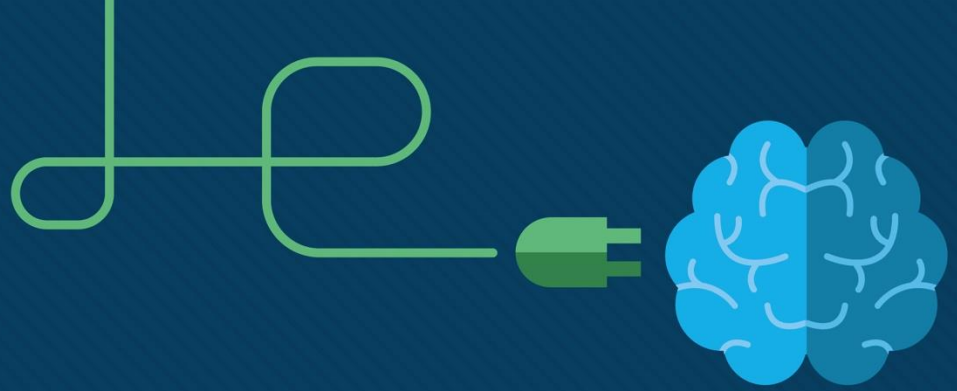


Modul 3: Protokolle und Modelle

Material für Instruktoren

Einführung in die Netzwerktechnik v7.0 (ITN)



Modul 3: Protokolle und Modelle

Einführung in die Netzwerktechnik v7.0 (ITN)

Modulziele

Modultitel: Protokolle und Modelle

Modulziel: Erläutern Sie, wie Netzwerkprotokolle Geräten den Zugriff auf lokale und Remote-Netzwerkressourcen ermöglichen.

Thema	Ziel
Die Regeln	Beschreiben Sie die Arten von Regeln, die für eine erfolgreiche Kommunikation erforderlich sind.
Protokolle	Erklären Sie, warum Protokolle in der Netzwerkkommunikation notwendig sind.
Protokollfamilien	Erläutern Sie den Zweck der Einhaltung einer Protokollfamilie.
Standardisierungsorganisationen	Erläutern der Rolle von Standardisierungsorganisationen und Etablierung von Protokollen zum Erleichtern der Interoperabilität in der Netzkommunikation
Referenzmodelle	Erläutern Sie, wie das TCP/IP-Modell und das OSI-Modell verwendet werden, um die Standardisierung im Kommunikationsprozess zu erleichtern.
Datenkapselung	Erläutern Sie, wie die Datenkapselung es ermöglicht, Daten über das Netzwerk zu transportieren.
Datenzugriff	Erläutern Sie, wie lokale Hosts auf lokale Ressourcen in einem Netzwerk zugreifen.

Klassenaktivität – Entwurf eines Kommunikationssystems

Entwurf eines Kommunikationssystems

Ziele:

- Erläutern der Rolle von Protokollen und Standardorganisationen zum Erleichtern der Interoperabilität in der Netzkommunikation

3.1 Die Regeln

Die Regeln
Video — Geräte in einer Blase

In diesem Video werden die Protokolle erläutert, die Geräte verwenden, um ihren Platz im Netzwerk zu sehen und mit anderen Geräten zu kommunizieren.

Kommunikationsgrundlagen

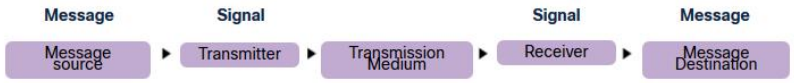
Netzwerke können in Größe und Komplexität variieren. Es ist nicht genug, eine Verbindung zu haben, Geräte müssen sich darauf einigen, „wie“ Sie kommunizieren.

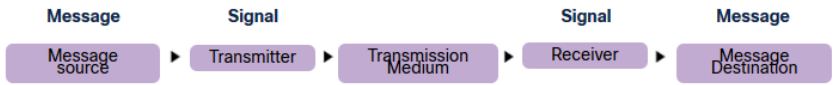
Es gibt drei Elemente für jede Kommunikation:

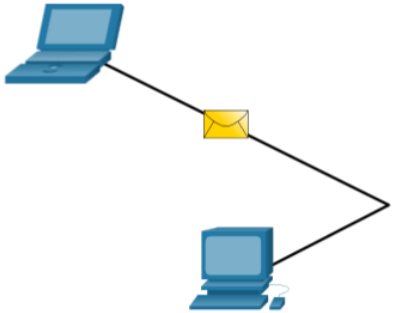
- Es gibt eine Quelle (Absender).
- Es gibt ein Ziel (Empfänger).
- Es gibt einen Kanal (Medium), der den Kommunikationspfad vorsieht.

Kommunikationsprotokolle

- Alle Kommunikationen werden durch Protokolle geregelt.
- Protokolle sind die Regeln, nach denen die Kommunikation erfolgt.
- Diese Regeln variieren je nach Protokoll.







Festlegen von Regeln

- Menschen müssen festgelegte Regeln oder Vereinbarungen einhalten, nach denen eine Unterhaltung abläuft.
- Die erste Nachricht ist schwer zu lesen, da sie nicht richtig formatiert ist. Die zweite zeigt die Nachricht, die richtig formatiert ist

```
humans communication between govern rules. It is verydifficult tounderstand messages that are not
correctly formatted and donot follow the established rules and protocols. A estrutura da
gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por
muitos individuos diferentes.
```

```
Rules govern communication between humans. It is very difficult to understand messages that are
not correctly formatted and do not follow the established rules and protocols. The structure of
the grammar, the language, the punctuation and the sentence make the configuration humanly
understandable for many different individuals.
```

Festlegen von Regeln

Protokolle müssen die folgenden Anforderungen erfüllen:

- Bekannter Absender und Empfänger
- Eine gemeinsame Sprache und Grammatik
- Geschwindigkeit und zeitliche Steuerung der Übertragung
- Anforderungen an Bestätigung oder Rückmeldung

Netzwerkprotokollanforderungen

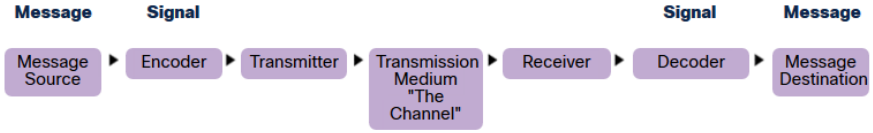
Gemeinsame Computerprotokolle müssen übereinstimmen und folgende Anforderungen enthalten:

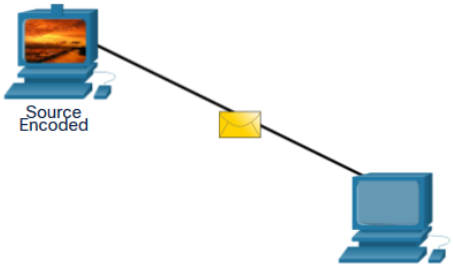
- Nachrichtenkodierung
- Nachrichtenformatierung und -kapselung
- Nachrichtengröße
- Zeitliche Steuerung von Nachrichten
- Nachrichtenübermittlungsoptionen

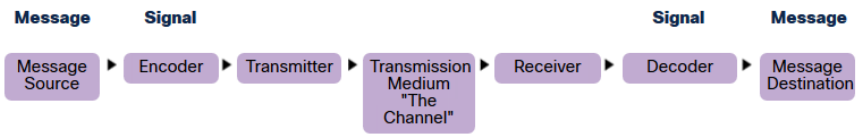
Die Regeln

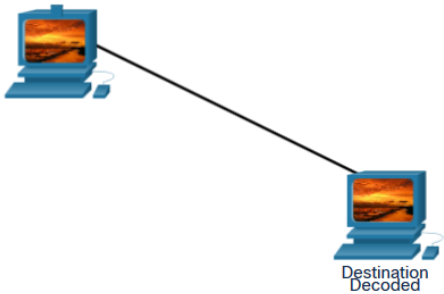
Nachrichtenkodierung

- Die Kodierung ist der Umwandlungsprozess von Informationen in eine andere für die Übermittlung geeignete Form.
- Bei der Dekodierung wird dieser Prozess umgekehrt, um die Informationen zu interpretieren.



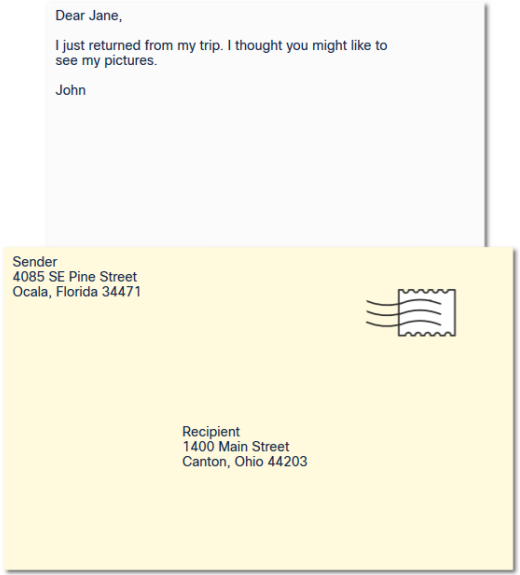


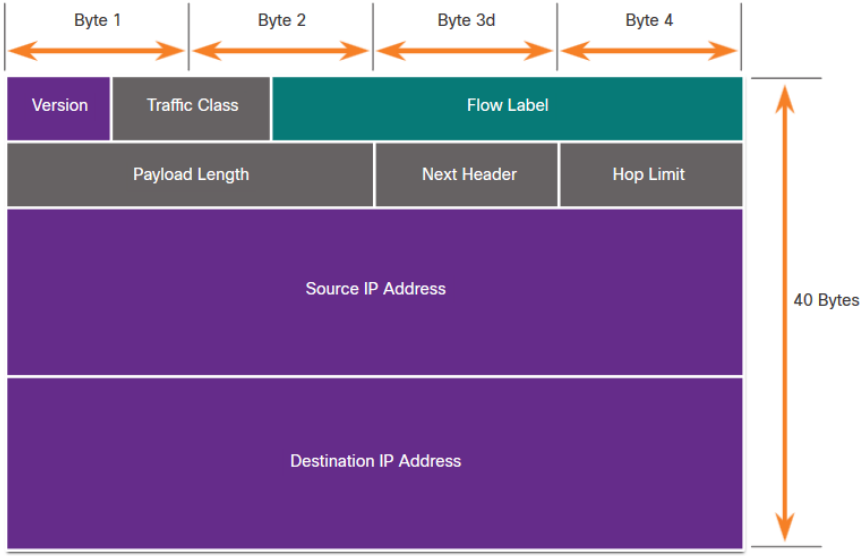




Nachrichtenformatierung und Kapselung

- Wenn eine Nachricht von einer Quelle zu einem Ziel gesendet werden soll, muss sie ein bestimmtes Format oder eine bestimmte Struktur einhalten.
- Das Nachrichtenformat hängt vom Nachrichtentyp und dem für die Übertragung genutzten Kanal ab.

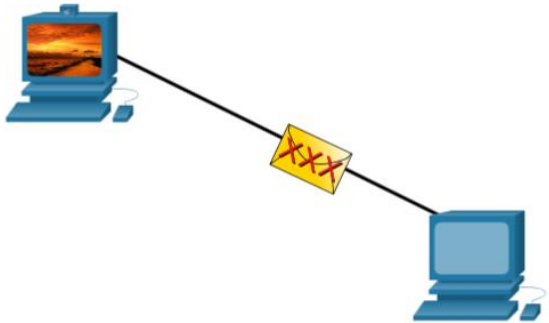


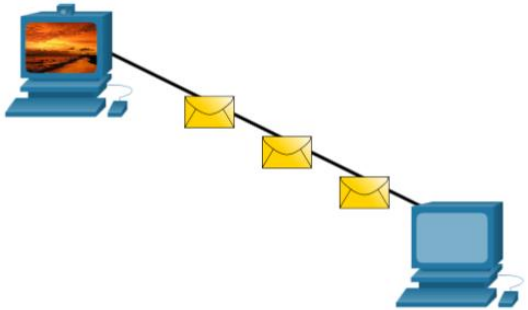


Nachrichtengröße

Die Kodierung zwischen Hosts muss in einem für das Medium geeigneten Format geschehen.

- Nachrichten, die über das Netzwerk geschickt werden, müssen zunächst vom Absender in Bits umgewandelt werden.
- Die Bits werden in ein Muster aus Licht, Klängen oder elektrischen Impulsen umgewandelt.
- Der Zielhost empfängt und dekodiert die Signale, um die Nachricht interpretieren zu können.





Zeitliche Steuerung von Nachrichten

Zeitliche Steuerung von Nachrichten umfasst folgendes:

Flusskontrolle— Verwaltet die Datenübertragungsrate und definiert, wie viele Informationen gesendet werden können und wie schnell sie geliefert werden können.

Antwort-Zeitüberschreitung — Verwaltet, wie lange ein Gerät wartet, wenn es keine Antwort vom Ziel hört.

Zugriffsmethode —legt fest, wann jemand eine Nachricht senden darf.

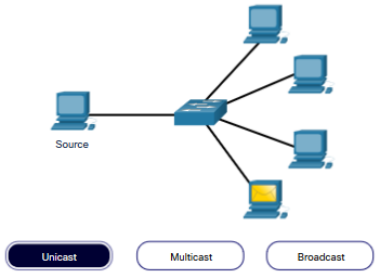
- Es kann verschiedene Regeln für Probleme wie „Kollisionen“ geben. Dies ist der Fall, wenn mehrere Geräte gleichzeitig Daten senden und die Nachrichten beschädigt werden.
- Einige Protokolle sind proaktiv und versuchen, Kollisionen zu verhindern; andere Protokolle sind reaktiv und stellen nach der Kollision eine Wiederherstellungsmethode ein.

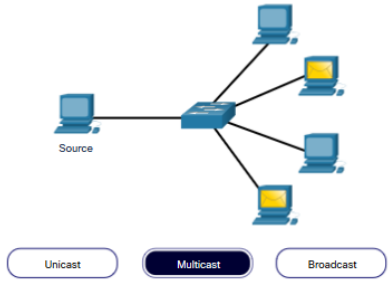
Nachrichtenübermittlungsoptionen

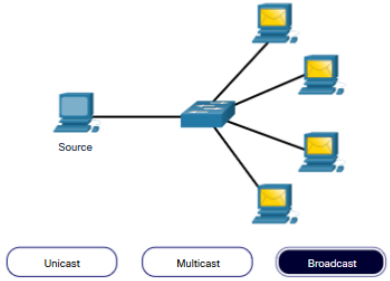
Die Nachrichten können auf verschiedene Weise zugestellt werden:

- **Unicast —** eins zu eins Kommunikation
- **Multicast —** eins zu vielen, normalerweise nicht alle
- **Broadcast** — eins zu allen

Hinweis: Broadcasts werden in IPv4-Netzwerken verwendet, sind jedoch keine Option für IPv6. Später werden wir auch „Anycast“ sehen als zusätzliche Bereitstellungsoption für IPv6.

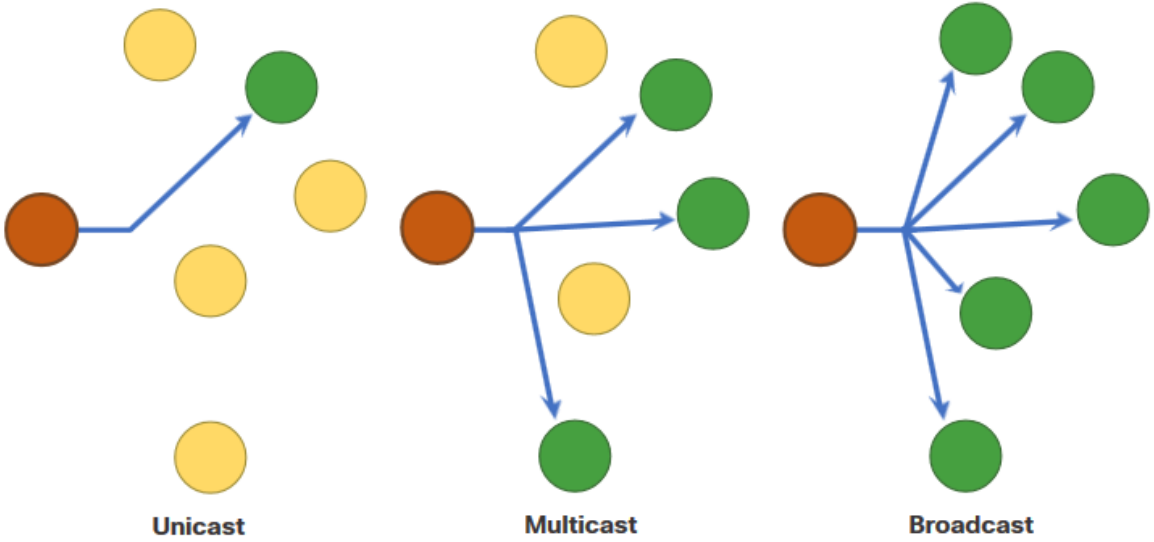






Eine Notiz zum Knotensymbol

- Dokumente können das Knotensymbol, normalerweise einen Kreis, verwenden, um alle Geräte darzustellen.
- Die Abbildung veranschaulicht die Verwendung des Knoten-Symbols für Zustellungsoptionen.



3.2 Protokolle

Netzwerkprotokoll Überblick

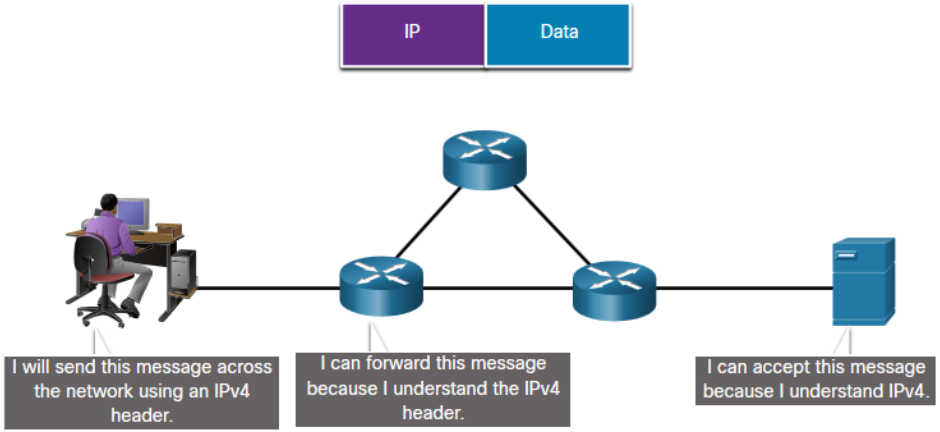
Netzwerkprotokolle definieren einen gemeinsamen Regelsatz.

- Kann auf Geräten implementiert werden in:
  - Software
  - Hardware
  - Beidem
- Protokolle haben ihre eigenen:
  - Funktion
  - Format
  - Regeln

Protokolltyp	Beschreibung
Netzwerkkommunikation	die Kommunikation von zwei oder mehr Geräten über ein oder mehrere Netzwerke ermöglichen
Netzwerk Sicherheit	sichere Daten für Authentifizierung, Datenintegrität und Datenverschlüsselung
Routing	ermöglicht den Routern Routerinformationen auszutauschen, Pfadinformationen zu vergleichen und den besten Pfad auszuwählen
Serviceerkennung	dient zur automatischen Erkennung von Geräten oder Diensten

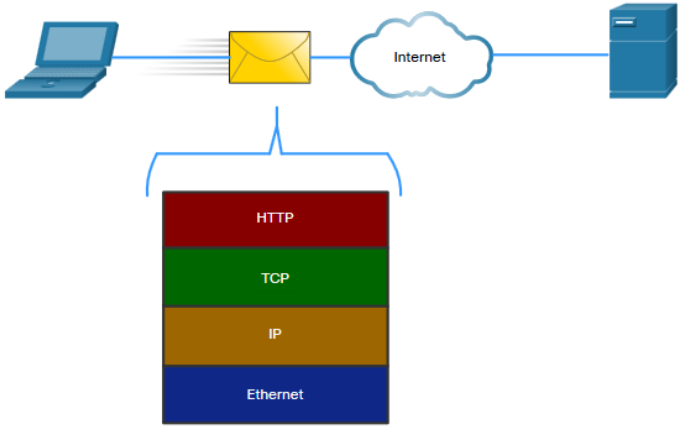
Netzwerkprotokoll — Funktionen

- Geräte verwenden vereinbarte Protokolle zur Kommunikation.
- Protokolle können eine oder mehrere Funktionen haben.



Funktion	Beschreibung
Adressierung	Bekannter Absender und Empfänger
Zuverlässigkeit	Garantierte Übertragung
Flusskontrolle	Sorgt für effiziente Datenflüsse
Sequenzierung	Beschriftet jedes übertragene Datensegment eindeutig
Fehlererkennung	Bestimmt, ob Daten während der Übertragung beschädigt wurden
Anwendungsschnittstelle	Prozess-zu-Prozess-Kommunikation zwischen Netzwerkanwendungen

Protokollzusammenspiel



- Netzwerke erfordern die Verwendung mehrerer Protokolle.
- Jedes Protokoll hat seine eigene Funktion und Format.

Protokoll	Funktion
Hypertext Transfer Protocol (HTTP)	▪ Regelt, wie ein Webserver und ein Web-Client interagieren. ▪ Definiert Inhalt und Format
Transmission Control Protocol (TCP)	▪ Verwaltet die einzelnen Gespräche ▪ Garantierte Übertragung ▪ Verwaltet die Flusssteuerung
Internet Protocol (IP)	Überträgt Nachrichten global vom Absender an den Empfänger
Ethernet	Überträgt Nachrichten von einer Netzwerkkarte an eine andere Netzwerkkarte im selben Ethernet-Lan (Local Area Network)

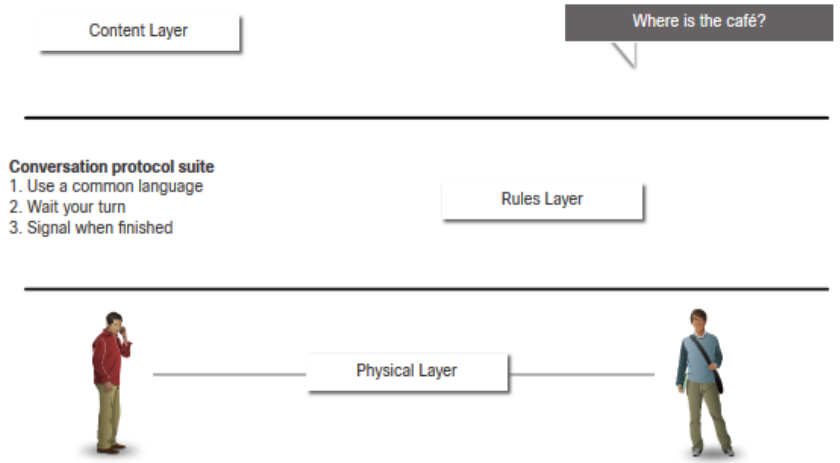
3.3 Protokollfamilien

Netzwerkprotokollfamilien

Protokolle müssen in der Lage sein, mit anderen Protokollen zu arbeiten.

Protokollfamilie:

- Eine Gruppe zusammenhängender Protokolle, die für die Ausführung der Kommunikation benötigt werden, wird als Protokollfamilie bezeichnet.
- Regelwerke, die zusammenarbeiten, um ein Problem zu lösen.



Protocol suites are sets of rules that work together to help solve a problem.

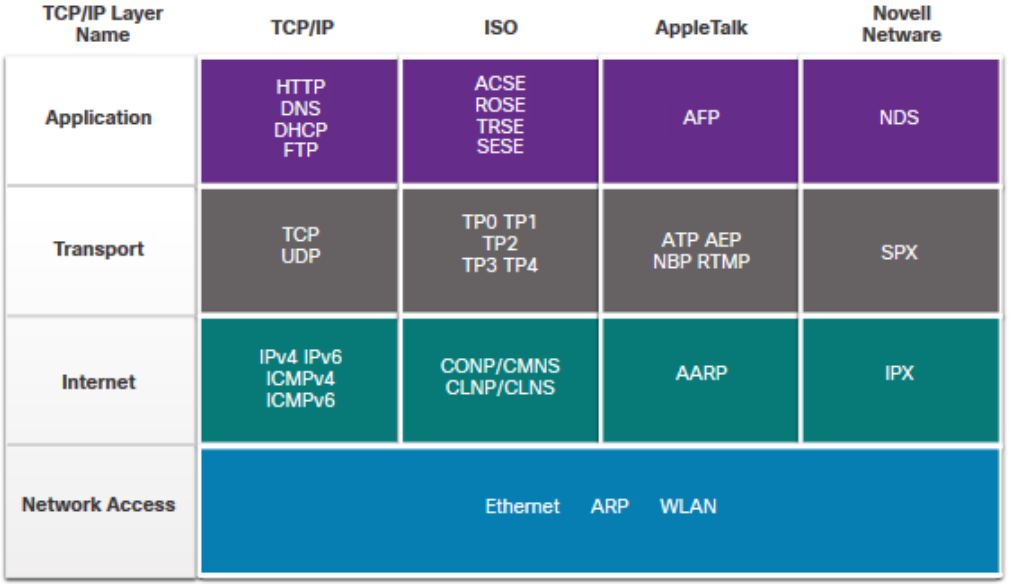
Die Protokolle werden in Bezug auf Schichten betrachtet:

- Höhere Ebenen
- Tiefere Ebenen - Befassen sich mit dem Verschieben von Daten und Bereitstellung von Diensten für die oberen Schichten

Entwicklung von Protokollfamilien

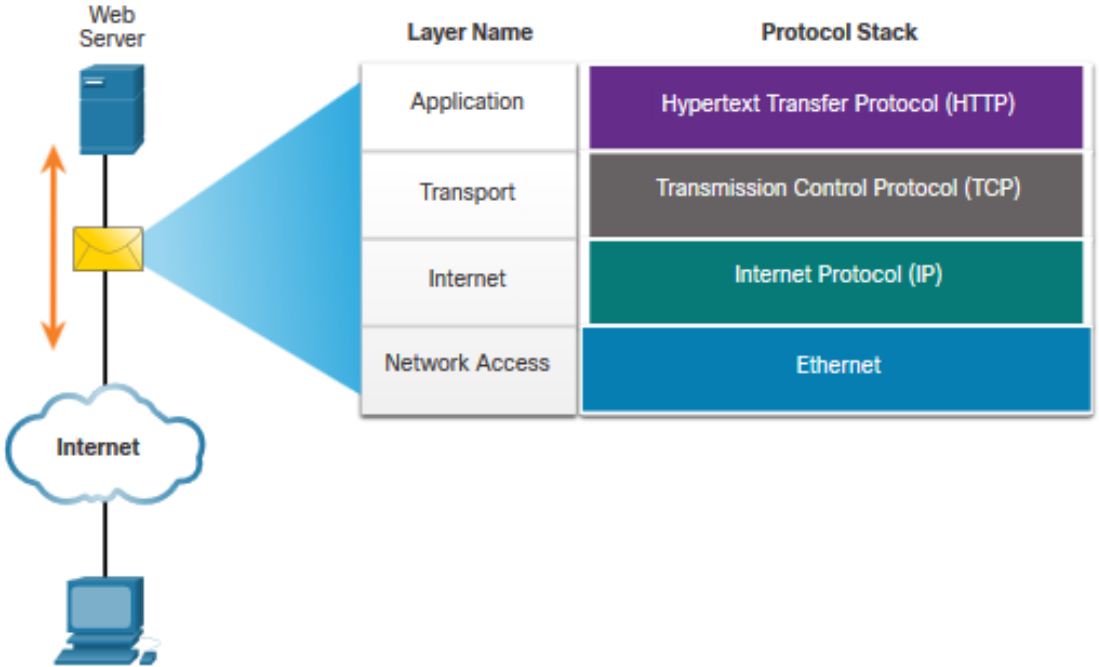
Es gibt mehrere Protokollfamilien.

- **Internet Protokollfamilie oder TCP/IP -** Die gängigste Protokollfamilie, die von der Internet Engineering Task Force (IETF) verwaltet **wird**
- **Open Systems Interconnection (OSI) Protokolle -** Entwickelt von der International Organization for Standardization (ISO) und der International Telecommunications Union (ITU)
- **AppleTalk —** Proprietäre Suite von Apple Inc.
- **Novell NetWare-** Proprietäre Familie entwickelt von Novell Inc.



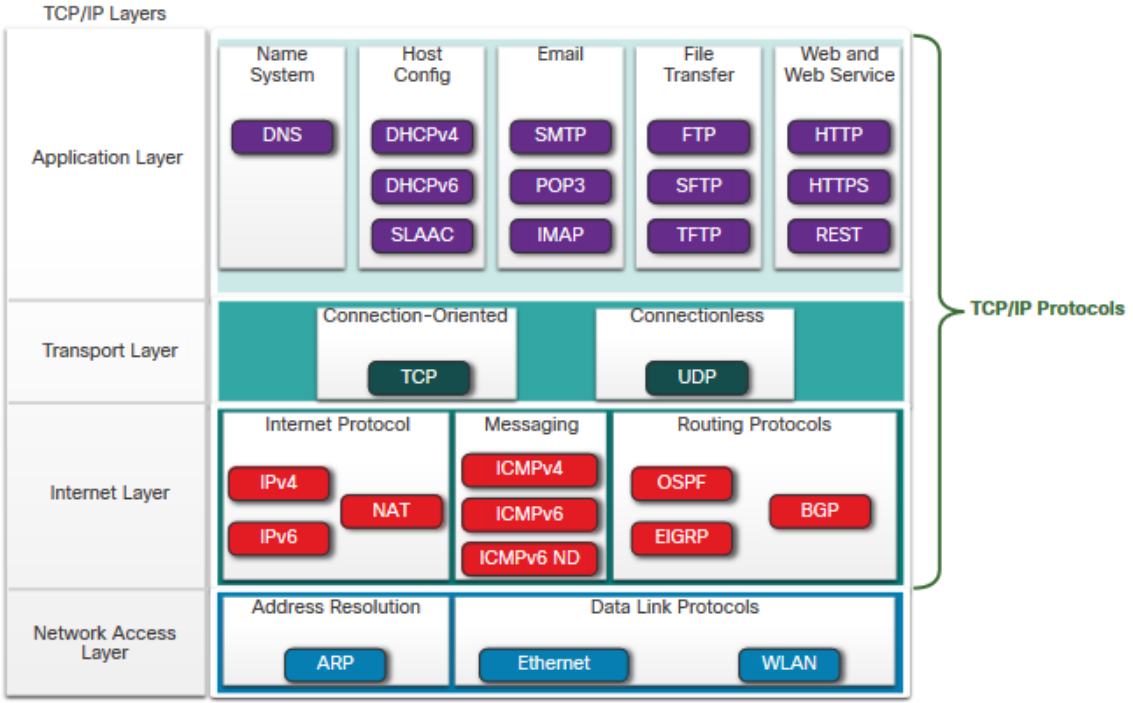
TCP/IP-Protokoll — Beispiel

- TCP/IP-Protokolle arbeiten auf der Ebene der Anwendungsschicht, Transportschicht und Internetschicht.
- Die am häufigsten verwendeten Netzwerkzugriffsschicht LAN-Protokolle sind Ethernet und WLAN (Wireless LAN).



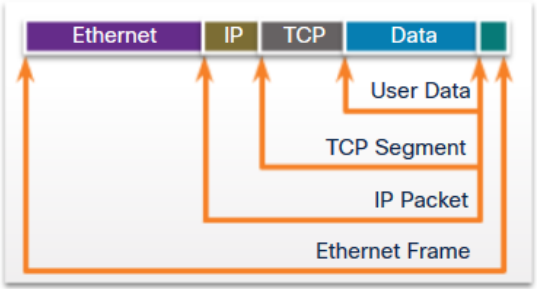
TCP/IP Protocol Suite

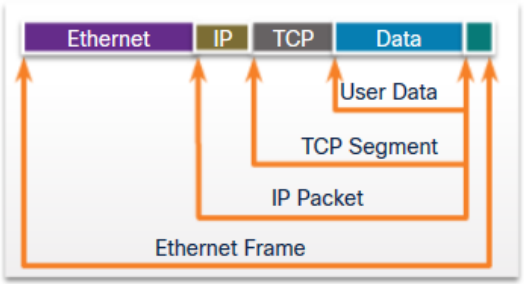
- TCP/IP ist die vom Internet verwendete Protokollfamilie und enthält viele Protokolle.
- TCP/IP ist:
  - Eine offene Standardprotokollfamilie, die für die Öffentlichkeit frei verfügbar ist und von jedem Anbieter verwendet werden kann
  - Eine standardbasierende Protokollfamilie ist eine Protokollfamilie, die von der Netzwerkbranche gebilligt und durch eine Standardisierungsorganisation genehmigt wurde.



TCP/IP-Kommunikationsprozess

- Ein Webserver, der eine Webseite kapselt und an einen Client sendet.
- Ein Client, der die Webseite für den Webbrowser entpackt.





3.4 - Standardisierungsorganisationen

Offene Standards

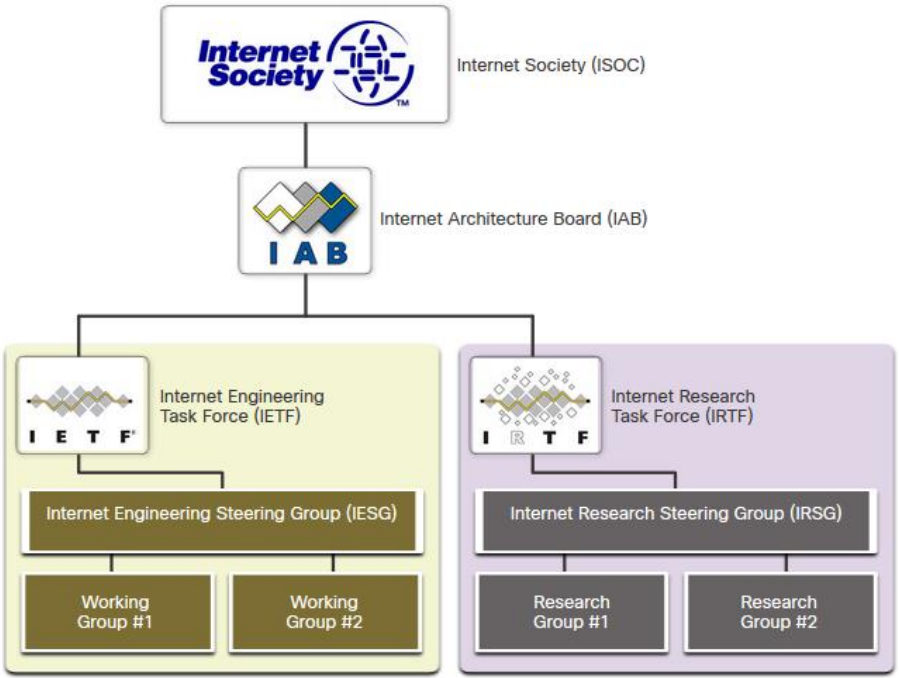
Offene Standards fördern:

- Interoperabilität
- Mitbewerberlösungen
- Innovation

Standardisierungsorganisationen sind:

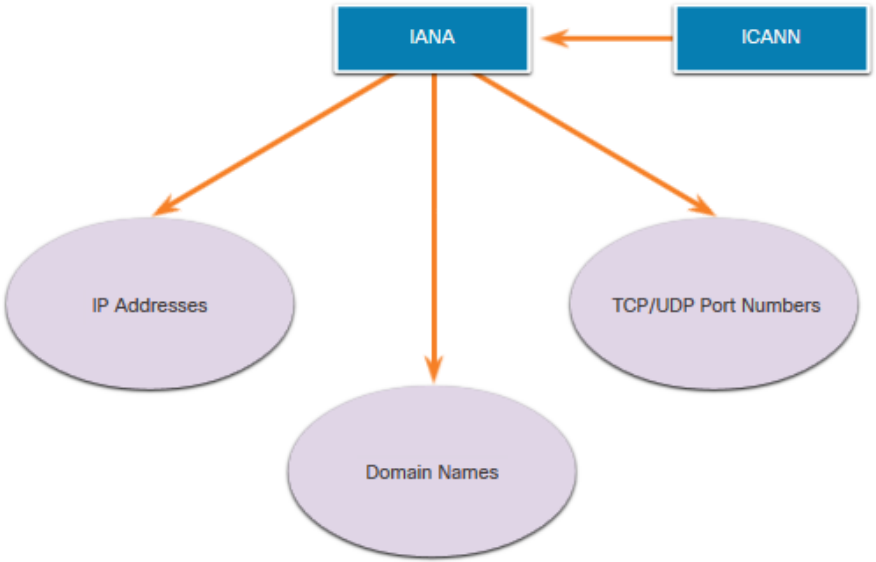
- herstellerneutral
- gemeinnützige Organisationen
- gegründet, um das Konzept offener Standards zu entwickeln und zu fördern.

Internetstandards



- **Internet Society (ISOC)** - Fördert die offene Entwicklung und Entwicklung des Internets
- **Internet Architecture Board (IAB)** – Verantwortlich für die gesamte Verwaltung und Entwicklung von Internetstandards.
- **Internet Engineering Task Force (IETF)** – Entwickelt, aktualisiert und verwaltet Internet- und TCP/IP-Technologien.
- **Internet Research Task Force (IRTF)** - Schwerpunkt auf Langzeitforschung im Zusammenhang mit Internet- und TCP/IP-Protokollen

Internetstandards (Fortsetzung)



Normungsorganisationen, die an der Entwicklung und Unterstützung von TCP/IP beteiligt sind

- **Internet Corporation for Assigned Names and Numbers (ICANN)** – Koordiniert von den USA aus IP-Adresszuweisung, die Verwaltung von Domänennamen und die Zuweisung anderer Informationen mit TCP/IP-Protokollen.
- **Internet Assigned Numbers Authority (IANA)** – Verantwortlich für die Überwachung und Verwaltung der IP-Adresszuweisung, für die Domänennamenverwaltung und für Protokollkennungen für ICANN.

Standardisierungsorganisationen für

Elektronik und Kommunikation

- **Institute of Electrical and Electronics Engineers** (**IEEE**, ausgesprochen „I-triple-E“) – Organisation für Elektrotechnik und Elektronik, die sich der Förderung technologischer Innovation und der Entwicklung von Standards für viele Branchen widmet, wie beispielsweise für die Energiebranche, das Gesundheitswesen, die Telekommunikationsbranche und die Netzwerkbranche.
- **Electronic Industries Alliance (EIA)** – Bekannt für ihre Normen im Zusammenhang mit elektrischer Verkabelung, Steckverbindern und den 19-Zoll-Racks, die für den Einbau von Netzwerkgeräten verwendet werden.
- **Telecommunications Industry Association (TIA)** – Verantwortlich für die Entwicklung von Kommunikationsstandards in einer Vielzahl von Bereichen, darunter Funkgeräte, Funkmasten, VoIP-Geräte und Satellitenkommunikation.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**) - definiert Normen für Videokomprimierung, Internetprotokoll-Fernsehen (IPTV) und Breitbandkommunikation, wie z.B. DSL (Digital Subscriber Line).

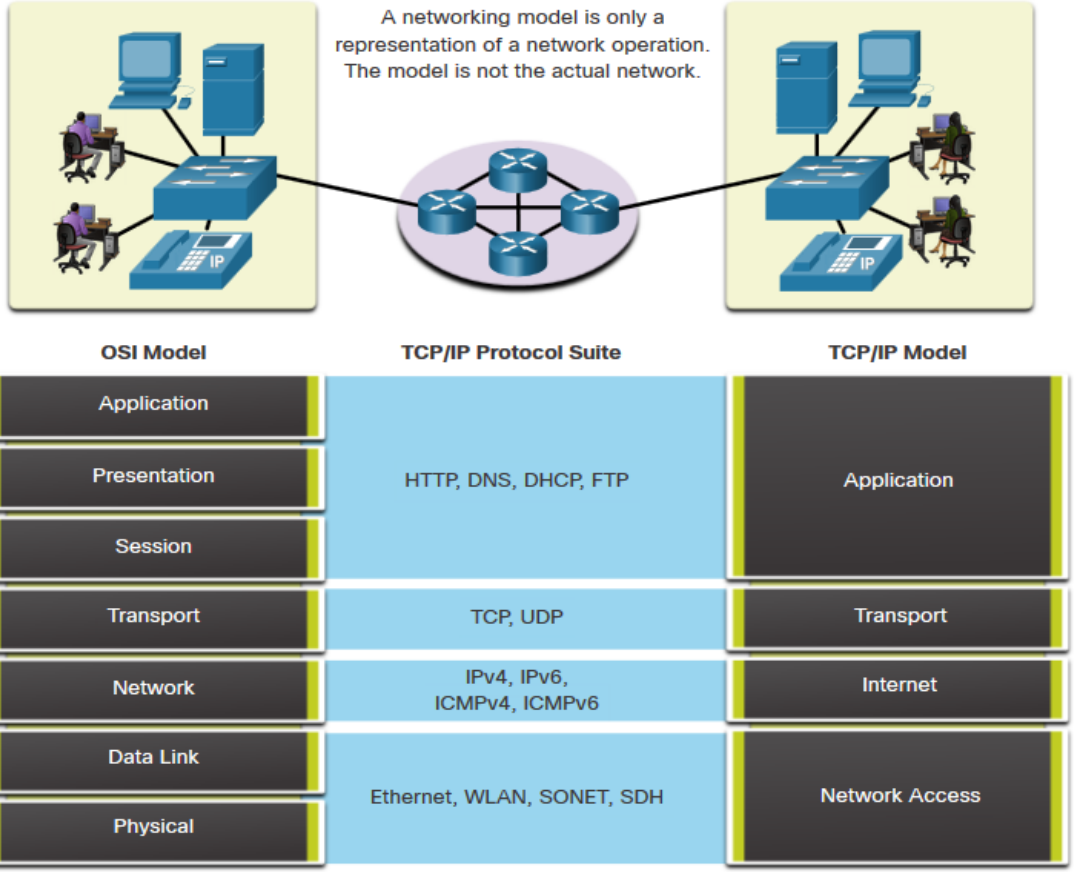
Übung – Recherche zu Netzwerkstandards

In dieser Übung führen Sie die folgenden Schritte aus:

- Teil 1: Recherche zu Netzwerkstandardisierungsorganisationen
- Teil 2: Reflektieren über Erfahrungen mit dem Internet und der Computervernetzung

3.5 – Referenzmodelle

Die Vorteile der Verwendung eines Schichtenmodells



Komplexe Konzepte wie die Funktionsweise eines Netzwerks können schwer zu erklären und zu verstehen sein. Aus diesem Grund wird ein Schichtenmodell verwendet.

Zwei Schichtenmodelle beschreiben Netzwerkoperationen:

- Open System Interconnection (OSI) Referenzmodell
- TCP/IP-Referenzmodell

Die Vorteile der Verwendung eines Schichtenmodells (Forts.)

Die Vorteile der Nutzung eines Schichtenmodells sind:

- Es unterstützt die Entwicklung von Protokollen, da Protokolle, die eine bestimmte Ebene verwenden, sich definierter Informationen bedienen und festgelegte Schnittstellen zu über- und untergeordneten Ebenen besitzen.
- Es fördert den Wettbewerb, weil Produkte von unterschiedlichen Herstellern miteinander kompatibel sind.
- Sie verhindern, dass sich Technologie- oder Funktionsänderungen in einer Schicht auf die Schichten darunter und darüber auswirken.
- Es stellt eine allgemeine Sprache bereit, um Netzwerkfunktionen und Einsatzmöglichkeiten zu beschreiben.

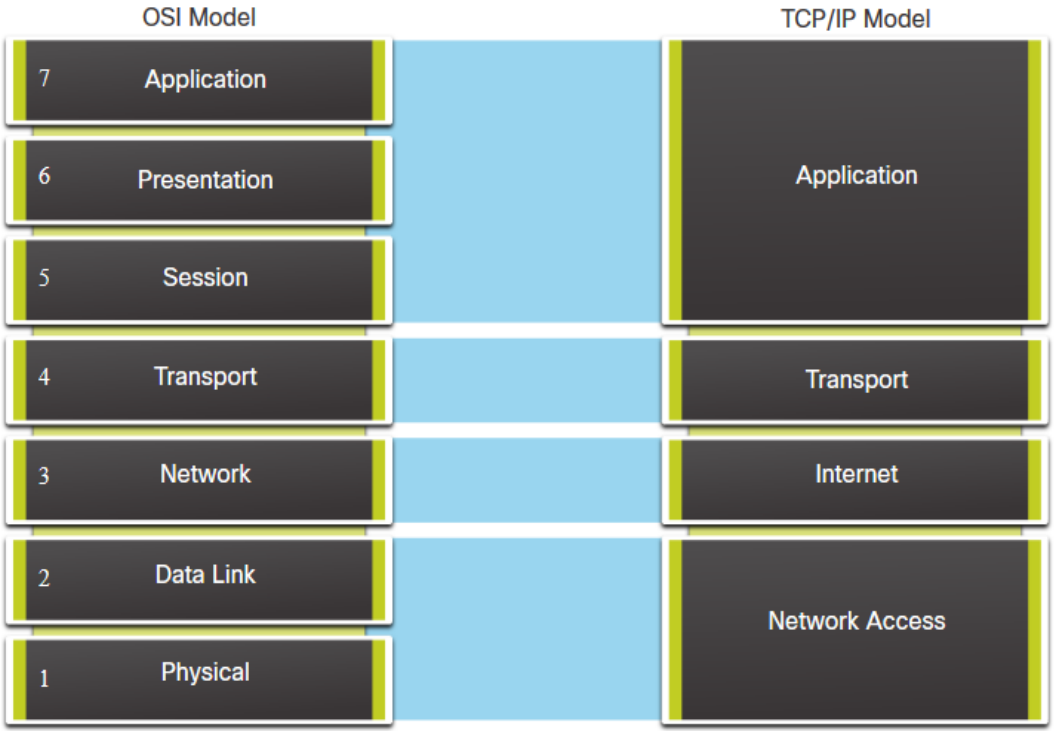
Das OSI-Referenzmodell

OSI-Modellschicht	Beschreibung
7 - Anwendung	Die Anwendungsschicht enthält die Protokolle, die für die Kommunikation zwischen Prozessen verwendet werden.
6 - Präsentation	Bietet einheitliche Darstellung der Daten, die zwischen den Diensten der Anwendungsschicht ausgetauscht werden.
5 - Sitzung	Bietet Dienste für die Präsentationsschicht und zum Verwalten des Datenaustauschs.
4 - Transport	definiert Dienste für die Segmentierung, die Übertragung und die Zusammensetzung der Daten für die einzelnen Kommunikationsverbindungen der Endgeräte.
3 - Netzwerk	stellt Dienste für den Austausch der einzelnen Datenblöcke über das Netzwerk bereit.
2 - Sicherung	Beschreibt Methoden zum Austausch von Daten-Frames über ein gemeinsames Medium.
1 - Bitübertragung	Beschreibt die Mittel zum Aktivieren, Verwalten und Deaktivieren physischer Verbindungen.

Das TCP/IP-Referenzmodell

TCP/IP-Modells	Beschreibung
Anwendung	Präsentiert die Daten dem Endbenutzer und übernimmt zusätzlich die Kodierung und die Dialogsteuerung
Transport	Unterstützt die Kommunikation zwischen unterschiedlichen Geräten über verschiedene Netzwerke hinweg
Internet	Bestimmt den besten Pfad durch das Netzwerk
Netzwerkzugriff	Steuert die Geräte und Medien, aus denen das Netzwerk besteht

OSI-Modell und TCP/IP-Modell im Vergleich



- Das OSI-Modell unterteilt die Netzwerkzugriffsschichte und die Anwendungsschicht des TCP/IP-Modells in mehrere Schichten.
- Die TCP/IP-Protokollfamilie gibt nicht an, welche Protokolle bei der Übertragung über ein physisches Medium verwendet werden sollen.
- Die OSI-Schichten 1 und 2 behandeln die notwendigen Verfahren, um auf das Medium zuzugreifen, und die physischen Träger, über die das Netzwerk Daten sendet.

Packet Tracer – TCP/IP- und OSI-Modell im laufenden Betrieb untersuchen

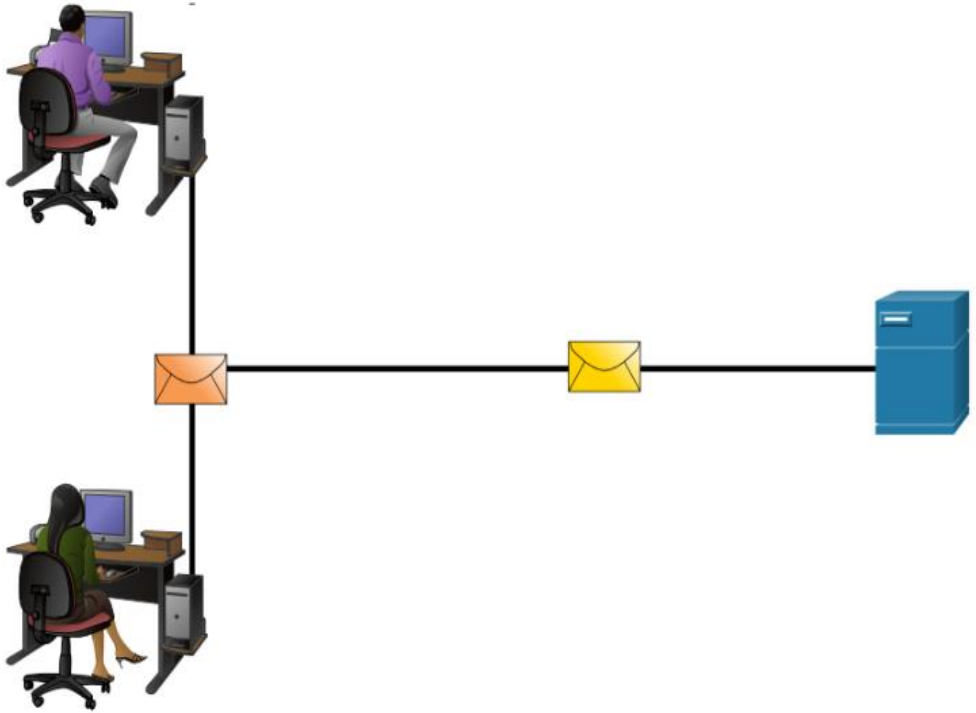
Diese Simulationsübung soll eine Grundlage zum Verständnis der TCP/IP-Protokollfamilie und der Beziehung zum OSI-Modell liefern. Der Simulationsmodus ermöglicht Ihnen, über das Netzwerk gesendete Dateninhalte in jeder Schicht zu analysieren.

In diesem Paket-Tracer werden Sie:

- Teil 1: Untersuchen des HTTP-Web-Datenverkehrs
- Teil 2: Anzeigen von Elementen der TCP/IP-Protokollfamilie

3.6 Datenkapselung

Segmentierungsmeldungen

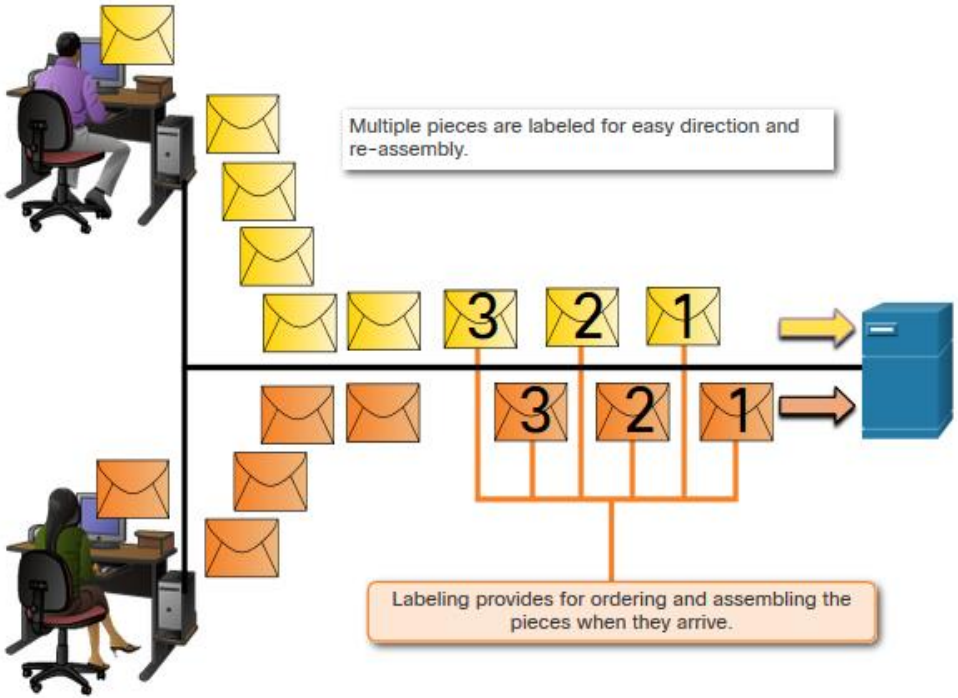


Segmentierung ist der Prozess der Aufteilung von Nachrichten in kleinere Einheiten. Multiplexing ist der Prozess der Zusammenführung von segmentierten Daten, die in mehrere Datenströme aufgeteilt wurden.

Die Segmentierung von Nachrichten hat die folgenden beiden Vorteile:

- **Erhöht die Geschwindigkeit** - Große Datenmengen können über das Netzwerk gesendet werden, ohne eine Kommunikationsverbindung zu binden.
- **Erhöht die Effizienz** - Nur Segmente, die das Ziel nicht erreichen, müssen erneut übertragen werden, nicht der gesamte Datenstrom.

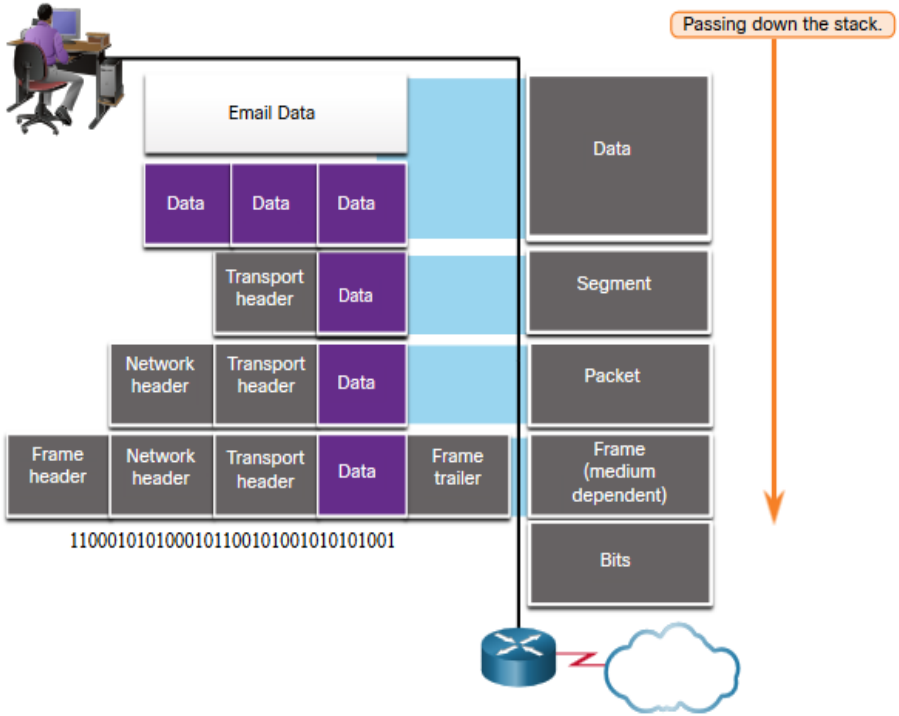
Sequenzierung



Sequenzierung von Nachrichten ist der Prozess der Nummerierung der Segmente, so dass die Nachricht am Ziel wieder zusammengesetzt werden kann.

TCP ist für die Sequenzierung der einzelnen Segmente verantwortlich.

Protocol Data Units (PDU)

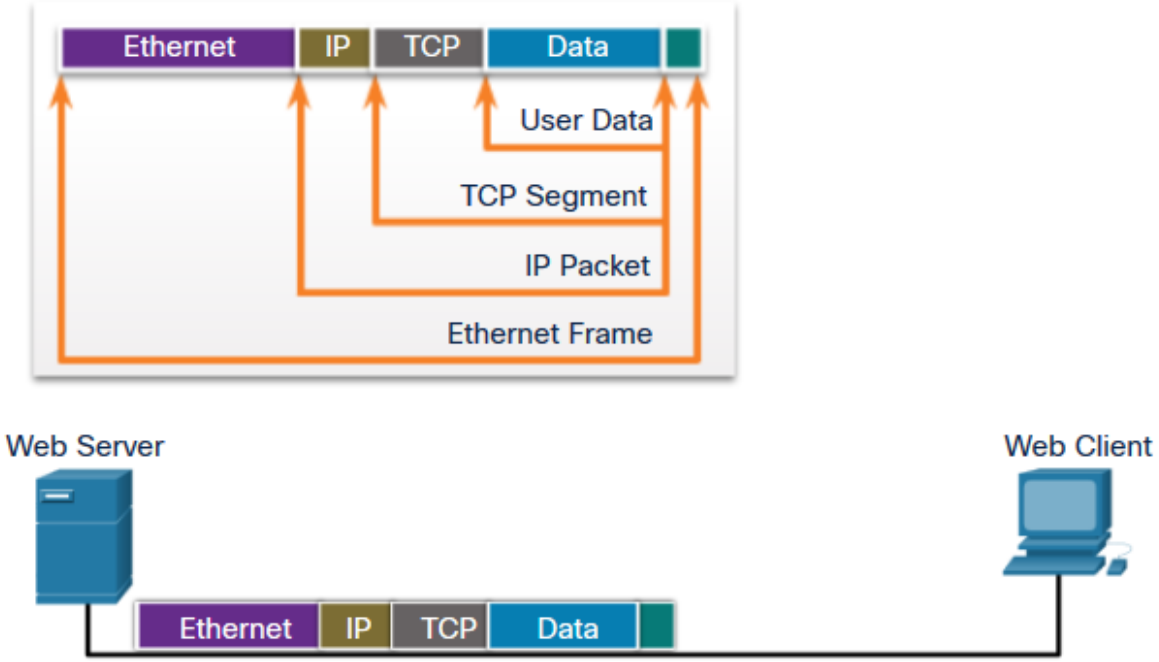


Die Kapselung ist der Prozess, bei dem Protokolle ihre Informationen zu den Daten hinzufügen.

- In jeder Phase des Vorgangs erhält die PDU einen anderen Namen, um deren neue Funktion anzuzeigen.
- Obwohl es für PDUs keine allgemeingültige Benennungskonvention gibt, werden die PDUs in diesem Kurs entsprechend der Protokolle der TCP/IP-Protokollfamilie benannt.
- Folgende PDUs werden im Protokollstapel weitergegeben:
  1. Daten (Datenstrom)
  2. Segment
  3. Paket
  4. Frame
  5. Bits (Bitstrom)

Beispiel für Datenkapselung

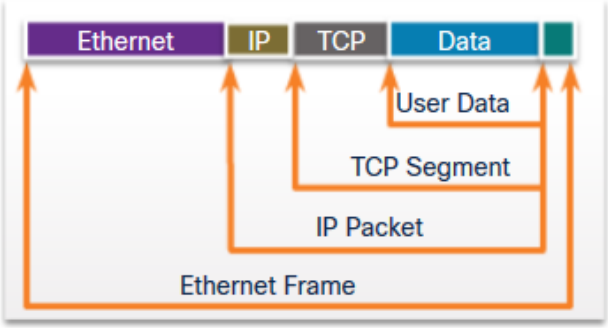
- Die Kapselung ist ein Top-Down-Prozess.
- Die höherliegende Schicht führt ihren Prozess aus und übergibt sie dann an die nächste Schicht des Modells. Dieser Vorgang wird von jeder Ebene wiederholt, bis er als Bitstrom gesendet wird.



Daten-Entkapselung

- Daten werden entkapselt, wenn sie den Stapel nach oben bewegen.
- Wenn ein Layer seinen Prozess abgeschlossen hat, wird der Header dieser Layers und der Rest an die nächste zu verarbeitende Ebene weitergeleitet. Dies wird auf jeder Ebene wiederholt, bis es sich um einen Datenstrom handelt, der die Anwendung verarbeiten kann.

1. Empfangene Bits (Bit-Stream)
2. Frame
3. Paket
4. Segment
5. Daten (Datenstrom)



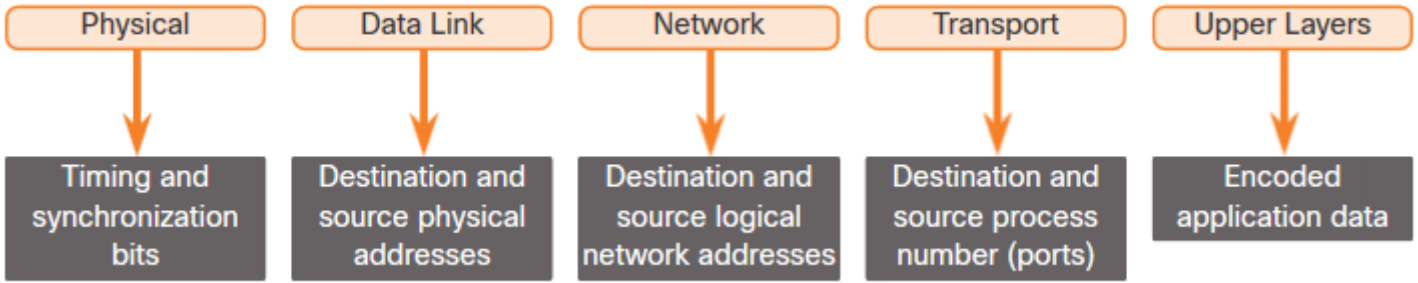
3.7 Datenzugriff

Adressen

Sowohl die Sicherungsschicht als auch die Vermittlungsschicht verwenden Adressierung, um Daten von der Quelle zum Ziel zu liefern.

Quell- und Zieladressen der Vermittlungsschicht – Verantwortlich für die Zustellung des IP-Pakets von der ursprünglichen Quelle zum endgültigen Ziel, entweder im selben Netzwerk oder in ein Remote-Netzwerk.

Quell- und Zieladressen der Sicherungsschicht – Verantwortlich für die Bereitstellung des Sicherungsschicht-Frames von einer Netzwerkkarte (NIC) an eine andere Netzwerkkarte im selben Netzwerk.

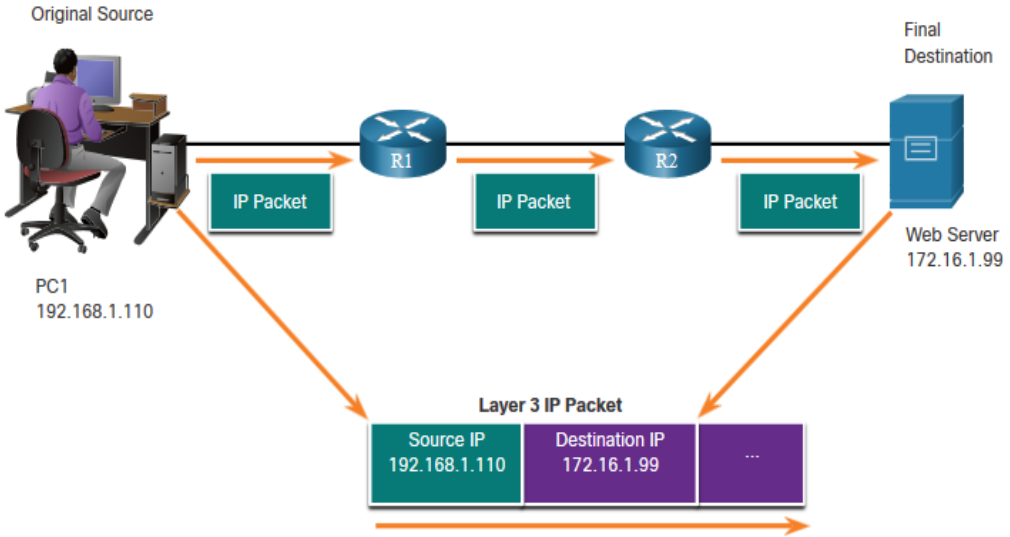


Logische Adressen der Vermittlungsschicht

Das IP-Paket enthält zwei IP-Adressen:

- **Quell-IP-Adresse** - Die IP-Adresse des sendenden Geräts, die ursprüngliche Quelle des Pakets.
- **Ziel-IP-Adresse** - Die IP-Adresse des empfangenden Geräts, das endgültige Ziel des Pakets.

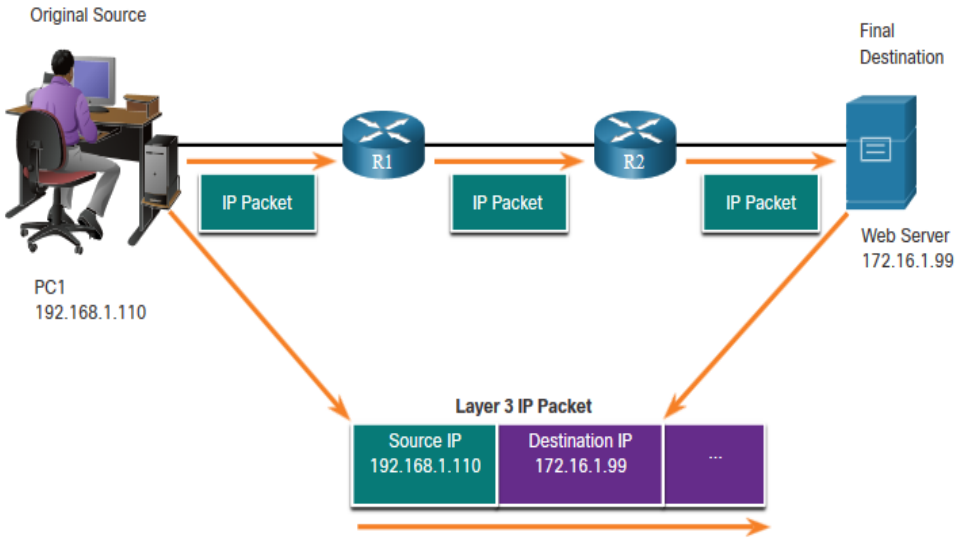
Diese Adressen können sich im gleichen Netzwerk oder in einem entfernten Netzwerk befinden.



Logische Adressen der Vermittlungsschicht (Fortsetzung)

IP-Adressen bestehen aus zwei Komponenten:

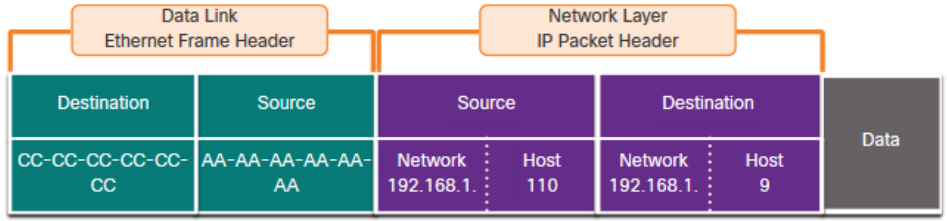
- **Netzwerkteil (IPv4) oder Präfix (IPv6)**
  - Der am weitesten links liegende Teil der Adresse zeigt an, zu welchem Netzwerk die IP-Adresse gehört.
  - Jedes LAN oder WAN verfügt über denselben Netzwerkteil.
- **Hostteil (IPv4) oder Schnittstellen-ID (IPv6)**
  - Der verbleibende Teil der Adresse identifiziert ein bestimmtes Gerät innerhalb der Gruppe.
  - Die Hostkomponente ist für jedes Gerät im Netzwerk eindeutig.

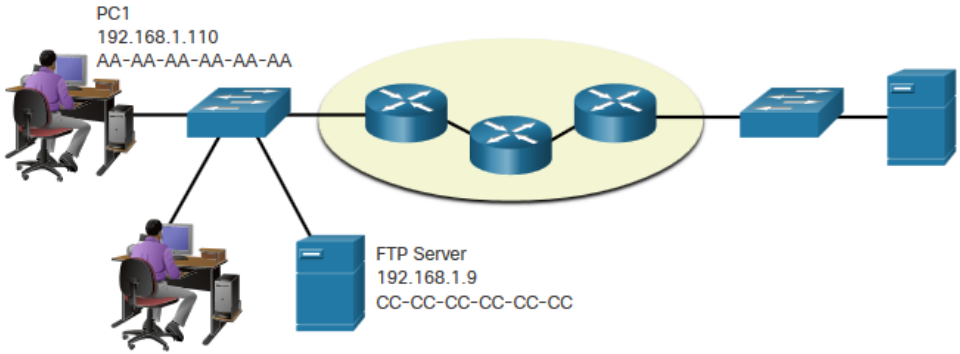


Geräte im selben Netzwerk

Wenn sich Geräte im selben Netzwerk befinden, haben Quelle und Ziel dieselbe Zahl im Netzwerkteil der Adresse.

- PC1 — 192.168.1.110
- FTP-Server — 192.168.1.9



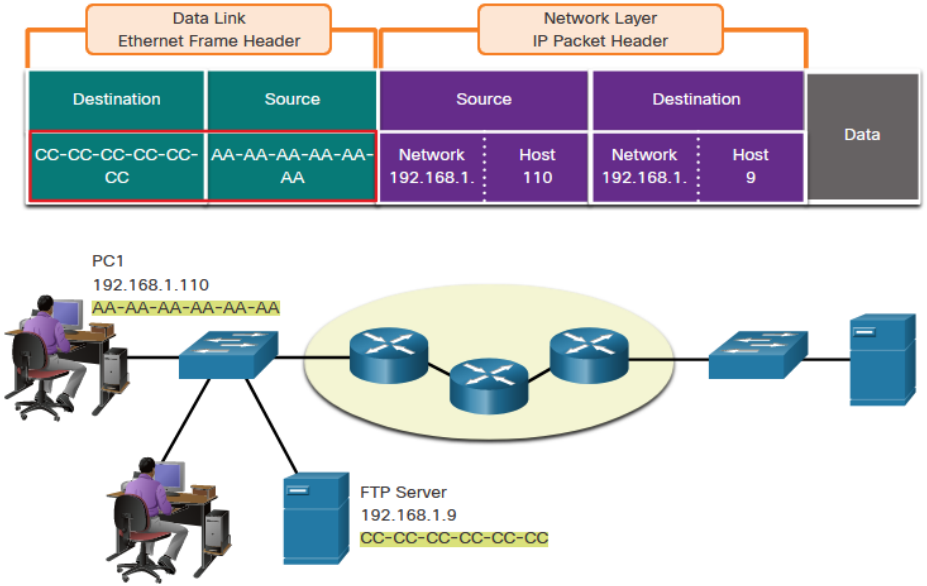


Rolle der Sicherungsschicht-Adressen: Gleiches IP-Netzwerk

Wenn sich Geräte im selben Ethernet-Netzwerk befinden, verwendet der Sicherungsschicht-Frame die tatsächliche MAC-Adresse der Ziel-Netzwerkkarte.

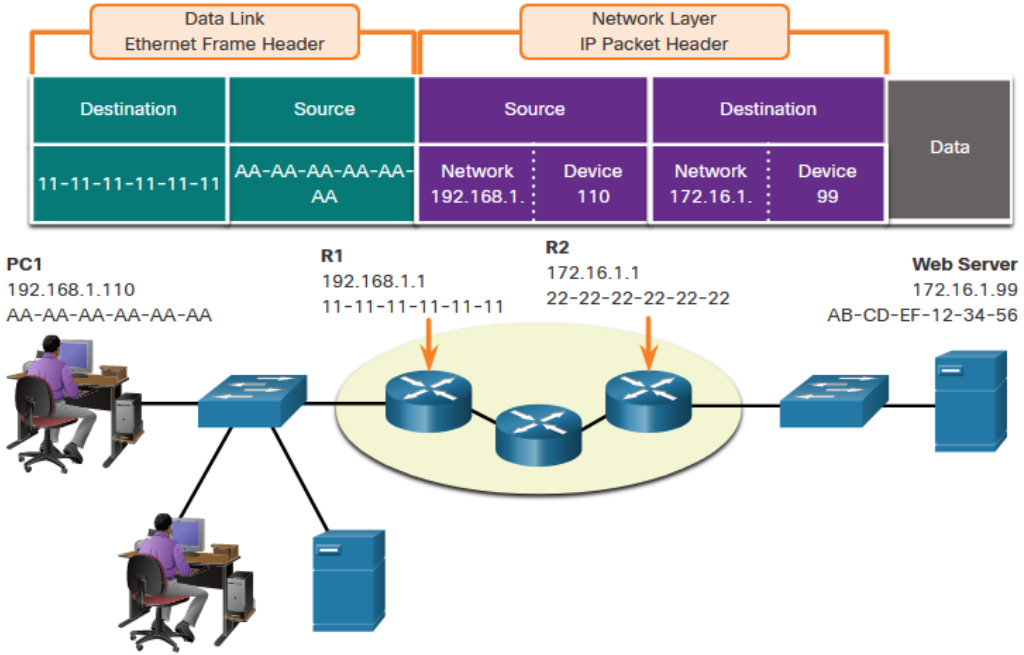
MAC-Adressen sind physisch in die Ethernet-NIC eingebettet und stellen lokale Adressierungen dar.

- Die Quell-MAC-Adresse ist die des Urhebers auf dem Link.
- Die Ziel-MAC-Adresse befindet sich immer auf demselben Link wie die Quelle, selbst wenn das endgültige Ziel ein einem entfernten Netzwerk ist.



Geräte in einem Remote-Netzwerk

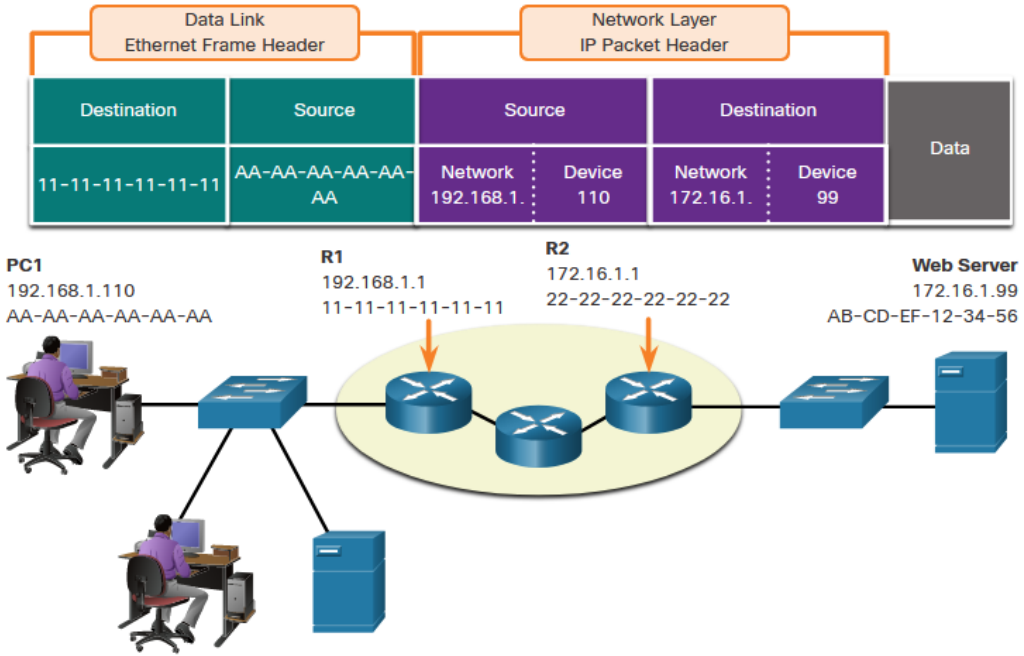
- Was passiert, wenn sich das eigentliche (endgültige) Ziel nicht im selben LAN befindet und weit entfernt ist?
- Was passiert, wenn PC1 versucht, den Webserver zu erreichen?
- Wirkt sich dies auf die Sicherungsschicht und die Vermittlungsschicht aus?



Rolle der Sicherungsschicht-Adressen

Wenn Quelle und Ziel einen anderen Netzwerkteil haben, bedeutet dies, dass sie sich in verschiedenen Netzwerken befinden.

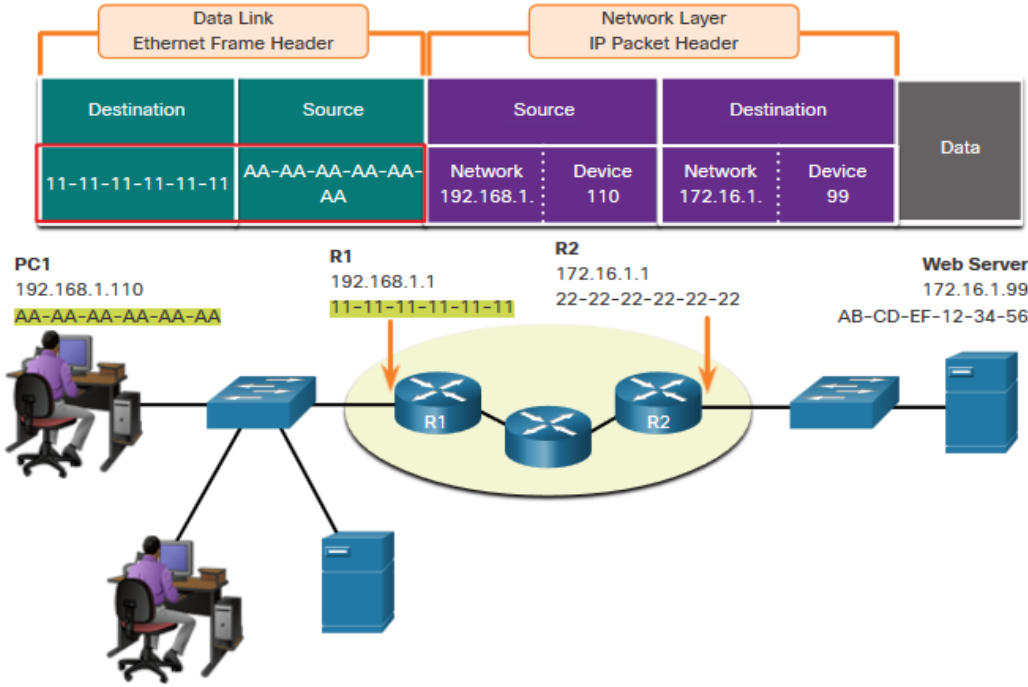
- PC1 — 192.168.1
- Webserver — 172.16.1



Rolle der Sicherungsschicht-Adressen: Verschiedene IP-Netzwerke

Wenn das endgültige Ziel entfernt ist, stellt Layer 3 dem Layer 2 die lokale Standard-Gateway-IP-Adresse zur Verfügung, die auch als Router-Adresse bezeichnet wird.

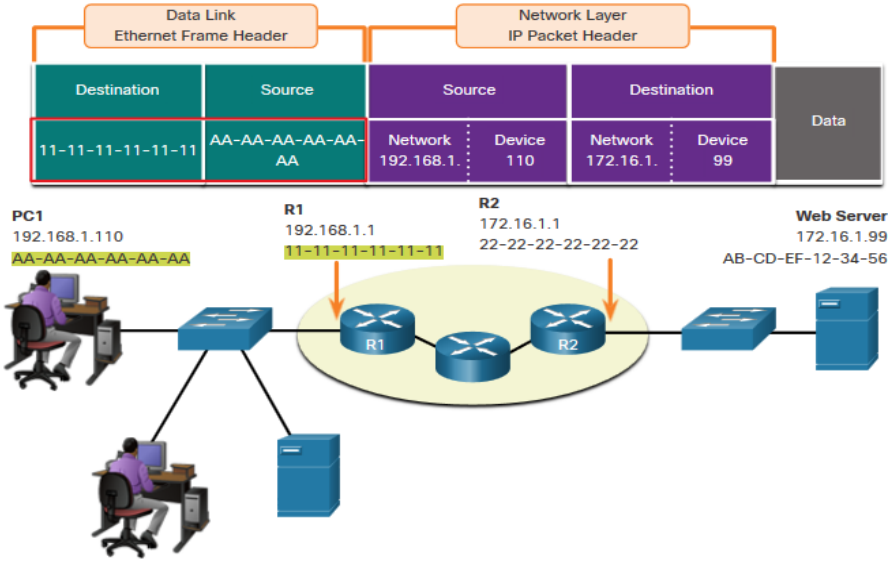
- Das Standard-Gateway (DGW) ist die Router-Schnittstellen-IP-Adresse, die Teil dieses LAN ist und die „Tür“ oder „Gateway“ zu allen anderen entfernten Standorten darstellt.
- Alle Geräte im LAN müssen über diese Adresse informiert werden, sonst beschränkt sich ihr Datenverkehr nur auf das LAN.
- Sobald ein Layer 2 Datenpaket von PC1 zum Standard-Gateway (Router) weitergeleitet wird, kann der Router den Routing-Prozess starten, um die Informationen zum tatsächlichen Ziel zu erhalten.



Datenzugriffsrolle der Sicherungsschicht-Adressen: Verschiedene IP-Netzwerke (Fortsetzung)

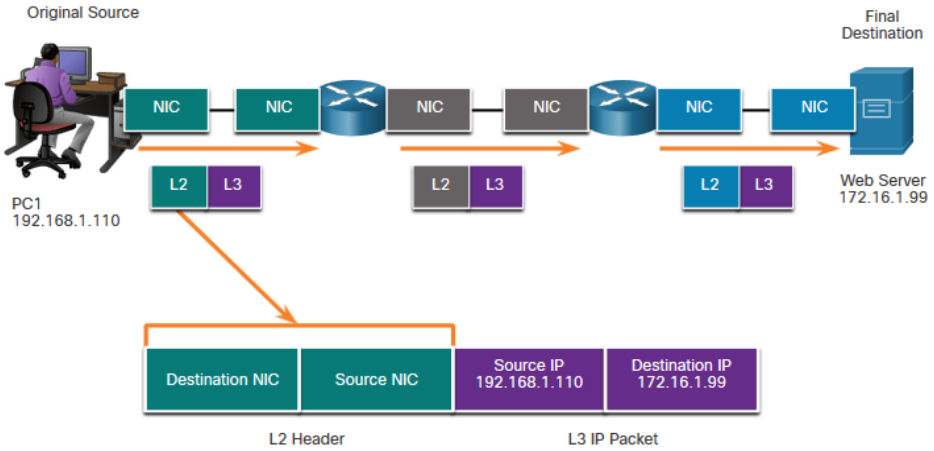
- Die Sicherungsschichtadressierung ist eine lokale Adressierung, sodass sie für jeden Link eine Quelle und ein Ziel hat.
- Die MAC-Adressierung für das erste Segment lautet:
  - Quelle — AA-AA-AA-AA-AA-AA (PC1) sendet den Frame.
  - Ziel — 11-11-11-11-11-11-11 (R1-Standard-Gateway-MAC) empfängt den Frame.

Hinweis: Während sich die lokale L2-Adressierung von Link zu Link oder Hop zu Hop ändert, bleibt die L3-Adressierung gleich.



Sicherungsschicht-Adressen

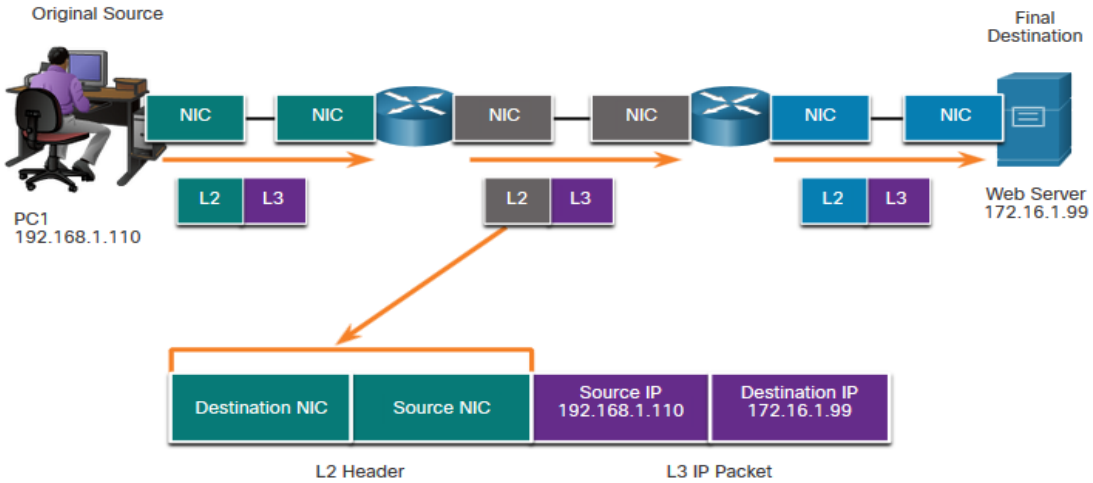
- Da es sich bei der Sicherungsschicht-Adressierung um eine lokale Adressierung handelt, verfügt sie über eine Quelle und ein Ziel für jedes Segment oder Hop der Reise zum Ziel.
- Die MAC-Adressierung für das erste Segment lautet:
  - Quelle — (PC1-NIC) sendet Frame
  - Ziel — (Erster Router - DGW-Schnittstelle) erhält Frame



Sicherungsschicht-Adressen (Fortsetzung)

Die MAC-Adresse für den zweiten Hop lautet:

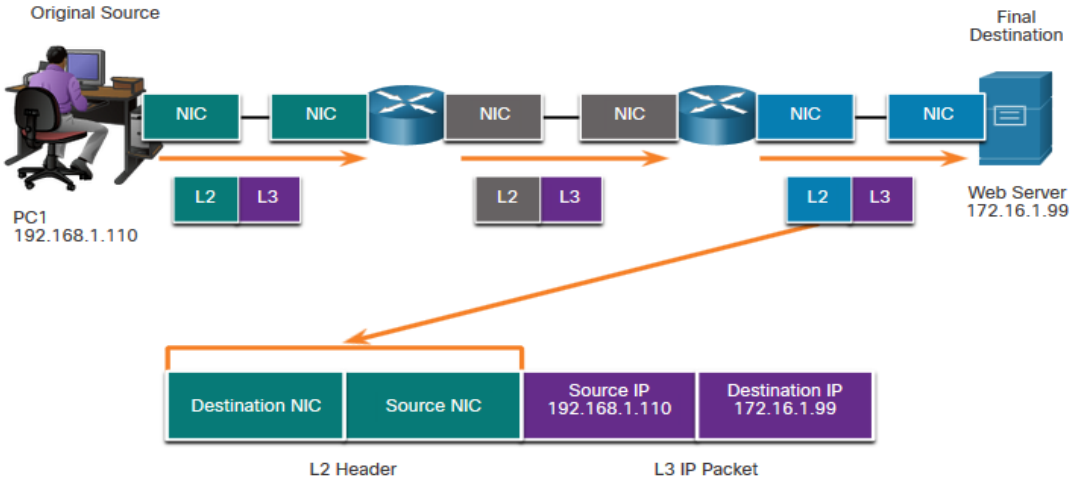
- Quelle — (erster Router- Exit-Interface) sendet Frame
- Ziel — (zweiter Router) empfängt Frame



Sicherungsschicht-Adressen (Fortsetzung)

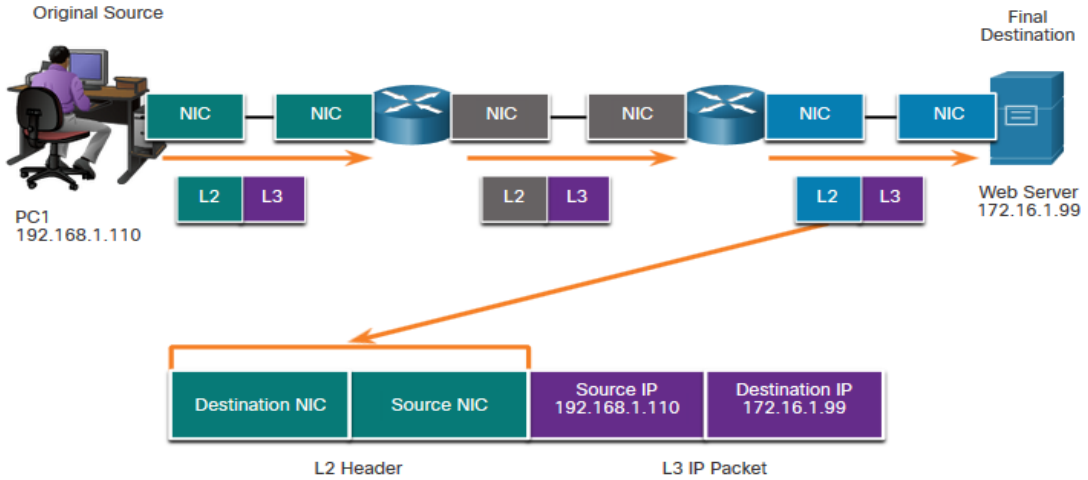
Die MAC-Adressierung für das letzte Segment lautet:

- Quelle — (zweiter Router- Exit-Schnittstelle) sendet Frame
- Ziel — (Webserver-NIC) empfängt Frame



Sicherungsschicht-Adressen (Fortsetzung)

- Beachten Sie, dass das Paket nicht geändert wird, aber der Frame geändert wird, daher ändert sich die L3-IP-Adressierung nicht von Segment zu Segment sondern nur die L2-MAC-Adressierung.
- Die L3-Adressierung bleibt gleich, da sie global ist und das endgültige Ziel immer noch der Webserver ist.



Übung – Installieren von Wireshark

In diesem Labor werden Sie Folgendes tun:

- Herunterladen und Installieren von Wireshark

Übung – Anzeigen vom Netzwerkverkehr mit Wireshark

In dieser Übung führen Sie die folgenden Schritte aus:

- Teil 1: Erfassen und Analysieren von lokalen ICMP-Daten in Wireshark
- Teil 2: Erfassen und Analysieren von Remote-ICMP-Daten in Wireshark

3.8 Modul Praxis und Quiz

Was habe ich in diesem Modul gelernt?

Die Regeln

- Protokolle müssen einen Sender und einen Empfänger haben.
- Häufige Computerprotokolle umfassen folgende Anforderungen: Nachrichtenkodierung, Formatierung und Kapselung, Größe, Zeitmessung und Übermittlungsoptionen.

Protokolle

- Um eine Nachricht über das Netzwerk zu senden, müssen mehrere Protokolle verwendet werden.
- Jedes Netzwerkprotokoll hat seine eigene Funktion, Format und Regeln für die Kommunikation.

Protokollfamilien

- Eine Protokollfamilie ist eine Gruppe von miteinander verbundenen Protokollen.
- TCP/IP-Protokollfamilie enthält die heutezutage verwendeten Protokolle.

Standardisierungsorganisationen

- Offene Standards fördern die Interoperabilität, den Wettbewerb und die Innovation.

Was habe ich in diesem Modul gelernt? (Forts.)

Referenzmodelle

- Die beiden im Netzwerk verwendeten Modelle sind das TCP/IP und das OSI-Modell.
- Das OSI-Modell hat sieben Schichten und das TCP/IP vier.

Datenkapselung

- Das Format, das eine Dateneinheit in der jeweiligen Schicht hat, wird als *Protokoll-Dateneinheit (Protocol Data Unit, PDU)* bezeichnet.
- Es gibt fünf verschiedene PDUs, die in der Datenkapselung verwendet werden: Daten, Segment, Paket, Frame und Bits

Datenzugriff

- Die Vermittlungsschicht und die Sicherungsschicht bieten Adressierung zum Transportieren von Daten durch das Netzwerk.
- Layer 3 bietet IP-Adressierung und Layer 2 bietet MAC-Adressierung.
- Die Art und Weise, wie diese Layer Adressierung behandeln, hängt davon ab, ob sich die Quelle und das Ziel im selben Netzwerk befinden oder ob sich das Ziel in einem anderen Netzwerk als der Quelle befindet.


CISCO