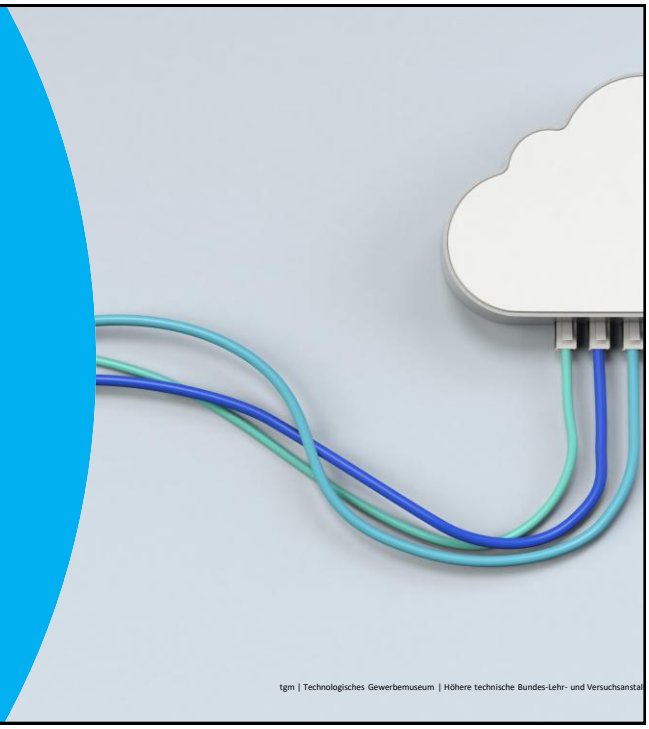
Protokolle und Modelle

NETZWERKTECHNIK / SEMESTER 1 UND 2



1

AGENDA

01 REGELN

02 PROTOKOLLE

03 PROTOKOLLSUITEN

04 STANDARDISIERUNGSORGANISATIONEN

05 REFERENZMODELLE

06 DATENKAPSELUNG

07 DATENZUGRIFF

tgm

2

NETZWERKTECHNIK / SEMESTER 1 und 2

Aktivität – Entwerfen eines Kommunikationssystems

- Sie haben gerade ein neues Auto für Ihren persönlichen Gebrauch gekauft. Nachdem Sie das Auto etwa eine Woche lang gefahren sind, stellen Sie fest, dass es nicht richtig funktioniert. Sie besprechen das Problem mit mehreren Ihrer Kollegen und beschließen, es zu einer Kfz-Reparaturwerkstatt zu bringen, die sie sehr empfehlen. Es ist die einzige Reparaturwerkstatt, die sich in unmittelbarer Nähe befindet.
- Wenn Sie in der Reparaturwerkstatt ankommen, stellen Sie fest, dass alle Mechaniker eine andere Sprache sprechen. Sie haben Schwierigkeiten, die Leistungsprobleme des Autos zu erklären, aber die Reparaturen müssen wirklich durchgeführt werden. Sie sind sich nicht sicher, ob Sie es nach Hause fahren können, um andere Optionen zu recherchieren.
- Sie müssen einen Weg finden, mit der Reparaturwerkstatt zusammenzuarbeiten, um sicherzustellen, dass Ihr Auto korrekt repariert wird.

Wie werden Sie mit den Mechanikern kommunizieren? Entwerfen Sie ein Kommunikationsmodell, um sicherzustellen, dass das Auto ordnungsgemäß repariert wird.

01

Regeln

NETZWERKTECHNIK / SEMESTER 1 und 2

Grundlagen der Kommunikation

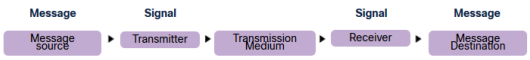
- Netzwerke können in Größe und Komplexität variieren. Es reicht nicht aus, eine Verbindung zu haben, die Geräte müssen sich darauf einigen, "wie" sie kommunizieren sollen.
- Jede Kommunikation besteht aus drei Elementen:
  - **Nachrichtenquelle (Absender):** Nachrichtenquellen sind Personen oder elektronische Geräte, die eine Nachricht an andere Personen oder Geräte senden müssen.
  - **Nachrichtenziel (Empfänger):** Das Ziel empfängt die Nachricht und interpretiert sie.
  - **Kanal**: Der Kanal beschreibt das bereitgestellte Medium, über welches die Nachricht von der Quelle zum Ziel gelangt.

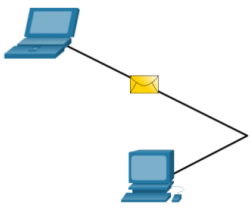
15

NETZWERKTECHNIK / SEMESTER 1 und 2

Kommunikationsprotokolle

- Die gesamte Kommunikation wird durch Protokolle geregelt.
- Protokolle sind die Regeln, denen die Kommunikation folgt.
- Diese Regeln variieren je nach Protokoll.





16

NETZWERKTECHNIK / SEMESTER 1 und 2

Etablierung von Regeln

- Einzelpersonen müssen festgelegte Regeln oder Vereinbarungen verwenden, um das Gespräch zu regeln.
- Die erste Nachricht ist schwer zu lesen, da sie nicht richtig formatiert ist. Die zweite zeigt die Nachricht korrekt formatiert an

```
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.
```


NETZWERKTECHNIK / SEMESTER 1 und 2

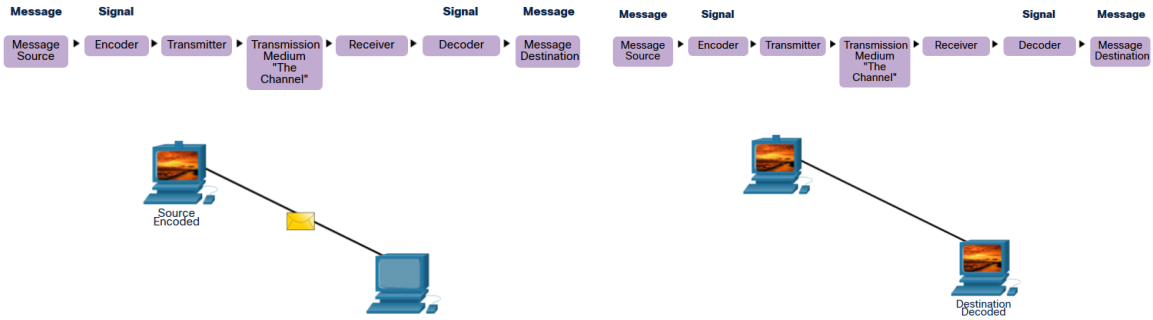
Etablierung von Regeln

- Protokolle müssen die folgenden Anforderungen berücksichtigen:
  - Ein identifizierter Sender und Empfänger
  - Gemeinsame Sprache und Grammatik
  - Geschwindigkeit und Timing der Lieferung
  - Anforderungen zur Bestätigung von Nachrichten

NETZWERKTECHNIK / SEMESTER 1 und 2

Nachrichtenkodierung

- Codierung ist der Prozess der Umwandlung von Informationen in eine andere Form für die Übertragung.
- Durch die Dekodierung wird dieser Prozess umgekehrt, um die Informationen zu interpretieren.



NETZWERKTECHNIK / SEMESTER 1 und 2

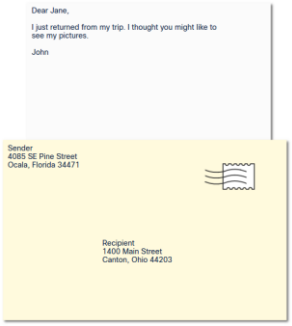
Nachrichtenkodierung

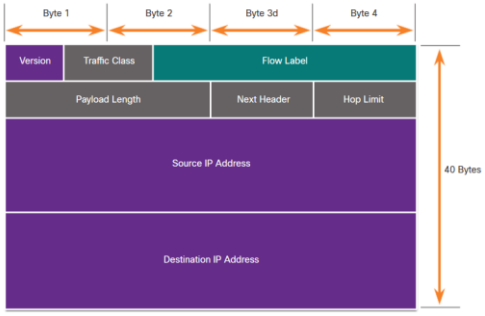
- Die Codierung zwischen Hosts muss in einem für das Medium geeigneten Format erfolgen.
  - Nachrichten, die über das Netzwerk gesendet werden, werden zunächst vom sendenden Host in Bits umgewandelt.
  - Jedes Bit ist in ein Muster von Spannungen an Kupferdrähten, Infrarotlicht in Glasfasern oder Mikrowellen für drahtlose Systeme codiert.
  - Der empfangende Host empfängt und dekodiert die Signale, um die Nachricht zu interpretieren.

NETZWERKTECHNIK / SEMESTER 1 und 2

Nachrichtenformatierung und -kapselung

- Wenn eine Nachricht gesendet wird, muss sie ein bestimmtes Format oder eine bestimmte Struktur verwenden.
- Die Nachrichtenformate hängen vom Typ der Nachricht und dem Kanal ab, der zum Übermitteln der Nachricht verwendet wird.





21

NETZWERKTECHNIK / SEMESTER 1 und 2

Nachrichtenformatierung und -kapselung

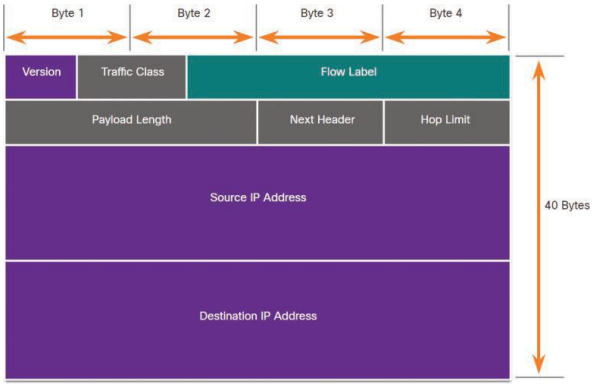
Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

22

NETZWERKTECHNIK / SEMESTER 1 und 2

Nachrichtenformatierung und -kapselung

- Internet Protocol (IP) ist ein Protokoll mit einer ähnlichen Funktion wie die das vorherige Kuvert-Beispiel.
- In der Abbildung identifizieren die Felder des IPv6-Pakets (Internet Protocol Version 6) die Quelle des Pakets und sein Ziel.
- IP ist für das Senden einer Nachricht von der Nachrichtenquelle zum Ziel über ein oder mehrere Netzwerke verantwortlich.



NETZWERKTECHNIK / SEMESTER 1 und 2

Timing der Nachricht

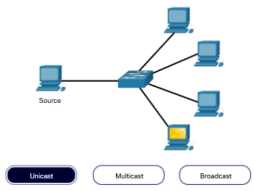
Das Timing der Nachricht umfasst Folgendes:

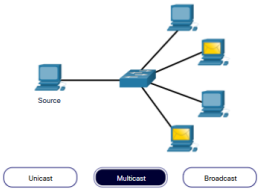
- **Flusskontrolle** – Verwaltet die Datenübertragungsrate und definiert, wie viele Informationen gesendet werden können und mit welcher Geschwindigkeit sie übermittelt werden können.
- **Antwort-Timeout** – Verwaltet, wie lange ein Gerät wartet, wenn es keine Antwort vom Ziel hört.
- **Zugriffsmethode** - Bestimmt, wann jemand eine Nachricht senden kann.
  - Verschiedene Regeln, um mit "Kollisionen" umzugehen. Dies ist der Fall, wenn mehr als ein Gerät gleichzeitig Datenverkehr sendet und dadurch die Nachrichten beschädigt werden.
  - Einige Protokolle sind proaktiv und versuchen, Kollisionen zu verhindern. Andere Protokolle sind reaktiv und legen eine Wiederherstellungsmethode fest, nachdem die Kollision aufgetreten ist.

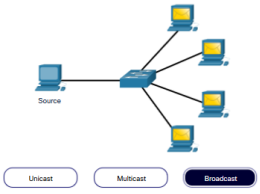
Optionen für die Nachrichtenübermittlung

Die Nachrichtenübermittlung kann auf eine der folgenden Methoden erfolgen:

- Unicast – Eins-zu-Eins-Kommunikation
- Multicast – ein bis viele, in der Regel nicht alle
- Broadcast – einer für alle
- Hinweis: Broadcasts werden in IPv4-Netzwerken verwendet, sind aber keine Option für IPv6. Später werden wird auch "Anycast" als zusätzliche Zustellungsoption für IPv6 eingeführt.







25

02

Protokolle

26

NETZWERKTECHNIK / SEMESTER 1 und 2

Übersicht über das Netzwerkprotokoll

- Netzwerkprotokolle definieren gemeinsame Formate und einen Satz von Regeln.
- Kann auf Geräten implementiert werden in:
  - Software
  - Hardware
  - Beidem
- Jedes Protokoll hat seine eigene:
  - Funktion
  - Format
  - Regeln zur Kommunikation

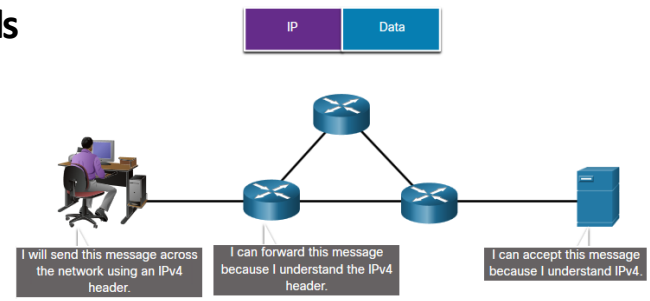
Type	Beschreibung
Netzwerkkommunikation	Ermöglichen der Kommunikation zwischen zwei oder mehr Geräten über ein oder mehrere Netzwerke
Netzwerksicherheit	Sichern Sie Daten, um Authentifizierung, Datenintegrität und Datenverschlüsselung bereitzustellen
Routing	Ermöglichen den Austausch von Routeninformationen, den Vergleich von Pfaden und die Auswahl des Besten
Service-Erkennung	Wird zur automatischen Erkennung von Geräten oder Diensten verwendet

27

NETZWERKTECHNIK / SEMESTER 1 und 2

Funktionen des Netzwerkprotokolls

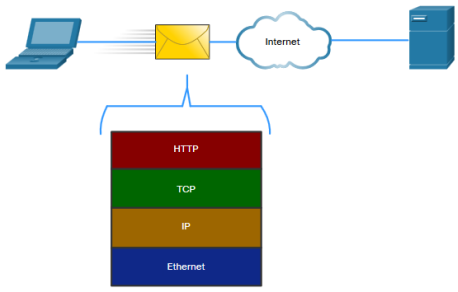
- Geräte verwenden vereinbarte Protokolle, um zu kommunizieren.
- Protokolle können mehrere Funktionen haben.



Function	Description
Adressierung	Identifiziert Sender und Empfänger
Zuverlässigkeit	Bietet garantierte Lieferung
Flusskontrolle	Stellt einen effizienten Datenfluss sicher
Sequenzierung	Eindeutige Markierung jedes übertragenen Datensegments
Fehlererkennung	Ermittelt, ob Daten während der Übertragung beschädigt wurden
Anwendungsschnittstelle	Prozess-zu-Prozess-Kommunikation zwischen Netzwerkanwendungen

28

Protokoll-Interaktion



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

Protocol	Funktion
Hypertext Transfer Protocol (HTTP)	▪ Steuert die Art und Weise, wie ein Webserver und ein Webclient interagieren ▪ Definiert Inhalt und Format
Transmission Control Protocol (TCP)	▪ Verwaltet die einzelnen Konversationen ▪ Bietet garantierte Lieferung ▪ Verwaltung der Flusskontrolle
Internet Protocol (IP)	Globale Zustellung von Nachrichten vom Absender zum Empfänger
Ethernet	Übermittelt Nachrichten von einer Netzwerkkarte zu einer anderen Netzwerkkarte im selben Ethernet Local Area Network (LAN)

29

03

Protokollsuiten

30

30

NETZWERKTECHNIK / SEMESTER 1 und 2

Netzwerkprotokoll-Suiten

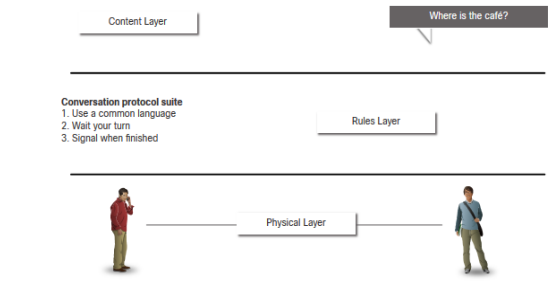
Protokolle müssen in der Lage sein, mit anderen Protokollen zu arbeiten.

Protokoll-Suite:

- Eine Gruppe miteinander verbundener Protokolle, die zum Ausführen einer Kommunikationsfunktion erforderlich sind
- Regelwerke, die zusammenarbeiten, um ein Problem zu lösen

Die Protokolle werden in Schichtenform betrachtet:

- Höhere Schichten – fokussieren auf den Inhalt
- Untere Schichten – fokussieren auf die Bewegung von Daten und der Bereitstellung von Diensten für die oberen Schichten



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

NETZWERKTECHNIK / SEMESTER 1 und 2

Entwicklung von Protokollsuiten

Es gibt mehrere Protokollsuiten.

- **Internet Protocol Suite** oder TCP/IP - Die gebräuchlichste Protokollsuite, die von der Internet Engineering Task Force (IETF) gepflegt wird
- **OSI-Protokolle** (Open Systems Interconnection) - Entwickelt von der Internationalen Organisation für Normung (ISO) und der Internationalen Fernmeldeunion (ITU)
- **AppleTalk** - Proprietäre Suite-Version von Apple Inc.
- **Novell NetWare** – Proprietäre Suite, die von Novell Inc. entwickelt wurde.

TCP/IP Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet ARP WLAN			

Application-Layer

Domain	Protocol
Name system	DNS: Domain Name System. DNS translates domain names, such as cisco.com, into IP addresses.
Host Config	DHCPv4: Dynamic Host Configuration Protocol for IPv4. A DHCPv4 server dynamically assigns IPv4 addressing information to DHCPv4 clients at startup and allows the addresses to be reused when no longer needed.
Host Config	DHCPv6: Dynamic Host Configuration Protocol for IPv6. DHCPv6 is similar to DHCPv4. A DHCPv6 server dynamically assigns IPv6 addressing information to DHCPv6 clients at startup.
Host Config	SLAAC: Stateless address autoconfiguration. SLAAC allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.
Email	SMTP: Simple Mail Transfer Protocol. SMTP enables clients to send email to a mail server and enables servers to send email to other servers.
Email	POP3: Post Office Protocol version 3. POP3 enables clients to retrieve email from a mail server and download the email to the client's local mail application.
Email	IMAP: Internet Message Access Protocol. IMAP enables clients to access email stored on a mail server as well as maintain email on the server.

33

Application-Layer

Domain	Protocol
FileTransfer	FTP: File Transfer Protocol. FTP sets the rules that enable a user on one host to access and transfer files to and from another host over a network. FTP is a reliable, connection-oriented, and acknowledged file delivery protocol.
FileTransfer	SFTP: SSH File Transfer Protocol. As an extension to Secure Shell (SSH) protocol, SFTP can be used to establish a secure file transfer session in which the file transfer is encrypted. SSH is a method for secure remote login that is typically used for accessing the command line of a device.
FileTransfer	TFTP: Trivial File Transfer Protocol. TFTP is a simple, connectionless file transfer protocol with best-effort, unacknowledged file delivery. It requires less overhead than FTP.
Web and web service	HTTP: Hypertext Transfer Protocol. HTTP is a set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
Web and web service	HTTPS: HTTP Secure. HTTPS is a secure form of HTTP that encrypts the data exchanged over the World Wide Web.
Web and web service	REST: Representational State Transfer. REST is a method of using application programming interfaces (APIs) and HTTP requests to create web applications.

34

NETZWERKTECHNIK / SEMESTER 1 und 2

Transport-Layer

Domain	Protocol
Connection oriented	TCP: Transmission Control Protocol. TCP enables reliable communication between processes running on separate hosts and provides reliable, acknowledged transmissions that confirm successful delivery.
Connectionless	UDP: User Datagram Protocol. UDP enables a process running on one host to send packets to a process running on another host. However, UDP does not confirm successful datagram transmission.

NETZWERKTECHNIK / SEMESTER 1 und 2

Internet-Layer

Domain	Protocol
Internet Protocol	IPv4: Internet Protocol version 4. IPv4 receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
Internet Protocol	IPv6: IP version 6. IPv6 is similar to IPv4 but uses a 128-bit address.
Internet Protocol	NAT: Network Address Translation. NAT translates IPv4 addresses from a private network into globally unique public IPv4 addresses.
Messaging	ICMPv4: Internet Control Message Protocol for IPv4. ICMPv4 provides feedback from a destination host to a source host about errors in packet delivery.
Messaging	ICMPv6: ICMP for IPv6. ICMPv6 is similar in functionality to ICMPv4 but is used for IPv6 packets.
Messaging	ICMPv6 ND: ICMPv6 Neighbor Discovery. ICMPv6 ND includes four protocol messages that are used for address resolution and duplicate address detection.

Internet-Layer

Domain	Protocol
Routing protocols	OSPF: Open Shortest Path First. OSPF is a link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
Routing protocols	EIGRP: Enhanced Interior Gateway Routing Protocol. EIGRP is a Ciscoproprietary routing protocol that uses a composite metric based on bandwidth, delay, load, and reliability.
Routing protocols	BGP: Border Gateway Protocol. BGP is an open standard exterior gateway routing protocol used between internet service providers (ISPs). BGP is also commonly used between ISPs and their large private clients to exchange routing information.

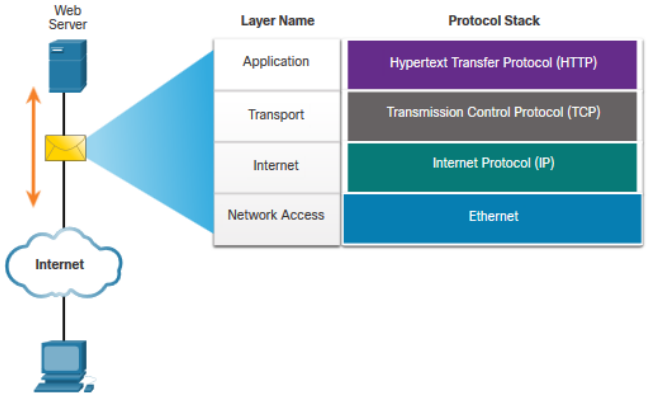
Network Access-Layer

Domain	Protocol
Address resolution	ARP: Address Resolution Protocol. ARP provides dynamic address mapping between an IPv4 address and a hardware address.
Data link protocols	Ethernet: Ethernet defines the rules for wiring and signaling standards of the network access layer.
Data link protocols	WLAN: Wireless local-area network. WLAN protocols define the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispiel für ein TCP/IP-Protokoll

- TCP/IP-Protokolle arbeiten auf Anwendungs-, Transport- und Internetebene.
- Die gebräuchlichsten LAN-Protokolle der Netzwerkzugriffsschicht sind Ethernet und WLAN (Wireless LAN).



tgm

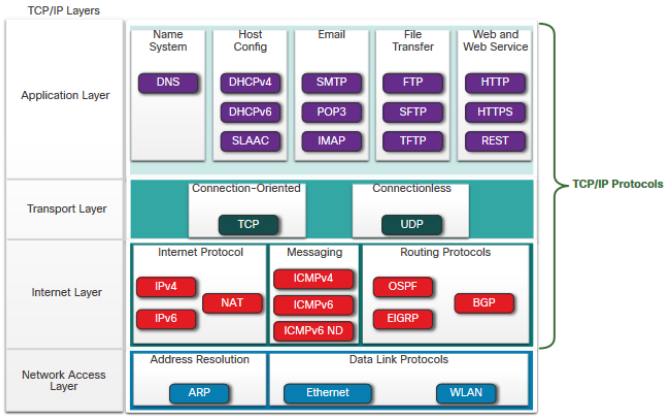
NETZWERKTECHNIK / SEMESTER 1 und 2

TCP/IP-Protokoll-Suite

- TCP/IP ist die vom Internet verwendete Protokollsuite und enthält mehrere Protokolle.

TCP/IP ist:

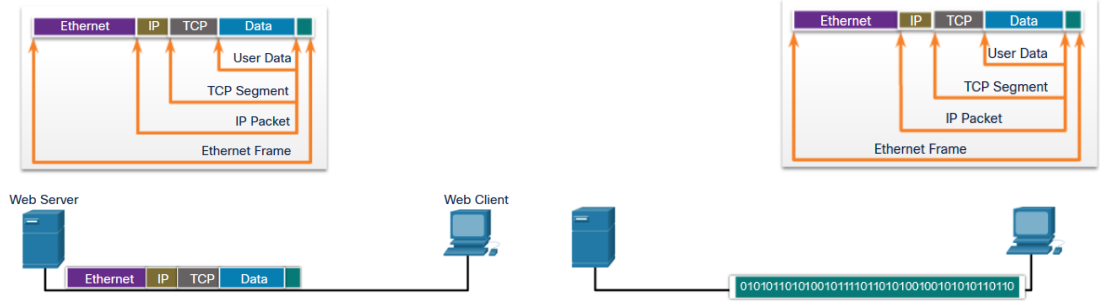
- Eine **offene** Protokollsuite, die der Öffentlichkeit frei zur Verfügung steht und von jedem Anbieter verwendet werden kann
- Eine **standard-basierte** Protokollsuite, die von der Netzwerkbranche unterstützt und von einer Standardisierungsorganisation genehmigt wird, um die Interoperabilität zu gewährleisten



tgm

TCP/IP-Kommunikationsprozess

- Ein Webserver, der die Information kapselt und die Webseite an einen Client sendet.
- Ein Client, der die Information entkapselt und die Webseite für den Webbrowser aufbereitet



41

04

Standardisierungs-organisationen

42

NETZWERKTECHNIK / SEMESTER 1 und 2

Offene Standards

Offene Standards fördern:

- Interoperabilität
- Wettbewerb
- Innovation

Normungsorganisationen sind:

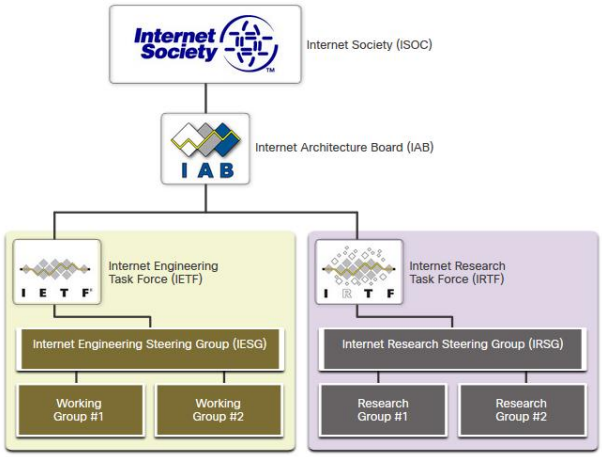
- Herstellerneutral
- Non-Profit-Organisationen
- Gegründet, um das Konzept der offenen Standards zu entwickeln und zu fördern.

43

NETZWERKTECHNIK / SEMESTER 1 und 2

Internet Standards

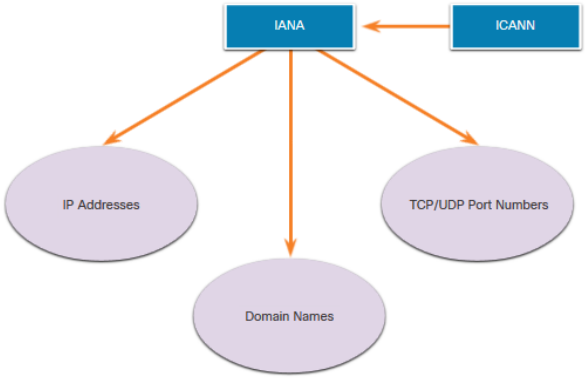
- **Internet Society (ISOC)** - Fördert die offene Entwicklung und Weiterentwicklung des Internets
- **Internet Architecture Board (IAB)** - Verantwortlich für das Management und die Entwicklung von Internetstandards
- **Internet Engineering Task Force (IETF)** - Entwicklung, Aktualisierung und Wartung von Internet- und TCP/IP-Technologien
- **Internet Research Task Force (IRTF)** - Konzentriert sich auf langfristige Forschung im Zusammenhang mit Internet- und TCP/IP-Protokollen
- .



44

Internet Standards

- Normungsorganisationen, die an der Entwicklung und Unterstützung von TCP/IP beteiligt sind
- **Internet Corporation for Assigned Names and Numbers (ICANN)** - koordiniert die Zuweisung von IP-Adressen, die Verwaltung von Domainnamen und die Zuweisung anderer Informationen
- **Internet Assigned Numbers Authority (IANA)** - Überwacht und verwaltet die Zuweisung von IP-Adressen, die Verwaltung von Domänennamen und Protokollkennungen für ICANN



Electronic and Communications Standards

- **Institute of Electrical and Electronics Engineers (IEEE, ausgesprochen "I-triple-E")** - widmet sich der Schaffung von Standards in den Bereichen Energie, Gesundheitswesen, Telekommunikation und Netzwerke
- **Electronic Industries Alliance (EIA)** - entwickelt Standards in Bezug auf elektrische Verkabelung, Steckverbinder und die 19-Zoll-Racks, die zur Montage von Netzwerkgeräten verwendet werden
- **Telecommunications Industry Association (TIA)** - entwickelt Kommunikationsstandards für Funkgeräte, Mobilfunkmasten, Voice-over-IP (VoIP)-Geräte, Satellitenkommunikation und mehr
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - definiert Standards für Videokomprimierung, Internet Protocol Television (IPTV) und Breitbandkommunikation, wie z. B. eine digitale Teilnehmerleitung (DSL)

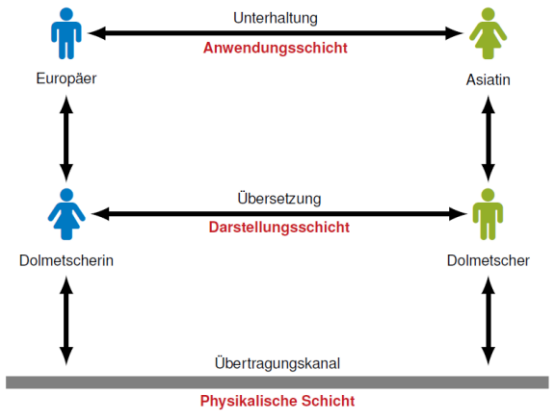
05

Referenz-modelle

47

Was sind Schichtenmodelle – ein einfaches Beispiel

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme, Kapitel 0, Technische Universität München, Lehrstuhl für Netzarchitekturen und Netzdienste]



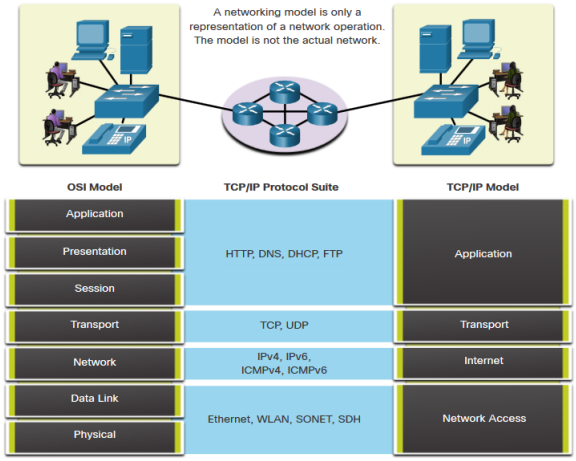
48

Die Vorteile der Verwendung eines Schichtmodells

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

Zwei Modelle existieren:

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



Die Vorteile der Verwendung eines Schichtmodells

- Unterstützung beim Protokolldesign, da Protokolle, die auf einer bestimmten Schicht arbeiten, über definierte Informationen verfügen, auf die sie reagieren, und über eine definierte Schnittstelle zu den oberen und unteren Schichten verfügen
- Fördern den Wettbewerb, da Produkte verschiedener Anbieter zusammenarbeiten können
- Verhindern, dass sich Technologie- oder Funktionsänderungen in einer Schicht auf andere Schichten darüber und darunter auswirken
- Bereitstellen einer gemeinsamen Sprache zum Beschreiben von Netzwerkfunktionen und Fähigkeiten

NETZWERKTECHNIK / SEMESTER 1 und 2

Das OSI-Referenzmodell

OSI Model Layer	Beschreibung
7 - Application	Enthält Protokolle, die für die Prozess-zu-Prozess-Kommunikation verwendet werden.
6 - Presentation	Stellt eine gemeinsame Darstellung der Daten bereit, die zwischen Diensten auf Anwendungsebene übertragen werden.
5 - Session	Stellt Dienste für die Darstellungsschicht zur Verwaltung der Dialoge und des Datenaustauschs.
4 - Transport	Definiert Dienste zum Segmentieren, Übertragen und Wiederzusammensetzen der Daten für die individuelle Kommunikation.
3 - Network	Bietet Dienste zum Austausch der einzelnen Datenteile über das Netzwerk.
2 - Data Link	Beschreibt Methoden zum Austauschen von Datenrahmen über ein allgemeines Medium.
1 - Physical	Beschreibt die Möglichkeiten zum Aktivieren, Aufrechterhalten und Deaktivieren physischer Verbindungen.

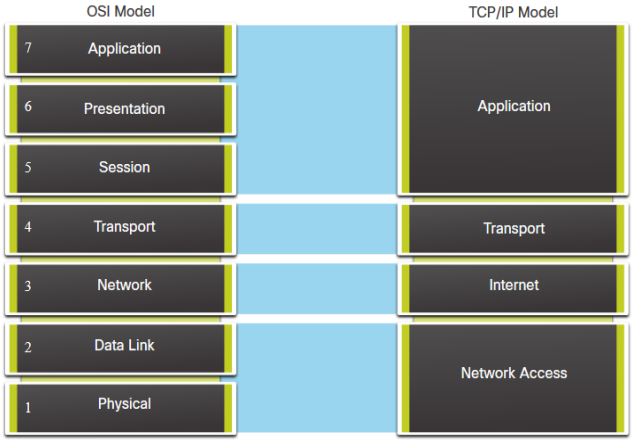
NETZWERKTECHNIK / SEMESTER 1 und 2

Das TCP/IP-Referenzmodell

TCP/IP Model Layer	Beschreibung
Application	Stellt Daten für den Benutzer sowie Codierung und Dialogfeldsteuerung dar.
Transport	Unterstützt die Kommunikation zwischen verschiedenen Geräten über verschiedene Netzwerke.
Internet	Bestimmt den besten Pfad durch das Netzwerk.
Network Access	Steuert die Hardwaregeräte und Medien, aus denen das Netzwerk besteht.

OSI and TCP/IP Model Comparison

- Das OSI-Modell unterteilt die Netzwerkzugriffsschicht und die Anwendungsschicht des TCP/IP-Modells in mehrere Schichten.
- Die TCP/IP-Protokollsuite spezifiziert nicht, welche Protokolle bei der Übertragung über ein physisches Medium verwendet werden sollen.
- OSI-Schichten 1 und 2 enthalten die notwendigen Prozeduren für den Zugriff auf das Übertragungsmedium.



53

06

Datenkapselung

54

54

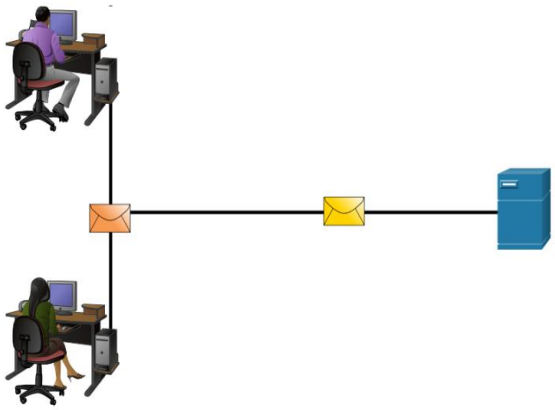
NETZWERKTECHNIK / SEMESTER 1 und 2

Segmentieren von Nachrichten

- Segmentierung ist der Prozess der Aufteilung von Nachrichten in kleinere Einheiten.
- Multiplexing ist der Prozess, bei dem mehrere Ströme segmentierter Daten miteinander verschachtelt werden.

Das Segmentieren von Nachrichten hat zwei Hauptvorteile:

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

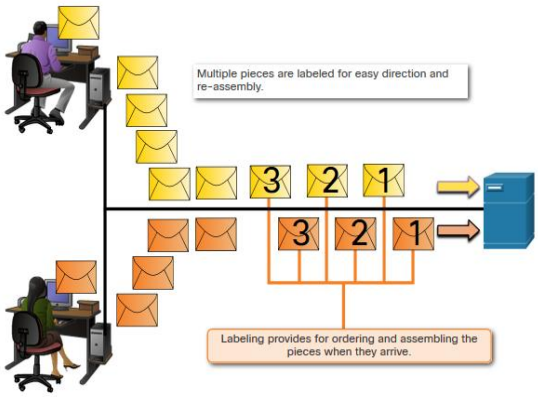


55

NETZWERKTECHNIK / SEMESTER 1 und 2

Sequenzierung

- Bei der Sequenzierung von Nachrichten werden die Segmente nummeriert, damit die Nachricht am Zielort wieder zusammengesetzt werden kann.
- TCP ist für die Sequenzierung der einzelnen Segmente zuständig.

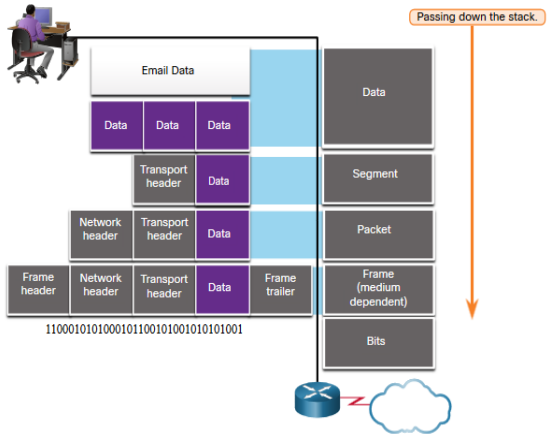


56

NETZWERKTECHNIK / SEMESTER 1 und 2

Protocol Data Units

- Kapselung ist der Prozess, bei dem Protokolle ihre Informationen zu den Daten hinzufügen.
- In jeder Phase des Prozesses erhält eine PDU einen anderen Namen, um ihre neuen Funktionen widerzuspiegeln.
- Es gibt keine allgemeingültige Namenskonvention für PDUs, hier werden die PDUs nach den Protokollen der TCP/IP-Suite benannt.
  - Daten (Datenstrom)
  - Segment
  - Paket
  - Rahmen
  - Bits (Bitstrom)

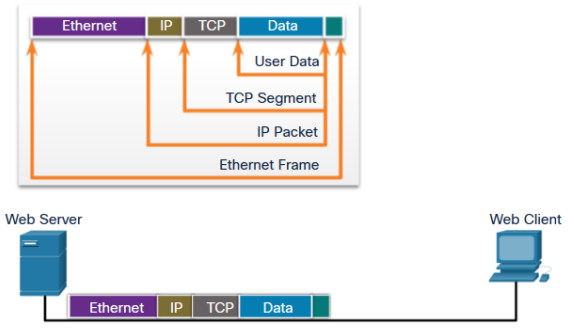


57

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispiel für eine Kapselung

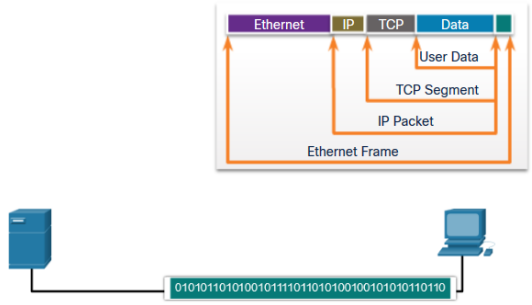
- Die Kapselung ist ein Top-Down-Prozess.
- Die darüber liegende Ebene führt ihren Prozess durch und übergibt ihn dann an die nächste Ebene des Modells. Dieser Vorgang wird von jeder Schicht wiederholt, bis sie als Bitstrom gesendet wird.



58

Beispiel für die Entkapselung

- Die Daten werden entkapselt, wenn sie im Stack nach oben verschoben werden.
- Wenn ein Layer seinen Prozess abgeschlossen hat, entfernt dieser Layer seinen Header und leitet ihn zur Verarbeitung an die nächste Ebene weiter. Dies wird auf jeder Schicht wiederholt, bis es sich um einen Datenstrom handelt, den die Anwendung verarbeiten kann.
  - Empfangen als Bits (Bitstrom)
  - Rahmen
  - Paket
  - Segment
  - Daten (Datenstrom)

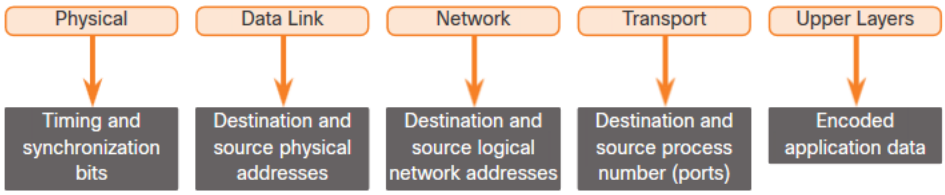


07

Datenzugriff

Adressen

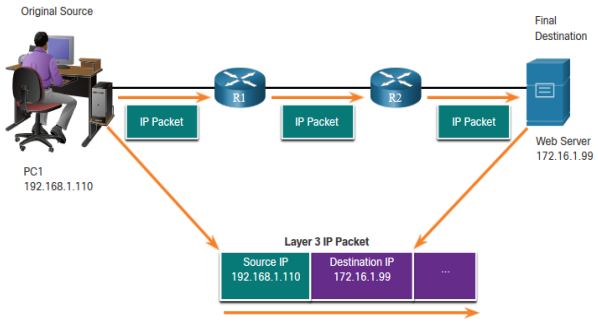
- Sowohl die Sicherungs- als auch die Netzwerkschicht verwenden die Adressierung, um Daten von der Quelle zum Ziel zu übermitteln.
- **Quell- und Zieladressen auf Netzwerkebene**: Verantwortlich für die Zustellung des IP-Pakets von der ursprünglichen Quelle zum endgültigen Ziel.
- **Quell- und Zieladressen der Sicherungsschicht** – Verantwortlich für die Bereitstellung des Frames von einer Netzwerkkarte (NIC) zu einer anderen Netzwerkkarte im selben Netzwerk.



Logische Layer-3-Adresse

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 lokal oder remote befinden.

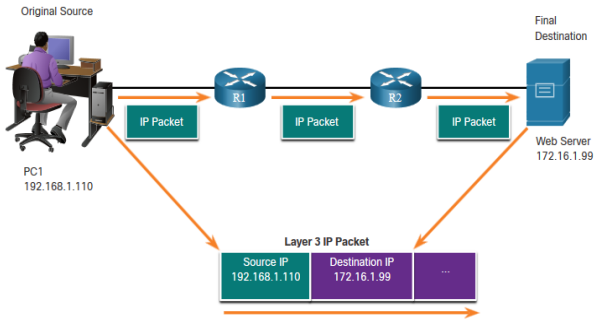


NETZWERKTECHNIK / SEMESTER 1 und 2

Logische Layer-3-Adresse

Eine IP-Adresse besteht aus zwei Teilen:

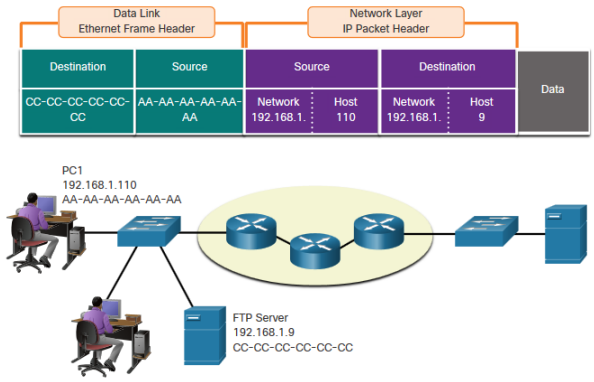
- **Netzwerkteil** (IPv4) oder Präfix (IPv6)
- Der linke Teil der Adresse gibt das Netzwerk an, in der die IP-Adresse Mitglied ist.
- **Hostteil** (IPv4) oder Schnittstellen-ID (IPv6)
- Der verbleibende Teil der Adresse identifiziert ein bestimmtes Gerät innerhalb des Netzwerkes.
- Dieser Teil ist für jedes Gerät im Netzwerk eindeutig.



NETZWERKTECHNIK / SEMESTER 1 und 2

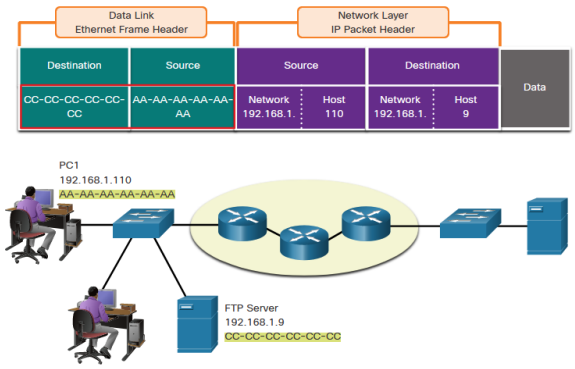
Geräte im selben Netzwerk

- Wenn sich Geräte im selben Netzwerk befinden, haben Quelle und Ziel dieselbe Nummer im Netzwerkteil der Adresse.
- PC1 – **192.168.1.**110
- FTP-Server – **192.168.1.**9



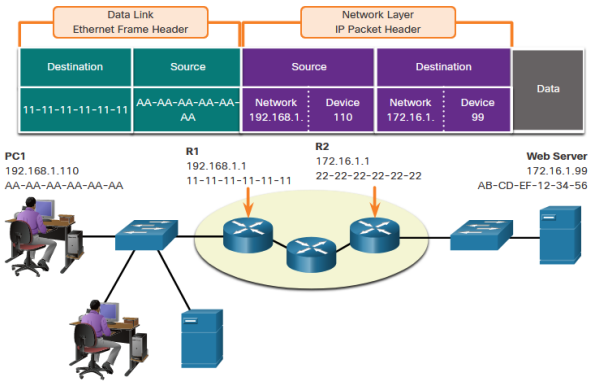
Rolle der Adressen der Sicherungsschicht: Gleiches IP-Netzwerk

- Wenn sich Geräte im selben Ethernet-Netzwerk befinden, verwendet der Data Link Frame die tatsächliche MAC-Adresse der Ziel-Netzwerkkarte.
- MAC-Adressen sind physisch in die Ethernet-Netzwerkkarte eingebettet und dienen der lokalen Adressierung.
- Die Quell-MAC-Adresse ist die des Absenders des Links.
- Die Ziel-MAC-Adresse befindet sich immer auf derselben Verbindung wie die Quelle, auch wenn das endgültige Ziel remote ist.



Geräte in einem Remote-Netzwerk

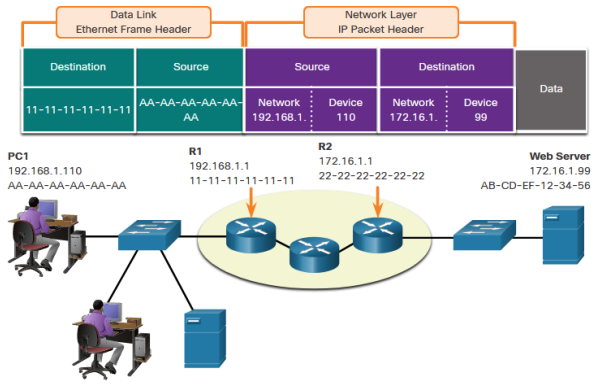
- Was passiert, wenn sich das eigentliche (endgültige) Ziel nicht im selben LAN befindet und remote ist?
- Was passiert, wenn PC1 versucht, den Webserver zu erreichen?
- Wirkt sich dies auf die Netzwerk- und Sicherungsschichten aus?



NETZWERKTECHNIK / SEMESTER 1 und 2

Rolle der Adressen der Netzwerkschicht

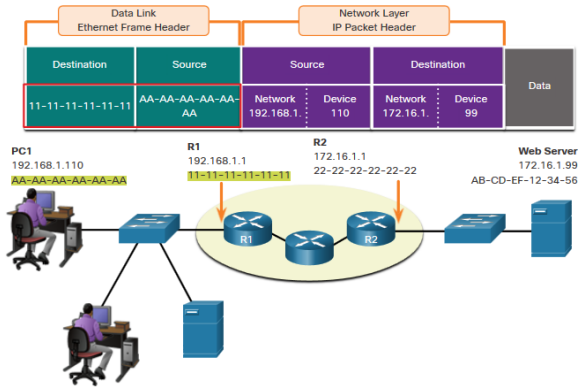
- Wenn Quelle und Ziel einen unterschiedlichen Netzwerkteil haben, bedeutet dies, dass sie sich in unterschiedlichen Netzwerken befinden.
- PC1 – **192.168.1**
- Webserver – **172.16.1**



NETZWERKTECHNIK / SEMESTER 1 und 2

Rolle der Adressen der Sicherungsschicht: Unterschiedliche IP-Netze

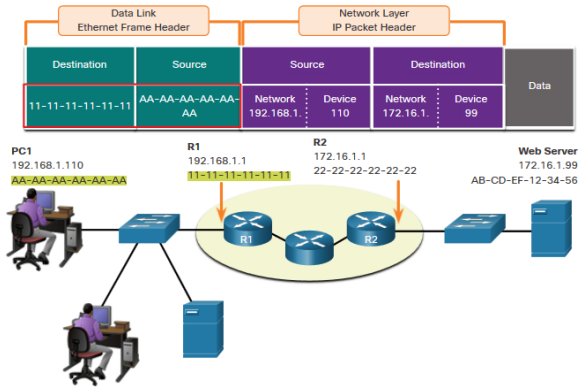
- Wenn das endgültige Ziel remote ist, stellt Layer 3 dem Layer 2 die lokale Standard-Gateway-IP-Adresse zur Verfügung.
- Das Standard-Gateway (DGW) ist die IP-Adresse der Router-Schnittstelle, die Teil dieses LAN ist und die "Tür" oder das "Gateway" zu allen anderen Remote-Standorten darstellt.
- Alle Geräte im LAN müssen über diese Adresse informiert werden, da sonst ihr Datenverkehr nur auf das LAN beschränkt wird.
- Sobald Layer 2 auf PC1 an das Standardgateway (Router) weitergeleitet wird, kann der Router den Routingprozess starten, um die Informationen an das tatsächliche Ziel zu übertragen.



NETZWERKTECHNIK / SEMESTER 1 und 2

Rolle der Adressen der Sicherungsschicht: Unterschiedliche IP-Netze

- Bei der Adressierung von Datenverbindungen handelt es sich um eine lokale Adressierung, sodass für jede Verbindung eine Quelle und ein Ziel vorhanden sind.
- 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 (R1 – Standard-Gateway-MAC) Empfängt den Frame.
- Hinweis: Während sich die lokale L2-Adressierung von Link zu Link oder von Hop zu Hop ändert, bleibt die L3-Adressierung gleich.

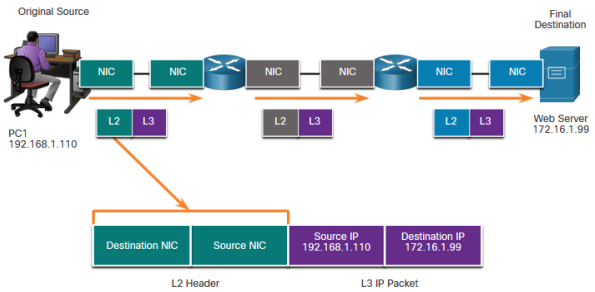


69

NETZWERKTECHNIK / SEMESTER 1 und 2

Data-Link Adresse

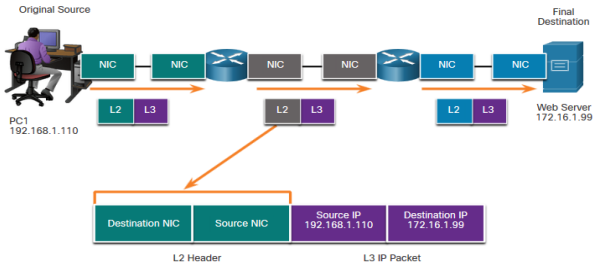
- Da es sich bei der Datenlink-Adressierung um eine lokale Adressierung handelt, gibt es für jedes Segment oder jeden Hop der Reise zum Ziel eine Quelle und ein Ziel.
- Die MAC-Adressierung für das erste Segment lautet:
- Quelle – (PC1 NIC) sendet Frame
- Ziel – (Erster Router – DGW-Schnittstelle) empfängt Frame



70

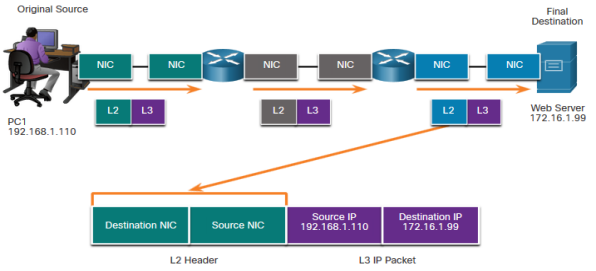
Data-Link Adresse

- Die MAC-Adressierung für den zweiten Hop lautet:
- Quelle – (Erste Router-Ausgangsschnittstelle) sendet Frame
- Ziel – (Zweiter Router) empfängt Frame



Data-Link Adresse

- Die MAC-Adressierung für das letzte Segment lautet:
- Quelle – (Zweiter Router – Ausgangsschnittstelle) sendet Frame
- Ziel – (Webserver-NIC) empfängt Frame



Data-Link Adresse

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