Adressierungskonzepte in der Netzwerktechnik

Unterrichtsfach	• Netzwerktechnik
Schulstufe	• 9. Schulstufe (1. Jg. HTBLA)
Thema	• Grundlagen: Adressierungskonzepte in der Netzwerktechnik
Fachliche Vorkenntnisse	• Bereich „Übertragungsmedien und Netztopologien“ • Schichtenmodelle in der Kommunikation (Mensch/Computer) • Umrechnung zwischen Binär-, Dezimal- und Hexadezimalzahlen
Fachliche Kompetenzen	Bereich „Schichtenmodelle und Protokolle“: • Modelle zur Rechnerkommunikation beschreiben können. • Anforderungen an Modelle zur Rechnerkommunikation allgemein charakterisieren können. • Die Applikation „Cisco Packet Tracer“ anwenden können.
Sprachliche Kompetenzen	• Einem Fachtext wesentliche Informationen entnehmen können. • Korrekte Fachsprache anwenden können.

Zeitbedarf	• 4 Unterrichtseinheiten à 50 Minuten
Material- & Medienbedarf	• Arbeitsrechner • Die App „Cisco Packet Tracer“ • Zusätzliches Papier, um die Berechnungen in Aufgabe 4 durchführen zu können (die Ausarbeitung muss mit abgegeben werden)
Methodisch-didaktische Hinweise	• Tools Scaffolds: Lückentext, Recherche, Worterklärungen, Kreuzworträtsel, Mindmap • Sozialformen: Einzel- und Partnerarbeit Das Unterrichtsbeispiel besteht aus 7 Aufgaben, die aufeinander aufbauen: • Die Berechnungen in Aufgabe 4 sollten die Schüler/innen der Lehrperson in Papierversion abgeben. • Die Aufgaben 5 und 6 können auch zu einem späteren Zeitpunkt durchgeführt werden. • Für Aufgabe 6 benötigt man die freie App „Cisco Packet Tracer“ – Näheres dazu auf S. 19.
Quellen	• Echolot: Sgbeer, https://commons.wikimedia.org/w/index.php?curid=8544983 (CC BY-SA 3.0) • Screenshot Aufgabe 6: erstellt mit Cisco Packet Tracer
Ersteller	• Johann Feichtenschlager

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 1: Adressen im Schichtenmodell

Sie haben sich bereits mit dem OSI-Schichtenmodell auseinandergesetzt. Das OSI-Schichtenmodell kennt auf drei der verschiedenen Schichten Adressierungen, die den Weg eines Pakets über ein Datennetz bestimmen und die Zustellung dieser Pakete garantieren. Das OSI-Schichtenmodell besteht aus sieben Schichten, denen folgende Adressierungen in einem IP-Netzwerk zugewiesen werden:

Schicht	**Adressierung**
Anwendungsschicht	-
Darstellungsschicht	-
Sitzungsschicht	-
Transportschicht	Portnummern
Netzwerkschicht	IPv4-Adressen
Sicherungsschicht	MAC-Adressen
Bitübertragungsschicht	-

Suchen Sie im Internet nach den verschiedenen Adressierungsarten.
Gute Seiten für Informationen dazu sind:

- MAC-Adressen: https://www.elektronik-kompendium.de/sites/net/1406201.htm
- IPv4-Adressen: https://www.elektronik-kompendium.de/sites/net/2011211.htm
- Portnummern: https://www.elektronik-kompendium.de/sites/net/1812041.htm

Die Ergebnisse Ihrer Recherche helfen Ihnen beim Ausfüllen des Lückentexts auf der nächsten Seite. Schreiben Sie die passenden Wörter und Zahlen in die Lücken. Die erste Lücke ist bereits ausgefüllt.

Hardwareadressen – Gerät – 48 – Herstellerkennung – ~~MAC-Adressen~~ – Dezimal
6 – Netzwerkanteil – Gerätekennung – 0 – Herstellerkennung – Bindestriche –
vier – Hostanteil – 4 – hexadezimalen von 0 bis 65.535
Dynamically Allocated Ports – UDP – Well Known Ports – Punkt – Registered Ports
Doppelpunkte – 255 – Softwareadressen – Subnetzmaske – IPv4-Adressen
8 – Anwendungen – TCP – 256 – zwei – 32

Adressierungskonzepte in der Netzwerktechnik

Die Sicherungsschicht verwendet in Computernetzen MAC-Adressen. Diese werden auch _____ genannt und identifizieren ein bestimmtes Interface am _____ in einem Computernetzwerk. Eine MAC-Adresse besteht aus _____ Bit oder _____ Byte. Sie ist in _____ Teile geteilt, die _____ und die _____ Die _____ wird abgekürzt als OUI (Organizationally Unique Identifier). Eine MAC-Adresse wird in _____ Zahlen, die entweder durch _____ oder _____ getrennt sind, dargestellt.

_____ werden in der dezentralen Kommunikation in der Netzwerkschicht eingesetzt. IPv4-Adressen werden auch als _____ bezeichnet. Sie können mit der Adresse auf einem Brief zu Ort, Straße und Hausnummer verglichen werden. Die IPv4-Adresse hat eine Länge von _____ Bit oder _____ Byte. Um IPv4-Adressen besser lesbar zu machen, wird sie in _____ Teile mit jeweils _____ Bit aufgeteilt. Die Darstellung erfolgt in vier _____zahlen, die jeweils durch einen _____ getrennt werden. Der Zahlenumfang beträgt pro Byte _____ Zahlen, die einen Zahlenbereich von _____ bis _____ ergeben. Auch diese Adressen haben zwei Anteile, den _____ und den _____ Die Größe der Anteile wird durch die sogenannte _____ bestimmt.

Für die Adressierung von _____ werden Portnummern verwendet. Portnummern haben einen Zahlenbereich _____ Portnummern sind mit den Protokollen _____ und _____ assoziiert. Es gibt drei verschiedene Kategorien von Ports: _____ (0 – 1.023), _____ (1.024 – 49.151) und _____ (49.152 – 65.535).

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 2: Die Konfiguration Ihres Arbeitsrechners untersuchen

Jedes Gerät, das mit einem Netzwerk verbunden ist, hat eine MAC-Adresse (Hardwareadresse) und eine IPv4-Adresse (Softwareadresse). Das gilt auch für Ihren Arbeitsrechner oder Ihr Mobiltelefon. Die folgenden Aufgaben widmen sich der Netzwerkkonfiguration Ihres Arbeitsrechners. Je nach Betriebssystem gibt es verschiedene Möglichkeiten, die Hardware- und Softwareadresse eines Rechners herauszufinden.

Windows-10-Rechner bieten drei Möglichkeiten, um die verschiedenen Adressen eines Rechners anzuzeigen:

- **Eingabeaufforderung:** Geben Sie im Suchfeld auf der linken Seite der Taskleiste „cmd.exe“ oder „Eingabeaufforderung“ ein. Es öffnet sich ein sogenanntes Command-Line Interface (CLI). Im Command-Line Interface geben Sie neben dem Command Prompt, zum Beispiel C:\>, den Befehl *ipconfig /all* ein. Es werden alle Netzwerkadapter des Rechners gelistet. Der aktive Adapter ist derjenige, dem auch ein sogenannter „Standardgateway“ zugewiesen wurde.
- **Windows PowerShell:** Geben Sie im Suchfeld „PowerShell” ein. Auch die PowerShell ist ein CLI (Command-Line Interface). Die Vorgehensweise ist gleich wie bei der Eingabeaufforderung.
- **Einstellungen -> Netzwerk und Internet -> Hardwareeigenschaften:** Mit dieser Option werden die Informationen zum genutzten Netzwerkadapter in einem GUI (Graphical User Interface) angezeigt.

Linux-Rechner, aber auch **Apple-Rechner** bieten zwei verschiedene Möglichkeiten, um diese Informationen anzuzeigen:

- **Terminal:** Beide Betriebssysteme bieten wie Windowssysteme ein CLI, um Befehle auszuführen. Mit dem Kommando *ifconfig* werden die Informationen über die installierten Netzwerkadapter angezeigt.
- **GUI:** Da verschiedene Linux-Distributionen existieren, sind die Informationen unterschiedlich abrufbar. Normalerweise findet man wie bei Windows-Systemen die Informationen unter den Einstellungen des Betriebssystems.

Adressierungskonzepte in der Netzwerktechnik

Die Abbildung zeigt das Command Line Interface (Eingabeaufforderung) von Windows:

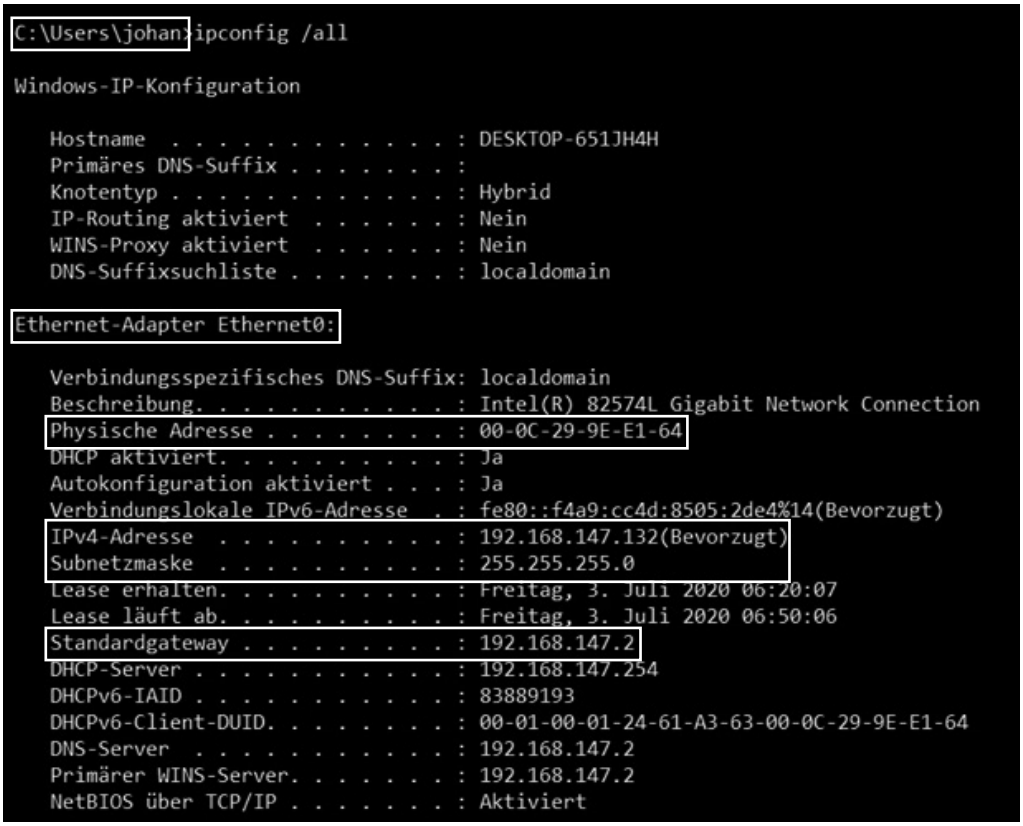
Command Prompt

Aktiver Adapter

MAC-Adresse oder Hardware-adresse

IPv4-Adresse oder Software-adresse

Standard-gateway



Finden Sie die Hardware- und Softwareadresse (MAC- und IPv4-Adresse) mittels einer der oben genannten Methoden heraus.

Beschreiben Sie Ihre Vorgangsweise und das Ergebnis in ganzen Sätzen.
Gehen Sie dabei auch auf diese Fragestellungen ein:

- Welches Betriebssystem ist auf Ihrem Rechner installiert?
- Welche Darstellungsmethode haben Sie verwendet?
- Welcher Netzwerkadapter wird genutzt?
- Wie lautet die MAC-Adresse (Hardwareadresse) Ihres Rechners?
- Wie lautet die IPv4-Adresse (Softwareadresse) und die dazugehörige Subnetzmaske?

Erstellen Sie in Partnerarbeit eine Mindmap, in der Sie die verschiedenen Möglichkeiten nennen, wie man die Hard- und Softwareadresse eines Rechners eruieren (herausfinden) kann. Verwenden Sie für die Erstellung der Mindmap folgenden Link: https://mind-map-online.de.

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 3: MAC-Adressen

MAC-Adressen werden auch als „Geräteadressen“, „Hardwareadressen“ oder „Physische Adressen“ bezeichnet. Sie haben eine Länge von 48 Bit und werden mit einer Größe von je 24 Bit in zwei Teile eingeteilt: die Herstellerkennung (Organizationally Unique Identifier – OUI) und die Gerätekennung. Eine MAC-Adresse wird in einer Folge von je 8 Bit in Hexadezimalschreibweise angegeben und durch einen Bindestrich oder einen Doppelpunkt getrennt.

Beispiele: 1C-1B-B5-92-38-80 oder 1C:1B:B5:92:38:80

- Recherchieren Sie auf der Webseite https://aruljohn.com/mac.pl, zu welchem Hersteller die MAC-Adresse des aktiven Netzwerkadapters Ihres Arbeitsrechners passt.
- Lassen Sie sich die MAC-Adressen von fünf Ihrer Mitschüler/innen geben und ermitteln Sie von diesen fünf Adressen die Hersteller.
- Stellen Sie die Ergebnisse als Tabelle dar und verwenden Sie dafür ein Tabellenkalkulationsprogramm (z. B. Microsoft Excel). Gliedern Sie die Tabelle so:

Name	**MAC-Adresse**	**OUI**	**Hersteller**
Max Mustermann	1C-1B-B5-92-38-80	1C-1B-B5	Intel Corporate
...	...	...	...

Sie können auf der Webseite https://aruljohn.com/mac.pl auch die OUIs der verschiedenen Hersteller recherchieren (herausfinden). Normalerweise ist ein Hersteller nicht nur auf eine einzige Herstellerkennung festgelegt, sondern besitzt eine Vielzahl an Oganizationally Unique Identifiers (OUI), um Produkte im Netzwerkbereich mit eindeutigen Kennungen zu versehen.

- Recherchieren Sie die Anzahl der MAC-Adressen, die im Besitz der folgenden Hersteller sind: ASUS, SAMSUNG, APPLE, MOTOROLA, SIEMENS, MICROSOFT, CISCO.
- Geben Sie die ersten drei Ergebnisse der Suche wie im nächsten Punkt angegeben an.
- Formulieren Sie ihre Ergebnisse in ein bis zwei kurzen Sätzen.

Beispiel:

Der Hersteller INTEL verfügt über 396 Herstellerkennungen. Die ersten drei OUIs in der Ergebnisliste sind 94-E6-F7, 4C-1D-96 und 50-E0-85.

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 4: IPv4-Adressierung

IPv4-Adressen und Subnetzmasken werden aufgrund besserer Lesbarkeit in der sogenannten „Dotted Decimal Notation", kurz DDN, aufgeschrieben. IPv4-Adressen oder Subnetzmasken bestehen aus vier Dezimalzahlen, die durch einen Punkt getrennt werden.

Beispiel: IPv4-Adresse 192.168.10.1 mit einer Subnetzmaske 255.255.255.0

Diese Darstellung steht stellvertretend für binäre Zahlen mit einer Länge von je 8 Bit. Mit 8 Bit lassen sich in dezimaler Schreibweise Zahlen von 0 bis 255 darstellen, wobei die Zahl 0 mit 0000 0000 in binärer Schreibweise angeschrieben wird. Die Zahl 255 entspricht in binärer Schreibweise 1111 1111. Nachdem einer der vier Teile einer IPv4-Adresse 8 Bit lang ist, beträgt die Länge einer IPv4-Adresse 32 Bit.

Beispiel: 192.168.10.1

192	168	10	1
1100 0000	1010 1000	0000 1010	0000 0001

Zu Beginn des Internets, als der Standard für IPv4-Adressen erstellt wurde, dachten die Ingenieure und Ingenieurinnen, die sich mit diesem Standard beschäftigten, dass die verschiedenen IPv4-Netze sich wie bei Telefonnetzen einteilen lassen würden und man an der IPv4-Adresse das Land des Kommunikationspartners erkennen sollte. Telefonnummern bestehen aus einer Länderkennzahl, einer Ortskennzahl und der Rufnummer.

Daher führte man verschieden IPv4-Adressklassen ein. Je nach Größe der Staaten sollten die Klassen zugewiesen werden. Man legte fünf Klassen (Klasse A bis Klasse E) fest, wobei nur die ersten drei Klassen A, B, C für die Verwendung als Unicast-Adressen vorgesehen sind.

Die IPv4-Adressen der Klasse D werden für Multicast-Adressierung verwendet und die IPv4-Adressen der Klasse E sind für experimentelle Anwendungen gedacht. Im Folgenden sehen Sie hier ausschließlich Klassen aus dem Unicast-Bereich, also die Klassen A bis C.

<table>
<tr><td colspan="5">Klasse A (0.0.0.0 bis 127.255.255.255)</td></tr>
<tr><td>0</td><td colspan="2">Netz-ID (7 Bit)</td><td colspan="2">Host-ID (24 Bit)</td></tr>
<tr><td colspan="5">Klasse B (128.0.0.0 bis 191.255.255.255)</td></tr>
<tr><td>1</td><td>0</td><td colspan="2">Netz-ID (14 Bit)</td><td>Host-ID (16 Bit)</td></tr>
<tr><td colspan="5">Klasse B (192.0.0.0 bis 223.255.255.255)</td></tr>
<tr><td>1</td><td>1</td><td>0</td><td>Netz-ID (21 Bit)</td><td>Host-ID (8 Bit)</td></tr>
</table>

Adressierungskonzepte in der Netzwerktechnik

Die ersten vier Bits in einer IPv4-Adresse (gelb gekennzeichnet) legen fest, zu welcher IPv4-Klasse diese IPv4-Adresse gehört. Das Verfahren zur Feststellung der Zugehörigkeit einer IPv4-Adresse nennt man „First Octet Rule“. Die vier durch Punkte getrennten Teile einer IPv4-Adresse werden auch als Oktette bezeichnet. Für die „First Octet Rule“ werden nur die ersten vier Bit im ersten Oktett herangezogen, um die IPv4-Klasse zu bestimmen.

Als Beispiel soll wieder die IPv4-Adresse 192.168.10.1 dienen. Sie betrachten nur das erste Oktett:

Die Dezimalzahl 192 ergibt in binärer Schreibweise die binäre Zahl 1100 0000. Man benötigt die ersten 4 Bits, um die IPv4-Klasse festzulegen. Die ersten vier Bits besteht aus der Bitfolge 1100 und gehören demnach zur IPv4-Klasse C.

In der Grafik besitzen die Klassen zusätzlich zu den ersten Bits zwei verschiedene Abschnitte: den Netzanteil und den Hostanteil. Der Netzanteil beschreibt die Anzahl der möglichen Netze, der Hostanteil bezeichnet die Anzahl der möglichen Hosts in einem Netzwerk.

Klasse	**Anzahl Netze**	**Anzahl Hosts**	**Subnetzmaske**
Class A	128 Netze	16.777.214 Adr./Netz	255.0.0.0
Class B	16.384 Netze	65.534 Adr./Netz	255.255.0.0
Class C	2.097.152 Netze	254 Adr./Netz	255.255.255.0

Diese drei Subnetzmasken bezeichnet man als Standardsubnetzmasken und diese legen Netz- und Hostanteil der Klassen in binärer Form fest. Der Netzanteil besteht binär aus Einsen, der Hostanteil aus binären Nullen. Zu der Anzahl der Hosts ist festzustellen, dass es sich hier um die Anzahl der nutzbaren IPv4-Adressen handelt. Die erste Adresse eines Netzes wird als Netz-ID, die letzte Adresse eines Netzes als Broadcast-ID bezeichnet.

Die IPv4-Adresse 192.168.10.1 gehört zur Klasse C und muss demnach durch die Subnetzmaske 255.255.255.0 definiert sein. Die Netzwerk-ID ist 192.168.10.0, die Broadcast-ID ist 192.168.10.255.

255	255	255	0
1111 1111	1111 1111	1111 1111	0000 0000

Adressierungskonzepte in der Netzwerktechnik

Bestimmen Sie mittels der „First Octet Rule“ die Klassen der gegebenen IPv4-Adresse und weisen Sie die Standardsubnetzmaske zu.

Geben Sie die Anzahl der nutzbaren Adressen sowie die Netzwerk-ID und die Broadcast-ID an. Verwenden Sie diese Tabelle:

IPv4-Adresse	Klasse	Subnetz-maske	Anzahl Host-Adressen	Netzwerk-ID	Broadcast-ID
192.168.10.1	C	255.255.255.0	254	192.168.10.0	192.168.10.255
10.20.30.255					
129.120.24.25					
204.132.10.20					
84.10.100.255					
172.16.25.55					

Zeigen Sie die Umwandlung des ersten Oktetts (erste Dezimalzahl) der gelisteten IPv4-Adressen von Dezimal in Binär!

Beispiel der Umwandlung des dezimalen Wertes 80 in eine binäre Zahl:
(IPv4-Adresse 80.20.20.20)

80 mod 2 = 0
40 mod 2 = 0
20 mod 2 = 0
10 mod 2 = 0
5 mod 2 = 1
2 mod 2 = 0
1 mod 2 = 1

Es ergibt sich für das erste Oktett der binäre Wert 1010000. Da die binäre Zahl nur 7 Bits besetzt, muss der Anfang mit Nullen aufgefüllt werden: 0101 000. Diese Adresse ist eine Klasse A IPv4-Adresse.

Adressierungskonzepte in der Netzwerktechnik

Lesen Sie sich den Text zu den IPv4-Adressen noch einmal aufmerksam durch und beantworten Sie die Fragen in ganzen Sätzen.

Was versteht man unter der „Dottet Decimal Notation“?

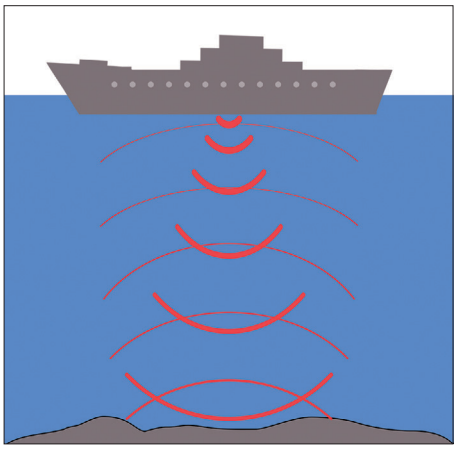
Warum werden IPv4-Adressen in Dezimalzahlen anstatt in binären Zahlen dargestellt?

Woran kann man die IPv4-Adressklasse festlegen und welches Verfahren hilft Ihnen dabei, die Zugehörigkeit zu einer Klasse zu identifizieren?

Wofür wird die Subnetzmaske benötigt?

Adressierungskonzepte in der Netzwerktechnik

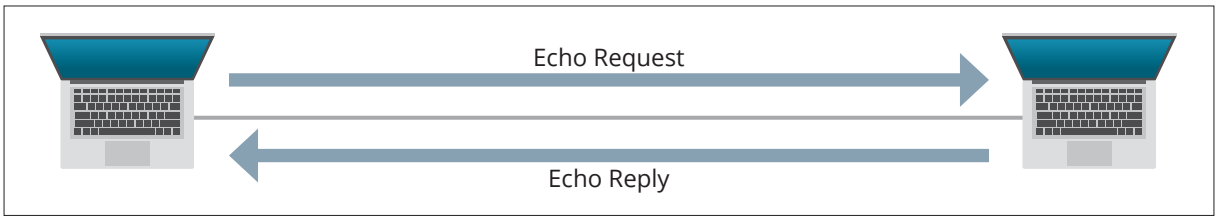
Aufgabe 5: Der „Ping“



Quelle: https://de.wikipedia.org/wiki/Echolot

„Das Echolot ist ein in der Schifffahrt verwendetes Gerät zur elektroakustischen Messung von Wassertiefen (Lotung). Gemessen wird die Zeit, die zwischen der Aussendung eines Schallimpulses (Wasserschall) und der Ankunft der vom Gewässerboden reflektierten Schallwellen verstreicht.“

Wie das Echolot ist der „Ping“ ein technisches Hilfsmittel, mit dem man die Zeit misst, die ein Signal benötigt, um von einem Sender zu einem Empfänger und wieder zurück zu gelangen. In der Kommunikationstechnik nennt man diesen Vorgang „Round-Trip-Time“ (RTT). Diese Technik ist dem Echolot sehr ähnlich. Sogar die Bezeichnungen für die Signalisierung wurde von der Seefahrt abgeleitet. Wie bei einem Echolot werden „Pings“ abgesetzt. Es wird in beiden Fällen auf ein Echo gewartet und damit die Zeit gemessen, die ein Signal benötigt, um zum Ausgangspunkt zurückzukehren.



Ein „Ping“ ist eine Anwendung des Protokolls ICMP (Internet Control Message Protocol), welches in das Internet Protocol eingebettet ist. ICMP ist ein Protokoll der Netzwerkschicht.

„Ping“ verwendet zwei Nachrichtentypen: „Ping“ sendet mit einem „Echo Request“ ein Paket an den Empfänger, der mit dessen IP-Adresse angegeben wird. Der Empfänger sendet ein „Echo Reply“ an den Empfänger zurück.

„Ping“ ist ein wichtiges Tool für Netzwerktechniker/innen, um eine Verbindung zu testen. Ist ein „Ping“ erfolgreich, besteht eine Verbindung zwischen Sender und Empfänger. Das bedeutet im Netzwerktechniker-Jargon, dass Konnektivität gegeben ist.

Adressierungskonzepte in der Netzwerktechnik

Öffnen Sie unter Windows die Eingabeaufforderung oder unter Linux/MAC-OS die Konsole.

Finden Sie die IPv4-Adresse Ihres Standardgateways heraus. Unter Windows finden Sie das Standardgateway mit dem Befehl „ipconfig“, unter Linux/MAC-OS mit dem Befehl „route -n“.

Linux/MAC-OS:

```
carver2712@ubuntu:~$ route -n
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.147.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.147.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
```

Beispiel eines „Pings“ zu 192.168.147.2:

C:\> ping 192.168.147.2

Recherchieren Sie im Internet die Bedeutung der Abkürzung „TTL“ und erörtern Sie, welche Statistiken nach Abschluss der Abarbeitung des „Pings“ angezeigt werden.

Schreiben Sie eine Zusammenfassung Ihrer Recherche und interpretieren Sie das Ergebnis des „Pings“.

Bitten Sie Ihren Sitznachbarn/Ihre Sitznachbarin um die IPv4-Adresse seines/ihres Rechners und setzen Sie zu dieser IPv4-Adresse „Pings“ ab. Erstellen Sie einen Screenshot der Ausgabe der „Pings“.

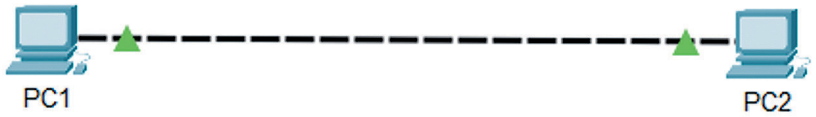
Adressierungskonzepte in der Netzwerktechnik

Aufgabe 6: Beobachtung eines „Pings“ im Packet Tracer

Diese Aufgabe widmet sich der Untersuchung eines „Pings“. Sie werden den Ablauf eines „Pings“ mit „Echo Request“ und „Echo Reply“ verfolgen und einige Fragestellungen dazu beantworten.

Für diese Aufgabe verwenden Sie die App „Cisco Packet Tracer“.

1. **Öffnen Sie die App und erstellen Sie folgende Topologie:**



2. **Konfigurieren Sie die PCs**. Klicken Sie dazu auf einen PC, wählen Sie unter der Registerkarte „Desktop“ die Applikation „IP Configuration“ und konfigurieren Sie folgende IPv4-Adressen und Subnetzmasken:

PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0

   Hinweis: Die IPv4-Adressen liegen im gleichen Netzwerk, haben also die gleiche Netzwerk-ID 192.168.1.0 mit der Standardsubnetzmaske 255.255.255.0.

3. **Prüfen Sie im jeweiligen „Command Prompt“** (zu finden unter der Registerkarte „Desktop“) den Erfolg Ihrer Konfigurationen.
   a. Wie lautet das Kommando?
   b. Geben Sie die MAC-Adressen der PCs an und erstellen Sie Screenshots der Ausgaben. (Beispiel: Die MAC-Adresse von PC1 lautet 23:24:25:12:AB:AC.)
   c. Wie wird die MAC-Adresse im „Cisco Packet Tracer“ ausgegeben? Stimmt die Ausgabe mit der gängigen Schreibweise für MAC-Adressen überein? Beschreiben Sie den Unterschied in ganzen Sätzen!

4. **Setzen Sie einen „Ping“ zwischen PC1 und PC2 ab.**
   a. Ist der „Ping“ erfolgreich?
   b. Erläutern Sie die Statistiken des „Pings“ (Statistics, Round Trip Times).

5. **Ändern Sie am PC2 die IPv4-Adresse** zu 192.168.10.2 und „pingen“ Sie diese vom PC1 aus. Der „Ping“ ist nicht erfolgreich. Warum ist der „Ping“ nicht erfolgreich?
   Der „Ping“ zwischen PC1 und PC2 ist nicht erfolgreich, weil …
   Ändern Sie die IPv4-Adresse am PC2 wieder auf 192.168.1.2 zurück!

Adressierungskonzepte in der Netzwerktechnik

6. **Untersuchung der ICMP-Pakete im Simulationsmodus:**

   a. Wechseln Sie in den Simulationsmodus und stellen Sie auf der rechten Seite des Fensters den Filter auf ICMP ein.

   b. Setzen Sie einen „Ping“ zu PC2 ab. Es erscheint ein Kuvert am PC1. Klicken Sie auf das Kuvert. Es öffnet sich ein neues Fenster, in welchem verschiedene Informationen zum Paket angezeigt werden. Beantworten Sie die folgenden Fragen.

   - Die Überschrift des Fensters lautet „PDU Information at Device: PC1“. Recherchieren Sie im Internet zu der Abkürzung „PDU“ und erläutern Sie kurz, was es mit der Abkürzung auf sich hat.
   - Sehen Sie sich die Informationen auf der rechten Seite unter „Out Layers“ an und listen Sie folgende Informationen:

Source IPv4-Adresse:		Destination IPv4-Adresse:	
ICMP Message Type:		Source MAC-Adresse:	
Destination MAC-Adresse:			

   - Wofür steht der ICMP Message Type?

     ☐ ICMP Echo Request ☐ ICMP Echo Reply

   - Klicken Sie auf „Layer 3“ unter „Out Layers“. Übersetzen Sie die vier Punkte unter den Tabellen zu „In Layers“ und „Out Layers“.

   c. Klicken Sie unter „Play Controls“ auf der rechten Seite des Fensters auf das Zeichen ⏯ . Das Kuvert bewegt sich zum PC2. Klicken Sie auf das Kuvert.

   - Sehen Sie sich die Informationen auf der rechten Seite unter „Out Layers“ an und listen Sie folgende Informationen:

Source IPv4-Adresse:		Destination IPv4-Adresse:	
ICMP Message Type:			

   - Wofür steht der ICMP Message Type?

     ☐ ICMP Echo Request ☐ ICMP Echo Reply

   - Klicken Sie auf „Layer 3“ unter „Out Layers“. Übersetzen Sie die drei Punkte unter den Tabellen zu „In Layers“ und „Out Layers“.
   - Vergleichen Sie die Informationen von „In Layers“ und „Out Layers“ am „Layer 3“. Erklären Sie die Änderungen der Inhalte in ganzen Sätzen.

   d. Mit der Tastenkombination ALT + P können Sie den Rest der Kommunikation ablaufen lassen. Tun Sie das, klicken Sie nach Ablauf der Kommunikation auf das Kuvert am PC 1 (es werden keine neuen Pakete versendet), sehen Sie sich die Informationen am „Layer 3“ und am „Layer 2“ an und übersetzen Sie diese.

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 7: Adressierung in der Transportschicht

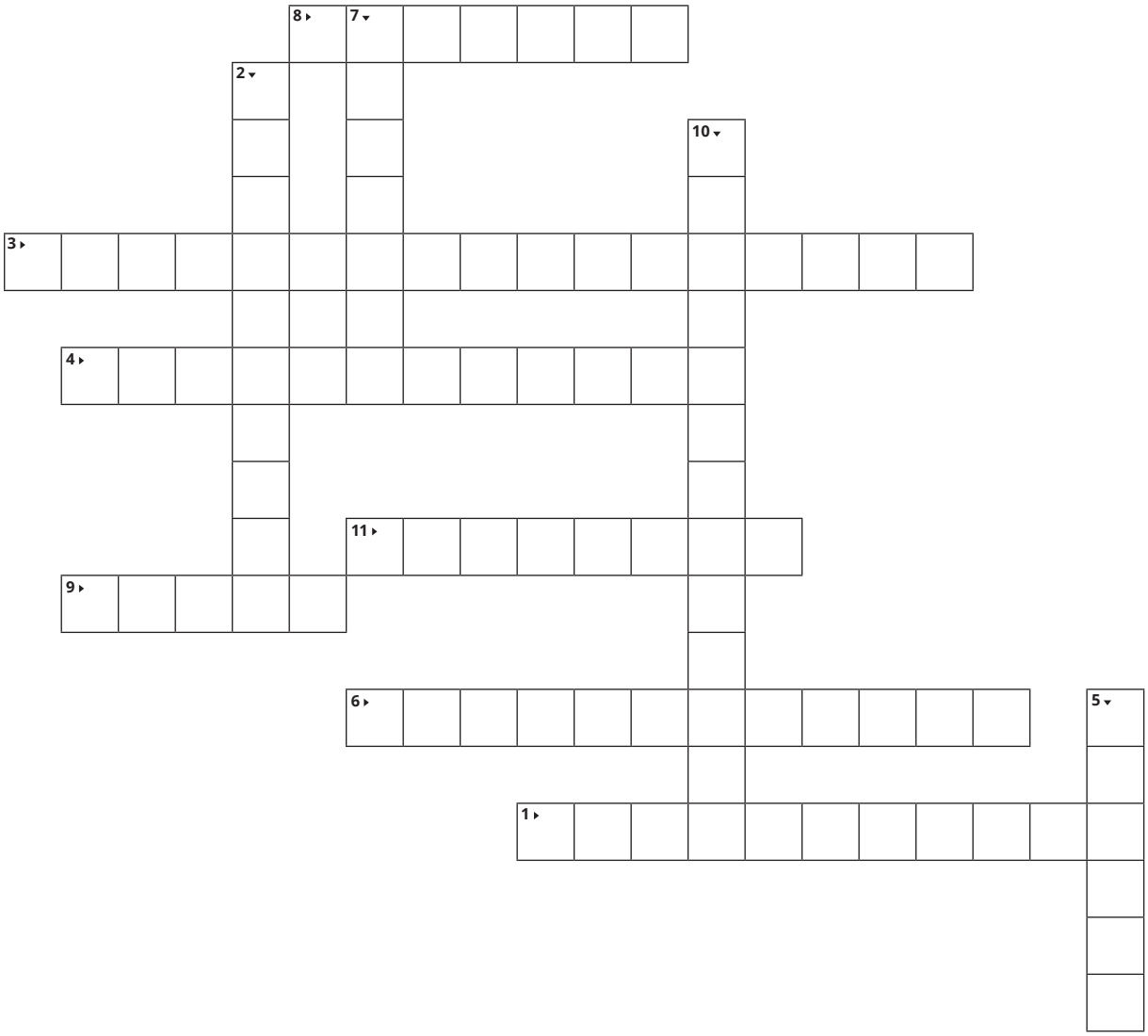
Die Transportschicht ist der Vermittler zwischen den anwendungs- und netzwerkorientierten Schichten. In der Transportschicht werden die Anwendungen mit sogenannten Portnummern adressiert. Ein Client sendet eine Anfrage (Request) an einen Server, welcher in Folge dem Client mit einer Antwort (Response) Inhalte zur Verfügung stellt oder Daten verarbeitet. Ein Ihnen sicherlich bekanntes Beispiel ist das Protokoll HTTP: Mit Hilfe eines am Client installierten Browsers werden von einem Webserver Inhalte angefordert und im Browser dargestellt. HTTP wurde die Portnummer 80 zugewiesen. Dabei „horcht" der Server am Port 80, ob Anfragen an ihn gestellt werden.

Finden Sie mit Hilfe des Internets heraus, welche Protokolle hinter den angegebenen Portnummern stecken. Beschreiben Sie die Aufgabe der Protokolle und welches Transportprotokoll für die Übertragung verwendet wird:

Portnummer	**Beschreibung**
80 (Beispiel)	Die Portnummer 80 steht für das Hypertext Transfer Protocol (HTTP). HTTP wird für die Adressierung von Webserver eingesetzt, um Webinhalte abzurufen. HTTP verwendet als Transportprotokoll TCP.
443	
53	
21	
25	
23	

Adressierungskonzepte in der Netzwerktechnik

Aufgabe 8: Kreuzworträtsel



1. Name der Adressen, die Anwendungen adressieren (Mehrzahl)
2. Eine IPv4-Adresse besteht aus zwei Teilen. Wie wird der zweite Teil der IPv4-Adresse genannt?
3. Eine MAC-Adresse hat zwei Teile. Wie wird der erste Teil der MAC-Adresse bezeichnet?
4. Womit wird die Größe des Netz- und des Hostanteils einer IPv4-Adresse festgelegt?
5. Mit welchem Zeichen werden die Oktette einer IPv4-Adresse getrennt? (Mehrzahl)
6. Mit welchem Zeichen werden die 8 Bit einer MAC-Adresse getrennt? (Mehrzahl)
7. Name des Gerätes zur Tiefenmessung in der Schifffahrt
8. Gib die englische Bezeichnung für eine Echoanforderung an: Echo…
9. Gib die englische Bezeichnung für eine Echoantwort an: Echo …
10. Bezeichnung für „Verbindung“ im Netzwerktechniker-Jargon
11. Kommando, mit dem man die IPv4-Adresse des eigenen Rechners herausfindet.

Adressierungskonzepte in der Netzwerktechnik

Lösung – Aufgabe 1

Die Sicherungsschicht verwendet in Computernetzen MAC-Adressen. Diese werden auch Hardwareadressen genannt und identifizieren ein bestimmtes Interface am Gerät in einem Computernetzwerk. Eine MAC-Adresse besteht aus 48 Bit oder 6 Byte. Sie ist in zwei Teile geteilt, die Herstellerkennung und die Gerätekennung. Die Herstellerkennung wird abgekürzt als OUI (Organizationally Unique Identifier). Eine MAC-Adresse wird in hexadezimalen Zahlen, die entweder durch Bindestriche oder Doppelpunkte getrennt sind, dargestellt.

IPv4-Adressen werden in der dezentralen Kommunikation in der Netzwerkschicht eingesetzt. IPv4-Adressen werden auch als Softwareadressen bezeichnet. Sie können mit der Adresse auf einem Brief zu Ort, Straße und Hausnummer verglichen werden. Die IPv4-Adresse hat eine Länge von 32 Bit oder 4 Byte. Um IPv4-Adressen besser lesbar zu machen, wird sie in vier Teile mit jeweils 8 Bit aufgeteilt. Die Darstellung erfolgt in vier Dezimalzahlen, die jeweils durch einen Punkt getrennt werden. Der Zahlenumfang beträgt pro Byte 256 Zahlen, die einen Zahlenbereich von 0 bis 255 ergeben. Auch diese Adressen haben zwei Anteile, den Netzwerkanteil und den Hostanteil. Die Größe der Anteile wird durch die sogenannte Subnetzmaske bestimmt.

Für die Adressierung von Anwendungen werden Portnummern verwendet. Portnummern haben einen Zahlenbereich von 0 bis 65.535. Portnummern sind mit den Protokollen TCP und UDP assoziiert. Es gibt drei verschiedene Kategorien von Ports: Well Known Ports (0 – 1.023), Registered Ports (1.024 – 49.151) und Dynamically Allocated Ports (49.152 – 65.535).

Adressierungskonzepte in der Netzwerktechnik

Lösung – Aufgabe 4

Die Schüler/innen benötigen zusätzliches Papier, um die Berechnungen durchführen zu können. Die Ausarbeitung muss mit abgegeben werden.

IPv4-Adresse	Klasse	Subnetz-maske	Anzahl Host-Adressen	Netzwerk-ID	Broadcast-ID
192.168.10.1	C	255.255.255.0	254	192.168.10.0	192.168.10.255
10.20.30.255	A	255.0.0.0	16.777.214	10.0.0.0	10.255.255.255
129.120.24.25	B	255.255.0.0	65.534	129.120.0.0	129.120.255.255
204.132.10.20	C	255.255.255.0	254	204.132.10.0	204.132.10.255
84.10.100.255	A	255.0.0.0	16.777.214	84.0.0.0	84.255.255.255
172.16.25.55	B	255.255.0.0	65.534	172.16.0.0	172.16.255.255

10.20.30.255
10 mod 2 = 0
5 mod 2 = 1
2 mod 2 = 0
1 mod 2 = 1

$10_{10} = 1010_2$

8Bit: 0000 1010

Klasse A

129.120.24.25
129 mod 2 = 1
64 mod 2 = 0
32 mod 2 = 0
16 mod 2 = 0
8 mod 2 = 0
4 mod 2 = 0
2 mod 2 = 0
1 mod 2 = 1

$129_{10} = 1000\ 001$

Klasse B

204.132.10.20
204 mod 2 = 0
102 mod 2 = 0
51 mod 2 = 1
25 mod 2 = 1
12 mod 2 = 0
6 mod 2 = 0
3 mod 2 = 1
1 mod 2 = 1

$204_{10} = 1100\ 1100$

Klasse C

84.10.100.255
84 mod 2 = 0
42 mod 2 = 0
21 mod 2 = 1
10 mod 2 = 0
5 mod 2 = 1
2 mod 2 = 0
1 mod 2 = 1

$84_{10} = 1010100$

8 Bit: 0101 0100

Klasse A

172.16.25.55
172 mod 2 = 0
86 mod 2 = 0
43 mod 2 = 1
21 mod 2 = 1
10 mod 2 = 0
5 mod 2 = 1
2 mod 2 = 0
1 mod 2 = 1

$172_{10} = 1010\ 1100$

Klasse B

Adressierungskonzepte in der Netzwerktechnik

Informationen zum „Cisco Packet Tracer“ – Aufgabe 6

„Cisco Packet Tracer“ ist eine Applikation, um Netzwerke zu simulieren. „Cisco Packet Tracer“ ist zwar eine freie Software, aber man benötigt einen Account für die „Cisco Networking Academy“. Weiters muss die Schule mit der Cisco Network Academy mit einer Emailadresse assoziiert sein, um die Services der Cisco Networking Academy nutzen zu können.

Nutzungsrechte: „The Sites(s) and the Services also contain content owned by or licensed to Cisco („Cisco Content“). Cisco owns and retains all rights in the Cisco Content and the Services, including all intellectual property rights. Cisco hereby grants you a limited, revocable, nonsublicensable license to reproduce and display the Cisco Content (excluding any software code) solely for your personal use to view the Sites(s) and otherwise as necessary to use the Services. Except as set forth above, nothing contained in this Agreement shall be construed as conferring by implication, estoppel or otherwise any license or right under any trade secret, patent, trademark, copyright or other intellectual property right of Cisco or any third party. All licenses not expressly granted by Cisco are reserved.“

Der Link zur Cisco Networking Academy: https://www.netacad.com.

Um die Installationsdatei herunterzuladen, muss normalerweise eine Einführung in die Nutzung des „Cisco Packet Tracer“ absolviert werden. Die Einführung kann aber auch umgangen werden, indem man folgenden Download-Link verwendet:

https://www.packettracernetwork.com/download/download-packet-tracer.html.

Hier sind die aktuellen Versionen des „Cisco Packet Tracer“ für den Download bereitgestellt.

Nach der Installation des „Cisco Packet Tracer“ öffnet man die Applikation. Man wird aufgefordert, sich in die „Cisco Networking Academy“ einzuloggen. Wenn kein Account für die „Cisco Networking Academy“ vorhanden ist, kann man den „Cisco Packet Tracer“ auch als „Gast“ nutzen. In diesem Fall kann man aber die erstellten Topologien und Konfigurationen ab dem vierten Speichervorgang nicht mehr speichern.

Bevor man mit der Arbeit mit dem „Cisco Packet Tracer“ beginnt, sollte man eine Einführung mit den Schüler/innen absolvieren oder die Aufgabe gemeinsam mit ihnen lösen. Als Alternative bietet sich an, für die Schüler/innen Accounts zu erstellen und den Einführungskurs zu absolvieren. Dafür sind aber gute Englischkenntnisse erforderlich.

Adressierungskonzepte in der Netzwerktechnik

Lösung – Aufgabe 6

Zu 3a: Das Kommando lautet ipconfig /all.

Zu 3c: Die MAC-Adresse wird im „Cisco Packet Tracer" mit dem Format xxxx.xxxx.xxxx ausgegeben. Üblicherweise werden MAC-Adressen mit xx:xx:xx:xx:xx:xx oder xx-xx-xx-xx-xx-xx angegeben.

Zu 4b: siehe Aufgabe 5

Zu 5: Der „Ping" zwischen PC1 und PC2 ist nicht erfolgreich, weil die IPv4-Adressen nicht im selben Netz liegen.

Zu 6b Punkt 1: PDU steht für „Protocol Data Unit". PDUs dienen der Kommunikation zwischen gleichen Schichten auf entfernten Rechnern mittels gleichen Kommunikationsprotokollen. (https://www.itwissen.info/Protokoll-Dateneinheit-protocol-data-unit-PDU.html)

Zu 6b Punkt 2: Source IP: 192.168.1.1, Destination IP: 192.168.1.2, ICMP Message Type: 8 (zwei fehlen, im Gegensatz zur Aufgabe – Source MAC, Destination MAC)

Zu 6b Punkt 3: ICMP Echo Request

Zu 6b Punkt 4:

1. Der Ping-Vorgang startet den nächsten Ping-Request.
2. Der Ping-Prozess erstellt eine ICMP-Echoanforderungsnachricht und sendet sie an den unteren Prozess.
3. Die Quell-IP-Adresse ist nicht angegeben. Das Gerät stellt sie auf die IP-Adresse des Ports ein.
4. Die Ziel-IP-Adresse befindet sich im selben Subnetz. Das Gerät legt den nächsten Hop als Ziel fest.

Zu 6c Punkt 1: Source IP: 192.168.1.2, Destination IP: 192.168.1.1, ICMP Message Type: 0

Zu 6c Punkt 2: ICMP Echo Reply

Zu 6c Punkt 3:

1. Der ICMP-Prozess antwortet auf den Echo Request, indem der ICMP-Typ auf Echo Reply festgelegt wird.
2. Der ICMP-Prozess sendet ein Echo Reply.
3. Die Ziel-IP-Adresse befindet sich im selben Subnetz. Das Gerät legt den nächsten Hop als Ziel fest.
4. Pt. 4 fehlt (vgl. Aufgabe)

Zu 6c Punkt 4: Die eingehende Quell-IPv4-Adresse wird ausgehend zur Ziel-IPv4-Adresse. Die eingehende Ziel-IPv4-Adresse wird ausgehend zur Quell-IPv4-Adresse. Der ICMP-Nachrichtentyp ändert sich von Echo Request (8) auf Echo Reply (0).

Zu 6d:

1. Die Ziel-IP-Adresse des Pakets stimmt mit der IP-Adresse des Geräts oder der Broadcast-Adresse überein. Das Gerät entkapselt das Paket.
2. Das Paket ist ein ICMP-Paket. Der ICMP-Prozess verarbeitet es.
3. Der ICMP-Prozess hat eine Echo-Reply-Nachricht erhalten.
4. Der Ping-Prozess hat eine Echo-Reply-Nachricht erhalten.

Adressierungskonzepte in der Netzwerktechnik

Lösung – Aufgabe 7

Port 443:
HTTPS – Hypertext Transfer Protocol in verschlüsselter Form, TCP

Port 53:
DNS – Domain Name Service, TCP und UDP

Port 21:
FTP – File Transfer Protocol, TCP und UDP, Verbindungsaufbau und Steuerung der Übertragung von Daten

Port 25:
SMTP – Simple Mail Transfer Protocol für die Übermittlung von E-Mails, TCP

Port 23:
Telnet als unverschlüsseltes Textprotokoll zur Fernwartung von Netzwerkelementen

Adressierungskonzepte in der Netzwerktechnik

Lösung – Aufgabe 8