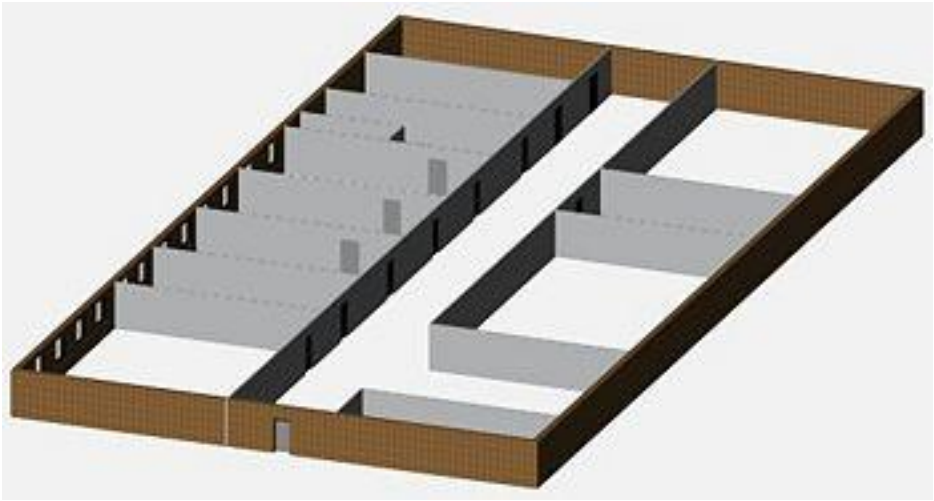
BS Info München

IT Systeme ITS10

Umzug in ein neues Firmengebäude



Aufgabe

Das Systemhaus INFOTECH systems hofft auf einen neuen Auftrag von der Werbeagentur GAB GmbH. Da die Mitarbeiterzahl der GAB GmbH stark gestiegen ist, wurde ein neues, größeres Büro angemietet.

Das Netzwerk der GAB GmbH soll mit sämtlichen PCs, Server, Druckern und Switches umgezogen werden. Zum neuen Büro gehört ein getrennter Serverraum mit einem eigenen DSL-Übergabepunkt. Die Firmenleitung der GAB GmbH wünscht die vollständige Inbetriebnahme der neuen Netzwerkstruktur.

Inhalt

Ausgangslage und Sollzustand

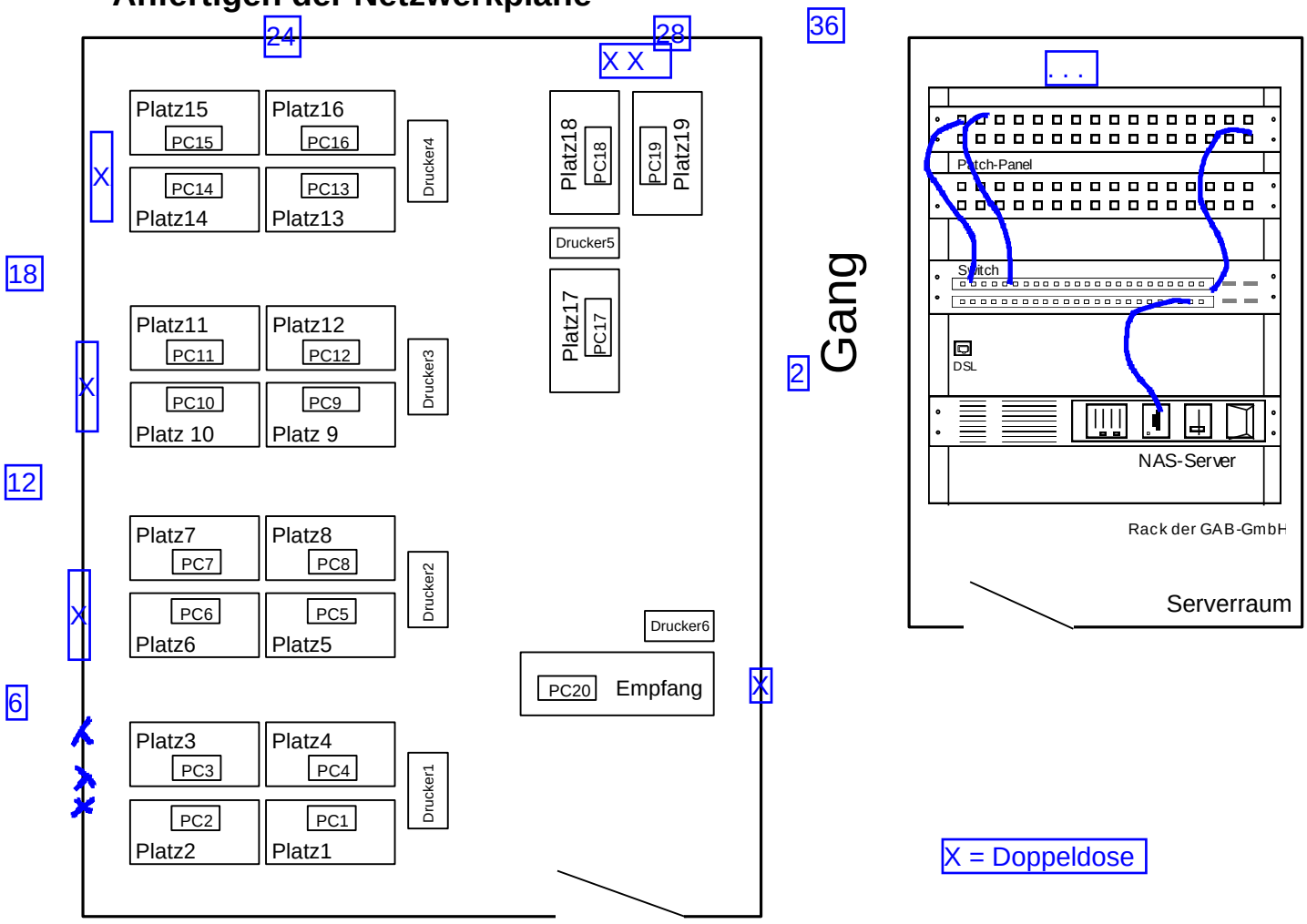
Das Netzwerk der GAB GmbH wurde bereits vor einiger Zeit durch die INFOTECH systems erneuert und verfügt nun über eine zeitgemäße Bandbreite von 1 GBit/s.
Aufgrund der guten Auftragslage ist die Mitarbeiterzahl der GAB GmbH stark gestiegen. Die Firmenleitung hat deshalb in einem anderen Bürogebäude ein neues Büro angemietet und wünscht die vollständige Inbetriebnahme des neuen Netzwerks.

Im neuen Büro der GAB GmbH sollen 20 PCs und 6 Drucker aufgebaut werden. In einem Serverraum, der von mehreren Firmen benutzt wird, ist für die GAB GmbH ein eigenes 19"-Rack vorgesehen. Darin befinden sich der NAS-Server und der DSL-Übergabepunkt.

Arbeitsschritte

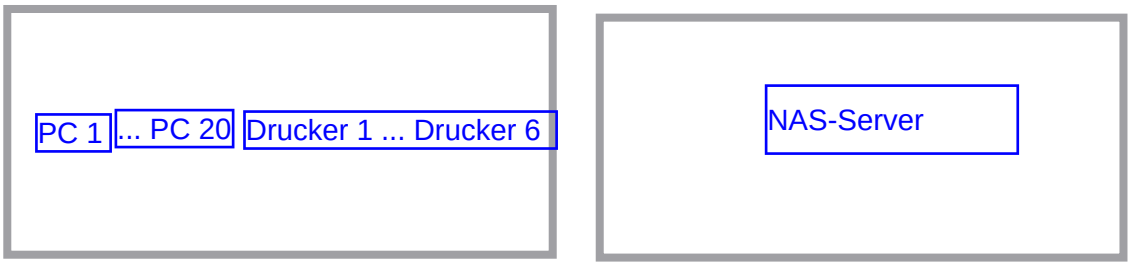
- Netzwerkpläne anfertigen (S.3)
- DSL-Router konfigurieren, einbauen und testen (S.4)
- Schichtenmodelle kennenlernen, Protokolle und Geräte einordnen (S.5)
- Netzwerkverkehr mit Wireshark analysieren (S.6)

Anfertigen der Netzwerkpläne



- Ergänzen Sie den Kabelverlauf im **physikalischen Netzplan** (oben). **A**
  Die Netzwerk-Leitungen sind, bevorzugt an den Außenwänden, in Brüstungs-wandkanälen zu verlegen, die Patchkabel werden zwischen den Tischen geführt. Markieren Sie auch die Netzwerkdosen in den Wandkanälen!

- Skizzieren Sie nachfolgend den **logischen Netzwerkplan**. **A**
  Hinweis: Informationen zu Netzwerkplänen finden Sie auf S.13 im Anhang!



Einbinden eines DSL-Routers

Ihre Aufgabe ist es, einen DSL-Router für die Internetanbindung zu konfigurieren.

Eigenschaften des DSL-Routers

A

Laden Sie die Installationsanleitung oder das Routerhandbuch des zur Verfügung gestellten DSL-Routers aus dem Internet. Informieren Sie sich, welche Eigenschaften, Funktionen und Konfigurationsmöglichkeiten der Router bietet und geben Sie die wichtigsten nachfolgend an. Ergänzen Sie die vorbereitete Tabelle!

Eigenschaften und Funktionen des DSL-Routers: _____ (Modell angeben!)

- z.B. *VoIP-Telefonanlage* -

-

-

-

-

Konfiguration des DSL-Routers

A

Beantworten Sie mit der Installationsanleitung oder dem Routerhandbuch folgende Fragen zur Router-Konfiguration!

Wie wird der DSL-Router auf die Werkseinstellungen zurückgesetzt?	Über Reset Button
Wie lauten nach dem Zurücksetzen Anmeldename und Router-Passwort?	Anmeldename: admin Passwort: funkwerk
Welche IP-Einstellungen verwendet der Router nach dem Zurücksetzen?	IP-Adresse: 192.168.0.254 Subnet-Maske: 255.255.255.0
Wie werden die am Router vorgenommenen Einstellungen dauerhaft gespeichert?	ÜbernehmenKonfiguratione
Wie müssen die Netzwerkeinstellungen des PC konfiguriert werden, damit im Browser der Zugriff auf das Web-interface des Routers möglich ist?	IP-Adresse im IP-Bereich

Praxistest **P**

- Führen Sie zunächst am Arbeitsplatz über eine direkte 1:1 Netzwerkverbindung (PC - Router) die Grundkonfiguration des DSL-Routers durch. Gehen Sie so vor, wie in der Installationsanleitung oder im Routerhandbuch beschrieben.
- Die IP-Adressen für die Arbeitsplätze sollen vom DSL-Router über das DHCP-Verfahren vergeben werden. Passen Sie den internen DHCP-Server des Routers so an, dass der IP-Bereich 192.168.0.20 - 192.168.0.50 verteilt wird.
- Falls das WLAN aktiv ist, deaktivieren Sie es.
- Stellen Sie Ihren PC auf DHCP ein und testen Sie, ob Ihr PC eine IP-Adresse vom Router zugeteilt bekommt.
  (evtl. zuerst **ipconfig /release** und dann **ipconfig /renew** eingeben).
- Speichern Sie die Router-Konfiguration.
- Bauen Sie nun den DSL-Router in das für Ihren Arbeitsplatz vorgesehene Rack im Serverraum ein und testen Sie die Verbindung.
- Ergänzen Sie den Router mit den wichtigsten Konfigurationsangaben in ihrem physikalischen und logischen Netzplan auf Seite 3.

Schichtenmodelle

Schichtenmodelle (OSI, DoD) werden in der Netzwerktechnik zur Veranschaulichung herangezogen. Dabei werden einzelne Aufgaben oder Funktionen des Systems einer Schicht (engl. *tier* oder *layer*) zugeordnet. Die Lehrkraft wird Ihnen dies in einem Vortrag erläutern!

OSI-Schicht		Aufgabe	zum Vergleich: DoD-Schicht	Protokoll-Beispiel	Netzwerk-komponente (nur höchste Schicht)
7	**Anwendung** *Application*	verschafft den Anwendungen Zugriff auf das Netzwerk	**Anwendung**	FTPHTT	Proxy
6	**Darstellung** *Presentation*	setzt die systemabhängige Darstellung der Daten (z.B. ASCII) in eine unabhängige Form um und ermöglicht somit den korrekten Datenaustausch zwischen unterschiedlichen Systemen			
5	**Sitzung** *Session*	Zugangskontrolle, baut Sitzungen zwischen Anwendungen auf, verwaltet und beendet sie			
4	**Transport** *Transport*	Organisation der Auslieferung der Datenpakete, Segmentierung von Datenpaketen, Sicherung des Transportes, Flusskontrolle	**Transport**	TCP	Paket-Filter
3	**Vermittlung** *Network*	Wegefindung in Netzen, Aufbau und Aktualisierung von Routingtabellen, Fragmentierung von Datenpaketen	**Internet**	ICMPIP	RouterLayer-3-
2	**Sicherung** *Data Link*	Zugriff auf das Übertragungsmedium regeln, möglichst fehlerfreie Übertragung gewährleisten, Definition von Daten-Frames	**Netzzugang**	Ethernet	Switch
1	**Bitübertragung** *Physical*	übertragungstechnische Verfahren, Definition der Daten-Bits, Kabel, Anschlüsse, Spannungen			Repeater

Tragen Sie die angegebenen Protokolle in die Spalte *Protokollbeispiel* ein: **A**
ARP, Ethernet, FTP, HTTP, ICMP, IP, SMTP, SSH, TCP, UDP

Tragen Sie die angegebenen Geräte in die Spalte *Netzwerkkomponente* ein:
Hub, Layer-3-Switch, Paket-Filter-Firewall, Proxy, Router, Switch

Netzwerkanalyse mit Wireshark

P

Um einige wichtige Netzwerkprotokolle näher kennen zu lernen, sollen Sie sich mit dem Netzwerkanalyse-Tool Wireshark vertraut machen. Sie werden den Austausch von Datenpaketen im Netzwerk beobachten und Fragen dazu beantworten.

Ihre Aufgabe besteht jetzt darin, mit Wireshark die bei der Ausführung des Ping-Befehls verwendeten Protokolle zu ermitteln und zu analysieren.

Vorbereitung

- Notieren Sie die IP-Adresse des von Ihnen benutzten Routers: 10.96.205.1
- Falls Sie vom DHCP-Server des Routers eine IP-Adresse bekommen haben: geben Sie die an Ihren PC vergebene IP-Adresse an: 10.96.205.73
- Öffnen Sie (z.B. bei uns über die Schnellstartleiste) eine Eingabeaufforderung und geben Sie den Ping-Befehl folgendermaßen ein: **`ping -t Zielrechner`**

`ping`	Aufruf des Programmes ping
`-t`	Option `-t` bedeutet Dauerping
`Zielrechner`	das Ziel des Pings, angegeben als IP-Adresse oder Hostname

  Beispiel:

  Eingabeaufforderung

  ```
  C:\>ping -t 192.168.10.245

  Ping wird ausgeführt für 192.168.10.245 mit 32 Bytes Daten:

  Antwort von 192.168.10.245: Bytes=32 Zeit<1ms TTL=128
  Antwort von 192.168.10.245: Bytes=32 Zeit<1ms TTL=128
  Antwort von 192.168.10.245: Bytes=32 Zeit<1ms TTL=128
  ```

  Hinweis: Ein Dauerping wird mit der Tastenkombination **`Strg-C`** abgebrochen!

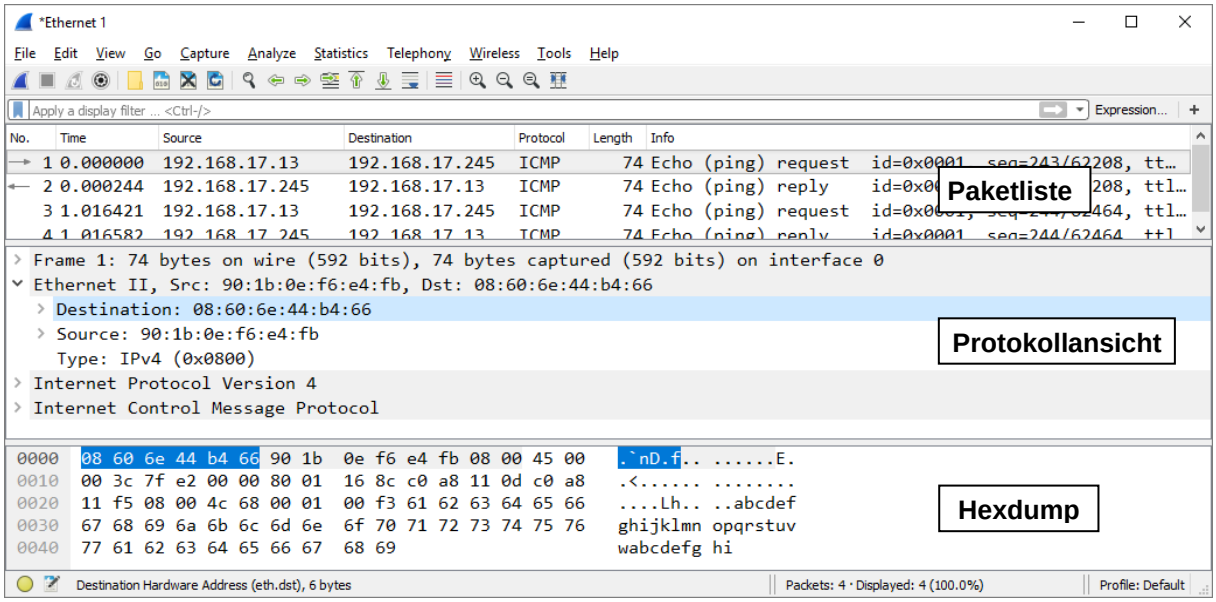
Aufzeichnen des Netzwerkverkehrs

- Senden Sie einen Dauerping an den Router.
- Öffnen Sie über das Startmenü den Netzwerk-Sniffer Wireshark und starten Sie das Mitschneiden (*capture*) der Netzwerkdaten. Dazu können Sie links im Begrüßungsbildschirm die Netzwerkkarte auswählen und auf das darüberliegende Feld "Start" klicken.

  Hinweise:
  - Möglicherweise müssen Sie das Mitschneiden zunächst einmal über das Menü unter *Capture* --> *Interfaces* bei der Intel-Netzwerkkarte starten.
  - Alle weiteren Mitschnitte starten Sie dann über den Flossen-Button in der Menüleiste.

- Stoppen Sie nach ca. 10 Sekunden die Aufzeichnung mit dem roten Stop-Button.

☐ Lassen Sie sich jetzt die aufgezeichneten Pakete anzeigen.
Sie sehen jetzt in etwa folgende Darstellung:



Paketliste In diesem Fenster sind alle Pakete (Frames) aufgelistet, welche die Netzwerkkarte gelesen oder gesendet hat

Protokollansicht Auflistung der beteiligten Protokolle des oben markierten Pakets (Frames) und es können weitere Details ausgelesen werden

Hexdump Alle Daten des Frames werden als Bytes hexadezimal dargestellt. Der Hex-Dump kann mit Rechtsklick in den leeren Bereich rechts (..*Show as bits*..) auch binär angezeigt werden

Analyse der Protokollstruktur

Betrachten Sie die Daten im Ethernet-Protokoll (Wireshark Protokollansicht) genauer!

```
- Ethernet II, Src:c0:25:06:a5:6e:18 (c0:25:06:a5:6e:18), Dst:00:19:99:d2:92:65
  + Destination: 00:19:99:d2:92:65 (00:19:99:d2:92:65)
  + Source:      c0:25:06:a5:6e:18 (c0:25:06:a5:6e:18)
    Type: IPv4 (0x0800)
```

☐ Um welche Information handelt es sich bei dem Eintrag *Destination* ?

Ziel MAC-Adresse

☐ Um welche Information handelt es sich bei dem Eintrag *Source* ?

MAC-Adresse des Senders

- Lassen Sie sich die Informationen zur Netzwerkkarte Ihres PCs mit dem Befehl **ipconfig /all** anzeigen.
  Geben Sie die MAC-Adresse Ihres PCs an: 00:2c:c8:24:cb:40

Eingabeaufforderung

```
C:\>ipconfig /all

Windows-IP-Configuration
  Host Name . . . . . . . . . . . . : PC-D2353
  Primärer DNS Suffix . . . . . . . :
  Knotentyp . . . . . . . . . . . . : Hybrid
  IP-Routing aktiviert. . . . . . . : No
  WINS-Proxy aktiviert. . . . . . . : No

Ethernet-Adapter Ethernet0:

  Verbindungsspezifisches DNS-Suffix: mschool-ad.muenchen.musin.de
  Beschreibung. . . . . . . . . . . : Intel(R) Ethernet I219-V
  Physische Adresse . . . . . . . . : 90-1B-0E-A3-28-6A
  DHCP aktiviert. . . . . . . . . . : Ja
  Autokonfiguration aktiviert . . . : Ja
  Verbindungslokale IPv6-Adresse  . : e80::6825:ef3c:57bf:488c%5(Bevorzugt)
  IPv4-Adresse  . . . . . . . . . . : 10.96.207.63(Bevorzugt)
  Subnetzmaske  . . . . . . . . . . : 255.255.255.0
  Lease erhalten. . . . . . . . . . : Montag, 5. Oktober 2020 09:36:58
  Lease läuft ab. . . . . . . . . . : Montag, 5. Oktober 2020 21:36:59
  Standardgateway . . . . . . . . . : 10.96.207.1
  DHCP-Server . . . . . . . . . . . : 10.86.200.62
```

- Prüfen Sie, ob die MAC-Adresse Ihres PCs mit derjenigen übereinstimmt, die Wireshark angezeigt hat. Ist die gleiche

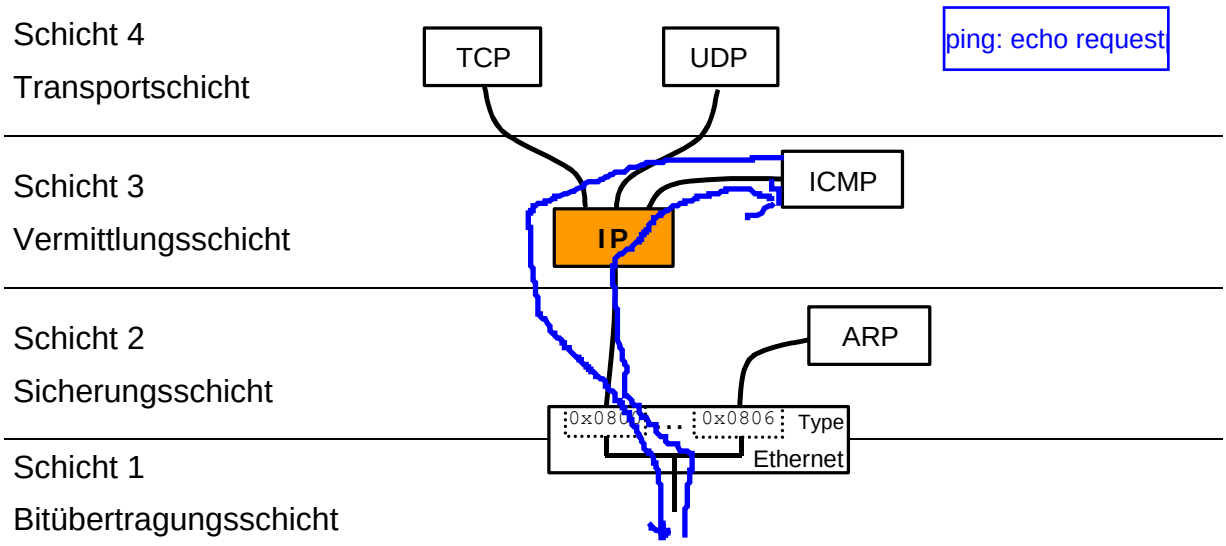
- Welchen Zweck erfüllt die Angabe **`Type: IPv4 (0x0800)`** im Ethernet-Protokoll (Schicht 2)?

  Legt fest das IPv4 und nicht IPv6 Verwendet wird

Zusammenfassung OSI-Modell

A

Fassen Sie jetzt alle gewonnenen Informationen in der unten angeführten Tabelle zusammen:
- Verbinden Sie die im Ping-Versuch verwendeten Protokolle
- notieren Sie neben den Protokollen die gesendeten Informationen der jeweiligen Schicht
- welche Bedeutung hat die Transportschicht (Schicht 4) in diesem Versuch?



A

Erläutern Sie folgende Begriffe mit Hilfe des Anhangs auf S.14:

Layer

Stack

Header

Trailer

Nutzdaten

Die folgenden Begriffe benennen Datenstrukturen. Ordnen Sie den Begriffen die Nummern der einzelnen Schichten zu: Bit ____, Frame ____, Paket ____, Segment ____

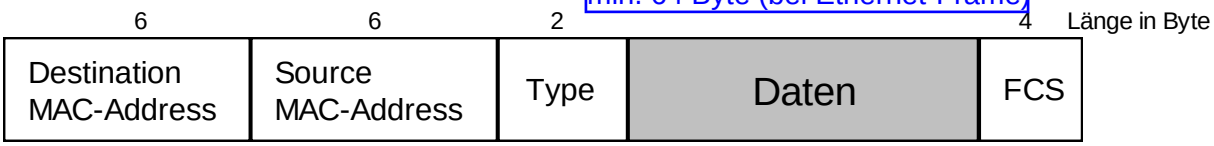
Ping normal 32 Byte wird daher aufgeblasen14

Einen Hexdump auswerten

A

a) Nachfolgend ist der schematische Aufbau eines Ethernet-Frames gezeigt:

min. 64 Byte (bei Ethernet-Frame)



Suchen und markieren Sie im nachfolgend angegebenen Hexdump die Felder *Destination MAC-Address*, *Source MAC-Address* und *Type*.

Hilfe: Klicken Sie in Wireshark auf die jeweiligen Felder.

Layer 3 Protokollfeld -> ICMP

IP-Header

```
0000  00 50 56 f8 6b 7b 00 0c  29 5a 0a ce 08 00 45 00
0010  00 3c 00 4e 00 00 80 01  5a 4e c0 a8 2f d2 c0 a8
0020  2f 02 08 00 31 5c 02 00  1a 00 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67  68 69
```

ICMP Typ 8 echo request ping

b) Übernehmen Sie die Daten aus dem oben dargestellten Hexdump und tragen Sie diese neben die entsprechenden Begriffe ein.

Destination MAC-Adresse 00:50:56:f8:6b:7b

Source MAC-Adresse 00:0c:29:5a:0a:ce

Type IPv4

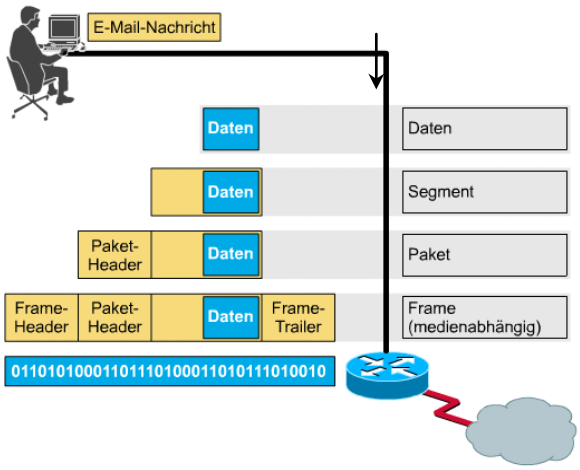
Welcher Schicht bzw. welchen Schichten sind diese Begriffe zuzuordnen? 2. Schicht (Data Link Layer)

c) Die sog. *Frame Check Sequence* (FCS) wird von der Schicht 2 an die Daten angehängt. Leider wird sie von Wireshark nicht angezeigt. Wozu dient die FCS?
Informieren Sie sich unter https://de.wikipedia.org/wiki/Ethernet darüber.

Zur Sicherstellung der Korrektheit und Vollständigkeit der einzelnen Frames (32-Bit-CRC-Prüfsumme)

d) Erklären Sie den Begriff der "Datenkapselung" in der Netzwerktechnik.
Verwenden Sie dabei die folgende Skizze!

Beispiel für Datenkapselung



Das heißt, dass mit jeder schicht eine neuer Header (K

ARP ermittelt die MAC-Adresse des Ziels

Um ein Ethernet-Frame senden zu können, benötigt der Absender die Ziel-MAC-Adresse (*Destination*). Diese ist ihm jedoch zunächst nicht immer bekannt.
Das ARP-Protokoll löst dieses Problem und liefert die MAC-Adresse zu einer bestimmten IP-Adresse. Der Rechner merkt sich die Zuordnung von IP zu MAC von den Geräten mit denen er bereits kommuniziert hat für eine bestimmte Zeit. Diese Zuordnung wird im **ARP-Cache** (auch: *ARP-Table*) gespeichert.

ARP-Cache anzeigen lassen

P

- ☐ Pingen sie mehrere Arbeitsplatzrechner im Klassenzimmer an.
- ☐ Lassen sie sich den ARP-Cache mit folgendem Befehl anzeigen: **`arp -a`**

Eingabeaufforderung

```
C:\>arp -a
Schnittstelle: 10.96.207.46 --- 0xa
  Internetadresse       Physische Adresse     Typ
  10.96.207.1           00-00-0c-07-ac-15     dynamisch
  10.96.207.37          00-26-73-f0-cc-2d     dynamisch
  10.96.207.40          00-26-73-f1-52-18     dynamisch
```

- ☐ Die IP-MAC-Zuordnung aller angepingten Arbeitsplatzrechner sollte aufgelistet sein.
- ☐ Löschen sie nun den ARP-Cache mit dem Befehl: **`arp -d`**

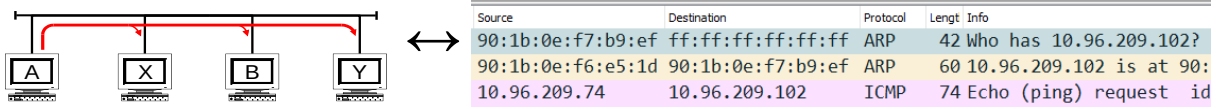
  Hinweis: Zum Löschen des ARP-Caches müssen Sie die Eingabeaufforderung als Administrator starten!
- ☐ Lassen sie sich den ARP-Cache noch einmal anzeigen, die Einträge sollten weg sein.
- ☐ Starten Sie nun wieder das Sniffern im Wireshark.
- ☐ Führen Sie erneut Pings an verschiedene Arbeitsplatzrechner durch.
- ☐ Stoppen Sie das Sniffern.
- ☐ Suchen Sie nach den ARP Paketen und analysieren Sie diese.
- ☐ Was fällt Ihnen bezüglich der MAC-Adressen auf?

- ☐ Lassen Sie sich den ARP-Cache erneut anzeigen. Sind die Einträge wieder vorhanden?

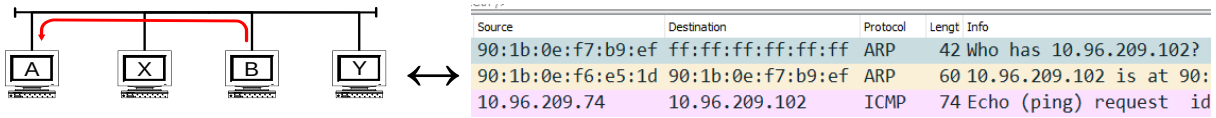
Zusammenhänge bei ARP erkennen

Erläutern Sie kurz den Zusammenhang zwischen dem Infobild und Wireshark-Ausschnitt.
Benutzen Sie dazu auch diese Begriffe: *ARP-Anfrage, ARP-Antwort, Broadcast, Unicast*

1. Schritt



2. Schritt



Für die Schnellen: HTTP-Sniffing

nice 2 know

Die Protokolle ermitteln, die bei der Abfrage eines Webservers verwendet werden!

- schneiden Sie den Netzwerkverkehr im Netzwerk-Sniffer Wireshark mit
- geben Sie im Browser die IP-Adresse eines Gerätes/Servers ein, das einen Web-Server laufen hat (z.B. DSL-Router, NAS oder unser Intranet auf 192.168.1.242)
- beenden Sie die Aufzeichnung
- analysieren Sie den Datenverkehr mit einen Rechtsklick auf eines der zugehörenden Daten-Pakete und wählen Sie im dessen Kontextmenü *Follow TCP-Stream* aus
- wählen Sie eines der zugehörenden Daten-Pakete aus und ergänzen Sie die Tabelle:

OSI-Schicht	DoD-Schicht	Protokoll
5 - 7	Anwendung	
4	Transport	
3	Internet	
1 - 2	Netzzugang	

Protokolle, die bei der Abfrage eines Webservers verwendet werden

- ***Profis*** würden folgende Tools benutzen, um einen Webserver zu testen (z.B. 192.168.1.242)

```
nping --tcp -p 80 192.168.1.242
cryping -http 192.168.1.242
wget --spider -S 192.168.1.242
curl 192.168.1.242
```

- ***Hacker*** benutzen **`netcat`** oder **`ncat`** aus den nmap-Programmen

  unter Windows: `(echo GET / & echo. & echo. ) | ncat 192.168.1.242 80`
  unter Linux: `echo -e "GET / \n\n" | netcat 192.168.1.242 80`

  Hinweis: Wenn Sie keinen Webserver zur Hand haben, geht das mit dem Tool **sfk** (*Swiss File Knife*). Bitten Sie Ihren **Nachbarplatz**, folgendes einzugeben: **`sfk httpserv`**
  Geben Sie dann die IP-Adresse des Nachbarplatzes in Ihrem Internet-Browser ein.
  Hinweise: Wenn die Firewall aktiv ist, funktioniert möglicherweise von außen der Zugriff auf den HTTP-Server nicht.
  Dann müssen Sie (als Administrator) auf dem Server die Firewall abschalten: **`netsh advfirewall set allprofiles state off`**
  oder Sie machen es so, wie es in www.itslot.de/2018/03/windows-firewall-regel-cmd-erstellen.html beschrieben ist.

  Alle angegebenen Tools sind auf den Laborrechnern bereits installiert!

  Probieren Sie alles aus und sniffern Sie dabei mit!

Für die ganz Schnellen: ARP kreativ einsetzen

nice 2 know

Wie könnten Sie die MAC-Adressen aller an einem Switch angeschlossen PCs und Drucker ermitteln?

Versuchen Sie es mal...

Anhang

Physikalischer und logischer Netzwerkplan

Physikalischer Plan

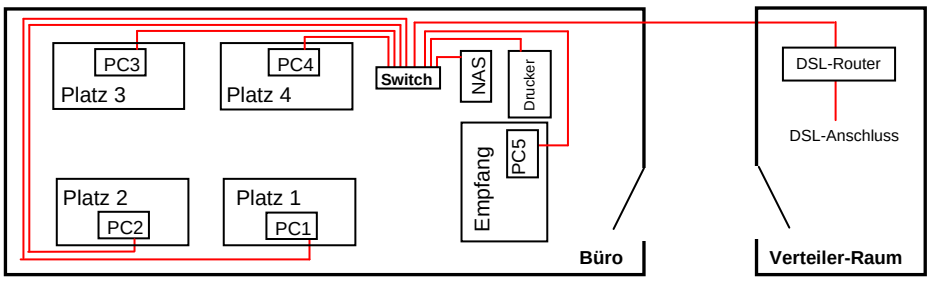
Ein physikalischer Netzwerkplan zeigt genau, wie die aktiven und passiven Komponenten verschaltet sind. Beispielsweise werden die Räumlichkeiten und der genaue Kabelverlauf dargestellt, Übertragungsgeschwindigkeit und Kabeltyp angegeben, die Bezeichnung der Netzwerkdosen gezeigt und Modell bzw. Hersteller der aktiven Komponenten genannt. Ein physikalischer Netzwerkplan eignet sich gut zur Fehlersuche auf Schicht 1.

Logischer Plan

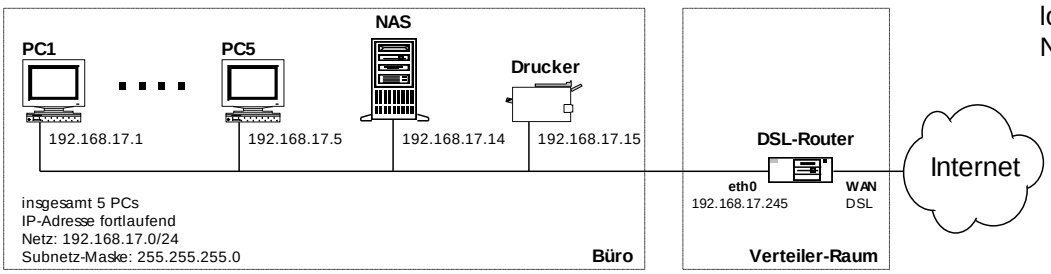
Beim logischen Netzwerkplan handelt es sich um eine vereinfachte Darstellung der Netzwerk-Topologie, ohne exakte Angaben der Kabelinstallationsstrecken.
Logische Pläne zeigen die Wege, wie die Daten im Netzwerk übertragen werden.
Dazu werden die einzelnen Funktionsbereiche dargestellt, die entstehen, wenn das physikalische Netzwerk über aktive Komponenten unterteilt wird, wie dies z.B. beim Routing oder bei der Bildung von VLANs der Fall ist. Wichtige aktive Komponenten sind im logischen Plan enthalten, z.B. PCs, Server, Router, Firewall.
Wichtig ist, dass alle Komponenten einen Namen haben und die IP-Adressen bzw. IP-Netze eingetragen sind. Bei Geräten mit mehreren Netzwerk-Interfaces (z.B. Router) sollten die Interface-Bezeichnungen mit angegeben werden (z.B. eth0, WAN, ...).

In der Praxis wird meist ein logischer Netzwerkplan gezeichnet, der aber auch noch die für das Verständnis wichtigen Kabelwege, Raum- und Dosennummern usw. enthalten kann.
Sehr oft kommen Visio-Zeichnungen zum Einsatz, da die Hersteller aktiver Netzwerkkomponenten häufig für ihre Geräte Bildbibliotheken (Stencil, Shapes) zur Verfügung stellen.

Beispiel:



physikalischer Netzwerkplan



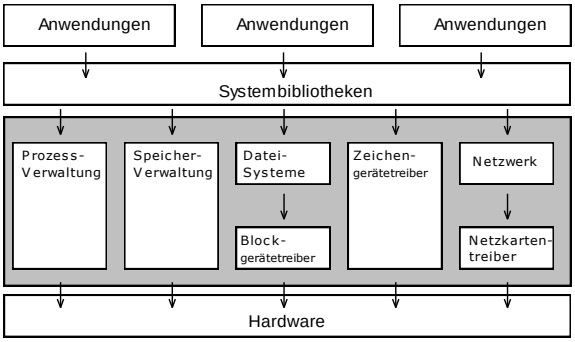
logischer Netzwerkplan

Was ist ein Schichtenmodell?

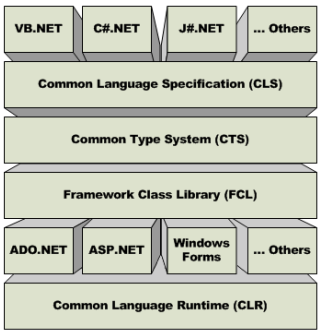
Schichtenmodelle werden häufig zur strukturierten Darstellung von Systemen verwendet. Dabei werden einzelne Aufgaben oder Funktionen des Systems einer Schicht (engl. *tier* oder *layer*) zugeordnet.

Durch eine Einteilung in Schichten kann ein System besser überblickt und die einzelnen Funktionen einfacher verstanden werden. Es können auch Fehler schneller eingekreist werden, somit wird die Wartung erleichtert.

Schichtenmodelle werden u.a. in der Netzwerktechnik (z.B. OSI, DoD), Softwaretechnik (z.B. .NET, Java, CORBA) und bei Betriebssystemen (z.B. beim Linux-Kernel) zur Veranschaulichung eingesetzt. Da die Schichten meist übereinander gestapelt dargestellt werden, bezeichnet man sie oft als Protokoll-Stapel oder Protokoll-*Stack*.



Betriebssystem: Linux-Kernel (grau)



Softwaretechnik: .NET

OSI-Schichtenmodell

Das OSI-Schichtenmodell (*Open Systems Interconnection Reference Model*) wurde als Designgrundlage für offene Kommunikationsprotokolle entwickelt und 1983 von der Internationalen Normungsorganisation ISO (*International Organization for Standardization* - www.iso.org) standardisiert.

Dazu wurden die Aufgaben der Kommunikation in Netzwerken in sieben aufeinander aufbauende Schichten (*layer*) unterteilt. Für jede Schicht existiert eine Beschreibung, in der steht, was diese zu leisten hat. Diese Anforderungen werden mit diversen Kommunikationsprotokollen realisiert.

OSI-Schicht		Aufgabe	zum Vergleich: DoD-Schicht	Protokoll-Beispiel	Netzwerk-komponente
7	**Anwendung** *Application*	verschafft den Anwendungen Zugriff auf das Netzwerk	**Anwendung**	*FTP HTTP SMTP SSH*	*Proxy*
6	**Darstellung** *Presentation*	setzt die systemabhängige Darstellung der Daten (z.B. ASCII) in eine unabhängige Form um und ermöglicht somit den korrekten Datenaustausch zwischen unterschiedlichen Systemen			
5	**Sitzung** *Session*	Zugangskontrolle, baut Sitzungen zwischen Anwendungen auf, verwaltet und beendet sie			
4	**Transport** *Transport*	Organisation der Auslieferung der Datenpakete, Segmentierung von Datenpaketen, Sicherung des Transportes, Flusskontrolle	**Transport**	*TCP UDP*	*Paketfilter-Firewall*
3	**Vermittlung** *Network*	Wegefindung in Netzen, Aufbau und Aktualisierung von Routingtabellen, Fragmentierung von Datenpaketen	**Internet**	*ICMP IP*	*Router Layer-3-Switch*
2	**Sicherung** *Data Link*	Zugriff auf das Übertragungsmedium regeln, möglichst fehlerfreie Übertragung gewährleisten, Definition von Daten-Frames	**Netzzugang**	*ARP Ethernet*	*Switch*
1	**Bitübertragung** *Physical*	übertragungstechnische Verfahren, Definition der Daten-Bits, Kabel, Anschlüsse, Spannungen			*Hub Repeater*

Übrigens: Was hat der Satz *"Please do not throw salami pizza away!"* mit dem OSI-Modell zu tun?

Protokolle

sind eine exakte Vereinbarung (ein Satz von Regeln und Formaten) darüber, wie Daten in Netzwerken ausgetauscht werden. Dieser Datenaustausch erfordert häufig ein Zusammenspiel von mehreren Protokollen, die unterschiedliche Aufgaben übernehmen (z.B. TCP/IP-Protokollfamilie). Um die damit verbundene Komplexität beherrschen zu können, werden die einzelnen Protokolle in Schichten organisiert.

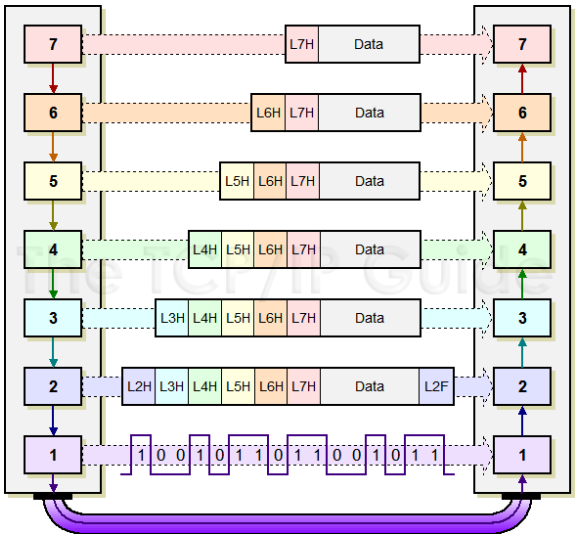
Der in einem Protokoll beschriebene Aufbau eines Datenpakets enthält für den Datenaustausch wichtige Informationen über das Paket, wie beispielsweise Absender und Empfänger, den Typ des Pakets (z.B. Verbindungsaufbau, Verbindungsabbau oder reine Nutzdaten), die Paketlänge und meist eine Prüfsumme.

Datenkapselung

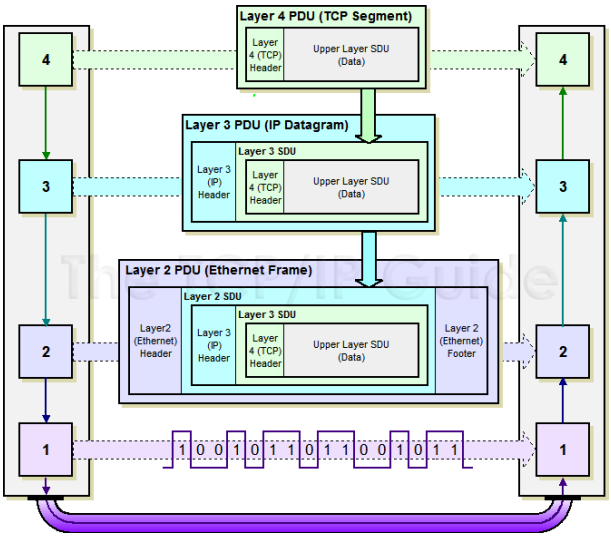
Beim Schichtendurchgang der Daten von oben nach unten fügt jede Schicht an dem ihr übergebenen Nutzdatenpaket (*payload*) ihre Protokollinformationen an. Befinden sich diese am Paketanfang werden sie als ***Header*** (Protokollkopf) bezeichnet, befinden Sie sich am Paketende, nennt man Sie ***Trailer*** (Protokollnachspann). Manchmal werden Trailer auch (als Wortspiel zu *header*) mit *footer* bezeichnet. Das nun aus Header und Payload bestehende Datenpaket wird von der darunterliegenden quasi als "Nutzdaten" betrachtet, sie fügt dann ihrerseits daran wieder ihre eigenen Protokollinformationen an.

Das Anfügen von Protokollinformationen an die Nutzdaten beim Schichtendurchgang von oben nach unten wird ***Einkapselung*** (*encapsulation*) genannt.

Auf der untersten Schicht wird das Nutzdatenpaket inklusive aller Protokollinformationen in technisch übertragbare Signale umgewandelt und über das physikalisch vorhandene Übertragungsmedium (z.B. LWL) zum Zielsystem transportiert.
Auf der Empfängerseite durchläuft das Datenpaket dann den umgekehrten Vorgang, d.h. jede Schicht auf der Empfängerseite wertet den von der entsprechenden Schicht auf der Senderseite hinzugefügten Header aus und entfernt ihn, bevor sie die Daten an die nächsthöhere Schicht weitergibt (Entkapselung, *de-encapsulation*).



Einkapselung im OSI-Modell
L7H: *Layer7-Header*
L2F: *Layer2-Footer* (L2-Trailer)



Einkapselung im DoD-Modell
SDU (*service data unit*): Nutzdaten der darüberliegenden Schicht
PDU (*protocol data unit*) = Header + SDU (+ evtl. Trailer)

Fragen

- die folgenden Fragen stammen aus dem Fragenpool. Sie zeigen den Umfang und die Intensität der Unterrichtsinhalte und dienen zur Vorbereitung auf Leistungskontrollen und Abschlussprüfung
- *manchmal* haben schwierige Fragen ein Sternchen "*", schwierigere zwei "**"
- es werden KEINE Lösungen bereitgestellt, Ziel ist es, dass SIE die Lösungen selbst erstellen!
- Nachfragen, Anmerkungen, Lob und Kritik können Sie an Ihre Lehrkraft richten

1.) Nennen Sie einige Unterschiede zwischen physikalischen und logischen Netzwerkplänen.

2.) Wozu wird DHCP eingesetzt?

3.) Wozu dient die Frame Check Sequence (FCS)?

4.) Wieviele Bit bzw. Byte hat eine MAC-Adresse?

5.) Durch Schichtenmodelle ergeben sich Vorteile bei der Systemadministration. Welche?

6.) Was ist ein Protokoll-*Stack*?

7.) Welchen Zweck erfüllt auf dem Layer 2 die Angabe *Type IP (0x0800)* ?

*Was würde die Angabe "0x0806" im Feld "Type" bedeuten?

8.) Kennzeichen Sie im Hexdump die Felder *MAC-Adresse Destination, MAC-Adresse Source, Type*.

```
0000  00 50 56 f8 6b 7b 00 0c  29 5a 0a ce 08 00 45 00
0010  00 3c 00 4e 00 00 80 01  5a 4e c0 a8 2f d2 c0 a8
0020  2f 02 08 00 31 5c 02 00  1a 00 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67  68 69
```

9.) Erklären Sie den netzwerktechnischen Begriff der "Datenkapselung".

10.) Was ist ein Protokoll?

11.) Was ist der wesentliche Unterschied zwischen Protokoll-Header und Protokoll-Trailer?

12.) Geben Sie einige Verwaltungs-Informationen an, die sich in einem Protokoll-Header befinden.

13.) Welche Protokolle kommen beim Ping-Befehl zum Einsatz?

Zu welchen Schichten gehören diese Protokolle jeweils?

14.) Was hat der Satz "Please do not throw salami pizza away!" mit dem OSI-Modell zu tun?

15.) Welche beiden Schichten haben DoD- und OSI-Schichtenmodell gemeinsam?

16.) Geben Sie für die OSI-Schichten 2, 3, 4 jeweils ein Protokoll an, das darauf arbeitet.

17.) Geben Sie für die OSI-Schichten 1, 1-2, 1-3 jeweils eine aktive Netzwerkkomponente an, die darauf arbeitet.

18.) Nennen Sie die deutschen oder englischen Bezeichnungen der OSI-Schichten und geben Sie für jede Schicht jeweils ein Protokollbeispiel oder eine aktive Netzwerkkomponente an.

19.) Wie ermittelt ein Rechner zu einer gegebenen IP-Adresse die dazugehörende MAC-Adresse?

20.) Wozu wird der ARP-Cache benötigt?

21.) Was machen folgende Befehle: *ipconfig, ipconfig /all, arp -a, arp -d, ping -t 127.0.0.1*