***Übungsblatt 1 Lösungen***

**✅ 1.1 Was ist ein Sniffer und wozu wird er eingesetzt?**

Ein **Sniffer** ist ein Programm oder Gerät, das **Netzwerkpakete mitschneidet und analysiert**.  
Es wird eingesetzt für:

* Netzwerkdiagnose und Fehleranalyse
* Sicherheitsüberwachung (z. B. verdächtiger Datenverkehr)
* Performance-Analyse
* Protokoll-Inspektion

Beispiel: **Wireshark**

### ✅ ****1.2 Was ist ein Mirror Port (Port Mirroring)?****

Ein **Mirror Port** ist ein spezieller Port auf einem Switch, an den **Kopien des Datenverkehrs anderer Ports** weitergeleitet werden.  
Ziel: Der gesamte Traffic eines Ports (oder mehrerer) kann dort von einem Sniffer überwacht werden, **ohne den normalen Verkehr zu beeinflussen**.

### ✅ ****1.3 Datenrate-Berechnung****

#### **Ein Port mit 100 Mbit/s duplex**:

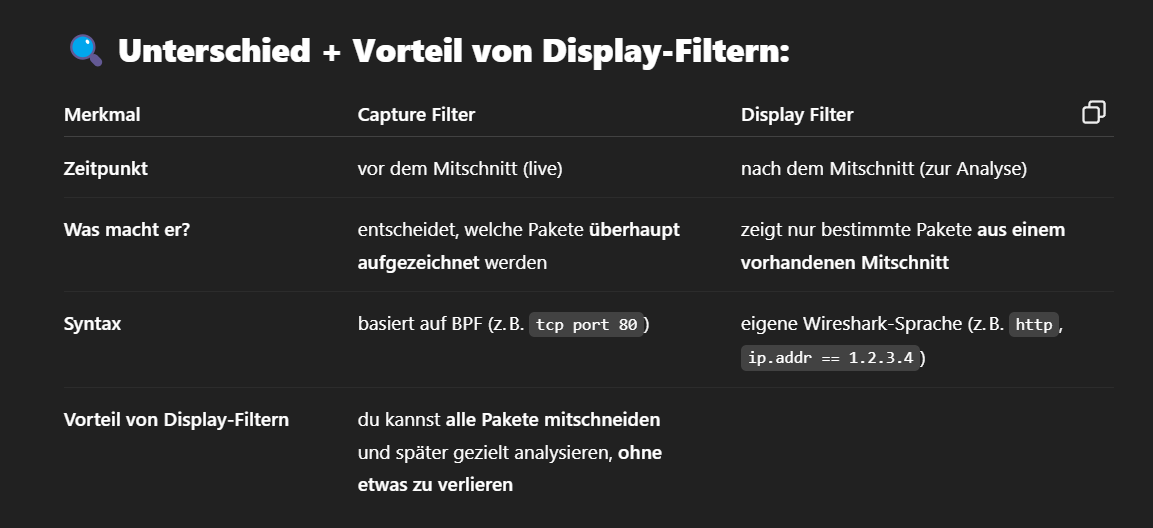
* **100 Mbit/s empfangen + 100 Mbit/s senden = 200 Mbit/s Gesamtdatenrate**
* Der Mirror-Port muss **mindestens 200 Mbit/s** verarbeiten können.

#### **Fünf Ports mit je 100 Mbit/s duplex**:

* Jeder Port = 200 Mbit/s → 5 × 200 Mbit/s = **1000 Mbit/s**
* **Mindestens 1 Gbit/s** (Gigabit-Port!) nötig für den Mirror-Port

### *2.1 Starten Sie Wireshark und sehen Sie sich die Capture Options an. Was ist ein Interface?* 📌 In Wireshark bedeutet Interface:

**„Wo soll Wireshark den Verkehr mitschneiden?“**  
Wenn du z. B. über WLAN im Internet surfst, musst du das **WLAN-Interface** auswählen.



***2.7 Überlegen Sie, welche (legalen und illegalen) Konsequenzen durch diese Transparenz entstehen. Welche technischen Herausforderungen stellen sich beim Sniffen? Diskutieren Sie mögliche Abwehrmaßnahmen.***

## 🔎 **1. Konsequenzen der Transparenz durch Sniffing**

### ✅ ****Legale Folgen / sinnvolle Nutzung:****

* **Netzwerkdiagnose und Fehlersuche**
* **Performance-Analyse** (z. B. wo ist der Flaschenhals?)
* **Sicherheitsüberwachung** (z. B. IDS-Systeme)
* **Analyse von Protokollen** in Ausbildung oder Entwicklung

### ❌ ****Illegale / kritische Nutzung:****

* **Abhören von Passwörtern** oder Sessions in unverschlüsseltem Verkehr (z. B. HTTP, FTP)
* **Auslesen von personenbezogenen Daten**
* **Man-in-the-Middle-Angriffe**
* **Industriespionage** oder Datenschutzverletzung (DSGVO!)

## 🧱 **2. Technische Herausforderungen beim Sniffing**

* **Switched Networks**: Switches senden Pakete nur an den Zielport → Sniffer sieht nichts ohne **Port Mirroring** oder **ARP-Spoofing**
* **Verschlüsselter Traffic (TLS/HTTPS)**: Inhalte sind **nicht lesbar**, außer mit Zugriff auf private Schlüssel oder durch MITM
* **Datenmenge**: hoher Traffic = riesige Datenmengen → schwer zu filtern/analysefähig zu halten
* **Timing**: manche Protokolle sind kurzlebig oder paketabhängig → schwer rekonstruierbar



**✅ 3.1 Wie ist das Internet aufgebaut? Welche Netzkomponente koppelt individuelle Teilnetze und wie werden Systeme adressiert?**

* Das Internet besteht aus vielen **autonomen Teilnetzen** (LANs, ISP-Netze, Uni-Netze, etc.)
* **Router** verbinden diese Netze miteinander
* Systeme werden über **IP-Adressen** adressiert (z. B. 192.0.2.1)
* Jede IP-Adresse ist **weltweit eindeutig** (bei IPv4 oder IPv6)

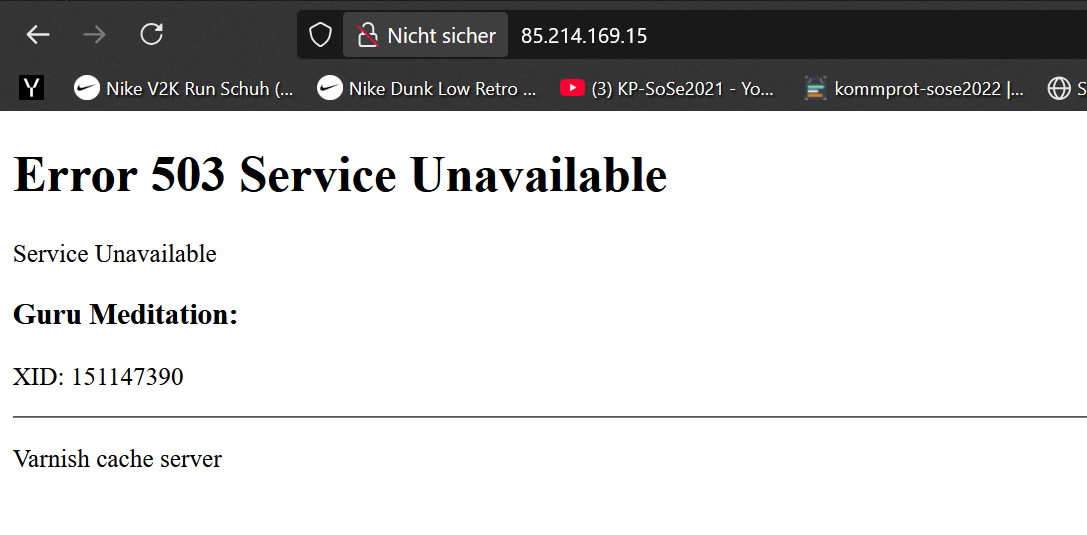
**✅ 3.2 Warum werden im Internet z. B. hs-fulda.de statt IP-Adressen verwendet?**

* IP-Adressen sind **schwer merkbar**, Domains sind **menschlich lesbar**
* Der **DNS (Domain Name System)** übersetzt Namen wie hs-fulda.de in IPs
* Vorteil: IP-Adresse kann sich ändern, der Name bleibt gleich

**3.4 In manchen Fällen gibt der DNS-Server mehrere IP-Adressen zurück – z. B.** IPv4 + IPv6**, oder** mehrere Server zur Lastverteilung**.  
Im Fall von www.hs-fulda.de ist aktuell** nur eine IPv4-Adresse eingetragen**, deshalb wird auch nur diese angezeigt**

**3.5**

Der Webserver antwortet auf die IP-Adresse, aber zeigt einen **Fehler 503**, da der Server ohne den richtigen **Host-Header** (z. B. www.hs-fulda.de) nicht weiß, welche Webseite geladen werden soll.  
Dieses Verhalten ist typisch bei Servern mit **virtuellem Hosting** und vorgeschaltetem **Cache (Varnish)**.



3.6.

Beim Aufruf der IP-Adresse von www.heise.de (193.99.144.85) zeigt der Server eine **funktionierende Antwortseite** an.  
Diese verweist auf https://www.heise.de/ping und zeigt, dass der Server **auch ohne Domainname** antworten kann — ein bewusst konfigurierter HTTP-Endpunkt zur Verfügbarkeitsprüfung.