OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

Prof. Dr. Waas

Praktikum zum Fach

**Kommunikationssysteme/
Rechnernetze**

Übung

TCPIP 1

EINFÜHRUNG IN WIRESHARK

Linux

(Version 02.03.2022 KVM)

1 EINFÜHRUNG

Ziel dieser Übung ist es, Sie mit dem Programm Wireshark vertraut zu machen. Dieses Programm ist ein **wichtiger Bestandteil** der in diesem Semester durchgeführten Übungen. Mit Wireshark können Daten direkt vom LAN aufgezeichnet und dargestellt werden.

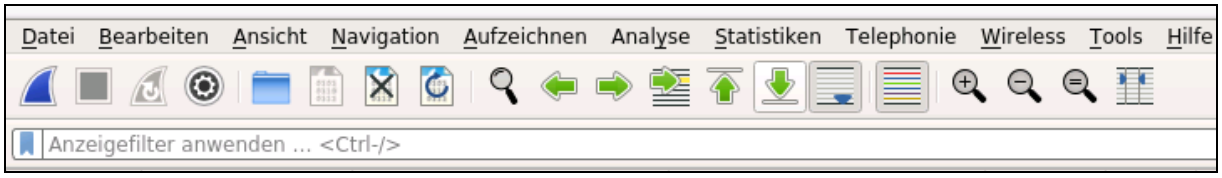
Das Programm kann unter den sog. Hackerparagrafen §202c StGB fallen, da es die Möglichkeit des Ausspähens und Abfangens von Daten vorbereitet und ermöglicht.

"Als Reaktion auf die wachsende Kritik hat der Rechtsausschuss des Deutschen Bundestages 2007 in einem Bericht (Bundestags-Drucksache 16/5449) darauf hingewiesen, dass der gutwillige Umgang mit Hackertools durch IT-Sicherheitsexperten nicht vom § 202c StGB erfasst werde. Auch die Bundesjustizministerin Brigitte Zypries verwies im Juli 2007 mehrfach darauf, dass dieser Paragraf nur die Vorbereitungshandlungen zu Computerstraftaten unter Strafe stelle." (Zitat: Wikipedia Hackerparagraf)

Dieses Tool wird in den Übungen zur Visualisierung von technischen Vorgängen im LAN-Bereich eingesetzt und soll die Lehre unterstützen. Die Verwendung dieses Tools ist im Rahmen der Laborübungen und nur im Labor ausdrücklich gestattet. Aufgezeichnete Pakete müssen vertraulich behandelt und am Ende des Semesters gelöscht werden. Daten mit versehentlich ausgespähten Passwörtern sind sofort zu löschen. Verschlüsselte Daten dürfen nicht entschlüsselt werden.

2 WIRESHARK STARTEN

- Starten Sie auf dem lokalen Labor-PC das Programm **WireShark**. Klicken Sie dazu doppelt auf das Wireshark Icon auf dem Desktop. Das folgende Bild zeigt einen Teil des Eröffnungsmenüs von Wireshark.



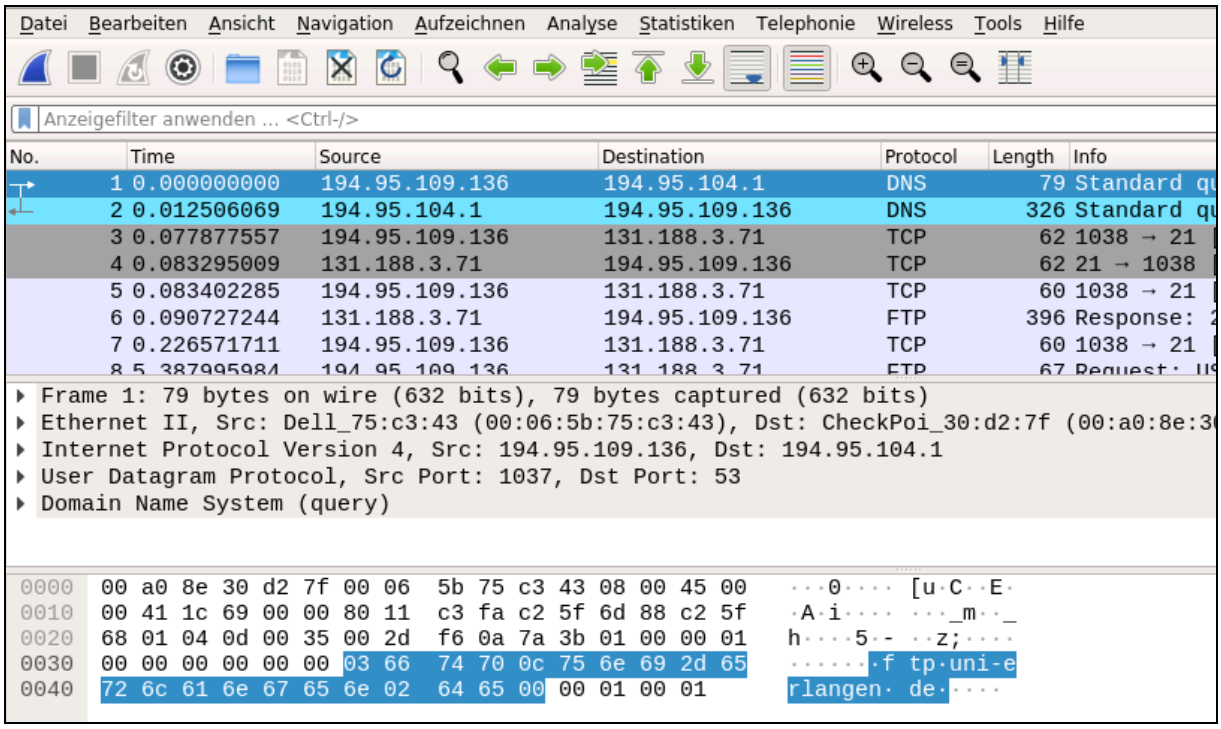
- Öffnen Sie das **Datei Menü** und wählen Sie **Öffnen...** aus.
- Wählen Sie im geöffneten Dateibrowser von Wireshark die Datei **/home/kurs/D/captures/ftp.enc** (Wireshark capture Date) aus.

Die Datei "ftp.enc" enthält eine Aufzeichnung von Ethernet Paketen aus früherer Zeit. Insbesondere wurde eine FTP-Sitzung aufgezeichnet. Es ist möglich eine frühere Aufzeichnung wieder zu laden und zu analysieren.

Das folgende Bild zeigt Ihnen die Aufbereitung der in der Datei ftp.enc gespeicherten Ethernet-Pakete. Es werden im Wireshark Fenster 3 Bereiche dargestellt:

- Summary-Pane
- Detail-Pane
- Hex-Pane

In jedem Bereich werden die Ethernetdaten anders aufbereitet und dargestellt.



Der oberste Bereich zeigt jedes Paket in einer Zeile an. Dieser Bereich wird Summary- Pane genannt.

Der mittlere Bereich zeigt für jedes Paket, der im Summary-Pane angewählt wird, eine detaillierte Darstellung an. Da ein Paket aus mehreren Teilen besteht, die von den jeweiligen Protokollschichten hinzugefügt wurden, können diese einzelnen Schichten aufgeklappt (expandiert) werden. Dazu muss man links auf das ► Symbol klicken.

Der unterste Bereich ist das sog. Hex-Pane. Dort wird der im Summary-Pane aktuell ausgewählte Paket in hexadezimaler Darstellung angezeigt. Wenn man im Detail-Pane einzelne Details anklickt, werden die dazugehörigen Bytes aus dem Hex-Pane farblich hinterlegt. Man kann also sehen, wie die Daten wirklich im Paket abgebildet werden.

3 ISO SCHICHTEN LAYER

Mit Wireshark kann man sehr schön die Protokollschichten verfolgen, aus denen ein Paket aufgebaut ist. (ISO Schichtenmodell). Im Detailfenster können die einzelnen Schichten expandiert (aufgeklappt) werden. Analog dazu werden im Hex-Fenster die zugehörigen Bytes farbig hinterlegt.

- Klicken Sie auf Paket **Nr. 6** im Summary-Pane.
- **Expandieren** Sie im **Detail-Pane** die **Frame-Anzeige** (auf ► bei Frame klicken). Die Frame-Anzeige stellt allerdings keine Protokollschicht dar, sondern liefert nur statistische Werte des Ethernet-Treibers, der dieses Paket aufgezeichnet hat, z.B. Uhrzeit der Aufzeichnung, Paketlänge, Netzwerkadapter usw.
- Expandieren Sie im Detail-Pane die **Ethernet-Schicht** (Zeile wird farblich hinterlegt).

- Finden Sie im **Hex-Pane** die zur Ethernet Schicht gehörenden Bytes (sind auch farblich hinterlegt).
- Klicken Sie innerhalb der expandierten Ethernet-Schicht auf **Type** und lokalisieren Sie im Hex-Pane, wo diese Information im Ethernet Paket liegt.
- Verfahren Sie analog dazu mit den anderen Schichten dieser Pakete und beantworten Sie die folgenden Fragen.

Kontrollfragen

- ☑ Wie lange ist das Paket insgesamt?
- ☑ Wie viele Bytes umfasst die Ethernet-Schicht dieses Pakets?
- ☑ An welcher Position im Paket befinden sich Ethernet-Source-Adresse und Ethernet-Destination- Adresse?
- ☑ Wo steht die Type-Information?
- ☑ An welcher Position beginnt die IP-Schicht?
- ☑ Wie lange ist der IP-Header der IP-Schicht des Pakets?
- ☑ An welcher Position beginnt die TCP-Schicht?
- ☑ Wie lange ist der TCP-Header der TCP-Schicht des Pakets?
- ☑ Wie viele Bytes an Nutzdaten wurden mit FTP in diesem Paket transportiert?
- ☑ Wie ist das Verhältnis der Schichten-Header zur tatsächlichen Nutzlast (FTP) in diesem Paket?

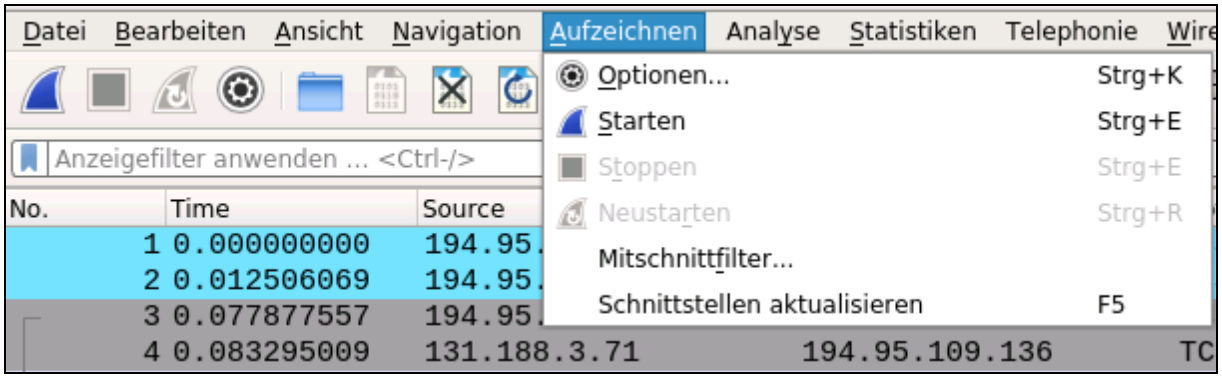
4 DARSTELLUNG ANDERER PROTOKOLLINFORMATIONEN

- Wählen Sie Paket **Nr. 6** und expandieren Sie die **Internet Protokoll Schicht**. Klicken Sie auf **Destination**. Im Detail-Pane sehen Sie die IP-Adresse 194.95.109.136. Wie wird die IP-Adresse im Hex-Pane dargestellt? Vergleichen Sie die dezimale Darstellung mit der hexadezimalen Darstellung. Stimmen beide überein?
- Vergleichen Sie die Haeder-Länge der **Transmission Control Protokoll Schicht** in Paket **Nr. 6.** mit der in Paket **Nr. 4**. Sind beide gleich lang? Was ist anders bei Paket Nr.4?
- Wenn TCP-Header unterschiedlich lang sein können, woher kann man dann wissen, an welcher Position die Nutzdaten beginnen? Suchen Sie die Erklärung in der TCP-Header!
- Betrachten Sie Paket **Nr. 5**. Dort taucht auf Ethernet Layer ein Feld mit dem Namen Padding auf. Ein Padding wird in dem Paket eingebaut, um die Mindestlänge von 64 Bytes zu garantieren. Ermitteln Sie die Länge aller Protokollschichten in diesem Paket ohne Padding.
  Hinweis: Die CRC Checksumme (32 Bit) wird nicht aufgezeichnet. Darum fehlen 4 Byte bei der Längenangabe des Pakets.

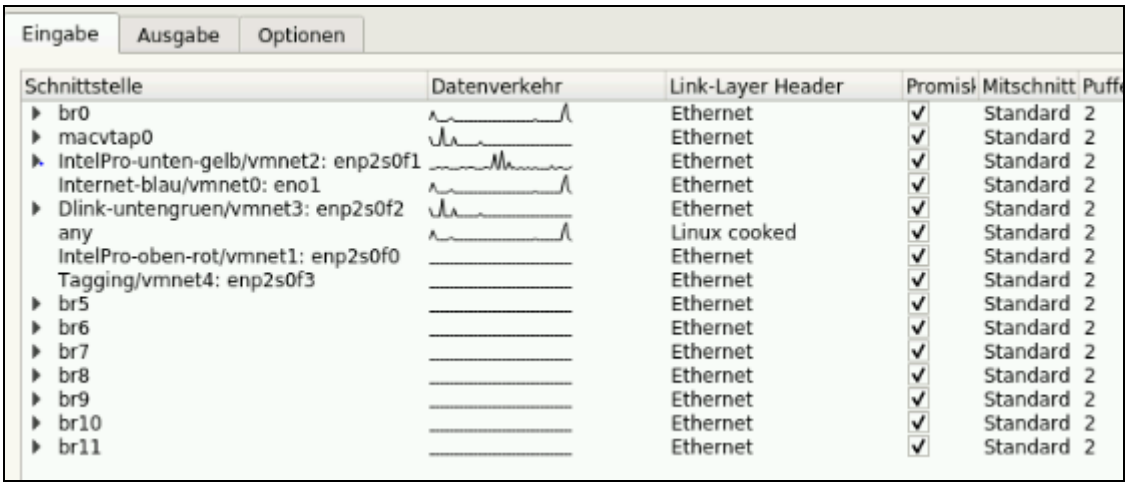
5 ETHERNET PAKETE AUFZEICHNEN

Mit Wireshark können auch Pakete direkt vom Ethernet aufgezeichnet werden. Da der Labor-PC mehrere Ethernet Interfaces hat, müssen Sie eines für die Messung auswählen. Wenn die Messung gestartet wurde, werden die Ethernet Pakete aufgezeichnet (sog. Capture) und sofort am Bildschirm dargestellt.

- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen** aus.



- Wählen Sie das Interface **Internet blau** und klicken Sie auf den **Start**-Button. Sofort wird mit der Messung begonnen und Sie können verfolgen, welche Pakete aufgezeichnet werden. Lassen Sie die Messung 1 Minute laufen. **Häkchen** bei **Promiscuos**!



- Öffnen Sie erneut das **Aufzeichnen Menü** und wählen Sie **Stoppen**. Nun wird die Messung wieder angehalten (Start und Stop geht auch über die Menüleiste).

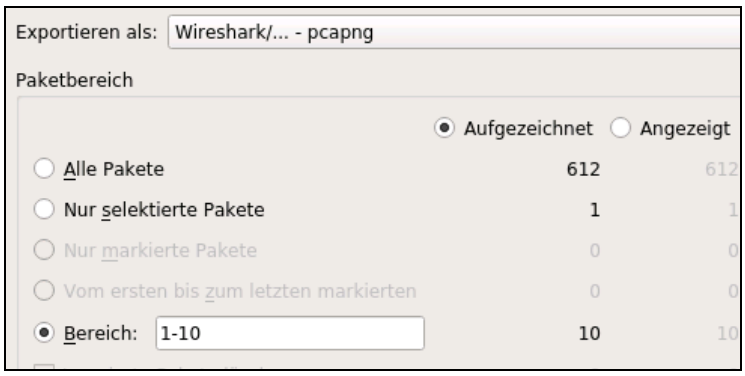
6 EXPORTIEREN / SPEICHERN VON PAKETEN

Sie können entweder alle oder nur bestimmte Pakete auf Datei speichern. Bitte löschen Sie am Ende der Übung wieder alle von Ihnen gespeicherten Dateien am Labor-PC.

- Öffnen Sie das **Datei** Menu und klicken Sie auf **Spezielle Pakete Exportieren**. Im folgenden Dialogfenster können Sie auswählen, wohin die Datei mit den Paketen gespeichert werden soll. Wählen Sie einen Dateinamen und merken Sie sich das Verzeichnis, in das gespeichert wird.

Wireshark unterstützt die Dateiformate verschiedener Netzwerktools. Für eine Weiterbearbeitung mit Wireshark verwenden Sie das **pcap**- Format.

- Wählen Sie aus, welche Pakete Sie speichern wollen. Dazu finden Sie im Dialogfenster unten links die folgende Anzeige. Dort können Sie einen Bereich (Range) von Paketen angeben, der gespeichert werden soll. Geben Sie die Range von 1 bis 10 ein.



- Weiterhin kann man einstellen, ob man die Pakete so speichern will, wie sie aufgezeichnet wurden, oder so, wie sie gerade in der Anzeige stehen. Es gibt für die Anzeige sog. Display Filter, mit denen man gewisse Pakete aus der Menge der aufgezeichneten Pakete auswählen (filtern) kann. Display Filter sind Thema der nächsten Übungsstunde.
- Wählen Sie das Verzeichnis **/home/kurs/Schreibtisch**, geben Sie einen Dateinamen ein und speichern Sie die Datei ab. Die Datei wird auf dem Desktop gespeichert.
- Laden Sie nun die eben gespeicherte Datei wieder. Öffnen Sie dazu das **Date Menü** und wählen Sie **Öffnen**. Geben Sie den Dateinamen an und klicken Sie auf **Öffnen**.
- Überprüfen Sie, dass nur 10 Pakete in der Datei gespeichert wurden.

Anmerkung: Mit **Save as** können nur alle aufgezeichneten Pakete abgespeichert werden.

- Verschieben Sie bitte die Datei in den Papierkorb (also löschen)!

7 AUSDRUCKEN

Sie können die Pakete auch in Textform ausdrucken. Um unseren Drucker zu schonen, soll aber nicht direkt ausgedruckt werden, sondern die Information in eine Datei gedruckt werden.

- Öffnen Sie das **Date Menü** und wählen Sie **Drucken**.

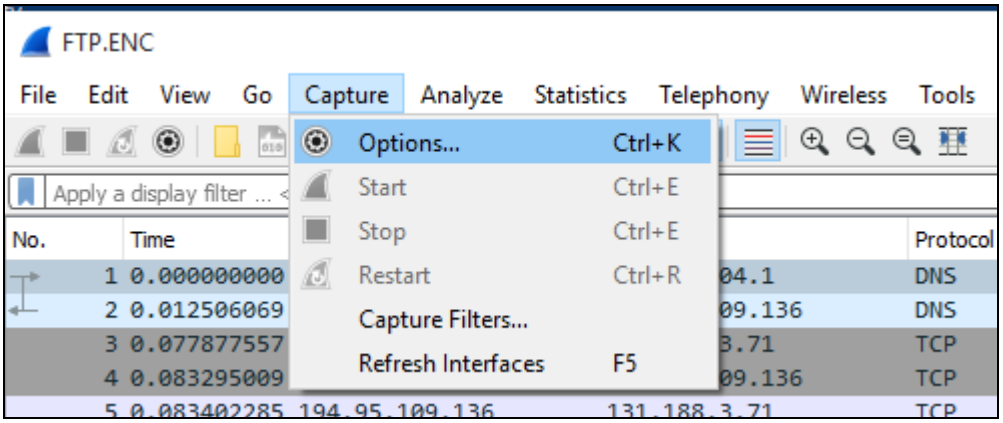
- Geben Sie als **Bereich 1 bis 3** ein. Damit werden nur die Pakete 1 bis 3 gedruckt.

- Wählen Sie als **Paketformat: Übersichtszeile, Details** und **alle aufgeklappt** aus und klicken Sie auf **Print…**.
- Wählen Sie **In PDF Datei drucken** aus.
- Wählen Sie die **Ausgabedatei** in **/home/kurs/Schreibtisch** aus und geben Sie einen Dateinamen ein.
- Klicken Sie auf **Drucken** und speichern Sie die Datei ab, sodass Sie sie nachher wiederfinden.
- Betrachten Sie den Inhalt der PDF-Datei.
- Verschieben Sie bitte diese PDF-Datei danach in den Papierkorb (also löschen)

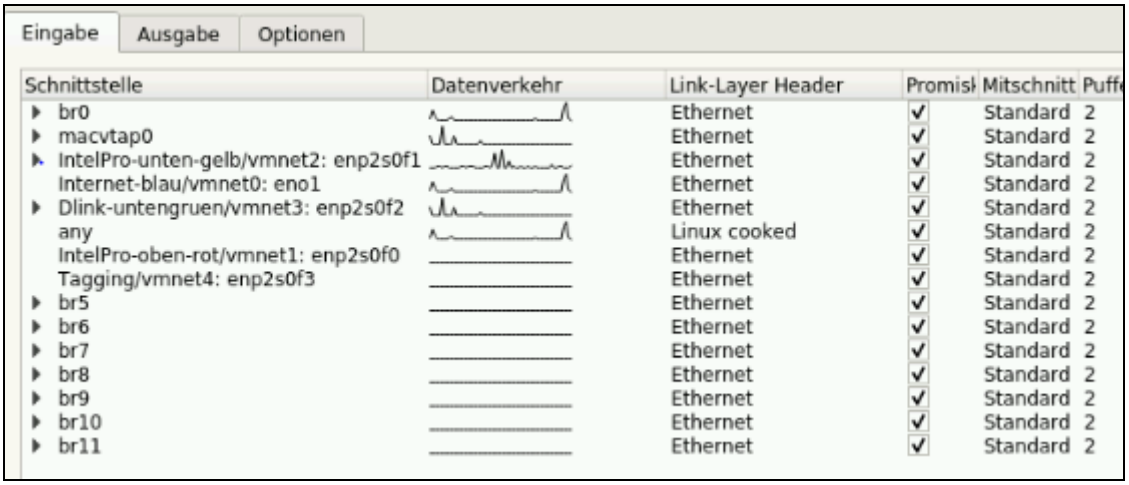
8 WEITERE MESSUNGEN

Nutzen Sie nun die verbleibende Zeit, um mit Wireshark etwas Übung zu bekommen.

- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Options** aus.



- Wählen Sie das Interface **Internet blau** aus. **Häkchen** bei **Promiskuitiv (engl. promiscuous)!**

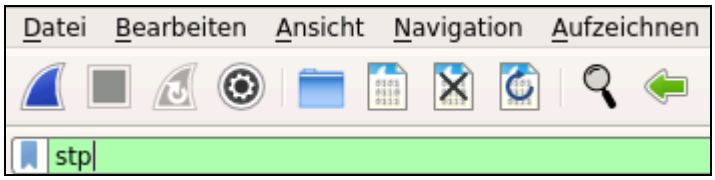


- Starten Sie die Messung und fahren Sie mit dem folgenden Kapitel fort.

8.1 EINIGE SPEZIELLE LAYER-2 PROTOKOLLE

Die folgenden Protokolle werden nicht in der Vorlesung behandelt. Trotzdem sollen sie im Rahmen des Praktikums kurz gezeigt werden. Es steht Ihnen frei, sich darüber bei z.B. Google weitere Informationen zu besorgen.

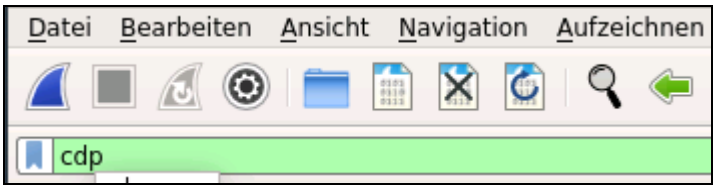
- Geben Sie in der Filterzeile (oben) **stp** ein. Damit filtern Sie alle stp-Pakete (stp=Spanning-Tree-Protocol). STP verhindert die Entstehung von Switching Loops.



Kontrollfragen

- ☑ In welchem **Zeitabstand** kommen diese Pakete?
- ☑ Wie lautet der **Port Identifier** in einer beliebigen Meldung? Darüber kann man manchmal schließen, an welchem Port des Switches man angeschlossen ist (Port-ID – 0x8000)

- Geben Sie in der Filterzeile (oben) **cdp** ein. Damit filtern Sie alle cdp-Pakete (cdp=Cisco Discovery Protocol)



Kontrollfragen

- ☑ An welchem Port des Cisco Switches (**Port ID**) ist ihr PC angeschlossen?
- ☑ In welchem **VLAN** sind Sie? (Was VLAN ist lernen Sie später)
- ☑ Welcher **Duplex Modus** hat Ihre LAN-Verbindung zum Switch? **Full Duplex** bedeutet in beide Richtungen gleichzeitig, **Half Duplex** bedeutet immer nur in eine Richtung zu einem Zeitpunkt.

9 ENDE DER ÜBUNG

- Beenden Sie alle **Programme** und **virtuelle Maschinen**! Im Rahmen der Übung an Ihrem Arbeitsplatz erzielte Messergebnisse können Sie im Labor auf Ihren Memorystick zur späteren Nachbearbeitung abspeichern. Gewonnene sicherheitsrelevante Informationen insbesondere Passwörter, dürfen nicht weitergegeben oder unbefugt verwendet werden. Geht leider nicht im Remotebetrieb.
- **Loggen** Sie sich aus dem Labor-PC **aus!**
- Lassen Sie den PC weiterlaufen. Er wird automatisch ausgeschaltet.

Bitte hinterlassen Sie Ihren Arbeitsplatz in ordentlichem Zustand!

Entsorgen Sie Mitgebrachtes selbst!

Schieben Sie den Stuhl an den Tisch!