

# **Praktikumsbericht 1 – Einführung 1 (Protokollanalyse)**

**Praktikum Teleinformatik**



Ecole d'ingénieurs et d'architectes de Fribourg  
Hochschule für Technik und Architektur Freiburg

M. Heinzer  
Michael.heinzer@edu.hefr.ch  
B. Leutwiler  
Bernhard.leutwiler@edu.hefr.ch

## Inhaltsverzeichnis

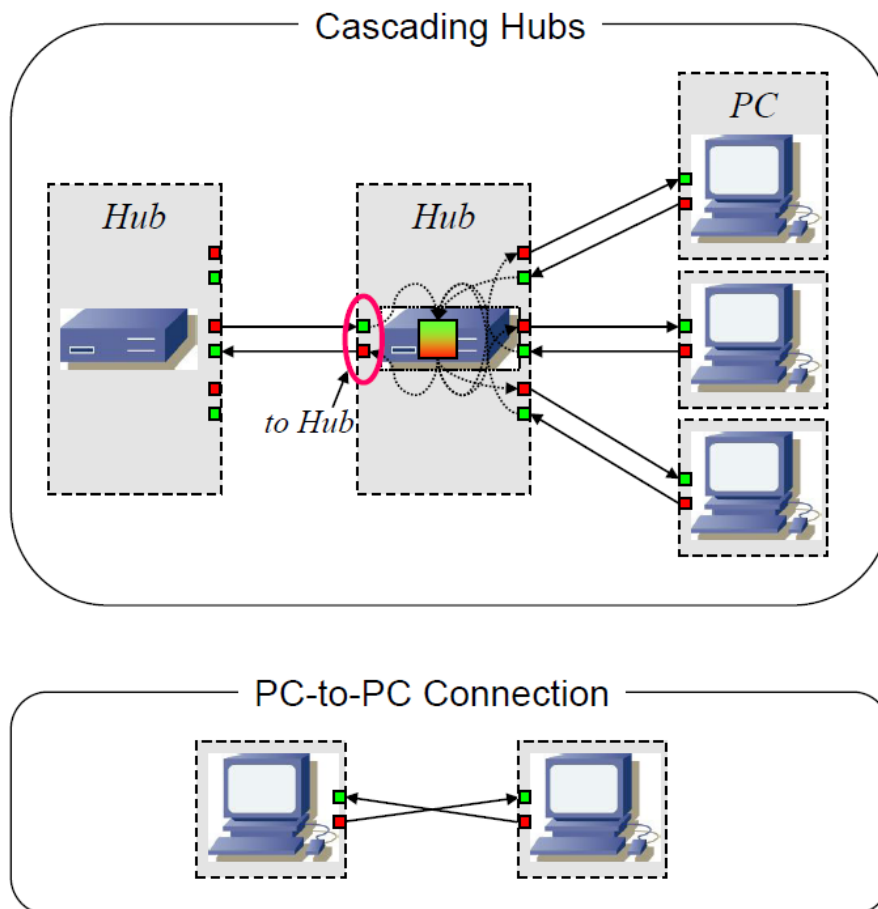
1. Einführung ..... 2
2. Beschreibung des Lösungsansatz des Problems und getätigte Arbeit (Struktur / Inhalt)..... 2
3. Schlussfolgerung..... 6

### 1. Einführung

In diesen ersten Laborstunden ging es vor allem um die Einführung in die Umgebung und Werkzeuge welche wir in den folgenden Wochen und Monaten gebrauchen werden. Genauer werden wir uns mit der Architektur der Protokolle, dem Programm Wireshark und der Analyse der Messungen beschäftigen.

### 2. Beschreibung des Lösungsansatz des Problems und getätigte Arbeit (Struktur / Inhalt)

Anschluss der Kabel:



Damit man Hubs miteinander verkabeln kann, braucht es entweder ein gekreuztes Kabel (Crossover cable) oder einen gekreuzten Port am Hub. Ansonsten sind die Sendeleitungen identisch und die

Empfangsleitungen und somit ist kein Datentransfer möglich. Neuere Geräte sind selber automatisch im Stande solche Fehler zu erkennen und umzuschalten.

### 3. Lösungen zu den Fragen

- P1:

Die Kabel sind an der Netzwerkkarte angeschlossen, wir haben 3 Ein/Ausgänge gefunden, zweimal ein Ethernet RJ-45 Anschluss und einmal ein ISDN-Anschluss.

- P2:

Zur Anzeige der Einstellungen empfiehlt es sich in der „cmd“ Konsole mit „ipconfig /all“ die Werte anzeigen zu lassen. Geändert werden diese dann in den Systemeinstellungen mit einem Rechtsklick auf die Netzwerkanschlüsse. Dort lassen sich die Schichten 1 und 2 sowie 3 und 4 konfigurieren.

- P3:

(1) Auf diesem Bildausschnitt sehen wir eine Übersicht der gefundenen Rahmen (Frames).

(2) Strukturierter Inhalt des Frames, sortiert nach den Protokollen.

(3) Der rohe Inhalt des Frames, angezeigt in Bytecode.

The screenshot shows the Wireshark interface with the following data:

No.	Time	Source	Destination	Protocol
58	6.000036	Cisco_2b:7a:85	Spanning-tree-(for-br	STP
59	6.229237	Cisco_2b:7a:85	Cisco_2b:7a:85	LOOP
60	6.424553	0.0.0.0	255.255.255.255	DHCP
61	6.426661	Cisco_61:9e:80	Broadcast	ARP
62	6.432469	160.98.30.9	224.0.0.5	OSPF
63	6.625451	0.0.0.0	255.255.255.255	DHCP
64	6.627933	0.0.0.0	255.255.255.255	DHCP
65	6.630069	160.98.30.1	255.255.255.255	DHCP
66	6.630450	160.98.30.1	255.255.255.255	DHCP
67	6.917047	160.98.30.25	239.255.255.250	SSDP
68	6.965668	fe80::20f:24ff:fe06:3	ff02::5	OSPF
69	7.607485	0.0.0.0	255.255.255.255	DHCP
70	7.630376	0.0.0.0	255.255.255.255	DHCP
71	7.632719	0.0.0.0	255.255.255.255	DHCP
72	7.634910	160.98.30.1	255.255.255.255	DHCP
73	7.635303	160.98.30.1	255.255.255.255	DHCP
74	7.807865	160.98.31.136	224.0.0.251	MDNS

Packet 25 details:

- Frame 25 (54 bytes on wire, 54 bytes captured)
- Ethernet II, Src: IntelCor\_1c:14:7f (00:1c:c0:1c:14:7f), Dst: Cisco\_61:9e:80 (00:1a:30:61:9e:80)
  - Destination: Cisco\_61:9e:80 (00:1a:30:61:9e:80)
  - Source: IntelCor\_1c:14:7f (00:1c:c0:1c:14:7f)
  - Type: IP (0x0800)
- Internet Protocol, Src: 160.98.30.25 (160.98.30.25), Dst: 160.98.2.13 (160.98.2.1)
  - Version: 4

Packet bytes:

```

0000 00 1a 30 61 9e 80 00 1c c0 1c 14 7f 08 00 45 00  ..0a.... .....E.
0010 00 28 01 f8 40 00 80 06 97 ed a0 62 1e 19 a0 62  .(.@... ..b...b
0020 02 0d 04 21 01 bd 40 e4 3e 55 58 f2 5a e6 50 11  ...!..@. >UX.Z.P.
0030 fc 03 61 05 00 00                                ..a...

```

- P4:

Die gefangenen Rahmen lassen sich auch in ein Textfile „drucken“. In diesem befindet sich dann die Rahmen wie sie im zweiten Abschnitt im Wireshark angezeigt werden, jedoch ist dies sehr unübersichtlich und es empfiehlt sich somit nicht für grössere Mengen. Man kann wählen ob nur die Überschrift der Rahmen oder auch der Inhalt angezeigt werden soll.

- P5:

Dadurch dass wir einen Hub benutzen werden alle eingehenden Pakete an alle Ausgänge versendet. Der Hub arbeitet nur auf der untersten Stufe des OSI-Modells, deshalb kann er nicht nach dem MAC-Adressen filtern und sendet allen Teilnehmern alle Pakete.

- P6:

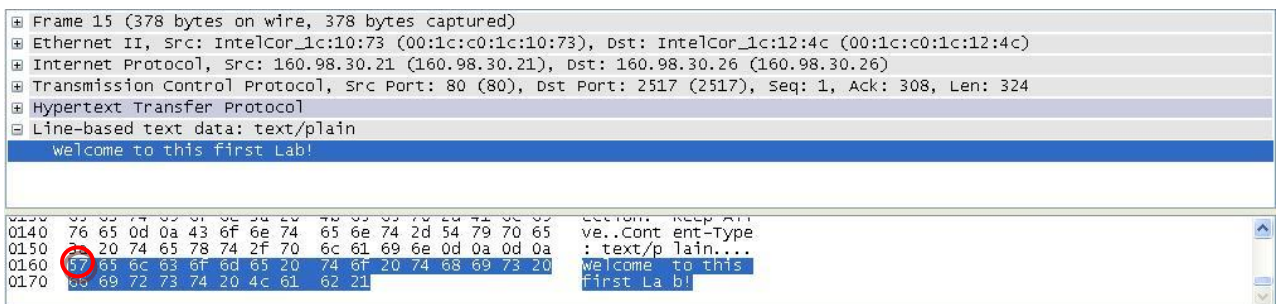
In den LAN-Kabeln (RJ-45) befinden sich nochmals verschiedene Drähte, auf diesen wird jeweils gesendet und empfangen. Damit nicht beide Stationen auf dem gleichen Draht senden oder empfangen hat man dies standardisiert. Hubs oder Switches nützen automatisch den jeweils anderen Draht. Wenn jedoch zwei Computer kommunizieren benötigt man ein Kabel bei welchem diese Drähte intern vertauscht wurden. So verhielt es sich früher, heute besitzen die meisten Netzwerkgeräte eine Funktion die ein solches Problem automatisch erkennt und behebt.

- P7:

Zuerst wird eine Verbindung mit TCP aufgebaut, danach kann das eigentliche Web Protokoll http die Anfrage für die Website stellen. Im folgenden Antwort-Paket wird dann die Text-Nachricht (Payload) übermittelt.

- P8:

Es befindet sich in der Payload Sektion des Protokolls http. Das heisst in der obersten Schicht des OSI-Modells. Es ist das erste Byte dieses Abschnittes.

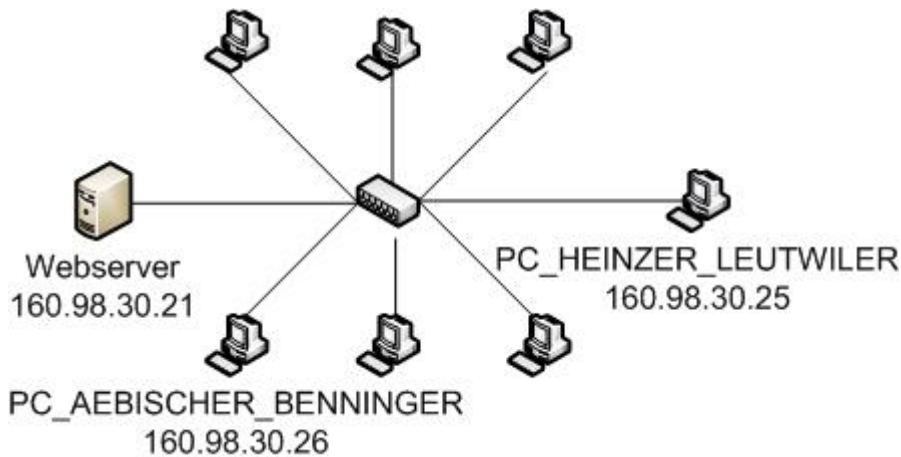


- P9:

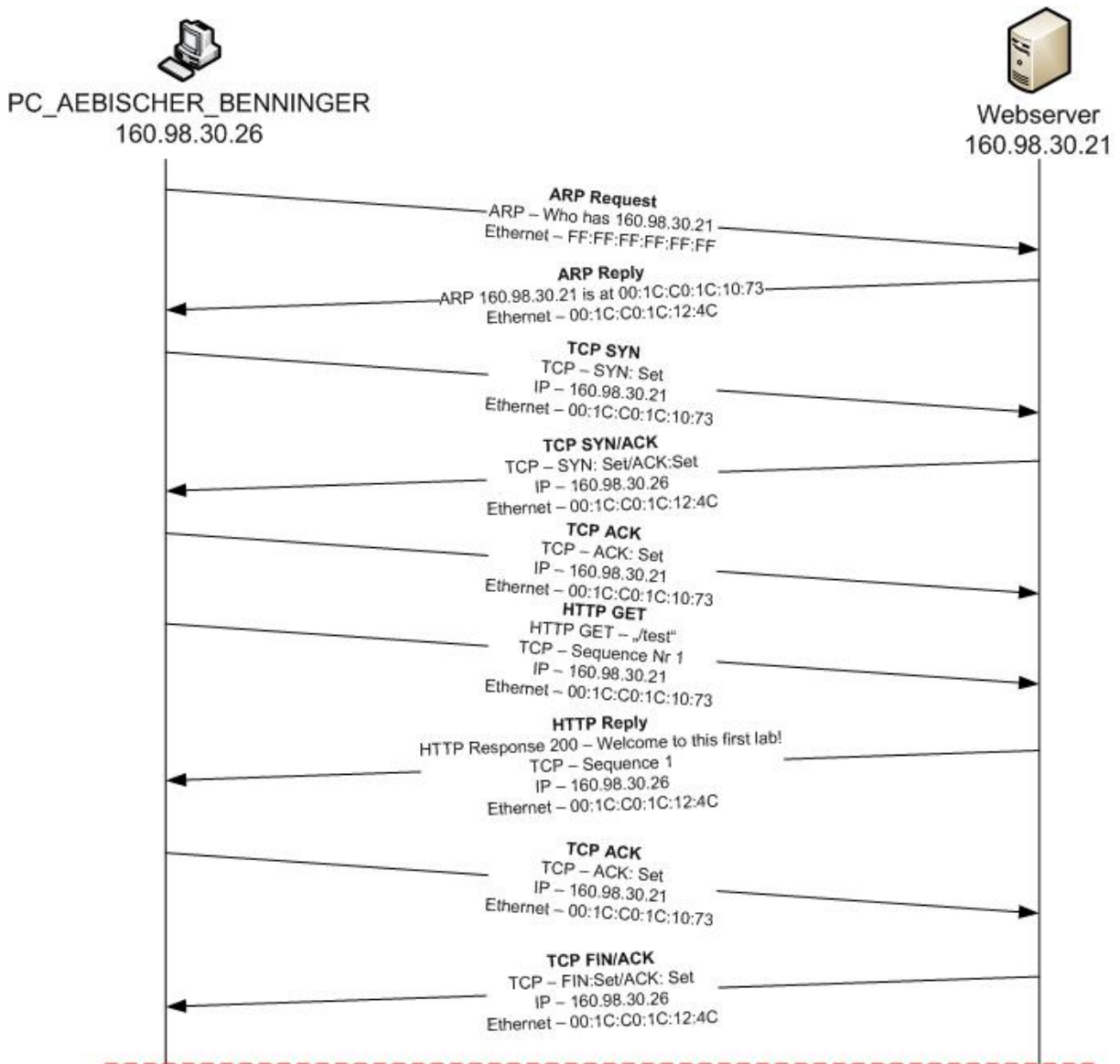
ETHER Header	IP Header	TCP Header	HTTP Header	Welcome to this first lab!	FCS
14 bytes	20 bytes	20 bytes	298 bytes	26 bytes	4 bytes

Gesamtgrösse: 378 bytes.

- P10:



- P11:



- P12:
  - Der Client erfragt die MAC-Adresse der Ziel-IP Adresse
  - Der Server meldet seine MAC-Adresse an den Client
  - Der Client fragt für einen Verbindungsaufbau
  - Der Server bestätigt die Anfrage und sendet zur Sicherheit ebenfalls eine Anfrage
  - Der Client bestätigt die Anfrage
  - Der Client sendet bereits im http Protokoll eine Anfrage für den Text an der Stelle „/test“
  - Der Server sendet die angefragte Nachricht zurück
  - Der Client bestätigt dem Server den Erhalt der korrekten Nachricht
  - Der Client sendet ein Endsignal der Verbindung
  - Die Verbindung ist beendet
- P13:
  - Nach Protokoll
  - Nach Host oder Destination Adresse (IP und MAC)
  - Follow TCP Stream (TCP Stream verfolgen und abhängige Rahmen anzeigen)
- P14:

Im HTTP-Get Rahmen ändert sich die Information „User-Agent“

#### 4. Schlussfolgerung

Abschliessend können wir sagen dass diese Laborstunden uns einen ersten kurzen Einblick in die Teleinformatik erlaubt haben. Diese Stunden haben für uns zwar nichts neuer hervorgebracht, doch wir konnten uns gut an die neue Umgebung gewöhnen.