Lösungsvorschlag

Rechnernetze und verteilte Systeme im Sommersemester 2013

Übungsblatt 2

1. **Mini-Beispiel zu Wireshark**

   Sofern noch nicht vorhanden, installieren Sie zunächst den Netz-Protokoll-Analysator Wireshark auf Ihrem Rechner. Im CIP-Pool ist Wireshark bereits installiert. Sie finden Wireshark in Ihrer Paketverwaltung, oder auf *http://www.wireshark.org/*. Laden Sie dann von der Webseite der Vorlesung die Datei `trace1.pcap` herunter.

   Öffnen Sie diese Datei mit Wireshark und interpretieren Sie, den mitgeschnittenen Datentransfer. Vernachlässigen Sie dabei zunächst alle Angaben der Ebenen Ethernet II und Internet Protocol, betrachten Sie nur den Teil, der dem Internet Control Message Protocol zugeordnet ist.

   (a) Wie sind die Nachrichten aufgebaut, d.h. wie sind die Daten strukturiert und welche Informationen enthalten sie?

   Lösung:

   Typ (1 Byte), Code (1 Byte), Prüfsumme (2 Byte), Bezeichner (2 Byte), Sequenznummer (2 Byte), evtl. Blinddaten. Darstellung aus RFC 792 (http://tools.ietf.org/html/rfc792)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Identifier          |       Sequence Number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Data ...
+-+-+-+-+-
```

   (b) Wie sieht das zeitliche Verhalten des Nachrichtenaustausches aus?

   Lösung:

   - (Anfrage – Antwort) bzw. (Echo Request – Echo Reply)
   - (ungefähr) 1 Sekunde warten
   - ggf. wiederholen, hier 4 Wiederholungen

   (c) Berechnen Sie die mittlere Verzögerung der Antworten auf die Anfragen!

   Lösung:

   Es lassen sich über die Rahmen-Informationen leicht die Verzögerungen ermitteln:

```
(gerundet)
14,8 ms
14,9 ms
15,3 ms
15,3 ms
-----------
15,075 ms im Durchschnitt
```

   (d) Wozu könnte der gezeigte Netzverkehr dienen?

   Lösung:

   Es handelt sich um sog. “Pings”. Diese sind ein Einsatz des ICMP zur Prüfung der Erreichbarkeit entfernter Rechner. Man sendet einen ICMP-Echo-Request und das Protokoll sieht vor, dass ein (Ziel-)Rechner, der einen solchen Request erhält, dem Absender mit einem ICMP-Echo-Reply antwortet.

   Gleichzeitig kann man auf diese Art und Weise den Round-Trip-Delay (manchmal auch Round-Trip-Time genannt) messen, also die Gesamtverzögerung beim Versenden einer Nachricht an den Zielrechner und der Antwort an den Quellrechner.

(e) Handelt es sich um eine verbindungsorientierte oder verbindungslose Kommunikation? Begründen Sie Ihre Antwort!

Lösung:
Es handelt sich um eine verbindungslose Kommunikation. Es gibt weder Verbindungsauf- noch -abbau und abgesehen von den aufsteigenden Sequenznummern gibt es keinen logischen Zusammenhang zwischen zwei gesendeten Anfragen. Insbesondere gibt es keine Abhängigkeiten so dass eine bestimmte Nachricht einer anderen vorausgehen müsste.

(f) Sie können die Funktion von der Kommandozeile mit dem Kommando `ping` ausführen. Finden Sie einen Rechner, der zwar im WWW-Browser erreichbar ist (also eine HTML-Seite zurückschickt), aber nicht auf ICMP-Echo-Requests antwortet!

Lösung:
Zum Beispiel Amazons Webseite `www.amazon.de`:

Ping:

```
$ ping -c 4 www.amazon.de                                          #Der Befehl auf der Kommandozeile
PING www.amazon.de (178.236.6.250) 56(84) bytes of data.           #Ausgabe des Programms
                                                                   #Ausgabe des Programms
--- www.amazon.de ping statistics ---                              #Ausgabe des Programms
4 packets transmitted, 0 received, 100% packet loss, time 2999ms   #Ausgabe des Programms
                       ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^            #Hervorhebung einer Textstelle in
                                                                   #der Zeile darüber
```

Die markierte Stelle der Ausgabe zeigt, dass keine Antworten erhalten wurden und das Programm folgert, dass alle Anfragen verloren gegangen sind.

WWW-Seite:

```
$ wget http://www.amazon.de -O -                                   #Der Befehl auf der Kommandozeile
--2013-04-29 09:55:52--  http://www.amazon.de/                     #Ausgabe des Prgramms
Resolving www.amazon.de... 178.236.6.250                           #Ausgabe des Prgramms
Connecting to www.amazon.de|178.236.6.250|:80... connected.        #Ausgabe des Prgramms
HTTP request sent, awaiting response... 200 OK                     #Ausgabe des Prgramms
Length: unspecified [text/html]                                    #Ausgabe des Prgramms
Saving to: "STDOUT"                                                #Ausgabe des Prgramms
                                                                   #Ausgabe des Prgramms
    [<=>                            ] 0           --.-K/s          #Ausgabe des Prgramms
                                                                   #Ausgabe des Prgramms
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"     #Ausgabe des Prgramms <-- HTML Dokument
   "http://www.w3.org/TR/html4/loose.dtd">                         #Ausgabe des Prgramms <-- HTML Dokument
                                                                   #Ausgabe des Prgramms <-- HTML Dokument
                                                                   #Ausgabe des Prgramms <-- HTML Dokument
                                                                   #Ausgabe des Prgramms <-- HTML Dokument
<html>                                                             #Ausgabe des Prgramms <-- HTML Dokument
<head>                                                             #Ausgabe des Prgramms <-- HTML Dokument

[... Ausgabe gekürzt ...]

    [    <=>                        ] 155,113      200K/s   in 0.8s #Ausgabe des Programms
                                                                   #Ausgabe des Programms
2013-04-29 09:55:53 (200 KB/s) - written to stdout [155113]        #Ausgabe des Programms
```

Auf Anfrage wird ein HTML Dokument ausgeliefert.

2. **Einführung in textbasiertes Arbeiten mit Linux**

Unter Linux stehen eine Reihe von Programmen zur Verfügung, mit denen Sie Teile des Vorlesungsinhalts nachvollziehen können. Die meisten Programme bedient man mit der (Text-)Konsole.

(a) Melden Sie sich mit Ihrer Benutzerkennung und Ihrem Passwort an einem Rechner des CIP-Pools an und öffnen Sie eine Konsole!

i. Ermitteln Sie den absoluten Pfad Ihres Home-Verzeichnisses und zeigen Sie dessen Inhalt an!

ii. Wechseln Sie in das Wurzelverzeichnis und dann zurück in Ihr Home-Verzeichnis!

iii. Was ist eine „man-Page"? *Hinweis:* Benutzen Sie den Befehl `man man`!

iv. Mit welchem Parameter zeigt `ls` auch versteckte Dateien an? *Hinweis:* man-Page: [`ls`(1)]!

(b) Der `ping`-Befehl schickt Anfragen zu dem per Hostname oder IP-Adresse spezifizierten Zielrechner, um festzustellen ob der Zielrechner erreichbar ist. Mit dem Erhalt einer Antwort zeigt `ping` die

RTD (roundtrip delay) an.

i. Versuchen Sie den Host ,,www.ifi.lmu.de" mit dem Programm `ping` zu erreichen! Dabei sollen 10 Anfragen im Abstand von 2 Sekunden und je 100 Bytes Nutzdaten verschickt werden.

ii. Wie sind die einzelnen Spalten in der Ausgabe des `ping`-Befehls zu interpretieren?

(c) Der `traceroute`-Befehl zeigt den Pfad von der Quelle bis zur Senke durch ein IP-Netz und misst die RTD zu jedem einzelnen Knoten auf diesem Pfad.

i. Interpretieren Sie die Ausgabe von `traceroute` zum Zielrechner ,,www.ifi.lmu.de"! Welche Informationen beinhaltet die erste Zeile der Ausgabe?

ii. In den darauffolgenden Zeilen stehen je drei Werte, meist in Millisekunden angegeben. Wofür stehen diese Werte?

iii. Die häufige Überprüfung des Pfades zu einem bestimmten Zielrechner mit `traceroute` zeigt manchmal andere Einträge mit einem verschiedenen Pfad. Was kann diese Beobachtung bedeuten?

(d) Mittels `ip` kann die gesamte Konfiguration eines Rechners bezüglich Netzen eingesehen und manipuliert werden, während `netstat` geeignet ist den aktuellen Zustand einzusehen. (Der Funktionsumfang der Programme überschneidet sich teilweise.)

i. Wieviele Schnittstellen existieren im Moment auf Ihrem Rechner?

ii. Welche der Schnittstellen Ihres Rechners sind im Moment aktiv?

iii. Lassen Sie sich die Routing-Tabelle Ihres Rechners anzeigen!

iv. Lassen Sie `netstat` alle aktiven TCP-Verbindungen Ihres Rechners ausgeben!

Lösung:

(a) Mit einer Konsole ...

i. Direkt nach dem erfolgreichen Anmelden am System bzw. dem Öffnen einer Konsole, zeigt `pwd` das Home-Verzeichnis des jeweiligen Benutzers an. Der Inhalt kann mit `ls` ausgegeben werden.

ii.
- `cd /` — zum Wechseln in das Wurzelverzeichnis
- `cd` — man muss sich nicht den Pfad zu seinem Home-Verzeichnis merken. Ein einfaches `cd` ist hinreichend. Der Pfad zum Home-Verzeichnis wird hier automatisch ergänzt bzw. angenommen.

iii. Eine man-Page ist eine Anleitung, meist zu einem Programm. Es gibt aber auch man-Pages für Konfigurationsdateien z.b. interfaces(5) für die Datei /etc/network/interfaces. Die Zahl in Klammern bezeichnet die "Section" der man-page: 1 steht für Shell-Programme und 5 für Konfigurationsdateien. Die ganze Liste ist:

```
1   Executable programs or shell commands
2   System calls (functions provided by the kernel)
3   Library calls (functions within program libraries)
4   Special files (usually found in /dev)
5   File formats and conventions eg /etc/passwd
6   Games
7   Miscellaneous (including macro packages and conven-
    tions), e.g. man(7), groff(7)
8   System administration commands (usually only for root)
9   Kernel routines [Non standard]
```

Manchmal ist es sinnvoll die Section explizit angeben. Es gibt z.B. printf(1) für das Formatierungsprogramm und printf(3) für die C-Funktion. Ein anderes Beispiel sind mount(2) und mount(8).

iv. `ls` zeigt mit dem Parameter `-a` auch versteckte Dateien an.

(b) ping-Befehl

i. Befehl-Syntax: `ping -c 10 -s 100 -i 2 www.ifi.lmu.de`

Beim normalen Verhalten des Programms werden 56 Byte + 8 Byte ICMP-Header Nachrichten verschickt. Hier, in dieser Aufgabe, sind Nachrichten mit 108 Byte Länge zu erwarten.

ii. Ausgabeninterpretation:

1.Zeile `PING pcheger01.nm.ifi.lmu.de (141.84.218.31) 100(128) bytes of data` — ping-Befehl, Startrechner (möglicherweise ohne Namensauflösung), Paketgröße — Das Prgramm informiert den Benutzer über die Anfragen die es stellen wird.

Ab 2. Zeile `108 bytes from pcheger01.nm.ifi.lmu.de (141.84.218.31): icmp_req=1 ttl=63 time=0.566 ms` — Paketgröße, Startrechner, Paketzähler, TTL(time to live) mit höchester Anzahl von Zwischenstationen (hops) bis zum Zielrechner und Antwortzeit — Optische Aufbereitung der empfangenen Antworten

(c) traceroute

i. `traceroute to www.ifi.lmu.de (141.84.218.31), 30 hops max, 60 byte packets` — traceroute-Befehl, Zielrechner (möglicherweise ohne Namensauflösung), maximale Anzahl erlaubter Zwischenstationen (hops), Paketgröße — Das Programm informiert den Benutzer über den Zielrechner, zu dem der Pfad ermittelt wird.

ii. Anzahl der Nachrichten, die ,,gleichzeitig" mit den selben Einstellungen versendet werden.

iii. Der Eintrag kann sowohl einen Ausfall auf dem bekannten Pfad signalisieren, als auch einen falschen/ungültigen Eintrag in der Routingtabelle (Routing-Schleife).

(d) ip & netstat

i. `ip link show` — zeigt alle vorhandenen Schnittstellen in einer nummerierten Liste an. Zum Beispiel mit sieben Schnittstellen:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:15:de:ad:be:ef brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master bond0 state UP qlen 1000
    link/ether 47:11:ba:dc:ab:1e brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master bond0 state UP qlen 1000
    link/ether 00:00:c0:de:ba:5e brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 09:00:ab:ad:1d:ea brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:00:0e:15:ba:c4 brd ff:ff:ff:ff:ff:ff
7: pan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN
    link/ether 00:00:c0:1d:be:er brd ff:ff:ff:ff:ff:ff
```

ii. Die Ausgabe von `ip link show` schreibt explizit `state UP` für jede aktive Schnittstelle.

iii. `ip route show`

iv. `netstat -t`

◇