07 Internet-Protokolle

1 Thema des Praktikums

Im Praktikum werden Methoden und Tools für die Diagnose und Fehlersuche betrachtet. Die Schwerpunkte des Praktikums sind:

- Address Resolution
- IP-Forwarding
- MTU Path Discovery

2 Vorbereitung

Für dieses Praktikum betrachten wir das vermaschte IP-Netzwerk gemäss Abbildung 1. Man beachte, dass die Subnetze an den beiden Standorten (Zürich ZH und Winterthur WIN) unterschiedlich sind:

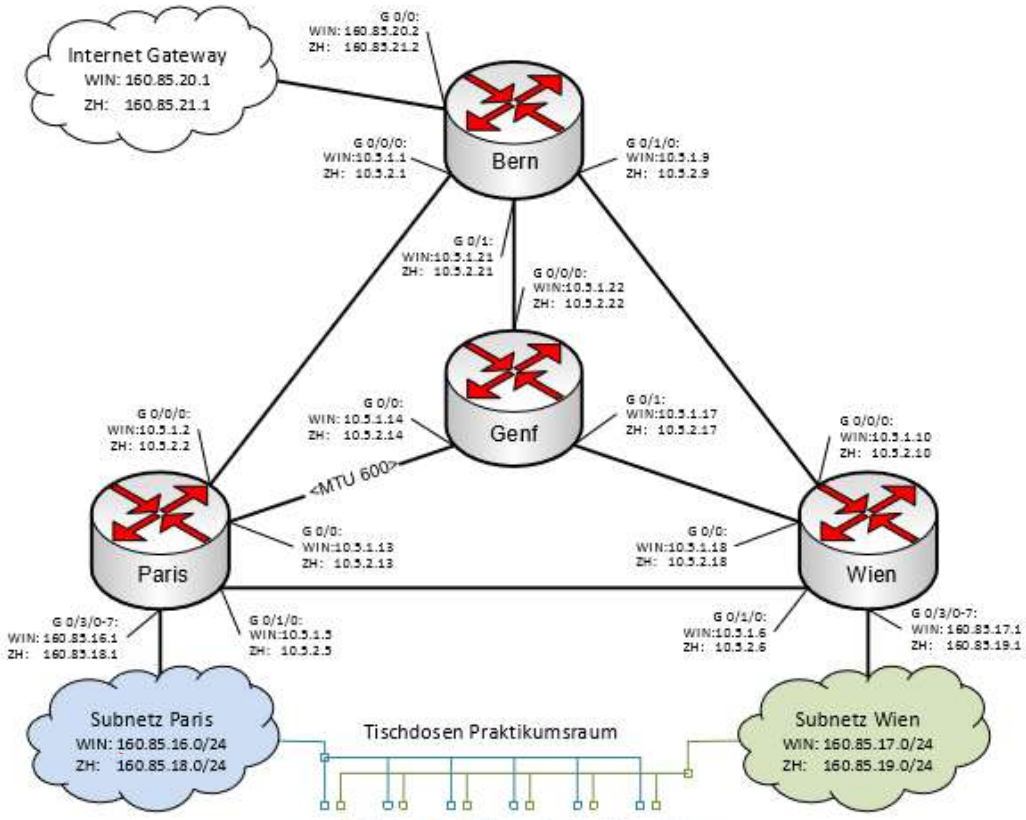

Abbildung 1: IP-Netzwerk des KT-Praktikums

Die zugehörigen Routen sind je nach Standort in Tabelle 1: Routen WIN oder Tabelle 2: Routen ZH zu finden. Die Routen zu den privaten Netzen 10.5.x.x zwischen den Routern sind ebenfalls vorhanden aber aus Platzgründen nicht aufgeführt.

Labor WIN

Router Bern (160.85.20.2):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.16.240	/28	via 10.5.1.10	.255
160.85.16.0	/24	via 10.5.1.2	.255
160.85.17.0	/24	via 10.5.1.10	.255
160.85.20.0	/24	direct, G 0/0	.255
0.0.0.0	/0	via 160.85.20.1	

Router Paris (160.85.16.1):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.17.0	/24	via 10.5.1.6	.255
160.85.16.0	/24	direct G 0/3/0-7	.255
0.0.0.0	/0	via 10.5.1.1	

Router Genf (10.5.1.22):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.16.192	/27	via 10.5.1.13	.223
160.85.17.0	/24	via 10.5.1.18	.255
0.0.0.0	/0	via 10.5.1.21	

Router Wien (160.85.17.1)			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.16.0	/25	via 10.5.1.5	.127
160.85.16.192	/26	via 10.5.1.17	.255
160.85.17.0	/24	direct, G 0/3/0-7	.255
0.0.0.0	/0	via 10.5.1.9	

Tabelle 1: Routen WIN

Labor ZH

Router Bern (160.85.21.2):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.18.240	/28	via 10.5.2.10	
160.85.18.0	/24	via 10.5.2.2	
160.85.19.0	/24	via 10.5.2.10	
160.85.21.0	/24	direct, G 0/0	
0.0.0.0	/0	via 160.85.21.1	

Router Paris (160.85.18.1):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.19.0	/24	via 10.5.2.6	
160.85.18.0	/24	direct G 0/3/0-7	
0.0.0.0	/0	via 10.5.2.1	

Router Genf (10.5.2.22):			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.18.192	/27	via 10.5.2.13	
160.85.19.0	/24	via 10.5.2.18	
0.0.0.0	/0	via 10.5.2.21	

Router Wien (160.85.19.1)			
Netzadresse	**Präfixlänge**	**Route**	**Broadcast-Adresse**
160.85.18.0	/25	via 10.5.2.5	
160.85.18.192	/26	via 10.5.2.17	
160.85.19.0	/24	direct, G 0/3/0-7	
0.0.0.0	/0	via 10.5.2.9	

Tabelle 2: Routen ZH

2.1 Vorbereitung zu Forwarding

- Bestimmen Sie die Adressbereiche der aufgeführten Subnetze, also deren Broadcast-Adressen und tragen Sie diese in Tabelle 1: Routen WIN oder Tabelle 2: Routen ZH ein. (Das letzte Byte genügt).

Nehmen Sie an, ein Host im Subnetz Wien sende IP-Pakete an die in Tabelle 3 aufgeführten Ziele im Subnetz Paris (siehe Abbildung 1).
pp steht für das standortspezifische dritte Adressbyte vom Netz Paris: also WIN *pp*=16 / ZH *pp*=18.

- Tragen Sie in Tabelle 3 die Namen der Router ein, die ein Paket auf seinem Weg passiert.

Ziele	160.85.*pp*.75	160.85.*pp*.171	160.85.*pp*.219	160.85.*pp*.236	160.85.*pp*.252
1. Hop	Wien	Wien	Wien	Wien	Wien
2. Hop	Paris	Genf	Genf	Genf	Genf
3. Hop		Paris	Paris	Bern	Bern
4. Hop				Paris	Wien
5. Hop					Genf
6. Hop					Bern

Tabelle 3: Vorbereitung - Traces von Wien nach Paris

Q01 *Welche besondere Situation liegt bei der letzten Ziel-IP-Adresse vor?*

Loop

2.2 Vorbereitung zu Paketgrössen

- Beantworten Sie die folgenden Fragen zum Ping-Befehl unter Linux:

Q02 *Wie sind die Request-Pakete aufgebaut, die der ping-Befehl sendet (siehe auch 1. Versuch zu OSI)?*

ICMP-Header, gefolgt vom Echo Request Payload

Q03 *Die Option **-s packetsize** erlaubt die Angabe der Daten-Bytes. Wie gross darf der Wert von **packetsize** maximal sein, damit eine bestimmte MTU (z.B. 600) nicht überschritten wird?*

MTU - Header 600 - 20 - 8 = 572

Q04 *Wofür steht die Abkürzung MTU?*

maximum transmission unit

Q05 *Gibt die MTU die maximale Grösse eines Frames (Layer 2) an oder die maximale Paketgrösse (Layer 3)?*

Paketgrösse

Q06 *Mit der Option **-M do** und **-M dont** kann die Fragmentierung der Ping-Pakete gesteuert werden. Welche Option verhindert die Fragmentierung?*

-M do

3 Versuchsdurchführung: Forwarding

Jede Bankreihe des Praktikumraums verfügt über je einen Anschluss in den Subnetzen Paris und Wien. Host A übernimmt die Empfängerseite im Subnetz Paris und bekommt mehrere IP-Adressen zugewiesen gemäss Tabelle 4. Der Host B ist der Sender und kommt ins Subnetz Wien.

- Trennen Sie alle PCs vom Schulnetz (lan1) und verbinden Sie lan2 von Host A mit dem Subnetz "Paris" (linker Arbeitsplatz) und lan2 von Host B mit dem Subnetz „Wien" (rechter Arbeitsplatz).
- Um Störungen zu vermeiden, schalten Sie lan1 ab, entfernen alle Adressen und Routen:

```
ip link set dev lan1 down
ip address flush dev lan1
ip route flush dev lan1
```

- Konfigurieren Sie die Netzwerkkarte lan2 des Hosts B für das Subnetz „Wien"; wobei gilt:
  ww wählen Sie entsprechend dem Standort: WIN=17, ZH=19
  aa setzen Sie gleich der Arbeitsplatznummer+10 (Beispiel für Arbeitsplatz 5 in ZH → 160.85.19.15)

```
ip address flush dev lan2
ip address add 160.85.ww.aa/24 broadcast + dev lan2
ip route add default via 160.85.ww.1
```

- Testen Sie die Konfiguration durch ein Ping zum Router Paris (WIN: 160.85.16.1, ZH: 160.85.18.1).
- Konfigurieren Sie lan2 von Host A mit den folgenden Adressen im Subnetz Paris.
  pp wählen Sie entsprechend dem Standort: WIN=16, ZH=18.
  Das vierte Adress-Byte wird wie angegeben berechnet, wobei *gg* Ihre Gruppennummer ist.

```
ip address flush dev lan2
ip address add 160.85.pp.64+gg/24 broadcast + dev lan2
ip address add 160.85.pp.160+gg/24 broadcast + dev lan2
ip address add 160.85.pp.208+gg/24 broadcast + dev lan2
ip address add 160.85.pp.225+gg/24 broadcast + dev lan2
ip address add 160.85.pp.241+gg/24 broadcast + dev lan2
ip route add default via 160.85.pp.1
```

- Testen Sie die Konfiguration durch ein Ping zum Knoten B.

3.1 Direktes Versenden / Adressauflösung

- Betrachten Sie die ARP-Caches der Hosts A und B und löschen Sie diese anschliessend.

```
ip neighbour show
ip neigh flush dev lan2
ip neigh show
```

- Machen Sie einen Datentransfer (`ping -c 4 <IP-von-HostA>`) vom Host B zum Host A. Beobachten Sie auf beiden Hosts die Netzwerkaktivität mit Wireshark.
- Schauen Sie sich die ARP-Caches der beiden Hosts nochmals an.

Q07 *Wessen Einträge sind in den ARP-Caches jetzt vorhanden?*

Host A: ...16.1
B: ...17.1

Q08 *Welche ARP-Meldungen sehen Sie mit Wireshark auf Host B? Wer hat diese Adressauflösung initiiert?*

Who has ...17.12 tell ...17.1
Who has ...17.1 tell ...17.12

Q09 *Welche ARP-Meldungen sehen Sie mit Wireshark auf Host A? Wer hat diese Adressauflösung initiiert?*

Who has ..16.65 tell ...16.1
Who has ...16.1 tell ..16.65

Q10 *Wo (zeitlich) stehen die ARP-Pakete in Bezug auf die ausgehenden ICMP-Pakete, die die Hosts generieren?*

1. vorher
2. nachher

Q11 *Warum gibt es nur vor dem ersten ping-Befehl eine Adressauflösung?*

wird im ARP-cache gespeichert

Der Befehl arping erlaubt das manuelle Versenden eines ARP-Requests. Der arping Befehl muss auf normalen Linux Systemen als super user (`sudo arping address`) ausgeführt werden.

- Testen Sie auf dem Host B mit arping die Erreichbarkeit des Routers Wien und vom Host A.

Q12 *Warum sind nicht beide erreichbar (obwohl beide Router mit dem normalen ping-Befehl erreichbar sind)?*

network interface nicht explizit definiert

- *Worin besteht der Unterschied zwischen dem arping- und den normalen ping-Befehl?*

anderes Layer (Data Link)

3.2 IP-Forwarding

- Verfolgen Sie mit dem Befehl `traceroute` die Pfade von Host B zu den Zieladressen in Tabelle 4 (gleiche Adressen wie oben für Host A) und tragen Sie die angezeigten IP-Adressen der Hops ein.
  `traceroute -n address`

	Zieladressen im Netz Paris (WIN *pp*=16, ZH *pp*=18)				
	160.85.*pp*.64+*gg*	160.85.*pp*.160+*gg*	160.85.*pp*.208+*gg*	160.85.*pp*.225+*gg*	160.85.*pp*.241+*gg*
1. Hop	10.5.1.5 W-P	W-B ... 9	W-G ... 17	W-G ... 17	W-G ...17
2. Hop		B-P ... 2	G-P ... 13	G-B ... 21	G-B ... 21
3. Hop				B-P ... 2	B-W ...10
4. Hop					...17
5. Hop					...21
6. Hop					...10

Tabelle 4: Messung - Traces von Wien nach Paris

...

Q13 *Gibt es Abweichungen (Route und im Informationsgehalt) zwischen Tabelle 3: Vorbereitung - Traces von Wien nach und Tabelle 4: Messung - Traces von Wien nach Paris?*

Ja, Nr. 2 geht via Bern und nicht via Genf

- Senden Sie ein Ping an die letzte IP-Adresse von Host A (160.85.*pp.241+gg*).

Q14 *Was bedeutet die Antwort, die der Ping empfängt?*

time to live exceeded
packet has travelled through too many routers

Zeigen Sie diese Resultate dem Praktikumsleiter.

4 MTU Path Discovery

- Finden Sie manuell die maximale MTU des Pfads von Wien via Genf nach Paris, in dem Sie die Fragmentierung verhindern (Parameter `-M do`) und die ICMP-Paket-Grösse schrittweise reduzieren (mit `-s` *packetsize* ausgehend von 1400).
  `ping -s packetsize -M do <Ziel-IP>`

Q15 *Welche Ziel IP-Adresse müssen Sie von Router Wien aus «anpingen»?*

...16.209

Q16 *Wie gross ist die MTU?*

Packetsize 572 → MTU 600

- Untersuchen Sie im Wireshark die auf Host B empfangenen ICMP-Pakete (z.B. bei `-s` 1400):

Q17 *Welchen eleganteren Weg gibt es, um die Path-MTU zu bestimmen?*

MTU of next hop:

- Die MTU Path Discovery bestimmt die kleinste MTU auf einem Pfad. Sie ist in heutigen Linux-Distributionen standardmässig eingeschaltet, wurde aber im KT-Labor ausgeschaltet. Schalten Sie diese auf Host B wieder ein. Sie benötigen dafür Privilegien.

```
sudo su
echo 0 > /proc/sys/net/ipv4/ip_no_pmtu_disc
echo 10 > /proc/sys/net/ipv4/route/mtu_expires
```

- Senden Sie vom Host B aus mindestens 20 ICMP-Pakete mit gesetztem Don't-Fragement-Bit («ping» mindestens 20 Sekunden laufen lassen) und beobachten Sie die Fehlermeldungen auf der Konsole sowie die Aufzeichnung im Wireshark.
  `ping -s 1400 -M do <Ziel-IP>`

Q18 *Welche beiden Fehlermeldungen gibt das Programm* ping *aus? Auf welchem Gerät wurde der Fehler, der die jeweilige Fehlermeldung zur Folge hat, ausgelöst? Wie passt das zu den Paketen, die in Wireshark aufgezeichnet wurden??*

From 10.5.1.17 ... frag needed and DF set (mtu=600)

local error: message too long, mtu=600

- Zeigen Sie diese Resultate dem Praktikumsleiter.