08 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
- IP-Fragmentierung und Reassembly
- 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:

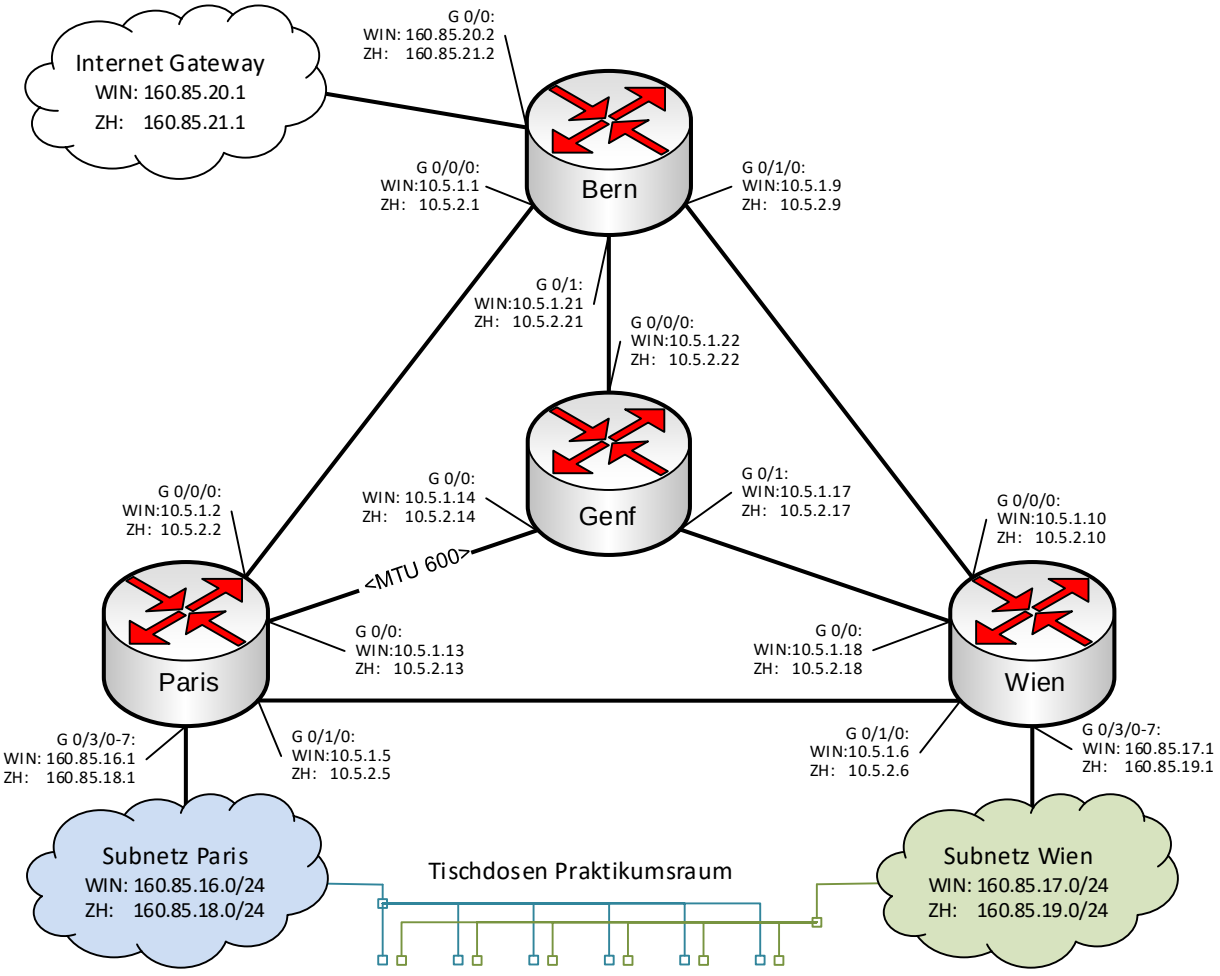

Abbildung 1: IP-Netzwerk des KT-Praktikums

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	
160.85.16.0	/24	via 10.5.1.2	
160.85.17.0	/24	via 10.5.1.10	
160.85.20.0	/24	direct, G 0/0	
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	
160.85.16.0	/24	direct G 0/3/0-7	
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	
160.85.17.0	/24	via 10.5.1.18	
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	
160.85.16.192	/26	via 10.5.1.17	
160.85.17.0	/24	direct, G 0/3/0-7	
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					
2. Hop					
3. Hop					
4. Hop					
5. Hop					
6. Hop					

Tabelle 3: Vorbereitung - Traces von Wien nach Paris

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

2.2 Vorbereitung zu Fragmentierung

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

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

---

*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?*

Wofür steht die Abkürzung MTU?

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

---

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

---

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 (eth0) und verbinden Sie eth1 von Host A mit dem Subnetz "Paris" (linker Arbeitsplatz) und Host B mit dem Subnetz „Wien" (rechter Arbeitsplatz).
- Um Störungen zu vermeiden, schalten Sie eth0 ab, entfernen alle Adressen und Routen:

```
ip link set dev eth0 down
ip address flush dev eth0
ip route flush dev eth0
```

- Konfigurieren Sie die Netzwerkkarte eth1 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 eth1
ip address add 160.85.ww.aa/24 broadcast + dev eth1
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 eth1 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 eth1
ip address add 160.85.pp.64+gg/24 broadcast + dev eth1
ip address add 160.85.pp.160+gg/24 broadcast + dev eth1
ip address add 160.85.pp.208+gg/24 broadcast + dev eth1
ip address add 160.85.pp.225+gg/24 broadcast + dev eth1
ip address add 160.85.pp.241+gg/24 broadcast + dev eth1
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 eth1
ip neigh show
```

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

Wessen Einträge sind in den ARP-Caches jetzt vorhanden?

A: 160.85.18.1 dev eth1 STALE
B: 160.85.19.1 dev eth1 STALE

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

Host B
Who has 160.85.19.1

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

Host B
"Who has …"

Wo (zeitlich) stehen die ARP-Pakete in Bezug auf die ICMP-Pakete des Ping-Befehls?

Die ARP Pakete werden vor den ICMP Paketen abgeschickt

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

Danach ist es in der ARP-Cache gespeichert

Der Befehl arping erlaubt das manuelle Versenden eines Ping-Requests.

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

Warum sind nicht beide erreichbar (obwohl der normale ping geht)?

Nur lokal

- *Besteht der Unterschied vom arping- und den normalen ping-Befehl?*

arping nur ARP-request

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` pp = 18 gg = 8

	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	160.85.19.1	160.85.19.1	160.85.19.1	160.85.19.1	160.85.19.1 10.5.2.17
2. Hop	10.5.2.5	10.5.2.9	10.5.2.17	10.5.2.17	10.5.2.21 10.5.2.10 10.5.2.17
3. Hop	160.85.18.72	10.5.2.2	10.5.2.13	10.5.2.21	10.5.2.21 10.5.2.10
4. Hop		160.85.18.168	160.85.18.216	10.5.2.2	10.5.2.17 10.5.2.21 10.5.2.10
5. Hop				160.85.18.233	10.5.2.17 10.5.2.21
6. Hop					10.5.2.10 10.5.2.17 bis TTL = 0

Tabelle 4:Messung - Traces von Wien nach Paris

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

Nein

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

Was bedeutet die Antwort, die der Ping empfängt?

Das Paket ist zu lange im Netzwerk

- Zeigen Sie diese Resultate dem Praktikumsleiter.

4 Versuchsdurchführung: Fragmentierung

- Falls nicht bereits erfolgt, konfigurieren Sie Host A im Subnetz Paris mit folgender Adresse: *160.85.pp.208+gg*, wobei *gg* für die Nummer der Gruppe/Bankreihe steht.
- Starten Sie Wireshark auf den beiden Hosts A sowie B. Deaktivieren Sie auf Wireshark automatische Reassemblierung (Edit→Prefs→Protocols→IPv4→Reassemble fragmented IPv4 datagrams = Off).
- Senden Sie vom Host B im Subnetz Wien ein ICMP-Paket an den Host A im Subnetz Paris wie folgt:
  `ping -s 1400 -M dont 160.85.pp.208+gg`
- Betrachten Sie die auf Host A eingehenden Fragmente. Tragen Sie die Anfangsposition und Länge der Daten in Tabelle 5 (eine Zeile pro Fragment):

	0	200	400	600	800	1000	1200	1400	1600
1		290							
2				610					
3		290							
4				610					
Beispiel:			400						

360

Tabelle 5

- *Wer hat warum die obigen Fragmente erzeugt?*

Der Router da wir Fragementierung zugelassen haben

- Senden Sie von Host B ein ICMP-Paket mit dem folgenden Befehl und vergleichen Sie die Fehlermeldung auf der Konsole mit der ICMP Meldung (Wireshark).
  `ping -s 1400 -M do 160.85.pp.208+gg`

Was bewirkt der Parameter **`-M do`** *und welche Auswirkung hat er?*

Fragementierung wird nicht mehr zugelassen, dadurch kann nichts mehr übermittelt werden

- Versuchen Sie nun dasselbe mit einem etwas längeren ICMP-Paket:
  `ping –s 1500 –M do 160.85.pp.1`

Wer erzeugt die angezeigte Meldung? Worin unterscheidet sich der Verkehr auf dem Netz?

der Router "Message too long"
Es kommt bei Host A keine Pakete an

Wie können Sie die MTU des Interfaces eth1 abfragen und bestimmen?

ifconfig

Warum ist oben eine Fragmentierung notwendig, obwohl die MTU und die Ping-Size beide 1500 sind?

Header wird auch dazu gezählt

Bis zu welchem maximalen Wert des Parameters **`–s`** *funktioniert der Befehl? Stimmt dies mit Ihrer Vorbereitung überein?*

1472

- Zeigen Sie diese Resultate dem Praktikumsleiter.

5 Zusatzaufgaben: 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 160.85.pp.208+gg`

Wie gross ist die MTU?

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

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

- 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 aus dem Subnetz Wien (Host B) ein ICMP-Paket mit folgendem Befehl und vergleichen Sie die empfangenen Fragmente mit Tabelle 5.

`ping -s 1400 -M want` ***160.85.pp.208+gg***

	0	200	400	600	800	1000	1200	1400	1600
1									
2									
3									
4									

Was bewirkt **`-M want`** *und worin besteht der Unterschied zur ersten Messung in Tabelle 5?*

- Senden Sie vom Host B aus dem Subnetz Wien ein ICMP-Paket mit gesetztem Don't-Fragement-Bit und beobachten Sie die Fehlermeldung auf der Konsole sowie die Aufzeichnung im Wireshark.

  `ping -s 1400 -M do` ***160.85.pp.208+gg***

Wer hat nun diese Fehlermeldung erzeugt? Was geschieht auf dem Netz?

- Zeigen Sie diese Resultate dem Praktikumsleiter.