Übungsblatt 05 – Netzwerkgrundlagen

Aufgabe A – Umsetzung des Routings

Setzen sie das aus der Planung hervorgegangene Netzwerk (bzw. die Netzwerke) mit den ihn bekannten Tools um.
Ihre Netzwerke bestehen aus mindestens drei VMs (Fünf VMs wäre optimal). Optimal sollten zwei VMs im Netzwerk *A* und *B* sein – also ein minimales *freeBSD* und ein Linux je LAN. Zwischen beiden Netzwerken „sitzt“ der Router (*freeBSD* mit GUI).

1. **Für die Hosts:**

   a) Bevor sie das Netzwerk umsetzen: Legen sie fest welche Netzwerkadapter zu welchem Netzwerk gehören! Ordnen sie entsprechend den Adaptern den Netzwerken zu.

   b) Wie in der vorigen Übung: Legen sie zu jedem Adapter IPv4 Adresse und Subnetzmaske fest. Die Netze sollten minimal sein!

   c) Überprüfen sie, ob auf allen Adaptern die für das statische Netzwerk der *DHCP*-Dienst ausgeschaltet ist.

   d) Setzen sie für alle benötigten Adapter die gewählten IPv4 Adressen und Subnetzmasken.

   e) Aktivieren sie die Netzwerkadapter und überprüfen sie, ob VMs innerhalb eines LANs sich bereits erreichen können.

   f) Lassen sie sich die aktuelle Routing-Tabelle anzeigen. Welche Informationen entnehmen sie dieser?

   g) Fahren sie mit der Konfiguration des Routers fort.

   h) Nachdem sie den Router aufgesetzt haben:

      i. Tragen sie auf den Hosts entsprechende Routen ein!

      ii. Überprüfen sie, ob sich die VMs über das LAN hinaus erreichen.

2. **Für den Router:**
   Der Router benötigt eine etwas andere Konfiguration.

   a) Wie bei den Hosts auch benötigt ihr Router IP-Adressen. Für jeden Adapter mindestens eine Adresse samt Subnetzmaske.

   b) Konfigurieren sie die Adapter des Routers mit IP-Adresse und Subnetzmaske.

   c) Der Router sollte anschließend alle Rechner erreichen können. Andersherum sollte natürlich alle VMs den gemeinsamen Router erreichen können.

   d) Aktivieren sie das Forwarding auf dem Router, sodass Pakete aktiv weitergeleitet werden können.

3. Sie können mithilfe eines kleine Chats testen, ob Pakete tatsächlich auf dem Router ankommen. Mithilfe des Tools *netcat* kann getestet werden, ob Pakete im anderen Netzwerk ankommen. Beide Seiten nutzen das Tool *netcat – nc*. Das Listing **??** zeigt die Seite des Servers, dieser Code stellt den Server bereit. Der Client darf sich anschließend mithilfe eines *Sockets (Tupel aus IP-Adresse und Port)* verbinden (s. Listing **??**).

```
#Server port > 1024
nc -l -p <port_number> <ip_of_server>
#example
nc -l -p 4711 10.0.0.1
```

```
#Client
nc <ip_of_server> <port_number>
#example
nc 10.0.0.1 4711
```

4. **Alternativ:** Wenn sie bereits mit Wireshark gearbeitet haben, können sie auch dies benutzen, um festzustellen, ob die Pakete korrekt ankommen.

5. **Router: Uplink**
   Alle VMs sollten sich nun erreichen können. Rechner außerhalb dieser Netzwerke können sie wahrscheinlich noch nicht erreichen. Beispielsweise Maschinen im Internet.

   a) Schauen sie sich die Routing-Tabellen des Routers und der Hosts an. Welche Informationen können sie diesen entnehmen? Welche Art Routen haben sie gesetzt?

   b) Muss am Router eine Anpassung der Routing-Tabelle vorgenommen werden, so das dieser Rechner außerhalb des Netzes erreicht?

   c) Falls ihre Hosts keine Default-Route haben, welcher Rechner wäre als Default-Gateway sinnvoll? Setzen sie in der Routing-Tabelle entsprechende Routen.

   d) Falls ihr Router noch keiner Rechner außerhalb des Netzes erreichen kann:

      i. Hat ihr Router ein Default-Gateway? Falls nein, welcher Rechner wäre das passende Gateway?

   e) Setzen sie für den Router eine Default-Route, sodass sie Rechner außerhalb des Netzes erreichen können.

   f) Überprüfen sie, ob sie Rechner außerhalb erreichen können!

      i. Versuchen sie Rechner innerhalb ihres physischen LANs via IP-Adresse zu erreichen – bspw. Smartphone, Toaster etc. Die IP-Adressen können sie entweder über den Router oder das Gerät selbst in Erfahrung bringen. Sie können auch die Werkzeuge *arp-ping*, *arp-scan* oder *nmap* nutzen.

ii. Versuchen sie einen Rechner des Internets via IP-Adresse zu erreichen (bspw.: 1.1.1.1).

iii. Versuchen sie einen Rechner des Internets über seinen Domainnamen zu erreichen (bspw. htw-berlin.de)

6. Da ihre einfachen Hosts wahrscheinlich noch keine Rechner außerhalb des LANs erreichen können, muss der Router nun um eine *NAT*-Funktionalität erweitert werde. Der Router muss neben dem Forwarding die Option des NAT-Gateways spendiert bekommen. Diese muss in der `/etc/rc.conf` bereitstehen. Tragen sie die *NAT*-Option ein. Legen sie hier ebenfalls das Interface für *NAT* fest. Es müssen keine speziellen *NAT*-Flags gesetzt werden.

7. Da wir *NAT* nutzen, muss die Firewall entsprechend gesetzt werden. Sie können entweder *pf* oder die Standard-Firewall nutzen.
   - Allgemein: https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/firewalls.html
   - Für *pf*: https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/firewalls-pf.html
   - Für *IPFW*: https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/firewalls-ipfw.html Abschnitt 30.4.4 In-Kernel NAT

8. Prüfen sie erneut, ob ihre VMs ohne grafische Oberfläche Rechner via IP-Adresse außerhalb des LANs, ihres Heimnetzes und des Internets erreichen können.

9. Konfiguration der *resolv.conf*

   a) Wahrscheinlich könnten ihre Hosts noch keine Rechner über den Domainnamen erreichen. Daher müssen sie diese noch konfigurieren. Tragen sie alle notwendigen Einträge in die Datei `/etc/resolv.conf` ein. Lesen sie entsprechend hier nach: https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/configtuning-configfiles.html

   b) Überprüfen sie, ob sie nun Rechner auch via Domainnamen ansprechen können.

Aufgabe B – IPv6

Da *IPv4* ein etwas betagteres Protokoll ist und sie fit für die Zukunft sein sollen, sollen sie abschließend ihr Netzwerk mittels *IPv6* umsetzen. Da *IPv6* eine wesentlich größere IP-Range besitzt ist in der Nachfolgenden Tabelle ein mögliches Adressschema aufgezeigt. Auch hier gilt: *IPv6* hat mehr Adressen, dies sollte sie jedoch nicht dazu verleiten verschwenderisch damit umzugehen!

	Netzwerk 1	**Netzwerk 2**
Prefix/L	fd	fd
Global ID	0da5a0170a	ac26d7d170
Subnet ID	5fd7	f78c
Combined/CID	fd0d:a5a0:170a:5fd7::/64	fdac:26d7:d170:f78c::/64
IPv6 addresses	fd0d:a5a0:170a:5fd7:xxxx:xxxx:xxxx:xxxx	fdac:26d7:d170:f78c:xxxx:xxxx:xxxx:xxxx

Sie sollen im Folgenden ein statisches *IPv6*-Netzwerk umsetzen. Ein Routing außerhalb ihrer lokalen Infrastruktur ist kein muss, da es immer noch Anbieter (oder Hardware) gibt, die keinen *IPv6* unterstützt.

1. Adaptieren sie ihren *IPv4*-Netzwerkaufbau auf *IPv6*. D.h. der grundsätzliche Aufbau des Netzwerkes soll nicht verändert werden. Sie fügen den Adaptern lediglich *IPv6*-Adressen hinzu.

2. Vergeben sie in ihrem Netzwerk entsprechende Adressen. Vergessen sie nicht entsprechende Adressen für den Router zu setzen.

3. Tragen sie für alle Teilnehmer entsprechende Routen ein.

4. Denken sie daran das Forwarding für IPv6 zu aktivieren!

5. Testen Sie Ihre Netzwerke mit *ping6*.

6. Falls ihr lokale Infrastruktur es zulässt, können sie auch ein Default-Gateway konfigurieren, sodass die VMs via *IPv6* ins Internet kommen.

7. Müssen sie Einträge in ihre *resolv.conf* ändern? Falls ja: Ändern sie dies entsprechend.