Übungsblatt 04 – Backbone Routing

Im Anschluss der letzten beiden Übungsblättern sollen Sie nun vorbereitend Ihr erstes komplexeres Netzwerk umsetzen. Die kleinen Separaten Netzwerke der letzten Laborübung sollen verknüpft werden und darüber hinaus sollen Sie für einen Anschluss an das Internet sorgen (der sogenannte Uplink). Im wesentlich wird ein solches Netzwerk auch als Backbone-Netzwerk beschrieben. Backbone-Routing wird auch an den großen Internet-Knoten umgesetzt (diese werden als Internet-Exchange-Point – IXP bezeichnet), wie etwas dem *DECIX* (https://www.de-cix.net/).
Wie Sie sehen können Sie nach nur drei Übungen schon einiges an Know-How vorweisen.
Inhalt:

- Routing & Backbone-Routing
- Planung eines komplexeren Netzwerkes mithilfe von Linux-Routern (Cisco gerne auf Anfrage!)
- Erweiterung der Tools für Netzwerkadministration
- *ip-tables*

Hilfreiche Links (gründlich lesen, kein einfaches Copy & Paste!):

- https://en.wikipedia.org/wiki/Domain_Name_System
- https://en.wikipedia.org/wiki/Iptables
- https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/
- https://www.digitalocean.com/community/tutorials/how-to-forward-ports-through-a-linux
- https://serverfault.com/questions/326493/basic-iptables-nat-port-forwarding

Aufgabe A – Planung des Netzwerkes

Wie in der letzten Übung arbeiten Sie zunächst in Gruppen von je vier Studierenden.
Bis dato sollten die Knoten Ihre beiden Netzwerke untereinander kommunizieren können. Dieser Aufbau soll nun so erweitert werden, dass Ihre Netzwerke (d.h. Ihre Bankreihe) mit den Rechnern der anderen Bankreihe kommunizieren können. Im wesentlichen kennen Sie also schon den Aufbau, Ihr Netzwerk bekommt lediglich einen extra Router. [1] Das Netzwerk soll im wesentlichen dem in Abb. 1 entsprechen.

[1] auch hier gilt: wenn genug Raspberry Pis vorhanden sind, können auch dedizierte Rechner als Router genutzt werden.

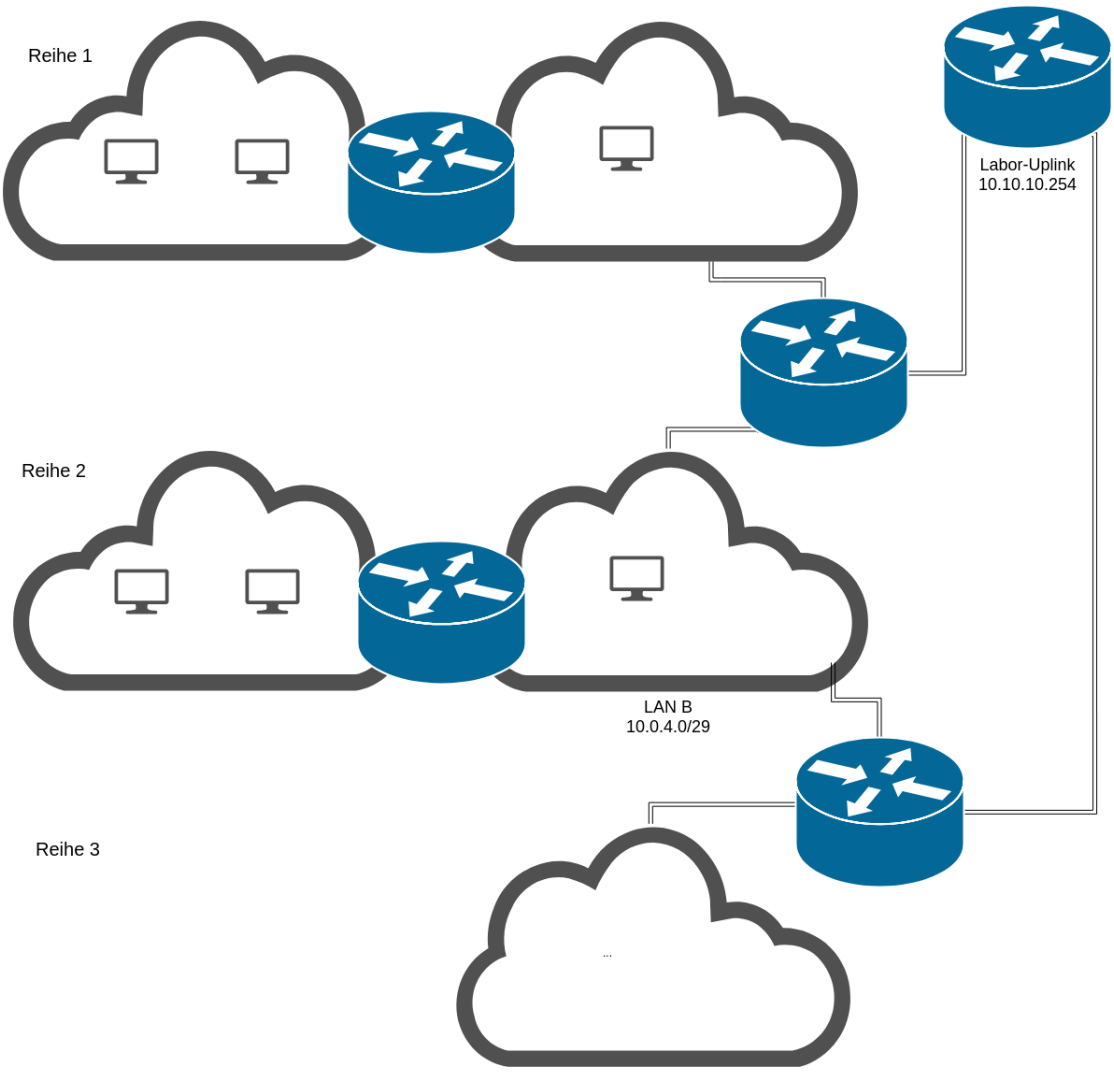

Abbildung 1: Skizze des Netzwerkes bestehend aus fünf Bankreihen á zwei LANs, sowie den Backbone-Routern

Folgendes Adressschema gilt:

Tabelle 1: Adressschema für das Labor

	IP || IP-Range
$LAN_{A\|B}$	10.0.$X_{\alpha\|\beta}$.Y/Size
Backbone	10.10.10.100 + ρ
Labornetz	10.0.0.0/8
Uplink	10.10.10.254
DNS	10.10.10.254

a.) Planen Sie entsprechend der Skizze Ihr Netzwerk. D.h. planen Sie entsprechende IP-Adressen, Subnetzmasken und Router ein.

b.) Skizzieren Sie Ihre lokalen Netzwerke, sowie das gesamte Netzwerk mitsamt der Router (Nutzen Sie geeignete Symbole).

c.) Planen Sie ebenso den Backbone-Router, sowie den Uplink (Router im Rack – Zugang zum DFN(Internet) ein.

Aufgabe B – Tools

1.) Zwei weitere bekannte Netzwerkanalyse-Tools sind *netstat* (*net-tools*) und *ss* aus der *iproute2* Werkzeugsammlung.

a.) Recherchieren Sie die wesentliche Funktionen von *netstat*, sowie *ss*.

b.) Notieren Sie sich anhand von Beispielen die Syntax der eben genannten Tools.

2.) *iptables* sind unter Linux allgemein als Firewall-Tool bekannt. [2] In der kommenden Übung übernimmt iptables eine etwas andere Aufgabe. Es sorgt zunächst dafür, dass unsere Raspberry Pis via *NAT*[3] Pakte in das Internet routen können.

a.) Recherchieren Sie mithilfe folgenden Links was *NAT* ist und warum dies unter *IPv4* genutzt werden muss.
https://en.wikipedia.org/wiki/Network_address_translation

b.) Machen Sie sich im groben klar, wie *NAT* umgesetzt wird.

c.) **Fakultativ:** Mit sehr hoher Wahrscheinlichkeit nutzt auch Ihr Router/Modem *NAT*, wie wird dies hier umgesetzt?

d.) Recherchieren Sie was unter einer Firewall im wesentlichen verstanden wird.

e.) Machen Sie sich klar, wie im Groben dies vonstatten geht.

f.) *iptables* kann genutzt werden, um die privaten Adressen auf öffentliche zu übersetzen. Lesen Sie folgenden Artikel:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s1-firewall-ipt-fwd.html
Versuchen Sie den Inhalt wirklich komplett zu verstehen. Notieren Sie sich alle notwendigen Schritte um das Masquerading via ip-tables einzuschalten.

g.) *iptables* unterstützt sowohl *SNAT* als auch *DNAT*. Recherchieren Sie kurz worin sich beider Arten unterscheiden.

[2] Mehr zu Firewalling in der IT-Security Übung.
[3] Um genau zu sein: SNAT