Linux Networking

Markus Gachnang und Martin Sprecher

25. September 2020

Inhaltsverzeichnis

1 Ausgangslage

2 Kochbuch

It is expected of you to hand in a step-by-step cookbook for the whole final setup. Explain important commands and reason your decisions. We should be able to fully retrace what you did to be able to assess your work. One cookbook is expected per group.

2.1 General

Change the password ... Also, change the hostname to the name given in LTB.

Wir verbinden uns auf jeden Container und ändern den Inhalt der Datei `/etc/hostname` auf den Namen des Containers. Dafür benützen wir `sudo nano /etc/hostname`, ändern den Namen und speichern mit Ctrl-O und beenden nano mit Ctrl-X. Zusätzlich rufen wir `sudo hostname <newHostName>` auf.
Wird setzten das Passwort des jeweiligen Containers auf seinen Namen mit `sudo passwd ins`.

2.2 IP Address Assignment

Use Netplan to assign the ip addresses to the interfaces. ...

Name	IP
Client	ENS2: 172.16.0.2
R1	ENS2: 172.16.0.1 ENS3: 10.0.1.1
R2	ENS2: 10.0.1.2 ENS3: 10.0.4.1 ENS4: 10.0.2.1
R3	ENS2: 10.0.2.2 ENS3: 10.0.5.1 ENS4: 10.0.3.1
R4	ENS2: 10.0.4.2 ENS3: 10.0.5.2 ENS4: 10.0.100.1
R5	ENS2: 10.0.3.2 ENS3: 192.168.1.1
Server	?: 192.168.1.100
MITM	ENS2: 10.0.100.2

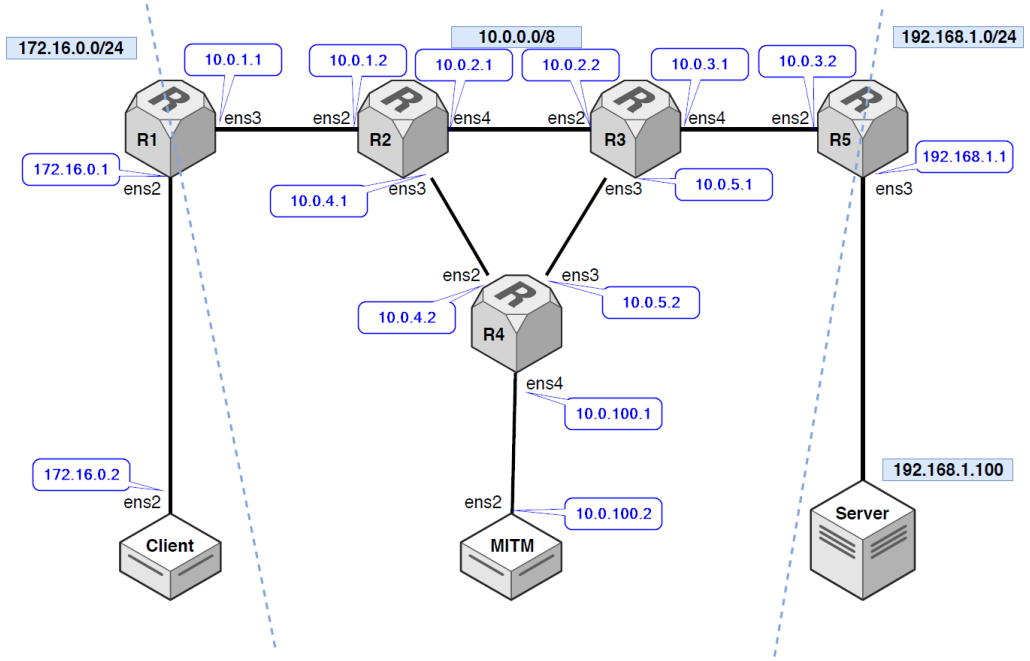

Abbildung 1: Netplan

Die Adressen sind so definiert, dass jede Verbindung ein eigenes Subnet hat. Bird sucht seine Nachbarn anhand des Broadcasts.
Wir ändern den netplan mit `sudo nano /etc/netplan/50-cloud-init.yaml`.

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    version: 2
    ethernets:
        ens2:
            dhcp4: false
            addresses: [172.16.0.1/24]
        ens3:
          dhcp4: false
          addresses: [10.0.1.1/24]
```

Listing 1: /etc/netplan/50-cloud-init.yaml on R1

Mit `netplan apply` übernehmen wir die neu definierten IP-Adressen.

2.3 BIRD

Now, your routers must run OSPF. ...

- OSPFv2 must run on the routers.
- Find a way to protect the CPU from too much OSPF processing.
- A restart of BIRD should not result in lost routes.

Wir definieren die Configuration von Bird indem wir "/etc/bird/bird.conf" anpassen.

2.4 IP Forwarding

"IP-Forwarding" ist standartgemäs ausgeschaltet. Mit `sysctl net.ipv4.ip_forward=1` aktivieren wird das weiterleiten der Packete erlaubt.

2.5 Script

Da wir keine Ahnung von "Bird" hatten, wurde das Anpassen und Testen der Configuration aufwendig, weshalb wir kurzer Hand ein Script erzeugten, welche die zuvor definierten Einstellungen anwendet:

```
#!/bin/bash

setup_hostname()
{
    echo "Set hostname to $1"
    echo "$1" > '/etc/hostname'
    hostname $1
}

setup_ip()
{
    echo "Setup netplan"
    cat <<EOF > '/etc/netplan/50-cloud-init.yaml'
# This file is generated from information provided by $0
# Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    version: 2
    ethernets:
EOF
    if [ $# -ge "1" ]; then
        echo " ens2 = $1"
        cat <<EOF >> '/etc/netplan/50-cloud-init.yaml'
        ens2:
            dhcp4: false
            addresses: [$1]
EOF
    fi
    if [ $# -ge "2" ]; then
        echo " ens3 = $2"
        cat <<EOF >> '/etc/netplan/50-cloud-init.yaml'
        ens3:
            dhcp4: false
            addresses: [$2]
EOF
    fi
    if [ $# -ge "3" ]; then
        echo " ens4 = $3"
        cat <<EOF >> '/etc/netplan/50-cloud-init.yaml'
        ens4:
            dhcp4: false
            addresses: [$3]
EOF
    fi
}

setup_bird()
{
    echo "Setup bird"
    cat <<EOF > '/etc/bird/bird.conf'
# This file is generated from information provided by $0
# Please refer to the documentation in the bird-doc package or BIRD User's
# Guide on http://bird.network.cz/ for more information on configuring BIRD
    and
# adding routing protocols.

# log "/var/log/bird.log" all;
log syslog { info, remote, warning, error, auth, fatal, bug };
```

```
60
61 # Change this into your BIRD router ID.
62 router id $1;
63
64 # The Device protocol is not a real routing protocol. It doesn't generate
       any
65 # routes and it only serves as a module for getting information about
       network
66 # interfaces from the kernel.
67 protocol device {
68     scan time 1; # Scan interfaces every 10 seconds
69 }
70
71 # The Kernel protocol is not a real routing protocol. Instead of
       communicating
72 # with other routers in the network, it performs synchronization of BIRD's
73 # routing tables with the OS kernel.
74 protocol kernel {
75     metric 64;       # Use explicit kernel route metric to avoid collisions
76                      # with non-BIRD routes in the kernel routing table
77     persist;         # Don't remove routes on BIRD shutdown
78     scan time 20;    # Scan kernel routing table every 20 seconds
79     import none;
80     export all;      # Actually insert routes into the kernel routing table
81 }
82
83
84 protocol rip {
85     export all;
86     import all;
87     interface "*";
88 }
89
90 protocol static {
91         import all;
92
93 EOF
94
95     for var in "$@"
96     do
97         echo " $var"
98         if [ "$var" != "$1" ]; then
99             echo "         route $var;" >> '/etc/bird/bird.conf'
100        fi
101    done
102
103    cat <<EOF >> '/etc/bird/bird.conf'
104 }
105
106 protocol ospf {
107     tick 1;        # The routing table calculation and clean-up of areas'
           databases is not performed when a single link
108                    # state change arrives. To lower the CPU utilization,
                           it's processed later at periodical intervals of num
109                    # seconds. The default value is 1.
110     import all;
111     #export filter {
112     #         ospf_metric1 = 1000;
113     #         if source = RTS_STATIC then accept; else reject;
114     #};
115
116     area 0 {
117         networks {
118             10.0.0.0/8;
119             172.16.0.0/24;
120             192.168.1.0/24;
```

```
121         };
122
123         interface "ens*" {
124             cost 5;
125             type broadcast;
126             hello 5;
127             retransmit 2;
128             wait 10;
129             dead 20;
130         };
131
132         interface "*" {
133                 cost 1000;
134                 stub;
135         };
136     };
137 }
138
139 EOF
140     sysctl net.ipv4.ip_forward=1
141     ip route flush table main
142     bird -p
143     birdc down
144     # bird -R
145     systemctl start bird
146     birdc show status
147     systemctl status bird
148 }
149
150 setup()
151 {
152     echo "Start setup for '$1'"
153     case $1 in
154         Client)
155             setup_hostname "Client"
156             setup_ip "172.16.0.2/24"
157             echo "            gateway4: 172.16.0.1" >> '/etc/netplan/50-
                    cloud-init.yaml'
158             ;;
159         MITM)
160             setup_hostname "MITM"
161             setup_ip "10.0.100.2"
162             echo "            gateway4: 10.0.100.1" >> '/etc/netplan/50-
                    cloud-init.yaml'
163             ;;
164         R1)
165             setup_hostname "R1"
166             setup_ip "172.16.0.1/24" "10.0.1.1/24"
167             setup_bird "1.1.1.1" "172.16.0.0/24 via \"ens2\""
168             # "10.0.0.0/8 via \"ens3\""
169             ;;
170         R2)
171             setup_hostname "R2"
172             setup_ip "10.0.1.2/24" "10.0.4.1/24" "10.0.2.1/24"
173             setup_bird "2.2.2.2"
174             # "10.0.1.0/24 via \"ens2\"" "10.0.4.0/24 via \"ens3\""
                    "10.0.3.0/24 via \"ens4\""
175             ;;
176         R3)
177             setup_hostname "R3"
178             setup_ip "10.0.2.2/24" "10.0.5.1/24" "10.0.3.1/24"
179             setup_bird "3.3.3.3"
180             #"10.0.2.0/24 via \"ens2\"" "10.0.4.0/24 via \"ens3\""
                    "10.0.5.0/24 via \"ens4\""
181             ;;
182         R4)
```

```
183             setup_hostname "R4"
184             setup_ip "10.0.4.2/24" "10.0.5.2/24" "10.0.100.1/24"
185             setup_bird "4.4.4.4"
186             ;;
187         R5)
188             setup_hostname "R5"
189             setup_ip "10.0.3.2/24" "192.168.1.1/24"
190             setup_bird "5.5.5.5" "192.168.1.0/24 via \"ens3\""
191             # "10.0.0.0/8 via \"ens2\""
192             ;;
193         *)
194             echo "name is unknewn..."
195             exit 1
196             ;;
197     esac
198     netplan apply
199 }
200
201 echo "CldInf Networker"
202 if [ "$EUID" -ne 0 ]; then
203     echo "Please run as root"
204     exit 1
205   elif [ $# -lt "1" ]; then
206     hostname=$(hostname)
207     case $hostname in
208         Client|MITM|R1|R2|R3|R4|R5)
209             setup $hostname
210             ;;
211         *)
212             echo "Usage: $0 <name>"
213             echo " name = Client, MITM, [R1 .. R5]"
214             exit 1
215             ;;
216     esac
217   else
218     setup $1
219 fi
```

Listing 2: /doConfig.sh

3 Verifizierung

Verify your routing implementation. Explain which exact commands you used for each verification step and show how they provide prove that your setup works.

3.1 Route Failover

Verify that your setup works. Prove that a route failover takes place in case ofa route outage. To do that, a well known tool can be used.

3.2 Passive Interfaces

Show that no OSPF packets are sent into the client and server networks,too.`tcpdump` and `tshark` are good tools for that, sniff on the suspicious interfaces and filter for OSPFv2 packets. To be sure that your filter works, sniff on an interface where you expect OSPF-messages, too.

3.3 Access Website

Finally, you must be able to access the webpage from the webserver. You can use `curl` or `wget` for that. The webserver listens on port 8080.

4 Performanz

Provide the measurement before and after the appliance of the `tc` commands.
Provide the exact used `tc` commands.

5 Referenzblatt

We also expect you to hand in a reference sheet for all the net-work commands used in this lab. Just list every command and its function. This reference must not be longer than one page.

Befehl	Funktion
`sudo nano <Pfad>`	Öffnen eines Files im Texteditor
`sudo nano hostname < newHostName>`	Zum ändern des Hostnames
`sudo nano passwd <user>`	Editieren vom passwd file im Terminal
`sudo birdc`	Zum kommunizieren mit einem laufenden BIRD
`sudo birdc show status`	Anzeigen vom router status, BIRD version, Laufzeit und Zeitpunkt von der letzten Rekonfiguration.
`sudo birdc show interfaces`	Anzeigen der Liste von allen Interfaces. Zeigt für jedes Interface, Typ, Status, MTU und die zugewiesene Adresse an.
`sudo birdc show ospf interface`	Anzeigen von detailierten Informationen über die OSPF Interfaces.
`birdc show ospf neighbors`	Anzeigen der Liste mit allen OSPF Nachbaren deren Zustand.
`birdc show ospf state`	Anzeigen von detailierten Informationen über OSPF Bereiche basierend auf der link-state database. Es zeigt die Netzwerk Topolgie, stub Netzwerke, zusammengeführte Netzwerke und Router von anderen Areas und externen Routen. Ausserdem zeigt es erreichbare Netzwerk Knoten an.
`ping -c <num> <ip>`	sendet num mal einen Ping an die ip
`blub`	blob
`blub`	blob
`blub`	blob
`blub`	blob

6 Anhänge

6.1 Routing

- Your delivered report must include the new usernames and pass-words of the hosts.
- Your delivery must contain the created netplan files and an ad-dress plan.
- Attach the BIRD config files to your cookbook and explain how you achieve the minimal requirements.
- Verify your routing implementation. Explain which exact commands you used for each verification step and show how they provide prove that your setup works.

Erarbeitung der BIRD-config ist im 2.3 erläutert. Verifikation der Routing unter 3.

6.2 Firewall

We're interested in the used `nmap` command, where the firewall runs and why you've choosen that location. Print the ruleset of the firewall and attach it to your report.