Laboratory III

Schörghofer Fabian

Reschenhofer Andreas

Course: Netzzuverlässigkeit und Virtualisierung

Lecturer: Mag. DI Ulrich Pache, BSc

13.06.2017

Table of Contents

List of Abbreviations

OSPF Open Shortest Path First

IP Internet Protocol

AS Autonomous System

BGP Border Gateway Protocol

MPLS Multiprotocol Label Switching

VPN Virtual Private Network

VRF Virtual Routing and Forwarding

AS Autonomes System

1 Ausgangslage

Ziel dieser Laboreinheit ist es ein Multiprotocol Label Switching (MPLS)-VPN zu konfigurieren. Dabei soll das ein VPN zwischen den Gruppenteilnehmer aufgebaut werden. Um dies über ein Providernetz zu ermöglichen wird Border Gateway Protocol (BGP) eingesetzt.

2 Topologie

Die Topologie (nachgebaut in Packet Tracer) ist in Abbildung 2.1 zu sehen.

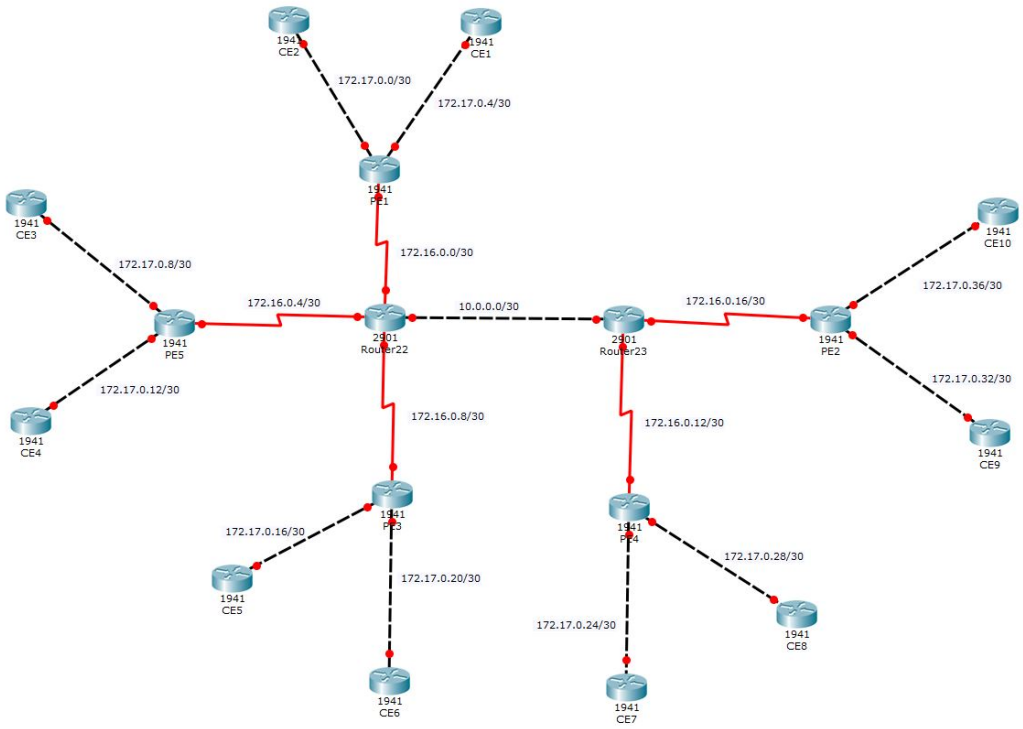

Figure 2.1: Topologie

Jeder Gruppe wurde ein Provider-Edge-Router (PEx) samt zwei Kunden-Routern (CEx) zugewiesen. Der Traffic der Kundenrouter sollte voneinander abgeschirmt sein, sodass auch IP-Adressbereiche mehrfach vergeben werden können, ohne dass es zu Adresskonflikten kommt.1

Die Router P1 und P2 wurden keiner Gruppe explizit zugewiesen, ihre Konfiguration wurde gemeinsam erledigt.

3 OSPF und BGP

Zwischen den Provider-Edge und dem P-Router wurde OSPF als Routingprotokoll konfiguriert, sowie MPLS auf allen Links aktiviert.

```
interface Serial0/0/0
  ..
  mpls ip
  ..

router ospf 1
 network 5.5.5.5 0.0.0.0 area 0
 network 172.16.0.4 0.0.0.3 area 0
```

Listing 3.1: PE5, MPLS und OSPF-Konfiguration

Alle Netze wurden in den Routing-Prozess eingetragen. Wichtig hierbei war eine Loopback-Adresse (5.5.5.5). Diese wird in einem nächsten Schritt als Quelladresse für Routing-Updates mittels BGP verwendet.

3.1 VRF

Mittels Virtual Routing and Forwarding (VRF) werden die Netze der Kunden voneinander getrennt, hierfür wird ein "virtueller" Router auf PE5 eingerichtet. Das Route-Target ist dabei gleich für alle Teilnehmer des VPNs. "65000" entspricht in dem Fall einem Autonomes System (AS).

```
ip vrf ce3
 rd 65000:3
 route-target export 65000:3
 route-target import 65000:3
```

Listing 3.2: VRF CE3

Pro Kunde existiert ein eigener Routing-Prozess, hier ebenfalls mittels Open Shortest Path First (OSPF) realisiert.

```
router ospf 2 vrf ce3
 router-id 5.5.5.3
 redistribute bgp 65000 subnets
```

Listing 3.3: OSPF für CE3

Der selbe Schritt wurde auch für den CE4 Router durchgeführt.

```
ip vrf ce4
 rd 65000:4
 route-target export 65000:4
 route-target import 65000:4

router ospf 3 vrf ce4
 router-id 5.5.5.4
 redistribute bgp 65000 subnets
```

Listing 3.4: VRF und OSPF CE4

3.2 BGP

Nach dem Erstellen der beiden VRF Prozesse konnte der BGP Prozess gestartet werden. Die AS-Nummer wird dabei dem lokalen "BGP Speaker" zugewiesen. Mittels "neighbor" wird die Internet Protocol (IP)-Adresse und die AS-Nummer für einen BGP Partner festgelegt. Mittels "address-family vpnv4" wird ein Virtual Private Network (VPN) mit dem Nachbar 1.1.1.1 erstellt. Über "address-family ipv4 vrf ce3" wird der zugehörige OSPF Prozess an das jeweilige gegenüberliegende VRF verteilt.

```
router bgp 65000
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 65000
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.1 send-community extended

 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
 exit-address-family

 address-family ipv4 vrf ce3
  redistribute ospf 2
 exit-address-family

 address-family ipv4 vrf ce4
  redistribute ospf 3
 exit-address-family
```

Listing 3.5: BGP Process

4 Monitoring

4.1 Switch

Der BGP und MPLS-Traffic sollte mitgeschnitten werden. Dazu wurde zwischen Router P1 und P2 ein Switch dazwischengesschaltet. Auf diesem Switch wurde anschließend ein Monitoring-Port (bei Cisco auch Span-Port genannt) eingerichtet.

Anschließend konnte ein angeschlossener PC den Traffic mittels Wireshark mitschneiden.

```
1 monitor session 1 source interface Fa0/1
2 monitor session 1 destination interface Fa0/3 , Fa0/10
```

Listing 4.1: Monitoring-Ports

In Listing 3.5 sieht man die Konfiguration des Monitor-Ports. Traffic der von und an Port Fa0/1 geschickt wird, wird auch an den Ports Fa0/3 und Fa0/10 ausgegeben.

4.2 Wireshark

Ein Beispiel für MPLS-Traffic ist in Abbildung 4.1 zu sehen. Erkennbar sind die MPLS-Labels zwischen Layer 2 und 3. Gesendet wird ein Ping.

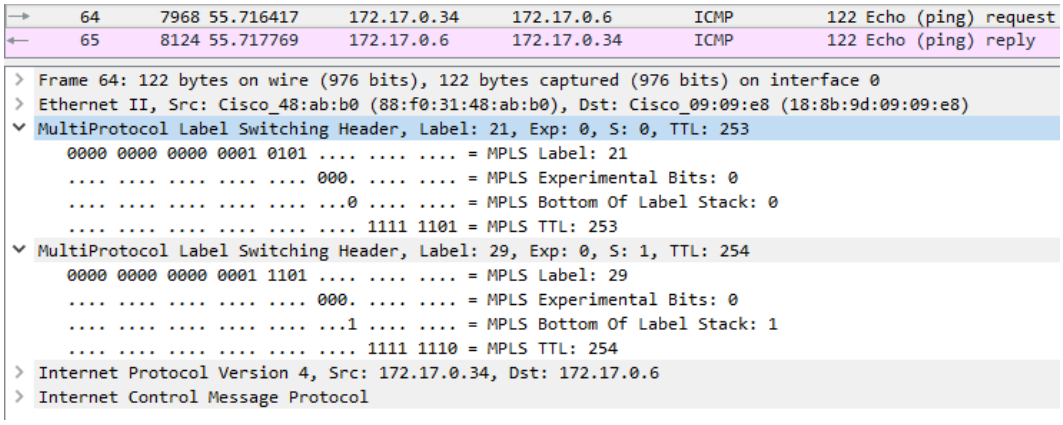

Figure 4.1: ICMP über MPLS

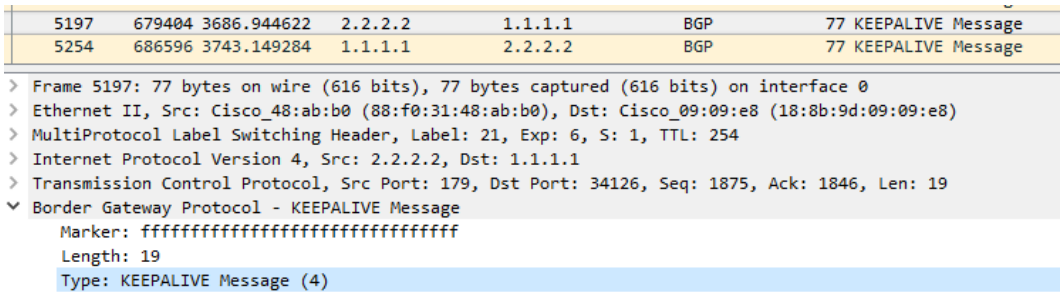

Figure 4.2: BGP-Keepalive

In Abbildung 4.2 sind BGP-Keepalive-Nachrichten zu sehen die periodisch ausgetauscht werden, ebenfalls über den MPLS-Tunnel.

4.3 Traceroutes

Mittels `traceroute` kann die Route zu einem Zielhost festgestellt werden. Führt man diesen Befehl am Router aus (Abbildung 4.3), so sieht man ebenfalls den MPLS-Tunnel, auf einem Endgerät (Abbildung 4.4) ist diese Information nicht sichtbar, da die MPLS-Label am Zielgerät nicht mehr im Frame vorhanden sind.

```
CE4#traceroute 172.17.0.2
Type escape sequence to abort.
Tracing the route to 172.17.0.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.17.0.14 0 msec 0 msec 0 msec
  2 172.16.0.6 [MPLS: Labels 21/30 Exp 0] 4 msec 0 msec 4 msec
  3 172.17.0.2 4 msec 0 msec *
CE4#
```

Figure 4.3: Traceroute-Router

```
C:\Users\its>tracert -d 172.17.0.2

Routenverfolgung zu 172.17.0.2 über maximal 30 Hops

  1    <1 ms    <1 ms    <1 ms  192.168.5.1
  2    <1 ms    <1 ms    <1 ms  172.17.0.14
  3     3 ms     3 ms     3 ms  172.16.0.6
  4     *        *        *     Zeitüberschreitung der Anforderung.
  5     2 ms     2 ms     2 ms  172.17.0.2

Ablaufverfolgung beendet.
```

Figure 4.4: Traceroute-Windows