Laborübung „Komplex ISP Netzwerk“

Schwerpunkte:

- BGP Pfadmanipulation *.*
- Flex-VPN mit Ikev2

Nachfolgend die Angabe zur Laborübung „Komplex ISP Network“.

1.1 Topologie

Gegeben sei folgende - GNS basierende - Topologie:

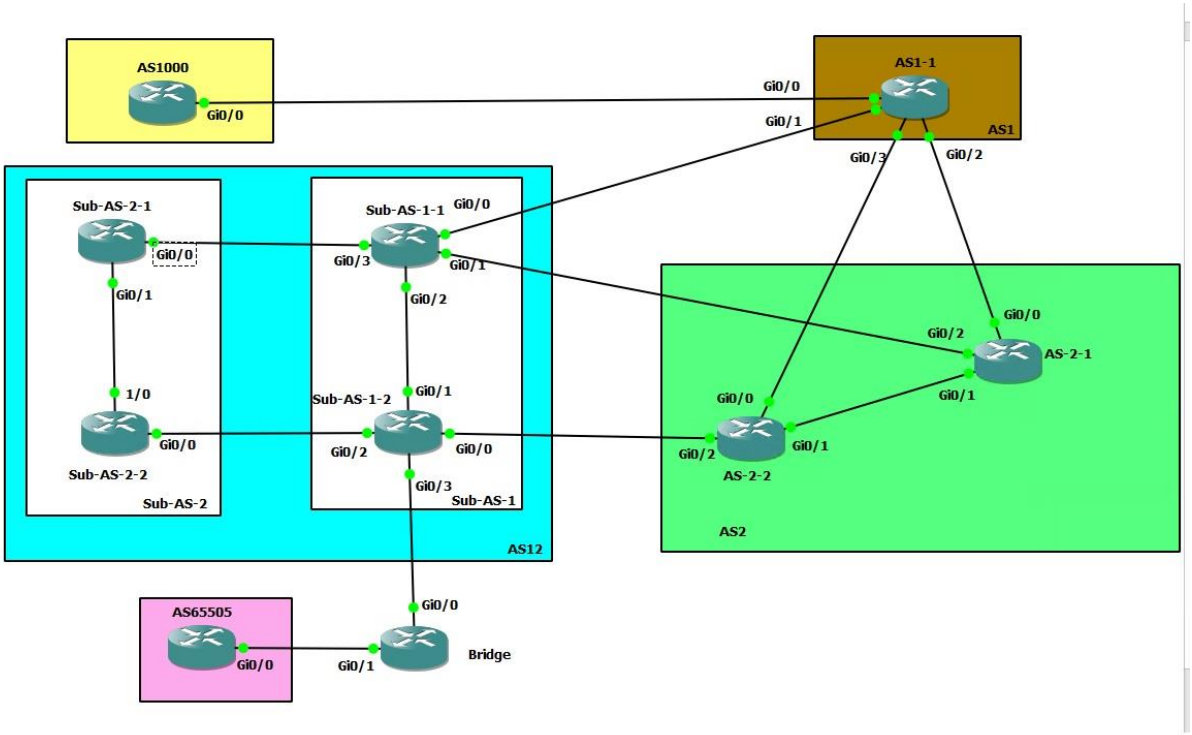


Abbildung 1.1: GNS-Topologie „Komplex ISP Network“

1.2 Die Aufgabenstellung

Gegeben Sie die Basistopologie aus Abbildung 1.1; in Summe 10 Router (+mindestes 3 weitere Router im AS 2).

Konfiguriere zunächst die Topologie aus Abbildung 1.1 + MPLS Backbone in AS2.

Das Adresskonzept lautet wie folgt:

Gerät	Interface	Description	IP
AS1-1	Gi 0/0	To_AS1000	203.0.113.1/30 2001:DB8::1/64
	Gi 0/1	To_AS-1-1	192.168.14.1/24
	Gi 0/2	To_AS-2-1	192.168.12.1/24
	Gi 0/3	To_AS-2-3	192.168.13.1/24
	Lo1		1.1.1.1/32
AS1000	Gi0/0	To_AS1-1	203.0.113.2/30 2001:DB8::2/64
	LO0		10.0.0.1/32
			2001:DB8:1::1/128
	LO1		12.34.0.1/16
			2001:DB8:12:34::1/64
	LO2		23.45.0.1/16
			2001:DB8:23:45::1/64
	LO3		66.77.0.1 255.255.128.0
			2001:DB8:66:77::1/64
	LO4		89.100.0.1 255.255.192.0
			2001:DB8:89:100::1/64
	LO5		91.200.0.1 255.255.192.0
			2001:DB8:91:200::1/64
	LO6		102.64.0.1 255.255.192.0
			2001:DB8:102:64::1/64
	LO7		123.45.0.1 255.255.128.0
			2001:DB8:123:45::1/64
	LO8		130.25.0.1 255.255.192.0
			2001:DB8:130:25::1/64
	LO9		175.45.200.1 255.255.248.0
			2001:DB8:175:45::1/64
	LO10		183.77.220.1 255.255.252.0
			2001:DB8:183:77::1/64
	LO11		185.100.0.1 255.255.224.0
			2001:DB8:185:100::1/64
	LO12		190.30.128.1 255.255.128.0
			2001:DB8:190:32::1/64
	LO13		195.225.0.1 255.255.224.0
			2001:DB8:195:225::1/64
	LO14		199.10.192.1 255.255.252.0
			2001:DB8:199:10::1/64
	LO15		210.45.128.1 255.255.254.0
			2001:DB8:210:45::1/64
	LO16		212.12.16.1 255.255.248.0
			2001:DB8:212:12::1/64
	LO17		216.80.192.1 255.255.252.0
			2001:DB8:216:80::1/64
	LO18		220.85.200.1 255.255.254.0
			2001:DB8:220:85::1/64
	LO19		221.25.0.1 255.255.224.0
			2001:DB8:225:25::1/64

AS2-1	Gi0/0	To_AS1-1	192.168.12.2/24
	Gi0/1	To_AS2-2	192.168.23.2/24
	Gi0/2	To_Sub-AS-1-1	192.168.24.2/24
	LO1		2.2.2.2/32
AS2-2	Gi0/0	To_AS1-1	192.168.13.3/24
	Gi0/1	To_AS2-1	192.168.23.3/24
	Gi0/2	To_Sub-AS-2-1	192.168.35.3/24
	Lo1		3.3.3.3/32
Sub-AS-1-1	Gi0/0	To_AS1-1	192.168.14.4/24
	Gi0/1	To_AS-2-1	192.168.24.4/24
	Gi0/2	To_Sub-AS-1-2	192.168.45.4/24
	Gi0/3	To_Sub-AS-2-1	192.168.46.4/24
	LO1		4.4.4.4/32
Sub-AS-1-2	Gi0/0	To_AS-2-2	192.168.35.5/30
	Gi0/1	To_Sub-AS-1-1	192.168.45.5/24
	Gi0/2	To_Sub-AS-2-2	192.168.57.5/24
	Gi0/3	To_Bridge	192.168.58.5/24
	LO1		5.5.5.5/32
Sub-AS-2-1	Gi0/0	To_Sub-AS-1-1	192.168.46.6/30
	Gi0/1	To_Sub-AS-2-2	192.168.67.6/30
	LO1		6.6.6.6/32
Sub-AS-2-2	Gi0/0	To_Sub-AS-1-2	192.168.57.7/30
	Gi0/1	To_Sub-AS-2-1	192.168.67.7/30
	LO1		7.7.7.7/32
Bridge	Gi0/0	To_Sub-AS-1-2	192.168.58.8/24
	Gi0/1	To_AS65505	192.168.89.8/30
	LO1		8.8.8.8/32
AS65505	Gi0/0	To_Bridge	192.168.89.9/30
	Lo1		9.9.9.9/32

Tabelle 1.2 : Adresskonzept

2. Konfigurationsanforderungen

Die Konfigurationsanforderungen entsprechen user-storries – sie stellen keineswegs eine Schritt-für-Schritt Anleitung (wie im vierten Jahrgang) dar.

Mit „A“ wird immer die Angabe, wie sie beispielsweise bei PLF’s verwendet wird dargestellt.

Mit „L“ wird ein Lösungsansatz vorgeschlagen.

Hinweis: Die Topologie entspricht CCNP Niveau und Bestandteil einer Worldskillsangabe.

2.1 IGP

A	Im AS 2, sowie im ges. AS 12 wird ein geeignetes IGP benötigt.
L	es wird OSPF vorgeschlagen. Für OSPF gilt: • authentifizierte Updates. • dedizierte Router-ID. • auch die LO’S werden via OSPF bekannt gegeben.

```
Sub-AS-1-1(config)#router ospf 1
Sub-AS-1-1(config-router)#network 4.4.4.4 0.0.0.0 area 0
Sub-AS-1-1(config-router)#network 192.168.45.0 0.0.0.255 area 0
Sub-AS-1-1(config-router)#network 192.168.46.0 0.0.0.255 area 0
Sub-AS-1-2(config)#router ospf 1
Sub-AS-1-2(config-router)#network 5.5.5.5 0.0.0.0 area 0
Sub-AS-1-2(config-router)#network 192.168.45.0 0.0.0.255 area 0
Sub-AS-1-2(config-router)#network 192.168.57.0 0.0.0.255 area 0
Sub-AS-2-1(config)#router ospf 1
Sub-AS-2-1(config-router)#network 6.6.6.6 0.0.0.0 area 0
Sub-AS-2-1(config-router)#network 192.168.67.0 0.0.0.255 area 0
Sub-AS-2-1(config-router)#network 192.168.46.0 0.0.0.255 area 0
Sub-AS-2-2(config)#router ospf 1
Sub-AS-2-2(config-router)#network 7.7.7.7 0.0.0.0 area 0
Sub-AS-2-2(config-router)#network 192.168.67.0 0.0.0.255 area 0
Sub-AS-2-2(config-router)#network 192.168.57.0 0.0.0.255 area 0
AS2-1(config)#router ospf 1
AS2-1(config-router)#network 2.2.2.2 0.0.0.0 area 0
AS2-1(config-router)#network 192.168.23.0 0.0.0.255 area 0
AS2-2(config)#router ospf 1
AS2-2(config-router)#network 3.3.3.3 0.0.0.0 area 0
AS2-2(config-router)#network 192.168.23.0 0.0.0.255 area 0
```

Beispielsweise sieht auf AS-1-1 die OSPF-Adjazenz wie folgt aus:

```
Sub-AS-1-1#sh ip ospf neighbor
192.168.67.6      1   FULL/BDR        00:00:35    192.168.46.6
GigabitEthernet0/3
5.5.5.5           1   FULL/BDR        00:00:37    192.168.45.5
GigabitEthernet0/2
```

2.2 Erreichbarkeit zwischen AS-1-2 und AS65505.

A	Die Router AS-1-2 und AS 65505 müssen sich erreichen können.
L	Es wird ein GRE-based Tunnel vorgeschlagen, aber

	• „Bridge“ darf nur die Grundkonfig habe, sowie etwaige statische Routen (max. 2) • Es sind diesbezüglich nur statische Routen auf „AS-1-2“ und „AS65505“ erlaubt.

```
Sub-AS-1-2(config)#ip route 192.168.89.9 255.255.255.255
192.168.58.8
```

```
AS65505(config)#ip route 192.168.58.5 255.255.255.255 192.168.89.8
```

```
Sub-AS-1-2(config)#interface Tunnel 0
Sub-AS-1-2(config-if)#tunnel source 192.168.58.5
Sub-AS-1-2(config-if)#tunnel destination 192.168.89.9
Sub-AS-1-2(config-if)#ip address 192.168.59.5 255.255.255.0
```

```
AS65505(config)#interface Tunnel 0
AS65505(config-if)#tunnel source 192.168.89.9
AS65505(config-if)#tunnel destination 192.168.58.5
AS65505(config-if)#ip address 192.168.59.9 255.255.255.0
```

Funktionsüberprüfung:

```
Sub-AS-1-2#ping 192.168.59.9
```

```
Sub-AS-1-2(config-if)#ip route 9.9.9.9 255.255.255.255 192.168.59.9
```

```
AS65505(config-if)#ip route 5.5.5.5 255.255.255.255 192.168.59.5
```

Funktionsüberprüfung:

```
Sub-AS-1-2# Sub-AS-1-2#ping 9.9.9.9 source 5.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
```

2.3 Notwendige iBGP und eBGP Beziehungen

A	Notwendige iBGP und eBGP Peerings herstellen.
L	• Es werden die jeweiligen LO’s für die iBGP Beziehungen verwendet. • Es werden die physischen Interfaces für die eBGP Beziehungen verwendet (ausgenommen 2.2). • eBGP zwischen AS1-1 und AS1000 • eBGP zwischen AS1-1 und AS-2-1 • eBGP zwischen AS1-1 und AS-2-2 • eBGP zwischen AS1-1 und SubAS-1-1 • iBGP zwischen AS2-1 und AS2-2 • eBGP zwischen AS2-1 und Sub-AS-1-2 • eBGP zwischen AS-2-2 und Sub-AS-1-2 • Peering in der confederation AS 1112 • eBGP zwischen Sub-AS-1-2 und AS65505 • zwischen AS1-1 und AS100 gibt es eine weitere eBGP Beziehung auf Basis IPv6. (Peering mit physischen Interface-IP’s)

2.3.1 : iBGP AS-2-1 & AS-2-2

```
AS2-1(config-router)#exit
AS2-1(config)#router bgp 2
AS2-1(config-router)#neighbor 3.3.3.3 remote-as 2
AS2-1(config-router)#neighbor 3.3.3.3 update-source Loopback0
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#neighbor 2.2.2.2 remote-as 2
AS2-2(config-router)#neighbor 2.2.2.2 update-source Loopback0
```

Funktionsüberprüfung:

```
AS2-2#show ip bgp summary
BGP router identifier 3.3.3.3, local AS number 2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
2.2.2.2         4           23       4       4        1    0    0
00:01:38        0
```

2.3.2 iBGP innerhalb der confederation AS12

```
Sub-AS-1-1(config-router)#router bgp 11
Sub-AS-1-1(config-router)#bgp confederation identifier 1112
Sub-AS-1-1(config-router)#bgp confederation peers 12
Sub-AS-1-1(config-router)#neighbor 5.5.5.5 remote-as 11
Sub-AS-1-1(config-router)#neighbor 5.5.5.5 update-source Loopback0
Sub-AS-1-1(config-router)#neighbor 6.6.6.6 remote-as 12
Sub-AS-1-1(config-router)#neighbor 6.6.6.6 update-source Loopback0
Sub-AS-1-1(config-router)#neighbor 6.6.6.6 ebgp-multihop 2
```

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#bgp confederation identifier 1112
Sub-AS-1-2(config-router)#bgp confederation peers 12
Sub-AS-1-2(config-router)#neighbor 4.4.4.4 remote-as 11
Sub-AS-1-2(config-router)#neighbor 4.4.4.4 update-source Loopback0
Sub-AS-1-2(config-router)#neighbor 7.7.7.7 remote-as 12
Sub-AS-1-2(config-router)#neighbor 7.7.7.7 update-source Loopback0
Sub-AS-1-2(config-router)#neighbor 7.7.7.7 ebgp-multihop 2
```

```
Sub-AS-2-1(config)#router bgp 12
Sub-AS-2-1(config-router)#bgp confederation identifier 1112
Sub-AS-2-1(config-router)#bgp confederation peers 11
Sub-AS-2-1(config-router)#neighbor 7.7.7.7 remote-as 12
Sub-AS-2-1(config-router)#neighbor 7.7.7.7 update-source Loopback0
Sub-AS-2-1(config-router)#neighbor 4.4.4.4 remote-as 11
Sub-AS-2-1(config-router)#neighbor 4.4.4.4 update-source Loopback0
Sub-AS-2-1(config-router)#neighbor 4.4.4.4 ebgp-multihop 2
```

```
Sub-AS-2-2(config)#router bgp 12
Sub-AS-2-2(config-router)#bgp confederation identifier 1112
Sub-AS-2-2(config-router)#bgp confederation peers 11
Sub-AS-2-2(config-router)#neighbor 6.6.6.6 remote-as 12
Sub-AS-2-2(config-router)#neighbor 6.6.6.6 update-source Loopback0
Sub-AS-2-2(config-router)#neighbor 5.5.5.5 remote-as 11
Sub-AS-2-2(config-router)#neighbor 5.5.5.5 update-source Loopback0
Sub-AS-2-2(config-router)#neighbor 5.5.5.5 ebgp-multihop 2
```

Funktionsüberprüfung:

```
Sub-AS-1-1#show ip bgp summary
BGP router identifier 4.4.4.4, local AS number 11
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
5.5.5.5         4           11       0       0        1    0    0
00:10:50 Idle
6.6.6.6         4           12       6       7        1    0    0
00:03:20        0
```

Man beachte, das shier nur AS11 und AS12 angezeigt wird, nicht aber die confederation AS1112. Die Überprüfung der Conferderations kann erst beim „tatsächlichen“ Routenaustausch überprüft werden.

2.3.3 eBGP zwischen AS1000 und AS1

```
AS1000(config-if)#router bgp 1000
AS1000(config-router)#neighbor 203.0.113.1 remote-as 1
```

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#neighbor 203.0.113.2 remote-as 1000
```

2.3.4 eBGP zwischen AS1 und AS2

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#neighbor 192.168.12.2 remote-as 2
AS1-1(config-router)#neighbor 192.168.13.3 remote-as 2
```

```
AS2-1(config)#router bgp 2
AS2-1(config-router)#neighbor 192.168.12.1 remote-as 1
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#neighbor 192.168.13.1 remote-as 1
```

2.3.5 eBGP zwischen AS2 und AS1112

```
AS2-1(config)#router bgp 2
AS2-1(config-router)#neighbor 192.168.24.4 remote-as 1112
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#neighbor 192.168.35.5 remote-as 1112
```

```
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#neighbor 192.168.24.2 remote-as 2
```

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#neighbor 192.168.35.3 remote-as 2
```

2.4.6 eBGP zwischen AS 1 und AS 11

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#neighbor 192.168.14.4 remote-as 1112
```

```
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#neighbor 192.168.14.1 remote-as 1
```

2.4.7 eBGP zwischen AS 1112 und AS 65505.9

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#neighbor 9.9.9.9 remote-as 65505.9
Sub-AS-1-2(config-router)#neighbor 9.9.9.9 update-source Loopback0
Sub-AS-1-2(config-router)#neighbor 9.9.9.9 ebgp-multihop 2
```

```
AS65505(config)#router bgp 65505.9
AS65505(config-router)#neighbor 5.5.5.5 remote-as 1112
AS65505(config-router)#neighbor 5.5.5.5 update-source Loopback0
AS65505(config-router)#neighbor 5.5.5.5 ebgp-multihop 2
```

Funktionsüberprüfung:

```
AS1-1#sh ip bgp summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
192.168.12.2    4            2     155     154        1    0    0
02:19:18        0
192.168.13.3    4            2     154     154        1    0    0
02:18:48        0
192.168.14.4    4         1112     147     146        1    0    0
02:11:30        0
203.0.113.2     4         1000     159     156        1    0    0
02:21:34        0
```

```
AS2-1#show bgp summary
BGP router identifier 2.2.2.2, local AS number 2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
3.3.3.3         4            2       4       4        1    0    0
00:00:28        0
192.168.12.1    4            1     157     158        1    0    0
02:22:06        0
192.168.24.4    4         1112     150     149        1    0    0
02:14:13        0
```

```
BGP router identifier 3.3.3.3, local AS number 2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
2.2.2.2         4            2       5       5        1    0    0
00:01:01        0
192.168.13.1    4            1     157     158        1    0    0
02:22:08        0
192.168.35.5    4         1112      14      12        1    0    0
00:09:21        0
```

```
Sub-AS-1-1#show ip bgp summary
BGP router identifier 4.4.4.4, local AS number 11
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
```

```
5.5.5.5         4           11      15      15        1    0    0
00:10:10        0
6.6.6.6         4           12       0       0        1    0    0
never    Idle
192.168.14.1    4            1     151     151        1    0    0
02:15:17        0
192.168.24.2    4            2     150     151        1    0    0
02:15:11        0
```

```
Sub-AS-1-2#show bgp summ
BGP router identifier 5.5.5.5, local AS number 11
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
4.4.4.4         4           11      16      16        1    0    0
00:11:18        0
7.7.7.7         4           12      16      16        1    0    0
00:11:20        0
9.9.9.9         4   4292935689      11      10        1    0    0
00:07:40        0
192.168.35.3    4            2      13      15        1    0    0
00:11:02        0
```

Man beachte, dass auf den Routern Sub-AS-2-1 und Sub-AS-2-2 bislang keine BGP Konfiguration vorhanden ist; weiters werden auch noch keine Routen via BGP verteilt.

2.4.8 eBGP zwischen AS 1 und AS 1000 via IPv6

```
AS1-1(config)#ipv6 unicast-routing
AS1-1(config)#router bgp 1
AS1-1(config-router)#neighbor 2001:db8::2 remote-as 1000
AS1-1(config-router)#address-family ipv4
AS1-1(config-router-af)#no neighbor 2001:db8::2 activate
AS1-1(config-router-af)#exit
AS1-1(config-router)#address-family ipv6
AS1-1(config-router-af)#neighbor 2001:db8::2 activate
AS1-1(config-router-af)#exit
```

```
AS1000(config)#ipv6 unicast-routing
AS1000(config)#router bgp 1000
AS1000(config-router)#neighbor 2001:db8::1 remote-as 1
AS1000(config-router)#address-family ipv4
AS1000(config-router-af)#no neighbor 2001:db8::1 activate
AS1000(config-router-af)#exit
AS1000(config-router)#address-family ipv6
AS1000(config-router-af)#neighbor 2001:db8::1 activate
```

Funktionsüberprüfung:

```
AS1000#sh bgp ipv6 unicast summary
BGP router identifier 221.25.0.1, local AS number 1000
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2001:DB8::1     4            1       5       4        1    0    0 00:00:51
0
```

2.4 BGP basierende Grundkonfiguration

A	Verwende Next-Hop-Self

2.4.1 iPv6 Routen in BGP

Der Router AS 1000 soll die Looppackinterfaces für späteres „Manipulieren“ advertisen:

```
AS1000(config)#router bgp 1000
AS1000(config-router)#address-family ipv4
AS1000(config-router-af)#redistribute connected
AS1000(config-router-af)#network 10.0.0.1 mask 255.255.255.255
```

Überprüfen wir nun, ob die von AS1000 bekannt gegebenen Routen auch auf AS1-1 aufscheinen:

```
AS1-1#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight Path
 *>   10.0.0.1/32      203.0.113.2              0             0 1000 i
 *>   12.34.0.0/16     203.0.113.2              0             0 1000 ?
 *>   23.45.0.0/16     203.0.113.2              0             0 1000 ?
 *>   66.77.0.0/17     203.0.113.2              0             0 1000 ?
 *>   89.100.0.0/18    203.0.113.2              0             0 1000 ?
 *>   91.200.0.0/18    203.0.113.2              0             0 1000 ?
 *>   102.64.0.0/18    203.0.113.2              0             0 1000 ?
 *>   123.45.0.0/17    203.0.113.2              0             0 1000 ?
 *>   130.25.0.0/18    203.0.113.2              0             0 1000 ?
 *>   175.45.200.0/21  203.0.113.2              0             0 1000 ?
 *>   183.77.220.0/22  203.0.113.2              0             0 1000 ?
 *>   185.100.0.0/19   203.0.113.2              0             0 1000 ?
 *>   190.30.128.0/17  203.0.113.2              0             0 1000 ?
 *>   195.225.0.0/19   203.0.113.2              0             0 1000 ?
 *>   199.10.192.0/22  203.0.113.2              0             0 1000 ?
 r>   203.0.113.0/30   203.0.113.2              0             0 1000 ?
 *>   210.45.128.0/23  203.0.113.2              0             0 1000 ?
 *>   212.12.16.0/21   203.0.113.2              0             0 1000 ?
 *>   216.80.192.0/22  203.0.113.2              0             0 1000 ?
 *>   220.85.200.0/23  203.0.113.2              0             0 1000 ?
 *>   221.25.0.0/19    203.0.113.2              0             0 1000 ?
```

Beim Betrachten der BGP-Tabelle sollte folgendes beachtet werden:

- Routenherkunft: da statisch auf AS1000 redistributiert, ist die Routenherkunft „?“,
- Außer für 10.0.0.1, das ja explizit im Network-Befehl angegeben wurde.
- Die Route 203.0.113.0/30 wurde nicht in der Routingtabelle via BGP installiert – Code „r“, da diese Route ja dem lokal connected network entspricht. Directly connected networks haben eine geringere administrative Distanz als BGP-Routen !!

Für IPv6 gilt:

```
AS1000(config)#router bgp 1000
AS1000(config-router)#address-family ipv6
AS1000(config-router-af)#network 2001:0db8:23:45::/64
AS1000(config-router-af)#network 2001:0db8:66:77::/64
AS1000(config-router-af)#network 2001:0db8:89:100::/64
AS1000(config-router-af)#network 2001:0db8:91:200::/64
AS1000(config-router-af)#network 2001:0db8:102:64::/64
AS1000(config-router-af)#network 2001:0db8:123:45::/64
AS1000(config-router-af)#network 2001:0db8:130:25::/64
```

```
AS1000(config-router-af)#network 2001:0db8:175:45::/64
AS1000(config-router-af)#network 2001:0db8:183:77::/64
AS1000(config-router-af)#network 2001:0db8:185:100::/64
AS1000(config-router-af)#network 2001:0db8:190:32::/64
AS1000(config-router-af)#network 2001:0db8:195:225::/64
AS1000(config-router-af)#network 2001:0db8:199:10::/64
AS1000(config-router-af)#network 2001:0db8:210:45::/64
AS1000(config-router-af)#network 2001:0db8:212:12::/64
AS1000(config-router-af)#network 2001:0db8:216:80::/64
AS1000(config-router-af)#network 2001:0db8:220:85::/64
AS1000(config-router-af)#network 2001:0db8:225:25::/64
```

```
AS1-1#show bgp ipv6 unicast

     Network          Next Hop            Metric LocPrf Weight Path
 *>   2001:DB8:23:45::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:66:77::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:89:100::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:91:200::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:102:64::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:123:45::/64
                      2001:DB8::2              0             0 1000 i
 *>   2001:DB8:130:25::/64
                      2001:DB8::2              0             0 1000 i
```

Da jetzt alle Netze im network-Befehl includiert sind, erscheinen nun diese Netze auch mit Routenherkunft „i“.

Damit wir die IPv6 Routen auch nach AS 2 verteilen können, gilt:

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#address-family ipv6
AS1-1(config-router-af)#neighbor 192.168.12.2 activate
AS1-1(config-router-af)#neighbor 192.168.13.3 activate
AS1-1(config-router-af)#exit
```

```
AS2-1(config)#ipv6 unicast-routing
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv6
AS2-1(config-router-af)#neighbor 192.168.12.1 activate
AS2-1(config-router-af)#neighbor 3.3.3.3 activate
AS2-1(config-router-af)#exit
```

```
AS2-2(config)#ipv6 unicast-routing
AS2-2(config)#router bgp 2
AS2-2(config-router)#address-family ipv6
AS2-2(config-router-af)#neighbor 192.168.13.1 activate
AS2-2(config-router-af)#neighbor 2.2.2.2 activate
AS2-2(config-router-af)#exit
```

Betrachten wir nun, wie IPv6 Routen aus AS 1 via BGP nach AS2 „angeboten“ werden:

```
AS2-1#show bgp ipv6 unicast
BGP table version is 1, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
```

```
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *    2001:DB8:23:45::/64
                       ::FFFF:192.168.12.1
                                                             0 1 1000 i
 *    2001:DB8:66:77::/64
                       ::FFFF:192.168.12.1
                                                             0 1 1000 i
 *    2001:DB8:89:100::/64
                       ::FFFF:192.168.12.1
                                                             0 1 1000 i
 *    2001:DB8:91:200::/64
                       ::FFFF:192.168.12.1
                                                             0 1 1000 i
```

Betrachten wir die Routingtabelle dazu:

```
AS2-1#show ipv6 route
IPv6 Routing Table - default - 1 entries
L   FF00::/8 [0/0]
     via Null0, receive
```

Es wird keine IPv6 Route in die Routingtabelle aufgenommen! Dies liegt daran, dass die entsprechende Routenherkunft auf AS2-1 für die IPv6 Routen nicht bekannt ist, siehe dazu auch der Eintrag `FFFF:192.168.12.1` in obiger Ansicht; `FFFF:192.168.12.1` steht dabei in BGP für einen Platzhalter. Grund dafür ist, dass in AS2 kein lokales IPv6 Netz existiert, somit werden auch keine „IPv6 Routen benötigt“.

2.4.2 Propagierung der Loopback-Interfaces in BGP

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#address-family ipv4
AS1-1(config-router-af)#network 1.1.1.1 mask 255.255.255.255
```

```
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#network 2.2.2.2 mask 255.255.255.255
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#address-family ipv4
AS2-2(config-router-af)#network 3.3.3.3 mask 255.255.255.255
```

```
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#address-family ipv4
Sub-AS-1-1(config-router-af)#network 4.4.4.4 mask 255.255.255.255
```

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#address-family ipv4
Sub-AS-1-2(config-router-af)#network 5.5.5.5 mask 255.255.255.255
```

```
Sub-AS-2-1(config)#router bgp 12
Sub-AS-2-1(config-router)#address-family ipv4
Sub-AS-2-1(config-router-af)#network 6.6.6.6 mask 255.255.255.255
```

```
Sub-AS-2-2(config)#router bgp 12
Sub-AS-2-2(config-router)#address-family ipv4
Sub-AS-2-2(config-router-af)#network 7.7.7.7 mask 255.255.255.255
```

```
AS65505(config)#router bgp 65505.9
AS65505(config-router)#address-family ipv4
```

```
AS65505(config-router-af)#network 9.9.9.9 mask 255.255.255.255
```

2.4.3 Routenherkunft überschreiben

Bislang werden BGP Routen nur „2 hops“ weitergegeben. Das liegt daran, dass die Routenherkunft in der lokalen Routingtabelle nicht aufgelöst werden kann – und somit die zwar mit BGP gelernte Route bekannt ist, aber nicht in die Routingtabelle übernommen wird.

Lösung dieses Problems ist

- Die Bekanntgabe der Routenherkunft in BGP (peering mit public-IP’s)
- Verwendung von next-hop-self

```
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#neighbor 3.3.3.3 next-hop-self
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#address-family ipv4
AS2-2(config-router-af)#neighbor 2.2.2.2 next-hop-self
```

```
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#address-family ipv4
Sub-AS-1-1(config-router-af)#neighbor 5.5.5.5 next-hop-self
Sub-AS-1-1(config-router-af)#neighbor 6.6.6.6 next-hop-self
```

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#address-family ipv4
Sub-AS-1-2(config-router-af)#neighbor 4.4.4.4 next-hop-self
Sub-AS-1-2(config-router-af)#neighbor 7.7.7.7 next-hop-self
```

2.5 Erweiterte BGP Features

A	Verwende BGP Auto.Summary; Router AS65505 wird später Netze im Bereich 9.0.0.0/8 bekannt geben.

Das Netz 9.0.0.0 soll nun als Summary-Route von AS65505.9 bekannt gegeben werden:

```
AS65505(config)#router bgp 65505.9
AS65505(config-router)#auto-summary
AS65505(config-router)#no network 9.9.9.9 mask 255.255.255.255
AS65505(config-router)#network 9.0.0.0
```

Funktionsüberprüfung:

```
AS65505#show ip bgp 9.0.0.0
BGP routing table entry for 9.0.0.0/8, version 58
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local
    0.0.0.0 from 0.0.0.0 (9.9.9.9)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced,
local, best
      rx pathid: 0, tx pathid: 0x0
```

Betrachten wir, ob diese Summaryroute auch von den anderen Routern so „verstanden“ wird:

```
AS2-2#sh ip route | inc 9.0
```

```
B      9.0.0.0/8 [20/0] via 192.168.35.5, 00:03:27
       89.0.0.0/18 is subnetted, 1 subnets
```

A	Um Routingtabellen „kleiner“ zu machen, muss BGP Summarization verwendet werden. Dazu sollen die Netze der Lo’s 10,11 & 12 zusammengefasst werden.

Folgende Netze sollen zusammengefasst werden:

```
AS1000#show ip int brief | begin Loopback10
Loopback10                 183.77.220.1    YES NVRAM  up                    up
Loopback11                 185.100.0.1     YES NVRAM  up                    up
Loopback12                 190.30.128.1    YES NVRAM  up                    up
```

```
AS1000(config)#router bgp  1000
AS1000(config-router)#address-family ipv4
AS1000(config-router-af)#aggregate-address 176.0.0.0 240.0.0.0 summary-
only
```

Betrachten wir nun einen Auszug aus der BGP-Table:

```
AS1000#sh ip bgp

     Network          Next Hop            Metric LocPrf Weight Path
 *>   176.0.0.0/4      0.0.0.0                             32768 i
 s>   183.77.220.0/22  0.0.0.0                  0          32768 ?
 s>   185.100.0.0/19   0.0.0.0                  0          32768 ?
 s>   190.30.128.0/17  0.0.0.0                  0          32768 ?
*>   195.225.0.0/19   0.0.0.0                  0          32768 ?
```

```
AS2-2#show ip bgp
*    176.0.0.0/4      192.168.35.5                         0 1112 1 1000 i
```

2.5.1 BGP Weight Attribute

A	Das Netz 12.34.0.0/16 wird von Sub-AS-1-1 via AS2 geroutet (anstelle direkt via AS1)
L	Route-map auf Sub-AS-1-1

Betrachten wir zunächst die Ausgangslage, also die Routen auf Sub-AS-1-1:

```
Sub-AS-1-1#sh ip bgp 12.34.0.0
BGP routing table entry for 12.34.0.0/16, version 5
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1           4           5
  Refresh Epoch 1
  2 1 1000
    192.168.24.2 from 192.168.24.2 (2.2.2.2)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  1 1000
    192.168.14.1 from 192.168.14.1 (1.1.1.1)
      Origin incomplete, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Man sieht, dass dass Netz 12.34.0.0 über 2 Nachbarn gelernt wurde (Paths: (2 available, best #2) Pfad 2 via 192.168.24.2 ist der bessere AS Path (der kürzere).

Diese Pfadwahl soll nun beeinflusst werden:

```
Sub-AS-1-1(config)#access-list 1 permit 12.34.0.0 0.0.255.255
Sub-AS-1-1(config)#route-map Set_BGP_Weight permit 10
Sub-AS-1-1(config-route-map)#match ip address 1
Sub-AS-1-1(config-route-map)#set weight 500
Sub-AS-1-1(config-route-map)#exit
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#neighbor 192.168.24.2 route-map Set_BGP_Weight
in
```

2.5.2 BGP Local Preference

A	Pakete mit Ziel 23.45.0.0/16 von AS 2 müssen immer via AS2-1 dieses AS verlassen.
L	Local Preference

```
AS2-1(config)#access-list 1 permit 23.45.0.0 0.0.255.255
AS2-1(config)#route-map BGP_Localpref permit 10
AS2-1(config-route-map)#match ip address 1
AS2-1(config-route-map)#set local-preference 750
AS2-1(config-route-map)#exit
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#neighbor 192.168.12.1 route-map BGP_Localpref in
```

Betrachten wir wieder das Ergebnis:

```
AS2-1#show ip bgp 23.45.0.0
BGP routing table entry for 23.45.0.0/16, version 11
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     4           5
  Refresh Epoch 2
  1112 1 1000
    192.168.24.4 from 192.168.24.4 (4.4.4.4)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 2
  1 1000
    192.168.12.1 from 192.168.12.1 (1.1.1.1)
      Origin incomplete, localpref 750, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Lokal funktioniert die Präferenz, wie aber sieht ein Nachbar-AS das Netz:

```
AS2-2#show ip bgp 23.45.0.0
BGP routing table entry for 23.45.0.0/16, version 63
Paths: (3 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  1 1000
    2.2.2.2 (metric 2) from 2.2.2.2 (2.2.2.2)
      Origin incomplete, metric 0, localpref 750, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
```

```
  Refresh Epoch 1
  1112 1 1000
    192.168.35.5 from 192.168.35.5 (5.5.5.5)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  1 1000
    192.168.13.1 from 192.168.13.1 (1.1.1.1)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

2.5.3 BGP Path Prepending

A	Jeder Traffic von AS1-1 zum Netz 9.0.0.0/8 muss via AS2 gegenüber AS1112 bevorzugt geroutet werden.
L	AS path prepending auf Sub-AS-1-1 konfiguriert ist, somit soll der Pfad via AS12 3 mal länger sein, als über AS2

Betrachten wir dazu wieder den Ausgangszustand; der beste Pfad zum Netz 9.0.0.0/8 ist via Sub-AS-1-1:

```
AS1-1#show ip bgp 9.0.0.0
BGP routing table entry for 9.0.0.0/8, version 84
Paths: (3 available, best #2, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  2 1112 4292935689
    192.168.12.2 from 192.168.12.2 (2.2.2.2)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  1112 4292935689
    192.168.14.4 from 192.168.14.4 (4.4.4.4)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 1
  2 1112 4292935689
    192.168.13.3 from 192.168.13.3 (3.3.3.3)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

```
Sub-AS-1-1(config)#access-list 2 permit 9.0.0.0 0.255.255.255
Sub-AS-1-1(config)#route-map BGP_Prepend permit 10
Sub-AS-1-1(config-route-map)#match ip address 2
Sub-AS-1-1(config-route-map)#set as-path prepend 1112 1112 1112 1112
Sub-AS-1-1(config-route-map)#exit
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#neighbor 192.168.14.1 route-map BGP_Prepend out
```

Betrachten wir das Ergebnis:

```
AS1-1#show ip bgp | begin 9.0.0.0
 *    9.0.0.0 192.168.14.4  0 1112 1112 1112 1112 1112 4292935689 i
 *>           192.168.12.2  0 2 1112 4292935689 i
 *            192.168.13.3  0 2 1112 4292935689 i
```

Man beachte, die Route zu 9.0.0.0/8 wurde via 192.168.14.4 (also Sub-AS-1-1) gelernt – und zwar mit AS 1112 4 x prepended + AS, somit ergibt sich eine Gesamt AS-Path-Length von 6; im Vergleich zur gelernten Route via 192.168.12.2 mit AS 2 + AS 65535.9 = Pfadlänge 2.

2.5.3 BGP Origin Code Attribute

A	Am AS1000 soll sichergestellt werden, dass die Herkunft von 66.77.0.0/17 vergleichbar zu einer redistributierten Route ist.

Sehen wir uns wieder die Ausgangssituation an:

```
Sub-AS-1-1#show ip bgp 66.77.0.0
BGP routing table entry for 66.77.0.0/17, version 13
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     19          20          22
  Refresh Epoch 2
  1 1000
    192.168.14.1 from 192.168.14.1 (1.1.1.1)
      Origin incomplete, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 2
  2 1 1000
    192.168.24.2 from 192.168.24.2 (2.2.2.2)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

Die Route wird als „incomplete“ gekennzeichnet bzw. in der BGP-Tabelle mit einem „?“ als Routenherkunft (Da ja via Redistribution nach BGP bekannt gegeben wurde).

```
AS1000(config)#router bgp 1000
AS1000(config-router)#address-family ipv4
AS1000(config-router-af)#network 66.77.0.0 mask 255.255.128.0
```

Betrachten wir wieder das Ergebnis:

```
Sub-AS-1-1#show ip bgp 66.77.0.0
BGP routing table entry for 66.77.0.0/17, version 32
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     19          20          22
  Refresh Epoch 2
  1 1000
    192.168.14.1 from 192.168.14.1 (1.1.1.1)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 2
  2 1 1000
    192.168.24.2 from 192.168.24.2 (2.2.2.2)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

```
Sub-AS-1-1#show ip bgp | inc 66.77
 *>   66.77.0.0/17     192.168.14.1                           0 1 1000 i
```

2.5.4 BGP MED Attribute

A	Mit Hilfe des MED Parameters in AS 2 soll das Routing auf AS1-1 derart beeinflusst werden, sodass der Pfad von AS1-1 zu 9.0.0.0/8 via AS2 als Pfad über AS-2-2 genommen wird.

Betrachten wir wieder die Ausgangssituation:

```
AS1-1#show ip bgp 9.0.0.0
BGP routing table entry for 9.0.0.0/8, version 111
Paths: (3 available, best #2, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  1112 1112 1112 1112 1112 4292935689
    192.168.14.4 from 192.168.14.4 (4.4.4.4)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  2 1112 4292935689
    192.168.12.2 from 192.168.12.2 (2.2.2.2)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 1
  2 1112 4292935689
    192.168.13.3 from 192.168.13.3 (3.3.3.3)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

Die Route zu 9.0.0.0/8 kann nicht via 192.168.14.4 (Sub-AS-1-1) gewählt werden, da wir ja Prepending betrieben haben; somit bleiben nur noch 192.168.12.2 und 192.168.13.3 als Herkunft über. In obigem Beispiel wurde 192.168.12.2 (AS-2-1) gewählt. Es soll nun aber statisch die Herkunft 192.168.13.3 gewählt werden:

```
AS2-1(config)#access-list 2 permit 9.0.0.0 0.255.255.255
AS2-1(config)#route-map BGP_Med permit 10
AS2-1(config-route-map)#match ip address 2
AS2-1(config-route-map)#set metric 800
AS2-1(config-route-map)#exit
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#neighbor 192.168.12.1 route-map BGP_Med out
```

Das Ergebnis:

```
AS1-1#show ip bgp 9.0.0.0
BGP routing table entry for 9.0.0.0/8, version 116
Paths: (3 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  2 1112 4292935689
    192.168.12.2 from 192.168.12.2 (2.2.2.2)
      Origin IGP, metric 800, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  1112 1112 1112 1112 1112 4292935689
    192.168.14.4 from 192.168.14.4 (4.4.4.4)
```

```
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  2 1112 4292935689
    192.168.13.3 from 192.168.13.3 (3.3.3.3)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Wir sehen, dass nun 192.168.13.3 explizit gewählt wird; bei 192.168.12.2 sehen wir die Metrik 800.

2.5.5 eBGP bevorzugt gegenüber iBGP

A	91.200.0.0/18 wird via BGP auf AS2-2 advertised, dazu sollte es 3 Routingtabelleneinträge geben; aber welcher wird als der beste Pfad ausgewählt?

Bevor wir die Ausgangssituation betrachten, fügen wir zu AS65505.9 noch ein weiteres LO hinzu:

```
AS65505(config)#interface Loopback1
AS65505(config-if)# ip address 41.41.41.41 255.255.255.255
AS65505(config-if)#router bgp 65505.9
AS65505(config-router)#address-family ipv4
AS65505(config-router-af)#network 41.41.41.41 mask 255.255.255.255
```

Betrachten wir wieder die Ausgangssituation:

```
AS2-2#sh ip bgp 41.41.41.41
BGP routing table entry for 41.41.41.41/32, version 194
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1           7
  Refresh Epoch 1
  1112 4292935689
    2.2.2.2 (metric 2) from 2.2.2.2 (2.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  1112 4292935689
    192.168.35.5 from 192.168.35.5 (5.5.5.5)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Wir sehen, dass auf AS2-2 das Netz 41.41.41.41 via 2.2.2.2 (internal) und 192.168.35.5 (external) bekannt ist. Bei gleicher Metrik und localpref – und auch gleichem AS-Path – ist somit nur die Herkunft eBGP und iBGP schlagend; eBGP wird bevorzugt.

2.5.6 BGP Communities

A	• Das Netz 102.64.0.0/18 darf nicht von AS1-1 zu AS2-1, AS2-2 und Sub-AS-1-1 advertised werden. • Das Netz 123.45.0.0/17 wird von AS1-1 zu AS2 und AS12 advertised, sodass eBGP peers diese Route nicht nochmals „readvertisen“ zu anderen BGP-Peers.

Betrachten wir 102.64.0.0:

```
AS1-1(config)#access-list 1 permit 102.64.0.0 0.0.63.255
AS1-1(config)#route-map BGP_Communities permit 10
```

```
AS1-1(config-route-map)#match ip address 1
AS1-1(config-route-map)#set community no-advertise
AS1-1(config)#router bgp 1
AS1-1(config-router)#address-family ipv4
AS1-1(config-router-af)#neighbor 192.168.14.4 route-map BGP_Communities
out
AS1-1(config-router-af)#neighbor 192.168.12.2 route-map BGP_Communities
out
AS1-1(config-router-af)#neighbor 192.168.13.3 route-map BGP_Communities
out
AS1-1(config-router-af)#neighbor 192.168.14.4 send-community
AS1-1(config-router-af)#neighbor 192.168.12.2 send-community
AS1-1(config-router-af)#neighbor 192.168.13.3 send-community
```

Ergebnis:

```
AS2-1#show ip bgp 102.64.0.0
BGP routing table entry for 102.64.0.0/18, version 76
Paths: (1 available, best #1, table default, not advertised to any peer)
Flag: 0x4100
  Not advertised to any peer
  Refresh Epoch 1
  1 1000
    192.168.12.1 from 192.168.12.1 (1.1.1.1)
      Origin incomplete, localpref 750, valid, external, best
      Community: no-advertise
      rx pathid: 0, tx pathid: 0x0
```

Betrachten wir 123.45.0.0:

Das Netz 123.45.0.0/17 soll von AS1-1 aus zu AS2 und AS11 advertised werden, aber die eBGP Peers sollen das Netz nicht weiter propagieren.

```
AS1-1(config)#access-list 2 permit 123.45.0.0 0.0.31.255
AS1-1(config)#route-map BGP_Communities permit 12
AS1-1(config-route-map)#match ip address 2
AS1-1(config-route-map)#set community no-export
```

```
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#neighbor 3.3.3.3 send-community
AS2-1(config-router-af)#neighbor 192.168.24.4 send-community
```

```
AS2-2(config-router)#address-family ipv4
AS2-2(config-router-af)#neighbor 2.2.2.2 send-community
AS2-2(config-router-af)#neighbor 192.168.35.5 send-community
```

```
Sub-AS-1-1(config)#router bgp 11
Sub-AS-1-1(config-router)#address-family ipv4
Sub-AS-1-1(config-router-af)#neighbor 5.5.5.5 send-community
Sub-AS-1-1(config-router-af)#neighbor 6.6.6.6 send-community
```

```
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#address-family ipv4
Sub-AS-1-2(config-router-af)#neighbor 4.4.4.4 send-community
Sub-AS-1-2(config-router-af)#neighbor 7.7.7.7 send-community
```

Ergebnis:

```
AS2-1#show  ip bgp 123.45.0.0
BGP routing table entry for 123.45.0.0/17, version 5
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Advertised to update-groups:
```

```
     19
  Refresh Epoch 1
  1 1000
    192.168.12.1 from 192.168.12.1 (1.1.1.1)
      Origin incomplete, localpref 750, valid, external, best
      Community: no-export
      rx pathid: 0, tx pathid: 0x0
```

Es gibt also keine export-community.

```
AS65505#show ip route 123.45.0.0
% Network not in table
```

2.5.7 BGP Route Filtering

A	Alle Netze mit /18 Prefix sollen gefiltert werden, diese Routen sollen in der Routingtabelle von AS65505 nicht aufscheinen.
L	Prefix-List auf Sub-AS-1-2

```
Sub-AS-1-2(config)#ip prefix-list Set_Filter-18 deny 0.0.0.0/0 ge 18 le
18
Sub-AS-1-2(config)#ip prefix-list Set_Filter-18 permit 0.0.0.0/0 le 32
Sub-AS-1-2(config)#router bgp 11
Sub-AS-1-2(config-router)#neighbor 9.9.9.9 prefix-list BLOCK-18 out
```

Ergebnis: (keine Netz emit /18):

```
AS65505#show ip bgp
BGP table version is 43, local router ID is 41.41.41.41
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   2.2.2.2/32       5.5.5.5                              0 1112 2 i
 *>   3.3.3.3/32       5.5.5.5                              0 1112 2 i
 *>   4.4.4.4/32       5.5.5.5                              0 1112 i
 r>   5.5.5.5/32       5.5.5.5                  0           0 1112 i
 *>   6.6.6.6/32       5.5.5.5                              0 1112 i
 *>   7.7.7.7/32       5.5.5.5                              0 1112 i
 *>   9.0.0.0          0.0.0.0                  0       32768 i
 *>   41.41.41.41/32   0.0.0.0                  0       32768 i
 *>   128.130.171.0/24 5.5.5.5                              0 1112 2 i
 *>   128.130.172.0/24 0.0.0.0                  0       32768 i
```

2.5.8 BGP Transit AS

A	AS 2 darf nicht als Transit-AS für 175.45.200.0/21 fungieren.
L	Distribution lists

```
AS2-1(config)#ip access-list standard Set_NoTransit
```

```
AS2-1(config-std-nacl)#deny 175.45.200.0 0.0.7.255
AS2-1(config-std-nacl)#permit any
AS2-1(config-std-nacl)#exit
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#neighbor 192.168.24.4 distribute-list
Set_NoTransit out
```

```
AS2-2(config)#ip access-list standard Set_NoTransit
AS2-2(config-std-nacl)#deny 175.45.200.0 0.0.7.255
AS2-2(config-std-nacl)#permit any
AS2-2(config-std-nacl)#exit
AS2-2(config)#router bgp 2
AS2-2(config-router)#address-family ipv4
AS2-2(config-router-af)# neighbor 192.168.35.5 distribute-list
Set_NoTransit out
```

Betrachten wir wieder das Ergebnis:

```
Sub-AS-1-1#show ip bgp 175.45.200.0
BGP routing table entry for 175.45.200.0/21, version 26
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     16          19          20
  Refresh Epoch 2
  1 1000
    192.168.14.1 from 192.168.14.1 (1.1.1.1)
      Origin incomplete, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

Das Netz wird nur via 192.168.14.1 angeboten.

2.5.9 BGP AS Path Filter

A	Alle Routen, die AS 2 traversieren werden gefiltert und dürfen den BGP Table von Sub-AS-2-1 nicht erreichen.

Betrachten wir dazu auszugsweise zunächst die BGP-Tabelle auf Sub-AS-2-1:

```
Sub-AS-2-1#show ip bgp
BGP table version is 95, local router ID is 6.6.6.6
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
…..
* i  2.2.2.2/32       5.5.5.5                  0    100      0 (11) 2 i
 *>                    4.4.4.4                  0    100      0 (11) 2 i
 * i  3.3.3.3/32       5.5.5.5                  0    100      0 (11) 2 i
 *>                    4.4.4.4                  0    100      0 (11) 2 i
```

```
* i                    5.5.5.5                  0    100      0 (11)
4292935689 i
 * i  10.0.0.1/32      5.5.5.5                  0    100      0 (11) 1
1000 i
 *>                    4.4.4.4                  0    100      0 (11) 1
1000 i
 * i  12.34.0.0/16     5.5.5.5                  0    100      0 (11) 2 1
1000 ?
 *>                    4.4.4.4                  0    100      0 (11) 2 1
1000 ?
 * i  23.45.0.0/16     5.5.5.5                  0    100      0 (11) 1
1000 ?
 *>                    4.4.4.4                  0    100      0 (11) 1
1000 ?
 *>   41.41.41.41/32   4.4.4.4                  0    100      0 (11)
4292935689 i
 * i                   5.5.5.5                  0    100      0 (11)
4292935689
```

Die „rot“ markierten Netze gehen via AS 2.

```
Sub-AS-2-1(config)#ip as-path access-list 1 deny _2_
Sub-AS-2-1(config)#ip as-path access-list 1 permit .*
Sub-AS-2-1(config)#route-map AS_PATH_FILTER permit 10
Sub-AS-2-1(config-route-map)#match as-path 1
Sub-AS-2-1(config-route-map)#router bgp 12
Sub-AS-2-1(config-router)#neighbor 4.4.4.4 route-map AS_PATH_FILTER in
Sub-AS-2-1(config-router)#neighbor 7.7.7.7 route-map AS_PATH_FILTER in
```

Der NAchfolgende Auszug aus der BGP Tabelle zeigt, dass keine Netze mehr aus AS2 vorhanden sind:

```
Sub-AS-2-1#show ip bgp
BGP table version is 27, local router ID is 6.6.6.6
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-
Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   1.1.1.1/32       4.4.4.4                  0    100      0 (11) 1 i
 * i                   5.5.5.5                  0    100      0 (11) 1 i
 r>   4.4.4.4/32       4.4.4.4                  0    100      0 (11) i
 r i                   5.5.5.5                  0    100      0 (11) i
 r>   5.5.5.5/32       4.4.4.4                  0    100      0 (11) i
 r i                   5.5.5.5                  0    100      0 (11) i
```

2.5.10 BPG Peer Groups

A	Auf AS1-1 soll eine peer-group erstellt werden und so viel Router wie möglich (Nachbarn von AS1-1) sollen Mitglieder sein.

Betrachten wir dazu die BGP-Konfiguration auf AS1-1:

```
AS1-1#sh run | sect bgp
router bgp 1
 bgp log-neighbor-changes
 neighbor 2001:DB8::2 remote-as 1000
 neighbor 192.168.12.2 remote-as 2
 neighbor 192.168.13.3 remote-as 2
 neighbor 192.168.14.4 remote-as 1112
 neighbor 203.0.113.2 remote-as 1000
 !
 address-family ipv4
  network 1.1.1.1 mask 255.255.255.255
  no neighbor 2001:DB8::2 activate
  neighbor 192.168.12.2 activate
  neighbor 192.168.12.2 send-community
  neighbor 192.168.12.2 route-map BGP_Communities out
  neighbor 192.168.13.3 activate
  neighbor 192.168.13.3 send-community
  neighbor 192.168.13.3 route-map BGP_Communities out
  neighbor 192.168.14.4 activate
  neighbor 192.168.14.4 send-community
  neighbor 192.168.14.4 route-map BGP_Communities out
  neighbor 203.0.113.2 activate
 exit-address-family
```

Wir sehen, dass die Nachbarn 192.168.12.2, 192.168.13.3 und 192.168.14.4 eine idente Konfiguration aufweisen.

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#neighbor BGP_PeerGroup_1 peer-group
AS1-1(config-router)#neighbor 192.168.12.2 peer-group BGP_PeerGroup_1
AS1-1(config-router)#neighbor 192.168.13.3 peer-group BGP_PeerGroup_1
AS1-1(config-router)#neighbor 192.168.14.4 peer-group BGP_PeerGroup_1
AS1-1(config-router)#address-family ipv4
AS1-1(config-router-af)#neighbor BGP_PeerGroup_1 send-community
AS1-1(config-router-af)#neighbor BGP_PeerGroup_1 route-map
BGP_Communities out
```

Und somit die leicht vereinfachte Konfiguration:

```
AS1-1#sh run | sect bgp
*Oct 15 20:51:21.845: %SYS-5-CONFIG_I: Configured from console by cisco
on consolerouter bgp 1
 bgp log-neighbor-changes
 neighbor BGP_PeerGroup_1 peer-group
 neighbor 2001:DB8::2 remote-as 1000
 neighbor 192.168.12.2 remote-as 2
 neighbor 192.168.12.2 peer-group BGP_PeerGroup_1
 neighbor 192.168.13.3 remote-as 2
 neighbor 192.168.13.3 peer-group BGP_PeerGroup_1
 neighbor 192.168.14.4 remote-as 1112
 neighbor 192.168.14.4 peer-group BGP_PeerGroup_1
 neighbor 203.0.113.2 remote-as 1000
```

2.5.11 BGP Soft Reconfiguration and Route Refresh

A	Sub-AS-2-1 und Sub-AS-2-2 peeren mit soft-reconfiguration

```
Sub-AS-2-1(config)#router bgp 12
```

```
Sub-AS-2-1(config-router)#neighbor 4.4.4.4 soft-reconfiguration inbound
Sub-AS-2-2(config)#router bgp 12
Sub-AS-2-2(config-router)#neighbor 5.5.5.5 soft-reconfiguration inbound
```

2.5.12 BGP Multipath

A	Das Netz 192.168.23.0/24 zwischen AS2-1 und AS2-2 muss von beiden Routern advertised werden – und zwar redundant in Richtung AS1-1.
L	• BGP Multipath: beide Strecken zwischen AS1-1 und AS2-1 bzw. AS2-2 sollen gewählt werden. • Nur maximal 2 Pfade dürfen als bester Pfad gewählt werden.

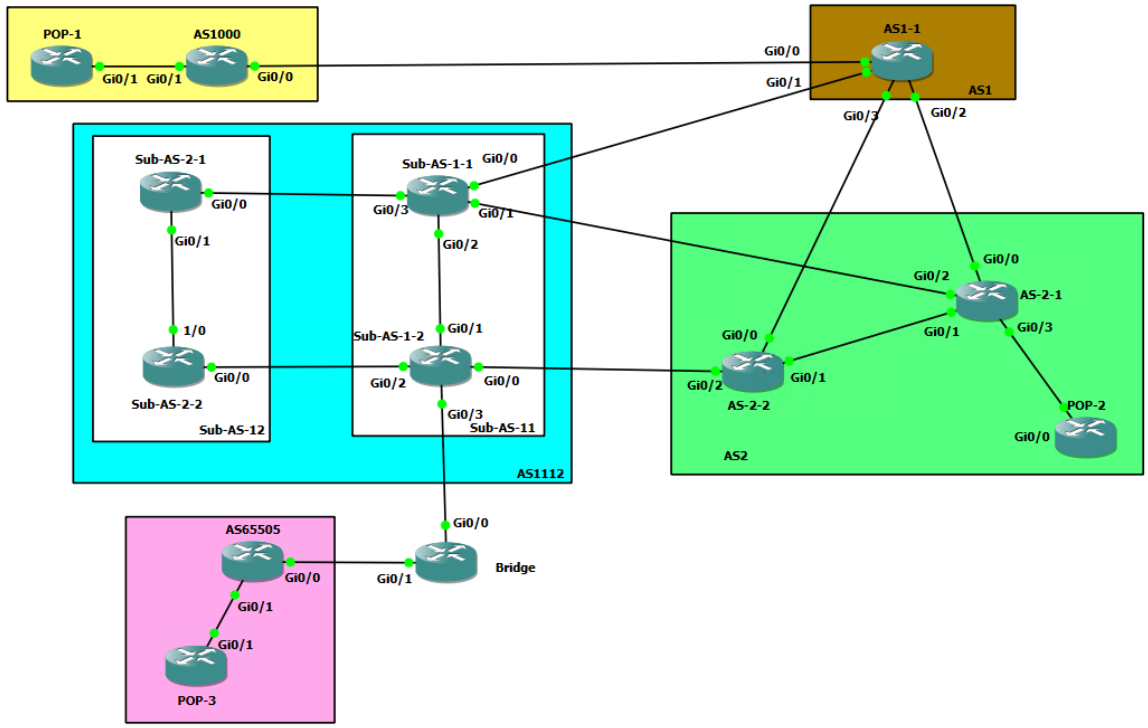
```
AS2-1(config)#router bgp 2
AS2-1(config-router)#address-family ipv4
AS2-1(config-router-af)#network 192.168.23.0 mask 255.255.255.0
```

```
AS2-2(config)#router bgp 2
AS2-2(config-router)#address-family ipv4
AS2-2(config-router-af)#network 192.168.23.0 mask 255.255.255.0
```

```
AS1-1(config)#router bgp 1
AS1-1(config-router)#address-family ipv4
AS1-1(config-router-af)#maximum-paths 2
```

3. Flex-VPN

Basierend auf dieser Topologie werden nun drei weitere Standorte hinzugefügt:



Zwischen diesen Standorten „POP-1“, „POP-2“ und „POP-3“ soll ein Flex-VPN konfiguriert werden; „POP-2“ fungiert dabei als Hub.

Im speziellen wird dieser Flex-VPN mit IkeV2 gesichert – und die notwendigen Routen automatisiert in der jeweiligen Routingtabelle installiert.

Nachfolgend die notwendigen Konfigurationen:

Achtung	Damit das automatische Routen-Update funktioniert, darf es auf den drei „POP-Routern“ keine Defaultrouten geben.
Achtung	Die korrekte Namensauflösung auf den Routern ist essenziell.

Nachfolgend die wesentlichen Grundkonfigurationsschritte:

```
Router(config)#hostname POP-1
POP-1(config)#ip domain-name VPN.5CN
POP-1(config)#ip cef
POP-1(config)#line con 0
POP-1(config-line)#login local
POP-1(config-line)#logging synchronous
POP-1(config-line)#line vty 0 924
POP-1(config-line)#login local
POP-1(config-line)#logging synchronous
POP-1(config-line)#
POP-1(config-line)#int gi 0/1
POP-1(config-if)#des to_ISP
POP-1(config-if)#ip address 128.130.170.2 255.255.255.0
POP-1(config-if)#no shut
POP-1(config-if)#exit
POP-1(config)#ip route 128.130.171.0 255.255.255.0 128.130.170.1
POP-1(config)#ip route 128.130.172.0 255.255.255.0 128.130.170.1
```

```
Router(config)#hostname POP-3
POP-3(config)#ip domain-name VPN.5CN
POP-3(config)#ip cef
POP-3(config)#line con 0
POP-3(config-line)#logging synchronous
POP-3(config-line)#line vty 0 924
POP-3(config-line)#logging synchronous
POP-3(config-line)#
POP-3(config-line)#int gi 0/1
POP-3(config-if)#des to_ISP
POP-3(config-if)#ip address 128.130.172.2 255.255.255.0
POP-3(config-if)#no shut
POP-3(config-if)#exit
POP-3(config)#
POP-3(config)#ip route 128.130.170.0 255.255.255.0 128.130.172.1
POP-3(config)#ip route 128.130.171.0 255.255.255.0 128.130.172.1
```

```
Router(config)#hostname POP-2
POP-2(config)#ip domain-name VPN.5CN
POP-2(config)#ip cef
POP-2(config)#line con 0
POP-2(config-line)#logging synchronous
POP-2(config-line)#line vty 0 924
POP-2(config-line)#logging synchronous
POP-2(config-line)#
POP-2(config-line)#int gi 0/0
POP-2(config-if)#des to_ISP
POP-2(config-if)#ip address 128.130.171.2 255.255.255.0
POP-2(config-if)#no shut
POP-2(config-if)#exit
POP-2(config)#
POP-2(config)#ip route 128.130.170.0 255.255.255.0 128.130.171.1
POP-2(config)#ip route 128.130.172.0 255.255.255.0 128.130.171.1
```

3.1 Flex-VPN-Konfig

- Authentifizierung mit symmetrischen pre-shared-keys via FQDN.
- Via AAA authorization wird eine Defaultroute installiert.
- Am HUB wird ein Tunnel-Template verwendet.

Flex-VPN als Speaker:

```
OP-1(config)#! FlexVPN :: HUB :: Keyring
POP-1(config)#crypto ikev2 keyring IKEV2_KEYRING
POP-1(config-ikev2-keyring)# peer POP-2
POP-1(config-ikev2-keyring-peer)#  address 128.130.171.2
POP-1(config-ikev2-keyring-peer)#  pre-shared-key local cisco123
POP-1(config-ikev2-keyring-peer)#  pre-shared-key remote cisco123
POP-1(config-ikev2-keyring-peer)#exit
POP-1(config-ikev2-keyring)#
POP-1(config-ikev2-keyring)#! FlexVPN :: HUB :: Authorization Policy
POP-1(config-ikev2-keyring)#aaa new-model
POP-1(config)#aaa authorization network FLEXVPN_LOCAL local
POP-1(config)#
POP-1(config)#crypto ikev2 authorization policy IKEV2_AUTHORIZATION
POP-1(config-ikev2-author-policy)#route set interface
POP-1(config-ikev2-author-policy)#route set access-list FLEXVPN_ROUTES
POP-1(config-ikev2-author-policy)#exit
POP-1(config)#
POP-1(config)#ip access-list standard FLEXVPN_ROUTES
POP-1(config-std-nacl)#permit host 12.12.12.12
POP-1(config-std-nacl)#exit
POP-1(config)#
POP-1(config)#int lo 20
POP-1(config-if)#ip address 12.12.12.12 255.255.255.0
POP-1(config-if)#exit
POP-1(config)#
POP-1(config)#! FlexVPN :: HUB :: Profile
POP-1(config)#crypto ikev2 profile IKEV2_PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
POP-1(config-ikev2-profile)#match identity remote fqdn domain VPN.5CN
POP-1(config-ikev2-profile)#identity local fqdn POP-1.VPN.5CN
POP-1(config-ikev2-profile)#authentication remote pre-share
POP-1(config-ikev2-profile)#authentication local pre-share
POP-1(config-ikev2-profile)#keyring local IKEV2_KEYRING
POP-1(config-ikev2-profile)#$oup psk list FLEXVPN_LOCAL
IKEV2_AUTHORIZATION
POP-1(config-ikev2-profile)#exit
POP-1(config)#
POP-1(config)#! FlexVPN :: HUB :: IPSec - Profile
POP-1(config)#crypto ipsec profile IPSEC_PROFILE
POP-1(ipsec-profile)#set ikev2-profile IKEV2_PROFILE
POP-1(ipsec-profile)#exit
POP-1(config)#
POP-1(config)#! FlexVPN :: HUB :: static VTI
POP-1(config)#interface Tunnel 0
POP-1(config-if)#ip address 172.16.1.1 255.255.255.0
POP-1(config-if)#tunnel source gi 0/1
POP-1(config-if)#tunnel destination 128.130.171.2
POP-1(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
POP-1(config-if)#exit
POP-3(config)#! FlexVPN :: HUB :: Keyring
```

```
POP-3(config)#crypto ikev2 keyring IKEV2_KEYRING
POP-3(config-ikev2-keyring)# peer POP-2
POP-3(config-ikev2-keyring-peer)#  address 128.130.171.2
POP-3(config-ikev2-keyring-peer)#  pre-shared-key local cisco123
POP-3(config-ikev2-keyring-peer)#  pre-shared-key remote cisco123
POP-3(config-ikev2-keyring-peer)#exit
POP-3(config-ikev2-keyring)#
POP-3(config-ikev2-keyring)#! FlexVPN :: HUB :: Authorization Policy
POP-3(config-ikev2-keyring)#aaa new-model
POP-3(config)#aaa authorization network FLEXVPN_LOCAL local
POP-3(config)#crypto ikev2 authorization policy IKEV2_AUTHORIZATION
POP-3(config-ikev2-author-policy)#route set interface
POP-3(config-ikev2-author-policy)#route set access-list FLEXVPN_ROUTES
POP-3(config-ikev2-author-policy)#exit
POP-3(config)#
POP-3(config)#ip access-list standard FLEXVPN_ROUTES
POP-3(config-std-nacl)#permit host 13.13.13.13
POP-3(config-std-nacl)#exit
POP-3(config)#
POP-3(config)#int lo 20
POP-3(config-if)#ip address 13.13.13.13 255.255.255.0
POP-3(config-if)#exit
POP-3(config)#
POP-3(config)#! FlexVPN :: HUB :: Profile
POP-3(config)#crypto ikev2 profile IKEV2_PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
POP-3(config-ikev2-profile)#match identity remote fqdn domain VPN.5CN
POP-3(config-ikev2-profile)#identity local fqdn POP-3.VPN.5CN
POP-3(config-ikev2-profile)#authentication remote pre-share
POP-3(config-ikev2-profile)#authentication local pre-share
POP-3(config-ikev2-profile)#keyring local IKEV2_KEYRING
POP-3(config-ikev2-profile)#$roup psk list FLEXVPN_LOCAL
IKEV2_AUTHORIZATION
POP-3(config-ikev2-profile)#exit
POP-3(config)#
POP-3(config)#! FlexVPN :: HUB :: IPSec - Profile
POP-3(config)#crypto ipsec profile IPSEC_PROFILE
POP-3(ipsec-profile)#set ikev2-profile IKEV2_PROFILE
POP-3(ipsec-profile)#exit
POP-3(config)#
POP-3(config)#! FlexVPN :: HUB :: static VTI
POP-3(config)#interface Tunnel 0
POP-3(config-if)#ip address 172.16.1.2 255.255.255.0
POP-3(config-if)#tunnel source gi 0/1
POP-3(config-if)#tunnel destination 128.130.171.2
POP-3(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
POP-3(config-if)#exit
```

```
POP-2(config)#! FlexVPN :: HUB :: Keyring
POP-2(config)#crypto ikev2 keyring IKEV2_KEYRING
POP-2(config-ikev2-keyring)# peer POP-1
POP-2(config-ikev2-keyring-peer)#  address 128.130.170.2
POP-2(config-ikev2-keyring-peer)#  pre-shared-key local cisco123
POP-2(config-ikev2-keyring-peer)#  pre-shared-key remote cisco123
POP-2(config-ikev2-keyring-peer)# !
POP-2(config-ikev2-keyring-peer)# peer POP-2
POP-2(config-ikev2-keyring-peer)#  address 128.130.172.2
POP-2(config-ikev2-keyring-peer)#  pre-shared-key local cisco123
POP-2(config-ikev2-keyring-peer)#  pre-shared-key remote cisco123
POP-2(config-ikev2-keyring-peer)# !
POP-2(config-ikev2-keyring-peer)# exit
```

```
POP-2(config-ikev2-keyring)#exit
POP-2(config)#
POP-2(config)#! FlexVPN :: HUB :: Authorization Policy
POP-2(config)#aaa new-model
POP-2(config)#aaa authorization network FLEXVPN_LOCAL local
POP-2(config)#
POP-2(config)#crypto ikev2 authorization policy IKEV2_AUTHORIZATION
POP-2(config-ikev2-author-policy)#route set interface
POP-2(config-ikev2-author-policy)#route set access-list FLEXVPN_ROUTES
POP-2(config-ikev2-author-policy)#exit
POP-2(config)#
POP-2(config)#ip access-list standard FLEXVPN_ROUTES
POP-2(config-std-nacl)#permit any
POP-2(config-std-nacl)#exit
POP-2(config)#
POP-2(config)#
POP-2(config)#! FlexVPN :: HUB :: Profile
POP-2(config)#crypto ikev2 profile IKEV2_PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
POP-2(config-ikev2-profile)#match identity remote fqdn domain VPN.5CN
POP-2(config-ikev2-profile)#identity local fqdn POP-2.VPN.5CN
POP-2(config-ikev2-profile)#authentication remote pre-share
POP-2(config-ikev2-profile)#authentication local pre-share
POP-2(config-ikev2-profile)#keyring local IKEV2_KEYRING
POP-2(config-ikev2-profile)#$oup psk list FLEXVPN_LOCAL
IKEV2_AUTHORIZATION
POP-2(config-ikev2-profile)#virtual-template 1
POP-2(config-ikev2-profile)#exit
POP-2(config)#
POP-2(config)#! FlexVPN :: HUB :: IPSec - Profile
POP-2(config)#crypto ipsec profile IPSEC_PROFILE
POP-2(ipsec-profile)#set ikev2-profile IKEV2_PROFILE
POP-2(ipsec-profile)#exit
POP-2(config)#
POP-2(config)#! FlexVPN :: HUB :: Dynamic VTI
POP-2(config)#int lo 1
POP-2(config-if)#ip address 172.16.1.254 255.255.255.255
POP-2(config-if)#exit
POP-2(config)#
POP-2(config)#interface Virtual-Template 2 type tunnel
POP-2(config-if)#!tunnel source gi 0/0
POP-2(config-if)#ip unnumbered loopback 1
POP-2(config-if)#tunnel protection ipsec profile IPSEC_PROFILE
POP-2(config-if)#exit
```

3.2 Evaluierung der Konfiguration

Schlüsselfaktor ist die Ikev2 Authentifizierung, sowie die Verschlüsselung des Traffics:

```
POP-2#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf
Status
1         128.130.171.2/500     128.130.170.2/500     none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/3976 sec
```

```
Tunnel-id Local                 Remote                fvrf/ivrf
Status
2         128.130.171.2/500     128.130.172.2/500     none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/3970 sec

 IPv6 Crypto IKEv2  SA
```

Wir sehen, dass beide VPN's up sind (Status Ready). Mit show crypto ipsec sa würde man auch die SA's sehen.

```
POP-2#show crypto ipsec sa | inc ACTIVE
        Status: ACTIVE(ACTIVE)
        Status: ACTIVE(ACTIVE)
        Status: ACTIVE(ACTIVE)
        Status: ACTIVE(ACTIVE)
```

```
POP-2#show crypto ipsec sa | inc peer
   current_peer 128.130.170.2 port 500
   current_peer 128.130.172.2 port 500
```

```
POP-2#show crypto ipsec sa | inc interface
interface: Virtual-Access1
interface: Virtual-Access2
```

Wir sehen also vier SAS's (inbound und outbound, pro VPN zwischen „POP-2" und „POP-1" und „POP-2" und „POP-3". Als Interface für den Flex-VPN wird „Virtual-Access1" und „Virtual-Access2" angezeigt.

Aufgrund des Tunnel-Templates werden nun nach „Bedarf" die realen Tunnel-Interfaces erstellt:

```
POP-2#show derived-config interface Virtual-Acc
POP-2#show derived-config interface Virtual-Access 1
Building configuration...

Derived configuration : 205 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback1
 tunnel source 128.130.171.2
 tunnel destination 128.130.170.2
 tunnel protection ipsec profile IPSEC_PROFILE
 no tunnel protection ipsec initiate
```

```
POP-2#show derived-config interface Virtual-Access 2
Building configuration...

Derived configuration : 205 bytes
!
interface Virtual-Access2
 ip unnumbered Loopback1
 tunnel source 128.130.171.2
 tunnel destination 128.130.172.2
 tunnel protection ipsec profile IPSEC_PROFILE
 no tunnel protection ipsec initiate
end
```

Die entsprechenden Routen werden auf den Geräten „automatisch" installiert:

```
POP-2#show ip route

      12.0.0.0/32 is subnetted, 1 subnets
S        12.12.12.12 is directly connected, Virtual-Access1
      13.0.0.0/32 is subnetted, 1 subnets
S        13.13.13.13 is directly connected, Virtual-Access2
      128.130.0.0/16 is variably subnetted, 4 subnets, 2 masks
S        128.130.170.0/24 [1/0] via 128.130.171.1
C        128.130.171.0/24 is directly connected, GigabitEthernet0/0
L        128.130.171.2/32 is directly connected, GigabitEthernet0/0
S        128.130.172.0/24 [1/0] via 128.130.171.1
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Loopback1
S        172.16.1.1/32 is directly connected, Virtual-Access1
S        172.16.1.2/32 is directly connected, Virtual-Access2
L        172.16.1.254/32 is directly connected, Loopback1
```

Konkret sollten dabei folgende Routen am Hub installiert werden:

- 12.12.12.12: Lokales Loopback auf „POP-2“
- 13.13.13.13: Lokales Loopback auf „POP-3“
- Die jeweiligen Tunnelendpunkte 172.16.1.1 und 172.16.1.2

```
POP-1#show ip route
S*   0.0.0.0/0 is directly connected, Tunnel0
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, Loopback20
L       12.12.12.12/32 is directly connected, Loopback20
     128.130.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       128.130.170.0/24 is directly connected, GigabitEthernet0/1
L       128.130.170.2/32 is directly connected, GigabitEthernet0/1
S       128.130.171.0/24 [1/0] via 128.130.170.1
S       128.130.172.0/24 [1/0] via 128.130.170.1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Tunnel0
L       172.16.1.1/32 is directly connected, Tunnel0
S       172.16.1.254/32 is directly connected, Tunnel0
```

```
POP-3#show ip route
S*   0.0.0.0/0 is directly connected, Tunnel0
     13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       13.13.13.0/24 is directly connected, Loopback20
L       13.13.13.13/32 is directly connected, Loopback20
     128.130.0.0/16 is variably subnetted, 4 subnets, 2 masks
S       128.130.170.0/24 [1/0] via 128.130.172.1
S       128.130.171.0/24 [1/0] via 128.130.172.1
C       128.130.172.0/24 is directly connected, GigabitEthernet0/1
L       128.130.172.2/32 is directly connected, GigabitEthernet0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Tunnel0
L       172.16.1.2/32 is directly connected, Tunnel0
S       172.16.1.254/32 is directly connected, Tunnel0
```

Final der Funktionstest:

```
POP-1#ping 13.13.13.13
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/44/103 ms
POP-1#traceroute 13.13.13.13
Type escape sequence to abort.
Tracing the route to 13.13.13.13
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.254 64 msec 44 msec 22 msec
  2 172.16.1.2 47 msec 79 msec *
```

```
POP-3#ping 12.12.12.12
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/43/77 ms
POP-3#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.254 81 msec 46 msec 28 msec
  2 172.16.1.1 86 msec 90 msec *
```

3 DMVPN

3.1 Vorbereitende Arbeiten

```
AS1000(config)#int gi 0/1
AS1000(config-if)#ip address 128.130.170.1 255.255.255.0
AS1000(config-if)#no shut
AS1000(config)#router bgp 1000
AS1000(config-router)#network 128.130.170.0 mask 255.255.255.0
```

```
AS2-1(config)#int gi 0/3
AS2-1(config-if)#ip address 128.130.171.1 255.255.255.0
AS2-1(config-if)#no shutdown
AS2-1(config)#router bgp 2
AS2-1(config-router)#network 128.130.171.0 255.255.255.0
```

```
POP-2(config-line)#int gi 0/0
POP-2(config-if)#des to_ISP
POP-2(config-if)#ip address 128.130.171.2 255.255.255.0
POP-2(config-if)#no shut
POP-2(config-if)#exit
POP-2(config)#
POP-2(config)#ip route 0.0.0.0 0.0.0.0 128.130.171.1
```