VLANs & Layer3-Switching

Musterlösung

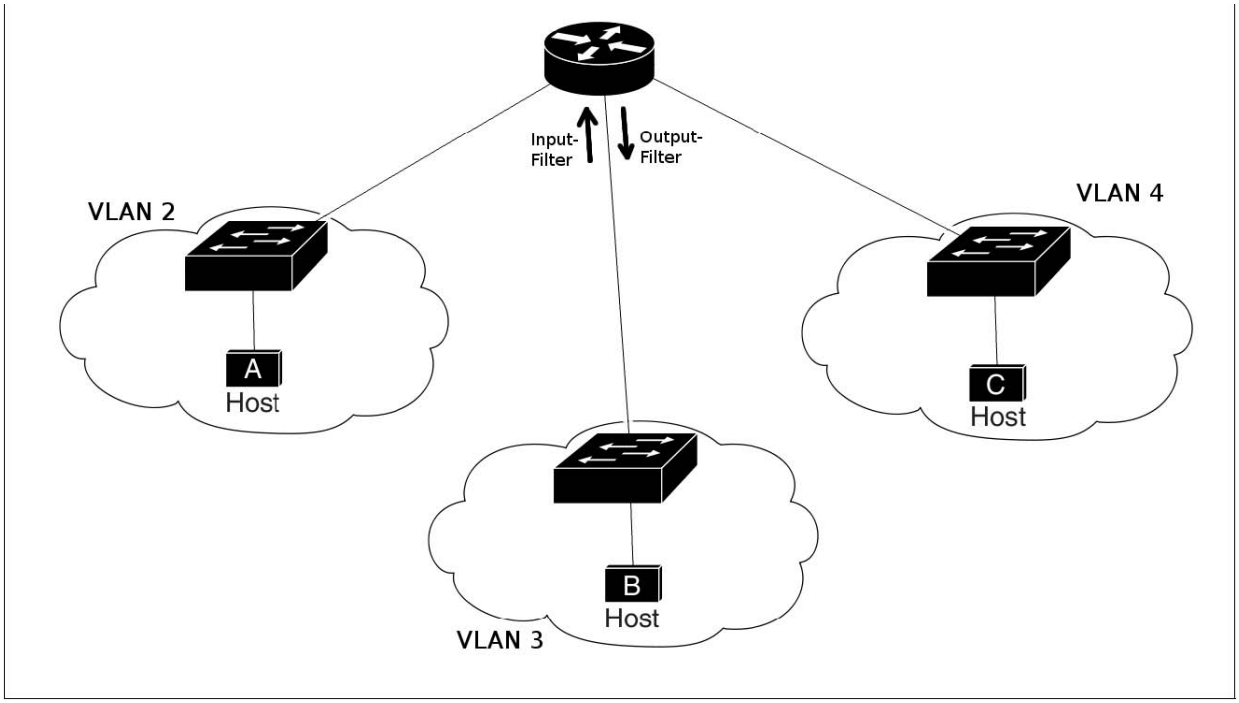

Abbildung 1: Zielaufbau -der Catalyst 3560 fungiert als Router mitsamt drei VLANs wobei Verkehr von/nach VLAN 3 über Filterregeln eingeschränkt wird

alle VMs in gleiches Subnetz und Pings ausführen

(PC-A: 192.168.10.10/24 PC-B: 192.168.10.11/24 PC-C: 192.168.10.12/24)

- Wireshark-Capture auf jeder VM starten (Filter: icrp or arp)
- Ergebnis: Ping geht da alle VMs nun in einem einzigen LAN sind und der Catalyst 3560 per default als einfacher Switch agiert

IP-Adressen wieder zurücksetzen

(PC-A: 192.168.10.10/24 PC-B: 192.168.20.10/24 PC-C: 192.168.30.10/24)

- folgende Dauerpings starten:
  -PC-A: ping -t 192.168.20.10 und ping -t 192.168.30.10
  -PC-B: ping -t 192.168.10.10 und ping -t 192.168.30.10
  -PC-C: ping -t 192.168.10.10 und ping -t 192.168.20.10

- Ergebnis: Ping geht nicht da alle VMs in verschiedenen IP-Subnetzen sind auf MAC-Ebene sind alle VMs jedoch noch in einem LAN (alle VMs empfangen fremde ARP-Pakete)

VLANs 2, 3 und 4 anlegen

interface-id = {fa0/2; fa0/14; fa0/24}
vlan-nr = {vlan2; vlan3; vlan4}

```
Switch>enable
Switch#configure terminal
Switch(config)# interface interface-id
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-nr
Switch(config-if)# exit
```

- Ergebnis: nun sind die VMs auch physikalisch getrennt nicht mal fremde Layer2-Pakete (z. B. ARP) sind mehr zu empfangen

Switch virtual interfaces (SVIs) anlegen

vlan id = {vlan2; vlan3; vlan4} ip adresse = {192.168.10.1; 192.168.20.1; 192.168.30.1} subnetzmaske = 255.255.255.0

```
Switch(config)# interface vlan id
Switch(config-if)# ip address ip adresse subnetzmaske
Switch(config-if)# exit
```

Routing aktivieren

Switch-oben(config)# ip routing

- Ergebnis: Ping geht da der Switch per default alle VLANs über die SVIs routet und nichts fltert (in \ireshark ist zu sehen das die Absender-MAC des Ping Replies nicht die der antwortenden VM sondern des SVIs ist)

Erste (extended) ACL erstellen

```
Switch(config)#access-list 100 permit ip
                                    192.168.10.0 0.0.0.255
                                    192.168.20.0 0.0.0.255
```

ACL auf SVI für VLAN 3 anwenden (direction: outgoing)

```
Switch(config)#interface vlan 3
Switch(config-if)#ip access-group 100 out
Switch(config-if)#exit
```

- Ergebnis: Ping zw. VLAN 2 und 3 geht Rest nicht (Ping Requests vom VLAN 3 gehen bis ins VLAN 4 die Replies aber werden genauso wie Anfragen aus VLAN 4 im Router verworfen)

Zweite (extended) ACL erstellen

```
Switch(config)#access-list 101 permit ip
                                    192.168.20.0 0.0.0.255
                                    192.168.10.0 0.0.0.255
```

ACL auf SVI für VLAN 3 anwenden (direction: incoming)

```
Switch(config)#interface vlan 3
Switch(config-if)#ip access-group 101 in
Switch(config-if)#exit
```

- Ergebnis: Ping zw. VLAN 2 und 3 geht Rest nicht (Pakete vom VLAN 3 zu 4 und umgekehrt werden nun sofort im Router verworfen)

Kontrollfragen

☑ Was ist der Sinn und Zweck der VLAN-Technologie bzw. welchen Vorteil haben VLANs gegenüber dem physischen Aufbau?

Siehe "Theoretischer Hintergrund -VLAN"

☑ Können zwei Hosts aus verschiedenen VLANs miteinander kommunizieren?

Nicht ohne Hilfsmittel da VLANs voneinander getrennt sind. Mit einem Router dazwischen funktioniert die Kommunikation bei korrektem Routing jedoch.

☑ Was ist der Unterschied zwischen einem rein VLAN-fähigen Switch und einem Layer3-Switch?

Ein lediglich VLAN-fähiger Switch bietet die Möglichkeit seine Ports zu virtuellen Netzen (VLANs) zu gruppieren. Die Fähigkeit diese untereinander zu routen ist nicht gegeben. Der Layer3-Switch dagegen ist fähig seine einzelnen VLANs un¬tereinander nach vorgegebenen Regeln zu routen. Anmerkung: Heutzutage verfügen jedoch die meisten VLAN-fähigen Switche auch über solche Layer3-Features.

☑ Annahme: VM „PC-A“ befindet sich in **VLAN 2** und besitzt die IP 192.168.10.100/24 und VM„PC-B“ befindet sich in **keinerlei VLAN** und besitzt die IP 192.168.10.200/24 Es sind keine Zugriffsbeschränkungen in Form von ACLs o. ä. definiert
Frage: Kann A B pingen? Kann umgekehrt B A pingen?

A kann B nicht pingen. Ein VLAN ist von allen anderen Netzen (egal ob VLANs oder physikalische Netze) abgeschottet. Umgekehrt funktioniert auch kein Ping. Ein physikalisches Netz ist auch grundsätzlich von anderen Netzen getrennt.

☑ Annahme: 2 Hosts sind in getrennten VLANs und haben jeweils die IP 192.168.23.42/24
Frage: Was geschieht, wenn der Port des einen Host auf das VLAN umkonfiguriert wird in dem sich der andere Host befindet?

Da nun beide Hosts mit der gleichen IP im selben (V)LAN sind kommt es zu einem IP-Adresskonfikt. Einer der Hosts muss eine neue unbenutzte IP erhalten.

☑ Wie muss eine extended ACL lauten, die sämtlichen Verkehr in ein Netz mit der Adresse 10.12.0.0/16 ausgehend vom Netz 192.168.5.0/24 passieren lässt und den Rest blockt? In welche Richtung muss diese angewandt werden?

```
access-list 102 permit ip      192.168.5.0 0.0.0.255
                               10.12.0.0 0.0.255.255
```

Sie muss in Richtung out angewandt werden da der Verkehr an der Schwelle vom Router zum Zielnetz hinaus gefltert werden soll. Sämtlicher anderer Verkehr wird dank der impliziten letzten Regel deny any gefltert.

☑ Was müsste am Switch konfiguriert werden, wenn an Port FA0/4 ein zusätzlicher PC mit der IP-Adresse 192.168.10.20 angeschlossen werden sollte.

```
Switch(config)# int fa0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
```