Labo computernetwerken I – VLANs & STP

Waar een switch oorspronkelijk een self-learning, eenvoudig toestel was dat enkel gebruikt werd om één LAN op te bouwen, kent deze Ethernet technologie vandaag vele mogelijkheden. Het introduceren van VLANs laat toe dat in een bedrijf alle switches onderling met elkaar verbonden zijn, en dat elk (V)LAN éénder waar er een (L2) toestel staat beschikbaar is. De keerzijde van deze mogelijkheden is dat alle switches geconfigureerd moeten worden om VLANs, trunks, etherchannels, STP, … te ondersteunen.

In dit labo verkennen we enkele van deze configuraties in een simulatieomgeving genaamd Packet Tracer. Deze software laat toe om de typische instellingen die op switches gebeuren aan te raken, zonder effectieve hardware te moeten aankopen.

Netwerk beschrijving

1) Gegevens over de set-up

We vertrekken vanaf een bestaand packer tracer bestand, dat je op Ufora vindt.

De volgende hosts zijn verbonden met de (access layer) switches. De IP-adressen van deze hosts zijn reeds geconfigureerd. Let wel: noch de gateway, noch de DNS-server zijn ingesteld voor de PC hosts; op de CompServ is dit wel al geconfigureerd.

Hostname	IP-address	VLAN	L2 connection
PC10	10.20.101.10/26	10	S1 - Fa0/10
PC50	10.20.101.50/26		S2 - Fa0/10
PC78	10.20.101.78/26	20	S1 - Fa0/18
PC96	10.20.101.96/26		S3 - Fa0/18
PC182	10.20.101.182/25	33	S3 - Fa0/6
PC193	10.20.101.193/25		S2 - Fa0/6
CompServ	10.20.101.253/25		S0 – Gig1/0/6

De switches onderling zijn met elkaar verbonden met de volgende ethernet-poorten[1]:

Device	Port	Port	Device
S0	Gig1/0/1	Fa0/24	S1
S0	Gig1/0/2	Fa0/24	S2
S0	Gig1/0/3	Fa0/24	S3
S0	Gig1/0/4	Gig0/0	Rout
S2	Fa0/23	Fa0/23	S1
S2	Fa0/22	Fa0/22	S3

Het einddoel van dit labo is dat elke host kan pingen of surfen naar www.ugent.be (binnen de simulatie).

2) Opdracht: subnetten

1. Bereken de router interface voor de drie subnetten (die corresponderen met elke VLAN). Kies het **hoogst** mogelijke IP van het subnet. Wat worden de drie IP-adressen voor de router?

2. Stel deze berekende adressen in als default gateway bij alle 6 de host PCs. Configureer eveneens de DNS-server van het bedrijf bij elke host (DNS server is 10.20.101.253).

3. Ga na dat je momenteel _niet_ kan pingen van geen enkele host naar een andere host.
   De switches behoeven duidelijk nog enige configuratie!

[1] Bemerk dat het begrip 'poort' zowel op de transportlaag (TCP poort 80), als in de data-linklaag (ethernet poort) wordt gehanteerd. De context maakt steeds duidelijk wat er bedoeld wordt.

VLAN: access ports

Een host stuurt zijn Ethernet verkeer naar de switch als een normaal Ethernet frame. Als dit verkeer toegang moet krijgen tot een VLAN, is het de switch die deze toegang bepaalt
(en e.g. een VLAN tag toevoegt indien nodig).

Op een switch bepaalt de configuratie van de ethernetpoort dus tot welke VLAN de aangesloten host toegang kan krijgen.

1) Configuratie access ports

Elk merk van switch (HP, Huawei, Juniper, Cisco, …) heeft zijn eigen commando-set die toelaat om de switch in te stellen. In deze simulatieoefening gebruiken we de Cisco IOS CLI. Toegang tot de configuratie krijg je met deze commando's:

```
S1>enable
S1#configure terminal
S1(config)#
```

Of ook kortweg

```
S1>en
S1#conf t
```

Het eerste commando geeft je de nodige rechten (priviliges); het tweede toegang tot het configureren.

Een access port VLAN instellen kan nu als volgt, e.g. voor interface Fa0/1

```
S1(config)#int fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
S1(config-if)#
```

Als je terugkeert naar de initiële prompt, kan je een overzicht van de ingestelde VLANs bekijken met

```
S1#show vlan brief
```

2) Opdracht: access ports

1. Stel op elke switch (s1, s2, s3) de juiste poorten in, opdat alle 6 de host PCs in de juiste VLAN terecht komen.

2. Ga na dat hosts binnen de VLAN naar elkaar kunnen pingen (PC10 naar PC50; PC182 naar PC193). Ga ook na dat PC78 *niet* kan pingen naar PC96 – we bestuderen dit later.

3. Reflecteer over de verbinding s1-s2 en s2-s3. Hoe moeten deze poorten geconfigureerd zijn opdat het netwerk kan werken zoals het nu werkt. Leg uit.

VLANs: trunk

1) Configuratie trunk links

Verbindingen tussen switches behoren niet tot één VLAN: ze dragen het verkeer van meerdere VLANs. Switches voegen een '**`VLAN tag`**' toe als verkeer langs een dergelijke link wordt verzonden. Zo'n link noemen we een trunk link. Vanzelfsprekend kent een link twee kanten, en moeten we dus beide interfaces van de link op een identieke wijze configureren.

Een trunk instellen op een interface van een switch kan als volgt:

```
S1(config)#int fa0/1
S1(config-if)#switchport mode trunk
```

Als je terugkeert naar de initiële prompt, kan je een overzicht van de ingestelde trunk poorten bekijken:

```
S1#show int trunk
```

2) Opdracht: trunk links

1. Stel op switch s0 de juiste poorten in opdat (alle) nodige trunks actief worden in het netwerk.
2. Ga na dat een host uit VLAN 33 de server, die in deze VLAN vertoeft, de CompServ kan pingen.
3. Kan deze host een DNS query (naar www.ugent.be) uitvoeren naar de server?

Router-on-a-stick

VLANs zijn (door software) gescheiden netwerken: als je van het éne netwerk naar het andere netwerk wil verbinden, heb je een router nodig tussen beide netwerken.

Naast de mogelijkheid om meerdere access ports met een router te verbinden, bestaat een mogelijkheid om een trunk link naar de router te installeren. Hier moet de interface op de router dan zo ingesteld worden dat hij VLAN tags kan interpreteren. Een dergelijke configuratie noemt men 'router-on-a-stick'.

1) Configuratie subinterface

Om een VLAN interface toe te voegen op een router, maak je eerste een subinterface aan, die je vervolgens toelaat tot een welbepaalde VLAN.
Eens de subinterface bestaat, kan je er ook een IP-adres aan toekennen. E.g.

```
rout(config)#int gig0/0.27
rout(config-subif)#encapsulation dot1Q 27
rout(config-subif)#ip addr 10.20.123.191 255.255.255.192
```

Subinterfaces worden steeds aangemaakt op een bestaande (fysieke, untagged) interface. Deze moet op een router steeds actief gemaakt worden:

```
rout(config)#int gig0/0
rout(config-if)#no shut
```

Op de router werd reeds een default route ingesteld naar de ISP router (in the cloud):

```
rout(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.254
```

De routeringstabel op de router kan je nagaan met

```
S1#show ip route
```

2) Opdracht: router-on-a-stick

1. Stel op de router de nodige subinterfaces in, opdat de router de default gateway kan zijn voor elke VLAN van je netwerk.

2. Kan elke host de default gateway bereiken? Welke VLAN werkt wel, welke niet?

3) Troubleshoot

Enkel VLAN 33 lijkt te werken, hoewel overal alle VLANs in trunking worden toegelaten. Bekijk het VLAN overzicht op elke switch, en probeer na te gaan hoe elke VLAN actief kan krijgen in je hele netwerk. Hint: https://www.letsconfig.com/how-to-configure-vlan-on-cisco-switch/

1. Kan elke host nu de default gateway bereiken? Opnieuw zal je merken dat er bij PC96 een probleem blijft.

2. Kan PC78 surfen naar www.ugent.be? PC10?

STP

Het Spanning Tree Protocol (STP) organiseert het L2 netwerk zodanig dat er geen actieve loops kunnen bestaan. Echter, de default instelling is niet steeds optimaal. Afhankelijk van welke switch de root switch is, kan een link die je liever actief hebt toch in blocking mode blijven steken.

In je huidige netwerk zijn er 4 spanning trees actief: één voor elke VLAN (en ook nog één voor de default VLAN 1 die je niet gebruikt).

Als je terugkeert naar de initiële prompt, kan je een overzicht van de spanning trees bekijken:

```
S1#show spanning-tree
```

Op een switch kan je de prioriteit hoger instellen, hetzij met een getal, hetzij met een default waarde:

```
S(config)#spanning-tree vlan 1 root primary
```

1) Opdracht: STP

1. Configureer S0 als root voor elk van jouw VLANs.

2. Bekijk op S1, S2 en S3 welke poorten geblokkeerd zijn door het STP protocol.
   Beschrijf in je persoonlijke verslag hoe de tree er uitziet voor jouw drie VLANs

Extra

PC96 is volledig juist geconfigureerd, maar er is duidelijk iets mis met de L2 instellingen voor dit netwerk. Ga de trunks en VLANs na op switch S3. Kan je de fouten opsporen?