Vrijdag 16 juni 2023

Mark van Etten

Packet Tracer

3x 2960 switches

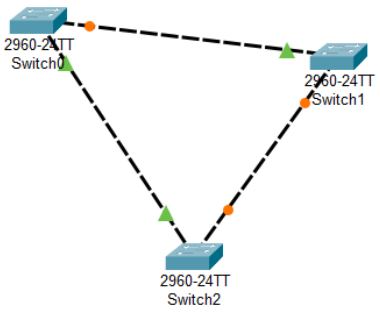
Broadcast storm.

Spanning Tree protocol

Loops met de switches kunnen niet meer ontstaan.

Er wordt een root switch bepaalt.

Loop:



1 Switch bepaalt dat hij de **root switch/root bridge** wordt.

Het verkeer gaat daar eerst heen/doorheen.

Hoe kom je erachter welke de root switch?

enable

show spanning-tree

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00E0.8F15.1336
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     00E0.8F15.1336
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Switch#
```

show mac-addres

Op moment dat je root switch hebt gevonden, en er wordt wat veranderd in de fysieke omgeving bijvoorbeeld nieuwe kabel dan wordt de root switch opnieuw bepaald.

Switches sneller root switch laten bepalen.

Spanning tree portfast

enable

config t

spanning-tree portfast default

Nieuwe root switch maken

Go to the switch you want to make root.

enable

config t

spanning-tree vlan 1 root primary

Alle poorten zijn default gekoppeld aan vlan1 bij Cisco.

VTP – Virtual Trunk port

Elke switch kan een VTP database hebben, deze moet eerst aangemaakt worden.

De vlans moet je kopiëren naar alle andere switches.

VTP automatiseert dat.

VLAN database wordt gekopieerd naar de andere switches.

VLAN aanmaken

Switch cmd

enable

config t

vlan 100

name test

end

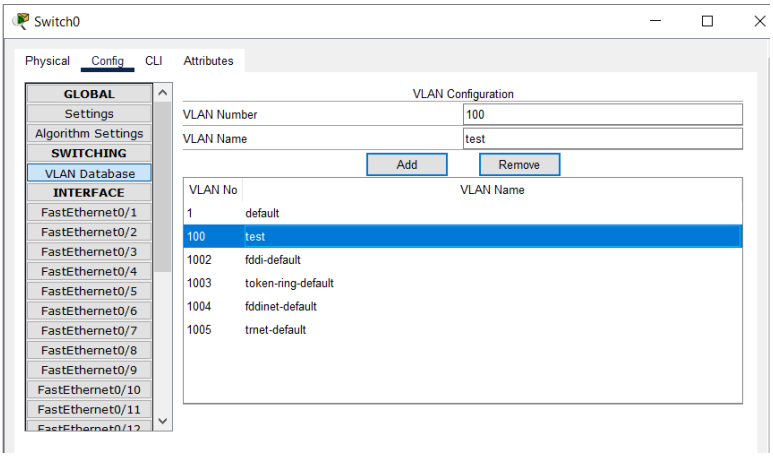
show vlan brief

Je ziet nu: vlan 100 – test

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
100  test                              active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Vlan database



Deze database moet gekopieerd worden naar de andere switches.

Server en een cliënt !

enable

Config t

vtp ?

vtp domain lian

vtp password (Bijvoorbeeld: vtp password Welkom01)

vtp version 2

vtp mode ?

vtp mode server

(transparent doet niks, bijv als er een switch tussen de server en de cliënt zit. 1 2 3. 2 = transparent)

Transparant kan gebruikt worden als security onderdeel. Bijvoorbeeld een extra switch toevoegen aan je netwerk in de vtp transparant mode. De switch is alleen een doorgeefluik.

Na een update van de VTP lijst wordt de informatie wel gewoon doorgestuurd. Pakket oke gewoon doorsturen.

Ga naar een andere switch

enable

config t

vtp domain lian

vtp version 2

vtp mode client

show vlan brief

show vtp status

```
Switch#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : lian
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BC94.8100
Configuration last modified by 0.0.0.0 at 3-1-93 00:48:08

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0xE9 0x3E 0x53 0x15 0xE1 0x4A 0xCD 0x78
                                    0xD8 0x4E 0xDD 0x21 0x08 0x5D 0x16 0x98

Switch#
```

1 server, de rest cliënt

Ga naar switch 0/vtp server

show vtp status

configuration revision = 1

Bij de cliënt was het: configuration revision = 0

Maak een nieuwe vlan aan op de vtp server.

config t

vlan 200

name test2

end

show vtp status

```
Configuration Revision            : 3
```

Dus als de configuration revision (cijfer) van cliënt hoger is dan de server dan wordt er niks geüpdate worden bij de cliënt.

Dus op de vtp server vlan wijzigingen maken, bijv naam wijzigen.
Meerdere keren uitvoeren tot de configuration revision (cijfers) weer gelijk staan.

enable

config t

interface vlan 1

EXAMENTIP: cliënt heeft misschien een hoger configuration revision cijfer dan de server.

Redundantie

HSRP – Hot standby router protocol

Netwerk redundant.

Ook veiliger tegen cyberattacks.

Situatie eerder.

2 routers aanwezig.

1 router moet uit het netwerk voor het netwerk bijvoorbeeld, het netwerkverkeer moet via de andere router gestuurd worden.

Oplossing HSRP:

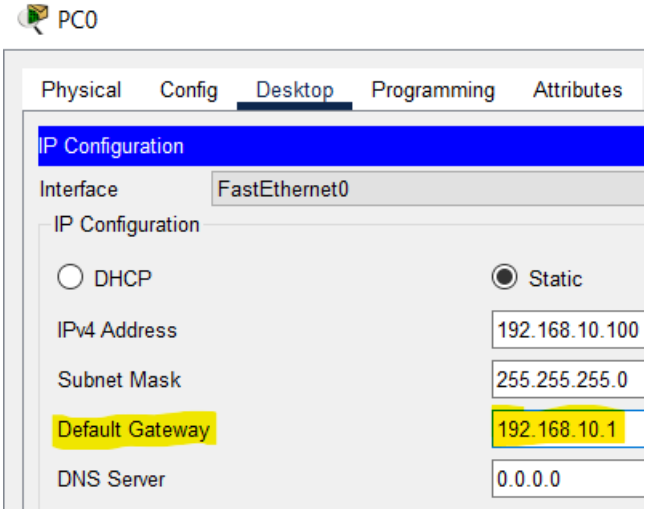
Virtueel ip adres instellen. PC kan dan verbinding maken met dat virtueel ip adres.

Aanwezig: 2x Router met een fixed ip adres.

Er wordt een Virtual Router met een virtual ip adres gemaakt.

De PC connecten met het virtual ip adres, dat is ook de default gateway!

Op PC is de default gateway het virtuele ip adres die is ingesteld bij een router.



Virtueel IP adres moet in hetzelfde subnet zitten!

ping /?

ping -n 1000 192.168.10.1

Eerst ga je naar de hoofd router.

Configureren van HSPR

```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

VLAN

Virtual LAN (VLAN) is een concept waarbij we de apparaten logisch kunnen indelen op laag 2 (datalinklaag). Je kan het zien alsof je meerdere switches hebt die het netwerk scheiden.

VLAN ranges

- VLAN 0 en 4095: Kun je niet gebruiken. Deze zijn gereserveerd.
- VLAN 1:Is het default vlan

• VLAN 2-1001: Een normaal vlan van 2 tot en met 1001 kun je gebruiken.

Configuratie vlan

1. Open cli van een switch
2. enable
3. config t
4. vlan vlan_id (bijvoorbeeld: vlan 2)
5. name vlan_name (bijvoorbeeld: name kantoor1)
6. interface interface_id (bijvoorbeeld: interface fa0/0)
7. switchport mode access
8. switchport access vlan vlan_id (Bijvoorbeeld: switchport access vlan 2)

Configure trunk ports (optional): If you need to configure a trunk port to carry multiple VLANs between switches, use the following command:

```
interface interface_id
switchport mode trunk
```

(Bijvoorbeeld: interface fa/0/0

switchport mode trunk)

9. end
10. copy running-config startup-config OF write memory

Troubleshoot: VLANx is down

Wanneer je een VLANx met een ip-adres hebt en deze de status down heeft. Doe dan het volgende : Breng VLAN1 down met het commando shutdown. Breng daarna VLANx online met no shutdown.

Trunkports

Als je een vlan aanmaakt en deze met andere vlans wil laten uitwisselen dan moet het ip-pakket wel weten in welke VLAN deze zat.

Het ip-pakket krijgt dan extra informatie over de vlan. Deze informatie komt in het 802.1Q header.

Om te zorgen dat dit format wordt ondersteund gebruik je dot1q encapsulation.

Deze stel je in op de switchport die met een andere switch moet communiceren.

interface x/x

switchport mode trunk

optioneel commando, niet altijd beschikbaar op switches

Ga naar de switch trunkport (interface)

config t

switchport trunk encapsulation dot1q

dot1q

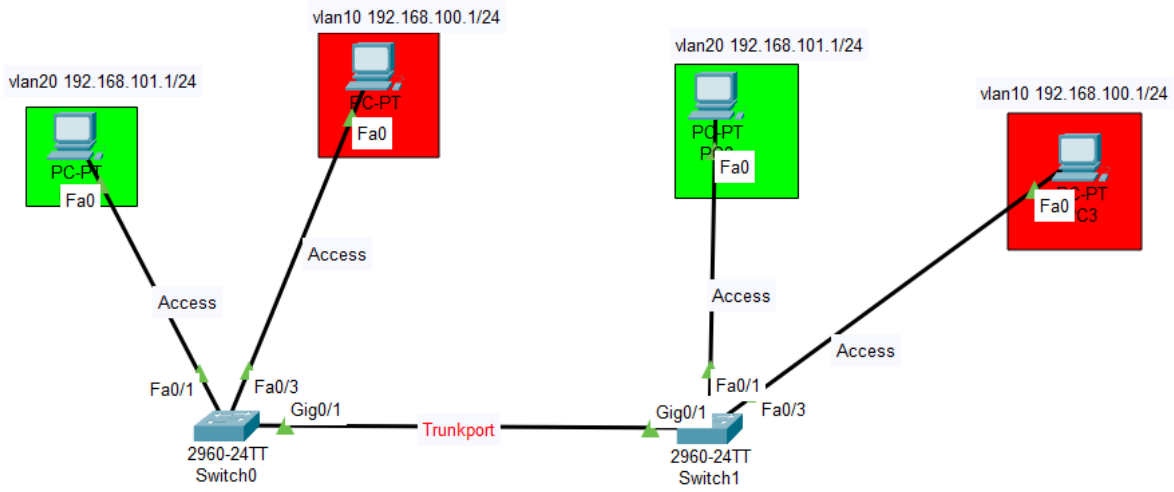
Er gebeurd dat het internetpakket (ethernetframe) verstuurd wordt dat het frame wordt aangepast, toevoeging aan het pakket.

Pakket van A naar B (komt uit vlan 2 of vlan 3). dot1q voegt de vlan toe aan het pakket. Switches weten dan waar het naartoe moet.

Optioneel kun je de switchport beveiligen met allowed.

Hiermee geef je aan welke vlans over de trunk mogen gaan. (xx vervang je met het VLAN-nummer)

switchport trunk allowed vlan 2,3

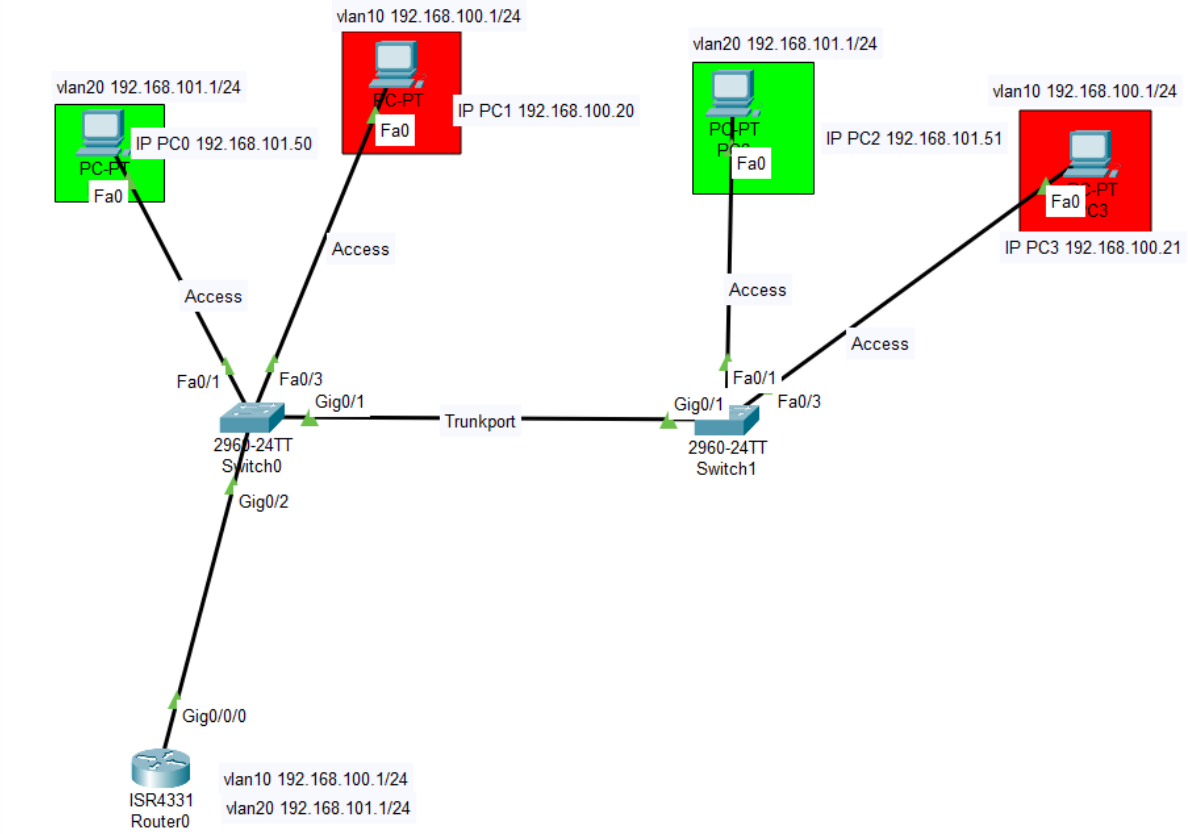


DHCP per VLAN

Zet alle computers op een ander statisch ip adres. Wel in dezelfde range.

Zie foto hierboven.

Nu de ip adressen:



(VLAN10) subinterface

Open de router

enable

config t

interface Gig0/0/0.1

ip address 192.168.100.1 255.255.255.0

no shutdown

end

write memory

show running-config

(VLAN20) subinterface

config t

interface Gig0/0/0.2

ip address 192.168.101.1 255.255.255.0

no shutdown

end

write memory

show running-config

trunking (router)/ Trunking mode

config t

interface Gig0/0/0.1

encapsulation dot1q 10

config t

interface Gig0/0/0.2

encapsulation dot1q 20

Open router cli

enable

config t

ip ?

ip dhcp pool ?

ip dhcp pool vlan10

network 192.168.100.0 255.255.255.0

Open router cli

enable

config t

ip dhcp pool vlan20

network 192.168.101.0 255.255.255.0

DHCP Exclusion vlan

Open de router cli

enable

config t

ip dhcp dhcp excluded-address 192.168.100.20 192.168.100.30

Ga naar je computer.

Zet deze op DHCP.

Zie welke ip adressen je krijgt. De exclusion ip adressen mag je pc NIET krijgen!

Default gateway + DNS Server uitdelen aan de PC’s (vlan10)

enable

config t

ip dhcp pool vlan10

?

default-router 192.168.100.1

dns-server 8.8.8.8

end

copy running-config startup-config

enable

config t

ip dhcp pool vlan20

?

default-router 192.168.101.1

dns-server 8.8.8.8

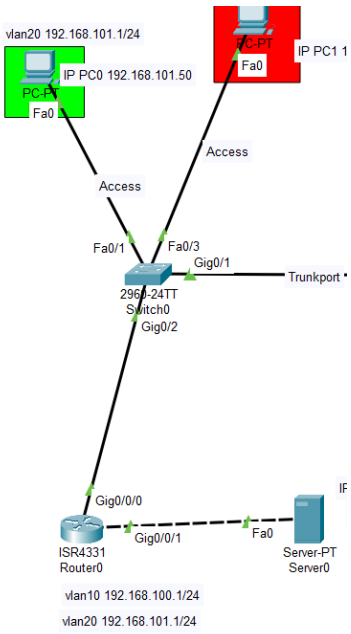
end

copy running-config startup-config

Access Control List (ACL)

Blokkeert of het staat iets toe.

PC maakt verbinding met webbrowser/server. We gaan http verkeer vanaf pc's blokkeren.



Bijvoorbeeld PC0 kan niet naar Server0

Wij gaan nu poort 80 blokkeren.

Pingen moet wel kunnen!

TCP – Transmission Control Protocol

HTTP/HTTPS, FTP/, SSH, maken gebruik van TCP protocol.

Versturen en ontvangen van data.

UDP –

- Streamen van video's/muziek (Youtube, Netflix, Spotify).
- VoIP
- Bellen
- rip routing

Voor snelle data gebruiken.

Er is geen check of data veilig is aangekomen.

Stel data verdwijnt of is niet goed aangekomen dan is het weg.

Bellen via TCP

Alle data wordt in kleine pakketjes gestopt.

- Hallo
- Hoe
- gaat
- het
- met
- jou?

Stel het pakketje 'gaat' is niet verstuurd dan stuurt TCP het alsnog.

Port 443 = https

port 80 = http

De toegang van alle PC's naar de webbrowser van de server zijn geblokkeerd. De server moet nog wel te pingen zijn.

Open router cli

enable

config t

ip access-list extended block_http (Acces list aanmaken)

?

deny ?

deny tcp any ?

OF deny tcp host 192.168.100.1

deny tcp any host 10.10.10.100 eq 80

exit

interface GigabitEthernet0/0/1

ip ?

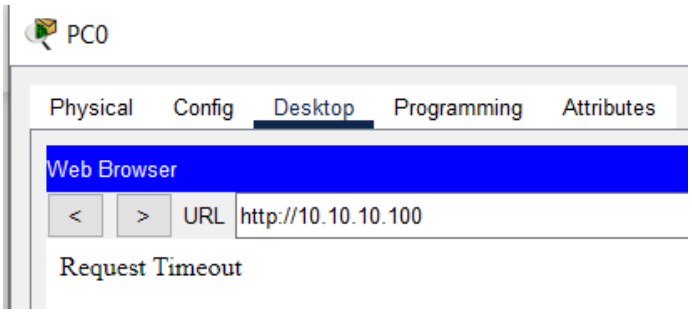
ip access-group block_http ?

ip access-group block_http out

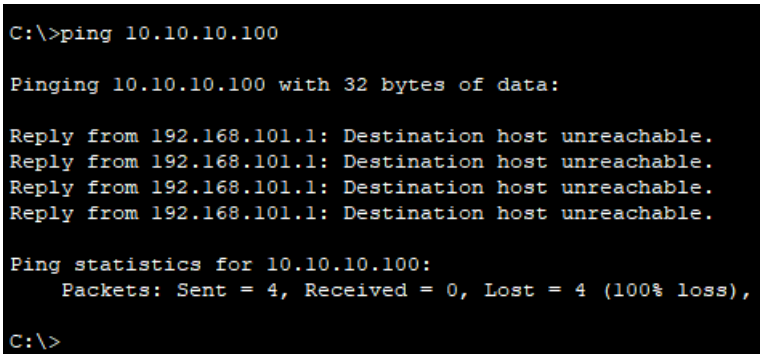
end

copy running-config startup-config

Ga naar PC0 > Desktop > Webbrowser > Voer IP adres in van de server.



Pingen kan nog niet vanaf pc0 naar server0



Kijk terug naar deze commands.

ip access-list extended block_http

deny tcp any host 10.10.10.100 eq 80

Alles wordt standaard geblokkeerd/gedenied.

Er moet dus nog een regel toevoegen!

Oplossing dus

Ga naar de router cli

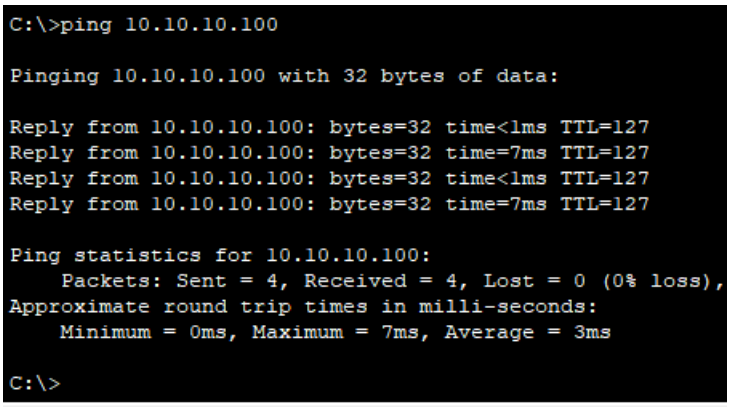
config t

ip access-list extended block_http

permit ip any any

Er is nu een regel toegevoegd. Ga nu naar pc en ping weer van pc naar de server.

Gelukt:



Regel weghalen? Zet ervoor: no

Bijvoorbeeld geconfigureerd bij de verkeerde interface.

config t

interface GigabitEthernet0/0/1

no ip access-group block_http out

Access list bestaat nog wel dan. Maar deze is niet meer gekoppeld aan de interface.

ACL regels worden van boven naar beneden gelezen.

Begin eerst met permit en daarna pas met de deny!

Samenvatting commands

ip access-list extended block_http

deny tcp any host 10.10.10.100 eq 80

deny tcp any host 10.10.10.100 eq 443

permit ip any any

interface GigabitEthernet0/0/1

ip access-group block_http out

Oude lijst verwijderen, nieuwe lijst aanmaken.

Router cli

enable

config t

Ga naar: ip access-list extended block_http

ip access-list extended permit_http (nieuwe lijst aanmaken)

permit tcp any host 10.10.10.100 eq 80

interface GigabitEthernet0/0/1

no ip access-group block_http out

ip access-group http out

OSPF

Dijkstra algoritme

Snelste berekenen van punt A naar punt B in een netwerk.

Multilayer switch

Dat is een router met switch functionaliteiten.

Dat is een switch die kan roteren.

Untagged

zie het als A2 met meerdere banen.

Rijdt er een motor, vrachtwagen, auto?

Oplossing? **dot1q**

Er komt een markering op.

Bij poorten (interface) stel je allowed in! vlan1 vlan2 etc.