**Netwerkbeheer**

**Mark van Etten**

**Inhoud**

[Spanning Tree protocol 3](#_Toc139737735)

[Hoe kom je erachter welke de root switch is? 4](#_Toc139737736)

[Switches sneller root switch laten bepalen. 5](#_Toc139737737)

[Nieuwe root switch maken 6](#_Toc139737738)

[VTP – Virtual Trunk port 7](#_Toc139737739)

[VLAN aanmaken voor VTP oefening, de vlan is nog niet gekoppeld aan een interface 8](#_Toc139737740)

[VTP – Virtual Trunk port configureren 9](#_Toc139737741)

[1 switch server maken (VTP) 9](#_Toc139737742)

[Troubleshooting VTP 11](#_Toc139737743)

[**EXAMENTIP: cliënt heeft misschien een hoger configuration revision cijfer dan de server.** 11](#_Toc139737744)

[HSRP – Hot standby router protocol 12](#_Toc139737745)

[Oplossing HSRP: 13](#_Toc139737746)

[Configureren van HSPR 13](#_Toc139737747)

[VLAN 15](#_Toc139737748)

[Configuratie vlan 15](#_Toc139737749)

[Troubleshoot: VLANx is down 15](#_Toc139737750)

[Trunkports 16](#_Toc139737751)

[Werkt de trunkverbinding? Hoe testen? 16](#_Toc139737752)

[dot1q 18](#_Toc139737753)

[Optioneel kun je de switchport beveiligen met allowed! 19](#_Toc139737754)

[**DHCP per VLAN** 19](#_Toc139737755)

[**DHCP Exclusion vlan** 22](#_Toc139737756)

[**Default gateway + DNS Server uitdelen aan de PC’s (vlan10)** 22](#_Toc139737757)

[**Access Control List (ACL)** 24](#_Toc139737758)

[ACL – (Herhaling + extra 7-7-2023) 28](#_Toc139737759)

[Inter-vlan routing 32](#_Toc139737760)

**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:**

Afbeelding met schermopname, lijn, diagram

Automatisch gegenereerde beschrijving

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 is?

|  |
| --- |
| enable |
| show spanning-tree |

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, scherm, software

Automatisch gegenereerde beschrijving

|  |
| --- |
| 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 |
| configure terminal |
| spanning-tree portfast default |

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

## Nieuwe root switch maken

**Go to the switch you want to make root!**

|  |
| --- |
| enable |
| configure terminal |
| spanning-tree vlan 1 root primary |

*Alle poorten zijn default gekoppeld aan vlan1 bij Cisco.*

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

# VTP – Virtual Trunk port

**VLAN Trunking Protocol is het protocol dat ervoor zorgt dat VLAN databases automatisch worden gekopieerd naar andere switches.**

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

Maak op een server nieuwe vlans aan! Niet op een cliënt (switch).

1 server en niet meer.

VTP server werkt alleen met een trunkverbinding! Eerst een trunkverbinding configureren/aansluiten!

Show vlan

## VLAN aanmaken voor VTP oefening, de vlan is nog niet gekoppeld aan een interface

**Ga naar een switch cli**

|  |
| --- |
| enable |
| configure terminal |
| vlan 100 |
| name lianIT |
| end |
| show vlan brief |
| Je ziet nu: vlan 100 – lianIT |
| copy startup-config running-config |

Vlan database Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving

Deze database moet gekopieerd worden naar de andere switches!

# VTP – Virtual Trunk port configureren

**Zorg dat er een trunkport is tussen 2 switches!**

**1 Server en meerdere cliënt switches!**

## 1 switch server maken (VTP)

|  |
| --- |
| enable |
| Config t |
| *vtp ?* |
| vtp domain lian |
| vtp password (Bijvoorbeeld: vtp password Welkom01) |
| vtp version 2 |
| *vtp mode ?* |
| vtp mode server |
| end |
| copy running-config startup-config |

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

*(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.

1 server, de rest cliënt

**Ga naar de andere switches, deze worden cliënts**

|  |
| --- |
| enable |
| configure terminal |
| vtp domain lian |
| vtp password Welkom01 |
| vtp version 2 |
| vtp mode client |
| end |
| show vlan brief |
| show vtp status  Afbeelding met tekst, schermopname, Lettertype, nummer  Automatisch gegenereerde beschrijving |

**Ga naar de 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.**

|  |
| --- |
| configure terminal |
| vlan 200 |
| name test2 |
| end |
| show vtp status |

**Dus als de configuration revision (cijfer) van cliënt hoger is dan van 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.**

## Troubleshooting VTP

• Configuration revision op de VTP client is lager dan VTP server.

• VTP Version is gelijk met server en client.

• VTP Domain Name is gelijk (hoofdletter gevoelig)

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

**Redundantie**

# HSRP – Hot standby router protocol

Het Hot Standby Router Protocol (HSRP) is een netwerk redundantie protocol van Cisco voor het realiseren van een redundant netwerk.

Met een redundantie protocol wordt automatische failover constructie tussen twee of meerdere routers mogelijk. Met dit protocol is de router als single point of failure (SPOF) onmogelijk. Het redundantie protocol gaat werken wanneer één of meerdere interfaces op een router, of de gehele router, uitvalt.

Netwerk redundant.

Ook veiliger tegen cyberattacks.

**Er zijn verschillende router redundantie protocollen; hier de belangrijkste:**

VRRP staat voor Virtual Router Redundancy Protocol. Het is een open protocol: dat betekent dat deze op andere netwerkapparaten, ongeacht het merk, beschikbaar is.

**Virtual Router**

Voor deze protocollen wordt gebruikt gemaakt van een Virtual (Router) IP. Via deze virtuele router wordt de default gateway op ingesteld.

**Preempt**

**Een Preempt is een stetting die je kan gebruiken om de 'oorspronkelijke' active router weer actief te maken.**

Voorbeeld:

Router A is active en preempt.

Router B is standby.

Wanneer Router A down gaat neemt Router B het over.

Wanneer Router A weer online is gaat Router B naar standby.

Zonder Preempt gebeurt dit niet en blijft Router B active.

**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. Afbeelding met tekst, schermopname, software, Webpagina

Automatisch gegenereerde beschrijving

**Virtueel IP adres moet in hetzelfde subnet zitten!**

*ping /?*

ping -n 1000 192.168.10.1

# Configureren van HSPR

**Eerst ga je naar de hoofd router.**

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Virtual Router (IP), default gateway cliënts (pc’s) will be that ip adress from all the cliënts.

Router 1

Go to the interface. Open cli and put in these commands.

enable

configure terminal

interface g0/1

ip address 192.168.10.2 255.255.255.0

standby version 2

standby 1 ip 192.168.10.1

standby 1 name HSRP\_Test

standby 1 priority 150

standby 1 preemt

no shutdown

end

copy running-config startup-config

Router 2

enable

configure terminal

interface g0/1

ip address 192.168.10.3 255.255.255.0

standby 1 name HSRP\_Test

standby version 2

standby 1 ip 192.168.10.1

no shutdown

end

copy running-config startup-config

# 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)

1. end
2. copy running-config startup-config

## 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

Trunkverbinding

Meerdere vlans over 1 verbinding laten gaan.

Trunkverbinding, Tussen 2 switches.

Tussen switch en pc; Acces verbinding.

Acces verbinding.

Port security instellen.

VLAN2 bijvoorbeeld op instellen.

## Werkt de trunkverbinding? Hoe testen?

|  |
| --- |
| show interfaces trunk |

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

|  |
| --- |
| show running config |

Ga naar de interface en kijk wat er staat!



# 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.

**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

**Ga naar een router of switch**

|  |
| --- |
| enable |
| config t |
| interface (gigabitethernet 0/0/1(.1 (subinterfacenumber)) |
| encapsulation dot1q vlanid (101) |
| end |
| copy running-config startup-config |

## 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

**Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving**

**DHCP per VLAN**

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

Zie foto hierboven.

Nu de ip adressen: Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

**(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

copy running-config startup-config

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

**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.

**Access Control List (ACL)**

**Access-list (ACL) is een set regels die is gedefinieerd voor het regelen van het netwerkverkeer en het verminderen van netwerkaanvallen.**

**ACL’s worden gebruikt om verkeer te filteren op basis van de set regels die zijn gedefinieerd voor het in- of uitgaan van het netwerk.**

Blokkeert of het staat verkeer toe.

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

Bijvoorbeeld PC0 kan niet naar Server0Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

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.

Afbeelding met tekst, schermopname, scherm, Lettertype

Automatisch gegenereerde beschrijving

Pingen kan nog niet vanaf pc0 naar server0

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**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: Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

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

# ACL – (Herhaling + extra 7-7-2023)

Ga naar de PC > Ga naar de Webbrowser > Typ het IP adres van de server in. Afbeelding met tekst, schermopname, software, Computerpictogram

Automatisch gegenereerde beschrijving

Deze medewerkers mogen bij deze server en deze medewerkers niet.

Deze pc mag niet bij de webserver mogen! Dichtzetten met een ACL.

**Ga naar router**

|  |
| --- |
| enable |
| configure terminal |
| *ip access-list ?* |
| *ip access-list extended ?* |
| ip access-list extended block\_http (dit is de naam) |
| *deny ?* |
| deny tcp |
| *deny tcp ?* |
| deny tcp |
| deny tcp 192.168.20.1 ? |
| *Source wildcard bits = Tegenovergesteld wat er staat van het subnetmask. 255.255.255.0 wordt: 0.0.0.255*  deny tcp 192.168.10.5 0.0.0.255 |
| *deny tcp 192.168.10.5 0.0.0.255 host 192.168.10.5 ?* |
| (Poortnummer 80 = http) |
| deny tcp 192.168.10.5 0.0.0.255 host 192.168.10.5 eq 80 |
| permit any any |

(Permit altijd onderaan)!

**Geconfigureerd nu:**

* Accesslist naam gegeven
* Extended

**Nu access list koppelen**

Ga naar gui Router waarmee pc is verbonden.

Ga naar de interface router waarmee de pc is verbonden.

|  |
| --- |
| *ip access-group ?* |
| ip access-group block\_http |
| *ip access-group block\_http ?* |
| ip access-group block\_http inbound |

Je kijkt naar de richting waarvan het verkeer komt. Nu dus van server naar pc. Dat is inbound!

Je kunt moeten pingen van pc naar server. Je mag van pc via de webbrowser niet naar ip adres van server!

**Deel 2.**

**Wireless.**

AP-PT (packet tracer apparaat)

Stel de instelling in bij config.

Afbeelding met tekst, computer, schermopname, scherm

Automatisch gegenereerde beschrijving

**OSPF -**

Commando’s staan al in het technisch ontwerp. Dit uitvoeren.

**B1-K2**

**Kerntaak 2/werkprocess 2**

**4-5 testen moet je doen! Niet oplossen, constateren, conclusie.**

Test of start-up config aanwezig is?

show flash:

Welke bestanden zijn er aangemaakt op router, switch?

**Je schrijft in het testformulier:** Ik zie op deze router of switch dat blabla niet aanwezig is. Je lost het Niet op!

**Omschrijving wat je gaat testen.**

Op alle devices uitvoeren!

**Uitvoering: Commando opschrijven welke je hebt gebruikt.**

**Aangeven: Hoe ga je testen? Met welk commando.**

**Geef aan wat je verwacht!**

Ik verwacht dat er een startup-config file aanwezig is/dat ik die zie

**Impact aangeven! Risico.**

**Afsluiten. Advies geven, wat te doen op het op te lossen?**

Alles wat je configureert opslaan met commando: copy running startup-config (ofzo ik gebruik tab toets in packet tracer).

**Examentips**

* Alle machines vast ip adres. Controleren en anders instellen.
* Alle machines kunnen elkaar pingen, zoals default gateway.
* Zet de ACL als laatste aan/configureer die als laatste!!

# Inter-vlan routing

Met een layer 3 switch (een multilayer switch) kun je je een switch ook als router gebruiken. Deze constructie noemen ze ook wel 'inter-vlan' routing.

Met een layer 3 switch kun je van netwerk x naar netwerk y packets versturen.

**Om te werken met inter-vlan, zorg dat de layer 3 switch ip-routing enabled is.**

En dat je vlan interface een ip-adres heeft.

**Commando’s**

|  |
| --- |
| #SW1(config) ip routing |
| #SW1(config) interface vlan 10 |
| #SW1(config-if)ip address 10.1.10.1 255.255.255.0 |