# Implementatie

Sedric Yaovi Lodonou

Opgesteld op 26/4/2020

Versie 1

Door de … zijn de verschillende oplossingen niet geïmplementeerd. Er is dus geen implementatie documentatie gemaakt maar verschillende scripts. Voor elke oplossing is er een script gecreëerd. Deze scripts kunnen in de toekomst geïmplementeerd worden wanneer het mogelijk is.

De scripts bestaan uit 2 delen. Deel a van het script is het script die uitgevoerd moet worden voor de implementatie voor de verschillende problemen, deel b is een kleine deel die zorgt voor het controleren van de resultaten van het uitgevoerde script. Deel c en d is deel a en b maar met uitleg van de code.

# Bittorent - Implementatie

### Bittorrent blokeren met Nbar

### Script: implementatie

!

*ip cef*

*class-map match-any CM-BLOCK-BT*

*match protocol bittorrent*

*match protocol kazaa2*

*match protocol gnutella*

*exit*

*policy-map PM-BLOCK-BT-POLICY*

*class CM-BLOCK-BT*

*drop*

*!!police cir 2000000*

*!!confirm-action drop*

*!!exceed-action drop*

*exit*

*exit*

*exit*

*int gig 0/1*

*ip nbar protocol-discovery*

*service-policy input PM-BLOCK-BT-POLICY*

*service-policy output PM-BLOCK-BT-POLICY*

*end*

*!*

*!*

### Script: Controle

show policy-map interface gig 0/1

Show running-config policy-map

Show running-config class-map

### Script: inplementatie uitleg

* + - CEF1 moet aangezet worden, Peer-to-Peer kan niet geblokkeerd worden als dit uitstaat.

ip cef

* + - Maak een clasc-map genaamd CM-BLOCK-BT

  class-map match-any CM-BLOCK-BT

* + - Macht de class map met de verschillende protocollen die verwerkt moeten worden. We gaan hier niet alleen bittorrent zetten, maar ook twee andere grote P2P protocollen.

  match protocol bittorrent

  match protocol kazaa2

match protocol gnutella

  exit

* + - Maak een policy map. Hierin worden alle regels omtrent de actie die genomen moeten worden , prioriteiten etc… eerste stap is de gemaakte policy erin te steken.

  policy-map PM-BLOCK-BT-POLICY

* + - Hiermee wordt alle verkeer die gelijk is aan het verkeer van de map CM-Block-BT direct gedropt

  class CM-BLOCK-BT

drop

* + - OF tweede optie is het limiteren door de bps(Bit Per Second) to limiteren , als het hoger is dan 200 moet het gedropt worden.

!!police cir 200

!!confirm-action drop

#exceed-action drop

  exit

  exit

  exit

* + - Ga naar de interface waar dit toegepast moet worden in het netwerk, want daar moet nbaar aangezet worden

  int gig 0/1

  ip nbar protocol-discovery

* + - The policy map moet toegepast worden op deze interface. Hier kan er ook vermelden worden of het een input of output is.

  service-policy input PM-BLOCK-BT-POLICY

  service-policy output PM-BLOCK-BT-POLICY

### Script: Controle uitleg

* + - Voor alle statistieken voor pakketjes die geconfigureerd zijn voor alle service policies op deze interface.

show policy-map interface gig 0/1

* + - Voor alle policy map configuraties

Show running-config policy-map

* + - Voor class map configuraties

Show running-config class-map

### Bittorent blokkeren met ACL

### Script: implanteren

!

Ip access-list 101 deny tcp ip 10.20.0.0 0.0.255.255 eq 6881-6889

#Op de inerface die naar Telenet als belgacon gaat

conf t

inter gig 0/2

Ip access-group 101 in

!

### Script: controleren

Show access-list ipv4 101

Copy access-list ipv4 101 {destination-acl}

Clear access-list ipv4 101

### Script: implantatie uitleg

* + - Maak acl mer nr 101. Deze acl laat geen tcp protocol die komt van poort range 6881 tot 6889 in het netwerk 10.20

Ip access-list 101 deny tcp ip 10.20.0.0 0.0.255.255 eq 6881-6889

#Op de inerface die naar Telenet als belgacon gaat

conf t

* + - Zet de acl in de juiste interface, zet het op inbound of outbound

inter gig 0/2

Ip access-group 101 in

### Script: controle uitleg

* + - Zie acl met nr 101

Show access-list ipv4 101

* + - Maak een copy van een bestaand acl en creëer zo een nieuwe acl

Copy access-list ipv4 101 {destination-acl}

* + - Verwijder de counter van de acl. Hierdoor gaat de counter op 0 staan en Kan er getest worden om te zien of het verkeer werkelijk geblokkeerd word

Clear access-list ipv4 101

# Telephonie / VOIP - Implementatie

### Auto-QoS

### Script: Implamentatie

### Script: Controle

### Script: implamentatie uitleg

### Script: Controle uitleg

access-list 102 permit udp any any range 16384 32776

class-map match-any LLQ\_voip

match access-group 102

match precedence critical

Exit

^z

Conf t

Policy-map LLQ\_voip

Class LLQ\_voip

bandwidth 3500

priority 3500

set precedence critical

exit

^z

Conf t

Int gig 0/2 (interface naar internet)

Service-output output LLQ\_voip

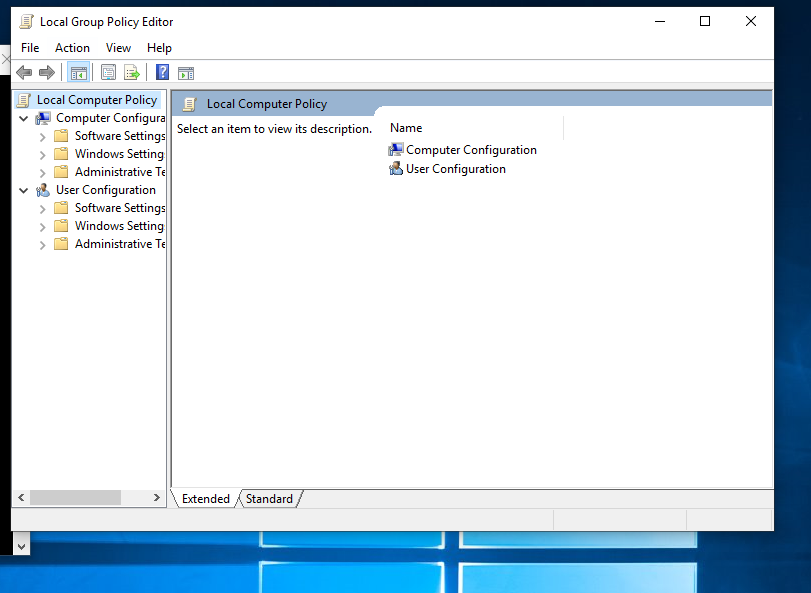
^z

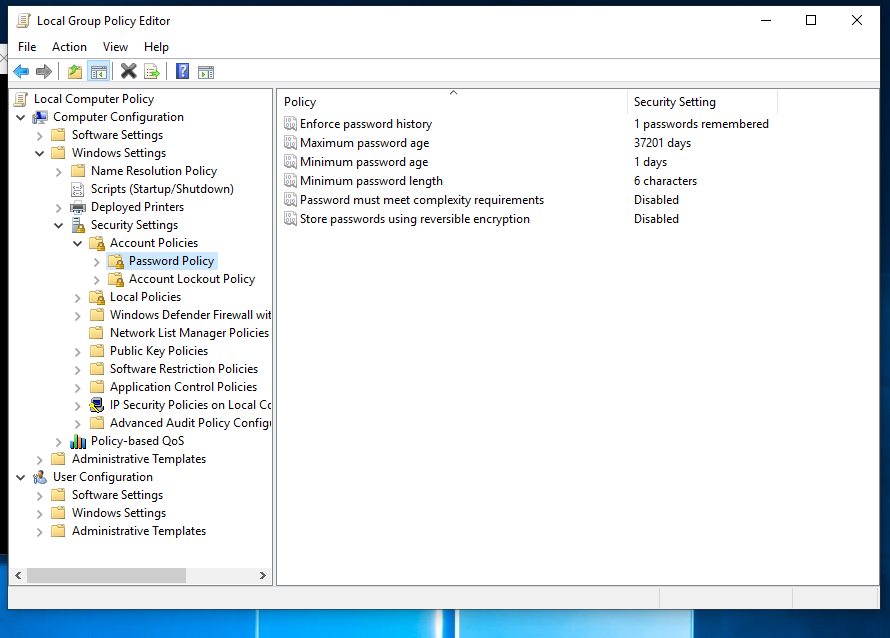
Show policy-map interface gig 0/2

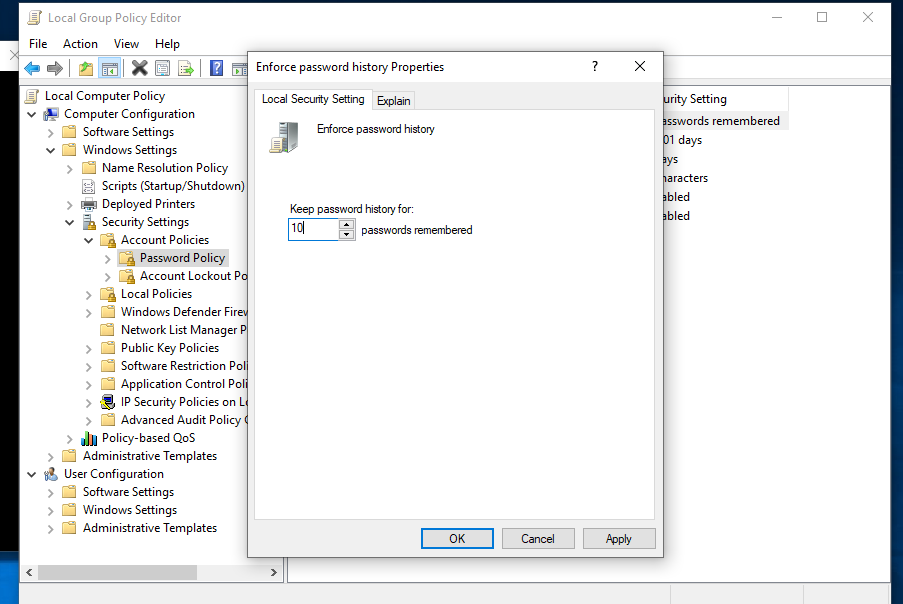
# Wachtwoorden- Implementatie

### Enforce password history

Hierdoor worden alle vorige wachtwoorden onthouden. Dit betekent dat er geen oude passorden opnieuw gebruikt kunnen worden. Bij het ingeven van een nieuw wachtwoord wordt eerst de lijst van opgeslagen wachtwoorden gecontroleerd, als het gekozen wachtwoord niet in de lijst is dan wordt het nieuwe wachtwoord geaccepteerd. Momenteel moeten de 10 vorige wachtwoorden opgeslagen worden.

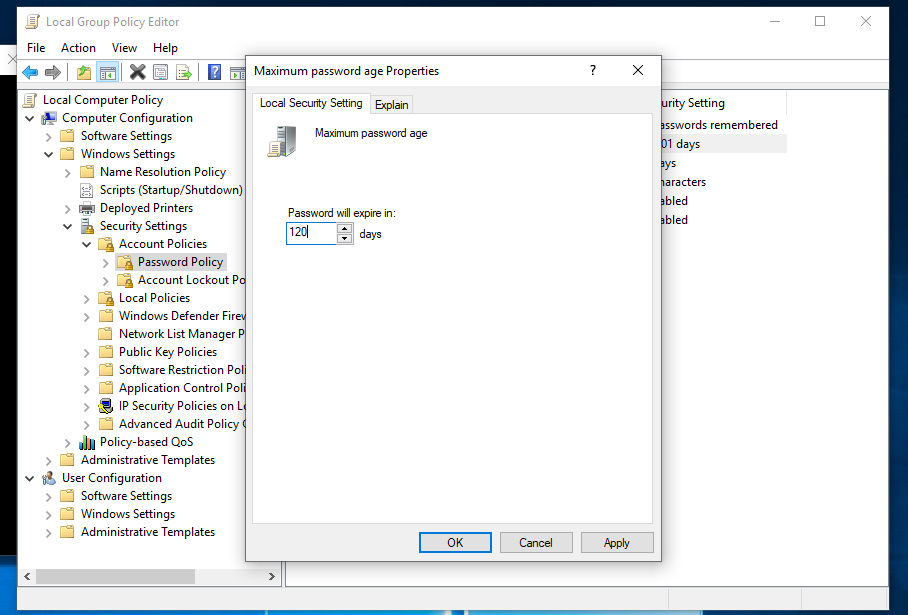






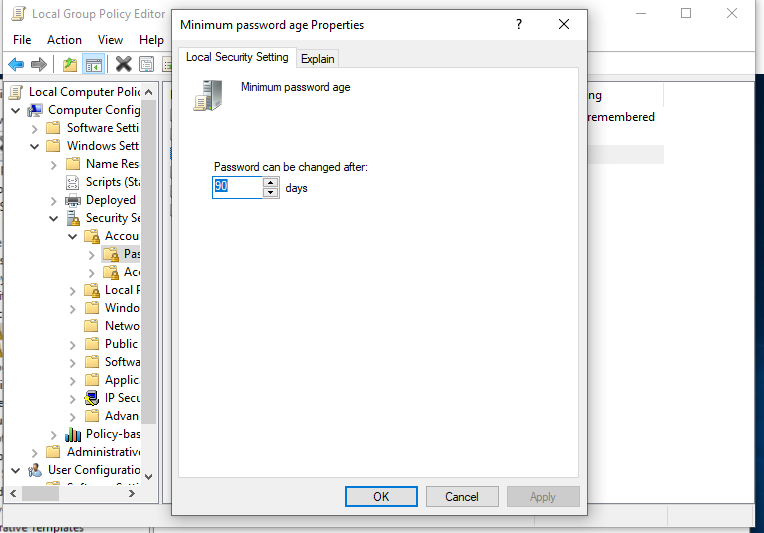
### “Max Password age”

Het wachtwoord moet ten laatste in 150dagen (5 maanden is de beste optie. Momenteel staat alles op 4 maanden omdat dit het eerste advies was) veranderd worden.



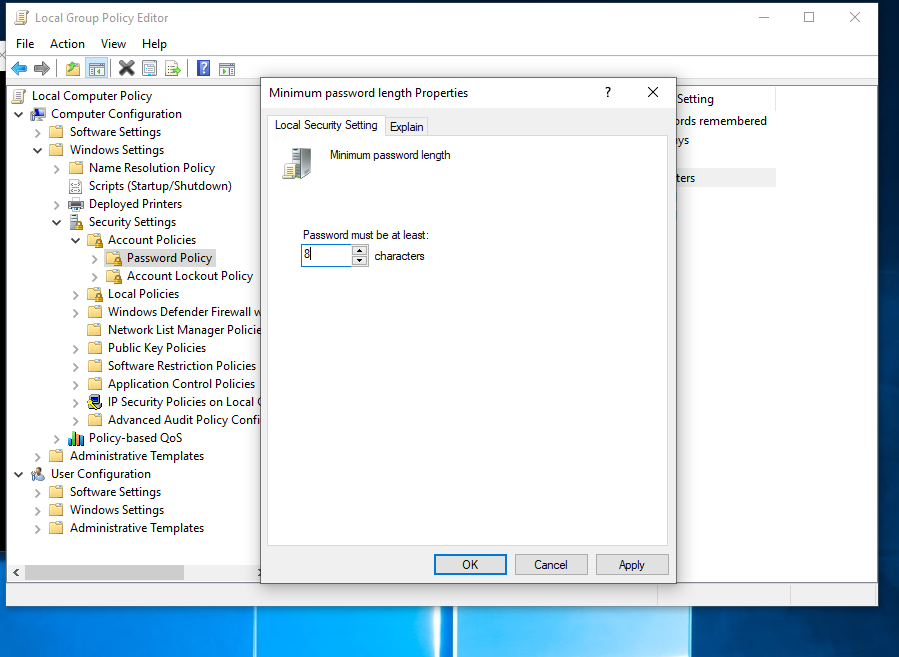
### Min Passwoord age

Na hoeveel maanden MAG het wachtwoord al veranderd worden. Voor drie maanden kunnen de gebruikers hun wachtwoord niet veranderen. Na 90 dagen kunnen de gebruikers hun wachtwoord veranderen tot de *Max Age*



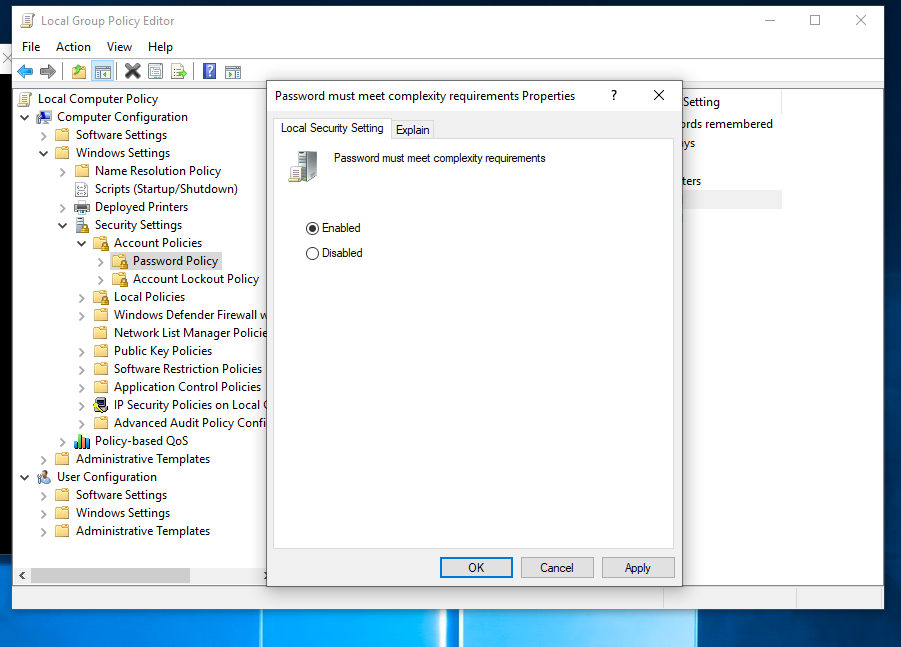
### Min Passwoord Length

Wachtwoord moet min een aantal karakters hebben. Die verhoogd de moeilijkheid graad van het wachtwoord. De min lengte hier is 8



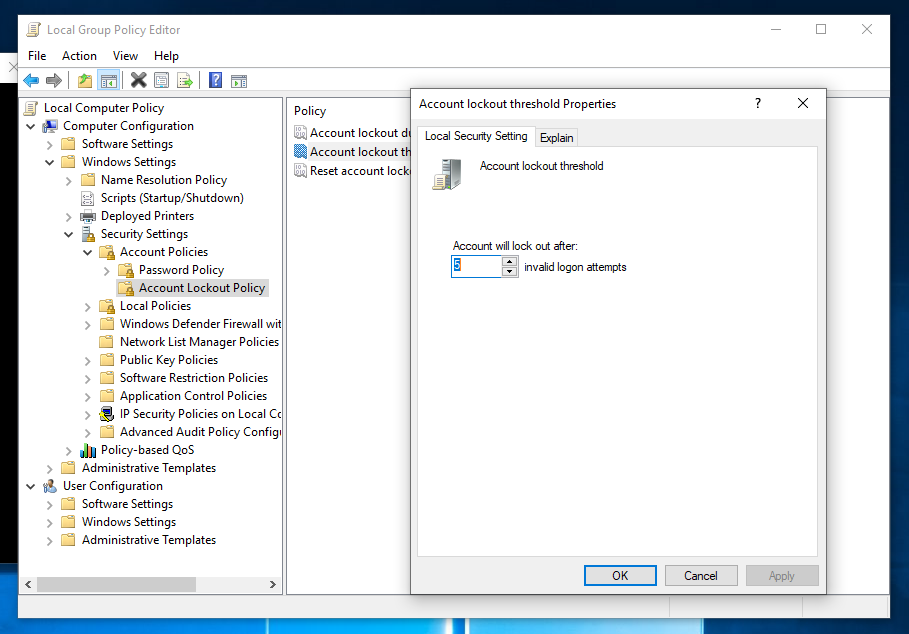
### Password complexity requirement

Dit zorgt ervoor dat er een wachtwoord gegeven wordt die een beetje moeilijker is dan gewoonlijks. Deze optie zorgt ervoor dat de wachtwoord verplicht een hoofdletter, kleinletter, symbool, cijfer etc bevat.



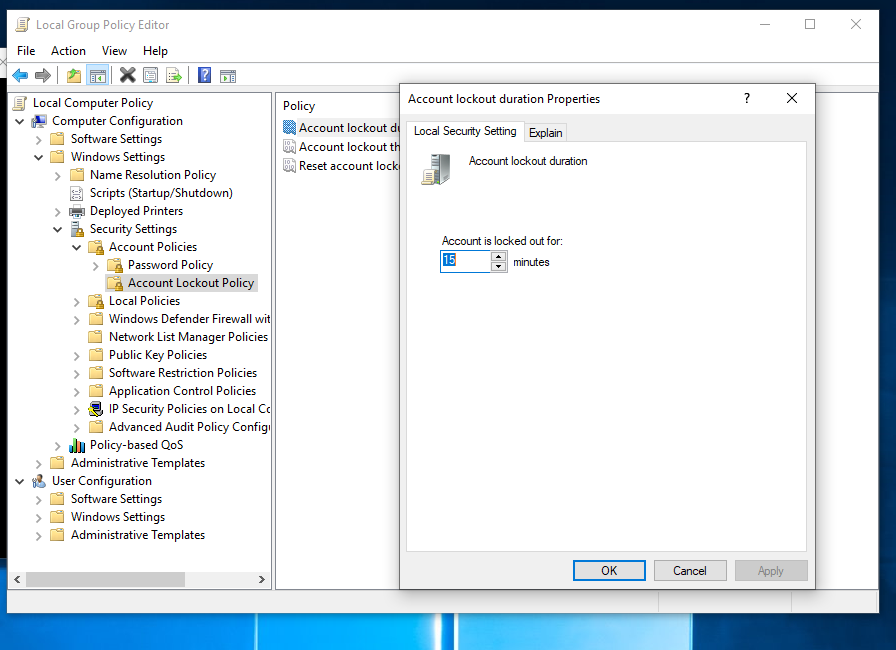
### Account Lockout Threshold

Na vijf pogingen zal de pc in lockdown gaan, dit is om attacks zoals brutforce attack tegen te gaan.



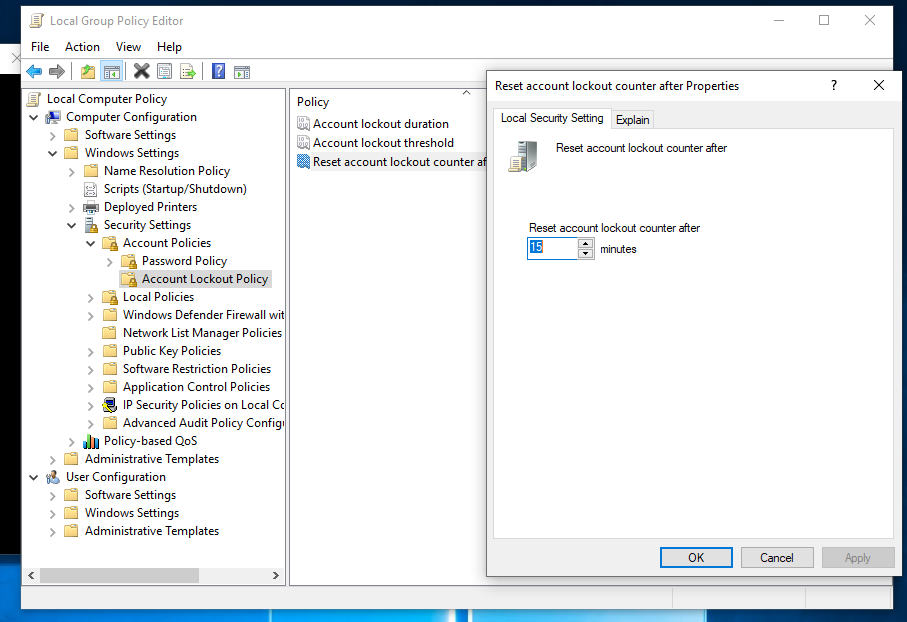
### Account Lockdown Duration

Hier kan de lengte van de lockdown ingesteld worden.



### Reset Lockdown counter

Na de lockdown duration timer op 0 is wordt de counter voor de ingegeven pogingen herstert.



# Per-Vlan Rapid Spaning Tree(PVST+)- Implementatie

### PVST+

### Script: Implamentatie

**!!LGL-FL2-A213-Dist-C3560v2-24p-Poe**

!

*enable*

*config t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4*

*spanning-tree vlan 1,2,10,90,99 root primary diameter 4*

*end*

*!*

***!!LGL-FL2-A201-C2860-24p***

*!*

*enable*

*Conf t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*end*

*!*

*!*

***!!LGL-FL4-FR-SF300-...***

*enable*

*Conf t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*end*

*!*

### *Script: Controle*

*Show spanning-tree*

*Show spanning-tree active*

*Show spanning-tree bridge*

*Show spanning-tree brief*

*Show spanning-tree interface*

*Show spanning-tree root*

*Show spanning-tree summary*

*Show spanning-tree vlan*

### Script: implamentatie uitleg

!!LGL-FL2-A213-Dist-C3560v2-24p-Poe

!

enable

config t

* Zet spanning-tree aan. Laat het de mode pvst+ gebruiken

spanning-tree mode rapid-pvst

* Dit een spanning-tree methode waaring er meerdere vlans op een kables verkeer kunnen versturen. Nu moet de verschillende vlans ingeven die iver deze connecties moeten gaan.

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

* Laat de vlans 20,30,40,50,60,70,100,120 deze switch gebruiken als secondary root brigde

spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4

* Laat de vlans 1,2,10,90,99 deze switch gebruiken als root bridge

Spanning-tree vlan 1,2,10,90,99 root primary diameter 4

end

!

!!LGL-FL2-A201-C2860-24p

!

enable

Conf t

spanning-tree mode rapid-pvst

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

end

!

!

!!LGL-FL4-FR-SF300-...

enable

Conf t

spanning-tree mode rapid-pvst

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

end

!

### Script: Controle uitleg

* + - Weergave van STP informatie

*Show spanning-tree*

* + - Weergave van alle actieve STP interfaces

*Show spanning-tree active*

* + - Weergave van de bridge ID, timers, en protocol voor het lokale bridge op de switch

*Show spanning-tree bridge*

* + - Kleine samenvatting van STP

*Show spanning-tree brief*

* + - Weergave van STP-status en configuraties voor een specifieke interface

*Show spanning-tree interface*

* + - Weergave van status en configuratie van de root bridge van de switch

*Show spanning-tree root*

* + - Samenvatting voor de STP

*Show spanning-tree summary*

* + - Weergave van STP-information voor een specifieke VLAN

*Show spanning-tree vlan*

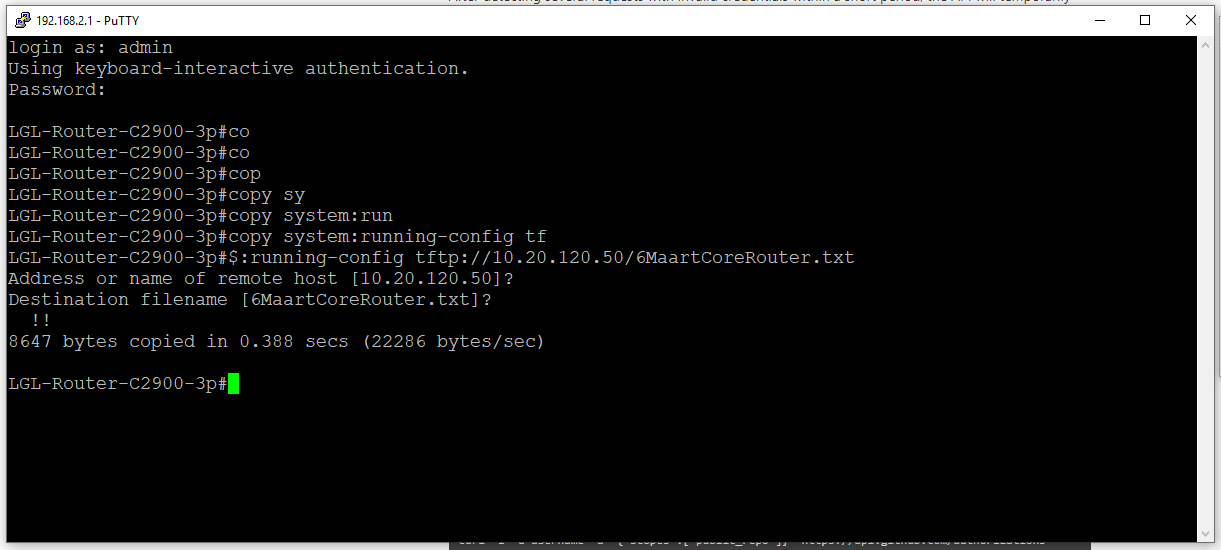
# Backup- Implementatie

### Configuratie tftpd

Current Directory 🡪 Locatie waar backup opgelagen moet worden.

Server Interface 🡪 de Interface die geconnecteerd met de router .

### Back-Up via command-line



!!verstuur een copie van de running config via de interface *Server Interface Address* en sla het op onder de naam  *DocumentNaam.txt*

copy system:running-config tftp://[*Server Interface Address*]/DocumentNaam.txt

!!Op 2000 series switches is het mogelijk dat de commando hiervoor anders is.

copy image tftp:// ://[*Server Interface Address*]/DocumentNaam.txt

!

CEF1: Cisco Express Forward is een switching techniek voor pakketjes op Cisco routers. Het optimaliseren van forwarden van de pekketen en het vergroten van de snelheid van het switching proces