# Opdracht

Beschrijving van de opdracht of toestand

**Probleem 1**

## Leerlingen mogen geen misbruiken van maken de netwerk op school

## Traag netwerk en/ of geen connectie.

### Het is al een gebeurt dat een kabel een beetje los was, waardoor we een bepaalde taak niet konden verrichten.

### Op sommige momenten wanneer er veel verkeer is dan loopt alles een beetje traag

**Probleem 2**

## Tijdens een telefonishe gesperek valt is de andere persoon soms niet goed

Verstaanbaar omdat stukjes weg vallen.

## Tijdens een telefonishe gesprek mogen er geen vertraging zijn. Hierdoor zijn sommige gesprekken niet verstaanbaar.

## **Probleem 3**

## De wachtwoorden zijn lang niet veranderd geweest. Er zijn ook geen beperkte tijds duur voor de wachtwoorden, de gebruikers mogen zelf kiezen wanneer ze hun wachtwoord veranderen. Dit gebeurt natuurlijk bijna nooit.

**Probleem 4**

## Er loopt veel verkeer van de Router’s interface gig 0/1 naar de LAN, dit zorgt soms vertraging.

**Probleem 5**

1.7 Momenteel wordt alle back-up van de config via conmmand-line gekopieerd en op de pc opgeslagen/ dit moet eenvoudiger en efficiënter. Alles is lokaal zowel de origineel als de back-up.

# Analyse van de opdracht

Wat moet ik doen.

**Probleem 1 : Illegale download**

## Ervoor zorgen dat leerlingen geen misbruik kunnen maken. Downloads op bepaalde site zoals bittorrent .

## Ervoor zorgen dat er load balance en redundantie, zodat er altijd een connectie is en zodat het verkeer word verdeeld door meerder kabels.

**Probleem 2 : VOIP**

## VOIP prioriteit geven over alle andere verkeer, zodat er geen pakketjes wegvallen.

**Probleem 3 : wachtwoorden**

## Een “Maximum Password Age” instellen voor de gebruikers zodat ze verplicht zijn om wachtwoorden te veranderen.

## Een Checklist opstellen die de gekozen wachtwoorden aan moeten voldoen.

**Probleem 4 : Etherchannel**

## Hier moeten we voor load-balance zorgen, zodat het verkeer verdeeld wordt en alles sneller verstuurd kan worden. Hierdoor zal de QOS van het netwerk verhogen.

**Probleem 5 : Back-ups optimaliseren**

## Het proces voor het kopiëren van de config versneller, maar ook ervoor zorgen dat het ergens anders dan op de pc van opgeslagen wordt.

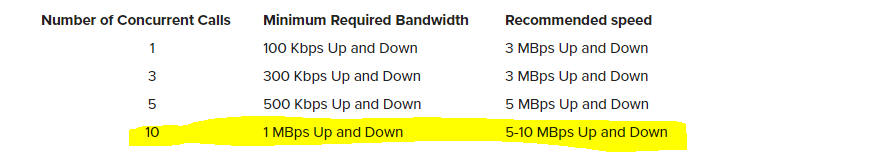
# Research en achtergrond

Onderzoeken welke optie of stappen best genomen moeten worden

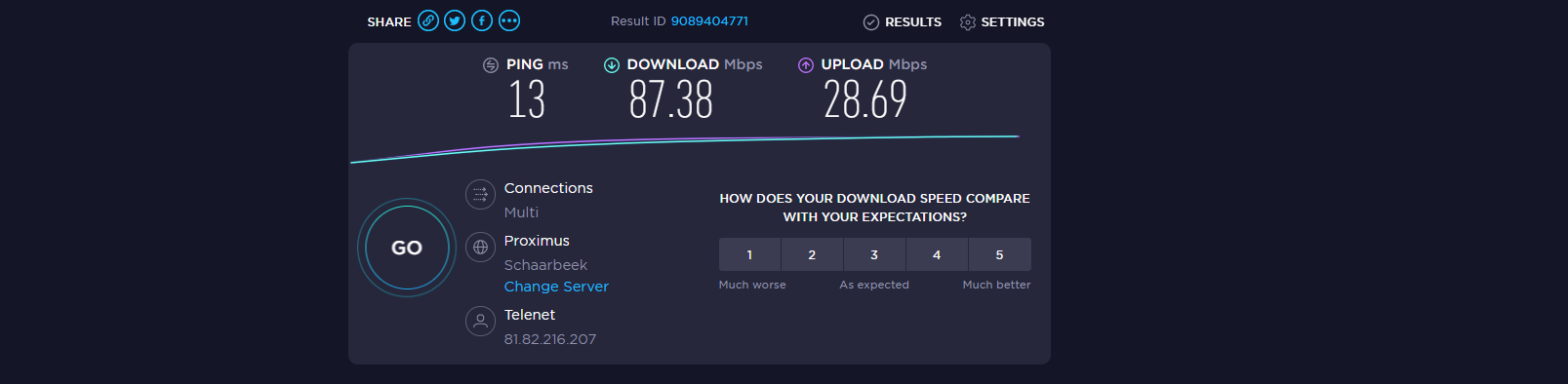
## Resultaten van mijn onderzoek of er een mogelijkheid is om bittorrent uit te zetten of blokkeren.

## Voip gebruikt 2 belangerijke protocools SIP en RTP. SIP(Session Initiation Protocol) wordt gebruikt voor het aanmaken en controleren van de connectie multimedia sessies zoals VOIP. RTP(Real-Time Transport Protocol) dit is een protocol die audio/media pakketten van VOIP vervoerd, RTP word gebruikt bij alle VOIP Communicaties. Om ervoor te zorgen dat er geen probleem is voor de VOIP zorgen ervoor dat dat VoIP een hoger prioriteit heeft en dat VoIP de minimum Kbps heeft.

Om QoS toe te passen op onse VoIp moeten eerste een paar berekingen doen. Ten eerste kijken we of we genoeg minimum verreisde bandwindth voor VoIp afhanklijk van de aantal gelijktijdige gesprekken. Hier is er ongeveer 10 gelijk tijdige gesprekken op een heel drukke dag

**

Hierna moet”en wqe een speedtest doen om te zien of we wel genoeg Bandwidth hebben voor al onze telefoons. Zoals we hieronder zien is dit geen probleem.



De min bandwidth voor ons is 1000kbps(1MBps), in de tabel hierboven wordt 5 tot10 MBps aangeraden. Beste zal iets zij tussen de 2 omdat we maar 28MBps upload hebben dus zal niet slim zijn om de helft te reserveren voor VOIP. 3 tot 5 MBps zal beste optie zijn voor ons.

Ten tweede kunnen we de UDP poorten die gebruikt worden door VOIP hoog prioriteit geven. UDP porten 16384 tot 32768.

## Ten eerste maken we een “password policy”, dit zijn een stel regels die zullen toegepast worden op de wachten om de ingegeven wachtwoord te controleren.

## Minstens 8 teken, niet hetzelfde als vorige wachtwoord, hoofdletters, klein letters, cijfers en speciale karakters.

## Daarna We zullen gebruik maken van de "Maximum Password Age Policy " van Windows om een tijdsduur in te stellen zodat de gebruikers verplicht zijn om hun wachtwoorden aan te passen. Kan gaan van 1 tot 999 dagen. Volgens BBB(Better Business Bureau) is het beter om het om de 30,60 tot 90 dagen te veranderen. 90 dagen is zeker de minimum voor ons, voor de personeel stel ik voor een "Max age" van 120 dagen(4 Maanden).

## EtherChannel is wanneer je een link creëer door meer poorten met elkaar te groeperen. Bij EtherChannel gaan we meerdere interfaces met elkaar verbinden en een logische interface van maken. Hierdoor is er load balance. Als ik een link met vier poorten gemaakt heb , wordt de informatie stroom verdeeld door die vier kabels. Waardoor mijn verkeer sneller zal zijn, want poort is minder belast. Als er een probleem met een van de kabels is, zal de communicatie normaal veder gaan met de overgebleven kabels. Het is mogelijk om tot 8 kabels in een channel zijn. Dit zorgt ook voor redundantie in de netwerk. Dus ook al valt 1 kabel uit of defect zal die link nog altijd bestaand omdat er andere kabels zijn die het werk veder verrichten. De link tussen de Core Router en de Core switch is een blangerijke link daar gaan we Etherchannel maken.

## Tweede deel van de oplossing die voor redudantie moet zorgen is spanningtree. Dit is een protocool die de snelste weg berekent en dan een andere weg aan duid als back-up als primaire link uit valt. We gaan de variatie Per-Vlan rapid Spanning tree gebruiken.

## We hebben een applicatie nodig die ons gaat helpen om via de commande-line in onze switch of router een backup to maken en op te slaan naar de gewenste locatie. Zodat we geen copy-past manouvre moeten doen en tijd kunnen winnen. Hiervoor maken we gebruik van tftpd(64), dit is een opensource applicatie die een paar handige features heeft waaronder tpftpserver die we kunnen gebruiken. ierHiermee kunne we via de commande-line opslaan naar onze toestel of een externe opslagruimte.

# Plan van aanpak

Na de onderzoek weet ik nu **WAT** precies gedaan kan worden. Om het op te lossen.

**Probleem 1 Illegale Download - Oplossing**

### Poorten die gebruikt worden door bittorent sluiten. Dit is niet de beste manier omdat bittorent een protocool is die zelf actief naar open poorten om connectie te maken met andere “peers”

### Bittorent protocool blokkeren in onze router zelf

### Via QOS kunnen ook bittorent low priority geven

**Probleem 2 VOIP - Oplossing**

4.2.1 configurenen van LLQ queuing op hier geef ik de rtp protocol de nodige MBps die we berekend

Hadden, we zorgen er ook voor dat rtp prioriteit krijgt.

**Probleem 3 Wachtwoorden - Oplosing**

4.4.1 We zullen de policies van de wachtwoorden aanpassen, zodat er een max periode is voor elke wachtwoord. Daarna zorgen we ervoor dat dat alle wachtwoorden moeten voldoen aan een paar regels. Daarna zorgen we een soort shutdown protocol die na een bepaalde aantal ingegeven foute wachtwoorden, het systeem in lockdown zet.

**Probleem 4 Redudantie - Oplossing**

4.5.1 EtherChannel toepassen zodat er altijd redudantie is en het data verkeer sneller zal zijn.

4.5.2 Stp configuren op de core switch, zodat er altijd de snellste weg gekozen wordt, en redudantie

in de netwerk is configuratie + kabels. We Maken gebruik van Per-Vlan rapid Spaning tree. Hierdoor configurenen we de spanning tree niet gewoon voor de switch maar per vlan die op de switcht is

**Probleem 5 Back-ups - Oplossing**

### Met tftp64 zal de proces sneller gaan , inplaats van te kopiëren en pasten.

# Designe van de oplossing

Hoe ga ik het oplossen

**Oplossing 1 Illegale download - Hoe**

### Via een ACL alle verkeer die van de poorten van bittorent komen niet toelaten. We maken een ACL ervoor omdat we deze ook weer kunnen gebruiken bij de configurratie van MQC Low Latency.

### Via Nbar kunnen BitTorrent protocool blokkeren

### MQC Low Latency gebuiken om ervoor te als extra toepassing om ervoor te zorgen dat downloads op bittorent de netwerk niet vertraagt. Mocht er toch op een bepaalde manier Bittorrtent binnen komen in onze netwerk kunne we ervoor zorgen dat hij een lage “Priority bandwidtch ”. Dit is een QOS feature.

**Oplossing 2 VOIP- Hoe**

### Om dit op te lossen maken we gebruik van LLQ (Low-Latency Queuing), dit is een Cisco feature die zorgt voor Priority Queinge(Pq). LLQ zorgt ervoor dat gevoelige en belangrijke data zoals voice krijgen hierdoor een voorkeursbehandeling vergeleken met alle andere verkeer, zodat ze als eerst verstuurd worden.

#### Ten eerste maken we een ACL die toegang geeft aan alle UDP poorten die gebruikt worden bij VOIP.

#### Daarna maken we een class map waarin we gemaakte ACL in zetten en dit de hoogste prioriteit geven.

#### Tenslotte zorgen we ervoor dat we VOIP de berekende bandwidth(3500) krijgt.

**Oplossing 3 Wachtwoorden- Hoe**

### In de AD zal ik een paar parameter instellen voor alle gebruikers. Eerst stel ik de “Enforce password history” in. Dit onthoud de vorige wachtwoorden, en dit zorgt ervoor dat deze niet opnieuw gebruikt kunnen worden. Als we 10 ingeven zal het de 10 laatste onthouden.

### Bij “Min Password age” geven we 90 in. Dit beteken dat de wachtwoorden pas na 90 dagen veranderd kunnen worden door de gebruiker. “Max Password age” is de max aantal dagen dat een wachtwoord gebruikt kan worden, we zullen voor 120 dagen(4 maanden) kiezen.

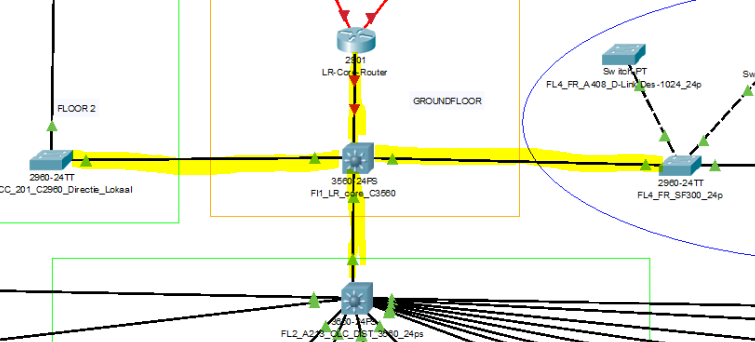
### Daarna stellen we de “Min password lenght” i, hier zetten we 8 , dit betekent dat de gekozen wachtwoorden een min van 8 karakters moet hebben. Ten slotte zetten we de complexiteit metric aan, hierdoor moeten de wachtwoorden minsten 1 kleinletter, 1 hoofdletter,1 cijfer en een speciale teken hebben.

### 5.1.5 Extra optie : een lockdown instellen. Na 5 foute wachtwoorden is er een lockdown van het account voor 15 Min, en de lockdown wordt na 15 weer opgeheven.

**Oplossing 4.1 Redudantie (EtherChannel)- Hoe**

### EtherChannel zal toegepast worden op de interface g0/1 van de Core Router omdat alle verkeer van en naar onze netwerk via die verbinding gaat. Als er een probleem met die connectie is dan zal alles plat liggen. Dus hier hebben we zeker redudantie en load balance nodig.

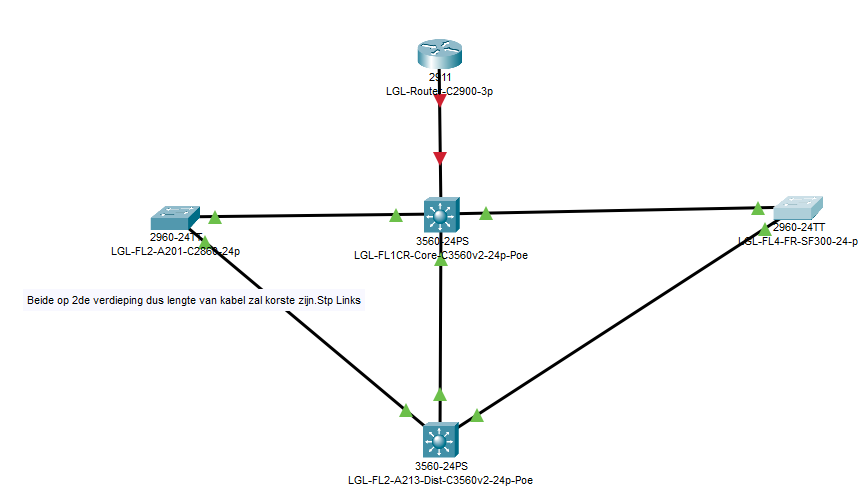
### EtherChannel zal toegepast geworden op de Core switch van de eerste verdieping(zie afbeelding). Alle verkeer gaat door die switch die vervolgens alle data doorstuurd naar waar ze moeten zijn. Momenteel is er geen etherchannel, wanneer wij etherchannel toepassen zal het verkeer sneler verstuurd kunnen worden en zal er ook redudantie zijn bij defecte of kabels die niet meer geconecteeerd zijn.

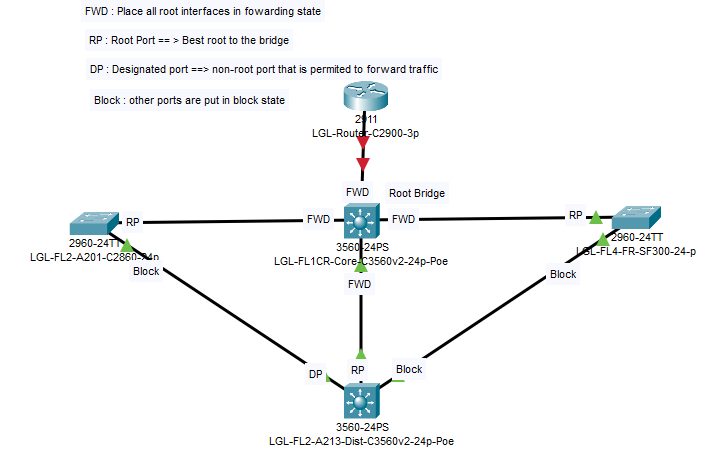


**Oplossing 4.2 Redudantie (STP en Etherchannel)- Hoe**

**OPTIE 1**

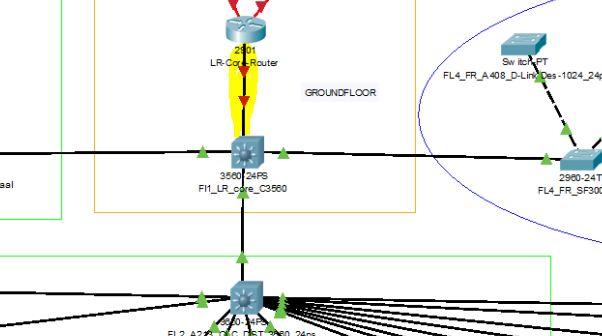
Ik heb configuraties gezien op verschillende apparaten voor STP maar er is nog geen fysiek connectie. Een Kabel moet geconnecteerd worden tussen de interface F 0/1 van FL2-A201 en hetzelfde interface op FL2-A213, en tussen F0/2 van FL2-A213 naar Fl4-FR.

****De STP is aangezet op de veracillende apparaten maar nog niet echt geconfigureert voor de verschillende Vlans en momenteel is STP aan maar wijn geen gebruik maken PVST+.



**OPTIE 2**

We passen etherChannel alleen toe op de connectie router en core switch, omdat we geen zelfde poort soort hebben voor de etherChannel alle gigabite poorten zijn bij de andere switches al in gebruikt.



**Oplossing 5 Back-ups - Hoe**

### Het installatie en configuratie proces voor de tftp64 is gemakkelijk en snel. De installer installeert de applicatie en wij moeten alleen kiezen welke map de back-up opgeslagen moet worden, en de server interface waar de connectie gemaakt moet worden. Na onze verandering inde configuratie moeten we via de commande-line in de router of switch maar 1 line code schrijven om de proces te voltooien.

# Implementatie

**Ik weet niet of ik het hier in tekst moet uitleggen of de configuratie zelf.**

**Oplossing 1 Illegale download - Implementatie**

### Een ACL list die niks binnen laat via de poorten van bittorent.

# 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

### Bittorrent blokeren met Nbar

ip cef

  class-map match-any LIMIT-TOR

  match protocol bittorrent

  exit

  policy-map QOS-LIMIT-TOR-POLICY

  class LIMIT-TOR

  police cir 2000000

  confirm-action drop

  exceed-action drop

  exit

  exit

  exit

  int gig 0/1

  ip nbar protocol-discovery

  service-policy input QOS-LIMIT-TOR-POLICY

  service-policy output QOS-LIMIT-TOR-POLICY

### MQC Low Latency (QOS)

Conf t

Class-map Bittorrent

Match protocol bittorent of **match access-group 101** (die vorige access list die we gecreëerd hebben)

Exit

^z

Conf t

Policy-map LLQ\_Bittorent

Class Bittorent

Priority percent 1%

Exit

Conf t

Int gig 0/2 (interface naar internet)

Service-output output LLQ\_Bittorent

^z

Show policy-map interface gig 0/2

**Oplossing 2 VOIP - Implementatie**

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)

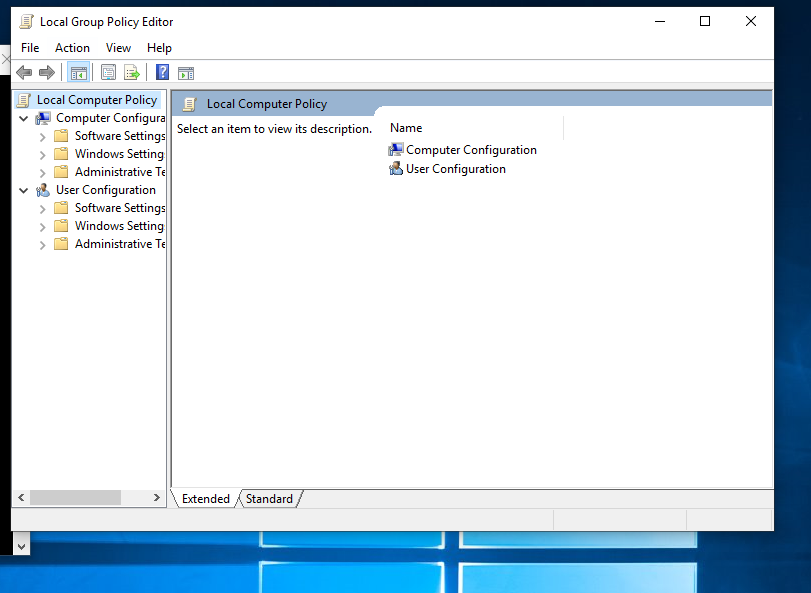
Service-output output LLQ\_voip

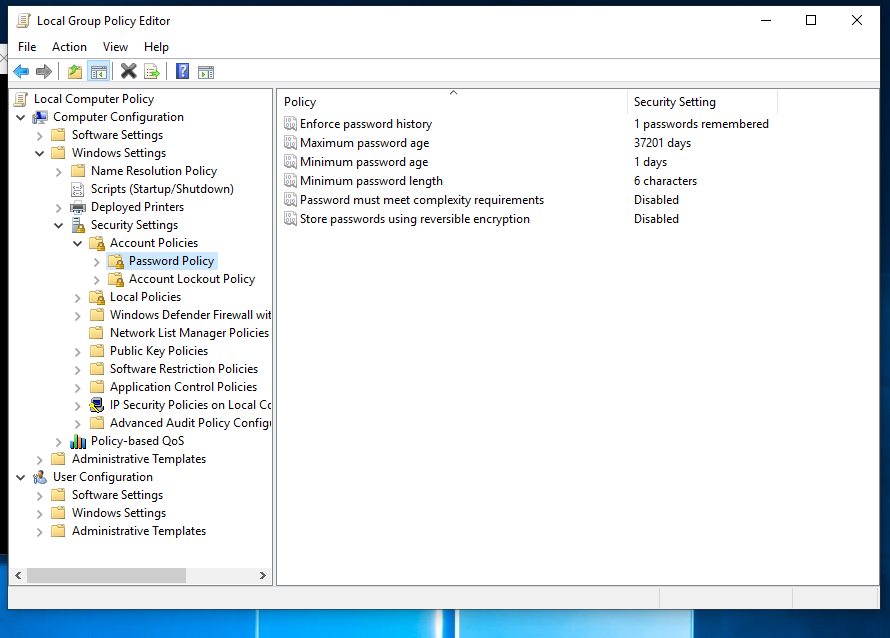
^z

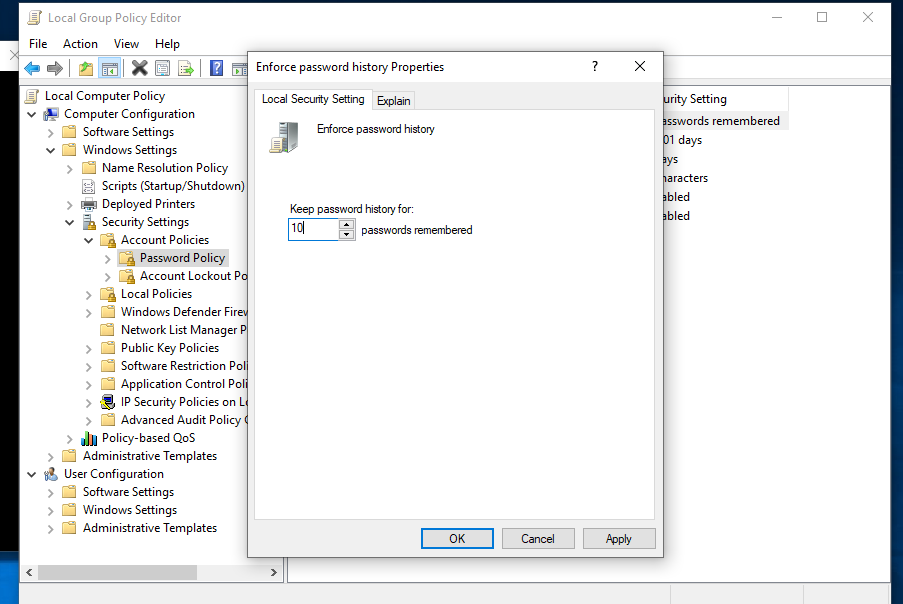
Show policy-map interface gig 0/2

**Oplossing 3 Wachtwoorden- Implementatie**

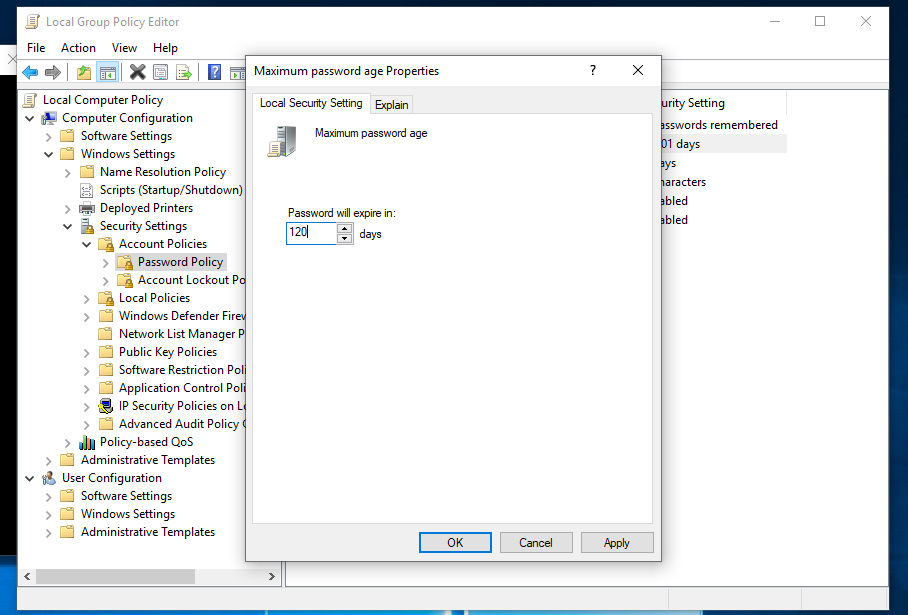
### Enforce password history



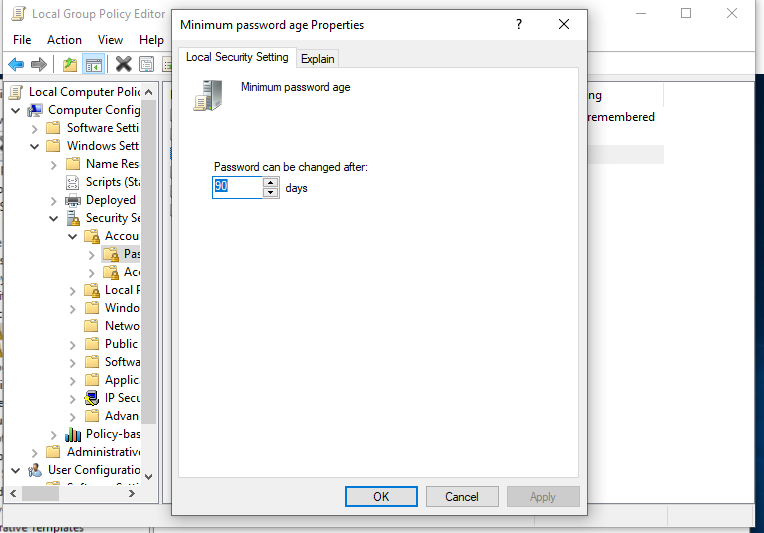




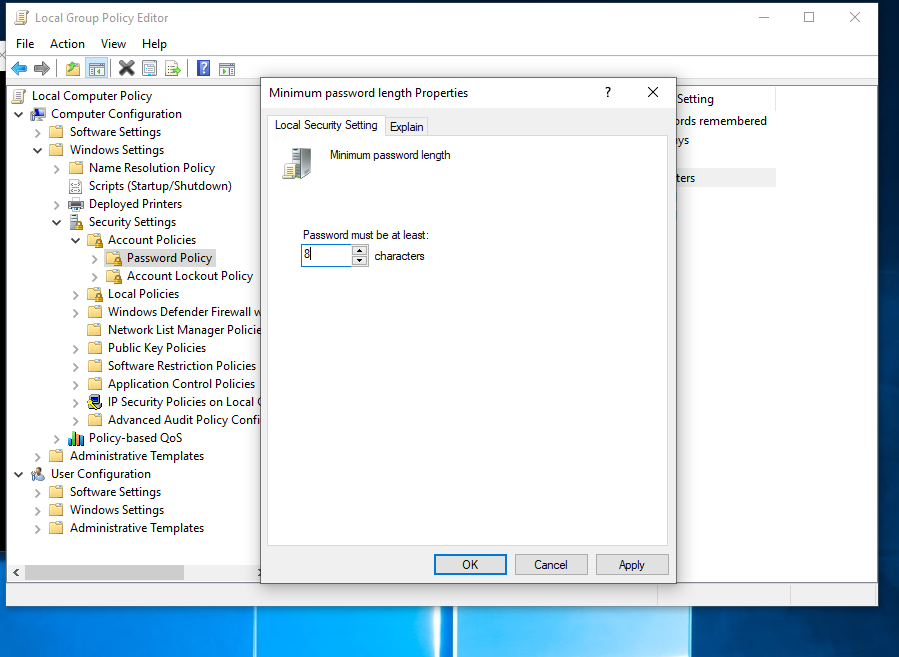
### “Max Password age”



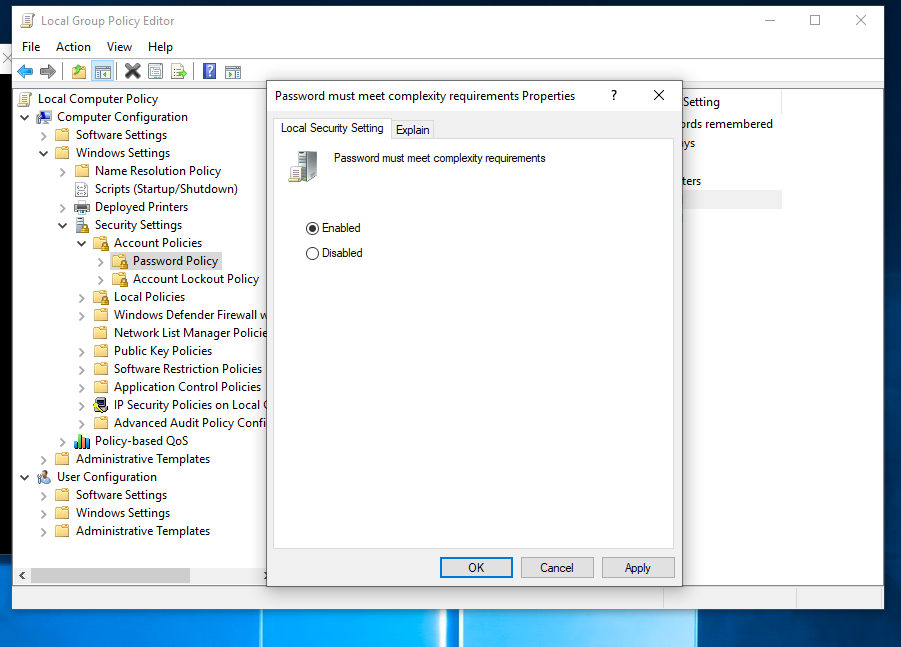
### Min Passwoord age



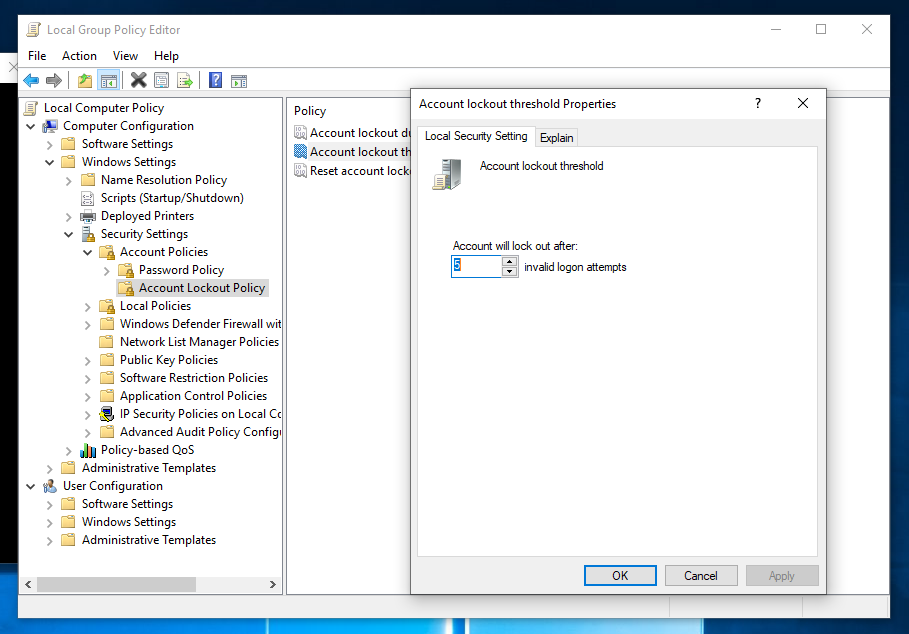
### Min Passwoord Length



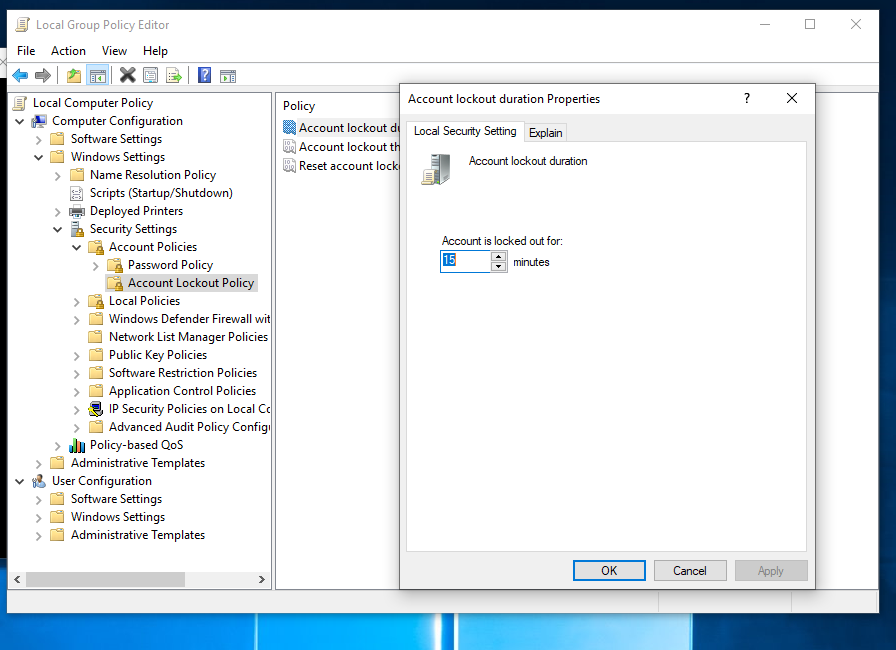
### Password complexity requirement



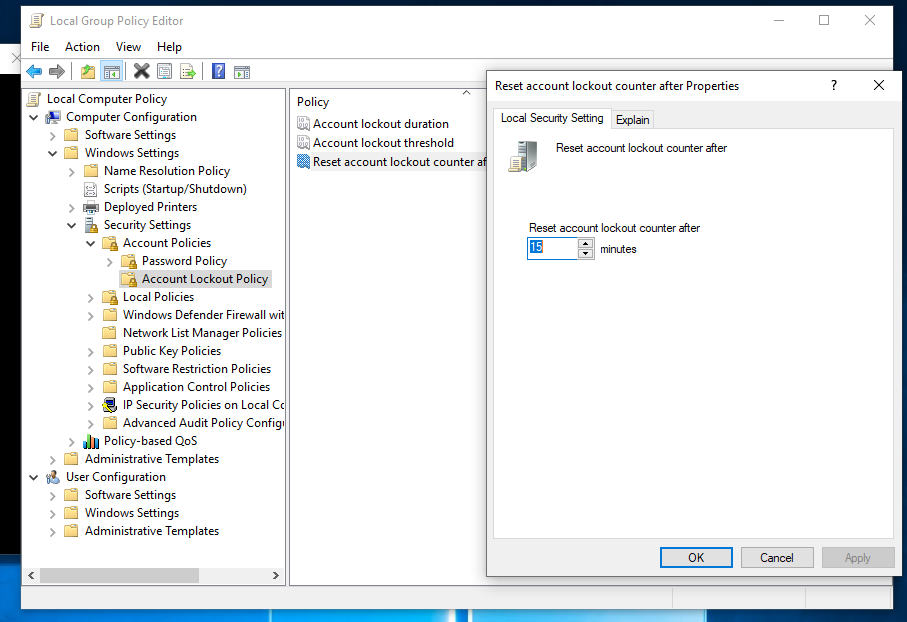
### Account Lockout Threshold



### Account Lockdown Duration



### Reset Lockdown counter



**Oplossing 4.1 EtherChannel - Implementatie**

### EthetChannel Van Core\_Router naar Core\_switch

**Oplossing 4.2 Per-Vlan Rapid Spaning Tree(PVST+)- Implementatie**

**LGL-FL1CR-Core-C3560v2-24p-Poe**

*>eneable*

*LGL-FL1CR-Core-C3560v2-24p-Poe#config t*

*LGL-FL1CR-Core-C3560v2-24p-Poe(Config)#spanning-tree mode rapid-pvst*

*LGL-FL1CR-Core-C3560v2-24p-Poe(Config)#spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*LGL-FL1CR-Core-C3560v2-24p-Poe(Config)#spanning-tree vlan 20,30,40,50,60,70,100,120 root primary diameter 4*

*LGL-FL1CR-Core-C3560v2-24p-Poe(Config)#spanning-tree vlan 1,2,10,90,99 secondary primary diameter 4*

*LGL-FL1CR-Core-C3560v2-24p-Poe(Config)#end*

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

*>enable*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe#config t*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe(config)#spanning-tree mode rapid-pvst*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe(Config)#spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe(Config)#spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe(Config)#spanning-tree vlan 1,2,10,90,99 root primary diameter 4*

*LGL-FL2-A213-Dist-C3560v2-24p-Poe(Config)#end*

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

*>enable*

*LGL-FL2-A201-C2860-24p#Conf t*

*LGL-FL2-A201-C2860-24p(config)#spanning-tree mode rapid-pvst*

*LGL-FL2-A201-C2860-24p(config)#spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*LGL-FL2-A201-C2860-24p(config)#end*

**LGL-FL4-FR-SF300-...#**

*LGL-FL4-FR-SF300-...>enable*

*LGL-FL4-FR-SF300-...>Conf t*

*LGL-FL4-FR-SF300-...(config)#spanning-tree mode rapid-pvst*

*LGL-FL4-FR-SF300-...(config)#spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*LGL-FL4-FR-SF300-...(config)#end*

**Oplossing 5 tftpd- Implementatie**

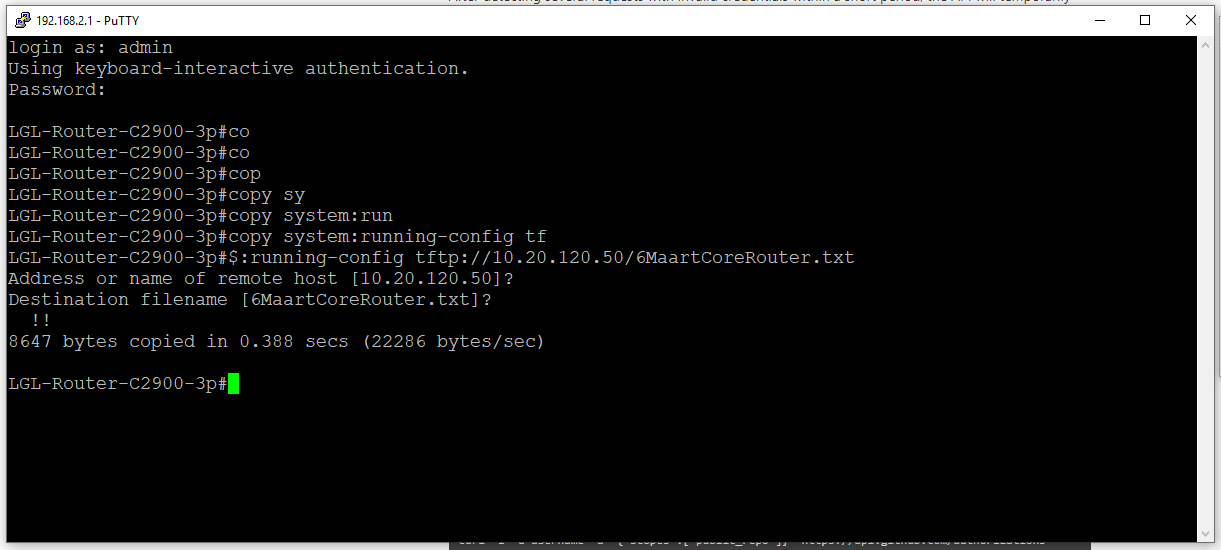
### Configuratie tftpd

### 

Current Directory 🡪 Locatie waar backup opgelagen moet worden.

Server Interface 🡪 de Interface die geconnecteerd met de router .

### Back-Up via command-line



# 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

# Evaluatie

Wat kan beter