# Design van de oplossing

Sedric Yaovi Lodonou

Opgesteld op 26/4/2020

Versie 1

Hoe ga ik het oplossen

**Oplossing 1 Illegale download - Hoe**

## Een veel gebruikte manier om netwerkverkeer te filteren zijn access control lists (ACL). Een ACL laat toegang tot bepaalde bronnen toe te staan (Permit) of te verbieden (Deny). Zie …..

## 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 Latenc(Zie ….).

## Er wordt gebruik gemaakt van Nbar (Zie …). Via Nbar kunnen BitTorrent protocol blokkeren. Elke externe verkeer die herkend wordt als BitTorrent zal niet toegelaten worden, en elke interne verkeer met BitTorrent protocol wordt gedropt

## Er wordt MQC Low Latency gebuikt als extra oplossing om ervoor te zorgen dat downloads op BitTorrent het netwerk niet vertraagt. Mocht er toch op een bepaalde manier BitTorrent binnen komen in het netwerk kunnen we ervoor zorgen dat hij een lage “Priority bandwidth ”. Dit is een QOS-feature.

**Oplossing 2 Telephonie/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**

## Er moet een paar parameters ingesteld worden in de AD voor de gebruikers. De parameters zijn password en privacy policy. Hiermee wordt de regels voor de voor de wachtwoorden ingesteld.

### Eerst wordt de “Enforce password history” ingesteld. Dit onthoudt de vorige wachtwoorden, en dit zorgt ervoor dat deze niet opnieuw gebruikt kunnen worden. Als we 10 ingeven zal het de 10 laatste onthouden.

### *Daarna stellen we de “Min password lenght” in, hier zetten we 8, dit betekent dat de gekozen wachtwoorden een min van 8 karakters moet hebben.*

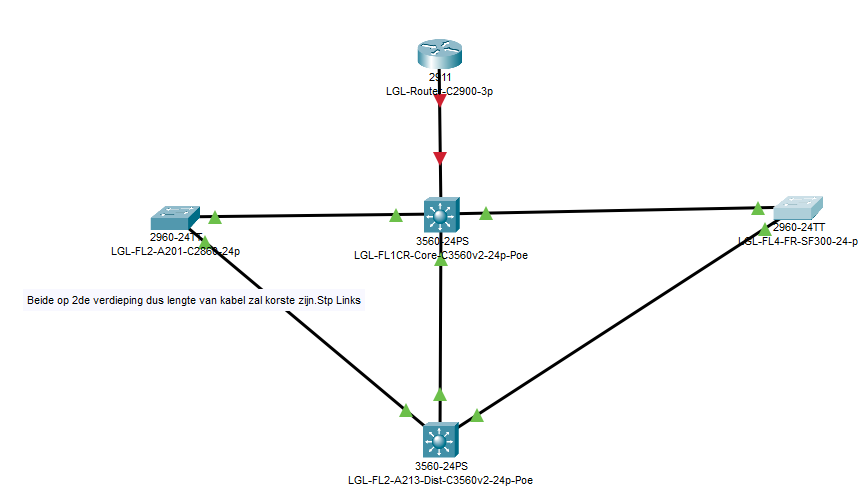
### 

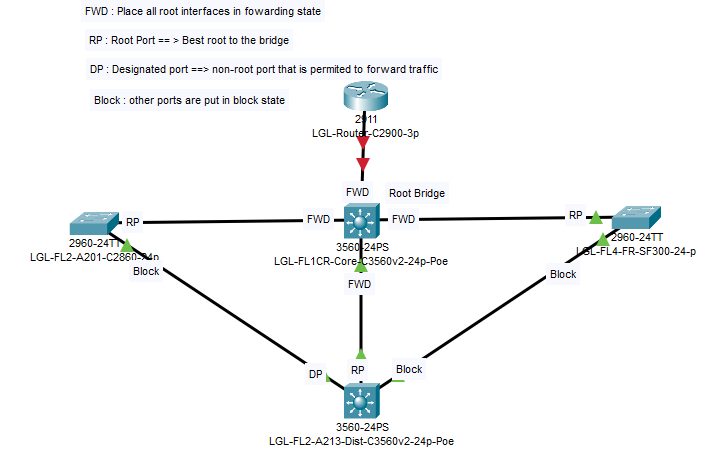
### *Ten slotte moet de complexiteit metric aangezet worden, hierdoor moeten de wachtwoorden minsten 1 kleinletter, 1 hoofdletter,1 cijfer en een speciale teken hebben. Dit is een soort checklist voor de nieuwe wachtwoorden.*

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

**Oplossing 4.2 Redudantie - Hoe**

Bij het doornemen van de configuraties op de verschillende toestellen blijkt dat Spanning Tree Protocol (STP) aan staat. Er is nog geen configuratie en er ontbreekt nog 2 connecties. 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 verschillende apparaten maar nog niet echt geconfigureerd voor de verschillende Vlans . De bedoeling is om gebruik te maken van PVST+.



**Oplossing 5 Back-ups - Hoe**

## Het installatie en configuratie proces voor de tftp64 is gemakkelijk en snel. De installer installeert de applicatie. Na de installatie moet de opslaglocatie van de back-up gekozen worden, daarna de server interface waar de connectie opgemaakt moet worden. Na onze verandering inde configuratie moeten we via de commande-line in de router of switch maar 1 line code schrijven om het proces te voltooien.