Onderwijsgroep Professionele Opleidingen Handelswetenschappen en bedrijfskunde

Improving the Quality of Service of a network by implementing the security model 'The CIA Triangle'

Bachelorproef en Stageverslag aangeboden door Sedric Yaovi Roland Lodonou tot het behalen van de graad van Bachelor in de Toegepaste Informatica

Begeleider Odisee: Yvan Rooseleer

Stagementor: Stefan Maenhout

Academiejaar 2019 - 2020

# Voorwoood

IK ben sedric Yaovi Roalnd Lodonou. Deze documentatie is geschreven in het kader van mijn Bachelor proef en Stageverslag voor de opleiding Toegepaste Informatica.

Ik heb mijn stage gelopen in CVO-Lethas. Het was geen stage waarbij ik een volledig netwerk in elkaar moest steken. Maar een stage die mij liet nadenken over hoe ik een bestaand netwerk beter kan maken voor de gebruikers. Hierdoor heb ik mijn kennis van Quality of Service, heel laag was kunnen verhogen.

Ik wil graag iedereen bedanken die mij geholpen hebben om deze stage tot een goed einde te brengen. Ten eest wil ik mijn stage mentor Yvan Rooseleer bedanken voor zijn begeleiding. Ik kreeg altijd goed advies en feedback over mijn werkmethode en was altijd bereid een contact moment in te planen voor een om mijn werk door te nemen. Ten tweede wil ik mijn stagebegeleider en mijn eerste aanspreek punt van CVO-lethas, stafan Maenhout bedanken. De communicatie was goed en altijd positief, hierdoor kon ik altijd extra uitleg of verduidelijking krijgen waardoor de taak heel duidelijk was.

**Informatiebronnen**

Om praktische redenen worden de informatiebronnen gecodeerd met vierkante haakjes. Bij de verwijzingen in de tekst is het gemakkelijk de informatiebron terug te vinden op basis van de code.

# Woordenlijst

QoS1: Quality Of Service

PPIDOO2 : Prepare, Plan, Design , Operate and Optimize

VoIP3  : Voice over Internet Protocol

NBar4 : Network Based Application Recognition

VPN5 : Virtual Private Network

FIFO6 :First IN First Out

WFQ7: Weighted Fair Queuing

CBWFQ8: Class-Based Weighted Fair Queuing

LLQ9: Low Latency Queuing

CEF10 : Cisco Express Fowoarding

PSVT+11 : Per-Vlan Rapid Spaning Tree

Tftpd12 : Darpa Suported Trivial File Transfer Protocol

# Figurenlijst

[Figuur 1 CVO-Lethas Logo 5](#_Toc41702469)

[Figuur 2 PPDIOO lifecycle 7](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702470)

[Figuur 3 Cisco Netflow Logo 10](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702471)

[Figuur 4 CIA Triad 11](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702472)

[Figuur 5 Zie wachtwoord 12](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702473)

[Figuur 6 Sterk Wachtwoord 12](#_Toc41702474)

[Figuur 7 IPsec 13](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702475)

[Figuur 8 AAA 13](file:///C:\Users\BL4CKD4G3R\Documents\BaWork\BaWork\Voorblad%20Stage%20en%20BP_2019-2020_v2.docx#_Toc41702476)

# Inhoudsopgave

Contents

[1. Voorwoood 2](#_Toc41714147)

[2. Woordenlijst 2](#_Toc41714148)

[3. Figurenlijst 3](#_Toc41714149)

[4. Inhoudsopgave 3](#_Toc41714150)

[5. Inleiding 5](#_Toc41714151)

[6. Opdrachtgever 5](#_Toc41714152)

[Logo 6](#_Toc41714153)

[CVO-Lethas Landsroem 6](#_Toc41714154)

[Contactpersonen 6](#_Toc41714155)

[7. Opdracht 5](#_Toc41714156)

[Wat 5](#_Toc41714157)

[Hoe 6](#_Toc41714158)

[I. Prepare 6](#_Toc41714159)

[II. Plan 6](#_Toc41714160)

[III. Design 7](#_Toc41714161)

[IV. Implement 7](#_Toc41714162)

[V. Test 7](#_Toc41714163)

[8. Prepare : Deel 1 - Req + Monitoring 7](#_Toc41714164)

[9.1 Requirements 8](#_Toc41714165)

[I. Telefoon (VoIP3) 8](#_Toc41714166)

[II. Onbelangrijke downloads 8](#_Toc41714167)

[III. Wachtwoorden 8](#_Toc41714168)

[IV. Redundantie 8](#_Toc41714169)

[9.2 Statische informatie verzamelen 8](#_Toc41714170)

[I. Nbar 8](#_Toc41714171)

[II. Netflow 8](#_Toc41714172)

[9. Prepare : Deel 2 - CIA Traid 7](#_Toc41714173)

[9.3 CIA Triad - uitleggen 8](#_Toc41714174)

[I. Confidentiality 8](#_Toc41714175)

[II. Intergrety 8](#_Toc41714176)

[III. Availability 8](#_Toc41714177)

[9.4 CIA triad - Toepassen 8](#_Toc41714178)

[I. Confidentiality 8](#_Toc41714179)

[II. Intergrety 8](#_Toc41714180)

[III. Availability 8](#_Toc41714181)

[10. Plan 7](#_Toc41714182)

[9.5 Taak 8](#_Toc41714183)

[I. Beschrijving 8](#_Toc41714184)

[II. Aanpak 8](#_Toc41714185)

[III. Mogelijk en gewenste resultaten 8](#_Toc41714186)

[IV. Vastellingen 8](#_Toc41714187)

[V. Advies 8](#_Toc41714188)

[11. Design 9](#_Toc41714189)

[12. Script(implementatie) 9](#_Toc41714190)

[13. testing 9](#_Toc41714191)

[14. Besluit 9](#_Toc41714192)

[15. Literatuurlijst 9](#_Toc41714193)

[16. Bijlage 9](#_Toc41714194)

# Inleiding

De bedoeling van deze stageproject was de optimaliseren en beveiligen van het netwerk van Lethas Landsroem. Het stageproject ging werd uitgevoerd op CVO-Lethas campus Landsroem, maar ik werk geïnformeerd dat de oplossing ook doorgevoerd zullen worden op de andere campussen.

Om het project overzichtelijker en duidelijker te maken werd de structuurmodel **PPIDOO2** toegepast. Met PPDIOO kan een project verdeeld worden in verschillend proces onderdelen. Door het volgen van het stappenplan, wordt er een duidelijke weg geschetst naar het eindresultaat van het project.

# Opdrachtgever

## Logo

A drawing of a face

Description automatically generated

Figuur 1 CVO-Lethas Logo

## CVO-Lethas Landsroem

CVO-Lethas is het grootste Centrum voor volwassenonderwijs in Brussel. CVO-Lethas heeft vier verschillende soorten opleidingen. Tweedekansonderwijs is voor studenten die diploma secundaire onderwijs willen halen. Nederlands voor anderstalige zijn Nederlandse lessen op eigen tempo. Talen zijn voor mensen die frans en/of Engels willen leren. Ten slotte geeft CVO-Lethas ook Informatie- en Communicatie Technieken. CVO-Lethas biedt dag- en avondonderwijs. Alles van wordt tot beeldwerking. Lethas heeft vier campussen in Brussel:

* **Lethas Landsroem**
* Lethas Rouppe
* Lethas Solvay
* Lethas Hovenier

## Contactpersonen

**Opdrachtgever:** CVO-Lethas Landsroem

**Contact:** Thierry Dierickx(Adjucnt-directeur)

**Stagebegeleider :** Stefan Maenhout(ICT-Coordinator)

**Stagementor:** Yvan Rooseleer

# Opdracht

## Wat

* Beveilliging en optimalisatie van netwerk is nodig omdat er steeds meer digitale hulpmiddelen gebruikt worden.
* De netwerkverbinding tussen de verschillende campussen verbeteren.
* Door de groei in interesse bij volwassenonderwijs zijn de ….

Adminstratie en secretariaat,

Campussen

Volwassenopnderwijs en campus.

## Opdracht en Probleemstellingen

### Onbelangrijke Downloads

* Gebruikers en cursisten mogen geen misbruiken van maken het netwerk op school
* Traag netwerk en/ of geen connectie

### Telefonie/VoIP

* Er mag geen vertraging oplopen tijdens een telefonisch gesprek, hierdoor vallen de pakketten soms weg waardoor de minder goed verstaanbaar is.

### Wachtwoorden

* De gebruikerswachtwoorden zijn nooit veranderd geweest omdat er geen beperkte tijdsduur zijn voor de wachtwoorden waardoor de gebruikers dit nooit doen

### Redudantie

* Het verkeer van de Core switch naar de dichtbij zijde switches op de verschillende verdiepingen hebben maar een weg, er is dus geen alternatieve route bij defecte of beschadigde connectie

### Back-up

* 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.

## Hoe

A picture containing device

Description automatically generatedOm deze project tot een goed eind te brengen moest er na gedacht worden over het toepassen van een bepaalde model of structuur. Het gekozen structuurmodel die toegepast wordt is de” *PPDOOO Lifecycle Approach to Network Design and Implementation”.*

Door deze werkmethode te toepassen is het gehele proces overzichtelijker en gemakkelijker uit elkaar te halen. Door hele project in onderdelen te splitsen, wordt er een bepaalde richting gevolgd van begin naar einde. Elke onderdeel heeft zijn eigen taak of doel. Hier beneden meer uitleg hoe PPDIOO toegepast is op het project.

Figuur 2 PPDIOO lifecycle

### Prepare

Dit proces vond plaatse voor de stageperiode. In deze fase werd er onderzoek gedaan naar QoS. Door de verschillend mails, face-to-face afspraken is er kan er nu een duidelijk plaatje geschetst worden voor de requirements. Ten slotte werd er statische informatie over het netwerkverkeer verzameld. Opzoeken van QoS design principes.

### Plan

Hier wordt de opbrachten gestructureerd om een beter overzicht te hebben. Elke opdracht wordt verdeeld in kleine taken, de opdracht is pas voldaan wanneer alle taken voltooid zijn. De verschillende taken worden gedaan met behulp van behulp van vijf vragen of categorieën. Beschrijving, aanpak, mogelijke of gewenste resultaten, vaststellingen en advies.

### Design

Hier worden de verschillende mogelijke oplossingen voor het probleem onderzocht en met elkaar vergeleken. Na de vergelijking wordt er een advies gegeven voor elke probleem. De verschilde adviezen worden uitgewerkt en voorgesteld aan de werkgever voor goedkeuring.

### Implement

Voor de verschillende oplossingen zijn er scripts geschreven die uitgevoerd kunnen worden wanneer dit opgelost is. De scripts kunnen gebruikt worden voor de implantatie van de oplossingen en na de implementatie kunnen ze ook gebruikt worden voor controle.

### Test

Er is wel een test scenario voorzien voor elke oplossing die geïmplanteerd moet worden. Ten tweede zijn er verschillende *show commands* bij elk e script die informatie geven over de werking van de configuraties.

# Prepare : Deel 1 - Req + Monitoring

De eerste grootste taak was informatie verzamelen bij verschillende bronnen. Eerste stap was informatie verzamelen bij de werkgever. Dit werd gedaan via mails en face-to-face meetings. Ten tweede moest onderzoek gedaan worden over het onderwerp. Ten slotte werd informatie verzameld over het netwerk zelf.

## Requirements

### Telefoon (VoIP3)

Tijdens een drukke dag wanneer er veel verkeer is in het netwerk en zijn de gesprekken soms niet verstaanbaar omdat er drops zijn. De opdrachtgever wil een goeie werking van de telefoons behouden zelfs bij hoge bandbreedte verbruik in het netwerk. Opdracht wil tijdens de drukke periodes zonder onderbrekingen tegelijkertijd telefoongesprekken kunnen voeren op alle telefoons.

### Onbelangrijke downloads

Netwerkverkeer die niet noodzakelijk is voor de dagelijkse prestaties moet zo weinig tot geen bandbreedte in beslag nemen. Opdrachtgever wil multimedia downloads tegenhouden of hun beschikbare bandbreedte beperken.

### Wachtwoorden

Momenteel zijn er geen password policy geïmplementeerd waardoord wachtwoorden nooit verander zijn. Er moeten nieuwe password policy geïmplanteerd via de Groupe Policy in de Actief Directory.

### Redundantie

Momenteel is er geen implementatie die voor redundantie zorgt in het netwerk. Voor QoS van een netwerk is redundantie ook belangrijk. De opdrachtgever wil meer redundantie in het netwerk.

## Statische informatie verzamelen

Voordat er geoptimaliseerd kan worden moet er eerst een beeld van de huidige situatie geschetst worden. Er wordt gebruik gemaakt van Netflow voor de verkeer monitoring. Daarnaast moet Nbar de verschillende protocollen herkennen en classificeren, om een duidelijk overzicht te krijgen van de verkeerstroom binnen het netwerk. Dit proces zal 10 dagen duren.

### Nbar

Nbar4 is een classificatie motor die verschillende protocollen en toepassingen kan herkennen en classificeren. Nbar geeft een overzicht over welke applicaties er precies gebruik worden in het network. Nbar schets een duidelijk plaatje over het netwerkverkeer en hoeveel netwerkbronnen elke protocol in beslag neemt. Door te zien welke protocollen veel voorkomen, is het gemakkelijker om te gaan optimaliseren. Nbar zal niet alleen gebruikt worden voor het analyseren, maar in later fase zal het ook gebruikt worden voor het optimaliseren van het netwerk. Zie Document Nbar

### Netflow

Figuur 3 Cisco Netflow Logo

Netflow is een netwerkprotocol die informatie verzameld en een toezicht houdt over de verkeersstroom van het netwerk. Netflow is ontwerpen door Cisco en werd in de 1996 beschikbaar gesteld op de Cisco routers. Netflow kan geconfigureerd worden om het verkeer van een interface in gaten te houden. Er is een mogelijkheid om alleen de binnenkomende en/of uitgaande verkeer op die interface te monitoren. Met Netflow geeft een weergave van het volume, de afkomst en bestemming en hoeveel verkeer in het netwerk gegenereerd wordt door die pakketten. Zie Document Netflow

# Prepare: Deel 2 – QoS + CIA Traid

Om Qos te kunne toepassen moet er een onderzoek gedaan naar welke van de volgende oplossing best geschikt is voor het bedrijf. Om een goeie beslissing te kunne nemen moet er naar verschillende aspecten van QoS kijken. En de beste oplossing voor de werknemer zal een combinatie zijn. Voor de volledige onderzoek en uitleg van Qos zie document *“QpSConcepts.doc”*

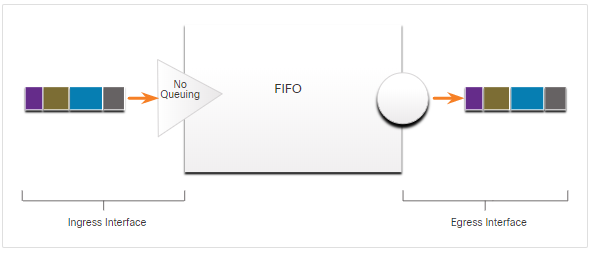
Security en QoS gaan hand in hand. Wanneer de security van het netwerk slecht is of gehakt, dan kan het bedrijf niet meer functioneren. In die situatie kan het bedrijf niet optimaal functioneren, de QoS van netwerk slechter wordt. Dit zal opgemerkt worden door de klanten.

## QoS Design

### Queuing Algoritme

#### FIFO6

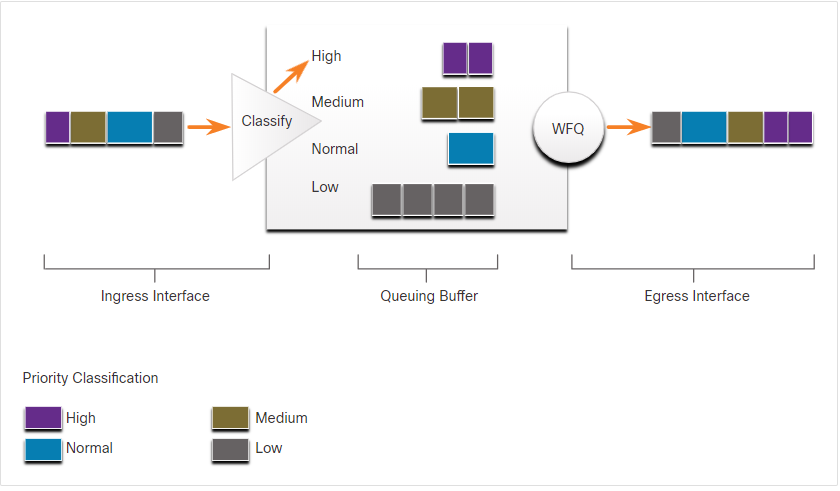
Dit is de eenvoudigste form van queuing. De pakketten worden in hetzelfde volgorde naar buiten gestuurd. Bij FIFO kan belangrijk en tijdsgevoelige verkeer gedropt worden bij een opstopping van de interface. FIFO is de snelste methode van queuing en wordt best gebruikt bij een grote link of een link met zeer weinig opstoppingen.



#### WFQ7

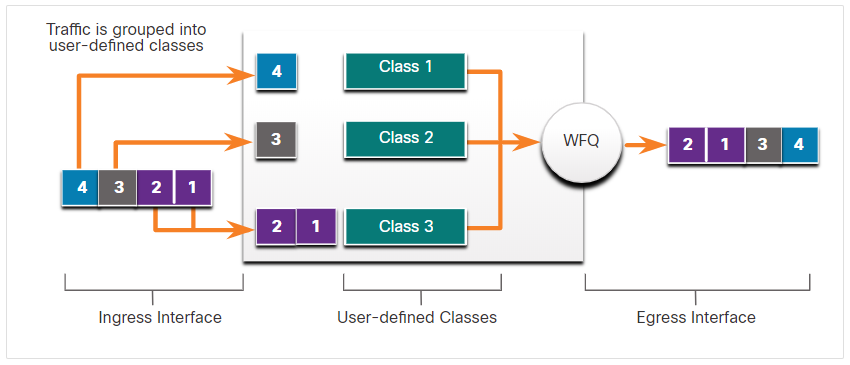
In komende verkeer wordt geclassificeerd en afhankelijk van de classificatie krijgen ze een prioriteitsniveau. Het verkeer met hoogste prioriteit mag eerst door. Elke inkomende pakket krijgt een prioriteit. Dit zorgt ervoor dat de volledige bandbreedte eerlijk verdeeld wordt tussen het verschillende verkeer in het netwerk.

WFQ zet het verkeer in verschillend soort afhankelijke van de Type of Service (TOS). De ToS gegevens in de IP-header wordt gebruikt om deze classificaties te maken. WFQ zorgt ervoor dat kleine interactieve verkeer zoals Telnet sessie en voice een hogere prioriteit krijgen dan grote verkeer zoals een ftp-sessie.



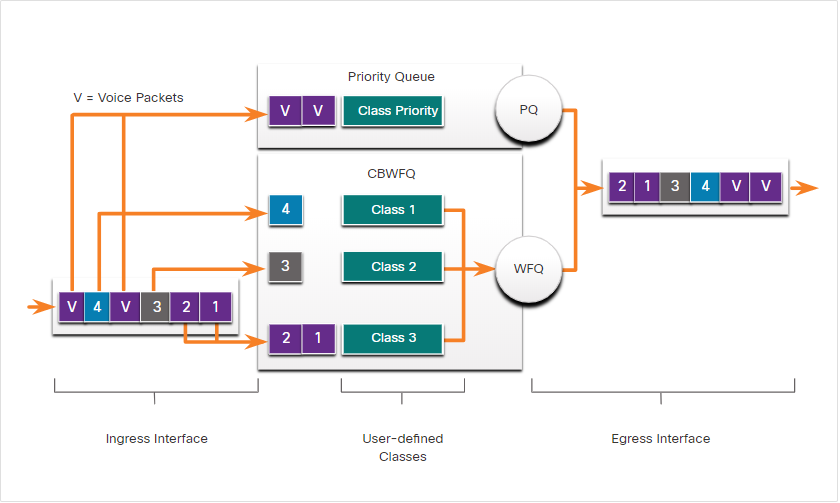
#### CBWFQ8

Dit is een verlenging van de WFQ. Hier moet gebruiker de verschillende klassen van het netwerkverkeer definiëren, doormidden van protocollen, Access control lists (ACLs)en de input interface. Elke class heeft zijn eigen FIFO-wachtrij. Elk class heeft zijn een paar karaktereigenschappen die geconfigureerd moeten worden. De karaktereigenschappen bandbreedte, weight en max pakketten in de wachtrij.



#### LLQ9

LLQ zorgt ervoor dat er een extra priority Queuing bij de CBWFQ. Hiermee kunnen we specifieke ervoor zorgen dat belangrijke en tijdgevoelige verkeer zoals Voice eerst gestuurd wordt.

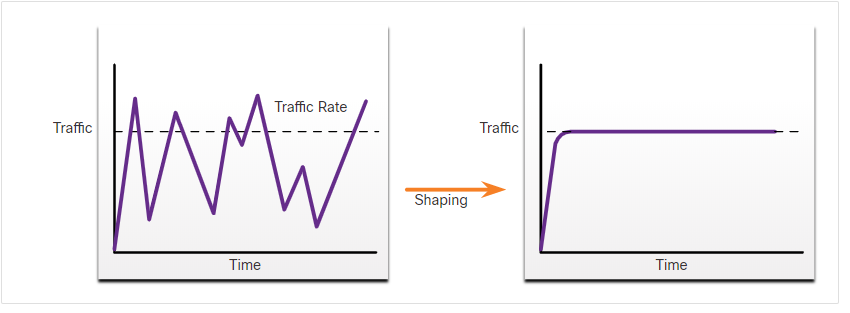


### QoS Implemetation Techniques

Dit zijn de mechanismes van Cisco Qos om opstopping tegen te houden.

#### Shaping

Shaping is een concept voor verkeer die naar buiten(outbound) gaan Shaping neemt het overschot van pakketten en zet ze in een wachtrij. Deze pakketten worden dan geplant om later te versturen over een bepaalde periode. De planning aspect van shaping zorgt ervoor dat pakketten die vertraging hebben, in een wachtrij gaan en wachten om later opnieuw opgestuurd te worden. Voorbeeld van planning functies voor shaping zijn CBWFQ en LLQ.



#### Policing

Policing is voor het verkeer die binnen(inbound) de interface komt. Wanneer het netwerkverkeer de maximun rate behaald, dan worden het overbodige verkeer gedropt. Policing wordt gebruikt door ISP.



### QoS Models

#### Integrated Service (IntServ)

Deze model is specifiek gemaakt voor de behoeften van de Real-Time Applicaties. Een applicatie stuurt een request van het netwerk voor een speciefiek service. De applicatie informeert het netwerk over zijn verkeersprofiel en vraagt om een bepaalde service die de vereisten bandbreedte en delay heeft. IntServ stuurt Resource Reservation Protocol (RSVP) naar de toestellen in het netwerk. Wanneer zij de nodige bandbreedte en delay kunnen reserveren, dan kan de applicatie beginnen te versturen.

#### Differentiated Services(DiffServ)

Elke pakket wordt gemarkeerd voordat ze het netwerk binnen komen, deze markering wordt gedaan op basis van verkeerstype. Het netwerk gebruikt die markering om te weten hoe het pakket behandeld moet worden. Dit betekent ook dat elke netwerk device de nodige vereisten aan, Dit is geen end-to-end Qos Strategie.

### Conclusie: QoS Concept

Eerst moesten er een QoS Model gekozen worden, de beste optie is DiffServ. Ten eerste is de IntServ een oud model. Ten tweede moeten alle toestellen in het netwerk RSVP ondersteunen en een verzoekt terug kunnen sturen. Wanneer dit niet gebeurt dan mislukt het proces. Ten slotte moeten alle toestellen in het netwerk alle verzoeken ven de verschillende applicaties apart bijhouden, dit kan heel verweldigend zijn op de toestellen.

Pakketten in het verkeer van de werkgever mogen niet gedropt worden, dus de beste optie is Shaping. Goeie voorbeelden van QoS algoritmes die hetzelfde soorten planningsmethode gebruiken zijn CBWFQ en LLQ.

Voor de Queuing algoritmes zijn de CBWFQ en LLQ de beste opties. Met deze twee algoritmes kunnen de verschillende pakketten geclassificeerd worden waardoor ze altijd herkenbaar zijn in het netwerk. Dit betekent ok dat de prioriteiten die een bepaalde Classen gegeven worden toegepast

## A close up of a logo Description automatically generated CIA Triad - uitleggen

Wanneer er gesproken wordt over *network* en/of *information security,* komt CIA Traid aan bod. Dit is een securitymodel dat bestaat uit drie elementen. Confidentiality, Integrity en Availability. Deze drie elementen worden gezien als de fundamentele elementen in data Security.

Figuur 4 CIA Triad

### Confidentiality

Confidentiality is een security principe die de toegang tot een bepaalde informatie beheerst. Toegang van informatie moet beperkt zijn tot alleen mensen die rechten hebben tot die informatie. Informatie moet verdeeld worden in verschillende categorieën, hoe hoger de categorie, hoe gevoeliger de data is. Gevoeligere informatie zal alleen toegankelijk zijn voor rechthebbende.

### Intergrety

Integrity is het behouden van consistente, nauwkeurige en betrouwbare data. Er moet maatregelen zijn zodat onrechtmatig personen geen toegang hebben en dat de data niet veranderd kan worden in transit.

### Availability

Gebruikers kunnen zonder onderbreking gegevens kunnen raadplegen. Connectie moet niet uitvallen wanneer een gebruiker bezig is. Dit kan een bedrijf betrouwbaar of juist niet betrouwbaar laten overkomen. Availability is heel belangrijk voor Qos.

## CIA triad - Toepassen

Na de Triad onderzocht te hebben, moeten de verschillende delen van de driehoek meer in detail bekijken. Elk deel van de driehoek wordt onderzocht. Er worden verschillende oplossingen geformuleerd die het probleem in die specifieke categorie moeten oplossen. Een succes indicatie dat deze concept goed toegepast werd, is dat er van elke deel minstens een oplossing toegepast wordt in het eindresultaat.

### Confidentiality

De oplossingen die hier besproken worden moeten de confidentialiteit van data verzekeren. Allen de mensen die recht hebben om een bepaalde data te zien, mogen die data zien.

#### Passwords

A close up of a sign

Description automatically generatedMensen moeten geen gevoelige informatie zoals wachtwoorden etc. weggooien in de prullenbak. Beste manier is het eerst nat te maken door te kauwen zodat te tekst niet meer leesbaar is en dan weggooien of doorspoelen.

Figuur 5 Zie wachtwoord

Gekozen wachtwoorden moeten voldoen aan een bepaalde checklist, min karakter,1 hoofdletter, kleine letters, een speciale teken, geen naam of woord die gevonden kan worden in het woordenboek. Laat gebruikers hun wachtwoorden na een afgesproken Maximum Password Age hun wachtwoord veranderen.

A picture containing screenshot, drawing

Description automatically generated

Figuur 6 Sterk Wachtwoord

#### IPsec

A picture containing sitting, street, table, phone

Description automatically generatedEen VPN5 is een privé netwerk die gemaakt is in een publiek netwerk. Een VPN verbindt twee endpoints met elkaar. Een bedrijf kan zijn hoofdkantoor verbinden met een offsite werkruimte. Een VPN is privé netwerk omdat de informatie die hij vervoert geëncrypteerd is. Er is confidentialiteit verwezenlijkt wanneer de informatie in de VPN-verkeer goed geëncrypteerd is, dit kan gedaan worden door IPsec. IPsec zorgt voor authentication, access control, integrity en confidentiality. De informatie kan geëncrypteerd en gecontroleerd worden. IPsec kan zowel gebruikt worden in remote-access als site-to-site VPN.

Figuur 7 IPsec

#### Access control models

Access control models maakt het gemakkelijker voor bedrijven om toegang tot sommige informaties te verbieden of beperken voor sommige werknemers. Werknemers moeten alleen toegang hebben tot informatie die relevant is voor hun functies etc. er zijn vier soorten Access control models. De Mandatory Access Controle, Discretionary Access Control, Role-Based Access Control en Attribute-Based Access Control. De 4 verschilledne access wordt nu niet in detail besproken omdat dit al gebeurd is in de document CIAtriad.pfd

#### Authentication, Authorization, Accounting

A close up of a sign

Description automatically generatedAAA is een tool die gebruikt wordt om gebruikers toegang te geven met *authentication*. Gebruiker kan inlopen in het systeem door gebruik te maken van gebruikersnaam en wachtwoord. Administrator kan gebruiker toevoegen en deleten en zo toegang geven tot data of de tegengesteld. Administrator kan het instellen om de authenticatie lokaal of via de server te laten gebeuren.

Figuur 8 AAA

Wat ze erop mogen doen, welke rechten ze hebben via *Authorization*. De administrator geeft specifieke rechten aan gebruikers en die rechten bepalen welke info de gebruiker kan zien en welke configuraties hij mag doen.

Bijhouden van acties die uitgevoerd werden door *Accounting*. Hierdoor wordt gegevens gemonitord en bijgehouden terwijl de gebruiker bezig is.

### Intergrety

De oplossingen die hier besproken zullen worden moeten ervoor zorgen dat de integriteit van de data behouden wordt. Dat moet bij het verzenden en aankomst hetzelfde zijn.

#### Version Controle

A close up of a computer

Description automatically generatedVersion Controle is een systeem die je gebruikt om up-to-date te zijn met je projecten en een productie omgeving. VCS geeft ook de mogelijkheid om samen te werken met andere mensen rond een project. Via branches is het mogelijk om op een sub-project van de Main project te werken waardoor de Main project nooit beschadigt, en zodra de sub-project in orde is kan het gemengd met het hoofdproject. Bij beschadiging van data kan het project teruggedraaid worden naar vorige versie.

Figuur 9 Version Controle

#### cryptographic Hash

A picture containing bird, flower

Description automatically generatedHasing is een wiskundige functie die gemakelijk te implementeren is, maar de revers engineering hiervan is moeilijk. Hasing wordt gebruikt om de integriteit van data te controleren en verzekeren. De functie neemt een variabel of volledig bericht genaamd message en creëer a tekst genaamd *HASH*, *message digest*, *diges*t, of *digital fingerprint*. Het is onmogelijk dat twee verschillende sets data hetzelfde hash output hebben. Zodra er iets aan het document veranderd zal er een andere hash uit komen. Omdat er geen twee data met hetzelfde hash kan zijn, wordt dit gebruikt om duplicatie en veranderingen op te sporen.

Figuur 10 Plain Text naar HASH

#### Host-Based Intrusion Detection

Intrusion Detection System is een software of hardware die het netwerk monitort en een alerts naar de administrator stuurt wanneer het een malicieus programma opmerkt. Een host-based Intrusion Detection Dystem is om hosts te beschermen tegen malware. HIDS doen aan monitoring en sturen een report van hun bevindingen. Hij kan log analysis, event correlation,

integrity checking, policy enforcement, rootkit detection, en \* alerting. HIDS hebben een file integrity checkig of \* data integrity monitoring. HIDS weerhouden gevonden malware te uit te voeren, mocht het een host bereiken. Hierdoor zorgt HIDS ervoor dat heel data in netwerk hun integriteit behouden.

#### Back-ups

A close up of a computer

Description automatically generatedHet is belangrijk dat er een of meerder back-ups zijn van de data. Als er voor een of andere reden het hoofd database een probleem heeft of er een probleem is het netwerk, moet er een back-up aanwezig zijn. Er moet zowel een lokaal back-up zijn, als een op de server. Back-up op de server zal het gemakkelijk maken om alle data te synchroniseren en te kunnen bijwerken. De lokale back-up kan gebruikt worden als er geen connectie is met de server, of wanneer het juist de server is die en probleem heeft.

Figuur 11 Meerdere back-ups

### Availability

De oplossing die hier besproken zullen worden is om ervoor te zorgen dat er altijd availability is. Ervoor zorgen dat er altijd een soort redundantie is om lange downtime te vermijden.

#### Hardware and software

Continue beschikbaarheid in het netwerk kan alleen gegarandeerd worden wanneer er een continue hardware en software onderhoud is. Hardware reparaties direct uitvoeren Wanneer er schade is. Zelfs beschadigde kabels kunnen voor problemen zorgen. Zorg ervoor dat de hardware op een goeie plaats is die voor langdurige productiviteit zal promoten. Dus laat je hardware toestellen niet rechtstreeks in de zon, of zet het niet in een ruimte waar er geen verluchting is etc. Er moet genoeg bandbreedte zijn voor communicatie en probeer bottlenecks te voorkomen.

Zorg ook dat de software kant in orde is. Wees altijd up-to-date met de laatste update, want dat kan performantie belemmeren. Wanneer er geen updates gebeuren dan kan je systeem zijn database ook niet bijwerken, waardoor hij een malicieus programma zal binnen laten.

#### Redundancy – STP

STP6 zorgt er voordat er maar een weg genomen zal worden en zet de andere on stand bij zodra er een probleem is met de hoofdweg dan neemt de redundante weg het over. STP voorkomt loops. Loops zorgen ervoor zorgen dat het netwerkverkeer langzamer is of zelf volledig stopt. STP zorgt er ook voor dat er een redundante weg is waardoor het netwerk kan blijven werken.

#### Redundancy – EtherChannel

**A screenshot of a cell phone

Description automatically generated**EtherChannel is wanneer er een link gecreëerd wordt door meerdere poorten met elkaar te groeperen. Bij EtherChannel worden meerdere interfaces met elkaar verbonden om een logische interface van maken. Hierdoor is er *load balance*. Als er een link met vier poorten gemaakt wordt, dan wordt de informatie stroom verdeeld door die vier kabels. Waardoor mijn verkeer sneller zal zijn, want de individuele poorten zijn 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 te hebben.

Figuur 12 EtherChannel

# Plan

Na de verschillende onderzoeken en voorbereidingen is het belangrijk om nu een goed plan van aanpak op te stellen. Hierdoor wordt het duidelijk hoe de problemen opgelost zullen worden en welke stappen genomen moeten worden.

De opgestelde probleemstellingen analyseren en veranderen in een lijst van opdrachten die opgelost moeten worden. Na het opstellen van de lijst is de bedoeling om verschillende taken op te schrijven die uitgevoerd moeten worden om het probleem op te lossen. De lijst met taken is een stappenplan van de weg die genomen gaat worden om het probleem op te lossen.

## Analyse van Opdracht

### Illegale Download

* Netwerkverkeer verminderen door downloads van bittorrent tegen te houden.

### Telefonie/VoIP

* VoIP-verkeer prioriteit geven over alle andere verkeer zodat er gen pakketjes wegvallen.
* De maximumaantal nodige bandbreedte voor alle telefoons toekennen aan de telefoons.

### Wachtwoorden

* Nieuwe password policy instellen
  + Een “Maximum Password Age” instellen voor de gebruikers zodat ze verplicht zijn om wachtwoorden te veranderen.
  + Een checklist opstellen die gebruikt zal worden om de gekozen ´wachtwoorden te valideren.

### Redundantie

* Een redundantie oplossing implementeren tussen de Core switch en direct verbonden switches

### Back-ups Opltimaliseren

* Het back-up proces van de configuraties versnellen.
* Back-up op meerdere plaatsen doen.

## Taak

Elke taak wordt ingedeeld in een paar secties. Dit is om een beter overzicht te krijgen van elke taak. Deze indeling schets een beeld rond wat er gedaan moet worden, hoe dat gedaan gaat worden, de resultaten van de taak en de adviezen voor de toekomst.

Er zijn 5 problemen die opgelost moeten worden. Elke probleem heeft minstens 5 taken en elke taak heeft de verschillende indelingen. Voor de volledige lijst van taken en de afwerkingen daarvan Zie DoorloopTijdEvaluatie.doc

### Beschrijving

In deze deel moet de taak beschrijven worden. Hier is de bedoeling om meer informatie te geven over wat de taak precies inhoudt.

### Aanpak

Nu de opdracht beter uitgelegd is in de vorige deel, kan hier meer uitgelegd worden over HOE. Hier moet uitleg gegeven worden over welke stappen genomen zullen worden om deze taak te voltooien. Hier wordt ook uitleg geven over welke materiaal of tools er gebuikt zullen worden.

### Mogelijk en gewenste resultaten

Wat wordt verwacht van de taak. Welke resultaten worden er verwacht. Wat is het doel van de taak.

### Vastellingen

Wat waren de resultaten na het uitvoeren van de taak. Is het gelukt of niet. Waren de resultaten hetzelfde als de verwachte resultaten?

### Advies

Wat zijn de adviezen voor de toekomst. Deze adviezen worden meegenomen naar de volgende taak, of worden gebruikt om huidige taak te verbeteren.

# Design

De volgende stap is te onderzoeken wat de beste opties is voor de verschillende opdrachten die opgelost moet worden. Hier zullen er verschillende opties aanbod komen. De beste en meeste nuttige oplossing moet uitgekozen worden en verder verwerkt worden.

## Bittorrent: Research

### ACL

Access Control List (ACL) zijn wordt gebruikt om het netwerkverkeer te filter. Het is een soort firewall die geïmplementeerd kan worden in een netwerk om de inkomende en uitgaande verkeerstroom te filteren. Een ACL kan toegepast worden op een specifieke interface als een inbound of outbound. Hiermee kan ervoor gezorgd worden dat bittorrent niet meer aanwezig zal zijn in het netwerk.

### Scavenger via Nbar

Een andere optie is het gebruiken van Nbar(Zie nbarConfig.pdf). Hiermee kunne we ervoor zorgen dat nbar een specifiek protocol deels- of niet toelaat. We gaan ervoor zorgen dat deze verkeerstype gemarkeerd wordt als Scavenger Class (Less-Than-Best-Service). Dit betekent dat p2p wel toegestaan wordt op het netwerk wanneer er genoeg bandbreedte is. Bij opstopping krijgt p2p heel weinig bandbreedte of soms worden de pakketten gedropt. Dit wordt toegepast bij verkeer die niet belangrijk is voor de dagdagelijkse prestaties. Dit kan door het verkeer een DSCP-waarde van SC1 te geven of via CBWFQ laag bandbreedte te geven

### Conclusie: Bittorrent

Voor deze probleem is de beste oplossing de nbar. De nbar is al actief voor het verzamelen van de verschillende statistieken, een extra functionaliteit eraan toevoegen zal geen impact hebben op het netwerk. Nbar is gemaakt om te helpen bij dit soort problemen en QoS te verbeteren dus het is van zelfspreken dat deze oplossing het beste optie is. Dit is de meeste flexibele oplossing voor deze probleem.

Bittorrent wordt niet heel vaak gebruikt, hierdoor is het wel beschikbaar wanneer het nodig. CVO-lethas is een school, tijdens de examenperiodes gebruiken leraren video’s voor bepaalde examen. Wanneer de statistieken opgevraagd wordt na het examen zal er zeker een protocol voor videostream aanwezig zijn. Dit kan ook het geval bij bittorent zijn.

Het is dus beter Scavenger te gebruiken, zodat het toch gebruikt kan worden. Maar bij wanner het druk is in het verkeer zal de prioriteiten 1% zijn, dus het zal geen andere verkeer storen

## Telefonie/VoIP: Research

### Auto-QoS

Dit is een manier voor de automatisering van QoS. Nadat auto-Qos aangemaakt wordt, gaat het in discovery mode. Tijdens deze discovery periode worden er informatie over hert netwerkverkeer bekeken. Door de auo-QoS kan er na de discovery periode een advies gevraagd worden voor het volledige netwerkverkeer.

Na de *discovery* periode wordt QoS toegepast door Auto-Qos. Het voordeel is dat deze QoS methode al alle informatie verzameld heeft over het verkeer van het volledige verkeer. Er wordt een weergave gemaakt voor de beste verdelingen van prioriteiten, bandbreedte van VoIP, video en

transactions. De bandbreedte en prioriteit kan ingesteld worden voor alles, waardoor het mogelijk is om een QoS implementatie te creëren die perfect is voor het netwerk.

Er wordt een QoS formule gemaakt die optimaal is voor het netwerk. Dit is auto-QoS dus het kan automatische aangepast worden als er een verandering is in het netwerk waardoor de ingestelde QoS niet meer effectief is.

### LLQ

Low-Latency Queing is een toepassing die in auto-QoS zit. LLC is een toepassing is prioriteit queuing biedt aan de protocol VoIP (RTP) verkeer. Het is dus mogelijk om in plaats van Auto-QoS , alleen LLQ te toepassen. Dit is dus allen voor de VoIP en het moet elke keer manueel aangepast worden bij veranderingen in het netwerkverkeer.

### Conclusie: VoIP

De beste optie is Auto-Qos omdat wee hier niet alleen VoIP hebben maar het volledige netwerkverkeer. Hiermee zal de QoS van het bedrijf altijd het beste keuze zijn voor het netwerk. Doordat het werkt via discovery van het netwerkverkeer, is de aanpassing van de QoS bij netverkeer veranderingen of bij het vergroten het netwerk heel eenvoudige.

## Wachtwoorden: Research

Voor de opdracht is de enige beste optie, dat het de nieuwe policy toegepast wordt via Active Directory

### Password Policy

Ten eerste maken we een “password policy”, dit zijn een stel regels die zullen toegepast worden op de wachten om het 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 150 dagen (5 Maanden).

### Conclusie: Wachtwoorden

De beste optie is 5 maanden. Een artikel van 2019 zegt dat wanner werknemers te vaak hun wachtwoorden moeten veranderen kan dit voor een echte security risk zorgen. Werknemers kiezen wachtwoorden die gemakkelijk zijn, of een afwijking van het vorige wachtwoord. DE gekozen wachtwoord policy zorgt ervoor dat het wachtwoord een niveau van compliciteit heeft.

## Redundantie: Research

### EtherChannel

EtherChannel is een link die gecreëerd wordt door meer poorten met elkaar te groeperen. Bij EtherChannel worden er meerdere interfaces met elkaar verbonden om een logische interface van maken. Hierdoor is er load balance. Als er een link met vier poorten gemaakt heb, wordt de informatiestroom verdeeld door die vier kabels. Waardoor het 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.

### Spannung tree Protocol

Tweede oplossing die voor redudantie moet zorgen is spanningtree. Dit is een protocol die de snelste weg berekent en dan een andere weg aan duidt als back-up als primaire link uitvalt. We gaan de variatie Per-Vlan rapid Spanning tree gebruiken.

### Conclusie: Redundantie

Voor deze probleem is de tweede oplossing het beste. Zoals boven besproken is Etherchannel niet van toepassing omdat er geen bottleneck is. STP zorgt voor redundantie die ervoor zorgt dat het netwerk altijd up zal zijn. Dit vermijdt het ontstaan van loops, loops kunnen voor grote vertraging in het netwerk zorgen. De vermelde pluspunten hierboven zorgen allebei voor een betere QoS voor het netwerk.

## Back-up: Research

### TFTPD

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 manoeuvre 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.

### Conclusie: Back-up

We hebben een applicatie nodig die ons gaat helpen om via de commande-line in onze switch of router een backup te maken en op te slaan naar de gewenste locatie. Zodat we geen copy-past manoeuvre 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.

## Bittorrent:Oplossing

### Scavenger

Er wordt gebruik gemaakt van Nbar. De p2p verkeer wordt gemarkeerd en krijgt een Scavenger classe. Hierdoor heeft p2p een lage prioriteit bij opstoppingen, waardoor belangrijke verkeer voorrang krijgen. Scavenger Classes hebben een prioriteit van 1%.

#### CEF

Dit zorgt ervoor dat de *packet forwarding* sneller gaat. Dit staat altijd uit op de toestellen dus moest eerst aanzetten.

#### Class-map

De verschillende verkeerstypes worden geclassificeerd door gebruik te maken van de *protocole*. Hier matchen we op de protocollen zelf.

#### Policy-map

Policy-map zegt wat er moet gebeuren met een het verkeer als het herkend wordt. Hier wordt er een DSCP-waarden van *CS1 gegeven. Dit is de laagste waarde.*

#### Interface

De QoS regel moet een interface gezet worden om de regel toe te kunnen passen. Eerst moet Nbar aangezet worden. De regels worden alleen toegepast op het verkeer die naar buiten gaat.

## Telefone/VoIP: Oplossing

### Telefonie/VoIP

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.

#### Class-map

De verschillende verkeerstypes worden geclassificeerd door gebruik te maken van de protocol of de DSCP-waarden.

#### *Match*

De classificatie moet gebeuren op een specifieke verkeerstype. Om dit te doen moet het verkeer gelijkgesteld worden aan een verkeerstype. Dit wordt gedaan met *match*

#### Protocol

Een van de manieren om het te matchen is via een protocol die herkend wordt door Nbar QoS. Met deze optie is het heel gemakkelijke omdat het op een specifiek protocol gedaan wordt

#### DSCP

Het machten kan ook gedaan worden met de DSCP-waarden. Dit is ook een hele goeie optie omdat de DSCP-waarde gereserveerd is voor een specifiek verkeerstype. BV: EF is voor VOIP. Ten tweede de waardes hebben ook direct een eigen prioriteit gekregen.

#### Policy-map

Via de policy map kan de verschillende policy aan de verschillende soort netwerkverkeer geven. Via de policy-map kunnen de prioriteiten beheerd worden.

## Wachtwoorden: Oplossing

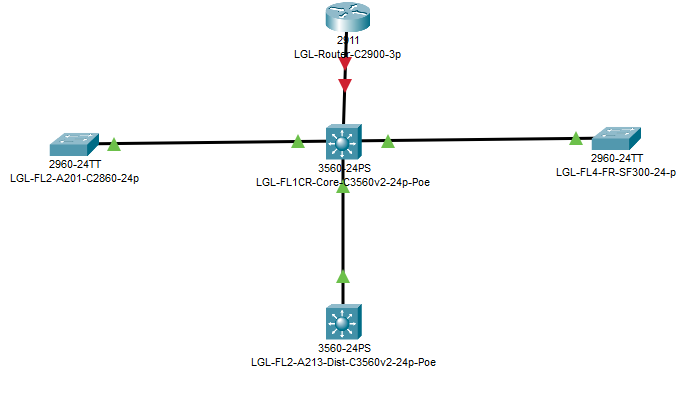
### AD

Via de Groupe Policy kan de Admin password policies implementeren. Deze verandering moeten worden gedaan via de Active Directory door de Admin. De Admin kan de policy toepassen op een specifieke *Group*, bv. Secretariaat. De implementaties worden dan doorgevoerd op alle gebruikers die in die groep zitten.

## Redundantie: Oplossing

### PVST+11

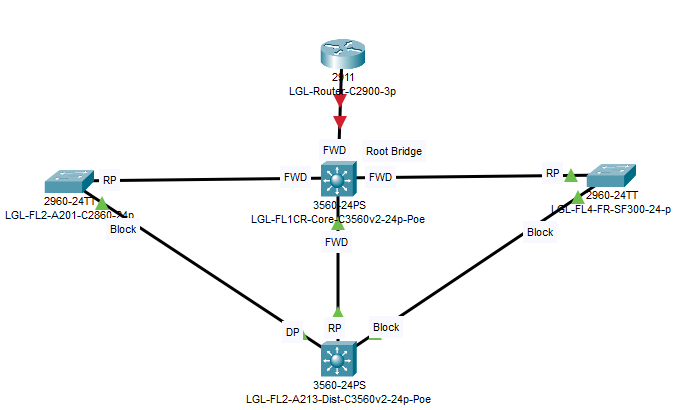
Bij het doornemen van de configuraties op de verschillende toestellen blijkt dat Spanning Tree Protocol (STP) aan staat. Er is nog geen configuratie en er ontbreekt nog 2 connecties.



Figuur 13 before STP

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.

#### Vlan

Bij pvst+ gebeurt spanning tree op tussen de vlans. Het is mogelijk om voor de eerste 5 vlans in het netwerk router a te kiezen als root en router b als secundairy. Voor de laatste 5 wordt de omgekeerde gedaan. Dit zorgt ervoor dat er zelfs tussen de vlan redundantie is.

Figuur 14 PSVT+

## Back-up: Oplossing

### TFTPD12

A close up of a sign

Description automatically generatedHet installatie en configuratie proces voor de tftpd64 is gemakkelijk en snel. De applicatie wordt geïnstalleerd. 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.

# Script (Implementatie)

De bedoeling van het project was om onderzoek te doen en vragen te stellen rond het optimaliseren van een netwerk. De bedoeling was om aan de hand van die onderzoeken en vragen, prototypes en oplossing te ontwikkelen die in de toekomst geïmplanteerd kunnen worden.

## Scripts uitleg

Alle oplossing zijn daarom ontwikkeld in een script form. Dat zijn regels codes die heel eenvoudige geïmplanteerd kunnen worden. De documentatie van het script van de verschillende oplossingen zijn onderverdeeld in vier delen. De volledige Scripts zijn te vinden op ImplemetatieScript.docx

De eerste deel is het script, die toegepast kan worden door te kopiëren/plakken in een switch of router. Tweede deel zijn de verschillende *show commands*, dit zal later besproken worden. In het derde deel wordt het volledige script geanalyseerd en uitleg gegeven over de verschillende codes. Ten slotte is er een uitleg van de verschillende *show commands* en waarvoor ze gebruikt worden.

### Scavenger

De scavenger implementatie zal ervoor zorgen dat de gekozen verkeerstype maar 1% prioriteit krijgt. De implentatie is heel eenvoudige. Bij het implementeren moet dit toegepast worden op de interface in de outbound richting. Dus dit betekent het verkeer naar buiten het netwerk.

### VoIP

De auto-Qos implementatie werd getest op het netwerk onder begeleiding, maar bleek niet te kunnen werken. Dit was omdat de OS-versie toch niet geüpdatet was. Auto-Qos is niet beschikbaar op de oudere versie van OS. Er os een LLQ-implementatie toegepast, met 2 verschillende policy-map. Dus voor deze opdracht werd er ook een script gemaakt voor de implementatie.

### PVST+

Deze script bestaat uit vier kleine script die geïmplementeerd moet worden op vier verschillende toestellen. De naam van de toestel waarop die deel van het script moet worden uitgevoerd, is te vinden in het vetgedrukt aan het begin van het script.

### Wachtwoorden

De policy voor de wachtwoorden werden uitgevoerd als test op de toestel van de stagiair. De werking was zoals verwacht. Voor deze oplossing is er geen script voorzien, maar screenshots van de verschillende stappen die genomen moeten worden om dit uit te voeren.

### TFTPD

Dit is een oplossing die heel snel en eenvoudig is toe toepassen. Voor deze oplossing zijn er ook screenshots voorzien. Deze oplossing werd toegepast door het stagebedrijf.

# Testing

## Shows

De *Show commands* kunnen gebruikt worden om configuraties te controleren. Via de show kunnen de configuraties gecontroleerd worden. Soms kan er met de show commands ook de werking van de configuratie gezien worden. De show commands zijn te vinden in de B of D van de scripts.

Naast de show commands voor het script, zijn er ook show en log command die gebruikt kunnen worden om het netwerk in het ook te houden. Er zijn *log* commands die gebruikt worden om via netflow het netwerkverkeer te bekijken. De verschillende commands die gebruikt werden bij de *prepare* fase voor het informatie verzamelen van het netwerkverkeer kan gebruikt worden om te testen.

Voor de scripts

## Test Scenarios

Voor elke probleem, werd er een test scenario gemaakt die gebuikt kan worden na de implementaties om de oplossingen te testen.

### PVST+

Om dit te testen moeten er test pakketjes verstuurd worden over een onderbroken connectie. Door de SPT moet er automatische een nieuwe weg gevonden worden. Dit kan getest worden bij de verschillende connectie om zeker te zijn dat er op de verschillende connectie redundantie is.

### Wachtwoorden

Bij implementatie een test periode van 30 dagen om te zien of alles goed werk, na de 30 dagen is de eerste mogelijkheid om wachtwoorden te wisselen, dat zal de eerste test zijn. Wanneer de gebruikers de wisseling doen kan er dan gecontroleerd worden of alles werkt zoals het hoort.

## Eigen Test

### Back-up

De evaluatie van deze oplossing of test van deze oplossing wordt direct gedaan tijdens het implementeren. Voor deze test is er geen wachttijd nodig. De test is geslaagd wanneer er een back-up gemaakt kan worden via de command-line naar en harde schijf of een server in het netwerk

### Wachtwoorden

De test zal 6 dagen duren. De boelding is om deze nieuwe policy in te stellen voor 6 dagen in plaats van de 4 maanden. Na 6 dagen zullen de nieuwe policy in werking treden. De verschillende regels waren actief. Na 6 dagen werd een nieuw wachtwoord gevraagd, bij het ingeven van een al gebruikt wachtwoord verschijnt er een error. Bij het ingeven van het foute wachtwoord, werd de Lock down geactiveerd.

# Besluit

Het grootte deel van het project was onderzoek. Ik heb veel moeten onderzoeken omdat ik helemaal niks wist over het onderwerp. En zelfs na het voltooien van het project, voelt het net of er nog veel meer te ontdekken valt over QoS.

Het project is goed afgerond en de bevindingen zijn met de verschillende begeleiders besproken geweest. “*Een succes indicatie dat deze concept goed toegepast werd, is dat er van elke deel minstens een oplossing toegepast wordt in het eindresultaat*.”Alle delen van de driehoek werden uitgewerkt.

De samenwerking met het bedrijf was heel aangenaam en verliep vlot.

# Literatuurlijst

# Bijlage