Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Ecriture de règles de conformité, mise à jour et création de cartes Weathermap, configuration de switches et correction de failles de sécurité

Félix TARI

STMicroelectronics

Responsable entreprise : Christophe BARBARISI

Responsable académique : Éric WÜRBEL

2018

Remerciements

Je tiens à remercier mon tuteur de stage Christophe BARBARISI pour la confiance qu'il m'a accordé en m'acceptant en stage et en me confiant des missions importantes et intéressantes.

Je remercie également Thierry BONNEL pour sa disponibilité et l'aide qu'il m'a apporté tout au long de mon stage.

Je suis très reconnaissant à l'équipe Réseau et Telecom avec qui j'ai passé ces 10 semaines pour leur sympathie au quotidien mais aussi toutes les personnes du service informatique pour leur accueil et gentillesse.

Table des matières

1 Introduction

Dans le cadre de mon DUT* Réseaux et Télécommunications de l'université d'Aix-Marseille, je devais réaliser un stage de fin d'études de dix semaines. Parmi les enseignements dispensés à l'IUT*, la matière qui m'intéresse particulièrement est celle des réseaux informatiques. C'est pourquoi j'ai souhaité orienter la recherche de stage vers ce domaine.

J'ai choisi d'effectuer mon stage dans cette entreprise car je savais que travailler dans un environnement informatique aussi développé que celui que j'ai rencontré allait me satisfaire pleinement.

Dans la première partie de ce rapport, je vous présenterai l'entreprise dans laquelle j'ai réalisé mon stage puis je vous expliquerai en détail en quoi ont consisté les missions que j'ai effectué.

2 Présentation de l'entreprise

2.1 Historique.

STMicroelectronics est née de la fusion entre la société Italienne Società Generale Semiconduttori et la société Française Thomson Semi-conducteurs en 1987. A sa tête se trouve Jean-Marc Chéry, PDG depuis Juin 2018.

Figure 1 : *Frise chronologique de* ***ST***

ST est une société implantée dans plusieurs pays comme le Maroc, en Italie, en Inde et en France avec les sites de Grenoble, Crolles et Rousset (site sur lequel j'ai effectué mon stage). Son siège social se trouve à Genève en Suisse. Elle emploie environ 45 500 salariés à travers le monde répartis dans 35 pays différents et possède au total : 11 sites de production principaux, plus de 80 bureaux de vente, 7 centres de R&D, et 39 centres de conception et d'application.

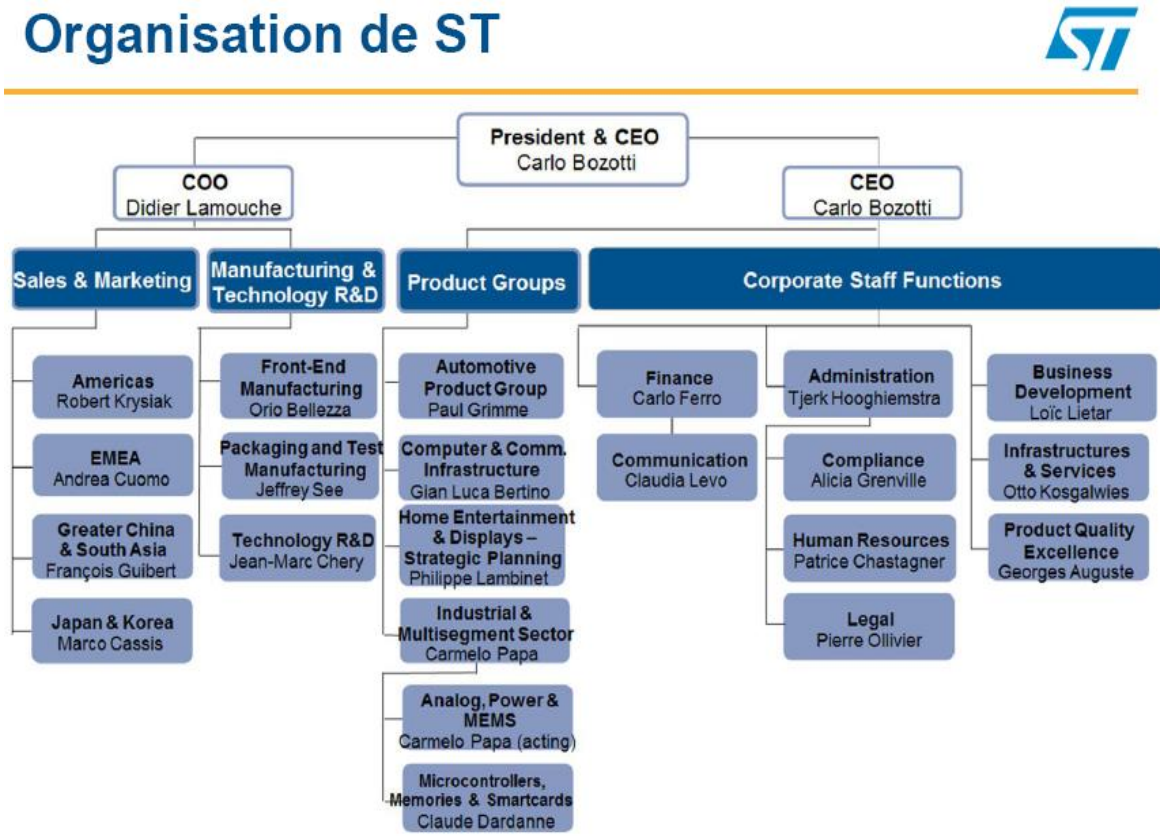


Figure 1 : *L'organisation de ST*

2.2 Activités

Le groupe STMicroelectronics est un des leaders de la technologie semi-conducteur, il est classé quatorzième vendeur mondial de semi-conducteurs au premier quadri semestre de 2018.

Le processus de production de semi-conducteurs peut être divisé en deux sous-processus communément désignés par les termes « front-end » et « back-end ». Le premier fait référence à l'étape de fabrication des puces à partir de plaquettes de silicium (appelées *wafers*) tandis que le deuxième concerne plutôt les parties de découpe des puces, d'assemblage et de tests.

Les sites de production « front-end » sont principalement situés en France et en Italie, tandis que les sites « back-end », nécessitant beaucoup plus de main d'œuvre, ont tendance à se trouver en Asie où le cout est moindre.

Le catalogue des produits de STMicroelectronics lui permet de se positionner sur 5 marchés différents réunis en 2 grandes catégories :

Sense & Power and Automotive
- Les MEMS et capteurs
- Les composants automobiles
- Les produits à faible consommation (Smart Power)

Embedded Processing Solutions
- Les mémoires et microcontrôleurs
- Les processeurs d'application

On retrouve ces produits dans différents domaines, notamment les télécommunications, les loisirs, les systèmes de paiement bancaires, les transports, mais aussi la santé et l'environnement.

A cela s'ajoute un panel de plus de 1500 clients (dont des géants comme Bosch, Apple, Samsung, Sony, Cisco, Hewlett-Packard ou encore Siemens), qui est une véritable force pour l'entreprise.

2.3 Le site de Rousset

Le site de Rousset est un site de fabrication de 37 ha « front-end ». Il a été créé en 1979 avec la construction d'une fab (Unité de production) produisant des puces sur des plaquettes de 4 pouces (100mm). Cette unité de production fût convertie en 1996 en une fab 6 pouces (150mm). En 2000, une unité 8 pouces (200mm) est inaugurée sur le site. Ce dernier produisit les deux technologies en parallèle pendant plusieurs années. La fab 6 pouces a, par la suite, été reconvertie en salle de tests pour les plaquettes de silicium (Electrical Wafer Sort) suite à un transfert des compétences vers l'Asie.

Figure 2 : *Le site de* ***STMicroelectronics*** *Rousset*

Actuellement le site de Rousset compte plus de 2700 salariés, une salle de test de 3500 m2, une salle blanche (fab) de 8 pouces, une production de7800 plaquettes semaine et un chiffre d'affaire en 2016 de 636 908 400 euros.

3 Présentation du cadre technique général du sujet

3.1 Contexte

Dans un contexte ou l'usine doit être en fonctionnement 24/24 pour assurer une qualité et une rapidité de production maximale, une seule interruption du réseau entrainerait des retards de fabrication conséquents et engendrerait donc une perte d'argent pour l'entreprise et potentiellement une perte de client.

Pour éviter ce qu'on appelle une ITP (Interruption temporaire de production) de nombreuses informations sont à surveiller : l'utilisation de la bande passante, l'état de fonctionnement des liens, les problèmes de câblage ou le bon cheminement des informations entre machines. De nombreux outils de supervision sont disponibles pour s'assurer du bon fonctionnement de toute ces variables.

Empêcher tout types d'intrusions ou attaques informatiques et aussi un gage de fiabilité auprès de clients prestigieux c'est pourquoi le service sécurité de Rousset fournit régulièrement des rapports de sécurité que le matériel informatique doit respecter.

Dans le contexte de l'informatique ou les progrès et innovations ne manquent pas, le site de Rousset se doit d'améliorer et renouveler en permanence son parc informatique. J'ai eu la chance de faire mon stage dans une période de remplacement du cœur de réseau du site.

3.2 Définition des objectifs du stage

Dans le contexte expliqué précédemment j'ai eu plusieurs tâches à accomplir.

Mon premier et principal objectif fut d'effectuer des tests de compliance* sur l'ensemble des équipements réseau (ici je parle de switches) du site de Rousset. Je devais donc m'assurer que certaines commandes présentes dans la configuration des switches ne pouvaient pas causer de problèmes de sécurité en m'appuyant sur un rapport fournit par le service sécurité, réciproquement si des commandes devaient apparaitre et n'y étaient pas je devais aussi le détecter.

Mon second objectif était la mise à jour et la création de cartes topologiques du réseau sur Weathermap. J'ai dû créer des nouvelles cartes qui n'existaient pas et mettre à jour d'anciennes cartes pour qu'elles correspondent à la topologie nouvellement modifiée par le changement du cœur de réseau.

J'ai eu à configurer des switches qui allaient remplacer des anciens ou des châssis qui allaient accueillir deux anciens switches. Durant la fin de mon stage j'ai participé à la correction de failles détectées par QUALYS.

Pour mener à bien ces missions j'ai dû apprendre à utiliser Cisco Prime Infrastructure (CPI*) un logiciel propriétaire Cisco de gestion du cycle de vie de réseaux convergés avec et sans fil.
J'ai également appris à me servir de Weathermap, un outil open source de visualisation de réseau, qui utilise des données récoltées par Nagios pour créer un aperçu de l'activité réseau sous forme de carte.

4 Tests de conformité

Cisco Prime Infrastructure un logiciel propriétaire Cisco de gestion du cycle de vie de réseaux convergés avec et sans fil. Il intègre Cisco Prime LAN Management Solutions (LMS) et Cisco Prime Network Control System (NCS).
CPI utilise le protocole SNMP pour récolter toutes les informations nécessaires des switches pour pouvoir les manager
Il possède de multiples fonctionnalités, dont le monitoring des différents équipements réseaux avec création de statistiques indicateurs de performances, propose un système d'alerte avec lequel on peut se tenir averti directement par mail ou SMS si quelque chose ne fonctionne pas correctement, archivage et visualisation de configurations et application de règles de conformité.

Au début de mon stage mon tuteur Christophe BARBARISI m'a confié un dossier papier écrit par le service sécurité. Ce dossier contenait les standards de sécurité réparties sur plusieurs chapitres que l'entreprise devait respecter en termes de configuration de switches. On m'a donc confié comme travail de créer avec CPI des règles de compliance pour chaque chapitre.

Dans un premier temps j'ai donc dû me familiariser avec cet outil étant donné que la formation que j'ai suivi jusqu'à maintenant ne proposait pas de cours à ce sujet. Une fois l'outil maitrisé j'ai pu commencer mon travail.

Une règle de conformité se nomme « policy » (« policies » au pluriel), il existe un menu de CPI dédié à la création, l'édition et la visualisation des policies. J'ai donc commencé par faire des recherches parmi celles déjà existantes pour vérifier s'il n'y en avait pas qui pourraient correspondre parfaitement ou partiellement à des chapitres de mon rapport. J'en ai trouvé quelques-unes et les ai renommés pour respecter un certain standard : STM-ROU-XXX
Ici le STM signifie STMicroelectronics, le ROU pour Rousset et le XXX est une chaine de caractères clés pour identifier et différencier cette policy des autres.

Après avoir terminé cette vérification j'ai commencé à répertorier dans un tableau Excel les correspondances entre les policies déjà découvertes et les chapitres du rapport du service sécurité. Au fur et à mesure de l'avancé de mon travail, je remplissais ce tableau (Voir annexe Figure 1).

A partir de ce moment, c'est moi qui ai dû créer toute les policies pour satisfaire les demandes de sécurité pour l'entreprise. J'en ai créé 9 et modifié 4 déjà existantes. Je ne vais pas détailler la création de chaque policy, mais plutôt celle d'une seule qui regroupe toutes les caractéristiques et connaissances que j'ai pu apprendre dans le but d'expliquer ce que j'ai dû faire pour cette mission.

Une policy se compose d'une ou plusieurs règles (rules) qui elles même contiennent une ou plusieurs conditions.

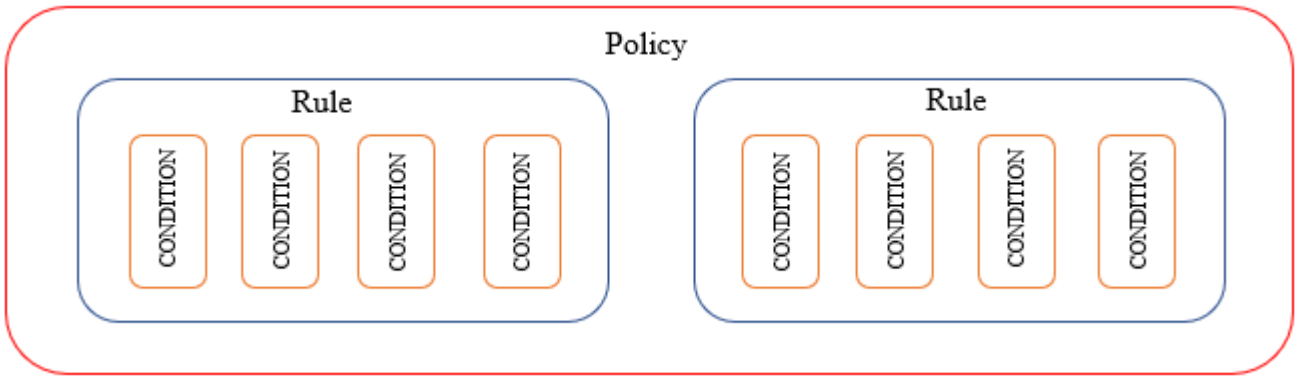


Figure 3 : *Composition d'une Policy*

4.1 Création d'une policy

La toute première étape est la création de la policy. Cette étape et les suivantes sont assez simples. En effet, CPI propose une interface graphique compréhensible et approchable quand on sait précisément ce qu'on veut faire ou chercher. Comme je l'ai dit précédemment, CPI a un menu dédié aux policies dans Menu -> Configuration -> Compliance -> Policies. C'est dans ce menu que 80 % du travail va être effectué et c'est donc ici que l'on va créer notre policy.

D'après le chapitre quinze du rapport du service sécurité qui traite du DHCP snooping*, les ports en mode trunk des switches d'accès doivent contenir la commande « ip dhcp snooping trust » et ceux en mode access doivent contenir la commande « ip dhcp snooping limit rate 100 ». C'est pour vérifier cela que j'ai créé la policy que je vais présenter. Une fois la policy créée et nommée on peut lui rajouter un descriptif pour que, dans le futur, les personnes voulant l'utiliser sachent exactement à quoi elle sert.

Cette étape ne demande pas de connaissances particulières, il suffit juste de cliquer sur une icône.

4.2 Créer une règle

Il va ensuite falloir écrire les règles qui vont la composer.

Pour cet exemple je vais créer deux règles :

- Premiere règle : Elle s'occupera seulement des interfaces en mode trunk donc celles où on veut verifier que la commande « ip dhcp snooping trust » soit présente.
- Deuxieme règle : Celle-ci s'occupera seulement des interfaces en mode access donc celles où on veut verifier que la commande « ip dhcp snooping limit rate 100 » soit présente.

Dans l'étape de création de règle je vais devoir renseigner une nouvelle fois un descriptif de ce qu'elle va effectuer, mais aussi son impact et les solutions envisageables si jamais la règle n'est pas respectée.

Ensuite je dois renseigner sur quels équipements je veux que la vérification s'effectue. J'ai choisi de cocher la case permettant d'appliquer la règle sur tous les équipements IOS sans tenir compte d'un modèle spécifique de switch, étant donné que je veux vérifier l'intégralité des switches.

Enfin je peux choisir de créer un input. Ici je veux vérifier que la commande « ip dhcp snooping trust » est présente. Mais, si un jour je préfère vérifier que ce soit la commande « ip dhcp snooping abcdef » (c'est un exemple pour expliquer la notion d'input mais dans ce contexte ça ne sert à rien étant donné que cette commande n'existe pas) qui est présente alors au lieu de changer les conditions nous allons devoir créer une saisie de texte.

Ici je veux créer un simple input de chaine de caractère sans valeur par défaut qui sera identifié par _parameter. Cet identifiant va être utilisé plus tard. Notons qu'on peut tout aussi bien rentrer une adresse ip, une liste de valeurs etc.

Maintenant que la règle est paramétrée je vais créer mes conditions.

4.3 Créer des conditions

La création des conditions est la partie la plus compliquée, mais aussi celle qui demande le plus de connaissances. Pour répondre à la demande initiale du chapitre 15 j'ai décidé d'écrire plusieurs conditions décrites ci-dessous.

Pour chaque règle il y aura donc 4 conditions :

- Première condition : Trier les switches par leurs hostnames pour ne garder que les switches d'accès.
- Deuxième condition (qui s'appliquera donc uniquement à la partie restante des switches triés à la première condition) : Regarder toutes les interfaces disponibles du switch.
- Troisième condition : Garder seulement les interfaces en mode trunk.
- Quatrième condition : Vérifier que la commande « ip dhcp snooping trust » est bien appliquée à l'interface.

Pour cette étape je vais accompagner mon rapport de captures d'écrans permettant une compréhension accrue de ce que j'ai réalisé.

4.3.1 Première condition : Trier les switch

Je rappelle ici que j'applique mes règles seulement aux switches d'accès. Après discussion avec mon tuteur, il m'a donné la liste des switches qui ne devaient pas être analysés. Pour cause de confidentialité, je ne peux pas donner les noms des switches, mais ils suivent tous une appellation standard qui change en fonction de leur utilité. Par exemple tous les switches dédiés aux ordinateurs de bureau ont la chaine de caractère OFF dans leur hostname. C'est donc plus facile de séparer un switch de bureau d'un switch de production.

Dans le menu condition scope (voir Figure 4) je dois préciser là ou va aller chercher la règle. Ici c'est « Device Command Outputs », c'est-à-dire la commande que je vais choisir va être exécutée sur les équipements et c'est le résultat retourné qui va être analysé. J'ai aussi la possibilité d'aller chercher directement dans la configuration du switch.

La commande choisie est « show running config | include hostname ». Ici la première partie de la commande sert à afficher la configuration de l'équipement et la deuxième partie (après le pipe) sert à afficher seulement les lignes incluant le mot « hostname ».

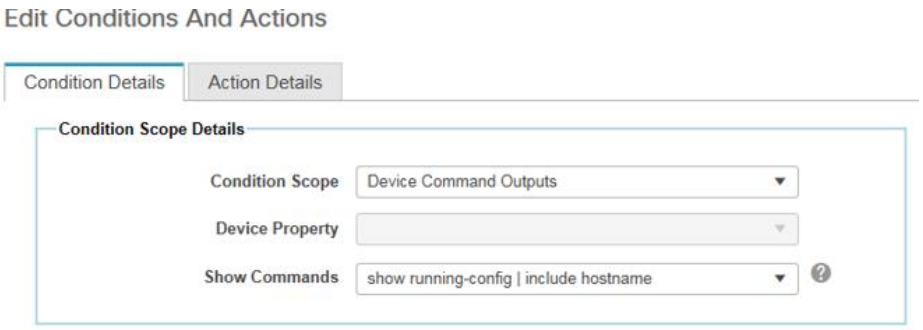


Figure 4 : *Condition Scope Details*

Pour finir je veux continuer à appliquer mes conditions mais seulement aux switches qui n'ont pas leur hostname composé des chaines de caractères BBN, CDR ou CDS. Je vais donc utiliser des expressions régulières.
Voici ce que renvoi la commande « show running config | include hostname » sur un switch. J'ai enlevé le début du hotstname pour des raisons de confidentialité.

```
 XXXXXXBBN1#show running-config | include hostname
hostname   XXXXXXBBN1
                   $(hostname).$(domain)
```

Figure 5 : *Résultat de la commande « show running config | include hostname »*

Je cherche donc une ligne commençant par hostname. Pour cela il faut utiliser le ^ avant le mot hostname.
Ensuite entre le mot hostname et le nom du switch il y a un espace. Pour représenter cette espace j'utilise un point dans l'expression régulière. Le point indique n'importe quel caractère. Pour représenter la chaine de caractère qui suit et qui peut être composée de lettres et de chiffres je mets simplement un « * » après le « . » pour indiquer une répétition de n'importe quel caractère. Enfin on indique la chaine de caractère qu'on veut identifier dans le hostname, pour identifier un nom contenant la chaine BBN on a donc : ***^hostname.*BBN***

Enfin, Je rajoute ensuite un point pour représenter un chiffre (ici le 1 après BBN)

Nous nous voulons aussi trier les switches CDR et CDS nous allons donc reprendre la même expression régulière en remplaçant BBN par CDR et en mettant un | entre les deux. Le | détermine une alternative, par exemple si on utilise a|b cela veut dire que ça sera ou a ou b.
Au final on obtient donc : ***^hostname.*BBN.|^hostname.*CDR.|^hostname.*CDS.***

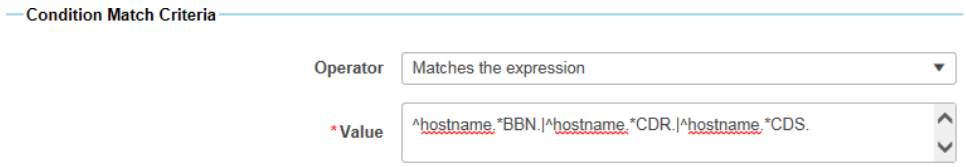


Figure 6 : *Condition Match Criteria*

Dans la fenêtre Action Details nous allons mettre « continue » si ça match avec l'expression régulière, c'est-à-dire si on ne trouve pas BBN, CDR ou CDS dans le hostname. En mettant « continue » je demande à CPI de continuer à exercer les conditions qui vont suivre seulement sur les switches qui auront matché.

Figure 7 : *Select Match action*

Si ça ne match pas je mets « does not raise a violation » pour ne pas déclencher d'alarmes et arrêter le processus.

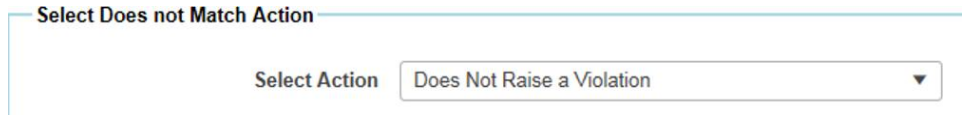


Figure 8 : *Select Does not match action*

Fin de la première condition.

4.3.2 Deuxième condition : Récolter les interfaces sous forme de blocks

A partir de maintenant toute les vérifications et/ou modifications qui vont être effectuées seront appliquées seulement sur les switches ne contenant pas BBN, CDR ou CDS dans leur hostname.

Pour cette condition je choisis de faire une recherche dans la configuration il faut donc la sélectionner dans le champ « scope ».

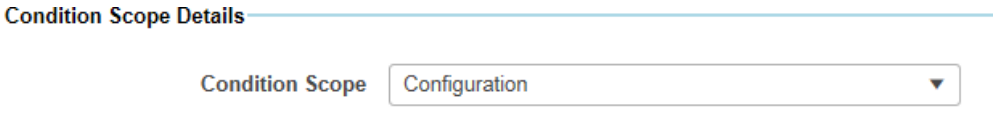


Figure 9 : *Condition scope details*

Ensuite mon but est d'analyser chaque interface et sa configuration. Dans la configuration générale d'un switch les paramètres d'une interface sont affichés en block (Voir annexe Figure 2). En cochant l'option « Parse as Blocks » et en écrivant l'expression régulière adéquat (Voir Figure 10 « Block Start Expression ») j'ai la possibilité d'analyser chaque interface et les paramètres qui lui sont associés.

Figure 10 : *Block Options plus l'expression régulière utilisée*

Cette condition ne sert qu'à identifier toutes les interfaces d'un switch il n'est donc pas utile de lever d'alarmes. Je ne change pas les Action Details, je laisse « Continue » pour « Match the expression » et « Does not raise a violation » pour « Does not Match ».

Pour résumer, à ce moment-là la condition 3 ne s'appliquera qu'aux interfaces (Condition 2) des switches d'accès (Condition 1)

4.3.3 Troisième condition : Garder les interfaces trunk

Le rôle de cette troisième condition va être de séparer les interfaces en mode trunk des autres.

Grace à la condition précédente j'ai des blocks, chaque block correspond à une interface. Pour analyser la configuration de chaque interface dans cette condition, je dois récupérer les blocks identifiés juste avant, pour cela il faut choisir « Previously Matched Blocks » (Voir Figure 11)

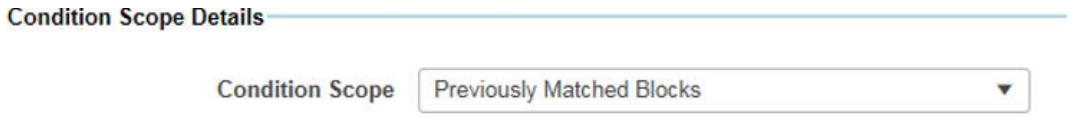


Figure 11 : *Condition scope details*

Pour vérifier que l'interface est un mode trunk il faut parcourir le block et trouver la commande « switchport mode trunk » qui est une chaine de caractère.

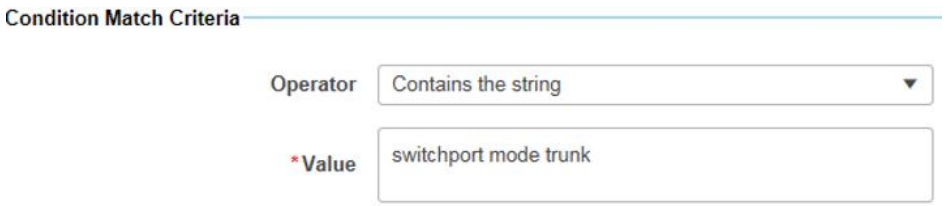


Figure 12 : *Condition match criteria pour identifier la commande cherchée.*

Pour les Actions Details c'est encore la même chose. Je continue si on détecte que c'est un port trunk et je ne lève aucunes alarmes dans le cas contraire.

Maintenant la dernière condition ne s'appliquera qu'aux interfaces (Condition 2) en mode trunk (Condition 3) des switches d'accès.

4.3.4 Quatrième condition : Vérifier la présence de la commande

Pour la quatrième et dernière condition je veux vérifier que la commande « ip dhcp snooping trust » est présente dans la configuration des interfaces trunk triées grâce à la condition précédente.

Même méthode que pour la troisième condition pour la « Condition Scope Details ». Mais ici j'inclus l'input que j'ai déclaré plus haut. Le paramétrage de cet input se fera au moment de lancer la Policy.

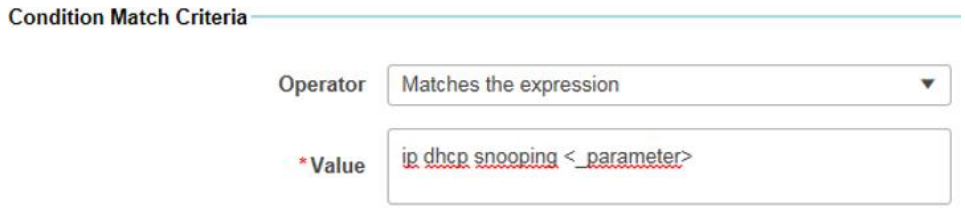


Figure 13 : *Condition match criteria pour identifier la commande cherchée avec l'input.*

Cette fois ci les actions changent.

Si ça match avec l'expression alors cela veut dire que la commande est présente dans la configuration de l'interface dont tout est validé. Dans ce cas on ne lève aucune alarme.

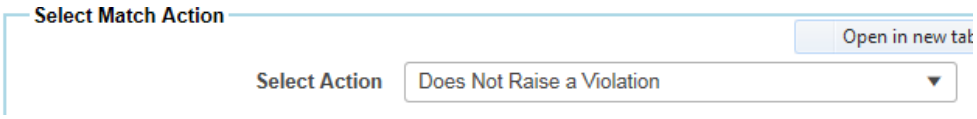


Figure 14 : *Select Match Action*

Cependant si ça ne match pas cela signifie que la commande n'est pas présente sur l'interface. Je vais donc lever une alerte (Raise a violation).
J'ai aussi la possibilité de choisir la gravité de l'alerte (ici je choisis Minor mais il existe aussi, dans l'ordre croissant de gravité, Info<Warning<Minor<Major<Critical) et enfin un message d'alerte personnalisé. Le <2.1> signifie Second condition/First parameter, cela permettra d'afficher dans le message d'erreur le numéro de l'interface ciblée. L'input est encore utilisé.

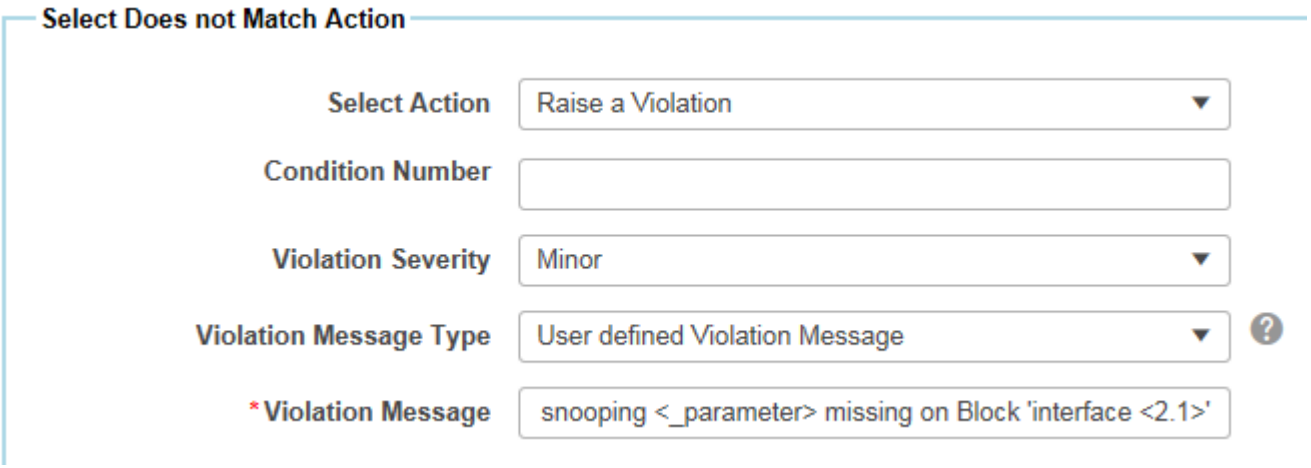


Figure 15 : *Select Does not Match Action*

Maintenant je dois sauvegarder la règle pour que la policy soit confirmée.
Pour résumer je viens de créer la règle qui ne s'applique qu'aux interfaces en mode trunk, il manque donc celle qui s'applique aux interfaces en mode access. Le processus est exactement le même à l'exception de la condition 3 ou cette fois au lieu de chercher la commande « switchport mode trunk » on cherche « switchport mode access ». CPI propose une fonction pour dupliquer les règles, j'ai donc dupliqué la première pour n'avoir qu'à modifier la condition 3 de la deuxième.

4.4 Créer un profile

Pour exécuter une Policy il faut l'insérer dans un profile dans le Menu -> Configuration -> Compliance -> Profiles.

La tache initiale demandée par mon tuteur était de créer un profile contenant toute les policies qui concernent le rapport du service sécurité. Je les ai donc toute créés, nommée et décrites pour en avoir un totale de 13.
J'ai mis ces 13 policies dans un profile que j'ai appelé, à la demande de mon tuteur, ROU-RMIS-CHECK.

C'est aussi ici que nous allons pouvoir remplir l'input. En remplissant comme ceci les inputs la valeur _parameter écrite précédemment dans la condition 4 sera remplacée par « trust »

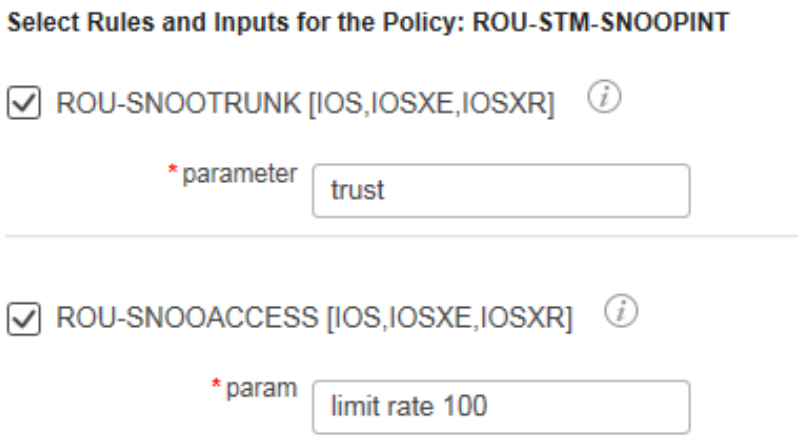


Figure 16: *Fenêtre de paramètres d'input*

Après avoir vérifié que toutes les policies soient bien présentes dans le profile il est temps de lancer le test.

4.5 Lancer un test

Avant de lancer le test je dois le paramétrer, j'ai donc la possibilité de choisir les équipements qui vont être vérifié, je peux par exemple sélectionner un seul switch pour tester mon profile sans que ça ne prenne trop de temps.
Ensuite deux choix s'offrent à moi :

- Lancer le test sur la configuration en cour dans les switches : C'est-à-dire envoyer des requêtes sur l'ensemble des switches. Les inconvénients de ce choix sont le temps élevé du test mais aussi la charge de trafic que toute les requêtes génèrent.
- Lancer le test sur les configurations archivées dans CPI : Ce choix prend moins de temps mais a un inconvénient. Si la configuration analysée est différente de celle qui est en cour (pour cause de modifications récentes par exemple) alors le résultat final sera faussé.

Je choisis donc la première possibilité pour obtenir les résultats les plus exacts.
Plus important encore, je peux choisir de programmer le test, dans un souci de gain de temps et d'optimisation mon tuteur m'a demandé de programmer le test tous les mois. Dans le cadre de cet exemple je choisis de le lancer une seule fois et tout de suite.

4.6 Visualiser les résultats d'un test

Une fois le test terminé il est possible de le visualiser en Naviguant dans le :
Menu -> Administration -> Dashboards -> Job dashboard
J'obtiens le détail du résultat avec le nombre d'erreurs, sur quel équipement, et le message d'alerte (Voir Annexe Figure 3). On peut très bien regarder toutes les erreurs dans ce tableau mais pour effectuer des tris ce n'est pas pratique notamment à cause des temps de chargement.

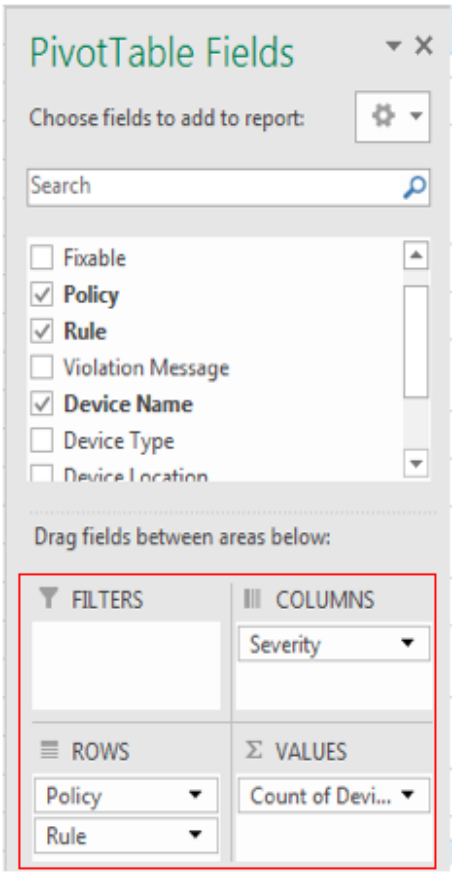
4.7 Faciliter la lecture d'un rapport grâce aux Pivot Tables sur Excel

Afin de faciliter la compréhension et la lecture d'un rapport on peut exporter le rapport sur Excel et utiliser des Pivot Tables.

Dans Excel je sélectionne le tableau brut à exporter et je clique sur « insert » puis « Pivot Tables ».

Nous allons pouvoir personnaliser notre Table. On peut voir que Excel reconnait automatiquement les différentes données qui sont présentes dans le rapport. On peut placer ces données dans quatre aires : les filtres, les colonnes, les lignes et les valeurs.
Pour l'exemple qui va suivre je vais créer une table affichant les différentes alerte existantes et leur nombre pour chaque Policy (Figure17).

En disposant nos données comme ceci nous obtenons ce résultat :



Count of Device Name	Column Labels						
Row Labels	Critical	Info	Major	Minor	Success	Warning	Grand Total
ROU-STM-DNS					115		115
DNS global config					115		115
ROU-STM-MANNET		14			446		460
enable password and enable secret					115		115
service password encryption					115		115
username xx password yyy		7			108		115
username xxx secret 5 yyyy		7			108		115
ROU-STM-MINSEC				115			115
ROU-MINSEC				115			115
ROU-STM-MOTD				20	95		115
ROU Global motd				20	95		115
ROU-STM-NTP					115	115	230
NTP access-group						115	115
NTP Sync IOS					115		115
ROU-STM-PORSEC		204		168	81	513	966
port security		204		168	81	513	966
ROU-STM-SCP				115			115
ROU-SCP				115			115
ROU-STM-SNMP					230		230
snmp community					115		115
snmp community rw					115		115
ROU-STM-SNOOP		4	25	40	59		128
dhcp snooping		4	25	40	59		128
ROU-STM-SNOOPINT				272	182		454
ROU-SNOOACCESS				226	90		316
ROU-SNOOTRUNK				46	92		138
ROU-STM-SSHV2				115	115		230
SSH timeout				115			115
SSHV2-Verif					115		115
ROU-STM-TELSSH					115		115
TRA-SSH					115		115
ROU-STM-WEBCONF					115		115
http services					115		115
Grand Total		14	208	25	845	1668	628	3388

Figure 17: *Organisation et visualisation de la ivot Table*

Les Pivot Tables permettent un accès plus rapide aux données que l'on veut afficher mais surtout un tri personnalisé qui n'est pas disponible sur CPI.

4.8 Travail demandé et problèmes rencontrés

Le but de cette mission était de pouvoir respecter les règles de sécurité standards fournies par le service sécurité en les regroupant sous forme de policies dans un profile et de pouvoir programmer le lancement des tests périodiquement. Dans un deuxième temps il fallait que je corrige les erreurs majeures et critiques (j'ai défini qu'es qui était critique ou majeur avec mon tuteur). J'ai complété cette mission avec succès

J'ai rencontré plusieurs problèmes comme les différences de version IOS qui n'affichaient pas certaine commande que je devais chercher avec mes règles. Maitrisant mal les expressions régulières j'ai dû effectuer une petite remise à niveau pour avancer dans mon travail. Avancer dans cette tache fut très long car pour vérifier que mes policies fonctionnaient je devais souvent effectuer des tests ce qui prenait environ 6 minutes pour chaque test plus le temps que les pages se chargent. Le fait que l'équipe avec qui je travaille ne maitrisait pas ou mal les tests de compliance j'ai dû progresser par moi-même.

Au cours de cette mission j'ai appris à maitriser CPI autant dans la création de règles de conformité qu'en visualisation de données et graphiques diverses en explorant les menus proposés. Le fait de travailler en relation avec les configurations de switches m'a permis de renforcer mes notions en termes de sécurité et d'apprendre de nouvelles commandes. J'ai découvert l'existence et l'utilisation des Pivot Tables et les utilise maintenant au quotidien dans mes autres taches.

5 Mise à jour et création de cartes Weathermap.

Weathermap, un outil open source de visualisation de réseau, qui utilise des données récoltées par Nagios pour créer un aperçu de l'activité réseau sous forme de carte. Nagios est un logiciel de supervision destiné à informer de problèmes éventuels dans votre système d'informations, il est, dans mon cas, hébergé sur un serveur apache.

Le travail que l'on m'a demandé de faire était de terminer la création des cartes correspondantes aux bureaux des bâtiments 6 et 8 pouces. J'ai eu à ma disposition l'éditeur graphique de Weathermap. Je me suis aperçu que ce qui était déjà présent sur les deux cartes était faux donc j'ai tout repris à Zéro.
Il existe deux façons différentes de créer une carte :

- Par l'éditeur graphique.
- En éditant directement le fichier de configuration de la carte qui se trouve dans /var/www/html/weathermap/configs.

J'ai commencé avec l'éditeur graphique pour placer mes switches, les configurer puis les relier entre eux.

5.1 Ajouter des Nodes

Je veux donc trois switches et deux liens. Le switch qu'on peut voir sur la photo est en fait une Node. Quand je clique sur la Node j'ai accès à son panneau de configuration.

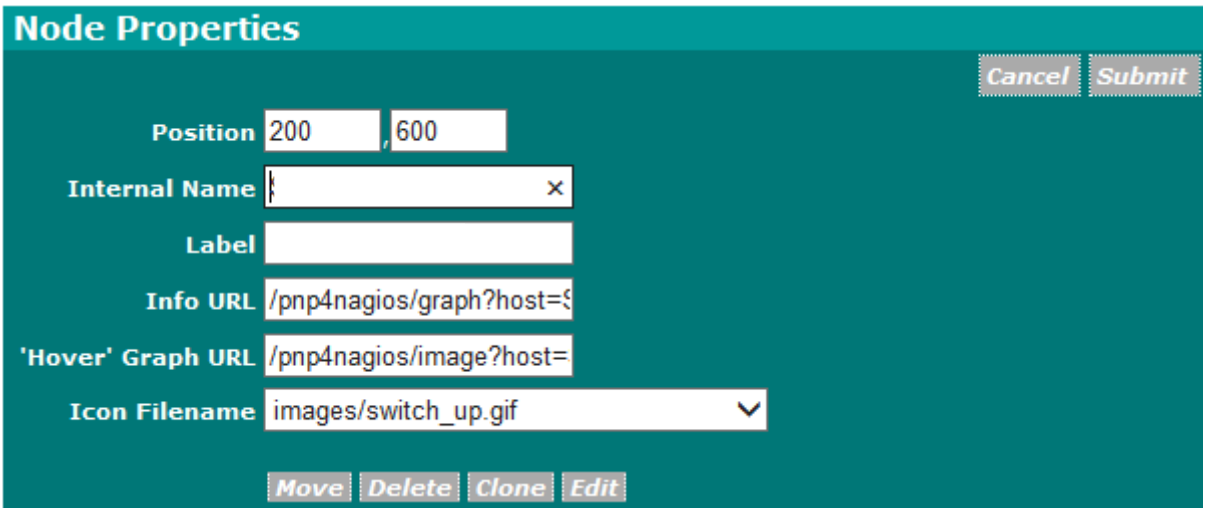


Figure 18: *Fenêtre de paramètres d'une Node*

La première étape est de définir la position de la Node, j'utilise un repère de 1900 x 800 pixels donc ici la Node est placée en 200 x 600.

La section Internal Name va définir le nom de la Node dans les fichiers de configuration tandis que le Label va seulement définir le nom du switch affiché sur la carte (la partie que j'ai flouté sur la Figure 18).
Les sections Info URL et 'Hover' Graph URL permettent de relier la Node aux données du switch récoltées par Nagios.
Enfin je peux affecter à cette Node n'importe quelle image du moment qu'elle est dans le dossier :
/var/www/html/weathermap/images.
Etant donné que des cartes existaient déjà j'ai pris la même image utilisée pour les switches.

5.2 Ajouter des liens

Viens maintenant la liaison des switches, pour ce faire je les relie simplement par un lien avec l'éditeur. En cliquant sur le lien j'ai accès à son panneau de configuration.

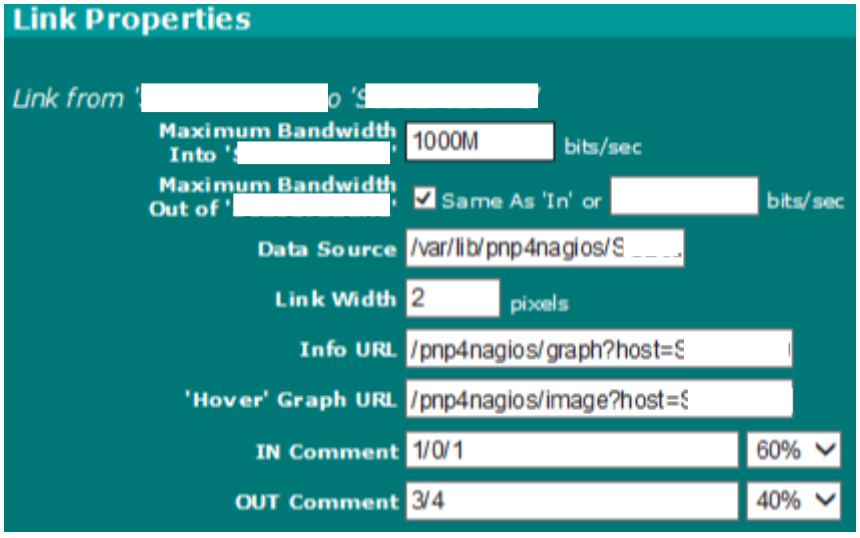


Figure 19: *Fenêtre de paramètres d'un lien*

Ici je peux donc configurer mon lien.
Les sections Data Source, Info URL et 'Hover' Graph URL permettent de relier le lien aux données des interfaces utilisées pour relier les deux switches entre eux. Les sections Maximum Bandwith et Link Width me donne la possibilité de modifier la bande passante maximale du lien et sa la taille qu'il aura sur la carte. Enfin je peux commenter le lien pour qu'apparaissent le numéro des interfaces et leur emplacement sur le lien en pourcentage, c'est-à-dire si le lien fait 100 pixels l'interface 1/0/1 sera marquée 60 pixels après le début du lien.

Quand un lien se crée il est droit et pour faciliter la visualisation des cartes j'ai dû les courber ou leur faire prendre des angles droits. L'éditeur ne permettant pas ceci (à causes de bugs) j'ai du directement aller modifier les paramètres des liens dans le fichier de configuration de la carte. J'en profite donc pour montrer comment cela se présente sous forme de texte.

```
NODE
        LABEL
        LABELOFFSET S
        INFOURL /pnp4nagios/graph?host=           &srv=_HOST_
        OVERLIBGRAPH /pnp4nagios/image?host=            srv=_HOST_&view=1&source=0
        ICON images/core_up.gif
        POSITION 850 150
```

Figure 19: *Configuration d'une Node en fichier texte*

```
LINK            node04171
        WIDTH 2
        INFOURL /pnp4nagios/graph?host=           &srv=IF-Gi0_1
        OVERLIBGRAPH /pnp4nagios/image?host=           &srv=IF-Gi0_1&view=1&source=0
        COMMENTPOS 60 40
        TARGET /var/lib/pnp4nagios/           'IF-Gi0_1.rrd:2:1
        INCOMMENT 0/1
        OUTCOMMENT 2/15
        NODES                    }
        BANDWIDTH 100M
```

Figure 19: *Configuration d'un lien en fichier texte*

Pour faire passer le lien par un point voulu (par exemple 51 51) je dois rajouter la ligne « VIA 51 51 »
Si je veux remplacer une courbure par un angle droit je rajoute la ligne « VIASTYLE angled »

A partir du moment ou j'ai maitrisé la création d'un switch et d'un lien j'ai pu avancer de plus en plus vite dans mon travail notamment en créant un fichier texte avec les lignes de configuration standard, j'avais donc plus qu'à changer le hostname et le numéro de l'interface puis à faire des copier-coller.

A la fin de mon stage j'avais donc créé deux cartes :

- Office 8 pouces
- Office 6 pouces (Voir annexe Figure 4)

À la suite de la migration du cœur de réseau et de deux locaux techniques j'ai aussi dû modifier les cartes :

- Office 8 pouces
- Test 6 pouces (Voir annexe Figure 5)
- Cœur de réseau (Voir annexe Figure 6)

Voici le résultat final de la carte Réseau Office 8 pouces :

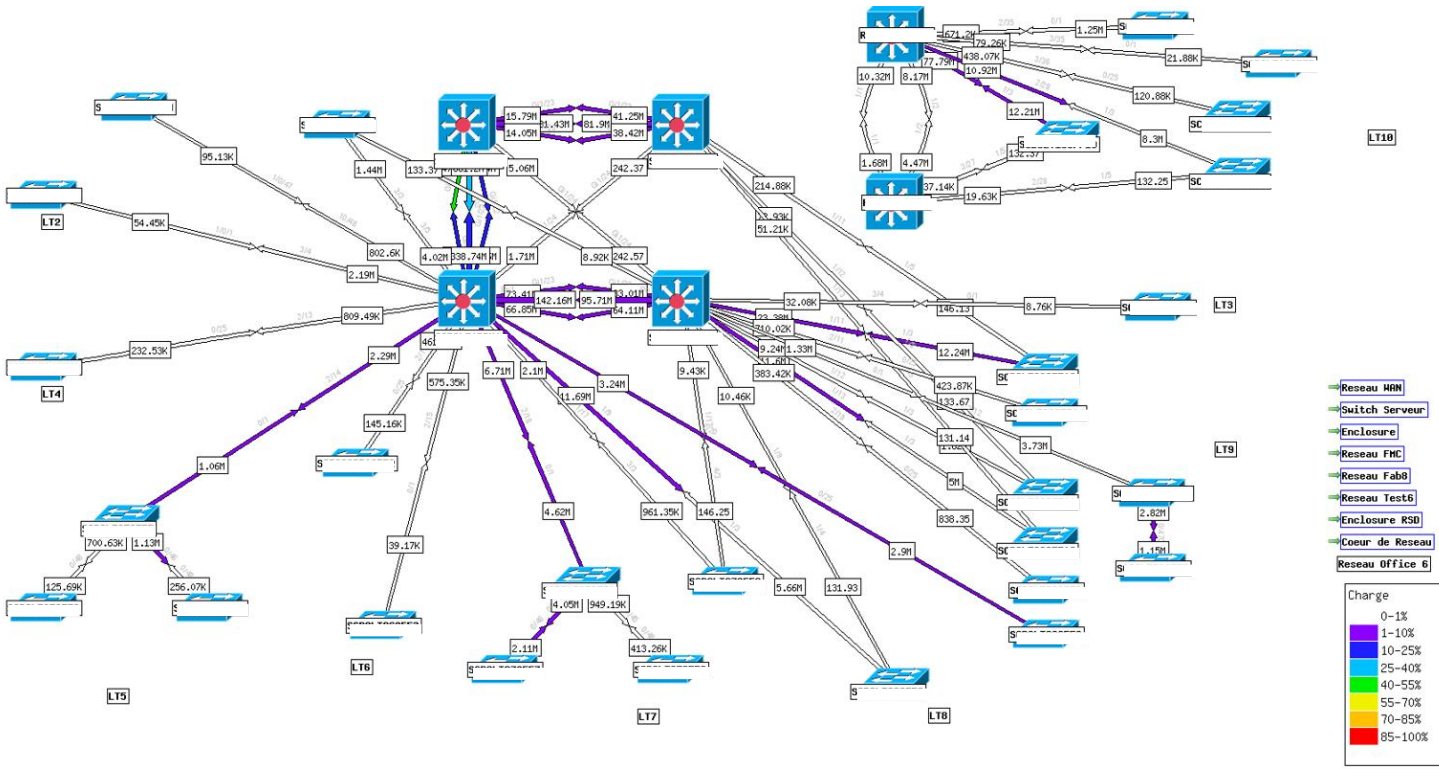


Figure 21: *Carte du Réseau Office 8 pouces*

5.3 Travail demandé et problèmes rencontrés

Mon travail était, en me basant sur des cartes imprimées, de refaire ces cartes mais sur Weathermap pour avoir en temps réel un aperçu du trafic pour chaque bâtiment. J'ai mené à bien cette mission jusqu'au bout.

J'ai rencontré plusieurs problèmes comme le fait que si je créé un lien de A vers B la configuration de ce lien ne sera pas la même que si j'avais relié B vers A. Pour palier à ce problème j'ai simplement utilisé le même sens de liaison pour toute mes cartes. Le serveur apache s'est aussi arrêté pendant une heure un jour m'empêchant toute modification. Je me suis aussi aperçu que malgré une bonne configuration il y avait certains switches ou liens qui ne fonctionnaient pas, en cherchant dans les fichiers de configuration j'ai compris qu'ils n'avaient pas été découvert par Nagios, j'ai donc lancé une découverte afin que tout fonctionne bien.

Ce travail fut très répétitif et long mais ce n'est rien comparé à ce que ces cartes peuvent nous apporter en termes d'informations en temps réel. J'ai donc appris à utiliser l'éditeur graphique de Weathermap et à me repérer dans ses fichiers de configuration. J'ai aussi appris de nouvelles commandes IOS pour voir à quels switches un autre pouvait être relié, à quelles interfaces et la bande passante du lien.

6 Configuration de switch et corrections de failles de sécurité

J'ai maintenant fini d'expliquer en quoi consistaient mes missions principale et secondaire, je vais maintenant parler des taches tertiaires que j'ai eu à faire.

6.1 Configuration de switches

Toujours dans une optique de renouvèlement du matériel informatique, mon tuteur m'a demandé de configurer un nouveau switch. Je devais donc mettre son OS (Operating System) à jour puis copier la configuration d'un switch déjà existant dans celui-ci. Je suis donc allé sur le site officiel de Cisco pour télécharger la dernière version d'IOS disponible pour le modèle de mon switch, en voulant l'installer j'ai malencontreusement effacé la version d'IOS présente sur la mémoire flash puis fait un reload.

Je me suis donc retrouvé avec un switch sans IOS qui démarrait qu'à partir du moniteur ROM. J'ai beaucoup cherché sur Internet comment revenir à la normale et j'ai trouvé des tutoriels expliquant comment faire des transferts de fichier par le câble console avec la commande Xmodem et TeraTerm (équivalent de Putty).
Le procédé affichant 10 heures de transfert, j'ai trouvé un moyen d'accélérer le processus en augmentant le débit de données à 115 200 bps (bauds per seconds).

Après avoir franchis cette étape j'ai copié la configuration de l'ancien switch dans un fichier Notepad++ puis dans le nouveau switch en changeant l'adresse du Vlan1 et les interfaces qui sont passées de Fast Ethernet à Gigabit-ethernet. Afin d'être sûr de moi j'ai installé un plugin de comparaison pour comparer l'ancienne et la nouvelle configuration. Voyant que certaines commandes n'apparaissaient pas dans l'une ou l'autre j'ai compris que c'était dû aux différentes versions d'IOS.

Dans un deuxième temps mon tuteur m'a demandé de commencer la configuration des interfaces d'un châssis qui allait remplacer deux anciens switches. Un châssis est composé de plusieurs « étages » par exemple un modèle 4506 aura 6 étages, un ou deux étages sont obligatoirement dédié aux cartes de supervision et les autres étages sont pour des cartes 24 ou 48 ports.

Pour identifier l'interface d'un switch normal on utilise Fast-Ethernet 0/13, sur un châssis on doit préciser le numéro d'étage en plus ce qui donne Fast-Ethernet 3/0/13 si c'est sur l'étage 3. Je devais donc récupérer les configurations des interfaces des switches 1 et 2 pour les transférer dans les étages 5 et 6 du châssis.
J'ai eu le temps de créer un fichier texte contenant toute les interfaces modifiées en fonction de l'étage qui allait les accueillir mais je suis arrivé à la fin de mon stage avant d'avoir pût injecter cette configuration dans le châssis.

6.2 Corrections de failles de sécurité

Durant la fin de mon stage l'équipe Administration Système m'a fourni un rapport d'un scan effectué par QUALYS (logiciel proposant des services de sécurité) révélant des centaines de failles de sécurité sur les IOS Cisco. Ce nombre de vulnérabilités dépassant de 18 % le seuil limite, mon tuteur m'a demandé de les réduire au maximum.

J'ai utilisé des Pivot Tables pour m'organiser et ensuite faire des recherches à propos des différentes vulnérabilités détectés et les solutions de contournement proposées. J'ai corrigé une centaine d'erreurs dont 90 venaient des mots de passes chiffrés en type 7 dans la configuration des switches, un mot de passe en type 7 est déchiffrable très facilement sur internet tandis qu'un mot de passe en type 5 énormément plus sécurisé.

Après cette session de correction un autre scan a été lancé et nous sommes passé à moins 7% de la limite autorisée.

7 Conclusion

Pour conclure ce rapport de stage j'ai mené à bien les deux missions importantes qui m'ont été confié, j'ai pu supprimer toute les erreurs critiques et majeures détectées sur CPI par mon profile et j'ai réussi à augmenter la visibilité du réseau du site avec mes cartes Weathermap. J'ai aussi pu corriger assez de vulnérabilité pour retomber en dessous de la limite autorisée. J'ai aussi écrit et mis à disposition une documentation permettant l'apprentissage de la création de tests de conformité.

Au cours de ce stage j'ai eu l'occasion de renforcer mes connaissances apprises à l'IUT et en acquérir de nouvelles concernant les IOS Cisco et les différentes méthodes disponibles pour sécuriser un réseau d'entreprise. J'ai aussi eu la chance de travailler avec une équipe d'intégrateur réseau de SFR venant participer à la migration du cœur de réseau du site de Rousset

Pour conclure ce stage de dix semaines je dois avouer que je me faisais une toute petite idée de ce que pouvait être le métier d'administrateur ou intégrateur réseau, j'ai découvert un « autre monde » que celui que j'ai côtoyé à l'IUT. J'ai commencé le 9 Avril avec de bonnes bases en termes de configurations de switches et même en connaissance de protocoles et cela m'a énormément aidé tout au long de mon stage et c'est pour cela que je me dois de remercier l'IUT Réseaux et télécommunications de Luminy pour la qualité et son enseignement et le matériel mis à disposition.

Ce stage m'a conforté dans mon idée de travailler dans le réseau en tant qu'administrateur ou intégrateur tout en ayant de fortes connaissances sur les aspects de sécurité.

8 Glossaire

SNMP, Simple Network Management Protocol

DUT, Diplôme Universitaire de Technologie

CPI, Cisco Prime Infrastructure

IUT, Institut Universitaire de Technologie

Compliance, Conformité

9 Sitographie

http://www.st.com/content/st_com/en/about/st_company_information/who-we-are.html

https://network-weathermap.com/

https://tools.cisco.com/security/center/publicationListing.x

10 Annexes

Rapport correspondance entre RMIS et policies			
Policy standard reference	**Detail of the standard**	**Policy correspondante**	**Actions à réaliser**
G002.02	Basic default configuration username and snmp community to delete	ROU-STM-WEBCONF ROU-STM-MANNET	Applicable
G002.03	Disable the web configuration	ROU-STM-WEBCONF	Applicable
G002.04	Disable telnet in support of SSH	ROU-STM-TELSSH	Applicable
G002.05	Disable SSH1 support	ROU-STM-SSHV2	Applicable
G002.06	1) Configure a domain name for the router 2) Specifies the version of SSH to be run on your router 3) Configures SSH control variables on your router 4) Disable Telnet access to the switch/router	1) ROU-STM-DNS 2) 3) ROU-STM-SSHV2 4) ROU-STM-TELSSH	1) Applicable 2) Applicable 3) Applicable 4) Applicable
G002.07	Disable the SCP server	ROU-STM-SCP	Applicable
G002.08	1) Enable 802.1x authentication 2) Set a maximum numbber of MAC associations per port 3) Enable ARP poisoning detection	ROU-STM-PORSEC	1) Non applicable 2) Applicable 3) Non applicable
G002.09	SNMP	ROU-STM-SNMP	Applicable
G002.10	Manage your network devices Out of Band		Non applicable
G002.11	Perform clock synchronization for all your network devices	ROU-STM-NTP	Applicable
G002.12	Backup your network devices		Non applicable
G002.13	Access ports security	ROU-STM-PORSEC	Applicable
G002.14	Minimum security settings for any network equipment	ROU-STM-MINSEC	Que la premiere partie est applicable
G002.15	Implement DHCP snooping	ROU-STM-SNOOP ROU-STM-SNOOPINT	Applicable
G002.16	Use Warning Banners	ROU-STM-MOTD	Applicable
G002.17	Disable all the services that are not needed		Non applicable
G002.18	Suscribe to Security Advisories		Non applicable
G002.19	Apply ST patch standard		Non applicable

Annexe Figure 1: *Correspondances entre Policies et chapitres du rapport*

```
!
interface FastEthernet0/6
description MBS A 01
switchport access vlan 59
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security aging time 1
switchport port-security violation restrict
switchport port-security aging type inactivity
no snmp trap link-status
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 100
!
```

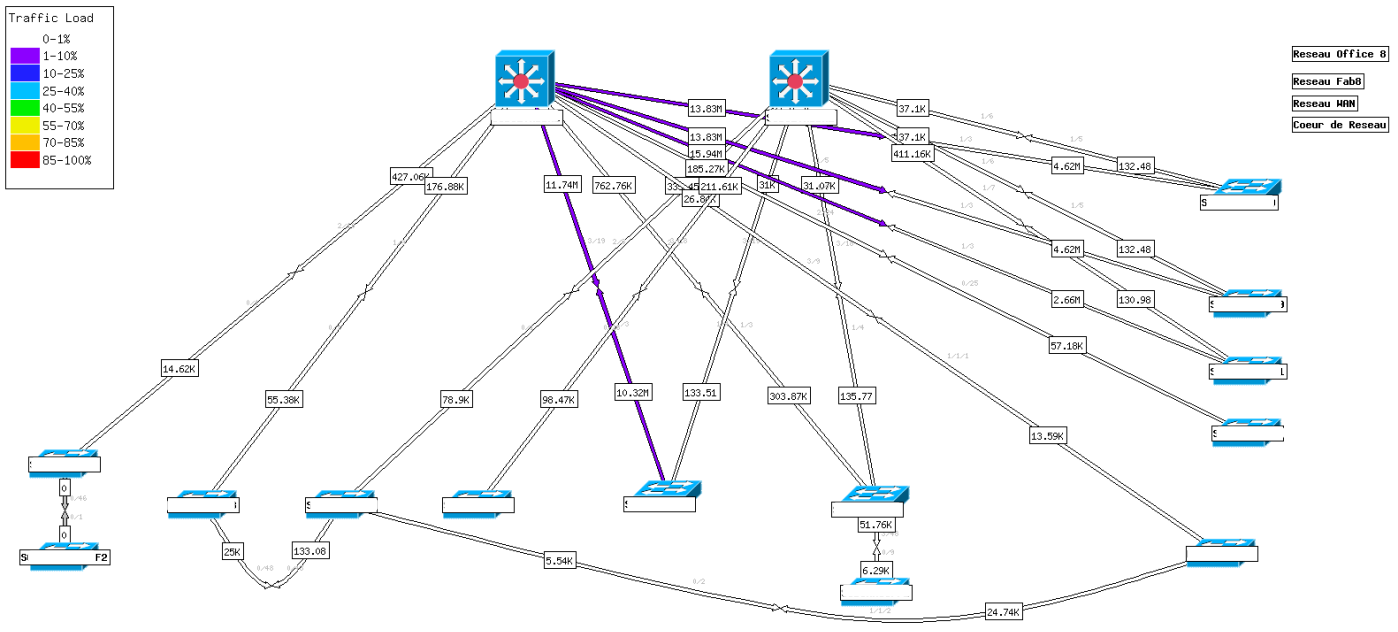
Annexe Figure 2: *Interface en block*

Policies/Rules (...					
All Policies	14	25	845	628	208
▶ ROU-STM-...	14	0	0	0	0
▶ ROU-STM-...	0	0	115	0	0
▶ ROU-STM-...	0	0	20	0	0
▶ ROU-STM-...	0	0	115	0	0
▼ ROU-STM-...	0	0	272	0	0
ROU-S...	0	0	46	0	0
ROU-S...	0	0	226	0	0
▶ ROU-STM-...	0	0	168	513	204
▶ ROU-STM-...	0	0	0	0	0
▶ ROU-STM-...	0	0	0	115	0
▶ ROU-STM-...	0	0	115	0	0
▶ ROU-STM-...	0	25	40	0	4
▶ ROU-STM-...	0	0	0	0	0
▶ ROU-STM-...	0	0	0	0	0
▶ ROU-STM-...	0	0	0	0	0

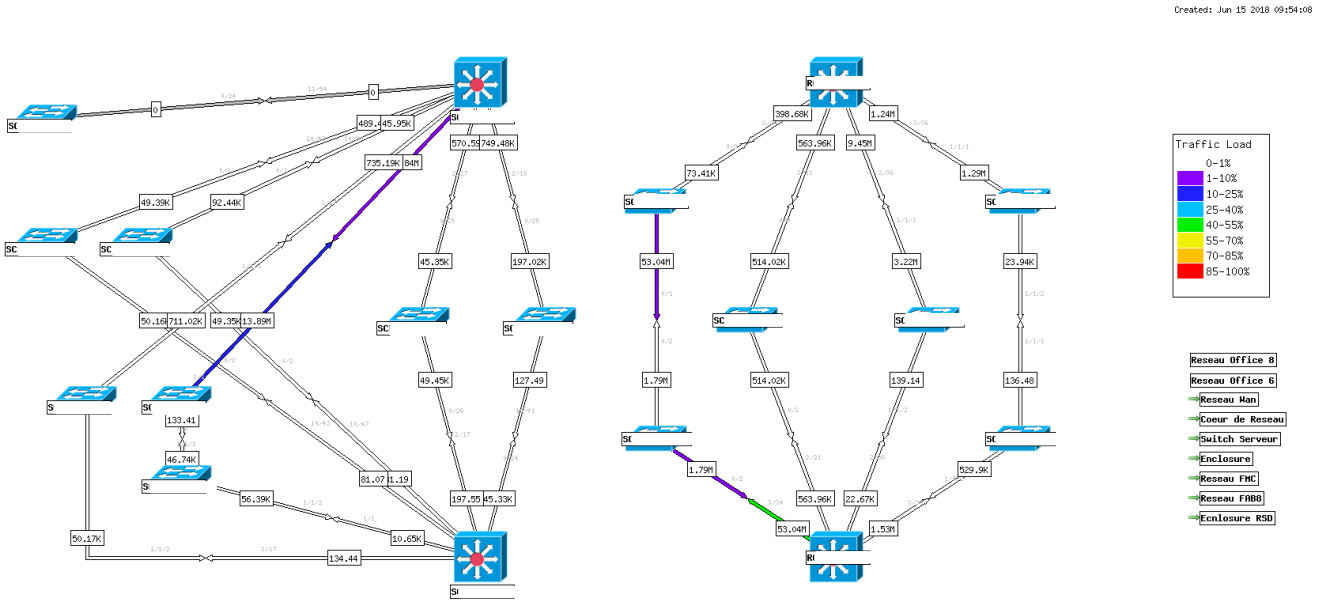
Annexe Figure 3: *Résultat test de compliance*

Severity	Fixable	Policy	Rule	Violation Message	Device Name	Device Type	Device Location
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	EWS
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560X-48T...	LTF
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560-48TS...	LTA
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560X-48T...	LTF
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560-48TS...	B3 ARM27
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560-48TS...	LT07
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 4506-E Sw...	ROUSSET 6 LTD
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco 3750 Stackable Swi...	ROUSSET 8" L...
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560X-48P...	LT03
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco 3750 Stackable Swi...	ROUSSET 8" L...
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560-48TS...	LT05
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst Blade Swit...	ROUSSET 8" L...
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560X-48P...	LT03
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 4507R plus...	ROUSSET 8 L...
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560-48TS...	B3 ARM27
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 4507R plus...	ROUSSET 8" L...
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	EWS
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	EWS
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	LTG
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	LTG
⚠	Not Fixable	ROU-STM-SN...	ROU-S...	command ip dhcp snoopin...		Cisco Catalyst 3560V2-48...	LTG

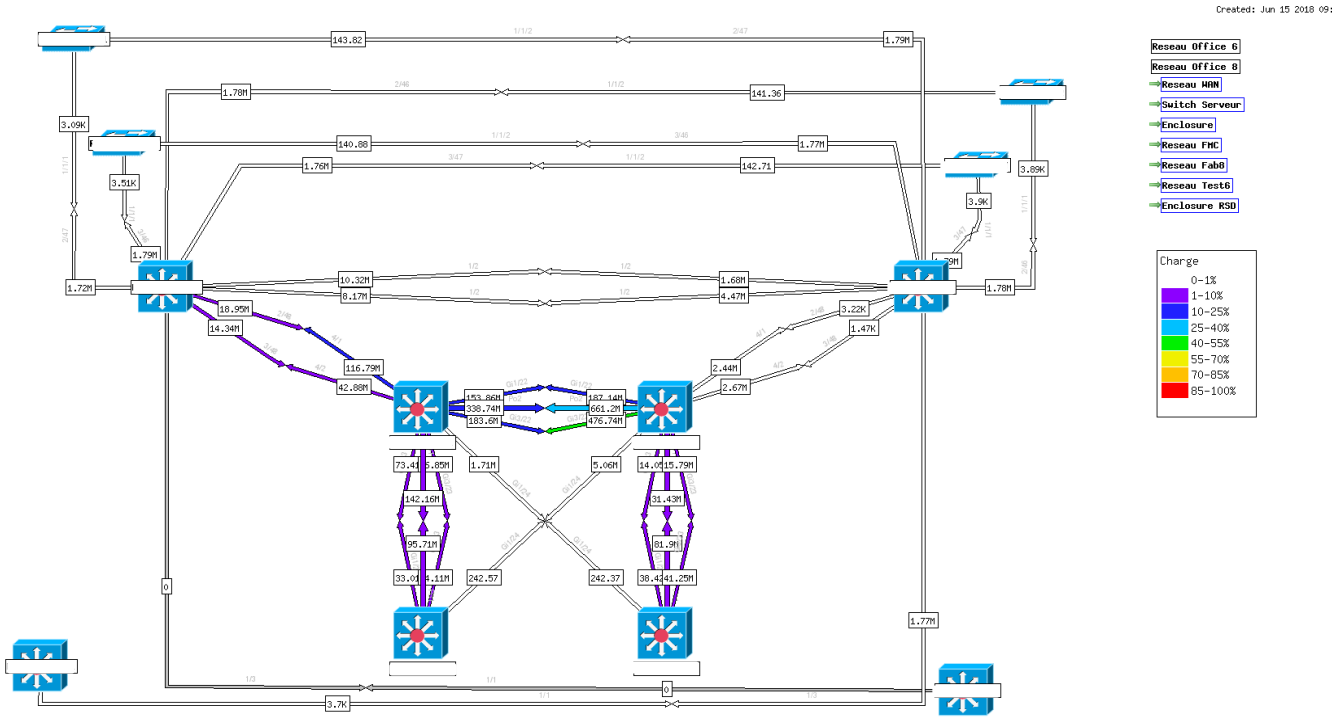
Annexe Figure 3: *Résultat test de compliance*



Annexe Figure 4: *Carte Office 6 pouces*



Annexe Figure 5: *Carte Test 6 pouces*



Annexe Figure 6: *Carte Cœur de réseau*