Théo Humbert

Projet 2 : Evolution infrastructure réseau

Table des matières

Annexes

- Procédure – Port-Security ;
- Procédure - Cisco ACL L3 Statique ;
- Procédure - Cisco Agrégation de liens LACP ;
- Procédure - Cisco Mise à jour IOS ;
- Procédure – Cisco switch 2950 Réinitialisation mot de passe ;
- Procédure – Cisco routeur 1800 séries Réinitialisation mot de passe ;
- Procédure - Cisco TFTP sauvegarde, restauration ;
- Liste des ACL ;
- Maquette Cisco Packet Tracer ;
- Schéma infrastructure ;
- Schéma câblage ;
- Photos de l'infrastructure ;
- Fichiers de configuration des équipements.

Contexte

L'entreprise **TiersLieux86** a confié un cahier des charges à **IT service86**, comprenant le maquettage et l'agrandissement de l'infrastructure du site de Chasseneuil. Le but étant d'améliorer la gestion des équipements d'interconnexion, d'assurer une meilleure sécurité mais aussi d'étudier et de mettre en place des solutions de tolérance de pannes tout en améliorant la bande passante. Dans un premier temps le client demande la réalisation d'une maquette pour ensuite prévoir le cout des solutions étudiées.

Voici le cahier des charges :

- La solution doit se faire avec les équipements réseau **CISCO** existants : l'ajout de matériel ne peut être envisagé que pour mettre en place de la tolérance de pannes ;
- La durée de **l'interruption de service** doit être minimale ;
- Les différents **commutateurs** ainsi que le routeur doivent disposer de réglages de base homogènes ;
- Les différentes configurations doivent pouvoir être **sauvegardées/ restaurées** rapidement et facilement ;
- Un système de **cloisonnement** du réseau à l'aide de **VLAN** devra être mis en place. Les commutateurs devront être facilement administrables afin de propager les configurations VLAN rapidement et aisément ;

- La **sécurité** au niveau du routeur devra être renforcée, les VLAN utilisateurs ne pouvant pas communiquer entre eux ;
- Des **procédures** permettant la sauvegarde / récupération des configurations, la mise à jour des IOS et la réinitialisation des mots de passe des switchs et du routeur devront être mises à disposition sur un serveur TFTP (l'utilisation du logiciel TFTP est acceptée) ;
- Un serveur **NTP** devra être mis en place pour la synchronisation des équipements réseau ;
- Un serveur **Syslog** devra être mis en place pour la collecte des journaux des équipements réseau ;
- Les évènements importants doivent être **journalisés** et stockés afin de faciliter le travail de l'administrateur ;
- Une **maquette** sur le simulateur Packet Tracer devra être réalisée afin de tester l'évolution de l'infrastructure réseau. Cette maquette devra permettre de vérifier le fonctionnement :
    - De **l'adressage** IP sur les équipements réseaux,
    - Du **DHCP**,
    - Du routage **interVLAN** ;
- Une présentation orale aidée d'un diaporama ou d'une vidéo se fera devant le directeur de TiersLieux86, le responsable Systèmes et Réseau d'ITS 86, afin de présenter de manière synthétique les changements effectués ;
- Les différentes solutions pourront faire l'objet de **documentations techniques** suivant la complexité de la mise en œuvre.

Concernant l'étude de l'évolution vers la tolérance de pannes des équipements réseau :

- La **tolérance aux pannes** des équipements actifs doit être mise en place ;
- Une maquette dissociée devra être réalisée afin de permettre de vérifier le fonctionnement de la tolérance aux pannes des équipements actifs :
    - Un moyen peu coûteux d'améliorer la bande passante est à prévoir au niveau des liaisons inter-commutateurs ;
    - De la tolérance de panne des commutateurs avec **RSTP**
    - De la tolérance de panne des routeurs (**HSRP ou GLBP**) ;
- Une présentation orale aidée d'un diaporama ou d'une vidéo se fera devant le directeur de TiersLieux86 et le responsable Systèmes et Réseau d'ITS 86, afin de présenter de manière synthétique les solutions mises en œuvre dans la maquette ;

Objectifs des missions

Chapitre 1 : Maquettage

- Structurer le projet ;
- Assimiler l'infrastructure ;
- Documenter grâce à des procédures ;
- Présenter le projet.

Chapitre 2 : Préparation du matériel

- Besoins technologiques ;
- Etude des solutions disponibles ;
- Analyse de l'interconnexion des équipements.

Chapitre 3 : Configuration basique du matériel

- Homogénéifié le parc ;
- Mettre en place les fonctionnalités standards des équipements.

Chapitre 4 : Amélioration de l'administration des équipements

- Permettre une gestion des ressources réseaux sécurisé ;
- Faciliter la réalisation des prochaines tâches ;
- Avoir une infrastructure fonctionnelle plus complète.

Chapitre 5 : Haute disponibilité

- Augmenter la résilience aux pannes du matériel ;
- Améliorer la bande passante disponible ;
- Permettre la répartition de charge.

Chapitre 6 : Sécurisation des équipements

- Améliorer la fiabilité des protocoles ;
- Renforcer les autorisations via des listes de contrôle d'accès ;
- Permettre un contrôle des flux réseaux ;
- Sécurisé les accès physiques aux machines ;
- Mettre en place des méthodes d'authentifications robustes.

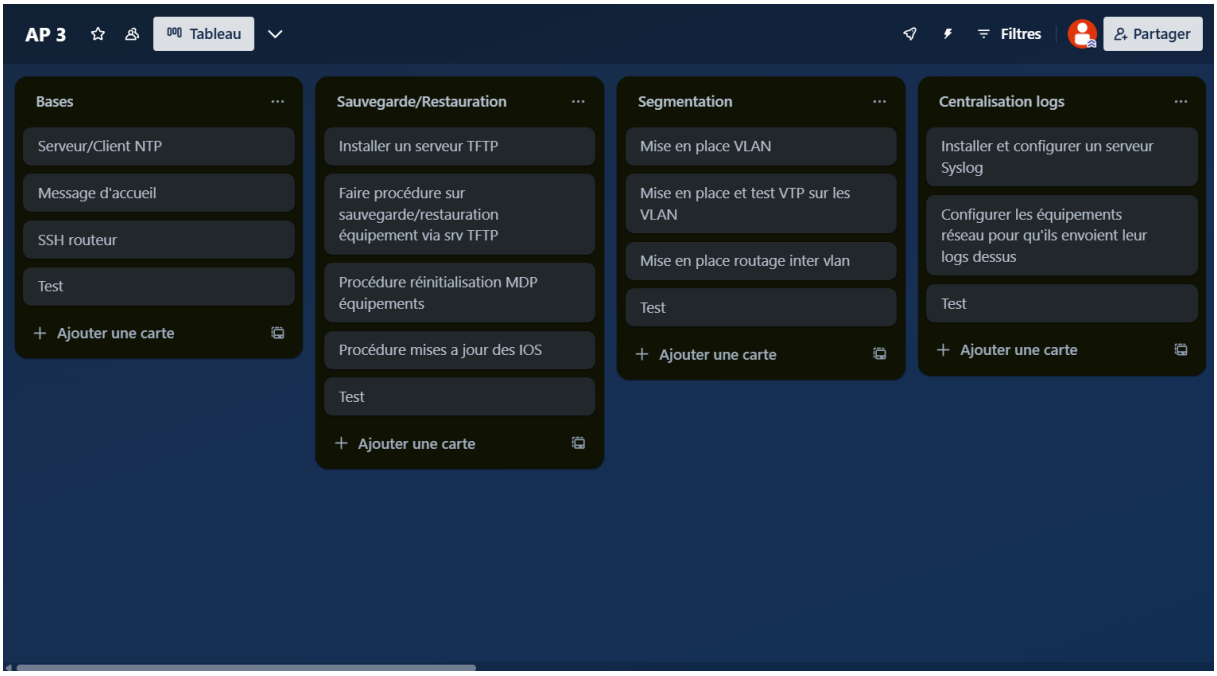
Chapitre 7 : intégration de l'infrastructure système

- Mettre en production l'infrastructure réseau réalisée.

Suivi de projet

Dans la continuité des projets précédent, j'ai établi une liste de tâches à réaliser selon le cahier des charges fournit. Pour avoir une vision plus claire de cet ensemble j'ai déployé cette liste sur un Dashboard de suivis de projet « Trello ».

Dans cette liste j'ai découpé les taches en sous tâches ce qui m'a permis d'avoir une meilleure vision organisationnelle pour le suivi de projet.

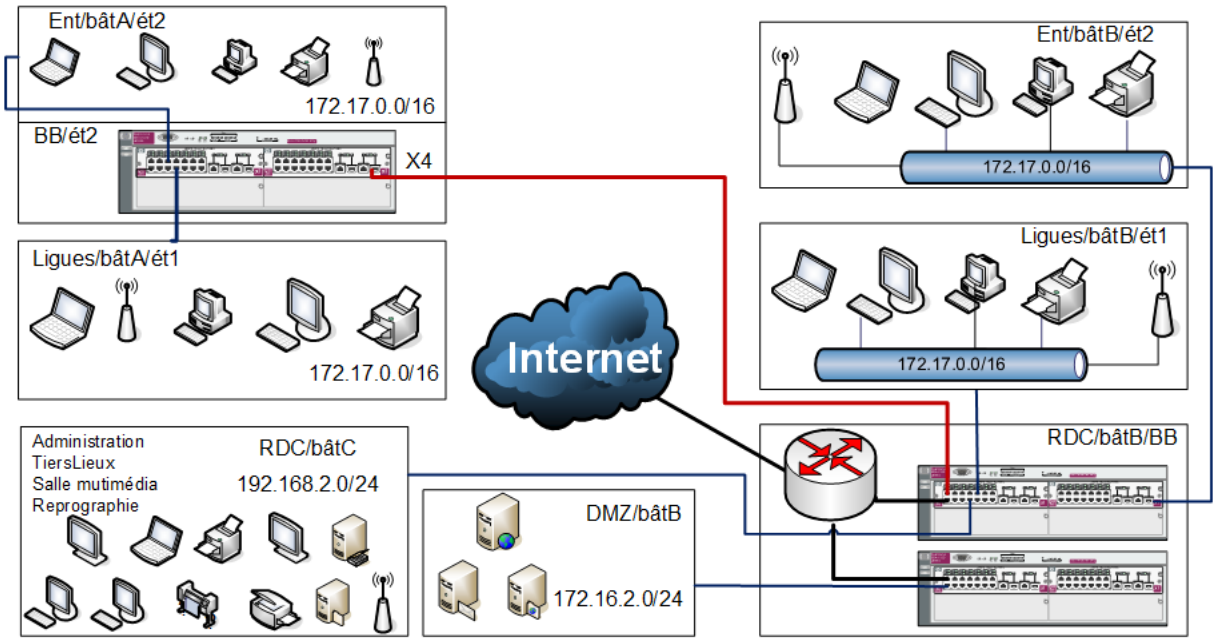


Chapitre 1 : Maquettage

Tâche 1 : Définition des besoins

Recensement des points sensibles

En partant de ce schéma, une étude sur les points faibles de l'architecture système et réseau a été menée.



On peut facilement se rendre compte que les probabilités d'interruption de service ou de perte de données sont assez hautes, aucune redondance, aucune sauvegarde ...

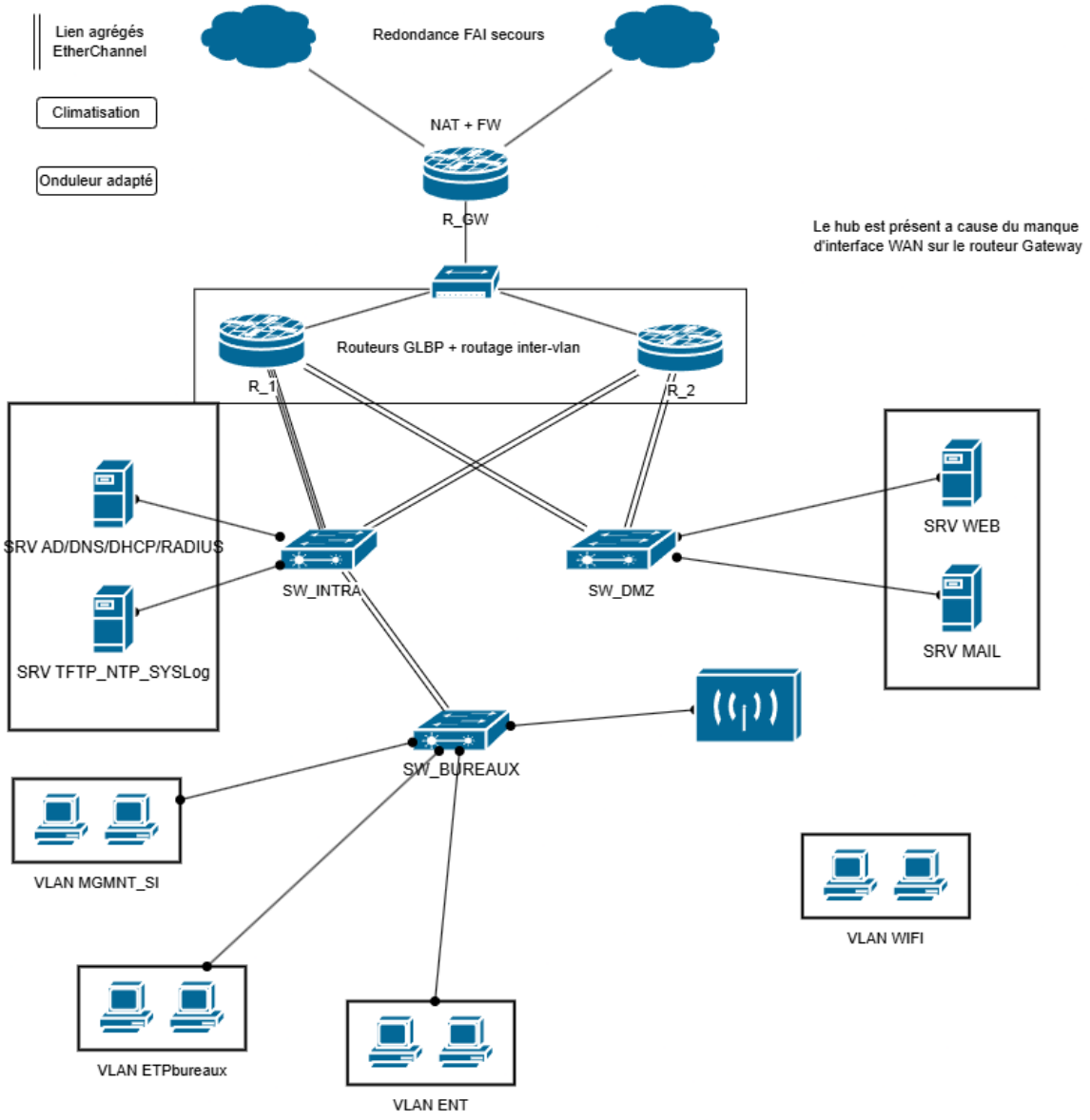
Voici un premier tableau répertoriant les problèmes physiques et leur solution.

Problèmes physique	Solutions
Aucune redondance des câbles	Spanning Tree
Le routeur est un élément critique s'il tombe en panne tout le réseau est interrompu	Ajout d'un ou deux routeurs avec solutions de redondance et de répartition de charges
Aucune redondance de liens	Agrégation Etherchannel
Fournisseurs d'accès à internet unique	Ajout d'une connexion WAN de secours
Tous les protocoles L3 sont gérés par un seul routeur	Ajout d'un routeur passerelle WAN
Aucune tolérance aux pannes du routeur	Mise en place redondance routeur HSRP
Risque de surchauffe des serveurs	Pose d'un climatiseur dans la salle des serveurs
Microcoupure de courant	Mise en place d'onduleur
La segmentation des sous réseaux est basique	Ajout de sous-réseaux : « serveurs » et « management système information »

Dans ce second tableau les problèmes logiciel/système ainsi que leur solution.

Problèmes logiciel/système	Solutions
En cas de crash ou d'une réinitialisation inopinée d'un équipement réseau la configuration peut être perdue	Backup des configurations sur un serveur TFTP
Aucune redondance du contrôleur de domaines	Déploiement d'un deuxième serveur Windows
Aucune trace des évènements	Mise en place d'un serveur de logs
Aucune sécurité au niveau des ports des switchs	Mise en place d'ACL MAC
Aucune règle de pare-feu	Mise en place d'un pare-feu
Aucune authentification sur l'administration des équipements	Mise en place d'un serveur RADIUS
Aucune répartition de charge	Ajout d'un protocole de répartition de charge

A la suite du recensement des points sensibles, un nouveau schéma a été fait en corrigeant les failles de l'architecture précédente :



Tâche 2 : Plan d'adressage

Nous découperons l'adressage des postes en fonctions de leur rôle, grâce à plusieurs sous réseaux :

- Employés TiersLieux86 : « **ETPbureaux** » ;
- Service de management du système informatique : « **MGMNT_SI** » ;
- Un sous réseau pour chaque entreprise accueillit : « **ENT** + nom entreprise » ;
    - Dans ce document nous représenterons l'ensemble des sous réseaux pour les entreprises par celui de l'entreprise Esporting donc : « **ENTesporting** ».
- Un sous réseau pour chaque salle de réunion selon le bâtiment A ou B : « **REUa** » et « **REUb** » ;
    - Nous utiliserons uniquement le réseau « **REUa** » par simplicité.
- Un sous réseau dissocié des autres, où seront positionnés les différents serveurs accessibles depuis le WAN, la DMZ : « **DMZ** » ;
- Un sous réseau pour le Wi-Fi à disposition des entreprises : « **WIFI ENT** »
    - NB : Le réseau « **ETPbureaux** » et « **MGMNT_SI** » bénéficieront aussi d'un réseau wifi mais l'adressage sera le même.

Réseau	Adresse	VID	Passerelle
ETPbureaux	192.168.2.0/24	2	192.168.2.254
MGMNT_SI	192.168.3.0/24	3	192.168.3. 254
SRV	10.2.0.0/24	10	10.2.0. 254
ENT • ENTesporting • REUa	172.17.0.0/16 • 172.17.11.0/24 • 172.17.21.0/24	X	172.17.X.254
		11	172.17.11. 254
		21	172.17.21. 254
WIFI	172.17.80.0/24	80	172.17.80. 254
DMZ	172.16.2.0/24	99	172.16.2. 254
WAN	192.36.253.20 (192.168.1.250)		192.36.253.254 (192.168.1.1)

NB : L'adresse IP publique attribuée sera une adresse faisant partie de mon réseau local, pour pouvoir mettre en place le **NAT** et accéder à internet.

Désormais on peut associer les adresses IP fixes aux serveurs, commutateurs, routeurs et au point d'accès wifi, et leur attribué un nom :

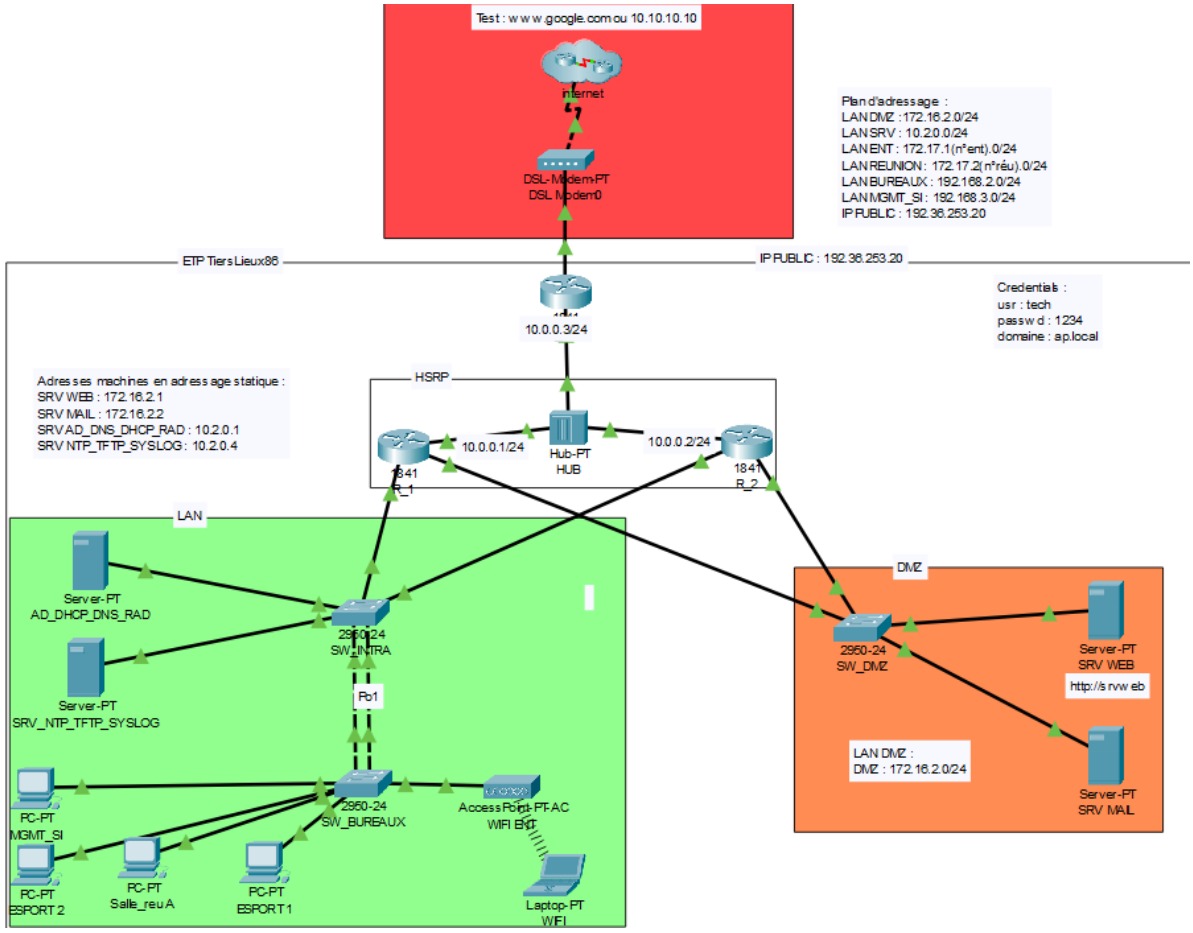
Rôle	NOM	IP de management
Routeur interne 1 (1803)	R_1	192.168.3.253
Routeur interne 2 (1801)	R_2	192.168.3.252
Routeur WAN (1841)	R_GW	10.0.0.3
Commutateur 1	SW_INTRA	192.168.3.202
Commutateur 2	SW_BUREAUX	192.168.3.204
Commutateur 3	SW_DMZ	192.168.3.203
Borne Wi-Fi	WAP200	192.168.3.200
Contrôleur de domaine : AD DS/DNS/DHCP/RADIUS	AD/DNS/DHCP	10.2.0.1
Serveur NTP/SYSLOG/TFTP	SRVLNX	10.2.0.4

Interconnexion R_1, R_2 et R_GW :

Routeur	IP
R_1	10.0.0.1/24
R_2	10.0.0.2/24
R_GW	10.0.0.3/24

Tâche 3 : Simulation

Une fois la maquette finie, on peut avoir un aperçu plus ou moins fiable de l'infrastructure réel, néanmoins on se rend compte que l'aspect visuel ressemble beaucoup au schéma précédent :



NB : Cette maquette réalisée sur Cisco Packet Tracer, est disponible dans mon portfolio.

En revanche elle est à prendre avec des pincettes car plusieurs protocoles ne sont pas supportés en simulation, de plus ceux qui sont supportés on quelques limitations.

Problèmes rencontrés

Pendant la réalisation de la maquette plusieurs problèmes sont survenus principalement lié aux limitations du logiciel, c'est pourquoi il se peut que certaines technologies ne soient pas en place sur la maquette.

Chapitre 2 : Préparation du matériel

Tâche 1 : Inventaire des besoins

Grâce à la maquette réalisée précédemment on peut désormais prévoir le **matériel** nécessaire.

(Bien entendue la vitesse des ports et des équipements est un critère très important mais ici l'infrastructure entière sera basée sur du 100Mb/s pour des raisons de coûts)

Grâce au cahier des charges et à la maquette, on sait qu'il nous faut :

- **Trois routeurs** administrables, supportant le routage, le **NAT**, des protocoles de **redondances**, les **ACL**, la norme **802.1q**…
- **Trois switchs** de niveau 2 **administrables**, supportant **LACP**, la **sécurisation** des ports, la norme **802.1q**… ;
- Un switch non administrable afin d'assurer **la connectivité des 3 routeurs** ;
- Un point d'accès wifi prenant en charge **plusieurs SSID** ;
- Un serveur qui gèrera **NTP, TFTP et Syslog** ;
- Un serveur contrôleur de domaine avec **DHCP, DNS et RADIUS** ;
- Quelques **clients** de test ;
- Des câbles Ethernet RJ45 croisés ;
- Des câbles Ethernet RJ45 droits.

Tâche 2 : Solutions retenues

Pour la sélection du matériel je me suis tourné vers la marque **Cisco**, premièrement car je possède quelques connaissances sur ces équipements, mais aussi car ce sont les plus répandus du fait de leurs innovations dans ce domaine mais aussi leur ancienneté dans celui-ci et de ce fait ce sont aussi les équipements les plus abordables sur le marché.

Réseau		
Nom	Modèle	Version
R_GW	Cisco 1841	IOS 15.0(1)M1
R_1	Cisco 1803	IOS 12.4(24)T1
R_2	Cisco 1801	IOS 12.4(24)T1
SW_INTRA	Cisco Catalyst 2950	IOS 12.1(22)EA13
SW_BUREAUX	Cisco Catalyst 2950	IOS 12.1(22)EA13
SW_DMZ	Cisco Catalyst 2950	IOS 12.1(22)EA13
WAP 200	Cisco WAP200	2.0.1.3-ETSI
Switch non administrable	TP-LINK	
Carte ethernet USB RJ45 X5	Adaptateur TP-LINK	
Carte WIFI	Atheros AR9271	

Cable ethernet RJ45 croisé X10	Cat 6a UTP	
Cable ethernet RJ45 droit X10	Cat 6a UTP	
Câble console X5	USB > RJ45	

Virtualisation		
Machine	Solution	Version
Hyperviseur	VMWare Workstation	17
Serveur AD/DHCP/DNS/RADIUS	VM Windows server	2022
Clients VLAN X4	VM Windows	11

Tâche 3 : Schéma câblage

Toutes les informations réunies, il est temps d'étudier la méthodologie d'interconnexion des équipements.

Pour simplifier la mise en place, une politique de gestion des ports est établie :

Pour les **commutateurs** :

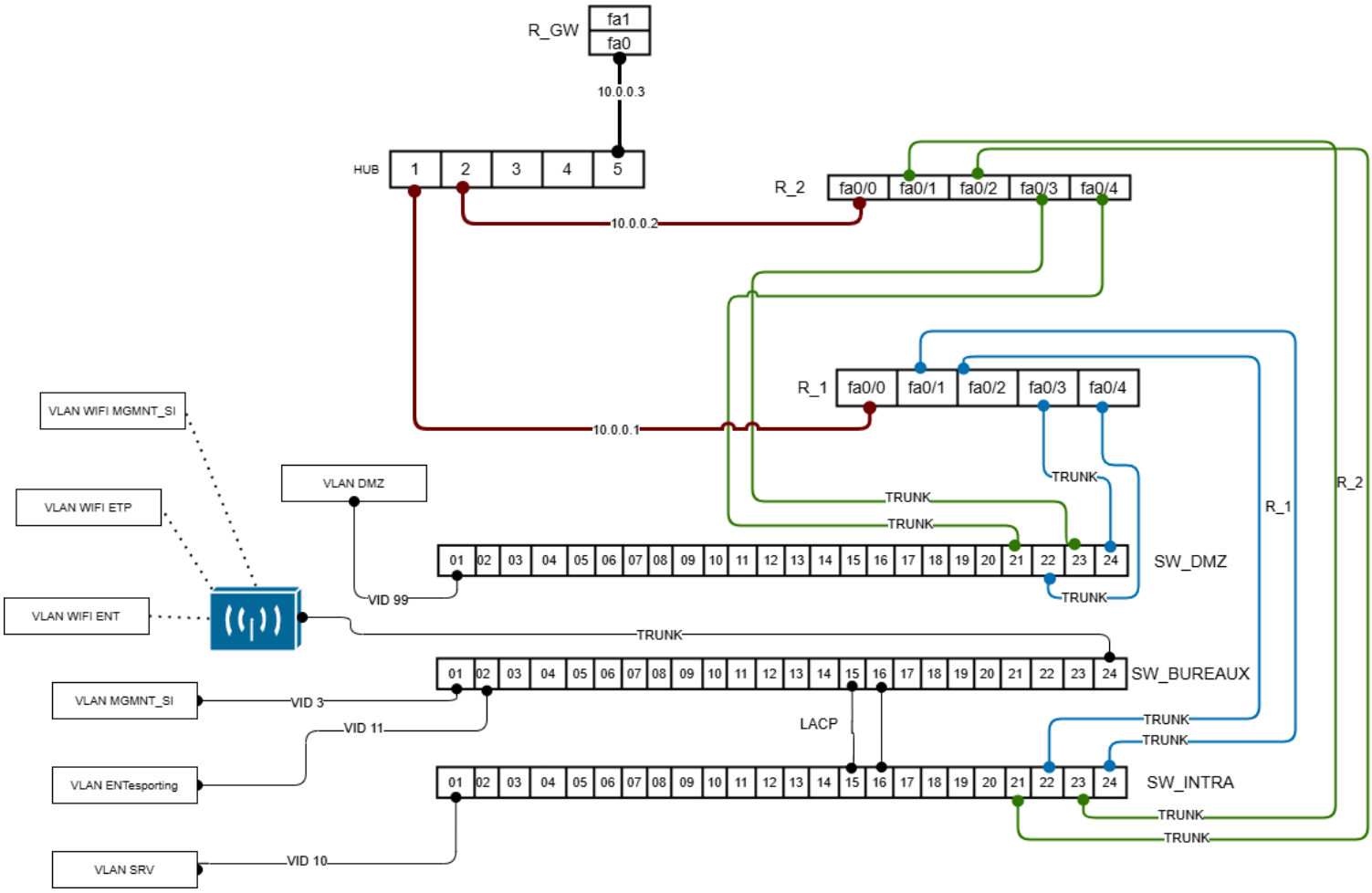
- Les interconnexions entre les équipements réseaux hétérogènes s'effectueront sur les ports les plus grands en partant de Fa0/24 ;
- Les interconnexions sur les machines homogènes utiliseront les ports les plus grand en partant de Fa 0/16 ;
- Les ports d'accès seront les plus petits en partant de Fa0/1 ;
- Les ports Gigabits ne seront pas utilisés.

Pour les **routeurs** :

NB : Sur les routeurs 1801 et 1803 les ports de Fa0/1 a Fa0/8 sont des ports de switching, seul les ports Fa0/0 sont des interfaces de niveau 3.

- Les ports Fa0/1 et Fa0/2 des deux routeurs sont affectés à SW_INTRA ;
- Les ports Fa0/3 et Fa0/4 seront eux associés à SW_DMZ ;
- Quant aux ports Fa 0/0 des routeurs R_1, R_2 et R_GW il serviront à l'interconnexions de ceux-ci ;
- Le port Fa0/1 de R_GW sera destiné à accueillir la connexion vers le WAN.

Voici un schéma récapitulant l'organisation des branchements



Problèmes rencontrés

Les câbles RJ45 croisés sont compliqué à trouver, le plus simple était de me procurer les matériels et matériaux afin de pouvoir les concevoir moi-même.

Les 3 routeurs ne disposent pas d'assez de ports de niveau 3 pour pouvoir tous être interconnectés, même si ce n'est pas une bonne pratique j'ai dû assurer l'interconnexion via un switch non administrable.

Mettre en place une infrastructure entière avec plusieurs client/serveurs chez soi n'est pas si simple, j'ai passé pas mal de temps à chercher une méthode, j'ai fini par opter pour des cartes réseaux USB – RJ45 en en attribuant une par sous réseau.

Chapitre 3 : Configuration basique du matériel

Tâche 1 : Déploiement du matériel

Sur ma machine hôte se trouvent **5 cartes réseaux filaires** et une **carte wifi**, 5 de ces cartes représentent les différents sous réseaux, elles sont associées aux machines virtuelles représentant **les postes clients et/ou serveurs**, sur VMWare toutes les cartes filaires sont **pontées** avec les VM (pour que je puisse administrer toutes les machines depuis mon système hyperviseur), cela me permet de disposer des **deux serveurs** via une seul carte réseau physique.

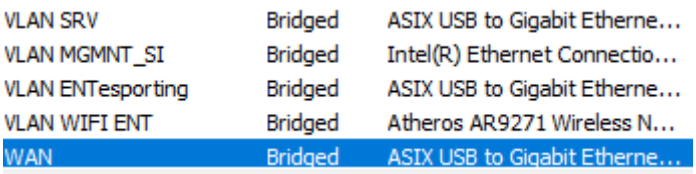
La carte réseau filaire restante est réserver pour la connexion au WAN :

Cartes réseaux		
Nom	Réseaux/VID	IP
WIFI ENT	WIFI ENT/80	172.17.80.199/24
VLAN ENT	ENTesporting/11	172.17.11.199/24
VLAN SRV	SRV/10	10.2.0.199/24
VLAN MGMNT_SI	MGMNT_SI/3	192.168.3.199/24
VLAN DMZ	DMZ/99	172.16.2.199/24
WAN		192.36.253.20 (192.168.1.250)

Machines virtuelles				
Nom	Rôle	IP	Carte réseau	Mode
MGMNT_SI	Client	192.168.3.10/DHCP	VLAN MGMNT_SI	Bridge
ENTesporting	Client	172.17.11.10/DHCP	VLAN ENT	Bridge
WIFI	Client	172.17.80.10/DHCP	WIFI ENT	Intégré
DMZ	Serveur	172.16.2.1	VLAN DMZ	Bridge
AD-DNS-DHCP	Serveur	10.2.0.1	VLAN SRV	Bridge
SRVLNX	Serveur	10.2.0.4	VLAN SRV	Bridge

Désormais on peut procéder à une installation conventionnelle des différentes machines virtuelles et de leurs OS, on notera que le serveur active directory est un clone de celui utilisé dans la première réalisation.

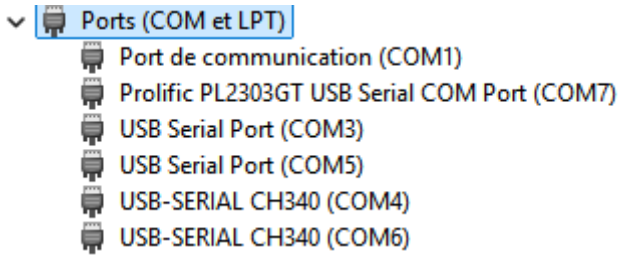
Ensuite, une fois les OS installés, j'ai créé les ponts/bridge de mes cartes réseaux afin de pouvoir les utiliser dans VMware :



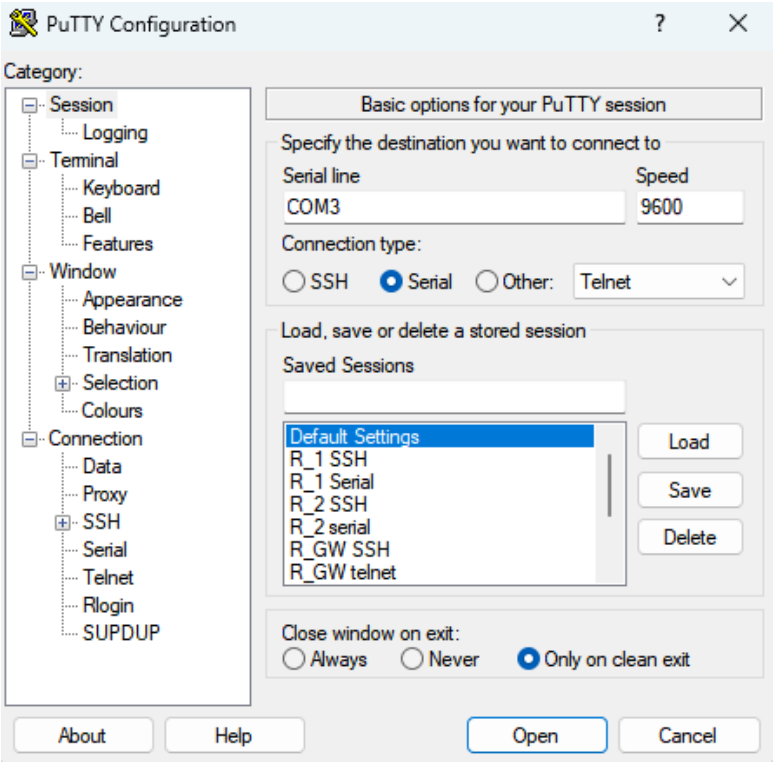
Puis j'ai associé ces ponts aux différentes machines clientes/serveurs.

Une fois la partie virtuelle prête à l'emploi, on commence l'installation des équipements, dans un premier temps uniquement l'alimentation électrique des appareils et les branchements de câbles consoles.

Il ne reste plus qu'à installer le logiciel **PuTTY** qui permets de se connecter aux équipements réseaux grâce aux câbles consoles pour ça il faut se rendre dans le gestionnaire de périphériques de votre hôte et vérifier quelle sont **les ports COM** actif :



On a plus qu'à renseigner ces ports dans PuTTY et lancer la connexion :



Tâche 2 : Configuration standard

Identification

Une fois le matériel installé, et la connexion console établie, la première étape est de changer le **nom d'hôte** de toutes les machines et leur attribuer une **adresse IP** qui servira à l'administration.

Equipement réseau		
Nom	Modèle	IP management (SSH)
R_GW	Routeur Cisco 1841	10.0.0.3
R_1	Routeur Cisco 1803	192.168.3.253
R_2	Routeur Cisco 1801	192.168.3.252
SW_INTRA	Switch Cisco Catalyst 2950	192.168.3.202
SW_BUREAUX	Switch Cisco Catalyst 2950	192.168.3.203
SW_DMZ	Switch Cisco Catalyst 2950	192.168.3.204
WAP200	AP Wi-Fi WAP200	192.168.3.200

On configure donc les noms d'hôte ainsi que leur adresse IP grâce à la commande : ***« ip host NOM ADRESSE_IP »,*** et ce sur chaque machine sauf la borne wifi bien entendu.

Bannière de connexion

Le client a demandé la mise en place d'un message d'accueil, qui apparaîtra à chaque connexion sur tous les équipements réseaux afin de prévenir l'utilisateur qu'il doit être habilité à utiliser les équipements sans quoi il doit immédiatement se déconnecter de l'appareil.

Voici le message que le client a transmis :

###
L'Acces a cet equipement est strictement restreint aux seules personnes

Autorisees. Cet equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes pas une personne autorisee !

Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an authorized user!
###

Afin de correspondre avec l'encodage des équipements Cisco tous les accents doivent être retirés.

On entre la commande ***« banner motd '' »*** dont le dernier caractère est un échappement, lorsque l'on a fini d'entrer son message il suffit d'appuyer sur '' pour y mettre fin :

```
SW_BUREAUX(config)#banner motd "
Enter TEXT message.  End with the character '"'.
###
$aux seules personnes autorisees. Cet equipement est la propriete de
$6 deconnectez-vous immediatement si vous n'etes pas une personne autorisee !
$------------------------------------------------------------------------
Unauthorized access prohibited
Authorized access only
$TiersLieux86 disconnect IMMEDIATELY if you are not an authorized user !
###
"
SW_BUREAUX(config)#exi
SW_BUREAUX#wr
Building configuration...
[OK]
SW_BUREAUX#
*Mar  1 01:12:15.627: %SYS-5-CONFIG_I: Configured from console by console
SW_BUREAUX#reload
Proceed with reload? [confirm]
```

VTP

Le **VLAN Trunking Protocol** a été développé par Cisco, dans le but d'optimiser la gestion de la base de données des VLAN des appareils réseaux. Ceux-ci peuvent être configurés selon 3 états :

- **Serveur** : l'ajout, la suppressions ou tous paramètres liés aux VLAN de niveau 2 se fera sur l'appareil ayant ce rôle ;
- **Client** : obtiendra la configuration VLAN du serveur ;
- **Transparent** : l'équipement ne prendra compte d'aucune configuration VLAN qui lui sera envoyé par VTP.

Pour liés ces appareils, lors de la configuration de **VTP** il faut créer un **domaine de diffusion** qui servira à savoir si un équipement doit recevoir ou envoyé des configurations VLAN, on notera qu'un seul appareil peut avoir le rôle de serveur par domaine.

VTP possède une fonctionnalité optionnelle appelé le « **pruning** » qui permets d'optimiser la bande passante, la configuration d'un VLAN se transmettra uniquement sur les commutateurs ayant des ports d'accès dans ceux-ci, par exemple si un switch a 2 endpoints dans les VLAN 1 et 3 il est inutile que ce switch récupère la configuration du VLAN 2.

Dans notre infrastructure notre routeur 1803 « **R1** » aura le rôle de **serveur**, **R_2**, **SW_BUREAUX**, **SW_DMZ** et **SW_INTRA** auront le rôle de **client**.

Ici le **domaine** VTP sera « **ETP_NW** », on va donc commencer avec la configuration du serveur :

```
R_1(config)#vtp domain ETP_NW
Changing VTP domain name from NULL to ETP_NW
```

On active la version la plus récente :

```
R_1(config)#vtp version 2
VTP mode already in V2.
```

Le VTP pruning :

```
R_1(config)#vtp pruning
Pruning switched on
```

Puis on définit un mot de passe :

```
R_1(config)#vtp password 1234
Setting device VLAN database password to 1234
R_1(config)#
```

On passe ensuite à la configuration des clients :

```
SW_INTRA(config)#
SW_INTRA(config)#vtp domain ETP_NW
Changing VTP domain name from 0* to ETP_NW
SW_INTRA(config)#VTP version 2
VTP mode already in V2.
SW_INTRA(config)#vtp pass
SW_INTRA(config)#vtp password 1234
Password already set to 1234
SW_INTRA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW_INTRA(config)#
```

On configure les VLAN de niveau 2 sur le serveur VTP :

```
R_1(config)#vlan 2
R_1(config-vlan)#name ETPbureaux
R_1(config-vlan)#vlan 3
R_1(config-vlan)#name MGMNT_SI
R_1(config-vlan)#vlan 10
R_1(config-vlan)#name SRV
R_1(config-vlan)#vlan 11
R_1(config-vlan)#name ENTesporting
R_1(config-vlan)#vlan 21
R_1(config-vlan)#name REUa
R_1(config-vlan)#vlan 80
R_1(config-vlan)#name WIFI_PUB
R_1(config-vlan)#vlan 99
R_1(config-vlan)#name DMZ
R_1(config-vlan)#
```

Tâche 3 : routage inter-vlan

Une fois les VLAN de niveau 2 crées, on va maintenant créer les **interfaces de niveau 3** afin d'assurer le **routage inter-VLAN**.

Il existe principalement deux méthodes :

- **Le RoAS** (Router As Stick) : Le fonctionnement est basé sur la configuration de sous-interface (sub-interface) du routeur, en leur associant une configuration IP qui servira de passerelle puis l'encapsulation 802.1q qui elle tagguera les trames des VLAN ;

- **Le SVI** (Switch Virtual Interface) : pour cette méthode il faut savoir qu'elle est plus adaptée sur un switch de niveau 3, ce routage consiste à créer les interfaces VLAN en leur associant une configuration IP sans encapsulation contrairement aux sous-interfaces, puis de configurer une ou plusieurs interfaces L2 du switch L3 ou du routeur en mode trunk puis en configurant l'encapsulation 802.1q directement sur le ou les ports cibles.

Ces deux méthodes sont à peu près équivalentes hors mi que le routage SVI ne condamnera pas une interface L3.

Dans mon cas j'utiliserais la seconde méthode (SVI) car les routeurs en ma possessions sont assez anciens et ils ne possèdent qu'une interface physique qui sera connecter au WAN.

En se référant au plan d'adressage on peut réénumérer les sous réseaux composant l'infrastructure :

Nom du réseau	Plage IP	Passerelle	VLAN ID
Administration ETP	192.168.2.0/24	192.168.2.254	2
Management SI	192.168.3./24	192.168.3.254	3
Serveur	10.2.0.0/24	10.2.0.254	10
Entreprise Esporting	172.168.11.0/24	172.17.11.254	11
Salle de réunion A	172.17.21.0/24	172.17.21.254	21
WIFI_PUB	172.17.80.0/24	172.17.80.254	80
DMZ	172.16.2.0/24	172.16.2.254	99

Rappel : Comme expliqué plus haut, chaque entreprise dispose du dernier octet de son adresse, par exemple pour la prochaine entreprise l'adressage sera : 172.17.12.0/24.

On se rend sur R_1, puis on crée l'interface logique correspondante à chaque VLAN en leurs attribuant une configuration IP :

```
R_1(config-if)#int vlan 2
R_1(config-if)#ip address 192.168.2.254 255.255.255.0
R_1(config-if)#int vlan 3
R_1(config-if)#ip address 192.168.2.254 255.255.255.0
*Jan  1 04:11:17.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3
R_1(config-if)#ip address 192.168.3.254 255.255.255.0
R_1(config-if)#int vlan 10
R_1(config-if)#ip address 192.254 255.255.255.0
*Jan  1 04:11:35.335: %LINK-3-UPDOWN: Interface Vlan10, chang
R_1(config-if)#ip address 10.2.0.254 255.255.255.0
R_1(config-if)#int vlan 11
R_1(config-if)#ip address 10.2..254 255.255.255.0
*Jan  1 04:11:53.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, cha
R_1(config-if)#ip address 172.17.11.254 255.255.255.0
R_1(config-if)#int vlan 21
R_1(config-if)#
*Jan  1 04:15:06.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan21, changed state to up
R_1(config-if)#ip address 172.17.21.254 255.255.255.0
R_1(config-if)#int vlan 80
R_1(config-if)#
*Jan  1 04:15:19.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan80, changed state to up
R_1(config-if)#ip address 172.17.80.254 255.255.255.0
R_1(config-if)#int vlan 99
R_1(config-if)#
*Jan  1 04:15:31.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
R_1(config-if)#ip address 172.16.2.254 255.255.255.0
R_1(config-if)#
```

Ensuite afin d'assurer le routage on configure le port du routeur relié au commutateur en mode trunk, ici le Fa 1 et on active l'encapsulation dot1q de la norme IEE 802.1q :

```
R_1(config)#int fa 1
R_1(config-if)#switchport trunk encapsulation dot1q
R_1(config-if)#swit
R_1(config-if)#switchport mode trunk
R_1(config-if)#
```

Tâche 4 : Routage statique/OSPF

A cette étape il faut configurer le routage entre les routeurs, pour cela on utilisera le protocole **OSPF** pour **Open Shortest Path First** afin de router de façon dynamique les réseaux vers le WAN, c'est un protocole ouvert crée par l'IETF.

L'avantage de ce protocole de routage par rapport à ses prédécesseurs est qu'il est bien plus rapide, les routes qui seront utiliser seront celle avec le plus petit coût, dans des infrastructures plus grandes qu'ici, les routeurs sont regroupés par zone « area ».

On se rend sur R_1 puis, en premier on attribue un processus OSPF ainsi qu'un ID au routeur :

- ID R_1 : 1.1.1.1 ;
- ID R_2 : 2.2.2.2 ;
- ID R_GW : 3.3.3.3.

```
R_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_1(config)#router ospf 100
R_1(config-router)#router-id 1.1.1.1
R_1(config-router)#
```

Ensuite on active la journalisation des évènements OSPF, puis la **redistribution des sous réseaux** connectés :

```
R_1(config-router)#log-adjacency-changes
R_1(config-router)#redi
R_1(config-router)#redistribute connec
R_1(config-router)#redistribute connected su
R_1(config-router)#redistribute connected subnets
R_1(config-router)#
```

Il ne reste plus qu'à indiquer **l'interface d'interconnexion** suivit d'un masque réseau inversé et de la zone de travail des routeurs :

```
R_1(config-router)#network 10.0.0.1 0.0.0.0 area 0
R_1(config-router)#
```

- R_2 : « 10.0.0.2 0.0.0.0 area 0 » ;
- R_GW : « 10.0.0.3 0.0.0.0 area 0 ;

On réalise le même procédé sur R_2.

Pour le routage de R_GW, on lui donne la **route par défaut** qui mène vers internet, qu'il va redistribuer à R_1 et R_2 à savoir : « 0.0.0.0 0.0.0.0 192.168.1.1» où 192.168.1.1 est l'adresse IP de la passerelle de mon réseau local.

```
S*    0.0.0.0/0 [1/0] via 192.168.1.1
```

Puis on configure OSPF avec les paramètres définit plus haut, en incluant la redistribution de route statique, son réseau 10.0.0.3 0.0.0.0 area 0, et on active l'option « **default-information originate** » qui permets de détecter la route par défaut a redistribué, c'est une surcouche a la redistribution statique.

```
router ospf 100
 router-id 3.3.3.3
 redistribute static
 network 10.0.0.3 0.0.0.0 area 0
 default-information originate
```

Tâche 5 : Traduction d'adresse PAT

Afin d'assurer la connectivité du réseau interne au **WAN** nous mettrons en place une **traduction d'adresse dynamique basé sur les ports**, de sorte qu'à chaque périphérique qui contacte l'extérieur du réseau, lui soit associé **l'adresse publique avec un numéro de port** qui permets de reconnaitre la machine dans le réseau.

Pour cela, il faut définir les interfaces d'entrée et de sortie du réseau sur le routeur passerelle R_GW :

```
R_GW(config)#int fa 0/0
R_GW(config-if)#ip nat inside
R_GW(config-if)#int fa0/1
R_GW(config-if)#ip nat outside
```

Ensuite il faut créer une **Access Control List** permettant de définir qui a le droit de sortir sur le réseau, pour l'instant **l'ACL** sera basique et permettra à toutes les machines de sortir du réseau, le but pour le moment est juste d'assurer la connexion au WAN :

```
R_GW(config)#ip access-list standard 1
R_GW(config-std-nacl)#permit any
R_GW(config-std-nacl)#
```

Puis on applique l'ACL a la traduction d'adresse ainsi que le mode de traduction voulu ici overload qui correspond au **PAT** (Port Addresse Translation) :

```
ip nat inside source list 1 interface FastEthernet0/1 overload
```

Le NAT est désormais en place.

Tâche 6 : DHCP

Pour que les clients connectés au réseau puissent bénéficier d'une **configuration IP automatique**, un serveur **DHCP** a été déployé ainsi que les **agents relais sur le router R_1**.

J'ai donc dû dans un premier temps configurer les étendues DHCP sur le contrôleur de domaine.

Étendue [172.17.80.0] WIFI ENT	** Actif **
Étendue [172.17.21.0] REUa	** Actif **
Étendue [172.17.11.0] ENTesporting	** Actif **
Étendue [192.168.2.0] ETPbureaux	** Actif **
Étendue [192.168.3.0] MGMNT_SI	** Actif **

Chaque réseau bénéficie d'une plage **de X.X.X.10 à X.X.X.100** afin de laisser les adresses de début et de fin libres, en cas de besoin ces étendues pourront être modifiées.

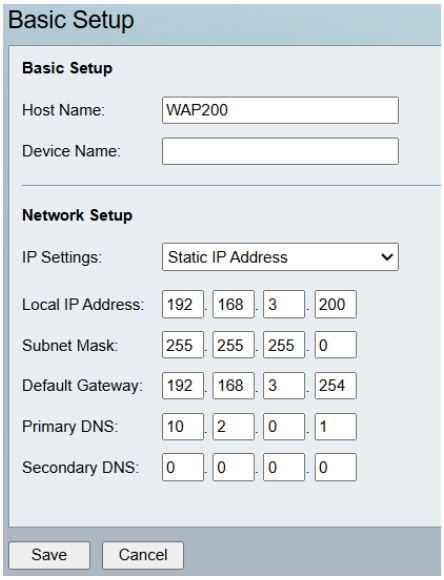
Pour la configuration de l'agent relais, il suffit de configurer **les interfaces logiques de R_1** pour leur ajouter le relais DHCP grâce à la commande suivante : « ***ip helper-address 10.2.0.1*** ».

```
R_1>en
Password:
R_1#conf t
Enter configuration commands, one per line.
R_1(config)#int vlan 2
R_1(config-if)#ip he
R_1(config-if)#ip hell
R_1(config-if)#ip help
R_1(config-if)#ip helper-address 10.2.0.1
R_1(config-if)#int vlan 3
R_1(config-if)#ip helper-address 10.2.0.1
R_1(config-if)#int vlan 11
R_1(config-if)#ip helper-address 10.2.0.1
R_1(config-if)#int vlan 21
R_1(config-if)#ip helper-address 10.2.0.1
R_1(config-if)#int vlan 80
R_1(config-if)#ip helper-address 10.2.0.1
```

Tâche 7 : WIFI

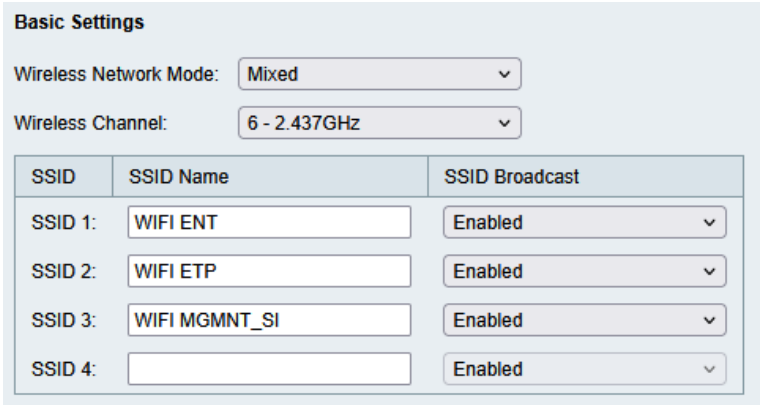
En premier lieu on se connecte directement au port de la borne d'accès depuis un poste, avec une interface configurer en 192.168.1.0/24 afin de pouvoir se connecter à la page web d'administration par défaut qui est en 192.168.1.245.

Ensuite on change le nom d'hôte du point d'accès par **WAP200**, puis l'adresse IP que l'on passe en 192.168.3.200/24 et la passerelle réseau qui est 192.168.3.254 et on sauvegarde.



On change la configuration IP de l'interface connecté à la borne pour correspondre avec son adresse et on retourne sur la page d'administration.

Désormais on peut créer les **SSID** ici « WIFI ENT » et « WIFI ETP» **l'un pour les entreprises juniors** et l'autre pour **les employés de TiersLieux86**. Mais il faut aussi créer un SSID pour **l'administration du système informatique** « WIFI MGMNT_SI »



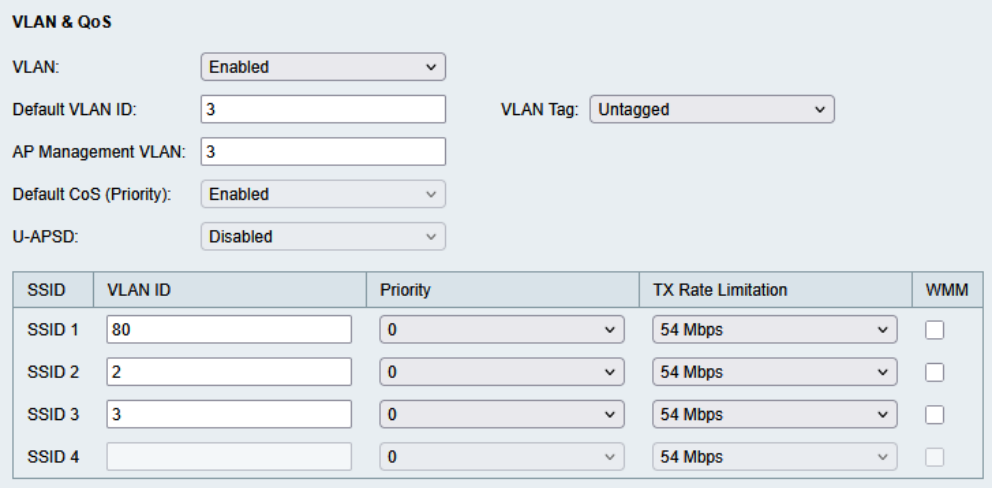
Ensuite il faut configurer la sécurité de ces SSID : on active l'isolation entre SSID, l'authentification **WPA2 personnal** et on entre **une clé de sécurité**. Plus tard les **SSID WIFI ETP et MGMNT_SI** s'authentifieront grâce à un **serveur radius**.

Dans les options de VLAN, il faut mettre le tag de VLAN sur **untagged** afin que tout le flux wifi puisse passer sur le même port car la borne ne possède qu'un port Ethernet. On règle le VLAN de management sur le VID 3.

NB : le VLAN natif est 1 et non pas 3 !

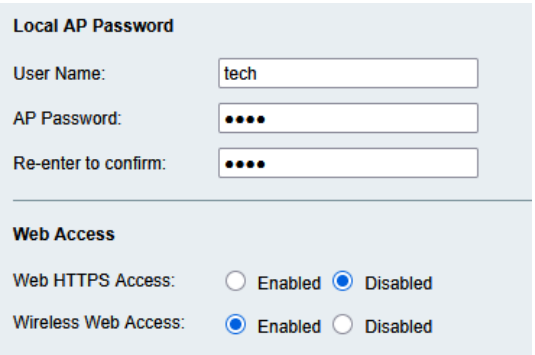
Puis on attribue à chaque SSID un **VID** (VLAN Identification) :

- WIFI ENT : VID 80 ;
- WIFI ETP : VID 2;
- WIFI MGMNT_SI : VID 3 .



L'administration de la borne WIFI se fera par l'adresse IP de celle-ci, plus tard les équipes SI pourront mettre en place une résolution de nom DNS.

Pour pouvoir administrer la borne il **faut activer l'accès web**, par la même occasion on change **les logins par défaut**. L'activation **http** est obligatoire car la borne gère plusieurs SSID sous différents VLAN et ne possède qu'un seul port, une administration directe n'est donc pas possible.

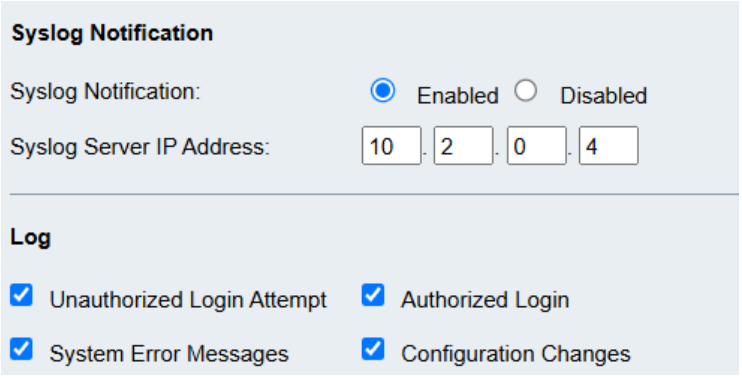


La borne étant assez ancienne, les **mises à jour du firmware ne sont plus disponibles**. Dans le cas contraire il aurait fallu mettre à jour le micrologiciel.

A cause de la vétusté de celle-ci les protocoles **TLS/SSL** utilisés ne sont plus prit en charge par nos navigateurs. Lorsque j'active l'accès **HTTPS** plus **aucune connexion à l'interface** d'administration n'est possible et ce même en changeant les paramètres des navigateurs.

Nous utiliserons donc un **accès http malgré la vulnérabilité de celui-ci**. Pour augmenter la sécurité du point d'accès**, des ACL seront créé** pour éviter les connexions depuis les réseaux indésirables.

Dernier réglage, il faut définir le **serveur de logs**, ici 10.2.0.4 ainsi que les types de logs à transmettre.



Il ne reste plus qu'à brancher notre AP au SW_BUREAUX sur le **port fa 0/24 configuré en Trunk**

Tâche 8 : Rapport de test

Bannière

```
###
L'acces a cet equipement est strictement restreint aux seules personnes autorisees. Cet equipement est
 la propriete de
TiersLieux86 deconnectez-vous immediatement si vous n'etes pas une personne autorisee !
------------------------------------------------------------------------------
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 disconnect IMMEDIATELY if you are not an authorized user !
###

R_2>en
Password:
R_2#
```

VTP

Configuration

```
R_2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 38
Maximum VLANs supported locally : 18
Number of existing VLANs        : 12
VTP Operating Mode              : Client
VTP Domain Name                 : ETP_NW
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE1 0x89 0xEB 0xE3 0xD8 0x35 0x8F 0x8B
Configuration last modified by 0.0.0.0 at 1-1-00 03:07:54
```

Base de données VLAN

```
R_2#sh vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5, Fa6, Fa7, Fa8
2    ETPbureaux                       active
3    MGMNT_SI                         active
10   SRV                              active
11   ENTesporting                     active
21   REUa                             active
80   WIFI_PUB                         active
99   DMZ                              active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Connectivité inter-vlan (tester avec 10.2.0.4)

```
tech@SRVLNX:~$ ping 10.2.0.254
PING 10.2.0.254 (10.2.0.254) 56(84) bytes of data.
64 bytes from 10.2.0.254: icmp_seq=1 ttl=255 time=1.61 ms
```

```
tech@SRVLNX:~$ ping 192.168.3.254
PING 192.168.3.254 (192.168.3.254) 56(84) bytes of data.
64 bytes from 192.168.3.254: icmp_seq=1 ttl=255 time=0.863 ms
```

```
tech@SRVLNX:~$ ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.
64 bytes from 192.168.2.254: icmp_seq=1 ttl=255 time=0.728 ms
```

```
tech@SRVLNX:~$ ping 172.17.11.254
PING 172.17.11.254 (172.17.11.254) 56(84) bytes of data.
64 bytes from 172.17.11.254: icmp_seq=1 ttl=255 time=2.63 ms
```

```
tech@SRVLNX:~$ ping 172.17.21.254
PING 172.17.21.254 (172.17.21.254) 56(84) bytes of data.
64 bytes from 172.17.21.254: icmp_seq=1 ttl=255 time=2.62 ms
```

```
tech@SRVLNX:~$ ping 172.17.80.254
PING 172.17.80.254 (172.17.80.254) 56(84) bytes of data.
64 bytes from 172.17.80.254: icmp_seq=1 ttl=255 time=2.58 ms
```

```
tech@SRVLNX:~$ ping 172.16.2.254
PING 172.16.2.254 (172.16.2.254) 56(84) bytes of data.
64 bytes from 172.16.2.254: icmp_seq=1 ttl=255 time=2.78 ms
```

Connectivité WAN

```
tech@SRVLNX:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=8.05 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=9.10 ms
```

NAT/PAT

On constate que les adresses internes sont bien reconnues grâce aux ports qui y sont associés.

```
R_GW#sh ip nat translations
Pro Inside global         Inside local          Outside local         Outside global
icmp 192.168.1.250:11550  10.2.0.4:11550        1.1.1.1:11550         1.1.1.1:11550
icmp 192.168.1.250:11641  10.2.0.4:11641        1.1.1.1:11641         1.1.1.1:11641
```

WIFI

Attribution d'adresse IP :	Automatique (DHCP)	Modifier
Attribution du serveur DNS :	Automatique (DHCP)	Modifier
SSID :	WIFI ENT	Copier
Protocole :	Wi-Fi 4 (802.11n)	
Type de sécurité :	WPA2 - Personnel	
Fabricant :	Atheros Communications Inc.	
Description :	[CommView] Atheros AR9271 Wireless Network Adapter	
Version du pilote :	2.0.0.73	
Bande passante réseau :	2,4 GHz	
Canal réseau :	6	
Vitesse de connexion (Réception/ Transmission) :	54/54 (Mbps)	
Adresse IPv6 locale du lien :	fe80::7e47:fae3:3a09:291d%18	
Adresse IPv4 :	172.17.80.10	
Serveurs DNS IPv4 :	10.2.0.1 (non chiffré)	
Adresse physique (MAC) :	00-C0-CA-98-11-05	

DHCP

Propriétés de Ethernet0

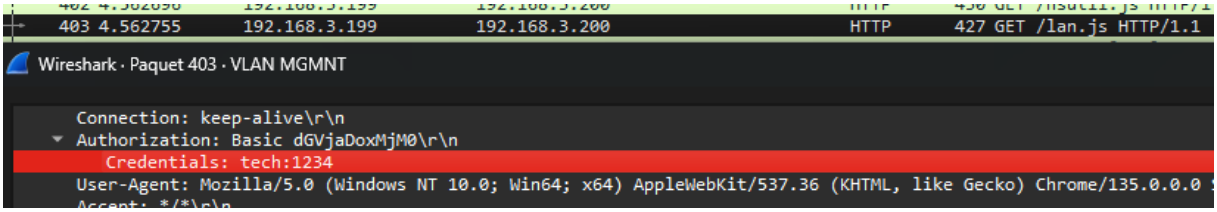
Attribution d'adresse IP :	Automatique (DHCP)
Attribution du serveur DNS :	Automatique (DHCP)
Vitesse de connexion (Réception/ Transmission) :	1000/1000 (Mbps)
Adresse IPv6 locale du lien :	fe80::914f:798b:8c14:d5a%4
Adresse IPv4 :	192.168.3.10
Serveurs DNS IPv4 :	10.2.0.1 (non chiffré)
Suffixe DNS principal :	ap.local
Fabricant :	Intel Corporation
Description :	Intel(R) 82574L Gigabit Network Connection
Version du pilote :	12.19.1.32
Adresse physique (MAC) :	00-0C-29-6B-53-51

Problèmes rencontrés

Les routeurs R_1 (modèle 1803) et R_2 (modèle 1801) **ne supportent que 8 VLAN** de niveau 3, il faudra faire évoluer ces équipements au plus vite.

Le point d'accès dispose de protocole de chiffrement HTTPS trop vieux et vulnérable pour être utilisé avec nos navigateurs (erreur de chiffrement, je n'ai trouvé aucune solution à ma portée), j'utilise donc l'administration web http même si grâce à un **sniffeur de réseau** on récupérer les identifiants.

Capture de trame avec **Wireshark** :



On peut très simplement voir les paquets qui transitent entre les postes d'administration et le point d'accès **ici les crédentials sont en clair** : « tech :1234 ».

Afin d'obtenir une connexion au WAN depuis le réseau du projet en passant par le mien, j'ai dû **ponter la carte réseau de mon PC hôte** connectée au routeur de mon FAI, à la carte réseau **WAN associée à R_GW**. Grâce à l'utilitaire Windows 11 « **netsh** ».

NB : pour réaliser un pontage il faut d'abord préciser l'ID de la carte de sortie puis l'ID de l'entrée :

```
PS C:\WINDOWS\system32> netsh bridge create 19 18
```

Où 19 est l'ID de la carte connectée à ma box et 18 à R_GW.

Chapitre 4 : Amélioration de l'administration des équipements

Tâche 1 : Trivial File Transfer Protocol

Afin de pouvoir **sauvegarder les configurations des équipements réseau**, il faut mettre en place un serveur **TFTP**, celui-ci se fera sous une machine virtuelle **Debian 12**.

J'installe les paquets nécessaires au bon fonctionnement du serveur TFTP : **tftpd-hpa**, ensuite je **configure le fichier du serveur tftp** afin de ranger tous les fichiers liés aux équipement Cisco dans un dossier bien défini :

```
  GNU nano 7.2
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp/cisco"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure --create -v"
```

Puis je **modifie les autorisations** sur ce dossier afin que mes appareils puissent y accéder.

Et pour finir je lance mon serveur TFTP :

```
tech@SRVLNX:/srv/tftp$ sudo systemctl enable tftpd-hpa
tftpd-hpa.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable tftpd-hpa
```

NB : La section suivante a été faite après la mise en place de SSH sur les divers équipements.

Je me suis rendu compte que récupérer les fichiers de configuration des équipements était assez chronophage, j'ai donc écrit **un script BATCH** pour récupérer ces fichiers au travers du serveur TFTP.

Pour ça il a fallu que j'active la fonction de serveur TFTP des routeurs, en précisant quel fichier peut être récupéré, il est possible d'y ajouter une ACL, nous y reviendrons dans un moment.

```
R_1(config)#tftp-server system:running-config
R_1(config)#
```

Grâce à « **plink** » qui est la commande version **console de PuTTY** j'initialise une **session SSH** vers le serveur TFTP (le mot de passe est en dur dans le script, cela pour faire l'objet d'un projet d'évolution) puis depuis cette session, j'interroge les routeurs en leur demandant leur fichier de configuration courante :

"

plink SRVLNX_SSH -pw 1234 -batch
"tftp 192.168.3.253 -c get running-config /srv/tftp/cisco/r_1-confg.txt;
tftp 192.168.3.252 -c get running-config /srv/tftp/cisco/r_2-confg.txt;
tftp 192.168.3.201 -c get running-config /srv/tftp/cisco/r_gw-confg.txt"

"

Puis toujours sur le même script a la suite de ces tâches la session est déconnectée, il ne me reste plus qu'à récupérer depuis ma machine hôte les fichiers du serveur linux grâce à winscp.com (version console de winscp) :

"

winscp.com sftp://10.2.0.4/ /username=tech /password=1234
/command "get /srv/tftp/cisco/*
C:\Users\Schrapnel57\Downloads\TFTP_CISCO\"
exit

"

On pourrait améliorer ce script pour qu'il s'exécute automatiquement pour sauvegarder les configurations.

Pour l'opération en sens inverse, il faut effectuer la manipulation depuis l'équipement concerné, néanmoins on peut quand même envoyer les configurations depuis notre hôte vers le serveur linux grâce à un script :

"

winscp.com sftp://10.2.0.4/ /username=tech /password=1234
/command "put C:\Users\Schrapnel57\Downloads\TFTP_CISCO\r_gw-confg.txt
/srv/tftp/cisco/r_gw-confg.txt" "exit"

"

Une deuxième méthode de sauvegarde améliorée consiste à démarrer les équipements depuis un fichier de configuration situé sur le serveur TFTP, dans le cas où le serveur ne répond pas, les équipements démarre sur la configuration locale en journalisant les évènements.

Je ne mettrais pas en place cette solutions par manque de temps, j'utiliserais uniquement la première méthode.

Tâche 2 : Secure SHell

Malgré le fait que je dispose de 5 câbles consoles, il est plus simple d'administrer ces équipements via **SSH**.

NB : Il faut vérifier la présence du terme « K2 » dans la version IOS, les switchs Cisco catalyst 2950 ne possèdent pas automatiquement cette version, il a fallu que je trouve ces versions de manière disons, parallèles car ces fichiers ne sont plus officiellement disponibles.

Avant tout pour que la connexion SSH fonctionne il faut avoir configurer un mot de passe pour le mode « enable » : ***« enable password MOTDEPASSE ».***

Tout d'abord on indique le domaine ici **ap.local**, ensuite on crée un nouveau modèle d'authentification, on renseigne les credentials login/password, puis on génère une **clé cryptographique RSA de 1024 Bit** afin de la rendre plus robuste.

```
SW_INTRA(config)#aaa new-model
SW_INTRA(config)#username tech password 1234
SW_INTRA(config)#ip domain-name ap.local
SW_INTRA(config)#crypto key generate rsa
The name for the keys will be: SW_INTRA.ap.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
Generating RSA keys ...
[OK]

00:43:18: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW_INTRA(config)#
```

Une fois la clé générée on passe à la configuration SSH, en indiquant la **version** à utiliser, le **nombre de tentative d'authentification**, le **temps d'inactivité** avant déconnexion et on **désactive telnet** :

```
SW_INTRA(config)#ip ssh version 2
SW_INTRA(config)#ip ssh au
SW_INTRA(config)#ip ssh authentication-retries 5
SW_INTRA(config)#ip ssh ti
SW_INTRA(config)#ip ssh time-out 60
SW_INTRA(config)#line vty 0 4
SW_INTRA(config-line)#input transport ssh
                      ^
% Invalid input detected at '^' marker.

SW_INTRA(config-line)#transport input ssh
SW_INTRA(config-line)#
```

Puis on vérifie la configuration :

```
SW_BUREAUX#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 5
SW_BUREAUX#
```

On applique cette configuration sur tous les équipements.

Mention spéciale pour R_GW : ce routeur faisant office de passerelle vers le WAN, aucune route menant à son interface 10.0.0.3 n'est configurées sur l'hyperviseur hôte, il faut donc en créer une temporaire vers l'adresse LAN de R_GW, c'est-à-dire 10.0.0.3 :

```
PS C:\WINDOWS\system32> route add 10.0.0.3 192.168.3.254
 OK!
PS C:\WINDOWS\system32> ping 10.0.0.3

Envoi d'une requête 'Ping'  10.0.0.3 avec 32 octets de données :
Réponse de 10.0.0.3 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.0.3 : octets=32 temps=1 ms TTL=254
Réponse de 10.0.0.3 : octets=32 temps=1 ms TTL=254
```

Automatisation connexion SSH

Dans un premiers temps, j'ai utilisé le logiciel PuTTY, pour chaque matériel j'avais créé une **session personnalisée**, mais au fil du temps je trouvais que ce client SSH n'était **pas très ergonomique,** j'ai donc écrit un petit **script BATCH** qui me permets de me connecter à tous les équipements en un seul click, ce script ouvre un terminal découpé en plusieurs partie pour afficher **plusieurs terminal SSH sur la même fenêtre**, j'ai aussi pu déployer les sessions sur différents onglets afin de catégoriser par groupe de machine : routeurs, commutateurs et serveur.

Ce script BATCH est lié à des **sessions personnalisées** de **powershell** qui exécute une commande personnalisée au lancement.

Script BATCH (qui se résume à une seule ligne) :

«
wt -p "SSH R_GW" ; split-pane -p "SSH R_1" ; split-pane -p "SSH R_2" ; new-tab -p "SSH SW_INTRA" ; split-pane -p "SSH SW_DMZ" ; split-pane -p "SSH SW_BUREAUX" ; new-tab -p "SSH NTP/LOG/TFTP"
»

Exemple de session personnalisée powershell :

```
"commandline": "ssh tech@10.2.0.4",
"guid": "{fd9ae2ac-f921-4abd-90e3-27bf4d6f43d2}",
"hidden": true,
"name": "SSH NTP/LOG/TFTP",
"tabTitle": "NTP/LOG/TFTP 10.2.0.4"
```

Tâche 4 : Network Time Protocol

Nous utiliserons notre **serveur linux** pour mettre en place un **serveur NTP** sur lequel toutes les machines du réseau seront synchroniser, même les postes utilisateurs.

Pour cela j'utiliserais le paquet **chrony**, puis je modifie le fichier de configuration en y ajoutant plusieurs pools de serveur NTP de stratum 2 :

```
server 0.fr.pool.ntp.org iburst
server 1.fr.pool.ntp.org iburst
server 2.fr.pool.ntp.org iburst
server 3.fr.pool.ntp.org iburst
```

J'ajoute les plages IP autorisées à se synchroniser :

```
allow 10.2.0.0/24
allow 192.168.3.0/24
allow 192.168.2.0/24
allow 10.0.0.3/32
allow 172.17.0.0/16
```

Dans le cas d'une panne d'accès au WAN, j'indique au serveur NTP de se servir de lui-même comme source de temps en incluant les lignes suivantes dans le fichier de configuration :

```
server 127.127.1.1
```

```
local stratum 4
```

Ensuite je peux démarrer le service chrony :

```
tech@SRVLNX:~$ sudo systemctl start chronyd
tech@SRVLNX:~$
```

On vérifie les sources de temps :

```
tech@SRVLNX:~$ chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- ns1.univ-montp3.fr            2   6    17    57  -3014us[-3014us] +/-   64ms
^+ 27.ip-51-68-44.eu             3   6    17    58  +1028us[+2061us] +/-   19ms
^- silas.dioptre.fr              2   6    17    58  -1125us[-1125us] +/-   29ms
^* ntp.univ-angers.fr            2   6    17    58    -25us[+1008us] +/-   43ms
```

On peut désormais passer à la **configuration des équipements réseaux**, celle-ci s'effectuera de la même façon sur tous les commutateurs et routeurs.

Pour cela il faut définir la **timezone** a utilisé par les équipements, en France l'horodatage est CET +1 en hiver et CET +2 en été, heureusement pour nous les appareils **gèrent le passage aux heures d'hivers/d'été** :

```
R_1(config)#clock timezone CET 1
R_1(config)#clock summer-time CET recurring last sunday march 03:00 last sunday october 02:00 60
```

Ensuite on peut paramétrer la **synchronisation NTP** en indiquant la source sur laquelle prendre l'information et l'adresse du serveur NTP :

```
R_1(config)#ntp server 10.2.0.4
R_1(config)#ntp source vlan 3
```

Voilà, il ne reste plus qu'a appliquer ce procédé sur chaque machine.

Dernier paramètre, on configure la **journalisation NTP** :

```
R_1(config)#ntp logging
R_1(config)#
```

Pour le contrôleur de domaine nous configurerons sa **synchronisation NTP** pour qu'elle se fasse **depuis le serveur Debian**, ainsi tous les **postes du domaine récupèrerons les informations NTP du serveur Debian** à travers le contrôleur de domaine :

```
PS C:\Users\Administrateur> w32tm /config /manualpeerlist:"10.2.0.4" /syncfromflags:manual
La commande s'est terminée correctement.
PS C:\Users\Administrateur> Restart-Service w32time
```

Tâche 5 : Syslog, Rsyslog/LogAnalyzer

Le serveur Debian a aussi pour rôle la **centralisation des logs**, pour que ces logs puissent transiter, j'utilise un serveur « **rsyslog** », puis pour avoir un interface graphique le serveur web « **loganalyzer** ».

En premier lieu on configure rsyslog pour qu'il puisse **accueillir les journaux des équipements**, pour cela j'installe le paquet rsyslog, en suite je modifie le fichier de configuration :

```
tech@SRVLNX:/var/log$ sudo nano /etc/rsyslog.conf
```

De sorte à permettre les paquets **UDP d'entrer sur le port 514** :

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

D'autoriser les appareils dans la plage **192.168.3.0/24 et 10.0.0.3 a envoyé des logs** :

```
$AllowedSender UDP, 127.0.0.1, 192.168.3.0/24, 10.0.0.3/32
```

Je dis à rsyslog de créer un dossier de **journalisation pour chaque hôte** :

```
#template
$template Incoming-logs, "/var/log/%HOSTNAME%/logging.log"
```

Puis, on lui indique de trier les logs en fonction de ce modèle :

```
*.*  ?Incoming-logs
```

Une fois le serveur prêt, il faut **configurer les clients**. Pour ça il suffit d'indiquer le **niveau des logs** que l'on veut faire remonter, le **serveur Syslog**, **l'interface source** chargé d'envoyé les logs au serveur et on peut **activer la journalisation** :

```
R_1(config)#logging trap 7
R_1(config)#logging 10.2.0.4
R_1(config)#logging source vlan 3
R_1(config)#logging on
R_1(config)#
```

NB : pour l'interface source il faut que l'adressage de celui-ci soit autorisé dans le fichier de configuration de rsyslog sinon l'équipement ne sera pas autorisé à envoyer les logs.

Désormais il ne nous reste plus qu'a envoyé ce flux de journaux dans une **base de données** reliée au serveur web, pour ça il faut installer une **pile LAMP** sur notre serveur, attention à bien installer **« php-mysqli »** sinon loganalyzer ne fonctionnera pas.

On **sécurise l'installation MySQL**, puis on **installe le module MySQL** de rsyslog :

```
tech@SRVLNX:/$ sudo apt-get install rsyslog-mysql -y
```

Cet utilitaire fait apparaitre une fenêtre afin de configurer **automatiquement la base données rsyslog**.

Une fois la base de données crée, on **télécharge loganalyzer**, le **décompresse**, on **crée un répertoire** dans la racine du serveur web on **copie les fichiers** dans celui-ci et enfin on **accorde la propriété** de ce dossier à l'utilisateur apache : www-data.

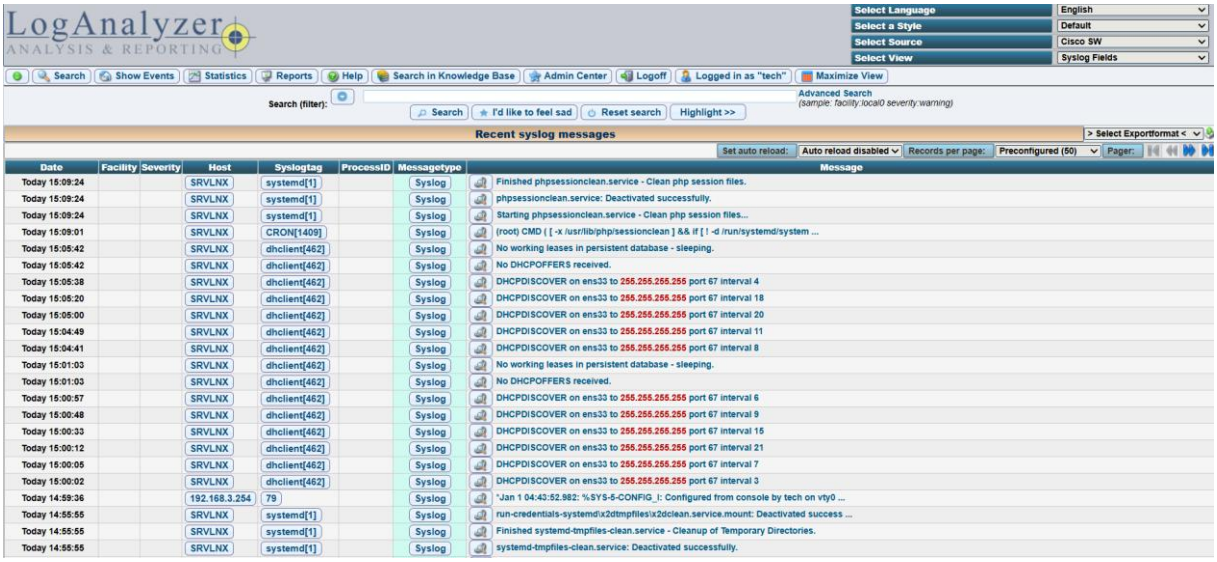
Avant de lancer notre serveur et de commencer à l'utiliser il faut effectuer une petite **modification dans un script PHP**, car sinon à partir d'une certaine étape d'installation de loganalyzer une erreur peut survenir, car ce script PHP fait appel à une **fonction désuète** dans php8, il **faut donc la commenter, il suffit de modifier ce fichier** :

```
root@SRVLNX:/# nano /var/www/html/loganalyzer/include/functions_common.php
```

Et de commenter la ligne ***« RemoveMagicQuotes() ; »***

```
// --- Check and Remove Magic Quotes!
//RemoveMagicQuotes();
```

Une fois fait, je me connecte au serveur web via l'adresse IP de ma machine puis procède a **l'initialisation du serveur web**.



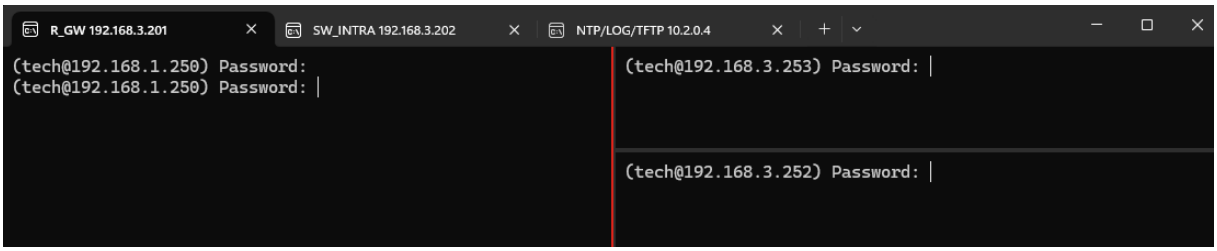
Tâche 6 : Rapport de test

TFTP

```
SW_DMZ#copy running-config tftp:
Address or name of remote host []? 10.2.0.4
Destination filename [sw_dmz-confg]?
!!
2537 bytes copied in 2.964 secs (856 bytes/sec)
SW_DMZ#
```

```
tech@SRVLNX:/srv/tftp/cisco$ ls
r_1-confg.txt  r_2-confg.txt  r_gw-confg.txt  sw_dmz-confg
```

SSH



NTP

```
R_GW#sh ntp status
Clock is synchronized, stratum 5, reference is 10.2.0.4
nominal freq is 250.0000 Hz, actual freq is 250.0160 Hz, precision is 2**24
reference time is EBBF2E60.1137B296 (13:43:28.067 CET Fri May 2 2025)
clock offset is -19.8424 msec, root delay is 32.46 msec
root dispersion is 25.53 msec, peer dispersion is 2.32 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000064066 s/s
system poll interval is 64, last update was 30 sec ago.
R_GW#sh ntp ass
R_GW#sh ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.2.0.4        51.68.44.27      4     33     64   377  1.958 -19.842  2.328
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R_GW#
```

SYSLOG

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 14:48:50			192.168.3.203	26		Syslog	00:38:33: %SYS-5-CONFIG_I: Configured from console by tech on vty0 (192.168.3.1 ...
Today 14:48:49			192.168.3.202	30		Syslog	00:38:32: %SYS-5-CONFIG_I: Configured from console by tech on vty0 (192.168.3.1 ...
Today 14:48:00			192.168.3.204	23		Syslog	00:37:45: %SYS-5-CONFIG_I: Configured from console by tech on vty0 (192.168.3.1 ...
Today 14:21:48			10.0.0.3	33		Syslog	*May 2 12:21:47.313: NTP Core (NOTICE): Clock is synchronized.
Today 14:21:48			10.0.0.3	32		Syslog	*May 2 12:21:47.313: NTP Core (INFO): synchronized to 10.2.0.4, stratum 4
Today 14:19:43			192.168.3.253	74		Syslog	May 2 12:19:42.899: NTP Core (INFO): system event 'event_peer/strat_chg' (0x04 ...
Today 14:19:43			192.168.3.253	73		Syslog	*May 2 12:19:42.899: NTP Core (NOTICE): Clock is synchronized.

Problèmes rencontrés

Les algorithmes de chiffrement proposés par les équipements Cisco en ma possession ne sont plus sécurisés, Windows émet un avertissement et bloque la connexion SSH lors de chaque tentative, j'ai donc du modifié quelques paramètres au niveau de la configuration SSH pour chaque hôte.

Pour la configuration de LogAnalyzer il faut bien penser à installer MySQLi sinon une erreur serveur nous bloquera, de même si la fonction « RevokeMagicQuotes() » n'est pas commentée.

Pour l'instant le serveur web n'est pas sécurisé, je ne pourrais pas mettre en place le chiffrement TLS/SSL par manque de temps.

Chapitre 5 : Haute disponibilité

Tâche 1 : Link Aggregation Control Protocol

SW_INTRA et SW_BUREAUX sont connectés l'un à l'autre grâce à **un seul câble**, celui-ci constitue un **point sensible et congestionne la bande passante**.

Pour remédier à ça, il existe plusieurs protocoles notamment **LACP** (Link Aggregation Control Protocol) qui est un **protocole standard de l'IEEE 802.3ad** et **PaGP** (Port Aggregation Protocol) qui est **propriétaire Cisco**.

Ces fonctionnalités permettent **d'agréger plusieurs liens entre eux**, par exemple deux liens physiques peuvent devenir un seul lien logique.

L'agrégation de liens peut être configurer d'une troisième façon : **l'EtherChannel** qui est aussi **propriétaire Cisco** mais contrairement aux deux autres protocoles celui-ci est **statique**.

LACP se configure sur les ports soit en mode « **active** », qui permettra au port de négocier les liaisons, soit en « **passive** » ici le port attendra la négociation.

En PaGP, ces modes sont respectivement « **desirable** » et « **auto** » et possèdent les mêmes fonctions.

Dans notre cas on active **LACP sur les 2 ports** du SW_BUREAUX, puis on effectue **la même configuration sur les deux ports** associer sur SW_INTRA, il faut penser à passer l'agrégat en mode trunk.

```
SW_BUREAUX(config)#int ra fa 0/15 - 16
SW_BUREAUX(config-if-range)#chann
SW_BUREAUX(config-if-range)#channel-gr
SW_BUREAUX(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

SW_BUREAUX(config-if-range)#int po1
SW_BUREAUX(config-if)#switchport mode trunk
```

Désormais si l'un des deux câbles ou un des ports venaient à ne plus être fonctionnels, **l'interconnexion des sous-réseaux sera toujours assurée**.

Tâche 2 : Rapid Per Vlan Spanning Tree Protocol

L'EtherChannel n'étant pas supporté sur les ports de switching des routeurs R_1 et R_2, la problématique de la **tolérance aux pannes entre les liens** R_1/R_2 et SW_INTRA/SW_DMZ était de mise.

Pour pallier ce risque les **connexions depuis les switchs vers les routeurs ont été doublées** afin de mettre en place le protocole Cisco **Rapid Per Vlan Spanning Tree**.

Le Spanning Tree est un protocole de **niveau 2**, **standard de l'IEEE 802.1D**, il détecte la **présence de boucle** en envoyant des **bridge protocole data unit** (BPDU) puis lorsqu'une boucle est présente, les commutateurs élisent un **switch racine** qui décidera en fonction de plusieurs facteurs, du meilleur chemin à garder puis bloquera les ports des autres commutateurs qui ont le coût le plus élevé, c'est l'état « **blocking** ».

Cisco a sa propre version du STP, le PVST ou **Per Vlan Spanning Tree** sont **fonctionnement est identique** à celui de STP mais au lieu de s'appliquer globalement comme STP, PVST applique une instance de STP à **chaque VLAN** comme son nom l'indique.

Ces protocoles de détection de boucle sont lents, il faut **environ 40 secondes** à un port pour prendre le relais en cas d'incident.

Néanmoins il existe une version plus rapide le **RSTP et le RPVST** qui sont les mêmes acronymes mais on y ajoute le R pour « Rapid », ces solutions permettent de passer à un temps de convergence **d'environ 5 secondes**, grâce à un algorithme de convergence qui fait passer le nombre d'état avant de passer en **Forwarding, de 4 à 3 : Discarding, Learning, Forwarding**.

On applique donc ce mode sur les 3 switchs :

```
SW_DMZ(config)#spanning-tree mode rapid-pvst
```

On configure le routeur R_1 en mode « **root** » afin qu'il décide de l'état des ports selon les changements de topologie, (R_1 et R_2 ne supportent pas le RPVST, ils sont en STP standard) :

```
R_1(config)#spanning-tree vlan 10 root primary
 VLAN 10 bridge priority set to 8192
 VLAN 10 bridge max aging time unchanged at 20
 VLAN 10 bridge hello time unchanged at 2
 VLAN 10 bridge forward delay unchanged at 15
```

NB : impossible de sélectionner plusieurs VLAN en même temps j'ai donc dû procéder un par un.

Ensuite afin que le protocole gagne encore en vitesse de convergence, on active le **portfast** et le **bpduguard** sur tous les ports d'accès par défaut des switchs.

La fonctionnalité portfast permet de **passer un port directement en mode forwarding** sans passer par tous les modes qui le précède.

Quant à bpduguard, il permet **d'empêcher la connexion d'un commutateur pirate** sur un port d'accès, s'il reçoit des bdpu le port se désactivera.

L'activation par défaut **permet de déployer les fonctionnalités sur les ports d'accès** de façon automatique.

```
SW_DMZ(config)#spanning-tree portfast de
SW_DMZ(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
```

```
SW_DMZ(config)#spanning-tree portfast bpduguard default
SW_DMZ(config)#
```

Tâche 3 : Hot Standby Routing Protocol

La mise en place de **tolérance aux pannes** au niveau 3 nécessite un deuxième routeur, ainsi que la configuration d'un protocole de **redondance**, ici j'utiliserais **HSRP** (dans la section « problème », j'explique pourquoi pas GLBP).

Ce protocole doit être configurer sur minimum **deux routeurs**, il faut mettre en place les sous réseaux sur chaque routeur avec une petite spécifité : il faut attribuer a chaque passerelle de même réseau une adresse **IP différentes**, car nos routeurs s'identifiront entre eux grâce aux adresses distincte mais aux yeux des autres appareils seront vue par leur **adresse commune qui est l'adresse passerelle**.

Afin de gagner du temps dans la configuration des deux routeurs, **j'utilise le serveur TFTP** pour récupérer les fichiers de configuration de chacun, et les **édites à la main** en appliquant les configurations nécessaire pour l'utilisation de HSRP, cette manipulation me permets aussi de **« copier-coller » la configuration basique de R_1 vers R_2** sans avoir à tout faire manuellement.

HSRP fonctionne par groupe, **chaque réseau est mis dans un groupe** HSRP lui permettant de reconnaitre son ou ses pairs sur les autres routeurs **grâce à un ID de groupe**, chaque routeur est soit **actif soit passif** mais il ne peut y avoir **qu'un seul routeur actif par réseau**, ce rôle est attribué grâce à une **priorité,** qui est définit lors de la configuration ou manuellement. Ensuite il faut attribuer **l'adresse IP virtuelle de passerelle**, puis permettre aux routeurs de devenir actif en fonction de la **priorité la plus haute**.

Ici R_1 sera notre routeur actif :

```
interface Vlan21
 ip address 172.17.21.253 255.255.255.0
 standby 21 ip 172.17.21.254
 standby 21 priority 150
 standby 21 preempt
```

Et R_2 notre routeur passif ou de « secours »

```
interface Vlan21
 ip address 172.17.21.252 255.255.255.0
 ip helper-address 10.2.0.1
 standby 21 ip 172.17.21.254
 standby 21 preempt
```

NB : Afin de garantir une optimisation de la bande passante, il faut affecter un nom à chaque groupe « standby » que l'on configurera dans les routeurs membre des groupes. Le but étant d'indiquer ces noms de groupes dans le relais DHCP afin de ne pas avoir de surcharge de requête DHCP.

```
interface Vlan2
 ip address 192.168.2.253 255.255.255.0
 ip access-group etp_in in
 ip helper-address 10.2.0.1 redundancy V2
 standby version 2
 standby 2 ip 192.168.2.254
 standby 2 priority 150
 standby 2 preempt
 standby 2 authentication md5 key-chain HSRP
 standby 2 name V2
```

Tâche 4 : Répartition de charge

On possède désormais deux routeurs qui peuvent prendre le relais entre eux si jamais l'un tombe en panne, en revanche tant qu'un des deux routeurs ne tombe pas en panne, on se retrouve avec un **routeur qui ne fonctionne quasiment pas** et qui pourrais permettre **d'améliorer la bande passante disponible**.

Cependant, il est possible, grâce au **protocole RPVST** de **diviser la charge sur chaque réseau**.

NB : il faut bien différencier SPT et PVST pour cette partie, car PVST est propriétaire Cisco et peut prendre en charge plusieurs réseau ou VLAN, contrairement à RSTP ou STP qui sont des protocoles standards IEEE 802.1D et 802.1W.

Pour cela il suffit de définir les routeurs racine en fonction des VLAN, dans notre cas R_1 s'occupera du routage des VLAN 1,2,3 et 10 et R_2 des VLAN 11,21,80 et 99.

Mais pour continuer de bénéficier de la redondance des passerelles grâce à HSRP, il faut aussi définir les **racines secondaires** sur les routeurs, R_1 est donc racine primaire des VLAN 1,2,3 et 10 mais il sera la racine secondaire du 11,21,80 et 99 et **vice-versa pour R_2**.

Configuration root R_1 :

```
                                    Root Hello Max  Fwd
Vlan                Root ID         Cost Time  Age Delay  Root Port
---------------- ------------------ ----- ---- ---- -----  ----------------
VLAN1            8192 001e.13be.ba0a     0    2   20    15  This bridge is root
VLAN2            8192 001e.13be.ba0b     0    2   20    15  This bridge is root
VLAN3            8192 001e.13be.ba0c     0    2   20    15  This bridge is root
VLAN10           8192 001e.13be.ba0d     0    2   20    15  This bridge is root
VLAN11           8192 001d.45c9.36e0    38    2   20    15  FastEthernet4
VLAN21           8192 001d.45c9.36e1    38    2   20    15  FastEthernet4
VLAN80           8192 001d.45c9.36e2    38    2   20    15  FastEthernet4
VLAN99           8192 001d.45c9.36e3    38    2   20    15  FastEthernet4
```

Configuration root R_2 :

```
                                        Root Hello Max  Fwd
Vlan                Root ID             Cost Time  Age Delay  Root Port
---------------- ------------------- ----- ---- ---- -----  ----------------
VLAN1            8192 001e.13be.ba0a    38    2   20    15  FastEthernet4
VLAN2            8192 001e.13be.ba0b    38    2   20    15  FastEthernet4
VLAN3            8192 001e.13be.ba0c    38    2   20    15  FastEthernet4
VLAN10           8192 001e.13be.ba0d    38    2   20    15  FastEthernet4
VLAN11           8192 001d.45c9.36e0     0    2   20    15  This bridge is root
VLAN21           8192 001d.45c9.36e1     0    2   20    15  This bridge is root
VLAN80           8192 001d.45c9.36e2     0    2   20    15  This bridge is root
VLAN99           8192 001d.45c9.36e3     0    2   20    15  This bridge is root
```

On peut visualiser les liaisons bloquées :

```
R_2#sh spanning-tree active brief
```

Pour le VLAN 10 dont R_1 est la racine primaire, on peut voir que tous les liens sont en fowarding (fwd) ou « envoie » (les interfaces de la machine racine **primaire sont toujours en envoie**, ce sont les interfaces des équipements « **esclaves** » qui sont bloquées) :

```
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1        128.1    128    19 FWD     0  8192 001e.13be.ba0d 128.1
FastEthernet2        128.2    128    19 FWD     0  8192 001e.13be.ba0d 128.2
FastEthernet3        128.3    128    19 FWD     0  8192 001e.13be.ba0d 128.3
FastEthernet4        128.4    128    19 FWD     0  8192 001e.13be.ba0d 128.4
```

Tandis que sur R_2 un seul port est FWD :

```
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1        128.1    128    19 BLK    19 32778 000e.833c.ab00 128.23
FastEthernet2        128.2    128    19 BLK    19 32778 000e.833c.ab00 128.21
FastEthernet3        128.3    128    19 BLK    19 32778 000d.29ca.8600 128.23
FastEthernet4        128.4    128    19 FWD    19 32778 000d.29ca.8600 128.21
```

Sur SW_INTRA un seul port est BLK (bloquer) car ce port est le lien redondant vers R_1 :

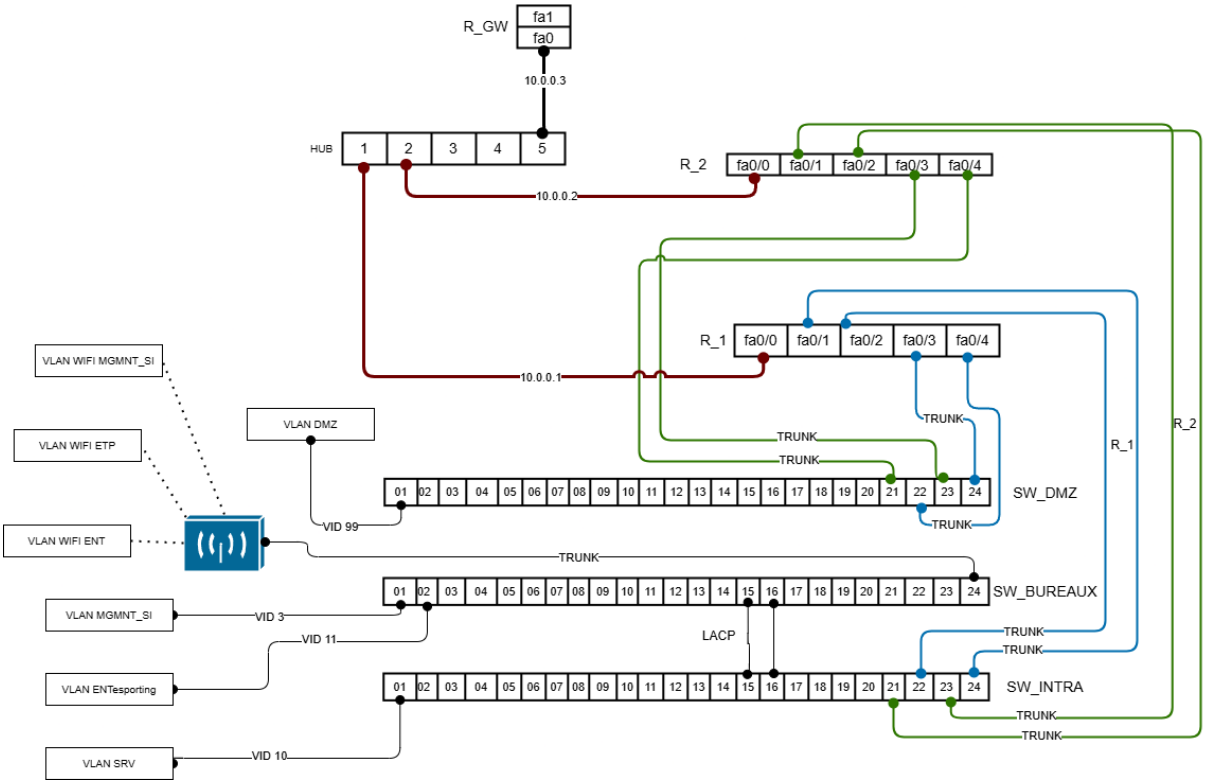
```
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/21           Desg FWD 19        128.21   P2p Peer(STP)
Fa0/22           Altn BLK 19        128.22   P2p Peer(STP)
Fa0/23           Desg FWD 19        128.23   P2p Peer(STP)
Fa0/24           Root FWD 19        128.24   P2p Peer(STP)
Po1              Desg FWD 12        128.65   P2p
```

On a le même agencement sur SW_DMZ :

```
Fa0/21           Desg FWD 19        128.21   P2p Peer(STP)
Fa0/22           Altn BLK 19        128.22   P2p Peer(STP)
Fa0/23           Desg FWD 19        128.23   P2p Peer(STP)
Fa0/24           Root FWD 19        128.24   P2p Peer(STP)
```

Tâche 5 : Rapport de test

Rappel câblage



STP (RPVST)

Pour vérifier le fonctionnement du Spanning Tree, il suffit d'éteindre le port d'un switch puis d'observer le changement de topologie :

Par exemple sur SW_DMZ j'éteins le port Fa0/24 :

```
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/21           Desg FWD 19        128.21   P2p Peer(STP)
Fa0/22           Altn BLK 19        128.22   P2p Peer(STP)
Fa0/23           Desg FWD 19        128.23   P2p Peer(STP)
Fa0/24           Root FWD 19        128.24   P2p Peer(STP)
```

On constate que le port alternatif (ALTN) prend le relais :

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    Edge P2p
Fa0/21           Desg BLK 19        128.21   P2p Peer(STP)
Fa0/22           Root FWD 19        128.22   P2p Peer(STP)
Fa0/23           Desg BLK 19        128.23   P2p Peer(STP)
```

LACP

Pour vérifier le bon fonctionnement il suffit d'utiliser la commande ***: « show Etherchannel summary »*** qui nous indiquera les agrégats et s'ils sont opérationnels ou non.

```
SW_INTRA#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------
1      Po1(SU)         LACP      Fa0/15(Pd)  Fa0/16(P)
```

```
SW_INTRA#sh int trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/21      on           802.1q         trunking      1
Fa0/22      on           802.1q         trunking      1
Fa0/23      on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1
Po1         on           802.1q         trunking      1
```

HSRP

Dans un premier temps on vérifie la configuration HSRP « standby » pour être sûr que les deux routeurs sont bien synchronisés :

(Le 1er screenshot a été pris pendant la configuration de la répartition de charge, d'où les différences de priorités)

```
R_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    150 P Active  local           192.168.2.252   192.168.2.254
Vl3         3    150 P Active  local           192.168.3.252   192.168.3.254
Vl10        10   150 P Active  local           10.2.0.252      10.2.0.254
Vl11        11   100 P Active  local           172.17.11.252   172.17.11.254
Vl21        21   100 P Active  local           172.17.21.252   172.17.21.254
Vl80        80   100 P Active  local           172.17.80.252   172.17.80.254
Vl99        99   100 P Active  local           172.16.2.252    172.16.2.254
```

```
R_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    100 P Standby 192.168.2.253   local           192.168.2.254
Vl3         3    100 P Standby 192.168.3.253   local           192.168.3.254
Vl10        10   100 P Standby 10.2.0.253      local           10.2.0.254
Vl11        11   100 P Standby 172.17.11.253   local           172.17.11.254
Vl21        21   100 P Standby 172.17.21.253   local           172.17.21.254
Vl80        80   100 P Standby 172.17.80.253   local           172.17.80.254
Vl99        99   100 P Standby 172.16.2.253    local           172.16.2.254
```

Ensuite, on effectue un test pratique, pour ça il suffit d'éteindre une passerelle sur le routeur primaire, puis de vérifier que R_2 prend bien le relais.

Désactivation du VLAN 2 :

```
R_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    150 P Init    unknown         unknown         192.168.2.254
Vl3         3    150 P Active  local           192.168.3.252   192.168.3.254
Vl10        10   150 P Active  local           10.2.0.252      10.2.0.254
```

Adaptation sur R_2 :

```
R_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    100 P Active  local           unknown         192.168.2.254
Vl3         3    100 P Standby 192.168.3.253   local           192.168.3.254
Vl10        10   100 P Standby 10.2.0.253      local           10.2.0.254
```

Répartition de charge STP

Idem que le test de redondance des passerelles : on vérifie d'abord le résumé HSRP :

R_1 :

```
R_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    150 P Active  local           192.168.2.252   192.168.2.254
Vl3         3    150 P Active  local           192.168.3.252   192.168.3.254
Vl10        10   150 P Active  local           10.2.0.252      10.2.0.254
Vl11        11   100 P Standby 172.17.11.252   local           172.17.11.254
Vl21        21   100 P Standby 172.17.21.252   local           172.17.21.254
Vl80        80   100 P Standby 172.17.80.252   local           172.17.80.254
Vl99        99   100 P Standby 172.16.2.252    local           172.16.2.254
```

R_2 :

```
R_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    100 P Standby 192.168.2.253   local           192.168.2.254
Vl3         3    100 P Standby 192.168.3.253   local           192.168.3.254
Vl10        10   100 P Standby 10.2.0.253      local           10.2.0.254
Vl11        11   150 P Active  local           172.17.11.253   172.17.11.254
Vl21        21   150 P Active  local           172.17.21.253   172.17.21.254
Vl80        80   150 P Active  local           172.17.80.253   172.17.80.254
Vl99        99   150 P Active  local           172.16.2.253    172.16.2.254
```

Les deux routeurs ont bien la charge des VLAN attribués.

Maintenant on va tester la solution dans un cas pratique :

1. Je vais faire un ping continue depuis un PC client (172.17.11.0/24 VLAN11) vers le contrôleur de domaine (10.2.0.1 VLAN 10) ;

```
C:\Users\admins>ping 10.2.0.1 -t

Envoi d'une requête 'Ping'  10.2.0.1 avec 32 octets de données :
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=6 ms TTL=127
```

2. Eteindre le port root sur SW_INTRA (la racine passe de Fa0/23 a Fa0/21);

```
VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    8192
             Address     001d.45c9.36e0
             Cost        19
             Port        23 (FastEthernet0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     000e.833c.ab00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Altn BLK 19        128.21   P2p Peer(STP)
Fa0/22           Desg FWD 19        128.22   P2p Peer(STP)
Fa0/23           Root FWD 19        128.23   P2p Peer(STP)
Fa0/24           Desg FWD 19        128.24   P2p Peer(STP)
Po1              Desg FWD 12        128.65   P2p
```

➔

```
VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    8192
             Address     001d.45c9.36e0
             Cost        19
             Port        21 (FastEthernet0/21)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     000e.833c.ab00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/21           Root FWD 19        128.21   P2p Peer(STP)
Fa0/22           Desg BLK 19        128.22   P2p Peer(STP)
Fa0/24           Desg BLK 19        128.24   P2p Peer(STP)
Po1              Desg FWD 12        128.65   P2p
```

3. Vérifier si le ping reprend ;

```
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Délai d'attente de la demande dépassé.
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
```

4. Rallumer le port (on constate que le procédé met plus de temps dans ce sens, dans l'onglet « problème » se trouve une explication) ;

```
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 172.17.11.2 : Impossible de joindre l'hôte de destination.
Délai d'attente de la demande dépassé.
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
Réponse de 10.2.0.1 : octets=32 temps=1 ms TTL=127
```

5. Eteindre l'interface passerelle sur R_2, ici VLAN 11 ;

```
R_2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    100 P Standby 192.168.2.253   local           192.168.2.254
Vl3         3    100 P Standby 192.168.3.253   local           192.168.3.254
Vl10        10   100 P Standby 10.2.0.253      local           10.2.0.254
Vl11        11   150 P Init    unknown         unknown         172.17.11.254
Vl21        21   150 P Active  local           172.17.21.253   172.17.21.254
Vl80        80   150 P Active  local           172.17.80.253   172.17.80.254
Vl99        99   150 P Active  local           172.16.2.253    172.16.2.254
R_1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    150 P Active  local           192.168.2.252   192.168.2.254
Vl3         3    150 P Active  local           192.168.3.252   192.168.3.254
Vl10        10   150 P Active  local           10.2.0.252      10.2.0.254
Vl11        11   100 P Active  local           unknown         172.17.11.254
Vl21        21   100 P Standby 172.17.21.252   local           172.17.21.254
Vl80        80   100 P Standby 172.17.80.252   local           172.17.80.254
Vl99        99   100 P Standby 172.16.2.252    local           172.16.2.254
```

6. Et on s'aperçoit que le ping continu ne s'est pas interrompu.

On bénéficie donc de **deux niveaux de tolérance aux pannes** l'un sur la couche réseau pour les passerelles, et l'autre sur la couche liaison grâce au spanning tree, mais aussi d'une répartition de charge, qui n'est pas la plus performante mais qui optimise les flux réseaux.

Problèmes rencontrés

Les routeurs R_1 et R_2 sont assez vieux, de ce fait il est impossible d'utiliser RSTP ou RPVST, en conséquence la convergence est ralentie lors d'incident sur les routeurs, en revanche, les switchs utilisent RPVST, les différents protocoles sont inter compatible, du coup on bénéficie quand même de la rapidité de ces derniers mais uniquement sur un incident survenant sur les switchs (couche liaison).

Aux vues du fonctionnement de la répartition de charge du protocole GLBP, il m'a semblé plus judicieux d'utiliser HSRP pour la redondance L3 combiné à STP qui ajoute une redondance de couche 1 et 2 mais qui en plus permet de répartir la charge sur les routeurs avec le même fonctionnement GLBP (round-robin), cette méthode est plus fastidieuse à mettre en place mais permets de bénéficier de tous les avantages de GLBP avec une plus forte tolérance aux pannes.

Chapitre 6 : Sécurisation des équipements

Tâche 1 : Sécurisation globale

NTP

On ajoute une ACL dans le fichier de configuration **chrony** autorisant uniquement les appareils du réseau à se synchroniser :

```
allow 10.2.0.1
allow all 192.168.3.253
allow 192.168.3.252
allow 192.168.3.202
allow 192.168.3.203
allow 192.168.3.204
allow 10.0.0.3
allow 172.16.2.0/24
local stratum 4
```

HSRP

Pour que les routeurs **s'authentifient** entre eux, afin d'éviter l'usurpation de passerelle par un routeur pirate, on va **définir un mot de passe haché en MD5** que les deux routeurs s'échangeront lors des **négociations HSRP** afin de prouver leurs authenticités.

Tout d'abord on crée un **trousseau de clé** ici : « HSRP », on **crée une clé** : « key 1 », puis **on définit** la valeur avec un **indicateur de difficulté** (obsolète aujourd'hui sur ces modèles) :

```
R_1(config)#key chain HSRP
R_1(config-keychain)#key 1
R_1(config-keychain-key)#key-string 7 1234
R_1(config-keychain-key)#
```

Ensuite on assigne ce **trousseau à chaque groupe HSRP** des routeurs (la méthode est identique sur tous les routeurs faisant partie des groupes HSRP) :

```
R_2(config-if)#standby 3 authentication md5 key-chain HSRP
R_2(config-if)#int vlan 10
R_2(config-if)#standby 10 authentication md5 key-chain HSRP
R_2(config-if)#int vlan 11
R_2(config-if)#standby 11 authentication md5 key-chain HSRP
```

OSPF

Pour empêcher l'usurpation de paquet OSPF, on attribue un mot de passe hasher en MD5 a chaque interface concernée par OSPF.

```
R_1(config)#in fa0
R_1(config-if)#ip ospf authentication message-digest
R_1(config-if)#ip ospf message-digest-key 1 md5 1234
R_1(config-if)#end
```

Running-config

Pour éviter que les **mots de passes soient affichés en clair** dans les fichiers de configuration, on chiffre les mots de passe grâce à la commande : « ***service password-encryption*** »

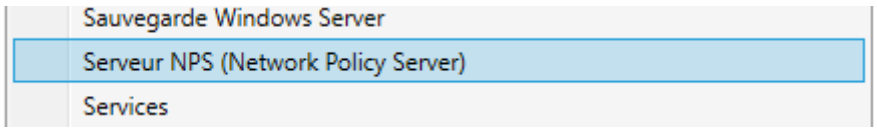
```
enable password 7 025756085F
```

Tâche 2 : NPS RADIUS

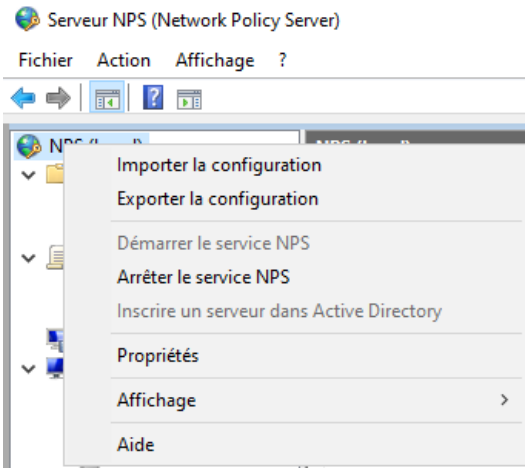
Authentification équipement réseau

Afin de **s'authentifier depuis l'annuaire active directory** qui fera office d'autorité de connexion, on installe le rôle de Network Policy Server sur le contrôleur de domaine.

Une fois le **rôle installer** on **active le serveur d'authentification**, en se rendant dans la barre d'outils > Serveur NPS :



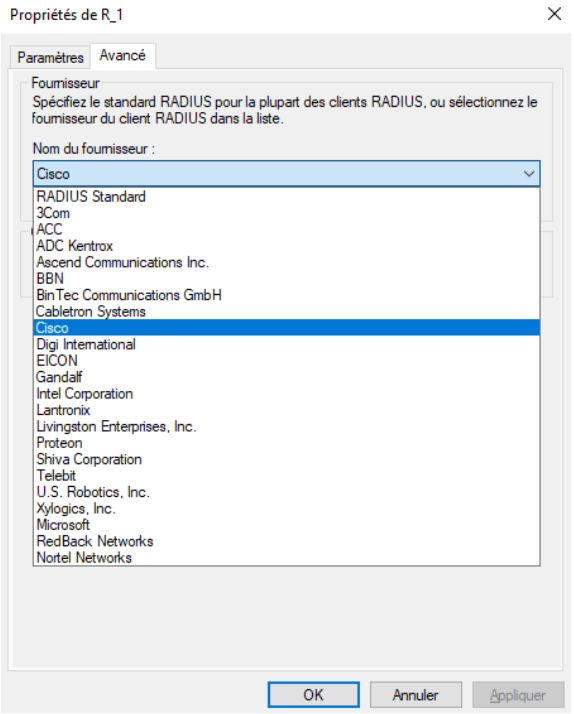
Ensuite on « inscrit un serveur dans Active Directory » :



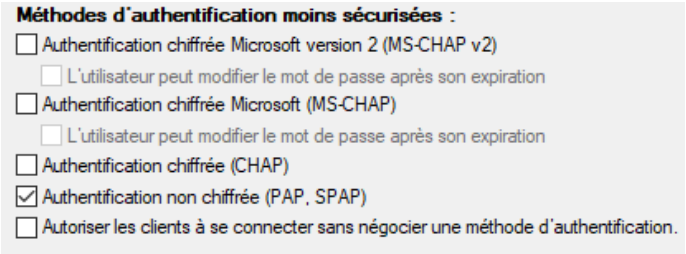
Puis on **crée nos clients RADIUS** qui sont nos commutateurs et routeurs en définissant une clé de partage, il **faudra l'utiliser aussi pour la configuration coté client** :

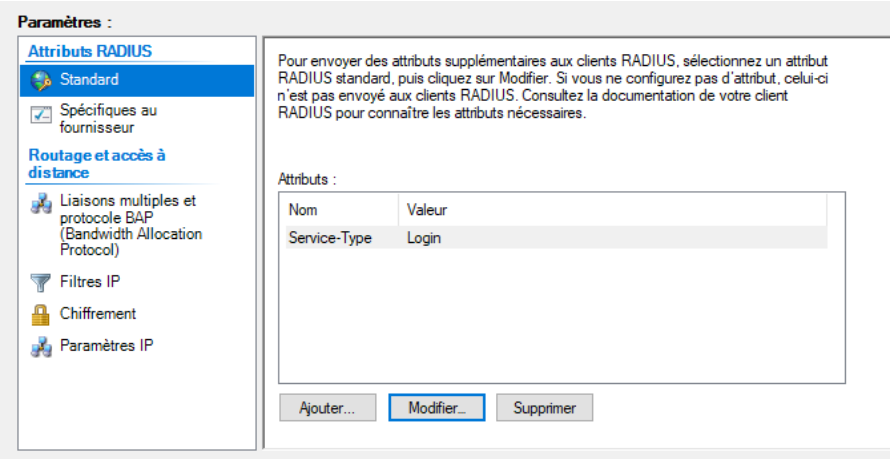
R_1	192.168.3.253	Cisco	Activé
R_2	192.168.3.252	Cisco	Activé
R_GW	192.168.3.3	Cisco	Activé
SW_DMZ	192.168.3.204	Cisco	Activé
SW_BUREAUX	192.168.3.203	Cisco	Activé
SW_INTRA	192.168.3.202	Cisco	Activé

Lors de la création des clients il faut **renseigner la marque du matériel** (ici Cisco) :

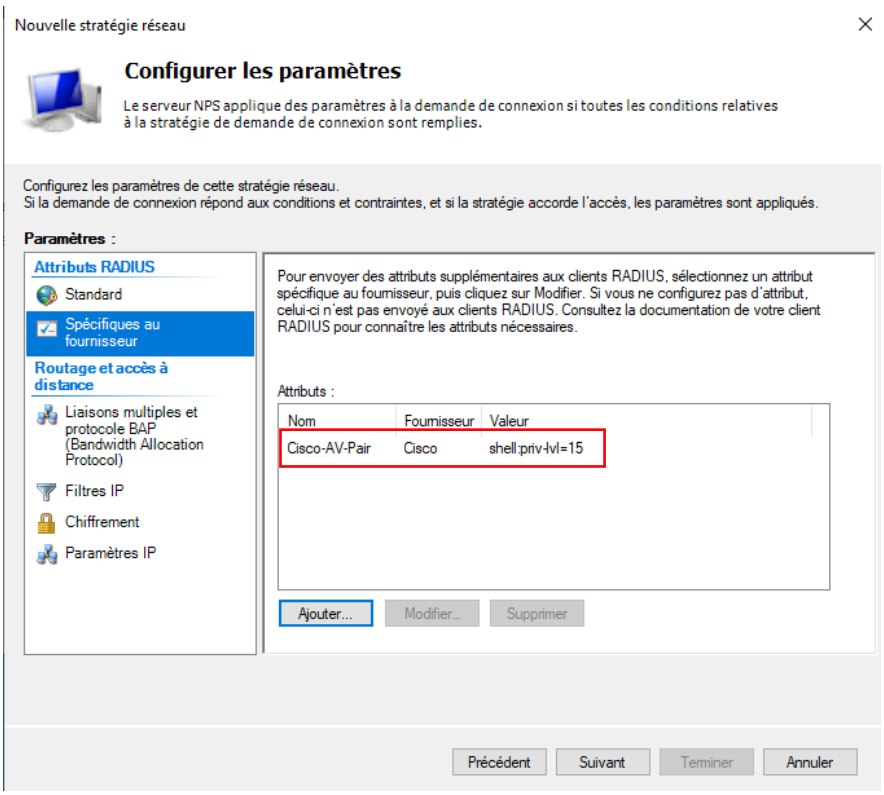


Une fois fait, on crée une **nouvelle stratégie réseau**, qui nous permettra de se connecter grâce à différents facteurs, notamment la vérification si l'utilisateur (active directory) est **autorisé à se connecter** au matériel par l'attribution d'un groupe a cette stratégie, de même il faut modifier un paramètre afin de retourner les logins à l'équipement, mais surtout on devra activer l'authentification non chiffrée sans quoi on ne pourra pas se connecter.





On ajoute le fournisseur de l'équipement toujours pour **permettre l'inter-compatibilité**, mais aussi pour **attribuer le niveau de privilège** a la connexion de l'utilisateur :



Il nous reste plus qu'à **configurer la partie Cisco**.

Pour ça il faut crée un **groupe de serveur radius**, puis ajouter un **serveur radius** a celui-ci :

```
R_2(config)#aaa group server radius AP
```

```
R_2(config-sg-radius)#server-private 10.2.0.1 key 1234
```

Les ports attribuer par défaut sont **1645** pour l'authentification et **1646** pour la gestion étant donné qu'ils correspondent à mon serveur NPS je **laisse les options par défaut** et renseigne la clé d'échange du serveur.

Ensuite, il faut paramétrer le **mode d'authentification** par défaut qui sera effectué, ainsi que les **autorisations**, dans le cas où le serveur viendrait à tomber en panne, je spécifie en **dernière priorité l'authentification local** :

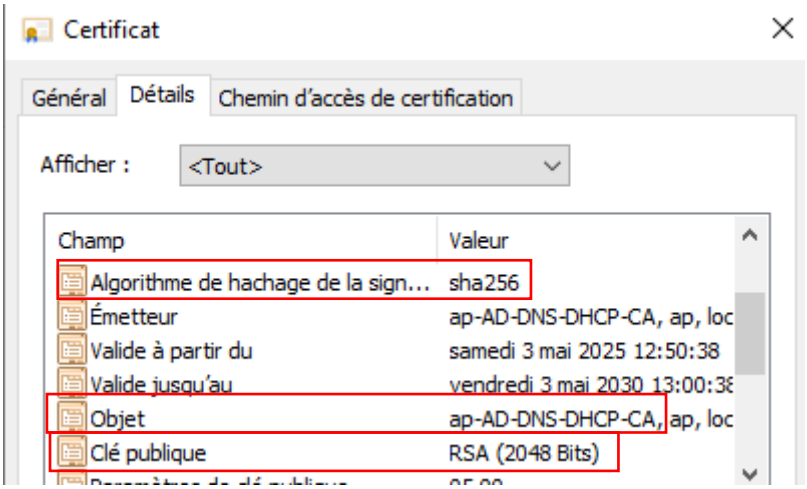
```
aaa authentication login default group AP local
aaa authorization exec default group AP local
```

Nous procéderons au test de ce dernier a la fin de la mission.

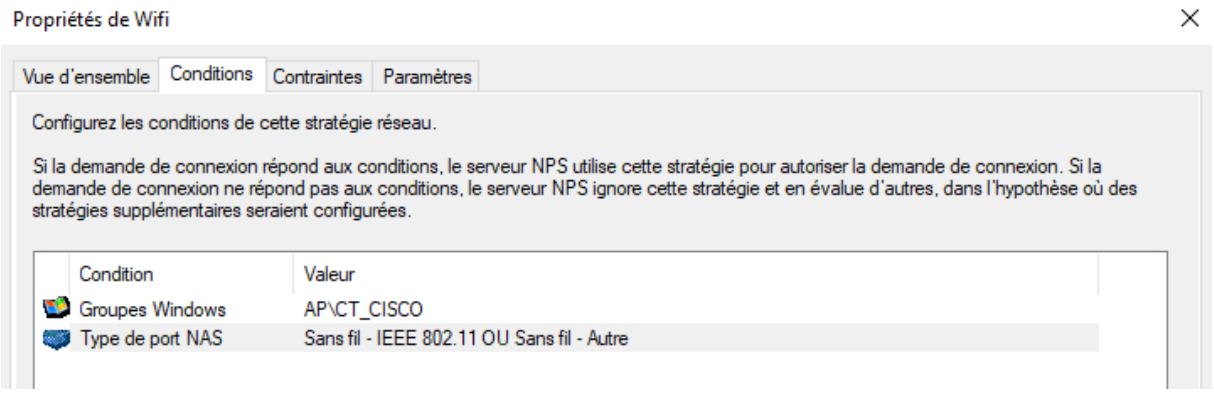
Authentification Wi-Fi

Pour sécuriser les **SSID des réseaux ETP et MGMNT_SI, la norme WPA2-enterprise est mise en place.**

Ce procédé nécessite la mise en place d'un **serveur de certification**, que supportera notre contrôleur de domaine, pour cela il faut dans un premier temps installer le rôle d'autorité de certification, puis crée un certificat lors de la configuration du rôle, ici nous utiliserons **l'algorithme de hachage SHA256** ainsi qu'une **clé publique de type RSA de 2048 bits** :

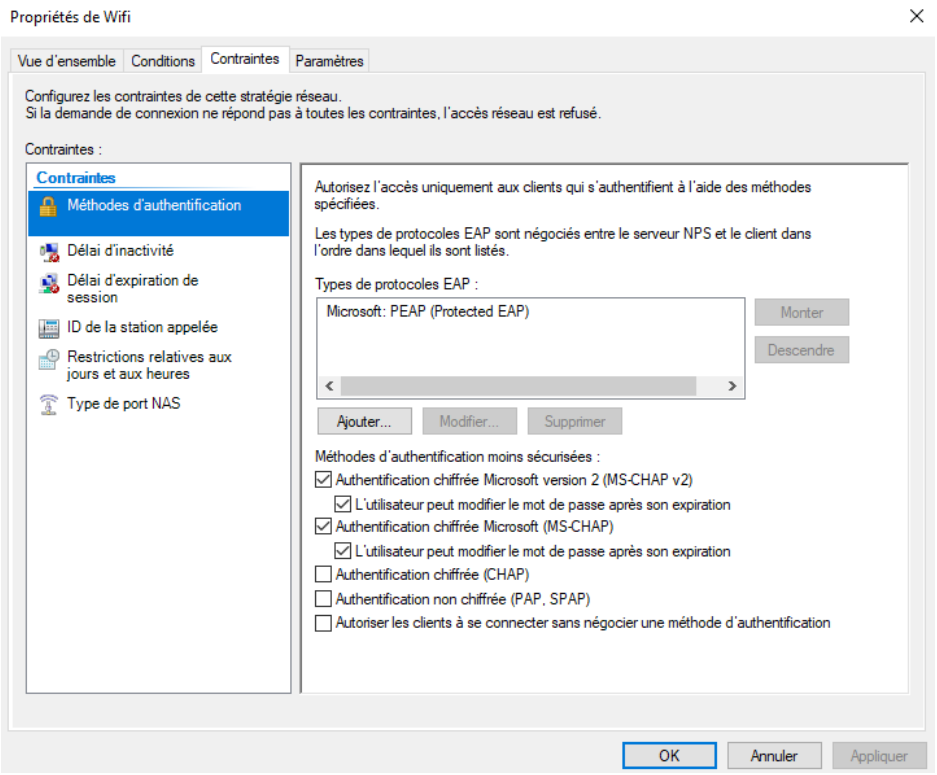


Une fois notre certificat crée, on peut définir la stratégie réseau sur notre serveur NPS que nous appellerons « ***Wifi*** », cette fois-ci dans les conditions d'accès on ajoutera le type de port NAS à savoir : « ***Sans fil -IEEE 802.11*** » ainsi que « ***Sans fil – Autre*** » :

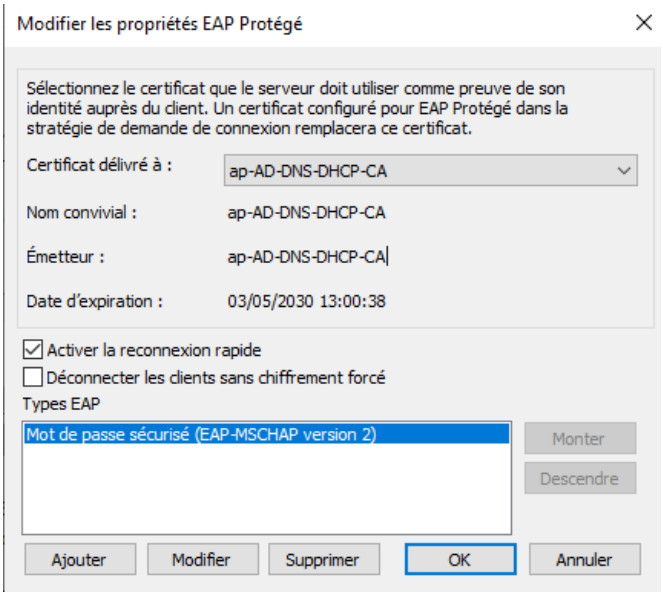


NB : A la différence de l'authentification pour les équipements, ici à l'étape de configuration des paramètres, on peut laisser les valeurs défaut.

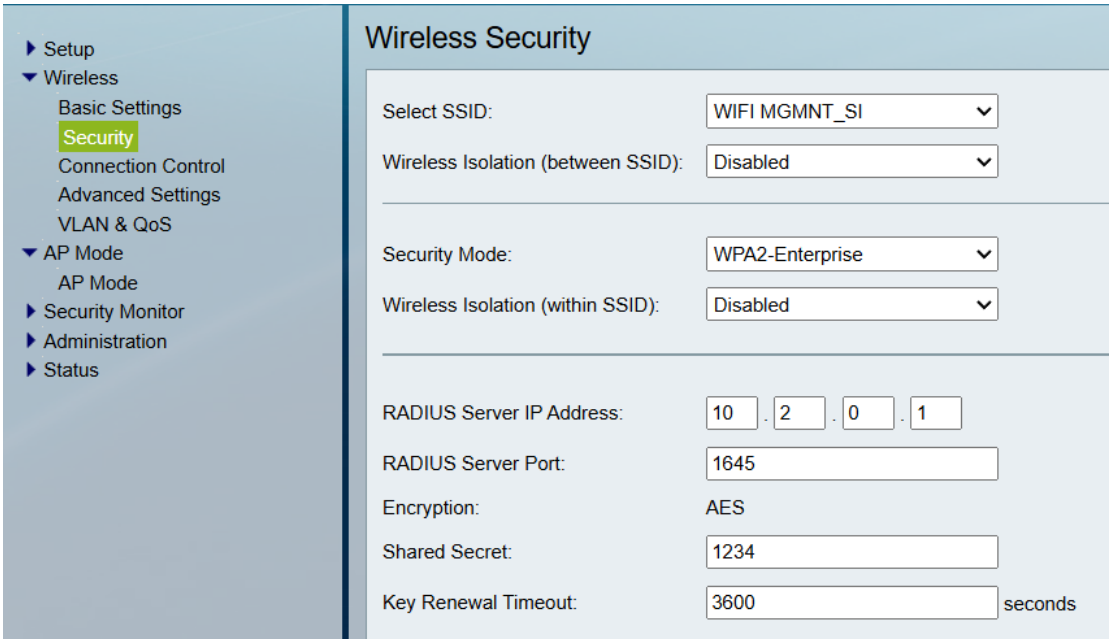
Ensuite dans les contraintes nous ajouterons le protocole « ***Microsoft : PEAP (Protected EAP)*** » et nous cocherons les cases de même manière que sur le screenshot :



Et c'est à ce moment que l'on va configurer l'utilisation du certificat précédemment crée, on modifie les propriétés du protocole EAP précédemment ajouté, pour y associer le certificat crée juste avant :



Une fois fait, on passe à la configuration du point d'accès, on se rend dans l'onglet ***security***, puis on entre les paramètres du serveur NPS en sélectionnant le SSID ciblé :



Notre authentification est en place, de même que pour le procédé précédent nous vérifierons le bon fonctionnement dans la tâche « rapport de test ».

Tâche 3 : Sécurité L2 (Port-security)

Pour sécuriser les ports des commutateurs contre des attaques de types de ***mac-flooding***, ainsi que pour contrôler les machines qui se connecte on met en place la

fonctionnalité de ***port-security***, qui permets de définir des ACL d'adresses MAC autoriser sur les ports d'accès.

Afin de gagner du temps dans la configuration et de diminuer la marge d'erreurs on définit les adresses mac autorisé de manière dynamique, c'est-à-dire ***sticky***. Puis on autorise un historique du nombre d'adresse MAC par port de 10 sur les ports 1 à 8 :

```
SW_BUREAUX#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Fa0/1            10           1                 0         Shutdown
     Fa0/2            10           1                 0         Shutdown
     Fa0/3            10           0                 0         Shutdown
     Fa0/4            10           0                 0         Shutdown
     Fa0/5            10           0                 0         Shutdown
     Fa0/6            10           0                 0         Shutdown
     Fa0/7            10           0                 0         Shutdown
     Fa0/8            10           0                 0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
SW_BUREAUX#sh port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   3    2cf0.5d98.c363    SecureSticky        Fa0/1         -
  11    c8a3.62b0.b60b    SecureSticky        Fa0/2         -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Ensuite, on définit le comportement en cas de non-conformité, dans notre cas on éteindra le port grâce à la commande « ***switchport port-security violation shutdown*** » sur toutes les interfaces concernées.

Tâche 4 : Sécurité L3 (ACL)

Pour contrôler les flux entrants et sortants, un ensemble de règles de contrôle d'accès ont été mises en place, pour une partie ce sont des listes de contrôle d'accès (ACL) **standard** dans lesquelles uniquement l'autorisation ou l'interdiction suivit d'une plage IP ou d'un hôte peut être spécifié ces types **d'ACL** sont assez basique et ne permettent pas une gestion des flux trop complexe.

Mais pour la majeure partie des ACL déployées ce sont des ACL **étendues**, dans lesquelles ont peut définir non seulement l'action (autoriser ou interdire) mais aussi la source, la destination, le port et le tout agrémenté d'opérateurs tel que : égale (eq), plus grand que (gt), plus petit que (lt) … ce qui rend ce type de règles très efficaces et modulables.

Etant donné la complexité et le nombre de règle mise en place, je ne m'épancherais pas sur chacune d'elles, mais la listes des ACL en place est disponible en annexe.

Le but ici est segmenter les flux réseaux en fonction de leur besoin et de leur criticité, par exemple, le réseau où se trouve les serveurs interne aura des règles d'accès bien plus restrictive et plus contrôler que le réseau des entreprises utilisatrices ou que la DMZ.

Voici un tableau démontrant le découpage de réseau selon la sécurité nécessaire des contrôles d'accès :

Réseau	Niveau de sécurité (5 = Maximum)
Serveur interne	5
Management SI	4
Bureaux TiersLieux86	3
Réseaux entreprises utilisatrices	3
DMZ	2

Une fois les contrôles d'accès mis en place sur les sous réseaux, pour encore améliorer la sécurité, un certain nombre de règle dites « **réflexives** » ont été déployées sur l'interface interne du routeur passerelle.

Le but des **ACL réflexives** est de ne laisser passer uniquement les communications qui ont été initialisées d'un certains coté, quand un poste interne se connecte à internet et effectue une recherche, le routeur va automatiquement autoriser le chemin retour de ce trafic pendant un certains temps, puis si ce temps arrive à expiration sans relance depuis l'intérieur alors le trafic sera bloqué.

Ce dispositif permet une gestion fire wall intelligente et dynamique ce qui accrue de manière non négligeable la sécurité de l'infrastructure.

Tâche 5 : Rapport de test

NTP

```
tech@SRVLNX:~$ sudo chronyc clients
[sudo] password for tech:
Hostname                      NTP   Drop Int IntL Last     Cmd   Drop Int  Last
===============================================================================
10.0.0.3                      534      0   6   -    40       0      0   -     -
10.2.0.1                      399      0  10   -   390       0      0   -     -
192.168.3.202                 371      0   6   -    25       0      0   -     -
192.168.3.253                 289      0   6   -   20h       0      0   -     -
192.168.3.252                 290      0   6   -   20h       0      0   -     -
192.168.3.203                 371      0   9   -    79       0      0   -     -
192.168.3.204                 454      0   6   -    62       0      0   -     -
```

HRSP

```
    56 19.901783    192.168.3.252    224.0.0.102      HSRPv2    114 Hello (state Standby)
▸ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
▾ Cisco Hot Standby Router Protocol
  ▸ Group State TLV: Type=1 Len=40
  ▾ MD5 Authentication TLV: Type=4 Len=28
      MD5 Algorithm: MD5 (1)
      Padding: 0x00
      MD5 Flags: 0
      Sender's IP Address: 192.168.3.252
      MD5 Key ID: 1
      MD5 Authentication Data: f81c07af2118e11cc902685ea8b92241
```

OSPF

```
   149 211.242924    10.0.0.1         224.0.0.5        OSPF      138 Hello Packet
▾ Open Shortest Path First
  ▾ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 52
      Source OSPF Router: 1.1.1.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x0000 (None)
      Auth Type: Cryptographic (2)
      Auth Crypt Key id: 1
      Auth Crypt Data Length: 16
      Auth Crypt Sequence Number: 946700621
      Auth Crypt Data: 598371f63fb73cb5478edd9bf9bd92a5
```

Radius

Administration

```
R_1#sh radius statistics
                                Auth.       Acct.       Both
         Maximum inQ length:      NA          NA          1
       Maximum waitQ length:      NA          NA          1
       Maximum doneQ length:      NA          NA          1
       Total responses seen:       2           0          2
     Packets with responses:       2           0          2
  Packets without responses:       0           0          0
  Access Rejects           :       0
 Average response delay(ms):      24           0         24
 Maximum response delay(ms):      40           0         40
  Number of Radius timeouts:       0           0          0
       Duplicate ID detects:       0           0          0
 Buffer Allocation Failures:       0           0          0
Maximum Buffer Size (bytes):      84           0         84
Malformed Responses       :       0           0          0
Bad Authenticators        :       0           0          0
Unknown Responses         :       0           0          0
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/2
 1646/0
```

```
132 10.972196    10.2.0.252      10.2.0.1        RADIUS    126 Access-Request id=2
133 11.030209    10.2.0.1        10.2.0.252      RADIUS    163 Access-Accept id=2
134 11.030219    10.2.0.1        10.2.0.252      RADIUS    163 Access-Accept id=2,
```

Wi-fi

SSID :	WIFI MGMNT_SI
Protocole :	802.11g
Type de sécurité :	WPA2 - Entreprise
Fabricant :	Realtek Semiconductor Corp.
Description :	TP-Link Wireless MU-MIMO USB Adapter
Version du pilote :	1030.44.1014.2024
Type d'informations de connexion :	Microsoft: PEAP (Protected EAP)
Bande passante réseau :	2,4 GHz
Canal réseau :	6
Vitesse de connexion (Réception/ Transmission) :	54/54 (Mbps)
Adresse IPv6 locale du lien :	fe80::5be5:6373:eb5d:5f57%12
Adresse IPv4 :	192.168.3.13
Serveurs DNS IPv4 :	10.2.0.1 (non chiffré)
Suffixe DNS principal :	ap.local
Adresse physique (MAC) :	30-DE-4B-89-5E-71

Port-security

```
SW_INTRA#sh port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 3
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 3
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0
```

Problèmes rencontrés

La mis en place des ACL a demandé une grande quantité de travail, en raison du niveau de sécurité qui a été mit en place ainsi que du nombre de règle.

Points à améliorer

- Chiffrer les flux HTTP du serveur NTP/SYSLOG/TFTP ;
- Le remplacement des équipements par de plus récent afin de bénéficier de protocole plus sécurisé, d'augmenter la bande passante mais aussi de pallié le point critique du switch d'interconnexion des routeurs ;
- Ajouter un contrôleur de domaine pour la tolérance aux pannes de celui-ci ;
- Crée un script d'automatisation des sauvegardes ;
- Ajouter un serveur NAS ;
- Ajout d'une connexion internet de secours ;
- Mettre en place une gestion des flux plus simple, comme un pare feu dédié ;
- Déployer un serveur de gestion des incidents et de parc (GLPI).

Bilan

Désormais notre infrastructure est fonctionnelle, elle comporte plusieurs technologies différentes toutes imbriquer les unes avec les autres afin de former une architecture réseaux fiable, sécurisée et fonctionnelle.

L'infrastructure mise en place possède non seulement les **fonctionnalités standards** d'un SI notamment, le routage (interne mais aussi externe), la segmentation réseau, la traduction d'adresses vers l'extérieur, la configuration automatique de l'adressage IP ainsi qu'un point d'accès wifi.

Mais aussi d'autres capacités tel que la **tolérance aux pannes** grâce à la redondance des routeurs via HSRP, la redondance des médias grâce au spanning tree.

Ou encore, une **administration améliorée des équipements** a travers la mise en place de l'accès a distance via SSH, la journalisation centralisée de ces équipements via rsyslog combiner à un serveur web qui procure une interface graphique pour visualiser les logs, un serveur TFTP permettant de réaliser des sauvegardes mais aussi d'en restaurer ou de mettre à jours les images systèmes des machines et enfin un serveur de temps sur lequel toutes les machines composant le SI se synchronisent.

Bien entendu, une infrastructure digne de ce nom doit aussi avoir des **mécanismes de sécurité** puissant, c'est pour cela que nous avons renforcé plusieurs points sensibles, comme la régulation des synchronisation NTP via une ACL d'adresse, la protection du spanning tree contre les commutateurs pirates, la sécurisation des ports des commutateurs qui ne permettent qu'un certain nombre d'adresses MAC à se connecter. Mais la fonctionnalité la plus puissante de ce système est la précision des **règles de filtrages IP**, que ce soit interne comme le cloisonnement entre les différents VLAN, mais aussi externe afin d'empêcher les connexions malveillantes vers des équipements critiques.

De plus, des modalités **d'authentifications robustes** sont en place, tel que l'authentification via un serveur RADIUS pour certains SSID ou pour les connexions SSH aux équipements réseaux. Certains protocoles ont été sécurisés en modifiant les mots de passe par défaut et en ajoutant une fonction hashage.

En conclusion, notre infrastructure est désormais prête pour la mise en production, celle-ci possède toutes les fonctionnalités imposées par le cahier des charges et même plus. Ainsi que toute la documentation nécessaire à son utilisation.

Compétences couvertes

Bloc 1

- Gérer le patrimoine informatique ;
- Répondre aux incidents et aux demandes d'assistance et d'évolution ;
- Travailler en mode projet ;
- Mettre à disposition des utilisateurs un service informatique.

Bloc 2

- Concevoir une solution d'infrastructure réseau ;
- Installer, tester et déployer une solution d'infrastructure réseau ;
- Exploiter, dépanner et superviser une solution d'infrastructure réseau.

Bloc 3

- Sécuriser les équipements et les usages des utilisateurs ;
- Garantir de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ;
- Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service.

Sources

- Accès SSH sur un équipement Cisco | Cisco | IT-Connect
- Définir un mot de passe sur un matériel Cisco | Cisco | IT-Connect
- Changer la bannière d'accueil des appareils Cisco | Cisco | IT-Connect
- Cisco - Configurer un client NTP | Cisco | IT-Connect
- Attribuer un nom d'hôte de périphérique sur les commutateurs gérés de la gamme 300 à l'aide de l'interface de ligne de commande - Cisco
- 11.4.2.2 Sauvegarde et restauration via TFTP
- Configuration vlan sur un switch Cisco
- Configuration d'un trunk entre deux switch – CISCOMADESIMPLE.BE
- VTP (ou comment se simplifier la vie avec les VLAN) – Réussir son CCNA
- Mise en place de VLANs et de routage inter-VLANs | Cisco | IT-Connect
- Gestion des logs SYSLOG - cisco.goffinet.org
- Lab Spanning-Tree et Rapid Spanning-tree Cisco - cisco.goffinet.org
- EtherChannel sous Cisco avec LACP | Cisco | IT-Connect
- Mise en place du protocole GLBP sous Cisco | Cisco | IT-Connect
- Redondance de passerelle protocole HSRP - cisco.goffinet.org
- Mise en place du protocole HSRP | Cisco | IT-Connect
- GLBP : Gateway Load-Balancing Protocol – CISCOMADESIMPLE.BE
- Quelques éléments supplémentaires sur la sécurité d'un switch Cisco - YouTube
- Faire soi même un câble RJ45 croisé et le vérifier
- Cisco | Le filtrage MAC sur les switchs Catalyst
- Configuring MAC ACLs [Support] - Cisco Systems
- Configuration ACL Standard - Guide Complet
- Configuration du NAT sur un routeur Cisco – CISCOMADESIMPLE.BE
- Les adresses IP privées et publiques | Administration Réseau | IT-Connect
- Network Address Translation (NAT44) - cisco.goffinet.org
- Tutoriel RADIUS Switch | All IT Network
- Authentification radius sur un router avec SSH | CISCO PACKET TRACER FOREVER
- Authentification 802.1X sur un réseau Ethernet (Port-Based Authentication) – WS-C2950 vs WS-C3750 – CISCOMADESIMPLE.BE
- ACLs Cisco IPv4 et IPv6 - cisco.goffinet.org
- Introduction au protocole de routage dynamique OSPF - cisco.goffinet.org
- Configuration du routage ospf - routeur Cisco
- How to configure logging in Cisco IOS - Cisco Community
- Envoi des logs d'un équipement Cisco vers un serveur Syslog - Astarox
- Mise en place d'un serveur de temps (NTP) sous Linux | Commandes et Système | IT-Connect
- Comment configurer un serveur Rsyslog sur Debian 12 - Shapehost
- Installer Syslog sur Debian 12 - Doknet
- Serveur de log Syslog :: Formatux
- Installation et paramétrage logwatch | webdevpro.net
- config switch cisco 2950
- NTP : la synchronisation temporelle avec Chrony | Services | IT-Connect

- chrony – chrony.conf(5)
- Adding a Local Network Time Server in Linux
- chrony – chrony.conf(5)
- chrony – chronyc(1)
- Synchronisation temporelle NTP - cisco.goffinet.org
- Configuring NTP on a Cisco Device – No Blinky Blinky
- Les listes de contrôle d'accès (ACL) avec Cisco | IT-Connect
- Spanning-Tree et Rapid Spanning-tree Cisco - cisco.goffinet.org
- Switchport Port-Security (Sécurité sur les ports) Cisco en IOS - cisco.goffinet.org
- Configurer le Routage Inter-VLAN : Routeur et Switch n3
- WAP200AG.book
- Diapositiva 1
- CMSBE_F04_ACL.pdf
- OSPF : Configuration Basique | Networklab
- Cisco IOS Binaries Collection 2019 12 : Free Download, Borrow, and Streaming : Internet Archive
- IOS upgrade via FTP (Cisco) - Grandmetric
- Installer LogAnalyzer sur Debian 12 - La procédure complète - Doknet
- [Tuto] Centraliser les journaux d'événements Linux avec Rsyslog et LogAnalyzer (+ vidéo) – NEPTUNET.FR
- GLBP | Networklab
- Chrony et NTP | DevSecOps
- Linux - Windows : prioriser une route ou interface pour accéder à Internet