MISSION 3 : SECURITE RESEAU & VLANS PARTIE 1

SOMMAIRE

PRÉSENTATION DU TP :

La mission 3 consiste à mettre en place une architecture de vlan et de routage de vlan, elle a pour but de nous faire étudier leurs fonctionnements et nous apprendre a correctement configuré les Switchs et les routeurs. De plus cette mission met aussi en œuvre une batterie de serveur, ftp,http, tftp, ntp ,… qui nous apprend à travers un environnement concret de crée des services et les maintenir tout en documentant nos actions.

MÉTHODE :

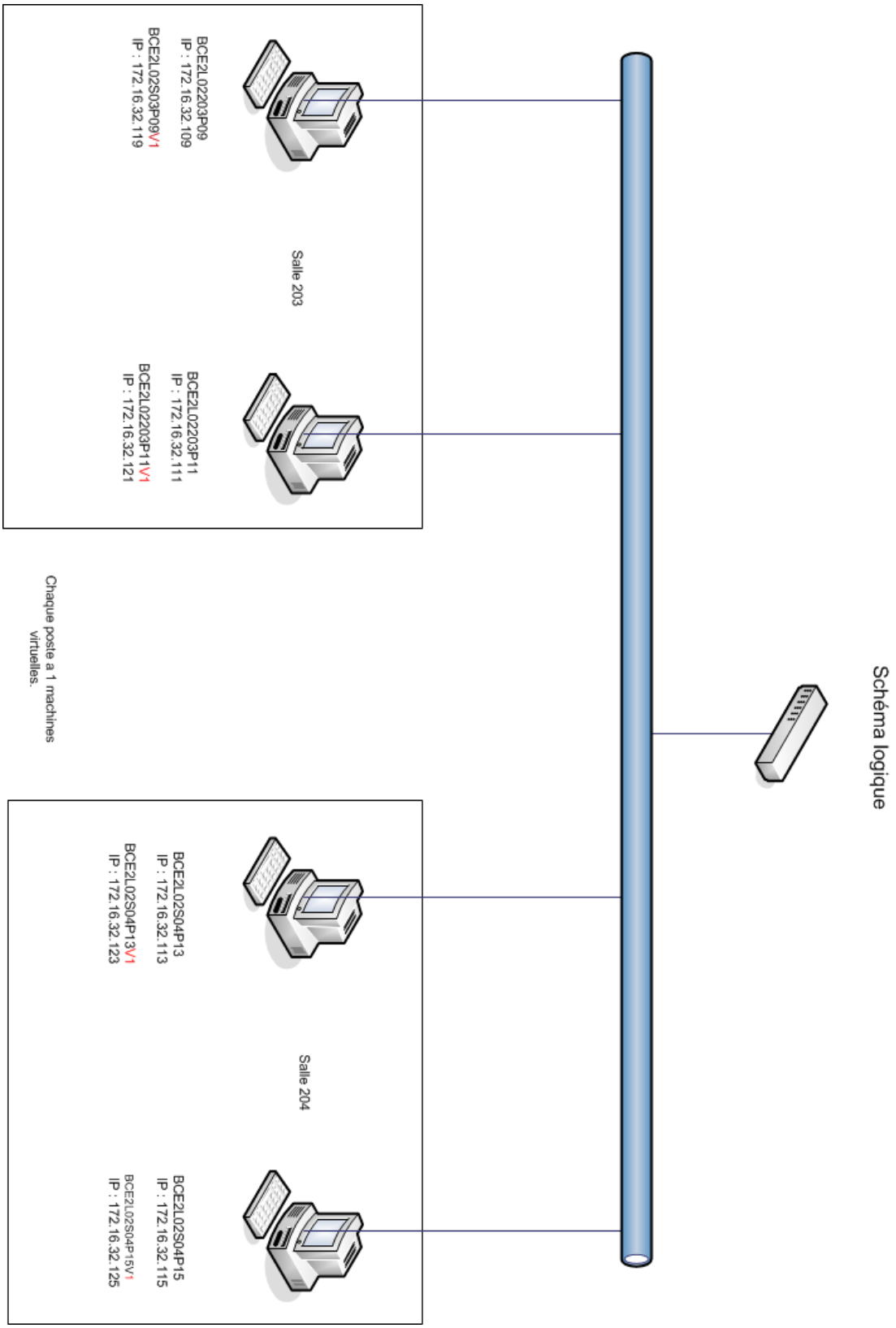
I) PARTIE A : TRAVAIL DE REFLEXION

1) PLAN D'ADRESSAGE IP DU RESEAU

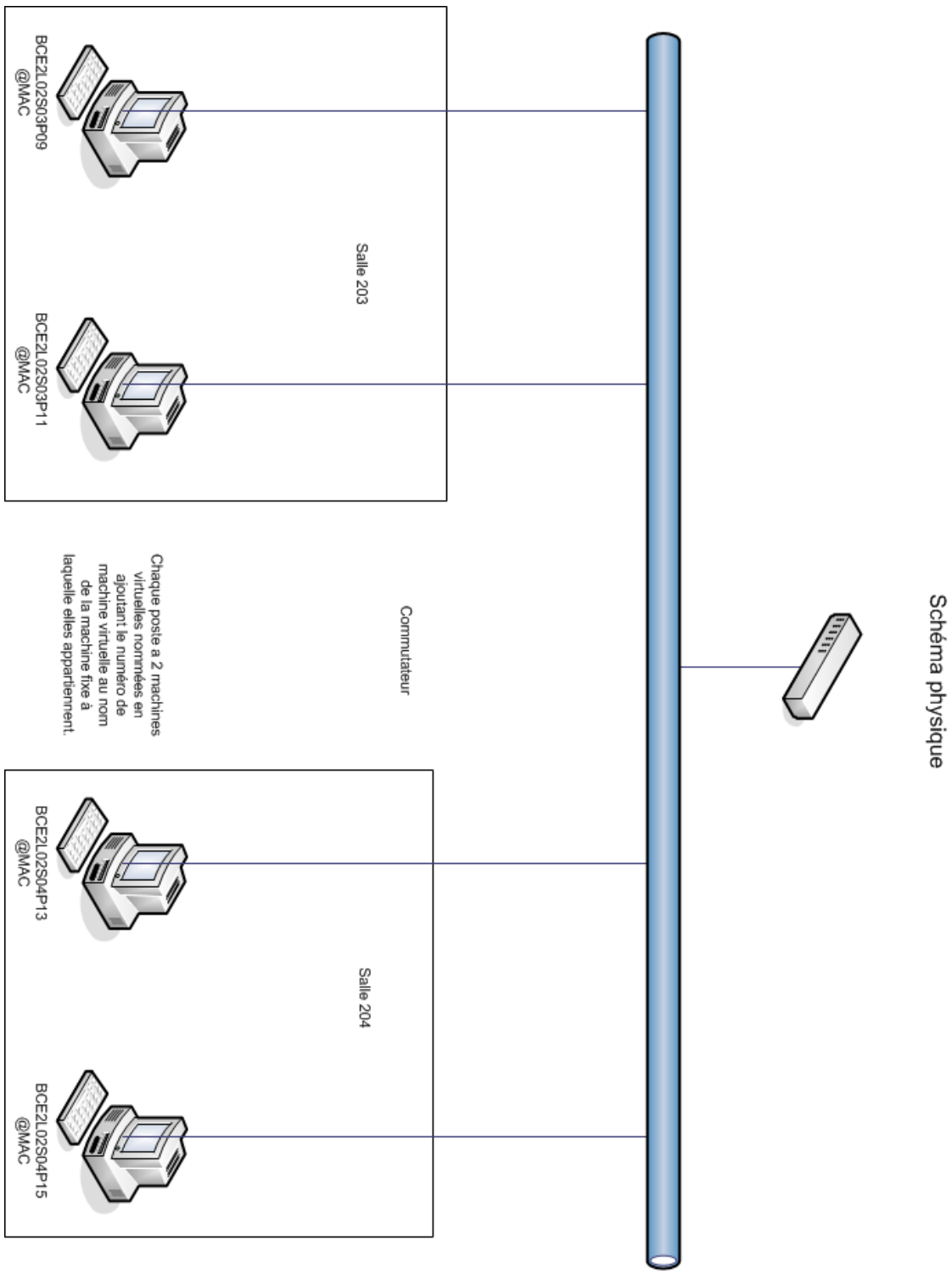
Ligue B (Badminton) du bâtiment C au 2e étage.

Réseau : 172.16.32.0			
	Nom des postes	Physique	VM - 01
Adrien F.	BCE2L02203P09 BCE2L02S03P09V1	172.16.32.109	172.16.32.119
Alexandre P.	BCE2L02203P11 BCE2L02S03P11V1	172.16.32.111	172.16.32.121
Adrien S.	BCE2L02S04P13 BCE2L02S04P13V1	172.16.32.113	172.16.32.123
Alexandre B.	BCE2L02S04P15 BCE2L02S04P15V1	172.16.32.115	172.16.32.125

2) SHEMA LOGIQUE DU RESEAU



3) SHEMA PHYSIQUE



4) TABLEAU D'AFFECTATION PORT VLAN-SWITCH

Ports	9	10	11	12	13	14	15	16	24
SAT	Port 9	Port 11	Port 13	Port 15	Non utilisé	Non utilisé	Non utilisé	Non utilisé	
IP	172.16.32.109	172.16.32.111	172.16.32.113	172.16.32.115	Non utilisé	Non utilisé	Non utilisé	Non utilisé	
VLANs	VLAN 32	VLAN 32	VLAN 32	VLAN 32	Non utilisé	Non utilisé	Non utilisé	Non utilisé	VLAN 128

II) PARTIE B : TRAVAIL DE RECHERCHE PREALABLE A LA MISE EN OEUVRE

1) LES TYPES DE VLAN A METTRE EN ŒUVRE

Il existe 3 types différents de VLAN :

- VLAN de niveau 1 (ou VLAN par port) : on y définit les ports du commutateur qui appartiendront à tel ou tel VLAN. Cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN.
- VLAN de niveau 2 (ou VLAN par adresse MAC) : on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1, car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée.
- VLAN de niveau 3 (ou VLAN par adresse IP) : même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN.

Conclusion quant au type de vlan à utiliser :

Les vlan de niveau 2 sont souvent utilisés pour des cas spéciaux, et très fastidieux a mettre en place pour un réseau d'entreprise de taille moyenne, car l'on doit rentrer chaque adresse MAC a la main.

Le vlan de niveau 3 peut être très intéressant, car il permettrait de rendre flexible le nombre de postes sans toucher a la configuration des switchs, car, soit par un serveur DHCP soit parce que l'adresse IP est statique, l'ordinateur qui se trouve dans le réseau de la maison des ligues rejoindra automatiquement le VLAN de la maison des ligues, mais cela entraîne un manque dans la sécurité, car l'adresse IP est facilement changeable se qui permettrais de changer de vlan facilement.

Le vlan de niveau 1 est intéressant, car il permettra de définir quel port appartient au vlan de la ligue badminton. Toutefois cette configuration n'est pas flexible pour l'ajout de poste supplémentaire par la suite et sa mise en place est fastidieuse, mais très sécurisée, car seul un certain port donné on accès au vlan.

Je conclus donc en disant qu'il faudra mettre en place un vlan de niveau 1 par port pour sa sécurité et qu'il est le plus simple à mettre en place contrairement au vlan de niveau 2.

2) CARACTERISTIQUE PHYSIQUE ET LOGICIEL DU MATERIEL D'INTERCONEXION RESEAU :

Switch1 :

Fabriquant : Cisco

Modele : Catalyst 2960 Serie

N.S : FCQ1603Y1E3

Nombre de Ports :

24 Ports ont 100 Mbit/s

2 Ports ont 1 Gb/s

Nombre de ports utilisé :

7 Ports ont 100 Mbit/s

Nombre de ports libres :

17 Ports ont 100 Mbit/s

2 Ports ont 1 Gbit/s

Version de l'os :

IOS 12.2SE5

Switch2 :

Fabriquant : Cisco

Modele : Catalyst 2960 Serie

N.S : FCQ1603Y1EP

Nombre de Ports :

24 Ports ont 100 Mbit/s

2 Ports ont 1 Gb/s

Nombre de ports utilisé :

0 Port a 100 Mbit/s

Nombre de ports libres :

24 Ports ont 100 Mbit/s

2 Ports ont 1 Gbit/s

Version de l'os :

IOS 12.2SE5

Nombre de routeurs types Cisco : 2

CISCO 1 :

Fabriquant : Cisco

Modele : ISR 29911

N.S: FCZ160570EK

Nombre de ports :

2 interfaces serie

3 ports ont 1Gbit/s

Nombre de ports utilisé :

2 ports ont 1Gbit/s

Nombre de ports libre :

1 Port a 1Gbit/s

2Ports serie

Verstion de l'os :

IOS 15.0 M5

Caractéristique :

4 slot d'extension, dont 1, utilisé par carte série

Adresse Ip de l'interface GE 0/1 : 172.20.193.44

Adresse Ip de l'interface GE 0/2 : 192.168.4.1

Route par défaut du routeur : 172.20.0.254

CISCO 2 :

Fabriquant : Cisco

Modele : ISR 29911

N.S: FCZ160570CU

Nombre de ports :

2 interfaces serie

3 ports ont 1Gbit/s

Nombre de ports utilisé :

0 port a 1Gbit/s

Nombre de ports libre :

3 Ports ont 1Gbit/s

2 Ports serie

Verstion de l'os : 15.0 M5

Caractéristique :

4 slot d'extension, dont 1, utilisé par carte série

3) COMMANDE CISCO POUR LES VLAN :

Commande pour la création d'un VLAN :

```
config t
vlan 2
name administration // nom du vlan
exit
```

Association d'une interface a un Vlan :

```
interface fastEthernet 0/1 // interface a ajouter au vlan
switchport mode access
switchport access vlan 3 //ajoute l'interface au vlan 3
exit
```

Définir un port trunck :

```
interface gigabitEthernet 1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

4) MODE D'ACCES AU MATERIEL D'INTERCONNECTION :

a)HyperTerminal est un programme qui permet de se connecter à d'autres ordinateurs,, des services en ligne et des ordinateurs hôtes. Intégré à Windows, l'Hyperterminal se présente en fait comme un bloc-notes doté de fonctionnalités de communication.

b) Telnet est un protocole permettant d'émuler un terminal à distance, cela signifie qu'il permet d'exécuter des commandes saisies au clavier sur une machine distante. L'outil *Telnet* est une implémentation du protocole Telnet, cela signifie qu'il s'agit de la traduction des spécifications en langage informatique pour créer un programme permettant d'émuler un terminal.

c)Il suffit de taper l'adresse IP du routeur dans le navigateur pour accéder à l'interface web du routeur.

d) Vlan Truncking Protocol permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des vlans sur l'ensemble d'un réseau local.

POUR SECURISER LES MODE D'ACCES IL NOUS FAUT LES COMMANDES DE BASES

- Ajout de mot de passe pour l'authentification
- Chiffrer tous les mots de passe d'un coup
- Activation et désactivation d'une interface web
- Créer une bannière de connexion
- Blocage des ports non fiables contre attaque DHCP
- Sécuriser les ports avec adresse Mac
- Vérification de la sécurité des ports

AJOUT DE MOT DE PASSE POUR L'AUTHENTIFICATION

```
Routeur-cisco(config)#enable secret m02p@55E
Routeur-cisco(config)#line con 0
Routeur-cisco(config-line)#password P@55w0rdcon5
Routeur-cisco(config-line)#login
Routeur-cisco(config-line)#exit
Routeur-cisco(config)#line vty 0 4
Routeur-cisco(config-line)#password P@55w0rdcon5
Routeur-cisco(config-line)#login
Routeur-cisco(config-line)#end
Routeur-cisco#
```

CHIFFRER TOUS LES MOTS DE PASSE

```
Routeur#conf t
Routeur(config)#service password-encryption
```

ACTIVATION ET DESACTIVATION D'UNE INTERFACE WEB

```
Routeur-cisco(config)#int fa0/0
Routeur-cisco(config-if)#no shutdown

Routeur-cisco(config)#int fa0/0
Routeur-cisco(config-if)#shutdown
```

CREER UNE BANNIERE DE CONNEXION

```
Comm1#configure terminal
Comm1(config)#banner login « Personnel autorisé uniquement » :
```
Configurer une bannière de connexion.

Ou alors :

```
Comm1(config)#banner login & ou « & » :
```
définit fin du texte

BLOCAGE DES PORTS NON FIABLE CONTRE ATTAQUE DHCP

La procédure ci-après illustre la manière de configurer la surveillance DHCP sur un commutateur Cisco IOS :

Étape 1. Activez la surveillance DHCP à l'aide de la commande de configuration globale ip DHCP snooping.
Étape 2. Activez la surveillance DHCP pour des réseaux locaux virtuels spécifiques au moyen de la commande ip DHCP snooping vlan number [nombre].
Étape 3. Au niveau de l'interface, définissez les ports comme étant fiables ou non en définissant les ports fiables avec la commande ip DHCP snooping trust.
Étape 4. (Facultatif) Pour limiter la fréquence à laquelle un pirate peut perpétuellement transmettre de fausses requêtes DHCP au serveur DHCP via des ports non fiables, utilisez la commande ip DHCP snooping limit rate fréquence.

SECURISER LES PORTS AVEC ADRESSE MAC

Il existe plusieurs façons de configurer la sécurité des ports.

Les sections suivantes décrivent les moyens de configurer la sécurité des ports sur un commutateur Cisco :
Adresses MAC sécurisées statiques : les adresses MAC sont configurées manuellement à l'aide de la commande de configuration d'interface switchport port-security mac-address adresse_mac. Les adresses MAC configurées de cette manière sont stockées dans la table d'adresses et sont ajoutées à la configuration en cours sur le commutateur.
Adresses MAC sécurisées dynamiques : les adresses MAC sont assimilées de manière dynamique et stockées uniquement dans la table d'adresses. Les adresses MAC configurées ainsi sont supprimées au redémarrage du commutateur.
Adresses MAC sécurisées rémanentes : vous pouvez configurer un port pour assimiler dynamiquement des adresses MAC, puis enregistrer ces dernières dans la configuration en cours.

VERIFICATION DE LA SECURITE DES PORTS

`Routeur#show port-security [interface id_interface]` : *Pour afficher les paramètres de sécurité des ports du commutateur ou de l'interface spécifiée*
`Routeur#show port-security [interface id_interface]` : *Pour afficher toutes les adresses MAC sécurisées configurées dans toutes les interfaces de commutation ou sur une interface définie avec informations d'obsolescence pour chacune*

5) SAUVEGARDE ET RESTAURATION DE MATERIEL D'INTERCONNECTION

Il est possible de sauvegarder la configuration d'un switch de plusieurs façons, avec plusieurs commandes de base.

SAUVEGARDE PAR COMMANDE DE BASE :

La première :

```
Switch# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

La deuxième :

```
Switch# write
Building configuration...
[OK]
switch#
```

La troisième, Sauvegarde par TFTP :

```
Switch1#copy startup-config tftp:
Address or name of remote host []? *serveur TFTP*
Destination filename [Switch1-confg]?
```

SAUVEGARDE AUTOMATIQUE SUR SERVEUR FTP :

Au vu des risques de crashs momentanés des matériels d'interconnexion et dans l'optique d'être performant dans la résolution des problèmes, il est préférable d'opter pour une sauvegarde automatique et récurrente vers un serveur, ici FTP.

On utilisera le programme *Kron* qui est un planificateur de tâches.

Mise en place :

Il faut se connecter en switch en mode privilégié

```
switch> enable
switch# conf t
```

Ensuite on va créer une policy-list pour inclure *Kron* qu'on nommera backupconfig

```
switch(config)# kron policy-list backupConfig
```

Donc maintenant que la policy est créée, on va ajouter une commande, la commande cli qui enverra running-config afin d'envoyer la configuration courante à un serveur distant (FTP,TFTP,HHTP etc)

Ici on utilise un serveur FTP.

```
switch(config-kron-policy)# cli show running-config | redirect
ftp://<host>/<path>/cisco.txt
```

Maintenant il faut préciser à quel moment cette commande s'effectuera, pour ça on créer une occurrence qu'on nommera backupConfig_occurence.
On précisera l'heure de sauvegarde automatique à 00h00, chaque jour.

```
switch(config)# kron occurrence backupConfig_occurence at 00h00 recurring
switch(config-kron-occurrence)# policy-list backupConfig
switch(config-kron-occurrence)# exit
switch(config)# exit
```

Tout est programmé il suffit de vérifier après l'heure de sauvegarde si tout c'est bien déroulé.

RESTAURATION D'UNE SAUVEGARDE :

La commande qui va suivre supprime toute la configuration de démarrage

```
switch# write erase
Erasing the nvram filesystem will remove all configuration files!
Continue ? [confirm]
[OK]
Erase of nvram: complete
switch#
```

Et celle-ci toutes les VLAN installés

```
switch# delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
switch#
```

Restauration à partir d'un TFTP :

```
switch#copy tftp://192.168.8.10/configswitch system:running-config ou
startup-config
```

6) ORGANISATION DES TACHES ET GANTT

ORGANISATION DES TACHES

1. Réflexion sur le plan d'adressage (configuration IP) et sur le VLAN à utiliser.

Utilisation des règles établies afin de trouver un plan d'adressage (configuration IP des machines) et de choisir un type de VLAN.

2. Réalisation de schémas physique et logique d'une solution possible.

Réaliser un schéma physique revient à faire un schéma du réseau après la mise en application de la solution en y annotant les adresses MAC.

Tandis que le schéma logique revient à faire un schéma du réseau après la mise en application de la solution en y annotant les adresses IP.

3. Réflexion sur l'affectation des ports du Switch.

Tâche de type organisationnelle, cette tâche est soit réalisée suivant des règles pré-établies, soit selon une logique si aucune règle spécifique n'a été donnée.

4. Réflexion et choix des modes d'accès et leurs sécurisations.

Le choix des modes d'accès et leurs sécurisations sont également un choix très important pour éviter que le réseau ne soit qu'un vulgaire gruyère au niveau de la sécurité.

5. Réflexion et choix des modes de sauvegarde et de restauration.

Le choix du mode de sauvegarde et de restauration de la configuration du Switch est un choix déterminant, car s'il y a un problème à ce niveau, c'est tout le réseau qui en subit les conséquences.

6. Simulation sur CISCO PACKET TRACER.

Ceci est un test de la solution, afin de voir ce qui ne va pas et ainsi pouvoir corriger les erreurs éventuelles.

7. Réflexion et réalisation d'un diagramme de GANTT pour la mise en œuvre de la solution.

Ceci est un travail de type organisationnel, c'est le planning des tâches afin de mettre en œuvre la solution.

8. Installation des machines.

Installation du système d'exploitation choisi, ici WINDOWS 7, pour qu'il soit le même dans tout le réseau M2L.

9. Configuration du Switch.

Ceci est le travail permettant de créer le réseau a proprement parler (configuration des ports,des modes d'accès, des modes de sauvegarde et de restauration, ainsi que la création et la configuration du VLAN).

10. Configuration des machines.

Configuration IP de toutes les machines du réseau (ordinateurs).

11. Test de la solution.

C'est la phase finale, si cette phase se déroule bien alors la solution a été mise en place avec succès.

La dernière colonne sert d'estimation en heures(h) ou en minutes(m) :

	1	2	3	4	5	6	7	8	9	10	11	Dur.
1		*	*	*	*							1h
2						*						30m
3						*						2h
4						*						2h
5						*						2h
6							*					2h
7								*				2h30
8									*			3h
9										*		1h30
10											*	30m
11												30m

DIAGRAMME DE GANTT :