Mission 3 – Phase A:
Sécurité réseau & VLANs

Les objectifs :

Etre capable de mettre en place une architecture de couche 2 sécurisée.

Les ressources :

Les documents transmis par le DSI.

Les ressources spécifiques

Le chef de projet se fera remettre les documents suivants par le DSI

- Fiches routeurs
- Fiches commutateurs
- 03-Mission-Schema-V00.pkt

Webographie

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swvlan.pdf
http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swg2950.pdf
http://routeur.clemanet.com/configuration-base-routeur-cisco.php
http://clemanet.com/configuration-base-switch.php

Phase A – solution d'infrastructure réseau

Pour mieux segmenter et sécuriser le réseau au sein de la maison des Ligues, il est convenu de découper l'adresse réseau 172.16.0.0 /16 en sous-réseaux. Pour information, le réseau actuel (donc avant la sécurisation) est rappelé en *annexe A*.

Règles du plan d'adressage à utiliser à partir de cette mission et pour les missions futures

Chaque étage de chaque bâtiment se verra attribuer un réseau **en /24**.

- Les deux octets de poids forts seront **172.16**. pour préserver l'existant et permettre un déploiement progressif
- Le troisième octet respectera la codification suivante : le chiffre des dizaines sera égal au rang alphabétique du bâtiment, le chiffre des unités correspondra au numéro de l'étage.
- La valeur de ce troisième octet servira aussi d'identifiant pour le VLAN

*Exemple : l'adresse réseau 172.16.**12**.0 /24 correspond au réseau du Bâtiment **A 2ème** étage. Ce réseau sera associé au vlan **12**.*

Un réseau sera dédié à la gestion des matériels d'interconnexions. Ce sera le réseau 172.16.128.0 / 24, il correspondra au VLAN 128 (management).

Cette mise en place a une influence sur le plan d'adressage des postes et serveurs au sein des Ligues.

Règles d'adressage fixe des STA

- L'adressage IP sera fixe.
- La valeur pour l'octet de poids faible sera égale à une valeur de base majorée du numéro de la prise de branchement.
- Pour les machines physiques, la valeur de base sera égale à 100.
- Pour la première VM (VM en mode bridge) d'une machine physique, l'octet de poids faible sera majoré de 10 par rapport à l'IP physique
- Pour la deuxième VM (VM en mode bridge) d'une machine physique, l'octet de poids faible sera majoré de 20 par rapport à l'IP etc…

Exemple :
Soit une machine physique dans le LAN 172.16.10.0 /24. Cette machine physique est brassée sur la prise 7. Elle dispose de 2 VM actives. Cela donnera le plan suivant

Nom →	*M-Physique*	*VM-01*	*VM-02*
IP en CIDR →	*172.16.10.107 /24*	*172.16.10.117 /24*	*172.16.10.127 /24*

Règles de brassage sur les matériels d'interconnexion

La mise en place de VLANs impose de la rigueur dans le branchement des STA sur les ports des switchs. Un serveur branché sur un 'mauvais' port peut devenir inaccessible aux utilisateurs. Les règles de gestion de l'affectation des ports sont présentées dans *l'annexe B.*

Remarque importante : ces règles de gestion devront être respectées scrupuleusement. Elles s'appliquent aux étudiants de BTS SIO2.

Contexte transposé en fonction de la salle 193

L'équipe **A** sera responsable de la ligue **A**thlétisme, l'équipe **B** de la ligue **B**adminton, l'équipe **C** de la ligue **C**anoë. L'équipe **D** 'se situera' dans le bâtiment B au rez de chaussée (le cœur de réseau).

Pour des **raisons pratiques liées à la longueur du câble console**, les postes A1, B1, C1, D1 seront les postes d'administration réseau des matériels d'interconnexion. Les postes A2, B2, C2, D2 seront affectés aux chefs de projets. Les postes A3, B3, C3 et D3 seront affectés aux Gestionnaires des serveurs. Les postes A4, B4 et C4 seront des postes utilisateurs pour les tests.

Poteau de brassage	Administrateur réseau	Chef de projet	Gestionnaire serveur	Utilisateur

L'annexe C précise uniquement l'implantation physique des salles des ligues (au sein de M2L) dont vous aurez la charge dans le cadre de cette mission.
L'annexe D vous rappelle les règles de nommages des postes utilisées au sein de M2L
L'annexe E détaille le rôle du service responsable du cœur de réseau

Travail à faire

Partie A – travail de réflexions

Le chef de projet **de chaque équipe** attribue à chaque membre une des 4 tâches ci-dessous à réaliser.
(Remarques : vous devez respecter les règles de présentations indiquées dans le document contexte général. Exceptionnellement, pour l'élaboration des documents, les postes seront démarrés et resteront brassés en mode Production)

1) Chaque équipe rédigera un document sous WORD présentant :
   - le plan d'adressage complet de son réseau
   - les configurations ip des STA
   - les noms attribués aux STA
2) Chaque équipe réalisera sous VISIO :
   - un schéma physique
   - un schéma logique
3) Chaque équipe réalisera sous EXCEL :
   - un tableau présentant l'affectation (au niveau des VLANs) des ports des matériels d'interconnexion utilisés et les liens de brassage.
4) Chaque équipe personnalisera le fichier Packet Tracer (transmis par le DSI au chef de projet) en fonction de sa situation. Les STA devront être nommés, configurés et brassés.
   Attention, vous ne devez pas supprimer les objets, vous pouvez les déplacer. Mais, il faut garder la structure des organisations autour des baies.

Partie B – travail de recherches préalables à la mise en œuvre

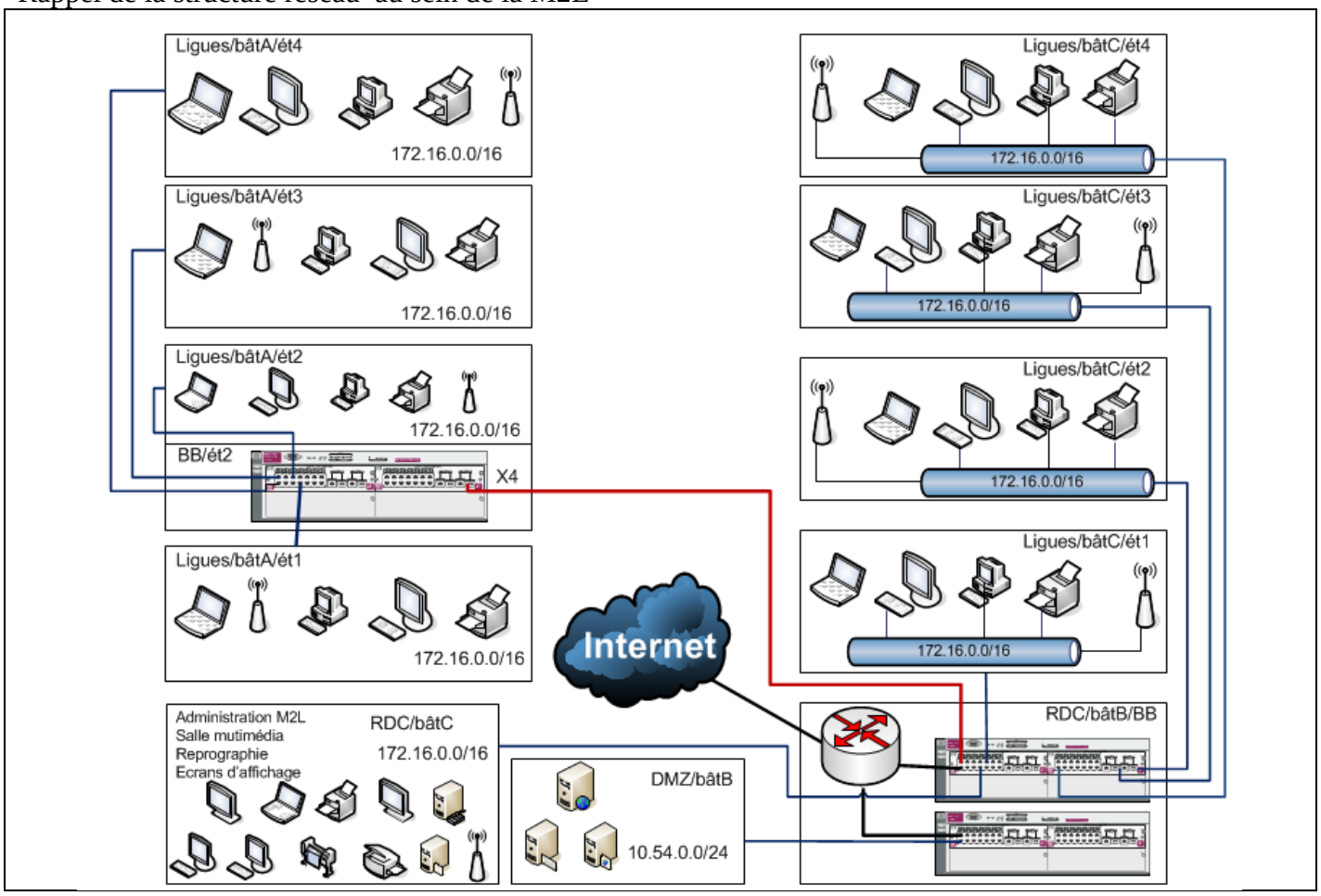
Avant la mise en place des VLAN et des sécurisations, il est nécessaire de s'informer efficacement.
Le chef de projet **des équipes A, B et C** attribue à chaque membre une des 4 tâches ci-dessous à réaliser.

1) Chaque équipe rédigera un document sous WORD présentant :
   - le type de VLAN à mettre en œuvre
   - les caractéristiques physiques et logicielles des matériels d'interconnexion disponibles
   - les commandes de base pour la création des VLAN
2) Chaque équipe rédigera un document sous WORD présentant :
   - Les différents modes d'accès possibles aux matériels d'interconnexion disponibles
   - Les commandes de base pour sécuriser ces modes d'accès
3) Chaque équipe rédigera un document sous WORD présentant :
   - Les différentes possibilités de sauvegarde et restauration des configurations des matériels d'interconnexion disponibles
   - Les commandes de base pour la mise en œuvre des sauvegardes et des restaurations
4) Chaque équipe rédigera un document sous WORD présentant :
   - La liste des différentes tâches à effectuer tant au niveau des STA que des matériels d'interconnexion. Une description sommaire accompagnera chaque tâche, un temps de mise en œuvre sera estimé
   - Un Gantt sera élaboré

Le chef de projet **de l'équipe D** participe et supervise à l'élaboration des documents conformément aux rôles définis en *annexe* E.

Annexe A - Schéma actuel de la M2L

Rappel de la structure réseau au sein de la M2L



Annexe B : Règles de gestion de l'affectation des ports aux niveaux des switch des baies

*Attention, **le rôle des ports désignés ci-dessous en gras et soulignés** sera le même pour toutes les tâches futures des étudiants de BTS SIO2 (SISR, PPE). Ces contraintes sont définies par les enseignants SISR du BTS SIO. Eux seuls sont à même de faire évoluer les règles.*

Au niveau des baies A à D

Chaque switch CISCO d'une baie sera organisé de la manière suivante :

- **les ports 1 et 2** seront toujours réservés pour les liaisons montantes vers la baie générale
- **les ports 3 et 4** seront toujours réservés pour les liaisons entre switch d'une même baie.
- **les ports 5 et 6** seront toujours réservés pour les liaisons entre switch et routeur d'une même baie
- Les ports 9 à 16 seront réservés pour le VLAN de cette mission.
- **Le dernier port** sera toujours réservé au VLAN de management.

Au niveau de la baie générale

Au niveau du switch CISCO de la baie générale, **les 8 premiers ports** seront réservés pour les liaisons descendantes vers les baies suivant ce tableau :

Baie Générale / Port switch →	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Baie A	1	2						
Baie B			1	2				
Baie C					1	2		
Baie D							1	2

Les 4 ports suivants [09 ; 12] seront toujours réservés pour les liens vers les routeurs
Les 4 ports suivants [13 ; 16] seront toujours réservés pour les serveurs d'entreprise
Le dernier port sera toujours réservé au VLAN de management (VLAN 128)

Remarque : l'affectation ne signifie pas obligatoirement brassage

Annexe C : Emplacement physique des locaux des ligues (extrait)

Ligue Athletisme (code L01) : Bâtiment C, 1 er étage, salles 101,102
Ligue Badminton (code L02) : Bâtiment C, 2 eme étage, salles 203,204
Ligue Canoe (code L03) : Bâtiment C, 3 eme étage, salles 305,306

Annexe D : Intégration des postes informatiques des ligues

Lorsque les ligues acquièrent du matériel informatique, il y a une phase obligatoire d'intégration qui consiste à paramétrer les noms des postes selon les règles de gestion suivantes :

B[code bâtiment]E[numéro étage]L[numéro ligue]S[numéro salle].P[numéro poste]
Code bâtiment qui peut être A ou C
N° étage est compris entre 1 et 4 (puisque les locaux du rez-de-chaussée n'hébergent pas de ligues)
N° ligue sur 2 chiffres : correspond à un nombre attribué à la ligue allant pour l'instant de 01 à 24
N° salle sur 2 chiffres : correspond aux bureaux occupés par les ligues
N° poste sur 2 chiffres : correspond au numéro écrit sur la prise murale

Exemple : le nom d'hôte BAE2L06S01P01 correspond au poste installé sur la prise N°1 du bureau A201 occupé par la ligue de Volley, bureau situé au deuxième étage du bâtiment A.

Annexe E : Rôles attribués au service informatique du cœur de réseau

Le Service Informatique gère le cœur de réseau. Il s'occupe de l'interconnexion entre les VLAN selon les contraintes définies en annexe. Lui **seul** sera amené à attribuer une adresse IP du VLAN 128. Il définira, via une note de service, une stratégie de sécurité d'accès aux matériels d'interconnexion. Cette note de service devra être validée par le DSI avant d'être transmise à l'administrateur réseau de chaque ligue qui sera ensuite chargé de son application. Un technicien du SI fera un suivi de l'affectation des adresses du VLAN 128 via une feuille Excel. Un tableau regroupera pour chaque nœud d'interconnexion le nom du dit matériel, son adresse IP, les identifiants de connexion. Les tables de routage InterVLAN seront définies.
A ce jour, les nœuds d'un VLAN de ligue sont autorisés à communiquer uniquement avec les autres nœuds de ce même VLAN et avec les serveurs situés au sein du service Informatique. Toute dérogation devra faire l'objet d'une demande auprès du SI via une note de service rédigée par l'administrateur de la ligue.