



## MISE EN PLACE D'UN DOMAINE ET DECOUPAGE DU RESEAU

Les structures hébergées sont toutes sur le même réseau. Cette solution à l'avantage d'être simple mais pose de nombreux soucis de sécurité, notamment du fait des personnes de passage dans les locaux de la M2L munies de matériels nomades et se connectant via le WIFI.

Une organisation basée sur les vlans va donc également être mise en œuvre.

Au niveau de l'accès WIFI, seule la borne sera paramétrée et la séparation des flux testée,

La téléphonie IP sera séparée des autres flux et bénéficiera par la suite d'un paramétrage pour la QoS, pour le moment seul le VLAN doit être créé et testé.

Il a été décidé de créer une nouvelle forêt et de migrer progressivement les services administratifs vers le nouveau domaine créé. Un nouveau serveur Windows Serveur 2025 hébergé sur un serveur PROXMOX (PVE latest) va donc être installé afin de gérer ce nouveau domaine. Cela s'accompagnera en même temps du remplacement du routeur principal.

### Outils à disposition

Les commutateurs CISCO sur lesquels sont connectés les prises murales sont dotés de la norme 802.1q et permettent notamment la création de VLAN par ports. Le numéro de VLAN est 100 pour les postes fixes, 200 pour les postes nomades et 300 pour la téléphonie IP. D'autres VLAN par la suite pourront être créés.

Le routeur choisi peut être un routeur Cisco. Le serveur WS2025 sur le PVE hébergera les services AD et DNS et DHCP. Vous vous assurez être en mesure d'administrer vos machines depuis vos postes d'administrateurs

### La mission

La mission consiste à mettre en œuvre la solution et à effectuer l'ensemble des tests.

Le domaine devant être créé est "m2lX.lan" où X représente le numéro de votre groupe. Des utilisateurs devront être créés pour chacune des trois ligues (basket, hand, volley). (voir fichier excel -> ListeUser.xlsx).

Les utilisateurs des ligues devront avoir en fond d'écran une image libre de droit en rapport avec leur sport et devront avoir **des droits limités** sur le poste pour des raisons de sécurité. Vous proposerez **les restrictions** à appliquer.

Les utilisateurs sont tous des membres de la structure de la M2L, certains sont en CDI, CDD et stagiaire, vous proposerez les évolutions nécessaires pour gérer les flux d'entrées et de sorties du personnel.

Par souci de sécurité, les données des utilisateurs ne devront pas être stockées sur le poste utilisateur.

Vous découvrirez des faiblesses et vulnérabilités sur votre serveur Active Directory en vous aidant de ressources Internet et vous donnerez des solutions pour limiter/contrer/éviter les conséquences/exploits possibles.

Chaque ligne devra disposer :

- D'un partage de groupe, pour lequel chacun a la possibilité d'écrire/lire/modifier mais ne peut pas supprimer.
- D'un partage global pour lequel seule la direction a un accès total.
- Les partages devront être montés automatiquement sur la session utilisateur.
- Les partages devront être accessibles hors ligne et devront disposer d'un système d'historisation.

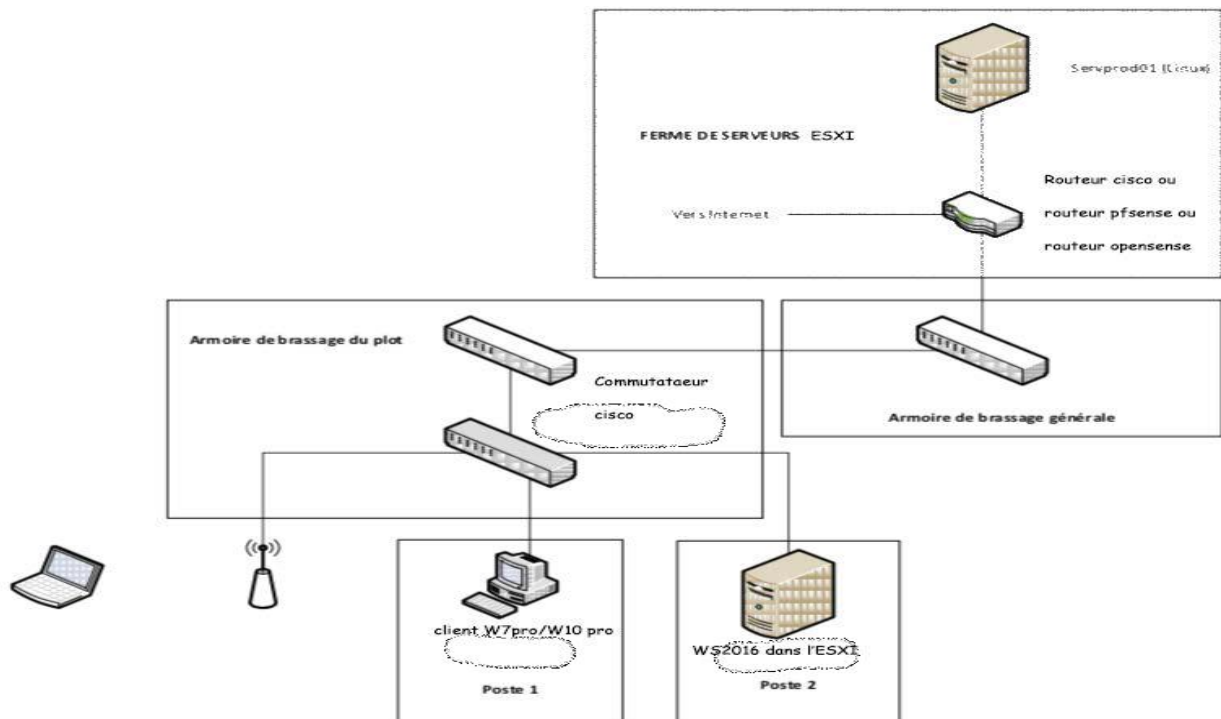
Le routeur sera installé pour la liaison Internet/dmz/lan.

Le service HTTPS situé sur le serveur de production de la DMZ doit être accessible à partir de l'URL :

<https://www.m2IX.lan> (à faire dans une autre mission)

La configuration du commutateur et du routeur devra être sauvegardée dans un dossier de partage accessible uniquement par les administrateurs sur le serveur WS2025 et sur un nextcloud.

La configuration physique suivante ressemble à cette mise en œuvre :



## Réception

### Étape 1 :

Avant de vous lancer dans la réalisation, vous préparerez un document texte présentant de manière détaillée les tâches techniques à réaliser et leur répartition entre les membres du groupe. Une prévision temporelle pour chaque tâche doit être prévue. Une présentation devra être faite oralement au professeur.

### Étape 2 :

La réception du projet consistera en une démonstration de la solution. La présentation inclura l'accès au réseau d'utilisateurs de postes fixes et de postes nomades, l'accès aux postes W10/W11 intégrés au domaine par des comptes d'utilisateurs du domaine, l'accès par URL au serveur HTTPS se trouvant sur le serveur de production depuis un poste fixe, la sauvegarde de la configuration du commutateur et routeur ainsi que les tests de séparation de flux entre les postes fixes, les postes nomades et la téléphonie IP.

Les documents d'accompagnement à rendre seront :

- Un plan du réseau détaillé sous Visio
- Une notice technique sur la mise en place des VLAN
- Une notice technique sur la sauvegarde externe de la configuration du switch.
- Un document récapitulatif sur les GPO utilisées, scripts mise en place et des configurations particulières réalisées sur les différents services.

Prochaine mission (AP3.3) le 04 Novembre 2025