

BTS SIO SISR 1

Atelier de professionnalisation (Projet 2)

Construit autour de

La Maison Des Ligues Lorraine (M2L)

REFONTE DE L'INFRASTRUCTURE RESEAU DE LA M2L

Professeurs impliqués dans ce projet :

- Younsi Mustapha/Mohamed Chernikh (Réseau)
- Mohammed Karroum (Système, Responsable des ateliers de professionnalisation)

Date d'émission : 06/05/2021

Important :

- Les questions éventuelles au sujet du présent projet doivent être formulées par courriel à l'attention de M KARROUM, en mettant en copie tous les formateurs qu'y sont impliqués.
- Les projets doivent être remis définitivement aux formats docx et pdf le **17 juin 2021 18h00, dernier délai.**
- La partie réseau sera simulée sous Packet Tracer 8.x
- La partie système sera virtualisée sous VirtualBox ou vmWare

Après avoir acquis des équipements informatiques dans le cadre des appels d'offres 1.1 et 1.2, l'infrastructure doit être à présent mise en place. Les trois serveurs vont être répartis comme suit :

- 1 serveur hébergeant les différentes VMs Windows
- 1 serveur hébergeant les différentes VMs en distribution Linux
- 1 serveur hébergeant les services FTP et WEB situé dans la DMZ (A mettre en place ultérieurement)

Les postes seront déployés auprès des ligues et des différents services de la M2L.

C'est l'objet de ce projet.

Partie 1 : Administration réseau (Mustapha Younsi/Mohamed Chernikh)

Contexte

La M2L est chargée d'offrir un service d'accès pour les ligues et pour ses services aux ressources hébergées comme aux ressources externes. L'accès aux ressources externes par les postes de travail doit être protégé afin d'empêcher toute intrusion non sollicitées provenant de l'extérieur.

M2L fournit de plus un accès aux ressources hébergées en interne pour les utilisateurs externes (exemple : accès à l'Intranet de réservation des salles, accès ftp, accès WEB, etc.).

Structure du réseau M2L

L'Infrastructure réseau

La structure générale du réseau comprend :

- Les sous réseaux de l'association M2L (VLANs)
- Les sous réseaux des ligues (VLANs)

Le réseau M2L héberge tous les serveurs dans une baie de serveurs installée dans le service Informatique. On y trouve un serveur d'annuaire, de fichiers, d'application, de supervision, gestion de parc informatique et d'incident, mais aussi les services DHCP, DNS, FTP, http, etc.

Plan d'adressage IP

Le réseau général est construit sur l'adresse 172.16.0.0 avec un masque de 19 bits. Ceci permet de couvrir l'ensemble du plan d'adressage et les évolutions du réseau par rapport au contexte de la M2L. L'administrateur a réservé un masque de 26 bits par sous réseau. Les sous réseaux couvrent les services de la M2L et les ligues par le plan d'adressage 172.16.X.0/26 (où X est le numéro du VLAN correspondant aux ligues et aux services de la M2L).

Le tableau en Annexe 1 décrit le plan d'adressage IP de l'ensemble du réseau, **qu'il faut compléter**. Ce plan d'adressage tient compte d'une exploitation des adresses IP en mode dynamique par deux serveurs DHCP (lire partie système).

Pour ce projet, l'administrateur vous demande de respecter les règles d'ingénierie suivantes :

- Pour chaque sous réseau les 12 adresses les plus hautes sont réservées pour les adresses fixes (172.16.X.51/26 à 172.16.X.62/26) La passerelle occupera l'adresse la plus haute.
- Le plan d'adresse IP du réseau général doit pouvoir couvrir les sous réseaux M2L et une capacité de 80 lignes qui est la capacité maximale admissible de l'infrastructure bâtiment de l'association.
- Le plan d'adresse IP sera administré par 2 serveurs DHCP qui assureront chacun la gestion d'une plage d'adresses propre. Si un serveur DHCP devient indisponible, l'autre serveur assurera la gestion de l'ensemble du parc pour chaque sous réseau. Il ne devra pas y avoir de duplication possible d'adresses IP. Pour des raisons de sécurité le bail DHCP sera ramené à 8 heures.
- Chaque sous réseau est déterminé par son numéro de VLAN dans le plan d'adressage général 172.16.0.0 /19 selon la règle : 172.16.x.0 /26 où x = Numéro de VLAN.

Un sous réseau est géré par 2 serveurs DHCP, hébergeant chacun la moitié de l'étendue des adresses basses, soit :

- 172.16.X.1 à 172.16.X.25 géré par le serveur DHCP exécutant Windows 2016 Server
- 172.16.X.26 à 172.16.X.50 géré par le serveur DHCP exécutant Debian 10 Server

Les éléments du réseau

Ce réseau regroupe les fonctions suivantes :

- Une structure de VLAN est utilisée pour les sous réseaux de la M2L. Cette structure permet de limiter les domaines de diffusion.
Les VLAN sont identifiés dans le plan d'adressage IP par le troisième octet qui prend pour valeur le N° du VLAN, ainsi le service Informatique est placé à l'adresse 172.16.2.0 /26 qui représente le VLAN 2 ou encore le VLAN 10 de la ligue Tennis 172.16.10.0/26.
- Le routage des VLAN utilise la technique des interfaces VLAN dans le commutateur de niveau 3 et l'encapsulation 802.1Q , implémentée dans les switch.

Nota : La maquette n'intègre que les 2 premiers VLAN de l'association M2L (Vlan INFORMATIQUE et administratif) et les 3 premières lignes (Tennis, Basket et Athlétisme)

Plan d'adressage IP

Vous préparerez et documenterez les données d'adressage IP pour chaque sous réseau sous forme d'un tableau qui comprendra l'adresse de réseau, masque, Broadcast, plage d'adresses utilisables, plage d'adresses fixes et adresse IP de passerelle.

Infrastructure de commutation

Chaque ligue est intégrée à un sous réseau dans un VLAN. La maquette comprend la ligue de Tennis, d'Athlétisme et la ligue de Basket avec 1 postes informatique par ligue au titre de poste client. La première ligue se verra attribuer le numéro de VLAN 10. Les ligues suivantes seront numérotées VLAN 11, VLAN 12 etc...

Pour l'installation vous prévoyez 10 ports par service sur le commutateur SW1M2L. Le commutateur des ligues SW2LIG hébergera les 2 premières ligues et SW3LIG la troisième avec 10 ports par ligues pour chacun.

La Mission

Dans ce contexte vous devez préparer le déploiement du réseau M2L qui comprendra les tâches suivantes :

- La préparation du plan d'adressage IP pour les départements M2L et les 3 premières ligues (Ligue de Tennis, Basket Ball et Athlétisme),
- Installation de l'infrastructure de commutation des Ligues et de M2L comme décrit dans le schéma général,
- Installation du réseau Backbone et des services réseau,
- Réalisation des tests et validation de la maquette

Chacune de ces phases sera planifiée et préparée dans un document qui comprendra un document projet, document technique de déploiement et cahier de recette.

Vous préparerez les documents nécessaires au déploiement de l'ensemble des sous réseaux (Ligues et M2L) qui comprendront :

- Le document de projet qui présentera l'organisation du projet, les phases de conception, de déploiement et de tests avec les délais de réalisation,
- Le document technique d'infrastructure qui décrira les fonctions installées avec les données de configuration, les fichiers de configuration, tableaux de brassage, choix des matériels et leurs caractéristiques techniques,
- Le document de recette qui présentera la liste des tests qui seront réalisés permettant de valider l'infrastructure.

Vous utiliserez des équipements réseau (routeurs et commutateurs de niveau 2 sous Packet Tracer pour la partie réseau) et des serveurs et postes virtualisés (sous VirtualBox ou vmWare).

Les équipements de réseau seront configurés en utilisant les lignes de commandes script CLI Cisco avec une configuration de base qui sécurisera l'accès aux CLI :

- Nommer les équipements,
- Crypter tous les mots de passe,
- Sécuriser par mot de passe enable
- Configurer l'accès à distance Telnet,
- Les ports d'accès des switch seront configurés pour invalider le processus spanning-tree

Le login Telnet est **admin**, mot de passe **admin** et le mot de passe enable est **cisco**.

La mission sera réalisée en final sur site par des techniciens d'intervention et il est par conséquent important de préparer tous les documents d'installation nécessaires à la bonne conduite du projet :

- document de projet qui décrira les différentes tâches, les actions à mener pour la réalisation, le planning pour chaque action et pour chaque tâche. Vous détaillerez les charges en Homme/jour, les livrables et les phases de validation/livraison.
- documentations techniques des équipements (description technique, liste du matériel, document de câblage)
- tableaux d'adressage, tableaux de brassage, fichiers de configuration.
- Cahier de recette, couverture de tests.

Partie 2 : Administration système (Mohammed KARROUM)

Le contexte

L'une des préoccupations de l'administrateur de la Maison des Ligues consiste à offrir un service de qualité dans un temps raisonnable aux différents services de la M2L et aux différentes ligues. Afin d'optimiser sa charge de travail et de répondre rapidement aux sollicitations des responsables des ligues et des services, il opte pour l'automatisation de certaines tâches administratives.

Les objectifs à atteindre consistent :

- Mission 2.1 : Migration du réseau vers une architecture client / serveur de type domaine

L'architecture réseau actuel de la M2L n'offre pas une meilleure organisation du réseau et ne permet pas de centraliser l'administration et une meilleure gestion de la sécurité.

Comme dit précédemment, cette migration système s'inscrit dans la refonte du réseau après les appels d'offres 1.1 et 1.2. Elle accompagne ainsi la nouvelle architecture réseau en annexe 1. Le réseau de la M2L et des ligues va comporter plusieurs périmètres de sécurité :

- chaque service et chaque ligue sera organisé en VLAN
- la DMZ qui sera créée dans un sous réseau sera étudiée ultérieurement.

Au niveau de l'Active Directory, chaque VLAN se traduira par une unité d'organisation qui contiendra tous les objets de la ligue ou du service : groupes, utilisateurs, ordinateurs, imprimantes, etc.

La mission consiste donc à créer le domaine (m2l.lan) sur un serveur exécutant Windows 2016/19 R2 server et d'y créer les différents services et ligues.

- Mission 2.2 : Création de l'environnement utilisateur par script à partir d'une feuille Excel

La mission consiste à automatiser la création de l'environnement pour chaque utilisateur d'une ligue. Lors de l'installation d'une ligue, l'administrateur de la M2L communique un fichier Excel au responsable de la ligue, lui permettant par la suite d'organiser les utilisateurs, les ressources et de fixer les niveaux d'accès et les quotas sur disque dur. La structure de la fiche Excel est donnée ci-après (laquelle peut être adaptée au besoin). Elle constitue un modèle de référence pour le script.

On entend ici par environnement utilisateur ce qui suit :

- création de l'utilisateur (login, mot de passe, etc.)
- son appartenance au groupe

- son profil itinérant
- les dossiers auxquels il pourrait accéder en réseau
- son dossier personnel dans lequel il stockera ses travaux
- son quota disque concernant le stockage de ses données
- les autorisations dont il bénéficie pour accéder aux différentes ressources

Structure de la fiche Excel

Nom	Prénom	Login	Mot de passe	Quota	Seuil Quota	Accès	Etc.

Il est important de noter les contraintes suivantes :

- Le login sera généré à partir des nom et prénom de l'utilisateur, par une formule Excel. Il obéit à la syntaxe suivante : **<premier caractère du prénom>.<nom>**. Pour Sylvie Dupont, on obtiendra : **s.dupont** (tout en minuscule).
- Le mot de passe sera généré par une macro Excel, conformément à la stratégie de sécurité des mots de passe requise par le système d'exploitation. Il pourrait être modifié par l'utilisateur à la première ouverture de session. Il sera généré à partir d'une chaîne de caractères composée de : **abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !?@.**
- La longueur du mot de passe doit être supérieure ou égale à 10 caractères.

Remarque : Le nombre de colonnes Excel peut être étendu pour des raisons administratives. Les objets utilisateurs, groupes, unités d'organisation seront inscrits dans l'annuaire Active Directory moyennant les commandes LDAP.

- Mission 2.4 : Mise en place de serveurs DHCP redondants

Documents à exploiter : Annexes 1 et 2.

Afin d'automatiser l'attribution des adresses IP, il a été décidé de mettre en place deux serveurs DHCP redondants par fractionnement de l'étendue. D'après les informations recueillies, un service de la M2L ou une ligue comporte au maximum 25 ordinateurs. Ainsi, une étendue de 25 adresses sera, pour l'instant, largement suffisante.

Le serveur DHCP1 cohabitera avec le serveur-contrôleur de domaine. Il hébergera la première moitié de l'étendue d'un VLAN, soit :

Adresse début : 172.16.X.1
 Adresse fin : 172.16.X.25

Le serveur DHCP2 sera installé sur une distribution Linux (Debian). Il hébergera la seconde moitié de l'étendue d'un VLAN, soit :

Adresse début : 172.16.X.26

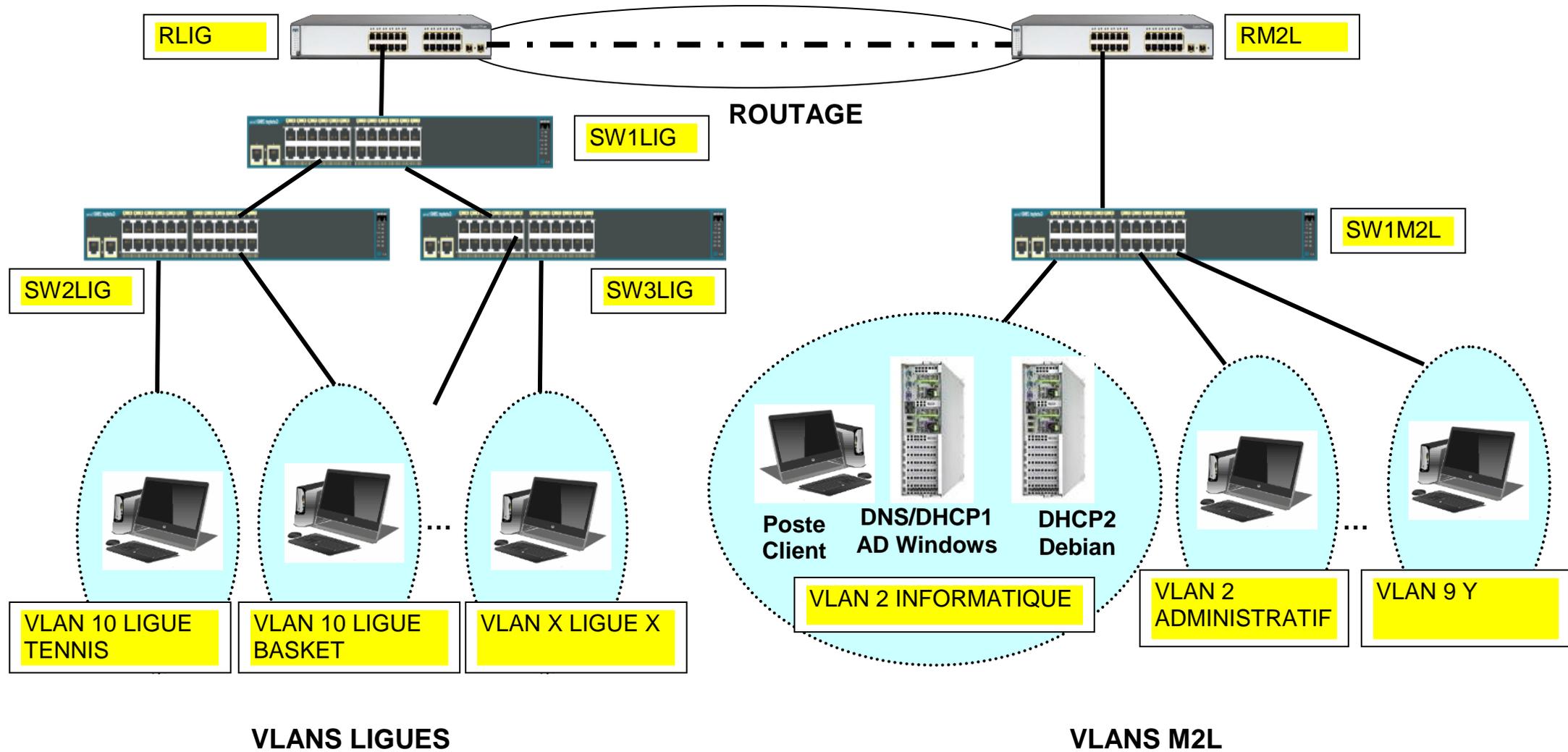
Adresse fin : 172.16.X.50

Les serveurs DHCP doivent fournir tous les paramètres réseau nécessaires aux clients DHCP.

Pour chaque mission, il vous est demandé de rédiger une documentation technique présentant les outils et les logiciels mis en œuvre, la méthodologie employée ainsi que les tests prévus pour valider le service tout en mentionnant l'impact résultant de l'intégration du nouveau service au sein du réseau.

ANNEXE 1 : SCHEMA DE L4INFRASTRUCTURE

@IP SOUS R2SEAU : 172.16.X.0/26 OU X REPRESENTE LE NUMERO DU VLAN DESIGNE
NB : LE VLAN 1 EST EN GENERAL RESERVE A L'ADMINISTRATION ; IL N'EST DONC PAS UTILISE



ANNEXE 2 - PLAN D'ADRESSAGE

VLAN M2L	VLAN 2 INFORMATIQUE	VLAN 3 ADMINISTRATIF	VLAN 4 DIR GENERALE	VLAN 5 COMMERCIAL	VLAN 6 JURIDIQUE	VLAN 6 RESSOURCES
Masque						
Adresse du réseau						
Adresse Bdcast						
Plage adresse DHCP1						
Plage adresse DHCP2						
Plage fixe						
Serveurs DHCP						
Passerelle						

VLAN LIGUES	TENNIS VLAN10	ATHLE VLAN11	BASKET VLAN12	----	----	LIGUE N VLAN N
Masque						
Adresse du réseau						
Adresse Bdcast						
Plage adresse DHCP1						
Plage adresse DHCP2						
Plage fixe						
Passerelle						

Plan d'adressage des serveurs physiques

Machine Hôte	Nom	VM	Adresse IP	Masque	passerelle
VIRT1-WIN 172.16.2.51 /26	AD-DHCP1	AD, DNS, DHCP1	172.16.2.61	255.255.255.192	172.16.2.62
VIRT2-LIN 172.16.2.52 /26	DEB-DHCP2	DHCP2, PROXY	172.16.2.60	255.255.255.192	172.16.2.62
	NAG-EON	NAGIOS/EON	172.16.2.56	"	"

ANNEXE 3 - PLAN DE BRASSAGE

Le plan de brassage consiste faire du câblage des équipements réseau

Brassage switchs ligues / M2L

A dresser par vos soins dans un tableau

Brassage Routeurs

A dresser par vos soins dans un tableau