

N°candidat : 02045677973
TARASSE Saossane

EPSI Montpellier
BTS SIO SISR 2024/2025

Epreuve E6
Situation N°1

Segmentation du réseau

Mise en place des VLANS sur le coeur du réseau

Table de matière:

Contexte: Maison des Ligues de Lorraine	3
Besoins	3
Objectifs du projet	4
Choix Techniques:	5
Avantages:	5
Inconvénients:	5
Matériels:	5
Explication de la solution proposée:	6
Configuration des bridges sur Proxmox	8
Configuration des VLANs sur PfSense	10
Configuration des VLANs sur les commutateurs HP 1820-8G	14
Conclusion	16
Annexe	17

Contexte: Maison des Ligues de Lorraine

La Maison des Ligues de Lorraine (M2L) est un établissement sous l'égide du Conseil Régional de Lorraine, ayant pour mission principale d'assurer la gestion et le support des ligues sportives régionales ainsi que d'autres structures hébergées.

Afin de garantir un fonctionnement optimal et sécurisé, la M2L met à disposition des infrastructures adaptées, incluant des ressources matérielles et logistiques, permettant aux ligues de bénéficier d'un environnement stable et performant.

Dans cette optique, la M2L souhaite moderniser et centraliser la gestion de son infrastructure informatique. Cette modernisation vise à simplifier l'administration des utilisateurs, la gestion des adresses IP et le déploiement d'applications au sein de son réseau.

En adoptant une solution intégrée et automatisée, la M2L aspire à renforcer la sécurité, optimiser la gestion des accès et faciliter l'organisation des ressources informatiques pour les ligues sportives qu'elle héberge.

Besoins

- Séparer les flux réseaux des différentes **ligues sportives hébergées**.
- Isoler les **services administratifs** internes de la M2L.
- Prévoir un VLAN pour les **visiteurs ou intervenants externes**.

Sécurité et contrôle d'accès

- Éviter que des utilisateurs non autorisés accèdent à des ressources critiques.
- Permettre uniquement la communication intra-VLAN
- Filtrage des communications selon le rôle.

Optimisation du trafic réseau

- Réduire les domaines de broadcast.
- Améliorer la performance réseau en isolant les communications inutiles entre différents services.

Facilité de gestion et évolutivité

- Simplifier le **déploiement d'applications** en les affectant à des VLAN spécifiques (ex: GLPI sur VLAN 20)
- Centraliser la **gestion IP** avec un plan d'adressage structuré par VLAN.

Objectifs du projet

Ce projet vise à améliorer la gestion et la segmentation du réseau en mettant en place des VLANs sur le cœur du réseau de l'organisation. L'objectif est de renforcer la sécurité, optimiser les performances et assurer une meilleure administration des ressources réseau.

Segmentation du réseau à l'aide de VLANs pour isoler les différents services et améliorer la sécurité.

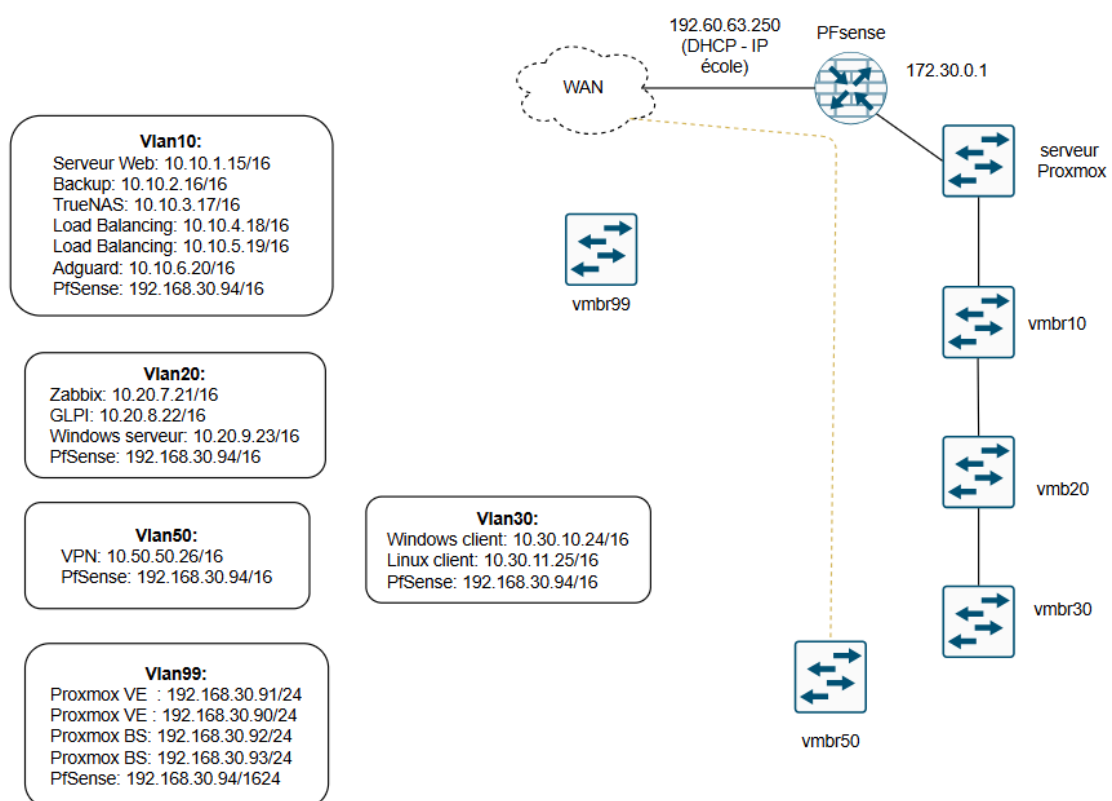
Configuration des switches pour assurer l'interconnexion des VLANs et le routage adéquat.

Mise en place du routage inter-VLAN pour permettre la communication entre les différents segments du réseau via un routeur ou un firewall.

Attribution dynamique des adresses IP via DHCP en fonction des VLANs.

Sécurisation du réseau avec des ACLs (Listes de contrôle d'accès) et le filtrage des accès.

Gestion centralisée des équipements réseau à travers une solution d'administration adaptée.



Choix Techniques:

Avantages:

Isolation des services: Les VLANs séparent les flux réseau empêchant les appareils du VLAN 10 de communiquer directement avec le VLAN 20. Ce qui permet d'éviter la propagation des menaces.

Réduction de broadcast: La création de VLANs va permettre une amélioration des performances en réduisant les domaines de broadcast. Autrement dit, les portes du switch ne seront pas inondées de messages. Tous les appareils qui sont connectés sur le même réseau local, plus précisément ceux qui partagent le même segment IP, ne recevront pas les messages des autres appareils qui ne sont pas dans le même domaine de diffusion.

Gestion centralisée: Permet un déploiement homogène des politiques de sécurité.

Inconvénients:

Configuration: Une mauvaise configuration des liens **trunks** peut bloquer le trafic VLAN.

VLAN 1 (VLAN par défaut) transporte les trames non taguées ce qui crée un risque si un attaquant se connecte.

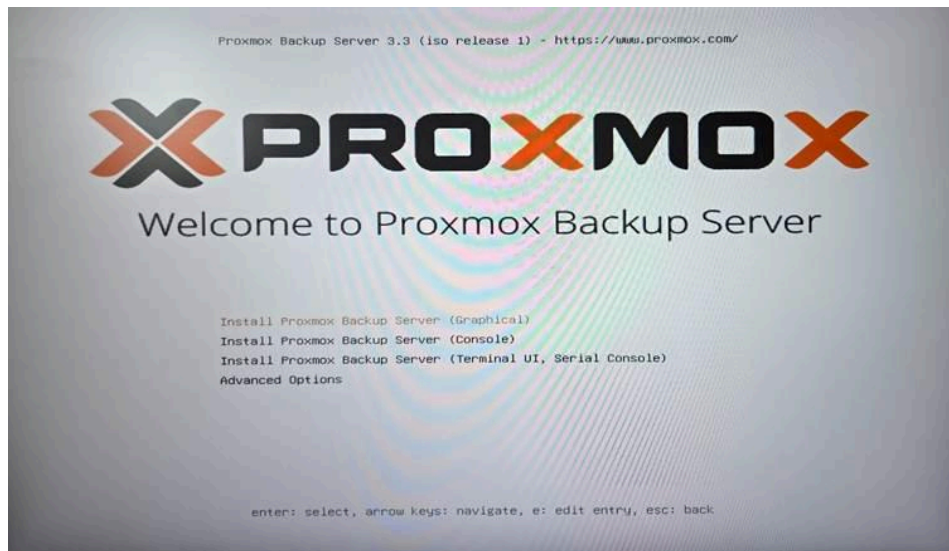
Un port configuré en mode access (sans tag) au lieu de trunk (tagué) bloque le trafic inter-vlan.

Matériels:

- 2 commutateurs HP 1820-8G
- 4 serveurs Asus Pro Q570M
- Proxmox v 8.2

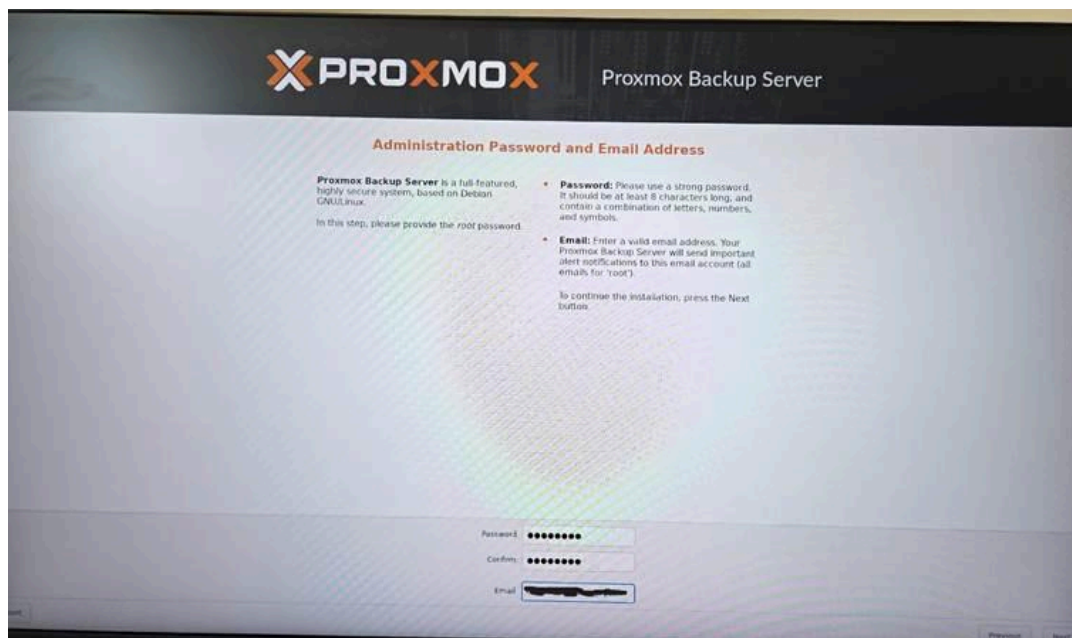
Explication de la solution proposée:

Installation Proxmox Backup server:

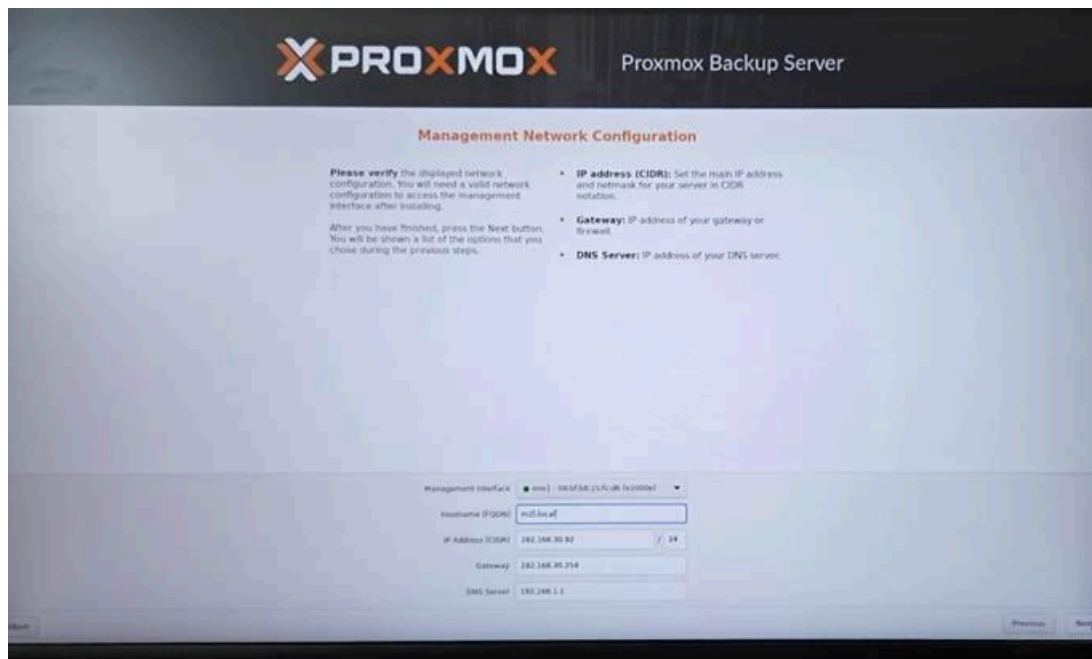


Pour cette installation j'ai choisi de prendre « **Install Proxmox Backup Server (Graphical)** », car plus simple et rapide.

On choisit un disque ou une machine qu'on souhaite avoir en backup.



Nous choisissons un mot de passe avec une adresse mail qui nous servira pour le serveur backup qui nous enverra diverses notifications importantes.



On choisi l'adresse IP la dans ce cas nous allons prendre, **192.168.30.92/24**, avec une Gateway **192.168.30.254** ainsi qu'un DNS **192.168.1.1**

Une fois l'installation terminée, un message s'affiche pour confirmer la réussite de l'installation avec également l'adresse IP de notre Proxmox à savoir 192.168.30.92:8007

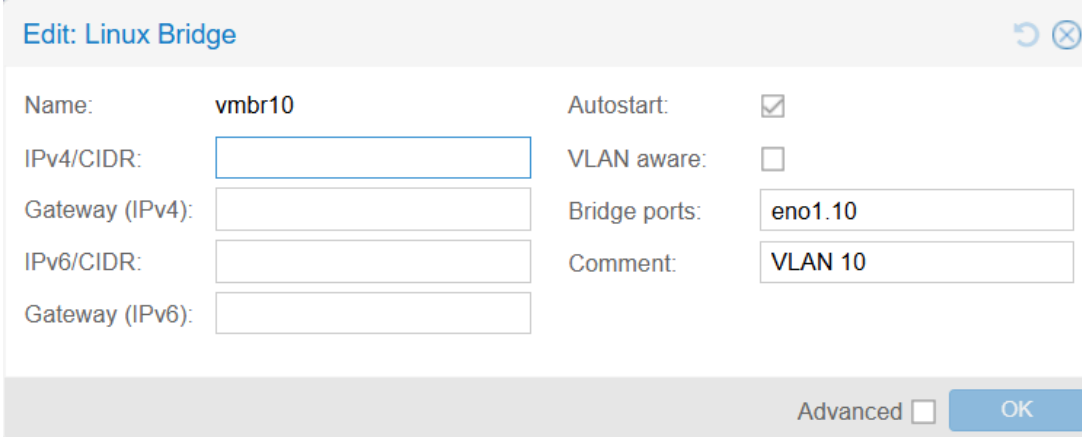
Configuration des bridges sur Proxmox

Les VLANs servent à segmenter et organiser des machines de façon flexible et sécurisée. Les vmbr agissent comme des commutateurs virtuels.

En associant un VLAN spécifique à un vmbr, on permet à chaque VM de rejoindre le bon segment réseau.

Pour faciliter la gestion, nous avons associé un VLAN 10 à un vmbr10, un VLAN 20 à un vmbr20 et ainsi de suite. De cette façon, on simplifie l'identification et la gestion des VLAN.

Le bridge permet de relier des VM entre elles et/ou au réseau physique via une interface physique ou un VLAN.



The screenshot shows the 'Edit: Linux Bridge' configuration window in Proxmox. The window has a title bar with a refresh icon and a close button. The configuration fields are as follows:

Field	Value
Name:	vmbr10
IPv4/CIDR:	
Gateway (IPv4):	
IPv6/CIDR:	
Gateway (IPv6):	
Autostart:	<input checked="" type="checkbox"/>
VLAN aware:	<input type="checkbox"/>
Bridge ports:	eno1.10
Comment:	VLAN 10

At the bottom right, there is an 'Advanced' checkbox (unchecked) and an 'OK' button.

Sur l'interface web de Proxmox, nous allons créer des “**Linux Bridge**” que l'on va associer au VLAN.

Ici le bridge se nomme vmbr10, ce qui indique que ce bridge est dédié au VLAN 10.

Le champ **IP** est ici vide, ce qui signifie que le bridge n'a pas d'IP attribuée sur le serveur.

Cette pratique sert à isoler le réseau des VM de Proxmox renforçant la sécurité.

Il n'est pas nécessaire de configurer une IP ici. En cochant la case 'VLAN aware', le bridge héritera automatiquement de l'IP définis au niveau du VLAN.

L'**autostart** est coché ce qui signifie que le bridge sera activé automatiquement dès le démarrage du serveur.

L'option **VLAN aware** n'est pas activée, ce qui signifie que le bridge ne gère pas plusieurs VLANs, il est dédié à un seul VLAN.

Le “**Bridge ports**” est ici connecté sur l’interface réseau eno1.10 qui est une sous-interface de l’interface physique eno1. Cette sous-interface est configurée pour transporter uniquement le trafic du VLAN 10 (tagué 10). Ce qui signifie que tout trafic entrant ou sortant par ce bridge sera automatiquement tagué/dé-tagué pour le VLAN 10.

Nous réalisons la même procédure pour les VLANs suivants.

	Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
Summary	eno1	Network Device	Yes	No	No					
Notes	enp1s0f0	Network Device	No	No	No					
Shell	enp1s0f1	Network Device	No	No	No					
System	enp3s0	Network Device	No	No	No					
Network	enp4s0	Network Device	No	No	No					
Certificates	enp5s0	Network Device	No	No	No					
DNS	vmbr0	Linux Bridge	Yes	Yes	No	eno1		192.168.30.90/24	192.168.30.254	
Hosts	vmbr10	Linux Bridge	Yes	Yes	No	eno1.10				VLAN 10
Options	vmbr20	Linux Bridge	Yes	Yes	No	eno1.20				VLAN 20
Time	vmbr30	Linux Bridge	Yes	Yes	No	eno1.30				VLAN 30
System Log	vmbr50	Linux Bridge	Yes	Yes	No	eno1.50				VLAN 50
	vmbr99	Linux Bridge	Yes	Yes	No	eno1.99		10.99.1.1/16		VLAN 99

Tous les **vmbr** doivent bien être **activés**. On vérifie que chaque vmbr est associé au bon vlan et au bon port.

Les **interfaces physiques** présentes sur le serveur sont **inactives** sauf si elles sont utilisées par un bridge. eno1 est le seul utilisé.

Le **vmbr0** est le **bridge principal**, connecté à l’interface physique **eno1**. Celle-ci a une adresse IP et une passerelle car c’est l’interface d’administration de Proxmox. Elle permet à l’hôte d’être accessible sur ce réseau.

Tous les **bridges** sont dédiés à des VLANs spécifiques, chacun connecté à une sous-interface de eno1. Ils n’ont pas **d’adresses IP**, ce qui signifie que l’hôte n’est pas accessible sur ces réseaux.

Cependant le **vmbr99** possède une adresse IP pour permettre à **Proxmox** d’être actif sur le réseau VLAN 99.

Configuration des VLANs sur PfSense

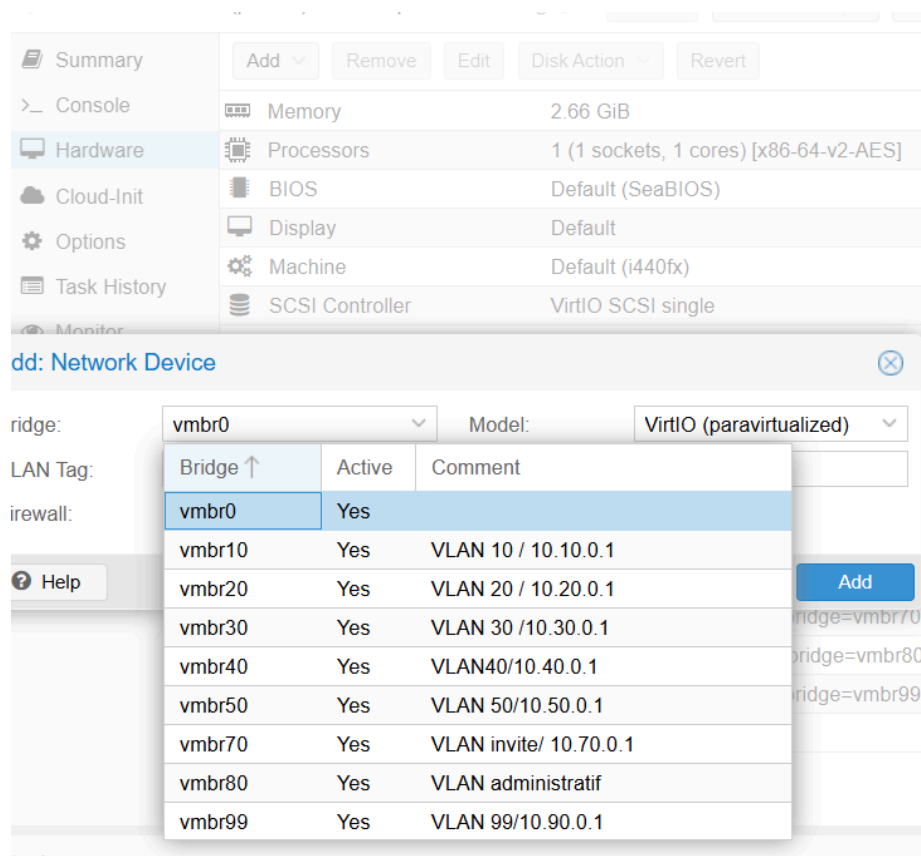
Configurer des VLAN sur PfSense permet de segmenter et sécuriser un réseau de manière souple et efficace, tout en centralisant la gestion et le contrôle du trafic entre les différents segments.

Ici PfSense agit comme un pare-feu pour tous les VLANs. On peut appliquer des règles d'accès et de filtrage très fines entre les différents réseaux.

Nous allons configurer une VM cliente Windows et une VM PfSense pour avoir accès à l'interface web.

Une fois sur l'interface web, nous allons créer nos VLANs en allant sur "interfaces", "Assignements", "VLAN".

Afin de bien configurer nos VLANs, nous devons entrer une adresse MAC que nous devons d'abord créer sur l'interface Proxmox.



Nous allons créer une adresse MAC sur la VM PfSense dans la fonctionnalité Hardware en ajoutant une nouvelle interface, on sélectionne le VLAN que l'on souhaite configuré sur PfSense.

Summary	Add Remove Edit Disk Action Revert	
Console	Memory	2.66 GiB
Hardware	Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]
Cloud-Init	BIOS	Default (SeaBIOS)
Options	Display	Default
Task History	Machine	Default (i440fx)
Monitor	SCSI Controller	VirtIO SCSI single
Backup	Hard Disk (scsi0)	VM:vm-300-disk-0,iothread=1,size=32G
Replication	Network Device (net0)	virtio=BC:24:11:79:1B:AA,bridge=vmbr0
Snapshots	Network Device (net1)	virtio=BC:24:11:A3:E4:53,bridge=vmbr10
Firewall	Network Device (net2)	virtio=BC:24:11:18:03:1D,bridge=vmbr20
Permissions	Network Device (net3)	virtio=BC:24:11:45:02:B3,bridge=vmbr30
	Network Device (net4)	virtio=BC:24:11:EB:F1:8D,bridge=vmbr40
	Network Device (net5)	virtio=BC:24:11:90:F5:D6,bridge=vmbr50
	Network Device (net6)	virtio=BC:24:11:95:2F:0E,bridge=vmbr70
	Network Device (net7)	virtio=BC:24:11:FA:E5:7A,bridge=vmbr80
	Network Device (net8)	virtio=BC:24:11:55:AB:4F,bridge=vmbr99
	Unused Disk 0	local-lvm:vm-300-disk-0

Une adresse MAC va donc être attribuée. C'est celle-ci que nous allons devoir sélectionner sur notre interface PfSense.

Par exemple, nous allons créer le VLAN 5.

Pour cela nous allons créer sur l'interface de Proxmox l'adresse MAC du VLAN.

Add: Network Device

Bridge:

vmbr0

Model:

VirtIO (paravirtualized)

VLAN Tag:

Firewall:

Help

Device (net6)

Device (net7)

Device (net8)

Disk 0

Bridge ↑

Active

Comment

vmbr0

Yes

vmbr10

Yes

VLAN 10 / 10.10.0.1

vmbr20

Yes

VLAN 20 / 10.20.0.1

vmbr30

Yes

VLAN 30 / 10.30.0.1

vmbr40

Yes

VLAN40/10.40.0.1

vmbr5

Yes

test

vmbr50

Yes

VLAN 50/10.50.0.1

vmbr70

Yes

VLAN invite/ 10.70.0.1

vmbr80

Yes

VLAN administratif

vmbr99

Yes

VLAN 99/10.90.0.1

Add

1e

Description

Nous allons bien noter l'adresse MAC afin de ne pas se tromper au moment de configurer le VLAN sur l'interface de PfSense.

⇌ Network Device (net9) virtio=BC:24:11:E4:85:41,bridge=vibr5,firewall=1

Sur l'interface PfSense, nous allons aller dans "interfaces", "Assignements", "VLANs".

Parent Interface	VLAN Tag	VLAN Priority	Description
vtnet9 (bc:24:11:e4:85:41)			
vtnet0 (bc:24:11:79:1b:aa) - wan			
vtnet1 (bc:24:11:a3:e4:53) - opt1			
vtnet2 (bc:24:11:18:03:1d) - opt2			
vtnet3 (bc:24:11:45:02:b3) - lan			
vtnet4 (bc:24:11:eb:f1:8d) - opt3			
vtnet5 (bc:24:11:90:f5:d6) - opt4			
vtnet6 (bc:24:11:95:2f:0e) - opt5			
vtnet7 (bc:24:11:fa:e5:7a) - opt6			
vtnet8 (bc:24:11:55:ab:4f) - opt7			

Save

On va sélectionner la bonne adresse MAC, nommer notre VLAN et enregistrer. Afin d'activer le VLAN, nous allons aller dans "interfaces", "Assignements"

VLANs

vtnet9 (bc:24:11:e4:85:41)

Sélectionné vtnetx puis ajouté.

Nous allons maintenant configurer l'interface. En description, nous allons ajouter le nom du VLAN. Mettre l'IPv4 en static. Dans notre cas nous allons mettre comme IP, 10.5.0.1/16. Nous allons activer l'interface en cochant la case du haut.

Interfaces / OPT8 (vtnet9.5)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex fo

Static IPv4 Configuration

IPv4 Address /

Enregistrer et appliquer les changements.

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

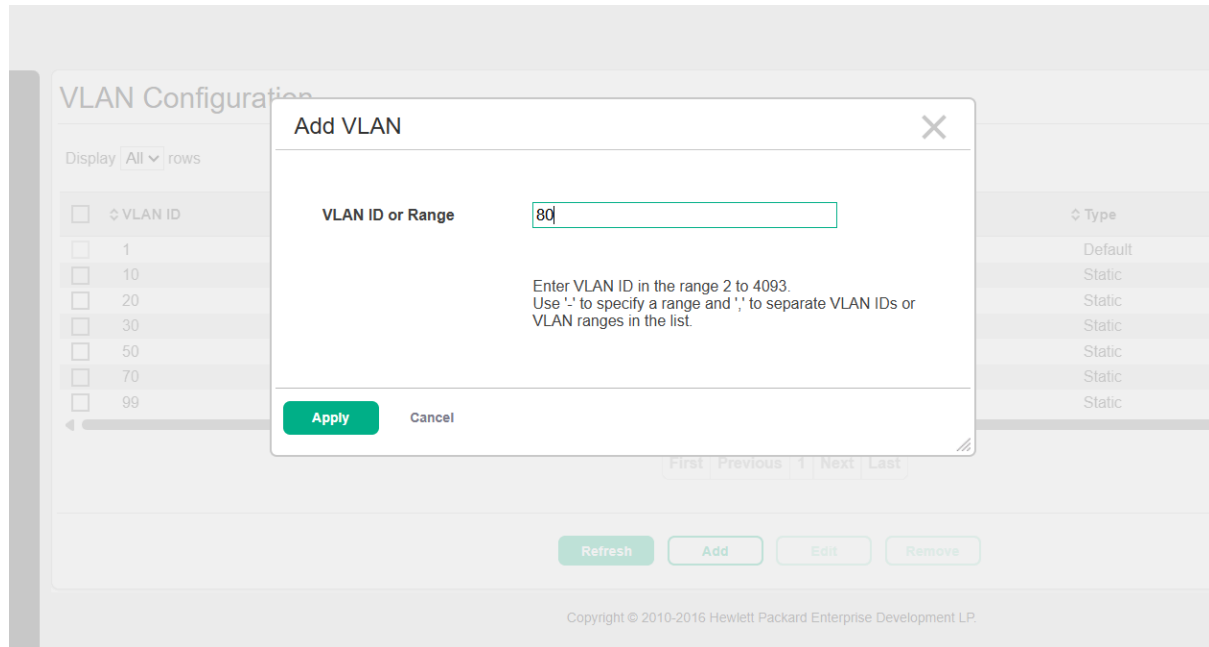
Interface	Network port	
WAN	<input type="text" value="vtnet0 (bc:24:11:79:1b:aa)"/>	
VLAN30	<input type="text" value="vtnet3 (bc:24:11:45:02:b3)"/>	<input type="button" value="Delete"/>
VLAN10	<input type="text" value="vtnet1 (bc:24:11:a3:e4:53)"/>	<input type="button" value="Delete"/>
VLAN20	<input type="text" value="vtnet2 (bc:24:11:18:03:1d)"/>	<input type="button" value="Delete"/>
VLAN50	<input type="text" value="vtnet4 (bc:24:11:eb:f1:8d)"/>	<input type="button" value="Delete"/>
VLAN99	<input type="text" value="vtnet5 (bc:24:11:90:f5:d6)"/>	<input type="button" value="Delete"/>
VLAN40	<input type="text" value="vtnet6 (bc:24:11:95:2f:0e)"/>	<input type="button" value="Delete"/>
VLAN70	<input type="text" value="vtnet7 (bc:24:11:fa:e5:7a)"/>	<input type="button" value="Delete"/>
VLAN80	<input type="text" value="vtnet8 (bc:24:11:55:ab:4f)"/>	<input type="button" value="Delete"/>
VLAN5	<input type="text" value="vtnet9 (bc:24:11:e4:85:41)"/>	<input type="button" value="Delete"/>
Available network ports:	<input type="text" value="ovpn3 (Accès distant OpenVPN)"/>	<input type="button" value="Add"/>

Nous vérifions une dernière fois nos configurations, si nous avons bien attribuer les adresses MAC au bon VLAN et on enregistre.

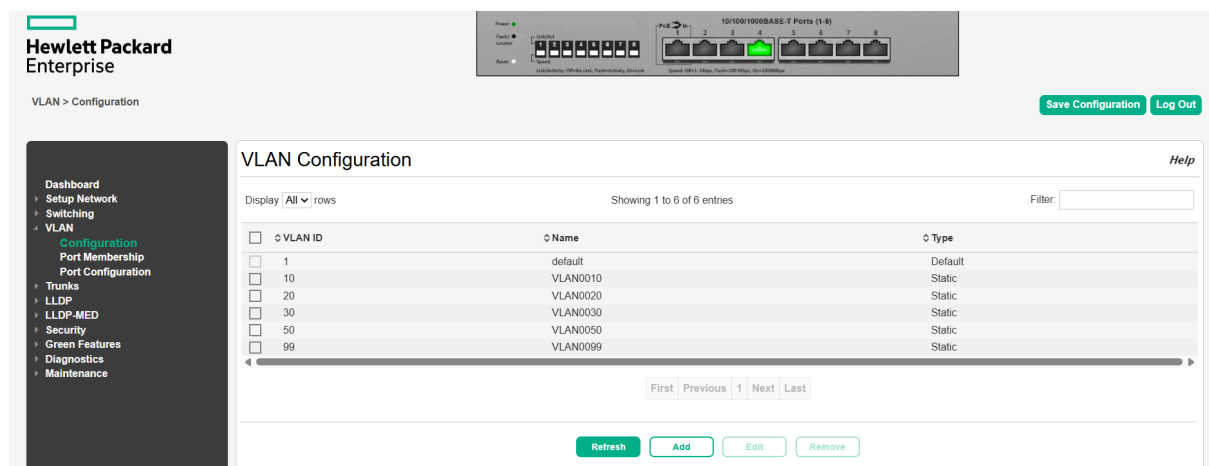
Configuration des VLANs sur les commutateurs HP 1820-8G

Nous allons dans un premier temps créer tout nos VLANs

Exemple: Création du VLAN 80



Nous allons vérifier que tous nos VLANs sont créés avant de les configurer.



Pour configurer des VLANs sur des commutateurs nous avons besoin de “tagged” ou de “untagged” selon les besoins.

Un lien trunk est nécessaire pour faire passer plusieurs VLANs sur un même câble.

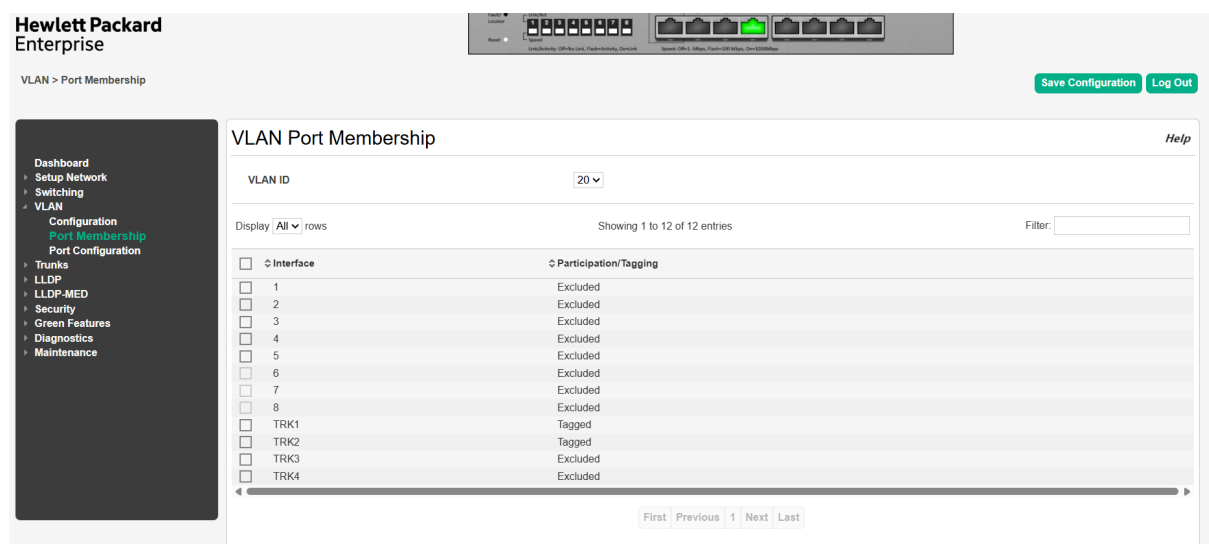
Tagged signifie que le port va transmettre les trames de ces VLANs en ajoutant une étiquette (un tag 802.1Q) qui indique à quel VLAN chaque trame appartient.

Ce procédé est utilisé lors du routage pour transporter plusieurs VLANs sur un même lien, avec des tags pour les identifier.

Cependant, parfois des trames arrivent sans étiquette, dites « **non-tagguées** » ou « **untagged** » : le switch va les placer automatiquement dans le VLAN natif (par défaut), généralement le VLAN 1.

Le VLAN natif sert à ranger automatiquement le trafic qui circule sur le trunk sans étiquette, pour qu'il ne soit pas perdu et soit bien traité sur le réseau.

Ce procédé est utilisé au moment de transmettre l'information d'un VLAN en particulier.



Hewlett Packard Enterprise

VLAN > Port Membership

Save Configuration Log Out

VLAN Port Membership

VLAN ID: 20

Display: All rows Showing 1 to 12 of 12 entries Filter:

Interface	Participation/Tagging
1	Excluded
2	Excluded
3	Excluded
4	Excluded
5	Excluded
6	Excluded
7	Excluded
8	Excluded
TRK1	Tagged
TRK2	Tagged
TRK3	Excluded
TRK4	Excluded

First Previous 1 Next Last

Nous allons toujours « **tagger** » les TRK1 et TRK2, qui sont les **agrégations de liens** que nous avons créées (cf. doc LACP), car nous avons besoin que l'information que nous voulons envoyer soit envoyée sur le bon VLAN et, pour cela, les commutateurs doivent communiquer entre eux pour distribuer les trames au bon port.

Exactement la même configuration doit être faite sur les deux commutateurs.

Conclusion

La mise en place des VLANs au sein de l'infrastructure réseau de la Maison des Ligues de Lorraine a permis d'apporter une segmentation claire, sécurisée et adaptée aux besoins spécifiques des différents services hébergés.

A l'aide des outils comme Proxmox, PfSense et les commutateurs HP 1820-8G, on a pu segmenter efficacement le réseau, ce qui a contribué à une meilleure isolation des flux, une réduction des risques de sécurité et une optimisation des performances globales du réseau.

L'utilisation de ports « tagged » sur un lien trunk permet d'identifier précisément chaque VLAN lors du transport de plusieurs réseaux virtuels sur un même câble, assurant ainsi la séparation et la gestion efficace des flux réseau entre les commutateurs

Annexe

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 01				
Nom, prénom : Saossane TARASSE		N° candidat : 0204567797 3				
<input checked="" type="checkbox"/> Épreuve ponctuelle	<input type="checkbox"/> Contrôle en cours de formation	Date :				
Organisation support de la réalisation professionnelle La Maison des Ligues de la Lorraine, établissement du Conseil Régional de Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées. Elle assure l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région. M2L souhaite mettre en place une solution pour segmenter son réseau						
Intitulé de la réalisation professionnelle Mise en place des VLANS sur le coeur du réseau						
Période de réalisation : 23/09/2024 - 19/11/2024		Lieu : EPSI MONTPELLIER				
Modalité : <input type="checkbox"/> Seul <input checked="" type="checkbox"/> En équipe						
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau						
Conditions de réalisation ¹ (ressources fournies, résultats attendus) <table border="0"> <tr> <td>Ressources fournies :</td> <td>Résultats attendus :</td> </tr> <tr> <td> <ul style="list-style-type: none"> • Cahier des charges M2L • Serveur Asus Pro Q570M • Proxmox VE 8.2 • Switch D-link x2 </td> <td> <ul style="list-style-type: none"> • segmentation de réseau • sécurisation des accès </td> </tr> </table>			Ressources fournies :	Résultats attendus :	<ul style="list-style-type: none"> • Cahier des charges M2L • Serveur Asus Pro Q570M • Proxmox VE 8.2 • Switch D-link x2 	<ul style="list-style-type: none"> • segmentation de réseau • sécurisation des accès
Ressources fournies :	Résultats attendus :					
<ul style="list-style-type: none"> • Cahier des charges M2L • Serveur Asus Pro Q570M • Proxmox VE 8.2 • Switch D-link x2 	<ul style="list-style-type: none"> • segmentation de réseau • sécurisation des accès 					
Description des ressources documentaires, matérielles et logicielles utilisées ² <ul style="list-style-type: none"> • Schéma réseau M2L, tableau des VLANS • Documentation d'installation et configuration de Proxmox VE • Documentation d'installation et configuration de switch 						
Modalités d'accès aux productions ³ et à leur documentation Lien de production : https://skullburn84.github.io/Portfolio/documentation.html Lien de documentations : <ul style="list-style-type: none"> • VLAN : https://skullburn84.github.io/Portfolio/vlan • pfSense : https://skullburn84.github.io/Portfolio/pfsense • Proxmox : https://skullburn84.github.io/Portfolio/proxmox 						