Dossier 02 - Réseau

Réalisé par : El Majdouli Hamza

Table des matières

Dossier 02 - Réseau

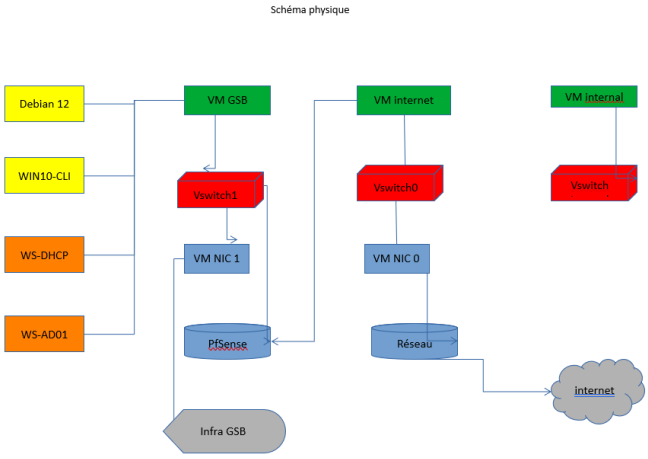
Epreuve E6 - Cas GSB

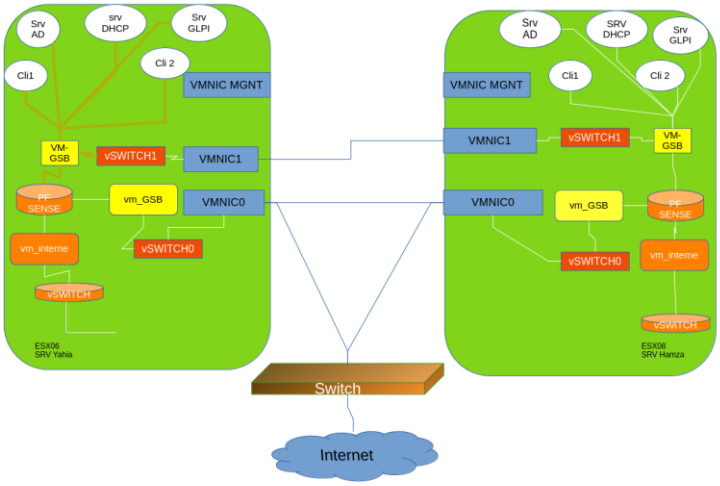
Dossier 02 - Réseaux (SR)

El Majdouli Hamza

INE : 081829944DC

Sommaire :





	Yahia					Commun	Hamza			
OS	Client Windows	Serveur Windows / AD	DHCP Windows	Serveur GLPI -Debian 12	DMZ – debian12	Pfsence – FreeBSD	Client Windows	Serveur Windows / AD	DHCP-Windows	DMZ – debian12
Nom	Client-01	SRV-AD1	SRV-AD1 (DHCP)	SRV-GLPI	yahia	pFsence	Client-02	SRV-AD0806	SRV-AD02	yahia
@IP	172.16.06.102	172.16.06.101	172.16.06.101	172.16.06.200	192.168.255.253	Wan → vmx3 → 10.51.08.254 Lan → vmx1 → 172.16.08.254 DMZ → vmx0 → 192.168.255.254	172.16.08.102	172.16.08.102	172.16.08.102	192.168.255.253
@MAC	00-0C-29-FF-AB-7C	00-0C-29-C5-BE-94	00-0C-29-C5-BE-94	00:0c:29:51:9c:20	00:0c:29:cb:66:27	GSB : 00:0c:29:3e:9e:93	00-0C-29-E0-6F-5C	00-0C-29-5D-AC-15	00-0C-29-5D-AC-15	00:0c:29:cb:66:27
Masque réseau	255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0	255.255.255.252	Wan : 255.0.0.0Lan : 255.255.0.0Dmz	255.255.0.0	255.255.0.0	255.255.0.0	255.255.255.252
Passerelle	172.16.06.254	172.16.12.254	172.16.12.254	172.16.12.101	192.168.255.254	10.0.0.1	172.16.06.101	172.16.08.254	172.16.08.254	192.168.255.254
DNS1	172.16.06.101	127.0.0.1	127.0.0.1	9.9.9.11	9.9.9.11		172.16.06.101	127.0.0.1	127.0.0.1	9.9.9.11

Mot de passe de l’infrastructure :

ESXi hamza btsSIO351 yahia btsSIO351

Switch A1.1 root btsSIO351

Switch A1.2 root cisco

Borne Wifi admin btsSIO351

PfSense admin btsSIO351

Client windows hamza btsSIO351 hamza btsSIO351

Client debian root root

Serveur AD Administrateur btsSIO351

Serveur Web root root

Management btsSIO351

Zabbix : root zabbix Admin zabbix (interface)

GLPI : glpi glpi(Super Admin) root root(Serveur)

Configurations des routeurs

Dossier 02 – Réseau (SR)

DHCP

1. Installer le rôle DHCP

Ouvre le Server Manager.

Clique sur "Add roles and features".

Clique sur Next jusqu'à atteindre "Server Roles".

Coche DHCP Server.

Clique sur Next, puis Install.

À la fin, clique sur Complete DHCP configuration.

Valide l'autorisation DHCP avec un compte administrateur.

2. Configurer une nouvelle étendue DHCP (scope)

Dans le Server Manager, va dans Tools > DHCP.

Ouvre ton serveur DHCP (nom du serveur → IPv4).

Clique droit sur IPv4, puis New Scope.

Suis l'assistant :

Nom de l'étendue : par exemple Etendue_LAN

Plage d'adresses : ex. 192.168.1.100 à 192.168.1.200

Longueur du préfixe : généralement 24 (masque 255.255.255.0)

Exclusions (optionnel) : ex. 192.168.1.110 si une IP est déjà utilisée

Durée du bail : par défaut (8 jours), ou ajuste selon ton besoin

Options supplémentaires :

Gateway (routeur) : ex. 192.168.1.1

DNS : IP du DNS (ex. serveur local ou 9.9.9.11)

Terminer la configuration → l'étendue est maintenant active.

Dans la console DHCP, clique droit sur l'étendue et choisis "Activate".

Supervision / SNMP (ex : Zabbix)

-Crée une machine en mettant l'iso Zabbix

- changer l'adresse IP

-installer l'agent zabbix sur le serveur AD

-configurer l'agent zabbix en mettant l'ip du serveur Zabbix

TFTP

1. Qu'est-ce que TFTP ?

2. Caractéristiques de TFTP :

Simplicité : Le protocole est très simple, avec une structure minimale. Il n'a pas de mécanismes avancés comme l'authentification ou le chiffrement, ce qui le rend rapide et léger.

Pas de sécurité : Contrairement à FTP ou SFTP, TFTP ne propose aucune forme de sécurité. Cela en fait un protocole moins sûr, souvent utilisé dans des réseaux internes sécurisés.

Port utilisé : TFTP fonctionne sur le port UDP 69.

Mode de fonctionnement : Il fonctionne principalement en mode UDP (User Datagram Protocol), ce qui signifie qu'il n'y a pas d'établissement de connexion comme avec le TCP, ce qui le rend encore plus léger.

3. Utilisations courantes de TFTP :

Mise à jour des équipements réseau : Beaucoup de dispositifs réseau comme les routeurs ou les switches utilisent TFTP pour charger des configurations ou des mises à jour de firmware.

Récupération de fichiers de configuration : Par exemple, un switch peut télécharger un fichier de configuration de démarrage via TFTP.

Dépannage : Lors du démarrage de certains équipements, TFTP est utilisé pour charger des fichiers nécessaires à la récupération de l'appareil.

4. Principe de fonctionnement de TFTP :

TFTP fonctionne avec une architecture client-serveur où un serveur TFTP héberge les fichiers et un client TFTP (un périphérique réseau) demande des fichiers ou envoie des fichiers au serveur.

Voici les principales étapes du processus :

Demande de fichier (Read Request, RRQ) : Le client TFTP envoie une demande de lecture (RRQ) pour récupérer un fichier à partir du serveur.

Réponse du serveur (Data) : Le serveur TFTP répond en envoyant des segments de données.

Ack des segments de données : Après avoir reçu un segment de données, le client ou le serveur envoie un accusé de réception (ACK) pour confirmer la réception correcte.

5. Configuration d'un serveur TFTP :

La configuration d'un serveur TFTP dépend du système d'exploitation sur lequel il est exécuté. Voici un guide de base pour la configuration sous différents systèmes.

5.1. Sur un serveur Linux (ex. Ubuntu) : sur le serveur zabbix

Installer le serveur TFTP : Ouvre un terminal et installe le serveur TFTP avec la commande suivante

VLAN

1. Sur un switch manageable Cisco (CLI)

➤ Créer les VLANs :

bash

CopierModifier

enable

configure terminal

vlan 10

name PC

exit

vlan 20

name SERVEURS

Associer les ports aux VLANs (mode access) :

interface range fa0/1 - 5

switchport mode access

switchport access vlan 10

interface range fa0/6 - 10

switchport access vlan 20

Configurer un port trunk (vers routeur ou pfSense) :

interface fa0/24

switchport mode trunk

switchport trunk allowed vlan 10,20

2. Ce qu'il faut comprendre

3. Routage inter-VLAN (via pfSense)

Pour que les VLANs communiquent entre eux, il faut un routeur ou un switch de niveau 3.

Exemple sur pfSense :

Crée une interface pour chaque VLAN :

VLAN 10 → Interface OPT1 avec IP 192.168.10.1/24

VLAN 20 → Interface OPT2 avec IP 192.168.20.1/24

Active le DHCP sur chaque interface si nécessaire.

Ajoute les règles de pare-feu si tu veux autoriser la communication entre VLANs.

LACP

Qu'est-ce que LACP ?

LACP (IEEE 802.3ad) permet d'agréger plusieurs ports physiques en un lien logique unique (appelé Link Aggregation Group, ou LAG) pour :

Augmenter la bande passante

Offrir une tolérance de panne (si un lien tombe, les autres continuent)

Exemple : agréger 2 ports Ethernet à 1 Gbit/s → un lien logique à 2 Gbit/s

Prérequis

Deux équipements compatibles LACP (ex. switchs managés, pfSense, serveurs)

Même configuration des ports (vitesse, duplex, VLAN…)

Câbles branchés en croisé (ou auto MDI/MDI-X)

Exemple de configuration LACP

Sur un switch Cisco :

interface range fa0/1 - 2

channel-group 1 mode active

interface port-channel 1

mode active : LACP actif port-channel 1 : lien logique

STP (Spanning Tree Protocol – norme IEEE 802.1D) sert à éviter les boucles réseau lorsqu'il y a des connexions redondantes entre switchs.

Pourquoi c'est important ?

Sans STP, une boucle réseau peut :

Saturer le réseau (trames qui tournent en boucle)

Faire tomber tous les équipements du LAN

Comment fonctionne STP ?

Fonctionnement de base :

Élection d'un switch racine (Root Bridge)

Chaque switch calcule le chemin le plus court pour atteindre ce switch racine.

Les autres chemins redondants sont bloqués pour éviter les boucles.

En cas de panne d'un lien, STP réactive un lien bloqué → redondance assurée

Types de ports STP

Configuration STP sur un switch Cisco

➤ Activer STP (souvent activé par défaut)

show spanning-tree

➤ Changer la priorité pour forcer un switch comme Root Bridge :

spanning-tree vlan 1 priority 4096

➞ Plus la priorité est basse, plus le switch est préféré comme Root Bridge (valeur par défaut = 32768)

Modes STP disponibles

➤ Activer RSTP sur Cisco :

spanning-tree mode rapid-pvst

Commandes de vérification

show spanning-tree vlan 1

show spanning-tree root

Routage / Agrégation de lien

1. Routage

Objectif :

Permettre la communication entre plusieurs réseaux (ex. entre différents VLANs ou entre un LAN et Internet).

Types de routage :

Exemple de routage inter-VLAN sur pfSense :

Tu as déjà vu ça dans ton réseau ! Si tu as :

VLAN 10 : 192.168.10.0/24

VLAN 20 : 192.168.20.0/24 Alors pfSense aura deux interfaces :

VLAN10 : 192.168.10.1

VLAN20 : 192.168.20.1

Et il route automatiquement les paquets entre les deux (sauf si bloqué par des règles firewall).

2. Agrégation de lien (LACP)

Assembler plusieurs interfaces physiques pour créer un lien logique plus rapide et redondant.

Exemple :

2 liens 1 Gbit/s entre un switch et un serveur → LACP → 2 Gbit/s logiques (selon les flux).

Exemple d’agrégation de lien (LACP) entre switch et pfSense :

Sur pfSense :

Interfaces > Assignments > LAGG

Crée un LAGG avec em0 + em1

Mode : LACP

Attribue cette interface LAGG à VLANs ou IP directement

PfSense (pare-feu + règles NAT)

1. PARE-FEU PFSENSE – FONCTIONNEMENT

Contrôler qui a le droit de communiquer avec qui sur ton réseau, et vers Internet.

Par défaut, pfSense :

Bloque tout ce qui entre (depuis WAN)

Autorise ce qui sort (depuis LAN vers Internet)

Exemples de règles pare-feu :

Exemple 1 : Autoriser l'accès Internet depuis le VLAN 10

Menu : Firewall > Rules > VLAN10

plaintext

Action : Pass

Interface : VLAN10

Protocol : any

Source : VLAN10 net

Destination : any

Exemple 2 : Bloquer l'accès d'un VLAN au reste du réseau

Menu : Firewall > Rules > VLAN20

Action : Block

Source : VLAN20 net

Destination : RFC1918 networks (privés)

Ajoute ensuite une règle "Pass" vers any pour autoriser Internet

Conseil :

L'ordre des règles compte : pfSense lit de haut en bas

Si aucune règle ne correspond, le trafic est bloqué

2. NAT (Network Address Translation)

Traduire les adresses IP privées (LAN) en IP publique (WAN) pour accéder à Internet ou rediriger vers des services internes.

NAT SORTANT (Outbound NAT)

Par défaut en mode automatique : pfSense NAT tout le trafic LAN → WAN automatiquement.

➤ Pour un contrôle manuel :

Firewall > NAT > Outbound

Passe en "Hybrid" ou "Manual"

Tu peux alors définir quelles IPs sortent sur quelle IP publique (multi-WAN, failover…)

NAT ENTRANT (Port Forward)

Utilisé pour rendre un serveur local accessible depuis Internet (ex : serveur web, RDP, etc.).

Exemple : Rediriger port 80 du WAN vers un serveur interne

Menu : Firewall > NAT > Port Forward > Add

Interface : WAN

Protocol : TCP

Destination : WAN address

Destination port range : 80 (HTTP)

Redirect target IP : 192.168.10.100

Redirect target port : 80

Coche “NAT reflection” si tu veux tester depuis l’intérieur du réseau

pfSense ajoute automatiquement une règle pare-feu WAN si tu coches la case correspondante

1. Qu’est-ce qu’une DMZ ?

Une DMZ est une zone isolée du réseau interne où l’on place les services exposés à Internet :
➞ serveurs web, mail, FTP, caméras, etc.

Objectifs :

Protéger le réseau interne même si un service est piraté

Séparer les flux internes, Internet et publics

Contrôler finement qui accède à quoi

2. Schéma typique avec pfSense

less

INTERNET

[WAN]

pfSense

/ | \

[LAN] [DMZ] [VLANs…]

192.168.1.0 192.168.2.0 ...

LAN : réseau interne sécurisé

DMZ : réseau public semi-sécurisé

WAN : vers Internet

Wifi (SSID, authentification)

1. Qu’est-ce qu’un SSID ?

Le SSID (Service Set Identifier) est le nom du réseau Wi-Fi visible quand tu cherches un Wi-Fi.

Un point d’accès peut diffuser plusieurs SSID, chacun sur un VLAN différent.

4. Types d’authentification Wi-Fi

5. Configuration du VLAN Wi-Fi sur pfSense

Supposons :

VLAN 20 = Wi-Fi Invités

VLAN 30 = Wi-Fi Pro

➤ Sur pfSense :

Interfaces > Assignments > VLANs

Crée VLAN 20 sur interface LAN ou trunk

Donne-lui une IP (ex. 192.168.20.1/24)

Active DHCP pour ce VLAN (optionnel)

➤ Dans Firewall > Rules > VLAN20 :

Autorise accès Internet (vers WAN)

Bloque accès aux autres VLANs (LAN net, VLAN10, etc.)

VPN (nomade)

1. Qu'est-ce qu'un VPN nomade ?

Un VPN nomade permet à un utilisateur (depuis l'extérieur, par exemple chez lui ou en déplacement) de :

se connecter à distance au réseau de l'entreprise,

accéder aux ressources internes (serveurs, imprimantes, caméras…),

en toute sécurité grâce au chiffrement.

2. Solution recommandée sur pfSense

OpenVPN (intégré à pfSense, compatible avec tous les OS)

3. Configuration OpenVPN nomade sur pfSense

➤ Étape 1 : Créer une autorité de certification (CA)

System > Cert. Manager > CAs

Clique sur "Add"

Donne un nom : VPN-CA

Remplis les champs obligatoires

Clique sur Save

➤ Étape 2 : Créer un certificat serveur

System > Cert. Manager > Certificates

Type : Server Certificate

Choisir la CA créée

Nom : OpenVPN-Server

➤ Étape 3 : Assistant OpenVPN

VPN > OpenVPN > Wizards

Sélectionne Local User Access

Choisir la CA et le certificat créés

Définir un Tunnel Network : ex. 10.8.0.0/24

Définir le Local Network à atteindre : ex. 192.168.10.0/24 (ton LAN ou VLAN PC)

Ports : par défaut 1194/UDP

DNS : laisse vide ou ajoute 192.168.10.1 si besoin

Crée un compte utilisateur VPN (ex. hamza^2) avec un certificat utilisateur

➤ Étape 4 : Créer une règle pare-feu

Firewall > Rules > WAN

Autoriser le trafic vers le port VPN :

Protocol : UDP

Destination port : 1194

➤ Étape 5 : Exporter le profil VPN (facile !)

Installer le package d'exportation : System > Package Manager > Available Packages > openvpn-client-export

Aller dans : VPN > OpenVPN > Client Export

Clique sur le lien de téléchargement correspondant à ton utilisateur (ex. .ovpn pour Windows ou mobile)

4. Connexion côté client

➤ Sur Windows :

Installer OpenVPN Connect ou OpenVPN GUI

Importer le fichier .ovpn téléchargé

Se connecter avec l'identifiant (si demandé)

➤ Sur Android/iOS :

Installer OpenVPN Connect

Importer le fichier .ovpn via email, Nextcloud, etc.

5. Sécurité et conseils

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui permet à un serveur de fournir automatiquement des adresses IP et d'autres paramètres réseau à des appareils (comme des ordinateurs, smartphones, imprimantes, etc.) sur un réseau.

Voici une explication détaillée pour ton dossier de l'épreuve E5 :

1. Objectif du DHCP :

Le DHCP est utilisé pour simplifier l'administration des réseaux IP. Plutôt que de configurer manuellement une adresse IP sur chaque appareil du réseau, le DHCP attribue automatiquement une adresse IP à chaque appareil qui se connecte. Cela permet d'éviter les conflits d'adresses IP et facilite la gestion du réseau.

2. Fonctionnement du DHCP :

Lorsque un appareil (client DHCP) se connecte au réseau et n'a pas encore d'adresse IP, il va passer par une série d'étapes pour obtenir cette adresse :

Découverte (DHCP Discover) : Le client envoie un message de type DHCP Discover à tout le réseau (broadcast) pour signaler qu'il recherche un serveur DHCP.

Offre (DHCP Offer) : Le serveur DHCP répond en envoyant un message DHCP Offer qui contient une adresse IP proposée et d'autres paramètres réseau (comme la passerelle par défaut, le serveur DNS, la durée du bail d'adresse IP, etc.).

Demande (DHCP Request) : Le client choisit l'offre la plus appropriée et envoie un message DHCP Request au serveur DHCP pour accepter l'offre.

Accusé de réception (DHCP Acknowledge) : Enfin, le serveur envoie un message DHCP Acknowledge pour confirmer l'attribution de l'adresse IP et des paramètres associés.

Ce processus est souvent appelé DORA (Discover, Offer, Request, Acknowledge).

3. Composants principaux du DHCP :

Serveur DHCP : C'est un dispositif (souvent un serveur ou un routeur) qui attribue les adresses IP et gère le bail d'adresses.

Client DHCP : C'est un appareil qui demande une adresse IP via DHCP (ex : un ordinateur, un smartphone, etc.).

Pool d'adresses IP : C'est une plage d'adresses IP définie par l'administrateur réseau, que le serveur DHCP attribue aux clients. Une fois qu'un client a obtenu une adresse IP, celle-ci est réservée pour une période déterminée appelée bail.

Bail DHCP : Il s'agit du temps pendant lequel une adresse IP attribuée à un client est valide. Une fois le bail expiré, l'adresse peut être réattribuée à un autre appareil ou renouvelée par le même appareil.

4. Avantages du DHCP :

Simplification de la gestion réseau : Pas besoin d'assigner manuellement les adresses IP aux appareils.

Prévention des conflits d'adresses IP : Le serveur gère les attributions d'adresses pour éviter que plusieurs appareils n'aient la même adresse.

Adaptabilité : Le DHCP s'adapte facilement aux changements dans le réseau (ajout ou retrait d'appareils).

Configuration automatisée : Le serveur DHCP peut envoyer d'autres paramètres de configuration réseau, comme la passerelle, les serveurs DNS, etc.

5. Inconvénients et limitations du DHCP :

Dépendance au serveur DHCP : Si le serveur DHCP tombe en panne, aucun appareil ne pourra obtenir une adresse IP.

Sécurité : Le protocole DHCP n'est pas conçu pour être sécurisé, donc un attaquant pourrait potentiellement configurer un serveur DHCP malveillant pour envoyer de mauvaises informations aux clients.

6. Sécurisation du DHCP :

Il existe des mécanismes pour sécuriser le DHCP, comme l'utilisation de DHCP snooping sur les switches pour limiter les ports qui peuvent être des serveurs DHCP, ou la mise en place de baux DHCP réservés, qui permettent de lier une adresse MAC spécifique à une adresse IP spécifique.

7. DHCP et son rôle dans un réseau local :

Dans un réseau local (LAN), le DHCP simplifie la gestion des adresses IP pour un grand nombre de périphériques, ce qui est crucial dans des environnements où de nombreux appareils se connectent et se déconnectent régulièrement.

Exemple d'application dans un réseau :

Imaginons un bureau avec 50 ordinateurs. Plutôt que de configurer manuellement une adresse IP pour chaque ordinateur, le serveur DHCP attribue une adresse IP à chaque machine qui se connecte au réseau. Une fois l'adresse IP attribuée, le serveur peut aussi

fournir les paramètres de passerelle et de serveur DNS, de sorte que chaque ordinateur puisse accéder à Internet sans aucune configuration manuelle.

La supervision d'un réseau informatique est un processus clé pour garantir son bon fonctionnement, sa performance et sa sécurité. Le protocole SNMP (Simple Network Management Protocol) est l'un des principaux outils utilisés pour surveiller et gérer les équipements réseau tels que les routeurs, switches, serveurs, imprimantes, et autres périphériques.

Voici une explication détaillée pour ton dossier concernant la supervision via SNMP :

1. Qu'est-ce que le SNMP ?

Le SNMP est un protocole de communication standard utilisé pour gérer et superviser les périphériques réseau. Il permet à un système de gestion de réseau (souvent un serveur ou une station de travail dédiée à la gestion) de collecter des informations sur les périphériques (comme les routeurs, switches, serveurs, etc.), de surveiller leur état, de configurer certains paramètres et d'alerter l'administrateur réseau en cas de problème.

2. Composants du SNMP :

Gestionnaire SNMP (SNMP Manager) : C'est le logiciel ou la station de gestion réseau qui envoie des requêtes SNMP aux dispositifs réseau pour collecter des informations. Il analyse les données reçues et présente des rapports à l'administrateur.

Agent SNMP : C'est le logiciel qui fonctionne sur les périphériques réseau (routeurs, switches, serveurs, imprimantes, etc.). L'agent répond aux requêtes SNMP du gestionnaire et envoie des informations sur l'état et les performances du périphérique.

Base de données MIB (Management Information Base) : Il s'agit d'une base de données utilisée par le protocole SNMP pour stocker des informations relatives à la configuration et à l'état du périphérique. Elle est structurée sous forme d'objets identifiables, et chaque périphérique peut avoir sa propre MIB.

3. Fonctionnement du SNMP :

Le SNMP fonctionne en échangeant des messages entre le gestionnaire SNMP et les agents SNMP. Ces messages sont appelés des PDU (Protocol Data Units). Les principaux types de messages SNMP sont :

GET : Le gestionnaire envoie une requête GET pour obtenir la valeur d'un objet dans la MIB d'un périphérique.

SET : Le gestionnaire envoie une requête SET pour modifier une valeur dans la MIB d'un périphérique.

TRAP : L'agent envoie un message TRAP pour informer le gestionnaire d'un événement particulier (comme une alerte de panne).

GETNEXT : Utilisé pour parcourir la MIB d'un périphérique en récupérant successivement des objets de données.

Exemple de flux :

Le gestionnaire SNMP demande l'état de la mémoire d'un serveur via une requête GET.

L'agent SNMP du serveur répond avec les données de mémoire.

Si le gestionnaire détecte un problème (par exemple, une surcharge de la mémoire), il peut envoyer une commande SET pour ajuster la configuration, ou il peut déclencher des alertes basées sur les informations reçues.

4. Version du SNMP :

Il existe plusieurs versions du SNMP :

SNMPv1 : La première version, mais elle a des limitations de sécurité, car les informations sont envoyées en clair.

SNMPv2c : Introduit des améliorations par rapport à SNMPv1, comme des commandes plus efficaces. Cependant, il ne résout pas complètement les problèmes de sécurité.

SNMPv3 : La version la plus sécurisée, qui inclut des mécanismes d'authentification et de chiffrement des messages pour protéger les données sensibles échangées entre les agents et le gestionnaire.

5. Configuration d'un serveur SNMP :

Pour configurer un agent SNMP sur un périphérique, il faut généralement :

Activer le service SNMP sur l'appareil (routeur, switch, serveur, etc.). Cela peut se faire via l'interface de gestion de l'appareil (par exemple, une interface web ou une ligne de commande).

Configurer la communauté SNMP : La communauté est comme un mot de passe qui permet l'accès aux données SNMP. Il existe deux types de communautés :

Community Read (lecture) : Permet au gestionnaire d'obtenir des informations du périphérique, mais pas de les modifier.

Community Write (écriture) : Permet de modifier des paramètres du périphérique.

Définir les paramètres de sécurité (surtout avec SNMPv3) : Cela inclut l'authentification et le chiffrement pour garantir la confidentialité et l'intégrité des communications.

Ajouter des hôtes autorisés : Limiter l'accès aux gestionnaires SNMP spécifiques pour éviter les accès non autorisés.

6. Surveillance à l'aide de SNMP :

La surveillance SNMP implique la collecte de différentes métriques sur les périphériques réseau pour vérifier leur bon fonctionnement. Voici quelques exemples de données collectées via SNMP :

Utilisation du processeur : Pour surveiller les performances du processeur de l'équipement.

Utilisation de la mémoire : Pour détecter les problèmes liés à l'utilisation excessive de la mémoire.

Disponibilité du périphérique : Pour s'assurer que le périphérique est en ligne et fonctionne correctement.

Statistiques de réseau : Comme le nombre de paquets reçus/envoyés, les erreurs réseau, les collisions, etc.

Température : Surveiller la température des équipements, en particulier les serveurs et les routeurs.

Alertes TRAP : En cas d'événement critique (panne, surcharge, etc.), l'agent SNMP peut envoyer une alerte TRAP pour prévenir le gestionnaire.

7. Outils de supervision SNMP :

Il existe plusieurs outils permettant de surveiller et de gérer les équipements réseau via SNMP. Quelques exemples populaires incluent :

PRTG Network Monitor : Un outil complet qui permet de surveiller les réseaux en temps réel avec des alertes SNMP.

SolarWinds Network Performance Monitor : Utilisé pour détecter des problèmes de performance réseau en se basant sur SNMP.

Nagios : Un outil de surveillance open-source qui utilise SNMP pour surveiller les périphériques réseau.

8. Avantages de la supervision SNMP :

Centralisation de la gestion réseau : Le SNMP permet d'obtenir des informations détaillées de plusieurs équipements à partir d'un seul point de gestion.

Détection précoce des problèmes : Les alertes SNMP permettent de détecter rapidement des problèmes potentiels, comme des défaillances matérielles ou des surcharges.

Automatisation de la gestion : Il est possible d'automatiser certaines actions via SNMP, telles que la mise à jour de configurations ou le redémarrage de périphériques.

Interopérabilité : SNMP est largement supporté par différents fabricants de matériel, ce qui permet une gestion hétérogène du réseau.

La configuration de TFTP (Trivial File Transfer Protocol) est essentielle pour le transfert de fichiers simples dans un réseau, notamment pour la gestion des équipements réseau comme des routeurs, des switches ou des serveurs. TFTP est un protocole très léger, souvent utilisé dans des environnements où la simplicité et la rapidité sont plus importantes que les fonctionnalités avancées et la sécurité.

Voici une explication détaillée sur le TFTP et sa configuration :

Installer le serveur TFTP : Ouvre un terminal et installe le serveur TFTP avec la commande suivante :

La configuration VLAN (Virtual Local Area Network) est un processus essentiel pour la segmentation du réseau, permettant de diviser un réseau physique en plusieurs réseaux logiques. Cela permet d'améliorer la gestion, la sécurité, et les performances du réseau en isolant les différents types de trafic.

Voici une explication détaillée sur la configuration des VLANs :

1. Qu'est-ce qu'un VLAN ?

Un VLAN (Virtual Local Area Network) est une segmentation logique d'un réseau local physique en plusieurs sous-réseaux distincts, indépendamment de la topologie physique. Un VLAN permet de créer des groupes d'appareils qui peuvent communiquer entre eux comme s'ils étaient dans le même réseau local, même s'ils sont physiquement séparés.

Les VLANs sont utilisés pour :

Isoler le trafic : Séparer les différents types de trafic (ex : réseaux de gestion, utilisateurs, serveurs) pour des raisons de sécurité.

Améliorer les performances : Réduire le nombre de paquets diffusés sur un réseau.

Simplifier la gestion : Faciliter la gestion et la configuration des réseaux complexes.

2. Types de VLANs :

VLAN de données : Ce sont les VLANs les plus courants, utilisés pour séparer les utilisateurs ou les appareils d'un réseau en différents groupes fonctionnels.

VLAN de gestion : Utilisé pour la gestion des équipements réseau (comme les switches, routeurs, etc.).

VLAN de voix (VLAN Voice) : Utilisé pour le trafic VoIP (voix sur IP), afin d'assurer la qualité du service (QoS).

VLAN par défaut : Le VLAN par défaut est généralement le VLAN 1, et tous les ports d'un switch sont affectés à ce VLAN par défaut si aucun autre VLAN n'est spécifié.

3. Fonctionnement des VLANs :

Un VLAN fonctionne en utilisant des étiquettes dans les trames Ethernet pour identifier à quel VLAN appartient chaque paquet. Chaque VLAN a un identifiant unique appelé ID VLAN, qui peut être un nombre compris entre 1 et 4095. Lorsque des périphériques communiquent au sein du même VLAN, ils peuvent échanger des informations comme s'ils étaient sur le même réseau physique. Si des périphériques sur des VLANs différents doivent communiquer, cela nécessite un routage inter-VLAN.

4. Avantages des VLANs :

Sécurité améliorée : En isolant différents types de trafic, il est plus difficile pour un attaquant de compromettre tout le réseau.

Optimisation du trafic : Réduire le domaine de diffusion (broadcast domain) permet de diminuer le trafic inutile sur le réseau.

Flexibilité et scalabilité : Ajouter un nouveau VLAN ou modifier la configuration du réseau est relativement simple sans perturber les autres VLANs.

5. Configuration des VLANs sur un switch Cisco :

La configuration d'un VLAN sur un switch Cisco (qui est l'un des équipements les plus utilisés dans les réseaux) se fait en plusieurs étapes. Voici les principales étapes de la configuration :

5.1. Accéder à l'interface de gestion du switch :

Se connecter au switch via une connexion console, SSH ou Telnet pour accéder à l'interface de ligne de commande (CLI).

5.2. Créer un VLAN :

Pour créer un VLAN, il faut entrer en mode configuration globale et utiliser la commande vlan :

STP (Spanning Tree Protocol) est un protocole de commutation utilisé pour éviter les boucles dans un réseau Ethernet de type commuté. Ces boucles peuvent survenir lorsque plusieurs chemins existent entre les switches dans un réseau, ce qui peut entraîner un phénomène de boucle infinie, surchargeant ainsi le réseau et causant des défaillances. STP permet d'assurer qu'il n'y ait qu'un seul chemin actif entre deux points du réseau, tout en permettant la redondance en désactivant les autres chemins inutilisés pour éviter les boucles.

1. Pourquoi utiliser STP ?

STP est utilisé pour :

Éviter les boucles réseau : Si plusieurs chemins existent entre deux switches, STP détermine automatiquement le meilleur chemin et désactive les chemins redondants pour éviter les boucles.

Assurer la redondance : En cas de défaillance d'un chemin, STP active un autre chemin redondant pour maintenir la connectivité du réseau.

2. Concepts de base de STP :

2.1. Racine du pont (Root Bridge) :

Le Root Bridge est l'équipement central du réseau, désigné comme le "pont racine". C'est l'équipement auquel tous les autres switches s'orientent pour choisir le meilleur chemin pour acheminer les données. Le Root Bridge est sélectionné sur la base de l'ID du bridge (qui combine la priorité et l'adresse MAC).

2.2. ID du pont (Bridge ID) :

L'ID du pont est une combinaison de l'adresse MAC et d'un numéro de priorité. La priorité par défaut est 32768, et c'est ce qui détermine l'ID du pont. L'ID le plus bas devient le Root Bridge. L'ID du pont est un facteur essentiel dans la sélection du Root Bridge.

2.3. Chemins désignés (Designated Ports) :

Ce sont les ports des switches qui sont utilisés pour acheminer les données vers et depuis un segment spécifique. Un chemin désigné est le seul chemin actif pour un segment de réseau donné.

2.4. Ports bloqués (Blocked Ports) :

Ce sont les ports qui sont désactivés pour éviter des boucles. STP bloque les chemins redondants et les rend inactifs tant que le chemin principal est disponible.

2.5. Coût du chemin (Path Cost) :

Le coût d'un chemin est un nombre qui représente la "distance" du chemin jusqu'au Root Bridge. Le chemin avec le coût le plus bas est préféré. Le coût de chaque lien est calculé en fonction de la bande passante (par exemple, un lien de 100 Mbps aura un coût plus élevé qu'un lien de 1 Gbps).

3. État des ports dans STP :

Un port STP peut être dans l'un des états suivants :

Blocking : Le port est bloqué et ne transmet pas de données.

Listening : Le port attend pour s'assurer qu'il n'y a pas de boucles.

Learning : Le port apprend les adresses MAC pour construire sa table de commutation.

Forwarding : Le port transmet des données.

Disabled : Le port est administrativement désactivé.

4. Les différentes versions de STP :

STP (IEEE 802.1D) : C'est la version de base, utilisée principalement dans des réseaux plus petits.

RSTP (Rapid Spanning Tree Protocol – IEEE 802.1w) : C'est une version améliorée qui réduit le temps de convergence et est plus rapide que STP classique.

MSTP (Multiple Spanning Tree Protocol – IEEE 802.1s) : Il permet de gérer plusieurs instances de spanning tree pour mieux prendre en charge les VLANs multiples.

5. Configuration de STP sur un switch Cisco :

Voici comment configurer STP sur un switch Cisco.

5.1. Vérification de la configuration STP :

Avant de configurer STP, il est important de vérifier son état actuel sur le switch :Switch# show spanning-tree

Cette commande affiche des informations sur la topologie STP actuelle, notamment le Root Bridge, les états des ports, et les coûts de chemin.

5.2. Modifier la priorité du Root Bridge :

Par défaut, un switch est élu Root Bridge si son ID de pont est le plus bas. Si tu veux forcer un switch spécifique à devenir le Root Bridge, tu peux abaisser sa priorité.

Accéder à l'interface de configuration : on se connecte au switch via la ligne de commande.

Le routage et l'agrégation de liens (AGR, ou Link Aggregation) sont des concepts essentiels pour améliorer la performance et la redondance d'un réseau. Voici comment ces deux processus sont utilisés et configurés dans un environnement réseau, en particulier sur des switches et des routeurs Cisco.

1. Routage (Routage IP) :

Le routage est un processus utilisé pour acheminer les paquets de données entre différents réseaux. Un routeur examine les paquets entrants, consulte ses tables de routage pour déterminer le meilleur chemin et les envoie ensuite vers leur destination.

1.1. Types de routage :

Il existe principalement deux types de routage :

Routage statique : Les chemins sont définis manuellement par un administrateur réseau. Il n'y a pas de mise à jour automatique des routes.

Routage dynamique : Utilise des protocoles comme RIP, OSPF, ou BGP pour échanger automatiquement des informations de routage entre les routeurs et mettre à jour les tables de routage.