MARZOUGUI Houdaifa

EL SHIKH Zakaria

LAKHLIFI Merwane

BTS SIO 1

Document de validation de compétences

AP4-GSBVélanne

27/05/2025

Equipe 7

1. Présentation du contexte d'entreprise

L'entreprise GSB projette de cloisonner son réseau et vient de réaliser une étude afin d'établir le plan d'adressage réseau et le nommage des vlans.

Chaque étage dispose d'une baie de brassage qui le relie par une fibre à la baie centrale de la salle serveurs.

Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.

Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.

Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

Chaque salle de réunion dispose d'un vidéoprojecteur, d'enceintes et d'un tableau numérique interactif.

La salle "Démonstration" est destinée à l'accueil des organismes de santé (AFSSAPS notamment) et des partenaires scientifiques. Elle dispose de paillasses et d'équipements de laboratoire, en plus d'une salle de réunion.

L'entreprise vous confie la responsabilité de maquetter cette étude afin de valider le projet.

2. Objectifs attendus

L'objectif principal de ce projet est de concevoir et mettre en place une infrastructure réseau cloisonnée, en respectant un plan d'adressage IP précis et en utilisant la segmentation par VLAN. Chaque service de l'entreprise doit disposer de son propre VLAN, ce qui permettra d'organiser logiquement le réseau tout en renforçant la sécurité et la gestion des flux.

Il est également attendu que les VLAN soient configurés sur les différents commutateurs de l'entreprise, avec un routage InterVLAN mis en place grâce à un routeur Cisco. Ce routage devra permettre aux différents services d'accéder aux ressources partagées tout en respectant les restrictions d'accès définies dans le cahier des charges.

Un autre objectif technique est de mettre en place un accès distant sécurisé à l'ensemble des équipements réseau. Cette administration devra se faire via le protocole SSH, uniquement accessible par les membres du service Réseau & Système, à l'exception d'un stagiaire spécifique qui ne doit pas y avoir accès.

Le projet prévoit également la création et la configuration de listes de contrôle d'accès (ACL) pour gérer précisément les droits d'accès aux différentes zones du réseau. Par exemple,

certains serveurs comme le TFTP, le serveur Active Directory ou encore le WebIntranet ne doivent être accessibles qu'à certains VLAN, et même à certaines adresses IP exclues du réseau.

Un objectif supplémentaire concerne la sauvegarde des configurations. Toutes les configurations mises en œuvre devront être sauvegardées sur un serveur TFTP, conformément aux procédures de gestion de patrimoine informatique.

Enfin, les étudiants devront réaliser un ensemble de tests pour valider le bon fonctionnement de leur solution, produire une documentation technique complète, rédiger un compte rendu de validation des compétences, et réaliser une présentation orale du projet. L'ensemble de ces éléments vise à simuler une situation professionnelle concrète où les compétences techniques et de communication sont mobilisées.

3. Plan de travail

A.1 Réalisation du schéma réseau

Concevoir le schéma réseau logique de votre solution répondant au cahier des charges. Vous pourrez utiliser les outils tels que Visio Packet Tracer ou tout autre outil de conception.

A.2 Mise en place de l'accès distant SSH

A.3 Création des Vlans

Paramétrer individuellement les différents switchs en respectant le cahier des charges et les informations de nommage fournies.

A.4 Routage InterVlan

Assurer la communication des différents services autorisés vers le serveur

A.5 Tests

Élaborer Réaliser l'ensemble des tests nécessaires à la validation de la solution proposée.

A.6 Réalisation des ACL

Réalisation des règles d'accès aux différentes zones

A.7 Sauvegarde

Réaliser l'ensemble des sauvegardes nécessaires

A.8 Compte rendu de validation de compétences

Rédiger le compte rendu de validation de compétences avec captures d'écrans commentées et tests de toutes les actions réalisées. Le poster sur votre portfolio

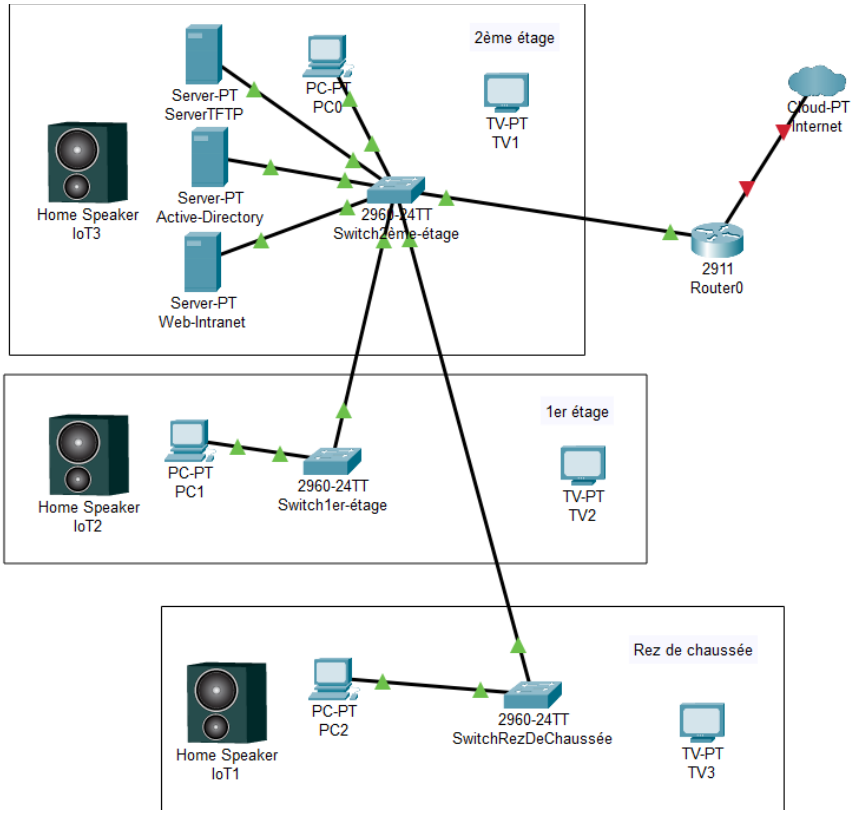
A.9 Compte rendu Chef de projet

Réaliser une présentation orale du projet

4. Réalisation

A1- Réalisation du schéma réseau

J'ai fait le schéma réseau en respectant les conditions demandées c'est-à-dire en prenant en compte les étages, les équipements, les câbles, etc…



A2- Mise en place de l'accès distant SSH

- Configuration de base du routeur
- SSH sécurisé (pour administrer à distance pour le Vlan 10 du réseau et système sauf le stagiaire)

```
R_Groupe7>en
R_Groupe7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_Groupe7(config)#hostname Routeur-GSB
Routeur-GSB(config)#no ip domain-lookup
Routeur-GSB(config)#
```

```
Routeur-GSB(config)#ip domain-name gsb.local
Routeur-GSB(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Routeur-GSB.gsb.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

Routeur-GSB(config)#
May 13 11:40:20.475: %SSH-5-ENABLED: SSH 1.99 has been enabled
Routeur-GSB(config)#username admin privilege 15 secret Admin123
```

```
Routeur-GSB(config)#line vty 0 4
Routeur-GSB(config-line)#transport input ssh
Routeur-GSB(config-line)#login local
Routeur-GSB(config-line)#exit
```

A3- Création des Vlans

Ce que j'ai fait :

- Création des 8 VLANs (10, 20, 30, 40, 50, 150, 200, 300) avec les noms et adressages imposés.
- Configuration des ports switch en mode "access" ou "trunk" selon leur rôle.
- Vérification avec `show vlan brief` et tests de connectivité entre ports.

Pourquoi :
→ Pour segmenter le réseau selon les services (Direction, Commercial, Visiteurs, etc.) et isoler les flux (B1.1 - Gestion du patrimoine).

```
SW-RDC#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
10   Reseau_Systeme                    active
20   Direction_DSI                     active
30   Administratif                     active
40   Commercial                        active
50   Developpement                     active
150  Visiteurs                         active
200  Demonstration                     active
300  Serveurs                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

COM3 - PuTTY

```
SW-RDC>
SW-RDC>
SW-RDC>
SW-RDC>en
SW-RDC#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : ap4
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0072.780f.9300
Configuration last modified by 0.0.0.0 at 3-7-93 03:29:40
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 13
Configuration Revision            : 8
MD5 digest                        : 0x23 0x47 0x40 0xDF 0x4B 0x7D 0xDE 0xFB
                                    0x80 0xF4 0xF3 0xBD 0xB9 0x4C 0xE7 0xB4
SW-RDC#
```

```
sw1#sh running-config int gi0/1
Building configuration...

Current configuration : 59 bytes
!
interface GigabitEthernet0/1
 switchport mode trunk
end

sw1#sh running-config int gi0/2
Building configuration...

Current configuration : 59 bytes
!
interface GigabitEthernet0/2
 switchport mode trunk
end
```

A4- Routage intervlan

- Activation du routage IP
- Configuration des sous-interfaces pour chaque VLAN (routage inter-VLAN)

```
Routeur-GSB(config-subif)#ip address 172.18.0.254 255.255.0.0
% 172.18.0.0 overlaps with GigabitEthernet0/0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.150
Routeur-GSB(config-subif)#encapsulation dot1Q 150
Routeur-GSB(config-subif)#ip address 192.168.150.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.200
Routeur-GSB(config-subif)#encapsulation dot1Q 200
Routeur-GSB(config-subif)#ip address 192.168.200.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.300
Routeur-GSB(config-subif)#encapsulation dot1Q 300
```

```
Routeur-GSB(config)#int gi0/0.10
Routeur-GSB(config-subif)#encapsulation dot1Q 10
Routeur-GSB(config-subif)#ip add
Routeur-GSB(config-subif)#ip address 192.168.10.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.20
Routeur-GSB(config-subif)#encapsulation dot1Q 20
Routeur-GSB(config-subif)#ip address 192.168.20.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.30
Routeur-GSB(config-subif)#encapsulation dot1Q 30
Routeur-GSB(config-subif)#ip address 192.168.30.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.40
Routeur-GSB(config-subif)#encapsulation dot1Q 40
Routeur-GSB(config-subif)#ip address 192.168.40.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.50
Routeur-GSB(config-subif)#encapsulation dot1Q 50
Routeur-GSB(config-subif)#ip address 192.168.50.254 255.255.255.0
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#ip routing
```

A5- Tests

Ce que j'ai fait :

- Vérification des ACLs avec `ping` et `telnet` depuis différents VLANs.
- Tests de restrictions (ex: VLAN 150 ne peut pas accéder au serveur AD).
- Capture des résultats avec Wireshark/Packet Tracer.

Pourquoi :
→ Pour valider le bon fonctionnement des règles de sécurité et du routage (B1.2 - Réponse aux incidents).

A6- Réalisation des ACL

- ACLs du routeur pour sécuriser l'accès :
- 1-Blocage de l'accès du stagiaire (192.168.10.1) au TFTP (supposé être à 172.18.0.10)
- 2-Blocage de l'accès du stagiaire commercial (192.168.40.1) au WebIntranet (172.18.0.20)
- 3-Blocage des VLAN 150 (Visiteurs) et 200 (Démonstration) vers AD
- 4-Interdiction du VLAN 200 d'accéder à Internet (sortie NAT simulée ici)

```
Routeur-GSB(config)#access-list 103 deny ip 192.168.200.0 0.0.0.255 any
Routeur-GSB(config)#access-list 103 permit ip any any
Routeur-GSB(config)#int gi0/1
Routeur-GSB(config-if)#ip access-group 103 in
Routeur-GSB(config-if)#exit
```

```
Routeur-GSB(config)#$ 102 deny ip 192.168.150.0 0.0.0.255 host 172.18.0.30
Routeur-GSB(config)#$ 102 deny ip 192.168.200.0 0.0.0.255 host 172.18.0.30
Routeur-GSB(config)#ac
Routeur-GSB(config)#access-list 102 permit ip any any
Routeur-GSB(config)#int gi0/0.150
Routeur-GSB(config-subif)#ip access-group 102 in
Routeur-GSB(config-subif)#exit
Routeur-GSB(config)#int gi0/0.200
Routeur-GSB(config-subif)#ip access-group 102 in
Routeur-GSB(config-subif)#exit
```

```
Routeur-GSB(config)#access-list 101 permit ip any any
Routeur-GSB(config)#int gi0/0.40
Routeur-GSB(config-subif)#ip access-group 101 in
```

```
Routeur-GSB(config)#$ 101 deny ip host 192.168.40.1 host 172.18.0.20
```

A7- Sauvegarde

Ce que j'ai fait :

- Sauvegarde des configurations (routeur/switches) via TFTP sur le serveur 172.18.0.50.
- Vérification avec `show archive`.

Pourquoi :
→ Pour assurer la restauration en cas d'incident (B1.1 - Gestion des sauvegardes).

```
Routeur-GSB#copy running-config tftp
Address or name of remote host []? 172.18.0.50
Destination filename [routeur-gsb-confg]? routeur-gsb-config
```