

<b>DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE</b>		N° réalisation :
Nom, prénom :		N° candidat :
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : ..... / ..... /.....
Organisation support de la réalisation professionnelle		
Intitulé de la réalisation professionnelle		
Période de réalisation : ..... Lieu : .....		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
<b>Compétences travaillées</b> <input type="checkbox"/> Concevoir une solution d'infrastructure réseau <input type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation <sup>1</sup> (ressources fournies, résultats attendus)		
Description des ressources documentaires, matérielles et logicielles utilisées <sup>2</sup>		
Modalités d'accès aux productions <sup>3</sup> et à leur documentation <sup>4</sup>		

<sup>1</sup> En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

<sup>2</sup> Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

<sup>3</sup> Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

<sup>4</sup> Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

**ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle  
(verso, éventuellement pages suivantes)**

**Épreuve E6 - Administration des systèmes et des réseaux (option SISR)**

**Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**



**BTS Services Informatiques aux  
Organisations  
Opt SISR**

**Gabriel Pilarski**

SIO 26

# ***Projet Personnel Encadré Numéro 1***

## Présentation du projet

Ce projet s'inscrit dans le cadre du BTS SIO, option SISR.

Il consiste à mettre en place une **architecture réseau segmentée** pour une entreprise disposant de **deux bâtiments (Bâtiment A et Bâtiment B)** ainsi que d'un **local technique**.

L'entreprise utilise plusieurs types d'équipements (postes utilisateurs, serveur RADIUS, postes partenaires), ce qui nécessite une **organisation claire du réseau** afin d'améliorer la **sécurité**, la **gestion des accès** et la **disponibilité** de l'infrastructure.

---

## Contexte et situation initiale

Dans la situation initiale, l'ensemble des équipements réseau n'était pas correctement segmenté, ce qui pouvait entraîner :

- Des risques de sécurité,
- Une mauvaise isolation des services,
- Une gestion plus complexe des accès entre les utilisateurs internes, externes et techniques.
- 

Il était donc nécessaire de **repenser l'architecture réseau** afin de séparer les flux.

L'entreprise fait donc appel à une entreprise experte en segmentation réseau, l'entreprise EVT ( Expert Vlan Trunking ) pour segmenter les différentes parties de son réseau et donc clarifier l'organisation.

---

## Problématique ?

Comment segmenter le réseau de l'entreprise entre plusieurs bâtiments et services afin d'améliorer la sécurité, la gestion des accès et l'administration du réseau, tout en permettant une communication fluide et règlementer ?

## Objectifs du projet

Les objectifs principaux du projet sont :

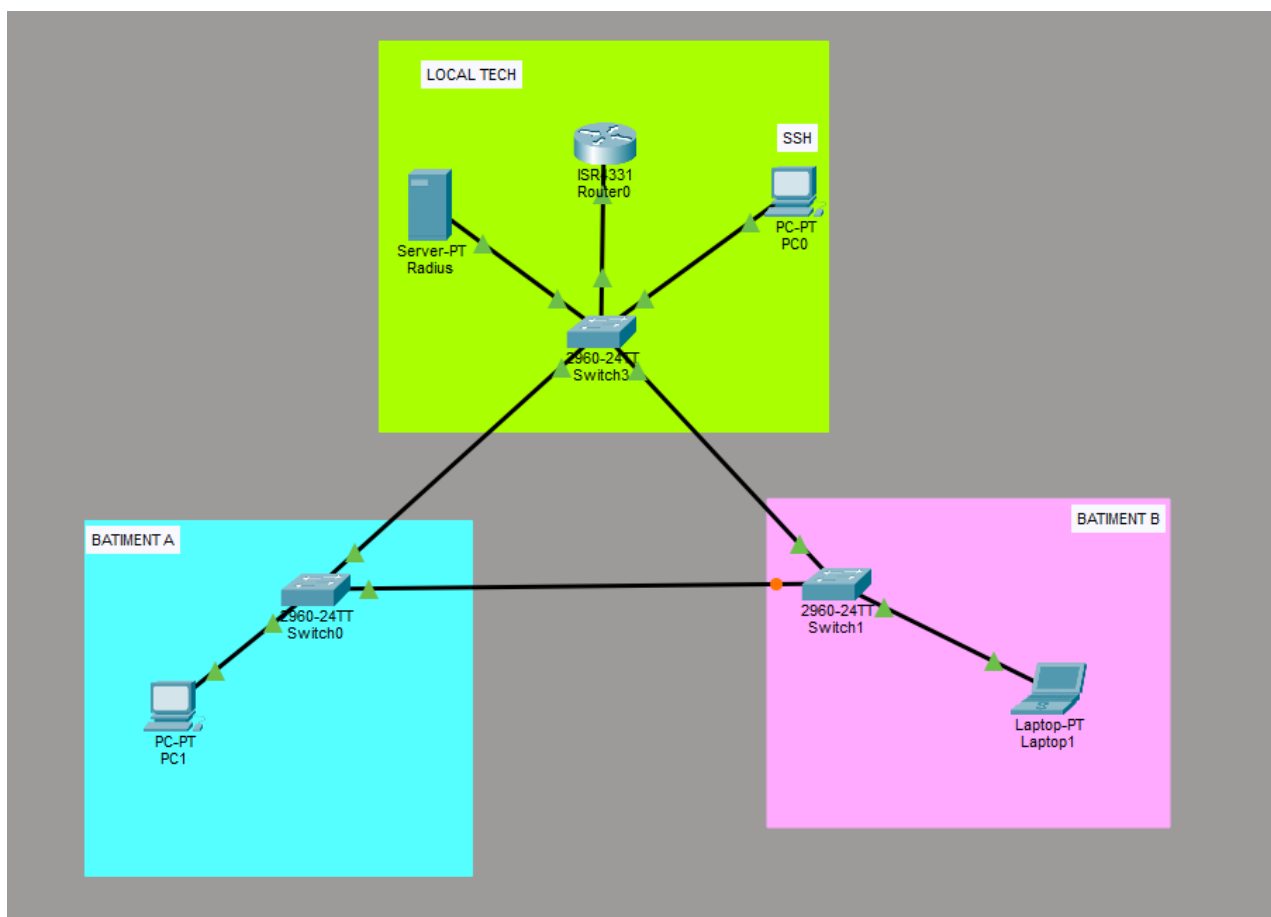
- Segmenter le réseau à l'aide de **VLAN** selon les usages et les profils d'utilisateurs
- Mettre en place des **liaisons trunk** entre les switches pour transporter plusieurs VLAN sur un même câble physique.
- Isoler les équipements sensibles, notamment le **serveur RADIUS**
- Contrôler les accès entre les différents VLAN

---

## Présentation de l'architecture réseau

L'architecture repose sur :

- Un **switch central** situé dans le local technique
- Deux switches d'accès situés dans le **bâtiment A** et le **bâtiment B**
- Un **routeur** assurant le routage inter-VLAN
- Un **serveur RADIUS** dédié à l'authentification
- Des postes utilisateurs répartis selon les bâtiments



---

## Organisation des VLAN

Voici le plan fait par l'entreprise EVT pour la méthode de segmentation des réseaux.

Le réseau est découpé en plusieurs VLAN afin d'isoler les usages :

- **VLAN 20 – Bureautique**  
Regroupe les postes internes des utilisateurs ainsi que le poste administrateur.
- **VLAN 40 – Partenaires**  
Destiné aux postes externes du bâtiment B, avec des droits d'accès limités.
- **VLAN 50 – RADIUS**  
VLAN dédié au serveur RADIUS, accessible uniquement depuis le bâtiment A et le service technique.

Cette segmentation permet une meilleure sécurité et une gestion plus efficace du réseau.

---

## Sécurité et restrictions d'accès

Le serveur RADIUS est placé dans un VLAN spécifique afin de protéger ce service sensible. Les accès sont volontairement restreints :

- Le **bâtiment A** et le **service technique** peuvent accéder au serveur RADIUS
- Le **bâtiment B** n'a pas accès à ce VLAN

Cette configuration permet de limiter les risques d'intrusion et de respecter le principe du moindre privilège.

---

## Conclusion de la présentation

Ce projet permet de mettre en œuvre une **architecture réseau structurée et sécurisée**, basée sur l'utilisation de VLAN, de trunks et du routage inter-VLAN.

Il répond aux besoins de l'entreprise tout en améliorant la sécurité, la lisibilité et l'évolutivité du réseau.

## Annexe :

- **Configuration R1**

```
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
ip access-group ACL_VLAN40 in
interface GigabitEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.0
ip access-list extended ACL_VLAN40
deny ip 192.168.40.0 0.0.0.255 host 192.168.50.2
permit ip any any
```

- **Configuration Switch types :**

**\*\*SW1 (Bât A — 192.168.50.4) \*\***

```
interface Vlan50
ip address 192.168.50.4 255.255.255.0
ip access-group ACL_V50_IN in
ip access-list extended ACL_V50_IN
deny ip 192.168.40.0 0.0.0.255 host 192.168.50.2
permit ip any any
radius-server host 192.168.50.2 auth-port 1812 acct-port 1813 key 123456
```

**\*\*SW2 (Bât B — 192.168.50.5)\*\***

```
interface Vlan50
ip address 192.168.50.5 255.255.255.0
ip access-group ACL_V50_IN in
ip access-list extended ACL_V50_IN
deny ip 192.168.40.0 0.0.0.255 host 192.168.50.2
permit ip any any
radius-server host 192.168.50.2 auth-port 1812 acct-port 1813 key 123456
```

**\*\*SW3 (Local Tech — 192.168.50.6)\*\***

```
interface Vlan50
ip address 192.168.50.6 255.255.255.0
ip access-list extended ACL_V50_IN
deny ip 192.168.40.0 0.0.0.255 host 192.168.50.2
permit ip any any
radius server NPS
address ipv4 192.168.50.2 auth-port 1812 acct-port 1813
key 123456
```

**\*\*Commun à tous les équipements\***

```
aaa new-model
aaa group server radius RAD-GRP
server name NPS
aaa authentication login SSH-AUTH group radius local
aaa authorization exec SSH-AUTH group radius local
ip ssh version 2
```

- **Serveur radius**

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
  - Clients RADIUS
  - Groupes de serveurs RA
- Stratégies
  - Stratégies de demande
  - Stratégies réseau
  - Gestion
  - Gestion des modèles

**Stratégies réseau**

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou...

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
accès_admin_equipements	Activé	1	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	999999	Refuser l'accès	Non spécifié

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
  - Clients RADIUS
  - Groupes de serveurs RA
- Stratégies
  - Stratégies de demande
  - Stratégies réseau
  - Gestion
  - Gestion des modèles

**Clients RADIUS**

Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fo...

Nom convivial	Adresse IP	Fabricant du périphérique	État
R1	192.168.50.1	RADIUS Standard	Activé
SW1	192.168.50.4	RADIUS Standard	Activé
SW2	192.168.50.5	RADIUS Standard	Activé
SW3	192.168.50.6	RADIUS Standard	Activé