PPE 1 - SWITCHING

Architecture réseau PME - Greentech

LANGLET Eloïse
SIO26

Sommaire

I- Contexte

- GreenTech Réparation est une PME spécialisée dans la réparation et le reconditionnement d'équipements électroniques. L'entreprise vient d'acquérir ses premiers locaux et souhaite mettre en place une infrastructure réseau adaptée à son activité.
- Elle dispose de plusieurs services :
  - Un atelier de réparation
  - Un service administratif
  - Un service comptabilité
  - Un service informatique
- Ces services manipulent des données sensibles (clients, finances, salaires). Il est donc nécessaire de garantir la sécurité, la fiabilité et la confidentialité des informations.
- Le gérant souhaite disposer d'un réseau simple à administrer, évolutif et respectant un budget limité. L'objectif est donc de concevoir une architecture réseau performante, sécurisée et adaptée aux besoins de l'entreprise.

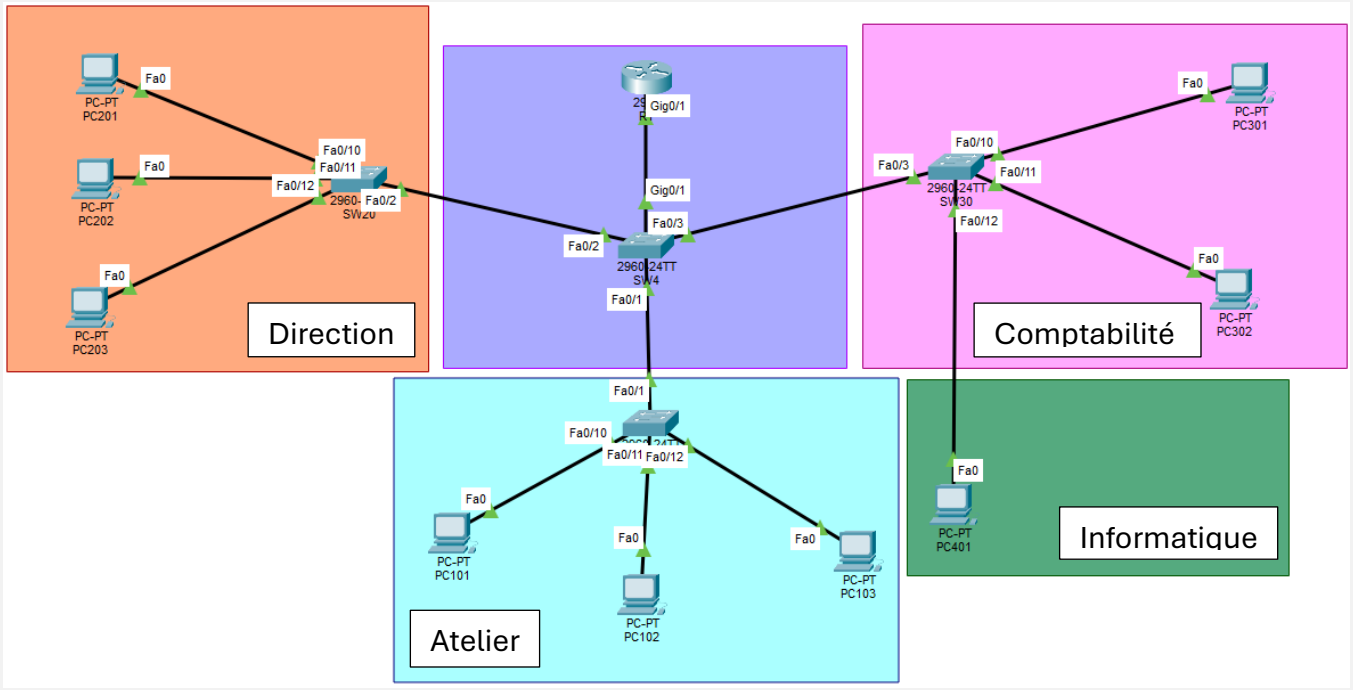
II- Analyses des besoins et missions

- Afin de répondre aux besoins du gérant et d'assurer un fonctionnement optimal de l'infrastructure réseau, une analyse des besoins a été réalisée. Les tableaux ci-dessous présentent les principales problématiques identifiées, les risques associés, ainsi que les solutions mises en œuvre J'ai distingué les besoins explicites du gérant et, les besoins structurels et techniques de l'entreprise.

Besoins du gérant / de l'entreprise	Problématique identifiée	Risques si la problématique n'est pas traitée	Objectif informatique	Solution informatique
Séparer les services	Réseau unique	Fuite de données, mauvaise sécurité, ralentissements	Isoler les services, sécurité	Création de VLANs (10, 20, 30, 40)
Bloquer Internet pour l'atelier	Les machines de réparation n'ont pas besoin d'y avoir accès	Virus, piratage, perte de productivité	Bloquer l'accès Internet au VLAN Atelier	ACL sur le routeur
Protéger les données sensibles	Données financières exposées	Vol d'informations, problèmes juridiques	Sécuriser les échanges réseau	Segmentation VLAN + Règles ACL
Centraliser l'administration du réseau	Gestion difficile sans accès global	Pannes longues, mauvaise maintenance	Donner un accès total à l'informatique	VLAN 40 avec autorisation complète
Simplifier l'attribution des adresses IP	Configuration manuelle fastidieuse	Erreurs IP, conflits réseau	Automatiser l'adressage	Mise en place de DHCP sur le routeur

Besoins structurels de l'entreprise	Problématique identifiée	Risques si la problématique n'est pas traitée	Objectif informatique	Solution informatique
Assurer une communication entre les équipements	VLANs séparés	Impossibilité d'échanger	Permettre le routage inter-VLAN	Routeur avec sous-interfaces
Sécuriser l'accès aux équipements réseau	Accès non contrôlé	Intrusion, sabotage	Restreindre l'administration	Configuration de SSH
Permettre le transport de plusieurs VLANs	Plusieurs VLANs sur un lien	Blocage des communications	Transporter les VLANs	Configuration des ports trunk
Faciliter la maintenance du réseau	Manque de traçabilité	Difficulté de dépannage	Identifier les équipements	Nommage, bannière, documentation
Garantir la stabilité du réseau	Connexions instables	Coupures réseau	Optimiser les ports	PortFast, configuration adaptée

III- Architecture réseau



Sur le schéma ci-contre, le routeur R1 assurer le routage inter-VLAN et le service DHCP. Les switches SW10, SW20, SW30 et SW40 assurent la distribution réseau. Les liaisons trunk permettent le transport de plusieurs VLANs. Chaque service est isolé dans un VLAN spécifique afin de renforcer la sécurité.

IV- Adressage IP

VLAN	Service	Réseau	Pool
10	Atelier	192.168.10.0/24	192.168.10.10 – 192.168.10.50
20	Administration	192.168.20.0/24	192.168.20.10 – 192.168.20.50
30	Comptabilité	192.168.30.0/24	192.168.30.10 – 192.168.30.50
40	IT	192.168.40.0/24	192.168.40.10 – 192.168.40.50

Le plan d'adressage a été conçu afin d'assurer une organisation claire et évolutive. Ce plan permet une identification rapide des équipements par service.

V- Mise en œuvre des configurations

Switches 10, 20

❖ **Configuration de base:**

```
Enable
conf t
hostname SWX0
no ip domain-lookup
enable secret SIO26
banner motd #Acces strictement reserve#
ip domain-name SIO
crypto key generate rsa general-keys modulus 1024
username elanglet privilege 15 secret SIO26
ip ssh version 2
line vty 0 15
password SIO26
login local
transport input ssh
line con 0
login
```

❖ **Configuration spécifique :**

Pour la suite de la configuration j'ai créé les VLANs et je les ai associés aux ports correspondants. Les ports utilisateurs sont configurés en mode access avec PortFast afin d'améliorer la rapidité de connexion.

```
vlan X0
name VLANX0-XXX
exit
interface vlan X0
ip address 192.168.X0.2 255.255.255.0
no shutdown
interface fastethernet 0/X
switchport mode access
```

<table>
<tr><td>Switches 10, 20</td><td>switchport access vlan X0
spanning-tree portfast
interface fastethernet 0/10
switchport mode access
switchport access vlan X0
spanning-tree portfast
interface fastethernet 0/11
switchport mode access
switchport access vlan X0
spanning-tree portfast
interface fastethernet 0/12
switchport mode access
switchport access vlan X0
spanning-tree portfast
service password-encryption
end
wr</td></tr>
<tr><td>Switch 30</td><td><u>J’ai repris la configuration de base :</u>
- Nom
- Domaine
- Mots de passe + chiffrement des mots de passe
- Bannière
- SSH
- Création des VLANs 30 et 40

J’ai configuré le port Fa0/3 en mode trunk pour qu’il puisse transporter et accepter les trames des VLANs 30 et 40.</td></tr>
<tr><td>Switch 40</td><td><u>J’ai repris la configuration de base :</u>
- Nom
- Domaine
- Mots de passe + chiffrement des mots de passe
- Bannière
- SSH
- Configuration des interfaces
- Sauvegarde de la configuration

❖ <u>Création des VLANs + attribution des adresses IPs (faites pour chaque VLAN) :</u>
vlan 10
name VLAN10-Atelier
exit
interface vlan 10
ip address 192.168.10.2 255.255.255.0
no shutdown

❖ <u>Création des interfaces trunks :</u>
- <u>Vers le switch SW30:</u>
interface fastethernet 0/3
description TRUNK_vers_SW30</td></tr>
</table>

<table>
<tr><td>Switch 40</td><td>
switchport mode trunk
switchport trunk allowed vlan 30,40
no shutdown
- <u>Vers le routeur R1:</u>
interface gigabitethernet 0/1
description Trunk_vers_routeur_R1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
no shutdown
</td></tr>
<tr><td>Routeur</td><td>
<u>J’ai repris la configuration de base:</u>
- Nom
- Domaine
- SSH
- Mots de passe + chiffrement des mots de passe
- Création des VLANs + activation des interfaces
- Sauvegarde de la configuration

❖ <u>Configuration des sous-interfaces :</u>
Le routeur assure le routage inter-VLAN à l’aide de sous-interfaces. Chaque VLAN possède une sous-interface avec son adresse IP passerelle. En voici un exemple :
interface g0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

❖ <u>Configuration de DHCP:</u>
- <u>Exclusions d’adresses (faites pour chaque VLAN) :</u>
ip dhcp excluded-address 192.168.10.1 192.168.10.9
- <u>Pools DHCP (faits pour chaque VLAN) :</u>
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8

❖ <u>ACL :</u>
- <u>ACL étendue :</u>
ip access-list extended SECURITE-VLAN
- <u>Bloquer VLAN 10 vers Internet:</u>
deny ip 192.168.10.0 0.0.0.255 any
- <u>Autoriser le VLAN 40 à avoir un accès total au sein de l’infrastructure :</u>
permit ip 192.168.40.0 0.0.0.255 any
- <u>Restreindre les VLANs 20 et 30 :</u>
permit icmp 192.168.20.0 0.0.0.255 host 192.168.20.1
permit ip 192.168.20.0 0.0.0.0.255 192.168.20.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 any
- <u>Application de l’ACL étendue sur la bonne interface :</u>
interface g0/1.X0
ip access-group SECURITE-VLAN in
- <u>Autoriser les requêtes DHCP:</u>
permit udp any eq 68 any eq 67
permit udp any eq 67 any eq 68
</td></tr>
</table>

VI- Tests et validation

❖ **Plusieurs tests ont été réalisés :**

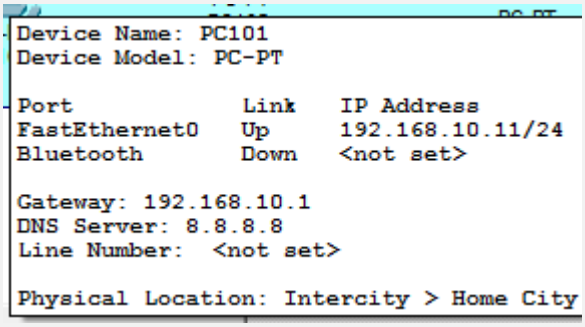
- Test DHCP : attribution automatique des IP,
- Test ping entre VLANs,
- Test accès Internet,
- Test ACL,
- Test accès SSH.

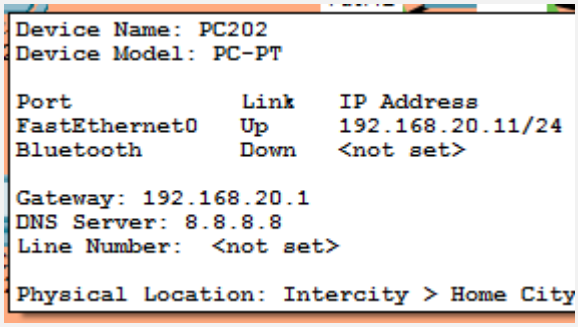
❖ **Résutats :**

- Le VLAN 10 n'a pas accès à Internet,
- Le VLAN 40 accède à tous les réseaux,
- Les autres VLANs sont restreints,
- Le DHCP fonctionne correctement,
- L'infrastructure est conforme aux attentes.

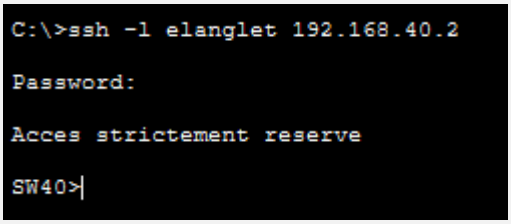
❖ **Exemples :**

L'un des PCs de l'atelier (VLAN10) récupère une adresse IP en lien avec son VLAN. Idem pour l'un des PCs du VLAN 20.





La connexion SSH sur les équipements réseau est fonctionnelle.



VII- Annexes

Les mots de passe seront tous : SIO26

Le domaine : SIO

SSH username : elanglet