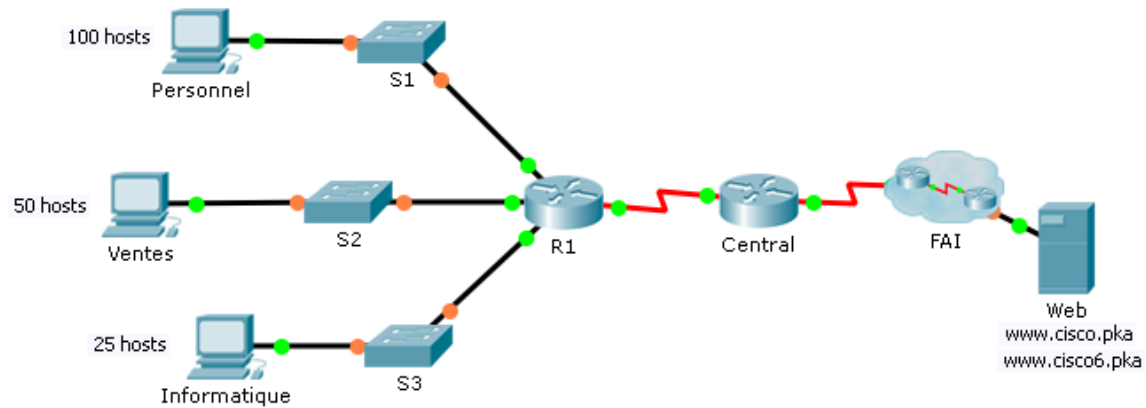


# Packet Tracer - Exercice d'intégration des compétences

## Topologie



## Table d'adressage

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
		Adresse/Préfixe IPv6	Adresse IPv6 link-local	
R1	G0/0			N/A
		2001:DB8:ACAD::1/64	FE80::1	N/A
	G0/1			N/A
		2001:DB8:ACAD:1::1/64	FE80::1	N/A
	G0/2			N/A
		2001:DB8:ACAD:2::1/64	FE80::1	N/A
Central	S0/0/0	172.16.1.2	255.255.255.252	N/A
		2001:DB8:2::1/64	FE80::1	N/A
	S0/0/1	209.165.200.226	255.255.255.252	N/A
		2001:DB8:1::1/64	FE80::2	N/A
S1	VLAN 1			
S2	VLAN 1			
S3	VLAN 1			
Personnel	Carte réseau			
		2001:DB8:ACAD::2/64	FE80::2	FE80::1
Ventes	Carte réseau			
		2001:DB8:ACAD:1::2/64	FE80::2	FE80::1
IT	Carte réseau			
		2001:DB8:ACAD:2::2/64	FE80::2	FE80::1
Web	Carte réseau	64.100.0.3	255.255.255.248	64.100.0.1
		2001:DB8:CAFE::3/64	FE80::2	FE80::1

## Contexte/scénario

Le routeur Central, le cluster ISP et le serveur web sont complètement configurés. Il vous a été demandé de créer un nouveau schéma d'adressage IPv4 comprenant 4 sous-réseaux au moyen du réseau 192.168.0.0/24. Le département IT a besoin de 25 hôtes. Le département des ventes a besoin de 50 hôtes. Le sous-réseau du reste de l'équipe a besoin de 100 hôtes. Un sous-réseau invité de 25 hôtes sera ajouté ultérieurement. Il vous a également été demandé de finaliser les paramètres de sécurité de base ainsi que les configurations des interfaces sur R1. Vous devrez aussi configurer l'interface SVI et la sécurité de base sur les commutateurs S1, S2 et S3.

### Conditions requises

#### Adressage IPv4

- Créez des sous-réseaux qui satisfont les besoins des hôtes en utilisant l'adresse 192.168.0.0/24.
  - Staff : 100 hôtes
  - Ventes : 50 hôtes
  - IT : 25 hôtes
  - Réseau invité à ajouter ultérieurement : 25 hôtes
- Documentez les adresses IPv4 attribuées dans la table d'adressage.
- Enregistrez le sous-réseau du réseau invité : \_\_\_\_\_

#### Configurations des PC

- Configurez l'adresse IPv4 attribuée, le masque de sous-réseau et la passerelle par défaut des PC Personnel, Ventes et IT, conformément à votre schéma d'adressage.
- Attribuez les adresses IPv6 de monodiffusion et link-local ainsi que la passerelle par défaut des réseaux Personnel, Ventes et IT, conformément à la table d'adressage.

#### Configurations de R1

- Configurez le nom du périphérique conformément à la table d'adressage.
- Désactivez la recherche DNS.
- Attribuez **Ciscoenpa55** comme mot de passe chiffré du mode d'exécution privilégié.
- Attribuez **Ciscoconpa55** comme mot de passe de console et activez la connexion.
- 10 caractères minimum doivent être utilisés pour tous les mots de passe.
- Chiffrez tous les mots de passe en clair.
- Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit. Veillez à inclure le terme **Warning** (Avertissement) dans la bannière.
- Configurez toutes les interfaces Gigabit Ethernet.
  - Configurez les adresses IPv4 conformément à votre schéma d'adressage.
  - Configurez les adresses IPv6 conformément à la table d'adressage.
- Configurez le protocole SSH sur R1 :
  - Choisissez le nom de domaine **CCNA-lab.com**.
  - Générez une clé RSA de **1024** bits.
  - Configurez les lignes VTY pour l'accès SSH.
  - Utilisez les profils utilisateur locaux pour l'authentification.
  - Créez un utilisateur **Admin1** avec un niveau de privilèges défini à **15** à l'aide du mot de passe chiffré pour **Admin1pa55**.
- Configurez la console et les lignes VTY de telle sorte qu'elles se déconnectent après cinq minutes d'inactivité.
- Bloquez pendant trois minutes quiconque n'arrive pas à se connecter au bout de quatre tentatives en deux minutes.

## Configurations des commutateurs

- Configurez le nom du périphérique conformément à la table d'adressage.
- Configurez l'interface SVI avec l'adresse IPv4 et le masque de sous-réseau définis dans votre schéma d'adressage.
- Configurez la passerelle par défaut.
- Désactivez la recherche DNS.
- Attribuez **Ciscoenpa55** comme mot de passe chiffré du mode d'exécution privilégié.
- Attribuez **Ciscoconpa55** comme mot de passe de console et activez la connexion.
- Configurez la console et les lignes VTY de telle sorte qu'elles se déconnectent après cinq minutes d'inactivité.
- Chiffrez tous les mots de passe en clair.

## Vérification de la connectivité

- Accédez à **www.cisco.pka** à l'aide du navigateur web à partir des PC Personnel, Ventes et IT.
- Accédez à **www.cisco6.pka** à l'aide du navigateur web à partir des PC Personnel, Ventes et IT.
- Tous les PC sont censés pouvoir envoyer des requêtes ping vers tous les périphériques.