

Important : Réalisez l'ensemble des tâches en capturant les étapes dans un fichier Word (Pensez à alimenter votre portefeuille à partir de ce TP)

# TP01 : Réseau local

## Topologie :

### 1. Serveurs :

- Serveur DHCP : 192.168.1.250/24 (Connecté au switch1)
- Serveur WEB : 192.168.1.251/24 (Connecté au switch1)
- Serveur DNS : 192.168.1.252/24 (Connecté au switch1)

### 2. Ordinateurs :

- PC1 : Configuration via DHCP (Connecté au switch1)
- PC2 : Configuration via DHCP (Connecté au switch1)
- Laptop1 : Configuration via DHCP (Connecté à l'Access Point 1)

### 3. Interconnexion :

- Access Point 1 connecté au Switch1
- Routeur1 connecté au Switch1 (192.168.1.1/24)
- Routeur1 connecté à Routeur2 (1.1.1.2/30)
- Routeur2 connecté à Routeur1 (1.1.1.1/30)

## Travail à faire :

### 1. Réalisez la topologie ci-dessus sur Cisco Packet Tracer :

- Utilisez le routeur Cisco 2911 et le commutateur Cisco 2960 pour créer la topologie réseau.
- **Astuce** : Organisez les équipements de manière logique pour représenter la segmentation du réseau et faciliter le dépannage.

### 2. Configurer le Serveur DHCP :

- Configurez une plage d'adresses de 192.168.1.10 à 192.168.1.110.
- Définissez la passerelle par défaut sur 192.168.1.1.
- Définissez le serveur DNS sur 192.168.1.252.
- **Explication** : Le DHCP automatise l'attribution d'adresses IP, de passerelles et de serveurs DNS, ce qui simplifie la gestion du réseau.

### 3. Configurer le Serveur DNS :

- Ajoutez un enregistrement de type A pour le domaine www.sisr2.local pointant vers l'adresse IP du serveur Web (192.168.1.251).
- **Explication** : Le DNS (Domain Name System) est utilisé pour résoudre les noms de domaine en adresses IP, ce qui permet aux utilisateurs d'accéder aux services en utilisant des noms de domaine faciles à retenir.

### 4. Configurer le Serveur Web :

- Modifiez le fichier index.html pour personnaliser le contenu de la page web.

- **Explication :** Cette étape permet de s'assurer que le serveur Web est correctement configuré et que les utilisateurs peuvent accéder à la page web via le réseau.

#### 5. **Tester la Connectivité (ICMP) :**

- Utilisez la commande ping pour vérifier la connectivité entre tous les périphériques (PC1, PC2, Laptop1, serveurs, routeurs).
- **Explication :** Les pings aident à vérifier la connectivité réseau et à diagnostiquer les problèmes de communication.

#### 6. **Tester la Résolution de Noms (DNS) :**

- Exécutez la commande ping `www.sisr2.local` sur le PC portable Laptop1.
- **Explication :** Cela teste à la fois la connectivité réseau et la résolution de noms DNS.

#### 7. **Accéder au Site Web via PC1 :**

- Accédez au site web `www.sisr2.local` depuis PC1 en utilisant un navigateur.
- **Explication :** Confirmez que le serveur Web est accessible sur le réseau local et que la résolution DNS fonctionne correctement.

#### 8. **Surveillance du Trafic en Mode Simulation :**

- Activez le mode simulation dans Cisco Packet Tracer.
- Surveillez et documentez le trafic **ICMP** entre les périphériques.
- Surveillez et documentez le trafic **DHCP** lors de l'attribution des adresses IP.
- Surveillez et documentez le trafic **DNS** lors de la résolution de noms.
- Surveillez et documentez le trafic **HTTP** lors de l'accès au site web.
- **Explication :** Le mode simulation permet de visualiser et d'analyser le comportement du réseau en détail.

#### 9. **Étude de Cas : Problèmes de Connectivité :**

- Imaginez que PC1 ne parvienne pas à se connecter à `www.sisr2.local`. Diagnostiquez le problème potentiel et proposez une solution.
- **Questions de Réflexion :**
  - Comment diagnostiqueriez-vous un problème de configuration DHCP ?
  - Que se passe-t-il si le serveur DNS est mal configuré ?
  - Quelles commandes et outils utiliseriez-vous pour dépanner un problème de connectivité réseau ?

#### 10. **Concepts Avancés : Sécurité et VLANs :**

- **Configurer des ACL (Access Control Lists) sur les Routeurs :**
  - Bloquez le trafic ICMP entre certaines parties du réseau pour des raisons de sécurité.
  - **Explication :** Les ACL sont utilisées pour contrôler le trafic réseau et sécuriser les segments de réseau sensibles.
- **Configurer des VLANs sur le Switch :**
  - Créez des VLANs distincts pour les serveurs et les utilisateurs pour segmenter le trafic réseau.

- **Explication :** La segmentation de réseau via des VLANs améliore la sécurité et la performance en isolant les domaines de diffusion.

#### 11. Créer une Documentation Complète :

- Pour chaque étape, documentez les configurations, les commandes utilisées et les résultats observés.
- **Explication :** La documentation est essentielle pour la gestion continue du réseau et pour faciliter le dépannage à l'avenir.