# Pratique des réseaux

## SR200

## Livret d’ateliers

# Table des matières

# Atelier 1 : Réaliser une première utilisation de la commande « ping »

```
C:\>ping -h
Option incorrecte -h.

Utilisation : ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
              [-r count] [-s count] [[-j host-list] | [-k host-list]]
              [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
              [-4] [-6] nom_cible

Options :
    -t             Effectue un test ping sur l'hôte spécifié jusqu'à son arrêt.
                   Pour afficher les statistiques et continuer,
                   appuyez sur Ctrl+Attn.
                   Pour arrêter, appuyez sur Ctrl+C.
    -a             Résout les adresses en noms d'hôtes.
    -n count       Nombre de demandes d'écho à envoyer.
    -l size        Taille du tampon d'envoi.
    -f             Active l'indicateur Ne pas fragmenter dans le paquet (IPv4
                   uniquement).
    -i TTL         Durée de vie.
    -v TOS         Type de service (IPv4 uniquement. La
                   configuration de ce paramètre n'a aucun effet sur le type
                   de service dans l'en-tête IP).
    -r count       Itinéraire d'enregistrement du nombre de sauts (IPv4
                   uniquement).
    -s count       Horodatage du nombre de sauts (IPv4 uniquement).
    -j host-list   Itinéraire source libre parmi la liste d'hôtes (IPv4
                   uniquement).
    -k host-list   Itinéraire source strict parmi la liste d'hôtes (IPv4
                   uniquement).
    -w timeout     Délai d'attente pour chaque réponse, en millisecondes.
    -R             Utilise l'en-tête de routage pour tester également
                   l'itinéraire inverse (IPv6 uniquement).
                   D'après la RFC 5095, l'utilisation de cet en-tête de routage
                   est déconseillée. Certains systèmes peuvent supprimer des
                   demandes d'écho si cet en-tête est utilisé.
    -S srcaddr     Adresse source à utiliser.
    -c compartment Identificateur de compartiment de routage.
    -p             Effectue un test ping sur l'adresse de fournisseur
                   de la virtualisation réseau Hyper-V.
    -4             Force l'utilisation d'IPv4.
    -6             Force l'utilisation d'IPv6.


C:\>
```

**Objectif** : Cet atelier a pour but de vous familiariser avec l'une des commandes les plus fondamentales en réseau - la commande "ping". Vous apprendrez à tester la présence et la réactivité d'une machine sur le réseau en utilisant cette commande simple mais puissante.

**Matériel Nécessaire** :

- Un ordinateur connecté à un réseau (local ou Internet).

**Instructions** :

1. Ouvrez l'invite de commande (Windows) ou le terminal (macOS/Linux).
2. Tapez la commande suivante. en remplaçant <adresseIP> par l'adresse IP de la machine que vous souhaitez tester (par exemple. l'adresse IP de Google est souvent utilisée pour ce type de test : 8.8.8.8).
3. ping <adresseIP>
4. Observez les résultats retournés par la commande.
5. Répétez l'opération en utilisant l'adresse d'un site web que vous connaissez. par exemple : ping www.google.com
6. Notez vos observations et réfléchissez à ce que signifient les différentes réponses obtenues de la commande ping.

**Résultat Attendu** : Vous devriez voir une série de réponses indiquant le temps (en millisecondes) nécessaire pour que les paquets atteignent la destination et reviennent à votre machine. Si la destination n'est pas accessible. la commande ping indiquera une erreur de timeout ou une impossibilité de joindre l'hôte.

- Guide pas à pas pour la Correction **:**

**Vérification des Étapes** :

1. **Ouverture de l'Invite de Commande / Terminal** :
    1. Assurez-vous que les participants ont correctement accédé à l'interface de commande de leur système d'exploitation.
2. **Exécution de la Commande Ping avec une Adresse IP** :
    1. Vérifiez que la commande a été correctement saisie : ping 8.8.8.8 (ou une autre adresse IP valide).
    2. Confirmez que les participants observent des lignes indiquant le temps de réponse. ce qui signifie que la machine distante est accessible.
3. **Exécution de la Commande Ping avec un Nom de Domaine** :
    1. Assurez-vous que la commande a été entrée correctement. par exemple : ping www.google.com.
    2. Validez que les résultats incluent à la fois la résolution du nom de domaine en adresse IP et les temps de réponse. démontrant que le DNS fonctionne correctement et que le site est accessible.
4. **Interprétation des Résultats** :
    1. Discutez des différents temps de réponse observés et de ce qu'ils impliquent sur la latence. sur la gigue (jitter). entre la source et la destination.
    2. Expliquez la signification d'une perte de paquets. si elle se produit. et ce que cela peut indiquer sur la qualité de la connexion réseau.
5. **Gestion des Erreurs** :
    1. Si un participant rencontre des messages d'erreur tels que "Request timed out" ou "Destination host unreachable". guidez-le à travers le diagnostic possible (problème de connexion. adresse IP incorrecte. ou le site cible ne répond pas).

**Affichage du résultat des commandes Ping**

```
C:\>ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=6 ms TTL=119
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=119
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=119
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=119

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 6ms, Maximum = 8ms, Moyenne = 7ms
```

```
C:\>ping www.fff.fr

Envoi d'une requête 'ping' sur www.fff.fr [18.239.208.61] avec 32 octets de données :
Réponse de 18.239.208.61 : octets=32 temps=15 ms TTL=247
Réponse de 18.239.208.61 : octets=32 temps=15 ms TTL=247
Réponse de 18.239.208.61 : octets=32 temps=16 ms TTL=247
Réponse de 18.239.208.61 : octets=32 temps=19 ms TTL=247

Statistiques Ping pour 18.239.208.61:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 15ms, Maximum = 19ms, Moyenne = 16ms
```

**Conclusion de l'Atelier** : Félicitez les participants pour avoir réussi cet atelier et encouragez-les à utiliser la commande ping comme un premier outil de diagnostic pour vérifier la connectivité réseau. Soulignez l'importance de comprendre comment les données voyagent à travers le réseau et comment des outils simples peuvent fournir des informations précieuses sur l'état du réseau.

# Atelier 2 : Situer une machine distante dans un réseau.

```
C:\>tracert /?

Utilisation : tracert [-d] [-h SautsMaxi] [-j ListeHôtes] [-w délai]
              [-R] [-S srcaddr] [-4] [-6] nom_cible

Options :
   -d                 Ne pas convertir les adresses en noms d'hôtes.
   -h SautsMaxi       Nombre maximum de sauts pour rechercher la cible.
   -j ListeHôtes      Itinéraire source libre parmi la liste des hôtes
                      (IPv4 uniquement).
   -w délai           Attente d'un délai en millisecondes pour chaque réponse.
   -R                 Chemin de suivi (IPv6 uniquement).
   -S srcaddr         Adresse source à utiliser (IPv6 uniquement).
   -4                 Force utilisant IPv4.
   -6                 Force utilisant IPv6.

C:\>
```

**Objectifs :**

- Situer une machine distante dans un réseau.
- Visualiser le chemin emprunté par les paquets.
- Savoir interpréter le résultat de la commande (perte de paquet. goulot d'étranglement. présence d'un firewall).

**Étapes prévues :**

1. Ouvrir un interpréteur de commande cmd.exe.
2. Saisir la syntaxe tracert 8.8.8.8. puis tracert -d 8.8.8.8 et comparer les résultats.
3. Répéter l'opération sur les machines destinations : www.sfr.fr. www.bnf.fr. www.fnac.fr.

**Constats :**

- La commande tracert -d s'affiche plus rapidement car elle ne fait pas de résolution DNS.
- Les premiers sauts sont identiques. car le départ est toujours le même.
- La présence d'astérisques (*) et leurs significations.
- Il est possible de visualiser les différents réseaux traversés et de localiser la source d'un problème.

- Guide pas à pas pour la Correction **:**

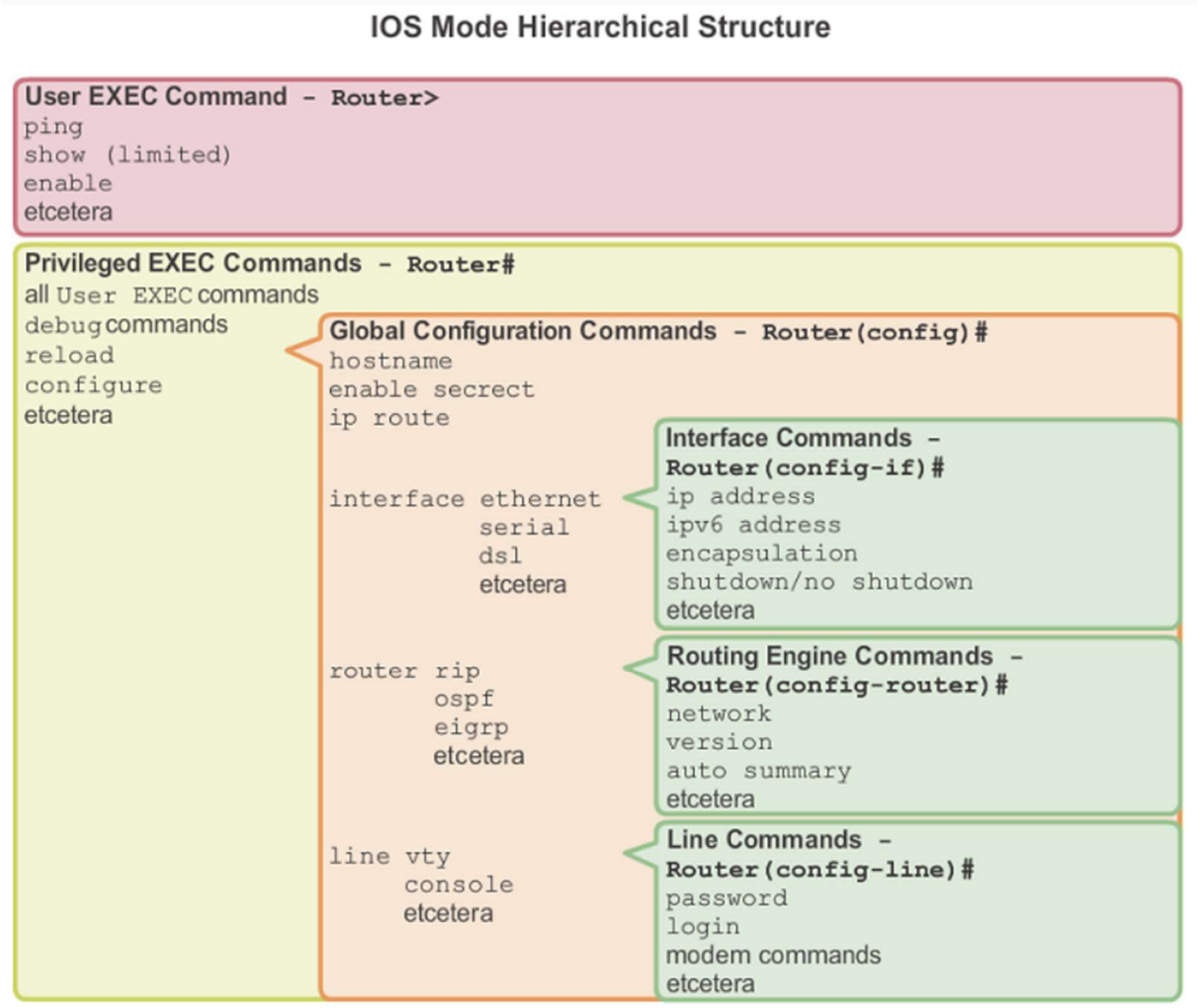
1. **Ouverture de l'interpréteur de commande :**
    1. Appuyez sur la touche Windows + R pour ouvrir la fenêtre Exécuter.
    2. Tapez "cmd" dans la zone de texte et appuyez sur Entrée pour ouvrir l'invite de commande.
2. **Exécution de la commande tracert :**
    1. Dans l'invite de commande. saisissez la commande suivante : tracert 8.8.8.8.
    2. Observez les résultats affichés. y compris les adresses IP des sauts intermédiaires.
3. **Comparaison avec la commande tracert -d:**
    1. Réexécutez la commande en utilisant la syntaxe tracert -d 8.8.8.8.
    2. Comparez les résultats avec la première commande pour noter les différences.
4. **Répétition de l'opération avec d'autres destinations :**
    1. Saisissez la commande tracert -d suivie des adresses des autres destinations : www.sfr.fr. www.bnf.fr. www.fnac.fr.
    2. Analysez les résultats pour identifier les routes empruntées par les paquets et détecter d'éventuels problèmes.
5. **Interprétation des résultats :**
    1. Notez la signification des astérisques (*) dans les résultats.
    2. Identifiez les éventuels goulets d'étranglement ou la présence de firewalls à partir des résultats obtenus.
6. **Discussion et conclusion :**
    1. Discutez des observations faites et des implications pour la résolution de problèmes réseau.
    2. Concluez sur l'importance de l'utilisation de l'outil tracert pour diagnostiquer les problèmes de connectivité et de performance réseau.

**Affichage du résultat des commandes Tracert**

```
Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

  1     1 ms     1 ms     1 ms  192.168.250.254
  2     8 ms     7 ms     7 ms  station11.multimania.isdnet.net [194.149.174.108]
  3     8 ms     *        *     station1.multimania.isdnet.net [194.149.174.98]
  4     7 ms     8 ms     7 ms  google2.par.franceix.net [37.49.236.2]
  5    10 ms    10 ms    11 ms  108.170.255.139
  6     9 ms    13 ms     8 ms  142.250.224.199
  7     7 ms     7 ms     8 ms  dns.google [8.8.8.8]

Itinéraire déterminé.
```

```
C:\>tracert -d 8.8.8.8

Détermination de l'itinéraire vers 8.8.8.8 avec un maximum de 30 sauts.

  1     3 ms     2 ms     1 ms  192.168.250.254
  2     8 ms     8 ms     7 ms  194.149.174.108
  3     9 ms     7 ms     8 ms  194.149.174.98
  4     7 ms     7 ms     7 ms  37.49.236.2
  5    10 ms     9 ms     9 ms  108.170.255.139
  6     8 ms    12 ms     7 ms  142.250.224.199
  7    19 ms    17 ms    18 ms  8.8.8.8

Itinéraire déterminé.

C:\>_
```

# Atelier 3 : Naviguer dans les modes de l'IOS pour nommer un switch




**Objectifs :**

- Naviguer dans les modes de l'IOS pour nommer un switch.
- Constater la différence entre la running config et la startup config.

Instructions pour les Stagiaires :

1. **Sauvegarder la running config** :
    1. Utilisez la commande copy running-config startup-config pour sauvegarder la configuration actuelle.
2. **Renommer l'équipement avec le nom SW0** :
    1. Accédez au mode de configuration globale en tapant configure terminal.
    2. Utilisez la commande hostname SW0 pour renommer l'équipement.
    3. Revenez au mode de configuration en tapant exit.

3. **Observations et Commentaires** :
    1. Observez les modifications apportées au prompt du switch suite au changement de nom.
    2. Réfléchissez aux implications de ce changement.
4. **Utiliser la commande Show running-config et Show startup-config** :
    1. Utilisez la commande show running-config pour afficher la configuration actuelle.
    2. Utilisez la commande show startup-config pour afficher la configuration de démarrage.
5. **Sauvegarder la configuration actuelle** :
    1. Utilisez à nouveau la commande copy running-config startup-config pour sauvegarder la configuration modifiée.
6. **Répéter l'opération pour nommer les équipements suivants en SW1 et SW2** :
    1. Suivez les mêmes étapes précédentes pour renommer les équipements SW1 et SW2.

- Guide pas à pas pour la Correction :

1. **Sauvegarder la running config** :

```lua
SWO# copy running-config startup-config
```

2. **Renommer l'équipement avec le nom SW0 :**

```arduino
SWO# configure terminal
SWO(config)# hostname SWO
SWO(config)# exit
```

3. **Observations et Commentaires :**
    1. Observer le changement de prompt après avoir renommé l'équipement.
4. **Utiliser la commande Show running-config et Show startup-config :**

```lua
SWO# show running-config
SWO# show startup-config
```

5. **Sauvegarder la configuration actuelle** :

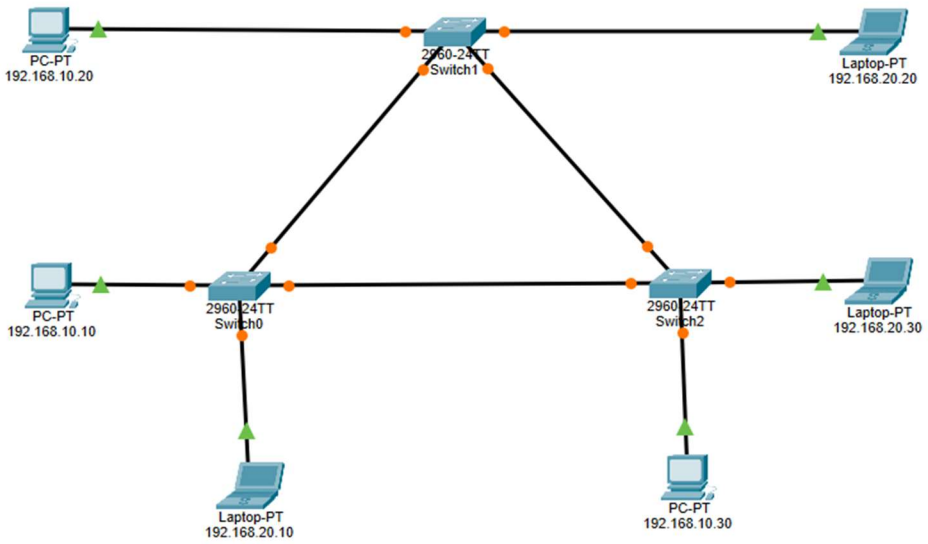
```lua
SWO# copy running-config startup-config
```

6. **Répéter l'opération pour nommer les équipements suivants en SW1 et SW2** :
    1. Répéter les mêmes étapes en remplaçant "SW0" par "SW1" pour SW1 et "SW2" pour SW2.

**Remarques :**

- Assurez-vous de suivre précisément les étapes fournies pour accomplir les objectifs de l'atelier.
- Prenez le temps d'observer les changements et de comprendre les commandes utilisées.

# Atelier 4 - Mise en œuvre du Spanning-Tree




**Objectifs :**

- Visualiser l'état du Spanning-Tree du laboratoire.
- Configurer les root-bridge.

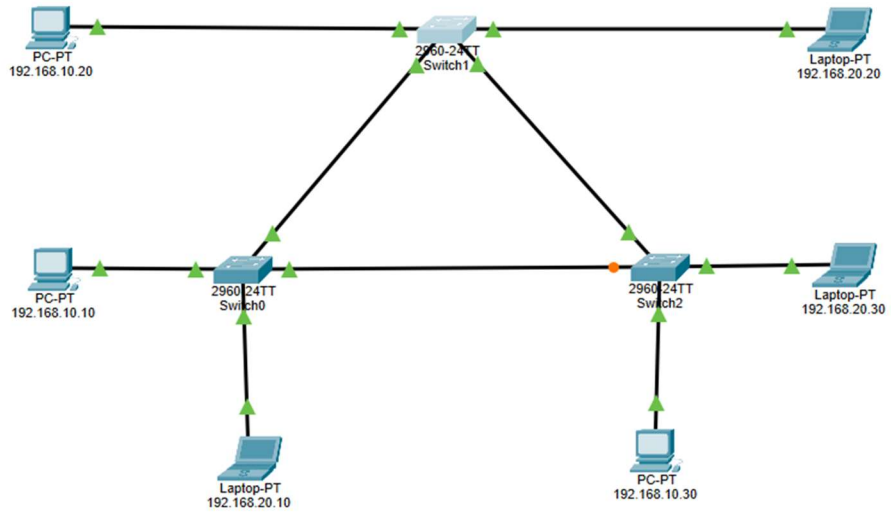
**Étapes prévues :**

1. Aller sur chacun des trois switch et exécuter la commande "show spanning-tree".
2. Observer les sorties de chaque switch et vérifier quel switch est le « root ».
3. Se rendre sur le SW1 pour le passer en « root » en utilisant la syntaxe "spanning-tree vlan 1 priority 0".
4. Toujours sur le SW1. visualiser le changement avec la commande "show spanning-tree".

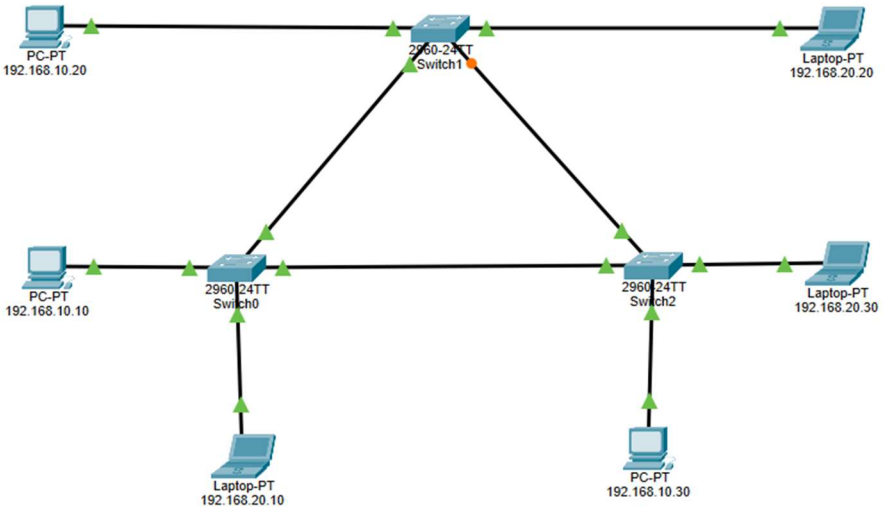
- Guide pas à pas pour la Correction **:**

1. **Visualisation de l'état du Spanning-Tree :**
    1. Ouvrir une session sur chacun des trois switchs à l'aide de l'interface de ligne de commande (CLI).
    2. Exécuter la commande "show spanning-tree" sur chaque switch pour afficher l'état actuel du Spanning-Tree.
2. **Identification du switch root :**
    1. Analyser les sorties de chaque switch pour déterminer lequel d'entre eux est désigné comme le switch racine du Spanning-Tree.
    2. Noter l'identifiant du switch root pour référence ultérieure.
3. **Configuration du switch SW1 comme root-bridge :**
    1. Se connecter au switch SW1 en utilisant l'interface de ligne de commande.
    2. Entrer dans le mode de configuration en saisissant la commande "configure terminal".
    3. Modifier la priorité du switch pour le VLAN 1 en utilisant la commande "spanning-tree vlan 1 priority 0".
    4. Quitter le mode de configuration en saisissant la commande "end".
4. **Visualisation du changement :**
    1. Exécuter à nouveau la commande "show spanning-tree" sur le switch SW1 pour visualiser le changement de priorité et confirmer qu'il est désormais le switch racine.
5. **Vérification du fonctionnement :**
    1. Effectuer des vérifications supplémentaires pour s'assurer que le switch SW1 fonctionne comme prévu en tant que root-bridge. notamment en examinant les liaisons montantes et la topologie du réseau (rechercher la LED "ambre" symboliser par une pastille sur Packet tracer).
6. **Discussion et conclusion :**
    1. Discuter des observations faites et de l'importance du Spanning-Tree dans la prévention des boucles dans les réseaux Ethernet.
    2. Conclure sur l'impact de la configuration du root-bridge sur la stabilité et les performances du réseau.

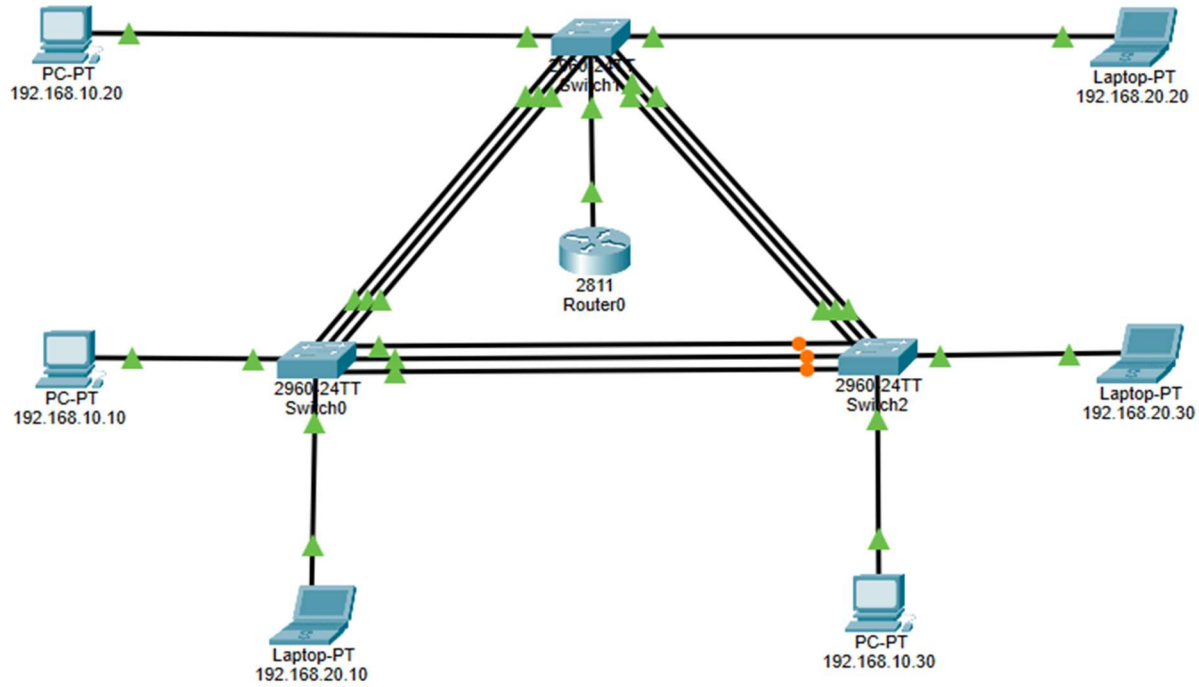
### Visualisation du port bloqué au début du TP




### Visualisation du port bloqué après le changement de switch root



# Atelier 5 : Paramétrer des liens LAG 802.3ad entre des switch



**Objectif de l'atelier :**

Paramétrer des liens LAG 802.3ad entre des switch

**Énoncé de l'Atelier :**

Dans cet atelier, nommé "LAG 802.3ad", vous allez explorer l'agrégation de liens (Link Aggregation Group - LAG) et son utilisation pour augmenter la bande passante et améliorer la résilience du réseau. Vous apprendrez à paramétrer les liens LAG en utilisant le protocole LACP (Link Aggregation Control Protocol) sur des switches Cisco pour créer des canaux d'agrégation de liens entre les switchs.

Les étapes sont les suivantes :

1. Configurer des canaux d'agrégation sur les switchs SW0 et SW1 pour agréger les ports fa 0/1-3.
2. Configurer des canaux d'agrégation sur les switchs SW1 et SW2 pour agréger les ports fa 0/4-6.
3. Configurer des canaux d'agrégation sur les switchs SW2 et SW0 pour agréger les ports fa 0/7-9.
4. Vérifier la configuration et l'état des agrégations de liens sur les trois switchs.

- Guide pas à pas pour la Correction :

1. **Configuration de LAG sur SW0 et SW1** :
    - Accédez au switch SW0 en mode de configuration.
    - Tapez **interface range fa 0/1-3** pour sélectionner les interfaces que vous souhaitez agréger.
    - Entrez **channel-protocol lacp** pour définir le protocole LACP pour la négociation LAG.
    - Tapez **channel-group 1 mode active** pour activer le groupement dans un canal d'agrégation et démarrer la négociation LACP.
    - Répétez les étapes sur SW1 pour les mêmes interfaces.
2. **Configuration de LAG sur SW1 et SW2** :
    - Sur le switch SW1, répétez le processus pour les ports fa 0/4-6 en utilisant **interface range fa 0/4-6**, **channel-protocol lacp**, et **channel-group 2 mode active**.
    - Répétez la configuration sur SW2 pour les mêmes ports.
3. **Configuration de LAG sur SW2 et SW0** :
    - Sur le switch SW2, sélectionnez les ports avec **interface range fa 0/7-9**.
    - Appliquez **channel-protocol lacp** et **channel-group 3 mode active**.
    - Finalisez en appliquant la même configuration sur SW0 pour les ports correspondants.
4. **Vérification de la Configuration des Canaux d'Agrégation** :
    - Sur chaque switch, exécutez **show etherchannel summary** pour visualiser le résumé et l'état de tous les canaux d'agrégation.
    - Confirmez que les canaux sont correctement configurés (Groupe 1 sur SW0 et SW1, Groupe 2 sur SW1 et SW2, Groupe 3 sur SW2 et SW0) et que l'état est "P" (ce qui signifie qu'ils sont en mode actif et connectés).

Cette configuration devrait aboutir à un réseau optimisé en termes de bande passante et de tolérance aux pannes, où chaque lien agrégé offre une capacité de transit accrue et une redondance en cas de défaillance d'un seul lien physique.

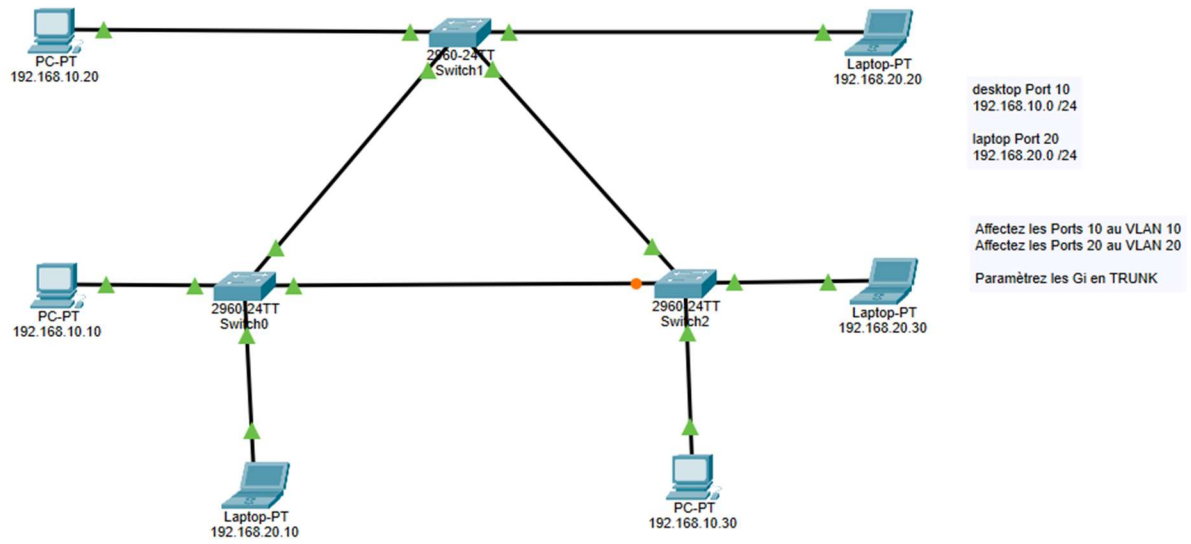
## Visualisation des LAG paramétrés dans le TP

```
sw0#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+---------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
3      Po3(SU)           LACP   Fa0/7(P) Fa0/8(P) Fa0/9(P)
sw0#
```

```
sw1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+---------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
2      Po2(SU)           LACP   Fa0/4(P) Fa0/5(P) Fa0/6(P)
sw1#
```

```
sw2#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+---------------------------------------------

2      Po2(SU)           LACP   Fa0/4(P) Fa0/5(P) Fa0/6(P)
3      Po3(SU)           LACP   Fa0/7(P) Fa0/8(P) Fa0/9(P)
sw2#
```

# Atelier 6 - Paramétrage des VLans




**Affectation des Vlans par défaut :**

```
Port              Link   VLAN   IP Address          MAC Address
FastEthernet0/1   Down   1      --                  0060.2F93.D801
FastEthernet0/2   Down   1      --                  0060.2F93.D802
FastEthernet0/3   Down   1      --                  0060.2F93.D803
FastEthernet0/4   Down   1      --                  0060.2F93.D804
FastEthernet0/5   Down   1      --                  0060.2F93.D805
FastEthernet0/6   Down   1      --                  0060.2F93.D806
FastEthernet0/7   Down   1      --                  0060.2F93.D807
FastEthernet0/8   Down   1      --                  0060.2F93.D808
FastEthernet0/9   Down   1      --                  0060.2F93.D809
FastEthernet0/10  Up     1      --                  0060.2F93.D80A
FastEthernet0/11  Down   1      --                  0060.2F93.D80B
FastEthernet0/12  Down   1      --                  0060.2F93.D80C
FastEthernet0/13  Down   1      --                  0060.2F93.D80D
FastEthernet0/14  Down   1      --                  0060.2F93.D80E
FastEthernet0/15  Down   1      --                  0060.2F93.D80F
FastEthernet0/16  Down   1      --                  0060.2F93.D810
FastEthernet0/17  Down   1      --                  0060.2F93.D811
FastEthernet0/18  Down   1      --                  0060.2F93.D812
FastEthernet0/19  Down   1      --                  0060.2F93.D813
FastEthernet0/20  Up     1      --                  0060.2F93.D814
FastEthernet0/21  Down   1      --                  0060.2F93.D815
FastEthernet0/22  Down   1      --                  0060.2F93.D816
FastEthernet0/23  Down   1      --                  0060.2F93.D817
FastEthernet0/24  Down   1      --                  0060.2F93.D818
GigabitEthernet0/1 Up    1      --                  0060.2F93.D819
GigabitEthernet0/2 Up    1      --                  0060.2F93.D81A
Vlan1             Down   1      <not set>           0009.7C36.7648
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

**Objectifs :**

- Affecter les VLANs aux interfaces FastEthernet (Fa).
- Paramétrer les interfaces GigabitEthernet (Gi) en mode Trunk.

**Enoncé :**

1. **Affecter le VLAN10 pour les interfaces Fa 0/10** :
    1. Accédez au mode de configuration de l'interface Fa 0/10 en tapant interface fastEthernet 0/10.
    2. Utilisez la commande switchport mode access pour configurer le port en mode access.
    3. Affectez le VLAN 10 en tapant switchport access vlan 10.
    4. Désactivez la négociation automatique en tapant switchport nonegotiate.
    5. Répétez les mêmes étapes pour l'interface Fa 0/20 avec le VLAN 20.
2. **Configurer les ports Gi 0/1 et Gi 0/2 en mode Trunk** :
    1. Accédez au mode de configuration de l'interface Gi 0/1 en tapant interface gigabitEthernet 0/1.
    2. Utilisez la commande switchport mode trunk pour configurer le port en mode Trunk.
    3. Désactivez la négociation automatique en tapant switchport nonegotiate.
    4. Répétez les mêmes étapes pour l'interface Gi 0/2.

- Guide pas à pas pour la Correction :

1. **Affecter le VLAN10 pour les interfaces Fa 0/10** :

```
scss
Copy code

SWO# configure terminal
SWO(config)# interface fastEthernet 0/10
SWO(config-if)# switchport mode access
SWO(config-if)# switchport access vlan 10
SWO(config-if)# switchport nonegotiate
SWO(config-if)# exit

SWO(config)# interface fastEthernet 0/20
SWO(config-if)# switchport mode access
SWO(config-if)# switchport access vlan 20
SWO(config-if)# switchport nonegotiate
SWO(config-if)# exit
```

2. **Configurer les ports Gi 0/1 et Gi 0/2 en mode Trunk :**

```
arduino
Copy code

SWO# configure terminal
SWO(config)# interface gigabitEthernet 0/1
SWO(config-if)# switchport mode trunk
SWO(config-if)# switchport nonegotiate
SWO(config-if)# exit

SWO(config)# interface gigabitEthernet 0/2
SWO(config-if)# switchport mode trunk
SWO(config-if)# switchport nonegotiate
SWO(config-if)# exit
```

**Remarques :**

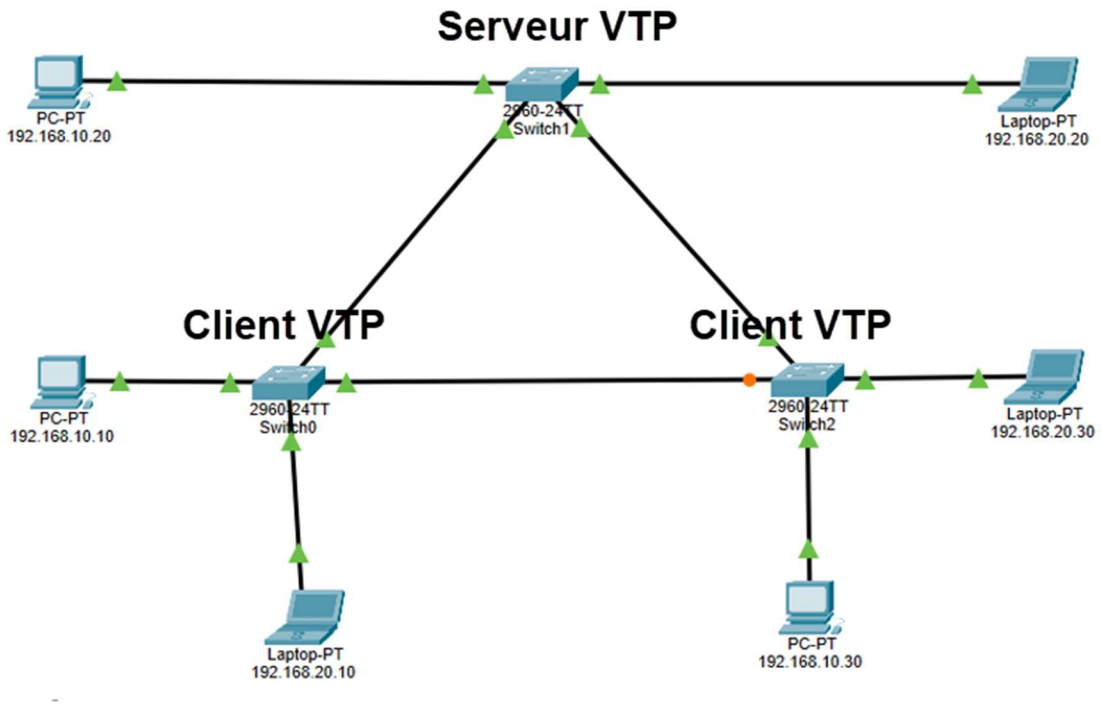
- Suivez attentivement les étapes fournies pour accomplir les objectifs de l'atelier.
- Assurez-vous de comprendre les commandes utilisées et leurs implications.
-

**Affectation des Vlans en fin d'exercice :**

| Port | Link | VLAN | IP Address | MAC Address |
|---|---|---|---|---|
| FastEthernet0/1 | Down | 1 | -- | 0060.2F93.D801 |
| FastEthernet0/2 | Down | 1 | -- | 0060.2F93.D802 |
| FastEthernet0/3 | Down | 1 | -- | 0060.2F93.D803 |
| FastEthernet0/4 | Down | 1 | -- | 0060.2F93.D804 |
| FastEthernet0/5 | Down | 1 | -- | 0060.2F93.D805 |
| FastEthernet0/6 | Down | 1 | -- | 0060.2F93.D806 |
| FastEthernet0/7 | Down | 1 | -- | 0060.2F93.D807 |
| FastEthernet0/8 | Down | 1 | -- | 0060.2F93.D808 |
| FastEthernet0/9 | Down | 1 | -- | 0060.2F93.D809 |
| FastEthernet0/10 | Up | 10 | -- | 0060.2F93.D80A |
| FastEthernet0/11 | Down | 1 | -- | 0060.2F93.D80B |
| FastEthernet0/12 | Down | 1 | -- | 0060.2F93.D80C |
| FastEthernet0/13 | Down | 1 | -- | 0060.2F93.D80D |
| FastEthernet0/14 | Down | 1 | -- | 0060.2F93.D80E |
| FastEthernet0/15 | Down | 1 | -- | 0060.2F93.D80F |
| FastEthernet0/16 | Down | 1 | -- | 0060.2F93.D810 |
| FastEthernet0/17 | Down | 1 | -- | 0060.2F93.D811 |
| FastEthernet0/18 | Down | 1 | -- | 0060.2F93.D812 |
| FastEthernet0/19 | Down | 1 | -- | 0060.2F93.D813 |
| FastEthernet0/20 | Up | 20 | -- | 0060.2F93.D814 |
| FastEthernet0/21 | Down | 1 | -- | 0060.2F93.D815 |
| FastEthernet0/22 | Down | 1 | -- | 0060.2F93.D816 |
| FastEthernet0/23 | Down | 1 | -- | 0060.2F93.D817 |
| FastEthernet0/24 | Down | 1 | -- | 0060.2F93.D818 |
| GigabitEthernet0/1 | Up | -- | -- | 0060.2F93.D819 |
| GigabitEthernet0/2 | Up | -- | -- | 0060.2F93.D81A |
| Vlan1 | Down | 1 | <not set> | 0009.7C36.7648 |

- Hostname: Switch

# Atelier 7 : Comprendre l'usage du VTP (VLAN Trunking Protocol).




**Objectifs :**

- Comprendre l'usage du VTP (VLAN Trunking Protocol).
- Configurer un switch en tant que serveur VTP.
- Configurer des switches en tant que clients VTP.
- Visualiser la configuration de VTP sur les switches.

- Guide pas à pas pour la Correction :

1. **Paramétrage du switch SW1 en tant que serveur VTP :**
    1. Se connecter au switch SW1 via l'interface de ligne de commande.
    2. Entrer dans le mode de configuration en saisissant la commande "configure terminal".
    3. Configurer le domaine VTP avec la commande "vtp domain cisco-lab".
    4. Définir le mot de passe VTP avec la commande "vtp password pafou".
    5. Spécifier la version VTP avec la commande "vtp version 2".
    6. Configurer le mode VTP en tant que serveur avec la commande "vtp mode server".
    7. Quitter le mode de configuration en saisissant la commande "end".
2. **Paramétrage des switches SW0 et SW2 en tant que clients VTP :**
    1. Répéter les mêmes étapes que précédemment pour se connecter et entrer en mode de configuration sur les switches SW0 et SW2.
    2. Utiliser les commandes fournies pour configurer le domaine VTP. le mot de passe VTP. la version VTP et le mode VTP en tant que clients.
3. **Visualisation de la configuration VTP :**
    1. Exécuter les commandes "show vtp status". "show vtp password" et "show vtp counter" sur chaque switch pour visualiser les paramètres de configuration VTP.
    2. Observer les résultats pour vérifier que le paramétrage VTP a été correctement appliqué sur tous les switches.
4. **Validation du fonctionnement :**
    1. Effectuer des vérifications supplémentaires pour s'assurer que le protocol VTP fonctionne comme prévu. notamment en vérifiant la synchronisation des VLANs entre le serveur et les clients.
    2. Examiner les logs ou les messages de confirmation pour confirmer le bon fonctionnement de la configuration VTP.

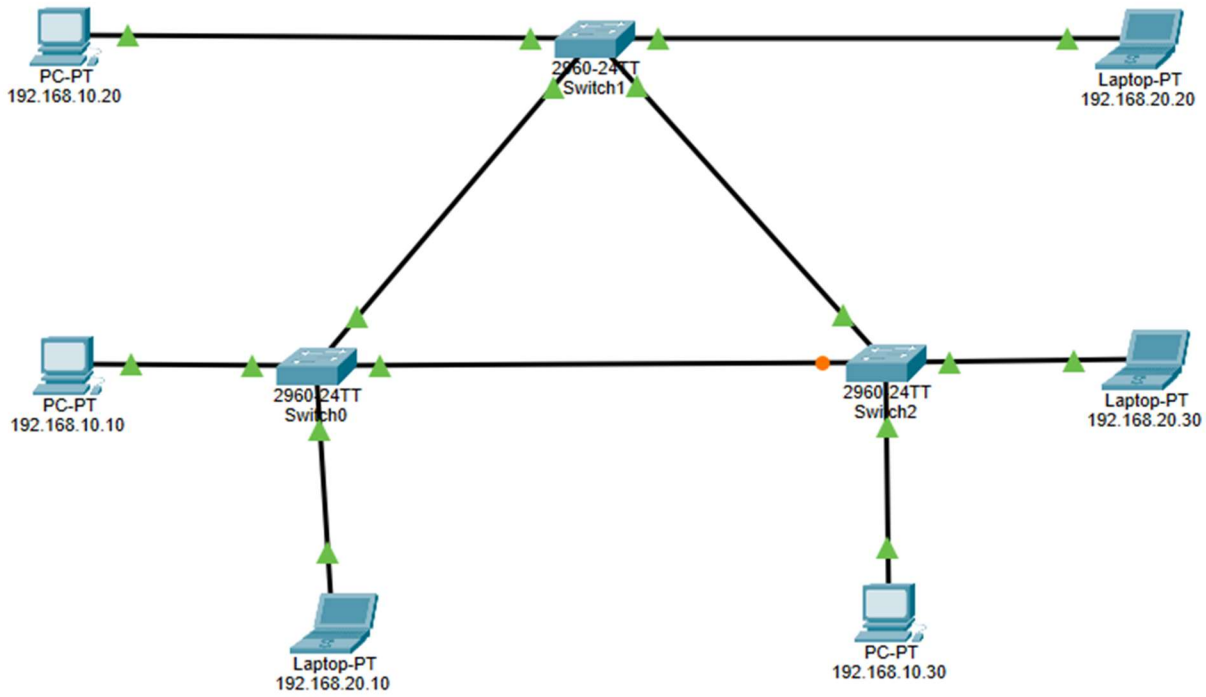
### Visualisation du paramétrage VTP :

```
sw0#sh vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : cisco-lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6B 0x09 0x4B 0x1C 0x8D
0x5F 0x6A 0x85
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:21
sw0#sh vtp password
VTP Password: pafou
sw0#
```

```
sw1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : cisco-lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6B 0x09 0x4B 0x1C 0x8D
0x5F 0x6A 0x85
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:21
Local updater ID is 0.0.0.0 (no valid interface found)
sw1#sh vtp password
VTP Password: pafou
sw1#
```

```
SW2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Client
VTP Domain Name                 : cisco-lab
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6B 0x09 0x4B 0x
Configuration last modified by 0.0.0.0 at 3-1-93 00
```

# Atelier 8 - Mise en place d'un routeur pour le routage inter Vlans




**Objectifs de l'atelier :**

- Configurer et vérifier les sub-interfaces sur un routeur Cisco pour séparer le trafic réseau en VLANs distincts.
- Assigner des adresses IP appropriées aux sub-interfaces pour permettre la communication inter-VLAN.
- Activer et gérer les interfaces de routage sur un routeur pour assurer le flux de données entre différents segments de réseau.
- Mettre en place et diagnostiquer une configuration de trunk sur un switch Cisco, essentielle pour le routage inter-VLAN.
- Utiliser des commandes de diagnostic pour vérifier les configurations d'interface et la présence de routes dans la table de routage, s'assurant ainsi que le routage inter-VLAN est opérationnel.

**Énoncé de l'Atelier :**

Dans cet atelier, vous serez amenés à configurer des sub-interfaces pour la gestion des VLANs sur un routeur Cisco 2800. Vous apprendrez à visualiser et à comprendre la configuration des interfaces IP d'un routeur ainsi qu'à interpréter la table de routage. Ces compétences sont essentielles pour la gestion d'un réseau segmenté en VLANs et pour le routage inter-VLAN.

Les étapes sont les suivantes :

1. Connectez un routeur Cisco 2800 à l'interface GigabitEthernet 0/0 du switch SW2 sur le port FastEthernet 0/24.

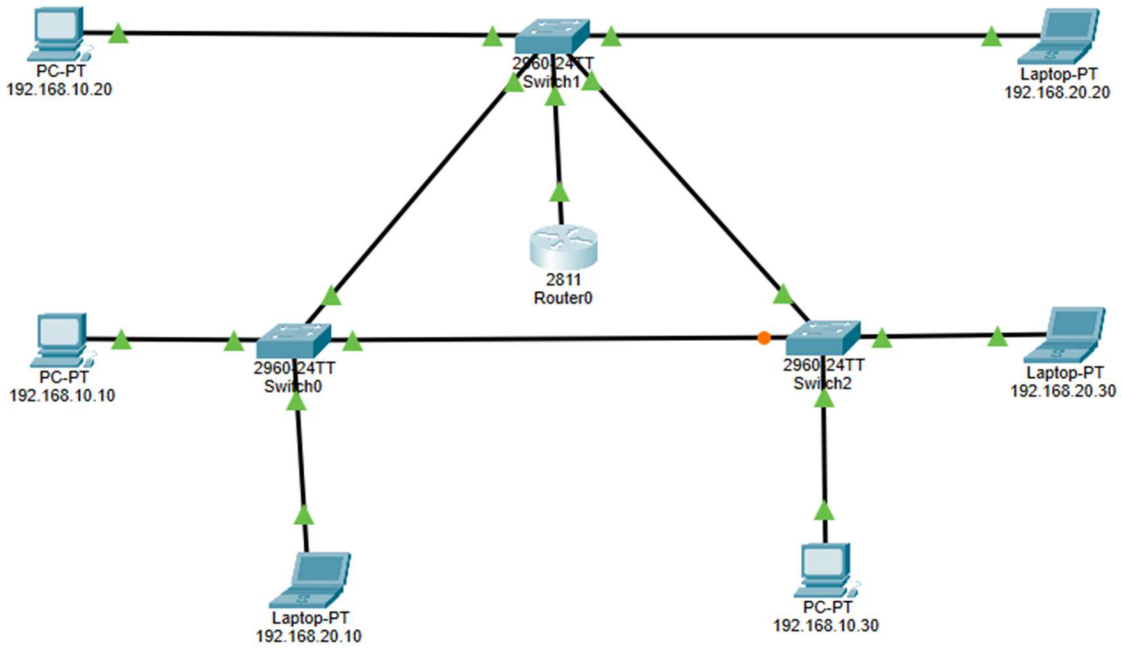
2. Configurez les sub-interfaces sur le routeur pour les VLANs 10 et 20, attribuez-leur les adresses IP correspondantes.
3. Activez l'interface Gi 0/0 du routeur.
4. Configurez le port Fa 0/24 du SW2 pour fonctionner en mode trunk.
5. Vérifiez la configuration IP des interfaces sur le routeur.
6. Examinez l'état des interfaces du switch pour s'assurer que le port Fa 0/24 est correctement configuré.
7. Consultez la table de routage du routeur pour vérifier la présence des routes nécessaires.

- Guide pas à pas pour la Correction **:**

1. **Ajout du Routeur 2800 sur SW2** :
    - Connectez physiquement le routeur 2800 à SW2 en utilisant le port GigabitEthernet 0/0 sur le routeur et le port FastEthernet 0/24 sur le switch.
2. **Configuration des Sub-Interfaces** :
    - Accédez au mode de configuration du routeur (**configure terminal**).
    - Entrez **interface GigabitEthernet 0/0.10** pour créer la sub-interface pour le VLAN 10.
    - Configurez la sub-interface avec **encapsulation dot1Q 10** pour spécifier le VLAN 10.
    - Attribuez l'adresse IP avec **ip address 192.168.10.254 255.255.255.0**.
    - Répétez les étapes pour la sub-interface du VLAN 20 en utilisant **interface GigabitEthernet 0/0.20**, **encapsulation dot1Q 20**, et l'adresse IP **192.168.20.254 255.255.255.0**.
3. **Activation de l'Interface Gi 0/0** :
    - Dans le mode de configuration du routeur, entrez **interface GigabitEthernet 0/0**.
    - Utilisez la commande **no shutdown** pour activer l'interface.
4. **Configuration du Port Trunk sur SW2** :
    - Sur SW2, passez en mode de configuration (**configure terminal**).
    - Entrez **interface FastEthernet 0/24**.
    - Configurez le port en mode trunk avec **switchport mode trunk** et désactivez la négociation avec **switchport nonegotiate**.
5. **Vérification de l'Interface sur le Routeur** :
    - Exécutez **show ip interface brief** pour vérifier que les sub-interfaces sont correctement configurées et activées.
6. **Vérification de l'État du Port Trunk sur SW2** :
    - Utilisez **show interface status** pour confirmer que le port Fa 0/24 est configuré en mode trunk.
7. **Affichage de la Table de Routage** :
    - Sur le routeur, exécutez **show ip route** pour visualiser les routes. Assurez-vous que les routes pour les VLANs 10 et 20 sont présentes.

Cet atelier renforce la compétence pratique des stagiaires en matière de configuration de réseau avancée, y compris la segmentation de réseau et les aspects essentiels du routage inter-VLAN.

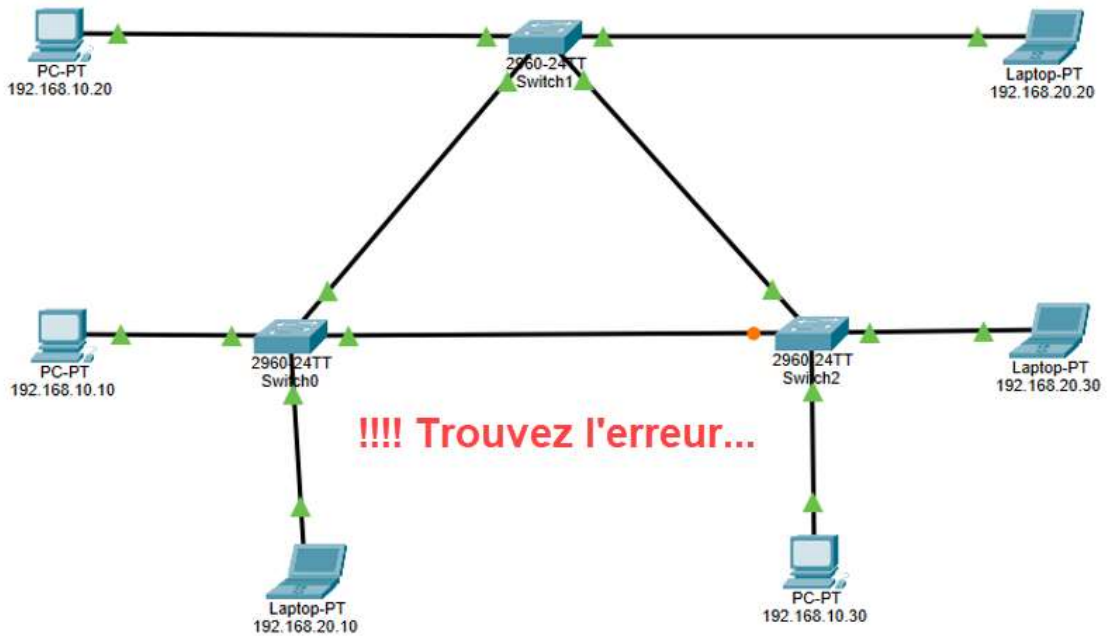
### Maquette après connexion du routeur :




### Contrôle de la configuration des interfaces

```
Port                Link   VLAN   IP Address          IPv6 Address                              MAC Address
FastEthernet0/0     Up     --     <not set>           <not set>                                 00E0.F981.5701
FastEthernet0/0.10  Up     --     192.168.10.254/24   <not set>                                 00E0.F981.5701
FastEthernet0/0.20  Up     --     192.168.20.254/24   <not set>                                 00E0.F981.5701
FastEthernet0/1     Down   --     <not set>           <not set>                                 00E0.F981.5702
Vlan1               Down   1      <not set>           <not set>                                 0001.97A1.3229
Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

# Atelier 9 : Dépannage à partir d'un maquette réseau sur un émulateur




**Objectif de l'Atelier Double** : L'atelier vise à développer les compétences de diagnostic réseau des stagiaires, en les amenant à identifier et résoudre des pannes spécifiques dans un environnement de laboratoire contrôlé. Les stagiaires vont apprendre à analyser systématiquement les problèmes de connectivité et à appliquer leurs connaissances théoriques dans la pratique, en s'attaquant à deux problèmes de configuration réseau communs : une mauvaise passerelle par défaut et un branchement incorrect sur un VLAN.

Énoncé de l'Atelier : Vous êtes responsable du bon fonctionnement d'un réseau composé de trois switches Cisco 2960 et de diverses machines Windows. Deux pannes critiques ont été signalées :

- Panne 1 : Le Laptop 20.20 ne parvient plus à communiquer avec le Desktop 10.30.
- Panne 2 : Le Laptop 20.10 est isolé et ne parvient pas à communiquer avec les autres dispositifs du réseau.

Votre mission est d'effectuer une série de tests de diagnostic pour identifier et corriger les sources de ces problèmes.

- Guide pas à pas pour la Correction **:**

**Panne 1 : Communication interrompue entre Laptop 20.20 et Desktop 10.30**

Étapes de Diagnostic :

1. Vérifiez que Laptop 20.20 et Desktop 10.30 sont allumés et connectés physiquement au réseau.
2. Testez la connectivité réseau sur les deux machines avec des commandes comme **ipconfig** ou **ifconfig** pour s'assurer qu'elles disposent d'une adresse IP valide.
3. Sur le Laptop 20.20, vérifiez la configuration de la passerelle par défaut avec **ipconfig** sous Windows (ou **netstat -rn** sous Linux). Confirmez que la passerelle est correcte.
4. Si la passerelle est incorrecte, reconfigurez-la avec la bonne adresse IP. Sous Windows, cela peut être fait via les paramètres du réseau ou avec la commande **netsh**.
5. Une fois la passerelle corrigée, utilisez **ping** pour tester la connectivité avec le Desktop 10.30.

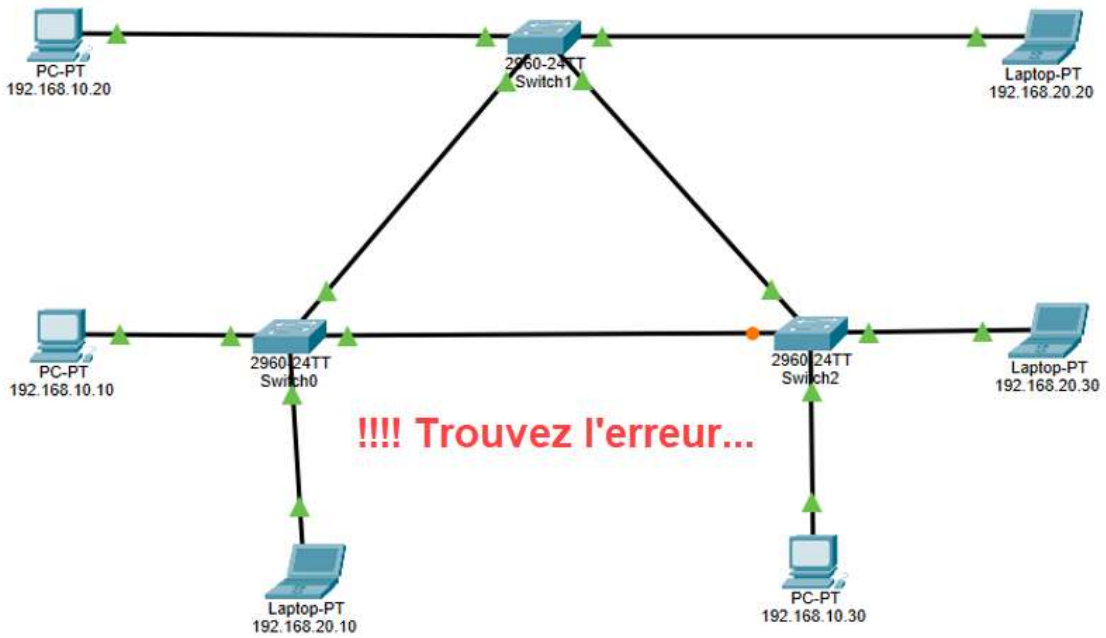
**Panne 2 : Laptop 20.10 isolé du réseau**

Étapes de Diagnostic :

1. Sur le Laptop 20.10, confirmez que les paramètres réseau sont correctement configurés avec **ipconfig**.
2. Vérifiez le port physique sur le switch où le Laptop 20.10 est connecté et assurez-vous qu'il correspond à celui indiqué sur la maquette.
3. Si le Laptop 20.10 est connecté au mauvais port, déplacez le câble vers le bon port qui correspond au VLAN approprié.
4. Testez à nouveau la connectivité après le changement de port avec des commandes comme **ping** vers une adresse connue dans le réseau.
5. Si la connectivité n'est pas restaurée, vérifiez la configuration du VLAN sur le switch pour confirmer que le port est assigné au bon VLAN.

En suivant ces étapes, les stagiaires devraient être capables de résoudre les pannes présentées et de restaurer la connectivité réseau pour les deux machines concernées.

# Atelier 10 : résoudre des problèmes de routage dans un réseau interconnecté




**Objectif de l'Atelier** :

L'atelier est conçu pour améliorer la capacité des stagiaires à comprendre et à résoudre des problèmes de routage dans un réseau interconnecté. L'exercice se concentre sur l'identification des problèmes liés au routage inter-VLAN et la compréhension de l'importance des configurations de routage sur les périphériques réseau.

**Énoncé de l'Atelier :**

Vous êtes confronté à un problème de communication entre les réseaux de votre environnement réseau qui comprend trois switches Cisco 2960 et un routeur. Actuellement, aucun trafic ne peut passer d'un réseau à l'autre. Vous devez enquêter sur la connectivité inter-réseau et déterminer la cause de ce défaut de routage.

- Guide pas à pas pour la Correction **:**

1. **Vérification initiale** :
    - Assurez-vous que tous les périphériques sont allumés et connectés.
    - Utilisez la commande **ping** pour tester la connectivité au sein du même réseau (intra-VLAN).
2. **Vérification de la configuration du routeur** :
    - Connectez-vous au routeur via la console ou SSH.
    - Examinez la configuration du routeur avec la commande **show running-config** pour voir si le routage IP est activé. Recherchez la ligne "no ip routing" dans la configuration.
3. **Réactivation du routage IP** :
    - Si le routage IP est désactivé, réactivez-le avec la commande **ip routing** dans le mode de configuration globale.
    - Sauvegardez la configuration avec **write memory** ou **copy running-config startup-config**.
4. **Vérification du routage inter-VLAN** :
    - Vérifiez que les interfaces du routeur sont correctement configurées avec les adresses IP et les sous-réseaux correspondant à chaque VLAN.
    - Assurez-vous que les switchs sont correctement configurés pour permettre le routage inter-VLAN (à l'aide de commandes telles que **show vlan brief** et **show ip route**).
5. **Tests post-correction** :
    - Testez la connectivité entre les VLANs avec **ping** en utilisant les adresses IP des périphériques dans des VLANs différents.
    - Si le ping échoue, vérifiez à nouveau les configurations des VLANs et du routeur, y compris les routes statiques ou le protocole de routage dynamique.
6. **Dépannage supplémentaire** :
    - Si le problème persiste, vérifiez les configurations de sécurité comme les listes de contrôle d'accès (ACL) qui pourraient bloquer le trafic inter-VLAN.
    - Considérez également de redémarrer le routeur si toutes les configurations semblent correctes mais que le routage ne fonctionne toujours pas, ce qui peut résoudre les problèmes liés aux processus de routage.

# Annexe :

- "cheat sheet", pour le paramétrage des VLANs sur un équipement Cisco IOS :

**Créer un VLAN :**

```
Switch# configure terminal
Switch(config)# vlan [numéro_vlan]
Switch(config-vlan)# name [nom_du_vlan]
Switch(config-vlan)# end
```

**Affecter un Port à un VLAN :**

```
Switch# configure terminal
Switch(config)# interface [type_d'interface][numéro_d'interface]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan [numéro_vlan]
Switch(config-if)# end
```

**Paramétrer un Port en Trunk :**

```
Switch# configure terminal
Switch(config)# interface [type_d'interface][numéro_d'interface]
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan [liste_de_vlans]
Switch(config-if)# end
```

**Paramétrer le VLAN Natif sur un Trunk :**

```
Switch# configure terminal
Switch(config)# interface [type_d'interface][numéro_d'interface]
Switch(config-if)# switchport trunk native vlan [numéro_vlan]
Switch(config-if)# end
```

**Supprimer un VLAN :**

```
Switch# configure terminal
Switch(config)# no vlan [numéro_vlan]
Switch(config)# end
```

**Vérifier la Configuration des VLANs :**

```
Switch# show vlan brief
```

**Vérifier la Configuration des Ports de Trunk :**

```
Switch# show interfaces trunk
```

**Sauvegarder la Configuration :**

```
Switch# copy running-config startup-config
```

**Remarques :**

- Remplacez **[numéro_vlan]** par le numéro de VLAN souhaité.
- **[nom_du_vlan]** est le nom descriptif que vous souhaitez donner au VLAN.
- **[type_d'interface]** et **[numéro_d'interface]** se réfèrent au type (ex: FastEthernet, GigabitEthernet) et au numéro de l'interface que vous souhaitez configurer.
- **[liste_de_vlans]** peut être une liste séparée par des virgules ou un intervalle de VLANs pour les trunks (ex: 10,20,30 ou 10-30).

Utilisez cette "cheat sheet" pour paramétrer rapidement les VLANs et effectuer les vérifications de base sur les switches Cisco IOS.

- "cheat sheet" pour le paramétrage de Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) et Multiple Spanning Tree Protocol (MSTP) sur des équipements Cisco IOS

**Activer STP (déjà activé par défaut) :**

```
Switch# configure terminal
Switch(config)# spanning-tree mode pvst
Switch(config)# end
```

**Activer RSTP :**

```
Switch# configure terminal
Switch(config)# spanning-tree mode rapid-pvst
Switch(config)# end
```

**Activer MSTP :**

```
Switch# configure terminal
Switch(config)# spanning-tree mode mst
Switch(config)# end
```

**Définir la priorité d'un switch dans STP :**

```
Switch# configure terminal
Switch(config)# spanning-tree vlan [numéro_vlan] priority [valeur_priorité]
Switch(config)# end
```

(La valeur de priorité doit être un multiple de 4096.)

**Définir le coût d'un port dans STP :**

```
Switch# configure terminal
Switch(config)# interface [type_d'interface][numéro_d'interface]
Switch(config-if)# spanning-tree vlan [numéro_vlan] cost [valeur_coût]
Switch(config-if)# end
```

**Activer le portfast sur un port (ne devrait être utilisé que sur les ports d'extrémité) :**

```
Switch# configure terminal
Switch(config)# interface [type_d'interface][numéro_d'interface]
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

**Configuration globale du MSTP (exemple pour une instance) :**

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name [nom_region]
Switch(config-mst)# revision [numéro_revision]
Switch(config-mst)# instance [numéro_instance] vlan [liste_de_vlans]
Switch(config-mst)# end
```

**Affecter la priorité d'un switch dans MSTP :**

```
Switch# configure terminal
Switch(config)# spanning-tree mst [numéro_instance] priority [valeur_priorité]
Switch(config)# end
```

**Vérifier l'état de Spanning Tree :**

```
Switch# show spanning-tree
```

**Vérifier l'état de Spanning Tree pour un VLAN spécifique :**

```
Switch# show spanning-tree vlan [numéro_vlan]
```

**Vérifier l'état de MST :**

```
Switch# show spanning-tree mst
```

**Sauvegarder la Configuration :**

```
Switch# copy running-config startup-config
```

**Remarques :**

- Remplacez **[numéro_vlan]** par le numéro de VLAN approprié.
- **[valeur_priorité]** et **[valeur_coût]** sont à définir selon la topologie et les exigences du réseau.
- **[nom_region]** et **[numéro_revision]** sont à configurer pour MSTP afin de définir la région de spanning tree et sa révision.
- **[numéro_instance]** se réfère à l'instance MST pour laquelle vous configurez la priorité.

Cette référence rapide peut être utilisée pour configurer et gérer le Spanning Tree Protocol sur vos switchs Cisco IOS.