

Cisco

Lab 4-2 : Les VLANs

Dépannage des VLANs et des liens Trunks



Objectifs

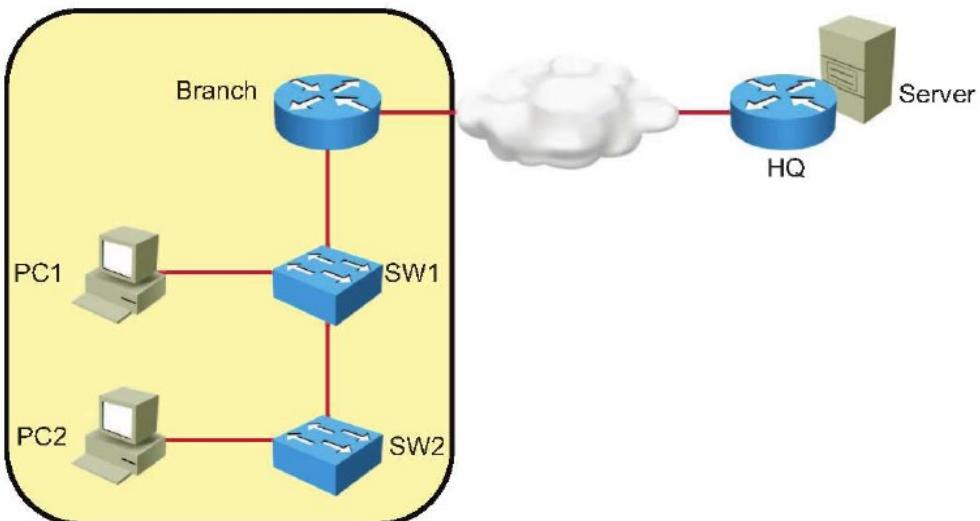
Dans cette activité vous allez parcourir différents tickets d'incident en rapport avec les VLANs et les trunks. Identifiez les problèmes qui se présentent, et corrigez les problèmes.

Vous aurez terminé cette activité lorsque vous aurez atteint les objectifs suivants :

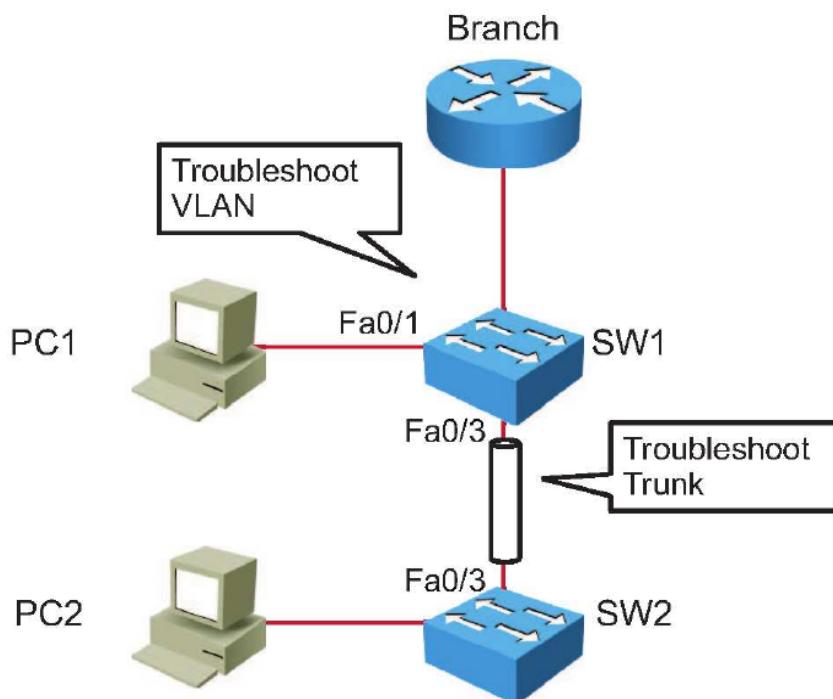
1. Dépanner les VLANs
2. Dépanner les Trunks

Visualisation des objectifs :

Visual Objective for Lab 4-1: Configuring Expanded Switched Networks



Detailed Visual Objective



Ressources Requises :

Ci-joint les ressources requises pour ce TP

Liste de commandes :

Le tableau décrit les commandes utilisées dans cette activité et sont classées alphabétiquement afin que vous puissiez facilement localiser les informations dont vous avez besoin. Reportez-vous à cette liste si vous avez besoin d'aide lors de la configuration et la poursuite de cette activité.

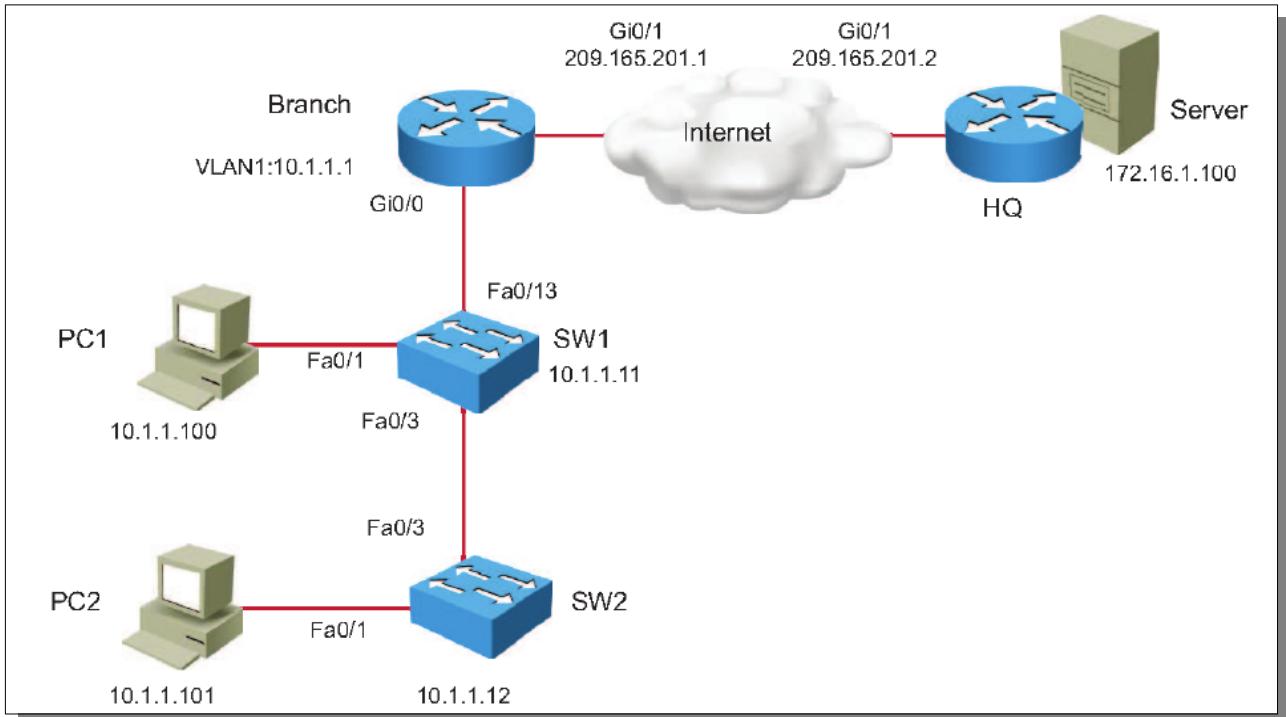
Commandes	Descriptions
Configure terminal	Entrer en mode de configuration globale
Interface <i>interface</i>	Entrer en mode de configuration de l'interface spécifiée
Show interface <i>mode</i>	Affiche le status d'une interface et ses statistiques
show interfaces <i>interface</i> switchport	Affiche des informations sur l'interface et son mode VLAN (access/trunk)
show vlan	Affiche les information d'un VLAN particulier
switchport mode trunk	Configure le comportement d'un port vis-à-vis des VLANs, en tant que trunk.
switchport nonegotiate	Désactive le protocole DTP pour l'établissement automatique du trunk
Switchport trunk native vlan <i>vlan_id</i>	Configure le VLAN natif sur une interface trunk
Vlan <i>N°_VLAN</i>	Crée le VLAN sur l'appareil actuel, en lui attribuant un numéro spécifique. À utiliser en mode de configuration globale

Aide à la mise en place :

Appareil	Périphériques	Utilisateur	Mot de passe
Branch	Cisco 2901 ISR	Console : ccna	Console : cisco
HQ	Cisco 2901 ISR	Console : ccna	Console : cisco
SW1	Catalyst 2960 Series Switch	Console : ccna	Console : cisco
SW2	Catalyst 2960 Series Switch	Console : ccna	Console : cisco
PC1	N'importe quel PC	XXX	XXX
PC2	N'importe quel PC	XXX	XXX

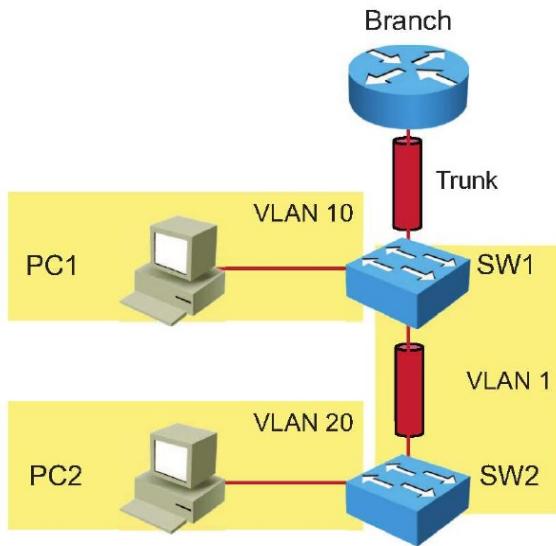
Topologie et Adressage IP

Les appareils sont connectés par le biais de leurs interfaces Ethernet. La capture ci-dessous illustre la topologie, les noms et les types d'interfaces, ainsi que les adresses IP qui sont utilisées dans ce lab.



Appareils	Interfaces	Adresses IP
Branch	Gi0/1	209.165.201.1/27
Branch	Gi0/0.1	10.1.1.1/24
Branch	Gi0/0.10	10.1.10.1/24
Branch	Gi0/0.20	10.1.20.1/24
Branch	Serial0/0/0	192.168.1.1/24
HQ	Gi0/1	209.165.201.2/27
HQ	Loopback0	172.16.1.100/24
HQ	Serial0/0/0	192.168.1.2/24
SW1	VLAN 1	10.1.1.11/24
SW2	VLAN 1	10.1.1.12/24
PC1	Connection réseau local par interface Ethernet	10.1.1.100/24
PC2	Connection réseau local par interface Ethernet	10.1.1.101/24

	interface Ethernet	
--	--------------------	--



3 VLANs sont configurés sur les switchs. VLAN1 est utilisé à des fins d'accès à distance aux appareils pour leur administration, VLAN10 est utilisé pour la connexion de PC1, VLAN20 pour la connexion de PC2. Un trunk est configuré entre les switchs SW1 et SW2. SW1 est connecté au routeur Branch via un lien trunk unique. Le Schéma illustre ces différentes connexions.

Tâche 1 : Dépanner la connectivité VLAN

Après avoir configuré le réseau, votre collègue veut faire quelques modifications supplémentaires et a fini par briser la connectivité de certains utilisateurs. En vous référant aux premières pages du document pour bien garder à l'esprit les connectivités qui devraient être mises en place et leurs paramétrages, rétablissez la connectivité. Le routeur Branch devrait être en mesure de faire un routage direct, sans instruction particulière, entre les VLAN 1, 10, et 20, donc PC1 et PC2 devraient pouvoir se ping entre eux.

On vous informe que les utilisateurs au sein du VLAN10 ne peuvent pas communiquer. Plus précisément, un utilisateur sur PC1 ne peut pas ping sa passerelle par défaut se trouvant sur le routeur Branch. Un ingénieur réseau expérimenté vous confirme que le problème ne se situe pas entre le Switch SW1 et le routeur Branch.

Étape 1 :

Accédez à PC1, faites un ping de sa passerelle et confirmez le problème qui vous a été reporté.

Le ping ne devrait pas être fonctionnel.

```
c:\>ping 10.1.10.1
Pinging 10.1.10.1 with 32 bytes of data:
Reply from 10.1.10.100: Destination host unreachable.

Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Étape 2 :

Accédez au Switch 1, et vérifiez le statut de l'interface se connectant à PC1, l'interface doit être « up ».

```
SW1#show interfaces fastEthernet0/1
FastEthernet0/1 is up, line protocol is up (connected)
<output omitted>
```

Étape 3 :

Vérifiez le mode du port concernant sa configuration VLAN et le port qu'il laisse passer.

```
SW1#show interfaces fastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Étape 4 :

Vérifiez la base de donnée VLAN interne de l'appareil à l'aide de la commande show appropriée :

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
20	VLAN0020	active	
100	VLAN0100	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

Étape 5 :

Résolvez le problème en créant le VLAN10 sur SW1.

Étape 6 :

Vérifiez à nouveau la base de données VLAN interne de l'appareil, vous devriez y voir cette fois le VLAN 10.

SW1#show vlan			
VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	VLAN0010	active	Fa0/1
20	VLAN0020	active	
100	VLAN0100	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

Étape 7 :

Vérifiez à nouveau le statut du port pour ce qui est du mode de configuration VLAN, comme à l'étape 3. Constatez que le port n'est plus inactif !

Étape 8 :

Pour finir, retournez sur PC1 et faites un ping de sa passerelle par défaut, 10.1.10.1, encore une fois. Le ping doit réussir !

```
c:\>ping 10.1.10.1
Pinging 10.1.10.1 with 32 bytes of data:
Reply from 10.1.10.1: bytes=32 time=2ms TTL=255
Reply from 10.1.10.1: bytes=32 time<1ms TTL=255
Reply from 10.1.10.1: bytes=32 time=1ms TTL=255
Reply from 10.1.10.1: bytes=32 time=1ms TTL=255
Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Tâche 2 : Dépanner le lien trunk entre les switchs

Vous avez été informé que les utilisateurs de VLAN10 ne peuvent pas communiquer avec les utilisateurs du VLAN20. Plus précisément, un utilisateur de PC1 ne peut réussir un ping vers le PC2. En tant qu'ingénieur réseau, vous devez corriger ce problème. L'ingénieur réseau expérimenté vous confirme que le problème se trouve sur le lien trunk établi entre SW1 et SW2 !

Étape 1 :

Accédez au PC1, et faites un ping vers le PC2 dont l'adresse en 10.1.20.100. Constatez que le ping échoue effectivement, ce qui confirme le problème signalé.

```
c:\>ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Étape 2 :

Accédez au Switch SW1, examinez le status de l'interface FastEthernet 0/3, car c'est elle qui connecte SW1 et SW2. Confirmez que l'interface est bien active et qu'il s'agit donc d'un problème de plus haut niveau sur le modèle OSI

```
SW1#show interfaces fastEthernet0/3
FastEthernet0/3 is up, line protocol is up (connected)
<output omitted>
```

Étape 3 :

Sur SW1 toujours, vérifiez le mode de fonctionnement du port vis à vis de la technologie VLAN. Vous constaterez que la négociation de l'établissement du port est activée, et qu'en plus de ça, il est en mode access, ne pouvant laisser passer qu'un seul VLAN, et non pas en mode trunk !

```
SW1#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
<output omitted>
```

Étape 4 :

Sur SW2 cette fois, vérifiez que la configuration du port FastEthernet0/3.

```
SW2#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
<output omitted>
```

Vous remarquerez que la configuration est identique à celle de SW1, pourquoi ?

Étape 5 :

Retournez sur SW1 et passez l'interface FastEthernet0/3 en mode trunk. Désactivez la négociation du trunk (DTP) également. Puis vérifiez la nouvelle configuration, comme toujours.

```
SW1#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<output omitted>
```

Étape 6 :

Faites de nouveau un ping de PC1 vers PC2. Constatez que le ping ne passe toujours pas. Il y a évidemment un autre problème dans notre configuration réseau au niveau du trunk entre les switchs.

```
c:\>ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Étape 7 :

Observez le retour de la console sur chacun des switchs. Le CDP (Cisco Discovery Protocol) vous informe d'une incohérence entre les VLAN natifs choisis sur chaque switch.

```
SW1#
Sep  5 08:42:00.725: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on FastEthernet0/3 (20), with SW2 FastEthernet0/3 (15).
SW2#
Sep  5 08:41:00.191: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on FastEthernet0/3 (15), with SW1 FastEthernet0/3 (20).
```

Vous pouvez le vérifier par vous-même sur chacun des switch via cette commande :

```
SW1#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 20 (VLAN0020)
<output omitted>
```

```
SW2#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 15 (VLAN0015)
<output omitted>
```

Supposons que le router Branch reçoive une trame de PC2, qui se trouve dans le VLAN20. Cette trame va atteindre le switch SW1, mais parce que SW1 a comme VLAN natif le VLAN 20, elle ne sera pas taguée pour traverser le lien trunk vers SW2. SW2 a comme VLAN natif le VLAN 15, et pour cette raison, toutes les trames arrivant vers ce switch appartiendront par défaut au VLAN 15. La trame n'arrivera donc jamais à PC2.

Étape 8 :

Sur SW1, déclarez VLAN 1 comme étant le VLAN natif sur l'interface FastEthernet 0/3. Faites la même chose sur SW2, sur son interface FastEthernet 0/3.

Étape 9 :

Retournez sur PC1 et faites un ping de PC2. Le ping doit maintenant réussir

```
C:\>ping 10.1.20.100
Pinging 10.1.20.100 with 32 bytes of data:
Reply from 10.1.20.100: bytes=32 time=4ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Reply from 10.1.20.100: bytes=32 time=1ms TTL=127
Ping statistics for 10.1.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

N'oubliez pas : le temps que le protocole ARP fasse son travail (corrélation entre l'adresse IP, logique, de la machine que l'on tente de joindre, et son adresse MAC, physique), les premières requêtes ping peuvent échouer !