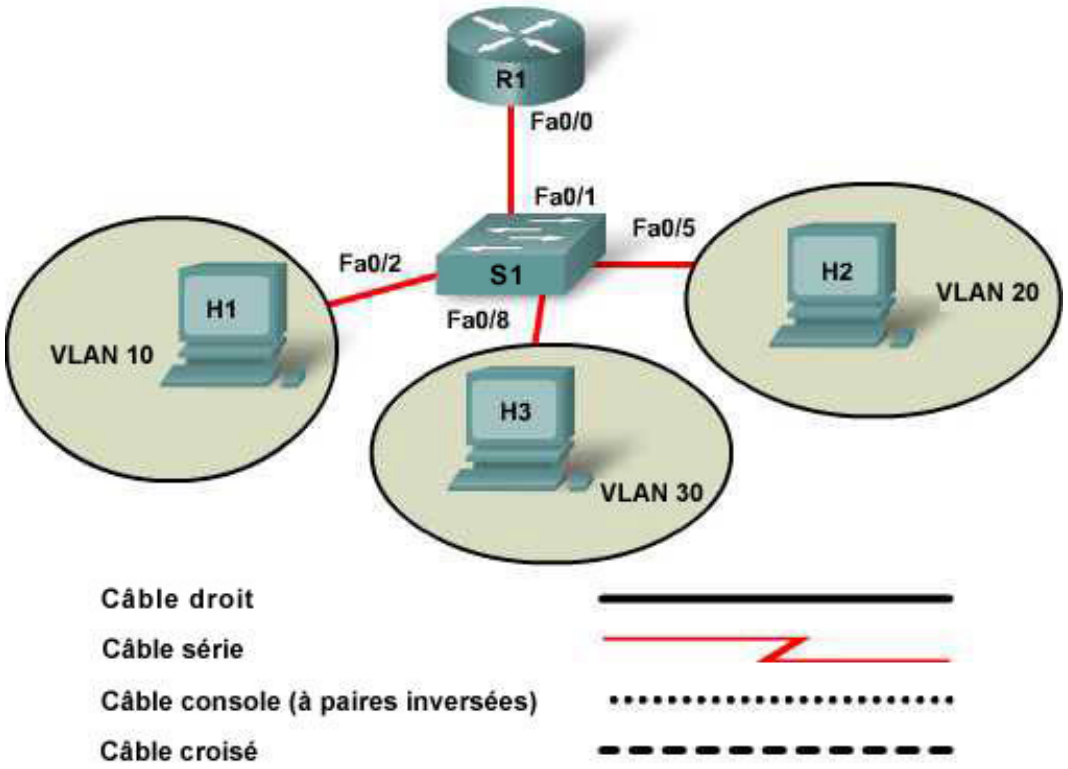
# Travaux pratiques 8.4.5 : Configuration et vérification de listes de contrôle d'accès pour filtrer le trafic entre réseaux locaux virtuels (VLAN)




| Périphérique | Nom de l'hôte | Adresse IP FastEthernet | Adresse IP de la passerelle par défaut | Numéros et noms VLAN | Affectations de ports de commutateur | Mot de passe secret actif | Mot de passe enable/ vty et console |
|---|---|---|---|---|---|---|---|
| Routeur 1 | R1 | Fa0/0 : aucun<br>Fa0/0.1 : 192.168.1.1/24<br>Fa0/0.2 : 192.168.2.1/24<br>Fa0/0.3 : 192.168.3.1/24<br>Fa0/0.4 : 192.168.4.1/24 | | | | class | cisco |
| Commutateur 1 | S1 | 192.168.1.2/24 | 192.168.1.1 | VLAN 1 Natif<br>VLAN 10 Serveurs<br>VLAN 20 Utilisateurs1<br>VLAN 30 Utilisateurs2 | Fa0/1<br>Fa0/2<br>Fa0/5<br>Fa0/8 | class | cisco |

| Périphérique | Nom de l'hôte | Adresse IP FastEthernet | Adresse IP de la passerelle par défaut | Numéros et noms VLAN | Affectations de ports de commutateur | Mot de passe secret actif | Mot de passe enable/ vty et console |
|---|---|---|---|---|---|---|---|
| Hôte 1 | H1 | 192.168.2.10/24 | 192.168.2.1 | | | | |
| Hôte 2 | H2 | 192.168.3.10/24 | 192.168.3.1 | | | | |
| Hôte 3 | H3 | 192.168.4.10/24 | 192.168.4.1 | | | | |

## Objectifs

- Configurer des réseaux locaux virtuels sur un commutateur
- Configurer et vérifier l'agrégation
- Configurer un routeur pour le routage entre réseaux locaux virtuels
- Configurer, appliquer et tester une liste de contrôle d'accès pour filtrer le trafic entre réseaux locaux virtuels

## Contexte / Préparation

Installez un réseau similaire à celui du schéma. Tout routeur doté d'une interface indiquée dans le schéma de topologie peut être utilisé. Exemple : les routeurs de la gamme 800, 1600, 1700, 1800, 2500, 2600, 2800 ou toute combinaison de ces routeurs sont utilisables.

Les informations présentées dans ces travaux pratiques s'appliquent au routeur 1841. Il est possible d'utiliser d'autres routeurs ; cependant la syntaxe des commandes peut varier. Les interfaces peuvent être différentes en fonction du modèle de routeur. Par exemple, sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet 0 peut être FastEthernet 0/0. Le commutateur Cisco Catalyst 2960 est fourni préconfiguré : il ne nécessite que l'affectation d'informations de sécurité de base avant la connexion à un réseau.

Ressources nécessaires :

- Un commutateur Cisco 2960 ou comparable
- Un routeur Cisco 1841 ou comparable
- Trois PC Windows avec un programme d'émulation de terminal
- Au moins un câble console à connecteur RJ-45/DB-9 pour configurer le routeur et le commutateur
- Quatre câbles droits Ethernet

**REMARQUE :** vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. Les instructions d'effacement et de rechargement de la mémoire du commutateur et du routeur figurent dans la section Tools du site Academy Connection.

**REMARQUE : Routeurs SDM** – Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lorsque le routeur est redémarré. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. La procédure indiquée dans ces travaux pratiques utilise des commandes IOS et ne nécessite pas l'utilisation de SDM. Si vous voulez utiliser SDM, reportez-vous aux instructions du Manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection. Consultez votre formateur si besoin.

### Étape 1 : connexion du matériel

a. Connectez l'interface Fa0/0 du Routeur 1 à l'interface Fa0/1 du Commutateur 1 à l'aide d'un câble droit.

b. Connectez les PC à l'aide de câbles console pour procéder aux configurations sur le routeur et le commutateur.

c. Connectez les PC hôtes avec des câbles droits aux ports du commutateur suivants : Hôte 1, vers Fa0/2 ; Hôte 2, vers Fa0/5 ; Hôte 3, vers Fa0/8.

### Étape 2 : configuration de base du routeur R1

### Étape 3 : configuration de R1 pour prendre en charge le trafic entre réseaux locaux virtuels

L'interface FastEthernet 0/0 sur R1 sera divisée en sous-interfaces pour acheminer le trafic provenant de chacun des trois réseaux locaux virtuels. L'adresse IP de chaque sous-interface deviendra la passerelle par défaut pour le réseau virtuel auquel elle est associée.

```
R1#configure terminal
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0,2
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0,3
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0,4
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.4.1 255.255.255.0
R1(config-subif)#end
R1#copy running-config startup-config
```

Pourquoi la commande **no shutdown** est-elle uniquement exécutée sur l'interface FastEthernet 0/0 ?

_____

Pourquoi est-il nécessaire d'indiquer le type d'encapsulation sur chaque sous-interface ?

_____

### Étape 4 : configuration de base du commutateur S1

### Étape 5 : création et désignation de trois réseaux locaux virtuels sur S1 puis attribution de ports à ces réseaux

Ce réseau contient un réseau local virtuel pour la batterie de serveurs et deux pour des groupes d'utilisateurs.

Pourquoi est-il recommandé de placer la batterie de serveurs dans un réseau local virtuel séparé ?

_____

a. Entrez les commandes suivantes pour créer les trois réseaux virtuels :

```
S1(config)#vlan 10
S1(config)#name Serveurs
S1(config)#vlan 20
S1(config)#name Utilisateurs1
```

```
S1(config)#vlan 30
S1(config)#name Utilisateurs2
```

b. Attribuez un port à chaque réseau, conformément à la table d'adressage.

```
S1#configure terminal
S1(config)#interface fastethernet0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10

S1(config)#interface fastethernet0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20

S1(config)#interface fastethernet0/8
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

**REMARQUE :** dans le cadre de ces travaux pratiques, une seule interface représentative est attribuée à chaque réseau local virtuel. Pour attribuer plusieurs ports à un réseau virtuel, utilisez le paramètre **range**. Par exemple, pour attribuer les ports 0/2 à 0/4 au réseau VLAN 10, utilisez la séquence de commandes suivante :

```
S1(config)#interface range fastethernet 0/2 - 4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
```

### Étape 6 : création de l'agrégation sur S1

Entrez la commande suivante pour définir l'interface Fa0/1 comme port agrégé :

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

Pourquoi est-il facultatif d'indiquer le protocole d'agrégation (dot1q, ISL) qui sera utilisé ?

_____

### Étape 7 : configuration des hôtes

Configurez chaque hôte avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut corrects, en fonction de la table d'adressage.

Prévoyez la réponse à la question suivante : si les configurations sont correctes, à quels périphériques un utilisateur sur PC1 doit-il pouvoir envoyer une requête ping qui aboutisse ?

_____

### Étape 8 : vérification du fonctionnement du réseau

a. À partir de chaque hôte connecté, envoyez une requête ping aux deux autres hôtes et à chacune des adresses IP des sous-interfaces du routeur.

La requête ping a-t-elle abouti ? _____

Si la réponse est non, vérifiez la configuration du routeur, du commutateur et de l'hôte pour trouver l'erreur.

b. À partir du commutateur S1, envoyez une requête ping à la passerelle par défaut du routeur 192.168.1.1.

La requête ping a-t-elle abouti ? _____

c. Utilisez la commande **show ip interface brief** pour vérifier l'état de chaque interface ou sous-interface.

Quel est l'état des interfaces ?

**R1 :**

FastEthernet 0/0 : _____

FastEthernet 0/0.1 : _____

FastEthernet 0/0.2 : _____

FastEthernet 0/0.3 : _____

FastEthernet 0/0.4 : _____

**S1 :**

Interface VLAN1 : _____

d. Envoyez de nouvelles requêtes ping jusqu'à ce qu'elles aboutissent.

## Étape 9 : configuration, application et test d'une liste de contrôle d'accès étendue pour filtrer le trafic entre réseaux locaux virtuels

Les membres du réseau local virtuel Utilisateurs1 ne doivent pas pouvoir atteindre la batterie de serveurs, tandis que les membres de l'autre réseau doivent pouvoir se joindre mutuellement ainsi qu'atteindre le routeur. Utilisateur1 doit pouvoir atteindre des réseaux locaux virtuels autres que la batterie de serveurs.

a. Créez les instructions de la liste de contrôle d'accès étendue :

```
R1(config)#access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
R1(config)#access-list 100 permit ip any any
```

R1 possède une interface FastEthernet 0/0 et quatre sous-interfaces. Où doit être placée cette liste et dans quelle direction ? Pourquoi ?

_____

b. Appliquez la liste de contrôle d'accès et effectuez un test en envoyant une requête ping de PC2 à PC1 et à PC3.

Si la liste fonctionne correctement, les requêtes ping de PC2 à PC1 doivent échouer. Toutes les autres requêtes ping doivent aboutir. Si les résultats ne répondent pas à ces critères, corrigez la syntaxe et l'emplacement de la liste de contrôle d'accès.

## Étape 10 : remarques générales

a. Pourquoi est-il recommandé d'effectuer et de vérifier des configurations de base et de réseau local virtuel avant de créer et d'appliquer une liste de contrôle d'accès ?

_____

_____

b. Quels résultats auraient été produits si la liste de contrôle d'accès était placée sur la sous-interface FastEthernet 0/0.3 en sortie et si PC2 avait envoyé une requête ping à PC3 ?

_____