TP 1

Configuration & gestion de la sécurité d'un commutateur

Objectif

L'objectif de ces travaux pratiques est d'examiner et configurer un commutateur de réseau local autonome. Ses fonctions de base par défaut sont vérifiés et ses paramètres modifiés pour s'assurer que le réseau local est sécurisé et optimisé.
Pour cela, il faut :

- Créer une configuration de base de commutateur
- Gérer la table d'adresses MAC
- Configurer la sécurité des ports

Schéma de la topologie

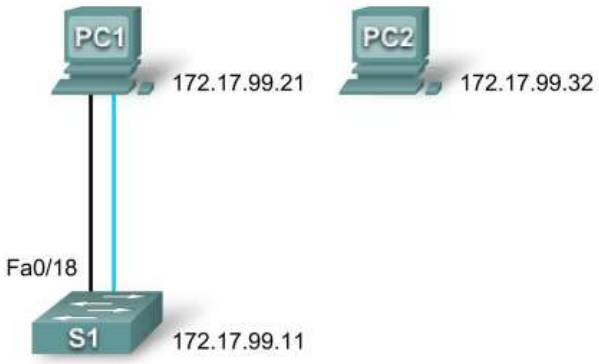

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	Carte réseau	172.17.99.21	255.255.255.0	172.17.99.1
PC2	Carte réseau	172.17.99.22	255.255.255.0	172.17.99.1
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

I. Tâche 1 : suppression d'une configuration existante & Vérification de la configuration par défaut

Étape 1: Etablir une connexion à la console du commutateur sur le post PC1

Étape 2: Supprimer le fichier de configuration initiale du commutateur de la mémoire NVRAM
Quelle commande faut-il utiliser ?

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Entrée]
[OK]
```

```
Erase of nvram: complete
```

Étape 3: Recharger le commutateur. **Quelle commande faut-il utiliser ?**

```
Switch#reload
Proceed with reload? [confirm] [Entrée]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<résultat omis>

Press RETURN to get started! [Entrée]

Switch>
```

Étape 4: Examiner la configuration en cours d'exécution du commutateur en utilisant la commande « **show running-config** ».

1. Combien d'interfaces Fast Ethernet le commutateur possède-t-il ? 24
2. Combien d'interfaces Gigabit Ethernet le commutateur possède-t-il ? 2
3. Quelle est la plage de valeurs affichée pour les lignes vty ? 16

Étape 5: Afficher les informations du logiciel Cisco IOS.

1. Quelle commande faut-il utiliser ? show version
2. Quelle version de Cisco IOS le commutateur exécute-t-il ? 12.2(25)SEE3 (peut varier)
3. Quel est le nom du ficher de l'image système ? C2960-LANBASE-M (peut varier)
4. Quelle est l'adresse MAC de base de ce commutateur ? varie

Étape 6: Examiner les propriétés par défaut de l'interface Fast Ethernet utilisée par PC1.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s

<Output Omitted>
```

1. L'interface est-elle activée ou désactivée ? elle doit être active
2. Quelle est l'adresse MAC de l'interface ? varie (ici 0060.5c36.4412)
3. Quels sont les paramètres de vitesse et de mode bidirectionnel de l'interface ? Mode bidirectionnel simultané, 100 Mbits/s

Étape 7: Examiner le contenu de la mémoire flash.

1. Deux commandes permettent d'examiner la mémoire flash, déterminer-les.
   dir flash: ou **show flash**
2. Quels sont les fichiers ou répertoires trouvés suite à l'exécution de l'une des deux commandes ? c2960-lanbase-mz.122-25.FX.bin (dépend s'il y a d'autres, exemple vlan.dat…)

III. Tâche 2 : création d'une configuration de base de commutateur

Étape 1: Passer en mode de configuration globale, et attribuer au commutateur le nom « **S1** »

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#hostname S1
S1(config)#exit
S1#
```

Étape 2: Passer en mode « **config-line** » pour la console et attribuer au mot de passe de connexion la valeur « **cisco** ». Configurer également les lignes vty 0 à 15 en utilisant le même mot de passe.

1. Quel est la liste des commandes à utiliser ?

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

2. Pourquoi la commande **login** est-elle requise ?

Sans la commande **login**, le commutateur ne requiert pas de mot de passe

Étape 3: Définir le mot de passe secret « class » pour le mode de commande.

```
S1(config)#enable secret class
```

Étape 4: Configurer l'adresse de la couche 3 du commutateur.

1. Créer un réseau local virtuel (VLAN 99) sur le commutateur.
2. Définir une adresse IP du commutateur sur 172.17.99.11 avec 255.255.255.0 comme masque de sous-réseau sur l'interface virtuelle interne VLAN 99, et activer-la. (Donner la liste de commandes correspondantes)

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

Étape 5: affecter les ports FastEthernet 0/1, 0/8 et 0/18 sur le VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

(pareil pour les autres interfaces)

Étape 6: Définir la passerelle par défaut du commutateur.

Afin de préciser la façon dont le commutateur transfère les trames de l'inter-réseau, il faut spécifier une adresse de passerelle par défaut qui pointe vers un routeur ou un commutateur de couche 3. On suppose que l'interface du réseau local soit 172.17.99.1 sur le routeur, et on utilise les commandes suivantes pour la définition de la passerelle par défaut.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Étape 7: Vérifier les paramètres d'interface sur VLAN 99 en utilisant la commande « show interface vlan 99 ».

```
S1#show interface vlan 99
```

```
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
<résultat omis>
```

1. Quelle est la bande passante définie sur cette interface ? BW 1000000 Kbits

Étape 8: Configurer l'adresse IP et la passerelle par défaut (172.17.99.11) pour le PC1. Vérifier ensuite sa connectivité en envoyant une requête « ping » au commutateur à partir du PC1

Ping doit réussir

Étape 9: Configurer les paramètres de vitesse du port et du mode bidirectionnel pour l'interface Fast Ethernet 0/18. Utiliser la liste des commandes suivante :

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

Vérifier les paramètres sur l'interface à l'aide de la commande « **show interface fastethernet 0/18** »

Étape 10: Enregistrer le fichier de configuration en cours sur la mémoire NVRAM. Quelle commande faut-il utiliser pour la sauvegarde.

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Entrée]
Building configuration...
[OK]
S1#
```

IV. Tâche 3 : gestion de la table MAC

Étape 1: Déterminer et enregistrer les adresses de couche 2 (physique) des cartes d'interface réseau des PC1 et PC2 (accès à partir des PCs).

Pour Déterminer les adresses (physiques) de couche 2 pour les cartes réseau PC, utiliser la commande **ipconfig /all** sur l'invite de commande (cmd)

Étape 2: Identifier les adresses MAC apprises par le commutateur.

1. Quelle commande faut-il utiliser pour afficher la table MAC? S1#**show mac-address-table**
2. Supprimer les adresses MAC existantes, en utilisant la commande « **clear mac-address-table dynamic** » en mode d'exécution privilégié.
3. Vérifier le résultat en affichant de nouveau la table MAC.

(Assurez-vous que la table d'adresses MAC a été effacée)

4. Envoyer une requête « **ping** » au commutateur S1 depuis PC1, ensuite, vérifier de nouveau la table MAC

L'adresse MAC du PC1 réapparaît de nouveau dans la table MAC du commutateur avec l'indication d'apprentissage dynamique

Étape 3: configurer une adresse MAC statique.

1. Configurer une adresse MAC statique sur l'interface Fast Ethernet 0/18 à l'aide de l'adresse qui a été enregistrée par PC1. Utiliser les commandes suivantes :

```
S1(config)#mac-address-table static [@MAC PC1] vlan 99 interface
fastethernet 0/18
S1(config)#end
```

2. Vérifier les nouvelles entrées de la table MAC

```
S1#show mac-address-table
```

L'adresse MAC du PC1 apparait dans la table MAC avec indication d'apprentissage statique

Étape 4: supprimer l'entrée MAC statique, en ajoutant « no » au début de la commande utilisée dans l'étape précédente.

1. Vérifier de nouveau la table MAC et s'assurer que l'adresse MAC a été supprimée

V. Tâche 4 : configuration de la sécurité des ports

Étape 1: configurer un deuxième hôte.

1. Définir l'adresse IP de PC2 sur 172.17.99.22, avec pour masque de sous-réseau 255.255.255.0 et pour passerelle de sous-réseau 172.17.99.11. Ne pas connecter encore ce PC au commutateur
2. Vérifier que PC1 et le commutateur sont correctement configurés en envoyant une requête « ping » à l'adresse IP de VLAN 99 du commutateur depuis l'hôte.

Étape 2: configurer la sécurité sur un port d'accès.

1. Etudier les options permettant de définir la sécurité des ports, en utilisant la commande « **switchport port-security ?** » en mode de configuration spécifique « **config-if** » de l'interface Fast Ethernet 0/18

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

2. Quelle commande utiliser pour configurer un port de commutateur pour n'accepter que deux périphériques ?

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
```

3. Quelle commande utiliser pour activer l'apprentissage rémanent d'un port du commutateur ?

```
S1(config-if)#switchport port-security mac-address sticky
```

4. Quelle commande utiliser pour désactiver le port en cas de violation ?

```
S1(config-if)#switchport port-security violation shutdown
```

5. Appliquer ces trois commandes à l'interface Fast Ethernet 0/18 en vue de la sécuriser.

Étape 3: vérifier les résultats.

1. Afficher les paramètres de sécurité du port à l'aide de la commande « **show port-security interface fa0/18** ».
   a. Combien d'adresses sécurisées sont alloués sur Fast Ethernet 0/18 ? 2
   b. Quelle est la mesure de sécurité appliquée à ce port ? désactivé
2. Examiner le fichier de configuration, y a-t-il dans la liste de la configuration en cours des instructions qui reflètent directement la mise en œuvre de la sécurité ? oui

Étape 4: modifier les paramètres de sécurité.

1. Sur l'interface Fast Ethernet 0/18, faites passer le nombre maximum d'adresses MAC de sécurité des ports à 1

```
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security violation shutdown
```

2. Vérifier les résultats :
   a. Afficher les nouveaux paramètres de sécurité en utilisant la commande « **show port-security interface fa0/18** »
   b. Lancer une requête « ping »sur l'adresse VLAN 99 du commutateur depuis PC1 pour vérifier la connectivité et actualiser la table d'adresses MAC
   c. Déconnecter le PC1 raccordé à fa0/18 depuis le commutateur, et connecter à sa place PC2. Envoyer ensuite une requête « ping » à l'adresse de VLAN 99 du commutateur depuis PC2. Décrire ce qui se passe suite à cette opération.

   Des messages de violation sont envoyés à la console. Voici les messages de console que le participant voit apparaître (le résultat spécifique à la sécurité des ports étant mis en évidence) :

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18,
changed state
to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18,
changed state
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0019.b90a.ab38 on port FastEthernet0/18.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18,
changed stateto down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Étape 5: réactiver le port

1. Reconnecter PC1 à fa0/18 et entrer les commandes suivantes sur le commutateur pour réactiver le port

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#end
```

2. Vérifier la connectivité en envoyant une requête « ping » de PC1 vers le commutateur S1.