

ACTIVITE 3

Gestion d'un switch

L'objectif de cette activité est de vous familiariser avec les commandes CISCO qui permettent la gestion du switch.

Pour paramétrer le switch, vous utiliserez la fiche "Fiche SWITCH - Commandes CISCO.pdf". Elle propose une description des principales commandes utilisées pour la configuration d'un switch.

Pour la suite de la l'activité, reprendre le fichier "Packet Tracer" utilisé lors de l'activité 2.

Gestion des adresses MAC

👉 1 – Faites communiquer les différents postes PC0, PC1, PC2 et PC3 (ping, ...). Ne faites pas communiquer les postes PC4, PC5 et PC6.

🔗 2 – Affichez la table des adresses MAC du switch (table ARP). Que constatez-vous ?

Commande CISCO : `TP_Switch2#show mac-address-table`

On dispose des adresses MAC des postes ayant traversé au moins une fois le switch. Pour chaque adresse MAC on a le VLAN (ici le vlan 1) et le port correspondant.

"DYNAMIC" signale que le switch a ajouté l'adresse MAC de façon dynamique.

"STATIC" signale que l'adresse MAC a été ajoutée par l'administrateur.

🔗 3 – Relevez les adresses MAC des postes PC4, PC5 et PC6.

Poste PC 4 : `0009.7CDC.EBAC`

Poste PC 5 : `00E0.B046.4E90`

Poste PC 6 : `0001.648C.D02A`

🔗 4 – Relevez les noms des interfaces du SWITCH utilisées pour connecter les postes PC4, PC5 et PC6.

Interface SWITCH pour le poste PC4 : `gig4/1`

Interface SWITCH pour le poste PC5 : `gig8/1`

Interface SWITCH pour le poste PC6 : `gig9/1`

👉 5 – Ajoutez manuellement les adresses MAC des postes PC4, PC5 et PC6 dans la table ARP du Switch.

Commande CISCO : `TP_Switch2(config)#mac-address-table static 0009.7CDC.EBAC vlan 1 interface gig4/1`

🔗 6 – Affichez la table des adresses MAC du switch. Que remarque-t-on ?

Commande CISCO : `TP_Switch2#show mac-address-table`

Remarque : Les adresses MAC et les adresses IP associées sont ajoutées à la table ARP du SWITCH. On remarque quelles sont ajoutées en mode "STATIC" puisque c'est l'administrateur qui les a ajoutées. On constate aussi que les adresses MAC "DYNAMIC" sont effacées de la table au bout de quelques minutes s'il n'y a pas eu de communication entre le poste et le SWITCH.

👉 7 – Pensez à sauvegarder votre travail (config actuelle vers démarrage).

Commande CISCO : `TP_Switch2#copy runnin-config startup-config`

✍ 8 – Proposez la commande pour effectuer un redémarrage avec une temporisation de 10 minutes (pas simulable sous Packet Tracer).

Commande CISCO : **TP_Switch2#reload in 10 (Pas simulable sous Packet Tracer)**

✍ 9 – Effectuez un redémarrage du switch, affichez la configuration et vérifiez que tout est correct.

Commandes CISCO :

TP_Switch2#reload

(mot de passe pour connecter la console au switch)

TP_Switch2#enable (plus mot de passe)

TP_Switch2#show running-config

A partir de maintenant, nous allons définir les adresses MAC qui peuvent accéder au switch. Il faut commencer par activer l'option sécurité sur l'interface que l'on désire contrôler. On travaillera sur les interfaces connectées aux postes PC1 et PC2.

✍ 10 – Relevez les adresses MAC des postes PC1 et PC2 ainsi que les interfaces utilisées sur le switch.

Poste PC 1 : **00E0.B09C.A19C**

Interface du switch : **gig1/1**

Poste PC 2 : **00D0.FFA1.EA85**

Interface du switch : **gig2/1**

✍ 11 – Activez la sécurité sur l'interface connectée au poste PC2.

Commandes CISCO :

TP_Switch2(config)#interface gig2/1

TP_Switch2(config-if)#switchport mode access

TP_Switch2(config-if)#switchport port-security

✍ 12 - Autorisez l'adresse MAC de PC2 à utiliser le switch.

Commande CISCO :

TP_Switch2(config-if)#switchport port-security mac-address 00D0.FFA1.EA85

✍ 13 – Testez en mode simulation :

- Communication (enveloppe PDU) de PC2 vers PC1. Conclusion ?

Cela fonctionne, le Poste 2 n'est pas bloqué car son adresse MAC est reconnue et acceptée par l'interface gig2/1 du switch. Fonctionnement normal

- Communication (enveloppe PDU) de PC1 vers PC2. Conclusion ?

Cela fonctionne puisque PC1 est connecté sur une interface gig1/1 non sécurisé, donc elle autorise toutes les communications par son port.

✍ 14 – Intervertissez les câbles des postes PC1 et PC2. Testez en mode simulation :

- Communication (enveloppe PDU) de PC2 vers PC1. Conclusion ?

Cela fonctionne puisque PC2 est connecté sur une interface gig1/1 non sécurisé, donc elle autorise toutes les communications par son port.

- Communication (enveloppe PDU) de PC1 vers PC2. Conclusion ?

Pas de communication car l'adresse MAC de PC1 ne correspond pas à celle définie au niveau de l'interface gig2/1. Le switch se met en sécurité et bloque l'interface gig2/1.

✍ 15 – Intervertissez à nouveau les câbles entre PC1 et PC2. Réactivez l'interface gig2/1.

Commande CISCO :

TP_Switch2(config)#interface gig2/1

TP_Switch2(config-if)#shutdown (il faut d'abord désactiver administrativement puis réactiver)

TP_Switch2(config)#no shutdown

✍ 16 – Vérifiez si l'adresse MAC de PC2 est associée à la bonne interface du switch (afficher la table d'adresse MAC). Refaire les pings entre PC1 et PC2. Conclusion ?

La communication entre PC1 et PC2 est correcte, le switch identifie bien l'adresse MAC de PC2.

Pour PC1 il n'y a pas de sécurité.

✍ 17 – Si l'adresse MAC de PC 2 n'apparaît pas dans la table, alors il faut aussi réactiver la sécurité sur l'interface concernée (voir les questions 11 et 12).

Commandes CISCO :

TP_Switch2(config)#interface gig2/1

TP_Switch2(config-if)#switchport mode access

TP_Switch2(config-if)#switchport port-security

TP_Switch2(config-if)#switchport port-security mac-address 00D0.FFA1.EA85

Détection automatique de l'adresse MAC

✍ 18 – Relevez l'adresse MAC du poste PC3 ainsi que l'interface utilisée sur le switch.

Poste PC 3 : 00D0.97E8.D1C1

Interface du switch : gig3/1

✍ 19 – Affichez la table des adresses MAC du switch et vérifiez que l'adresse MAC du poste 3 n'est pas présente.

Commande CISCO : TP_Switch2#show mac-address-table

✍ 20 – Activez la sécurité sur l'interface connectée au poste PC3.

Commandes CISCO :

TP_Switch2(config)#interface gig3/1

TP_Switch2(config-if)#switchport mode access

TP_Switch2(config-if)#switchport port-security

✍ 21 - Autorisez l'adresse MAC de PC3 à utiliser le switch (méthode découverte automatique de la première adresse MAC).

Commande CISCO : Switch (config-if)# switchport port-security mac-address sticky

✍ 22 – Affichez la table des adresses MAC du switch et vérifiez que l'adresse MAC du poste 3 n'est toujours pas présente.

Commande CISCO : TP_Switch2#show mac-address-table

✍ 23 – Faites un ping de PC3 vers PC4 et vérifiez si l'adresse MAC du poste 3 apparaît dans la table des adresses MAC. Conclusion :

L'adresse MAC de PC3 apparaît (en mode STATIC) dans la table

✍ 24 – Affichez les informations relatives à la sécurité de l'interface. Vérifiez que cela correspond à nos choix de sécurité.

Commande CISCO : **TP_Switch2# show port-security interface gig3/1**

✍ 25 – Intervertissez les câbles des postes PC3 et PC4. Faire un ping de PC4 vers PC3. Conclusion ?

Lorsque le ping est envoyé, le switch détecte l'adresse MAC de PC4 qui n'est pas celle autorisée (c'est l'adresse MAC de PC3 qui est autorisée sur ce port). Le switch bloque le port gig3/1 et on ne peut plus communiquer via ce port.

✍ 26 – Réactivez l'interface. Testez.

Commandes CISCO :

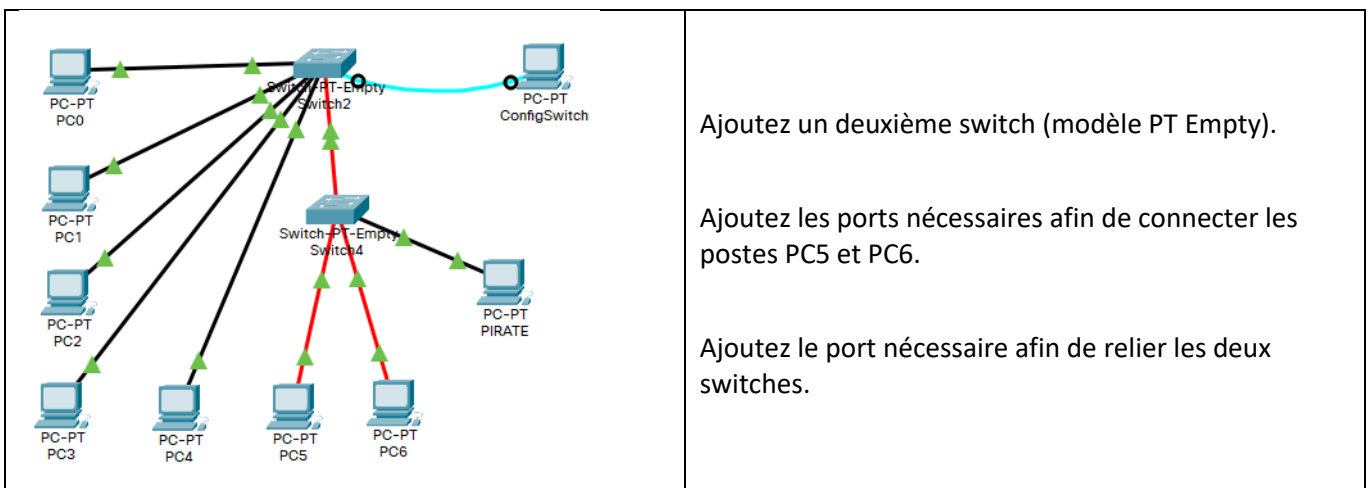
TP_Switch2(config)#interface gig3/1

TP_Switch2(config-if)#shutdown (il faut d'abord désactiver administrativement puis réactiver)

TP_Switch2(config)#no shutdown

A partir de maintenant, nous allons travailler sur l'interface qui connecte les postes PC5 et PC6.

👉 27 – Pour tester notre réseau, il faudra modifier le schéma :



✍ 28 – Relevez l'interface utilisée sur le switch principal pour connecter le switch secondaire.

Interface du switch : **gig8/1**

✍ 29 – Faites le nécessaire pour limiter le nombre de poste pouvant accéder sur ce port à 2. Cela veut dire que si vous connectez plus de deux postes alors le port se bloquera (mise en sécurité)

Commande CISCO :

TP_Switch2 (config)# interface gig8/1

TP_Switch2(config-if)#switchport mode access

TP_Switch2(config-if)#switchport port-security

TP_Switch2(config-if)#switchport port-security maximum 3

👉 30 – Faire un ping de PC5 vers PC0 puis de PC6 vers PC2 puis de "Pirate" vers PC3.

✍ 31 – Conclusion :

Lorsque le Poste PIRATE pingue PC3 alors le port se bloque : plus de trois "Postes" sur la même interface.