**Synthèse Réseaux et télécom – Q1**

**Ctrl+Z = exit**

**Config switch de base :**

1. **Attribuez un nom au commutateur.**

Switch# **configure terminal**

Switch(config)# **hostname S1**

S1(config)# **exit**

1. **Sécurisez l'accès à la console.**

S1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **line console 0**

S1(config-line)# **password letmein**

S1(config-line)# **login**

S1(config-line)# **exit**

**Une autre méthode est par la db local de toutes les I/O**

**En enable : username NomLog Mdp**   
**Allez dans conf t : line console 0**    
**login local**

1. **Sécurisez l'accès au mode privilégié.**

S1> **enable**

S1#**configure terminal**

S1(config)# **enable password c1$c0**

S1(config)# **exit**

1. **Configurez un mot de passe chiffré pour sécuriser l'accès au mode privilégié.**

Le mot de passe d'activation **enable password** doit être remplacé par le mot de passe secret chiffré plus récent à l'aide de la commande **enable secret** . Définissez **itsasecret** en tant que mot de passe secret actif.

S1# **config t**

S1(config)# **enable secret itsasecret**

S1(config)# **exit**

**Le mot de passe secret actif (enable secret) s'affiche sous forme chiffrée, tandis que le mot de passe d'activation (enable) s'affiche en clair.**

1. **Chiffrez les mots de passe d'activation (enable) et de console.**

S1# **config t**

S1(config)# **service password-encryption**

S1(config)# **exit**

**La commande service password-encryption chiffre tous les mots de passe actuels et futurs.**

1. **Configurer une bannière MOTD (message of the day).**

S1# **config t**

S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**

S1(config)# **exit**

**Le message s'affichera lorsque quelqu'un se connectera au commutateur par le biais du port de console.**

Pourquoi une bannière ?

**Chaque commutateur devrez avoir une bannière pour avertir les utilisateurs non autorisés que l'accès est interdit. Cette bannière peut également être utilisée pour envoyer des messages au personnel/techniciens de réseau (arrêts imminents du système, personne à contacter pour l'accès, etc.).**

1. **Enregistrer les fichiers de configuration dans la mémoire NVRAM**

S1# **copy running-config startup-config**

Destination filename [startup-config]?**[Enter]**

Building configuration...

[OK]

* On enregistre la config en cours

**Résumé** :

**Switch> enable**

**Switch# config t**

**Enter configuration commands, one per line.  End with CNTL/Z.**

**Switch(config)# hostname S2**

**S1(config)# line console 0**

**S1(config-line)# password letmein**

**S1 (config-line) # connexion**

**S1 (config-line) # activer le mot de passe c1$c0**

**S1(config)# enable secret itsasecret**

**S1 (config) # banner motd #tout texte ici#**

**S1(config)# service password-encryption**

**S1 (config) # exit**

**S1# copy running-config startup-config**

*Fin du document*

**Config IP switch :**

S1#**configure terminal**

Enter configuration commands, one per line.  End with CNTL/Z.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.253 255.255.255.0**

S1(config-if)# **no shutdown**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

**La commande no shutdown fait passer l'interface à l'état actif par voie administrative.**

**Config IP router :**

R1(config)# **interface gigabitethernet 0/0**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **description LAN connection to S1**

**IPV6 :**

1. **Étape 1: Vérifiez que le routeur est découvert pour tous les voisins.**

Pour visualiser les voisins **: show ipv6 neighbors**

Pour vider la table des voisins : **clear ipv6 neighbors**

Quand un périphérique nécessite-t-il le processus de découverte des voisins IPv6 ?

**Lorsque l'adresse MAC de destination n'est pas connue. Ce processus est similaire à ARP avec IPv4.**

Comment un routeur contribue-t-il à minimiser la quantité de trafic de découverte de voisins IPv6 sur un réseau ?

**Le routeur conserve les tables voisines de sorte qu'il n'a pas besoin d'initier ND pour chaque hôte de destination.**

Comment IPv6 minimise-t-il l'impact du processus ND sur les hôtes réseau ?

**Il utilise une adresse de multidiffusion de sorte que seule une poignée d'adresses écoutent les messages de découverte des voisins. IPv6 crée une adresse MAC de destination multidiffusion spécialement conçue qui inclut une partie de l'adresse du nœud.**

En quoi le processus de découverte des voisins diffère-t-il lorsqu'un hôte de destination se trouve sur le même réseau local et lorsqu'il se trouve sur un réseau local distant ?

**Lorsqu'un hôte de destination se trouve sur le même segment LAN, seul le périphérique correspondant à l'adresse IPv6 répond et d'autres périphériques déposent le paquet. Lorsque le périphérique est distant, le périphérique de passerelle (généralement un routeur) fournit l'adresse MAC de l'interface locale pour le MAC de destination, puis recherche l'adresse MAC sur le réseau distant. Le routeur placera ensuite la paire d'adresses IPv6/Mac répondant dans la table Neighbor IPv6. (similaire à un tableau ARP dans IPv4)**

**Configuration router :**

1. **Activation d'IPv6**

R1(config)#ipv6 unicast-routing   
R1(config)#

**Config :**

**ipv6 address 2001:db8:a::1/64**

**ipv6 address FE80::1 link-local**

Donner une adresse IPv6 en mode autoconfiguration (norme eui-64) :

(config-if)# ipv6 address <préfixe>/<masque> eui-64

Routage statique en IPv6 :

(config)# ipv6 route <adresse-réseau>/<masque> <passerelle>

Affichage de la NVRAM : **Show startup-config**

Enregistrez le fichier de configuration initiale dans la mémoire Flash à l'aide des commandes suivantes :

R1# **copy startup-config flash**

Destination filename [startup-config]

**Info de verification:**

Affichage de la config en cours :  S1# show running-config

Affichage de la version de l’IOS : S1#show version

Affichage du statut des interfaces : S1#Show ip interface brief

Bonus : Pourquoi certains ports FastEthernet sur les commutateurs sont-ils activés tandis que d'autres sont hors service?isissez vos réponses ici

**Les ports FastEthernet sont activés lorsque des câbles sont connectés aux ports, sauf s'ils ont été désactivés manuellement par les administrateurs. Dans le cas contraire, les ports sont hors service.**

Qu'est-ce qui pourrait empêcher l'envoi d'une requête ping entre des ordinateurs?

**Adresse IP incorrecte, média déconnecté, commutateur hors tension ou ports désactivés sur le plan administratif, pare-feu.**

*Fin du document*

Visualisation Infos des interfaces router :

R1> **show ip interface brief**

R1> **show ip interface InterfaceNameNumber**

Par exemple : show ip interface gigabiethernet 0/0

Visualisation de la table de routage

R1> **show ip route**

Comment un routeur traite-t-il un paquet destiné à un réseau qui ne figure pas dans la table de routage ?

**Un routeur n'envoie des paquets que vers un réseau répertorié dans la table de routage. Si un réseau ne figure pas dans cette table, le paquet est abandonné.**

Vérification de la gateway sur un routeur : **show run, show interfaces, show ip protocols**

INFO/CONFIG PC  :

1. **Quelle est mon adresse IPv4?**

Cliquez sur **Home PC** posé sur le bureau , et puis cliquez sur l'onglet **Desktop** (bureau)> **Command Prompt** (invite de commandes).

Entrez la commande **ipconfig** et examinez les informations d'adressage IPv4 pour **Home PC**

C:\> **ipconfig**

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:

   Link-local IPv6 Address.........: FE80::240:BFF:FEA6:4D5A

   IPv6 Address......................: ::

   IPv4 Address....................: 192.168.0.75

   Subnet Mask.....................: 255.255.255.0

   Default Gateway......................: ::192.168.0.1

L'adresse IPv4 est 192.168.0.75, qui est connue sous le nom d' **adresse IPv4 privée**. La plupart des ordinateurs clients et d'autres périphériques utilisent une adresse IPv4 privée. Ce sont des appareils qui n'ont pas besoin d'un autre appareil pour y accéder à partir d'Internet. Les adresses IPv4 privées sont utilisées pour conserver le nombre limité d' **adresses IPv4 publiques** routables globalement.

Vous pouvez utiliser la commande **route -n get default** pour déterminer la passerelle par défaut sur un ordinateur utilisant le système d'exploitation macOS ou Linux.

1. **Tracer le chemin entre la source et la destination**

C:\> **tracert www.hawaii.edu**

Tracing route to web00.its.hawaii.edu [172.31.149.56]

over a maximum of 30 hops:

  1 3 ms 4 ms 3 ms 10.0.0.1

  2 13 ms 16 ms 11 ms 10.120.89.61

  3 44 ms 18 ms 18 ms po-302-1222-rur02.monterey.ca.sfba.comcast.net [10.110.178.133]

  4 13 ms 14 ms 13 ms po-2-rur01.monterey.ca.sfba.comcast.net [10.139.198.129]

**Info PDU :**    
   
D'après les informations collectées durant la capture dans Packet Tracer, sur quel numéro de port le serveur web (**Web Server**) écoute-t-il la requête web ?

**La première PDU HTTP demandée par le client web affiche le port 80 sous le port DST de la couche 4.**

Sur quel port le serveur web (**Web Server**) est-il à l'écoute d'une requête DNS ?

**La première PDU DNS demandée par le client web affiche une destination de couche 4 du port 53.**

Les fils différents vont-ils modifier le traitement de la PDU de quelque manière que ce soit ? **Non**

Le **concentrateur** a-t-il perdu certaines informations ? Non

Que fait le **concentrateur** des adresses MAC et IP ? Rien

Le **point d'accès** sans fil a-t-il utilisé les informations qui lui ont été communiquées ?

**Oui Il les a réencapsulées au format 802.11 sans fil.**

Pourquoi les adresses MAC doivent-elles apparaître dans cet ordre ?

1. **Un commutateur peut commencer plus rapidement à transmettre une trame vers une adresse MAC connue si la destination est indiquée en premier.**

Quel périphérique utilise des adresses MAC commençant par 00D0:BA ? **Le routeur**

INFO ARP :

Sur un pc : Observez la table Arp : **arp -a**

Vider la table Arp :  **arp -d**

D'une manière générale, à quel moment un périphérique final émet-il une requête ARP ?

**Lorsqu'il ne connaît pas l'adresse MAC du destinataire.**

Sur un switch : **show mac-address-table**.

Sur un routeur : show arp

Info : **L’adresse de passerelle de l’interface du routeur est stockée dans la configuration IPv4 des hôtes. Si l’hôte destinataire ne se situe pas sur le même réseau, l’hôte source fait appel au processus ARP pour déterminer l’adresse MAC de l’interface du routeur qui sert de passerelle.**

Avant line vty avec login et transport input ssh

Routeur securité :

Router#conf t    
Router(config)# hostn R0

R0(config)# ip domain-n

R0(config)#ip domai-name CIA

R0(config)#crypto key generate rsa

how many bits in the modulus [512] :1024

R0(Config)# ip ssh version2

Connexion : ssh –L Username Addr\_IP

Password :

Router(config)# **ip route** *AdresseDuRéseau MasqueDeSous-réseau InterfaceDeSortie*