TP 5

CISCO et le simulateur Packet Tracer

Partie 1 : Matériels CISCO

1) Le système d'exploitation Cisco

Les routeurs, switchs et catalysts Cisco sont classés par gamme comprenant chacune plusieurs modèles. L'IOS, le système d'exploitation, est le même sur l'ensemble des matériels. L'IOS se décline selon plusieurs gammes appelées packages dont les fonctionnalités varient en fonction des capacités du matériel. Les switchs fonctionnent aux niveaux 1 et 2, les routeurs aux niveaux 1,2 et 3, les catalysts sont des switchs (donc niveau 2) ayant des fonctionnalités de routage (niveau 3) plus ou moins réduites selon la gamme.

2) Architecture matériel

L'architecture compte 5 composants :

Le CPU : de la puissance du CPU dépend la capacité de traitement du matériel.

La mémoire flash : sous forme d'une barrette ou d'une carte permet de stocker une ou plusieurs images de l'IOS souvent compressées.

La ROM : mémoire permanente contenant le code de diagnostique du matériel ainsi que le code de chargement de l'image contenu dans la mémoire flash vers la RAM. C'est l'équivalent du BIOS.

La RAM : mémoire volatile contenant toutes les informations permettant au matériel de fonctionner (table de routage, table ARP, table de VLAN, ...). L'IOS se charge en RAM au démarrage du matériel.

La NVRAM : mémoire non volatile, c'est la mémoire de masse, l'espace de stockage de la configuration.

Au démarrage le programme de la ROM charge une image de la Flash vers la RAM, la première action de l'IOS est de charger la configuration stockée dans la NVRAM vers la RAM. Si on modifie la configuration présente dans la NVRAM en cours de fonctionnement, le matériel ne prendra en compte les modifications qu'au prochain chargement de cette configuration dans la RAM. Si on modifie la configuration présente dans la RAM en cours de fonctionnement, le matériel prendra en compte les modifications instantanément.

3) Configuration du matériel

Il existe différents moyens pour configurer le matériel :

– Par la porte console (c'est une liaison série avec un terminal) qui donne accès à la CLI (Command Line Interface), une console de commande en ligne.

– Par Telnet ou SSH pour avoir accès à la CLI à distance (nécessite que le matériel possède une adresse IP).

– Par TFTP en chargeant une configuration complète (nécessite que le matériel possède une adresse IP).

– Par l'interface WEB CMS (Cluster Management Suite) lorsqu'elle existe (nécessite que le matériel possède une adresse IP).

– Par SNMP par une console d'administration SNMP (nécessite généralement que le matériel possède une adresse IP).

La configuration initiale se fait donc par la console.

4) Interpréteur de commande (CLI exec)

L'interpréteur de commande, comme son nom l'indique, est responsable de l'interprétation des commandes que vous tapez. La commande interprétée, si elle est correcte, réalise l'opération demandée.

```
lab-bt#sh arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 128.253.154.204 0 0080.c723.989f ARPA Ethernet0

Internet 128.253.154.110 0 0040.951a.24c4 ARPA Ethernet0

Internet 128.253.154.116 - 0010.7bc2.07cf ARPA Ethernet0

Internet 128.253.154.2 0 0000.4d21.8405 ARPA Ethernet0

Internet 128.253.154.9 0 0040.055a.9476 ARPA Ethernet0

lab-bt#
```

Si lors de la configuration initiale un (ou des) password a été configuré, vous devez introduire ce password pour accéder à l'interpréteur de commande.

Il y a 2 modes d'exécution sur un routeur Cisco :

1. Le mode utilisateur (prompt : >)
2. Le mode privilégié (prompt : #)

Lors de la connexion initiale avec le routeur, vous arrivez dans le mode utilisateur. Pour passer au mode privilégié, vous devez introduire la commande "enable" et ensuite introduire un mot de passe. Le mode utilisateur sert uniquement à la visualisation des paramètres (pas de la configuration) et des différents status du routeur. Par contre, le mode privilégié permet, en plus de la visualisation des paramètres, la configuration du routeur et le changement de paramètres dans la configuration.

L'interpréteur de commande des routeurs Cisco est très souple et vous permet de demander les commandes disponibles. Vous désirez savoir les commandes qui commencent par "ho", rien de plus simple, ho ? <enter>. Il est aussi possible d'utiliser l'expansion de commande comme sous Unix (avec la touche de tabulation). Si il n'y pas de confusions possibles, vous pouvez utiliser les abréviations de commande. Par exemple, "sh ip int brie" au lieux de "show ip interface brief". Cela permet de gagner du temps et de rendre la vie un peu plus facile.

5) Les fichiers de configuration

Dans un routeur cisco (en général), il existe différents fichiers de configuration. Il y a un fichier de configuration dans la nvram (startup-config), qui est lu au démarrage du routeur et copié en mémoire.

Il y a un autre fichier de configuration dans la mémoire vive (running-config).

La "startup-config" est conservée dans la nvram sous forme ASCII. Tandis que la “running-config” est dans la ram sous forme binaire.

6) Configuration générale

Lorsque vous désirez passer en mode configuration, vous devez taper (en mode enable) :

```
conf terminal
```

Cela signifie que vous configurer le routeur en mode terminal. Il est tout à fait possible de configurer via TFTP par exemple. A ce moment le prompt change en :

```
router(config)#
```

Donc vous êtes dans la racine de la configuration du routeur et vous pouvez configurer les paramètres généraux.

7) Configuration des interfaces

Mais lors de la configuration d’un routeur, vous configurez souvent des interfaces. Il est donc nécessaire de passer du mode configuration générale vers la configuration de l’interface.

Voici un exemple :

```
router> enable
password :
router#configure terminal
router(config)#interface ethernet 0
router(config-if)#ip address 10.1.1.1 255.255.255.0
router(config-if)#exit
router(config)#exit
router#copy running-config startup-config
```

Dans cet exemple, on peut voir la configuration de l’interface ethernet 09 avec son addresse IP et son masque réseau. Lors de ce genre de configuration, nous modifions la configuration "running" et donc nous réalisons un "copy running-config startup-config" pour sauver la configuration dans la nvram.

8) Configuration des lignes VTY

Il existe aussi différent types d’interfaces à configurer. Par exemple, la configuration des interfaces vituelles (pour l’accès via telnet du cli-exec) se fait de la même manière que les interfaces.

```
gw-int>enable
password :
gw-int#configure terminal
```

```
gw-int(config)#line vty 0 6
gw-int(config-line)#password MonSuperPasswordd
gw-int(config-line)#exec-timeout 15 0
gw-int(config-line)#exit
gw-int(config)#exit
gw-int#
```

Dans ce cas, on configure le password pour 7 sessions possibles via telnet sur le routeur. On spécifie le password (sinon on ne sait pas se connecter à distance) ainsi que le timeout d'utilisation pour fermer les sessions quand elles ne sont plus utilisées.

9) Configuration des interfaces routages

La configuration des protocoles de routage est réalisé de la même manière que les interfaces.

"router leprotocolederoutage"

Protocole de routage	Description
bgp	Border gateway protocol
egp	Exterior gateway protocol
igrp	Interior gateway protocol
isis	ISO IS-IS
iso-igrp	IGRP pour les réseaux OSI
ospf	Open shortest path first
rip	Routing information protocol
static	Static CLNS routing

```
ip-int-gw>enable
password :
ip-int-gw#configure terminal
ip-int-gw(config)#router ospf 303
ip-int-gw(config-router)#network 145.30.6.0
ip-int-gw(config-router)#exit
ip-int-gw(config)#exit
ip-int-gw#
```

10) Access Lists

Les routeurs Cisco fournissent la possibilité de faire du filtering. Les “access lists” peuvent être configurées pour tous les protocoles routables (IP, IPX, AppleTalk, ...). Vous pouvez configurer les “access lists” sur chaque routeur de façon indépendante.

Les “access lists” permettent de prévenir l’accès sur votre réseau. Les “access lists” ne sont pas uniquement destinées à la sécurité mais peuvent être utilisées dans le cadre de contrôles d’ouverture de ligne (DDR, ...).

Utilisation des access lists

Les access list filtrent le traffic réseau en contrôlant si des paquets routés sont transférés ou bloqués sur le(les) interface(s) du routeur. Un routeur peut examiner chaque paquet suivant ce que vous avez spécifié dans les access lists. Il est à noter que la sécurité est minimum, un utilisateur averti pourrait contourner les access lists. Les critères d’une access list sont l’adresse de source du traffic, la destination du traffic, le niveau de protocole ou d’autres informations. Pourquoi utiliser des access lists.

Il y a beaucoup de raisons pour configurer des access lists :
- Restreindre la mise à jour des tables de routage
- Contrôler le flux du réseau (pour les route-map par exemple)
- Et bien sûr limiter les accès aux réseaux ou à des services spéficiques du routeur.

Vous pouvez utiliser les access lists pour fournir un niveau minimum de sécurité. Si aucune acess lists n’est configurée, le traffic passe sans aucune restriction à travers le routeur.

Création d’access lists

Il y a 2 étapes pour la création de listes de contrôle. La première est de créer l’access list et la seconde étape est de l’appliquer sur l’interface. Lors de la création de l’acess list, il faut lui assigner un identificateur unique. Dans la majorité des cas, vous devrez utiliser un numéro (suivant le type de protocole à filtrer). Il est aussi possible d’utiliser une access list basée un nom mais uniquement avec certains protocoles.

Protocole	Espace
IP	1 à 99
Extended IP	100 à 199
Ethernet type code	200 à 299
Ethernet address	700 à 799
Transparent bridging (protocol type)	200 à 299
Transparent bridging (vendor code)	700 à 799
Extended transparent bridging	1100 à 1199

DECnet & extended DECnet	300 à 399
XNS	400 à 499
Extended XNS	500 à 599
Appletalk	600 à 699
Source-route bridging (protocol type)	200 à 299
Source-route bridging (vendor code)	700 à 799
IPX	800 à 899
Extended IPX	900 à 999
IPX SAP	1000 à 1099
VINES	1 à 100

La création d'une access list est une suite de critères avec les paramètres sources, destinations, ou types de protocole. Pour une access list donnée (un numéro unique ou un nom unique) vous pouvez avoir plusieurs entrées. Vous n'êtes pas limité dans la taille de la liste (juste par la mémoire). Par contre, plus la liste est longue, plus elle prend du temps à être parcourue (!).

Exemple :

```
interface serial 0/4
ip addresse 192.168.1.254 255.255.255.0
ip access-group 1 in
!
!
access-list 1 permit 192.168.1.1
access-list 1 deny 192.168.2.0 0.0.0.255
```

A la fin de chaque access lists, il y a la règle implicite "deny all traffic". Ce qui signifie que ce qui n'est pas spécifié est interdit.

L'ordre des entrées dans l'access-list est important et c'est la première règle qui satisfait qui est prise en compte.

Lors de la modification d'une access list, il est difficile de la modifier. Il vous est impossible d'insérer une règle dans l'acces list. La seule solution est d'effacer la liste et de la recréer (même si vous avez 300 entrées). Vous pouvez aussi copier la liste en TFTP et ensuite la recharger en TFTP.

Partie 2 : Utilisation du simulateur Packet Tracer

Nous allons utiliser le simulateur Packet Tracer de CISCO. Vous le trouverez ici : http://nicolas.durand.perso.esil.univmed.fr/pub/reseaux/tp5/

Dans sa version 4 (et supérieure) la configuration des matériels est simplifiée grâce à l'interface graphique (les commandes équivalentes s'affichent alors dans la console). Vous pouvez tout de même taper les commandes directement dans la console d'un matériel, si vous le désirez.

Tout au long du TP, vous noterez les commandes que vous obtenez lors de l'utilisation et la configuration de vos matériels. Notez seulement les commandes la première fois *quelles sont rencontrées.*

Remarque : vous avez la possibilité de modifier un matériel en lui ajoutant des modules (par exemple, des ports Ethernet 100Mb supplémentaires). Pour faire cela, vous devez éteindre le matériel, modifier les modules, puis le rallumer. ATTENTION : si vous avez modifié la configuration du matériel, vous devez *enregistrer* la configuration dans la NVRAM du matériel en question avant de l'éteindre, sinon vous perdrez votre configuration.

Travail à réaliser :

Concevez un petit réseau d'entreprise en utilisant Packet Tracer. Il y aura par exemple un sous-réseau pour la comptabilité, l'administration, un autre pour la production, … Il faudra aussi prévoir des serveurs (DNS, Web, …), …

Pensez à noter dans un document les explications de votre réseau : les sous-réseaux, les machines, leurs rôles, leurs adresses, leurs configurations, … (toutes informations jugées importantes).

A envoyer par email : le document et le fichier ".pkt" du réseau réalisé avec Packet Tracer.