Cisco: Commandes Utiles

Toutes les commandes de bases

- Activer le SSH
- Changer la vitesse des interfaces
- Configuration de base d'un élément actif Cisco
- Routage dynamique BGP
- Routage Dynamique OSPF (MD5)
- Routage Dynamique RIP
- ROUTEUR - Configurer les ACL
- ROUTEUR - Configurer un DHCP sur un routeur Cisco
- ROUTEUR - Routage hybride EIGRP
- ROUTEUR - Routage statique
- ROUTEUR - Tunnel IPSec entre 2 routeurs
- SWITCH - Activer VTP
- SWITCH - Créer un Vlan
- Switch - Port Monitoring (Switch Port Analyzer)
- Switch - Port Security
- CISCO - Premiers pas

Activer le SSH

Secure SHell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

```
Switch(config)#hostname 2960-RG
2960-RG(config)#ip domain-name mondomaine.local
2960-RG(config)#crypto key generate rsa general-keys modulus 1024
2960-RG(config)#ip ssh version 2
2960-RG(config)#line vty 0 15
```

Changer la vitesse des interfaces

```
R1(config)#interface <nom de l’interface>
R1(config-if)#speed <valeur en mb/s>
```

Configuration de base d'un élément actif Cisco

Voici une configuration de base utilisable en copié/collé pour réaliser vos pré-configuration.

Elle permet de mettre le nom de la machine, le mot de passe pour le mode configuration, le mot de passe pour le mode console et le mot de passe pour les sessions vty (ici, 2 autorisé seulement).

On demande aussi à ne pas être dérangé lors de l'utilisation de la console par les messages systèmes.

Aussi, la bannière indispensable pour indiquer les risques encouru par un utilisateur non autorisé.

```
conf t

hostname X

enable secret XYXYXYXYXY

banner motd  % =========Toute personne non autorise se verra poursuivi en fonction des lois en vigueur ============ %

service password-encryption

no ip domain-lookup

line console 0

password XXXXYYXXXX

login

logging synchronous

line vty 0 2

password YYYYYXXYYYY

login

logging synchronous

exit
```

Routage dynamique BGP

Théorie

BGP pour Border Gateway Protocol est le protocole qui est utilisés afin de faire du routage dynamique. Mais contrairement à OSPF, RIP ou EIGRP, BGP est un protocole EGP (Exterior Gateway Protocol), utilisé pour l'échange d'informations de routage entre des systèmes autonomes (FAI, fournisseurs de contenu, ...).

BGP utilise le port TCP/179.

(Très) Bonne pratique:

Pour tous les protocoles de routage (excepté RIP), positionner le router-id 'manuellement'. Le router-id possède le format d'une adresse IP mais peut ne pas correspondre a une adresse IP définie sur le routeur, cependant, il est plus simple, et plus logique du point de vue administration et exploiatation que cette adresse IP corresponde à une address de loopback définie localement.

Le router-id determine (entre autre) qui est le serveur BGP et qui est le client BGP. Le routeur possédant le router-id le plus élevé sera le client (TCP) et initiera la connexion vers le serveur - qui sera donc le routeur avec router-id le plus petit.

Mise en oeuvre

```
Router(config)# router bgp <numéro-as>
Router(config-router)# bgp router-id <addresse-ip>
Router(config-router)# neighbor <adresse-ip> remote-as <numéro-as>
Router(config-router)# network adresse-réseau [mask masque-réseau]
```

Vérification

La commande `show ip route bgp` permet de visualiser les routes acquises par le protocole BGP.

La commande `show ip bgp` permet de vérifier que les réseaux IPv4 reçus et annoncés figurent bien dans la table BGP.

La commande `show ip bgp summary` ou `show bgp ipv4 unicast summary` permet de vérifier les voisins BGP IPv4 et d'autres informations BGP.

Source

https://www.cisco.com/c/fr_ca/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Routage Dynamique OSPF (MD5)

`router ospf <process-id>` (entre 1 et 65535)
`router-id <rid>` (en forme de 0.0.0.0, qui n’est pas une adresse ip)
`network <network-address> <wildcard-mask> area <area-id>`
`passive-interface <interface-name>` (pour empêcher la transmission de message)
`auto-cost reference-bandwidth <débit en Mb/s>` (sur chaque routeur, pour changer le cout)
`show ip ospf neighbor` (voir les routeur voisins)

OSPF MD5

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MYPASS
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
```

Routage Dynamique RIP

> En v1 il ne prends pas en compte les masques, contrairement à la v2. Si la v1 reçois des paquets de v2, il va les lire comme des v1. La v2 ne lit que les paquets de la v2.

Activer RIP

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network network-address
```

(paramètres du protocole de routage)

```
R1#show ip protocols
```

(liste des routes)

```
R1#show ip route
```

(désactive les classes automatiques (que en version 2))

```
R1(config-router)#no auto-summary
```

(ajouter une route)

```
R1#ip route 0.0.0.0 0.0.0.0
```

(route par défaut propagé)

```
R1#default-information originate
```

(empêche la transmission des routes via RIP)

```
R1(config-router)#passive interface g0/0
```

(empêche à toute les pattes de transmettre)

```
R1(config-router)#passive interface default
```

(autorise la transmission du RIP)

```
R1(config-router)#no passive interface
```

ROUTEUR - Configurer les ACL

```
RT_MAIN > enable
RT_MAIN # conf t
```

Création de la liste 10

```
RT_MAIN (config) # access-list 10 permit 192.168.10.0 0.0.0.255
```

Config de l'interface

```
RT_MAIN (config) # interface eth 1/0
```

Application liste out

```
RT_MAIN (config-if) # ip access-group 1 out
```

Cette règle ACL standard autorise le réseau 192.168.10.0 à sortir de l'interface eth0 pour communiquer avec le réseau 192.168.12.0.
Le réseau 192.168.11.0 ne pourra pas communiquer avec le réseau 192.168.12.0.

Acl pour faire passer les ip impaires :

```
access-list 10 permit 192.168.0.1 0.0.0.254
```

Exemple de commande:

```
access-list 102 permit tcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eq 22
```

J'autorise sur le reseau 192.168.2.0 d'aller sur l'HTTP vers le réseau 3.0

Attention: On peut mettre qu'une ACL in et une ACL out par pattes

ROUTEUR - Configurer un DHCP sur un routeur Cisco

Se connecter et passe en mode config terminal

```
ROUTER > enable
ROUTER # conf t
```

Créer une étendue DHCP

```
ROUTER (config) # ip dhcp pool LAN1
```

Définir la passerelle

```
ROUTER (dhcp-config) # default-router 192.168.1.1
```

Définir l'adresse et le masque de l'étendue

```
ROUTER (dhcp-config) # network 192.168.1.0 255.255.255.0
```

Définir le(s) serveur(s) DNS

```
ROUTER (dhcp-config) # dns-server 192.168.1.254
ROUTER (dhcp-config) # exit
```

Exclure des adresses

```
ROUTER (config) # ip dhcp excluded-address 192.168.1.1 192.168.1.254
```

ROUTEUR - Routage hybride EIGRP

Activer l'EIGRP
`router eigrp <autonomous-system>` (la valeur autonomous-system doit être la même sur tous les routeurs)

Dire au routeur sur quel réseau il doit opérer
`network <network> <wildcard-mask>`
Pour trouver le wildcard-mask, il suffit de soustraire 255 à chaque partie du masque
Exemple:

	255	255	255	255
-	255	255	255	0
=	0	0	0	255

Dans cet exemple, un masque **255.255.255.0** aura donc un wildcard de **0.0.0.255**

Une fois l'EIGRP activé, le routeur va commencer à envoyer des "HELLO PACKET" pour découvrir les autres routeurs EIGRP et essayer d'établir une relation de voisinage (neighbor relationship)

Il reste plus qu'a faire la même chose sur chaque routeur

Pour voir la liste des routeurs "voisins", il suffit d'utiliser la commande
`show ip eigrp neighbors`

Exemple de configuration

```
R1(config)#router eigrp 1
R1(config-router)#network 192.168.1.0 0.0.0.255
```

ROUTEUR - Routage statique

2019-05-23_13h23_47.png

Premier routeur :
Notre premier routeur connaît les routes pour aller sur le réseau 1.0 et 2.0 puisqu'il y est connecté, par contre, il ne sait pas comment accéder aux réseaux 3.0, 4.0 et 5.0. Il faut donc lui indiquer le chemin à prendre. (En gros il est perdu et on lui donne un GPS)

```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.253
```
(on veut aller sur le réseau 3.0, pour y accéder, il est nécessaire de passer par la "patte" 192.168.2.253.)
```
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.253
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.253
```

Deuxième routeur :
Quant à lui, notre deuxième routeur ne connaît pas le chemin pour 1.0 et 5.0
```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.254
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.253
```

Troisième routeur :
Notre troisième routeur ne connaît pas le chemin pour aller en 3.0, 2.0 et 1.0.
```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.4.254
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.4.254
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.254
```

ROUTEUR - Tunnel IPSec entre 2 routeurs

On entend souvent qu'il est difficile de faire du VPN IPSec entre 2 routeurs. Bon, c'est en partie vrai mais pas tant que ça.

Voici un exemple concret d'une topologie VPN fonctionnel.

N'oubliez pas de faire attention à la sécurité si vous souhaitez vous en inspirer.

VPN-IpSec-schema.png

Les routeurs Maxime et Jean-Clément vont être configuré pour faire du VPN entre eux, le routeur Stéphane simule un FAI.

Configuration des interfaces

R-Maxime	R-Jean-Clément	R-Stéphane

`hostname Maxime`
`interface g0/0`
`ip add 70.0.0.1 255.255.255.252`
`no shut`
`interface g0/1`
`ip add 192.168.6.254 255.255.255.0`
`no shut`
`exit`
	`hostname JC`
	`interface g0/0`
	`ip add 60.0.0.2 255.255.255.252`
	`no shut`
	`interface g0/1`
	`ip add 192.168.5.254 255.255.255.0`
	`no shut`
	`exit`
		`hostname Stephane`
		`interface fa0/0`
		`ip address 60.0.0.1 255.255.255.252`
		`no shut`
		`interface fa0/1`
		`ip address 70.0.0.2 255.255.255.252`
		`no shut`

Configuration des routes

Une route par défaut pour les routeurs Maxime et Jean-Clément et 2 routes pour le routeur Stéphane

R-Maxime	R-Jean-Clément	R-Stéphane
`ip route 0.0.0.0 0.0.0.0 g0/0`	`ip route 0.0.0.0 0.0.0.0 g0/0`	`ip route 192.168.5.0 255.255.255.0 fa0/0` `ip route 192.168.6.0 255.255.255.0 fa0/1`

Configuration VPN

R-Maxime

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key schtroumph address 60.0.0.2 255.255.255.252

crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac
exit
access-list 101 permit ip 192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
crypto map babar 12 ipsec-isakmp
set peer 60.0.0.2
set transform-set schtroumph
match address 101
exit
interface g0/0
crypto map babar
exit
```

R-Jean-Clément

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 7200
crypto isakmp key schtroumph address 70.0.0.1 255.255.255.252

crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac
exit
access-list 101 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
crypto map babar 12 ipsec-isakmp
set peer 70.0.0.1
set transform-set schtroumph
match address 101
exit
interface g0/0
crypto map babar
exit
```

Il faut peut être quelques explications.

Configuration du ISAKMP (IKE)

- `crypto isakmp policy X` permet d'initier une règle de connexion avec un autre routeur. Le X peut être ce que vous voulez comme nombre.
- Ensuite, on configure le type de `hash` (faite ? après `hash` pour connaitre les options). Ici ce sera en md5
- `authentication pre-share` permet d'indiquer l'utilisation d'un mot de passe partagé entre les 2 routeur pour l'initialisation de la connexion.
- `group 2` C'est le type de groupe pour Diffie-Hellman.
  Les groupes Diffie-Hellman déterminent la force de la clé utilisée dans le processus d'échange de clés. Les groupes portant un numéro supérieur sont plus sûrs, mais il faut plus de temps pour créer la clé.

  - Groupe Diffie-Hellman 1 : groupe 768 bits
  - Groupe Diffie-Hellman 2 : groupe 1024 bits
  - Groupe Diffie-Hellman 5 : groupe 1536 bits
  - Groupe Diffie-Hellman 14 : groupe 2 048 bits
  - Groupe Diffie-Hellman 15 : groupe 3 072 bits
  - Groupe Diffie-Hellman 19 : groupe de courbe elliptique 256 bits
  - Groupe Diffie-Hellman 20 : groupe de courbe elliptique 384 bits

  Les deux pairs d'un échange VPN doivent utiliser le même groupe, qui est négocié pendant la phase 1 du processus de négociation IPSec. Lorsque vous définissez un tunnel BOVPN manuel, vous spécifiez le groupe Diffie-Hellman pendant la phase de création d'une connexion IPSec. Cette phase désigne le stade où deux pairs créent un canal sécurisé et authentifié pour communiquer.
  Attention à votre débit, si c'est en local (si si, c'est faisable dans certains cas), choisissez ce que vous voulez, si c'est distant et faible en débit, attention à la taille de la clef !
- `lifetime 7200` Durée de vie de la clé de session
- `crypto isakmp key schtroumph address 70.0.0.1` C'est **LA** commande qui définit le mot de passe et l'adresse **PUBLIC** du routeur destinataire.

Configuration et Application de l'IPSec

- `access-list 101 permit ip 192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255` Création d'une ACL permettant au réseau de Maxime d'atteindre le réseau LAN de Jean-Clément
- `crypto ipsec transform-set schtroumph esp-aes esp-sha384-hmac` Création d'une transformation IPSec et utilisation du mot de passe définit avant et de la méthode de chiffrement. Il y a plusieurs choix pour la méthode de chiffrement et son option. Pensez à utiliser le ?
- `crypto map babar X ipsec-isakmp`
  `set peer 70.0.0.1`
  `set transform-set schtroumph`
  `match address 101` Ces commandes permettent la création de la Crypto Map (et son nom babar) et de définir le destinataire de ce VPN, le mot de passe d'initialisation de connexion et l'ACL à utiliser.

- `interface g0/0`
  `crypto map babar` Maintenant, on applique la Crypto Map (via son nom) à l'interface de sortie WAN du routeur.

Il est possible d'avoir plusieurs map à appliquer en fonction du nombre de site que vous souhaitez interconnecter.

La condition de fonctionnement est l'utilisation des mêmes options et mots de passe sur le routeur distant.

Et normalement, ça ping :)

Vous voyez, c'est pas trop difficile.

SWITCH - Activer VTP

VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local.

```
2960-RG(config)#vtp domain “nom”
2960-RG(config)#vtp mode server / client / transparent
2960-RG(config)#vtp password “password”
2960-RG(config)#vtp version 2
```

SWITCH - Créer un Vlan

Créer un seul Vlan

```
2960-RG(config)# vlan 2
```

Créer plusieurs Vlans

```
2960-RG(config)# vlan 3,4,5
```

Afficher la liste

```
2960-RG# show vlan
```

Pour l’affecter à un port

```
2960-RG(config)# interface fastEthernet 0/1
2960-RG(config-if)# switchport mode access
2960-RG(config-if)# switchport access vlan 3
```

Pour plusieurs ports

```
2960-RG(config)# interface range fastEthernet 0/5-8
2960-RG(config-if-range)# switchport mode access
2960-RG(config-if-range)# switchport access vlan 4
```

Switch - Port Monitoring (Switch Port Analyzer)

Mise en place du port monitoring sur un switch Cisco

- Soit l'interface source : fa0/1 -> Le port à monitorer
- Soit l'interface de destination : fa0/2 -> Miroir du port monitoré, on peut y raccorder une sonde pour analyser le flux réseau. (Solution Ntop)

```
SW01# configure terminal
SW01(config)# monitor session 1 source interface fa 0/1 both (Rx/Tx)
SW01(config)# monitor session 1 destination interface fa 0/2
SW01(config-if-range)#end
```

- Afficher les surveillances SPAN d'un switch

```
SW01#show monitor all
```

- Désactivation SPAN

```
SW01#config terminal
SW01(config)#no monitor session all
SW01(config)#end
SW01# wr
```

- Exemple de mise en oeuvre

fdyCr3FWEPvXLOLb-image-1568310136439.png

Switch - Port Security

Configuration de la sécurité des ports

- Activer la sécurité des ports sur les ports Fast Ethernet 0/1 et 0/2.

`conf t`

`interface fa0/1`

`switchport mode access`

`switchport port-security`

`interface fa0/2`

`switchport mode access`

`switchport port-security`

- Opter pour le niveau maximum, de sorte qu'un seul périphérique puisse accéder aux ports Fast Ethernet 0/1 et 0/2.

`switchport port-security maximum 1`

- Sécuriser les ports de sorte que l'adresse MAC d'un périphérique soit apprise de manière dynamique et ajoutée à la configuration en cours.

`Switchport port-security mac-address sticky`

- Définir la violation de sorte que les ports Fast Ethernet 0/1 et 0/2 ne soient pas désactivés en cas de violation, mais que les paquets soient abandonnés s'ils proviennent d'une source inconnue.

`switchport port-security violation protect`

- Désactiver tous les ports inutilisés restants.

`Interface range fa0/3-24`

`shutdown`

`exit`

- Pour vérifier l'état d'un port (fa0/2 par exemple).

`sh port-security inter fa0/2`

CISCO - Premiers pas

Il faut penser aux jeunes et leur permettre de se débrouiller dans cet environnement inconnu.

IOS de Cisco (le nom du système d'exploitation) est assez bien fait et permet de se débrouiller sans connaitre par cœur des centaines de commandes.

Mais commençons par le début.

Pour utiliser du Cisco à moindre coût, le plus simple est de s'enregistrer sur le site de Cisco Netacad (site pour l'apprentissage) puis de télécharger le logiciel Packet Tracer :

https://www.netacad.com/fr/courses/packet-tracer

Comment télécharger Packet Tracer

Pour télécharger Packet Tracer, procédez comme suit afin de créer votre inscription à la Networking Academy :

- Cliquez sur le bouton « S'inscrire pour télécharger Packet Tracer »
- Inscrivez-vous au cours Introduction to Packet Tracer
- Complétez votre inscription à la Networking Academy
- Lancer le cours Introduction to Packet Tracer
- Les instructions de téléchargement se trouvent dans le cours

Ensuite, il faut l'installer et l'ouvrir.

Le tutoriel fait, vous êtes capable de prendre un élément et le placer dans l'espace de travail.

N'oubliez pas !!

Comme dans la vie, il faut parfois allumer la machine pour y avoir accès ou modifier sa configuration physique. Le logiciel tient le même principe pour les éléments qui peuvent s'éteindre avec un interrupteur.

Le CLI

C'est la Command Line Interface de l'IOS qui permet de taper les commandes dans un élément.

C'est ici que vous travaillerez le plus car, et vous le verrez avec l'expérience, c'est plus rapide et simple que l'interface web quand elle existe.

Informations pratique à savoir !!

* Si vous voulez connaitre les commandes possibles là où vous êtes (quelque soit le mode, quelque soit la commande commencé), il faut utiliser le **"?"** Il vous donnera toujours les commandes qui peuvent suivre.

* Si vous voulez taper plus vite vos commandes, vous n'êtes pas obligé de terminer la commande complétement, juste les premières lettres suffisent souvent

* Pour compléter ses commandes, au lieu de la taper entièrement, vous pouvez utiliser la touche "Tabulation" pour compléter la commande. Cela permet aussi de vérifier si vous pouvez réaliser ou non une commande. Attention toutefois à être dans le bon menu pour avoir la complétion

Entrer en mode Enable et Configuration Terminal

Pour commencer, il faut entre en mode **Enable**:

`enable` ou en version courte `en`

Ce mode vous permet de faire différentes choses comme des pings ou vérifier les résultats de configurations.

Pour par exemple connaitre les interfaces de votre éléments vous pouvez taper ceci :

```
show ip interface brief
```

et en version courte

```
sh ip int b
```

Cette commande listera les interface et la configuration associé à chaque interface.

.

C'est aussi en mode Enable que l'on peut sauvegarder la configuration qui est en actuellement utilisé en configuration enregistré (il y a une différence entre la configuration enregistré et celle utilisé).

`copy running-configuration startup-configuration` en version courte : `copy run star`

C'est après le mode Enable que l'on peut entre en monde **Configuration Terminal**.

`configuration terminal` ou en version courte **`conf t`**

Ce mode permet de configurer l'ensemble des fonctionnalités de l'élément. Que ce soit les interfaces, VLAN, routage, sécurité ...

Chaque type de configuration peut vous amener dans un sous menu spécifique. La commande pour en sortir est ***`exit`*** *.*

Par exemple, pour attribuer une adresse ip à l'interface g0/0 (interface Gigabit 0/0) il faut taper les commandes suivantes :

`interface g0/0` << nom de l'interface

`ip address 192.168.1.1 255.255.255.0` << mettre l'adresse ip 192.168.1.1 avec le masque 255.255.255.0 (/24)

`no shutdown` << allumer le port

Si vous avez un doute, vous pouvez entre en mode configuration de l'interface puis taper **"?"** , cela listera toutes les possibilités.

Le "do"

Lorsque vous configurez votre éléments, pour éviter de devoir revenir au menu principal ou en mode Enable (faisable avec le CTRL+Z), vous pouvez utiliser le "do" et la commande associé en mode Enable.

Si nous sommes toujours en mode configuration de l'interface et que nous souhaitons vérifier que la commande fonctionne, il faut taper :

`do sh ip int b`

Cela listera les interfaces comme en mode Enable et vous verrez la Gigabit 0/0 configuré avec l'adresse 192.168.1.1 .

Pour plus d'informations ou des compléments, vous pouvez lire cet article :

https://www.commentcamarche.net/faq/17126-routeurs-cisco-parametres-de-base

RanMaxime - V1 2019-10-25