Aide mémoire des commandes de commutateurs et routeurs Cisco

Changer de mode

```
switch> enable□□□□# Commande pour passer du Mode 1 au Mode 2.
switch# conf t□□□□# Commande pour passer du Mode 2 au Mode 3.
switch(config)#             # Nous sommes désormais dans le mode 3
```

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
```

Configurer un port

```
switch(config)# interface fastEthernet 0/1
switch(config-if)# switchport access vlan 50
switch(config-if)# exit
switch(config)#
```

Configurer une plage de port

```
switch(config)# interface range fastEthernet 0/1-24
switch(config-if)# switchport access vlan 30
switch(config-if-range)# exit
switch(config)#
```

Réinitialiser le switch

```
switch# write erase
switch# reload
```

Configurer SSH

- Vérification de la prise en compte du protocole ssh par l'IOS
- Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l'IOS.
- La commande pour vérifier la version de l'IOS est:

```
2960-RG#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 07-Aug-10 23:04 by prod_rel_team
```

- Le protocole ssh peut être activé par défaut. Vérifions avec la commande suivante

  ```
  2960-RG#show ip ssh
  SSH Enabled - version 2.0
  Authentication timeout: 60 secs; Authentication retries: 3
  ```

- Configuration du nom d'hote et du nom de domaine. Le nom du switch ainsi que le nom de domaine doivent avoir été configurés.

- Création de la clé

```
2960-RG(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: 2960-RG.mondomaine.fr
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

2960-RG(config)#
*Mar 1 00:42:43.625: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Activation de ssh

```
 2960-RG(config)#ip ssh version 2
```

- Options ajoutées au service ssh
- - les évènements associés aux connexions ssh sont enregistrés dans les logs.
- - Un timeout de 60 secondes est ajouté en cas d'inactivité durant l'authentification.
- - Nous laissons trois essais pour la connexion au switch. Suite à ces essais, la connexion est fermée.

```
2960-RG(config)#ip ssh logging events
2960-RG(config)#ip ssh time-out 60
2960-RG(config)#ip ssh authentication-retries 3
```

- Configuration de l'authentification et ajout d'un compte administrateur

```
2960-RG(config)#aaa new-model
2960-RG(config)#aaa authentication login default local
2960-RG(config)#aaa authorization exec default local
2960-RG(config)#username admin secret P@55w0rd
```

- Désactivation de telnet pour l'accès au switch

```
2960-RG(config)#line vty 0 15
2960-RG(config-line)#login local
2960-RG(config-line)#transport input ssh
```

- Vérification de la configuration

```
2960-RG#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
```

SSH est maintenant activé. nous pouvons accéder au switch avec un client ssh (par exemple putty pour windows).

Activation du routage statique

```
switch(config)#sdm prefer landbase-routing
switch(config-if)#switch#write
switch#reload
```

Configurer le routage statique

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
```

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 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
```

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
```

Relai DHCP

```
switch(config)# interface vlan 100
switch(config-if)# ip helper-address 172.31.64.10
switch(config-if)# ip helper-address 172.31.64.30
```

Configurer un DHCP sur un routeur Cisco

Se connecter et passe en mode config terminal
ROUTER > enable
ROUTER # conf t

```
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
```

Affichage du routage

```
switch#show ip route
```

Activer le trunk

```
SW_POD4_BOT#configure terminal
SW_POD4_BOT(config)#interface gigabitEthernet 0/2
SW_POD4_BOT(config-if)#switchport mode trunk
W_POD4_BOT(config-if)#switchport trunk allowed vlan none
SW_POD4_BOT(config-if)#switchport trunk allowed vlan add 400
SW_POD4_BOT(config-if)#switchport trunk allowed vlan add 300
SW_POD4_BOT(config-if)#switchport trunk allowed vlan add 200
SW_POD4_BOT(config-if)#switchport trunk allowed vlan add 100
```

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

QoS en fonction d'une interface source

Déclaration de classes de flux :

```
MonRouteur#configure terminal
MonRouteur(config)#class-map match-all prio-sur-interface
MonRouteur(config-cmap)#match input-interface fa1/0
MonRouteur(config-cmap)#exit
MonRouteur(config)#
```

Déclaration d'une politique de QoS :

```
MonRouteur (config)#policy-map ma-politique-qos
MonRouteur (config-pmap)#class prio-sur-interface
MonRouteur (config-pmap-c)#set ip dscp cs7
MonRouteur (config-pmap-c)#exit
MonRouteur (config-pmap)#exit
MonRouteur (config)#
```

Application de la politique de QoS sur une interface :

```
MonRouteur(config)#interface fa0/1
MonRouteur(config-if)#service-policy output ma-politique-qos
MonRouteur(config-if)#exit
MonRouteur(config)#exit
```

QoS en fonction du protocole

Déclaration d'une nouvelle classe de flux :

```
MonRouteur (config)#class-map match-all prio-sur-ftp
MonRouteur (config-cmap)#match protocol ftp
MonRouteur (config-cmap)#exit
MonRouteur (config)#
```

Élargissement de la politique de QoS :

```
MonRouteur (config)#policy-map ma-politique-qos
MonRouteur (config-pmap)#class prio-sur-ftp
MonRouteur(config-pmap-c)#bandwidth percent 10       // On réserve 10% de la bande passante
pour ce flux
MonRouteur (config-pmap-c)#set ip dscp cs1
MonRouteur (config-pmap-c)#exit
MonRouteur (config-pmap)#exit
MonRouteur (config)#
```

Routage sur un routeur

```
# VLAN SORTIE
switch(config)# Interface GigabitEthernet 0/1.400
switch(config-if)# encapsulation dot1q 400
switch(config-if)# ip address 172.31.192.1 255.255.192.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#

# VLAN SERVEURS
switch(config)# Interface GigabitEthernet 0/1.300
```

```
switch(config-if)# encapsulation dot1q 300
switch(config-if)# ip address 172.31.64.1 255.255.192.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#

# VLAN SUPERVISION
switch(config)# Interface GigabitEthernet 0/1.200
switch(config-if)# encapsulation dot1q 200
switch(config-if)# ip address 172.31.128.1 255.255.192.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#

# VLAN SERVICES UTILISATEURS
switch(config)# Interface GigabitEthernet 0/1.100
switch(config-if)# encapsulation dot1q 100
switch(config-if)# ip address 172.31.0.1 255.255.192.0
switch(config-if)# no shutdown
switch(config-if)# ip helper-address 172.31.64.10
switch(config-if)# ip helper-address 172.31.64.30
switch(config-if)# exit
switch(config)#

# Route par défaut

interface GigabitEthernet 0/1
switch(config)#ip route 0.0.0.0 0.0.0.0 172.31.192.2
switch(config)#no shutdown
```

Routage groupé (redondance de routeurs)

J'ai deux routeurs :
RT 1 - 192.168.0.1
RT 2 - 192.168.0.2

Et nous allons créé une interface virtuelle qui permettra la redondance :

SW 1 :

```
// Activation de RIP
SW-1(config)#router rip
SW-1(config-router)#version 2

// Définition de tous les réseaux auquel le routeur est connectés
SW-1(config-router)#network 192.168.0.0
SW-1(config-router)#network 172.16.0.0

// Maximum de Sauts autorisés (n)
SW-1(config-router)default-metric n

// Réglage des conteurs de retenue
// timers basic update invalid holddown flush
// update = envoie en seconde des mises à jours de routage ;
// invalid = temps pour être invalide ;
// holddown = l'intervalle pendant lequel les informations de routage sur les meilleurs chemins sont supprimées ;
// flush = le délai écoulé avant que la route ne soit retirée de la table de routage.
//
//
SW-1(config-router)#timers basic 30 180 180 260

// Propagation de la route par défaut
SW-1(config-router)#default-information originate

// Désactivation de l'auto agrégation
SW-1(config-router)#no auto-summary

// Luter contre les boucles réseau
SW-1(config-router)#ip split-horizon

// Route par défaut
SW-1(config-router)#ip default-network W.X.Y.Z



// Mise en oeuvre du HSRP
// Où 1 est le numéro du groupe HSRP et l'ip est l'adresse réseau virtuelle du groupe
SW-1(config-router)#standby 1 ip 192.168.0.254
```

SW 2 :

```
// Activation de RIP
SW-2(config)#router rip
SW-2(config-router)#version 2

// Définition de tous les réseaux auquel le routeur est connectés
SW-2(config-router)#network 192.168.0.0
SW-2(config-router)#network 172.16.0.0

// Maximum de Sauts autorisés (n)
SW-2(config-router)default-metric n

// Réglage des conteurs de retenue
// timers basic update invalid holddown flush
// update = envoie en seconde des mises à jours de routage ;
// invalid = temps pour être invalide ;
// holddown = l'intervalle pendant lequel les informations de routage sur les meilleurs
chemins sont supprimées ;
// flush = le délai écoulé avant que la route ne soit retirée de la table de routage.
//
//
SW-2(config-router)#timers basic 30 180 180 260

// Propagation de la route par défaut
SW-2(config-router)#default-information originate

// Désactivation de l'auto agrégation
SW-2(config-router)#no auto-summary

// Luter contre les boucles réseau
SW-2(config-router)#ip split-horizon

// Route par défaut
SW-2(config-router)#ip default-network W.X.Y.Z



// Mise en oeuvre du HSRP
```

```
// Où 1 est le numéro du groupe HSRP et l'ip est l'adresse réseau virtuelle du groupe
SW-2(config-router)#standby 1 ip 192.168.0.254
SW-2(config-router)#standby 1 priority 120
SW-2(config-router)#standby 1 preempt
```

La tolérance de panne a bien été installée !

NTP Maitre

```
SW-2(config-router)#ntp master 1
```

NTP Esclaves

```
SW-2(config-router)#ntp server 192.168.1.1
```

NAT

```
// Création d'une ACL
routeur1(config)#ip access-list standard NAT_INTERNET_VLAN2
routeur1(config-std-nacl)#permit 192.168.2.0 0.0.0.255
routeur1(config-std-nacl)#exit

// NAT Sortant
routeur1(config)#int gi0/1
routeur1(config-if)#ip nat outside
routeur1(config-if)#exit

// NAT Entrant
routeur1(config)#int gigabitEthernet 0/0.2
routeur1(config-subif)#ip nat inside
routeur1(config-if)#exit

// Affectation
routeur1(config)#ip nat inside source list NAT_INTERNET_VLAN2 interface GigabitEthernet0/1
overload

// Porte de sortie
routeur1(config)#ip nat inside source static 192.168.2.1 223.0.0.1
```

```
// Redirection de port
routeur1(config)#ip nat inside source static tcp 192.168.2.1 80 223.0.0.1 80
```

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
```

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
```

Changer la vitesse des interfaces

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

Revision #15
Created 24 November 2024 17:34:32 by Nicolas
Updated 4 February 2025 23:20:55 by Nicolas