Fiche ROUTEUR
Commandes CISCO

Mise à jour 27 février 2025

Pour info

Il est souhaitable de désactiver la recherche DNS lors de la configuration d'un routeur avec la commande :

routeur(config)#**no ip domain-lookup** pour un ROUTEUR

1 – Besoin d'aide

Router> **?** Router# **?** Router(config)#**conf t ?**	Affiche l'ensembles des commandes pour le mode sélectionné.
Router# **show ?**	En fonction du mode (>, #, config), affiche les paramètres possibles pour la commande sélectionnée. Dans notre cas, tous les paramètres associés à la commande show.

2 – Faites le SHOW

Router#**show running-config**	Affiche la configuration actuelle du routeur
Router#**show startup-config**	Affiche la configuration utilisée lors du démarrage du routeur
Router#**show ip interface brief**	Affiche l'état des interfaces
Router#**show ip interface g0/1**	Affiche l'état de l'interface G0/1
Router#**show interfaces trunk**	Affiche toutes les interfaces qui sont actuellement configurées pour fonctionner en mode trunk.
Router#**show clock**	Affiche la date et l'heure
Router#**show vlan**	Affiche la liste des VLAN. On peut aussi utiliser "**show vlan brief**".
Router#**show access-lists**	Affiche les ACL
Router#**show interfaces status**	Résume les informations pour l'ensemble des ports
Router# **show ip route**	Affiche la table de routage
Router# **show ip protocols**	Affiche les protocoles utilisés
Router# **show ip eigrp neighbors**	Affiche la table de voisinage pour le protocole EIGRP
Router# **show cdp neighbors**	Affiche les informations de voisinage CDP
Router# **show ip dhcp binding**	Permet de vérifier la table des liaisons DHCP (association adresse IP --> Adresse MAC).
Router#**show mac-address-table**	Affichage de la table d'adresses MAC

3 - Sauvegarder la configuration du routeur

Pour infos

Lors du démarrage du routeur, la configuration "Startup-config" est copiée en mémoire RAM et devient "Running-config". Toutes les modifications effectuées par la suite, seront sauvegardées dans le fichier "running-config".
Pour que les modifications soient prises en compte lors du prochain démarrage du routeur, il faut que le contenu du ficher "running-config" soit copié dans le "statup-config".
Le fichier "startup-config" est sauvegardé dans la NVRAM (Non Volatile RAM = EPROM).
A l'arrêt du routeur, la mémoire RAM est effacé et le contenu du fichier "running-config" est perdu.

Router#**Copy running-config startup-config**	Copie la configuration actuelle vers la configuration de démarrage
Router#**Copy startup-config running-config**	Copie la configuration de démarrage vers la configuration actuelle.
Router# **write erase**	Supprime la configuration de démarrage et redémarre le routeur.
Router# **erase startup-config** Router# **del vlan.dat**	Supprime la configuration de démarrage et les VLAN
Router# **reload**	Redémarre le routeur

4 - Renommer le routeur

Router(config)#**hostname** *nouveauNomDuSwitch* Router(config)#**ip domain-name** *monDomaine.local*	Permet de nommer le routeur. Permet de définir un nom de domaine local pour le routeur.
Router(config)#**no hostname** *nouveauNomDuSwitch* Router(config)#**no ip domain-name** *monDomaine.local*	Permet de supprimer le nom ou le nom de domaine.

5 - Configuration d'une interface

Router(config)#**interface *G0/0*** Router(config-if)#**description** *votre_description* Router(config-if)#**ip address 192.168.1.1 255.255.255.0** Router(config-if)#**no shutdown**	Sélectionne l'interface G0/0 pour modification. Description du rôle de l'interface (pas obligatoire). Affecte l'adresse IP et le masque à l'interface. Activation de l'interface
Router(config)#**interface *nom_interface*** Router(config-if)#**shutdown**	Désactivation de l'interface.

6 - Configuration d'une sous-interface

R1(config)#**interface G0/0.10** R1(config-subif)# **description** *votre_description* R1(config-subif)#**encapsulation dot1Q** 10 R1(config-subif)#**ip add 192.168.10.1 255.255.255.0** R1(config-subif)#exit	Sélectionne la sous-interface G0/0.10 pour modification. Description du rôle de l'interface (pas obligatoire). Protocole utilisé **dot1Q** pour le VLAN numéro **10** Affecte l'adresse IP et le masque de la sous-interface. Pensez à activer l'interface principale G0/0
Répétez le processus pour chaque VLAN à router. Une adresse IP sur un sous-réseau unique doit être affectée à chaque sous-interface de routeur pour que le routage se produise.	

7 - Gestion des mots de passe / Bannière

Router(config)#**line con 0** Router(config-line)#**password** VotreMotDePasse Router(config-line)#**login** Router(config-line)#**exit**	Création d'un mot de passe pour la connexion console. "Login" permet d'activer l'interface de console.
Router(config)#**line vty 0 4** Router(config-line)#**password** VotreMotDePasse Router(config-line)#**login** Router(config-line)#**end**	Création d'un mot de passe pour la connexion lignes virtuelle (de 0 à 15). "Login" permet d'activer la ligne.
Router(config)#**enable password** VotreMotDePasse	Mot de passe pour le mode privilège
Router(config)#**enable secret** VotreMotDePasse	Mot de passe pour le mode privilège (crypté)
Router(config)#**service password-encryption**	Activation du service *password-encryption (permet de chiffrer les mots de passe)*
Router(config)# **banner motd $** votre commentaire ici entre les deux caractères spéciaux **$**	Permet de configurer la bannière du switch

Router(config)# **ip http server** Router(config)# **ip http secure-server**	Activation du protocole http (1ère ligne) ou HTTPS (2éme ligne)
Router(config)#**ip domain-name** votreNomDeDomaine Router(config)#**crypto key generate rsa** On demande le nombre de bits. Répondre : 512 par exemple	Activation du module SSH (accès par les lignes VTY)
Router(config)# **ip authentification local** Router(config)#**username** admin ***privilege*** *15* **secret** MotDePasse	Definition d'un utilisateur local Nom de l'administrateur : admin Niveau de sécurité : 15 (c'est le plus élevé)
Router(config)#**ip ssh version** 1 Router(config)#**line** vty 0 4 Router(config-line)#**transport input ssh** Router(config-line)#**login local** Router(config)#**ip ssh time-out** 75 Router(config)#**ip ssh authentication-retries** 3	Activation SSH (version en fonction du routeur) Délai d'inactivité en seconde avant déconnexion. Nombre max de tentatives : 3

REMARQUES :
- Par défaut, les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Il faut activer le service *encryption-password pour chiffrer les mots de passe.*
- La connexion au routeur s'effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles (appelées VTY).
- On peut créer un mot de passe pour l'accès aux différents terminaux (console et virtuel) et un mot de passe pour l'accès au mode privilégié (enable).
- Suivant le modèle du routeur, le nombre de bits de la clé RSA et compris entre 360 et 2048, et la version ssh entre 1 et 2.

8 - Configuration adresses IP – MAC – Table ARP

Router# **show mac-address-table**	Affichage de la table des adresses MAC et des interfaces du routeur
Router(config)# **mac-address-table static** @MAC vlan 1 **interface** fastethernet0/1	Ajout d'une adresse MAC dans la table

9 - Routes statiques

Méthode 1 Router(config)#**ip route** 192.168.1.0 255.255.255.0 G0/0	Le réseau de destination 192.168.1.0 avec le masque 255.255.255.0 est accessible à partir de l'interface G0/0 (méthode 1) ou en passant par la passerelle 192.168.2.254 (méthode 2)
Méthode2 Router(config)#**ip route** 192.168.1.0 255.255.255.0 192.168.2.254	
Méthode 1 Router(config)#**ip route** 0.0.0.0 0.0.0.0 G0/0	Le réseau de destination 0.0.0.0 (toutes les autres routes non définies dans la table de routage) avec le masque 0.0.0.0 (tous types de masque) est accessible à partir de l'interface G0/0 (méthode 1) ou en passant par la passerelle 192.168.2.254 (méthode 2)
Méthode 2 Router(config)#**ip route** 0.0.0.0 0.0.0.0 192.168.2.254	
Router(config)# **no ip route** 192.168.1.0 255.255.255.0 G0/0	Supprime la route 192.168.1.0

Remarque :
La méthode 2 est plus efficace car on connait l'adresse IP de la passerelle, pour la méthode 1, le routeur devra déterminer la passerelle (perte de temps) sauf s'il n'y a que deux interfaces sur le tronçon.

10 – Routes dynamiques (RIP)

Router(config)#router rip	Active le mode de configuration RIP.
Router(config-router)#network 192.192.0.0	Active le protocole RIP sur le réseau 192.168.0.0
Router(config-router)#version 2	Active la version du protocole RIP. La version 2 étant la plus récente, elle n'est pas disponible sur les anciens modèle de routeur (Se renseigner au préalable).
Router(config-router)#no auto-summary	Désactive la fonction auto-résumé (vivement conseillé). Le RIP version 1, par défaut, effectue un "auto-résumé" des routes annoncées en utilisant le masque de sous-réseau de classe A, B ou C. Par exemple, si vous avez un réseau avec des **sous-réseaux de longueurs différentes**, l'auto-résumé agrégera les routes en fonction du masque de sous-réseau par défaut (A, B ou C), ce qui pourrait entraîner des informations de routage incorrectes ou non optimales.
Router(onfig-router)#passive-interface G0/0	Permet d'exclure une interface (donc un sous-réseau) des messages transmis aux autres routeurs.

11 – Routes dynamique (OSPF)

Router(config)#router ospf 1	Active le mode de configuration OSPF. Le 1 (process-id) et un nombre entre 1 et 65535. Il identifie le processus OSPF sur le routeur. On peut exécuter plusieurs processus (un par zone par exemple) sur un même routeur
Router(config-router)#network 192.168.0.0 0.0.0.255 area 0	Active le protocole OSPF sur le réseau 192.168.0.0. Il faut aussi préciser le complément du masque de sous réseau (0.0.0.255 pour un masque 255.2555.255.0) et préciser une zone. Tous les

	routeurs se situant dans la même zone peuvent recevoir les informations des autres routeurs.

12 – Routes dynamiques (EIGRP)

R1(config)#router eigrp 1	Active le mode de configuration EIGRP. Le 1 (process-id) et un nombre entre 1 et 65535. Il identifie le processus OSPF sur le routeur. On peut exécuter plusieurs processus (un par zone par exemple) sur un même routeur
R1(config-router)#network 192.168.1.0	On précise sur quel réseau on active le protocole EIGRP
R1(config-router)#passive-interface G0/1	On précise les interfaces passives qui ne doivent pas envoyer d'informations.
R1(config-router)#metric weights tos_k1 tos_k2 tos_k3 tos_k4 tos_k4	(Facultatif) On peut préciser les valeurs spécifiques pour les métriques (1 pour valider). (tos : Type Of Trafic) **tos_k1**: Valeur par défaut : 1. (bande passante et retard.) **tos_k2**: Valeur par défaut : 0. (bande passante et délai.) **tos_k3**: Valeur par défaut : 1. (fiabilité et délai.) **tos_k4**: Valeur par défaut : 0. (fiabilité et coût.) **tos_k5**: Valeur par défaut : 0. (coût.)

13 – Service DHCP

R1(config)#**ip dhcp pool R1-LAN** R1(dhcp-config)#**network 192.168.1.0 255.255.255.0**	Création d'un pool (un ensemble d'adresses IP) qui porte le nom "R1-LAN". Le pool créé sera associé à ce réseau 192.168.1.0
R1(dhcp-config)#**default-router 192.168.1.1**	On précise l'adresse de la passerelle associée à un pool DHCP.
R1(dhcp-config)#**dns-server 192.168.1.254**	On précise l'adresse du DNS associée à un pool DHCP.
R1(config)# **ip dhcp excluded-address 192.168.1.1 192.168.1.50**	On précise au DHCP une plage d'adresse à exclure de l'adressage automatique. Adresses généralement réservées pour des imprimantes, caméras IP, …
R1(config)#interface g0/3 R1(config-if)#ip helper-address 10.0.0.5	Relais DHCP : si le service ce situe sur un autre routeur alors on lui indique son adresse, 10.0.05 dans notre cas.
R1(config)#interface G0/2 R1(config-if)#ip address dhcp R1(config-if)#no shutdown	L'interface G0/2 demandera une adresse IP au serveur DHCP se trouvant sur le même réseau. Il ne faut pas oublier d'activer l'interface.

14 – Service NAT

Router(config)#**access-list** 1 **permit** 192.168.10.0 0.0.0.255	Création d'une liste avec le réseau interne concerné par le service NAT. On peut ajouter plusieurs réseaux internes sur la même liste.
Router(config)#Ip nat inside source list 1 interface GigabitEthernet0/0 overload	Association de la liste 1 (réseaux internes) à l'interface externe G0/0
R1(config)#interface GigabitEthernet0/1 R1(config-if)#ip nat inside R1(config-if)#exit	Permet de préciser que l'interface G0/1 appartient au réseau interne pour le service NAT
R1(config)#interface GigabitEthernet0/1.10 R1(config-subif)#ip nat inside	Permet de préciser que la sous interface G0/1.10 appartient au réseau interne pour le service NAT
R1(config)#interface GigabitEthernet0/0 R1(config-subif)#ip nat outside R1(config-subif)#exit	Permet de préciser que l'interface G0/0 appartient au réseau externe pour le service NAT

15 – Listes ACL

Numéro (seulement en IPv4) : Numéro de la liste ACL (1-99 et 1300-1999 pour une ACL standard, 100-199 et 2000-2699 pour une ACL étendue).
permit ou **deny** : Spécifie si le trafic correspondant doit être autorisé ou bloqué.
protocole : (au choix) icmp, ip, tcp, udp, eigrp, ospf, … ou un nombre représentant le protocole utilisé (exemple : 80 pour http)
@IP source : Adresse IP source du trafic.
wildcard : Masque générique pour l'adresse IP source (0.0.0.0 signifie qu'aucun bit ne doit correspondre).
opérateur : lt (less than - moins que), gt (greater than - plus que), eq (equal - égal à), neq (not equal - non équivalent), range (inclusive range - étendue d'une plage).
port : valeur nominative ou numéraire : de 0 à 65535 ou, par exemple, www, telnet, ftp, etc.
@IP_destination : Adresse IP destination du trafic.
log (optionnel) : Permet de consigner les correspondances.

Router(config)#**access-list** *numéro* {**deny**|**permit**} *@IP_source wildcard* [**log**]	ACL Standard (uniquement en IPv4)
Router(config)#**access-list** *numéro* {**deny ou permit**} *protocole @IP_source wildcard [opérateur port] @IP_destination wildcard [opérateur port]* [**log**]	ACL Etendue (IPv4 et IPv6)
R1(config)#ip access-list extended DENY_PC1 R1(config-ext-nacl)#deny host 192.168.5.2 R1(config-ext-nacl)#exit R1(config)#int G0/0 R1(config-if)#ip access-group DENY_PC1 out	Création d'une ACL nommée "DENY_PC1" qui bloque l'adresse 192.168.5.2. L'ACL est ajouté à l'interface G0/0 en sortie.
R1(config)#no ip access-list extended R1_G00	Supprime la liste R1_G00 du routeur
R1(config)#no access-list 1	Supprime toutes les règles associées à la liste 1 du routeur.
R1(config)#ip access-list extended R1_ACL R1(config-ext-nacl)# 65 deny tcp host 192.168.1.10 host 35.0.05.1 eq 21	Permet d'ajouter une règle à la ligne 65 d'une ACL existante nommée R1_ACL.

16 – Pare-feu ZPF

Bien comprendre les étapes de la configuration d'un pare-feu à politique basée sur les zones

Etape 1 (zone security …) :
Il faut nommer les zones que l'on veut contrôler : Zone intérieure, extérieure, zone 1, 2 ou 3, …

Etape 2 (access-list 101 permit ip …) :
On définit les règles sans les associées à une interface ou à une zone : ACL 1, ACL 2, …

Etape 3 (class-map type … / match access-group …) :
Création d'une classe (mappage de classe) : On va ajouter à la classe les règles que l'on souhaite utiliser.

Etape 4 (policy-map type … / class type inspect …) :
Il faut définir la politique de sécurité entre deux zones en sélectionnant un mappage de classe (étape 3) et en précisant l'action à faire (inspect, drop, …) lorsque on aura des "match".

Etape 5 (zone-pair security …) :
Définir la paire de zone que l'on veut contrôler et préciser le sens de la communication (source / destinataire) : par exemple zone intérieure (source) et zone 2 (destinataire) forment une paire de zone.

Etape 6 (interface …/ zone-member security …) :
Associer les interfaces (G0/0, S0/1/0, …) avec les zones définies à l'étape 1.

Etape 7 (show policy-map …) :
Tester la ZPF.

R1(config)#zone security **NomDeLaZone**	Création d'une zone nommée **NomDeLaZone**
R3(config)#class-map type inspect match-all **NomClassMap** R3(config-cmap)#match access-group **NumeroACL** R3(config-cmap)#exit	Création d'une classe de mappage nommée **NomClassMap** Association de la classe et de l'ACL (**NuméroACL**) Retour au mode config
R3(config)#policy-map type inspect **NomDeLaPolitique** R3(config-pmap)#class type inspect **NomClassMap** R3(config-pmap-c)#inspect	Permet de définir le nom de la politique de sécurité On précise le nom du mappage de classe à associer à la politique de sécurité Action à faire (inspect | drop | pass)
R3(config)#zone-pair security **NomPaire Zones** source **NomZone1** destination **NomZone2** R3(config-sec-zone-pair)#service-policy type inspect **NomDeLaPolitique** R3(config-sec-zone-pair)# exit	Création d'une paire de zones nommée **NomPaire Zones** en précisant le nom de la zone source **NomZone1** et celui de la zone de destination **NomZone2**. On précise le nom de la politique de sécurité associé à cette paire de zones
R3(config)#interface g0/0 R3(config-if)#zone-member security **NomDeLaZone** R3(config-if)#exit	Connexion à l'interface Association de la zone (**NomDeLaZone**) à l'interface G0/0 du routeur.

17 - Configuration de l'heure et de la date

Router#**clock set** 13:10:00 9 november 2016	Configuration de l'heure et de la date
Router#**show clock**	Affiche la date et l'heure

18 - Divers (non actif sous Packet tracer)

Router#**reload in** 5	Redémarrage du routeur dans 5 minutes
Router#**reload at** 16:00	Redémarrage à une heure précise
Router#**reload cancel**	Annule le redémarrage.