Synthèse
Commandes Cisco

Premier Bloc
Sécurité des systèmes
Année académique 2019-2020

Rédigé par Sénéchal Julien

22 Mars 2020

ATTENTION - LORSQUE VOUS VOYEZ "[]", CELA SIGNIFIE QUE VOUS DEVEZ MODIFIER CETTE VALEUR EN FONCTION DE CE QUI Y EST NOTÉ

1 Les Routeurs

1.1 Commandes de bases

- Se mettre en mode *EXEC* : *enable*
- Configurer le terminal : *configure terminal*
- Changer le nom de notre routeur : *hostname [nom]*
- Sortir de n'importe quel mode/environnement (ex : EXEC, Configure terminal, interfaces,...) : *exit*
- Vérifier tous les ports du routeur : *show ip interface brief*
- Pour connaître les protocoles utilisés (ex : *rip*) : *show ip protocols*

1.2 Effacer la configuration d'un routeur

Vous devez être en mode *EXEC* pour cela :
- *erase startup-config*
- *reload*

1.3 Commandes interfaces

- Configurer une interface : *interface [nom_interface]*
- Changer l'adresse IP : *ip address [IP] [NetMask]*
- Décrire une interface : *description [La description]*
- Garder l'interface active (obligatoire pour utiliser une interface) : *no shutdown*
- Vitesse de la clock (uniquement sur le DCE) : *clock rate [vitesse]*

1.4 Créer des routes

- Route récursive (On choisit la cible en fonction de son IP) :
  ip route [IP de destination des paquets] [NetMask du réseaux destinataire] [IP routeur]
- Route directement connectée (On envoie les paquets directement dans un *Serial*) :
  ip route [IP de destination des paquets] [NetMask du réseaux destinataire] [serial connecté au routeur]

1.5 Logging Synchronous

On peut recevoir des messages du routeur qui trouble l'entrée des commandes. Pour éviter ça, on peut demander un *Logging Synchronous*.
Pour ce faire, une fois dans *Router(config#)* :
- *Line console 0*
- *logging synchronous*
- *exit*

1.6 Sécurité

- Pour mettre un mode de passe au *EXEC MODE* : *enable secret [mdp]*
- Pour encrypter les mots de passe dans le fichier de configuration : *service password-encryption*
- Pour choisir le nombre de caractère minimum pour tous les mots de passe du routeur :
  security passwords min-length [nb de caractère]
- Pour empêcher les attaques par force brute, nous pouvons mettre un cooldown entre chaque erreur : *login block-for [secondes] attempts [nombre de tentatives] within [secondes].*
  Le premier champ sert a indiquer le nombre de seconde de cooldown entre chaque tentative. Le dernier champ sert à indiquer le nombre de secondes que l'utilisateur peut prendre pour renseigner son mot de passe.

— Pour pouvoir permettre de se déconnecter du routeur automatiquement après un temps d'inactivitée :
line console 0
exec-timeout [minutes] [secondes]
live vty 0 4
exec-timeout [minutes] [secondes]
exit

1.7 Etablir une connection SSH

Il faut assigner le nom de domaine :
ip domain-name [nom de domaine]
Puis, il faut créer un utilisateur pour le SSH. Si le privilège de l'utilisateur n'est pas spécifié dans la commande, celui-ci aura automatiquement les privilèges *EXEC* (niveau 15).
username [nom] privilege [level] secret [MotDePasse]
Maintenant, nous allons configurer notre "VTY line" afin d'accepter le SSH.
line vty 0 4
Ici le "0 4" va permettre l'ouverture de 5 sessions maximum. (Ne me demandez pas pourquoi, c'est juste le fruit de mes recherches.) Maintenant il faut renseigner par quel moyen on veut se connecter
transport input ssh
login local
exit
crypto key generate rsa
Après cela, on nous demande de rentrer le nombre de bits pour le modulus, entrez *"1024"*

1.8 Configuration RIP

Rentrez en mode EXEC, puis en mode configuration du terminal.
Entrez *routeur rip* pour commencer la configuration du protocole RIP.
Faites bien attention a marquer *version 2* par après, sans quoi votre protocole ne prendra pas en compte les NetMasks !

— Définir les interfaces concernées par le RIP : *network [IP]*
— Définir les interfaces n'étant pas connectée à un routeur (par Sécurité) : *passive-interface [interface (ex : g0/0)]*
— Désactiver le résumé de routes : *no auto-summary*

ATTENTION : Le réseaux "Internet" ne participe pas au routage RIP ! Pour *Internet*, nous utiliserons une route statique !
Ensuite, afin de pouvoir propager notre route vers *Internet* sur tout le RIP, nous allons devoir configurer cela :
— *routeur rip* (pour ce remettre en configuration RIP)
— *default-information originate* (Seulement sur le routeur qui nous a servi a configurer notre route !)
Pour vérifier que tout est opérationnel : *show ip route* ou *show ip route rip*
Au cas où vous constatez un problèmes avec vos routes, et voulez recommencer, la commande *clear ip route ** va supprimer toutes les routes présentes sur **le** routeur sur lequel vous avez lancer la commande !

1.9 IPV6

— Pour activer l'IPV6 sur le routeur : *ipv6 unicast-routing*
— Définir l'adresse : *ipv6 address [adresse + CIDR] eui-64*
(le protocole *eui-64* va permettre en quelque sorte de remplacer un DHCP en permettant automatiquement de transmettre aux machines sur le réseau l'adresse du réseau et va ainsi permettre aux machines de créer leurs adresses IPV6 sur base de leur adresse MAC pour qu'il n'y aie pas de répétition. L'adresse obtenue sur les PC se nomme le *SLAAC*. Donc, utile uniquement sur les interfaces LAN.)
— On n'oublie pas le *no shutdown*

1.9.1 Routage statique en IPV6

— Routes directement connectée : *ipv6 route [adresse + CIDR] [interface]*
— Routes récursives : *ipv6 route [adresse + CIDR] [adresse routeur]*

- Routes par défaut : *ipv6 route ::/0 [interface]*
  Le *"::/0"* signifie la même chose que le 0.0.0.0 0.0.0.0 en IPV4
- Pour supprimer une route :
  no ipv6 route [adresse + CIDR] [adresse routeur/interface (selon si récursive ou directement connectée)]

1.9.2 RIPng

- Pour activer le RIPng sur votre routeur, faites *ipv6 rip [nom-de-domaine] enable* dans la configuration de vos interfaces. Le "nom de domaine" peut être ce que vous voulez si non précisé dans les consignes du moment du vous utilisiez le même sur vos autres routeurs faisant partie de votre RIPng. Ne pas mettre cette commande sur les interfaces LAN pour des raisons de sécurité.
- Une fois le RIPng activé sur toutes les interfaces non-LAN de vos routeurs, afin que les interfaces LAN puissent s'en servir, entrez la commande *ipv6 router rip [nom-de-domaine]* dans la configuration du terminal, puis faites *redistribute connected.*
- De la même manière que sur le RIPv2, la commande *ipv6 rip [nom-de-domaine] default-information originate* vous permettra de définir une route par défaut envoyant par exemple sur *internet.* Uniquement à mettre sur l'interface du routeur vers lequel doivent sortir les paquets de cette route par défaut.
- Pour voir les routes créés a partir de votre rip et vos routes statiques, faites *show ipv6 route*

2 Les Switchs

2.1 Les commandes de bases

- Se mettre en mode *EXEC* : *enable*
- Sortir de n'importe quel mode/environnement (ex : EXEC, Configure terminal, interfaces,...) : *exit*
- Vérifier tous les ports du switch : *show ip interface brief*
- Pour éteindre plusieurs interfaces en même temps :
  interface range [range1] , [range2] , [range3]
  shutdown
  Exemple : *interface range FastEthernet0/1–4 , GigabitEthernet0/1-2*

2.2 Supprimer la configuration d'un Switch

Vous devez être en mode *EXEC* pour cela :

- *delete flash:vlan.dat*
- *erase startup-config*
- *reload*

2.3 Etablir une connection SSH

Il faut assigner le nom de domaine :
ip domain-name [nom de domaine]
Puis, il faut créer un utilisateur pour le SSH. Si le privilège de l'utilisateur n'est pas spécifié dans la commande, celui-ci aura automatiquement les privilèges *EXEC* (niveau 15).
username [nom] privilege [level] secret [MotDePasse]
Maintenant, nous allons configurer notre "VTY line" afin d'accepter le SSH.
line vty 0 15
Ici le "0 15" va permettre l'ouverture de 16 sessions maximum. Maintenant il faut renseigner par quel moyen on veut se connecter
transport input ssh
login local
exit
crypto key generate rsa
Après cela, on nous demande de rentrer le nombre de bits pour le modulus, entrez *"1024"*

2.4 Sécurité

- Pour pouvoir permettre de se déconnecter du routeur automatiquement après un temps d'inactivitée :
  line console 0
  exec-timeout [minutes] [secondes]
  live vty 0 15
  exec-timeout [minutes] [secondes]
  exit
- Pour empêcher les attaques par force brute, nous pouvons mettre un cooldown entre chaque erreur : *login block-for [secondes] attempts [nombre de tentatives] within [secondes].*
  Le premier champ sert a indiquer le nombre de seconde de cooldown entre chaque tentative. Le dernier champ sert à indiquer le nombre de secondes que l'utilisateur peut prendre pour renseigner son mot de passe.