Travaux pratiques - Accès aux périphériques réseau avec SSH

Topologie

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

Partie 1 : Configurer les paramètres de base des périphériques

Partie 2 : Configurer le routeur pour l'accès SSH

Partie 3 : Configurer le commutateur pour l'accès SSH

Partie 4 : SSH à partir de l'interface en ligne de commande du commutateur

Contexte/scénario

Autrefois, Telnet était le protocole réseau le plus utilisé pour configurer à distance des périphériques réseau. Telnet ne chiffre pas les informations entre le client et le serveur. Cela permet à un analyseur de réseau d'intercepter les mots de passe et les données de configuration.

Secure Shell (SSH) est un protocole réseau qui établit une connexion d'émulation de terminal sécurisée avec un routeur ou un autre périphérique réseau. SSH chiffre toutes les informations qui transitent via la liaison réseau et assure l'authentification de l'ordinateur distant. Il est en train de remplacer rapidement Telnet en tant qu'outil de connexion à distance de prédilection des professionnels réseau. Ce protocole est très souvent utilisé pour se connecter à une machine distante et exécuter des commandes ; cependant, il peut également transférer des fichiers à l'aide de ses protocoles associés SFTP (Secure FTP) ou SCP (Secure Copy).

Les périphériques réseau qui communiquent entre eux doivent être configurés de manière à prendre en charge SSH. Au cours de ces travaux pratiques, vous allez activer le serveur SSH sur un routeur et vous vous connecterez à ce routeur à l'aide d'un PC sur lequel le client SSH est installé. Sur un réseau local, la connexion est normalement établie en utilisant Ethernet et IP.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif des interfaces de routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. En cas de doute, contactez votre formateur.

Ressources requises

- 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 1 ordinateur (Windows 7 ou 8, équipé d'un programme d'émulation de terminal, tel que Tera Term, et de Wireshark)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Partie 1: Configurer les paramètres de base des périphériques

Dans la première partie, vous allez configurer la topologie du réseau et configurer les paramètres de base, tels que les adresses IP des interfaces, l'accès des périphériques et les mots de passe sur le routeur.

Étape 1: Câblez le réseau conformément à la topologie.

Étape 2: Initialisez et redémarrez le routeur et le commutateur.

Étape 3: Configurez le routeur.

a. Accédez au routeur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

d. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

e. Attribuez **cisco** comme mot de passe de console et activez la connexion.

f. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

g. Chiffrez les mots de passe en clair.

h. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

i. Configurez et activez l'interface G0/1 sur le routeur à l'aide des informations contenues dans la table d'adressage.

j. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 4: Configurez PC-A.

a. Configurez PC-A avec une adresse IP et un masque de sous-réseau.

b. Configurez une passerelle par défaut pour PC-A.

Étape 5: Vérifiez la connectivité du réseau.

Envoyez une requête ping de PC-A vers R1. Si la requête ping échoue, dépannez la connexion.

Partie 2: Configurer le routeur pour l'accès SSH

L'utilisation de Telnet pour accéder à un périphérique réseau présente un risque de sécurité, car toutes les informations sont transmises en clair. SSH chiffre les données de la session et assure l'authentification du périphérique, c'est pourquoi ce protocole est recommandé pour les connexions à distance. Dans la deuxième partie, vous allez configurer le routeur pour qu'il accepte les connexions SSH sur les lignes VTY.

Étape 1: Configurez l'authentification du périphérique.

Les noms du périphérique et du domaine sont utilisés dans la clé de chiffrement (crypto key) lorsqu'elle est générée. Par conséquent, ces noms doivent être entrés avant l'exécution de la commande **crypto key**.

a. Configurez le nom du périphérique.

```
Router(config)# hostname R1
```

b. Configurez le domaine du périphérique.

```
R1(config)# ip domain-name ccna-lab.com
```

Étape 2: Configurez la méthode de la clé de chiffrement.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Étape 3: Configurez un nom d'utilisateur de base de données locale.

```
R1(config)# username admin privilege 15 secret adminpass
```

Remarque : un privilège de niveau 15 offre à l'utilisateur des droits d'administrateur.

Étape 4: Activez SSH sur les lignes VTY.

a. Activez Telnet et SSH sur les lignes VTY entrantes à l'aide de la commande **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

b. Modifiez la méthode de connexion de façon à ce que la base de données locale soit utilisée pour la vérification de l'utilisateur.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Étape 5: Enregistrez la configuration en cours dans le fichier de configuration initiale.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Étape 6: Créez une connexion SSH avec le routeur.

a. Démarrez Tera Term à partir de PC-A.

b. Établissez une session SSH avec R1. Utilisez le nom d'utilisateur **admin** et le mot de passe **adminpass**. Vous devriez pouvoir établir une session SSH avec R1.

Partie 3: Configurer le commutateur pour l'accès SSH

Dans la troisième partie, vous allez configurer le commutateur figurant dans la topologie pour qu'il accepte les connexions SSH. Une fois le commutateur configuré, ouvrez une session SSH à l'aide de Tera Term.

Étape 1: Configurez les paramètres de base sur le commutateur.

a. Accédez au commutateur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

d. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

e. Attribuez **cisco** comme mot de passe de console et activez la connexion.

f. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

g. Chiffrez les mots de passe en clair.

h. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

i. Configurez et activez l'interface VLAN 1 sur le commutateur à l'aide des informations contenues dans la table d'adressage.

j. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 2: Configurez le commutateur pour les connexions SSH.

Pour configurer SSH pour le commutateur, utilisez les mêmes commandes que celles que vous avez utilisées pour configurer SSH sur le routeur dans la deuxième partie.

a. Configurez le nom du périphérique comme indiqué dans la table d'adressage.

b. Configurez le domaine du périphérique.

```
S1(config)# ip domain-name ccna-lab.com
```

c. Configurez la méthode de la clé de chiffrement.

```
S1(config)# crypto key generate rsa modulus 1024
```

d. Configurez un nom d'utilisateur de base de données locale.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Activez Telnet et SSH sur les lignes VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input telnet ssh
```

f. Modifiez la méthode de connexion de façon à ce que la base de données locale soit utilisée pour la vérification de l'utilisateur.

```
S1(config-line)# login local
S1(config-line)# end
```

Étape 3: Créez une connexion SSH avec le commutateur.

Démarrez Tera Term à partir de PC-A, puis établissez une connexion SSH avec l'interface SVI sur S1.

Êtes-vous en mesure d'ouvrir une session SSH avec le commutateur ?

Partie 4: SSH à partir de l'interface en ligne de commande du commutateur

Le client SSH est intégré au logiciel Cisco IOS et peut être exécuté à partir de l'interface en ligne de commande (CLI). Dans la quatrième partie, vous établirez une connexion SSH avec le routeur à partir de l'interface en ligne de commande sur le commutateur.

Étape 1: Affichez les paramètres disponibles pour le client Cisco IOS SSH.

Utilisez le point d'interrogation (**?**) pour afficher les paramètres disponibles avec la commande **ssh**.

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Étape 2: Établissez une connexion SSH au routeur R1 à partir de S1.

a. Vous devez utiliser l'option **–l admin** lorsque vous établissez une connexion SSH à R1. Vous pouvez ainsi vous connecter en tant qu'utilisateur **admin**. Lorsque vous y êtes invité, tapez **adminpass** pour le mot de passe.

```
S1# ssh -l admin 192.168.1.1
Password:
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************

R1#
```

b. Vous pouvez revenir à S1 sans fermer votre session SSH à R1 en appuyant sur **Ctrl+Maj**+**6**. Relâchez les touches **Ctrl+Maj**+**6** et appuyez sur **x**. L'invite du mode d'exécution privilégié du commutateur s'affiche.

```
R1#
S1#
```

c. Pour revenir à la session SSH sur R1, appuyez sur Entrée sur une ligne de l'interface en ligne de commande vierge. Il vous faudra peut-être appuyer sur Entrée une deuxième fois pour afficher l'invite de l'interface en ligne de commande du routeur.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]


R1#
```

d. Pour mettre fin à la session SSH sur R1, tapez **exit** à l'invite du routeur.

```
R1# exit


[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Quelles versions de SSH sont prises en charge à partir de l'interface en ligne de commande ?

Remarques générales

Comment permettriez-vous à plusieurs utilisateurs, chacun disposant de leur propre nom d'utilisateur, d'accéder à un périphérique réseau ?

Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des différentes combinaisons d'interfaces Ethernet et série possibles dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes Cisco IOS.