Travaux pratiques - Utilisation de la CLI pour recueillir des informations sur les périphériques réseau

Topologie

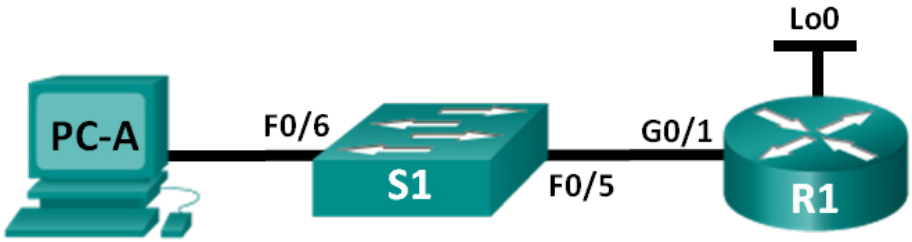


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

1re partie : Configurer la topologie et initialiser les périphériques

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez le routeur et le commutateur.

2e partie : Configurer les périphériques et vérifier la connectivité

- Attribuez une adresse IP statique à la carte réseau de PC-A.
- Configurez les paramètres de base sur R1.
- Configurez les paramètres de base sur S1.
- Vérifiez la connectivité du réseau.

3e partie : Collecter des informations sur le périphérique

- Recueillez des informations sur R1 avec les commandes de l'interface en ligne de commande de l'IOS.
- Recueillez des informations sur S1 avec les commandes de l'interface en ligne de commande de l'IOS.
- Recueillez des informations sur PC-A avec l'interface en ligne de commande.

Contexte/scénario

La documentation d'un réseau en état de fonctionnement est l'une des tâches les plus importantes que doit effectuer un professionnel des réseaux. Le fait de documenter correctement les adresses IP, les numéros de modèle, les versions de l'IOS, les ports utilisés, et de faire des tests de sécurité facilite grandement le dépannage d'un réseau.

Dans ce TP, vous allez créer un petit réseau, configurer les périphériques, ajouter une sécurité de base, puis documenter les configurations en exécutant différentes commandes sur le routeur, le commutateur et le PC pour recueillir les informations nécessaires.

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 2960s 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 : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

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 PC (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

1re partie : Configuration de la topologie et initialisation des périphériques

Dans la deuxième partie, vous allez mettre en place la topologie du réseau, effacer les configurations s'il y a lieu, et configurer les paramètres de base sur le routeur et le commutateur.

Étape 1: Câblez le réseau conformément à la topologie.

a. Connectez les périphériques représentés dans la topologie et effectuez le câblage nécessaire.

b. Mettez sous tension tous les périphériques de la topologie.

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

2e partie : Configuration des périphériques et vérification de la connectivité

Dans cette deuxième partie, vous allez mettre en place la topologie du réseau et configurer les paramètres de base sur le routeur et le commutateur. Reportez-vous à la topologie et à la table d'adressage au début de ce TP pour trouver le nom des périphériques et les informations d'adressage.

Remarque : l'annexe A contient des informations sur la configuration demandée dans la 2e partie. Essayez de terminer la deuxième partie avant de passer à cette annexe.

Étape 1: Configurez l'adresse IPv4 du PC.

Configurez l'adresse IPv4, le masque de sous-réseau et l'adresse de la passerelle par défaut du PC-A en fonction de la table d'adressage.

Étape 2: Configurez le routeur.

Si vous avez besoin d'aide pour l'étape 2, reportez-vous à l'annexe A.

a. Accédez au routeur par la console et passez en mode d'exécution privilégié.

b. Réglez l'heure sur le routeur.

c. Passez en mode de configuration globale.

1) Attribuez un nom de périphérique au routeur en fonction de la table topologique et de la table d'adressage.

2) Désactivez la recherche DNS.

3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

4) Choisissez **class** comme mot de passe chiffré pour le mode d'exécution privilégié.

5) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.

6) Chiffrez les mots de passe en clair.

7) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.

8) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.

9) Générez une clé de module RSA. Indiquez **512** pour le nombre de bits.

d. Configurez l'accès avec les lignes vty.

1) Utilisez la base de données locale pour l'authentification pour SSH.

2) Activez SSH uniquement pour l'accès par connexion.

e. Repassez en mode de configuration globale.

1) Créez l'interface Loopback 0 et attribuez l'adresse IP en fonction de la table d'adressage.

2) Configurez et activez l'interface G0/1 sur le routeur.

3) Configurez les descriptions d'interface pour G0/1 et L0.

4) Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 3: Configurez le commutateur.

Si vous avez besoin d'aide pour l'étape 3, reportez-vous à l'annexe A.

a. Accédez au commutateur par la console et passez en mode d'exécution privilégié.

b. Réglez l'heure sur le commutateur.

c. Passez en mode de configuration globale.

1) Attribuez un nom de périphérique sur le commutateur en vous basant sur la table topologique et la table d'adressage.

2) Désactivez la recherche DNS.

3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

4) Choisissez **class** comme mot de passe chiffré pour le mode d'exécution privilégié.

5) Chiffrez tous les mots de passe en clair.

6) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.

7) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.

8) Générez une clé de module RSA. Indiquez **512** pour le nombre de bits.

9) Créez et activez une adresse IP sur le commutateur d'après la table topologique et la table d'adressage.

10) Configurez la passerelle par défaut sur le commutateur.

11) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.

d. Configurez l'accès avec les lignes vty.

1) Utilisez la base de données locale pour l'authentification pour SSH.

2) Activez SSH uniquement pour l'accès par connexion.

3) Passez dans le mode approprié pour configurer les descriptions d'interface pour F0/5 et F0/6.

4) Enregistrez la configuration en cours dans le fichier de configuration initiale.

Étape 4: Vérifiez la connectivité du réseau.

a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse IP du VLAN 1 de S1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

b. À partir de l'invite de commande du PC-A, envoyez une requête ping à l'adresse IP de la passerelle par défaut sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

c. À partir de l'invite de commande du PC-A, envoyez une requête ping à l'interface de bouclage sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

d. Reconnectez-vous via la console au commutateur et envoyez une requête ping à l'adresse IP G0/1 sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

3e partie : Collecte d'informations sur les périphériques réseau

Dans la troisième partie, vous allez utiliser différentes commandes pour recueillir des informations sur les périphériques de votre réseau, ainsi que sur les caractéristiques des performances. La documentation du réseau est un élément très important de la gestion du réseau. Il est essentiel d'inclure les deux topologies, physique et logique, autant que de vérifier les modèles de plate-forme et les versions IOS de vos périphériques réseau. Un professionnel doit savoir quelles commandes utiliser pour collecter ces informations.

Étape 1: Recueillez des informations sur R1 en utilisant les commandes de l'IOS.

L'une des étapes de base consiste à recueillir des informations sur le périphérique physique, ainsi que des informations relatives au système d'exploitation.

a. Exécutez la commande adéquate pour obtenir les informations suivantes :

Modèle de routeur :

Version de l'IOS :

RAM totale :

NVRAM totale :

Mémoire Flash totale :

Fichier d'image IOS :

Registre de configuration :

Module technologique :

Quelle commande avez-vous exécutée pour recueillir ces informations ?

b. Exécutez la commande appropriée pour afficher un récapitulatif des informations importantes sur les interfaces de routeur. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Remarque : indiquez uniquement les interfaces qui possèdent des adresses IP.

c. Exécutez la commande appropriée pour afficher la table de routage. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

d. Quelle commande utiliseriez-vous pour afficher le mappage des adresses couche 2 -> couche 3 sur le routeur ? Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

e. Quelle commande utiliseriez-vous pour avoir des informations détaillées sur toutes les interfaces du routeur ou sur une interface spécifique ? Inscrivez cette commande ci-dessous.

f. Cisco propose un protocole très puissant. Celui-ci fonctionne sur la couche 2 du modèle OSI. Il peut vous aider à déterminer comment les périphériques Cisco sont physiquement connectés, ainsi que les numéros de modèle et même les versions IOS et l'adressage IP. Quelle commande (ou commandes) utiliseriez-vous sur le routeur R1 pour recueillir des informations sur le commutateur S1 qui vous aideront à compléter le tableau ci-dessous ?

ID de périphérique	Interface locale	Fonctionnalité	Numéro de modèle	ID du port distant	Adresse IP	Version du logiciel IOS

Commande :

g. Vous pouvez tester très simplement vos périphériques réseau en essayant d'y accéder via Telnet. Souvenez-vous toutefois que Telnet n'est pas un protocole sécurisé. En principe, il ne doit pas être activé. À l'aide d'un client Telnet, tel que Tera Term ou PuTTY, essayez d'établir une connexion Telnet avec R1 en utilisant l'adresse IP de la passerelle par défaut. Notez vos résultats ci-dessous.

h. À partir du PC-A, faites un test pour vous assurer que SSH fonctionne correctement. Avec un client SSH, tel que Tera Term ou PuTTY, établissez une connexion SSH avec R1 à partir du PC-A. Si vous recevez un message d'avertissement à propos d'une différence de clé, cliquez sur **Continue**. Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés, ceux que vous avez créés dans la deuxième partie. Avez-vous réussi ?

Les différents mots de passe configurés sur votre routeur doivent être aussi fiables et protégés que possible.

Remarque : les mots de passe utilisés pour notre TP (**cisco** et **class**) ne respectent pas les meilleures pratiques. Ils sont utilisés uniquement pour les TP. Par défaut, le mot de passe de console et tous les mots de passe vty configurés s'affichent en clair dans votre fichier de configuration.

i. Vérifiez que tous vos mots de passe du fichier de configuration sont chiffrés. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Commande : _____

Le mot de passe de console est-il chiffré ?

Le mot de passe SSH est-il chiffré ?

Étape 2: Recueillez des informations sur S1 avec les commandes IOS.

De nombreuses commandes utilisées sur R1 peuvent également l'être avec le commutateur. Cependant, il y a des différences pour certaines commandes.

a. Exécutez la commande adéquate pour obtenir les informations suivantes :

Modèle de commutateur :

Version de l'IOS :

NVRAM totale :

Fichier d'image IOS :

Quelle commande avez-vous exécutée pour recueillir ces informations ?

b. Exécutez la commande appropriée pour afficher un récapitulatif des informations importantes sur les interfaces de commutateur. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Remarque : n'indiquez que les interfaces actives.

c. Exécutez la commande appropriée pour afficher la table des adresses MAC du commutateur. Indiquez les adresses MAC dynamiques uniquement dans l'espace prévu à cet effet ci-dessous.

d. Assurez-vous que l'accès VTY via Telnet est désactivé sur S1. À l'aide d'un client Telnet, tel que Tera Term ou PuTTY, essayez d'établir une connexion Telnet avec S1 en utilisant l'adresse 192.168.1.11. Notez vos résultats ci-dessous.

e. À partir du PC-A, faites un test pour vous assurer que SSH fonctionne correctement. Avec un client SSH, tel que Tera Term ou PuTTY, établissez une connexion SSH avec S1 à partir du PC-A. Si vous recevez un message d'avertissement à propos d'une différence de clé, cliquez sur **Continue**. Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés. Avez-vous réussi ?

f. Complétez le tableau ci-dessous avec les informations sur le routeur R1 en utilisant la ou les commandes appropriées sur S1.

ID de périphérique	Interface locale	Fonctionnalité	Numéro de modèle	ID du port distant	Adresse IP	Version du logiciel IOS

La commande **show cdp neighbors detail** peut être utilisée à partir de l'invite du mode d'exécution utilisateur ou du mode d'exécution privilégié.

g. Vérifiez que tous vos mots de passe du fichier de configuration sont chiffrés. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Commande :

Le mot de passe de console est-il chiffré ?

Étape 3: Recueillez les informations sur PC-A.

Avec différentes commandes d'utilitaire Windows, rassemblez des informations sur PC-A.

a. À l'invite de PC-A, exécutez la commande **ipconfig /all** et notez les résultats ci-dessous.

Quelle est l'adresse IP de PC-A ?

Quel est le masque de sous-réseau de PC-A ?

Quelle est l'adresse de la passerelle par défaut de PC-A ?

Quelle est l'adresse MAC de PC-A ?

b. Exécutez la commande appropriée pour tester la pile de protocoles TCP/IP avec la carte réseau. Quelle commande avez-vous utilisée ?

c. Envoyez une requête ping à l'interface de bouclage de R1 à partir de l'invite de commande de PC-A. La requête ping a-t-elle abouti ?

d. Exécutez la commande appropriée sur PC-A pour tracer la liste de sauts de routeur pour les paquets provenant du PC-A et à destination de l'interface de bouclage de R1. Indiquez la commande et les résultats ci-dessous. Quelle commande avez-vous utilisée ?

e. Exécutez la commande appropriée sur PC-A pour trouver les mappages d'adresses couches 2 -> couche 3 figurant sur votre carte réseau. Notez les résultats ci-dessous. Indiquez uniquement les réponses pour le réseau 192.168.1.0/24. Quelle commande avez-vous utilisée ?

Remarques générales

Pourquoi est-il important de documenter vos périphériques réseau ?

Tableau récapitulatif des interfaces de routeur

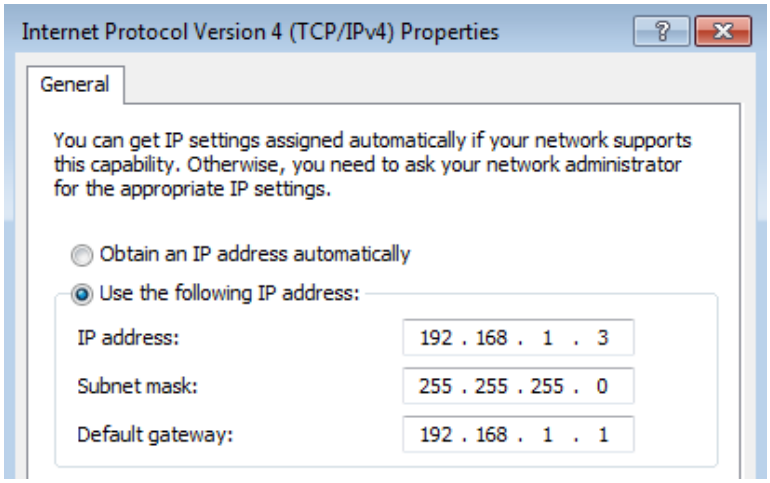
Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 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 combinaisons possibles des interfaces Ethernet et série 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 de Cisco IOS.

Annexe A : Informations de configuration relatives à la procédure de la 2e partie

Étape 1 : Configurez l'adresse IPv4 du PC.

Configurez l'adresse IPv4, le masque de sous-réseau et l'adresse de la passerelle par défaut du PC-A en vous basant sur la table d'adressage du début de ce TP.



Étape 2 : Configurez le routeur.

a. Accédez au routeur par la console et passez en mode d'exécution privilégié.

```
Router> enable
Router#
```

b. Réglez l'heure sur le routeur.

```
Router# clock set 10:40:30 6 February 2013
Router#
```

c. Passez en mode de configuration globale.

```
Router# config t
Router(config)#
```

1) Attribuez un nom d'hôte au routeur. Servez-vous de la table topologique et de la table d'adressage.

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

2) Désactivez la recherche DNS.

```
R1(config)# no ip domain-lookup
```

3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

```
R1(config)# banner motd #Warning! Unauthorized Access is prohibited.#
```

4) Choisissez **class** comme mot de passe chiffré pour le mode d'exécution privilégié.

```
R1(config)# enable secret class
```

5) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

6) Chiffrez les mots de passe en clair.

```
R1(config)# service password-encryption
```

7) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.

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

8) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.

```
R1(config)# username admin secret cisco
```

9) Générez une clé de module RSA. Indiquez **512** pour le nombre de bits.

```
R1(config)# crypto key generate rsa modulus 512
```

d. Configurez l'accès avec les lignes vty.

1) Utilisez la base de données locale pour l'authentification pour SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

2) Activez SSH uniquement pour l'accès par connexion.

```
R1(config-line)# transport input ssh
```

e. Repassez en mode de configuration globale.

```
R1(config-line)# exit
```

1) Créez l'interface Loopback 0 et attribuez l'adresse IP en fonction de la table d'adressage.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

2) Configurez et activez l'interface G0/1 sur le routeur.

```
R1(config-if)# int g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
```

3) Configurez les descriptions d'interface pour G0/1 et L0.

```
R1(config-if)# description Connected to LAN
R1(config-if)# int lo0
R1(config-if)# description Emulate ISP Connection
```

4) Enregistrez la configuration en cours dans le fichier de configuration initiale.

```
R1(config-if)# end
R1# copy run start
```

Étape 3 : Configurez le commutateur.

a. Accédez au commutateur par la console et passez en mode d'exécution privilégié.

```
Switch> enable
Switch#
```

b. Réglez l'heure sur le commutateur.

```
Switch# clock set 10:52:30 6 February 2013
```

c. Passez en mode de configuration globale.

```
Switch# config t
```

1) Attribuez un nom d'hôte sur le commutateur en vous basant sur la table topologique et la table d'adressage.

```
Switch(config)# hostname S1
```

2) Désactivez la recherche DNS.

```
S1(config)# no ip domain-lookup
```

3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited.#
```

4) Choisissez **class** comme mot de passe chiffré pour le mode d'exécution privilégié.

```
S1(config)# enable secret class
```

5) Chiffrez tous les mots de passe en clair.

```
S1(config)# service password-encryption
```

6) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.

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

7) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.

```
S1(config)# username admin secret cisco
```

8) Générez une clé de module RSA. Indiquez **512** pour le nombre de bits.

```
S1(config)# crypto key generate rsa modulus 512
```

9) Créez et activez une adresse IP sur le commutateur d'après la table topologique et la table d'adressage.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shut
```

10) Configurez la passerelle par défaut sur le commutateur.

```
S1(config)# ip default-gateway 192.168.1.1
```

11) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.

```
S1(config-if)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
```

d. Configurez l'accès avec les lignes vty.

1) Utilisez la base de données locale pour l'authentification pour SSH.

```
S1(config-line)# line vty 0 15
S1(config-line)# login local
```

2) Activez SSH uniquement pour l'accès par connexion.

```
S1(config-line)# transport input ssh
```

3) Passez dans le mode de configuration approprié pour configurer les descriptions d'interface pour F0/5 et F0/6.

```
S1(config-line)# int f0/5
S1(config-if)# description Connected to R1
S1(config-if)# int f0/6
S1(config-if)# description Connected to PC-A
```

4) Enregistrez la configuration en cours dans le fichier de configuration initiale.

```
S1(config-if)# end
S1# copy run start
```