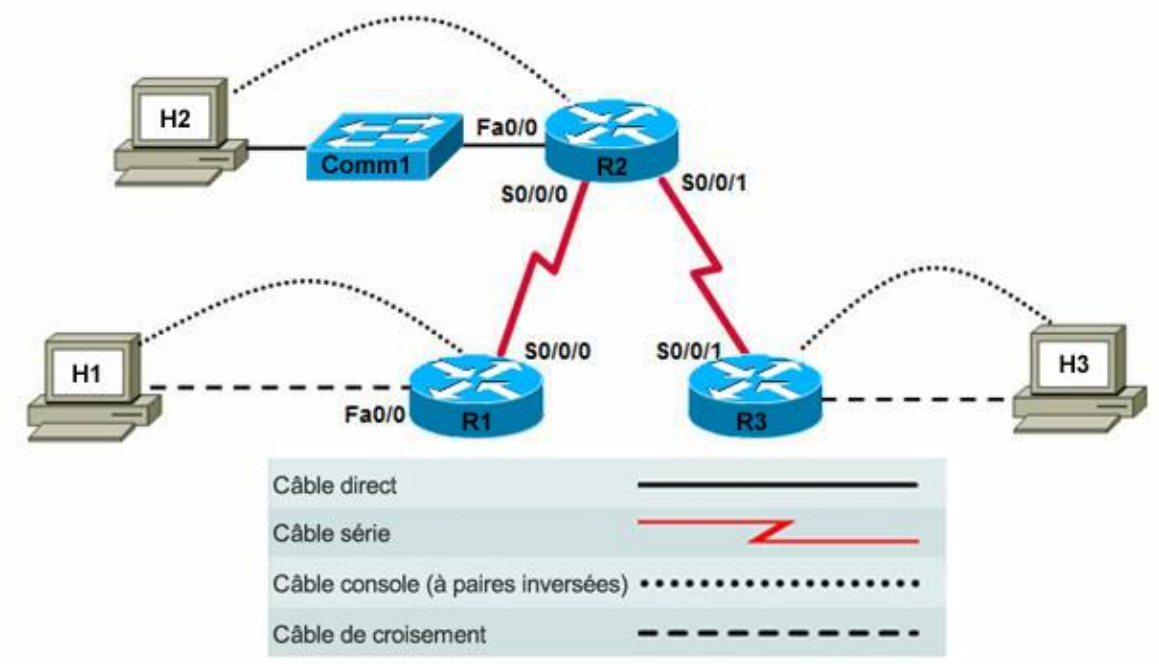
Travaux pratiques 9.5.3 Utilisation de Telnet et SSH pour accéder aux périphériques réseau



Périphérique	Nom de l'hôte	Interface	Adresse IP	Masque de sous-réseau	Instructions du réseau RIPv2
R1	R1	Série 0/0/0 (ETTD)	10.10.10.1	255.255.255.0	10.0.0.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0	192.168.1.0
R2	R2	Série 0/0/0 (DCE)	10.10.10.2	255.255.255.0	10.0.0.0
		Série 0/0/1 (DCE)	172.16.1.1	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.2.1	255.255.255.0	192.168.2.0
R3	R3	Série 0/0/1 (ETTD)	172.16.1.2	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.3.1	255.255.255.0	192.168.3.0
Comm1	S1	VLAN 1 (admin)	192.168.2.99	255.255.255.0	N/D

Objectifs

- Établir et gérer les connexions Telnet vers un routeur et un commutateur distants
- Vérifier si la couche application entre la source et la destination fonctionne correctement
- Vérifier les informations des routeurs distants, à l'aide des commandes **show**
- Configurer un routeur pour accepter les connexions SSH, à l'aide de l'interface de ligne de commande (ILC) Cisco IOS.
- Établir une connexion entre un routeur utilisant le client SSH ILC et un routeur distant exécutant le serveur SSH

Contexte / Préparation

Telnet est un excellent outil de dépannage de problèmes liés aux fonctions des couches supérieures. L'utilisation de Telnet pour accéder aux périphériques réseau permet aux techniciens d'exécuter des commandes sur chaque périphérique, comme s'il s'agissait de périphériques locaux. En outre, la possibilité d'accéder aux périphériques via Telnet indique qu'il existe une connectivité des couches inférieures entre les périphériques. Telnet est disponible sur la grosse majorité des périphériques réseau.

Telnet est un protocole non sécurisé, ce qui signifie que toutes les données transmises peuvent être capturées et lues. Le protocole SSH permet un accès plus sécurisé aux périphériques distants. La plupart des versions récentes de Cisco IOS contiennent un serveur SSH et un client SSH. Dans certains périphériques, ce service est activé par défaut. D'autres périphériques requièrent une activation manuelle du serveur SSH. De même, vous pouvez utiliser un ordinateur distant doté d'un client SSH pour démarrer une session ILC sécurisée.

Ces travaux pratiques se concentrent sur l'utilisation de Telnet et SSH pour accéder à distance aux routeurs afin de collecter des informations les concernant et de vérifier la connectivité des couches les plus hautes. Dans le cadre de ces travaux pratiques, vous apprendrez à établir une connexion Telnet depuis la station de travail, utilisée en tant que client et entre un routeur et un autre routeur distant. De plus, vous apprendrez à configurer l'accès SSH sur un routeur et à établir une connexion à l'aide d'un client ILC de Cisco IOS basé sur un routeur.

Installez un réseau similaire à celui du schéma de topologie. Tout routeur répondant aux exigences indiquées dans ce schéma en matière d'interface peut être utilisé, par exemple les routeurs 800, 1600, 1700, 1800, 2500 ou 2600 ou une combinaison de ces routeurs. Reportez-vous au tableau Relevé des interfaces de routeur, présenté à la fin de ce document, pour déterminer les identifiants d'interface à utiliser en fonction de l'équipement disponible. En fonction du modèle de routeur utilisé, la sortie que vous obtenez peut différer de celle indiquée dans ces travaux pratiques.

Ressources requises

Les ressources requises sont les suivantes :

- Un routeur 1841, ou autre routeur similaire, équipé de deux interfaces série et d'une interface Fast Ethernet
- Deux routeurs 1841, ou autres routeurs similaires, équipés d'une interface série et d'une interface Fast Ethernet
- Un commutateur Cisco 2960, ou un autre commutateur équivalent, pour le réseau local R2
- Trois ordinateurs équipés de Windows XP (les hôtes H2 et H3 sont principalement destinés à la configuration des routeurs R2 et R3.)
- Câbles droits et câbles de croisement Ethernet de catégorie 5, selon les besoins
- Deux câbles série null
- Un câble de console pour configurer les routeurs
- Un accès à l'invite de commande de l'hôte H1
- Un accès à la configuration réseau TCP/IP de l'hôte H1

Sur les hôtes H1, H2 et H3, démarrez une session HyperTerminal vers chaque routeur.

Remarque : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. Pour plus d'informations sur l'effacement, reportez-vous au Manuel des travaux pratiques, disponible dans la section Tools du site Academy Connection. Si vous n'êtes pas sûr de la procédure, demandez conseil à votre formateur.

Étape 1 : utilisation de Telnet pour vérifier la configuration et la connectivité des périphériques

Tâche 1 : création du réseau et vérification de la connexion de la couche réseau

Étape 1 : configuration des informations de base sur chaque routeur et sur le commutateur

a. Installez et configurez le réseau conformément au schéma topologique et au tableau de configuration des périphériques. Pour plus d'informations sur la définition des noms d'hôtes, mots de passe et adresses d'interfaces, reportez-vous s'il y a lieu aux instructions présentées dans les travaux pratiques 5.3.5, « Configuration des paramètres de base d'un routeur à l'aide de l'interface de ligne de commande Cisco IOS ».

b. Configurez RIPv2 sur chaque routeur, et annoncez les réseaux présentés dans le tableau de configuration des périphériques. Pour plus d'informations sur la configuration du protocole de routage RIP, reportez-vous aux instructions présentées dans les travaux pratiques 6.1.5, « Configuration et vérification du protocole RIP ».

c. Définissez les paramètres de base sur le commutateur Comm1 : nom de l'hôte, mots de passe et adresse IP du réseau local virtuel VLAN 1. Pour plus d'informations, reportez-vous aux instructions présentées dans les travaux pratiques 5.4.4 « Configuration du commutateur Cisco 2960 ».

Étape 2 : configuration des hôtes

Configurez les hôtes H1, H2 et H3 en définissant une adresse IP, un masque de sous-réseau et une passerelle par défaut compatibles avec l'adresse IP de l'adresse d'interface de la passerelle par défaut pour le réseau local auquel ils sont reliés.

Étape 3 : vérification de la connexion de bout en bout de la couche réseau

a. Sur l'hôte H1, ouvrez une fenêtre **Invite de commandes** en cliquant sur **Démarrer** > **Exécuter** et en tapant **cmd**. Vous pouvez également sélectionner **Démarrer** > **Tous les programmes** > **Accessoires** > **Invite de commandes**.

b. Utilisez la commande **ping** pour tester la connectivité de bout en bout. Depuis l'hôte H1, sur le réseau local de R1, envoyez une requête ping à l'hôte H3 sur le réseau local de R3 (par exemple, 192.168.3.2).

```
C:\>ping 192.168.3.2
```

c. Si H3 n'est pas relié à R3, envoyez une requête ping à l'adresse IP 172.16.1.2 de l'interface série Serial 0/0/1 de R3.

```
C:\>ping 172.16.1.2
```

d. Si la requête ping aboutit sur R3, que peut-on en conclure sur la connectivité de couche OSI entre H1 et R3 ? _____

Remarque : si la requête ping a échoué, corrigez les configurations du routeur et de l'hôte et vérifiez les connexions.

Tâche 2 : établissement d'une session Telnet depuis un ordinateur hôte

Étape 1 : établissement d'une connexion Telnet de H1 au routeur distant R2

Le logiciel Cisco IOS du routeur dispose d'un logiciel client-serveur Telnet intégré. La plupart des systèmes d'exploitation possèdent un client Telnet. Un grand nombre de systèmes d'exploitation serveur sont également équipés d'un serveur Telnet, bien que les systèmes d'exploitation des ordinateurs de bureau de Microsoft Windows n'en possèdent pas.

En règle générale, vous ne pourrez pas accéder directement à un routeur via la console mais vous pourrez établir une connexion Telnet avec d'autres routeurs. La connexion Telnet vers un routeur s'effectue généralement depuis un ordinateur hôte. Vous pourrez alors établir une connexion Telnet avec les autres routeurs, accessibles via le réseau.

a. Depuis l'invite de commande de H1, établissez une connexion Telnet avec l'interface Fast Ethernet 0/0 du routeur R2.

```
C:\>telnet 192.168.2.1
```

b. Entrez le mot de passe **cisco** pour accéder au routeur.

c. Quelle est l'invite affichée sur le routeur ? _____

d. Entrez la commande **show version**.

e. Quelle est la version du logiciel Cisco IOS du routeur distant R2 ? _____

f. De combien d'interfaces, et de quel type est équipé le routeur distant R2 ? _____

g. Si la connexion Telnet entre H1 et R2 aboutit, que peut-on en conclure sur la connectivité de couche OSI entre les périphériques ?

_____

Étape 2 : fin de la session Telnet entre H1 et le routeur distant R2

Terminez la session Telnet entre H1 et R2 en tapant la commande **exit**.

Tâche 3 : exécution d'opérations Telnet de base entre les routeurs

Étape 1 : établissement d'une connexion Telnet entre R1 et le routeur distant R2

Remarque : Telnet utilise les lignes vty du routeur distant pour se connecter. Si les lignes vty ne sont pas configurées pour une connexion ou si aucun mot de passe n'est défini, vous ne pourrez pas vous connecter au routeur distant via Telnet.

a. Établissez une connexion Telnet avec l'adresse IP 10.10.10.2 de l'interface série Serial 0/0/0 de R2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Entrez le mot de passe **cisco** pour accéder au routeur.

c. Quelle est l'invite affichée sur le routeur ? _____

Étape 2 : examen des interfaces du routeur distant R2

a. Exécutez la commande **show ip interface brief** à l'invite de commande de l'ordinateur distant.

```
R2>show ip interface brief
```

b. Citez les interfaces actives du routeur distant R2. _____

Étape 3 : affichage de la table de routage sur le routeur distant

Exécutez la commande **show ip route** à l'invite de commande du routeur. Quelles sont les routes que R2 a découvertes depuis RIP ?

_____

```
R2>show ip route
```


Étape 4 : affichage des voisins CDP pour R2

a. Utilisez le protocole CDP (Cisco Discovery Protocol) pour afficher les informations concernant les périphériques Cisco directement attachés à R2. Exécutez la commande **show cdp neighbors** à l'invite de commande du routeur.

b. Dressez la liste de tous les ID de périphériques connectés au routeur distant. Quelle est la plateforme de chaque périphérique ?

_____

```
R2>show cdp neighbors
```

Étape 5 : suspension de la session Telnet active sur R2

a. Utilisez le raccourci clavier **Ctrl-Shift-6,** puis appuyez sur la touche **x**. Cette action permet uniquement d'interrompre la session et de revenir au routeur précédent. Elle ne provoque pas la déconnexion de ce routeur.

b. Quelle est l'invite affichée sur le routeur ? _____

Étape 6 : reprise de la session Telnet active sur R2

a. À l'invite de commande du routeur, appuyez sur la touche **Entrée**. Quelle doit être la réponse du routeur ?

_____

Appuyer sur la touche **Entrée** entraîne la reprise de la session Telnet, précédemment suspendue.

b. Quelle est l'invite affichée sur le routeur ? _____

Étape 7 : fermeture de la session Telnet sur R2

a. Terminez la session Telnet en tapant **exit**.

b. Quelle doit être la réponse du routeur ? _____

c. Quelle est l'invite affichée sur le routeur ? _____

Remarque : lorsque la session Telnet est suspendue, vous pouvez mettre fin à cette connexion à partir de cette session, en entrant la commande **disconnect** et le numéro de session.

Tâche 4 : exécution d'opérations Telnet entre plusieurs routeurs

Étape 1 : établissement d'une connexion Telnet entre R1 et le routeur distant R2

a. Depuis R1, établissez une connexion Telnet avec l'adresse IP 10.10.10.2 de l'interface série Serial 0/0/0 de R2.

b. Entrez le mot de passe **cisco** pour accéder au routeur.

Étape 2 : établissement d'une session Telnet supplémentaire de R2 à R3

a. Depuis R2, établissez une connexion Telnet avec l'adresse IP 172.16.1.2 de l'interface série Serial 0/0/1 de R3.

b. Entrez le mot de passe **cisco** pour accéder au routeur.

c. Quelle est l'invite affichée sur le routeur ? _____

Étape 3 : suspension de la session Telnet sur R3

a. Utilisez le raccourci clavier **Ctrl-Shift-6**, puis appuyez sur la touche **x**.

b. Quelle est l'invite affichée sur le routeur ? _____

Étape 4 : affichage des sessions Telnet actives

Entrez la commande **show sessions** à l'invite de commande de R1. Quel est le nombre de sessions actives ? _____

Remarque : la session par défaut est indiquée par un astérisque (*). Il s'agit de la session reprise lorsque vous appuyez sur la touche **Entrée**.

```
R2>show sessions
```

Étape 5 : reprise de la session Telnet active sur R2

a. À l'invite de commande du routeur, appuyez sur la touche **Entrée**. Quelle doit être la réponse du routeur ?

_____

b. Quelle est l'invite affichée sur le routeur ? _____

c. Pourquoi l'invite indique-t-elle R3 ? _____

Étape 6 : déconnexion des sessions entre R1 et R2 et R3

a. Entrez la commande **exit** à l'invite de commande de R3, puis appuyez sur la touche **Entrée** pour fermer la connexion à R3.

```
R3>exit
[Connection to 172.16.1.2 closed by foreign host]
R2>
```

b. Suspendez la session de R2 depuis R1 (session 1 sur R1) en utilisant le raccourci clavier **Ctrl-Shift-6**, puis en appuyant sur la touche **x**. Utilisez la commande **disconnect** pour mettre fin à la connexion à R2.

```
R1>disconnect 1
Closing connection to 10.10.10.2 [confirm]
```

Tâche 4 : suppression du mot de passe vty de R3

Étape 1 : établissement d'une connexion Telnet entre R1 et le routeur distant R3

a. Établissez une connexion Telnet avec l'adresse IP 172.16.1.2 de l'interface série Serial 0/0/1 de R3.

```
R1>telnet 172.16.1.2
Trying 172.16.1.2 ... Open
User Access Verification
Password:
```

b. Entrez le mot de passe **cisco** pour accéder au routeur.

c. Quelle est l'invite affichée sur le routeur ? _____

Étape 2 : suppression du mot de passe vty depuis le mode d'exécution privilégié sur R3

a. Entrez la commande **enable** à l'invite R3>, puis entrez le mot de passe **class**.

b. Quelle est l'invite affichée sur le routeur ? _____

c. Supprimez le mot de passe pour les lignes vty sur R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#no password
R3(config-line)#end
R3#
```

d. Terminez la session Telnet de R3 et revenez à R1.

```
R3#exit
[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Étape 3 : établissement d'une nouvelle connexion Telnet entre R1 et le routeur distant R3

a. Établissez une connexion Telnet avec l'adresse IP 172.16.1.2 de l'interface série Serial 0/0/1 de R3.

```
R1>telnet 172.16.1.2
```

b. Pouvez-vous établir une connexion Telnet vers R3 ? _____ n

c. Quel est le message affiché et pourquoi ?

_____

_____

Étape 4 : connexion à R3 via la console et redéfinition du mot de passe vty

a. Entrez la commande **enable** à l'invite R3>, puis entrez le mot de passe **class**.

b. Redéfinissez le mot de passe pour les lignes vty sur R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#end
R3#
```

Étape 2 : utilisation de SSH pour vérifier la configuration et la connectivité des périphériques

Secure Shell, ou SSH, est une version chiffrée RSA de Telnet. Toutes les informations, y compris les identifiants utilisateur, les mots de passe et les données qui transitent entre un client et un serveur SSH, sont chiffrées. SSH étant un protocole de couche application, une connexion SSH prouve que toutes les couches OSI fonctionnent correctement, notamment le chiffrement de la couche présentation.

Tâche 1 : configuration de SSH sur le routeur R2

Étape 1 : établissement d'une connexion Telnet entre R1 et le routeur distant R2

a. Établissez une connexion Telnet avec l'adresse IP 10.10.10.2 de l'interface série Serial 0/0/0 de R2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Entrez le mot de passe **cisco** pour accéder au routeur.

c. Quelle est l'invite affichée sur le routeur ? _____

Étape 2 : configuration du serveur SSH sur R2

a. Créez un nom de domaine et un identifiant utilisateur Telnet/SSH, ainsi qu'un mot de passe, pour les connexions vty distantes.

Remarque : en créant un identifiant utilisateur et un mot de passe, et en définissant un mot de passe d'ouverture de session locale pour les lignes vty, toute tentative de connexion Telnet ou SSH à ce routeur requiert la saisie du nom d'utilisateur et du mot de passe créés.

Étant donné que l'utilisateur admin dispose d'un niveau de privilège de 15 (niveau le plus élevé) et que le niveau de privilège 15 est configuré pour les lignes vty, l'invite de commande du routeur passe directement en mode d'exécution privilégié (enable) lors de la connexion à R2 via Telnet ou SSH.

L'utilisation d'un identifiant utilisateur et d'un mot de passe particuliers pour sécuriser l'accès Telnet et SSH vty au routeur n'affecte pas le mot de passe de la console (line con 0), ni le mot de passe secret actif.

```
Router#config terminal
R2(config)#ip domain-name customer.com
R2(config)#username admin privilege 15 password 0 cisco123
R2(config)#exit
```

b. Configurez les lignes de terminal vty pour accepter les connexions distantes entrantes des clients Telnet et SSH, et validez l'identifiant utilisateur dans la base de données locale de noms d'utilisateur du routeur.

```
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input telnet ssh
R2(config-line)#exit
```

Remarque : si Telnet n'est pas spécifié dans la commande **transport input** ci-dessus, seules les connexions SSH distantes seront autorisées sur ce routeur.

c. Générez la paire de clés de chiffrement RSA dont se servira le routeur pour l'authentification et le chiffrement des données SSH qui sont transmises. Entrez **768** pour le nombre de bits du modulus. La valeur par défaut est de 512.

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.customer.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512] 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
*Mar 20 13:17:50.123: %SSH-5-ENABLED: SSH 1.99 has been enabled

R2(config)#exit
```

d. Vérifiez si SSH est activé et la version utilisée, en entrant la commande **show ip ssh**.

```
R2#show ip ssh
```

e. Remplissez les informations suivantes en fonction du résultat de la commande **show ip ssh** :

Version de SSH active_____
Délai d'authentification_____
Nombre de tentatives d'authentification_____

f. Exécutez la commande **show running-config**. Quelle indication nous indique que le serveur SSH a été configuré sur R2 ? _____

_____

g. Enregistrez la configuration en cours (running-config) dans la configuration initiale (startup-config).

```
R2#copy running-config startup-config
```

h. Terminez la session Telnet de R2 et revenez à R1.

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1#
```

Tâche 2 : connexion à R2 via le client SSH ILC de R1

Remarque : vous pouvez également vous connecter à un routeur ou à un commutateur SSH à l'aide d'un ordinateur équipé d'un client à interface graphique (GUI) tel que PuTTY. Cette procédure est décrite dans les travaux pratiques 8.3.4 : « Configuration d'un routeur distant à l'aide de SSH ».

Étape 1 : utilisation de la fonctionnalité d'aide contextuelle ILC de Cisco IOS avec la commande ssh

Depuis la session de terminal de R1, utilisez la fonctionnalité d'aide contextuelle ILC de Cisco IOS pour afficher les options d'ouverture de session pour le client SSH de R1.

```
R1#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
  WORD  IP address or hostname of a remote system

R1#ssh -l admin ?
  -c    Select encryption algorithm
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system
```

Étape 2 : connexion à R2 avec SSH

Dans cette étape, vous apprendrez à vous connecter au serveur SSH de R2 depuis le client SSH ILC de R1. Vous établirez une session distante sécurisée avec R2, à partir de laquelle vous pourrez exécuter les commandes show et configuration.

a. Connectez-vous à R2 en spécifiant l'identifiant utilisateur **admin** et le mot de passe **cisco123**, qui ont été définis précédemment, ainsi que l'adresse IP de l'interface série S0/0/0 de R2.

```
R1#ssh -l admin 10.10.10.2

Password:
Unauthorized Use Prohibited
R2#
```

b. Pourquoi l'invite de commande du routeur est-elle en mode d'exécution privilégié (enable) ?

_____

c. Sur R2, exécutez la commande **show ssh** pour afficher les connexions SSH du routeur.

```
R2#show ssh
Connection Version Mode Encryption   Hmac       State           Username
0          1.99     IN   aes128-cbc  hmac-sha1  Session started  admin
0          1.99     OUT  aes128-cbc  hmac-sha1  Session started  admin
%No SSHv1 server connections running.
```

d. Terminez la session SSH de R2 et revenez à R1.

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1>
```

Remarque : si vous utilisez le raccourci clavier **Ctrl-Shift-6**, puis appuyez sur la touche **x**, les commandes utilisées précédemment avec Telnet seront les mêmes pour SSH.

Tâche 3 : remarques générales

a. **Connectivité HTTP** : vous pouvez également vérifier la connectivité de couche application à l'aide de l'interface HTTP pour un routeur ou un commutateur. Si la commande **ip http server** est présente dans la configuration courante du périphérique, vous pouvez ouvrir un navigateur sur un ordinateur équipé d'une connectivité réseau à l'adresse IP (ou au nom, si DNS est activé) du routeur ou du commutateur et accéder à l'application HTTP de gestion d'interface graphique du périphérique. Il peut s'agir d'une interface HTTP de base pour les routeurs non-SDM ou de SDM et SDM Express pour les routeurs SDM. HTTP étant un protocole de couche application, une connexion HTTP prouve que toutes les couches OSI fonctionnent correctement.

b. Comparez les avantages et les inconvénients de Telnet et de SSH.

_____

_____

_____

c. Si vous pouvez envoyer une requête ping à une interface de routeur mais que vous ne pouvez pas vous y connecter à l'aide de Telnet ou de SSH, d'où peut provenir le problème, et quelles sont les couches du modèle OSI qui seront affectées ?

_____

_____

_____

Résumé des interfaces des routeurs				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (Comm1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (Comm1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (Comm1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
Remarque : pour connaître la configuration exacte du routeur, consultez les interfaces. Vous pouvez ainsi identifier le type du 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. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque périphérique. Ce tableau d'interfaces 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 une commande Cisco IOS.				