Travaux pratiques - Analyse de Telnet et de SSH dans Wireshark

Topologie

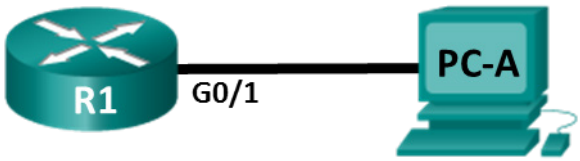


Table d'adressage

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

Objectifs

Partie 1 : Configurer les périphériques pour l'accès SSH

Partie 2 : Analyser une session Telnet avec Wireshark

Partie 3 : Analyser une session SSH avec Wireshark

Contexte/scénario

Au cours de ces travaux pratiques, vous allez configurer un routeur pour qu'il accepte les connexions SSH, et vous utiliserez Wireshark pour capturer et afficher des sessions Telnet et SSH. Vous verrez ainsi l'importance du chiffrement avec SSH.

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 différer 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 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 périphériques pour l'accès SSH

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.

Étape 3: Configurez les paramètres de base sur le routeur.

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

b. Passez en mode de configuration.

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

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

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

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

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

h. Chiffrez les mots de passe en clair.

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

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

Étape 4: Configurez R1 pour l'accès SSH.

a. Configurez le domaine du périphérique.

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

b. Configurez la méthode de la clé de chiffrement.

```
R1(config)# crypto key generate rsa modulus 1024
```

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

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

d. Activez Telnet et SSH sur les lignes VTY.

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

e. 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
```

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

Étape 6: 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 7: vérification de la connectivité du réseau.

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

Partie 2: Analyser une session Telnet avec Wireshark

Dans la deuxième partie, vous allez utiliser Wireshark pour capturer et afficher les données transmises d'une session Telnet sur le routeur. Vous utiliserez Tera Term pour établir une connexion Telnet à R1, vous connecter, puis exécuter la commande **show run** sur le routeur.

Remarque : si aucun logiciel client Telnet/SSH n'est installé sur votre ordinateur, vous devez en installer un avant de continuer. Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) et PuTTY (www.putty.org) sont deux logiciels Telnet/SSH libres couramment utilisés.

Remarque : par défaut, Telnet n'est pas disponible à partir de l'invite de commande dans Windows 7. Pour activer Telnet afin de l'utiliser dans l'invite de commande, cliquez sur **Démarrer > Panneau de configuration > Programmes > Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités Windows**. Cochez la case **Telnet Client** (Client Telnet), puis cliquez sur **OK**.

Étape 1: Capturez des données.

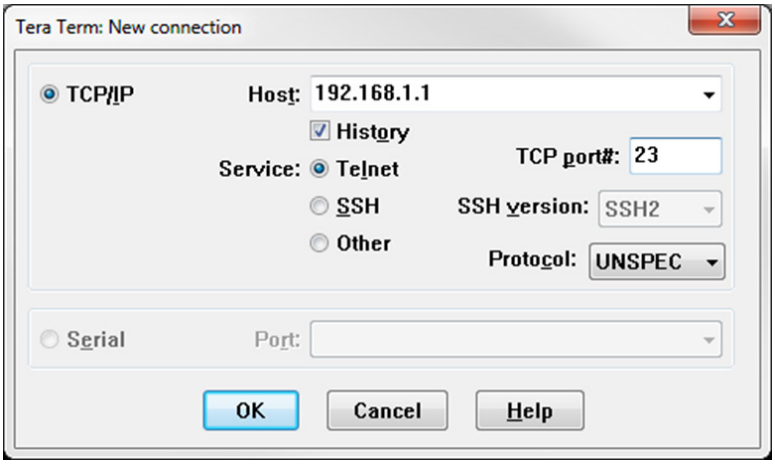
a. Démarrez Wireshark.

b. Commencez à capturer des données sur l'interface LAN.

Remarque : si vous ne pouvez pas commencer la capture sur l'interface LAN, vous devrez peut-être ouvrir Wireshark à l'aide de l'option **Exécuter en tant qu'administrateur**.

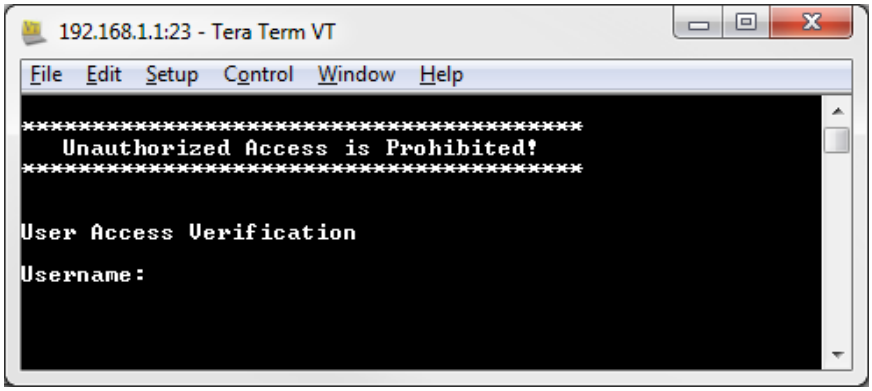
Étape 2: Démarrez une session Telnet pour accéder au routeur.

a. Ouvrez Tera Term et sélectionnez la case d'option **Telnet Service** (Service Telnet) et dans le champ Host (Hôte), entrez **192.168.1.1**.



Quel est le port TCP par défaut pour les sessions Telnet ?

b. À l'invite Username:, entrez **admin** et à l'invite Password:, entrez **adminpass**. Ces invites apparaissent parce que vous avez configuré les lignes VTY pour pouvoir utiliser la base de données locale à l'aide de la commande **login local**.



c. Exécutez la commande **show run**.

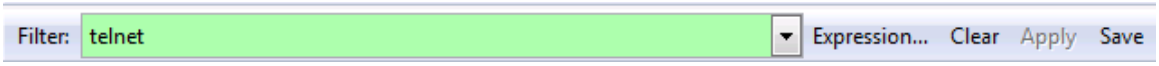
```
R1# show run
```

d. Entrez **exit** pour quitter la session Telnet et sortir de Tera Term.

```
R1# exit
```

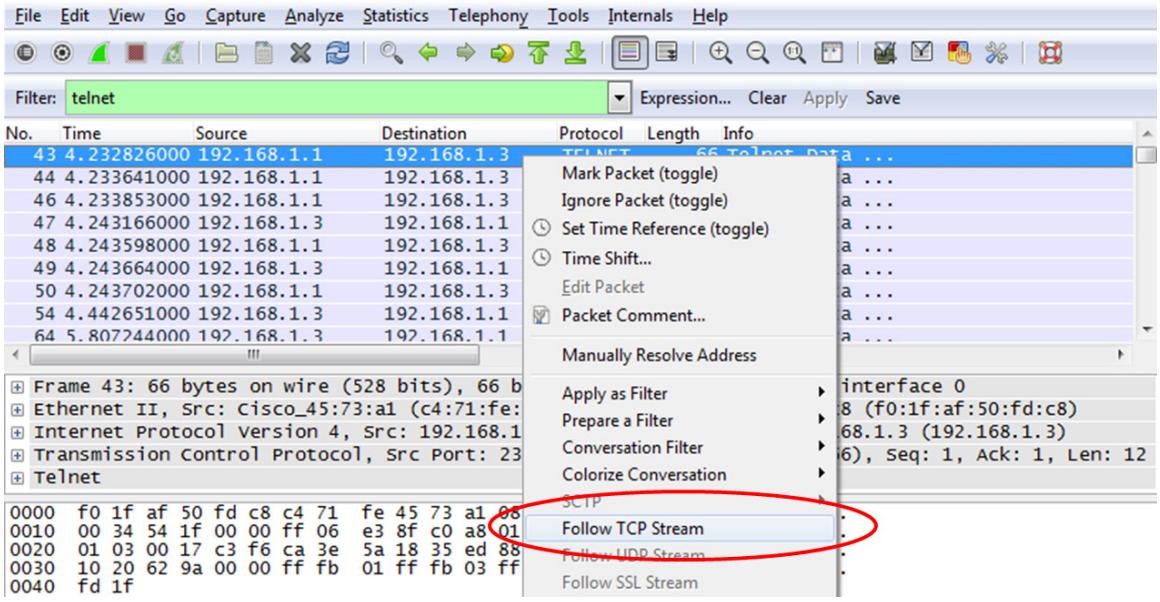
Étape 3: Arrêtez la capture Wireshark.

Étape 4: Appliquez un filtre Telnet sur les données de capture Wireshark.

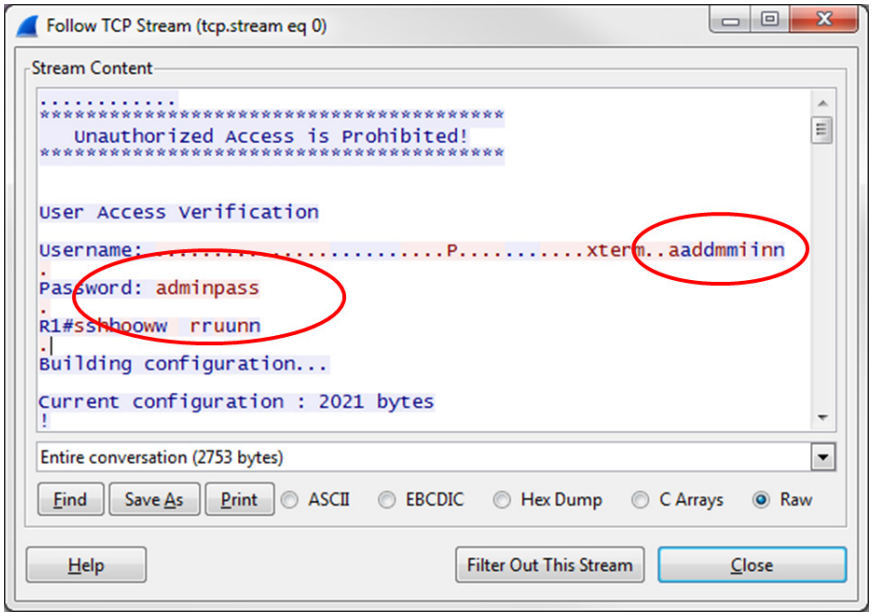


Étape 5: Utilisez la fonction Follow TCP Stream (Suivre le flux TCP) dans Wireshark pour afficher la session Telnet.

a. Cliquez avec le bouton droit sur l'une des lignes **Telnet** dans la section **Packet list** (Liste des paquets) de Wireshark et, dans la liste déroulante, sélectionnez l'option **Follow TCP Stream** (Suivre le flux TCP).



b. La fenêtre Follow TCP Stream (Suivre le flux TCP) affiche les données de votre session Telnet avec le routeur. La session complète s'affiche en clair, y compris votre mot de passe. Notez que le nom de l'utilisateur et la commande **show run** que vous avez entrés s'affichent avec des caractères en double. Cela provient du paramètre d'écho dans Telnet qui vous permet d'afficher les caractères que vous tapez à l'écran.



c. Une fois que vous avez fini de passer en revue votre session Telnet dans la fenêtre **Follow TCP Stream** (Suivre le flux TCP), cliquez sur **Close** (Fermer).

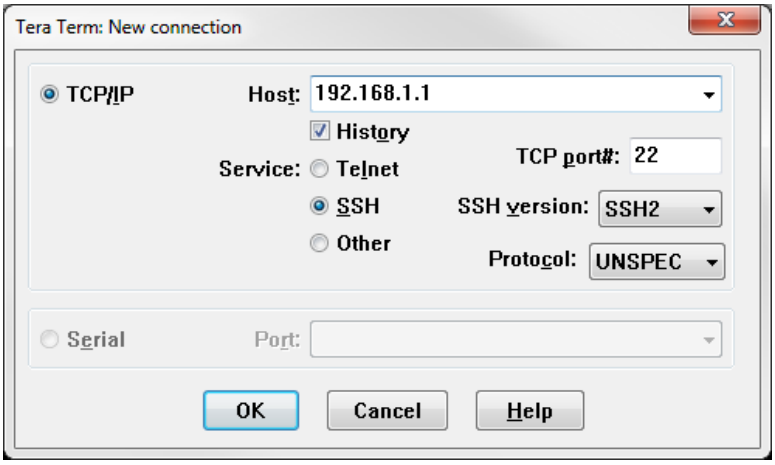
Partie 3: Analyser une session SSH avec Wireshark

Dans la quatrième partie, vous allez utiliser le logiciel Tera term pour établir une session SSH avec le routeur. Wireshark permet de capturer et d'afficher les données de cette session SSH.

Étape 1: Ouvrez Wireshark et commencez à capturer des données sur l'interface LAN.

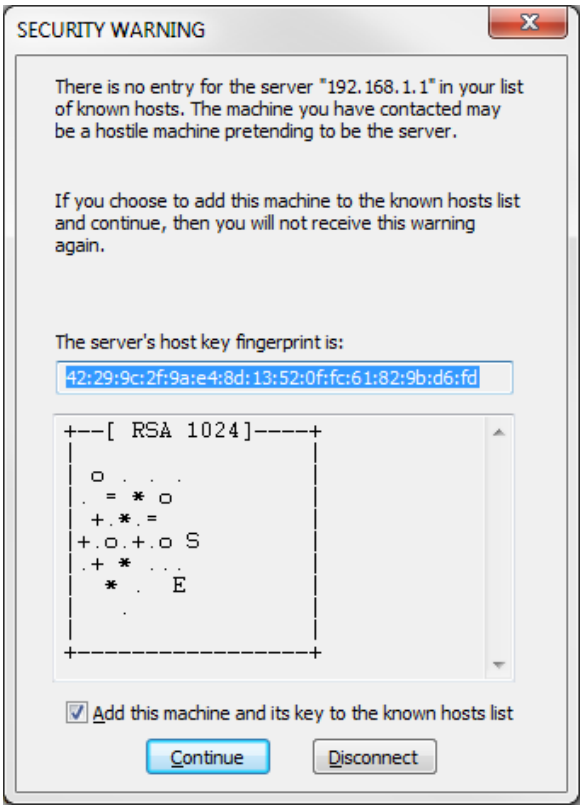
Étape 2: Démarrez une session SSH sur le routeur.

a. Ouvrez Tera Term et saisissez l'adresse IP de l'interface G0/1 de R1 dans le champ Host (Hôte) de la fenêtre New Connection (Nouvelle connexion) de Tera Term. Assurez-vous que la case d'option **SSH** est sélectionnée et cliquez sur **OK** pour vous connecter au routeur.

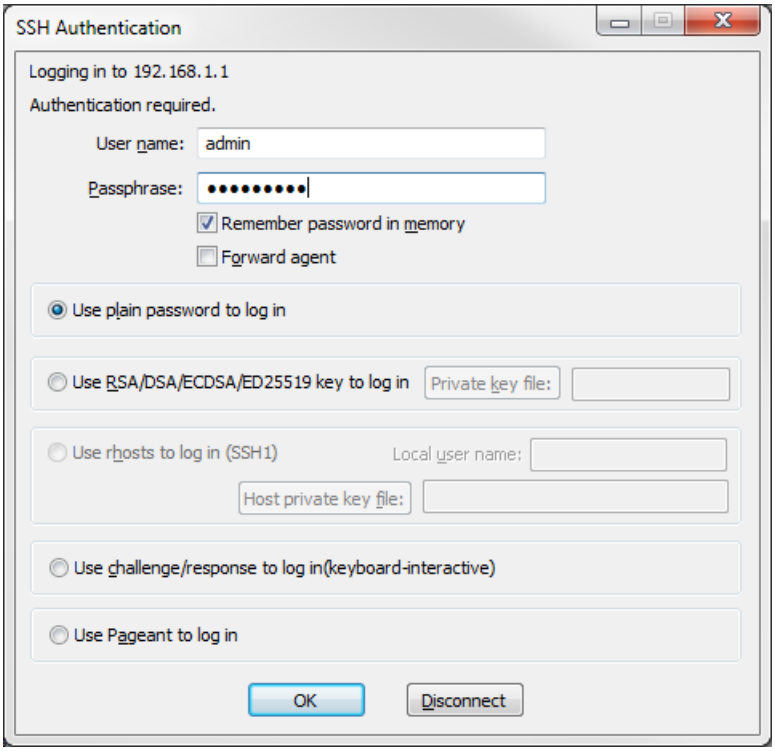


Quel est le port TCP utilisé par défaut pour les sessions SSH ?

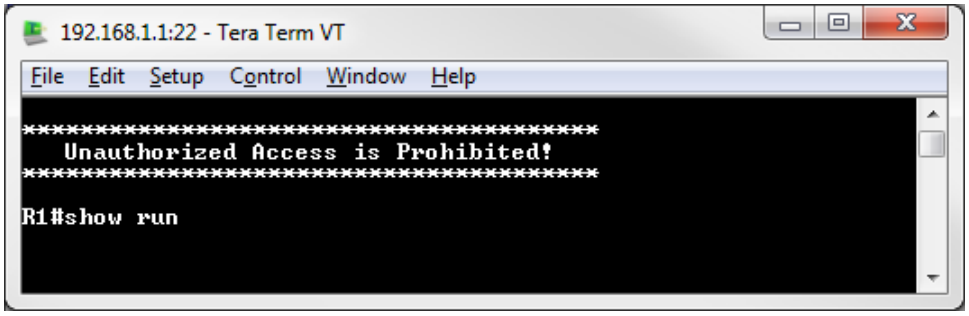
b. La première fois que vous établissez une session SSH à un périphérique, un avertissement de sécurité (**SECURITY WARNING**) vous informe que vous ne vous êtes pas encore connecté à ce périphérique. Ce message fait partie du processus d'authentification. Lisez l'avertissement de sécurité, puis cliquez sur **Continue** (Continuer).



c. Dans la fenêtre d'authentification SSH, entrez **admin** comme nom d'utilisateur et **adminpass** pour le mot de passe. Cliquez sur **OK** pour accéder au routeur.



d. Vous avez ouvert une session SSH sur le routeur. L'aspect du logiciel Tera term est très similaire à une fenêtre de commandes. À l'invite de commande, exécutez la commande **show run**.

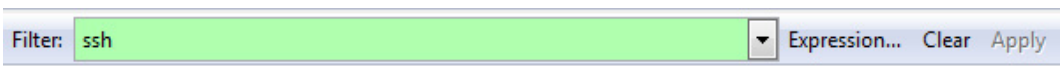


e. Quittez la session SSH en exécutant la commande **exit**.

```
R1# exit
```

Étape 3: Arrêtez la capture Wireshark.

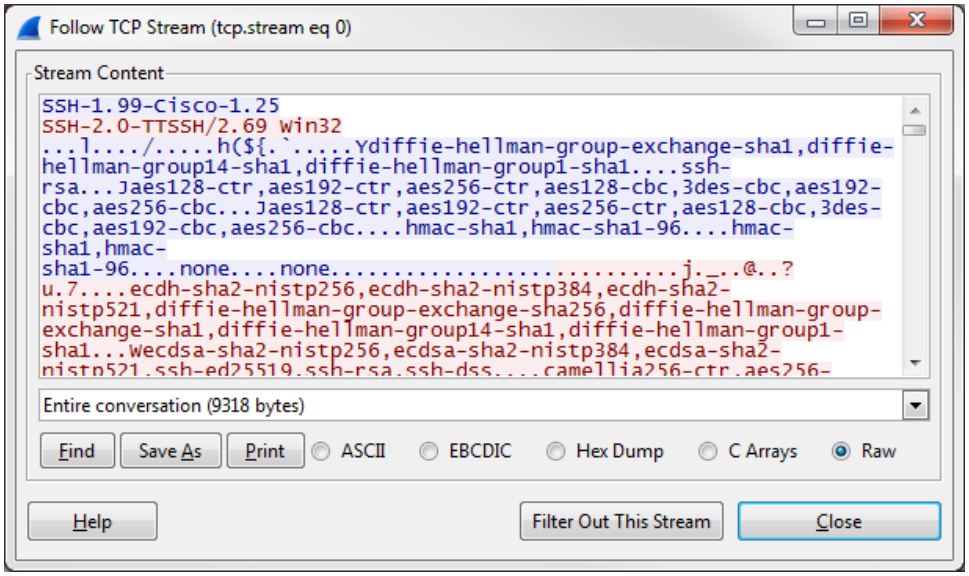
Étape 4: Appliquez un filtre SSH sur les données de capture Wireshark.



Étape 5: Utilisez la fonction Follow TCP Stream (Suivre le flux TCP) dans Wireshark pour afficher la session SSH.

a. Cliquez avec le bouton droit sur l'une des lignes **SSHv2** dans la section **Packet list** (Liste des paquets) de Wireshark et, dans la liste déroulante, sélectionnez l'option **Follow TCP Stream** (Suivre le flux TCP).

b. Examinez la fenêtre **Follow TCP Stream** (Suivre le flux TCP) de votre session SSH. Les données ont été chiffrées et sont illisibles. Comparez les données de votre session SSH aux données de votre session Telnet.



Pourquoi SSH est-il préférable à Telnet pour les connexions distantes ?

c. Après avoir examiné votre session SSH, cliquez sur **Close** (Fermer).

d. Fermez Wireshark.

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**
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 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.