Travaux pratiques – Accès aux périphériques réseau avec SSH

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	NA
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

1re partie : Configurer les paramètres de base du périphérique

2e partie : Configurer le routeur pour l'accès SSH

3e partie : Analyser une session Telnet avec Wireshark

4e partie : Analyser une session SSH avec Wireshark

5e partie : Configurer le commutateur pour l'accès SSH

6e partie : SSH à partir de l'ILC du commutateur

Contexte/scénario

Autrefois, Telnet était le protocole réseau le plus utilisé pour configurer à distance des périphériques réseau. Cependant, les protocoles tels que Telnet n'authentifient pas ou ne chiffrent 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 permet d'établir 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).

Pour que SSH fonctionne, les périphériques réseau qui communiquent doivent être configurés pour le prendre en charge. 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 où un client SSH est installé. Sur un réseau local, la connexion est normalement établie en utilisant Ethernet et IP.

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. Vous aurez également pour défi de configurer par vous-même un commutateur pour les connexions SSH.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

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 de l'interface du 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 ordinateur (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal, tel que Tera Term, et de Wireshark)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet tel qu'indiqués dans la topologie

1re partie : 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. Définissez **class** comme mot de passe chiffré d'exécution privilégié.

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

f. Définissez **cisco** comme mot de passe vty et activez la connexion.

g. Chiffrez tous 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.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Étape 5 : Vérifiez la connectivité du réseau.

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

2e partie : 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 texte 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 en partie dans la clé de chiffrement (crypto key) lorsqu'elle est générée. Par conséquent, ces noms doivent être entrés avant d'exécuter 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 adminprivilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

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#
```

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

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#
```

3e partie : Analyser une session Telnet avec Wireshark

Dans la troisième 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 un package logiciel de client Telnet/SSH n'est pas installé sur votre ordinateur, vous devez en installer un avant de continuer. Deux packages Telnet/SSH de logiciels libres sont Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) et PuTTy (www.putty.org).

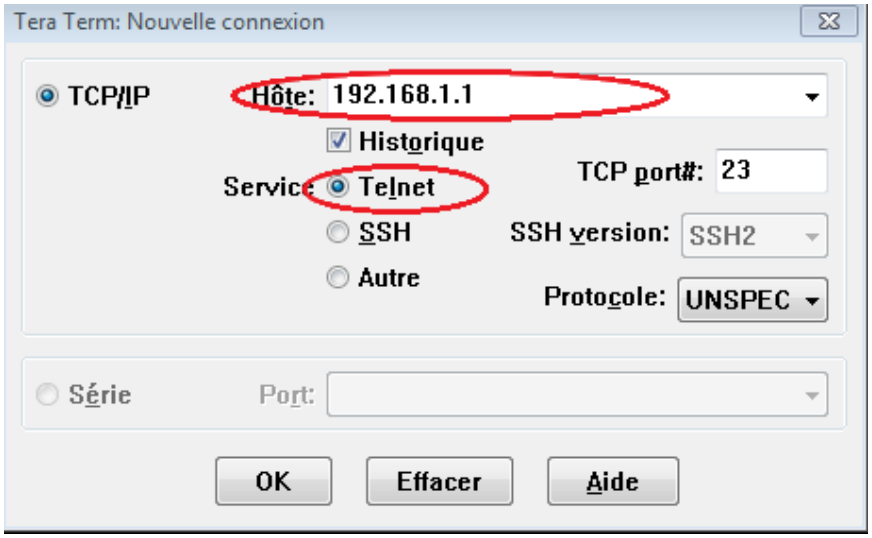
Remarque : Telnet n'est pas disponible à partir de l'invite de commandes dansWindows 7, par défaut. Pour activer Telnet afin de l'utiliser dans l'invite de commandes, cliquez sur **Démarrer** >**Panneau de configuration**>**Programmes**>**Programmes et fonctionnalités**>**Activer ou désactiver des fonctionnalités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

Étape 1 : Ouvrez Wireshark et 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.

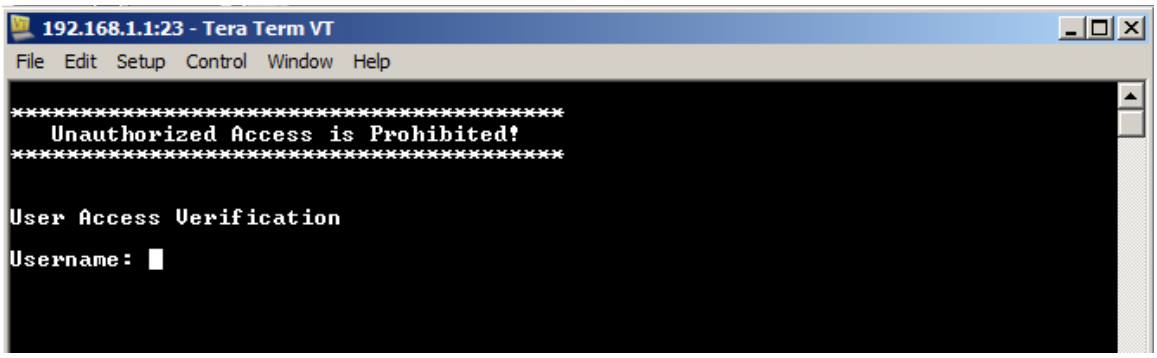
a. Ouvrez Tera Term et sélectionnez la case d'option **Service Telnet** et dans le champ Hôte, entrez **192.168.1.1**.



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**.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.



c. Saisissez la commande **show run**.

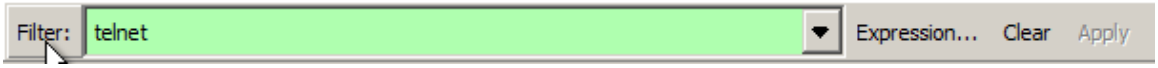
```
R1# show run
```

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

```
R1# exit
```

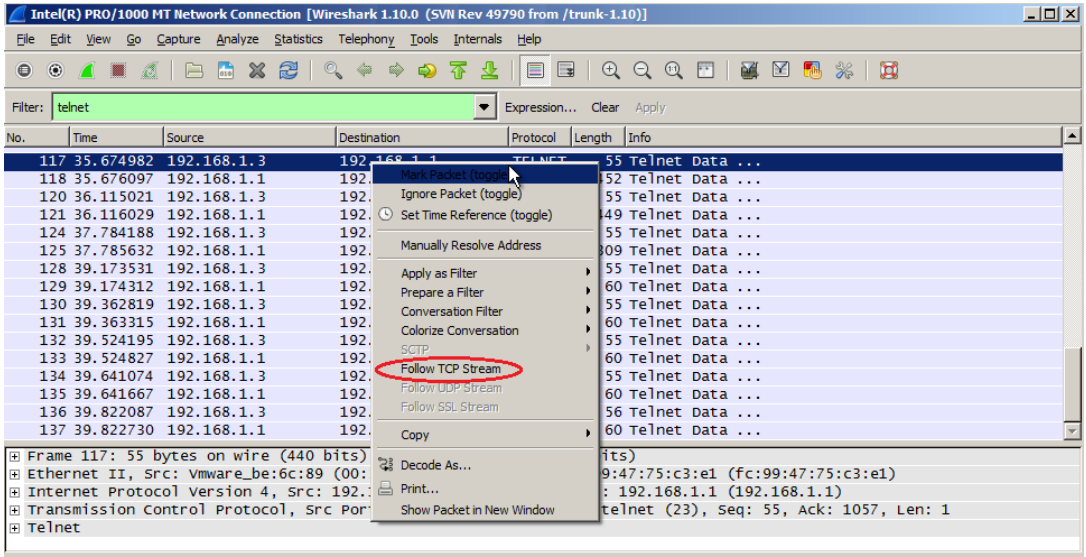
Étape 3 : Arrêtez la capture Wireshark.

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



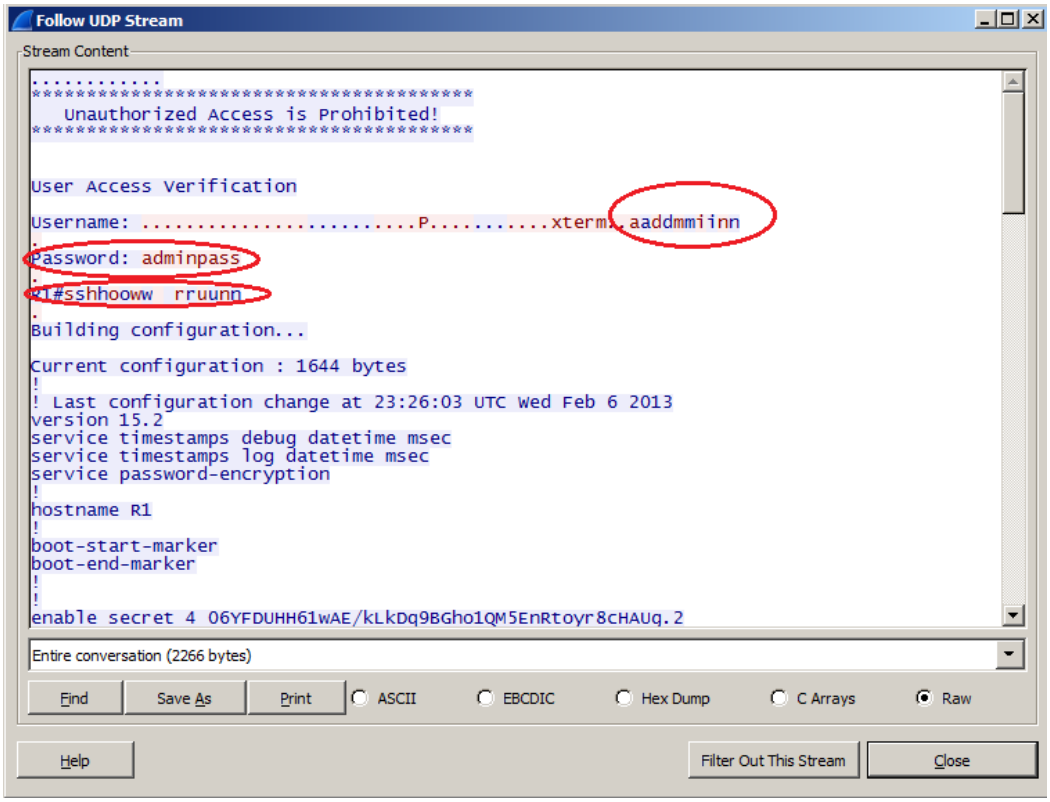
Étape 5 : Utilisez la fonction Follow TCP Stream dans Wireshark pour afficher la session Telnet.

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 **Follow TCP stream (Suivre le flux TCP)**.



© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

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 texte 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)**.

4e partie : Analyser une session SSH avec Wireshark

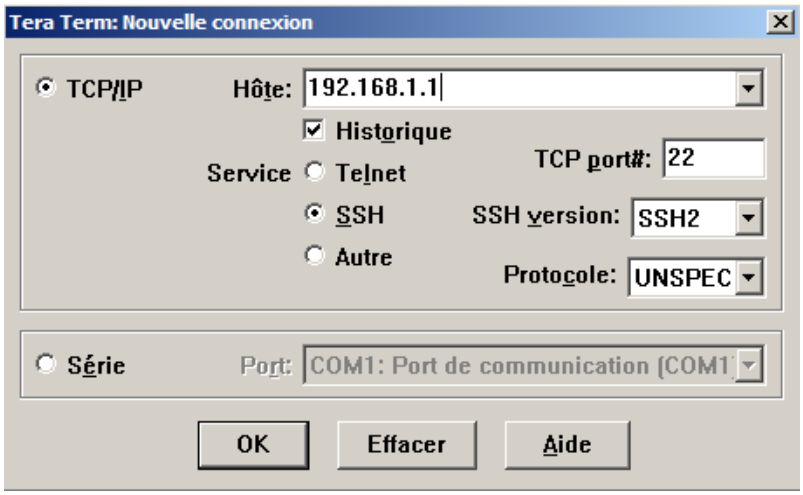
Dans la quatrième partie, vous allez utiliser le logiciel Tera term pour établir une session SSH avec le routeur. Wireshark permet de capturer et d'afficher les données de cette session SSH.

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

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

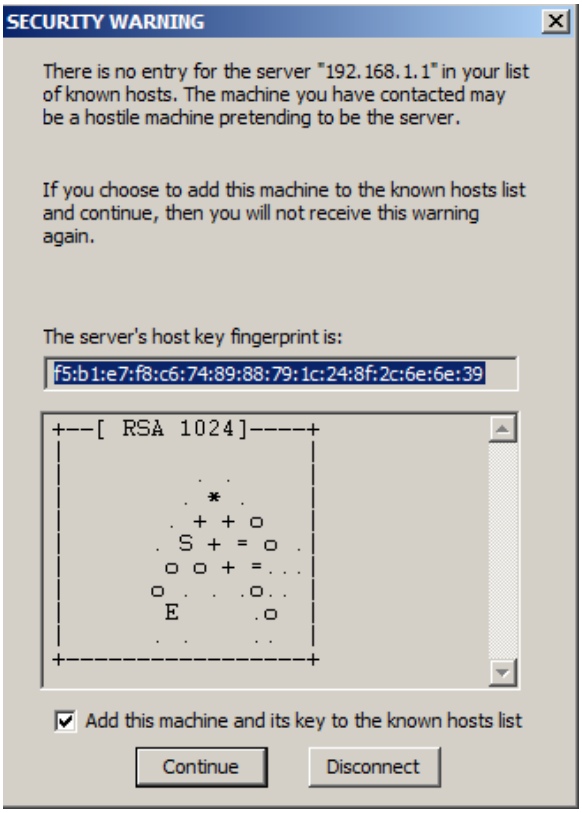
Étape 2 : Démarrez une session SSH sur le routeur.

a. Ouvrez Tera Term et entrez l'adresse IP de l'interface G0/1 de R1 dans le champ Hôte: de la fenêtre Tera Term: Nouvelle connexion. Vérifiez que la case d'option **SSH** est sélectionnée, puis cliquez sur **OK** pour vous connecter au routeur.



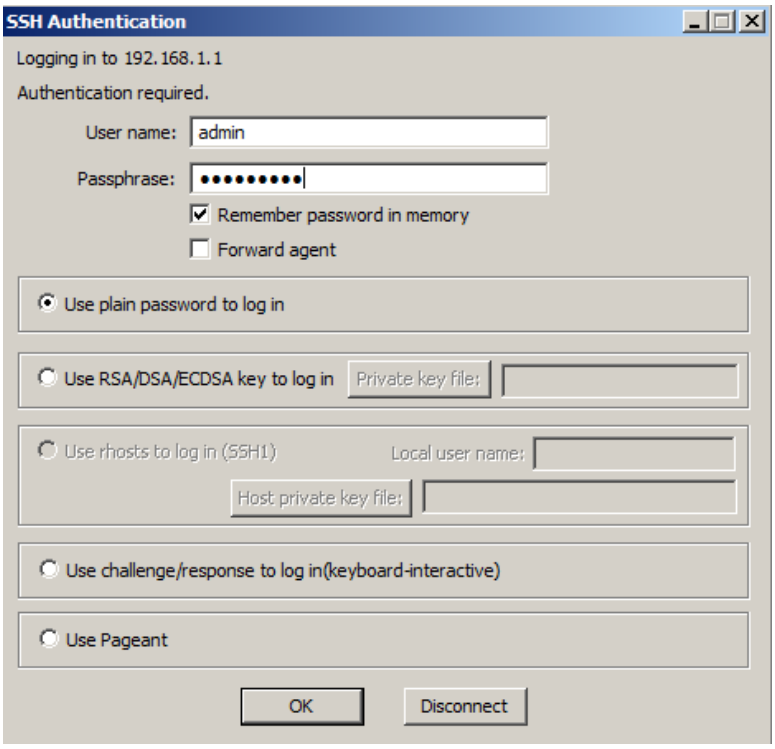
Quel est le port TCP par défaut pour les sessions SSH ?

b. La première fois que vous avez établi une session SSH à un périphérique, un avertissement de sécurité **(SECURITY WARNING)** vous informe que vous 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.**

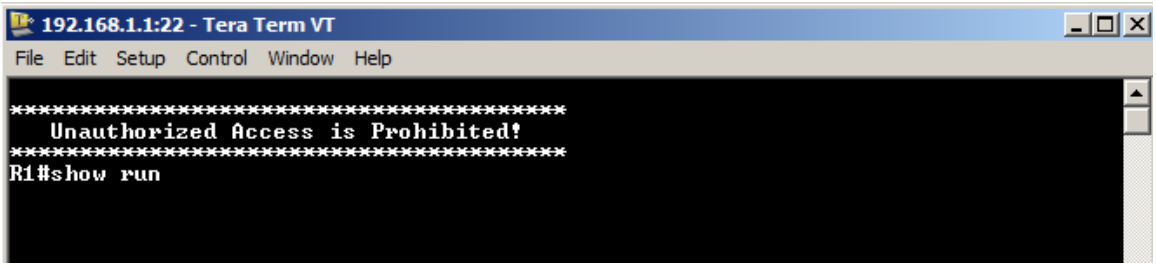


© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

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 commandes, exécutez la commande **show run**.



e. Quittez la session SSH et sortez de Tera Term en tapant la commande **exit**.

```
R1# exit
```

Étape 3 : Arrêtez la capture Wireshark.

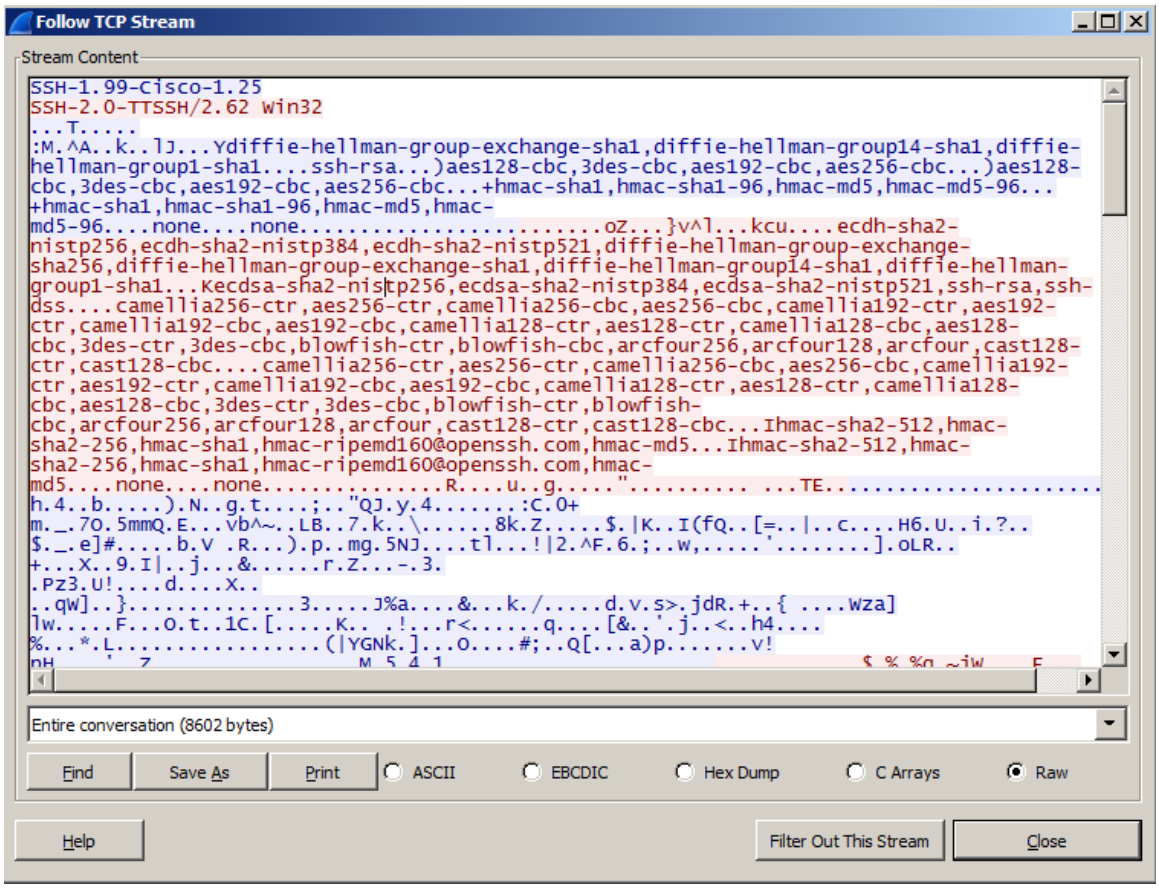
Étape 4 : Appliquez un filtre SSH sur les données de capture Wireshark.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Étape 5 : Utilisez la fonction Follow TCP Stream dans Wireshark pour afficher la session Telnet.

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.

5e partie : Configurer le commutateur pour l'accès SSH

Dans la cinquième partie, vous devez configurer le commutateur dans la topologie pour accepter les connexions SSH. Une fois que le commutateur a été configuré, ouvrez une session SSH sur celui-ci au moyen de Tera term.

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

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.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Étape 3 : Créez une connexion SSH au commutateur.

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

Étape 4 : Le cas échéant, procédez à un dépannage.

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

6e partie : SSH à partir de l'ILC du commutateur

Le client SSH est intégré au logiciel Cisco IOS et peut être exécuté à partir de l'interface en ligne de commande (ILC). Dans la sixième partie, vous établirez une connexion SSH au routeur à partir de l'ILC 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 **–ladmin** 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 d'exécution privilégiée du commutateur devrait s'afficher.

```
R1#
S1#
```

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

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


R1#
```

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

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'ILC ?

Remarques générales

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

Tableau récapitulatif de l'interface du routeur

Récapitulatif de l'interface du routeur				
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 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.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.