


Travaux pratiques 8.3.3b Configuration d'un routeur distant avec SSH



Câble direct	—————
Câble série	———  ———
Câble console (à paires inversées)
Câble de croisement	- - - - -

Objectifs

- Utiliser SDM pour configurer un routeur à accepter les connexions SSH
- Configurer le logiciel client SSH sur un PC
- Établir une connexion avec un routeur à services intégrés Cisco à l'aide de SSH version 2
- Vérifier la configuration en cours existante
- Configurer un routeur non SDM pour SSH à l'aide de l'interface de ligne de commande Cisco IOS

Contexte / Préparation

Autrefois, le protocole de réseau le plus utilisé pour configurer à distance des périphériques de réseau était Telnet. Cependant, les protocoles tels que Telnet ne permettent pas d'authentification ou de chiffrement des informations entre client et serveur. Un analyseur de réseau peut donc intercepter des mots de passe et des informations 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 de 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 ou SCP.

Pour que SSH fonctionne, les périphériques réseau qui communiquent doivent le prendre en charge. Au cours de ces travaux pratiques, vous activez le serveur SSH sur un routeur à configurer et vous vous connectez à ce routeur à l'aide d'un PC où le client SSH est installé. Sur un réseau local, la connexion est normalement établie en utilisant Ethernet et IP. Les périphériques réseau connectés via d'autres types de liaisons, comme une liaison série, peuvent également être gérés à l'aide de SSH à condition de prendre en charge IP. Comme Telnet, SSH est un protocole Internet intrabande basé sur TCP/IP.

Vous pouvez utiliser Cisco SDM ou les commandes ILC de Cisco IOS pour configurer SSH sur le routeur. Le routeur à services intégrés Cisco 1841 accepte les versions SSH 1 et 2 ; la version 2 est préférable. Le client SSH utilisé pour les besoins de ces travaux pratiques, PuTTY, peut être téléchargé gratuitement. Si vous utilisez un routeur où SDM n'est pas installé, utilisez les commandes ILC de Cisco IOS pour configurer SSH. Des instructions sont fournies à l'étape 2 de ces travaux pratiques. Pour effectuer la configuration de base du routeur, reportez-vous aux 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 ».

Cisco SDM est pris en charge sur un grand nombre de routeurs Cisco et de versions du logiciel Cisco IOS. SDM est préinstallé sur de nombreux routeurs Cisco récents. Ces travaux pratiques utilisent un routeur Cisco 1841, avec SDM (et SDM Express) préinstallé. Vous pouvez utiliser un modèle de routeur qui prend en charge SDM. Si SDM n'est pas installé sur ce routeur, vous pouvez télécharger gratuitement la version la plus récente à l'adresse suivante : <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm>. À partir de cette page Web, vous pouvez aussi afficher ou télécharger le document « Downloading and Installing Cisco Router and Security Device Manager ». Ce document indique la configuration système requise et fournit des instructions pour l'installation de SDM.

Remarque : si vous utilisez SDM pour configurer SSH, vous devez effectuer les Travaux pratiques 5.2.3, « Configuration d'un routeur à services intégrés avec SDM Express » sur le routeur à utiliser avant de passer à ces travaux pratiques. Il est supposé dans ces travaux pratiques que le routeur a été précédemment configuré avec des paramètres de base.

Remarque : si la configuration initiale (startup-config) est effacée sur un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut au redémarrage du routeur. Dans ce cas, il est nécessaire de définir une configuration de routeur de base à l'aide des commandes Cisco IOS. Reportez-vous à la procédure qui se trouve à la fin de ces travaux pratiques ou renseignez-vous auprès de votre formateur.

Ressources requises

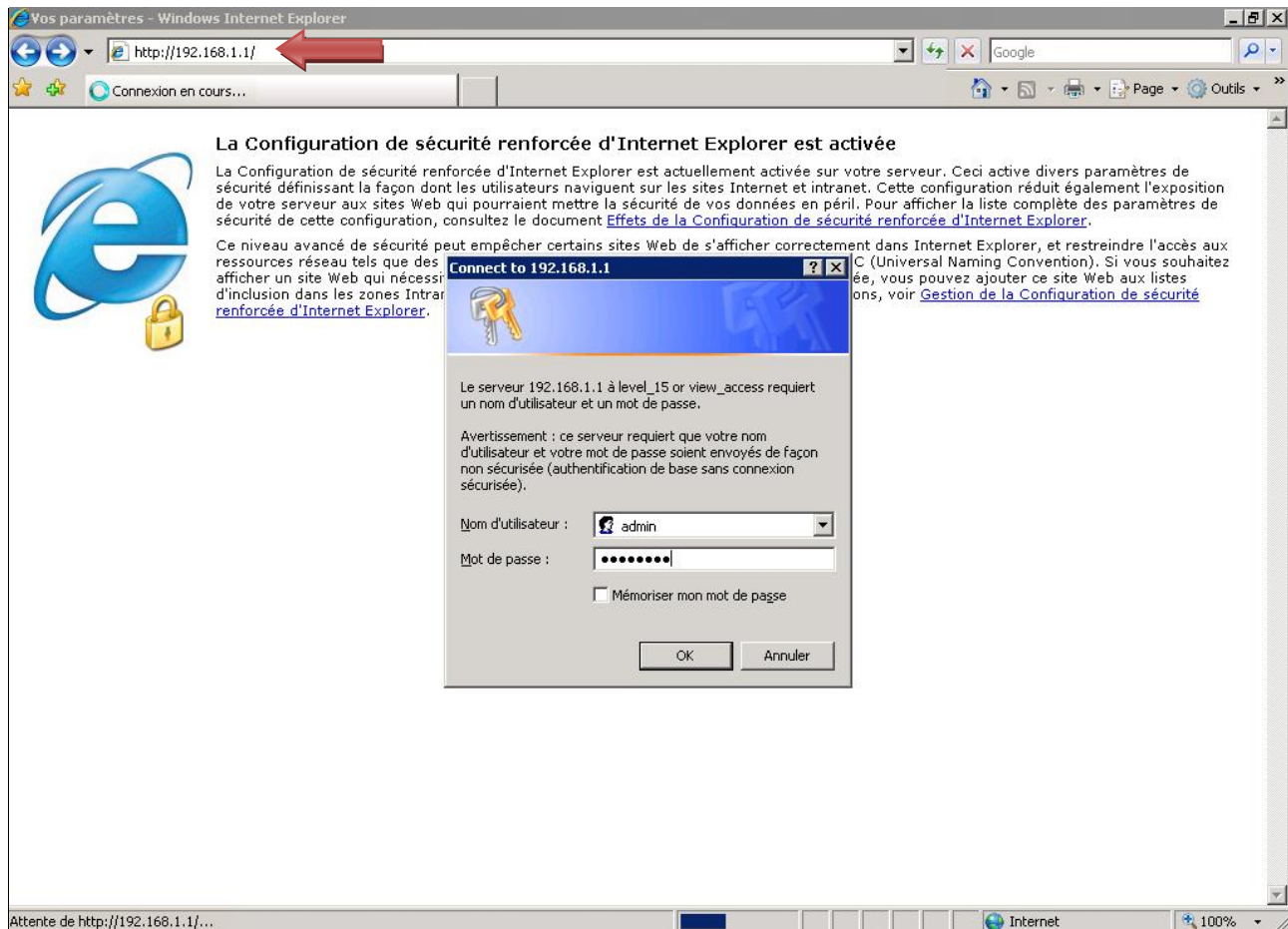
Ressources nécessaires :

- Routeur à services intégrés Cisco 1841 avec SDM version 2.4 installé et configuration de base effectuée
- (Facultatif) Autre modèle de routeur Cisco avec SDM installé
- (Facultatif) Autre modèle de routeur Cisco sans installation de SDM (Cisco IOS version 12.2 ou ultérieure : doit prendre en charge SSH)
- Ordinateur Windows XP avec Internet Explorer 5.5 ou version ultérieure et SUN Java Runtime Environment (JRE) version 1.4.2_05 ou ultérieure (ou Java Virtual Machine (JVM) 5.0.0.3810)
- Dernière version du client putty.exe installée sur le PC et accessible sur le bureau
- Câble Ethernet droit ou croisé de catégorie 5 (pour SDM et SSH)
- (Facultatif) Câble console, si le routeur doit être configuré à l'aide de l'ILC
- Accès à l'invite de commande du PC
- Accès à la configuration réseau TCP/IP du PC

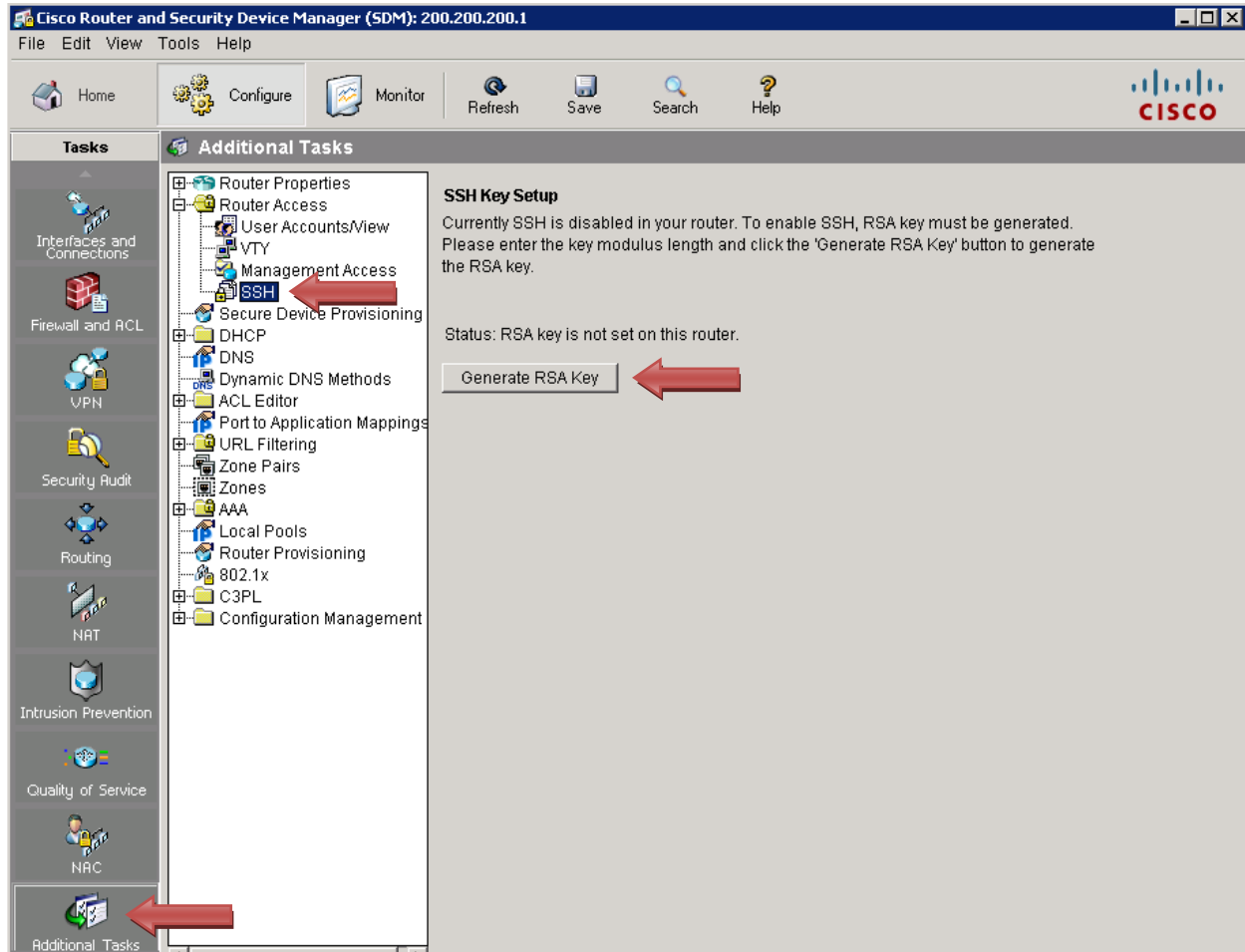
Étape 1 : utilisation de SDM pour configurer le routeur à accepter les connexions SSH

Remarque : si vous configurez un routeur sur lequel SDM n'est pas installé, lisez les instructions de l'étape 1 pour voir comment SSH est configuré en tant que tâche séparée lorsque vous utilisez SDM, et passez à l'étape 2.

- a. Connectez-vous à l'interface Fa0/0 du routeur. Ouvrez le navigateur Web et connectez-vous à `http://192.168.1.1`. Lorsqu'un message vous y invite, entrez **admin** comme nom d'utilisateur et **cisco123** comme mot de passe. Cliquez sur **OK**. Cisco SDM se charge.

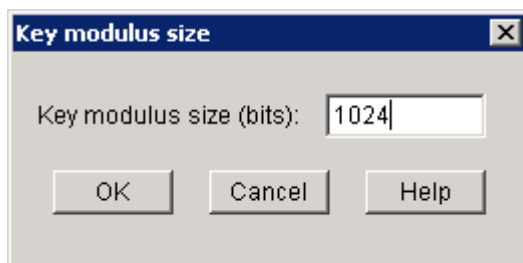


- b. Cliquez sur le bouton **Configure** de la barre d'outils. Dans le volet des tâches (Tasks), cliquez sur **Additional Tasks**. Dans le volet Additional Tasks, développez **Router Access**, puis cliquez sur la tâche **SSH**. Cliquez ensuite sur le bouton **Generate RSA Key**.

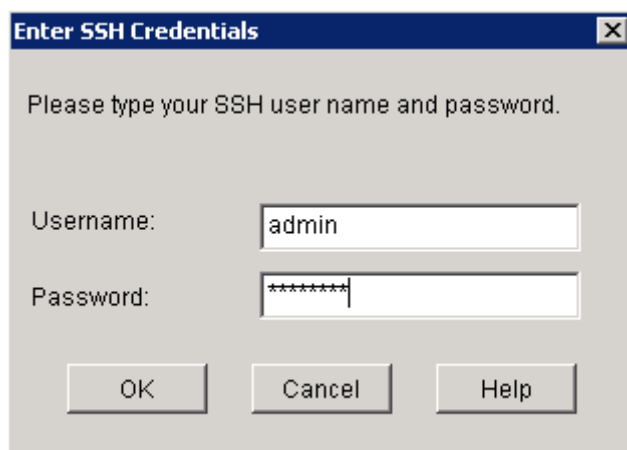


Remarque : si le message **SSH Key Setup** indique « RSA key exists and SSH is enabled in your router » et que **Status** est « RSA key is set on this router », c'est que vous avez effectué les Travaux pratiques 5.2.3, « Configuration d'un routeur à services intégrés avec SDM Express ». Au cours de ces travaux pratiques, lorsque vous avez configuré la sécurité, l'un des paramètres de sécurité activés par défaut était « Enhance security on this router ». Si cette case est cochée, SSH est automatiquement configuré pour l'accès au routeur, la bannière d'avertissement de la présence d'intrus est affichée, une longueur minimum de mot de passe est imposée et le nombre de tentatives de connexion infructueuses est limité.

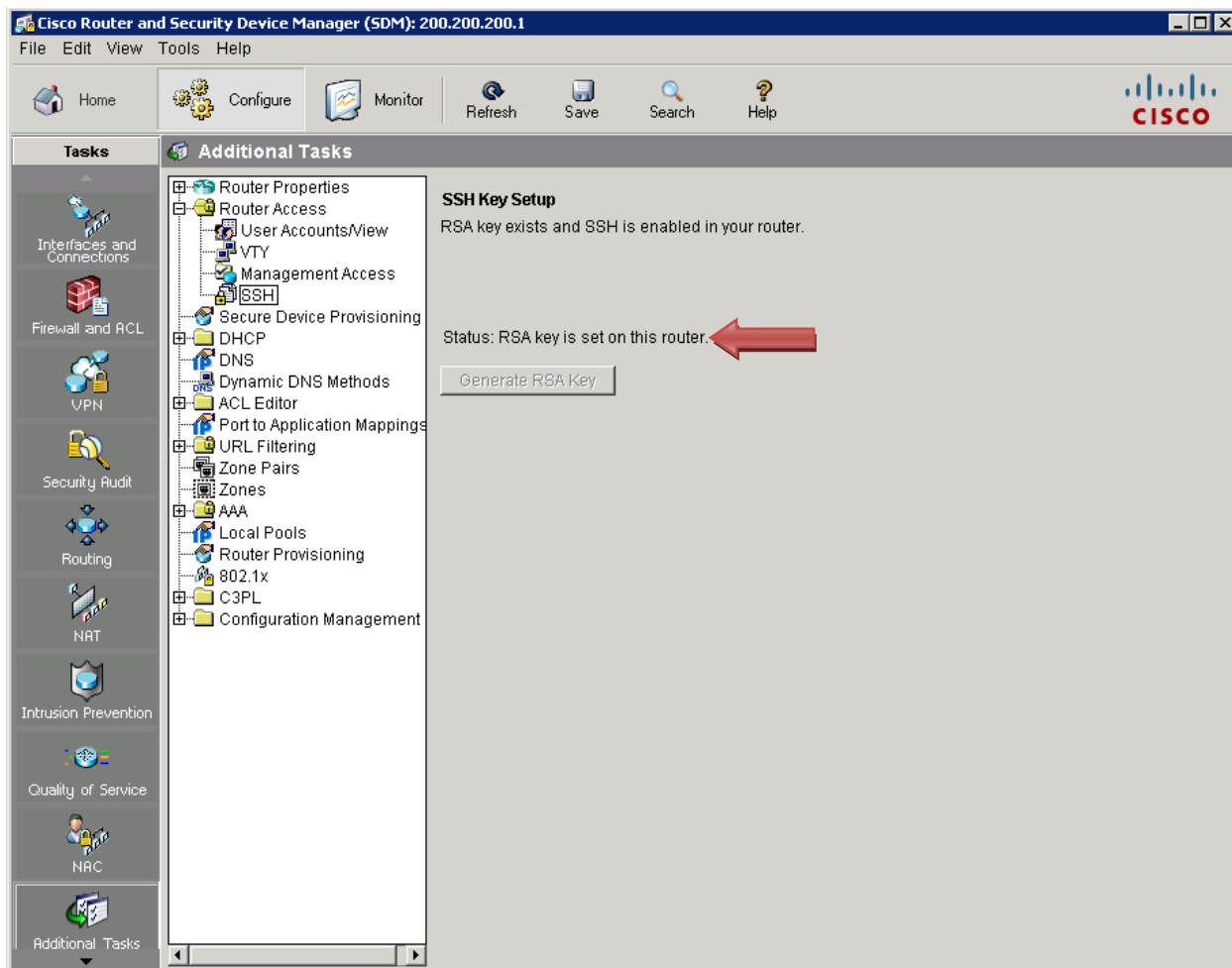
- c. Dans la boîte de dialogue **Key modulus size**, entrez une taille de clé de **1024** bits. Cliquez sur **OK**.



- d. Dans la boîte de dialogue **Enter SSH Credentials**, entrez **admin** comme nom d'utilisateur et **cisco123** comme mot de passe. Cliquez sur **OK**.



- e. Notez que la clé RSA est à présent définie sur le routeur.

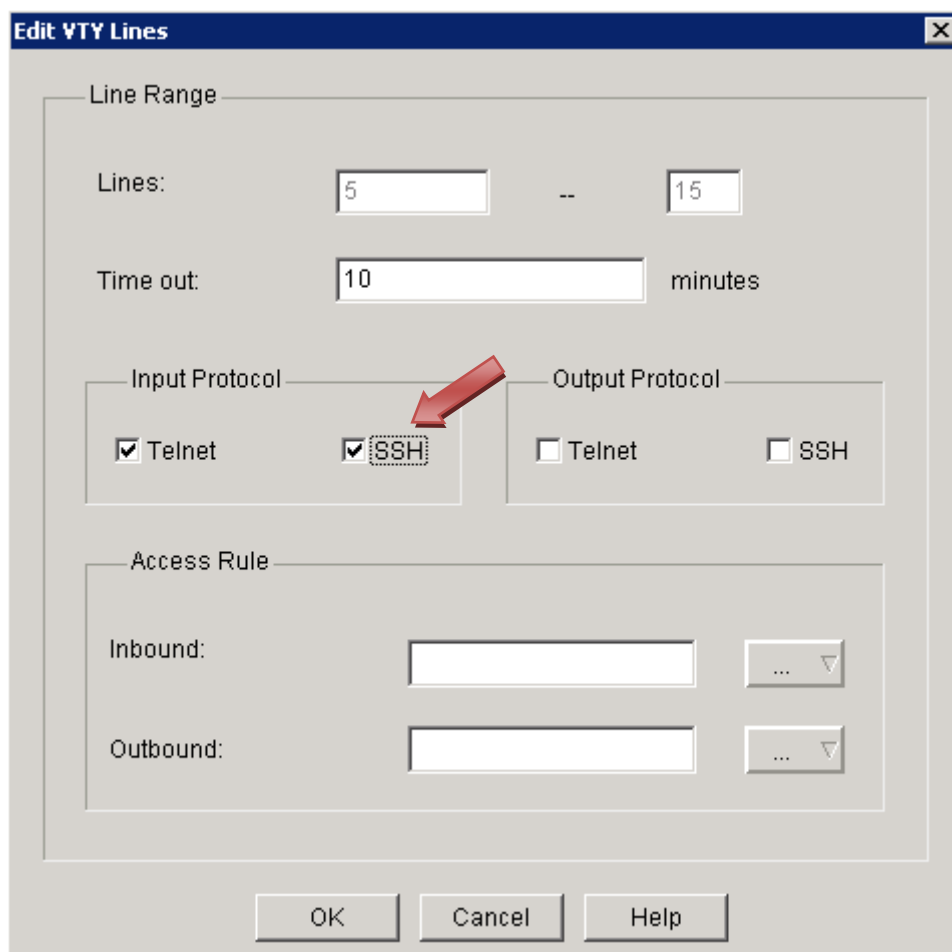


- f. Dans le volet Additional Tasks, cliquez sur l'option **VTY**. Sélectionnez **Input Protocols Allowed**, puis cliquez sur le bouton **Edit**.

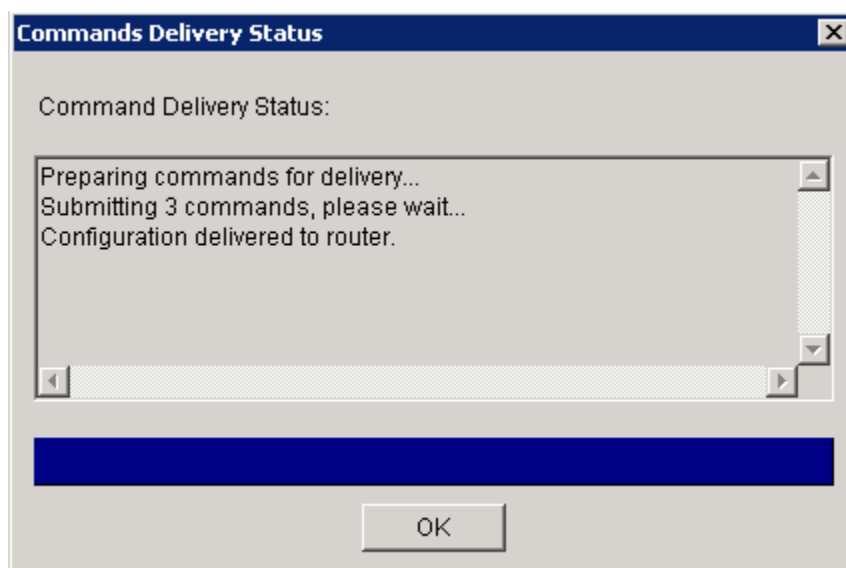
The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The left pane displays the 'Additional Tasks' tree, where 'VTY' is selected under 'Router Access'. The right pane shows the 'VTYs' configuration table. The table has two sections for different line ranges. The first section is for 'Line Range 0-4' and the second for 'Line Range 5-15'. The 'Input Protocols Allowed' row in the second section is highlighted. A red arrow points to the 'VTY' option in the tree, another red arrow points to the 'Input Protocols Allowed' row, and a third red arrow points to the 'Edit...' button in the top right corner.

Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None
Line Range	5-15
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None

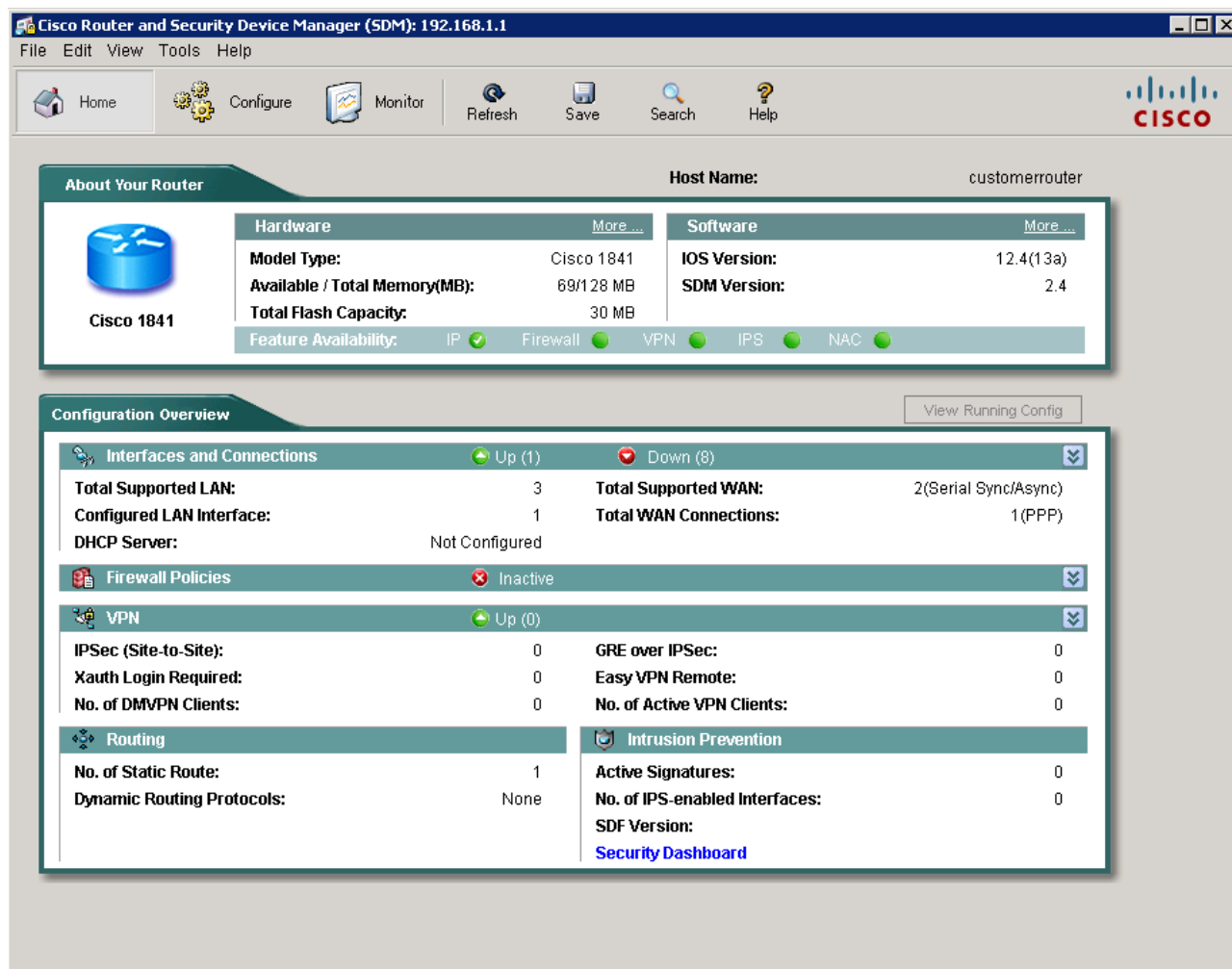
- g. Activez la case à cocher **SSH** sous **Input Protocol**, puis cliquez sur **OK**.



- h. Lorsque la fenêtre **Commands Delivery Status** s'ouvre, cliquez sur **OK**.



- i. Fermez Cisco SDM en cliquant sur **X** (Fermer) dans l'angle supérieur droit de la fenêtre.



- j. Cliquez sur **Yes** pour confirmer la fermeture de SDM et passez à l'étape 3. (L'étape 2 montre comment configurer le protocole SSH sur un routeur non SDM).

Étape 2 : (facultative) configuration de SSH sur un routeur non SDM

Remarque : si vous configurez SSH sur un routeur où SDM est déjà installé, vous pouvez sauter l'étape 2 et passer directement à l'étape 3.

- a. Connectez le port console du routeur à un PC et au programme HyperTerminal, comme décrit dans les Travaux pratiques 5.1.3, « Mise en marche d'un routeur à services intégrés ».
- b. Connectez-vous au routeur. À l'invite du mode d'exécution privilégié, entrez les commandes ILC de Cisco IOS comme illustré ci-dessous. Ces commandes n'incluent pas tous les mots de passe qui doivent être définis. Reportez-vous aux 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 » pour plus d'informations sur les paramètres de configuration.

Remarque : le routeur doit disposer de la version 12.2 ou ultérieure du logiciel Cisco IOS. Dans cet exemple, le routeur est un modèle Cisco 2620XM avec Cisco IOS 12.2(7r).

- c. Configurez les informations de base du routeur et de l'interface.

```
Router#config terminal
Router(config)#hostname CustomerRouter
CustomerRouter(config)#ip domain-name customer.com
CustomerRouter(config)#username admin privilege 15 password 0 cisco123
CustomerRouter(config)#interface FastEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
```

- d. Configurez les lignes de terminal vty entrantes afin d'accepter Telnet et SSH.

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

- e. 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 module. La valeur par défaut est de 512.

```
CustomerRouter(config)#crypto key generate rsa
```

```
How many bits in the modulus [512] 768
```

```
CustomerRouter(config)#exit
```

- f. Vérifiez que SSH a bien été activé ainsi que la version qui est utilisée.

```
CustomerRouter#show ip ssh
```

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

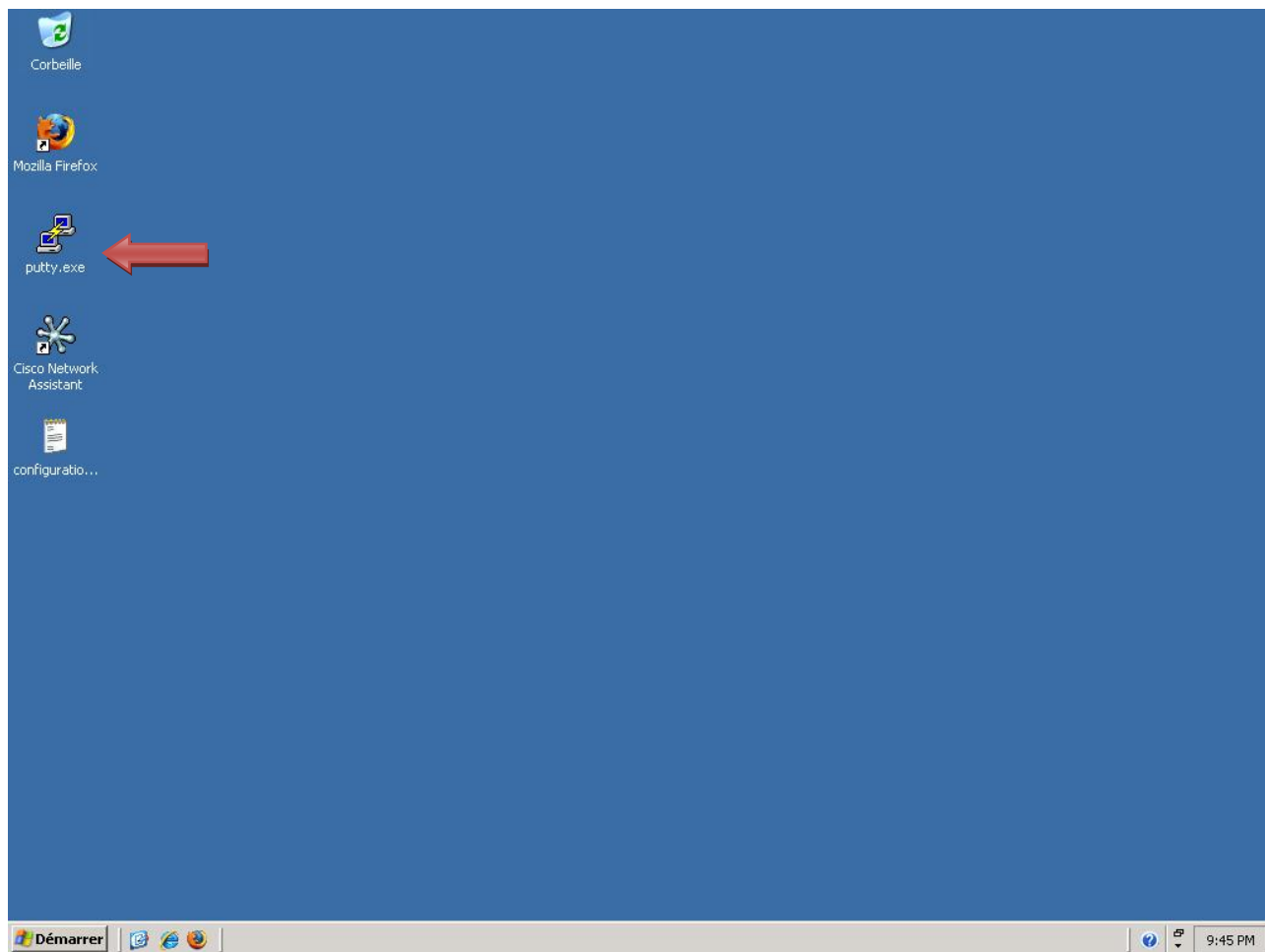
```
Version SSH activée _____
Délai d'authentification _____
Nombre de tentatives d'authentification _____
```

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

```
CustomerRouter#copy running-config startup-config
```

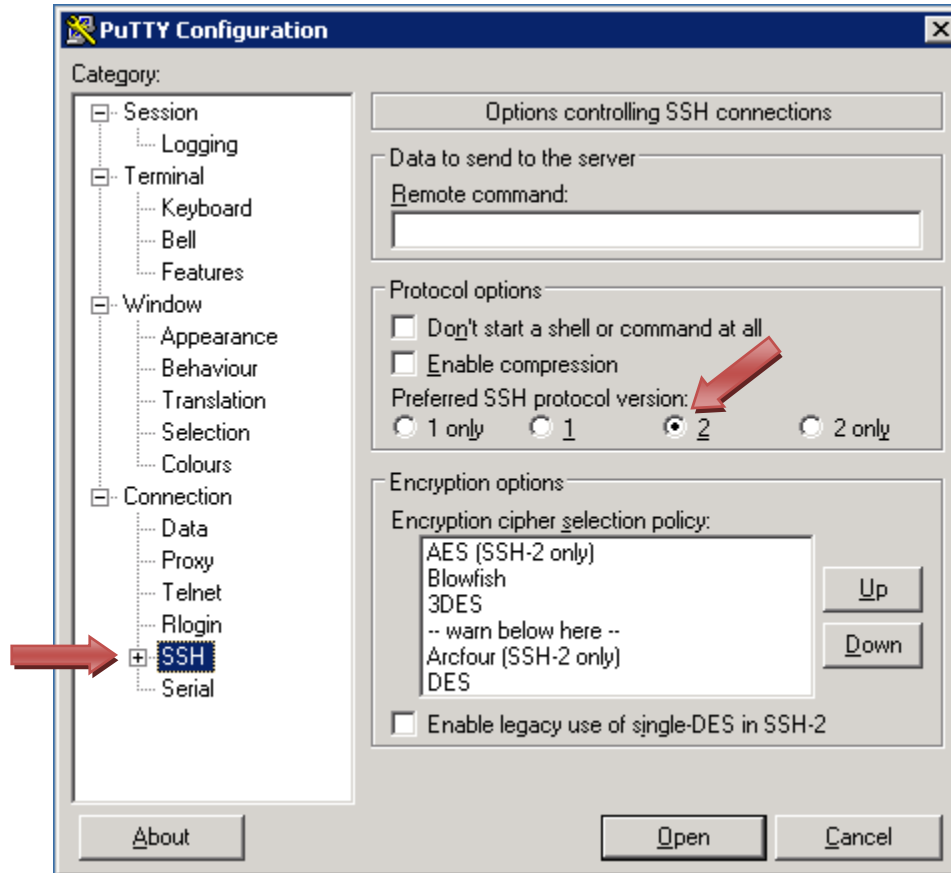
Étape 3 : configuration du client SSH et connexion du PC au routeur à services intégrés

- a. Téléchargez putty.exe et placez l'application sur le bureau. Lancez PuTTY en double-cliquant sur l'icône putty.exe.

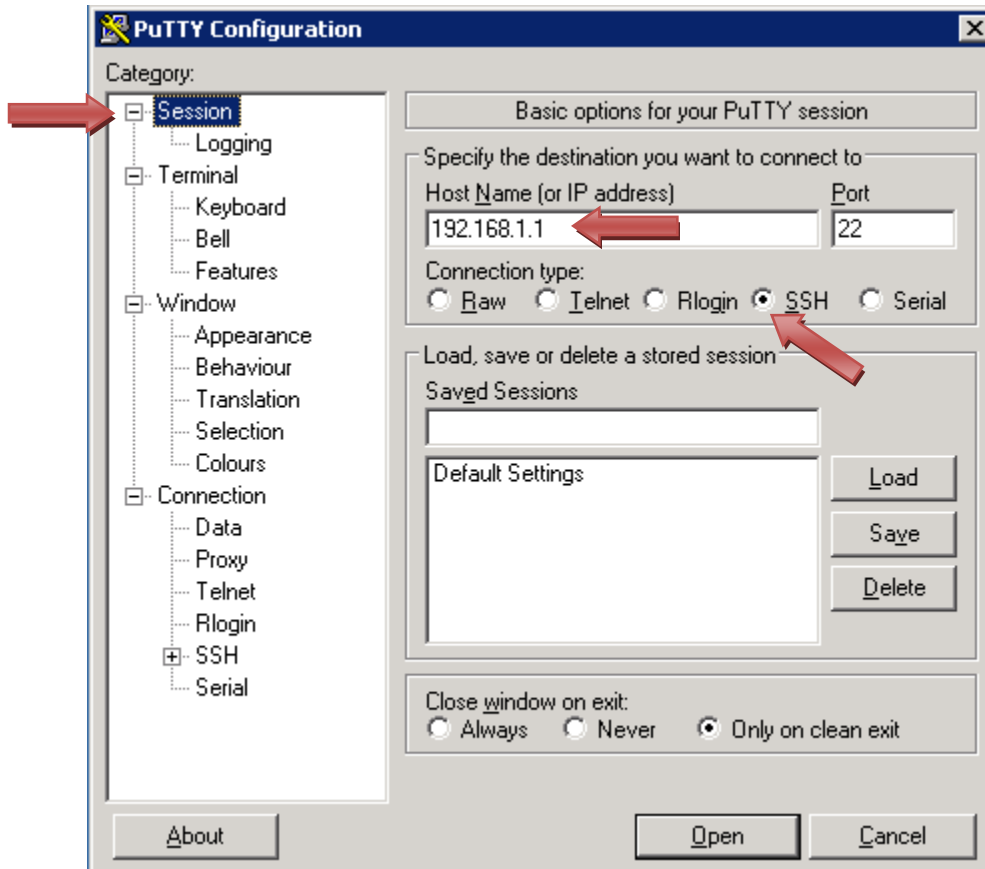


- b. Dans le volet Category, cliquez sur **SSH**. Vérifiez que la version préférée du protocole SSH est définie à 2.

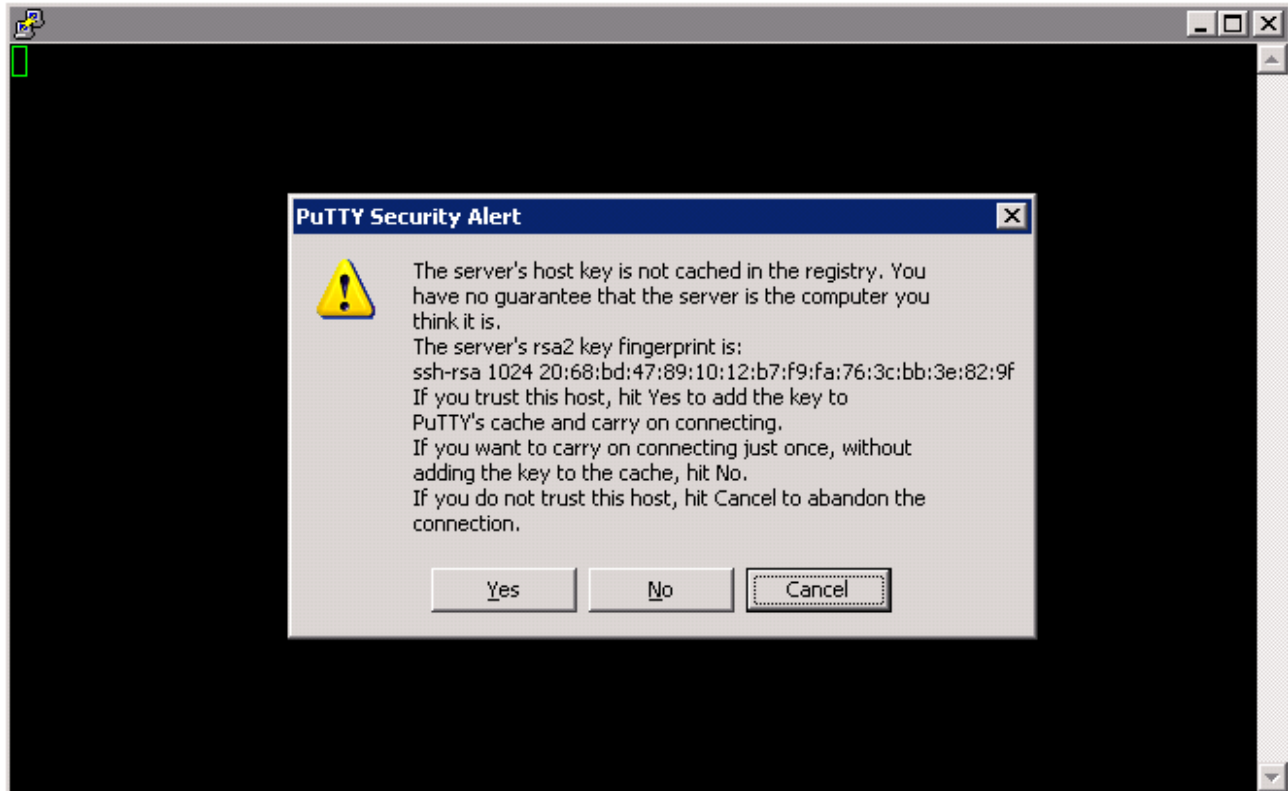
Remarque : le client Putty se connecte même si le serveur SSH exécute la version 1 de SSH.



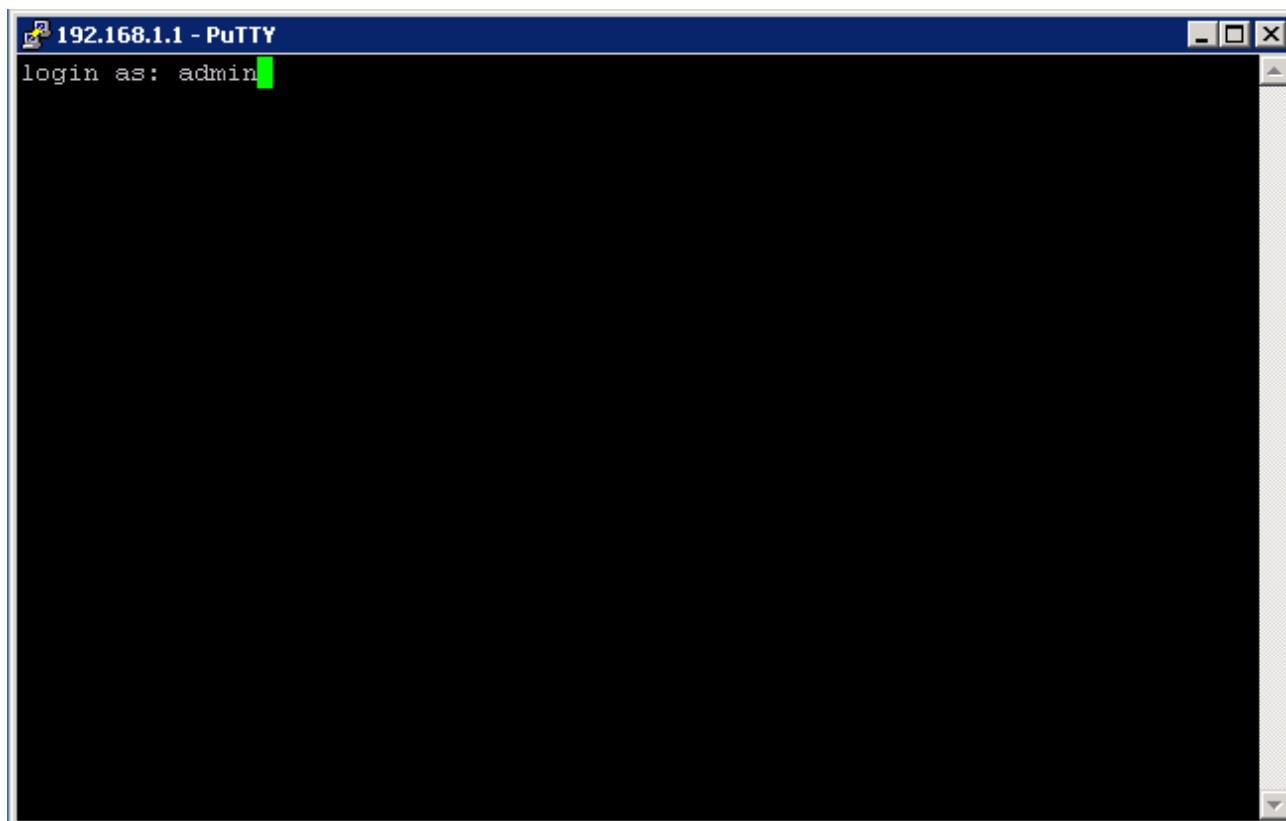
- c. Dans le volet Category, cliquez sur **Session**. Entrez l'adresse IP de l'interface de réseau local du routeur, qui est 192.168.1.1. Vérifiez que SSH est sélectionné pour le type de connexion. Cliquez sur **Open**.



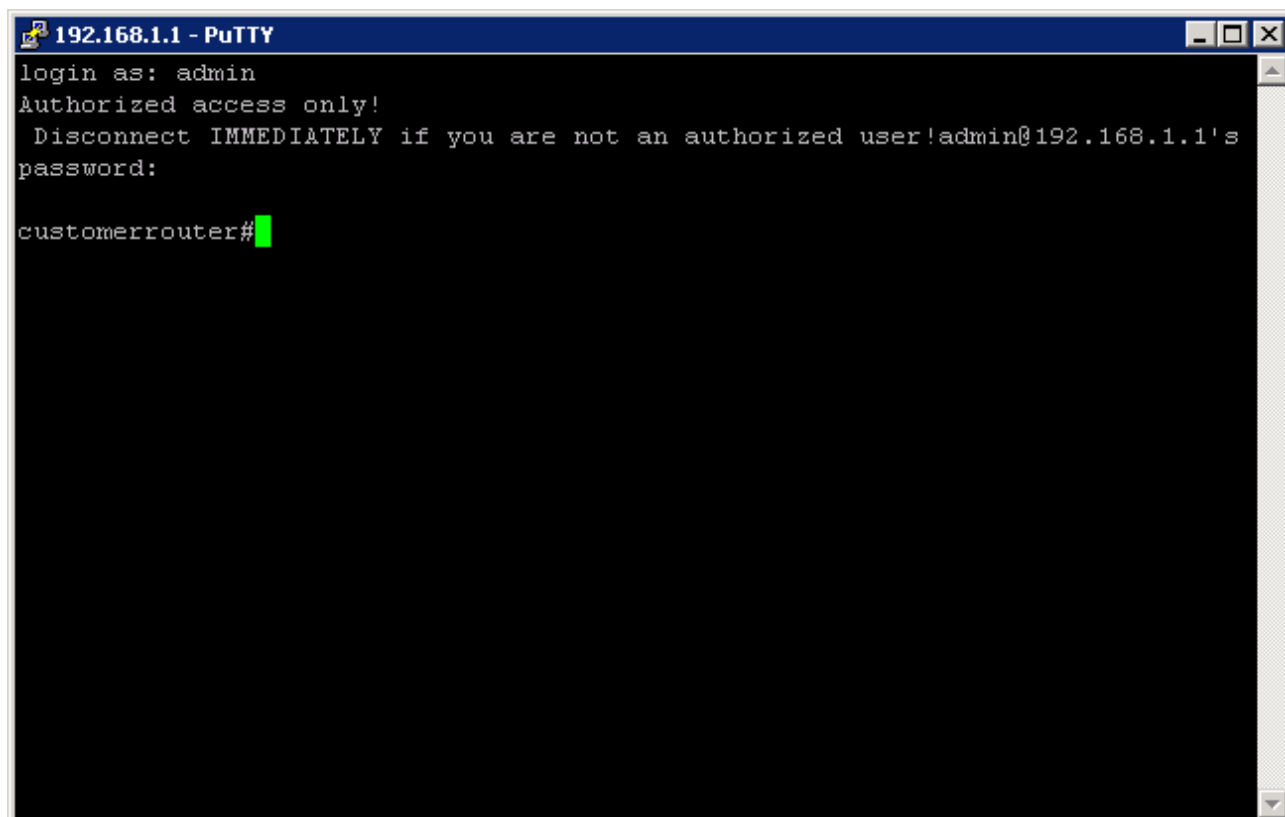
- d. La première fois que la connexion est établie avec SSH sur le routeur à services intégrés Cisco 1841 à l'aide d'un client SSH, une clé de connexion est mise en cache dans le registre de la machine locale. Dans la fenêtre PuTTY Security Alert, cliquez sur **Yes** pour continuer.



- e. À l'invite de connexion, tapez le nom d'utilisateur de l'administrateur, **admin**, puis appuyez sur **Entrée**.



- f. À l'invite du mot de passe, tapez le mot de passe de l'administrateur, **cisco123**, puis appuyez sur **Entrée**.

A screenshot of a PuTTY terminal window titled "192.168.1.1 - PuTTY". The terminal displays the following text: "login as: admin", "Authorized access only!", "Disconnect IMMEDIATELY if you are not an authorized user!admin@192.168.1.1's", "password:", and "customerrouter#" with a green cursor. The terminal has a black background and a blue title bar.

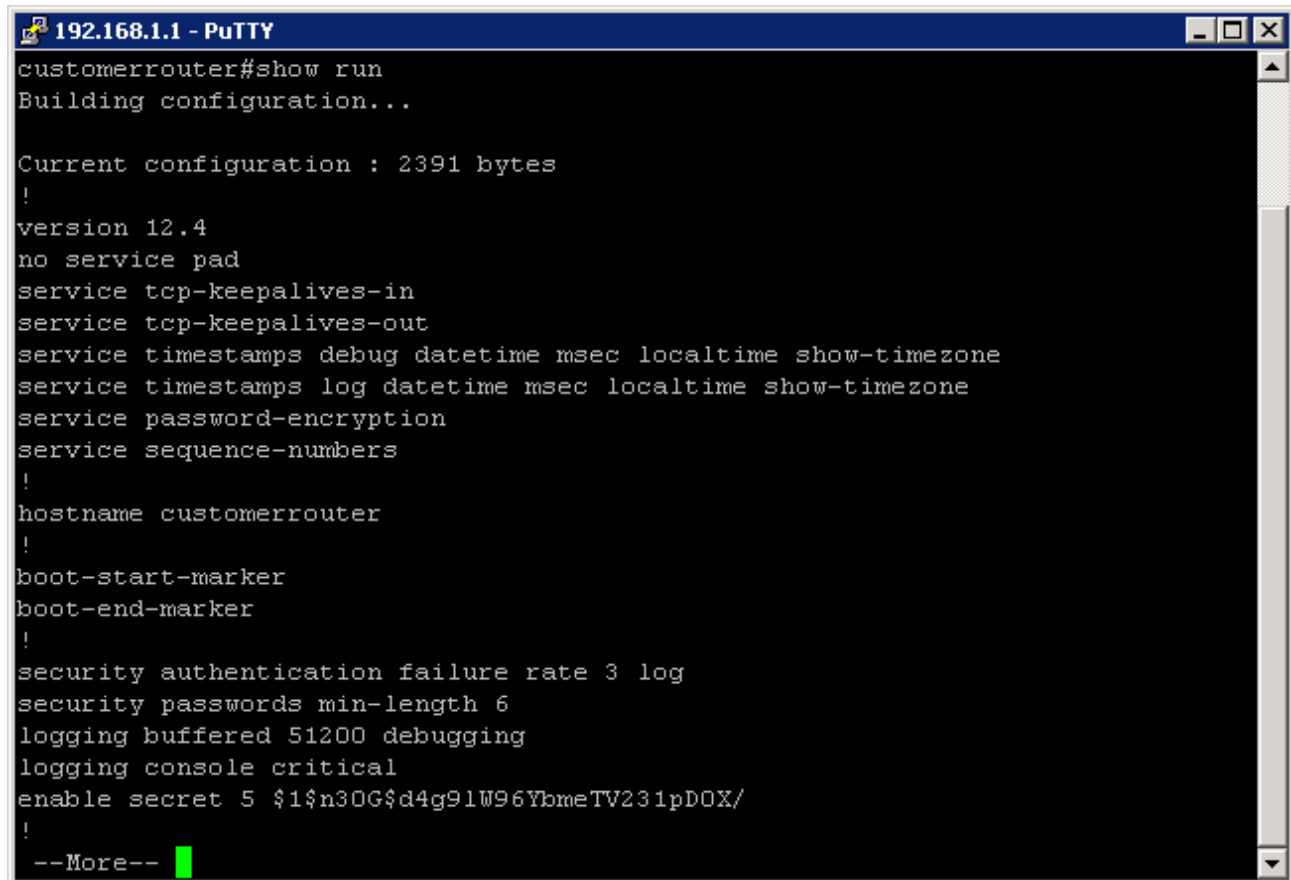
```
192.168.1.1 - PuTTY
login as: admin
Authorized access only!
Disconnect IMMEDIATELY if you are not an authorized user!admin@192.168.1.1's
password:
customerrouter#
```


Étape 4 : vérification de la configuration du routeur à services intégrés Cisco 1841

- a. Pour vérifier la configuration du routeur, tapez **show run** à l'invite du mode d'exécution privilégié, puis appuyez sur **Entrée**.

Remarque : il n'est pas nécessaire de passer du mode utilisateur au mode d'exécution privilégié si vous utilisez SDM, car c'est le mode paramétré par défaut.

- b. Appuyez sur la touche **Espace** pour faire défiler la configuration en cours du routeur.

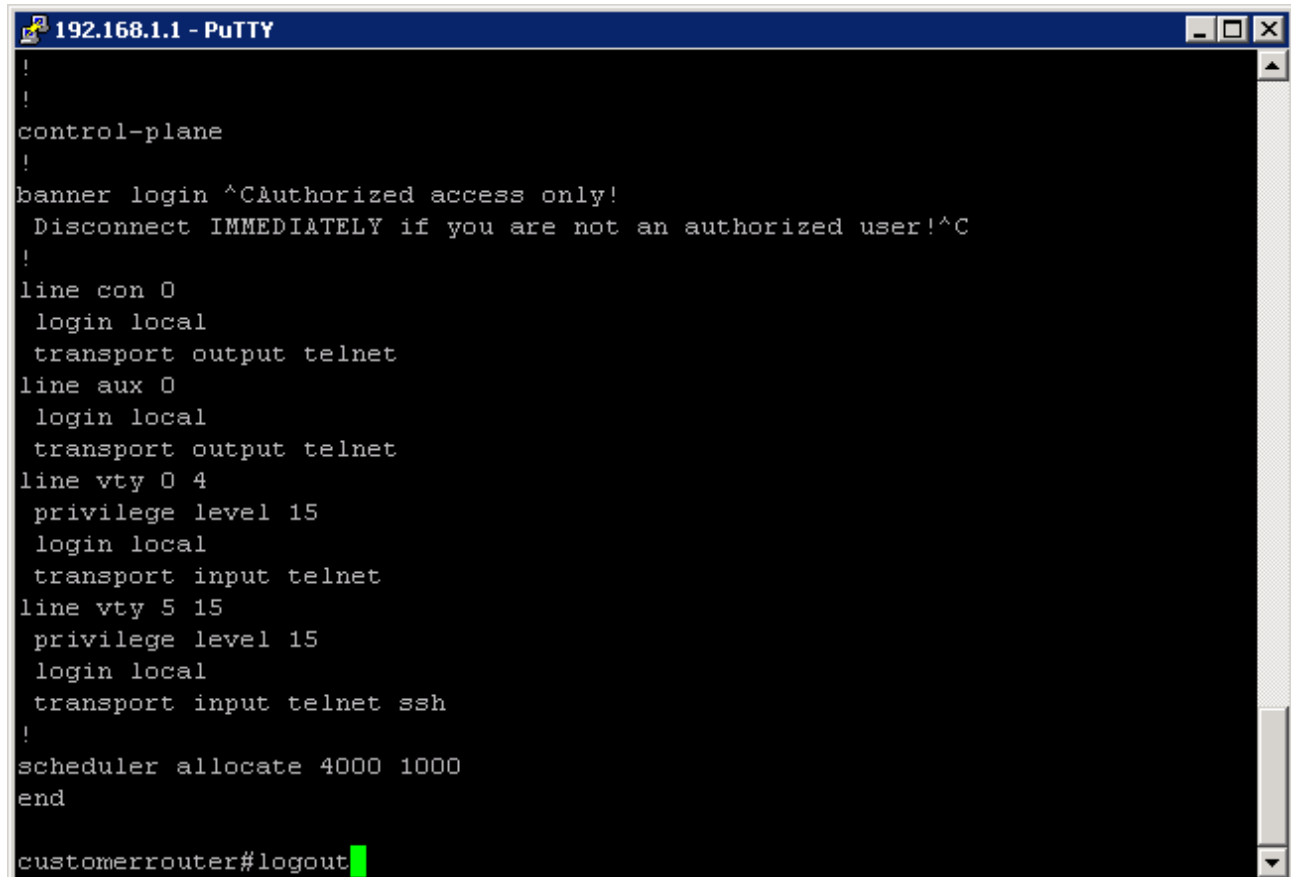


```
192.168.1.1 - PuTTY
customerrouter#show run
Building configuration...

Current configuration : 2391 bytes
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname customerrouter
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
logging console critical
enable secret 5 $1$n30G$d4g9lW96YbmeTV231pDOX/
!
--More--
```

Étape 5 : déconnexion du routeur à services intégrés Cisco 1841

Pour vous déconnecter du routeur après avoir vérifié la configuration, tapez **logout** à l'invite du mode d'exécution privilégié, puis appuyez sur **Entrée**.



```
192.168.1.1 - PuTTY
!
!
control-plane
!
banner login ^CAuthorized access only!
  Disconnect IMMEDIATELY if you are not an authorized user!^C
!
line con 0
  login local
  transport output telnet
line aux 0
  login local
  transport output telnet
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet ssh
!
scheduler allocate 4000 1000
end
customerrouter#logout
```

Étape 6 : remarques générales

- a. Quels sont les avantages et inconvénients comparés de Telnet et SSH ?

- b. Quel est le port par défaut pour SSH ? _____ Quel est le port par défaut pour Telnet ? _____

- c. Quelle version de la plateforme Cisco IOS était affichée dans la configuration en cours ?

Configuration Cisco IOS de base pour afficher SDM

Si la configuration initiale (startup-config) est effacée sur un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut au redémarrage du routeur. Vous devez créer une configuration de base comme suit. Pour plus de détails sur la configuration et l'utilisation de SDM, reportez-vous au guide de démarrage rapide du gestionnaire SDM

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

1) Définissez l'adresse IP du routeur Fa0/0. (Il s'agit de l'interface à laquelle le PC se connecte à l'aide d'un navigateur afin d'afficher SDM). L'adresse IP du PC doit être définie sur 10.10.10.2 255.255.255.248.

Remarque : un routeur SDM autre que le routeur 1841 peut nécessiter une connexion à un port différent pour accéder à SDM.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

2) Activez le serveur HTTP/HTTPS du routeur.

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

3) Créez un compte utilisateur avec un niveau de privilège défini sur 15 (activez les privilèges). Remplacez *nom d'utilisateur* et *mot de passe* par le nom d'utilisateur et le mot de passe que vous voulez configurer.

```
Router(config)# username <nom d'utilisateur> privilege 15 password 0
<mot de passe>
```

4) Configurez SSH et Telnet pour la session locale et un niveau de privilège défini sur 15.

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