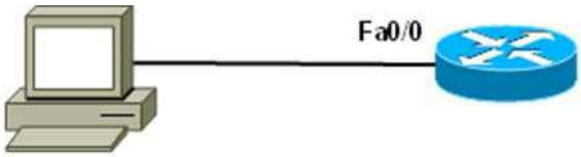
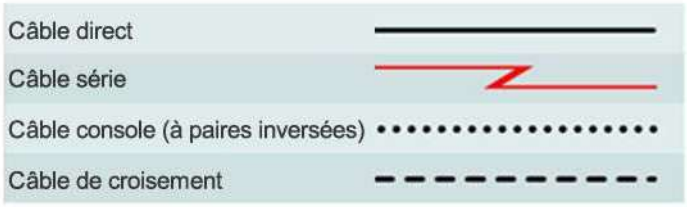
Travaux pratiques 5.5.5 Configuration d'un routeur distant avec SSH





Objectifs

Configurer un routeur pour accepter les connexions SSH

Configurer le logiciel client SSH sur un PC

Établir une connexion avec un routeur de service intégré Cisco à l'aide de SSH version 2

Vérifier la configuration en cours existante

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 un client et un serveur Telnet. Par conséquent, un analyseur de réseau peut être utilisé pour 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 allez activer le serveur SSH sur un routeur à configurer et vous vous connecterez à ce routeur à l'aide d'un PC où le client SSH est installé. Pour une utilisation 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 in band basé sur TCP/IP.

Dans le cadre de ces travaux pratiques, vous pouvez utiliser Cisco SDM ou les commandes ILC de Cisco IOS pour configurer SSH sur le routeur.

Le routeur de service intégré Cisco 1841 accepte les versions SSH 1 et 2 ; la version 2 de préférence. Le client SSH utilisé pour les besoins de ces travaux pratiques, PuTTY, peut être téléchargé gratuitement.

Il est pris en charge sur un grand nombre de routeurs Cisco et de versions de la plateforme logicielle Cisco IOS. SDM est préinstallé sur de nombreux routeurs Cisco récents. Si vous utilisez un routeur 1841, SDM (et SDM Express) y est préinstallé. Il est supposé dans ces travaux pratiques que vous utilisez le routeur Cisco 1841. Vous pouvez utiliser un autre modèle à condition qu'il soit capable de prendre en charge SDM. Si vous installez un routeur pris en charge sur lequel SDM n'est pas installé, vous pouvez télécharger la dernière version gratuitement sur le site : http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

À partir de l'adresse URL indiquée ci-dessus, affichez ou téléchargez le document « Downloading and Installing Cisco Router and Security Device Manager ». Ce document fournit des instructions pour l'installation de SDM sur votre routeur. Il indique les numéros de modèle et les versions IOS spécifiques qui peuvent prendre en charge SDM, ainsi que la quantité de mémoire requise.

REMARQUE : Si vous utilisez SDM pour configurer SSH, vous devez effectuer les Travaux pratiques 5.2.3, « Configuration d'un routeur de service intégré 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 vous utilisez un routeur où SDM n'est pas installé, utilisez les commandes ILC de Cisco IOS pour configurer SSH. Des instructions sont fournies pour sa configuration à l'aide des commandes ILC de Cisco IOS pour les routeurs qui n'exécutent pas SDM 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 de paramètres de base de routeur avec l'ILC IOS ».

REMARQUE : Routeur SDM dont la configuration initiale a été effacée : Si la configuration a été supprimée d'un routeur SDM, SDM ne se réaffiche plus par défaut lors du redémarrage du routeur. Il est alors nécessaire de créer une configuration de routeur de base à l'aide des commandes IOS. Reportez-vous à la procédure décrite à la fin de ces travaux pratiques ou contactez votre formateur.

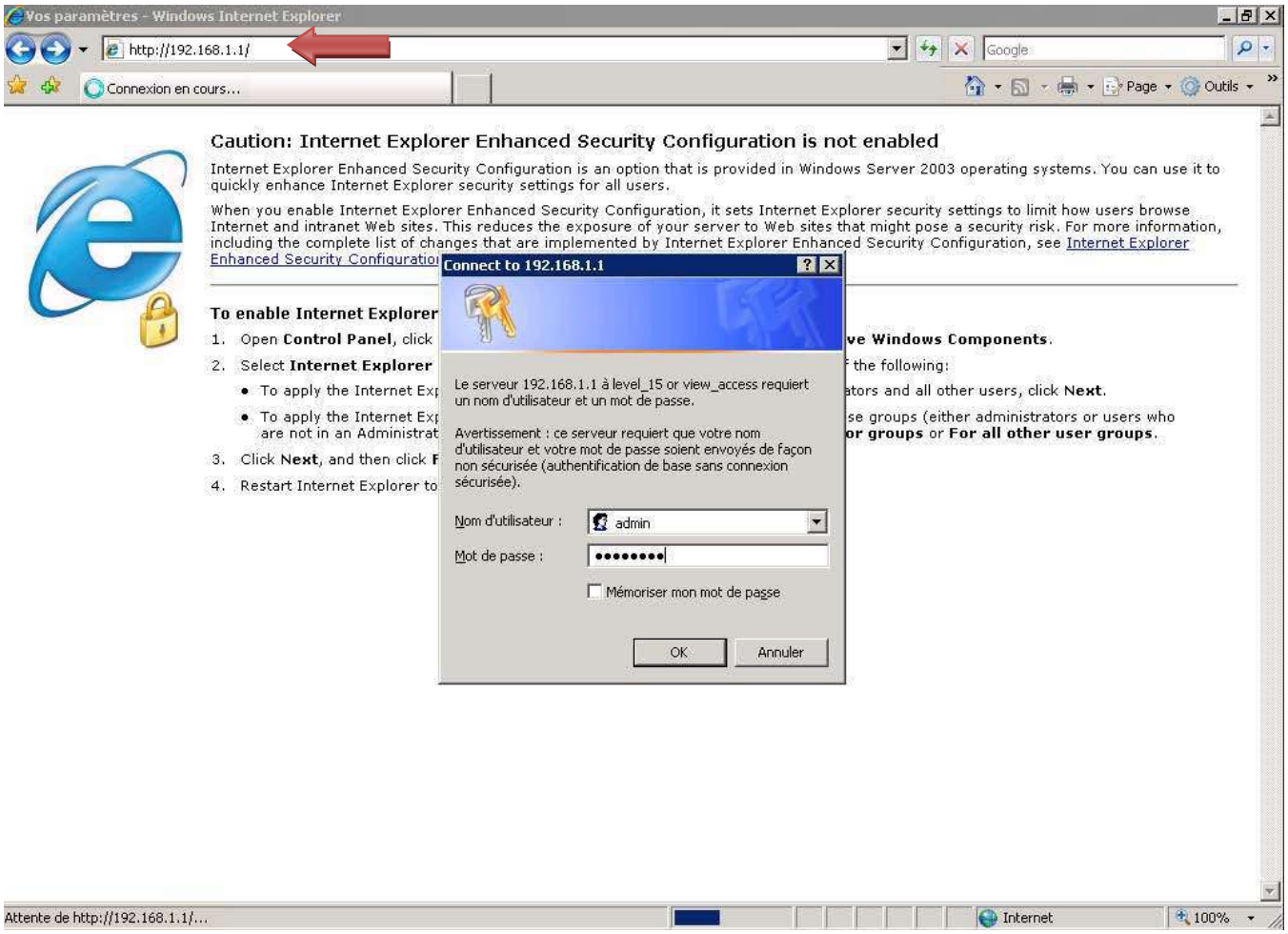
Ressources requises :

- Routeur de service intégré Cisco 1841 avec SDM version 2.4 installé et configuration de base effectuée (très important : voir la remarque 2 de l'étape 1)
- (Facultatif) Autre modèle de routeur Cisco avec SDM installé
- (Facultatif) Autre modèle de routeur Cisco sans installation de SDM (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 commandes PC
- Accès à la configuration réseau TCP/IP du PC

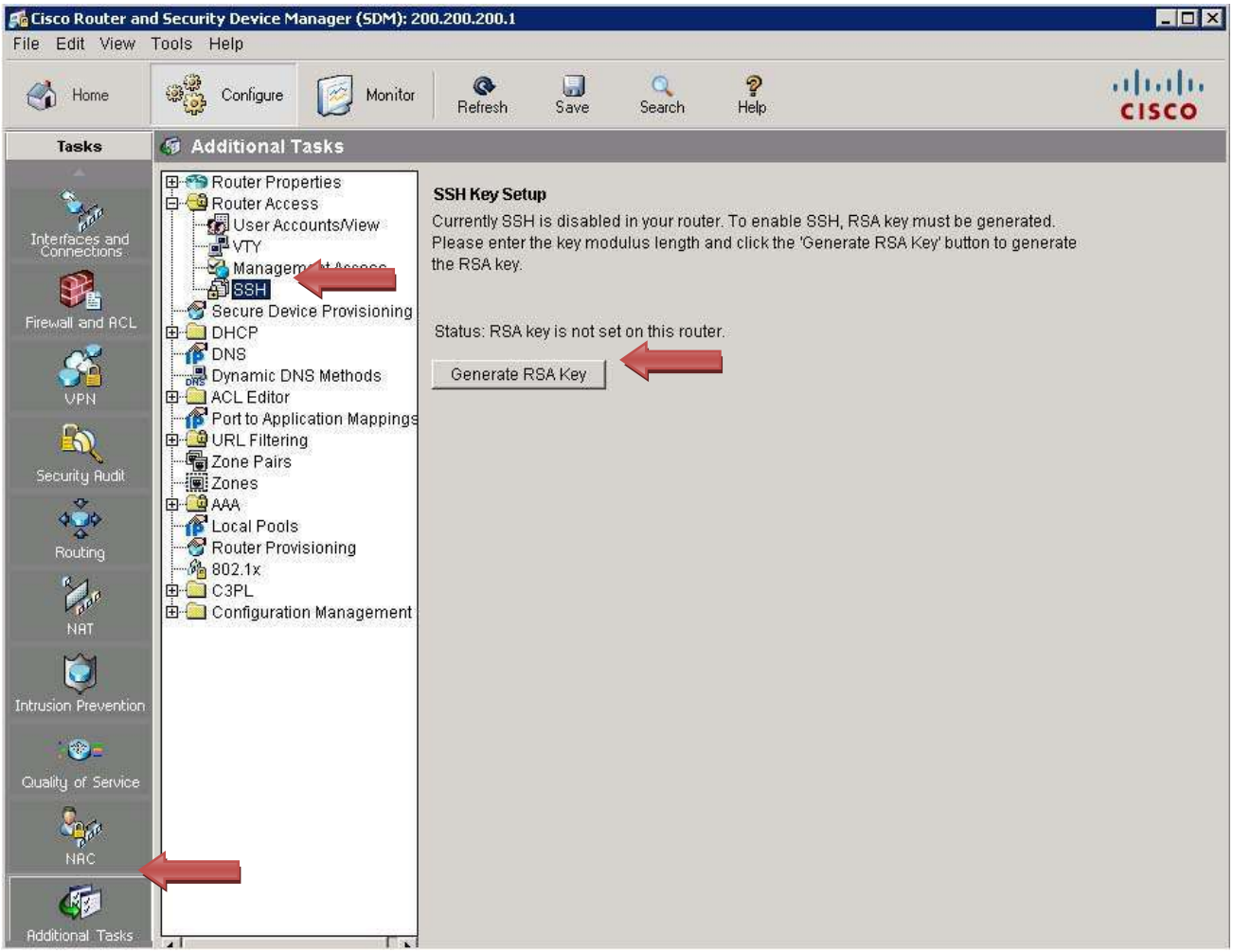
Étape 1 : Configuration du routeur de service intégré afin d'accepter les connexions SSH à l'aide de SDM

REMARQUE : Si SDM n'est pas installé sur le routeur : Si vous configurez SSH sur 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 ; sinon, effectuez l'étape 1 et passez à l'étape 3.

a. Ouvrez le navigateur Web et connectez-vous à http://192.168.1.1. Lorsqu'un message vous y invite, entrez **admin** pour le nom d'utilisateur et **cisco123** pour le mot de passe. Cliquez sur **OK**. Cisco SDM se charge.

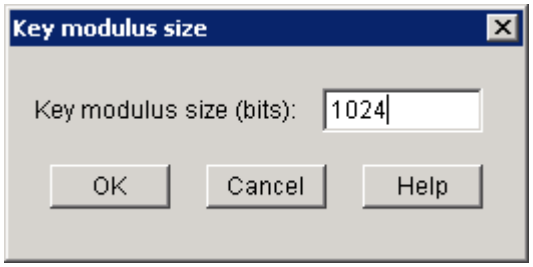


b. Une fois SDM chargé, cliquez sur le bouton **Configure** de la barre d'outils. Dans le volet des tâches (Tasks), cliquez sur **Additional Tasks**. Dans le volet Additional Tasks, développez **Router Access**, puis cliquez sur la tâche **SSH**. Cliquez ensuite sur le bouton **Generate RSA Key**.

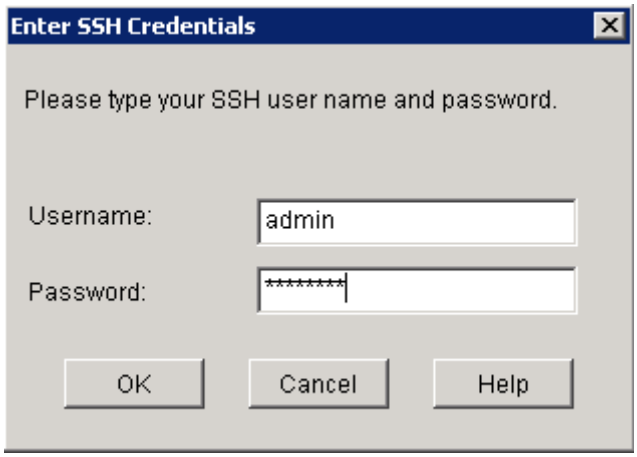


REMARQUE : Si SSH est déjà configuré : Si le message **SSH Key Setup** indique « RSA key exists and SSH is enabled in your router » et que **Status** est « RSA key is set on this router », c'est probablement parce que vous avez effectué les Travaux pratiques 5.2.3, « Configuration d'un routeur de service intégré avec SDM Express ». Souvenez-vous qu'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 se mot de passe est imposée et le nombre de tentatives de connexion infructueuses est limité.

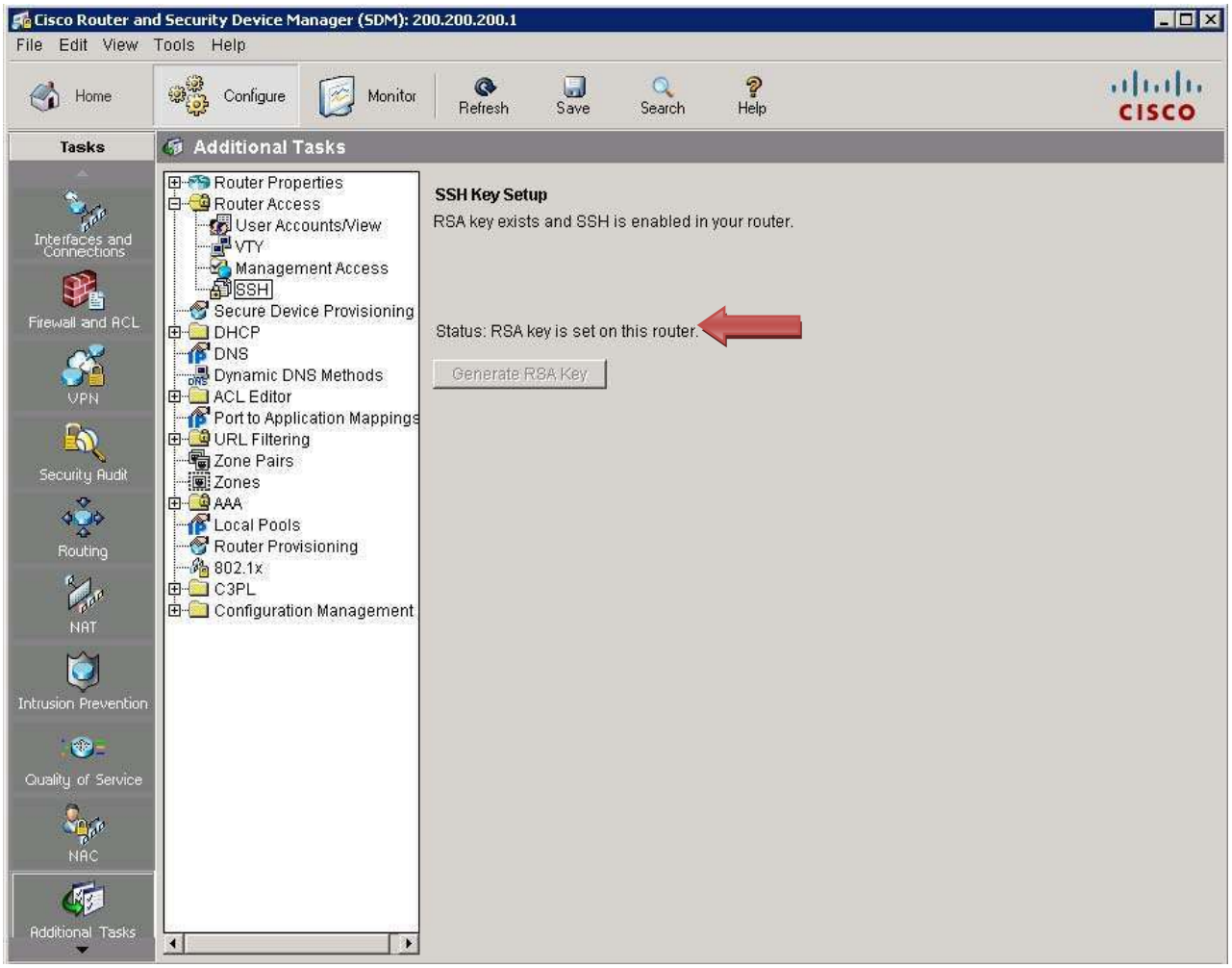
c. Dans la boîte de dialogue Key modulus size, entrez une taille de clé de **1 024** bits. Cliquez sur **OK**.



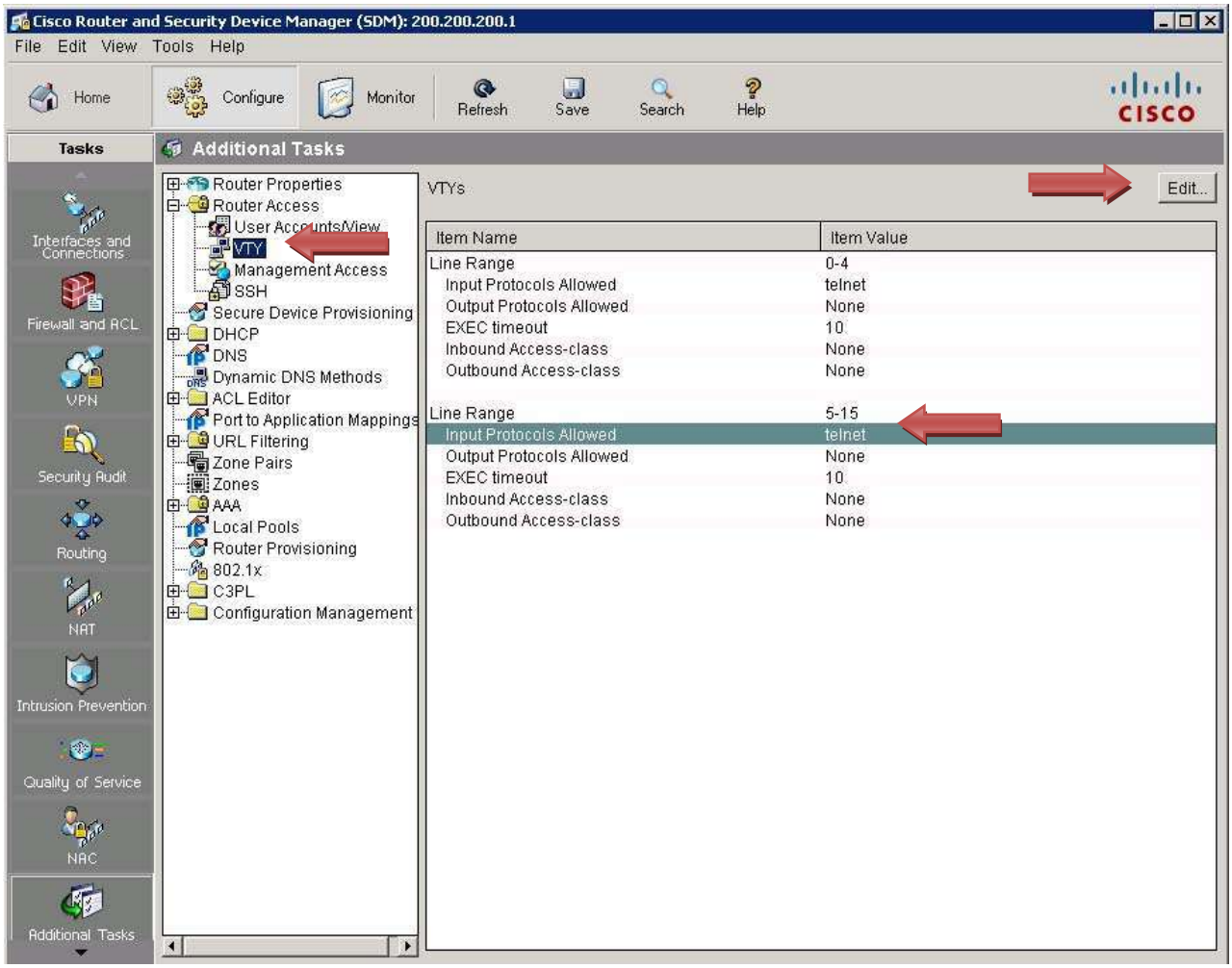
d. Dans la boîte de dialogue Enter SSH Credentials, entrez **admin** comme nom d'utilisateur et **cisco123** comme mot de passe. Cliquez sur **OK**.



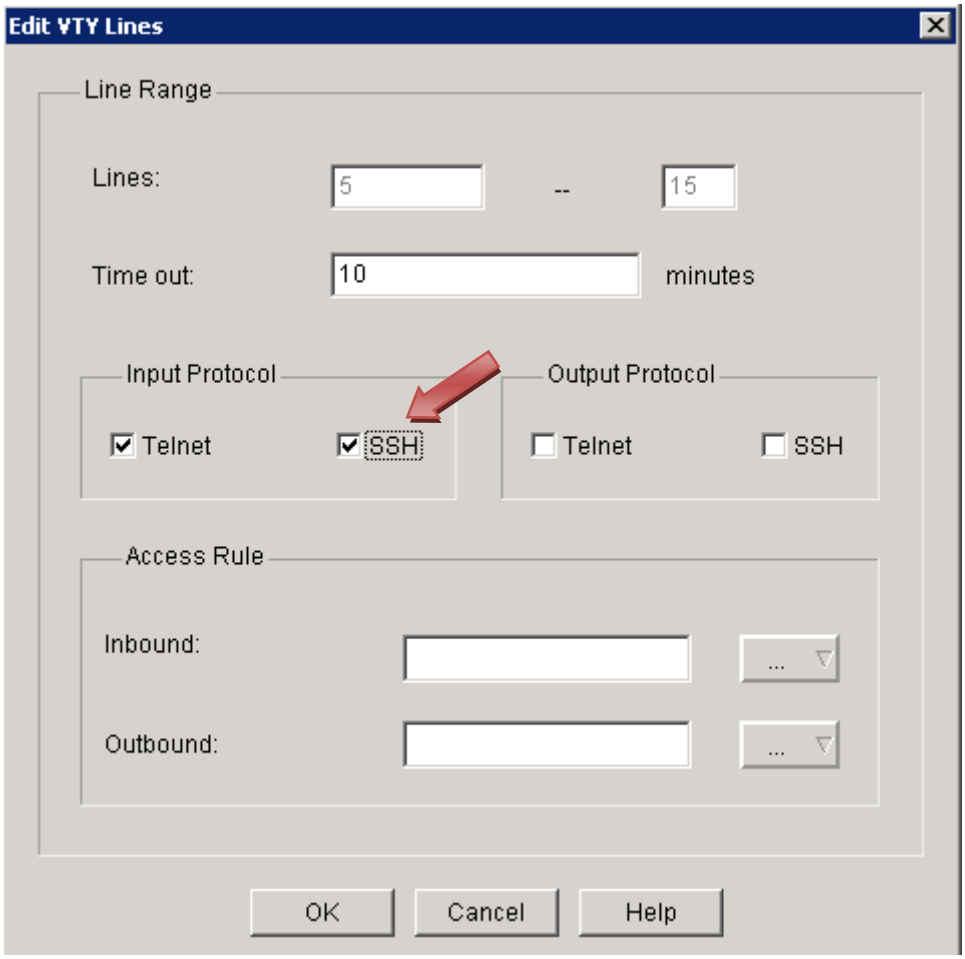
e. Notez que la clé Rivest, Shamir et Adelman (RSA) est actuellement définie sur le routeur.



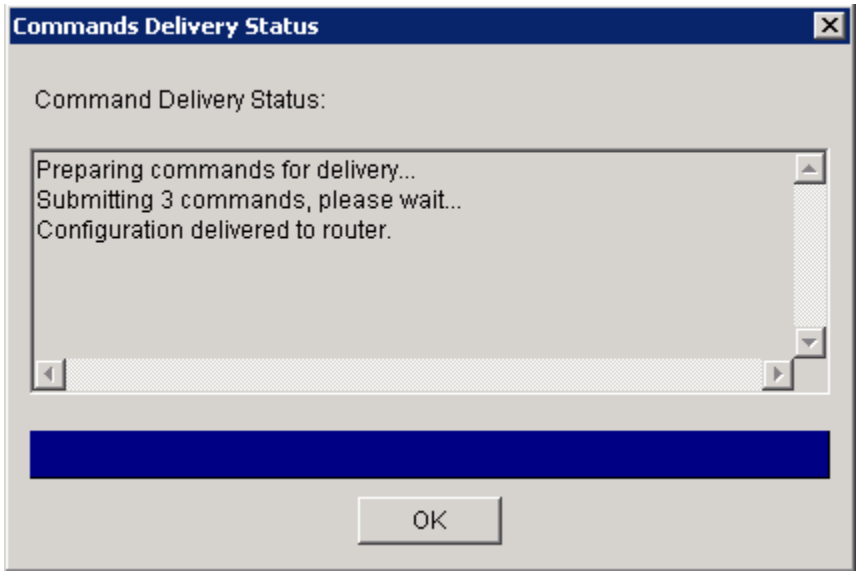
f. Dans le volet Additional Tasks, cliquez sur l'option **VTY**. Sélectionnez **Input Protocols Allowed**, puis cliquez sur le bouton **Edit**.



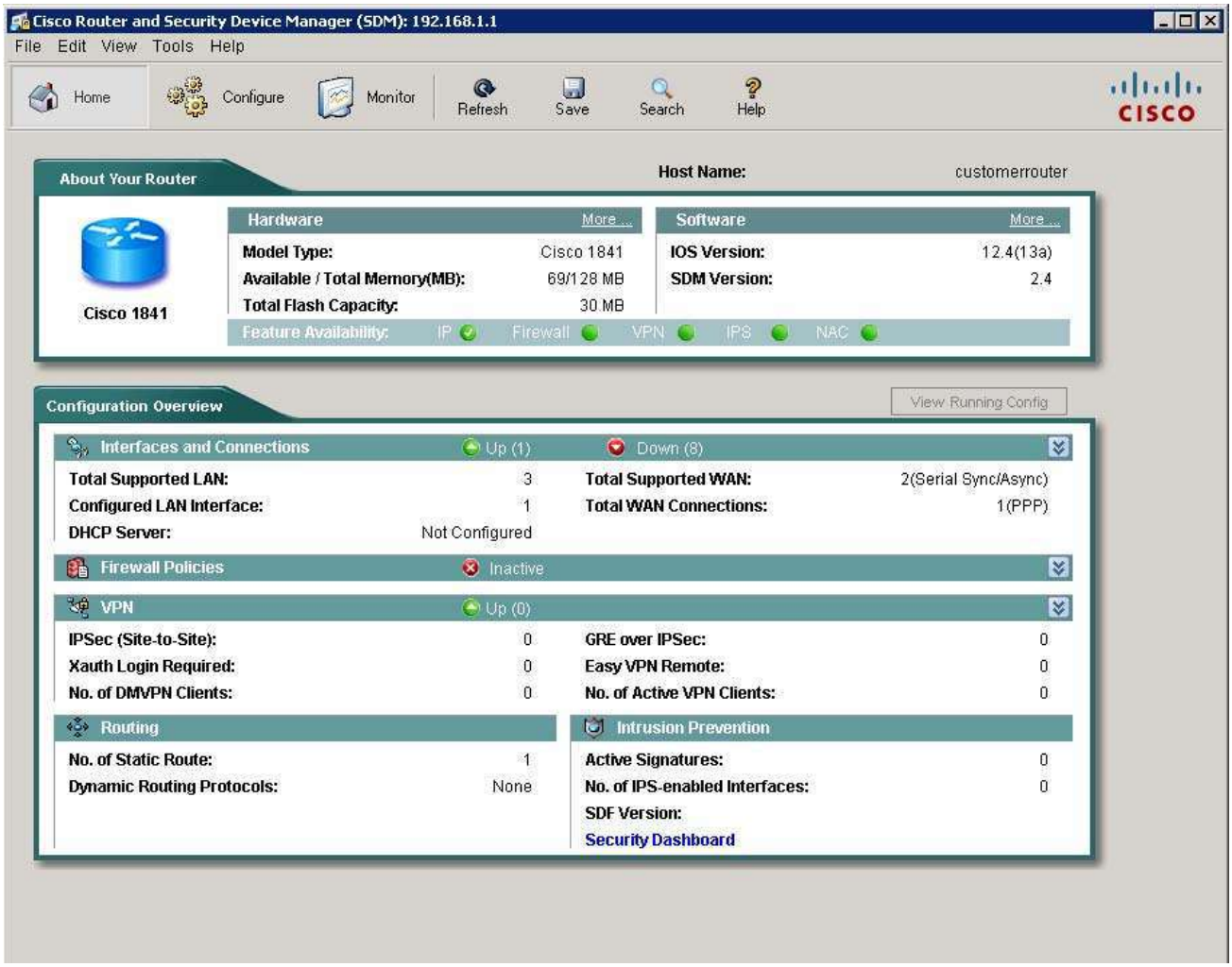
g. Activez la case à cocher en regard de **SSH**, puis cliquez sur **OK**.



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.

Étape 2 : (FACULTATIF) 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. Si vous configurez la réception des connexions SSH sur un routeur où SDM n'est pas installé, connectez le port console du routeur à un PC et au programme HyperTerminal, comme décrit dans les Travaux pratiques 5.1.2, « Mise en marche d'un routeur de service intégré ».

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 5.3.4, « Configuration des paramètres de base de routeur avec l'ILC IOS » pour plus d'informations sur les paramètres de configuration.

REMARQUE : Le routeur doit exécuter IOS 12.0 ou version ultérieure. Dans cet exemple, le routeur est un modèle Cisco 2620XM avec 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 modulus. 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** :

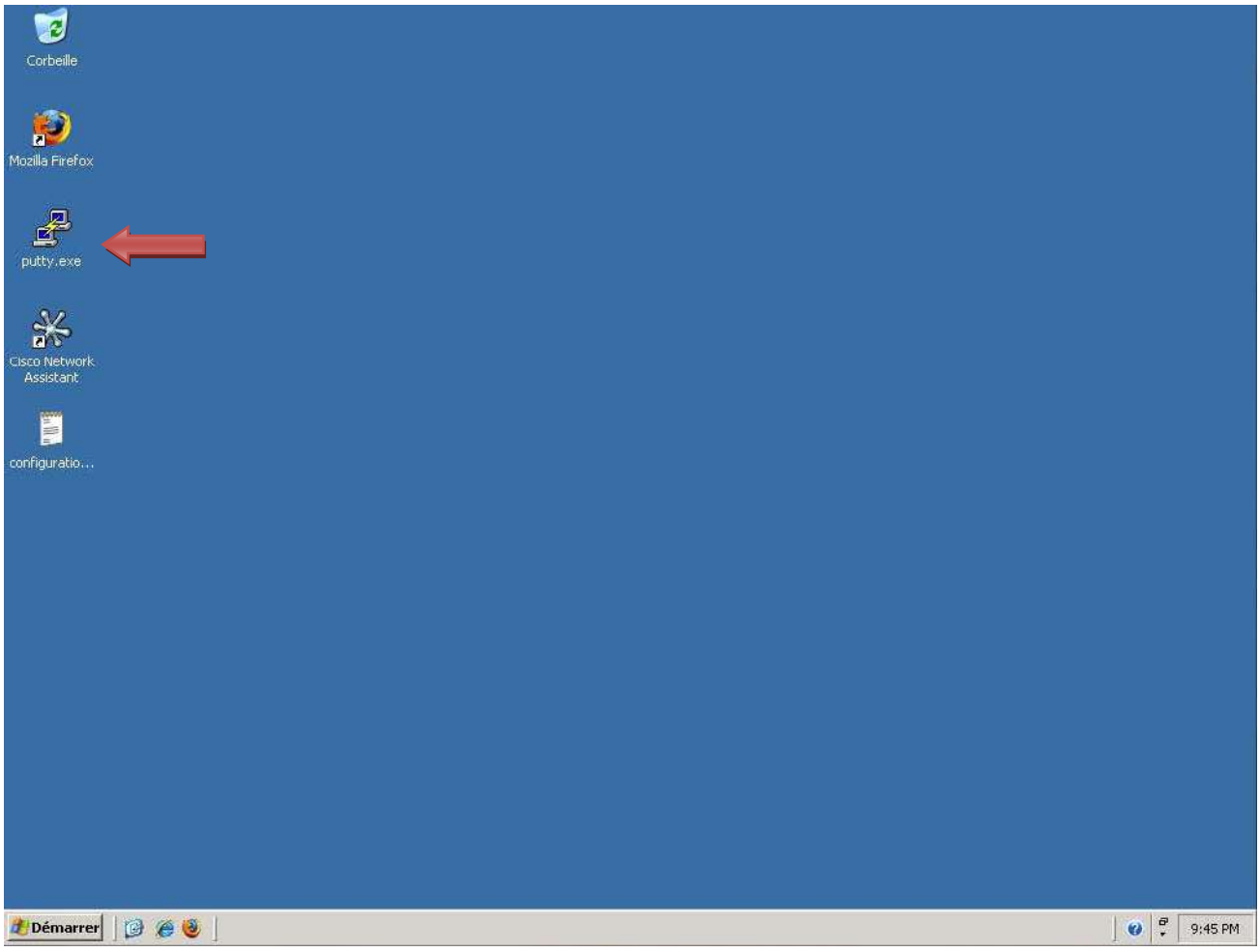
Version SSH activée : _____
Délai d'authentification : _____
Nombre de tentatives d'authentification : _____

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

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

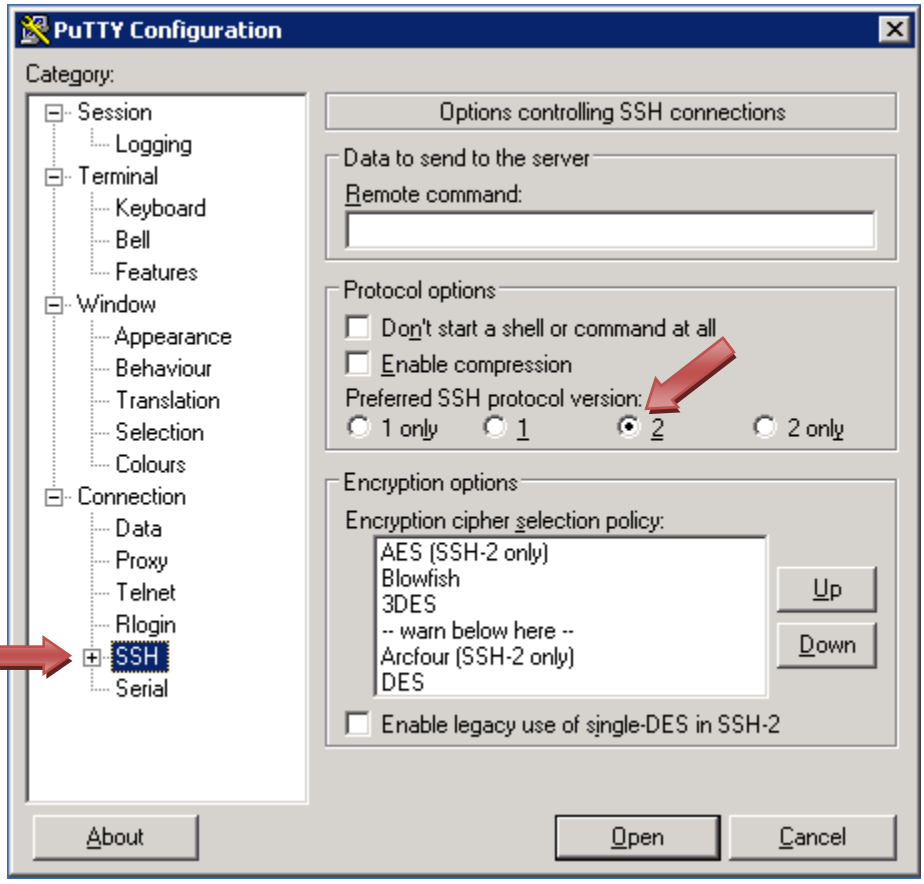
Étape 3 : Configuration du client SSH et connexion du PC au routeur de service intégré

a. Procurez-vous une copie de putty.exe et placez l'application sur le bureau. Lancez PuTTY en double-cliquant sur l'icône **putty.exe**.

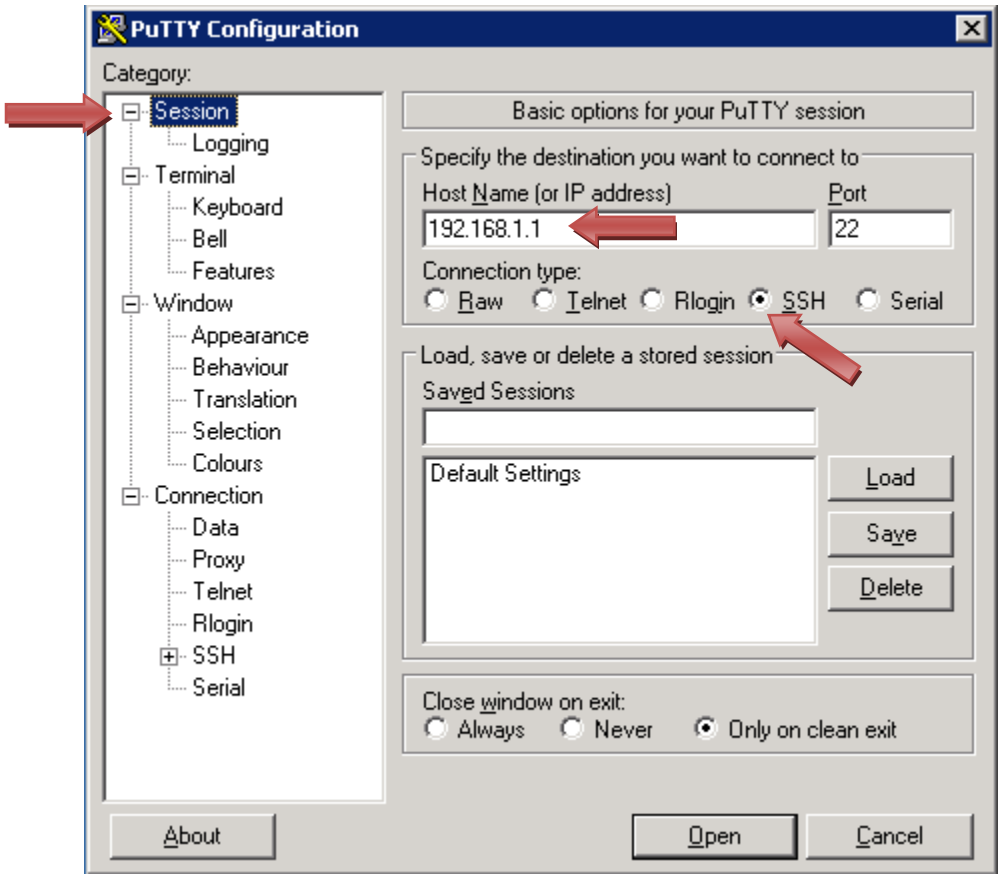


b. Dans le volet Category, sélectionnez **SSH** et vérifiez que la version préférée du protocole SSH est définie à **2**.

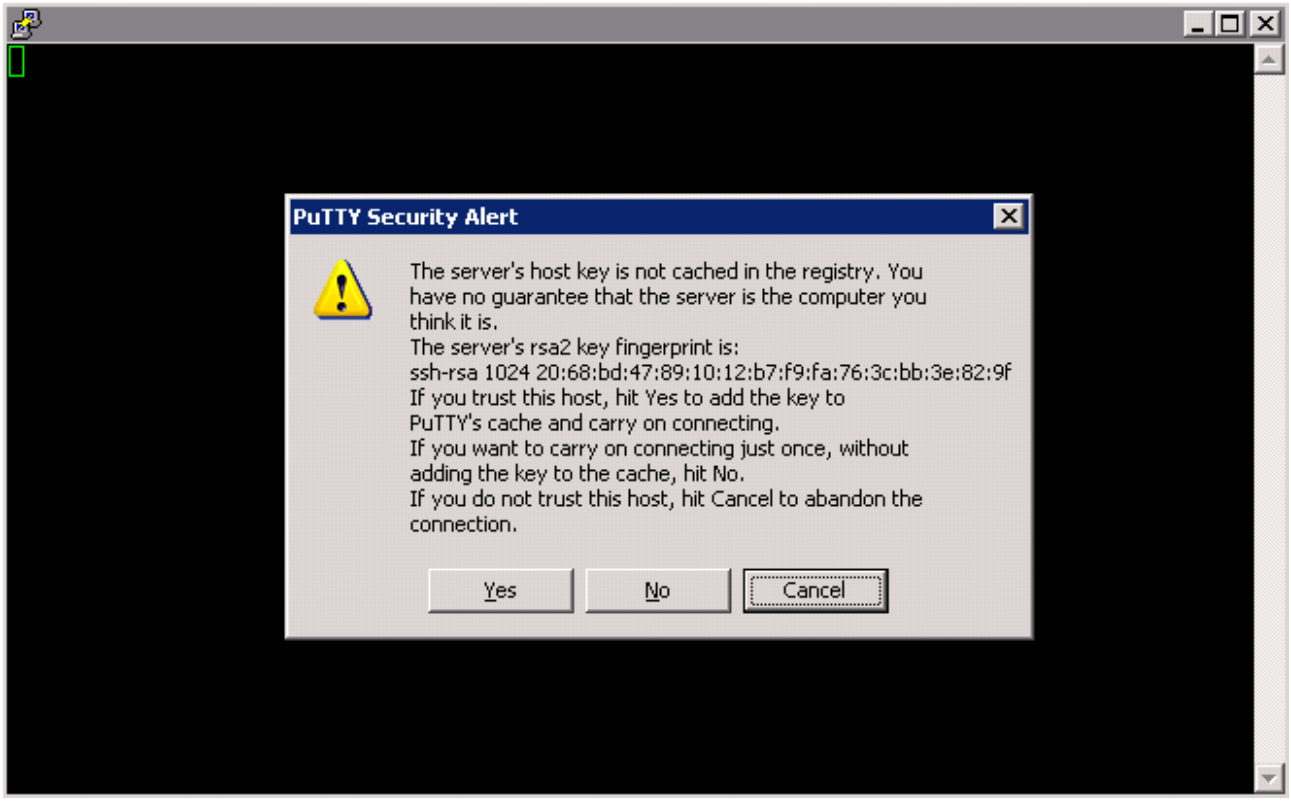
REMARQUE : Le client Putty se connectera même si le serveur SSH exécute la version 1 de SSH.



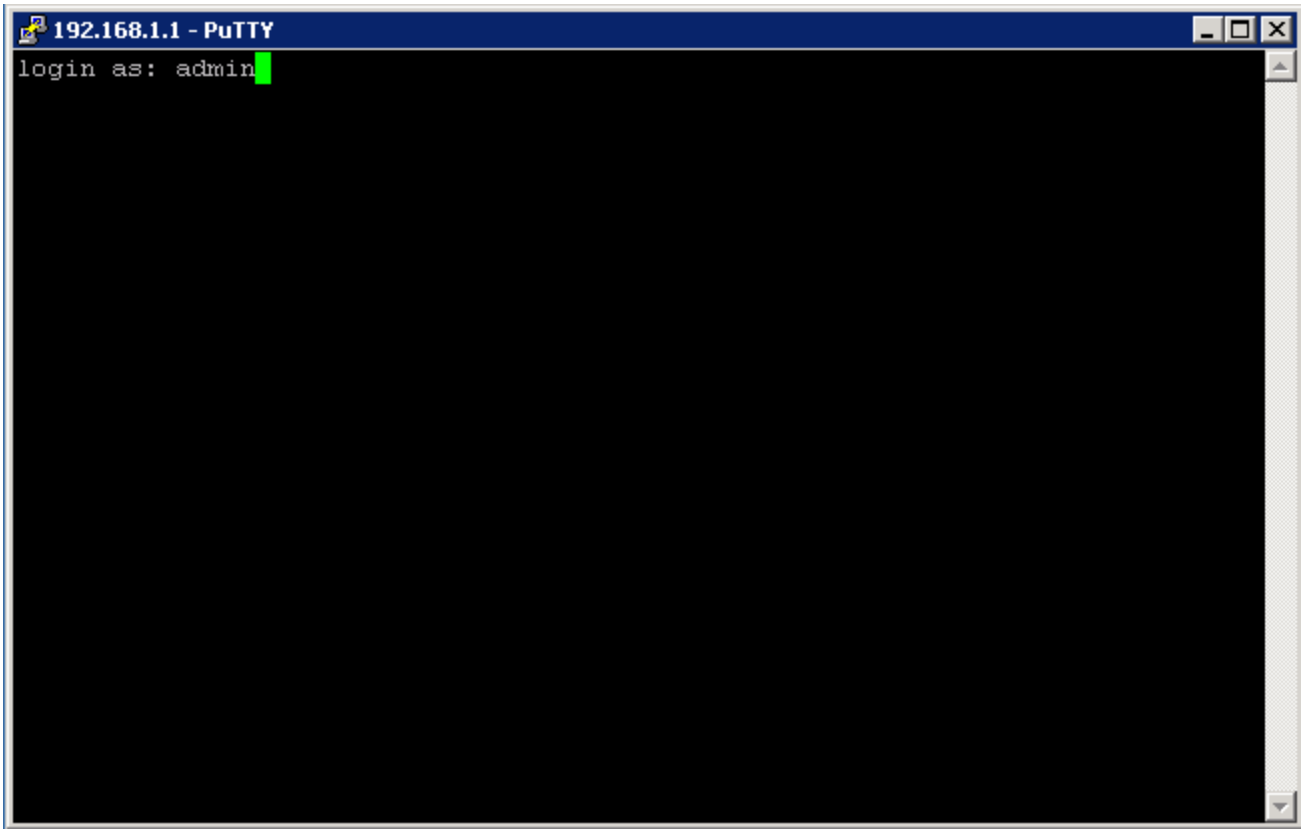
c. Dans le volet Category, sélectionnez **Session** et entrez l'adresse IP de l'interface de réseau local du routeur, qui est 192.168.1.1. Vérifiez que SSH est sélectionné pour le type de connexion. Cliquez sur **Open**.



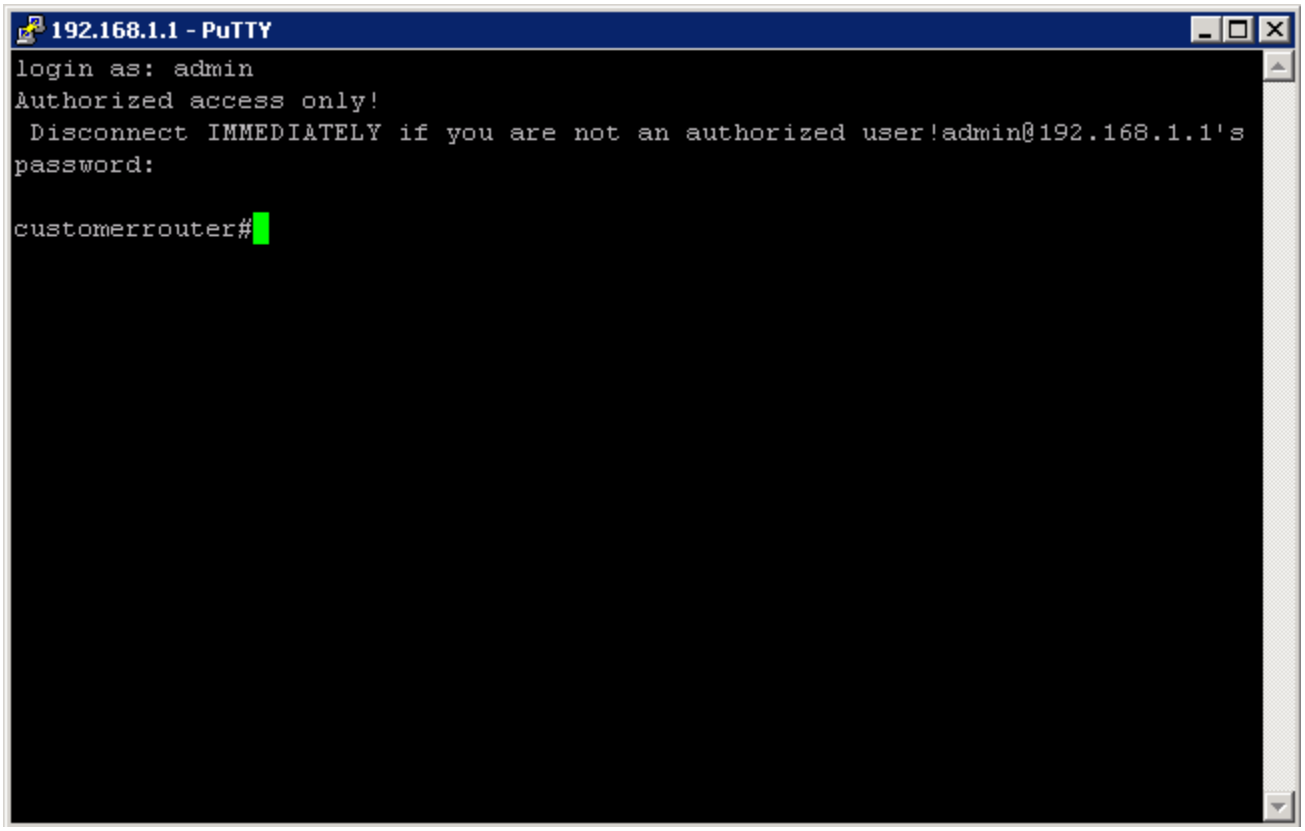
d. La première fois que la connexion est établie avec le service SSH sur le routeur de service intégré Cisco 1841 à l'aide d'un client SSH, une clé de connexion est mise en cache dans le registre de la machine locale. Dans la fenêtre PuTTY Security Alert, cliquez sur **Yes** pour continuer.



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 cliquez sur **Entrée**.

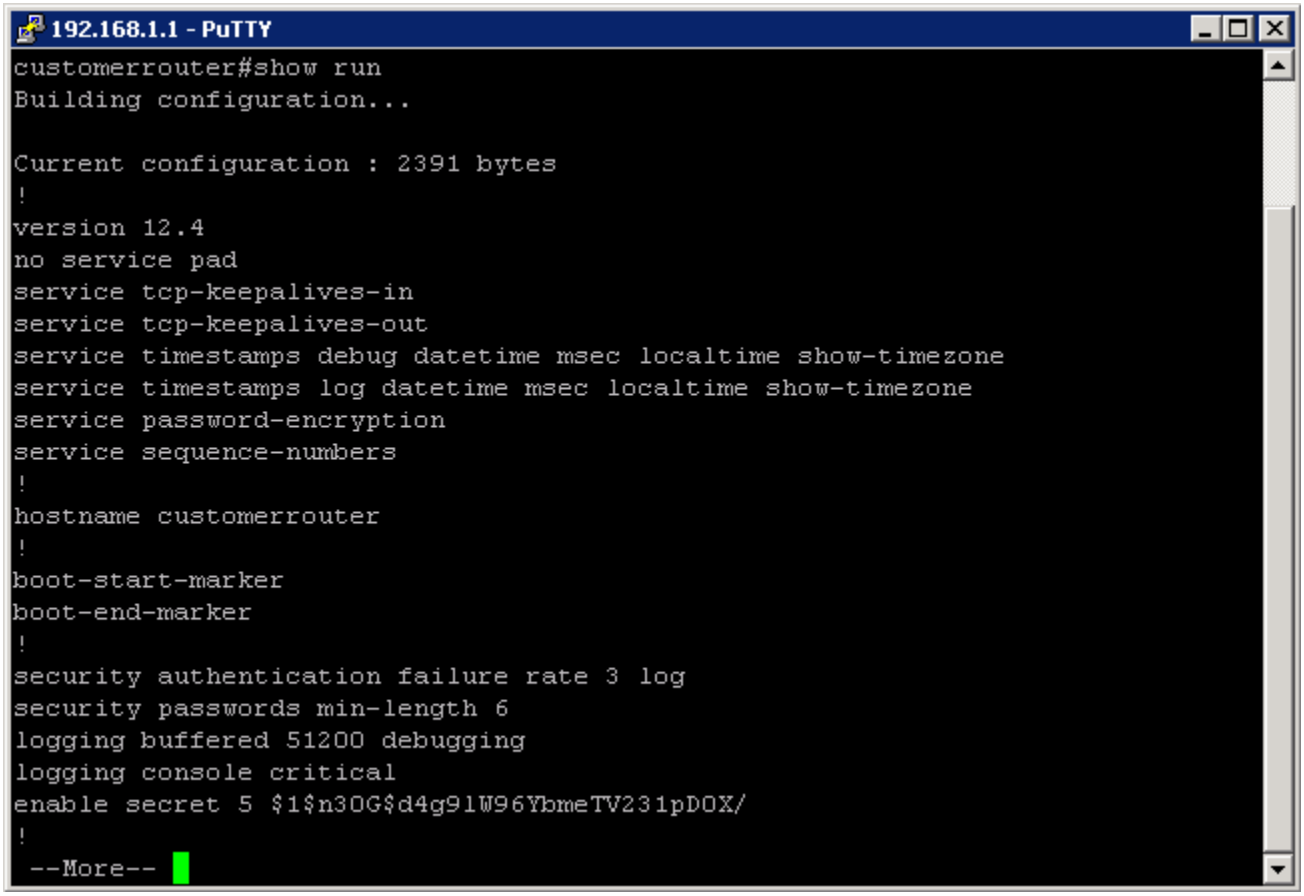


Étape 4 : Vérification de la configuration du routeur de service intégré Cisco 1841

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

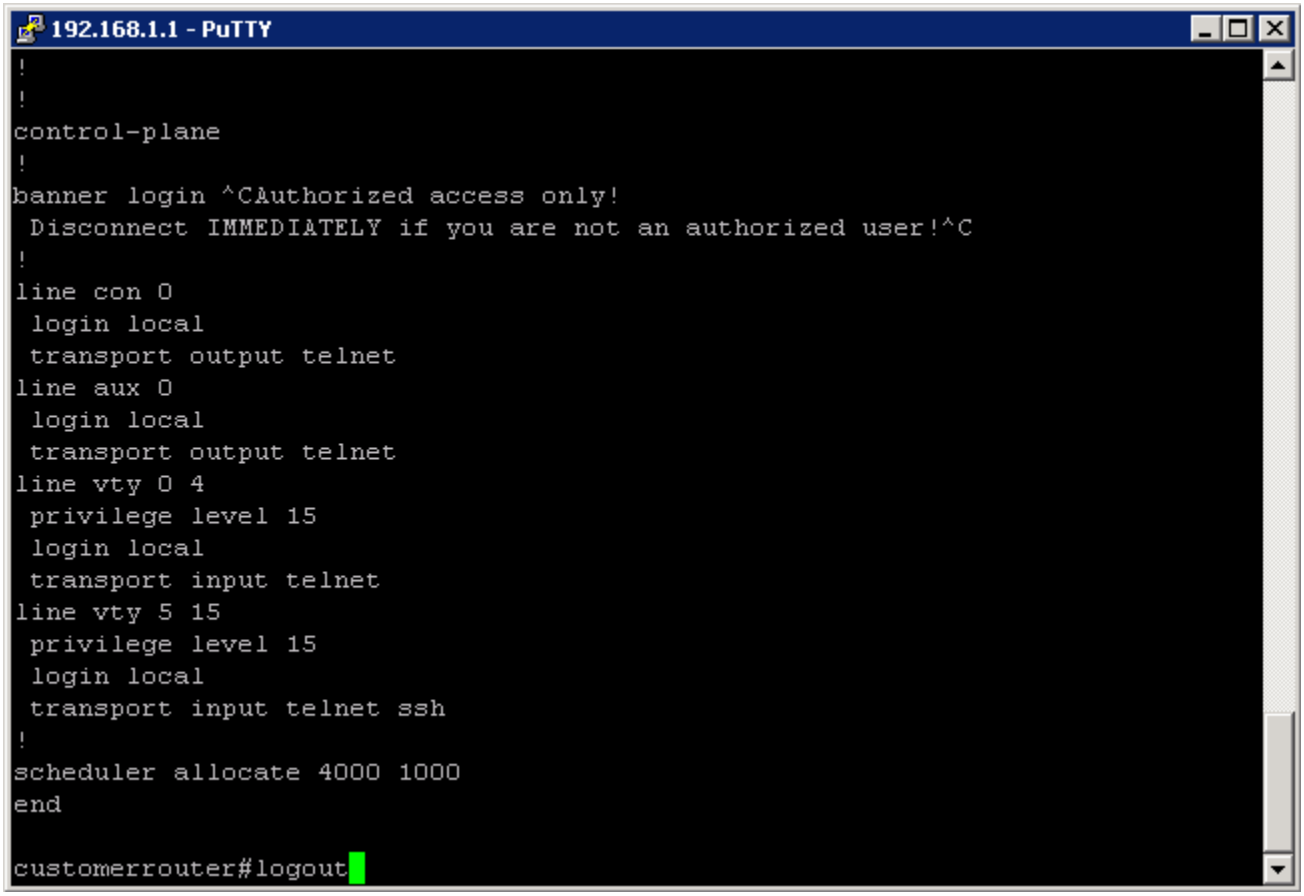
REMARQUE : Il n'est pas nécessaire de passer du mode utilisateur au mode d'exécution privilégié car ce mode est le mode paramétré par défaut après la configuration de SDM Express et SDM.

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



Étape 5 : Déconnexion du routeur de service intégré 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**.



Étape 6 : Réflexion

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 IOS de base du routeur SDM pour activer SDM

Si la configuration initiale est supprimée d'un routeur SDM, SDM ne s'affiche plus par défaut lors du redémarrage du routeur. Il est alors nécessaire de créer une configuration de base comme suit. Pour plus d'informations au sujet de la configuration et de l'utilisation de SDM, consultez le SDM Quick Start Guide :

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

1) Définissez l'adresse IP Fa0/0 du routeur (il s'agit de l'interface à laquelle un PC se connecte au moyen d'un navigateur pour activer SDM. L'adresse IP du PC doit être réglée sur 10.10.10.2 255.255.255.248).

REMARQUE : Il est possible qu'un routeur SDM autre que le 1841 requière 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, en utilisant les commandes Cisco IOS suivantes :

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

3) Créez un compte utilisateur avec le niveau de privilège 15 (activer les privilèges).
   Router(config)# **username** <username> **privilege 15 password 0** <password>

   Remplacez <username> et <password> par le nom d'utilisateur et le mot de passe que vous souhaitez configurer.

4) Configurez SSH et Telnet pour la connexion locale et le niveau de privilège 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**