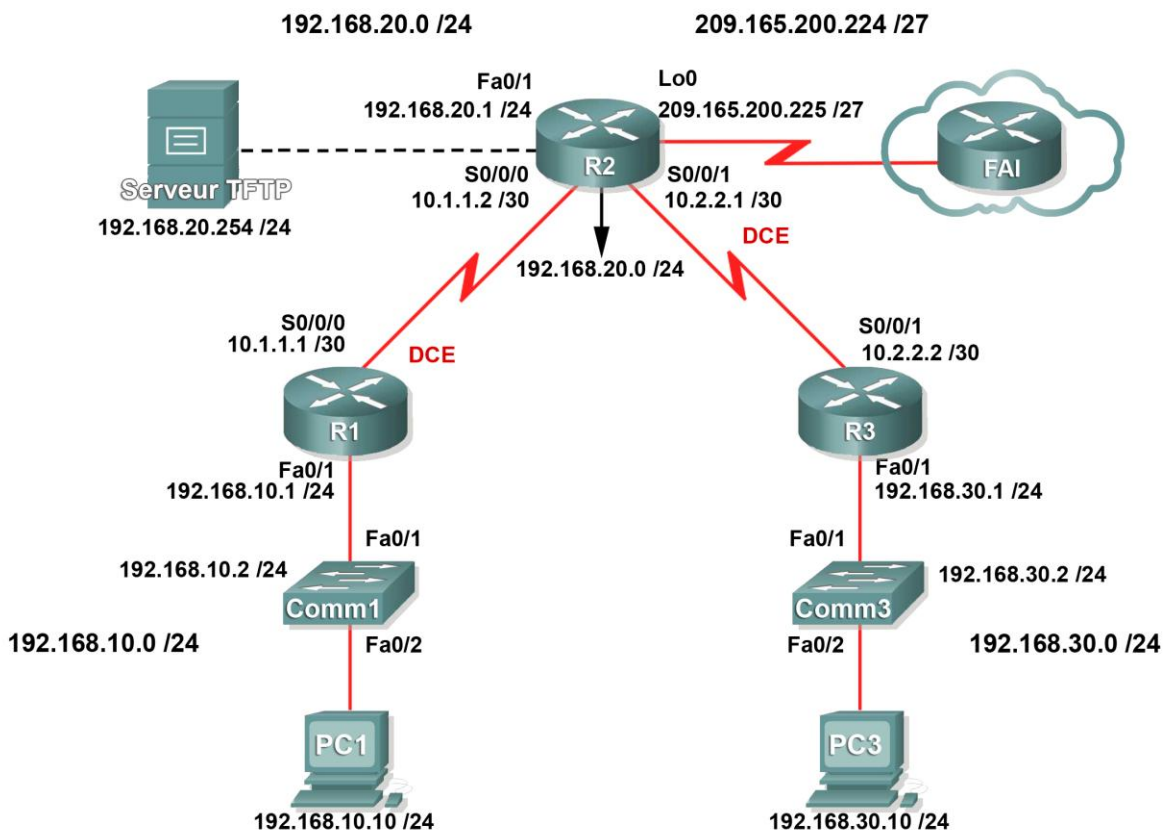


## Travaux pratiques 4.6.1 : configuration de base de la sécurité

### Diagramme de topologie



### Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/1	192.168.10.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	Fa0/1	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
R3	Fa0/1	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
Comm1	VLAN10	192.168.10.2	255.255.255.0	N/D
Comm3	VLAN20	192.168.30.2	255.255.255.0	N/D

<b>PC1</b>	<b>Carte réseau</b>	192.168.10.10	255.255.255.0	192.168.10.1
<b>PC3</b>	<b>Carte réseau</b>	192.168.30.10	255.255.255.0	192.168.30.1
<b>Serveur TFTP</b>	<b>Carte réseau</b>	192.168.20.254	255.255.255.0	192.168.20.1

## Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Câbler un réseau conformément au diagramme de topologie
- Supprimer la configuration de démarrage et recharger un routeur pour revenir aux paramètres par défaut
- Exécuter les tâches de configuration de base d'un routeur
- Configurer la sécurité de base des ports
- Désactiver les services et interfaces Cisco inutilisés
- Protéger les réseaux d'entreprise contre des principales attaques externes et internes
- Comprendre et gérer les fichiers de configuration Cisco IOS ainsi que le système de fichiers Cisco
- Configurer et utiliser Cisco SDM (Security Device Manager) et SDM Express pour définir la sécurité de base d'un routeur
- Configurer les réseaux locaux virtuels (VLAN) sur les commutateurs

## Scénario

Dans le cadre de ces travaux pratiques, vous apprendrez à configurer les paramètres de sécurité de base du réseau. Pour ce faire, vous utiliserez le réseau illustré sur le diagramme de topologie. Vous apprendrez également à configurer la sécurité d'un routeur de trois manières : en utilisant l'interface de ligne de commande (ILC), la fonction de sécurité automatique, ou Cisco SDM. Enfin, vous apprendrez à gérer le logiciel Cisco IOS.

## Tâche 1 : préparation du réseau

### Étape 1 : câblage d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel routeur durant les travaux pratiques, à condition qu'il soit équipé des interfaces indiquées dans la topologie.

Remarque : ces travaux pratiques ont été développés et testés à l'aide de routeurs 1841. si vous utilisez les routeurs 1700, 2500 ou 2600, les sorties des routeurs et les descriptions des interfaces apparaîtront différemment.

### Étape 2 : suppression des configurations existantes sur les routeurs

## Tâche 2 : exécution des configurations de routeur de base

### Étape 1 : configuration des routeurs

Configurez les routeurs R1, R2 et R3 conformément aux instructions suivantes :

- Configurez le nom d'hôte du routeur conformément au diagramme de topologie.
- Désactivez la recherche DNS.
- Configurez une bannière de message du jour.
- Configurez les adresses IP sur R1, R2 et R3.
- Activez la version 2 du protocole RIP sur l'ensemble des routeurs de tous les réseaux.
- Créez une interface de bouclage sur R2 afin de simuler une connexion Internet.
- Configurez un serveur TFTP sur R2. Vous pouvez télécharger le logiciel serveur TFTP à partir de : <http://tftpd32.jounin.net/>

### Étape 2 : configuration des interfaces Ethernet

Configurez les interfaces Ethernet de PC1, PC3 et du serveur TFTP à l'aide des adresses IP et des passerelles par défaut figurant dans la table d'adressage fournie au début de ces travaux pratiques.

### Étape 3 : test de la configuration d'un PC par l'envoi d'une commande ping à la passerelle par défaut, à partir de chaque PC et du serveur TFTP

## Tâche 3 : sécurisation du routeur par rapport aux accès non autorisés

### Étape 1 : configuration des mots de passe sécurisés et authentification AAA

Configurez des mots de passe sécurisés sur R1 à l'aide d'une base de données locale. Dans ces travaux pratiques, le mot de passe à utiliser est **ciscoccna**.

```
R1(config)#enable secret ciscoccna
```

Comment la configuration d'un mot de passe enable secret contribue-t-elle à protéger un routeur d'une attaque ?

La commande **username** permet de définir un nom d'utilisateur et un mot de passe, enregistrés localement sur le routeur. Par défaut, le niveau de privilège de l'utilisateur est défini sur 0 (le niveau d'accès le plus bas). Vous pouvez modifier le niveau d'accès assigné à un utilisateur en ajoutant le mot clé **privilege 0 - 15** avant le mot clé **password**.

```
R1(config)#username ccna password ciscoccna
```

La commande **aaa** permet d'activer le protocole AAA (Authentication, Authorization and Accounting : authentification, autorisation et comptabilisation) de manière globale sur le routeur. Cette commande est utilisée lors de la connexion au routeur.

```
R1(config)#aaa new-model
```

Vous pouvez créer une liste d'authentification qui est consultée lorsqu'un utilisateur tente de se connecter au périphérique, une fois que vous l'aurez appliquée aux lignes vty et aux lignes de la console. Le mot clé **local** indique que la base de données de l'utilisateur est enregistrée localement sur le routeur.

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

Les commandes suivantes indiquent au routeur que les utilisateurs qui tentent de se connecter doivent être authentifiés via la liste que vous venez de créer.

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

Dans la section de configuration en cours suivante, quel élément vous semble non sécurisé ?

```
R1#show run
<résultat omis>
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
<résultat omis>
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
  logging synchronous
  login authentication LOCAL_AUTH
line aux 0
line vty 0 4
  login authentication LOCAL_AUTH
!
```

---

---

---

Pour appliquer un chiffrement simple sur les mots de passe, entrez la commande suivante en mode de configuration globale :

```
R1(config)#service password-encryption
```

Pour vérifier cela, exécutez la commande **show run**.

```
R1#show run
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
<résultat omis>
!
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
  logging synchronous
  login authentication LOCAL_AUTH
line aux 0
line vty 0 4
  login authentication LOCAL_AUTH
!
```

## Étape 2 : protection des lignes de console et des lignes VTY

Vous pouvez faire en sorte que le routeur déconnecte une ligne qui a été inactive pendant une période donnée. Si un ingénieur réseau est connecté à un périphérique réseau, qu'il est appelé et qu'il part subitement, cette commande permet de le déconnecter automatiquement au bout de la période indiquée. Les commandes suivantes permettent la déconnexion d'une ligne au bout de 5 minutes.

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

La commande suivante permet d'empêcher les tentatives de connexion en force. Le routeur bloque les tentatives de connexion pendant 5 minutes si un utilisateur effectue 2 tentatives de connexion sans y parvenir au bout de 2 minutes. Pour répondre aux objectifs de ces travaux pratiques, la durée définie est particulièrement courte. Une action supplémentaire consiste à consigner chaque tentative de ce type.

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 5 log
```

Pour vérifier cela, essayez de vous connecter à R1, à partir de R2, via le protocole Telnet à l'aide d'un nom d'utilisateur et d'un mot de passe incorrects.

### Sur R2 :

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:
```

```
% Authentication failed

User Access Verification

Username: cisco
Password:

% Authentication failed

[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

#### Sur R1 :

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

### Tâche 4 : sécurisation de l'accès au réseau

#### Étape 1 : prévention de la propagation d'une mise à jour de routage RIP

Quelle machine peut recevoir des mises à jour de routage RIP sur un segment de réseau au niveau duquel le protocole RIP est activé ? S'agit-il de la configuration la plus appropriée ?

---

---

---

La commande **passive-interface** empêche les routeurs d'envoyer des mises à jour de routage à toutes les interfaces, excepté celles configurées pour participer à ces mises à jour. Cette commande doit être exécutée lors de la configuration du protocole RIP.

La première commande permet de définir toutes les interfaces en mode passif (l'interface reçoit uniquement les mises à jour de routage RIP). La deuxième commande permet de rétablir le mode actif pour certaines interfaces (qui peuvent alors envoyer et recevoir des mises à jour RIP).

#### R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

#### R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

#### R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```

## Étape 2 : prévention de la réception non autorisée des mises à jour RIP

Pour sécuriser le protocole RIP, vous devez tout d'abord bloquer les mises à jour RIP inutiles. Vous devez ensuite protéger les mises à jour RIP au moyen d'un mot de passe. Pour ce faire, vous devez d'abord configurer la clé à utiliser.

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

Ces informations doivent être ajoutées à tous les routeurs destinés à recevoir des mises à jour RIP.

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

Pour utiliser la clé, vous devez configurer chacune des interfaces participant aux mises à jour RIP. Ces interfaces sont celles qui ont été précédemment activées à l'aide de la commande **no passive-interface**.

### R1

```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

À ce stade, R1 ne reçoit plus les mises à jour RIP issues de R2, étant donné que ce dernier n'est pas encore configuré pour utiliser une clé permettant les mises à jour de routage. Vous pouvez observer cette situation sur R1, en exécutant la commande **show ip route** et en vérifiant qu'aucune route provenant de R2 ne figure dans la table de routage.

Effacez les routes IP à l'aide de la commande **clear ip route \*** ou attendez l'expiration de leur délais d'attente.

### R1#show ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, *-candidate default, U-per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
      10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C      192.168.10.0 is directly connected, Serial0/0/0
```

Pour utiliser l'authentification de routage, vous devez configurer R2 et R3. Notez que chaque interface active doit être configurée.

### R2

```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
```

```
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```

### R3

```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

## Étape 3 : vérification du fonctionnement du routage RIP

Une fois les trois routeurs configurés en vue d'utiliser l'authentification de routage, les tables de routage doivent à nouveau être alimentées avec toutes les routes RIP. À présent, R1 doit disposer de toutes les routes via RIP. Vérifiez cela à l'aide de la commande **show ip route**.

```
R1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, *-candidate default, U-per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R    10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C    10.1.1.0/24 is directly connected, Serial0/0/0
```

## Tâche 5 : consignation des activités via le protocole SNMP (Simple Network Management Protocol)

### Étape 1 : configuration de la consignation via le protocole SNMP vers le serveur syslog

Il peut être utile d'effectuer une consignation via SNMP dans le cadre de la surveillance de l'activité d'un réseau. Les informations ainsi consignées peuvent être envoyées vers un serveur syslog du réseau, où elles peuvent être analysées et archivées. Soyez prudent lorsque vous configurez une consignation (syslog) sur le routeur. Lors du choix de l'hôte de consignation, rappelez-vous que ce dernier doit être connecté à un réseau fiable ou protégé, ou bien à une interface de routeur dédiée ou isolée.

Au cours de ces travaux pratiques, vous apprendrez à configurer l'ordinateur PC1 en tant que serveur syslog pour R1. Utilisez la commande **logging** pour sélectionner l'adresse IP du périphérique vers lequel les messages SNMP sont envoyés. Dans l'exemple suivant, l'adresse IP de PC1 est utilisée.

```
R1(config)#logging 192.168.10.10
```

**Remarque : si vous souhaitez consulter les messages syslog, le logiciel syslog doit être installé et exécuté sur PC1.**

Dans l'étape suivante, vous allez définir le niveau de gravité des messages à envoyer au serveur syslog.



## Étape 2 : configuration du niveau de gravité SNMP

Le niveau des messages SNMP peut être ajusté afin de permettre à l'administrateur de déterminer les types de messages envoyés au périphérique syslog. Les routeurs prennent en charge différents niveaux de consignation. Il existe huit niveaux, allant de 0 (Urgence, le système est instable) à 7 (Débogage, des messages contenant des informations sur le routeur sont envoyés). Pour configurer les niveaux de gravité, utilisez le mot clé associé à chaque niveau, comme indiqué dans le tableau ci-dessous.

Niveau de gravité	Mot clé	Description
0	emergencies	Système inutilisable
1	alerts	Action immédiate requise
2	critical	Conditions critiques
3	errors	Conditions d'erreur
4	warnings	Conditions d'avertissement
5	notifications	Condition normale mais sensible
6	informational	Messages informatifs
7	debugging	Messages de débogage

La commande **logging trap** permet de définir le niveau de gravité. Le niveau de gravité inclut le niveau spécifié et tout ce qui figure au-dessous (du niveau normal au niveau de gravité spécifié). Définissez R1 sur le niveau 4 pour capturer des messages avec des niveaux de gravité 4, 5, 6 et 7.

```
R1(config)#logging trap warnings
```

Quel est le danger de définir un niveau de gravité trop élevé ou trop faible ?

---

---

---

**Remarque : si vous avez installé le logiciel syslog sur PC1, lancez-le et consultez les messages générés.**

## Tâche 6 : désactivation des services réseau Cisco inutilisés

### Étape 1 : désactivation des interfaces inutilisées

Pourquoi est-il nécessaire de désactiver les interfaces inutilisées sur les périphériques réseau ?

Dans le diagramme de topologie, vous pouvez voir que R1 ne doit utiliser que les interfaces S0/0/0 et Fa0/1. Toutes les autres interfaces sur R1 doivent être désactivées sur le plan administratif, à l'aide de la commande de configuration d'interface **shutdown**.

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown
```

```
*Sep 10 13:40:240.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Sep 10 13:40:250.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

Pour vérifier si toutes les interfaces inactives de R1 ont bien été désactivées, utilisez la commande **show ip interface brief**. Les interfaces désactivées manuellement sont répertoriées comme étant désactivées sur le plan administratif.

```
R1#sh ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	192.168.10.1	YES	manual	up	up
Serial0/0/0	10.1.0.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

### Étape 2 : désactivation des services globaux inutilisés

De nombreux services ne sont pas requis dans la plupart des réseaux modernes. Si les services inutilisés restent activés, les ports restent ouverts et peuvent alors être utilisés pour compromettre un réseau. Désactivez tous les services inutilisés sur R1.

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

### Étape 3 : désactivation des services d'interface inutilisés

Les commandes ci-après sont saisies au niveau de l'interface et doivent être appliquées à chaque interface sur R1.

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachable
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

Quel type d'attaque la désactivation des commandes IP redirects, IP unreachable et IP directed broadcasts peut-elle empêcher ?

---

---

---

### Étape 4 : utilisation de la fonction AutoSecure pour sécuriser un routeur Cisco

À l'aide d'une seule commande en mode CLI (Interface de ligne de commande), la fonction AutoSecure vous permet de désactiver les services IP communs pouvant être exploités par des attaques réseau et d'activer des fonctions et des services IP pouvant être utiles dans la protection d'un réseau lors d'une attaque. La fonction AutoSecure simplifie la configuration de la sécurité d'un routeur et renforce la configuration de ce même routeur.

Elle vous permet d'appliquer plus rapidement les mêmes fonctions de sécurité que celles que vous venez d'appliquer (sauf pour la sécurisation du protocole RIP) à un routeur. Comme vous avez déjà sécurisé R1, utilisez la commande **auto secure** sur R3.

```
R3#auto secure
```

```
--- AutoSecure Configuration ---
```

```
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
```

```
AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
```

```
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
```

```
Gathering information about the router for AutoSecure
```

```
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	down	down
FastEthernet0/1	192.168.30.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	manual	down	down
Serial0/0/1	10.2.2.2	YES	manual	up	up

Enter the interface name that is facing the internet: **Serial0/0/1**  
Securing Management plane services...

Disabling service finger  
Disabling service pad  
Disabling udp & tcp small servers  
Enabling service password encryption  
Enabling service tcp-keepalives-in  
Enabling service tcp-keepalives-out  
Disabling the cdp protocol

Disabling the bootp server  
Disabling the http server  
Disabling the finger service  
Disabling source routing  
Disabling gratuitous arp  
Enable secret is either not configured or  
Is the same as enable password  
Enter the new enable password: **ciscoccna**  
Confirm the enable password: **ciscoccna**  
Enter the new enable password: **ccnacisco**  
Confirm the enable password: **ccnacisco**

Configuration of local user database  
Enter the username: **ccna**  
Enter the password: **ciscoccna**  
Confirm the password: **ciscoccna**  
Configuring AAA local authentication  
Configuring Console, Aux and VTY lines for  
local authentication, exec-timeout, and transport  
Securing device against Login Attacks  
Configure the following parameters

Blocking Period when Login Attack detected: **300**

Maximum Login failures with the device: **5**

Maximum time period for crossing the failed login attempts: **120**

Configure SSH server? **Yes**  
Enter domain-name: **cisco.com**

Configuring interface specific AutoSecure services  
Disabling the following ip services on all interfaces:

no ip redirects  
no ip proxy-arp  
no ip unreachable  
no ip directed-broadcast  
no ip mask-reply  
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)  
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC firewall feature: **no**  
Tcp intercept feature is used prevent tcp syn attack  
On the servers in the network. Create autosec\_tcp\_intercept\_list  
To form the list of servers to which the tcp traffic is to be observed

Enable TCP intercept feature: **yes**

This is the configuration generated:

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
line vty 0 4
  login authentication local_auth
  transport input telnet
line tty 1
  login authentication local_auth
  exec-timeout 15 0
line tty 192
  login authentication local_auth
  exec-timeout 15 0
login block-for 300 attempts 5 within 120
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
```

```
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface FastEthernet0/1
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface Serial0/0/0
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
interface Serial0/0/1
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
interface Serial0/1/0
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
interface Serial0/1/1
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end

Apply this configuration to running-config? [yes]:yes

The name for the keys will be: R3.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

R3#

```
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

Comme vous pouvez le constater, la fonction AutoSecure permet une configuration plus rapide qu'une configuration ligne par ligne. Toutefois, la configuration manuelle présente également des avantages, que nous aborderons dans les travaux pratiques relatifs au dépannage. Lorsque vous utilisez la fonction AutoSecure, il se peut que vous désactiviez un service dont vous avez besoin. Soyez toujours très prudent et déterminez soigneusement les services dont vous avez besoin avant d'utiliser AutoSecure.

## Tâche 7 : gestion de Cisco IOS et des fichiers de configuration

### Étape 1 : affichage des fichiers IOS

Cisco IOS est le logiciel qui permet aux routeurs de fonctionner. Il se peut que votre routeur dispose de suffisamment de mémoire pour stocker plusieurs images Cisco IOS. Il est important de savoir quels fichiers sont stockés sur votre routeur.

Exécutez la commande **show flash** pour afficher le contenu de la mémoire flash de votre routeur.

Attention : soyez très prudent lorsque vous exécutez des commandes impliquant la mémoire flash. Une erreur dans la saisie d'une commande peut entraîner la suppression de l'image Cisco IOS.

R2#**show flash**

```
-#- --length-- -----date/time----- path
1      13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4      833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar
```

8679424 bytes available (23252992 bytes used)

En parcourant cette liste, vous pouvez déjà déterminer les éléments suivants :

- L'image est destinée à un routeur 1841 (c**1841**-ipbase-mz.124-1c.bin).
- Le routeur utilise une image de base IP (c**1841-ipbase**-mz.124-1c.bin).
- La version du logiciel Cisco IOS est 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin).
- SDM est installé sur ce périphérique (**sdmconfig**-18xx.cfg, **sdm**.tar).

Vous pouvez utiliser la commande **dir all** pour afficher tous les fichiers sur le routeur.

R2#**dir all**

Directory of archive:/

No files in directory

No space information available

Directory of system:/

```
 3  dr-x          0          <no date>  memory
 1  -rw-         979          <no date>  running-config
 2  dr-x          0          <no date>  vfiles
```

No space information available

Directory of nvram:/

```

189 -rw-          979          <no date> startup-config
190 ----          5          <no date> private-config
191 -rw-          979          <no date> underlying-config
  1 -rw-          0          <no date> ifIndex-table

```

196600 bytes total (194540 bytes free)

Directory of flash:/

```

 1 -rw- 13937472 May 05 2007 20:08:50 +00:00 c1841-ipbase-mz.124-1c.bin
 2 -rw-      1821 May 05 2007 20:25:00 +00:00 sdmconfig-18xx.cfg
 3 -rw- 4734464 May 05 2007 20:25:38 +00:00 sdm.tar
 4 -rw-  833024 May 05 2007 20:26:02 +00:00 es.tar
 5 -rw- 1052160 May 05 2007 20:26:30 +00:00 common.tar
 6 -rw-   1038 May 05 2007 20:26:56 +00:00 home.shtml
 7 -rw-  102400 May 05 2007 20:27:20 +00:00 home.tar
 8 -rw-  491213 May 05 2007 20:27:50 +00:00 128MB.sdf
 9 -rw-  398305 May 05 2007 20:29:08 +00:00 sslclient-win-1.1.0.154.pkg
10 -rw- 1684577 May 05 2007 20:28:32 +00:00 securedesktop-ios-3.1.1.27-
k9.pkg

```

31932416 bytes total (8679424 bytes free)

## Étape 2 : transfert des fichiers via le protocole TFTP

Le protocole TFTP est utilisé lors de l'archivage et de la mise à jour du logiciel Cisco IOS d'un périphérique. Cependant, dans ces travaux pratiques, nous n'utilisons pas des fichiers Cisco IOS réels car toute erreur commise lors de la saisie d'une commande peut entraîner la suppression de l'image Cisco IOS du périphérique. À la fin de cette section, vous trouverez un exemple de transfert TFTP de fichiers Cisco IOS.

Pourquoi est-il important de disposer d'une version actualisée du logiciel Cisco IOS ?

---

Lors d'un transfert de fichiers via TFTP, il est important de vérifier la communication entre le serveur TFTP et le routeur. Pour ce faire, exécutez une requête ping entre ces deux périphériques.

Pour commencer le transfert du logiciel Cisco IOS, créez un fichier nommé **test** sur le serveur TFTP, dans le dossier racine TFTP. Ce fichier peut être vide, car cette étape sert uniquement à illustrer les étapes effectuées. Chaque programme TFTP stocke les fichiers dans un emplacement différent. Consultez le fichier d'aide du serveur TFTP pour déterminer le dossier racine.

À partir de R1, procédez à l'extraction du fichier et enregistrez-le dans la mémoire flash.

R2#**copy tftp flash**

Address or name of remote host []? **192.168.20.254** (adresse IP du serveur TFTP)

Source filename []? **Test** (nom du fichier que vous avez créé et enregistré sur le serveur TFTP)

Destination filename [test]? **test-server** (nom arbitrairement attribué au fichier lors de son enregistrement sur le routeur)

Accessing tftp://192.168.20.254/test...

Loading test from 192.168.20.254 (via FastEthernet0/1): !

[OK - 1192 bytes]



```
1192 bytes copied in 0.424 secs (2811 bytes/sec)
```

Vérifiez l'existence du fichier dans la mémoire flash à l'aide de la commande **show flash**.

```
R2#show flash
```

```

-- --length-- -----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11     1192 Sep 12 2007 07:38:18 +00:00 test-server

```

```
8675328 bytes available (23257088 bytes used)
```

Les routeurs peuvent également agir comme des serveurs TFTP. Cela peut être utile si un périphérique a besoin d'une image et que l'un de vos périphériques utilise déjà cette image. Configurons R2 en tant que serveur TFTP de R1. Notez que les images Cisco IOS sont spécifiques aux plates-formes de routeur et aux besoins en matière de mémoire. Soyez prudent lorsque vous transférez une image Cisco IOS d'un routeur à l'autre.

La syntaxe de commande est la suivante : **tftp-server nvram: [nomfichier1 [alias nomfichier2]**

La commande ci-après permet de configurer R2 en tant que serveur TFTP. R2 envoie son fichier de configuration de démarrage aux périphériques qui le demandent, via TFTP (nous utilisons la configuration de démarrage pour une question de simplicité). Le mot-clé **alias** permet aux périphériques de demander le fichier en utilisant l'alias **test** au lieu du nom de fichier complet.

```
R2 (config) #tftp-server nvram:startup-config alias test
```

À présent, nous pouvons demander le fichier à partir de R2 en utilisant R1.

```
R1#copy tftp flash
```

```

Address or name of remote host []? 10.1.1.2
Source filename []? test
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]

```

```
1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

Vérifiez une nouvelle fois que le fichier **test** a été correctement copié à l'aide de la commande **show flash**.

```
R1#show flash
```

```

-- --length-- -----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml

```

```
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11      1192 Sep 12 2007 07:38:18 +00:00 test-server
12     1192 Sep 12 2007 07:51:04 +00:00 test-router
```

8671232 bytes available (23261184 bytes used)

À présent, supprimez les fichiers inutiles de la mémoire flash de R1, pour éviter d'utiliser trop d'espace mémoire. **Soyez particulièrement prudent lorsque vous effectuez cette opération !** La suppression accidentelle de la mémoire flash vous obligerait à réinstaller l'ensemble de l'image IOS du routeur. Si le routeur vous invite à supprimer la mémoire flash, via **erase flash**, cela indique qu'il se passe quelque chose d'anormal. Il est extrêmement rare de devoir supprimer l'ensemble de la mémoire flash. Le seul cas légitime où cela peut se produire est lors de la mise à niveau du système IOS vers une grande image IOS. Si l'invite **erase flash** s'affiche comme dans l'exemple, ARRÊTEZ IMMÉDIATEMENT. Ne validez PAS. Demandez IMMÉDIATEMENT l'aide de votre formateur.

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

Vérifiez que les fichiers ont été supprimés à l'aide de la commande **show flash**. Ceci est seulement un exemple. N'effectuez pas cette tâche.

```
R1#show flash
#- --length-- -----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
```

8679424 bytes available (23252992 bytes used)

Voici un exemple de transfert TFTP d'un fichier d'image Cisco IOS.

**N'effectuez PAS cet exemple sur vos routeurs. Lisez-le simplement.**

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
```

```
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via Serial0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<résultat omis>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]
```

```
13937472 bytes copied in 1113.948 secs (12512 bytes/sec)
```

### Étape 3 : restauration d'un mot de passe à l'aide de ROMmon

Si, pour une raison quelconque, vous ne parvenez plus à accéder à un périphérique car vous ignorez, avez perdu ou oublié le mot de passe, vous pouvez encore y accéder en modifiant le registre de configuration. Le registre de configuration indique au routeur la configuration à charger lors du démarrage. Dans le registre de configuration, vous pouvez demander au routeur de démarrer à partir d'une configuration vierge, non protégée par un mot de passe.

Pour modifier le registre de configuration, la première étape consiste à afficher le paramètre actuel, à l'aide de la commande **show version**. Ces opérations sont exécutées sur le routeur R3.

```
R3#show version
```

```
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller
```

```
ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
```

```
R3 uptime is 25 minutes
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"
```

```
Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
Processor board ID FTX1118X0BN
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)
```

Configuration register is 0x2102

La seconde étape consiste à recharger le routeur et à appuyer sur la touche Pause, lors du démarrage. L'emplacement de la touche **Pause** est différente d'un ordinateur à l'autre. En général, elle se trouve dans le coin supérieur droit du clavier. Une pause permet au périphérique de basculer en mode appelé ROMmon. Dans ce mode, il n'est pas nécessaire que le périphérique ait accès à un fichier d'image Cisco IOS.

```
R3#reload
```

```
Proceed with reload? [confirm]
```

```
*Sep 12 08:27:280.670: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload command.
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
```

```
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled
```

```
Readonly ROMMON initialized
rommon 1 >
```

Modifiez la valeur du registre de configuration par une valeur permettant de charger la configuration initiale du routeur. Cette configuration ne dispose pas de mot de passe configuré, mais elle prend en charge les commandes Cisco IOS. Définissez la valeur du registre de configuration sur 0x2142.

```
rommon 1 > confreg 0x2142
```

La valeur du registre étant modifiée, vous pouvez démarrer le périphérique à l'aide de la commande **reset**.

```
rommon 2 > reset
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0xd4a9a0
Self decompressing the image :
#####
#####
# [OK]
```

<résultat omis>

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Press RETURN to get started!

#### Étape 4 : restauration du routeur

À présent, copiez la configuration de démarrage vers la configuration en cours, restaurez cette configuration, puis rétablissez le registre de configuration à sa valeur par défaut (0x2102).

Pour copier la configuration de démarrage de la mémoire NVRAM vers la mémoire en cours, entrez la commande **copy startup-config running-config**. Attention : *ne saisissez pas* la commande **copy running-config startup-config**, car vous risquez de supprimer la configuration de démarrage.

```
Router#copy startup-config running-config
Destination filename [running-config]? {enter}

2261 bytes copied in 0.576 secs (3925 bytes/sec)
```

```
R3# :show running-config
<résultat omis>
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
!
<résultat omis>
!
```

```
key chain RIP_KEY
  key 1
    key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/1
  ip address 192.168.30.1 255.255.255.0
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  no ip directed-broadcast
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/1
  ip address 10.2.2.2 255.255.255.252
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  no ip directed-broadcast
  shutdown
  ip rip authentication mode md5
  ip rip authentication key-chain RIP_KEY
!
<résultat omis>
!
line con 0
  exec-timeout 5 0
  logging synchronous
  login authentication
  transport output telnet
line aux 0
  exec-timeout 15 0
  logging synchronous
  login authentication local_auth
  transport output telnet
line vty 0 4
  exec-timeout 15 0
  logging synchronous
  login authentication local_auth
  transport input telnet
!
end
```

Dans cette configuration, la commande **shutdown** s'affiche sur toutes les interfaces, car ces interfaces sont toutes fermées. Le plus important est que vous puissiez voir les mots de passe (enable, enable secret, VTY, console) au format chiffré ou non. Vous pouvez réutiliser les mots de passe non chiffrés. Vous devez remplacer les mots de passe chiffrés par un nouveau mot de passe.

#### R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)#enable secret ciscoccna
```

```
R3(config)#username ccna password ciscoccna
```

Exécutez la commande **no shutdown** sur chaque interface que vous souhaitez utiliser.

```
R3(config)#interface FastEthernet0/1
R3(config-if)#no shutdown
R3(config)#interface Serial0/0/0
R3(config-if)#no shutdown
```

Vous pouvez exécuter une commande **show ip interface brief** afin de confirmer que la configuration de votre interface est correcte. Chacune des interfaces que vous souhaitez utiliser doit afficher « up ».

```
R3#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet0/1	192.168.30.1	YES	NVRAM	up	up
Serial0/0/0	10.2.2.2	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	NVRAM	administratively down	down

Entrez la commande **config-register** valeur du registre de configuration. La variable valeur du registre de configuration peut être la valeur que vous avez notée à l'étape 3 ou 0x2102. Enregistrez la configuration en cours.

```
R3(config)#config-register 0x2102
R3(config)#end
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Quels sont les inconvénients d'une récupération de mot de passe ?

---



---



---

## Tâche 8 : utilisation de SDM pour la sécurisation d'un routeur

Au cours de cette tâche, vous allez utiliser SDM (Security Device Manager) et l'interface utilisateur graphique pour sécuriser le routeur R2. L'utilisation de SDM est plus rapide que la saisie de chaque commande et vous permet davantage de contrôle que la fonction AutoSecure.

Vérifiez si SDM est installé sur le routeur :

```
R2#show flash
-#- --length-- -----date/time----- path
1      13937472 Sep 12 2007 08:31:42 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6        1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11         2261 Sep 25 2007 23:20:16 +00:00 Tr (RIP)
12       2506 Sep 26 2007 17:11:58 +00:00 save.txt
```

**Si SDM N'est PAS installé sur le routeur, vous devez l'installer pour continuer la procédure. Pour ce faire, demandez les instructions à votre formateur.**

### Étape 1 : connexion à R2 via le serveur TFTP

Créez un nom d'utilisateur et un mot de passe sur R2.

```
R2(config)#username ccna password ciscoccna
```

Activez le serveur sécurisé http sur R2, puis connectez-vous à R2 à l'aide d'un navigateur Web sur le serveur TFTP.

```
R2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue "write memory" to save new certificate
R2(config)#end
R2#copy run start
```

À partir du serveur TFTP, ouvrez un navigateur Web et accédez à <https://192.168.20.1/>. Connectez-vous avec le nom d'utilisateur et le mot de passe créés précédemment :

Nom d'utilisateur : **ccna**

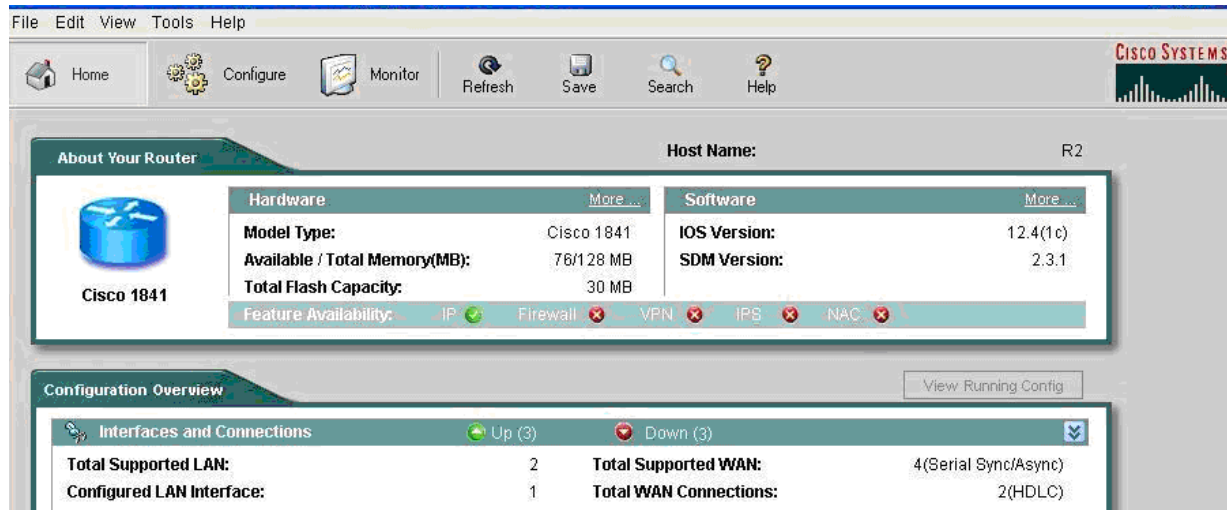
Mot de passe : **ciscoccna**

Sélectionnez l'application **Cisco Router and Security Device Manager**.

Ouvrez Internet Explorer et entrez l'adresse IP de R2 dans la barre d'adresse. Une nouvelle fenêtre s'ouvre. Assurez-vous que tous les bloqueurs de fenêtre publicitaire intempestive sont désactivés sur votre navigateur. Assurez-vous également que JAVA est bien installé et mis à jour.

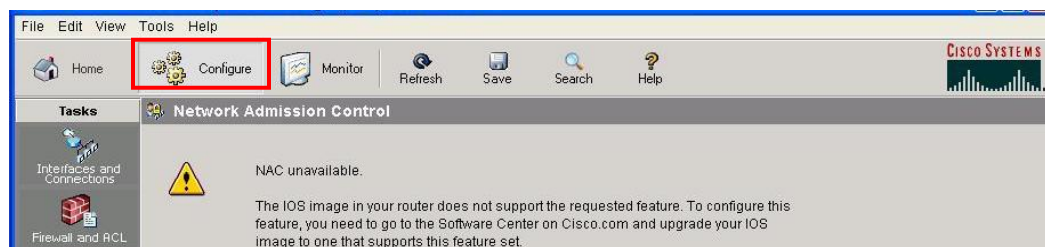


Une fois le chargement effectué, une nouvelle fenêtre SDM s'ouvre.

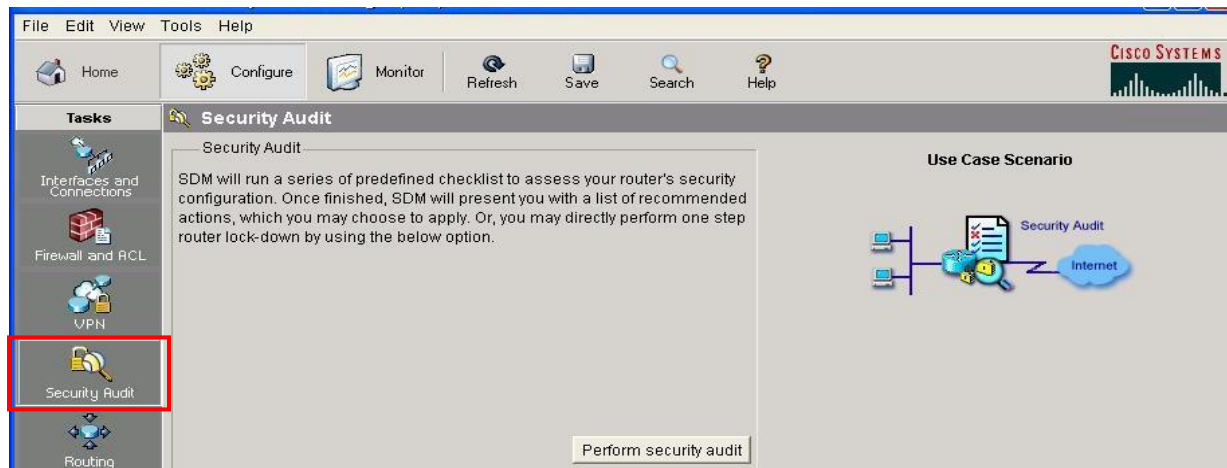


## Étape 2 : accès à la fonction d'audit de sécurité

Cliquez sur le bouton **Configure** dans la partie supérieure gauche de la fenêtre.



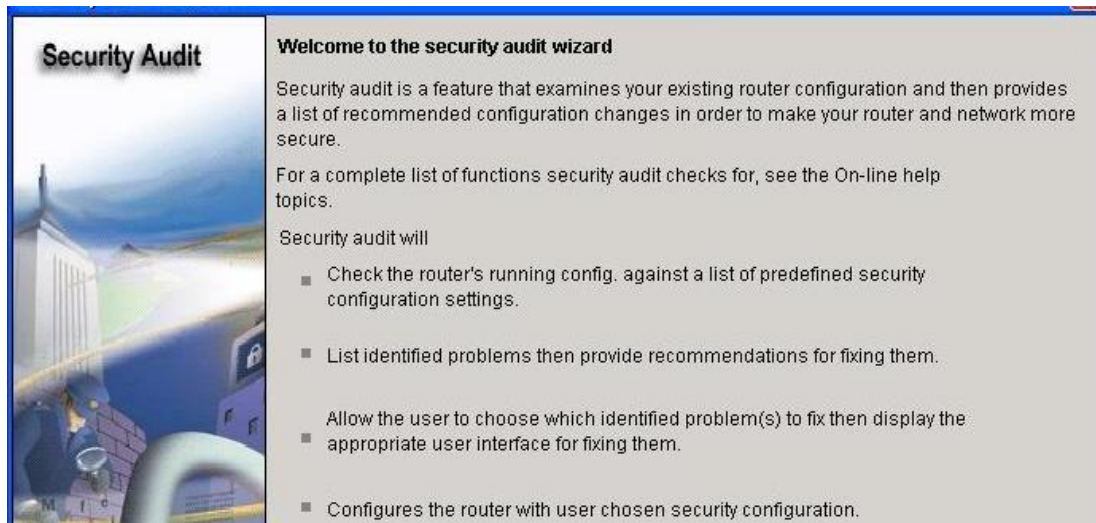
Cliquez ensuite sur **Security Audit**, dans le panneau de gauche.



Une autre fenêtre s'ouvre.



### Étape 3 : exécution d'un audit de sécurité

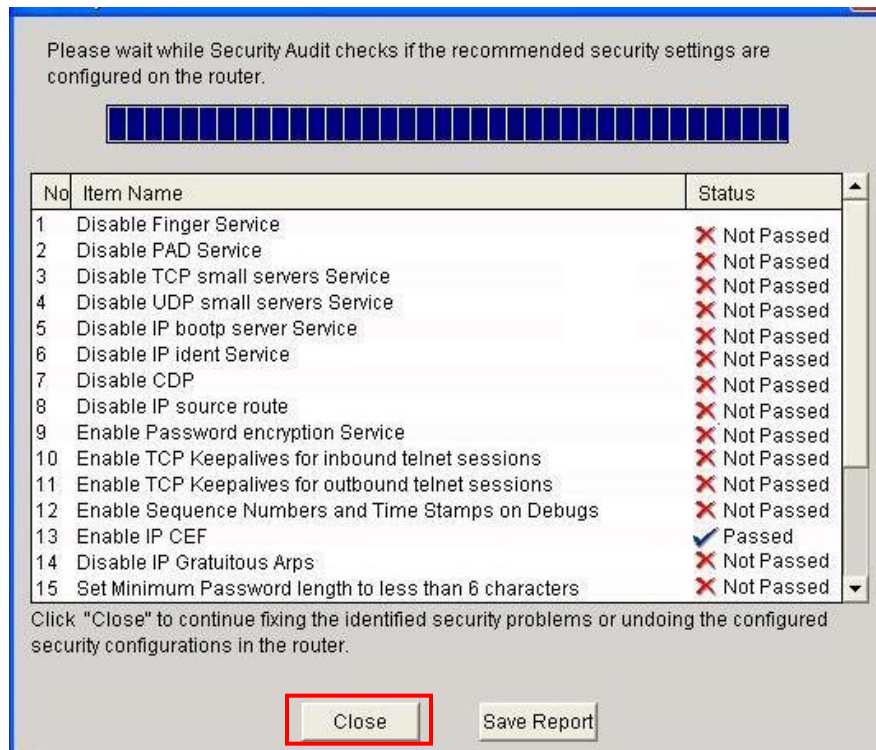


Une brève présentation de la fonction d'audit de sécurité s'affiche. Cliquez sur **Next** pour ouvrir la fenêtre de configuration de l'interface de la fonction d'audit de sécurité, Security Audit Interface configuration.



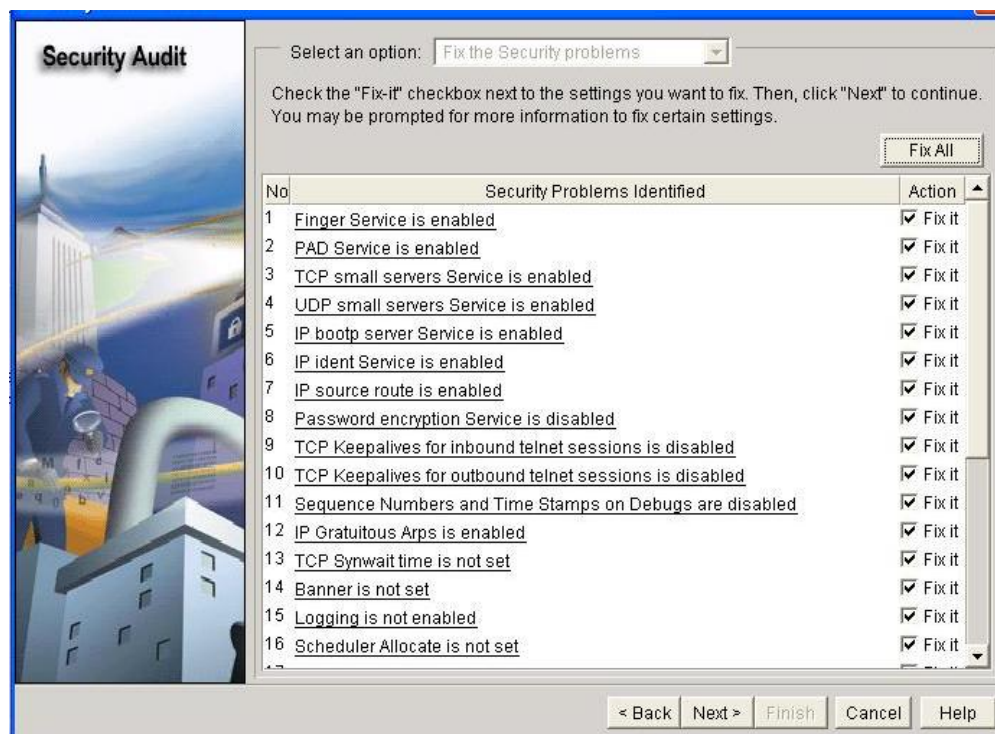
Une interface doit être définie sur Outside (Untrusted) (non fiable) si vous ne pouvez garantir la légitimité du trafic issu de cette interface. Dans cet exemple, les interfaces FastEthernet0/1 et Serial0/1/0 ne sont pas fiables. D'une part, Serial0/1/0 est directement connecté à Internet. D'autre part, Fastethernet0/1 est connecté à la partie accès au réseau. Un trafic illégitime peut donc s'infiltrer.

Après avoir défini les interfaces sur Outside (extérieure) et Inside (intérieure), cliquez sur **Next**. Une nouvelle fenêtre s'ouvre, indiquant que SDM est en train d'effectuer un audit de sécurité.

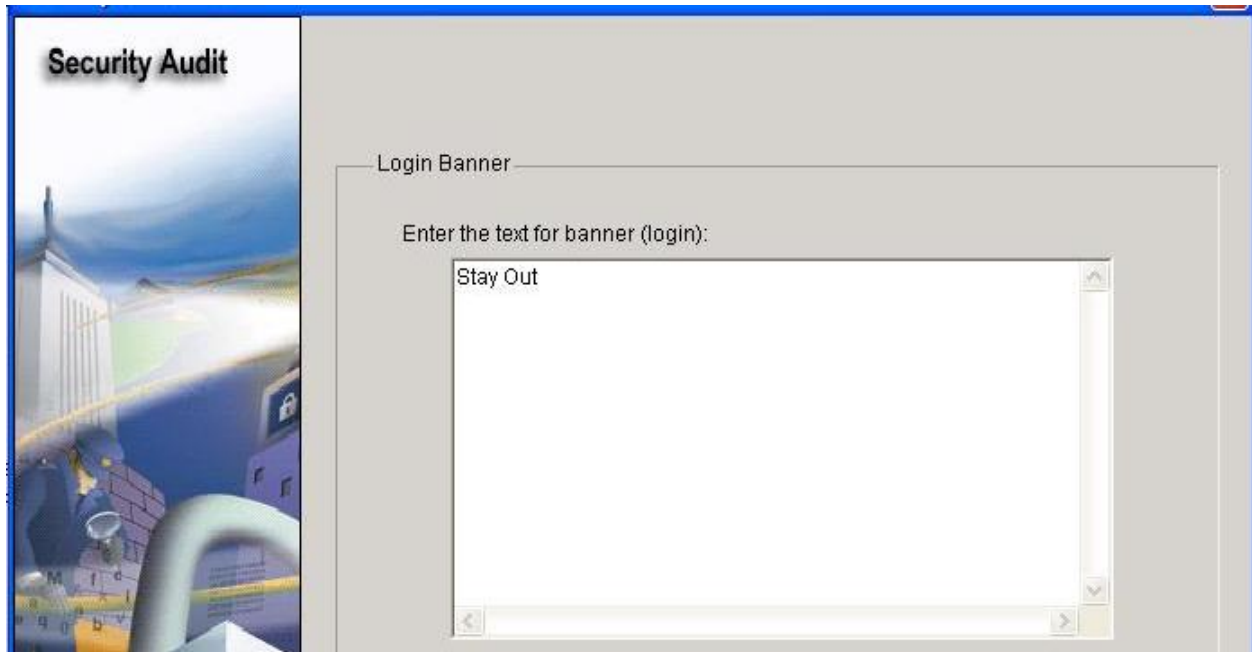


Comme vous pouvez le constater, la configuration par défaut n'est pas sécurisée. Cliquez sur le bouton **Close** pour continuer.

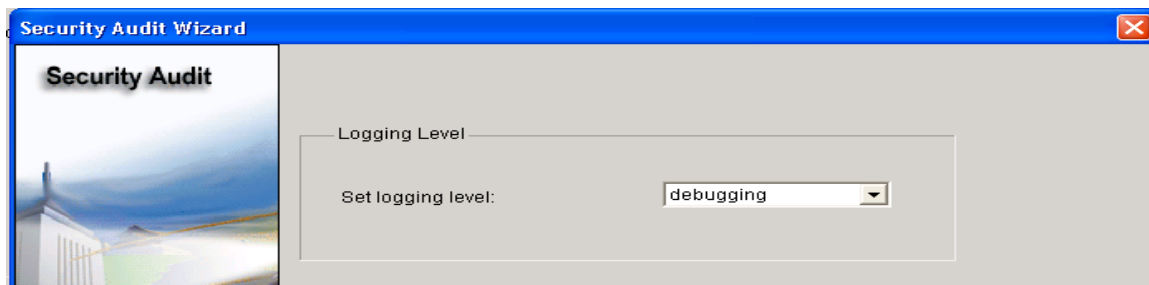
#### Étape 4 : application des paramètres au routeur



Cliquez sur le bouton **Fix All** pour appliquer toutes les corrections de sécurité proposées. Ensuite, cliquez sur le bouton **Next**.

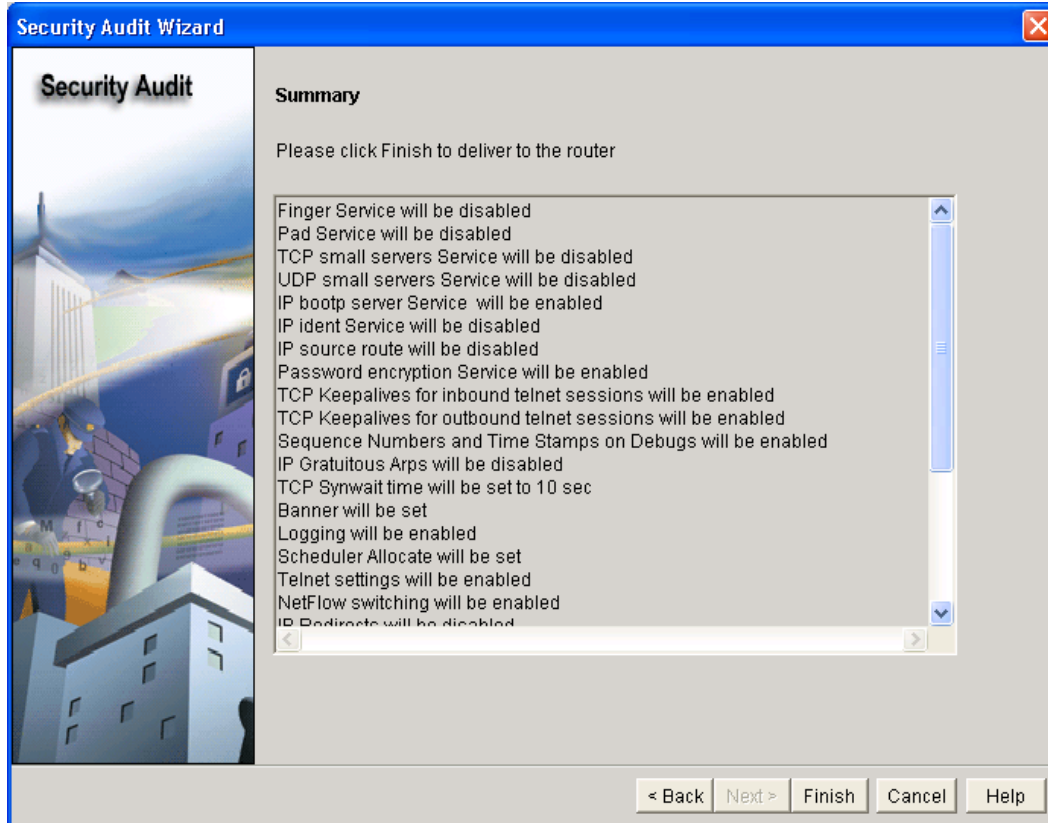


Configurez un message de bannière à utiliser comme message du jour pour le routeur, puis cliquez sur **Next**.

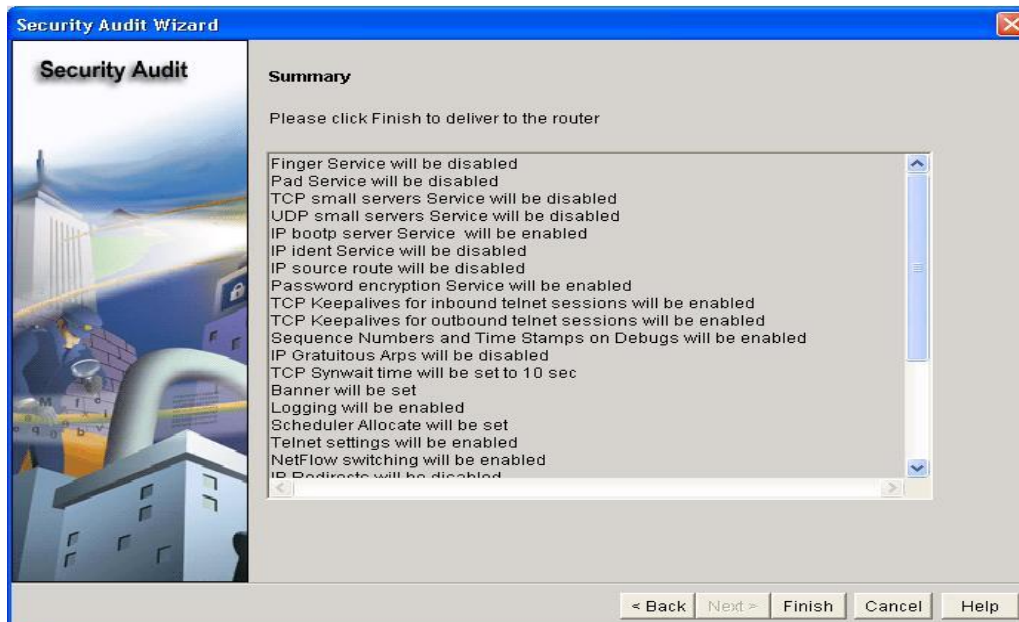


Déterminez ensuite le niveau de gravité des journaux de déROUTement que le routeur devra envoyer au serveur syslog. Dans ce scénario, le niveau de gravité est défini sur le débogage. Cliquez sur **Next** pour afficher un récapitulatif des modifications sur le point d'être apportées au routeur.

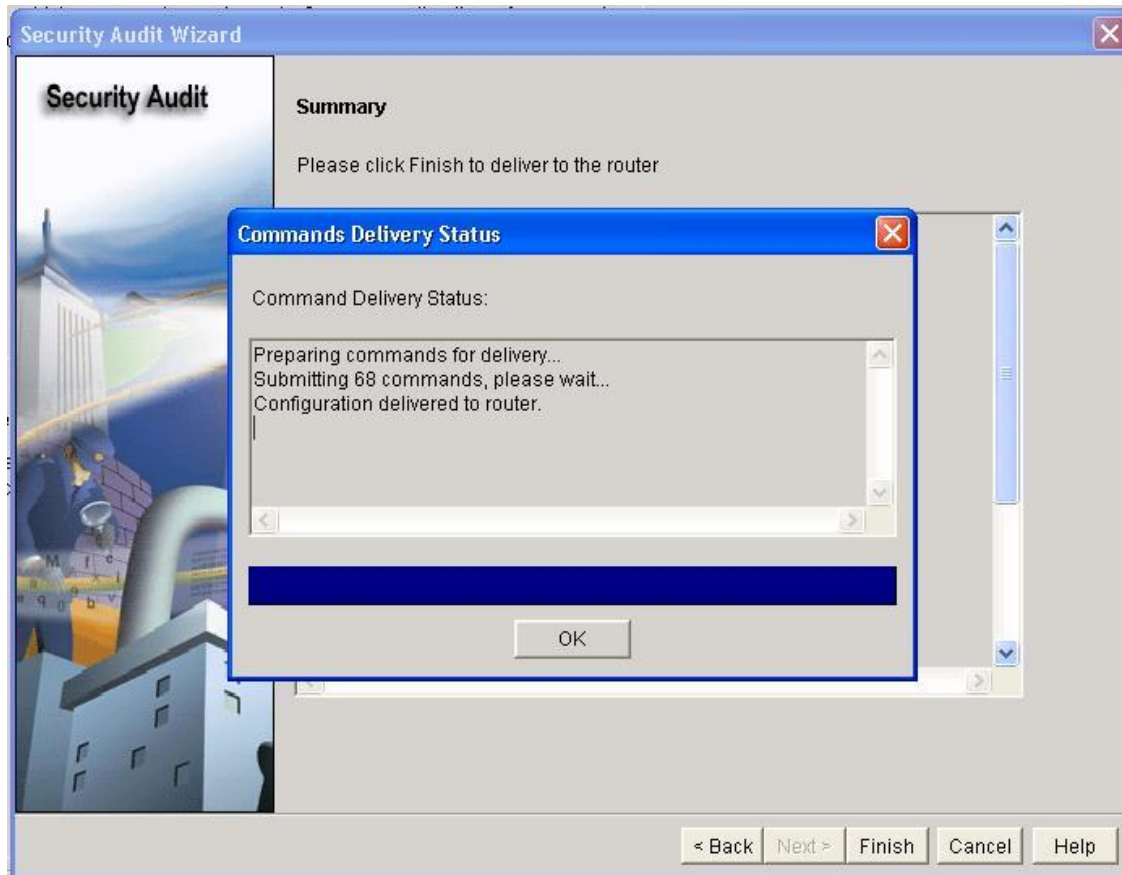
## Étape 5 : validation de la configuration du routeur



Après avoir vérifié les modifications sur le point d'être effectuées, cliquez sur **Finish**.







Cliquez sur **OK** pour quitter SDM.

### Tâche 9 : documentation des configurations des routeurs

Exécutez la commande **show run** sur chaque routeur et capturez les configurations.

### Tâche 10 : remise en état

Supprimez les configurations et rechargez les routeurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les PC hôtes habituellement connectés aux autres réseaux (réseaux locaux de votre site ou Internet).

## Annexe : installation de SDM

### Diagramme de topologie



### Scénario

Au cours de ces travaux pratiques, vous allez préparer l'accès au routeur via Cisco Security Device Manager (SDM), à l'aide de commandes de base, afin d'établir une connectivité entre SDM et le routeur. Vous installerez ensuite l'application SDM en local sur votre PC hôte. Enfin, vous installerez SDM dans la mémoire flash d'un routeur.

### Étape 1 : préparation

Pour commencer ces travaux pratiques, supprimez toutes les configurations existantes et rechargez les périphériques. Une fois les périphériques rechargés, définissez les noms d'hôte appropriés. Vérifiez si le commutateur est correctement configuré, de sorte que le routeur et l'hôte soient situés sur le même réseau local virtuel. Par défaut, tous les ports du commutateur sont assignés au réseau local virtuel VLAN 1.

Assurez-vous que votre PC dispose de la configuration minimale requise pour la prise en charge de SDM. SDM peut être installé sur un PC exécutant l'un des systèmes d'exploitation suivants :

- Microsoft Windows ME
- Microsoft Windows NT 4.0 Workstation avec Service Pack 4
- Microsoft Windows XP Professionnel
- Microsoft Windows 2003 Server (Standard Edition)
- Microsoft Windows 2000 Professionnel avec Service Pack 4

Remarque : Windows 2000 Advanced Server n'est pas pris en charge.

En outre, un navigateur Web utilisant SUN JRE version 1.4 ou ultérieure, ou un navigateur ActiveX, doit être activé.

### Étape 2 : préparation du routeur pour SDM

Pour commencer, créez, sur le routeur, un nom d'utilisateur et un mot de passe que vous utiliserez pour SDM. Cette connexion doit bénéficier d'un niveau de privilège défini sur 15, afin de permettre à SDM de modifier des paramètres de configuration sur le routeur.

```
R1(config)# username ciscosdm privilege 15 password 0 ciscosdm
```

L'accès HTTP au routeur doit être configuré pour permettre l'exécution de SDM. Si votre image le prend en charge (vous devez disposer d'une image IOS qui prend en charge la fonction de chiffrement), vous devez également activer un accès HTTPS sécurisé, à l'aide de la commande **ip http secure-server**. L'activation du protocole HTTPS se répercute sur les clés de chiffrement

RSA. Cela est normal. Assurez-vous également que le serveur HTTP utilise la base données locale lors du processus d'authentification.

```
R1(config)# ip http server
R1(config)# ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Jan 14 20:19:45.310: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan 14 20:19:46.406: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue "write memory" to save new certificate
R1(config)# ip http authentication local
```

Pour terminer, configurez les lignes de terminal virtuel du routeur afin de procéder à l'authentification par l'intermédiaire de la base de données d'authentification locale. Autorisez l'entrée de lignes de terminal virtuel via les protocoles Telnet et SSH.

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

### Étape 3 : configuration de l'adressage

Configurez l'interface Fast Ethernet sur le routeur, avec l'adresse IP indiquée sur le diagramme. Si vous avez déjà configuré l'adresse IP adéquate, ignorez cette étape.

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

Attribuez ensuite une adresse IP au PC. Si le PC dispose déjà d'une adresse IP dans le même sous-réseau que le routeur, vous pouvez ignorer cette étape.

Exécutez une requête ping sur l'interface Ethernet de R1 depuis le PC. Vous devez recevoir des réponses. Dans le cas contraire, vérifiez le réseau local virtuel des ports de commutation, ainsi que l'adresse IP et le masque de sous-réseau de chaque périphérique connecté au commutateur.

### Étape 4 : extraction de SDM sur l'hôte

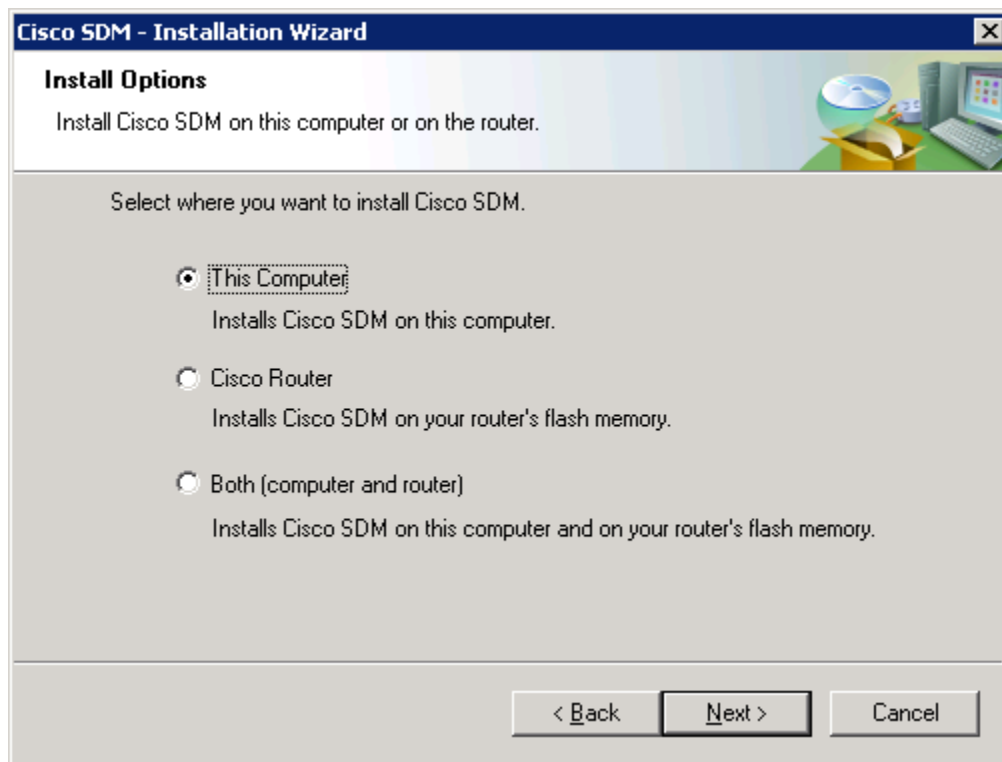
À présent, le routeur est configuré pour être accessible à partir de SDM et la connectivité est établie entre le routeur et le PC. Vous pouvez dès lors configurer le routeur à l'aide de SDM. Vous devez commencer par l'extraction du fichier zip de SDM vers un répertoire de votre disque dur. Dans cet exemple, nous utilisons le répertoire « C:\sdm\ ». Vous pouvez bien entendu utiliser le chemin de votre choix.

Le logiciel SDM est quasiment prêt pour la configuration du routeur. La dernière étape consiste à l'installer sur le PC.

### Étape 5 : installation de l'application SDM sur le PC

Double-cliquez sur le programme exécutable **setup.exe** pour ouvrir l'assistant d'installation. Une fois l'assistant affiché, cliquez sur **Next**. Acceptez les termes du contrat de licence, puis cliquez sur **Next**.

Sur l'écran suivant, choisissez un emplacement d'installation de SDM parmi les trois emplacements proposés.



Vous pouvez installer l'application SDM sur l'ordinateur, sans la placer dans la mémoire flash du routeur, vous pouvez l'installer sur le routeur sans affecter l'ordinateur ou vous pouvez l'installer à la fois sur le routeur et sur l'ordinateur. Ces différents types d'installation sont très similaires. Si vous ne souhaitez pas installer SDM sur votre ordinateur, passez directement à l'étape 7.

Sinon, cliquez sur **This Computer**, puis sur **Next**. Utilisez le répertoire de destination par défaut, puis cliquez à nouveau sur **Next**.

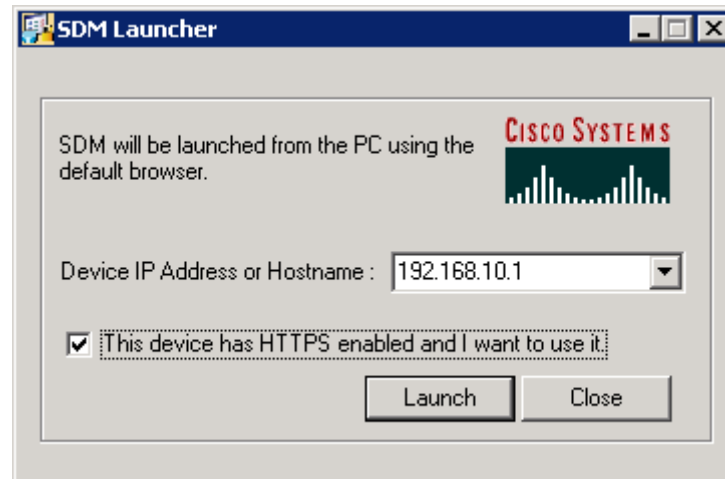
Cliquez sur **Install** pour démarrer l'installation.

Le logiciel procède à l'installation, puis une dernière boîte de dialogue vous invite à lancer SDM. Activez la case à cocher **Launch Cisco SDM**, puis cliquez sur **Finish**.

## Étape 6 : exécution de SDM depuis l'ordinateur

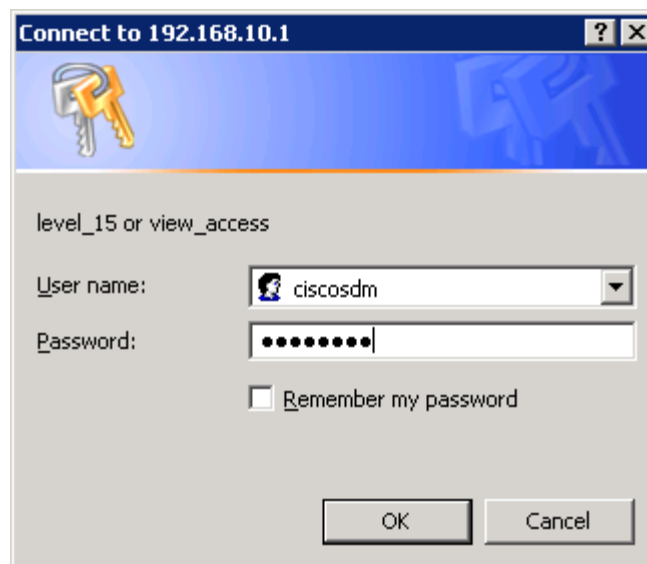
Si vous avez activé l'option Launch Cisco SDM lors de l'étape 5, l'application SDM doit se lancer depuis le programme d'installation. Dans le cas contraire, ou si vous exécutez SDM sans l'avoir installé, cliquez sur l'icône **Cisco SDM** sur le bureau. La boîte de dialogue de démarrage de l'application SDM s'affiche. Renseignez l'adresse IP du routeur, indiquée dans le diagramme, en tant qu'adresse IP du périphérique. Si vous avez activé le serveur sécurisé HTTP lors de l'étape 2, activez la case à cocher **This device has HTTPS enabled and I want to use it**.



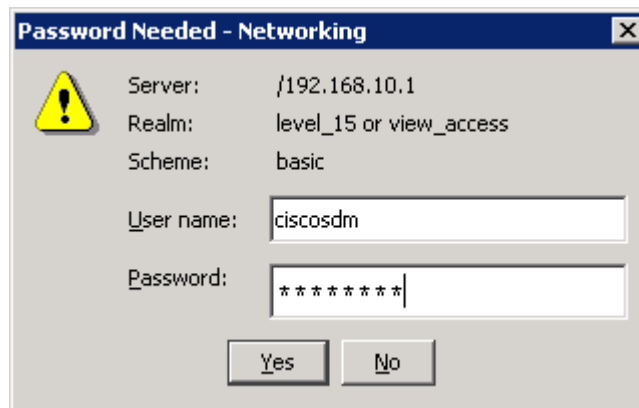


Cliquez sur **Yes** lorsque le message d'avertissement de sécurité s'affiche. Sachez qu'au début, Internet Explorer peut bloquer l'application SDM. Vous devez alors l'autoriser ou modifier les paramètres de sécurité d'Internet Explorer pour pouvoir l'utiliser. Selon la version d'Internet Explorer que vous utilisez, l'un de ces paramètres est tout particulièrement important pour exécuter SDM en local. Ce paramètre se trouve dans le menu **Outils**, sous **Options Internet**. Cliquez sur l'onglet **Avancé**, puis sous l'en-tête **Sécurité**, activez la case à cocher **Autoriser le contenu actif à s'exécuter dans les fichiers de la zone Ordinateur local**.

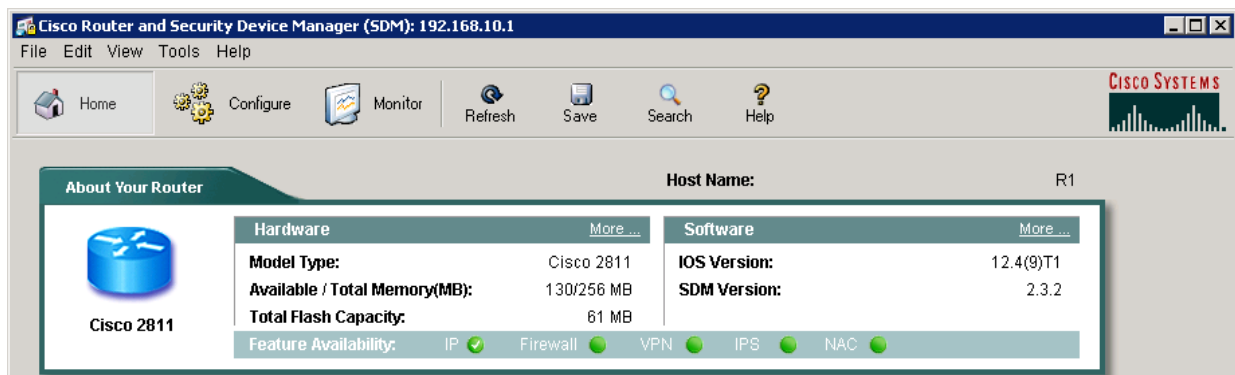
Entrez le nom d'utilisateur et le mot de passe que vous avez créés auparavant.



Vous pouvez être amené à accepter un certificat provenant de ce routeur. Pour continuer, acceptez le certificat. Entrez ensuite le nom d'utilisateur et le mot de passe du routeur, puis cliquez sur **Yes**.



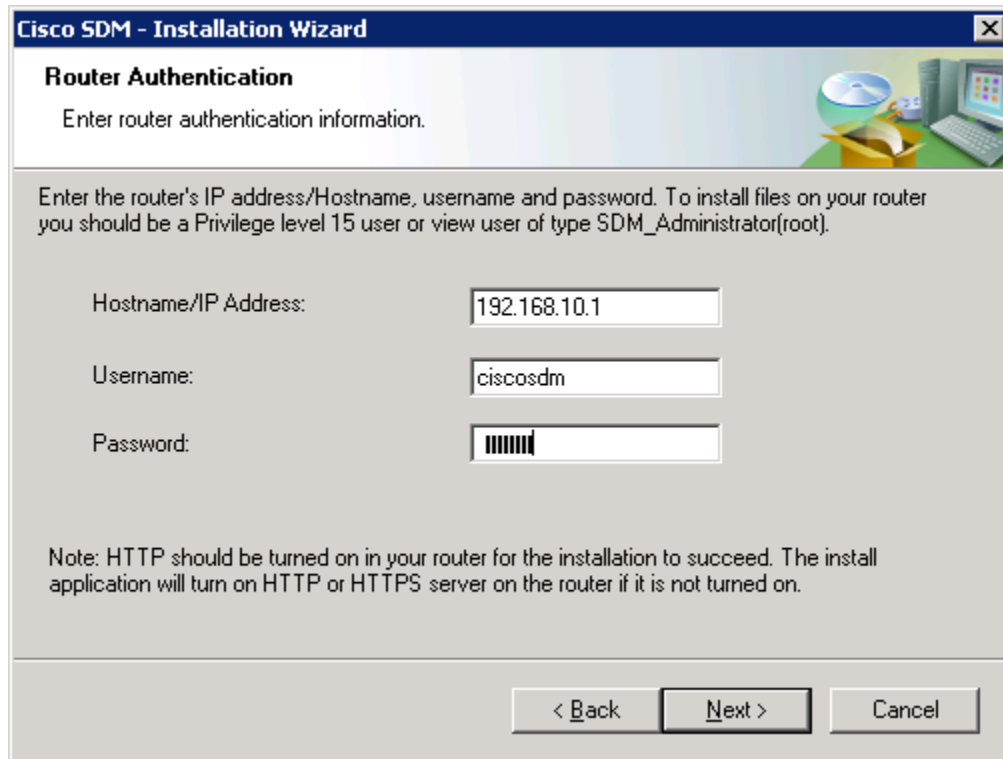
SDM procède à la lecture de la configuration à partir du routeur. Si la configuration ne présente aucune erreur, vous pourrez accéder au tableau de bord de l'application de SDM. Si la configuration affichée vous semble correcte, cela signifie que vous avez réussi à configurer SDM et à vous y connecter. Les informations affichées peuvent varier en fonction de la version de SDM utilisée.



## Étape 7 : installation de SDM sur le routeur

Effectuez les instructions de l'étape 6 jusqu'à ce que l'invite présentée dans la figure suivante s'affiche. Lorsque cette fenêtre s'affiche, cliquez sur **Cisco Router** pour installer SDM dans la mémoire flash du routeur. Si vous ne souhaitez pas installer SDM dans la mémoire flash du routeur, ou si l'espace disponible en mémoire flash est insuffisant, n'essayez pas d'installer SDM sur le routeur.

Entrez les informations relatives au routeur afin de permettre au programme d'installation d'installer SDM sur le routeur et d'y accéder à distance.



The image shows a screenshot of the 'Cisco SDM - Installation Wizard' window, specifically the 'Router Authentication' step. The window has a blue title bar with the text 'Cisco SDM - Installation Wizard' and a close button. Below the title bar, the text 'Router Authentication' is displayed in bold, followed by the instruction 'Enter router authentication information.' To the right of this text is a small graphic of a CD, a router, and a laptop. Below this, a larger text block states: 'Enter the router's IP address/Hostname, username and password. To install files on your router you should be a Privilege level 15 user or view user of type SDM\_Administrator(root).' There are three input fields: 'Hostname/IP Address:' with the value '192.168.10.1', 'Username:' with the value 'ciscosdm', and 'Password:' with a masked password represented by eight asterisks. Below these fields is a note: 'Note: HTTP should be turned on in your router for the installation to succeed. The install application will turn on HTTP or HTTPS server on the router if it is not turned on.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Cisco SDM - Installation Wizard**

**Router Authentication**

Enter router authentication information.

Enter the router's IP address/Hostname, username and password. To install files on your router you should be a Privilege level 15 user or view user of type SDM\_Administrator(root).

Hostname/IP Address: 192.168.10.1

Username: ciscosdm

Password: [masked]

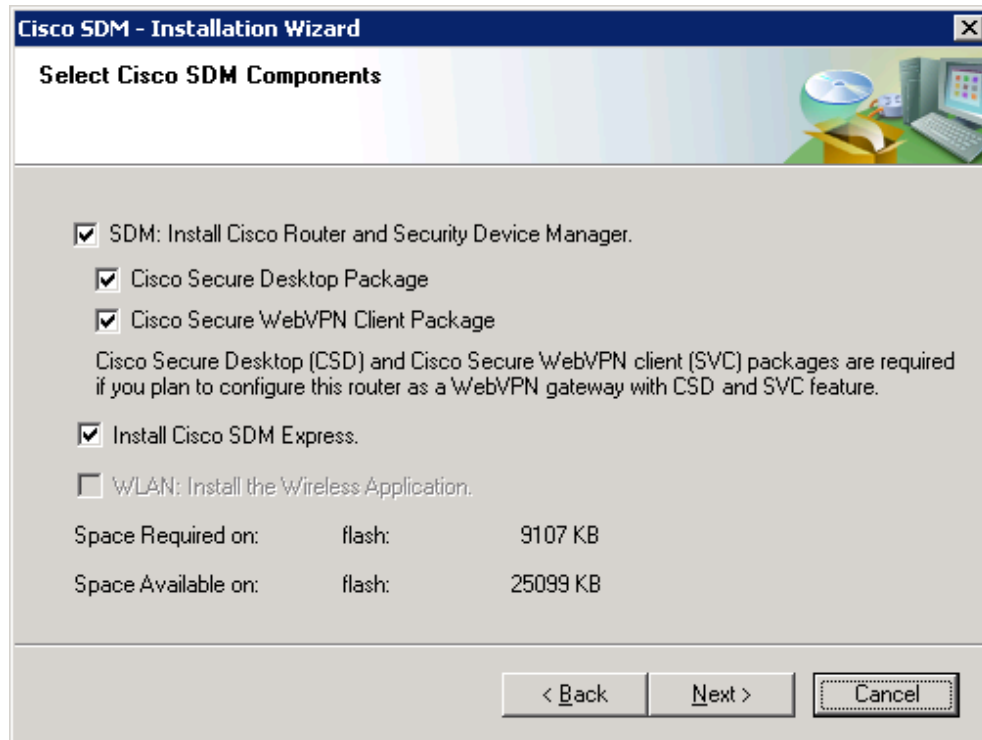
Note: HTTP should be turned on in your router for the installation to succeed. The install application will turn on HTTP or HTTPS server on the router if it is not turned on.

< Back Next > Cancel

Cisco SDM se connecte au routeur. Certains messages consignés dans la console peuvent s'afficher. Cela est normal.

```
Jan 14 16:15:26.367: %SYS-5-CONFIG_I: Configured from console by  
ciscosdm on vty0 (192.168.10.50)
```

Choisissez **Typical** comme type d'installation, puis cliquez sur **Next**. Conservez les options d'installation par défaut, puis cliquez sur **Next**.



Cliquez enfin sur **Install** pour lancer le processus d'installation. Au cours de l'installation, d'autres messages peuvent être consignés dans la console. Le processus d'installation peut prendre un certain temps (observez les horodatages affichés sur la sortie de la console pour estimer la durée du processus sur un Cisco 2811). La durée du processus varie selon le modèle du routeur.

```
Jan 14 16:19:40.795: %SYS-5-CONFIG_I: Configured from console by
ciscosdm on vty0 (192.168.10.50)
```

À la fin de l'installation, vous êtes invité à lancer SDM sur le routeur. Avant d'effectuer cette opération, accédez à la console et exécutez la commande **show flash:**. Notez tous les fichiers stockés par SDM dans la mémoire flash. Avant l'installation, le premier fichier, c'est-à-dire l'image IOS, était le seul répertorié.

```
R1# show flash:
```

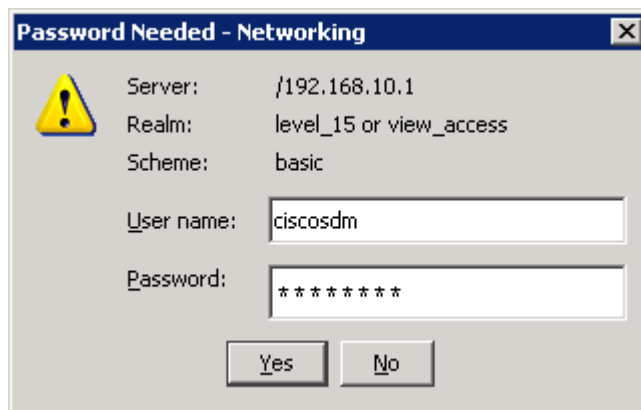
```
CompactFlash directory:
File Length Name/status
  1 38523272 c2800nm-advipservicesk9-mz.124-9.T1.bin
  2 1038 home.shtml
  3 1823 sdmconfig-2811.cfg
  4 102400 home.tar
  5 491213 128MB.sdf
  6 1053184 common.tar
  7 4753408 sdm.tar
  8 1684577 securedesktop-ios-3.1.1.27-k9.pkg
  9 398305 sslclient-win-1.1.0.154.pkg
 10 839680 es.tar
[47849552 bytes used, 16375724 available, 64225276 total]
62720K bytes of ATA CompactFlash (Read/Write)
```

## Étape 8 : exécution de l'application SDM à partir du routeur

Ouvrez Internet Explorer et accédez à l'adresse URL « <https://<IP address>/> » ou « <http://<IP address>/> », selon que vous avez ou non activé le serveur sécurisé HTTP au cours de l'étape 2. Lorsque vous êtes invité à accepter le certificat, cliquez sur **Yes**.

Ignorez les avertissements liés à la sécurité et cliquez sur **Run**.

Entrez le nom d'utilisateur et le mot de passe que vous avez configurés au cours de l'étape 2.



SDM procède à la lecture de la configuration à partir du routeur.

Une fois le chargement de la configuration actuelle du routeur terminé, la page d'accueil de Cisco SDM s'affiche. Si la configuration affichée vous semble correcte, cela signifie que vous avez réussi à configurer SDM et à vous y connecter. Les informations affichées peuvent être différentes de celles qui figurent dans l'illustration suivante, selon le numéro de modèle du routeur, la version de l'IOS, etc.

