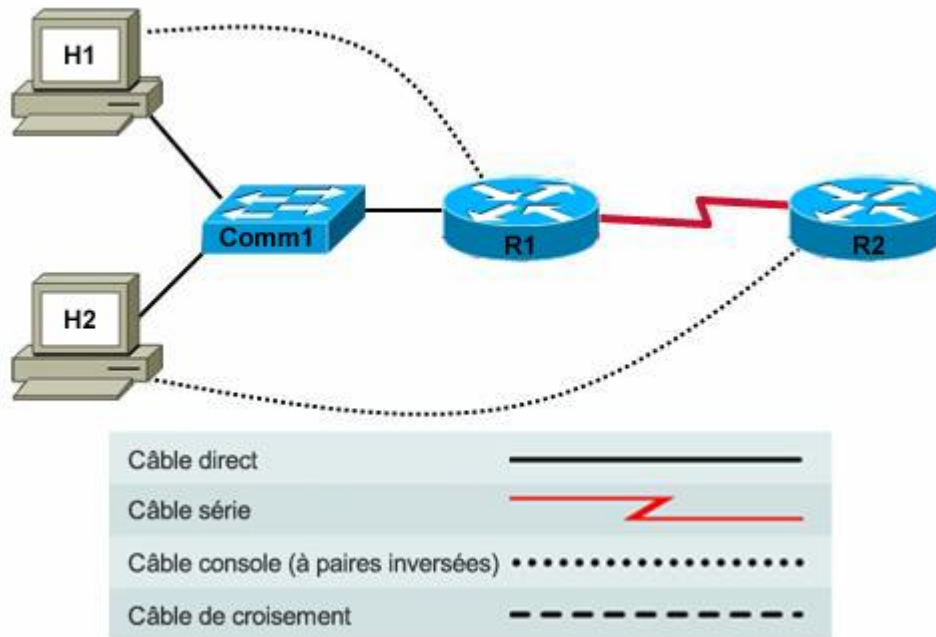


Travaux pratiques 5.3.8 Configuration de la fonction PAT (traduction d'adresses de port) avec SDM et de la fonction NAT statique à l'aide des commandes Cisco IOS



Périphérique	Nom de l'hôte	Interface	Adresse IP	Masque de sous-réseau
R1	CustomerRouter	Série 0/0/0 (ETTD)	209.165.200.225	255.255.255.224
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0
R2	ISP	Série 0/0/0 (DCE)	209.165.200.226	255.255.255.224

Objectifs

- Configurer les paramètres de routeur de base à l'aide de l'ILC Cisco IOS
- Configurer la traduction d'adresses de port (PAT) à l'aide de l'assistant Cisco SDM Basic NAT Wizard
- Vérifier les traductions NAT à l'aide de commandes Cisco IOS
- Configurer et vérifier la fonction NAT statique à l'aide de commandes Cisco IOS

Contexte / Préparation

Dans la tâche 1 de ces travaux pratiques, vous utiliserez l'assistant Cisco SDM Basic NAT Wizard pour configurer la traduction d'adresses de réseau (NAT) à l'aide d'une adresse IP globale externe unique. Celle-ci prend en charge des connexions à Internet à partir de nombreuses adresses privées internes. Cette fonctionnalité est également connue sous le nom de « surcharge NAT » ou de traduction d'adresses de port (PAT).

Dans la tâche 2, vous utiliserez des commandes Cisco IOS pour configurer la fonction NAT statique sur le routeur client afin de mapper définitivement les adresses publiques à des adresses privées de serveurs internes.

Il est supposé dans ces travaux pratiques que vous utilisez le routeur Cisco 1841. Vous pouvez utiliser n'importe quel autre modèle, à condition qu'il prenne en charge le gestionnaire SDM. Si vous installez un routeur pris en charge sur lequel SDM n'est pas installé, vous pouvez télécharger la dernière version gratuitement à l'adresse : <http://www.cisco.com/cgi-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 prennent en charge SDM, ainsi que la quantité de mémoire requise.

Ressources nécessaires :

- un routeur à services intégrés Cisco 1841 (ou comparable) avec SDM version 2.4 ou ultérieure comme routeur client ;
- un routeur Cisco 1841 (ou autre) comme routeur du FAI ;
- un commutateur Cisco 2960 (ou autre commutateur/concentrateur) pour connecter les hôtes H1, H2 et le routeur client ;
- un ordinateur Windows XP (hôte H1) 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) ;
- un ordinateur Windows XP (hôte H2) ;
- des câbles Ethernet directs de catégorie 5 ;
- un câble série null (R1 à R2) ;
- des câbles console (H1 à R1 et H2 à R2) ;
- l'accès à l'invite de commandes des hôtes H1 et H2 ;
- l'accès à la configuration réseau TCP/IP des hôtes H1 et H2.

À partir de chaque ordinateur hôte, démarrez une session HyperTerminal avec le routeur connecté.

Remarque : assurez-vous que les routeurs et commutateurs ont été réinitialisés et n'ont pas de configuration initiale. Pour plus d'informations sur la réinitialisation, reportez-vous au Manuel des travaux pratiques situé dans la section Tools (Outils) du site Academy Connection. Demandez de l'aide au formateur si vous n'êtes pas sûr de la procédure à suivre.

Tâche 1 : configuration des paramètres de routeur de base et de la fonction PAT

Étape 1 : création du réseau et configuration des paramètres IP des ordinateurs hôtes

- a. Vérifiez que les ordinateurs hôtes sont connectés suivant le schéma de topologie.

Remarque : un routeur autre que le Cisco 1841 peut nécessiter une connexion d'hôte à un port autre que Fast Ethernet 0/0 pour accéder au gestionnaire SDM.

- b. Configurez les hôtes avec des adresses IP statiques à l'aide des paramètres suivants.

Hôte H1 :

Adresse IP : 192.168.1.5
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.1.1

Hôte H2 :

Adresse IP : 192.168.1.9
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.1.1

Étape 2 : configuration des paramètres de base du routeur client à l'aide de l'ILC Cisco IOS

Configurez le nom d'hôte, les mots de passe et les interfaces en préparation de l'utilisation du gestionnaire SDM.

```
Router>enable
Router#config t
Router(config)#hostname CustomerRouter
CustomerRouter(config)#enable secret class
CustomerRouter(config)#username admin privilege 15 secret cisco123
CustomerRouter(config)#line con 0
CustomerRouter(config-line)#password cisco
CustomerRouter(config-line)#login
CustomerRouter(config-line)#line vty 0 4
CustomerRouter(config-line)#password cisco
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#interface FastEthernet0/0
CustomerRouter(config-if)#description LAN Default Gateway
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#interface Serial0/0/0
CustomerRouter(config-if)#ip address 209.165.200.225 255.255.255.224
CustomerRouter(config-if)#description WAN link to ISP
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
CustomerRouter(config)#ip http server
CustomerRouter(config)#ip http authentication local
```

Étape 3 : configuration des paramètres de base du routeur FAI à l'aide de l'ILC Cisco IOS

- a. Établissez une session HyperTerminal avec le routeur du FAI et effacez la configuration initiale à l'aide de la commande **erase startup-config** à partir de l'invite du mode privilégié. Redémarrez le routeur à l'aide de la commande **reload**.
- b. Configurez le nom d'hôte, les mots de passe et les interfaces.

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#exit
ISP(config)#interface serial 0/0/0
ISP(config-if)#description WAN link to CustomerRouter
ISP(config-if)#ip address 209.165.200.226 255.255.255.224
ISP(config-if)#clock rate 64000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#ip http server
ISP(config)#exit
```

Étape 4 : connexion au routeur client à l'aide de SDM

- a. Sur l'hôte H1, désactivez le cas échéant les programmes de blocage des fenêtres publicitaires intempestives. Ces programmes empêchent les fenêtres de SDM de s'afficher.
- b. L'interface utilisateur graphique SDM ne se charge pas automatiquement sur le routeur. Vous devez ouvrir un navigateur Web pour accéder à SDM. Accédez à l'adresse <http://192.168.1.1>.

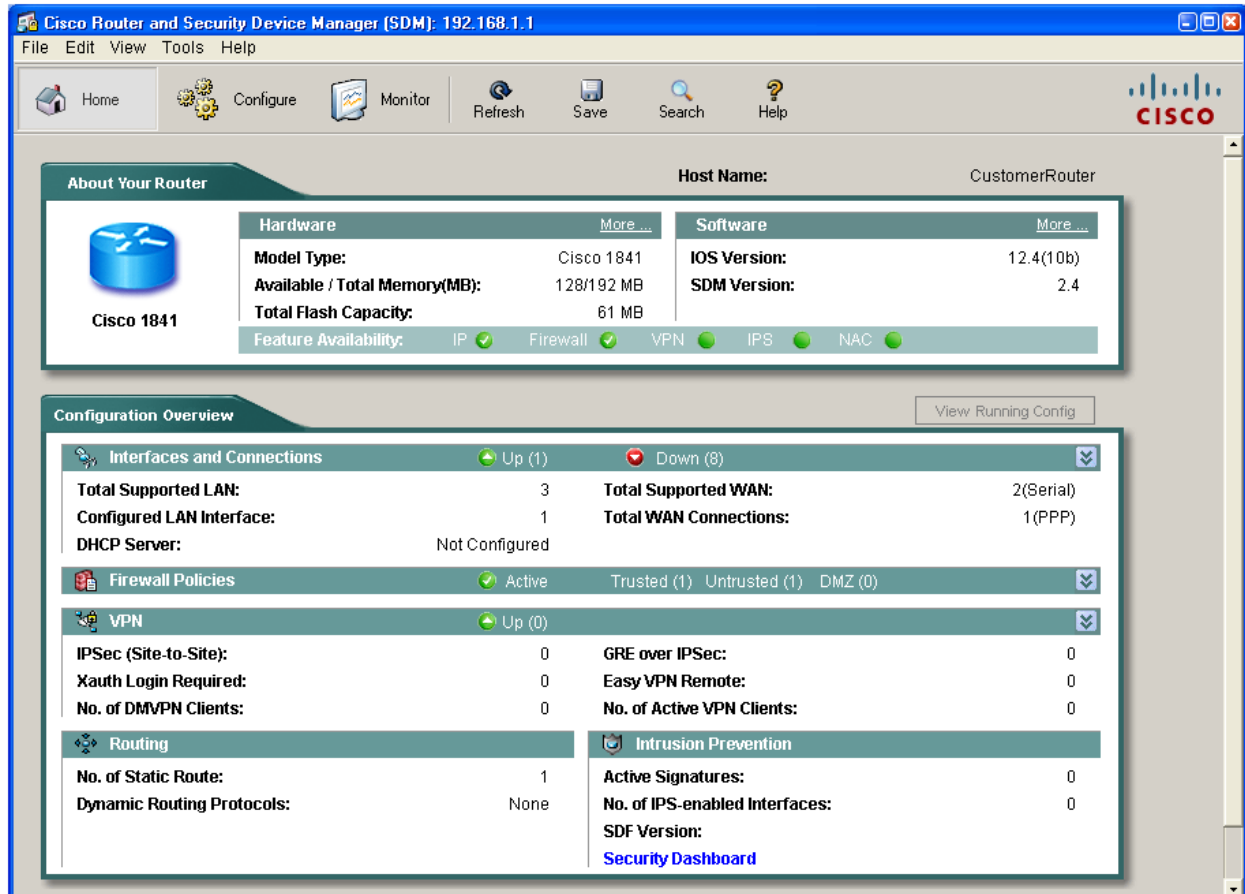
Remarque : si le navigateur ne parvient pas à se connecter, vérifiez le câblage et les connexions et assurez-vous que la configuration IP du PC est correcte.

- c. Dans la boîte de dialogue **Connexion à**, entrez **admin** comme nom d'utilisateur et **cisco123** comme mot de passe. Les informations d'ouverture de session ont été configurées à l'étape 2. Cliquez sur **OK**. L'application Web SDM principale démarre. Si vous êtes invité à utiliser le protocole HTTPS, cliquez sur **Annuler**. Si une fenêtre Avertissement de sécurité s'affiche, cliquez sur **Oui** pour faire confiance à l'application Cisco.



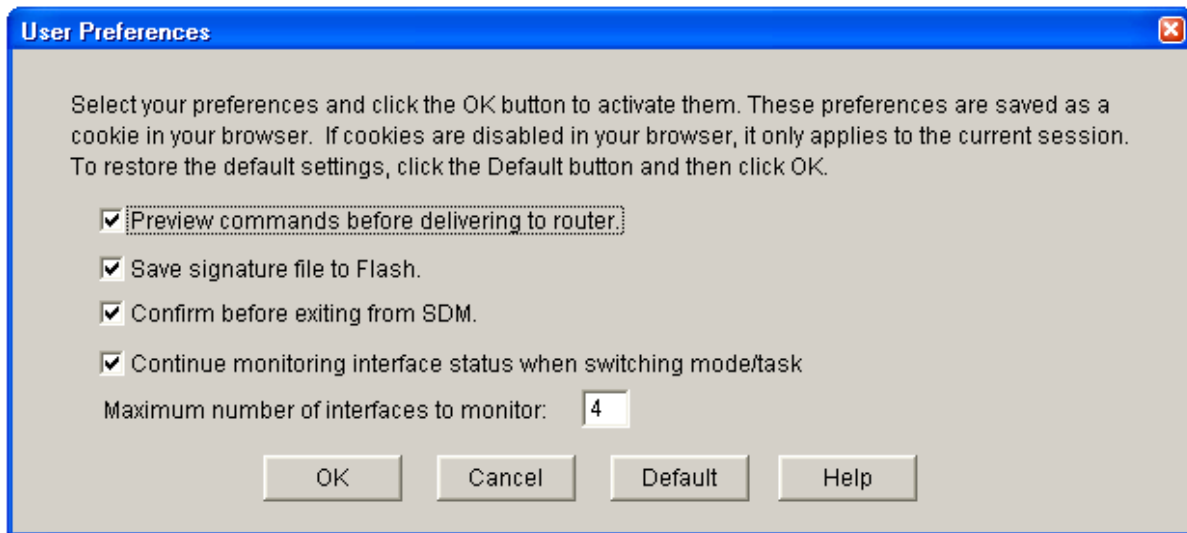
- d. Vérifiez que vous utilisez SDM 2.4 ou version ultérieure. L'écran initial de SDM s'affichant immédiatement après la connexion indique le numéro de version en cours. Celui-ci est également affiché sur l'écran principal de SDM illustré ci-dessous, ainsi que la version du logiciel Cisco IOS.

Remarque : si la version utilisée n'est pas 2.4 ou une version ultérieure, avertissez le formateur avant de poursuivre ces travaux pratiques. Vous devrez alors télécharger le fichier ZIP le plus récent sur l'ordinateur hôte H1. Dans le menu Tools de l'interface graphique utilisateur de SDM, sélectionnez l'option **Update SDM** pour spécifier l'emplacement du fichier ZIP et installer la mise à jour.



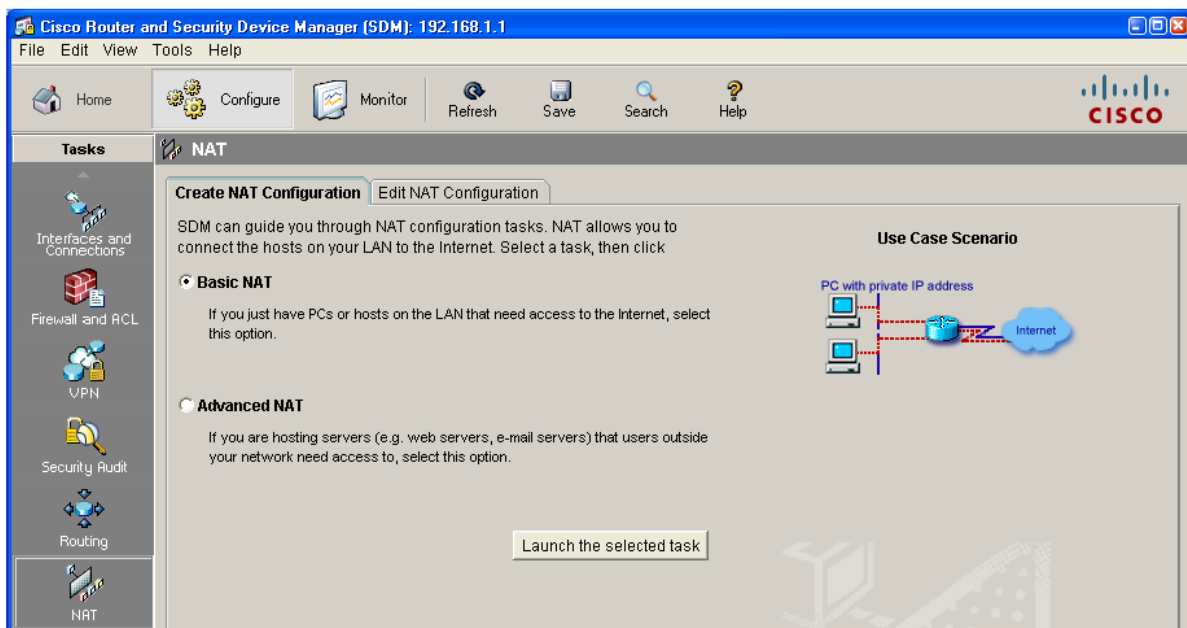
Étape 5 : configuration de SDM pour afficher les commandes de l'ILC Cisco IOS

- a. Dans le menu Edit de la fenêtre principale de SDM, sélectionnez **Preferences**.
- b. Activez la case à cocher **Preview commands before delivering to router**. Lorsque cette option est activée, vous pouvez afficher les commandes de configuration de l'interface de ligne de commande Cisco IOS avant qu'elles soient transmises au routeur, ce qui vous permet de vous familiariser avec les commandes utilisées.

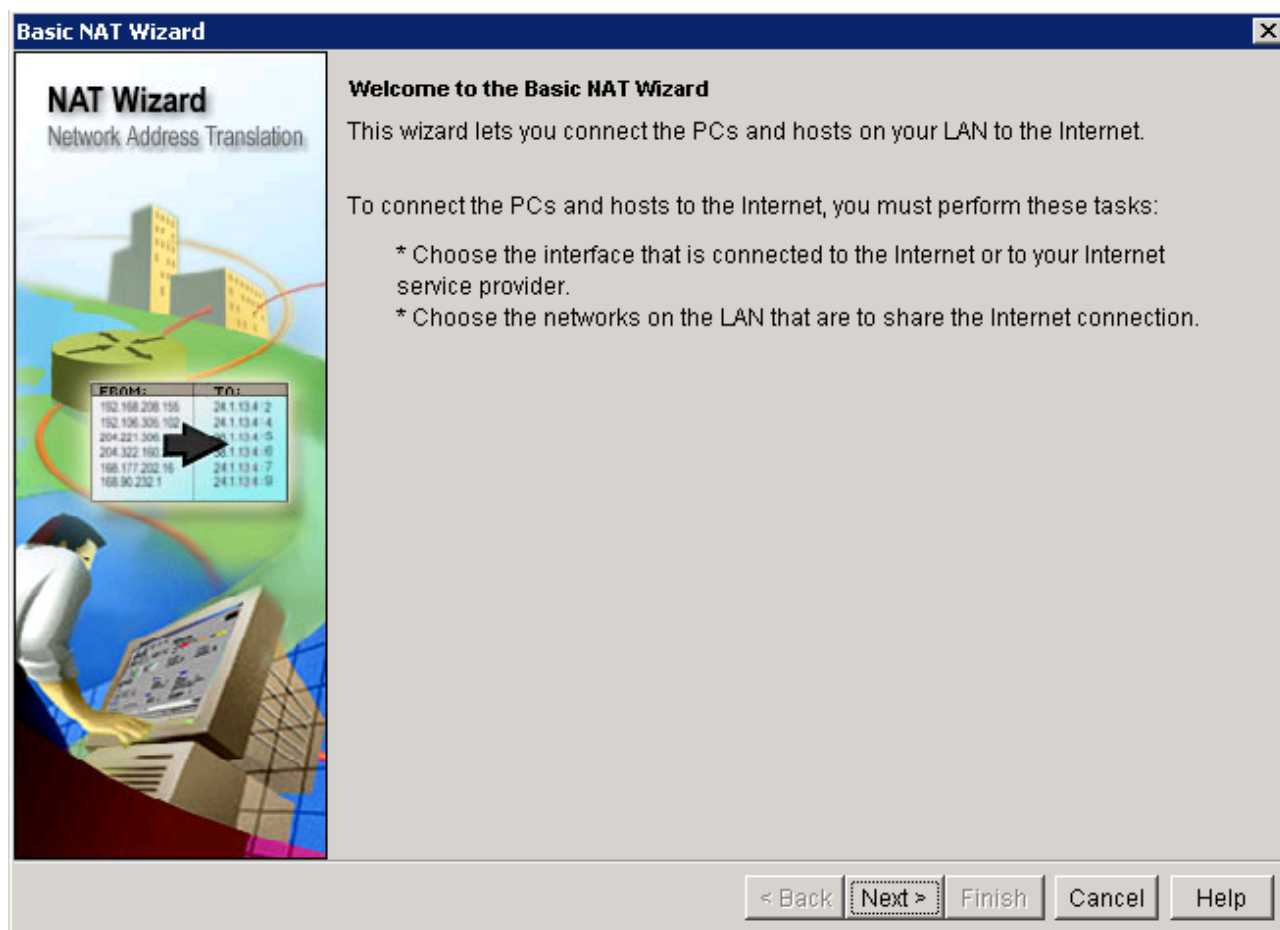


Étape 6 : lancement de l'assistant Basic NAT Wizard

- a. Dans le menu Configure, cliquez sur le bouton **NAT** pour afficher la page de configuration NAT. Cliquez sur la case d'option **Basic NAT**, puis sur **Launch the selected task**.



- b. Dans la fenêtre Welcome to the Basic NAT Wizard, cliquez sur **Next**.



Étape 7 : sélection de l'interface de réseau étendu pour NAT

- a. Choisissez l'interface de réseau étendu (WAN) Serial0/0/0 dans la liste. Cochez la case en regard de la plage d'adresses IP représentant le réseau interne de 192.168.1.0 à 192.168.1.255. Il s'agit de la plage qui nécessite une conversion à l'aide du processus NAT.

Basic NAT Wizard

NAT Wizard
Network Address Translation

Sharing the Internet Connection

If this router has a connection to the Internet, specify how you want PCs and hosts on the LAN to share this connection.

Choose the interface that connects to the Internet or your Internet service provider:

Serial0/0/0 Details...

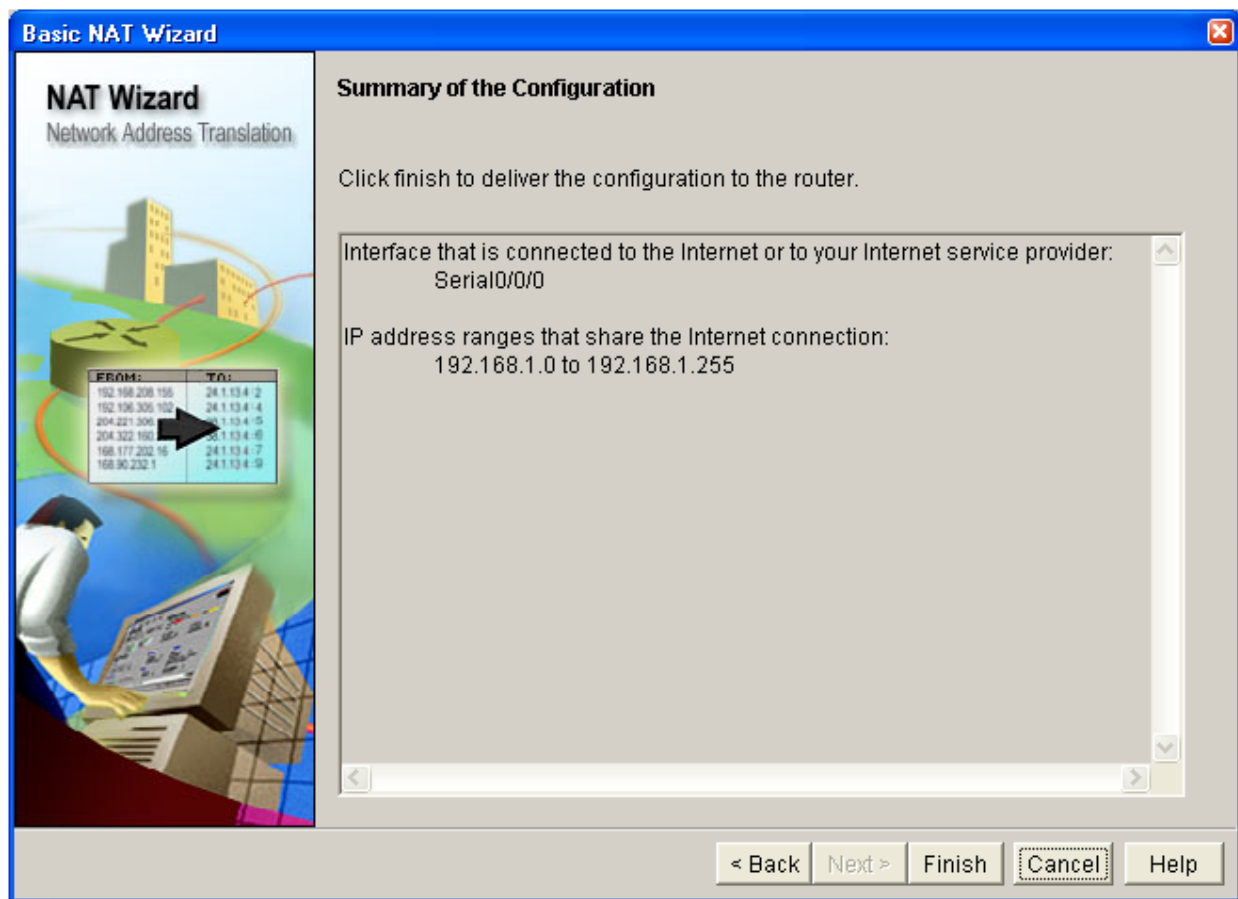
The following ranges of IP addresses are allocated to networks directly connected to the router. Check the box next to each network that is to share the connection that you specified:

	IP address range	Connected Through	Comment
<input checked="" type="checkbox"/>	192.168.1.0 to 192.168.1.255	FastEthernet0/0	
<input type="checkbox"/>	209.165.200.224 to 209.165.200.255	Serial0/0/0	

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

< Back Next > Finish Cancel Help

- b. Cliquez sur **Next** et, après avoir lu le contenu de la page Summary of the Configuration, cliquez sur **Finish**.

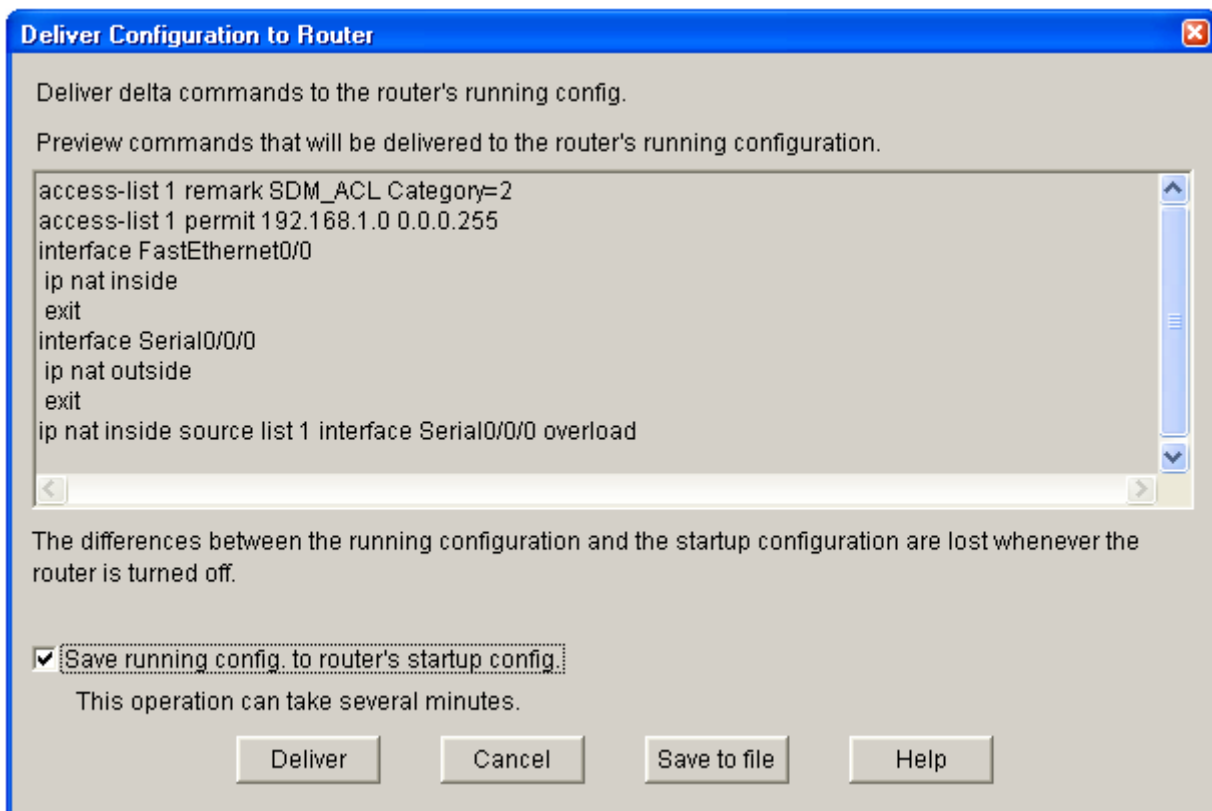


- c. Dans la fenêtre **Deliver Configuration to Router**, examinez les commandes ILC générées par Cisco SDM. Il s'agit des commandes qui seront transmises au routeur pour configurer la fonction NAT. Ces commandes peuvent également être entrées manuellement à partir de l'ILC pour effectuer la même tâche. Activez la case à cocher **Save running config to router's startup config**.

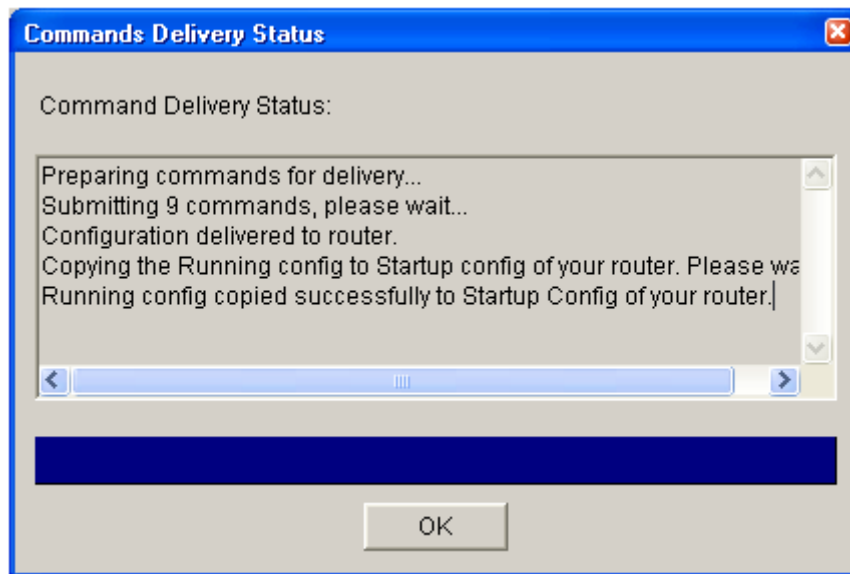
Remarque : par défaut, les commandes que vous venez de générer ne mettent à jour que le fichier de configuration en cours lorsqu'elles sont transmises. Si vous redémarrez le routeur, vous perdez les modifications que vous avez apportées. Si vous activez cette case à cocher, le fichier de configuration initiale est également mis à jour et le routeur charge les nouvelles commandes dans la configuration en cours lors de son redémarrage.

Si vous préférez ne pas enregistrer les commandes dans la configuration initiale pour le moment, utilisez l'option **File > Write to Startup config** de SDM ou la commande **copy running-config startup-config** de l'ILC à partir d'une session de terminal ou Telnet.

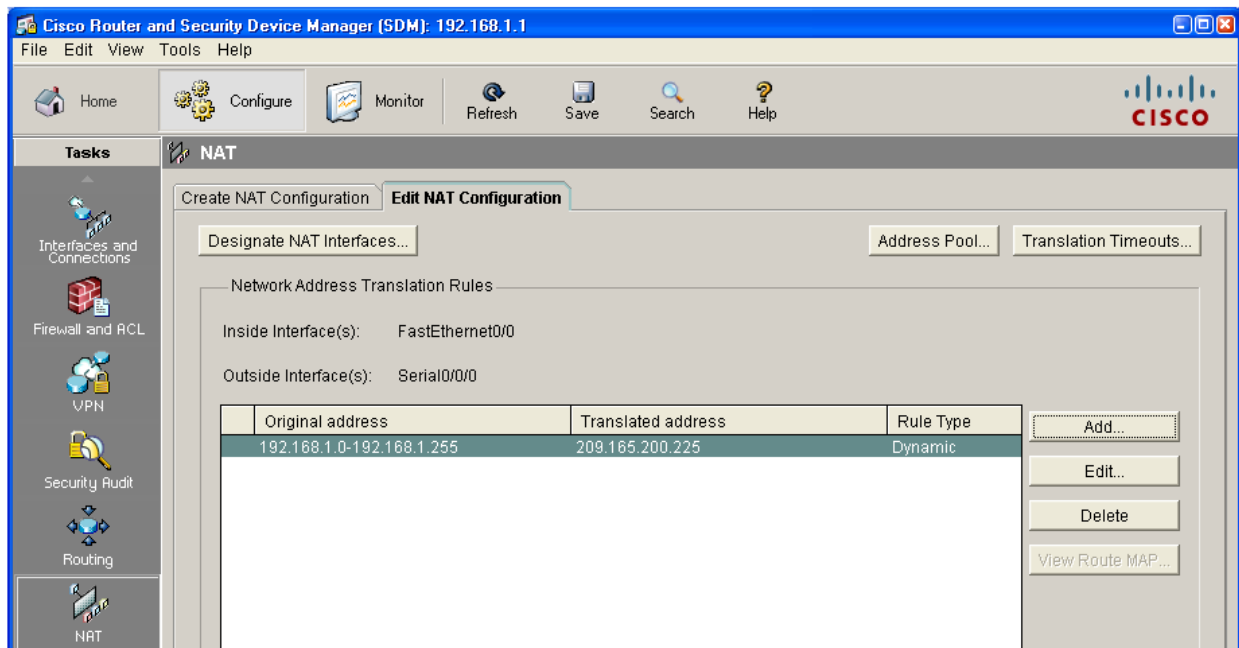
- d. Cliquez sur **Deliver** pour terminer la configuration du routeur.



- e. Dans la fenêtre **Commands Delivery Status**, notez le texte indiquant que la configuration en cours a été copiée correctement dans la configuration initiale. Cliquez sur **OK** pour quitter l'assistant.



- f. L'écran NAT final montre que l'interface interne est Fa0/0 et l'interface externe S0/0/0. Les adresses privées internes (d'origine) sont traduites de manière dynamique en adresses publiques externes.



- g. Sélectionnez **File > Exit** dans le menu principal SDM pour terminer la session SDM. Cliquez sur **Yes** pour confirmer que vous souhaitez quitter SDM.

Étape 8 : vérification de la fonctionnalité NAT

- a. Sur l'hôte H1, ouvrez une fenêtre d'invite de commandes et envoyez une requête ping à l'interface série du routeur du FAI à l'adresse 209.165.200.226. La requête ping aboutit-elle ? _____

- b. À partir de la fenêtre du terminal du routeur client, entrez la commande **show ip nat translations** pour afficher l'adresse privée interne de l'hôte H1 traduite en adresse publique externe 0/0/0 série.

```
CustomerRouter#show ip nat translations
Pro  Inside global      Inside local    Outside local    Outside global
icmp 209.165.200.225:512 192.168.1.2:512 209.165.200.226:512 209.165.200.226:512
```

- c. Quel type d'adresse NAT est l'adresse IP de l'hôte H1 ? _____
- d. Quel type d'adresse NAT est l'adresse IP publique 0/0/0 série du routeur client ? _____
- e. Quel type d'adresse NAT est l'adresse IP publique 0/0/0 série du routeur du FAI ? _____

- f. Envoyez une requête ping coup sur coup tout d'abord à partir de H1, puis de H2, à l'interface série du routeur du FAI à l'adresse 209.165.200.226. La requête ping a-t-elle abouti ? _____

- g. Utilisez la commande **show ip nat translations** pour afficher l'adresse privée interne de l'hôte H1 traduite en adresse publique externe 0/0/0 série.

```
CustomerRouter#show ip nat translation
Pro  Inside global      Inside local    Outside local    Outside global
icmp 209.165.200.225:512 192.168.1.2:512 209.165.200.226:512 209.165.200.226:512
icmp 209.165.200.225:513 192.168.1.9:512 209.165.200.226:512 209.165.200.226:513
```

- h. Quelle est la différence entre les traductions de l'hôte H1 et de l'hôte H2 ? _____
- i. Utilisez la commande **clear ip nat translations *** pour effacer la table de traduction NAT du routeur, et entrez à nouveau **show ip nat translations** pour vérifier que les traductions sont effacées.

```
CustomerRouter#clear ip nat translations *
CustomerRouter#show ip nat translation
```

- j. À partir de H1, envoyez une requête ping à l'interface série du routeur client à l'adresse 209.165.200.225. La requête ping aboutit-elle ? _____
- k. À partir de la fenêtre du terminal du routeur client, utilisez à nouveau la commande **show ip nat translations** pour afficher les traductions d'adresses.
- l. Y a-t-il des traductions à présent ? _____ . Pourquoi ? _____

- m. Sur l'hôte H1, ouvrez un navigateur tel qu'Internet Explorer et entrez l'adresse IP de l'interface série du routeur du FAI à <http://209.165.200.226> dans la zone d'adresse. Quel est le résultat ? _____

- n. Affichez la table de traduction NAT à l'aide de la commande **show ip nat translations**. La traduction apparaît-elle dans la table NAT ? _____

```
CustomerRouter#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
tcp  209.165.200.225:1059 192.168.1.2:1059 209.165.200.226:80 209.165.200.226:80
---  209.165.200.229      192.168.1.9
```

- o. Pour la traduction de l'adresse locale interne IP de H1, quel est le protocole et l'adresse IP:numéro de port pour les adresses (de destination) locale externe et globale externe et que représente le numéro de port externe ? _____

Tâche 2 : configuration et vérification de la fonction NAT statique à l'aide de l'ILC Cisco IOS

Étape 1 : configuration d'un mappage statique pour le serveur

L'hôte H2, avec l'adresse IP 192.168.1.9/24, a été désigné comme serveur Web public. Il nécessite donc une adresse IP publique affectée définitivement. Cette affectation est définie via un mappage NAT statique.

- a. Pour configurer un mappage NAT statique, utilisez la commande **ip nat inside source static**.

```
Gateway(config)#ip nat inside source static 192.168.1.9 209.165.200.229
```

Ceci mappe définitivement l'adresse publique 209.165.201.229 à 192.168.1.9, l'adresse interne du serveur Web. Toute tentative d'accès à l'adresse publique 209.165.200.229 est transmise par le routeur à l'hôte H2 à l'adresse privée 192.168.1.9.

- b. Affichez la table de traduction NAT à l'aide de la commande **show ip nat translations**. Le mappage statique apparaît-il dans les résultats de la commande ? _____

```
CustomerRouter#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
---  209.165.200.229  192.168.1.9      ---              ---
```

Étape 2 : test de la fonctionnalité NAT statique

- a. Envoyez une requête ping de l'hôte H1 à l'adresse NAT statique publique mappée à l'hôte H2. La requête ping aboutit-elle ? _____
- b. Affichez la table de traduction NAT à l'aide de la commande **show ip nat translations**. La traduction apparaît-elle dans la table NAT ? _____

```
CustomerRouter#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.225:512 192.168.1.2:512 209.165.200,229:512 209.165.200,229:512
---  209.165.200.229      192.168.1.9      ---              ---
```

- c. Quelle est l'adresse locale externe et globale externe utilisée dans la traduction ? _____

- d. À partir de la fenêtre HyperTerminal du routeur du FAI, envoyez une requête ping à l'hôte H2 avec la traduction NAT statique à l'adresse 192.168.1.9. La requête ping aboutit-elle ? _____

- e. À partir du routeur du FAI, envoyez une requête ping à l'adresse statique publique mappée au serveur interne H2 à 209.165.201.229. La requête ping aboutit-elle ? _____ Pourquoi ?

- f. Quelle est la traduction de l'adresse globale interne en adresse d'hôte locale interne ?

```
CustomerRouter#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.229:5 192.168.1.9:5 209.165.200.226:5 209.165.200.226:5
--- 209.165.200.229    192.168.1.9    ---            ---
```

Étape 3 : enregistrement des configurations des routeurs

En mode d'exécution privilégié, enregistrez la configuration en cours dans la configuration initiale.

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

Tâche 3 : remarques générales

- a. Évaluez les compétences dont vous avez besoin pour configurer NAT à l'aide des commandes de l'ILC Cisco IOS. Quels sont selon vous les avantages et les inconvénients de l'utilisation de Cisco SDM ?

- b. Pourquoi, d'après vous, l'option par défaut est-elle de ne mettre à jour que le fichier de configuration en cours du routeur lorsque les commandes sont transmises ? Pourquoi ne pas mettre à jour le fichier de configuration initiale à chaque fois ? Quels sont les avantages et inconvénients de chacune de ces méthodes par rapport à l'autre ?
