Travaux pratiques : configuration du protocole SNMP (version de l'instructeur)

Remarque à l'intention de l'instructeur : le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

Topologie

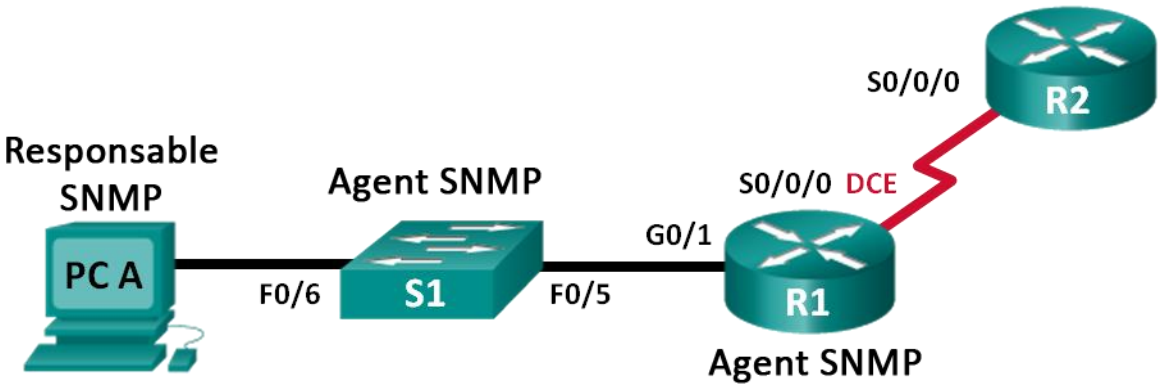


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

Partie 1 : création du réseau et configuration des paramètres de base du périphérique

Partie 2 : configuration d'un gestionnaire et d'agents SNMP

Partie 3 : conversion de codes OID avec l'explorateur d'objets Cisco SNMP

Contexte/scénario

Le protocole SNMP (Simple Network Management Protocol) est un protocole de gestion du réseau ainsi qu'une norme IETF pouvant être utilisés à la fois pour surveiller et contrôler des clients sur un réseau. Le protocole SNMP peut être utilisé pour obtenir et définir les variables relatives à l'état et à la configuration d'hôtes réseau, comme des routeurs et des commutateurs, et d'ordinateurs clients sur le réseau. Le gestionnaire SNMP peut interroger les agents SNMP afin d'obtenir des données ou ces données peuvent être envoyées automatiquement au gestionnaire SNMP grâce à la configuration de déroutements sur les agents SNMP.

Au cours de ces travaux pratiques, vous allez télécharger, installer et configurer le logiciel de gestion SNMP sur PC-A. Vous configurerez également un routeur et un commutateur Cisco en tant qu'agents SNMP. Après

la capture des messages de notification SNMP à partir de l'agent SNMP, vous convertirez les codes d'ID d'objet/MIB en vue de découvrir les détails des messages à l'aide de l'explorateur d'objets Cisco SNMP.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau Résumé des interfaces du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Remarque à l'intention de l'instructeur : reportez-vous au Manuel de travaux pratiques pour l'instructeur, pour connaître les procédures d'initialisation et de redémarrage des périphériques.

Remarque : les commandes **snmp-server** utilisées au cours de ces travaux pratiques entraîneront la génération d'un message d'avertissement de la part du commutateur Cisco 2960 lors de l'enregistrement du fichier de configuration dans la mémoire vive non volatile. Afin d'empêcher la génération de ce message d'avertissement, vérifiez que le commutateur utilise le modèle **lanbase-routing**. Le modèle IOS est contrôlé par le gestionnaire de base de données des commutateurs (SDM, Switch Database Manager). Lorsque vous modifiez le modèle de préférence, le nouveau modèle est utilisé après le redémarrage, même si la configuration n'a pas été enregistrée.

```
S1# show sdm prefer
```

Utilisez les commandes suivantes pour attribuer le modèle **lanbase-routing** en tant que modèle SDM par défaut.

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end
S1# reload
```

Ressources requises

- 2 routeurs (Cisco 1941 équipés de Cisco IOS version 15.2(4)M3, image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 1 PC (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal tel que Tera Term)
- 1 ordinateur (Windows 7, Vista ou XP, équipé d'un accès Internet)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet et série conformément à la topologie
- Logiciel de gestion SNMP (programme PowerSNMP Free Manager de Dart Communications ou serveur Syslog Kiwi de SolarWinds, version d'évaluation gratuite de 30 jours)

Partie 1 : Création du réseau et configuration des paramètres de base du périphérique

Dans la Partie 1, vous allez définir la topologie du réseau et configurer les périphériques en utilisant les paramètres de base.

Étape 1 : Câblez le réseau conformément à la topologie.

Étape 2 : Configurez l'hôte de PC.

Étape 3 : Le cas échéant, initialisez et redémarrez le commutateur et les routeurs.

Étape 4 : Configurez les paramètres de base des routeurs et du commutateur.

a. Désactivez la recherche DNS.

b. Configurez les noms des périphériques conformément à la topologie.

c. Configurez les adresses IP telles qu'indiquées dans la table d'adressage. (Ne configurez pas l'interface S0/0/0 sur R1 à ce stade.)

d. Attribuez **cisco** comme mot de passe pour la console et vty et activez la connexion.

e. Attribuez **class** comme mot de passe chiffré du mode d'exécution privilégié.

f. Configurez **logging synchronous** pour empêcher les messages de console d'interrompre la commande.

g. Vérifiez la connectivité entre les périphériques LAN en exécutant la commande ping.

h. Copiez la configuration en cours en tant que configuration de démarrage.

Partie 2 : Configuration d'un gestionnaire et d'agents SNMP

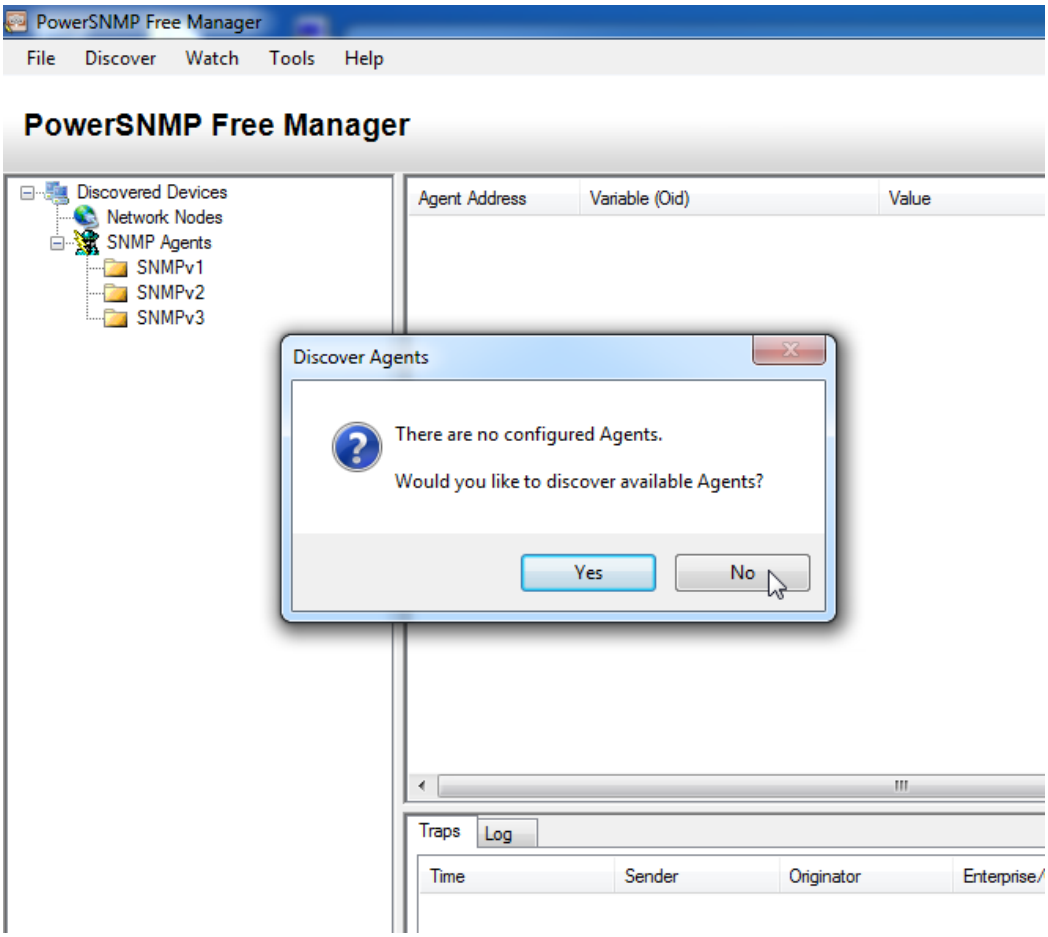
Dans la Partie 2, le logiciel de gestion SNMP sera installé et configuré sur PC-A, tandis que R1 et S1 seront configurés en tant qu'agents SNMP.

Étape 1 : Installez un programme de gestion SNMP.

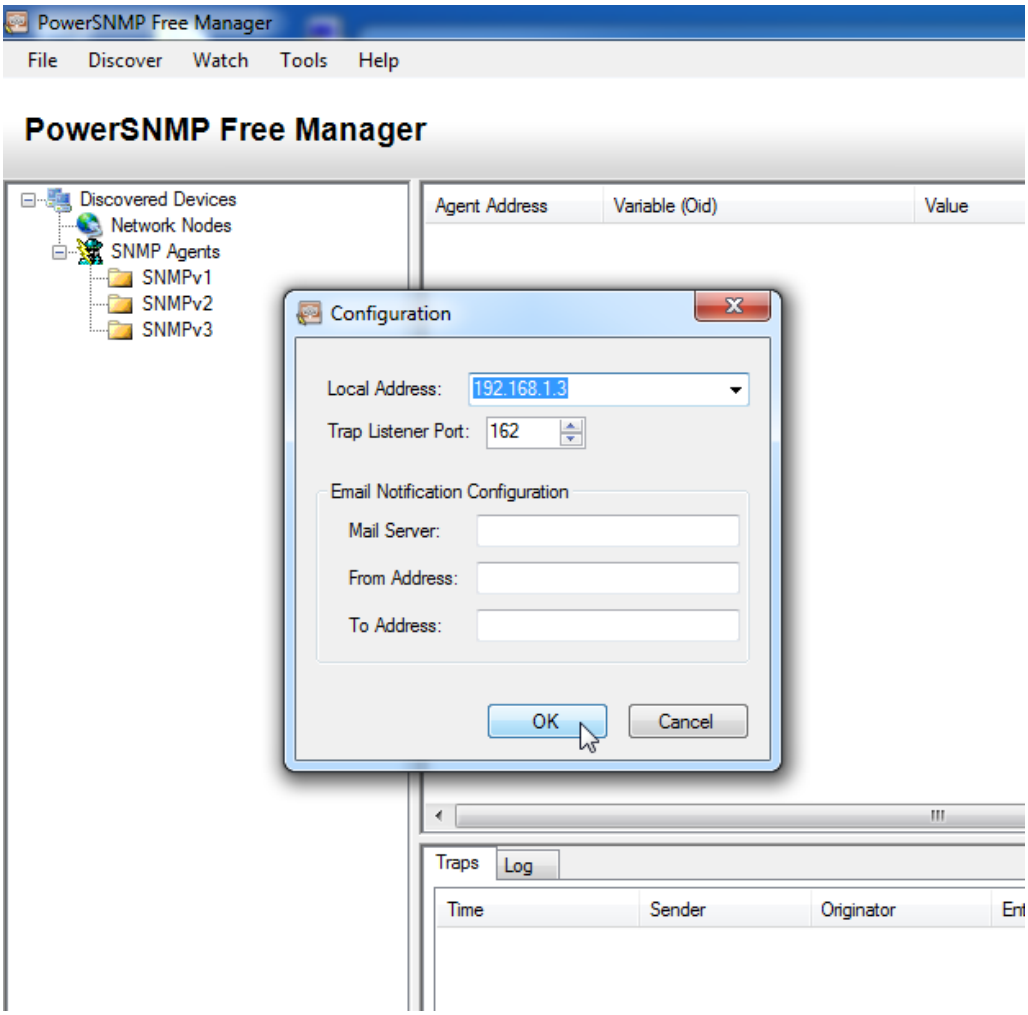
a. Téléchargez et installez l'outil PowerSNMP Free Manager de Dart Communications à partir de l'URL suivante : http://www.dart.com/snmp-free-manager.aspx.

b. Démarrez le programme PowerSNMP Free Manager.

c. Cliquez sur **No** si vous êtes invité à détecter les agents SNMP disponibles. Vous détecterez les agents SNMP après la configuration de SNMP sur R1. Le programme PowerSNMP Free Manager prend en charge les versions 1, 2 et 3 de SNMP. Ces travaux pratiques utilisent SNMPv2.



d. Dans la fenêtre contextuelle Configuration (si aucune fenêtre contextuelle n'apparaît, accédez à Tools > Configuration), définissez l'adresse IP locale de manière à écouter le réseau 192.168.1.3, puis cliquez sur **OK**.



Remarque : si vous êtes invité à détecter les agents SNMP disponibles, cliquez sur **No** et passez à la partie suivante des travaux pratiques.

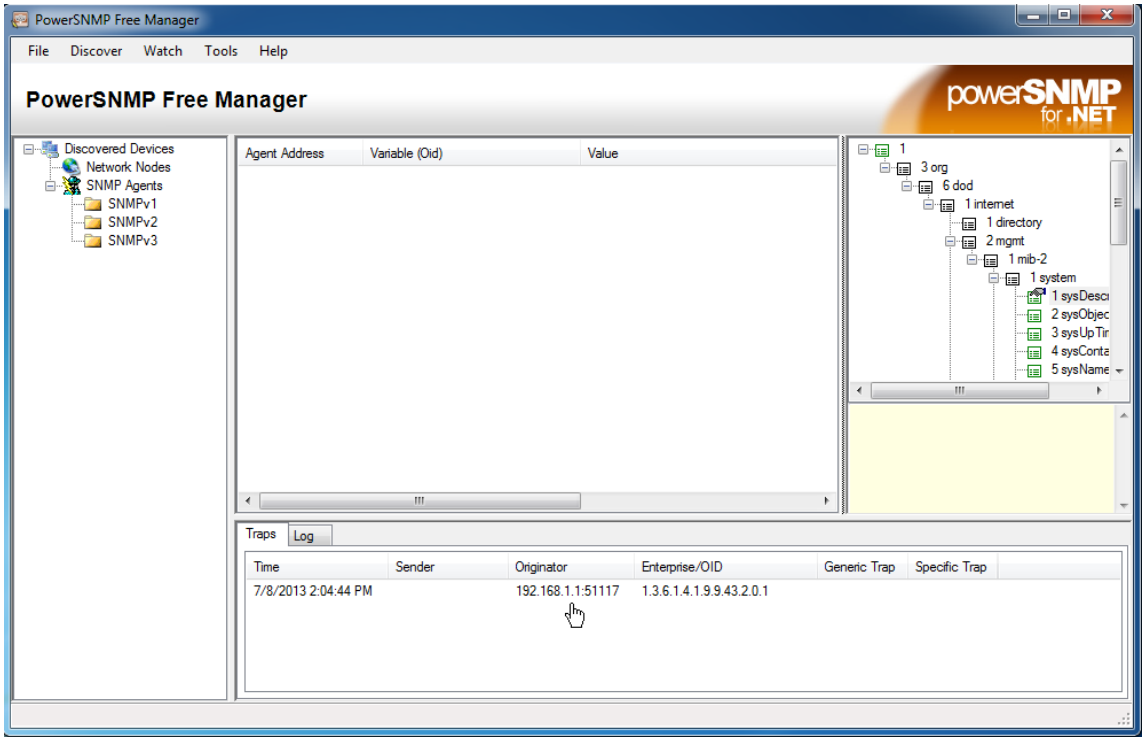
Étape 2 : Configurez un agent SNMP.

a. Sur R1, exécutez les commandes suivantes à partir du mode de configuration globale afin de configurer le routeur en tant qu'agent SNMP. Dans la ligne 1 ci-dessous, l'identifiant de communauté SNMP est **ciscolab**, avec des privilèges en lecture seule, tandis que la liste d'accès nommée SNMP_ACL définit quels hôtes sont autorisés à obtenir des informations SNMP de la part de R1. Aux lignes 2 et 3, l'emplacement du gestionnaire SNMP et les commandes de contact fournissent des informations de contact descriptives. La ligne 4 spécifie l'adresse IP de l'hôte qui recevra les notifications SNMP, la version SNMP ainsi que l'identifiant de communauté. La ligne 5 active tous les déroutements SNMP par défaut, tandis que les lignes 6 et 7 créent la liste d'accès nommée, destinée à contrôler quels hôtes sont autorisés à obtenir des informations SNMP de la part du routeur.

```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
```

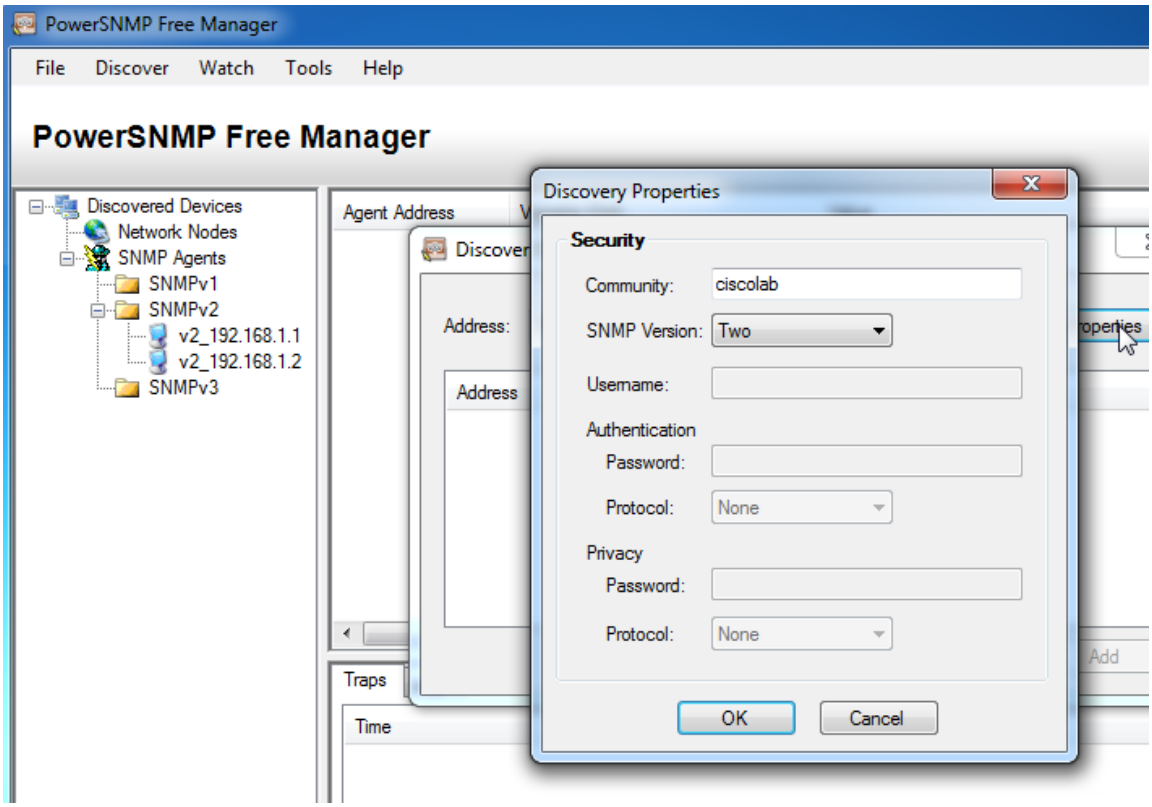
```
R1(config-std-nacl)# permit 192.168.1.3
```

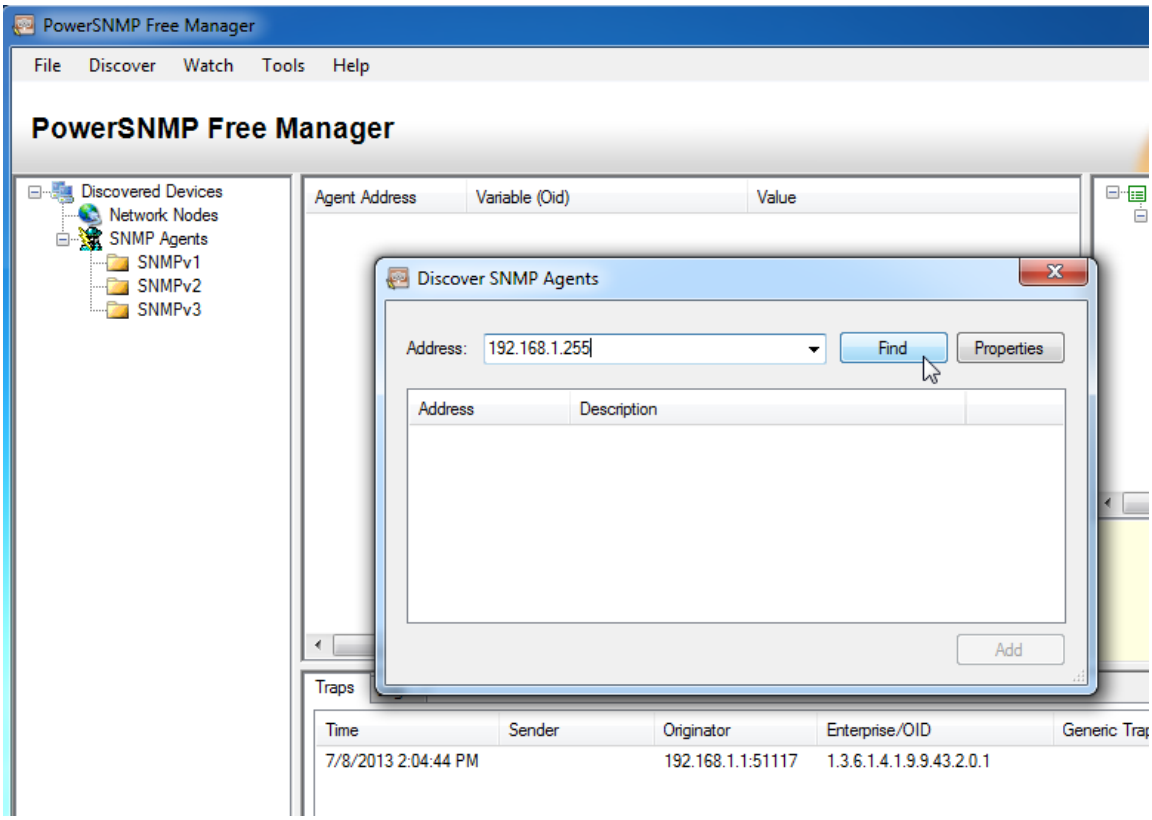
b. À ce stade, il se peut que vous constatiez que le programme PowerSNMP Free Manager reçoit des notifications en provenance de R1. Si ce n'est pas le cas, vous pouvez essayer de forcer l'envoi d'une notification SNMP en exécutant une commande **copy run start** sur R1. En cas d'échec, passez à l'étape suivante.

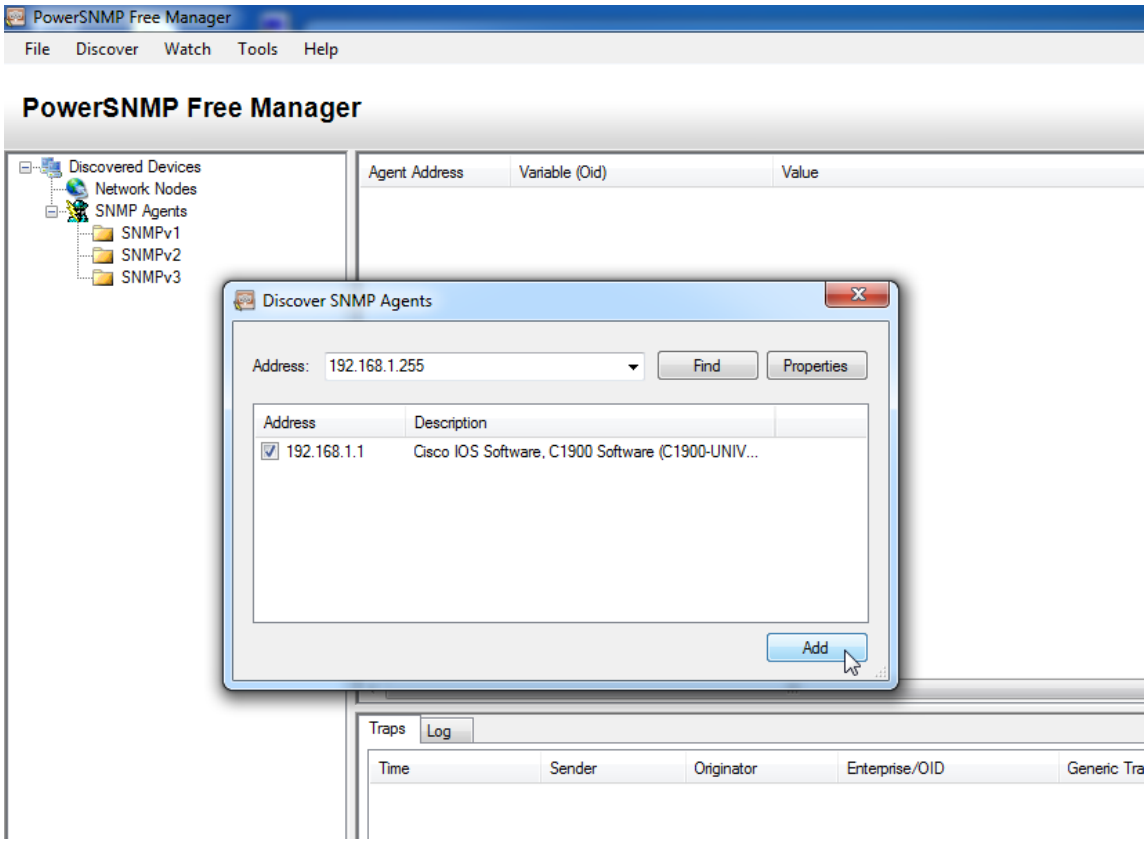


Étape 3 : Détectez les agents SNMP.

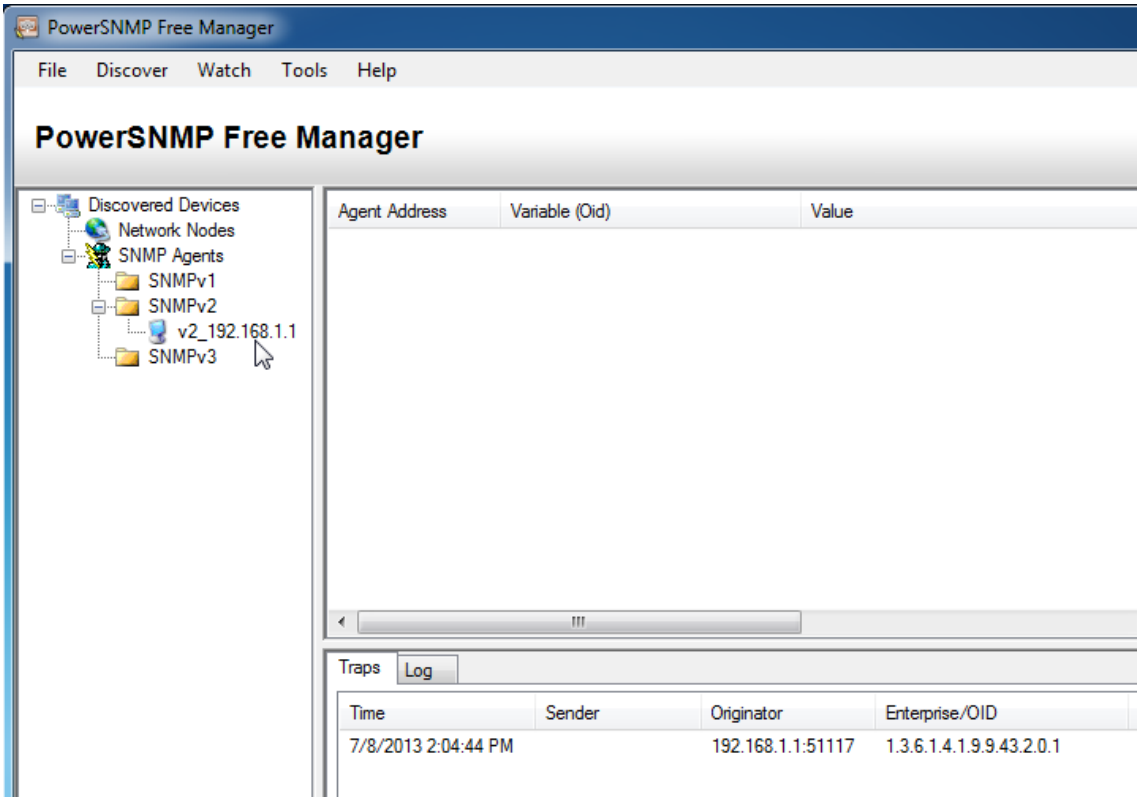
a. Dans l'outil PowerSNMP Free Manager sur PC-A, ouvrez la fenêtre **Discover > SNMP Agents**. Entrez l'adresse IP **192.168.1.255**. Dans la même fenêtre, cliquez sur **Properties** et définissez la communauté à **ciscolab** et la version SNMP à la valeur 2 (**Two)**, puis cliquez sur **OK**. Vous pouvez maintenant cliquer sur **Find** pour détecter tous les agents SNMP sur le réseau 192.168.1.0. L'outil PowerSNMP Free Manager devrait trouver R1 à l'adresse 192.168.1.1. Cliquez sur la case à cocher, puis sur **Add** pour ajouter R1 en tant qu'agent SNMP.







b. Dans le programme PowerSNMP Free Manager, R1 est ajouté à la liste des agents SNMPv2 disponibles.



c. Configurez S1 en tant qu'agent SNMP. Vous pouvez utiliser les mêmes commandes **snmp-server** que celles que vous avez utilisées pour configurer R1.

```
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server location snmp_manager
S1(config)# snmp-server contact ciscolab_admin
S1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
S1(config)# snmp-server enable traps
S1(config)# ip access-list standard SNMP_ACL
S1(config-std-nacl)# permit 192.168.1.3
```

d. Après la configuration de S1, les notifications SNMP en provenance de 192.168.1.2 s'affichent dans la fenêtre Traps du programme PowerSNMP Free Manager. Dans le programme PowerSNMP Free Manager, ajoutez S1 en tant qu'agent SNMP en appliquant le même processus que celui utilisé pour la détection de R1.

Partie 3 : Conversion de codes OID avec l'explorateur d'objets Cisco SNMP

Dans la Partie 3, vous allez forcer l'envoi des notifications SNMP au gestionnaire SNMP situé au niveau de PC-A. Vous convertirez ensuite les codes OID reçus en noms afin de découvrir la nature des messages. Les codes MIB/OID peuvent être aisément convertis à l'aide de l'explorateur d'objets Cisco SNMP disponible à l'adresse suivante : http://www.cisco.com.

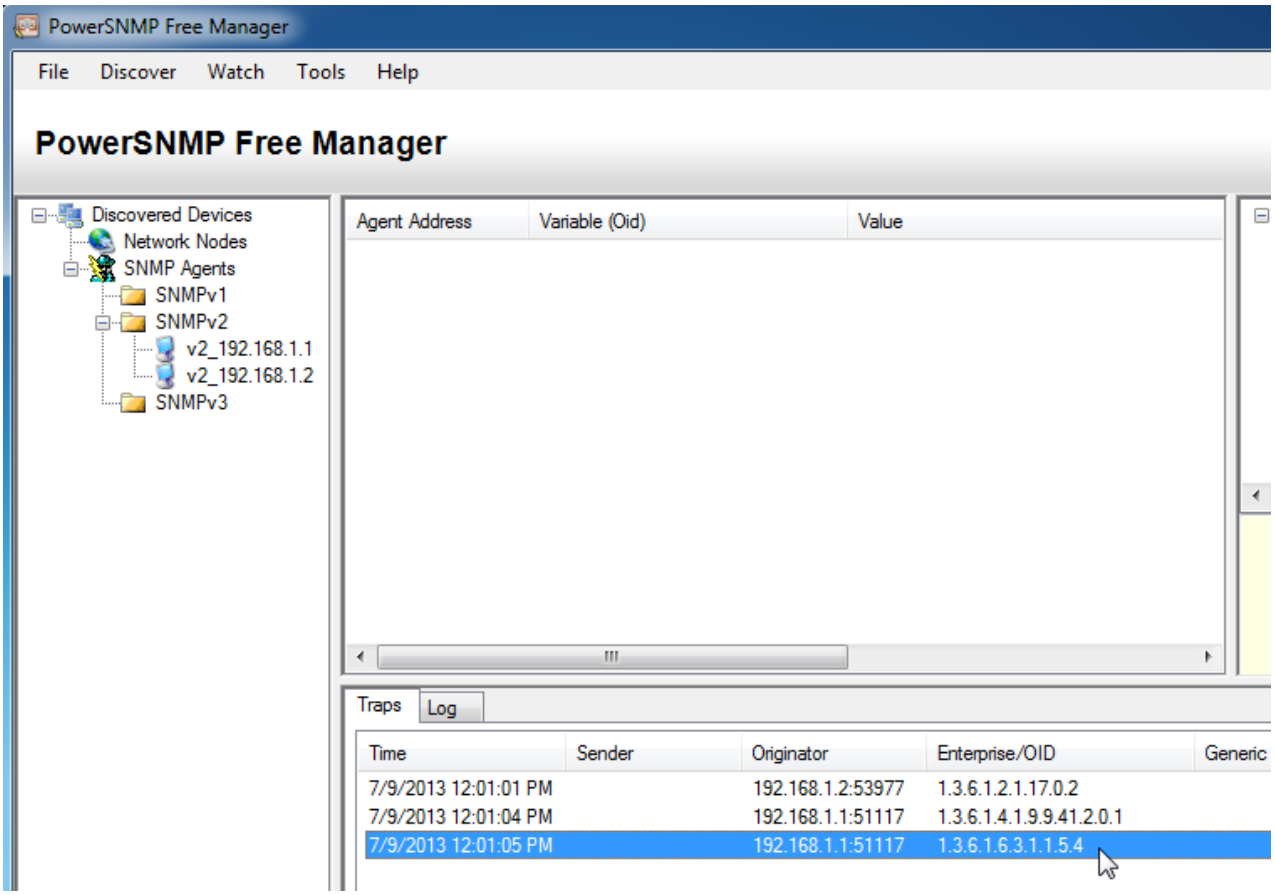
Étape 1 : Effacez les messages SNMP actuels.

Dans l'outil PowerSNMP Free Manager, cliquez avec le bouton droit dans la fenêtre **Traps** et sélectionnez **Clear** pour effacer les messages SNMP.

Étape 2 : Générez un déroutement et une notification SNMP.

Sur R1, configurez l'interface S0/0/0 conformément à la table d'adressage située au début de ces travaux pratiques. Accédez au mode de configuration globale et activez une interface afin de générer une notification de déroutement SNMP à envoyer au gestionnaire SNMP au niveau de PC-A. Notez que les numéros de code d'entreprise/OID sont visibles dans la fenêtre des déroutements.

```
R1(config)# interface s0/0/0
R1(config)# ip address 192.168.2.1 255.255.255.252
R1(config)# clock rate 128000
R1(config)# no shutdown
```



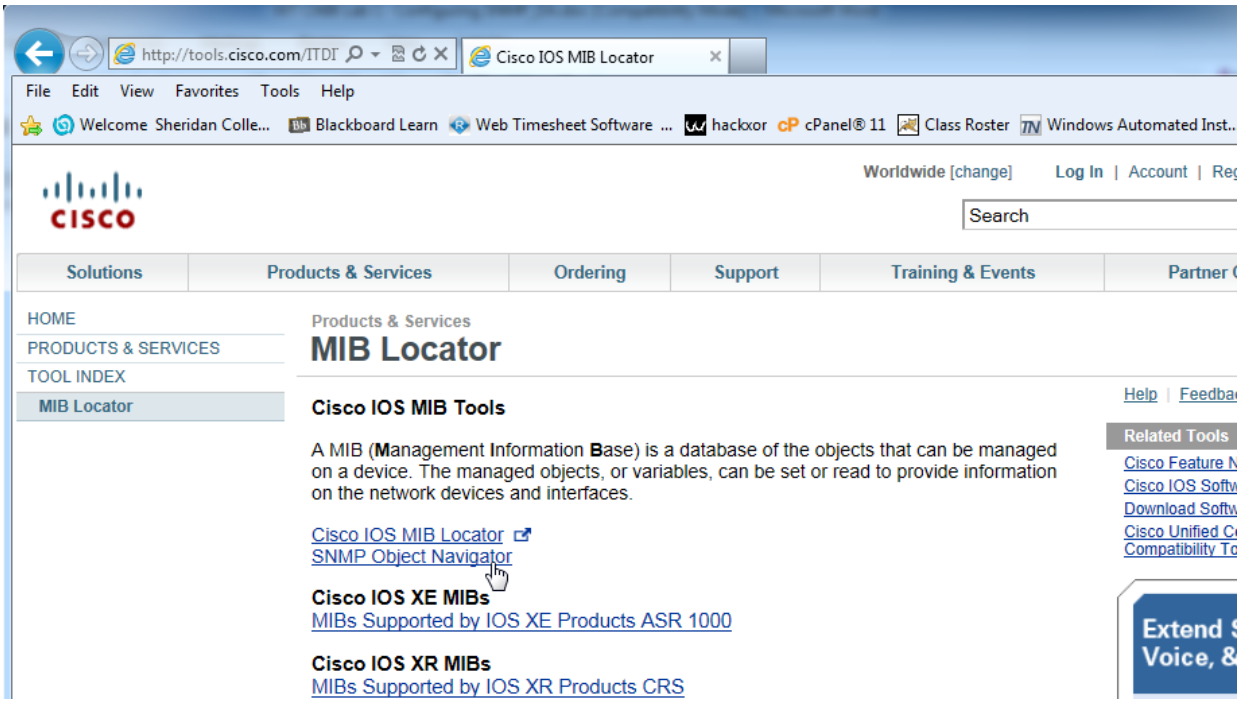
Étape 3 : Décodez les messages MIB/OID SNMP.

À partir d'un ordinateur disposant d'un accès Internet, ouvrez un navigateur Web et accédez à l'adresse http://www.cisco.com.

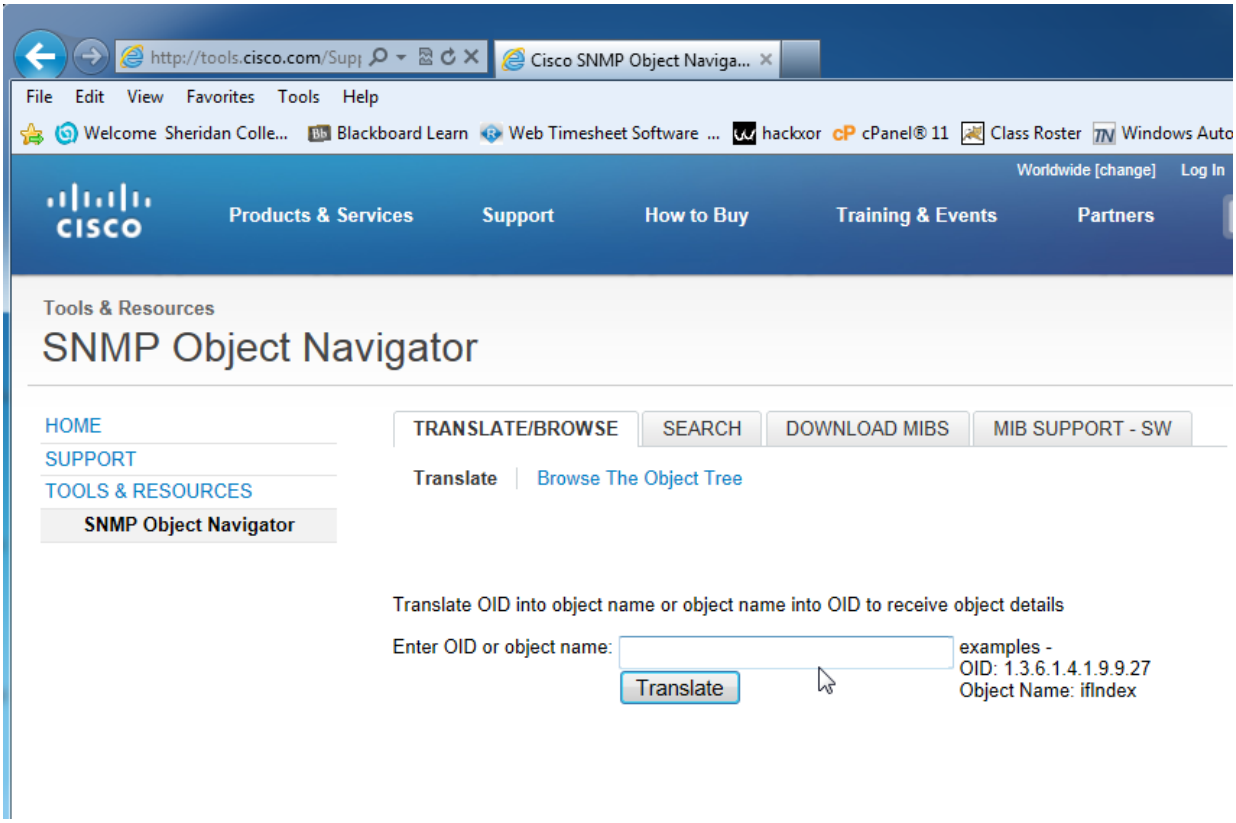
a. À l'aide de l'outil de recherche situé en haut de la fenêtre, recherchez **SNMP Object Navigator**.

b. Sélectionnez **SNMP Object Navigator MIB Download MIBs OID OIDs** dans les résultats.

c. Accédez à la page **MIB Locator**. Cliquez sur **SNMP Object Navigator**.



d. Dans la page **SNMP Object Navigator**, décodez le numéro de code OID à l'aide de l'utilitaire PowerSNMP Free Manager généré à la Partie 3, Étape 2. Entrez le numéro de code OID et cliquez sur **Translate**.



e. Enregistrez ci-dessous les numéros de code OID ainsi que les traductions des messages correspondants.

_____

_____

_____

_____

_____

Par exemple, la description du code OID 1.3.6.1.6.3.1.1.5.4 en tant que déroutement linkUp signifie que l'entité SNMP, qui joue le rôle d'agent, a détecté que l'objet ifOperStatus a quitté l'état « down » pour l'une de ses liaisons de communication et qu'elle est passée dans un autre état (mais pas l'état notPresent). Cet autre état est indiqué par la valeur incluse de l'objet ifOperStatus.

Remarques générales

1. Citez quelques-uns des avantages potentiels de la surveillance d'un réseau à l'aide du protocole SNMP ?

_____

_____

_____

_____

_____

Les réponses peuvent varier, mais les étudiants peuvent évoquer la capacité du protocole SNMP, en tant que protocole de plate-forme ouverte et croisée, de fonctionner avec de nombreux types de périphériques différents, y compris des ordinateurs hôte, sur le réseau. Le protocole SNMP bénéficie de la présence d'un administrateur réseau dont le travail consiste à contrôler l'état et la configuration des hôtes réseau sur la totalité de ce dernier.

2. Pourquoi est-il préférable de n'utiliser que l'accès en lecture seule avec le protocole SNMPv2 ?

_____

_____

Parce que le protocole SNMPv2 ne prend en charge que les identifiants de communauté non chiffrés et que par conséquent l'utilisation d'un accès en lecture/écriture représenterait un risque de sécurité plus élevé.

Tableau récapitulatif des interfaces de routeur

Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes de Cisco IOS.

Configurations des périphériques

Routeur R1

```
R1#show run
Building configuration...

Current configuration : 5969 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
```

```
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
!
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
```

```
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps c3g
snmp-server enable traps entity-sensor threshold
snmp-server enable traps adslline
snmp-server enable traps vdsl2line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp cbgp2
snmp-server enable traps isis
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-
change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
```

```
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps waas
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps firewall serverstatus
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.1.3 version 2c ciscolab
!
control-plane
```

```
!
line con 0
 password cisco
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Routeur R2

```
R2#show run
Building configuration...

Current configuration : 1251 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
 no ip address
```

```
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.2.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
```

```
end
```

Commutateur S1

```
S1#show run
Building configuration...

Current configuration : 4618 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
```

```
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list standard SNMP_ACL
 permit 192.168.1.3
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
```

```
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-
guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet police
snmp-server enable traps fru-ctrl
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps ipsla
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.1.3 version 2c ciscolab
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```