Atelier – Configuration et vérification des listes ACL IPv4 standard

Topologie

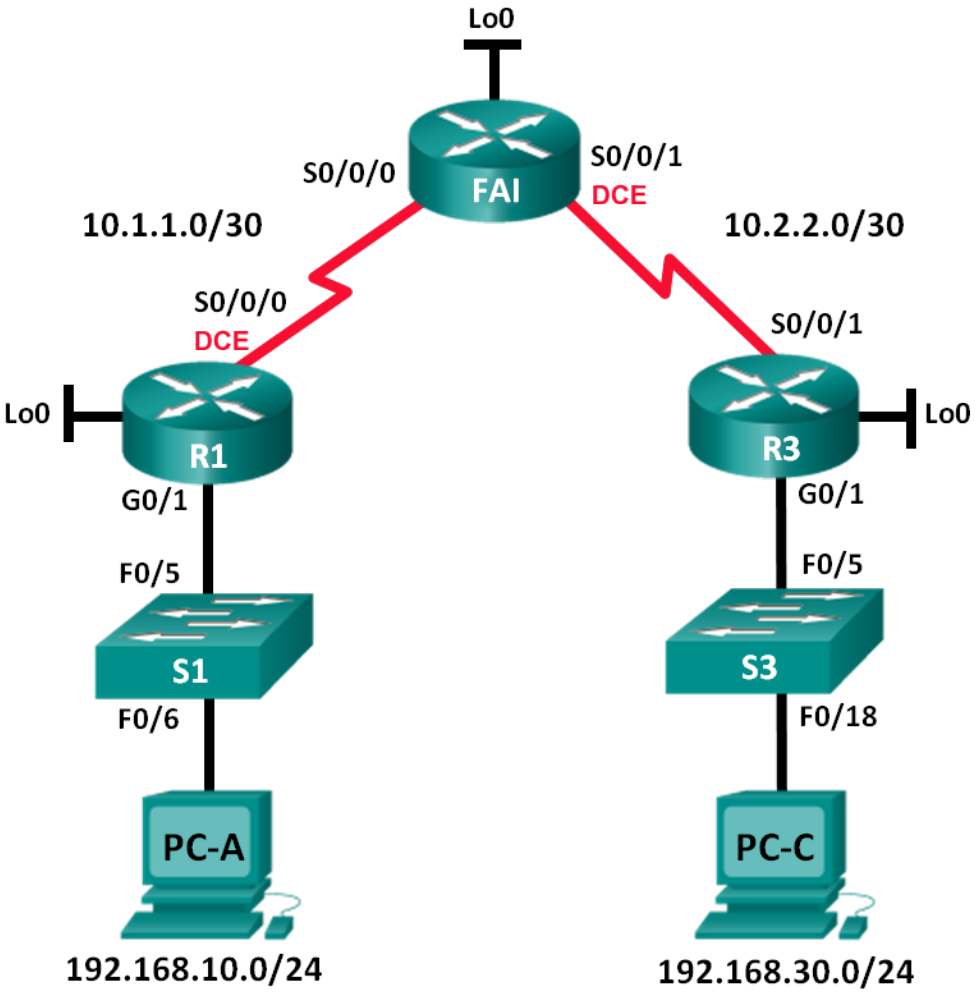

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192168.20,1	255.255.255.0	N/A
	S0/0/0 (ETCD)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (ETCD)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	Carte réseau	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	Carte réseau	192.168.30.3	255.255.255.0	192.168.30.1

Objectifs

Partie 1 : configurer la topologie et initialiser les périphériques

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2 : Configurer les périphériques et vérifier la connectivité

- Attribuez une adresse IP statique aux PC.
- Configurez les paramètres de base sur les routeurs.
- Configurez les paramètres de base sur les commutateurs.
- Configurez le routage OSPF sur les routeurs R1, ISP et R3.
- Vérifiez la connectivité entre les périphériques.

Partie 3 : configuration et vérification des listes de contrôle d'accès numérotées et nommées standard

- Configurez, appliquez et vérifiez une liste de contrôle d'accès standard numérotée.
- Configurez, appliquez et vérifiez une liste de contrôle d'accès nommée.

Partie 4 : modification d'une liste de contrôle d'accès standard

- Modifiez et vérifiez une liste de contrôle d'accès standard nommée.
- Testez la liste de contrôle d'accès.

Contexte/scénario

La sécurité réseau est un sujet important lors de la conception et de la gestion des réseaux IP. La possibilité de configurer des règles appropriées pour filtrer les paquets, sur base de politiques de sécurité définies, est une compétence importante.

Dans ces travaux pratiques, vous allez configurer le filtrage des règles pour deux bureaux représentés par R1 et R3. La direction a établi certaines stratégies d'accès entre les LAN situés au niveau de R1 et R3, que vous devez implémenter. Le routeur ISP situé entre R1 et R3 ne comportera aucune liste de contrôle d'accès. Aucun accès administratif ne serait octroyé à un routeur ISP étant donné que vous pouvez uniquement contrôler et gérer votre propre matériel.

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 différer de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. En cas de doute, contactez votre formateur.

Ressources requises

- 3 routeurs (Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaires)
- 2 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet et série conformément à la topologie

Partie 1 : Configurer la topologie et initialiser les périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et supprimer toutes les configurations s'il y a lieu.

Étape 1 : Câblez le réseau conformément à la topologie indiquée.

Étape 2 : Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2 : Configuration des périphériques et vérification de la connectivité

Dans la Partie 2, vous configurerez les paramètres de base sur les routeurs, les commutateurs et les ordinateurs. Reportez-vous à la topologie et à la table d'adressage pour le nom des périphériques et les informations d'adressage.

Étape 1 : Configurez les adresses IP sur PC-A et PC-C.

Étape 2 : Configurez les paramètres de base pour les routeurs.

a. Accédez au routeur par la console et passez en mode de configuration globale.

b. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le routeur.

```
no ip domain-lookup
hostname R1
```

```
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configurez le nom du périphérique conformément à la topologie.

d. Créez des interfaces de bouclage sur chaque routeur comme indiqué dans la table d'adressage.

e. Configurez les adresses IP d'interface conformément à la topologie et à la table d'adressage.

f. Attribuez une fréquence d'horloge de 128000 aux interfaces série DCE.

g. Activez l'accès Telnet.

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

Étape 3 : (Facultatif) Configurez les paramètres de base sur les commutateurs.

a. Accédez au commutateur par la console et passez en mode de configuration globale.

b. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le commutateur.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

c. Configurez le nom du périphérique conformément à la topologie.

d. Configurez l'adresse IP de l'interface de gestion représentée conformément à la topologie et à la table d'adressage.

e. Configurez une passerelle par défaut.

f. Activez l'accès Telnet.

g. Copier la configuration en cours en tant que configuration de démarrage

Étape 4 : Configurez le routage RIP sur les routeurs R1, ISP et R3.

a. Configurez le protocole RIP version 2 et diffusez tous les réseaux sur les routeurs R1, ISP et R3. La configuration OSPF pour les routeurs R1 et ISP est incluse à titre de référence.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0

ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0
```

b. Après la configuration du protocole RIP sur les routeurs R1, ISP et R3, vérifiez que tous les routeurs disposent de tables de routage complètes répertoriant tous les réseaux. Dépannez si ce n'est pas le cas.

Étape 5 : Vérifiez la connectivité entre les périphériques.

Remarque : il est très important de vérifier si la connectivité fonctionne **avant** de configurer et d'appliquer des listes d'accès ! Veillez à vous assurer que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

a. À partir de PC-A, envoyez une requête ping vers PC-C et l'interface de bouclage sur R3. Les requêtes ping ont-elles abouti ? _____

b. À partir de R1, envoyez une requête ping vers PC-C et l'interface de bouclage sur R3. Les requêtes ping ont-elles abouti ? _____

c. À partir de PC-C, envoyez une requête ping vers PC-A et l'interface de bouclage sur R1. Les requêtes ping ont-elles abouti ? _____

d. À partir de R3, envoyez une requête ping vers PC-A et l'interface de bouclage sur R1. Les requêtes ping ont-elles abouti ? _____

Partie 3 : Configuration et vérification des listes de contrôle d'accès numérotées et nommées standard

Étape 1 : Configurez une liste de contrôle d'accès standard numérotée.

Les listes de contrôle d'accès standard filtrent le trafic en fonction de l'adresse IP de la source. L'une des meilleures pratiques types pour les listes de contrôle d'accès standard consiste à la configurer et l'appliquer aussi près que possible de la destination. Pour la première liste de contrôle d'accès, créez une liste de contrôle d'accès numérotée standard qui autorise le trafic de tous les hôtes du réseau 192.168.10.0/24 et de tous les hôtes du réseau 192.168.20.0/24 pour accéder à tous les hôtes du réseau 192.168.30.0/24. La stratégie de sécurité indique également qu'une entrée de contrôle d'accès (ACE) **deny any**, également appelée instruction ACL, doit figurer à la fin de toutes listes de contrôle d'accès.

Quel masque générique utiliseriez-vous pour permettre à tous les hôtes sur le réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24 ?

_____

En suivant les meilleures pratiques recommandées par Cisco, sur quel routeur placeriez-vous cette liste de contrôle d'accès ? _____

Sur quelle interface placeriez-vous cette liste de contrôle d'accès ? Dans quelle direction l'appliqueriez-vous ?

_____

a. Configurez la liste de contrôle d'accès sur R3. Utilisez 1 pour le numéro de liste d'accès.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c. Vérifiez une liste de contrôle d'accès numérotée.

L'utilisation de diverses commandes **show** peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

Pour afficher la liste d'accès 1 dans son intégralité avec toutes les listes de contrôle d'accès, quelle commande utiliseriez-vous ?

_____

Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction ?

_____

1) Sur R3, exécutez la commande **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) Sur R3, exécutez la commande **show ip interface g0/1**.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

3) Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.10.0/24 et le réseau 192.168.30.0/24. À partir de l'invite de commande de PC-A, envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti ? _____

4) Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.20.0/24 et le réseau 192.168.30.0/24. Vous devez effectuer une requête ping étendue et utiliser l'adresse de bouclage 0 sur R1 comme source. Envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti ? _____

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d. À partir de l'invite de R1, envoyez une requête ping à l'adresse IP de PC-C.

```
R1# ping 192.168.30.3
```

La requête ping a-t-elle abouti ? Les élèves doivent justifier la réponse.

_____

_____

_____

Étape 2 : Configurez une liste de contrôle d'accès standard nommée.

Créez une liste de contrôle d'accès standard nommée conformément à la stratégie suivante : autoriser le trafic de tous les hôtes sur 192.168.40.0/24 à accéder à tous les hôtes sur le réseau 192.168.10.0/24. En outre, autorisez uniquement les accès du PC-C hôte au réseau 192.168.10.0/24. Cette liste d'accès devrait s'appeler BRANCH-OFFICE-POLICY.

En suivant les meilleures pratiques recommandées par Cisco, sur quel routeur placeriez-vous cette liste de contrôle d'accès ? _____

Sur quelle interface placeriez-vous cette liste de contrôle d'accès ? Dans quelle direction l'appliqueriez-vous ?

_____

a. Créez la liste de contrôle d'accès nommée standard ACL BRANCH-OFFICE-POLICY sur R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
```

```
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Sur base de la première entrée de contrôle d'accès d'autorisation dans la liste d'accès, quelle est l'autre façon d'écrire celà ?

_____

b. Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Vérifiez une liste de contrôle d'accès nommée.

1) Sur R1, exécutez la commande **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Y a-t-il une différence entre cette liste de contrôle d'accès sur R1 et la liste de contrôle d'accès sur R3 ? Le cas échéant, quelle est-elle ?

_____

_____

_____

_____

_____

2) Sur R1, exécutez la commande **show ip interface g0/1**.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  La liste d'accès sortante est BRANCH-OFFICE-POLICY
  Inbound access list is not set
<résultat omis>
```

3) Testez la liste de contrôle d'accès. À partir de l'invite de commande sur PC-C, envoyez une requête ping à l'adresse IP de PC-A. Les requêtes ping ont-elles abouti ? _____

4) Testez la liste de contrôle d'accès pour vous assurer que seul l'hôte PC-C soit autorisé à accéder au 192.168.10.0/24. Vous devez effectuer une requête ping étendue et utiliser l'adresse G0/1 sur R3 comme source. Envoyez une requête ping à l'adresse IP de PC-A. Les requêtes ping ont-elles abouti ? _____

5) Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.40.0/24 et le réseau 192.168.10.0/24. Vous devez effectuer une requête ping étendue et utiliser l'adresse de bouclage 0 sur R3 comme source. Envoyez une requête ping à l'adresse IP de PC-A. Les requêtes ping ont-elles abouti ? _____

Partie 4 : Modification d'une liste de contrôle d'accès standard

En entreprise, il est courant que les stratégies de sécurité évoluent. Pour cette raison, les listes de contrôle d'accès peuvent être modifiées. Dans la partie 4, vous allez modifier l'une des listes de contrôle d'accès que vous avez précédemment configurées pour l'adapter à la nouvelle politique de gestion mise en place.

La direction a décidé que les utilisateurs du réseau 209.165.200.224/27 devait disposer d'un accès intégral au réseau 192.168.10.0/24. La direction veut également que les listes de contrôle d'accès sur tous ses routeurs suivent des règles cohérentes. Une entrée de contrôle d'accès **deny any** doit être placée à la fin de toutes les listes de contrôle d'accès. Vous devez modifier la liste de contrôle d'accès BRANCH-OFFICE-POLICY.

Vous allez ajouter deux lignes supplémentaires à cette liste de contrôle d'accès. Il existe deux manières de le faire :

OPTION 1 : exécutez une commande **no ip access-list standard BRANCH-OFFICE-POLICY** en mode de configuration globale. Cela aurait pour effet de supprimer l'intégralité de la liste de contrôle d'accès sur le routeur. Selon l'IOS du routeur, l'un des scénarios suivants se produirait : tout filtrage des paquets serait annulé et tous les paquets seraient autorisés à transiter par le routeur ; ou, parce que vous n'avez pas supprimé la commande **ip access-group** sur l'interface G0/1, le filtrage serait toujours en place. Quoi qu'il en soit, lorsque la liste de contrôle d'accès a disparu, vous pouvez la retaper dans son intégralité, ou la copier-coller à partir d'un éditeur de texte.

OPTION 2 : vous pouvez modifier les listes de contrôle d'accès existantes en ajoutant ou en supprimant des lignes spécifiques dans la liste elle-même. Cela peut être pratique, en particulier avec des listes de contrôle d'accès comportant de nombreuses lignes de code. Le fait de retaper la liste de contrôle d'accès entière ou de la copier-coller peut facilement engendrer des erreurs. La modfication de lignes spécifiques dans la liste de contrôle d'accès est facile à effectuer.

Remarque : dans le cadre de ces travaux pratiques, utilisez la deuxième option.

Étape 1 : Modifiez une liste de contrôle d'accès standard nommée.

a. En mode EXEC privilégié du routeur R1, lancez la commande **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

b. Ajoutez deux lignes supplémentaires à la fin de la liste de contrôle d'accès. À partir du mode de configuration globale, modifiez la liste de contrôle d'accès BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. Vérifiez la liste de contrôle d'accès.

1) Sur R1, exécutez la commande **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny   any
```

Devez-vous appliquer la liste BRANCH-OFFICE-POLICY à l'interface G0/1 sur R1 ?

_____

_____

2) À partir de l'invite de commande du routeur ISP, exécutez une requête ping étendue. Testez la liste de contrôle d'accès pour voir si elle permet le trafic entre le réseau 209.165.200.224/27 et le réseau 192.168.10.0/24. Vous devez effectuer une requête ping étendue et utiliser l'adresse de bouclage 0 sur ISP comme source. Envoyez une requête ping à l'adresse IP de PC-A. Les requêtes ping ont-elles abouti ? _____

Remarques générales

1. Comme vous pouvez le constater, les listes de contrôle d'accès standard sont particulièrement puissantes et fonctionnent très bien. Pourquoi auriez-vous jamais besoin d'utiliser les listes de contrôle d'accès étendues ?

   _____

   _____

   _____

   _____

2. Généralement, il y a plus d'éléments à taper lors de l'utilisation d'une liste de contrôle d'accès nommée par opposition à une liste de contrôle d'accès numérotée. Pour quelle raison choisiriez-vous des listes de contrôle d'accès nommées plutôt que des listes d'accès numérotées ?

   _____

   _____

   _____

   _____

Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	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)
1 900	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)
2 801	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)
2 811	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)
2 900	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 différentes combinaisons d'interfaces Ethernet et série possibles 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 Cisco IOS.