Travaux pratiques : configuration et vérification des listes de contrôle d'accès IPv6

Topologie

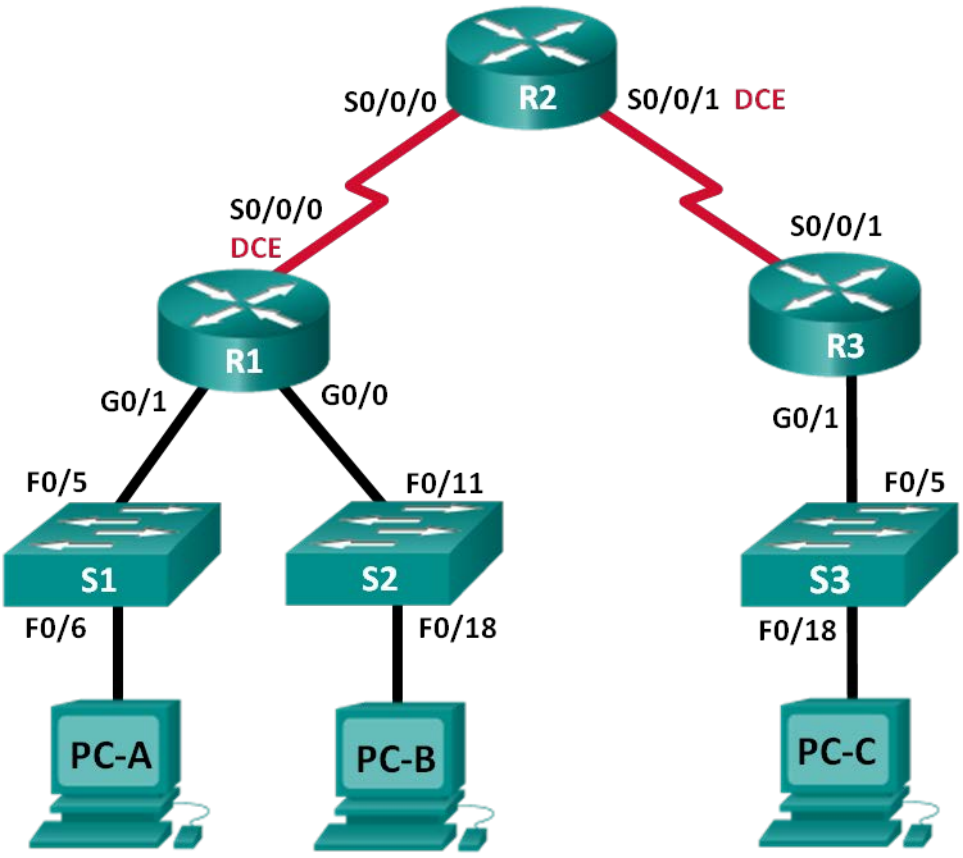


Table d'adressage

Périphérique	Interface	Adresse IP	Passerelle par défaut
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Objectifs

Partie 1 : configuration de la topologie et initialisation des périphériques

Partie 2 : configuration des périphériques et vérification de la connectivité

Partie 3 : configuration et vérification des listes de contrôle d'accès IPv6

Partie 4 : modification des listes de contrôle d'accès IPv6

Contexte/scénario

Vous pouvez filtrer le trafic IPv6 en créant des listes de contrôle d'accès (ACL) IPv6 et en les appliquant aux interfaces de la même façon que vous créez des listes de contrôle d'accès nommées IPv4. Les types de liste de contrôle d'accès IPv6 sont étendues et nommées. Les listes de contrôle d'accès standard et numérotées ne sont plus utilisés avec IPv6. Pour appliquer une liste de contrôle d'accès IPv6 à une interface vty, vous utilisez la nouvelle commande **ipv6 traffic-filter**. La commande **ipv6 access-class** est toujours utilisée pour appliquer une liste de contrôle d'accès IPv6 aux interfaces.

Au cours de ces travaux pratiques, vous appliquerez des règles de filtrage IPv6 puis vérifierez qu'elles limitent les accès comme prévu. Vous modifierez également une liste de contrôle d'accès IPv6 et supprimez les compteurs de correspondance.

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 2960s 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.

Ressources requises

3 routeurs (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)

3 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)

3 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation du 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: Configuration de la topologie et initialisation des 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.

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 au début de ces travaux pratiques pour le nom des périphériques et les informations d'adressage.

Étape 1: Configurez les adresses IPv6 sur tous les ordinateurs.

Configurez les adresses de monodiffusion globale IPv6 conformément à la table d'adressage. Utilisez l'adresse link-local **FE80::1** pour la passerelle par défaut sur tous les ordinateurs.

Étape 2: Configurez les commutateurs.

a. Désactivez la recherche DNS.

b. Attribuez le nom d'hôte.

c. Attribuez **ccna-lab.com** comme nom de domaine.

d. Chiffrez les mots de passe en clair.

e. Créez une bannière MOTD avertissant les utilisateurs de l'interdiction de tout accès non autorisé.

f. Créez une base de données utilisateur locale avec **admin** comme nom d'utilisateur et **classadm** comme mot de passe.

g. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

h. Attribuez **cisco** comme mot de passe de console et activez la connexion.

i. Activez la connexion sur les lignes VTY en utilisant la base de données locale.

j. Générez une clé de chiffrement RSA pour SSH avec une taille de module de 1024 bits.

k. Modifiez les lignes VTY d'entrée de transport à tous pour SSH et Telnet uniquement.

l. Attribuez une adresse IPv6 à VLAN 1 en fonction de la table d'adressage.

m. Désactivez administrativement toutes les interfaces inactives.

Étape 3: Configurez les paramètres de base sur tous les routeurs.

a. Désactivez la recherche DNS.

b. Attribuez le nom d'hôte.

c. Attribuez **ccna-lab.com** comme nom de domaine.

d. Chiffrez les mots de passe en clair.

e. Créez une bannière MOTD avertissant les utilisateurs de l'interdiction de tout accès non autorisé.

f. Créez une base de données utilisateur locale avec **admin** comme nom d'utilisateur et **classadm** comme mot de passe.

g. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

h. Attribuez **cisco** comme mot de passe de console et activez la connexion.

i. Activez la connexion sur les lignes VTY en utilisant la base de données locale.

j. Générez une clé de chiffrement RSA pour SSH avec une taille de module de 1024 bits.

k. Modifiez les lignes VTY d'entrée de transport à tous pour SSH et Telnet uniquement.

Étape 4: Configurez les paramètres IPv6 sur R1.

a. Configurez l'adresse de monodiffusion IPv6 sur l'interface G0/0, G0/1 et S0/0/0.

b. Configurez l'adresse link-local IPv6 sur les interfaces G0/0, G0/1 et S0/0/0. Utilisez **FE80::1** pour l'adresse link-local sur chacune des trois interfaces.

c. Définissez la fréquence d'horloge sur S0/0/0 à 128000.

d. Activez les interfaces.

e. Activez le routage monodiffusion IPv6.

f. Configurez une route par défaut IPv6 pour utiliser l'interface S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Étape 5: Configurez les paramètres IPv6 sur R2.

a. Configurez l'adresse de monodiffusion IPv6 sur les interfaces S0/0/0 et S0/0/1.

b. Configurez l'adresse link-local IPv6 sur les interfaces S0/0/0 et S0/0/1. Utilisez **FE80::2** pour l'adresse link-local sur les deux interfaces.

c. Définissez la fréquence d'horloge sur S0/0/1 à 128000.

d. Activez les interfaces.

e. Activez le routage monodiffusion IPv6.

f. Configurez les routes IPv6 statiques pour la prise en charge du trafic des sous-réseaux du réseau local des routeurs R1 et R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Étape 6: Configurez les paramètres IPv6 sur R3.

a. Configurez l'adresse de monodiffusion IPv6 sur les interfaces G0/1 et S0/0/1.

b. Configurez l'adresse link-local IPv6 sur les interfaces G0/1 et S0/0/1. Utilisez **FE80::1** pour les adresses link-local sur les deux interfaces.

c. Activez les interfaces.

d. Activez le routage monodiffusion IPv6.

e. Configurez une route par défaut IPv6 pour utiliser l'interface S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

Étape 7: Vérifiez la connectivité.

a. Chaque PC devrait être capable d'envoyer correctement une requête ping à tout autre PC dans la topologie.

b. Établissez une connexion Telnet à R1 à partir de tous les ordinateurs de la topologie.

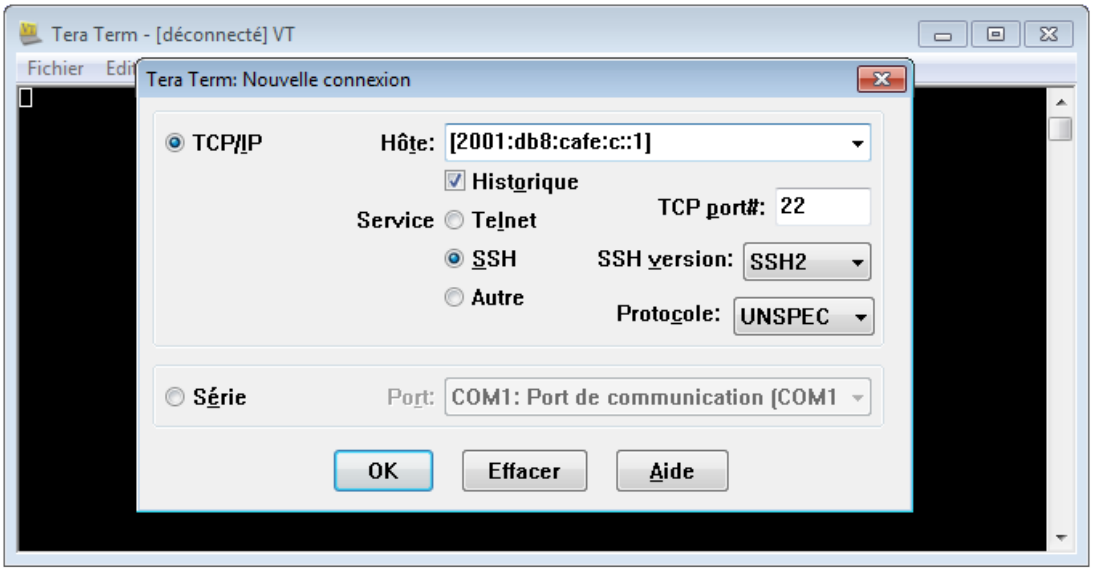
c. Établissez une connexion SSH à R1 à partir de tous les ordinateurs de la topologie.

d. Établissez une connexion Telnet à S1 à partir de tous les ordinateurs de la topologie.

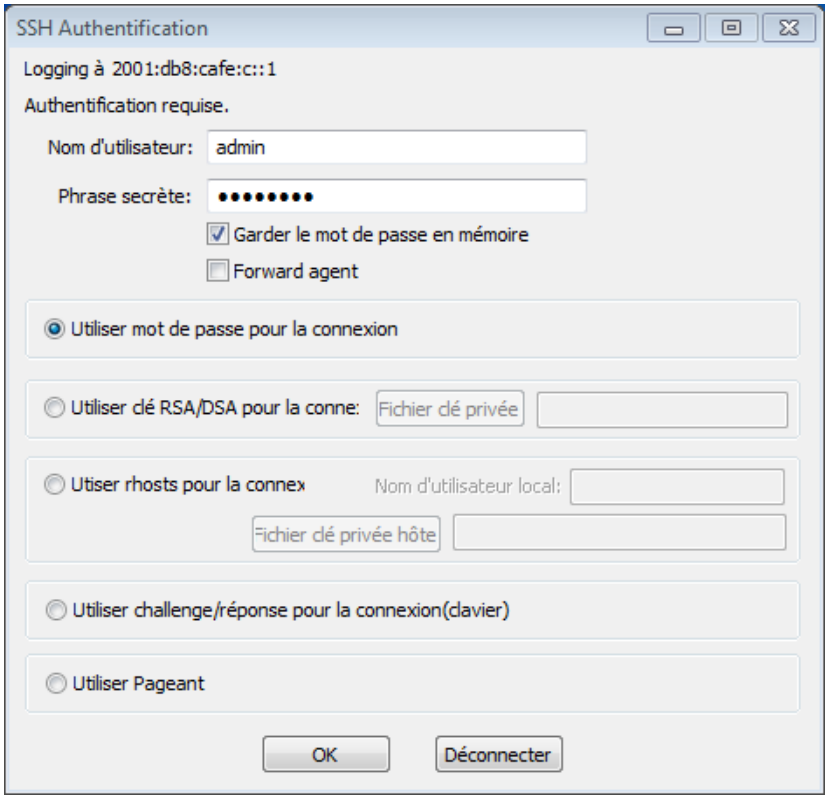
e. Établissez une connexion SSH à S1 à partir de tous les ordinateurs de la topologie.

f. Dépannez les problèmes de connectivité dès maintenant parce que les listes de contrôle d'accès que vous créez dans la Partie 3 de ces travaux pratiques restreindront l'accès à certaines zones du réseau.

Remarque : Tera Term requiert l'insertion de l'adresse IPv6 cible entre parenthèses. Entrez l'adresse IPv6 comme indiqué, cliquez sur **OK**, puis cliquez sur **Continuer** pour accepter l'avertissement de sécurité et vous connecter au routeur.



Saisissez les identifiants utilisateur configurés (nom d'utilisateur **admin** et mot de passe **classadm**) et sélectionnez **Utiliser mot de passe pour la connexion** dans la boîte de dialogue SSH Authentification. Cliquez sur **OK** pour continuer.



Partie 3: Configuration et vérification des listes de contrôle d'accès IPv6

Étape 1: Configurez et vérifiez les restrictions VTY sur R1.

a. Créez une liste de contrôle d'accès pour autoriser uniquement les hôtes du réseau 2001:db8:acad:a::/64 à établir une connexion Telnet à R1. Tous les hôtes doivent uniquement pouvoir établir une connexion ssh à R1.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
R1(config-ipv6-acl)# permit tcp any anyeq 22
```

b. Appliquez la liste de contrôle d'accès RESTRICT-VTY aux lignes VTY de R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

c. Affichez la nouvelle liste de contrôle d'accès.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
permittcp 2001:DB8:ACAD:A::/64 any sequence 10
permittcp any anyeq 22 sequence 20
```

d. Vérifiez que la liste de contrôle d'accès RESTRICT-VTY autorise uniquement le trafic Telnet à partir du réseau 2001:db8:acad:a::/64.

Comment la liste de contrôle d'accès RESTRICT-VTY permet-elle uniquement aux hôtes du réseau 2001:db8:acad:a::/64 d'établir une connexion Telnet à R1 ?

Quelle est la fonction de la deuxième instruction permit dans la liste de contrôle d'accès RESTRICT-VTY ?

Étape 2: Limitez les accès via Telnet au réseau 2001:db8:acad:a::/64.

a. Créez une liste de contrôle d'accès appelée RESTRICTED-LAN qui bloquera les accès Telnet au réseau 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

b. Appliquez la liste de contrôle d'accès RESTRICTED-LAN à l'interface G0/1 pour tout le trafic sortant.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

c. Établissez une connexion Telnet à S1 à partir de PC-B et PC-C pour vérifier que Telnet a été restreint. Établissez une connexion SSH à S1 à partir de PC-B pour vérifier qu'il reste accessible via SSH. Dépannez le cas échéant.

d. Utilisez la commande **show ipv6 access-list** pour afficher la liste de contrôle d'accès RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
permit ipv6 any any (45 matches) sequence 30
```

Notez que chaque instruction identifie le nombre d'occurrences ou de correspondances qui ont eu lieu depuis que la liste de contrôle d'accès a été appliquée à l'interface.

e. Utilisez **clear ipv6 access-list** pour réinitialiser les compteurs de correspondance pour la liste de contrôle d'accès RESTRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

f. Affichez de nouveau la liste de contrôle d'accès avec la commande **show access-lists** pour vérifier que les compteurs ont été effacés.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
permit ipv6 any any sequence 30
```

Partie 4: Modification des listes de contrôle d'accès IPv6

Dans la Partie 4, vous allez modifier la liste de contrôle d'accès RESTRICTED-LAN que vous avez créée dans la Partie 3. Il est toujours judicieux de supprimer la liste de contrôle d'accès de l'interface à laquelle elle est appliquée avant de la modifier. Une fois que vous avez terminé vos modifications, réappliquez la liste de contrôle d'accès à l'interface.

Remarque : de nombreux administrateurs réseau créeront une copie de la liste de contrôle d'accès et modifieront la copie. Au terme des modifications, l'administrateur supprimera l'ancienne liste de contrôle d'accès et appliquera la liste de contrôle d'accès récemment modifiée à l'interface. Cette méthode conserve la liste de contrôle d'accès jusqu'à ce que vous soyez prêt à appliquer la copie modifiée de cette dernière.

Étape 1: Supprimez la liste de contrôle d'accès sur l'interface.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Étape 2: Utilisez la commande show access-lists pour afficher la liste de contrôle d'accès.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (36 matches) sequence 30
```

Étape 3: Insérez une nouvelle instruction de liste de contrôle d'accès au moyen de la numérotation séquentielle.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a
eq 23 sequence 15
```

À quoi sert cette nouvelle instruction permit ?

Étape 4: Insérez une nouvelle instruction ACL à la fin de la liste de contrôle d'accès.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Remarque : cette instruction permit est uniquement utilisée pour voir comment ajouter une instruction à la fin d'une liste de contrôle d'accès. Cette ligne ACL ne trouverait jamais de correspondance parce que l'instruction permit précédente correspond à tout.

Étape 5: Utilisez la commande do show access-lists pour afficher la modification de la liste de contrôle d'accès.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
```

```
        deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
        permit ipv6 any any (124 matches) sequence 30
    permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Remarque : la commande **do** peut être utilisée pour exécuter toute commande d'exécution privilégiée à partir du mode de configuration globale ou d'un sous-mode.

Étape 6: Supprimez une instruction de liste de contrôle d'accès.

Utilisez la commande **no** pour supprimer l'instruction permit que vous venez d'ajouter.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Étape 7: Utilisez la commande do show access-list RESTRICTED-LAN pour afficher la liste de contrôle d'accès.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (214 matches) sequence 30
```

Étape 8: Appliquez à nouveau la liste de contrôle d'accès RESTRICTED-LAN à l'interface G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Étape 9: Testez les modifications de la liste de contrôle d'accès.

Établissez une connexion Telnet vers S1 à partir de PC-B. Dépannez le cas échéant.

Remarques générales

1. Quel est l'élément qui entraîne l'augmentation du compte de correspondances dans l'instruction RESTRICTED-LAN **permit ipv6 any any** ?

2. Quelle commande utiliseriez-vous pour réinitialiser les compteurs pour la liste de contrôle d'accès sur les lignes VTY ?

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.