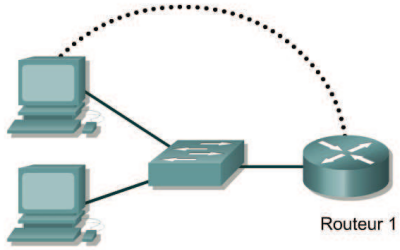
TP 11.2.1a Configuration de listes de contrôle d'accès standard



Désignation du routeur	Nom du routeur	Adresse FA0/0	Masque de sous-réseau	Mot de passe " enable secret "	Mot de passe console/ enable/VTY
Routeur 1	GAD	192.168.14.1	255.255.255.0	classe	cisco

Objectif

- Configurer et appliquer une liste de contrôle d'accès standard en vue d'autoriser ou de refuser un type de trafic particulier.
- Tester la liste de contrôle d'accès pour déterminer si les résultats escomptés ont été atteints.

Prérequis/Préparation

Installez un réseau similaire à celui du schéma. Tout routeur doté d'une interface indiquée dans le schéma ci-dessus peut être utilisé, par exemple les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Reportez-vous au tableau qui se trouve à la fin du TP pour repérer les identifiants d'interfaces à utiliser en fonction de l'équipement disponible. Dans ce TP, les informations affichées par le routeur lors de sa configuration ont été obtenues avec un routeur de la gamme 1721. Celles-ci peuvent varier légèrement avec un autre routeur. Les étapes qui suivent doivent être exécutées sur chaque routeur, sauf indication contraire.

Lancez une session HyperTerminal comme indiqué dans le TP intitulé Établissement d'une session en mode console avec HyperTerminal.

Remarque : Suivez les instructions d'effacement et de rechargement qui se trouvent à la fin de ce TP. Exécutez ces étapes sur le routeur utilisé dans ce TP avant de continuer.

Étape 1 Configurez le nom d'hôte et les mots de passe sur le routeur Gadsden

a. Sur le routeur Gadsden, entrez le mode de configuration globale et configurez le nom d'hôte comme indiqué dans le tableau. Configurez ensuite la console, le terminal virtuel et les mots de passe enable. Configurez l'interface FastEthernet sur le routeur conformément au tableau.

Étape 2 Configurez les hôtes sur le segment Ethernet

a. Hôte 1

Adresse IP	192.168.14.2
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

b. Hôte 2

Adresse IP	192.168.14.3
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

Étape 3 Enregistrez les informations de configuration en mode privilégié

```
GAD#copy running-config startup-config
```

Étape 4 Envoyez une requête ping à la passerelle par défaut à partir de chacun des deux hôtes pour confirmer la connectivité

a. Si les requêtes ping échouent, corrigez la configuration et recommencez jusqu'à ce qu'elles réussissent.

Étape 5 Interdisez l'accès à l'interface Ethernet à partir des hôtes

a. Créez une liste de contrôle d'accès qui interdira l'accès à FastEthernet 0 depuis le réseau 192.168.14.0.

b. À l'invite de configuration du routeur, entrez la commande suivante :

```
GAD(config)#access-list 1 deny 192.168.14.0  0.0.0.255
GAD(config)#access-list 1 permit any
```

c. À quoi sert la deuxième instruction ? _____

Étape 6 Envoyez des requêtes ping au routeur à partir des hôtes

a. Ces requêtes ping ont-elles réussi ? _____

b. Justifiez votre réponse._____

Étape 7 – Appliquez la liste de contrôle d'accès à l'interface

a. À l'invite du mode interface FastEthernet 0, entrez la commande suivante :

```
GAD(config-if)#ip access-group 1 in
```

Étape 8 Envoyez des requêtes ping au routeur à partir des hôtes

a. Ces requêtes ping ont-elles réussi ? _____

b. Justifiez votre réponse._____

Étape 9 Créez une nouvelle liste de contrôle d'accès

a. À présent, créez une liste de contrôle d'accès pour interdire l'envoi de requêtes ping depuis les hôtes dont le numéro est pair et l'autoriser depuis les hôtes impairs.

b. À quoi ressemblera cette liste de contrôle d'accès ? Terminez cette commande par une adresse IP de comparaison appropriée (aaa.aaa.aaa.aaa) et un masque générique (www.www.www.www) :

```
access-list 2 permit aaa.aaa.aaa.aaa  www.www.www.www
```

c. Pourquoi l'instruction **permit any** n'est-elle pas nécessaire cette fois-ci ?

_____

Étape 10 Appliquez la liste de contrôle d'accès à l'interface de routeur appropriée

a. Commencez par supprimer l'ancienne liste de contrôle d'accès en entrant **no ip access-group 1 in** à l'invite du mode de configuration d'interface.

b. Appliquez la nouvelle liste d'accès en entrant **ip access-group 2 in**

Étape 11 Envoyez des requêtes ping au routeur à partir des hôtes

a. La requête ping de l'hôte 1 a-t-elle réussi ? _____

b. Justifiez votre réponse. _____

c. La requête ping de l'hôte 2 a-t-elle réussi ? _____

d. Justifiez votre réponse. _____

Après avoir réalisé les étapes précédentes, déconnectez-vous en entrant **exit**. Mettez le routeur hors tension.

Effacement et rechargement du routeur

Passez en mode privilégié à l'aide de la commande **enable**.

Si le système vous demande un mot de passe, entrez **class**. Si « class » ne fonctionne pas, demandez de l'aide au professeur.

```
Router>enable
```

À l'invite du mode privilégié, entrez la commande **erase startup-config**.

```
Router#erase startup-config
```

Vous obtenez le message suivant :

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

Appuyez sur **Entrée** pour confirmer.

La réponse suivante devrait s'afficher :

```
Erase of nvram: complete
```

Ensuite, à l'invite du mode privilégié, entrez la commande **reload**.

```
Router#reload
```

Vous obtenez le message suivant :

```
System configuration has been modified. Save? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

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

Appuyez sur **Entrée** pour confirmer.

La première ligne de la réponse est la suivante :

```
Reload requested by console.
```

Après le rechargement du routeur, la ligne suivante s'affiche :

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

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Press RETURN to get started!
```

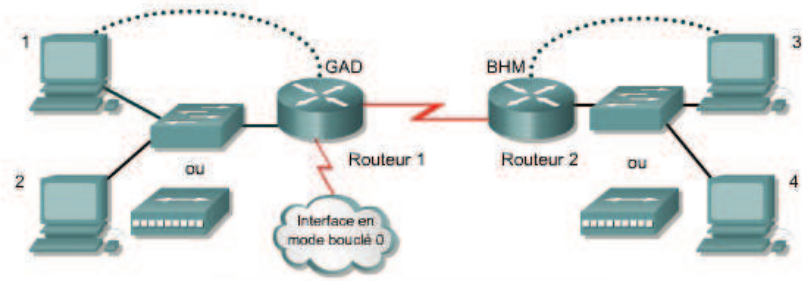
Appuyez sur **Entrée**.

Le routeur est prêt et le TP peut commencer.

Relevé des interfaces de routeur

Modèle de routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2	Interface 5
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	
Pour connaître la configuration exacte du routeur, observez les interfaces. Vous pourrez ainsi identifier le type du 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. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque appareil. Ce tableau d'interfaces ne comporte aucun autre type d'interface même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI pourrait illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans une commande IOS.					

TP 11.2.1b Listes de contrôle d'accès standard



Nom du routeur	Adresse FA0/0	Type d'interface S0/0	Adresse S0/0	Adresse LO0	Routage	Mot de passe enable	Mot depasse VTY
GAD	192.168.1.1 /24	DCE	192.168..2.1 /24	172.16.1.1 /24	RIP	cisco	class
BHM	192.168.3.1 /24	DTE	192.168.2.2 /24	--	RIP	cisco	class

Hôte	Adresse IP	Masque de sous-réseau	Passerelle
1	192.168.1.2	255.255.255.0	192.168.1.1
2	192.168.1.3	255.255.255.0	192.168.1.1
3	192.168.3.2	255.255.255.0	192.168.3.1
4	192.168.3.3	255.255.255.0	192.168.3.1

Objectif

Planifier, configurer et appliquer une liste de contrôle pour autoriser ou refuser un certain type de trafic et tester la liste de contrôle pour déterminer si les résultats escomptés ont été atteints.

Scénario

Le bureau principal de la société, qui se trouve à Gadsden (GAD), offre des services aux agences telles que le bureau de Birmingham (BHM). La sécurité et les performances ne sont pas des préoccupations majeures pour ces bureaux. Une liste de contrôle standard doit être mise en œuvre comme un outil simple et efficace de contrôle du trafic.

Infrastructure

L'hôte 3 représente un ordinateur en libre service qui doit disposer d'un accès limité au réseau local.

L'hôte 4 représente un hôte qui se trouve dans le bureau de Birmingham et l'interface en mode bouclé 0 sur le routeur GAD représente Internet.

Étape 1 Interconnexion de base des routeurs

a. Connectez les routeurs comme indiqué dans le schéma.

Étape 2 Configuration de base

a. Le routeur peut avoir conservé la configuration qu'il avait lors d'une précédente utilisation. Pour cette raison, effacez la configuration de démarrage et rechargez le routeur pour supprimer toutes les configurations restantes. À l'aide des informations apparaissant à la première page, configurez le routeur et l'hôte puis vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs.

b. Pour simuler Internet, ajoutez la configuration suivante au routeur GAD.

```
GAD(config)#interface loopback0
GAD(config-if)#address 172.16.1.1 255.255.255.0
GAD(config-if)#exit
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-if)#^z
```

Étape 3 Définissez les besoins en termes de liste de contrôle d'accès

a. L'ordinateur en libre service (hôte 3) doit disposer d'un accès limité au réseau local. Il faut donc créer une liste de contrôle standard pour empêcher le trafic provenant de cet hôte d'atteindre les autres réseaux. La liste de contrôle d'accès doit bloquer le trafic provenant de cet hôte mais autoriser tout autre trafic provenant de ce réseau. Dans ce cas, l'utilisation d'une liste de contrôle IP standard est appropriée car elle permet un filtrage en fonction de l'adresse source vers n'importe quelle destination.

b. Quelle est l'adresse source du poste de travail interactif ? _____

Étape 4 Planifiez les besoins en termes de liste de contrôle d'accès

a. Comme dans la plupart des projets, la planification est l'étape la plus importante du processus. Il faut d'abord définir les informations requises pour créer la liste de contrôle d'accès. Une liste de contrôle d'accès est constituée d'une série d'instructions ACL. Chacune des ces instructions est ajoutée de façon séquentielle à la liste de contrôle d'accès. Étant donné que la liste contient plusieurs instructions, il faut prévoir soigneusement la position de l'instruction.

b. Il a été décidé que cette liste nécessite deux étapes logiques. Chacune de ces étapes peut être accomplie par une instruction. Un éditeur de texte tel que Bloc-notes peut être utilisé en tant qu'outil de planification pour définir la logique et écrire la liste. Décrivez la logique dans l'éditeur de texte en entrant les lignes suivantes :

```
! arrêter le trafic provenant de l'hôte 3

! autoriser tout autre trafic
```


c. La liste de contrôle d'accès actuelle sera définie en fonction de cette logique. À l'aide des tables ci-dessous, indiquez les informations requises pour chaque instruction.

arrêter le trafic provenant de l'hôte 3			
N° de liste	Refuser ou autoriser	Adresse d'origine	Masque générique

autoriser tout autre trafic			
N° de liste	Refuser ou autoriser	Adresse d'origine	Masque générique

d. Quel serait le résultat si vous n'aviez pas inséré l'instruction autorisant toutes les autres adresses source ?

_____

e. Quel serait le résultat si l'ordre des deux instructions était inversé ?

_____

f. Pourquoi les deux instructions utilisent-elles le même numéro de liste de contrôle d'accès ?

_____

g. L'étape finale du processus de planification consiste à déterminer le meilleur emplacement pour la liste de contrôle d'accès et le sens dans lequel elle doit être appliquée. Examinez le schéma d'interréseau et choisissez l'interface et le sens d'application (direction) appropriés. Consignez les informations requises dans le tableau ci-dessous :

Routeur	**Interface**	**Direction**

Étape 5 Écrivez et appliquez la liste de contrôle d'accès

a. Utilisez la logique précédemment définie et les informations consignées de la liste de contrôle d'accès pour compléter les commandes dans l'éditeur de texte. La syntaxe de la liste doit être similaire à la syntaxe suivante :

```
! arrêter le trafic provenant de l'hôte 3
  access-list #deny adresse masque_générique
! autoriser tout autre trafic
   access-list #permit adresse masque_générique
```

b. Ajoutez à ce fichier texte les instructions de configuration pour l'application de la liste.

Les instructions de configuration ont la syntaxe suivante :

```
interface type #/#
ip access-group #{in, out}
```


c. Il faut maintenant appliquer la configuration du fichier texte au routeur. Passez en mode configuration sur le routeur approprié, puis copiez et collez la configuration. Observez l'affichage CLI pour vous assurer qu'aucune erreur ne s'est produite.

Étape 6 Vérifiez la liste de contrôle d'accès

Maintenant que la liste de contrôle d'accès est créée, elle doit être confirmée et testée.

a. La première étape consiste à vérifier si la liste a été configurée correctement dans le routeur. Utilisez la commande **`show access-lists`** pour vérifier la logique de la liste de contrôle d'accès. Notez le résultat.

_____

_____

_____

b. Ensuite, vérifiez si la liste d'accès a été appliquée, d'une part à l'interface appropriée et d'autre part dans le bon sens. Utilisez donc la commande **`show ip interface`** pour contrôler l'interface. Examinez le résultat pour chacune des interfaces et notez les listes qui leur sont appliquées.

Interface _____

Liste de contrôle d'accès pour le trafic externe _____

Liste de contrôle d'accès pour le trafic interne _____

c. Pour terminer, testez le fonctionnement de la liste de contrôle d'accès en envoyant des paquets à partir de l'hôte source et vérifiez que le résultat escompté est atteint (envoi autorisé ou refusé selon le cas). Pour ce test, utilisez une requête ping.

```
[  ] vérifier que l'hôte 3 PEUT envoyer une requête ping à l'hôte 4
[  ] vérifier que l'hôte 3 NE PEUT PAS envoyer de requête ping à l'hôte 1
[  ] vérifier que l'hôte 3 NE PEUT PAS envoyer de requête ping à l'hôte 2
[  ] vérifier que l'hôte 3 NE PEUT PAS envoyer de requête ping à GAD Fa0/0
[  ] vérifier que l'hôte 3 NE PEUT PAS envoyer de requête ping à GAD LO0
[  ] vérifier que l'hôte 4 PEUT envoyer une requête ping à l'hôte 1
[  ] vérifier que l'hôte 4 PEUT envoyer une requête ping à l'hôte 2
[  ] vérifier que l'hôte 4 PEUT envoyer une requête ping à GAD Fa0/0
[  ] vérifier que l'hôte 4 PEUT envoyer une requête ping à GAD LO0
```

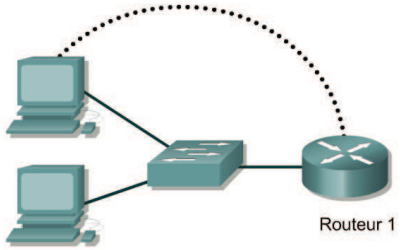
Étape 7 Décrivez par écrit la liste de contrôle d'accès

a. Toute administration réseau doit comporter une documentation. Utilisez le fichier texte créé pour la configuration et ajoutez-y des commentaires. Ce fichier doit également contenir les résultats générés par les commandes **`show access-lists`** et **`show ip interface`**.

b. Le fichier doit être sauvegardé avec le reste de la documentation réseau. La convention d'attribution de noms doit refléter la fonction du fichier et indiquer la date de mise en œuvre.

c. Lorsque vous avez terminé, effacez la configuration de démarrage sur les routeurs, retirez les câbles et les adaptateurs, puis rangez-les. Enfin, déconnectez-vous et mettez les routeurs hors tension.

TP 11.2.2a Configuration de listes de contrôle d'accès étendues



Désignation du routeur	Nom du routeur	Adresse FA0/0	Masque de sous-réseau	Mot de passe " enable secret "	Mot de passe console/ enable/VTY
Routeur 1	GAD	192.168.14.1	255.255.255.0	classe	cisco

Objectif

- Configurer et appliquer une liste de contrôle d'accès étendue en vue d'autoriser ou de refuser un type de trafic particulier.
- Tester la liste de contrôle d'accès pour déterminer si les résultats escomptés ont été atteints.

Prérequis/Préparation

Installez un réseau similaire à celui du schéma. Tout routeur doté d'une interface indiquée dans le schéma ci-dessus peut être utilisé, par exemple les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Reportez-vous au tableau qui se trouve à la fin du TP pour repérer les identifiants d'interfaces à utiliser en fonction de l'équipement disponible. Dans ce TP, les informations affichées par le routeur lors de sa configuration ont été obtenues avec un routeur de la gamme 1721. Celles-ci peuvent varier légèrement avec un autre routeur. Les étapes qui suivent doivent être exécutées sur chaque routeur, sauf indication contraire.

Lancez une session HyperTerminal comme indiqué dans le TP intitulé Établissement d'une session en mode console avec HyperTerminal.

Remarque : Suivez les instructions d'effacement et de rechargement qui se trouvent à la fin de ce TP. Exécutez ces étapes sur le routeur utilisé dans ce TP avant de continuer.

Étape 1 Configurez le nom d'hôte et les mots de passe sur le routeur GAD

a. Sur le routeur GAD, passez en mode de configuration globale et configurez le nom d'hôte comme indiqué dans le tableau. Configurez ensuite la console, le terminal virtuel et les mots de passe enable. Configurez l'interface FastEthernet sur le routeur conformément au tableau.

b. Autorisez l'accès HTTP en exécutant la commande **ip http server** en mode de configuration globale.

Étape 2 Configurez les hôtes sur le segment Ethernet

a. Hôte 1

Adresse IP	192.168.14.2
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

b. Hôte 2

Adresse IP	192.168.14.3
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

Étape 3 Enregistrez les informations de configuration en mode privilégié

```
GAD#copy running-config startup-config
```

Étape 4 Envoyez une requête ping à la passerelle par défaut à partir de chacun des deux hôtes pour confirmer la connectivité

a. Si les requêtes ping échouent, corrigez la configuration et recommencez jusqu'à ce qu'elles réussissent.

Étape 5 Connectez-vous au routeur en utilisant un navigateur Web

a. À partir d'un hôte, connectez-vous au routeur en utilisant un navigateur Web afin de vous assurer que la fonction de serveur Web est active.

Étape 6 Interdisez l'accès HTTP (port 80) à l'interface Ethernet à partir des hôtes

a. Créez une liste de contrôle d'accès qui interdira l'accès via le Web à FastEthernet 0 depuis le réseau 192.168.14.0.

b. À l'invite de configuration du routeur, entrez la commande suivante :

```
GAD(config)#access-list 101 deny tcp 192.168.14.0 0.0.0.255 any eq 80
GAD(config)#access-list 101 permit ip any any
```

c. À quoi sert la deuxième instruction ? _____

Étape 7 Appliquez la liste de contrôle d'accès à l'interface

a. À l'invite du mode interface FastEthernet 0, entrez la commande suivante :

```
GAD(config-if)#ip access-group 101 in
```


Étape 8 Envoyez des requêtes ping au routeur à partir des hôtes

a. Ces requêtes ping ont-elles réussi ? _____

b. Si oui, pourquoi ? _____

Étape 9 Connectez-vous au routeur en utilisant un navigateur Web

a. Avez-vous pu vous connecter ? _____

Étape 10 Établissez des connexions Telnet avec le routeur à partir des hôtes

a. Avez-vous pu vous connecter au routeur via Telnet ? _____

b. Justifiez votre réponse. _____

Après avoir réalisé les étapes précédentes, déconnectez-vous en entrant **exit**. Mettez le routeur hors tension.

Effacement et rechargement du routeur

Passez en mode privilégié à l'aide de la commande **enable**.

Si le système vous demande un mot de passe, entrez **class**. Si « class » ne fonctionne pas, demandez de l'aide au professeur.

```
Router>enable
```

À l'invite du mode privilégié, entrez la commande **erase startup-config**.

```
Router#erase startup-config
```

Vous obtenez le message suivant :

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

Appuyez sur **Entrée** pour confirmer.

La réponse suivante devrait s'afficher :

```
Erase of nvram: complete
```

Ensuite, à l'invite du mode privilégié, entrez la commande **reload**.

```
Router#reload
```

Vous obtenez le message suivant :

```
System configuration has been modified. Save? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

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

Appuyez sur **Entrée** pour confirmer.

La première ligne de la réponse est la suivante :

```
Reload requested by console.
```

Après le rechargement du routeur, la ligne suivante s'affiche :

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

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Press RETURN to get started!
```

Appuyez sur **Entrée**.

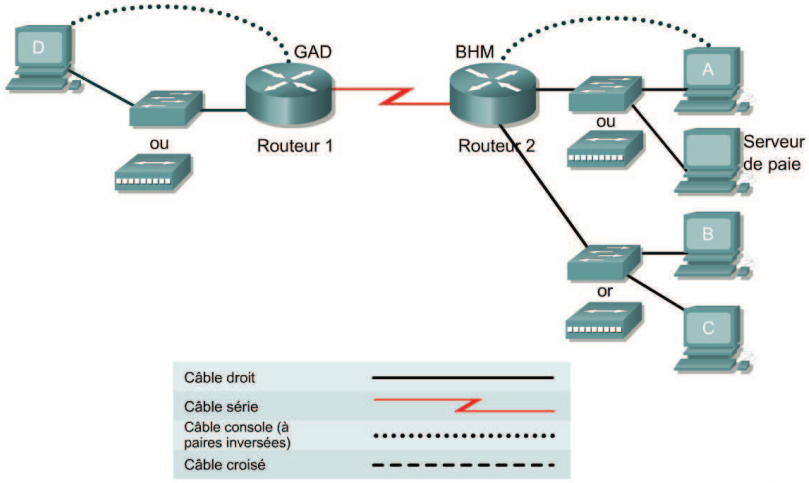
Le routeur est prêt et le TP peut commencer.

Relevé des interfaces de routeur

Modèle de routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2	Interface 5
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Pour connaître la configuration exacte du routeur, observez les interfaces. Vous pourrez ainsi identifier le type du 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. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque appareil. Ce tableau d'interfaces ne comporte aucun autre type d'interface même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI pourrait illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans une commande IOS.

TP 11.2.2b Listes de contrôle d'accès étendues simples



Désignation du routeur	Nom du routeur	Mot de passe " enable secret "	Mot de passe console/ enable/VTY	Protocole de routage	Instructions réseau RIP
Routeur 1	GAD	class	cisco	RIP	172.16.0.0
Routeur 2	BHM	class	cisco	RIP	192.168.1.0 172.16.0.0

Désignation du routeur	Adresse Fast Ethernet 0	Type d'interface Serial 0	Adresse Serial 0	Adresse Fast Ethernet 1	Entrées de la table d'hôtes IP
Routeur 1	172.16.2.1/24	DTE	172.16.1.1/24		BHM
Routeur 2	192.168.1.17/28	DCE	172.16.1.2/24	192.168.1.18/28	GAD

Hôte	Adresse IP	Masque de sous-réseau	Passerelle
Serveur de paie	192.168.1.18	255.255.255.240	192.168.1.17
A	192.168.1.19	255.255.255.240	192.168.1.17
B	192.168.1.34	255.255.255.240	192.168.1.33
C	192.168.1.35	255.255.255.240	192.168.1.33
D	172.16.2.2	255.255.255.0	172.16.2.1

Objectif

Configurer des listes de contrôle d'accès étendues pour filtrer le trafic réseau/réseau, hôte/réseau et réseau/hôte.

Scénario

Une société spécialisée dans le marketing dispose de deux sites. Le bureau principal se trouve à Birmingham (BHM). La société dispose par ailleurs d'une agence à Gadsden (GAD). L'administrateur chargé des télécommunications pour les deux sites a besoin de concevoir et de mettre en œuvre des listes de contrôle d'accès afin d'améliorer la sécurité et les performances. Sur le site de Birmingham, on distingue deux groupes d'utilisateurs du réseau. L'un de ces groupes est chargé de l'administration, l'autre de la production. Ils sont connectés à des réseaux distincts. Les deux réseaux sont interconnectés à l'aide d'un routeur.

Le site Gadsden est un réseau d'extrémité ; il comporte seulement un réseau local (LAN).

Étape 1 – Configuration de base des routeurs et des hôtes

a. Connectez les routeurs et les hôtes comme indiqué dans le schéma. Définissez tous les paramètres de base des routeurs : nom d'hôte, mot de passe enable, accès Telnet et interfaces. Utilisez le schéma et les tableaux ci-dessus à titre de référence.

Note : Le routeur BHM nécessite deux interfaces Ethernet

b. Configurez tous les routeurs de la manière suivante :

```
BHM#show running-config

<informations ignorées>

hostname BHM
!
enable secret class
!
interface FastEthernet0
 ip address 192.168.1.17 255.255.255.240
!
interface Serial0
 ip address 172.16.1.2 255.255.255.0
 clock rate 56000
!
interface FastEthernet1
 ip address 192.168.1.33 255.255.255.240
!
router rip
 network 172.16.0.0
 network 192.168.1.0
!
line vty 0 4
 password cisco
 login
!
end


BHM#
GAD#show running-config

<informations ignorées>

!
hostname GAD
!
```

```
enable password class
!
interface FastEthernet0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0
 ip address 172.16.1.1 255.255.255.0
!
router rip
 network 172.16.0.0
!
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

GAD#
```

c. Configurez les hôtes en utilisant les informations appropriées définies précédemment. Avant d'appliquer une liste de contrôle d'accès, il est important de vérifier l'accessibilité entre les systèmes.

Vérifiez l'accessibilité en envoyant, depuis chaque système, une requête ping à tous les systèmes et à tous les routeurs.

d. Chacun des hôtes doit être capable d'envoyer une requête ping aux autres hôtes et aux interfaces de routeurs. Si des requêtes ping envoyées à certaines interfaces échouent, le problème doit être localisé et corrigé. Vérifiez systématiquement les connexions de la couche physique qui est à l'origine de la plupart des problèmes de connectivité. Ensuite, vérifiez les interfaces de routeur. Assurez-vous que ces dernières ne sont pas désactivées, mal configurées et que RIP est correctement configuré. Enfin, n'oubliez pas que les hôtes doivent avoir des adresses IP valides ainsi que des passerelles par défaut spécifiées.

e. Maintenant que l'infrastructure est en place, vous devez sécuriser l'interréseau.

Étape 2 Empêchez les utilisateurs du groupe Production d'accéder au réseau Gadsden

a. Selon la politique de la société, seul le groupe Administration doit pouvoir accéder au site Gadsden. Le groupe Production ne doit pas y avoir accès.

b. Configurez une liste de contrôle d'accès étendue qui autorise le groupe Administration à accéder au site Gadsden. Vous devez en revanche en interdire l'accès au groupe Production.

c. Une analyse minutieuse révèle qu'il serait préférable d'utiliser une liste de contrôle d'accès étendue et de l'appliquer à l'interface de sortie S0 sur le routeur BHM.

Remarque : N'oubliez pas qu'une fois la liste de contrôle d'accès configurée, le routeur traite les instructions qu'elle contient dans l'ordre de leur création. Il n'est pas possible de réorganiser une liste de contrôle d'accès, ni même d'ignorer, de modifier ou de supprimer des instructions dans une liste de contrôle d'accès numérotée. C'est pourquoi il peut s'avérer utile de créer la liste dans un éditeur de texte, Bloc-notes par exemple, puis de coller les commandes au niveau du routeur, plutôt que de les entrer directement.

d. Précisez les éléments suivants :

```
BHM#conf terminal
Entrez les commandes de configuration (une par ligne).  Terminez avec
   CNTL/Z.
BHM(config)#access-list 100 deny ip 192.168.1.32 0.0.0.15 172.16.2.0
0.0.0.255
```


e. Cette instruction définit une liste de contrôle d'accès étendue appelée « 100 ». Elle interdit l'accès IP à tous les utilisateurs sur le réseau 192.168.1.32 – 192.168.1.47 s'ils tentent d'accéder au réseau 172.16.2.0. Bien qu'il soit possible de définir une liste plus générale, celle-ci pourrait autoriser les utilisateurs du groupe Production à accéder à d'autres sites (éventuellement disponibles) via l'interface S0.

f. N'oubliez pas qu'il existe un refus global implicite à la fin de chaque liste de contrôle d'accès. Vous devez maintenant vous assurer que le groupe Administration peut accéder au réseau Gadsden. Vous pourriez être plus restrictif, mais autorisez simplement tout autre type de trafic. Entrez les instructions suivantes :

```
BHM(config)#access-list 100 permit ip any any
```

g. À présent, il faut appliquer la liste de contrôle d'accès à une interface. Vous pourriez appliquer la liste au trafic destiné à l'interface Fa0/1 du réseau de production. Toutefois, en cas de fort trafic entre le réseau d'administration et le réseau de production, le routeur devrait vérifier chacun des paquets. Cela risquerait d'entraîner une surcharge inutile au niveau du routeur. Vous devez donc appliquer la liste de contrôle d'accès à tout trafic externe passant par l'interface S0 du routeur BHM.

Précisez les éléments suivants :

```
BHM(config)#interface s0
BHM(config-if)#ip access-group 100 out
```

h. Utilisez la commande **show running-config** pour vérifier la syntaxe de la liste de contrôle d'accès. Voici les instructions valides devant figurer dans la configuration :

```
interface Serial0
 ip access-group 100 out

<informations ignorées>

access-list 100 deny   ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
access-list 100 permit ip any any
```

i. La commande **show access-lists** est également très utile. Elle génère des informations similaires à celles-ci :

```
BHM#show access-lists
Extended IP access list 100
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
```

j. La commande **show access-lists** affiche également des compteurs qui indiquent le nombre de fois où la liste a été utilisée. Aucun compteur n'est présenté ici car aucune vérification correspondante n'a encore été effectuée.

Remarque : Utilisez la commande **clear access-list counters** pour réinitialiser les compteurs de listes de contrôle d'accès.

k. Testez la liste de contrôle d'accès en vérifiant l'accessibilité au réseau Gadsden à partir des hôtes d'administration et de production.

L'hôte de production (B) peut-il envoyer une requête ping à l'hôte Gadsden (D) ? _____

L'hôte de production (C) peut-il envoyer une requête ping à l'hôte Gadsden (D) ? _____

L'hôte d'administration (A) peut-il envoyer une requête ping à l'hôte Gadsden (D) ? _____

L'hôte de production (B) peut-il envoyer une requête ping à l'hôte d'administration (A) ? _____

L'hôte de production (B) peut-il envoyer une requête ping à l'interface série du routeur Gadsden ? _____

l. Les hôtes de production (B) et (C) doivent pouvoir envoyer des requêtes ping à l'hôte d'administration (A) et à l'interface série du routeur Gadsden. Toutefois, ils ne doivent pas pouvoir envoyer de requêtes ping à l'hôte Gadsden (D). Le routeur doit dans ce cas renvoyer un message indiquant « Destination inaccessible ».

   Exécutez la commande **show access-lists**. Quel est le nombre de correspondances ?

   _____

   Remarque : La commande **show access-lists** affiche le nombre de correspondances par ligne. Par conséquent, le nombre de correspondances « deny » peut paraître surprenant, mais il faut savoir que les requêtes ping correspondent à l'instruction « deny » et à l'instruction « permit ».

m. Pour mieux comprendre le fonctionnement de la liste de contrôle d'accès, continuez à utiliser régulièrement la commande **show access-lists**.

Étape 3 Autorisez un utilisateur du groupe Production à accéder au réseau Gadsden

a. Vous recevez un appel d'un utilisateur du groupe Production (B). Cet utilisateur est chargé d'échanger certains fichiers entre le réseau de production et le réseau Gadsden. Vous devez modifier la liste de contrôle d'accès pour l'autoriser à accéder au réseau Gadsden, tout en refusant l'accès aux autres utilisateurs du réseau de production.

b. Configurez une liste de contrôle d'accès étendue pour accorder à cet utilisateur l'accès au réseau Gadsden.

c. Il n'est malheureusement pas possible de réorganiser une liste de contrôle d'accès, ni même d'ignorer, de modifier ou de supprimer des instructions dans une liste de contrôle d'accès numérotée. Dans le cas des listes numérotées, toute tentative de suppression d'une instruction entraîne la suppression de l'intégralité de la liste.

d. Vous devez donc supprimer la liste de contrôle d'accès étendue initiale et en créer une nouvelle. Pour supprimer la liste 100, entrez les éléments suivants :

```
BHM#conf t
Entrez les commandes de configuration (une par ligne). Terminez avec
   CNTL/Z.
BHM(config)#no access-list 100
```

Utilisez la commande **show access-lists** pour vous assurer que la liste a été supprimée.

e. Créez maintenant une nouvelle liste de contrôle d'accès étendue. Le filtrage doit aller du particulier au général. La première ligne de la liste doit donc autoriser l'hôte de production (B) à accéder au réseau Gadsden. Les autres lignes doivent être identiques à celles de la liste précédente.

f. En vue du filtrage de l'hôte de production (B), la première ligne de la liste doit se présenter comme suit :

```
BHM(config)#access-list 100 permit ip host 192.168.1.34 172.16.2.0
0.0.0.255
```

La liste de contrôle d'accès autorise donc l'hôte de production (B) à accéder au réseau Gadsden.

g. À présent, interdisez aux autres hôtes de production l'accès au réseau Gadsden, et autorisez l'accès à tout autre hôte. Reportez-vous à l'étape précédente pour la définition des deux lignes suivantes de la configuration.

   La commande **show access-list** affiche des informations similaires à celles-ci :

```
BHM#show access-lists
Extended IP access list 100
    permit ip host 192.168.1.34 172.16.2.0 0.0.0.255
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
BHM#
```

h. Testez la liste de contrôle d'accès en vérifiant l'accessibilité au réseau Gadsden à partir des hôtes d'administration et de production.

L'hôte de production (B) peut-il envoyer une requête ping à l'hôte Gadsden (D) ? _____

L'hôte de production (C) peut-il envoyer une requête ping à l'hôte Gadsden (D) ? _____

L'hôte de production (B) doit maintenant pouvoir envoyer une requête ping à l'hôte Gadsden (D). En revanche, tous les autres hôtes de production (C) ne doivent pas pouvoir envoyer de requête ping à cet hôte Gadsden (D). Le routeur doit ainsi renvoyer à l'hôte (C) un message indiquant « Destination inaccessible ».

Étape 4 Autorisez les utilisateurs du site Gadsden à accéder au serveur de paie du groupe Administration

a. Le groupe Administration héberge le serveur de paie. Les utilisateurs du site Gadsden peuvent avoir besoin d'un accès FTP et HTTP au serveur de paie afin de télécharger des rapports de paie.

b. Configurez une liste de contrôle d'accès étendue pour accorder aux utilisateurs du site Gadsden l'accès FTP et HTTP au serveur de paie uniquement. Ils doivent également bénéficier d'un accès ICMP pour pouvoir envoyer des requêtes ping au serveur. En revanche, ils ne doivent pas pouvoir envoyer de requêtes ping aux autres hôtes du réseau d'administration.

c. Pour éviter tout trafic indésirable entre les sites, vous devez configurer une liste de contrôle d'accès étendue sur le routeur Gadsden.

d. Anticipez qu'un accès en mode privilégié au routeur GAD sera requis occasionnellement. Vous devez donc configurer un accès Telnet à ce dernier. Vous éviterez ainsi d'avoir à vous rendre sur le site Gadsden pour la configuration.

e. Établissez une connexion Telnet avec le routeur Gadsden à partir du routeur Birmingham et passez en mode enable. Effectuez un dépannage, si nécessaire.

   Remarque : L'un des pièges les plus courants lors de la configuration de listes de contrôle d'accès sur des routeurs distants est de verrouiller l'accès à ces derniers par inadvertance. Cela ne constitue pas un problème si le routeur se trouve à proximité (en local). En revanche, cela peut devenir un problème critique si le routeur est situé dans une autre zone géographique.

f. C'est pourquoi il est vivement recommandé d'exécuter la commande **reload in 30** sur le routeur distant. De cette manière, le routeur distant se recharge automatiquement dans les 30 minutes suivant l'exécution de cette commande. Si l'accès au routeur est verrouillé, sa configuration précédente sera rechargée, ce qui permettra à l'administrateur d'accéder de nouveau au routeur. Utilisez la commande **reload cancel** pour désactiver le rechargement en attente.

g. Configurez une liste de contrôle d'accès étendue pour autoriser l'accès FTP au serveur de paie. L'instruction de la liste de contrôle d'accès doit être similaire à celle-ci :

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq ftp
```


Grâce à cette ligne, tous les hôtes du réseau Gadsden peuvent bénéficier d'un accès FTP au serveur de paie à l'adresse 192.168.1.18.

Plutôt que d'utiliser le mot clé « any », quel élément est-il possible de définir ?

_____

Plutôt que d'utiliser le mot clé « host », quel élément est-il possible de définir ?

_____

Plutôt que d'utiliser le mot clé « ftp », quel élément est-il possible de définir ?

_____

h. Configurez maintenant la ligne suivante de la liste de contrôle d'accès afin d'autoriser l'accès HTTP au serveur de paie. L'instruction de la liste de contrôle d'accès doit être similaire à celle-ci :

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq www
```

Grâce à cette ligne, tous les hôtes du réseau Gadsden peuvent bénéficier d'un accès FTP au serveur de paie à l'adresse 192.168.1.18.

Plutôt que d'utiliser le mot clé « www», quel élément est-il possible de définir ?

_____

i. Configurez maintenant la ligne suivante de la liste de contrôle d'accès afin d'autoriser l'accès ICMP au serveur de paie. L'instruction de la liste de contrôle d'accès doit être similaire à celle-ci :

```
GAD(config)#access-list 110 permit icmp any host 192.168.1.18
```

Grâce à cette ligne, tous les hôtes du réseau Gadsden peuvent envoyer une requête ping au serveur de paie à l'adresse 192.168.1.18.

j. Enfin, aucun utilisateur du site Gadsden ne doit pouvoir accéder aux autres hôtes du réseau d'administration. Il peut s'avérer judicieux d'inclure une instruction « deny », même si cela n'est pas obligatoire. L'ajout de cette instruction constitue un rappel utile et facilite la lecture de la liste de contrôle d'accès. L'instruction de la liste de contrôle d'accès doit être similaire à celle-ci :

```
GAD(config)#access-list 110 deny ip any 192.168.1.16 0.0.0.15
```

k. À présent, il faut appliquer la liste de contrôle d'accès à une interface. Pour éviter tout trafic indésirable, vous devez appliquer la liste de contrôle d'accès au trafic externe passant par l'interface S0 du routeur Gadsden.

Précisez les éléments suivants :

```
GAD(config)#interface s0
GAD(config-if)#ip access-group 110 out
```


l. Testez la liste de contrôle d'accès en vérifiant l'accessibilité au serveur de paie à partir d'un hôte Gadsden (D).

L'hôte Gadsden (D) peut-il envoyer une requête ping au serveur de paie ? _____

L'hôte Gadsden (D) peut-il envoyer une requête ping à l'hôte (A) ? _____

L'hôte Gadsden doit être capable d'envoyer une requête ping au serveur de paie uniquement. Le routeur doit toutefois renvoyer le message « Destination inaccessible » lorsque l'hôte tente d'envoyer une requête ping à l'hôte d'administration (D).

Étape 5 Décrivez par écrit la liste de contrôle d'accès

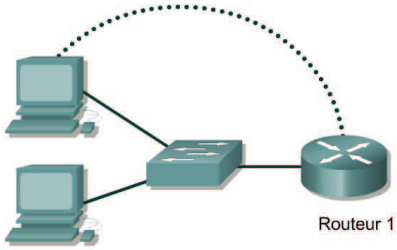
a. Toute administration réseau doit comporter une documentation. Utilisez le fichier texte créé pour la configuration et ajoutez-y des commentaires. Ce fichier doit également contenir les informations générées par les commandes **show access-lists** et **show ip interface**.

b. Le fichier doit être sauvegardé avec le reste de la documentation réseau. La convention d'attribution de noms doit refléter la fonction du fichier et indiquer la date de mise en œuvre.

c. Ce TP sur les listes de contrôle d'accès étendues est terminé.

d. Lorsque vous avez terminé, effacez la configuration de démarrage sur les routeurs, retirez les câbles et les adaptateurs, puis rangez-les. Enfin, déconnectez-vous et mettez le routeur hors tension.

TP 11.2.3a Configuration de listes de contrôle d'accès nommées



Désignation du routeur	Nom du routeur	Adresse FA0/0	Masque de sous-réseau	Mot de passe " enable secret "	Mot de passe console/ enable/VTY
Routeur 1	GAD	192.168.14.1	255.255.255.0	class	cisco

Objectif

- Créer une liste de contrôle d'accès nommée en vue d'autoriser ou de refuser un type de trafic particulier.
- Tester la liste de contrôle d'accès pour déterminer si les résultats escomptés ont été atteints.

Prérequis/Préparation

Installez un réseau similaire à celui du schéma. Tout routeur doté d'une interface indiquée dans le schéma ci-dessus peut être utilisé, par exemple les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Reportez-vous au tableau qui se trouve à la fin du TP pour repérer les identifiants d'interfaces à utiliser en fonction de l'équipement disponible. Dans ce TP, les informations affichées par le routeur lors de sa configuration ont été obtenues avec un routeur de la gamme 1721. Celles-ci peuvent varier légèrement avec un autre routeur. Les étapes qui suivent doivent être exécutées sur chaque routeur, sauf indication contraire.

Lancez une session HyperTerminal comme indiqué dans le TP intitulé Établissement d'une session en mode console avec HyperTerminal.

Remarque : Suivez les instructions d'effacement et de rechargement qui se trouvent à la fin de ce TP. Exécutez ces étapes sur le routeur utilisé dans ce TP avant de continuer.

Étape 1 Configurez le nom d'hôte et les mots de passe sur le routeur Gadsden

a. Sur le routeur Gadsden, passez en mode de configuration globale et configurez le nom d'hôte comme indiqué dans le tableau. Configurez ensuite la console, le terminal virtuel et les mots de passe enable. Configurez l'interface FastEthernet sur le routeur conformément au tableau.

Étape 2 Configurez les hôtes sur le segment Ethernet

a. Hôte 1

Adresse IP	192.168.14.2
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

b. Hôte 2

Adresse IP	192.168.14.3
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.14.1

Étape 3 Enregistrez les informations de configuration en mode privilégié

```
GAD#copy running-config startup-config
```

Étape 4 Envoyez une requête ping à la passerelle par défaut à partir de chacun des deux hôtes pour confirmer la connectivité

a. Si les requêtes ping échouent, corrigez la configuration et recommencez jusqu'à ce qu'elles réussissent.

Étape 5 Interdisez l'accès à l'interface Ethernet à partir des hôtes

a. Créez une liste de contrôle d'accès nommée qui interdira l'accès à FastEthernet 0 depuis le réseau 192.168.14.0.

b. À l'invite de configuration, entrez la commande suivante :

```
GAD(config)#ip access-list standard no_access
GAD(config-std-nacl)#deny 192.168.14.0 0.0.0.255
GAD(config-std-nacl)#permit any
```

c. À quoi sert la troisième instruction ? _____

Étape 6 Envoyez des requêtes ping au routeur à partir des hôtes

a. Ces requêtes ping ont-elles réussi ? _____

b. Si oui, pourquoi ? _____

Étape 7 Appliquez la liste de contrôle d'accès à l'interface

a. À l'invite du mode interface FastEthernet, entrez la commande suivante :

```
GAD(config-if)#ip access-group no_access in
```

Étape 8 Envoyez des requêtes ping au routeur à partir des hôtes

a. Ces requêtes ping ont-elles réussi ? ___

b. Justifiez votre réponse. _

Après avoir réalisé les étapes précédentes, déconnectez-vous en entrant **exit**. Mettez le routeur hors tension.

Effacement et rechargement du routeur

Passez en mode privilégié à l'aide de la commande **enable**.

Si le système vous demande un mot de passe, entrez **class**. Si « class » ne fonctionne pas, demandez de l'aide au professeur.

```
Router>enable
```

À l'invite du mode privilégié, entrez la commande **erase startup-config**.

```
Router#erase startup-config
```

Vous obtenez le message suivant :

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

Appuyez sur **Entrée** pour confirmer.

La réponse suivante devrait s'afficher :

```
Erase of nvram: complete
```

Ensuite, à l'invite du mode privilégié, entrez la commande **reload**.

```
Router#reload
```

Vous obtenez le message suivant :

```
System configuration has been modified. Save? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

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

Appuyez sur **Entrée** pour confirmer.

La première ligne de la réponse est la suivante :

```
Reload requested by console.
```

Après le rechargement du routeur, la ligne suivante s'affiche :

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

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Press RETURN to get started!
```

Appuyez sur **Entrée**.

Le routeur est prêt et le TP peut commencer.

Récapitulatif des interfaces de routeur

Modèle de routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2	Interface 5
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	

Pour connaître la configuration exacte du routeur, observez les interfaces. Vous pourrez ainsi identifier le type du 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. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque appareil. Ce tableau d'interfaces ne comporte aucun autre type d'interface même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI pourrait illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans une commande IOS.