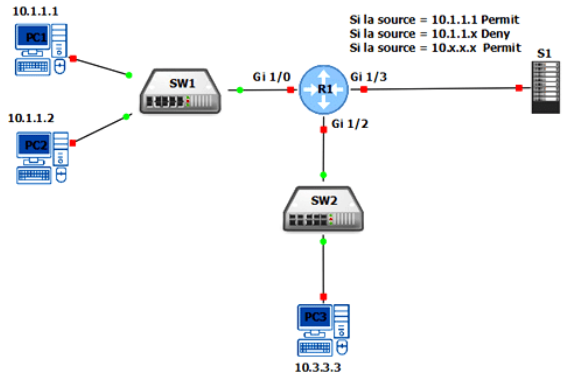
ACL (Access Control List)



Extrait du référentiel : BTS CIEL option A (Informatique et Réseaux)		Niveau(x)
C06 VALIDER UN SYSTÈME INFORMATIQUE	Sécurisation des réseaux (ACL, mots de passe, pare-feu)	3
C09 INSTALLER UN RÉSEAU INFORMATIQUE	Pare-feu, ACL	3

Objectifs du TP :

- Introduction aux ACLs
- Qu'est-ce qu'une liste de contrôle d'accès ?
- Conversation TCP
- Le filtrage des paquets
- Fonctionnement des ACLs
- Les ACLs standards et étendues
- Numérotation et nommage des ACLs
- Les masques génériques
- Création des ACLs
- Emplacement des ACLs
- Exercices

Support d'activité :

- Logiciels : Cisco Packet Tracer et suite bureautique
- Fichiers : Exercice.pka, Exercice7.pka et Configurer un routeur cisco.pdf
- Ce document au format PDF

Vous rédigerez un compte-rendu numérique.
Résumez les questions avant de répondre.
Pensez aux captures d'écran pour imager votre compte-rendu.
Sauvegardez votre travail régulièrement !
Des modifications peuvent exister selon la version du logiciel utilisée.

À rendre en fin de séance :
Votre compte-rendu numérique nommé : **TP_Cyber_ACL_VOTRENOM.PDF**

INTRODUCTION AUX ACLs

La sécurité du réseau est un sujet de taille, la compréhension approfondie des **listes de contrôle d'accès** est l'une des principales compétences requises chez un administrateur réseau.

Les concepteurs de réseaux utilisent des **pare-feu** pour protéger les réseaux de toute utilisation non autorisée. Les pare-feu sont des solutions logicielles ou matérielles permettant de mettre en œuvre des stratégies de sécurité du réseau. Prenons l'exemple d'un verrou de porte dans une pièce à l'intérieur d'un bâtiment. Le verrou autorise uniquement les utilisateurs autorisés et munis d'une clé ou d'une carte d'accès à entrer. De la même façon, un pare-feu filtre les paquets non autorisés ou dangereux, les empêchant ainsi d'accéder au réseau. Sur un routeur Cisco, vous pouvez configurer un pare-feu simple, qui assurera les fonctions de base de filtrage du trafic à l'aide de listes de contrôle d'accès. Les administrateurs utilisent des listes de contrôle d'accès pour bloquer le trafic ou n'autoriser qu'un trafic spécifique sur leurs réseaux.

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou aux protocoles de couche supérieure. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau. Des listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés.

Sécuriser le réseau est la principale raison vous incitant à configurer des listes de contrôles d'accès.

QU'EST-CE QU'UNE LISTE DE CONTRÔLE D'ACCÈS ?

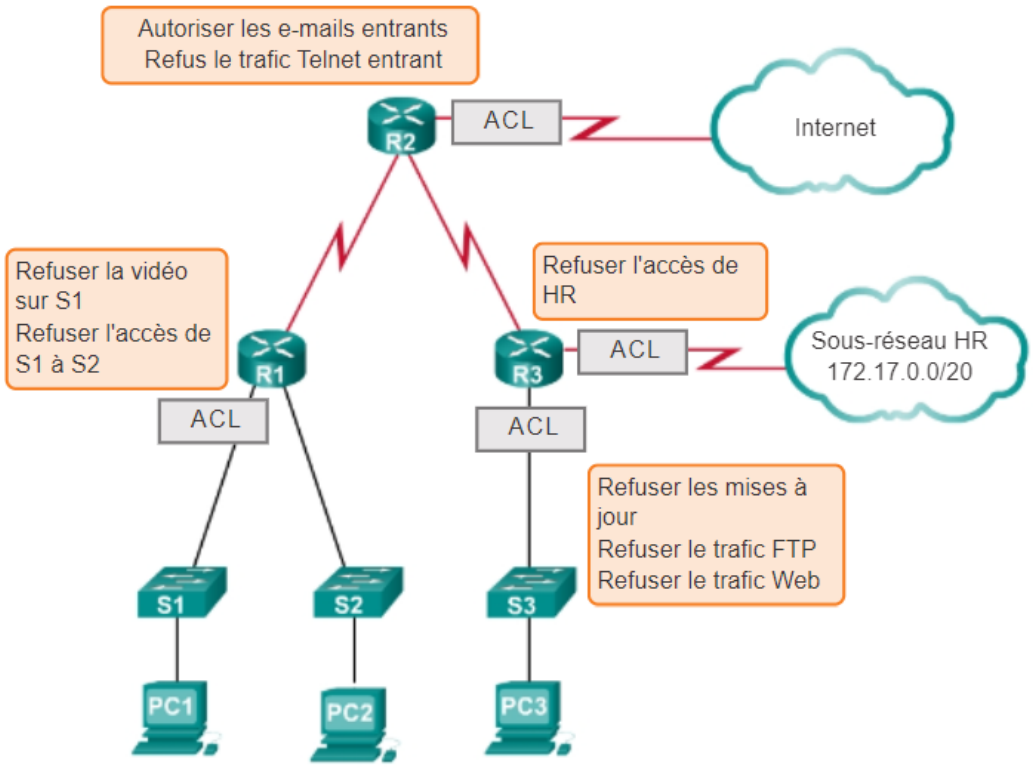
Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Les listes de contrôle d'accès font partie des fonctionnalités les plus utilisées du logiciel Cisco IOS.
Une fois configurées, les listes de contrôle d'accès assurent les tâches suivantes :

- Elles limitent le trafic réseau pour accroître les performances réseau. Si la stratégie de l'entreprise interdit, par exemple, le trafic vidéo sur le réseau, vous pouvez configurer et appliquer des listes de contrôle d'accès pour bloquer ce trafic. Ainsi, la charge réseau est nettement réduite et les performances réseau sont sensiblement améliorées.
- Elles contrôlent le flux de trafic. Les listes de contrôle d'accès peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise vu les conditions du réseau, la bande passante est préservée.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'y avoir accès. Par exemple, l'accès au réseau du département Ressources humaines peut être limité aux utilisateurs autorisés.
- Elles filtrent le trafic en fonction de son type. Ainsi, une liste de contrôle d'accès peut autoriser le trafic des e-mails, mais bloquer tout le trafic Telnet.
- Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau. Les listes de contrôle d'accès peuvent autoriser ou refuser à un utilisateur l'accès à certains types de fichier, tels que FTP ou HTTP.

Par défaut, aucune liste de contrôle d'accès n'est configurée sur les routeurs. Par conséquent, les routeurs ne filtrent pas le trafic, par défaut. Le trafic qui entre dans le routeur est routé uniquement en fonction des informations de la table de routage. Toutefois, lorsqu'une liste de contrôle d'accès

est appliquée à une interface, le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.

En dehors de l'autorisation ou du blocage du trafic, les listes de contrôle d'accès peuvent être utilisées pour sélectionner les types de trafic à analyser, à acheminer et à traiter selon d'autres méthodes. Par exemple, les listes de contrôle d'accès permettent de classer le trafic par ordre de priorité. Cette fonction s'assimile à une carte VIP pour un concert ou un événement sportif. La carte VIP offre aux spectateurs privilégiés des avantages qui ne sont pas proposés aux détenteurs d'un billet standard, notamment l'entrée prioritaire ou le droit d'accéder à une zone privée.
La figure ci-dessous présente un exemple de topologie sur laquelle des listes de contrôle d'accès sont appliquées.



Exemple de topologie avec des listes de contrôle d'accès

CONVERSATION TCP

Les listes de contrôle d'accès permettent aux administrateurs de contrôler le trafic entrant et sortant d'un réseau. Il peut tout simplement s'agir d'autoriser ou de refuser le trafic en fonction des adresses réseau ou bien d'atteindre des objectifs plus complexes, notamment contrôler le trafic réseau en fonction du port TCP demandé. Pour comprendre le principe de filtrage du trafic appliqué par une liste de contrôle d'accès, le plus simple est d'examiner le dialogue qui intervient dans une conversation TCP, notamment lorsque vous demandez une page Web.

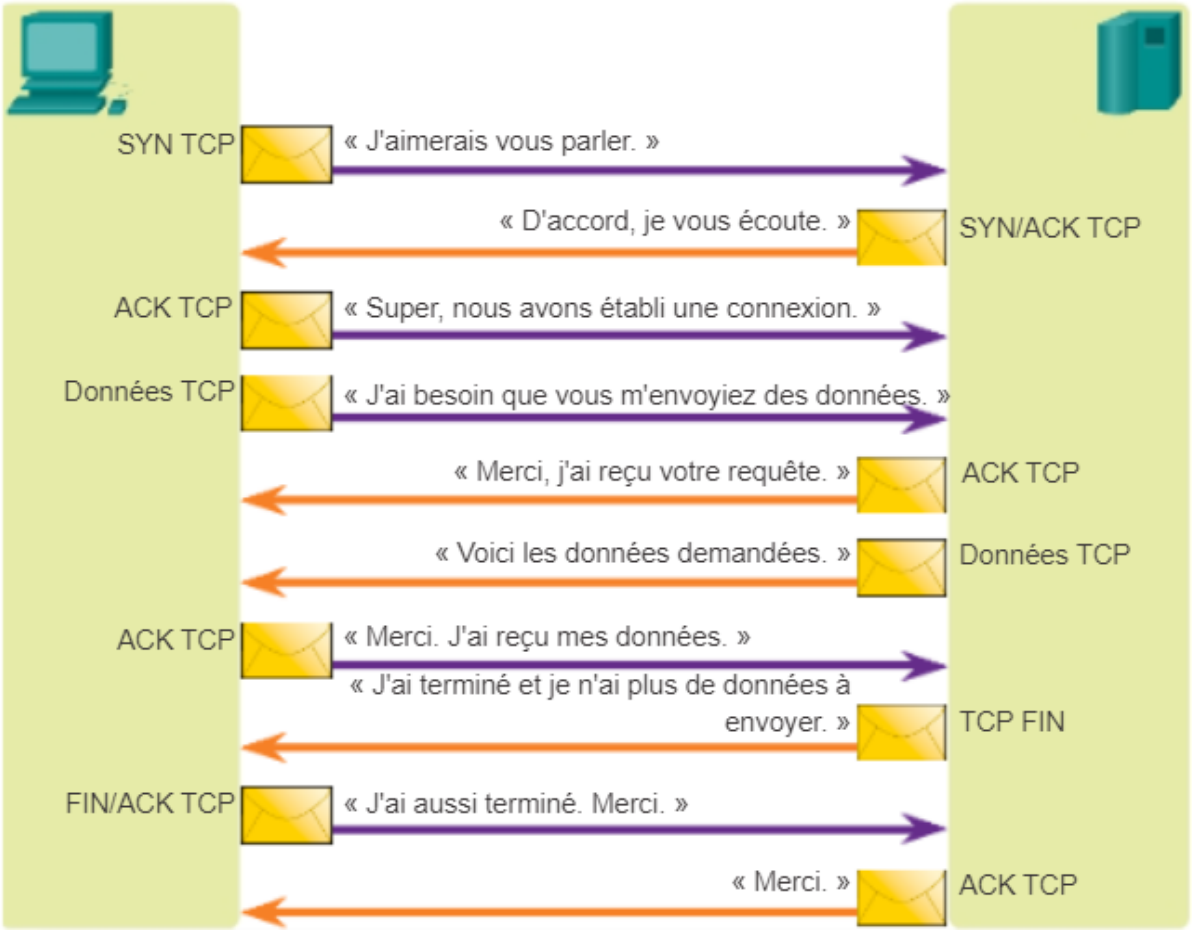
Communication TCP
Lorsqu'un client demande des données à un serveur Web, le protocole IP gère les communications entre le PC (source) et le serveur (destination). Le protocole TCP gère les communications entre le navigateur Web (application) et le logiciel du serveur réseau.

Lorsque vous envoyez un e-mail, consultez une page Web ou téléchargez un fichier, le protocole TCP se charge de répartir les données en segments pour IP avant leur envoi. TCP gère également l'assemblage des données à partir des segments lorsqu'elles arrivent. Le processus TCP ressemble à une conversation dans laquelle deux nœuds se transmettent des données sur un réseau.

TCP fournit un service de flux d'octets fiable et orienté connexion.

« **Orienté connexion** » signifie que les deux applications doivent établir une connexion TCP avant de pouvoir échanger des données.

TCP est un protocole bidirectionnel simultané. En d'autres termes, chaque connexion TCP prend en charge une paire de flux d'octets, chaque flux étant unidirectionnel. TCP comprend un mécanisme de contrôle de flux pour chaque flux d'octets permettant au récepteur de limiter le volume de données que l'expéditeur peut transmettre. TCP implémente également un mécanisme de contrôle de l'encombrement.
La figure ci-dessous illustre une conversation TCP/IP. Les segments TCP sont identifiés par des indicateurs qui décrivent leur objectif : une synchronisation (SYN) commence la session, ACK est un accusé de réception signalant qu'un segment prévu a été reçu et un segment FIN termine la session. Un paquet SYN/ACK confirme que le transfert est synchronisé. Les segments de données TCP comprennent le protocole de niveau supérieur requis pour transmettre les données d'application à l'application appropriée.



Conversation TCP

Le segment de données TCP identifie également le port correspondant au service demandé. Par exemple, HTTP correspond au port 80, SMTP au port 25 et FTP aux ports 20 et 21. La Figure 2 montre les plages des ports UDP et TCP.

Plage de numéros de port	Groupe de ports
0 à 1023	Ports réservés
De 1024 à 49151	Ports inscrits
49152 à 65535	Ports dynamiques et/ou privés

Numéros de port

Ports TCP inscrits :	
1863	MSN Messenger
2000	Cisco SCCP (VoIP)
8008	Alternate HTTP
8080	Alternate HTTP

Ports TCP réservés :	
21	FTP
23	Telnet
25	SMTP
80	HTTP
143	IMAP
194	Internet Relay Chat (IRC)
443	Secure HTTP (HTTPS)

Ports TCP

Ports UDP inscrits :	
1812	RADIUS Authentication Protocol
5004	RTP (Voice and Video Transport Protocol)
5060	SIP (VoIP)

Ports UDP réservés :	
69	TFTP
520	RIP

Ports UDP

Ports TCP/UDP inscrits courants :	
1433	MS SQL
2948	WAP (MMS)

Ports TCP/UDP réservés courants :	
53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

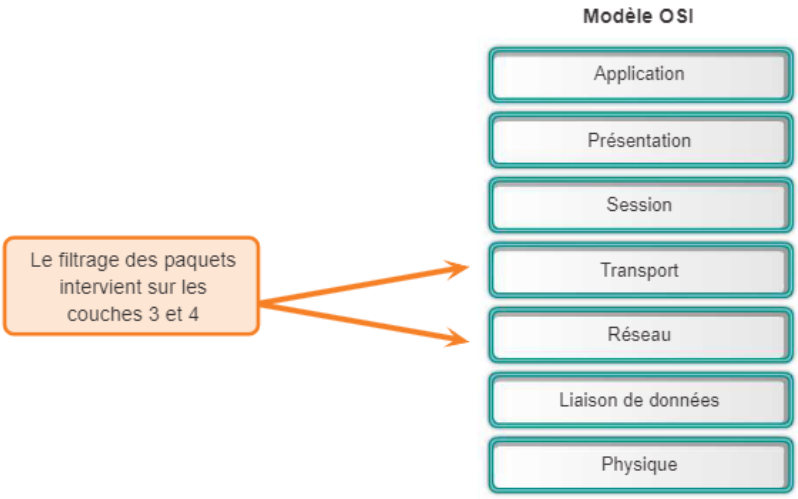
Ports communs aux protocoles UDP et TCP

LE FILTRAGE DES PAQUETS

Comment les listes de contrôle d'accès utilisent-elles les informations transmises lors d'une conversation TCP/IP pour filtrer le trafic ?

Le **filtrage des paquets**, parfois appelé **filtrage statique des paquets**, contrôle l'accès à un réseau en analysant les paquets entrants et sortants et en les transmettant ou en rejetant selon des critères spécifiques, tels que l'adresse IP source, les adresses IP de destination et le protocole transporté dans le paquet.

Un routeur filtre les paquets lors de leur transmission ou de leur refus conformément aux règles de filtrage. Lorsqu'un paquet arrive sur un routeur de filtrage des paquets, le routeur extrait certaines informations de l'en-tête de paquet. Celles-ci lui permettent de décider si le paquet peut être acheminé ou non en fonction des règles de filtre configurées. Comme le montre la figure ci-dessous, le filtrage des paquets peut fonctionner sur différentes couches du modèle OSI ou sur la couche Internet du modèle TCP/IP.



Filtrage des paquets

Un routeur de filtrage de paquets utilise des règles pour déterminer s'il doit autoriser ou refuser le trafic. Un routeur peut également effectuer le filtrage des paquets au niveau de la couche 4, la couche transport. Le routeur peut filtrer les paquets en fonction des ports source et de destination du segment TCP ou UDP. Ces règles sont définies à l'aide de listes de contrôle d'accès.

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus, appelées **entrées de contrôle d'accès** (ACE). Les ACE sont couramment appelées des instructions de liste de contrôle d'accès. Des ACE peuvent être créés pour filtrer le trafic en fonction de critères tels que l'adresse source, l'adresse de destination, le protocole et les numéros de port. Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations du paquet à chaque ACE, dans l'ordre séquentiel, afin de déterminer si le paquet correspond à l'une des instructions. Si une correspondance est trouvée, le paquet est traité en conséquence. Vous pouvez ainsi configurer des listes de contrôle d'accès en vue de contrôler l'accès à un réseau ou à un sous-réseau.

Pour évaluer le trafic réseau, la liste de contrôle d'accès extrait les informations suivantes de l'en-tête de paquet de couche 3 :

- Adresse IP source
- Adresse IP de destination
- Type de message ICMP

La liste de contrôle d'accès peut également extraire des informations de couche supérieure à partir de l'en-tête de couche 4, notamment :

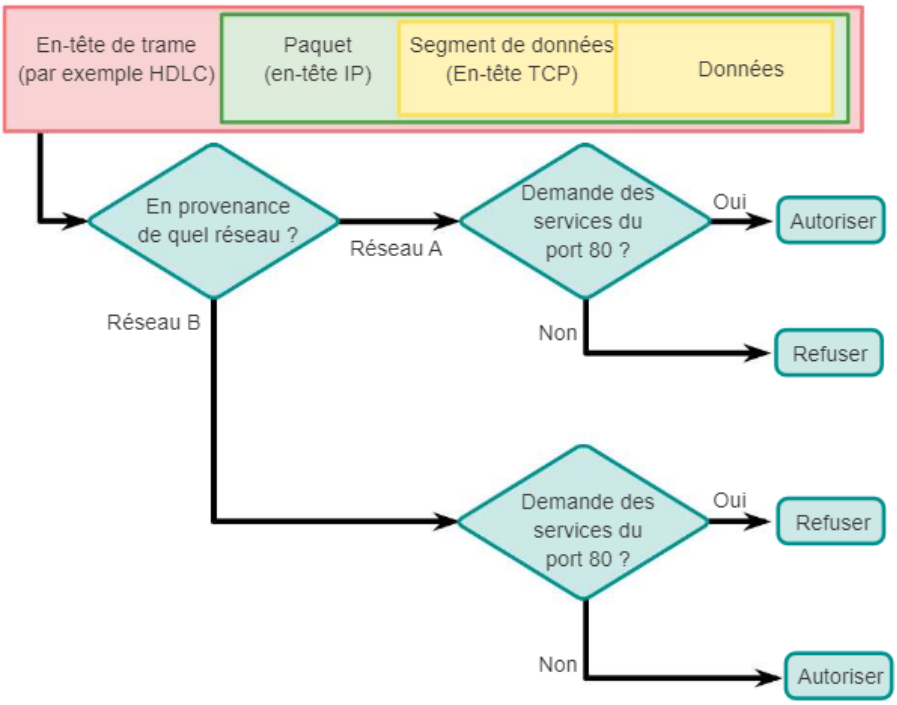
- Port source TCP/UDP
- Port de destination TCP/UDP

Exemple de filtrage des paquets

Pour comprendre comment un routeur utilise le filtrage des paquets, imaginez qu'un gardien a été placé devant une porte verrouillée. Le gardien a reçu pour instruction de ne laisser passer que les personnes dont les noms figurent sur une liste. Il filtre le passage des personnes conformément à la liste des noms autorisés. Les listes de contrôle d'accès fonctionnent de la même façon et prennent des décisions en fonction de critères définis.

Par exemple, une liste de contrôle d'accès peut être configurée pour « autoriser l'accès Web aux utilisateurs du réseau A, mais leur refuser l'accès à tous les autres services. Refuser l'accès HTTP aux utilisateurs du réseau B, mais leur autoriser tous les autres accès. », et ce, de manière logique.

Regardez la figure ci-dessous qui présente un exemple de processus décisionnel d'un filtrage de paquets.



Exemple de filtrage de paquets

Dans l'exemple ci-dessus, le filtrage de paquet vérifie chaque paquet comme suit :

- S'il s'agit d'un paquet SYN TCP du réseau A et qu'il utilise le port 80, son passage est autorisé. Tout autre accès est refusé à ces utilisateurs.
- S'il s'agit d'un paquet SYN TCP du réseau B et qu'il utilise le port 80, son passage est bloqué. Néanmoins, tout autre accès est autorisé.

Ceci n'est qu'un exemple. Plusieurs règles peuvent être configurées pour autoriser ou refuser plus précisément des services aux utilisateurs spécifiques.

FONCTIONNEMENT DES ACLs

Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie. Elles ne gèrent pas les paquets provenant du routeur lui-même.
Les listes de contrôle d'accès sont configurées pour s'appliquer au trafic entrant ou sortant, comme le montre la figure ci-dessous.

Les listes de contrôle d'accès entrantes filtrent les paquets entrant dans une interface spécifique avant qu'ils ne soient acheminés vers l'interface de sortie.

Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.

- **Listes de contrôle d'accès entrantes** : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet. Si le paquet est autorisé à l'issue des tests, il est soumis au routage. Les listes de contrôle d'accès entrantes sont idéales pour filtrer les paquets lorsque le réseau relié à une interface d'entrée est la seule source des paquets devant être inspectés.
- **Listes de contrôle d'accès sortantes** : les paquets entrants sont acheminés vers l'interface de sortie, puis traités par le biais de la liste de contrôle d'accès sortante. Les listes de contrôle d'accès sortantes sont particulièrement efficaces lorsqu'un même filtre est appliqué aux paquets provenant de plusieurs interfaces d'entrée avant de quitter la même interface de sortie.

La dernière instruction d'une liste de contrôle d'accès est toujours une instruction **`implicit deny`**. Cette instruction est automatiquement ajoutée à la fin de chaque liste de contrôle d'accès, même si elle n'est pas physiquement présente. L'instruction `implicit deny` bloque l'ensemble du trafic. En raison de ce refus implicite, une liste de contrôle d'accès qui n'a pas au moins une instruction d'autorisation bloquera tout le trafic.

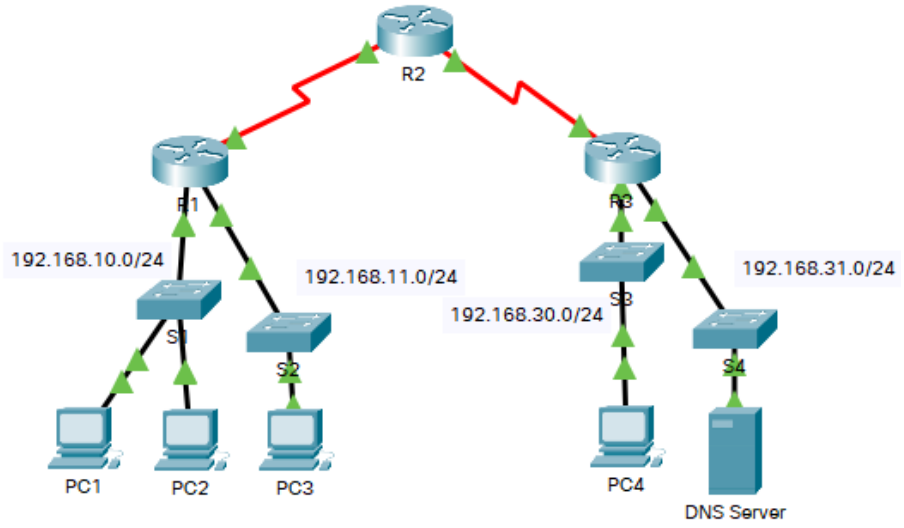
EXERCICE 1 : FONCTIONNEMENT DES ACLs

Question 1

À l'aide du logiciel « **Cisco Packet Tracer** », ***ouvrez*** le fichier « **exercice.pka** ».
Fermez la fenêtre « **PT Activity** » apparaissant à l'écran.

Vous allez observer comment une liste de contrôle d'accès peut être utilisée pour empêcher un ping d'atteindre les hôtes sur des réseaux distants.
Après avoir retiré la liste de contrôle d'accès de la configuration, les requêtes ping aboutiront.

Ici le routeur « R1 » est configuré avec une liste de contrôle d'accès interdisant les requêtes ping vers le réseau extérieur.



Extrait de l'architecture physique et logique de l'exercice

En utilisant le mode simulation (filtre ICMP et enveloppe PDU : simple PDU) :

Effectuez un test d'echo de niveau 3 entre PC1 et PC2.

Effectuez un test d'echo de niveau 3 entre PC1 et PC3.

Pourquoi les requêtes ping ont-elles abouti ?

Effectuez un test d'echo de niveau 3 entre PC1 et PC4.

Effectuez un test d'echo de niveau 3 entre PC1 et DNS Server.

Pourquoi les requêtes ping ont-elles échoué ?

Question 2

Vous allez maintenant supprimer la liste de contrôle d'accès du routeur R1 et vérifiez que les requêtes ping aboutissent.

Affichez la ou les listes de contrôle d'accès actuelles en utilisant la commande :

```
R1#show access-lists
```

Vous devez obtenir le résultat ci-dessous :

```
Extended IP access list 101
        10 deny icmp any any echo
        20 permit ip any any
```

La première ligne de la liste de contrôle d'accès empêche le trafic de paquets d'écho ICMP (requêtes ping) de **n'importe quelle** source vers **n'importe quelle** destination. La deuxième ligne de la liste de contrôle d'accès autorise tout autre trafic **ip** depuis **n'importe quelle** source vers **n'importe quelle** destination.

Pour qu'une liste de contrôle d'accès affecte le fonctionnement d'un routeur, elle doit être appliquée quelque part. Ici elle est utilisée pour filtrer le trafic sur une interface. Bien que vous puissiez voir les informations IP avec la commande **`show ip interface`**, dans certaines situations il est plus judicieux d'utiliser simplement la commande **`show run`**.

En utilisant l'une de ces deux commandes ou les deux, à quelle interface la liste de contrôle d'accès est-elle appliquée ?

Vous pouvez supprimer des listes de contrôle d'accès de la configuration en exécutant la commande **`no access list`** *`[numéro de la liste de contrôle d'accès]`*.
La commande **`no access-list`** supprime toutes les listes de contrôle d'accès configurées sur le routeur et la commande **`no access-list`** [*`numéro de la liste de contrôle d'accès`*] supprime une liste en particulier.

Question 3

En mode de configuration globale, ***supprimez*** la liste de contrôle d'accès.

Donnez la commande (ligne complète) que vous avez utilisé.

Vérifiez que PC1 peut maintenant envoyer des requêtes ping à PC4 et à DNS Server.

LES ACLs STANDARDS ET ÉTENDUES

Il existe deux types de listes de contrôle d'accès IPv4 Cisco : les listes standards et les listes étendues.

Les listes de contrôle d'accès IPv6 Cisco sont similaires aux listes de contrôle d'accès étendues IPv4.

- Listes de contrôle d'accès standard :
Les listes de contrôle d'accès standards peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source. La destination du paquet et les ports concernés ne sont pas évalués. L'exemple de commande ci-dessous autorise tout le trafic provenant du réseau 192.168.30.0/24. Compte tenu de l'instruction implicite « `deny any` » à la fin de la liste, tout autre trafic est bloqué avec cette liste. Les listes de contrôle d'accès standards sont créées en mode de configuration globale.

```
access-list permit 192.168.30.0 0.0.0.255
```

`0.0.0.255` est un masque générique que vous découvrirez un peu plus loin dans l'activité.

Les listes de contrôle d'accès standards filtrent les paquets IP en fonction de l'adresse source uniquement.

- Listes de contrôle d'accès étendues :
Les listes de contrôle d'accès étendues filtrent les paquets IPv4 en fonction de différents critères :
- Type de protocole
- Adresse IPv4 source
- Adresse IPv4 de destination
- Ports TCP ou UDP source
- Ports TCP ou UDP de destination
- Informations facultatives sur le type de protocole pour un contrôle plus précis

Sur l'exemple de commande ci-dessous :

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

La liste de contrôle d'accès `103` autorise tout le trafic provenant des adresses du réseau 192.168.30.0/24 à entrer sur n'importe quel réseau IPv4 si le port de destination de l'hôte est `80` (HTTP). Les listes de contrôle d'accès étendues sont créées en mode de configuration globale.

NUMÉROTATION ET NOMMAGE DES ACLs

Les listes de contrôle d'accès standards et étendues et leur liste d'instructions peuvent être identifiées par **un numéro** ou par **un nom**.

Les listes de contrôle d'accès numérotées sont pratiques pour déterminer le type de liste sur des réseaux de petite taille dont la définition du trafic est plus homogène. Toutefois, le numéro n'indique pas la fonction d'une liste de contrôle d'accès. C'est pourquoi, depuis la version 11.2 de Cisco IOS, vous pouvez utiliser un nom pour identifier une liste de contrôle d'accès Cisco.

Concernant les listes de contrôle d'accès numérotées, les numéros 200 à 1 299 ne sont pas disponibles, car ils sont utilisés par d'autres protocoles dont la plupart sont anciens ou obsolètes.

Par exemple les numéros de protocole ACL 600 à 699 sont utilisés par Appletalk et les numéros 800 à 899 par IPX, deux protocoles anciens.

Liste de contrôle d'accès numérotée :

Attribution d'un numéro en fonction du protocole à filtrer.
- Plages 1 à 99 et 1 300 à 1 999 : listes de contrôle d'accès IP standard
- Plages 100 à 199 et 2 000 à 2 699 : listes de contrôle d'accès IP étendue

Liste de contrôle d'accès nommée :

Attribution d'un nom à la liste de contrôle d'accès.
- Les noms doivent se composer de caractères alphanumériques.
- Il est conseillé d'écrire le nom en MAJUSCULES.
- Les noms ne doivent pas contenir d'espaces ni de signes de ponctuation.
- Il est possible d'ajouter et de supprimer des entrées de la liste de contrôle d'accès.

LES MASQUES GÉNÉRIQUES

Les listes de contrôle d'accès IPv4 incluent l'utilisation de **masques génériques**. Un masque générique est une chaîne de 32 chiffres binaires utilisés par le routeur pour déterminer quels bits de l'adresse examiner afin d'établir une correspondance.

À la différence des listes de contrôle d'accès IPv4, les listes de contrôle d'accès IPv6 n'utilisent pas de masques génériques. Au lieu de cela, la longueur de préfixe est utilisée pour indiquer dans quelle mesure l'adresse IPv6 source ou de destination doit correspondre. Les listes de contrôle d'accès IPv6 ne pas sont traitées dans cette activité.

Comme les masques de sous-réseau, les chiffres 1 et 0 du masque générique indiquent comment traiter les bits d'adresse IP correspondants. Cependant, dans un masque générique, ces bits sont utilisés à d'autres fins et suivent des règles différentes.
Les masques de sous-réseau utilisent les chiffres binaires 1 et 0 pour identifier la partie réseau, la partie sous-réseau et la partie hôte d'une adresse IP. Les masques génériques utilisent les chiffres binaires 1 et 0 pour filtrer des adresses IP ou des groupes d'adresses IP, afin d'autoriser ou de refuser l'accès aux ressources.

Les masques génériques et les masques de sous-réseau diffèrent dans leur méthode de mise en correspondance des 1 et des 0 binaires. Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0 :
- Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.
- Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse.

La figure ci-dessous montre comment les différents masques génériques filtrent les adresses IP.

Position de bit d'octet et valeur d'adresse du bit

128	64	32	16	8	4	2	1		**Exemples**
0	0	0	0	0	0	0	0	=	Correspondance de tous les bits d'adresse (correspondance complète)
0	0	1	1	1	1	1	1	=	Les 6 derniers bits d'adresse sont ignorés
0	0	0	0	1	1	1	1	=	Les 4 derniers bits d'adresse sont ignorés
1	1	1	1	1	1	0	0	=	Les 6 premiers bits d'adresse sont ignorés
1	1	1	1	1	1	1	1	=	Tous les bits dans l'octet sont ignorés

Les masques génériques sont souvent appelés **masques inverses**. En effet, contrairement à un masque de sous-réseau, où le chiffre binaire 1 équivaut à une correspondance et le chiffre binaire 0 à une non-correspondance, les masques génériques procèdent de façon inverse.

Utilisation d'un masque générique

Le tableau ci-dessous présente les résultats obtenus après l'application d'un masque générique 0.0.255.255 à une adresse IPv4 32 bits. N'oubliez pas que le chiffre binaire 0 équivaut à une valeur renvoyant une correspondance.

Les masques génériques sont également utilisés lors de la configuration de certains protocoles de routage IPv4 tels que le protocole OSPF, pour les activer sur des interfaces spécifiques.

	Adresse décimale	Adresse binaire
Adresse IP à traiter	192.168.10.0	11000000.10101000.00001010.00000000
Masque générique	0.0.255.255	00000000.00000000.11111111.11111111
Adresse IP résultante	192.168.0.0	11000000.10101000.00000000.00000000

Le calcul du masque générique demande un peu de pratique. La figure ci-dessous présente trois exemples de masques génériques.

Exemple 1

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.0	00000000.00000000.00000000.00000000
Résultats	192.168.1.1	11000000.10101000.00000001.00000001

Exemple 2

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	255.255.255.255	11111111.11111111.11111111.11111111
Résultats	0.0.0.0	00000000.00000000.00000000.00000000

Exemple 3

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.255	00000000.00000000.00000000.11111111
Résultats	192.168.1.0	11000000.10101000.00000001.00000000

Dans le premier exemple, le masque générique stipule que chaque bit de l'adresse IPv4 192.168.1.1 doit avoir une correspondance exacte.

Dans le deuxième exemple, le masque générique indique que la correspondance est systématique.
Dans le troisième exemple, le masque générique stipule que tous les hôtes du réseau 192.168.1.0/24 correspondent.

Ces exemples sont relativement simples. Cependant, le calcul des masques génériques peut être plus complexe.

Masques génériques correspondant à des plages
Les deux exemples ci-dessous sont plus complexes. Dans l'exemple 1, les deux premiers octets et les quatre premiers bits du troisième octet doivent présenter une correspondance exacte. Les quatre derniers bits du troisième octet et le dernier octet peuvent être n'importe quel nombre valide. Par conséquent, le masque vérifie la plage des réseaux 192.168.16.0 à 192.168.31.0.

Exemple 1

	Décimal	Binaire
Adresse IP	192.168.16.0	11000000.10101000.00010000.00000000
Masque générique	0.0.15.255	00000000.00000000.00001111.11111111
Plage de résultats	192.168.16.0 à 192.168.31.255	11000000.10101000.00010000.00000000 à 11000000.10101000.00011111.11111111

L'exemple 2 représente un masque générique avec une correspondance des deux premiers octets et du bit le moins significatif du troisième octet. Le dernier octet et les sept premiers bits du troisième octet peuvent être n'importe quel nombre valide. Ainsi, vous avez un masque qui autorise ou refuse tous les hôtes de sous-réseau depuis le réseau principal 192.168.0.0.

Exemple 2

	Décimal	Binaire
Adresse IP	192.168.1.0	11000000.10101000.00000001.00000000
Masque générique	0.0.254.255	00000000.00000000.11111110.11111111
Résultat	192.168.1.0	11000000.10101000.00000001.00000000
	Tous les sous-réseaux impairs sur le réseau principal 192.168.0.0	

Le calcul des masques génériques peut être complexe. La méthode la plus rapide consiste à soustraire le masque de sous-réseau à 255.255.255.255.

Calcul du masque générique : exemple 1
Supposons que vous souhaitiez autoriser l'accès de tous les utilisateurs du réseau 192.168.3.0. Sachant que le masque de sous-réseau est 255.255.255.0, vous pouvez utiliser 255.255.255.255 et y soustraire le masque de sous-réseau 255.255.255.0. Cette solution génère le masque générique 0.0.0.255.

Exemple 1

```
  255.255.255.255
- 255.255.255.000
  000.000.000.255
```

Calcul du masque générique : exemple 2
Supposons maintenant que vous souhaitiez autoriser les 14 utilisateurs du sous-réseau 192.168.3.32/28 à accéder au réseau. Le masque du sous-réseau IP est 255.255.255.240. Nous utilisons donc 255.255.255.255 et y soustrayons le masque de sous-réseau 255.255.255.240. Cette solution génère le masque générique 0.0.0.15.

Exemple 2

```
  255.255.255.255
- 255.255.255.240
  000.000.000.015
```

Calcul du masque générique : exemple 3
Supposons que vous souhaitiez faire correspondre uniquement les réseaux 192.168.10.0 et 192.168.11.0. Utilisons 255.255.255.255 et soustrayons le masque de sous-réseau normal, à savoir 255.255.254.0 dans cet exemple. Cette solution génère 0.0.1.255.

Exemple 3

```
  255.255.255.255
- 255.255.254.000
  000.000.001.255
```

Vous pouvez obtenir le même résultat en utilisant des instructions telles que les suivantes :

```
R1(config)# access-list 10 permit 192.168.10.0
R1(config)# access-list 10 permit 192.168.11.0
```

Il est bien plus efficace de configurer le masque générique de la manière suivante :

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.1.255
```

Étudiez la configuration ci-dessous pour mettre en correspondance les réseaux de la plage 192.168.16.0 à 192.168.31.0 :

```
R1(config)# access-list 10 permit 192.168.16.0
R1(config)# access-list 10 permit 192.168.17.0
R1(config)# access-list 10 permit 192.168.18.0
R1(config)# access-list 10 permit 192.168.19.0
R1(config)# access-list 10 permit 192.168.20.0
R1(config)# access-list 10 permit 192.168.21.0
R1(config)# access-list 10 permit 192.168.22.0
R1(config)# access-list 10 permit 192.168.23.0
R1(config)# access-list 10 permit 192.168.24.0
R1(config)# access-list 10 permit 192.168.25.0
R1(config)# access-list 10 permit 192.168.26.0
R1(config)# access-list 10 permit 192.168.27.0
R1(config)# access-list 10 permit 192.168.28.0
R1(config)# access-list 10 permit 192.168.29.0
R1(config)# access-list 10 permit 192.168.30.0
R1(config)# access-list 10 permit 192.168.31.0
```

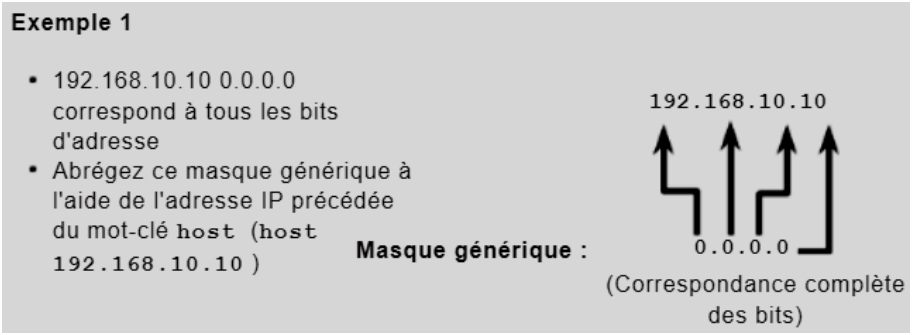
Les 16 instructions de configuration précédentes peuvent être réduites en une seule instruction en utilisant le masque générique approprié comme indiqué ci-dessous :

```
R1(config)# access-list 10 permit 192.168.16.0 0.0.15.255
```

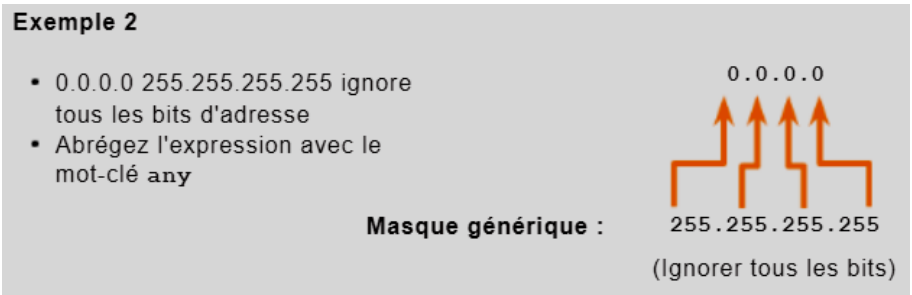
Travailler avec des représentations décimales de bits de masque générique peut être fastidieux. Les mots-clés **host** (hôte) et **any** (tous) permettent d'identifier les utilisations les plus courantes des masques génériques, et simplifient ainsi cette tâche. Ils suppriment la saisie des masques génériques lorsque vous identifiez un hôte spécifique ou un réseau. Ces mots-clés facilitent également la lecture d'une liste de contrôle d'accès en offrant des indices visuels comme la source ou la destination des critères.

Le mot-clé **host** remplace le masque 0.0.0.0. Ce masque indique que tous les bits de l'adresse IPv4 doivent correspondre ou qu'un seul hôte est conforme.
Le mot-clé **any** remplace l'adresse IP et le masque 255.255.255.255. Ce masque indique qu'il convient d'ignorer l'intégralité de l'adresse IPv4 ou d'accepter n'importe quelle adresse.

Exemple 1 : processus de masque générique avec une adresse IP unique
Dans l'exemple 1 ci-dessous, au lieu de saisir **`192.168.10.10 0.0.0.0`**, vous pouvez utiliser **`host 192.168.10.10`**.



Exemple 2 : processus de masque générique avec une adresse IP à concordance quelconque
Dans l'exemple 2, au lieu de saisir **`0.0.0.0 255.255.255.255`**, vous pouvez utiliser le mot-clé **any** seul.



Les mots-clés **`host`** et **any** peuvent également être utilisés lors de la configuration d'une liste de contrôle d'accès IPv6.

L'exemple ci-dessous indique comment utiliser le mot-clé **any** pour remplacer l'adresse IPv4 0.0.0.0, avec un masque générique 255.255.255.255.

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 permit any
```

L'exemple 2 montre comment utiliser le mot-clé **host** pour remplacer le masque générique lors de l'identification d'un hôte unique.

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit host 192.168.10.10
```

EXERCICE 2 : MASQUE GÉNÉRIQUE

Question 1

Calculez les masques génériques permettant de filtrer les réseaux selon le tableau ci-dessous.

Réseau	Masque générique
192.168.0.0/24	
192.168.0.0/20	
10.1.0.0/16	
10.0.0.0/30	
172.16.0.0/15	

Question 2

Selon les commandes suivantes ***précisez*** la plage réseau et/ou la ou les machines concernées par le filtrage.

Commandes	Plage réseau ou machine(s) filtrée(s)
`access-list 51 permit 192.168.0.0 0.0.1.255`	
`access-list 101 permit ip 192.168.0.0 0.0.0.255 any`	
`access-list 107 deny ip 169.254.0.0 0.0.255.255 any`	
`access-list 77 permit 172.16.0.0 0.0.0.1`	
`access-list 110 deny icmp any 192.168.1.254 255.255.255.255 echo`	
`access-list 100 permit ip any host 10.0.0.1 eq 21`	
`access-list 2000 permit ip 172.16.0.0 0.1.255.255 host 192.168.0.1 eq 80`	
`access-list 1 permit 192.168.0.0 0.0.0.255`	

Question 3

Complétez le tableau (dernière colonne par les mots Autoriser ou Refuser) ci-dessous en fonction de l'instruction de liste de contrôle d'accès et l'adresse de comparaison.

Instruction de liste de contrôle d'accès	Adresse de comparaison	Autoriser ou Refuser
`access-list 50 permit 192.168.122.128 0.0.0.63`	192.168.122.195	
`access-list 20 permit 192.168.223.64 0.0.0.15`	192.168.223.72	
`access-list 21 permit 192.0.2.11 0.0.0.15`	192.0.2.17	
`access-list 33 permit 198.51.100.58 0.0.0.63`	198.51.100.3	

CRÉATION DES ACLs

L'écriture des listes de contrôle d'accès peut être une tâche complexe. Pour chaque interface, plusieurs stratégies peuvent être nécessaires pour gérer le type de trafic autorisé à entrer dans cette interface ou en sortir. Le routeur représenté sur la figure ci-dessous dispose de deux interfaces configurées pour IPv4 et IPv6. Si nous avions besoin de listes de contrôle d'accès pour les deux protocoles, sur les deux interfaces et dans les deux directions, nous aurions besoin de huit listes de contrôle d'accès distinctes. Chaque interface possèderait quatre listes de contrôle d'accès : deux pour IPv4 et deux pour IPv6. Pour chaque protocole, une liste de contrôle d'accès sert au trafic entrant et une autre au trafic sortant.

Une liste par interface, par direction et par protocole

Avec deux interfaces et deux protocoles, ce routeur peut avoir un total de huit listes de contrôle d'accès appliquées

Il n'est pas nécessaire de configurer les listes de contrôle d'accès dans les deux directions. Le nombre de listes de contrôle d'accès et leur direction appliquée à l'interface dépendront des exigences.

Vous trouverez ci-dessous quelques instructions pour utiliser les listes de contrôle d'accès :

- Utilisez des listes de contrôle d'accès sur les routeurs pare-feu entre votre réseau interne et un réseau externe, par exemple Internet.
- Utilisez des listes de contrôle d'accès sur un routeur situé entre deux sections de votre réseau pour contrôler le trafic entrant ou sortant sur une partie donnée du réseau interne.
- Configurez des listes de contrôle d'accès sur les routeurs périphériques situés à la périphérie de vos réseaux. Cela permet de fournir une protection de base contre le réseau externe ou entre une zone plus sensible et une zone moins contrôlée de votre réseau.
- Configurez des listes de contrôle d'accès pour tout protocole réseau configuré sur les interfaces de routeur périphérique.

Règles :

Vous pouvez configurer une liste de contrôle d'accès par protocole, par direction et par interface :

- **Une liste de contrôle d'accès par protocole** : pour contrôler le flux du trafic sur une interface, définissez une liste de contrôle d'accès pour chaque protocole activé sur l'interface.
- **Une liste de contrôle d'accès par direction** : les listes de contrôle d'accès contrôlent le trafic dans une seule direction à la fois sur une interface. Vous devez créer deux listes de contrôle d'accès ; la première pour contrôler le trafic entrant et la seconde pour contrôler le trafic sortant.
- **Une liste de contrôle d'accès par interface** : les listes de contrôle d'accès contrôlent le trafic dans une seule interface, par exemple, Gigabit Ethernet 0/0.

Méthodes recommandées pour les ACLs :

L'utilisation des listes de contrôle d'accès nécessite beaucoup de précision et de soin. Les erreurs peuvent vous coûter cher et se solder par des pannes de réseau, d'importants efforts de dépannage et des services réseau médiocres. Avant de configurer une liste de contrôle d'accès, une planification de base s'impose. Le tableau ci-dessous décrit les directives fondamentales des meilleures pratiques en matière de listes de contrôle d'accès.

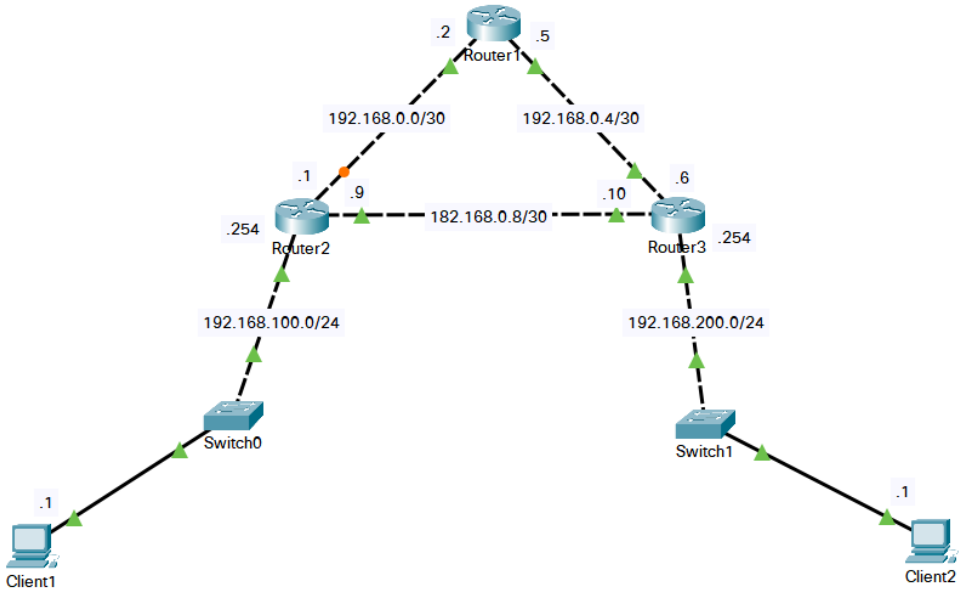
Directive	Avantage
Créez vos listes de contrôle d'accès conformément à la stratégie de sécurité de votre entreprise.	Vous serez ainsi certain d'implémenter les instructions relatives à la sécurité organisationnelle.
Préparez une description des tâches que devront effectuer les listes de contrôle d'accès.	Vous éviterez ainsi de créer d'éventuels problèmes d'accès par mégarde.
Utilisez un éditeur de texte pour créer, modifier et enregistrer les listes de contrôle d'accès.	Vous pourrez ainsi créer une bibliothèque de listes de contrôle d'accès réutilisables.
Testez vos listes de contrôle d'accès sur un réseau de développement avant de les implémenter sur un réseau de production.	Vous éviterez ainsi de commettre des erreurs coûteuses.

EXERCICE 3 : CONFIGURATION ACL STANDARD

Question 1

À l'aide du logiciel **Cisco Packet Tracer**, ***réalisez*** la topologie (physique et logique) conformément au schéma page suivante.

Toutes les machines doivent pouvoir se contacter.



Topologie de l'exercice

Vérifiez la connectivité entre les machines.

FAÎTES VALIDER LA QUESTION 1 PAR LE PROFESSEUR AVANT DE POURSUIVRE !

On souhaite filtrer le trafic en configurant des ACLs conformément au fonctionnement attendu ci-dessous :

- Routeur 1 ne peut pas communiquer avec le réseau 192.168.100.0/24.
- Routeur 1 ne peut pas communiquer avec le réseau 192.168.200.0/24.
- Client1 ne peut pas communiquer avec Routeur1.
- Le réseau 192.168.200.0/24 ne peut pas communiquer avec le Routeur1.
- Le reste du trafic est autorisé.

Voir chapitre 12 « Les ACLs » contenu dans le fichier « Configurer un routeur cisco.pdf » se trouvant dans le dossier « Support » de l'activité.

Empêcher Routeur1 de communiquer avec le réseau 192.168.100.0/24 :

Entrez les commandes suivantes :

```
…
Routeur2(config)#no access-list 1
Routeur2(config)#access-list 1 deny host 192.168.0.2
Routeur2(config)#access-list 1 deny host 192.168.0.5
Routeur2(config)#access-list 1 permit any
Routeur2(config)#interface fastethernet 0/0
Routeur2(config-if)#ip access-group 1 out
Routeur2(config-if)#exit
…
```

La présence de la commande **no access-list 1** permet de supprimer l'ACL si elle existait précédemment.
L'interface **fastethernet 0/0** peut être différente selon votre montage.

Empêcher Routeur1 de communiquer avec le réseau 192.168.200.0/24 :

Entrez les commandes suivantes :

```
…
Routeur3(config)#no access-list 1
Routeur3(config)#access-list 1 deny host 192.168.0.2
Routeur3(config)#access-list 1 deny host 192.168.0.5
Routeur3(config)#access-list 1 permit any
Routeur3(config)#interface fastethernet 0/0
Routeur3(config-if)#ip access-group 1 out
Routeur3(config-if)#exit
…
```

Empêcher Client1 de communiquer avec Routeur1 :

Entrez les commandes suivantes :

```
…
Routeur1(config)#no access-list 1
Routeur1(config)#no access-list 2
Routeur1(config)#access-list 1 deny host 192.168.100.1
Routeur1(config)#access-list 1 permit any
Routeur1(config)#access-list 2 deny host 192.168.100.1
Routeur1(config)#access-list 2 permit any
Routeur1(config)#interface fastethernet 0/0
Routeur1(config-if)#ip access-group 1 in
Routeur1(config)#interface fastethernet 0/1
Routeur1(config-if)#ip access-group 2 in
Routeur1(config-if)#exit
…
```

Empêcher le réseau 192.168.200.0/24 de communiquer avec Routeur1 :

Entrez les commandes suivantes :

```
…
Routeur1(config)#access-list 1 deny 192.168.200.0 0.0.0.255
Routeur1(config)#access-list 1 permit any
Routeur1(config)#access-list 2 deny 192.168.200.0 0.0.0.255
Routeur1(config)#access-list 2 permit any
Routeur1(config)#interface fastethernet 0/0
Routeur1(config-if)#ip access-group 1 in
Routeur1(config)#interface fastethernet 0/1
Routeur1(config-if)#ip access-group 2 in
Routeur1(config-if)#exit
…
```

Question 2

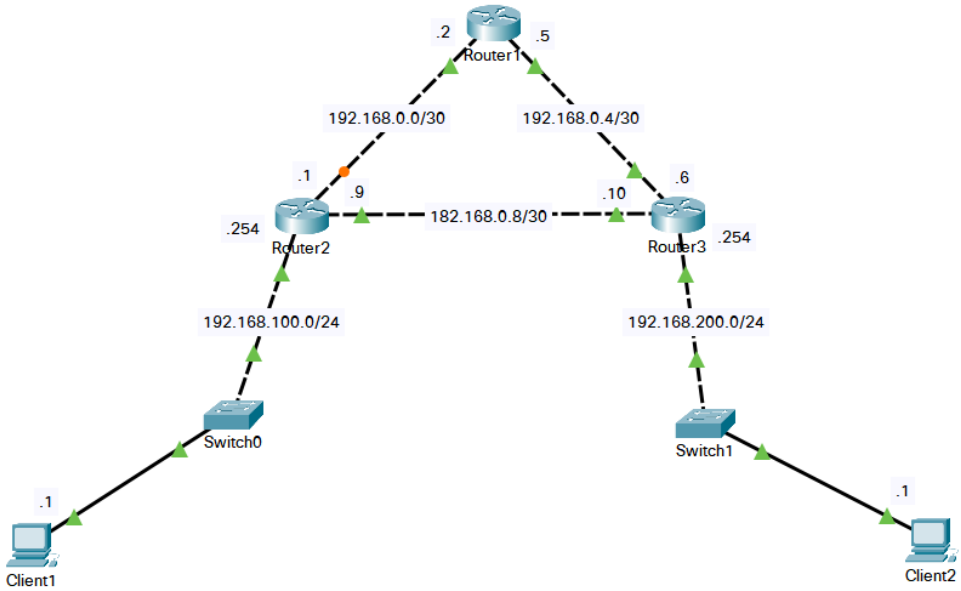
Vérifiez le fonctionnement des ACLs à l'aide de tests d'echo de niveau 3.
Vérifiez la configuration des ACLs à l'aide des commandes : **`show access-lists`** et **`show access-lists ID`**.

Les listes de contrôle d'accès standard sont simples et rapides à mettre en œuvre, par contre elles sont moins puissantes que les ACLs étendues et leur fonctionnement implique que le trafic filtré soit supprimé au dernier moment, autrement dit, le trafic circule sur le réseau pour rien.
Les listes de contrôle d'accès standard doivent être placées au plus près de la destination.
Avant de commencer une ACL, il est important d'utiliser la commande **`no access-list ID`** qui permet de supprimer l'ACL ***ID***.

EXERCICE 4 : CONFIGURATION ACL ÉTENDUE

À l'aide du logiciel Cisco Packet Tracer, ***réalisez*** la topologie conformément au schéma ci-dessous (vous pouvez réutiliser la topologie de l'exercice 3).

Chaque machine doit pouvoir contacter l'autre.



Topologie de l'exercice

On souhaite configurer des ACLs conformément au fonctionnement attendu ci-dessous :

- Autorisez le trafic Telnet à destination de tous les routeurs depuis les réseaux 192.168.100.0/24 et 192.168.200.0/24.
- Autorisez le trafic ICMP echo et reply entre les réseaux 192.168.100.0/24 et 192.168.200.0/24.
- Le reste du trafic est implicitement interdit.

Entrez les commandes suivantes sur Routeur2 :

```
…
Routeur2(config)#no access-list 100
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.1 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.2 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.5 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.6 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.9 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.0.10 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.100.254 eq telnet
Routeur2(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255 host
192.168.200.254 eq telnet
Routeur2(config)#access-list 100 permit icmp 192.168.100.0 0.0.0.255 host
192.168.0.1 192.168.200.0 0.0.0.255 eq echo
Routeur2(config)#access-list 100 permit icmp 192.168.100.0 0.0.0.255 host
192.168.0.1 192.168.200.0 0.0.0.255 eq echo-reply
Routeur2(config)#interface fastethernet 0/0
Routeur2(config-if)#ip access-group 100 in
Routeur2(config-if)#exit
…
```

Question 2

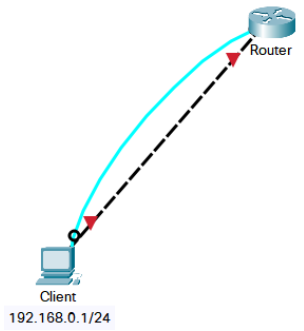
En vous inspirant de la configuration de Routeur 2, ***configurez*** Routeur3.
Vérifiez le fonctionnement des ACLs à l'aide de la commande **`ping`** ou **`Telnet`**.

Les listes de contrôle d'accès étendues permettent de spécifier la source et la destination du trafic, elles peuvent être placées près de la source du trafic et ainsi éviter que du trafic inutile circule sur le réseau. Elles permettent également de spécifier les protocoles à filtrer.

Il existe deux principes pour créer des ACLs : soit refuser quelques flux réseau et autoriser le reste, soit autoriser quelques flux réseaux et refuser le reste.
La seconde méthode est privilégiée car elle est plus sécurisée.
La première méthode présente l'avantage d'être plus simple à mettre en œuvre. Dans les deux cas, il faut avoir une bonne connaissance des flux réseau générés par toutes les applications.

EXERCICE 5 : RESTRICTION D'ACCÈS TELNET PAR ACL STANDARD

À l'aide du logiciel **Cisco Packet Tracer**, ***réalisez*** la topologie conformément au schéma ci-dessous.



Topologie de l'exercice

Question 1

Mettez en place la topologie ci-dessus.
Vérifiez la connectivité.

Question 2

Entrez les commandes suivantes sur le routeur :

```
…
Routeur(config)#access-list 1
Routeur(config)#access-list 1 permit host 192.168.0.1
Routeur(config)#line vty 0 4
Routeur(config-line)#password P@sswOrd
Routeur(config-line)#login
Routeur(config-line)#banner login #Access Restreint#
Routeur(config-line)#access-class 1 in
Routeur(config-line)#exit
…
```

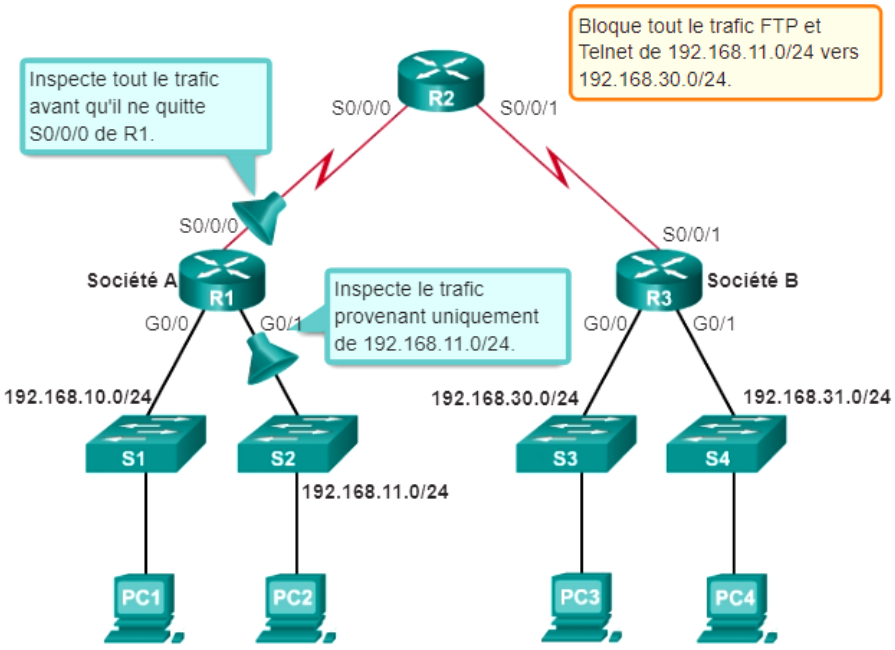
Seul la machine possédant l'IP 192.168.0.1 peut se connecter en Telnet.
Pour vérifier le bon fonctionnement de l'ACL, ***changez*** l'adresse IP du Client.

EMPLACEMENT DES ACLs

Comme les listes de contrôle d'accès standard, les listes de contrôle d'accès étendues peuvent filtrer le trafic en fonction de l'adresse source. Cependant, une liste de contrôle d'accès étendue peut également filtrer le trafic en fonction de l'adresse de destination, du protocole et du numéro de port. Cela offre aux administrateurs réseau davantage de flexibilité au niveau du type de trafic pouvant être filtré et de la position de la liste. La règle de base pour le placement des listes de contrôle d'accès étendues consiste à les placer aussi près que possible de la source. Cela

empêche le trafic indésirable d'être envoyé sur plusieurs réseaux pour être finalement refusé lorsqu'il atteint sa destination.

Les administrateurs réseau peuvent placer des listes de contrôle d'accès uniquement sur les périphériques qu'ils contrôlent. Par conséquent, cet emplacement doit être déterminé par la portée du contrôle dont dispose l'administrateur réseau. Sur la figure ci-dessous, l'administrateur de la société A, qui comprend les réseaux 192.168.10.0/24 et 192.168.11.0/24 (appelés .10 et .11 dans cet exemple), souhaite contrôler le trafic vers la société B. En particulier, l'administrateur souhaite refuser le trafic Telnet et FTP provenant du réseau .11 vers le réseau 192.168.30.0/24 (.30, dans cet exemple) de la société B. Dans un même temps, le reste du trafic provenant du réseau .11 doit être autorisé à quitter la société A sans aucune restriction.



Emplacement des ACLs étendues

Il existe plusieurs façons d'atteindre ces objectifs. Une liste de contrôle d'accès étendue placée sur R3 et bloquant le trafic Telnet et FTP provenant du réseau .11 serait une solution, mais l'administrateur ne contrôle pas R3. En outre, cette solution autorise le passage du trafic indésirable sur l'ensemble du réseau avant de le bloquer lorsqu'il arrive à destination. Cette situation affecte les performances réseau globales.

Il est plus judicieux de placer une liste de contrôle d'accès étendue sur R1, qui spécifie les adresses source et de destination (réseaux .11 et .30, respectivement) et applique la règle « Le trafic Telnet et FTP provenant du réseau .11 n'est pas autorisé à accéder au réseau .30 ». La figure montre deux interfaces de R1 sur lesquelles il est possible d'appliquer la liste de contrôle d'accès étendue :

- **Interface S0/0/0 de R1 (sortante)** : il est possible d'appliquer une liste de contrôle d'accès étendue sortante sur l'interface S0/0/0. Étant donné que la liste de contrôle d'accès étendue peut examiner les adresses source et de destination, seuls les paquets FTP et Telnet provenant de 192.168.11.0/24 seront refusés. Le reste du trafic provenant de 192.168.11.0/24 et des autres réseaux sera acheminé par R1. L'inconvénient de cette position de la liste de contrôle d'accès étendue sur l'interface est que tout le trafic sortant de S0/0/0 doit être traité par la liste de contrôle d'accès, y compris les paquets provenant de 192.168.10.0/24.

- Interface G0/1 de R1 (entrante) : l'application d'une liste contrôle d'accès étendue au trafic entrant dans l'interface G0/1 signifie que seuls les paquets provenant du réseau 192.168.11.0/24 sont soumis à la liste de contrôle sur R1. Puisque le filtre doit être limité aux seuls paquets quittant le réseau 192.168.11.0/24, l'application de la liste de contrôle d'accès étendue à G0/1 constitue la meilleure solution.

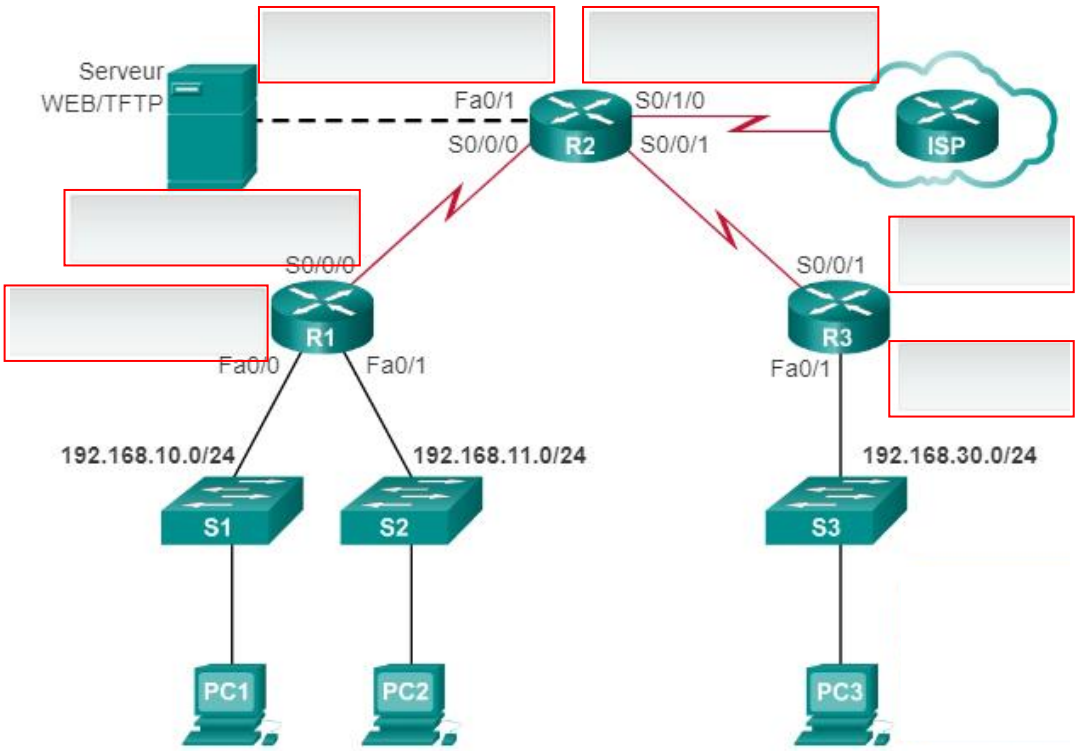
EXERCICE 6

Question

Évaluez les stratégies réseau.
Déterminez le meilleur positionnement des ACLs.
Complétez les encadrés par : **ACL standard** ou **ACL étendue**.

Stratégie réseau n°1 : utilisez une ACL standard pour empêcher le réseau 192.168.10.0/24 d'accéder à Internet via le FAI.

Stratégie réseau n°2 : utilisez une ACL étendue pour empêcher le réseau 192.168.30.0/24 d'accéder au serveur Web/TFTP.



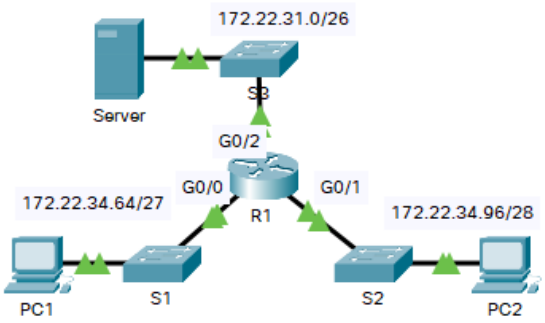
Topologie de l'exercice

Deux encadrés sont à compléter !

EXERCICE 7

À l'aide du logiciel **Cisco Packet Tracer**, ***ouvrez*** le fichier **Exercice7.pka**.
Suivez les indications apparaissant dans la fenêtre « **PT Activity** ».

Contexte :
Deux employés ont besoin d'accéder aux services fournis par le serveur. PC1 a uniquement besoin d'un accès FTP tandis que PC2 a uniquement besoin d'un accès Web. Les deux ordinateurs peuvent envoyer une requête ping au serveur, mais pas entre eux.



Topologie de l'exercice

FAÎTES VALIDER VOTRE TRAVAIL PAR LE PROFESSEUR !

N'OUBLIEZ PAS VOTRE COMPTE-RENDU !