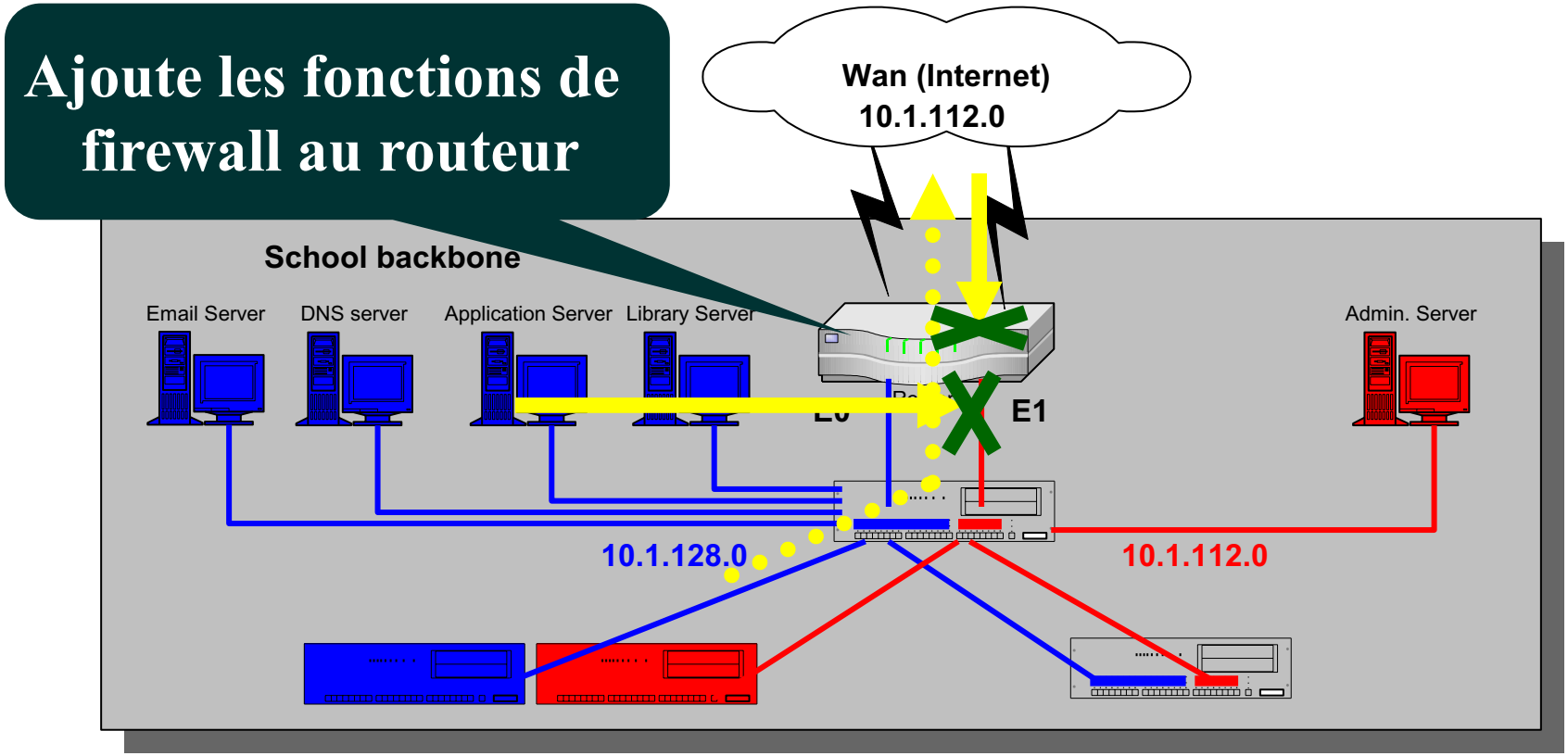
Les listes de contrôle d'accès

- A quoi ça sert
- Comment ça marche
- ACL standard ou étendue
- Les masques génériques (Wildcard Masks)
- La configuration des ACLs.

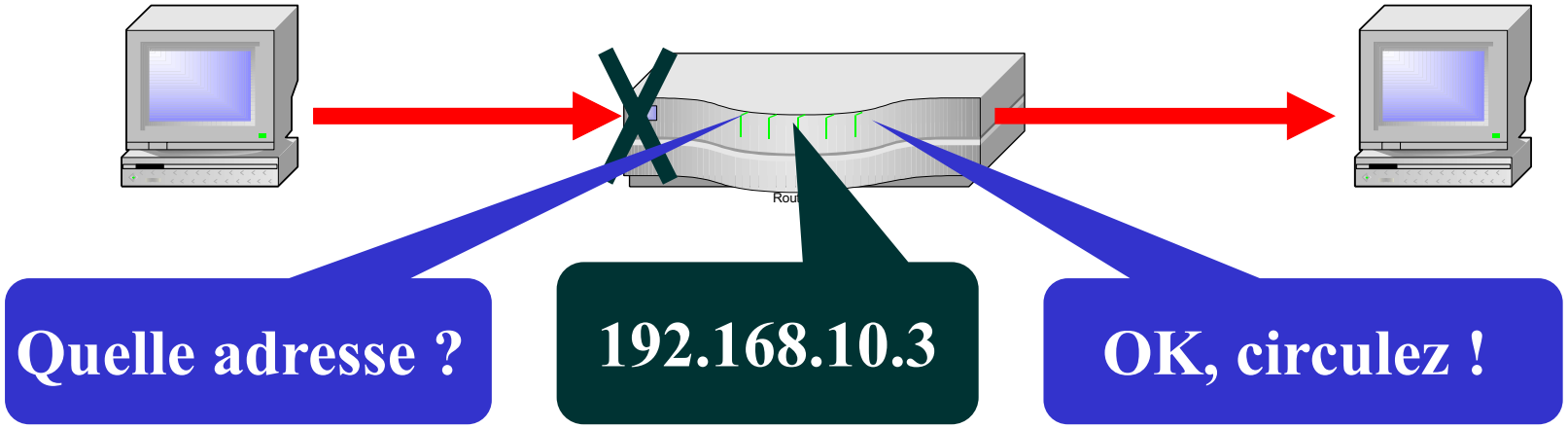
ACL - A quoi ça sert



- Contrôler le trafic à l'intérieur d'un réseau local
- Contrôler le trafic depuis l'extérieur (WAN) vers l'intérieur d 'un réseau local

ACL - Comment ça marche

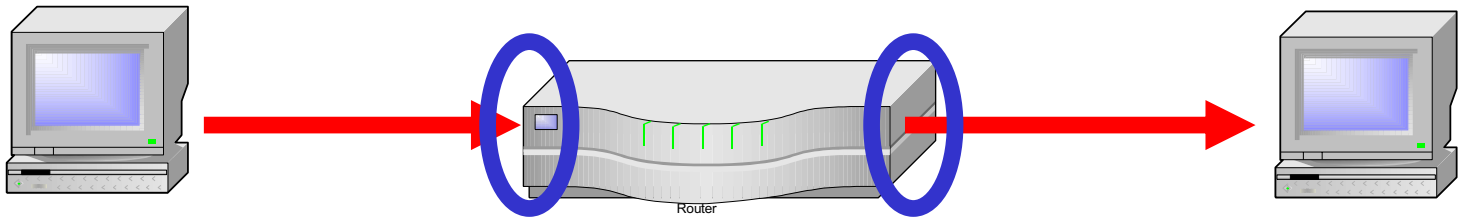
- Filtre les paquets en utilisant des éléments des couches 3 (adresses IP) et 4 (numéros de port des applications) de TCP-IP ;
- Par défaut, une liste de contrôle non paramétrée refuse tous les accès.



- Le paramétrage de l'ACL décide quel hôte ou groupe d'hôte peut (permit) ou ne peut pas (deny) transiter par le routeur.

ACL - Comment ça marche (2)

- Les ACLs sont créées en mode de configuration globale.
- Elles doivent ensuite être affectée à un (ou plusieurs) ports.

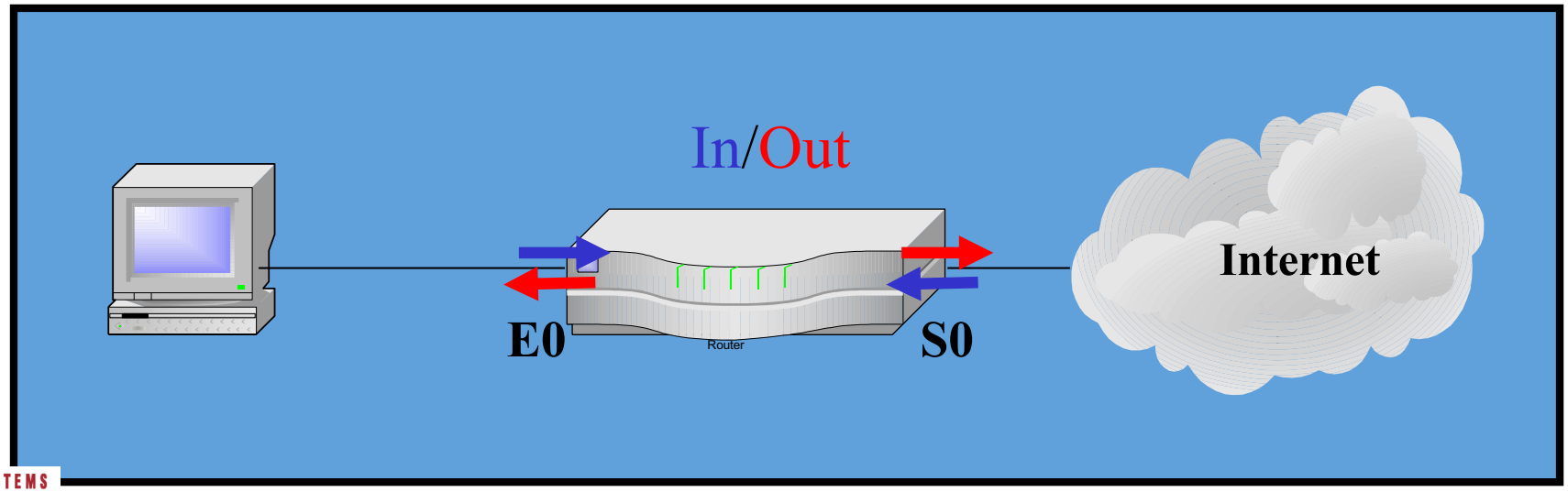


- Grâce aux *masques génériques (wildcard mask)*, le contrôle peut s'appliquer à un réseau, un sous-réseau, un hôte ou une catégorie d'hôtes.
- Ne contrôle pas les paquets émis par le routeur lui-même.

Les paramètres *In* et *Out*

(Inbound-Outbound)

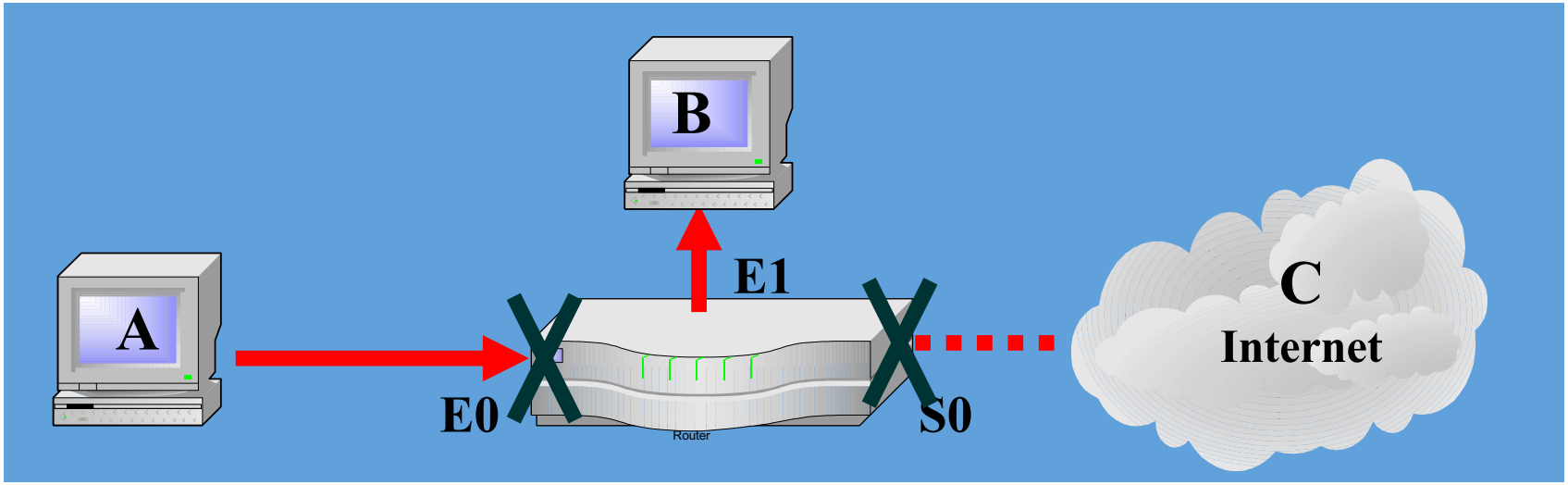
- Par défaut, ce paramètre est configuré sur *out (vers le réseau)*
- Le paramètre *In* (vers le routeur) ou *Out* se place sur l'interface à laquelle on veut appliquer la liste d'accès



Quel port choisir

Deux solutions pour bloquer A vers B

- ACL 1 Deny A
- Attribut ACL 1 à l'interface E0 **in**

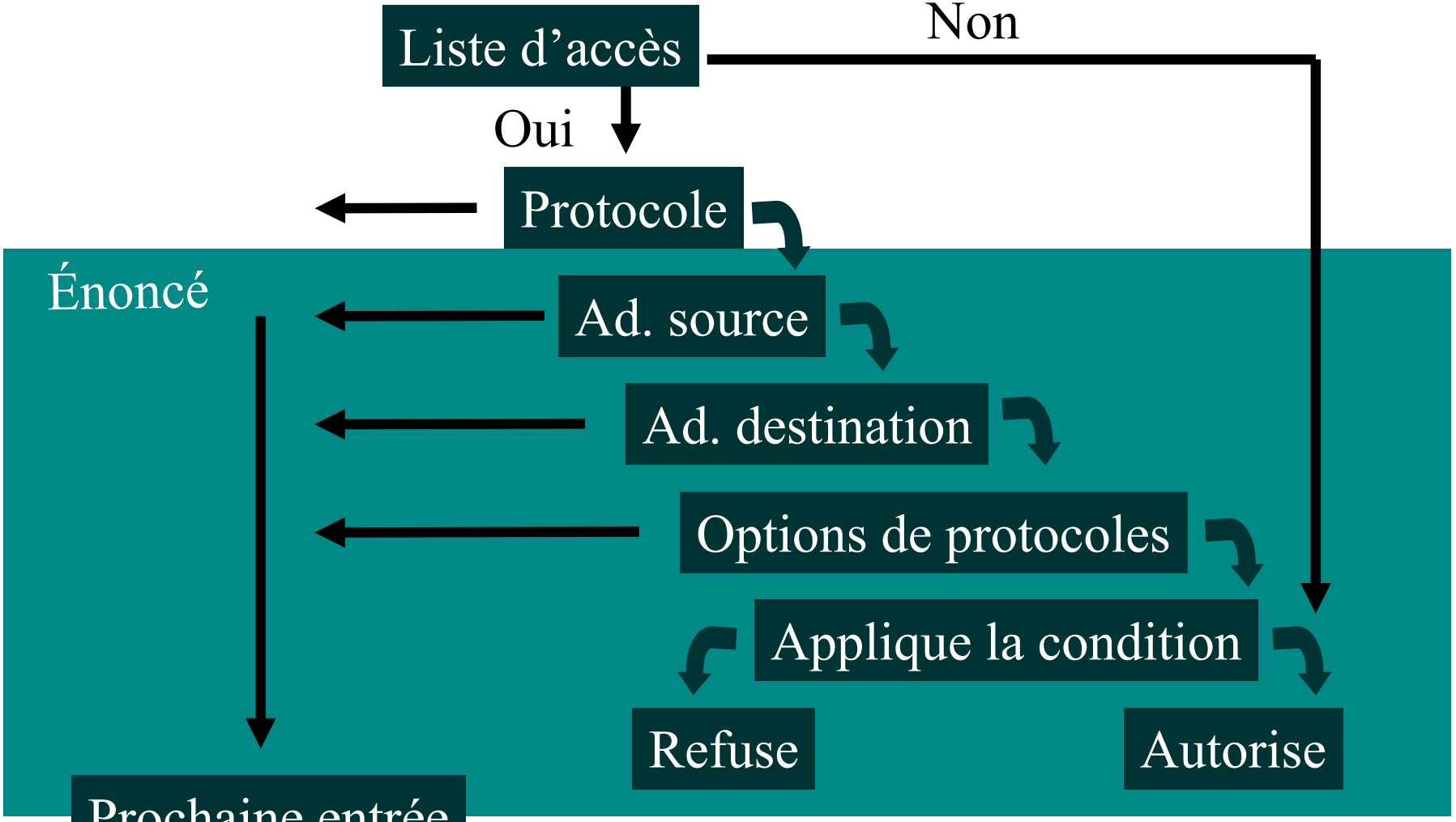


- ACL 1 Deny A
- Attribut ACL 1 à l'interface E1 **out**

ACL standard ou étendue ?

- Les listes de contrôles standards filtrent l'accès :
  - à partir de l'adresse source uniquement .
- Les listes de contrôle étendues peuvent filtrer l'accès :
  - selon l'adresse de source et de destination ;
  - selon les types de protocole de transport (TCP, UDP)
  - et le numéro de port (couche application).

Liste de conditions de l'ACL étendue



Les types de liste d’accès

L’ACL s’applique au protocole routé choisi

Type de liste d'accès	Numéros d'identification
IP Standard Extended	1-99 100-199 Named (Cisco IOS 11.2 and later)
IPX Standard SAP filters	800-899 1000-1099
Apple Talk	600-699

Permission ou refus

- Par défaut, dès qu'une liste d'accès est créée, elle refuse le passage à tout ce qui n'est pas spécifiquement autorisé
- De façon implicite (cela n'apparaît pas à la ligne de commande) la liste de contrôle d'accès se termine par l'instruction «**refuse tout**» ('deny any').
- En général, l'administrateur devrait donner des permissions (permit) plutôt que des interdictions (deny).

Les masques génériques

(Wildcard Masks)

- Utilisés pour identifier les cibles des ACLs.
- Dans la ligne suivante :

Router (config)# access-list 11 deny 192.168.18.0 0.0.0.255

- Le masque générique indique que l'accès est refusé à tous les postes du réseau **192.168.18.0.**

Les masques génériques (2)

Addresse

1100 0000 . 1010 1000 . 0001 0010 . 0000 0000

0000 0000 . 0000 0000 . 0000 0000 . 1111 1111

Masque générique

Inverse du MSR

Router (config)# access-list 11 permit 192.168.18.0 0.0.0.255

- Les «0» signifient que le nombre doit être pris en compte (match).
- Les «1» indiquent que le nombre doit être ignoré.
- Dans ce cas, l'énoncé ignore tout ce qui concerne la partie hôte de l'adresse.

Les masques génériques (3)

Addresse

1100 0000 . 1010 1000 . 0001 0010 . 0000 0000

0000 0000 . 0000 0000 . 0000 0000 . 1111 1110

Masque générique

Router (config)# access-list 11 permit 192.168.18.0 0.0.0.254

- Ici, l'énoncé ignore tout ce qui concerne la partie hôte de l'adresse, sauf le dernier bit.
- Tous les hôtes pairs du réseau se voient autoriser l'accès.

Les masques génériques (4)

Addresse

1100 0000 . 1010 1000 . 0001 0010 . 0000 0101

0000 0000 . 0000 0000 . 0000 0000 . 0000 0000

Masque générique

Router (config)# access-list 11 permit 192.168.18.5 0.0.0.0

- Avec ce masque, les 32 bits de l'adresse doivent être prises en compte (réseau et hôte)
- Dans ce cas, l'hôte 192.168.18.5 est le seul à se voir autoriser l'accès.

Les masques génériques (5)

Router (config)# access-list 11 permit any

Autorise l'accès à tous

(0.0.0.0 255.255.255.255)

Router (config)# access-list 11 host 192.168.16.1

Autorise l'accès pour le poste 192.168.16.1 uniquement (192.168.16.1 0.0.0.0)

Les masques génériques (6)- Exemple

Corp(config)#**access-list 10 deny 172.16.16.0 0.0.3.255**

Cette configuration permet au routeur de refusé le trafique de la plage réseau (172.16.16.0 jusqu'au 19.0)

Corp(config)#**access-list 10 deny 172.16.16.0 0.0.7.255**

Corp(config)#**access-list 10 deny 172.16.32.0 0.0.15.255**

Corp(config)#**access-list 10 deny 172.16.64.0 0.0.63.255**

Dernier exemple : du réseau 192.168.160.0 jusqu'au 192.168.191.255

Corp(config)#**access-list 10 deny 192.168.160.0 0.0.31.255**

Les lignes de commandes

- Refuse tout accès aux membres du réseau 192.168.128.0 vers toutes les destinations

Router (config)# access-list 101 deny ip 192.168.128.0 0.0.0.255 any

Router (config)# access-list 101 permit ip any any

- Applique les restrictions d'accès à l'interface E1 vers l'intérieur

Router (config)# int e1

Router (config-if)# ip access-group 101 in

Les lignes de commandes

- Autorise l'accès au Web aux postes désignés (10.1.128.1 à 10.1.128.254)

Router (config)# access-list 102 permit tcp 10.1.128.0 0.0.0.255 host 10.1.96.0 eq 80

- Applique les restrictions d'accès à l'interface E0 vers l'intérieur

  Router (config)# int e0

  Router (config-if)# ip access-group 102 in

Les lignes de commandes

- Refuse tout accès depuis toutes les sources vers toutes les destinations

```
Router (config)# access-list 103 deny  ip any any
```

- Applique les restrictions d'accès à l'interface S0 vers l'intérieur

```
Router (config)# int s0
Router (config-if)# ip access-group 103 in
```

Autres lignes de commandes

- Les mentions, lt, gt, eq, neq sont des opérateurs logiques utilisés pour autoriser les accès par type d ’application.
  permit tcp host 10.14.72.10 host 192.168.10.3 lt 1024
- La mention range
  permit tcp host 10.14.72.10 range 1024 1072 host 192.168.10.3 range 1024 1072

Contrôle dynamique des accès sur le trafic IP avec processus d'authentification des utilisateurs (lock and key features)

- Le **Lock and Key** est une fonctionnalité d'ACL dynamique sur les routeurs Cisco. Il permet de contrôler l'accès au réseau en exigeant une authentification utilisateur avant d'autoriser le trafic

Contrôle dynamique des accès sur le trafic IP avec processus d'authentification des utilisateurs (lock and key features)

Principe de fonctionnement :

1. **Initialement, tout le trafic est bloqué** : L'ACL dynamique ne contient aucune règle autorisant le trafic.
2. **Authentification de l'utilisateur** : Un utilisateur tente d'accéder à une ressource et initie une connexion Telnet (ou SSH) vers le routeur.
3. **Création d'une entrée ACL temporaire** : Après une authentification réussie via un serveur AAA (TACACS+ ou RADIUS) ou en local, une règle dynamique est insérée dans l'ACL pour permettre le trafic IP de l'utilisateur spécifique.
4. **Expiration et suppression de l'accès** : Après une période d'inactivité ou un timer prédéfini, la règle dynamique est supprimée, bloquant de nouveau l'accès.

Contrôle dynamique des accès sur le trafic IP avec processus d'authentification des utilisateurs (lock and key features)

- **Configuration de Lock and Key sur un routeur Cisco :**

1. Configuration de l'ACL dynamique :

```
Router(config)# ip access-list extended DYNAMIC-ACL
Router(config-ext-nacl)# deny ip any any
```

2. Activation de l'authentification (exemple avec Telnet) :

```
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# autocommand access-enable timeout 10
```

Contrôle dynamique des accès sur le trafic IP avec processus d'authentification des utilisateurs (lock and key features)

- **Configuration de Lock and Key sur un routeur Cisco :**
- **3. Ajout des utilisateurs locaux (si pas d'AAA externe) :**

Router(config)# username user1 password cisco123

4. Application de l'ACL sur une interface :

Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip access-group DYNAMIC-ACL in

Reflexive ACL (ACL Réflexive)

- Filtrage dynamique des connexions initiées **depuis l'intérieur du réseau**.
- **Suit les sessions TCP/UDP** et permet uniquement les réponses.
- Utilisé souvent dans les pare-feux de type **stateful**.

Reflexive ACL (ACL Réflexive)

- Router(config)# ip access-list extended OUTBOUND
- Router(config-ext-nacl)# permit tcp any any reflect SESSION-TCP
- Router(config-ext-nacl)# permit udp any any reflect SESSION-UDP
- Router(config)# ip access-list extended INBOUND
- Router(config-ext-nacl)# evaluate SESSION-TCP
- Router(config-ext-nacl)# evaluate SESSION-UDP
- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip access-group OUTBOUND out
- Router(config-if)# ip access-group INBOUND in

Autorise uniquement les réponses aux connexions initiées depuis l'intérieur du réseau.

Time-Based ACL (ACL Temporelle)

- Applique des règles **en fonction d'un planning horaire**.
- Très utile pour restreindre l'accès à certaines heures.

```
Router(config)# time-range WORK-HOURS
Router(config-time-range)# periodic weekdays 09:00 to 17:00

Router(config)# ip access-list extended OFFICE-ACCESS
Router(config-ext-nacl)# permit tcp any any eq 80 time-range WORK-HOURS
Router(config-ext-nacl)# deny ip any any
Router(config)# interface GigabitEthernet0/3
Router(config-if)# ip access-group OFFICE-ACCESS in
```

Autorise le trafic HTTP uniquement **de 9h à 17h** en semaine.

IPv6 ACL

- Similaire aux ACL IPv4 mais adaptées aux adresses IPv6.
- Utilisation obligatoire de **nommées ACLs**.

```
Router(config)# ipv6 access-list BLOCK-TELNET
Router(config-ipv6-acl)# deny tcp any any eq 23
Router(config-ipv6-acl)# permit ipv6 any any
Router(config)# interface GigabitEthernet0/4
Router(config-if)# ipv6 traffic-filter BLOCK-TELNET in
```

Bloque Telnet (port 23) sur IPv6.

Les lignes de commandes

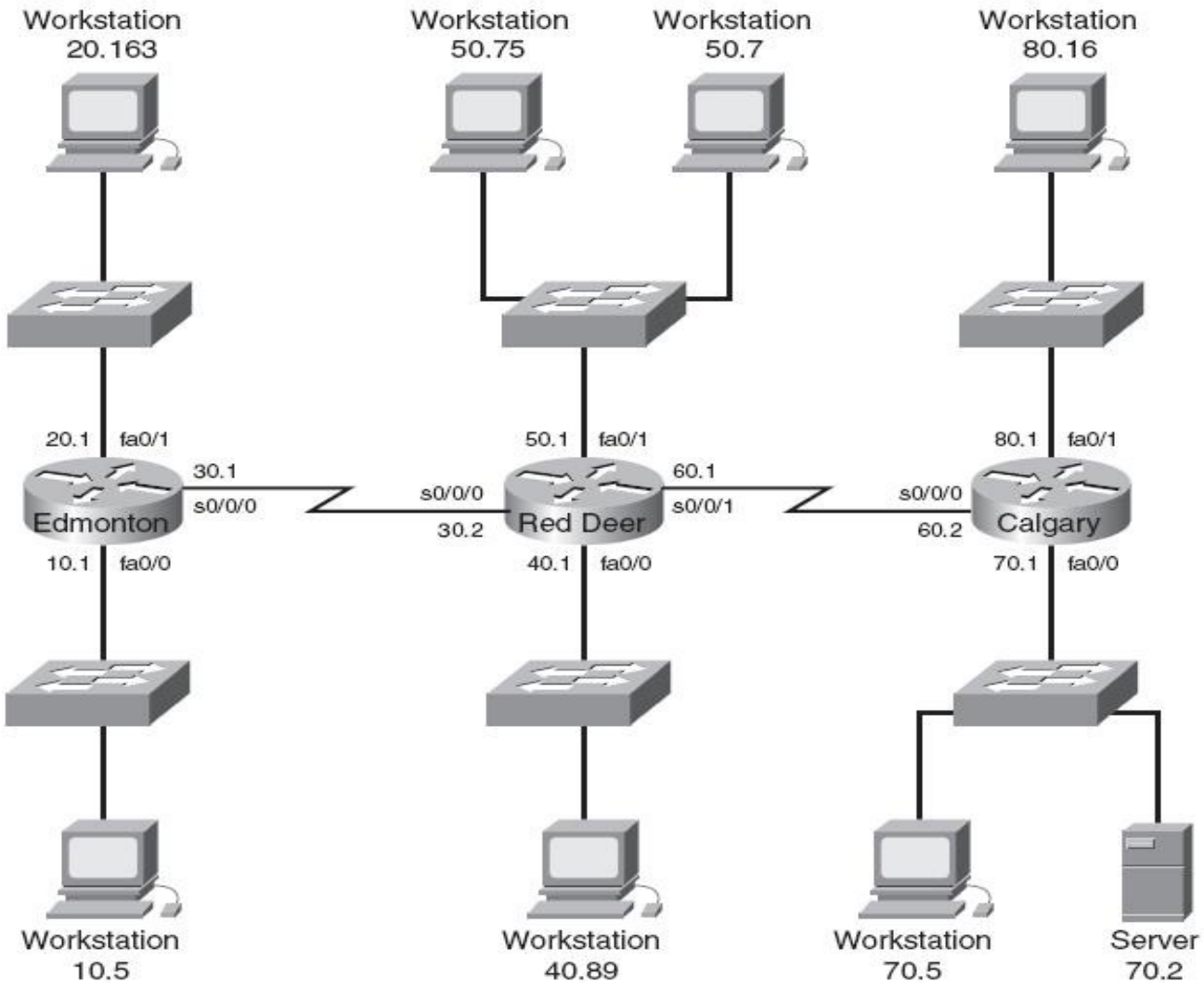
- La commande *show interface* permet de voir si une liste de contrôile d'accès est activée.
- La commande *show access-list* permettent de vérifier le contenu des listes de contrôle d'accès.

Les 6 règles des ACLs

- Une seule ACL par direction, par interface et par protocole.
- Toute ACL se termine par une exclusion globale.
- ACL IP standard (1-99) et étendue (100-199)
- Par défaut, l'ACL s'applique sur la sortie (*out*).
- Les ACLs standards sont près de la destination.
  Les ACLs étendues sont près de la source.
- Les ACLs ne s'appliquent pas aux paquets générés par les routeurs.

Les autres fonctions des ACLs

- Identification des paquets pour priorisation et contrôle des listes d'attentes ;
- Meilleur contrôle des mises à jour des tables de routage ;
- Contrôle dynamique des accès sur le trafic IP avec processus d'authentification des utilisateurs (lock and key features) ;
- Identification des paquets pour encryption ;
- Contrôle des accès Telnet au routeur ;
- Contrôle d'accès au DDR (Dial-on-Demand Routing).


Workstation
20.163
Workstation
50.75
Workstation
50.7
Workstation
80.16
20.1
fa0/1
50.1
fa0/1
80.1
fa0/1
30.1
s0/0/0
s0/0/0
30.2
60.1
s0/0/1
s0/0/0
60.2
Edmonton
Red Deer
Calgary
10.1
fa0/0
40.1
fa0/0
70.1
fa0/0
Workstation
10.5
Workstation
40.89
Workstation
70.5
Server
70.2

```
Edmonton(config)#access list 115 deny ip host
172.16.10.5 host 172.16.50.7
```

```
Edmonton(config)#access list 115 permit ip any ar
```

```
Edmonton(config)#interface fastethernet 0/0
```

```
Edmonton(config)#ip access-group 115 in
```

```
RedDeer(config)#access-list 10 deny 172.16.10.0
0.0.0.255
```

```
RedDeer(config)#access-list 10 permit any
```

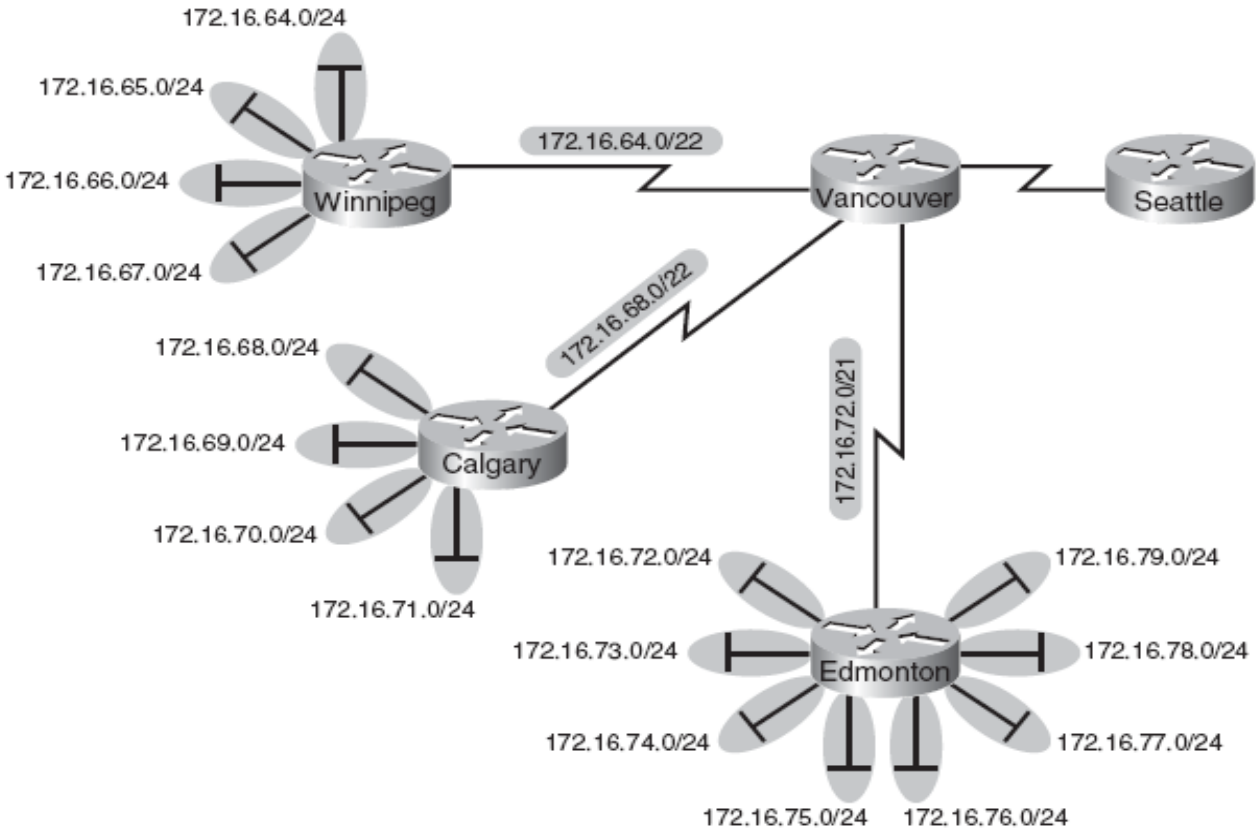
```
RedDeer(config)#interface fastethernet 0/0
```

```
RedDeer(config)#ip access-group 10 out
```

```
RedDeer(config)#access-list 20 permit host
172.16.10.5
```

```
RedDeer(config)#line vty 0 4
```

```
RedDeer(config-line)#access-class 20 in
```



Summarize/résumer

/21	/22	/23	/21
172.16.64.0	172.16.64.0	172.16.64.0	172.16.64.0
			172.16.65.0
		172.16.64.0	172.16.66.0
			172.16.67.0
	172.16.68.0	172.16.64.0	172.16.68.0
			172.16.69.0
		172.16.64.0	172.16.70.0
			172.16.71.0
172.16.72.0	172.16.72.0	172.16.64.0	172.16.72.0
			172.16.73.0
		172.16.64.0	172.16.74.0
			172.16.75.0
	172.16.76.0	172.16.64.0	172.16.76.0
			172.16.77.0
		172.16.64.0	172.16.78.0
			172.16.79.0