Sécurité avancée des réseaux

ACL

IUT d'Auxerre
Département RT
2ème année 2013-2014
ZHANG Tuo
tuo.zhang@u-bourgogne.fr

Outline

- Les principes de ACL
  - C’est quoi
  - Motivation& Rôle, comment ça marche
  - Les commandes
- Masque générique
- Les types de ACL, préciser les détails
  - Standard
  - Étendue
- Guide & Règle
- More exemples
- Conclusion

Les principes

ACL

C’est quoi le ACL?

- *Access Control List*（ACL）
  - Liste de contrôle d’accès， Conditions appliquées au trafic circulant via une interface d’un routeur
  - Indiquer au routeur les types de paquets à accepter ou à rejeter en fonction de conditions précises
  - Permet de gérer le trafic et de sécuriser l’accès d’un réseau en entrée comme en sortie

- Principe fonctionnement de ACL
  - analyser les informations de l’entête paquets de couches 3 et 4
  - faire le filtrage d’après les règles pré-défis

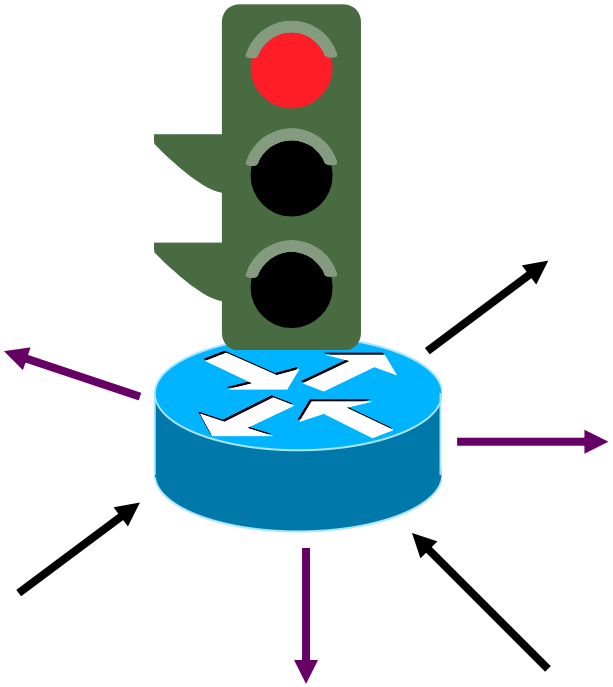
Motivation & Rôle 2-1

- Fournir un niveau de sécurité d'accès réseau de base
- Appliquer dans QoS

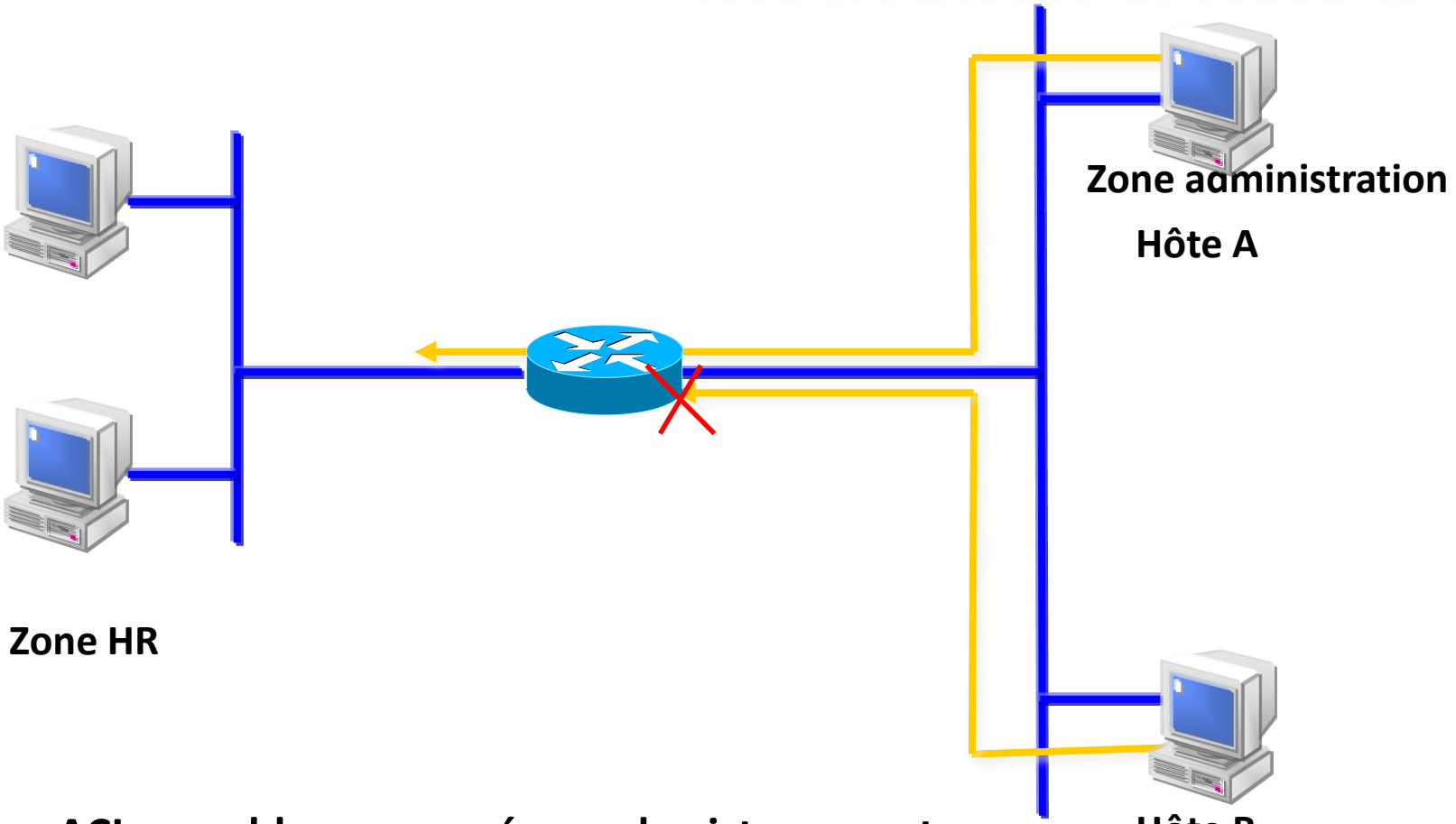
pour contrôler le flux de trafic

- Limiter le trafic réseau et

Accroître les performances

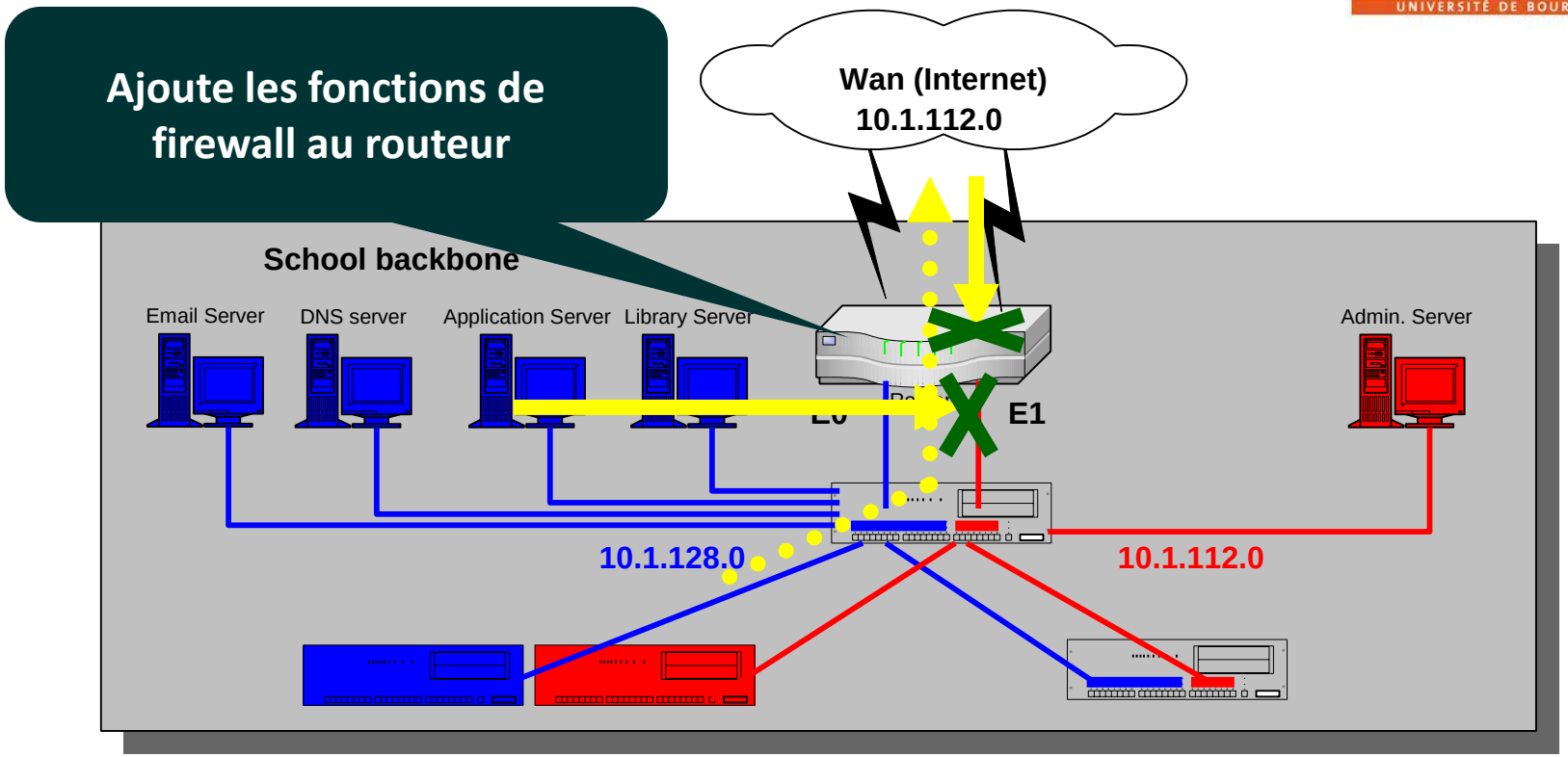


Motivation & Rôle 2-2



Appliquer ACL pour bloquer un réseau de vister un autre

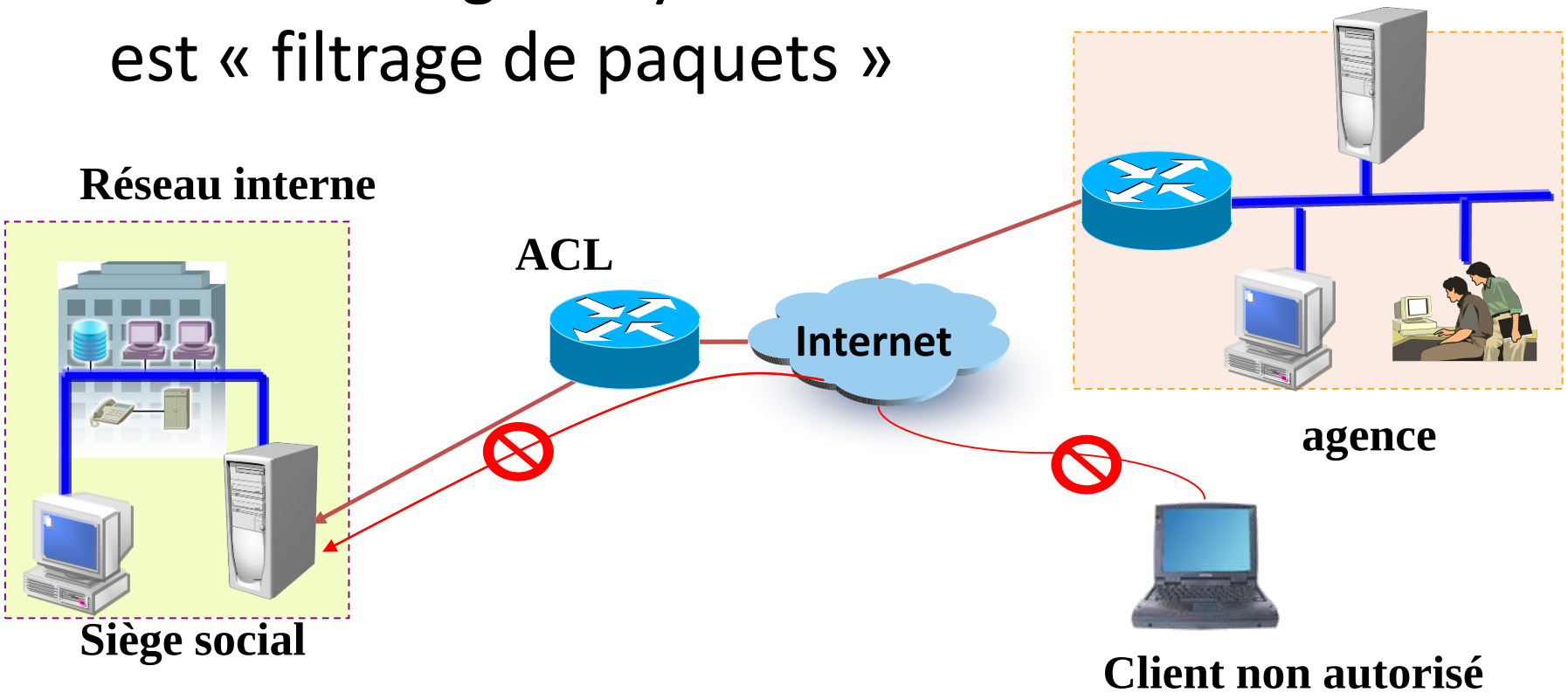
ACL - A quoi ça sert



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

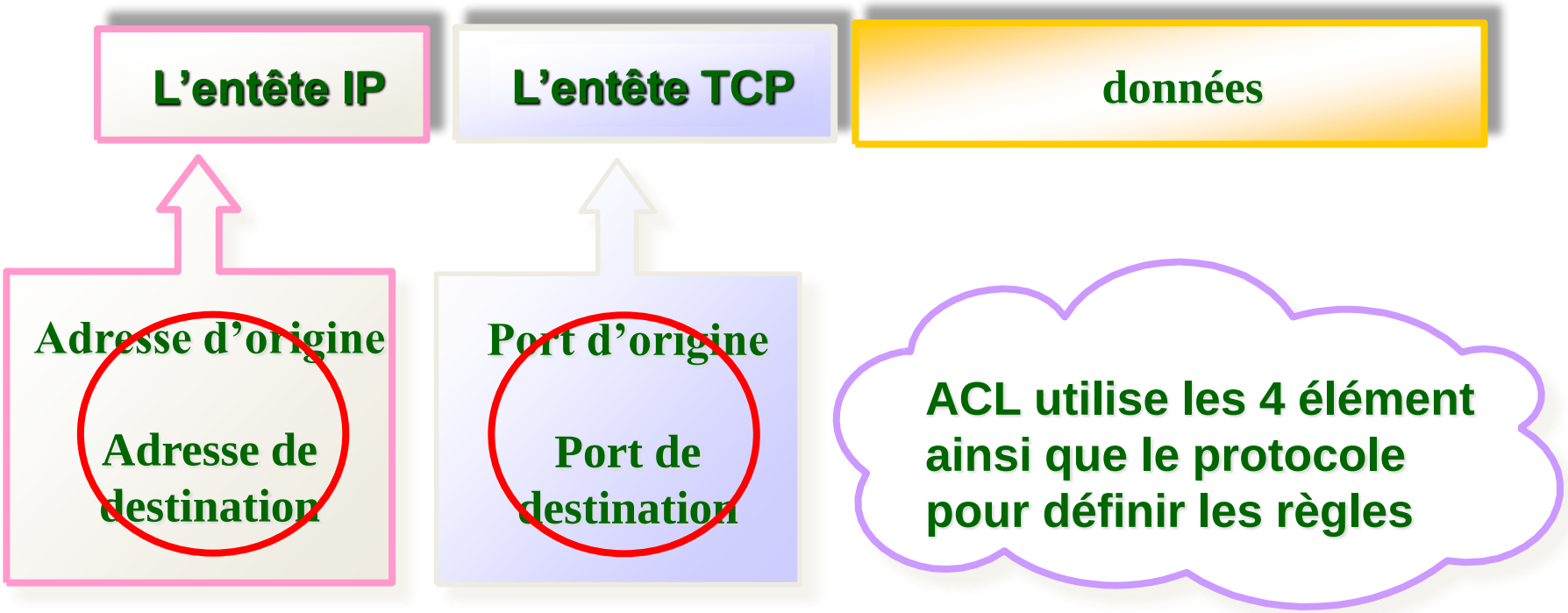
Fonctionnement 2-1

- Le technologie noyau de réalisation ACL est « filtrage de paquets »



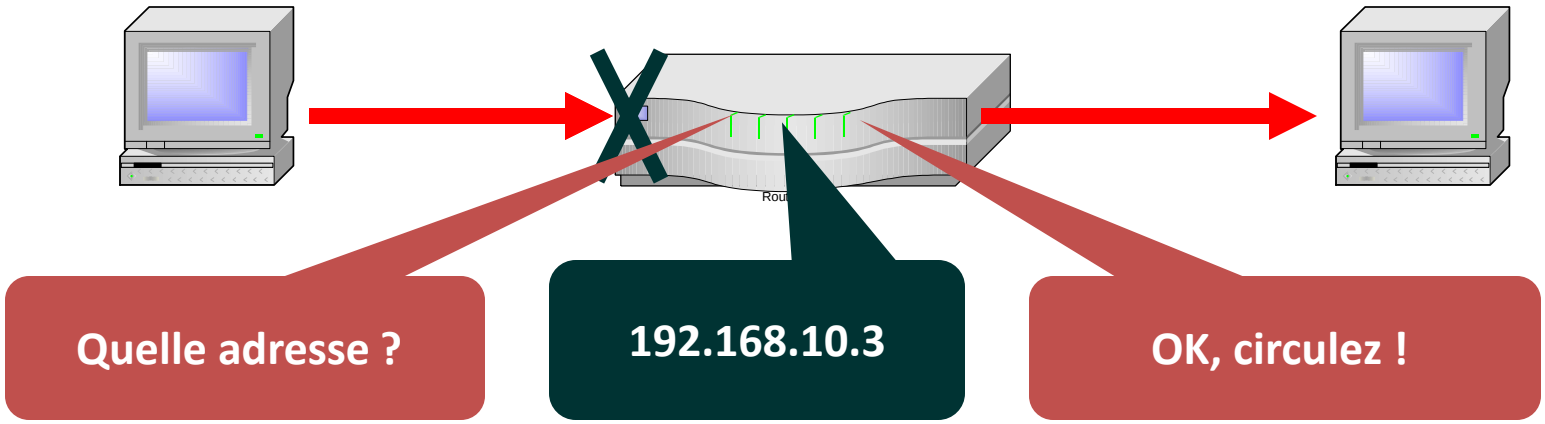
Fonctionnement 2-2

- Le routeur examine chaque paquet afin de déterminer s'il doit l'acheminer ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès.
- Certaines conditions dans une ACL sont des adresses source et de destination, des protocoles et des numéros de port de couche supérieure.



ACL - Comment ça marche 2-1

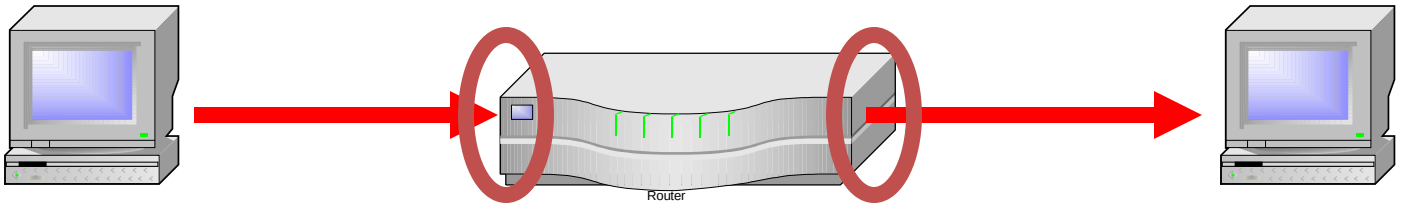
- Filtre les paquets en utilisant des éléments des couches 3 (adresses IP) et 4 (numéros de port des applications) de TCP-IP ;
- Par défaut, une liste de contrôle non paramétrée refuse tous les accès.



- 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 2-2

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

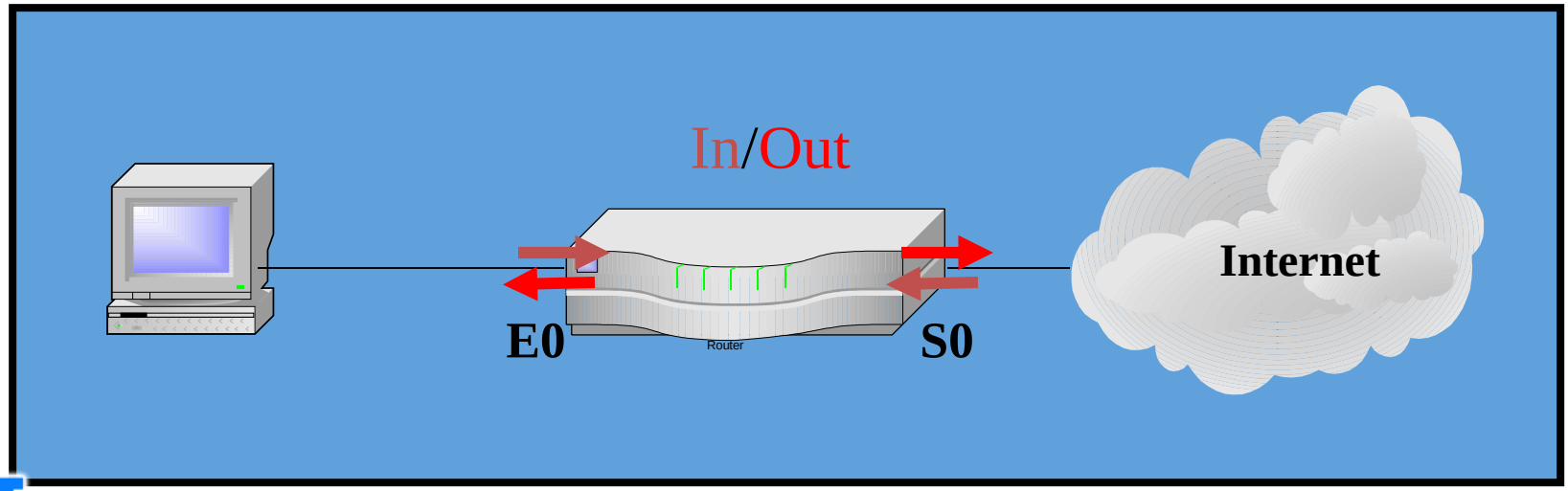


- Grâce aux *masques génériques (wildcard mask)*, le contrôle peut s'appliquer à un réseau, un sous-réseau, un hôte ou une catégorie d'hôtes.
- Ne contrôle pas les paquets émis par le routeur lui-même.

Les paramètres *In* et *Out*

(Inbound-Outbound)

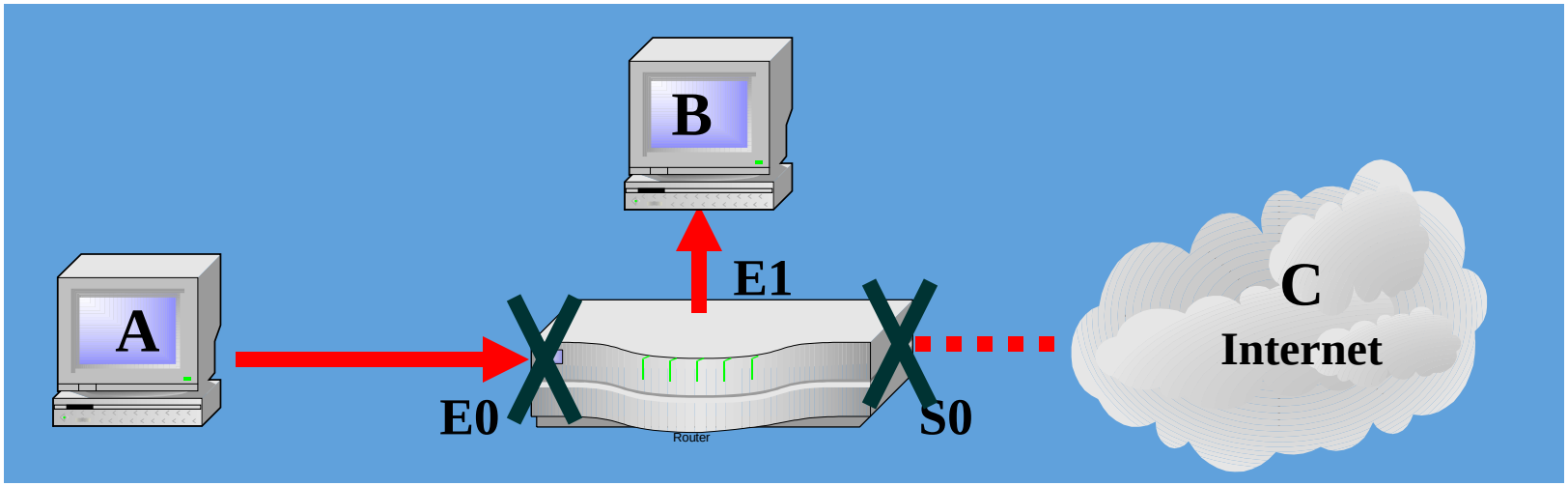
- Par défaut, ce paramètre est configuré sur *out (vers le réseau)*
- Le paramètre *In* (vers le routeur) ou *Out* se place sur l'interface à laquelle on veut appliquer la liste d'accès



Quel port choisir

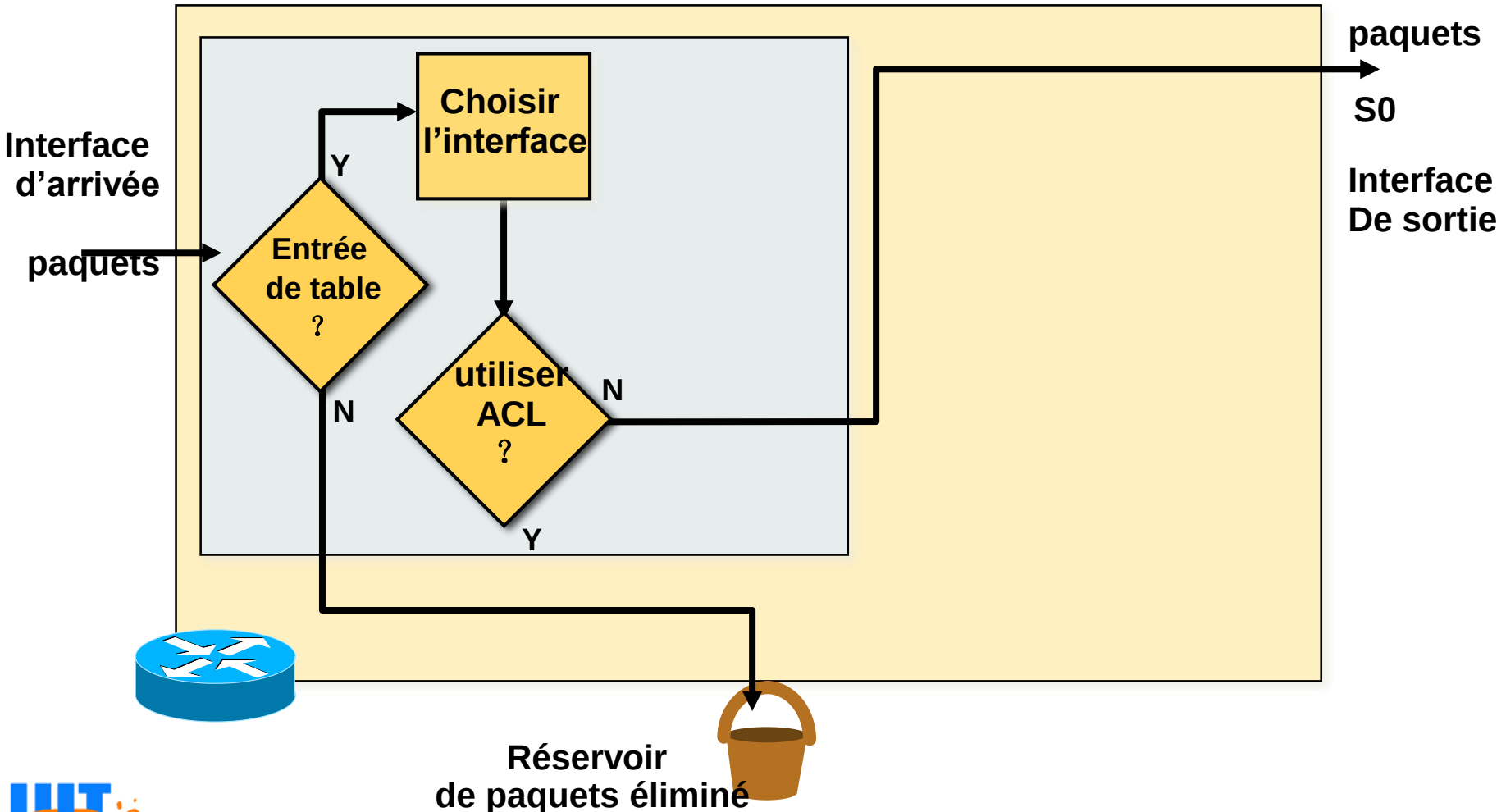
Deux solutions pour bloquer A vers B

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

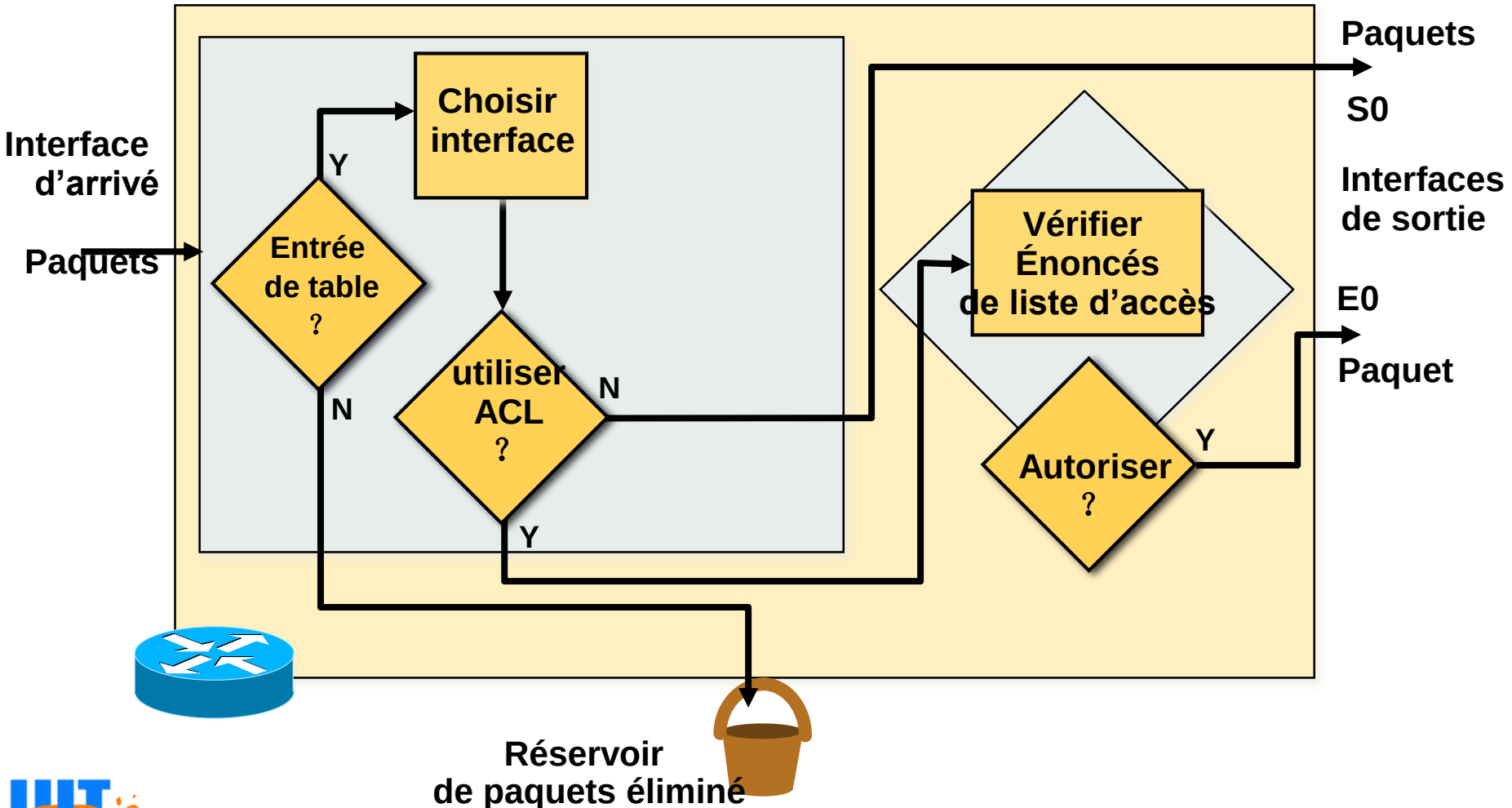


- ACL 1 Deny A
- Attribut ACL 1 à l'interface E1 **out**

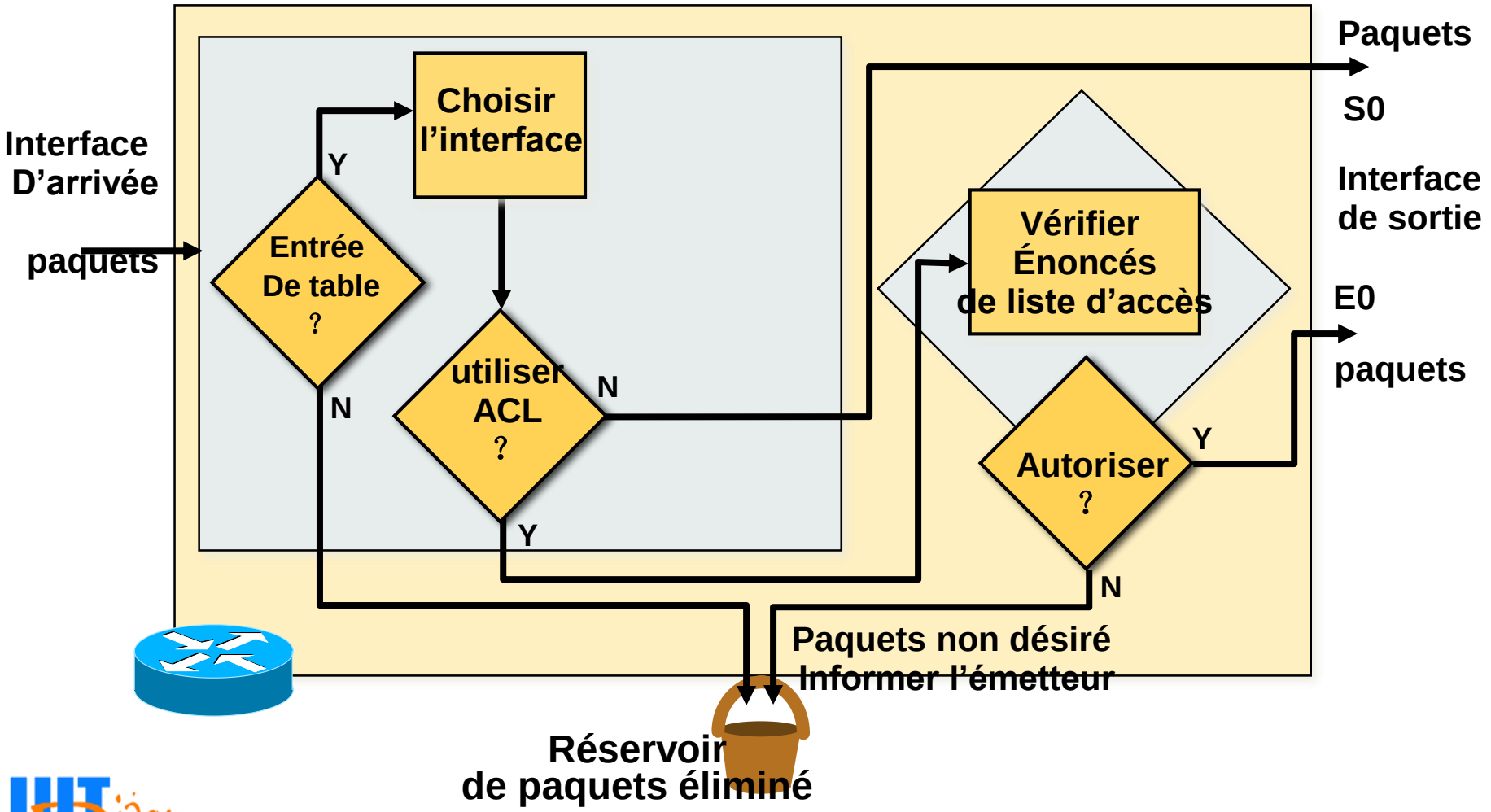
Les processus de contrôle *In* et *Out* (1)



Les processus de contrôle *In* et *Out* (2)

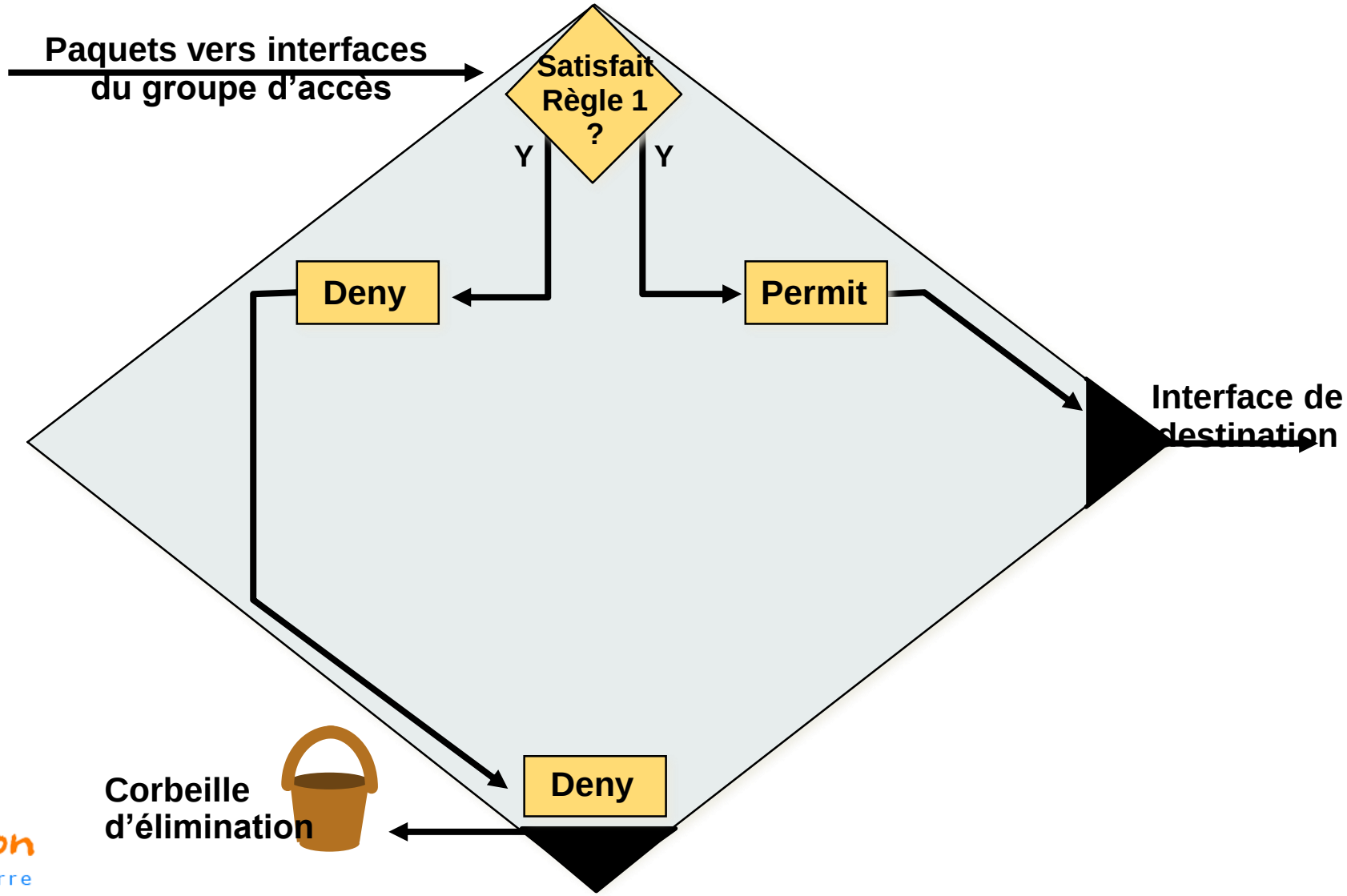


Les processus contrôle de *In* et *Out* (3)

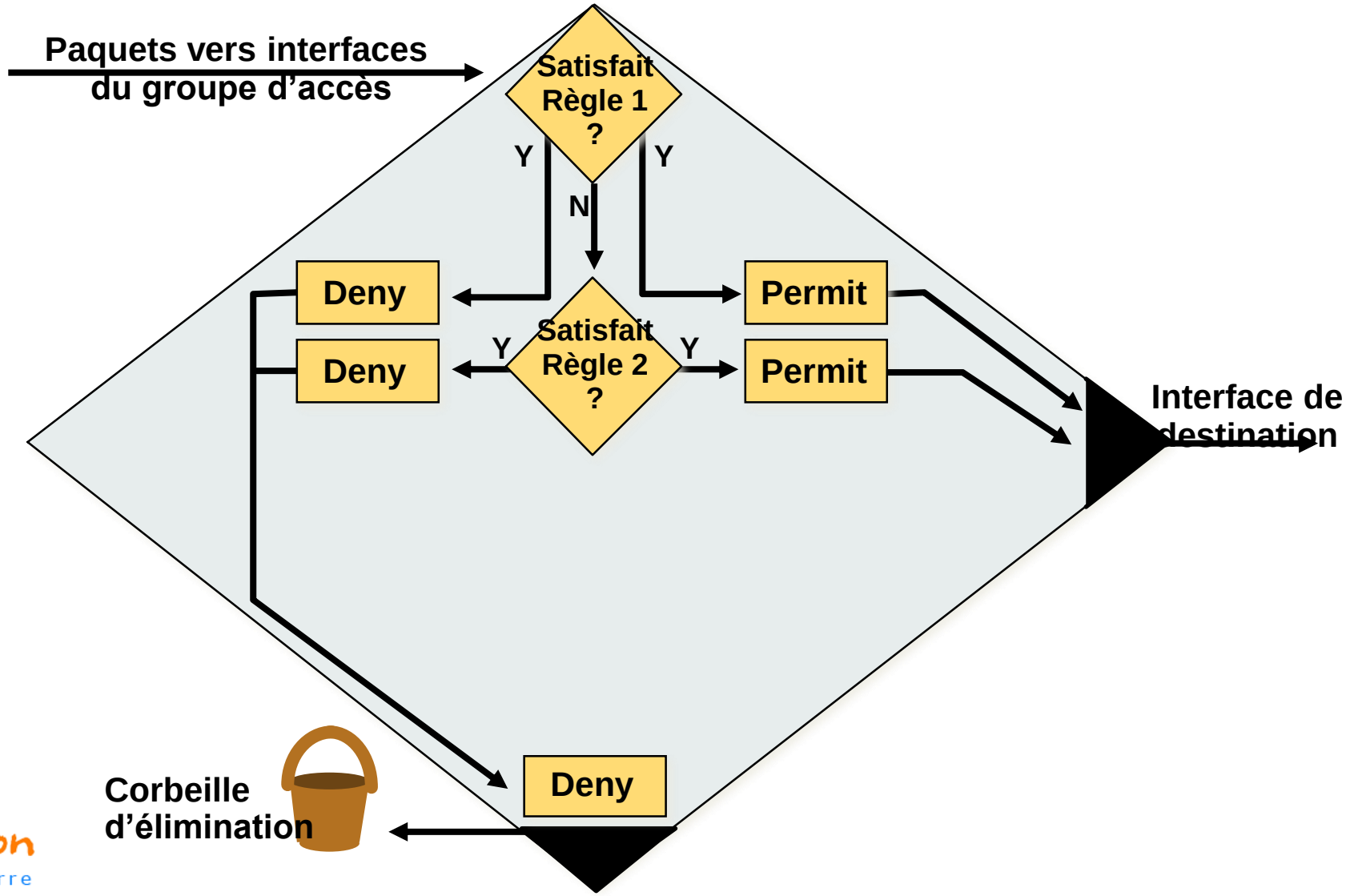


Si il y a aucun matching sur vérifier énoncés de liste d'accès，on rejete le paquet

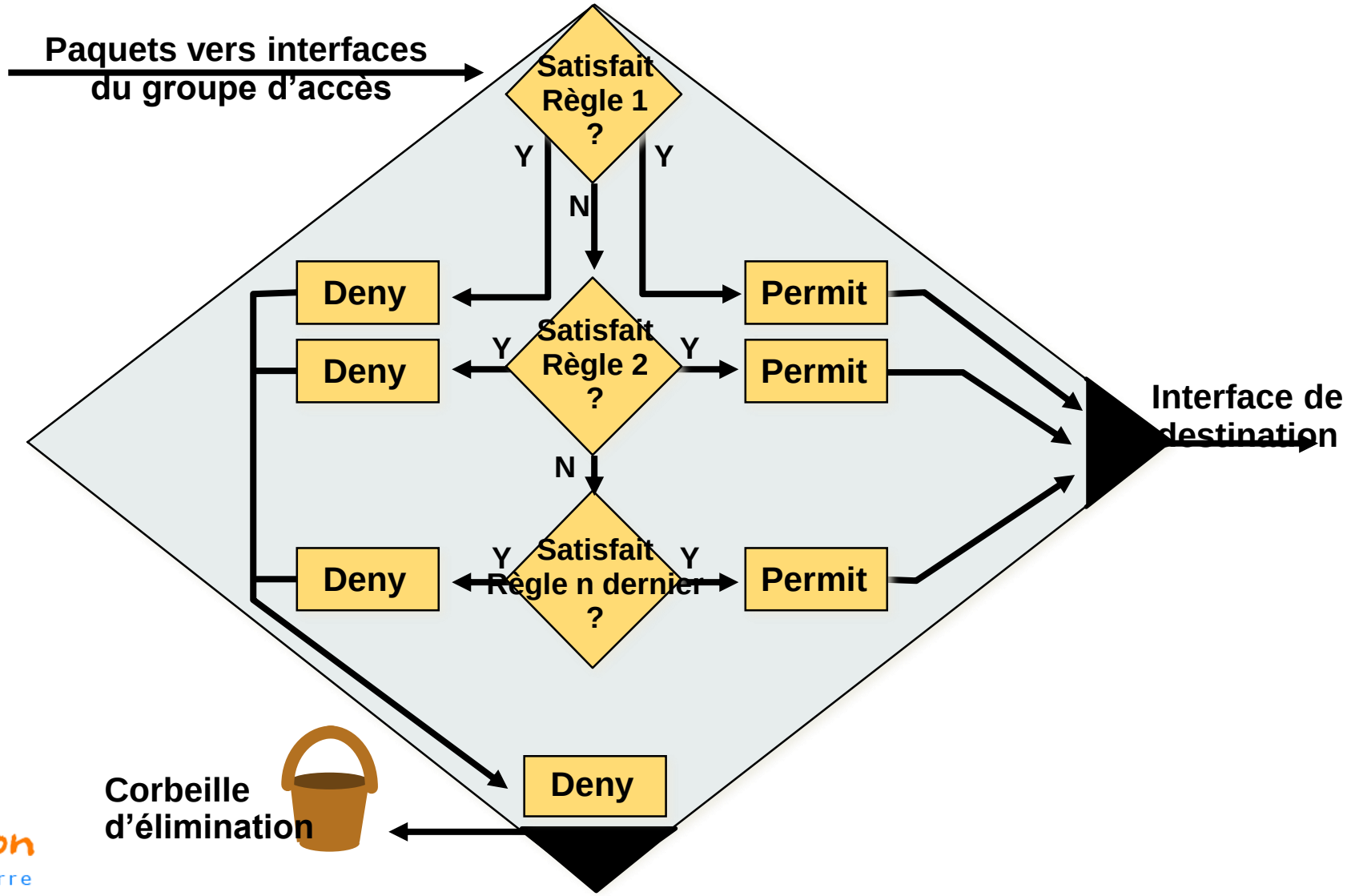
Les processus de vérifier énoncé de AC (1)



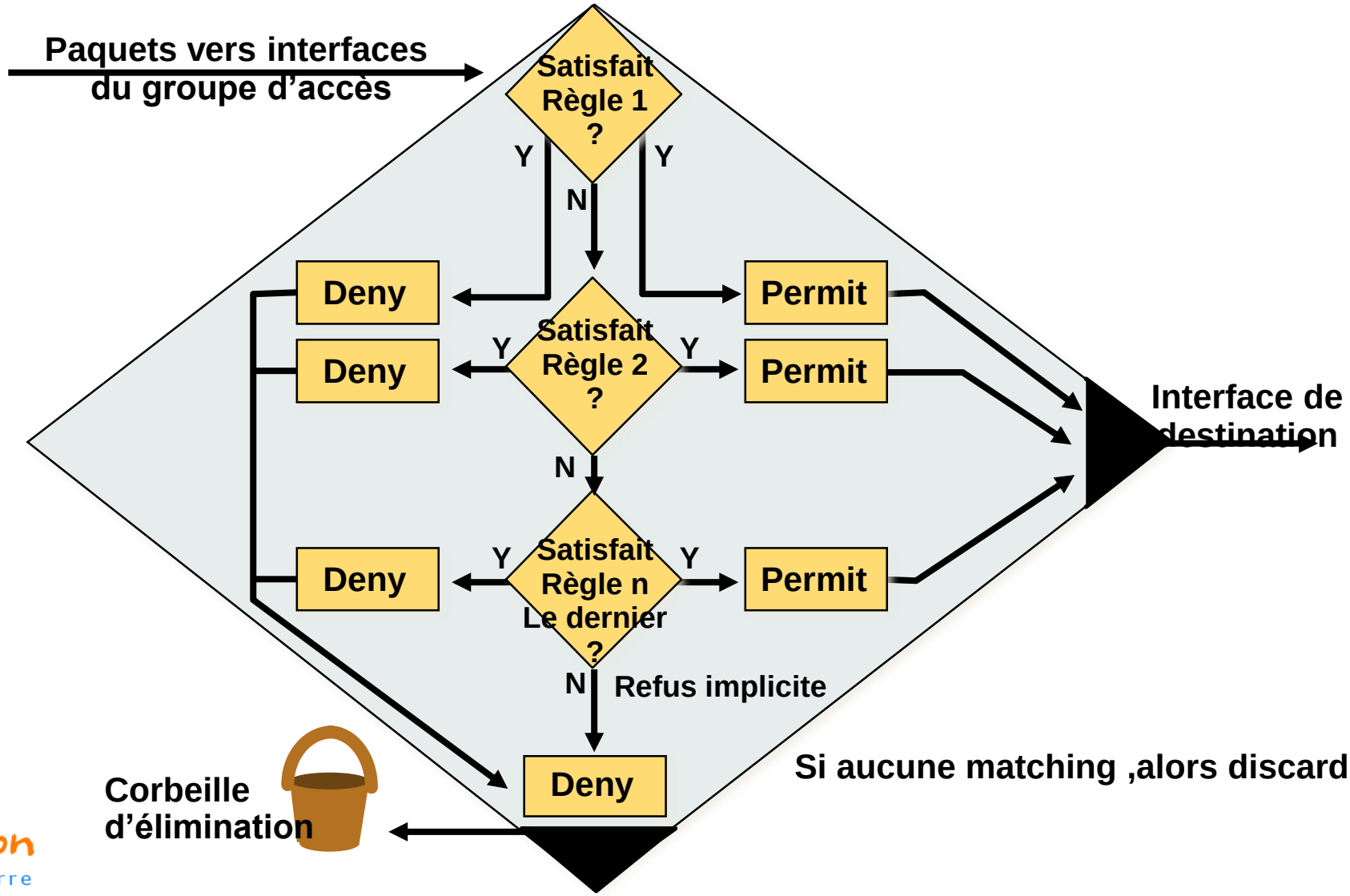
Les processus de vérifier énoncé de ACL(4-2)



Les processus de vérifier énoncé de ACL(4-3)



Les processus de vérifier énoncé de ACL(4-4)



Algorithme de processus

- Algorithme
  - Le routeur teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin.
  - Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées.
  - Si une instruction de condition autorisant l'accès à tout le trafic est située en haut de la liste, aucune instruction ajoutée en dessous ne sera vérifiée.
  - Si aucune des instructions ne correspond au paquet, une instruction implicite **`deny any`** est placée à la fin de la liste par défaut.

Commande in et out de ACL

- On utilise ip access-group pour appliquer ACL dans une certaine interface(créer ACL)

```
Router(config)#
 access-list access-list-number { permit | deny } { test conditions }
```

- Une direction de l'interface, on peut utiliser q'une seul access-list(binding ACL à interface)

```
Router(config-if)#
 { protocol } access-group access-list-number {in | out}
```

Commande Deny et permit

Router(config)#access-list *access-list-number* **{permit|deny} {test conditions}**

permet les paquets de passer l'interface qui utilisent ACL

Refuser les paquets

Exemple ACL

- Premier démarche， créer ACL

```
Router(config)#access-list 1 deny   172.16.4.13  0.0.0.0
Router(config)#access-list 1 permit  172.16.0.0  0.0.255.255
Router(config)#access-list 1 permit  0.0.0.0  255.255.255.255
```

- Deuxième démarche ， appliquer la direction out de l’interface e0

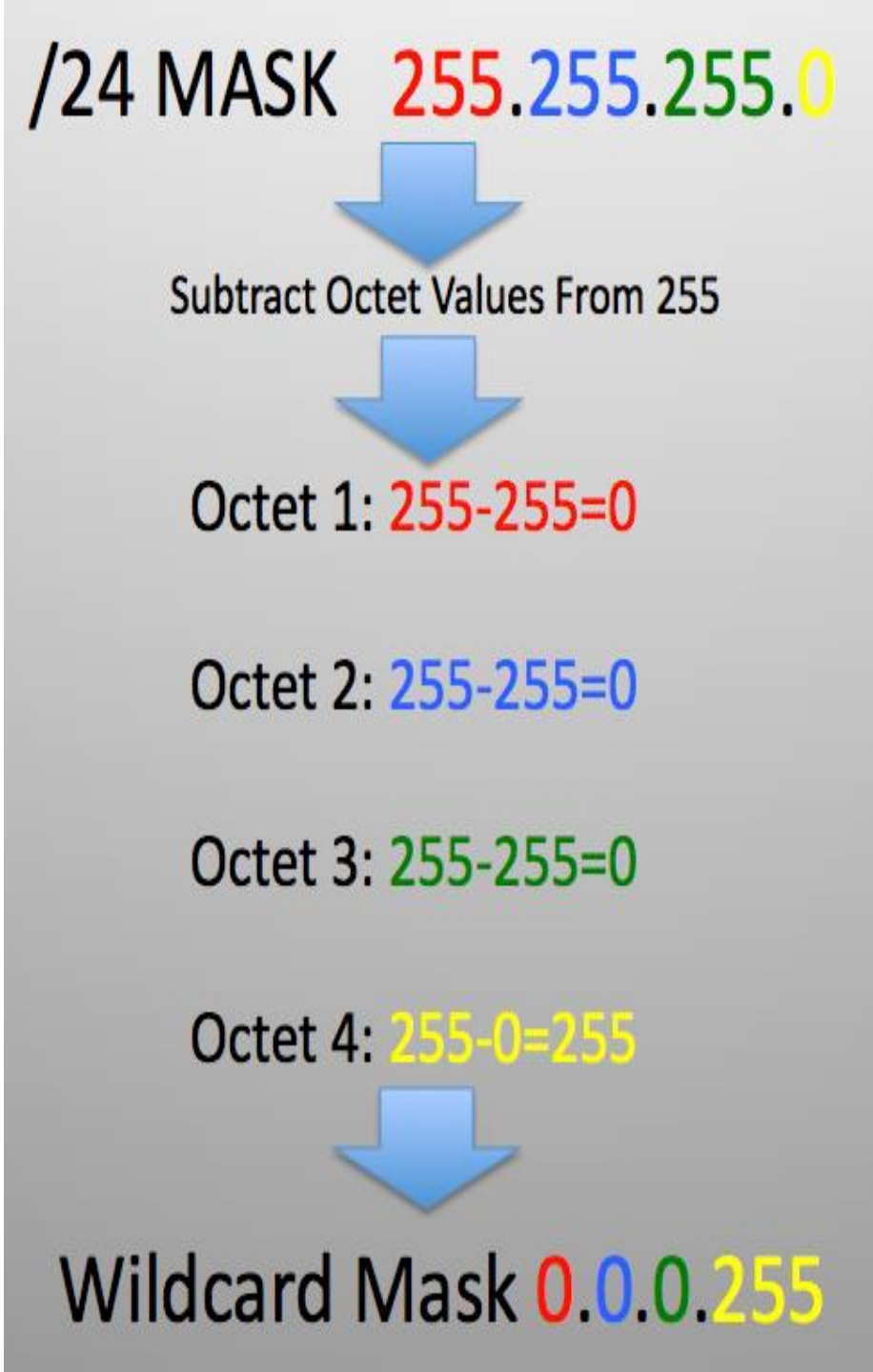
```
Router(config)#interface  fastethernet 0/0
Router ( config-if ) #ip access-group 1  out
```

A wildcard mask is a mask of bits that indicate which parts of an @IP are available for examination.
In Cisco, it is used to:

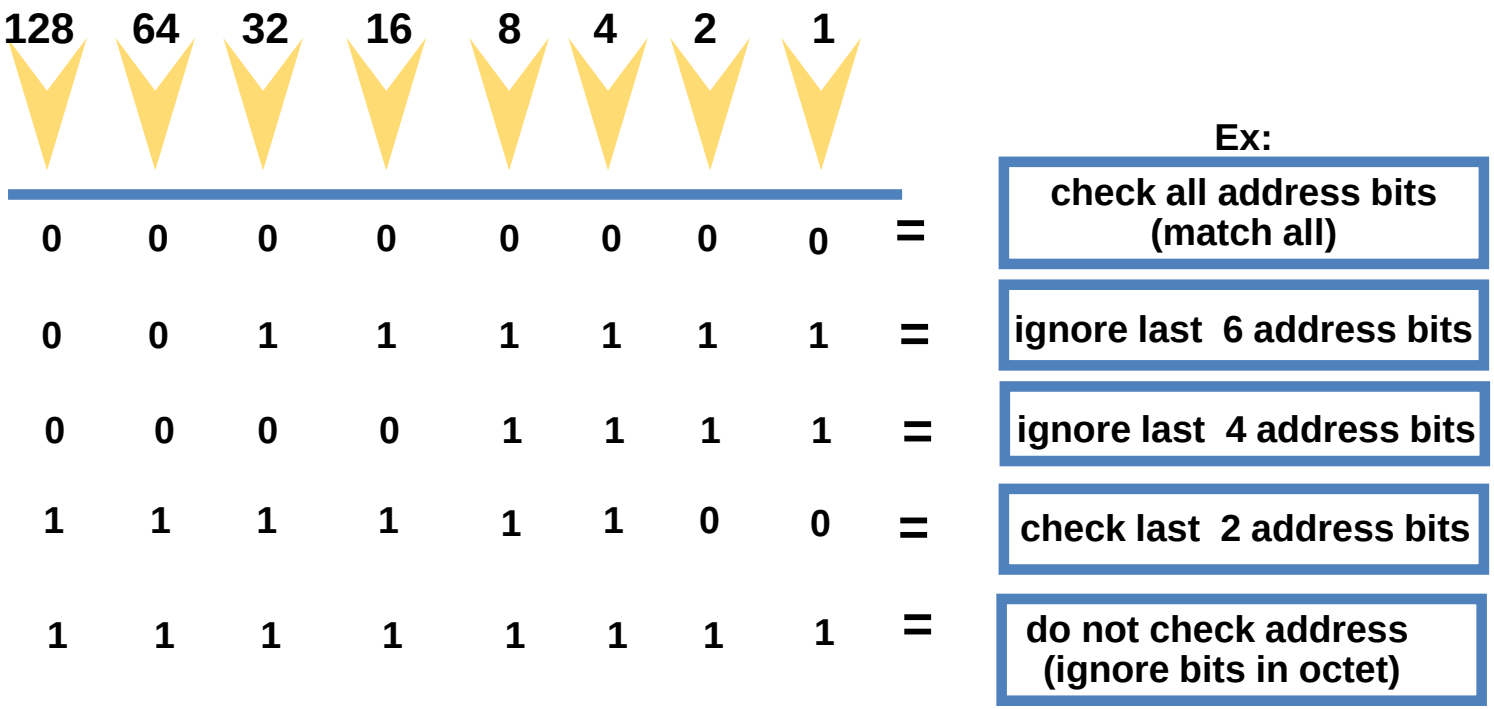
- To indicate the size of a network or subnet for some routing protocols, such as OSPF.
- To indicate what IP addresses should be permitted or denied in access control lists (ACLs).

Les masques génériques

WILDCARD MASKS



Les masques génériques (Wildcard Masks)



0 signifient que le nombre doit être pris en compte(match).

1 Indiquent que le nombre doit être ignoré.

Les masques génériques

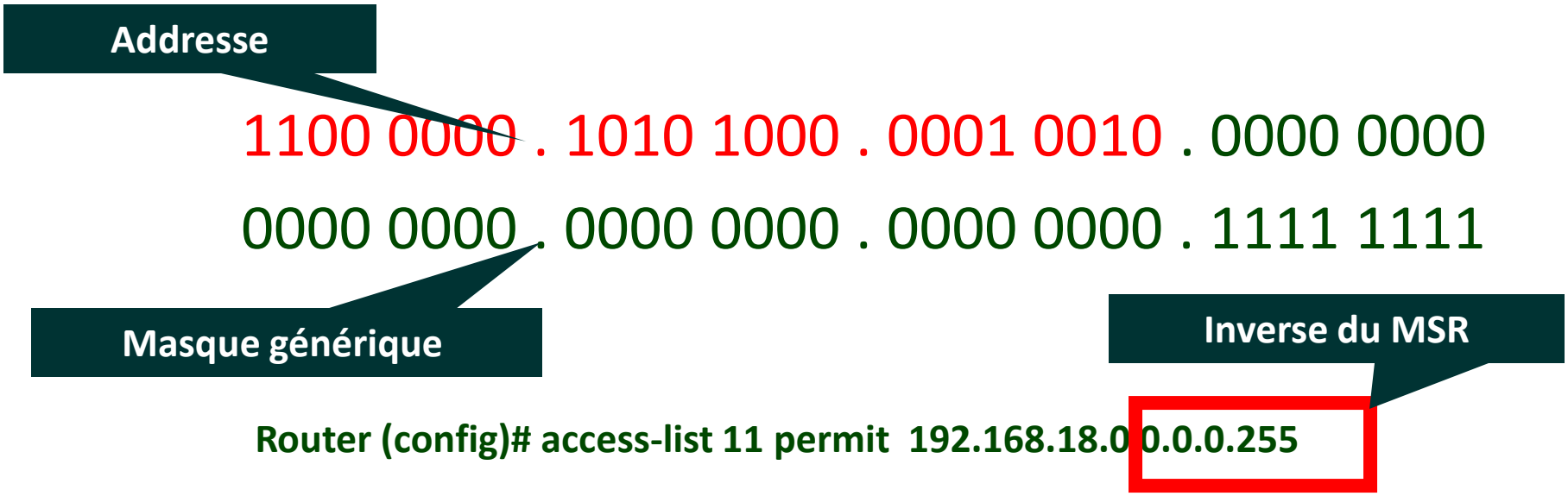
(Wildcard Masks)

- 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**

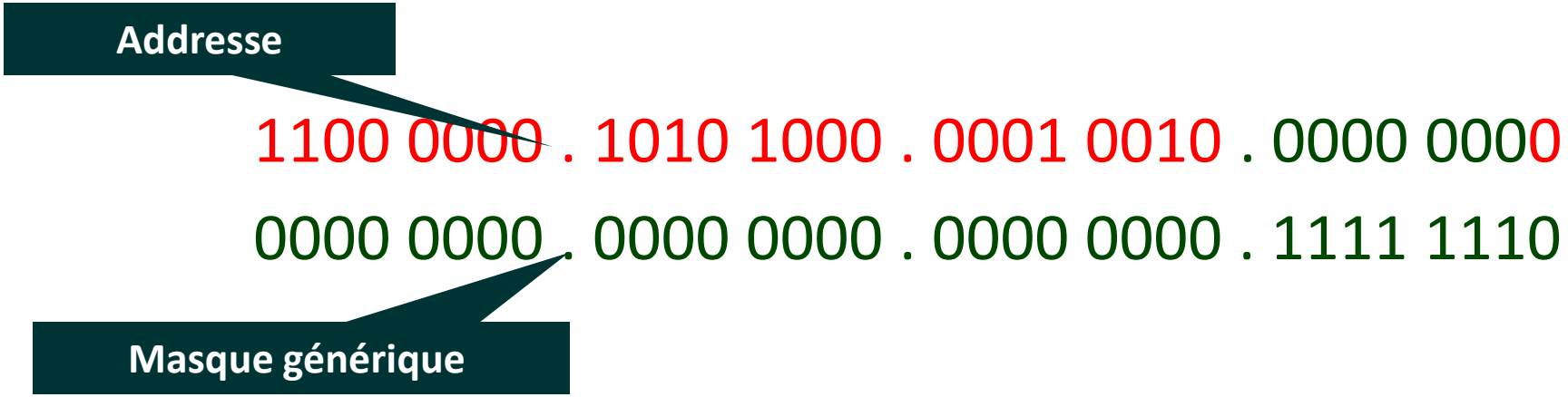
- Le masque générique indique que l'accès est refusé à tous les postes du réseau **192.168.18.0.**

Les masques génériques (ex 3-1)



- 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.

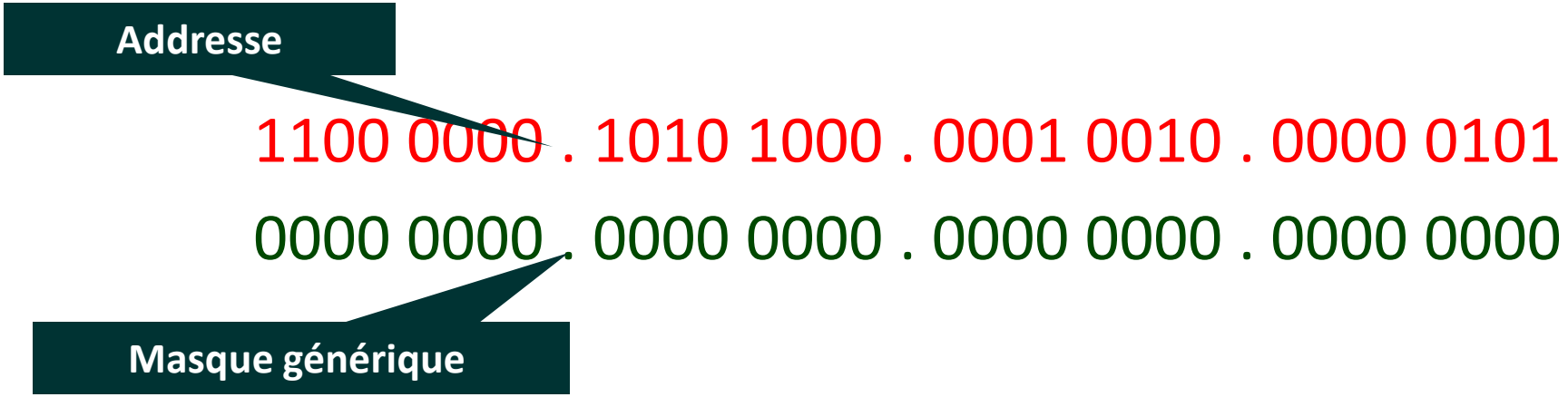
Les masques génériques (ex 3-2)



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.

Les masques génériques (ex 3-3)



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 –Keyword ‘any’

- ‘any’ peut remplacer 0.0.0.0 255.255.255.255

Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

||

Router(config)#access-list 1 permit any

Les masques génériques -Keyword ‘host’

- ‘host’ signifie qu’il faut *match all* bits de@IP

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

||

Router(config)#access-list 1 permit host 172.30.16.29

Les masques génériques keyword

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)

Bilan-Masque générique

- Masque générique
  - Les masques génériques utilisent les uns et les zéros binaires pour filtrer des adresses IP individuelles ou de groupes pour autoriser ou refuser un accès à des ressources à l'aide d'une adresse IP précise.
  - Un masque générique est une quantité de 32 bits divisés en quatre octets.
  - Un masque générique est jumelé à une adresse IP.
  - Le masque générique agit typiquement "à l'inverse" du masque sous-réseaux.
  - Exemples

Adresse IP	***masque générique***	=	***filtre***
172.16.0.0	0.0.255.255	=	172.16.x.x
192.168.10.0	0.0.0.255	=	192.168.10.x
0.0.0.0	255.255.255.255	=	x.x.x.x **(any)**
172.16.10.15	0.0.0.0	=	172.16.10.15 (hôte)

Les types de ACL

- ACL de types basiques
  - ACL standard
  - ACL étendue
- Les autre types de ACL
  - ACL basé sur address MAC
  - ACL basé sur le temps

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).

- Il existe différents types de listes de contrôle d'accès :
  - IP standard
  - IP étendues
  - IPX
  - AppleTalk

- Numéro d'identification
  - Chaque ACL est identifiée par un numéro unique (Cisco)

ACL standard ou étendue

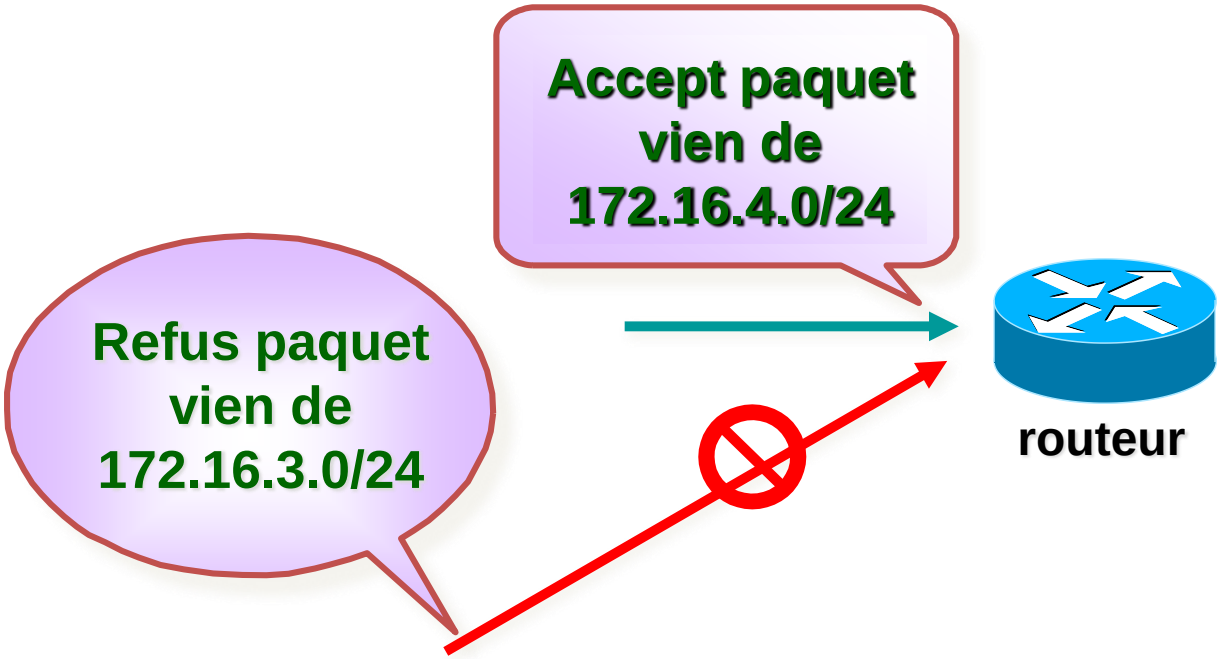
ACL type		Numéro d'identification
IP	Standard Extended Named	1-99 100-199, 1300-1999, 2000-2699 Name (Cisco IOS 11.2 and later)
IPX	Standard Extended SAP filters Named	800-899 900-999 1000-1099 Name (Cisco IOS 11.2. F and later)

ACL

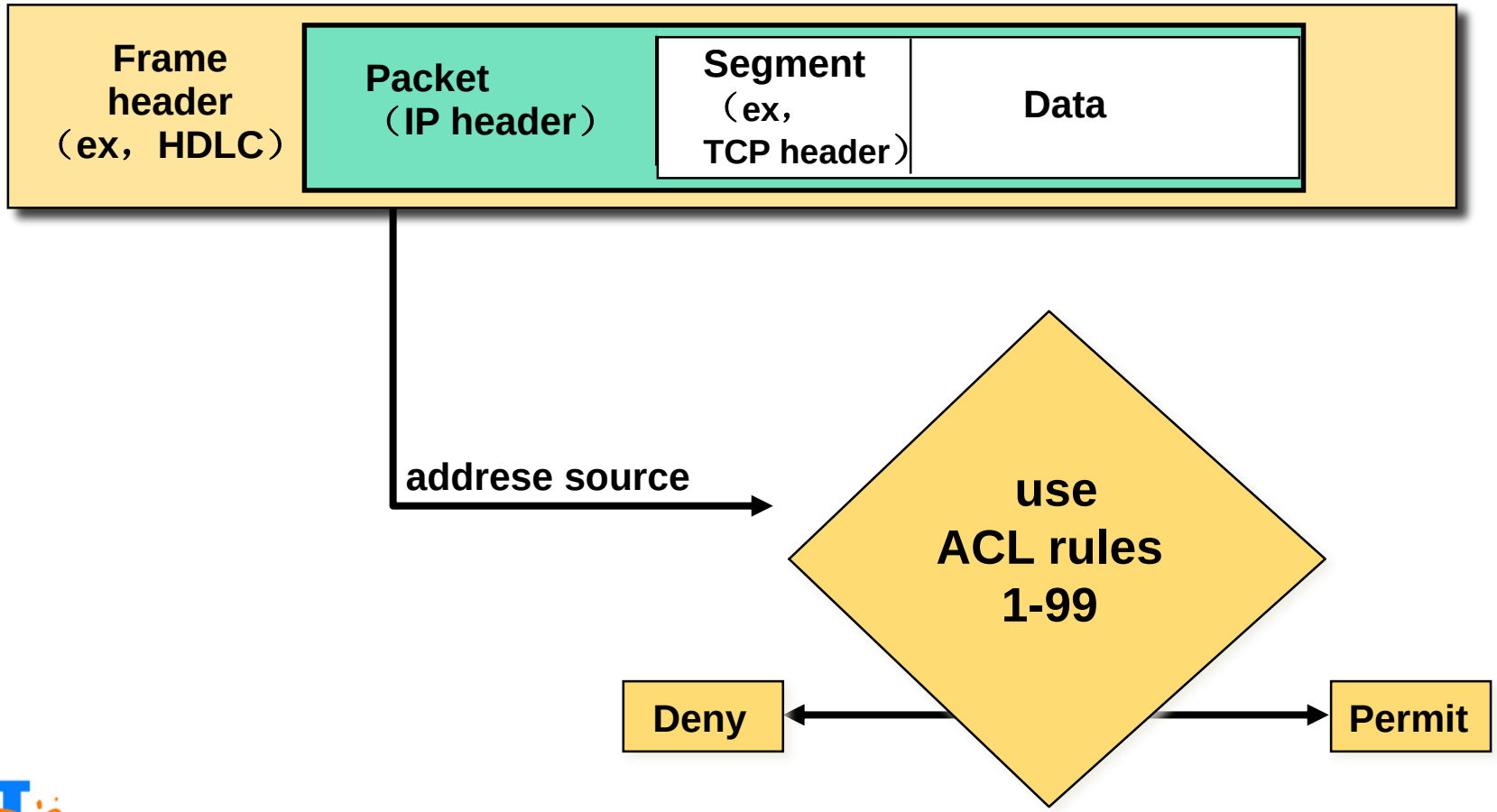
STANDARD

ACL standard 2-1

- Filtrage à partir de l'adresse source uniquement



ACL standard 2-2



Configuration standard ACL

- 1° , créer ACL en utilisant commande 'access-list'

Router(config)#access-list *access-list-number*
{ permit | deny } source [source- wildcard] [log]

- **2° , binding ACL à une interface en utilisant 'ip access-group'**

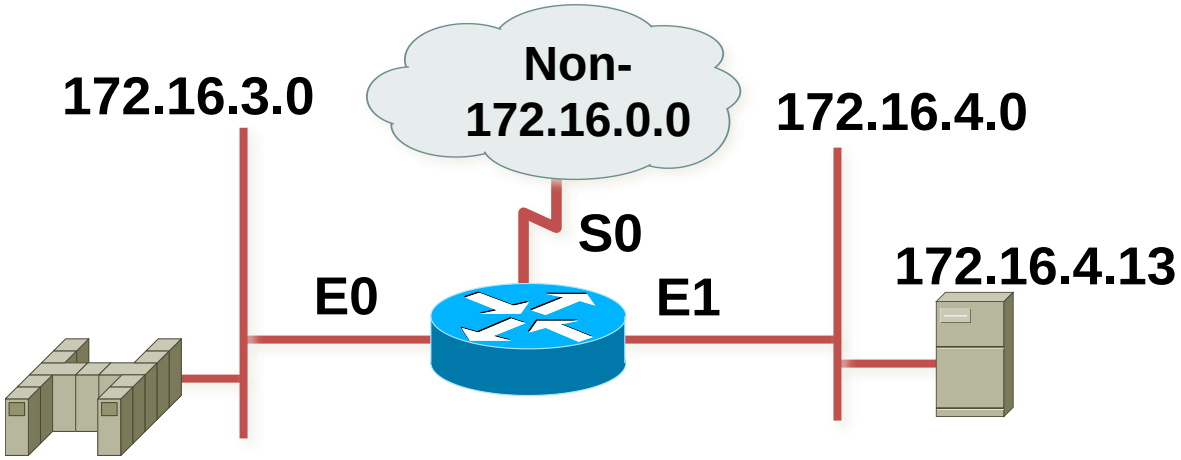
Router(config-if)#ip access-group *access-list-number* **{ in | out }**

Les paramètres de standard ACL

- Syntaxe Cisco IOS
  - `Router(config)# access-list access-list-number {deny | permit | remark} source [source-wildcard] [log]`

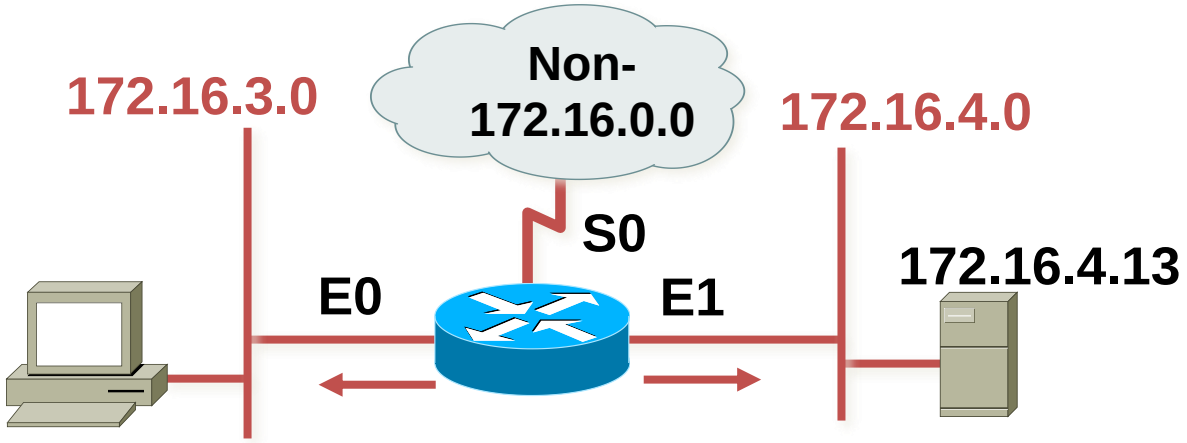
- Description des paramètres:
  - ✓ *access-list-number* : numéro de l'ACL
  - ✓ **deny** : refuse l'accès si la condition est respectée
  - ✓ **permit** : autorise l'accès si la condition est respectée
  - ✓ **remark** : Ajoute une remarque à propos des instructions ACL pour plus de lisibilité
  - ✓ *source* : Adresse IP du réseau ou de l'hôte source *source-wildcard* : Masque générique
  - ✓ **log** : provoque un message de journalisation informatif

Standard ACL exemple1




```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

Standard ACL exemple1

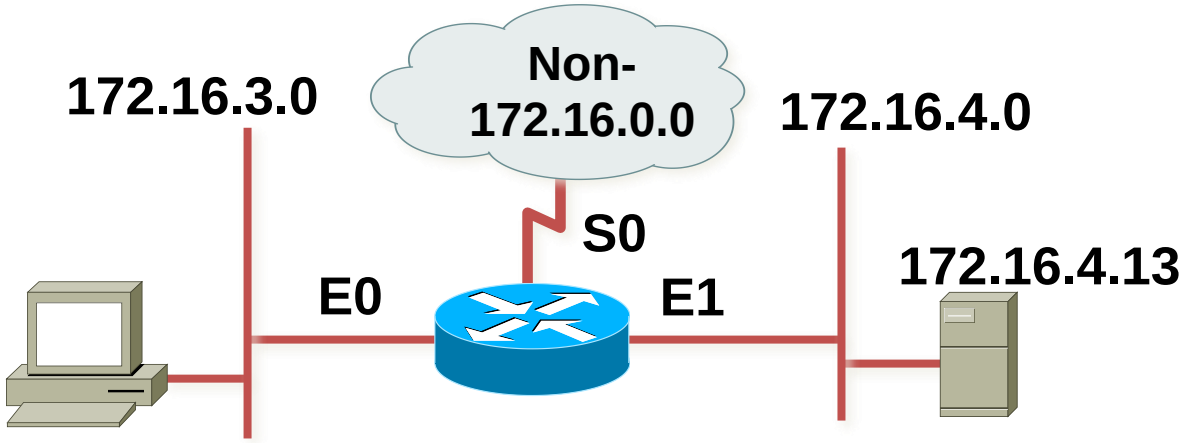



```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

Permet que les réseau 3.0 et 4.0

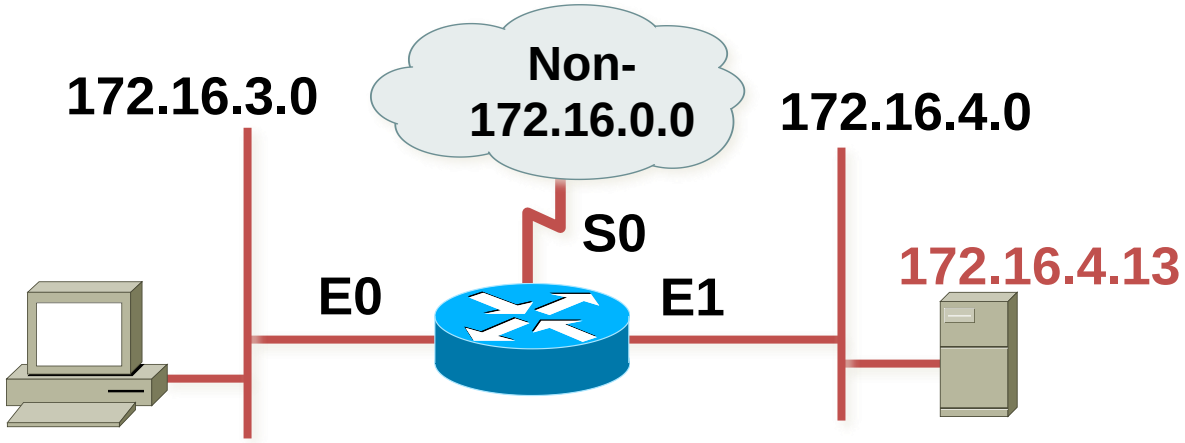
Standard ACL exemple2




```
access-list 1 deny 172.16.4.13 0.0.0.0
```

refus un hôte spécifique

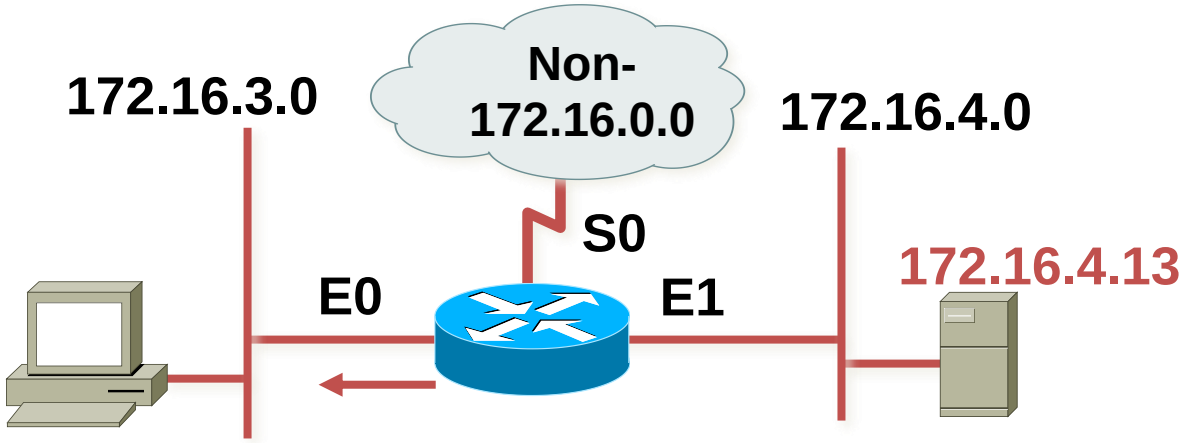
Standard ACL exemple2




```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

refus un hôte spécifique

Standard ACL exemple2

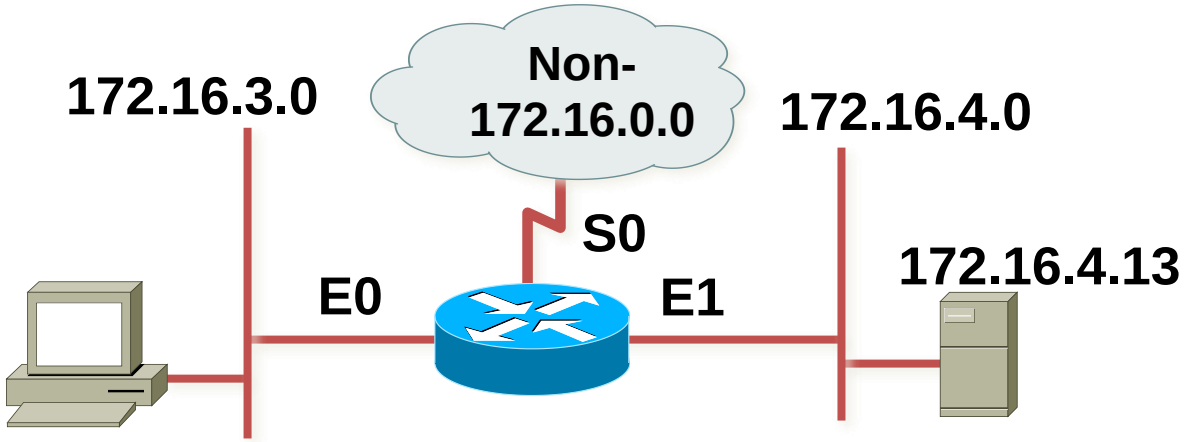



```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

refus un hôte spécifique

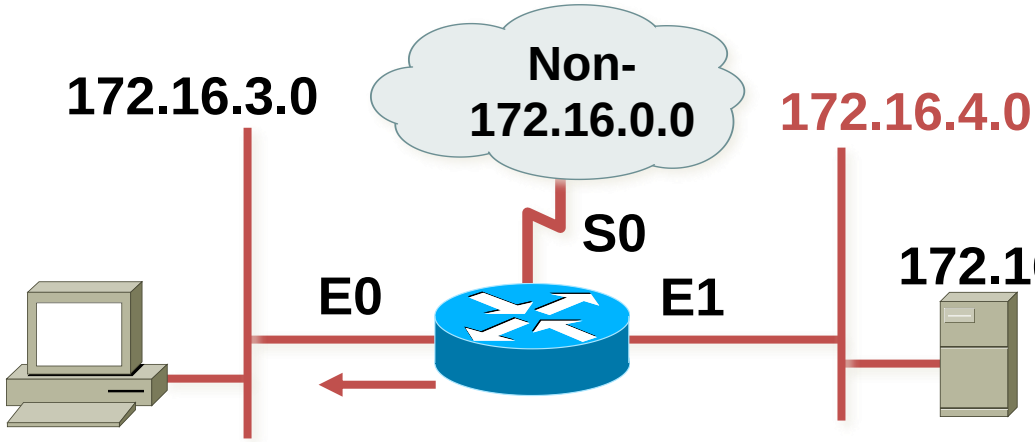
Standard ACL exemple2




```
access-list 1 deny 172.16.4.0  0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
```

refus un réseau spécifique

Standard ACL exemple2




```
access-list 1 deny 172.16.4.0   0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

refus un réseau spécifique

ACL

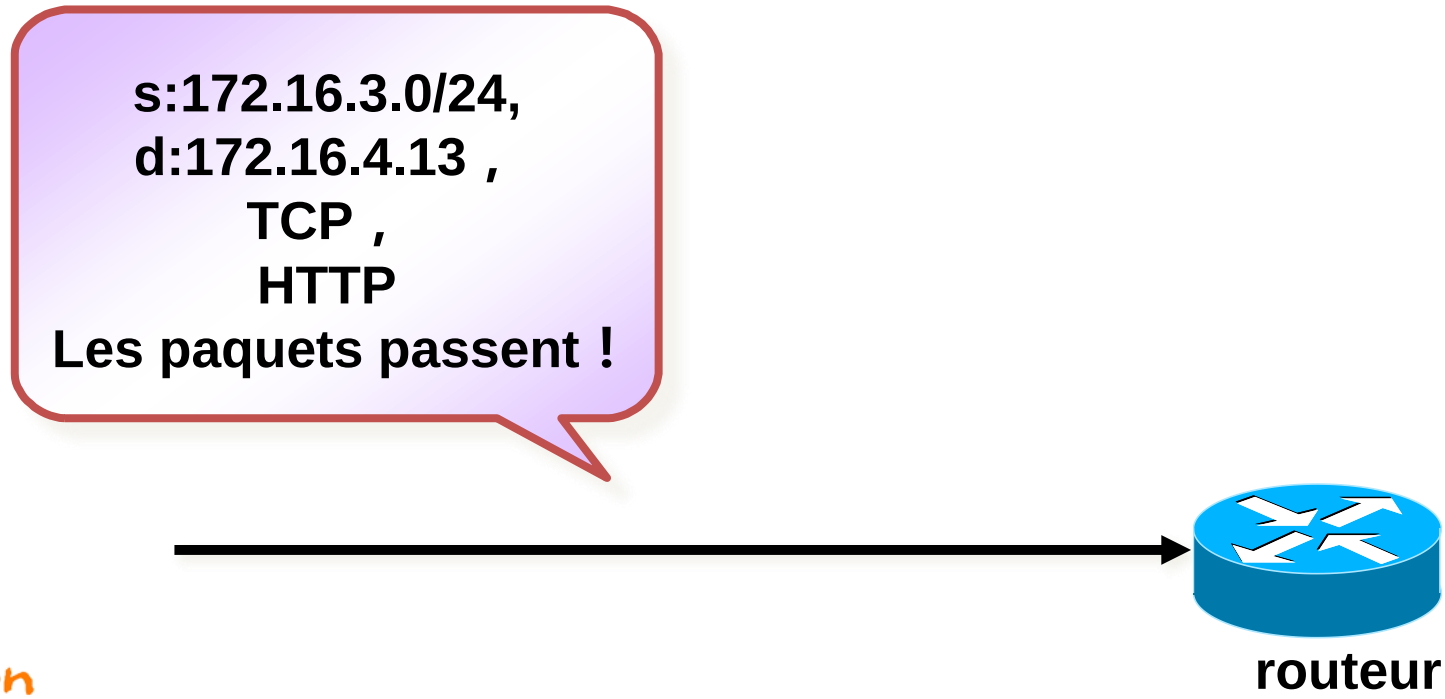
ETENDUE

ACL étendue

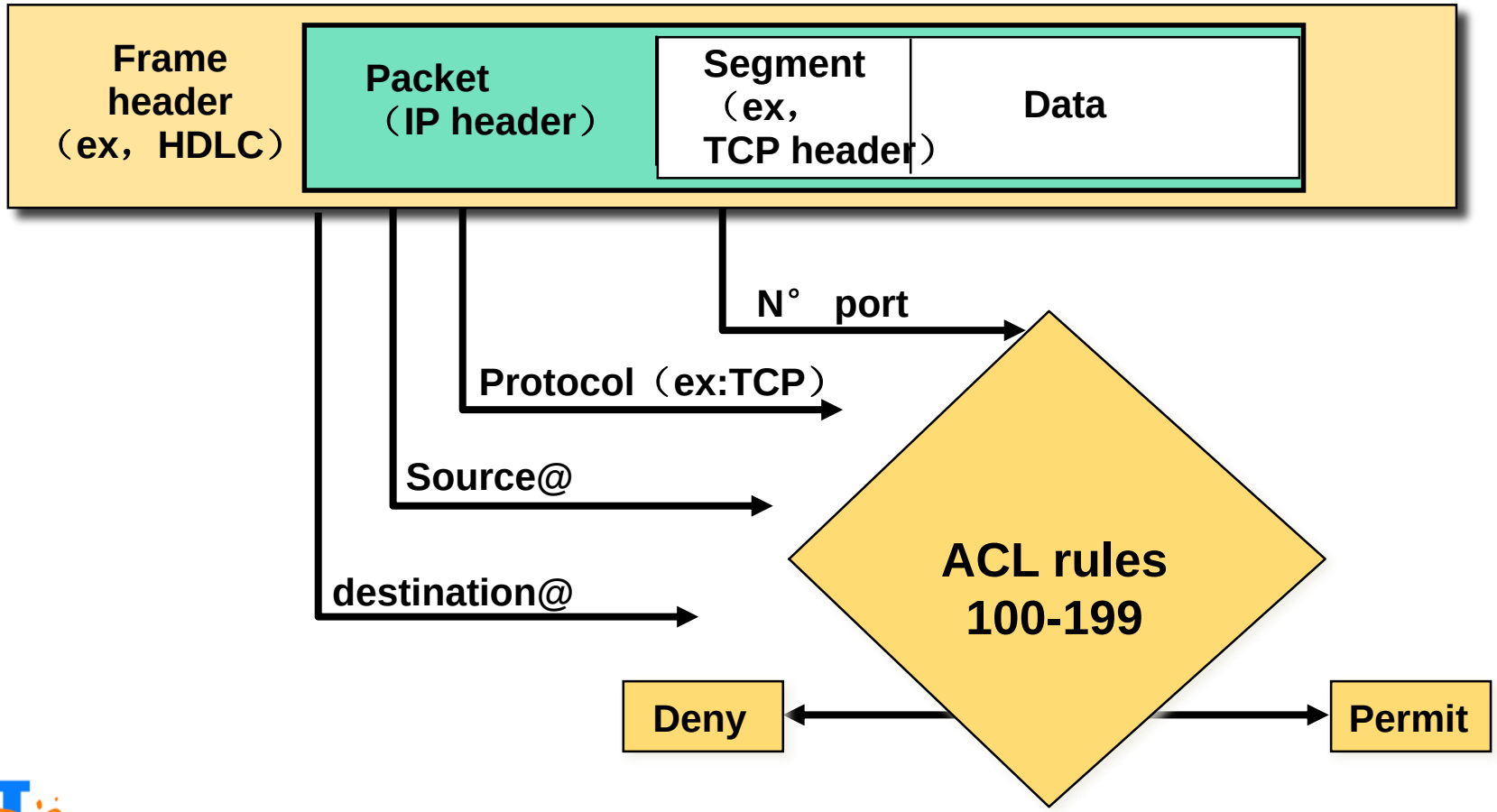
- Définition
  - Les listes d'accès étendues autorisent ou refusent l'acheminement des paquets en fonction des adresses d'origine et de destination, des protocoles et des numéros de port.
  - Numéros d'identification des ACL standard (Cisco)
    - 100-199
    - 2000-2699
  - Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle

ACL étendue

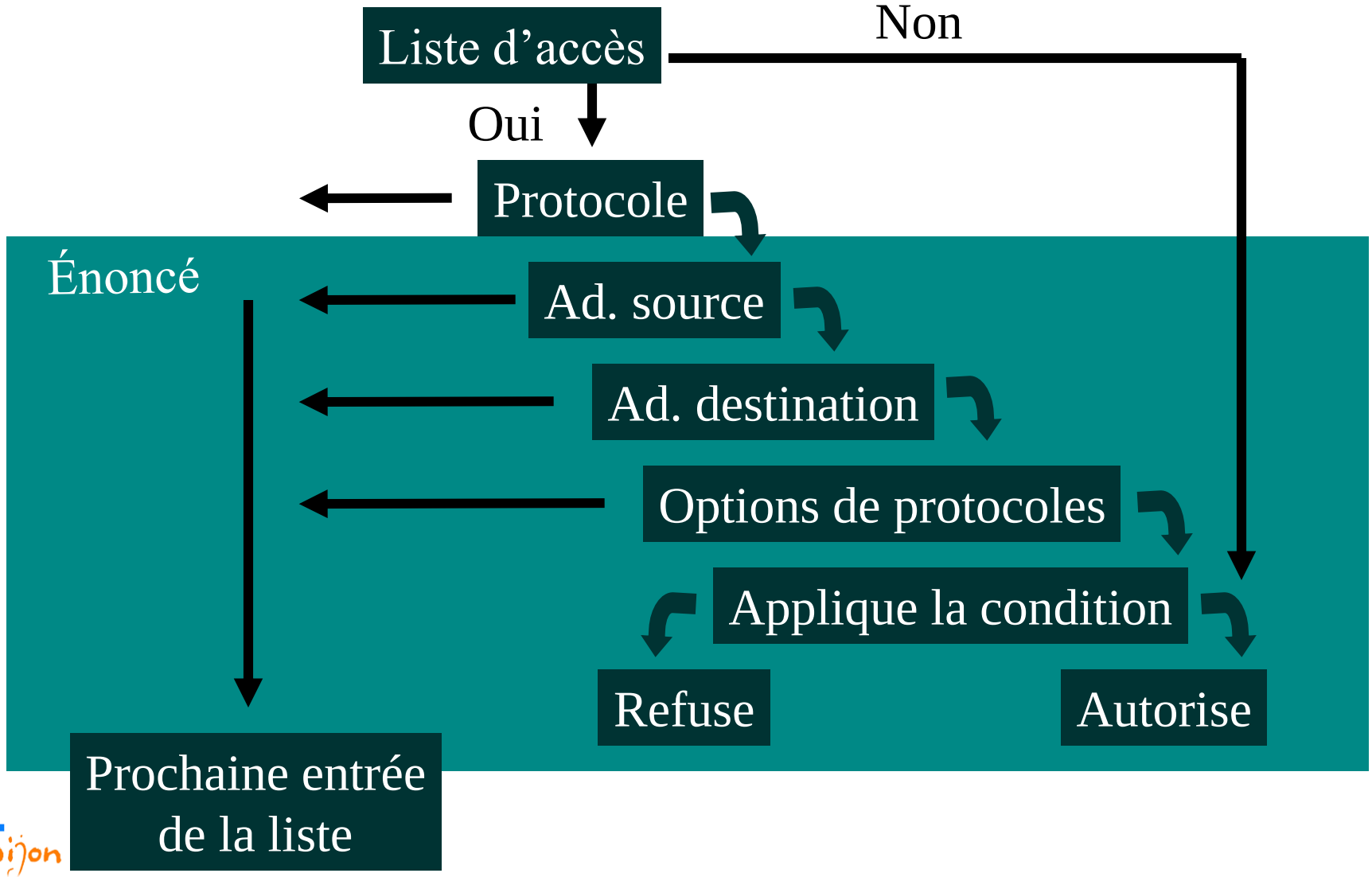
- Plus des infos sur le paquet pour dire accepter ou refuser



ACL étendue


Frame header （ex，HDLC）
Packet （IP header）
Segment （ex， TCP header）
Data
N° port
Protocol（ex:TCP）
Source@
destination@
ACL rules 100-199
Deny
Permit

Liste de conditions de l'ACL étendue



ACL étendue-les paramètres

- Syntaxe Cisco ISO
  - Router(config)# **access-list** *access-list-number* [**dynamic** *dynamic-name*[**time-out** *minutes*]]{**deny** | **permit** | **remark**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [icmp-type] [icmp-code] [icmp-message] [igmp-type] [**operator** *operand*] [**port** *port-number*] [**established**] [**fragments**]

ACL étendue-les paramètres

- Description des paramètres
  - **dynamic** *dynamic-name* : liste d'accès dynamique
  - ***time-out*** *minutes* : durée absolue d'une liste dynamique
  - *protocol* : spécifie le nom ou le numéro d'un protocole Internet (ex : tcp, udp, icmp, ou un entier entre 0 et 255)
  - *destination* : Adresse IP du réseau ou de l'hôte destination
  - *destination-wildcard* : Masque générique
  - **precedence** *precedence* : filtrage suivant le niveau de priorité
  - **tos** *tos* : filtrage suivant le niveau de service

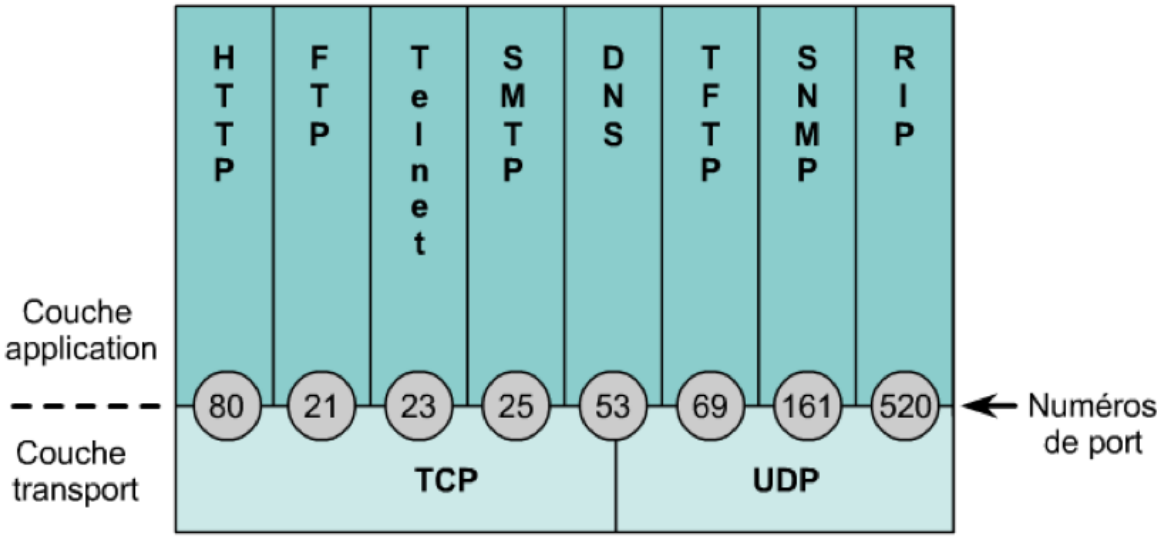
ACL étendue-les paramètres

- Description des paramètres
  - **operator** *operand* : compare les ports de destination ou de source. Si l'opérateur est placé après l'adresse source et son masque, il doit correspondre au port source (idem pour la destination). Les opérandes incluent :
    - **lt** : moins que
    - **gt** : plus grand que
    - **eq** : égal
    - **neq** : non égal
    - **range** : gamme inclusive (définit par deux numéros de port)
  - **port** *port-number* : spécifie le nom ou le numéro décimal d'un port TCP ou UDP

- **established** : indique une connexion établie TCP

- **fragments** : applique l'ACL aux fragments de paquets

- Ports de couche transport



- Seuls les trafics des services autorisés doivent être permis (explicitement)

N°	keyword	description	TCP/UDP
20	FTP-DATA	(..	TCP
21	FTP	/..	TCP
23	TELNET	..	TCP
25	SMTP	..	TCP
42	NAMESERVER	..	UDP
53	DOMAIN	..)	TCP/UDP
69	TFTP	..	UDP
80	WWW	..	TCP

ACL étendue-configuration

```
Router(config)# access-list access-list-number
{ permit | deny } protocol source source-wildcard
[operator port] destination destination-wildcard
[ operator port ]  [ established ] [log]
```

Création ACL étendue

```
Router(config-if)# ip access-group access-list-
number  { in | out }
```

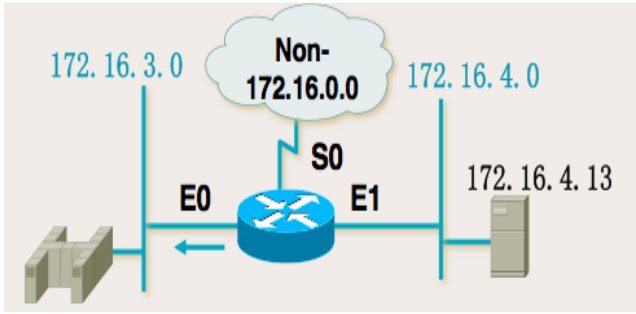
démarrer ACL étendue dans une interface spécifique

Exemple1： refuser ftp passe via E0

- 1° :créer ACL qui refuse s:172.16.4.0、d:172.16.3.0、en utilisant ftp

Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

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



- 2° appliquer à E0 out

Router(config)#interface fastethernet 0/0

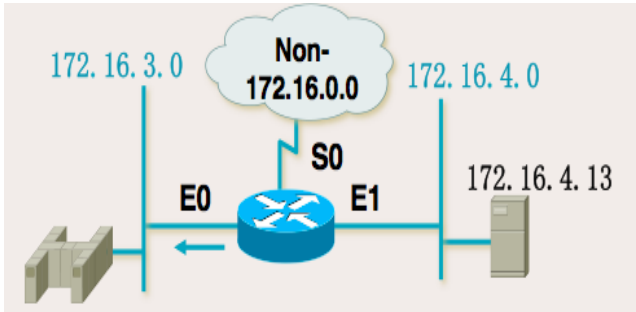
Router (config-if) #ip access-group 101 out

Exemple2： refuser telnet passe via E0

- 1°， créer ACL qui refuse s:172.16.4.0、d:172.16.3.0、en utilisant telnet

Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23

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



- 2° appliquer à E0 out

Router(config)#interface fastethernet 0/0

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

Named ACL-configuration

- Cisco IOS Release >11.2 new feature

```
Router(config)# ip access-list { standard | extended } name
```

- Name isolé

```
Router(config {std- | ext-}nacl)# { permit | deny }
{ ip access list test conditions }
{ permit | deny } { ip access list test conditions }
no { permit | deny } { ip access list test conditions }
```

- pas besion de spécifier N° de ACL avant configurer permit et deny
- Command “no” pour supprimer phrase spécifque de named ACL

```
Router(config-if)# ip access-group name { in | out }
```

- Utilise named ACL en interface spécifique

Named ACL-exemple

- 1°， créer ACL au nom de cisco

  Router(config)#ip access-list extended *cisco*

- 2°， indiquer les conditions de permit et deny

  Router (config-ext-nacl) # deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23

  Router (config-ext-nacl) # permit ip any any

- 3°， appliquer à E0 out

  Router (config) #interface fastethernet 0/0

  Router (config-if) #ip access-group *cisco* out

Look up configuration de ACL

```
wg_ro_a#show ip int e0
Ethernet0 is up, line protocol is up
  Internet address is 10.1.1.11/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  <text ommitted>
```

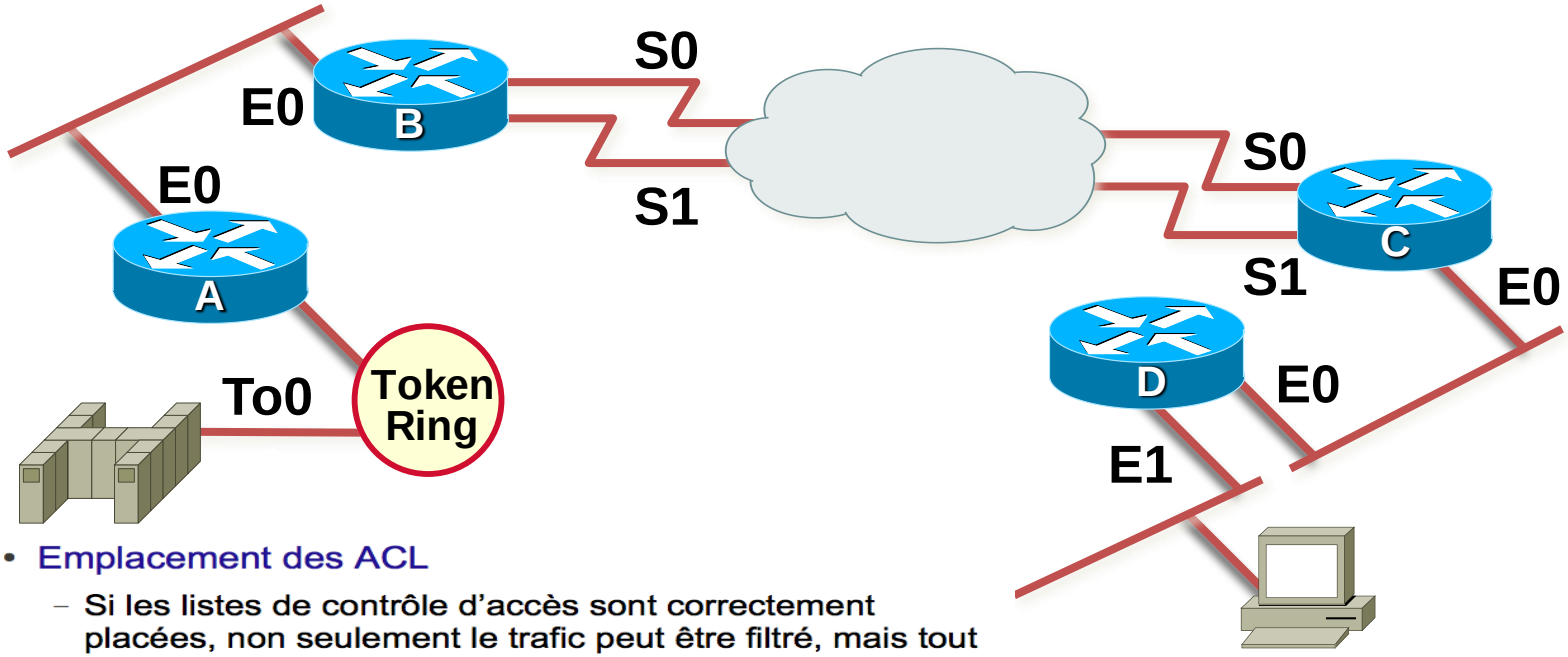
Look up phrases de ACL

```
wg_ro_a#show {protocol} access-list {access-list number}
```

```
wg_ro_a#show access-lists {access-list number}
```

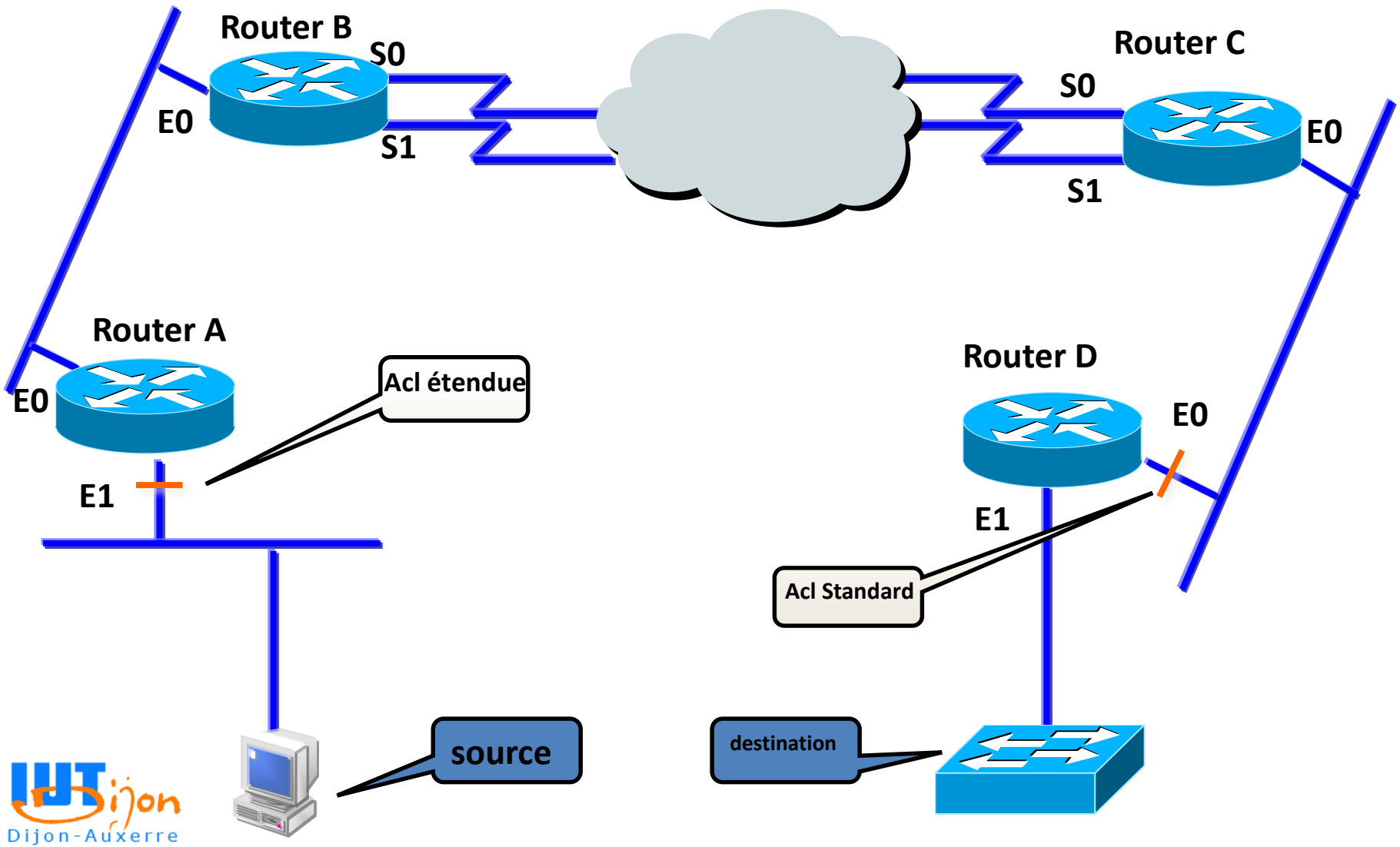
```
wg_ro_a#show access-lists
Standard IP access list 1
    permit 10.2.2.1
    permit 10.3.3.1
    permit 10.4.4.1
    permit 10.5.5.1
Extended IP access list 101
    permit tcp host 10.22.22.1 any eq telnet
    permit tcp host 10.33.33.1 any eq ftp
    permit tcp host 10.44.44.1 any eq ftp-data
```

Mise en œuvre des ACL (2-1)



- Emplacement des ACL
  - Si les listes de contrôle d'accès sont correctement placées, non seulement le trafic peut être filtré, mais tout le réseau devient plus performant.
  - Si le trafic est filtré, la liste de contrôle d'accès doit être placée à l'endroit où elle aura le plus grand impact sur les performances.
  - La règle générale est de placer les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé.
  - les listes de contrôle d'accès standard ne précisent pas les adresses de destination, vous devez les placer le plus près possible de la destination.

Mise en œuvre des ACL (2-2)



Les choses à respecter

GUIDE & RÈGLE

Guide de configuration ACL(!!!)

- Numéro d'indentification nous indique quelle ACL que l'on peut utiliser.
- Assigner une seule ACL par interface, par port, par direction et par protocole.(une seule ACL inbound et une seule ACL outbound par interface)
- Le contenu de ACL décide l'ordre de contrôle de donnée. La position de l'instruction de contrainte dans ACL est importante.
- Il faut mettre la condition qui est le plus strict à l'avance.
- Il y a une instruction (implicit deny all) à la fin de ACL.
- Chaque 'correcte ACL' doit avoir au moins une instruction de permit.
- Créer ACL tout d'abord, et puis l'appliquer sur l'interface. L'ordre des instructions ACL est importante.
- ACL ne peut pas filtrer les données se produisent par lui-même. (CAD Les ACL ne permettant pas de filtrer le trafic généré par le routeur.)

Les 8 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.
- On utilise la commande no access-list *number* pour supprimer l'emsemble de ce ACL
- Une ACL se termine par un deny any implicite (deny all)
- ✓ Il faut le ACL contenir au minimum une ligne permit

more

EXEMPLES

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

- La mention *established* autorise les retours pour les applications qui fonctionnent à double sens (Bit de Ack sur 1)

  permit tcp any eq 80 192.168.10.0 255.255.255.0 gt 1000 established
- 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

Référence:http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

Les lignes de commandes

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

EX: ACL 122 appliquée en entrée du routeur, sens internet=>LAN

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-
   prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

EX: ACL 122 appliquée en entrée du routeur, sens LAN=>internet

```
ip address 64.24.14.1/24
ip address group 122 in
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq 22
access-list 122 permit udp 64.24.14.1 0.0.0.255 any eq domain
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo-reply
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq ftp
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq http
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any gt 1023 established
access-list 122 permit udp 64.24.14.1 0.0.0.255 any gt 1023
```

Exo1

- Rédigez une liste d'accès standard nommée qui s’appelle «George» sur le routeur0, interface E1 pour bloquer ordinateur A(@ip=72.16.10.35) d'envoyer les informations à l'ordinateur B; mais permettra tout autre trafic.

Exo1

Router#configure terminal (or config t)

Router(config)#ip access-list standard George

Router(config-std-nacl)#deny host 72.16.70.35

Router(config-std-nacl)#access-list permit any

Router(config-std-nacl)#interface e1

Router(config-if)#ip access-group George out

Router(config-if)#exit

Router(config)#exit

Exo2

- Rédigez une liste d'accès étendue nommée qui s ’appelle "Gracie" sur le routeur 0, Interface E0. pour refuser le trafic HTTP destiné au serveur web 192.168.207.27, mais permettra tout autre trafic HTTP pour atteindre le réseau de 192.168.207.0. Refuser tous les autres trafics IP.

Exo2

Router# configure terminal (or config t)
Router(config)#ip access-list extended Gracie
Router(config-ext-nacl)# deny tcp any host 192.168.207.27 eq 80
Router(config-ext-nacl)# permit tcp any 192.168.207.0 0.0.0.255 eq 80
Router(config-ext-nacl)# interface e0
Router(config-if)# ip access-group Gracie in
Router(config-if)# exit
Router(config)# exit