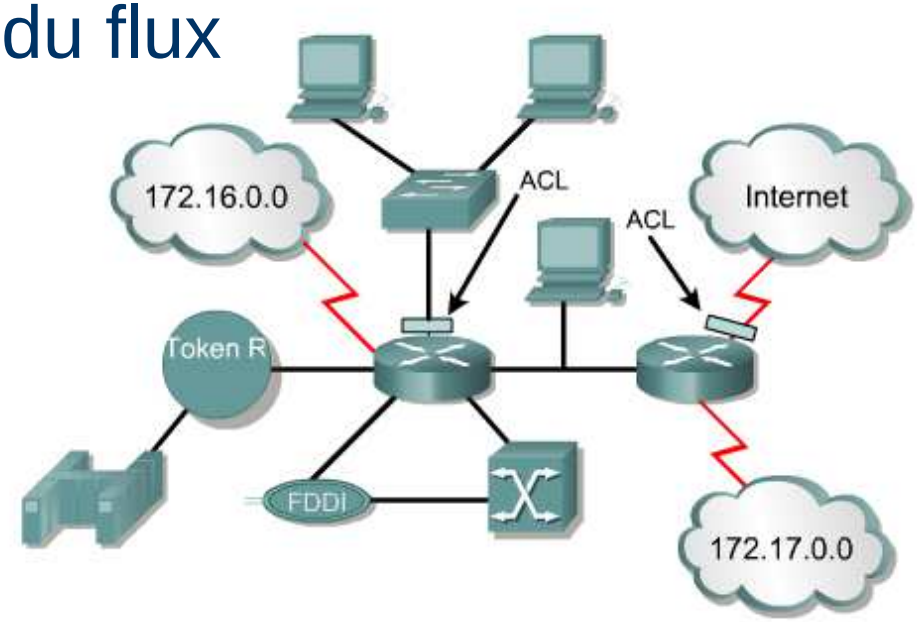
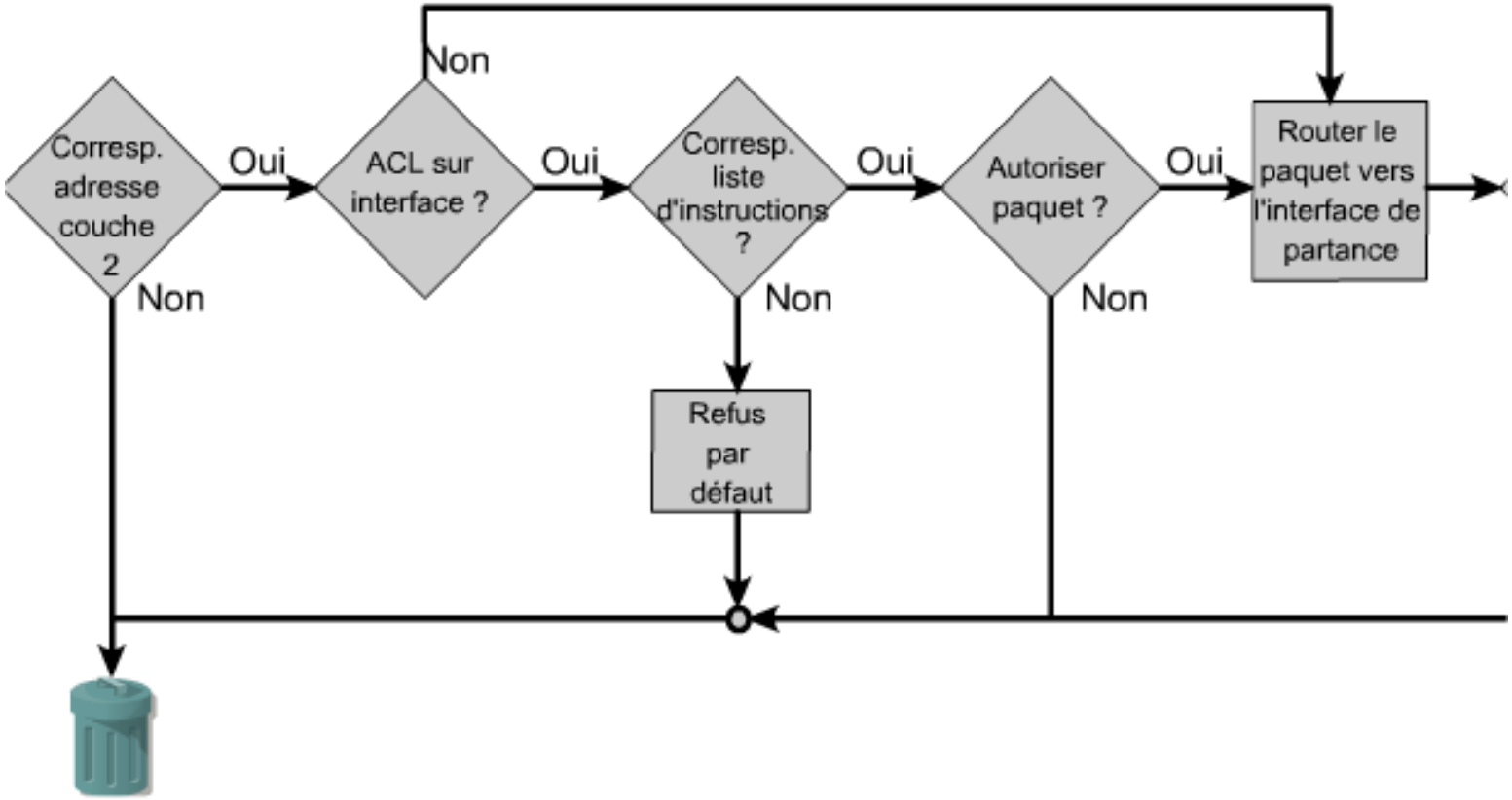
Access Control List

Généralités

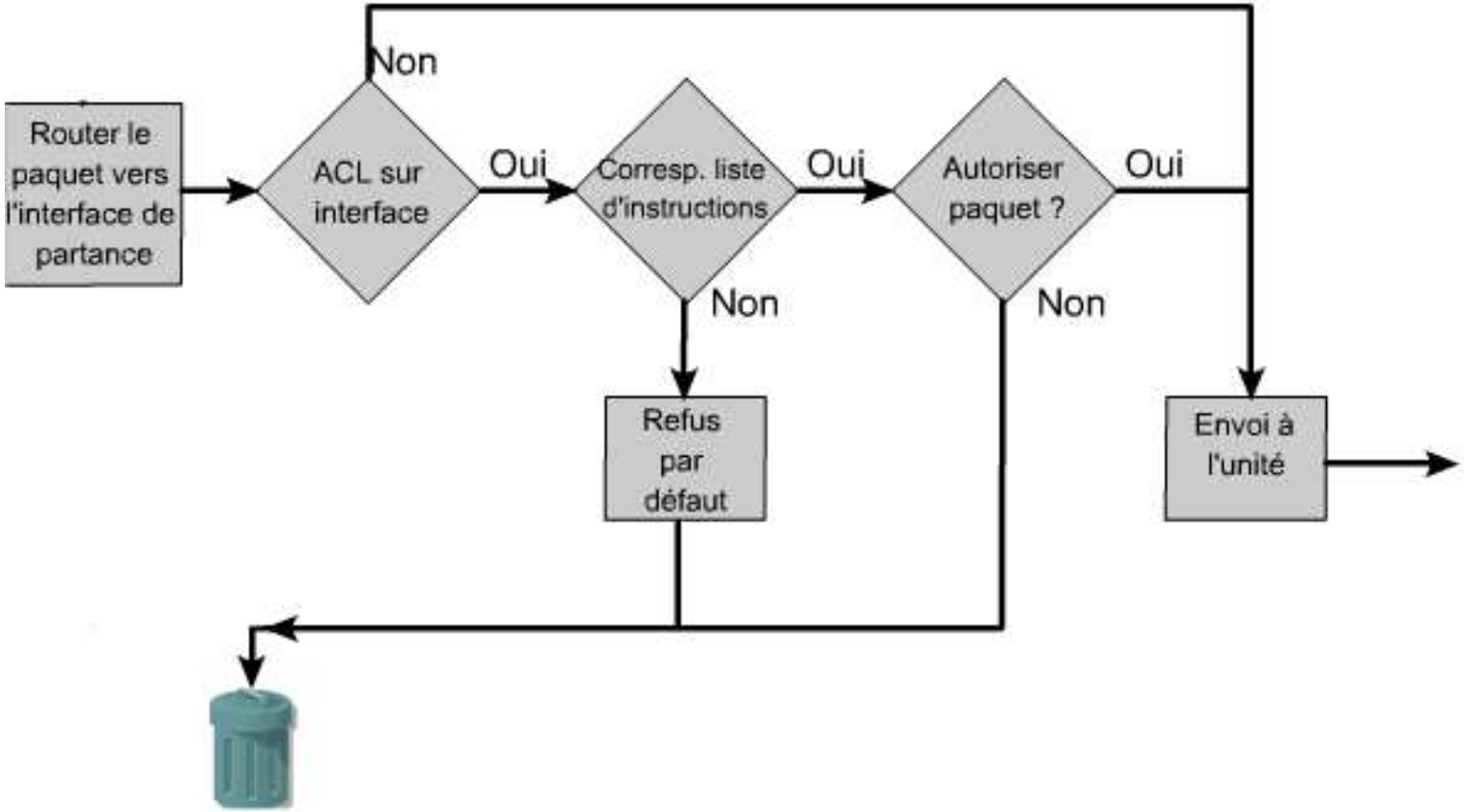
- Une ACL permet de filtrer un flux sur un routeur ; ne remplace pas un véritable pare-feu
- Utilisable sur une interface en entrée ou en sortie du flux



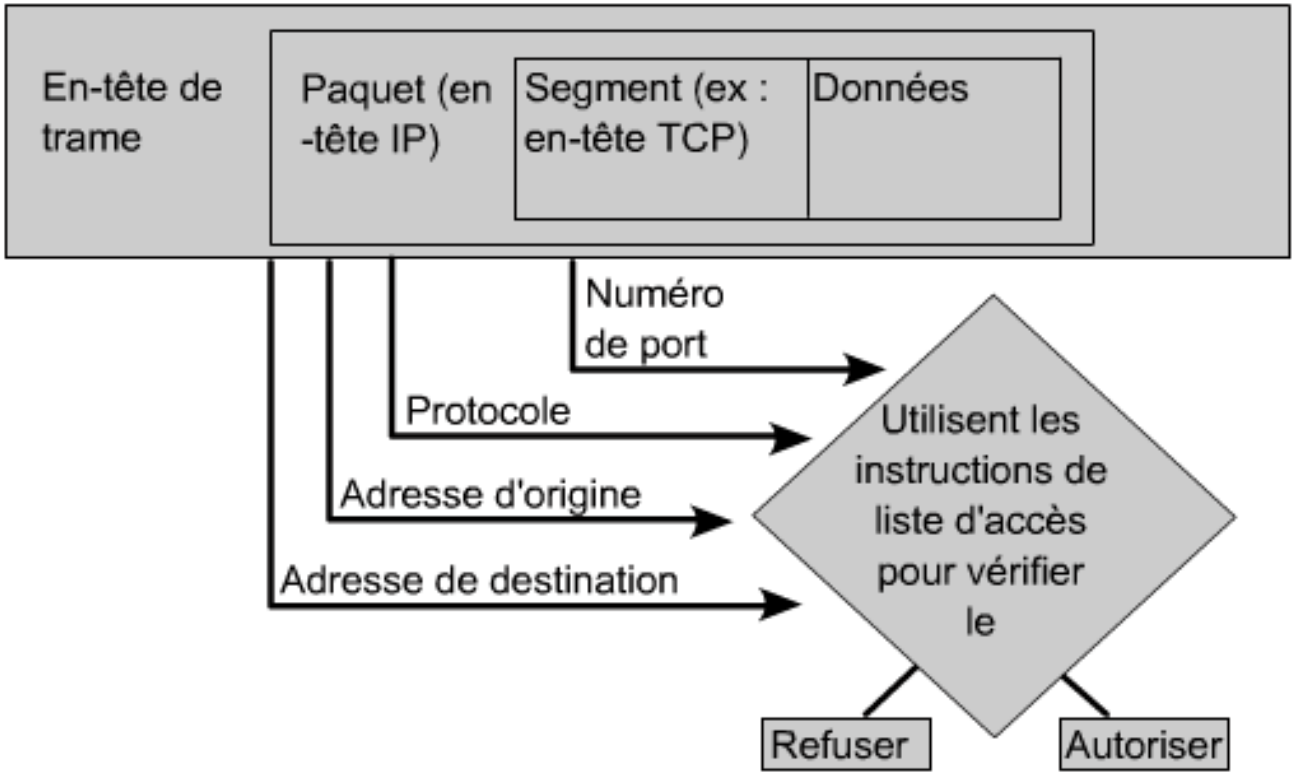
ACL vs Routage (I)



ACL vs Routage (II)



Eléments de filtrage et actions



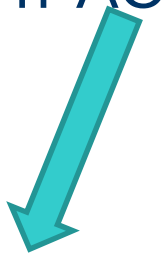
Types d’acls

- Standard : filtrage de la source du trafic
  - à placer au plus proche de la destination du trafic
- Étendue : filtrage de la source, de la destination et du protocole du trafic
  - à placer au plus proche de la source du trafic
- Nommée : ressemble aux étendues mais d’une manipulation plus aisée

Mise en œuvre - I (standard/étendue)

- Définition de l'ACL

  (config)#access-list n°ACL {permit|deny}…

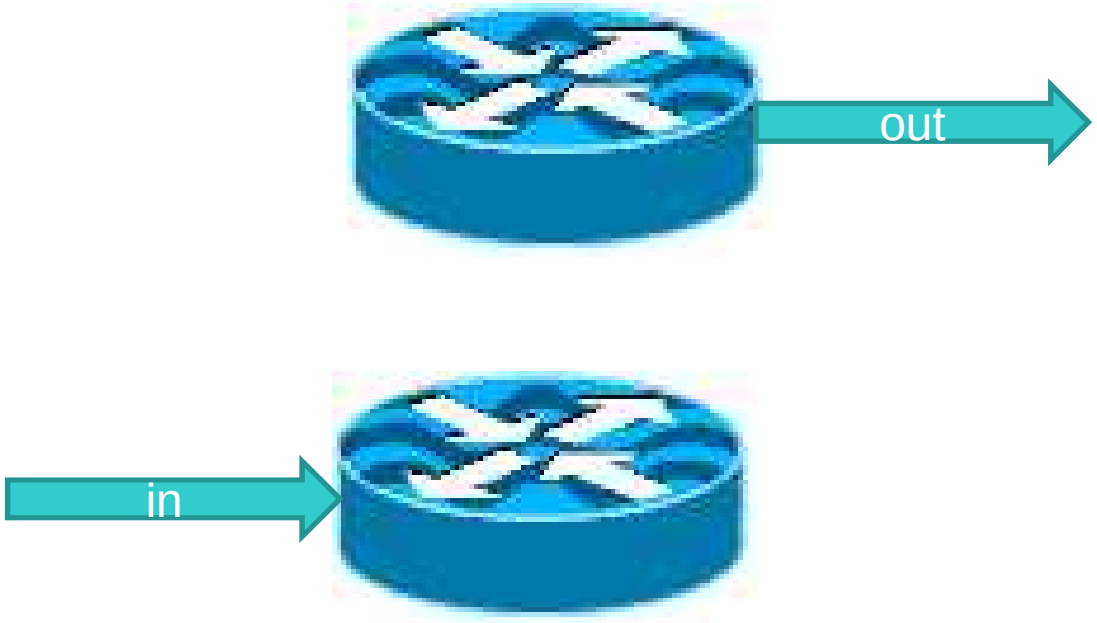


Protocole	Plage
IP standard	1-99, 1300-1999
IP étendu	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX étendu	900-999
Protocole IPX Service Advertising	1000-1099

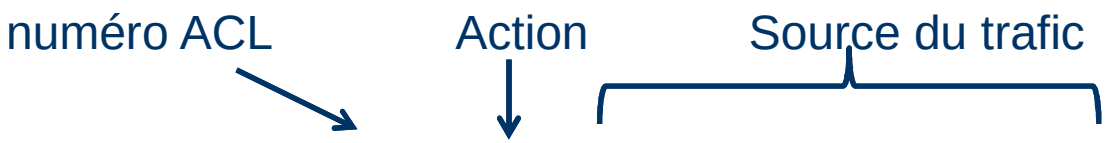
Mise en œuvre - II

- Mise en place de l'ACL

  (config-if)# ip access-group n°ACL {in|out}



Exemple d'ACL standard



access-list 2 permit 172.16.1.0 0.0.0.255
on autorise le trafic en provenance du réseau 172.16.1.0/24

access-list 2 deny 10.0.0.1 0.0.0.0
et *on interdit le trafic en provenance de la machine 10.0.0.1*

interface fa0/0
ip access-group 2 in
à rentrer par l'interface fa0/0

Exemple d'ACL étendue

access-list 101 permit ip 12.1.1.0 0.0.0.255 0.0.0.0 255.255.255.255
on autorise le trafic IP en provenance du réseau 12.1.1.0/24 et vers n'importe quelle destination

access-list 101 deny tcp 9.9.9.9 0.0.0.0 10.0.0.0 0.0.0.255
et *on interdit le trafic TCP en provenance de l'adresse 9.9.9.9 et à destination du réseau 10.0.0.0/24*

interface fa0/0
  ip access-group 101 out
à sortir par l'interface fa0/0

Commandes utiles

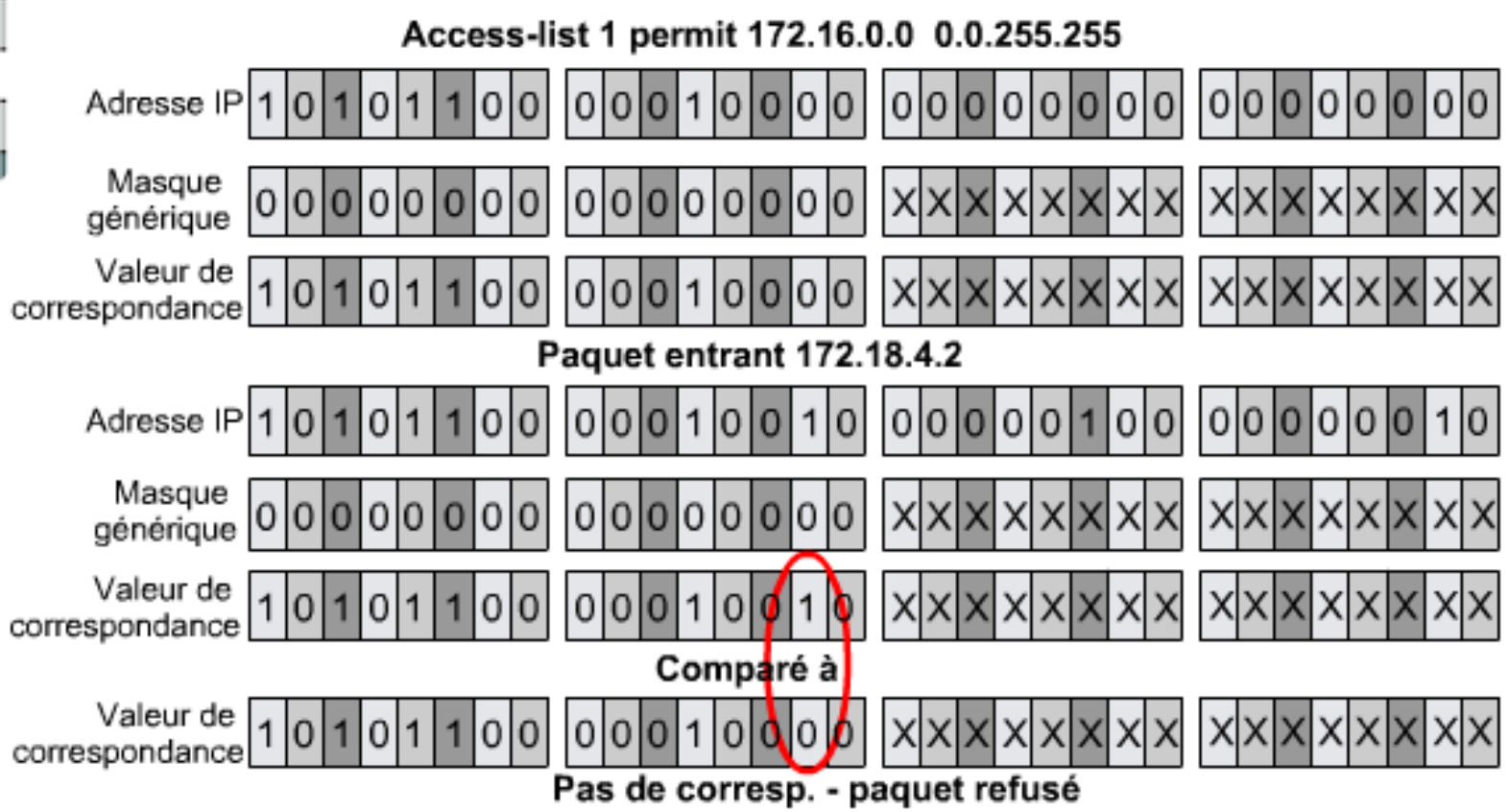
show access-list / show ip access-lists

```
Extended IP access list 102
    10 permit icmp any 10.0.0.0 0.255.255.255 echo-reply
    20 deny icmp any 10.0.0.0 0.255.255.255
    30 permit ip any any (2 match(es))
Extended IP access list 101
    10 permit icmp 10.0.0.0 0.255.255.255 any
    20 permit tcp 10.0.0.0 0.255.255.255 any eq www
```

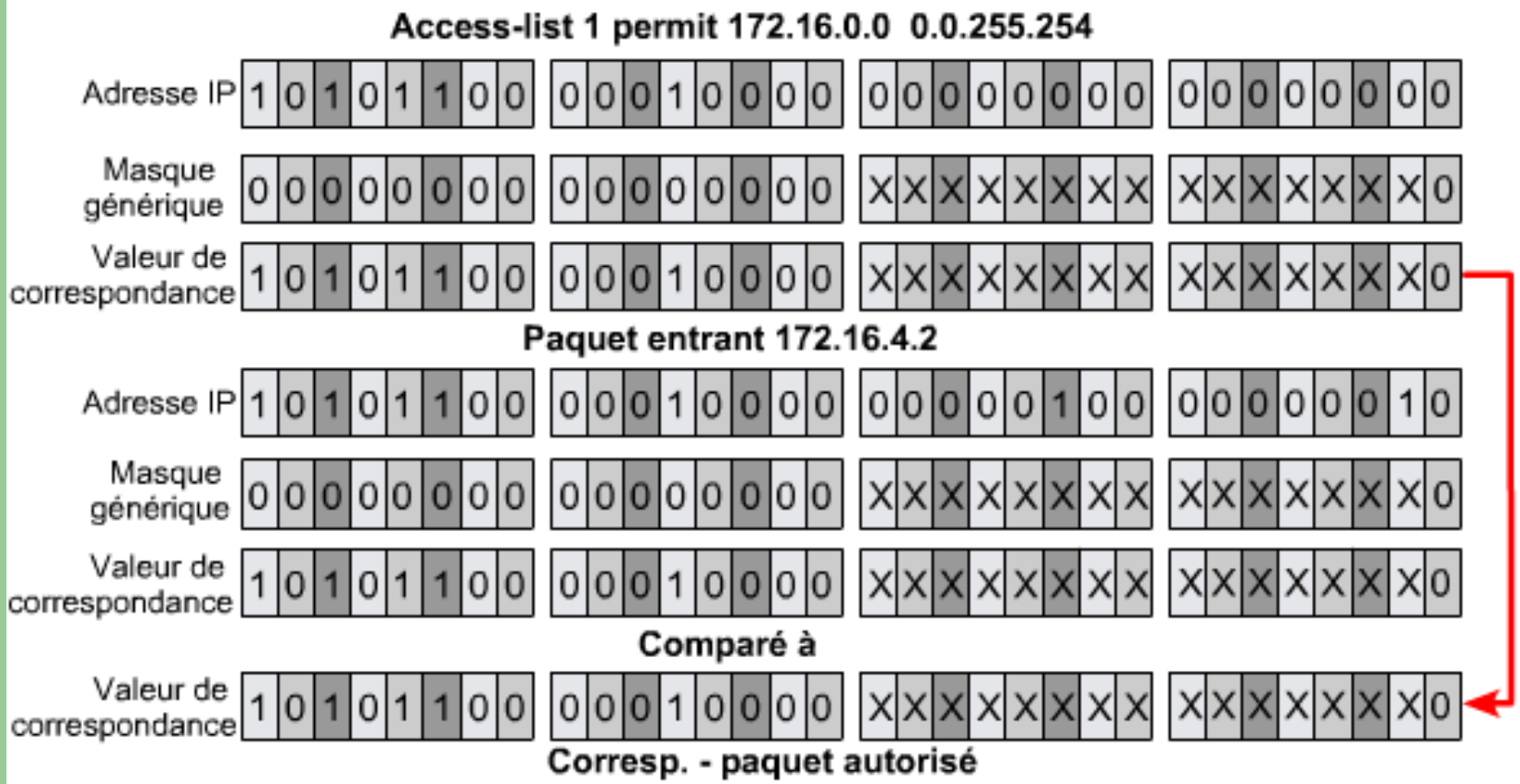
Masque générique (I)

- Détermine seulement si une règle s'applique ou non au paquet
- Si le $x^{ième}$ bit est à 0 dans le masque, alors les $x^{ième}$ bits de l'adresse du paquet et de l'adresse de la liste doivent correspondre
- Si le $x^{ième}$ bit est à 1 dans le masque, alors aucune correspondance n'est exigée entre les $x^{ième}$ bits de l'adresse du paquet et de l'adresse de la liste

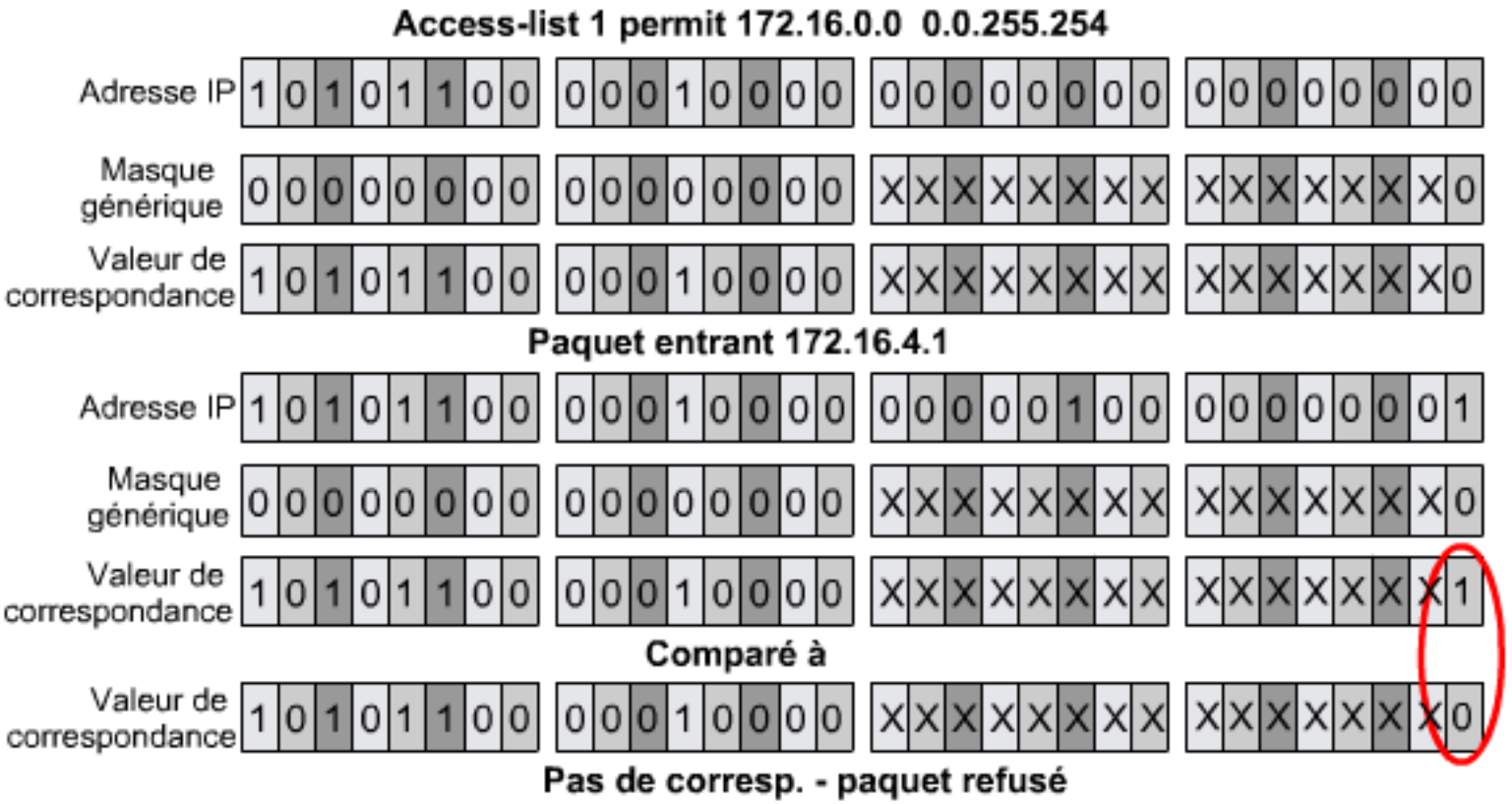
Masque générique (II)



Masque générique (III)



Masque générique (IV)



Les raccourcis host et any

- host : correspondance parfaite sur l'hôte

  host @ip @ip 0.0.0.0

- any : aucune correspondance sur rien

  any 0.0.0.0 255.255.255.255

Exemple

access-list 101 permit ip 12.1.1.0 0.0.0.255 any

on autorise le trafic IP en provenance du réseau 12.1.1.0/24 et vers n'importe quelle destination

access-list 101 deny tcp host 9.9.9.9 10.0.0.0 0.0.0.255

et *on interdit le trafic TCP en provenance de l'adresse 9.9.9.9 et à destination du réseau 10.0.0.0/24*

A NE PAS OUBLIER !!!

- Une acl standard se termine implicitement par un

  deny any

- Une acl étendue se termine implicitement par un

  deny ip any any

Exemples

access-list 2 permit 172.16.1.10 0.0.0.0
access-list 2 deny any

access-list 101 permit tcp host 172.16.1.10 any eq telnet
access-list 101 deny ip any any

ACL nommées

- Identification intuitive d’une liste d’accès à l’aide d’un nom alphanumérique
- Élimination de la limite de 99 listes d’accès standard et de 100 listes d’accès étendues
- Possibilité de modifier des listes de contrôle d’accès sans avoir à les éliminer, puis à les reconfigurer

Mise en œuvre

- Définition de l’ACL

  (config)#ip access-list {extended|standard} nom

- Mise en place de l’ACL

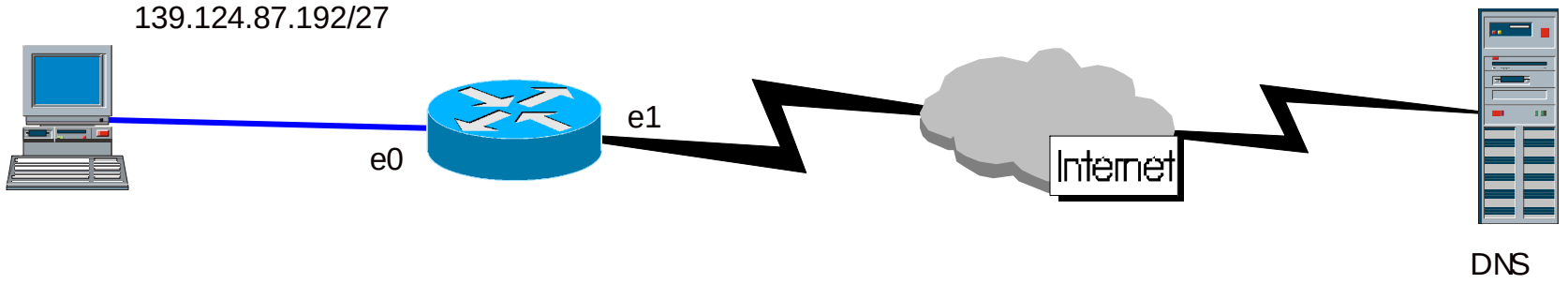
  (config-if)# ip access-group nom {in|out}

Exemple

```
ip access-list extended test
    permit ip host 2.2.2.2 host 3.3.3.3
    permit udp 10.0.0.0 0.0.0.255 host 8.8.8.5 eq 169
    deny icmp any any

int fa0/0
    ip access-group test in
```

Étude de cas – DNS (1)




```
ip access-list extended filtre1
    permit udp any eq 53 139.124.87.192 0.0.0.31 gt 1023
    deny ip any any

interface ethernet1
    ip access-group filtre1 in
```

Étude de cas – DNS (2)

- udp any eq 53 nécessaire car vous ne savez pas à l'avance quel DNS les utilisateurs vont choisir

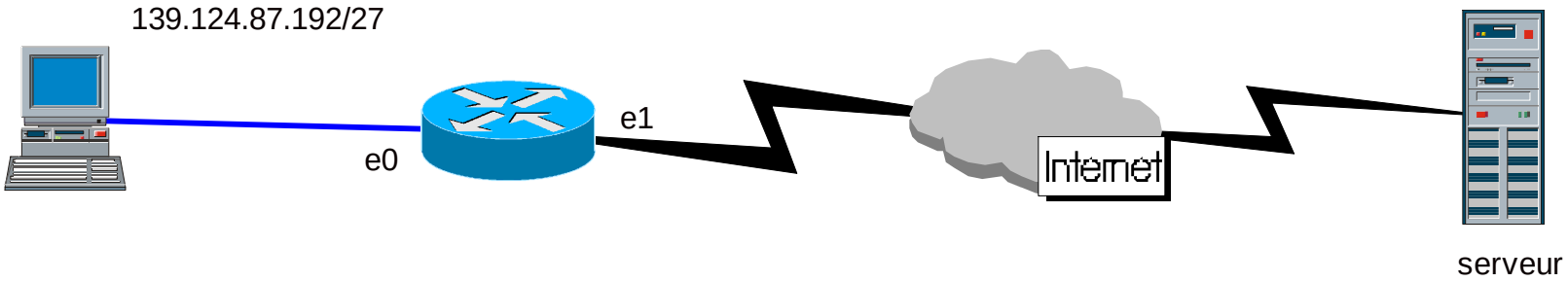
  => on ne contrôle plus la source du trafic

  => tous les autres protocoles sur UDP sont bloqués

- 139.124.87.192 0.0.0.63 gt 1023 nécessaire car vous ne savez pas à l'avance sur quel port votre machine va dialoguer avec le DNS

  => tous les ports UDP > 1023 sont ouverts

Étude de cas – tcp (1)



ip access-list extended filtre1
    permit tcp any 139.124.87.192 0.0.0.31 established
    deny ip any any

interface ethernet1
    ip access-group filtre1 in

Étude de cas – tcp (2)

- established nécessaire pour s'assurer que le trafic rentrant correspond à une réponse (vérification de la présence d'un des flags ACK ou RST)

  => rien ne prouve que la session a été initiée par une machine du réseau 139.124.87.192

  => quid d'un segment forgé SYN+ACK ou RST+ACK ?