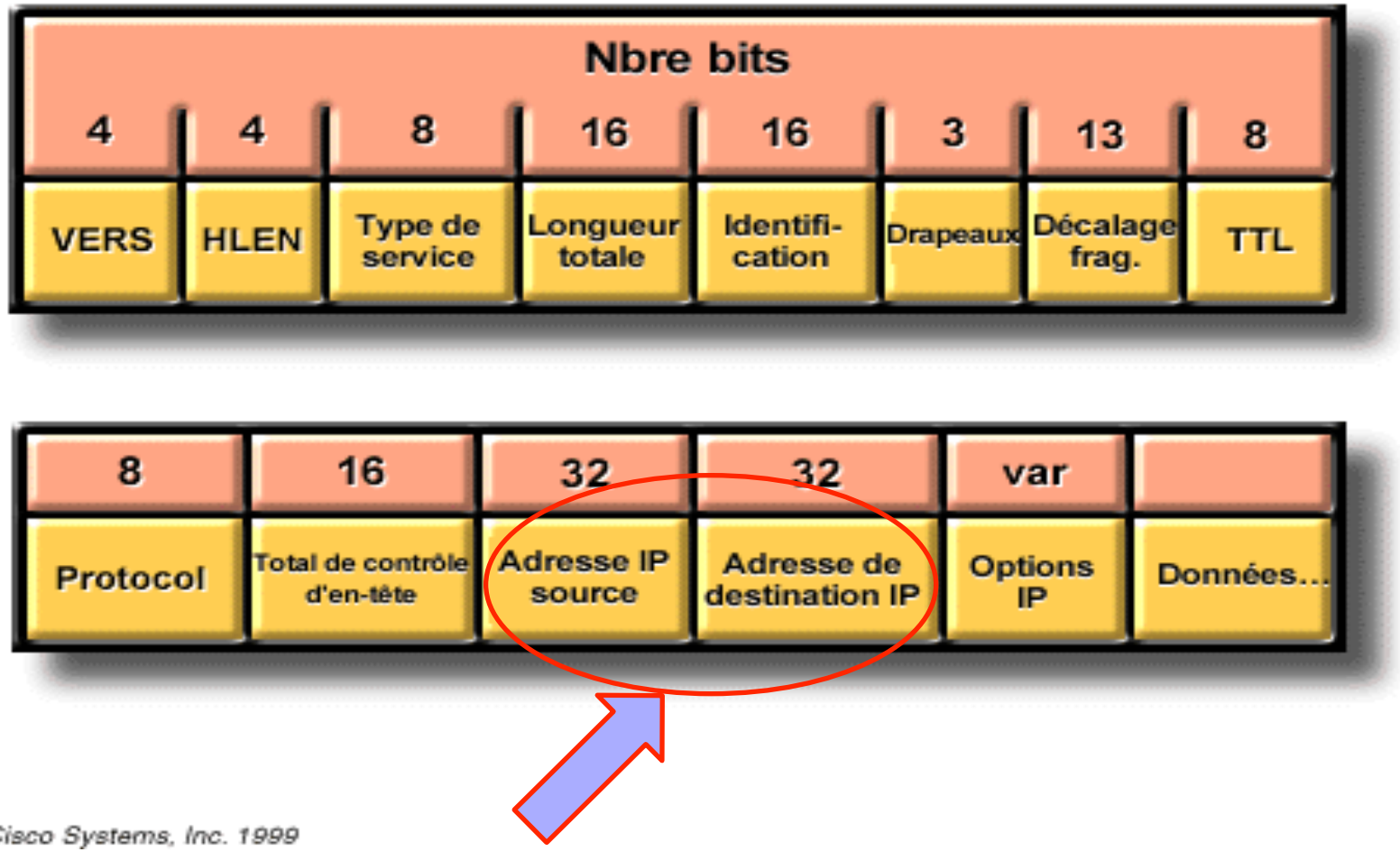
ACL: Filtrage des paquets

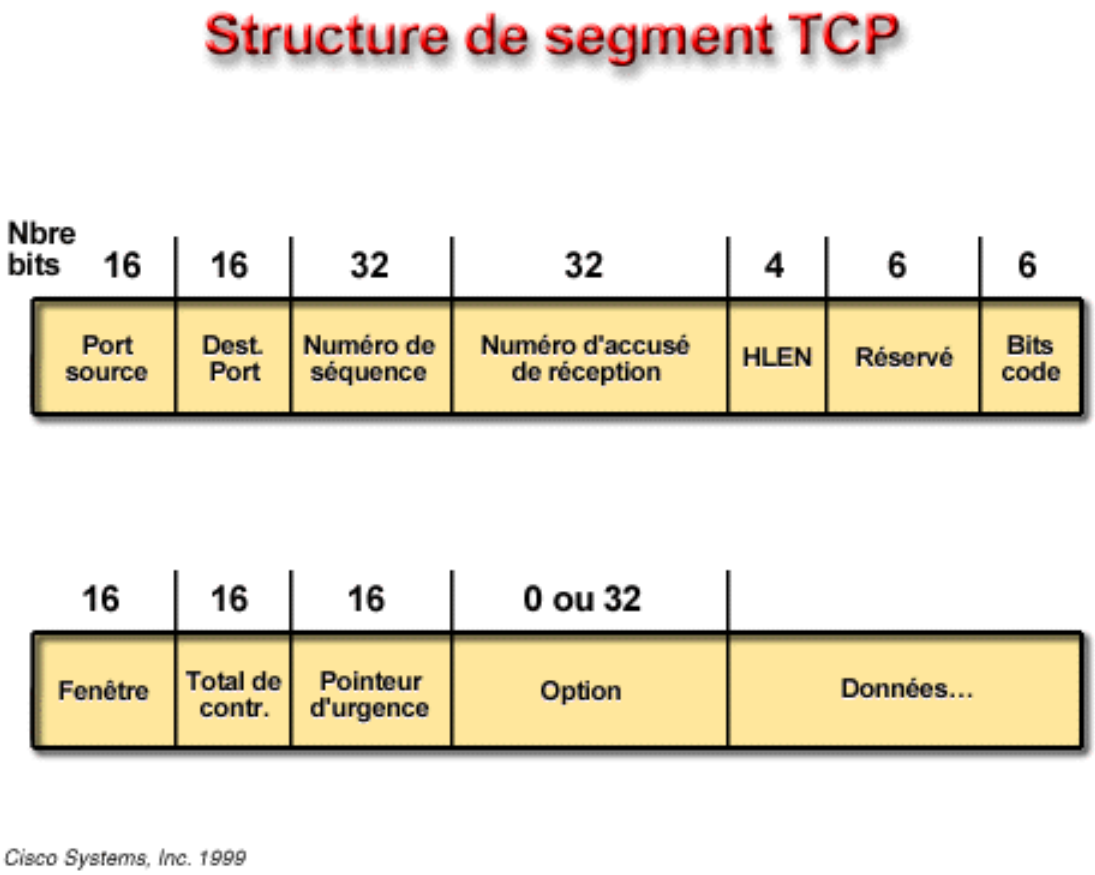
Pr. KH. Ibrahimi, SMI, S6

Datagramme IP

Le datagramme IP



Segment TCP


Structure de segment TCP
Nbre bits
16
16
32
32
4
6
6
Port source
Dest. Port
Numéro de séquence
Numéro d'accusé de réception
HLEN
Réservé
Bits code
16
16
16
0 ou 32
Fenêtre
Total de contr.
Pointeur d'urgence
Option
Données...
© Cisco Systems, Inc. 1999

ACL: Filtrage des paquets

- Le filtrage des paquets au sein d'un routeur sont de deux types:
  - filtrage des paquets statique (basé @IP source)
  - filtrage des paquets dynamique (IP, TCP, UDP, ICMP)
- Le filtrage permet le contrôle d'accès à un réseau en analysant les paquets entrants et sortants
- Décision: autoriser ou arrêter la transmission des paquets en fonction de critères prédéfinis par un routeur.
- Un routeur de filtrage des paquets se réfère aux règles pour déterminer s'il doit autoriser ou refuser le trafic en fonction des adresses IP source et de destination, du port source, du port de destination et du protocole des paquets.

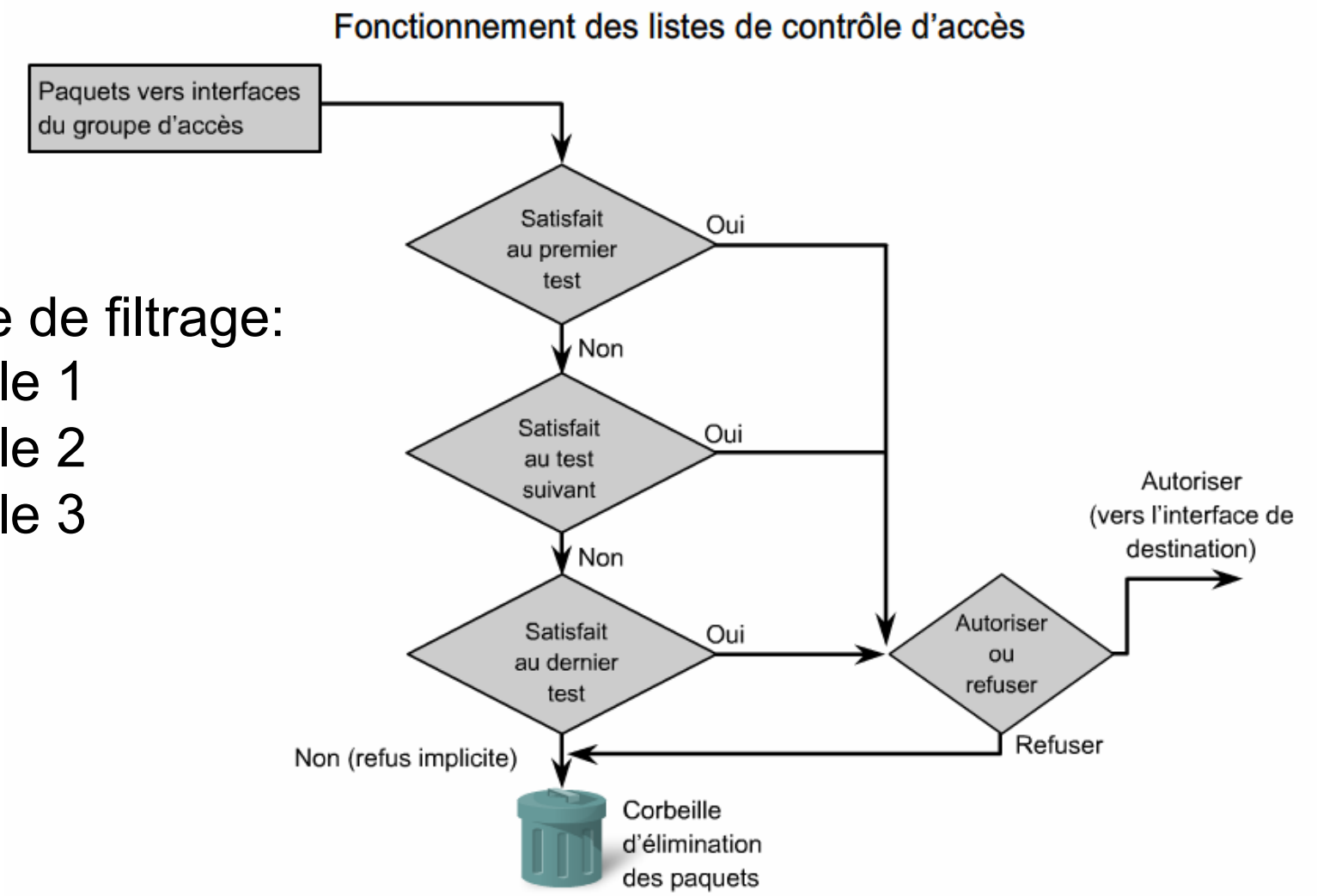
Les éléments de la règle

- Une règle de filtrage des paquets IP est en fonction des informations des entêtes.
- Entête du paquet IP:
  - Adresse IP source
  - Adresse IP de destination
- Entête du segment TCP/UDP
  - Port source TCP/UDP
  - Port de destination TCP/UDP
- Message ICMP
- La règle d'accès est appliquée à un routeur.
- Règle = condition logique
- L'ensemble des règles d'accès est appelé une liste de contrôle d'accès. Les règles sont utilisées de manière séquentielle.

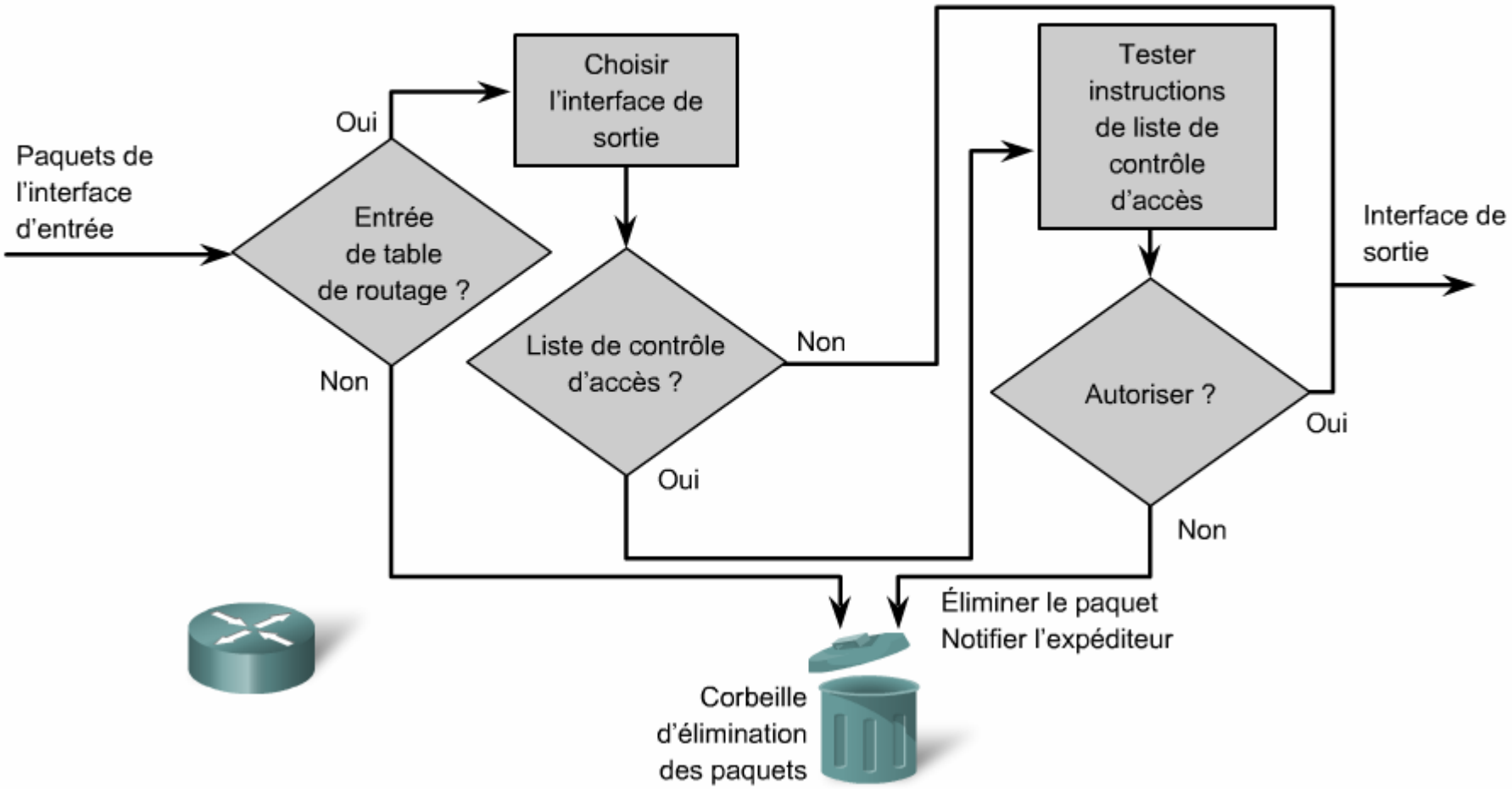
Règle

- Vous pouvez configurer une liste de contrôle 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.
  - direction : deux listes sont nécessaires, la première pour contrôler le trafic entrant et la seconde pour contrôler le trafic sortant.
  - interface : les listes de contrôle d'accès contrôlent le trafic pour une interface, telle que Fast Ethernet 0/0.
- Listes de contrôle d'accès entrantes : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Si le paquet est rejeté, il ne va pas être traité par le routage.
- Listes de contrôle d'accès sortantes : les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante.

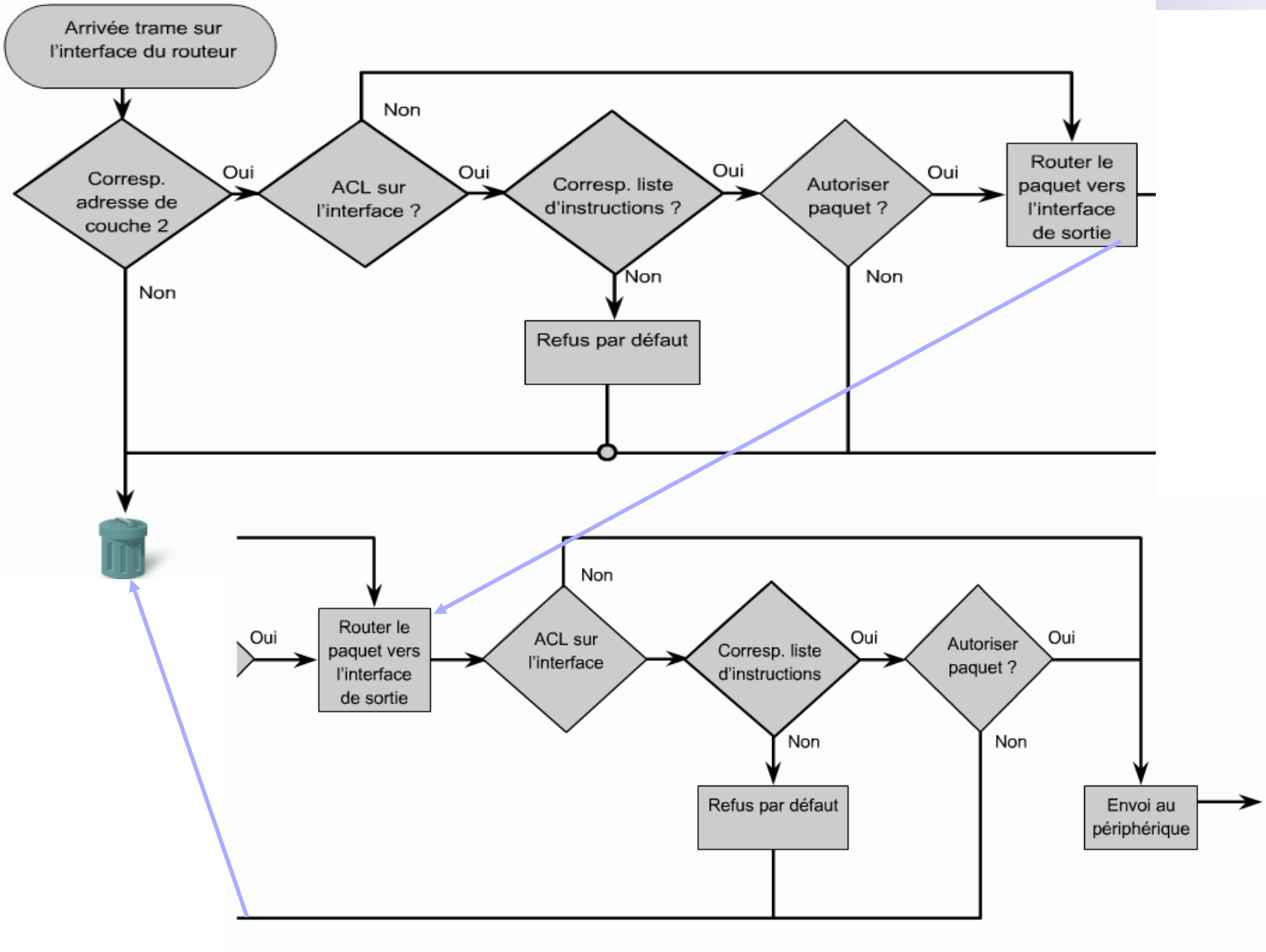
Liste de filtrage:
Règle 1
Règle 2
Règle 3
…..



Exemple de liste de contrôle d'accès sortante



Processus de liste de contrôle d'accès (ACL) et de routage dans un routeur



Types de liste de contrôle d'accès Cisco

- **Listes de contrôle d'accès standard**: permettent d'autoriser et de refuser le trafic en provenance d'adresses IP source. La destination du paquet et les ports concernés n'ont aucune incidence.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

- **Les listes de contrôle d'accès étendues (dynamique):** filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP de destination, les ports TCP ou UDP source, les ports TCP ou UDP de destination, et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

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

Une liste de contrôle d'accès standard

- Étape 1. Création d'une liste de contrôle d'accès en spécifiant un numéro ou un nom de liste et des conditions d'accès.
  - Numéro de la liste entre 1 et 99 ou bien de 1300 et 1999
  - Syntaxe: #access-list numero_liste permit/deny/remark source (@IP/any)
  - Source = @IP d'une machine spécifique ou d'un réseau de provenance du paquet / bien n'importe quelle machine du réseau avec la commande any (0.0.0.0 255.255.255.255).
  - Exemple: #access-list 2 deny 192.168.10.1 (refuser)
  - #access-list 2 permit 192.168.10.0 0.0.0.255 (autoriser)
  - #access-list 2 remark *Une liste appliquer sur l'interface FastEth1*
- Étape 2. Application d'une liste de contrôle d'accès aux interfaces ou aux lignes du terminal.
  - Choisir une interface #interface Fa0/0
  - Activer la liste avec la commande #ip access-group 2 in/out
  - Une dernière règle soit accepter tout ou bien refuser tout. #access-list 2 permit/ deny any.

Une liste de contrôle d'accès étendue

- Étape 1. Création d' une liste de contrôle d'accès en spécifiant un numéro ou un nom de liste et des conditions d'accès.
  - Numéro de la liste doit être entre 100 et 199 ou bien de 2000 et 2699.
  - Syntaxe: #access-list numéro_list permit/deny protocole source masque_générique destination (@IP_hôte/réseau)
  - Protocole = TCP, UDP, ICMP ou tout simplement IP.
  - Exemple:
  - #access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 (autoriser tout paquet IP du réseau 192.168.100.0 vers le réseau 192.168.200.0)
  - #access-list 101 deny TCP any any eq 23 (telnet) (refuser Telnet)
- Étape 2. Application d'une liste de contrôle d'accès aux interfaces ou aux lignes du terminal.
  - Choisir une interface #interface Fa0/0
  - Activer la liste avec la commande #ip access-group 2 in/out

Une liste de contrôle d'accès nommée

- Standard. Création:
  - Syntaxe: R(config)#access-list standard nom
  - Nom = alphanumérique, unique et ne peut pas commencer par un numéro.
  - Exemple: R(config)#access-list standard SMI
  - #deny 192.168.10.1 (refuser)
  - #permit 192.168.10.0 0.0.0.255 (autoriser)
- Etendue. Création:
  - Syntaxe: R(config)#ip access-list extended nom
  - Nom = alphanumérique, unique et ne peut pas commencer par un numéro.
  - R(config)#ip access-list extended FSK
  - #permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 (autoriser tout paquet IP du réseau 192.168.100.0 vers le réseau 192.168.200.0)
  - #deny TCP any any eq 23 (telnet) (refuser Telnet)
- Apliquer la liste sur une interface sortant/entrant
  - Activer la liste avec la commande #ip access-group FSK in/out
- Vérification: **#show access-lists [numéro | nom].**

Contrôle d'accès basé sur le Temps

- Ceci dit, il est important de noter qu'elles autorisent un contrôle d'accès basé sur le temps.
- L'implémentation des listes de contrôle d'accès basées sur le temps nécessite la création d'une plage horaire, qui définit certains moments de la journée et de la semaine.
- Identifiez la plage horaire par un nom, désignez-la par une fonction.
- La fonction se voit imposer des restrictions temporelles.
- Syntaxe: #time-range SMI_Temps_Acces
- #periodic Monday Friday 8:00 to 16:00
- #access-list 101 deny TCP any any eq 23 time-range SMI_Temps_Acces