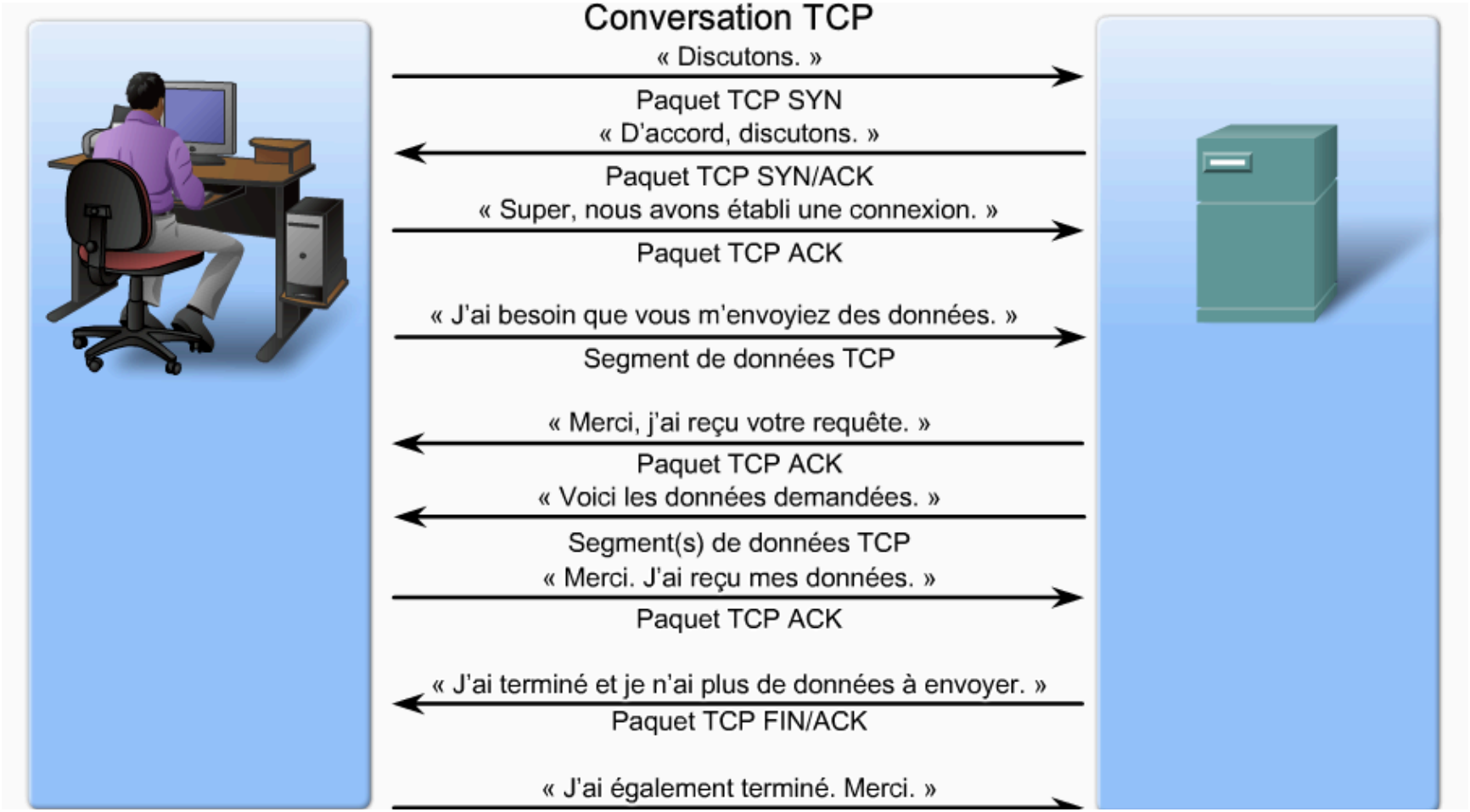
Listes de contrôle d’accès
ACL Cisco

Philippe.Arnould@univ-pau.fr

Conversation TCP

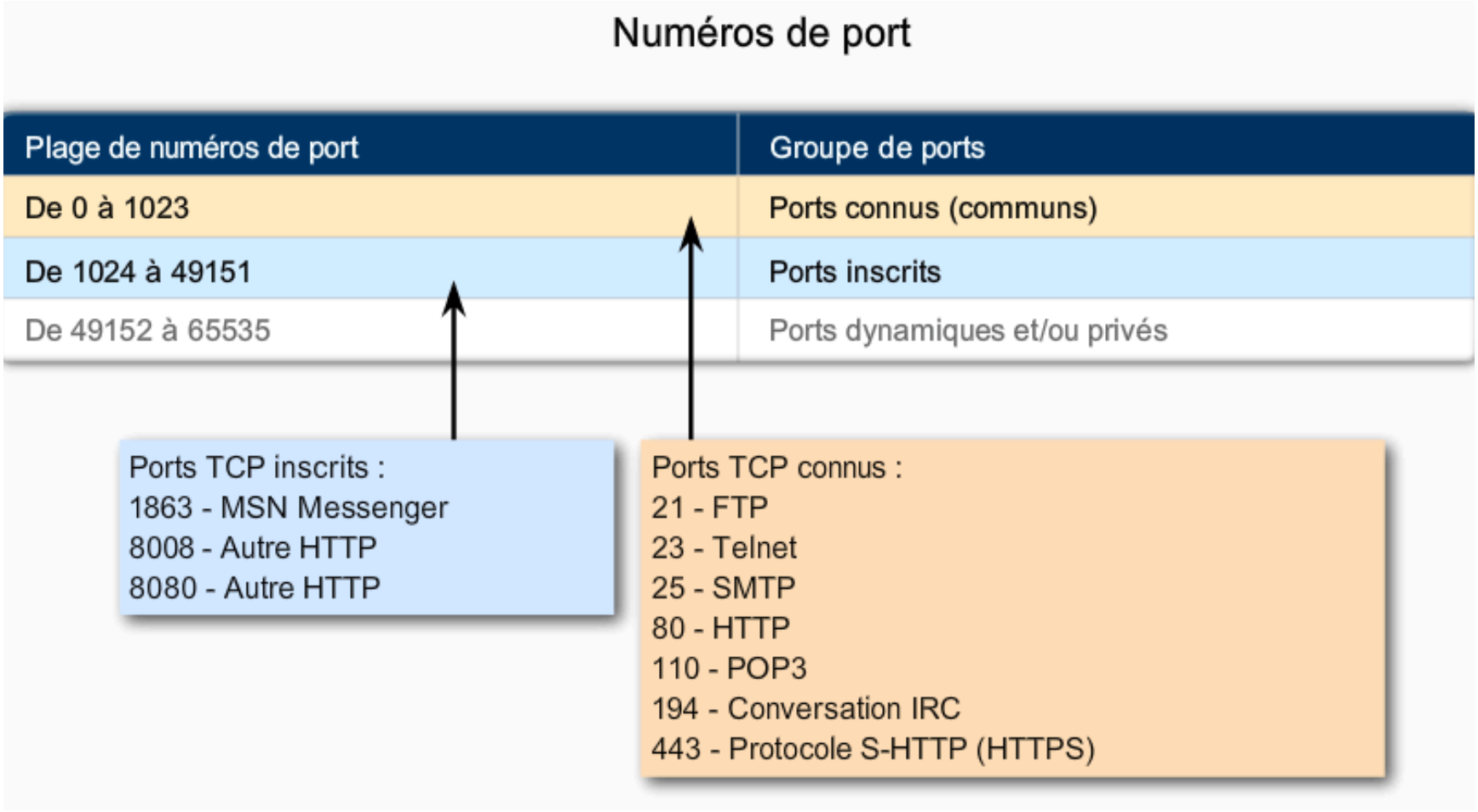


Listes des ports

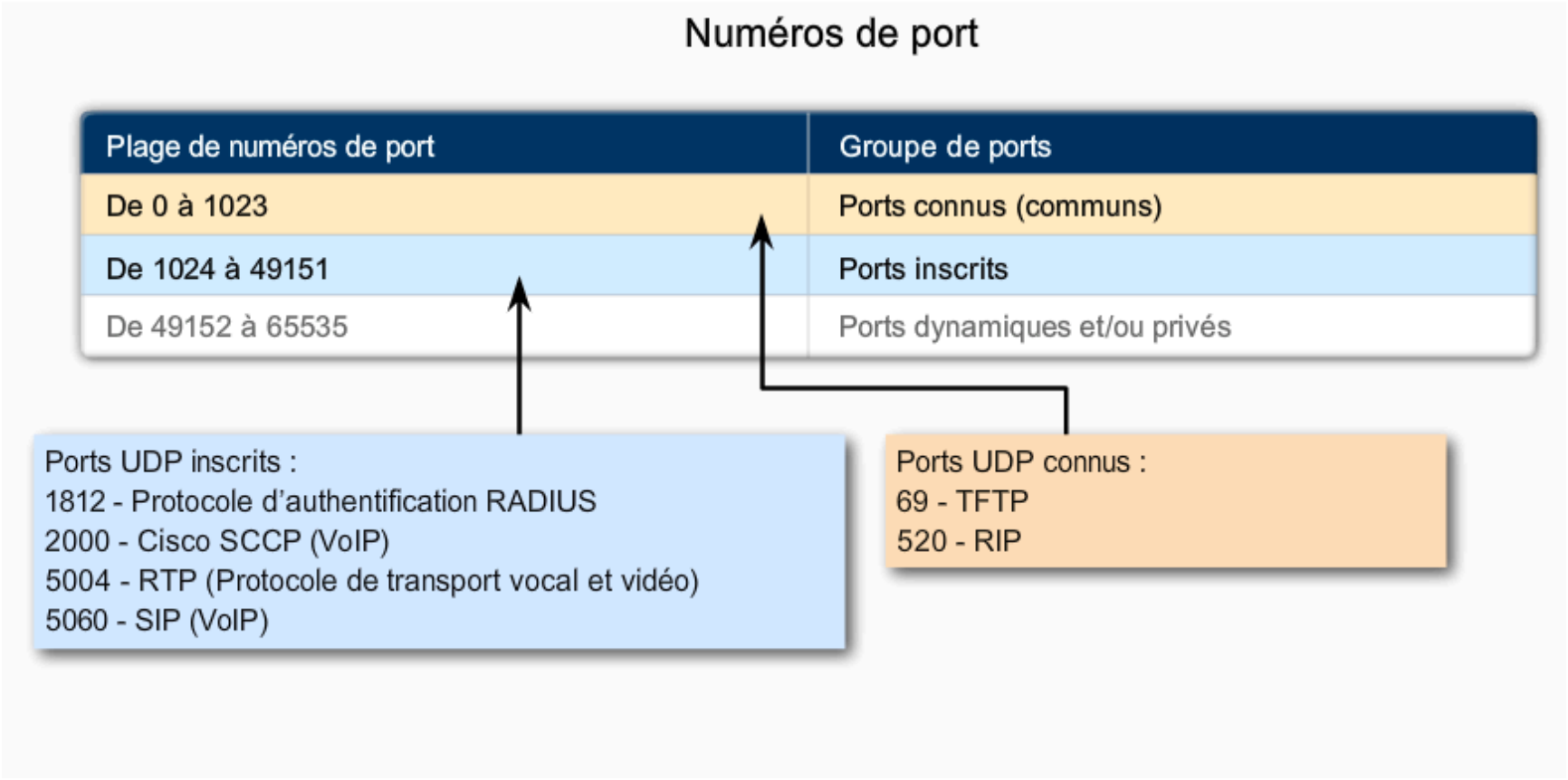
Numéros de port

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

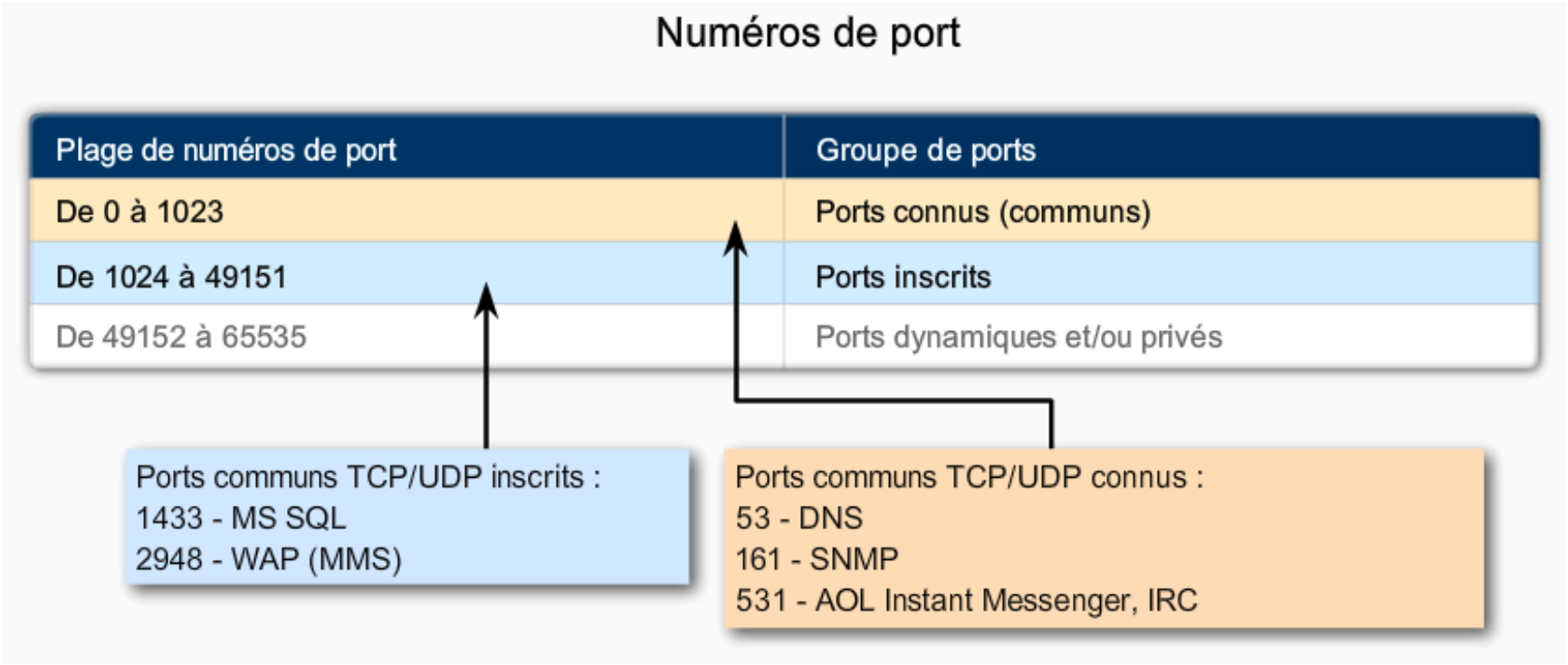
Listes des ports



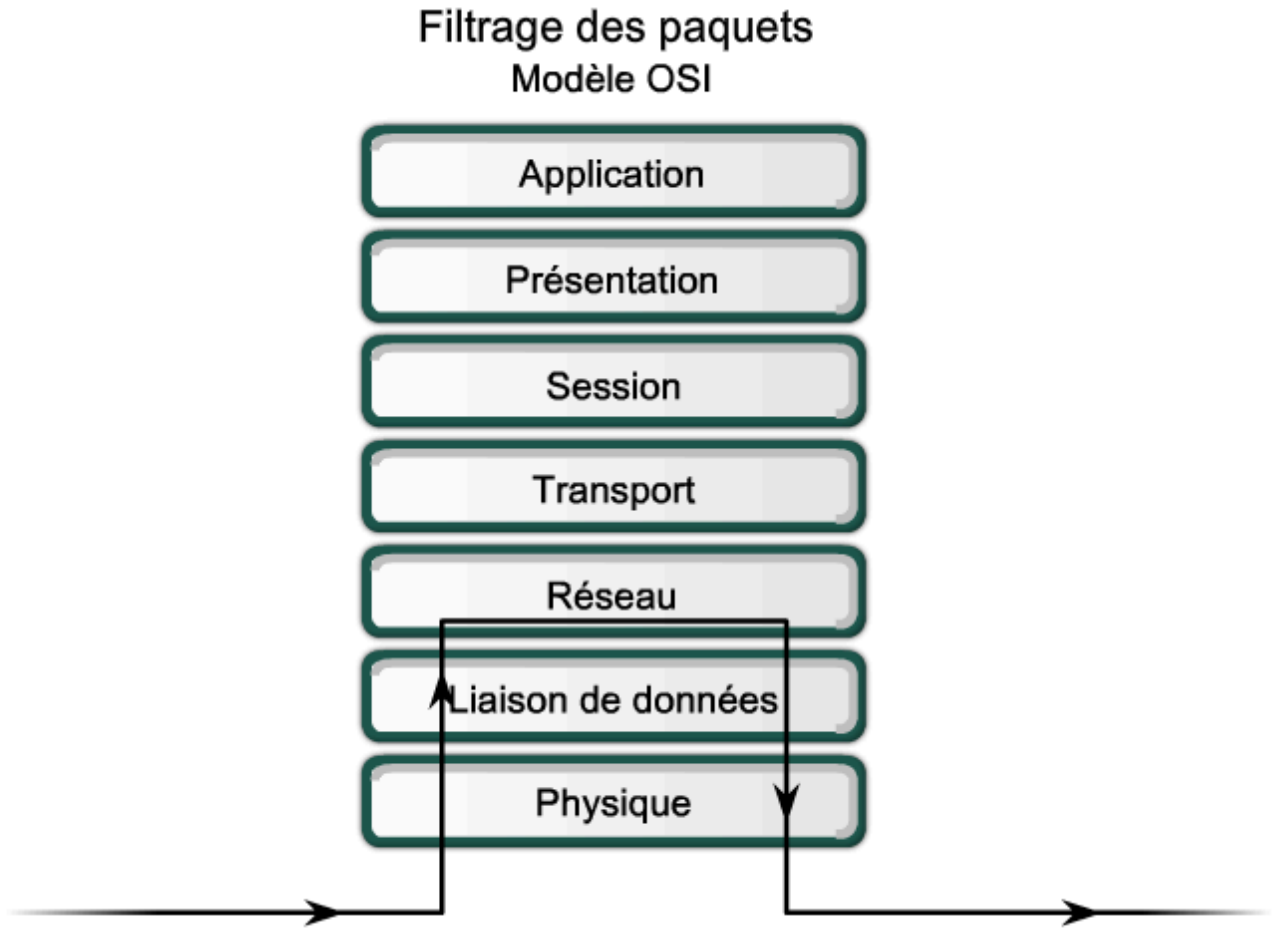
Listes des ports



Listes des ports

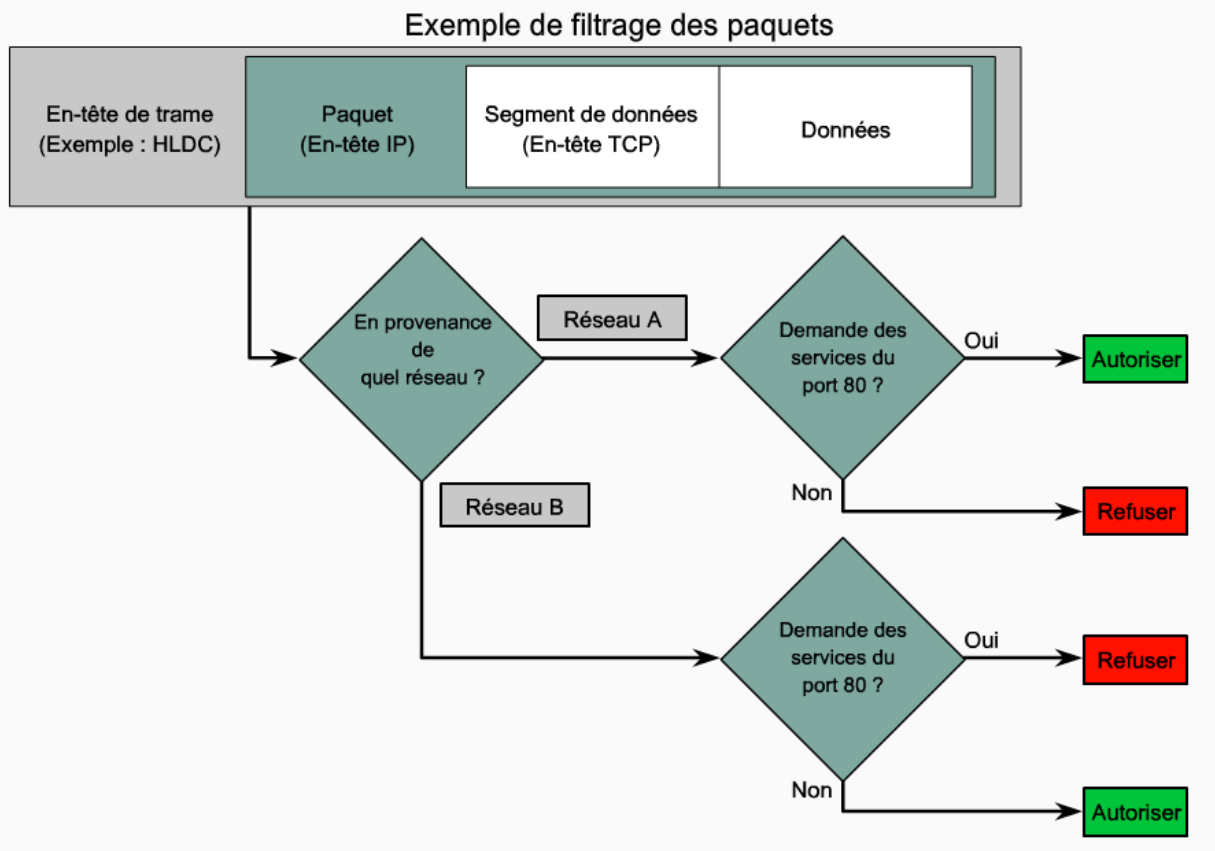


Filtrage de paquets

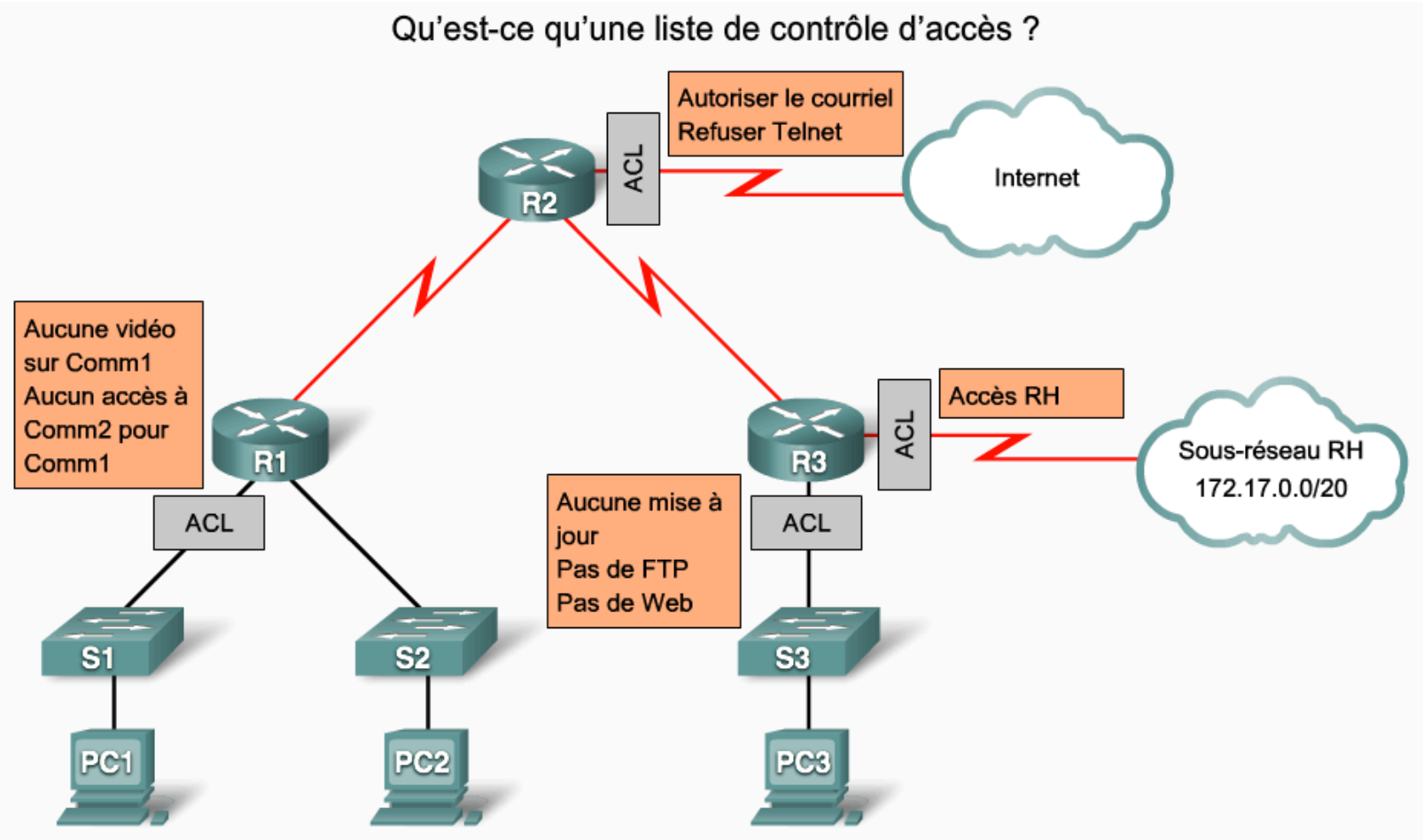


Filtrage de paquets

- « Autoriser l'accès Web aux utilisateurs du réseau A uniquement. Refuser l'accès Web aux utilisateurs du réseau B, mais leur autoriser tout autre accès »

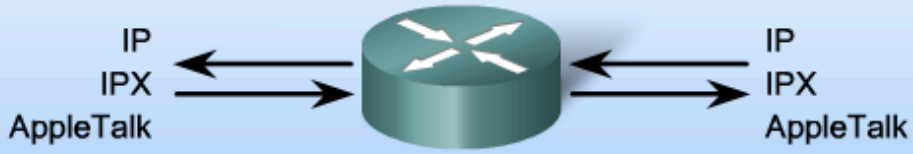


Listes de contrôle d’accès



Listes de contrôle d’accès

Filtrage du trafic avec liste de contrôle d’accès sur un routeur



Une liste par interface, par direction et par protocole

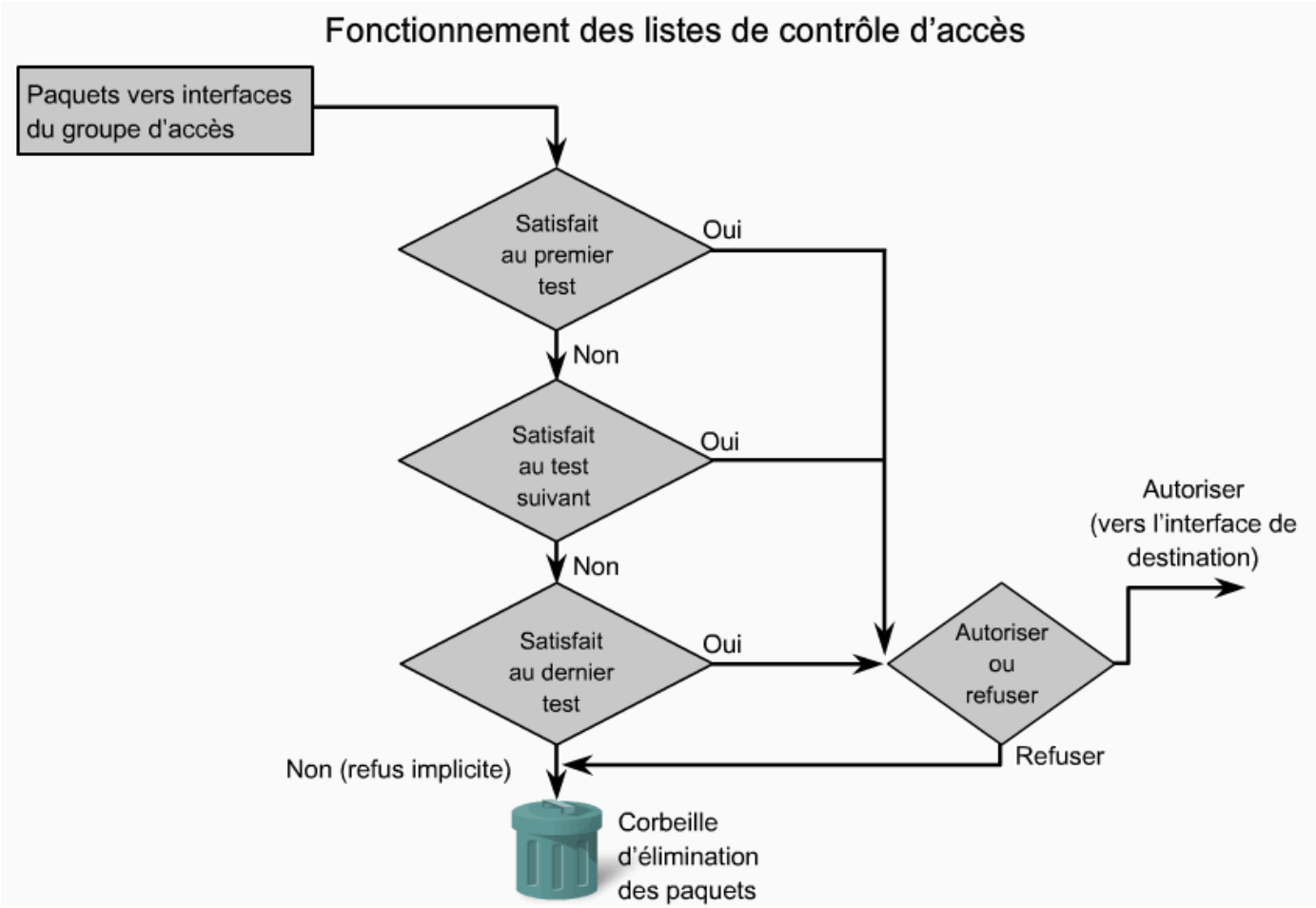
Avec deux interfaces et trois protocoles, ce routeur peut avoir un total de 12 listes de contrôle d’accès appliquées.

Règle des trois P pour l’utilisation des listes de contrôle d’accès

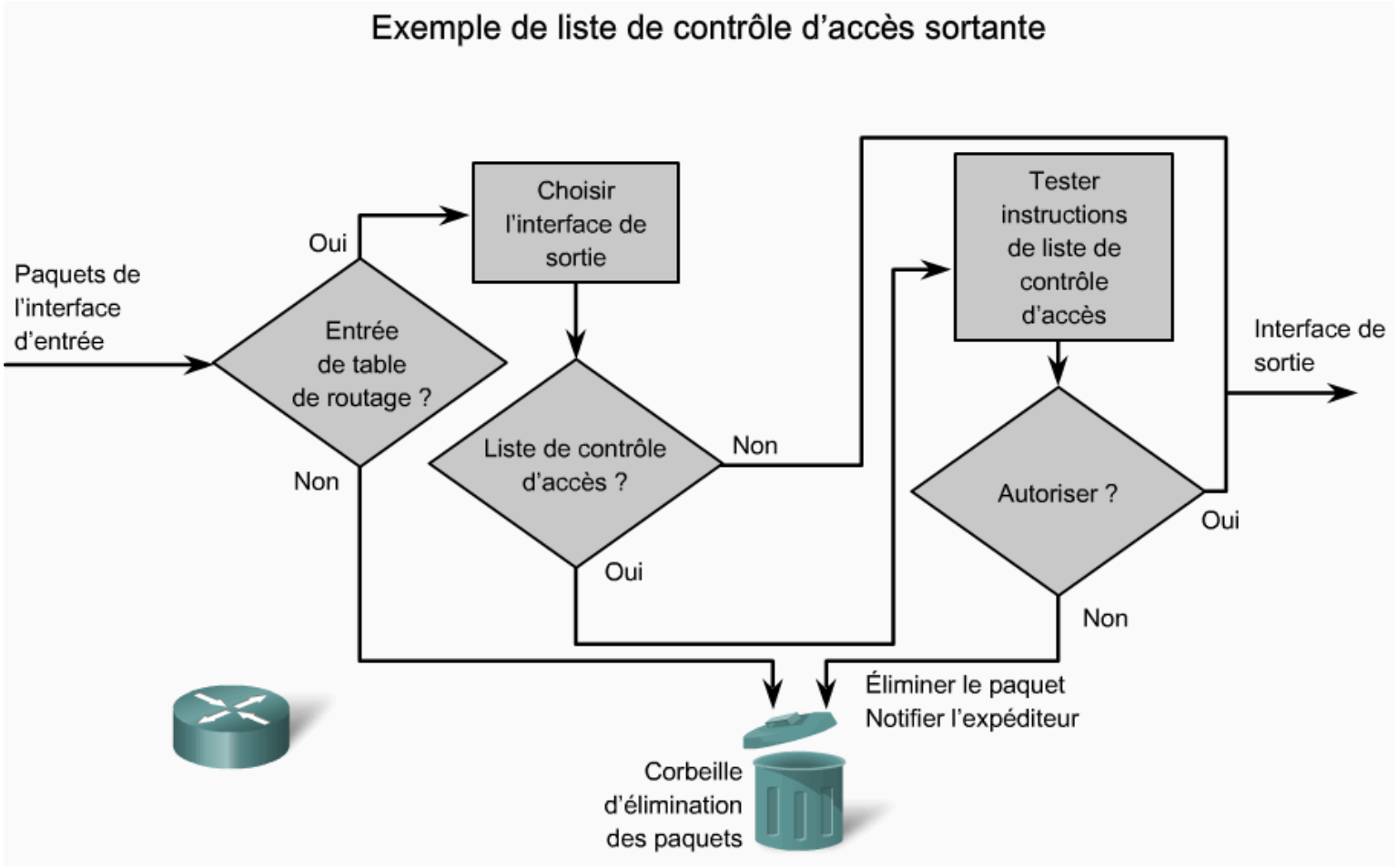
Une seule liste de contrôle d’accès est autorisée par protocole, par interface et par direction :

- Une liste de contrôle d’accès par protocole (exemple : IP ou IPX)
- Une liste de contrôle d’accès par interface (exemple : FastEthernet0/0)
- Une liste de contrôle d’accès par direction (exemple : IN ou OUT)

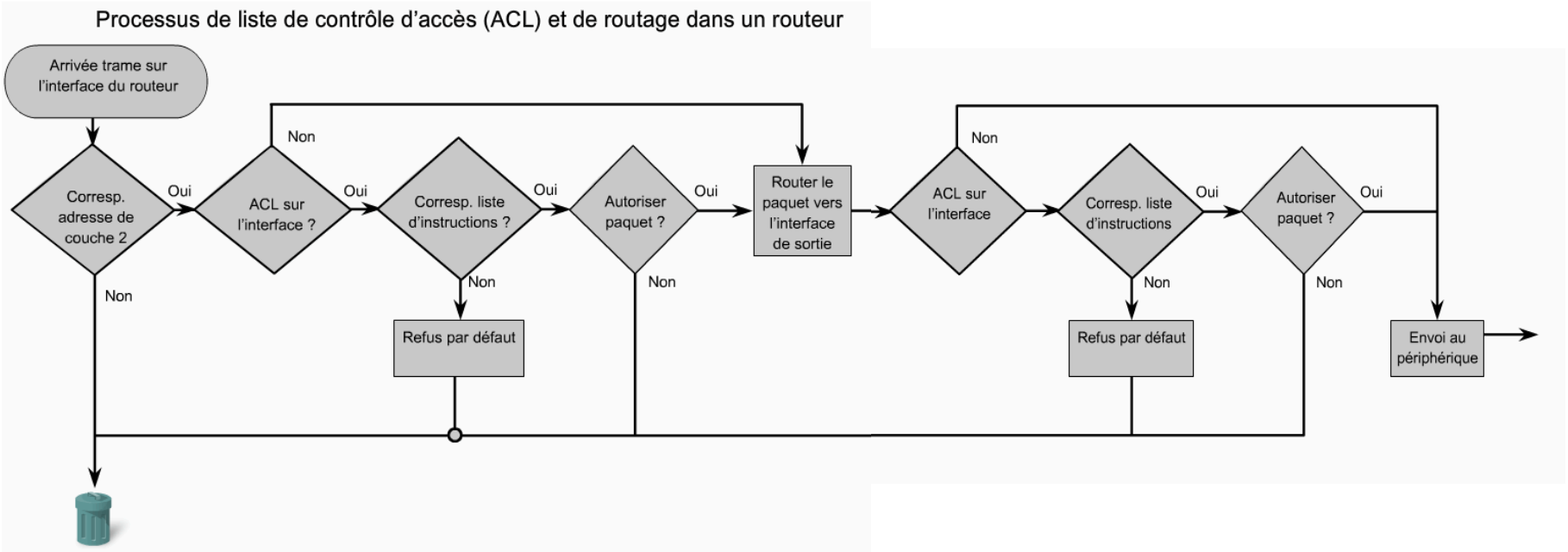
Listes de contrôle d’accès



Listes de contrôle d’accès



Listes de contrôle d’accès



Types de Listes de contrôle d’accès

Types de liste de contrôle d’accès (ACL) Cisco

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

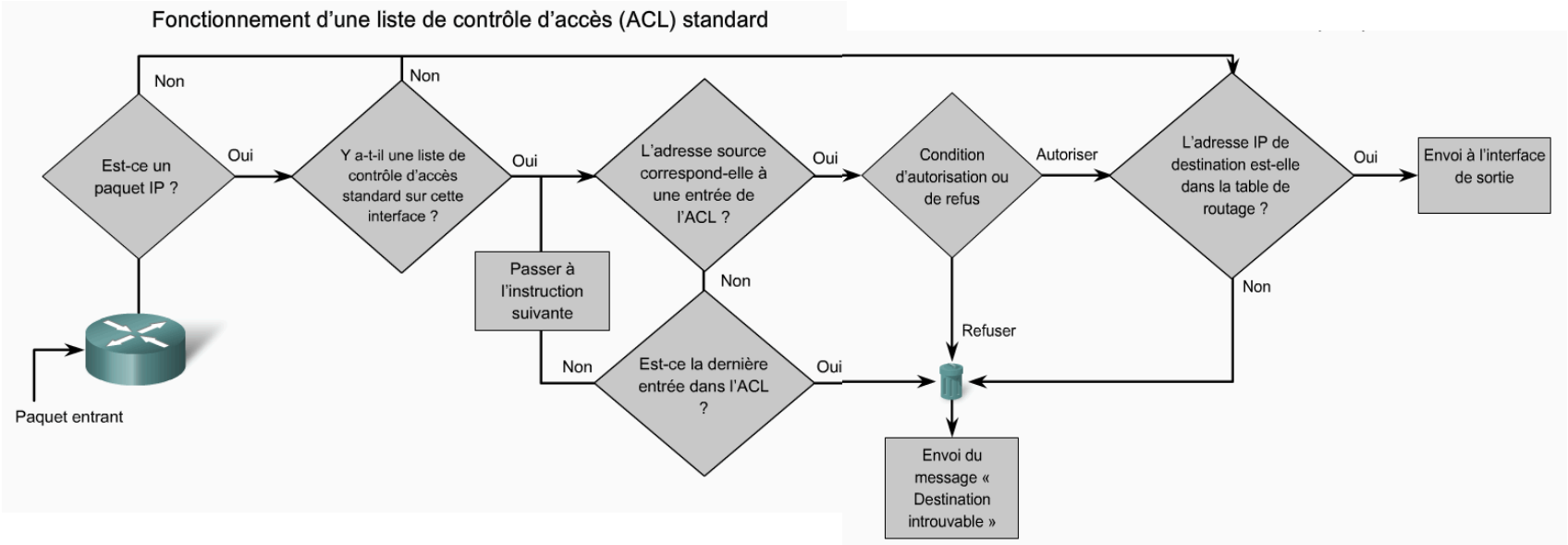
```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Les listes de contrôle d’accès étendues filtrent les paquets IP en fonction des attributs suivants :

- Adresse IP source et adresse IP de destination
- Ports TCP et UDP source et de destination
- Type de protocole (IP, ICMP, UDP, TCP ou numéro du protocole)

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

ACL standard



Listes de contrôle d’accès

Numérotation et attribution d’un nom aux listes de contrôle d’accès

Liste de contrôle d’accès numérotée :

Vous affectez un numéro en fonction du protocole à filtrer :

- (1 à 99) et (1300 à 1999) : liste de contrôle d’accès IP standard
- (100 à 199) et (2000 à 2699) : liste de contrôle d’accès IP étendue

Liste de contrôle d’accès nommée :

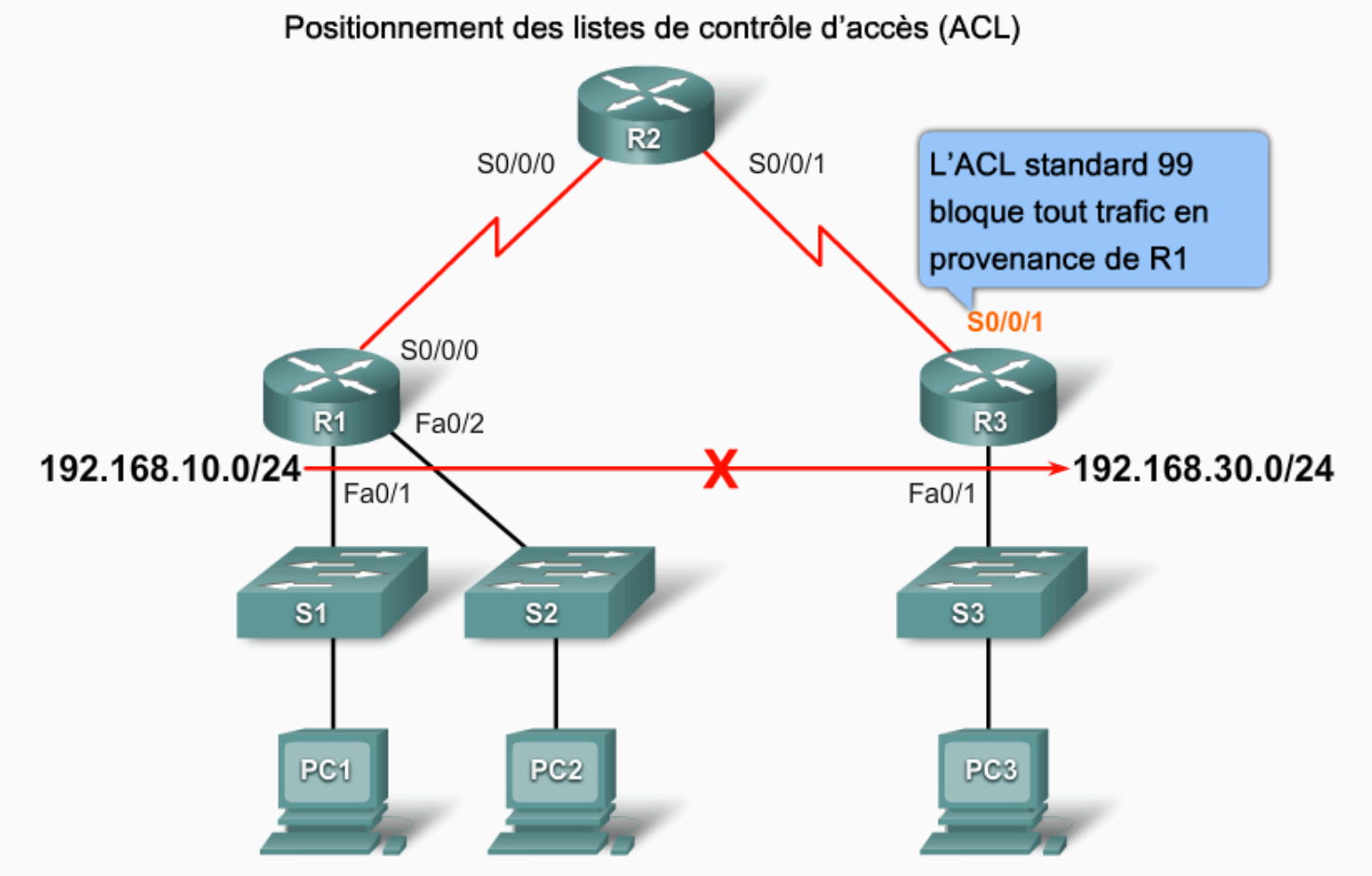
Vous affectez un nom en indiquant celui de la liste de contrôle d’accès :

- Les noms peuvent comporter des caractères alphanumériques.
- Nous vous recommandons d’écrire le nom en MAJUSCULES.
- Les noms ne peuvent pas contenir d’espaces ou de marques de ponctuation ; ils doivent commencer par une lettre.
- Vous pouvez ajouter ou supprimer des entrées dans la liste de contrôle d’accès.

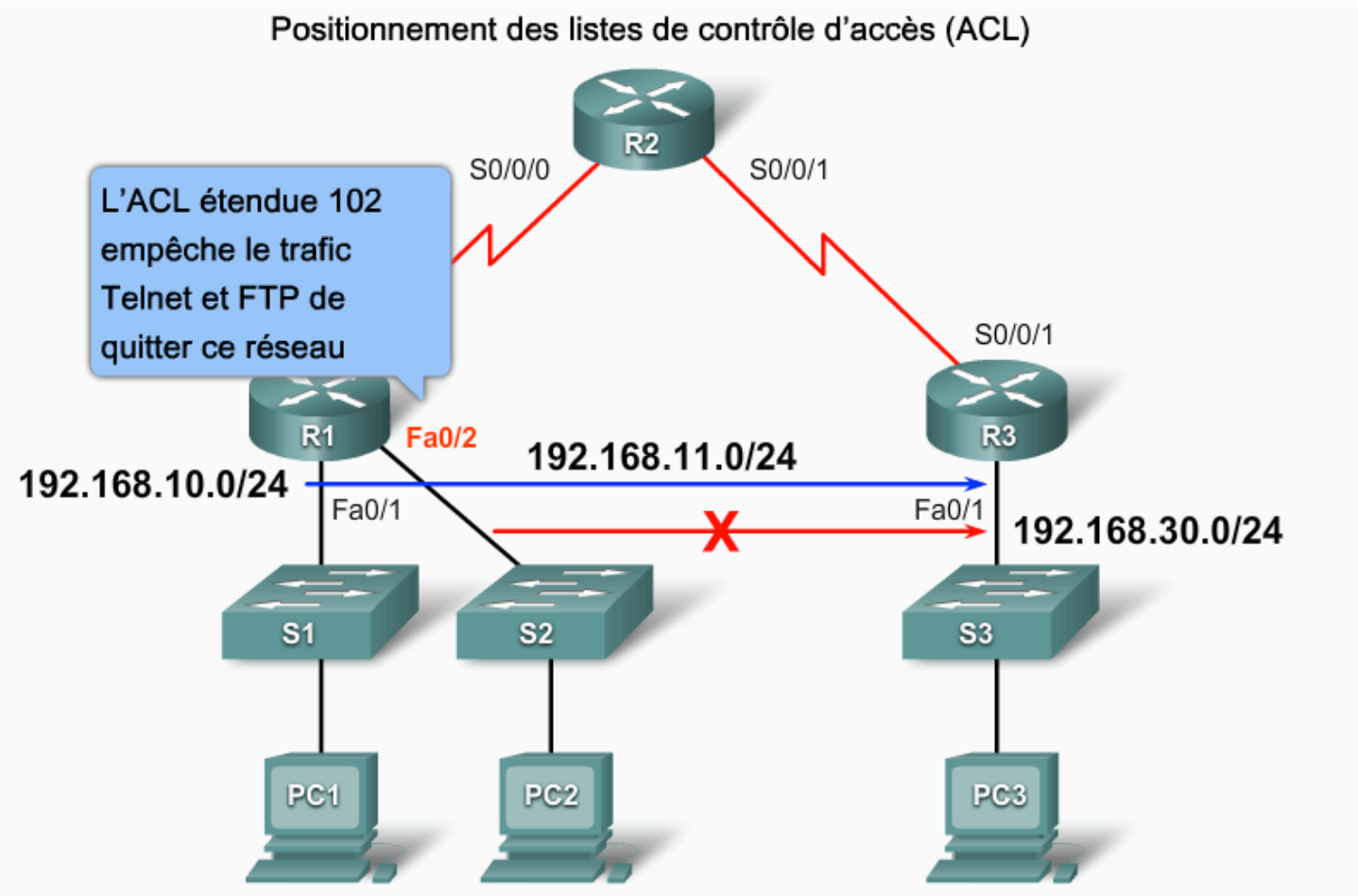
Positionnement des liste de contrôle d'accès

- Placez **les listes de contrôle d'accès étendues** le plus près possible de la source du trafic refusé. Ainsi, le trafic indésirable est filtré sans traverser l'infrastructure réseau.
- Étant donné que **les listes de contrôle d'accès standard** ne précisent pas les adresses de destination, placez-les le plus près possible de la destination.

Positionnement des liste de contrôle d'accès



Positionnement des liste de contrôle d'accès



Listes de contrôle d’accès

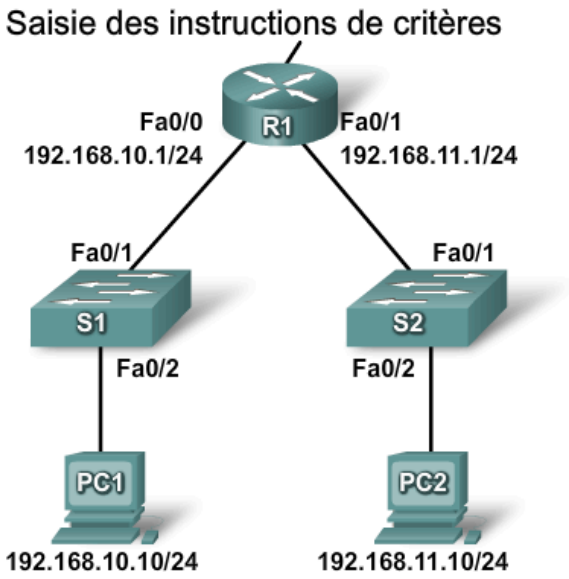
Méthodes recommandées pour les listes de contrôle d’accès

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.

Positionnement des liste de contrôle d'accès

- Exercice

Configuration une Listes de contrôle d'accès standard



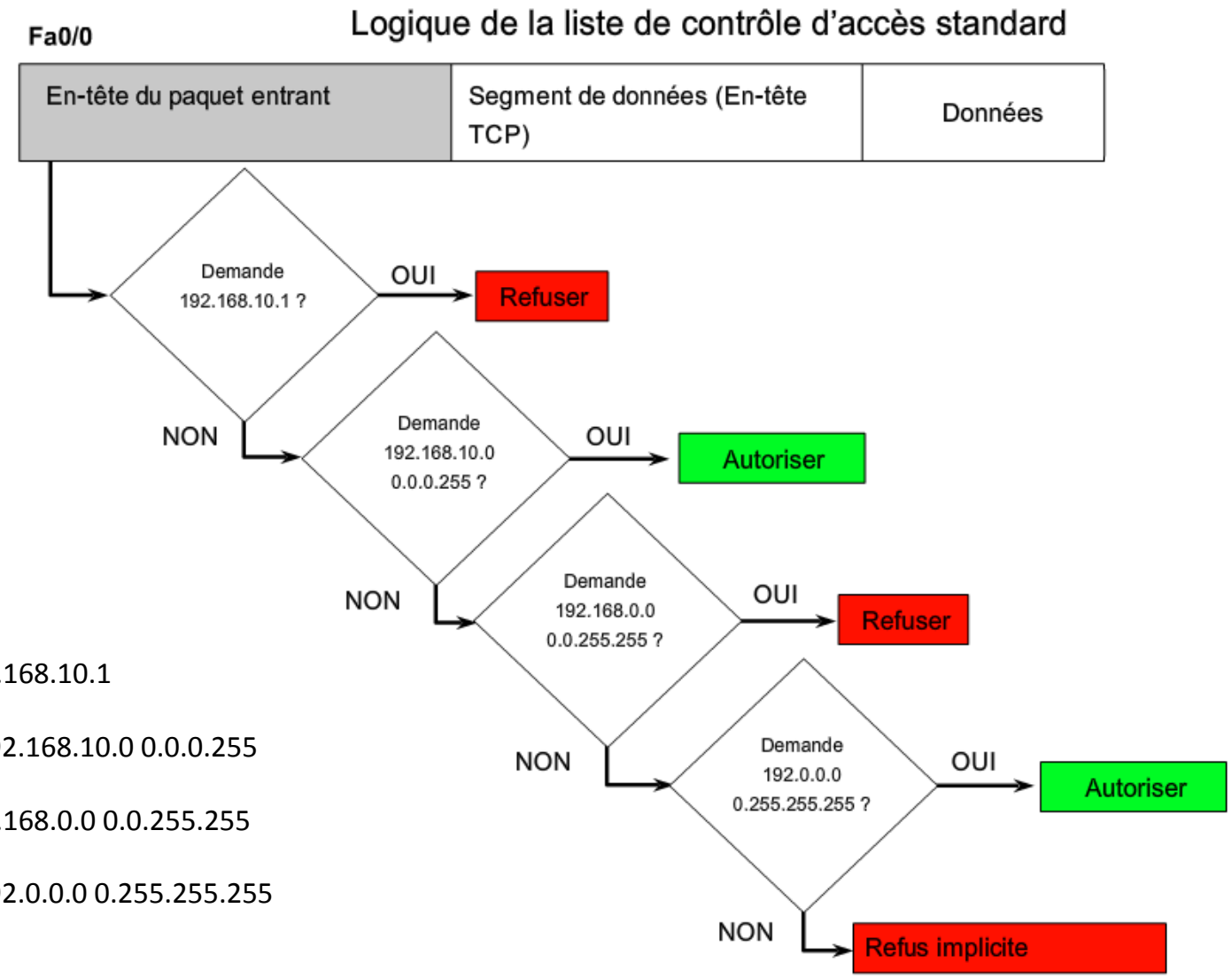
ACL 101

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

Listes de contrôle d’accès standard



- access-list 2 deny 192.168.10.1
- access-list 2 permit 192.168.10.0 0.0.0.255
- access-list 2 deny 192.168.0.0 0.0.255.255
- access-list 2 permit 192.0.0.0 0.255.255.255

Listes de contrôle d’accès standard

Documentation d’une liste de contrôle d’accès

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 10 remark Permit hosts from the 192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0
R1(config)# exit
R1#
*Oct 25 20:12:13.781: %SYS-5-CONFIG_I: Configured from console by consoleshow ?
R1# show run
Building configuration...
!
<output omitted>
!
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0
!
<output omitted>
```

Listes de contrôle d’accès standard

Suppression d’une liste de contrôle d’accès

```
R1# show access-list
Standard IP access list 10
    10 permit 192.168.10.0
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1#
*Oct 25 19:59:41.142: %SYS-5-CONFIG_I: Configured from console by console
R1# show access-list

R1#
```

Listes de contrôle d'accès standard

Procédure de configuration des listes de contrôle d'accès standard

Étape 1 Utilisation de la commande de configuration globale **access-list** pour créer une entrée dans une liste de contrôle d'accès IPv4 standard.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

Entrez la commande globale **no access-list** pour supprimer toute la liste de contrôle d'accès. L'exemple d'instruction fait correspondre toutes les adresses commençant par 192.168.10.x. Utilisez l'option **remark** pour ajouter une description à la liste de contrôle d'accès.

Étape 2 Utilisation de la commande de configuration d'interface pour sélectionner une interface à laquelle appliquer la liste de contrôle d'accès.

```
R1(config)# interface FastEthernet 0/0
```

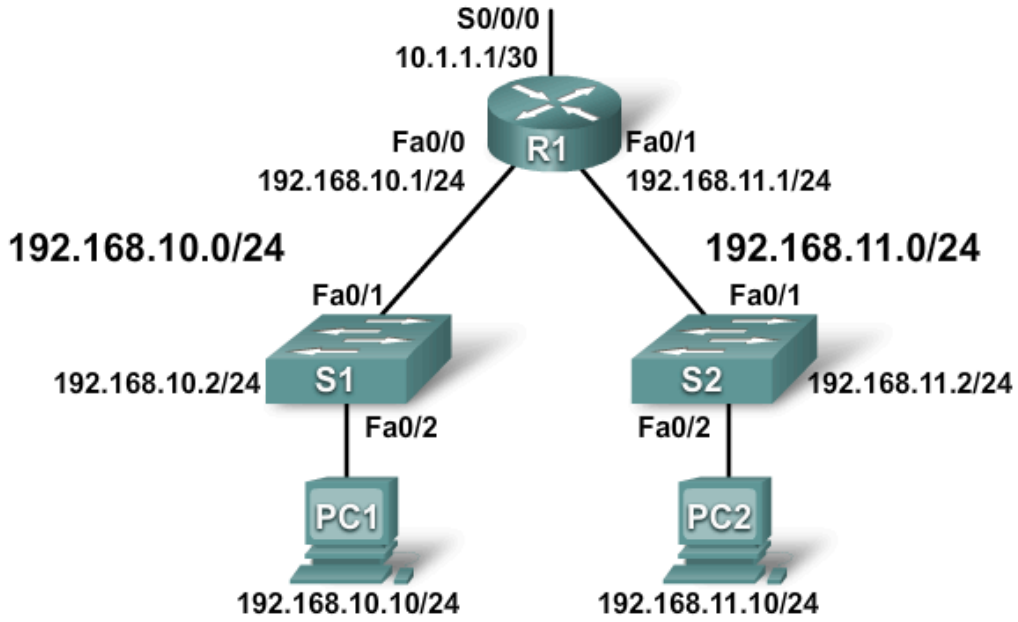
Étape 3 Utilisation de la commande de configuration d'interface **ip access-group** pour activer la liste de contrôle d'accès existante sur une interface.

```
R1(config-if)# ip access-group 1 out
```

Pour supprimer une liste de contrôle d'accès IP d'une interface, entrez la commande **no ip access-group** sur l'interface. Cet exemple active la liste de contrôle d'accès 1 IPv4 standard sur l'interface, tel un filtre de sortie.

Listes de contrôle d’accès standard

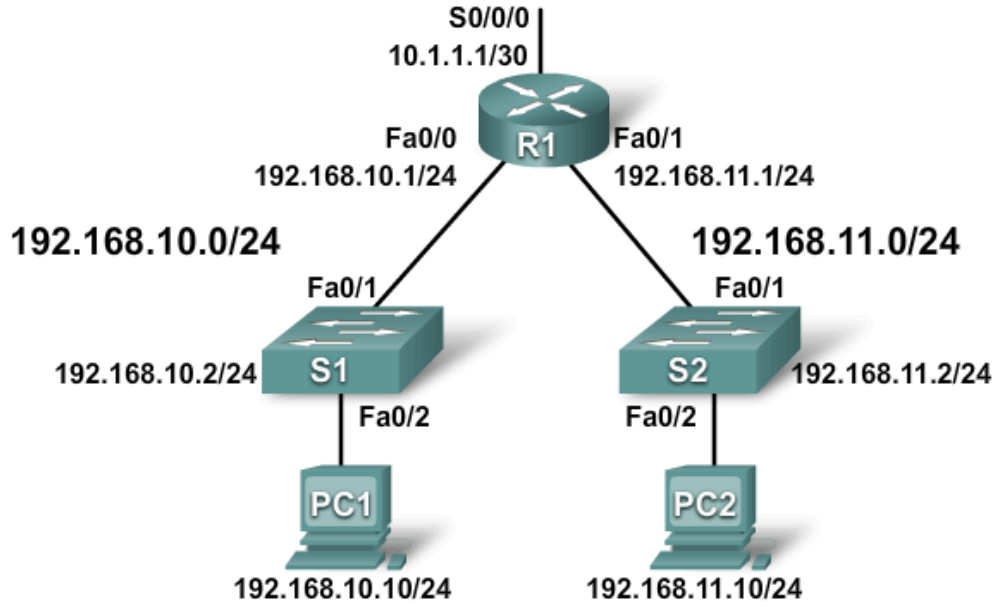
Liste de contrôle d’accès standard pour autoriser mon réseau uniquement




```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 1 out
```

Listes de contrôle d’accès standard

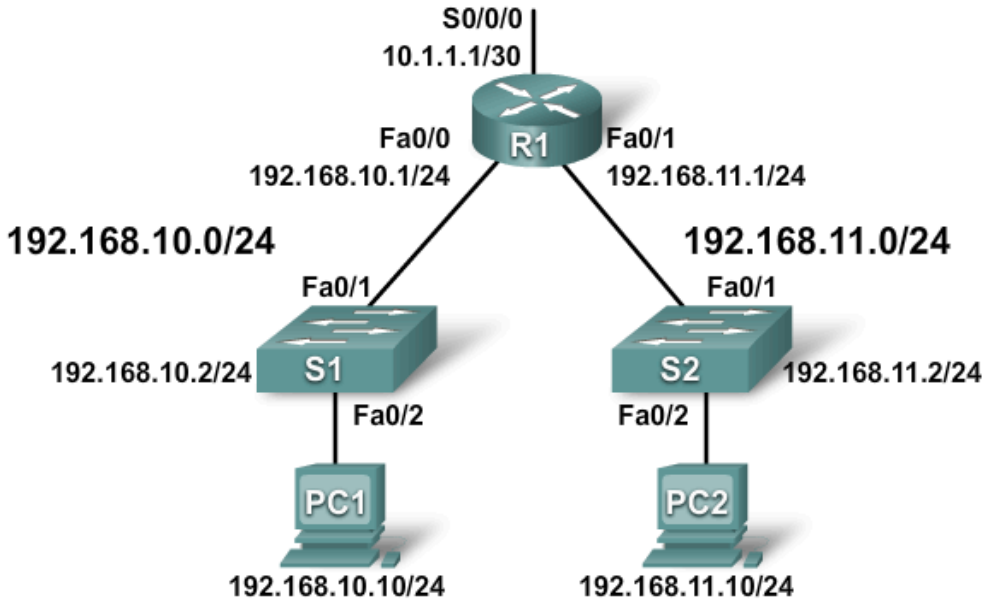
Liste de contrôle d’accès standard pour refuser un hôte spécifique




```
R1(config)#no access-list 1
R1(config)#access-list 1 deny 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface S0/0/0
R1(config-if)#ip access-group 1 out
```

Listes de contrôle d’accès standard

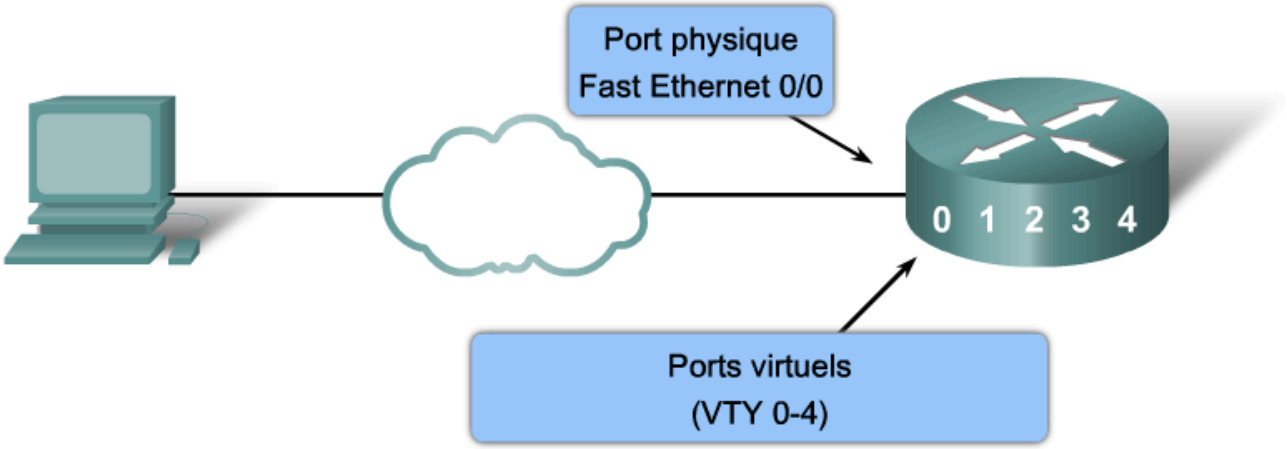
Liste de contrôle d’accès standard pour refuser un sous-réseau spécifique




```
R1(config)#no access-list 1
R1(config)#access-list 1 deny 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#interface S0/0/0
R1(config-if)#ip access-group 1 out
```

Listes de contrôle d’accès standard

Listes de contrôle d’accès standard pour contrôler l’accès au terminal virtuel




```
R1(config)#access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 21 permit 192.168.11.0 0.0.0.255
R1(config)#access-list 21 deny any

R1(config)#line vty 0 4
R1(config-line)#login
R1(config-line)#password secret
R1(config-line)#access-class 21 in
```

Listes de contrôle d’accès standard

Édition des listes de contrôle d’accès numérotées

Étape 1	R1#**show running-config | include access-list** **access-list 20 permit 192.168.10.100** **access-list 20 deny 192.168.10.0 0.0.0.255**
Étape 2	**access-list 20 permit 192.168.10.11** **access-list 20 deny 192.168.10.0 0.0.0.255**
Étape 3	R1#**conf t** Enter configuration commands, one per line. End with CTRL/Z. R1(config)#**no access-list 20** R1(config)#**access-list 20 permit 192.168.10.100** R1(config)#**access-list 20 deny 192.168.10.0 0.0.0.255**

Listes de contrôle d’accès standard

Commentaires sur les listes de contrôle d’accès

Exemple 1 :

```
Router(config)# access-list 1 remark Permit only Jones workstation through
Router(config)# access-list 1 permit 192.168.10.13
Router(config)# access-list 1 remark Do not allow Smith through
Router(config)# access-list 1 deny 1 192.168.10.14
```

Exemple 2 :

```
Router(config)# ip access-list extended TELNETTING
Router(config-ext-nacl)# remark Do not allow Jones workstation to Telnet
Router(config-ext-nacl)# deny tcp host 192.168.10.13 any eq telnet
```

Listes de contrôle d’accès standard

Exemple de liste de contrôle d’accès nommée

```
Router(config)# ip access-list [standard | extended] name
```

- La chaîne du nom alphanumérique doit être unique et ne peut pas commencer par un numéro

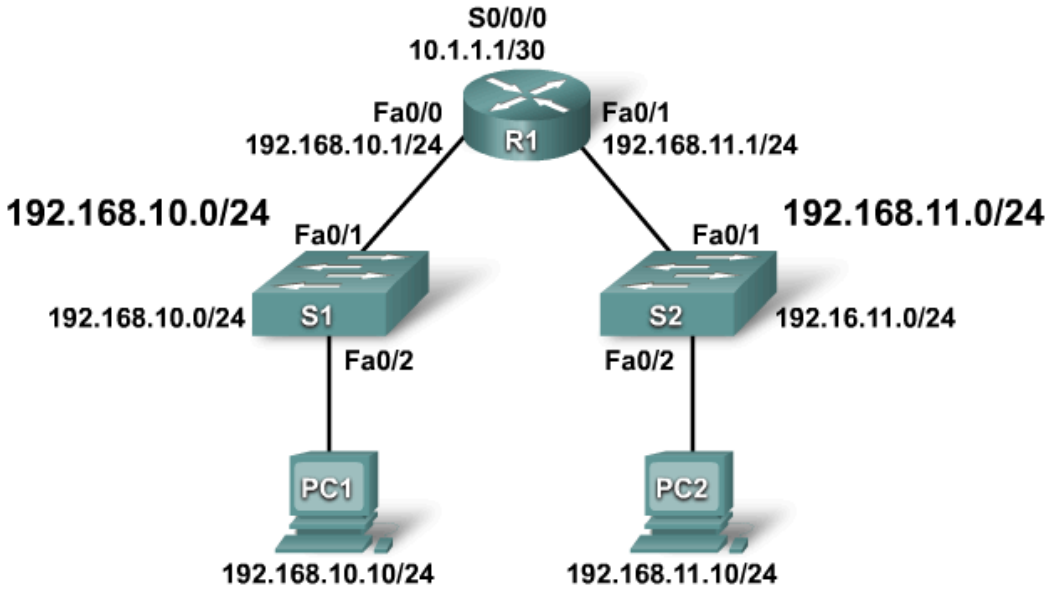
```
Router(config-std-nacl)# [permit | deny | remark] {source [source-wildcard]} [log]
```

```
Router(config-if)#ip access-group name [in | out]
```

- Active la liste de contrôle d’accès IP nommée sur une interface

Listes de contrôle d’accès standard

Exemple de liste de contrôle d’accès nommée




```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
```

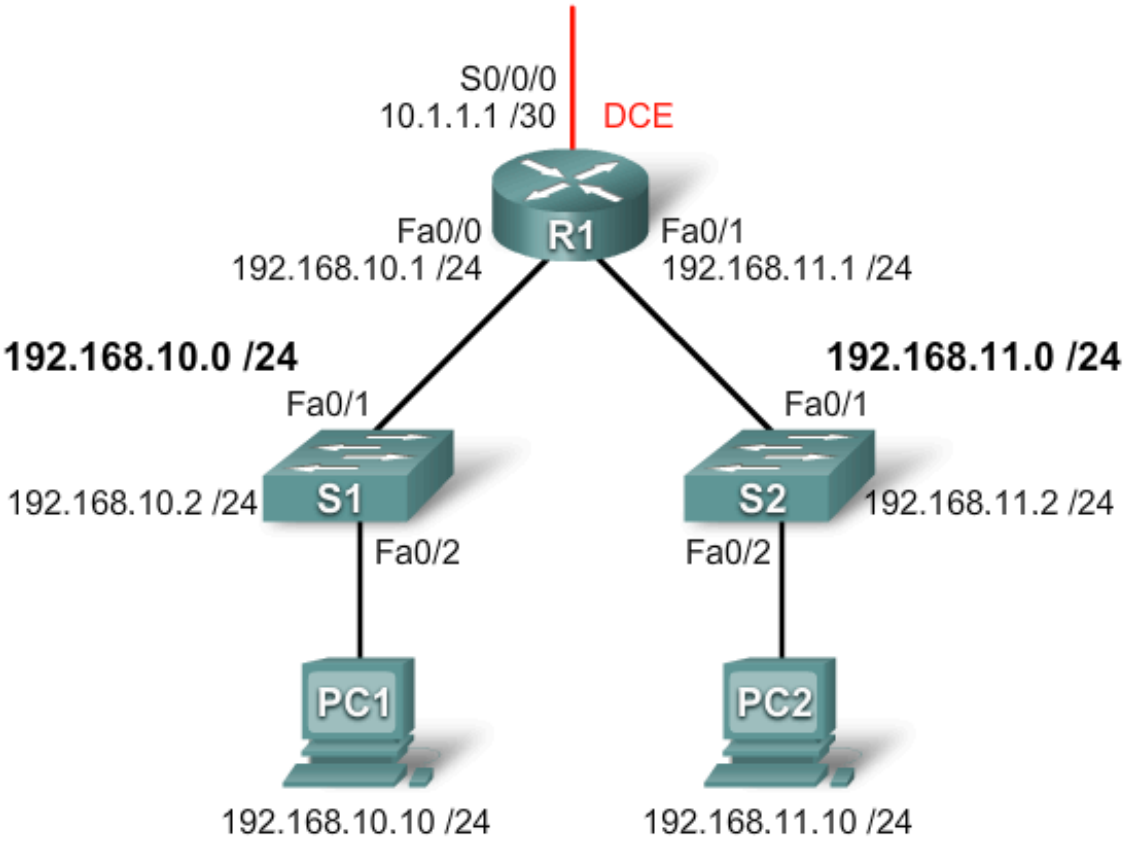
Listes de contrôle d’accès standard

Contrôle des instructions de listes de contrôle d’accès

```
R1# show access-lists { numéro-liste-accès|nom }
```

```
R1# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
    20 permit tcp host 192.168.10.2 any eq ftp
    30 permit tcp host 192.168.10.2 any eq ftp-data
```

Listes de contrôle d’accès standard



Listes de contrôle d’accès standard

```
R1# show access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard WEBSERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Listes de contrôle d'accès étendues

- Pour un filtrage du trafic plus précis :
  - les listes de contrôle d'accès étendues
  - numérotées entre 100 et 199, 2000 et 2699 (maximum de 799 listes)
  - On peut attribuer un nom aux listes de contrôle d'accès étendues.

Listes de contrôle d’accès étendues

Exemples de listes de contrôle d’accès étendues

Utilisation des numéros de port

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Utilisation des mots clés

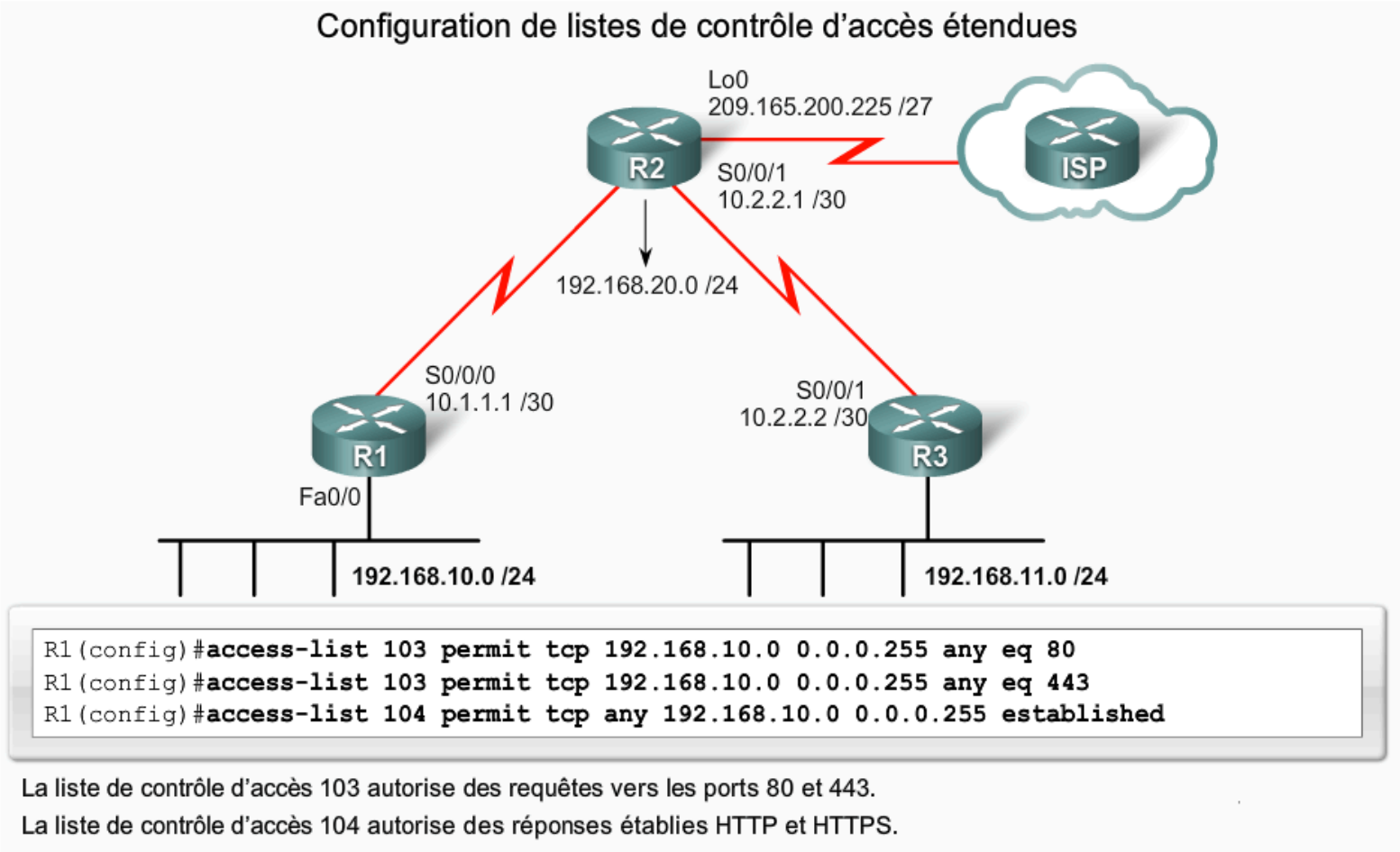
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Listes de contrôle d’accès étendues

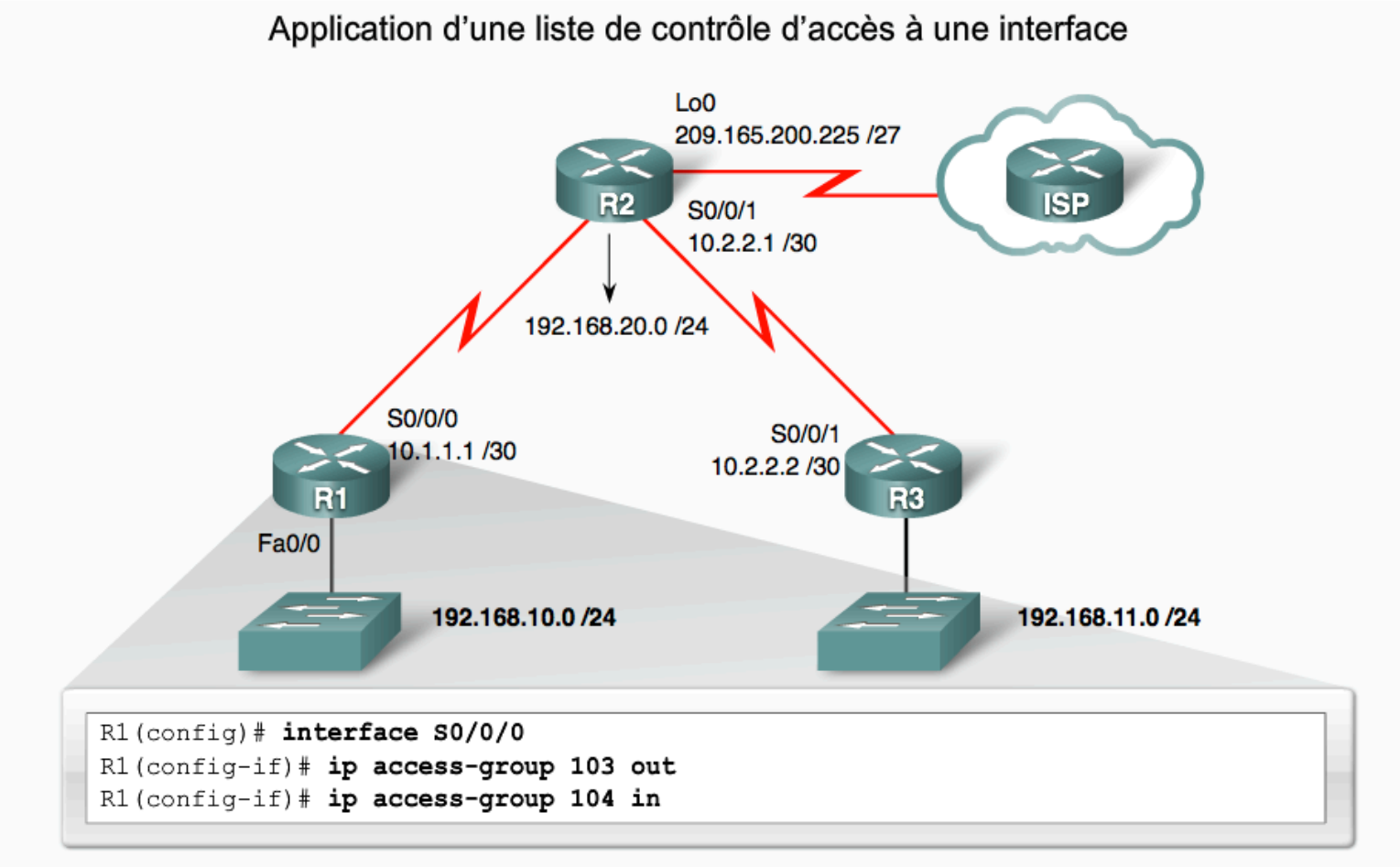
```
R1(config)#access-list 101 permit tcp any eq ?

  <0-65535> Port number
  bgp Border Gateway Protocol (179)
  chargen Character generator (19)
  cmd Remote commands (rcmd, 514)
  daytime Daytime (13)
  discard Discard (9)
  domain Domain Name Service (53)
  drip Dynamic Routing Information Protocol (3949)
  echo Echo (7)
  exec Exec (rsh, 512)
  finger Finger (79)
  ftp File Transfer Protocol (21)
  ftp-data FTP data connections (20)
  gopher Gopher (70)
  hostname NIC hostname server (101)
  ident Ident Protocol (113)
  irc Internet Relay Chat (194)
  klogin Kerberos login (543)
  kshell Kerberos shell (544)
  login Login (rlogin, 513)
  lpd Printer service (515)
  nntp Network News
```

Listes de contrôle d’accès étendues

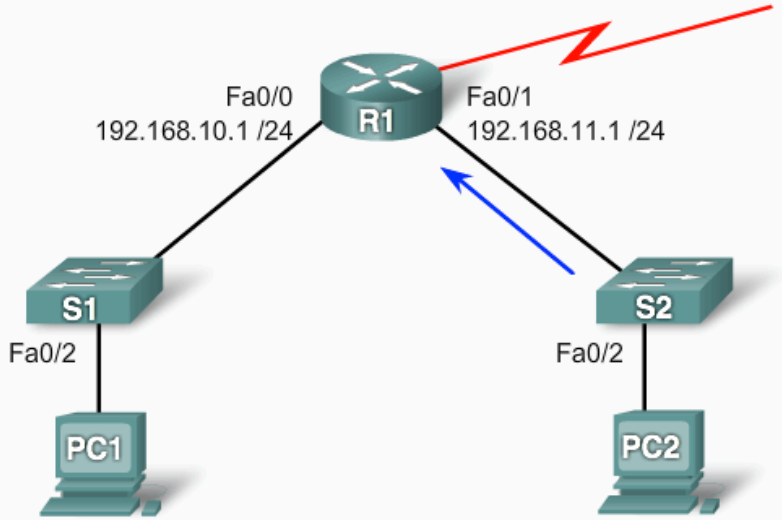


Listes de contrôle d’accès étendues



Listes de contrôle d’accès étendues

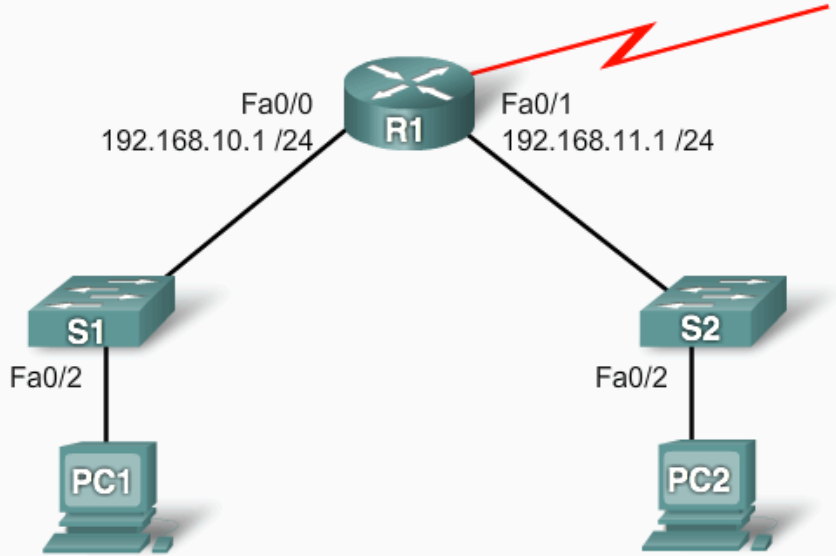
Liste de contrôle d’accès étendue pour refuser le trafic FTP des sous-réseaux




```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 21
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 20
R1(config)# access-list 101 permit ip any any
R1(config)# interface Fa0/1
R1(config-if)# ip access-group 101 in
```

Listes de contrôle d’accès étendues

Liste de contrôle d’accès étendue pour refuser le trafic Telnet uniquement du sous-réseau

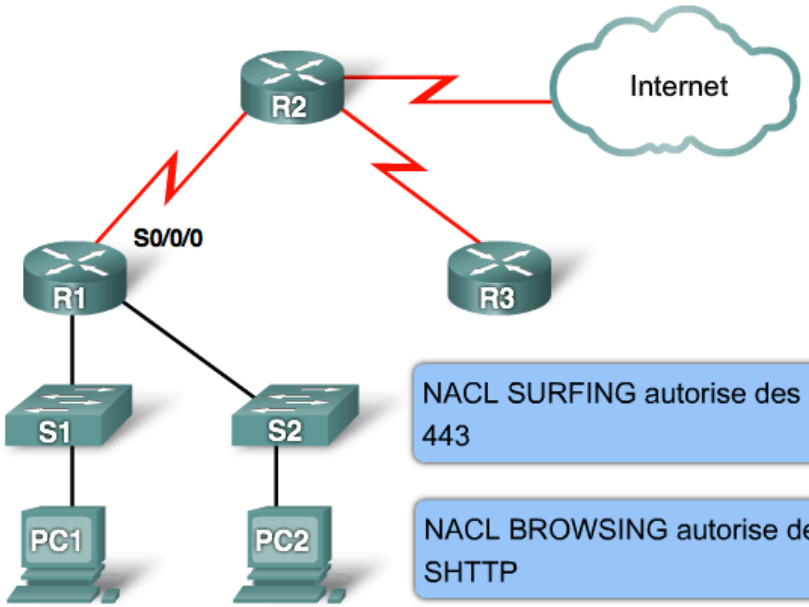



```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255  any eq 23
R1(config)#access-list 101 permit ip any any

R1(config)# interface Fa0/0
R1(config-if)#ip access-group 101 out
```

Listes de contrôle d’accès étendues nommées

Configuration de listes de contrôle d’accès étendues nommées



NACL SURFING autorise des requêtes vers les ports 80 et 443

NACL BROWSING autorise des réponses établies HTTP et SHTTP

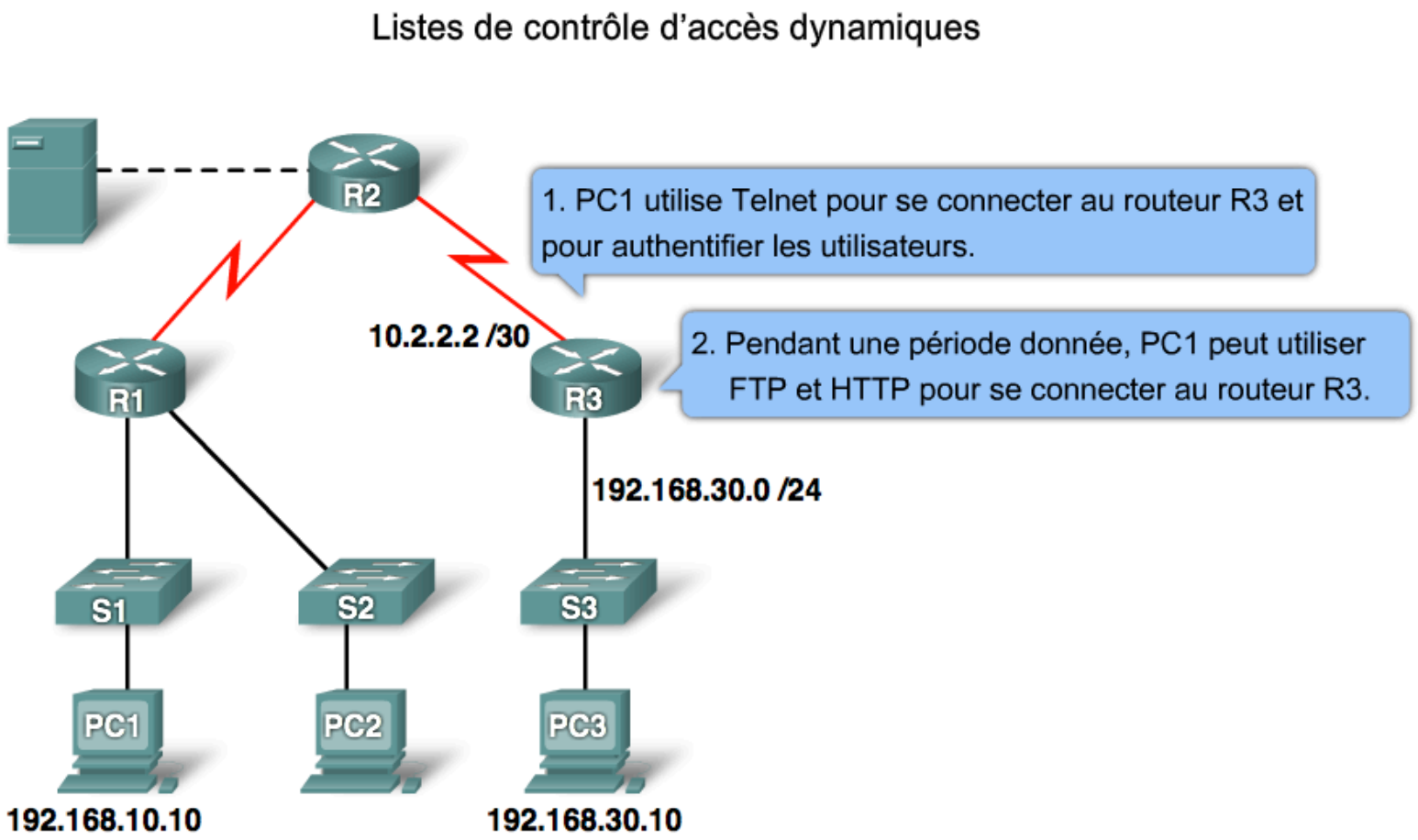
```
R1(config)# access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.225 any eq 443
R1(config)# access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
```

Listes de contrôle d’accès complexes

Types de listes de contrôle d’accès complexes

Listes de contrôle d’accès complexes	Description
Listes de contrôle d’accès dynamiques (verrou)	Les utilisateurs souhaitant traverser le routeur sont bloqués tant qu’ils n’utilisent pas Telnet pour se connecter au routeur et tant qu’ils n’ont pas été authentifiés.
Listes de contrôle d’accès réflexives	Autorisent le trafic sortant et limitent le trafic entrant en réponse aux sessions provenant du routeur lui-même.
Listes de contrôle d’accès basées sur le temps	Autorisent le contrôle d’accès en fonction du jour et de la semaine.

Listes de contrôle d’accès dynamiques



Listes de contrôle d’accès dynamiques

Étape 1	`R3(config)#username Student password 0 cisco`

Étape 2	`R3(config)# access-list 101 permit any host 10.2.2.2 eq telnet`
	`R3(config)#access-list 101 dynamic testlist timeout 15`
	`permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255`

Étape 3	`R3(config)#interface serial 0/0/1` `R3(config-if)# ip access-group 101 in`

Étape 4	`R3(config)#line vty 0 4`
	`R3(config-line)# login local`
	`R3(config-line)#  autocommand access-enable host timeout 5`

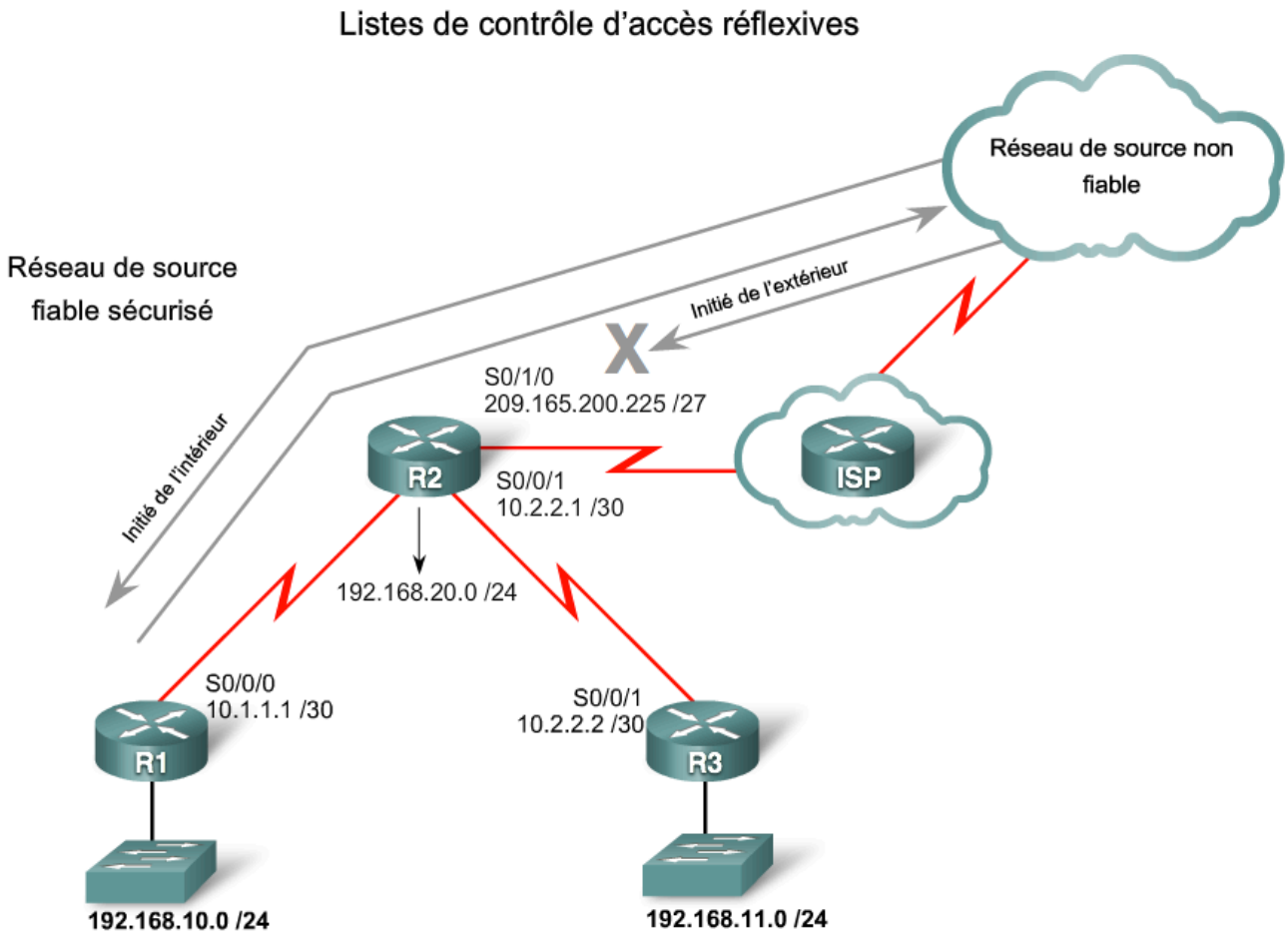
Listes de contrôle d’accès réflexives

- imposent au trafic de réponse issu de la destination d’un paquet sortant connu et récent d’accéder à la source de ce paquet.
- meilleur contrôle du trafic autorisé sur le réseau et augmentation des capacités des listes de contrôle d’accès étendues.

Listes de contrôle d'accès réflexives

- filtrage de session plus efficace qu'une Listes de contrôle d'accès étendue, qui utilise le paramètre **established**
- Bien que de concept comparable au paramètre established, les listes de contrôle d'accès réflexives fonctionnent également pour les protocoles UDP et ICMP, dépourvus de bits de reçu (ACK) ou de réinitialisation (RST).
- L'option established ne fonctionne pas avec les applications qui modifient de manière dynamique le port source pour le trafic de session. L'instruction permit established vérifie uniquement les bits ACK ou RST (réinitialisation) ; elle ignore les adresses source ou de destination.
- Les listes de contrôle d'accès réflexives ne s'appliquent pas directement à une interface. En revanche, elles sont « imbriquées » dans une Listes de contrôle d'accès IP étendue nommée appliquée à cette interface.

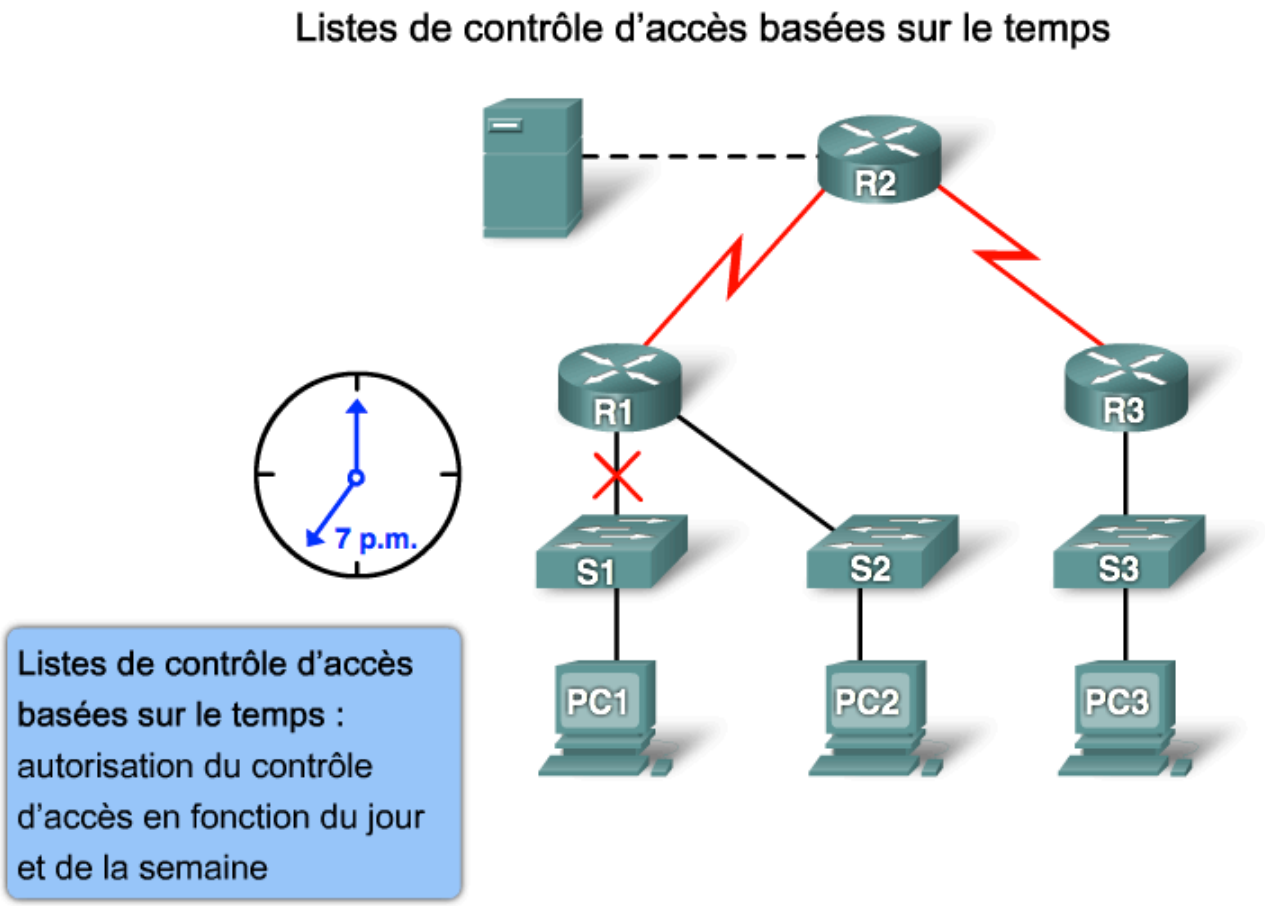
Listes de contrôle d’accès réflexives



Listes de contrôle d'accès réflexives

Étape 1	R2(config)#**ip access-list extended OUTBOUNDFILTERS** R2(config-ext-nacl)# **permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC** R2(config-ext-nacl)# **permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC**
Étape 2	R2(config)#**ip access-list extended INBOUNDFILTERS** R2(config-ext-nacl)# **evaluate TCPTRAFFIC** R2(config-ext-nacl)# **evaluate ICMPTRAFFIC**
Étape 3	R2(config)#**interface S0/1/0** R2(config-if)#**ip access-group INBOUNDFILTERS in** R2(config-if)#**ip access-group OUTBOUNDFILTERS out**

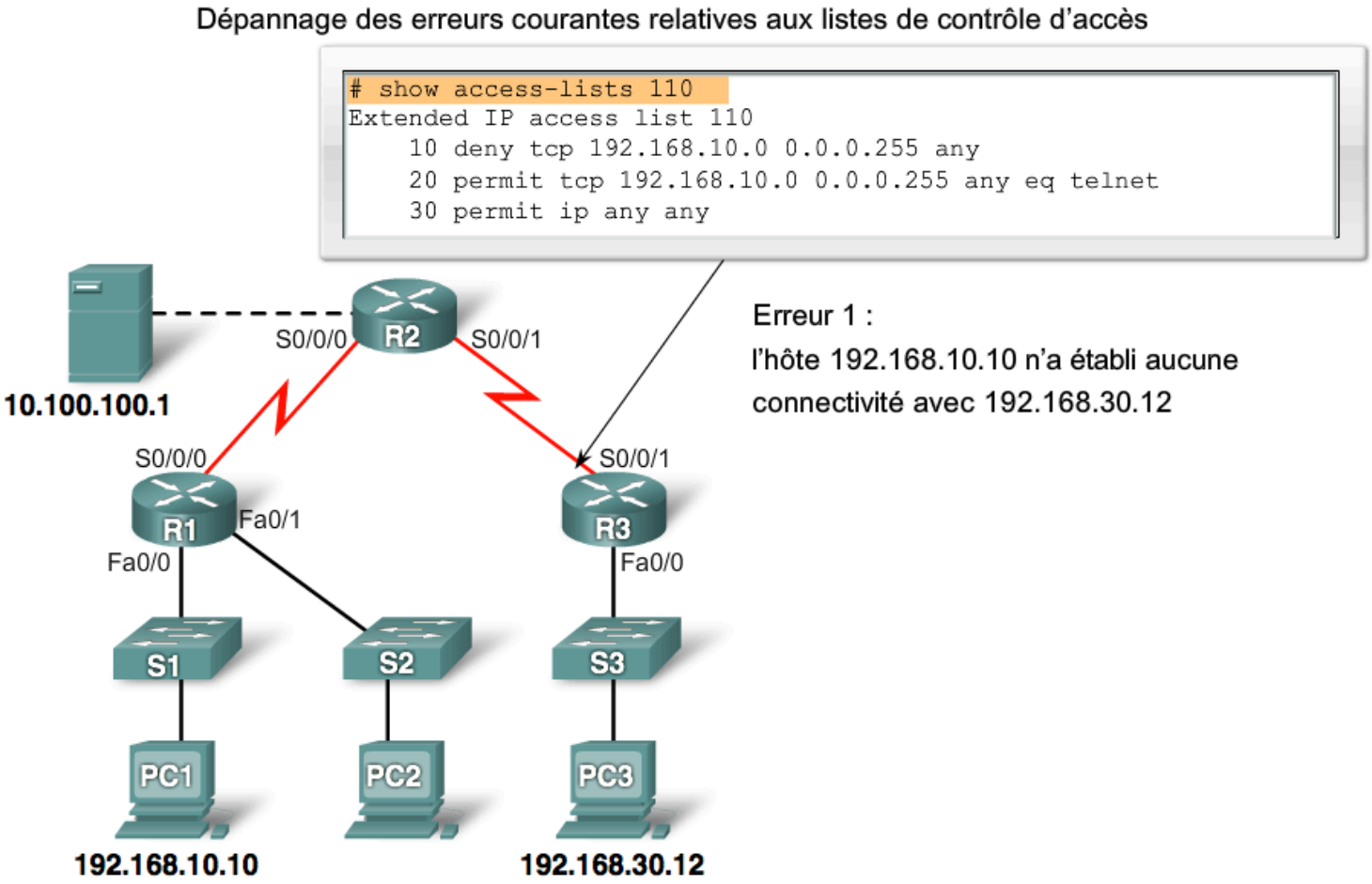
Listes de contrôle d’accès basées sur le temps



Listes de contrôle d'accès basées sur le temps

Étape 1	R1(config)#**time-range EVERYOTHERDAY** R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00**
Étape 2	R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Étape 3	R1(config)#**interface s0/0/0** R1(config-if)#**ip access-group 101 out**

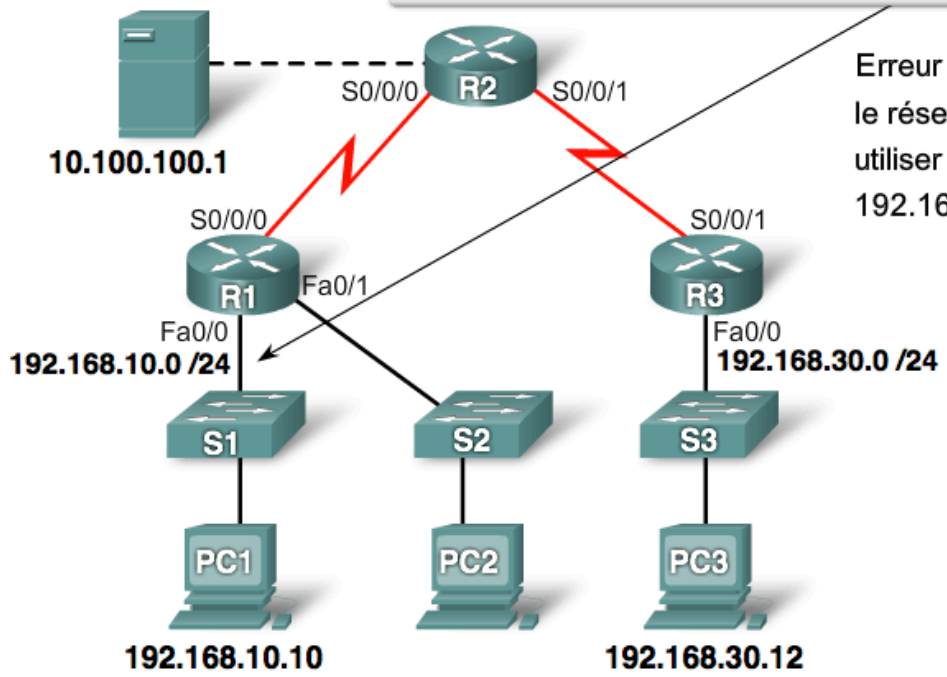
Erreurs courante relatives aux listes de contrôle d'accès



Erreurs courante relatives aux listes de contrôle d'accès

Dépannage des erreurs courantes relatives aux listes de contrôle d'accès

```
# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.255.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 10.100.100.1 eq smtp
    30 permit tcp any any
```



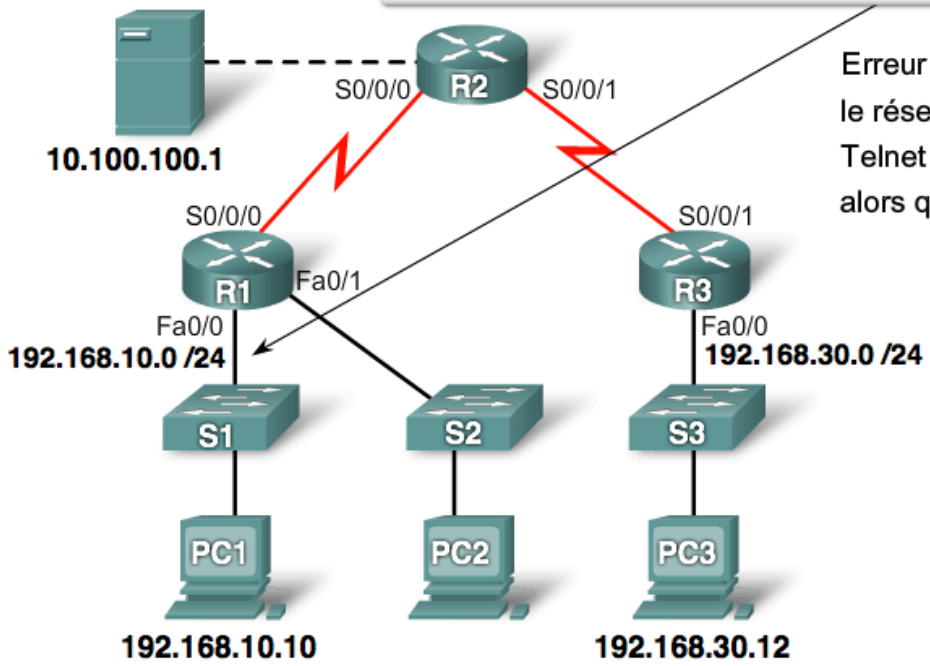
Erreur 2 :

le réseau 192.168.10.0 /24 ne peut pas utiliser TFTP pour se connecter au réseau 192.168.30.0 /24.

Erreurs courante relatives aux listes de contrôle d'accès

Dépannage des erreurs courantes relatives aux listes de contrôle d'accès

```
# show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.1.0 0.0.0.255 host 192.168.30.0 eq smtp
    30 permit ip any any
```

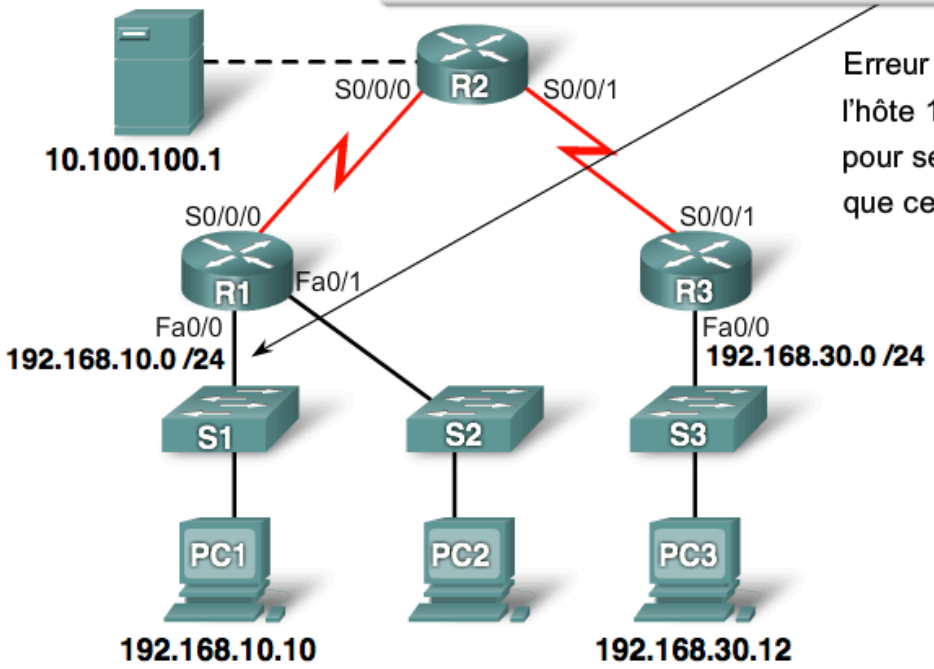


Erreur 3 :
le réseau 192.168.10.0 /24 peut utiliser Telnet pour se connecter à 192.168.30.0/24 alors que cette connexion doit être interdite.

Erreurs courante relatives aux listes de contrôle d'accès

Dépannage des erreurs courantes relatives aux listes de contrôle d'accès

```
# show access-lists 140
Extended IP access list 140
10 deny tcp host 192.168.10.1 any eq telnet
   20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
   30 permit ip any any
```



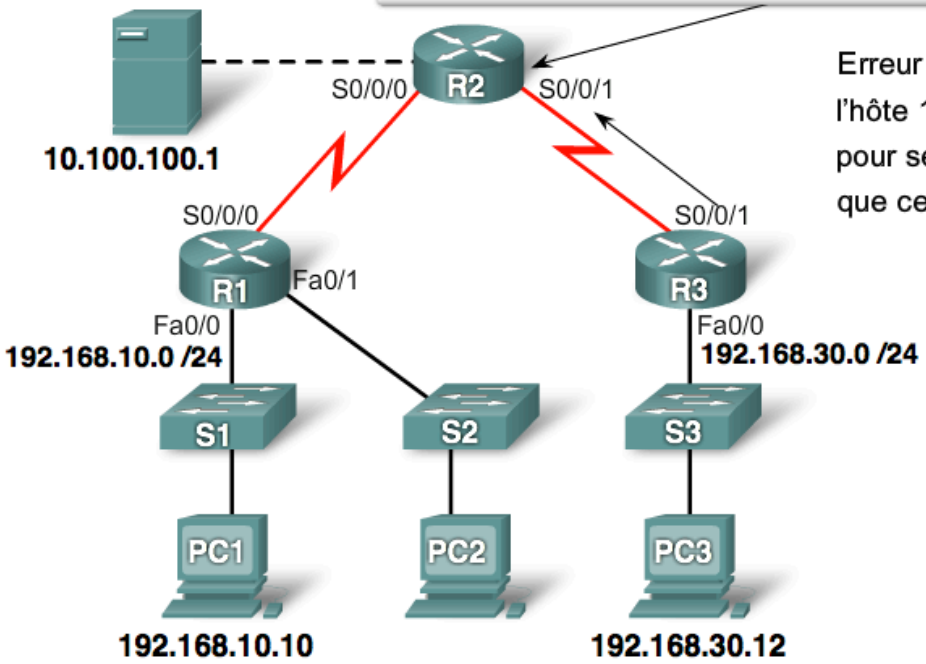
Erreur 4 :

l'hôte 192.168.10.10 peut utiliser Telnet pour se connecter à 192.168.30.12 alors que cette connexion doit être interdite.

Erreurs courante relatives aux listes de contrôle d'accès

Dépannage des erreurs courantes relatives aux listes de contrôle d'accès

```
# show access-lists 150
Extended IP access list 150
    10 deny tcp host 192.168.30.12 any eq telnet
    20 permit ip any any
```



Erreur 5 :

l'hôte 192.168.30.12 peut utiliser Telnet pour se connecter à 192.168.10.10 alors que cette connexion doit être interdite.