

Les ACL Cisco

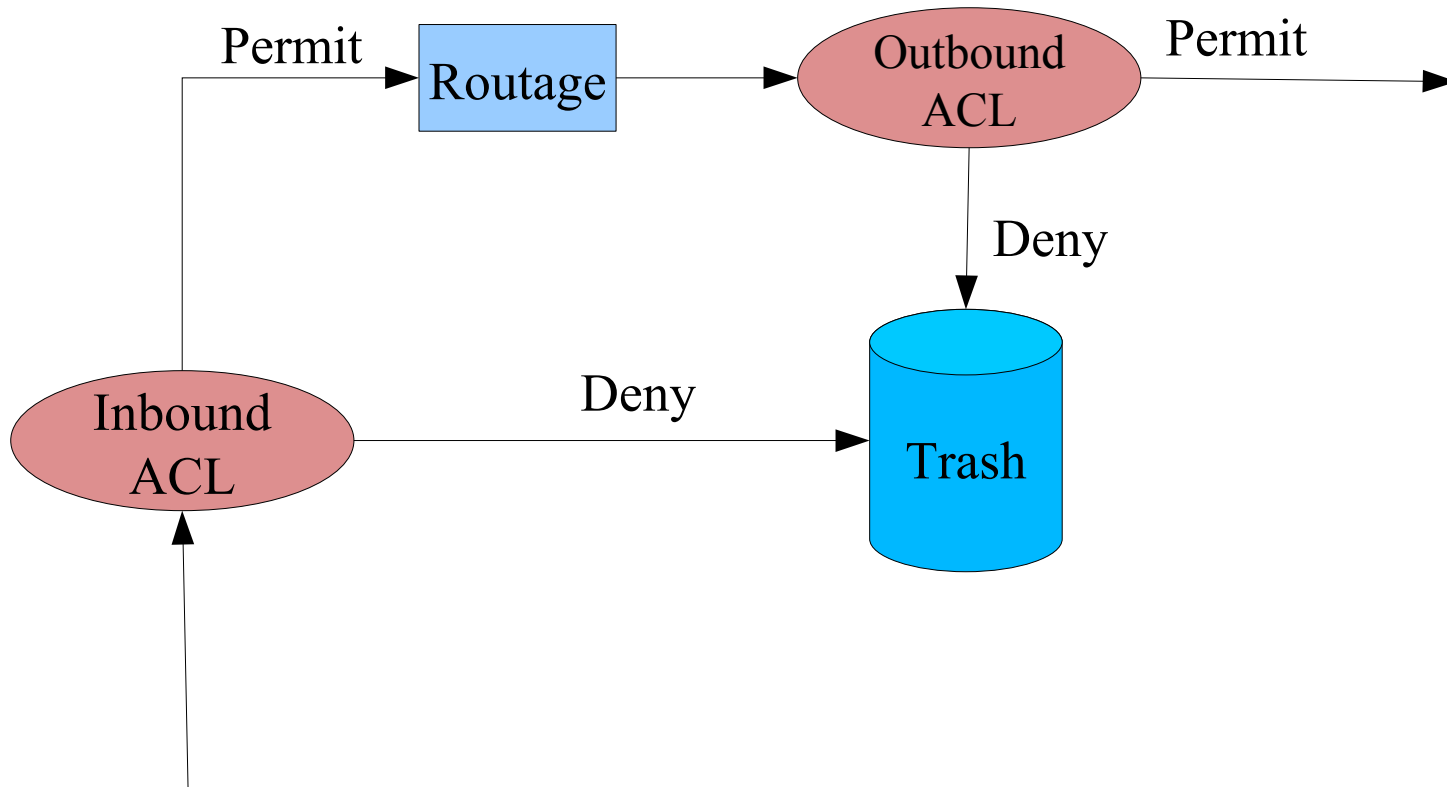
Les ACL Cisco

Présentation

Les ACL Cisco ?

- ▶ Les ACL (Access Control Lists) permettent de filtrer des packets suivant des critères définis par l'utilisateur
- ▶ Sur des packets IP, il est ainsi possible de filtrer les paquets entrants ou sortant d'un routeur en fonction
 - ▶ De l'IP source
 - ▶ De l'IP destination
 - ▶ ...
- ▶ Il existe 2 types d'ACL
 - ▶ Standard : uniquement sur les IP sources
 - ▶ Etendue : sur quasiment tous les champs des en-têtes IP, TCP et UDP

Schéma du principe



Les ACL Cisco

Fonctionnement et configuration

La logique des ACL

- ▶ Il est possible de résumer le fonctionnement des ACL de la façon suivante :
 - ▶ Le paquet est vérifié par rapport au 1er critère défini
 - ▶ S'il vérifie le critère, l'action définie est appliquée
 - ▶ Sinon le paquet est comparé successivement par rapport aux ACL suivants
 - ▶ S'il ne satisfait aucun critère, l'action *deny* est appliquée
- ▶ Les critères sont définis sur les informations contenues dans les en-têtes IP, TCP ou UDP
- ▶ Des masques ont été définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition
 - ▶ Ce masque définit la portion de l'adresse IP qui doit être examinée
 - ▶ 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés
 - ▶ `deny 10.1.3.0` avec 0.0.0.255 : refus de toutes les IP commençant par 10.1.3

Standard IP Access List Configuration

- ▶ Fonctionnement des ACL
 - ▶ Test des règles les unes après les autres
 - ▶ Si aucune règle n'est applicable, rejet du paquet
- ▶ Définition d'une règle
 - ▶ `access-list number [deny|permit] source [source-wildcard]`
 - ▶ Number compris entre 1 et 99 ou entre 1300 et 1999
 - ▶ `access-list number remark test`
- ▶ Activation d'une ACL sur une interface
 - ▶ `ip access-group [number | name [in | out]]`
- ▶ Visualiser les ACL
 - ▶ `show access-lists [number | name]` : toutes les ACL quelque soit l'interface
 - ▶ `show ip access-lists [number | name]` : les ACL uniquement liés au protocole IP

Exemple (1/3)

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
```

- ▶ `access-list 1 deny 172.16.3.10 0.0.0.0`
 - ▶ Refuse les paquets d'IP source 172.16.3.10
 - ▶ Le masque (également appelé wildcard mask) signifie ici que tous les bits de l'adresse IP sont significatifs
- ▶ `access-list 1 permit 0.0.0.0 255.255.255.255`
 - ▶ Tous les paquets IP sont autorisés
 - ▶ Le masque 255.255.255.255 signifie qu'aucun bit n'est significatif

Exemple (2/3)

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
access-list 1 deny host 172.16.3.10
access-list 1 permit any
```

- ▶ Une notation améliorée est possible pour remplacer
 - ▶ le masque 255.255.255.255 qui désigne une machine
 - ▶ Utilisation du terme **host**
 - ▶ 0.0.0.0 avec le wildcard masque à 255.255.255.255 qui désigne tout le monde
 - ▶ Utilisation du terme **any**

Exemple (3/3)

```
interface Ethernet0  
ip address 172.16.1.1 255.255.255.0  
ip access-group 1 out
```

```
interface Ethernet1  
ip address 172.16.2.1 255.255.255.0  
ip access-group 2 in
```

```
access-list 1 remark Stoppe tous les paquets d'IP source 172.16.3.10  
access-list 1 deny host 172.16.3.10  
access-list 1 permit any
```

```
access-list 2 remark Autorise que les trames d'IP source 172.16.3.0/24  
access-list 2 permit 172.16.3.0 0.0.0.255
```

Les extended ACL

- ▶ Les extended ACL permettent filtrer des paquets en fonction
 - ▶ de l'adresse de destination IP
 - ▶ Du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, ...)
 - ▶ Port source
 - ▶ Port destination
 - ▶ ...

La syntaxe et exemple

- ▶ `access-list number { deny | permit } protocol source source-wildcard destination dest.-wildcard`
 - ▶ number : compris entre 100 et 199 ou 2000 et 2699
- ▶ `access-list 101 deny ip any host 10.1.1.1`
 - ▶ Refus des paquets IP à destination de la machine 10.1.1.1 et provenant de n'importe quelle source
- ▶ `access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23`
 - ▶ Refus de paquet TCP provenant d'un port > 1023 et à destination du port 23 de la machine d'IP 10.1.1.1
- ▶ `access-list 101 deny tcp any host 10.1.1.1 eq http`
 - ▶ Refus des paquets TCP à destination du port 80 de la machine d'IP 10.1.1.1

Les ACL nommés

- ▶ Une ACL numéroté peut être composé de nombreuses règles. La seule façon de la modifier et de faire
 - ▶ `no access-list number`
 - ▶ Puis de la redéfinir
- ▶ Avec les ACL nommées, il est possible de supprimer qu'une seule ligne au lieu de toute l'ACL
- ▶ Sa définition se fait de la manière suivante
 - ▶ `Router(config)# ip access-list extended bart`
 - ▶ `Router(config-ext-nacl)# deny tcp host 10.1.1.2 eq www any`
 - ▶ `Router(config-ext-nacl)# deny ip 10.1.1.0 0.0.0.255 any`
 - ▶ `Router(config-ext-nacl)# permit ip any any`
- ▶ Pour supprimer une des lignes, il suffit de refaire un
 - ▶ `ip access-list extended bart`
 - ▶ Puis un `no deny ip 10.1.1.0 0.0.0.255 any`

L'accès au vty avec une ACL

- ▶ Pour utiliser une ACL dans le but de contrôler l'accès au vty (donc au telnet)

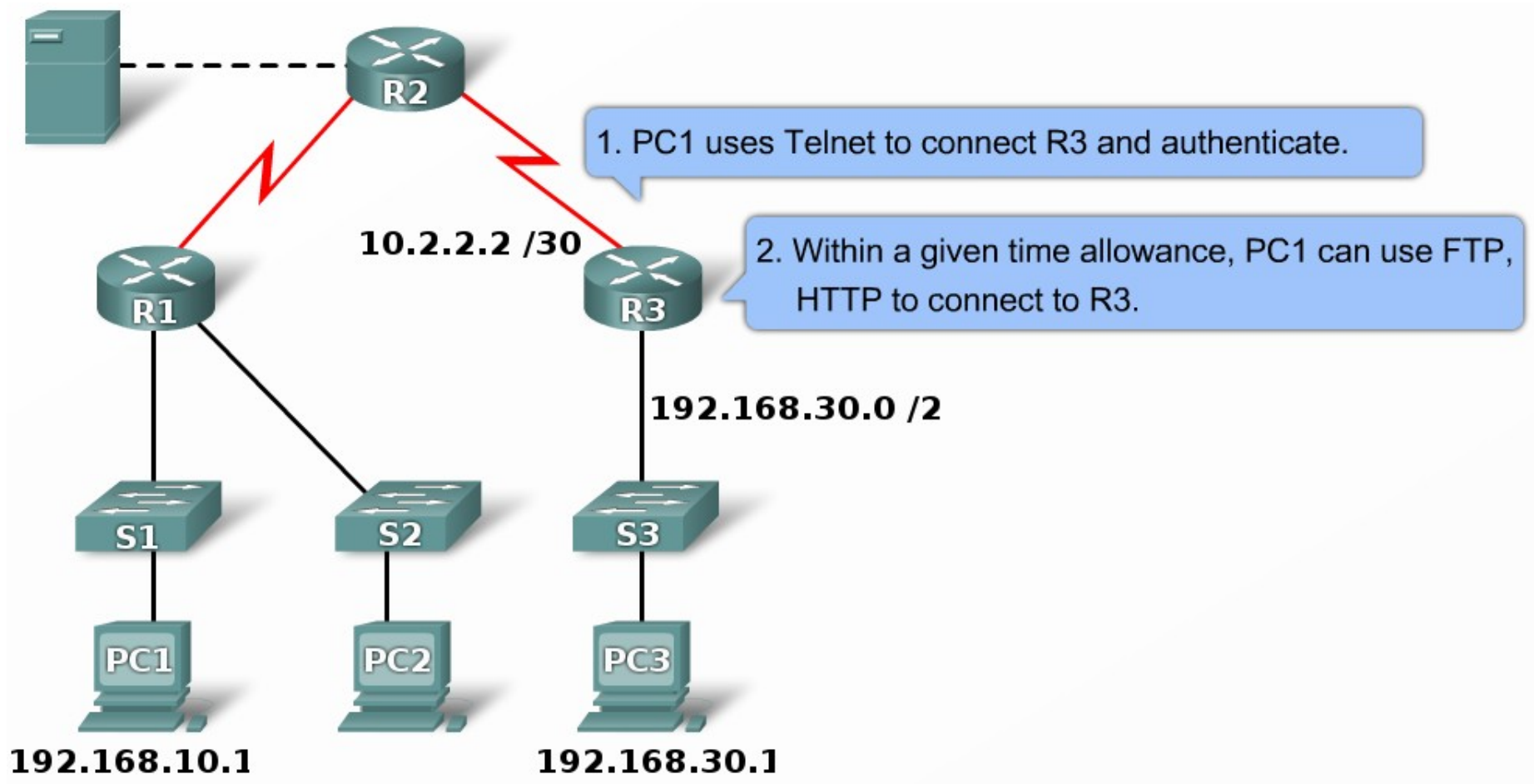
- ▶ `access-class number { in | out }`

```
line vty 0 4
    login
    password Cisco
    access-class 3 in
!
!
access-list 3 permit 10.1.1.0 0.0.0.255
```

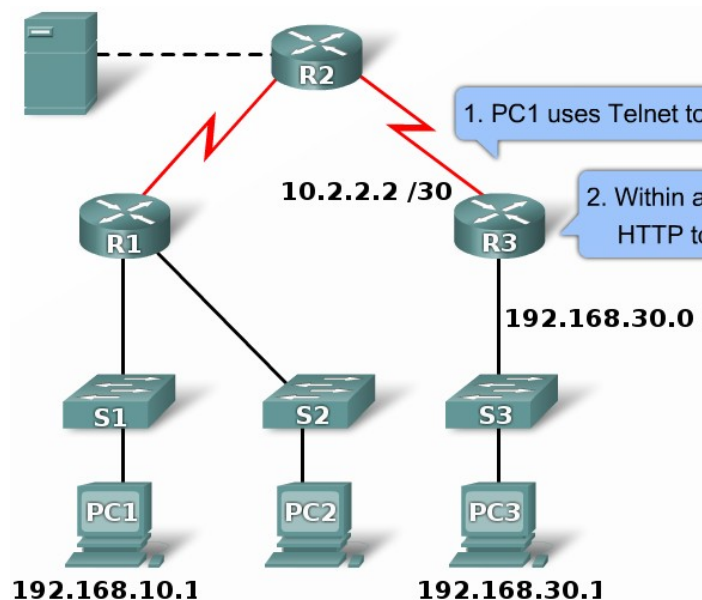
Les ACL Cisco

Les ACL complexes

Les ACL dynamiques



Les ACL dynamiques : configuration



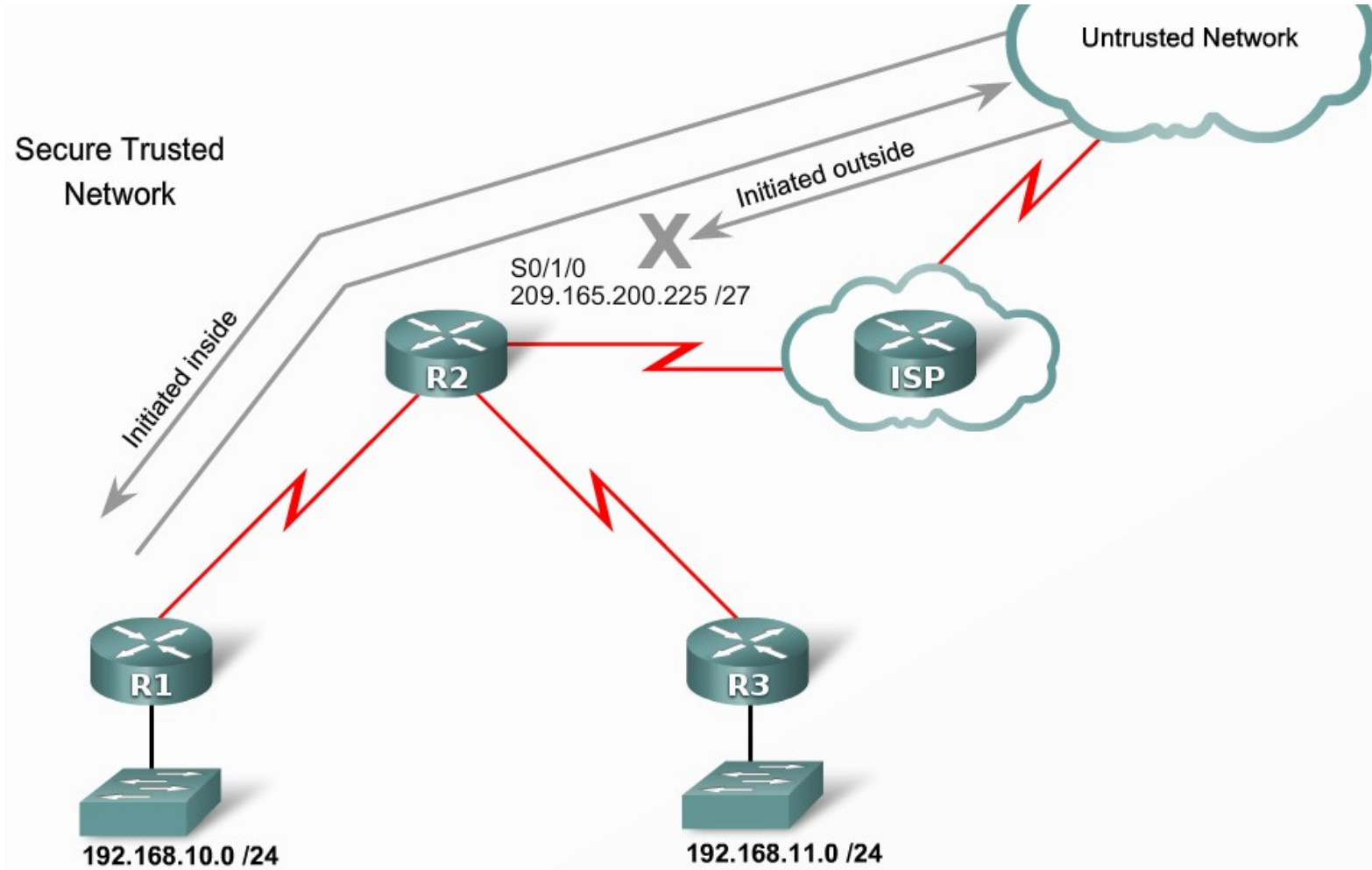
```
R3(config)#username Student password 0 cisco
```

```
R3(config)# access-list 101 permit tcp 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
```

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

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

Reflexive ACLs



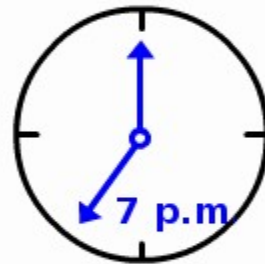
Reflexive ACLs : configuration

```
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
```

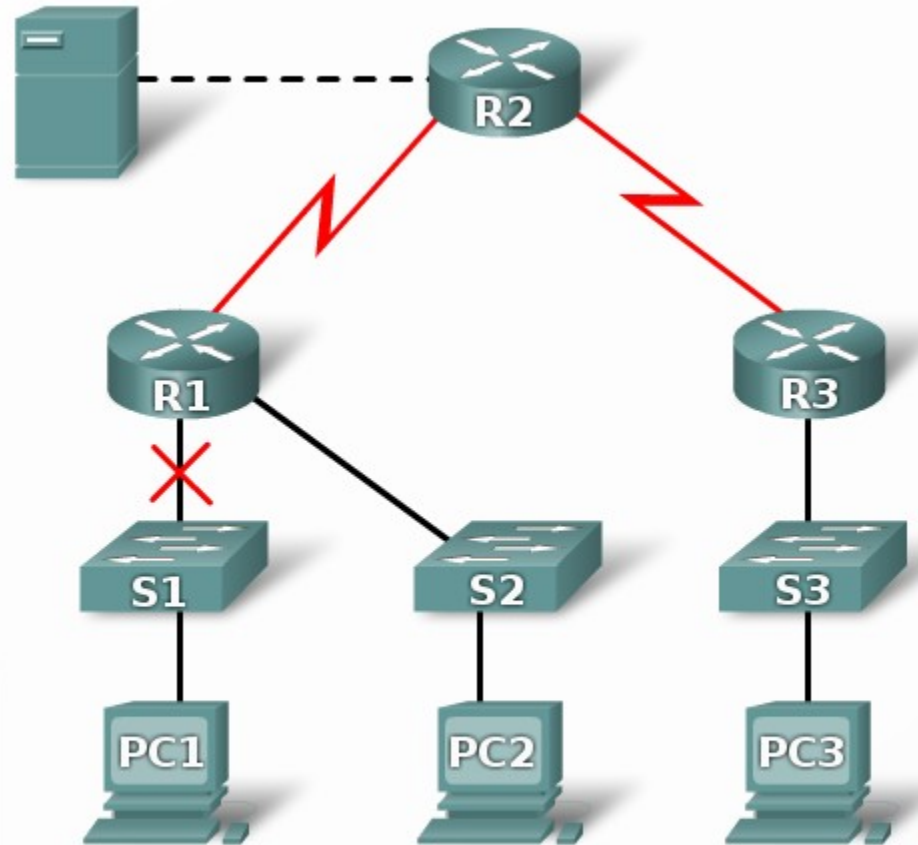
```
R2(config)#ip access-list extended INBOUNDFILTERS  
R2(config-ext-nacl)# evaluate TCPTRAFFIC  
R2(config-ext-nacl)# evaluate ICMPTRAFFIC
```

```
R2(config)#interface S0/1/0  
R2(config-if)#ip access-group INBOUNDFILTERS in  
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```

Time based ACL



Time-based ACLs:
Allow for access control
based on the time of day
and week



Time-based ACL configuration

```
R1 (config) #time-range EVERYOTHERDAY  
R1 (config-time-range) #periodic Monday Wednesday Friday 8:00 to  
17:00
```

```
R1 (config) #access-list 101 permit tcp 192.168.10.0 0.0.0.255  
any eq telnet time-range EVERYOTHERDAY
```

```
R1 (config) #interface s0/0/0  
R1 (config-if) #ip access-group 101 out
```

Les ACL Cisco

En production

Quelques conseils

- ▶ La création, la mise à jour, le debuggage nécessitent beaucoup de temps et de rigueur dans la syntaxe
- ▶ Il est donc conseillé
 - ▶ De créer les ACL à l'aide d'un éditeur de texte et de faire un copier/coller dans la configuration du routeur
 - ▶ Placer les extended ACL au plus près de la source du paquet que possible pour le détruire le plus vite possible
 - ▶ Placer les ACL standard au plus près de la destination sinon, vous risquez de détruire un paquet trop tôt
 - ▶ Rappel : les ACL standard ne regardent que l'IP source
 - ▶ Placer la règle la plus spécifique en premier
 - ▶ Avant de faire le moindre changement sur une ACL, désactiver sur l'interface concerné celle-ci (no ip access-group)