

Réseaux de Campus R301

Cours 3:

- NAT
- DHCP
- ACL
- VRRP, HSRP

1

1

La translation d'adresse (NAT)

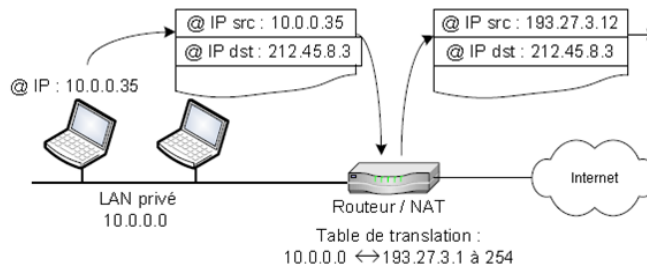
- ❏ Pour palier à la pénurie d'adresses IPv4, il est possible de configurer un réseau d'entreprise en utilisant des espaces d'adressage réservés aux réseaux privés de l'Internet.
- Le réseau de classe A 10.0.0.0, les réseaux de classe B allant de 172.16.0.0 à 172.31.0.0, ainsi que ceux de classe C allant de 192.168.0.0 à 192.168.255.0 sont définis par la RFC1918 comme non attribués sur l'Internet et réservés à un usage privé.
 - Il est alors possible de relier ces réseaux à l'Internet public en utilisant un dispositif de translation d'adresses ou NAT (Network Address Translation) proposé par la plupart des routeurs.
 - Ces derniers vont attribuer à la volée une adresse publique aux machines internes qui souhaitent établir une connexion avec l'Internet, et effectuer une traduction automatique des adresses IP dans l'en-tête des paquets.

2

2

NAT: exemple

- ❑ Sur le schéma, le LAN privé n'est plus limité par le nombre d'adresses (jusqu'à 16 millions pour la classe A privée 10.0.0.0)
- ❑ Les adresses publiques correspondent à la classe C 193.27.3.0 qui ne comporte que 254 adresses.
- ❑ Si plus de 254 machines veulent accéder simultanément à l'Internet, les numéros de port seront utilisés pour différencier 2 machines ayant une adresse Internet partagée.



3

3

PAT: Port Address Translation

- ❑ Dans l'exemple précédent, si le LAN privée comporte plus de 254 machines désirant accéder à Internet, il faudra mettre en œuvre la translation de port. Et c'est d'ailleurs la technique qui est le plus souvent employée.
- ❑ Grâce au PAT, une seule adresse IP publique suffit pour relier un grand nombre de machine d'un LAN privé à Internet.
- ❑ Ci-dessous la table PAT d'un routeur relié à Internet:

LAN privé		Internet	
@IP (privée) source	N° port source	@IP (publique) source	N° port source
10.0.0.1	56009	193.27.3.12	49152
10.0.0.2	60015	193.27.3.12	49153
10.0.0.3	48732	193.27.3.12	49154
.....

- ❑ Les procédés de translation (NAT & PAT) apportent un premier niveau de sécurité au LAN

4

4

PAT: Epilogue

❑ Port forwarding:

❑ Si j'ai deux serveurs web accessibles à partir d'une seule IP publique il faudra mettre en place un **proxy reverse**.

5

5

PAT: Epilogue

❑ D'abord il faut associer la même ip publique pour deux noms de domaines différents.

Donc deux enregistrements DNS

www.bob.info à 112.45.67.109

Et www.alice.info à 112.45.67.109 (même IP publique...car j'en ai qu'une)

Puis lorsqu'un client fait une requête <http://www.bob.info> ou <http://www.alice.info> ça renvoie sur le même serveur Web et là si c'est configuré comme ci-dessous (extrait conf apache), pour le site bob.info c'est le site en local qui répond et pour l'autre alice.info c'est Proxypass...la requête est renvoyée vers <http://192.168.0.1>

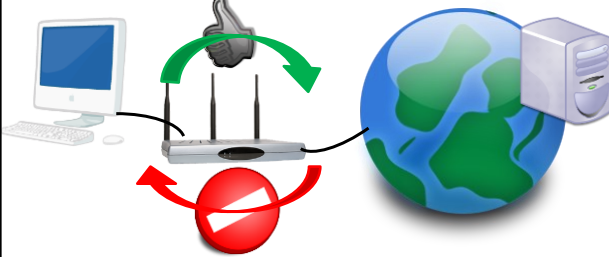
```
NameVirtualHost *
#
# Premier vhost (site d'origine)
#
<VirtualHost *>
  ServerName www.bob.info
  DocumentRoot /var/www/localhost/htdocs
</VirtualHost>
#
# Second vhost utilisant le reverse proxy
# 192.168.0.1 est l'exemple d'IP du second serveur http
#
<VirtualHost *>
  ServerName www.alice.info
  ProxyPass / http://192.168.0.1/
  ProxyPassReverse / http://192.168.0.1/
</VirtualHost>
```

6

6

NAT: quelques remarques s'imposent

❑ Le NAT dynamique permet de sortir sur Internet mais ne permet pas d'être joignable. Une machine de l'extérieur ne peut initier une requête.



❑ Du point de vue de la sécurité, cela apporte un petit plus!

❑ Translation des messages ICMP.

➤ La fonction « ping » n'utilise ni UDP, ni TCP, donc n'utilise pas de numéro de port.

➤ Le routeur se base sur l'identifiant ICMP présent dans l'en-tête des messages ICMP

En-tête ICMP

Type	Code	Checksum
Identifiant		Numéro de séquence
Masque d'adresse		
0	16	32bits

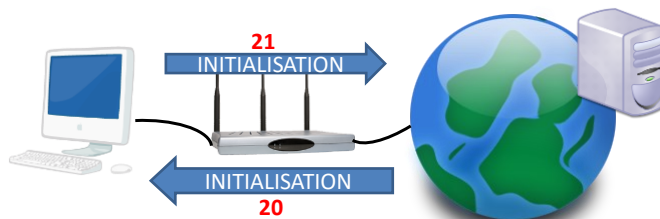
7

7

NAT/FTP Mode passif et mode actif

❑ FTP utilise deux canaux: - 21 commandes
- 20 data

❑ En mode actif l'initialisation se fait sur le port 21, puis le serveur FTP initie une ouverture de connexion pour les « data » depuis l'extérieur.

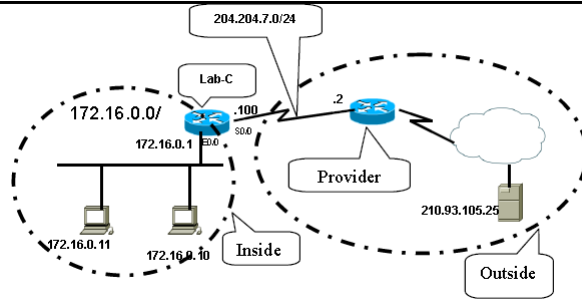


❑ Solution: un proxy qui va lire les informations contenues dans les données FTP. Ce proxy est capable de voir quelle machine a initialisé la connexion sur le port 21 et autorise alors l'initialisation de la connexion (pour les DATA) venant de l'extérieur.

8

8

NAT/PAT



Création d'une ACL (Liste de Contrôle d'Accès) « standard » (sur adresse IP) : ici, toutes les adresses des stations de l'Intranet sont éligibles à la translation.

Lab-C(config)#access-list 10 permit 172.16.0.0 0.0.0.255

Activation du PAT

Lab-C(config)#ip nat inside source list 10 interface S0/0 overload

Définition des interfaces du routeur Intranet/Internet

Lab-C(config)#interface ethernet 0/0

Lab-C(config-if)#ip nat inside

Lab-C(config-if)#interface serial 0/0

Lab-C(config-if)#ip nat outside

Plusieurs transactions utilisant la même adresse "Inside Global"

Lab-C#show ip nat translations

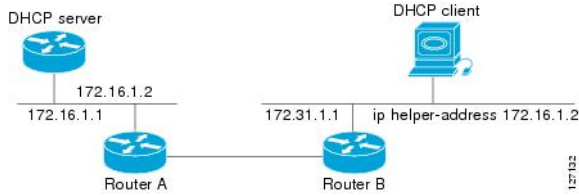
9

9

DHCP (rappels)

10

Transfert des « broadcasts » UDP à un serveur DHCP en utilisant la commande « Helper Address »



Perform this task to configure the DHCP relay agent to forward packets to a DHCP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip helper-address address**
5. **exit**

NOTE

The **ip helper-address** command forwards broadcast packets as a unicast to eight different UDP ports by default:

- TFTP (port 69)
- DNS (port 53)
- Time service (port 37)
- NetBIOS name server (port 137)
- NetBIOS datagram server (port 138)
- Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)
- TACACS service (port 49)
- Host Name Service (port 42)

To close some of these ports, use the **no ip forward-protocol udp x** command at the global configuration prompt, where x is the port number you want to close. The following command stops the forwarding of broadcasts to port 49:

```
Router(config)#no ip forward-protocol udp 49
```

To open other UDP ports, use the **ip forward-helper udp x** command, where x is the port number you want to open.

```
Router(config)#ip forward-protocol udp 517
```

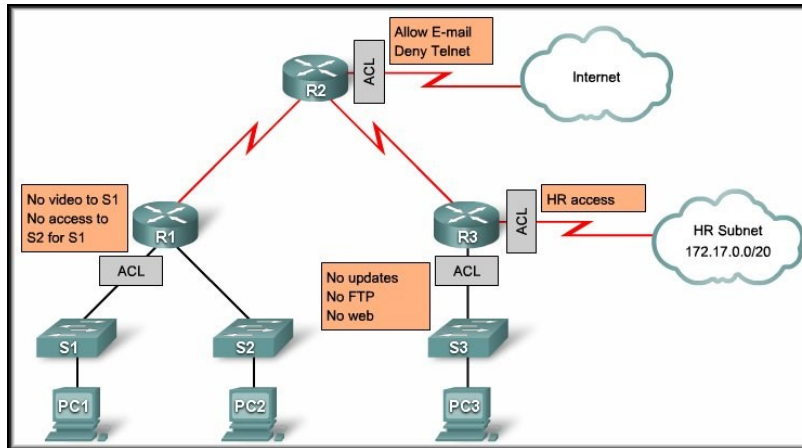
11

Listes de contrôle d'accès

12

Listes de contrôle d'accès

On utilise les ACL pour sécuriser les réseaux



13

Utiliser les ACL pour sécuriser les réseaux

- ACLs vous permettent de contrôler le trafic entrant et/ou sortant du réseaux.
 - Cela peut être très simple en autorisant ou refusant le trafic d'un hôte ou d'un réseaux tout entier
 - Ou bien on peut contrôler le trafic en s'appuyant sur le port TCP utilisé par l'application

14

Utiliser les ACLs pour sécuriser le réseau.



15

Utiliser les ACLs pour sécuriser le réseau.

- Le segment TCP identifie le port correspondant au service demandé...TCP

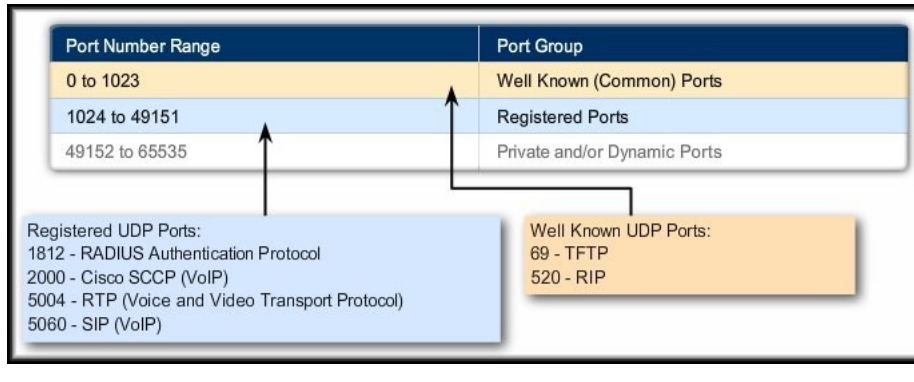
Port Number Range	Port Group
0 to 1023	Well Known (Common) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Registered TCP Ports: 1863 - MSN Messenger 8008 - Alternate HTTP 8080 - Alternate HTTP	Well Known TCP Ports 21 - FTP 23 - Telnet 25 - SMTP 80 - HTTP 110 - POP3 194 - Internet Relay Chat (IRC) 443 - Secure HTTP (HTTPS)
--	--

16

Utiliser les ACLs pour sécuriser le réseau.

- Le segment UDP identifie le port correspondant au service demandé...UDP



17

Utiliser les ACLs pour sécuriser le réseau.

- Filtrage de paquets:
 - Une liste de contrôle d'accès peut extraire les informations suivantes de l'en-tête des paquets, les valider conformément aux règles, et prendre des décisions d'autorisation ou de refus en fonction des critères suivants :
 - Adresse IP source.
 - Adresse IP destination
 - et....
 - Port source TCP/UDP.
 - Port destination TCP/UDP.

18

La règle des "3 P"

- Une ACL par protocole.
- Une ACL par direction.
- Une ACL par interface.

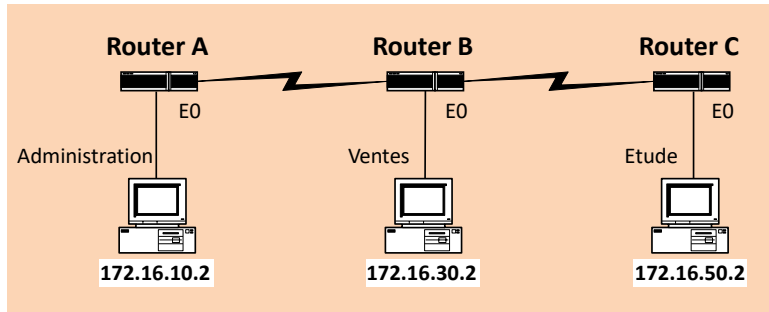
19

□ Identification des listes de contrôle d'accès

Type de liste		Valeur de l'identifiant
IP	Standard Etendue	1 à 99 100 à 199
IPX	Standart Filtre SAP	800 à 899 1000 à 1099
Apple Talk		600 à 699

20

❑ Le routeur A laisse passer le trafic en provenance du réseau des ventes et de l'hôte 172.16.50.2



```
RouterA(config)#
access-list 11 permit 172.16.30.0 0.0.0.255
access-list 11 permit 172.16.50.2 0.0.0.0
```

Dernière instruction implicite → deny any

21

❑ Bits de masque générique

128	64	32	16	8	4	2	1	
↓	↓	↓	↓	↓	↓	↓	↓	
Position de bit d'octet et valeur d'adresse du bit								
Exemples								
0	0	0	0	0	0	0	0	=
0	0	1	1	1	1	1	1	=
0	0	0	0	1	1	1	1	=
1	1	1	1	1	1	0	0	=
1	1	1	1	1	1	1	1	=
<div>Vérifier tous les bits d'adresse (correspondance complète)</div> <div>Ignorer les 6 derniers bits d'adresse</div> <div>Ignorer les 4 derniers bits d'adresse</div> <div>Vérifier les 2 derniers bits d'adresse</div> <div>Ne pas vérifier l'adresse (ignorer les bits dans l'octet)</div>								

0 => bit à tester
1 => bit ignoré

22

```
RouterA(config)#
access-list 11 permit 172.16.50.2 0.0.0.0
```

=

```
RouterA(config)#
access-list 11 permit host 172.16.50.2
```

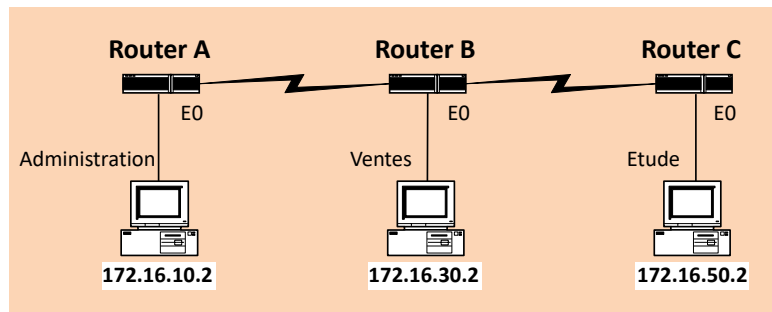
23

❑ Le routeur A bloque le trafic uniquement en provenance de l'hôte 172.16.50.2

```
RouterA(config)#
access-list 11 deny host 172.16.50.2
access-list 11 permit any
```

Dernière instruction implicite

deny any

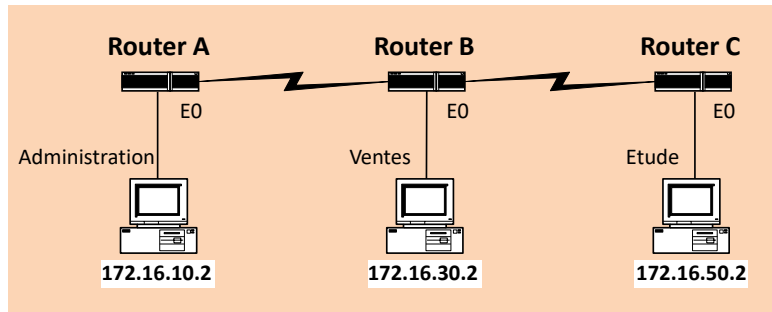


24

❑ Appliquer la liste d'accès à l'interface.

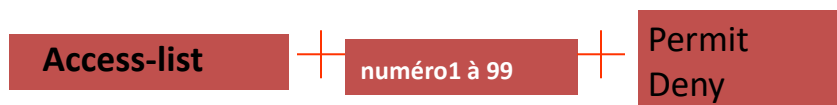
RouterA(config)# interface e0

RouterA(config-if)# ip access-group 11 out



25

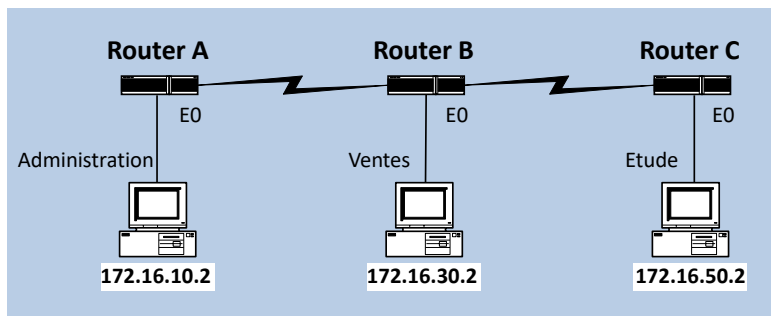
Listes standards



26

Liste de contrôle d'accès étendue

Le routeur A permet à la station 172.16.50.2 du bureau d'étude l'accès au serveur web de l'administration d'adresse IP 172.16.10.2.

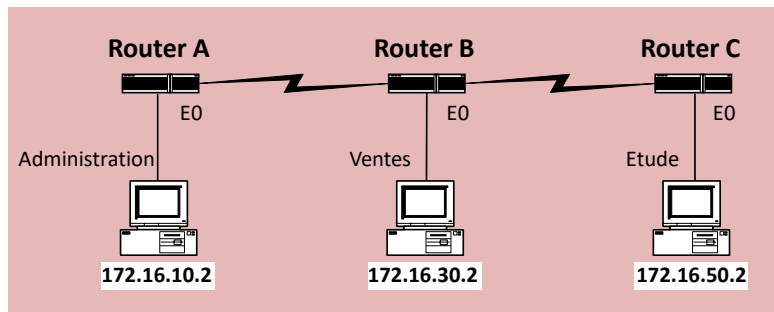


27

❑ Liste de contrôle d'accès étendue

RouterA(config)#

Access-list 110 permit tcp host 172.16.50.2
host 172.16.10.2 eq 80



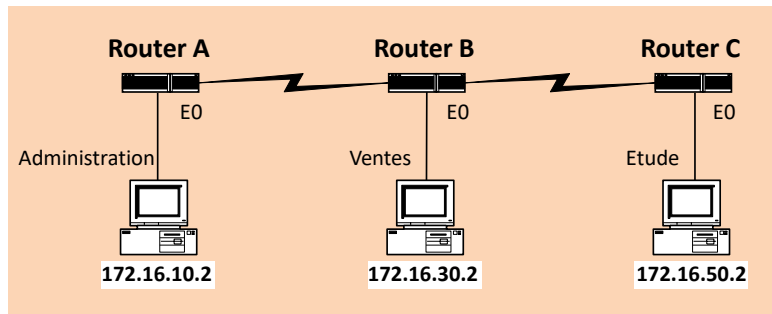
RouterA(config)# inter e0

RouterA(config-if)# ip access-group 110 out

28

❑ Liste de contrôle d'accès étendue

Le routeur A permet à n'importe quelle station du service des ventes d'accéder au serveur web de l'administration.



RouterA(config)#

Access-list 110 permit tcp 172.16.30.0 0.0.0.255
host 172.16.10.2 eq 80

29

Où placer les listes d'accès ? Là où elle auront le plus grand impact « on efficiency »

Standard

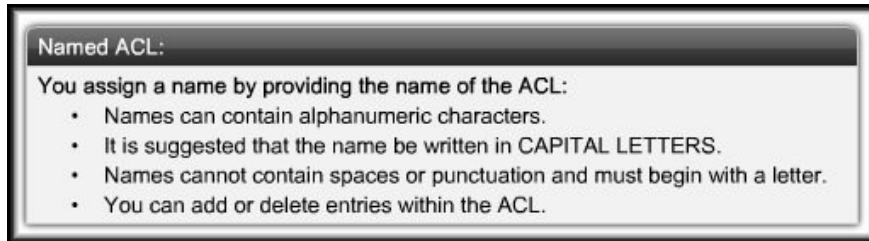
- Le plus près possible de la destination. (pour supprimer tout le trafic vers cette destination et éviter que le réseau source ne se retrouve bloqué pour les autres réseaux)

Etendue

- Le plus près possible de la source. (pour utiliser moins de bande passante.)

30

ACLs nommées



- Utiliser des ACL nommées:
 - Une ACL numérotée n'indique pas son but.
 - Depuis la version Cisco IOS Release 11.2, on peut utiliser les ACL nommées.

31

Remarques sur les ACLs

- Vous devez avoir la règle la plus fréquemment utilisée en bout de liste.
- Vous devez avoir au moins une autorisation dans une ACL sinon tout le trafic sera bloqué.
- La commande **#show access-list** permet de visualiser les ACLs configurées sur le routeur.

32

- Le mot clé “remark” permet de documenter en détail le but de l’ACL.
- Exemple:

```

R1(config)#access-list 10 remark Allow 192.168.10.0 hosts
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 deny any
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#sh run
Building configuration...

Current configuration : 576 bytes
!
<output omitted>
!
access-list 10 remark Allow 192.168.10.0 hosts
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 10 deny any
!
!
line con 0

```

Max. 100 characters

Note where the access list appears in the running configuration.

33

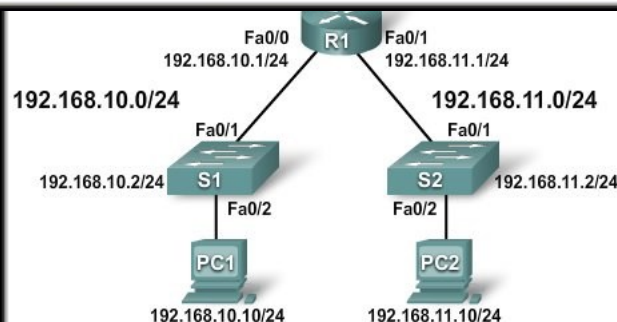
- Exemple d’ACL nommée.

```

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)#deny any
R1(config-std-nacl)#end

R1(config)#interface Fa0/1
R1(config-if)# ip access-group NO_ACCESS out

```



34

- Les ACLs nommées ont un gros avantage par rapport aux ACLs numérotées car elles sont plus faciles à éditer.

```

R1#show access-lists
Standard IP access list WEBSERVER
 10 permit host 192.168.10.10
 20 deny 192.168.10.0 0.0.0.255
 30 deny 192.168.11.0 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 192.168.11.0
R1(config-std-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show access-lists
Standard IP access list WEBSERVER
 10 permit host 192.168.10.10
 15 permit host 192.168.11.0
 20 deny 192.168.10.0 0.0.0.255
 30 deny 192.168.11.0 0.0.0.255
R1#

```

35

Pour les ACLs étendues

```

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

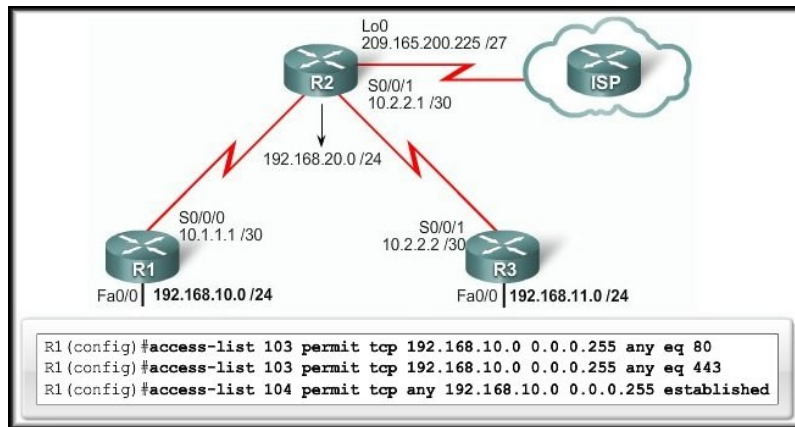
```

- Ce paramètre autorise les réponses au trafic qui a initié la demande.
- Le routeur autorisera uniquement le trafic "établi" à revenir et bloquera tout le reste.

36

Exemple

- Restreindre l'accès à Internet uniquement pour les navigateurs.
 - ACL 103 s'applique au trafic quittant le réseau.
 - ACL 104 pour le trafic entrant sur le réseau.



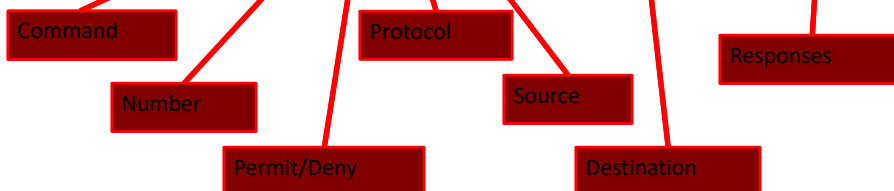
37

HTTP requiert que les réponses reviennent vers le réseau! Seul le trafic « established » par 103 sera autorisé à revenir grâce à 104; le reste sera bloqué.

```

R1 (config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1 (config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443

R1 (config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
  
```

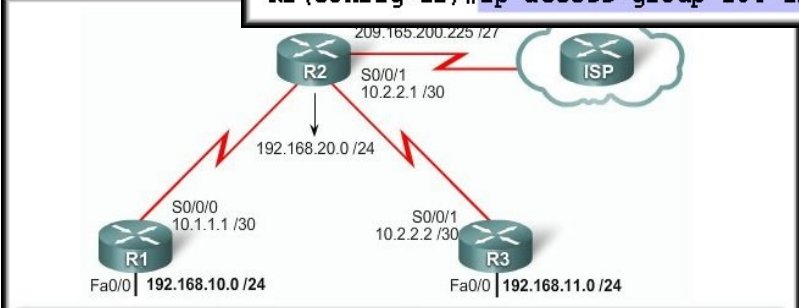


38

```

R1 (config)#interface s0/0/0
R1 (config-if)#ip access-group 103 out
R1 (config-if)#ip access-group 104 in

```



```

R1 (config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1 (config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1 (config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established

```

39

Créer des ACLs nommées étendues

```

R1 (config)#ip access-list extended SURFING
R1 (config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 eq 80
R1 (config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 eq 443
R1 (config-ext-nacl)#exit

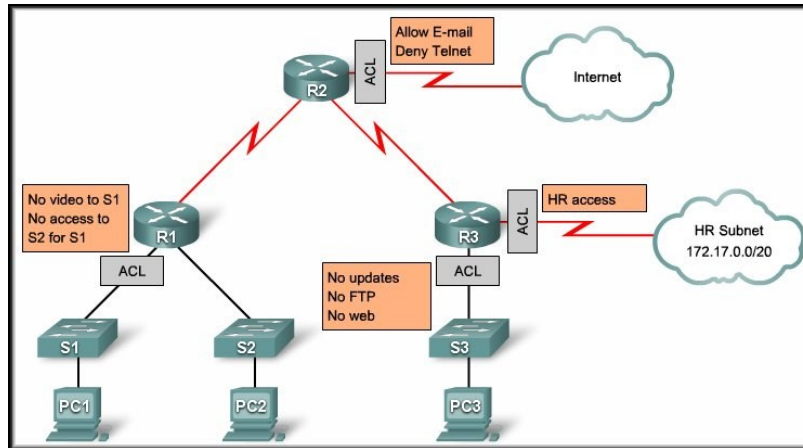
R1 (config)#ip access-list extended BROWSING
R1 (config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255 established
R1 (config-ext-nacl)#exit

```

40

Access Control Lists

Configurer des ACLs complexes



41

Qu'est ce que les ACLs complexes?

- 3 types:
 - Dynamic (lock-and-key):
 - Les utilisateurs qui souhaitent traverser le routeur sont bloqués à moins qu'ils ne se soient connectés en Telnet au routeur et se soient authentifiés.
 - Reflexive:
 - Autorise le trafic sortant et limite le trafic entrant à celui qui a été initié depuis l'intérieur.
 - Time-based:
 - L'accès est permis à certaines heures de la journée.

42

Interdire l'accès en Telnet

- R1
- ip access-list standard VTY_LOCAL
- permit 10.1.1.0 0.0.0.255
- deny any log
- !
- line vty 0 4
- access-class VTY_LOCAL in

43

Redondance au premier saut

44

Protocoles FHRP (First Hop Redundancy Protocols, protocoles de redondance au premier saut)

Les protocoles STP permettent de mettre en place une redondance physique au sein d'un réseau commuté. Cependant, un hôte situé au niveau de la couche d'accès d'un réseau hiérarchique peut également bénéficier de passerelles par défaut alternatives.

Les diapos qui suivent traitent des protocoles de redondance au premier saut

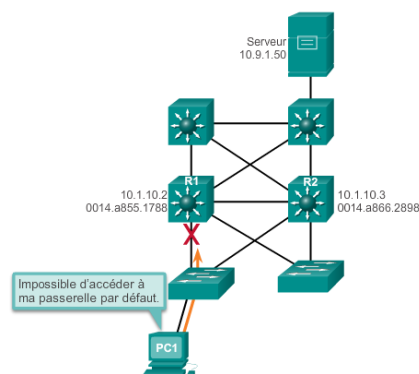
45

Concept de protocoles de redondance au premier saut

Limitations de passerelle par défaut

- Si la passerelle par défaut ne peut pas être atteint, le dispositif local ne peut pas envoyer des paquets en dehors du segment de réseau local.
- Même si un routeur redondant existe qui pourrait servir de passerelle par défaut à ce segment, il n'y a aucune méthode dynamique par laquelle ces dispositifs peuvent déterminer l'adresse d'une nouvelle passerelle par défaut.

Limitations de passerelle par défaut

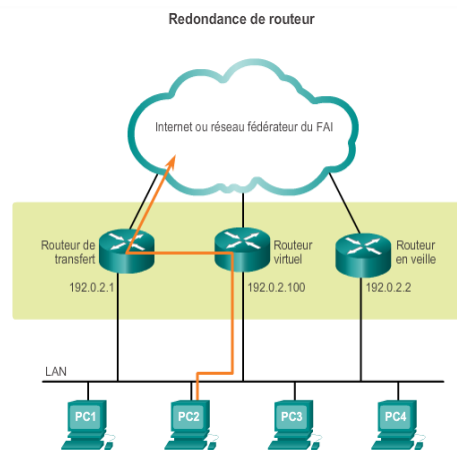


46

Concept de protocoles de redondance au premier saut

Redondance de routeur

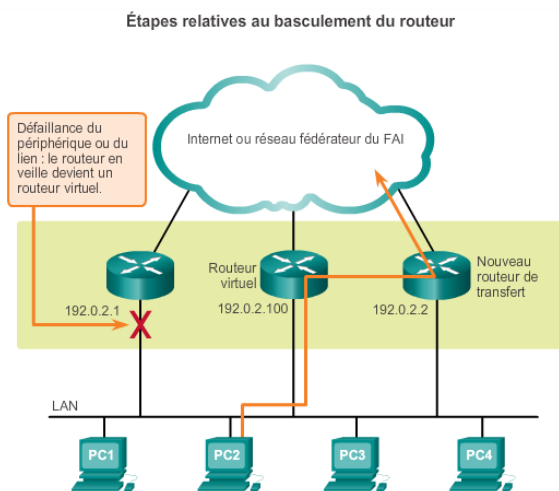
- Des routeurs multiples sont configurés pour un fonctionnement conjoint, de manière à présenter l'illusion d'un routeur unique au regard des hôtes du LAN
- La capacité d'un réseau à effectuer une reprise dynamique après la défaillance d'un périphérique jouant le rôle de passerelle par défaut est appelée « redondance au premier saut ».



47

Concept de protocoles de redondance au premier saut

Étapes relatives au basculement du routeur



48

Varieties of First-Hop Redundancy Protocols

Protocoles de redondance de premier saut

- Hot Standby Router Protocol (HSRP) . Propriétaire Cisco
- HSRP for IPv6
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
- VRRPv3
- Gateway Load Balancing Protocol (GLBP)
- GLBP for IPv6
- ICMP Router Discovery Protocol (IRDP)

49

Varieties of First-Hop Redundancy Protocols

Protocoles de redondance de premier saut

- Hot Standby Router Protocol (HSRP) . Propriétaire Cisco
- HSRP for IPv6
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
- VRRPv3
- Gateway Load Balancing Protocol (GLBP)
- GLBP for IPv6
- ICMP Router Discovery Protocol (IRDP)

50

Caractéristiques du protocole

- Adresse IP virtuelle **et** adresse MAC virtuelle
 - Mac virtuelle = 00-00-5E-00-01-XX (XX = n° du groupe VRRP)
- Priorité de 1 à 255 (100 par défaut)
- En cas d'égalité de priorité, c'est le routeur de plus grande adresse IP qui est maître.
- Si IP virtuelle = IP de l'interface, alors le routeur est maître (priorité = 255)
- Le routeur maître émet des messages VRRP (champ protocole IP 112 et adresse multicast 224.0.0.18) toutes les secondes.
- En cas de non réception de message pendant le timeout (3,6 s par défaut), un routeur de secours se considérera maître.
- Si l'option « préemption » est activée, le routeur de secours passera maître si la priorité du maître baisse sous la sienne.

51

Partage de charge

- On peut créer plusieurs groupes VRRP
- Un routeur peut être maître pour un groupe et secours pour un autre.
- Ainsi les hôtes de 2 sous-réseaux feront partie d'un groupe VRRP différent et utiliseront une passerelle différente

52

Exemple de configuration pour VRRP

```

Interface vlan 10
-if)#Vrrp 1 description data master
-if)# Vrrp 1 priority 100
-if)# Vrrp 1 ip 192.168.10.254
-if)# Vrrp 1 preempt
-if)# Vrrp 1 timers advertise 2
-if)# Vrrp 1 track 1 decrement 20
config)#track 1 interface fa0/24
line-protocol
-if)# Interface vlan 20
-if)# Vrrp 2 description voix
backup
-if)# Vrrp 2 priority 90
-if)# Vrrp 2 ip 192.168.20.254
-if)# Vrrp 2 preempt
-if)# Vrrp 2 timers learn

```

```

Interface vlan 10
-if)#Vrrp 1 description data backup
-if)# Vrrp 1 priority 90
-if)# Vrrp 1 ip 192.168.10.254
-if)# Vrrp 1 preempt
-if)# Vrrp 1 timers learn
-if)# Interface vlan 20
-if)# Vrrp 2 description voix master
-if)# Vrrp 2 priority 100
-if)# Vrrp 2 ip 192.168.20.254
-if)# Vrrp 2 preempt
-if)# Vrrp 2 timers advertise 2
-if)# Vrrp 2 track 1 decrement 20
config)#track 1 interface fa0/24 line-protocol

```

53

Préemption

- Le routeur qui a une plus grande priorité que le routeur maître, devient maître, même si le routeur maître actuel est toujours actif
- Activé par défaut
- Le routeur qui a l'adresse IP du groupe VRRP ne tient pas compte de ce paramètre et préempte toujours.

54

[illegible]

55

HSRP for IPv4

HSRP routers communicate with each other by exchanging HSRP hello packets. These packets are sent to the destination IP multicast address 224.0.0.2 (reserved multicast address used to communicate to all routers) on UDP port 1985. The active router sources hello packets from its configured IP address and the HSRP virtual MAC address while the standby router sources hellos from its configured IP address and the interface MAC address, which might be the burned-in address (BIA). The BIA is the last six bytes of the MAC address that is assigned by the manufacturer of the network interface card (NIC).

Because hosts are configured with their default router as the HSRP virtual IP address, hosts must communicate with the MAC address associated with the HSRP virtual IP address. This MAC address is a virtual MAC address, 0000.0C07.ACxy, where xy is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group 1 uses the HSRP virtual MAC address of 0000.0C07.AC01. Hosts on the adjoining LAN segment use the normal Address Resolution Protocol (ARP) process to resolve the associated MAC addresses.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, which is used by version 1. HSRP version 2 permits an expanded group number range of 0 to 4095 and uses a new MAC address range of 0000.0C9F.F000 to 0000.0C9F.FFFF.

Multiple HSRP

The switch supports Multiple HSRP (MHSRP), an extension of HSRP that allows load sharing between two or more HSRP groups. You can configure MHSRP to achieve load-balancing and to use two or more standby groups (and paths) from a host network to a server network.

56

Basic HSRP Configuration

Before we discuss more advanced HSRP concepts, let's create a basic HSRP configuration to get an idea of how this all works. For this scenario we will use a topology consisting of just two routers. Keep in mind that one or both of these routers could be multilayer switches such as a 6509 or 3750 as well. But for this discussion let's just refer to them as routers.

R1 and R2 will both be configured to be in standby group 1. The HSRP address will be given an IP address of 192.168.1.1/24. All hosts on the segment and in the VLAN will use this address as their default gateway.

```
R1(config)#interface ethernet0
R1(config-if)#ip address 192.168.1.2
R1(config-if)#standby 1 ip 192.168.1.1
```

```
R2(config)#interface ethernet0
R2(config-if)#ip address 192.168.1.3
R2(config-if)#standby 1 ip 192.168.1.1
```

To see the status of HSRP use the command
show standby

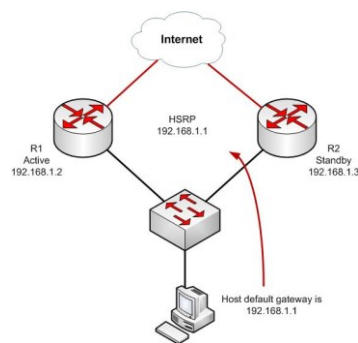
57

Controlling the Active HSRP Router

The default priority is 100. The higher priority will determine which router is active. If both routers are set to the same priority, the first router to come up will be the active router.

```
R1(config)#interface ethernet0
R1(config-if)#ip address
192.168.1.2
R1(config-if)#standby 1 ip
192.168.1.1
R1(config-if)#standby 1
priority 200 <-- Add this to
force R1 to be active
```

```
R2(config)#interface ethernet0
R2(config-if)#ip address 192.168.1.3
R2(config-if)#standby 1 ip 192.168.1.1
```



58

Advanced HSRP Configuration - Load Balancing

So now you can see how great HSRP is and how it allows us to have high availability between multiple routers for a single network. But our standby routers aren't doing anything and are just sitting there! Depending on the model router you are using, this can be a lot of money just sitting idle.

To solve this problem, we can configure HSRP to be load balanced between routers. This doesn't help us with a single HSRP group, but for multiple HSRP groups we can spread the load and have each HSRP group be active on different routers.

By configuring multiple HSRP groups on a single interface, HSRP load balancing can be achieved. Here is how we accomplish this.

```
R1(config)#interface ethernet0
R1(config-if)#ip address 192.168.1.2
R1(config-if)#standby 1 ip 192.168.1.1
R1(config-if)#standby 1 priority 200
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 name network-one
!
R1(config)#interface ethernet1
R1(config-if)#ip address 10.1.1.2
R1(config-if)#standby 2 ip 10.1.1.1
R1(config-if)#standby 2 name network-two
```

```
R2(config)#interface ethernet0
R2(config-if)#ip address 192.168.1.3
R2(config-if)#standby 1 ip 192.168.1.1
R2(config-if)#standby 1 name network-one
!
R2(config)#interface ethernet1
R2(config-if)#ip address 10.1.1.3
R2(config-if)#standby 2 ip 10.1.1.1
R2(config-if)#standby 2 priority 200
R2(config-if)#standby 2 preempt
R2(config-if)#standby 2 name network-two
```