Bachelor Cycle

Cisco Networking

PW #9

Summary

- Access Control List (ACL)

- ACL
  - Types
  - Standard ACL Configuration
  - Extended ACL Configuration
  - Named ACL Configuration

Access Control List (1/2)

- Allow to control network access (in & ou)

- An ACL is a list of rules

- Defining addresses / ports allowed or prohibited

- Advantages
  - ✧ Limit network traffic
  - ✧ Increase network performance
  - ✧ Restrict routing tables updates
  - ✧ Secure access between networks
  - ✧ Prohibit protocols

Access Control List (2/2)

- An ACL can be apply only on ONE interface

- A standard ACL is apply near the destination

- An extended ACL is apply near the source
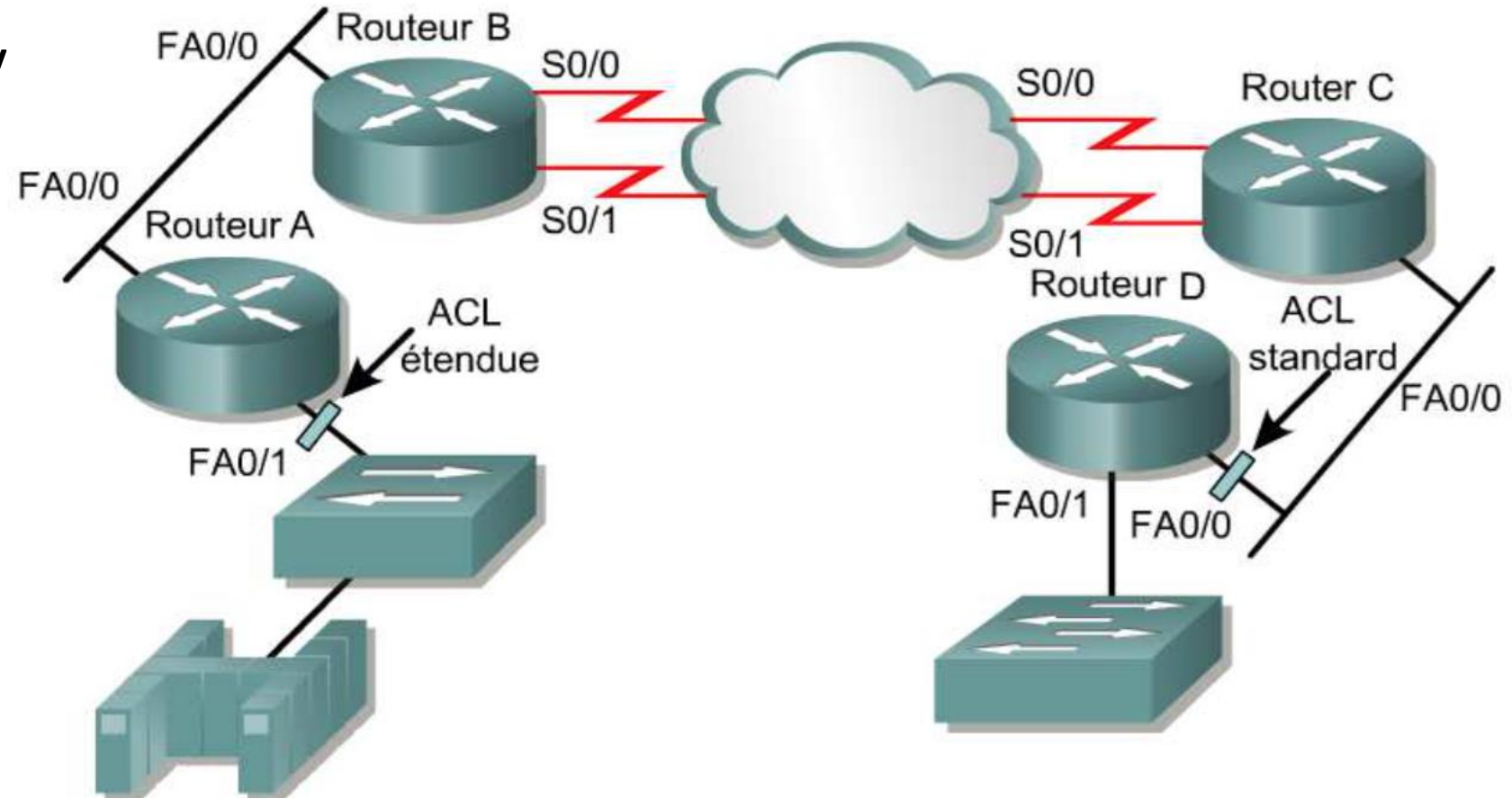
ACLs Types

- Two ACLs types

- Standard ACL
  - ✧ Number between 1 to 99 and 1300 to 1999
  - ✧ Filtering is based only on source addresses

- Extended ACL
  - ✧ Number between 100 to 199 and 2000 to 2699
  - ✧ Filtering based on :
    - ➢ Source and destination addresses
    - ➢ Protocol encoded in the Network Layer header
    - ➢ Port number encoded in the Transport Layer header

Standard ACL Configuration (1/2)

```
Lab1-ro1841-1(config)#>access-list [number] [permit | deny] [source] [wildcard_source]
```

• Assign ACL to an interface

```
Lab1-ro1841-1(config)#>ip access-group <ACL number> {in|out}
```

Standard ACL Configuration

- Example : allow only 172.16.0.0 network

```
Lab1-ro1841-1(config)#>access-list 1 permit 172.16.0.0 0.0.255.255
```

```
Lab1-ro1841-1(config)#interface fastEthernet 0/0
Lab1-ro1841-1(config-if)#ip access-group 1 out
Lab1-ro1841-1(config-if)#>exit
Lab1-ro1841-1(config)#interface fastEthernet 0/1
Lab1-ro1841(config-if)#ip access-group 1 out
Lab1-ro1841-1(config-if)#>exit
```

Extended ACL Configuration

Lab1-ro1841-1(config)#>access-list [number] [permit | deny} [protocol] [addr_source] [wildcard_source] [addr_destination] [wildcard_destination] [operator] [port | number]

- Protocols
  - ✧ Ip - tcp – udp – icmp – ospf – igrp - …etc.
- Operators
  - ✧ Lower than (it) - Greater than (gt) - Equal to (eq) - No equal to (neq)
- Assign ACL to an interface

Lab1-ro1841-1(config)#>ip access-group <ACL number> {in|out}

Named ACL Configuration

- Permit to identify an ACL with a character string

- Authorize to remove entries inside an ACL list

- **<u>Warning</u> : The name must be single**

> Lab1-ro1841-1(config)#>ip access-list {standard|extended} <name>
> Lab1-ro1841(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq www

Practical Work (1/2)

- Set up connectivity in the whole network using RIP or EIGRP

- Set up a web service and a FTP on the host acting as server

- Set up a standard ACL in order to deny access to 192.168.1.0/29 network for host C
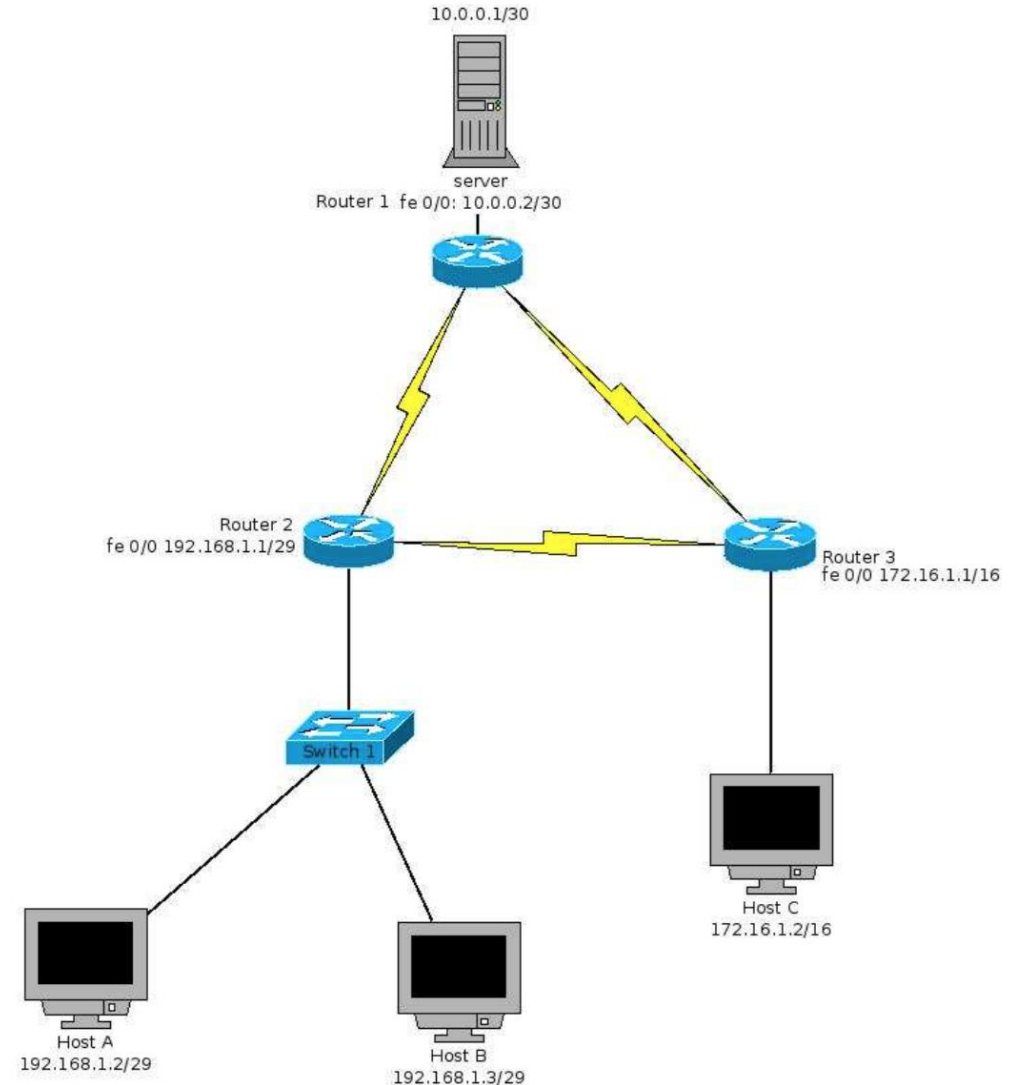
Practical Work (2/2)

- Deny access to web service for the host A and the host B

- Deny access to FTP only for the host B

- Allow ping only on the server for host C

- Configure VTYs on routers in order to accept only connection from host A