



**Antonio Cianfrani**

# **Access Control List (ACL)**

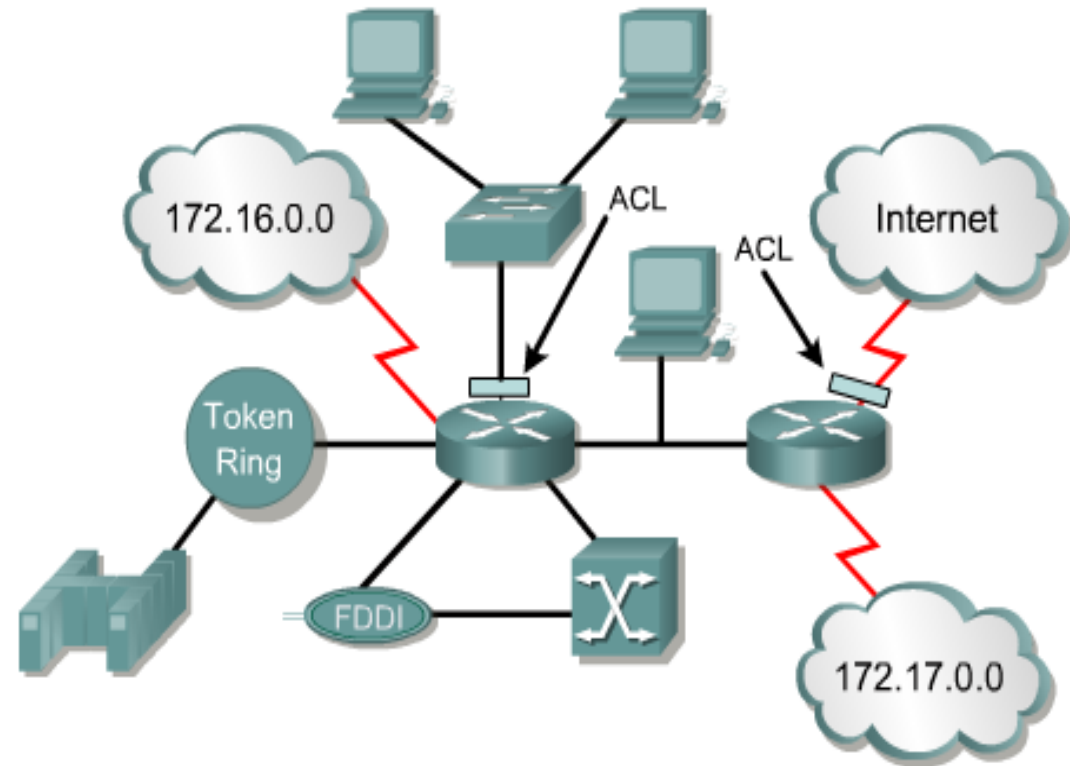
# Index



- **ACL?**
- **How to configure**
  - Standard ACL
  - Extended ACL
  - Named ACL
- **Limiting the vty access**

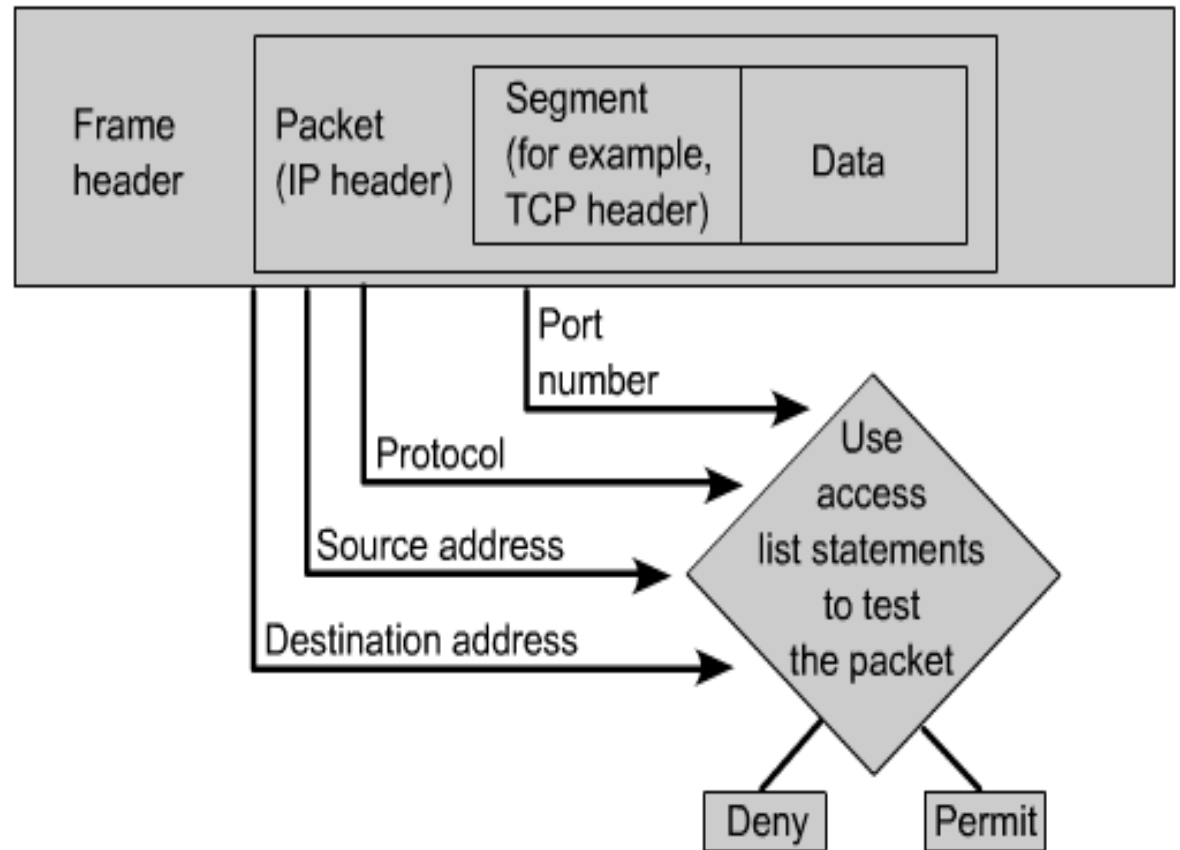
# ACL (1/3)

- Control lists applied to traffic incoming in / outgoing from a router
- Rules to determine if packets must be processed and forwarded or blocked and dropped by the router
- Configured on the router and applied to interfaces to control network access




# ACL (2/3)

- Defined on the basis of the IP addresses, protocol, direction, port, etc...
- The ACL can be applied for incoming packets (**inbound**) or outgoing packets (**outbound**)



# ACL (3/3)



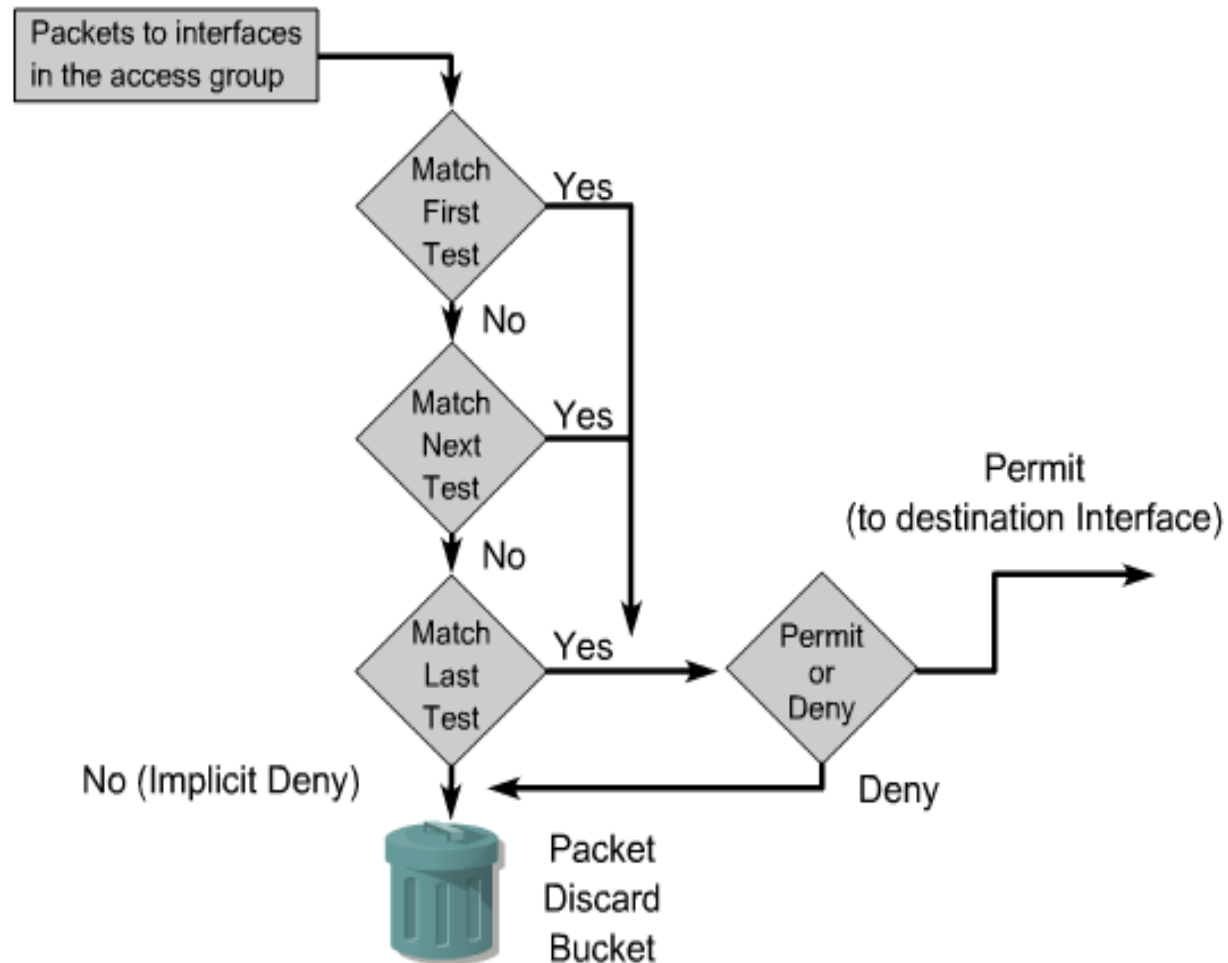
- Motivations
  - Limiting the network traffic
  - Controlling the traffic flows
  - Basic level of security
  - Allowing or denying the network access on the basis of traffic type
- If no ACLs are configured on a router, all the packets will be processed and forwarded

# Inbound & Outbound interface

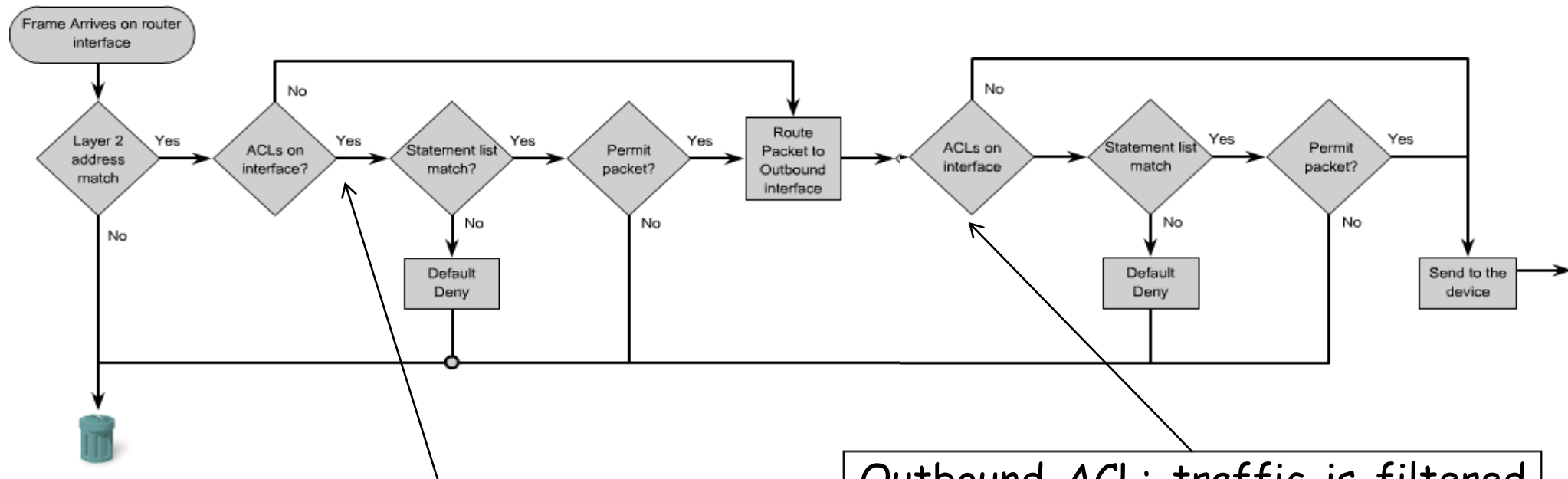
- The packets direction on an interface:
  - ✓ **Inbound:** incoming packets.
  - ✓ **Outbound:** outgoing packets.
- When associating an *ACL* to an interface, the direction must be specified.

# ACL: list of rules

- An ACL is an ordered list of rules about permitting or denying packets processing/forwarding on an interface
- The ordering of rules must be carefully defined!



# ACL implementation



Inbound ACL: traffic is filtered before routing processing ... and applied to all incoming packets

Outbound ACL: traffic is filtered after routing processing ... and applied only to the packets forwarded through this interface



# Creating an ACL (1/2)

- ACL are created in the global configuration mode.
- Three ACL types
  - **Standard:** packets filtering is based only on the source IP address.
  - **Extended:** packets filtering is based on source and destination IP address, protocol, and destination port.
  - **Named:** can be both Standard and Extended, are identified by a name and provide a more flexible configuration procedure.
- Classical Standard and Extended ACLs are identified by a unique (router-level) number (Numbered ACL)
  - Different ranges for standard and extended ACL

# Creating an ACL (2/2)

- The command to define a rule for an ACL identified by number X is "**access-list X**" followed by specific parameters
  - After the definition, an ACL must be associated to one (or more) interface(s) on a specific direction
- The command "**no access-list X**" removes the ACL x
- The command to associate an ACL to an interface is "**ip access-group**", in the interface configuration mode.
- An ACL can be associated also to a sub-interface

# ACL example

```
Router(config)#no access-list 2
```

```
Router(config)#  
access-list 2 deny 172.16.1.1  
access-list 2 permit 172.16.1.0 0.0.0.255  
access-list 2 deny 172.16.0.0 0.0.255.255  
access-list 2 permit 172.0.0.0 0.255.255.255  
interface ethernet 0  
ip access-group 2 in
```

# The wildcard mask (1/2)

- The wildcard mask is a 32 bits string
- A wildcard define the matching of an ACL rule regarding IP addresses
  - 0 → the corresponding value of the IP address must be checked
  - 1 → the corresponding value of the IP address doesn't have to be checked

***172.16.0.0    0.0.255:***

***172.16.2.3 → matching***

***172.15.0.1 → no matching***

# The wildcard mask (2/2)

- Two keywords to be used for ACL definition:
  - any
  - host
- “**any**” means 255.255.255.255 for the wildcard mask:
  - Always a matching, independently of the IP address.
- “**host**” means 0.0.0.0 for the wildcard mask:
  - All the bits of the IP address must be checked.

# Verifying the ACL (1/3)

- "show ip interface"
- "show access-list"
- "show running-config"

# Verifying the ACL (2/3)

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set ←
  Inbound access list is 2 ←
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set ←
  Inbound access list is 101 ←
```

# Verifying the ACL (3/3)

```
Router#show access-lists
Standard IP access list 2
  deny   172.16.1.1
  permit 172.16.1.0, wildcard bits 0.0.0.255
  deny   172.16.0.0, wildcard bits 0.0.255.255
  permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
  permit tcp 192.168.6.0 0.0.0.255 any eq telnet
  permit tcp 192.168.6.0 0.0.0.255 any eq ftp
  permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny   172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq telnet
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq ftp
.
```



# Standard ACL (1/3)

- A standard ACL filters on the basis of the source IP address
  - The access-list number must be in the range [1, 99] (also [1330, 1999] in last IOS version)
- The command syntax is :

```
Router(config)#access-list access-list-number  
{deny | permit} source [source-wildcard ]
```

- To remove the ACL:

```
Router(config)#no access-list access-list-number
```

# Standard ACL (2/3)

```
access-list 2 deny    172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny    172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0  0.255.255.255
```

- Access list number range of 1-99
- Filter only on source IP address
- Wildcard masks
- Applied to port closest to destination

# Standard ACL (3/3)

Parameter	Description
<i>access-list-number</i>	Number of an ACL. This is a decimal number from 1 to 99 (for a standard IP ACL).
<b>deny</b>	Denies access if the conditions are matched.
<b>permit</b>	Permits access if the conditions are matched.
<i>source</i>	Number of the network or host from which the packet is being sent. There are two ways to specify the <i>source</i> : <ul style="list-style-type: none"><li>•Use a 32-bit quantity in four-part, dotted- decimal format.</li><li>•Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.55.</li></ul>
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the source. There are two ways to specify the <i>source-wildcard</i> : <ul style="list-style-type: none"><li>•Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</li><li>•Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.</li></ul> (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the <b>logging console</b> command.)
<b>log</b>	The message includes the ACL number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at five-minute intervals, including the number of packets permitted or denied in the prior five-minute interval.

# Standard ACL: summary

<b>Step 1</b>	<p>Define the ACL by using the following command:</p> <pre>Router(config)#<b>access-list</b> <i>access-list-number</i>     {<b>permit</b>   <b>deny</b>} {<i>test-conditions</i>}</pre> <p>A global statement identifies the ACL. Specifically, the 1-99 range is reserved for standard IP. This number refers to the type of ACL. In Cisco IOS Release 11.2 or newer, ACLs can also use an ACL name, such as <code>education_group</code>, rather than a number.</p> <p>The <b>permit</b> or <b>deny</b> term in the global ACL statement indicates how packets that meet the test conditions are handled by Cisco IOS software. <b>permit</b> usually means the packet will be allowed to use one or more interfaces that you will specify later. The final term or terms specifies the test conditions used by the ACL statement.</p>
<b>Step 2</b>	<p>Next, you need to apply ACLs to an interface by using the <b>access-group</b> command, as in this example:</p> <pre>Router(config-if)#{<i>protocol</i>} <b>access-group</b> <i>access-list-number</i></pre> <p>All the ACL statements identified by <i>access-list-number</i> are associated with one or more interfaces. Any packets that pass the ACL test conditions can be permitted to use any interface in the access group of interfaces.</p>

# Extended ACL (1/4)

- The Extended ACLs provide a more accurate control on network traffic.
- The Extended ACLs allow to filter traffic considering **IP source and destination addresses, the protocol and the destination port number**.
  - Example: an extended ACL can permit e-mail traffic toward a specific destination and denies file transfers and web browsing toward the same destination.
- The command syntax is similar to the one of standard ACL: *"access-list"*
- The *"ip access-group"* command associate an extended ACL to an interface

# Extended ACL (2/4)

- The ACL statements could be very long.
  - Can be simplified using the *host* and *any* options
- The port number field is optional:
  - equal (eq), not equal (neq), greater than (gt) and less than (lt).
- The extended ACL identifier must belong to the range [101,199].

# Extended ACL (3/4)

```
Router(config)#access-list access-list-number {permit | deny}  
protocol source  
[source-mask destination destination-mask operator operand]  
[established]
```

Paramter	Description
<i>access-list-number</i>	Identifies the list using a number in the range 100 to 199.
<b>permit</b>   <b>deny</b>	Indicates whether this entry allows or blocks the specified address.
<i>protocol</i>	The protocol, such as IP, TCP, UDP, ICMP, GRE, or IGRP.
<b>source</b> and <b>destination</b>	Identifies source and destination addresses.
<i>source-mask</i> and <i>destination-mask</i>	Wildcard mask; zeros indicate positions that must match, ones indicate do not care positions.
<i>operator operand</i>	lt, gt, eq, neq (less than, greater than, equal, not equal), and a port number.
<b>established</b>	Allows TCP traffic to pass if the packet uses an established connection (for example, has ACK bits set).

# Extended ACL (4/4)

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Access list number range of 100-199
- Source destination IP address
- Layer 4 protocol number
- Applied to port closest to source host



# Port Numbers

```
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

Transport Protocol (119)

pim-auto-rp PIM Auto-RP (496)

pop2 Post Office Protocol v2 (109)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

sunrpc Sun Remote Procedure Call (111)

syslog Syslog (514)

tacacs TAC Access Control System (49)

talk Talk (517)

telnet Telnet (23)

time Time (37)

uucp Unix-to-Unix Copy Program (540)

whois Nicname (43)

www World Wide Web (HTTP, 80)

# Named ACL (1/3)

- The named ACLs are identified by a name.
- A named ACL can be standard or extended
- named ACLs can be modified with no need of starting from scratch
  - It is possible to remove a single statement and to add a new one in any position
- The command to create a named ACL is "ip access-list"
  - An ACL sub-configuration CLI exists

# Named ACL (2/3)

```
ip access-list {extended|standard} name
```

```
router(config-ext-nacl)#permit|deny protocol source  
source-wildcard [operator [port]] destination  
destination-wildcard [operator [port]] [established]  
[precedence precedence] [tos tos] [log] [time-range time-  
range-name]
```

```
ip interface ethernet0/5  
ip address 192.168.5.1 255.255.255.0  
ip access-group Internetfilter out  
ip access-group marketinggroup in  
...  
ip access-list standard Internetfilter  
permit 10.1.1.1  
deny any  
ip access-list extended marketing_group  
permit tcp any 172.30.0.0.0.255.255.255 eq telnet  
deny udp any any  
deny udp any 171.30.0.0.0.255.255.255 lt 1024  
deny ip any log
```

# Named ACL (3/3)

```
Rt1(config)#ip access-list extended server-access
Rt1(config-ext-nacl)#permit TCP any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit UDP any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#^Z
Applying the named list:
Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

# Modificare una Named ACL

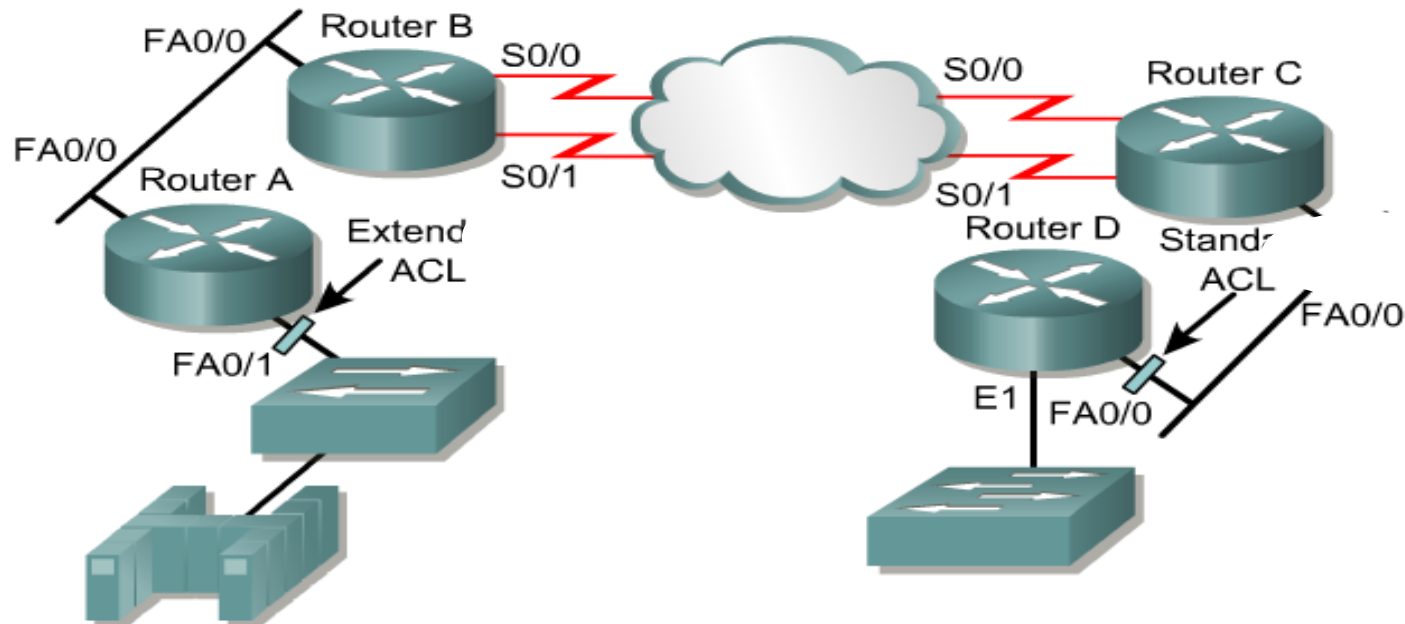
```
R1(config)#ip access-list extended SERVER-ACCESS
R1(config-ext-nacl)# no 20
R1(config-ext-nacl)# 20 permit ip host 192.168.1.77 any
R1(config-ext-nacl)# end
R1#show access-lists
Extended IP access list SERVER-ACCESS
 10 permit ip host 192.168.1.66 host 192.168.3.75
 20 permit ip host 192.168.1.77 any
 30 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75
```

```
R1(config)#ip access-list extended SERVER-ACCESS
R1(config-ext-nacl)# 25 deny ip host 192.168.1.88 any
R1(config-ext-nacl)# end
R1#show access-lists
Extended IP access list SERVER-ACCESS
 10 permit ip host 192.168.1.66 host 192.168.3.75
 20 permit ip host 192.168.1.77 any
 25 deny ip host 192.168.1.88 any
 30 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75
```

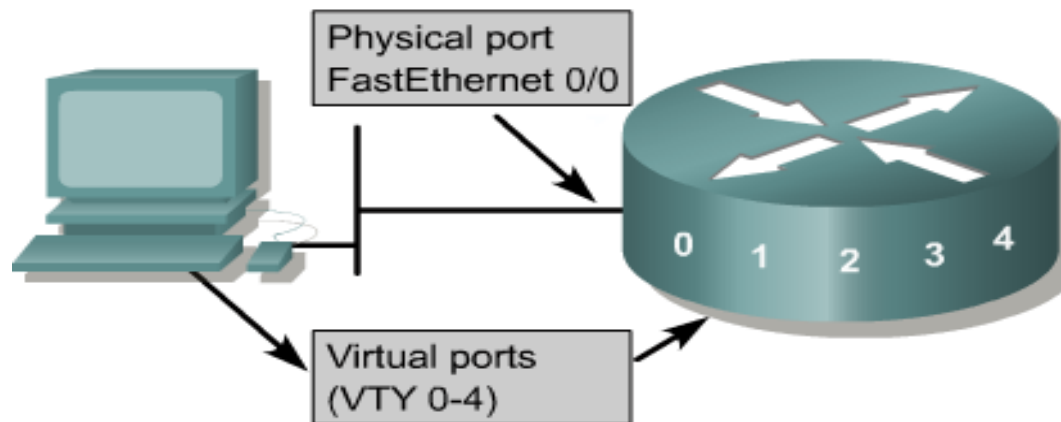
# Locating the ACL

## ■ General rules:

- The standard ACLs should be put as close as possible to the destination (since it is not possible to specify the destination)
- The extended ACLs should be put as close as possible to the source (to filter earlier the traffic, and so reducing routers work)



# Limiting the telnet access



## Cisco - Hyperterminal

Creating the standard list:

```
Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
```

```
Rt1(config)#access-list 2 permit 172.16.2.0 0.0.0.255
```

```
Rt1(config)#access-list 2 deny any
```

Applying the access list:

```
Rt1(config)#line vty 0 4
```

```
Rt1(config)#login
```

```
Rt1(config)#password secret
```

```
Rt1(config)#access-class 2 in
```