

# ACCESS LIST standard

Le ACL (Access Control List) sono una lista di comandi che vengono applicati in sequenza alle interfacce di un router allo scopo di filtrare i pacchetti in entrata e in uscita.

Le ACL possono essere usate per tutti i protocolli di rete routabili.

La ACL possono essere adoperate per:

1. Fornire un livello base di sicurezza: ad esempio restringendo gli accessi a una determinata rete o sottorete;
2. Definire quali pacchetti debbano essere processati prima di altri in modo da aumentare la performance di una rete (queuing)
3. Decidere il tipo di traffico che può transitare ad esempio permettendo l'invio di mail e/o impedire l'accesso tramite Telnet.

Le clausole ACL vengono elaborate dal router sequenzialmente seguendo l'ordine con cui sono state inserite. L'elaborazione si interrompe appena un pacchetto soddisfa una condizione. Se nessuna condizione è soddisfatta il pacchetto viene scartato.

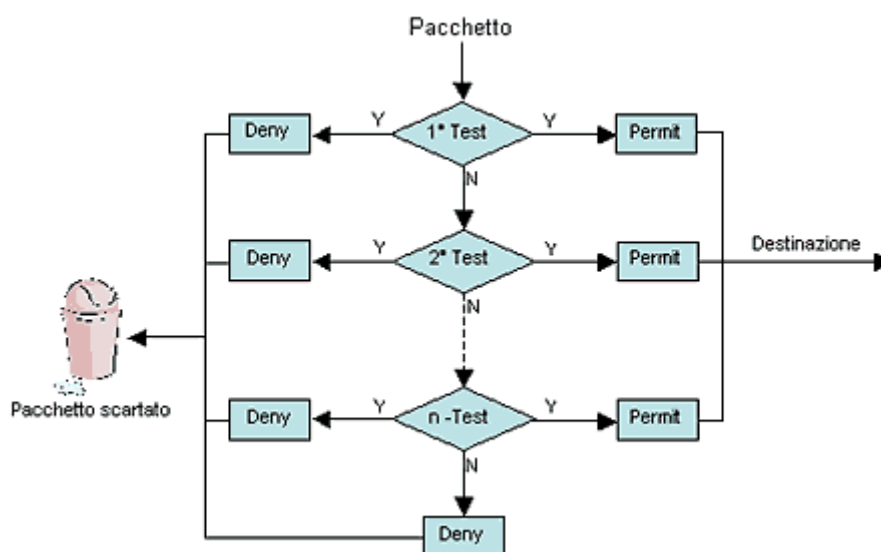


Figura 1

## Configurazione di una ACL

La creazione di ACL su un router Cisco deve seguire i seguenti passi:

**1.** Definire la ACL con il comando:

```
Router(config)# access-list access-list number {permit|deny} {test-conditions}
```

- *access-list number* è il numero univoco che identifica ogni ACL e che ne definisce il tipo (vedi tabella). Dalla versione 11.2 del Cisco IOS si può utilizzare un nome al posto del numero.

Protocollo	Range Access-list number
IP ( <i>deprecato</i> )	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

- Permit e deny definiscono le condizioni:  
Permit indica che il pacchetto ha il permesso di utilizzare una o più interfacce specificate di seguito;  
deny indica che il pacchetto deve essere rimosso.

**2.** si deve applicare la ACL a una o più interfacce:

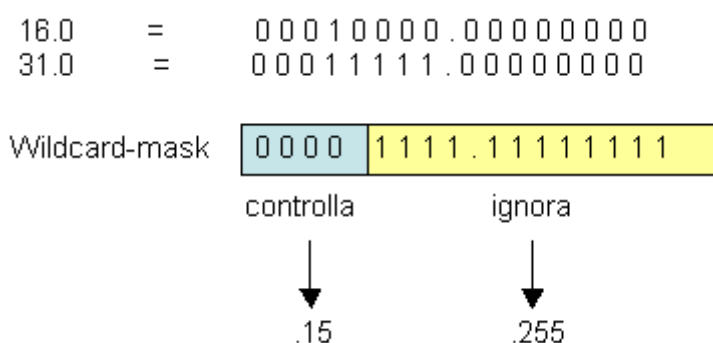
Router(config-if)# **access-group** access-list number

#### La wildcard mask

La wildcard mask è un numero di 32-bit diviso in 4 ottetti, simile alla subnet-mask. La differenza sostanziale è che la wildcard-mask indica quali bit di un indirizzo IP devono essere controllati in un'ACL: il valore 0 nella wildcard-mask indica che il bit corrispondente deve essere controllato, il valore 1 che deve essere ignorato.

Es. Si supponga di voler testare gli indirizzi IP da 172.50.16.0 a 172.50.31.0.

In questo caso conviene analizzare esclusivamente gli ultimi due ottetti:



Per cui, in questo caso, la wildcard-mask avrà la forma 0.0.15.255.

Si possono anche utilizzare delle abbreviazioni. Nel caso si vogliano controllare tutti gli indirizzi (Cisco li indica con l'IP 0.0.0.0) si può utilizzare il termine any; per un singolo indirizzo si utilizza il termine host.

**Es.**

Invece di utilizzare la sintassi

```
Router(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```

```
Router(config)# access-list 1 permit 172.30.24.12 0.0.0.0
```

si può utilizzare

```
Router(config)# access-list 1 permit any
```

```
Router(config)# access-list 1 permit host 172.30.24.12
```

## ACCESS LIST estese

Le ACL estese forniscono una maggiore flessibilità e controllo se paragonate a quelle standard. Le ACL estese, infatti, possono effettuare il controllo non solo sull'indirizzo del mittente, ma anche su quello del destinatario, su uno specifico protocollo, sul numero di porta o su altri parametri.

### Configurazione di un'ACL Estesa

Per definire un'ACL Estesa sui router Cisco entrare in configuration mode ed eseguire i seguenti passi:

1. Sintassi **access-list** estesa:

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

Parametri	Descrizione
<i>Access-list-number</i>	Numero dell'ACL. Ne indica il nome e il tipo (es. da <b>100</b> a <b>199</b> e da <b>2000</b> a <b>2699</b> per le ACL IP Estese).
<i>Permit</i>	Permette l'accesso se le condizioni sono soddisfatte
<i>Deny</i>	Nega l'accesso se le condizioni sono soddisfatte
<i>Protocol</i>	Il protocollo di comunicazione; es. IP, TCP, UDP, ICMP, IGRP, ...
<i>Source e Destination</i>	Indirizzo del mittente e del destinatario / any.
<i>Souce-wildcard e Destination-wildcard</i>	La wildcard mask che deve essere applicata all'indirizzo sorgente e a quello di destinazione / any.
<i>Operator operand</i>	Un operatore logico: lt, gt, eq, neq, range (less than, greater than, equal, not equal, range) <b>e il numero o il nome della</b>

	<b>porta</b> TCP o UDP. Nel caso dell'operatore <i>range</i> occorre inserire due valori <i>operand</i> (es. range 21 25)																																				
	<table><tr><th>Porta</th><th>Keyword</th><th>Descrizione</th><th>TCP/UDP</th></tr><tr><td>20</td><td>FTP-DATA</td><td>FTP (data)</td><td>TCP</td></tr><tr><td>21</td><td>FTP</td><td>FTP</td><td>TCP</td></tr><tr><td>23</td><td>TELNET</td><td>Terminal connection</td><td>TCP</td></tr><tr><td>25</td><td>SMTP</td><td>SMTP</td><td>TCP</td></tr><tr><td>42</td><td>NAMESERVER</td><td>Host Name Server</td><td>UDP</td></tr><tr><td>53</td><td>DOMAIN</td><td>DNS</td><td>TCP/UDP</td></tr><tr><td>69</td><td>TFTP</td><td>TFTP</td><td>UDP</td></tr><tr><td>80</td><td></td><td>WWW</td><td>TCP</td></tr></table>	Porta	Keyword	Descrizione	TCP/UDP	20	FTP-DATA	FTP (data)	TCP	21	FTP	FTP	TCP	23	TELNET	Terminal connection	TCP	25	SMTP	SMTP	TCP	42	NAMESERVER	Host Name Server	UDP	53	DOMAIN	DNS	TCP/UDP	69	TFTP	TFTP	UDP	80		WWW	TCP
Porta	Keyword	Descrizione	TCP/UDP																																		
20	FTP-DATA	FTP (data)	TCP																																		
21	FTP	FTP	TCP																																		
23	TELNET	Terminal connection	TCP																																		
25	SMTP	SMTP	TCP																																		
42	NAMESERVER	Host Name Server	UDP																																		
53	DOMAIN	DNS	TCP/UDP																																		
69	TFTP	TFTP	UDP																																		
80		WWW	TCP																																		
<i>Established</i>	(Optional) Si utilizza solo con il protocollo TCP: indica una "established connection". Il controllo viene effettuato solo se il datagramma ha settato il bit di ACK o RST, mentre non ci sono controlli sul pacchetto iniziale per stabilire la connessione.																																				
<i>Precedence</i>	(Optional) Indica un numero da 0 a 7, che specifica la precedenza del pacchetto rispetto a un altro (Queuing).																																				
<i>Log</i>	(Optional) Attiva i messaggi di log. Questi comprendono l'indirizzo sorgente, il numero di pacchetti e l'esito del controllo (permit o deny). I log vengono generati a intervalli di 5 minuti.																																				

## 2. Sintassi **access-group**:

Router(config-if)# **ip access-group** *access-list number* {**in**|**out**}

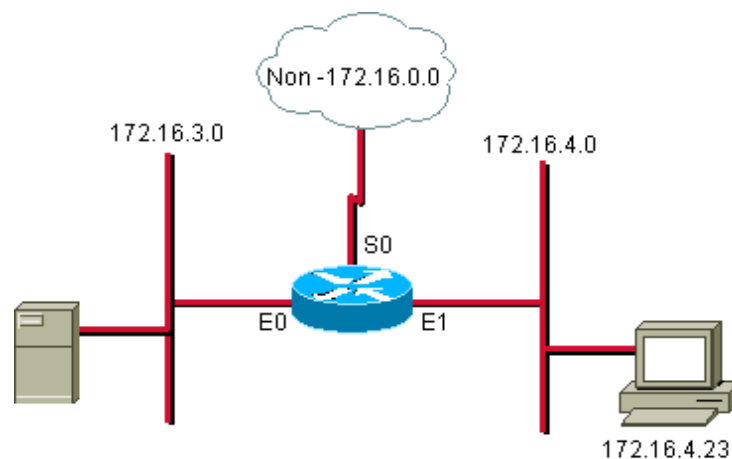
Parametri	Descrizione
Access-list-number	Indica il numero della ACL che deve essere legata all'interfaccia.
In out	Specifica se la ACL va applicata all'interfaccia in entrata o in uscita. Un'ACL in input fa sì che il router applichi prima l'ACL e poi effettui il routing, mentre in output prima il routing e poi l'ACL. Se non è specificato, per default è out.

Nota: Per cancellare un ACL o rimuoverla da un'interfaccia del Router occorre utilizzare rispettivamente i seguenti comandi:

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

Router(config-if)# **no ip access-group** *access-list number*

E' consigliabile, prima di cancellare un'ACL, rimuoverla da tutte le interfacce.

**ESEMPI DI ACL ESTESE****Figura 1**

**Esempio n. 1:** negare il traffico FTP da una determinate rete o sottorete

Questo esempio dimostra come bloccare esclusivamente il traffico FTP.

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21  

access-list 101 permit ip 172.16.4.0 0.0.0.255 any  

(access-list 101 deny any any – implicit, non visibile nella lista)
```

```
interface ethernet 0  

ip access-group 101
```

**Esempio n. 2:** permettere esclusivamente l'invio di E-mail

In questo esempio viene bloccato sull'interfaccia E0 tutto il traffico a esclusione della posta elettronica.

```
access-list 102 permit tcp 172.16.3.0 0.0.0.255 any eq 25 (o eq smtp)  

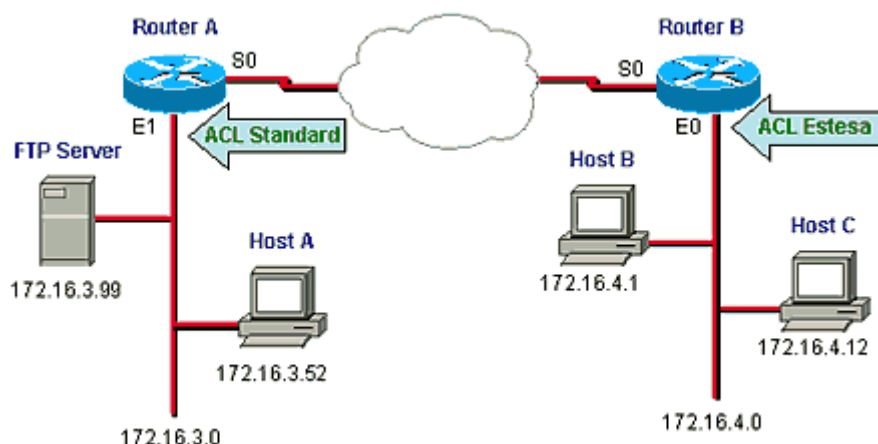
(access-list 102 deny any any– implicit, non visibile nella lista)
```

```
interface ethernet 0  

ip access-group 102 out
```

**ESEMPIO**

Si vuole negare all'host B l'accesso al Server FTP e allo stesso tempo negare all'host C qualsiasi accesso alla rete 172.16.3.0.



**Figura 2**

**Sul Router A:**

```
access-list 1 deny host 172.16.4.12
access-list 1 permit any
```

```
interface ethernet 1
ip access-group 1
```

```
access-list 101 deny tcp host 172.16.4.15 172.16.3.0 0.0.0.255 eq ftp
access-list 101 permit ip 172.16.4.0 0.0.0.255 any
```

```
interface ethernet 0
ip access-group 101
```

## Verificare le ACL

Per visualizzare le informazioni sulle ACL si possono utilizzare i seguenti comandi:

Router> **show access-list** [access-list number]: mostra il contenuto di tutte le ACL caricate sul router (utilizzando l'opzione *access-list number* vengono elencate solo le condizioni di una determinata ACL);

Router> **show ip interface** [interface-type number] : mostra le informazioni sulle interfacce IP e quindi anche la presenza di un'eventuale ACL collegata all'interfaccia (le opzioni *interface-type* e *number* permettono di indicare una determinata interfaccia).