

ACL standard ed estesa con Packet Tracer

Le ACL (Access Control List) sono una lista di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita.

Esistono due tipi di ACL, standard ed estese:

1. Le **ACL standard** vengono utilizzate per bloccare o permettere il traffico da una rete o da un host specifico o per negare una suite di protocolli. L'aspetto fondamentale delle ACL standard è che il controllo viene esclusivamente effettuato sull'indirizzo sorgente.
2. Le **ACL estese** forniscono una maggiore flessibilità e controllo poichè 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.

Le ACL possono essere usate per tutti i protocolli di routing.

Esistono varie ragioni per decidere di adoperare le ACL:

- **Fornire un livello base di sicurezza:** si può per esempio restringere l'accesso ad una determinata rete o sottorete;
- **Limitare il traffico e aumentare la performance della rete:** si può, infatti, decidere che alcuni pacchetti vengano processati prima di altri. Questo viene in particolare riferito come queuing.
- **Decidere quale tipo di traffico può essere trasmesso:** si può permettere l'invio di e-mail ed impedire allo stesso tempo il Telnet.

Le ACL vengono elaborate dal router in maniera sequenziale in base all'ordine in cui sono state inserite le varie clausole. Appena un pacchetto soddisfa una delle condizioni, la valutazione s'interrompe ed il resto delle ACL non viene preso in considerazione. Il pacchetto viene quindi inoltrato o eliminato secondo l'istruzione eseguita. Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (si considera che alla fine di un ACL non vuota ci sia l'istruzione deny any ovvero nega tutto). Infatti, se un'access-list è vuota, il router sottintende **permit any**, se invece, presenta anche una sola entry, il router considera un **deny any** implicito.

L'ordine con cui sono scritte le ACL è importante: essendo eseguite in sequenza, è necessario inserire le condizioni più restrittive all'inizio e poi quelle più generiche.

Sui router Cisco, ogni ACL è identificata da un numero univoco che ne definisce il tipo:

- da 1 a 99 e da 1300 a 1999 sono le ACL Standard che si riferiscono al protocollo IP;
- da 100 a 199 e da 2000 a 2699 sono le ACL estese riferite a IP.

La sintassi del comando per creare una **ACL Standard** sui router Cisco è:

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

Il significato dei parametri presenti nel comando è descritto nella seguente tabella:

Parametri	Descrizione
Access-list-number	indica il nome e il tipo di ACL (es. da 1 a 99 per le ACL IP standard)
Permit	Permette l'accesso se le condizioni sono soddisfatte
Deny	Nega l'accesso se le condizioni sono soddisfatte
Source	Introduce l'indirizzo sorgente del pacchetto
Source wildcard	Indica la wildcard mask che deve essere applicata all'indirizzo sorgente (opzionale, se viene omessa di default viene messa a 0.0.0.0 che indica l'indirizzo di un host)
Log	Attiva i messaggi di log che 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. opzionale

Una volta definite le condizioni si deve applicare la ACL all'interfaccia desiderata,

il comando da usare è:

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

dove: in|out specifica se la ACL va applicata all'interfaccia in entrata o in uscita.

Una ACL in input fa sì che il router applichi prima la ACL e poi effettui il routing, mentre in output prima il routing e poi la ACL.

NOTA: Su un router si può definire un' ACL per il protocollo IP per ogni interfaccia logica (ogni interfaccia "subif" può avere la propria ACL), per ogni direzione (IN o OUT). Ad esempio, se prendiamo l'interfaccia Ethernet 0/0 di un router, possiamo avere per quest'interfaccia al massimo 2 ACL, una in ingresso ed una in uscita.

Quando si crea una ACL, i **parametri host e any sono utilizzabili al posto delle wildcard:**

```
access-list 9 deny 192.168.15.99 0.0.0.0 <=> access-list 9 deny host 192.168.15.99
```

Sequenza di passi per la creazione delle ACL standard

1. Entrare nel CLI (Command Line Interface) del router
2. Entrare in modalità configurazione (configure terminal)
3. Assegnare un nome all'access list (ad esempio per le standard 1-99)
4. Indicare se permette o nega (permit-deny)
5. Inserire IP dell'host o della rete
6. Ripetere i passaggi 4-5 per inserire altre regole
7. Assegnare la regola creata all'interfaccia(interface *nome interfaccia*)
8. Assegnare la regola all'interfaccia selezionata in input-output

Esempio

R1>enable

R1#configure terminal

R1(config)#access-list 1 deny 192.168.1.1 0.0.0.0 *(blocca host con IP 192.168.1.1, utilizzando la wildcard)*

R1(config)#access-list 1 permit any *(permette a tutti gli altri ip di essere inoltrati)*

R1(config)#interface fastEthernet 0/1 *(apertura della configurazione dell'interfaccia)*

R1(config-if)#ip access-group 1 out *(assegnazione regole dell'ACL 1 all'interfaccia in modalità output)*

Comandi utili:

Router# **show access-lists** *(Visualizza le ACL presenti nel Router)*

Router# **show ip access-lists** *(Visualizza le IP ACL presenti nel Router)*

Router# **show access-lists id_ACL** *(Visualizza il contenuto di una ACL)*

Router# **show ip interface** *(Visualizza il posizionamento e la direzione delle ACL)*

Router# **show ip interface nome_interfaccia** *(Visualizza le ACL applicate ad un'interfaccia specifica)*

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** *(Elimina l'intera ACL con il numero specificato)*

Router(config-if)#**no ip access-group access-list number** *(Rimuove, dall'interfaccia su cui si sta operando, la ACL con il numero specificato)*

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

È possibile eliminare le singole entry di una ACL, usando i comandi seguenti:

Router(config)# **ip access-list {standard|extended} access-list-number**

Router(config-std-nacl)# **no entry-number**

Esempio

Router# **show access-lists** *(visualizzo le ACL)*

```
Standard IP access list 10
 10 permit 192.168.0.0 0.0.0.255
 20 permit host 192.168.2.1
 30 permit host 192.168.3.1
 40 deny any
```

Se ad esempio voglio cancellare la regola 20:

Router# **conf t**

Router(config)# **ip access-list standard 10** *(entra nella modalità di configurazione della ACL)*

Router(config-std-nacl)#**no 20** *(elimina la singola entry)*

Configurazione di una ACL estesa sui router CISCO

NOTA: Poichè il default è *deny all*, tutto quello che si vuol far transitare deve essere espressamente specificato.

Entrare in *configuration mode* e definire l'**ACL estesa** secondo la sintassi:

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

Il significato dei parametri presenti nel comando è descritto nella seguente tabella:

Parametri	Descrizione
Access-list-number	Numero dell'ACL. Ne indica il nome e il tipo (es. da 100 a 199 e da 2000 a 2699 per le ACL IP Estese). E' importante ricordare che le ACL estese utilizzano <i>access-list number</i> differenti da quelli utilizzati dalle standard, anche se riferiti allo stesso protocollo.
Permit	Permette l'accesso se le condizioni sono soddisfatte
Deny	Nega l'accesso se le condizioni sono soddisfatte
Protocol	Il protocollo di comunicazione; es. IP, TCP, UDP, ICMP, IGRP, ...
Source e Destination	Indirizzo del mittente e del destinatario.
Souce-wildcard e Destination-wildcard	La wildcard mask che deve essere applicata all'indirizzo sorgente e a quello di destinazione.

Per visualizzare le informazioni sulle ACL si possono utilizzare gli analoghi comandi utilizzati per le ACL standard.

Una ACL IP **estesa per TCP** è composta nel modo seguente:

- access-list acl-number {permit | deny} tcp
- {source source-wildcard | any}
- {destination destination-wildcard | any}
- [operator destination-port][destination-port]

dove

- operator può essere: lt,gt,eq,neq.
- destination-port: è il solito intero a 16 bit senza segno

Una ACL IP, **estesa per ICMP**, è composta nel modo seguente:

- access-list acl-number {permit | deny} icmp
- {source source-wildcard | any}
- {destination destination-wildcard | any}
- [icmp-type [icmp-code] | icmp-message]

I messaggi ICMP possono essere filtrati in base ad icmp-type, icmp-type + icmp-code o come icmp-message.

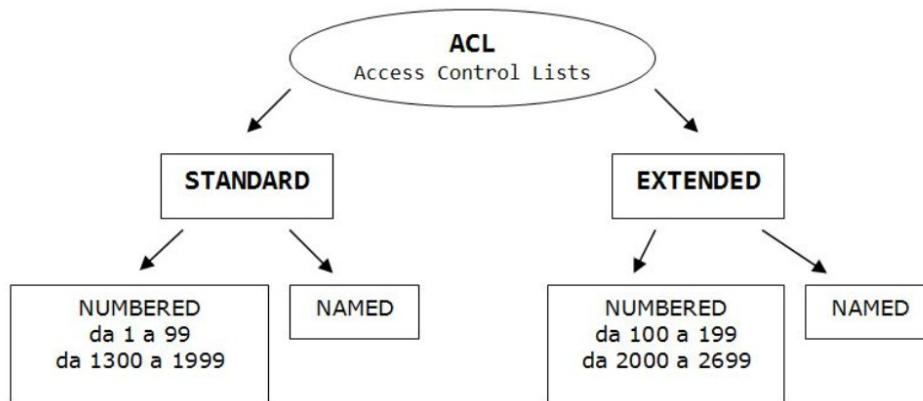
Una ACL IP **estesa per UDP** è composta come di seguito:

- access-list acl-number {permit | deny} udp
- {source source-wildcard | any}
- {destination destination-wildcard | any}
- [operator destination-port][destination-port]

dove

- operator può essere: lt,gt,eq,neq

Le ACL Standard ed Estese, possono essere sia numeriche che con nome (scelto dall'amministratore)



Sintassi per creare una ACL standard named:

```
Router(config)#ip access-list standard nome_ACL
Router(config-std-nacl)# [deny|permit] ip-sorgente
```

Si noti che, a differenza delle ACL numeriche, il comando **access-list** è preceduto dal comando **IP**.

Esempio:

```
Router(config)#ip access-list standard mia_acl
Router(config-std-nacl)#permit 192.168.10.0 0.0.0.255
```

Nel caso si una ACL named, per assegnarla ad un'interfaccia, basta usare il solito comando, utilizzando questa volta il nome dell'ACL. Ad esempio:

```
Router(config)#interface fa 0/0
Router(config-if)#ip access-group mia_acl out
```

Sintassi per creare una ACL estesa named:

```
Router(config)#ip access-list extended nome-ACL
Router(config-ext-nacl)# deny|permit protocollo ip_sorgente wildcard_mask
ip_destinazione wildcard_mask condizione applicazione
```

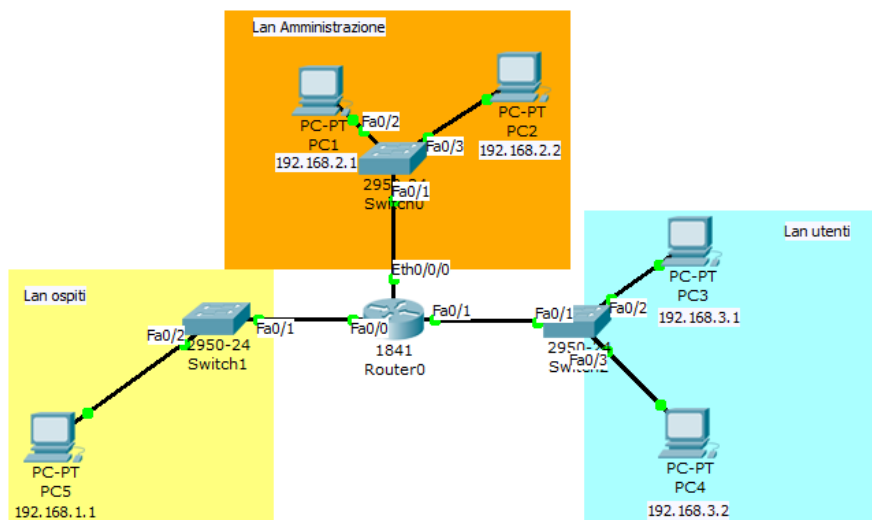
Esempio:

```
Router(config)#ip access-list extended blocco-telnet
Router(config-ext-nacl)#access-list 101 deny tcp 172.16.2.0 0.0.0.255 any eq telnet
```

Esercitazione 1

Creare una **ACL standard** che blocchi i pacchetti in transito dal router dalla LAN Ospiti alla LAN Utenti, permettendo allo stesso tempo alla LAN Amministrazione di poter inviare e ricevere i pacchetti con tutte le LAN presenti nella rete.

Schema logico



Schema indirizzamenti IP









Nome Lan	IP	Subnet-mask	Nome host	Gateway
Lan Amministrazione	192.168.2.1	255.255.255.0	PC1	192.168.2.1 28
Lan Amministrazione	192.168.2.2	255.255.255.0	PC2	192.168.2.1 28
Lan Ospiti	192.168.1.1	255.255.255.0	PC5	192.168.1.1 28
Lan Utenti	192.168.3.1	255.255.255.0	PC3	192.168.3.1 28
Lan Utenti	192.168.3.2	255.255.255.0	PC4	192.168.3.1 28

Configurazione router

Router(config)#access-list 1 permit 192.168.2.0 0.0.0.255	permette a tutti gli host della rete Amministrazione di inviare e ricevere i pacchetti
Router(config)#access-list 1 deny any	blocca tutti i pacchetti delle altre reti LAN
Router(config)#int f0/1	apre l'interfaccia fast-ethernet 0/1
Router(config-if)#ip access-group 1 out	assegna all'interfaccia la regola ACL 1 in output
Router(config-if)#exit	Termina la configurazione dell'interfaccia
Router(config)#int f0/0	apre l'interfaccia fast-ethernet 0/0
Router(config-if)#ip access-group 1 out	assegna all'interfaccia la regola ACL 1 in output
Router(config-if)#^Z	Permette l'uscita dalla modalità di configurazione
Router#	

Verifica funzionalità

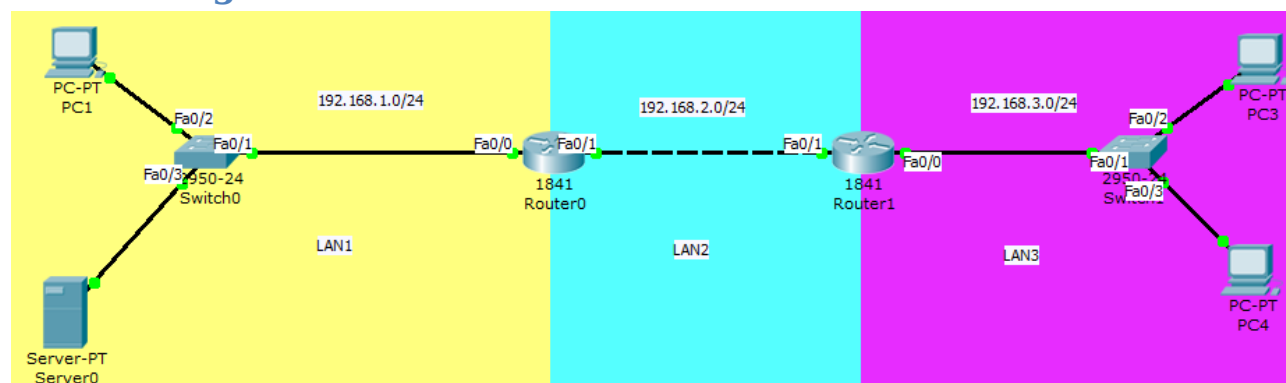
Effettuare dei ping di verifica e controllo tra le postazioni e verificare la corretta configurazione del router.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC5	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC5	PC4	ICMP		0.000	N	2	(edit)	(delete)
	Failed	PC3	PC5	ICMP		0.000	N	3	(edit)	(delete)

Esercitazione 2

Realizzare una **ACL estesa** per bloccare l'accesso al WEB-Server installato nella LAN1 da parte della LAN3, tranne che per l'host 192.168.3.1. La ACL dovrà bloccare inoltre tutti gli altri tipi di pacchetto.

Schema logico



Schema indirizzamenti IP

Nome Lan	IP	Subnet-mask	Nome host	Gateway
Lan 1	192.168.1.1	255.255.255.0	PC1	192.168.1.128
Lan 1	192.168.1.100	255.255.255.0	SERVER-0	192.168.1.128
Lan 2	192.168.2.128	255.255.255.0	ROUTER-0 F0/1	
Lan 2	192.168.2.129	255.255.255.0	ROUTER-1 F0/1	
Lan 3	192.168.3.1	255.255.255.0	PC3	192.168.3.128
Lan 3	192.168.3.2	255.255.255.0	PC3	192.168.3.128

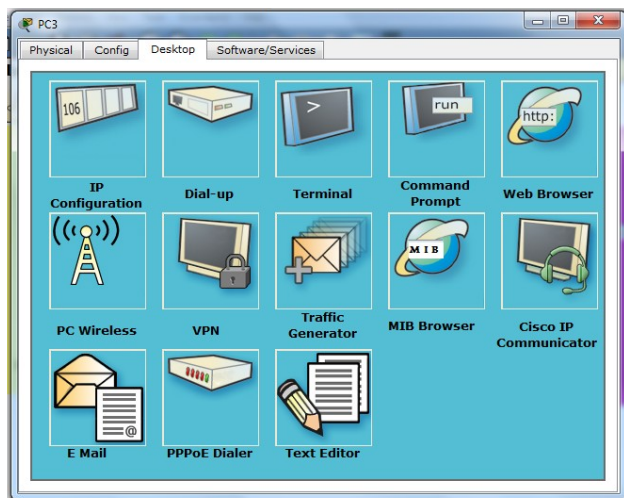
Configurazione router

Il router da programmare è il ROUTER 0, ricordiamo che vanno create le route (statiche o RIP), nei router, suggeriamo, prima di creare l'ACL, di verificare che le route siano corrette tramite il comando ping dai vari host.

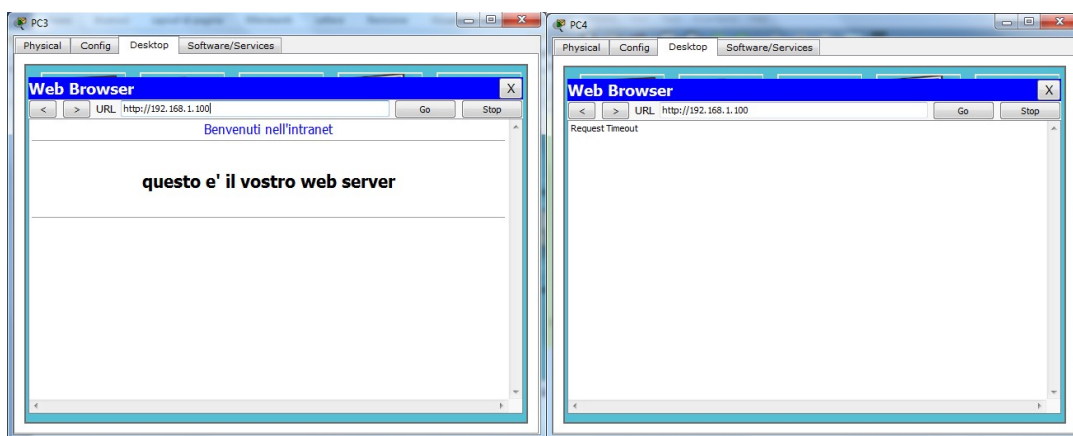
Router>en	
Router#conf t	
Router(config)#access-list 110 permit tcp host 192.168.3.1 host 192.168.1.100 eq 80	crea l'access list estesa (100-199) permettendo il traffico dall'host 192.168.3.1 verso l'host della LAN1 192.168.1.100 (WEB-SERVER) alla porta 80
Router(config)#access-list 110 deny ip any any	Blocca tutto l'altro traffico
Router(config)#int f0/0	Configura la porta del router
Router(config-if)#ip access-group 110 out	Assegnazione ACL-E alla porta
Router(config-if)#^Z	Esce dalla configurazione (CTRL +Z)

Verifica funzionalità

Per verificare la funzionalità aprire la scheda desktop dell'host PC3, selezionare WebBrowser, inserire nella barra URL dell'indirizzo, IP del Web-Server (192.168.1.100), provare anche con il PC 4.



RisultatoPC3



Risultato PC4

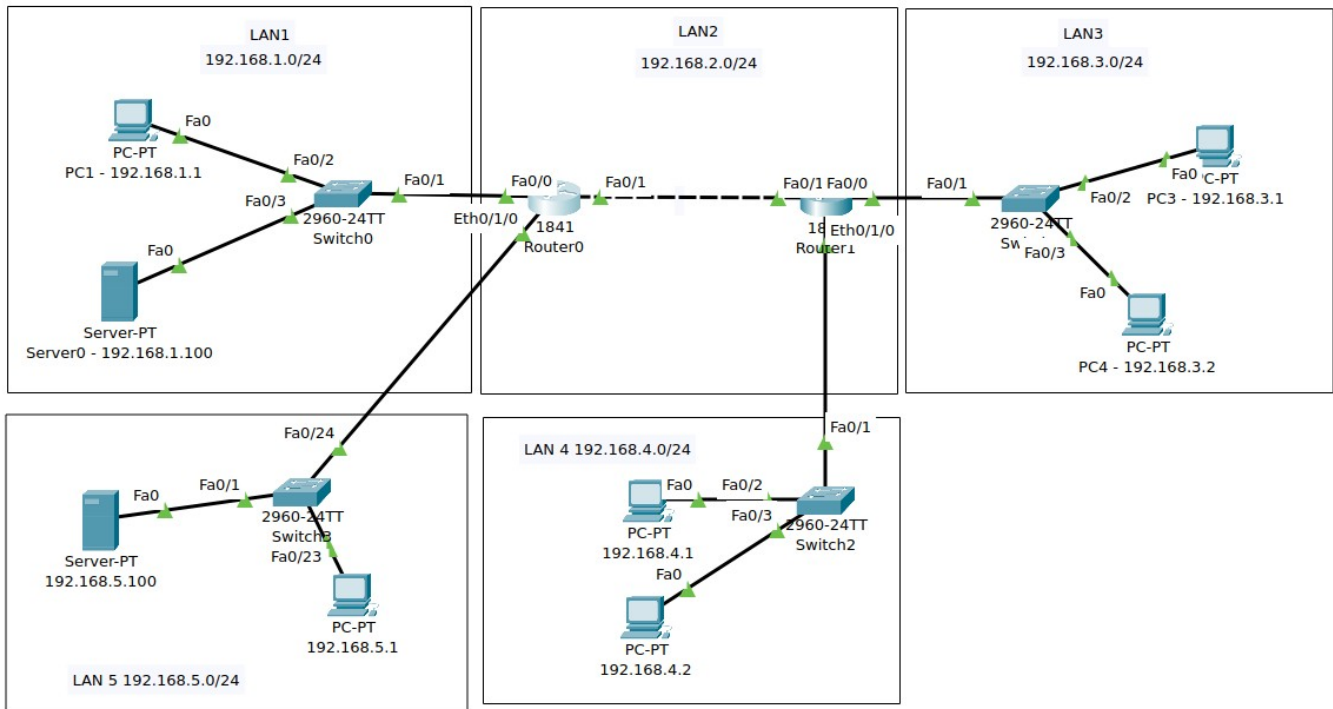
Esercitazione 3:

Modificare la rete dell'esercitazione 2, aggiungendo le due nuove reti LAN 4 e LAN 5 con le dovute rotte.

Inoltre, creare una ACL numerica in modalità out sull'interfaccia verso la LAN 5 del Router 0 che permetta:

- il passaggio di tutto il traffico IP dalla LAN 4 alla LAN 5.
- il passaggio del solo traffico FTP dalla LAN 3 al Server 192.168.5.100

Creare infine una ACL con nome in modalità IN sull'interfaccia che collega il Router 1 alla LAN 4 che permetta il solo passaggio del traffico ICMP dall'host 192.168.4.1 all'host 192.168.3.1.



Soluzione

Sul Router 0:

```
Router(config)#access-list 120 permit ip 192.168.4.0 0.0.0.255 any
```

```
Router(config)#access-list 120 permit tcp 192.168.3.0 0.0.0.255 host 192.168.5.100 eq 21
```

```
Router(config)#interface ethernet 0/1/0
```

```
Router(config-if)#ip access-group 120 out
```

Sul Router 1:

```
Router(config)#ip access-list extended pingOK
```

```
Router(config-ext-nacl)#permit icmp host 192.168.4.1 host 192.168.3.1
```

```
Router(config)#interface ethernet 0/1/0
```

```
Router(config-if)#ip access-group pingOK in
```