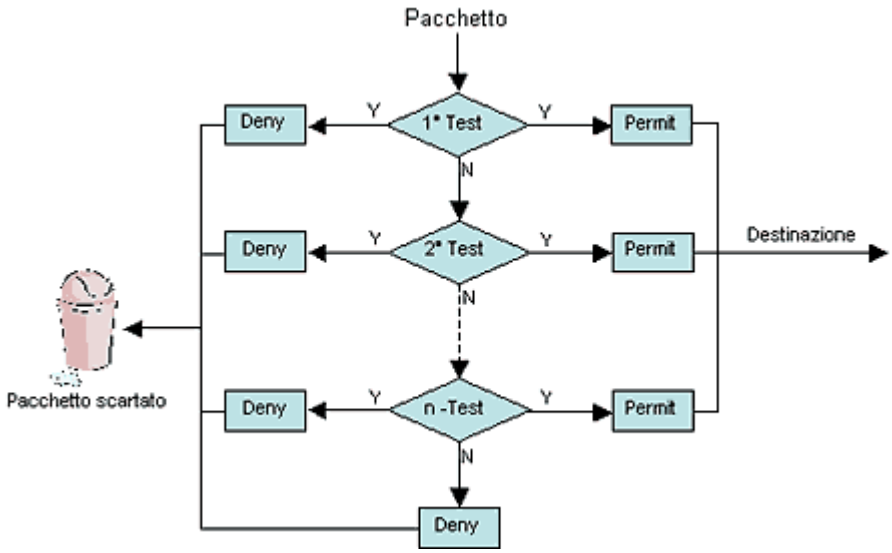
Le ACL (Access Control List) sono un elenco di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita.
Esistono varie ragioni per decidere di adoperare le ACL:

- fornire un livello base di sicurezza: si può per esempio restringere gli accessi a 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;
- decidere quale tipo di traffico può essere trasmesso: si può permettere l'invio di e-mail e impedire allo stesso tempo il Telnet.

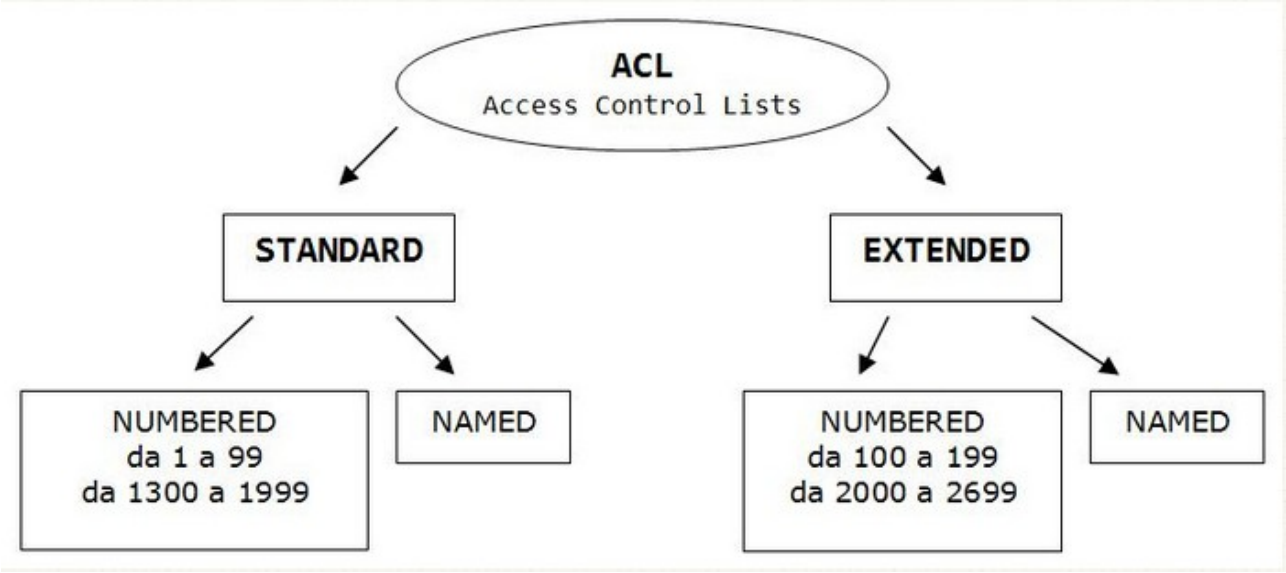
Le ACL vengono elaborate dal router in maniera sequenziale in base all'ordine in cui sono state inserite le varie clausole. Appena un pacchetto soddisfa una delle condizioni, la valutazione si interrompe e il resto delle ACL non viene preso in considerazione. Il pacchetto viene quindi inoltrato o eliminato secondo l'istruzione eseguita. Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (si considera cha alla fine di una ACL non vuota ci sia l'istruzione *deny any* ovvero nega tutto). L'ordine con cui si scrivono le ACL è importante, infatti essendo eseguite in sequenza è necessario inserire le condizioni più restrittive all'inizio. Sui router Cisco ogni ACL è identificata da un numero univoco che ne definisce il tipo: da 1 a 99 si riferiscono al protocollo IP, da 100 a 199 sono quelle estese, sempre riferite a IP.



Se una access-list è vuota, il router sottintende *permit any*. Inoltre una Wildcard Mask omessa si suppone essere 0.0.0.0 (host).

Le regole da ricordare per le ACL

- Evitare l'uso di ACL quando non necessario (appesantiscono i router).
- Porre le ACL standard in prossimità della destinazione dei pacchetti.
- Porre le ACL estese in prossimità della sorgente dei pacchetti.
- Verificare sempre il funzionamento di una ACL dopo averla attivata.




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

Il significato dei parametri presenti nel comando è descritto nella **tabella 1**.

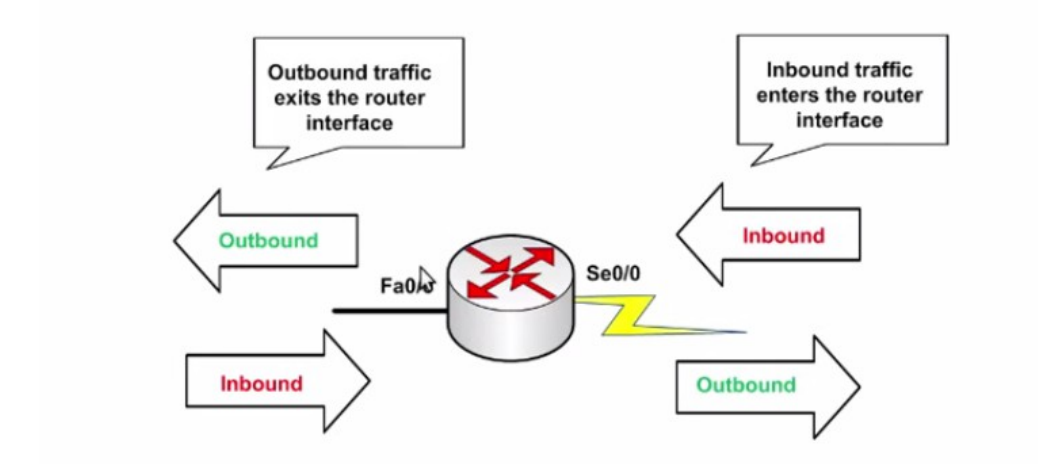
tabella 1 Parametri del comando di definizione di una ACL sui router Cisco

Parametri	Descrizione
Access-list-number	Numero della ACL. Ne indica il nome e il tipo (per 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	Indirizzo sorgente del pacchetto.
Souce wildcard	(Optional) La wildcard mask che deve essere applicata all'indirizzo sorgente.
Log	(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.

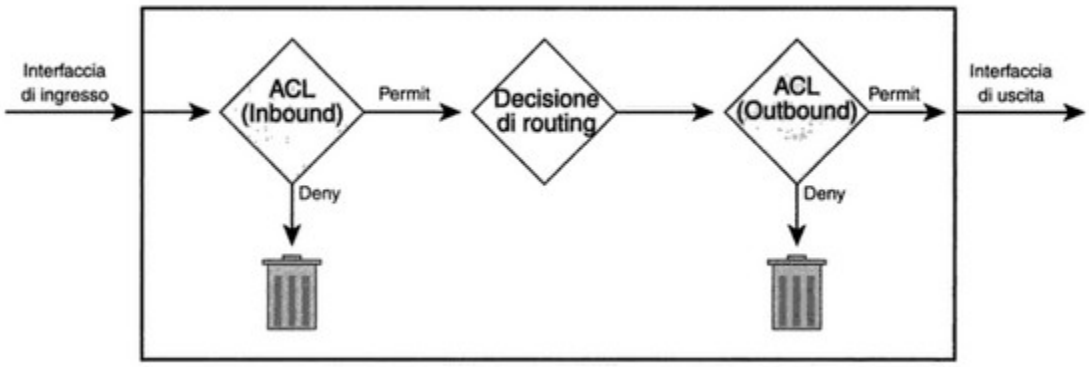
Una volta definite le condizioni si deve applicare la ACL all'interfaccia desiderata, il comando da usare è:

```
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 routine, mentre in output prima il routine e poi la ACL. Se non è specificato, per default è out.



Posizioni relative alle inbound ACL e alle outbound ACL.



Per eliminare una ACL bisogna utilizzare il comando:

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

Per avere l'intera lista delle **ACL** presenti sulla nostra macchina, basta digitare:

Router# sh access-list

mentre se volessimo listare le regole che costituiscono una determinata ACL, occorre lanciare il comando:

Router# sh `access-list access-list number`

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.

Sequenza di passi da seguire per la creazione delle ACL standard

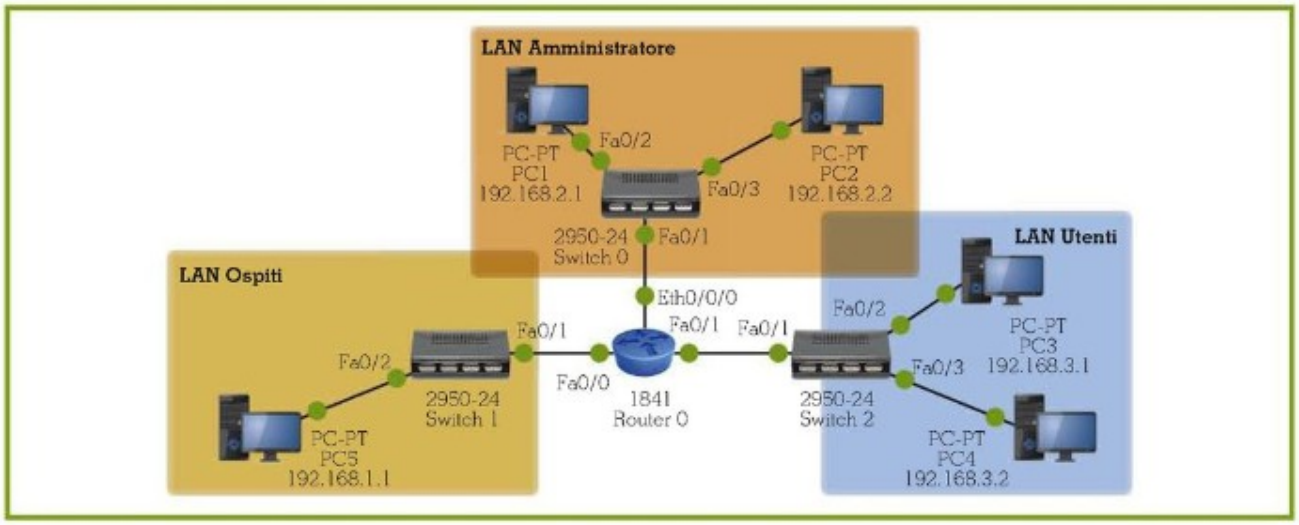
1. Entrare nel CLI (Command Line Interface) del router.
2. Entrare in modalità configurazione (configure terminal).
3. Assegnare un nome all'access list (standard 1-99).
4. Indicare se permette o nega (permit-deny).
5. Inserire IP dell'host o della rete.
6. Ripetere i passaggi 4-5 per inserire altre regole.
7. Assegnare la regola creata all'interfaccia (interface *nomeInterfaccia*).
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, si utilizza la wildcard)*
R1(config)#access-list 1 permit any *(permette a tutti gli altri ip di essere inoltrati)*
R1(config)#interface fastEthernet 0/1 *(aperture interfaccia)*
R1(config-if)#ip access-group 1 out *(assegnazione regole dell'access-list 1 all'interfaccia in modalità output)*

Testo Creare una ACL standard che blocchi i pacchetti transitanti dal router dalla LAN Ospiti alla LAN Utenti, permettendo alla LAN Amministrazione di poter inviare e ricevere i pacchetti con tutte le LAN presenti.

SCHEMA LOGICO



SCHEMA INDIRIZZAMENTI IP

Nome LAN	IP	Subnet-mask	Nome host	Gateway
LAN Amministrazione	192.168.2.1	255.255.255.0	PC1	192.168.2.128
LAN Amministrazione	192.168.2.2	255.255.255.0	PC2	192.168.2.128
LAN Ospiti	192.168.1.1	255.255.255.0	PC5	192.168.1.128
LAN Utenti	192.168.3.1	255.255.255.0	PC3	192.168.3.128
LAN Utenti	192.168.3.2	255.255.255.0	PC4	192.168.3.128

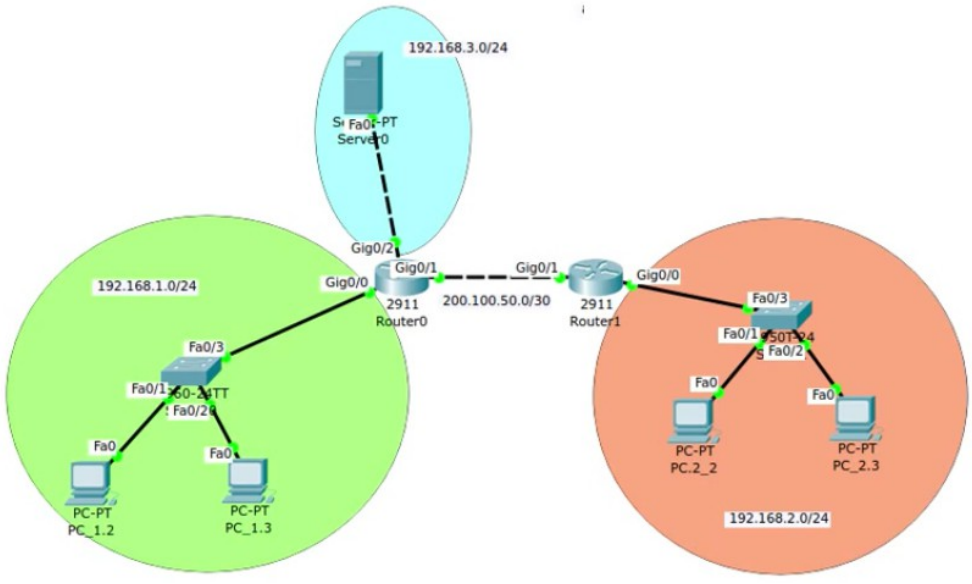
Router(config)#access-list 1 permit 192.168.2.0 0.0.0.255	Permette a tutti gli host della rete amministrazione di inviare e ricevere i pacchetti
Router(config)#access-list 1 deny any	Blocca tutti i pacchetti delle altre reti LAN
Router(config)#int f0/1	Apertura interfaccia fast-ethernet
Router(config-if)#ip access-group 1 out	Assegnazione all'interfaccia della regola ACLS 1 in output
Router(config-if)#exit	Uscita configurazione interfaccia
Router(config)#int f0/0	Apertura intercaccia fast-ethernet 0/0
Router(config-if)#ip access-group 1 out	Assegnazione regola ACLS 1 all'interfaccia in output
Router(config-if)# ^Z	Uscita modalità configurazione
Router#	

Verifica funzionalità

Effettuare dei ping di certifica 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)

PC_2.3 NON deve accedere alla rete VERDE



Extended ACL (1/4)

Le ACL Extended sono molto spesso usate più delle standard perché offrono un controllo decisamente maggiore

Le ACL Extended controllano gli **indirizzi di sorgente e destinazione** dei pacchetti, i **protocolli** e **le porte**

- Esempio: una ACL extended può permettere traffico e-mail verso una destinazione specifica e negare il file transfer e il web browsing verso la stessa destinazione

La sintassi delle extended ACL è simile a quella delle standard: "*access-list*"

Il comando "*ip access-group*" associa una extended ACL ad una interfaccia

Extended ACL (2/4)

La sintassi delle extended ACL è tale per cui gli statement possono essere molto lunghe

- si possono abbreviare con l'uso delle opzioni di host o any

Alla fine delle ACL extended si può aggiungere, per guadagnare maggiore precisione, il campo che specifica il port number (è opzionale) del TCP o dell'UDP

Si possono anche specificare operazioni logiche, come uguale (eq), non uguale (neq), più grande di (gt) e minore di (lt).

Gli identificatori delle extended ACL vanno da 100 a 199

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

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 *access-list number* 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.
Operator *operand*	Un operatore logico: lt, gt, eq, neq, range (less than, greater than, equal, not equal, range) e il numero o il nome della porta TCP o UDP (vedi Tabella n.1). Nel caso dell'operatore *range* occorre inserire due valori *operand* (es. range 21 25)
Established	(Optional) Si utilizza solo con il protocollo TCP: indica una "estabilished 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.

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

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

º 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 sorce-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* .

Alcuni esempi di icmp message:

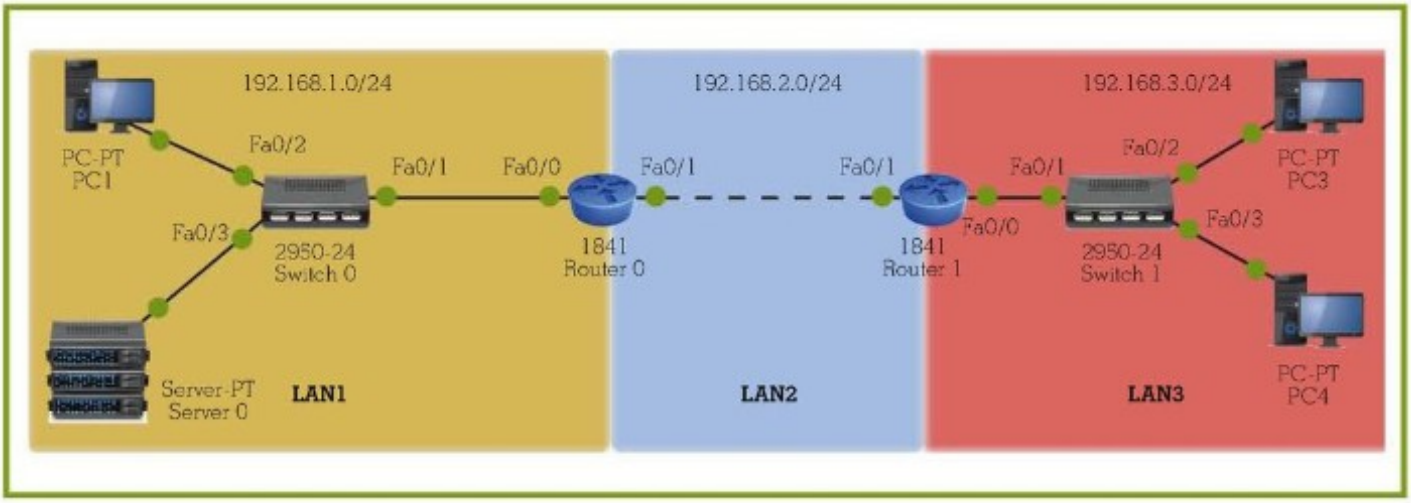
echo	echo-reply	administratively-prohibited
time-exceeded	ttl-exceeded	unreachable
traceroute	packet-too-big	network-unknown
port-unreachable	unreachable	host-unknown
host-unreachable	net-unknown	net-unreachable

Valore Decimale	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
70		Gopher	TCP/IP
80		WWW	TCP

Testo Realizzare una ACL estesa per bloccare l'accesso al web server installato nella LAN1 da parte della LAN3, tranne che per host 192.168.3.1, inoltre si dovranno bloccare tutti gli altri tipi di pacchetto.

Esecuzione

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

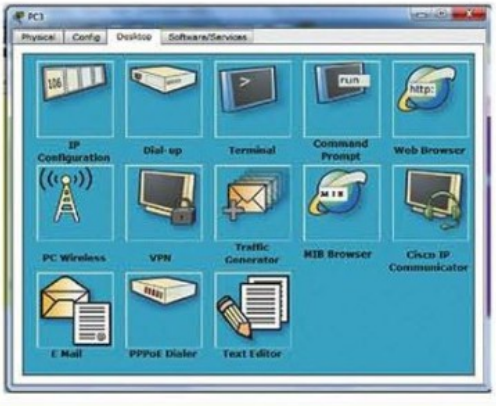
Il router da programmare è il ROUTER 0; ricordiamo che vanno create le route (statiche o RIP) nei router, suggeriamo, prima di creare l'ACL, di verificare che le route siano corrette tramite il comando ping dai vari host.

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 traffic TCP dell'host 192.168.3.1 verso 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	Configurazione porta router
Router(config-if)#ip access-group 110 out	Assegnazione ACL-E alla porta
Router(config-if)# ^Z	Uscita configurazione (CTRL +Z)

Verifica funzionalità

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

RisultatoPC3

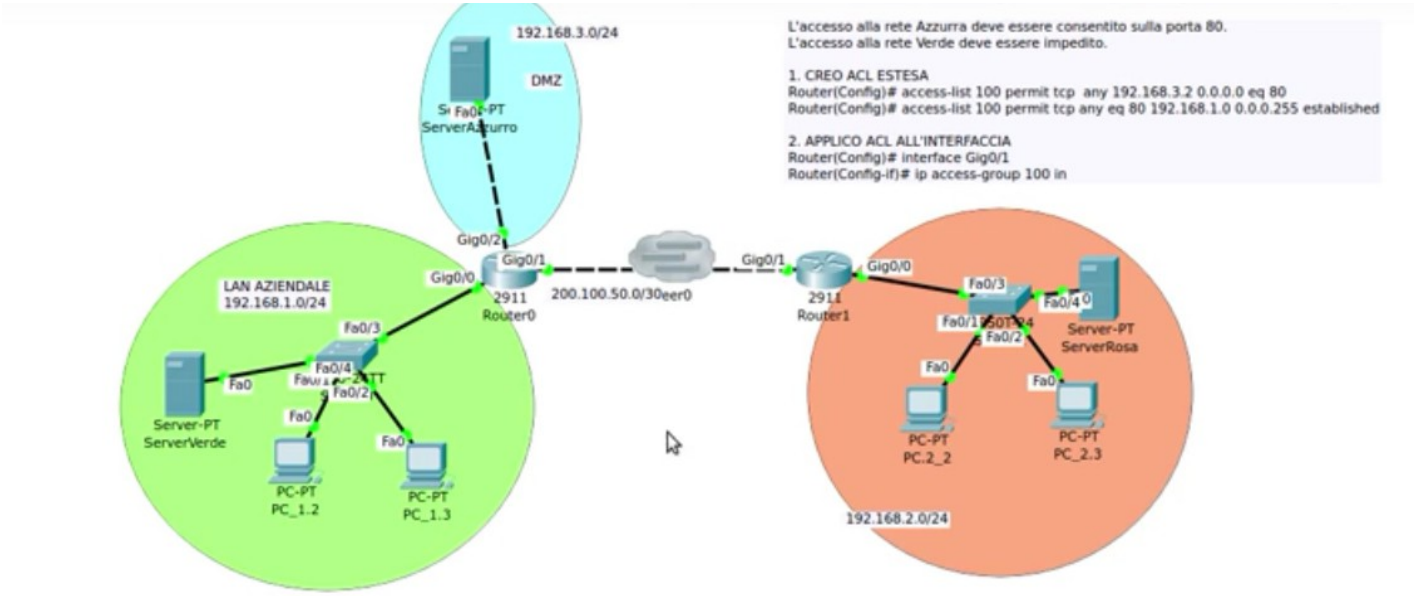


Risultato PC4

L'accesso alla rete Azzurra deve essere consentito sulla porta 80.
L'accesso alla rete Verde deve essere impedito.

1. CREO ACL ESTESA
Router(Config)# access-list 100 permit tcp any 192.168.3.2 0.0.0.0 eq 80
Router(Config)# access-list 100 permit tcp any eq 80 192.168.1.0 0.0.0.255 established

2. APPLICO ACL ALL'INTERFACCIA
Router(Config)# interface Gig0/1
Router(Config-if)# ip access-group 100 in



Configurazione di ACL standard con nome

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

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

Esempio:
ip access-list standard permit-ip
permit 172.16.2.144 0.0.0.7

Configurazione di ACL estese con nome

Di nuovo, si evidenzia che a differenza delle ACL numeriche, il comando **access-list** è preceduto dal comando **IP**.

Sintassi:
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:
ip access-list extended blocco-telnet
deny tcp 172.16.2.0 0.0.0.255 any eq telnet

Scrittura di una tipica ACL "FIREWALL"

È ricorrente la richiesta di scrivere una ACL con nome "FIREWALL" che filtri il traffico in ingresso, sulla seriale collegata all'ISP, secondo i seguenti criteri:

- permetta il traffico HTTP entrante verso il Server Web
- permetta il traffico di rientro delle sessioni TCP aperte dall'interno
- permetta il transito delle risposte ai PING lanciati dall'interno
- blocchi esplicitamente ogni altro tipo di traffico entrante:

```
R(config)#ip access-list extended FIREWALL
R(config-ext-nacl)#permit tcp any host Web-Server-IP eq www
R(config-ext-nacl)#permit tcp any any established
R(config-ext-nacl)#permit icmp any any echo-reply
R(config-ext-nacl)#deny ip any any
R(config-ext-nacl)#interface serial0
R(config-if)#ip access-group FIREWALL in
R(config-if)#exit
```