Esercitazioni di Laboratorio 4

LE ACCESS CONTROL LIST CON PACKET TRACER

Una lista di controllo degli accessi, spesso chiamata col nome inglese di Access Control List (ACL), è un meccanismo usato per esprimere regole complesse che determinano l'accesso ad alcune risorse di un sistema informatico.

Tra le sue applicazioni principali si ha la configurazione di firewall e router e dei diritti di accesso a file e directory da parte del sistema operativo sui propri utenti.

Le ACL vengono realizzate per:
- limitare il traffico in rete;
- fornire controllo del flusso di traffico (es. le ACL possono restringere la consegna degli update di routing);
- offrire un livello base di sicurezza per l'accesso alla rete;
- decidere che tipi di traffico debbano essere instradati o bloccati alle interfacce del router;
- permettere a un amministratore di controllare che un client possa accedere a una rete;
- schermare alcuni host per permettere o negare accesso a parte della rete.

Nelle ACL vengono quindi elencate in ordine le regole che indicano quali utenti o processi di sistema possono accedere a degli oggetti, e quali operazioni sono possibili su particolari oggetti.
Ciascuna regola, definita Access Control Entry (ACE), esprime una o più proprietà dell'oggetto da valutare (sempre in riferimento all'esperienza, l'indirizzo sorgente di un pacchetto IP), e se queste proprietà sono verificate indica quale decisione prendere (es. far passare il pacchetto oppure rifiutarlo).
La valutazione inizia dalla prima regola e continua fino a quando le condizioni di una regola non sono verificate. Se le condizioni sono verificate, la valutazione finisce e viene applicata la decisione presa; altrimenti, la valutazione prosegue alla regola successiva. Se nessuna regola viene soddisfatta, viene applicata una decisione di default, chiamata policy dell'ACL.

Le ACL possono essere usate per controllare il traffico ai livelli 2, 3, 4 e 7: in passato venivano usate le ACL numeriche per filtrare il traffico in base al campo Ethernet Type delle Trame oppure in base agli indirizzi MAC mentre oggi le ACL sono più spesso basate sugli indirizzi IPv4 o IPv6 e sulle Porte TCP e/o UDP.

Le ACL utilizzano un nuovo tipo di maschera, la WildCard Mask.

WildCard Mask

La WildCard Mask è un numero di 32 bit diviso in 4 ottetti. Quest'ultimo conserva la stessa divisione (8 bit per ottetto) della notazione decimale puntata degli indirizzi IPv4. Questa, solitamente, viene abbinata a un indirizzo IP, in modo simile alla SubNet Mask e i bit assumono valori 1 o 0 per stabilire come elaborare i corrispondenti bit dell'indirizzo IP. Il termine stesso indica il procedimento di checking su una qualsiasi Access List, tramite una maschera.

L'analogia nasce dal Jolly (WildCard), usato nel gioco del poker, che permette l'abbinamento, a tale carta, di una qualsiasi altra pari, presente nel mazzo.

Più precisamente, gli 0 e 1 nella WildCard Mask stabiliscono se i bit, corrispondenti nell'indirizzo IP, devono essere controllati o ignorati. Ogni bit a 0, della WildCard Mask, indica che il bit corrisposto dev'essere incluso nel processo di controllo dell'uguaglianza, mentre il valore 1 tralascia ogni vincolo di confronto.

ESEMPIO

Vediamo un esempio per comprendere l'utilizzo della WildCard mask: si supponga di voler effettuare un controllo dell'indirizzo IP: 169.12.5.0/24, che appartiene a una B 169.12.0.0 dove possono essere create 255 reti che contengono 253 host ognuna.

Si desidera bloccare il traffico in arrivo dai seguenti indirizzi IP: da 169.12.5.4 a 170.12.5.7.

169.12.5.0, in binario, è tradotto in 10101010.00001100.00000101.00000000 e la subnet mask è 11 111111.11111111.11111111.00000000 (un /24, come già visto, è un 255.255.255.0).

Guardando gli indirizzi da bloccare in formato binario si osserva che c'è una parte di indirizzo che non cambia:

```
169.12.5.4 - 10101010.00001100.00000101.000001 00
169.12.5.5 - 10101010.00001100.00000101.000001 01
169.12.5.6 - 10101010.00001100.00000101.000001 10
169.12.5.7 - 10101010.00001100.00000101.000001 11
```

Tramite la WildCard Mask, è possibile raggruppare gli indirizzi IP interessati in un'unica dicitura e, come per il CIDR, ridurre il numero di ACL da impostare per bloccare il traffico.
In questo caso è possibile impostare una sola ACL per fermare i dati in arrivo dal range che va dal 169.12.5.4 al 169.12.5.7: è sufficiente individuare l'indirizzo di inizio sequenza che corrisponde all'insieme dei bit non mutevoli:

```
Dot Notation   parte dell'indirizzo non mutevole   parte mutevole
-------------------------------------------------------------
169.12.5.4 10101010.00001100.00000101.000001 + 00
169.12.5.5 10101010.00001100.00000101.000001 + 01
169.12.5.6 10101010.00001100.00000101.000001 + 10
169.12.5.7 10101010.00001100.00000101.000001 + 11
```

In tutti e quattro gli indirizzi la parte che non cambia è 170.12.5.4 e sarà l'inizio sequenza che ci permette di individuare la WildCard Mask esatta, composta dal valore 1 nella posizione dei bit che mutano, cioè solo gli ultimi 2:
la WildCard Mask, in forma binaria, sarà 00000000.00000000.00000000.00000011.
In forma decimale puntata 0.0.0.3.

Scrivere le ACL

Prima di scrivere le ACL è necessario aggiungere il comando che indica se il gruppo di dispositivi/servizi relativo all'ACL è da riferirsi alle richieste in entrata (in e inbound) oppure in uscita (out e outbound).

Definire In, Out, Inbound, Outbound

Vediamo le differenze tra le diverse situazioni:

- out: si riferisce al traffico che ha attraversato il router e lascia l'interfaccia;
- in: è il traffico che arriva sulla interfaccia e poi passa attraverso il router;
- inbound: se la lista di accesso è in entrata, quando il router riceve un pacchetto, il software Cisco IOS controlla i criteri della ACL e se al pacchetto è consentito l'accesso continua a elaborarlo altrimenti lo scarta;
- outbound: se la lista di accesso è in uscita, quando il software riceve l'indirizzo dell'interfaccia d'uscita, controlla i criteri della ACL e se è consentito a quel pacchetto di raggiungere l'interfaccia, lo trasmette, altrimenti lo scarta.

◀ The out ACL has a source on a segment of any interface other than the interface to which it is applied and a destination off of the interface to which it is applied.
The in ACL has a source on a segment of the interface to which it is applied and a destination off of any other interface. ▶

Quindi per applicare le ACL alle interfacce e alle linee VTY, in ingresso o in uscita dal router, si utilizzano i seguenti comandi:

```
R(config-if)#ip access-group numero {in | out}      // per le interfacce
R(config-line)#access-class numero {in | out}       // per le linee VTY
```

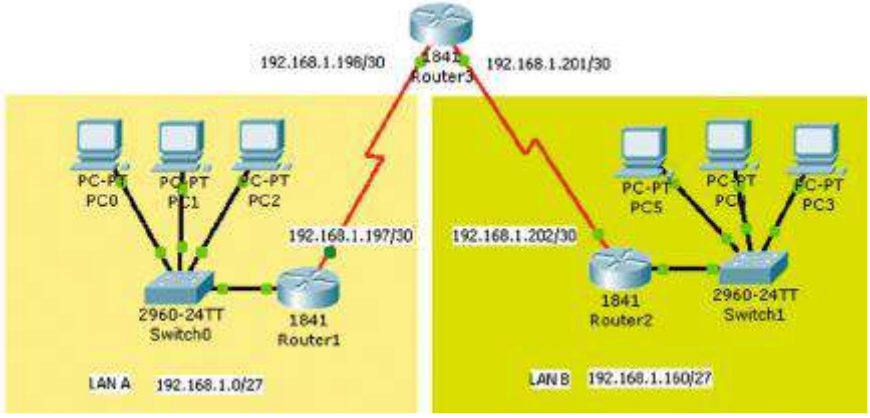
ACL Standard

Le ACL Standard numeriche per IPv4 e IPv6 hanno numero da 1 a 99 e da 1300 a 1999; esse controllano solo l'IP sorgente dei Pacchetti, e non possono indicare alcun protocollo L4-L7:

```
R(config)#access-list numero {permit | deny} IP-sorgente [wildcard mask]
```

ESEMPIO

Consideriamo la rete di figura, è richiesto di scrivere la ACL affinché i PC della LAN A non possano accedere alla LAN B.



I comandi sono i seguenti:

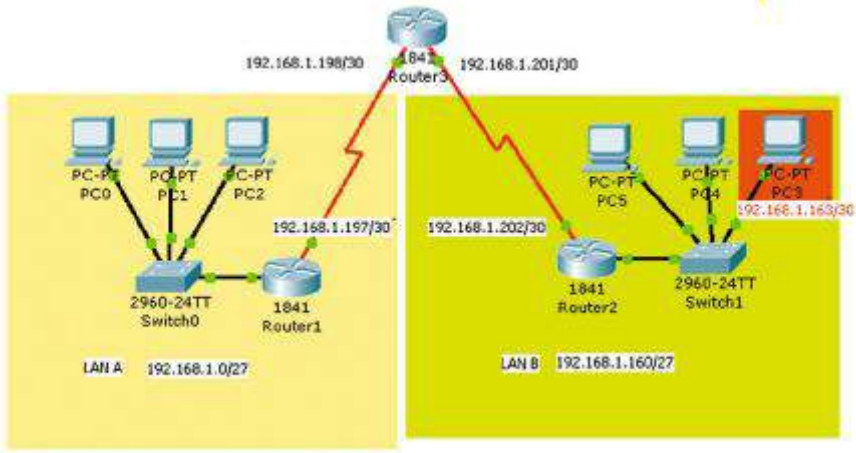
```
Router2(config)#access-list 10 deny 192.168.1.0 0.0.0.31 //wildcard 0.0.0.00011111
Router2(config)#access-list 10 permit any
```

(Il file con memorizzata la rete è *1.St ACL con network deny.pkt*).

Prova adesso!

Realizza la rete mostrata in figura a pagina precedente e verifica il funzionamento prima dell'inserimento della ACL. Quindi inserisci nel router2 la ACL sia manualmente attraverso l'interfaccia CLI che modificando il file di configurazione Running Config aggiungendo le righe come sotto indicato:

Se invece volessimo vietare l'accesso di un solo computer, per esempio il PC3 di indirizzo IP 192.168.1.163 indicato nella figura:



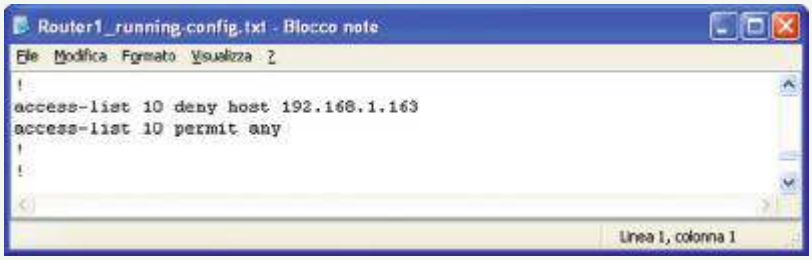
i comandi sono i seguenti:

```
Router1(config)#access-list 10 deny host 192.168.1.163
Router1(config)#access-list 10 permit any
```

(Il file con memorizzata la rete è *2.St ACL con PC deny.pkt*).

Prova adesso!

Realizza la rete mostrata in figura a pagina 207 e verifica il funzionamento prima dell'inserimento della ACL. Quindi inserisci nel router1 la ACL sia manualmente attraverso l'interfaccia CLI che modificando il file di configurazione Running Config aggiungendo le righe come sotto indicato:



Quindi modifica le ACL dei due router in modo che i router con indirizzo pari possano raggiungere tutti gli altri host mentre quelli di indirizzo dispari possano raggiungere solo gli host della propria sottorete.

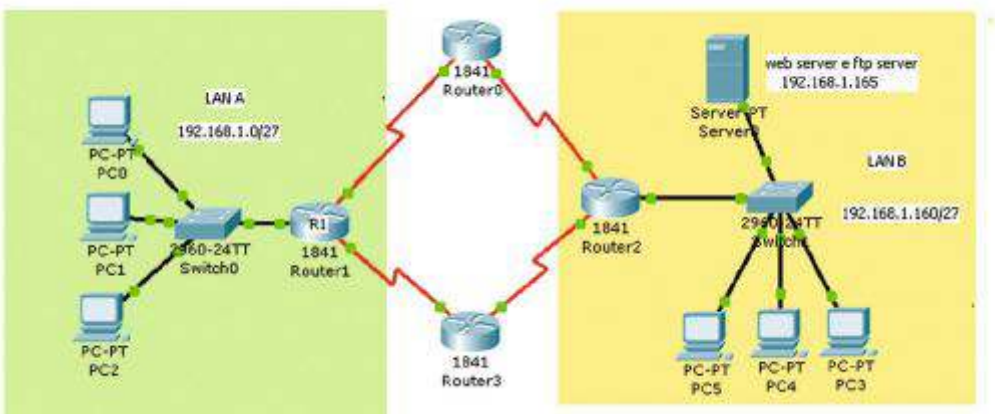
ACL Estese

Le ACL Estese numeriche per IPv4 e IPv6 hanno numero da 100 a 199 e da 2000 a 2699; esse controllano i Pacchetti in base sia all'IP sorgente sia alla destinazione, e possono anche indicare un protocollo L4 (TCP o UDP) e L7 (Porte Well-known).
La sintassi (semplificata) del comando è:

```
R(config)#access-list numero {permit | deny} protocollo
IP-sorgente wildcard mask [operator Port [Port]]
IP-destinaz wildcard mask [operator Port [Port]] [established]
```

ESEMPIO

Nella rete seguente si vuole inibire alla LAN A di utilizzare il Web server e il servizio FTP offerto sempre dallo stesso server 192.168.1.165.



I comandi per la configurazione del router 1 sono i seguenti:

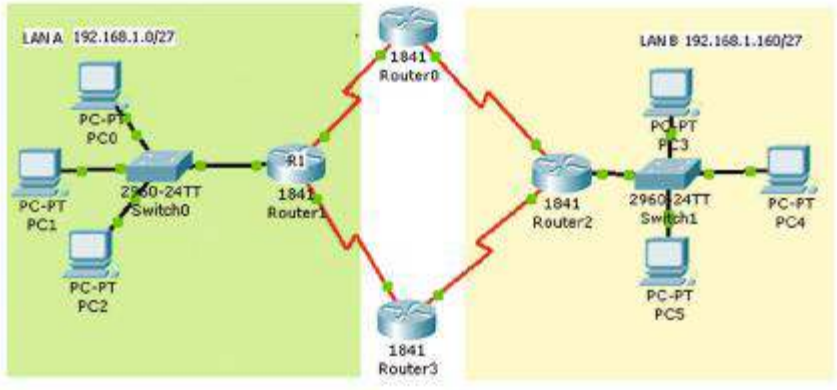
Ricordiamo di aggiungere il comando per la configurazione della interfaccia:

```
R1(config-if)#ip access-group 100 in
```

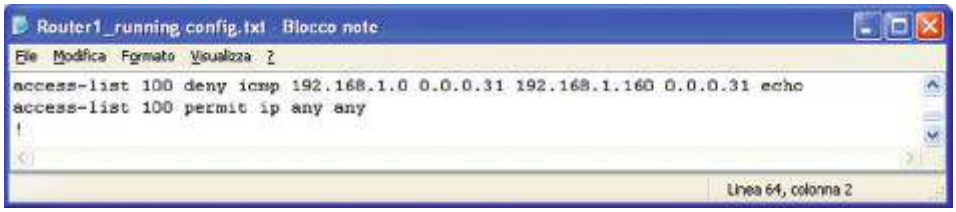
(Il file con memorizzata la rete è *3.Ext ACL con limitazione servizi.pkt*).

ESEMPIO

Vediamo un secondo esempio dove la LAN A non può accedere a LAN B ma LAN B può accedere a LAN A utilizzando ICMP.



I comandi per la configurazione del router 1 sono i seguenti:



ricordiamo di aggiungere il comando per la configurazione della interfaccia:

```
R1(config-if)#ip access-group 100 in
```

(Il file con memorizzata la rete è *3.Ext ACL con limitazione servizi.pkt*).

Concludiamo con due osservazioni.

1. Le ACL, sia standard sia estese, hanno un deny finale implicito; se devono consentire il traffico diverso da quello specificato, inserire un permit finale esplicito.
2. Le ACL possono anche avere un nome invece di un numero; vengono create col comando:

```
R(config)#ip access-list {standard | extended} nome-ACL
```

Le "entry" di una ACL con nome possono essere cancellate, aggiunte anche in posizione intermedia o modificate singolarmente, a differenza delle ACL numeriche che si possono solo riscrivere tutte.

Zoom su...

ROUTER E ACL

Descriviamo la sequenza delle operazioni che vengono eseguite da un router nell'analisi di un pacchetto:

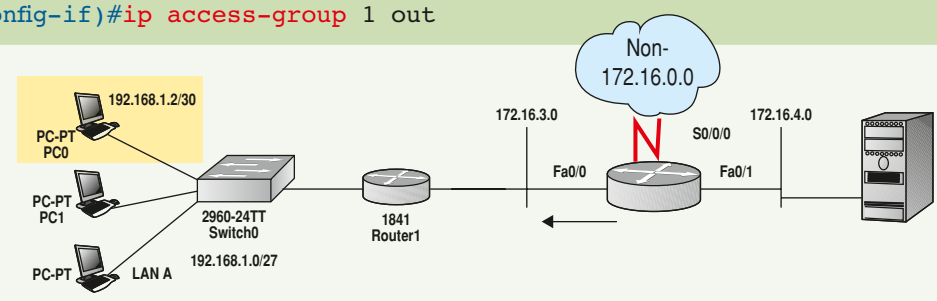
1. non appena una PDU di strato 2 entra in un'interfaccia, il router verifica l'indirizzo di strato 2 se corrisponde al suo indirizzo o è un indirizzo di broadcast;
2. se il check è positivo, il router estrae allora il pacchetto ed esamina la ACL associata all'*interfaccia di ingresso*, sempre che ne sia definita una;
3. il router esegue ogni comando della ACL;
4. se si riscontra una corrispondenza sulla condizione corrispondente a un comando, il router compie l'azione collegata a quel comando;
5. se il pacchetto è accettato il router eseguirà la funzione di instradamento;
6. se è definita una ACL sull'*interfaccia di uscita*, il pacchetto sarà di nuovo testato in base ai comandi contenuti in questa ACL;
7. se tutti i test autorizzano il pacchetto a proseguire il suo cammino, questo viene incapsulato nel protocollo di strato 2 definito sull'interfaccia d'uscita.

Prova adesso!

Nella rete seguente.

1. Configura il router in modo tale che la subnet 172.16.4.0 non debba accedere solo alla subnet 172.16.3.0 utilizzando una ACL1 per l'interfaccia di uscita:

```
R1(config)#access-list 1 deny 172.16.4.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)#interface fa0/0
R1(config-if)#ip access-group 1 out
```



2 Vieta il traffico FTP tra le due subnet utilizzando una ACL2 estesa:

```
R1(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
;21 = Porta comandi dell'FTP
R1(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
R1(config)#access-list 101 permit ip any any
R1(config)#interface fa0/1
R1(config-if)#ip access-group 101 in   ;evita traffico nel Router
```

3 Progetta ora due nuove ACL affinché vengano rispettati i seguenti vincoli:

ACL3: restringe l'accesso alle linee VTY in modo che non venga inoltrato il traffico proveniente da tutti gli indirizzi del tipo 192.168.Z.90 (per ogni Z≠X);

ACL4: restringe l'accesso alle interfacce d'ingresso del router in modo che venga inoltrato il traffico diretto verso l'host PC0 e il traffico ICMP diretto verso le interfacce del router.

4 Verifica la correttezza dell'ACL definita con il comando RouterX# show access-list e mediante i comandi PING e TRACEROUTE.

5 Salva il file di configurazione attuale in quello di startup.

```
RouterX# copy run start.
```