ACL

Definizione ACL standard

Le ACL standard, nel range [1,99], consentono di filtrare il traffico dati, quindi di permetterne o bloccarne il transito, valutando l'indirizzo IP sorgente (un host o un gruppo di host).

Osserviamo un esempio pratico:

```
R2(config)#access-list 10 permit host 192.168.2.1
```

Gli elementi coinvolti nel comando sono i seguenti:

- **10**: identificativo numerico univoco, nel range [1,99];
- **permit**: comportamento associato alla regola;
- **host 192.168.2.1**: indirizzo IP sorgente.

Implicitamente, Cisco IOS definisce e mette in coda anche la seguente regola:

```
R2(config)#access-list 10 deny any
```

Cosa significa? Significa che tutto il traffico dati il cui indirizzo IP non corrisponde all'indirizzo IP definito nella regola precedente, verrà bloccato.

Dunque l'ACL definitiva avrà la seguente configurazione:

```
access-list 10 permit host 192.168.2.1
access-list 10 deny any
```

Definizione ACL estese

Le ACL estese offrono una maggiore granularità nel filtraggio del traffico dati. Non si limitano ad ispezionare il solo indirizzo IP sorgente, bensì un'ampia suite di attributi (sia dello strato protocollare di rete che di trasporto).

Ad esempio, la seguente regola consente di far transitare il solo traffico dati di tipo TCP proveniente da 1.1.1.1 e diretto alla porta 80 di 2.2.2.1:

```
R2(config)#access-list 110 permit tcp host 1.1.1.1 host 2.2.2.1 eq www
```

Come per le ACL standard, implicitamente Cisco IOS definisce e mette in coda anche la seguente regola:

```
R2(config)#access-list 110 deny ip any any
```

Per maggior chiarezza, consiglio comunque di esplicitarla.

Dunque l'ACL definitiva avrà la seguente configurazione:

```
access-list 110 permit tcp host 1.1.1.1 host 2.2.2.1 eq www
access-list 110 deny ip any any
```

Applicazione

Il seguente comando attiva una ACL, ovvero associa l'ACL ad una specifica interfaccia:

```
ip access-group acl-number in [out]
```

Ad esempio, supponiamo di voler associare l'ACL numero 10 all'interfaccia GigabitEthernet0/1, affinché sia filtrato il traffico dati **in ingresso**:

```
R(config)#interface GigabitEthernet0/0
R(config-if)#ip access-group 10 in
```

Il comportamento complessivo associato all'interfaccia, ovvero la sua policy di filtraggio, sarà il seguente:

permetti il traffico in transito dall'interfaccia GigabitEthernet0/0 e, in particolare, i pacchetti in ingresso il cui indirizzo IP sorgente è 192.168.2.1; nega tutto il resto.

Per eliminare l'associazione:

```
R(config)#interface GigabitEthernet0/0
R(config-if)#no ip access-group 10 in
```

Visualizzazione

Per visualizzare i dettagli di una specifica ACL (e il numero eventuale di pacchetti bloccati o permessi):

```
R#show access-lists 110
```

Per visualizzare i dettagli di tutte le ACL presenti:

```
R#show access-lists
```