Switch D-Link

Configurare le Access Control List (Switch Smart e Managed)

Che cos'è un ACL

Le ACL (Access Control List) sono una delle funzioni più comunemente utilizzate nella sicurezza della rete e mirano al filtraggio del traffico.

Una ACL è costituita da un insieme di istruzioni che consentiranno o negheranno un particolare tipo di traffico. Per prendere tale decisione, il pacchetto verrà confrontato con ogni regola configurata (permit / deny) in modo sequenziale fino a quando non corrisponde a una di esse. Ecco perché l'ordine in cui vengono stabilite le regole è fondamentale per ottenere l'operazione desiderata.

Questa interessante funzione è inclusa in tutta la nostra gamma di switch Smart (dalla famiglia DGS-1210, solo via WEB, mentre dalla famiglia DGS-1250 anche via CLI) e, naturalmente, in tutta la serie Managed.

Tipi di access-list

A seconda delle esigenze saremo in grado di configurare il tipo di ACL più adatto al nostro scenario. Possiamo scegliere tra questi quattro gruppi:

- ✓ **Standard**
  Si possono filtrate indirizzi IP di origine o di destinazione (*) (o entrambi)
- ✓ **Extended**
  È possibile aggiungere il tipo e il numero di porta
- ✓ **Extended MAC**
- ✓ Il filtro viene eseguito in base agli indirizzi MAC specificati
- ✓ **Extended Expert**
- ✓ Combina e include tutte le opzioni di cui sopra

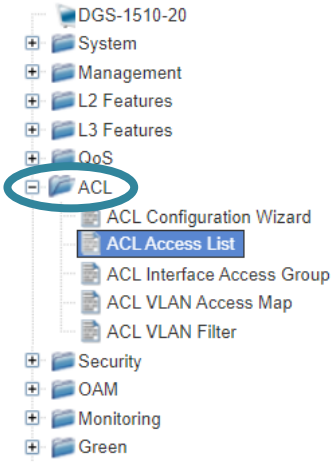
  Quest'ultimo gruppo è presente dalla serie **DGS-1510** in poi

(*) Possono essere configurati sia per **IPv4 che per IPv6 poiché gli** switch **D-Link** sono pronti per l'uso di entrambe le tecnologie

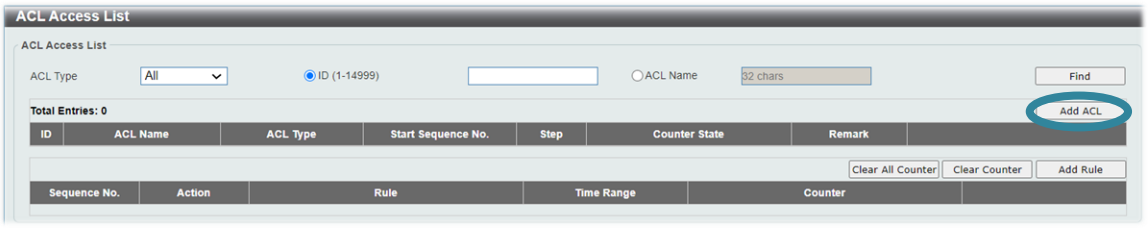
Come viene implementata una ACL dall'interfaccia utente WEB?

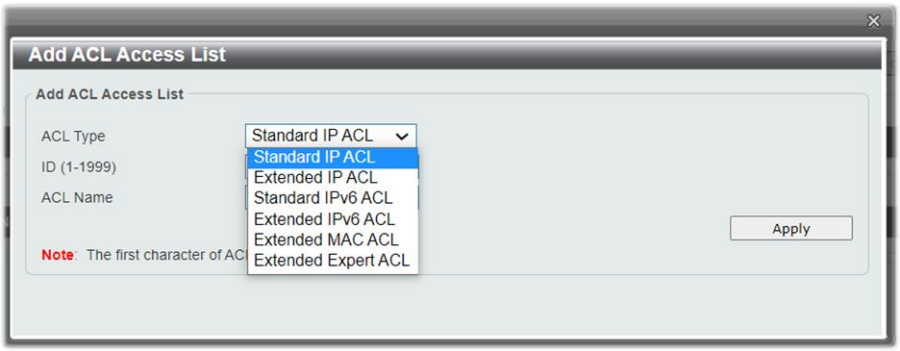
Per creare e configurare un ACL è possibile utilizzare la procedura guidata che ci renderà più facile crearla e attivarla.
In questo esempio blocchiamo l'accesso ad un indirizzo IP (192.168.0.2) tramite una ACL standard da una porta dello switch.

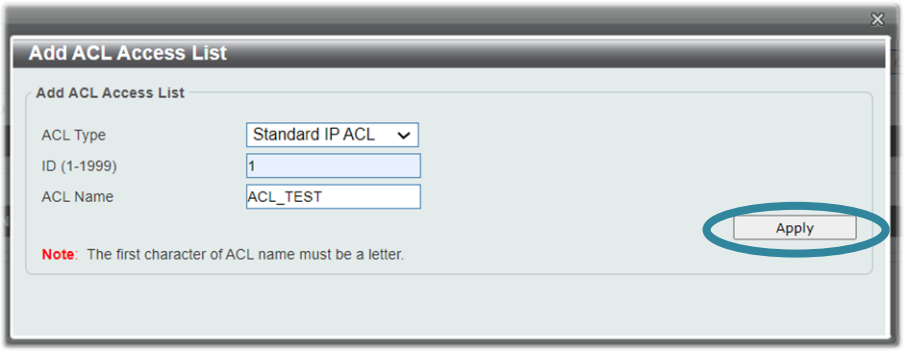
All'interno del menu ACL, accediamo al sottomenu **ACL Access List**



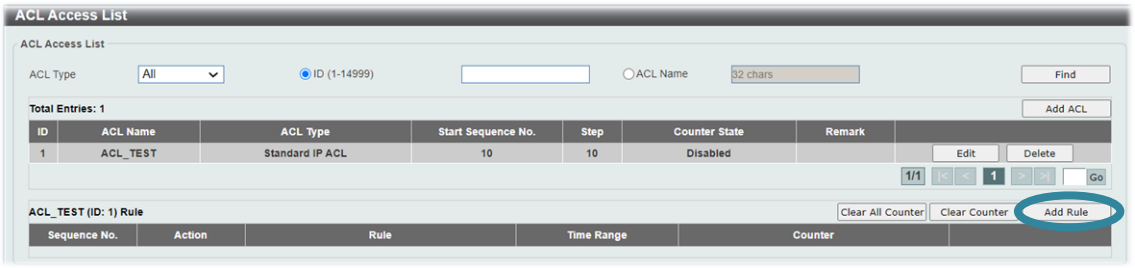
Creiamo la nuova **ACL** tramite l'opzione **Add ACL,** dove ci viene chiesto anche il tipo di ACL da creare. In questo caso selezioniamo **Standard IP ACL** e poi clicchiamo sul tasto **APPLY**



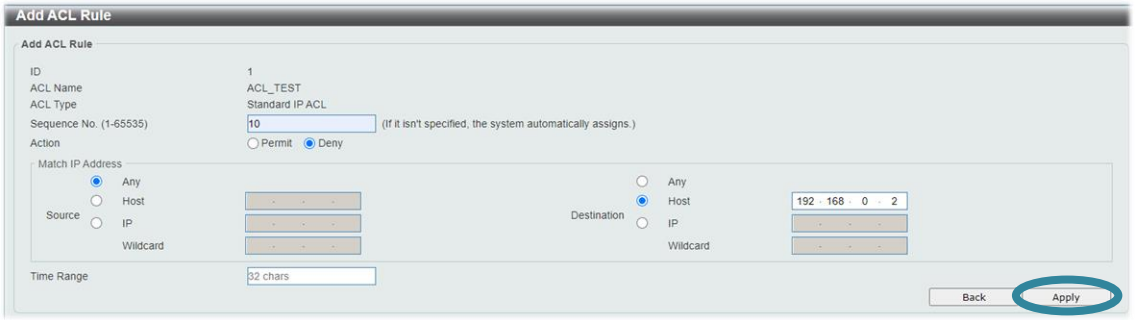




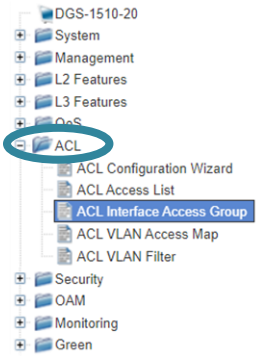
Successivamente, selezioniamo l'ACL precedentemente creata e aggiungiamo le regole che vogliamo associare ad essa usando l'opzione **Add Rule**

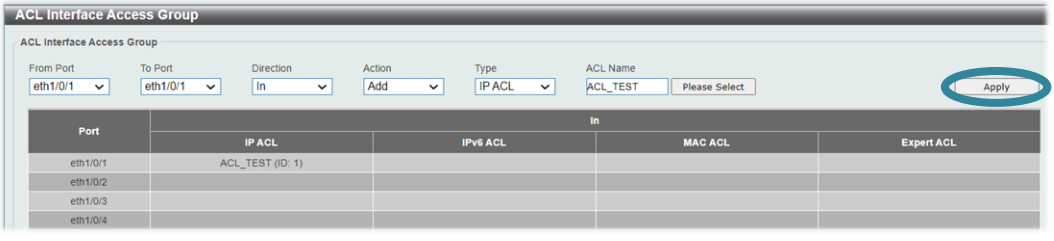


Inseriamo l'indirizzo IP in Destination /Host (192.168.0.2)



Infine, **applichiamo tale ACL** sulla interfaccia in cui intendiamo eseguire il filtraggio





Ora dalla porta 1 non si potrà più comunicare con l'IP 192.168.0.2

Come viene implementata una ACL tramite CLI?
(Valida solo per switch che supportano la configurazione tramite porta consolle dalla serie DGS-1250 /1510 e Managed)

I passaggi sono simili a quelli menzionati per l'interfaccia **grafica.**
Ecco i **comandi da** eseguire:

Creazione ACL:

```
Switch#configure terminal
Switch(config)#ip access-list ACL_TEST
```

Dopo averla creata, è possibile aggiungere le regole che si desidera associare ad essa:

```
Switch(config-ip-acl)#deny any host 192.168.0.2
```

```
DGS-1510#configure terminal
DGS-1510(config)#ip access-list ACL_TEST
DGS-1510(config-ip-acl)#deny any host 192.168.0.2
```

```
DGS-1510#show access-list ip ACL_TEST

Standard IP access list ACL_TEST(ID: 1999)
    10 deny any host 192.168.0.2
```

Infine, associamo **l'ACL** alle **interfacce Ethernet (in questo caso dalla 1 alla 2)** che vogliamo filtrare:

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-2
Switch(config-if-range)#ip access-group ACL_TEST
```

```
DGS-1510#configure terminal
DGS-1510(config)#interface range ethernet 1/0/1-2
DGS-1510(config-if-range)#ip access-group ACL_TEST
```

Le porta dalla 1 alla 2 non potranno comunicare con l'IP 192.168.0.2

Fine configurazione