Le ACL sono utilizzate all’interno dei Firewall packet filtering.  
In poche parole i Firewall sono i dispositivi che controllano il traffico in arrivo e in uscita di una rete, prevenendo così attacchi e accessi indesiderati. I firewall che filtrano i pacchetti IP sono quelli di tipo packet filtering. Permettono di bloccare o consenitre il traffico di dati che attraversa il firewall specificando l’indirizzo IP, ed eventualmente il protocollo e la porta dei dispostivi che si vogliono controllare.  
Le ACL sono proprio le regole che vengono scritte per attuare tale controllo.

**ACL**

Le ACL permettono la limitazione del traffico in rete e un livello base di sicurezza per l’accesso ad essa.  
Ogni regola ACL prende il nome di ACE (access control entry); al momento del controllo dell’ACL se le sue proprietà vengono soddisfatte viene effettuata l’azione vera e propria di controllo, ovvero se permettere o bloccare la trasmissione.

La valutazione delle ACL inizia dalla prima regola e continua finché le condizioni di una regola non sono soddisfatte. Ciò vuol dire che la valutazione di una lista di regole per un pacchetto termina appena le sue condizioni sono verificate da una ACE. Se nessuna regola viene verificata viene applicata la policy di default del firewall. Ne esistono di due tipi:

* Open policy: vengono permesse tutte le connessioni non specificatamente bloccate
* Closed policy: vengono bloccate tutte le connessioni non specificatamente consentite

Ovviamente la seconda consente un maggior livello di sicurezza ma è più indicata per una DMZ poiché altrimenti per un normale utilizzo della rete andrebbero consentiti tutti i siti e i protocolli/porte utilizzabili.

Esistono 2 tipi di ACL: standard ed estese. Cosa cambia? Le prime permettono il controllo del solo indirizzo mittente. Ciò vuol dire che sono utili per controllare il traffico in entrata, un po' meno per quello in uscita.

Mentre quelle estese permettono di effettuare controlli sia sull’indirizzo IP mittente che destinatario e anche sul protocollo e porta utilizzati permettendo un controllo più completo.

Una ACL, vista così, sembra che possa controllare un singolo dispositivo. Viene così in nostro aiuto la wildcard mask che consente di selezionare un gruppo di host basandosi sull’IP di uno di essi.

**WILDCARD MASK**

Il funzionamento delle wildcard mask non è banale. Si basa fondamentalmente sulla conversione in binario dell’indirizzo IP.  
Ma cos’è praticamente? È un numero di 32 bit diviso da 4 ottetti, proprio come l’indirizzo IP. È l’inverso della subnet mask.