Maschera non è un termine esclusivamente pirandelliano, anche in altri settori esistono cose o entità, che vogliono mascherarsi, fingere di essere altro oppure più cose allo stesso tempo. È il caso della Wildcard Mask. Cos’è? Una maschera, numerica, perciò astratta, che muta un indirizzo base in una moltitudine di indirizzi. Vediamo perché risulta utile.

È utilizzata nelle ACL (Access Control List) le quali sono utilizzate nei Firewall (in dettaglio in quelli packet filtering). I Firewall sono i dispositivi che controllano il traffico in arrivo e in uscita di una rete, prevenendo così attacchi e accessi indesiderati. Le ACL sono le regole che verranno attuate dai firewall packet filtering per svolgere la loro funzione di controllo.   
La wildcard mask è utilizzata nelle ACL per ottimizzarne la scrittura e la struttura condensando in una sola regola più regole uguali che differiscono solamente per l’indirizzo IP a cui esse si rivolgono.

Esempio: si vogliono bloccare 4 host in successione a partire da 192.168.0.8.  
 Struttura regola ACE: access-list [numero] [permit|deny] [IP-sorgente] [wildcard-mask]  
 La regola ACE da scrivere sarà: access-list 1 deny 192.168.0.8 0.0.0.3  
Perché 0.0.0.3? Perché la wildcard mask è un numero formato da 32 bit diviso in 4 ottetti ed ha bit a 1 dove i bit confrontati tra gli indirizzi sono diversi. I bit a 1 della Wildcard Mask non saranno oggetto di confronto durante il controllo dell’indirizzo della regola.

Un altro esempio: si vuole bloccare l’accesso agli indirizzi 192.168.0.41 e 192.168.0.57 ad una rete.  
A prima vista sembrano numeri lontani fra loro, ma analizziamo in binario i loro ultimi ottetti:  
192.168.0.41 001**0**1001   
192.168.0.57 001**1**1001  
Come si può notare cambia solo un bit. Pertanto la Wildcard Mask equivale a: 000**1**0000 ovvero 0.0.0.16

Scrivendo la seguente ACE:   
 access-list 1 deny 192.168.0.9 0.0.0.16  
verranno bloccati tutti gli IP che hanno gli stessi bit dell’indirizzo IP 192.168.0.41, ad eccezione del 5° bit dell’ultimo ottetto che risulta indifferente.

Ecco una realizzazione pratica:

Le ACL sono utilizzate all’interno dei Firewall packet filtering.  
In poche parole. I firewall che filtrano i pacchetti IP sono quelli di tipo packet filtering.

Permettono di bloccare o consentire 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.