Proceso de configuración de ACL

El proceso de creación de una ACL se lleva a cabo creando la lista y posteriormente asociándola a una interfaz entrante o saliente.
Configuración de ACL estándar
Router(config)#access-list[1-99][permit|deny][dirección de origen][mascara comodín]
Donde:
1-99 Identifica el rango y la lista.
Permit|deny indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección especificada.
Dirección de origen identifica la dirección IP de origen.
Mascara comodín o wildcard identifica los bits del campo de la dirección que serán comprobados.
La mascara predeterminada es 0.0.0.0 (coincidencia de todos los bits).
Asociación de la lista a una interfaz
Router(config-if)#ip access-group[nº de lista de acceso][in|out]
Donde:
Número de lista de acceso indica el número de lista de acceso que será aplicada a esa interfaz.
In|out selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.
Ejemplo de una ACL estándar denegando una red:
Router#configure terminal
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.0
Router(config)#access-list 10 permit any
Router(config)#interface serial 0
Router(config-if)#ip access-group 10 in
Se ha denegado al host 192.168.1.0 y luego se ha permitido a cualquier origen,
Posteriormente se asocio la ACL a la interfaz Serial 0.
Configuración de ACL extendida
El proceso de configuración de una ACL IP extendida es el siguiente:
Router(config)#access-list[100-199][permit|deny][protocol][dirección de origen][mascara comodín][dirección de destino][mascara de destino][puerto][establisehed][log]
100-199 identifica el rango y número de lista
Permit|deny: indica si la entrada permitirá o bloqueara la dirección especificada.
Protocolo: como por ejemplo IP, TCP, UDP, ICMP
Dirección origen y destino: identifican direcciones IP de origen y destino.
Mascara wildcard origen y mascara destino: Son las mascaras comodín. Las 0 indican las posiciones que deben coincidir, y los 1 las "que no importan".
Puerto:(opcional) puede ser por ejemplo: lt (menor que), gt (mayor que), eq (igual a), o neq (distinto que) y un número de puerto de protocolo correspondiente.
Establisehed: (opcional) Se usa solo para TCP de entrada. Esto permite que él rafico TCP pase si el paquete utiliza una conexión ya establecida (por ejemplo posee un conjunto de bits ACK)
Log: (opcional) Envía un mensaje de registro a la consola a un servidor syslog determinado.
Algunos de los números de puertos más conocidos:
20 Datos del protocolo FTP
21 FTP
23 Telnet
25 SMTP
69 TFTP
53 DNS

Asociación de la lista a una interfaz
Router(config-if)#ip access-group[nº de lista de acceso][in|out]
Donde:
Número de lista de acceso indica el número de lista de acceso que será aplicada a esa interfaz.
In|out selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.

Ejemplo de una ACL Extendida denegando un host hacia el puerto 80 de una red:
Router(config)#access-list 120 deny tcp host 204.204.10.1 any eq 80
Router(config)#access-list 120 permit ip any any
Router(config)#interface serial 1
Router(config-if)#ip access-group 120 in
Se ha denegado al host 204.204.10.1, (identificándolo con la abreviatura "host") hacia el puerto 80 de cualquier red de destino (usando el termino any). Posteriormente se permite todo trafico IP. Esta ACL se

asocio a la interfaz Serial 1 como entrante.
Aplicación de una ACL a la linea de telnet
Para evitar intrusiones no deseadas en las conexiones de telnet se puede crear una lista de acceso estándar y asociarla a la Line VTY. El proceso de creación se lleva a cabo como una ACL estándar denegando o permitiendo un origen hacia esa interfaz. El modo de asociar la ACL a la Línea de telnet es el siguiente:
router(config)#line vty 0 4
router(config-line)#access-class[Nº de lista de acceso][in|out]

Como eliminar las listas de acceso
Desde el modo interfaz donde se aplico la lista:
Router(config-if)#no ip access-group[Nº de lista de acceso]
Desde el modo global elimine la ACL
router(config)#no access-list[Nº de lista de acceso]