Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES DE COMUNICACIONES

Práctica : Listas de control de acceso

María Dolores Cano Baños

Natalio López Martínez

Referencias:

- Todd Lammle, “CCNA: Cisco Certified Network Associate. Study Guide”. 4ª Edición. Sybex Inc. 2004.

Objetivos

El principal objetivo de esta práctica es aprender a configurar listas de control de acceso (ACLs) en un *router* CISCO 1751, entendidas como un mecanismo eficiente para el filtrado de paquetes. La práctica comprende listas de control de acceso extendidas. Como objetivo secundario, podemos añadir el familiarizarse con las funciones y la configuración básica de un *router* CISCO 1751.

Introducción

Una lista de control de acceso es una lista de condiciones que permiten clasificar los paquetes que intentan atravesar un *router*. Dicha clasificación puede servirnos para filtrar paquetes de acuerdo con una determinada política de seguridad. Por ejemplo, permitir que sólo algunas máquinas, no pertenecientes a la red corporativa puedan acceder al servidor WEB o al servidor de correo de una empresa, o que sólo determinados usuarios tengan acceso a Internet. Las listas de control de acceso también pueden servirnos como indicativo de tráfico de interés en un túnel IPSec. En esta práctica, las usaremos para el filtrado de paquetes.

Desarrollo de la práctica

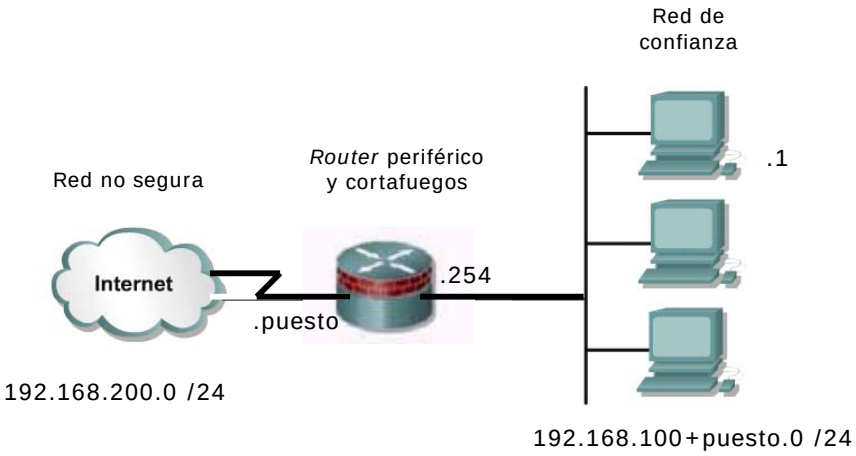


Figura 1

Cada puesto consta de:

- Un *router* CISCO 1751
  - Este *router* tiene dos funciones: por un lado, el encaminamiento de paquetes desde/hacia la red interna y, por otro, actuar de cortafuegos, filtrado los paquetes de confianza y descartando los demás.
- Un cable de consola
  - Para la conexión del *router* y el PC, a través del puerto de consola.
- Dos PCs

- Un PC como terminal de configuración del *router*
- Otro PC como generador/receptor de tráfico.

- Un cable cruzado UTP, con conectores RJ-45
  - Para la conexión del *router* y el PC, a través de la interfaz Ethernet.

2. Configuración Básica de un *router* CISCO 1751

2.1 Conexión a un *router* CISCO

Podemos conectarnos a un *router* CISCO para configurarlo, verificar su correcta configuración o para obtener estadísticas. Aunque existen distintas posibilidades para conseguir esa conexión, la forma más habitual -y la que utilizaremos en esta práctica- es a través del puerto de consola. Para acceder a la consola del *router*, hay que ejecutar el hyperterminal de windows o si estamos en linux ejecutaremos el programa de Linux *Kermit*, sabiendo que los parámetros para la comunicación a través del puerto serie deben configurarse de la siguiente manera:

Velocidad de la línea -> 9600
Bits de datos -> 8
Paridad -> sin paridad
Bits de *stop* -> 2
Control de flujo -> *hardware*

Nota: Los comandos a ejecutar para conseguir la configuración deseada en linux son:

```
>Kermit
C-kermit> set serial 8N1
C-kermit>set carrier-watch off
C-Kermit>set line /dev/ttyS0
C-Kermit>set speed 9600
C-Kermit> connect
```

2.2 Puesta en marcha de un *router* CISCO

Una vez que nos hemos conectado al *router*, hay que encenderlo (el interruptor de encendido se sitúa en el panel trasero del mismo). Al encender el equipo, en primer lugar, se carga en la memoria RAM el sistema operativo IOS. A continuación, el IOS busca una configuración válida para el *router* en la NVRAM y, si la encuentra, la carga en la RAM. De lo contrario pasa al modo *setup*, donde se nos pregunta si queremos entrar en el dialogo de configuración inicial:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog?
[yes/no]:
```

Si la respuesta es “sí”, permanecemos en el modo *setup* e iremos configurando paso a paso distintos parámetros del *router*. Sin embargo, muchos de esos parámetros no son de interés para el correcto desarrollo de esta práctica, por lo que **la respuesta debe ser “no”**. En cuyo caso se nos formulará una segunda pregunta:

Would you like to terminate autoinstall? [yes]:[enter]

En este caso nuestra **respuesta debe ser “sí”.** De esta forma accederemos a la interfaz de línea de comandos (CLI).

La interfaz de línea de comandos tiene dos modos de funcionamiento:

- *User exec mode*
- *Privileged exec mode*

Desde el modo *user exec mode* (cuyo *prompt* es *Router*>) se pueden ver distintas estadísticas y pasar al modo privilegiado usando el comando enable:

Router> // Modo user exec

Router>enable

Router# // Modo privileged exec

Desde el modo privilegiado (cuyo *prompt* es *Router*#), además de ver distintas estadísticas, se puede modificar la configuración del *router*.

2.3 Configuración específica de la práctica

Para poder modificar la configuración actual del *router* (la que está cargada en la RAM), es necesario trabajar en alguno de los modos de configuración.

Desde el modo privilegiado, podemos pasar al modo de configuración global y desde éste a modos de configuración más específicos. Por ejemplo, para configurar los parámetros de una interfaz o de un protocolo de encaminamiento (RIP, OSPF).

Para pasar del modo privilegiado al modo de configuración global, se utiliza el comando ***configure terminal***. Los parámetros que se modifican en este modo afectan de forma global a todo el *router*.

Router#

Router# configure terminal

Router(config)# // Modo de configuración global

Router(config)# Ctrl^Z // Regreso a modo privilegiado

Router#

2.3.1 Configuración de la interfaz Ethernet

En primer lugar hay que asignarle una IP a la interfaz, y en segundo lugar, activarla. La secuencia de comandos a ejecutar en este caso sería:

Router#configure terminal

Router(config)# interface FastEthernet 0/0

Router(config-if)#ip address 192.168.14.1 255.255.255.0

// Dirección --- máscara de red

Router(config-if)#no shutdown

// Activar la interfaz

NOTA: Dependiendo del modelo del router, la interfaz se denomina FastEthernet 0/0 ó FastEthernet 0.

2.3.2 Configuración de las listas de control de acceso

A la hora de crear una lista de control de acceso hay que tener en cuenta lo siguiente:

1. Cuando un paquete se compara con una lista de control de acceso, cada una de las líneas de la lista se examina de forma secuencial hasta que haya coincidencia.
2. Una vez encontrada la coincidencia, el paquete se acepta o se rechaza (dependiendo de lo que indique la línea), y el proceso de comparación se detiene.
3. Existe una sentencia “deny” implícita al final de cualquier lista de acceso. Esto significa que si un paquete no cumple ninguna de las condiciones enumeradas en la lista, será rechazado.
4. Cada vez que se añade una línea a la lista de acceso, dicha línea se sitúa al final de la lista.
5. No se puede eliminar una línea de una lista de acceso. Hay que eliminar la lista completa.
6. Si la lista de acceso no incluye al menos una sentencia “permit”, se rechazarán todos los paquetes, debido la sentencia implícita “deny”.

Los *routers* CISCO permiten crear distintos tipos de listas de control de acceso, nosotros veremos las dos más habituales: las listas de control de acceso estándar y las listas de control de acceso extendidas.

Las listas de control de acceso estándar utilizan la dirección IP origen del paquete para comparar. No distinguen entre protocolos. Sin embargo, las listas de control de acceso extendidas, además de poder comparar en función de la dirección IP de origen o destino, permiten discriminar en función del protocolo de nivel 4 (tcp, udp, icmp) y de la aplicación (www, telnet, ftp, ...)

Al final del guión de la práctica se incluye un apéndice con el formato de los comandos que permiten crear listas de acceso estándar y extendidas (Sólo en reprografía).

Una vez creada, para que una lista de control de acceso sea efectiva es necesario aplicarla a una interfaz, en sentido entrante (in) o saliente (out) siempre desde el punto de vista del router. Sólo se puede asignar una lista de control de acceso por interfaz y sentido de la comunicación. La secuencia de comandos que nos permite crear una lista de control de acceso estándar y aplicarla a una interfaz en un sentido es la siguiente:

Router# configure terminal

//Crear la lista de acceso

Router(config)# access-list 10

Router(config-acl)# deny host 172.16.20.1

Router(config-acl)# exit

//Aplicarla a la interfaz en sentido entrante

Router(config)# interface FastEthernet 0/0

Router(config-if)# ip access-group 10 in

Para eliminar la lista, la secuencia de comandos sería:

Router(config)# interface ethernet 0/0

Router(config-if)# no ip access-group 10 in

Router(config-if)#exit

Router(config)# no access-list 10 deny host 172.16.20.1

2.3.3 Otros comandos de utilidad

show running-config

Este comando muestra la configuración actual del *router*.

show interface

Este comando muestra la información relativa a una interfaz: su dirección IP, si está o no activa, qué tipo de encapsulado utiliza, etc.

show ip interface

Este comando muestra información relativa a una interfaz, relacionada con el protocolo IP.

show ip route

Este comando muestra la tabla de encaminamiento del equipo.

show ip access-list

Este comando muestra las listas de acceso existentes.

show controllers *interface interface-number*

Este comando proporciona información sobre la interfaz física. Si se trata de una interfaz serial, nos dirá que tipo de cable tiene conectado: DCE o DTE.

copy run start

Este comando permite volcar el contenido de la memoria RAM en la memoria NVRAM.

erase startup-config

Este comando permite borrar el fichero de configuración almacenado en la memoria no volátil. Fichero que se carga en la memoria RAM del sistema en el momento del arranque.

reload

Este comando permite reiniciar el equipo.

?

Este es el comando de ayuda. Tecleando ? en cualquier modo podemos ver la lista de comandos que se pueden ejecutar en ese modo. Asimismo, muestra todas las posibles opciones que acompañan a un comando.

hostname

Con este comando podemos darle un nombre al *router*. Este nombre sólo tiene significado local.

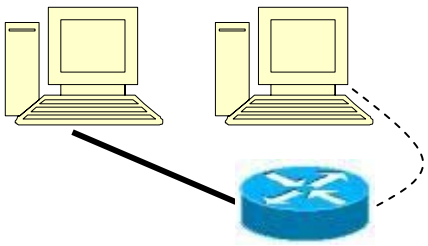
Router#configure terminal

Router(config)#hostname Puesto11

Puesto11(config)#

En esta página WEB: www.cisco.com/univercd , se puede encontrar más información sobre los comandos incluyendo numerosos ejemplos de uso.

Escenario



Interfaz LAN ——————

Consola ---------

Figura 2

Ejercicios

1. Conecte el *router* y los PCs siguiendo la topología de la figura 2.

2. Modifique la configuración de su PC de tal forma que su dirección IP sea 192.168.14.2, con máscara de red 255.255.255.0 y pasarela por defecto su *router* (192.168.14.1).

Configuración inicial

3. Borre el fichero de configuración situado en la NVRAM, reinicie el *router* y acceda a la línea de comandos. ¿Qué comandos ha utilizado?

4. Modifique el nombre de su *router*, de tal forma que refleje el puesto en el que está, por ejemplo, Puesto-11. ¿Qué comando se utiliza para hacerlo?

5. Configure la interfaz de red Ethernet del router con la dirección 192.168.14.1.

6. En el modo de configuración global, inserte el comando ip http server. Desde el PC, abra un navegador y ponga como URL http://192.168.14.1. Ha de abrirse el servidor web del router.

Listas de control de acceso extendida

Una vez solucionados todos los problemas de conectividad, vamos a una lista de control de acceso.

7. ¿Qué valores se pueden utilizar como identificador para las listas de acceso extendidas?

8. Cree una lista de control de acceso extendida que impida el tráfico web procedente de cualquier máquina de la red 192.168.14.0 y aplíquela a la interfaz correspondiente. ¿En qué sentido (entrante, saliente)? Indique cuál es resultado mostrado por el comando show access-list.

9. Ejecute desde el *PC* el comando un ping al router. ¿Es exitoso? ¿Debería serlo?

10. Abra de nuevo un navegador y ponga como URL http://192.168.14.1 ¿Qué ocurre en este caso?¿Por qué?

Apéndice (Comandos para crear las listas de control de acceso)

access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | ***icmp-message***] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol (UDP)

For UDP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-

	Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
timeout *minutes*	(Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword. Some protocols allow further qualifiers described below.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

	Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. By default, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging

	messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.
log-input	(Optional) Includes the input interface and source MAC address or VC in the logging output.
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A

	port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, SYN or URG control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the " Access List Processing of Fragments" and " Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Global configuration

Examples

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following example permits 131.108.0/24 but denies 131.108/16 and all other subnets of 131.108.0.0:

```
access-list 101 permit ip 131.108.0.0 0.0.0.0     255.255.255.0
0.0.0.0
access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0
0.0.255.255
```

access-list (IP standard)

To define a standard IP access list, use the standard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]

no **access-list** *access-list-number*

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and source-wildcard of 0.0.0.0 255.255.255.255.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate the logging messages to appear when the number of matches reaches a

	configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.

Defaults

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Modes

Global configuration

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0  0.0.0.255
access-list 1 permit 128.88.0.0  0.0.255.255
access-list 1 permit 36.0.0.0  0.255.255.255
```

```
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3  0.0.0.0
```

ip access-group

To control access to an interface, use the **ip access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ip access-group {*access-list-number* | *access-list-name*}{**in** | **out**}

no **ip access-group** {*access-list-number* | *access-list-name*}{**in** | **out**}

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
access-list-name	Name of an IP access list as specified by an **ip access-list** command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Command Modes

Interface configuration

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
interface ethernet 0
 ip access-group 101 out
```

access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

access-class ***access-list-number*** {**in** [**vrf-also**] | **out**}

no access-class ***access-list-number*** {**in** | **out**}

Syntax Description

access-list-number	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
vrf-also	Accepts incoming connections from interfaces that belong to a VRF.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Command Modes

Line configuration

Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0  0.0.0.255
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 36.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 36.0.0.0 0.255.255.255
 line 1 5
 access-class 10 out
```