www.howtonetwork.com

CCNA: ACCESS CONTROL LIST (ACL) CHEAT SHEET

Overview

An ACL consists of sequential series of statements known as an Access Control Entry (ACE). Each ACE specifies a matching criteria and an action which can be either Permit or deny. The matching criteria can be various things such as source/destination address or protocol such as TCP or UDP. For an individual ACE all configured matching values must match in order for that ACE to be considered as match. The specifics of sequence determine how ACL will behave, so it recommended to include the most relevant ACE in the beginning of the ACL.

If a packet does not match any of the access control entries in an ACL then it matches an Implicit Deny ACE that is present at the bottom in all ACLs. The Implicit Deny ACE is a deny all statement that denies all packets. In case this behavior is not required and packets that do not match any ACE must be forwarded, an ACE must be specified at the bottom of ACL that permits all packets. This type of ACE is known as explicit permit.

Access Control List is a multipurpose tool that is typically used as filtering tool. ACLs can be used for

- Filtering traffic entering and existing an interface
- Controlling access to VTY lines
- Route update filtering
- As a traffic classification tool when used with QoS
- Dial-on-demand routing (DDR) with ISDN
- Restricting output of debug commands

Types of Access List

There are two types of IP Access Lists

1. Standard ACL

Traffic is filtered based on source address of the IP packet. Since only the source address is matched, therefore, standard ACLs are efficient in filtering traffic closet to the destination

2. Extended

Traffic can be filtered based on source address as well as destination address and other filed in IP header including source and destination protocol and port number, ToS and IP Precedence bits and TCP flags, TTL value

Numbered and Named ACLsC

An ACL can be identified as either named or numbered.

Numbered standard ACLs range 1-to-99 and 1300-to-1999 and extended ACL ranges from 100-to-199 and 2000-to-2699

Named ACL allows (easier) naming convention to be used instead of numbers

ACL Rule

Only one ACL per interface, per protocol, per direction is allowed

Inbound packets are always processed by an ACL (if applied) before being routed. Outbound packets are routed before processed by an ACL (if applied)

ACLs are processed in sequential order, therefore most specific traffic match must occur in the beginning of the ACL

An empty ACL permits all traffic

Wildcard Mask

Address filtering uses wildcard masking indicate whether to check or ignore corresponding IP address bit when comparing address bits in an ACL entry

Wildcard mask is sometime referred as an inverted mask because 1 and 0 means the opposite of subnet mask. Wildcard mask bit 0 means check the corresponding bit and 1 means ignore the corresponding bit

If wildcard mask is not specified, an implicit wildcard mask of 0.0.0.0 is assumed

Unlike subnet mask, wildcard mask allow non-contiguous bits in the mask

ACL Syntax

An ACL is implemented in two steps:

1. define an ACL with "access-list or ip access-list" command
2. apply the ACL under specific interface in the required direction with "ip access-group" command

STEP-1: Define and ACL

Standard ACL:

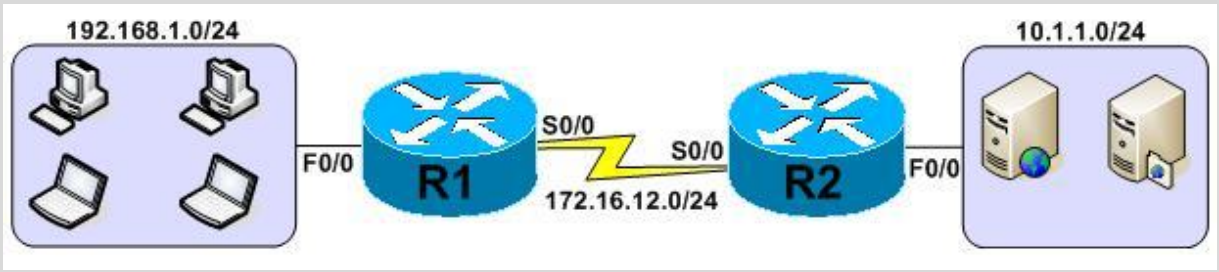
access-list acl-number {permit|deny} {host|source source-wildcard|any}

Extended ACL:

access-list acl-number {permit|deny} protocol source wildcard [operator [port]] destination wildcard [operator [port]] [precedence precedence] [tos tos]

STEP-2: Apply the ACL

interface <interface-id>
 ip access-group {number|name} {in|out}



Configuration Example: Standard ACL

Requirement: Web-Server 10.1.1.10 behind R2 should not be accessible by hosts 192.168.1.10 & 11

Router R1:

```
access-list 10 deny host 192.168.1.10
access-list 10 deny host 192.168.1.11
access-list 10 permit any
!
interface serial0/0
 ip address 172.16.12.2 255.255.255.0
 ip access-group 10 in
```

Configuration Example: Extended ACL

Requirement: Any access on port 80 should not be allowed from host 192.168.1.10 and 11 to web-server 10.1.1.10. Other hosts on the 192.168.1.0/24 network should be allowed access the web server only on port 80

Router R1:

```
access-list 101 deny tcp host 192.168.1.10 host 10.1.1.10 eq 80
access-list 101 deny tcp host 192.168.1.11 host 10.1.1.10 eq 80
access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.10 eq 80
!
interface fastethernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 in
```

Troubleshooting Command

```
show running-configuration | include access-list
show access-list [name | number]
```