Access List Tutorial

February 13th, 2011 Go to comments

In this tutorial we will learn about access list.

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces. Just imagine you come to a fair and see the guardian checking tickets. He only allows people with suitable tickets to enter. Well, an access list's function is same as that guardian.

Access lists filter network traffic by controlling whether packets are forwarded or blocked at the router's interfaces based on the criteria you specified within the access list.

To use ACLs, the system administrator must first configure ACLs and then apply them to specific interfaces. There are 3 popular types of ACL: Standard, Extended and Named ACLs.

Standard IP Access List

Standard IP lists (1-99) only check source addresses of all IP packets.

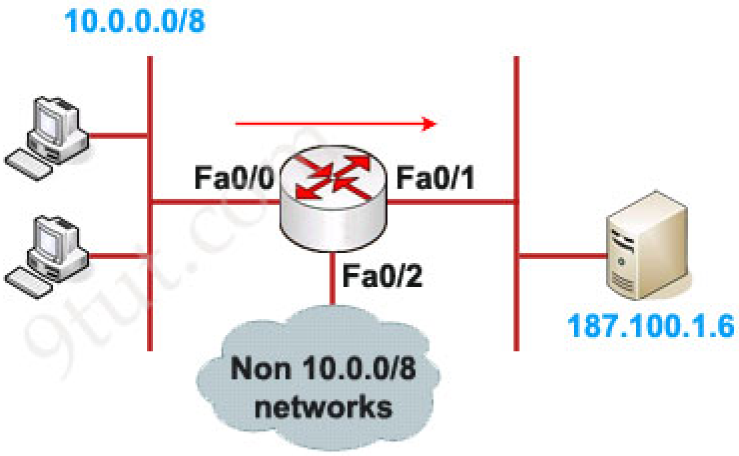
Configuration Syntax

```
access-list access-list-number {permit | deny} source {source-mask}
```

Apply ACL to an interface

```
ip access-group access-list-number {in | out}
```

Example of Standard IP Access List



Configuration:

In this example we will define a standard access list that will only allow network 10.0.0.0/8 to access the server (located on the Fa0/1 interface)

Define which source is allowed to pass:

```
Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
```

(there is always an implicit deny all other traffic at the end of each ACL so we don't need to define forbidden traffic)

Apply this ACL to an interface:

```
Router(config)#interface Fa0/1
Router(config-if)#ip access-group 1 out
```

The ACL 1 is applied to permit only packets from 10.0.0.0/8 to go out of Fa0/1 interface while deny all other traffic. So can we apply this ACL to other interface, Fa0/2 for example? Well we can but shouldn't do it because users can access to the server from other interface (s0 interface, for example). So we can understand why an standard access list should be applied close to the destination.

Note: The "0.255.255.255" is the wildcard mask part of network "10.0.0.0". We will learn how to use wildcard mask later.

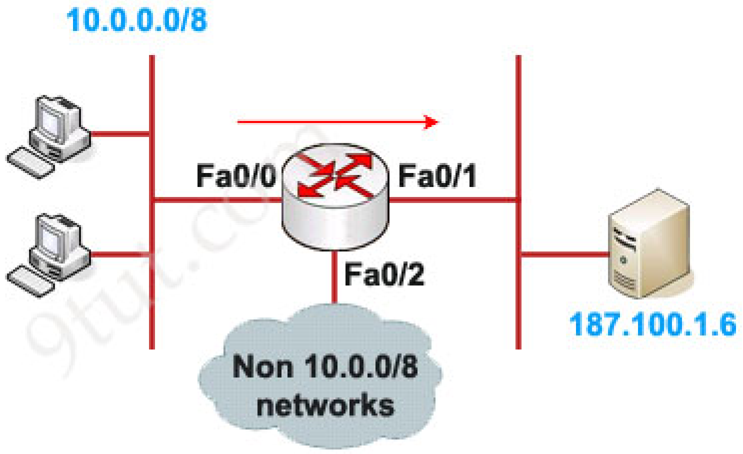
Extended IP Access List

Extended IP lists (100-199) check both source and destination addresses, specific UDP/TCP/IP protocols, and destination ports.

Configuration Syntax

access-list *access-list-number* {permit | deny} *protocol* source {source-mask} destination {destination-mask} [eq destination-port]

Example of Extended IP Access List



In this example we will create an extended ACL that will deny FTP traffic from network 10.0.0.0/8 but allow other traffic to go through.

Note: FTP uses TCP on port 20 & 21.

Define which protocol, source, destination and port are denied:

```
Router(config)#access-list 101 deny tcp 10.0.0.0 0.255.255.255 187.100.1.6 0.0.0.0 eq 21

Router(config)#access-list 101 deny tcp 10.0.0.0 0.255.255.255 187.100.1.6 0.0.0.0 eq 20

Router(config)#access-list 101 permit ip any any
```

Apply this ACL to an interface:

```
Router(config)#interface Fa0/1
Router(config-if)#ip access-group 101 out
```

Notice that we have to explicit allow other traffic (access-list 101 permit ip any any) as there is an “deny all” command at the end of each ACL.

As we can see, the destination of above access list is “187.100.1.6 0.0.0.0” which specifies a host. We can use “host 187.100.1.6” instead. We will discuss wildcard mask later.

In summary, below is the range of standard and extended access list

Access list type	Range
Standard	1-99, 1300-1999
Extended	100-199, 2000-2699

Pages: 1 2

Comments (7) Comments

1. Lonny Wormald
   January 21st, 2020

   Marvelous, what a weblog it is! This website provides helpful information to us, keep it up.

2. Shad Pinkham
   January 21st, 2020

   Thanks for sharing your thoughts. I really appreciate your efforts and I am waiting for your next write ups thanks once again.

3. Leilani Creamer
   January 22nd, 2020

   Hi, after reading this amazing paragraph i am as well glad to share my familiarity here with friends.

4. Hipiri
   January 23rd, 2020

   Hello, the rule of thumb is.

   first deny then anything else is permitted right?

5. @9 tut: Regarding your Extended Access List example
   February 1st, 2020

   @9 tut: Regarding your Extended Access List example, isn’t it better to implement the Extended ACL closest to the source / traffic to be matched? (so that you can prevent unnecessary bandwidth usage as the frame would be sent all the way down to the destination if you choose Fa0/1, rather than dropping it closest to the source at Fa0/0).
   In this case, interface Fa0/0 and apply ACL as: ip access-group 101 in (instead of out) ?

6. Them
   February 6th, 2020

   where are the questions May you please provide link

7. Brozzo
   August 19th, 2021

   True ….. Extended ACL are best done close to the source to eliminate unnecessary bandwidth consumption.

Add a Comment

Name

Submit Comment

Subscribe to comments feed
CCNA – VTP Questions CCNA – Hotspot

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions
- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2
- EIGRP Questions

- NAT Questions
- NTP Questions
- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3
- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial
- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI
- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy
- Frame Relay Tutorial

- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial
- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
  - CCNA Website
  - ENCOR Website
  - ENSDWI Website
  - ENARSI Website
  - DevNet Website
  - CCIE R&S Website
  - Security Website
  - Wireless Website
  - Design Website
  - Data Center Website
  - Service Provider Website
  - Collaboration Website

Top