Access List Tutorial

February 13th, 2011 Go to comments

Named IP Access List

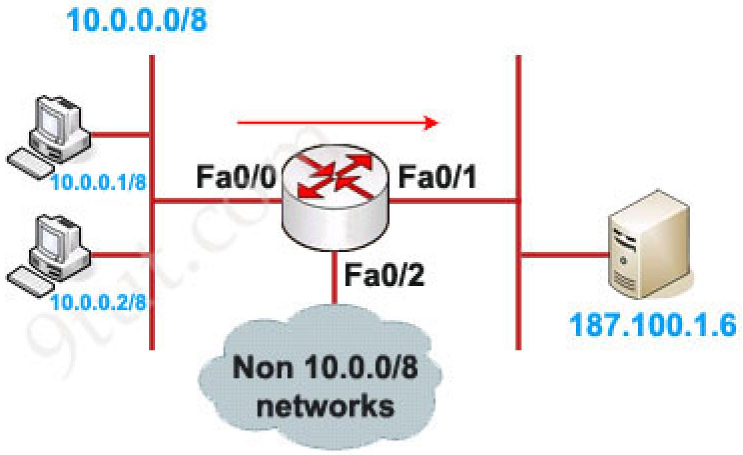
This allows standard and extended ACLs to be given names instead of numbers

Named IP Access List Configuration Syntax

ip access-list {standard | extended} {name | number}

Example of Named IP Access List

This is an example of the use of a named ACL in order to block all traffic except the Telnet connection from host 10.0.0.1/8 to host 187.100.1.6.



Define the ACL:

```
Router(config)#ip access-list extended in_to_out permit tcp host 10.0.0.1 host 187.100.1.6 eq telnet
```

(notice that we can use ‘telnet’ instead of port 23)

Apply this ACL to an interface:

```
Router(config)#interface Fa0/0
```

```
Router(config-if)#ip access-group in_to_out in
```

Where to place access list?

Standard IP access list should be placed close to destination.

Extended IP access lists should be placed close to the source.

How many access lists can be used?

You can have one access-list per protocol, per direction and per interface. For example, you can not have two access lists on the inbound direction of Fa0/0 interface. However you can have one inbound and one outbound access list applied on Fa0/0.

How to use the wildcard mask?

Wildcard masks are used with access lists to specify a host, network or part of a network.

The zeros and ones in a wildcard determine whether the corresponding bits in the IP address should be checked or ignored for ACL purposes. For example, we want to create a standard ACL which will only allow network 172.23.16.0/20 to pass through. We need to write an ACL, something like this:

access-list 1 permit 172.23.16.0 255.255.240.0

Of course we can't write subnet mask in an ACL, we must convert it into wildcard mask by converting all bits 0 to 1 & all bits 1 to 0.

255 = 1111 1111 -> convert into 0000 0000

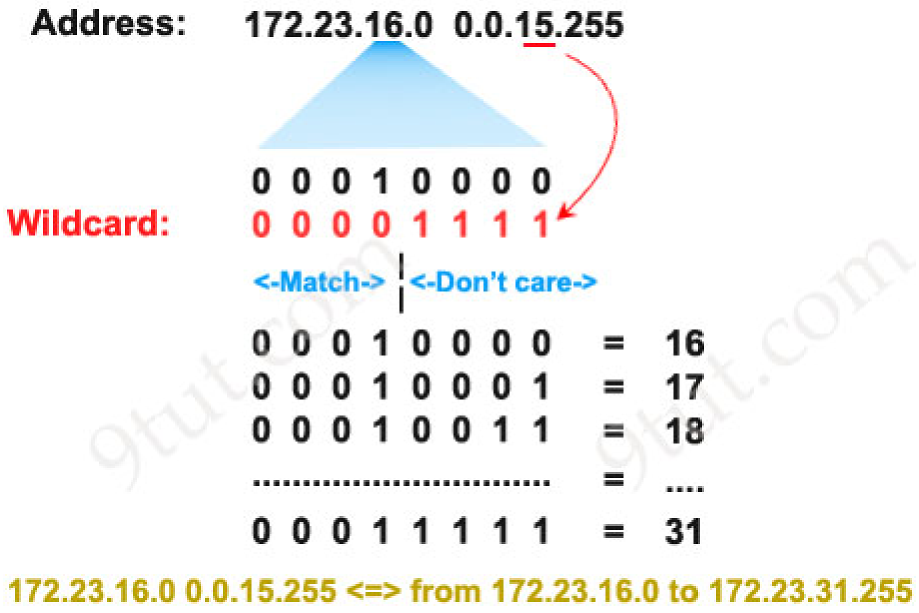
240 = 1111 0000 -> convert into 0000 1111

0 = 0000 0000 -> convert into 1111 1111

Therefore 255.255.240.0 can be written in wildcard mask as 00000000.00000000.00001111.11111111 = 0.0.15.255

Remember, for the wildcard mask, **1′s are I DON'T CARE, and 0′s are I CARE**. Now let's analyze our wildcard mask.

Two first octets are all 0's meaning that we care about the network **172.23**.x.x. The third octet, 15 (0000 1111 in binary), means that we care about first 4 bits but don't care about last 4 bits so we allow the third octet in the form of 0001xxxx (minimum:0001**0000 =** 16; maximum: 000**1111** = 31).



The fourth octet is 255 (all 1 bits) that means I don't care.

Therefore **network 172.23.16.0 0.0.15.255** ranges from **172.23.16.0** to **172.23.31.255**.

Some additional examples:

+ Block TCP packets on port 30 from any source to any destination:

```
Router(config)#access-list 101 deny tcp any any eq 30
```

+ Permit any IP packets in network 192.23.130.128 with subnet mask 255.255.255.248 to any network:

```
Router(config)#access-list 101 permit ip 192.23.130.128 0.0.0.7 any
```

Apply the access control list to an interface:

```
Router(config)#interface fastEthernet0/0

Router(config-if)#ip access-group 101 in
```

Note: An ACL applied to the main interface does not affect the traffic of subinterfaces. If we want to filter traffic on subinterfaces, we have to assign ACL to each subinterface separately.

There are some differences between numbered ACL and named ACL:

+ Only numbered ACL is supported on VTY lines (by using the access-class command)
+ Only named ACL support Noncontiguous Ports (allows you to specify noncontiguous ports in a single ACL statement). For example:

```
Router(config)#ip access-list extended noncontiguousPorts
Router(config-ext-nacl)# permit tcp any eq telnet ftp any eq 23 45 34
```

+ Only with named ACL, we can easily remove an individual entry. For example:

```
R1# show access-list

Standard IP access list nat_traffic
10 permit 10.1.0.0, wildcard bits 0.0.255.255
20 permit 10.2.0.0, wildcard bits 0.0.255.255
30 permit 10.3.0.0, wildcard bits 0.0.255.255
```

Then to remove the second statement (the line “20 permit 10.2.0.0, wildcard bits 0.0.255.255”) we just need to type “no 20”:

```
R1(config)#ip access-list standard nat_traffic
R1(config-std-nacl)#no 20
```

But for numbered ACL, we have to recreated the whole ACL when entries are moved.

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