**Standard access lists**

Because a standard access list filters only traffic based on source traffic, all you need is the IP address of the host or subnet you want to permit or deny. ACLs are created in global configuration mode and then applied on an interface. The syntax for creating a standard ACL is

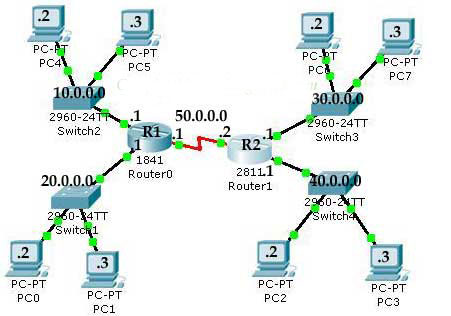
access-list {1-99 | 1300-1999} {permit | deny} source-address

[wildcard mask]

In this article we will configure standard access list. If you want read the feature and characteristic of access list reads this previous article.

[Access control list](http://computernetworkingnotes.com/ccna_certifications/access_control_list.htm)

In this article we will use a RIP running topology. Which we created in RIP routing practical.

[](http://computernetworkingnotes.com/ccna_certifications/rip_routing.htm)

**Three basic steps to configure Standard Access List**

* Use the access-list global configuration command to create an entry in a standard ACL.
* Use the interface configuration command to select an interface to which to apply the ACL.
* Use the ip access-group interface configuration command to activate the existing ACL on an interface.

With Access Lists you will have a variety of uses for the wild card masks, but typically For CCNA exam prospective you should be able to do following:

1. Match a specific host,
2. Match an entire subnet,
3. Match an IP range, or
4. Match Everyone and anyone

**Match specific hosts**

**Task**

*You have given a task to block 10.0.0.3 from gaining access on 40.0.0.0. While 10.0.0.3 must be able to communicate with networks. Other computer from the network of 10.0.0.0 must be able to connect with the network of 40.0.0.0.*

**Decide where to apply ACL and in which directions.**

Our host must be able to communicate with other host except 40.0.0.0 so we will place this access list on FastEthernet 0/1 of R2 (2811) connected to the network of 40.0.0.0. Direction will be outside as packet will be filter while its leaving the interface. If you place this list on R1(1841) then host 10.0.0.3 will not be able to communicate with any other hosts including 40.0.0.0.

To configure R2 double click on it and select CLI (Choose only one method result will be same)

***R2>enable***

***R2#configure terminal***

***Enter configuration commands, one per line. End with CNTL/Z.***

***R2(config)#access-list 1 deny host 10.0.0.3***

***R2(config)#access-list 1 permit any***

***R2(config)#interface fastEthernet 0/1***

***R2(config-if)#ip access-group 1 out***

**OR**

***R2>enable***

***R2#configure terminal***

***Enter configuration commands, one per line. End with CNTL/Z.***

***R2(config)#access-list 1 deny 10.0.0.3 0.0.0.0***

***R2(config)#access-list 1 permit any***

***R2(config)#interface fastEthernet 0/1***

***R2(config-if)#ip access-group 1 out***

To test first do ping from 10.0.0.3 to 40.0.0.3 it should be request time out as this packet will filter by ACL. Then ping 30.0.0.3 it should be successfully replay.

***PC>ping 40.0.0.3***

***Pinging 40.0.0.3 with 32 bytes of data:***

***Request timed out.***

***Request timed out.***

***Request timed out.***

***Request timed out.***

***Ping statistics for 40.0.0.3:***

***Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),***

***PC>ping 30.0.0.3***

***Pinging 30.0.0.3 with 32 bytes of data:***

***Request timed out.***

***Reply from 30.0.0.3: bytes=32 time=140ms TTL=126***

***Reply from 30.0.0.3: bytes=32 time=156ms TTL=126***

***Reply from 30.0.0.3: bytes=32 time=112ms TTL=126***

***Ping statistics for 30.0.0.3:***

***Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),***

***Approximate round trip times in milli-seconds:***

***Minimum = 112ms, Maximum = 156ms, Average = 136ms***

As we applied access list only on specific host so other computer from the network of 10.0.0.0 must be able to connect with the network of 40.0.0.0. To test do ping from 10.0.0.2 to 40.0.0.3

***PC>ipconfig***

***IP Address......................: 10.0.0.2***

***Subnet Mask.....................: 255.0.0.0***

***Default Gateway.................: 10.0.0.1***

***PC>ping 40.0.0.3***

***Pinging 40.0.0.3 with 32 bytes of data:***

***Request timed out.***

***Reply from 40.0.0.3: bytes=32 time=141ms TTL=126***

***Reply from 40.0.0.3: bytes=32 time=140ms TTL=126***

***Reply from 40.0.0.3: bytes=32 time=125ms TTL=126***

***Ping statistics for 40.0.0.3:***

***Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),***

***Approximate round trip times in milli-seconds:***

***Minimum = 125ms, Maximum = 141ms, Average = 135ms***

**Match an entire subnet**

**Task**

*You have given a task to the network of 10.0.0.0 from gaining access on 40.0.0.0. While 10.0.0.0 must be able to communicate with networks .*

**Wildcards**

Wildcards are used with access lists to specify an individual host, a network, or a certain range of a network or networks.

Formula to calculate wild card mask for access list

The key to matching an entire subnet is to use the following formula for the wildcard mask. It goes as follows:  
**Wildcard mask = 255.255.255.255 – subnet**  
So for example if my current subnet was 255.0.0.0, the mask would be 0.255.255.255.

***255.255.255.255***

***255 .0 .0 .0 -***

***----------------***

***0. 255 .255.255***

***----------------***

Once you have calculated the wild card mask rest is same as we did in pervious example

***R2>enable***

***Enter configuration commands, one per line. End with CNTL/Z.***

***R2(config)#access-list 2 deny 10.0.0.0 0.255.255.255***

***R2(config)#access-list 2 permit any***

***R2(config)#interface fastethernet 0/1***

***R2(config-if)#ip access-group 2 out***

***R2(config-if)#***

To test first do ping from 10.0.0.3 to 40.0.0.3 it should be request time out as this packet will filter by ACL. Then ping 30.0.0.3 it should be successfully replay.

Now do ping from 10.0.0.2 to 40.0.0.3 and further 30.0.0.2 result should be same as the packet is filtering on **network based**

**Match an IP range**

*You are a network administrator at ComputerNetworkingNotes.com. You task is to block an ip range of 10.3.16.0 – 10.3.31.255 from gaining access to the network of 40.0.0.0*

**Solutions**

Our range is 10.3.16.0 – 10.3.31.255. In order to find the mask, take the higher IP and subtract from it the lower IP.

***10.3.31.255***

***10.3.16.0 -***

***--------------***

***0.0.15.255***

***--------------***

In this case the wildcard mask for this range is 0.0.15.255.  
To permit access to this range, you would use the following:

***R2>enable***

***Enter configuration commands, one per line. End with CNTL/Z.***

***R2(config)#access-list 2 deny 10.3.16.0 0.0.15.255***

***R2(config)#access-list 2 permit any***

***R2(config)#interface fastethernet 0/1***

***R2(config-if)#ip access-group 2 out***

***R2(config-if)#***

One thing to note is that each non-zero value in the mask must be one less than a power of 2, i.e. 0, 1, 3, 7, 15, 31, 63, 127, 255.

**Match Everyone and Anyone**

This is the easiest of Access-Lists to create, just use the following:   
access-list 1 permit any   
**or**  
access-list 1 permit 0.0.0.0 255.255.255.255

**Secure telnet session via standard ACL**

This is among the highly tested topic in CCNA exam. We could use extended ACL to secure telnet session but if you did that, you’d have to apply it inbound on every interface, and that really wouldn’t scale well to a large router with dozens, even hundreds, of interfaces.Here's a much better solution:

***Use a standard IP access list to control access to the VTY lines themselves.***

To perform this function, follow these steps:

1. Create a standard IP access list that permits only the host or hosts you want to be able to telnet into the routers.
2. Apply the access list to the VTY line with the **access-class** command

***Secure R2 in a way that only 20.0.0.2 can telnet it beside it all other telnet session should be denied***

***R2>enable***

***R2#configure terminal***

***Enter configuration commands, one per line. End with CNTL/Z.***

***R2(config)#access-list 3 permit host 20.0.0.2***

***R2(config)#line vty 0 4***

***R2(config-line)#password vinita***

***R2(config-line)#login***

***R2(config-line)#access-class 3 in***

***To test do telnet from 20.0.0.2 first is should be successful.***

***PC>ipconfig***

***IP Address......................: 20.0.0.2***

***Subnet Mask.....................: 255.0.0.0***

***Default Gateway.................: 20.0.0.1***

***PC>telnet 50.0.0.2***

***Trying 50.0.0.2 ...***

***User Access Verification***

***Password:***

***R2>***

***Now telnet it from any other pc apart from 20.0.0.2. it must be filter and denied***

***PC>ipconfig***

***IP Address......................: 20.0.0.3***

***Subnet Mask.....................: 255.0.0.0***

***Default Gateway.................: 20.0.0.1***

***PC>telnet 50.0.0.2***

***Trying 50.0.0.2 ...***

***% Connection refused by remote host***

***PC>***