

(ICND1) 26(B). Named ACLs

(ICND2) 17(B). Named ACLs

ccnacoobook.com

Named access lists are an extension that makes ACLs easier to edit, remember, and use. They don't actually add any functionality. The differences between named and numbered ACLs include:

- Named ACLs are only used for IP access lists; their definition command begins with "ip."
- Since the choice of an ACL's number can't tell us whether a named ACL is standard or extended, that's specified in the command, too
- Named ACLs are defined using ACL subcommands.

Named ACLs are placed on an interface just like before; just use a name instead of a number.

NUMBERED ACL	NAMED ACL
<pre>R6(config)# access-list 44 permit host 192.168.3.22 R6(config)# access-list 44 permit 192.168.22.0 0.0.0.255</pre>	<pre>R6(config)# ip access-list standard MyACL R6(config-std-nacl)# permit host 192.168.3.22 R6(config-std-nacl)# permit 192.168.22.0 0.0.0.255 R6(config-std-nacl)# exit</pre>
<pre>R6(config)# interface gi0/0 R6(config-if)# ip access-group 44 in</pre>	<pre>R6(config)# interface gi0/0 R6(config-if)# ip access-group MyACL in</pre>
<pre>R6# show run begin access-list access-list 44 permit 192.168.3.22 access-list 44 permit 192.168.22.0 0.0.0.255</pre>	<pre>R6# show run begin access-list ip access-list standard MyACL permit 192.168.3.22 permit 192.168.22.0 0.0.0.255</pre>

Editing Named ACLs—thanks to the subcommand structure of named ACLs, you can remove one line of the access-list with the "no" command. If you tried that with a numbered ACL, Cisco would blow away the entire ACL! Cisco used to recommend that you edit ACLs in an external text file, then you would modify an ACL on a router by deleting the whole thing with a single "no" command and using copy/paste to replace it with the corrected version.

NUMBERED ACL	NAMED ACL
<pre>R6# show run begin access-list access-list 44 permit 192.168.3.22 access-list 44 permit 192.168.22.0 0.0.0.255</pre>	<pre>R6# show run begin access-list ip access-list standard MyACL permit 192.168.3.22 permit 192.168.22.0 0.0.0.255</pre>
<pre>R6(config)# no access-list 44 permit 192.168.3.22 R6(config)# do show run begin access-list</pre> <p><i>All of access list 44 is gone</i></p>	<pre>R6(config)# ip access-list standard MyACL R6(config-std-nacl)# no permit 192.168.3.22</pre> <pre>R6(config-std-nacl)# do show run begin MyACL ip access-list standard MyACL permit 192.168.22.0 0.0.0.255</pre> <p><i>Just the one line is missing</i></p>

ACL Line Numbering—Along with the configuration submode for named ACLs came the numbering of individual sub-command lines *within* the ACL. You can use that line numbering to delete specific lines or add new ones. This also applies to numbered ACLs; just use an ACL number rather than a name when entering the editing mode.

```
R6(config)# do sho access-lists MyACL
Standard IP access list MyACL
 10 permit 192.168.4.22
 20 permit 192.168.3.22
 30 permit 192.168.22.0, wildcard bits 0.0.0.255
R6(config)# ip access-list standard MyACL
R6(config-std-nacl)# no 10
R6(config-std-nacl)# 25 deny 192.168.22.0 0.0.0.15
R6(config-std-nacl)# do sho access-lists MyACL
Standard IP access list MyACL
 20 permit 192.168.3.22
 25 deny 192.168.22.0, wildcard bits 0.0.0.15
 30 permit 192.168.22.0, wildcard bits 0.0.0.255
```

Bonus: Editing Numbered ACLs Like Named ACLs—Even numbered ACLs benefit from the powerful editing features that were introduced with named ACLs. Simply pretend that the ACL number is a name.

```
R2# show run | begin access-list
access-list 44 permit 192.168.3.22
access-list 44 permit 192.168.22.0 0.0.0.255
!
...
R2(config)# ip access-list standard 44
R2(config-std-nacl)# no permit 192.168.3.22
R2(config-std-nacl)# do show run | begin access-list
access-list 44 permit 192.168.22.0 0.0.0.255
!
```