Rev. 20180926.151008

(ICND1) 26(A). Extended ACLs
(ICND2) 17(A). Extended ACLs

ccnacookbook.com

Extended ACL Syntax—choose one from each column. Ports follow the "eq" keyword and only make sense for TCP and UDP. You can also add "log" to the end, just like with standard ACLs. Unlike standard ACLs, extended ACLs require the "host" keyword if you're not using a wildcard.

Command	Number	Action	Kind	Source (IP, Wildcard, Port)	Dest.

`access-list`	`100-199`
	`2000-2699`
		`permit`
		`deny`
			`TCP`
			`UDP`
			`IP`
			`ICMP`
				`host 10.0.0.1`
				`10.0.0.0 0.0.0.255 eq 80`
				`host 10.0.0.1 eq telnet`
				`any`
					`(same)`

		`remark`		`say whatever you want`	

Matching—*All* parts of any *one* line of the ACL must match. This gives you the power of "and" (within each line) combined with "or" (between lines). You can match both TCP and UDP by using the keyword "IP"—you just can't use port numbers if you do. You can also compare port numbers for more than just equality ("eq"). See the table to the right for options.

OP	Meaning
eq, ne	equal, not equal
lt, gt	<, >
range	literally, "range x to y"

Common Ports—Some ports have a keyword, for example, for TCP 80, you could say "eq www."

TCP Port	UDP Port(s)	Application	ACL Keyword
20		FTP Data	`ftp-data`
21		FTP Control	`ftp`
22		SSH	
23		Telnet	`telnet`
25		SMTP (mail servers)	`smtp`
53	53	DNS	`domain`
	67	DHCP Server	`bootps` (dhcp uses bootp)
	68	DHCP Client (client calls from 68 to 67)	`bootpc`
	69	TFTP	`tftp`
80		HTTP (web)	`www`
110		POP (Post Office Protocol) version 3	`pop3`
	161	SNMP	`snmp`
443		SSL (often web)	
	514	Syslog	
	16,384 - 32,767	RTP (ip telephony & video)	

ICMP Matching—you can narrow ICMP matching based on the message type, in much the same way that you would narrow TCP and UDP matches based on their port number. You just won't use "eq" or any of it's siblings since the ICMP message type isn't expressed as a number. You also don't have to worry about separate source and destination message types (it's all one message).

```
R1# show ip access-list EDGE_IN | include icmp
    120 permit icmp any 203.0.113.168 0.0.0.7 echo (157 matches)
    130 permit icmp any any echo-reply
    140 permit icmp any any unreachable (469 matches)
    150 permit icmp any any time-exceeded
    160 permit icmp any any log
```

Matching Routing Protocol Updates—EIGRP and OSPF are their own protocols, just like ICMP.

Application	Protocol	Port	Destination Address
RIP v2	UDP	520	224.0.0.9
EIGRP	EIGRP		224.0.0.5 (hellos to all) and 224.0.0.6 (updates to DRs)
OSPF	OSPF		224.0.0.10

Placement—Extended ACLs should be placed near the source in order to save bandwidth downstream. This is the opposite of standard ACLs. Placement syntax is identical to standard ACLs, using the "ip access-group" or "ip access-class" command.