ACE Access Control Entry Example

R2(config)#

access-list 100 deny tcp 10.10.30.0 0.0.0.255 gt 49151 10.10.20.1 0.0.0.0 eq 23

			Source				Destination			
No.	Action	Protocol	IP	Wildcard	Qual.	Port	IP	Wildcard	Qual.	Port

Standard vs Extended ACLs

```
R1(config)#access-list ?
  <1-99>              IP standard access list
  <100-199>           IP extended access list
  <1300-1999>         IP standard access list (expanded range)
  <2000-2699>         IP extended access list (expanded range)
! truncated
```

Original Implementation: Standard vs Extended ACLs

- Standard ACLs reference the source address only
- Extended ACLs check based on the protocol, source address, destination address, and port number

- Standard ACL Range: 1 – 99
- Extended ACL Range: 100 - 199

ACL Improvement: Expanded Ranges

- Cisco expanded the original ACL Ranges
- Standard: 1-99, 1300-1999
- Extended: 100-199, 2000-2699

Standard Access List Example

```
R1(config)# access-list 1 deny 10.10.10.10 0.0.0.0
R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255
```

Standard Access List Example

- The default wildcard mask for a Standard ACL is 0.0.0.0, meaning an individual host address.

```
R1(config)# access-list 1 deny 10.10.10.10
```

- Do not forget to enter the wildcard when specifying an IP subnet

```
R1(config)# access-list 1 deny 10.10.10.0
```

Extended Access List Example

```
R1(config)# access-list 100 deny tcp 10.10.10.10 0.0.0.0
gt 49151 10.10.50.10 0.0.0.0 eq 23
R1(config)# access-list 100 permit tcp 10.10.10.0
0.0.0.255 gt 49151 10.10.50.10 0.0.0.0 eq telnet
```

Extended Access List Example

- There is no default wildcard mask for Extended ACLs

```
R1(config)#access-list 150 deny tcp 10.10.10.10 ge 1024 10.10.50.10 eq 23
                                                 ^
% Invalid input detected at '^' marker.
```

ACL Improvement: Named ACLs

- You can now reference ACLs by number or by a name
- Named ACLs begin with the command ‘ip access-list’ instead of ‘access-list’

```
R1(config)#ip access-list ?
  extended              Extended Access List
  standard              Standard Access List
! truncated
```

Named ACL Syntax

```
R1(config)#ip access-list standard Flackbox-Demo
R1(config-std-nacl)#deny 10.10.10.10 0.0.0.0
R1(config-std-nacl)#permit 10.10.10.0 0.0.0.255
```

Extended Access List Example

```
R1(config)# access-list 100 deny tcp 10.10.10.10 0.0.0.0
gt 49151 10.10.50.10 0.0.0.0 eq 23
R1(config)# access-list 100 permit tcp 10.10.10.0
0.0.0.255 gt 49151 10.10.50.10 0.0.0.0 eq telnet
```