ACL Action

```
R1(config)#access-list 100 ?
  deny      Specify packets to reject
  permit    Specify packets to forward
  remark    Access list entry comment
! Truncated
```

ACL Protocol

```
R1(config)#access-list 100 permit ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  ip       Any Internet Protocol
  ospf     OSPF routing protocol
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
! truncated
```

ACL Protocol

- Use TCP or UDP if you want the ACE to apply to traffic for a particular application between a source and destination address

```
R1(config)#access-list 100 deny tcp 10.10.10.0 0.0.0.255 10.10.50.0
0.0.0.255 eq 80
```

ACL Protocol

- Use IP if you want the ACE to apply to all traffic between a source and destination address

```
R1(config)#access-list 100 deny ip 10.10.10.0 0.0.0.255 10.10.50.0
0.0.0.255
```

ACL Source

```
R1(config)#access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

Wildcards

- Wildcards save you typing out the wildcard mask
- These examples mean the same thing:

```
R1(config)#access-list 100 permit tcp 10.10.10.10 0.0.0.0
R1(config)#access-list 100 permit tcp host 10.10.10.10

R1(config)#access-list 100 permit tcp 0.0.0.0 255.255.255.255
R1(config)#access-list 100 permit tcp any
```

Source Port Number

- Specifying the source port number is optional, it defaults to any port

```
R1(config)#access-list 100 permit tcp 10.10.10.0 0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

Destination Address

- The destination address uses the same format as the source address

```
R1(config)#access-list 100 permit tcp host 10.10.10.10 10.10.20.0
0.0.0.255
```

Final Options

- Additional options are available after entering the destination address such as destination port, TCP flags and logging.

```
R1(config)#access-list 100 permit tcp host 10.10.10.10 10.10.20.0 0.0.0.255 ?
  ack           Match on the ACK bit
  eq            Match only packets on a given port number
  established   Match established connections
  fin           Match on the FIN bit
  gt            Match only packets with a greater port number
  log           Log matches against this entry
  log-input     Log matches against this entry, including input interface
  lt            Match only packets with a lower port number
  neq           Match only packets not on a given port number
  range         Match only packets in the range of port numbers
  rst           Match on the RST bit
  syn           Match on the SYN bit
  urg           Match on the URG bit
```

Complete ACE Example

```
R1(config)#access-list 100 deny tcp host 10.10.10.10 10.10.20.0
0.0.0.255 eq www log
```

Verification – show access-lists

```
R2#sh access-lists 100
Extended IP access list 100
permit tcp host 10.10.30.10 host 10.10.20.1 eq telnet (13 match(es))
deny tcp 10.10.30.0 0.0.0.255 host 10.10.20.1 eq telnet (4 match(es))
```

- The ‘log’ keyword is not required to log hit counts. It is used to log to the console or an external monitoring server