Access Control Lists

- Access Control Lists were originally a security feature designed to control which traffic was allowed to transit a router
- ACLs now have multiple uses, such as specifying particular networks to apply QoS, NAT or VPN policies to
- They can be used to define IP networks to be filtered by a routing protocol
- Route filters can use named or numbered ACLs

IP Access-Group Command

- When configuring an ACL to secure traffic transiting a router, it must be applied to the interface with the ip access-group command.

```
ip access-list extended BLOCK_TELNET
 deny tcp any any eq telnet
 permit ip any any
!
interface GigabitEthernet0/0
 ip access-group BLOCK_TELNET in
```

ACL and Distribute List

- When configuring an ACL to filter routes in a routing protocol, it must be called via a Distribute List or Route Map
- Specifying an interface in a Distribute List is optional. It will be applied to all interfaces if one is not configured

```
ip access-list standard BLOCK_192.168.0.1/32
 deny 192.168.0.1 0.0.0.0
 permit any
!
router ospf 1
 distribute-list BLOCK_192.168.0.1/32 in Gig0/0
```

Route Filter Operation

- **Routes to be filtered** can be specified with an Access Control List or Prefix List
- ACLs and Prefix Lists can optionally be nested inside a Route Map
- The filter is **applied** with a Distribute List
- (Prefix Lists can be applied directly to neighbors in BGP)

```
R1(config-router)#distribute-list ?
  <1-199>       IP access list number
  <1300-2699>   IP expanded access list number
  WORD          Access-list name
  gateway       Filter based on gateway
  prefix        Filter prefixes in routing updates
  route-map     Filter prefixes based on route-map
```

Access Control List Types

- When configuring ACLs to secure which traffic is allowed to transit a router:
  - Standard ACLs permit or deny packets based on the source address only
  - Extended ACLs can specify the source and destination address
- You specify the subnet mask (via a wildcard mask). Default is /32 for Standard ACLs, you must specify for Extended ACLs

Standard ACLs for Route Filters – No Mask

- When a Standard ACL is used for route filtering:
- If no subnet mask is configured, it will match on the **exact prefix** and **any valid subnet mask** (does not allow you to specify particular subnet mask)
- For example:

```
access-list 1 deny 10.17.32.0
```

- Will filter a route to 10.17.32.0 with any subnet mask of /19 or greater
- 10.17.32.0 in binary is **00001010.00010001.001**00000.00000000
- Will match 10.17.32.0/24 and 10.17.32.0/28 etc
- It will not match 10.17.32.**1**/32

Standard ACLs for Route Filters – No Mask

- Full configuration:

```
access-list 1 deny 10.17.32.0
access-list 1 permit any
!
router ospf 1
 distribute-list 1 in Gig0/0
```

Standard ACLs for Route Filters – With Mask

- If a subnet mask is configured, it will match prefixes which match **the range**, with **any valid subnet mask** (does not allow you to specify particular subnet mask)
- For example:

```
access-list 1 deny 10.17.32.0 0.0.0.255
```

- Will match any 10.17.32.x route with any mask of /19 or greater
- It will match 10.17.32.0/24 and 10.17.32.0/28 etc
- It will also match 10.17.32.**1**/32
- And 10.17.32.0**/19**

Standard ACLs for Route Filters – With Mask

- Full configuration:

```
access-list 1 deny 10.17.32.0 0.0.0.255
access-list 1 permit any
!
router ospf 1
 distribute-list 1 in Gig0/0
```

Standard ACLs for Route Filters – No Mask

- When using an ACL with a Distribute List, a Standard ACL is the most simple option
- It is what you are most likely to see in the real world and on the test
- Extended ACLs can also be used but the command syntax can be confusing and have different meanings depending on where the Distribute List is applied – a Prefix List is usually a better option

Extended ACLs for IGP Route Filters

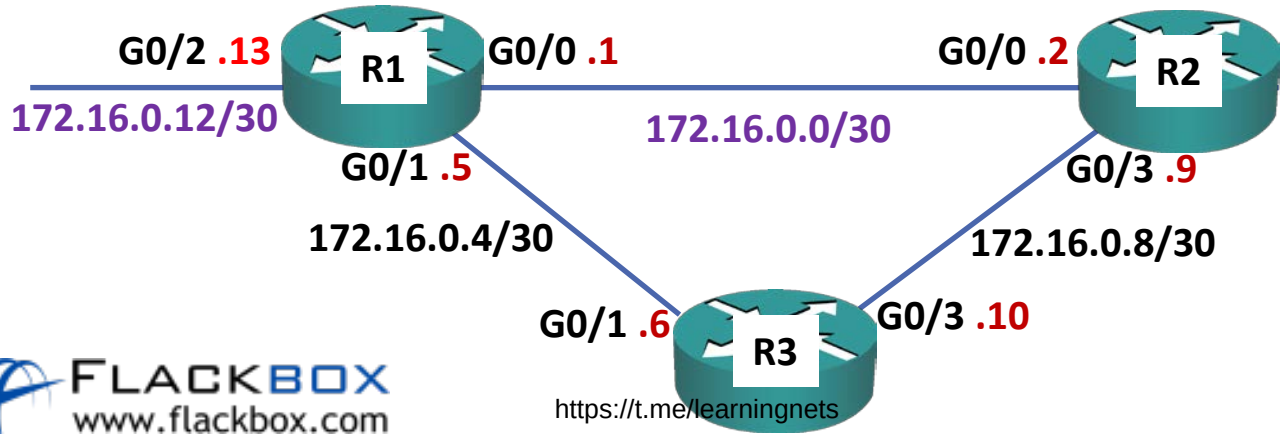
- If an extended ACL is used in a Distribute List applied to interfaces for an IGP protocol:
  - The source part of the ACL matches the neighbor's IP address that advertised a network
  - The destination part matches the advertised network (any specified subnet mask is ignored)
- If using a named extended ACL in EIGRP, the Distribute List must be configured before the ACL

Extended ACLs for IGP Route Filters – No Mask

- If no subnet mask is configured, it will match on the **exact prefix** and **any valid subnet mask** (does not allow you to specify particular subnet mask)
- This example will filter out the route to 172.16.0.0 (/30) **from R1**

```
R3(config)#router eigrp 100
R3(config-router)# distribute-list DEMO in

R3(config)#ip access-list extended DEMO
R3(config-ext-nacl)# deny ip host 172.16.0.5 host 172.16.0.0
R3(config-ext-nacl)# permit ip any any
```

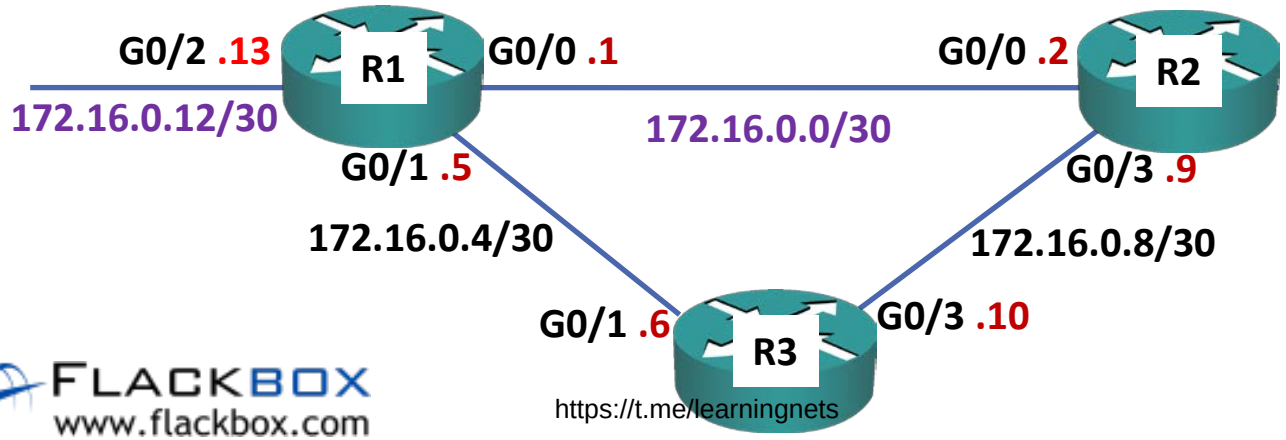


Extended ACLs for IGP Route Filters – With Mask

- If a subnet mask is configured, it will match prefixes which match **the range**, with **any valid subnet mask** (does not allow you to specify particular subnet mask)
- This example will filter out the routes to all 172.16.x.x/x networks **from R1**

```
R3(config)#router eigrp 100
R3(config-router)# distribute-list DEMO in

R3(config)#ip access-list extended DEMO
R3(config-ext-nacl)# deny ip host 172.16.0.5 172.16.0.0 0.0.255.255
R3(config-ext-nacl)# permit ip any any
```



Extended ACLs for BGP Route Filters – Example 1

- If an extended ACL is used in a distribute list for the BGP protocol, then the source part of the ACL identifies the network address, and the destination part specifies the subnet mask (allowing you to specify a particular subnet mask)
- This example will filter out the route to 203.0.113.0/24 to neighbor 198.51.100.1

```
ip access-list extended DEMO
 deny ip host 203.0.113.0 host 255.255.255.0
 permit ip any any

router bgp 65012
 neighbor 198.51.100.1 distribute-list DEMO out
```

Extended ACLs for BGP Route Filters – Example 2

- This example will filter out the route to any 203.0.x.x networks with exactly a /24 subnet mask to neighbor 198.51.100.1

```
ip access-list extended DEMO
 deny ip 203.0.0.0 0.0.255.255 host 255.255.255.0
 permit ip any any

router bgp 65012
 neighbor 198.51.100.1 distribute-list DEMO out
```

Extended ACLs in Route Maps & Redistribution

- If an extended ACL is used in a Route Map or redistribution, then the source part of the ACL identifies the network address, and the destination part specifies the subnet mask (allowing you to specify a particular subnet mask)