Slide 1

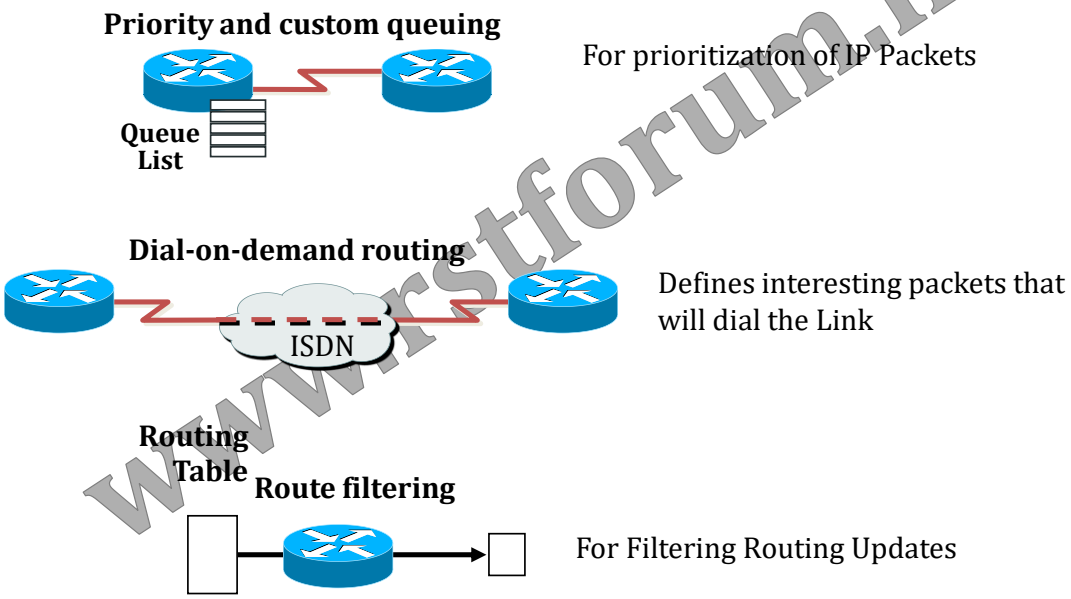

Routing
Switching
Tigers
Forum
Access-List
www.rstforum.net

Why use access-list ?

- Access-list Manage IP traffic as network access grows
- Access-list Filter data packets as they enter/exit router port
- Access-list filters packets on basis of layer 3 and above info.
- Access-list filters data packets only.

Slide 3

Other types of policies



Types of access-list

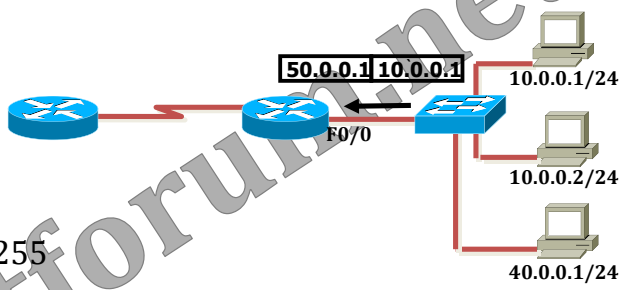
- Standard access-list
  - Filters packets on basis of source address
- Extended access-list
  - Filters packets on basis of
    - Source address and Destination address
    - Protocol(TCP/UDP/ICMP, etc.)
    - Port numbers (FTP-21/20, Telnet- 23, http-80, etc.)

Example

Standard Access-list

int fastethernet 0/0
ip access-group 1 in

access-list 1 deny 10.0.0.0 0.0.0.255



Extended Access-list

int fastethernet 0/0
ip access-group 101 in

access-list 101 deny tcp 10.0.0.0 0.0.0.255 50.0.0.0 0.0.0.255 eq 23

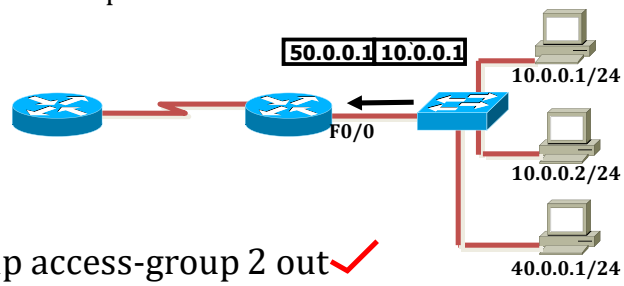
Slide 6

Rules Of Access-list

1. In Numbered Access-list numbers Indicates following
   - Which protocol is filtered (IP/IPX/AT)
   - Whether standard or Extended

Access List Type		Number Range/Identifier
IP	Standard	1-99
	Extended	100-199

2. Only 1 access-group on an interface for a protocol in a direction whether standard or extended.

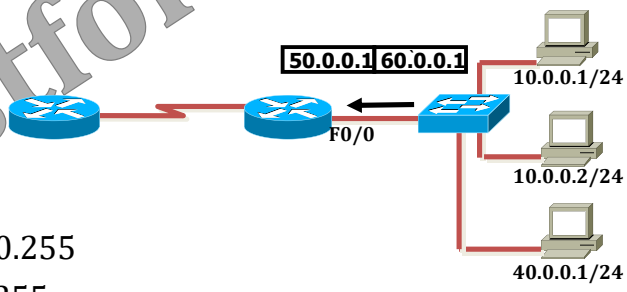


int fastethernet 0/0
ip access-group 1 in
ip access-group 2 in x
ip access-group 101 in x
ip access-group 1 out or ip access-group 2 out ✓

Rules Of Access-list

3. We can write multiple policies in a group but policies will be matched in top to bottom manner,

   Once a packet matches a policy it will do as directed by policy , no further of matching policies required

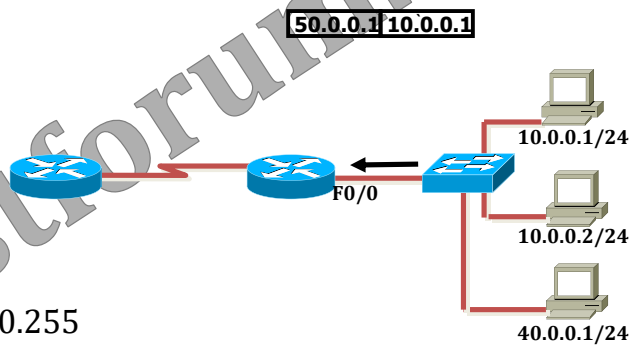


int fastethernet 0/0
ip access-group 1 in

access-list 1 permit 10.0.0.0 0.0.0.255
access-list 1 deny 20.0.0.0 0.0.0.255
access-list 1 permit 60.0.0.0 0.0.3.255
access-list 1 deny 10.0.0.1 0.0.0.0

Rules Of Access-list

4. Because Policies are matched in Top-To-Bottom manner hence most restrictive policy should come on top of list and broader policy should be at the bottom of list

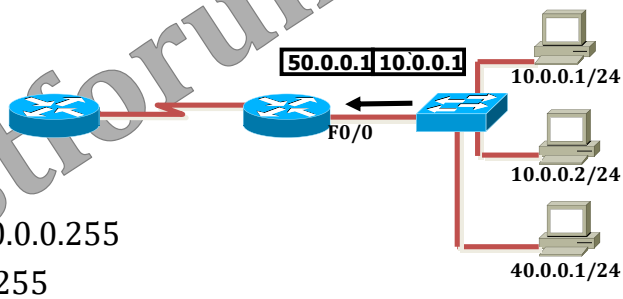


int fastethernet 0/0
ip access-group 1 in

access-list 1 permit 10.0.0.0 0.0.0.255
access-list 1 deny 20.0.0.0 0.0.0.255
access-list 1 permit 60.0.0.0 0.0.3.255
access-list 1 deny 10.0.0.1 0.0.0.0 or (access-list 1 deny host 10.0.0.1)

Rules Of Access-list

5. Selective removal and insertion of policies not allowed in numbered access-list



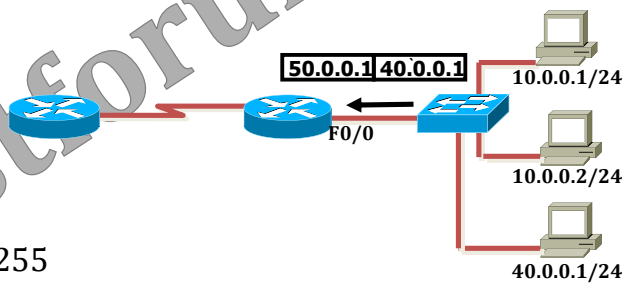
int fastethernet 0/0
ip access-group 1 in

no access-list 1 permit 10.0.0.0 0.0.0.255
access-list 1 deny 20.0.0.0 0.0.0.255
access-list 1 permit 60.0.0.0 0.0.3.255
access-list 1 deny 10.0.0.1 0.0.0.0

enable secret cisco
no enable secret

Rules Of Access-list

6. If Packet does not match any of the defined policies then last policy of every group is implicit deny, packets will get denied



int fastethernet 0/0
ip access-group 1 in

access-list 1 deny 10.0.0.0 0.0.0.255
access-list 1 deny 20.0.0.0 0.0.0.255
access-list 1 deny 60.0.0.0 0.0.3.255
access-list 1 deny 10.0.0.1 0.0.0.0

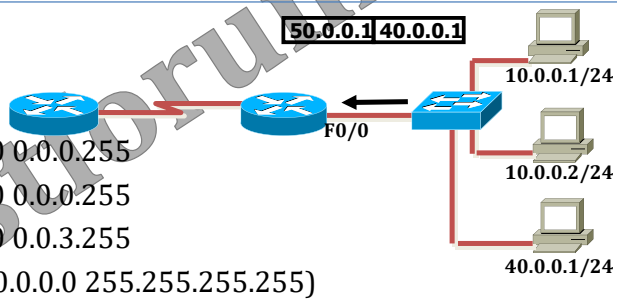
Slide 11

7. If all policies in a group are deny then last policy in the group should be permit any
   - Standard access-list: access-list 1 permit any
   - Extended access-list: access-list 101 permit ip any any

Standard Access-List

```
int fastethernet 0/0
ip access-group 1 in

access-list 1 deny 10.0.0.0 0.0.0.255
access-list 1 deny 20.0.0.0 0.0.0.255
access-list 1 deny 60.0.0.0 0.0.3.255
access-list 1 permit any (0.0.0.0 255.255.255.255)
```



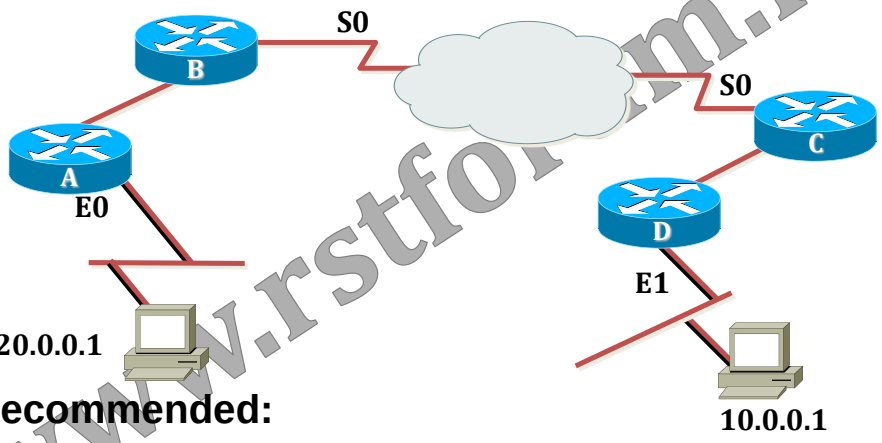
Extended Access-List

```
int fastethernet 0/0
ip access-group 101 in

access-list 101 deny tcp 10.0.0.0 0.0.0.255 30.0.0.0 0.0.0.255 eq 23
access-list 101 permit ip any any
```

Slide 12

Where to Place IP Access Lists



Recommended:

- Place extended access lists close to the source
- Place standard access lists close to the destination

Virtual Terminal Access Example

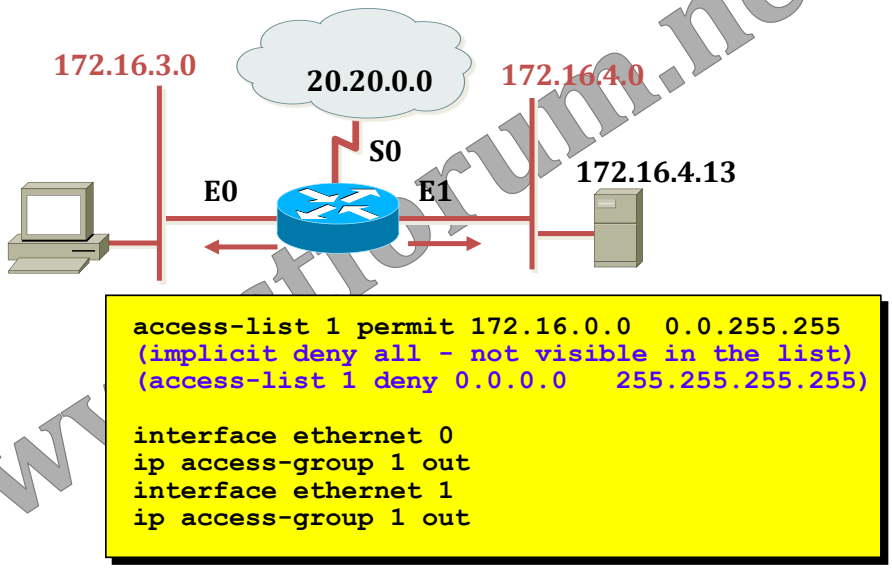
Controlling Inbound VTY Access

```
access-list 12 permit 192.89.55.0 0.0.0.255
!
line vty 0 4
 access-class 12 in
```

- **Permits only hosts in network 192.89.55.0 to connect to the router's vtys**

Slide 14

Standard IP Access List -Example 1



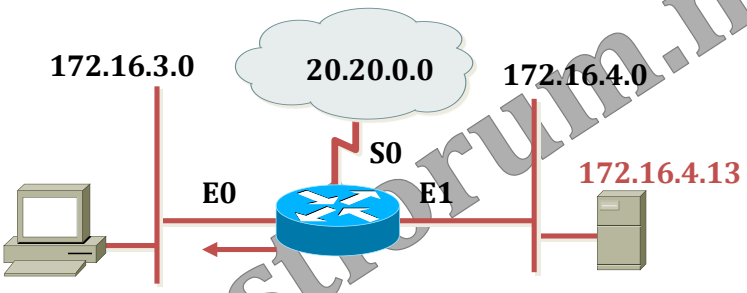

```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

- **Permit my network only**

Slide 15

Standard IP Access List -Example 2

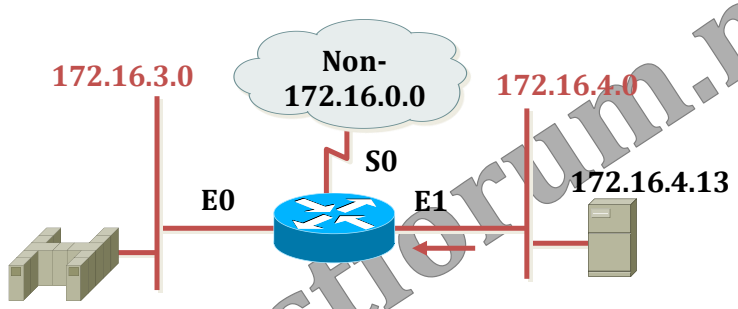


- **Deny a specific host**

```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255

interface ethernet 0
ip access-group 1 out
```

Extended IP Access List -Example 3

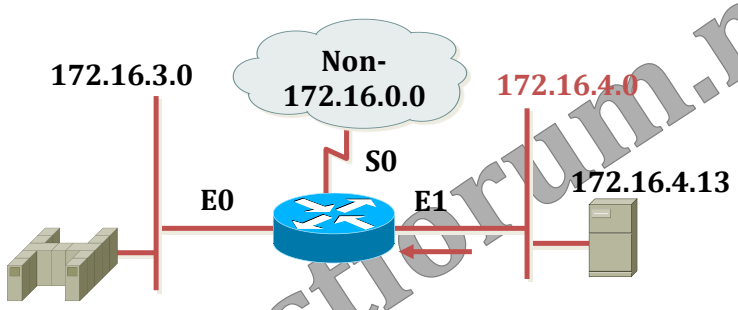


- Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 inside of E1
- Permit all other traffic

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any


interface ethernet 1
ip access-group 101 in
```

Extended IP Access List -Example 4



Deny Telnet from hosts in network 172.16.4.0/24 going out to any other host in any other network

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
access-list 101 permit ip any any

interface ethernet 1
ip access-group 101 in
```

Using Named IP Access Lists

NUMBERED ACCESS- LIST

Router(config)# access-list 1 permit 10.0.0.0 0.0.0.255

Router(config)# access-list 1 permit 20.0.0.0 0.0.0.255

Router(config)# Interface fastethernet 0/0

Router(config-if)# ip access-group 1 in

NAMED ACCESS- LIST

Router(config)# ip access-list standard abc

Router(config std-nacl)# permit 10.0.0.0 0.0.0.255

Router(config std-nacl)# permit 20.0.0.0 0.0.0.255

Router(config)# Interface fastethernet 0/0

Router(config-if)# ip access-group abc in