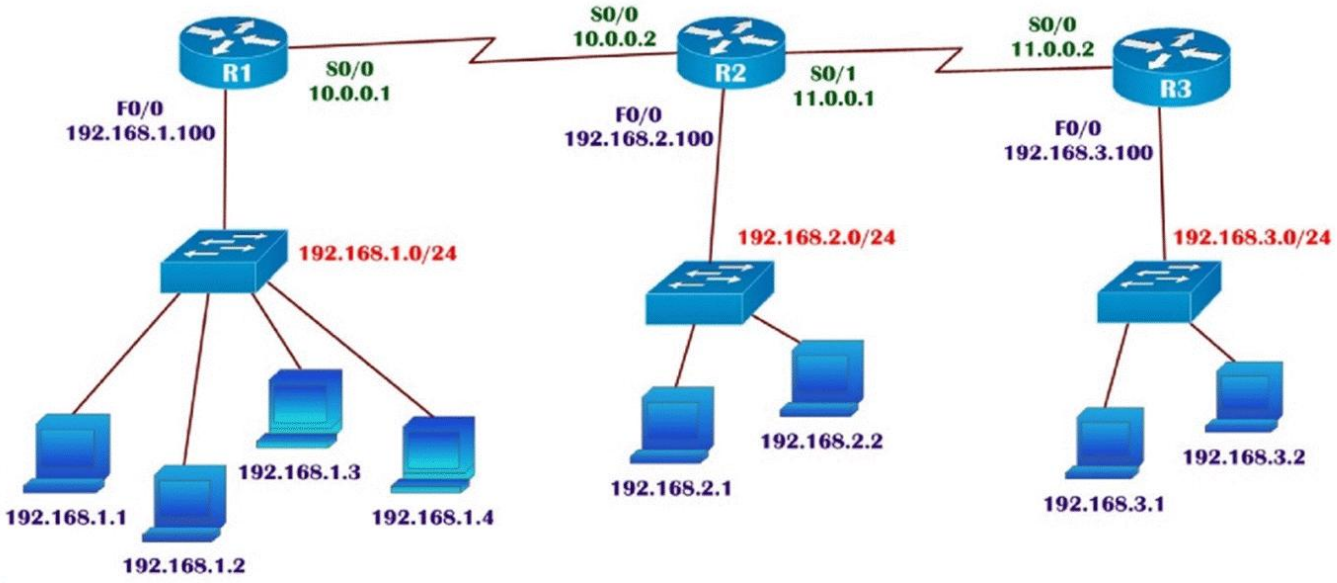
ACCESS CONTROL LIST (ACL)

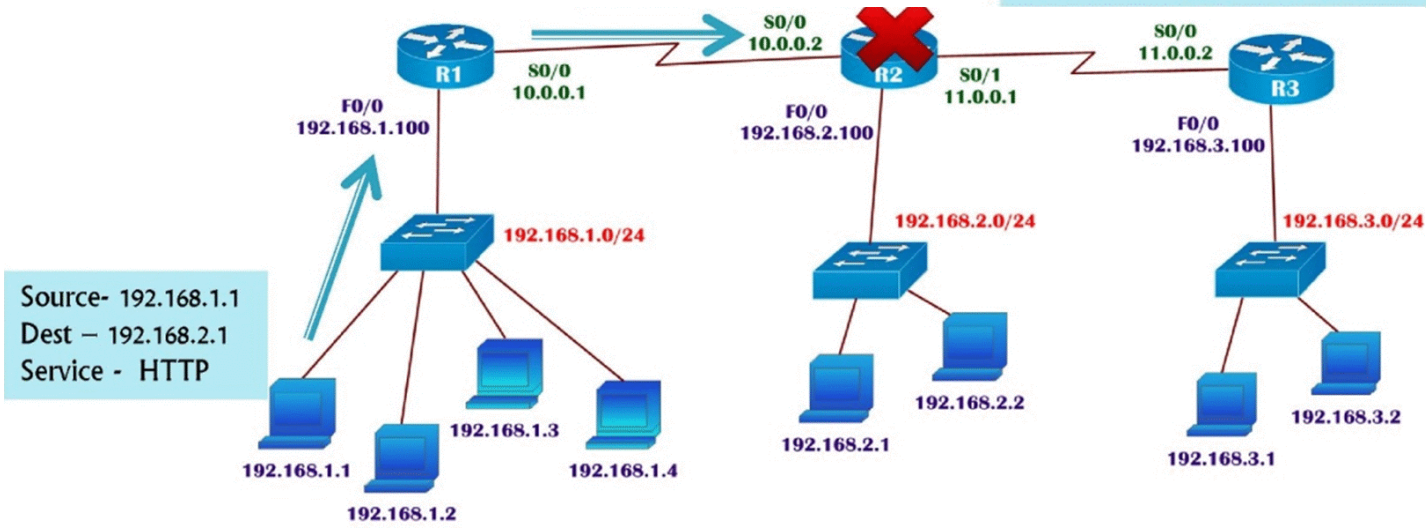
- ACL is a set of rules which will allow or deny the specific traffic moving through the router
- controls the flow of traffic from one network to other via router



Set of Rules - ACL

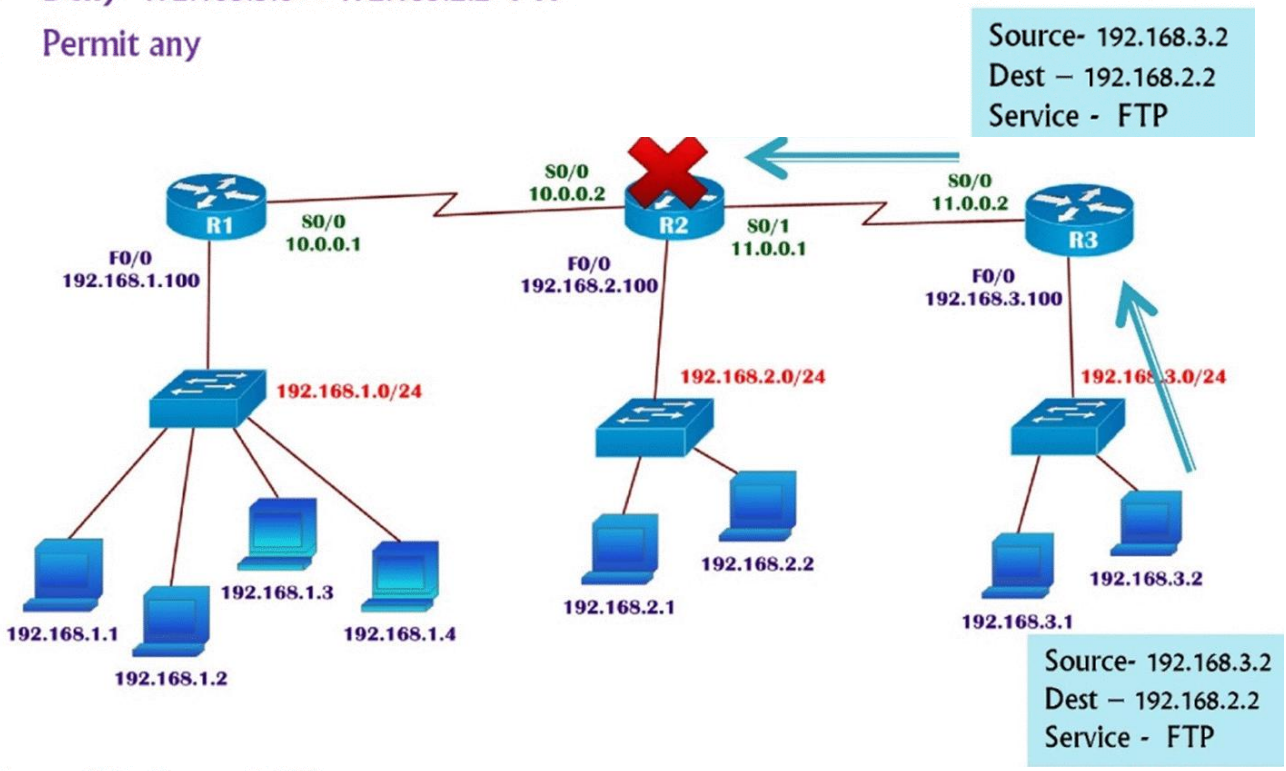
1. Deny 192.168.1.0 = 192.168.2.1 HTTP
2. Deny 192.168.3.0 = 192.168.2.2 FTP
3. Permit any

Source- 192.168.1.1
Dest – 192.168.2.1
Service - HTTP



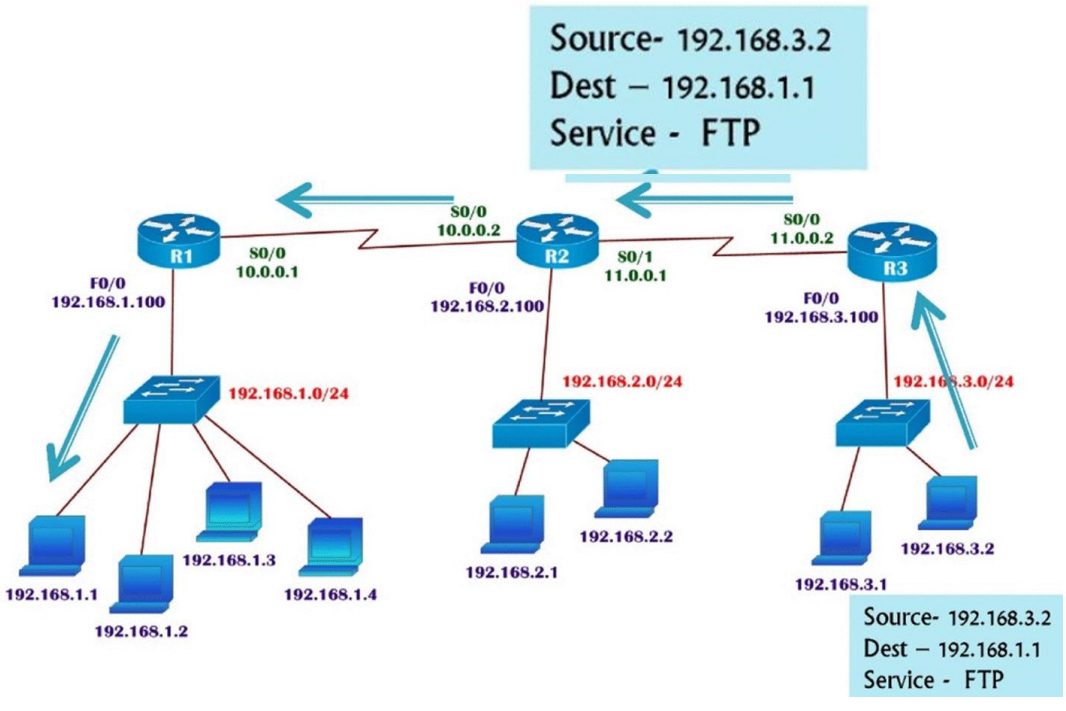
Set of Rules - ACL

1. Deny 192.168.1.0 = 192.168.2.1 HTTP
2. Deny 192.168.3.0 = 192.168.2.2 FTP
3. Permit any



Set of Rules - ACL

1. Deny 192.168.1.0 = 192.168.2.1 HTTP
2. Deny 192.168.3.0 = 192.168.2.2 FTP
3. Permit any



Types of Access-list

Named ACL - set of rules Identified by a name.

1. Deny 192.168.1.0 = 192.168.2.1 HTTP
2. Deny 192.168.3.0 = 192.168.2.2 FTP
3. Permit any

ACL - 120

Named ACL - set of rules rules Identified by a name.

1. Deny 192.168.1.0 = 192.168.2.1 HTTP
2. Deny 192.168.3.0 = 192.168.2.2 FTP
3. Permit any

ACL – CCNA

Standard ACL

1. Can be named or numbered.
2. The access-list number range is 1 – 99 (or 1300 – 1699)
3. Can block a Network, Host and Subnet. (not selected services)
4. All services are blocked.
5. Filtering is done based on only source IP address

Extended ACL

1. Can be named or numbered.
2. The access-list number range is 100 – 199 (or 2000-2699)
3. We can allow or deny a Network, Host, Subnet and Service
4. Selected services can be blocked.
5. Filtering is done based on source IP , destination IP , protocol, port no

Wild card mask

Tells the router which portion of the bits to match or ignore.

0 = must match

1 = ignore

Global Subnet Mask	255. 255. 255. 255	255. 255. 255. 255
- Subnet Mask	255. 255. 255. 0	255. 255. 255. 240
==========	==========	==========
Wildcard mask	0. 0. 0 . 255	0. 0. 0 . 15
==========	==========	==========

- Wild Card Mask for Network will be Inverse mask.(above method)

Wild card mask for single host

Default mask for one single host always = /32 = 255.255.255.255

Global Subnet Mask	255. 255. 255. 255
- Subnet Mask	255. 255. 255. 255
==========	==========
Wildcard mask	0. 0. 0 . 0
==========	==========

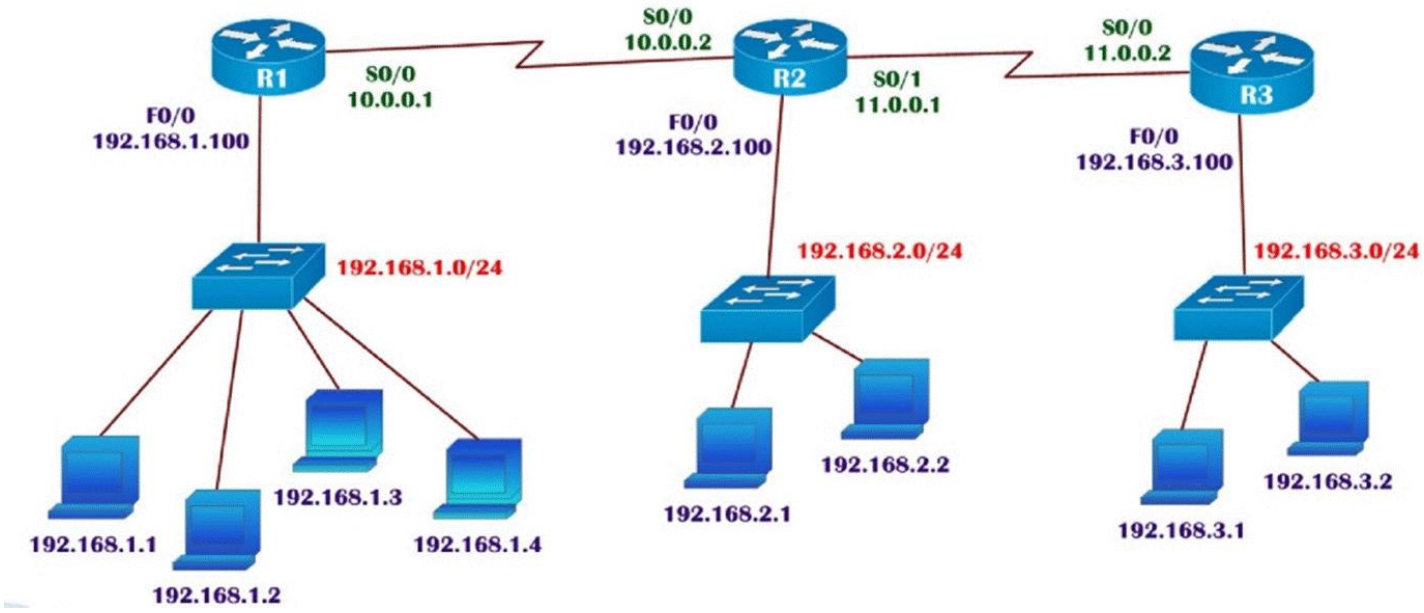
- Wild Card Mask for a Host will be always **0.0.0.0**

Lab : Standard Access-list

TASK: Configure the Appropriate router as per the rules given

1. Deny the host **192.168.1.1** communicating with **192.168.2.0**
2. Deny the host **192.168.1.2** communicating with **192.168.2.0**
3. Deny the network **192.168.3.0** communicating with **192.168.2.0**
4. Permit all the remaining traffic

NOTE: the Above ACL rules should not affect the other communication



Router(config)# **access-list** <acl no> <permit/deny> <source address> <source WCM>

```
R-2(config)# access-list 15 deny 192.168.1.1 0.0.0.0
R-2(config)#access-list 15 deny host 192.168.1.2
R-2(config)#access-list 15 deny 192.168.3.0 0.0.0.255
R-2(config)#access-list 15 permit any
```

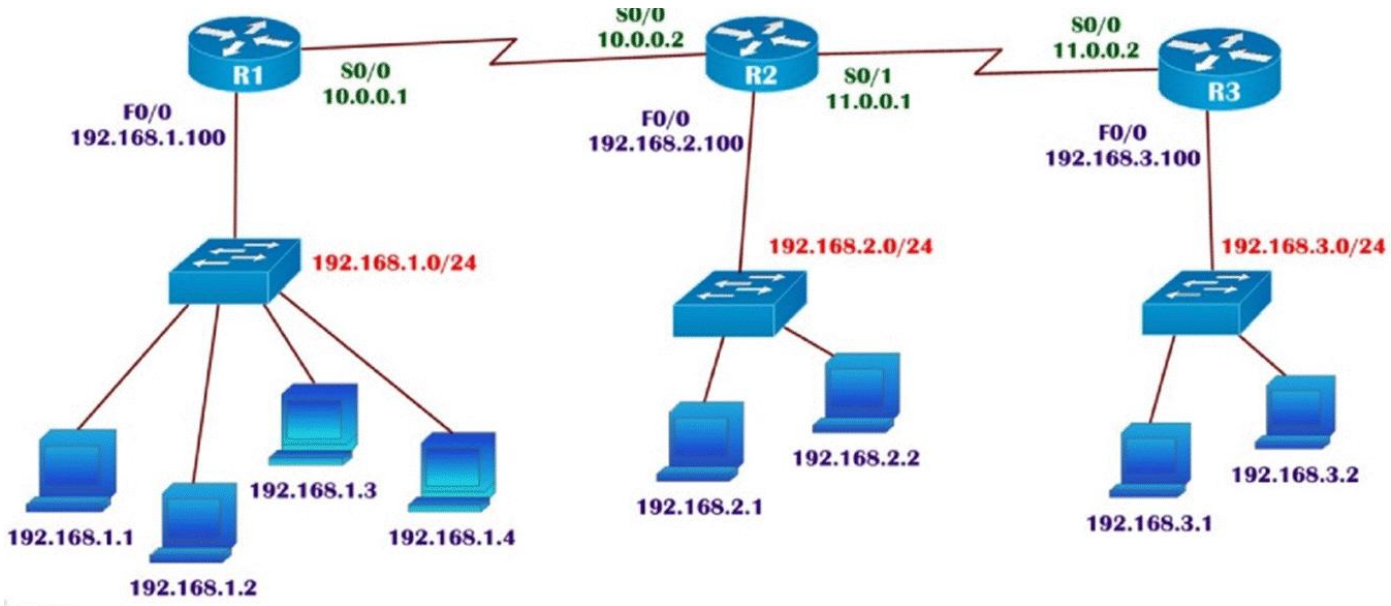
	Source	Destination
1)	Deny - 192.168.1.1	- 192.168.2.0
2)	Deny - 192.168.1.2	- 192.168.2.0
3)	Deny - 192.168.3.0	- 192.168.2.0
4)	Permit any	

Extended Access-list

TASK: **Configure the Appropriate router as per the rules given below**

1. Deny the users on LAN 192.168.2.0 should not access 192.168.1.3 HTTP service
2. Deny the users on LAN 192.168.3.0 should not access 192.168.1.4 FTP service
3. Deny the users on LAN 192.168.3.1 should not access 192.168.1.3 HTTP service
4. Deny the users on LAN 192.168.2.0 should not get DNS service from DNS server 192.168.1.4
5. Deny the users from the host between 192.168.3.2 and 192.168.1.2 should not be able to send ICMP (ping /trace) messages
6. Remaining hosts and services should be permitted

NOTE: the Above ACL rules should not affect the other communication



R-1(config)#**access-list 145 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.3 eq www**

R-1(config)#**access-list 145 deny tcp 192.168.3.0 0.0.0.255 host 192.168.1.4 eq ftp**

R-1(config)#**access-list 145 deny tcp host 192.168.3.1 host 192.168.1.3 eq www**

R-1(config)#**access-list 145 deny udp 192.168.2.0 0.0.0.255 host 192.168.1.4 eq domain**

R-1(config)#**access-list 145 deny icmp host 192.168.3.2 host 192.168.1.2 echo**

R-1(config)#**access-list 145 deny icmp host 192.168.3.2 host 192.168.1.2 echo-reply**

R-1(config)#**access-list 145 permit ip any any**