ACL (Access Control List):

o   ACL stands for Access Control List, also called Access List.

o   ACLs are always processed from top to down in sequential order.

o   A packet is compared with ACL conditions until it finds a match.

o   Once a match is found for packet, no further comparison will be done.

o   Interface will take action based on match condition.

o   There are two possible actions permit and deny in Access Control List.

o   If permit condition match, packet will be allowed to pass from interface.

o   If deny condition match, packet will be destroyed immediately.

o   Every Access Control List (ACL) has a default deny statement at end of it.

o   If a packet does not meet with any condition, it will be destroyed by default deny.

o   Empty Access Control List (ACL) will permit all traffic by default.

o   Implicit deny condition will not work with empty Access Control List (ACL).

o   Implicit deny condition work only if ACL has at least one user defined condition.

o   Access Control List (ACL) can filter only the traffic passing from interface.

o   It cannot filter the traffic originated from router on which it has been applied.

o   Standard Access Control List (ACL) can filter only the source IP address.

o   Standard Access Control List should be placed near the destination devices.

o   Extended Access Control List (ACL) should be placed near the source devices.

o   Each Access Control List (ACL) needs or require a unique number or name.

o   Only one ACL applied to an interface in each direction inbound and outbound.

o   Only have a single ACL per direction, it is impossible to have 2 inbound access lists.

o   ACL work on the network (Layer 3) and the transport (Layer 4) layer.

o   First, create an Access-List globally and then assign it to an interface.

o   Use for security, deny or permit access, filter traffic, accept or reject, allow or deny.

Advantages of ACL:

o   Access Control List Limits network traffic to increase network performance.

o   ACLs provide traffic flow control by restricting the delivery of routing updates.

o   ACLs controls, which type of traffic, are forwarded or blocked by the router.

o   ACLs helps to increase data security and confidentiality in an organization.

o   ACLs monitor unauthorized access to important files Access rights.

Types of Access List:

There are many types of Access Control List (ACLs) but mainly two.

Standard ACLs:

o   Standard ACLs filter the packet based on its source IP address.
o   Standard ACLs should be placed as close to destination devices as possible.
o   Number of Standard Access Control List (ACL) is start from 1 and end 99.
o   Standard Access Control List (ACL) is Old type of Access Control List (ACL).
o   Standard Access Control List (ACLs) are mainly used for normal filtering.

Extended ACLs:

o   Extended IP ACLs check both the source & destination, ports, & protocols.
o   Extended ACLs should be placed as close to the source devices as possible.
o   Number of Extended Access Control List (ACL) is start from 100 end 199.
o   Extended Access Control List is more powerful than standard Access List.
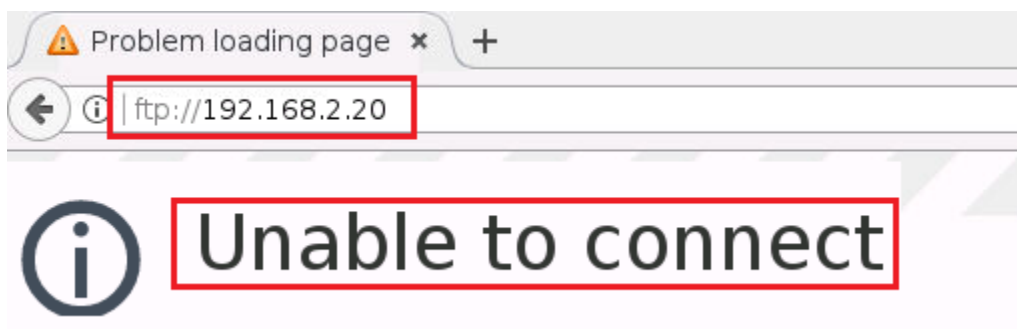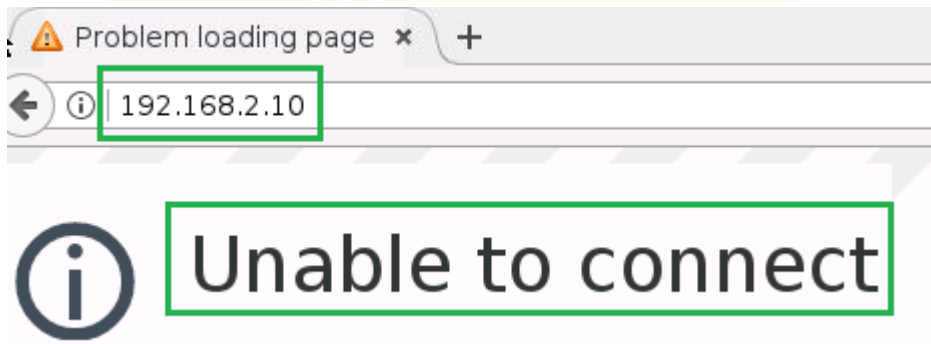
Time-Based ACL:

o   Time-based ACLs that allow for network access based on time or day.
o   Time-based ACLs are only active during a specified time range.
o   For TACL set the time range to be either periodic or absolute.
o   Configure time-based ACL, specify time range & then apply ACL.
o   To verify, run show access-lists and check if the ACL is active.
o   If it is in the time range and the ACL is filtering traffic.
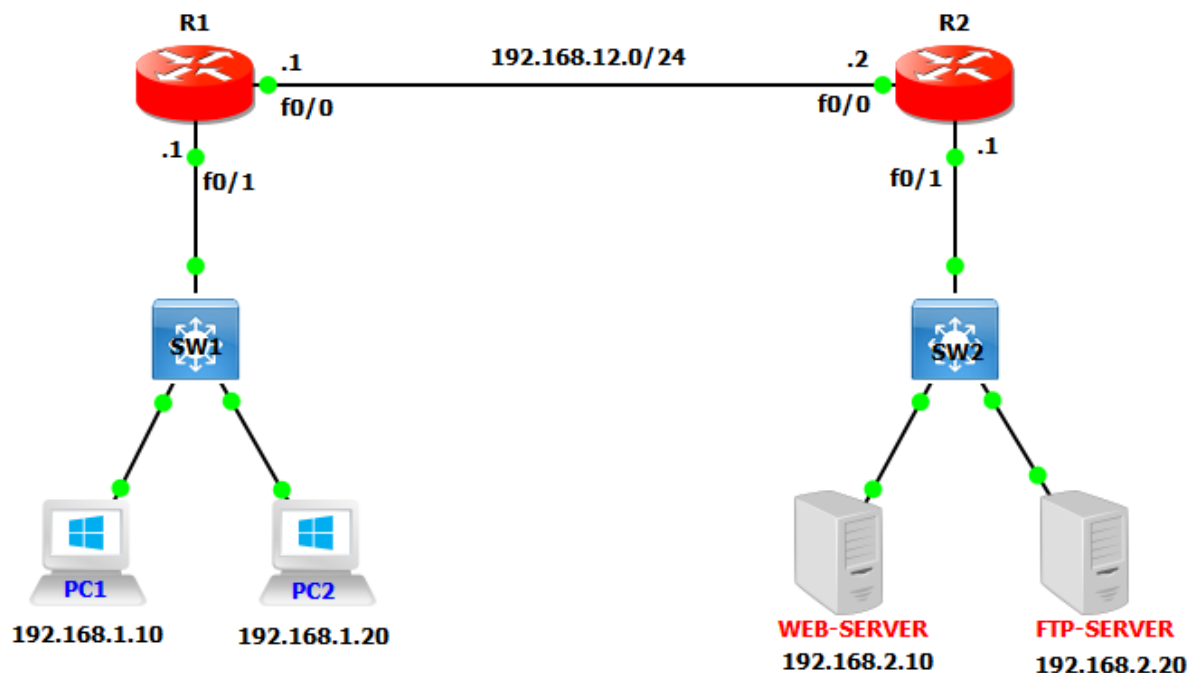
R1 Configuration	
R1(config)#interface f0/0 R1(config-if)#ip add 192.168.12.1 255.255.255.0 R1(config-if)#no shutdown	R1(config)#int f0/1 R1(config-if)#ip add 192.168.1.1 255.255.255.0 R1(config-if)#no shutdown
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2	
R2 Configuration	
R2(config)#interface f0/0 R2(config-if)#ip add 192.168.12.2 255.255.255.0 R2(config-if)#no shutdown	R2(config)#inter f0/1 R2(config-if)#ip add 192.168.2.1 255.255.255.0 R2(config-if)#no shutdown
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.1	

Standard ACL on R2 to deny PC1
R2(config)#access-list 1 deny host 192.168.1.10
R2(config)#access-list 1 permit any
R2(config-if)#ip access-group 1 out

```
R2#show access-lists
Standard IP access list 1
    10 deny    192.168.1.10 (18 matches)
    20 permit any
```

Problem loading page × +

← ⓘ 192.168.2.10

ⓘ Unable to connect

Problem loading page × +

← ⓘ ftp://192.168.2.20

ⓘ Unable to connect

← ⓘ | 192.168.2.10

Welcome to nginx!

If you see this page, the nginx web server is successfully working. Further configuration is required.

← ⓘ ✎ | ftp://192.168.2.20

Index of ftp://192.168.2.20/

☖ Up to higher level directory

Standard ACL on R2 to deny Whole Network
R2(config)#access-list 11 deny 192.168.1.0 0.0.0.255
R2(config)#access-list 11 permit any
R2(config-if)#ip access-group 11 out

```
Standard IP access list 11
    10 deny    192.168.1.0, wildcard bits 0.0.0.255 (34 matches)
    20 permit any
```

```
root@PC1:~# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10): 56 data bytes
36 bytes from 192.168.12.2: Packet Filtered
36 bytes from 192.168.12.2: Packet Filtered
36 bytes from 192.168.12.2: Packet Filtered
^C--- 192.168.2.10 ping statistics ---
root@PC2:~# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10): 56 data bytes
36 bytes from 192.168.12.2: Packet Filtered
36 bytes from 192.168.12.2: Packet Filtered
36 bytes from 192.168.12.2: Packet Filtered
^C--- 192.168.2.10 ping statistics ---
```
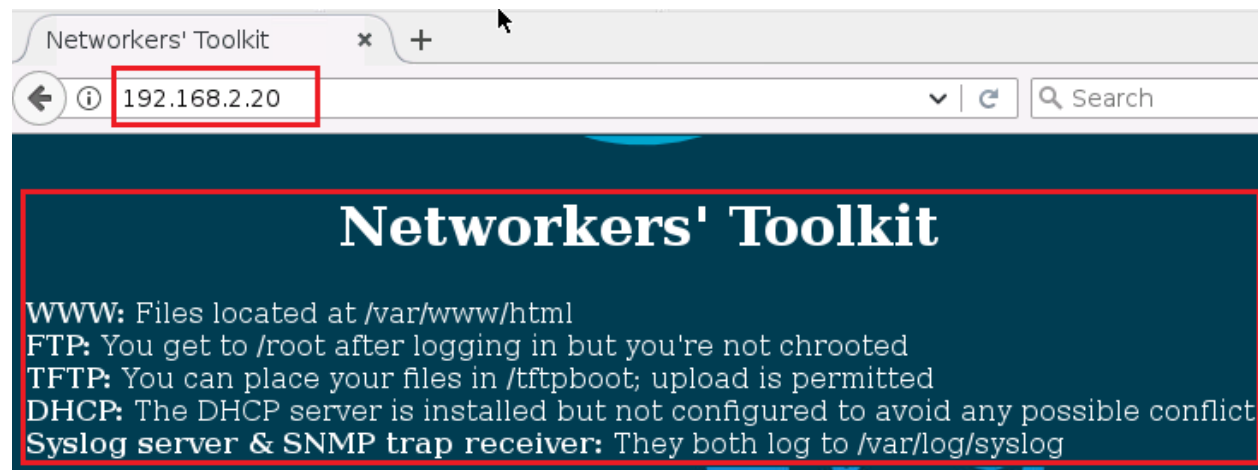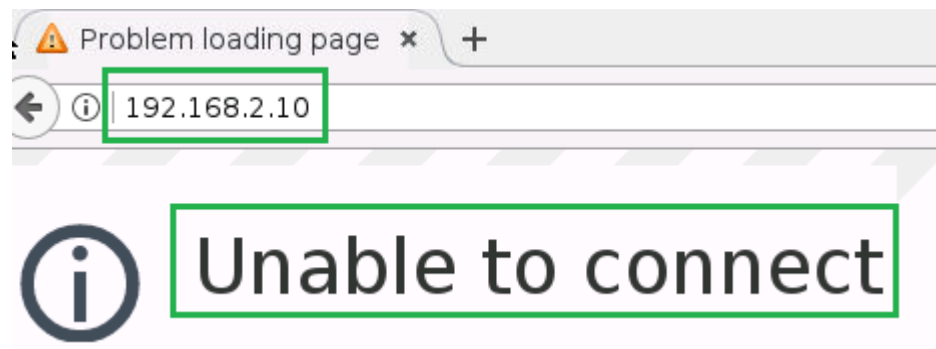
Extended ACL on R1 to Deny PC1 to Web-Server only HTTP
R1(config)#access-list 100 deny tcp host 192.168.1.10 host 192.168.2.10 eq 80
R1(config)#access-list 100 permit ip any any
R1(config)#interface f0/1   R1(config-if)#ip access-group 100 in

```
R1#show access-lists
Extended IP access list 100
    10 deny tcp host 192.168.1.10 host 192.168.2.10 eq www (3 matches)
    20 permit ip any any (42 matches)
```

⚠ Problem loading page ×   +

← ⓘ | 192.168.2.10

ⓘ **Unable to connect**

Networkers' Toolkit   ×   +

← ⓘ | 192.168.2.20   ∨ | ↻ | 🔍 Search

Networkers' Toolkit

WWW: Files located at /var/www/html
FTP: You get to /root after logging in but you're not chrooted
TFTP: You can place your files in /tftpboot; upload is permitted
DHCP: The DHCP server is installed but not configured to avoid any possible conflict
Syslog server & SNMP trap receiver: They both log to /var/log/syslog

```
root@PC1:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
64 bytes from 192.168.1.10: icmp_seq=0 ttl=64 time=0.066 ms
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.046 ms
```

Time ACL Configuration on R1
R1(config)# time-range TEST-TIME R1(config-time-range)# periodic weekdays 12:00 to 23:00 R1(config-time-range)# exit
R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any time-range TEST-TIME R1(config)# access-list 100 deny ip any any
R1(config)# interface FastEthernet 0/1 R1(config-if)# ip access-group 100 in

Infrastructure ACL (iACLs):

o   Using Infrastructure iACLs is a technique that was developed by ISPs.

o   It is now a common practice by enterprises and other organizations.

o   IACLs involves use of ACLs that prevent direct attacks to infrastructure devices.

o   Configure these ACLs to specifically allow only authorized traffic to infrastructure.

Infrastructure ACL
R1(config)#!--CMP Packet Filtering R1(config)#ip access-list extended INF R1(config-ext-nacl)#permit icmp any any echo-reply R1(config-ext-nacl)#permit icmp any any unreachable R1(config-ext-nacl)#permit icmp any any time-exceeded R1(config-ext-nacl)#deny icmp any any
R1(config-ext-nacl)#!--Deny Special-Use Address Sources R1(config-ext-nacl)#deny ip host 0.0.0.0 any R1(config-ext-nacl)#deny ip 127.0.0.0 0.255.255.255 any R1(config-ext-nacl)#deny ip 192.0.2.0 0.0.0.255 any R1(config-ext-nacl)#deny ip 224.0.0.0 15.255.255.255 any
R1(config-ext-nacl)#!--Filter Private Space. R1(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 any R1(config-ext-nacl)#deny ip 172.16.0.0 0.15.255.255 any R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255 any
R1(config-ext-nacl)#!--Deny Access to Internal infrastructure Addresses. R1(config-ext-nacl)#deny ip any 192.168.122.0 0.0.0.255
R1(config-ext-nacl)#!--Permit Transit Traffic. R1(config-ext-nacl)#permit ip any any