

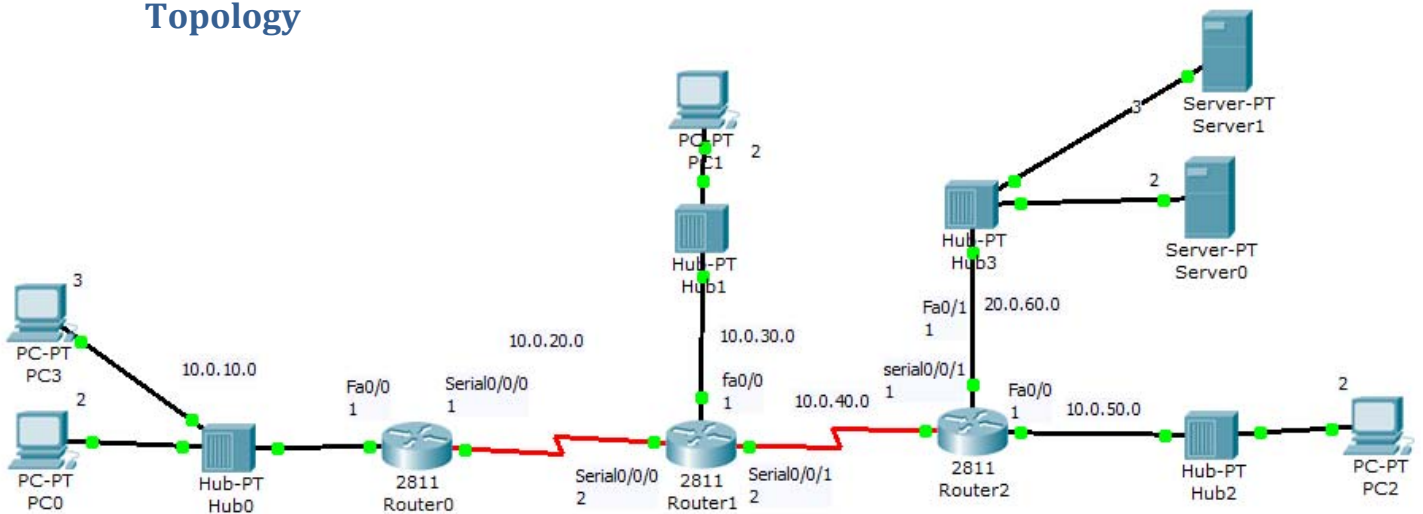
Wireless Lab 05

IP/TCP Layers Network Security III

Equipment

#	Item
4	PCs
4	Hubs
4	Router 2811
2	Server

Topology



3. Extended Access list - the whole story

Part 1:

Reboot before configuring router 2

10.0.10.0	10.0.30.0	10.0.50.0
Can ping 20.0.60.0	Can't ping 20.0.60.0	Can ping 20.0.60.0
Can't telnet 3.3.3.3	Can telnet 3.3.3.3	Can telnet 3.3.3.3
Can web browse 20.0.60.2	Can't web browse 20.0.60.2	Can web browse 20.0.60.2

```

R1>en
R1>config t
R1>access-list 198 deny icmp 10.0.30.0 0.0.0.255 20.0.60.0 0.0.0.255 echo
R1>access-list 198 permit icmp any 20.0.60.0 0.0.0.255 echo
R1>access-list 198 deny tcp 10.0.10.0 0.0.0.255 host 3.3.3.3 eq telnet
R1>access-list 198 permit tcp any host 3.3.3.3 eq telnet
R2>access-list 198 deny tcp 10.0.30.0 0.0.0.255 host 20.0.60.2 eq 80
R2>access-list 198 permit tcp any host 20.0.60.2 eq 80
R2>access-list 199 permit tcp host 20.0.60.2 any gt 1023
R2>access-list 199 permit icmp 20.0.60.0 0.0.0.255 any echo-reply
R2>end
  
```



```

config t
interface serial0/0/1
ip access-group 198 in
ip access-group 199 out
end
  
```

Testing	PC0	Ping 20.0.60.2 Ping 3.3.3.3 telnet 3.3.3.3 web browse "20.0.60.2"
	PC3	Ping 20.0.60.2 Ping 3.3.3.3 telnet 3.3.3.3 web browse "20.0.60.2"
	PC1	Ping 20.0.60.2 Ping 3.3.3.3 telnet 3.3.3.3 web browse "20.0.60.2"
	PC2	Ping 20.0.60.2 Ping 3.3.3.3 telnet 3.3.3.3 web browse "20.0.60.2"
	Server 0	Ping 10.0.10.2 Ping 10.0.30.2 Ping 10.0.50.2 telnet 3.3.3.3

Part 2

Reboot before configuring router 2

10.0.10.0	20.0.50.0	20.0.60.0
Can web browse 20.0.60.2 " http://localhost " Can send/receive emails	Can web browse 20.0.60.2 " http://localhost "	Can ping 10.0.10.2 Can ping 10.0.30.2 Can ping 10.0.50.2

```

R2
en
config t
access-list 198 deny icmp 10.0.30.0 0.0.0.255 20.0.60.0 0.0.0.255 echo
access-list 198 permit icmp any 20.0.60.0 0.0.0.255 echo-reply
access-list 198 permit icmp any 20.0.60.0 0.0.0.255 echo
access-list 198 deny tcp 10.0.10.0 0.0.0.255 host 3.3.3.3 eq telnet
access-list 198 permit tcp any host 3.3.3.3 eq telnet
access-list 198 deny tcp 10.0.30.0 0.0.0.255 host 20.0.60.2 eq 80
access-list 198 permit tcp any host 20.0.60.2 eq 80
access-list 198 permit tcp 10.0.10.0 0.0.0.255 host 20.0.60.3 eq pop3
  
```



```

access-list 198 permit tcp 10.0.10.0 0.0.0.255 host 20.0.60.3 eq SMTP
access-list 198 permit tcp 10.0.10.0 0.0.0.255 host 20.0.60.2 eq 53
access-list 198 permit udp 10.0.10.0 0.0.0.255 host 20.0.60.2 eq 53
access-list 199 permit tcp host 20.0.60.2 any gt 1023
access-list 199 permit tcp host 20.0.60.2 any eq pop3
access-list 199 permit tcp host 20.0.60.2 any eq smtp
access-list 199 permit tcp host 20.0.60.2 any eq 53
access-list 199 permit udp host 20.0.60.2 any eq 53
access-list 199 permit icmp 20.0.60.0 0.0.0.255 any echo-reply
access-list 199 permit icmp 20.0.60.0 0.0.0.255 any echo

end

config t
interface serial0/0/1
ip access-group 198 in
ip access-group 199 out
end
  
```

Testing	PC0	Send email web browse "localserver"
	PC3	Receive email web browse "localserver"
	Server 0	Ping 10.0.10.2 Ping 10.0.30.2 Ping 10.0.50.2 telnet 3.3.3.3

4. Named access list

Reboot before configuring router 2

```

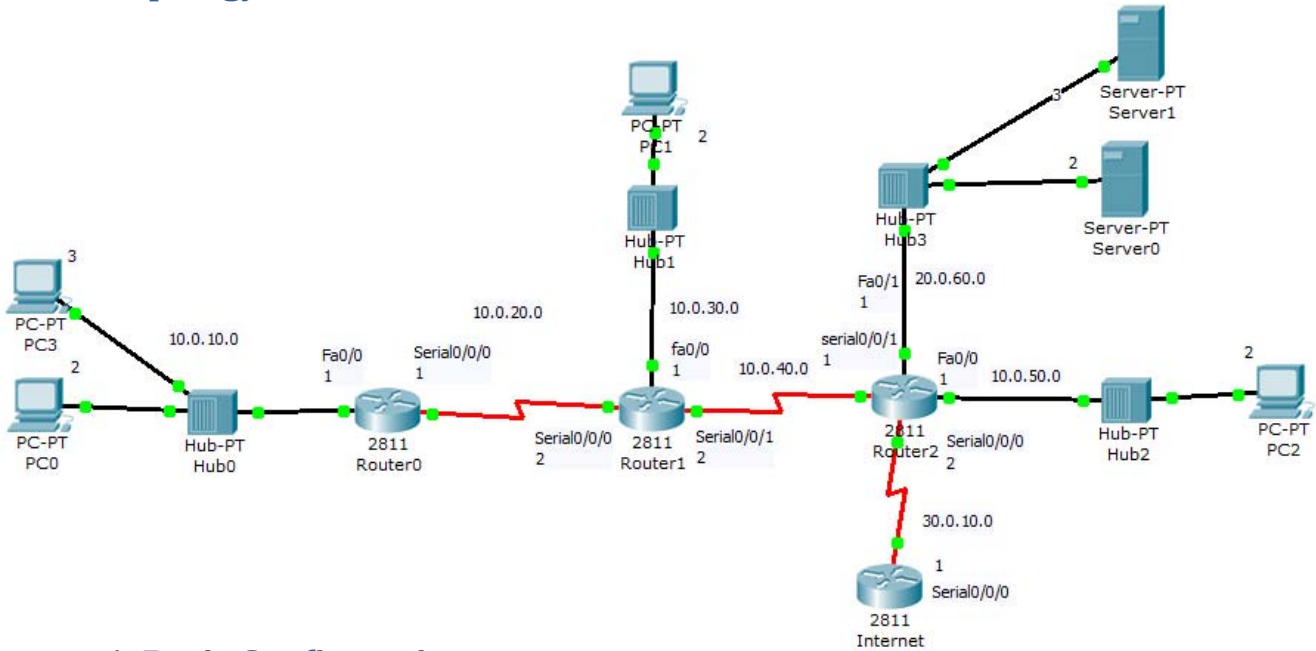
R1
en
config t
ip access-list extended ASL01
deny ip 10.0.10.0 0.0.0.255 host 3.3.3.3
permit ip any host 3.3.3.3
end

R2
en
config t
interface serial0/0/1
ip access-group ASL01 in
end
  
```

Testing	PC0	Send email web browse "localserver"
	PC3	Receive email

	web browse "localserver"
Server 0	Ping 10.0.10.2 Ping 10.0.30.2 Ping 10.0.50.2 telnet 3.3.3.3

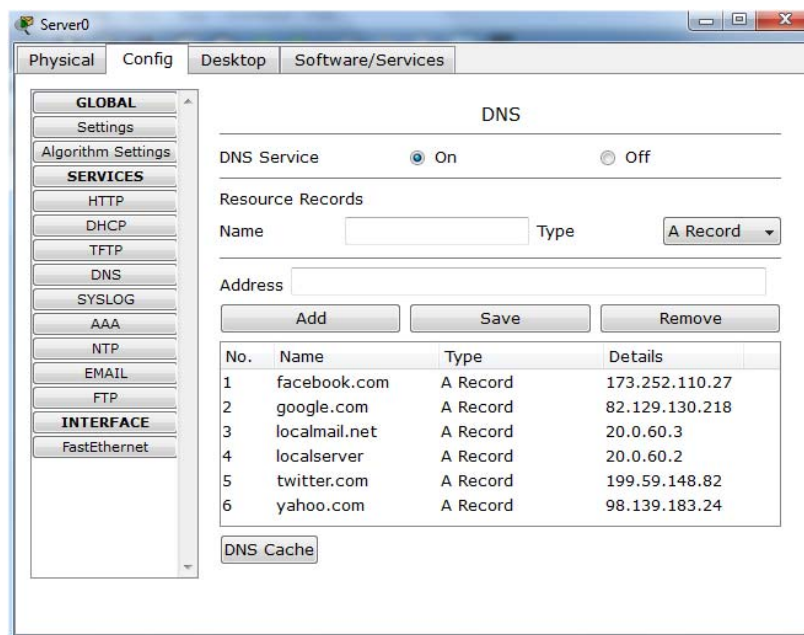
5. DMZ and internet simulation Topology



1. Basic Configuration

Reboot before configuring router 2

Sever 0:





```
l en
n config t
t interface serial0/0/0
e ip address 30.0.10.1 255.255.255.0
r no sh
n exit
e ip route 0.0.0.0 0.0.0.0 30.0.10.2
t
  interface loopback 1
  ip address 8.8.8.8 255.255.255.255
  no sh
  exit
  interface loopback 2
  ip address 4.2.2.2 255.255.255.255
  no sh
  exit
  interface loopback 3
  ip address 82.129.130.218 255.255.255.255
  no sh
  exit
  interface loopback 4
  ip address 98.139.183.24 255.255.255.255
  no sh
  exit
  interface loopback 5
  ip address 173.252.110.27 255.255.255.255
  no sh
  exit
  interface loopback 6
  ip address 199.59.148.82 255.255.255.255
  no sh

end
copy running-config startup-config
```

```
R en
o config t
u interface serial0/0/0
t ip address 30.0.10.2 255.255.255.0
e clock rate 2000000
r no sh
2 exit
  ip route 0.0.0.0 0.0.0.0 30.0.10.1

end
copy running-config startup-config
```



```
R en
o config t
u ip route 0.0.0.0 0.0.0.0 10.0.40.1
t end
e copy running-config startup-config
r
1
```

```
R en
o config t
u ip route 0.0.0.0 0.0.0.0 10.0.20.2
t end
e copy running-config startup-config
r
0
```

Testing	PC0	Ping google.com
	PC1	Ping twitter.com
	PC2	Ping yahoo.com
	Server 0	Ping 8.8.8.8

2. specifying which traffic can exit out the network

```
R en
o config t
u access-list 101 permit ip 20.0.60.0 0.0.0.255 any
t access-list 102 permit ip any any
e exit
r
2 config t
interface serial 0/0/0
ip access-group 101 out
ip access-group 102 in

end
```

Testing	PC0	Ping google.com	
	PC1	Ping twitter.com	
	PC2	Ping yahoo.com	
	Server 0	Ping 8.8.8.8	



3. protect network by allowing the originated traffic from the network

```

R en
o config t
u access-list 103 permit tcp any any established
t access-list 103 permit icmp any any echo-reply
e access-list 103 permit icmp any any unreachable
r access-list 103 deny ip any any
2 exit

config t
interface serial0/0/0
ip access-group 103 in
end
  
```

Testing	Server 0	Ping 8.8.8.8
	internet	Ping 20.0.60.2

4. activating allowed traffic to DMZ (email/dns/web/icmp)

```

R en
o config t
u access-list 104 permit tcp any host 20.0.60.2 eq www
t access-list 104 permit tcp any host 20.0.60.2 eq 53
e access-list 104 permit udp any host 20.0.60.2 eq 53
r access-list 104 permit tcp any host 20.0.60.3 eq pop3
2 access-list 104 permit tcp any host 20.0.60.3 eq SMTP
access-list 104 permit icmp any host 20.0.60.1
access-list 104 deny ip any any
access-list 105 permit ip any any
access-list 105 permit tcp any any gt 0
access-list 105 permit icmp any any
exit

config t
interface fa0/1
ip access-group 104 out
ip access-group 105 in
end

copy running-config startup-config
  
```



Testing	PC0	Browse http://localserver Send/receive email Ping localserver Ping localmail.net Ping 8.8.8.8 Ping google.com
	PC1	Browse http://localserver Send/receive email Ping localserver Ping localmail.net Ping 8.8.8.8 Ping google.com
	PC2	Browse http://localserver Send/receive email Ping localserver Ping localmail.net Ping 8.8.8.8 Ping google.com
	Server 0	Ping 8.8.8.8 Ping google.com Ping 10.0.10.2 Ping 10.0.30.2 Ping 10.0.50.2