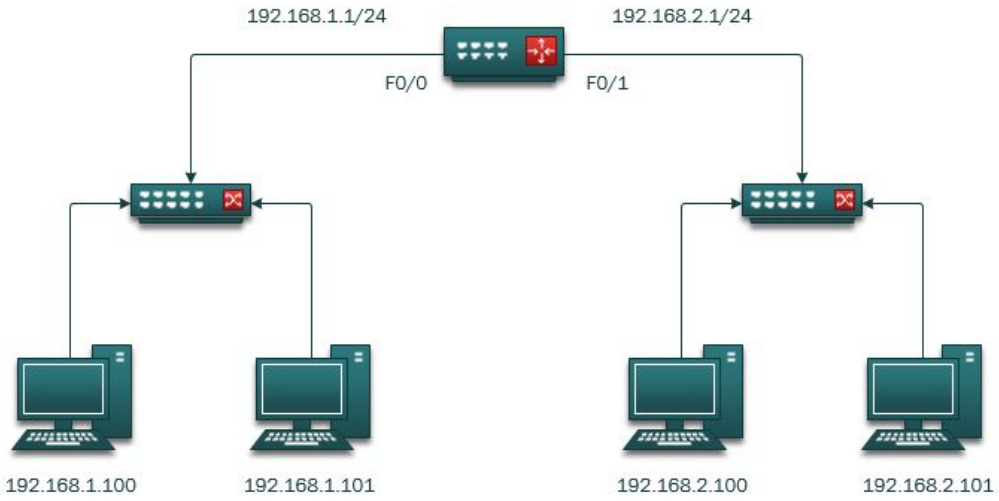
Table of Contents:

Initial Topology:



PC 2 [192.168.2.100]

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : istlabs.rit.edu
   Link-local IPv6 Address . . . . . : fe80::a5fc:bbc5:3561:b60c%8
   IPv4 Address. . . . . . . . . . . : 192.168.2.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
```

PC 3 [192.168.2.101]

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : istlabs.rit.edu
   Link-local IPv6 Address . . . . . : fe80::bc4d:25d2:216c:490c%5
   IPv4 Address. . . . . . . . . . . : 192.168.2.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
```

PC 5 [192.168.1.101]

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : istlabs.rit.edu
   Link-local IPv6 Address . . . . . : fe80::1909:29f2:f164:3d02%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

PC 6 [192.168.1.100]

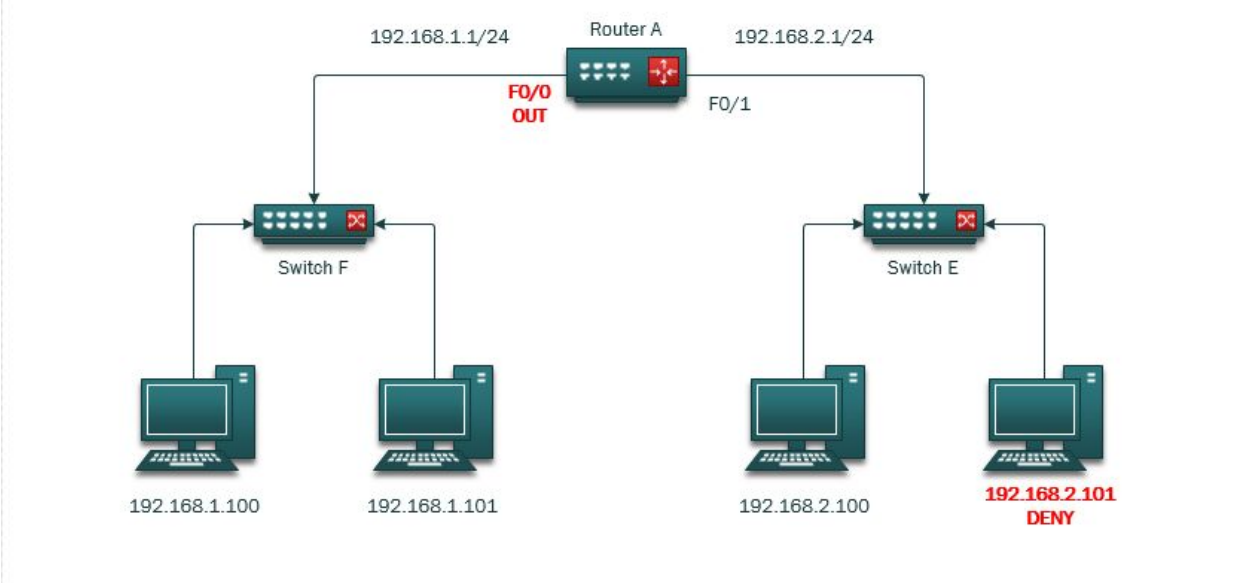
```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : istlabs.rit.edu
   Link-local IPv6 Address . . . . . : fe80::1803:ffe:ccf3:c168%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Section 1: Standard ACL

- Standard ACL's either permits or denies source IP address
- Standard ACL's should be placed as close to the destination as possible
- Standard ACL's should always be outbound on the destination default gateway

(F0/0) outbound [from network 2**(source)** to network 1**(destination)]**



Access-list 1 deny 192.168.2.101 0.0.0.0
Access-list permit any

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 deny 192.168.2.101
Router(config)#access-list 1 permit any
Router(config)#
```

Int f0/0
Ip access-group 1 out

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa
Router(config)#int fastEthernet 0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

Show access-list

```
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
```

Successful pings from network 2 [192.168.2.100]**-unblocked → to network 1**(both PC's)

```
C:\Users\Student>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=3ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Unsuccessful pings from network 2 [192.168.2.101]-**blocked to network 1** (both PC's)

```
C:\Users\Student>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.2.1: Destination net unreachable.
Reply from 192.168.2.1: Destination net unreachable.
Reply from 192.168.2.1: Destination net unreachable.
Reply from 192.168.2.1: Destination net unreachable.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

[wireshark capture] → unsuccessful pings from **network 2 [192.168.2.101] to network 1 [192.168.1.101]**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
11	11.894638	192.168.2.101	192.168.1.101	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (no response found!)
12	11.896259	192.168.2.1	192.168.2.101	ICMP	70	Destination unreachable (Communication administratively filtered)
14	12.900167	192.168.2.101	192.168.1.101	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (no response found!)
15	12.901798	192.168.2.1	192.168.2.101	ICMP	70	Destination unreachable (Communication administratively filtered)
16	13.915838	192.168.2.101	192.168.1.101	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (no response found!)
17	13.917518	192.168.2.1	192.168.2.101	ICMP	70	Destination unreachable (Communication administratively filtered)
19	14.931436	192.168.2.101	192.168.1.101	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (no response found!)
20	14.933087	192.168.2.1	192.168.2.101	ICMP	70	Destination unreachable (Communication administratively filtered)

Show Running Config [FastEthernet **0/0** → Router A]:

```
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
```

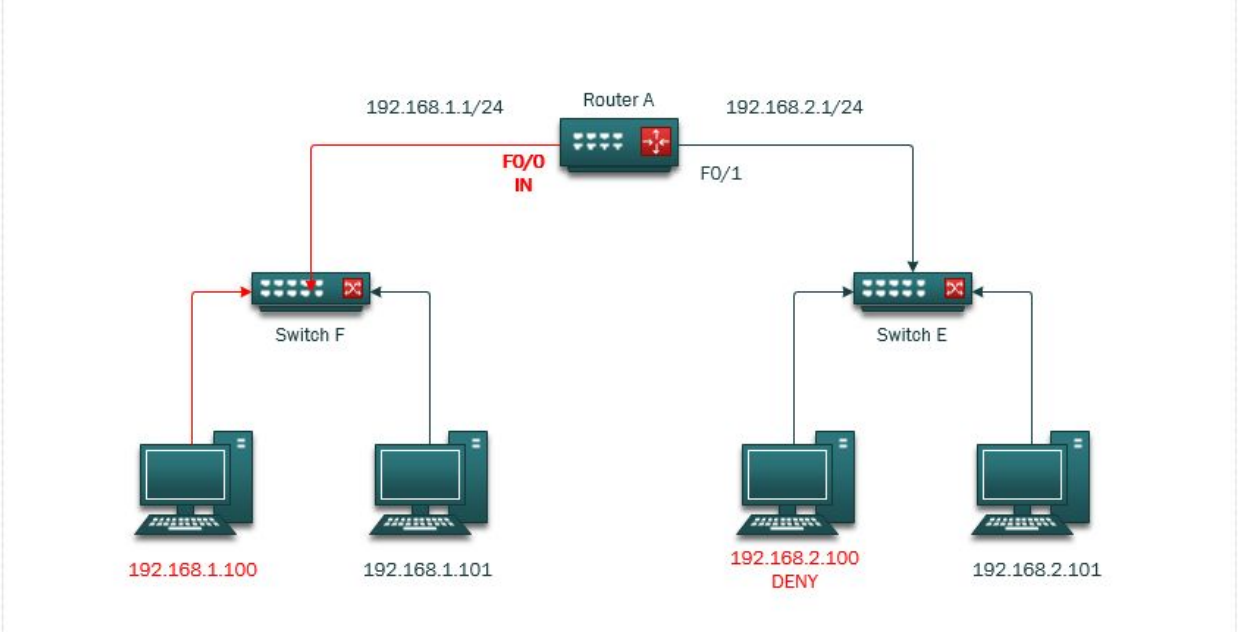
show access-list router standard ACL matches

```
Router>
Router>en
Router#sh access-list
Standard IP access list 1
    deny   192.168.2.101 (16 matches)
    permit any (8 matches)
Router#
```

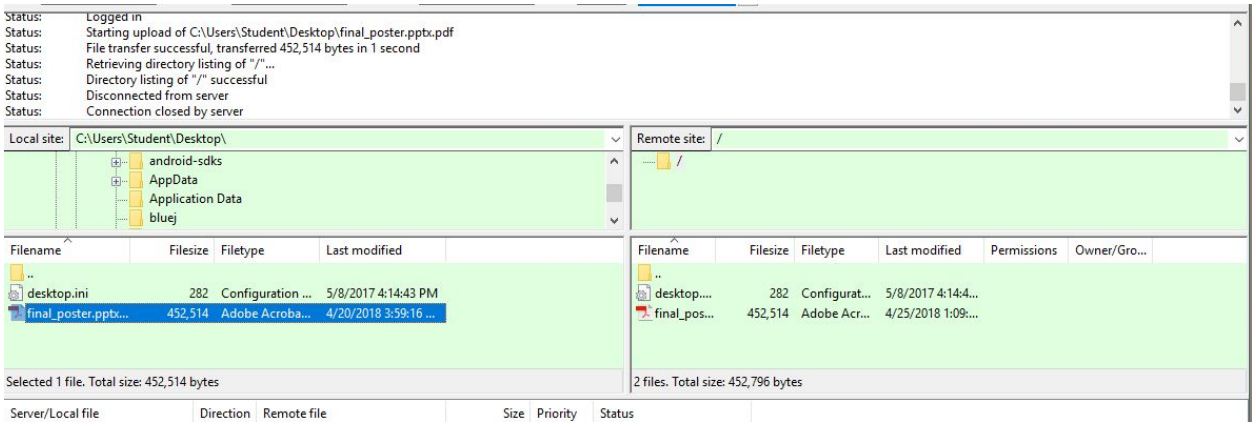
Section 2: **Extended ACL's**

- Extended ACL's filter for [protocol, source address, destination address, port number]
- Extended ACL's should be placed as close to the source as possible
- Extended ACL's should always be an inbound ACL on YOUR(source) default gateway

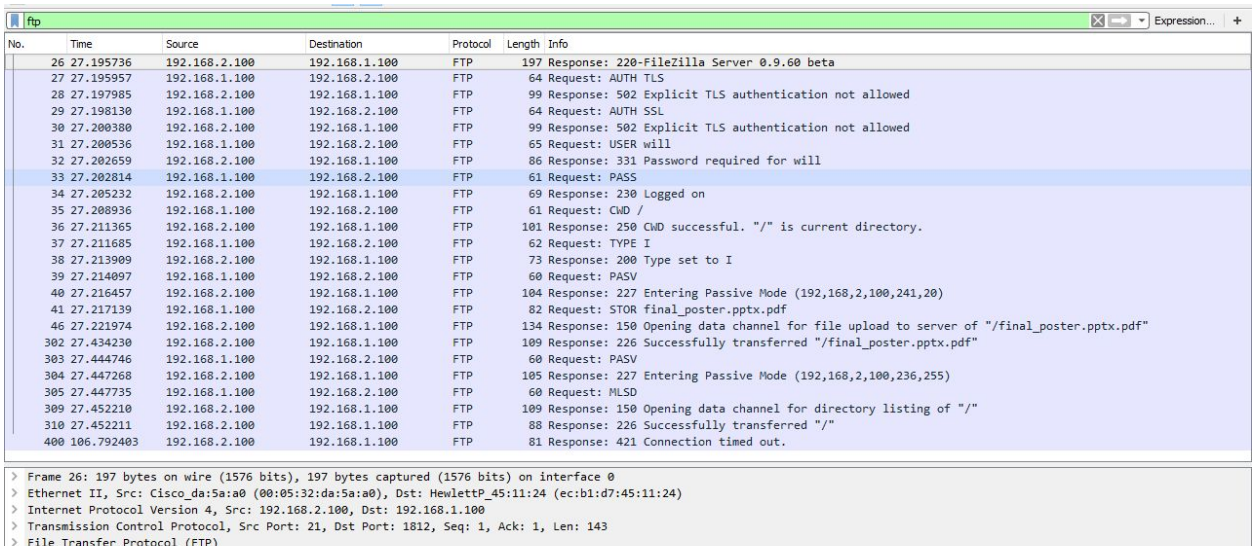
Deny FTP traffic(ports 20 & 21) **b/w 192.168.1.100**(Filezilla client) **& 192.168.2.100**(Filezilla server) **(F0/0) Inbound [**from network 1**(source)** to network 2**(destination)]**



Filezilla client **successful transfer** to filezilla server **- [before extended ACL]**



Wireshark capture**[ftp] - before extended ACL**



ftp

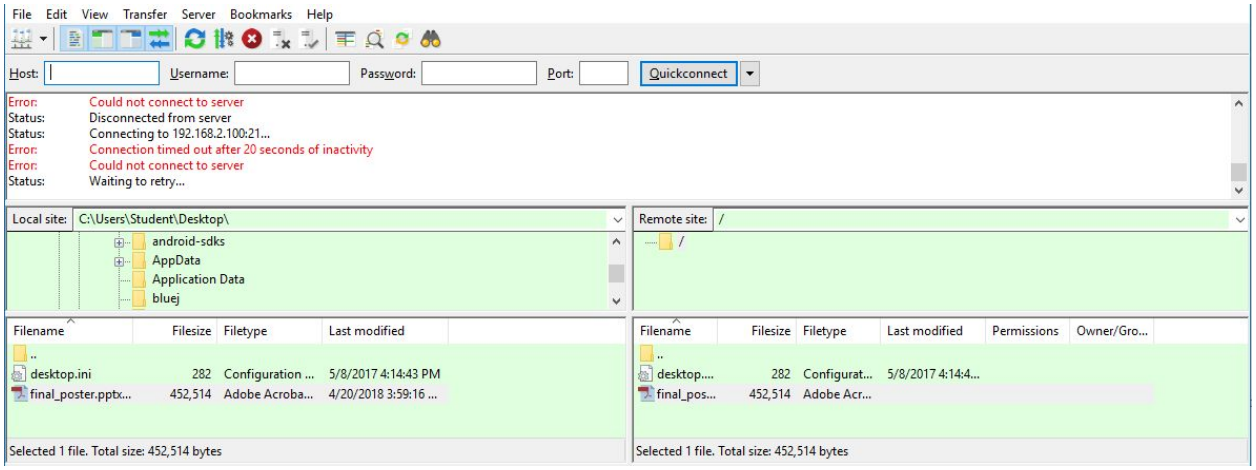
No.	Time	Source	Destination	Protocol	Length	Info
26	27.195736	192.168.2.100	192.168.1.100	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
27	27.195957	192.168.1.100	192.168.2.100	FTP	64	Request: AUTH TLS
28	27.197985	192.168.2.100	192.168.1.100	FTP	99	Response: 502 Explicit TLS authentication not allowed
29	27.198130	192.168.1.100	192.168.2.100	FTP	64	Request: AUTH SSL
30	27.200380	192.168.2.100	192.168.1.100	FTP	99	Response: 502 Explicit TLS authentication not allowed
31	27.200536	192.168.1.100	192.168.2.100	FTP	65	Request: USER will
32	27.202659	192.168.2.100	192.168.1.100	FTP	86	Response: 331 Password required for will
33	27.202814	192.168.1.100	192.168.2.100	FTP	61	Request: PASS
34	27.205232	192.168.2.100	192.168.1.100	FTP	69	Response: 230 Logged on
35	27.208936	192.168.1.100	192.168.2.100	FTP	61	Request: CWD /
36	27.211365	192.168.2.100	192.168.1.100	FTP	101	Response: 250 CWD successful. "/" is current directory.
37	27.211685	192.168.1.100	192.168.2.100	FTP	62	Request: TYPE I
38	27.213909	192.168.2.100	192.168.1.100	FTP	73	Response: 200 Type set to I
39	27.214097	192.168.1.100	192.168.2.100	FTP	60	Request: PASV
40	27.216457	192.168.2.100	192.168.1.100	FTP	104	Response: 227 Entering Passive Mode (192,168,2,100,241,20)
41	27.217139	192.168.1.100	192.168.2.100	FTP	82	Request: STOR final_poster.pptx.pdf
46	27.221974	192.168.2.100	192.168.1.100	FTP	134	Response: 150 Opening data channel for file upload to server of "/final_poster.pptx.pdf"
302	27.434230	192.168.2.100	192.168.1.100	FTP	109	Response: 226 Successfully transferred "/final_poster.pptx.pdf"
303	27.444746	192.168.1.100	192.168.2.100	FTP	60	Request: PASV
304	27.447268	192.168.2.100	192.168.1.100	FTP	105	Response: 227 Entering Passive Mode (192,168,2,100,236,255)
305	27.447735	192.168.1.100	192.168.2.100	FTP	60	Request: MLSD
309	27.452210	192.168.2.100	192.168.1.100	FTP	109	Response: 150 Opening data channel for directory listing of "/"
310	27.452211	192.168.2.100	192.168.1.100	FTP	88	Response: 226 Successfully transferred "/"
400	106.792403	192.168.2.100	192.168.1.100	FTP	81	Response: 421 Connection timed out.

```
> Frame 26: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface 0
> Ethernet II, Src: Cisco_da:5a:a0 (00:05:32:da:5a:a0), Dst: HewlettP_45:11:24 (ec:b1:d7:45:11:24)
> Internet Protocol Version 4, Src: 192.168.2.100, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 21, Dst Port: 1812, Seq: 1, Ack: 1, Len: 143
> File Transfer Protocol (FTP)
```

Deny FTP traffic(ports 20 & 21) **b/w 192.168.1.100**(Filezilla client) **& 192.168.2.100**(Filezilla server)
Access-list 100 deny tcp host 192.168.1.100 host 192.168.2.100 eq ftp
Access-list 100 permit ip any any

```
Router(config)#$ 100 deny tcp host 192.168.1.100 host 192.168.2.100 eq ftp
Router(config)#access-list 100 permit ip any any
Router(config)#exit
Router#
01:16:55: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa
Router(config)#int fastEthernet 0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
Router#
Router#
```

Filezilla client transfer to Filezilla server not successful **- [after extended ACL]**



File Edit View Transfer Server Bookmarks Help

Host: Username: Password: Port: Quickconnect

```
Error:    Could not connect to server
Status:   Disconnected from server
Status:   Connecting to 192.168.2.100:21...
Error:    Connection timed out after 20 seconds of inactivity
Error:    Could not connect to server
Status:   Waiting to retry...
```

Local site: C:\Users\Student\Desktop\

Remote site: /

android-sdks
AppData
Application Data
bluej

/

Filename	Filesize	Filetype	Last modified
..			
desktop.ini	282	Configuration ...	5/8/2017 4:14:43 PM
final_poster.pptx...	452,514	Adobe Acroba...	4/20/2018 3:59:16 ...

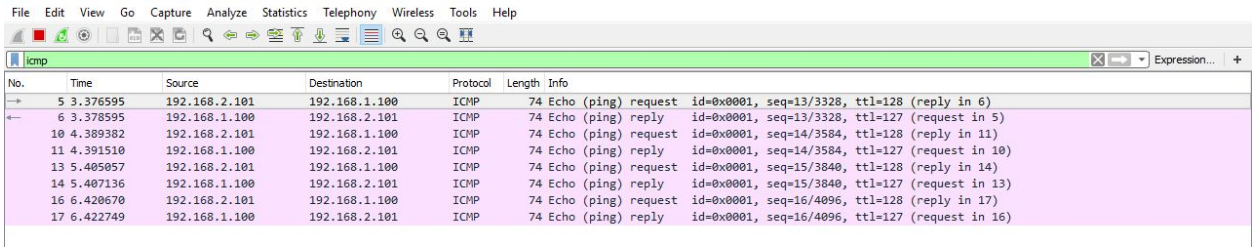
Selected 1 file. Total size: 452,514 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
desktop....	282	Configurat...	5/8/2017 4:14:4...		
final_pos...	452,514	Adobe Acr...			

Selected 1 file. Total size: 452,514 bytes

Empty wireshark capture**[ftp] - After extended ACL**

Successful ping network 2 [192.168.2.101] **to network 1** [192.168.1.101] → After extended ACL
NOTE: ***Access-list 100 permit ip any any*** *[does not deny ICMP traffic between networks]*



Show running config [FastEthernet **0/0** → Router A]:

```
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
!
```

Show access-list router extended ACL matches

```
Router#
Router#sh access-list
Extended IP access list 100
    deny tcp host 192.168.1.100 host 192.168.2.100 eq ftp (12 matches)
    permit ip any any (146 matches)
Router#
```

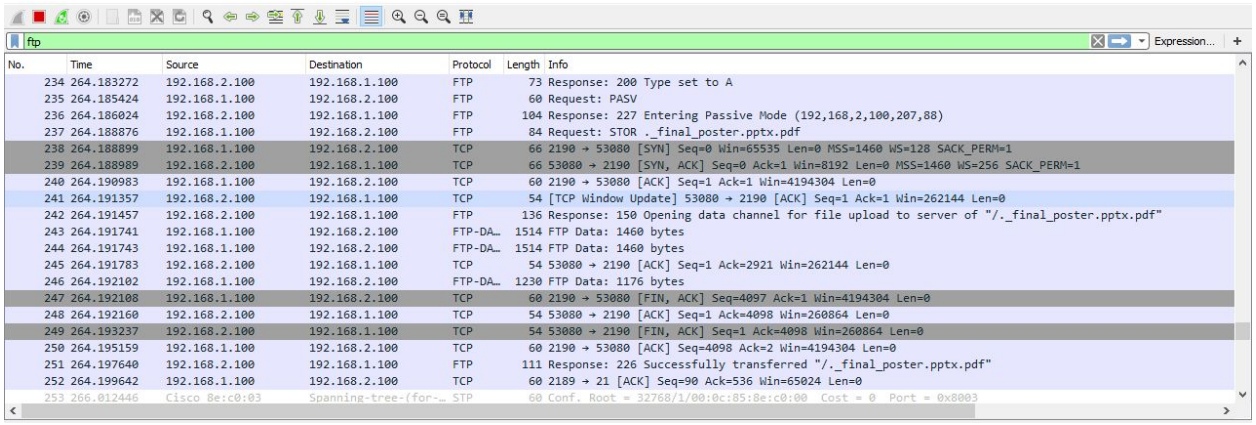
Section 3: Black hole routes

---

wireshark capture on **client** before blackhole and before ACL → **successful FTP traffic**

```
230 294.577527    192.168.1.100    192.168.2.100    FTP      61 Request: PASS
231 294.579810    192.168.2.100    192.168.1.100    FTP      69 Response: 230 Logged on
232 294.582743    192.168.1.100    192.168.2.100    FTP      61 Request: CWD /
233 294.585181    192.168.2.100    192.168.1.100    FTP     101 Response: 250 CWD successful. "/" is current directory.
234 294.585510    192.168.1.100    192.168.2.100    FTP      62 Request: TYPE A
235 294.587835    192.168.2.100    192.168.1.100    FTP      73 Response: 200 Type set to A
236 294.588010    192.168.1.100    192.168.2.100    FTP      60 Request: PASV
237 294.590643    192.168.2.100    192.168.1.100    FTP     104 Response: 227 Entering Passive Mode (192,168,2,100,207,88)
238 294.591473    192.168.1.100    192.168.2.100    FTP      84 Request: STOR ._final_poster.pptx.pdf
245 294.595566    192.168.2.100    192.168.1.100    FTP     136 Response: 150 Opening data channel for file upload to server of "/._final_poster.pptx.pdf"
250 294.602231    192.168.2.100    192.168.1.100    FTP     111 Response: 226 Successfully transferred "/._final_poster.pptx.pdf"
```

Before blackhole acl ftp **server** **wireshark** capture → **successful FTP traffic**



ftp

No.	Time	Source	Destination	Protocol	Length	Info
234	264.183272	192.168.2.100	192.168.1.100	FTP	73	Response: 200 Type set to A
235	264.185424	192.168.1.100	192.168.2.100	FTP	60	Request: PASV
236	264.186024	192.168.2.100	192.168.1.100	FTP	104	Response: 227 Entering Passive Mode (192,168,2,100,207,88)
237	264.188876	192.168.1.100	192.168.2.100	FTP	84	Request: STOR ._final_poster.pptx.pdf
238	264.188899	192.168.1.100	192.168.2.100	TCP	66	2190 → 53080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
239	264.188989	192.168.2.100	192.168.1.100	TCP	66	53080 → 2190 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
240	264.190983	192.168.1.100	192.168.2.100	TCP	60	2190 → 53080 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
241	264.191357	192.168.2.100	192.168.1.100	TCP	54	[TCP Window Update] 53080 → 2190 [ACK] Seq=1 Ack=1 Win=262144 Len=0
242	264.191457	192.168.2.100	192.168.1.100	FTP	136	Response: 150 Opening data channel for file upload to server of "/._final_poster.pptx.pdf"
243	264.191741	192.168.1.100	192.168.2.100	FTP-DA…	1514	FTP Data: 1460 bytes
244	264.191743	192.168.1.100	192.168.2.100	FTP-DA…	1514	FTP Data: 1460 bytes
245	264.191783	192.168.2.100	192.168.1.100	TCP	54	53080 → 2190 [ACK] Seq=1 Ack=2921 Win=262144 Len=0
246	264.192102	192.168.1.100	192.168.2.100	FTP-DA…	1230	FTP Data: 1176 bytes
247	264.192108	192.168.1.100	192.168.2.100	TCP	60	2190 → 53080 [FIN, ACK] Seq=4097 Ack=1 Win=4194304 Len=0
248	264.192160	192.168.2.100	192.168.1.100	TCP	54	53080 → 2190 [ACK] Seq=1 Ack=4098 Win=260864 Len=0
249	264.193237	192.168.2.100	192.168.1.100	TCP	54	53080 → 2190 [FIN, ACK] Seq=1 Ack=4098 Win=260864 Len=0
250	264.195159	192.168.1.100	192.168.2.100	TCP	60	2190 → 53080 [ACK] Seq=4098 Ack=2 Win=4194304 Len=0
251	264.197640	192.168.2.100	192.168.1.100	FTP	111	Response: 226 Successfully transferred "/._final_poster.pptx.pdf"
252	264.199642	192.168.1.100	192.168.2.100	TCP	60	2189 → 21 [ACK] Seq=90 Ack=536 Win=65024 Len=0
253	266.012446	Cisco_8e:c0:03	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/1/00:0c:85:8e:c0:00 Cost = 0 Port = 0x8003

Blackhole route command

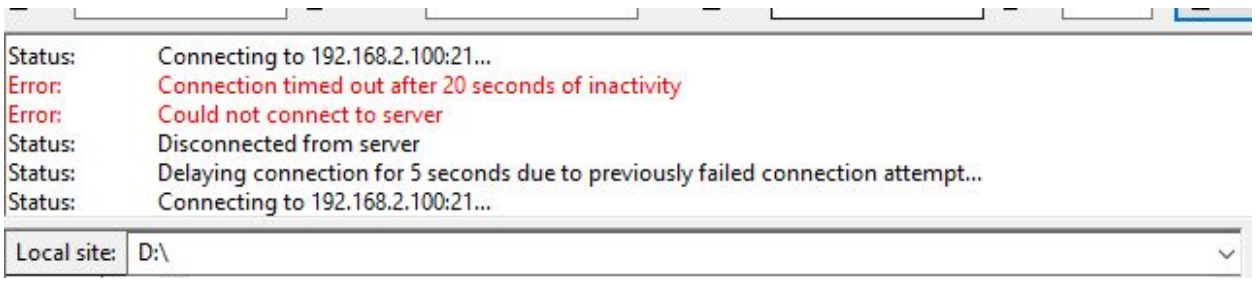
b/w **192.168.1.100**(Filezilla client) **& 192.168.2.100**(Filezilla server)

NOTE: The black hole route drops everything from **192.168.1.00**

```
Router_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router_A(config)#ip route 192.168.1.100 255.255.255.255 null0
Router_A(config)#
Router_A(config)#
Router_A(config)#exit
```

Filezilla client → after blackhole routing

[Cannot connect/transfer file] blackhole route successful



```
Status:     Connecting to 192.168.2.100:21...
Error:      Connection timed out after 20 seconds of inactivity
Error:      Could not connect to server
Status:     Disconnected from server
Status:     Delaying connection for 5 seconds due to previously failed connection attempt...
Status:     Connecting to 192.168.2.100:21...
Local site: D:\
```

Filezilla server wireshark capture → after blackhole route created
NOTE: No FTP traffic. Blackhole route successful

Conclusion:
When creating **standard access lists, extended access lists** or **blackhole routes**, the goals in the lab examples are similar - create two different networks, and selectively allow or deny certain traffic between these two networks by creating rules/routes on the router. I found the Extended ACLs the most useful because of how specific they can be written. I was able to specify the source, destination, port and protocol in the experiment I did. Then, using Filezilla, (both client and server) on network 1 and network 2 respectively, I was able to create port 20 and 21 FTP traffic. With the use of **standard access lists & blackhole routes,** I denied/dropped a specific IP address, regardless of the ports and protocol**.** With **extended access lists**, I only dropped/denied specifically FTP traffic from the source IP.