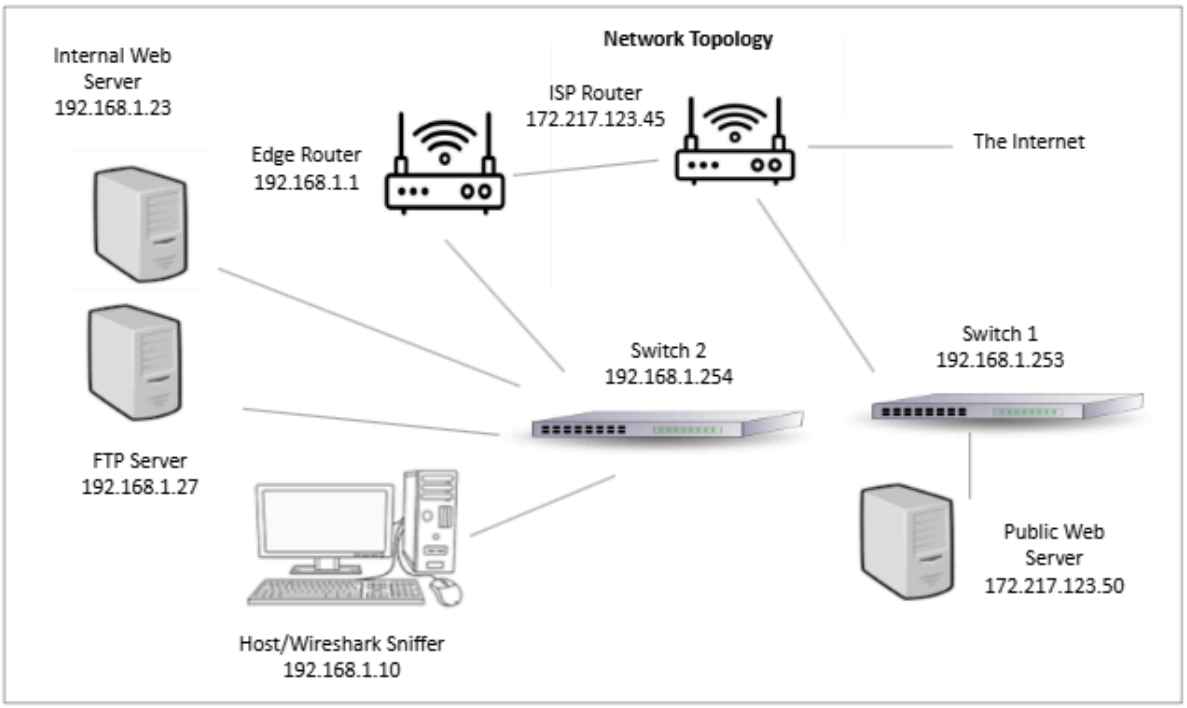
Eric Guzman
Professor Cannistra

2/20/2025
Internet Security

Lab 1

Description: In this lab we used lab hardware to analyze three forms of network traffic, HTTP, FTP and Telnet.

Topology:



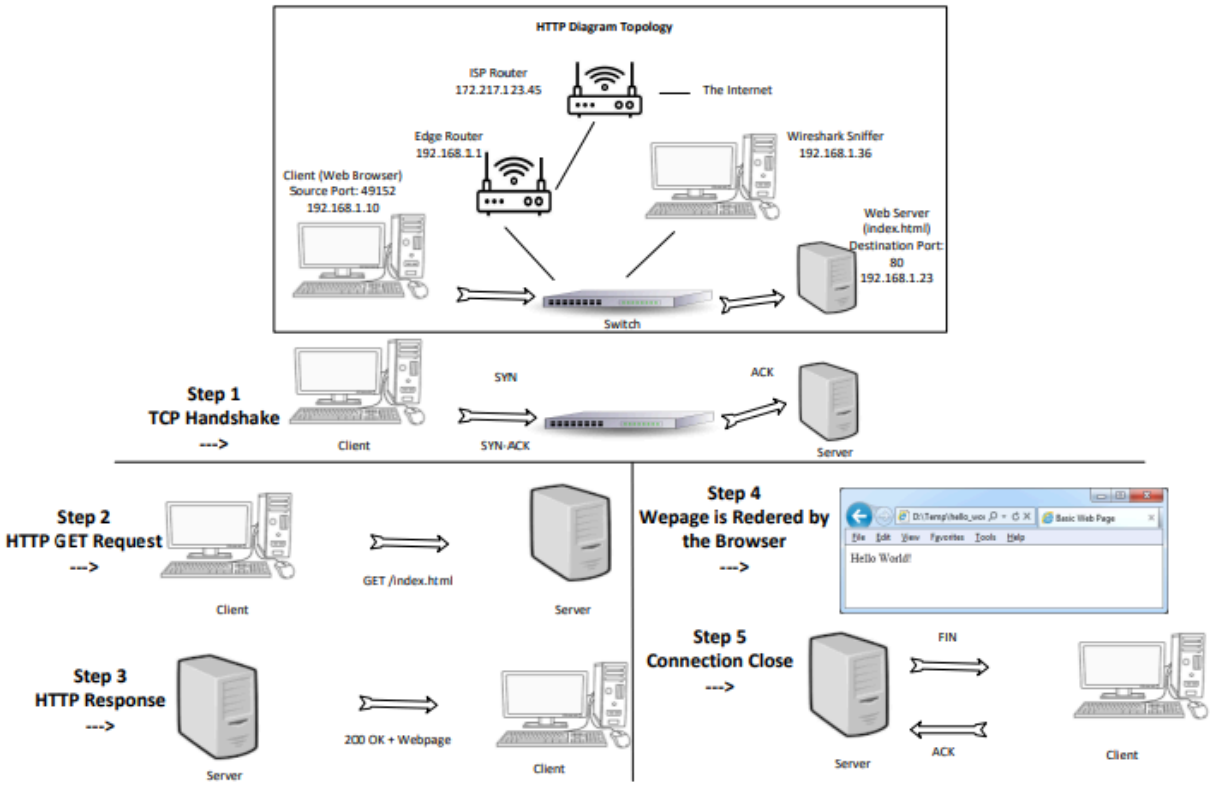
Syntax:

Command	Description	Mode of IOS
No shutdown	Makes sure the network interface is active	Interface configuration
Show ip route	Shows the routing table	Privileged exec

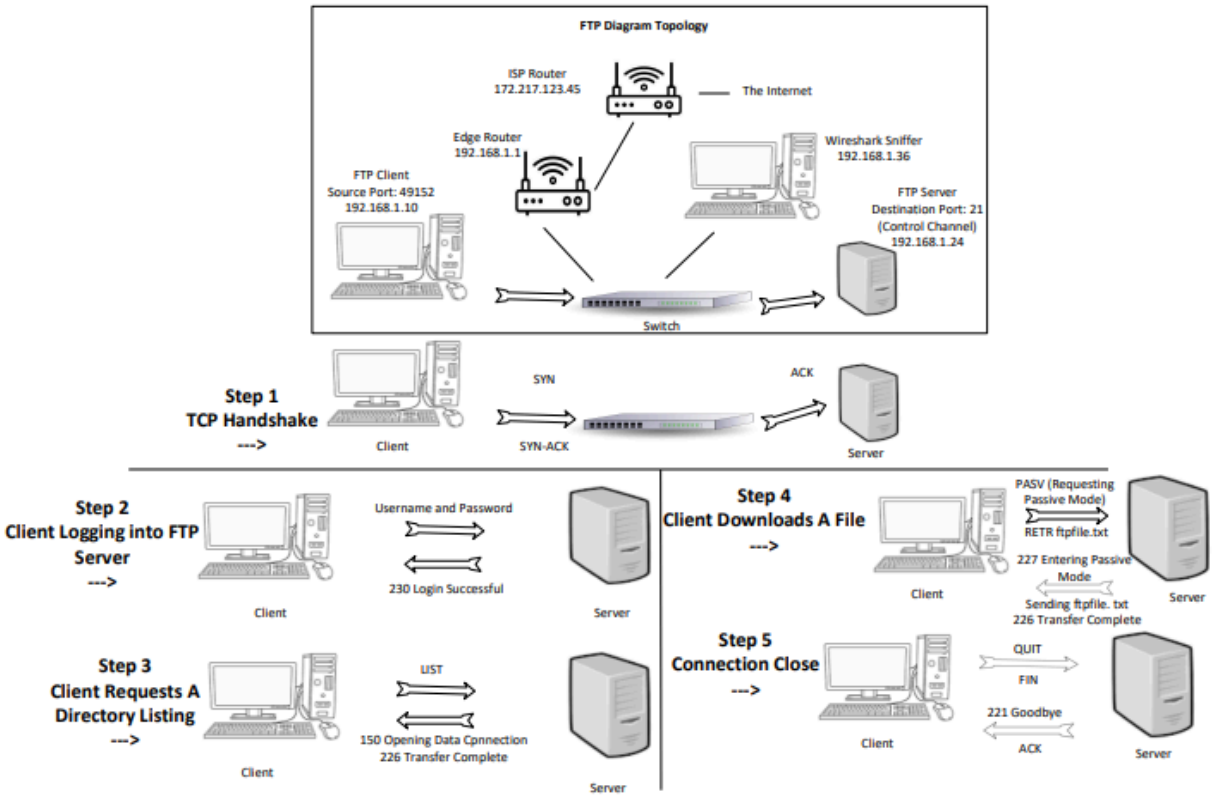
monitor session (#) source interface (int)	Starts a SPAN session, mirroring traffic from an interface	Global configuration

Task One:

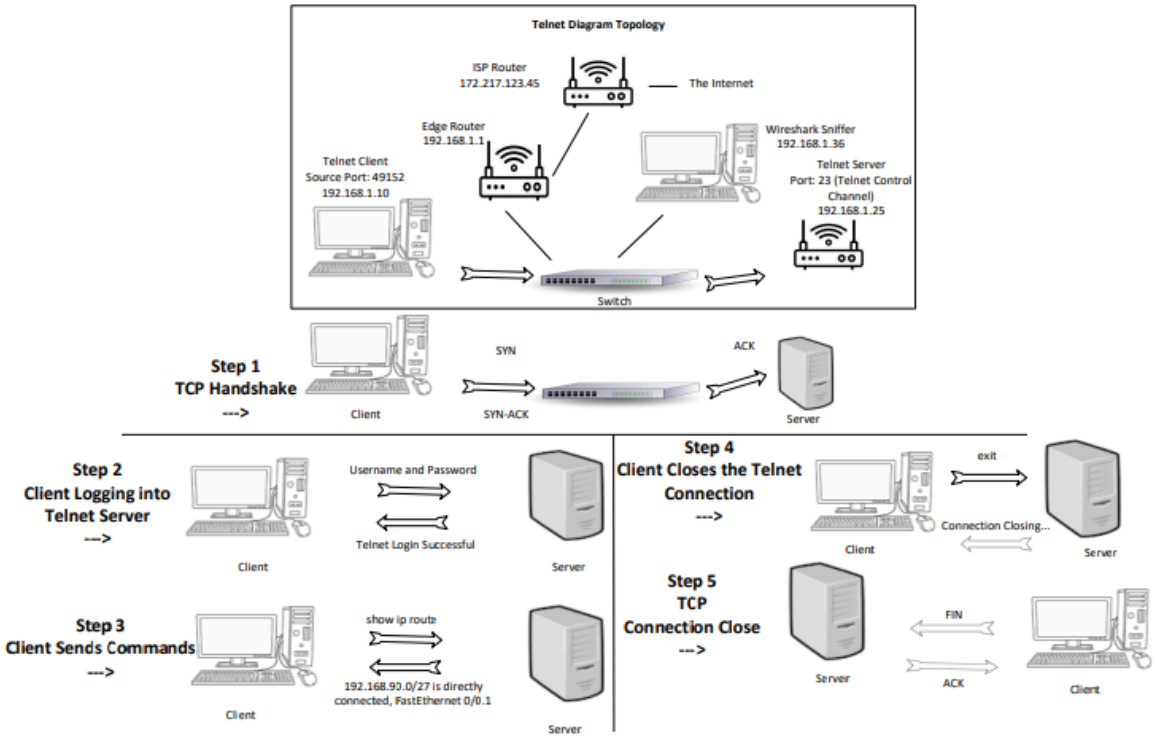
1. HTTP Diagram:



2. FTP Diagram:



3. Telnet Diagram



Task Two:

Verification:

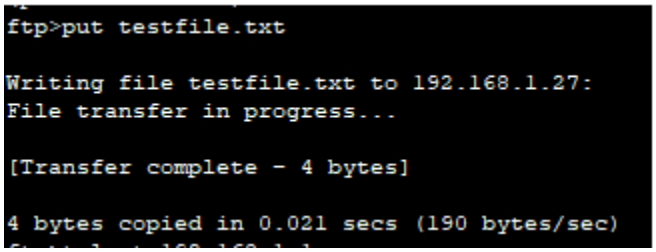
Connectivity:

```
C:\>ping 172.217.124.50

Pinging 172.217.124.50 with 32 bytes of data:

Reply from 172.217.124.50: bytes=32 time=32ms TTL=126
Reply from 172.217.124.50: bytes=32 time=21ms TTL=126
Reply from 172.217.124.50: bytes=32 time=21ms TTL=126
Reply from 172.217.124.50: bytes=32 time=22ms TTL=126

Ping statistics for 172.217.124.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 32ms, Average = 24ms
```

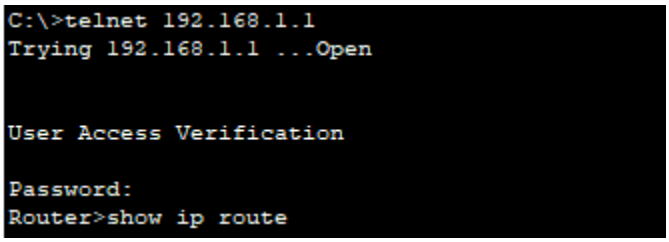
This screenshot shows that I have full connectivity across my topology since my FTP server can ping the Public Web Server.

This screenshot shows that my internet web page is able to be reached from the FTP server.

This screenshot shows that my internal webpage is able to be reached from the FTP server.

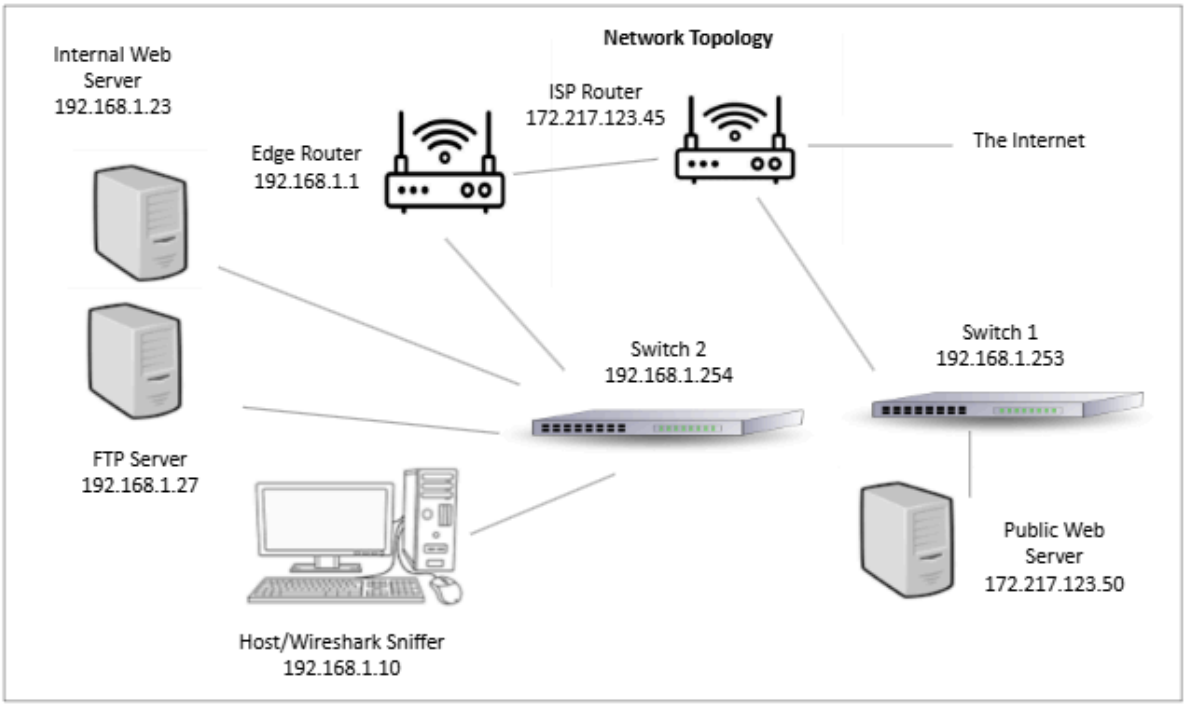


This screenshot shows that I am able to transfer a file to my FTP server from my Internal Web Server.



This screenshots show that I am able to telnet into the Edge Router from my Internal Web Server.

Lab Topology (Visio):



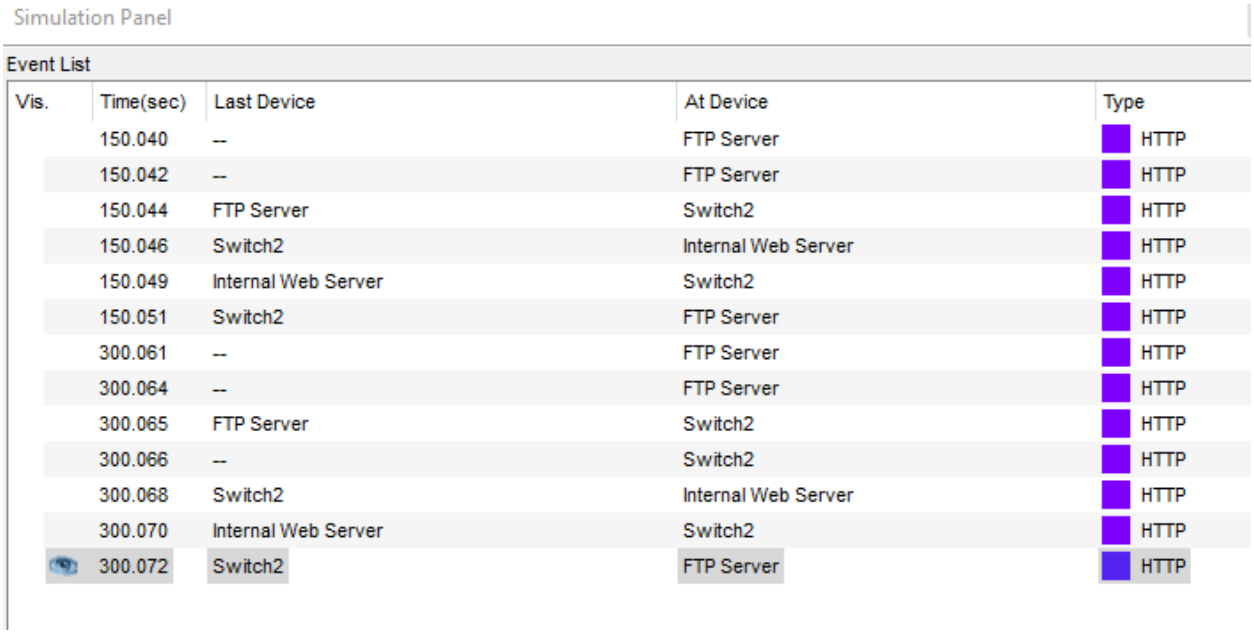
4. **Configuration Thoughts:**

   1. No, the internet hosts should not be able to transfer files to the internal FTP server as it poses a very significant risk and opens us up to multiple vulnerabilities. Someone could exploit known FTP vulnerabilities and get unauthorized access, upload some malicious files or try to compromise credentials. It is safer to not allow internet hosts to transfer anything to the server and we should set up firewall rules to deny any access from internet hosts.

   2. No, the internal web servers should not be able to be accessed from the internet. Allowing this would open us up to even more vulnerabilities such as DDoS attacks, unauthorized data access, web application vulnerabilities and many others.

Task Three:

4.



Vis.	Time(sec)	Last Device	At Device	Type
	150.040	--	FTP Server	HTTP
	150.042	--	FTP Server	HTTP
	150.044	FTP Server	Switch2	HTTP
	150.046	Switch2	Internal Web Server	HTTP
	150.049	Internal Web Server	Switch2	HTTP
	150.051	Switch2	FTP Server	HTTP
	300.061	--	FTP Server	HTTP
	300.064	--	FTP Server	HTTP
	300.065	FTP Server	Switch2	HTTP
	300.066	--	Switch2	HTTP
	300.068	Switch2	Internal Web Server	HTTP
	300.070	Internal Web Server	Switch2	HTTP
	300.072	Switch2	FTP Server	HTTP

These screenshots show what packet data was generated after I opened the http webpage.

5.

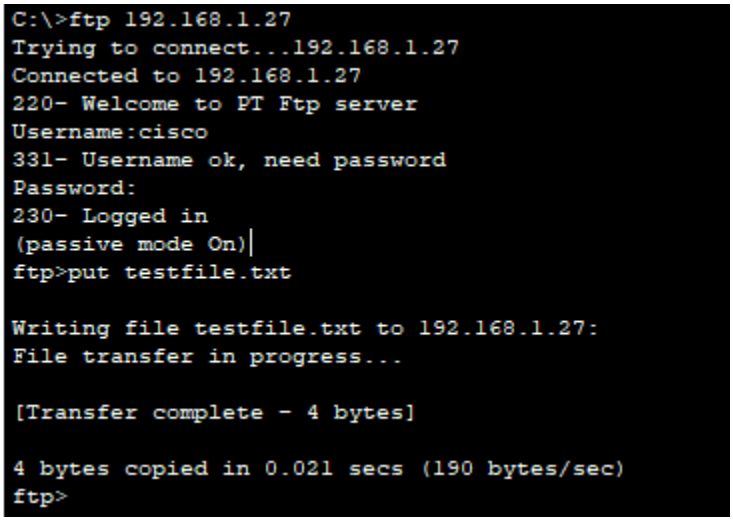
```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.217.123.45 to network 0.0.0.0

     172.217.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.217.123.44/30 is directly connected, FastEthernet0/0
L       172.217.123.46/32 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1
L       192.168.1.1/32 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.217.123.45
```

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.038	Switch2	Internal Web Server	TELNET
	0.038	--	Edge Router	TELNET
	0.039	Edge Router	Switch2	TELNET
	0.039	--	Edge Router	TELNET
	0.040	Switch2	Internal Web Server	TELNET
	0.040	--	Switch2	TELNET
	0.041	Edge Router	Switch2	TELNET
	0.041	--	Edge Router	TELNET
	0.042	Switch2	Internal Web Server	TELNET
	0.042	--	Switch2	TELNET
	0.043	Edge Router	Switch2	TELNET
	0.043	--	Edge Router	TELNET
	0.044	Switch2	Internal Web Server	TELNET
	0.044	--	Switch2	TELNET
	0.046	Edge Router	Switch2	TELNET
	0.046	Switch2	Internal Web Server	TELNET
	0.046	--	Edge Router	TELNET
	0.047	Edge Router	Switch2	TELNET
	0.047	--	Edge Router	TELNET
	0.048	Switch2	Internal Web Server	TELNET
	0.048	--	Switch2	TELNET
	0.050	Edge Router	Switch2	TELNET
	0.050	Switch2	Internal Web Server	TELNET
	0.052	Switch2	Internal Web Server	TELNET

These screenshots show what packet data was generated after I telnetted into the Edge Router and issued a show ip route command.

6.



	0.011	FTP Server	Switch2	FTP
	0.013	Switch2	Internal Web Server	FTP
	0.013	--	Internal Web Server	FTP
	0.014	Internal Web Server	Switch2	FTP
	0.016	Switch2	FTP Server	FTP
	0.016	--	FTP Server	FTP
	0.017	FTP Server	Switch2	FTP
	0.019	Switch2	Internal Web Server	FTP
	0.027	--	Internal Web Server	FTP
	0.029	--	Internal Web Server	FTP
	0.031	Internal Web Server	Switch2	FTP
	0.033	Switch2	FTP Server	FTP
	0.033	--	FTP Server	FTP
	0.035	--	FTP Server	FTP
	0.036	--	FTP Server	FTP
	0.037	FTP Server	Switch2	FTP
	0.038	--	Switch2	FTP
	0.040	Switch2	Internal Web Server	FTP

These screenshots show what packet data was generated after I transferred a file via FTP.

Conclusion:

In conclusion, I think that I made a huge mistake in not giving myself the necessary amount of time that I needed to get this lab done in time. Unfortunately I underestimated my skills and time I had available to work on this, leading me to not being able to get the live lab working in time. I

hope that this packet tracer alternative at least shows that I understand the networking concepts needed to be successful in this class. In future labs I will be sure to allocate more time and make sure I do things correctly so I do not end up having to do this again.