

Networking Project Report Template

Name: Nasir Olayinka

C25-08Cybersecurity

1. Introduction

This project demonstrates the configuration and implementation of network security measures in a simulated environment using Cisco Packet Tracer. The focus is on:

- Firewall configuration on the server
- ACLs to control access to critical resources
- Hardening of network devices
- Defense against ARP spoofing attacks
- Testing and verification of network security

2. Network Topology

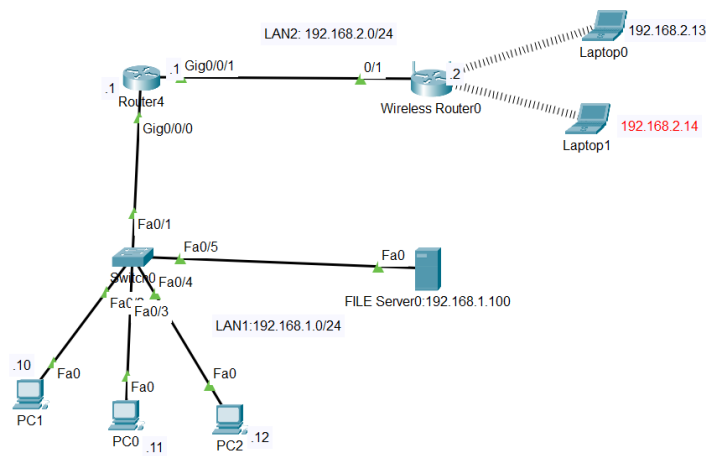


Diagram:

3. IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway	Notes
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1	LAN1 client
PC2	NIC	192.168.1.11	255.255.255.0	192.168.1.1	LAN1 client
PC3	NIC	192.168.1.12	255.255.255.0	192.168.1.1	LAN1 client
File Server	NIC	192.168.1.100	255.255.255.0	192.168.1.1	File/HTTP/FTP
Router1	G0/0/0	192.168.1.1	255.255.255.0	—	LAN1 Gateway
Router1	G0/0/1	192.168.2.1	255.255.255.0	—	LAN2 Gateway
Laptop0	Wireless	192.168.2.13	255.255.255.0	192.168.2.1	LAN2 client
Laptop1	Wireless	192.168.2.14	255.255.255.0	192.168.2.1	LAN2 client

5. Router1 ACL Configuration

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.100 eq 21
access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.100 eq 80
access-list 101 deny ip 192.168.2.0 0.0.0.255 host 192.168.1.100
```

access-list 101 permit ip any any

interface g0/0/1

ip access-group 101 in

6. Device Hardening Steps

- **Router1:**
 - Configured SSH login only
 - Deny Telnet
 - Set strong local user authentication

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#transport input ssh
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#banner motd #UNAUTHORIZED ACCESS WILL BE PROSECUTED#
Router(config)#
```

Showing IP SSH is configured(Router1):

```
UNAUTHORIZED ACCESS WILL BE PROSECUTED
```

```
Router1>en
Router1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Router1#
```

7. Security Simulation – ARP Spoofing Defense

- Configured **Port Security** to restrict number of MAC addresses per port.
- Enabled **MAC address sticky learning** to prevent spoofing.
- Verified that unauthorized devices are blocked.

Switch:

Enabled port security (sticky MAC, violation restrict):

```
Switch>EN
Switch#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fa0/6 - 24
^
% Invalid input detected at '^' marker.
Switch(config)#interface range fa0/6 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)# switchport port-security
Switch(config-if-range)# switchport port-security maximum 2
Switch(config-if-range)# switchport port-security violation restrict
Switch(config-if-range)# switchport port-security mac-address sticky
Switch(config-if-range)#SHUT DOWN
^
% Invalid input detected at '^' marker.
Switch(config-if-range)#SHUTDOWN
```

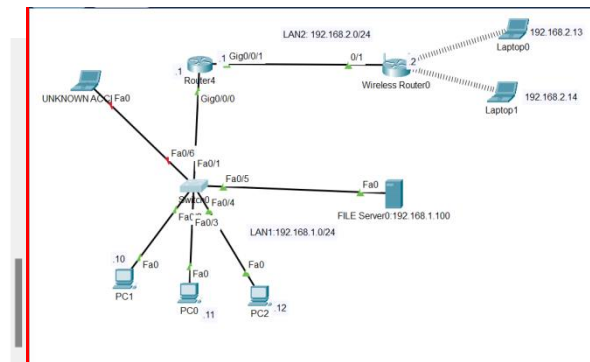
Disabled unused ports

```
Switch(config-if-range) #SHUTDOWN
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
Switch(config-if-range) #EXIT
Switch(config) #EXIT
```

7. Security Simulation – ARP Spoofing Defense

See unknown Computer trying to access switch port FA06 without success:

```
SW0#SHOW
% Incomplete command.
SW0#
SW0#SHOW PORT-SECURITY
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
      (Count)          (Count)          (Count)
-----
Fa0/6      2          0          0      Restrict
Fa0/7      2          0          0      Restrict
Fa0/8      2          0          0      Restrict
Fa0/9      2          0          0      Restrict
Fa0/10     2          0          0      Restrict
Fa0/11     2          0          0      Restrict
Fa0/12     2          0          0      Restrict
Fa0/13     2          0          0      Restrict
Fa0/14     2          0          0      Restrict
Fa0/15     2          0          0      Restrict
Fa0/16     2          0          0      Restrict
Fa0/17     2          0          0      Restrict
Fa0/18     2          0          0      Restrict
Fa0/19     2          0          0      Restrict
Fa0/20     2          0          0      Restrict
Fa0/21     2          0          0      Restrict
Fa0/22     2          0          0      Restrict
Fa0/23     2          0          0      Restrict
Fa0/24     2          0          0      Restrict
SW0#
```



8. Testing & Verification

Port Security Tests (Switch1)		
Test Description	Action Performed	Actual Result
PC (sticky MAC learned)	PC1 reconnected	Connection successful <input checked="" type="checkbox"/>
Connect unauthorized device (new MAC)	Rogue Laptop	Port security violation, no access <input checked="" type="checkbox"/>
Verify port security config	show port-security	Displays learned/sticky MAC <input checked="" type="checkbox"/>

Test	Source Device	Destination	Expected Result	Actual Result
Ping File Server	PC1	192.168.1.100	Success <input checked="" type="checkbox"/>	Success <input checked="" type="checkbox"/>
FTP to File Server	PC2	192.168.1.100	Success <input checked="" type="checkbox"/>	Success <input checked="" type="checkbox"/>
HTTP access to File Server	PC3	192.168.1.100	Success <input checked="" type="checkbox"/>	Success <input checked="" type="checkbox"/>
Ping File Server	Laptop0	192.168.1.100	Blocked <input checked="" type="checkbox"/>	Blocked <input checked="" type="checkbox"/>
Telnet File Server (Port 80)	Laptop1	192.168.1.100	Blocked <input checked="" type="checkbox"/>	Blocked <input checked="" type="checkbox"/>
SSH Access to Router1	Admin PC1	Router1	Success <input checked="" type="checkbox"/>	
Telnet Access to Router1	Any	Router1	Blocked <input checked="" type="checkbox"/>	

```
PC1 Command Prompt
C:\>ping 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128

Pinging 192.168.1.100: bytes=32 time=1ms TTL=128:
Statistics for 192.168.1.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.101
Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Pinging 192.168.1.101:
Statistics for 192.168.1.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128

Pinging 192.168.1.11:
Statistics for 192.168.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.12
Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128

Pinging 192.168.1.12:
Statistics for 192.168.1.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ftp 192.168.1.100
Trying to connect...192.168.1.100
Connected to 192.168.1.100
220- Welcome to PT Ftp server
User: cisco
331- Username ok, need password
Password:
230- Logged in
(pasvive mode On)
ftp>
ftp>quit
221- Service closing control connection.

Laptop0 Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.100
Trying to connect...192.168.1.100
Error opening ftp://192.168.1.100/ (timed out)
(Disconnecting from ftp server)
```

LAN1 PING TESTS/FTP Test

LAN2 FTP TEST to file server

```
PC1 Command Prompt
220- Welcome to PT Ftp server
User: cisco
331- Username ok, need password
Password:
230- Logged in
(pasvive mode On)
ftp>exit
Invalid or non supported command.
ftp>?
?
cd
delete
dir
get
help
passive
put
pwd
quit
rename
ftp>quit
221- Service closing control connection.
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.1
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.1
Password:
UNAUTHORIZED ACCESS WILL BE PROSECUTED
Router1#show access-lists
Extended IP access list 101
10 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.100 eq ftp
20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.100 eq www
30 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.100 (12 match(es))
40 permit ip any any (8 match(es))
50 deny ip 192.168.2.0 0.0.0.255 host 192.168.1.100
Router1#
```

SSH Access to Router1 from PC1 as admin.

9. Conclusion

The project successfully demonstrated:

- Implementation of ACLs to protect a File Server
- Server firewall configuration
- Hardening of network devices against unauthorized access
- Defense against ARP spoofing using switch port security
- Validation through successful and failed connectivity tests

This simulation highlights the importance of layered security controls in ensuring availability, integrity, and confidentiality in a network environment.