Project Report

SecureNet
Intrusion Detection System

May 14, 2024

—

Computer Networks

—

Waseem Rauf

Group Members:

Talha Bilal (K21-3349)
Ahmed Ali (K21-3212)
Taha Hassan (K21-4680)

Contents

1.INTRODUCTION

In today's interconnected landscape, computer networks serve as the backbone linking various devices, whether wired or wirelessly, ranging from computers and phones to printers and mobile devices. The internet, a vast network, governs data flow with speed limits and quotas, facilitating global resource sharing among different networks. While physically connecting computers remains an option, it often entails space and cable redundancies. Switches play a pivotal role in optimizing communication efficiency between multiple devices within networks. Understanding the complexities of networks necessitates practical experience, particularly in light of technological advancements. Simultaneously, network security stands as a cornerstone for safeguarding sensitive data and ensuring the integrity of systems. An Intrusion Detection System (IDS) plays a critical role in identifying and responding to unauthorized access attempts, malicious activities, and other security threats. With the increasing complexity of cyber threats, having an effective IDS is essential for safeguarding network assets and maintaining operational continuity.

1.1. Background

Virtual laboratories offer interactive, real-time simulations for practical experience in education, bridging gaps between theory and practice. They enable demonstrations of applications that are impossible or impractical to conduct in traditional laboratory settings. Computer simulations aid in modeling and analyzing various systems, from physics and chemistry to economics and social sciences. In network areas, simulation technology facilitates tasks like traffic simulation and overall structure modeling. Computer-aided simulation tools are crucial for network simulations, emphasizing performance and validity of protocols and algorithms. The development of network simulation tools aligns with the rapid advancements in network technologies, emphasizing support for commonly used algorithms and protocols.

1.2. Purpose of Report:

1. The significance of network security in the modern interconnected landscape.
2. To underscore the critical role of Intrusion Detection Systems (IDS) in safeguarding sensitive data and ensuring operational continuity.
3. To highlight the escalating complexity of cyber threats and the imperative need for effective security measures.
4. To advocate for proactive strategies and investment in IDS technologies to mitigate risks and uphold system integrity.

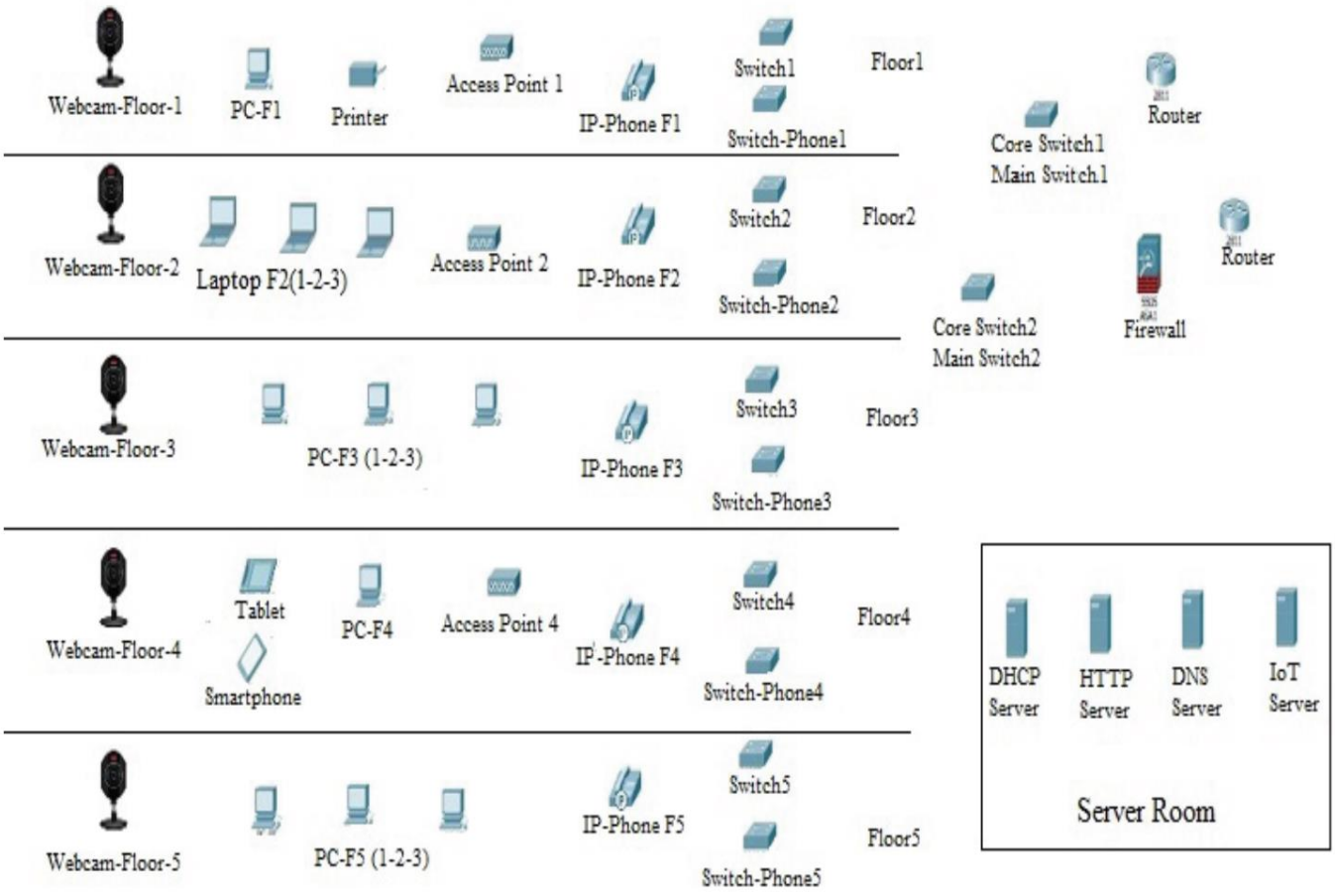
1.3. Intended Audience:

1. Network administrators and IT security professionals responsible for implementing and managing network security measures.
2. Executives and decision-makers in organizations seek to understand the importance of network security in maintaining business continuity.
3. Students and professionals in cybersecurity and network engineering fields looking to enhance their understanding of IDS technology and its applications.
4. Government agencies, regulatory bodies, and policymakers concerned with cybersecurity governance and policy formulation.

2. METHODOLOGY

2.1. Formation of Network Topology

The network is built using Cisco Packet Tracer Program, featuring a topology designed for a 5-storey hotel. It includes 7 computers, 5 laptops, 3 tablets, 5 IP phones, 14 switches, 3 routers, 5 access points, and various servers and devices. The network design encompasses security measures like a security wall and DHCP server. Additionally, devices such as cameras, tablets, smartphones, and an IoT server are integrated for diverse functionalities within the network.



3. RESULT

The results have been produced by the Packet Tracer for the different scenarios.

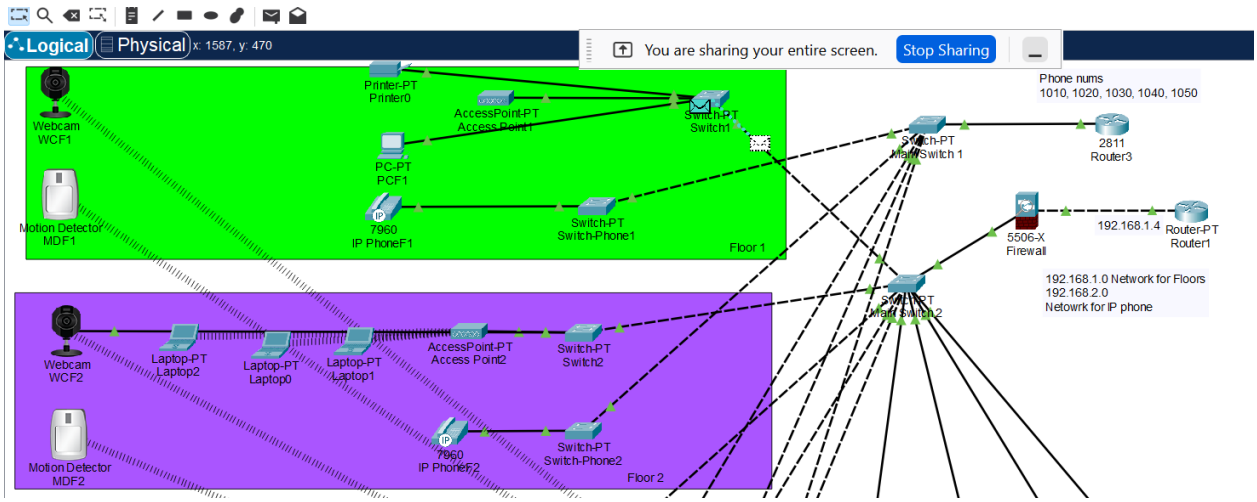
3.1. Scenarios

To prove the Packet Tracer is suitable and applicable to design and implement network. In addition, the Packet Tracer is very important to use in the learning computer networks, five different scenarios have been used.

3.1.1. Send Packet (between Two Floors) Scenario

In this scenario we will send a message from computer device on the first floor to another computer device on the fifth floor and we will note how the message moves step by step in order to reach the destination as shown below:

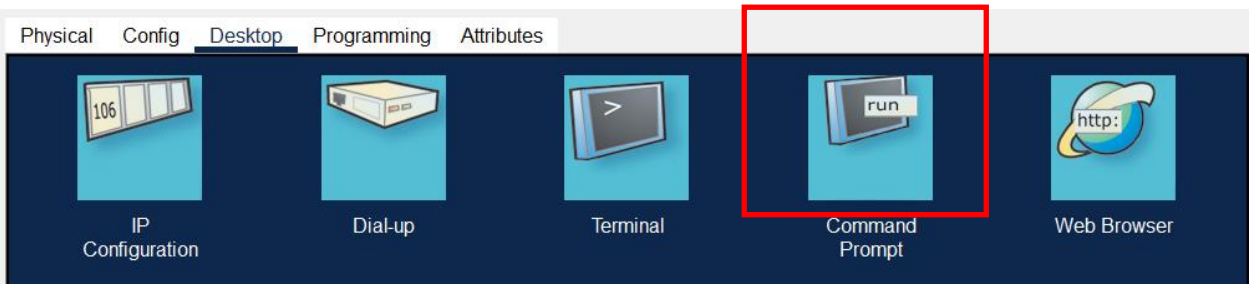
- First step, the packet was redirected to Switch.
- Second step, Switch1 redirected the package to Core Switch.
- Third step, Core Switch2, redirected the package to Switch.
- Forth step, Switch6, redirected the package to Access Point.
- Fifth step finally, the package was successfully sent from the Access Point to the target user (Laptop)



3.1.2. Command Line Interface (CLI) Scenario

In this scenario we will use the command line interface (CLI) between any two devices in the network to prove all devices connected between each other as shown below:

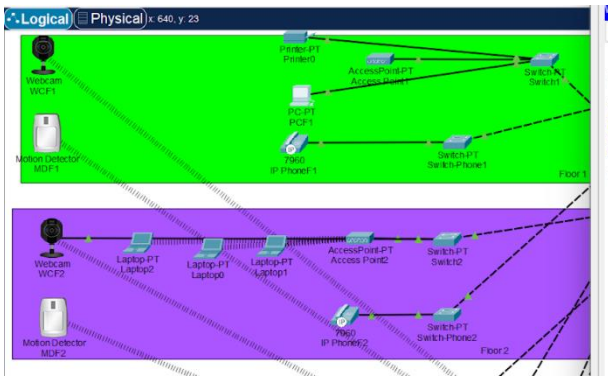
First step, we enter the computer device interface on any floor and login to Command Prompt in order to send ping between any two devices.
Second step, then we specify the target device IP address by giving the target ping command.



3.1.3. Website Scenario

In this scenario we will implement the Website for the purpose of accessing the Website pages as shown below:

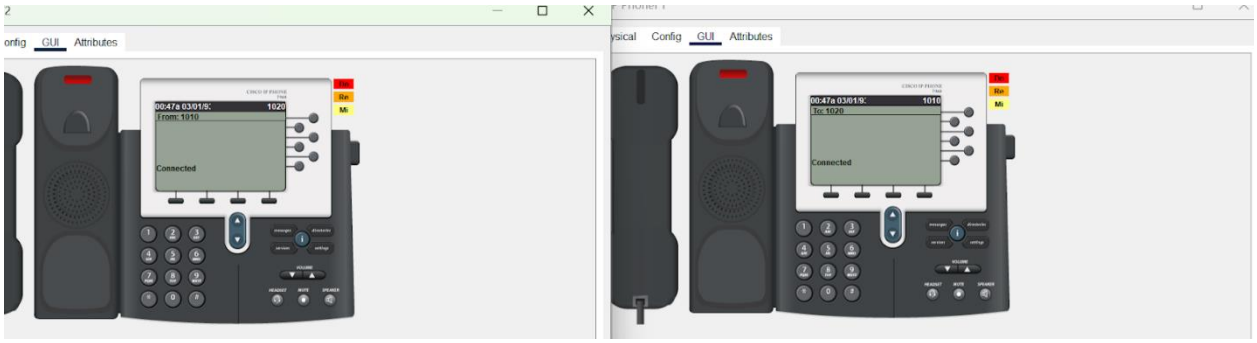
- First step, in order to login to the Website, it is entered to the interface of any network device connected to the network and the Web Browser button is clicked.
- Second step: Then http://hello.com is written on the address line. Once this is done, the DNS server will be asked for the IP address of hello.com. Since DNS server knows the IP address of the hello.com domain name, it directs the user to the IP address where the HTTP server is located so that the user will be faced with the web interface. Then, a phrase will appear on the page (Welcome to Our CN Project).



3.1.4. IP-Phone Scenario

In this scenario we will use IP-Phone device to make a telephone call between two phone devices located on second floor and fifth floor of the hotel to prove that the network is also used by telephone devices well.

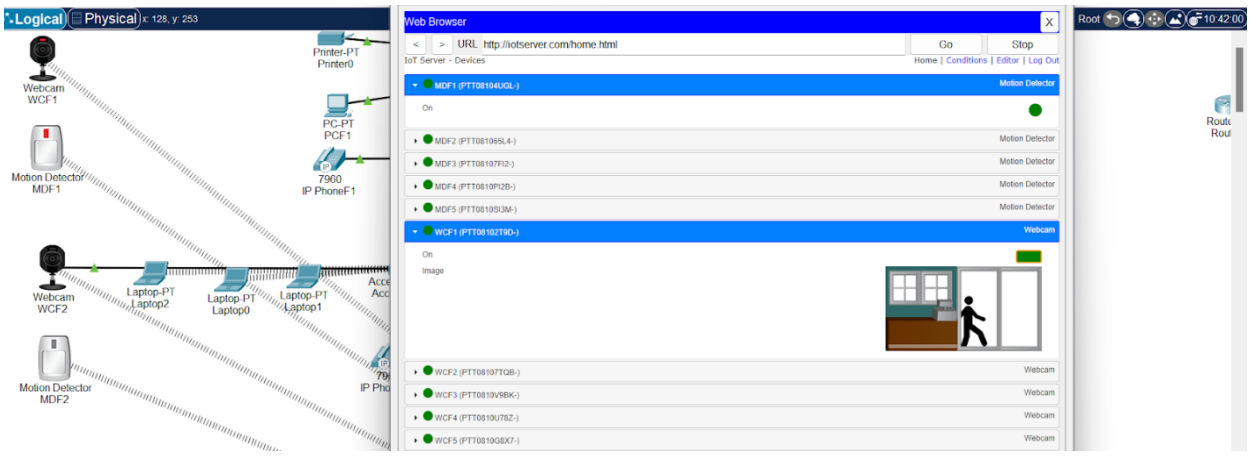
- First step, the interface of the phone on the second floor is entered.
- Second step, the 5th-floor telephone number is entered the phone (1040).
- Third step, the phone is opened by clicking on the phone.
- Forth step, the interface of the phone on the 5th floor is opened and the call is answered by clicking on the phone.



3.1.5. CCTV Scenario

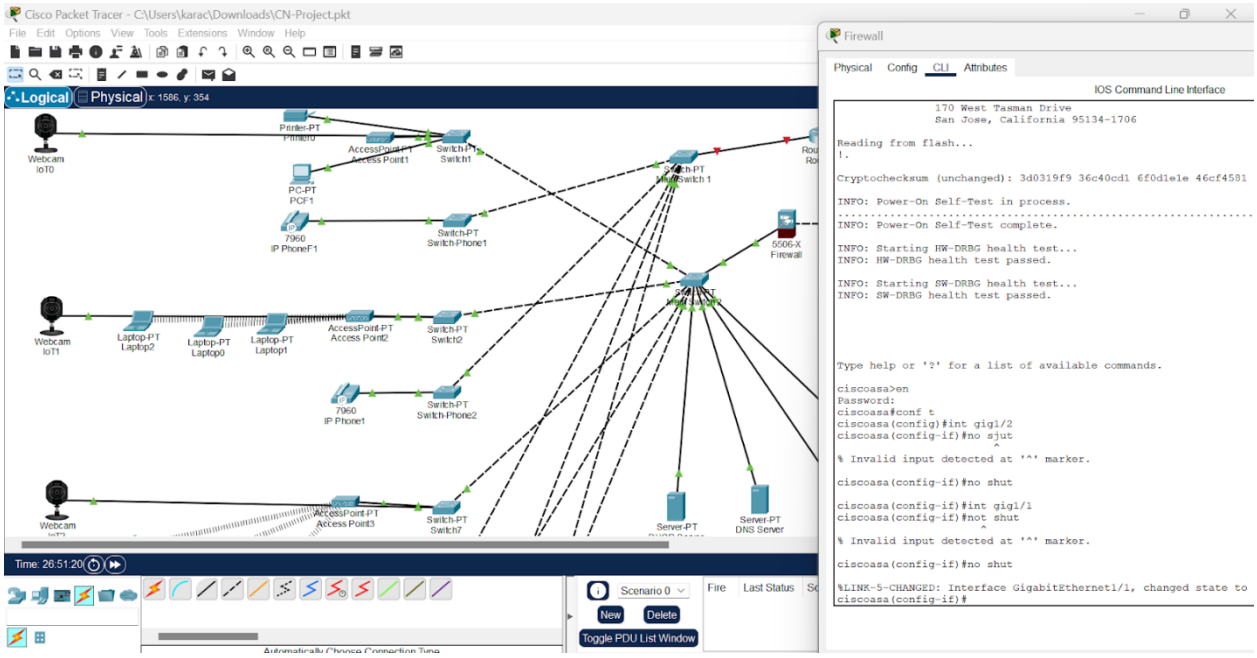
In this scenario, to prove that the security of the building is very important, surveillance cameras were used to monitor all the building floors and connect these cameras to the network. Moreover, Thanks to CCTV, the view from the security cameras is realized. The floors can be monitored at any time thanks to the cameras which are provided with each crawler and thus security is ensured. To monitor security cameras, enter the interface of a device connected to the network and perform the following steps:

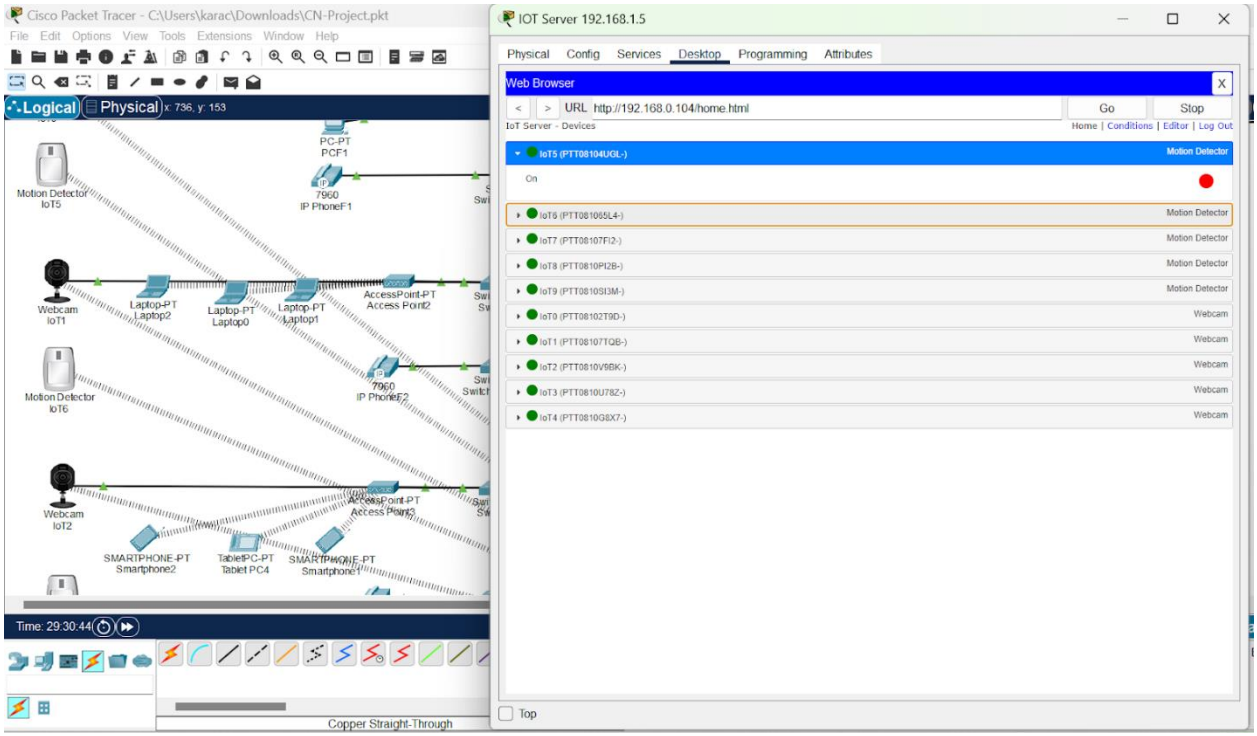
- First step, for the first time it is entered to the interface of the networked device and the web browser button is clicked.
- Second step: IoT server, IP address is written on address line.
- Third step, the floor to be watched is selected.
- The fourth and last step, after selecting the floor to be seen on the screen, people who enter the floor appear to us.

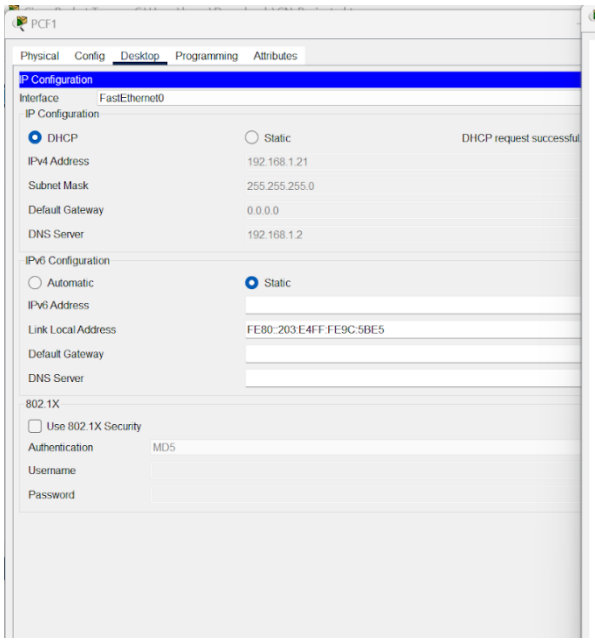


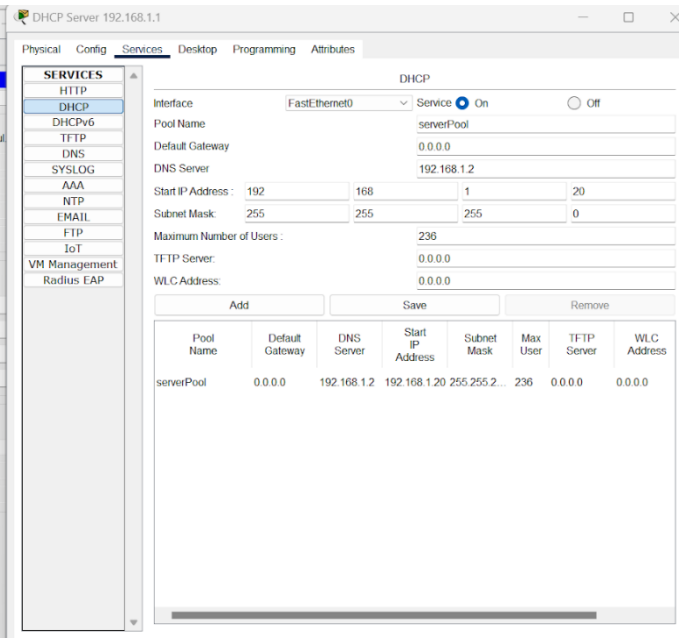
3.2. Topology

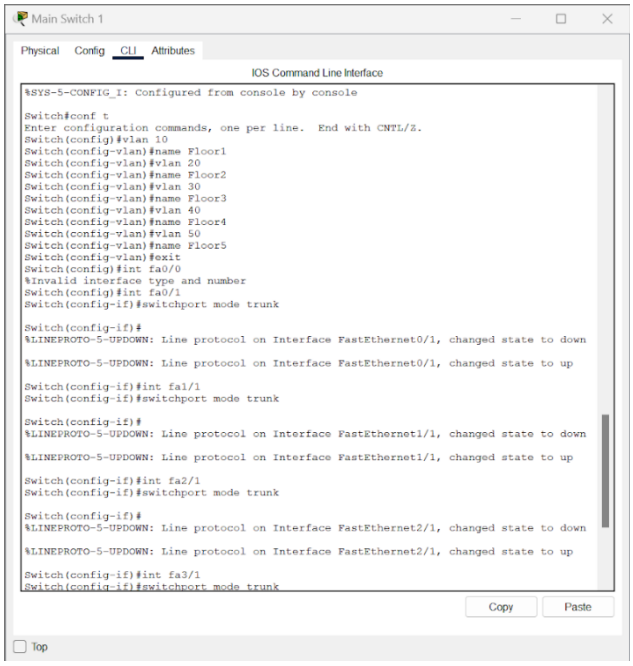
3.2.1. Configurational Steps

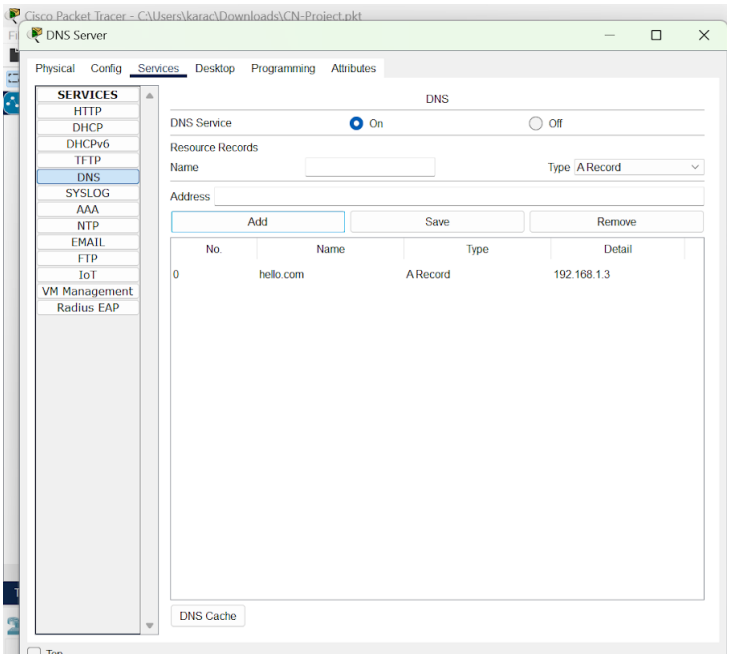


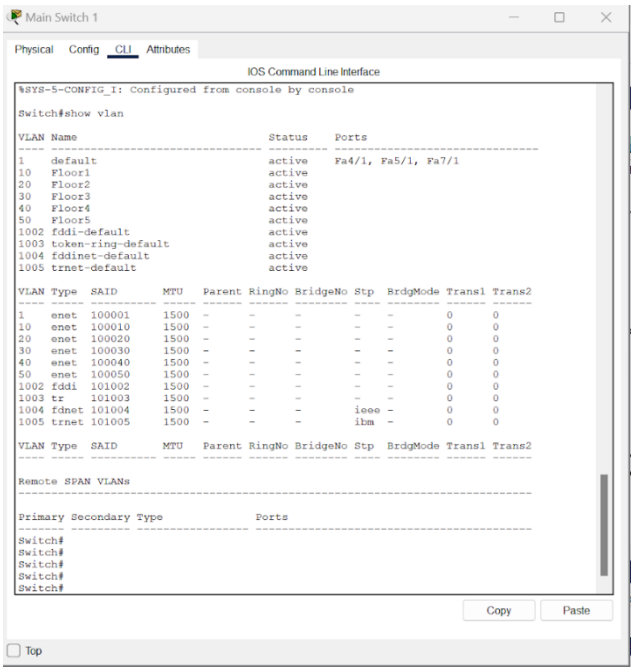


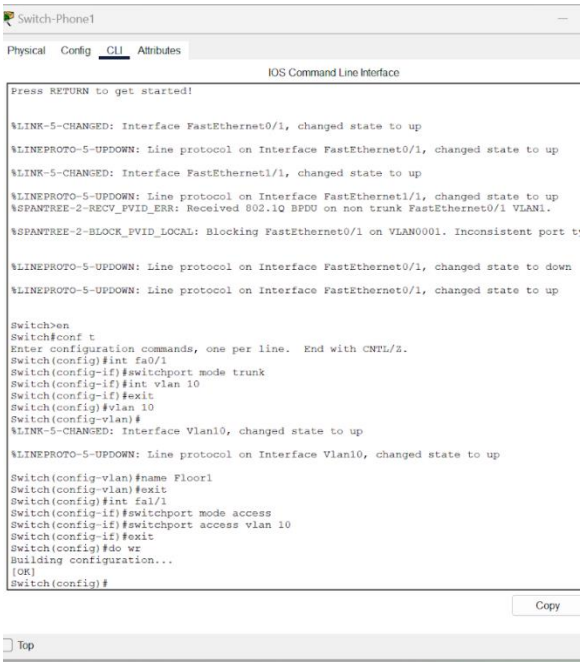

PCF1
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful
IPv4 Address 192.168.1.21
Subnet Mask 255.255.255.0
Default Gateway 0.0.0.0
DNS Server 192.168.1.2
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::203:E4FF:FE9C:5BE5
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password

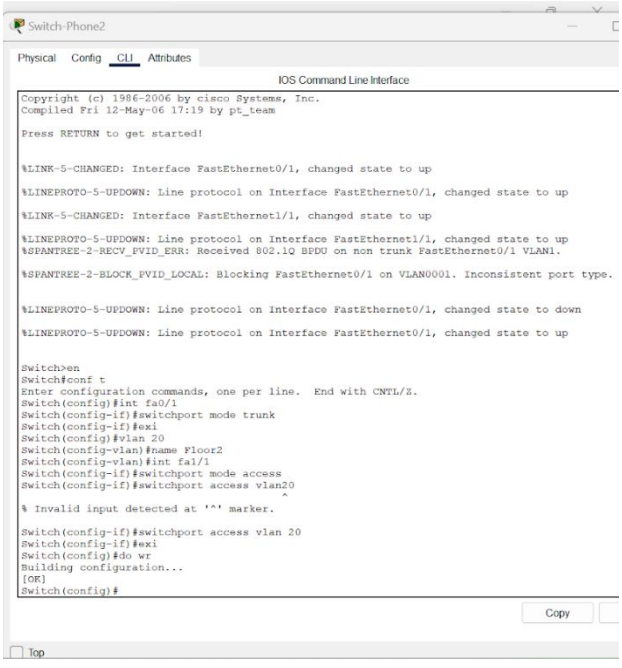

DHCP Server 192.168.1.1
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface FastEthernet0
Service On Off
Pool Name serverPool
Default Gateway 0.0.0.0
DNS Server 192.168.1.2
Start IP Address : 192 168 1 20
Subnet Mask: 255 255 255 0
Maximum Number of Users : 236
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0
Add Save Remove
Pool Name Default Gateway DNS Server Start IP Address Subnet Mask Max User TFTP Server WLC Address
serverPool 0.0.0.0 192.168.1.2 192.168.1.20 255.255.2... 236 0.0.0.0 0.0.0.0

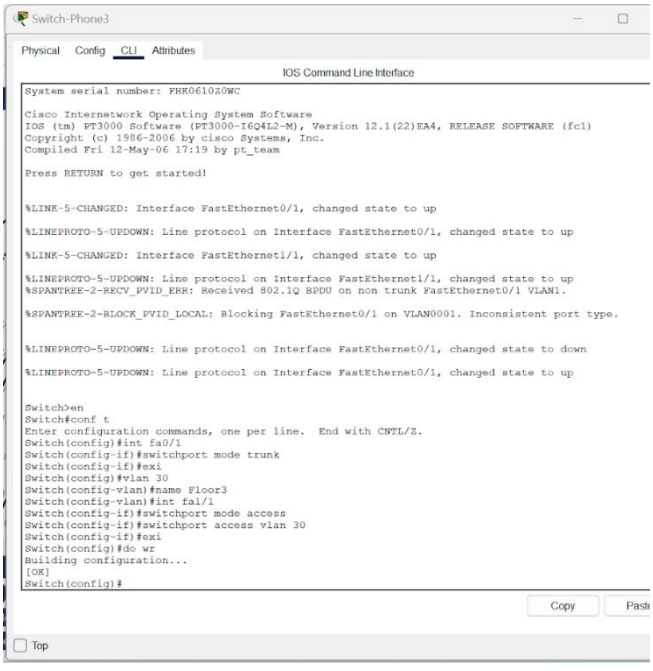

Main Switch 1
Physical Config CLI Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Floor1
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Floor2
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Floor3
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name Floor4
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name Floor5
Switch(config-vlan)#exit
Switch(config)#int fa0/0
%Invalid interface type and number
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#int fa1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
Switch(config-if)#int fa2/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to up
Switch(config-if)#int fa3/1
Switch(config-if)#switchport mode trunk
Copy Paste
Top

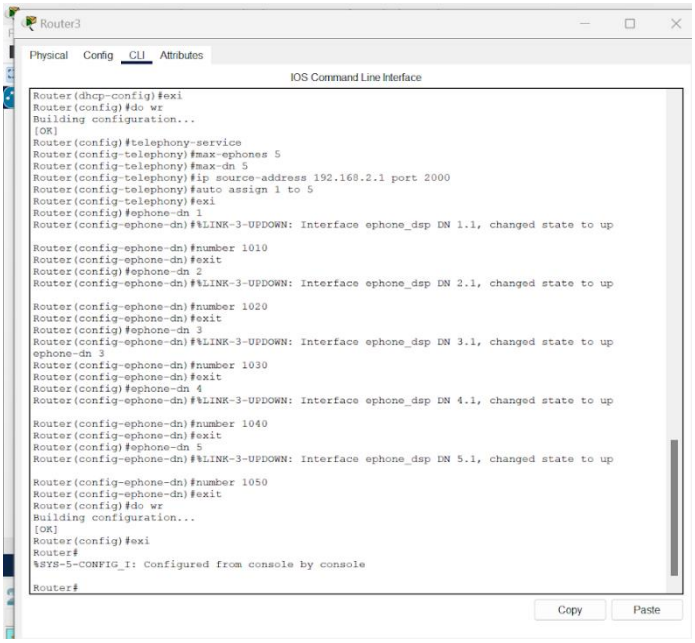

Cisco Packet Tracer - C:\Users\karac\Downloads\CN-Project.pkt
DNS Server
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service On Off
Resource Records
Name Type A Record
Address
Add Save Remove
No. Name Type Detail
0 hello.com A Record 192.168.1.3
DNS Cache

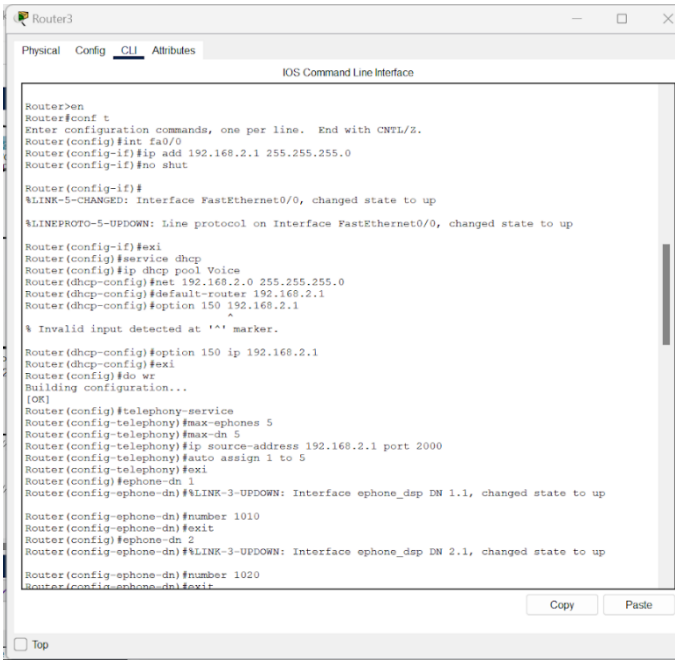

Main Switch 1
Physical Config CLI Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan
VLAN Name Status Ports
1 default active Fa4/1, Fa5/1, Fa7/1
10 Floor1 active
20 Floor2 active
30 Floor3 active
40 Floor4 active
50 Floor5 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
30 enet 100030 1500 - - - - - 0 0
40 enet 100040 1500 - - - - - 0 0
50 enet 100050 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
Remote SPAN VLANs
Primary Secondary Type Ports
Switch#
Switch#
Switch#
Switch#
Switch#
Copy
Paste
Top

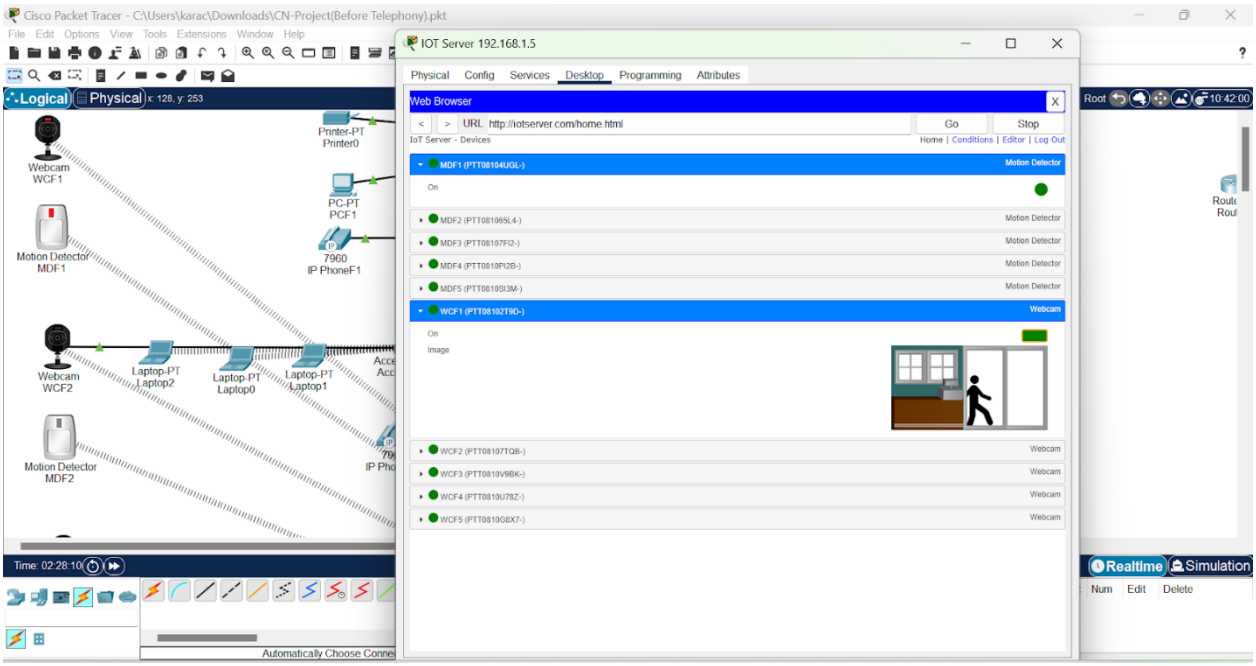

Switch-Phone1
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port t
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#int vlan 10
Switch(config-if)#exit
Switch(config)#vlan 10
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Switch(config-vlan)#name Floor1
Switch(config-vlan)#exit
Switch(config)#int fa1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
Copy
Top


Switch-Phone2
Physical Config CLI Attributes
IOS Command Line Interface
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exi
Switch(config)#vlan 20
Switch(config-vlan)#name Floor2
Switch(config-vlan)#int fa1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan20
% Invalid input detected at '^' marker.
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exi
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
Copy
Top

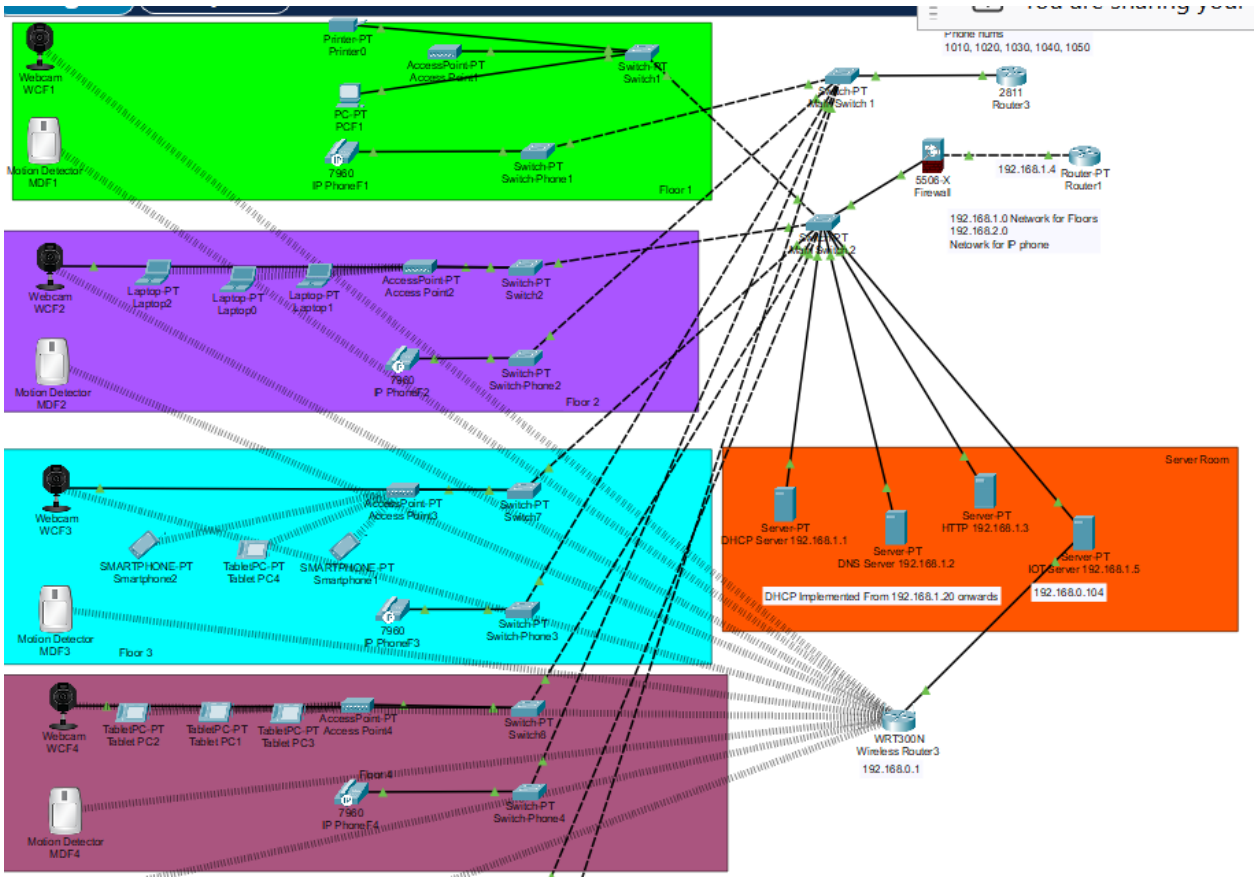

Switch-Phone3
Physical Config CLI Attributes
IOS Command Line Interface
System serial number: FHK0610Z0WC
Cisco Internetwork Operating System Software
IOS (tm) PT3000 Software (PT3000-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exi
Switch(config)#vlan 30
Switch(config-vlan)#name Floor3
Switch(config-vlan)#int fa1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exi
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
Copy
Top

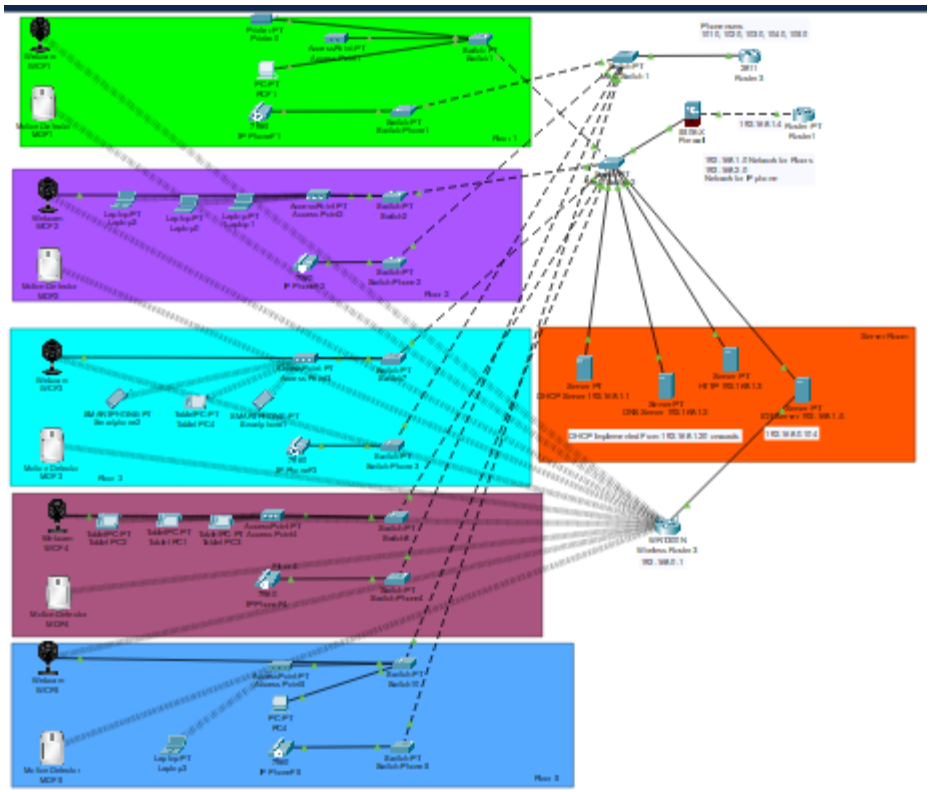

Router3
Physical Config CLI Attributes
IOS Command Line Interface
Router(dhcp-config)#exi
Router(config)#do wr
Building configuration...
[OK]
Router(config)#telephony-service
Router(config-telephony)#max-ephones 5
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.2.1 port 2000
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#exi
Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
Router(config-ephone-dn)#number 1010
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up
Router(config-ephone-dn)#number 1020
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up
Router(config-ephone-dn)#number 1030
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up
Router(config-ephone-dn)#number 1040
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 5
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state to up
Router(config-ephone-dn)#number 1050
Router(config-ephone-dn)#exit
Router(config)#do wr
Building configuration...
[OK]
Router(config)#exi
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Copy
Paste


Router3
Physical Config CLI Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exi
Router(config)#service dhcp
Router(config)#ip dhcp pool Voice
Router(dhcp-config)#net 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#option 150 192.168.2.1
^
% Invalid input detected at '^' marker.
Router(dhcp-config)#option 150 ip 192.168.2.1
Router(dhcp-config)#exi
Router(config)#do wr
Building configuration...
[OK]
Router(config)#telephony-service
Router(config-telephony)#max-ephones 5
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.2.1 port 2000
Router(config-telephony)#auto assign 1 to 5
Router(config-telephony)#exi
Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
Router(config-ephone-dn)#number 1010
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up
Router(config-ephone-dn)#number 1020
Copy
Paste
Top


Cisco Packet Tracer - C:\Users\karac\Downloads\CN-Project(Before Telephony).pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
IOT Server 192.168.1.5
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://iotserver.com/home.html
Go Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
MDF1 (PTT08104UGL-)
Motion Detector
On
MDF2 (PTT081065L4-)
MDF3 (PTT08107FI2-)
MDF4 (PTT0810PI2B-)
MDF5 (PTT0810SI3M-)
WCF1 (PTT08102T9D-)
Webcam
On
Image
WCF2 (PTT08107TQB-)
WCF3 (PTT0810V9BK-)
WCF4 (PTT0810U78Z-)
WCF5 (PTT0810G8X7-)
Webcam
Printer-PT Printer0
PC-PT PCF1
7960 IP PhoneF1
Webcam WCF1
Motion Detector MDF1
Webcam WCF2
Laptop-PT Laptop2
Laptop-PT Laptop0
Laptop-PT Laptop1
Motion Detector MDF2
Time: 02:28:10
Root
10:42:00
Realtime
Simulation
Num Edit Delete
Automatically Choose Connec

3.2.2. Full Network Topology





4. CONCLUSION

In conclusion, the implementation of an Intrusion Detection System (IDS) on Cisco Packet Tracer represents a proactive step towards enhancing network security. By leveraging Packet Tracer's capabilities, we aim to fortify network infrastructures by detecting and responding to security threats effectively. Through simulations of real-world network environments, we can evaluate the IDS's performance in identifying and mitigating various intrusions. This project empowers network administrators with a powerful tool to safeguard their networks against evolving cyber threats. Moving forward, the integration of IDS into network designs offers a crucial layer of defense, ensuring operational continuity and protecting sensitive data. As technology evolves, leveraging tools like Packet Tracer becomes essential in staying ahead of cyber threats and maintaining a robust security posture in interconnected environments.

5. REFERENCES

- Taşdelen, K. (2004). Interactive based, Interactive, Virtual Microcontroller , Laboratory Design for Engineering Education, Graduate Thesis, Süleyman Demirel University, Institute of Science, Isparta.

- Jakab František, Janitor Jozef, Visual Learning: Case Study of Cisco Networking Academy's PACKET TRACER 5.0 Application, Proc. Of 6th International Conference on Emerging eLearning Technologies and Applications

- Odom, W. (2004). Computer Networking first-step. Cisco Pres

- https://www.youtube.com/watch?v=_sr9yTw20FU