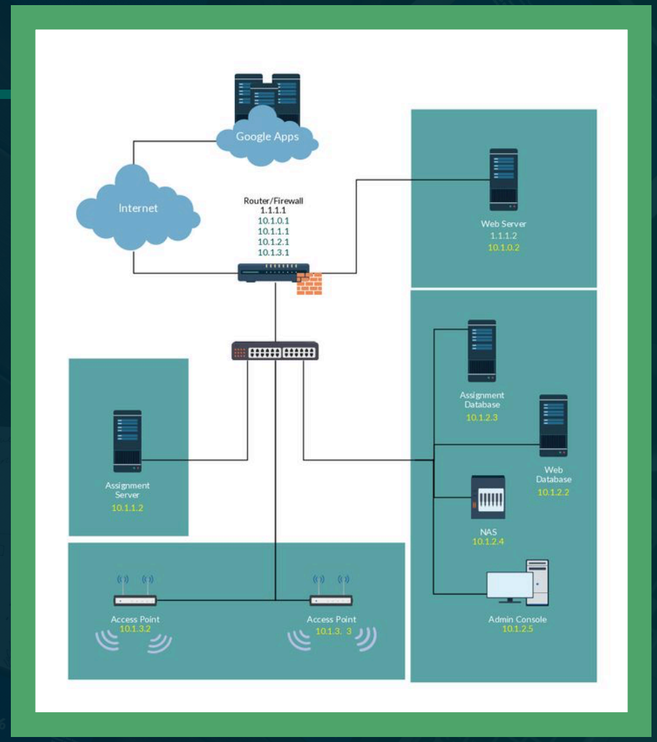
RAW Office Communications (Only Restricted within Building)

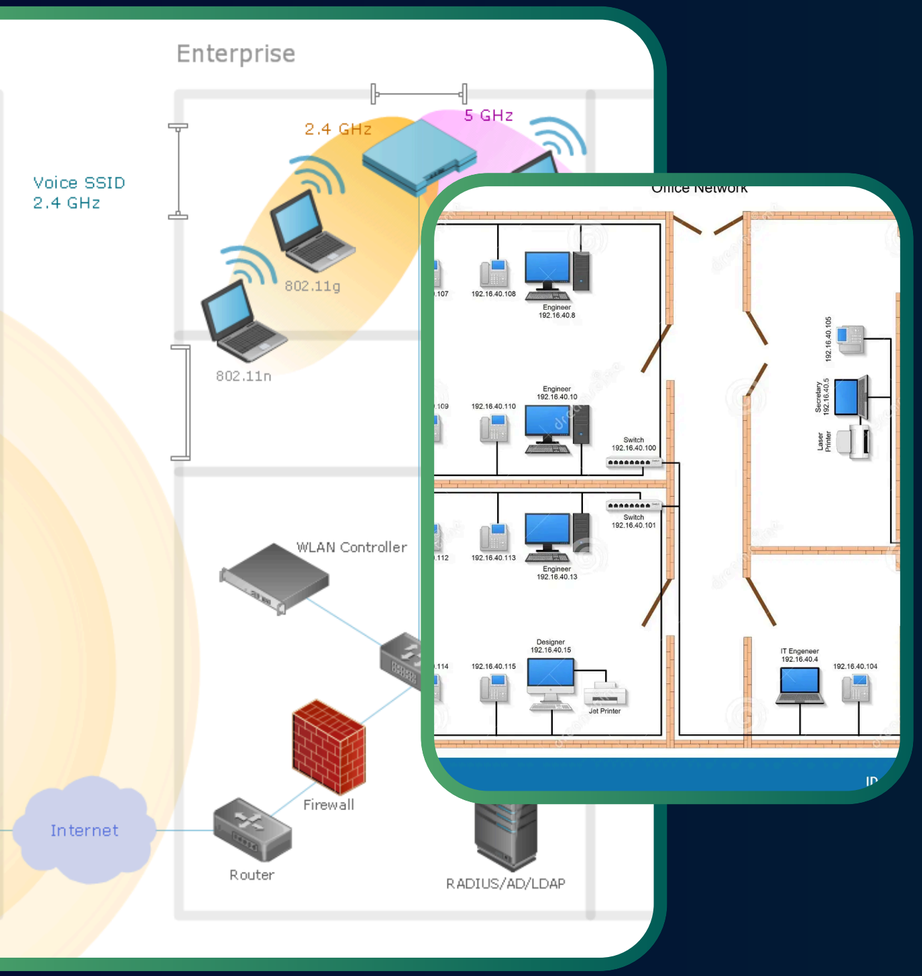
COMPUTER NETWORKS



Presented by:
E072- Manognaa Vakkalanka
E074- Hrishikesh Vartak
E075- Rashi Viz

CONTENTS

INTRODUCTION



The "RAW Office Building Communications" project envisions a closed-loop network system that is exclusively restricted to the internal operations of a physical office building.

It is a simulation of how a real-life office infrastructure might deploy a secure, reliable, and compartmentalized computer network to ensure seamless communication among employees, departments, and systems, without exposing the network to external threats.

The design emphasizes isolation, control, and security, aligning with modern cybersecurity best practices, especially in environments like military offices, R&D departments, financial institutions, and critical infrastructure.

REQUIREMENT OF THE CASE/SCENARIO

- Data sharing, VoIP, file transfer, and device access (printers, servers) occur only within the physical premises.
- Network access is controlled, monitored, and segmented (e.g., employees, IT team, management).
- Scalability and future readiness must be factored in to handle expansion and integration of smart office components.

- Confidentiality: Prevent data leaks outside the building.
- Integrity: Ensure data is not tampered with in transmission.
- Availability: Guarantee continuous communication within the office even during external outages.

Confidentiality

Prevent data leaks outside the building.

Firewall Protection

Use of internal firewalls (e.g., ASA) to restrict inter-departmental access and enforce security policies.

Access Control

Strict restrictions based on role or department.

Network Configuration

Devices used

- Routers and multilayer switches for routing and inter-VLAN communication.
- Cisco ASA 5505 firewall for inspecting and controlling traffic flow.
- Layer 2 switches for department-wise segmentation.
- DHCP server (optional, or static IPs for full control).
- End devices: desktops, VoIP phones, printers, etc

Security Mechanisms

- VLANs: Segregate departments.
- ACLs: Control access between VLANs.
- ASA Firewall Rules: Inspect traffic and enforce access policies.
- MAC Filtering: Allow only authorized devices to connect.
- No External Gateway: Default gateway is internal router/firewall; internet traffic is blocked.

Optional Enhancements

- Internal DNS and email servers.
- Local authentication (RADIUS/TACACS) for admin users.
- Failover router/firewall for redundancy.

Network Size

The network’s size is based on the current and future occupancy of the building. Since it's a raw office building, planning includes scalability.

Assumptions:

- 3 Floors with 4 departments per floor.
- Around 20 devices per department → 240 client devices.
- Additional 30 infrastructure devices (servers, switches, etc.)
- VoIP system for internal calls.

Categorization:

- Small-to-Medium Enterprise (SME) Network.
- Total Endpoints: ~270-300.
- Scalability: Structured to scale up to 500+ devices as the building becomes operational.

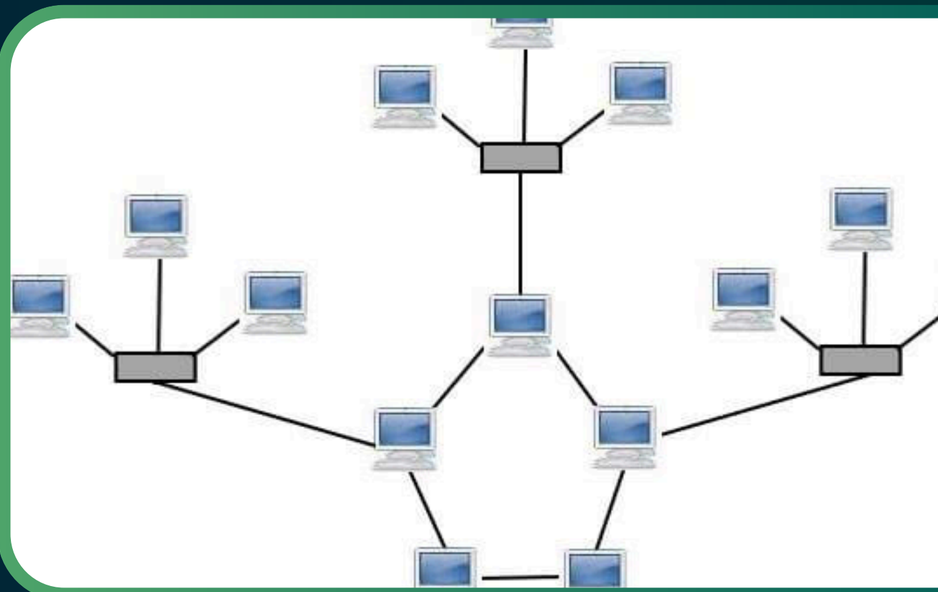
Network Topology

Star Topology (within departments)

- Each department's devices connect to a central switch.
- Easy to manage and isolate faults.

Hierarchical Topology (building-wide)

- Core router and ASA firewall sit at the top.
- Distribution layer (per floor switch/router).
- Access layer (department switches).
- Enables scalable design and layered security.



Benefits of This Topology:

Modular design: Easier to add or remove departments/floors.

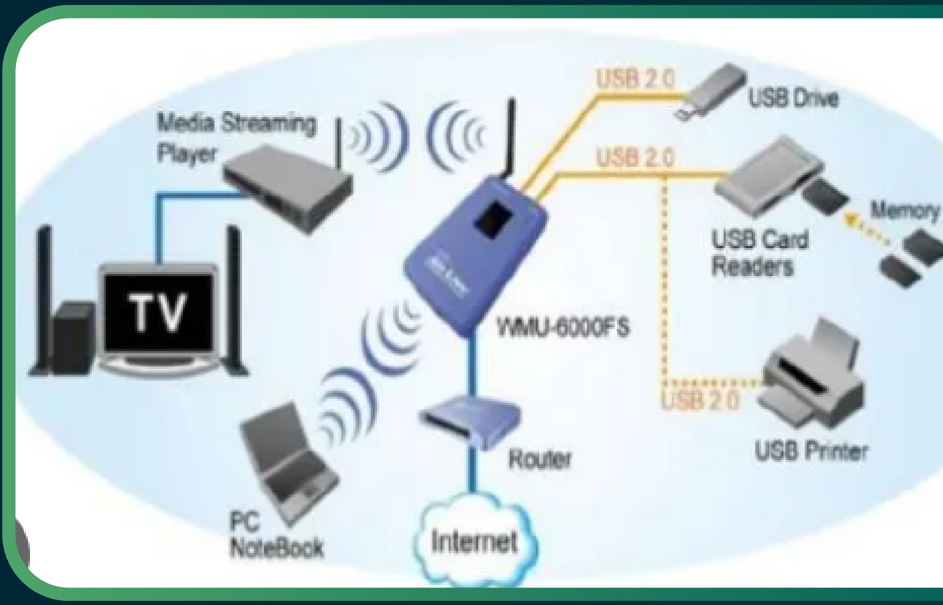
Fault tolerance: Issue in one VLAN doesn’t affect others.

Logical segmentation: Helps with implementing ACLs, monitoring, and control.

Enhanced security: Traffic can be inspected and filtered at multiple points.

Transmission Medium

The transmission medium plays a critical role in ensuring reliability, speed, and physical security.



1. Wired (Primary Medium):

Ethernet (Cat6/Cat6a/Cat7): For workstations & switches

Fiber Optic: For high-speed backbone links

🛡️ Benefits: More secure, faster, and less interference

2. Wireless (Controlled/Optional):

Wi-Fi (802.11ac/ax): Limited use with WPA3 & MAC filtering

🛡️ Often VLAN-isolated or disabled for security

Nodes in the Network

End Devices

- Desktop PCs / Laptops (used by employees)
- VoIP Phones (for internal calling)
- Printers / Scanners (shared departmental resources)
- Internal Servers (file servers, DNS, internal email, application servers)

Networking Devices

- Layer 2 Access Switches (in each department)
- Layer 3 Switch or Core Router (centralized control)
- Cisco ASA / NGFW (Next-Gen Firewall for segmentation and protection)
- Wireless Access Points (if used, VLAN-separated)
- DHCP, DNS, and Syslog Servers

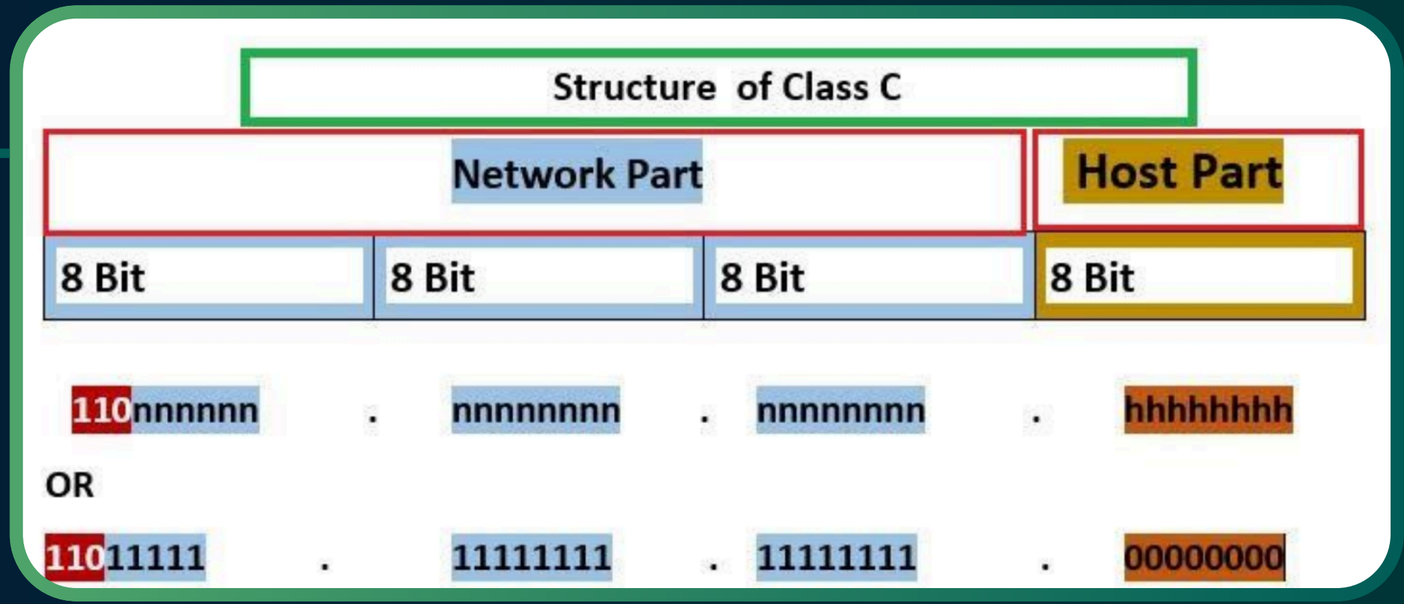
Security / Admin Devices:

- Monitoring tools (SIEM, SNMP collectors)
- Authentication servers (RADIUS/TACACS)
- Backup Servers or NAS devices (with isolated access)

IP Class Range

Suggested IP Class Range with Justification

The recommended IP class for this office network is Class C (192.168.X.X/24).



Reasons-

1. This is a private IP range, meaning it is restricted to internal use and does not allow direct external access.
2. It supports up to 254 devices per subnet, which is sufficient for an office building.
3. It prevents unnecessary IP wastage and allows for easy subnetting if required in the future.

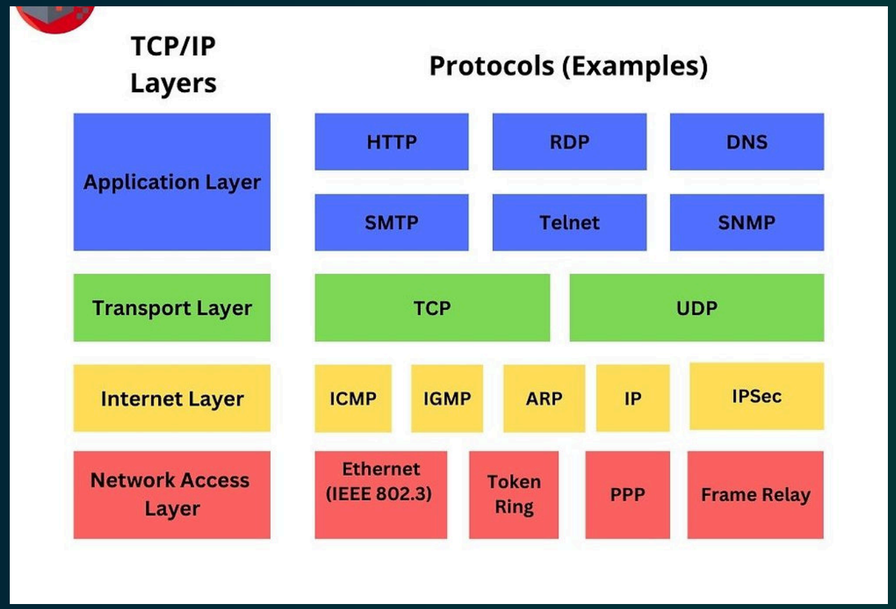
Protocol Model

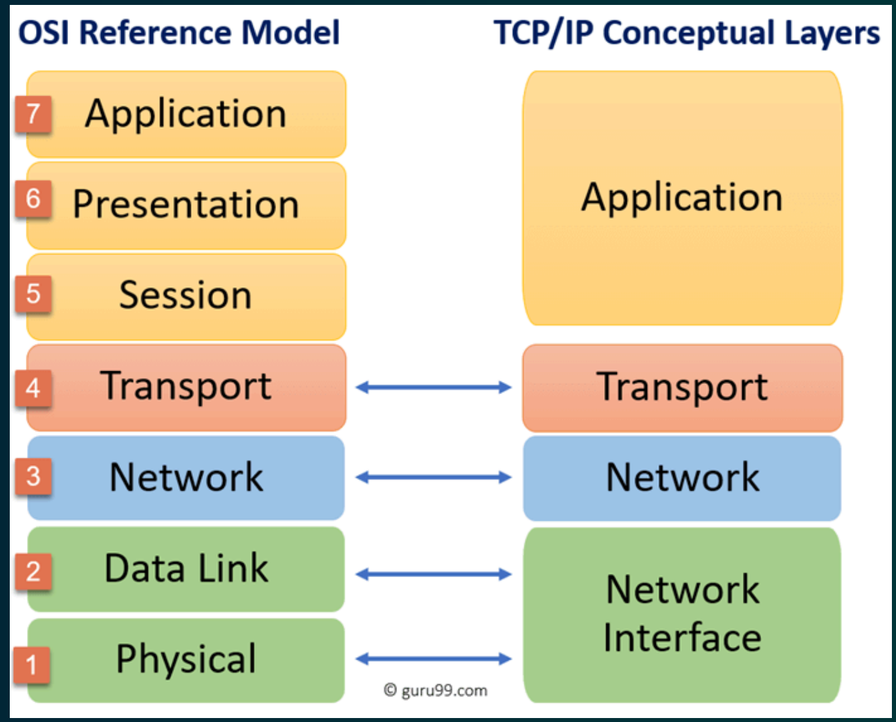
In real-world enterprise networks, the communication is designed using the TCP/IP Protocol Suite layered against the OSI Model.

- Network Layer: IPv4 will be used for addressing, though IPv6 could be considered for future expansion.
- Transport Layer: TCP is used for reliable communication, while UDP may be used for real-time applications like VoIP.
- Application Layer: Several protocols will be required:

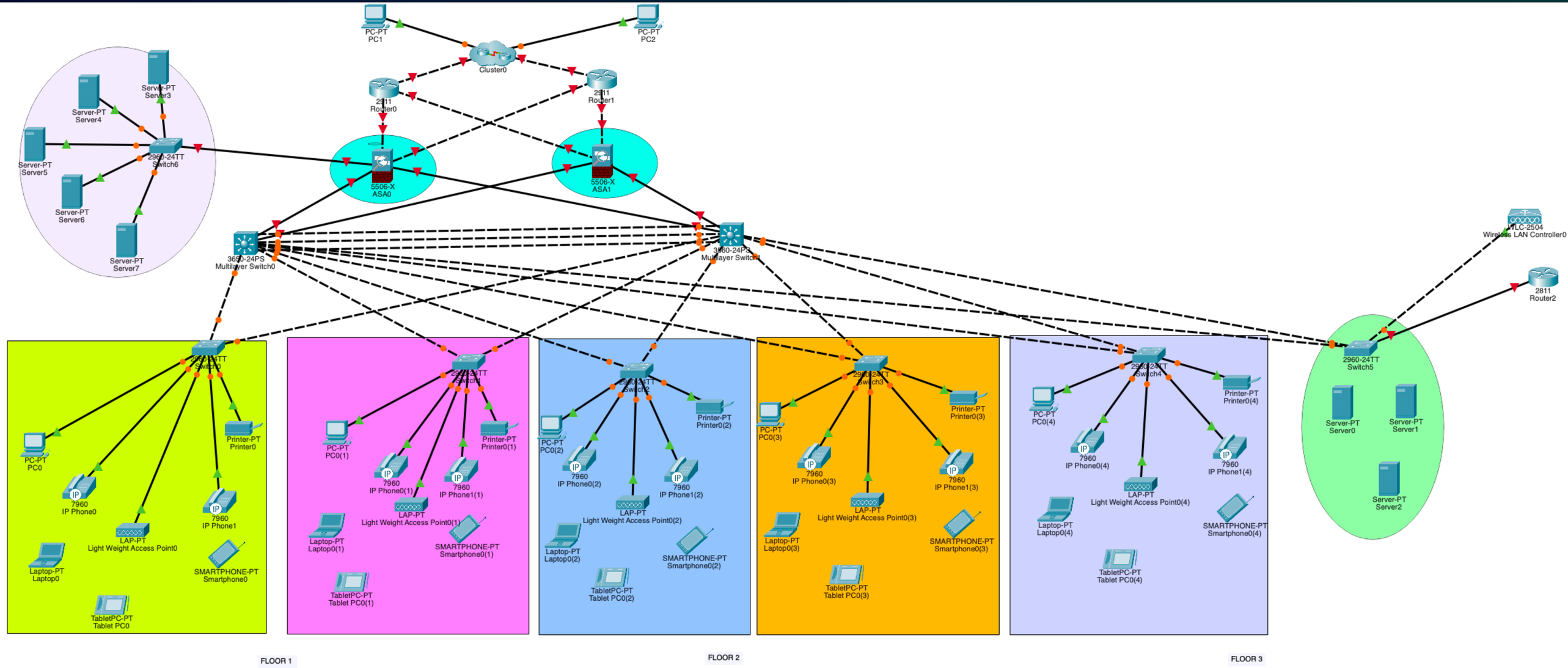
1. HTTP/HTTPS for internal web applications and document sharing.
2. SMTP/IMAP for email communication.
3. SMB (Server Message Block) for file sharing between employees.

This network setup ensures a secure, efficient, and scalable communication system within the RAW office building.





ARCHITECTURE DIAGRAM



FEATURES

Inter-Departmental Communication

Secure network for calls and messages

Multiple devices configured

Efficiency and Effectiveness

COMPONENTS

Firewall 5506 – Protects the internal network by controlling incoming and outgoing traffic, ensuring secure communication within the office.

Router 2911 – Connects different network segments within the office and directs internal data traffic efficiently.

Switch 2960 – Connects multiple wired devices within the office network, enabling seamless internal communication.

Switch 3560 (Multilayer Switch) – Combines switching and routing functions to manage complex internal office networks with high performance.

PC – Standard workstations for employees to access internal applications and communicate over the office network.

COMPONENTS

Printer – Networked printer for internal document printing and sharing across the office network.

IP Phone 7960 – Provides secure voice communication over the office's internal IP network.

LAP-PT (Lightweight Access Point) – Extends internal wireless coverage within the office for mobile connectivity.

Laptop – Portable computing device for employees to work and communicate over the internal office network.

Smartphone – Enables secure, mobile access to internal communication tools and services within the office.

COMPONENTS

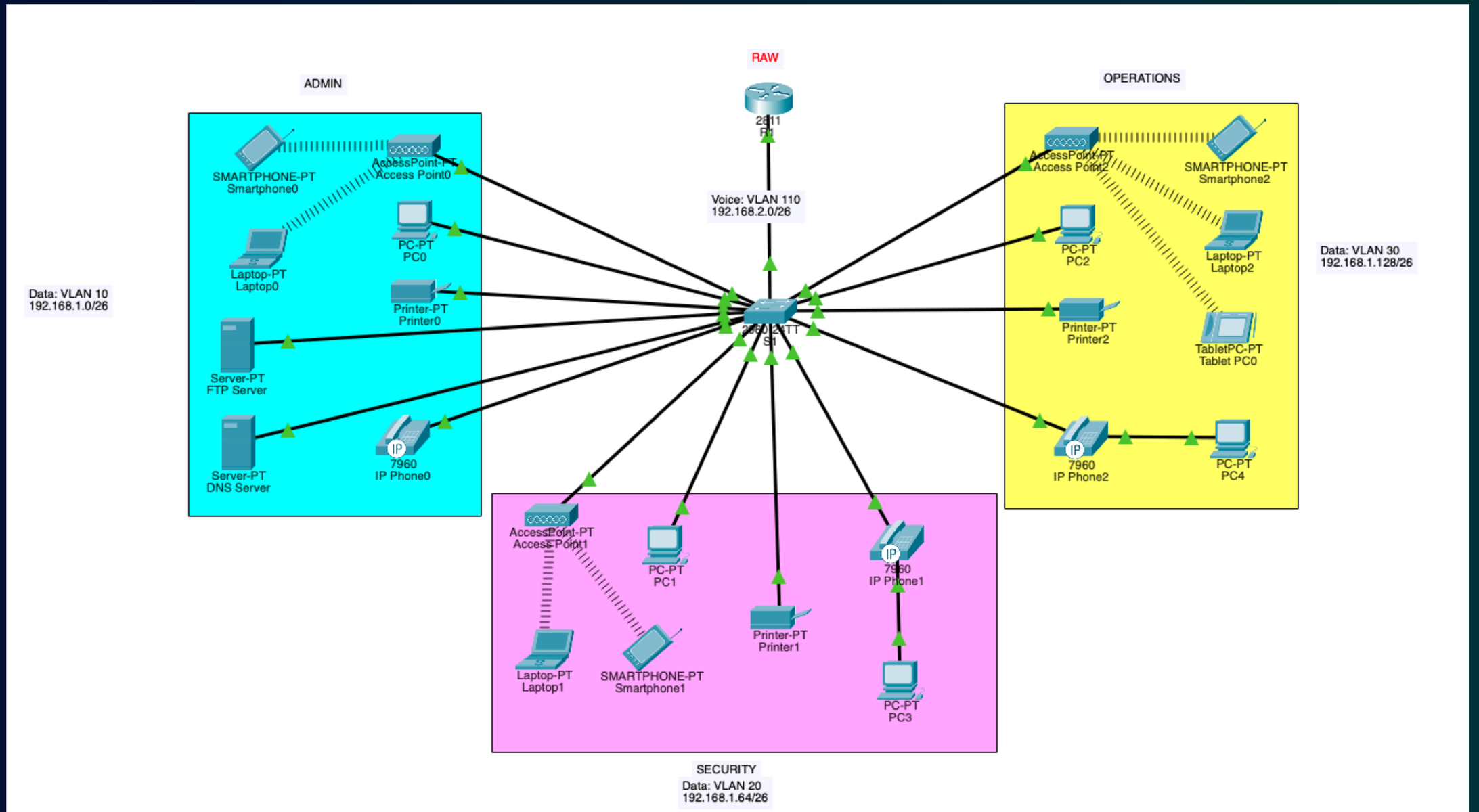
Tablet – Provides portable access to internal systems and communication tools for office mobility.

Server – Hosts internal applications, files, and services, centralising data access for office users.

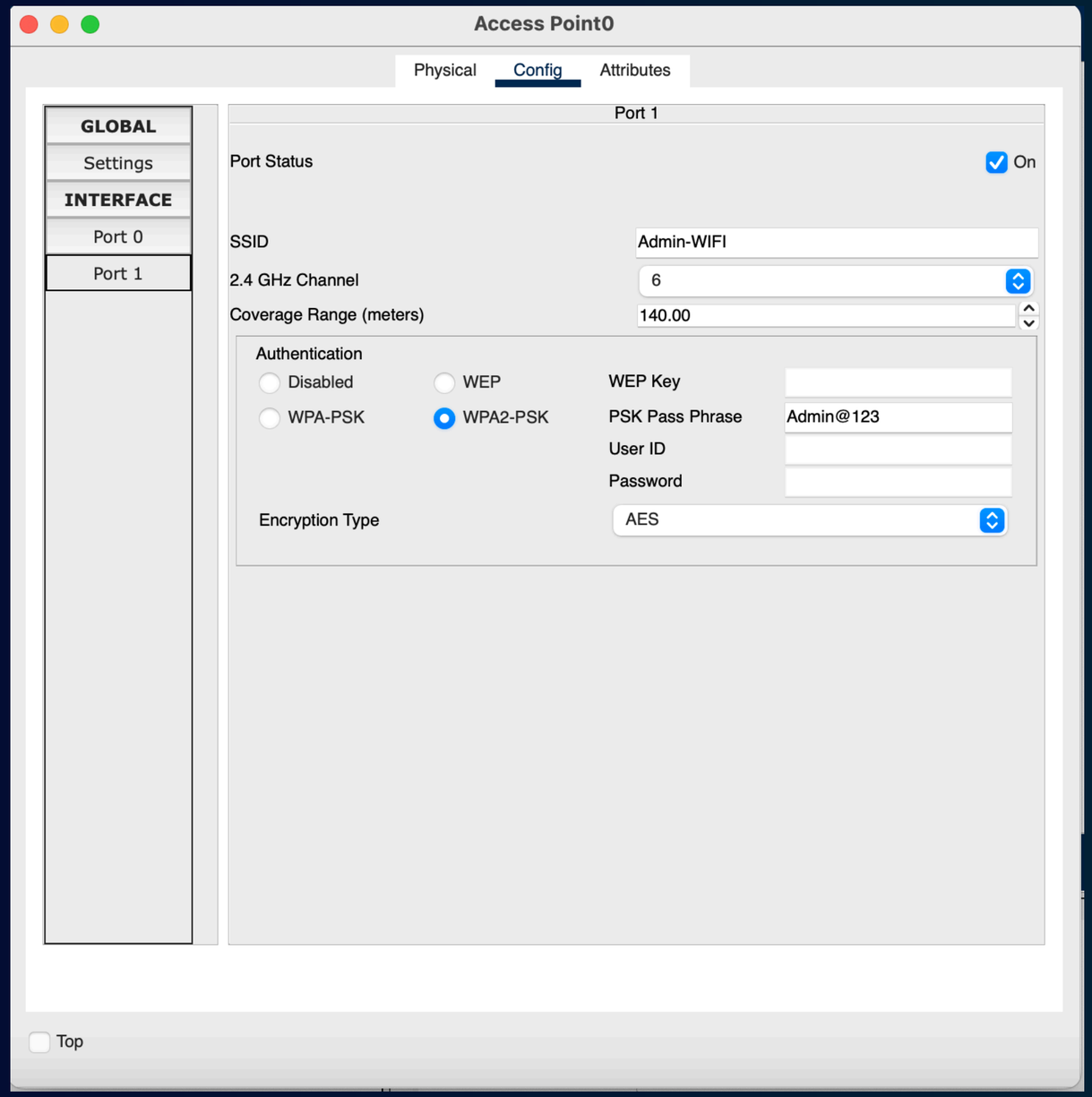
WLC (Wireless LAN Controller) – Manages and secures all office wireless access points for reliable internal connectivity.

Router 2811 – Connects and manages communication between different internal office networks securely and efficiently.

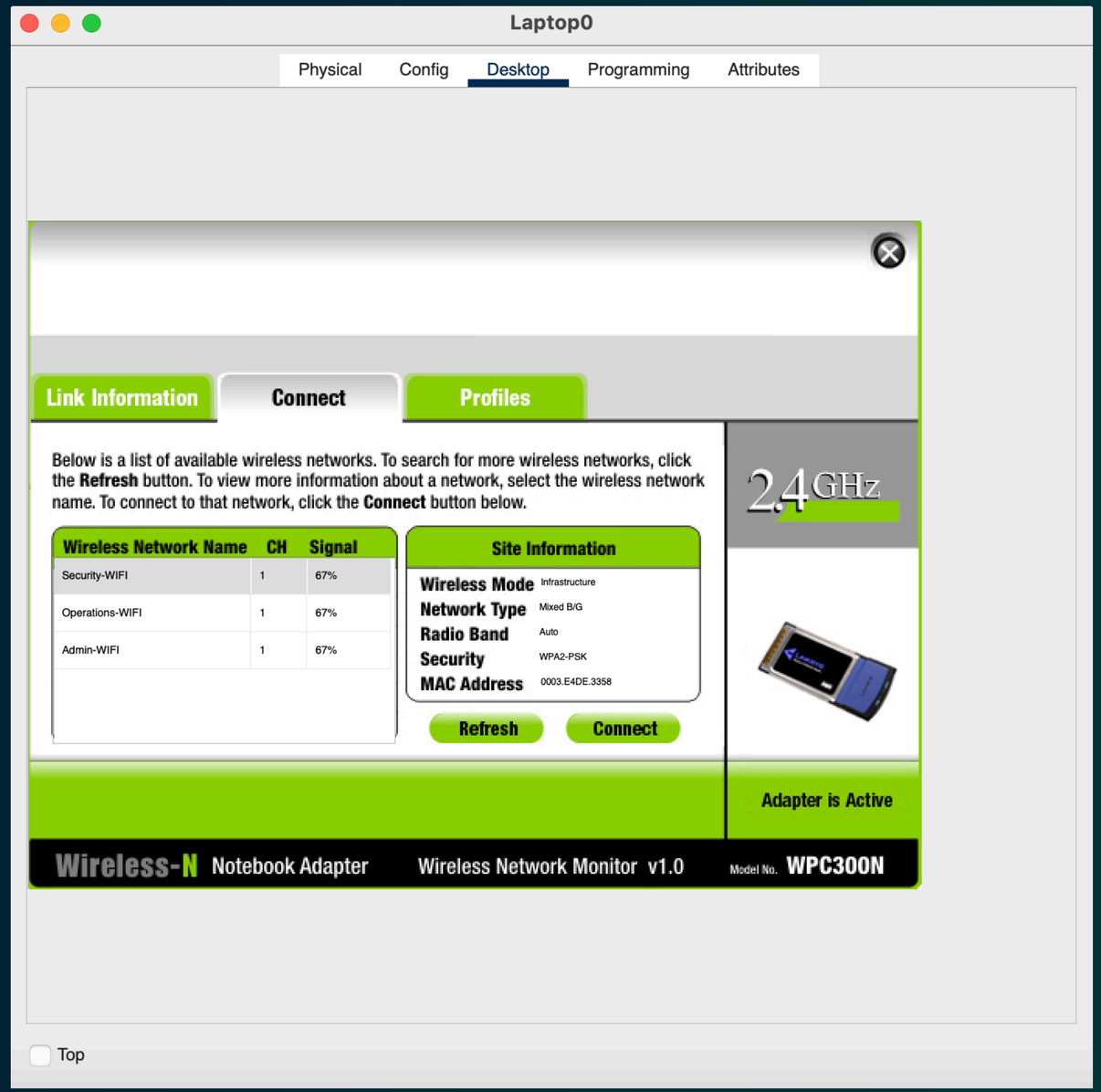
SIMULATION - CISCO PACKET TRACER



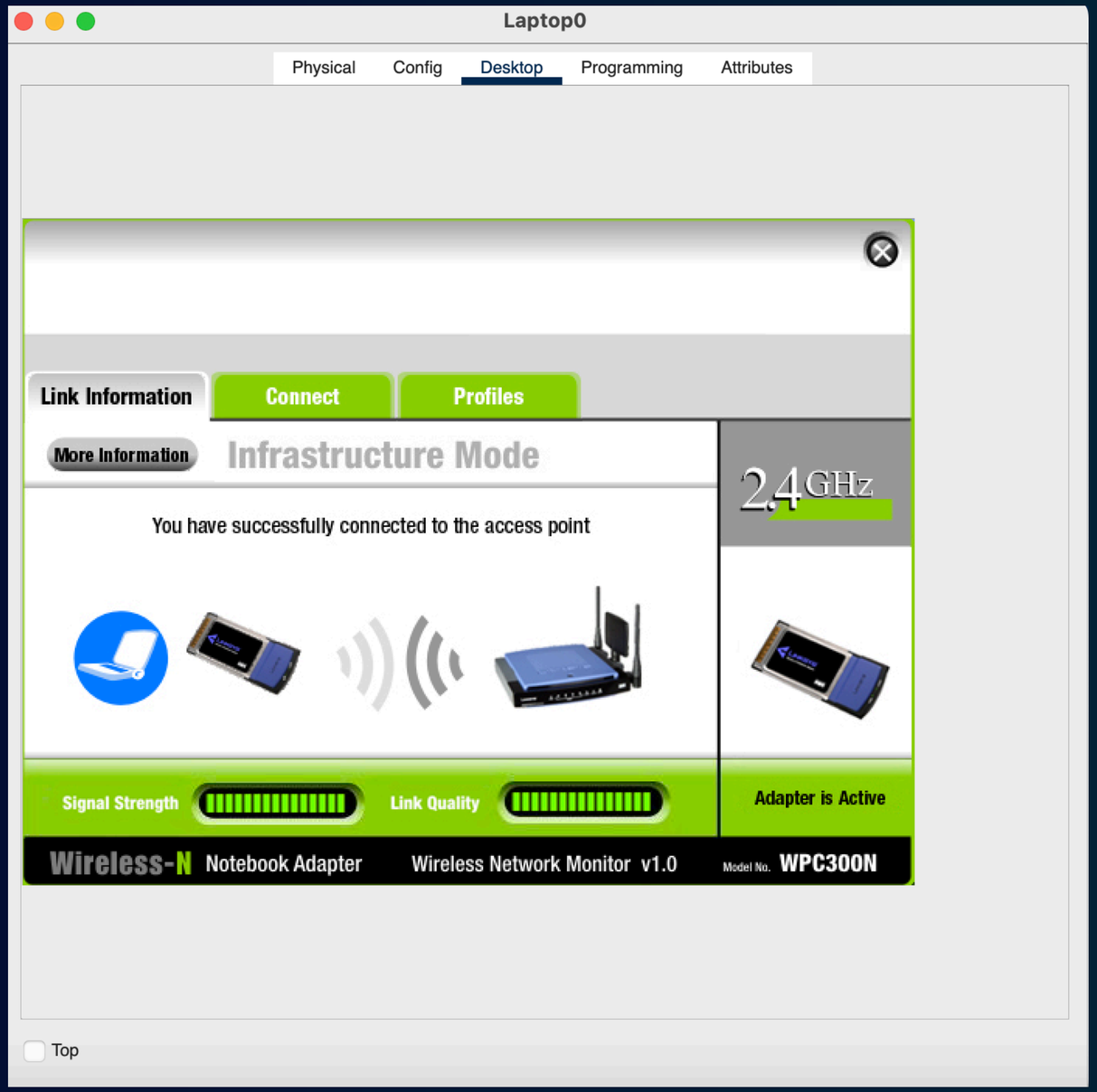
WIFI SETTINGS

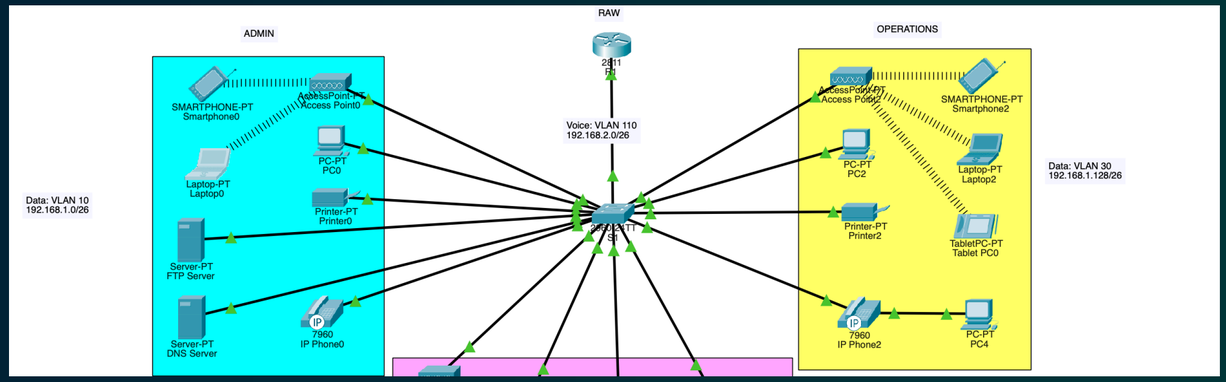


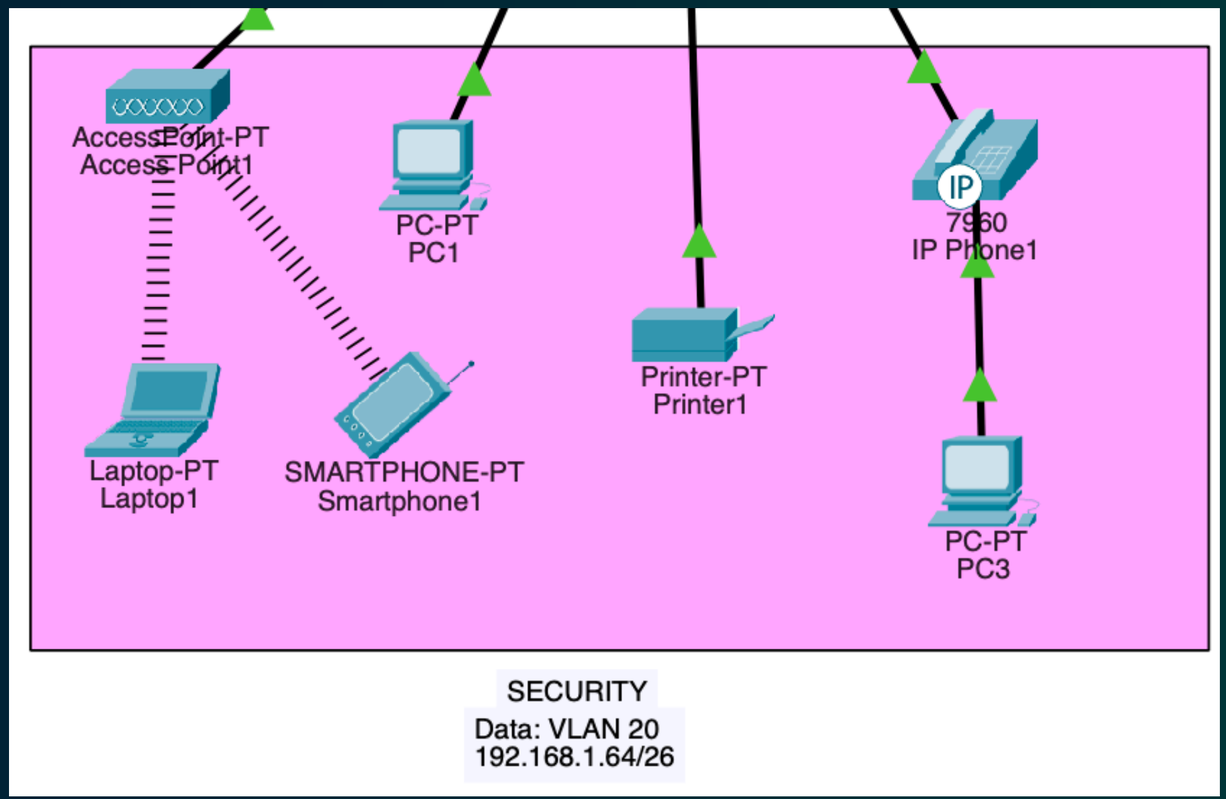
WIRELESS CONNECTION



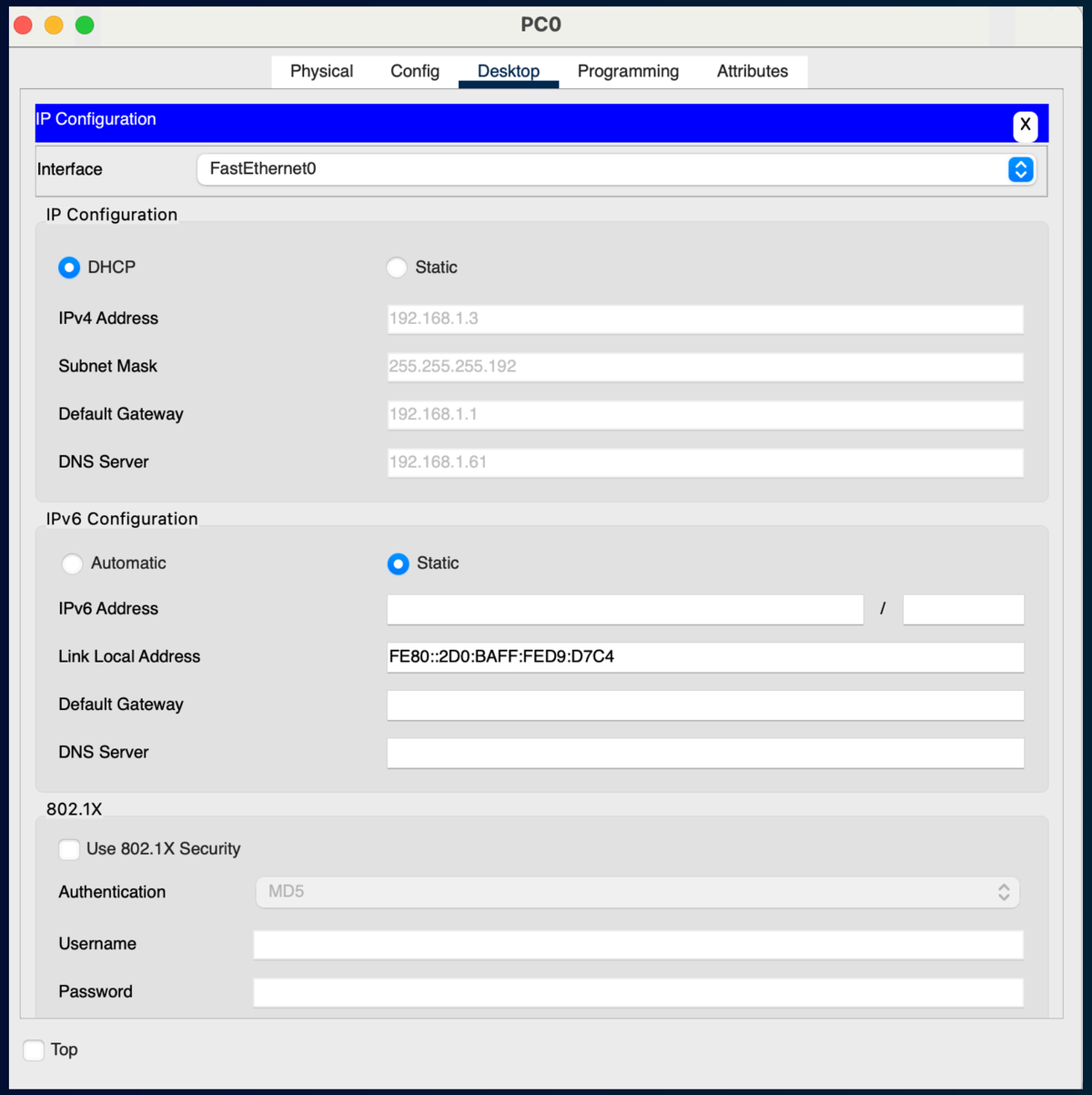
WIRELESS CONNECTION

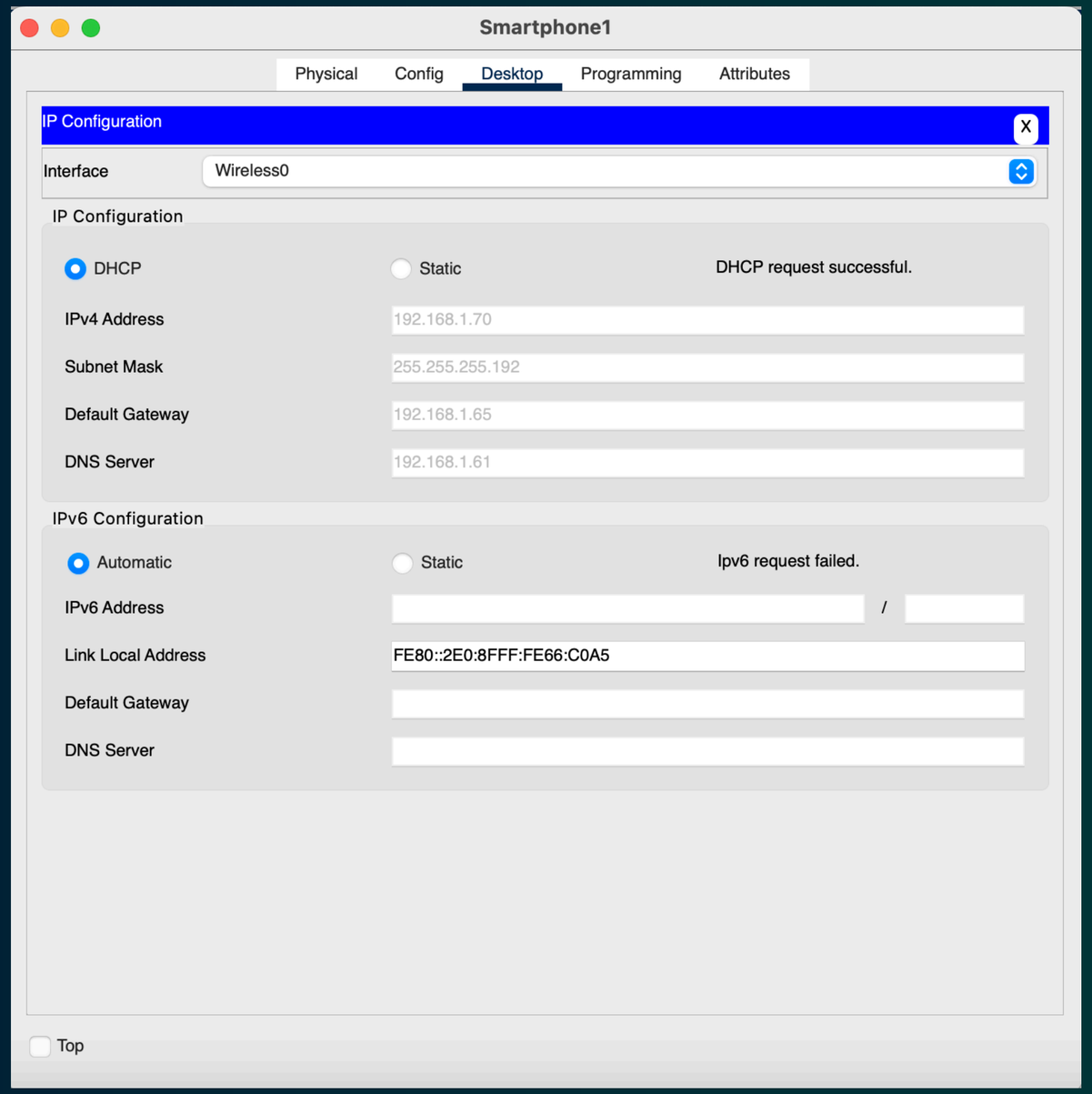




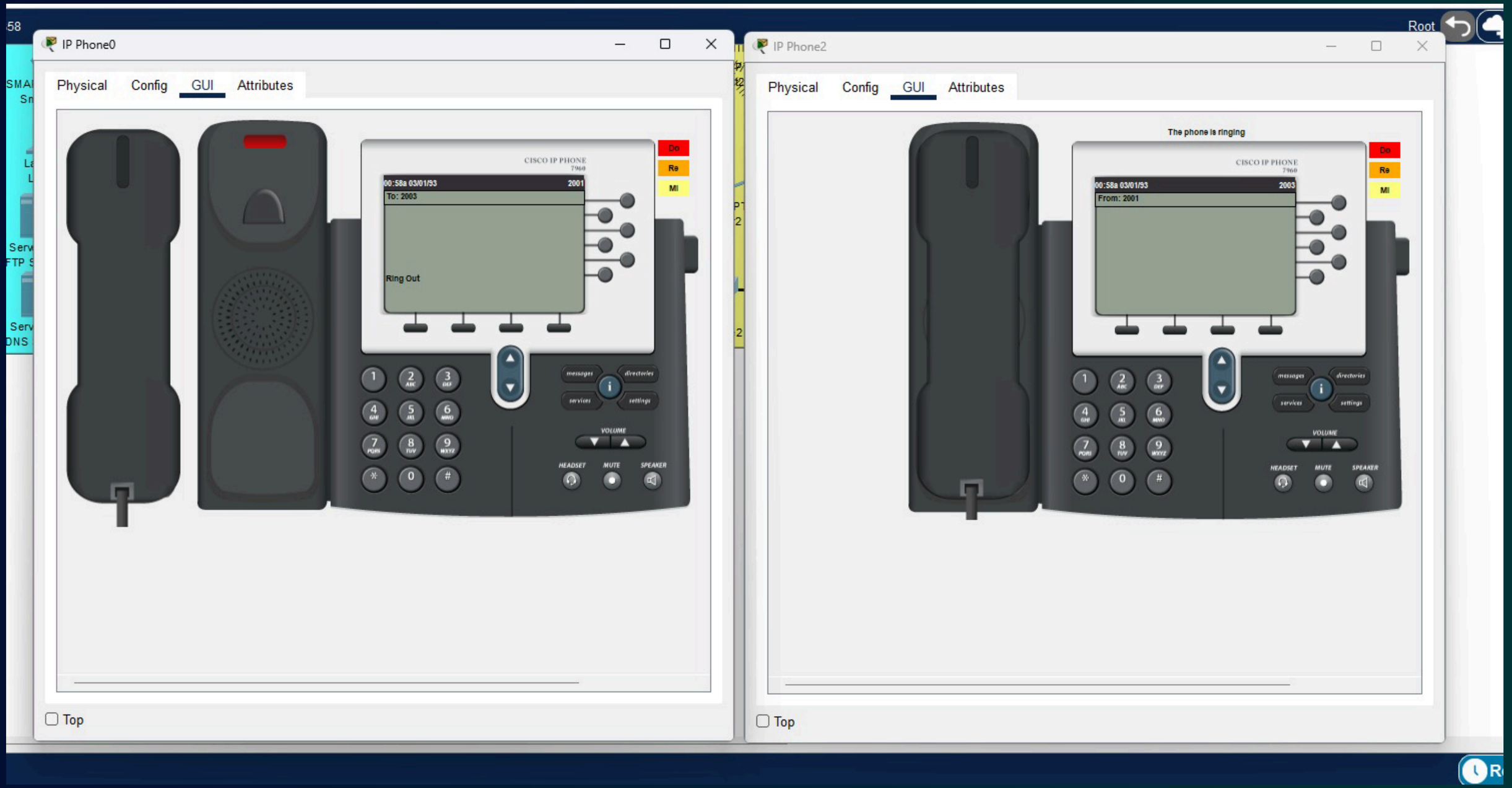


IP CONFIGURATION





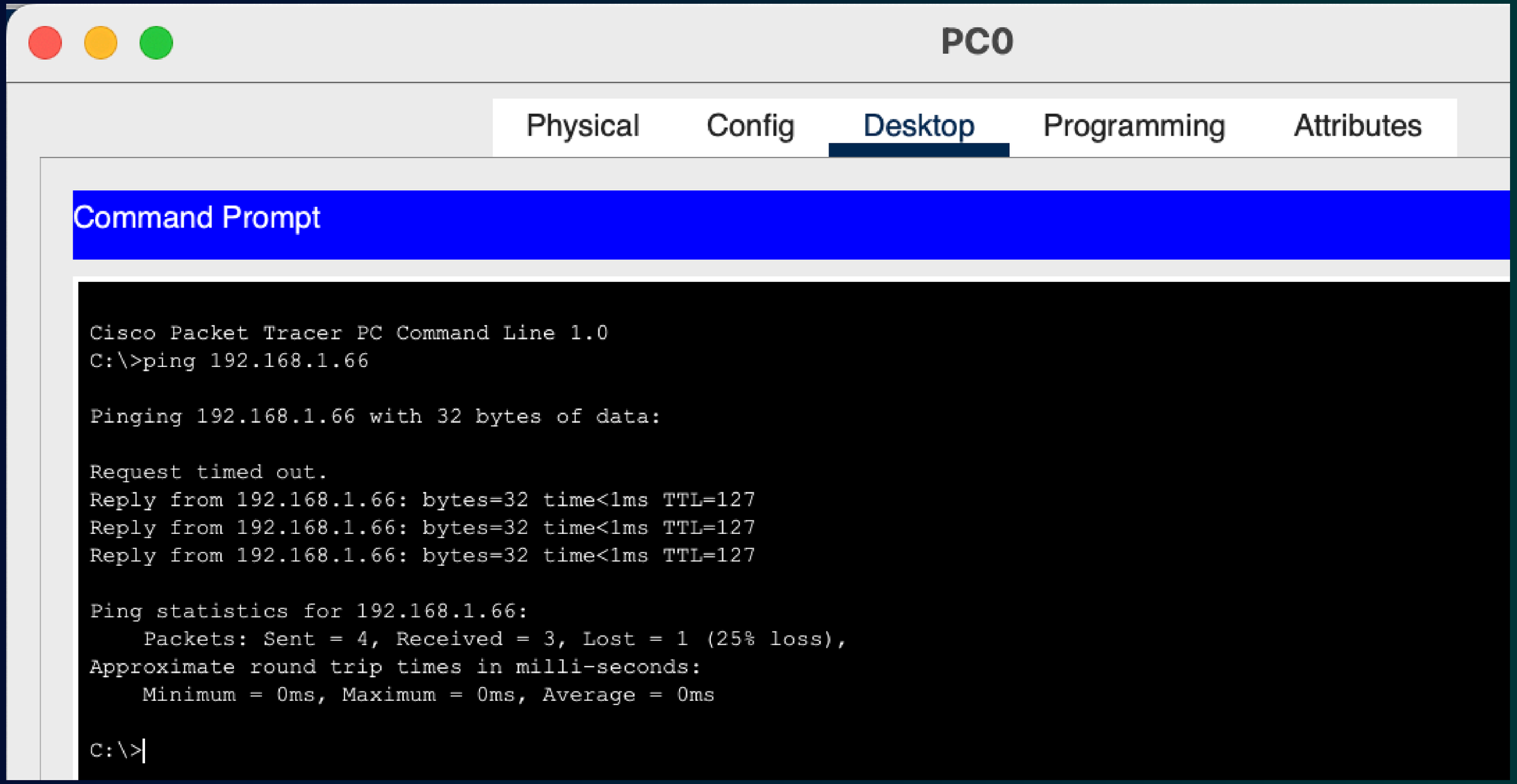
IP PHONE


IP Phone0
Physical
Config
GUI
Attributes
CISCO IP PHONE
7960
00:58a 03/01/93
2001
To: 2003
Ring Out
Do
Re
Mi
messages
directories
services
settings
VOLUME
HEADSET
MUTE
SPEAKER
Top
IP Phone2
Physical
Config
GUI
Attributes
The phone is ringing
CISCO IP PHONE
7960
00:58a 03/01/93
2003
From: 2001
Do
Re
Mi
messages
directories
services
settings
VOLUME
HEADSET
MUTE
SPEAKER
Top
Root

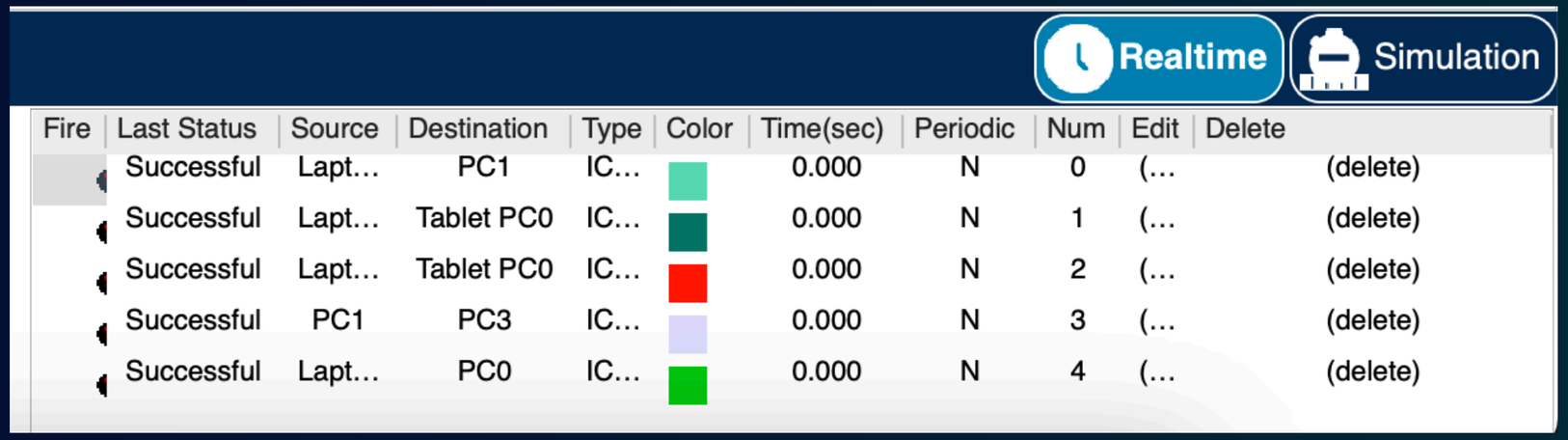
IP PHONE

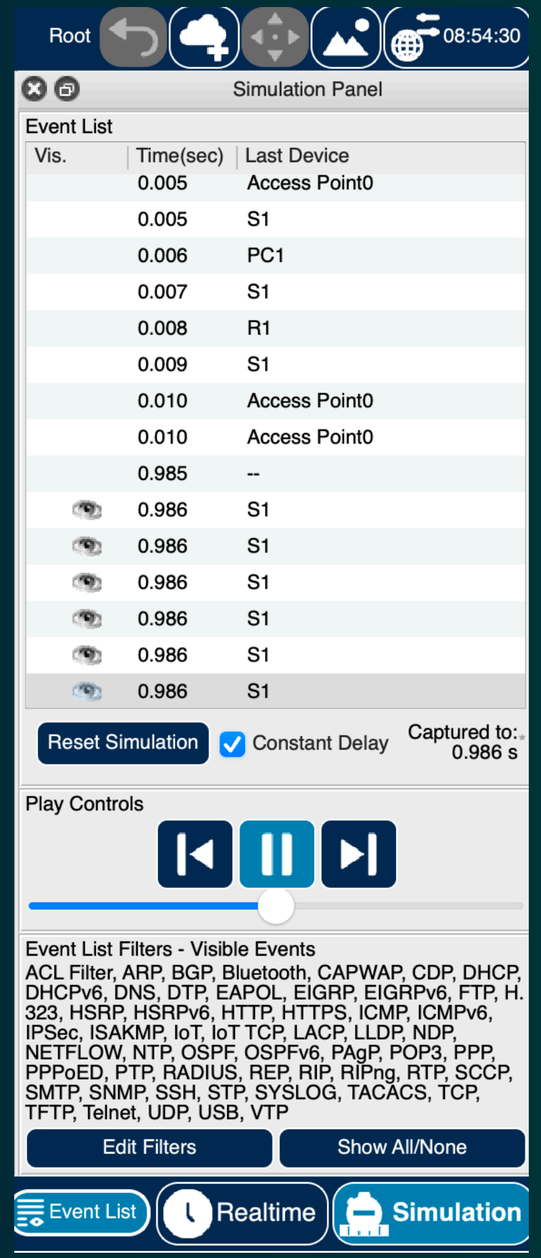

IP Phone0
Physical
Config
GUI
Attributes
CISCO IP PHONE
7960
00:59a 03/01/93
2001
To: 2003
Connected
Do
Re
Mi
messages
directories
services
settings
VOLUME
HEADSET
MUTE
SPEAKER
Top
IP Phone2
Physical
Config
GUI
Attributes
CISCO IP PHONE
7960
00:59a 03/01/93
2003
From: 2001
Connected
Do
Re
Mi
messages
directories
services
settings
VOLUME
HEADSET
MUTE
SPEAKER
Top
Root

COMMUNICATION



PACKET TRANSFER





FTP SERVER

Tablet PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Ping statistics for 192.168.1.62:
    Packets: Sent = 4, Received = 4
loss),
Approximate round trip times in mil
    Minimum = 18ms, Maximum = 33ms,

C:\>ftp raw-ftp.com
Trying to connect...raw-ftp.com
Connected to raw-ftp.com
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
```

FTP Server

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

DHCP Static

IPv4 Address 192.168.1.62

Subnet Mask 255.255.255.192

Default Gateway 192.168.1.1

DNS Server 192.168.1.61

IPv6 Configuration

Automatic Static

IPv6 Address /

Link Local Address FE80::260:2FFF:FEA1:DD0A

Default Gateway

DNS Server

802.1X

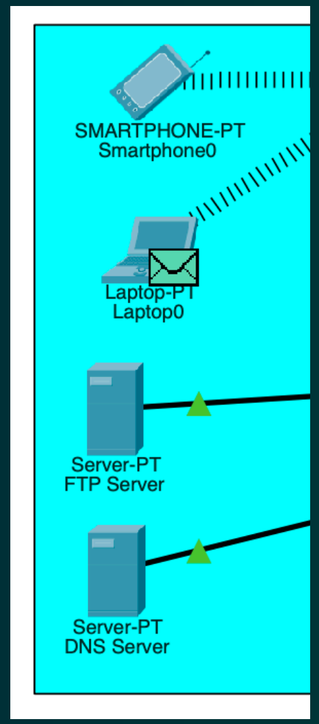
Use 802.1X Security

Authentication MD5

Username

Password

Top



REFERENCES

- https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5530-set-up-a-wireless-network-using-a-wireless-access-point-wap.html

- https://computernetworking747640215.wordpress.com/2019/11/22/how-to-configure-an-ftp-server-in-packet-tracer/

- https://www.packettracernetwork.com/tutorials/voipconfiguration.html

Thank You!