Network Design and Evaluation for Bay Resort Hotels

Date: 17/01/25
Unit: COMMUNICATIONS AND NETWORKING (COMP5071)

Executive Summary

This paper seeks to improve Bay Resort Hotels' network to enhance operations and guest experience. I created a secure Cisco Packet Tracer network that simulates connecting guest devices and front desk PCs. The paper describes how my network will handle check-ins, communicate with the corporate headquarters in London and their regional headquarters near Southampton, and provide strong Wi-Fi throughout the hotel.

I tried static and dynamic data routing and different VLAN configurations to test which suited speed and dependability better. I will also suggest features like premium Wi-Fi for faster connections and smart room keys.

Firewalls and WPA3 encryption ensure robust security. This design allows the hotel to quickly expand its network, saving money and providing excellent service to guests and staff.

Introduction

The goal is to design and evaluate a network infrastructure for Bay Resort Hotels. The system ensures strong connectivity, boosts operational efficiency, and meets guest and business needs.

The network design for a two-story hotel building measuring 200 meters by 100 meters focuses on public Wi-Fi coverage, wired and wireless check-in stations, safe guest and staff networks, and WAN connectivity to regional and head offices. Secure data protection, electronic room keys, and premium Wi-Fi are also important.

My network designs were simulated using Cisco Packet Tracer (CPT). These simulations test and analyze my logical and physical configurations, IP address allocation, VLAN implementation, and routing protocol performance to ensure the design meets Bay Resort Hotels' operational goals.

Business and Technical Requirements

Network Layout

The network must cover a 200m x 100m, two-floor building, ensuring complete connectivity for all areas of operation. The design should be scalable to support additional devices and future expansions.

Key Facilities

- **Front Desk and Rapid Check-In Stations:**
  - Six manned check-in/out stations and four unmanned rapid check-in/out kiosks requiring reliable wired or wireless connections.
- **Public Areas:**
  - Seamless Wi-Fi coverage in the lobby, lounge, restaurant, café, and bar.
- **Boutique Pay Stations:**
  - At least two wired or wireless card/cash pay stations in the boutique.
  - Support for customers to pick up and pay for online reservations.
- **Guest Rooms:**
  - Wi-Fi coverage in all rooms with optional paid upgrades for enhanced bandwidth.
- **WAN Connectivity:**
  - Secure and stable connections to the regional HQ (30 miles away) and the company head office (in London) to facilitate centralized management and web services.

Security and Fault Management Needs

- **Security:**
  - Compliance with 802.11i standards for Wi-Fi security.
  - Deployment of firewalls, virus scanners, access controls, port security, and WPA3 encryption.
- **Fault Management:**
  - Redundancy systems to prevent downtime and ensure reliability.
  - Use of SNMP for centralized network management and real-time fault monitoring.
  - Inclusion of backup configurations and automatic failover mechanisms.

Justification of Identified Requirements

- **Scalability:** The design must handle future growth, including guest devices, IoT, and additional networked services.
- **Reliability and Availability:** Continuous operation is essential for guest satisfaction and business processes. Redundant systems will prevent disruptions.
- **Cost-Efficiency:** Using switches over excessive routers balances performance and cost while maintaining scalability.

- **Guest Experience:** Reliable Wi-Fi and optional premium upgrades cater to diverse guest needs, enhancing satisfaction.
- **Security and Privacy:** Robust security protocols protect guest data and the hotel's network infrastructure.
- **WAN Connectivity:** Centralized web services and seamless communication with HQ and regional offices ensure operational efficiency.

Network Design

Logical Design

IPv4 Scheme and VLAN Segmentation

The network architecture maximizes IP address allocation and VLAN segmentation for enhanced security and performance by means of a structured IPv4 addressing system with subnetting.

- **VLAN Segmentation and Subnetting:**
    - VLAN segmentation separates network traffic, guaranteeing security and performance.
    - Using CIDR and VLSM, each VLAN has its own subnet to maximize IP use.

Routing Protocol Considerations

The network uses OSPF (Open Shortest Path First) dynamic routing because it's better than static routing:

- **Scalability:** OSPF supports future growth by supporting new services and devices without major changes.
- **Automatic Failover Systems:** Ensures minimal downtime for operational services.
- **Optimized Data Pathways:** Dynamic routing reduces latency, improving user experience.
- **Reduced Administrative Burden:** Dynamic protocols eliminate manual upgrades.

Static routing is simple and resource-efficient but lacks adaptability and failover for dynamic environments like Bay Resort Hotels.

Physical Layout

Ground Floor

Five ground-floor rooms house network equipment with wire closets.

- The main wiring closet is the ground floor's network hub.
- Boutique: Network devices aid inventory control and POS.
- The front desk has wired PCs, kiosks, and other check-in/out devices.
- Rapid check-in is near the entrance with unmanned check-in/out tools.
- The manager's office has administrative tools and secure connections.

Access points are strategically placed to ensure flawless connectivity for computers, tablets, and smartphones in public and operational areas.

First Floor

The first-floor server room and single-wire closet serve purposes. This area houses critical network architecture like servers and switches. First-floor access points connect guest rooms and staff devices to the internet.

Southampton Regional Headquarters

Network design at regional headquarters near Southampton includes:

- A router and PC for administrative tasks and connectivity.

London Headquarters

The London headquarters layout is similar:

- One router and one PC in the main wiring closet control centralized online services and connect regional sites.

Security and Fault Management

Managing Errors

These fault management techniques guarantee continuous service and fast resolution of problems:

- **Redundancy and Failover:**
  - Redundant systems reduce service disruptions during hardware or network breakdowns.
  - Critical services have automatic failover.
- **Network Monitoring:**
  - Centralized monitoring of network performance and defect detection is accomplished via SNMP.
  - Alerts instantly warn managers of possible problems.

- **Backup Configuration:**
    - Frequent updates of backup configurations guarantee quick recovery from unexpected events.
- **Fault Isolation:**
    - VLANs segment traffic to prevent local problems from affecting the entire system.
    - OSPF dynamic routing reroutes traffic across link failures, improving fault tolerance.

Safety Protocols

- **Wi-Fi Security:**
    - Following 802.11i Wi-Fi security guidelines.
    - WPA3 encryption applied in public areas and guest room Wi-Fi.
- **Firewalls:**
    - Deployed at strategic points, firewalls filter harmful traffic and stop unauthorized access.
- **Access Control:**
    - Role-based access controls ensure devices only have necessary resource access.
    - Port security prevents rogue device connections.
- **Intrusion Prevention Systems:**
    - IPS identifies and stops dubious actions or assaults.
- **Encryption and Secure Transactions:**
    - All sensitive information exchanges use encrypted communication methods.

Ideas for Network Improvements

The following ideas will future-proof the network and keep Bay Resort Hotels ahead in technology:

- **Integration of IoT Devices:**
    - Install smart thermostats, lighting, and voice-activated assistants in guest rooms.
    - Centralized monitoring by IoT devices allows predictive maintenance for vital equipment.
- **Scalability:**
    - IPv6 migration ensures the network can handle more devices and connections.
    - IPv6 includes IPsec for data transit security.
- **Increased WAN Optimization:**
    - MPLS provides reliable WAN connectivity.
- **Edge Computing for Low-Latency Applications:**
    - For real-time IoT analytics and video monitoring, edge computing handles data locally.

- **Using SDN:**
    - SDN simplifies network administration and optimizes resource allocation.

Evaluation of Design Decisions

- **Future Growth and Scalability:**
    - The proposed design is scalable with VLAN segmentation, OSPF, and a structured IPv4 system.
    - IPv6 migration strengthens future readiness.
- **Performance Improvement:**
    - Dynamic routing reduces latency and increases reliability.
- **Economic Efficiency:**
    - VLANs and switches are cheaper alternatives to expensive routing gear.
- **Safety:**
    - Firewalls, VLAN separation, and WPA3 encryption secure the network.
- **Guests' Experience:**
    - The design emphasizes fast, reliable Wi-Fi and premium options for diverse needs.

Conclusion and Recommendations

A detailed network architecture for Bay Resort Hotels' operational and commercial needs is presented. Dynamic routing, structured VLAN segmentation, and strong security ensure reliability and scalability.

Simulations demonstrate how the network reduces downtime and improves visitor experience.

Recommendations

- Switch to IPv6 for future-proofing.
- Use IoT solutions to improve operations.
- Conduct frequent security audits.
- Train staff on the new network architecture.
- Investigate edge computing and SDN for future use.

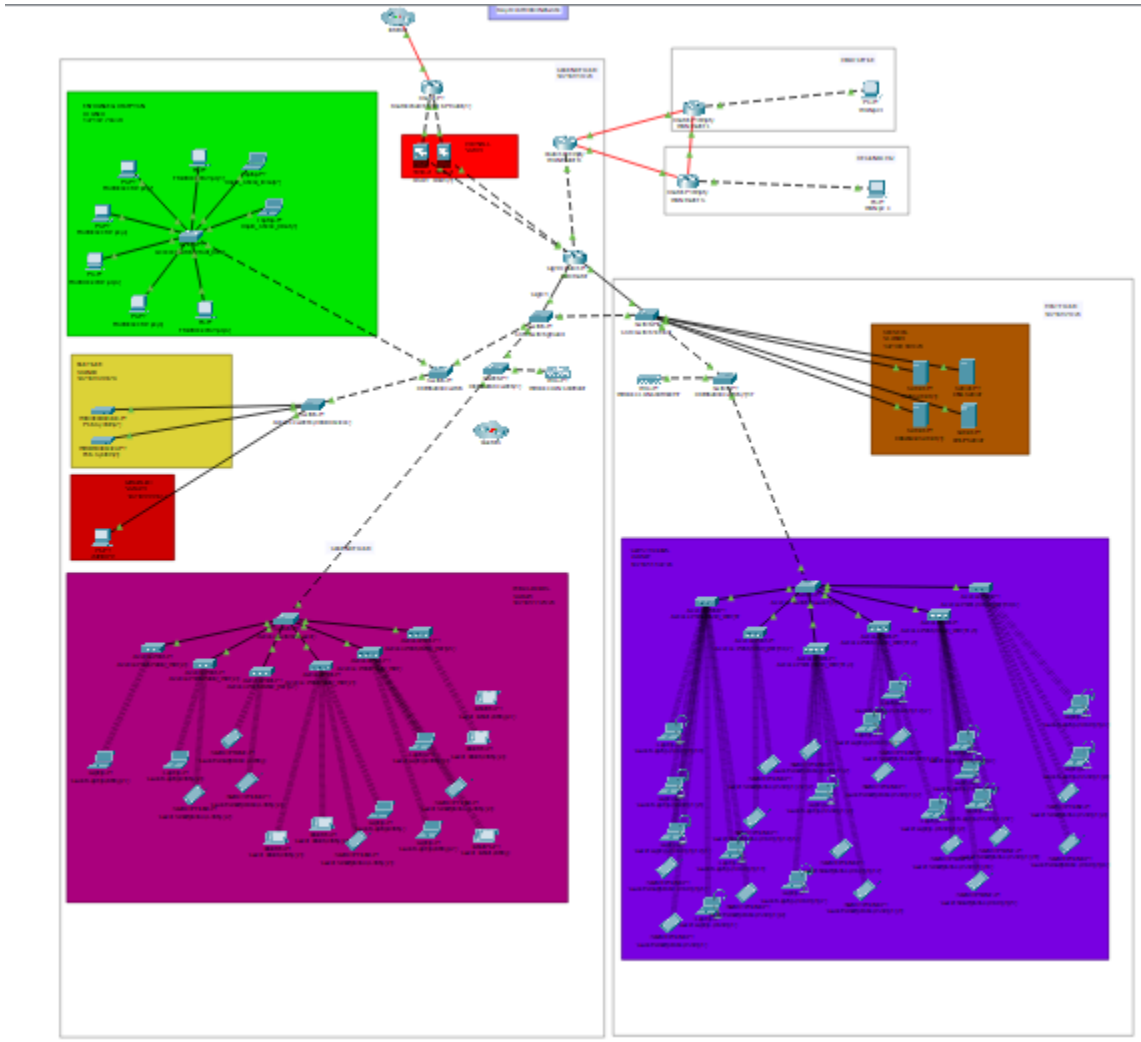
References

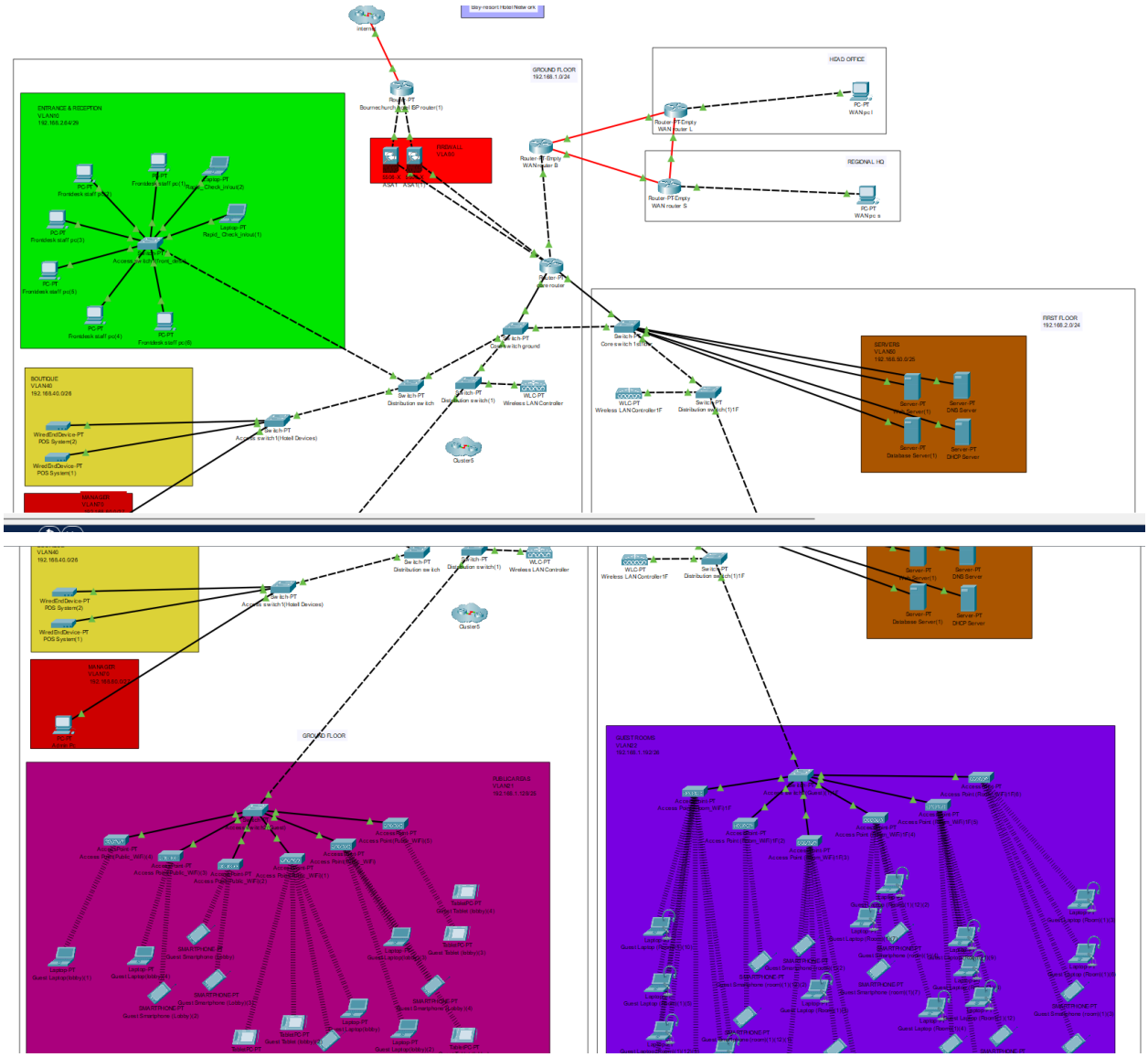
References (Bournemouth Harvard Style)

- Cisco Systems Inc. (n.d.) Cisco Packet Tracer - A powerful network simulation tool. Available from: https://www.cisco.com [Accessed 16 January 2025].
- IEEE Standards Association (2016) 802.11i-2004 - Amendment 6: Medium Access Control (MAC) Security Enhancements. Available from: https://standards.ieee.org [Accessed 16 January 2025].
- IPv6 Forum (n.d.). IPv6 benefits and deployment strategies. Available from: https://www.ipv6forum.com [Accessed 16 January 2025].
- Bournechurch Hotel IT Scenario Documentation (2025). Internal company scenario for network design project. Provided in course material.
- YouTube (n.d.) *Hotel Network Design*. Available from: https://www.youtube.com/watch?v=RwFJTJTe-OM&pp=ygUUaG90ZWwgbmV0d29yayBkZXNpZ24%3D [Accessed 17 January 2025].

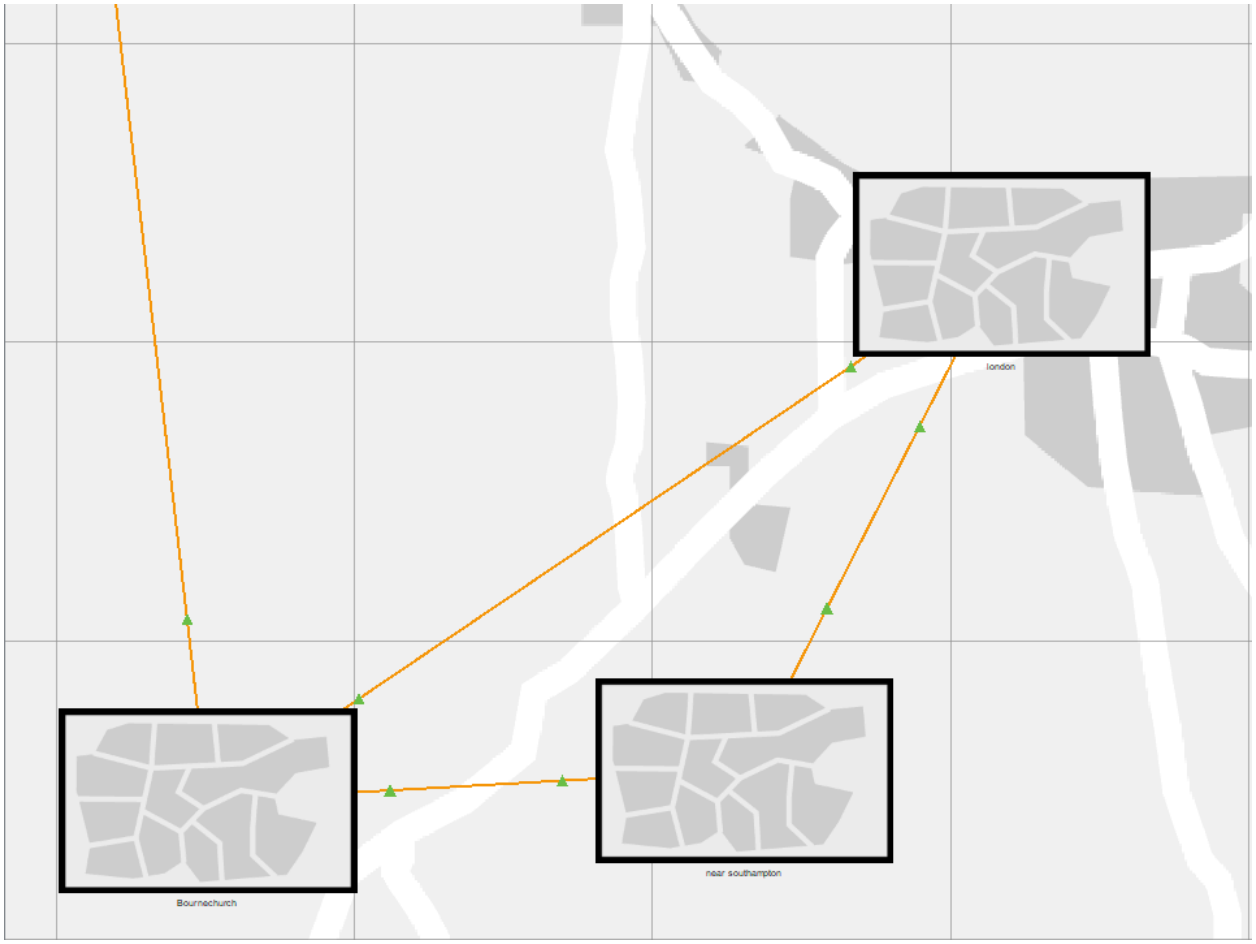
Appendices

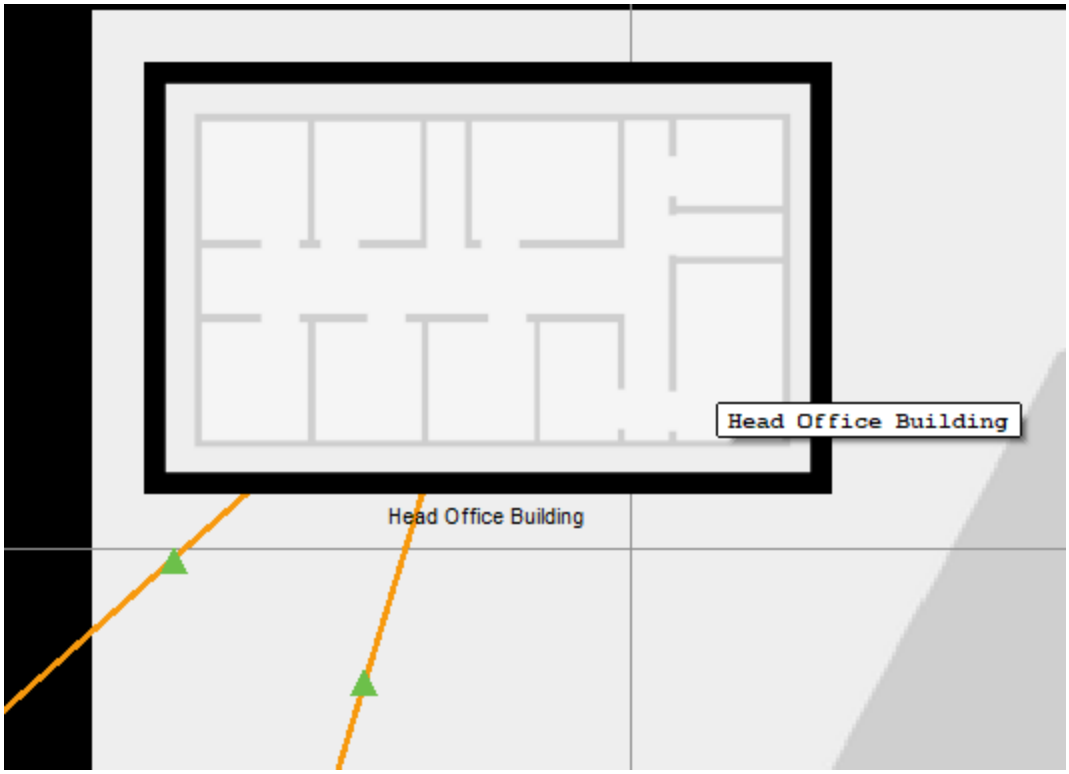
Appendix A: Logical Network Diagrams

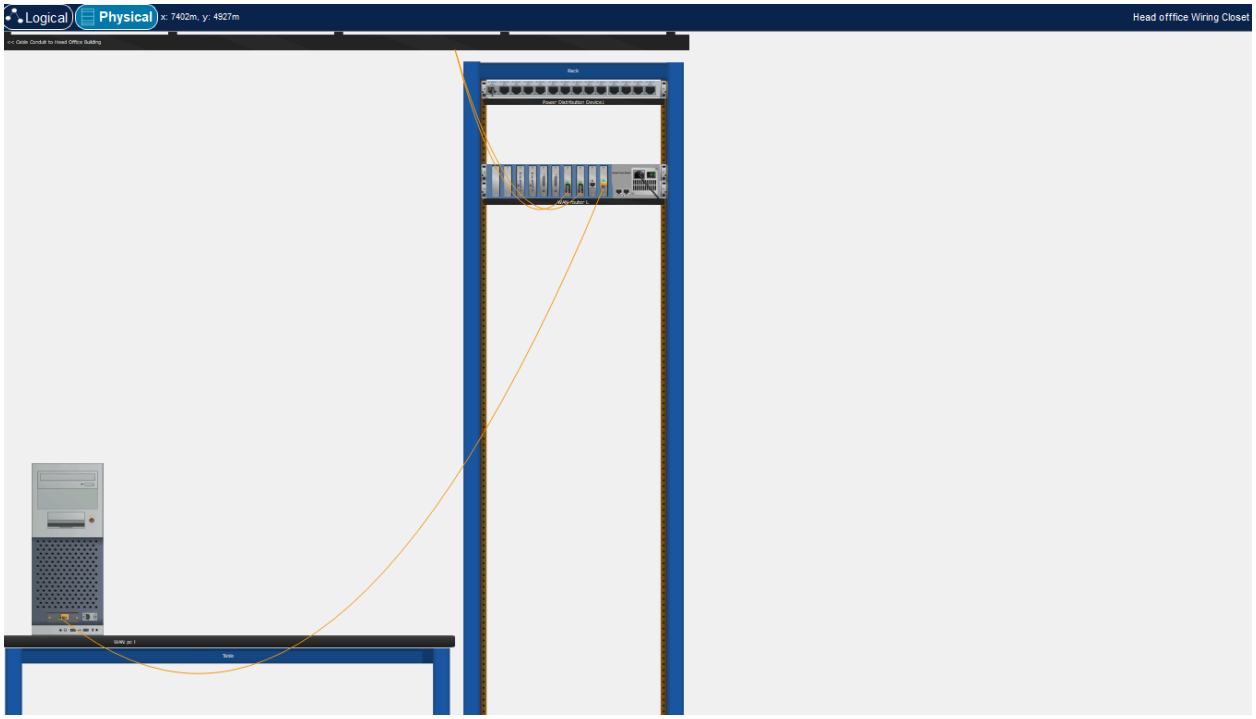


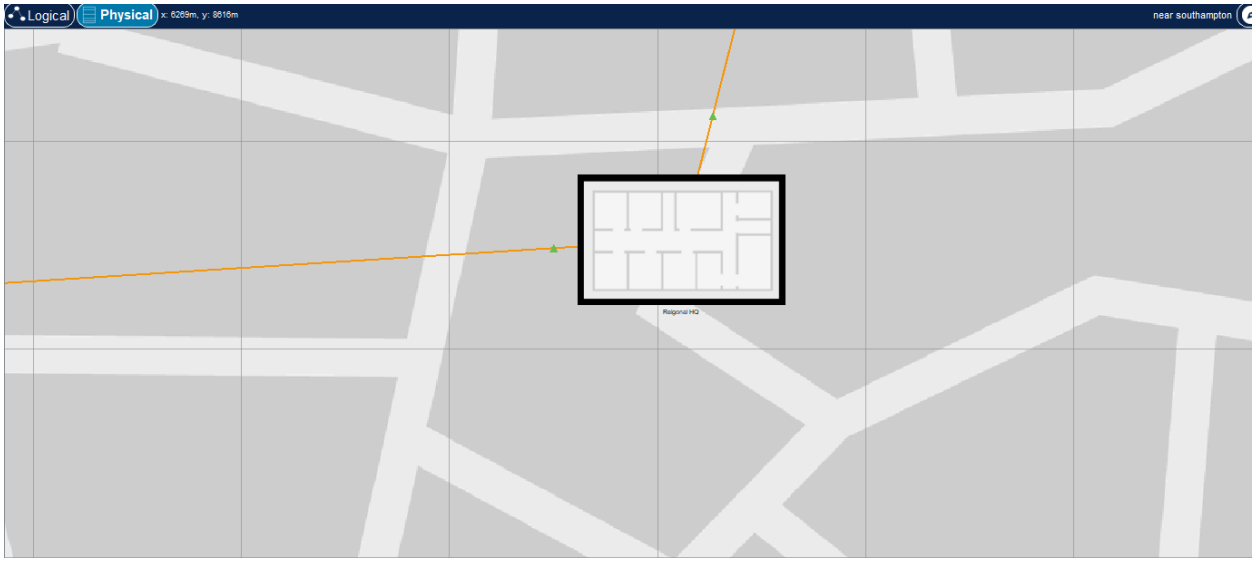


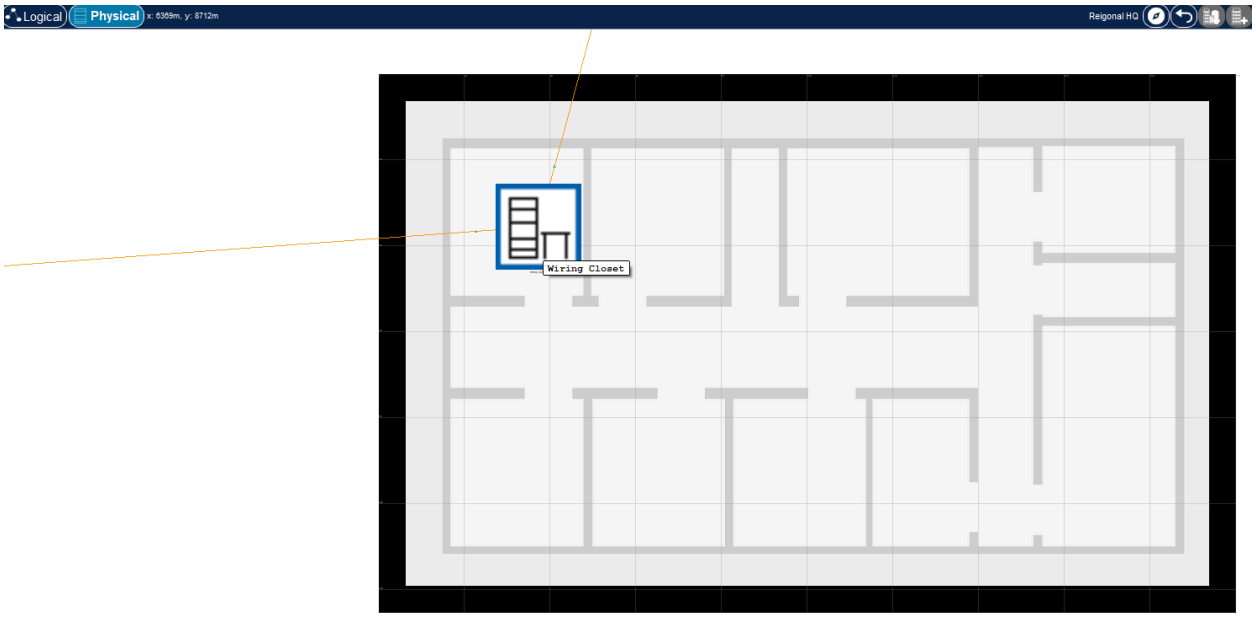
Appendix B: Physical Network Diagram

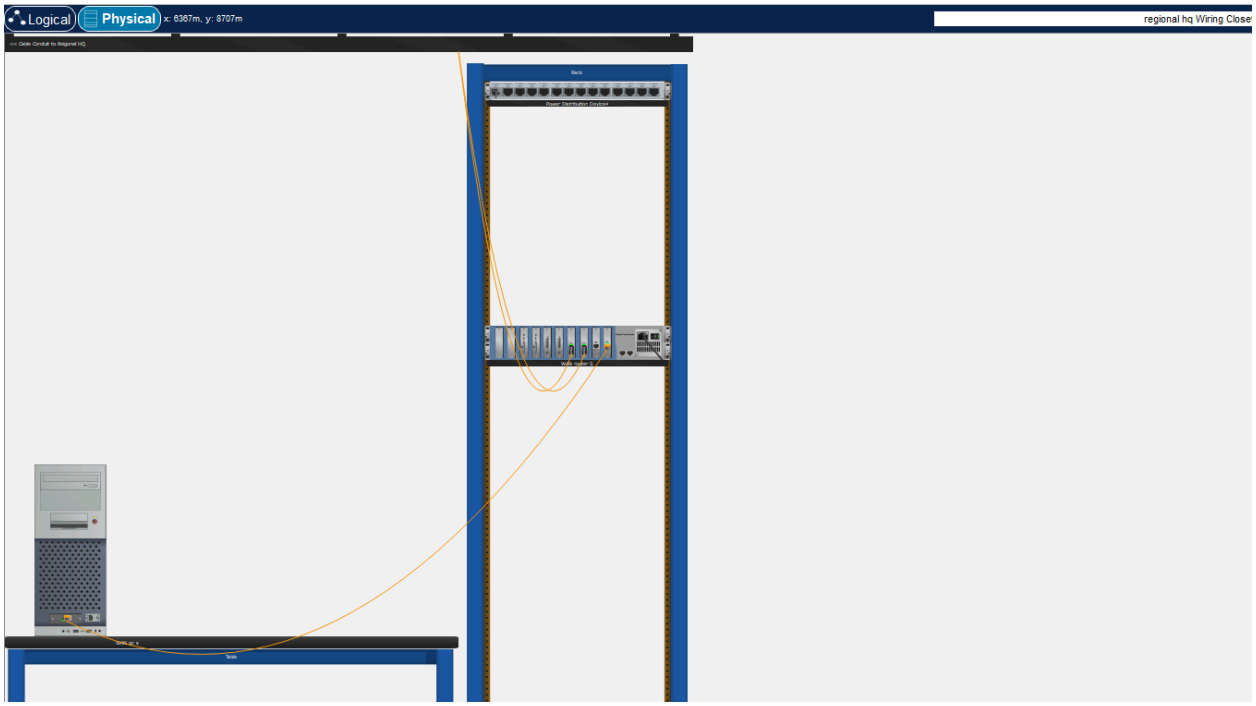

london
near southampton
Bournechurch

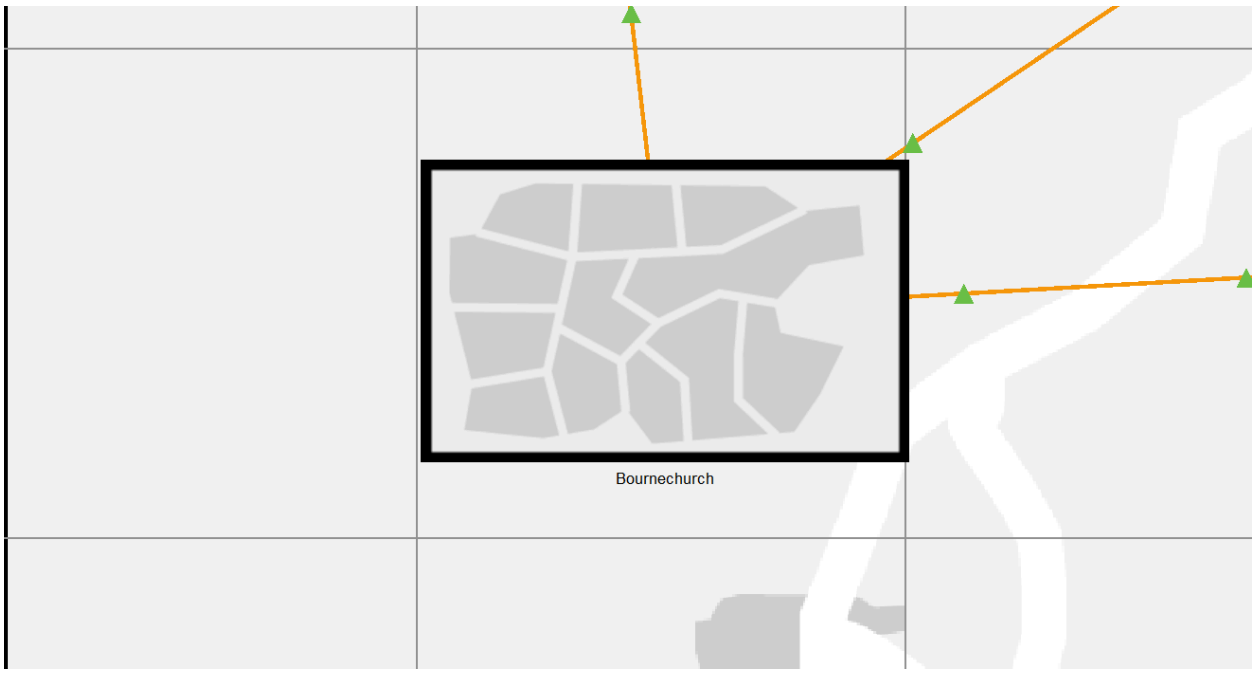

Head Office Building
Head Office Building

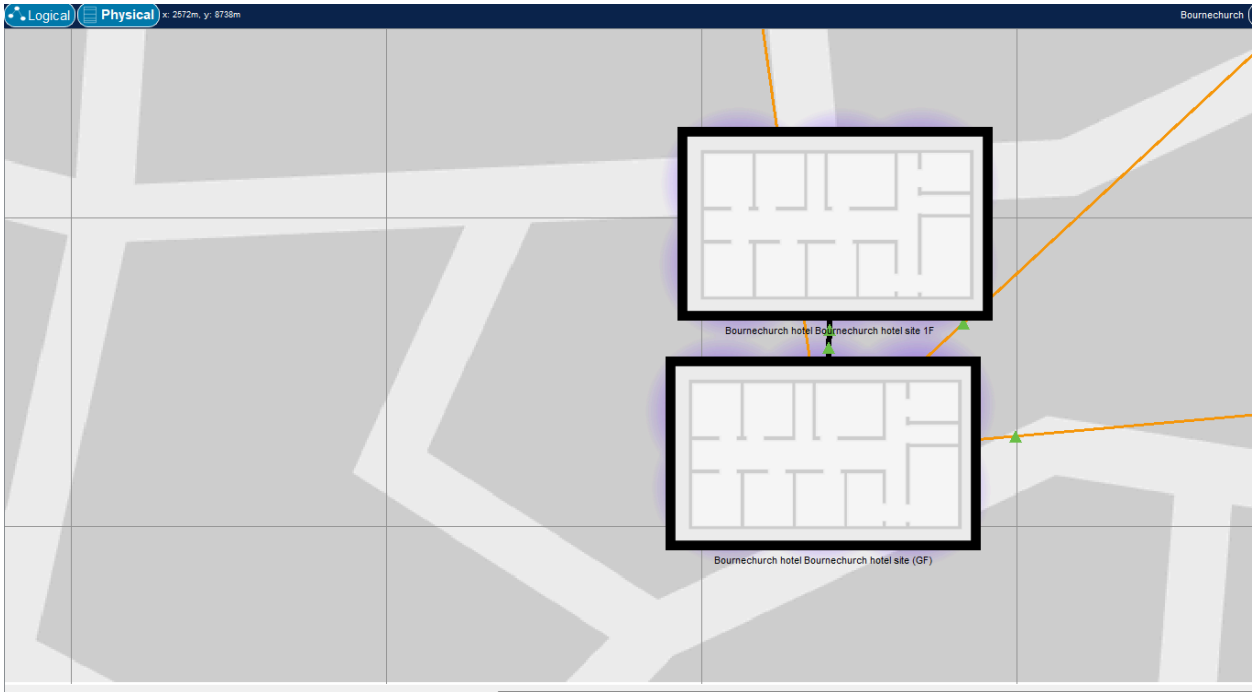

Logical
Physical
x: 7402m, y: 4927m
Head offfice Wiring Closet

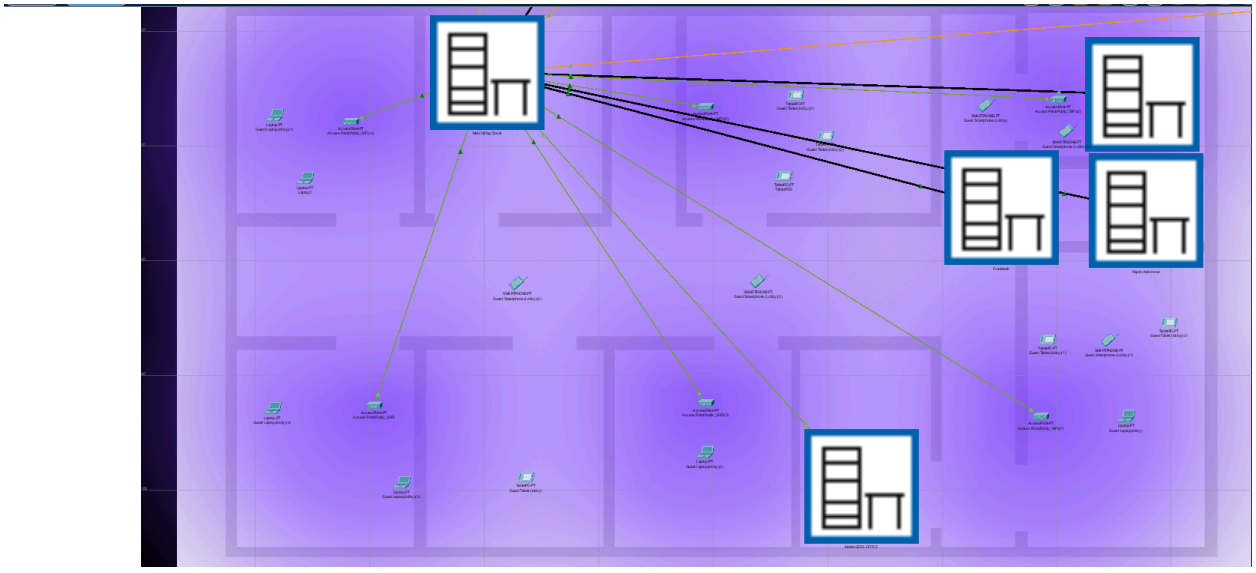

Logical
Physical
x: 6269m, y: 8616m
near southampton
Regional HQ


Logical
Physical
x: 6369m, y: 8712m
Regional HQ
Wiring Closet

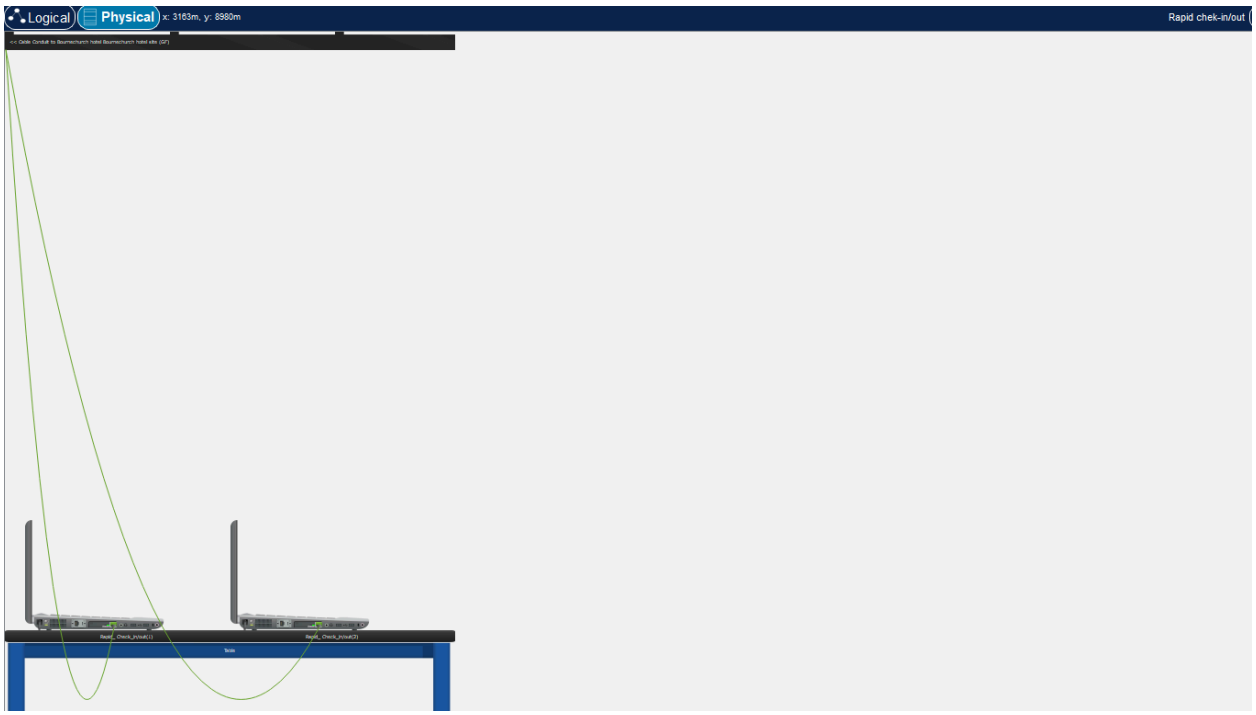

Logical
Physical
x: 6367m, y: 8707m
regional hq Wiring Closet

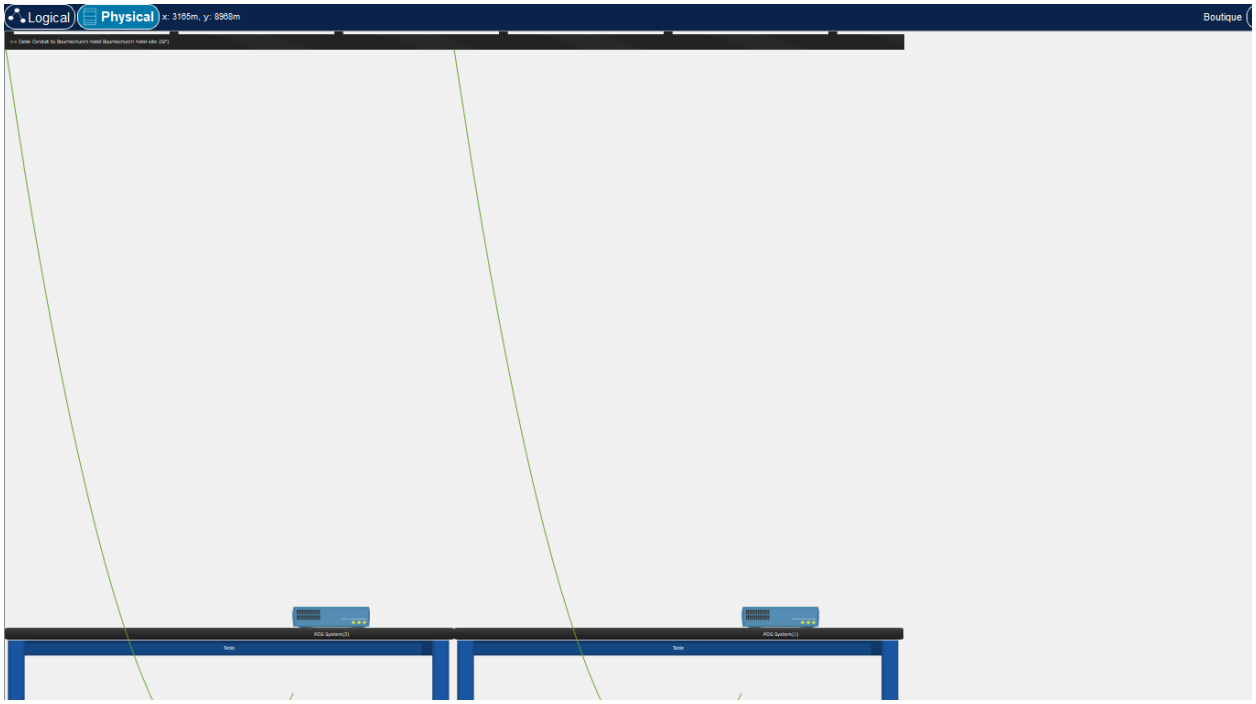

Bournechurch

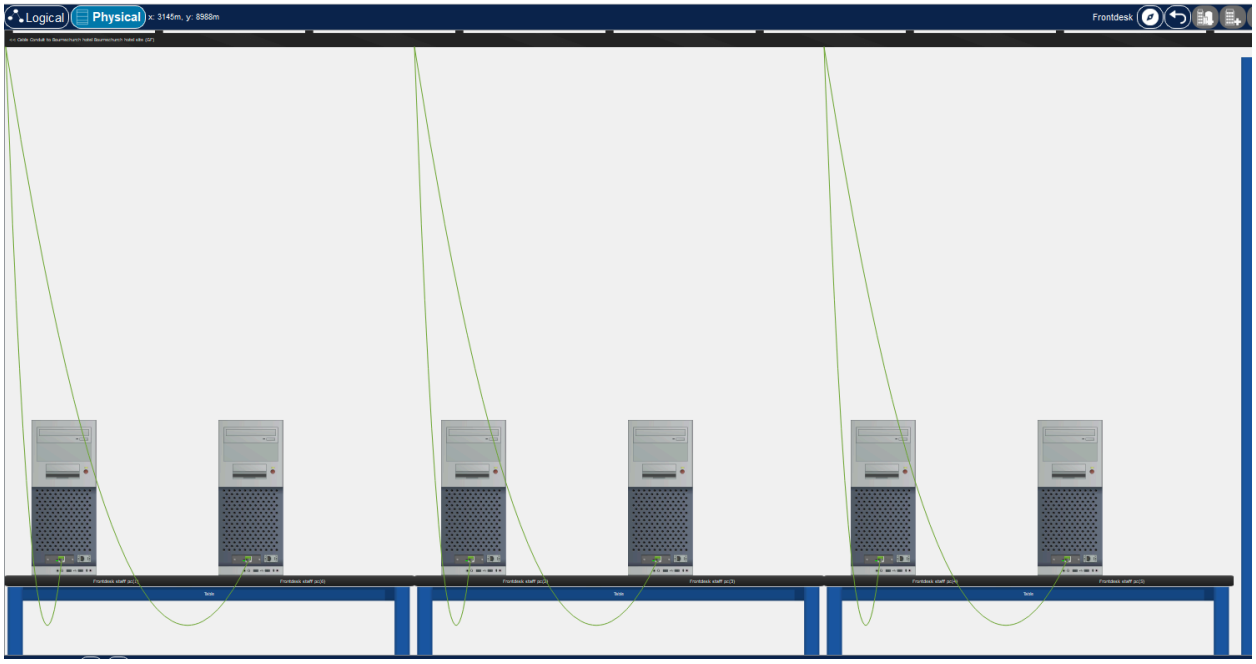

Logical
Physical
x: 2572m, y: 8738m
Bournechurch
Bournechurch hotel Bournechurch hotel site 1F
Bournechurch hotel Bournechurch hotel site (GF)



Logical
Physical
x: 3045m, y: 8964m
Main Wiring Closet
Rack
Cable Pegboard
Shelf
Table
POS System
Time: 12:01:26

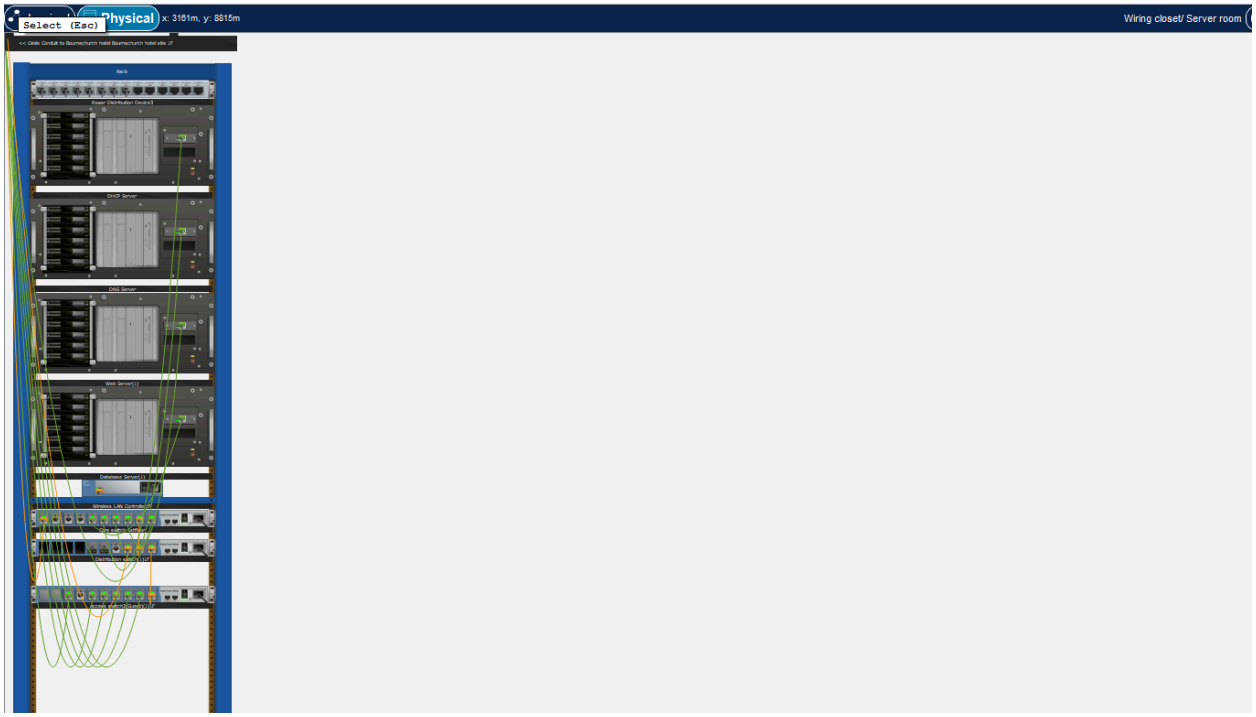

Logical
Physical
x: 3163m, y: 8980m
Rapid chek-in/out
Table


Logical
Physical
x: 3185m, y: 8968m
Boutique

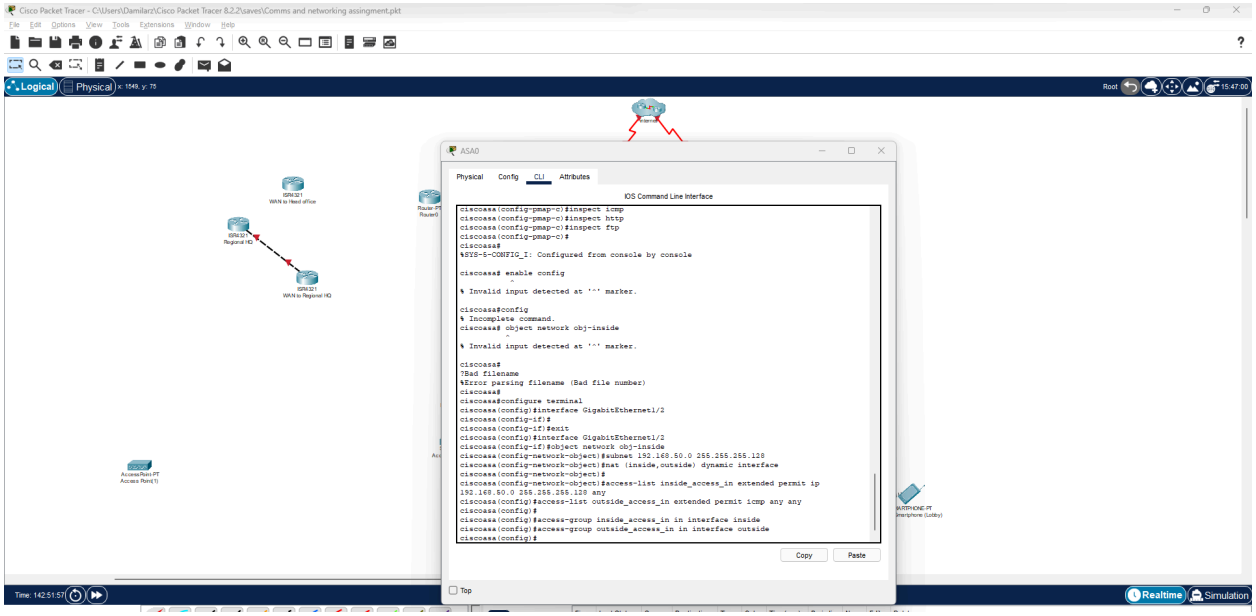

Logical
Physical
x: 3145m, y: 8968m
Frontdesk

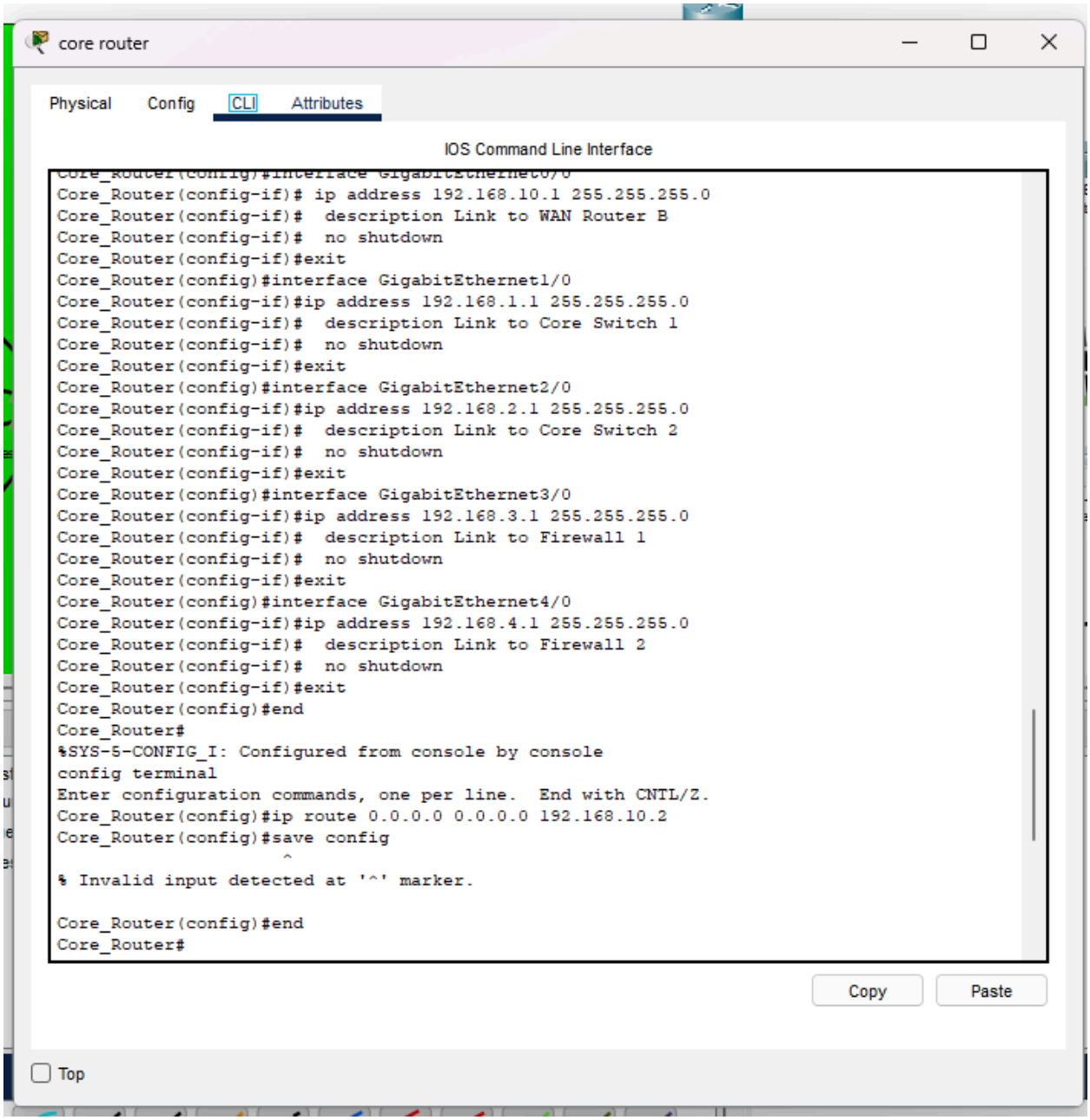
Logical
Physical
x: 3118m, y: 9029m
MANAGERS OFFICE
Logical Mode (Shift+L)
Time: 12:02:22

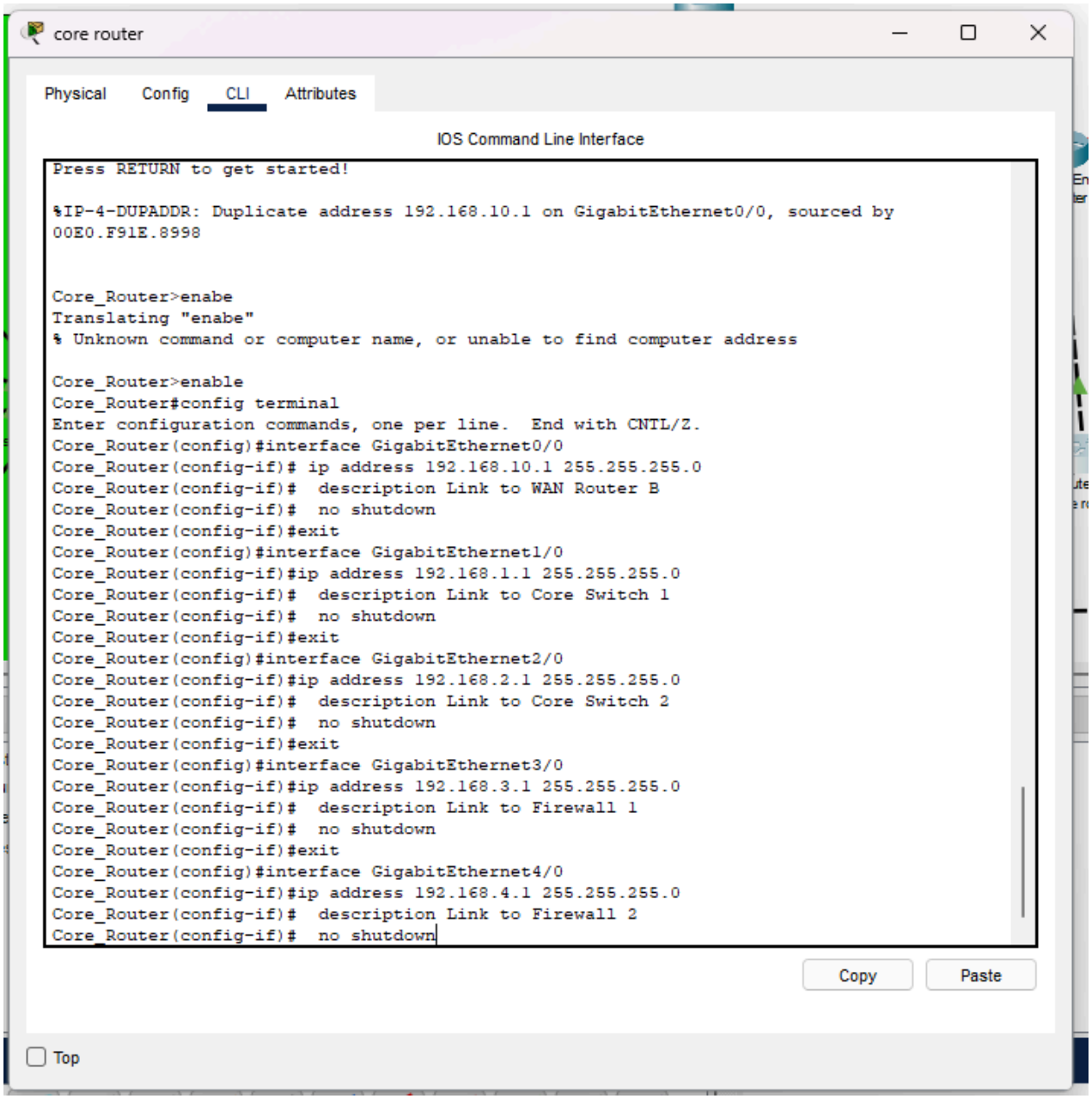
Logical
Physical
x: 3004m, y: 8801m
Bournechurch hotel Bournechurch hotel site 1F

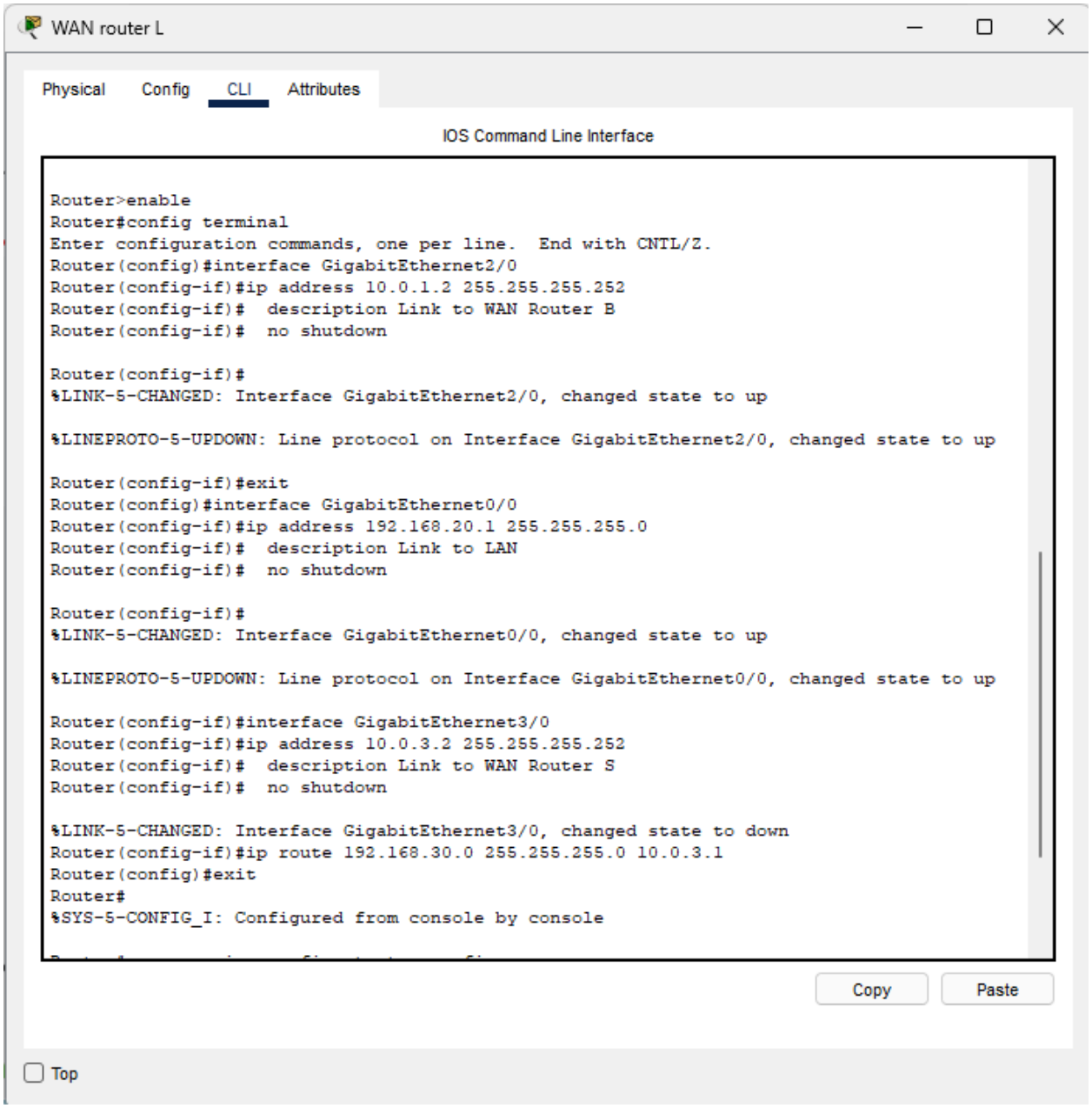

Select (Esc)
Physical
x: 3161m, y: 8815m
Wiring closet/ Server room

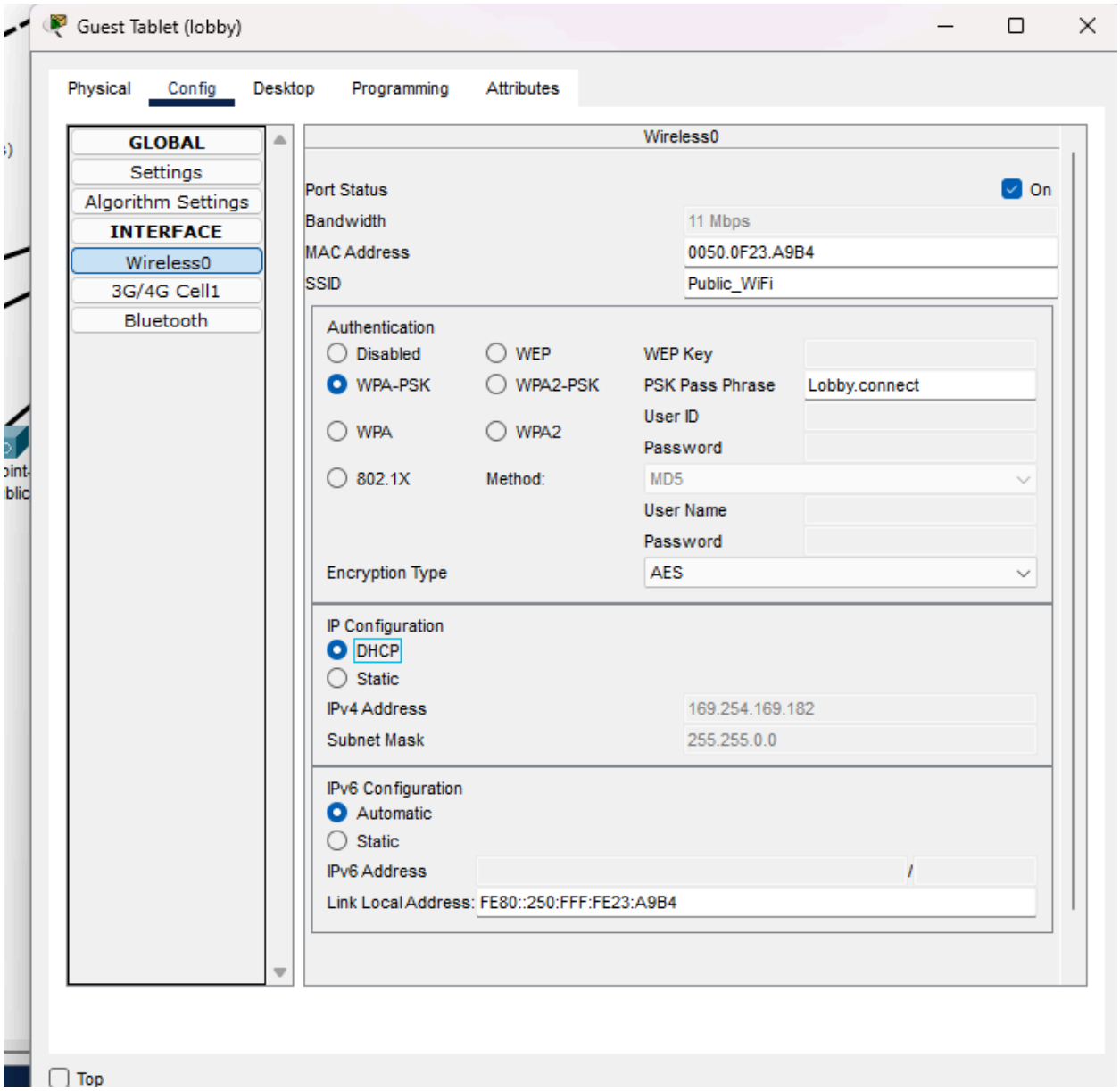
Appendix C: Cisco Packet Tracer Configurations

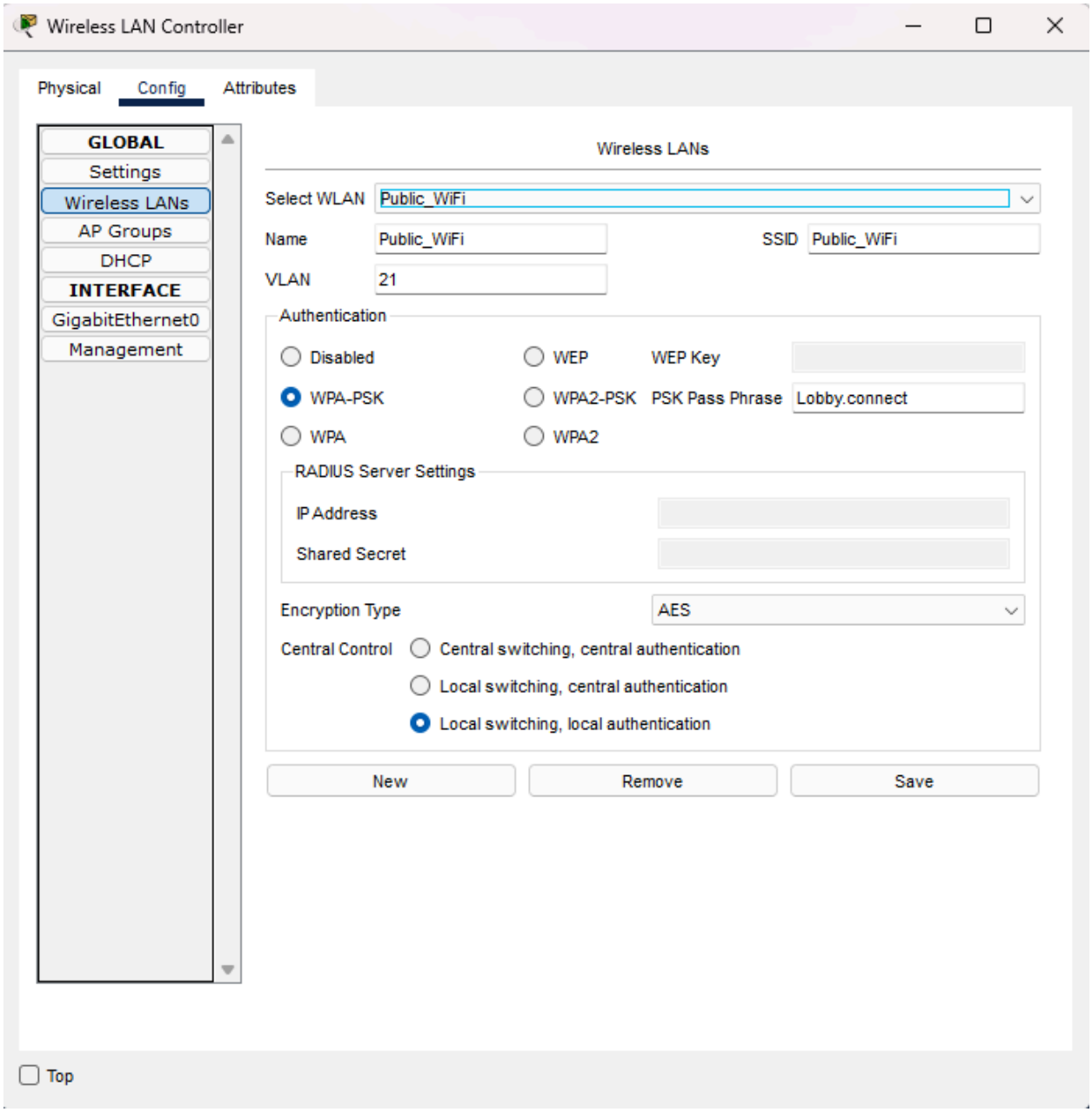


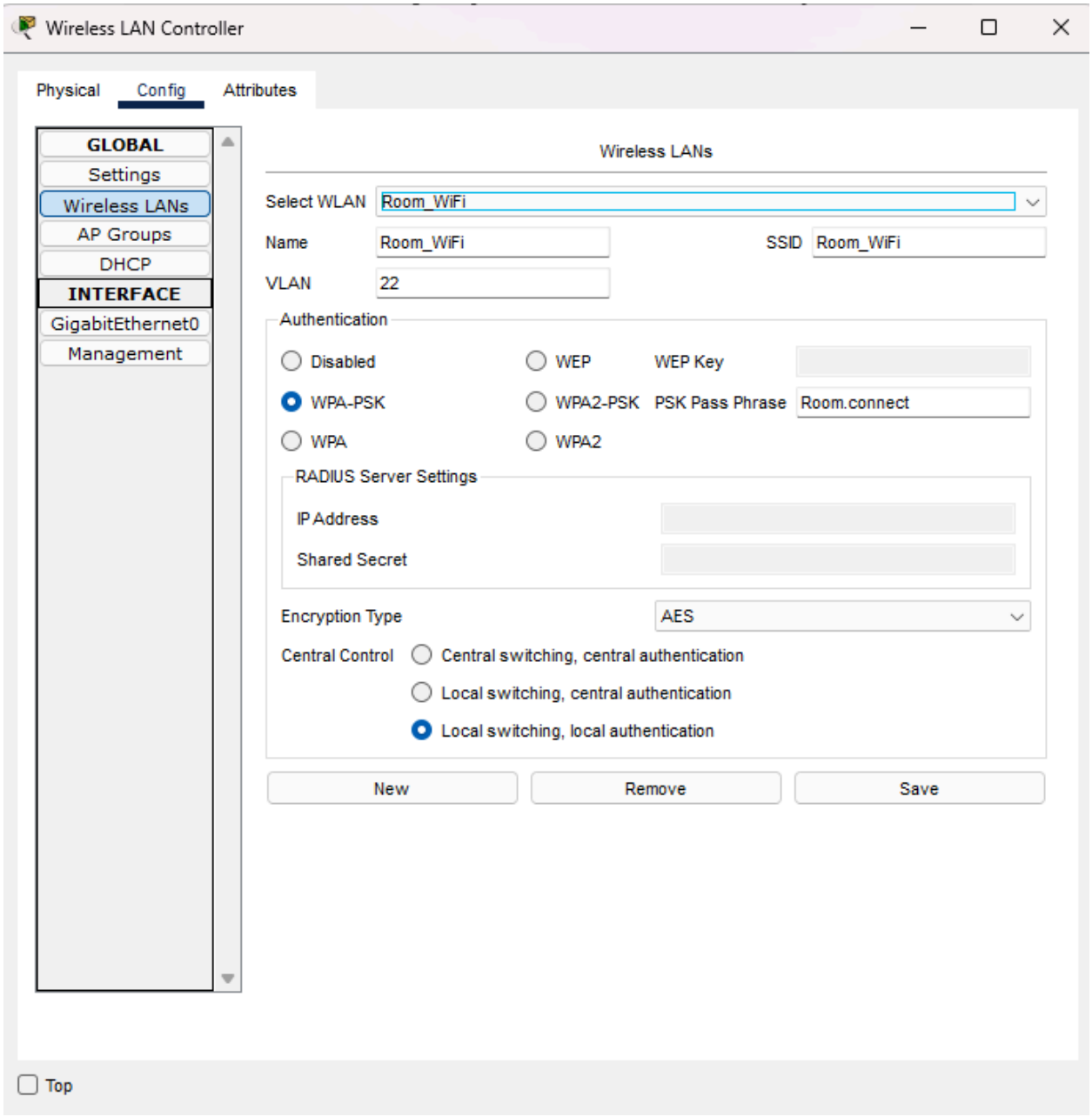

core router
Physical
Config
CLI
Attributes
IOS Command Line Interface
Core_Router(config-if)# ip address 192.168.10.1 255.255.255.0
Core_Router(config-if)# description Link to WAN Router B
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet1/0
Core_Router(config-if)#ip address 192.168.1.1 255.255.255.0
Core_Router(config-if)# description Link to Core Switch 1
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet2/0
Core_Router(config-if)#ip address 192.168.2.1 255.255.255.0
Core_Router(config-if)# description Link to Core Switch 2
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet3/0
Core_Router(config-if)#ip address 192.168.3.1 255.255.255.0
Core_Router(config-if)# description Link to Firewall 1
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet4/0
Core_Router(config-if)#ip address 192.168.4.1 255.255.255.0
Core_Router(config-if)# description Link to Firewall 2
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#end
Core_Router#
%SYS-5-CONFIG_I: Configured from console by console
config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core_Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
Core_Router(config)#save config
                   ^
% Invalid input detected at '^' marker.
Core_Router(config)#end
Core_Router#
Copy
Paste
Top

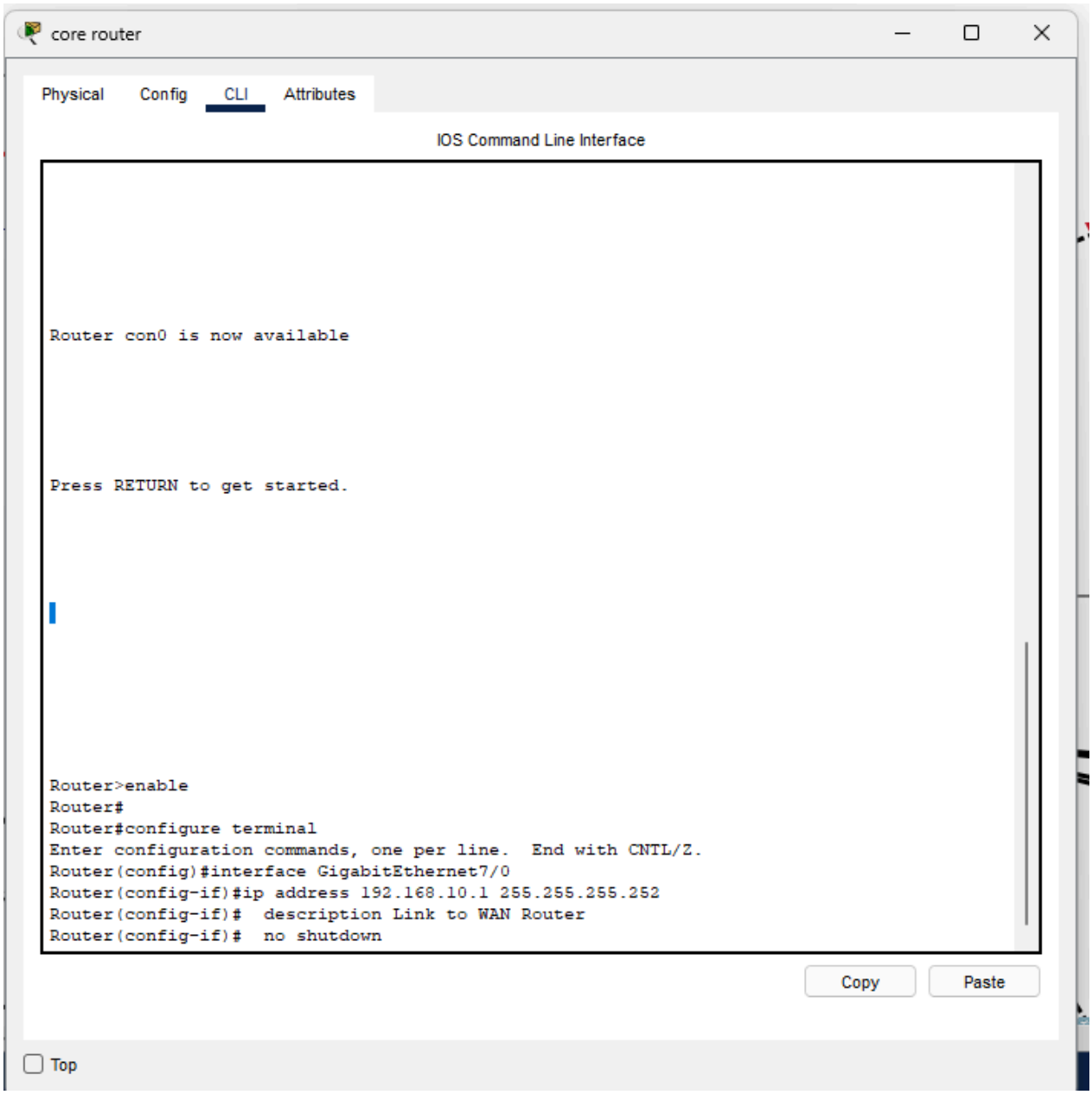

core router
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0, sourced by
00E0.F91E.8998
Core_Router>enabe
Translating "enabe"
% Unknown command or computer name, or unable to find computer address
Core_Router>enable
Core_Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core_Router(config)#interface GigabitEthernet0/0
Core_Router(config-if)# ip address 192.168.10.1 255.255.255.0
Core_Router(config-if)# description Link to WAN Router B
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet1/0
Core_Router(config-if)#ip address 192.168.1.1 255.255.255.0
Core_Router(config-if)# description Link to Core Switch 1
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet2/0
Core_Router(config-if)#ip address 192.168.2.1 255.255.255.0
Core_Router(config-if)# description Link to Core Switch 2
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet3/0
Core_Router(config-if)#ip address 192.168.3.1 255.255.255.0
Core_Router(config-if)# description Link to Firewall 1
Core_Router(config-if)# no shutdown
Core_Router(config-if)#exit
Core_Router(config)#interface GigabitEthernet4/0
Core_Router(config-if)#ip address 192.168.4.1 255.255.255.0
Core_Router(config-if)# description Link to Firewall 2
Core_Router(config-if)# no shutdown
Copy
Paste
Top

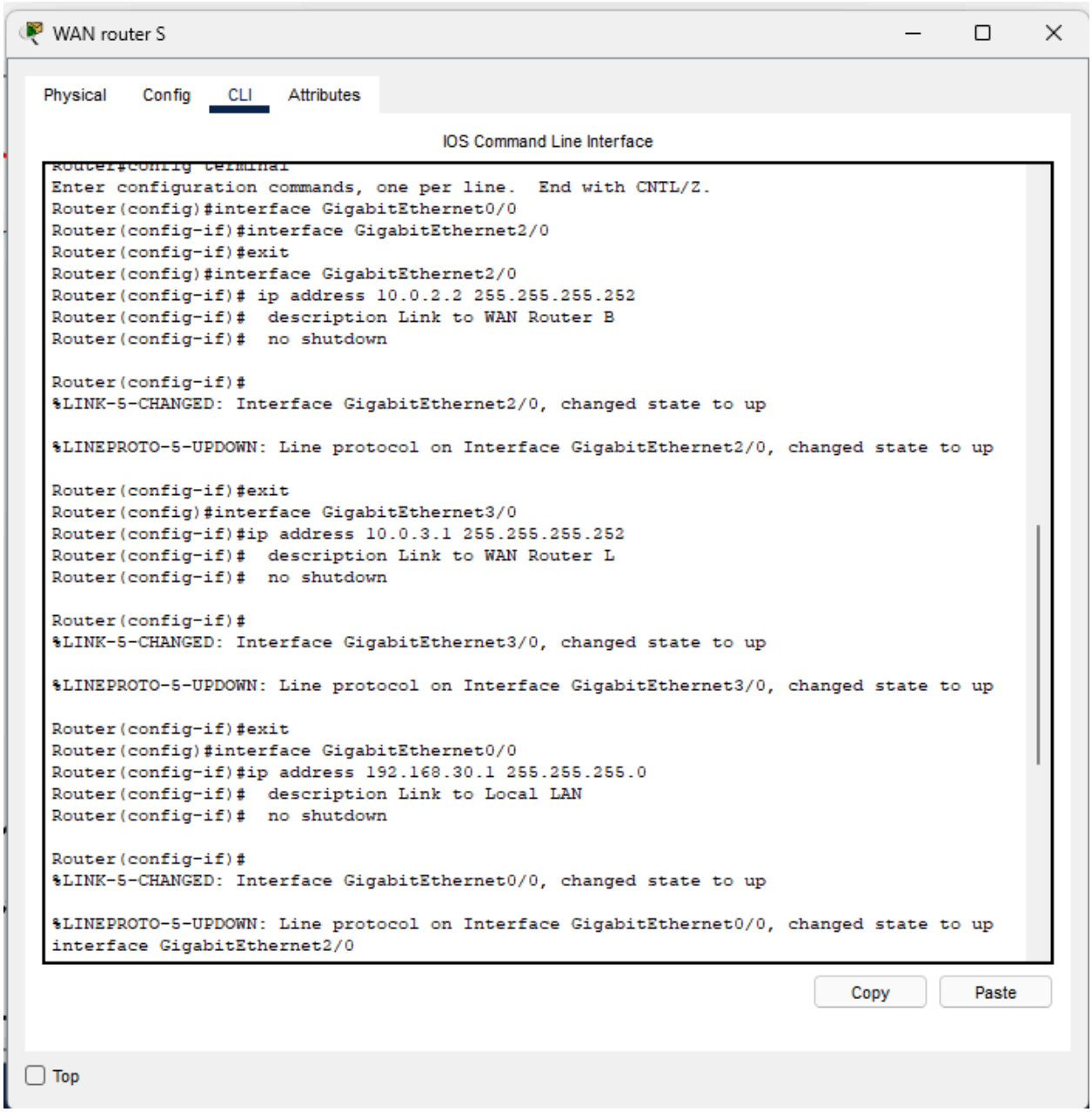

WAN router L
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet2/0
Router(config-if)#ip address 10.0.1.2 255.255.255.252
Router(config-if)# description Link to WAN Router B
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)# description Link to LAN
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router(config-if)#interface GigabitEthernet3/0
Router(config-if)#ip address 10.0.3.2 255.255.255.252
Router(config-if)# description Link to WAN Router S
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to down
Router(config-if)#ip route 192.168.30.0 255.255.255.0 10.0.3.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top

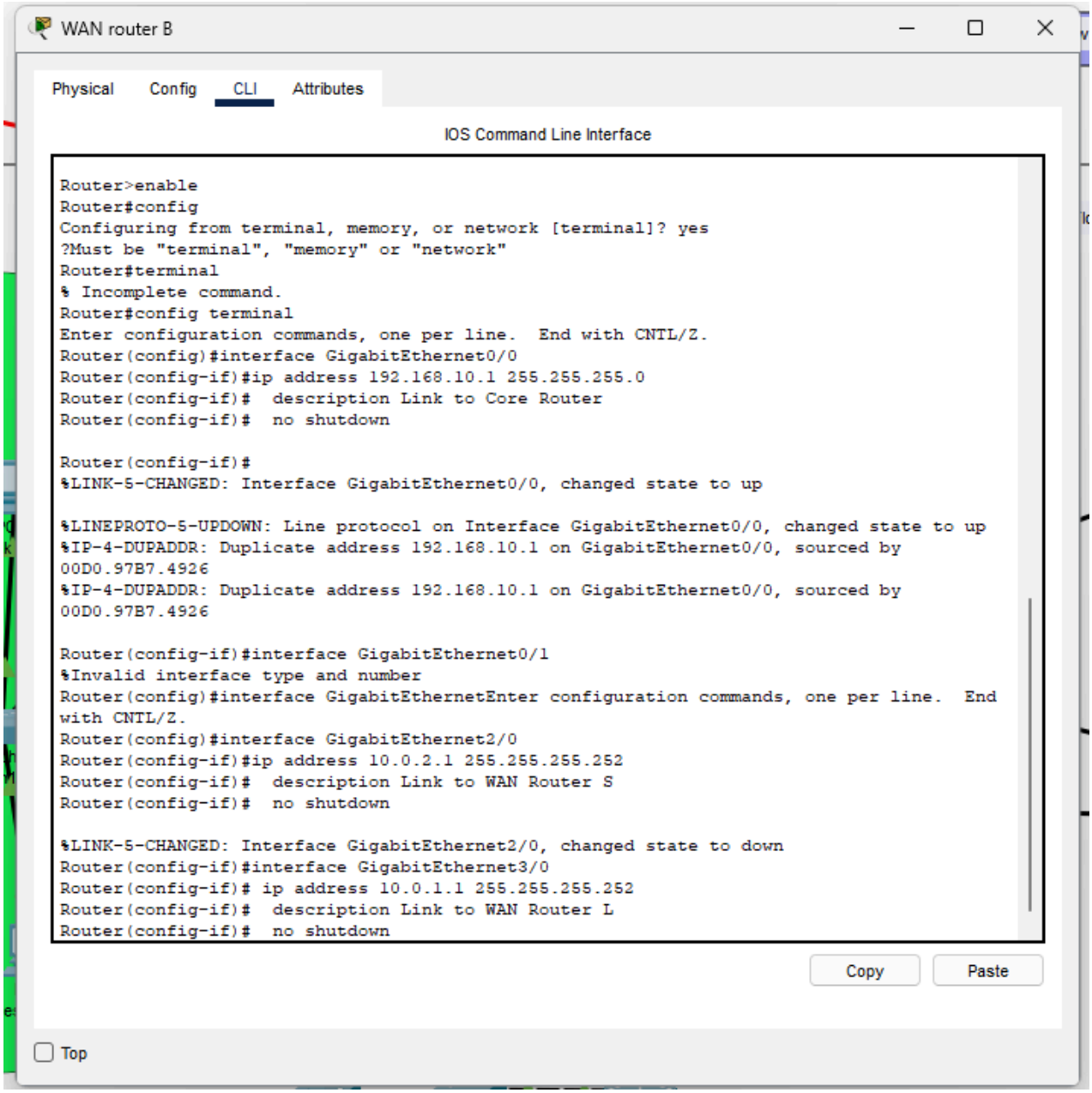

Guest Tablet (lobby)
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
3G/4G Cell1
Bluetooth
Wireless0
Port Status
On
Bandwidth
11 Mbps
MAC Address
0050.0F23.A9B4
SSID
Public_WiFi
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Lobby.connect
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
AES
IP Configuration
DHCP
Static
IPv4 Address
169.254.169.182
Subnet Mask
255.255.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address:
FE80::250:FFF:FE23:A9B4
Top

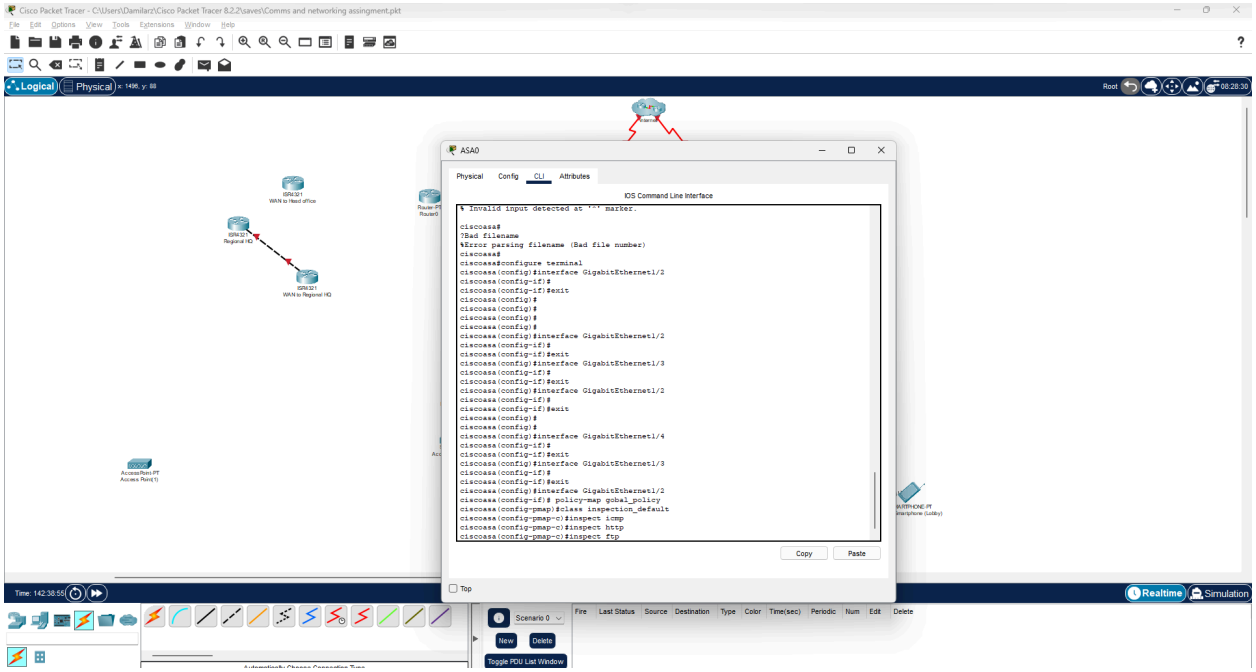

Wireless LAN Controller
Physical
Config
Attributes
GLOBAL
Settings
Wireless LANs
AP Groups
DHCP
INTERFACE
GigabitEthernet0
Management
Wireless LANs
Select WLAN
Public_WiFi
Name
Public_WiFi
SSID
Public_WiFi
VLAN
21
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Lobby.connect
WPA
WPA2
RADIUS Server Settings
IP Address
Shared Secret
Encryption Type
AES
Central Control
Central switching, central authentication
Local switching, central authentication
Local switching, local authentication
New
Remove
Save
Top

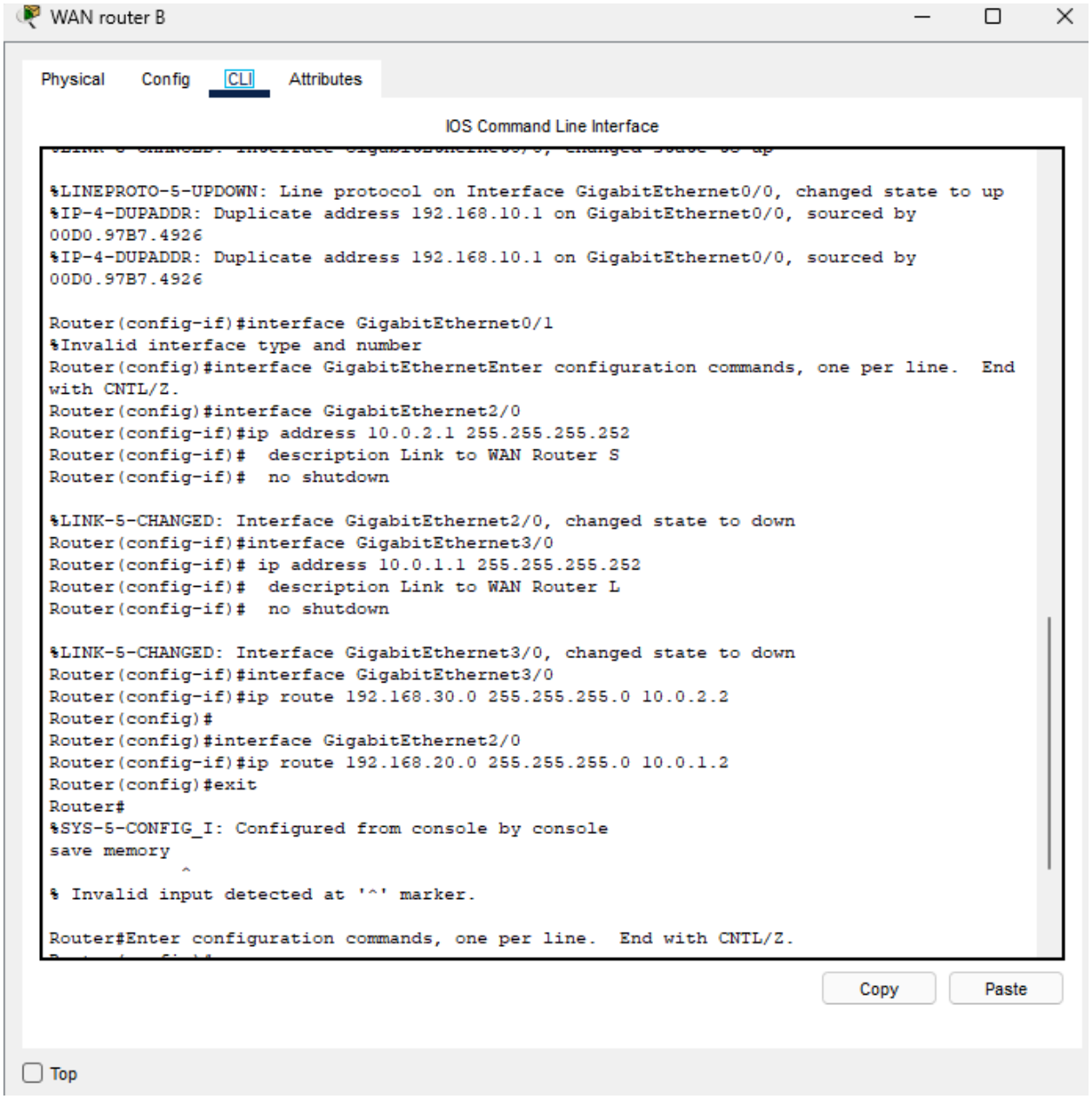

Wireless LAN Controller
Physical
Config
Attributes
GLOBAL
Settings
Wireless LANs
AP Groups
DHCP
INTERFACE
GigabitEthernet0
Management
Wireless LANs
Select WLAN
Room_WiFi
Name
Room_WiFi
SSID
Room_WiFi
VLAN
22
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Room.connect
WPA
WPA2
RADIUS Server Settings
IP Address
Shared Secret
Encryption Type
AES
Central Control
Central switching, central authentication
Local switching, central authentication
Local switching, local authentication
New
Remove
Save
Top

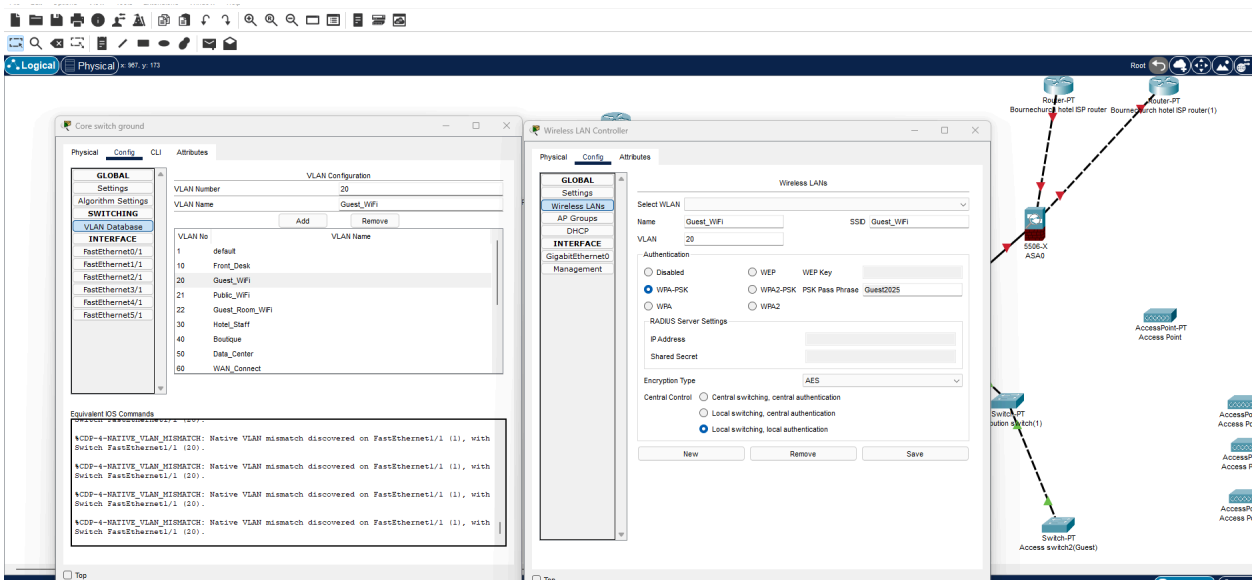

core router
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router con0 is now available
Press RETURN to get started.
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet7/0
Router(config-if)#ip address 192.168.10.1 255.255.255.252
Router(config-if)# description Link to WAN Router
Router(config-if)# no shutdown
Copy
Paste
Top


WAN router S
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#interface GigabitEthernet2/0
Router(config-if)#exit
Router(config)#interface GigabitEthernet2/0
Router(config-if)# ip address 10.0.2.2 255.255.255.252
Router(config-if)# description Link to WAN Router B
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
Router(config-if)#exit
Router(config)#interface GigabitEthernet3/0
Router(config-if)#ip address 10.0.3.1 255.255.255.252
Router(config-if)# description Link to WAN Router L
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to up
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)# description Link to Local LAN
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
interface GigabitEthernet2/0
Copy
Paste
Top


WAN router B
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? yes
?Must be "terminal", "memory" or "network"
Router#terminal
% Incomplete command.
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)# description Link to Core Router
Router(config-if)# no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0, sourced by
00D0.97B7.4926
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0, sourced by
00D0.97B7.4926
Router(config-if)#interface GigabitEthernet0/1
%Invalid interface type and number
Router(config)#interface GigabitEthernetEnter configuration commands, one per line. End
with CNTL/Z.
Router(config)#interface GigabitEthernet2/0
Router(config-if)#ip address 10.0.2.1 255.255.255.252
Router(config-if)# description Link to WAN Router S
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to down
Router(config-if)#interface GigabitEthernet3/0
Router(config-if)# ip address 10.0.1.1 255.255.255.252
Router(config-if)# description Link to WAN Router L
Router(config-if)# no shutdown
Copy
Paste
Top


Cisco Packet Tracer - C:\Users\Damilarz\Cisco Packet Tracer 8.2.2\saves\Comms and networking assingment.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
ASA0
Physical Config CLI Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
ciscoasa#
?Bad filename
%Error parsing filename (Bad file number)
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#interface GigabitEthernet1/4
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)# policy-map gobal_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#inspect ftp
Copy
Paste
Top
Time: 142:38:55
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete


WAN router B
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0, sourced by
00D0.97B7.4926
%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0, sourced by
00D0.97B7.4926
Router(config-if)#interface GigabitEthernet0/1
%Invalid interface type and number
Router(config)#interface GigabitEthernetEnter configuration commands, one per line. End
with CNTL/Z.
Router(config)#interface GigabitEthernet2/0
Router(config-if)#ip address 10.0.2.1 255.255.255.252
Router(config-if)# description Link to WAN Router S
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to down
Router(config-if)#interface GigabitEthernet3/0
Router(config-if)# ip address 10.0.1.1 255.255.255.252
Router(config-if)# description Link to WAN Router L
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to down
Router(config-if)#interface GigabitEthernet3/0
Router(config-if)#ip route 192.168.30.0 255.255.255.0 10.0.2.2
Router(config)#
Router(config)#interface GigabitEthernet2/0
Router(config-if)#ip route 192.168.20.0 255.255.255.0 10.0.1.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
save memory
^
% Invalid input detected at '^' marker.
Router#Enter configuration commands, one per line. End with CNTL/Z.
Copy
Paste
Top



Appendix E: VLAN and Subnet Allocation Details

VLAN allocation Table

VLAN ID	VLAN Name	Subnet ID	Subnet Mask	Purpose	Devices Included	Key Security Measures	WPA-PSK
10	Front Desk	192.168.2.64/29	255.255.255.248	Customer check-in/out operations	Wired PCs, Kiosks	ACLs, Firewall rules	FrontDesk123
21	Public Areas Wi-Fi	192.168.1.128/25	255.255.255.128	Public Wi-Fi	Lobby, Restaurant APs	VLAN Isolation, QoS Policies	Lobby.connect
22	Guest Room Wi-Fi	192.168.1.192/26	255.255.255.192	Private Guest Room Wi-Fi	Guest Room APs, Smart Devices	WPA3, VLAN ACLs, Enhanced QoS Policies	Room.connect
40	Retail Boutique	192.168.40.0/26	255.255.255.192	Retail payment & inventory	POS Systems, Inventory Devices	Encrypted Transactions	Shop.connect
50	Data Center	192.168.50.0/25	255.255.255.128	Critical infrastructure	DHCP, DNS, Web Servers	Strict Access Controls	
60	WAN Connectivity	192.168.70.0/30	255.255.255.252	Point-to-point WAN	WAN Routers, VPN Gateways	VPN Encryption	
70	Network Management	192.168.80.0/27	255.255.255.224	Network monitoring	Admin PCs, Monitoring Tools	RBAC, Restricted Internet Access	Manager@2025
80	Firewall	192.168.90.0/28	255.255.255.240	Centralized security	Firewall Appliances	Encrypted Traffic, VLAN ACLs	admin123

IPv4 Address Allocation Table

Subnet Name	Subnet ID	Subnet Mask	Usable IP Range	Broadcast Address	Purpose	Devices Included
Front Desk	192.168.2.64/29	255.255.255.248	192.168.2.65-70	192.168.2.71	Customer check-in/out operations	Wired PCs, Check-in Kiosks
Public Areas	192.168.1.128/25	255.255.255.128	192.168.1.129-254	192.168.1.255	Public area Wi-Fi	Lobby, Restaurant APs
Guest Rooms	192.168.1.192/26	255.255.255.192	192.168.1.193-254	192.168.1.255	Private Guest Room Wi-Fi	Guest Room APs, Smart Devices
Retail Boutique	192.168.40.0/26	255.255.255.192	192.168.40.1-62	192.168.40.63	Retail payment & inventory	POS Systems, Inventory Devices
Data Center	192.168.50.0/25	255.255.255.128	192.168.50.1-126	192.168.50.127	Critical infrastructure	DHCP, DNS, Web Servers
WAN Connectivity	192.168.70.0/30	255.255.255.252	192.168.70.1-2	192.168.70.3	Point-to-point WAN	WAN Routers, VPN Gateways
Network Mgmt	192.168.80.0/27	255.255.255.224	192.168.80.1-30	192.168.80.31	Network monitoring	Admin PCs, Monitoring Tools
Firewall	192.168.90.0/28	255.255.255.240	192.168.90.1-14	192.168.90.15	Centralized network security	Firewall Appliances

Appendix C: Device lists

Please note that the devices listed below are represented by the ones seen in my design

Ground Floor devices

Category	Model	Active Devices	Backup Devices	Purpose
ISP Router	Cisco 5105	1	1	WAN routing and external connectivity for Head Office
Firewall	Cisco ASA 5506-X	2	1	Network Security (High)
WAN Router	Cisco Catalyst 9600	1	0	Core routing for WAN
Core Switch	Cisco Catalyst 9500	1	1	Core routing for Ground Floor
Distribution Switch	Cisco Catalyst 9300	2	1	VLAN segmentation for Ground Floor
Wireless LAN Controller	Cisco Catalyst 9800	1	0	Wireless AP management for Ground Floor
Access Switch	Cisco Catalyst 9300	2	1	Wired device connections
Access Point	Cisco Catalyst 9100	6	0	Wi-Fi connectivity for public areas
Admin PC	Dell OptiPlex 5090	1	0	Administrative management
Wired POS System	Verifone VX 520	2	0	Point of Sale for hotel boutique

Front Desk PC	HP EliteDesk 800	6	0	Front desk operations
Rapid Check-In PC	HP All-in-One 24	2	0	Self-service check-in/out

1st Floor devices

Category	Model	Active Devices	Backup Devices	Purpose
Core Switch	Cisco Catalyst 9500	1	1	Core routing for First Floor
Wireless LAN Controller	Cisco Catalyst 9800	1	0	Wireless AP management for First Floor
Distribution Switch	Cisco Catalyst 9300	1	1	VLAN segmentation for First Floor
Access Switch	Cisco Catalyst 9300	1	1	Wired device connections
Access Point	Cisco Aironet 1850	6	0	Wi-Fi connectivity for guest rooms and public areas
Server	Dell PowerEdge R740	4	0	Application, web, and database hosting