Final Project from Networking Technologies Lab 2024/2025

Name & Surname : Artsiom Litvinchuk

Index Number: 54075

Group: IN5

Topic: Corporate Network Design for Techlead Innovation Ltd. (fictional name)

Part 1: Objective of the task:

The goal of the project is to design and implement a scalable, secure, and efficient network infrastructure for the new building of Techlead Innovation Ltd. (a fictional name), a company specializing in delivering innovative cloud solutions. The project aims to ensure seamless connectivity, effective management of IT resources, and protection against internal and external threats.

As part of the project, it is necessary to meet the requirements for availability, redundancy, and data protection, as well as enable communication between different departments of the company using advanced technologies such as VLAN, VoIP, DMZ, OSPF, DHCP, EtherChannel, and Cisco ASA firewalls.

The project includes the implementation of a hierarchical network model, configuration of VLAN networks with inter-VLAN routing, central management of wireless networks, redundancy and failover solutions, and IP resource allocation according to designated subnets. The final result of the project is a comprehensive network environment that supports business operations, ensures data protection, and provides tools for further expansion and adaptation of the infrastructure in response to future needs of Techlead Innovation Ltd.

Brief description of the project implementation:

The project involved the design and implementation of a corporate network for Techlead Innovation Ltd., providing a secure and efficient infrastructure. The network was based on a hierarchical model with the use of VLANs, enabling traffic isolation between departments and security management. The configuration included inter-VLAN routing, dynamic IP address assignment (DHCP), centralized Wi-Fi management, and access protection using ACL lists and Cisco ASA firewalls. Redundancy in connections was implemented to increase reliability, and key servers were placed in the DMZ zone. The network was tested to ensure compliance with requirements and scalability for the future.

Part 2: Addressong Plan

(Category)	(Network address / Subnet mask)	Host addresses	(Default gateway)	Broadcast
Management	192.168.20.0/24	192.168.20.1 - 192.168.20.254	192.168.20.1	192.168.20.255
WLAN	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.1	10.20.255.254
LAN	172.16.0.0/16	172.16.0.1 - 172.16.255.254	172.16.0.1	172.16.255.255
VoIP	172.30.0.0/16	172.30.0.1 - 172.30.255.254	172.30.0.1	172.30.255.255
DMZ	10.11.11.0/27	10.11.11.1 - 10.11.11.30	10.11.11.1	10.11.11.31
Inside servers	10.11.11.32/27	10.11.11.33 - 10.11.11.62	10.11.11.33	10.11.11.63

Between the cloud, ISP, firewalls, routers, and layer 3 switches.

Area	Network Address
(Cloud Area)	8.0.0.0/8
ISP1 — Internet	20.20.20.0/30
ISP2 — Internet	30.30.30.0/30
ISP1 — FWL1	105.100.50.0/30
ISP1 — FWL2	105.100.50.4/30
ISP2 — FW1	205.200.100.0/30
ISP2 — FW2	205.200.100.4/30
FWL1 — MLSW1	10.2.2.0/30
FWL1 — MLSW2	10.2.2.4/30
FWL2 — MLSW1	10.2.2.8/30
FWL2— MLSW2	10.2.2.12/30

Part 3: Technologies Implemented:

The network project for Cytonn Innovation Ltd. (fictional name) utilized the following devices:

1. **Routers**
   - Two routers with routing protocol support (OSPF) for connecting to ISP and routing between VLANs.

2. **Firewalls**
   - Two Cisco ASA 5500-X series devices providing network security and access control.

3. **Layer 3 Switches (L3)**
   - Catalyst 3850 switches (48-port) for the distribution layer, supporting VLAN routing.

4. **Layer 2 Switches (L2)**
   - Catalyst 2960 switches (48-port) for network segmentation and connecting hosts in various VLANs.

5. **Wireless LAN Controllers (WLC)**
   - Two Cisco WLC controllers enabling central management of Access Points (WAP).

6. **Access Points (WAP)**
   - Lightweight Access Points (LAP) deployed on each floor to provide WLAN coverage.

7. **Servers**
   - Physical servers for virtualization, running various virtual machines: DHCP server, DNS, RADIUS, FTP, Web, Email, NAS.

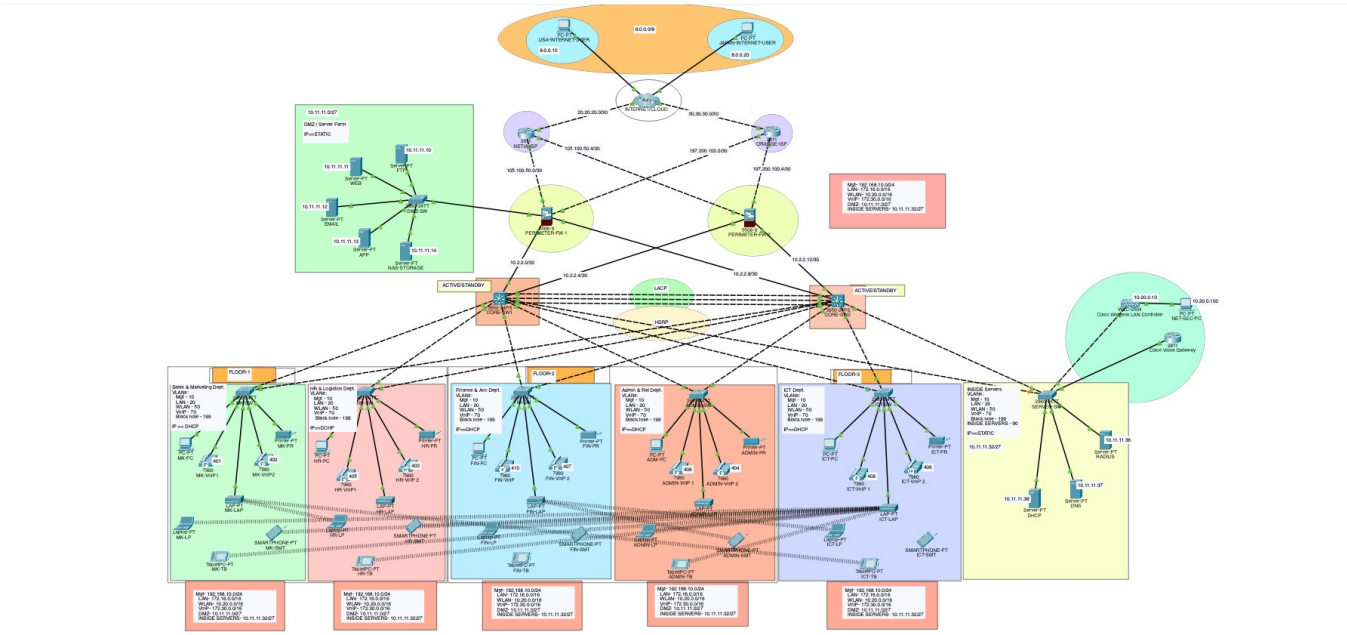
8. **VoIP Phones**
   - Cisco voice gateway and IP phones in departments enabling voice communication via VoIP.

9. **Other Devices**
   - Cisco ASA firewall configured to protect and filter traffic in DMZ and internal zones.
   - HSRP (Hot Standby Router Protocol) for enhanced redundancy and failover.

10. **End Devices**
    - Computers, laptops, and mobile devices in departments using LAN and WLAN, as well as a dedicated computer for remote tasks managed via SSH.

These devices, along with advanced VLAN configuration, ACLs, EtherChannel, and WLC management, ensure the

Część 4: Logical schema

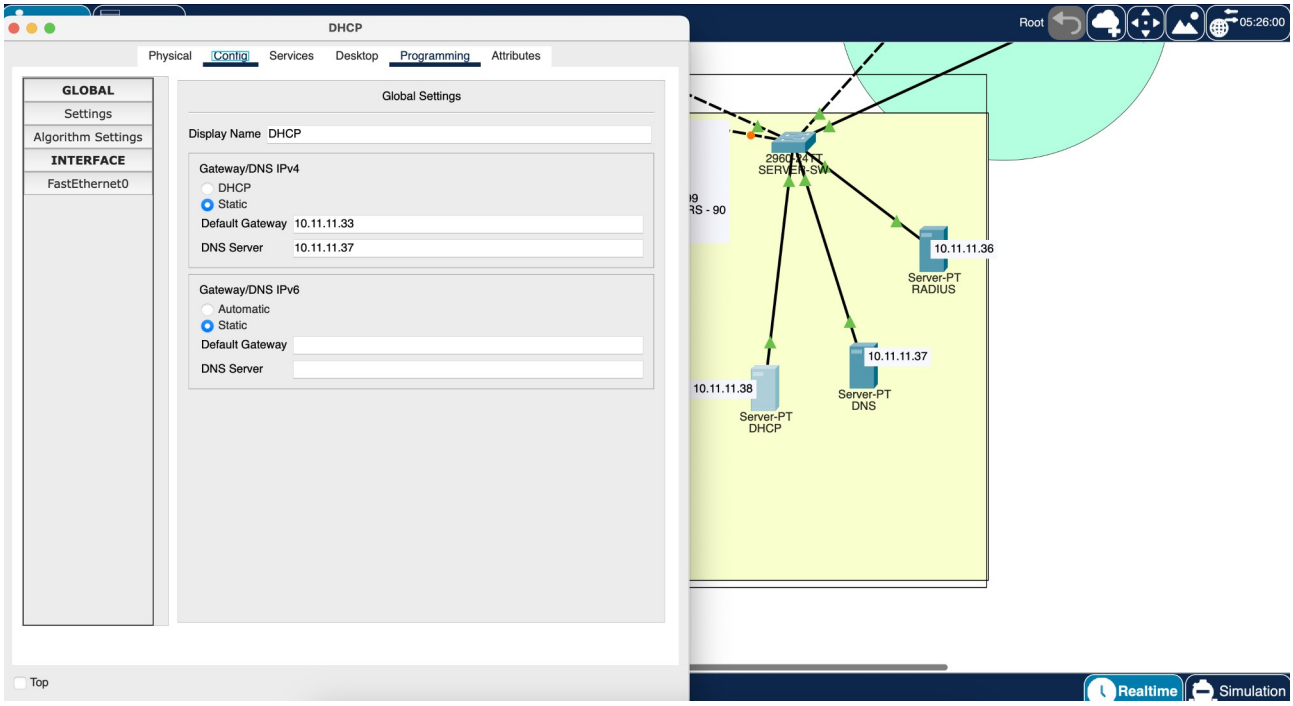


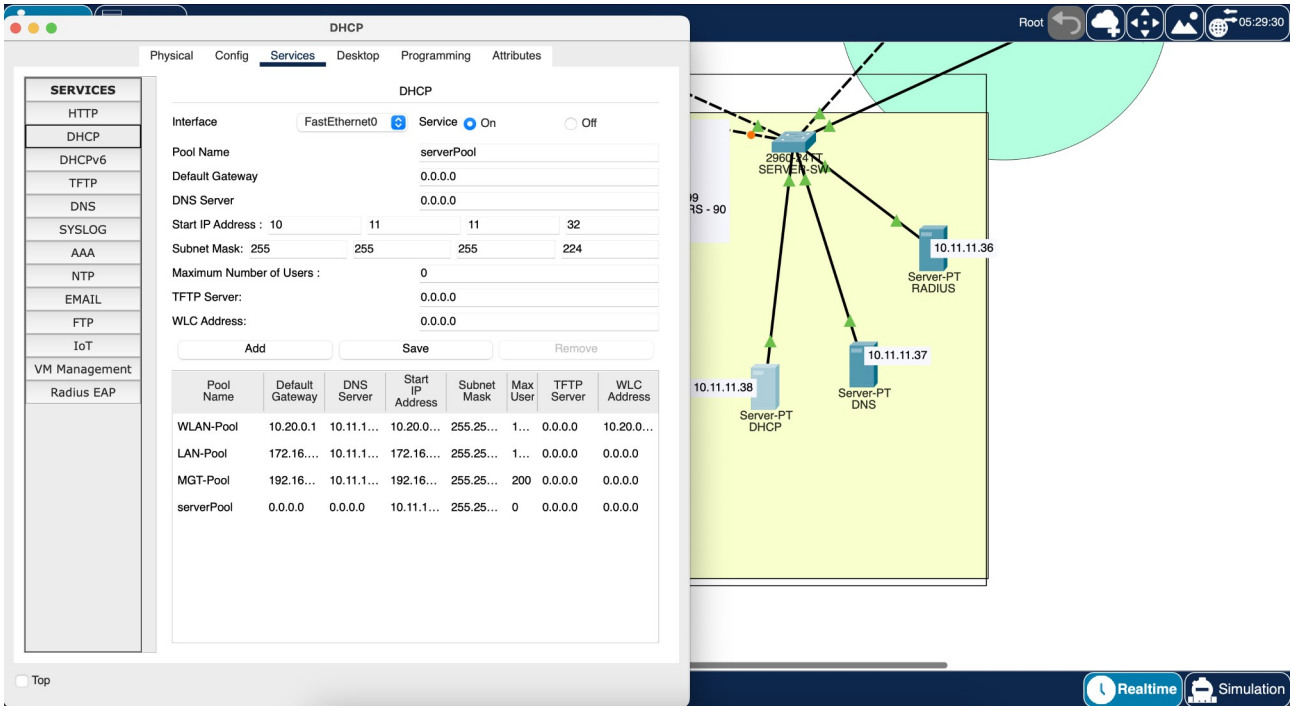
Part 5: Network device configuration exapmle

Routre configuration:

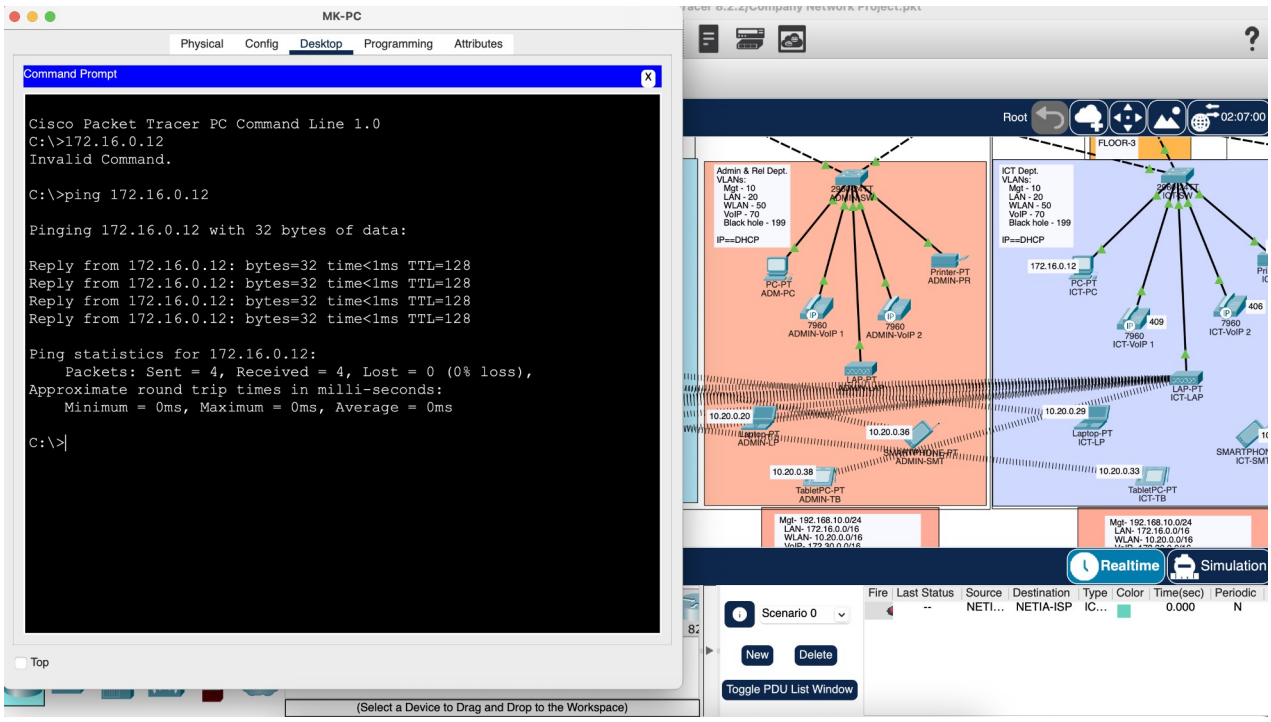
```
hostname Router1
enable secret cisco
line vty 0 4
password cisco
login
exit
service password-encryption
interface GigabitEthernet0/2
ip address 20.20.20.1 255.255.255.252
no shutdown
exit
router ospf 1
network 20.20.20.0 255.255.255.252
exit
access-list 10 permit
```

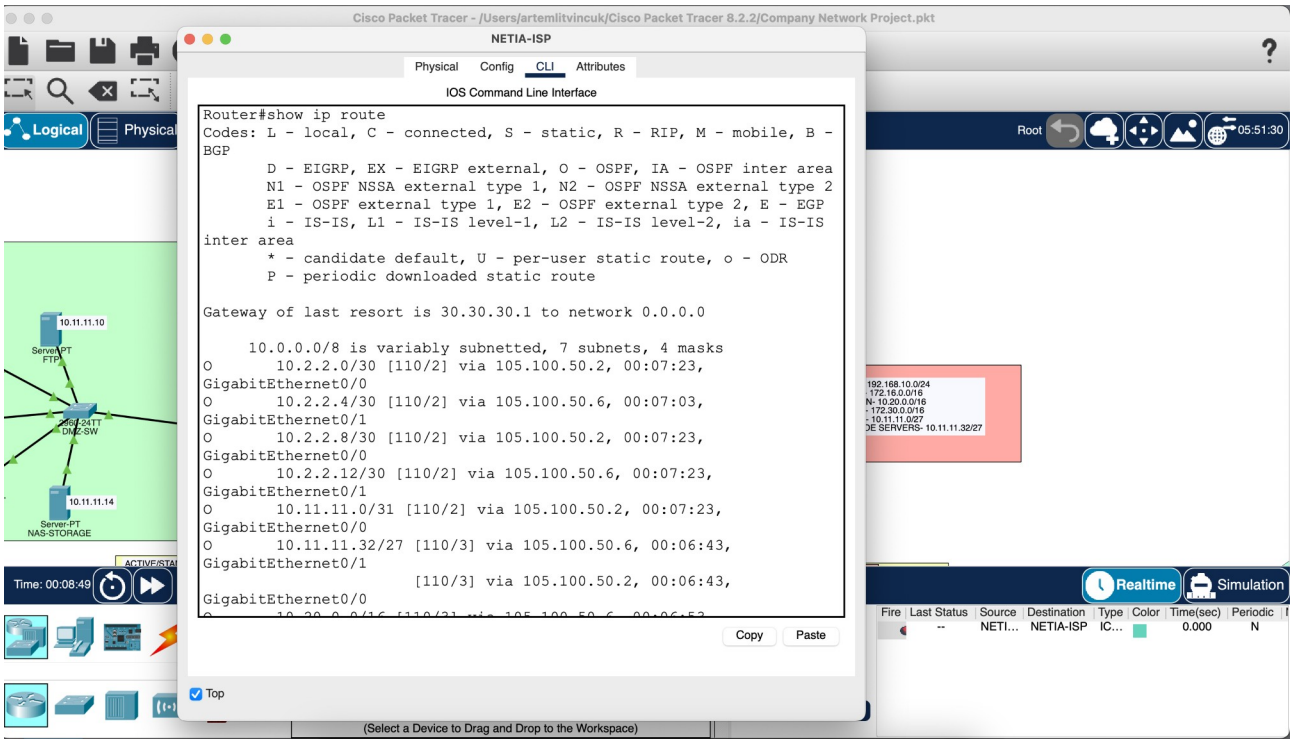
DHCP configuration:

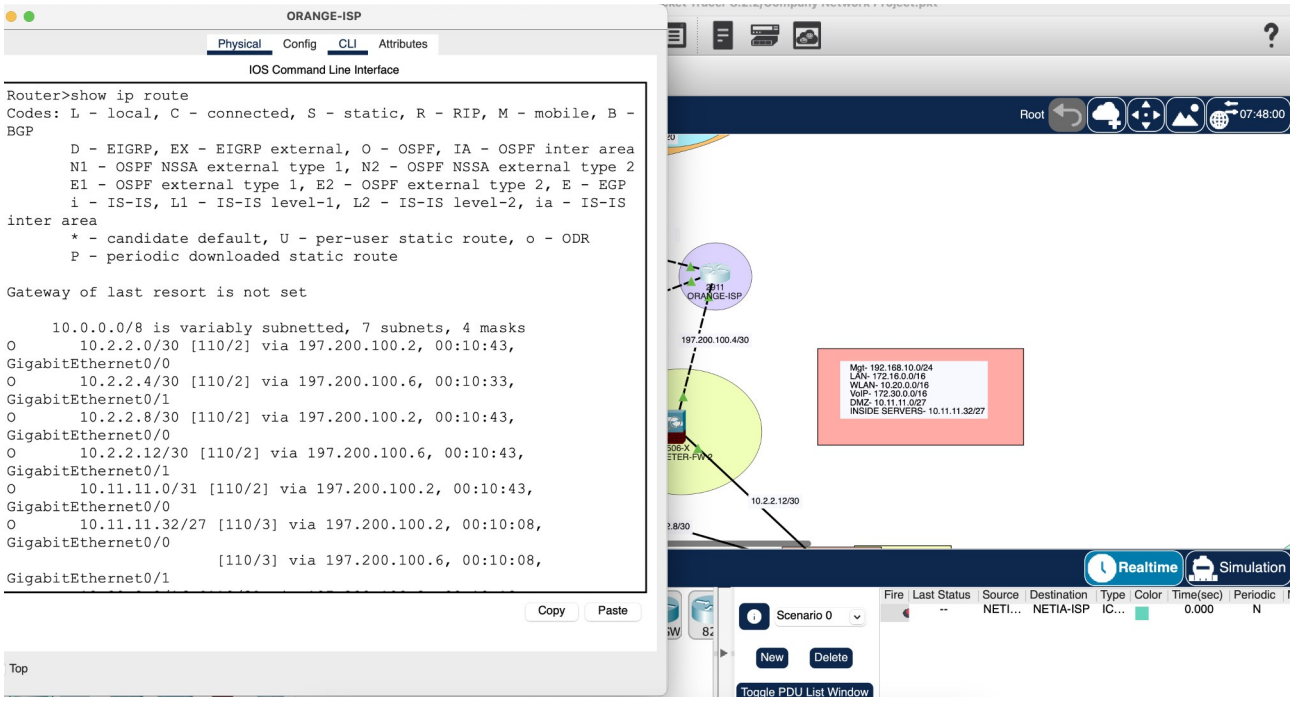


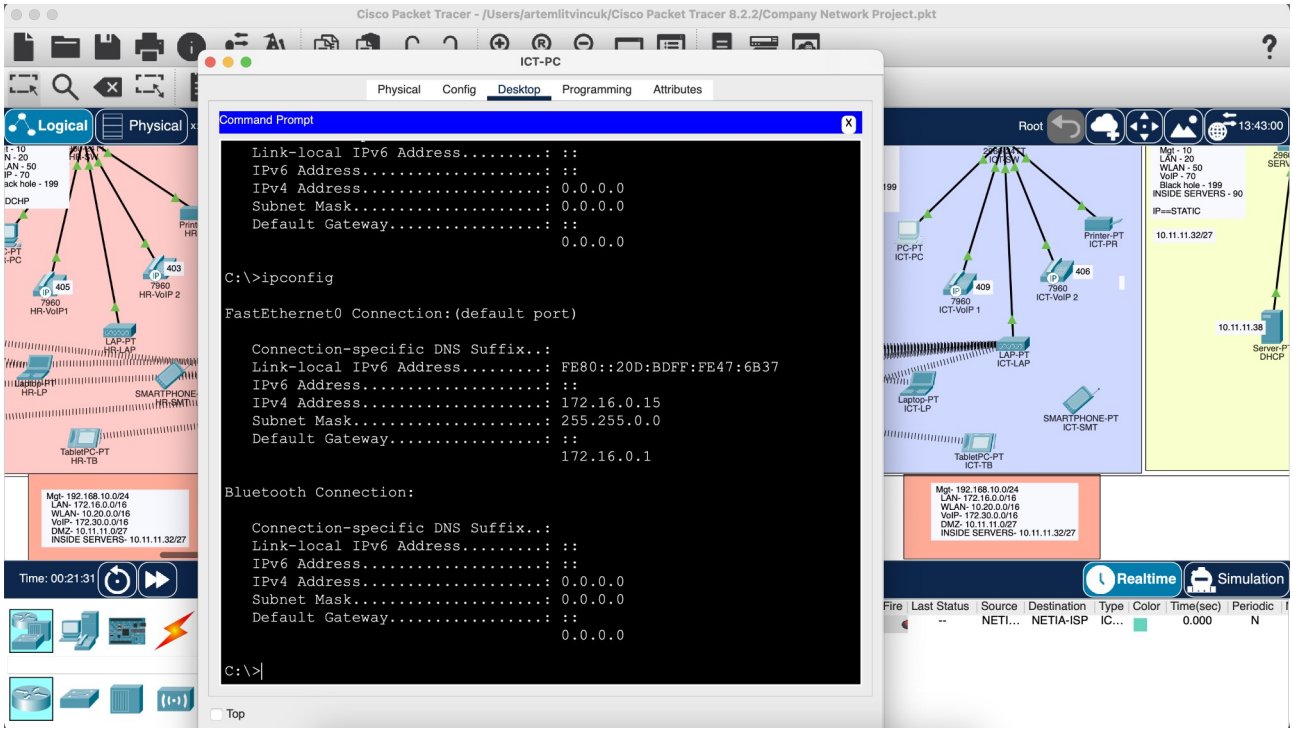


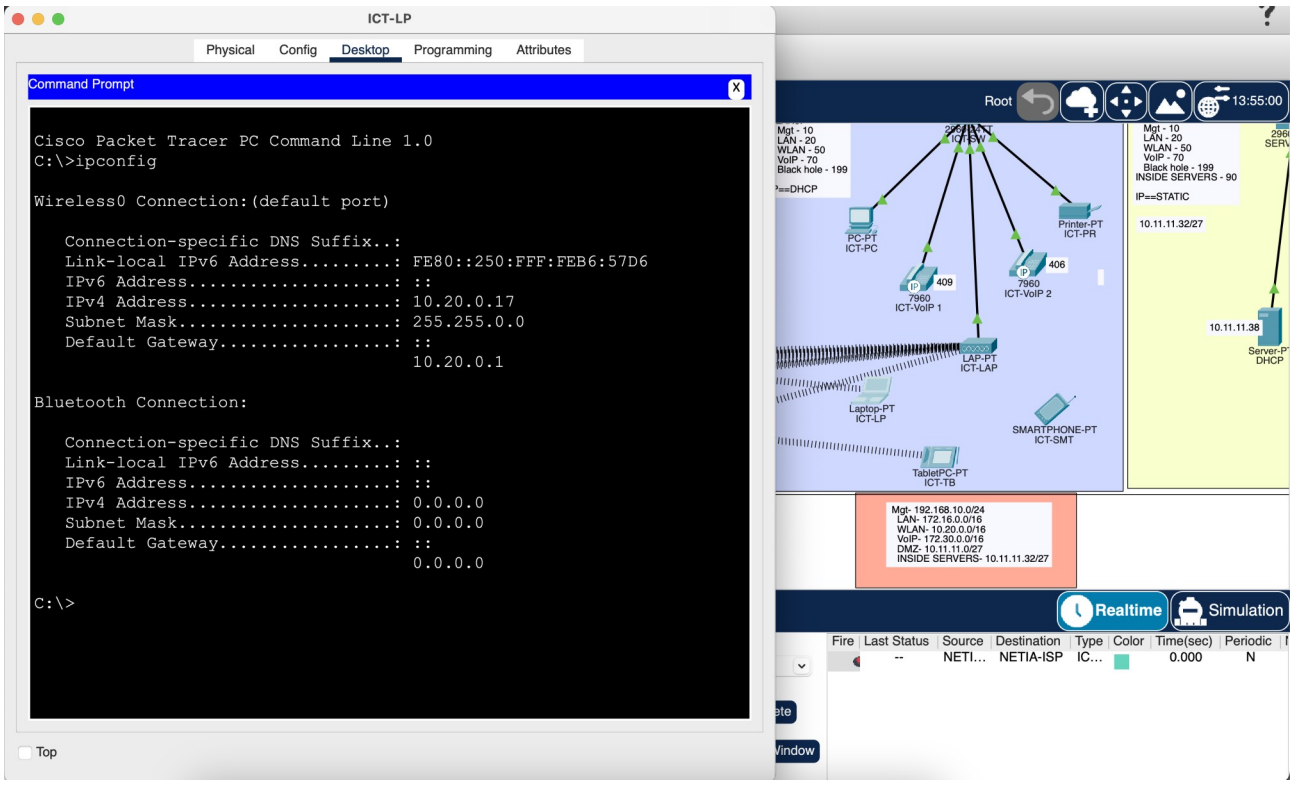
Part 6: Network implementation testing






ORANGE-ISP
Physical
Config
CLI
Attributes
IOS Command Line Interface
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 not set
10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
O 10.2.2.0/30 [110/2] via 197.200.100.2, 00:10:43, GigabitEthernet0/0
O 10.2.2.4/30 [110/2] via 197.200.100.6, 00:10:33, GigabitEthernet0/1
O 10.2.2.8/30 [110/2] via 197.200.100.2, 00:10:43, GigabitEthernet0/0
O 10.2.2.12/30 [110/2] via 197.200.100.6, 00:10:43, GigabitEthernet0/1
O 10.11.11.0/31 [110/2] via 197.200.100.2, 00:10:43, GigabitEthernet0/0
O 10.11.11.32/27 [110/3] via 197.200.100.2, 00:10:08, GigabitEthernet0/0
[110/3] via 197.200.100.6, 00:10:08, GigabitEthernet0/1
Copy
Paste
Top
Root
07:48:00
ORANGE-ISP
197.200.100.4/30
10.2.2.12/30
Mgt- 192.168.10.0/24
LAN- 172.16.0.0/16
WLAN- 10.20.0.0/16
VoIP- 172.30.0.0/16
DMZ- 10.11.11.0/27
INSIDE SERVERS- 10.11.11.32/27
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
NETI...
NETIA-ISP
IC...
0.000
N


Cisco Packet Tracer - /Users/artemlitvincuk/Cisco Packet Tracer 8.2.2/Company Network Project.pkt
ICT-PC
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::20D:BDFF:FE47:6B37
IPv6 Address.....: ::
IPv4 Address.....: 172.16.0.15
Subnet Mask.....: 255.255.0.0
Default Gateway.....: ::
172.16.0.1
Bluetooth Connection:
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
C:\>
Top
Logical
Physical
Time: 00:21:31
Root
13:43:00
Realtime
Simulation



Part 7: Conclusion

The project of creating the network infrastructure for Techlead Innovation sp. z o.o. (fictional name) was a significant step towards providing robust, secure, and efficient communication services. During the project's execution, many key components were successfully implemented, contributing to improving the operational efficiency of the company.

What has been achieved:

Secure network architecture: The use of DMZ zones and appropriate firewalls enabled effective protection of the company's data and resources against both external and internal threats.

Performance and redundancy: The implementation of technologies such as EtherChannel and HSRP protocols ensured increased availability and resilience of the network against failures.

VLAN management: Well-organized VLAN networks allowed for effective traffic segregation and better management of network resources, which is critical for the operational performance of different departments.

Cloud access: The infrastructure was prepared for integration with cloud computing, enabling teams to easily access global resources and services.

What can still be improved:

Monitoring and reporting: The introduction of more advanced network traffic monitoring systems and real-time data analysis would allow for faster responses to incidents and optimization of network performance.

Infrastructure expansion: Given the company's dynamic growth, it is advisable to plan for future infrastructure expansions, such as additional wireless access points and servers, to ensure continued growth without bandwidth issues.

Automation: Implementing network management automation tools could increase operational efficiency and reduce the risk of human errors.