Projekt końcowy z TS lab 2024/25

Imię i nazwisko : Artsiom Litvinchuk

Numer indeksu: 54075

Grupa: IN5

Temat: Projekt sieci firmowej dla Techlead Innovation sp. z o.o. (nazwa wymyślona)

Część 1: Cel realizowanego zadania:

Celem projektu jest zaprojektowanie i wdrożenie skalowalnej, bezpiecznej i wydajnej infrastruktury sieciowej dla nowego budynku Techlead Innovation sp. z o.o. (nazwa wymyślona) , firmy specjalizującej się w dostarczaniu innowacyjnych rozwiązań w chmurze. Projekt ma na celu zapewnienie bezproblemowej łączności, efektywnego zarządzania zasobami IT oraz ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi. W ramach realizacji projektu konieczne jest spełnienie wymogów dotyczących dostępności, redundancji i ochrony danych, a także umożliwienie komunikacji między różnymi działami firmy przy użyciu zaawansowanych technologii, takich jak VLAN, VoIP, DMZ, OSPF, DHCP, EtherChannel oraz firewalli Cisco ASA.

Projekt uwzględnia wdrożenie hierarchicznego modelu sieci, konfigurację sieci VLAN z trasowaniem między VLAN-ami, centralne zarządzanie siecią bezprzewodową, rozwiązania redundancji i failoveru oraz przydział zasobów IP według przeznaczonych podsieci. Finalnym efektem projektu jest kompleksowe środowisko sieciowe, które wspiera działalność biznesową, zapewnia ochronę danych oraz dostarcza narzędzi do dalszej rozbudowy i adaptacji infrastruktury w odpowiedzi na przyszłe potrzeby Techlead Innovation sp. z o.o. .

Krótki opis realizacji projektu

W projekcie zaprojektowano i wdrożono sieć firmową dla Techlead Innovation sp. z o.o. , zapewniającą bezpieczną i wydajną infrastrukturę. Sieć została oparta na hierarchicznym modelu z użyciem VLAN-ów, co umożliwia izolację ruchu między działami oraz zarządzanie bezpieczeństwem. Konfiguracja obejmowała routing między VLAN-ami, dynamiczne przydzielanie adresów IP (DHCP), centralne zarządzanie Wi-Fi oraz ochronę dostępu za pomocą list ACL i firewalli Cisco ASA. Zastosowano redundancję połączeń, aby zwiększyć niezawodność, a serwery kluczowe umieszczono w strefie DMZ. Sieć przetestowano, zapewniając zgodność z wymaganiami oraz skalowalność na przyszłość.

Część 2: Plan adresacji

Kategoria (Category)	**Adres Sieci / Maska (Network address / Subnet mask)**	**Adresy hostów (zakres) Host addresses**	**Domyślna Brama Sieciowa (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

Między chmurą, ISP, zaporami sieciowymi, routerami i przełącznikami warstwy trzeciej

Numer	**Adres Sieciowy**
Zona Chmury (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

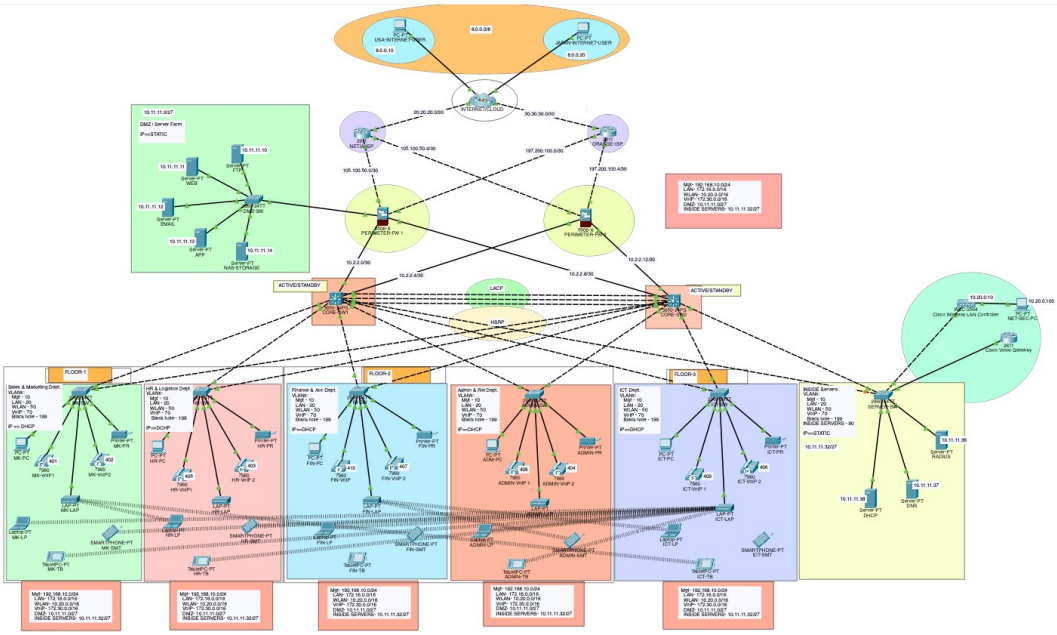
Część 3: Wykaz wykorzystanych urządzeń:

W projekcie sieciowym dla Cytonn Innovation Ltd. (nazwa wymyślona) wykorzystano następujące urządzenia:

1. **Routery**
    - Dwa routery z obsługą protokołów routingu (OSPF) do łączenia z ISP i routingu między VLAN-ami.
2. **Zapory sieciowe (Firewall)**
    - Dwa urządzenia Cisco ASA serii 5500-X zapewniające bezpieczeństwo sieci i kontrolę dostępu.
3. **Przełączniki warstwy 3 (L3)**
    - Przełączniki Catalyst 3850 (48-portowe) dla warstwy dystrybucji, obsługujące routing VLAN.
4. **Przełączniki warstwy 2 (L2)**
    - Przełączniki Catalyst 2960 (48-portowe) do segmentacji sieci i podłączenia hostów w różnych VLAN-ach.
5. **Kontrolery sieci bezprzewodowej (WLC)**
    - Dwa kontrolery WLC firmy Cisco, umożliwiające centralne zarządzanie punktami dostępowymi (WAP).
6. **Punkty dostępowe (WAP)**
    - Lekkie punkty dostępowe (LAP) rozmieszczone na każdym piętrze w celu zapewnienia zasięgu sieci WLAN.
7. **Serwery**
    - Fizyczne serwery do wirtualizacji, obsługujące różne maszyny wirtualne: serwer DHCP, DNS, Radius, FTP, Web, Email, NAS.
8. **Telefony VoIP**
    - Bramka głosowa Cisco oraz telefony IP w działach umożliwiające komunikację głosową przez VoIP.
9. **Inne urządzenia**
    - Cisco ASA firewall skonfigurowany do ochrony i filtracji ruchu w strefach DMZ i wewnętrznej.
    - HSRP (Hot Standby Router Protocol) dla zwiększenia redundancji i zapewnienia przełączania awaryjnego.
10. **Urządzenia końcowe**
    - Komputery, laptopy i urządzenia mobilne w działach, które korzystają z sieci LAN i WLAN, oraz dedykowany komputer dla zadań zdalnych administrowanych przez SSH.

Urządzenia te, wraz z zaawansowaną konfiguracją VLAN, ACL, EtherChannel i zarządzaniem przez WLC, zapewniają bezpieczeństwo, wysoką wydajność i skalowalność sieci.

Część 4: Schemat logiczny sieci

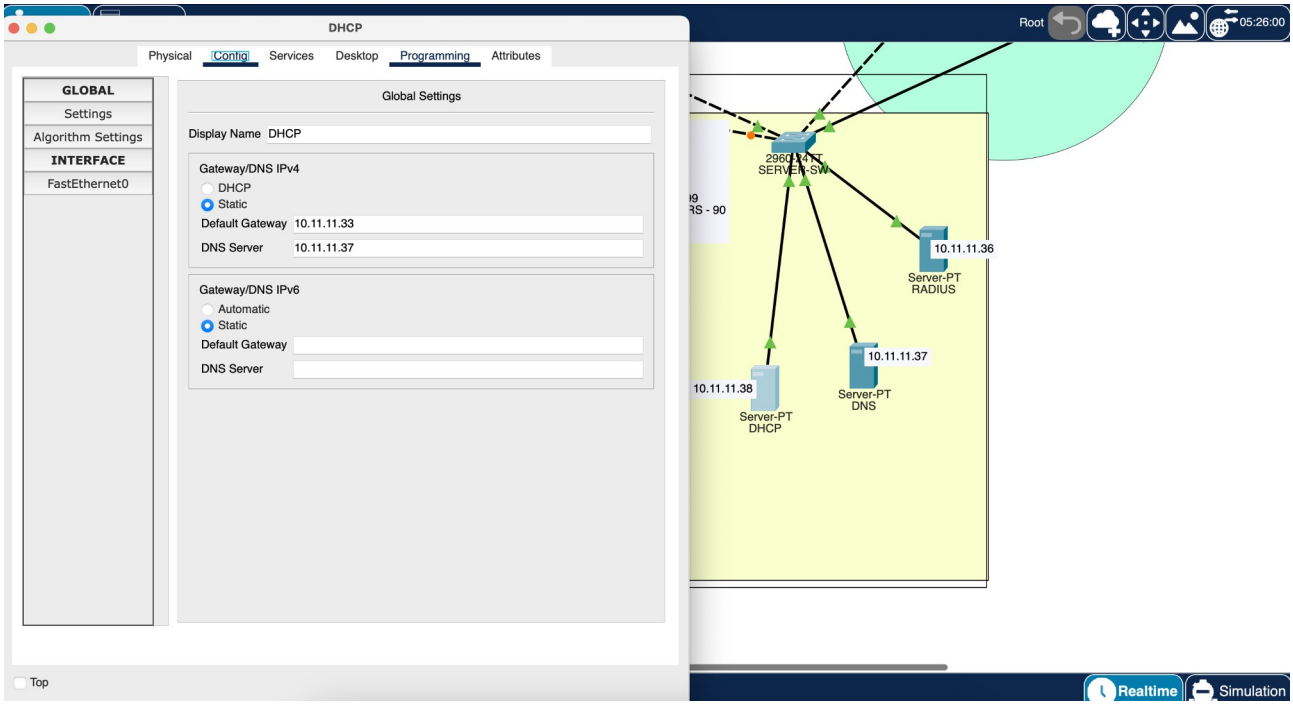


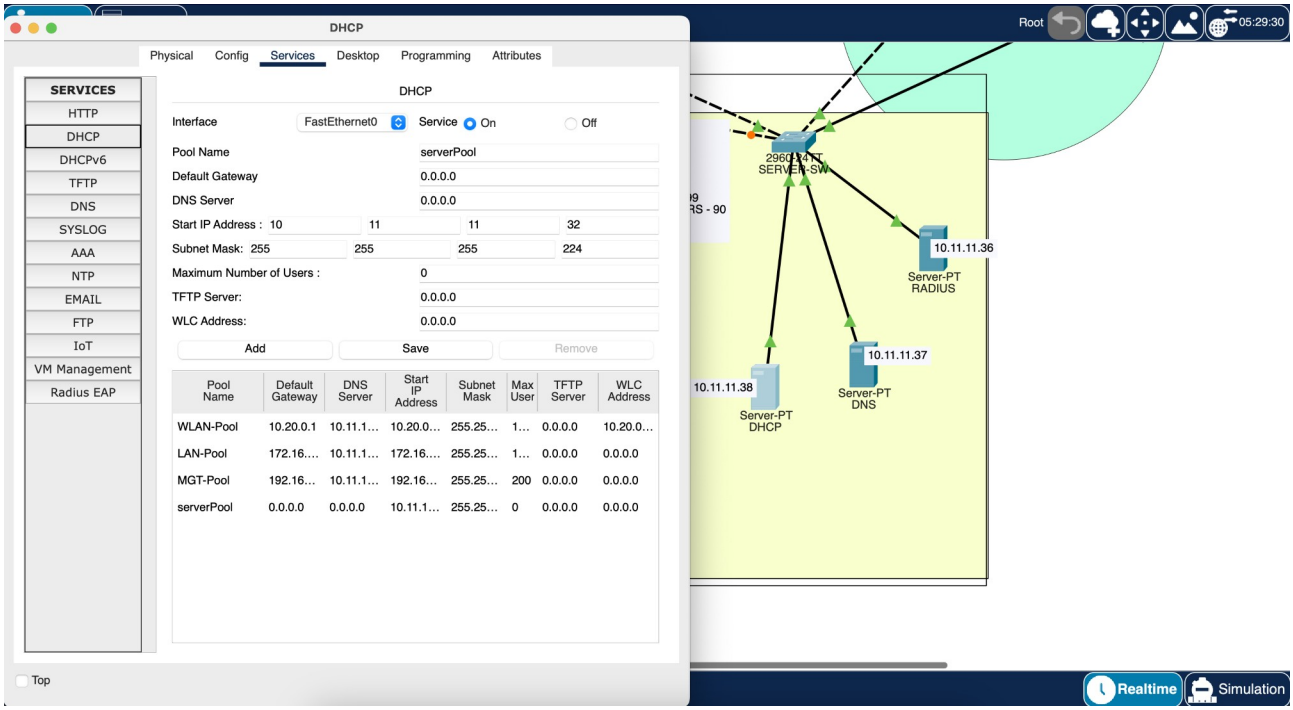
Część 5: Opis konfiguracji urządzeń:

Konfiguracja routera:

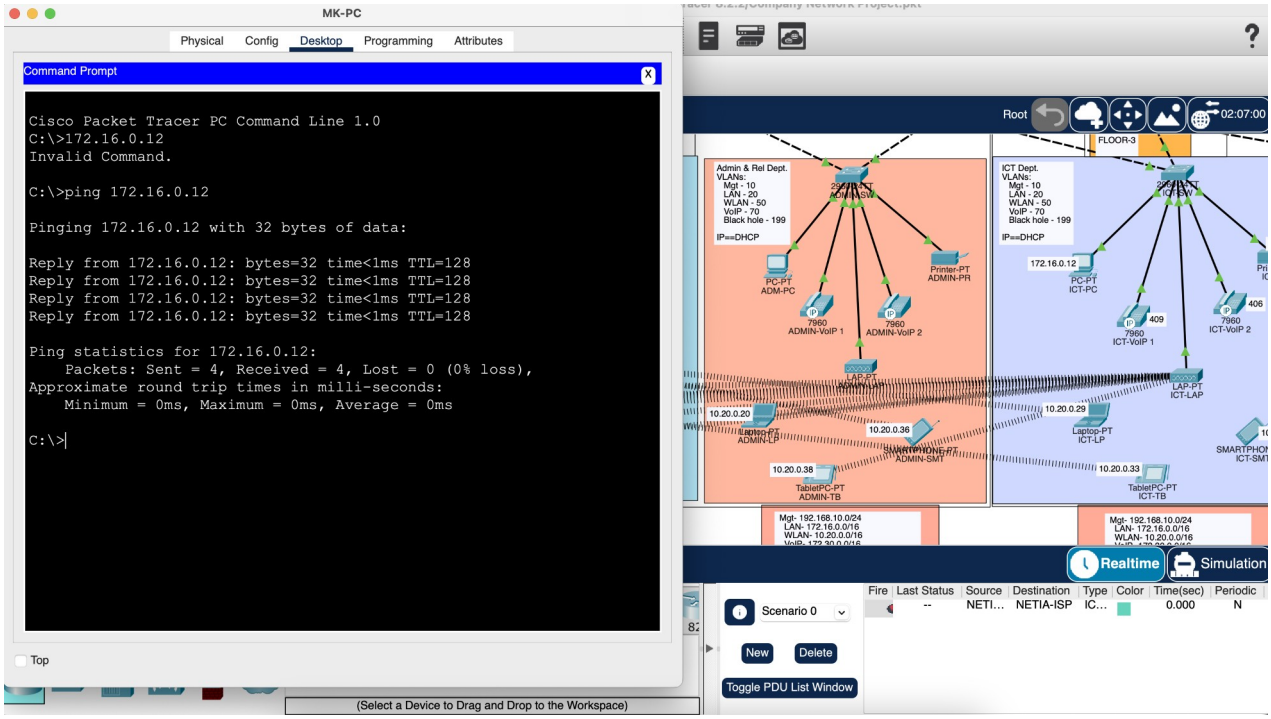
```
hostname Router1
enable secret cisco
line vty 0 4
password cisco
login
exit
service password-encryption
interface GigabitEthernet0/2
ip address 20.20.20.1 255.255.255.252
no shutdown
exit
router ospf 1
network 20.20.20.0 255.255.255.252
exit
access-list 10 permit
```

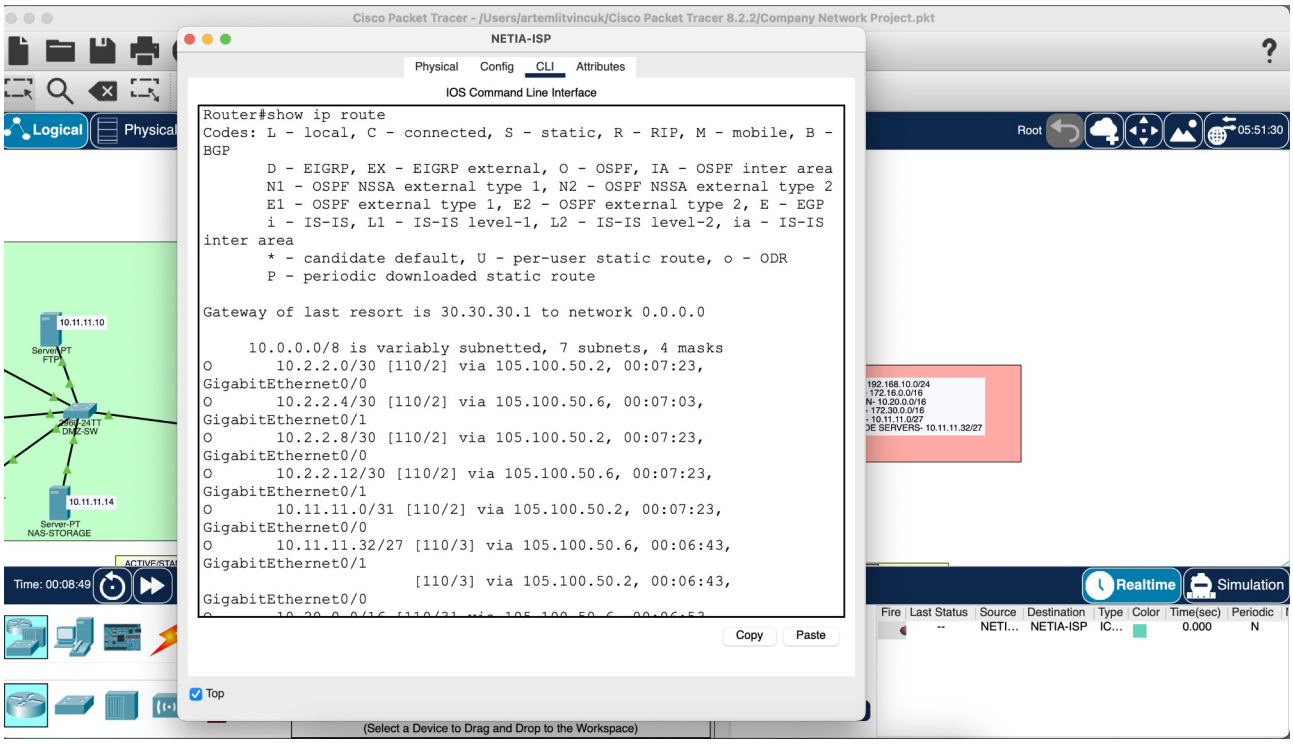
Konfiguracja serwera DHCP:

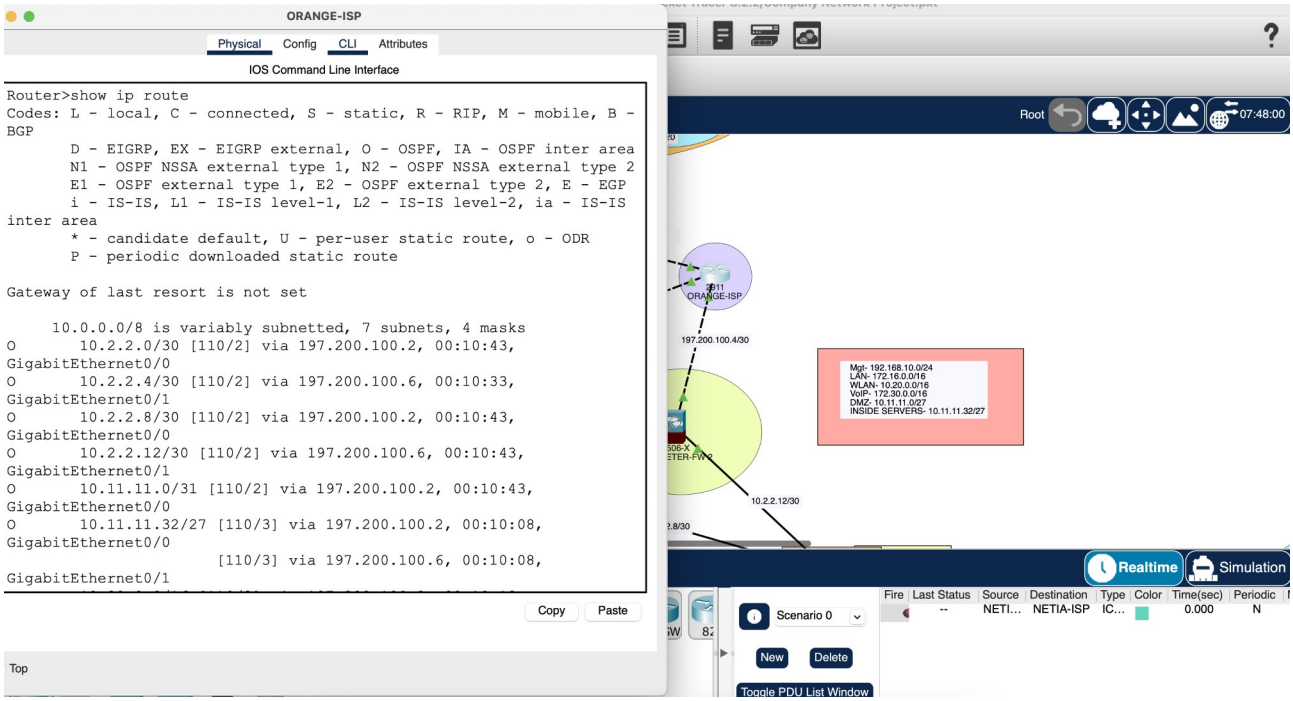


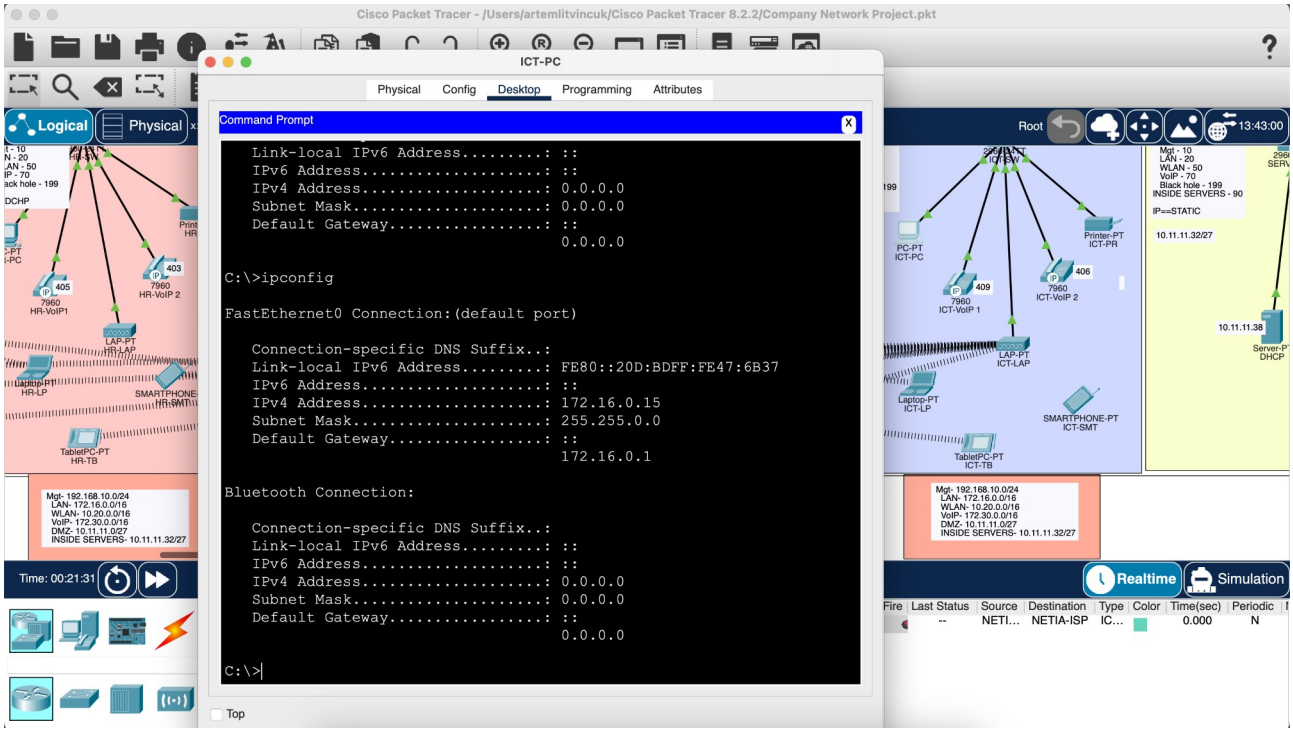


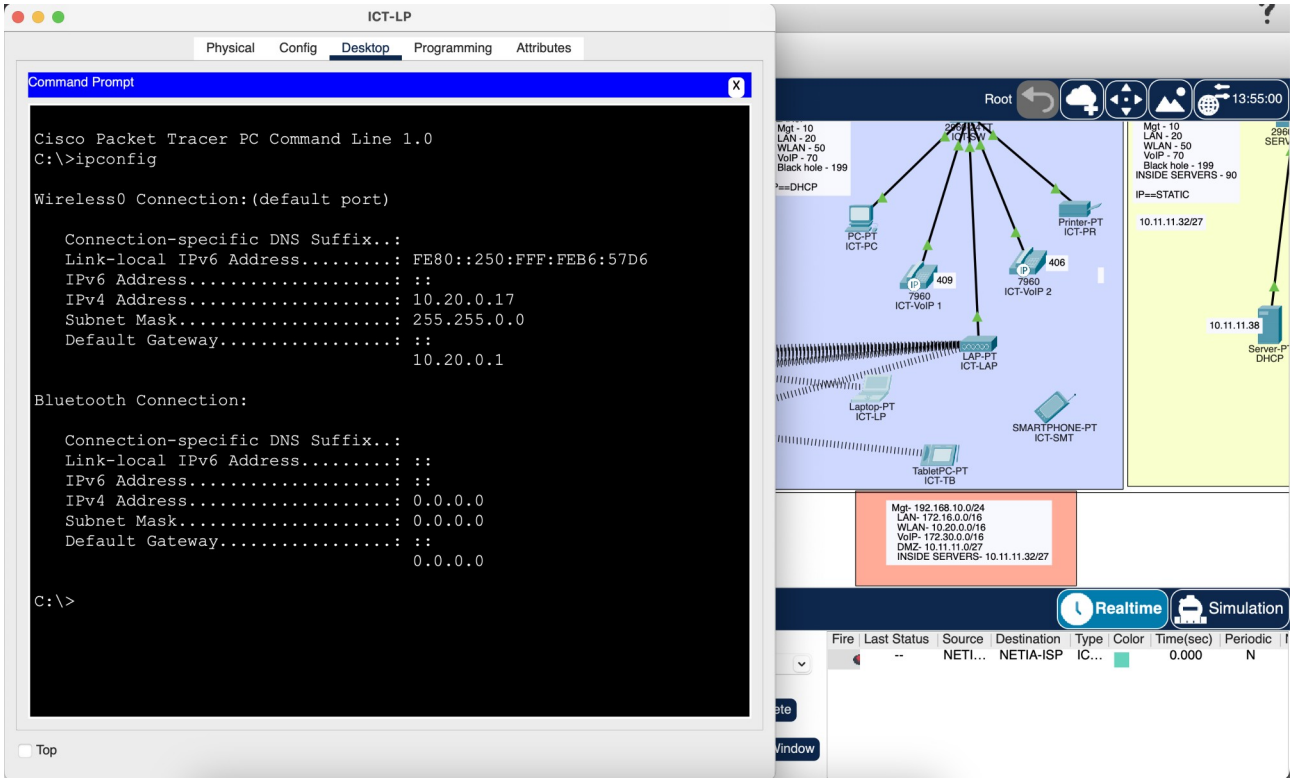
Część 6: Test zrealizowanej sieci






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
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic


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
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic



Część 7: Wnioski końcowe

Projekt stworzenia infrastruktury sieciowej dla Techlead Innovation sp. z o.o. (nazwa wymyślona) był istotnym krokiem w kierunku zapewnienia solidnych, bezpiecznych i wydajnych usług komunikacyjnych. W trakcie realizacji projektu udało się zrealizować wiele kluczowych elementów, które przyczynią się do zwiększenia efektywności operacyjnej firmy.

Co udało się osiągnąć:

1. Bezpieczna architektura sieciowa: Zastosowanie stref DMZ oraz odpowiednich zapór sieciowych pozwoliło na skuteczne zabezpieczenie danych i zasobów firmy przed zagrożeniami zewnętrznymi i wewnętrznymi.
2. Wydajność i redundancja: Implementacja technologii takich jak EtherChannel oraz protokoły HSRP zapewniły zwiększoną dostępność i odporność sieci na awarie.
3. Zarządzanie VLAN: Dobrze zorganizowane sieci VLAN umożliwiły efektywną segregację ruchu oraz lepsze zarządzanie zasobami sieciowymi, co jest istotne dla wydajności operacyjnej różnych działów.
4. Dostęp do chmury: Infrastruktura została przygotowana do integracji z chmurą obliczeniową, co umożliwi zespołom łatwy dostęp do zasobów i usług globalnych.

Co można jeszcze poprawić:

1. Monitoring i raportowanie: Wprowadzenie bardziej zaawansowanych systemów monitorowania ruchu sieciowego oraz analizy danych w czasie rzeczywistym pozwoliłoby na szybsze reagowanie na incydenty oraz optymalizację działania sieci.

2. Rozbudowa infrastruktury: Z uwagi na dynamiczny rozwój firmy, warto przewidzieć przyszłe rozszerzenia infrastruktury, takie jak dodatkowe punkty dostępu bezprzewodowego oraz serwery, co zapewni dalszy rozwój bez problemów z przepustowością.

3. Automatyzacja: Wdrożenie narzędzi do automatyzacji procesów zarządzania siecią mogłoby zwiększyć efektywność operacyjną oraz zredukować ryzyko błędów ludzkich.

Podsumowanie

Projekt został w pełni zrealizowany, zapewniając nie tylko bezpieczeństwo i efektywność, ale także elastyczność potrzebną do dalszego rozwoju. W przyszłości, kontynuowanie inwestycji w rozwój infrastruktury będzie kluczowe dla dalszego sukcesu firmy.