VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY

COMPUTER NETWORK

ASSIGNMENT 2

DEVELOP A NETWORK APPLICATION

CC01 — SEMESTER 241

LECTURER : Prof. NGUYEN LE DUY LAI

Student	ID	Marks
Phan Chí Vỹ	2252938	100%
Lê Nhân Văn	2252899	100%
Nguyễn Hoàng Vũ	2252919	100%

HO CHI MINH CITY – 2024

TABLE OF CONTENT

1. Step 1 (1 point): Find out suitable network structures for buildings

A. Analyze the network system requirements of the main Site and the two Auxiliary Sites

- **Main site:**

● 2 buildings A and B (5 floors with 10 rooms/floor) equipped with computers and medical devices.

● The data center, IT, and Cabling Central Local (using patch panels gathering wires) are located in a separate room, 50 meters from buildings A and B.

● Medium-scale: 600 workstations, 10 servers, 12 networking devices (or maybe more with security-specific devices).

● The wireless connection has to be covered for the whole Site.

● Using new technologies for network infrastructure including wired and wireless connections, fiber cabling (GPON), and GigaEthernet 1GbE/10GbE/40GbE.

● The main Site subnetwork connects two other Sites (Site DBP and Site BHTQ) subnetworks by 2 leased lines for WAN connection with a load-balancing mechanism.

● Uses a mix of licensed and open-source software.

- **Auxiliary sites:**

● The building has 2 floors, the first floor is equipped with 1 IT room and 1 Cabling Central Local.

● Small-scale: 60 workstations, 2 servers, 5 or more networking devices

- **Non-functional requirements:**

● Shared dataflow and workload balancing between the main and auxiliary sites.

● Cope with the company's growth rate of 20% in 5 years.

● High security, high availability, robustness when problems occur, ease of upgrading

● The total download estimation is about 1000 MB/day and the upload estimate is 2000 MB/day.

- The total download estimation is about 500 MB/day and the upload estimation is 100 MB/day.
- WiFi-connected devices from customers' access for downloading are about 500 MB/day.

B. Make a checklist to be surveyed at the installation locations

Physical Infrastructure

1. **Preferred Topology**: What network layout do you prefer? (Bus, Star, Ring, Mesh, Tree)
2. **New or Existing Network**: Will this network expand the current setup, or start from scratch?
3. **Cabling Between Floors**: How are cables routed between floors?
4. **Cabling Standards**: What standards do you follow for cabling?
5. **Department Layout**: How many departments, and where are they located in each building?

Logical Infrastructure

1. **WAN Preference**: Which WAN type do you prefer, SD-WAN or MPLS?
2. **VPN Needs**: What are the main requirements for VPN access?
3. **Surveillance**: Any specific needs or preferences for security cameras?
4. **Hospital Services**: How many hospital functions need network access?

Cost, Security, and Risks

1. **Current Network Issues**: Are there any known problems with the current setup?
2. **Past Incidents**: Any past network issues or security breaches?
3. **Security Policies**: What security rules do you have for staff, departments, and customers?
4. **Budget Approval**: Is the current equipment and budget proposal acceptable?
5. **Budget Flexibility**: Is there flexibility in the budget if more is needed?

C. Define areas with high load (network load) to select the appropriate device configuration (load balancers are placed in necessary locations):

Network Load Balancers are designed to handle high traffic volumes by distributing requests based on network-level data like IP addresses and destination ports. Working at OSI Layer 4, they focus on basic packet information without analyzing application-layer details, such as user location or session cookies. Key benefits include:

- **High Scalability** for managing millions of requests per second, even with variable workloads.
- **Static IP Support** to maintain consistent addressing.
- **Flexible Targeting** allowing external targets (outside VPC) via IP addresses.
- **Multi-Port Routing** enabling single instances to handle multiple applications across different ports.
- **Health Monitoring** through independent checks at the target group level, providing comprehensive service metrics.

Key High-Load Areas in the Hospital Network

- **Main Internet Gateway at Main Site**: As all internet-bound traffic flows through this point, the site' gateway is a critical congestion zone for the entire hospital network. Placing a load balancer inside the main internet gateway will help distribute traffic effectively across servers at both the main and branch locations.
- **Main Site Subnet Router**: Since this router manages the bidirectional traffic between the main and auxiliary sites, it is another potential bottleneck. Installing a load balancer here will aid in distributing internal traffic loads, enhancing connectivity across all branches and headquarters.

This configuration will improve overall performance and reliability, keeping critical data and applications accessible across the hospital system.

D. Choose a network structure that matches the building's architecture with convenience and aesthetics

Since the installation locations are buildings with many vertical floors, for the auxiliary sites it is better to put a single “brain” in the ground floor (IT Room and Cabling Central Local) for ease of management aesthetics of other floors. For the main site, we already have a separate room 50 meters away from the two building. This design helps in disaster-recovery, since the ground floor is easier to access for humans. Also loss could be mitigated in case of fire, which happens frequently in big cities like HCM city because fire always goes upward.

Main Site:

Site has two buildings A and B, therefore we decided to build networks for the two buildings similarly. In particular, each floor will have 10 rooms, each rooms will have the average of 5 devices, including PCs and a surveillance camera.

For the auxiliary sites:

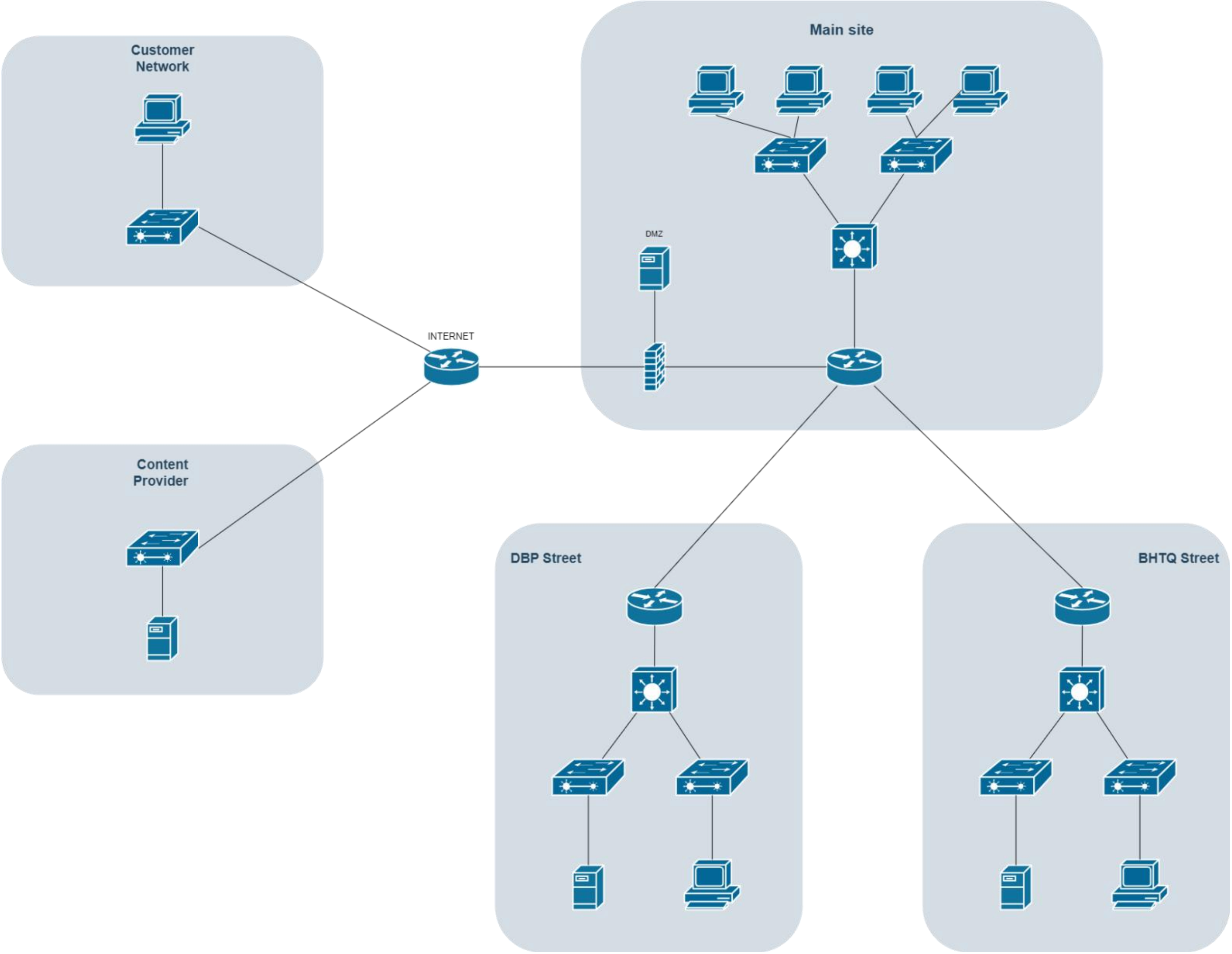
1st floor: Server room and IT department

- 3 public servers for load balancing with the Main Sites’s public servers, 1 private server for internal uses.
- 05 PCs for IT personnel.
- 02 switches for cabling between the floors.
- 01 routers with the leased DSL line.

2nd floor: Patient services department

- 40 PCs for nurses and doctors, 20 PCs for patients who do not have WiFi access.
- 01 switch to connect the PCs.
- 01 camera surveillance system.

E. Design the network usage in a wireless environment, applying network security standards and setting up partitions for network servers and devices (e.g., Server farm, DMZ, Firewall, ...)



The network is partitioned as demonstrated in the above figure.

- A DMZ was set up to provide public access from the internet to the service servers.
- A firewall was set up between the Company private WAN and the external public network.
- Only permitted traffic (trusted server on the internet) from outside is able to go into the private network.

2. Step 2 (1 point): List of minimum equipment, IP plan, and wiring diagram (cabling)

A. List of recommended equipment and typical specifications & IP plan

Here we present the device stack needed for the network setup. For core devices such as routers and firewalls, we proposed Cisco devices for reliability. For minor devices like access points, we preferred using less expensive options like the one from Linksys. Edge devices like servers and workstations can be chosen by the hospital themselves to suit their particular needs.

Device name	Technical specifications	Amount	Cost (Dec 2024)
Cisco 1941 Router	Product Code: CISCO1941/K9 Rack Units: 2RU Interfaces: 2 integrated 10/100/1000 Ethernet ports: GE0/0 & GE0/1 Expansion Slot(s): 2 enhanced High-Speed WAN Interface Card slots 1 Internal Service Module slot RAM: 512 MB (installed) / 2GB (max) Flash Memory: 256MB (installed) / 8GB (max) Dimensions: 34.3 cm x 29.2 cm x 8.9 cm Package Weight: 10.48 Kg	07	$3,482
Cisco WS-C2960-24TT-L Switch	Product Code: Cisco WS-C2960-24TT-L Ports 24 Ethernet 10/100 ports Uplinks 2 Ethernet 10/100/1000 ports VLAN IDs 4000 Dimensions (H x W x D) 4.4 x 44.5 x 23.6 cm Weight 3.6 kg Rack Height 1 RU	15	$2,869
Cisco ASA5505-BUN-k9 Firewall	Firewall Users 10 Maximum firewall throughput (Mbps) 150 Maximum connections 10,000 Maximum connections/second 3,000 Packets per second (64 byte) 85,000 Integrated ports 8 port 10/100 switch with 2 Power over Ethernet ports Maximum virtual interfaces (VLANs) 3 (trunking disabled)	01	$595
Linksys Cloud Managed AX3600 WiFi 6 Indoor Wireless Access Point	Dual-Band 802.11AX (2.4GHz + 5GHz) 4x4:4 Internal Antennas for AX3600 Speeds (1200Mbps + 2400Mbps) UL/DL OFDMA, 1024-QAM, Target Wake Time BSS Coloring, Tx Beamforming 802.3at PoE+ Support Limited Lifetime Cloud Management TAA Compliant	04	$399.99
Optical fiber cable & Copper			

cable supporting GigabitEthernet			
Optical fiber cable & Copper cable supporting FastEthernet			
Servers & Workstations	Selected by the hospital.		

IP addresing plan:

The connection between the IT cable room of the the Main Site and the firewall is 10.0.10.0/24.

For private network, all hosts have IP address format as:

$$192.168.[\mathrm{VLAN}].[\mathrm{host}]$$

where,

[VLAN] ranges from **2 .. 254**

[host] ranges from 1 .. 254

Additional rule:

- **Networking devices:** first available addresses within the range
- **Hosts:** last available addresses within the range
- All hosts in the Company private network are **assigned with a static IP address.**

There are special IP addresses and VLANs used for routing and network management:

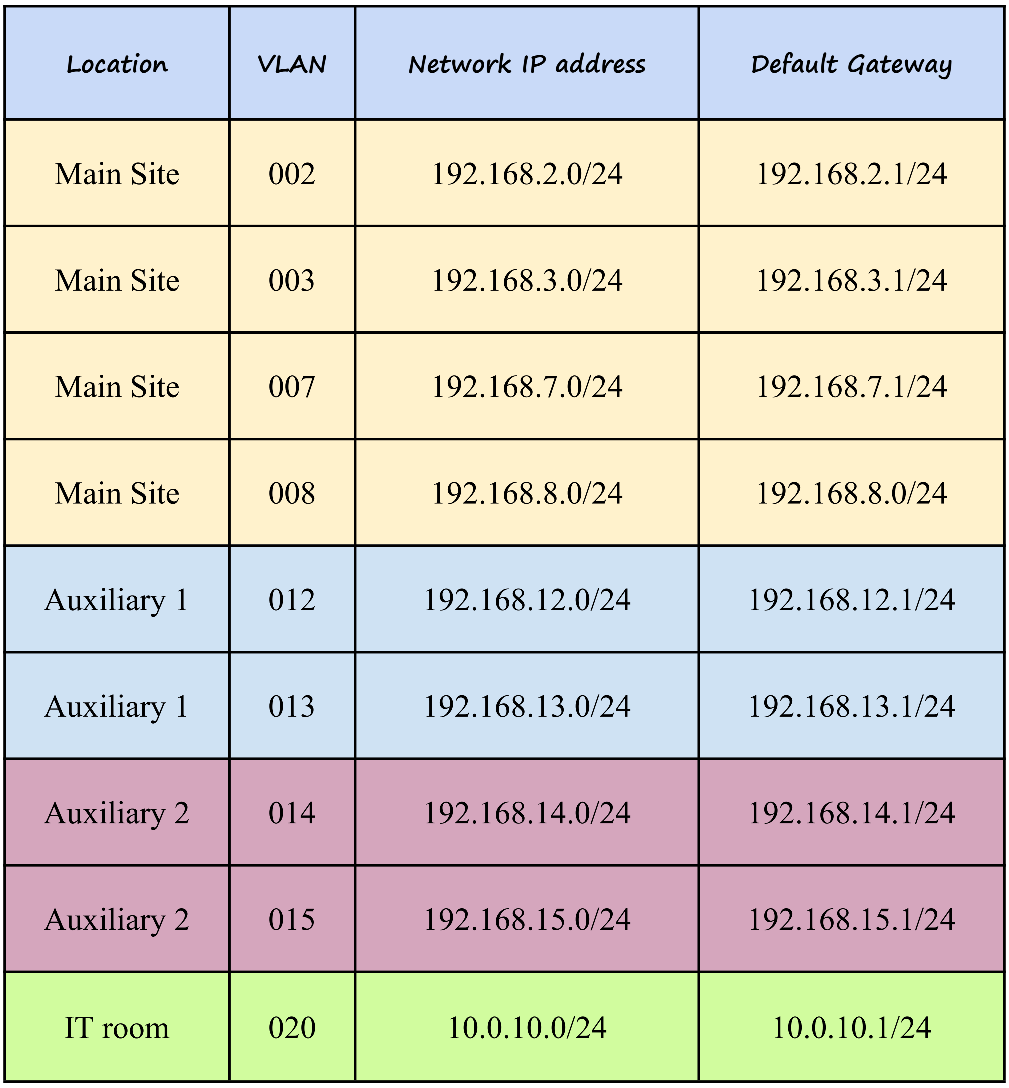
1. Network **10.0.1.0/24** is for WAN communication on leased DSL between Main Site and the Auxiliary Site 1.

2. Network **10.0.2.0/24** is for WAN communication on leased DSL between Main Site and the Auxiliary Site 2.

3. Network **10.0.3.0/24** is for communication between the hospital and the firewall.

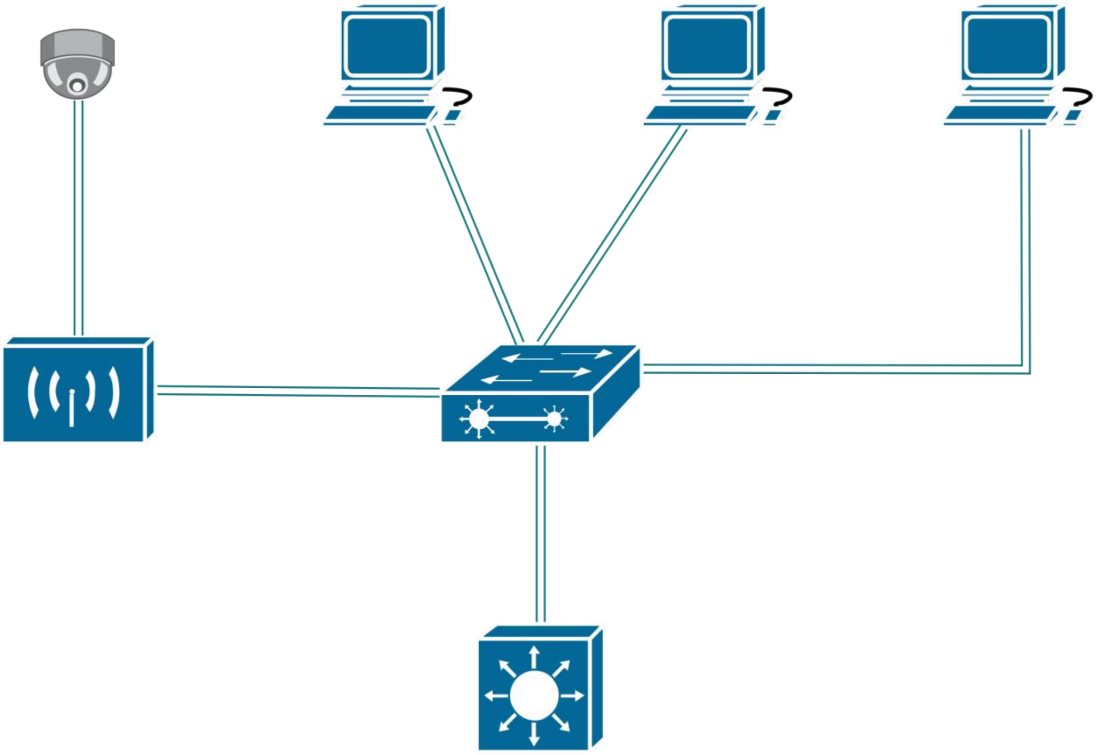
4. Network **8.8.8.0/24** is for communication between the firewall and Internet Gateway.

The summary of IP addresses is as follows:

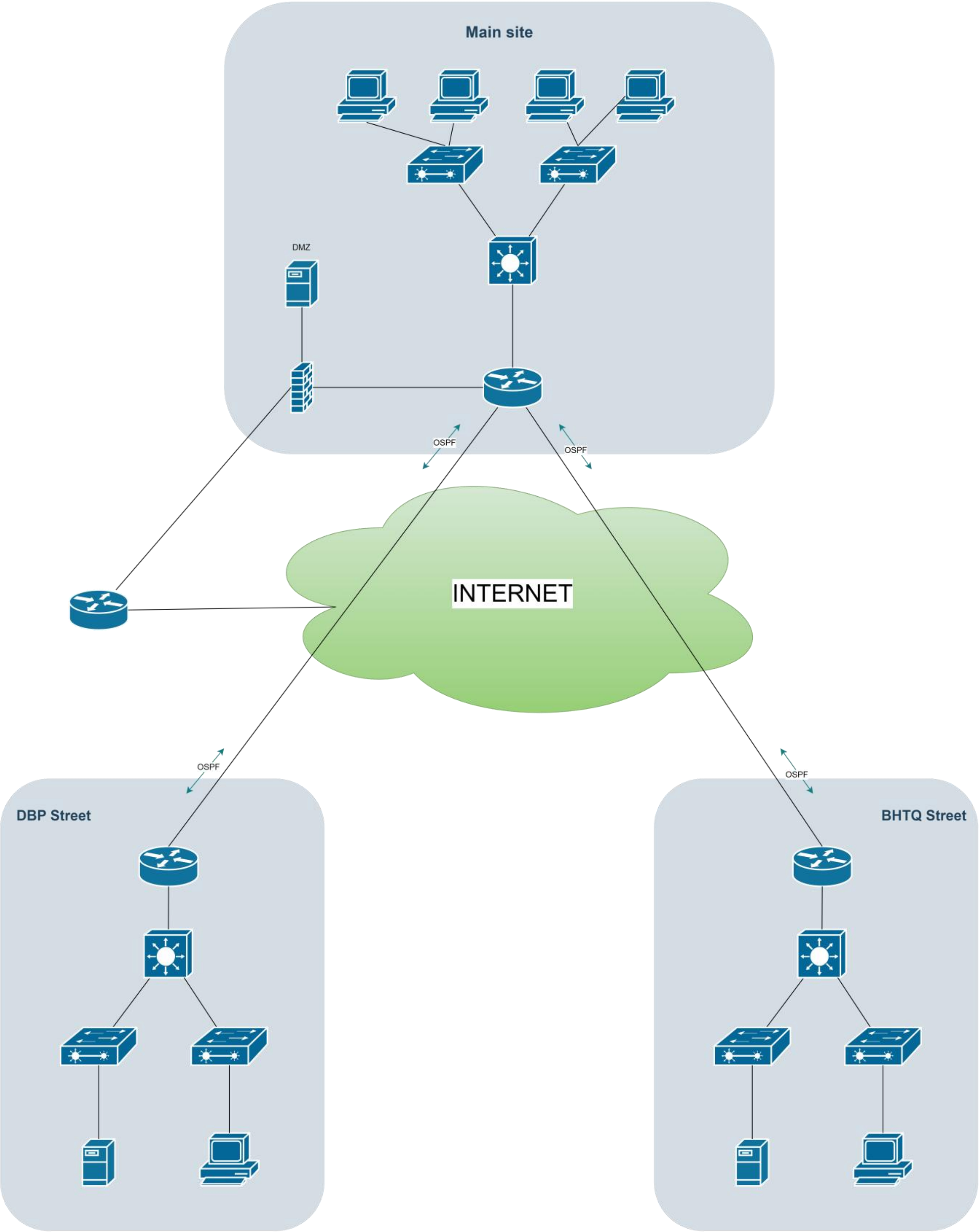


Location	VLAN	Network IP address	Default Gateway
Main Site	002	192.168.2.0/24	192.168.2.1/24
Main Site	003	192.168.3.0/24	192.168.3.1/24
Main Site	007	192.168.7.0/24	192.168.7.1/24
Main Site	008	192.168.8.0/24	192.168.8.0/24
Auxiliary 1	012	192.168.12.0/24	192.168.12.1/24
Auxiliary 1	013	192.168.13.0/24	192.168.13.1/24
Auxiliary 2	014	192.168.14.0/24	192.168.14.1/24
Auxiliary 2	015	192.168.15.0/24	192.168.15.1/24
IT room	020	10.0.10.0/24	10.0.10.1/24

B. Schematic physical setup of the network



C. WAN connection diagram between the main Site and the two Auxiliary Sites (using new WAN technology such as SD-WAN, MPLS, and OSPF routing protocol)



3. Step 3 (1 point): Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the company network

- **Summarize the estimated dataflows and workload of the system:**

  - Each server total download: $D_s = 1000MB/day$
  - Each server total upload: $U_s = 2000MB/day$
  - Each workstation total download: $D_w = 500MB/day$
  - Each workstation total upload: $U_w = 100MB/day$
  - Total WiFi-connected devices download: $Data_{wifi} = 500MB/day$
  - Peak hours : 3 hours
  - Network peak rate is 80% at peak hours
  - Hospital's growth rate of 20% in 5 years

- **The formula of network:**

  - 1 MBps = $\frac{8 * 2^{20}}{10^6}$ Mbps

  - The total data transfer :

$$Data = Number * (Upload + Download)$$

  - Peak Hour Throughput (PHT):

$$Throughput = Data * \frac{PeakRate}{PeakTime} = Data * \frac{0.8}{3 * 60 * 60} = \frac{Data}{13500}$$

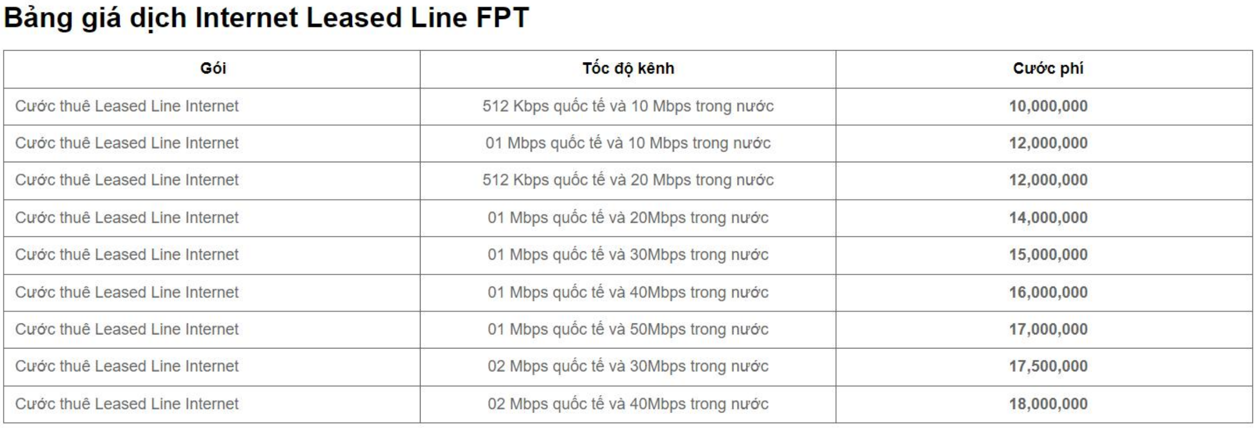
  - The minimum bandwidth for the next 5 years:

$$Bandwidth = Throughput * GrowthRate = Throughput * 1.2$$

- **Main Site**
  - **In wired Internet, there are:**
    - Number of server : $N_s = 10$
    - Number of workstation : $N_w = 600$
  - **The total data transfer by server:**
    - $\sum Data_{server} = N_s(D_s + U_s) = 10 * (1000 + 2000) = 30000(MB/day)$
  - **The total data transfer by workstation:**
    - $\sum Data_{workstation} = N_w(D_w + U_w) = 600 * (500 + 100) = 360000(MB/day)$
  - **The total data transfer in Main Site:**
    - $\sum Data_{Main\_Site} = \sum Data_{server} + \sum Data_{workstation} + \sum Data_{wifi}$
      $= 30000 + 360000 + 500 = 390500(MB/day)$
  - **The peak hour throughput in Main Site:**
    - $Throughput_{Main\_site} = \sum \frac{Data_{Main\_site}}{13500} = 28.9259(MBps)$
  - **The minimum bandwidth of Main Site:**
    - $Bandwidth_{Main\_site} = Throughput_{Main\_site} * 1.2 = 34.7111(MBps)$
- **Auxiliary Sites**
  - **In wired Internet, there are:**
    - Number of server : $N_s = 2$
    - Number of workstation : $N_w = 60$
  - **The total data transfer by server:**
    - $\sum Data_{server} = N_s(D_s + U_s) = 2 * (1000 + 2000) = 6000(MB/day)$
  - **The total data transfer by workstation:**
    - $\sum Data_{workstation} = N_w(D_w + U_w) = 60 * (500 + 100) = 36000(MB/day)$
  - **The total data transfer in an Auxiliary Site:**
    - $\sum Data_{Auxiliary\_Site} = \sum Data_{server} + \sum Data_{workstation} + \sum Data_{wifi}$
      $= 6000 + 36000 + 500 = 42500(MB/day)$
  - **The peak hour throughput in Auxiliary Site:**
    - $Throughput_{Auxiliary\_Site} = \sum \frac{Data_{Auxiliary\_Site}}{13500} = 3.1481(MBps)$

- **The minimum bandwidth of Auxiliary Site:**
  - $$Bandwidth_{Auxiliary\_Site} = Throughput_{Auxiliary\_Site} * 1.2 = 3.7777(MBps) = 30.2218(Mbps)$$

- **Suggest configuration for the hospital network**
  - From the expected bandwidth, the ISP lease line from each branch should be 40 Mbps, which scales well for the company for the next ten years.
  - From the FPT internet leased line, we could rent the 16 millions VNĐ/month package



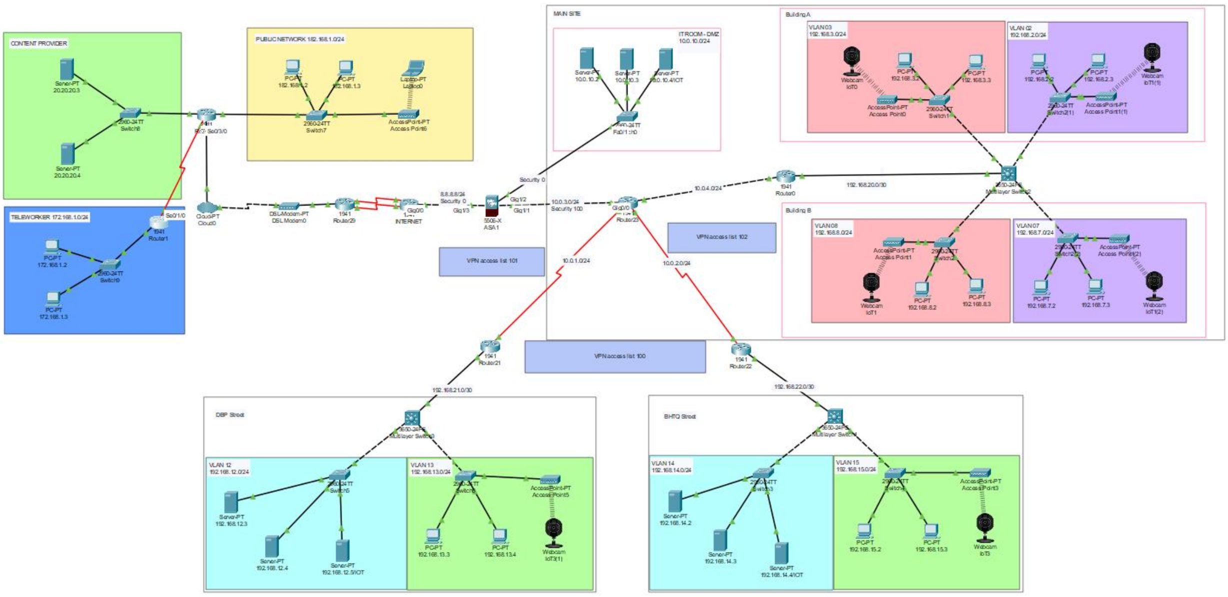
Bảng giá dịch Internet Leased Line FPT

Gói	Tốc độ kênh	Cước phí
Cước thuê Leased Line Internet	512 Kbps quốc tế và 10 Mbps trong nước	10,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 10 Mbps trong nước	12,000,000
Cước thuê Leased Line Internet	512 Kbps quốc tế và 20 Mbps trong nước	12,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 20Mbps trong nước	14,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 30Mbps trong nước	15,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 40Mbps trong nước	16,000,000
Cước thuê Leased Line Internet	01 Mbps quốc tế và 50Mbps trong nước	17,000,000
Cước thuê Leased Line Internet	02 Mbps quốc tế và 30Mbps trong nước	17,500,000
Cước thuê Leased Line Internet	02 Mbps quốc tế và 40Mbps trong nước	18,000,000

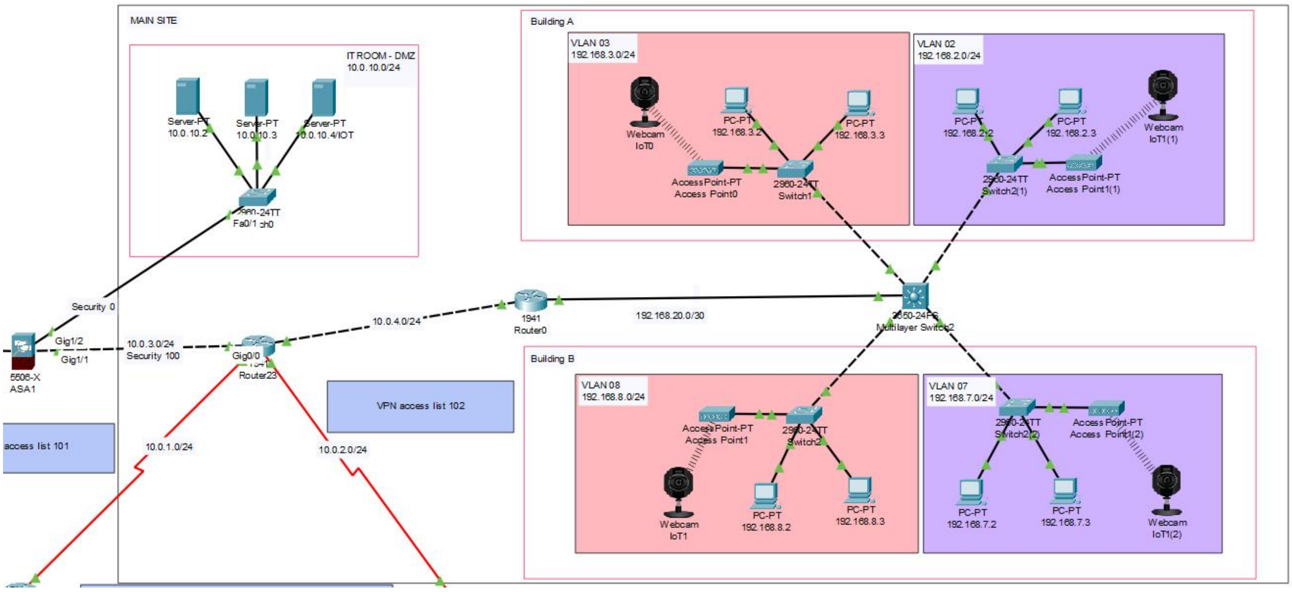
4. Step 4 (2 points): Design the network map using Packet Tracer or GNS3 simulation software

Due to limited space on Cisco Packet Tracer, the simulation network does not contain all floors, all workstations and servers. Instead, the design was simplified only for demonstration purposes. However, this network contains enough characteristics to simulate the actual network, supporting sufficient networking features.

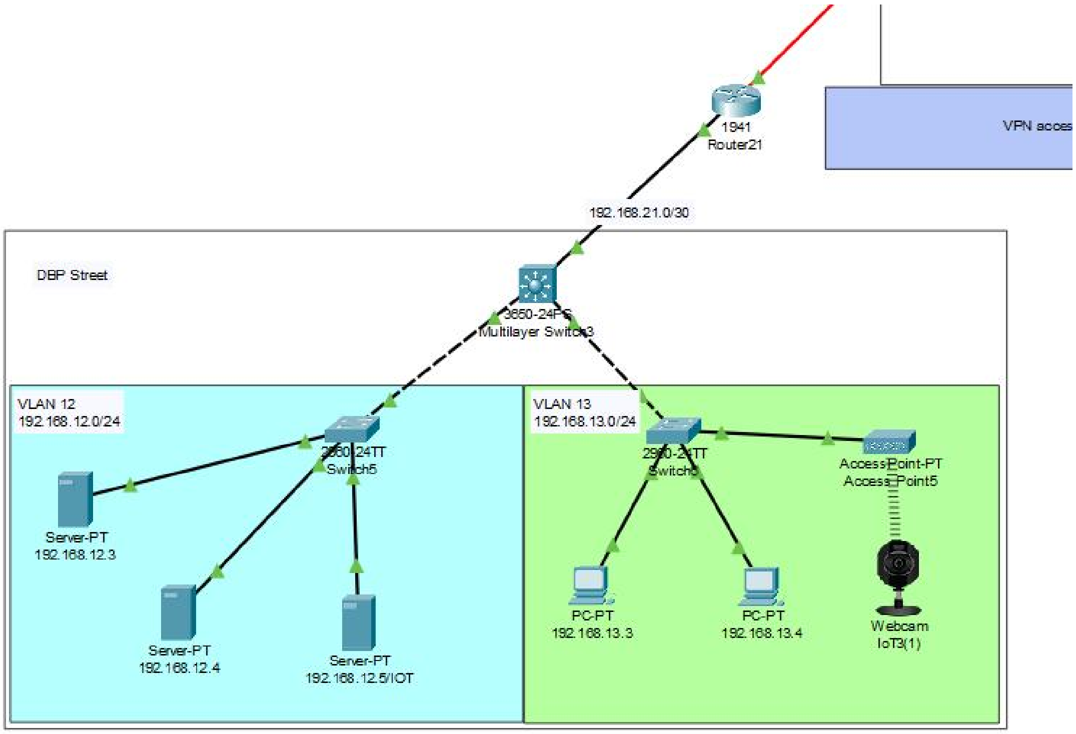
A. Overall structure of the network



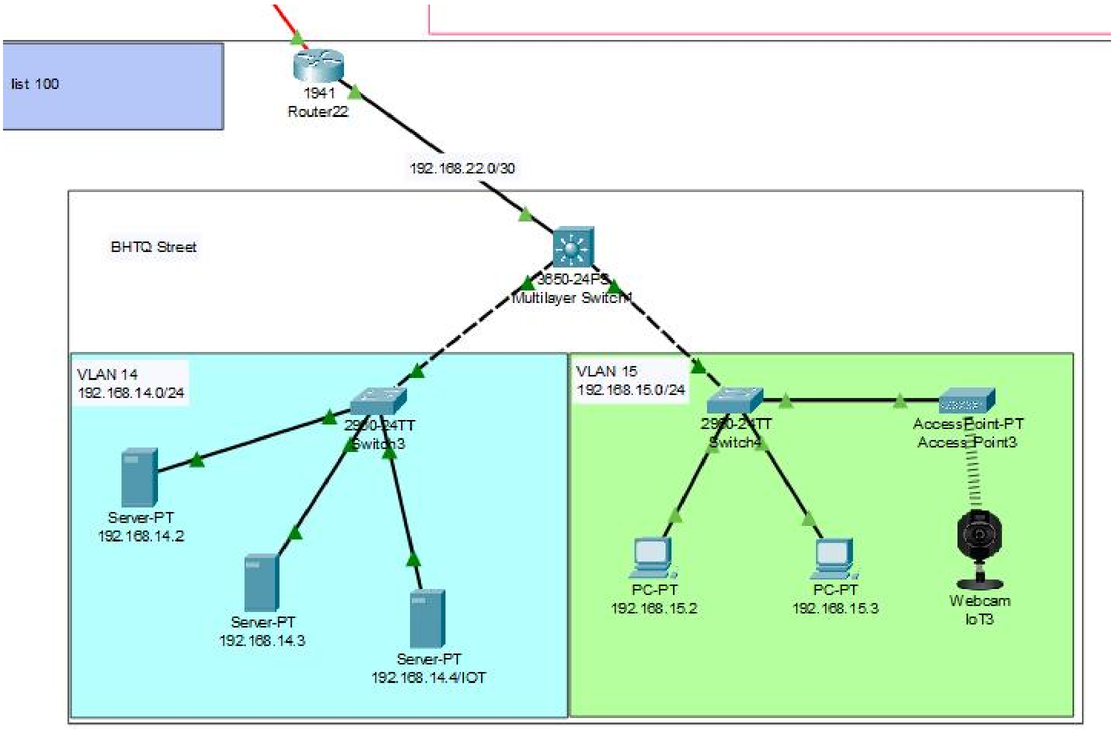
B. Main Site



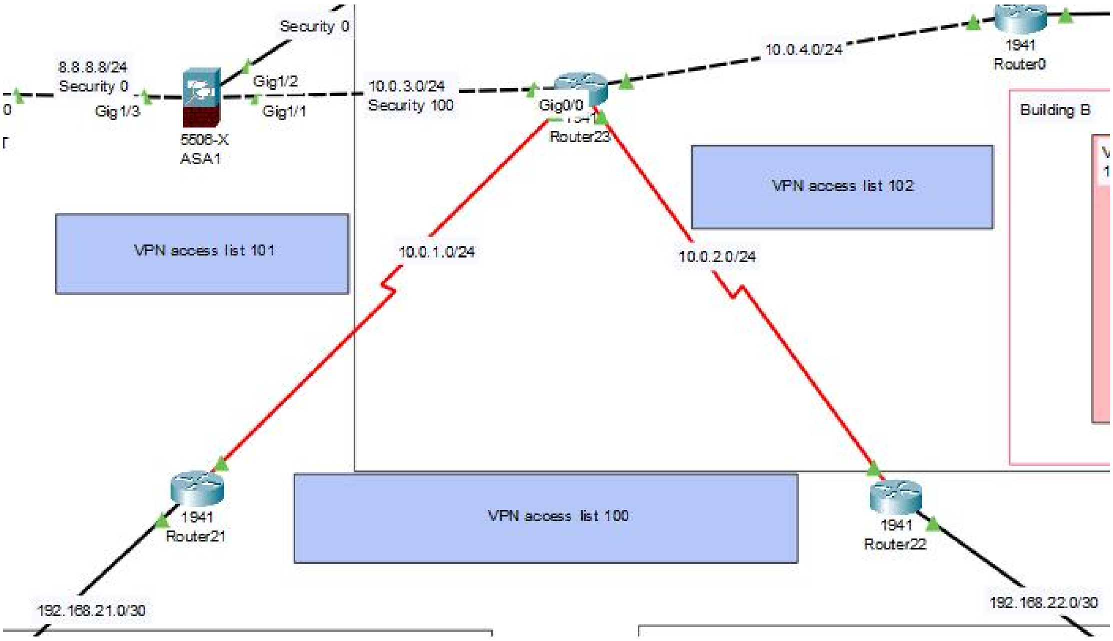
C. Auxiliary 1



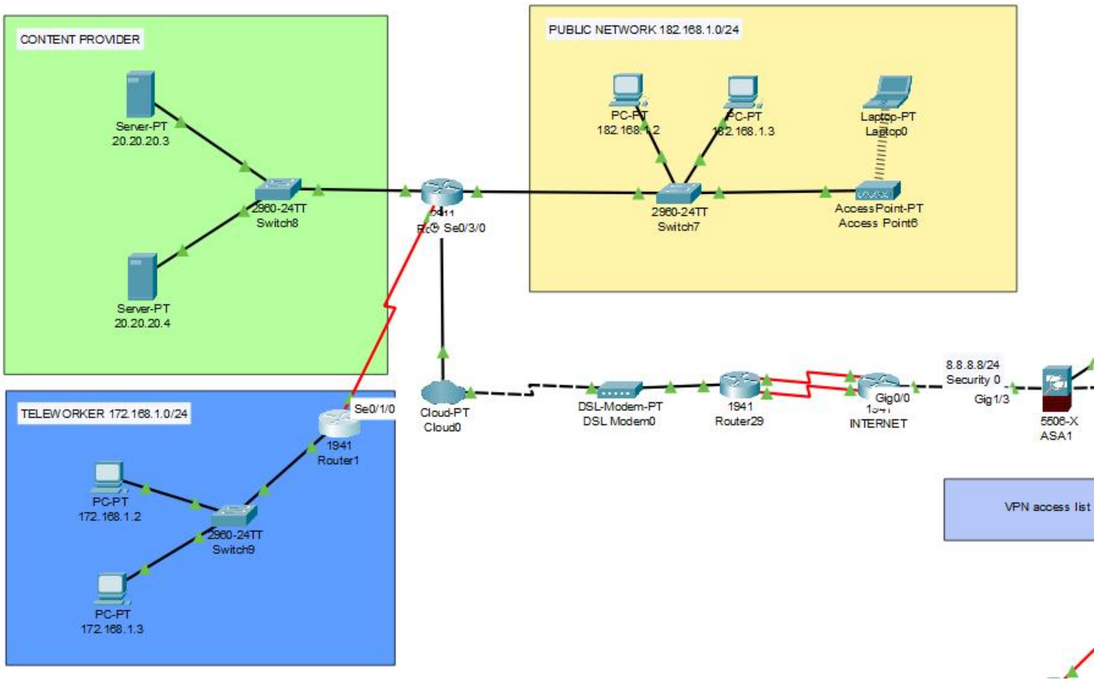
D. Auxiliary 2



E. Connection between Sites

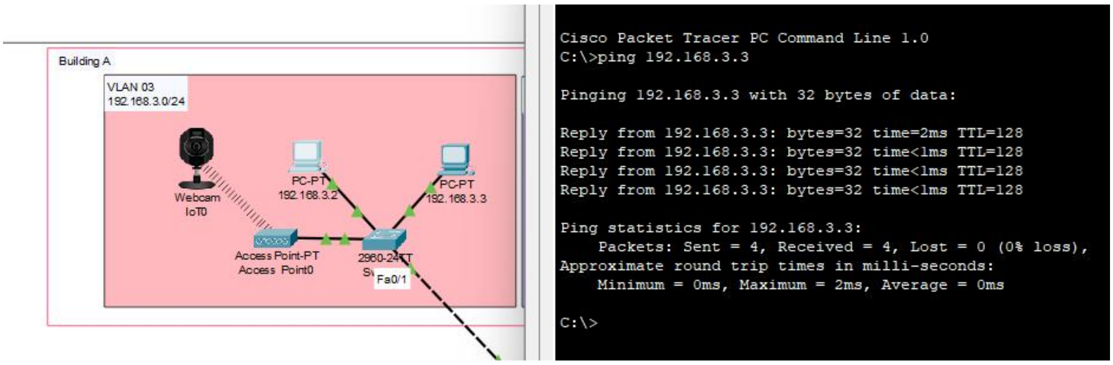


F. Internet



5. Step 5 (2 points): Test the system with popular tools such as ping, traceroute, etc. on the simulated system

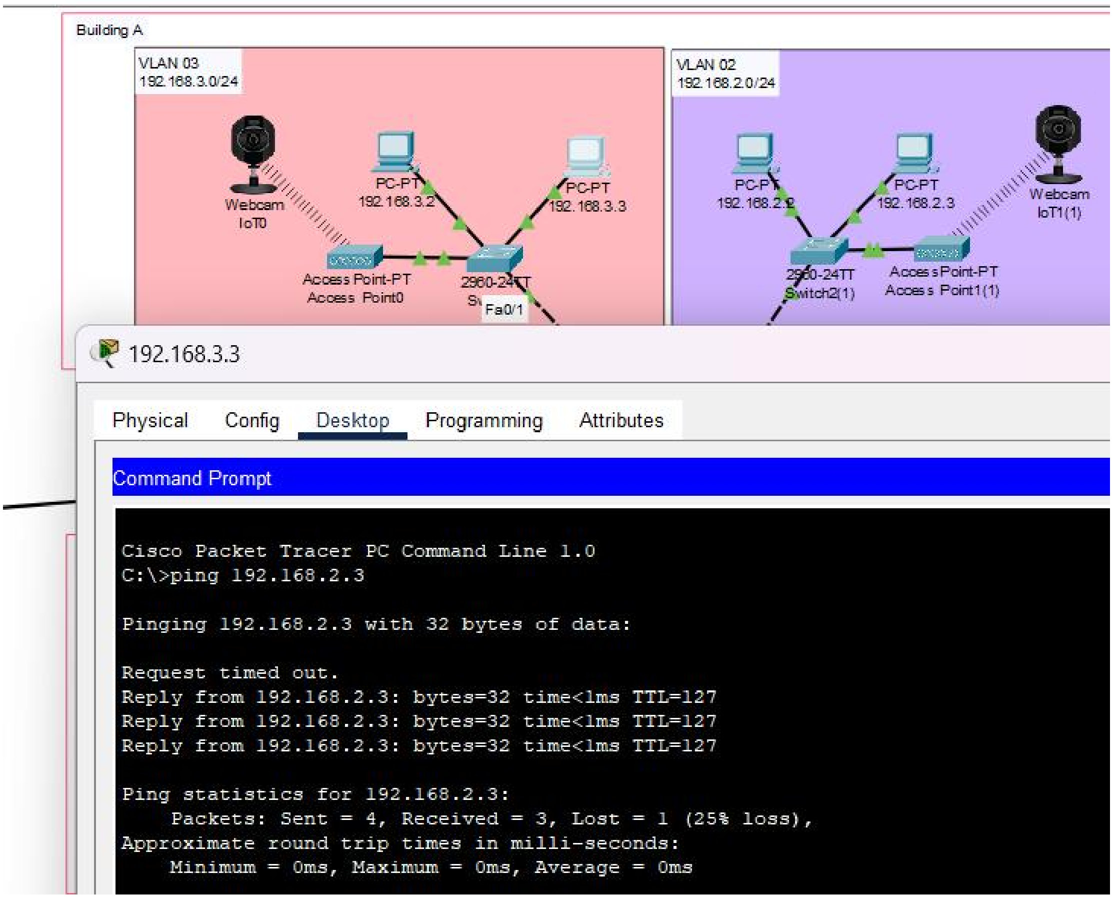
A. Connect between PCs in the same VLAN



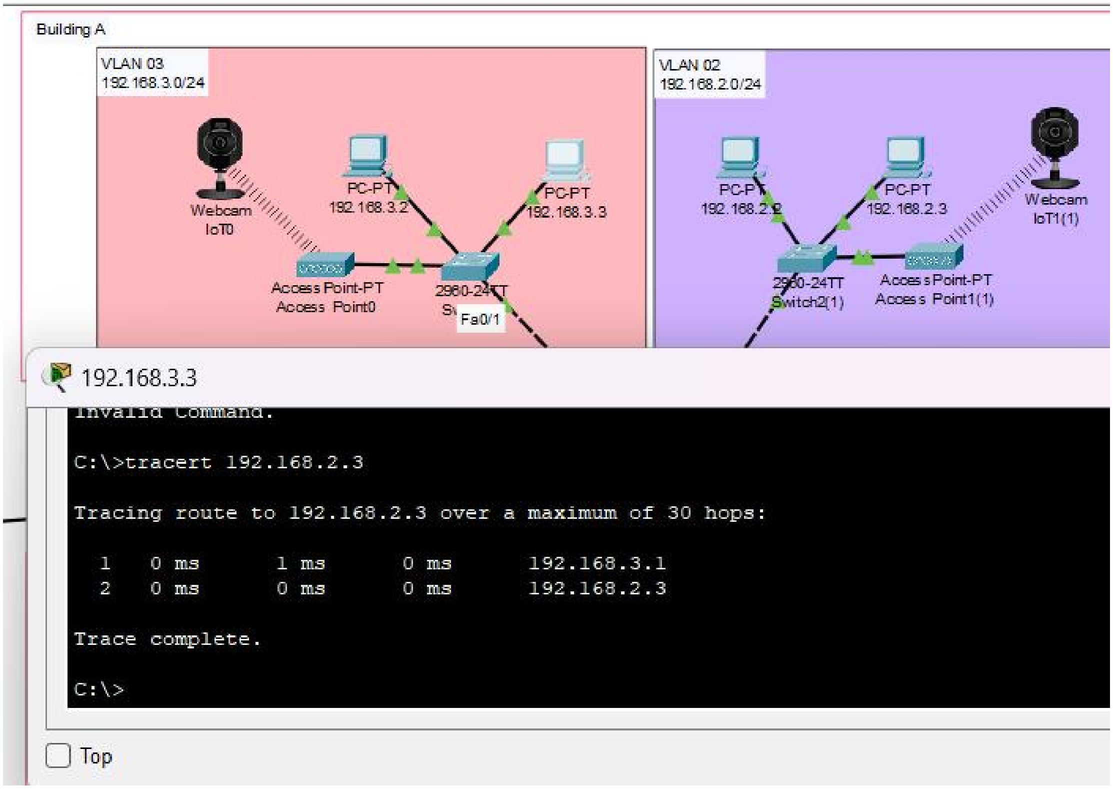
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

The experiment was carried out within VLAN 3 (192.168.3.0/24) computers.

B. Connect PCs between VLANs



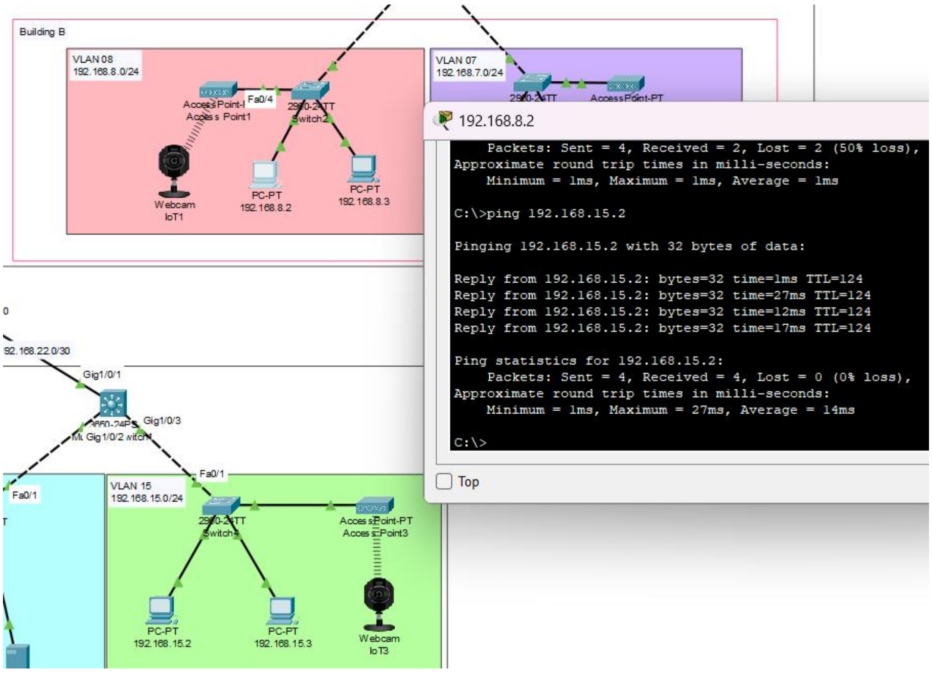
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



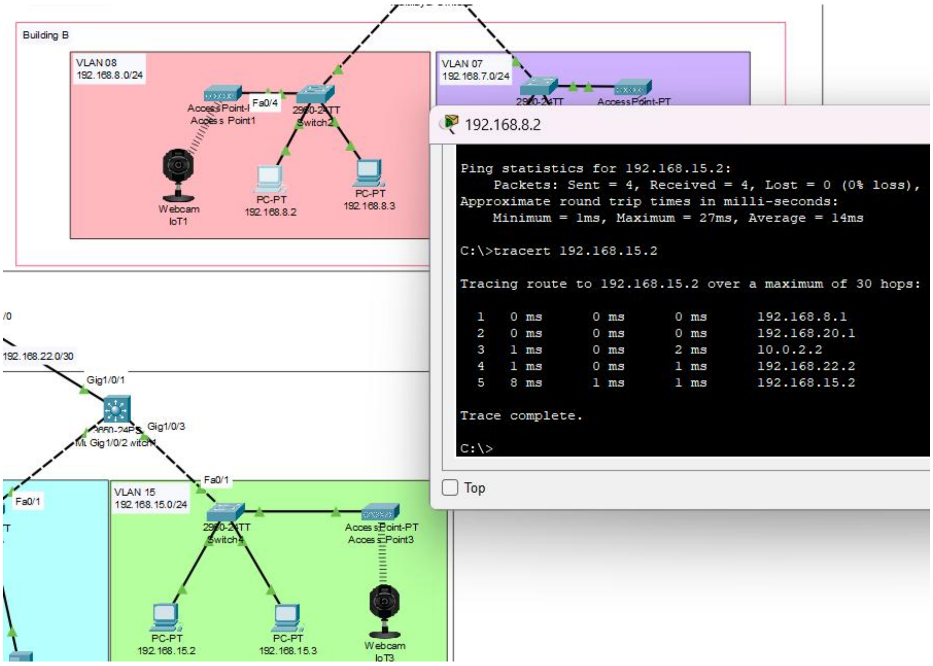
```
Invalid Command.

C:\>tracert 192.168.2.3

Tracing route to 192.168.2.3 over a maximum of 30 hops:

  1   0 ms      1 ms      0 ms      192.168.3.1
  2   0 ms      0 ms      0 ms      192.168.2.3

Trace complete.

C:\>
```

The experiment was carried out between VLAN 3 (192.168.3.0/24) and VLAN 2 (192.168.2.0/24) in the Main Site using ping and traceroute.

C. Connect PCs between the Main Site and the two Auxiliary Sites



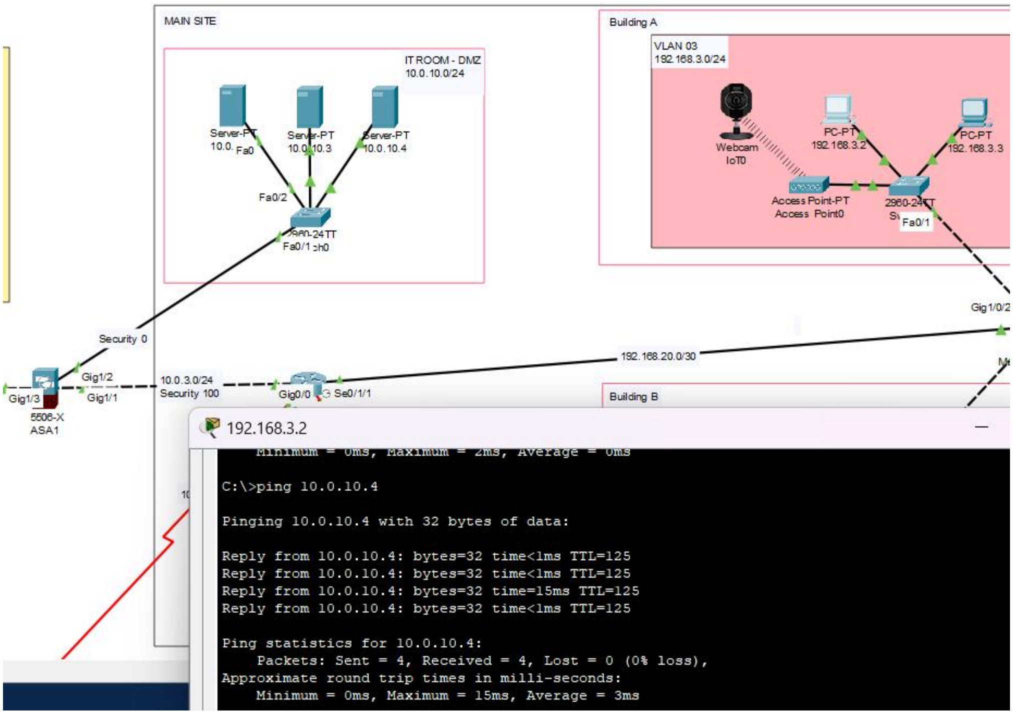
```
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.15.2

Pinging 192.168.15.2 with 32 bytes of data:

Reply from 192.168.15.2: bytes=32 time=1ms TTL=124
Reply from 192.168.15.2: bytes=32 time=27ms TTL=124
Reply from 192.168.15.2: bytes=32 time=12ms TTL=124
Reply from 192.168.15.2: bytes=32 time=17ms TTL=124

Ping statistics for 192.168.15.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 27ms, Average = 14ms

C:\>
```



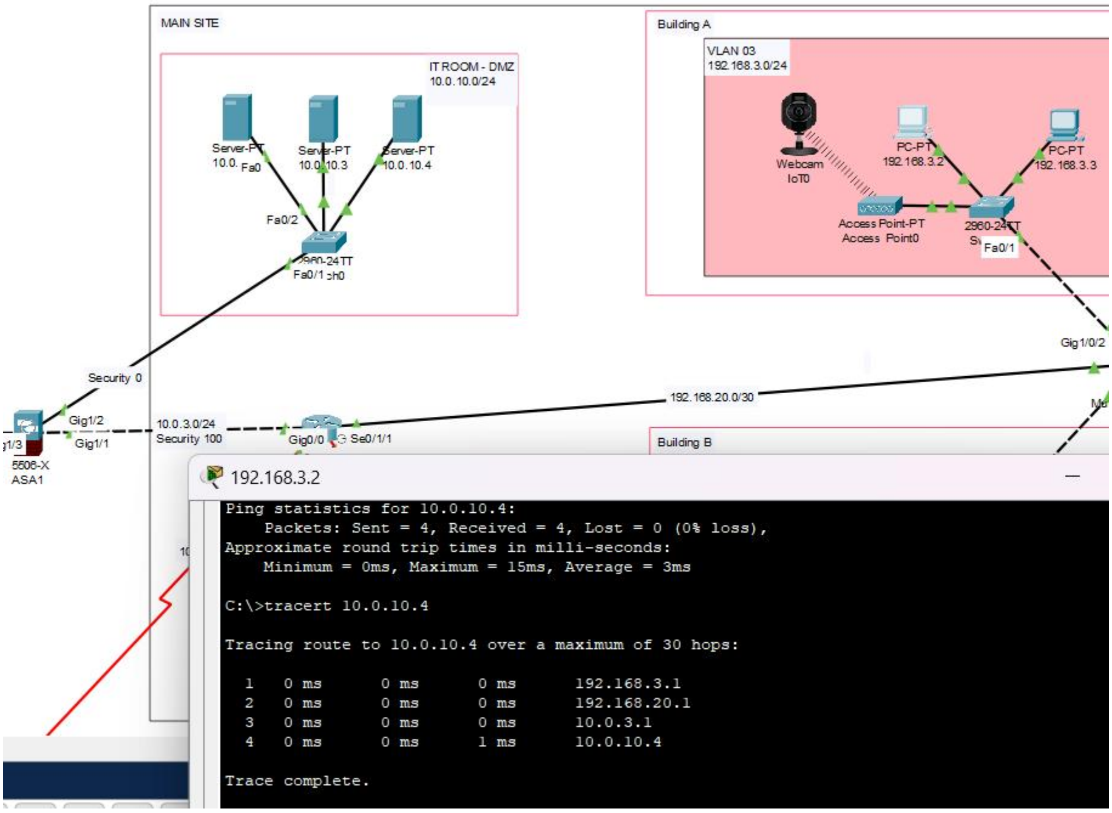
```
Ping statistics for 192.168.15.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 27ms, Average = 14ms

C:\>tracert 192.168.15.2

Tracing route to 192.168.15.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.8.1
  2   0 ms      0 ms      0 ms      192.168.20.1
  3   1 ms      0 ms      2 ms      10.0.2.2
  4   1 ms      0 ms      1 ms      192.168.22.2
  5   8 ms      1 ms      1 ms      192.168.15.2

Trace complete.

C:\>
```

The experiment was carried out between VLAN 8 (192.168.8.0/24) of the Main Site and VLAN 15 (192.168.15.0/24) of Auxiliary 2 (BHTQ Street) using both ping and traceroute.

D. Connect to servers in the DMZ



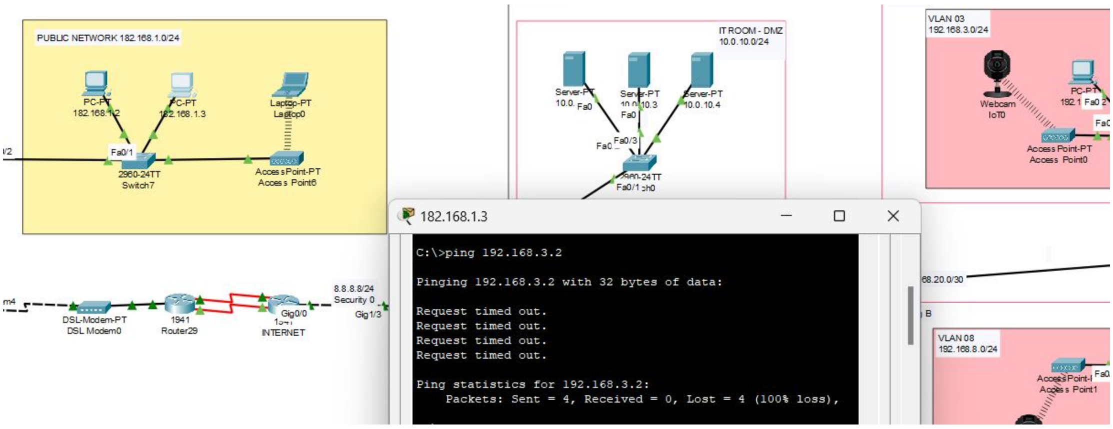
```
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 10.0.10.4

Pinging 10.0.10.4 with 32 bytes of data:

Reply from 10.0.10.4: bytes=32 time<1ms TTL=125
Reply from 10.0.10.4: bytes=32 time<1ms TTL=125
Reply from 10.0.10.4: bytes=32 time=15ms TTL=125
Reply from 10.0.10.4: bytes=32 time<1ms TTL=125

Ping statistics for 10.0.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms
```



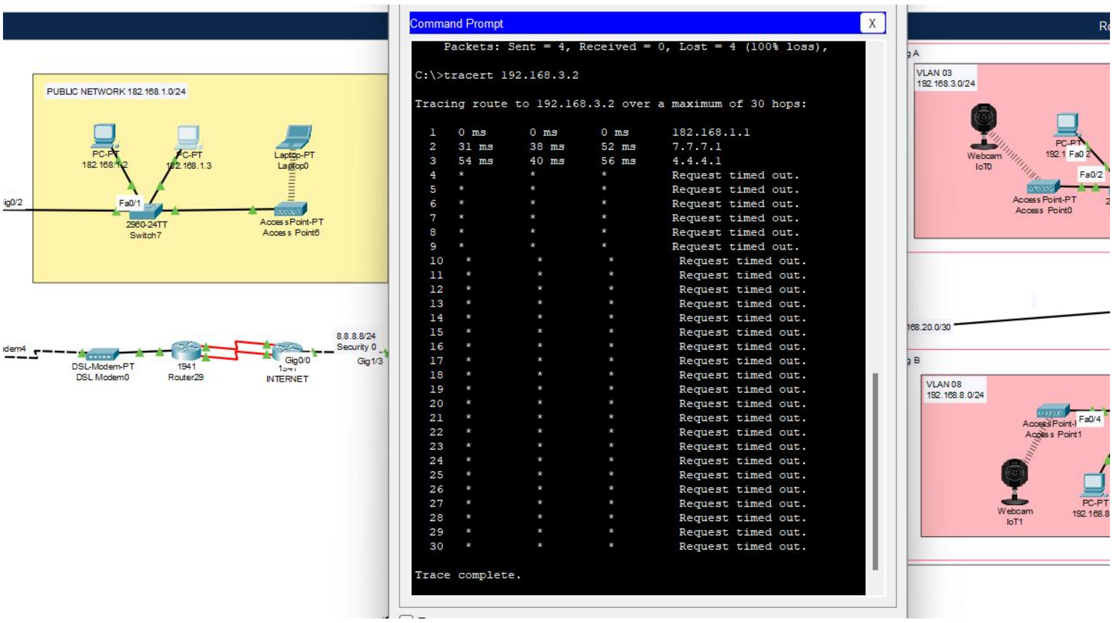
```
Ping statistics for 10.0.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\>tracert 10.0.10.4

Tracing route to 10.0.10.4 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.3.1
  2   0 ms      0 ms      0 ms      192.168.20.1
  3   0 ms      0 ms      0 ms      10.0.3.1
  4   0 ms      0 ms      1 ms      10.0.10.4

Trace complete.
```

The experiment was carried out between VLAN 3 (192.168.3.0/24) of the Main Site and the DMZ (10.0.10.0/24) using both ping and traceroute.

E. No connections from Customers' devices to PCs on the LAN



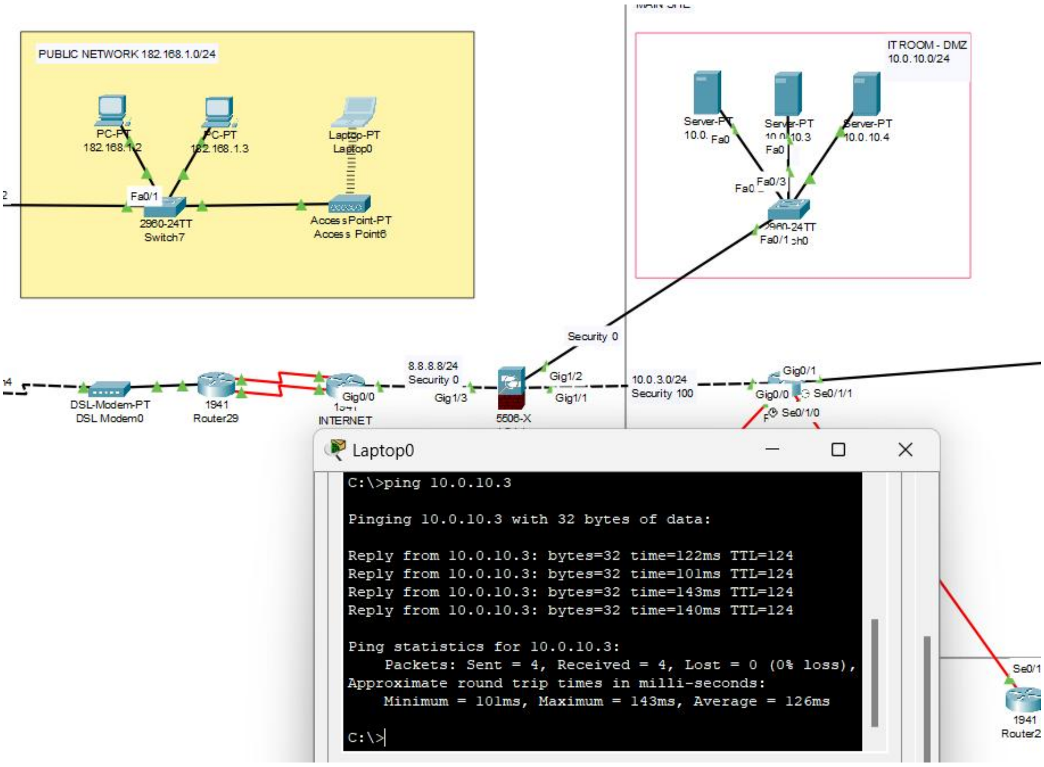
```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      182.168.1.1
  2   31 ms     38 ms     52 ms     7.7.7.1
  3   54 ms     40 ms     56 ms     4.4.4.1
  4   *         *         *         Request timed out.
  5   *         *         *         Request timed out.
  6   *         *         *         Request timed out.
  7   *         *         *         Request timed out.
  8   *         *         *         Request timed out.
  9   *         *         *         Request timed out.
  10   *         *         *         Request timed out.
  11   *         *         *         Request timed out.
  12   *         *         *         Request timed out.
  13   *         *         *         Request timed out.
  14   *         *         *         Request timed out.
  15   *         *         *         Request timed out.
  16   *         *         *         Request timed out.
  17   *         *         *         Request timed out.
  18   *         *         *         Request timed out.
  19   *         *         *         Request timed out.
  20   *         *         *         Request timed out.
  21   *         *         *         Request timed out.
  22   *         *         *         Request timed out.
  23   *         *         *         Request timed out.
  24   *         *         *         Request timed out.
  25   *         *         *         Request timed out.
  26   *         *         *         Request timed out.
  27   *         *         *         Request timed out.
  28   *         *         *         Request timed out.
  29   *         *         *         Request timed out.
  30   *         *         *         Request timed out.

Trace complete.
```

The experiment was carried out between a PC in Customer's network (182.168.1.0/24) and VLAN 3 (192.168.3.0/24) of the Main Site using both ping and traceroute.

F. Connect the Internet to a Web server

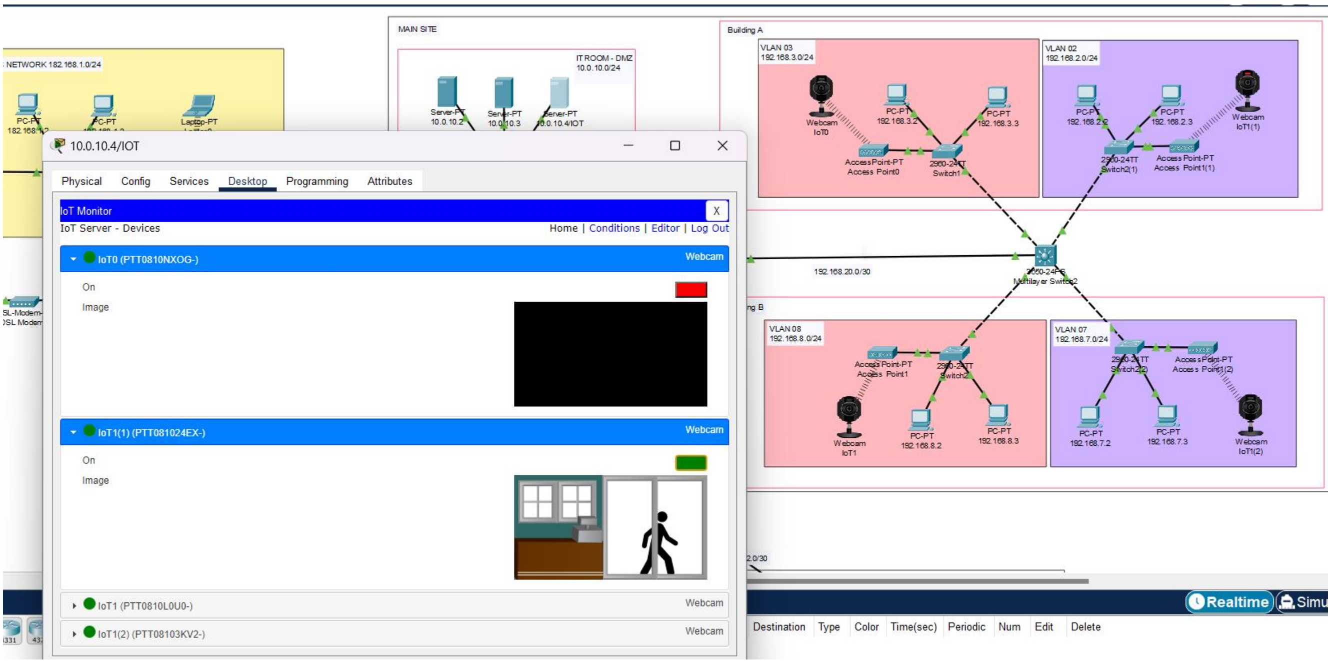


```
C:\>ping 10.0.10.3

Pinging 10.0.10.3 with 32 bytes of data:

Reply from 10.0.10.3: bytes=32 time=122ms TTL=124
Reply from 10.0.10.3: bytes=32 time=101ms TTL=124
Reply from 10.0.10.3: bytes=32 time=143ms TTL=124
Reply from 10.0.10.3: bytes=32 time=140ms TTL=124

Ping statistics for 10.0.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 101ms, Maximum = 143ms, Average = 126ms

C:\>
```

The experiment was carried out between a wireless laptop in Customer Public Network, pinging to the server in the DMZ.

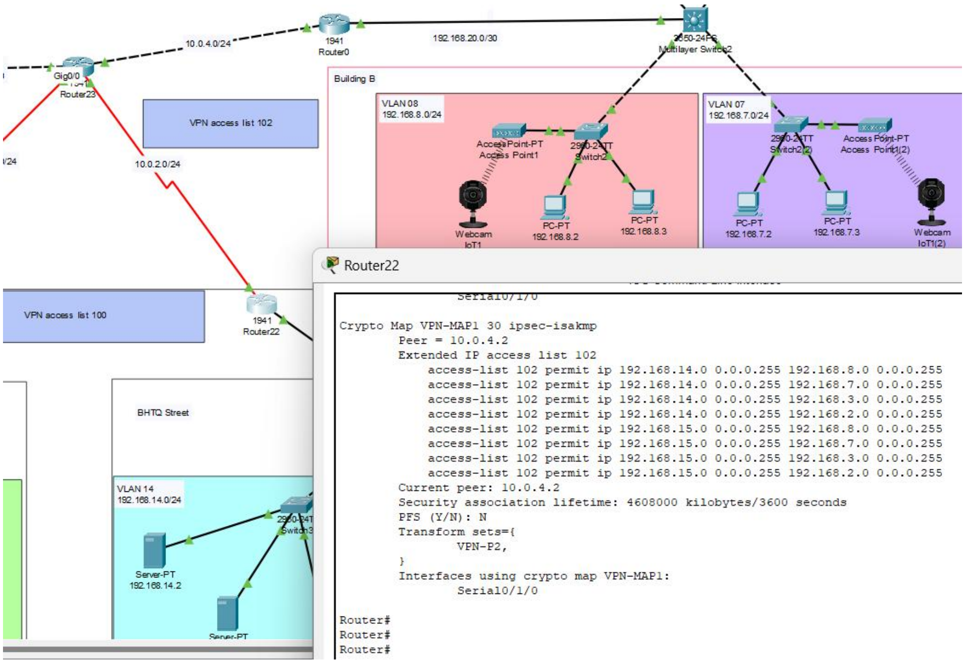
6. Extra: Camera System and VPN

A. Camera System

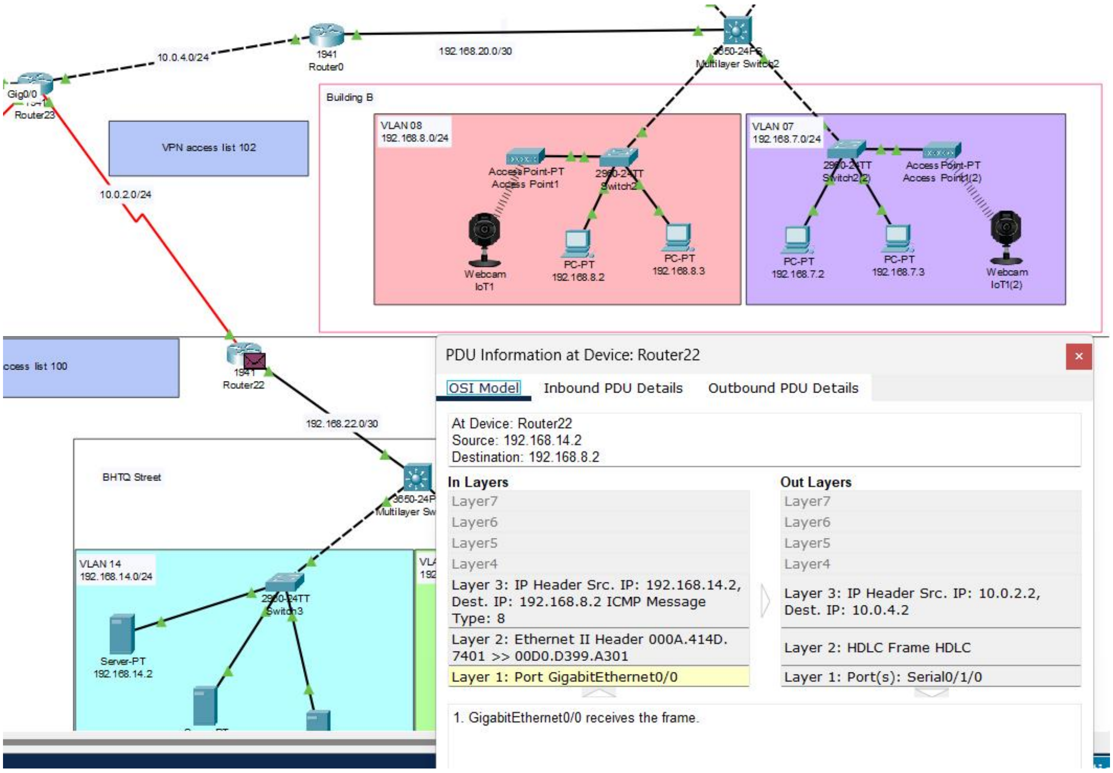


At the IT room of the main site and the the first floor of the branch system, we dedicated a server for IOT to manage all the surveillance cameras of each site. By typing the correct the username and password (admin, admin), we can access the IOT to view what each camera is recording and turning the cameras on/off.

B. VPN Site to Site



```
            Serial0/1/0

Crypto Map VPN-MAP1 30 ipsec-isakmp
        Peer = 10.0.4.2
        Extended IP access list 102
            access-list 102 permit ip 192.168.14.0 0.0.0.255 192.168.8.0 0.0.0.255
            access-list 102 permit ip 192.168.14.0 0.0.0.255 192.168.7.0 0.0.0.255
            access-list 102 permit ip 192.168.14.0 0.0.0.255 192.168.3.0 0.0.0.255
            access-list 102 permit ip 192.168.14.0 0.0.0.255 192.168.2.0 0.0.0.255
            access-list 102 permit ip 192.168.15.0 0.0.0.255 192.168.8.0 0.0.0.255
            access-list 102 permit ip 192.168.15.0 0.0.0.255 192.168.7.0 0.0.0.255
            access-list 102 permit ip 192.168.15.0 0.0.0.255 192.168.3.0 0.0.0.255
            access-list 102 permit ip 192.168.15.0 0.0.0.255 192.168.2.0 0.0.0.255
        Current peer: 10.0.4.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-P2,
        }
        Interfaces using crypto map VPN-MAP1:
                Serial0/1/0

Router#
Router#
Router#
```



PDU Information at Device: Router22

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: Router22
Source: 192.168.14.2
Destination: 192.168.8.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.14.2, Dest. IP: 192.168.8.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 10.0.2.2, Dest. IP: 10.0.4.2
Layer 2: Ethernet II Header 000A.414D.7401 >> 00D0.D399.A301	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): Serial0/1/0

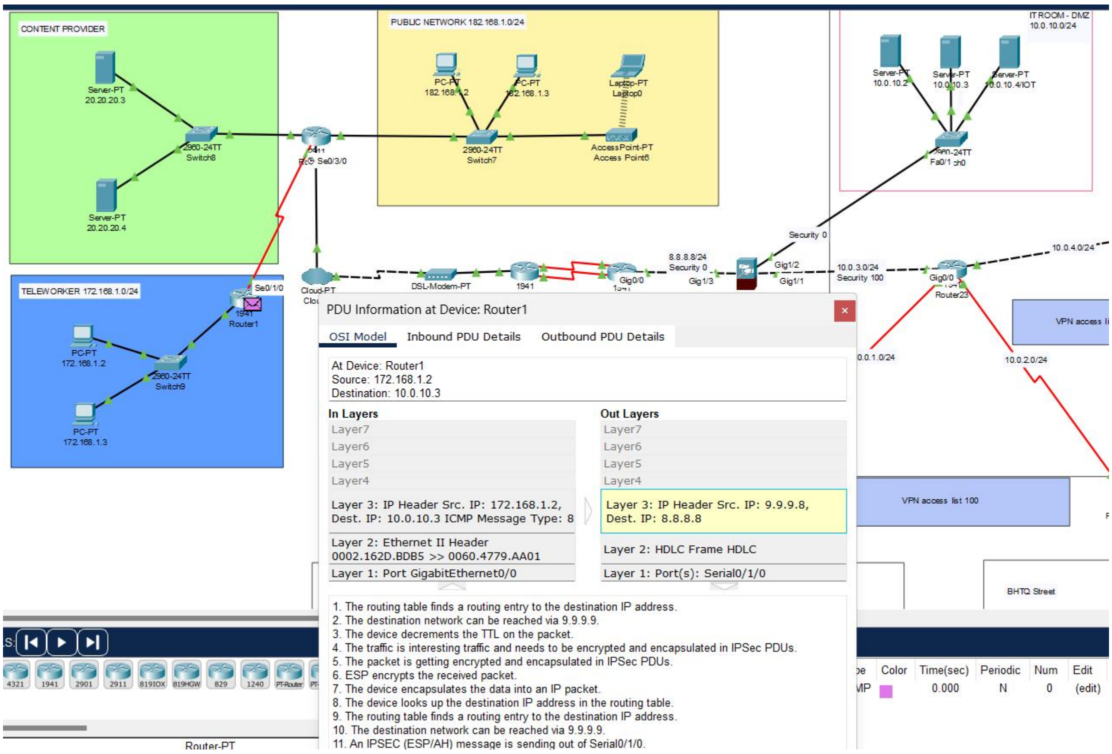
1. GigabitEthernet0/0 receives the frame.

This VPN was carried out between VLAN 14 of BHTQ Street and VLAN 8 of Main Site with the VPN setup in Router 22 and Router 0

For the VPN, we utilize IPSec (Internet Protocol Security) VPN, a robust protocol suite designed to establish encrypted tunnels between devices over untrusted networks, such as the Internet. IPSec ensures secure communication by providing confidentiality, integrity, and authentication, thereby protecting data transmission from unauthorized access or tampering.

In this configuration, the VPN is expected to encapsulate and encrypt data packets, changing the source IP address during transmission between sites. This encapsulation process ensures that sensitive information remains hidden, guaranteeing that no unauthorized party can view or intercept the transmitted data. By implementing IPSec, communication between sites is secure and safeguarded against threats like eavesdropping or data manipulation

C. VPN Teleworker



PDU Information at Device: Router1

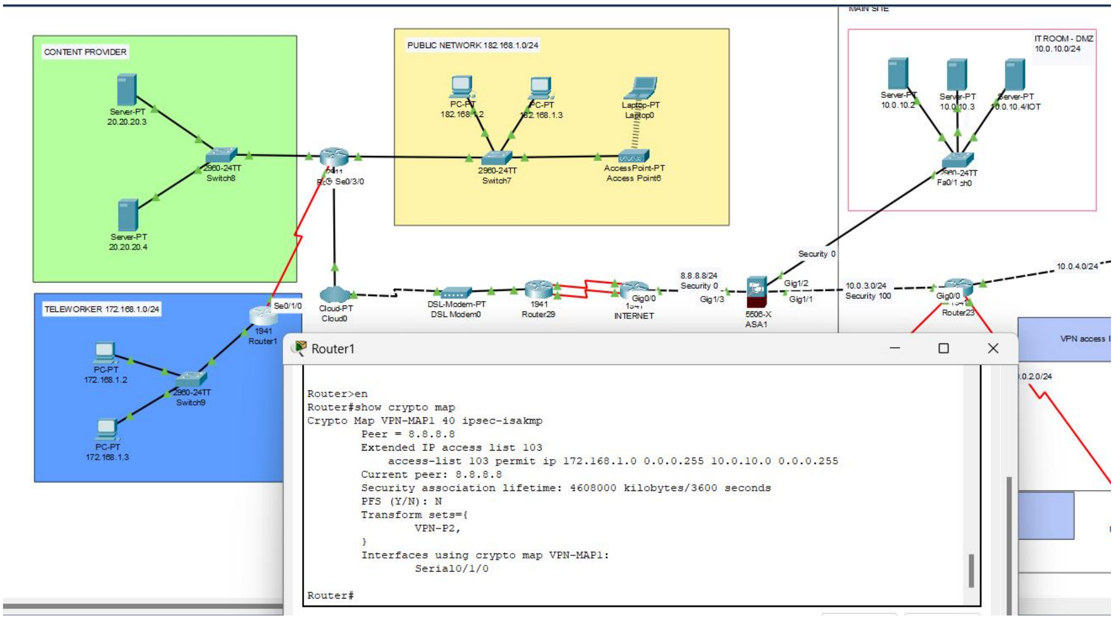
OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: Router1
Source: 172.168.1.2
Destination: 10.0.10.3

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 172.168.1.2, Dest. IP: 10.0.10.3 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 9.9.9.8, Dest. IP: 8.8.8.8
Layer 2: Ethernet II Header 0002.162D.BDB5 >> 0060.4779.AA01	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): Serial0/1/0

1. The routing table finds a routing entry to the destination IP address.
2. The destination network can be reached via 9.9.9.9.
3. The device decrements the TTL on the packet.
4. The traffic is interesting traffic and needs to be encrypted and encapsulated in IPSec PDUs.
5. The packet is getting encrypted and encapsulated in IPSec PDUs.
6. ESP encrypts the received packet.
7. The device encapsulates the data into an IP packet.
8. The device looks up the destination IP address in the routing table.
9. The routing table finds a routing entry to the destination IP address.
10. The destination network can be reached via 9.9.9.9.
11. An IPSEC (ESP/AH) message is sending out of Serial0/1/0.

pe	Color	Time(sec)	Periodic	Num	Edit
MP	🟪	0.000	N	0	(edit)



Router1

```
Router>en
Router#show crypto map
Crypto Map VPN-MAP1 40 ipsec-isakmp
        Peer = 8.8.8.8
        Extended IP access list 103
            access-list 103 permit ip 172.168.1.0 0.0.0.255 10.0.10.0 0.0.0.255
        Current peer: 8.8.8.8
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-P2,
        }
        Interfaces using crypto map VPN-MAP1:
                Serial0/1/0

Router#
```

This VPN was carried out between teleworkers with ip 172.168.1.0/24 and the DMZ. With VPN setup at Router 1 and the ASA firewall

Same as Site to Site IPSec VPN was used to safeguard files that comes from the teleworkers to the DMZ and vice versa, ensure that public network can't access and manipulate the data.

7. Step 6 (2 points): Re-evaluate the designed network system through the following features: reliability, ease of upgrade, diverse support software, safety, network security, etc

- **The remaining problems for the project:**
  - 1. Reliability
    - There is a single point of failure at the switches and routers due to Star Topology.
    - The network does not have any mechanism to backup packet. So, the chance of losing the packet is high.
    - The VLANs routing heavily depends on one-armed routers.
  - 2. Performance
    - There is no load balancer implemented at the Gateway, the workload is not distributed between the sites.
    - All traffic passes through one router at the Main Site, making it a potential congestion point.
  - 3. Ease of Upgrade
    - The network contains some legacy Cisco devices no longer supported by Cisco, making it hard to upgrade the network to adopt new technologies today.
  - 4. Security
    - Only the DMZ at the Main Site can be simulated, the servers at the branches were put behind the firewall so they do not belong to the DMZ, and the workload can not be shared.
    - Firewall filters the IP traffic, thus making the network vulnerable to IP spoofing.
  - 5. Features
    - Load balancing not yet implemented due to single firewall mechanism.

- Each sites has its own camera and does not share the camera system with other sites

- **Development orientation in the future**
  - Implement Dual Firewall mechanism for proper separation DMZ, allowing DMZ to be shared across branches for load balancing.
  - Implement a load balancing mechanism to ensure the availability of the network during peak hours.
  - Implement multiple routes between the network to avoid congestion and connection risks.
  - Implement Backup Servers to maintain reliable data transfer on the network.