DOKUZ EYLUL UNIVERSITY
ENGINEERING FACULTY
DEPARTMENT OF COMPUTER ENGINEERING

METROPOLITAN AREA NETWORK
SIMULATION PROJECT

by

Sefa Çelik - 2020510078

Ozan Kalkan - 2020510044

Hasan Balıkçi - 2021510012

İZMİR

03.05.2024

Content Table

1.Introduction

1.1. Project Definition and Problem Formulation

A computer network is a communication network where connected computers can communicate with each other and share resources. These networks are typically used for exchanging data, sharing resources, communicating, and collaborating among computers using wired or wireless connections.

A Metropolitan Area Network (MAN) is a computer network established within a geographical area, typically extending up to 60 kilometers in coverage. It facilitates data and resource sharing among devices within a large city or region. MAN acts as a transition point between Local Area Networks (LANs) and Wide Area Networks (WANs) by connecting multiple LANs. These networks consist of switches or routers interconnected with high-speed connections, often established using fiber optic cables. MANs can be large enough to cover entire cities or campuses.

There are numerous applications of MANs, including interconnecting local networks, positioning VoIP services, urban video surveillance systems, computer-to-computer connections, CAD/CAM transmission, and wide area network gateways. These networks are commonly used to connect offices of large companies or campuses of universities.

Advantages of MAN include high bandwidth, allowing access to numerous network access nodes, wide coverage area, distance between nodes, minimal delay for real-time traffic, integration of voice, data, and video, high availability, reliability, security, and noise immunity.

In summary, a Metropolitan Area Network (MAN) is a high-speed and reliable network type that facilitates data and resource sharing among devices within a city or region.

Our Metropolitan Area Network (MAN) design involves connecting two different branches in a city, each branch containing at least two routers (at least two routers for each branch), connecting these two branches through an Internet Service Provider (ISP).

The first branch network includes three different buildings, each with different units and requirements. The first building includes 3 desktop (PC) users, 3 wireless users (laptops), and 3 smartphone users. All users in this building can browse the web, send emails, and transfer files using their devices. The second building has 6 desktop users who can use Web and FTP. Two of the desktops are also used for VoIP conference activities. The third building houses a server farm

containing 10 Web servers, 4 FTP servers, 1 DHCP server, 1 mail server, and 1 domain name server (DNS).

The second branch includes three different buildings, each with different units and requirements. The first building has 5 desktop users, 5 wireless users, and 5 tablet users. They can connect to the Internet using wireless connections, browse the Web, and use email applications. The second building has 5 desktop users and 2 smartphone users. They can browse the web, edit applications, and transfer files. The third building includes 5 desktops and 2 mobile devices used for browsing the web, sending, and receiving emails.

This project addresses the need to establish and manage a network between different branches in a city. The design and simulation of this network were configured to meet various user needs.

1.2. The purpose and motivation of the project

This project addresses the need to establish and manage a network between different branches in a city. At the forefront of the project's implementation goal is to build a robust infrastructure in the field of cybersecurity. Today, one of the greatest threats faced by organizations and businesses is cyberattacks. Therefore, it is crucial for a company to have an integrated network infrastructure and ensure its security. This project aims to provide participants with practical experience in cybersecurity, enhancing their ability to implement and manage network security measures.

Additionally, another goal of the project is to reinforce fundamental networking knowledge. This project enables participants to enhance their knowledge and skills in fundamental networking topics such as network architecture, network security, network management, and network protocols. By developing a deep understanding of how networks operate, participants can take a more effective role in the design, implementation, and management processes of networks.

Furthermore, another benefit of the project is to help us understand today's complex network environments. Nowadays, businesses and organizations are often spread across multiple branches or regions, requiring the establishment of a secure and efficient communication network between these branches. This project allows participants to learn how to create and manage a network infrastructure between different branches by simulating real-world scenarios.

During the design of the project, efforts were made to effectively share network traffic, increase efficiency, and keep costs low, allowing participants to experience how to effectively build and manage a network.

For these reasons, this project presents an important opportunity for participants to enhance their knowledge and skills in the field of cybersecurity, reinforce fundamental networking knowledge, and understand today's network environments.

1.3. Term Definitions

Terms used in the project are defined below [9].

IP (Internet Protocol): IP is a communication protocol that governs data transmission over the internet. It enables the routing and delivery of data packets between computers. Computers and other devices communicate with each other on the internet using IP addresses.

IP addresses are unique identifiers for each device and can be in either IPv4 or IPv6 format. IPv4 addresses are typically represented by four sets of numbers (e.g., 192.168.1.1), while IPv6 addresses have a longer alphanumeric format.

IP facilitates communication by routing and delivering data packets to source and destination addresses. Each packet is sent to the IP address of the destination device and is routed to reach that destination through routers on the internet. This enables communication between computers and allows for data exchange.

MAC (Media Access Control): In computer networks, MAC is a unique identifier that defines the physical address of a network interface card (NIC). A MAC address is uniquely assigned to each network device and is usually pre-assigned to the NIC by the manufacturer. The MAC address enables devices to recognize each other and communicate in network communication. These addresses typically consist of 6 pairs of hexadecimal digits and are permanently written to a device's NIC. MAC addresses are used to facilitate device recognition and ensure that network traffic is directed to the correct devices. For example, in Ethernet or Wi-Fi networks, communication between devices is established and data is transmitted using MAC addresses. MAC addresses are stored in hardware on the NIC and cannot be changed, unlike IP addresses.

Web (World Wide Web): The Web is an information sharing platform created by bringing together documents and resources on the internet. The Web delivers content using languages such as HTML (Hypertext Markup Language). These pages can include various media content such as text, images, videos, audio files, and interactive elements.

Web browsers, the fundamental component of the Web, enable users to view web pages and interact with them. Users can browse the internet, perform searches, visit websites, and access various services through web browsers.

The Web operates on the HTTP (Hypertext Transfer Protocol), which facilitates data communication between servers and clients. A web browser sends a request to a web server, and the server responds with a response that fulfills the request. This allows users to access and interact with content on the web.

OSI (Open Systems Interconnection) Model: The OSI model is a reference model for data transmission in computer networks. This model simplifies complex network communication by separating the data transmission process into different layers. The OSI model was created to standardize how computer-to-computer communication occurs. It consists of a total of 7 layers:

- Physical Layer: Responsible for the physical transmission of data. Deals with physical components such as cables, connectors, signals, and electrical voltage.
- Data Link Layer: Ensures reliable data transmission. Provides data integrity and error correction. Works with MAC addresses.
- Network Layer: Provides packet routing and addressing. Works with IP addresses.
- Transport Layer: Organizes and controls data transmission. Provides data integrity and flow control. TCP and UDP operate at this layer.
- Session Layer: Manages communication sessions between two computers. Handles session establishment, maintenance, and termination.
- Presentation Layer: Converts data formats and performs encryption/decryption processes. Determines how data is presented.
- Application Layer: Facilitates communication with user applications (web browsers, email clients, etc.). This layer contains protocols, services, and applications. Protocols such as HTTP, FTP, SMTP operate at this layer.

Protocol: In computer networks and communication systems, protocols are established rules and standards for information exchange between devices. Protocols are used to regulate, format, transmit, receive, and process data transmission. These rules determine how data packets are created, addressed, routed, and processed. Protocols are used to facilitate compatible communication between different devices and systems and are typically organized in a layered structure. Various protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol) are commonly used for specific communication purposes.

TCP (Transmission Control Protocol): TCP is a communication protocol that provides reliable data transmission between computers. It is used for data transmission over the internet and is part of the TCP/IP protocol suite. TCP ensures reliable transmission by preventing packet loss and erroneous transmission during data transmission. To achieve this, it divides data into packets, verifies the receipt of each packet, and has the ability to resend missing or erroneous packets. Since TCP is a connection-oriented protocol, it manages the data flow after establishing communication and ensures that data is transmitted in an orderly manner.

DHCP (Dynamic Host Configuration Protocol): DHCP is a network communication protocol that automatically distributes network configuration information such as IP address, subnet mask, default gateway, and DNS server to devices (computers, phones, tablets, etc.) on a network. DHCP provides an easier and automatic method for network administrators to allocate and manage IP addresses.

DHCP Server: A DHCP server is a server that distributes IP addresses and other network configuration information to devices on the network using the DHCP protocol. When devices on the network request IP addresses, a DHCP server responds to these requests and assigns appropriate IP addresses. The DHCP server also coordinates IP address assignment operations to prevent IP address conflicts.

DNS (Domain Name System): DNS is a system that translates domain names (such as website names) into IP addresses on the Internet. People typically access websites using domain names (e.g., www.example.com), but computers connect to these sites using IP addresses. DNS works to find and direct users to the relevant IP address when they enter domain names.

DNS Server: A DNS server is a specialized computer that enables the functioning of DNS and responds to requests to resolve domain names to IP addresses. A DNS server stores a database where domain names are mapped to IP addresses and responds to incoming requests by resolving IP addresses from this database. DNS servers play a critical role in the infrastructure of the internet and are a crucial component in accessing websites.

FTP (File Transfer Protocol): FTP is a communication protocol used for transferring files between computers. It is employed to transfer files from one computer to another or to retrieve files from another computer. This protocol facilitates the secure and rapid transfer of files.

FTP operates on a server-client model. An FTP client connects to an FTP server to perform file transfer operations. Users can upload files to the server or download files from the server using an FTP client.

FTP Server: An FTP server is server software used to manage file transfer operations. An FTP server accepts connections from FTP clients and allows these clients to perform file transfer operations.

An FTP server securely manages file transfers by granting users access permissions to specific directories. It prevents unauthorized access by authenticating users and facilitates file transfer operations in a secure environment.

FTP is commonly used, especially in situations requiring the transfer of large files, such as uploading or downloading files for websites.

HTTP (Hypertext Transfer Protocol): HTTP is a protocol used for communication on the internet. It is a standard communication protocol for exchanging information between web browsers and web servers. HTTP enables web browsers to request web pages from web servers and allows servers to respond to these requests.

HTTPS (Hypertext Transfer Protocol Secure): HTTPS is the secure version of HTTP. HTTPS utilizes the SSL/TLS protocol to encrypt and secure communication. This ensures the confidentiality and integrity of data transmitted over HTTP. HTTPS enables the secure transmission of sensitive information, such as usernames, passwords, and credit card details, particularly used by websites.

Mail (Email): Email is a communication tool used for electronic communication. Users can communicate with each other by sending electronic messages to email addresses. Email messages typically contain text, attachments, images, or other types of media.

Mail Server: A mail server is server software used to manage email communication and provide users with access to their email accounts. A mail server performs functions such as transmitting, storing, and facilitating access to incoming and outgoing emails. Users can access their email accounts by connecting to the mail server using email clients (such as Outlook, Thunderbird, Gmail, etc.).

POP (Post Office Protocol): POP is a protocol that allows email clients (e.g., Outlook, Thunderbird) to retrieve emails from an email server. It enables users to download their emails from the server and save them to their local devices. By connecting to a POP server, users can retrieve email messages from their mailboxes. However, since the POP protocol downloads emails stored on the email server to local devices, the emails downloaded from the server are usually deleted from the server. Therefore, emails are downloaded only once and stored on local devices. POP3 (Post Office Protocol version 3) is the most widely used version of POP.

SMTP (Simple Mail Transfer Protocol): SMTP is a communication protocol used for sending emails. SMTP enables email clients (e.g., Outlook, Gmail) to send emails by connecting to an email server. Email messages created by the user are sent via the SMTP protocol and delivered to the recipient's email server. The recipient server then receives the email and delivers it to the recipient's inbox. SMTP can utilize security protocols like TLS (Transport Layer Security) to securely transmit email messages. This allows for encryption and authentication during the transmission of email messages.

SSH (Secure Shell): SSH is both a protocol and software used to establish a secure network connection. It facilitates secure communication between computers over a network. SSH is commonly used for remote access and file transfer purposes. By encrypting communication, SSH ensures the secure transfer of data and maintains privacy. Additionally, it provides a secure method for authentication, allowing users to securely access remote servers.

VoIP (Voice over Internet Protocol): VoIP is a technology that enables the digital transmission of voice communication over the internet. It allows for the transmission of voice data over internet connections instead of traditional telephone lines. VoIP transmits voice signals in the form of digital data packets, facilitating phone calls. This technology enables various forms of communication over the internet, including voice calls, video conferences, and voice messages. VoIP offers communication at lower costs compared to traditional telephone lines and often provides more flexibility and features.

Network: A system that facilitates the exchange of information and data between computers or other devices. This system uses connections and communication protocols to enable data exchange between different devices. For example, in a business network, employees can share files, communicate via email, or use a shared printer. In home networks, family members can connect to the internet, share home entertainment systems, or access file storage devices. Networks are used for various purposes such as communication, data sharing, resource

utilization, and collaboration. Depending on these purposes, different types of networks can be established, and various devices and communication protocols can be used.

Network Architecture: A concept that defines the physical and logical structure, components, and organization of computer networks. Network architecture encompasses elements that constitute the infrastructure enabling communication and data transmission between devices in a network. These elements include network devices (computers, routers, switches, access points, etc.), communication channels (wired or wireless communication paths), protocols, management strategies, and security measures. Network architecture is a broad concept that encompasses the design, configuration, and management of a network and is often organized in a layered structure. For example, the OSI (Open Systems Interconnection) model divides network architecture into seven layers, with each layer performing a specific communication task. Network architecture is designed and managed to enhance the efficiency, security, and scalability of a network.

Wireless: Wireless communication is a method of data transfer that utilizes wireless technologies such as radio waves or infrared light instead of cables. It is used to facilitate data transfer between computers, smartphones, tablets, and other devices. Various wireless technologies exist, including Wi-Fi, Bluetooth, and NFC. Wireless communication provides mobility and convenience as devices can communicate with each other without being tethered by cables.

Ethernet: Ethernet is a network technology used in local area networks (LANs). It utilizes wired connections for data transmission, typically through copper cables. Ethernet enables data transmission between computers, printers, routers, and other network devices. It can provide high-speed data transmission and offers a reliable connection. Ethernet networks form the backbone of computer networks and are used for services such as internet access, file sharing, printer sharing, and other network services.

Router: A router is a network device that manages data traffic within a network and facilitates communication between different networks. Its primary function is to receive incoming data packets, route them to their destinations, and determine the most optimal path. Routers typically connect devices to each other via IP addresses and operate on the Internet Protocol (IP). They are also used to facilitate data communication between multiple networks. Routers manage communication between different devices in a network and ensure secure communication.

Switch: A switch is a network device that manages data traffic within a network and facilitates communication between different devices. It forwards data packets between computers in a network, accelerating communication and optimizing bandwidth. Switches route data transmission based on Media Access Control (MAC) addresses, directing traffic to the intended device. This enhances network performance and makes communication more efficient.

Access Point: An access point is a device used to connect to wireless networks. It enables wireless devices to access the network. Wireless devices can join the network by connecting to an access point. Access points typically use Wireless Local Area Network (WLAN) technologies and manage data transmission in wireless networks. They facilitate communication between multiple wireless devices and manage access to the wireless network.

Server: In computer networks, a server is a computer program or hardware device that provides services to other devices (clients). Servers typically offer services such as file sharing, printing, web pages, email, databases, applications, or other network resources to clients. Servers are specifically configured to meet client requests and are often built using high-performance and reliable hardware. For example, a file server may provide file storage and sharing services to users on the network, a web server may serve web pages to clients over the internet, or an email server may manage email communication. Unlike other devices in the network, servers typically operate continuously and are ready to provide services to clients.

Packet: In computer networks, it refers to small data fragments used for data transmission. A packet is the smallest unit of data carried during transmission. Packets are used to facilitate communication between source and destination devices. Each packet consists of a header and a data section. The header contains communication information such as the packet's source, destination, sequence of transmission, and other relevant details. Packets are utilized to ensure reliability and efficiency in data transmission.

Frame: It is a unit used for carrying data in network communication. A frame is the smallest unit of data used for network data transmission. Frames are employed to facilitate communication between network devices. Each frame comprises a header, data, and sometimes a trailer section. The header contains information such as the frame's source, destination, type, and other communication details. Frames are utilized to ensure reliability, integrity, and error checking in data transmission.

Channel: It is the communication pathway used for information or data transmission. A channel is a physical or logical communication path or interface used to transfer data from a source to a destination. For example, an Ethernet cable in a wired network or a Wi-Fi connection in a wireless network constitutes a communication channel. Channels represent the communication mediums and protocols used in data transmission.

Message: It refers to a piece of information or communication transmitted from a source to a destination. A message is a communication unit sent from a source and may contain a specific purpose or content. Messages can be in the form of text, audio, images, data, or any other information type. For instance, email messages, text messages, or file transfers are examples of messages. Messages are utilized for information exchange and communication during the communication process.

ISP (Internet Service Provider): It is an organization known as an Internet Service Provider. ISPs are companies that provide users with internet access and offer various internet services. ISPs typically provide internet connectivity using various communication methods such as broadband, cable, DSL, fiber optics, or wireless technologies. They offer subscription services for internet access and usually allocate IP addresses to subscribers. ISPs may also provide web hosting, email services, domain name registration, and other internet services.

Workstation: These are computer systems connected to a computer network, typically used by users to perform daily tasks. Workstations can be desktop computers or laptops and enable users to run office applications, process data, access the internet, and perform other tasks. Workstations can communicate with other devices on the network and access shared resources. For example, a workstation can send documents to network printers, store files on network storage units, or communicate with other users on the network. Workstations are considered significant components in a network and are often integrated into the network to enhance productivity.

1.4. Related Work

Our research conducted within the scope of our project has revealed significant differences from other studies on network simulations. Particularly, we have undertaken various additional efforts to develop unique and efficient solutions concerning the design and performance of the network infrastructure.

Firstly, our approach of using a separate router for each building has allowed us to optimize network performance by isolating broadcast traffic within each building. This strategy aims to increase access to local services by isolating network traffic within each building, while also enhancing overall network performance.

Furthermore, we have focused on modularity and efficiency in our studies. In this context, we have ensured the isolation of groups of devices that need to work together and occasionally go offline together by connecting them to a single switch or access point. This approach aims to enhance the modularity of the network, facilitating interaction between units and improving network performance.

We believe that all these efforts will contribute positively to the success of our project and the effectiveness of the network infrastructure. These methods and solutions are poised to provide our project with a competitive edge in the industry and exceed industry standards.

2. Method and Simulation

2.1. Simulation and Modeling Concepts

In establishing our network, we followed a detailed planning and implementation process. Initially, we conducted studies to determine whether to build the network from top to bottom or from bottom to top. At this stage, we decided to build the network from top to bottom. This allowed us to establish the overall infrastructure of the metropolitan area network (MAN) and set a more secure progression method. Firstly, we decided to set up the ISP side using a router. We provided external connections to our network by serially connecting this router to main routers within two branches.

After establishing the external connections on the ISP side, we researched how to make the internal design of the branches more efficient and secure. As a result of our research, we decided to assign a separate router to each building to reduce broadcast traffic and achieve modularization between buildings. This approach prevented internal broadcast traffic from being forwarded externally and increased network efficiency by 7-8%. The routers used for each building were connected to the main router within the branch via serial connection[7][8].

To ensure proper communication among devices within each building, we used switches and wireless access points. This enabled each device to seamlessly connect to the network and communicate. When creating the internal networks of the branches, we organized devices and connection points according to their individual needs. By connecting devices that need to work together and require joint intervention in case of an issue to the same switch or wireless access point, we ensured modularity. Workstations and servers were connected to the network via wired Ethernet connections through switches, while tablets, smartphones, and laptops were connected wirelessly through access points.

The third building within the first branch was designated as the main server building. Inside this building, 10 WEB Servers, 4 FTP Servers, 1 DHCP Server, 1 Mail Server, and 1 DNS Server were added according to the requirements of each branch. The configurations of these added servers were then completed, and they were integrated into the network. These servers were consolidated on two main switches. The first switch was used for the 10 WEB Servers, while the second switch was used for the remaining servers. These two switches were combined on a separate main switch to ensure modularity, and the main router of the building was connected to this main switch. This allowed all devices within the network to be assigned IP addresses based on the IP pools we created on the DHCP Server [1]. Web connections and file transfer operations were enabled through the WEB Server and FTP Server we used [4]. The DNS Server we used allowed the IP addresses of WEB Servers to be defined with a meaningful domain [5]. Finally, the SMTP and POP protocols used on the Mail Server enabled inter-device mail service [3]. Thus, the servers created to meet the service needs of the devices were successfully integrated into the network and the services started to be actively used.

In conclusion, by following a detailed planning and implementation process, we established the network by adopting a top-down approach, then optimized the internal networks of each building by ensuring modularity and security. Proper communication provided by switches and wireless access points allowed devices to seamlessly connect to and communicate on the network. Configuration done at the main server building allowed us to add servers tailored to the requirements of the branches and integrate them into the network. In this way, we successfully completed the project efficiently and securely.

2.2. Simulation Environment/Tool

Simulation environments and tools are used to test and evaluate network configurations, protocols, and architectures. These tools can replicate real-world scenarios, analyze network behavior, and create simulated networks without causing harm to live systems.

Among the advantages of these tools are the ability to experiment, visualization and interaction, testing various configurations, collaborative learning, and troubleshooting. However, disadvantages include limited realism, constraints on device and network complexity, and a learning curve.

In our project, simulations were conducted using Cisco Packet Tracer. Cisco Packet Tracer is software developed by Cisco that enables the simulation of scenarios related to network configuration. It is highly useful for testing and visualizing network configurations before physically setting up real network devices.

Cisco Packet Tracer adopts a client-server architecture. Users utilize the client interface to design and configure network topologies, while the server manages simulation processes and interactions between devices. Packet Tracer combines logical and physical modeling approaches and can simulate network devices such as routers, switches, and hubs.

While Packet Tracer can simulate the devices of a large network, it may offer limited support for advanced features and protocols compared to real Cisco hardware. Users can configure and run simulations using the graphical interface. Packet Tracer provides various modules and components for designing, configuring, and simulating network topologies.

Simulation tools like Cisco Packet Tracer play a vital role in network education and training. Despite limitations compared to real-world networks, they provide indispensable resources for network professionals and students, offering advantages such as accessibility, usability, and collaborative learning.

2.3. Network Design Requirements

In our project, we designed the Metropolitan Area Network (MAN) to minimize traffic, increase modularity, and be as useful as possible according to the requirements. We adopted a server/client architecture for the network. The server/client architecture is a widely used structure in computer networks where one or more servers provide services to client devices. Servers typically handle functions such as storing large amounts of data, hosting applications, or providing other network services. For example, a file server can store files that clients can access. Clients, on the other hand, perform functions such as retrieving, storing, or processing data by accessing servers. Clients are typically user devices like personal computers, laptops, smartphones, or tablets. This architecture simplifies network management and centralizes resources, facilitating data sharing, collaboration, and efficient service management within the network. It is commonly used in large-scale networks and corporate environments, making network management easier while providing easy access to services for users.

For the network topology, we opted for a star topology. The star topology consists of other devices (computers, printers, servers, etc.) connected around a central main device (usually a switch or hub). One of the main reasons for this choice is the advantages provided by the star topology. Firstly, this topology offers a simple and easily manageable structure. The central main device coordinates all communication on the network, making network management and troubleshooting easier. Additionally, the star topology offers flexibility; in case of a device failure, other devices can continue to function on the network without being affected. However, the star topology also has some disadvantages. In particular, if the central main device fails, the entire network can be affected, and communication can be disrupted. Additionally, the use of additional cables and the cost of the central device in the star topology can increase. Nevertheless, considering the requirements of our project, we chose the star topology based on its advantages such as simple management, flexibility, and reliability. This allowed us to efficiently manage our network and create a structure that meets our requirements.

In the first branch, except for the second facility, all building branches and ISP routers involving VoIP connections were designed from scratch by selecting Router-PT Empty and configuring them according to the required ports [2]. We used the 2811 model as a router in the first branch's second facility to establish VoIP connections. For wired connections, we selected Switch-PT Empty and added Ethernet ports according to the required number of ports, configuring the switches accordingly. We also provided wireless connections by selecting Access-PT as the Access Point.

In conclusion, our network design utilized 8 Router-PT Empty, 1 2811 Router, 14 Switch-PT Empty, 4 Access Point PT, 17 Servers, 24 Workstations (PCs), 8 Laptops, 5 Tablets, 7 Smartphones, and 2 VoIP Phones, successfully completing the design. DHCP, DNS, FTP, POP3, SMTP, HTTP, HTTPS, TCP, and SSH protocols were used for communication between devices in the network [6].

2.4. Requirement Analysis

In our project, we conducted the requirement analysis by identifying functional requirements for different applications and services, determining performance requirements and constraints such as the number of users the network needs to support, and the network speed. After establishing the desired network structure, we defined the communication between devices, configured servers, determined which devices can access servers, and documented device permissions as requested.

In this project, a Metropolitan Area Network (MAN) consisting of two separate branches was designed. The network structure of the first branch comprises three different facilities. In the first facility, there are 3 PC users, 3 wireless users (laptops), and 3 smartphone users. These users can browse the web, send emails, and transfer files using their devices. The second facility has 6 PC users who can transfer files using web and FTP. Additionally, 2 PCs in this facility are used for VoIP conferencing activities. The third facility includes a server farm with 10 Web servers, 4 FTP servers, 1 DHCP server, 1 mail server, and 1 domain name server (DNS). The network structure of the second branch also consists of three different facilities. The first facility has 5 PC users, 5 wireless users, and 5 tablet users. These users can access the internet wirelessly, browse the web, and use email applications. The second facility includes 5 PC users and 2 smartphone users who can browse the web, edit applications, and transfer files. The third facility includes 5 PCs and 2 mobile devices, allowing users to browse the web and send/receive emails. The connections between these branches were established using various routing and connection technologies.

The performance requirements of the project encompass the various services and applications that the network needs to provide, as well as the overall speed and capacity expectations. Firstly, the network is expected to provide uninterrupted access to the services required by all users. This includes the continuous and fast execution of basic functions such as web browsing, email sending, and file transfer. Additionally, the network should support voice-based applications such as VoIP conferences by providing sufficient bandwidth and low latency. Another performance requirement is for the network to facilitate data communication reliably and quickly between the two branches, allowing users to effectively utilize the network for file sharing and communication. Finally, the overall performance of the network should be able to adapt to dynamic conditions such as increases in the number of users or changes in network traffic. This enables the network to respond to expansion and growth requirements while maintaining efficient operability without adversely affecting user experience. These performance requirements should be considered to ensure the healthy and effective operation of the network, and the compliance of the design with these criteria should be continuously evaluated.

2.5. Definitions of the System/Model

Assumptions and Structural Features Regarding Our Project's System and Model:

- Assumptions about Components and the System: It is assumed that communication between network components will be uninterrupted and reliable. Additionally, it is presumed that the network hardware is capable of supporting the desired services and applications.

- System Structure: The system used in our project is based on a star topology, where other devices are connected around a central main device (such as a switch or hub). This structure simplifies network management and facilitates expansion.

- Formulations and Hypotheses on Input Parameter Values: By analyzing factors determining network performance, the aim is to keep input parameters within specified value ranges.

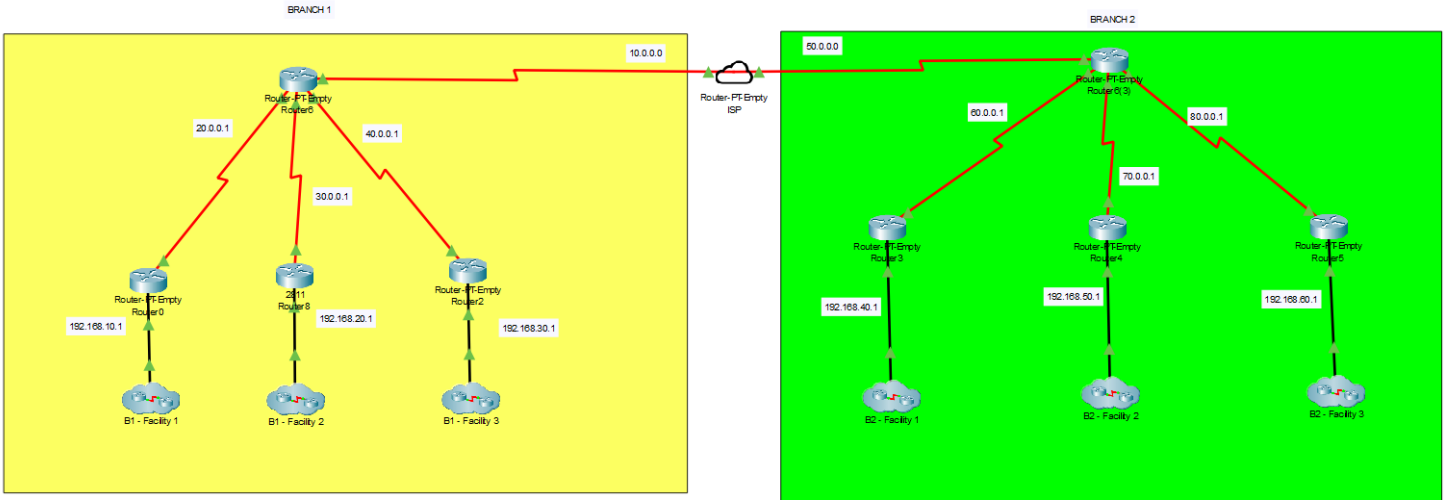
- Network Configuration: The network used in our project is divided into subnets using specific IP address ranges. Additionally, network configuration elements such as routing tables and IP addressing plans have been determined.

- Data Types, Data Sources, and Device Types: Data types used in our project generally consist of packets or frames. Data sources include user devices, servers, and routers, among other network components. Device types range from desktop computers, laptops, smartphones, tablets, servers, to routers.

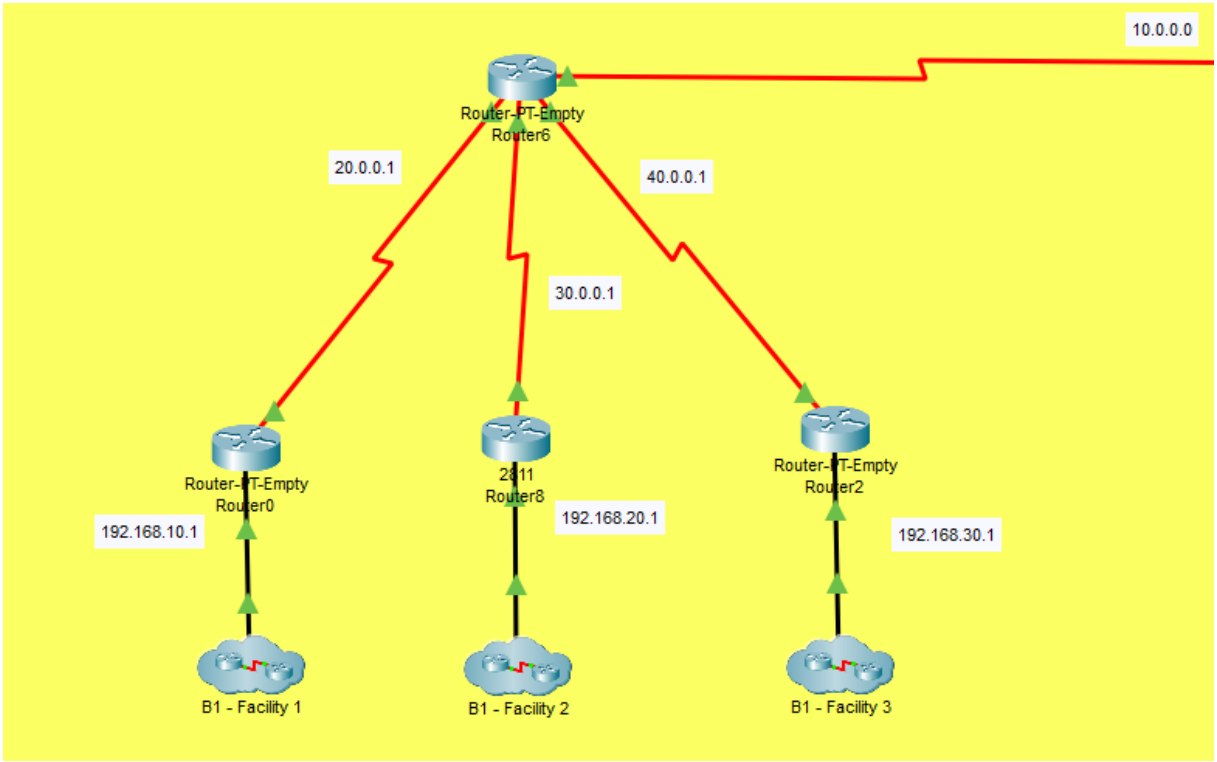
- Users' Goals and Numbers: The general goal of users in our project is to access resources on the network and communicate. The number of users defined for each branch and facility is determined considering the network's capacity and performance requirements.

Below are diagrams illustrating the general structure of the network we have created.

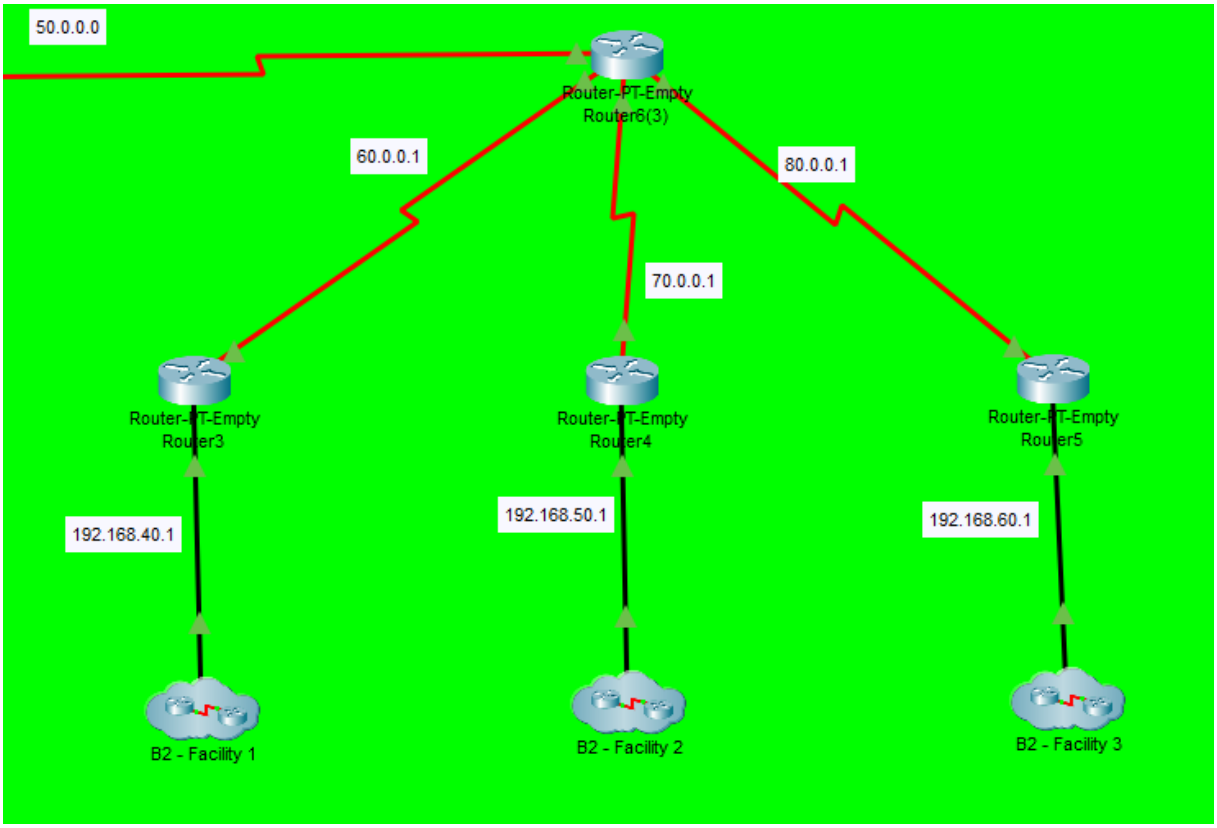
Logical Design of The System



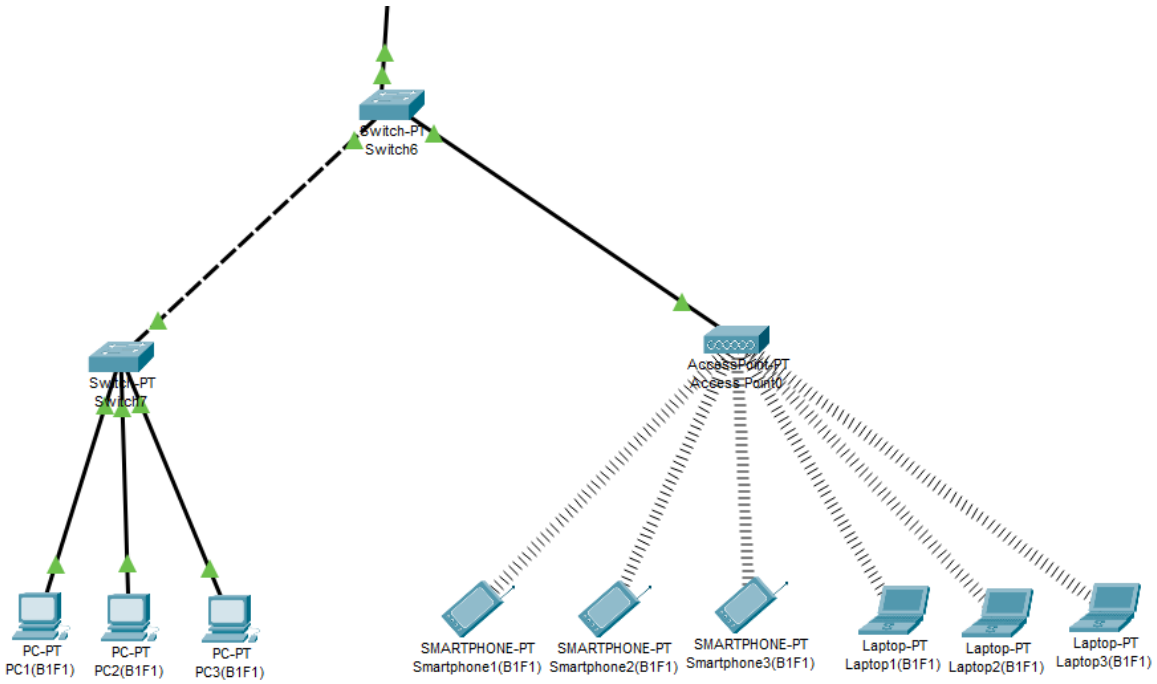
First Branch:



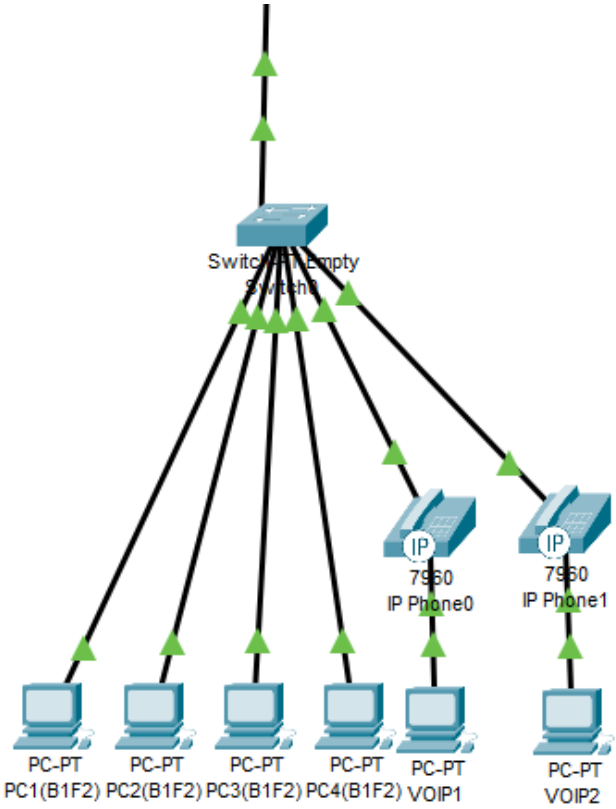
Second Branch:



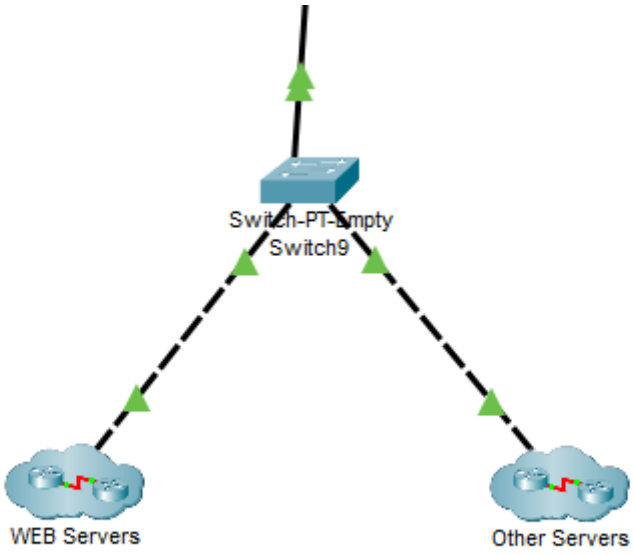
First Branch First Facility:



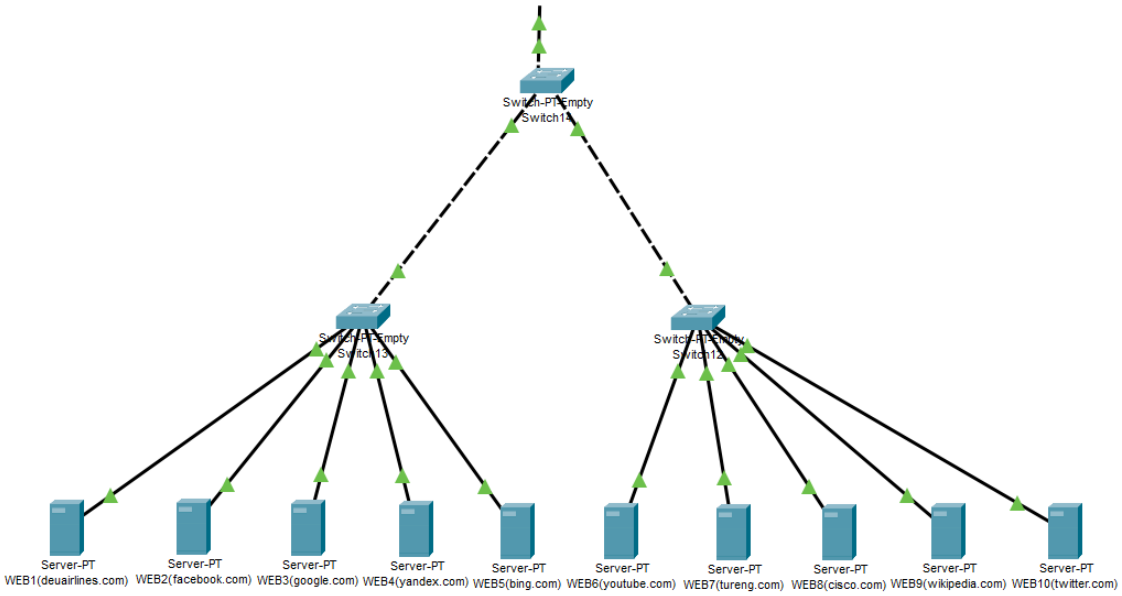
First Branch Second Facility:



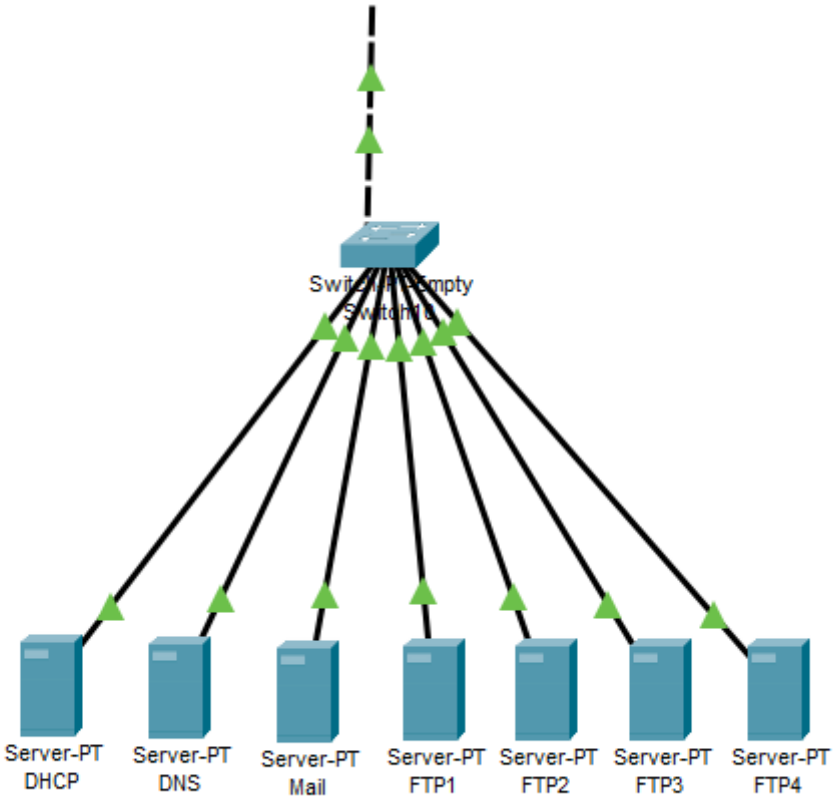
First Branch Third Facility:



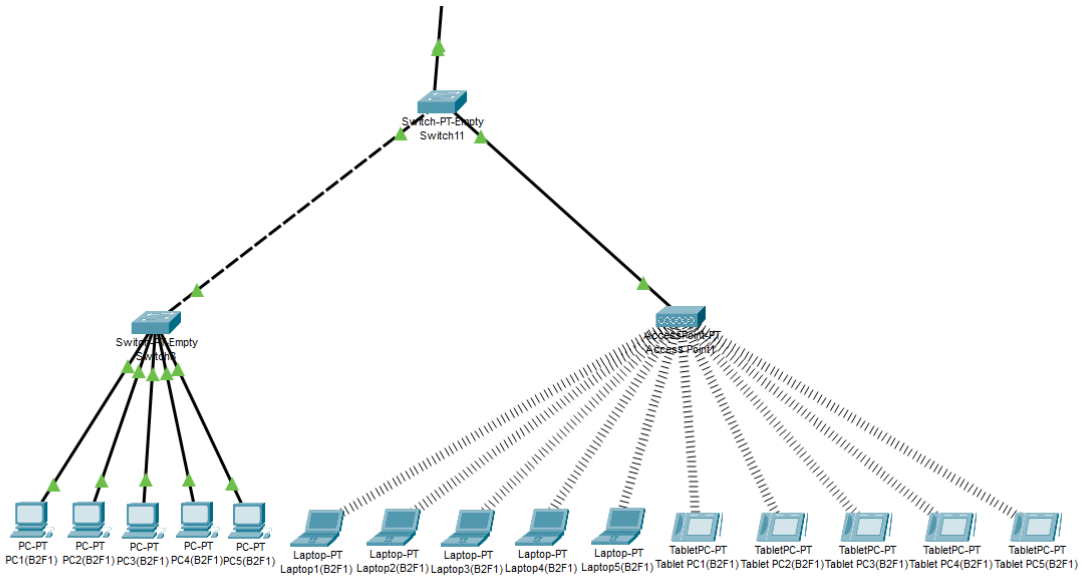
Web Servers:



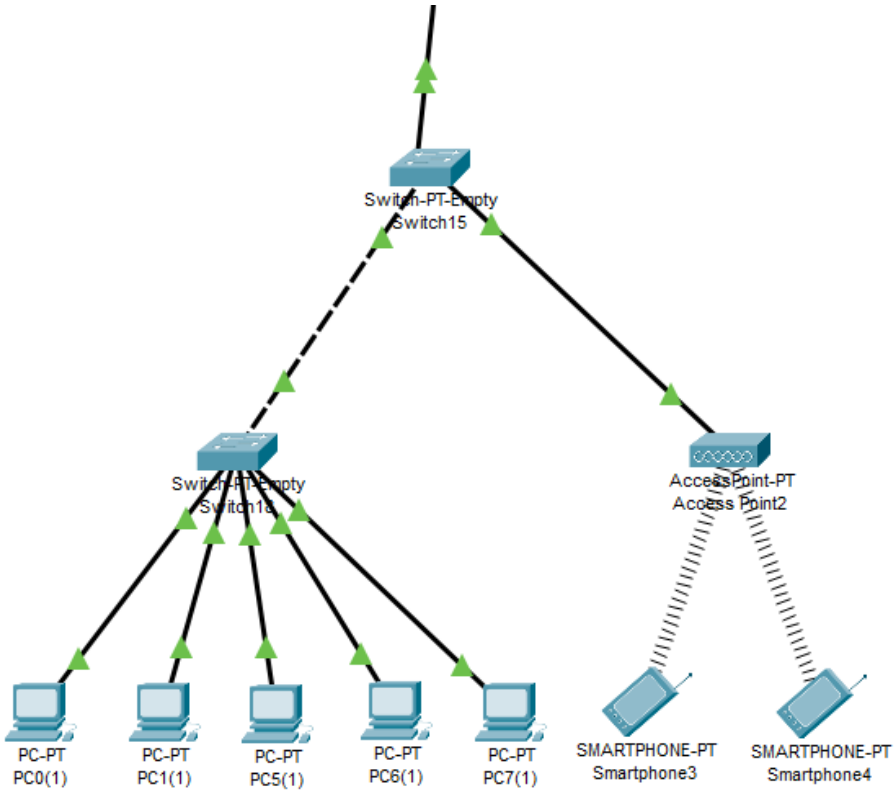
Other Servers:



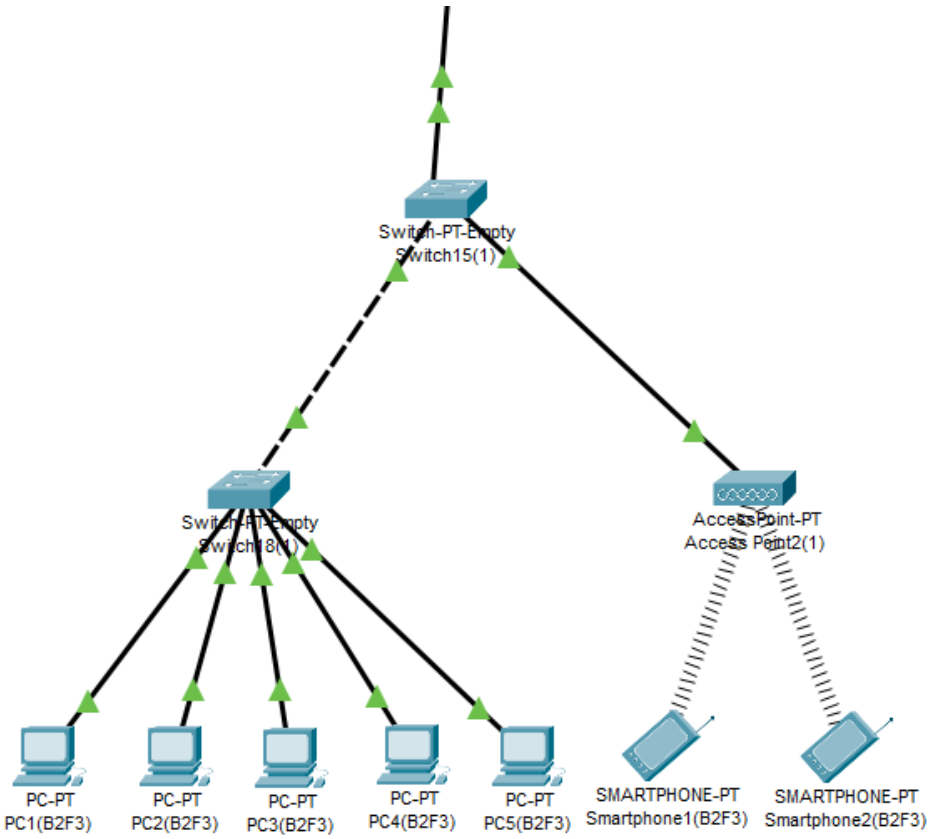
Second Branch First Facility:



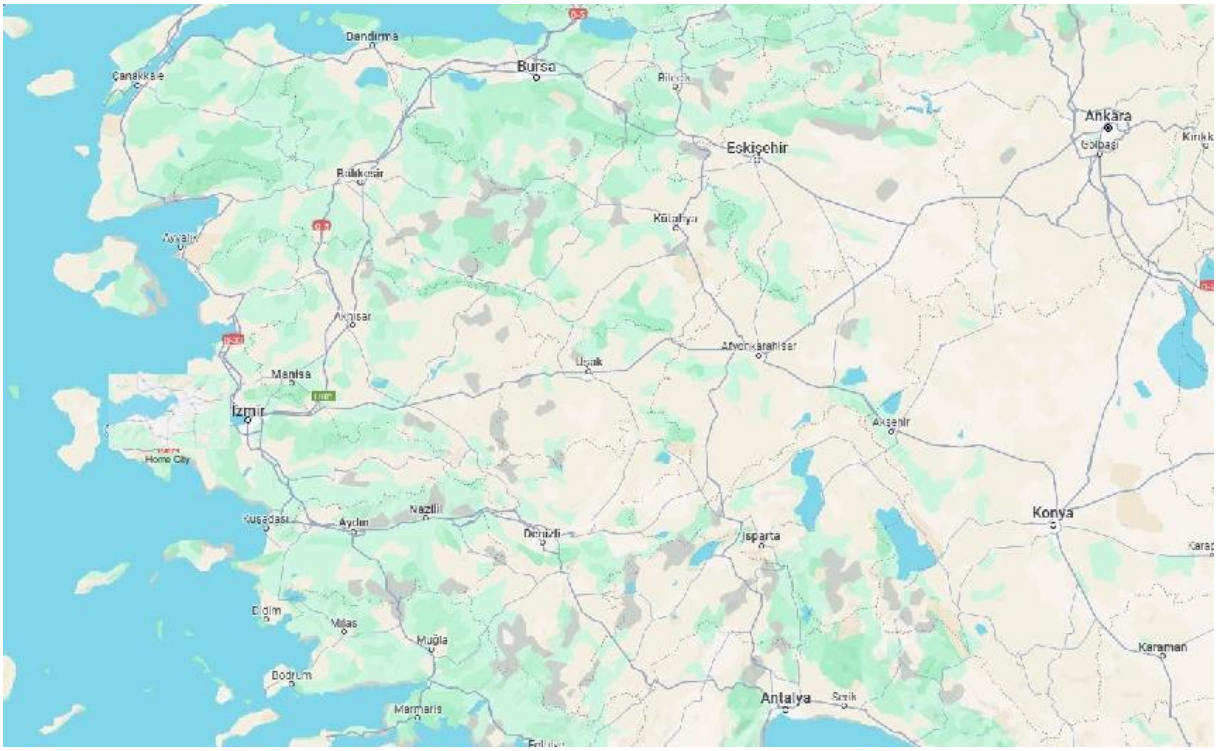
Second Branch Second Facility:

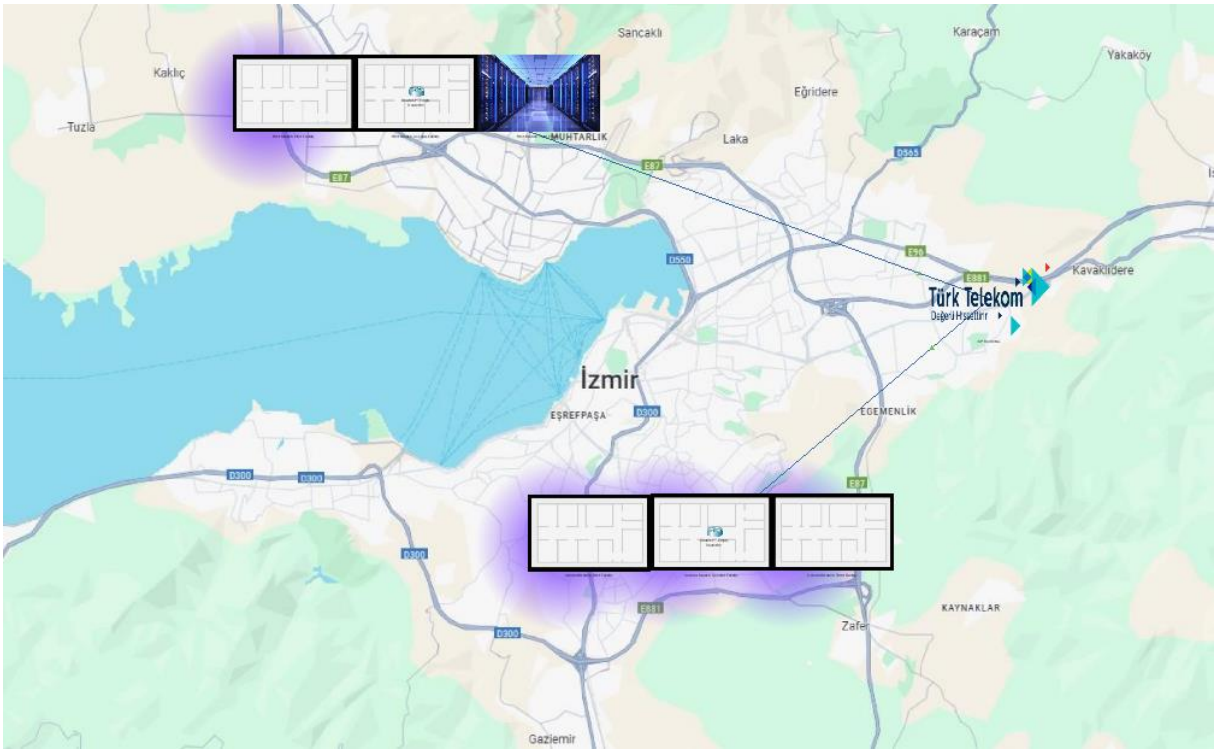


Second Branch Third Facility:

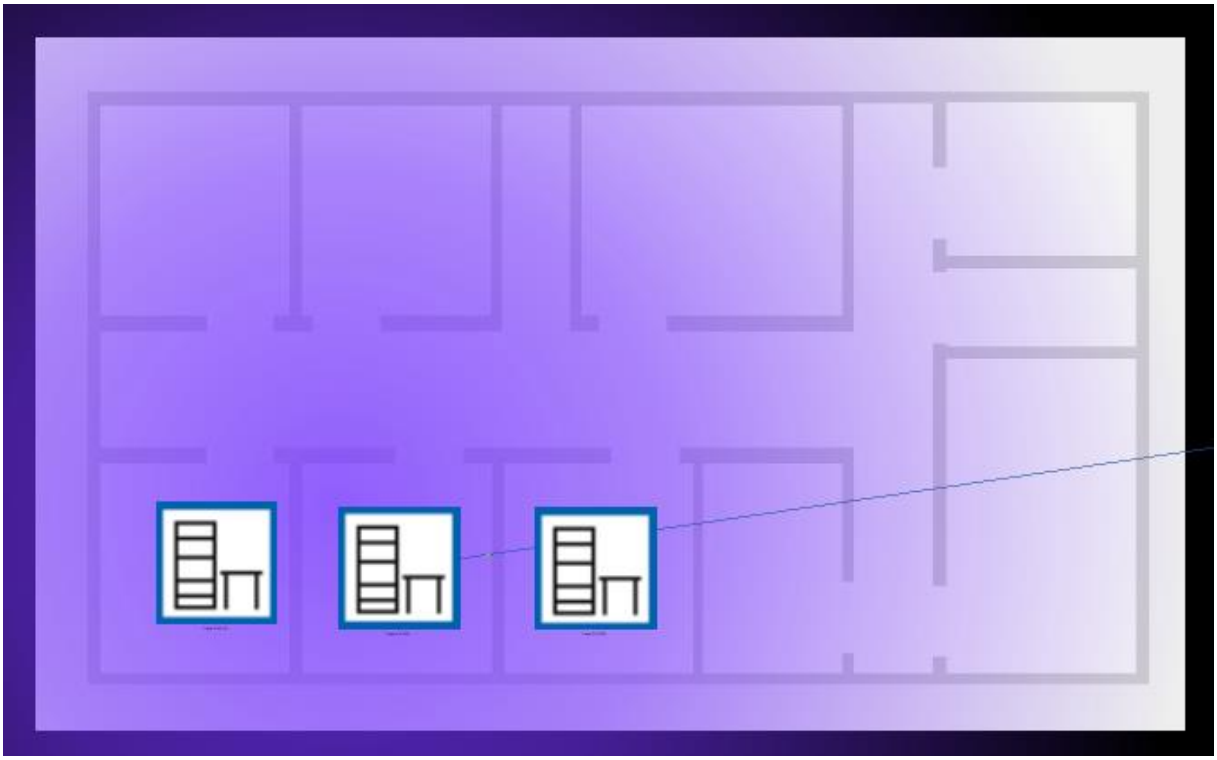


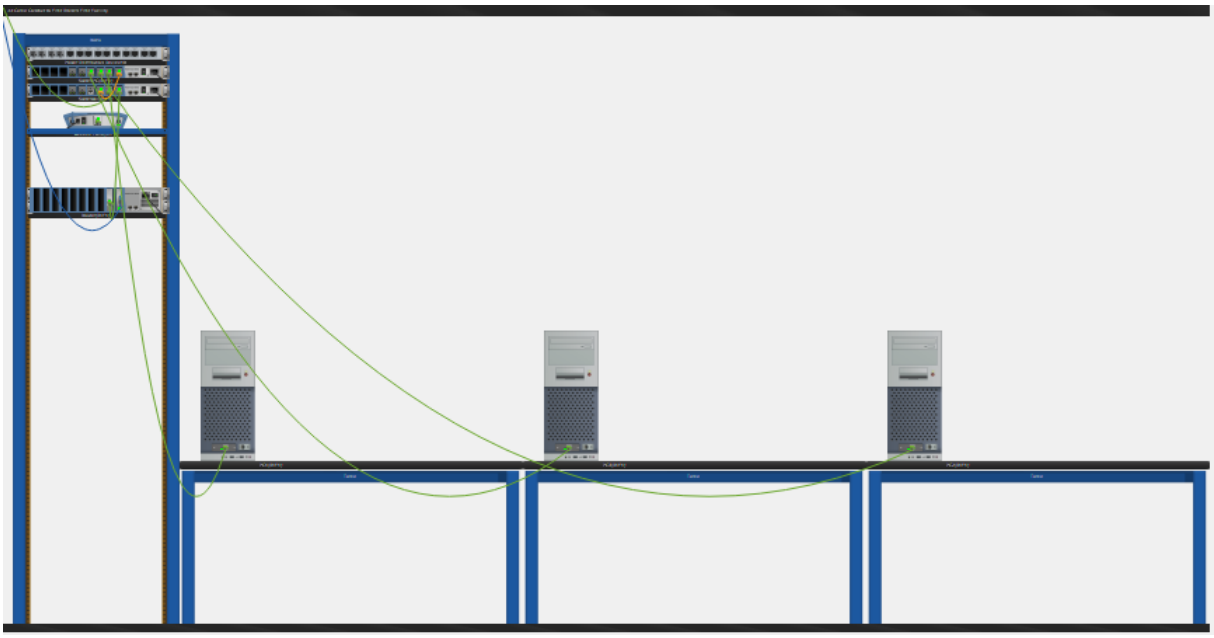
Physical Design of The System

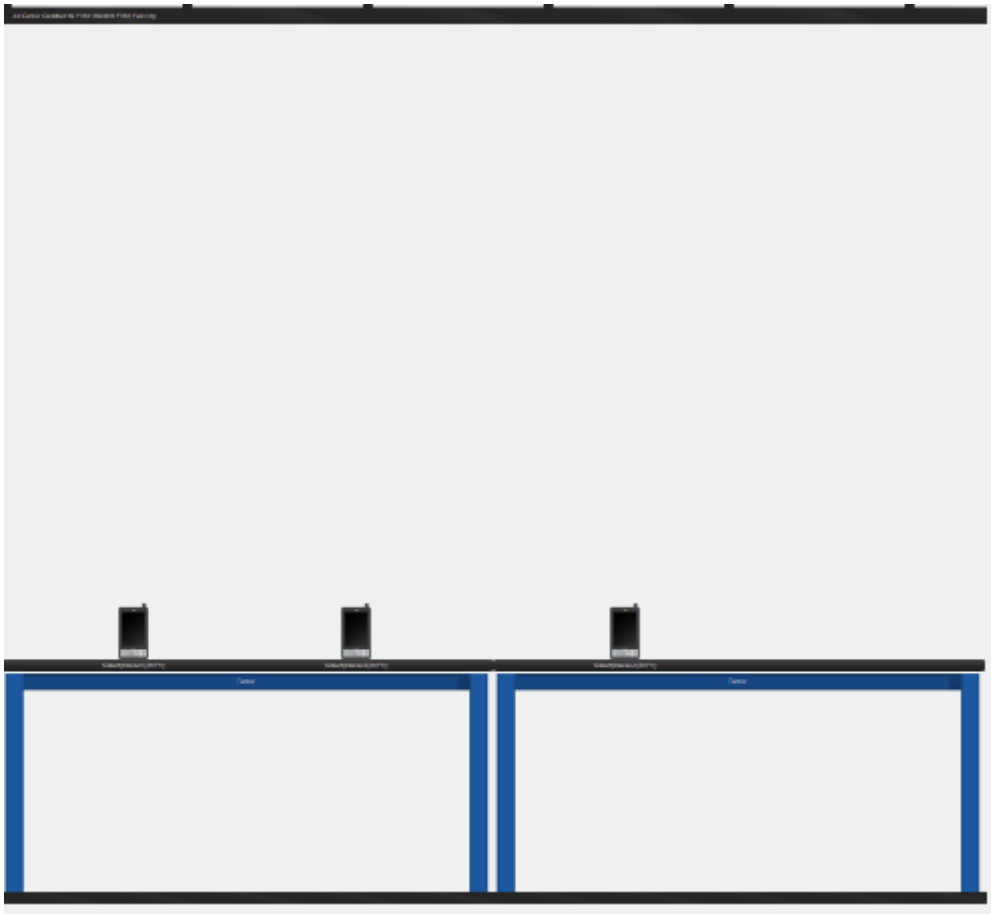




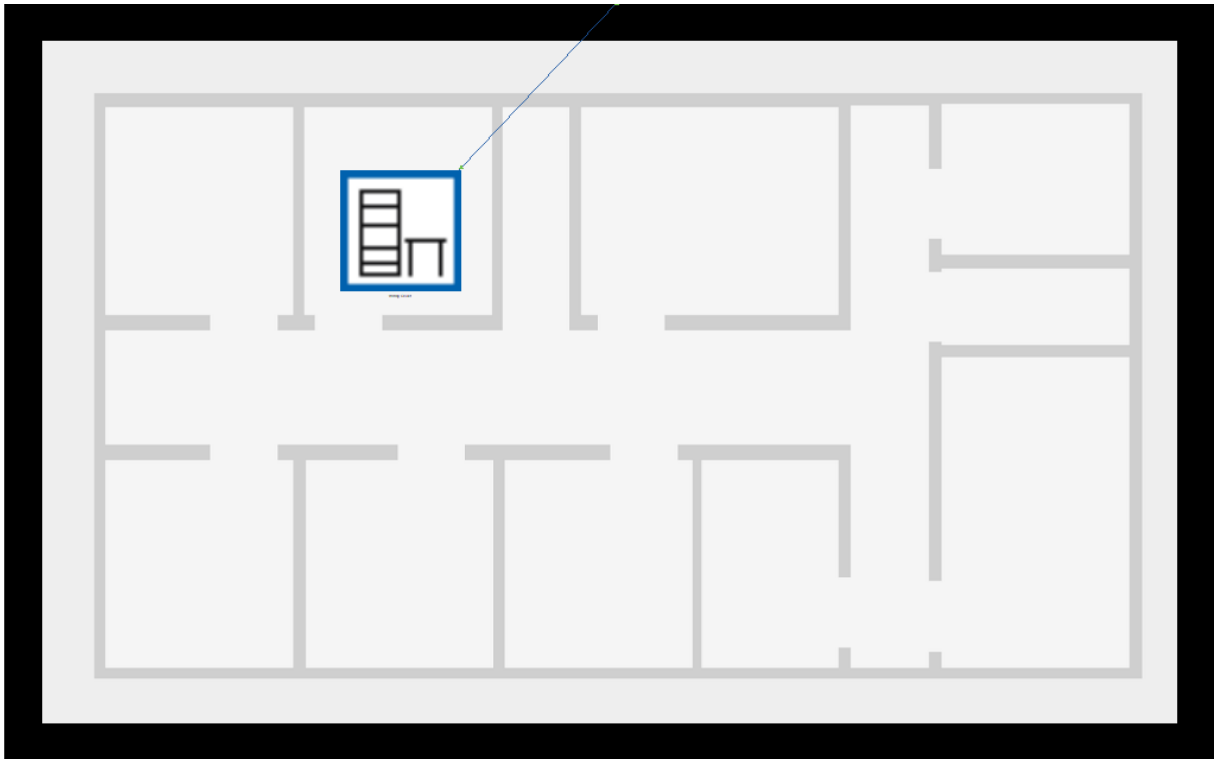
First Branch First Facility:

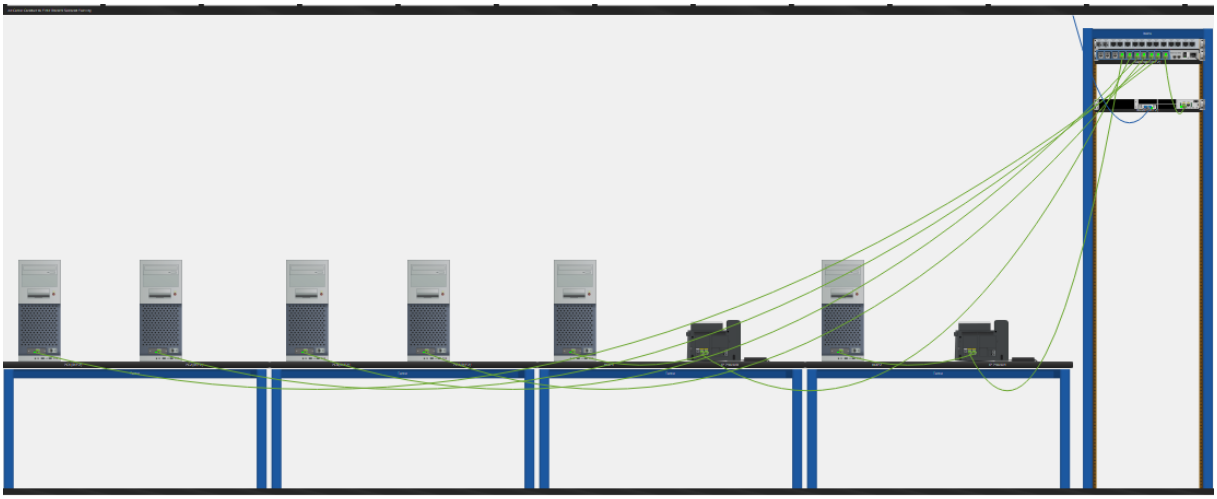




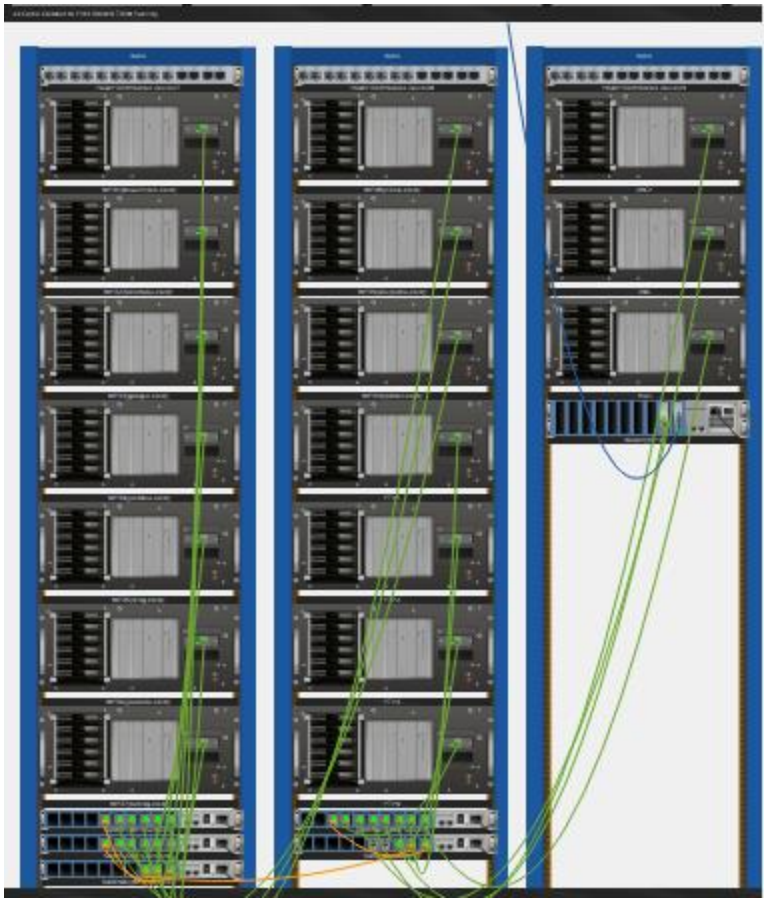


First Branch Second Facility:

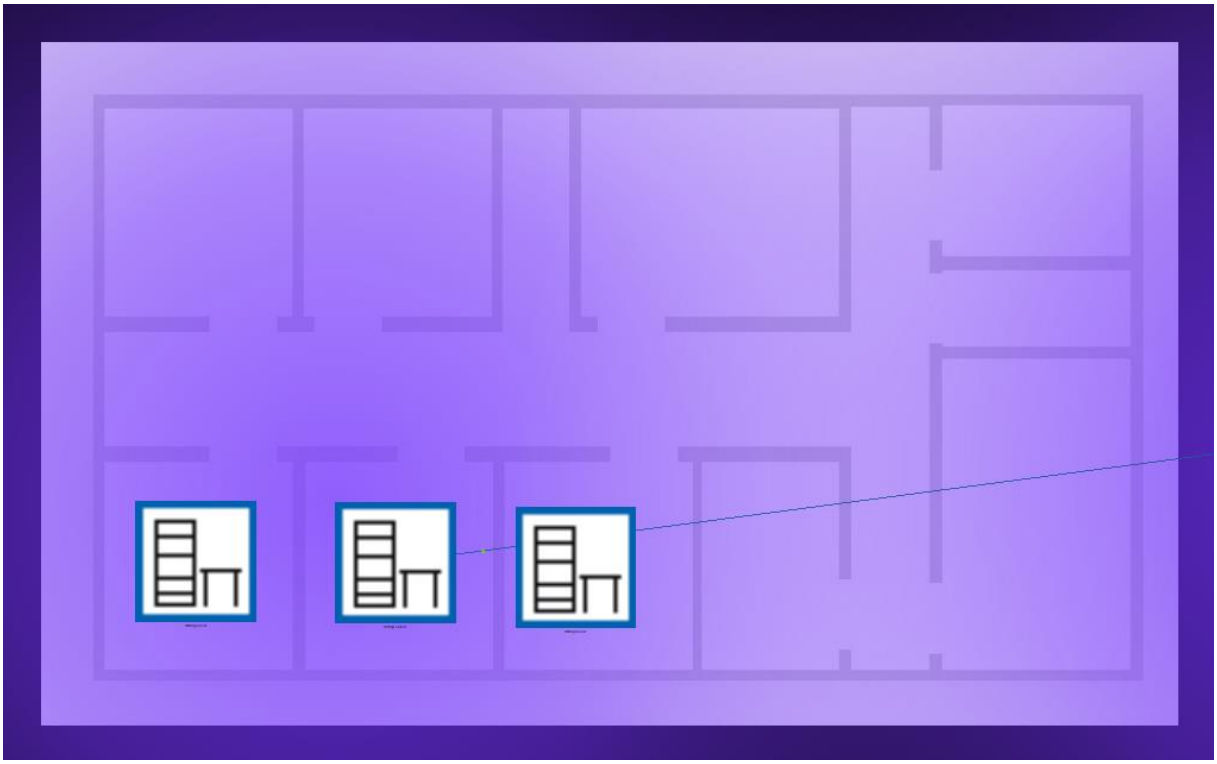


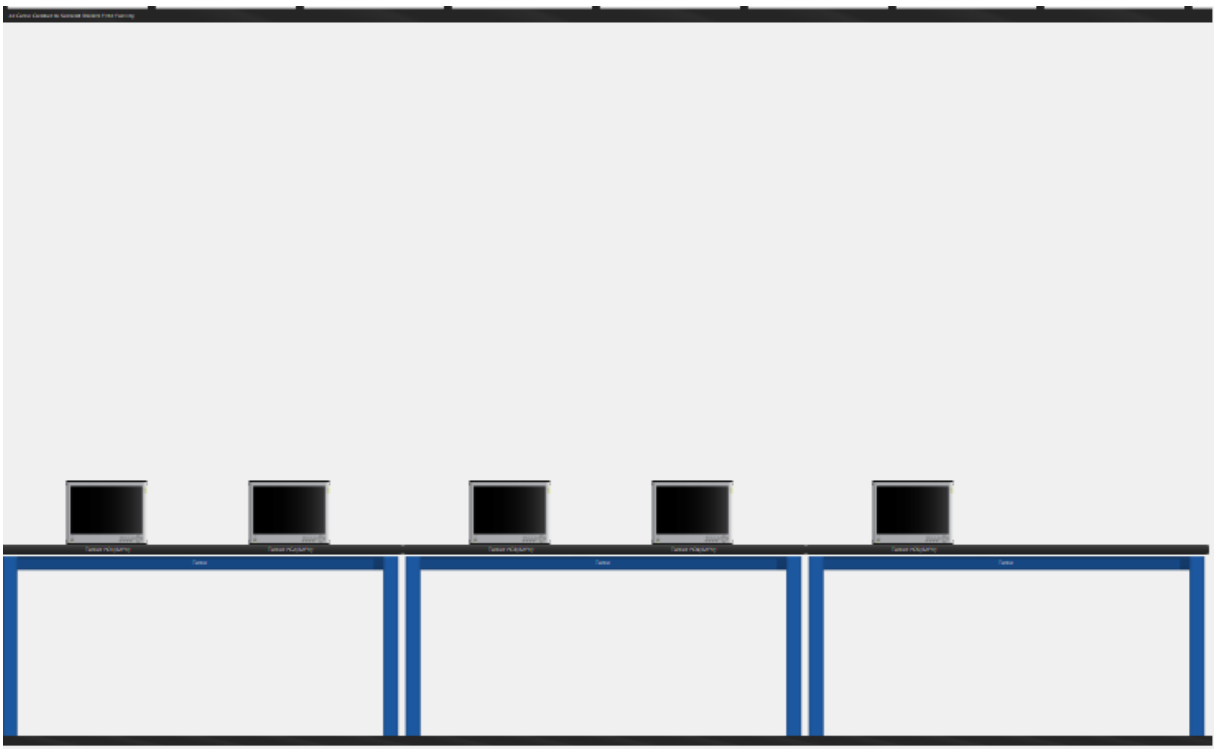


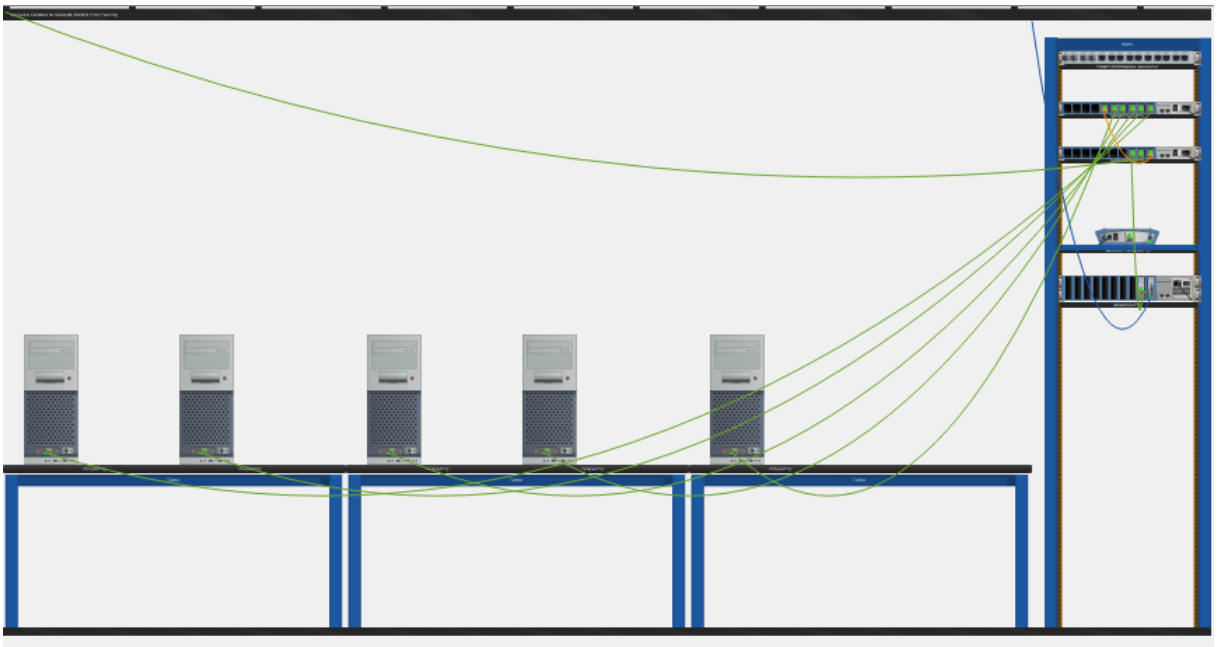
First Branch Third Facility:

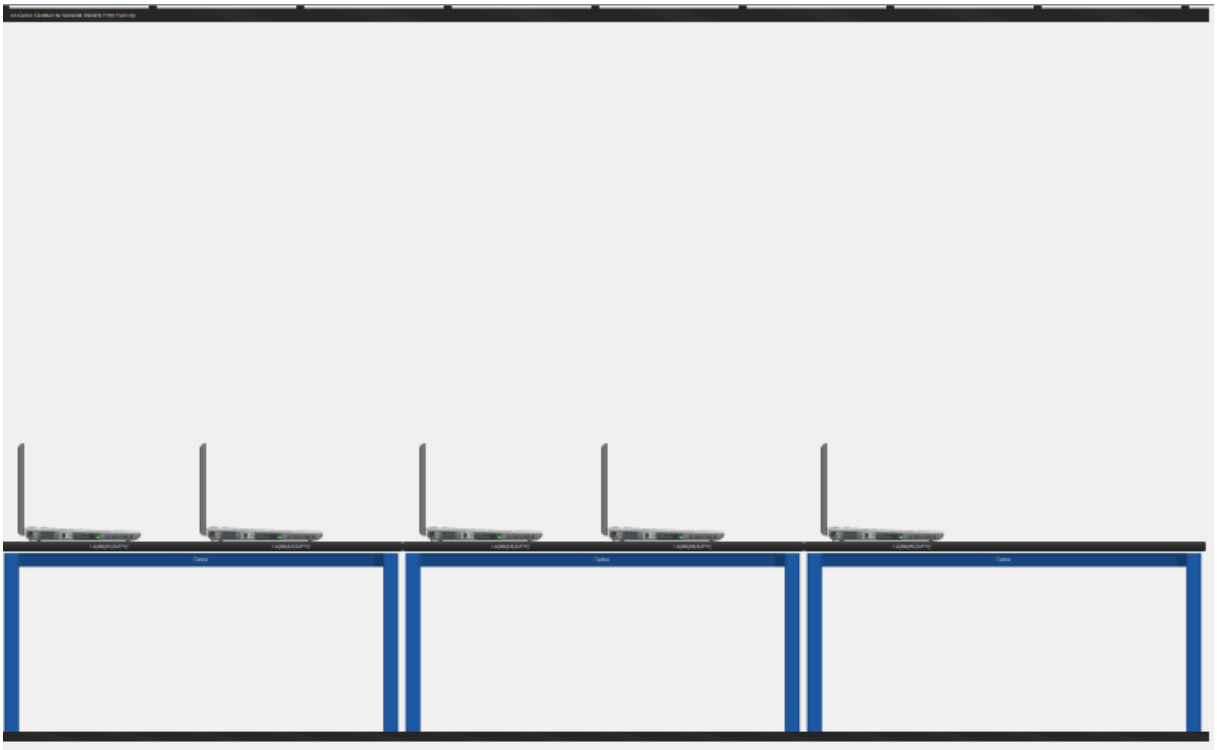


Second Branch First Facility:

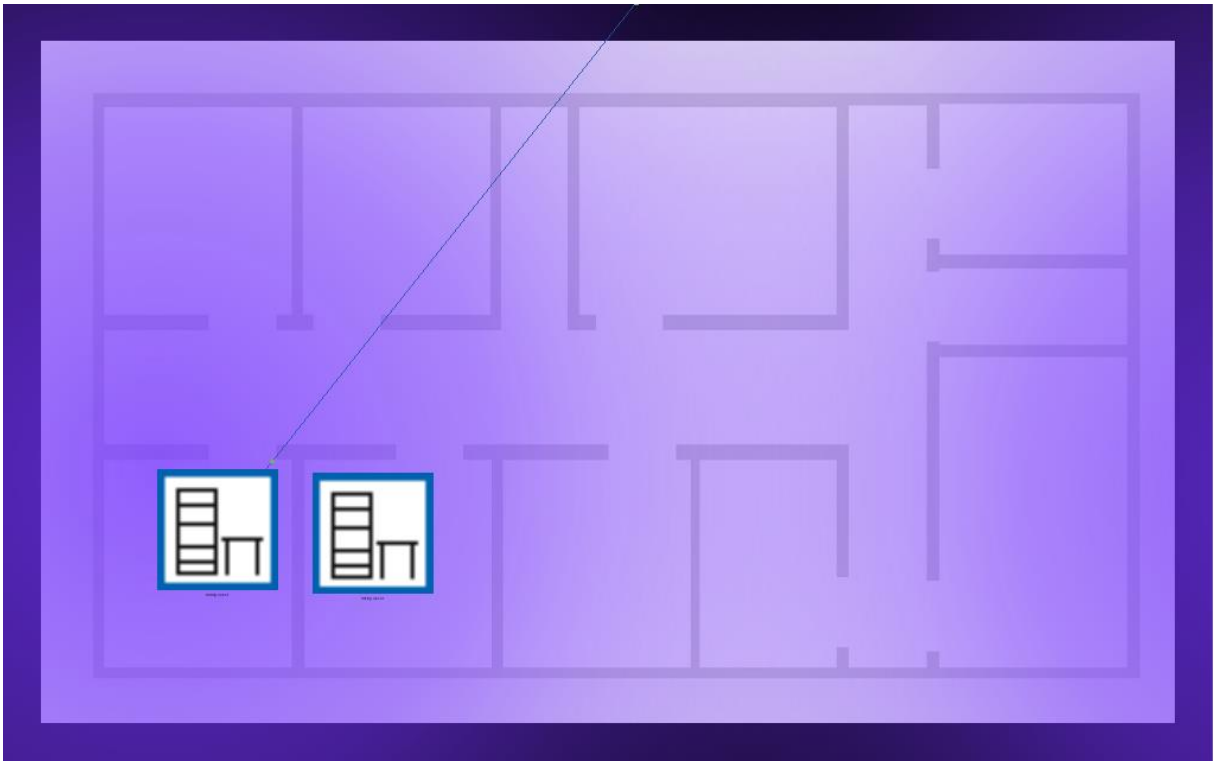


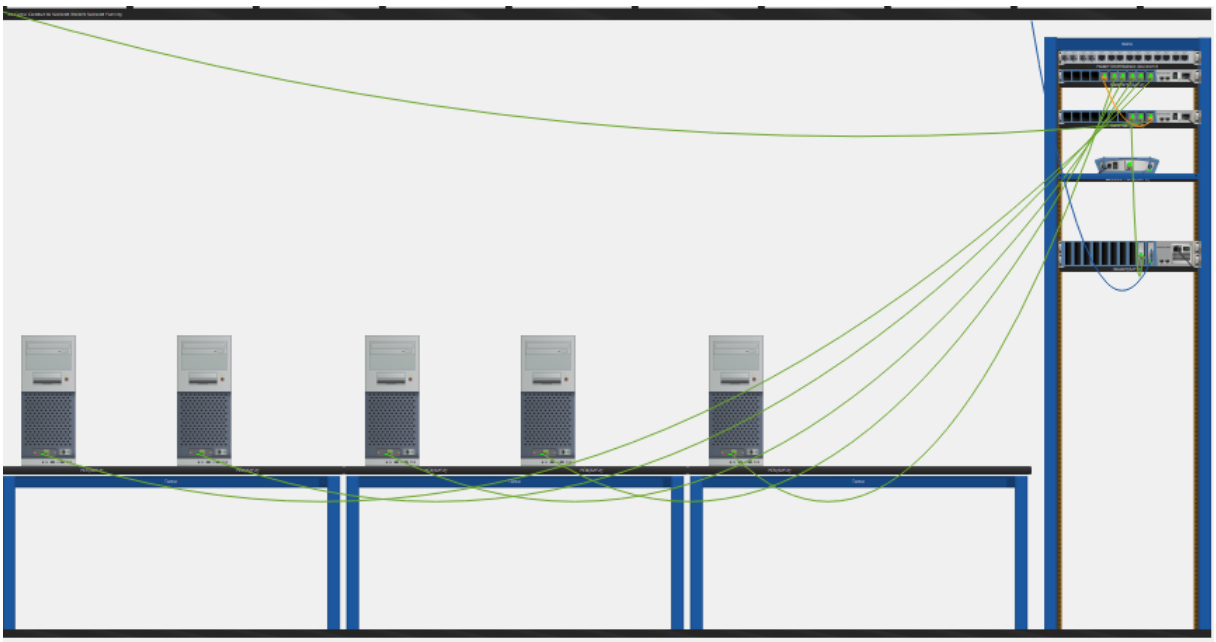


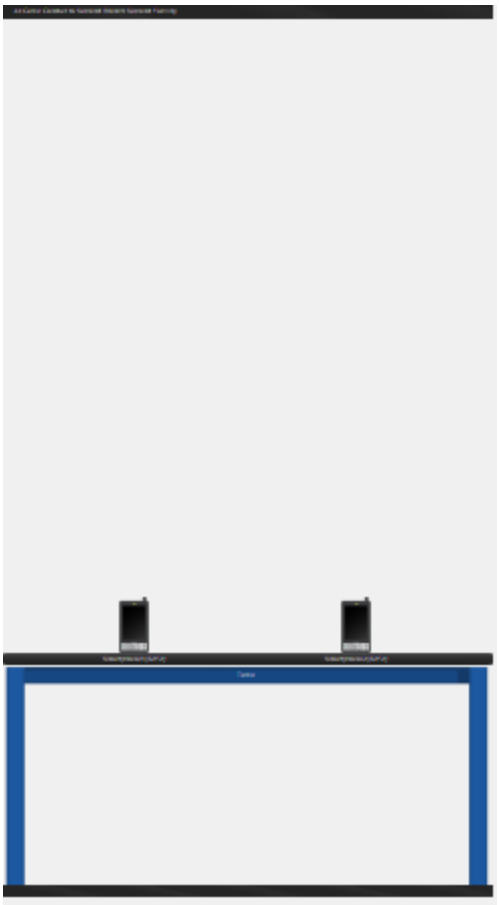




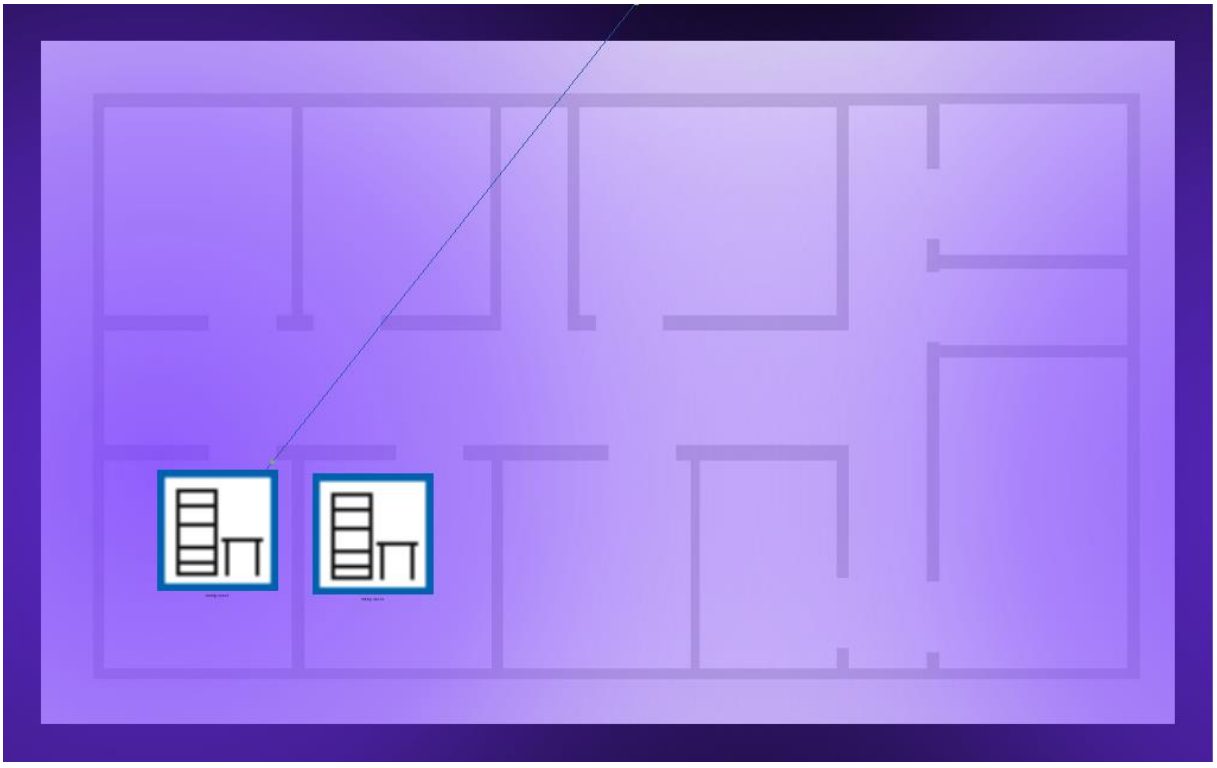
Second Branch Second Facility:

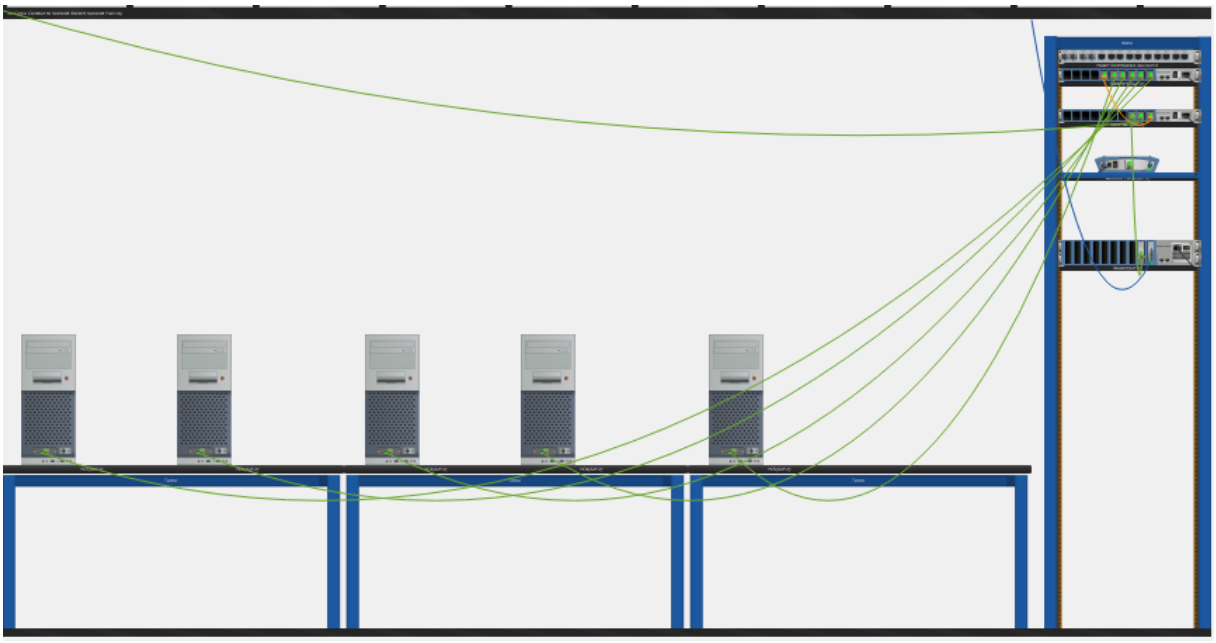


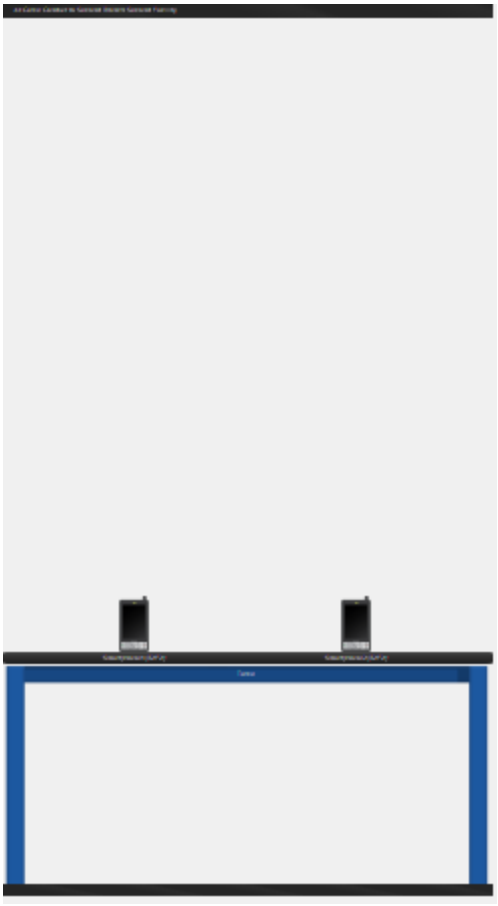




Second Branch Third Facility:

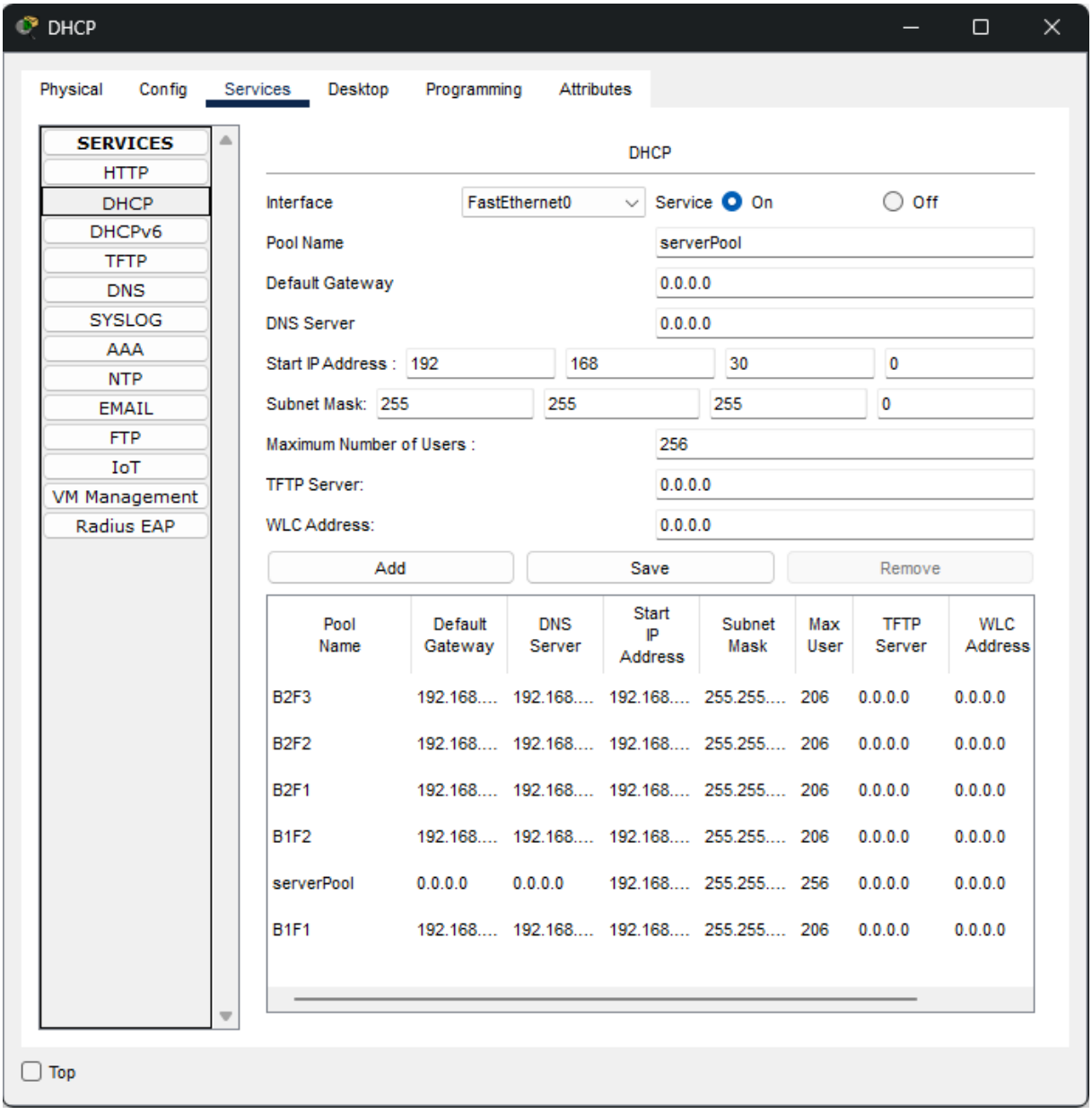




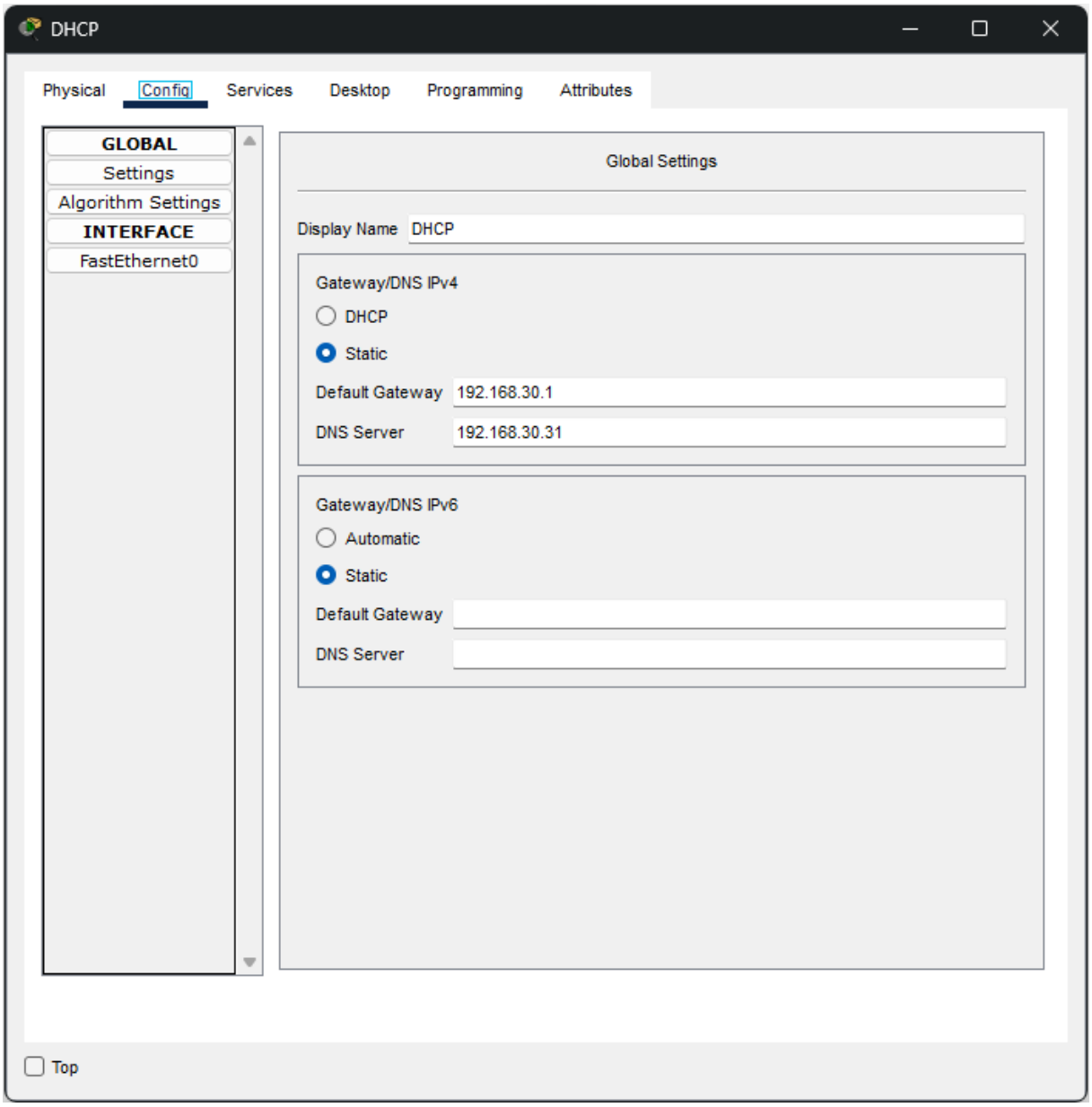


2.6. Simulation Elements

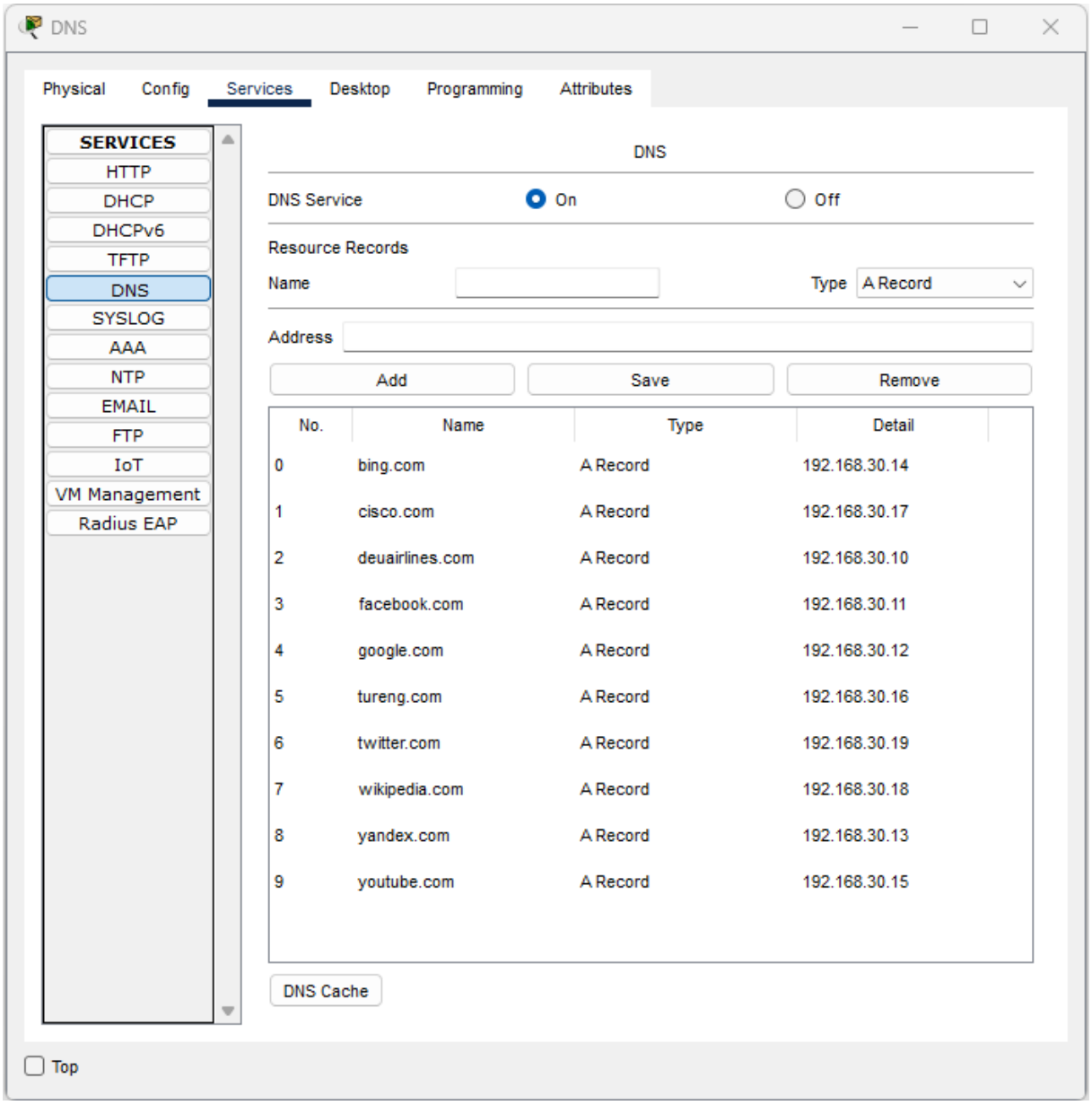
DHCP Server Services:



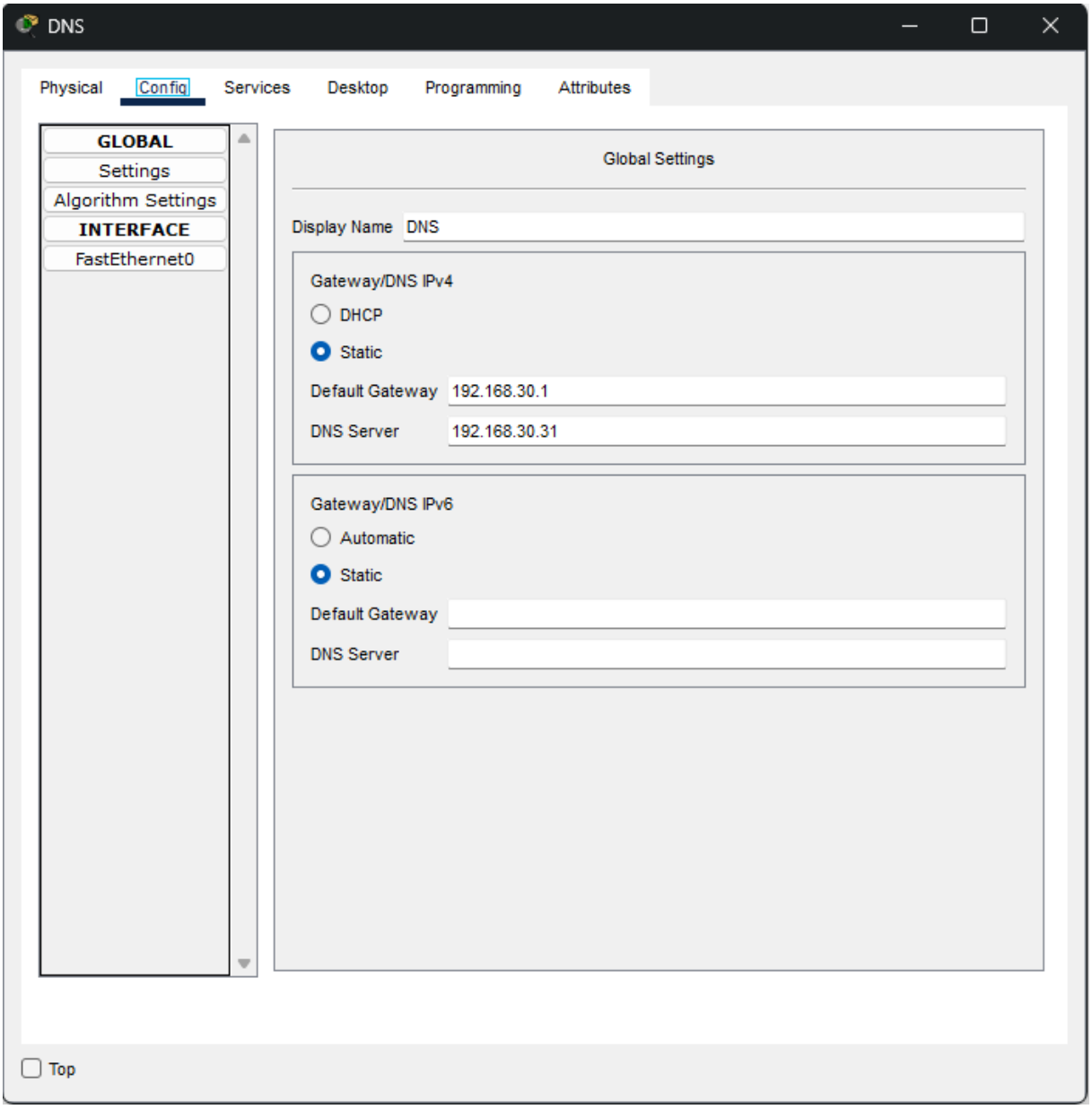
DHCP Server Config:



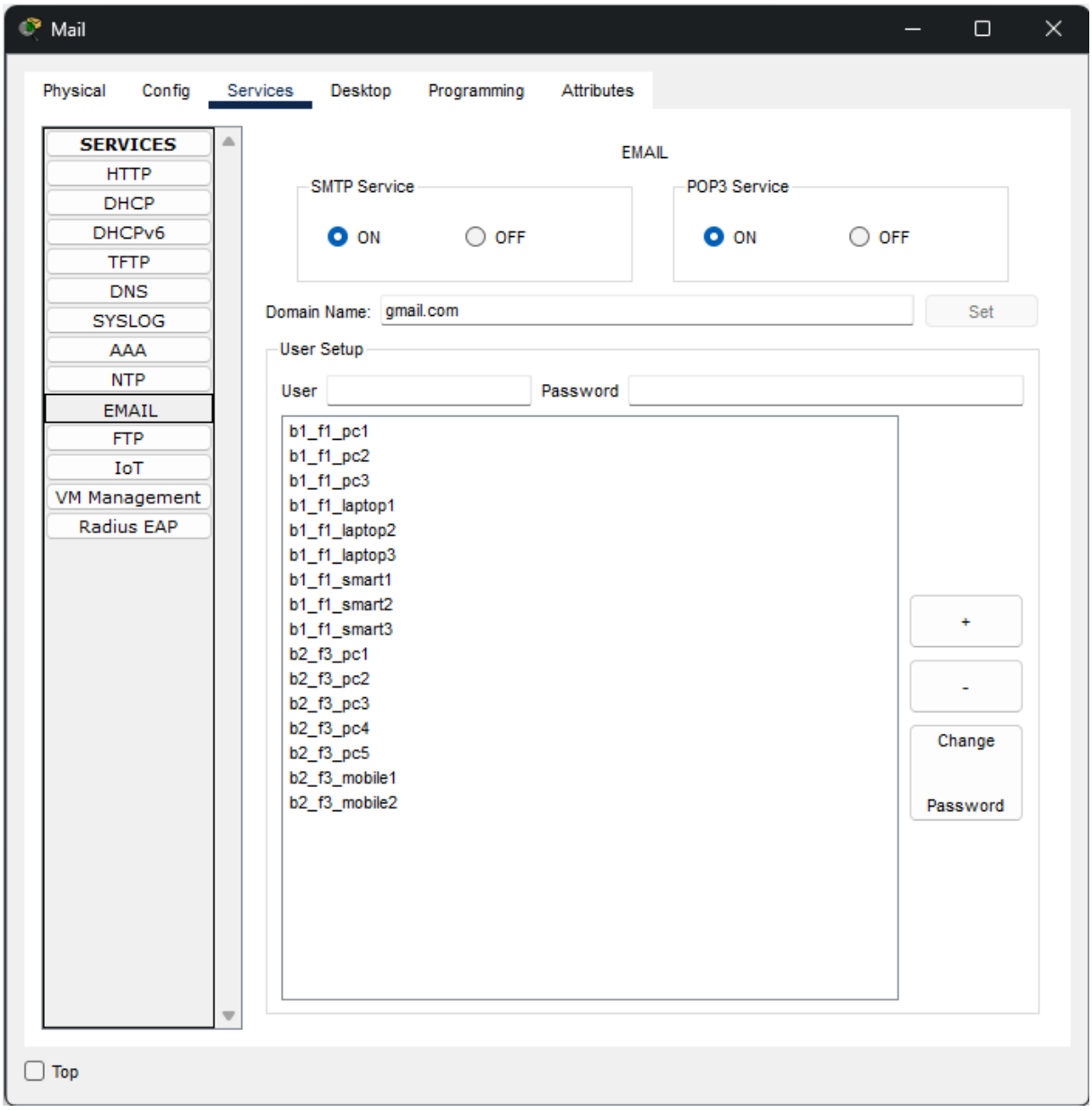
DNS Server Services:



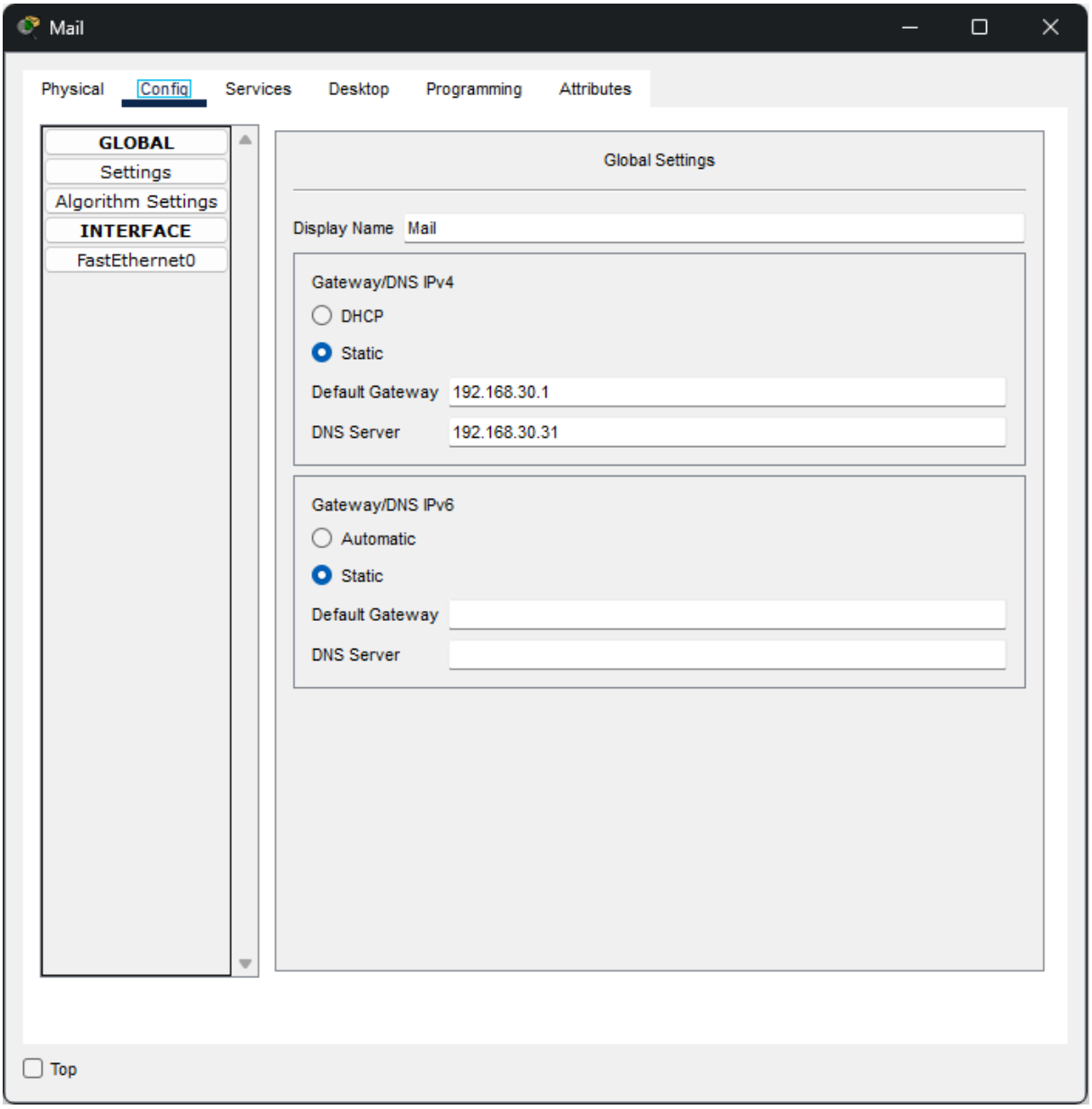
DNS Server Config:



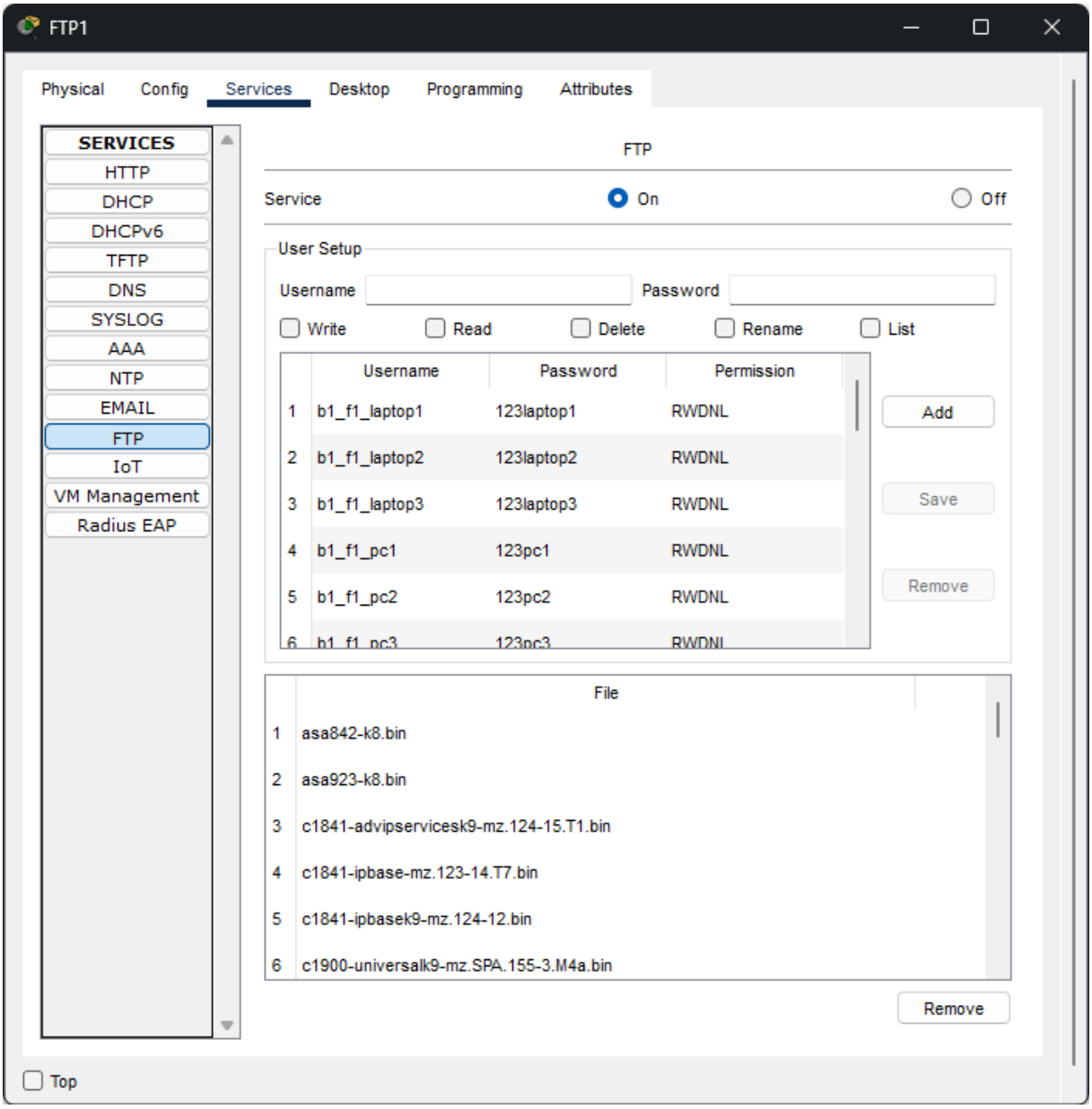
Mail Server Services:

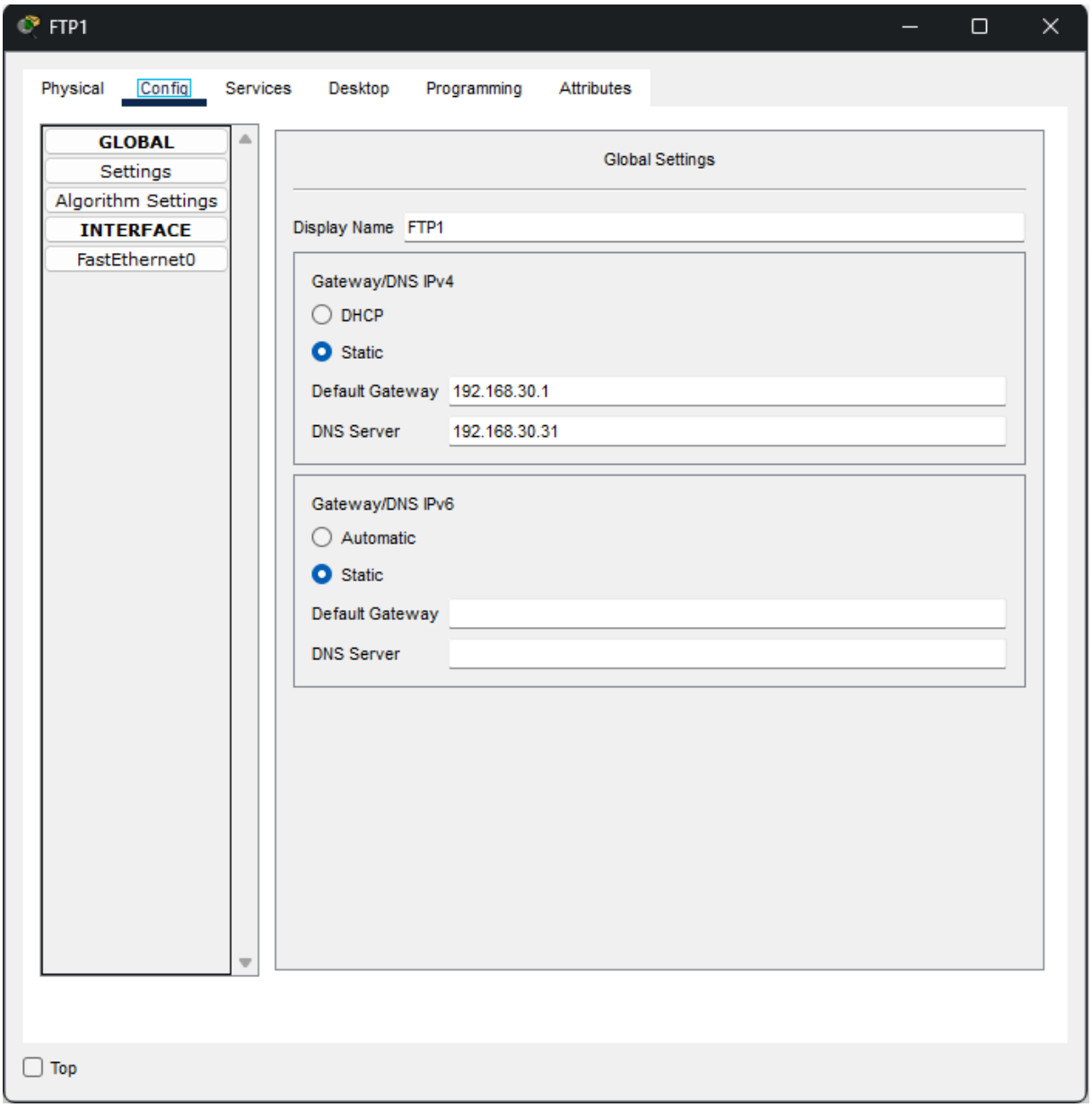


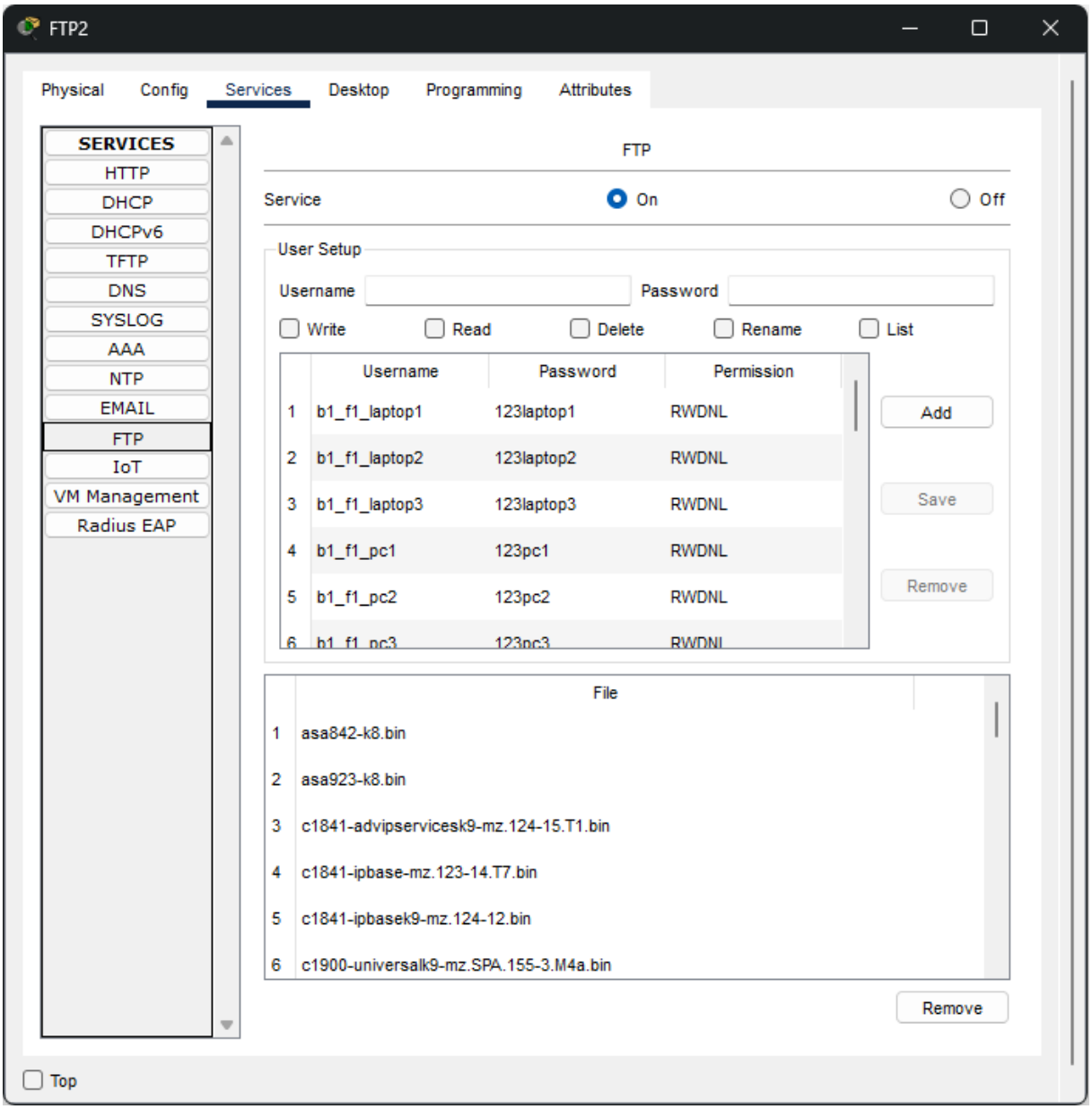
Mail Server Config:

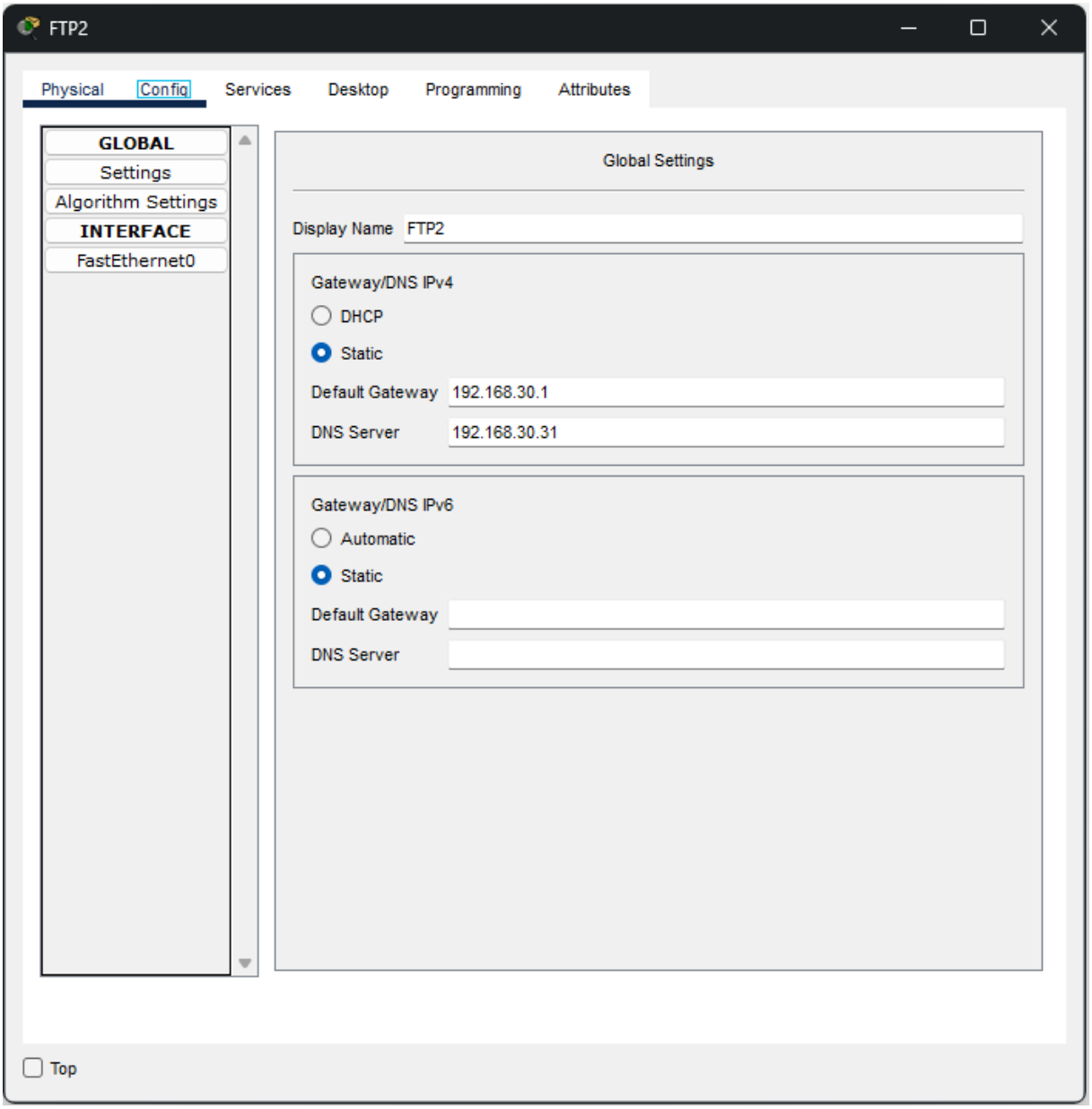


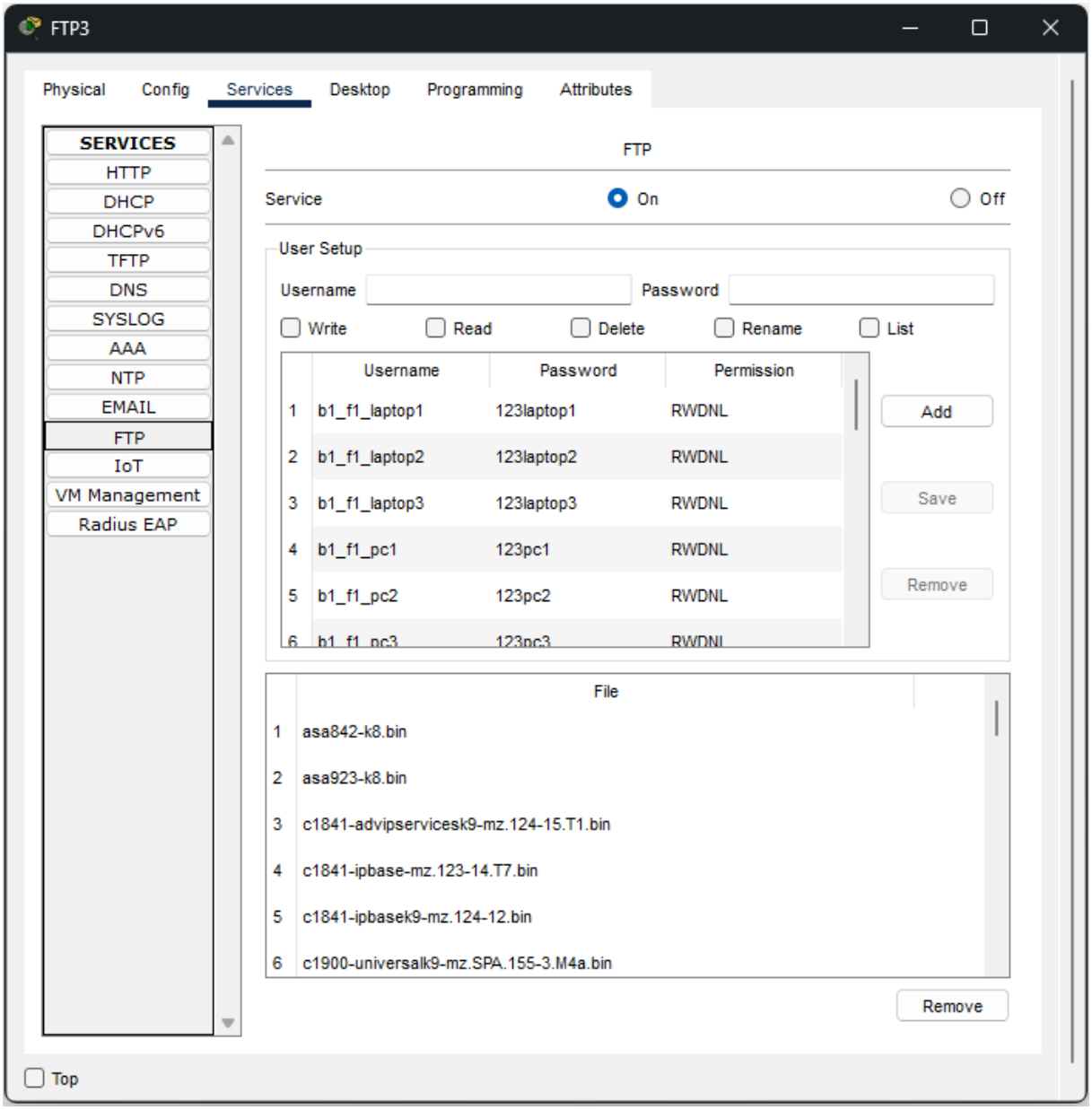
FTP Servers Services and Configs:

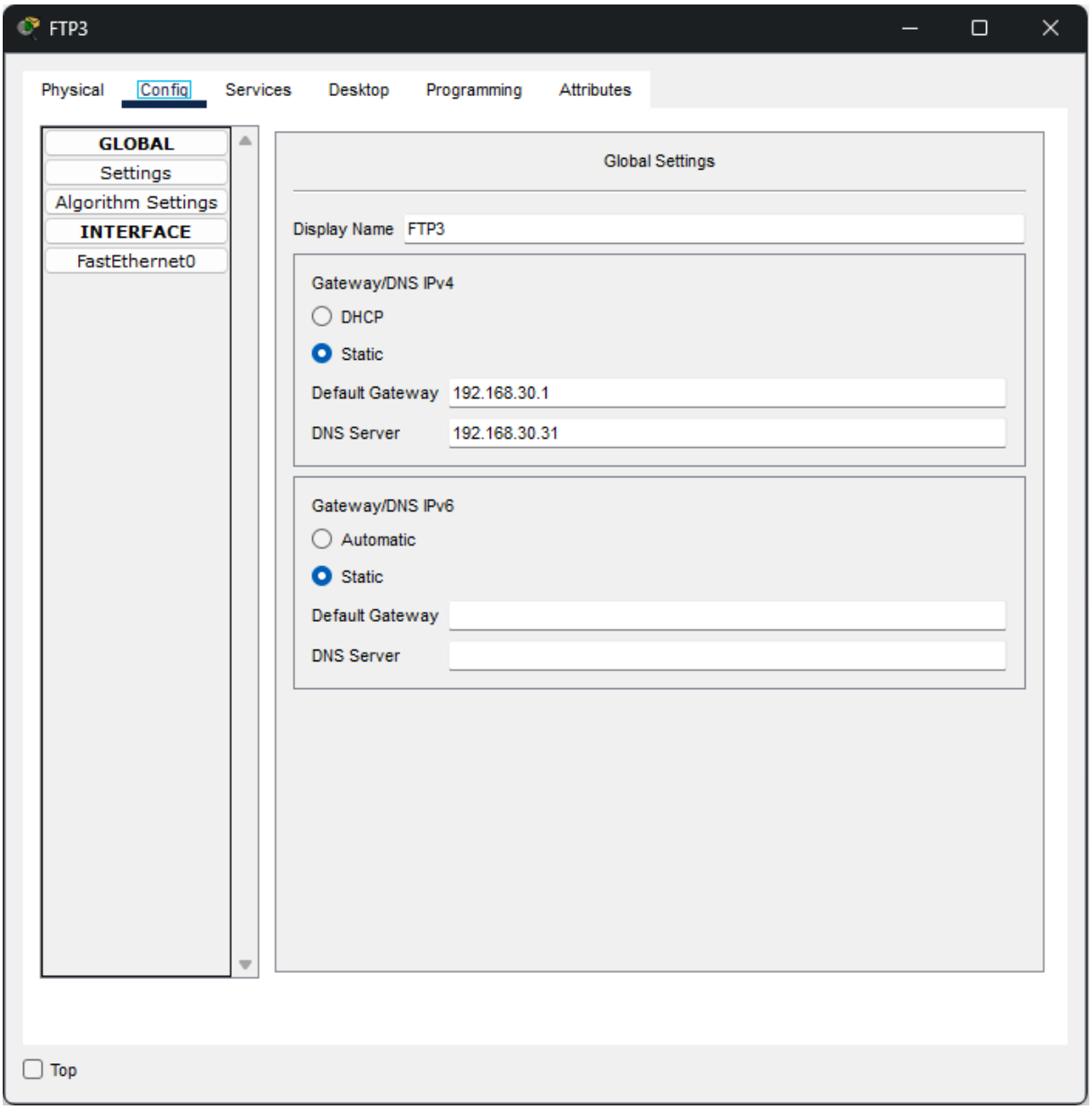


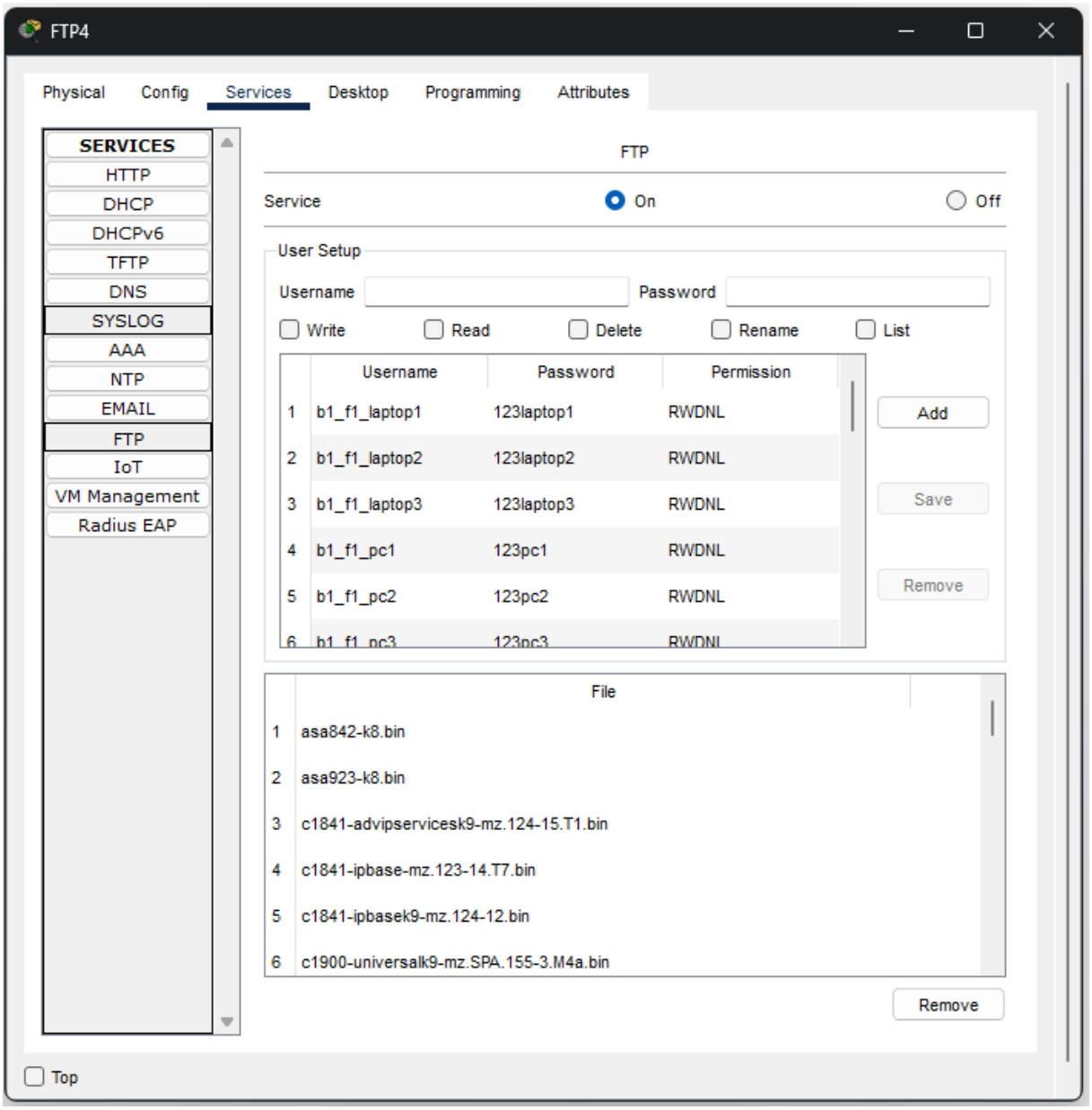

FTP1
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Global Settings
Display Name
FTP1
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.30.1
DNS Server
192.168.30.31
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

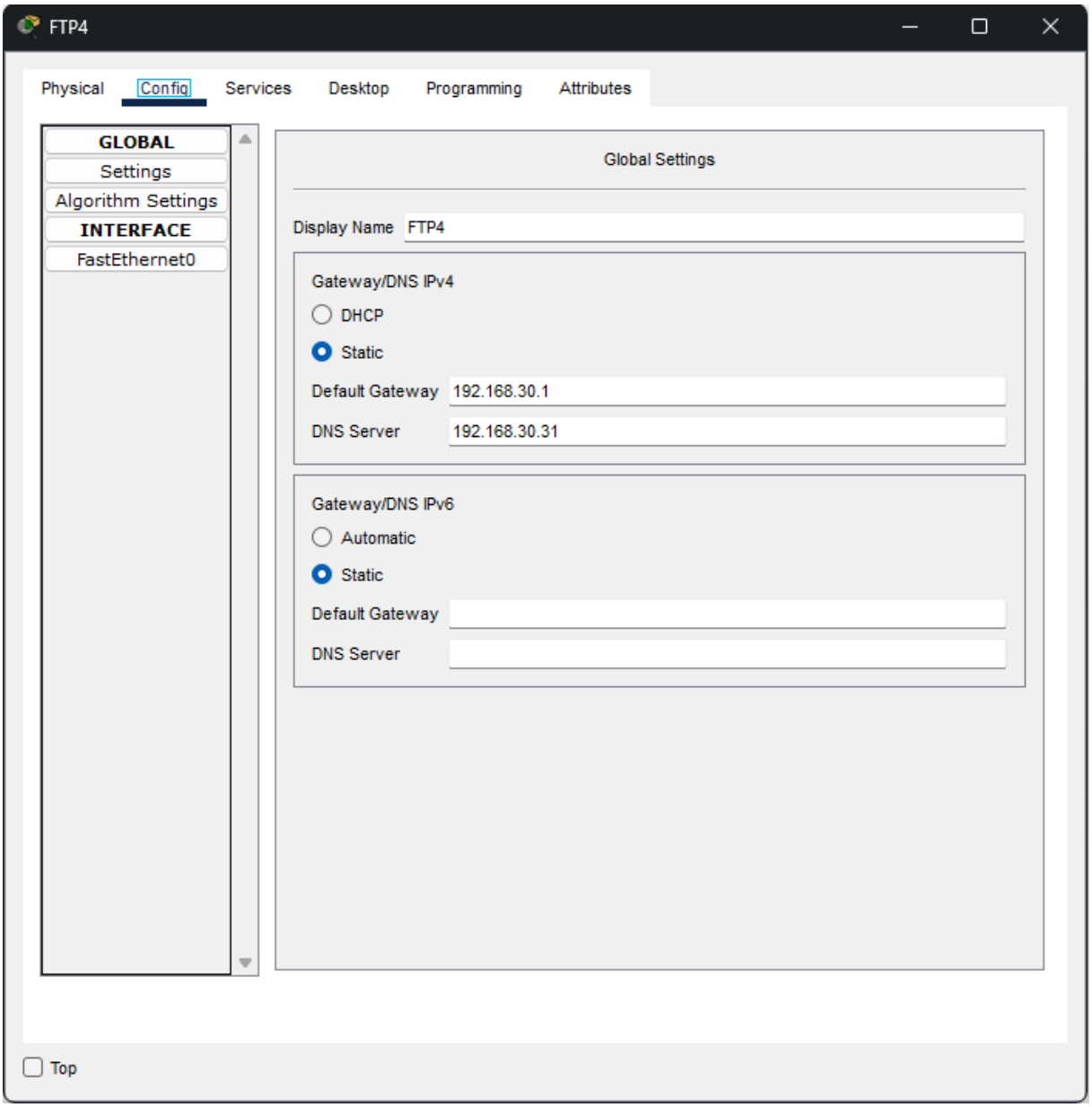

FTP2
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1 b1_f1_laptop1 123laptop1 RWDNL
2 b1_f1_laptop2 123laptop2 RWDNL
3 b1_f1_laptop3 123laptop3 RWDNL
4 b1_f1_pc1 123pc1 RWDNL
5 b1_f1_pc2 123pc2 RWDNL
6 b1_f1_pc3 123pc3 RWDNL
Add
Save
Remove
File
1 asa842-k8.bin
2 asa923-k8.bin
3 c1841-advipservicesk9-mz.124-15.T1.bin
4 c1841-ipbase-mz.123-14.T7.bin
5 c1841-ipbasek9-mz.124-12.bin
6 c1900-universalk9-mz.SPA.155-3.M4a.bin
Remove
Top


FTP2
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Global Settings
Display Name
FTP2
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.30.1
DNS Server
192.168.30.31
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

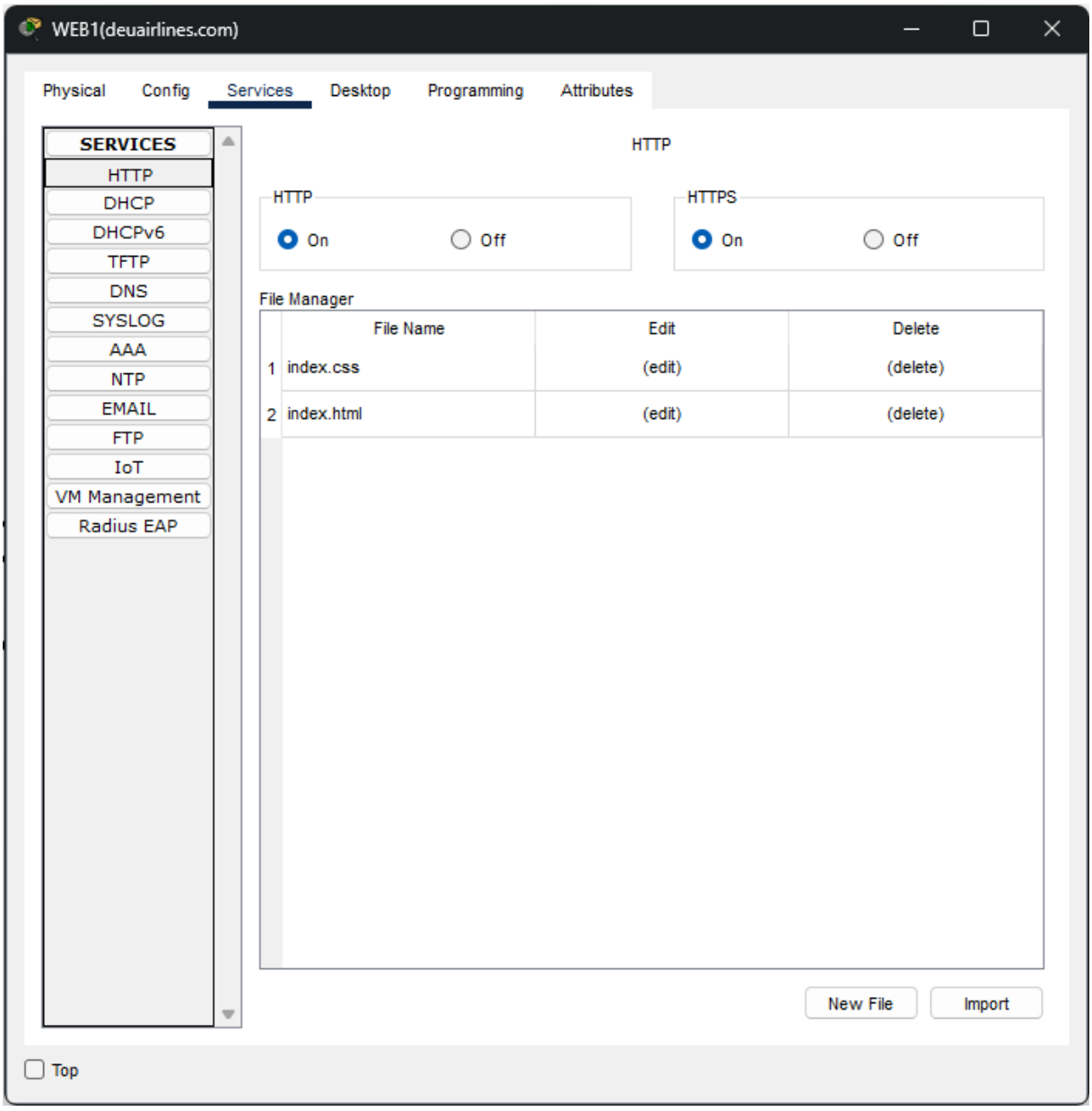

FTP3
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1 b1_f1_laptop1 123laptop1 RWDNL
2 b1_f1_laptop2 123laptop2 RWDNL
3 b1_f1_laptop3 123laptop3 RWDNL
4 b1_f1_pc1 123pc1 RWDNL
5 b1_f1_pc2 123pc2 RWDNL
Add
Save
Remove
File
1 asa842-k8.bin
2 asa923-k8.bin
3 c1841-advipservicesk9-mz.124-15.T1.bin
4 c1841-ipbase-mz.123-14.T7.bin
5 c1841-ipbasek9-mz.124-12.bin
6 c1900-universalk9-mz.SPA.155-3.M4a.bin
Remove
Top


FTP3
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Global Settings
Display Name
FTP3
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.30.1
DNS Server
192.168.30.31
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

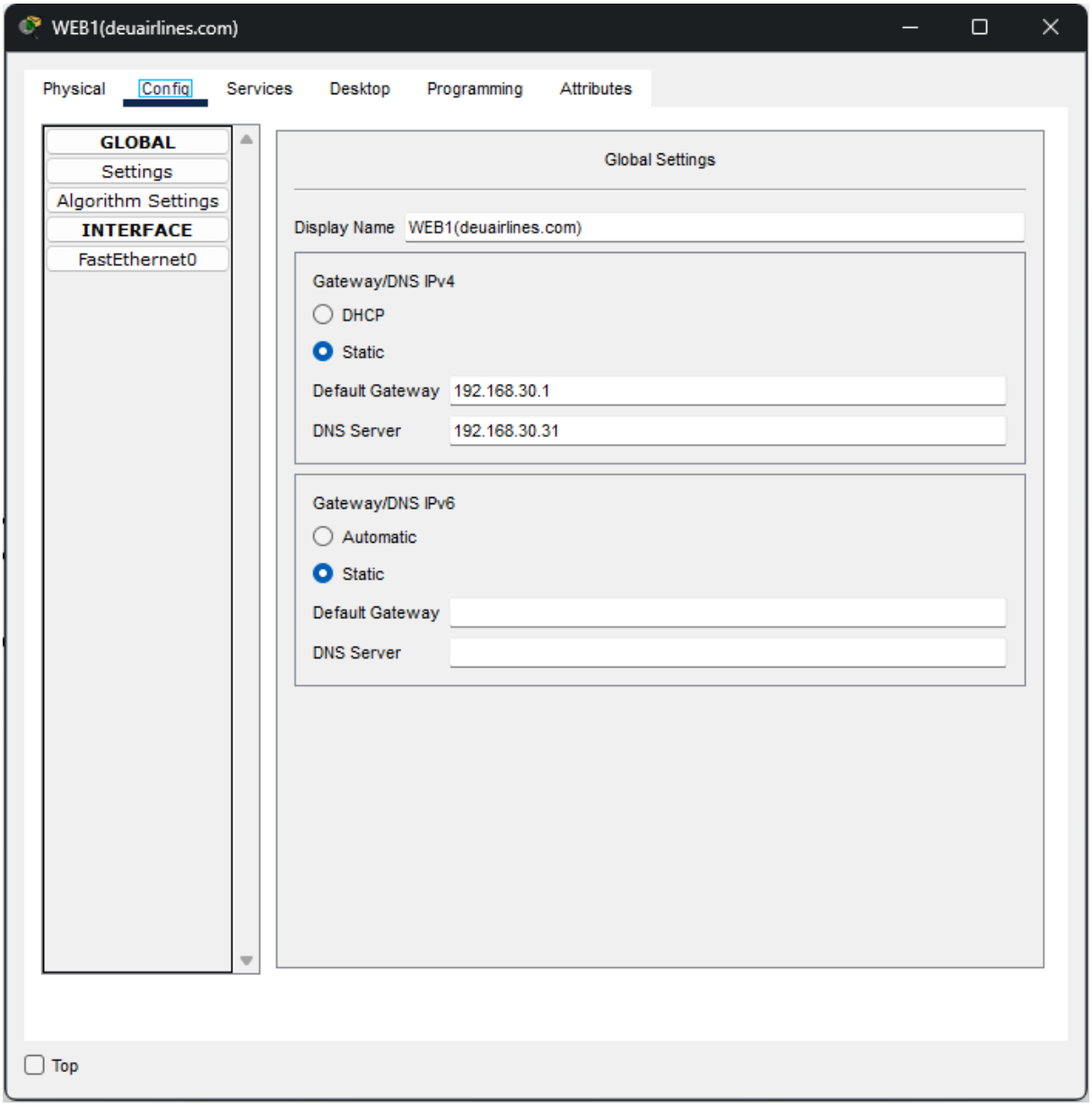

FTP4
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1 b1_f1_laptop1 123laptop1 RWDNL
2 b1_f1_laptop2 123laptop2 RWDNL
3 b1_f1_laptop3 123laptop3 RWDNL
4 b1_f1_pc1 123pc1 RWDNL
5 b1_f1_pc2 123pc2 RWDNL
Add
Save
Remove
File
1 asa842-k8.bin
2 asa923-k8.bin
3 c1841-advipservicesk9-mz.124-15.T1.bin
4 c1841-ipbase-mz.123-14.T7.bin
5 c1841-ipbasek9-mz.124-12.bin
6 c1900-universalk9-mz.SPA.155-3.M4a.bin
Remove
Top


FTP4
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Global Settings
Display Name
FTP4
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.30.1
DNS Server
192.168.30.31
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

Web Server Services:



Web Server Config:



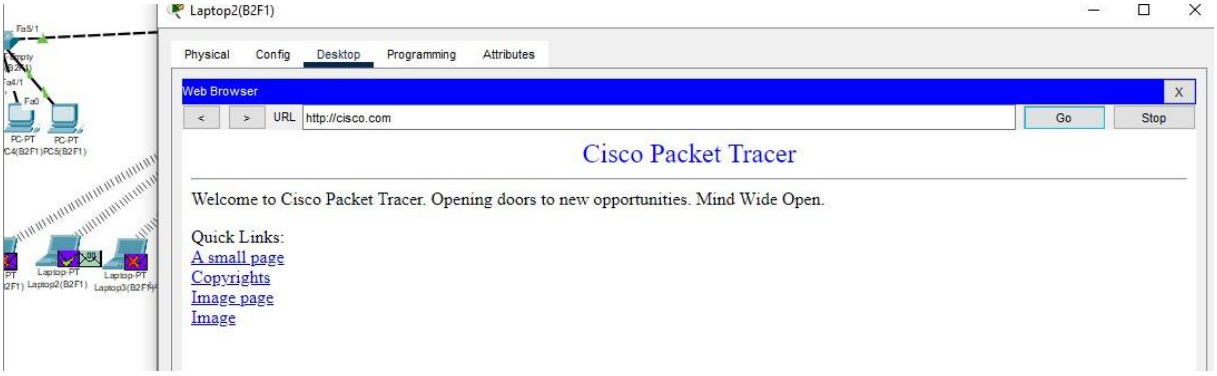
3.Traffic Analysis and Simulation Results

Simulation 1: A wireless user from first facility of second branch wants to read emails and browse Web.

WEB:

Laptop2(B2F1) at branch 2 facility 1 has used the following path to connect to the web server at branch 1 facility 3:

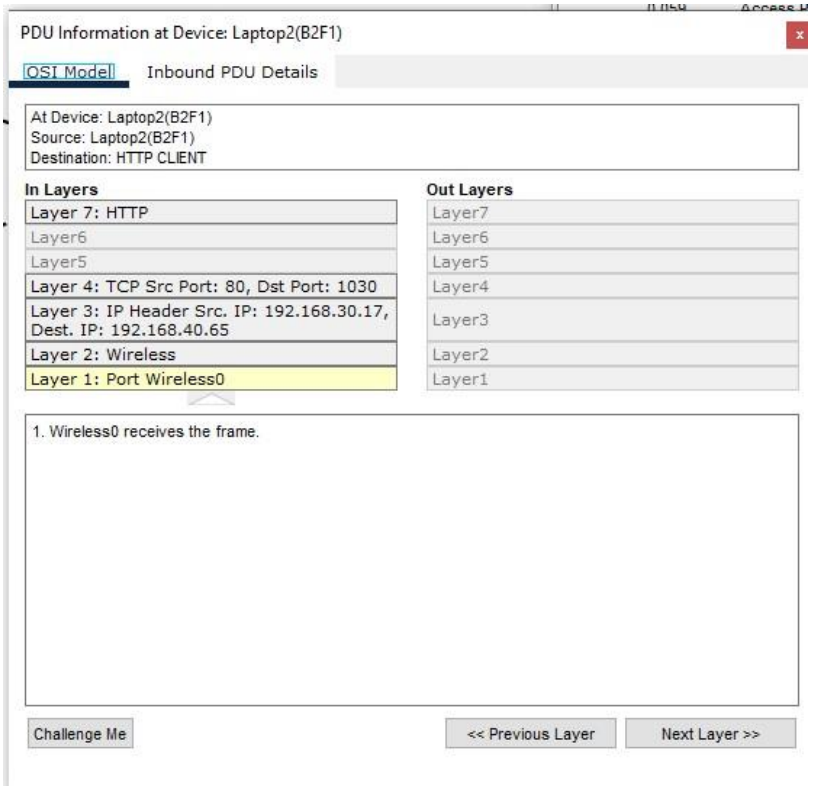
Access_Point(B2F1), SwitchAll(B2F1), Router(B2F1), RouterB2, RouterISP, RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(WebServers), Switch2(WebServers), WEB8(cisco.com).



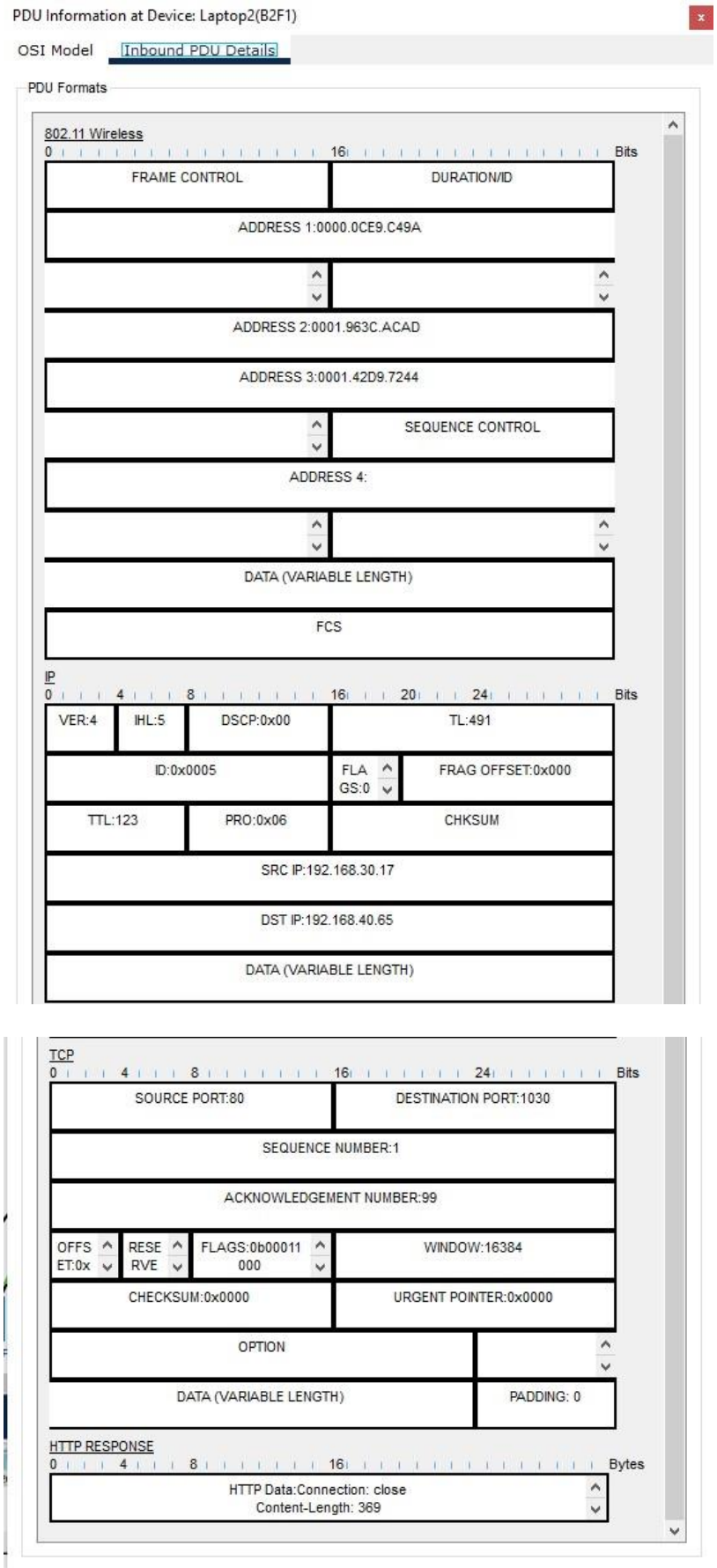
Result of Browsing WEB

	0.053	--	Laptop2(B2F1)	HTTP
	0.054	Laptop2(B2F1)	Access Point(B2F1)	HTTP
	0.054	RouterISP	RouterB1	TCP
	0.055	Access Point(B2F1)	SwitchAll(B2F1)	HTTP
	0.055	RouterB1	Router(B1F3)	TCP
	0.056	SwitchAll(B2F1)	Router(B2F1)	HTTP
	0.056	Router(B1F3)	SwitchAll(Servers)	TCP
	0.057	Router(B2F1)	RouterB2	HTTP
	0.057	SwitchAll(Servers)	SwitchAll(WEB Servers)	TCP
	0.058	RouterB2	RouterISP	HTTP
	0.058	SwitchAll(WEB Servers)	Switch2(WEB Servers)	TCP
	0.058	--	Access Point(B2F1)	HTTP
	0.059	Access Point(B2F1)	Laptop2(B2F1)	HTTP
	0.059	Access Point(B2F1)	Laptop1(B2F1)	HTTP
	0.059	Access Point(B2F1)	Laptop4(B2F1)	HTTP
	0.059	Access Point(B2F1)	Tablet PC1(B2F1)	HTTP
	0.059	Access Point(B2F1)	Laptop5(B2F1)	HTTP
	0.059	Access Point(B2F1)	Tablet PC5(B2F1)	HTTP
	0.059	Access Point(B2F1)	Tablet PC4(B2F1)	HTTP
	0.059	Access Point(B2F1)	Tablet PC3(B2F1)	HTTP
	0.059	Access Point(B2F1)	Tablet PC2(B2F1)	HTTP
	0.059	Access Point(B2F1)	Laptop3(B2F1)	HTTP
	0.059	RouterISP	RouterB1	HTTP
	0.059	Switch2(WEB Servers)	WEB8(cisco.com)	TCP
	0.059	Switch2(WEB Servers)	WEB8(cisco.com)	TCP
	0.060	RouterB1	Router(B1F3)	HTTP
	0.061	Router(B1F3)	SwitchAll(Servers)	HTTP
	0.062	SwitchAll(Servers)	SwitchAll(WEB Servers)	HTTP
	0.063	SwitchAll(WEB Servers)	Switch2(WEB Servers)	HTTP
	0.064	Switch2(WEB Servers)	WEB8(cisco.com)	HTTP
	0.065	WEB8(cisco.com)	Switch2(WEB Servers)	HTTP
	0.066	Switch2(WEB Servers)	SwitchAll(WEB Servers)	HTTP
	0.067	SwitchAll(WEB Servers)	SwitchAll(Servers)	HTTP
	0.068	SwitchAll(Servers)	Router(B1F3)	HTTP
	0.069	Router(B1F3)	RouterB1	HTTP
	0.070	RouterB1	RouterISP	HTTP
	0.071	RouterISP	RouterB2	HTTP
	0.072	RouterB2	Router(B2F1)	HTTP
	0.073	Router(B2F1)	SwitchAll(B2F1)	HTTP
	0.074	SwitchAll(B2F1)	Access Point(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Laptop2(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Laptop1(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Laptop3(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Laptop4(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Tablet PC1(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Laptop5(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Tablet PC5(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Tablet PC4(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Tablet PC3(B2F1)	HTTP
Visible	0.075	Access Point(B2F1)	Tablet PC2(B2F1)	HTTP

Event List for Browsing WEB



OSI Model of the last packet that is sent to Laptop

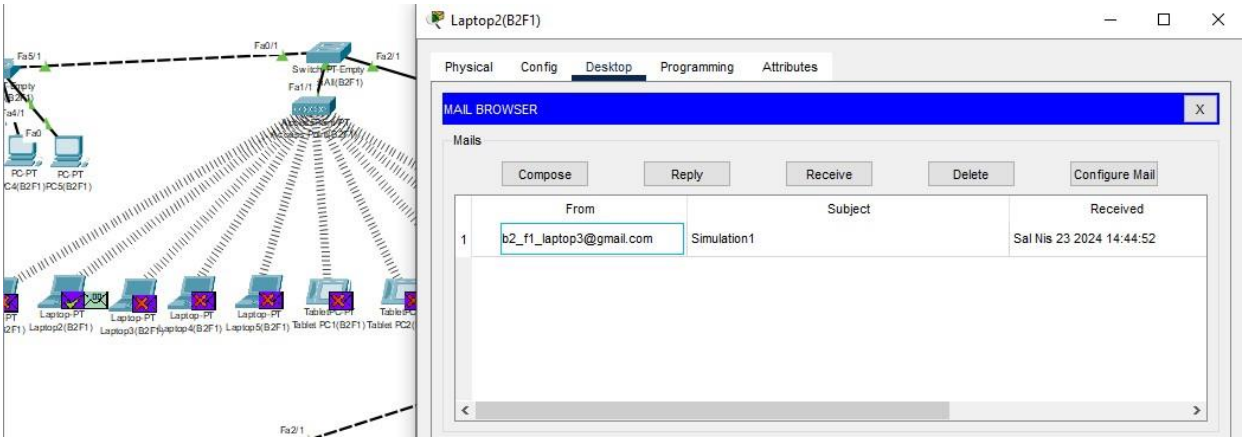


Inbound PDU Details of the Last Packet That is Sent to Laptop

MAIL:

Laptop2(B2F1) at branch 2 facility 1 has used the following path to receive an email from the mail server at branch 1 facility 3:

Access_Point(B2F1), SwitchAll(B2F1), Router(B2F1), RouterB2, RouterISP, RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(OtherServers), MailServer.



Result of Receiving E-mail

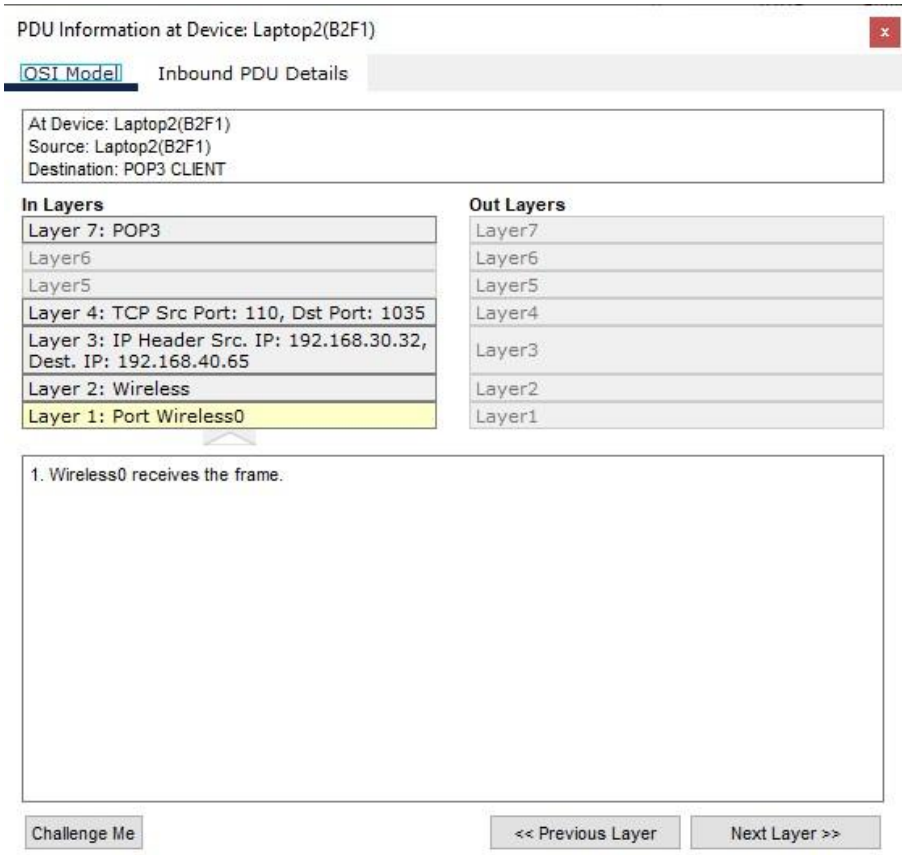
Simulation Panel

Event List

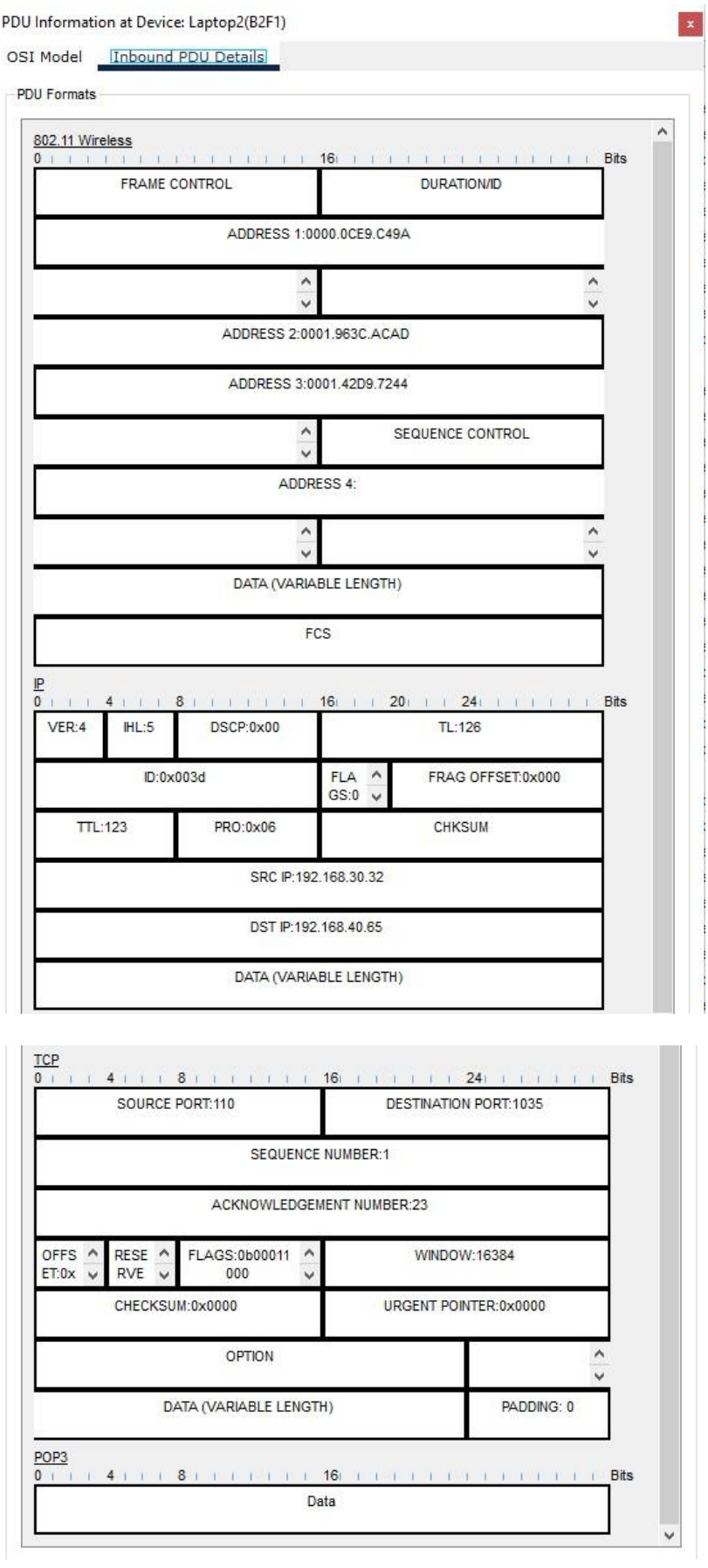
Vis.	Time(sec)	Last Device	At Device	Type
	0.024	--	Laptop2(B2F1)	POP3
	0.025	Laptop2(B2F1)	Access Point(B2F1)	POP3
	0.025	Router(B2F1)	RouterB2	TCP
	0.026	Access Point(B2F1)	SwitchAll(B2F1)	POP3
	0.026	RouterB2	RouterISP	TCP
	0.026	--	Access Point(B2F1)	TCP
	0.027	Access Point(B2F1)	Laptop2(B2F1)	TCP
	0.027	Access Point(B2F1)	Laptop1(B2F1)	TCP
	0.027	Access Point(B2F1)	Laptop4(B2F1)	TCP
	0.027	Access Point(B2F1)	Tablet PC1(B2F1)	TCP
	0.027	Access Point(B2F1)	Laptop5(B2F1)	TCP
	0.027	Access Point(B2F1)	Tablet PC5(B2F1)	TCP
	0.027	Access Point(B2F1)	Tablet PC4(B2F1)	TCP
	0.027	Access Point(B2F1)	Tablet PC3(B2F1)	TCP
	0.027	Access Point(B2F1)	Tablet PC2(B2F1)	TCP
	0.027	Access Point(B2F1)	Laptop3(B2F1)	TCP
	0.027	SwitchAll(B2F1)	Router(B2F1)	POP3
	0.027	RouterISP	RouterB1	TCP
	0.028	Router(B2F1)	RouterB2	POP3
	0.028	RouterB1	Router(B1F3)	TCP
	0.029	RouterB2	RouterISP	POP3
	0.029	Router(B1F3)	SwitchAll(Servers)	TCP
	0.030	RouterISP	RouterB1	POP3
	0.030	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.030	--	Access Point(B2F1)	POP3
	0.031	Access Point(B2F1)	Laptop2(B2F1)	POP3
	0.031	Access Point(B2F1)	Laptop1(B2F1)	POP3
	0.031	Access Point(B2F1)	Laptop4(B2F1)	POP3
	0.031	Access Point(B2F1)	Tablet PC1(B2F1)	POP3
	0.031	Access Point(B2F1)	Laptop5(B2F1)	POP3
	0.031	Access Point(B2F1)	Tablet PC5(B2F1)	POP3
	0.031	Access Point(B2F1)	Tablet PC4(B2F1)	POP3
	0.031	Access Point(B2F1)	Tablet PC3(B2F1)	POP3
	0.031	Access Point(B2F1)	Tablet PC2(B2F1)	POP3
	0.031	Access Point(B2F1)	Laptop3(B2F1)	POP3
	0.031	RouterB1	Router(B1F3)	POP3
	0.031	SwitchAll(Other Servers)	Mail	TCP
	0.032	Router(B1F3)	SwitchAll(Servers)	POP3
	0.033	SwitchAll(Servers)	SwitchAll(Other Servers)	POP3
	0.034	SwitchAll(Other Servers)	Mail	POP3
	0.035	Mail	SwitchAll(Other Servers)	POP3
	0.036	SwitchAll(Other Servers)	SwitchAll(Servers)	POP3
	0.037	SwitchAll(Servers)	Router(B1F3)	POP3
	0.038	Router(B1F3)	RouterB1	POP3
	0.039	RouterB1	RouterISP	POP3
	0.040	RouterISP	RouterB2	POP3
	0.040	RouterISP	RouterB2	POP3
	0.041	RouterB2	Router(B2F1)	POP3
	0.042	Router(B2F1)	SwitchAll(B2F1)	POP3
	0.043	SwitchAll(B2F1)	Access Point(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Laptop2(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Laptop1(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Laptop3(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Laptop4(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Tablet PC1(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Laptop5(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Tablet PC5(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Tablet PC4(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Tablet PC3(B2F1)	POP3
Visible	0.044	Access Point(B2F1)	Tablet PC2(B2F1)	POP3
Visible	0.044	--	Laptop2(B2F1)	TCP

Reset Simulation | Constant Delay | Captured to: 0.044 s

Event List of Receiving E-mail



OSI Model of the last packet that is sent to Laptop

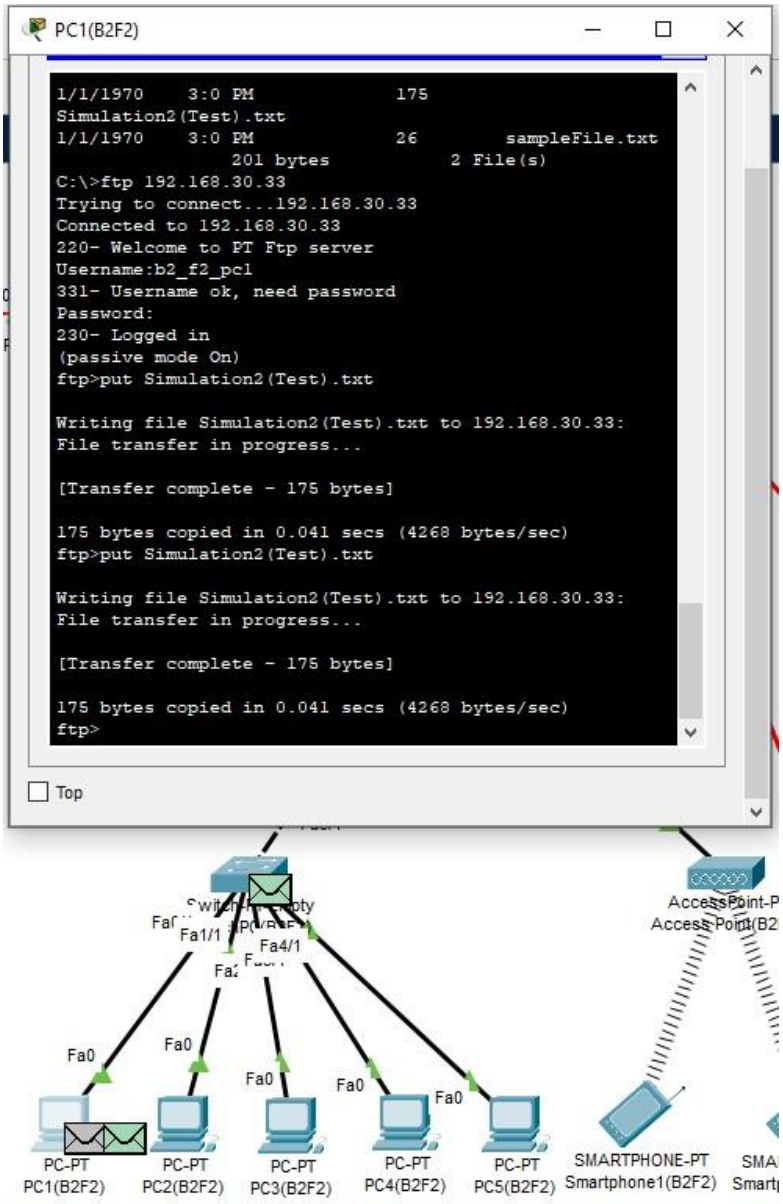


Inbound PDU Details of the Last Packet That is Sent to Laptop

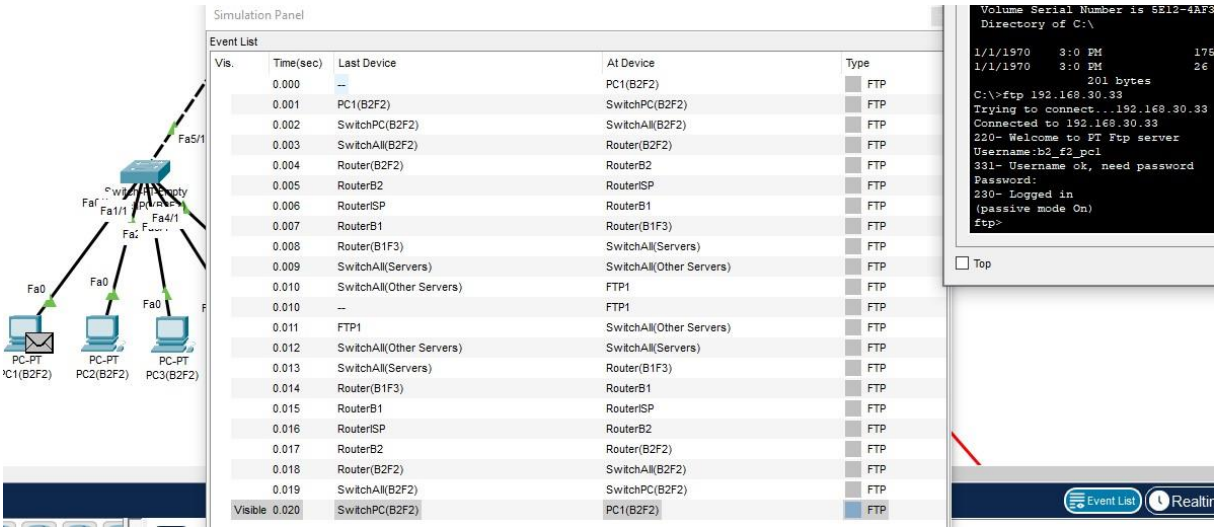
Simulation 2: A computer engineer from second facility of second branch developed a web application and wants to send his/her code files to FTP server in the third facility of first branch.

PC1(B2F2) at branch 2 facility 2 has used the following path to send a txt file to the FTP Server at branch 1 facility 3:

PC1(B2F2), SwitchPC(B2F2), SwitchAll(B2F2), Router(B2F2), RouterB2, RouterISP, RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(OtherServers), FTP1



Result of transferring a file to the FTP server



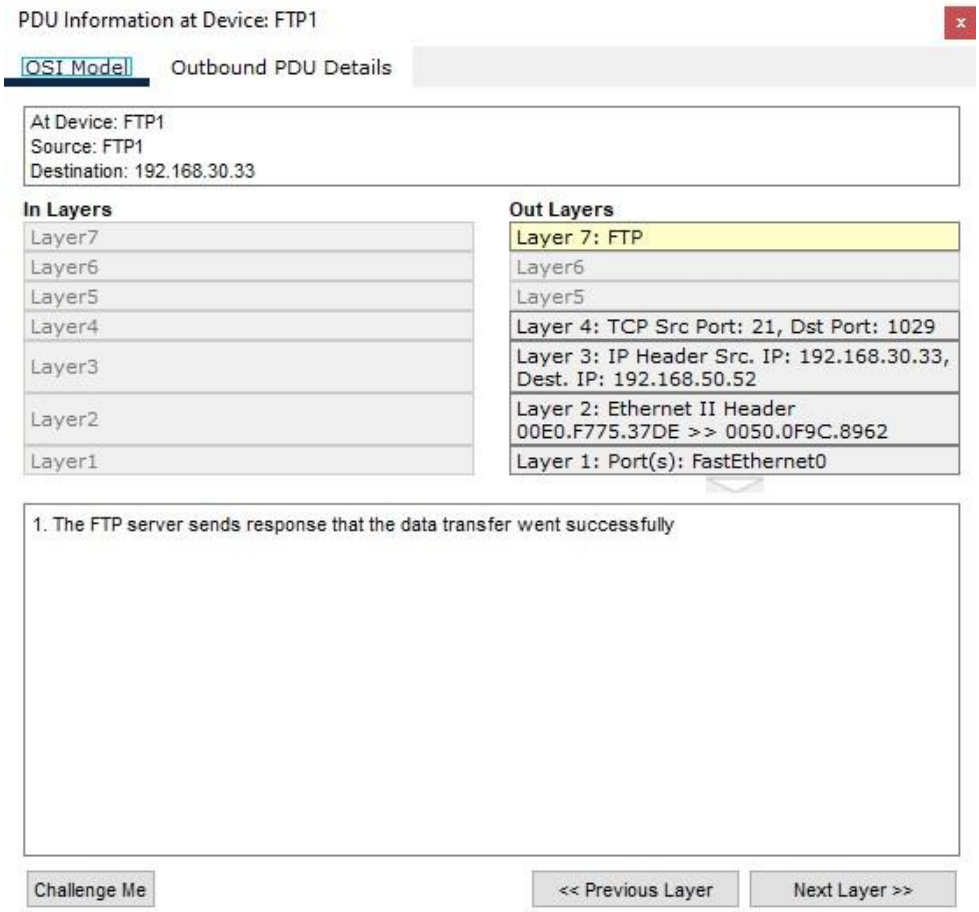
Password accepted message to PC

Simulation Panel

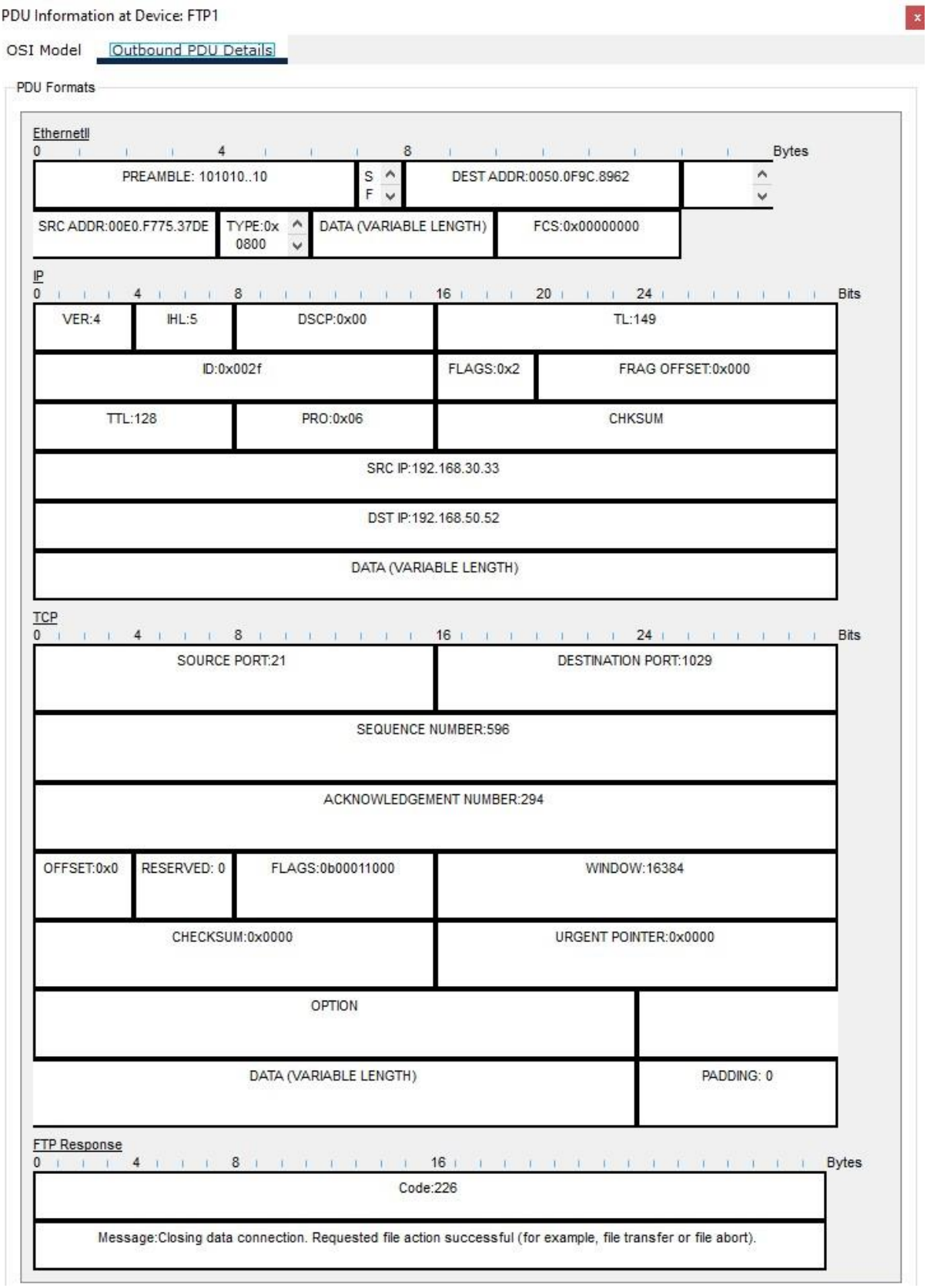
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.081	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.081	PC1(B2F2)	SwitchPC(B2F2)	TCP
	0.081	--	PC1(B2F2)	FTP
	0.082	PC1(B2F2)	SwitchPC(B2F2)	FTP
	0.082	SwitchAll(Other Servers)	FTP1	TCP
	0.082	SwitchPC(B2F2)	SwitchAll(B2F2)	TCP
	0.083	SwitchPC(B2F2)	SwitchAll(B2F2)	FTP
	0.083	SwitchAll(B2F2)	Router(B2F2)	TCP
	0.084	SwitchAll(B2F2)	Router(B2F2)	FTP
	0.084	Router(B2F2)	RouterB2	TCP
	0.085	Router(B2F2)	RouterB2	FTP
	0.085	RouterB2	RouterISP	TCP
	0.086	RouterB2	RouterISP	FTP
	0.086	RouterISP	RouterB1	TCP
	0.087	RouterISP	RouterB1	FTP
	0.087	RouterB1	Router(B1F3)	TCP
	0.088	RouterB1	Router(B1F3)	FTP
	0.088	Router(B1F3)	SwitchAll(Servers)	TCP
	0.089	Router(B1F3)	SwitchAll(Servers)	FTP
	0.089	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.090	SwitchAll(Servers)	SwitchAll(Other Servers)	FTP
	0.090	SwitchAll(Other Servers)	FTP1	TCP
	0.091	SwitchAll(Other Servers)	FTP1	FTP
	0.091	--	FTP1	FTP
	0.091	--	FTP1	TCP
	0.092	FTP1	SwitchAll(Other Servers)	FTP
	0.092	--	FTP1	TCP
	0.093	FTP1	SwitchAll(Other Servers)	TCP
	0.093	SwitchAll(Other Servers)	SwitchAll(Servers)	FTP
	0.094	SwitchAll(Other Servers)	SwitchAll(Servers)	TCP
	0.094	SwitchAll(Servers)	Router(B1F3)	FTP
	0.095	SwitchAll(Servers)	Router(B1F3)	TCP
	0.095	Router(B1F3)	RouterB1	FTP
	0.096	Router(B1F3)	RouterB1	TCP
	0.096	RouterB1	RouterISP	FTP
	0.097	RouterB1	RouterISP	TCP
	0.097	RouterISP	RouterB2	FTP
	0.098	RouterISP	RouterB2	TCP
	0.098	RouterB2	Router(B2F2)	FTP
	0.099	RouterB2	Router(B2F2)	TCP
	0.099	Router(B2F2)	SwitchAll(B2F2)	FTP
	0.100	Router(B2F2)	SwitchAll(B2F2)	TCP
	0.100	SwitchAll(B2F2)	SwitchPC(B2F2)	FTP
Visible	0.101	SwitchAll(B2F2)	SwitchPC(B2F2)	TCP
Visible	0.101	SwitchPC(B2F2)	PC1(B2F2)	FTP
Visible	0.101	--	PC1(B2F2)	TCP

Event List of Transfering a File to the FTP System



OSI Model of the last packet that is sent to PC1

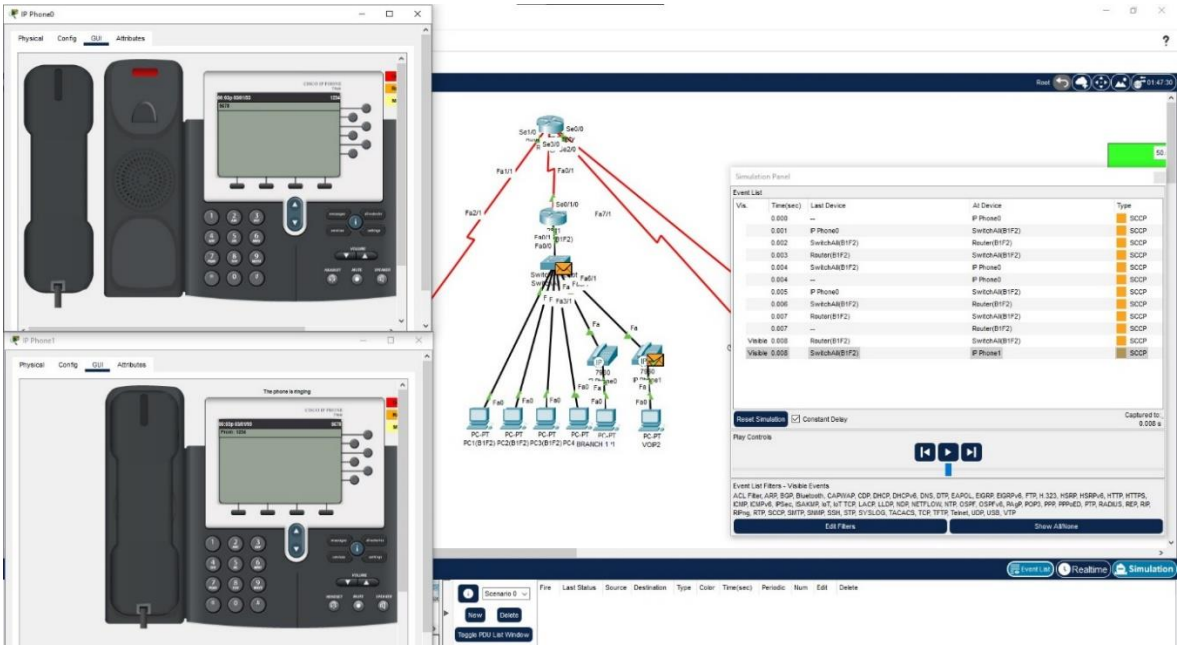


Outbound PDU Details of the Last Packet That is Sent to PC1 by FTP

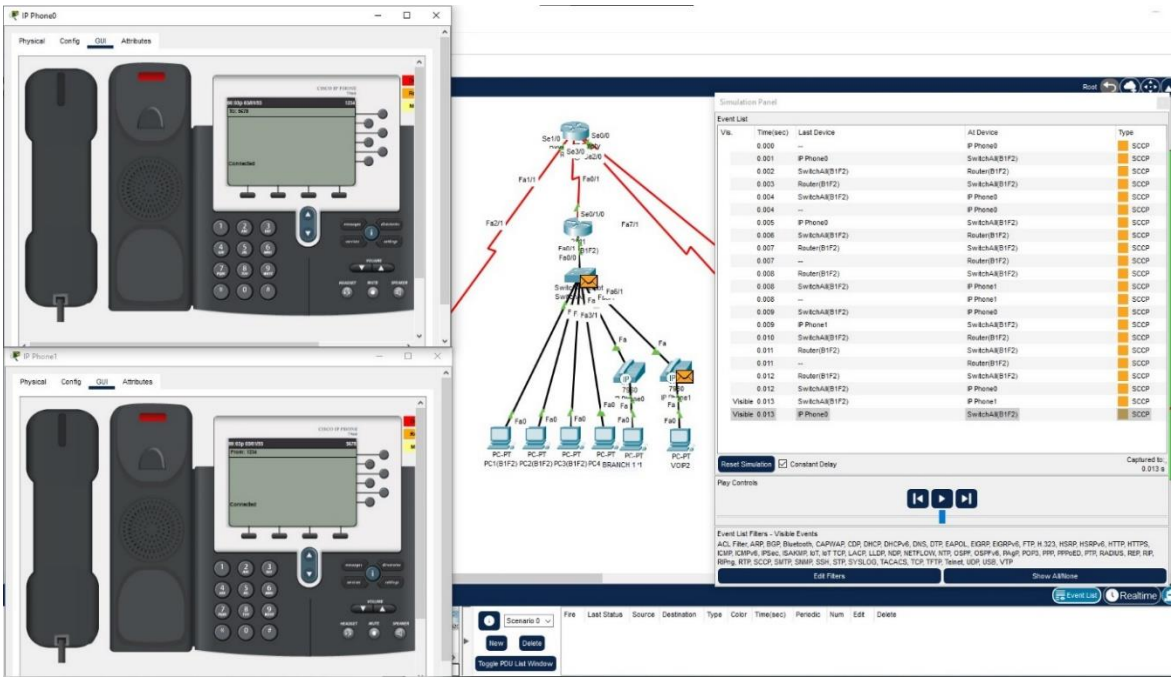
Simulation 3: Two users from second facility of first branch want to talk via VoIP.

The path for connection between two VoIP Phones is as follows:

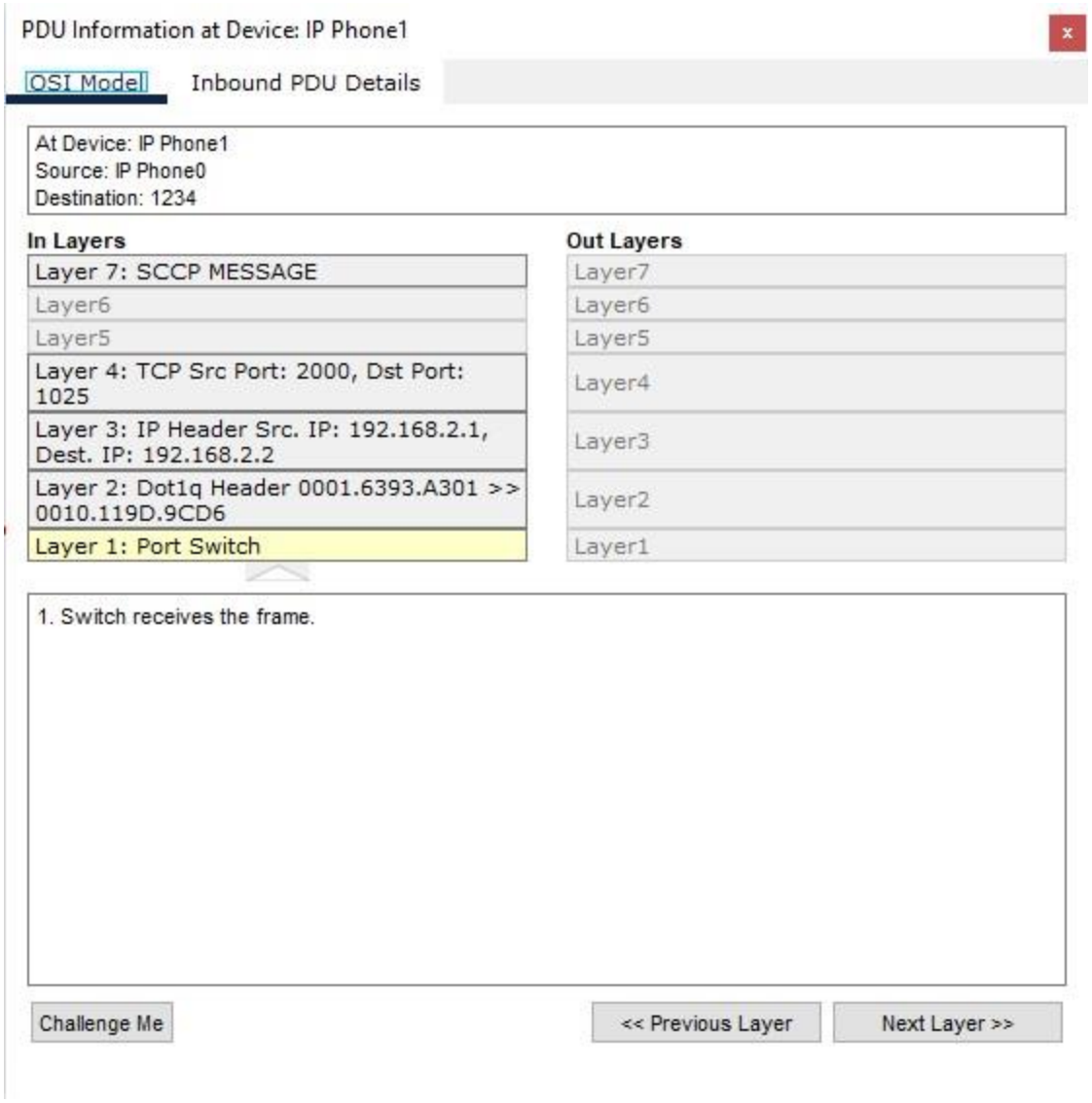
IpPhone0, SwitchAll(B1F2), Router(B1F2), SwitchAll(B1F2), IpPhone1



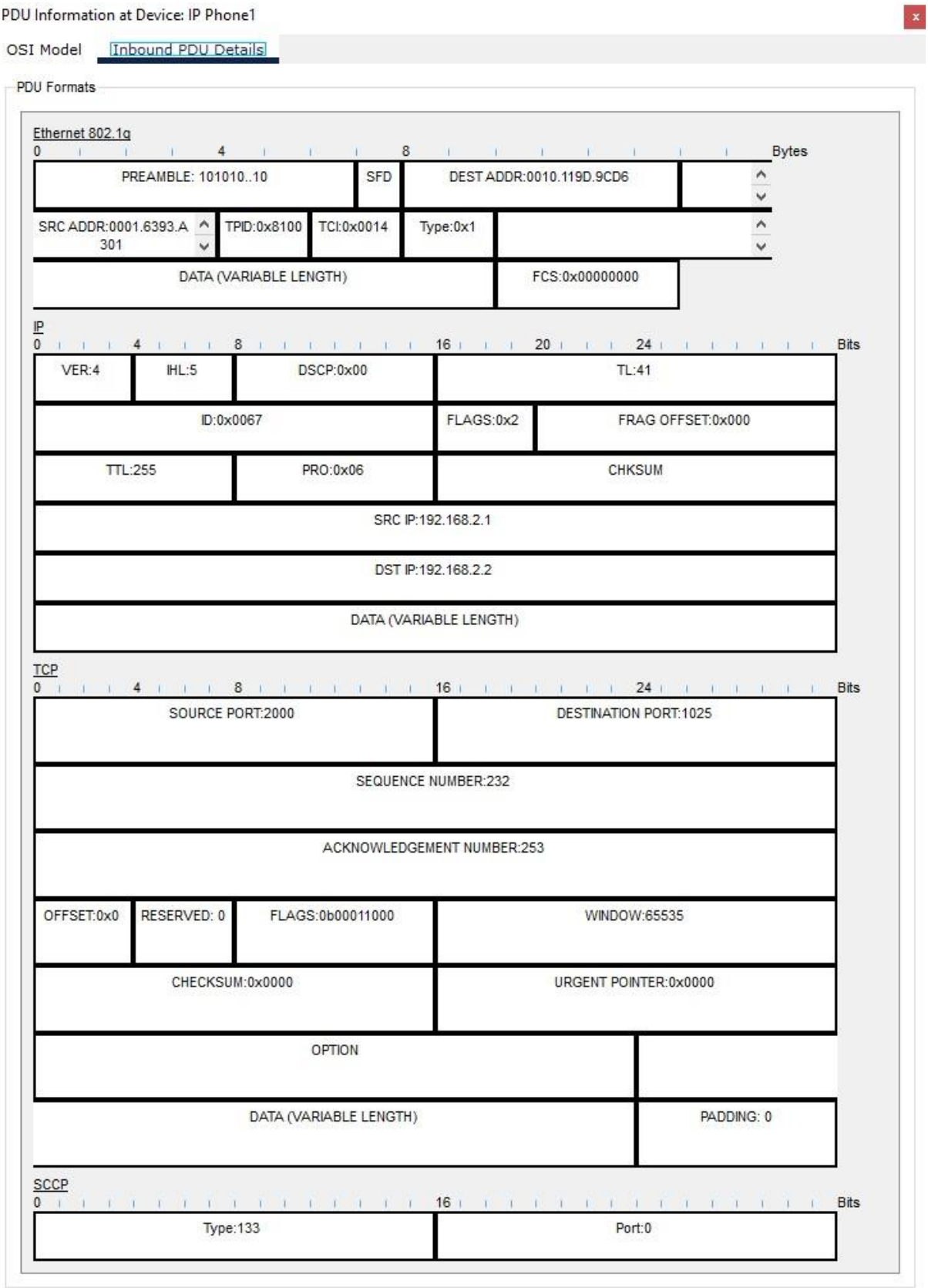
The Phone is Ringing



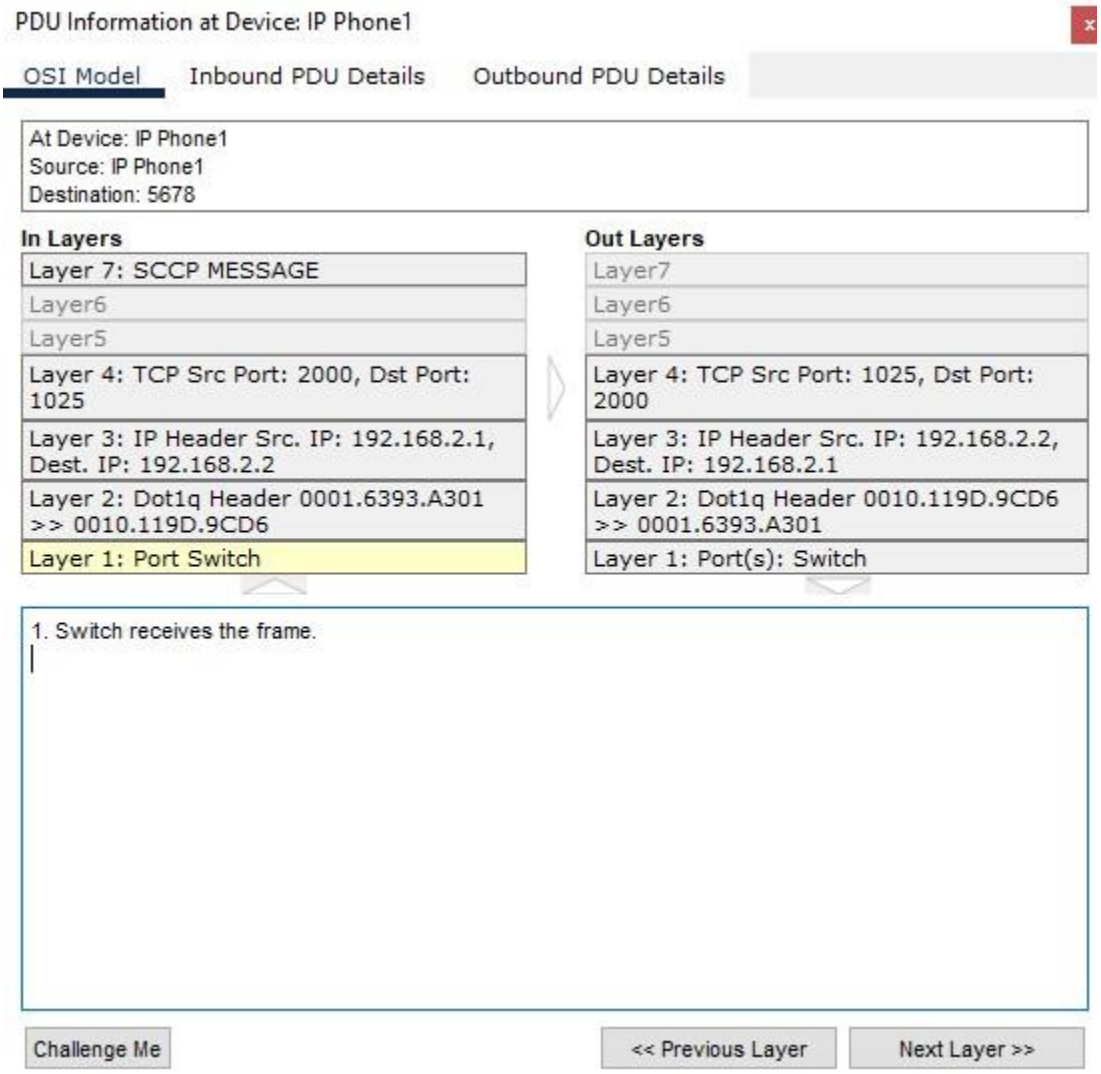
2 Phones are Connected



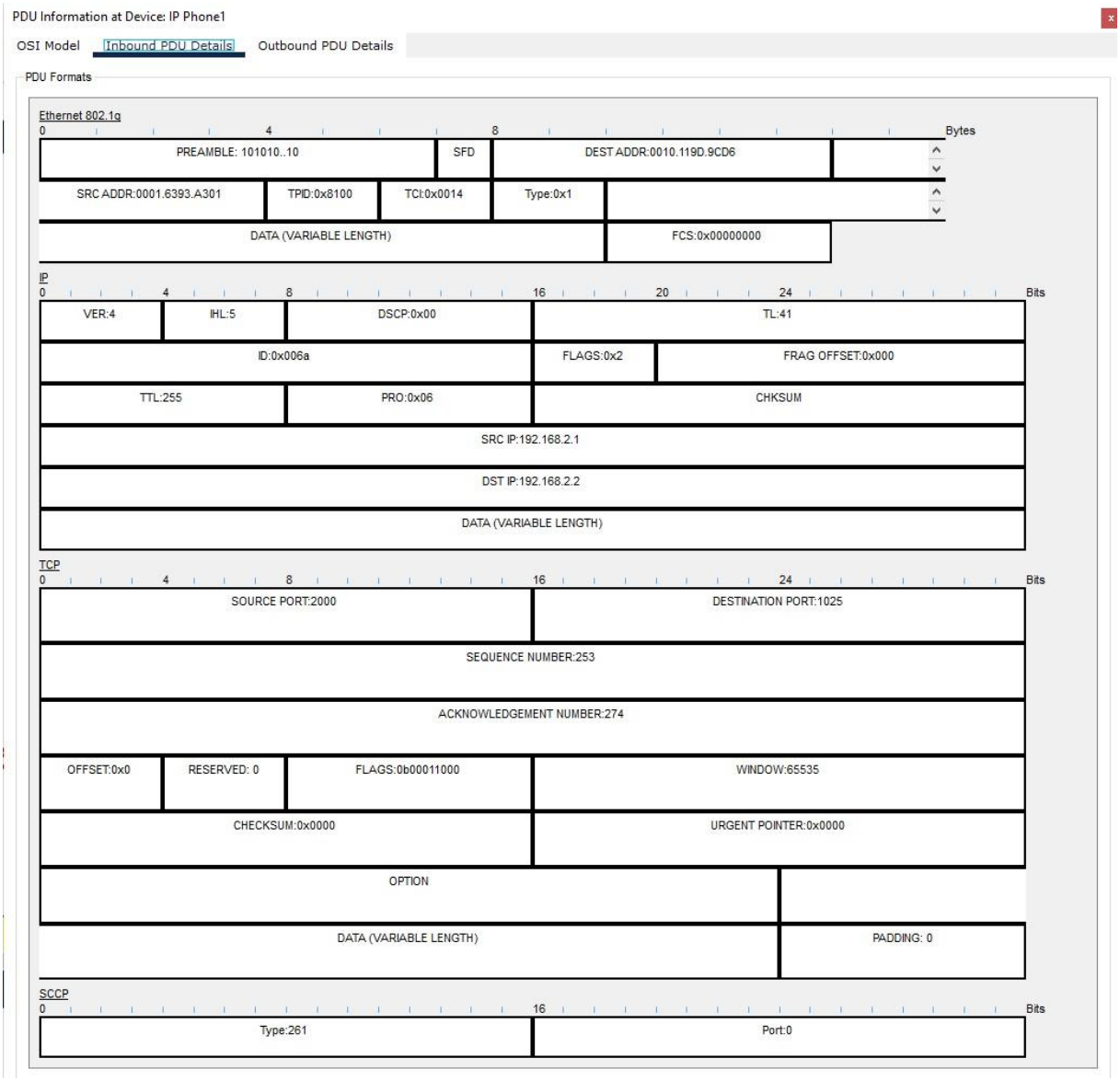
OSI Model of the packet that is sent to ring VoIP Phone1



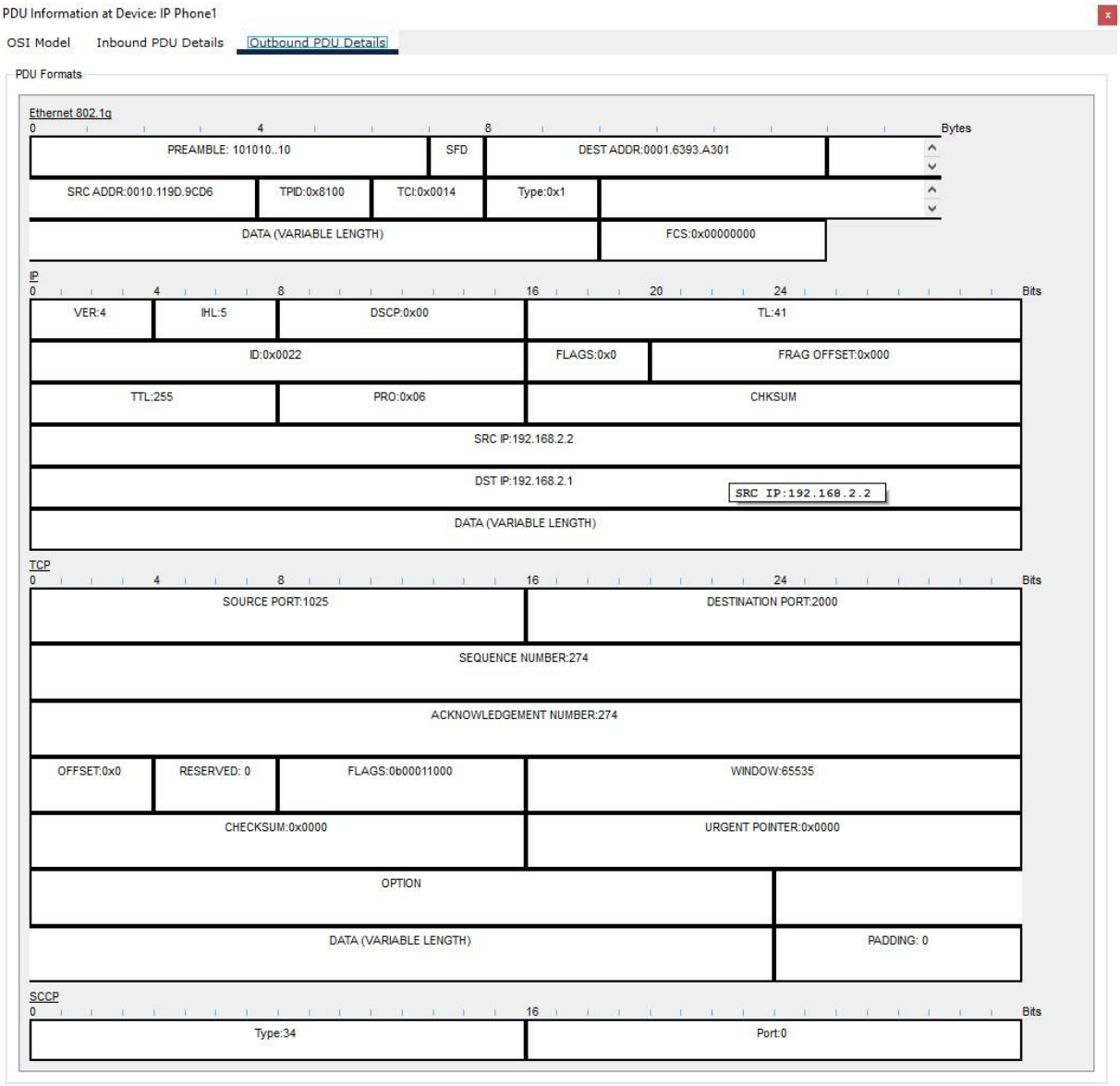
Inbound PDU Details of the packet that is sent to ring VoIP Phone1



OSI Model of the packet that is sent for connection established to VoIP Phone0



Inbound PDU Details of the packet that is sent for connection established to VoIP Phone0



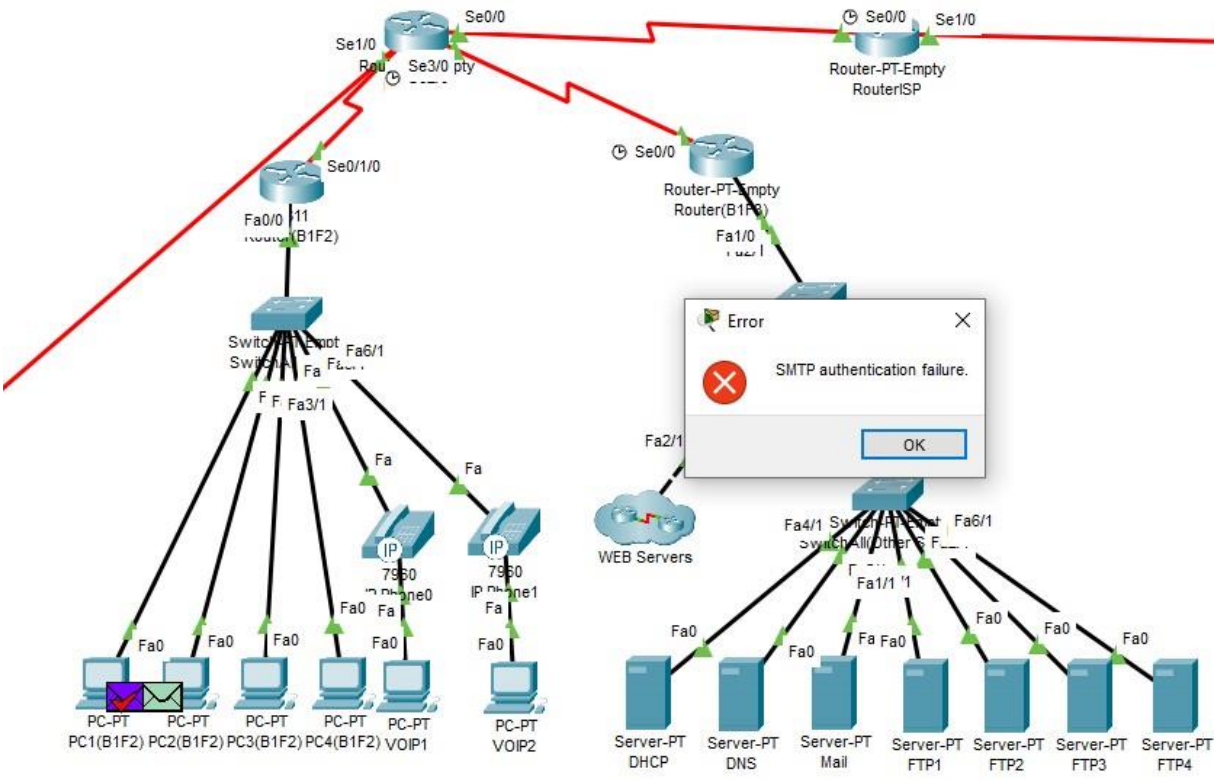
Outbound PDU Details of the packet that is sent for connection established to VoIP Phone0

Simulation 4: A user in the second facility of first branch wants to send an email message to his friend in the second facility of second branch.

An error message was received because PC1 tried to perform an unauthorized operation.

PC1(B1F2) at branch 1 facility 2 has used the following path to communicate with the Mail Server at branch 1 facility 3:

PC1(B1F2), SwitchAll(B1F2), Router(B1F2), RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(OtherServers), Mail



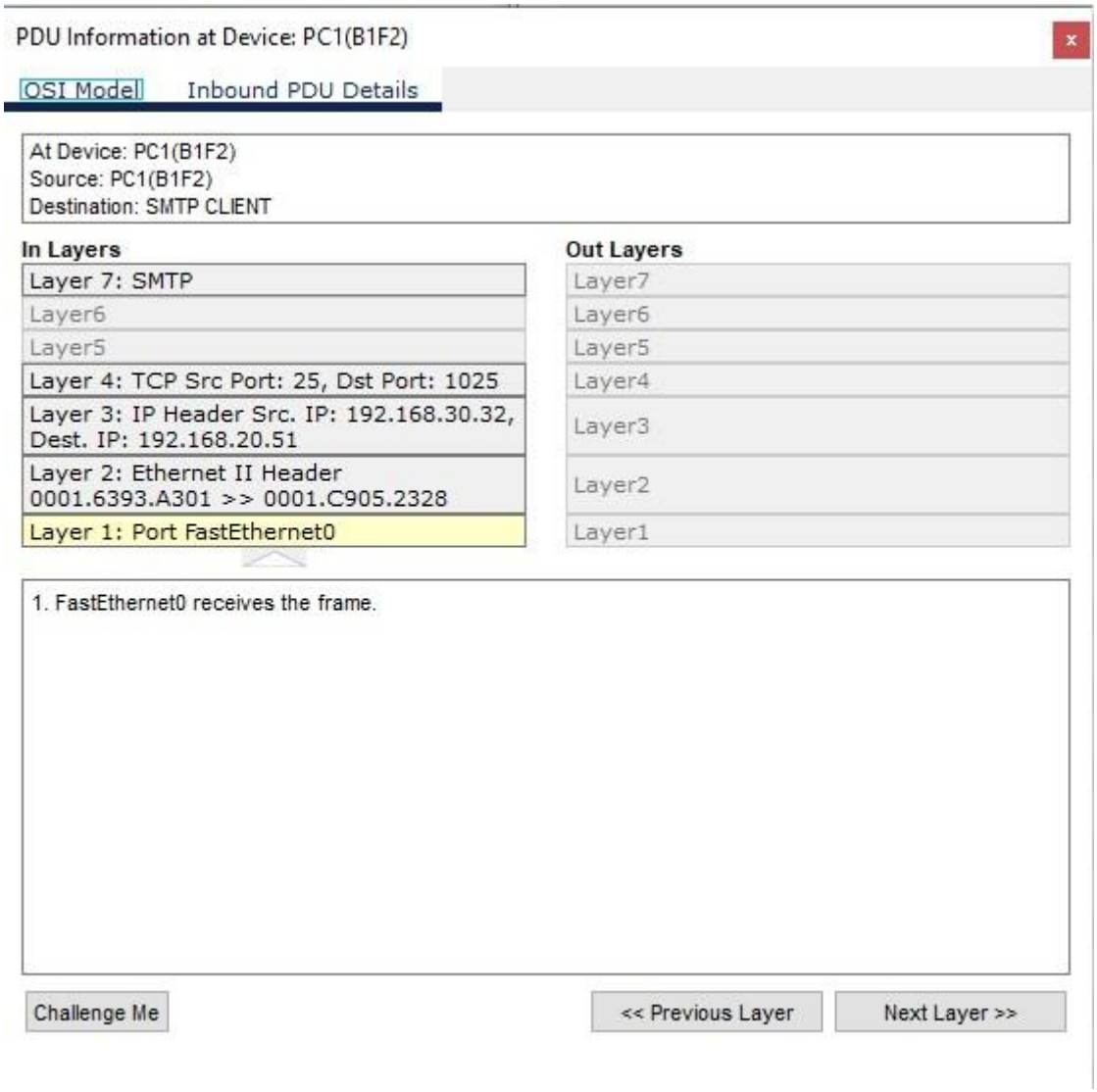
Result of Sending Mail to the Mail Server

Simulation Panel

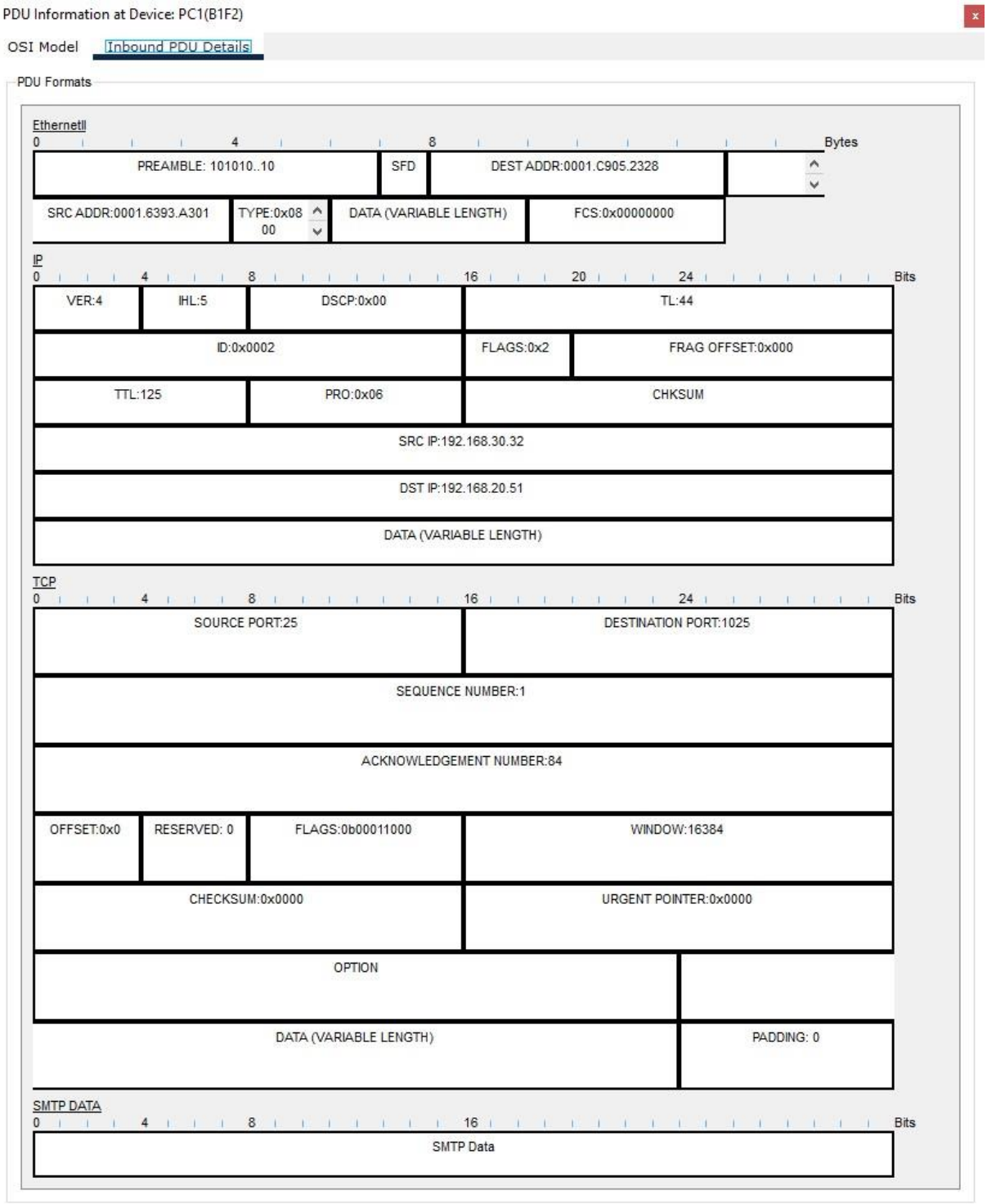
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.012	SwitchAll(Other Servers)	Mail	ARP
	0.012	SwitchAll(Other Servers)	FTP1	ARP
	0.012	SwitchAll(Other Servers)	FTP2	ARP
	0.012	SwitchAll(Other Servers)	FTP3	ARP
	0.012	SwitchAll(Other Servers)	DHCP	ARP
	0.012	SwitchAll(Other Servers)	DNS	ARP
	0.012	SwitchAll(Other Servers)	FTP4	ARP
	0.013	Mail	SwitchAll(Other Servers)	ARP
	0.014	SwitchAll(Other Servers)	SwitchAll(Servers)	ARP
	0.015	SwitchAll(Servers)	Router(B1F3)	ARP
	0.304	--	PC1(B1F2)	TCP
	0.305	PC1(B1F2)	SwitchAll(B1F2)	TCP
	0.306	SwitchAll(B1F2)	Router(B1F2)	TCP
	0.307	Router(B1F2)	RouterB1	TCP
	0.308	RouterB1	Router(B1F3)	TCP
	0.309	Router(B1F3)	SwitchAll(Servers)	TCP
	0.310	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.311	SwitchAll(Other Servers)	Mail	TCP
	0.312	Mail	SwitchAll(Other Servers)	TCP
	0.313	SwitchAll(Other Servers)	SwitchAll(Servers)	TCP
	0.314	SwitchAll(Servers)	Router(B1F3)	TCP
	0.315	Router(B1F3)	RouterB1	TCP
	0.316	RouterB1	Router(B1F2)	TCP
	0.317	Router(B1F2)	SwitchAll(B1F2)	TCP
	0.318	SwitchAll(B1F2)	PC1(B1F2)	TCP
	0.318	--	PC1(B1F2)	SMTP
	0.319	PC1(B1F2)	SwitchAll(B1F2)	TCP
	0.319	--	PC1(B1F2)	SMTP
	0.320	PC1(B1F2)	SwitchAll(B1F2)	SMTP
	0.320	SwitchAll(B1F2)	Router(B1F2)	TCP
	0.321	SwitchAll(B1F2)	Router(B1F2)	SMTP
	0.321	Router(B1F2)	RouterB1	TCP
	0.322	Router(B1F2)	RouterB1	SMTP
	0.322	RouterB1	Router(B1F3)	TCP
	0.323	RouterB1	Router(B1F3)	SMTP
	0.323	Router(B1F3)	SwitchAll(Servers)	TCP
	0.324	Router(B1F3)	SwitchAll(Servers)	SMTP
	0.324	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.325	SwitchAll(Servers)	SwitchAll(Other Servers)	SMTP
	0.325	SwitchAll(Other Servers)	Mail	TCP
	0.326	SwitchAll(Other Servers)	Mail	SMTP
	0.327	Mail	SwitchAll(Other Servers)	SMTP
	0.328	SwitchAll(Other Servers)	SwitchAll(Servers)	SMTP
	0.329	SwitchAll(Servers)	Router(B1F3)	SMTP
	0.330	Router(B1F3)	RouterB1	SMTP
	0.331	RouterB1	Router(B1F2)	SMTP
	0.332	Router(B1F2)	SwitchAll(B1F2)	SMTP
Visible	0.333	SwitchAll(B1F2)	PC1(B1F2)	SMTP

Event List of Sending Mail to Mail Server



OSI Model of the Last Packet that is sent to PC1

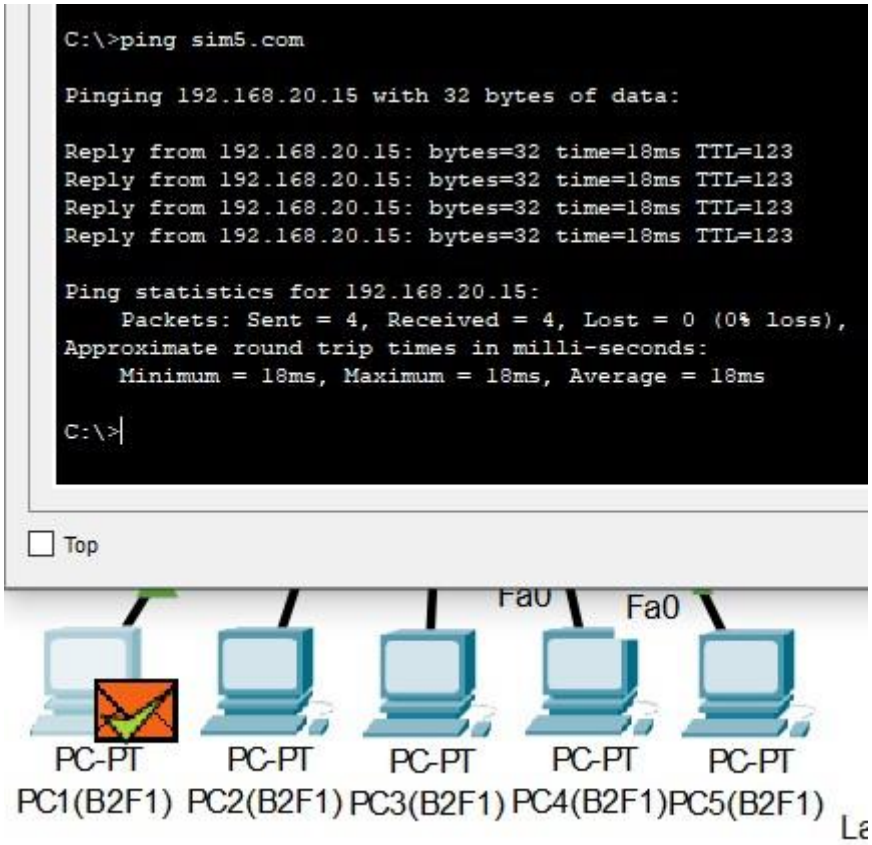


Inbound PDU Details of the Last Packet that is sent to PC1

Simulation 5: A user from first facility of second branch pings Web server of second facility of first branch.

PC1(B2F1) at branch 2 facility 1 has used the following path to ping the WEB Server at branch 1 facility 2:

PC1(B2F1), SwitchPC(B2F1), SwitchAll(B2F1), Router(B2F1), RouterB2, RouterISP, RouterB1, Router(B1F2), WEBServer.



Result of Successful Transmission of the Ping

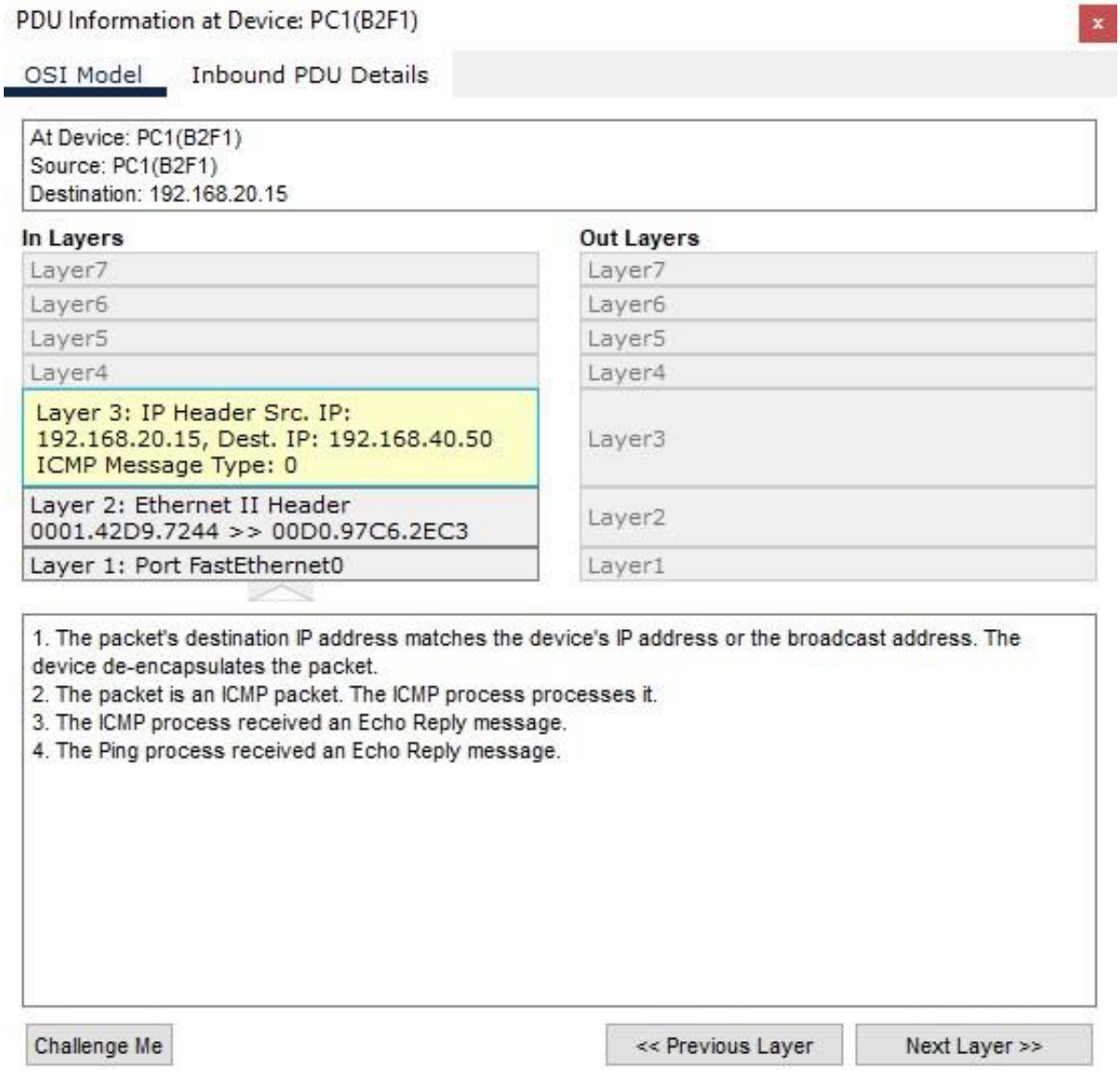
Simulation Panel

Event List

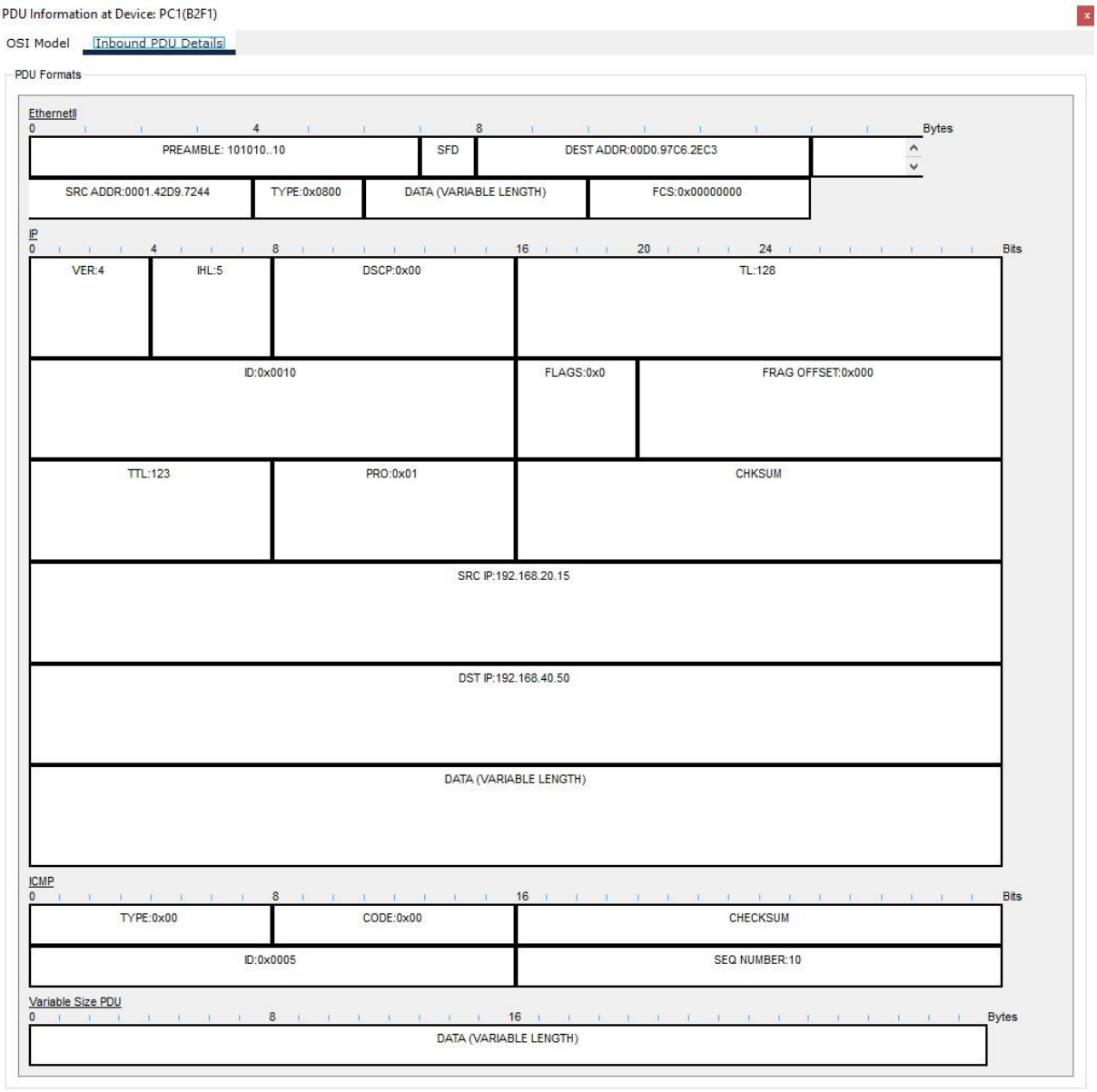
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1(B2F1)	DNS
	0.001	PC1(B2F1)	SwitchPC(B2F1)	DNS
	0.002	SwitchPC(B2F1)	SwitchAll(B2F1)	DNS
	0.003	SwitchAll(B2F1)	Router(B2F1)	DNS
	0.004	Router(B2F1)	RouterB2	DNS
	0.005	RouterB2	RouterISP	DNS
	0.006	RouterISP	RouterB1	DNS
	0.007	RouterB1	Router(B1F3)	DNS
	0.008	Router(B1F3)	SwitchAll(Servers)	DNS
	0.009	SwitchAll(Servers)	SwitchAll(Other Serv...	DNS
	0.010	SwitchAll(Other Servers)	DNS	DNS
	0.011	DNS	SwitchAll(Other Serv...	DNS
	0.012	SwitchAll(Other Servers)	SwitchAll(Servers)	DNS
	0.013	SwitchAll(Servers)	Router(B1F3)	DNS
	0.014	Router(B1F3)	RouterB1	DNS
	0.015	RouterB1	RouterISP	DNS
	0.016	RouterISP	RouterB2	DNS
	0.017	RouterB2	Router(B2F1)	DNS
	0.018	Router(B2F1)	SwitchAll(B2F1)	DNS
	0.019	SwitchAll(B2F1)	SwitchPC(B2F1)	DNS
	0.020	SwitchPC(B2F1)	PC1(B2F1)	DNS
	0.020	--	PC1(B2F1)	ICMP
	0.021	PC1(B2F1)	SwitchPC(B2F1)	ICMP
	0.022	SwitchPC(B2F1)	SwitchAll(B2F1)	ICMP
	0.023	SwitchAll(B2F1)	Router(B2F1)	ICMP
	0.024	Router(B2F1)	RouterB2	ICMP
	0.025	RouterB2	RouterISP	ICMP
	0.026	RouterISP	RouterB1	ICMP
	0.027	RouterB1	Router(B1F2)	ICMP
	0.028	Router(B1F2)	SwitchAll(B1F2)	ICMP
	0.029	SwitchAll(B1F2)	WEB8(Simulation5)	ICMP
	0.030	WEB8(Simulation5)	SwitchAll(B1F2)	ICMP
	0.031	SwitchAll(B1F2)	Router(B1F2)	ICMP
	0.032	Router(B1F2)	RouterB1	ICMP
	0.033	RouterB1	RouterISP	ICMP
	0.034	RouterISP	RouterB2	ICMP
	0.035	RouterB2	Router(B2F1)	ICMP
	0.036	Router(B2F1)	SwitchAll(B2F1)	ICMP
	0.037	SwitchAll(B2F1)	SwitchPC(B2F1)	ICMP
	0.038	SwitchPC(B2F1)	PC1(B2F1)	ICMP
	1.041	--	PC1(B2F1)	ICMP
	1.042	PC1(B2F1)	SwitchPC(B2F1)	ICMP
	1.043	SwitchPC(B2F1)	SwitchAll(B2F1)	ICMP
	1.044	SwitchAll(B2F1)	Router(B2F1)	ICMP
	1.045	Router(B2F1)	RouterB2	ICMP
	1.046	RouterB2	RouterISP	ICMP
	1.047	RouterISP	RouterB1	ICMP
	1.048	RouterB1	Router(B1F2)	ICMP

Vis.	Time(sec)	Last Device	At Device	Type
	1.049	Router(B1F2)	SwitchAll(B1F2)	ICMP
	1.050	SwitchAll(B1F2)	WEB8(Simulation5)	ICMP
	1.051	WEB8(Simulation5)	SwitchAll(B1F2)	ICMP
	1.052	SwitchAll(B1F2)	Router(B1F2)	ICMP
	1.053	Router(B1F2)	RouterB1	ICMP
	1.054	RouterB1	RouterISP	ICMP
	1.055	RouterISP	RouterB2	ICMP
	1.056	RouterB2	Router(B2F1)	ICMP
	1.057	Router(B2F1)	SwitchAll(B2F1)	ICMP
	1.058	SwitchAll(B2F1)	SwitchPC(B2F1)	ICMP
	1.059	SwitchPC(B2F1)	PC1(B2F1)	ICMP
	2.062	--	PC1(B2F1)	ICMP
	2.063	PC1(B2F1)	SwitchPC(B2F1)	ICMP
	2.064	SwitchPC(B2F1)	SwitchAll(B2F1)	ICMP
	2.065	SwitchAll(B2F1)	Router(B2F1)	ICMP
	2.066	Router(B2F1)	RouterB2	ICMP
	2.067	RouterB2	RouterISP	ICMP
	2.068	RouterISP	RouterB1	ICMP
	2.069	RouterB1	Router(B1F2)	ICMP
	2.070	Router(B1F2)	SwitchAll(B1F2)	ICMP
	2.071	SwitchAll(B1F2)	WEB8(Simulation5)	ICMP
	2.072	WEB8(Simulation5)	SwitchAll(B1F2)	ICMP
	2.073	SwitchAll(B1F2)	Router(B1F2)	ICMP
	2.074	Router(B1F2)	RouterB1	ICMP
	2.075	RouterB1	RouterISP	ICMP
	2.076	RouterISP	RouterB2	ICMP
	2.077	RouterB2	Router(B2F1)	ICMP
	2.078	Router(B2F1)	SwitchAll(B2F1)	ICMP
	2.079	SwitchAll(B2F1)	SwitchPC(B2F1)	ICMP
	2.080	SwitchPC(B2F1)	PC1(B2F1)	ICMP
	3.084	--	PC1(B2F1)	ICMP
	3.085	PC1(B2F1)	SwitchPC(B2F1)	ICMP
	3.086	SwitchPC(B2F1)	SwitchAll(B2F1)	ICMP
	3.087	SwitchAll(B2F1)	Router(B2F1)	ICMP
	3.088	Router(B2F1)	RouterB2	ICMP
	3.089	RouterB2	RouterISP	ICMP
	3.090	RouterISP	RouterB1	ICMP
	3.091	RouterB1	Router(B1F2)	ICMP
	3.092	Router(B1F2)	SwitchAll(B1F2)	ICMP
	3.093	SwitchAll(B1F2)	WEB8(Simulation5)	ICMP
	3.094	WEB8(Simulation5)	SwitchAll(B1F2)	ICMP
	3.095	SwitchAll(B1F2)	Router(B1F2)	ICMP
	3.096	Router(B1F2)	RouterB1	ICMP
	3.097	RouterB1	RouterISP	ICMP
	3.098	RouterISP	RouterB2	ICMP
	3.099	RouterB2	Router(B2F1)	ICMP
	3.100	Router(B2F1)	SwitchAll(B2F1)	ICMP
	3.101	SwitchAll(B2F1)	SwitchPC(B2F1)	ICMP
Visible	3.102	SwitchPC(B2F1)	PC1(B2F1)	ICMP

Event List of Ping



OSI Model in the Ping Result Packet Reaching the PC

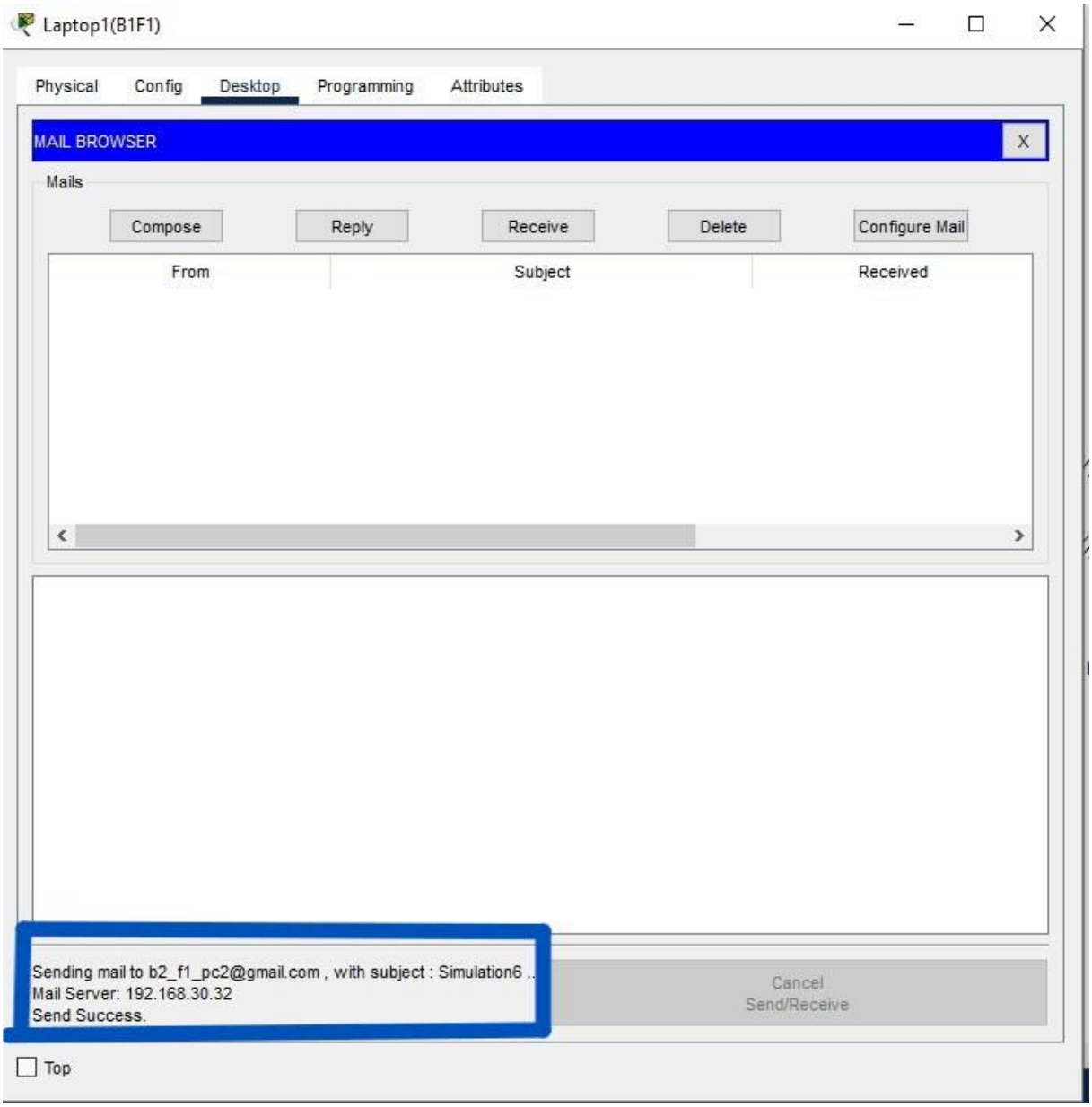


Inbound PDU Details in the Ping Result Packet Reaching the PC

Simulation 6: A laptop user from first facility of first branch office wants to send email to her friend in the first facility of second branch office.

Laptop1(B1F1) at branch 1 facility 1 has used the following path to communicate with the Mail Server at branch 1 facility 3:

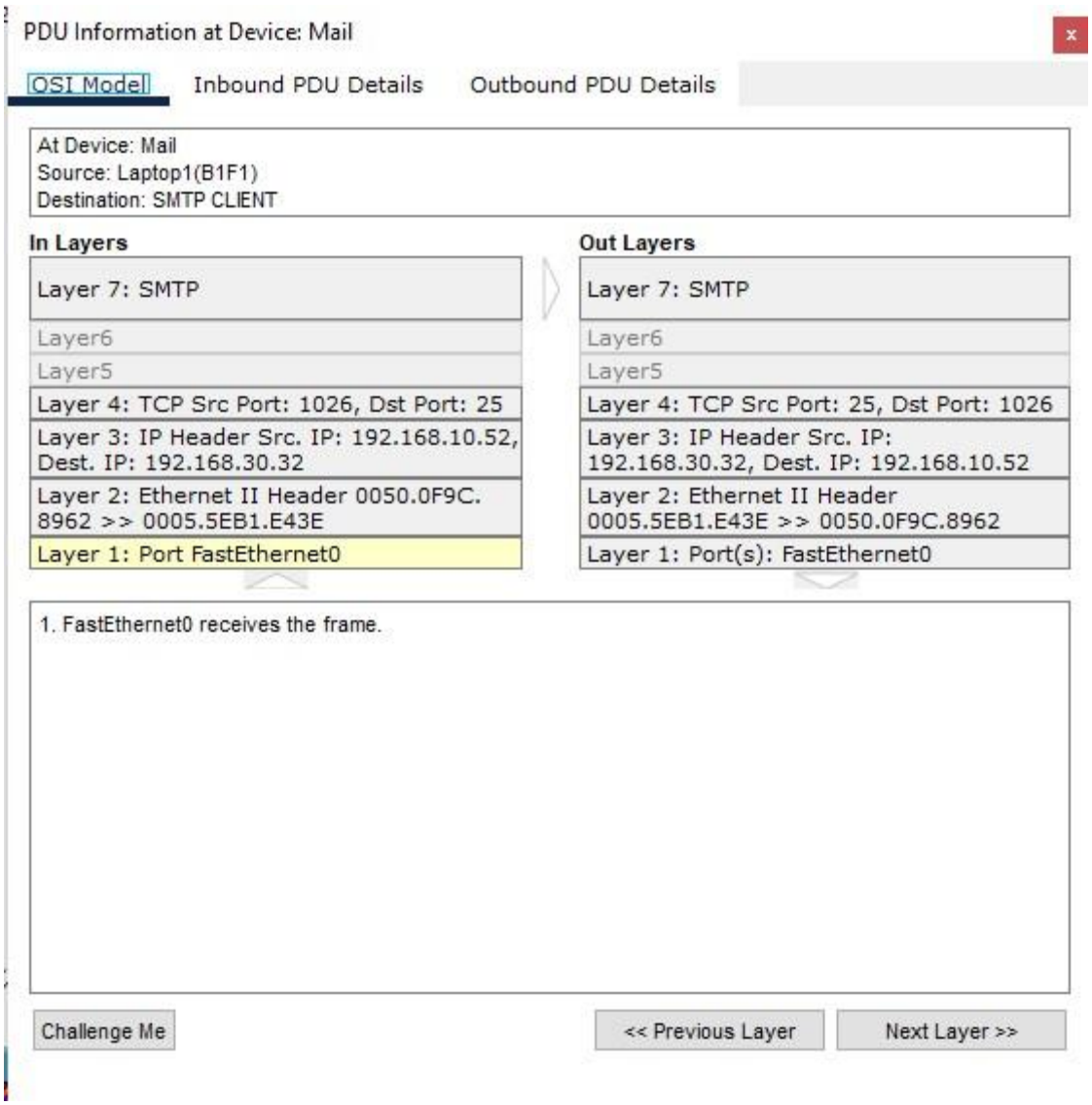
Laptop1(B1F1), Access Point(B1F1), SwitchAll(B1F1), Router(B1F1), RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(OtherServers), Mail.



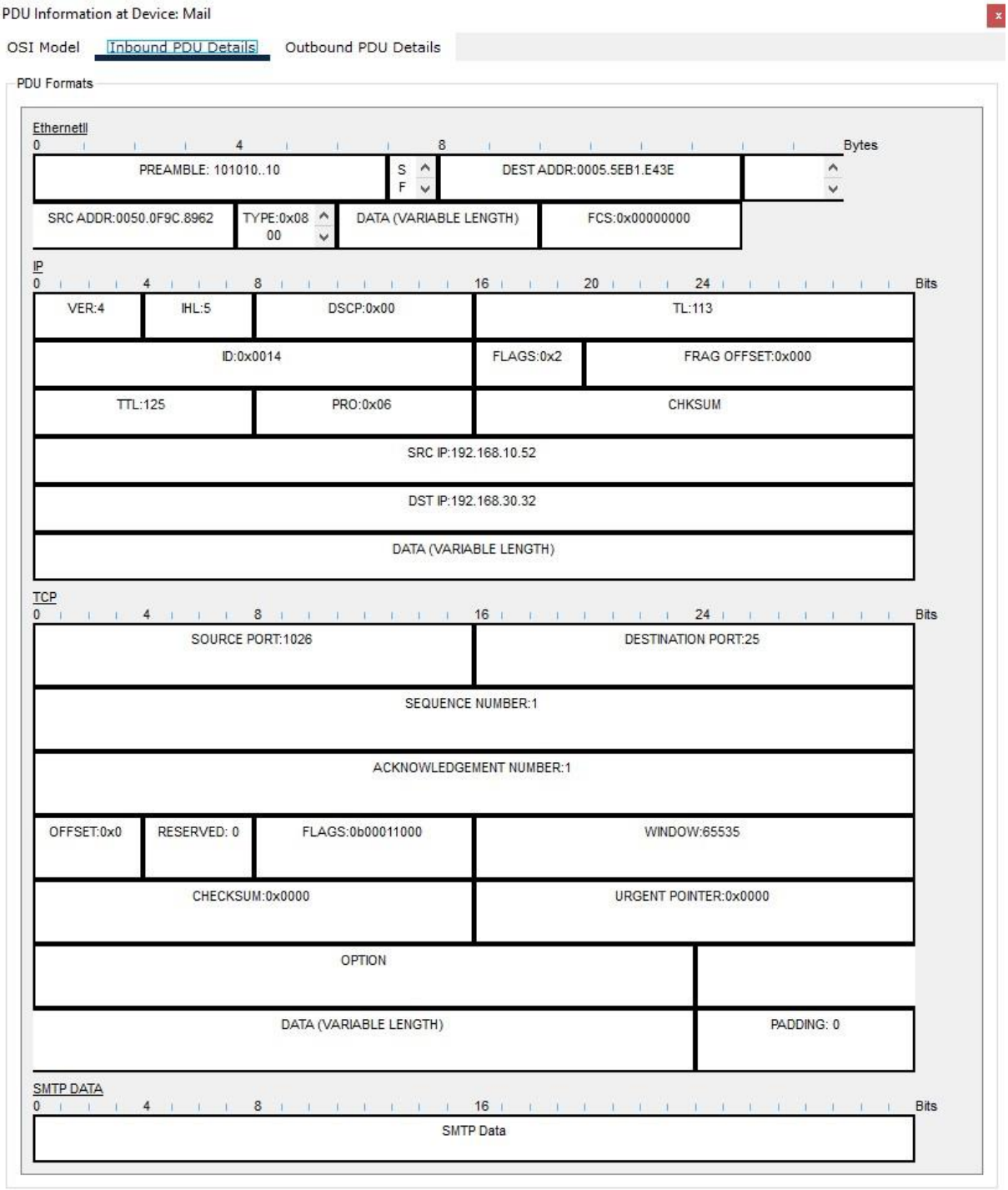
Result of Sending is Successful

	0.020	--	Laptop1(B1F1)	SMTP
	0.021	Laptop1(B1F1)	Access Point(B1F1)	SMTP
	0.021	SwitchAll(B1F1)	Router(B1F1)	TCP
	0.022	Access Point(B1F1)	SwitchAll(B1F1)	SMTP
	0.022	Router(B1F1)	RouterB1	TCP
	0.023	SwitchAll(B1F1)	Router(B1F1)	SMTP
	0.023	RouterB1	Router(B1F3)	TCP
	0.024	Router(B1F1)	RouterB1	SMTP
	0.024	Router(B1F3)	SwitchAll(Servers)	TCP
	0.024	--	Access Point(B1F1)	TCP
	0.025	Access Point(B1F1)	Smartphone3(B1F1)	TCP
	0.025	Access Point(B1F1)	Smartphone1(B1F1)	TCP
	0.025	Access Point(B1F1)	Laptop1(B1F1)	TCP
	0.025	Access Point(B1F1)	Laptop3(B1F1)	TCP
	0.025	Access Point(B1F1)	Smartphone2(B1F1)	TCP
	0.025	Access Point(B1F1)	Laptop2(B1F1)	TCP
	0.025	RouterB1	Router(B1F3)	SMTP
	0.025	SwitchAll(Servers)	SwitchAll(Other Servers)	TCP
	0.026	Router(B1F3)	SwitchAll(Servers)	SMTP
	0.026	SwitchAll(Other Servers)	Mail	TCP
	0.027	SwitchAll(Servers)	SwitchAll(Other Servers)	SMTP
	0.028	SwitchAll(Other Servers)	Mail	SMTP
	0.029	Mail	SwitchAll(Other Servers)	SMTP
	0.029	--	Access Point(B1F1)	SMTP
	0.030	Access Point(B1F1)	Smartphone3(B1F1)	SMTP
	0.030	Access Point(B1F1)	Smartphone1(B1F1)	SMTP
	0.030	Access Point(B1F1)	Laptop1(B1F1)	SMTP
	0.030	Access Point(B1F1)	Laptop3(B1F1)	SMTP
	0.030	Access Point(B1F1)	Smartphone2(B1F1)	SMTP
	0.030	Access Point(B1F1)	Laptop2(B1F1)	SMTP
	0.030	SwitchAll(Other Servers)	SwitchAll(Servers)	SMTP
	0.031	SwitchAll(Servers)	Router(B1F3)	SMTP
	0.032	Router(B1F3)	RouterB1	SMTP
	0.033	RouterB1	Router(B1F1)	SMTP
	0.034	Router(B1F1)	SwitchAll(B1F1)	SMTP
	0.035	SwitchAll(B1F1)	Access Point(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Smartphone3(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Smartphone1(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Laptop1(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Smartphone2(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Laptop3(B1F1)	SMTP
Visible	0.036	Access Point(B1F1)	Laptop2(B1F1)	SMTP

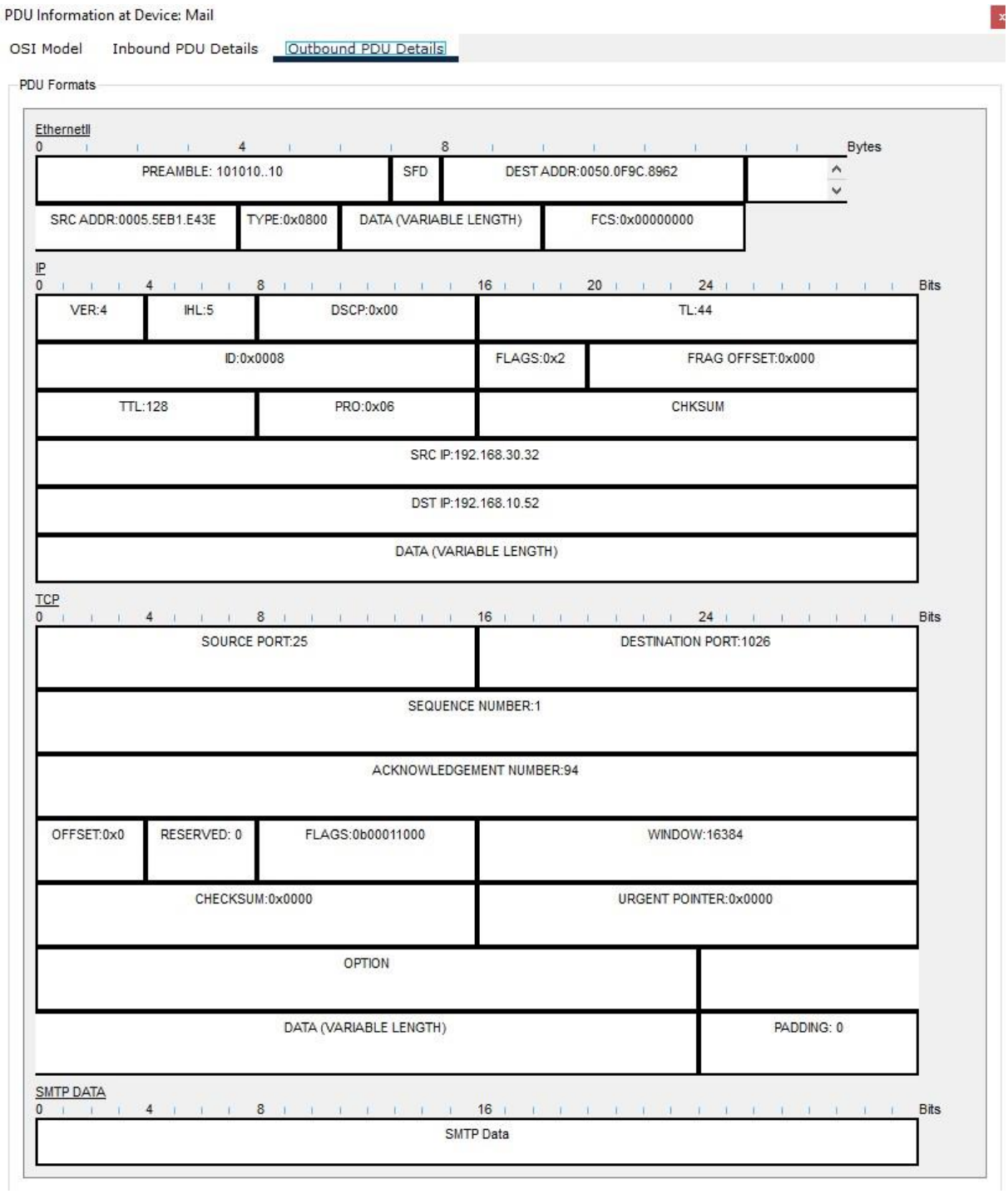
Event List of Laptop Sending Message and gets Received Message



OSI Model When Packet is Sent to the Mail



Inbound PDU Details of the Packet That is Sent to Mail

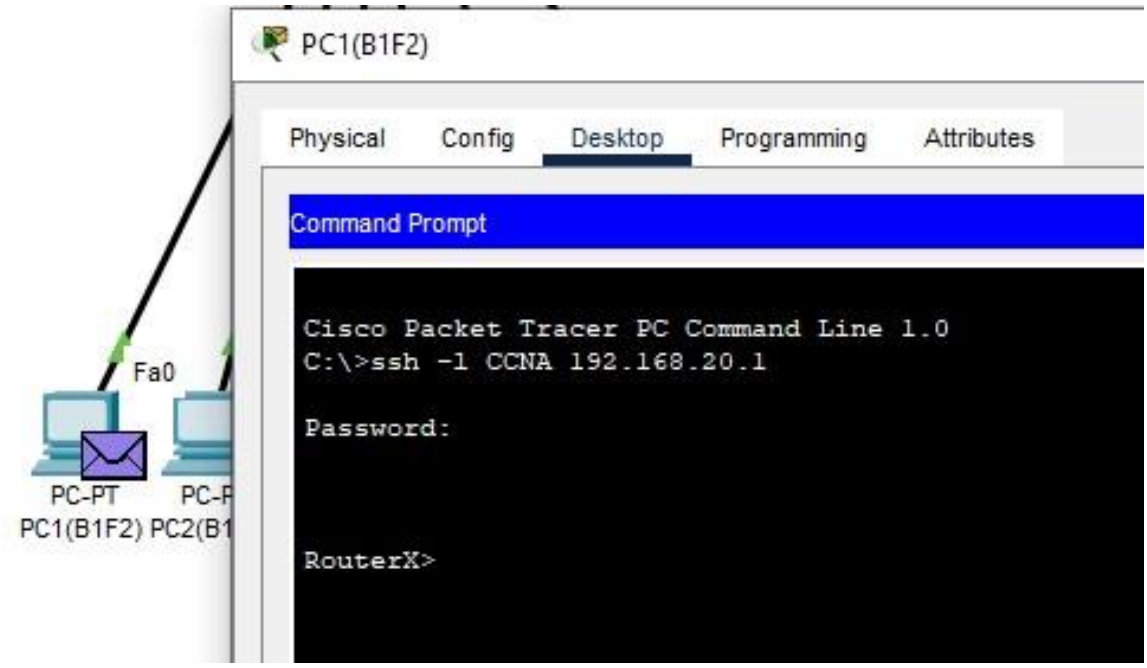


Outbound PDU Details of the Packet is Sent by Mail

Simulation 7: A pc user from second facility of first branch office wants to connect its router with ssh protocol.

PC1(B1F2) at branch 1 facility 2 has used the following path to connect to its routers CLI:

PC1(B1F2), SwitchAll(B1F2), Router(B1F2).

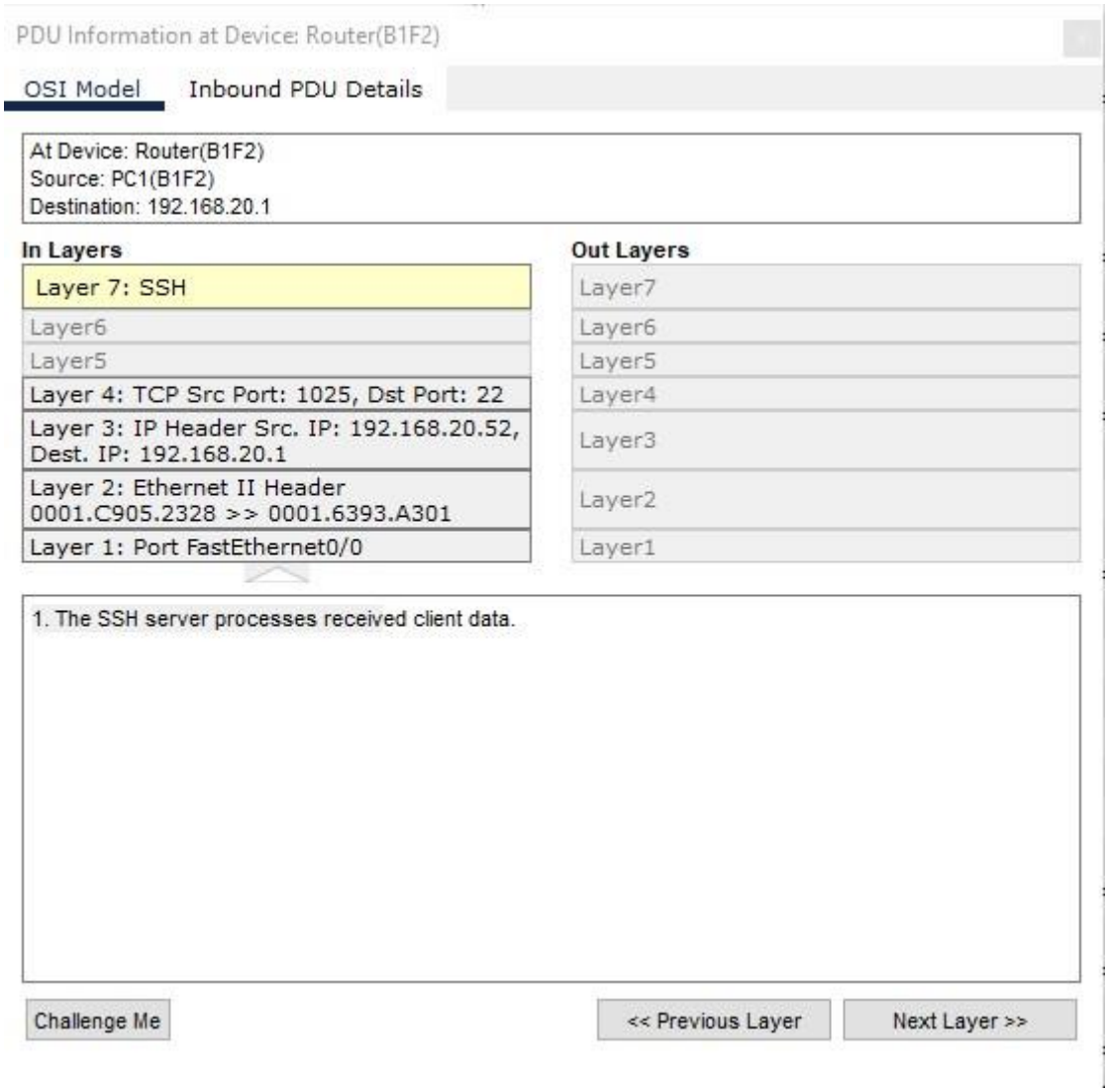


Result of Connecting to the Router

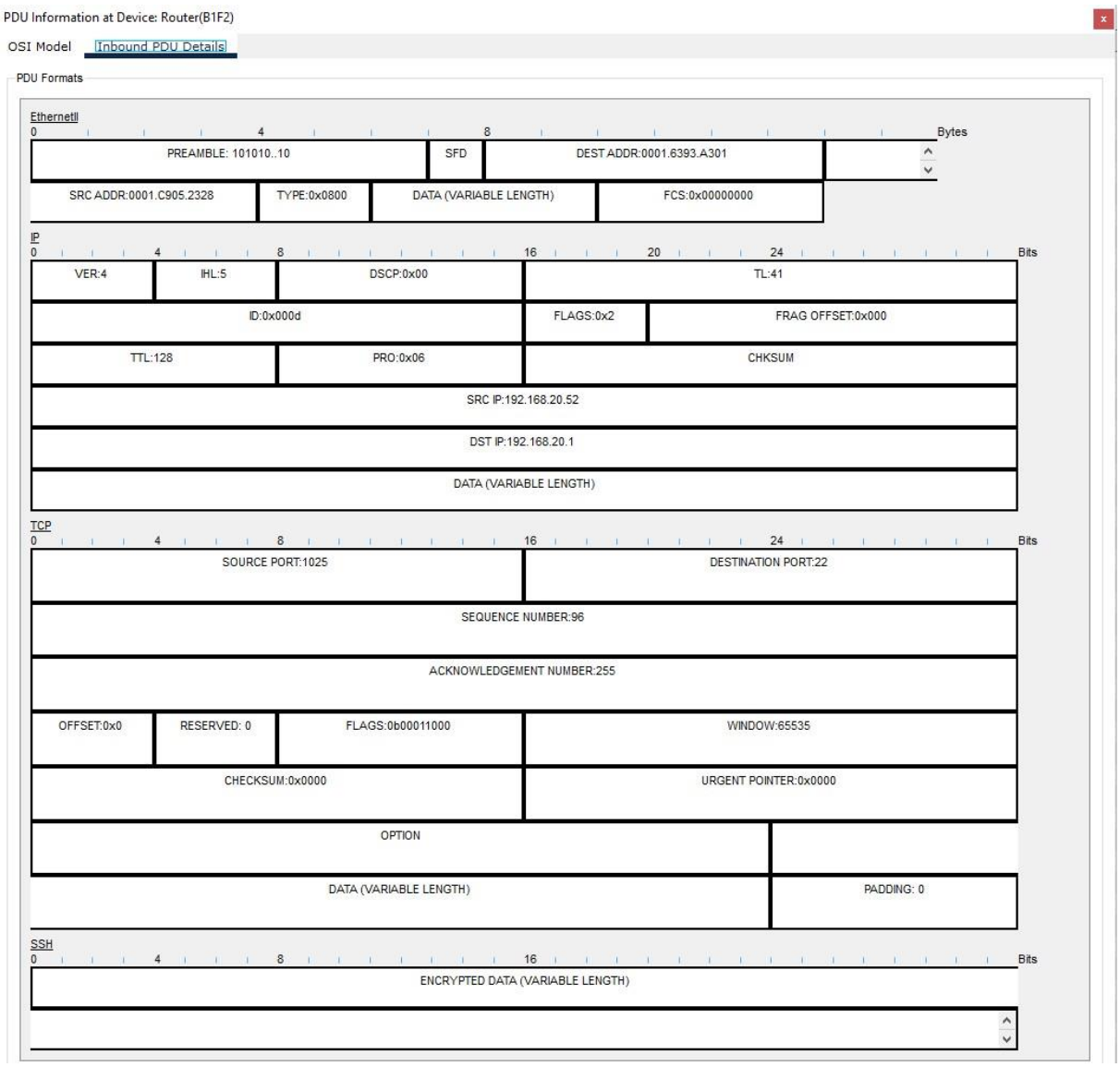
Vis.	Time(sec)	Last Device	At Device	Type
	0.010	--	Router(B1F2)	SSH
	0.011	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.012	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.012	--	PC1(B1F2)	SSH
	0.012	--	PC1(B1F2)	SSH
	0.013	PC1(B1F2)	SwitchAll(B1F2)	SSH
	0.014	SwitchAll(B1F2)	Router(B1F2)	SSH
	0.056	--	Router(B1F2)	TCP
	0.057	Router(B1F2)	SwitchAll(B1F2)	TCP
	0.058	SwitchAll(B1F2)	PC1(B1F2)	TCP
	0.058	--	PC1(B1F2)	SSH
	0.059	PC1(B1F2)	SwitchAll(B1F2)	SSH
	0.060	SwitchAll(B1F2)	Router(B1F2)	SSH
	0.060	--	Router(B1F2)	SSH
	0.061	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.061	--	Router(B1F2)	SSH
	0.062	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.062	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.062	--	Router(B1F2)	SSH
	0.063	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.063	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.064	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	TCP
	0.064	--	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	SSH
	0.064	--	PC1(B1F2)	SSH
	0.065	PC1(B1F2)	SwitchAll(B1F2)	TCP
	0.065	--	PC1(B1F2)	SSH
	0.066	PC1(B1F2)	SwitchAll(B1F2)	SSH
	0.066	SwitchAll(B1F2)	Router(B1F2)	TCP
	0.067	SwitchAll(B1F2)	Router(B1F2)	SSH
	0.067	--	Router(B1F2)	SSH
	0.068	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.069	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.069	--	PC1(B1F2)	SSH
	0.070	PC1(B1F2)	SwitchAll(B1F2)	SSH
	0.071	SwitchAll(B1F2)	Router(B1F2)	SSH
	0.071	--	Router(B1F2)	SSH
	0.072	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.072	--	Router(B1F2)	SSH
	0.073	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.073	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.073	--	Router(B1F2)	SSH
	0.074	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.074	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.074		Router(B1F2)	SSH

	0.074	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.074	--	Router(B1F2)	SSH
	0.075	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.075	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.075	--	Router(B1F2)	SSH
	0.075	--	PC1(B1F2)	TCP
	0.076	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.076	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.076	PC1(B1F2)	SwitchAll(B1F2)	TCP
	0.076	--	Router(B1F2)	SSH
	0.077	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.077	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.077	SwitchAll(B1F2)	Router(B1F2)	TCP
	0.077	--	Router(B1F2)	SSH
	0.078	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.078	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.078	--	Router(B1F2)	SSH
	0.078	--	PC1(B1F2)	TCP
	0.078	--	PC1(B1F2)	SSH
	0.078	--	PC1(B1F2)	SSH
	0.078	--	PC1(B1F2)	SSH
	0.079	--	Router(B1F2)	SSH
	0.079	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.079	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.079	PC1(B1F2)	SwitchAll(B1F2)	TCP
	0.079	--	PC1(B1F2)	SSH
	0.080	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.080	PC1(B1F2)	SwitchAll(B1F2)	SSH
	0.080	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.080	SwitchAll(B1F2)	Router(B1F2)	TCP
	0.080	--	Router(B1F2)	SSH
	0.081	Router(B1F2)	SwitchAll(B1F2)	SSH
	0.081	SwitchAll(B1F2)	PC1(B1F2)	SSH
	0.081	SwitchAll(B1F2)	Router(B1F2)	SSH
	0.081	--	PC1(B1F2)	TCP
	0.081	--	Router(B1F2)	SSH
Visible	0.082	SwitchAll(B1F2)	PC1(B1F2)	SSH
Visible	0.082	PC1(B1F2)	SwitchAll(B1F2)	TCP
Visible	0.082	Router(B1F2)	SwitchAll(B1F2)	SSH
Visible	0.082	--	PC1(B1F2)	SSH

Event List of Connecting to the Router With Ssh



OSI Model of connecting to the Router

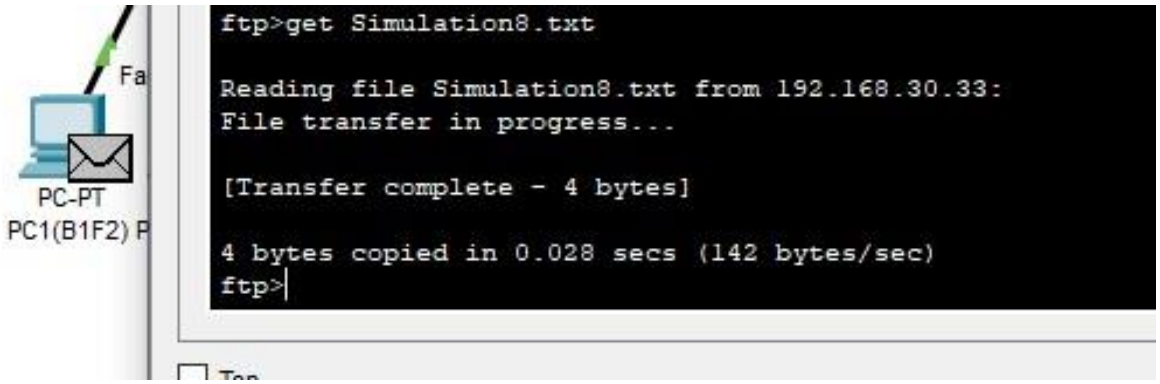


Inbound PDU Details of the Packet That is Sent to Router for Connection

Simulation 8: A pc user from second facility of first branch office wants to get a txt file from the FTP server.

PC1(B1F2) at branch 1 facility 2 has used the following path to connect to the FTP server at branch 1 facility 3:

PC1(B1F2), SwitchAll(B1F2), Router(B1F2), RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(Other Servers), FTP1.



Result of Get Command

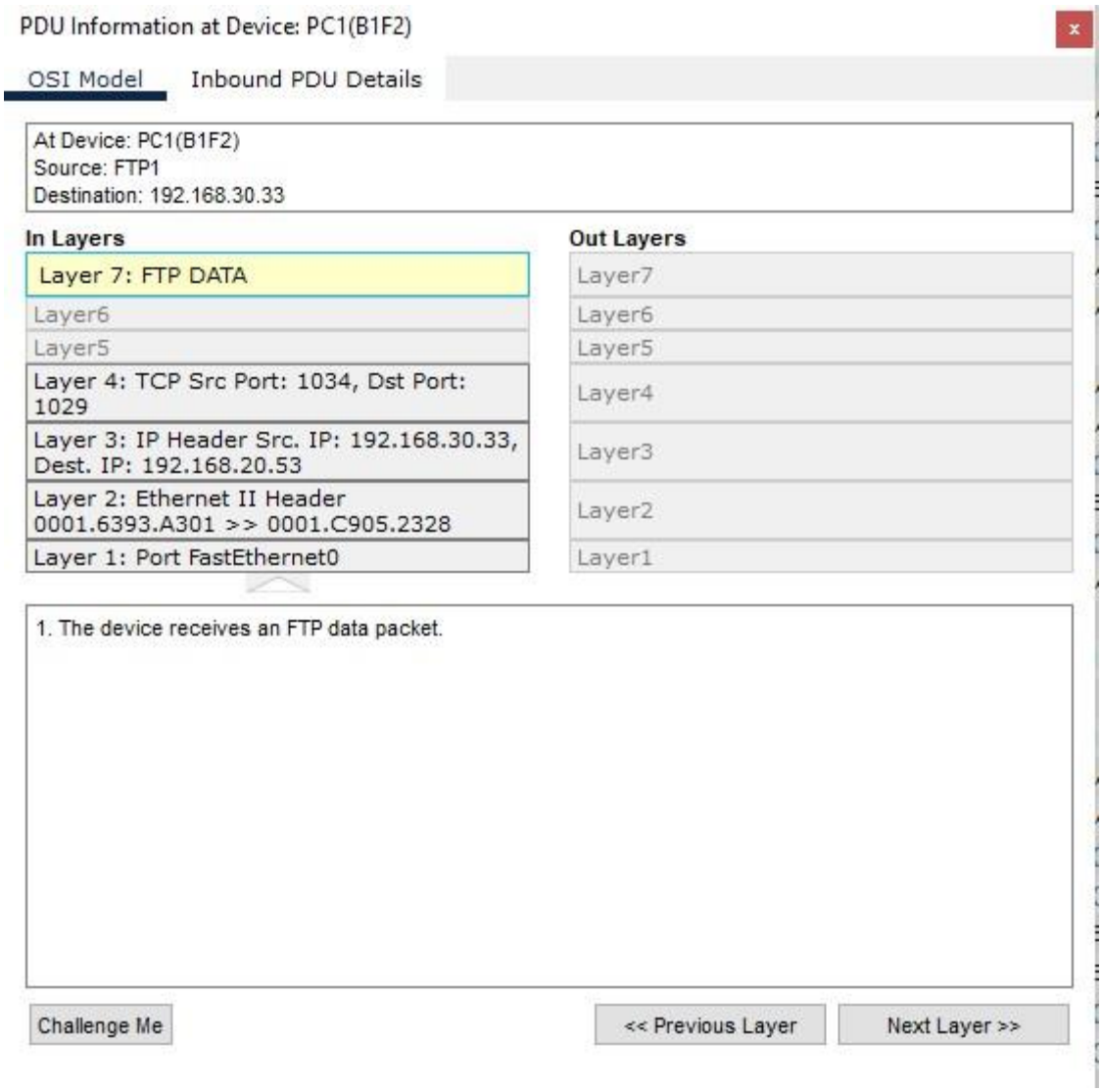
Simulation Panel

vent List

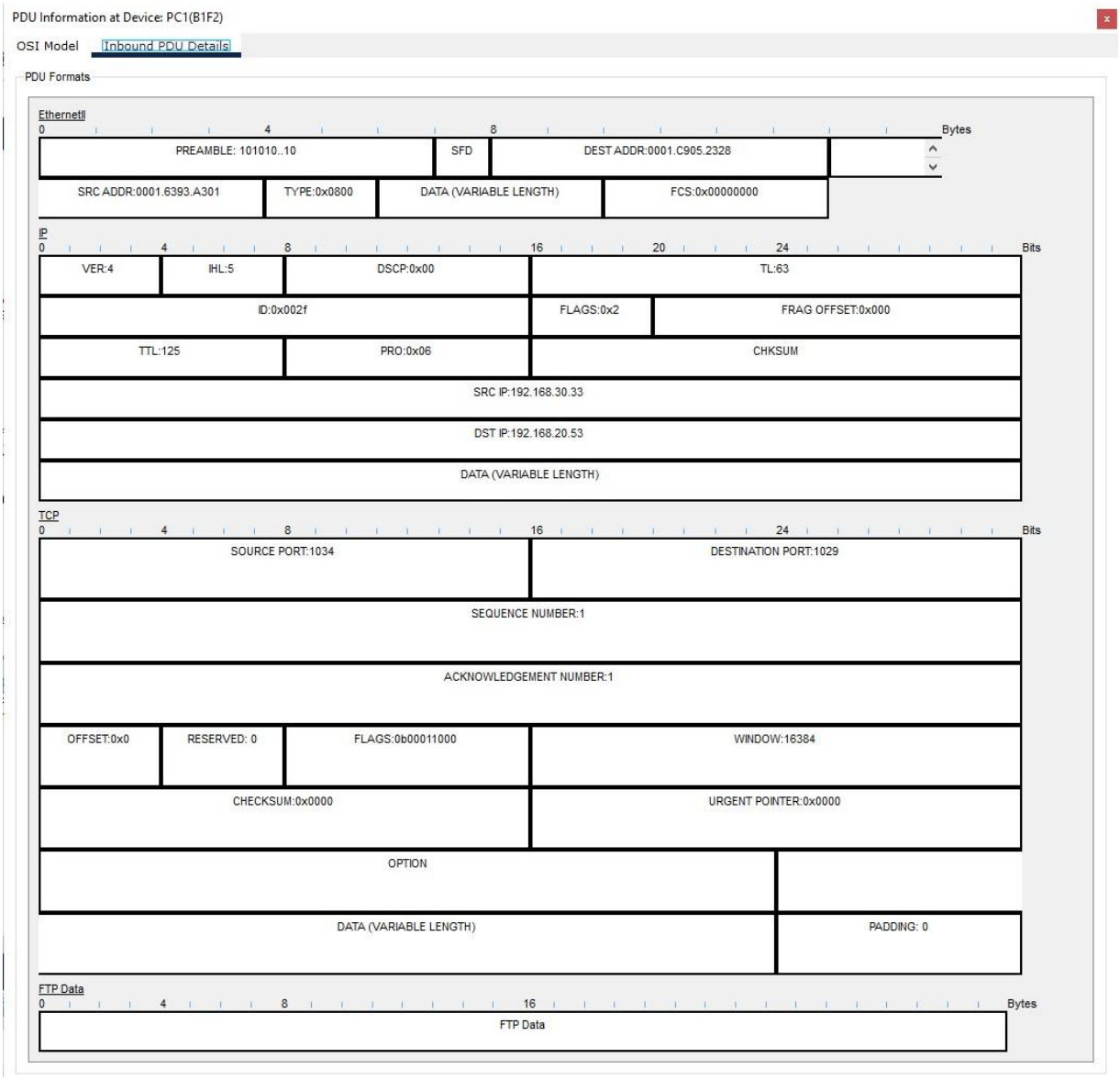
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1(B1F2)	FTP
	0.001	PC1(B1F2)	SwitchAll(B1F2)	FTP
	0.002	SwitchAll(B1F2)	Router(B1F2)	FTP
	0.003	Router(B1F2)	RouterB1	FTP
	0.004	RouterB1	Router(B1F3)	FTP
	0.005	Router(B1F3)	SwitchAll(Servers)	FTP
	0.006	SwitchAll(Servers)	SwitchAll(Other Serve...	FTP
	0.007	SwitchAll(Other Servers)	FTP1	FTP
	0.007	--	FTP1	FTP
	0.008	FTP1	SwitchAll(Other Serve...	FTP
	0.009	SwitchAll(Other Servers)	SwitchAll(Servers)	FTP
	0.010	SwitchAll(Servers)	Router(B1F3)	FTP
	0.011	Router(B1F3)	RouterB1	FTP
	0.012	RouterB1	Router(B1F2)	FTP
	0.013	Router(B1F2)	SwitchAll(B1F2)	FTP
	0.014	SwitchAll(B1F2)	PC1(B1F2)	FTP
	0.014	--	PC1(B1F2)	FTP
	0.015	PC1(B1F2)	SwitchAll(B1F2)	FTP
	0.016	SwitchAll(B1F2)	Router(B1F2)	FTP
	0.017	Router(B1F2)	RouterB1	FTP
	0.018	RouterB1	Router(B1F3)	FTP
	0.019	Router(B1F3)	SwitchAll(Servers)	FTP
	0.020	SwitchAll(Servers)	SwitchAll(Other Serve...	FTP
	0.021	SwitchAll(Other Servers)	FTP1	FTP
	0.021	--	FTP1	FTP
	0.022	FTP1	SwitchAll(Other Serve...	FTP
	0.023	SwitchAll(Other Servers)	SwitchAll(Servers)	FTP
	0.024	SwitchAll(Servers)	Router(B1F3)	FTP
	0.025	Router(B1F3)	RouterB1	FTP
	0.026	RouterB1	Router(B1F2)	FTP
	0.027	Router(B1F2)	SwitchAll(B1F2)	FTP
	0.028	SwitchAll(B1F2)	PC1(B1F2)	FTP
	0.028	--	PC1(B1F2)	FTP
	0.029	PC1(B1F2)	SwitchAll(B1F2)	FTP
	0.030	SwitchAll(B1F2)	Router(B1F2)	FTP
	0.031	Router(B1F2)	RouterB1	FTP
	0.032	RouterB1	Router(B1F3)	FTP
	0.033	Router(B1F3)	SwitchAll(Servers)	FTP
	0.034	SwitchAll(Servers)	SwitchAll(Other Serve...	FTP
	0.035	SwitchAll(Other Servers)	FTP1	FTP
	0.035	--	FTP1	FTP
	0.036	FTP1	SwitchAll(Other Serve...	FTP
	0.037	SwitchAll(Other Servers)	SwitchAll(Servers)	FTP
	0.038	SwitchAll(Servers)	Router(B1F3)	FTP
	0.039	Router(B1F3)	RouterB1	FTP
	0.040	RouterB1	Router(B1F2)	FTP
	0.041	Router(B1F2)	SwitchAll(B1F2)	FTP
	0.042	SwitchAll(B1F2)	PC1(B1F2)	FTP

	0.042	--	PC1(B1F2)		TCP
	0.043	PC1(B1F2)	SwitchAll(B1F2)		TCP
	0.044	SwitchAll(B1F2)	Router(B1F2)		TCP
	0.045	Router(B1F2)	RouterB1		TCP
	0.046	RouterB1	Router(B1F3)		TCP
	0.047	Router(B1F3)	SwitchAll(Servers)		TCP
	0.048	SwitchAll(Servers)	SwitchAll(Other Serve...		TCP
	0.049	SwitchAll(Other Servers)	FTP1		TCP
	0.050	FTP1	SwitchAll(Other Serve...		TCP
	0.051	SwitchAll(Other Servers)	SwitchAll(Servers)		TCP
	0.052	SwitchAll(Servers)	Router(B1F3)		TCP
	0.053	Router(B1F3)	RouterB1		TCP
	0.054	RouterB1	Router(B1F2)		TCP
	0.055	Router(B1F2)	SwitchAll(B1F2)		TCP
	0.056	SwitchAll(B1F2)	PC1(B1F2)		TCP
	0.057	--	PC1(B1F2)		TCP
	0.057	PC1(B1F2)	SwitchAll(B1F2)		TCP
	0.057	--	PC1(B1F2)		TCP
	0.058	PC1(B1F2)	SwitchAll(B1F2)		TCP
	0.058	SwitchAll(B1F2)	Router(B1F2)		TCP
	0.059	SwitchAll(B1F2)	Router(B1F2)		TCP
	0.059	Router(B1F2)	RouterB1		TCP
	0.060	Router(B1F2)	RouterB1		TCP
	0.060	RouterB1	Router(B1F3)		TCP
	0.061	RouterB1	Router(B1F3)		TCP
	0.061	Router(B1F3)	SwitchAll(Servers)		TCP
	0.062	Router(B1F3)	SwitchAll(Servers)		TCP
	0.062	SwitchAll(Servers)	SwitchAll(Other Serve...		TCP
	0.063	SwitchAll(Servers)	SwitchAll(Other Serve...		TCP
	0.063	SwitchAll(Other Servers)	FTP1		TCP
	0.063	--	FTP1		FTP
	0.064	SwitchAll(Other Servers)	FTP1		TCP
	0.064	FTP1	SwitchAll(Other Serve...		FTP
	0.065	SwitchAll(Other Servers)	SwitchAll(Servers)		FTP
	0.066	SwitchAll(Servers)	Router(B1F3)		FTP
	0.067	Router(B1F3)	RouterB1		FTP
	0.068	RouterB1	Router(B1F2)		FTP
	0.069	Router(B1F2)	SwitchAll(B1F2)		FTP
Visible	0.070	SwitchAll(B1F2)	PC1(B1F2)		FTP

Event List of Get File



OSI Model of File Sent Message

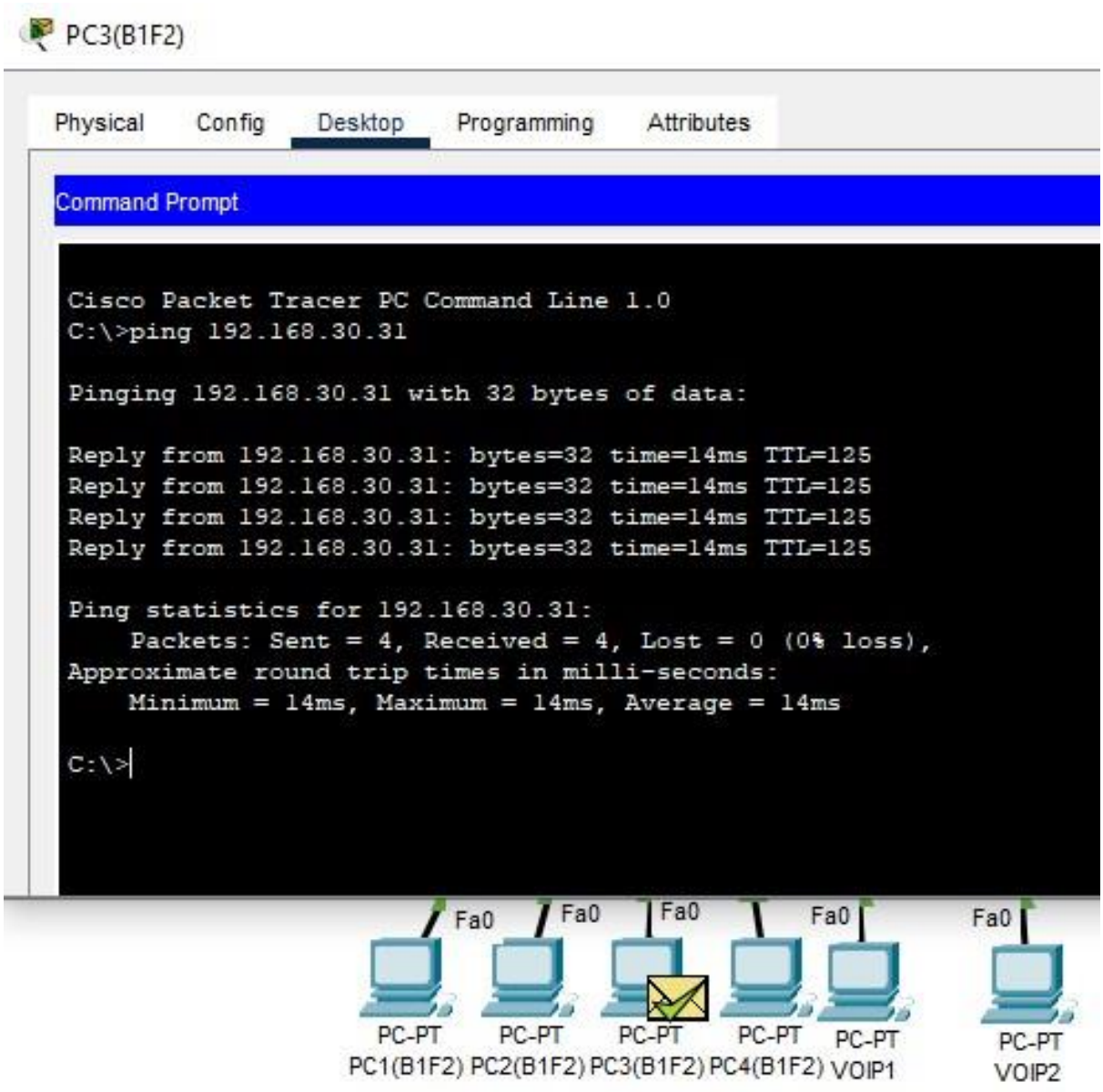


Inbound PDU Details of the Packet That Tells the File is Sent

Simulation 9: A pc user from second facility of first branch office wants to ping the DNS server.

PC3(B1F2) at branch 1 facility 2 has used the following path to ping the DNS server at branch 1 facility 3:

PC3(B1F2), SwitchAll(B1F2), Router(B1F2), RouterB1, Router(B1F3), SwitchAll(Servers), SwitchAll(Other Servers), DNS.

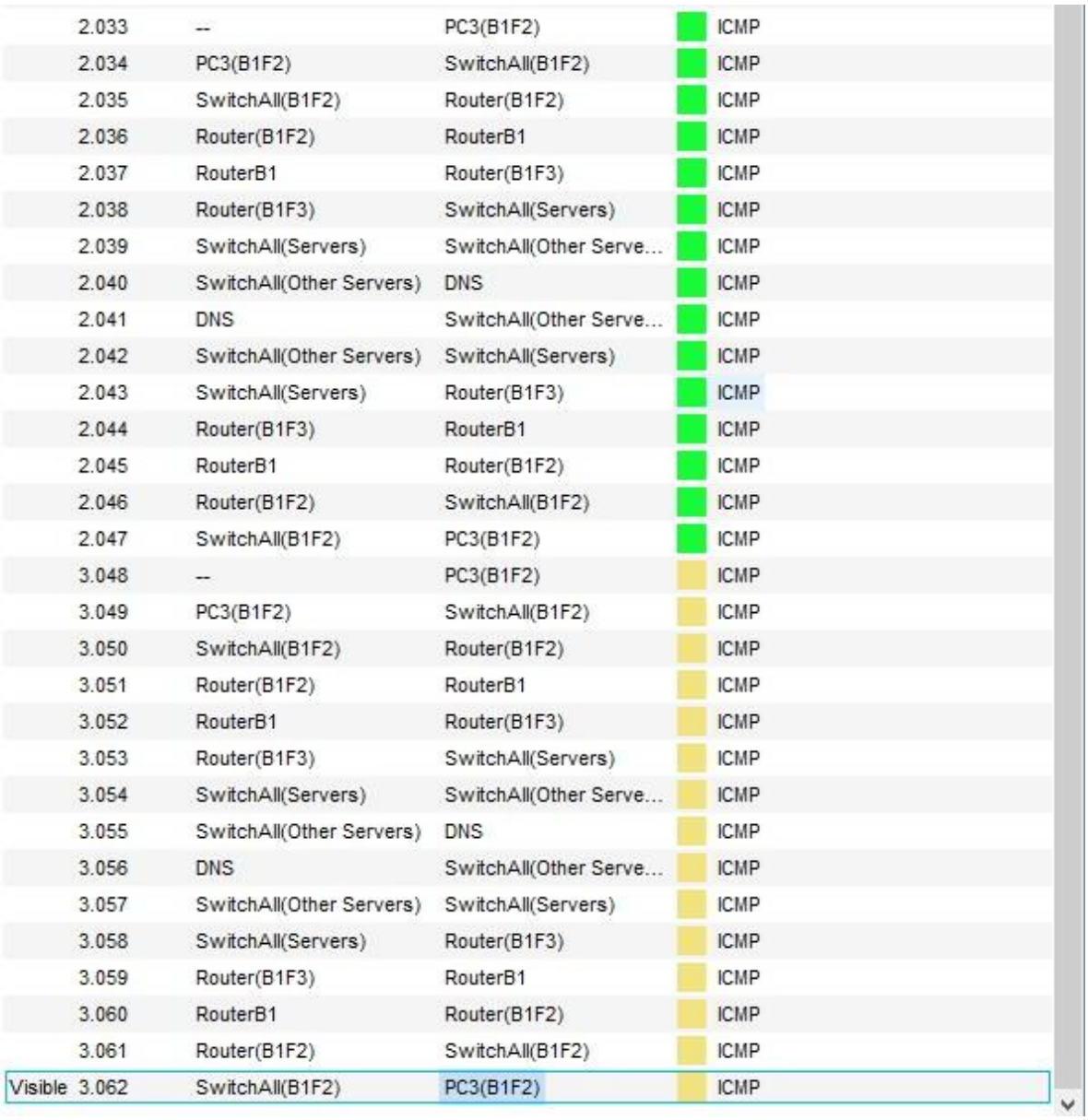


Result of Ping

Simulation Panel

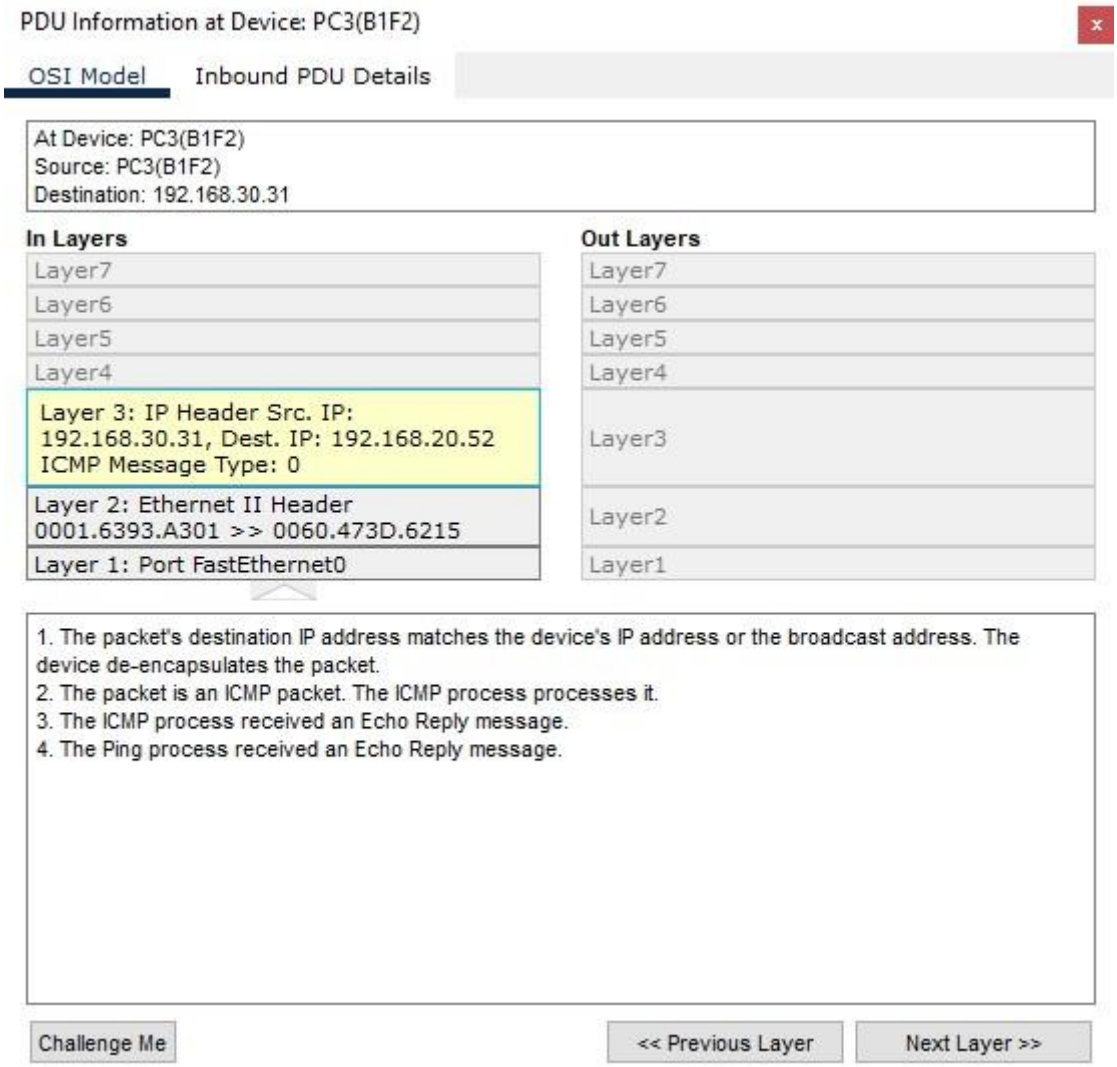
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC3(B1F2)	ICMP
	0.001	PC3(B1F2)	SwitchAll(B1F2)	ICMP
	0.002	SwitchAll(B1F2)	Router(B1F2)	ICMP
	0.003	Router(B1F2)	RouterB1	ICMP
	0.004	RouterB1	Router(B1F3)	ICMP
	0.005	Router(B1F3)	SwitchAll(Servers)	ICMP
	0.006	SwitchAll(Servers)	SwitchAll(Other Serve...	ICMP
	0.007	SwitchAll(Other Servers)	DNS	ICMP
	0.008	DNS	SwitchAll(Other Serve...	ICMP
	0.009	SwitchAll(Other Servers)	SwitchAll(Servers)	ICMP
	0.010	SwitchAll(Servers)	Router(B1F3)	ICMP
	0.011	Router(B1F3)	RouterB1	ICMP
	0.012	RouterB1	Router(B1F2)	ICMP
	0.013	Router(B1F2)	SwitchAll(B1F2)	ICMP
	0.014	SwitchAll(B1F2)	PC3(B1F2)	ICMP
	1.017	--	PC3(B1F2)	ICMP
	1.018	PC3(B1F2)	SwitchAll(B1F2)	ICMP
	1.019	SwitchAll(B1F2)	Router(B1F2)	ICMP
	1.020	Router(B1F2)	RouterB1	ICMP
	1.021	RouterB1	Router(B1F3)	ICMP
	1.022	Router(B1F3)	SwitchAll(Servers)	ICMP
	1.023	SwitchAll(Servers)	SwitchAll(Other Serve...	ICMP
	1.024	SwitchAll(Other Servers)	DNS	ICMP
	1.025	DNS	SwitchAll(Other Serve...	ICMP
	1.026	SwitchAll(Other Servers)	SwitchAll(Servers)	ICMP
	1.027	SwitchAll(Servers)	Router(B1F3)	ICMP
	1.028	Router(B1F3)	RouterB1	ICMP
	1.029	RouterB1	Router(B1F2)	ICMP
	1.030	Router(B1F2)	SwitchAll(B1F2)	ICMP
	1.031	SwitchAll(B1F2)	PC3(B1F2)	ICMP

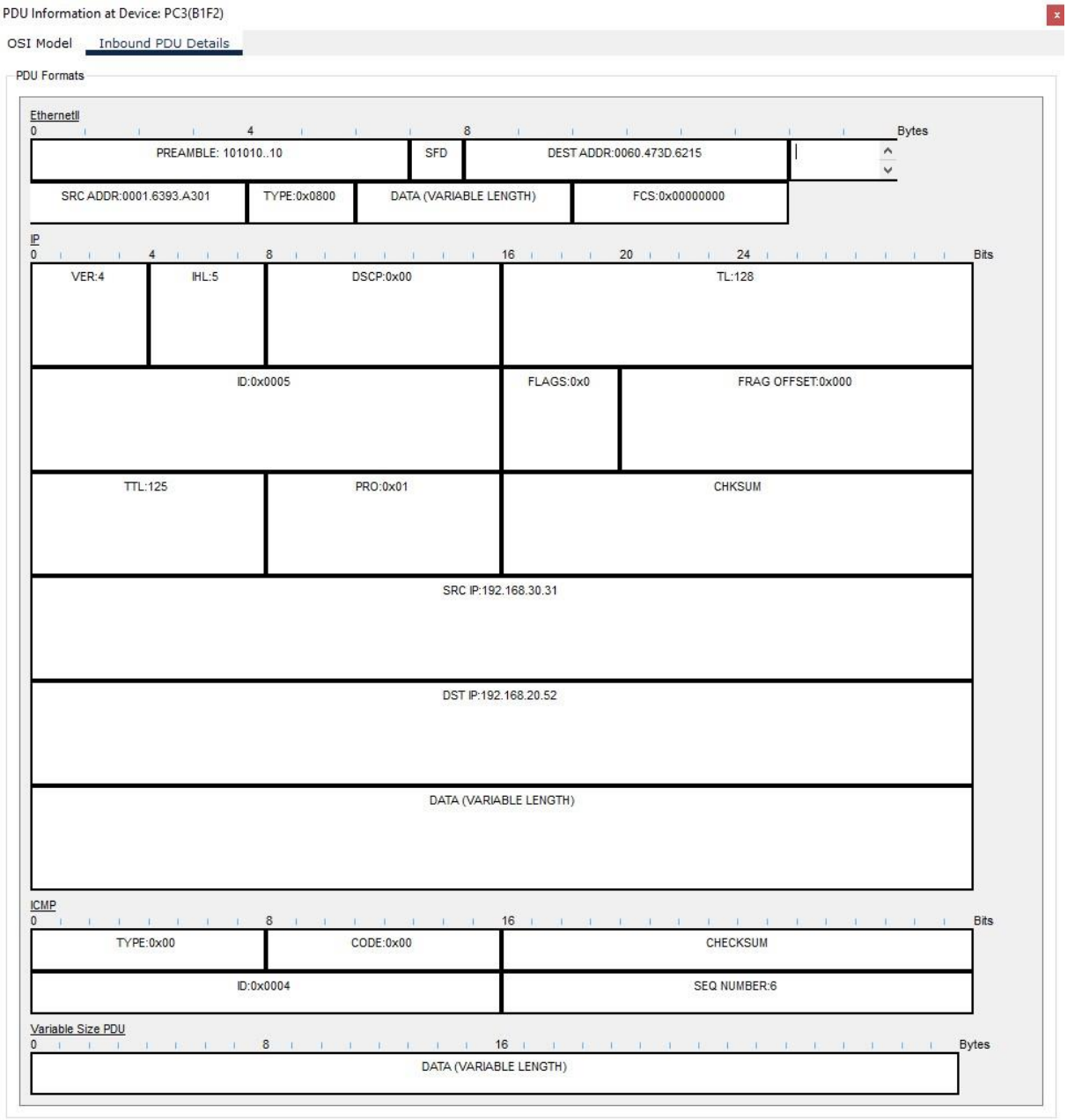


	2.033	--	PC3(B1F2)		ICMP
	2.034	PC3(B1F2)	SwitchAll(B1F2)		ICMP
	2.035	SwitchAll(B1F2)	Router(B1F2)		ICMP
	2.036	Router(B1F2)	RouterB1		ICMP
	2.037	RouterB1	Router(B1F3)		ICMP
	2.038	Router(B1F3)	SwitchAll(Servers)		ICMP
	2.039	SwitchAll(Servers)	SwitchAll(Other Serve...		ICMP
	2.040	SwitchAll(Other Servers)	DNS		ICMP
	2.041	DNS	SwitchAll(Other Serve...		ICMP
	2.042	SwitchAll(Other Servers)	SwitchAll(Servers)		ICMP
	2.043	SwitchAll(Servers)	Router(B1F3)		ICMP
	2.044	Router(B1F3)	RouterB1		ICMP
	2.045	RouterB1	Router(B1F2)		ICMP
	2.046	Router(B1F2)	SwitchAll(B1F2)		ICMP
	2.047	SwitchAll(B1F2)	PC3(B1F2)		ICMP
	3.048	--	PC3(B1F2)		ICMP
	3.049	PC3(B1F2)	SwitchAll(B1F2)		ICMP
	3.050	SwitchAll(B1F2)	Router(B1F2)		ICMP
	3.051	Router(B1F2)	RouterB1		ICMP
	3.052	RouterB1	Router(B1F3)		ICMP
	3.053	Router(B1F3)	SwitchAll(Servers)		ICMP
	3.054	SwitchAll(Servers)	SwitchAll(Other Serve...		ICMP
	3.055	SwitchAll(Other Servers)	DNS		ICMP
	3.056	DNS	SwitchAll(Other Serve...		ICMP
	3.057	SwitchAll(Other Servers)	SwitchAll(Servers)		ICMP
	3.058	SwitchAll(Servers)	Router(B1F3)		ICMP
	3.059	Router(B1F3)	RouterB1		ICMP
	3.060	RouterB1	Router(B1F2)		ICMP
	3.061	Router(B1F2)	SwitchAll(B1F2)		ICMP
Visible	3.062	SwitchAll(B1F2)	PC3(B1F2)		ICMP

Event List of Ping



OSI Model of Ping Packet



Inbound PDU Details of the last packet that is received by PC3

4. Conclusion

Based on the results of the project, we obtained significant findings regarding the Metropolitan Area Network (MAN) simulation and design. We designed a network that connects two different branches and meets the specific needs of each branch. In this design process, we identified the architecture and components of the network by considering the requirements of each branch and the needs of its users.

The primary purpose of our network design was to meet the communication needs of both branches and provide an efficient working environment. Accordingly, we provided specialized devices and services for each branch and optimized access to these services. Additionally, we used appropriate routing and switching strategies to enhance the overall performance of the network.

Our project allowed us to improve our skills in network simulation and design and address real-world scenarios. Moreover, it provided us with the opportunity to understand the complexity of network design and integrate various network components. This experience will help us be more effective and efficient in future network projects.

In conclusion, the project requirements were successfully fulfilled, and it equipped us with significant skills in network design and simulation. It also enabled us to develop solutions aligned with real-world scenarios. The findings we obtained contributed to a deeper understanding of network technologies and applications. This project laid the foundation for further advancing our knowledge and abilities in network engineering and computer networks.

5. References

[1] - Learn With Mukul. (2023, April 24). *DHCP (Dynamic Host Configuration Protocol) server using dynamic routing in Cisco Packet Tracer* | [Video]. YouTube. https://www.youtube.com/watch?v=fbnxNLy3YFY

[2] - ODDHYAN. (2022, August 22). *Configure Vlan and VoIP using Cisco Packet Tracer | ODDHYAN* [Video]. YouTube. https://www.youtube.com/watch?v=v20qsXTN2A4

[3] - Dr. Bryan Marshall. (2022, October 5). *Packet Tracer - Routers and email server* [Video]. YouTube. https://www.youtube.com/watch?v=GZng7ZUldqk

[4] - Anubhav Singh. (2018, March 15). *FTP server Cisco Packet Tracer* [Video]. YouTube. https://www.youtube.com/watch?v=MPTrbFzIn0Y

[5] - Cisco Packet Tracer Tutorial. (2017, August 12). *DNS and Web Server using Cisco Packet tracer* [Video]. YouTube. https://www.youtube.com/watch?v=JA8t_IEXcHc

[6] - Network TechZone. (2022, May 4). *Configuration of SSH in Cisco Router using Username and Password* [Video]. YouTube. https://www.youtube.com/watch?v=9G-o6WnynU4

[7] - Network for you. (2023, May 28). *34.How to Connect Head Office with Branch Office by using RIP? | CCNA 200-301 | Networkforyou* [Video]. YouTube. https://www.youtube.com/watch?v=XC7Q53ZjZdA

[8] - GeeksforGeeks. (2023, May 9). *Routing Information Protocol (RIP)*. GeeksforGeeks. https://www.geeksforgeeks.org/routing-information-protocol-rip/

[9] - GeeksforGeeks. (2022, September 21). *Computer network cheat sheet*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-network-cheat-sheet/