

AIM: Create the following servers using CISCO Packet Tracer.

- i) DHCP Server
- ii) DNS Server
- iii) FTP Server
- iv) EMAIL Server

THEORY:**i)DHCP Server****Introduction to DHCP Server:**

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the assignment of IP addresses, subnet masks, default gateways, and other network configuration parameters to devices on a network. DHCP servers dynamically allocate IP addresses from a predefined pool, simplifying network administration and ensuring efficient resource utilization. This protocol streamlines the process of network configuration, especially in environments with a large number of devices or frequent changes to network topology.

Advantages:

1. **Simplified Network Management:** DHCP automates the assignment of IP addresses, eliminating the need for manual configuration on individual devices. This reduces administrative overhead and minimizes the risk of configuration errors.
2. **Efficient Resource Allocation:** DHCP servers manage IP address allocation from a pool of available addresses, ensuring optimal utilization of IP address space within the network.
3. **Centralized Control:** Administrators can centrally manage DHCP settings and configurations, making it easier to implement changes, updates, and policy enforcement across the network.
4. **Flexibility and Scalability:** DHCP accommodates network growth and device mobility by dynamically assigning IP addresses to new devices and reallocating addresses as needed. This scalability feature is particularly beneficial in environments with a dynamic or expanding user base.
5. **Reduced Configuration Time:** DHCP significantly reduces the time required to configure new devices on the network, allowing users to connect and access network resources quickly and efficiently.

Disadvantages:

1. **Dependency on DHCP Server:** If the DHCP server becomes unavailable or malfunctions, devices may be unable to obtain IP addresses, leading to network connectivity issues.
2. **Potential for IP Address Conflicts:** Improperly configured DHCP servers or overlapping IP address ranges can result in address conflicts, causing network disruptions and connectivity issues.
3. **Security Concerns:** DHCP lacks inherent authentication mechanisms, making it susceptible to rogue DHCP servers and unauthorized IP address assignments. This vulnerability can be exploited for malicious purposes, such as network eavesdropping or unauthorized access.
4. **Limited Support for Network Devices:** Some network devices, such as printers, servers, and network appliances, may require static IP addresses for specific configurations or services. DHCP may not adequately support these devices, requiring manual intervention for address assignment.
5. **Performance Overhead:** DHCP transactions involve communication between clients and the server, which can introduce latency and overhead, especially in large-scale networks with high client turnover.

Real-World Application:

1. **Enterprise Networks:** DHCP is extensively used in enterprise networks to streamline IP address management for computers, mobile devices, and other networked devices. It simplifies the deployment of new devices and facilitates centralized management of network resources.
2. **Internet Service Providers (ISPs):** ISPs deploy DHCP servers to dynamically assign IP addresses to residential and business customers. This approach optimizes IP address utilization and enables ISPs to efficiently manage their address allocation resources.
3. **Public Wi-Fi Networks:** Public Wi-Fi hotspots, such as those in airports, cafes, and hotels, often utilize DHCP to provide seamless connectivity to users. DHCP enables quick and automated IP address assignment to mobile devices and laptops, enhancing the user experience.
4. **Home Networks:** DHCP is commonly used in home networks to allocate IP addresses to devices such as computers, smartphones, smart TVs, and gaming consoles. It simplifies network setup and maintenance for non-technical users, ensuring hassle-free connectivity within the home environment.
5. **Virtual Private Networks (VPNs):** DHCP is integrated into VPN solutions to assign IP addresses to remote clients connecting to the corporate network. This dynamic addressing scheme facilitates secure remote access and enables efficient resource utilization within the VPN infrastructure.

ii)DNS Server

Introduction to DNS Server:

The Domain Name System (DNS) is a critical component of the internet infrastructure that translates human-readable domain names into machine-readable IP addresses. DNS servers are responsible for resolving domain names to their corresponding IP addresses, enabling users to access websites, send emails, and connect to various internet services. DNS plays a pivotal role in simplifying internet navigation, enhancing accessibility, and facilitating efficient communication across global networks.

Advantages:

1. **Human-Readable Naming:** DNS allows users to access internet resources using easily memorable domain names (e.g., www.example.com) instead of complex IP addresses. This enhances usability and simplifies web navigation for users.
2. **Centralized Management:** DNS enables centralized management of domain name records, allowing administrators to update and maintain DNS configurations efficiently. This centralized approach streamlines the management of large-scale networks and facilitates rapid changes to domain configurations.
3. **Redundancy and Load Distribution:** DNS supports redundancy and load distribution through techniques like DNS caching and round-robin DNS. Caching reduces the response time for frequently accessed domain names, while round-robin DNS distributes traffic evenly among multiple servers to improve performance and reliability.
4. **Scalability:** DNS is highly scalable and can accommodate the growing demands of the internet by adding additional DNS servers and implementing hierarchical DNS structures. This scalability ensures that DNS infrastructure can handle increasing internet traffic and domain registrations.
5. **Fault Tolerance:** DNS supports fault tolerance through mechanisms like DNS replication and secondary DNS servers. Replication ensures that DNS records are duplicated across multiple servers, reducing the risk of service disruptions due to server failures or network outages.

Disadvantages:

1. **Single Point of Failure:** DNS servers represent a single point of failure in the network. If a DNS server becomes unavailable due to hardware failure, software issues, or network problems, it can result in service disruptions and make internet resources inaccessible.
2. **Security Vulnerabilities:** DNS is susceptible to various security threats, including DNS spoofing, cache poisoning, and distributed denial-of-service (DDoS) attacks. These vulnerabilities can compromise the integrity, availability, and confidentiality of DNS infrastructure and undermine trust in internet communications.
3. **Propagation Delays:** DNS changes, such as updates to domain records or changes in DNS configurations, may take time to propagate throughout the DNS hierarchy.

Propagation delays can lead to inconsistencies in DNS resolution and temporary disruptions in internet services.

4. **DNS Amplification Attacks:** DNS servers can be exploited in DNS amplification attacks, where attackers abuse DNS queries to generate large volumes of traffic directed at target servers. These attacks can overwhelm network resources, causing service degradation or outages.
5. **Complexity of Configuration:** Configuring and managing DNS servers can be complex, particularly in large-scale networks with multiple domains, subdomains, and complex DNS configurations. Administrators may require specialized knowledge and tools to effectively manage DNS infrastructure.

Real-World Application:

1. **Web Browsing:** DNS is integral to web browsing, as it translates domain names (e.g., www.google.com) into IP addresses, allowing users to access websites and web services.
2. **Email Communication:** DNS is used to resolve domain names in email addresses, enabling email clients to send and receive messages across the internet.
3. **File Sharing:** DNS facilitates file sharing and data transfer by resolving domain names to IP addresses, allowing users to access remote servers and network resources.
4. **Remote Access:** DNS is employed in remote access solutions, such as virtual private networks (VPNs), to resolve domain names for remote servers and enable secure access to corporate networks.
5. **Content Delivery Networks (CDNs):** CDNs rely on DNS to route user requests to geographically distributed servers, optimizing content delivery and improving website performance for global audiences.

iii)FTP Server

Introduction to FTP Server:

The File Transfer Protocol (FTP) is a standard network protocol used for transferring files between a client and a server on a computer network. FTP servers store and manage files that can be accessed and downloaded by authorized users or clients using FTP client software. FTP facilitates the efficient exchange of files over networks, enabling users to share documents, images, software updates, and other data resources.

Advantages:

1. **Ease of File Transfer:** FTP simplifies the process of transferring files between computers and servers over a network. Users can upload, download, and manage files remotely using FTP client software with minimal effort.
2. **Cross-Platform Compatibility:** FTP is supported by various operating systems and platforms, making it a versatile solution for file transfer across diverse computing

environments. Users can access FTP servers from Windows, macOS, Linux, and other operating systems.

3. **Flexible Authentication:** FTP servers support multiple authentication methods, including username/password authentication and anonymous access. Administrators can configure access controls to restrict or grant permissions based on user credentials and roles.
4. **Efficient Bandwidth Utilization:** FTP optimizes bandwidth utilization during file transfer by employing data compression and binary transfer modes. This ensures faster transfer speeds and efficient use of network resources, particularly for large files or bulk data transfers.
5. **Remote File Management:** FTP servers provide remote file management capabilities, allowing users to organize, rename, delete, and move files and directories on the server. This remote administration feature enhances productivity and workflow efficiency.

Disadvantages:

1. **Security Concerns:** FTP transmits data in plain text, making it vulnerable to eavesdropping, data interception, and unauthorized access. Without encryption, sensitive information such as usernames, passwords, and file contents may be exposed to security risks.
2. **Limited Data Protection:** FTP lacks built-in mechanisms for data integrity and encryption, increasing the risk of data corruption or tampering during transmission. Without encryption, sensitive data may be susceptible to interception or manipulation by malicious actors.
3. **Firewall and NAT Issues:** FTP can encounter compatibility issues with firewalls and network address translation (NAT) devices due to its use of separate control and data connections. Passive FTP mode may require additional configuration to traverse firewalls and NATs, leading to connectivity issues for some users.
4. **Complexity of Configuration:** Setting up and configuring an FTP server can be complex, particularly for users with limited networking or server administration experience. Administrators may need to configure firewall rules, user permissions, and security settings to ensure proper functionality and protection.
5. **File Transfer Overhead:** FTP introduces overhead during file transfer, including control messages, acknowledgments, and connection establishment procedures. This overhead may impact transfer speeds and efficiency, especially for small files or frequent transfers.

Real-World Application:

1. **Website Hosting:** FTP servers are commonly used by web hosting providers to allow website owners to upload and manage website files, including HTML documents, images, scripts, and multimedia content.

2. **Software Distribution:** FTP servers serve as repositories for software distribution, enabling software developers and vendors to distribute application updates, patches, and installation files to users and clients.
3. **Data Backup and Archiving:** Organizations use FTP servers for data backup and archiving purposes, allowing users to securely transfer and store backup copies of critical files and databases offsite for disaster recovery and compliance purposes.
4. **Media Sharing:** FTP servers facilitate media sharing and content distribution, allowing users to upload and share multimedia files, music, videos, and digital assets with friends, colleagues, or the public.
5. **Remote Access and Collaboration:** FTP servers support remote access and collaboration among geographically dispersed teams, enabling users to access shared files, documents, and project resources from any location with internet connectivity.

iv)Email Server

Introduction to Email Server:

An Email Server is a computer program or hardware appliance that manages and facilitates the exchange of electronic mail (email) messages between users within a computer network or across the internet. Email servers store, send, receive, and route email messages, providing users with the ability to communicate asynchronously via electronic mail. Email servers support various protocols such as SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), and POP3 (Post Office Protocol version 3) to handle the transmission, retrieval, and storage of email messages.

Advantages:

1. **Efficient Communication:** Email servers enable fast and efficient communication between individuals, organizations, and businesses, regardless of geographic location. Users can send and receive messages instantly, reducing the need for traditional mail or telephone communication.
2. **Global Reach:** Email servers facilitate communication on a global scale, allowing users to exchange messages with individuals and organizations worldwide. This global reach promotes international collaboration, networking, and information sharing across diverse geographical regions and time zones.
3. **Cost-Effective:** Email servers offer a cost-effective means of communication compared to traditional mail or courier services. Sending electronic messages incurs minimal costs, making email an affordable option for personal and business communication.
4. **Flexibility and Accessibility:** Email servers provide users with flexibility and accessibility, allowing them to access their email accounts from multiple devices and locations. Users can send, receive, and manage email messages using desktop email clients, webmail interfaces, or mobile email apps.

5. **Enhanced Productivity:** Email servers enhance productivity by enabling efficient communication, collaboration, and information sharing among individuals and teams. Users can exchange messages, documents, and multimedia content to facilitate decision-making, project coordination, and task management.

Disadvantages:

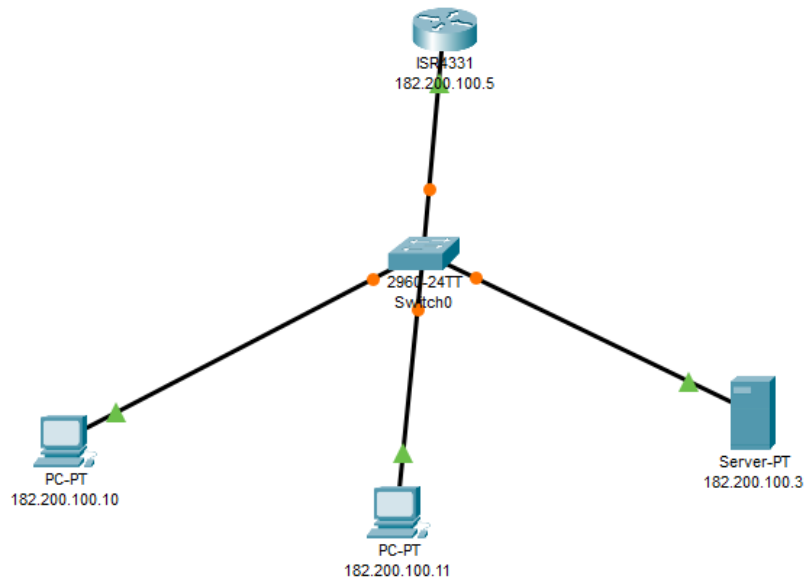
1. **Security Risks:** Email servers are susceptible to various security threats, including phishing attacks, malware, spam, and data breaches. Vulnerabilities in email protocols or server configurations can compromise the confidentiality, integrity, and availability of email communications and sensitive information.
2. **Spam and Unsolicited Emails:** Email servers often receive large volumes of spam and unsolicited emails, leading to cluttered inboxes, wasted storage space, and potential security risks. Managing spam filters and implementing anti-spam measures are essential to mitigate these issues.
3. **Email Overload:** Email servers may contribute to email overload, where users receive an excessive number of emails, leading to information overload, stress, and reduced productivity. Effective email management strategies, such as prioritization, filtering, and organization, can help users cope with email overload.
4. **Email Downtime:** Email servers may experience downtime due to hardware failures, software issues, network outages, or maintenance activities. Email downtime can disrupt communication and business operations, resulting in lost productivity, missed opportunities, and customer dissatisfaction.
5. **Privacy Concerns:** Email servers raise privacy concerns related to the collection, storage, and processing of personal and sensitive information contained in email messages. Ensuring compliance with data protection regulations and implementing encryption and access controls are essential to safeguard user privacy.

Real-World Application:

1. **Business Communication:** Email servers are widely used in business environments for internal and external communication, including employee correspondence, customer support, sales inquiries, and marketing campaigns.
2. **Academic Institutions:** Email servers are utilized by academic institutions for faculty-student communication, course announcements, administrative notifications, and research collaboration.
3. **Government Agencies:** Government agencies rely on email servers for official correspondence, public announcements, information dissemination, and inter-agency communication.
4. **Healthcare Organizations:** Email servers are employed by healthcare organizations for patient communication, appointment reminders, medical records exchange, and healthcare coordination.

5. **Personal Communication:** Email servers serve as a primary means of personal communication for individuals, families, and social groups, facilitating communication with friends, relatives, and acquaintances.

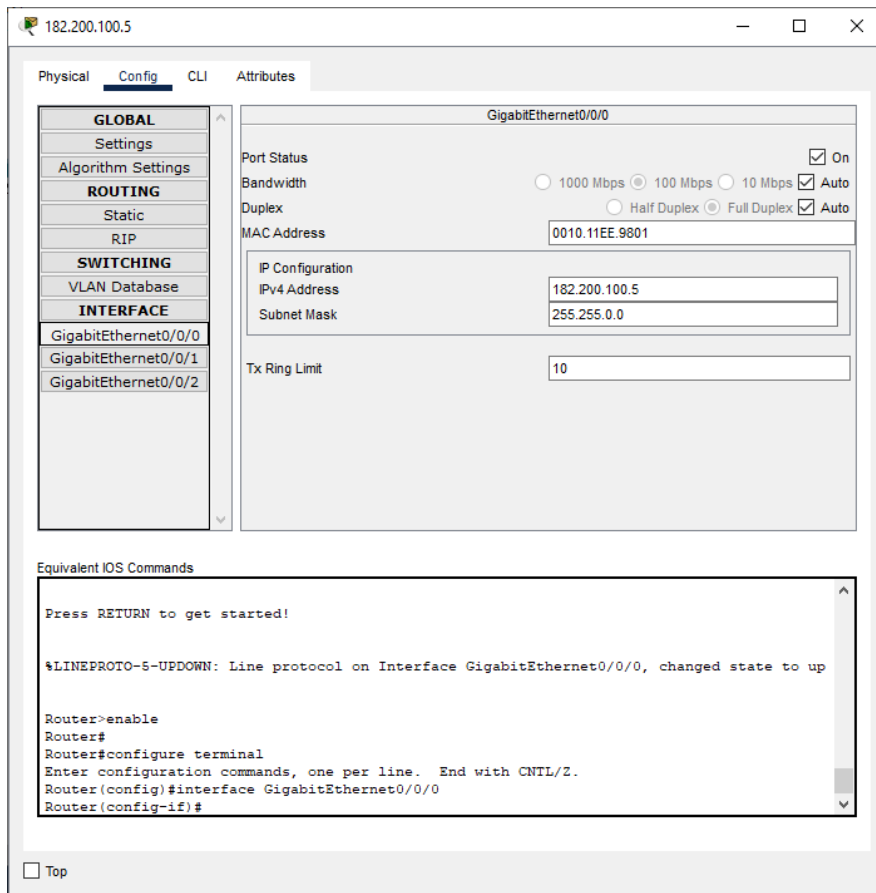
i) Network Structure for DHCP Server



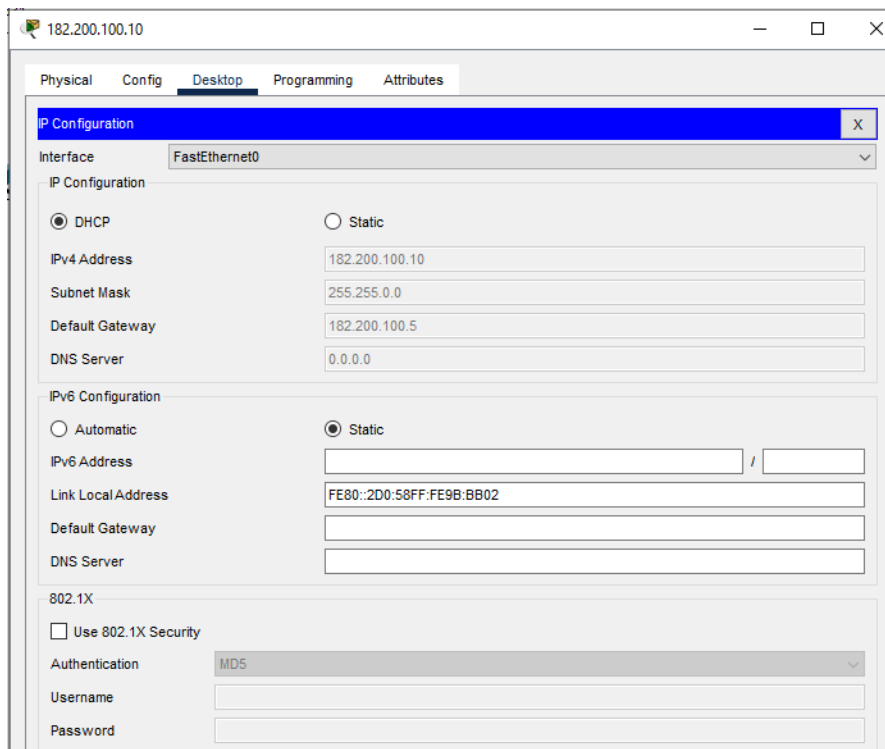
Configuration of DHCP server

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	182.200....	0.0.0.0	182.200....	255.255....	512	0.0.0.0	0.0.0.0

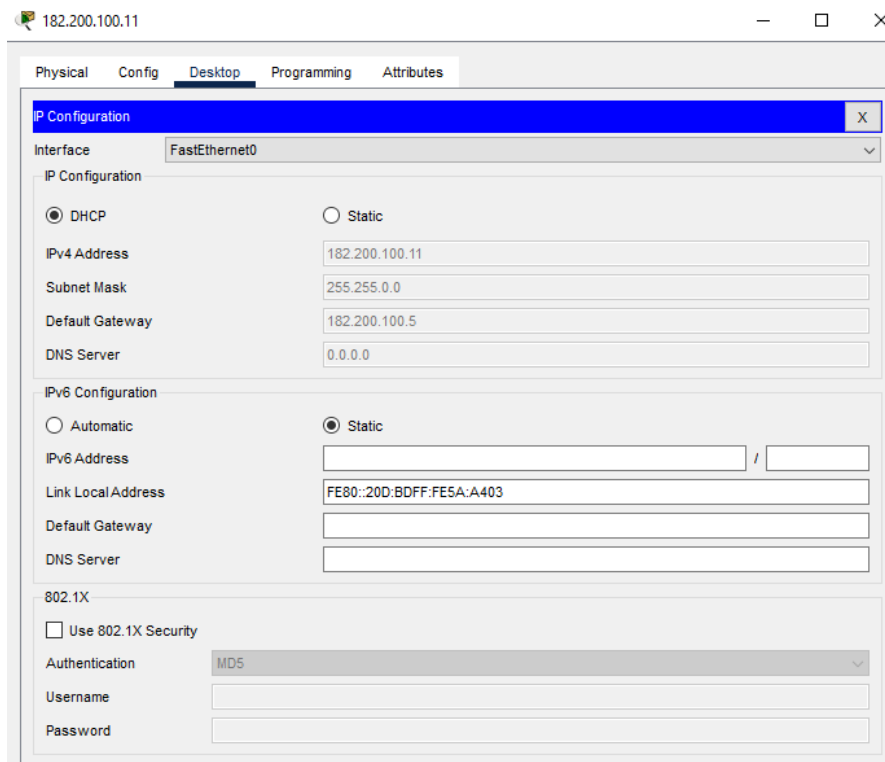
Configuration of Server



Configuration of PC1



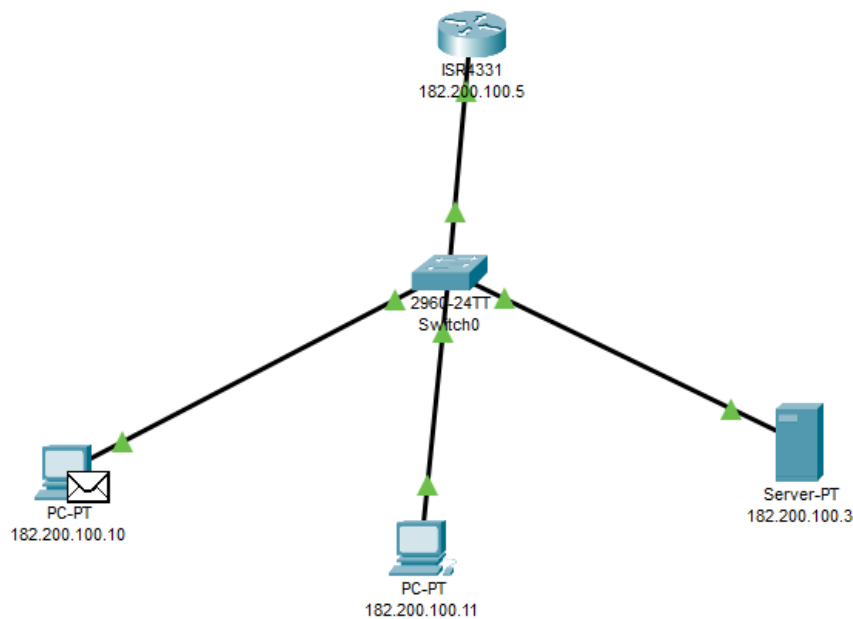
Configuration of PC2



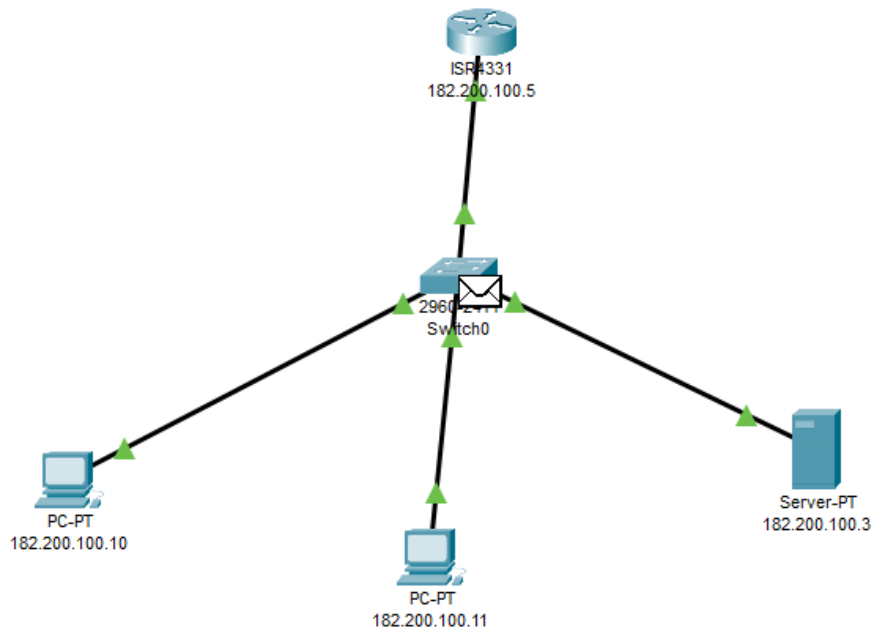
Verification of Connectivity for DHCP Server:

Sending a Simple PDU from PC 182.200.100.10 to PC 182.200.100.11

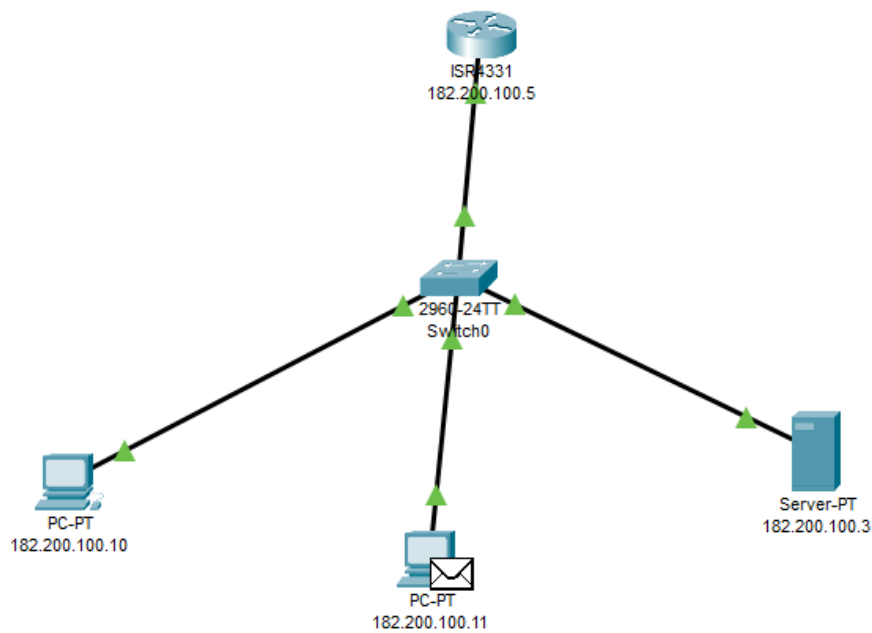
Step1:



Step2:

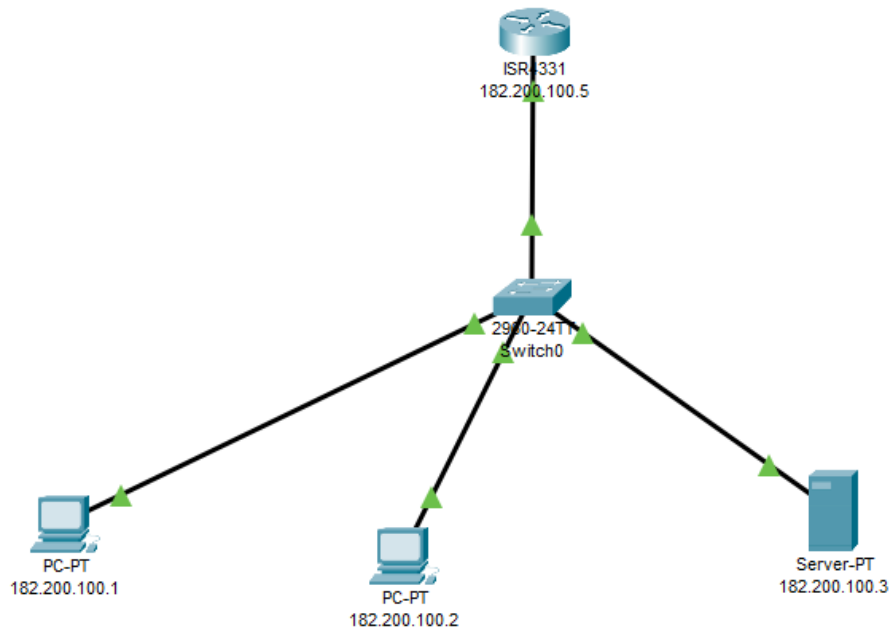


Step3:



A Simple PDU was sent successfully from PC 182.200.100.10 to PC 182.200.100.11

ii) Network Structure for DNS Server



Configuration of DNS server

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

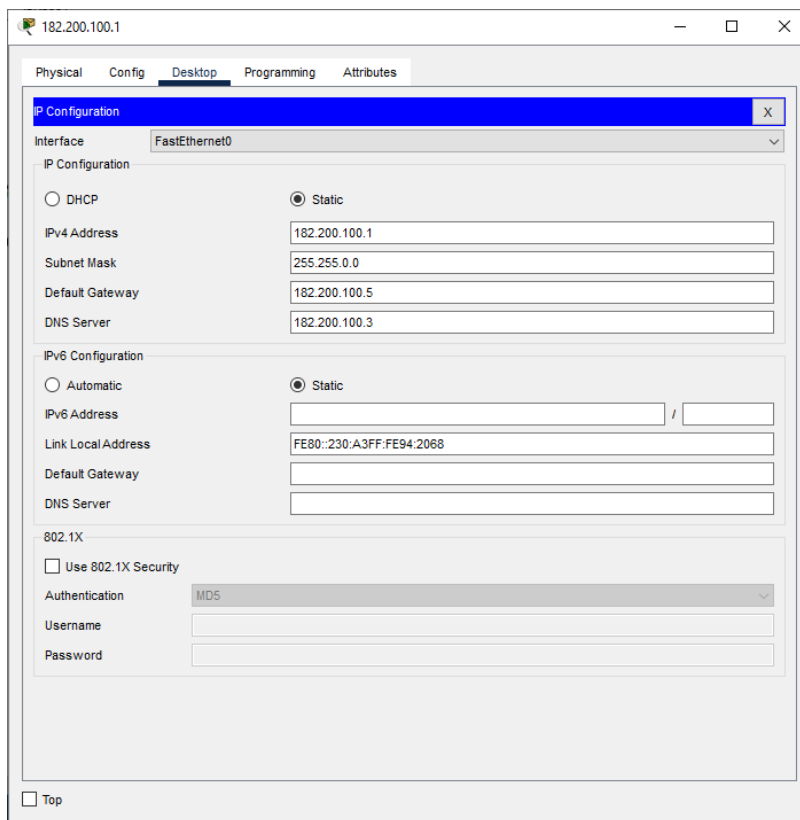
Name Type

Address

No.	Name	Type	Detail
0	www.diggaj.com	ARecord	182.200.100.3

☐ Top

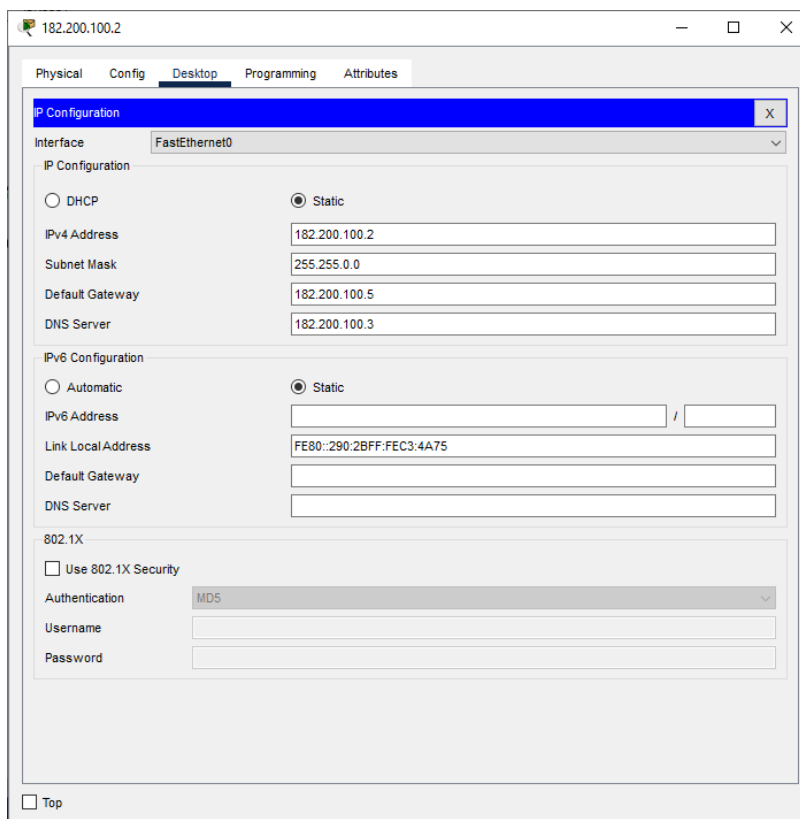
Configuration of PC1



The screenshot shows the configuration window for PC1 (182.200.100.1). The 'Desktop' tab is selected. The 'P Configuration' window is open, showing the 'FastEthernet0' interface. The 'IP Configuration' section has 'Static' selected. The 'IPv4 Configuration' section has 'Static' selected. The 'IPv6 Configuration' section has 'Static' selected. The '802.1X' section has 'Use 802.1X Security' unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

Field	Value
Interface	FastEthernet0
IP Configuration	Static
IPv4 Address	182.200.100.1
Subnet Mask	255.255.0.0
Default Gateway	182.200.100.5
DNS Server	182.200.100.3
IPv6 Configuration	Static
IPv6 Address	
Link Local Address	FE80::230:A3FF:FE94:2068
Default Gateway	
DNS Server	
802.1X	
Use 802.1X Security	<input type="checkbox"/>
Authentication	MD5
Username	
Password	

Configuration of PC2



The screenshot shows the configuration window for PC2 (182.200.100.2). The 'Desktop' tab is selected. The 'P Configuration' window is open, showing the 'FastEthernet0' interface. The 'IP Configuration' section has 'Static' selected. The 'IPv4 Configuration' section has 'Static' selected. The 'IPv6 Configuration' section has 'Static' selected. The '802.1X' section has 'Use 802.1X Security' unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

Field	Value
Interface	FastEthernet0
IP Configuration	Static
IPv4 Address	182.200.100.2
Subnet Mask	255.255.0.0
Default Gateway	182.200.100.5
DNS Server	182.200.100.3
IPv6 Configuration	Static
IPv6 Address	
Link Local Address	FE80::290:2BFF:FEC3:4A75
Default Gateway	
DNS Server	
802.1X	
Use 802.1X Security	<input type="checkbox"/>
Authentication	MD5
Username	
Password	

Configuration of Router

182.200.100.5

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0/0

GigabitEthernet0/0/1

GigabitEthernet0/0/2

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0003.E4D1.0401

IP Configuration

IPv4 Address 182.200.100.5

Subnet Mask 255.255.0.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

☐ Top

Contents of Web page

Server0

Physical Config Services Desktop Programming Attributes

Web Browser

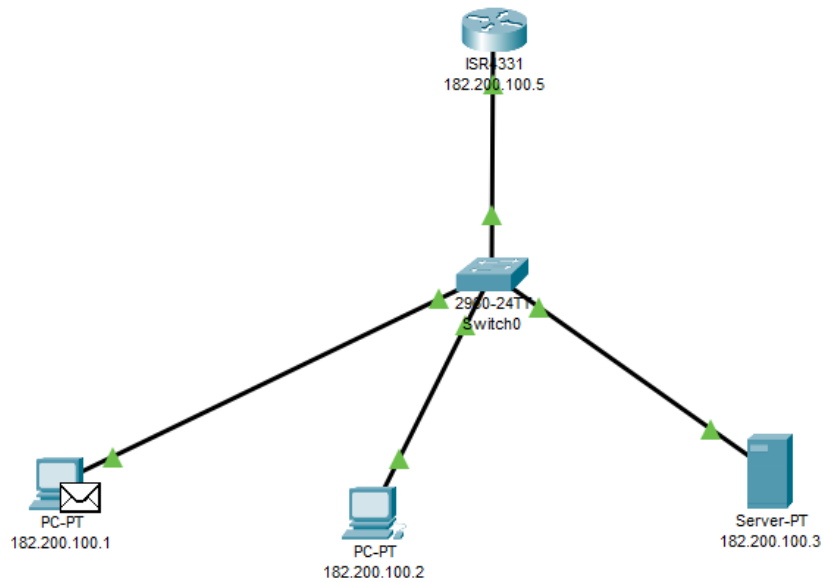
< > URL http://www.diggaj.com Go Stop

DIGGAJ UGVEKAR

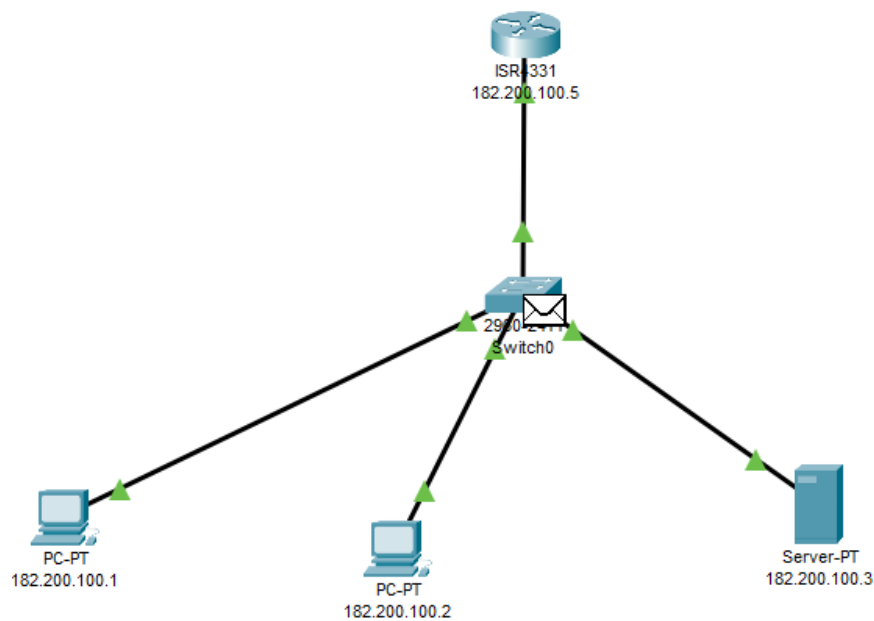
Verification of Connectivity for DNS Server:

Sending a Simple PDU from PC 182.200.100.1 to PC 182.200.100.2

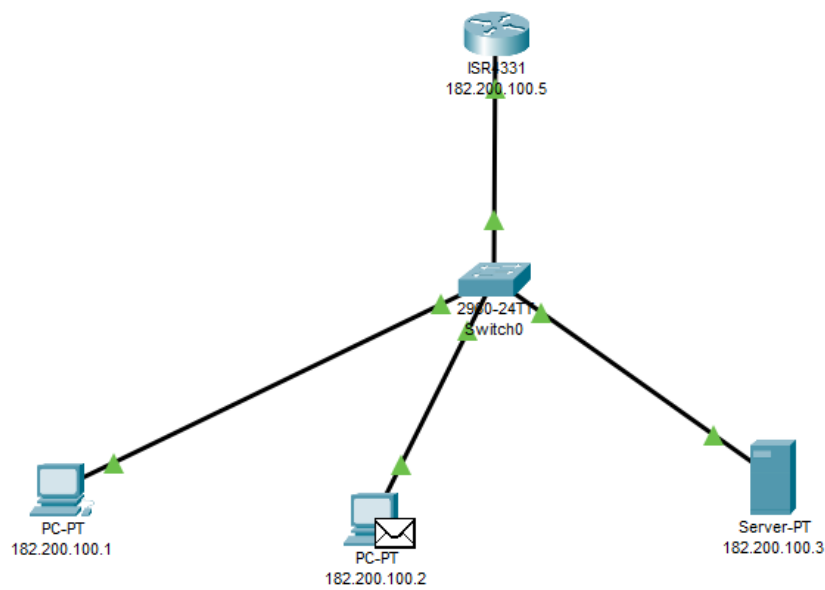
Step1:



Step2:

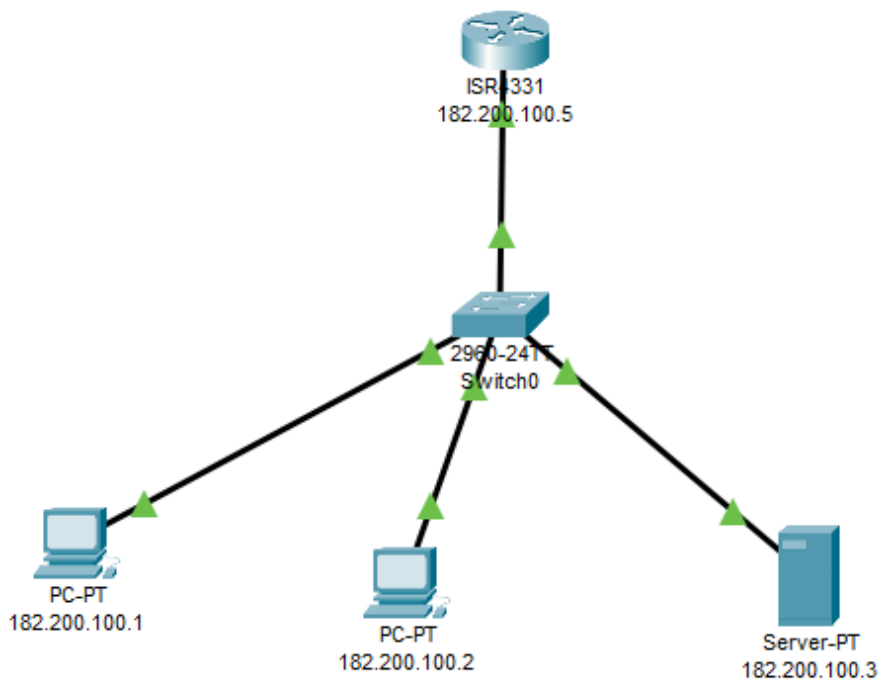


Step3:



A Simple PDU was sent successfully from PC 182.200.100.1 to PC 182.200.100.2

iii) Network Structure for FTP Server



Configuration of FTP server

The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. The 'FTP' service is highlighted in the left sidebar. The main area shows the 'FTP' service configuration. The 'Service' status is 'On'. Under 'User Setup', the 'Username' is 'diggaj' and the 'Password' is 'diggaj'. The permissions 'Write', 'Read', 'Delete', 'Rename', and 'List' are all checked. Below this is a table with columns 'Username', 'Password', and 'Permission'. The table contains two entries: '1 cisco cisco RWDNL' and '2 diggaj diggaj RWDNL'. To the right of the table are 'Add', 'Save', and 'Remove' buttons. Below the table is a 'File' section with a list of files: '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', and '7 c2600-advipservicesk9-mz.124-15.T1.bin'. A 'Remove' button is at the bottom right of the file list. At the bottom left of the window is a 'Top' button.

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	cisco	cisco	RWDNL	Add
2	diggaj	diggaj	RWDNL	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
- 7 c2600-advipservicesk9-mz.124-15.T1.bin

Remove

☐ Top

Configuration of PC1

The screenshot shows the '182.200.100.1' configuration window with the 'Desktop' tab selected. The 'IP Configuration' window is open, showing the 'FastEthernet0' interface. The 'IP Configuration' section has 'Static' selected. The 'IPv4 Address' is '182.200.100.1', 'Subnet Mask' is '255.255.0.0', 'Default Gateway' is '182.200.100.5', and 'DNS Server' is '0.0.0.0'. The 'IPv6 Configuration' section has 'Static' selected. The 'IPv6 Address' is empty, 'Link Local Address' is 'FE80::202:4AFF:FEDE:14C0', 'Default Gateway' is empty, and 'DNS Server' is empty. The '802.1X' section has 'Use 802.1X Security' unchecked, 'Authentication' is 'MD5', 'Username' is empty, and 'Password' is empty.

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface **FastEthernet0**

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication **MD5**

Username

Password

Configuration of PC2

182.200.100.1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 182.200.100.1

Subnet Mask 255.255.0.0

Default Gateway 182.200.100.5

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::202:4AFF:FEDE:14C0

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Configuration of Router

182.200.100.5

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0/0

GigabitEthernet0/0/1

GigabitEthernet0/0/2

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0000.0CBD.3B01

IP Configuration

IPv4 Address 182.200.100.5

Subnet Mask 255.255.0.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

☐ Top

Sending a File from PC1 to PC2

Cisco Packet Tracer PC Command Line 1.0

C:\>ping 182.200.100.5

Pinging 182.200.100.5 with 32 bytes of data:

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Ping statistics for 182.200.100.5:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 182.200.100.3

Pinging 182.200.100.3 with 32 bytes of data:

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Ping statistics for 182.200.100.3:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 182.200.100.3

Trying to connect...182.200.100.3

Connected to 182.200.100.3

220- Welcome to PT Ftp server

Username:diggaj

331- Username ok, need password

Password:

230- Logged in

(passive mode On)

ftp>put FILE1.txt

Writing file FILE1.txt to 182.200.100.3:

File transfer in progress...

[Transfer complete - 11 bytes]

11 bytes copied in 0.079 secs (139 bytes/sec)

ftp>dir

Listing /ftp directory from 182.200.100.3:

0 : FILE1.txt 11

PC2 Receiving a File from PC1

Cisco Packet Tracer PC Command Line 1.0

C:\>ping 182.200.100.5

Pinging 182.200.100.5 with 32 bytes of data:

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Reply from 182.200.100.5: bytes=32 time<1ms TTL=255

Ping statistics for 182.200.100.5:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 182.200.100.3

Pinging 182.200.100.3 with 32 bytes of data:

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time<1ms TTL=128

Reply from 182.200.100.3: bytes=32 time=4ms TTL=128

Ping statistics for 182.200.100.3:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ftp 182.200.100.3

Trying to connect...182.200.100.3

Connected to 182.200.100.3

220- Welcome to PT Ftp server

Username:diggaj

331- Username ok, need password

Password:

230- Logged in

(passive mode On)

ftp>dir

Listing /ftp directory from 182.200.100.3:

0 : FILE1.txt 11

ftp>get FILE1.txt

Reading file FILE1.txt from 182.200.100.3:

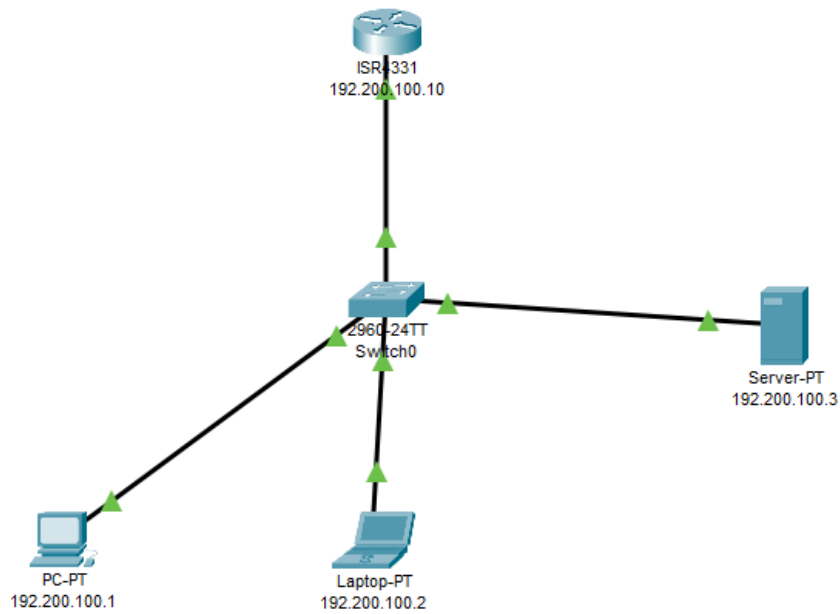
File transfer in progress...

[Transfer complete - 11 bytes]

11 bytes copied in 0 secs

The FILE1.txt was sent from PC1 and received by PC2 using FTP.

iv) Network Structure for Email Server



Email server Configuration

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management
- Radius EAP

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User Password

☐ Top

Router Configuration

192.200.100.10

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0/0

GigabitEthernet0/0/1

GigabitEthernet0/0/2

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.7060.3901

IP Configuration

IPv4 Address 192.200.100.10

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

☐ Top

PC1 Configuration

192.200.100.1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.200.100.1

Subnet Mask 255.255.255.0

Default Gateway 192.200.100.10

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::290:CFF:FEA8:A9E7

Default Gateway

DNS Server

PC2 Configuration

192.200.100.2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.200.100.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.200.100.10

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::202:4AFF:FE6E:1A0B

Default Gateway:

DNS Server:

Sending Email from PC1 to PC2

192.200.100.1

Physical Config **Desktop** Programming Attributes

Compose Mail X

Send To: abc@gmail.com

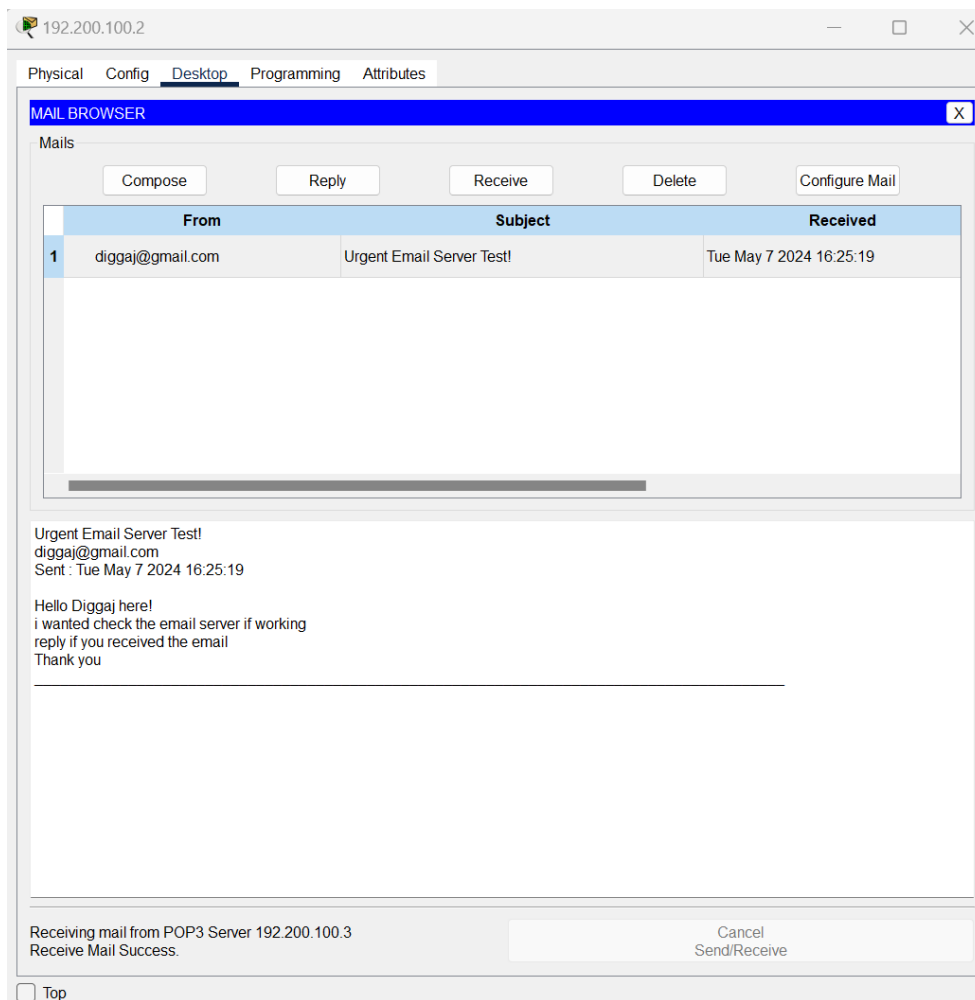
Subject: Urgent Email Server Test!

Hello Diggaj here!
i wanted check the email server if working
reply if you received the email
Thank you

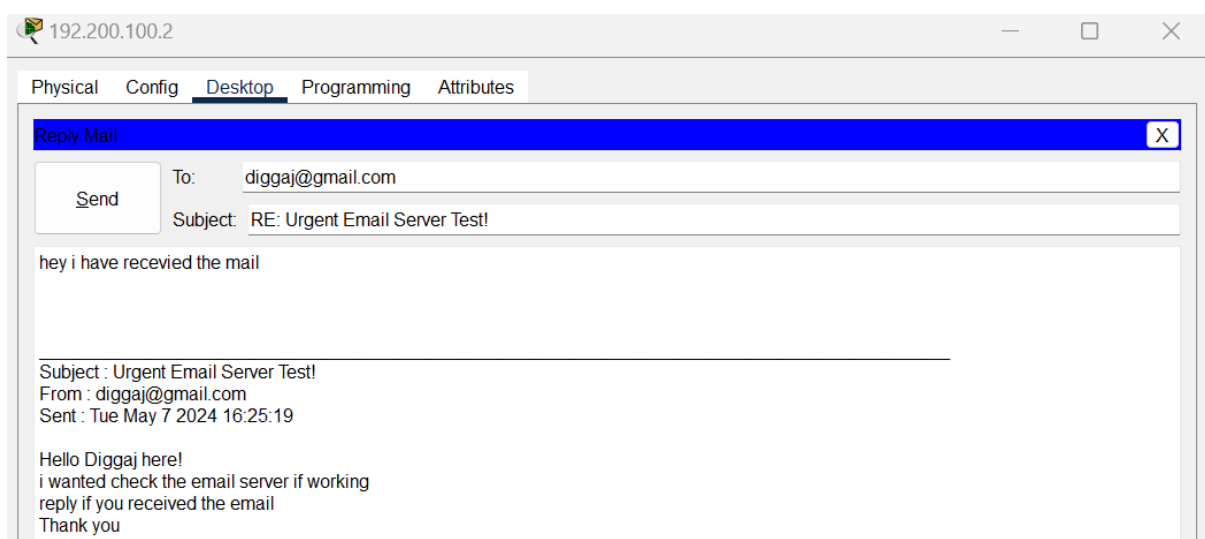
Sending mail to abc@gmail.com , with subject : Urgent Email Server Test! ... Mail Server: 192.200.100.3
Send Success.

Cancel
Send/Receive

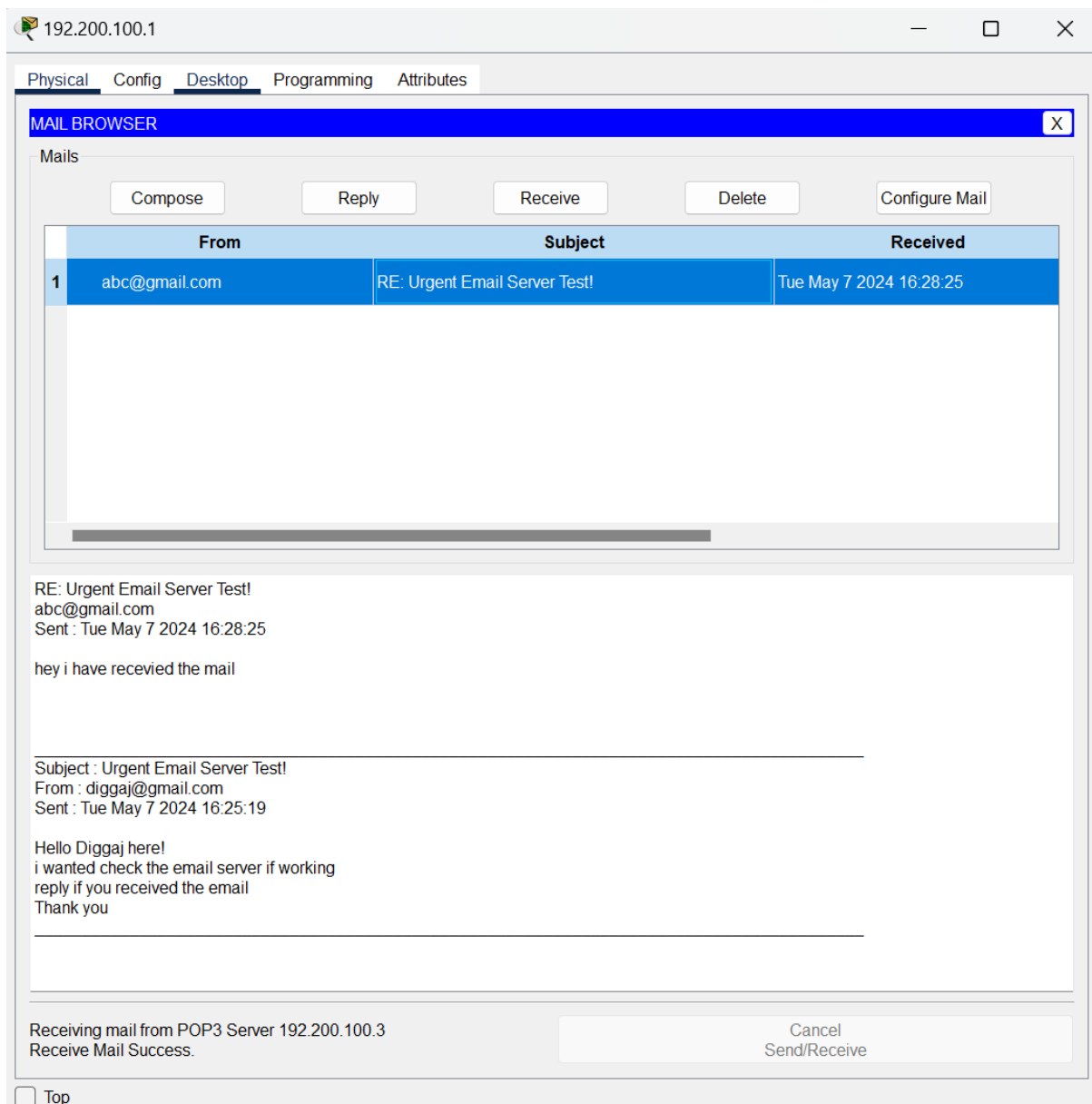
Receiving the Email by PC2



Reply to the received mail



The Reply email received by PC1 from PC2



CONCLUSION:

The DHCP, DNS, FTP, EMAIL Servers in Networking were studied, created and verified successfully.