

A Lab Report
On
COMPUTER NETWORKS
Submitted For
BACHELOR OF TECHNOLOGY
in
INFORMATION TECHNOLOGY

By
Vansh Dawra (22360)



**INDIAN INSTITUTE OF INFORMATION TECHNOLOGY UNA
HIMACHAL PRADESH**

**SUBMITTED TO
Dr. VIKRAM KUMAR**

LIST OF EXPERIMENTS

Lab Work	Description	Page No.	Signature
1)	Implementation of UTP patch cord cable utilizing RJ45 Connectors and CAT6 Cable and testing using LAN tester.	3	
2)	Wired LAN BOQ and implementation of 25 systems using passive network components.	5	
3)	Wireless LAN BOQ and implementation of 25 systems using passive network components.	7	
4)	Operation and Configuration of Layer II Switches.	9	
5)	Basic network configuration and troubleshooting commands.	11	
6)	Configuration of the Network firewall.	14	
7)	Deployment of GNS3 on Local Host Infrastructure and Virtualized Environment	16	
8)	Configuration and Implementation of CISCO1700 router in GNS3.	21	
9)	Determination of Optimal Network Routes utilizing Dijkstra's Algorithm.	25	
10)	Implementation of the LAN topologies using CISCO router and switches.	27	
11)	Configuration of static routing in a network consisting of two routers and 4 switches	31	
12)	Configuration of a RIP routing in a network build using CISCO 1700 routers.	33	
13)	Configuration of OSPF routing in a network build using CISCO 1700 Routers.	35	
14)	Implementation of basic access control list (ACL) in CISCO Routers	37	

Practical 1

Implementation and Testing of UTP Patch Cord Cable

Overview:

In this experiment, we implement Unshielded Twisted Pair (UTP) patch cord cables utilizing RJ45 connectors and CAT6 cables. UTP cables are commonly used in Ethernet networks for data transmission. We will also test the connectivity using a LAN tester.

Theory:

Unshielded Twisted Pair (UTP) cables form the backbone of modern networking infrastructure, comprising pairs of copper wires twisted together within a protective plastic sheath. These cables serve as the primary medium for transmitting data signals in Ethernet networks, with each pair of wires designated for specific transmission purposes. The RJ45 connectors, integral to UTP cables, play a pivotal role in facilitating connections between devices by effectively terminating the cable ends. These connectors adhere to standardized specifications, ensuring compatibility across various network devices and systems.



CAT6 cables, a significant advancement over previous iterations, represent a notable evolution in network cabling technology. With enhanced performance characteristics and increased bandwidth capacity, CAT6 cables offer superior data transmission speeds and reliability. Their design incorporates stringent standards to minimize signal interference and crosstalk, thereby optimizing network performance and ensuring consistent connectivity. As a result, CAT6 cables have become the preferred choice for modern networking installations, catering to the ever-growing demands of high-speed data transmission and network scalability.

Procedure:

- Gather all necessary materials including UTP patch cord cable, RJ45 connectors, CAT6 connectors, crimping tool, and LAN tester.
- Strip the outer jacket of the UTP cable using a cable stripper, exposing the inner wires.
- Untwist the pairs of wires and arrange them according to the TIA/EIA-568B

wiring standard.

- Trim the excess wire and insert the wires into the RJ45 connector.
- Use the crimping tool to crimp the connector securely onto the wires.
- Repeat the process for the other end of the cable.
- Use the LAN tester to check the continuity and proper wiring of the cable.
- If the cable passes the test, label it accordingly and store it for use.
- If the cable fails the test, troubleshoot and correct any wiring errors.
- Repeat the process for additional cables as needed.



Results:

The UTP patch cord cables were successfully constructed and tested using the LAN tester. All connections were found to be functional with no wiring issues.

Conclusion:

The experiment demonstrated the process of creating UTP patch cord cables using RJ45 connectors and CAT6 cables. Proper termination and testing ensure reliable connectivity in Ethernet networks

Practical 2

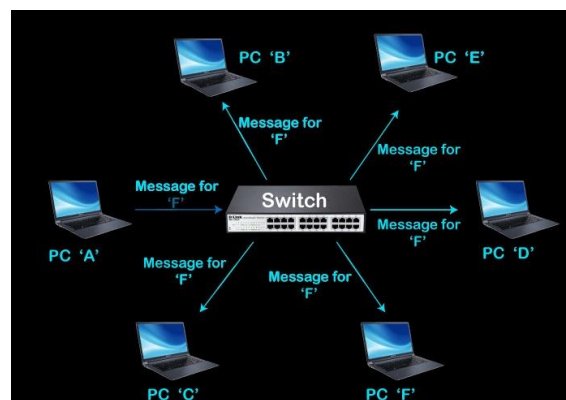
Wired LAN BOQ and Implementation of 25 Systems Using Passive Network Components

Overview:

This experiment involves preparing a Bill of Quantities (BOQ) for a wired Local Area Network (LAN) setup and implementing it for 25 systems using passive network components.

Theory:

A wired Local Area Network (LAN) is a network infrastructure composed of diverse passive network components essential for data transmission and connectivity. Among these components are Ethernet cables, patch panels, and switches, each playing a crucial role in establishing and maintaining network connectivity. Ethernet cables serve as the physical medium for transmitting data signals between devices, providing the backbone of the wired network infrastructure. Patch panels act as centralized points for terminating and organizing Ethernet cable connections, facilitating efficient cable management and troubleshooting. Additionally, switches function as network devices responsible for forwarding data packets between connected devices within the LAN.



The preparation of a Bill of Quantities (BOQ) is a fundamental step in planning a wired LAN installation. The BOQ meticulously outlines the quantities and types of passive network components required for the network deployment, ensuring the availability of necessary materials and resources. By meticulously detailing the components needed for the network installation, the BOQ streamlines the procurement process and serves as a comprehensive guide for network implementation. Overall, a wired LAN's effectiveness and reliability hinge upon the seamless integration and deployment of these passive network components, orchestrated through meticulous planning and adherence to industry standards.

Procedure:

- Perform a site survey to determine the layout and requirements of the wired LAN.
- Calculate the total length of cables needed based on the site survey.
- Prepare a bill of quantities (BOQ) listing all required components including cables, connectors, switches, and other networking equipment.
- Procure the necessary components from vendors based on the BOQ.
- Install the networking components according to the site survey and BOQ.
- Test each connection for proper functionality using network testing tools.
- Label each cable and connection for easy identification and maintenance.
- Configure network settings and security parameters on switches and other devices.
- Conduct final testing and validation of the entire wired LAN infrastructure.
- Document the installation and configuration process for future reference.

Results:

The wired LAN was successfully implemented for 25 systems using the passive network components specified in the BOQ. All systems were able to connect to the network and communicate effectively.

Conclusion:

The experiment demonstrated the process of preparing a BOQ for a wired LAN setup and implementing it using passive network components. Proper planning and installation ensure a reliable and efficient wired network infrastructure.

Practical 3

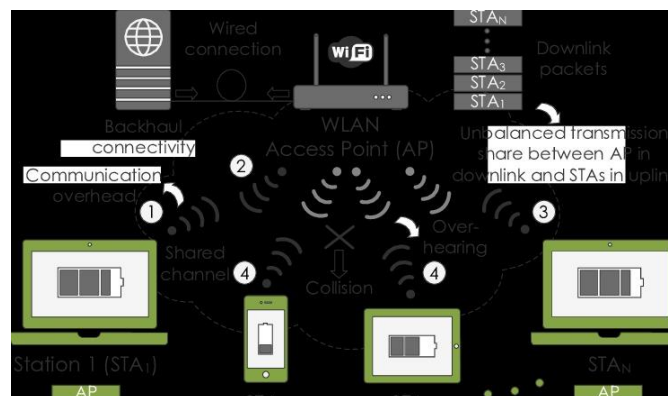
Wireless LAN BOQ and Implementation of 25 Systems Using Passive Network Components

Overview:

This experiment involves preparing a Bill of Quantities (BOQ) for a wireless Local Area Network (LAN) setup and implementing it for 25 systems using passive network components.

Theory:

A wireless Local Area Network (LAN) operates by utilizing wireless access points (APs) in lieu of traditional wired connections, offering seamless network connectivity to devices within its coverage area. Unlike wired LAN setups, wireless LANs eliminate the need for physical Ethernet cables, relying instead on radio frequency signals transmitted by APs to establish connections with network devices. The preparation of a Bill of Quantities (BOQ) plays a crucial role in planning and implementing a wireless LAN installation.



This document meticulously outlines the quantities and types of components necessary for setting up the wireless network infrastructure, including APs, antennas, and other associated equipment. By detailing the required components, the BOQ ensures efficient procurement and deployment of resources, facilitating the smooth and effective establishment of the wireless LAN.

Procedure:

- Conduct a site survey to identify coverage areas and requirements for the wireless LAN.
- Determine the number and placement of access points (APs) based on the site survey.
- Prepare a bill of quantities (BOQ) listing all required components including

APs, antennas, controllers, and other networking equipment.

- Procure the necessary components from vendors based on the BOQ.
- Install the APs and antennas in the designated locations according to the site survey and BOQ.
- Configure the wireless LAN controllers and APs with appropriate settings and security parameters.
- Conduct initial testing to ensure proper coverage and connectivity.
- Optimize AP placement and settings as needed to improve performance.
- Conduct final testing and validation of the entire wireless LAN infrastructure.
- Document the installation and configuration process for future reference.

Results:

The wireless LAN was successfully implemented for 25 systems using the passive network components specified in the BOQ. All systems were able to connect to the network and access the internet wirelessly.

Conclusion:

The experiment demonstrated the process of preparing a BOQ for a wireless LAN setup and implementing it using passive network components. Proper planning and installation ensure a reliable and efficient wireless network infrastructure.

Practical 4

Operation and Configuration of Layer II Switches.

Theory:

Layer 2 switches operate at the Data Link Layer (Layer 2) of the OSI model. Their primary function is to forward data frames within the same network or VLAN (Virtual Local Area Network) based on MAC addresses. Unlike hubs, which forward data to all connected devices, switches use MAC address tables to efficiently route data only to the intended recipient.

- **MAC Address Learning:** Layer 2 switches dynamically learn MAC addresses by examining the source MAC address of incoming frames. When a frame arrives on a port, the switch records the MAC address and the port it came from in its MAC address table. This process allows switches to build a database of MAC addresses and corresponding port locations.
- **Forwarding:** Upon receiving a frame, the switch checks its MAC address table to determine the port associated with the destination MAC address. If the MAC address is known, the switch forwards the frame only to the corresponding port. If the MAC address is unknown, the switch floods the frame out of all ports except the one it was received on, ensuring that the frame reaches its destination.
- **Filtering:** Layer 2 switches filter traffic based on MAC addresses, ensuring that frames are only forwarded to the appropriate destination ports. This filtering mechanism helps improve network efficiency by reducing unnecessary traffic transmission.
- **Loop Avoidance:** Network loops can lead to broadcast storms and network congestion. Layer 2 switches use protocols like the Spanning Tree Protocol (STP) to prevent loops by identifying and blocking redundant paths in the network topology. STP ensures a loop-free logical topology, allowing for reliable and efficient data transmission.

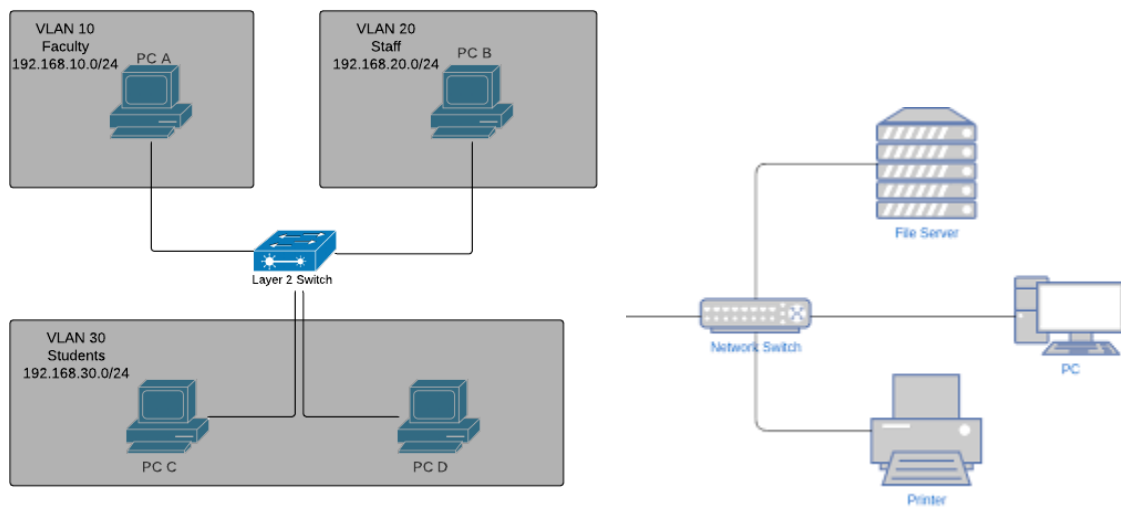
Procedure:

Configuration of Layer 2 switches involves several key steps:

1. **Accessing the Switch Interface:** Connect to the switch via a console cable or through a network connection using SSH (Secure Shell) or Telnet.
2. **Configuring Ports:** Set port parameters such as speed, duplex mode, and VLAN membership using the appropriate command-line interface (CLI) commands or graphical user interface (GUI) options.
3. **Creating VLANs:** Configure Virtual LANs to segment the network logically. Assign ports to VLANs to isolate traffic and improve network security and performance.
4. **Managing MAC Address Table:** Some switches allow manual entry or modification of MAC address table entries. Configure static MAC address entries for devices with known addresses to optimize network traffic.

5. **Enabling Spanning Tree Protocol (STP):** Activate STP to prevent network loops. Configure STP parameters such as priority, bridge priority, and port costs to ensure proper loop prevention.

Conclusion: Layer 2 switches play a critical role in network infrastructure by facilitating efficient and secure communication within LANs. Properly configuring Layer 2 switches ensures optimal network performance, scalability, and reliability. By understanding the theory behind Layer 2 switch operation and following the correct configuration procedures, network administrators can build robust and resilient networks that meet the needs of modern enterprises.



Practical 5

Basic Network Configuration and Troubleshooting Commands

Theory: Basic network configuration and troubleshooting commands are essential tools for network administrators to manage and maintain network connectivity and diagnose network-related issues. These commands provide valuable information about network settings, connectivity status, and potential problems.

- **ipconfig (Windows) / ifconfig (Linux/macOS)**

Function: Displays core network interface information including IP address, subnet mask, and default gateway.

Use case: Verifying basic IP configuration and checking if an address is assigned correctly

```
Windows IP Configuration

Ethernet adapter vEthernet (Wide Networking Switch {jg}):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4099:
    IPv4 Address. . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter vEthernet (Default Switch):
```

- **ping**

Function: Tests basic connectivity to another device on the network, uses ICMP (Internet Control Message Protocol) packets.

Use case: Checking if a computer, server, or network resource is reachable.

```
Pinging kinsta.com [104.18.42.131] with 32 bytes of data:
Reply from 104.18.42.131: bytes=32 time=11ms TTL=57
Reply from 104.18.42.131: bytes=32 time=9ms TTL=57
Reply from 104.18.42.131: bytes=32 time=9ms TTL=57
Reply from 104.18.42.131: bytes=32 time=10ms TTL=57

Ping statistics for 104.18.42.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 11ms, Average = 9ms
```

- **tracert (Windows) / traceroute (Linux/macOS)**

Function: Traces the complete route that packets take to reach a destination, showing each hop (router) along the way.

Use case: Identifying bottlenecks or points of failure within a network path.

```
C:\Users\pc>tracert -w 2000 -d www.google.com

Tracing route to www.google.com [62.162.67.35]
over a maximum of 30 hops:
  0  1 ms  <1 ms  <1 ms  192.168.1.1
  1  99 ms  16 ms  17 ms  46.217.200.1
  2  88 ms  20 ms  19 ms  195.26.150.33
  3  88 ms  19 ms  20 ms  62.162.67.35
```

- **nslookup**

Function: Queries DNS (Domain Name System) servers to translate domain names into IP addresses and vice versa.

Use case: Troubleshooting domain name resolution issues.

```
C:\Users\Niagahoster>nslookup google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4003:c01::8b
           2404:6800:4003:c01::8a
           2404:6800:4003:c01::64
           2404:6800:4003:c01::65
           74.125.130.139
           74.125.130.113
           74.125.130.138
           74.125.130.101
           74.125.130.100
           74.125.130.102
```

- **netstat**

Function: Displays a wealth of network information, including active connections, open ports, routing tables, and network statistics.

Use case: Spotting potential security issues with open ports, investigating network congestion

```
C:\Users\Admin>netstat

Active Connections

Proto Local Address Foreign Address State
```

Procedure: Using basic network configuration and troubleshooting commands involves the following steps:

1. **Opening Command Prompt or Terminal:** Launch the command-line interface on the operating system (Command Prompt for Windows or Terminal for Linux).
2. **Executing Commands:** Type the desired command (e.g., ipconfig, ping, tracert, netstat) followed by any required parameters or options and press Enter to execute the command.
3. **Interpreting Output:** Review the output generated by the command to gather information about network settings, connectivity status, or potential issues.
4. **Analyzing Results:** Analyze the output to identify any abnormalities, errors, or warning messages that may indicate network problems or misconfigurations.
5. **Taking Action:** Based on the information obtained from the commands, take appropriate actions to resolve network issues, such as adjusting network settings, troubleshooting hardware or software components, or contacting network support for further assistance.

Conclusion: Basic network configuration and troubleshooting commands are indispensable tools for network administrators to manage and troubleshoot network infrastructure effectively. By understanding the theory behind these commands and following the correct procedures for their use, administrators can diagnose and resolve network issues promptly, ensuring optimal network performance and reliability.

Practical-6

configuration of network firewall

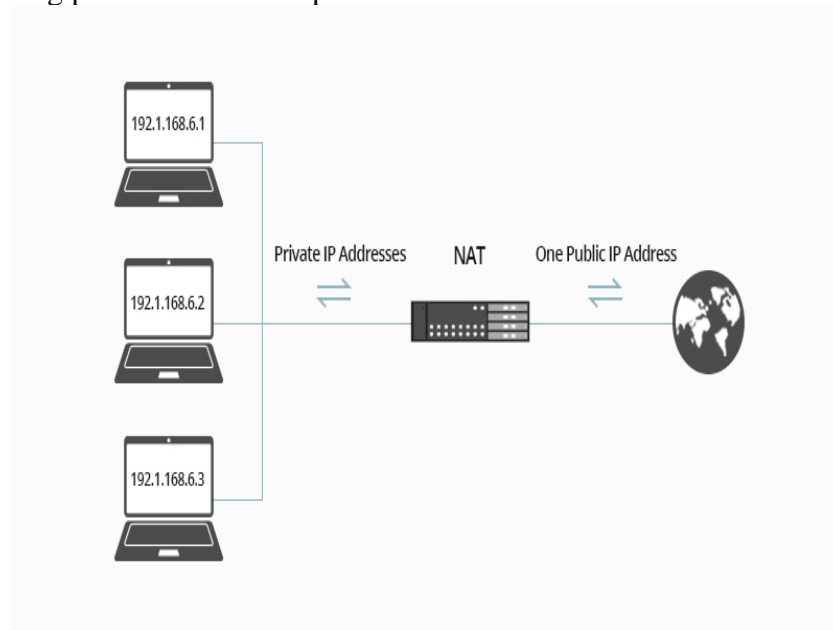
Theory:

A network firewall is a security device or software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between a trusted internal network and untrusted external networks (such as the internet), filtering traffic to prevent unauthorized access and protect against cyber threats.

- **Types of Firewalls:**

- **Stateful Firewall:** Stateful firewalls maintain a stateful inspection of network connections, tracking the state of active connections and allowing or denying traffic based on the context of each connection.
- **Stateless Firewall:** Stateless firewalls filter traffic based on predefined rules without maintaining connection state information. They inspect each packet individually and make filtering decisions based on criteria such as source and destination IP addresses, port numbers, and protocol types.

- **Firewall Rules:** Firewall rules specify the criteria for allowing or denying traffic based on various attributes, such as source and destination IP addresses, port numbers, protocol types, and packet characteristics. Administrators define firewall rules to permit legitimate traffic and block or log suspicious or unauthorized traffic.
- **Network Address Translation (NAT):** NAT is a technique used by firewalls to translate private IP addresses used within an internal network into public IP addresses visible on the internet. NAT allows multiple devices within a private network to share a single public IP address, enhancing network security and conserving public IP address space.

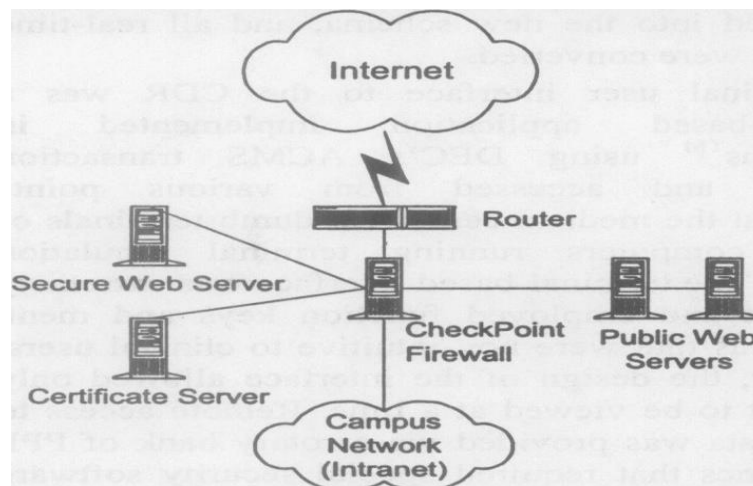


- **Logging and Monitoring:** Firewall logging and monitoring features provide visibility into network traffic, security events, and firewall activities. Logs contain information about allowed and denied traffic, security rule violations, intrusion attempts, and other network events, enabling administrators to analyze and respond to security incidents effectively.

Procedure:

Configuring a network firewall typically involves the following steps:

1. **Accessing the Firewall Interface:** Connect to the firewall management interface using a web browser or dedicated management software.
2. **Creating Firewall Rules:** Define inbound and outbound firewall rules to control traffic flow. Specify criteria such as source and destination IP addresses, port numbers, protocol types, and action (allow, deny, or log) for each rule.
3. **Configuring NAT Settings:** Configure NAT rules to translate internal private IP addresses to external public IP addresses. Define NAT policies to map internal IP addresses and port numbers to external IP addresses and ports for outbound internet access.
4. **Enabling Logging and Monitoring:** Enable firewall logging and monitoring features to generate logs of network traffic, security events, and firewall activities. Configure logging settings to specify the types of events to log and the destination for log storage.
5. **Testing and Validation:** Test the firewall configuration to ensure that firewall rules are correctly applied and traffic is filtered according to the specified criteria. Validate NAT functionality and monitor firewall logs for any anomalies or security events.



Conclusion: Network firewalls play a crucial role in safeguarding network infrastructure by controlling access to resources, protecting against unauthorized access, and mitigating security threats. By configuring firewall rules, implementing NAT policies, and enabling logging and monitoring features, administrators can enhance network security and maintain compliance with security policies and regulations.

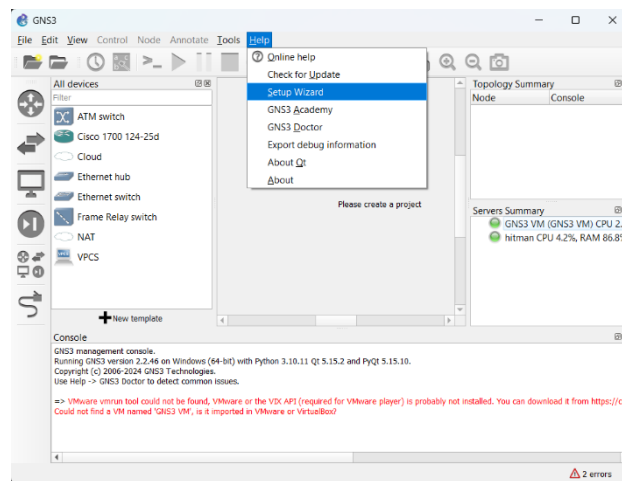
Practical 7

Deployment of GNS3 on Local Host Infrastructure and Virtualized Environment

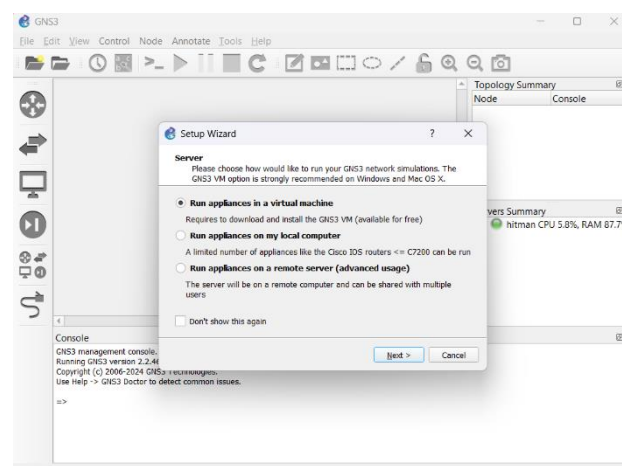
Objective: The objective of this experiment is to deploy the GNS3 (Graphical Network Simulator-3) software on both local host infrastructure and a virtualized environment. The aim is to gain practical experience in setting up GNS3 for network simulation and emulation, enabling the creation of virtual networks for testing and learning purposes.

Procedure:

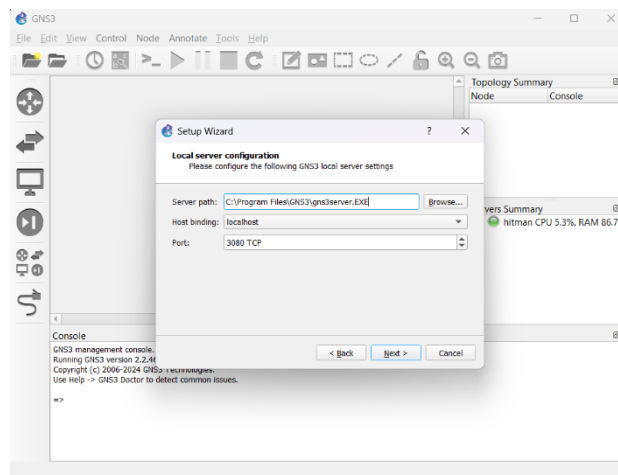
Step 1: Open GNS3 and go to help and then click on setup wizard



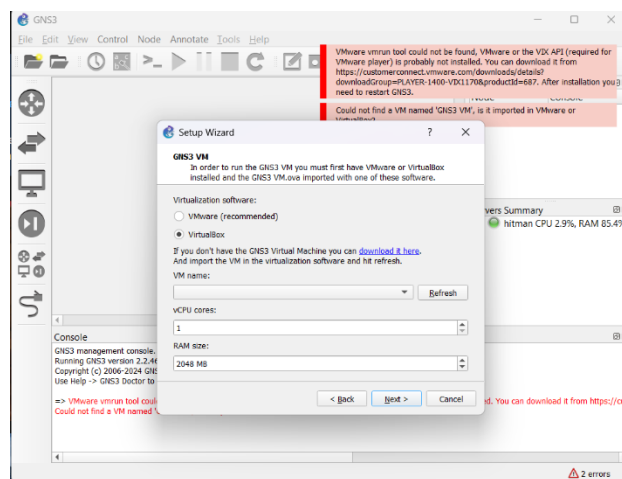
Step 2: Select Run appliances in virtual machine and click on next



Step 3: Click on next again



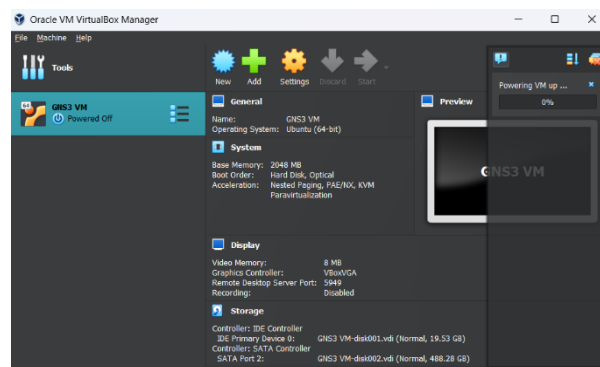
Step 4: Select VirtualBox and click on “download it here” and download it



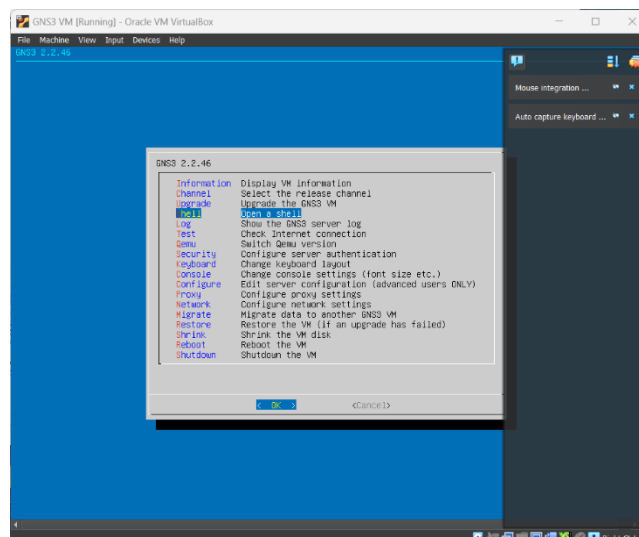
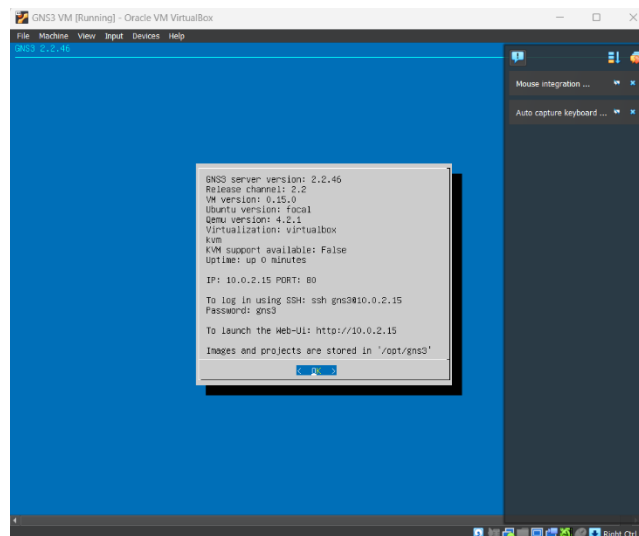
Step 5: after downloading navigate to the folder and run the vm file



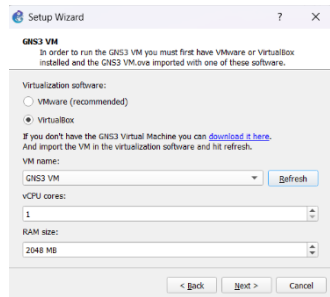
Step 6: After that start the GNS virtual machine



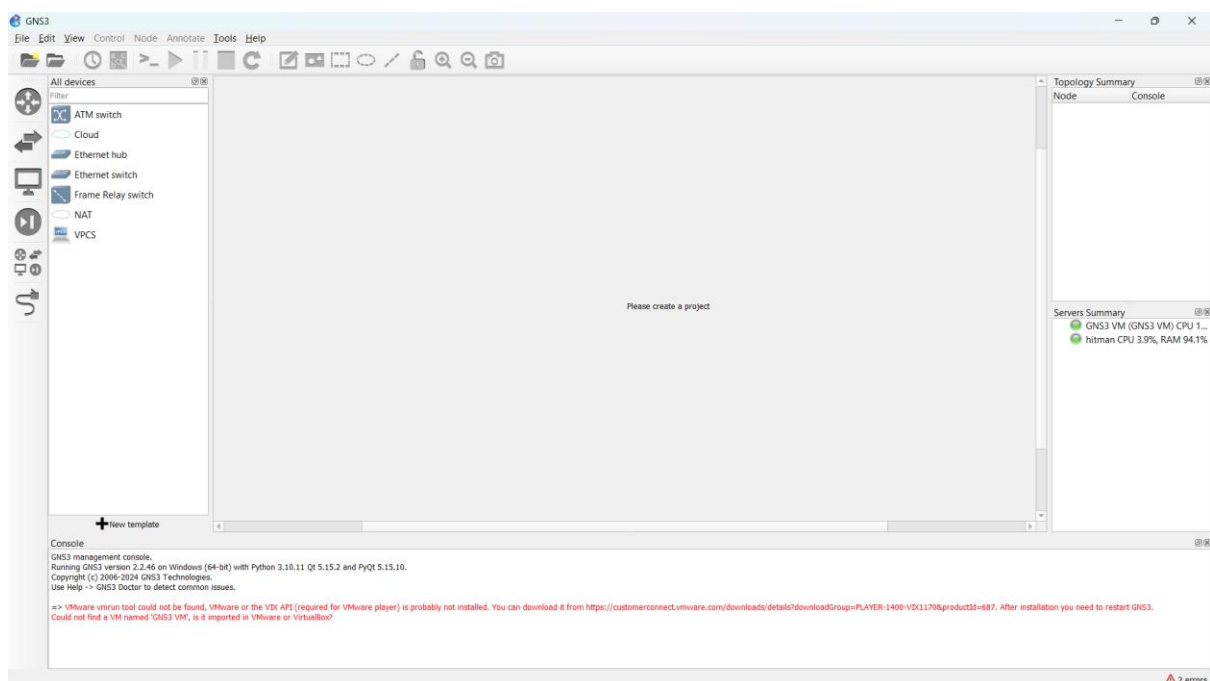
Step 7: When the VM powers up the following screen will appear navigate to shell



Step 8: Go back to GNS3 window and click on refresh and the VM will be automatically recognised



Step 9: Click on next



Outcome:

- Successfully deployed GNS3 on both local host infrastructure and a virtualized environment.
- Configured network topologies and integrated virtual and physical devices for simulation and testing purposes.
- Conducted network simulations to validate network configurations, routing protocols, and services.

- Tested and validated connectivity, routing, and traffic forwarding within the simulated environment.
- Identified and resolved network issues through troubleshooting exercises within GNS3.

Inference:

- GNS3 provides a powerful platform for network simulation and emulation, enabling users to create and test complex network scenarios in a virtual environment.
- Deployment of GNS3 on both local host infrastructure and virtualized environments offers flexibility and scalability for network simulation projects.
- Integration with physical network devices allows for more realistic simulations and testing of network configurations.
- Practical experience with GNS3 enhances understanding of networking concepts, protocols, and technologies through hands-on experimentation and exploration.

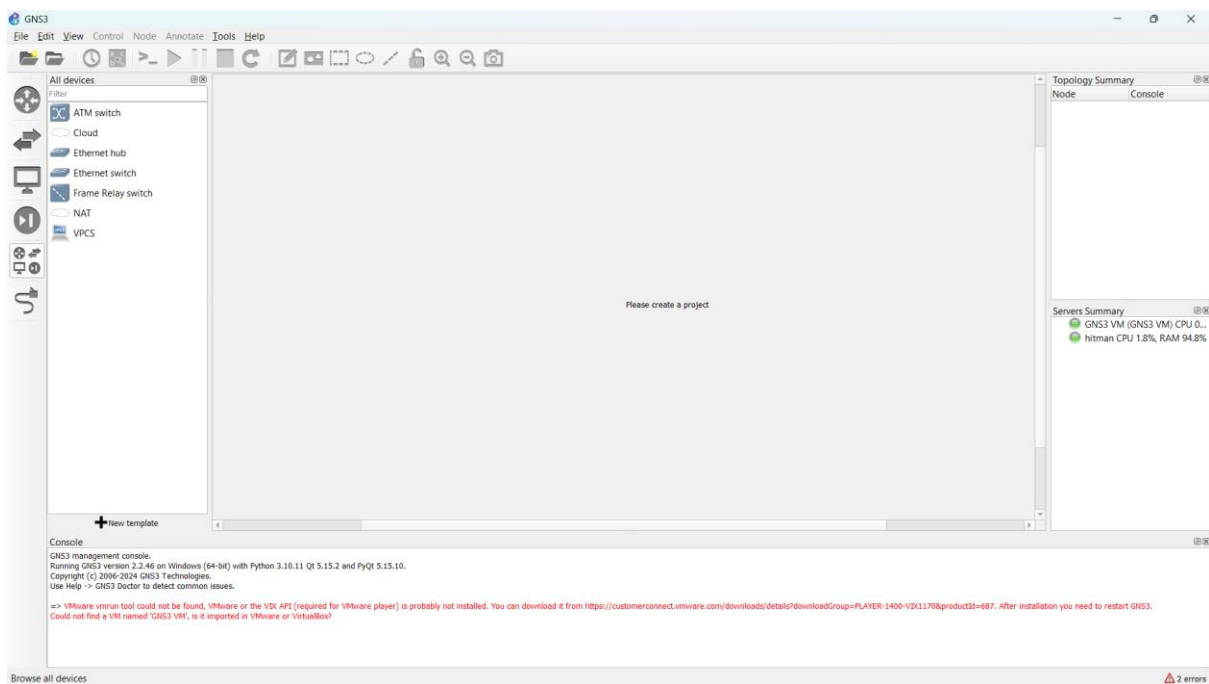
Practical 8

Configuration and Implementation of CISCO 1700 Router in GNS3

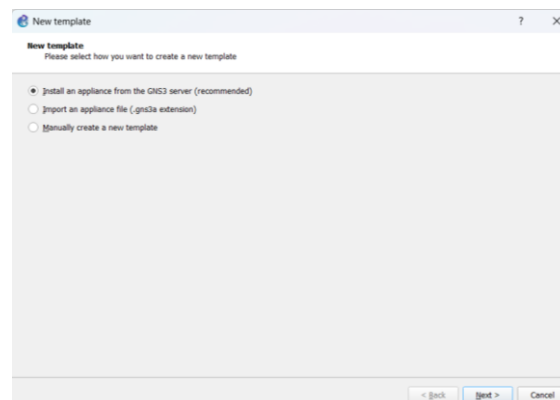
Objective: The objective of this experiment is to configure and implement a CISCO 1700 series router within the GNS3 network simulation environment. The aim is to gain hands-on experience in setting up a router, configuring basic networking features, and testing connectivity within a virtualized network environment.

Procedure:

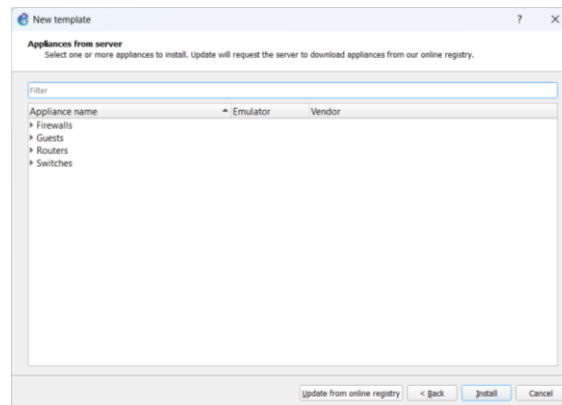
Step 1: Run GNS along with VM and select the components and click on new template at the bottom



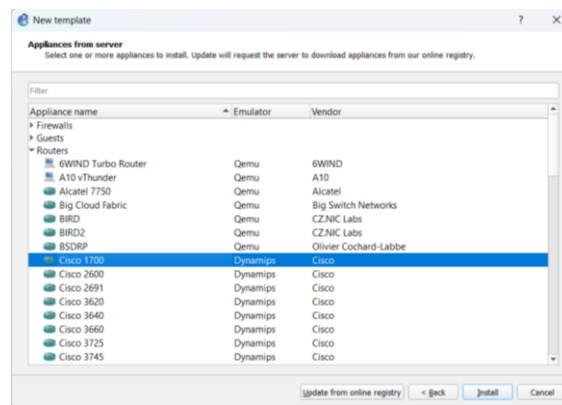
Step 2: Select the first option and click on GNS3



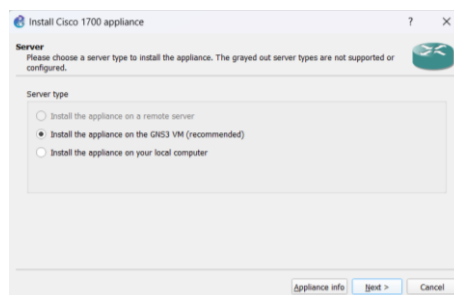
Step 3: Select routers



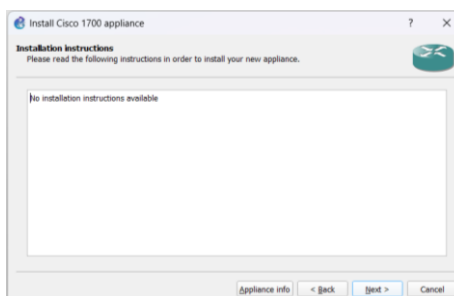
Step 4: Select CISCO 1700 router and click on Install



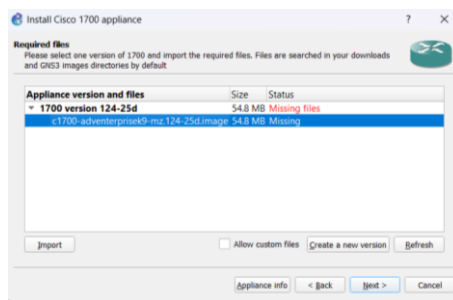
Step 5: Select Install the appliance on GNS3 VM and click on next



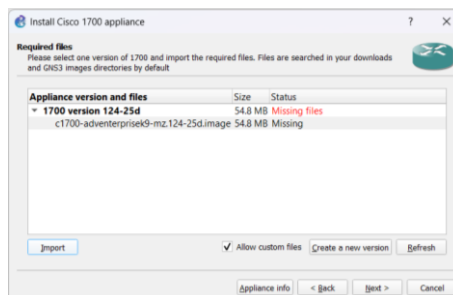
Step 6: Click on next again



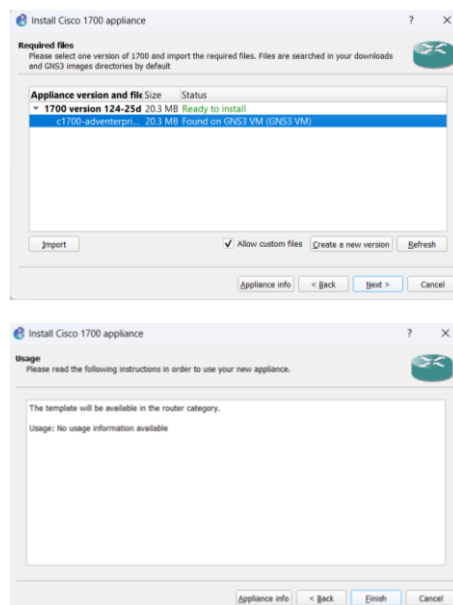
Step 7: Enable the allow custom files option and click on the missing files



Step 8: Click on import and select the file pertaining to CISCO1700 router to import



Step 9: After the import is done it will show ready to install select the router and click on next and then click on finish



Outcome:

- Successfully configured and implemented a CISCO 1700 router within the GNS3 network simulation environment.
- Configured basic router settings including hostname, domain name, and interface IP addresses.
- Established static or dynamic routing configurations to enable communication with remote networks.
- Tested and verified connectivity between the CISCO 1700 router and other devices within the simulated network topology.

Inference:

- The experiment demonstrates the effectiveness of GNS3 in simulating CISCO routers and facilitating hands-on learning experiences.
- Configuration and implementation of CISCO 1700 routers in GNS3 provide practical exposure to router setup, network configuration, and troubleshooting.
- By experimenting with GNS3, network professionals and students can gain proficiency in router configurations, routing protocols, and network design principles in a virtualized environment.
- GNS3 serves as an invaluable tool for network engineers, administrators, and learners to practice and experiment with router configurations and network scenarios without the need for physical hardware.

Practical 9

Determination of Optimal Network Routes (Dijkstra's Algorithm)

Objective: The objective of this experiment is to understand and implement Dijkstra's algorithm to determine the optimal routes in a network. The aim is to gain practical knowledge of how Dijkstra's algorithm works and how it can be applied to find the shortest paths between nodes in a network.

Procedure:

1. Setup:

- Define a network topology consisting of nodes (vertices) and links (edges) representing the network connections.
- Assign weights or costs to the links indicating the distance or cost of traversing from one node to another.

2. Initialization:

- Start with a source node and initialize the distance to itself as 0.
- Set the distances to all other nodes as infinity initially.

3. Iterative Process:

- Repeat the following steps until all nodes have been visited:
 - Select the unvisited node with the smallest distance from the source node as the current node.
 - For each neighbor of the current node, calculate the distance from the source node through the current node.
 - If the calculated distance is smaller than the previously recorded distance, update the distance to the neighbor node.
 - Mark the current node as visited.

4. Termination:

- Once all nodes have been visited, the algorithm terminates, and the shortest path distances from the source node to all other nodes are determined.

5. Path Reconstruction (Optional):

- If the shortest path to a specific destination node is required, backtrack from the destination node to the source node using the recorded shortest path information.

6. Verification:

- Validate the calculated shortest path distances by comparing them with known or manually calculated values.
- Test the algorithm with different network topologies and configurations to assess its accuracy and efficiency.

Outcome:

- Successfully implemented Dijkstra's algorithm to determine the optimal routes in a network.
- Calculated the shortest path distances from the source node to all other nodes in the network.

- Verified the accuracy of the algorithm by comparing the calculated shortest path distances with known or manually calculated values.
- Tested the algorithm with various network topologies to assess its performance and efficiency.

Inference:

- Dijkstra's algorithm is an effective method for finding the shortest paths in a network, particularly in scenarios where the network topology is known and the weights on the links represent distances or costs.
- The algorithm guarantees the shortest paths to all nodes from a given source node, making it suitable for routing and network optimization applications.
- Proper implementation and understanding of Dijkstra's algorithm are essential for network engineers and researchers to design efficient routing algorithms and network protocols.
- Experimentation with Dijkstra's algorithm in different network environments provides valuable insights into its behavior, performance, and limitations, aiding in its practical application in real-world scenarios.

Practical 10

Implementation of LAN Topologies Using CISCO Router and Switches in GNS

Objective: The objective of this experiment is to design and implement LAN topologies using CISCO routers and switches within the Graphical Network Simulator (GNS). The aim is to gain practical experience in configuring and interconnecting network devices to create functional LAN environments.

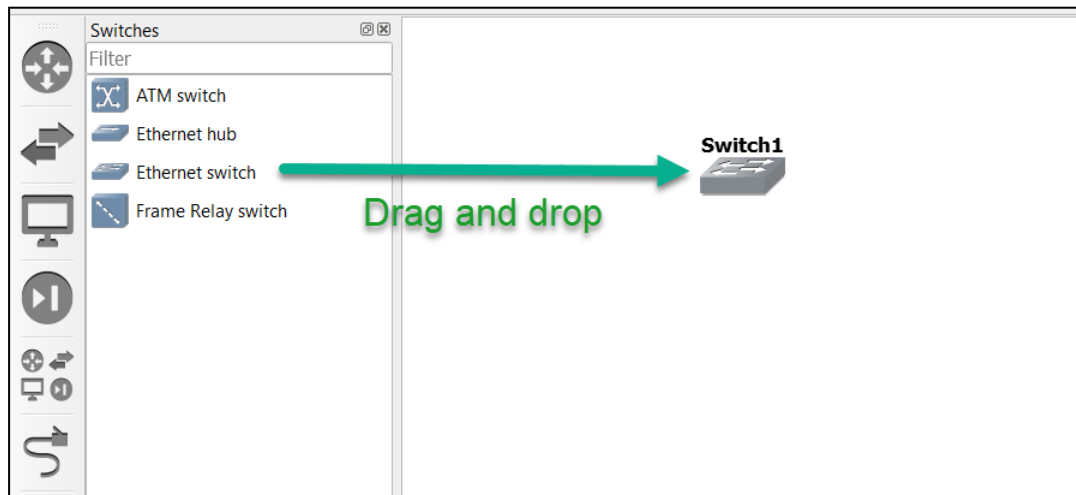
Procedure:

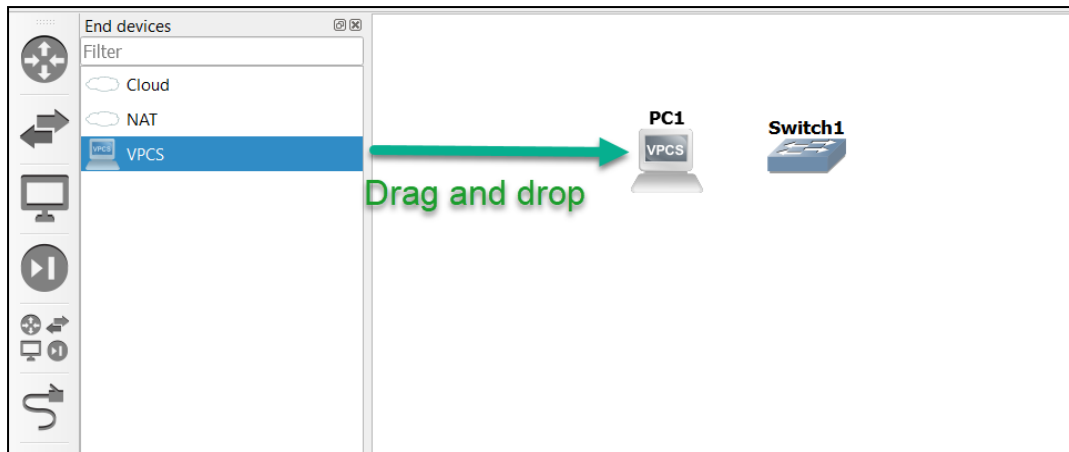
1. Topology Design:

- Determine the desired LAN topology, including the number of routers, switches, and connected devices (e.g., PCs, servers).
- Select appropriate CISCO router and switch models to represent the network devices in the GNS topology.

2. Device Placement:

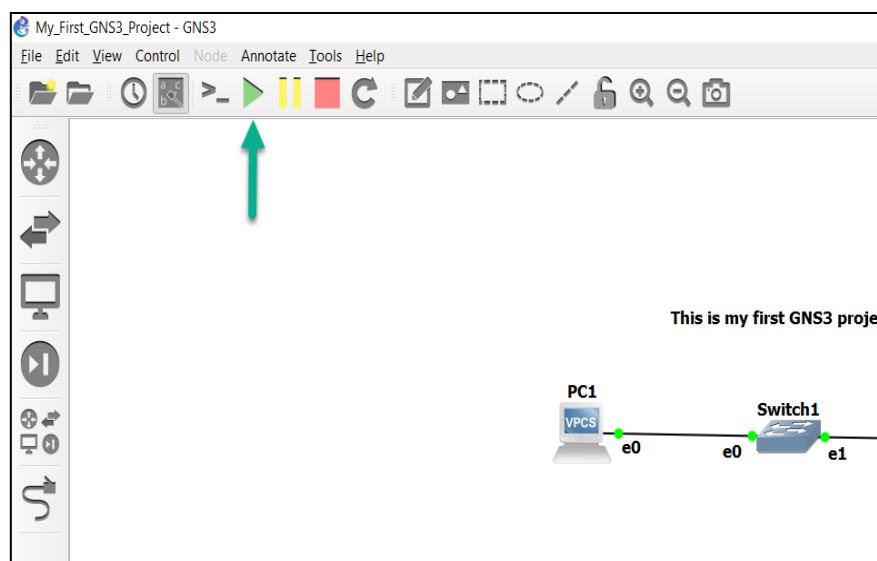
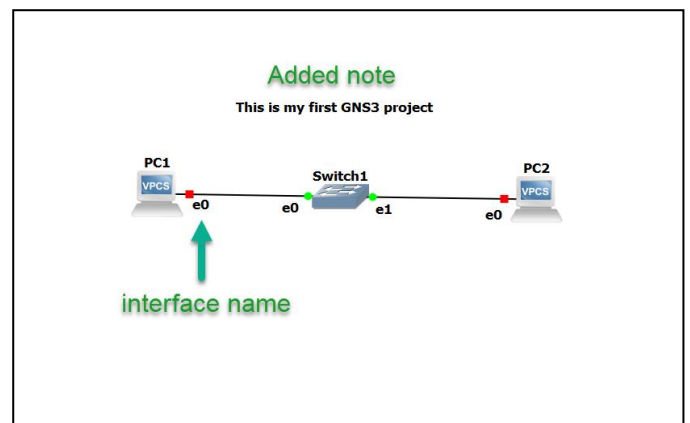
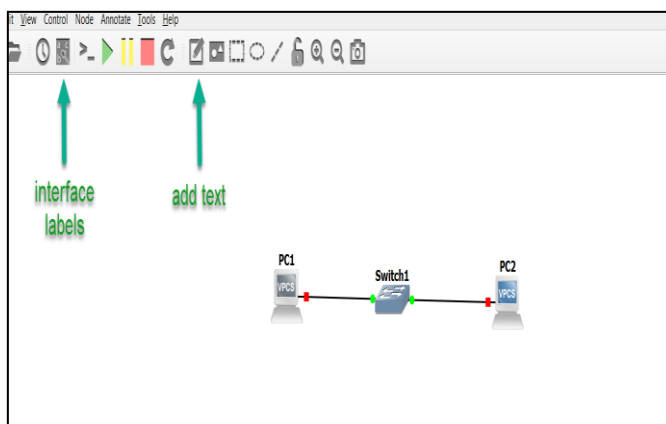
- Drag and drop CISCO router and switch icons onto the GNS workspace to represent the physical network devices.
- Arrange the devices in the topology according to the planned network layout and connectivity requirements.

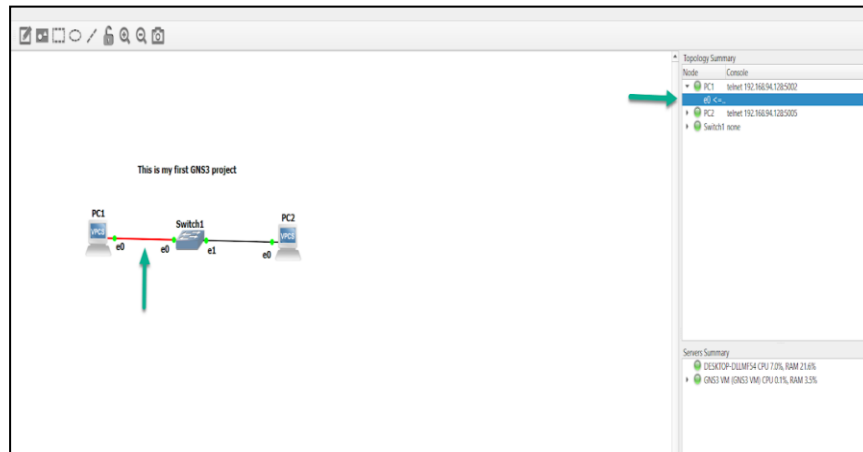




3. Interface Configuration:

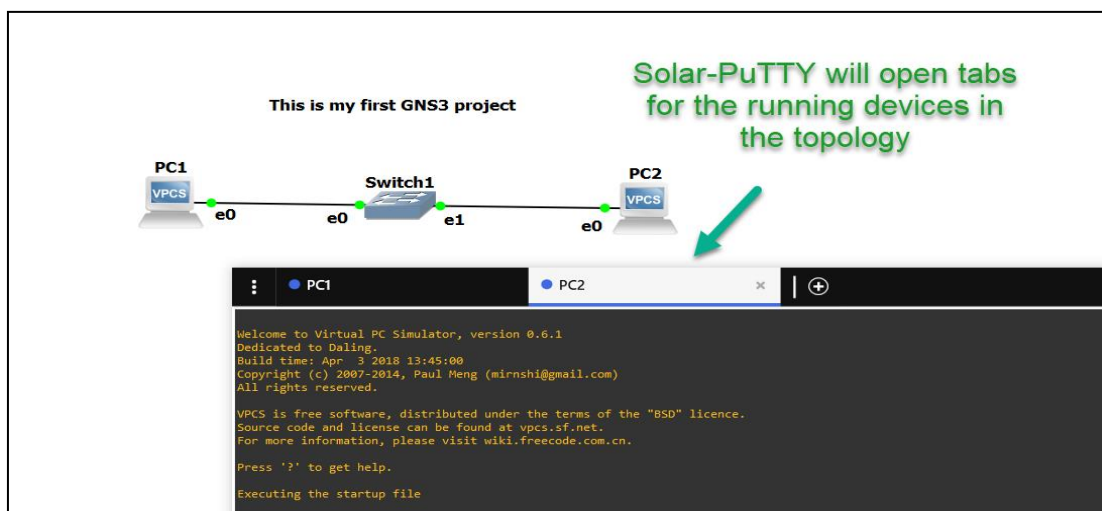
- Access the console of each CISCO router and switch within GNS.
- Configure IP addresses, subnet masks, and interface status on router interfaces.
- Assign IP addresses to the PCs and servers connected to the LAN.





4. Router Configuration:

- Configure router interfaces with IP addressing to enable inter-network communication.
- Assign IP addresses and subnet masks to router interfaces connected to LAN segments.



ign some IP addresses to PC-1 and PC-2, and ensure they can communicate with one another:

```
PC-1> ip 10.1.1.1 255.255.255.0
```

Checking for duplicate address...

```
PC1 : 10.1.1.1 255.255.255.0
```

```
PC-1>
```

```
PC-2> ip 10.1.1.2 255.255.255.0
```

Checking for duplicate address...

```
PC1 : 10.1.1.2 255.255.255.0
```

```
PC-2>
```

5. Testing and Verification:

- Start the GNS simulation and power on the virtual devices within the topology.
- Test connectivity between devices by pinging IP addresses across the network.
- Verify VLAN configurations and switch port settings.
- Verify router interface IP configurations.

Outcome:

- Successfully designed and implemented LAN topologies using CISCO routers and switches within the GNS environment.
- Configured router interfaces with IP addressing to enable inter-network communication.
- Configured switch interfaces with VLANs and trunking protocols to facilitate network segmentation.
- Assigned IP addresses to PCs and servers connected to the LAN.

Inference:

- While the experiment focused on setting up the LAN topology and configuring basic IP addressing, routing functionality was not implemented.
- The experiment provided valuable experience in configuring LAN devices, assigning IP addresses, and verifying connectivity within the LAN topology.
- Further experimentation and configuration would be needed to implement routing protocols or static routes on the routers to enable inter-VLAN communication or communication with external networks.
- This experiment lays the foundation for future exercises involving routing configuration and advanced network functionality within the LAN topology.

Practical 11

Configuration of static routing in a network consisting of two routers

Objective: The objective of this experiment is to configure static routing in a network consisting of two routers, two switches, and four PCs. The aim is to establish communication between PCs in different networks using static routes and verify connectivity by sending pings across the network.

Procedure:

1. Topology Design:

- Set up the network topology in a lab environment consisting of two routers, two switches, and four PCs.
- Connect the devices according to the planned topology, ensuring proper cabling and interface connections.

2. IP Address Assignment:

- Assign IP addresses to the Fast Ethernet interfaces of the routers, switches, and PCs to form two separate networks.
- Configure IP addresses, subnet masks, and default gateways for each device within their respective networks.

3. Router Configuration:

- Access the command-line interface (CLI) of each router.
- Configure IP addresses on the Fast Ethernet interfaces connected to the local network segments.
- Assign IP addresses on the Serial interfaces connected to each other to establish connectivity between routers.
- Use the ip route command to configure static routes on each router, specifying the destination network and next-hop router.

4. Switch Configuration:

- Configure VLANs on the switches to separate the network into logical segments, if necessary.
- Ensure that switch ports are properly configured and assigned to the appropriate VLANs.

5. PC Configuration:

- Configure IP addresses, subnet masks, and default gateways on each PC within their respective networks.
- Verify connectivity by pinging the default gateway and other PCs within the same network.

6. Testing Connectivity:

- From PC1 in network A, ping PC4 in network B to test inter-network communication.
- Verify successful ping responses and measure latency between the devices.
- Troubleshoot any connectivity issues by checking router configurations and verifying routing tables.

Outcome:

- Successfully configured static routing in the network environment, allowing communication between PCs in different networks.
- Configured IP addresses, subnet masks, and default gateways on routers, switches, and PCs to establish network connectivity.
- Configured static routes on routers to define paths to remote networks and enable inter-network communication.
- Verified connectivity by successfully pinging PCs across different networks.

Inference:

- Static routing provides a simple and effective method for defining network paths in small-scale networks where routing dynamics are predictable and stable.
- Proper configuration of IP addresses, subnet masks, and default gateways is crucial for establishing network connectivity and ensuring proper routing behavior.
- Static routes must be configured on each router to enable communication between different network segments.
- Testing connectivity between devices by sending pings verifies the effectiveness of the routing configuration and identifies any potential issues requiring troubleshooting.

Practical 12

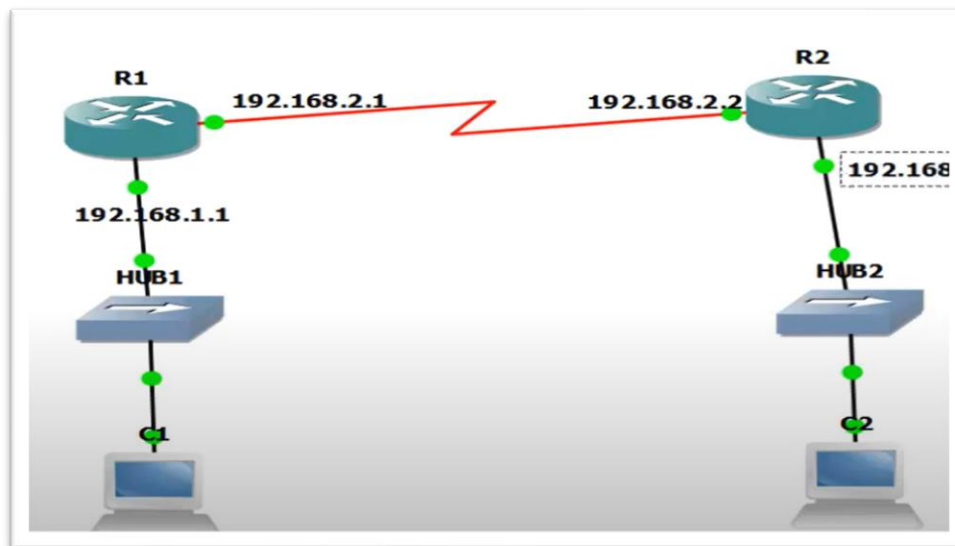
Configuration of RIP routing in a network build using CISCO 1700 routers in GNS 3.

Theory:

1. **RIP (Routing Information Protocol)** is a dynamic routing protocol used in local and wide area networks. It uses hop count as a routing metric to find the best path between the source and the destination network.
2. **Cisco 1700 routers** are configured to use RIP in GNS3, a network simulator. The routers exchange routing information to maintain up-to-date routing tables.
3. **The network interfaces** of the routers are configured with IP addresses and RIP is enabled on those interfaces.
4. **Routing updates** are exchanged every 30 seconds in RIP. These updates contain the entire routing table, which helps in maintaining the network topology.

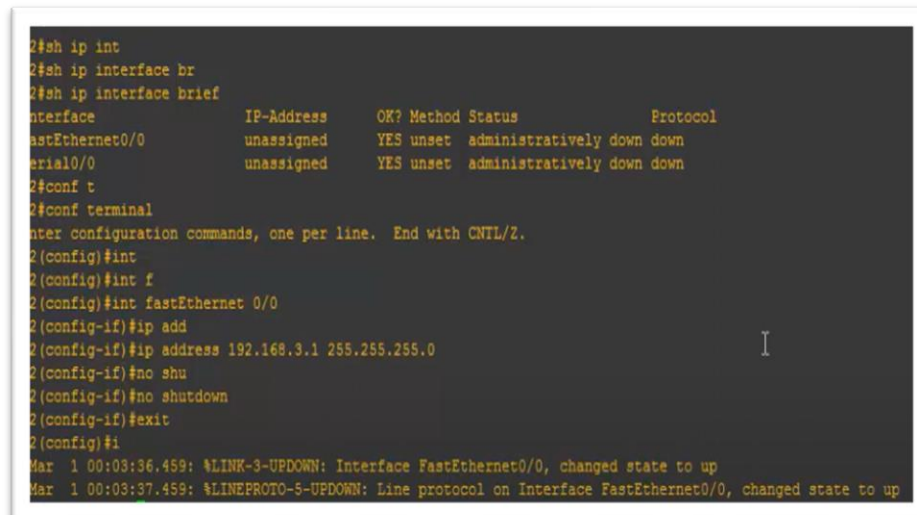
Procedure:

1. **Launch GNS3:** Start the GNS3 software. Create a new project for this specific network configuration task.
2. **Create Network Topology:** Drag and drop the Cisco 1700 routers onto the workspace. Connect them using the appropriate cables to form the desired network topology.



3. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
4. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router.

5. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router's settings.
6. **Configure Interfaces:** Assign an IP address and subnet mask to each interface that will participate in the RIP routing process. Use the ip address command followed by the IP address and subnet mask.



```
2#sh ip int
2#sh ip interface br
2#sh ip interface brief
interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          unassigned      YES unset  administratively down down
Serial0/0                 unassigned      YES unset  administratively down down
2#conf t
2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
2(config)#int
2(config)#int f
2(config)#int fastEthernet 0/0
2(config-if)#ip add
2(config-if)#ip address 192.168.3.1 255.255.255.0
2(config-if)#no shu
2(config-if)#no shutdown
2(config-if)#exit
2(config)#i
Mar  1 00:03:36.459: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Mar  1 00:03:37.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

7. **Enable Interfaces:** Use the no shutdown command to enable each interface. This will bring the interfaces up and make them ready for data transmission.
8. **Enable RIP:** Type router rip to enable RIP on the router. This will start the RIP routing process on the router.
9. **Specify Networks:** Use the network command followed by the network address to specify the networks that will participate in the RIP routing process. Do this for all directly connected networks.
10. **Verify Configuration:** Type end or press Ctrl+Z to exit the configuration mode. Use the show Ip route command to verify the RIP routing process. The routing table should show the routes learned via RIP

Conclusion:

The experiment of configuring RIP routing in a network using Cisco 1700 routers in GNS3 was successful. The routers were able to exchange routing information effectively, demonstrating the functionality of RIP. The network interfaces were correctly configured and the routing tables updated as expected. This experiment validates the effectiveness of RIP in managing dynamic routing in a network built with Cisco 1700 routers.

Practical 13

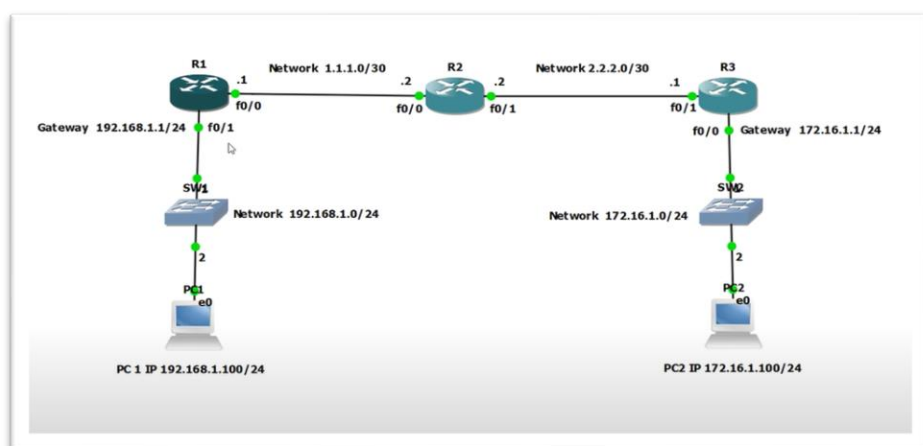
Configuration of OSPF routing in a network build using CISCO 1700 routers in GNS 3.

Theory:

1. **OSPF (Open Shortest Path First)** is a link-state routing protocol that uses Dijkstra's algorithm to find the shortest path for routing packets through a network.
2. **Cisco 1700 routers** are configured to use OSPF in GNS3, a network simulator. The routers exchange link-state information to maintain a complete topology of the network.
3. **The network interfaces** of the routers are configured with IP addresses and OSPF is enabled on those interfaces.
4. **Link-state advertisements (LSAs)** are exchanged between OSPF routers to share knowledge about the state of other network links.
5. **OSPF** provides a fast convergence time, meaning it quickly adapts to changes in the network topology, making it suitable for large networks.

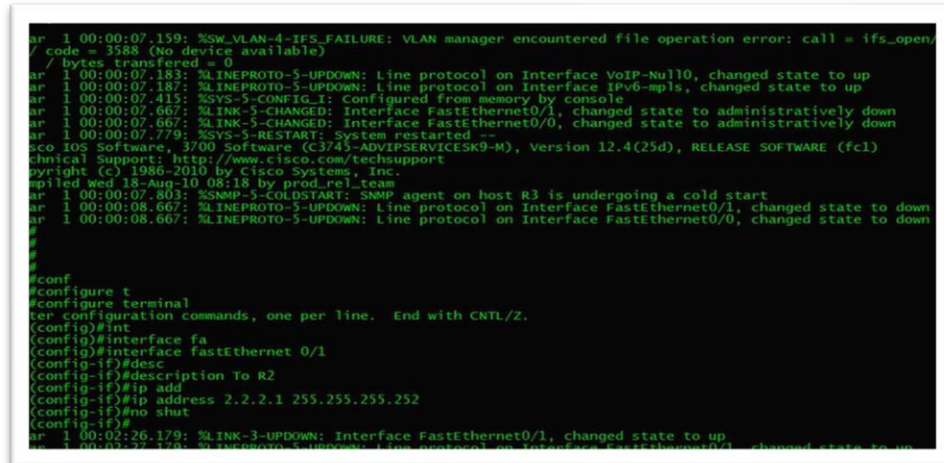
Procedure:

1. **Launch GNS3:** Start the GNS3 software. Create a new project for this specific network configuration task.
2. **Create Network Topology:** Drag and drop the Cisco 1700 routers onto the workspace. Connect them using the appropriate cables to form the desired network topology.



3. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
4. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router.

5. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router's settings.
6. **Configure Interfaces:** Assign an IP address and subnet mask to each interface that will participate in the OSPF routing process. Use the ip address command followed by the IP address and subnet mask.



```

ar 1 00:00:07.159: %SW_VLAN-4-IFS_FAILURE: VLAN manager encountered file operation error: call = ifs_open/
/ code = 3588 (No device available)
/ bytes transferred = 0
ar 1 00:00:07.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed state to up
ar 1 00:00:07.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface IPv6-mpls, changed state to up
ar 1 00:00:07.415: %SYS-5-CONFIG_I: Configured from memory by console
ar 1 00:00:07.667: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
ar 1 00:00:07.667: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
ar 1 00:00:07.779: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(25d), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
ar 1 00:00:07.803: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a cold start
ar 1 00:00:08.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
ar 1 00:00:08.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
#
#
#
#conf
#configure t
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#int
(config)#interface fa
(config)#interface FastEthernet 0/1
(config-if)#desc
(config-if)#description To R2
(config-if)#ip add
(config-if)#ip address 2.2.2.1 255.255.255.252
(config-if)#no shut
(config-if)#
ar 1 00:02:26.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
ar 1 00:02:26.179: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

```

7. **Enable Interfaces:** Use the no shutdown command to enable each interface. This will bring the interfaces up and make them ready for data transmission.
8. **Enable OSPF:** Type router ospf followed by a process ID to enable OSPF on the router. This will start the OSPF routing process on the router.
9. **Specify Networks:** Use the network command followed by the network address and wildcard mask to specify the networks that will participate in the OSPF routing process. Do this for all directly connected networks.
10. **Verify Configuration:** Type end or press Ctrl+Z to exit the configuration mode. Use the show ip ospf command to verify the OSPF routing process. The output should show the OSPF process ID and the networks participating in the OSPF process.

Conclusion:

The experiment of configuring OSPF routing in a network using Cisco 1700 routers in GNS3 was successful. The routers were able to exchange link-state information effectively, demonstrating the functionality of OSPF. The network interfaces were correctly configured and the routing tables updated as expected. This experiment validates the effectiveness of OSPF in managing dynamic routing in a network built with Cisco 1700 routers.

Practical 14

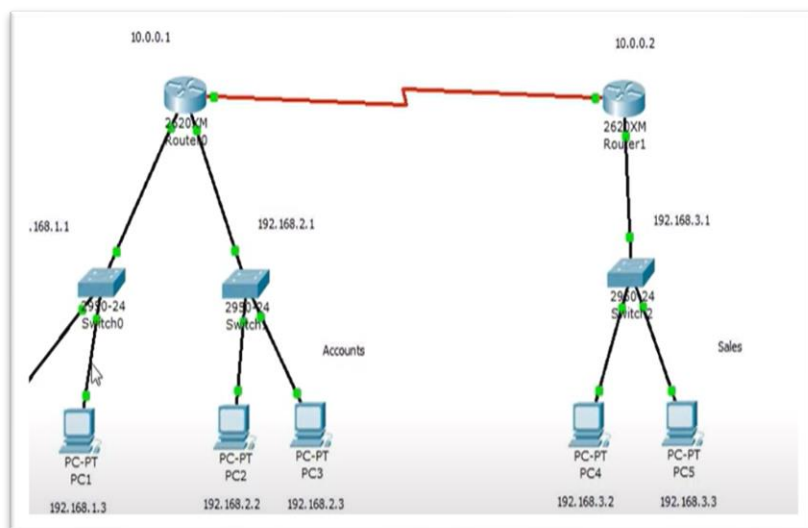
Implement a basic Access Control List (ACL) in Cisco router using GNS3.

Theory:

1. **Access Control List (ACL)** is a set of rules defined for controlling the network traffic and reducing network attacks.
2. **ACLs** are used to filter traffic based on the IP address, protocol, or port number on a Cisco router.
3. **GNS3 (Graphical Network Simulator-3)** is a network software emulator that allows the combination of virtual and real devices, used to simulate complex networks.
4. **The Cisco** router in GNS3 is configured to implement ACLs to control the incoming and outgoing traffic.
5. **Implementing ACL** involves creating an ACL and then applying that ACL to an interface on the router.

Procedure:

1. **Launch GNS3:** Start the GNS3 software. Create a new project for this specific network configuration task.
2. **Create Network Topology:** Drag and drop the Cisco routers onto the workspace. Connect them using the appropriate cables to form the desired network topology.



3. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
4. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router.

5. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router's settings.
6. **Create ACL:** Use the access-list command followed by an ACL number (between 1 and 99 for standard ACLs or between 100 and 199 for extended ACLs), an action (permit or deny), and a source IP address to create the ACL.
7. **Add More Rules:** Add more rules to the ACL as needed, using the same access-list command followed by the ACL number, action, and source IP address.
8. **Apply ACL to Interface:** Use the access-group command in the interface configuration mode to apply the ACL to an interface. Specify the direction of traffic (in or out) that the ACL should affect.

```
Router>
Router#
Router#
Router#sh acc
Router#sh access-lists
Standard IP access list 1
  deny 192.168.2.0 0.0.0.255
  permit any
Router#config t
Enter configuration commands, one per line. End with CNTL-Z
Router(config)#
Router(config)#
Router(config)#int
Router(config)#int
Router(config)#interface f
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip a
Router(config-if)#ip acc
Router(config-if)#ip access-group
```

9. **Exit Configuration Mode:** Type end or press Ctrl+Z to exit the configuration mode.
10. **Verify ACL:** Use the show access-lists command to verify that the ACL is working correctly. The output should show the ACL number, action, and source IP address for each rule in the ACL.

Conclusion:

The experiment of implementing a basic Access Control List (ACL) in a Cisco router using GNS3 was successful. The ACL was correctly configured and applied to the router's interface, effectively controlling the network traffic. This experiment validates the effectiveness of ACLs in enhancing network security and managing traffic in a network built with Cisco routers.