A Lab Report On

**COMPUTER NETWORKS**

Submitted For

**BACHELOR OF TECHNOLOGY**

in

**INFORMATION TECHNOLOGY**

By

**Harshit Mishra(22323)**



# 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. | 5 |  |
| 2) | Wired LAN BOQ and implementation of 25 systems using passive network components. | 7 |  |
| 3) | Wireless LAN BOQ and implementation of 25 systems using passive network components. | 9 |  |
| 4) | Operation and Configuration of Layer II Switches. | 11 |  |
| 5) | Basic network configuration and troubleshooting commands. | 13 |  |
| 6) | Configuration of the Network firewall. | 16 |  |
| 7) | Deployment of GNS3 on Local Host Infrastructure and Virtualized Environment | 18 |  |
| 8) | Configuration and Implementation of CISCO1700 router in GNS3. | 23 |  |
| 9) | Determination of Optimal Network Routes utilizing Dijkstra's Algorithm. | 27 |  |
| 10) | Implementation of the LAN topologies using CISCO router and switches. | 30 |  |
| 11) | Configuration of static routing in a network consisting of two routers and 4 switches | 32 |  |
| 12) | Configuration of a RIP routing in a network build using CISCO 1700 routers. | 35 |  |
| 13) | Configuration of OSPF routing in a network build using CISCO 1700 Routers. | 37 |  |
| 14) | Implementation of basic access control list (ACL) in CISCO Routers | 39 |  |

## Practical 1

### Aim: Implementation of UTP patch cord cable utilizing RJ45 Connectors and CAT6 Cable and testing using LAN tester.

**Theory:**

* UTP Cable: Unshielded Twisted Pair (UTP) cables are commonly used in networking for Ethernet connections. They consist of twisted pairs of copper wires, which reduce electromagnetic interference (EMI) and crosstalk.
* RJ45 Connector: This connector is the standard connector used for Ethernet connections. It has eight pins that correspond to the eight wires inside the UTP cable. Proper termination of these wires is crucial for a reliable connection.
* CAT6 Cable: CAT6 cables are designed for Gigabit Ethernet and other network protocols that require high data transfer rates. They offer better performance than CAT5e cables and are backward compatible with lower categories.

### Procedure:

* Preparation:

Gather the necessary materials: CAT6 cable, RJ45 connectors, crimping tool, cable stripper, and cable tester (LAN tester).

Measure and cut the desired length of CAT6 cable.

Use the cable stripper to remove the outer insulation, exposing the twisted pairs of wires.

* Termination:

Straighten and arrange the twisted pairs according to the T568A or T568B wiring standard. Trim the wires to the appropriate length and insert them into the RJ45 connector in the correct order.

Use the crimping tool to crimp the connector onto the cable securely, ensuring good contact between the wires and the connector pins.

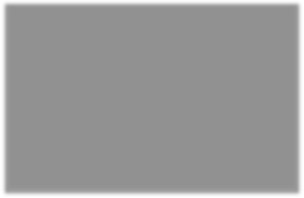
* Testing:

Use a LAN tester to verify the continuity and integrity of the connection.

Connect one end of the patch cord to the LAN tester and the other end to a known working network port or another LAN tester.

The LAN tester will indicate whether the connections are properly terminated and if there are any wiring faults, such as shorts or open circuits.

Verify that all eight wires are properly connected and that there is no crosstalk between them.



### Conclusion:

Creating a UTP patch cord cable using RJ45 connectors and CAT6 cable requires careful attention to detail to ensure proper termination and reliable performance. Following the correct wiring standards and using quality materials is essential for achieving optimal results. Testing the cable with a LAN tester helps identify any wiring faults and ensures that the connection meets the required specifications for Ethernet networking. A successfully tested patch cord cable can be confidently deployed in networking environments, providing reliable connectivity for data transmission**.**

## Practical 2

### Aim: Wired LAN BOQ and implementation of 25 systems using passive network components.

**Theory:**

* + **Wired LAN:** A wired Local Area Network (LAN) connects devices within a limited area, such as a home, office, or campus, using Ethernet cables. It provides reliable and high-speed communication between devices.
  + **Passive Network Components:** These include items like Ethernet cables, RJ45 connectors, patch panels, wall sockets, and cable management tools. They facilitate the physical connections within the network without requiring power.

### Procedure:

1. Planning and Design:

Determine the layout of the network, including the location of devices, such as computers, printers, and switches.

Calculate the quantity of passive network components required based on the network design and layout.

1. Bill of Quantities (BOQ):

Prepare a BOQ listing all the necessary passive network components, including: Ethernet cables (CAT6 or CAT6a), specifying lengths for each cable run.

RJ45 connectors for terminating cables.

Patch panels for connecting cables from various rooms to a central location. Wall sockets or keystone jacks for connecting devices to the network.

Cable management tools such as cable ties, cable trays, and labels.

1. Procurement:

Source the required passive network components based on the BOQ.

Ensure that all components meet the required standards and specifications for performance and compatibility.

1. Installation:

Install Ethernet cables according to the planned layout, ensuring proper cable management and avoiding interference from electrical sources.

Terminate each cable with RJ45 connectors, following the T568A or T568B wiring standards.

Install patch panels at the central location and terminate cables onto them, labeling each connection for easy identification.

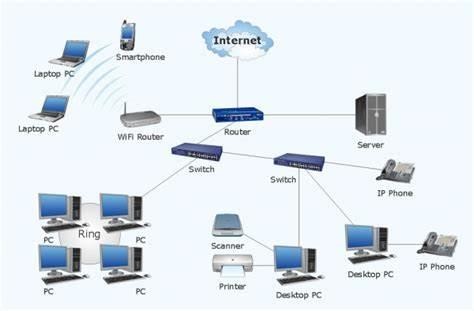
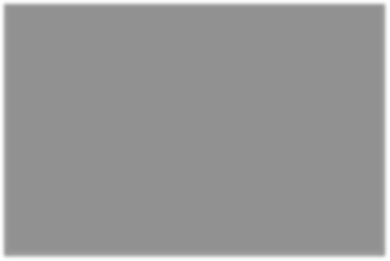
Install wall sockets or keystone jacks in each room where devices will connect to the network, ensuring proper labeling and organization.

1. Testing and Commissioning:

Use a cable tester to verify the continuity and integrity of each Ethernet cable connection. Test network connectivity between devices to ensure proper communication.

Configure network settings on devices such as IP addresses, subnet masks, and gateway addresses as needed.

Document the network layout, including cable runs, connections, and configurations.



### Conclusion:

Implementing a wired LAN for 25 systems using passive network components involves careful planning, procurement, installation, and testing. Following a structured approach ensures that the network meets performance requirements and provides reliable connectivity for all devices. Proper documentation of the network layout and configurations helps in troubleshooting and future expansions. With a well-designed and implemented LAN infrastructure, users can enjoy fast and stable network connectivity for their computing needs.

## Practical 3

### Aim: Wireless LAN BOQ and implementation of 25 systems using passive network components.

**Theory:**

* Wireless LAN (WLAN): A WLAN enables devices to connect to a network without the need for physical Ethernet cables. It relies on wireless access points (APs) to provide connectivity to devices within their range.
* Passive Network Components: Although WLAN primarily operates wirelessly, passive components such as Ethernet cables, patch panels, and wall sockets are still essential for connecting wired devices to the network and for the backhaul connections between wireless access points and the network infrastructure.

### Procedure:

* 1. Planning and Design:

Determine the coverage area for the WLAN, considering factors such as building layout, materials, and potential sources of interference.

Identify suitable locations for wireless access points to ensure adequate coverage and minimize dead zones.

Plan the placement of passive network components such as Ethernet cables, patch panels, and wall sockets for wired connections.

* 1. Bill of Quantities (BOQ):

Prepare a BOQ listing all required components for the WLAN implementation, including:

Wireless access points (quantity based on coverage requirements).

Ethernet cables for backhaul connections between access points and network infrastructure.

RJ45 connectors for terminating cables.

Patch panels for terminating backhaul cables at the network infrastructure. Wall sockets or keystone jacks for connecting wired devices.

* 1. Procurement:

Source the required components based on the BOQ, ensuring compatibility with the WLAN infrastructure and network standards.

Consider factors such as wireless standards (e.g., 802.11ac, 802.11ax), PoE (Power over Ethernet) support for access points, and cable quality for reliable connections.

* 1. Installation:

Install wireless access points at planned locations, ensuring optimal coverage and minimizing interference.

Install backhaul Ethernet cables between access points and network infrastructure, terminating them at patch panels.

Terminate Ethernet cables with RJ45 connectors and install wall sockets or keystone jacks for wired connections to devices.

Ensure proper cable management and labeling for easy identification and maintenance.

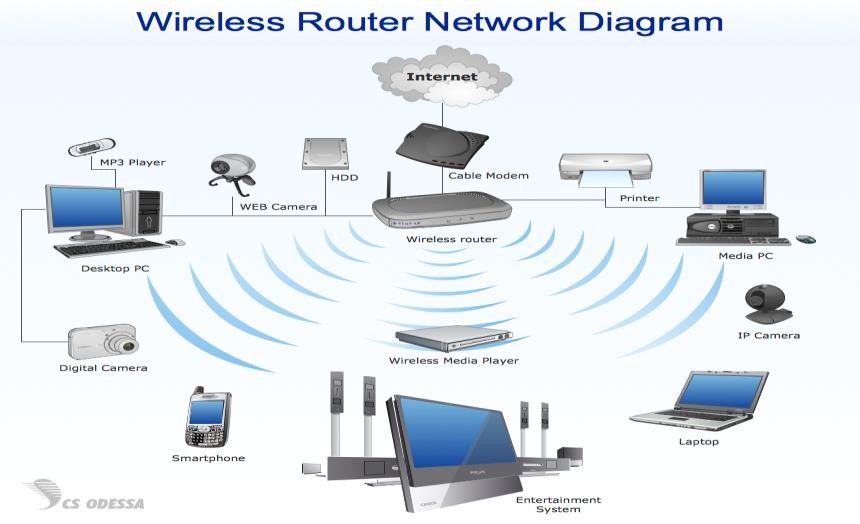
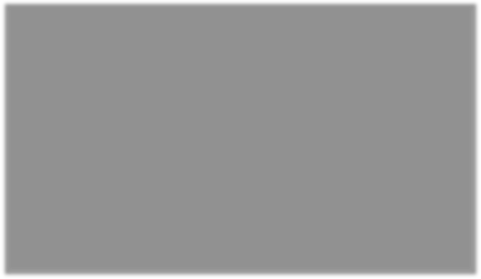
* 1. Testing and Commissioning:

Test wireless connectivity and coverage using tools such as wireless site survey software and signal strength meters.

Test wired connections for proper termination and connectivity.

Configure wireless access points with appropriate settings such as SSIDs, security protocols (e.g., WPA2), and channel assignments.

Verify network connectivity for all devices and ensure proper functioning of the WLAN.



### Conclusion:

Implementing a Wireless LAN for 25 systems using passive network components requires careful planning, procurement, installation, and testing. Proper placement of wireless access points and backhaul connections, along with high-quality passive components, ensures reliable wireless connectivity and seamless integration with wired devices. Thorough testing and commissioning help identify and resolve any issues, resulting in a robust WLAN infrastructure that meets the connectivity needs of the organization. With a well-implemented WLAN, users can enjoy the flexibility and mobility of wireless connectivity while maintaining the option for wired connections where needed.

## Practical 4

### Aim: Operation and configuration of Layer II switches

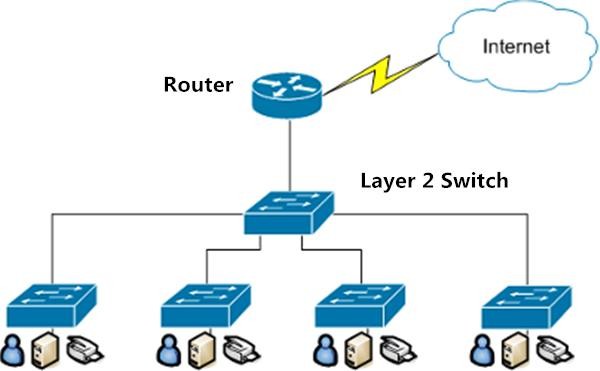
**Theory:** Layer 2 switches operate at the Data Link Layer (Layer 2) of the OSI model, and they are primarily responsible for forwarding frames based on the Media Access Control (MAC) addresses of devices within the same local network.

**Operation:**

1. **MAC Address Learning**: When a switch receives a frame on one of its ports, it reads the source MAC address of the frame and stores it in its MAC address table (also known as Content Addressable Memory - CAM table) along with the port through which the frame was received. This process allows the switch to learn which devices are connected to which ports.
2. **MAC Address Forwarding**: When a frame is received, the switch checks its MAC address table to determine the port associated with the destination MAC address. If the port is known, the switch forwards the frame only to that port. If the port is unknown, the switch floods the frame out of all ports except the one it was received on.
3. **Broadcast and Multicast Handling**: Switches forward broadcast and multicast frames to all ports except the one they were received on, ensuring that these frames reach all devices within the network segment.
4. **Loop Prevention**: Some Layer 2 switches implement protocols like Spanning Tree Protocol (STP) to prevent loops in the network topology, which could otherwise cause broadcast storms and network instability.

**Configuration:**

1. **Access Ports vs. Trunk Ports**: Layer 2 switches typically have two types of ports: access ports and trunk ports. Access ports are used to connect end devices like computers or printers, while trunk ports are used to interconnect switches or connect to routers. Configuring the appropriate port type ensures proper traffic handling.
2. **VLAN Configuration**: VLANs (Virtual Local Area Networks) can be configured on Layer 2 switches to logically segment the network into separate broadcast domains. This helps in improving network security, manageability, and efficiency. Switch ports can be assigned to specific VLANs to control which devices can communicate with each other.
3. **STP Configuration**: If Spanning Tree Protocol (STP) is used, switches need to be configured with appropriate STP settings to prevent loops in the network topology. This includes configuring the root bridge, setting port priorities, enabling or disabling specific STP features like PortFast or BPDU Guard, etc.
4. **MAC Address Table Management**: While most switches dynamically learn MAC addresses, they also often allow manual configuration of MAC address entries in the MAC address table. This can be useful for certain scenarios, such as ensuring a specific MAC address is always associated with a particular port.
5. **Port Security**: Layer 2 switches often support port security features to restrict access to a switch port based on MAC address. This prevents unauthorized devices from connecting to the network.
6. **Quality of Service (QoS)**: Some Layer 2 switches support QoS features to prioritize certain types of traffic over others. This can be useful in environments where certain applications or services require guaranteed levels of bandwidth or low latency.



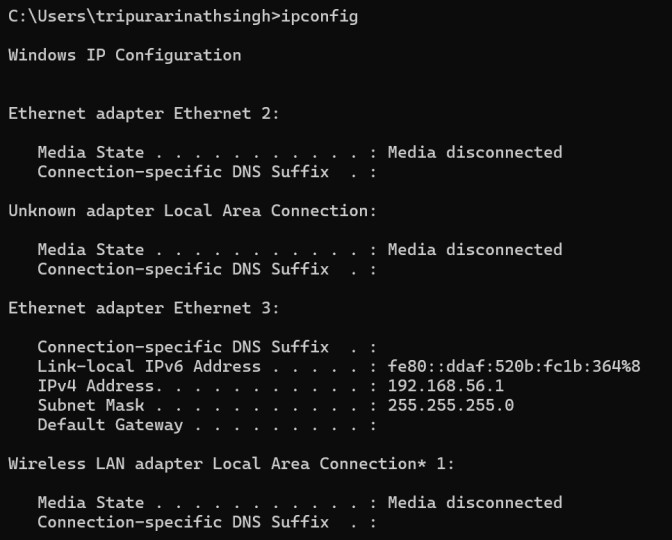
### Conclusion:

Overall, configuring a Layer 2 switch involves setting up its ports, VLANs, STP parameters, and optionally enabling additional features like port security and QoS based on the requirements of the network environment.

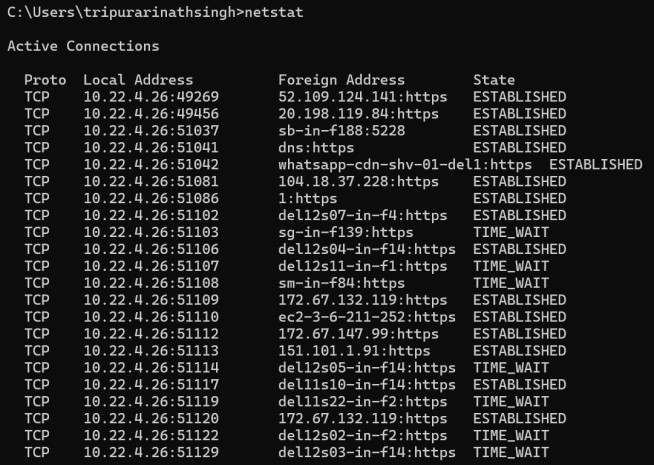
## Practical 5

### Aim: Basic Network configuration and troubleshooting commands such as Tracert, ipconfig. Theory:

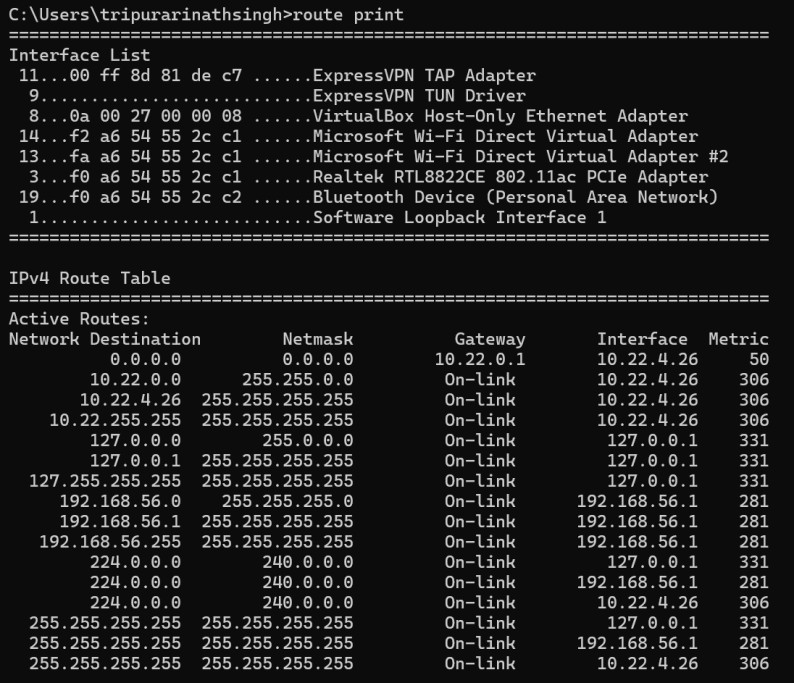
1. ipconfig/ifconfig:
   * Purpose: Displays the configuration of network interfaces.
   * Usage:
     + Windows (ipconfig): Shows IP address, subnet mask, default gateway, and DNS server configuration.
     + (ifconfig): Provides similar information about network interfaces.



1. ping:
   * Purpose: Tests connectivity between two networked devices using ICMP Echo Request/Reply messages.
   * Usage:
     + Sends ICMP packets to the specified destination.
     + Measures round-trip time (RTT) and packet loss.
2. tracert/traceroute:
   * Purpose: Determines the route packets take to reach a destination by sending packets with increasing TTL (Time-to-Live) values.
   * Usage:
     + Shows the IP addresses of routers along the path to the destination.
     + Helps diagnose routing issues and network congestion.
3. nslookup/dig:
   * Purpose: Queries DNS servers to retrieve DNS records, including IP addresses associated with domain names.
   * Usage:
     + Helps resolve domain names to IP addresses.
     + Useful for troubleshooting DNS resolution problems.
4. netstat:
   * Purpose: Displays network connections, routing tables, interface statistics, and other network-related information.
   * Usage:
     + Shows active TCP/UDP connections, listening ports, and routing table entries.
     + Helps identify network services and troubleshoot connection issues.



1. arp:
   * Purpose: Displays and modifies the ARP cache, which maps IP addresses to MAC addresses on a local network.
   * Usage:
     + Shows the MAC address associated with an IP address.
     + Useful for troubleshooting MAC address resolution problems.
2. route:
   * Purpose: Displays and modifies the local IP routing table, which contains information about routes to network destinations.
   * Usage:
     + Shows the routing table entries, including destination networks, gateways, and interface metrics.
     + Helps diagnose routing issues and configure static routes.



### Conclusion:

The conclusion of basic network configuration and troubleshooting commands, such as Tracers and ipconfig, underscores their significance in managing and diagnosing network issues effectively. These commands serve as fundamental tools for network administrators and users alike, providing valuable insights into network connectivity, configuration, and potential problems.

Through commands like ipconfig, users can quickly retrieve essential information about their network interfaces, IP addresses, subnet masks, and gateway configurations. This data is crucial for ensuring proper network connectivity and diagnosing connectivity issues.

## Practical 6

### Aim: Configuration of the Network Firewall

**Theory:** A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and malicious activities.

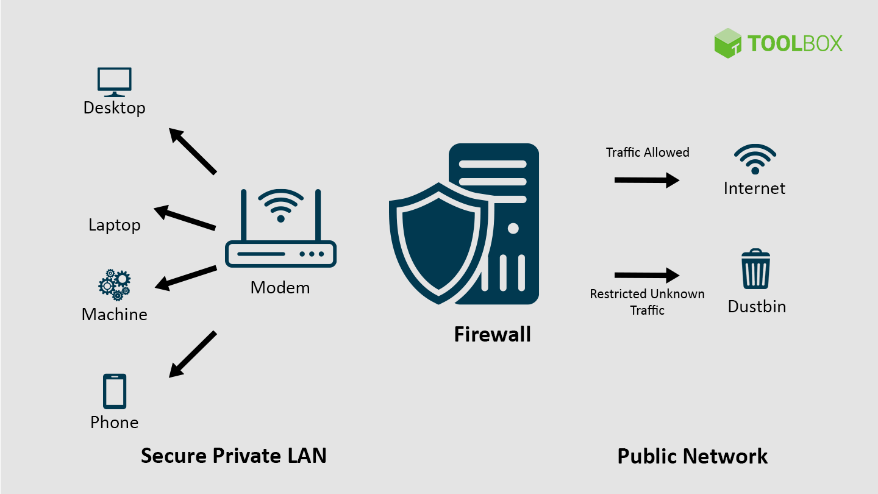
**Types of Firewalls:**

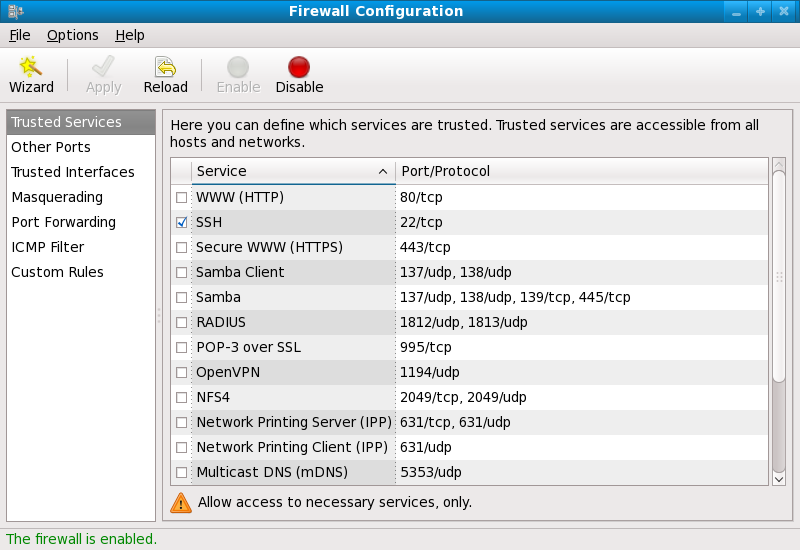
1. **Packet Filtering Firewalls:** Examines each packet of data that passes through the firewall and accepts or rejects it based on predetermined criteria, such as source/destination IP addresses, port numbers, and protocols.
2. **Stateful Inspection Firewalls:** Also known as dynamic packet filtering firewalls, these firewalls not only inspect individual packets but also keep track of the state of active connections.
3. **Proxy Firewalls:** Act as intermediaries between internal and external networks, receiving requests from internal clients and forwarding them on behalf of the clients.
4. **Next-Generation Firewalls (NGFW):** Combine traditional firewall functionality with additional features such as intrusion prevention, application awareness, and deep packet inspection.

**Firewall Placement:**

Firewalls can be deployed at various points within a network to provide different levels of protection:

* + **Perimeter Firewall:** Placed at the boundary between an internal network and an external network (e.g., the internet). It protects the entire internal network from external threats.
  + **Internal Firewall:** Deployed within the internal network to segment it into separate security zones and control traffic between them.
  + **Host-based Firewall:** Installed on individual devices (e.g., servers, workstations) to protect them from network-based attacks.





### Conclusion:

Configuring a network firewall is a critical aspect of network security management. By carefully defining and implementing firewall rules, organizations can effectively protect their network infrastructure, safeguard sensitive data, and mitigate the risks posed by cyber threats.

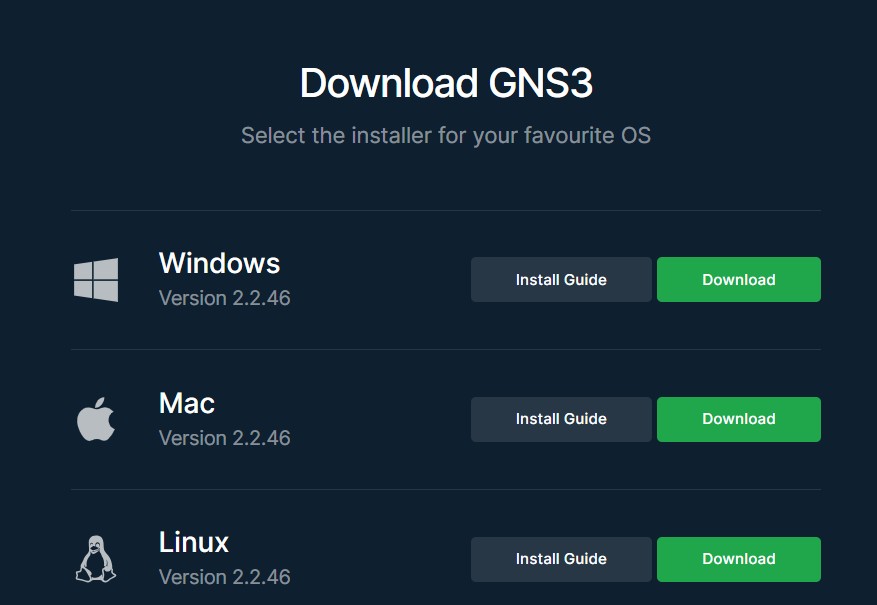
# Practical 7

### Aim: Deployment of GNS3 on Local Host Infrastructure and Virtualized Environment

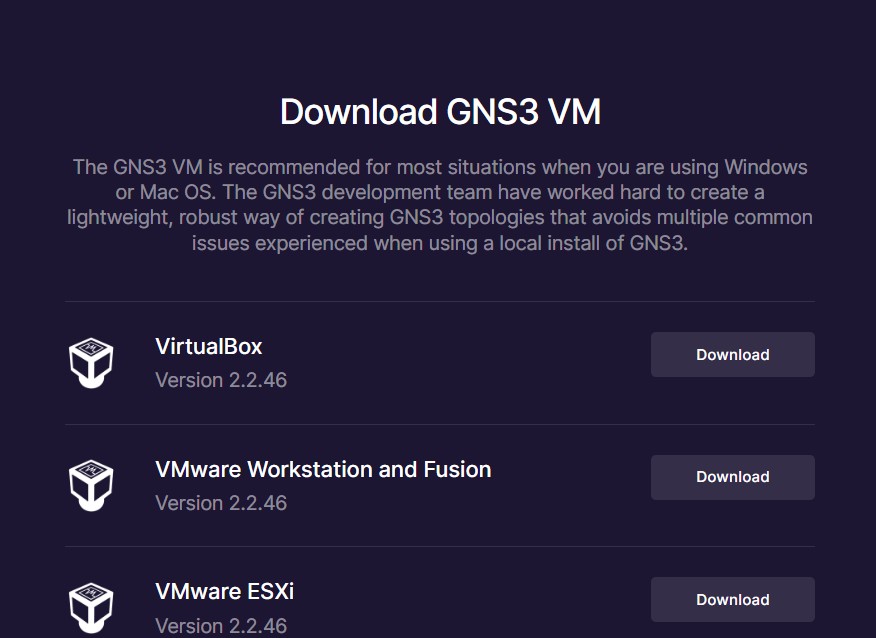
**Objective:** The objective of this experiment is to deploy the GNS3 (Graphical Network Simulator- 3) software on both local host infrastructure and a virtualized environment. The aim is to gain practical experience in setting up GNS3 for network simulation and emulation, enabling the creation of virtual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

### Procedure:

1. **Setup:**
   * Install GNS3 software on the local host infrastructure and the virtualized environment (such as VMware or VirtualBox).

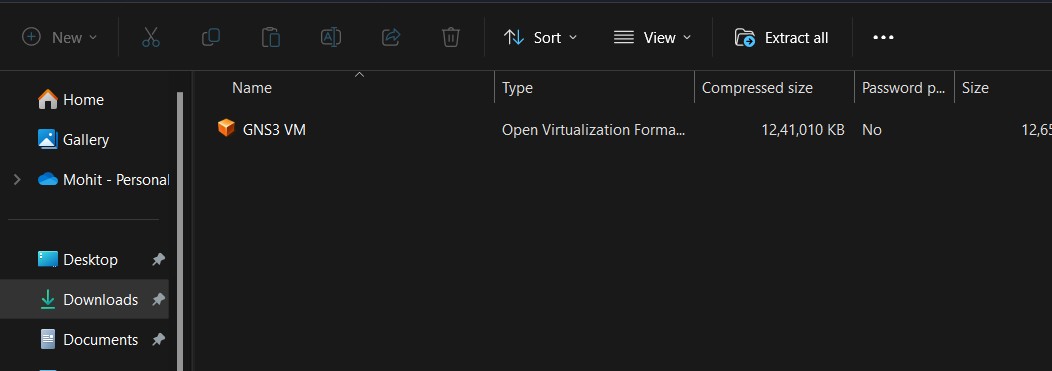


* + Ensure that the system meets the minimum requirements for running GNS3, including CPU, RAM, and storage capacity.

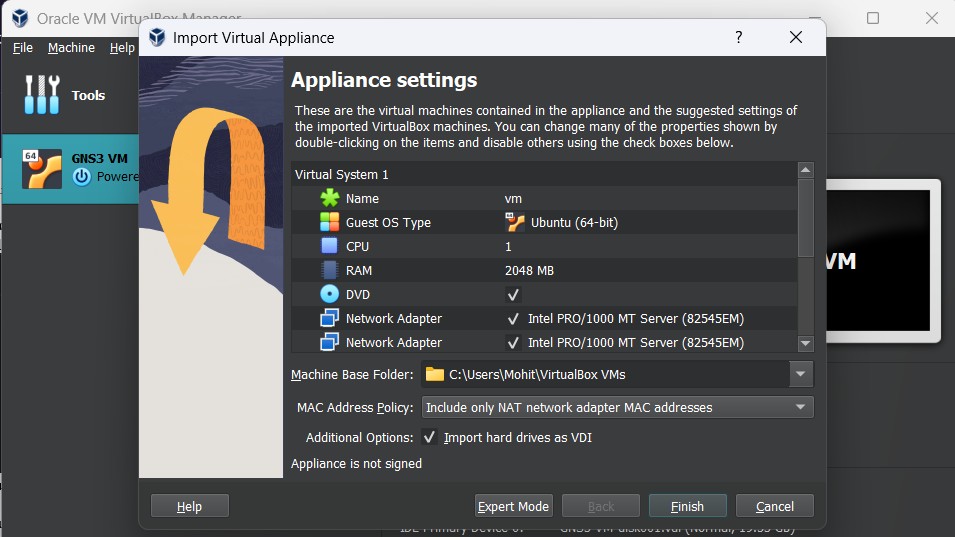


### Configuration on Local Host Infrastructure:

* + Launch the GNS3 application on the local host.

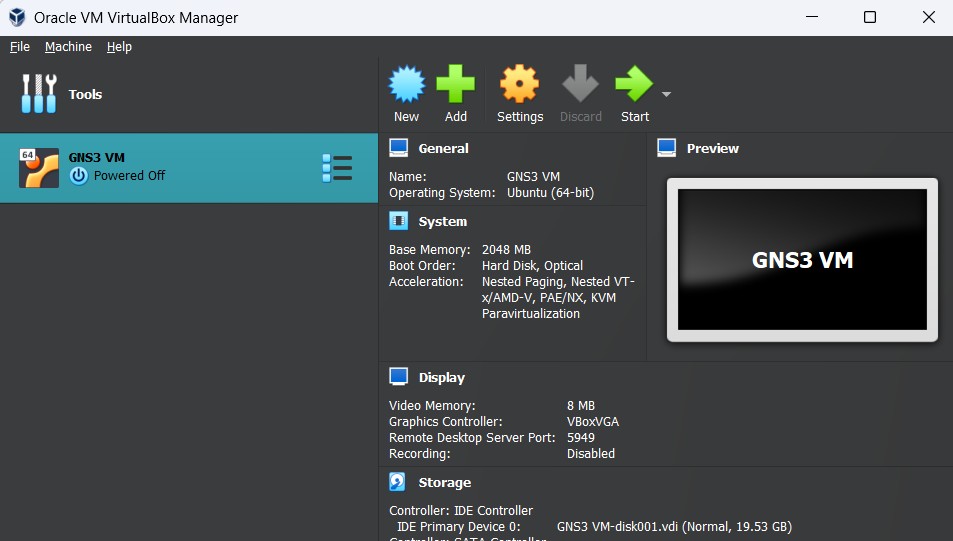


* + Configure GNS3 preferences, including workspace location, server settings, and interface bindings.



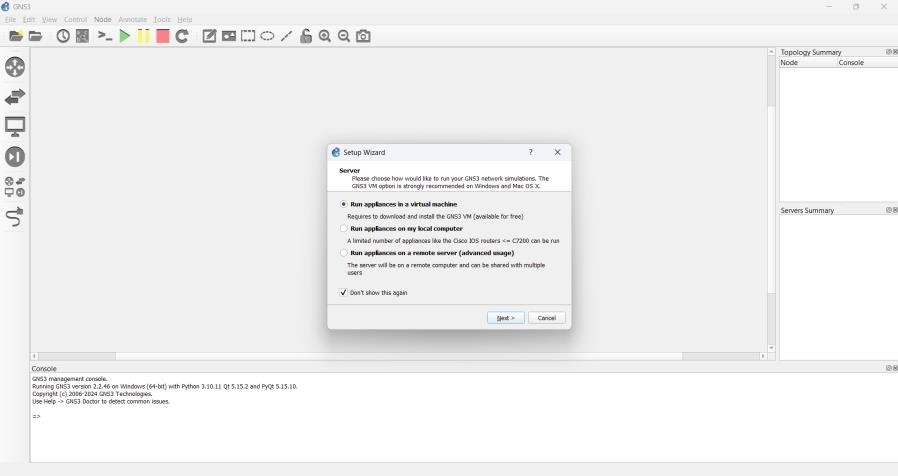
* + Import or create network topologies using routers, switches, and other virtual **devices**

available in GNS3.



### Configuration on Virtualized Environment:

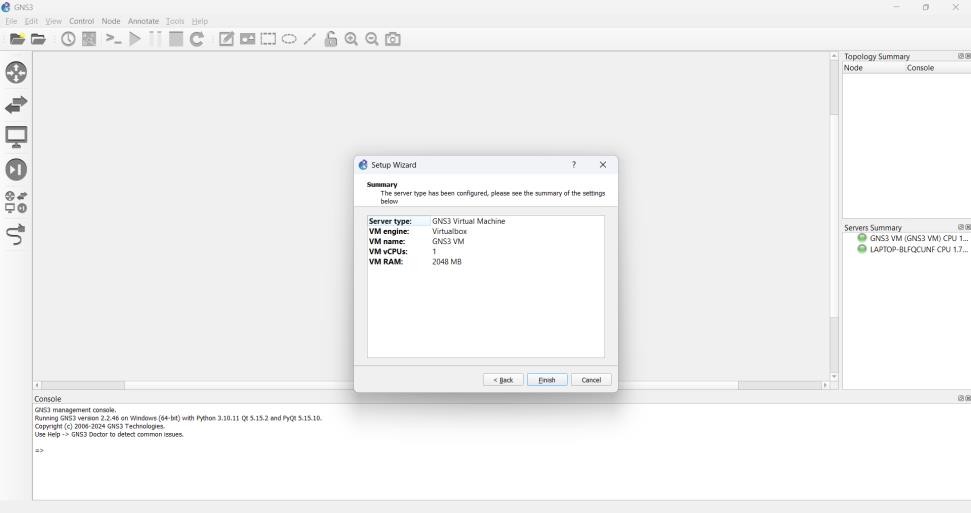
* + Set up a virtual machine (VM) on the virtualization platform (VMware or VirtualBox).



* + Install the GNS3 software within the virtual machine's operating system.
  + Configure GNS3 preferences and settings within the virtual machine to align with the local host infrastructure.

### Integration with Physical Network Devices:

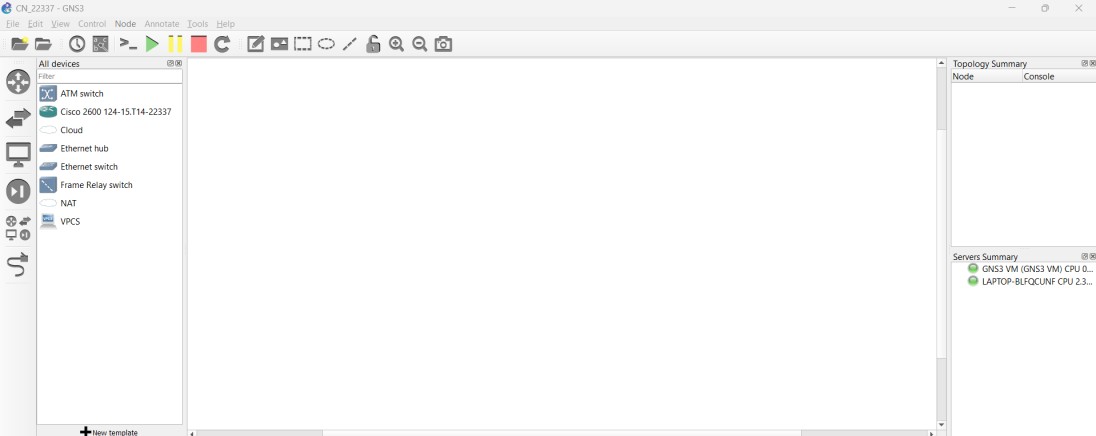
* + Connect GNS3 virtual devices to physical network devices (routers, switches) for simulating real-world network scenarios.



* + Configure network interfaces and mappings to establish connectivity between virtual and physical devices.

### Network Simulation and Emulation:

* + Create and configure network topologies within GNS3, including routers, switches, VLANs, and IP addressing schemes.
  + Start and run simulations to test network configurations, routing protocols, and network services.



* + Monitor network performance, traffic flows, and device behavior using built-in GNS3 tools and utilities.

### Testing and Validation:

* + Validate the functionality of network configurations by verifying connectivity, routing tables, and traffic forwarding.
  + Perform troubleshooting exercises to identify and resolve network issues within the simulated environment.

### 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.

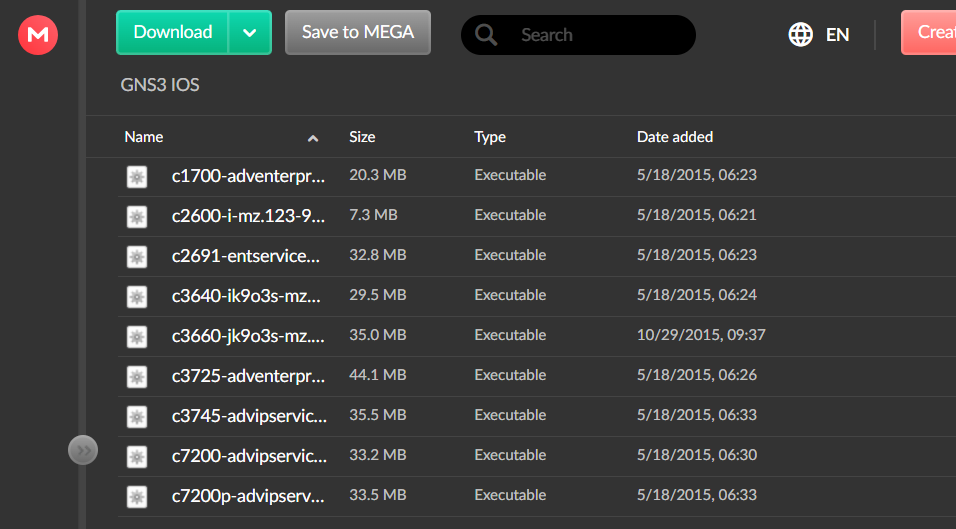
# Practical 8

### Aim: 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:

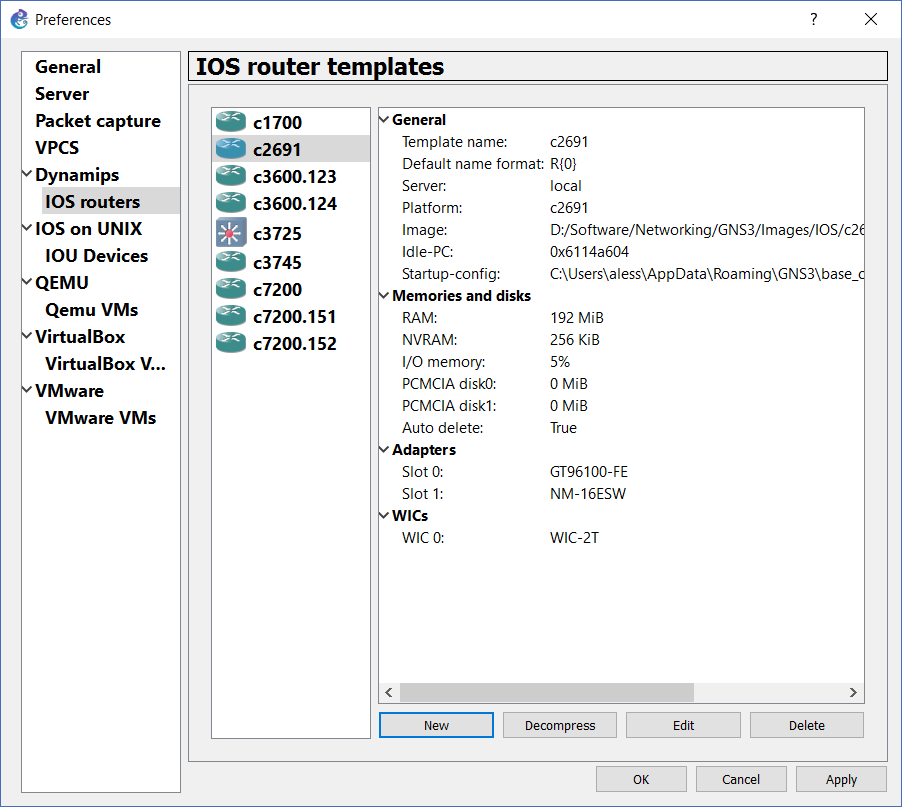
1. **Setup**:
   * Launch the GNS3 application and ensure the CISCO 1700 router image is imported into GNS3.



* + Drag and drop the CISCO 1700 router icon onto the GNS3 workspace.

### Router Configuration:

* + Double-click on the router icon to access the router console.



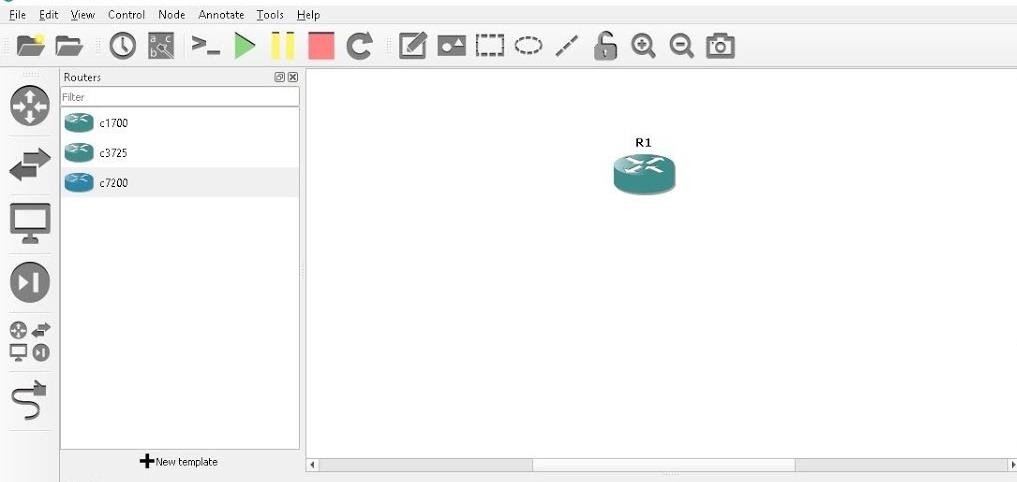
* + Power on the router and configure basic settings such as hostname and domain name.

### Interface Configuration:

* + Identify available interfaces on the CISCO 1700 router (e.g., FastEthernet, Serial).
  + Assign IP addresses and subnet masks to the router interfaces.
  + Activate interfaces using the no shutdown command.

### Static Routing Configuration:

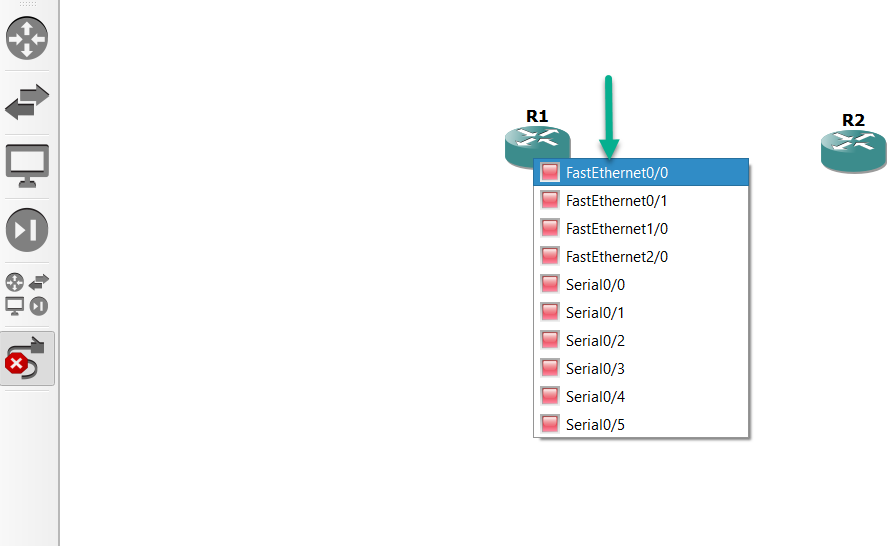
* + Configure static routes on the router to specify paths to remote networks.



* + Use the ip route command to define destination networks and next-hop routers.

### Dynamic Routing Configuration (Optional):

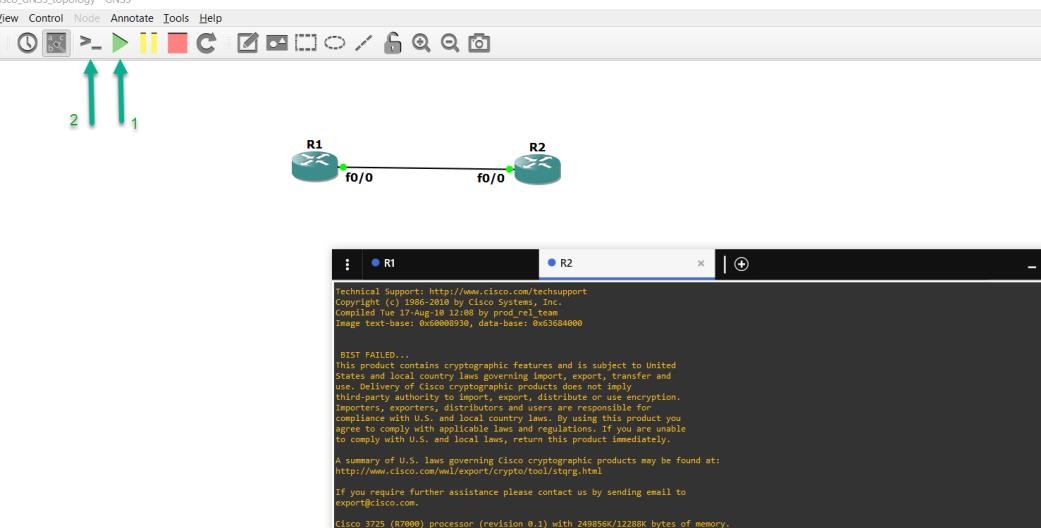
* + Implement dynamic routing protocols like OSPF or EIGRP for automatic route updates.



* + Configure router interfaces to participate in the routing process and exchange routing information with neighboring routers.

### Testing Connectivity:

* + Verify connectivity between the CISCO 1700 router and other devices in the GNS3 topology.
  + Use the ping command to test connectivity to remote networks and devices.



* + Ensure that static or dynamic routes are functioning correctly.

### Additional Configuration (Optional):

* + Implement additional features such as access control lists (ACLs), NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol), or VPN (Virtual Private Network) configurations based on requirements.

### 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**

### Aim: Determining Optical Network Route using Dijkstra's Algorithm

**Theory:** Dijkstra's Algorithm is a graph traversal algorithm that efficiently finds the shortest path between two nodes (source and destination) in a weighted graph. In the context of optical networks, nodes represent network routers or switches, and weights represent signal attenuation or other factors affecting transmission efficiency. The algorithm prioritizes paths with lower weights, ensuring the most efficient data transfer.

**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.

### Code:

#include <iostream> using namespace std; #include <limits.h> #define V 9

int minDistance(int dist[], bool sptSet[])

{

int min = INT\_MAX, min\_index; for (int v = 0; v < V; v++)

if (sptSet[v] == false && dist[v] <= min)

min = dist[v], min\_index = v; return min\_index;

}

void printSolution(int dist[])

{

cout << "Vertex \t Distance from Source" << endl; for (int i = 0; i < V; i++)

cout << i << " \t\t\t\t" << dist[i] << endl;

}

void dijkstra(int graph[V][V], int src)

{

int dist[V]; bool sptSet[V];

for (int i = 0; i < V; i++)

dist[i] = INT\_MAX, sptSet[i] = false; dist[src] = 0;

for (int count = 0; count < V - 1; count++) { int u = minDistance(dist, sptSet);

sptSet[u] = true;

for (int v = 0; v < V; v++)

if (!sptSet[v] && graph[u][v] && dist[u] != INT\_MAX

&& dist[u] + graph[u][v] < dist[v]) dist[v] = dist[u] + graph[u][v];

}

printSolution(dist);

}

int main()

{

int graph[V][V] = { { 0, 4, 0, 0, 0, 0, 0, 8, 0 },

{ 4, 0, 8, 0, 0, 0, 0, 11, 0 },

{ 0, 8, 0, 7, 0, 4, 0, 0, 2 },

{ 0, 0, 7, 0, 9, 14, 0, 0, 0 },

{ 0, 0, 0, 9, 0, 10, 0, 0, 0 },

{ 0, 0, 4, 14, 10, 0, 2, 0, 0 },

{ 0, 0, 0, 0, 0, 2, 0, 1, 6 },

{ 8, 11, 0, 0, 0, 0, 1, 0, 7 },

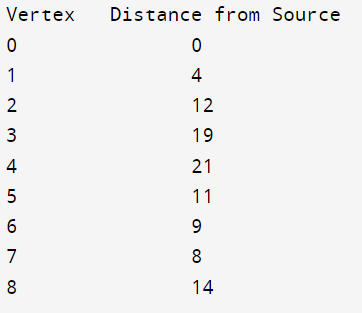
{ 0, 0, 2, 0, 0, 0, 6, 7, 0 } };

dijkstra(graph, 0);

return 0;

}

### Output:



**Conclusion:**

The implementation of Dijkstra's Algorithm to determine the optimal route for data transmission in an optical network. The provided code offers a basic framework and can be modified to incorporate additional factors specific to real-world networks, such as wavelength availability and signal modulation techniques. By employing Dijkstra's Algorithm, network operators can optimize data routing, improve network performance, and ensure efficient transmission across optical networks.

# Practical 10

### Aim: 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.

### 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.

### 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.

### 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.

1. 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:

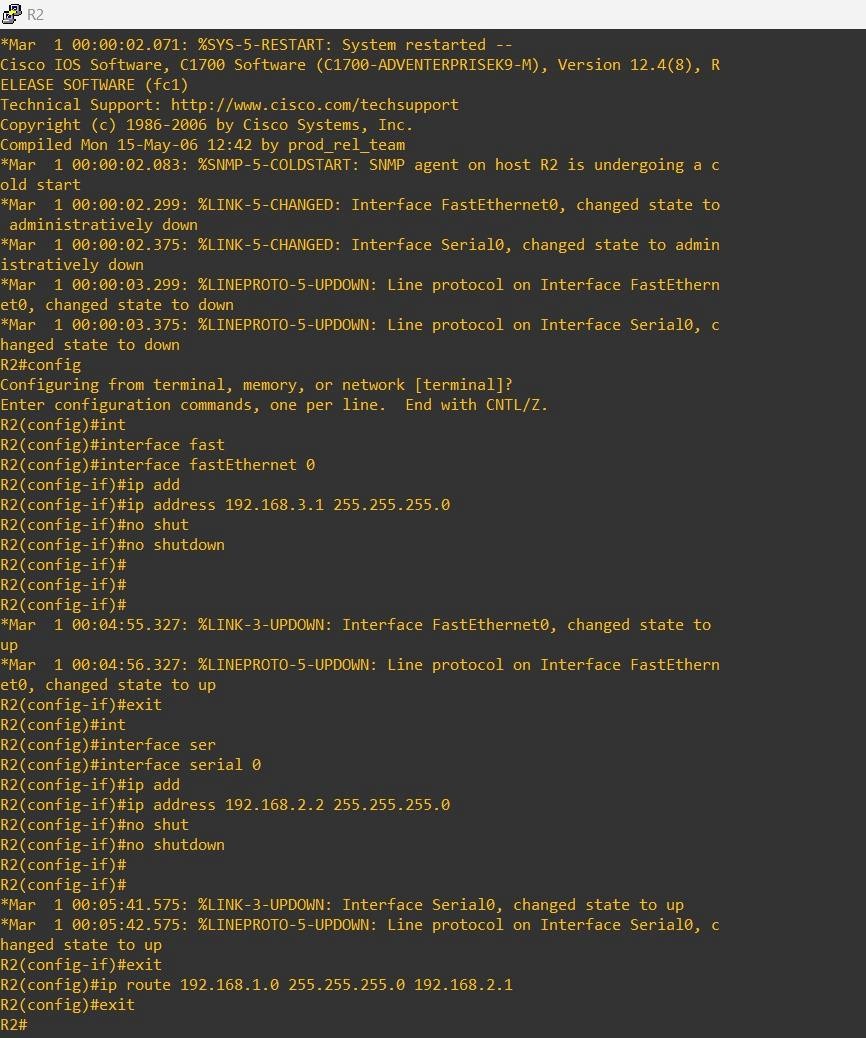
* While the experiment focused on setting up the LAN topology and configuring basic IP addressing, routing functionality was not implemented.
* The experiment provided valuable experience in configuring LAN devices, assigning IP addresses, and verifying connectivity within the LAN topology.
* Further 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.

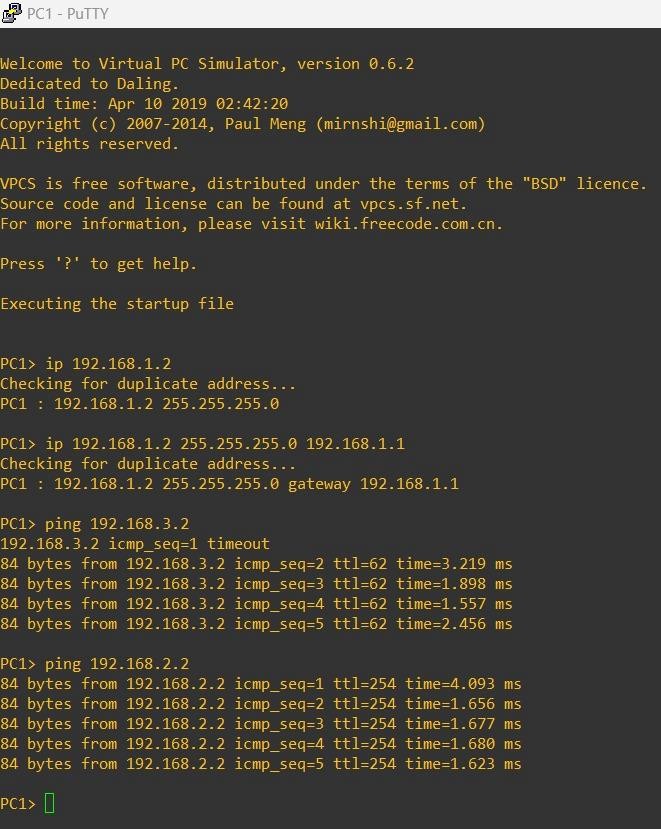
**Practical 11**

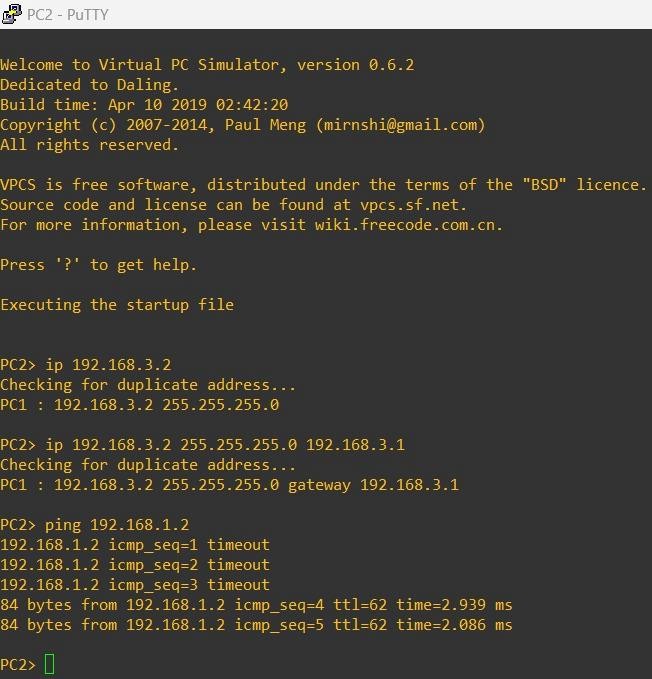
### Aim: Configuration of Static Routing in a Network with Two Routers and Four Switches

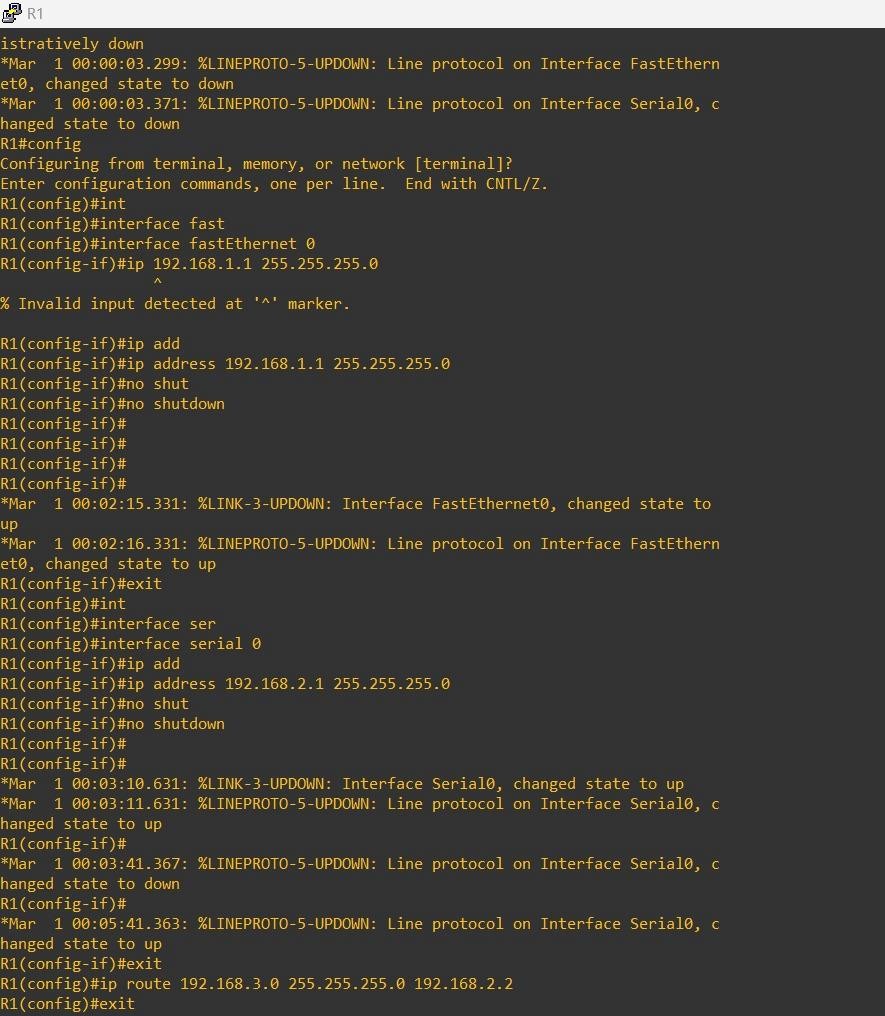
**Theory:** Static routing is a simple and efficient method of routing in which routes are manually configured by a network administrator. Unlike dynamic routing protocols, static routes do not change automatically based on network conditions but remain fixed until manually modified. In this setup, we have two routers acting as gateways for different network segments and switches to connect multiple devices within each segment. By configuring static routes on the routers, we can define the paths for forwarding packets between these segments.

### Configuration:









**Conclusion:**

In this practical report, we successfully configured static routing in a network setup comprising two routers and four switches. By configuring static routes on the routers, we established communication between different network segments. Static routing provides a simple and predictable method of routing, suitable for small-scale networks where routing tables are relatively static and network changes are infrequent. However, for larger and more dynamic networks, dynamic routing protocols may be more suitable to adapt to changing network conditions automatically.

## Practical 12

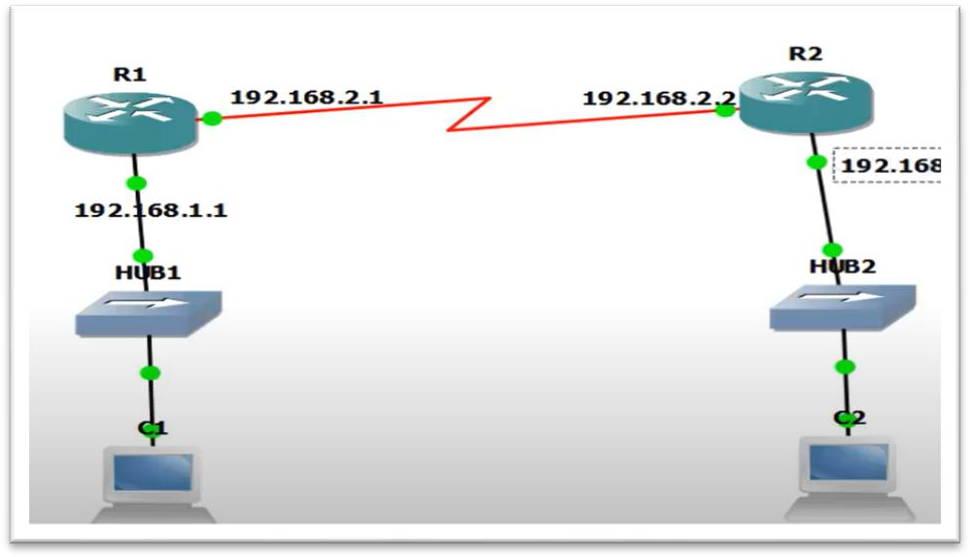
### Aim: Configuration of RIP routing in a network build using CISCO 1700 routers in GNS 3.

**Theory:**

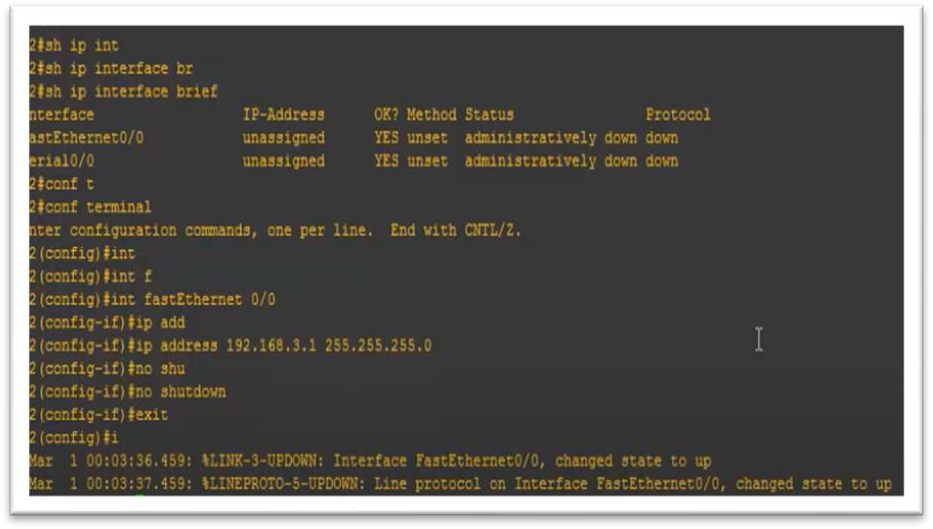
1. **RIP (Routing Information Protocol)** is a dynamic routing protocol used in local and wide area networks. It uses hop count as a routing metric to find the best path between the source and the destination network.
2. **Cisco 1700 routers** are configured to use RIP in GNS3, a network simulator. The 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.



1. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
2. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router**.**
3. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router’s settings**.**
4. **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**.**



1. **Enable Interfaces:** Use the no shutdown command to enable each interface. This will bring the interfaces up and make them ready for data transmission.
2. **Enable RIP:** Type router rip to enable RIP on the router. This will start the RIP routing process on the router.
3. **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**.**
4. **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

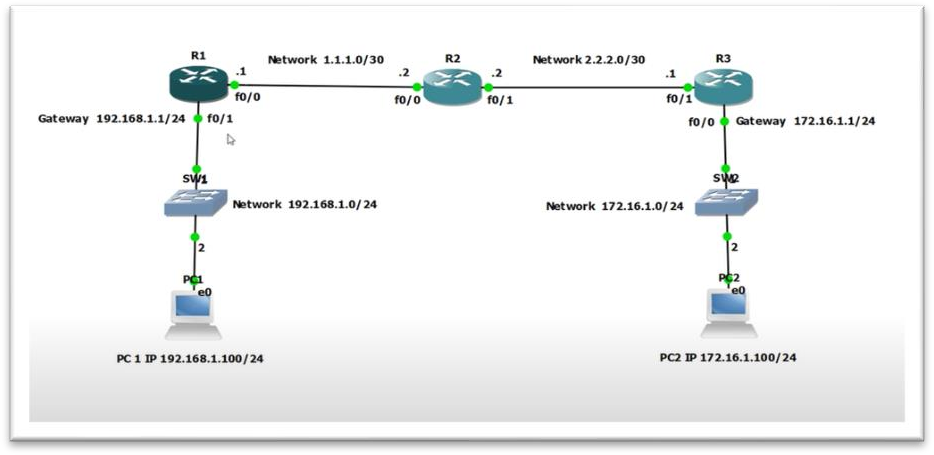
### Aim: Configuration of OSPF routing in a network build using CISCO 1700 routers in GNS 3.

**Theory:**

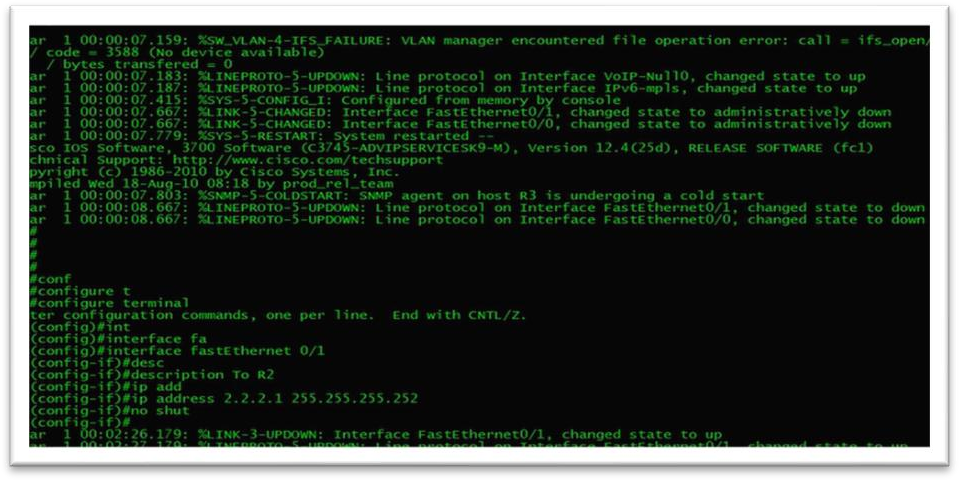
1. **OSPF (Open Shortest Path First)** is a link-state routing protocol that uses Dijkstra’s algorithm to find the shortest path for routing packets through a network.
2. **Cisco 1700 routers** are configured to use OSPF in GNS3, a network simulator. The routers exchange link-state information to maintain 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.



* 1. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
  2. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router.
  3. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router’s settings.
  4. **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.



* 1. **Enable Interfaces:** Use the no shutdown command to enable each interface. This will bring the interfaces up and make them ready for data transmission.
  2. **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.
  3. **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.
  4. **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.

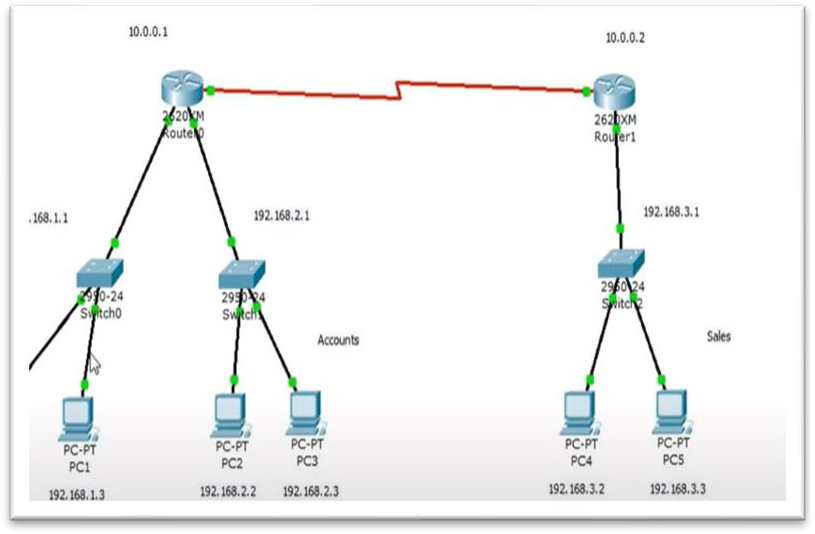
## Practical 14

### Aim: Implement a basic Access Control List (ACL) in Cisco router using GNS3. Theory:

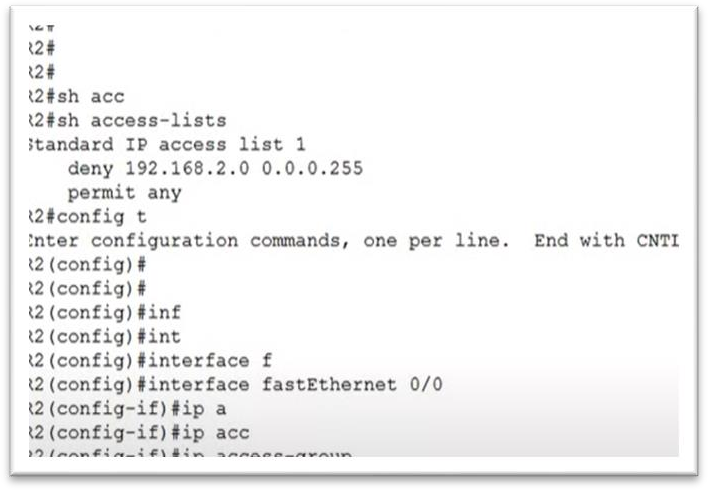
1. **Access Control List (ACL)** is a set of rules defined for controlling the network traffic and reducing network attacks.
2. **ACLs** are used to filter traffic based on the IP address, protocol, or port number on a Cisco router.
3. **GNS3 (Graphical Network Simulator-3)** is a network software emulator 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.



1. **Start the Routers:** Power on the routers in GNS3. This will initialize the routers and make them ready for configuration.
2. **Access Router Console:** Open the console of each router. This will provide you with a command-line interface for configuring the router.
3. **Enter Configuration Mode:** Type configure terminal to enter the global configuration mode. This mode allows you to modify the router’s settings.
4. **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.
5. **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.
6. **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.



1. **Exit Configuration Mode:** Type end or press Ctrl+Z to exit the configuration mode.
2. **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.