NetPath Illuminator: The Network Odyssey

Project Overview:

The objective of the " NetPath Illuminator" project is to integrate practical networking lab experiences with the creation of an innovative tool that allows students to explore the packet flow through various network devices and topologies as well as, if possible, extend the vision to create a tool which can provide the Real-Time Packet Journey as well as allow users to query the network events. This tool aims to create a real-time graphical representation of how data packets travel from their source to destination, navigating through the layers of a network, and highlighting the interactions with switches, routers, and across different subnet boundaries.

The project will synthesize the learning objectives from the seven networking labs/Levels into the development of a comprehensive system. Students will be able to input their network configurations and observe the dynamic journey of packets as they cross various network segments.

Project Description:

1. Networking Fundamentals Integration: Students will use knowledge gained from Level 1 to 8 to simulate network environments and visualize the packet flow in those scenarios. The concepts of ARP, MAC (Media Access Control) tables, Switching, IP routing, Routing tables, Static routing and Dynamic routing protocols will all contribute to the representation of packets as they traverse the network.

2. Packet Sniffer – Students can use the packet sniffer which is an inbuilt tool in Packet Capture (tutorial available at

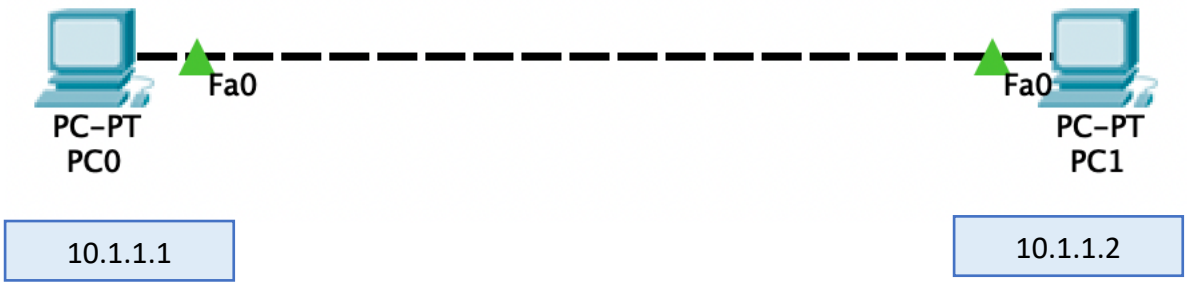
https://www.youtube.com/watch?v=gsCSKQAVT2M) or a tool like Wireshark to dump packet captures in various Levels in the pcap format.

3. Visualization Component: Students can put the packet captures into a database. Additionally, they can design a basic visualization system that graphically displays the packet flow at each Level. It should highlight the path packets take, including intermediate devices they traverse, any routing decisions made, and the final delivery to the destination.

Expansion beyond this project's parameters: Students can augment the project by developing an AI-powered packet analyzer. They would train their models using the captured packets. Students can draw inspiration from open-source projects such as Packet Buddy or Packet RAPTOR and incorporate their unique models.

Levels:

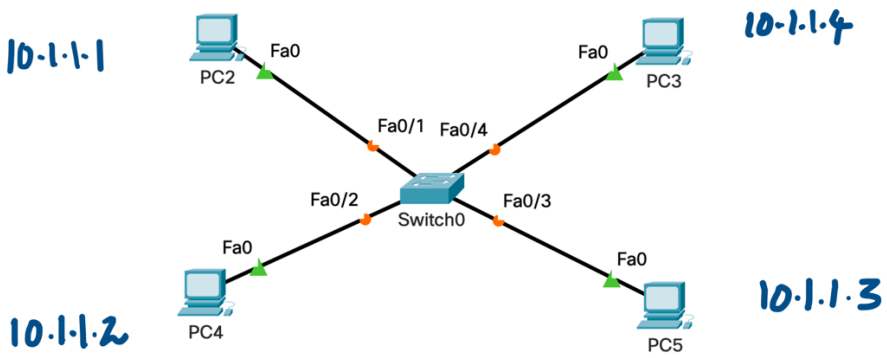
- Level-1: The objective is to establish a connection between two PCs and assign specific IP addresses to them. The main task is to examine the communication process using the "ping" command. Additionally, we will explore the purpose of Address Resolution Protocol (ARP) and understand why both MAC and IP addresses are necessary. We will also learn about ARP tables and how to view them.



(Hint: If you are using Cisco Packet Tracer, you can experiment with commands such as "arp -d" and "arp -a" on the computers. These

commands allow you to manage the Address Resolution Protocol (ARP) cache. By using "arp -d", you can delete entries from the ARP cache, and with "arp -a", you can view the contents of the ARP cache, which provides information about the IP-to-MAC address mappings.)

- **Level-2:** The objective is to establish a connection between multiple computers using a switch and assign unique IP addresses to each computer. The Level involves performing "ping" tests between neighboring computers to verify connectivity. Also, we will explore the MAC table in the switch and understand its fundamental functionalities such as learning, flooding, and forwarding. Furthermore, we will experiment with basic configuration and view commands on the switch to familiarize ourselves with its operation.



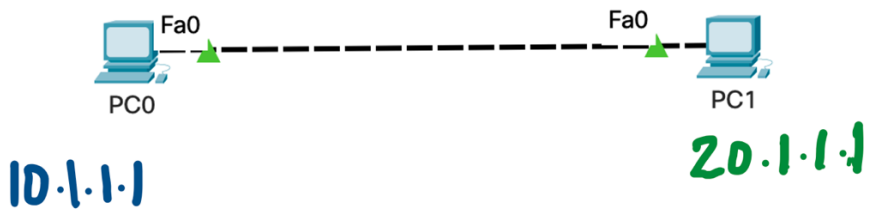
The command "show mac address-table" provides a view of the MAC address table entries stored on the switch. It reveals details such as MAC addresses associated with each port, VLAN assignments (where applicable), and the aging time designated for each entry. Additionally, students can delve deeper into the significance of VLANs, their configuration process, and the function of aging timers in network management.

To explore different command modes and configurations in Cisco IOS, you can begin with:

- User EXEC mode: Accessible upon login, limited to basic commands like 'show' and 'ping'.
- Privileged EXEC mode: Entered using 'enable', allows configuration changes and detailed troubleshooting.
- Global Configuration mode: Accessed with 'configure terminal', used for device-wide settings such as the switch's name ('hostname Switch1').
- Interface Configuration mode: Accessed with 'interface interface_name', used to configure specific interfaces on the switch ('interface FastEthernet0/1').
- Show Commands: Examples include 'show running-config' to display the current configuration of the switch.
- Troubleshooting Commands: Such as 'ping' to test connectivity.

These commands and modes are essential for configuring, monitoring, and troubleshooting Cisco devices effectively.

- **Level-3**: In this Level, two computers are connected directly to each other using a wire, and different IP addresses are assigned to them with separate subnets. When attempting to ping one PC from the other, the ping operation fails. The objective is to investigate the reason behind this failed ping, despite the direct connection between the computers.

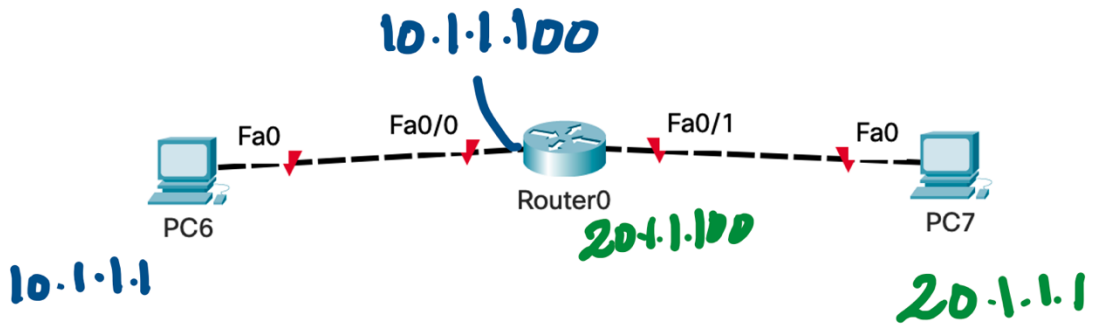


More Information: We observe that the ARP resolution is not occurring, leading to the failure of the ping. The Address Resolution Protocol (ARP) is responsible for mapping IP addresses to MAC addresses. In this case, since the computers are on different subnets, they are not in the same broadcast domain. As a result, the ARP messages from one PC cannot reach the other PC, preventing the MAC address resolution and subsequent successful communication.

This situation highlights the need for routers. Routers are devices that operate at the network layer (Layer 3) of the OSI model and facilitate

communication between different subnets or networks. By connecting the two computers through a router, it can perform the necessary routing functions, including ARP resolution between subnets. This enables successful communication between devices on different subnets by forwarding packets between them.

- **Level-4:** In this Level, the objective is to establish a connection between two computers using a router. The computers are configured to have different IP addresses. The Level involves performing a ping test from one computer to the other. Additionally, we will examine the routing table and route entries using commands such as "show ip route" and "show ip inter brief". This will allow us to understand how routing works and observe the routing entries.



It is also important to understand the concept of a default gateway and its significance in networking. The default gateway refers to the IP address of the router that serves as the exit point for traffic from a local network to other networks. The need for a default gateway arises when a device within a network needs to communicate with devices outside of its immediate network or subnet. When a device receives a packet destined for an external network, it checks its routing table to determine if it has a specific route for that destination. If there is no specific route available, the device forwards the packet to the default gateway.

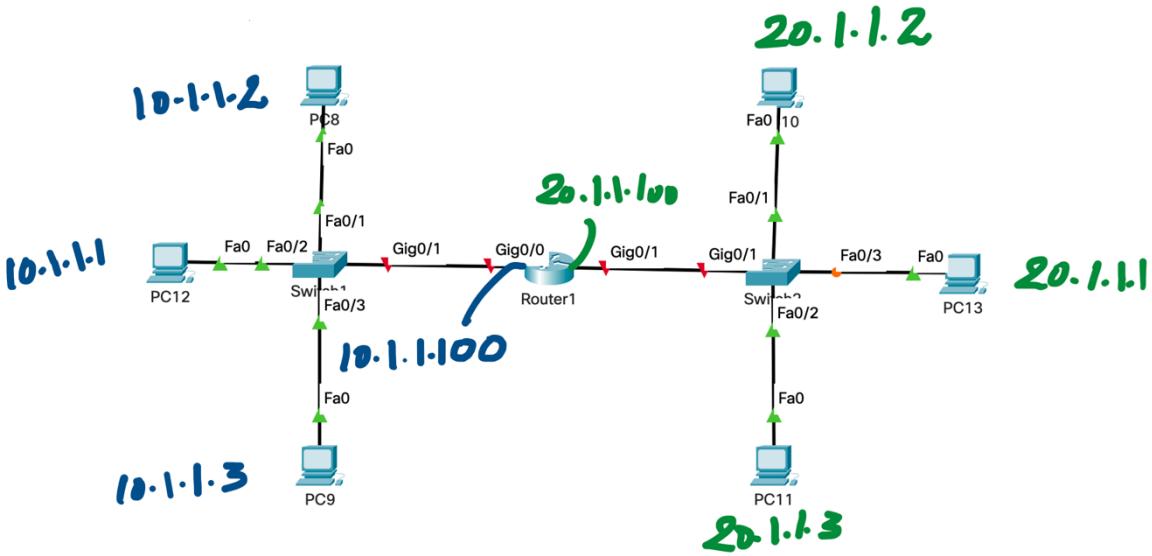
The default gateway acts as the intermediary, forwarding packets from the local network to external networks, such as the internet. It serves as the entry and exit point for traffic going in and out of the

local network, enabling communication with devices located in different networks or subnets.

In summary, the default gateway plays a crucial role in enabling network connectivity beyond the local network. It facilitates the routing of packets to external networks, allowing devices to communicate with resources outside of their immediate network.

- **Level-5:** The objective is to establish connectivity between multiple computers by utilizing two separate networks, a router, and a switch. The setup involves connecting the computers to the switch, which in turn is connected to the router, thereby enabling communication between the two networks.

  The Level focuses on understanding how ping operations work between the two networks. By initiating ping commands from computers in one network to computers in the other network, we can examine the functionality of inter-network communication.

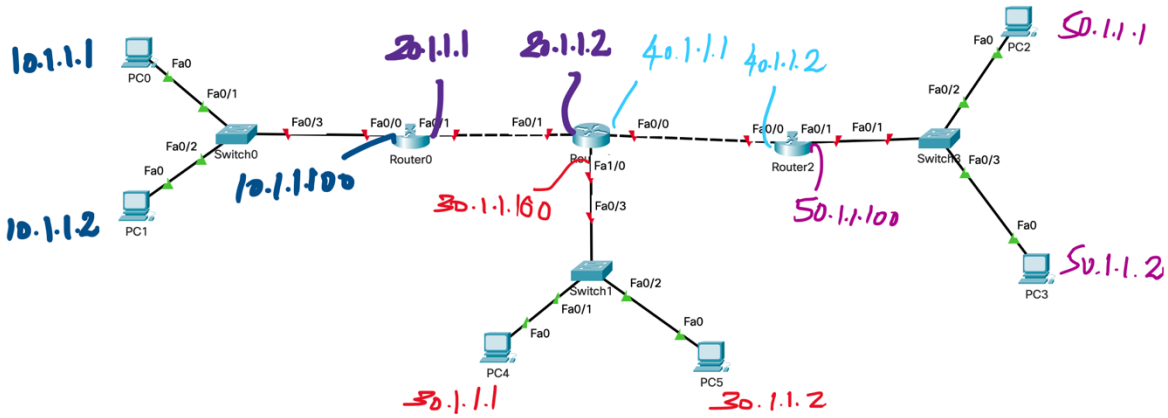


Additionally, we will explore the routing table in the router, which contains information about network routes and helps determine the best path for forwarding packets between the networks. The ARP table, which maintains IP-to-MAC address mappings, will also be examined to observe how address resolution occurs across the networks.

Furthermore, we will investigate the MAC table within the switch. The MAC table stores MAC addresses and associated ports, allowing the switch to efficiently forward frames to the correct destination.

By examining the routing table, ARP table, and MAC table, we can gain insights into the network's routing and switching operations, addressing resolution, and how the switch manages and forwards traffic between the connected networks.

- Level-6: The objective is to establish connectivity between different networks using routers. We will configure static routes to connect multiple networks. By utilizing the appropriate router commands, we can configure static routes and examine their configuration using the "show ip route" command.



Static routes are manually defined routes that specify the network destinations and next-hop routers to reach those destinations. By configuring static routes, we can direct traffic from one network to another through specific routers.

We will explore the routing information base (RIB) within the routers. The RIB is a database that contains routing information, including static routes, dynamic routes, and administrative distance values. It helps the router determine the best path for forwarding packets based on the destination IP address.

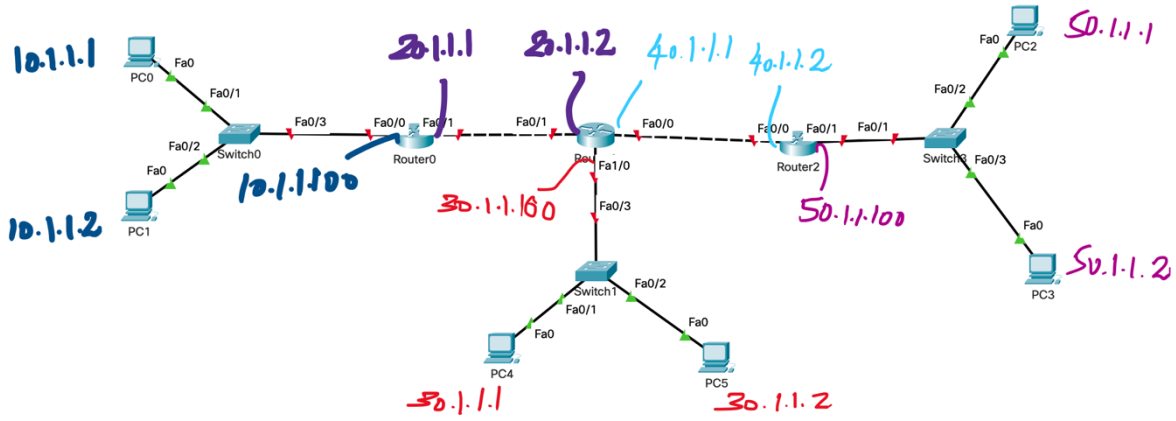
By using the "show ip route" command, we can view the contents of the RIB and observe the configured static routes. This command

provides valuable information about the routing table, including network prefixes, next-hop routers, and administrative distances.

Understanding the RIB and how routers work is crucial for comprehending the decision-making process involved in routing packets. Routers analyze the destination IP addresses of incoming packets, consult the RIB, and use various routing protocols or static route configurations to determine the best path for forwarding the packets toward their destinations.

By configuring static routes, examining the RIB, and studying the router's operation, we can gain insights into how routers handle packet forwarding and how network connectivity is established between different networks

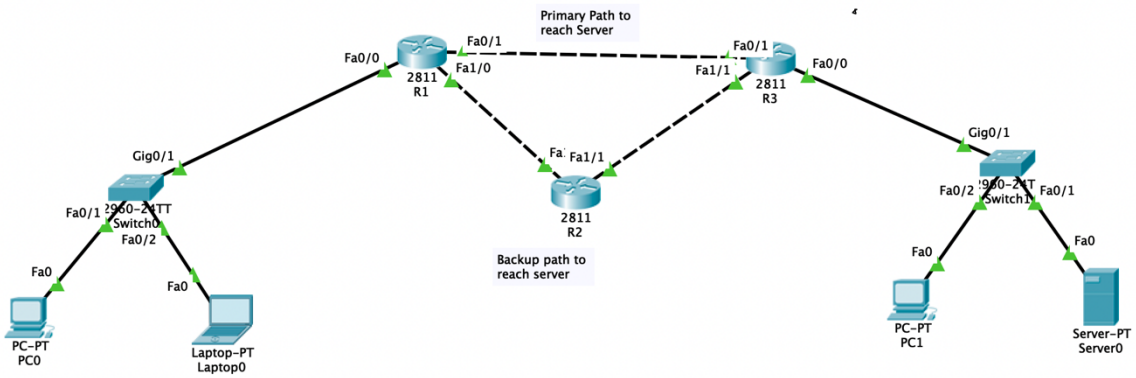
- **Level-7:** The objective is to establish connectivity between multiple networks using routers. We will configure a dynamic routing protocol, such as OSPF (Open Shortest Path First), on each router in the Level. The focus will be on understanding how OSPF operates and how it builds the routing table.



We will utilize OSPF-specific show commands to examine how OSPF works. These commands provide insights into OSPF's behavior, including the OSPF Neighbour relationships, the states of OSPF interfaces, and the OSPF routing table. By using the show ip route command, we can check the resulting IP route table, which contains information about OSPF-learned routes and their associated next hops.

By configuring OSPF, analyzing the OSPF show commands, examining the IP route table, and reviewing the show ip int brief table, we can gain a deeper understanding of how OSPF facilitates efficient routing within a network and how it dynamically builds the routing table to determine the best paths for packet forwarding.

Level-8: To establish network connectivity between multiple networks using routers by configuring OSPF (Open Shortest Path First) on each router. In this level, one needs to have Primary and Backup path (with one extra hop or one can even configure higher cost) to reach the server. With these two paths, one needs to capture the packets to reach to the server and observe the packet flow. Then one needs to shutdown the link Fa0/1 at R1 so that Primary path goes down. Then observe in the packet path. How OSPF dynamically reroutes packets after convergence.



Deliverables:

- Students must simulate all the above network Levels and do capture the commands mentioned.
- Students must utilize a packet sniffer or Wireshark to intercept the packets at each node during every Level Students should analyze the packets captured from different devices (nodes), students can extract relevant information from the packet headers, particularly noting changes occurring in the Ethernet and IP headers. This data will enable them to create a flow diagram illustrating the path of the packet flow from their device (host) to the external network.
- Students are free to select any flowchart creation tool to depict the packet path.

Assessment Criteria: Upon completion of the above projects, students are expected to -

- Explain the distinction between MAC learning and IP networking
- Differences between Layer 2 and Layer 3 networks.
- Explain the function of subnetting and the workings of the Address Resolution Protocol (ARP).
- Explain the role of a default gateway, the process required for packets to move between subnets, and the initial steps for troubleshooting connectivity issues.
- Should be able to differentiate between a router and a switch in more practical manner.
- Should be able to articulate the purpose of static routing and the method by which network connectivity is established across different networks.
- What does Routing Information Base (RIB) mean
- One should be able to define what a routing protocol is, the differences between static and dynamic routing protocols, and provide an example of a dynamic routing protocol.
- Explain how the ping function works? Additionally, elaborate on the significance of the ICMP protocol? Develop a ping program using C/C++. Implementing a basic ping program involves using sockets to send ICMP (Internet Control Message Protocol) echo requests and handle ICMP echo replies.
- Explain the basic flow of packet from PC to a web server located outside the campus.

By completing the "NetPath Illuminator" project, students will gain a practical understanding of networking concepts, apply their theoretical knowledge to a real-world application.