**Experiment-6**

**Part A**

**Aim:** Simulation of Open Shortest Path First (OSPF).

**Prerequisite:** Nil

**Outcome:** To impart knowledge of Computer Networking Technology

**Theory:**

Open Shortest Path First (OSPF) functions as an Interior Gateway Protocol (IGP) designed for routing data within a single autonomous system (AS). It operates as a link-state protocol, preserving a network topology database used to determine the most efficient path between any two nodes in the network. OSPF is classified as a classless protocol, which implies that it does not discriminate between various classes of IP addresses, rendering it a suitable option for networks with diverse IP address classes. It has earned a reputation for its dependability and scalability, making it a prevalent choice in enterprise networks.

OSPF employs a flooding algorithm to disseminate routing information across the network. When a router enters an OSPF network, it transmits a Hello packet to all its neighbouring routers, containing essential information like its IP address and the OSPF version it supports. If a neighbouring router responds to the Hello packet, they establish a neighbour relationship, allowing for the exchange of routing data.

The heart of OSPF's operation is its link-state database, which stores details about the network's topology. This database comprises link-state advertisements (LSAs), each conveying information about a single link, such as the link's IP address, cost, and state. The link-state database is instrumental in computing the shortest path between any two network nodes.

OSPF leverages the Dijkstra algorithm for determining the shortest path between nodes in the network. The Dijkstra algorithm constructs a tree of nodes where each node represents a potential path from the source node to the destination node. It starts by including the source node in the tree and subsequently appends nodes with the lowest cost to the tree. This process continues until the destination node is reached.

OSPF stands out as a dependable and scalable protocol extensively employed within enterprise networks. It operates as a link-state protocol, overseeing a network topology database crucial for determining the most efficient routes between any pair of network nodes. What sets OSPF apart is its classless nature, as it does not differentiate between various IP address classes. This feature makes OSPF a preferred option for networks that incorporate a diverse range of IP address classes. Consequently, OSPF remains a well-regarded choice for ensuring robust and adaptable network communication in enterprise settings.

**Procedure:**

1. Open Cisco Packet Tracer and simulate the sample topologies for OSPF.

2. Perform Necessary Operation on Switch to create and configure OSPF.

3. Check the connectivity between the devices.

**Part – B**

**Steps:**

1. Topology Setup: Create your network topology in Packet Tracer with routers and connections.

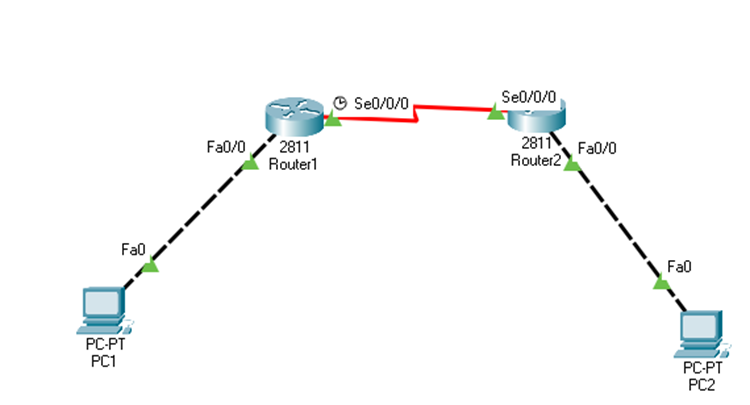
2. Router Configuration: Assign IP addresses and default gateways to the interfaces of your routers.

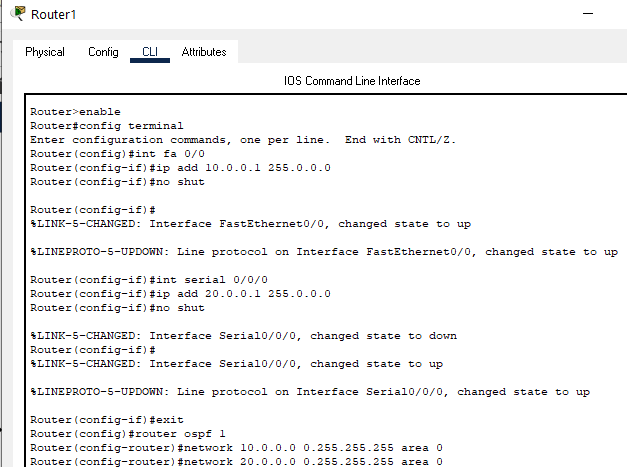
3. OSPF Configuration: Activate OSPF routing on your routers and set unique process ID for each OSPF instance. Also, define the network and area for OSPF.

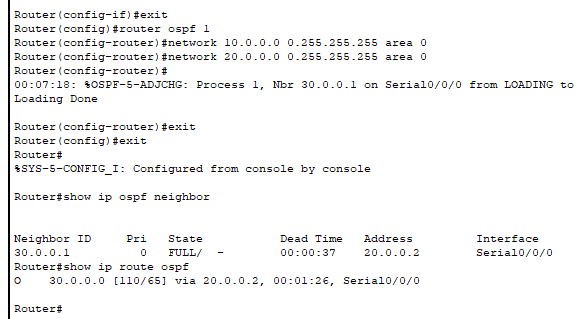
4. Implement OSPF Single Area Network: Configure the implementation of OSPF in the Network.

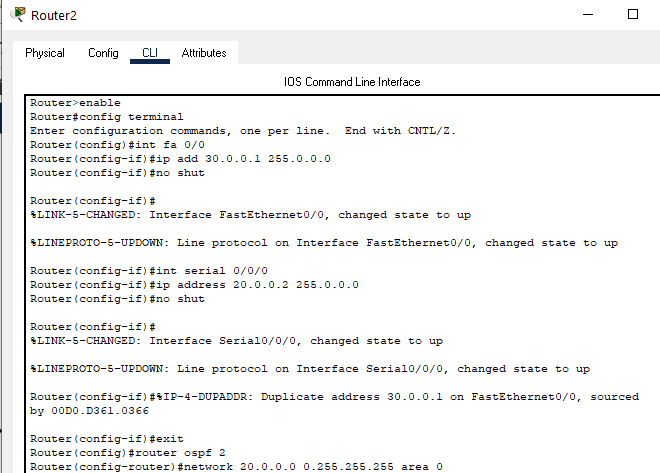
5. Verify OSPF Implementation: Use show commands to verify whether the implementation of OSPF is done correctly or not.

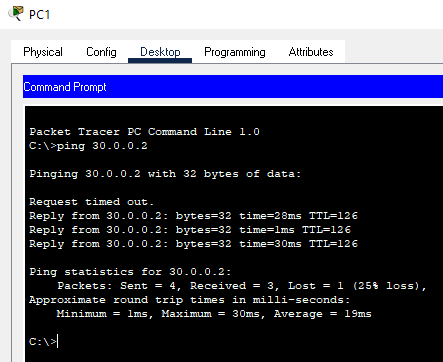
**Output:**











**Observation & Learning:**

During our OSPF implementation experiment in Cisco Packet Tracer, we noticed that OSPF effectively facilitated the establishment of dynamic routing, the exchange of routing information, and the continuous maintenance of network connectivity. This experience emphasized the crucial significance of maintaining consistent process IDs and accurately specifying network addresses when working with OSPF. Overall, the experiment underscored OSPF's pivotal role in automating routing procedures, guaranteeing the efficient transmission of data, and adapting to network alterations, thus emphasizing its essential contribution to the creation of resilient and dependable networks.

**Conclusion:**

In summary, the OSPF implementation experiment in Cisco Packet Tracer showcased OSPF's efficiency in dynamic routing, reinforcing the significance of process ID consistency and accurate network address configuration. It underscored OSPF's crucial role in building resilient and adaptable network infrastructures.

**Questions:**

**1. What is mean by AD value? In case of OSPF, what is its value?**

**Ans:**

In the context of OSPF (Open Shortest Path First), "AD" stands for Administrative Distance. Administrative Distance is a value used in routing protocols to indicate the trustworthiness or reliability of a particular route or source.

In OSPF, the administrative distance is typically set to 110. This value is used to indicate the trustworthiness of OSPF routes when there are multiple routing protocols running on a router. Generally, a lower administrative distance indicates a more trusted or preferred route. OSPF, being an Interior Gateway Protocol (IGP), is considered very reliable and is often assigned a lower administrative distance compared to other routing protocols like RIP (Routing Information Protocol) or EIGRP (Enhanced Interior Gateway Routing Protocol).

Here are some common administrative distance values for reference:

- OSPF: 110

- RIP (Routing Information Protocol): 120

- EIGRP: 90

- Directly connected routes: 0

When a router has multiple routes to the same destination, it selects the route with the lowest administrative distance as the preferred route.

**2. What are the different types of messages which propagates in OSPF?**

**Ans:** In OSPF (Open Shortest Path First), several types of messages are used to propagate routing information and maintain the integrity of the OSPF routing domain. These messages play a crucial role in the operation of the OSPF routing protocol. The main types of OSPF messages include:

1. Hello: Hello packets are used for neighbour discovery and forming neighbour adjacencies. They are exchanged between OSPF routers on the same network segment to establish and maintain neighbour relationships.

2. Database Description (DBD): DBD packets are used to describe the link-state database contents. During the OSPF neighbour formation process, routers exchange DBD packets to compare their link-state databases and identify the differences.

3. Link-State Request (LSR): LSR packets are sent by a router when it identifies differences in the link-state database after receiving DBD packets from a neighbour. LSR packets request specific link-state advertisements (LSAs) that the router is missing.

4. Link-State Update (LSU): LSU packets are used to respond to LSR packets by sending the requested LSAs. These packets contain the actual LSAs needed to synchronize the link-state databases between OSPF neighbours.

5. Link-State Acknowledgment (LSAck): LSU packets are acknowledged by LSAck packets, indicating that the LSU packets were received successfully. LSAcks help ensure the reliability of LSAs during the flooding process.

These OSPF message types work together to establish and maintain OSPF neighbour relationships, exchange routing information in the form of LSAs, and ensure the consistency of link-state databases across the OSPF network. OSPF routers use these messages to calculate and maintain the shortest path tree and provide efficient routing within an OSPF routing domain.

**3. What are some features offered by the static routing?**

**Ans:** Static routing is a simple and fundamental method of routing in computer networks. It offers several features and advantages, including:

1. Simplicity: Static routing is easy to configure and manage because network administrators manually define the routes. There is no dynamic route computation or complex routing protocols involved.

2. Predictability: With static routes, the network administrator has full control over the routing table. This predictability can be advantageous in certain situations, as you know exactly how traffic will be forwarded.

3. Low Overhead: Static routing has minimal impact on network resources because it does not involve the overhead associated with dynamic routing protocols, such as OSPF or BGP.

4. Security: Static routes can be used to define specific paths for traffic, which can enhance network security by restricting the flow of traffic to known routes.

5. Isolation: You can use static routes to isolate parts of your network. For example, you can configure routes that prevent certain traffic from crossing into or out of specific network segments.

6. Load Balancing: While static routes do not provide dynamic load balancing, network administrators can implement basic load balancing by manually configuring multiple static routes with the same destination but different next-hop gateways.

7. Backup Routes: You can use static routes to set up backup paths in case a primary route fails. This can help improve network redundancy.

8. Small Networks: Static routing is well-suited for small networks with a limited number of routers and simple routing requirements.

9. No Convergence Delays: Unlike dynamic routing protocols that may take time to converge and adapt to network changes, static routes remain constant until manually changed. This can be advantageous in some situations where rapid changes are not desirable.

However, it is important to note that static routing also has limitations. It does not adapt to network changes automatically, so it is not suitable for large and complex networks where routes change frequently. In such cases, dynamic routing protocols like OSPF, BGP, or EIGRP are typically preferred. Static routes are best used when you have a specific need for fine-grained control over routing or for small, stable network environments.