

**Network Topology – 02:** This topology demonstrates communication between two different networks using a single router. Each network has its own Layer 2 switch, and the router (a Layer 3 device) enables communication between these networks by serving as their default gateway.

- Fig 2.1 shows the topology with two networks: 10.0.0.0 and 11.0.0.0.
- Each network has its own switch and hosts.
- The router connects both networks and provides gateway IP addresses for communication.

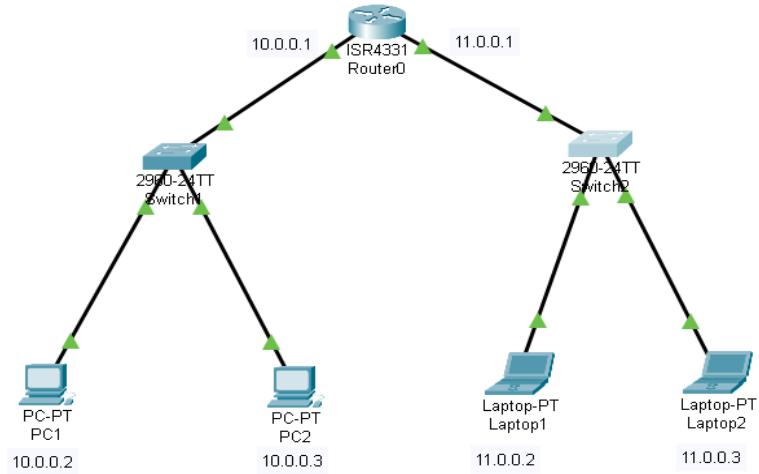


Fig: 2.1

- The default gateway for each host is the first usable IP address in the subnet.
- In the 10.0.0.0 network, the gateway is 10.0.0.1. The host details can be verified using the `ipconfig` command (Fig 2.2).
- Initially, the ARP cache remains empty since no communication has yet occurred.
- Similarly, in the 11.0.0.0 network, the default gateway is 11.0.0.1 (Fig 2.3), and again the ARP cache is empty.

The screenshot shows a Cisco Packet Tracer Command Line window. The user has run the command `C:\>ipconfig`. The output displays network configurations for two connections: FastEthernet0 and Bluetooth. For the FastEthernet0 connection, the IPv4 Address is 10.0.0.2, Subnet Mask is 255.0.0.0, and Default Gateway is 10.0.0.1. The Bluetooth connection has an IPv4 Address of 0.0.0.0, Subnet Mask of 0.0.0.0, and a Default Gateway of 0.0.0.0. A final command `C:\>arp -a` is run, which returns the message "No ARP Entries Found".

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:5CFF:FE0B:D8E3
IPv6 Address.....: :::
IPv4 Address.....: 10.0.0.2
Subnet Mask.....: 255.0.0.0
Default Gateway.....: :::
10.0.0.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0

C:\>arp -a
No ARP Entries Found
C:\>

```

Fig: 2.2 – IP Address of Host

This screenshot is identical to Fig 2.2, showing the same IP configuration for the host's FastEthernet0 connection and the absence of ARP entries.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:5CFF:FE01:6985
IPv6 Address.....: :::
IPv4 Address.....: 11.0.0.2
Subnet Mask.....: 255.0.0.0
Default Gateway.....: :::
11.0.0.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0

C:\>arp -a
No ARP Entries Found
C:\>

```

Fig: 2.3

The two Layer 2 switches initially have empty MAC address tables.

- This can be confirmed with the command `show mac address-table dynamic`.
- Fig 2.4 shows Switch1's MAC address table (empty).
- Fig 2.5 shows Switch2's MAC address table (empty).

Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#show mac address-table dynamic
Mac Address Table
-----
Vlan Mac Address Type Ports
---
```

Fig: 2.4 – Switch1 MAC Address table

Switch2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#
Switch#show mac address-table dynamic
Mac Address Table
-----
Vlan Mac Address Type Ports
---
```

Switch#  
Switch#

Fig: 2.5 – Switch2 MAC address table

- A single router is sufficient for communication between the two networks.
- The router's routing table lists the connected networks (Fig 2.6).

Router0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/8 is directly connected, GigabitEthernet0/0/0
L        10.0.0.1/32 is directly connected, GigabitEthernet0/0/0
          11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.0.0.0/8 is directly connected, GigabitEthernet0/0/1
L        11.0.0.1/32 is directly connected, GigabitEthernet0/0/1

Router#
Router#
Router#
```

Fig: 2.6 – Routing table of Router 0

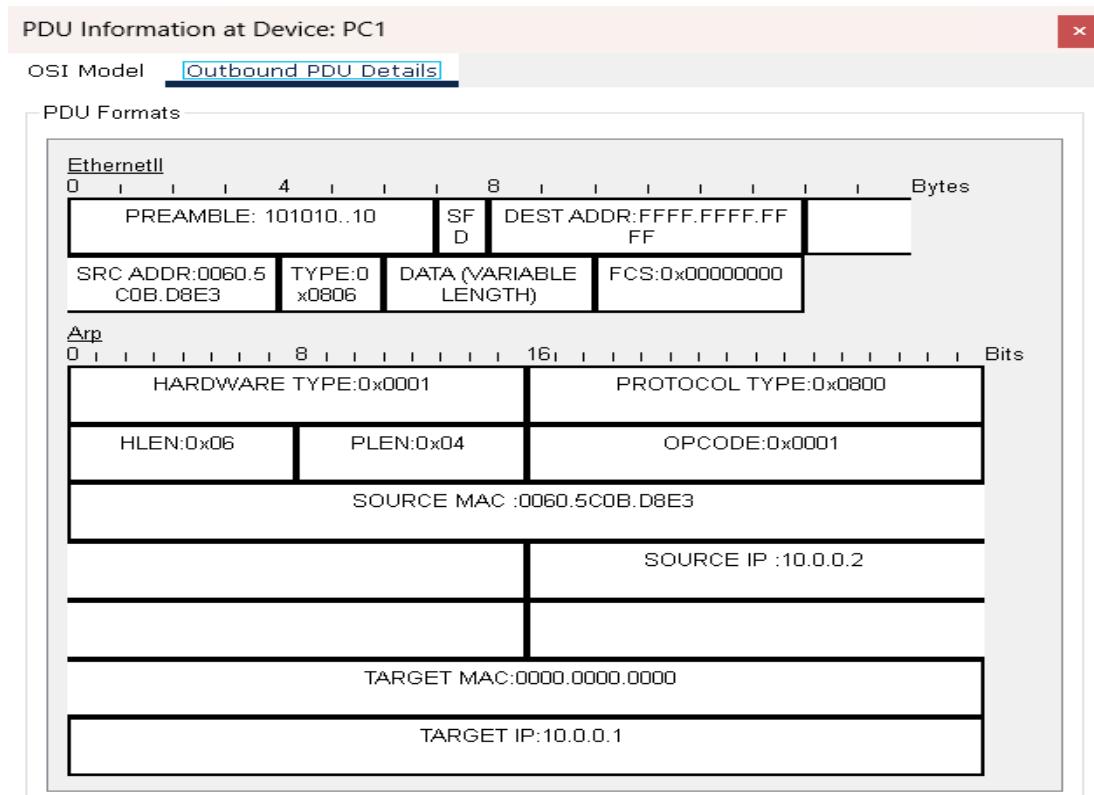


Fig: 2.7 – ARP Broadcast by Host 10.0.0.2

When Host 10.0.0.2 initiates communication, it checks its ARP cache. Since the destination MAC is unknown, it sends an ARP broadcast (Fig 2.7).

- If the switch does not yet know the MAC address, it forwards the broadcast to all devices.
- In Fig 2.8, the ARP request is received by 10.0.0.3, which is not the intended target, so the packet is dropped. However, the switch learns the MAC address.
- The router then helps the source reach the destination in the other network.

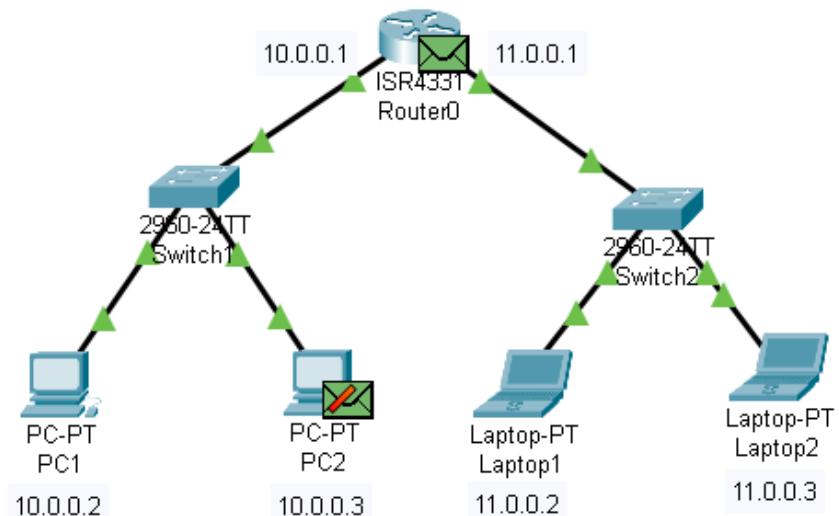


Fig: 2.8 -Packet drop by PC 2

- The ICMP packet is sent to the router (the default gateway). Since the router does not yet know the MAC address of the remote destination, it also sends an ARP request to the 11.0.0.0 network (Fig 2.9 and Fig 2.10).

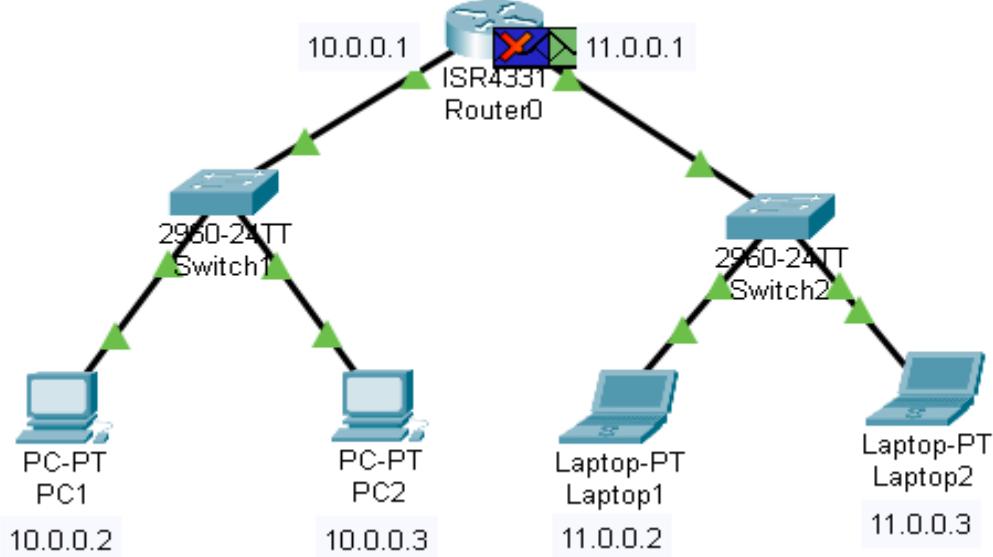


Fig: 2.9 – ICMP packet drop

- Fig 2.12 shows the ARP reply from the correct host (11.0.0.3). Now the router has the MAC address mapping.
- In Fig 2.9 we can see the ICMP packet drop because it reached the default gateway but the router doesn't have the destination mac address so again the ARP broadcast to the 11.0.0.0 network will be done

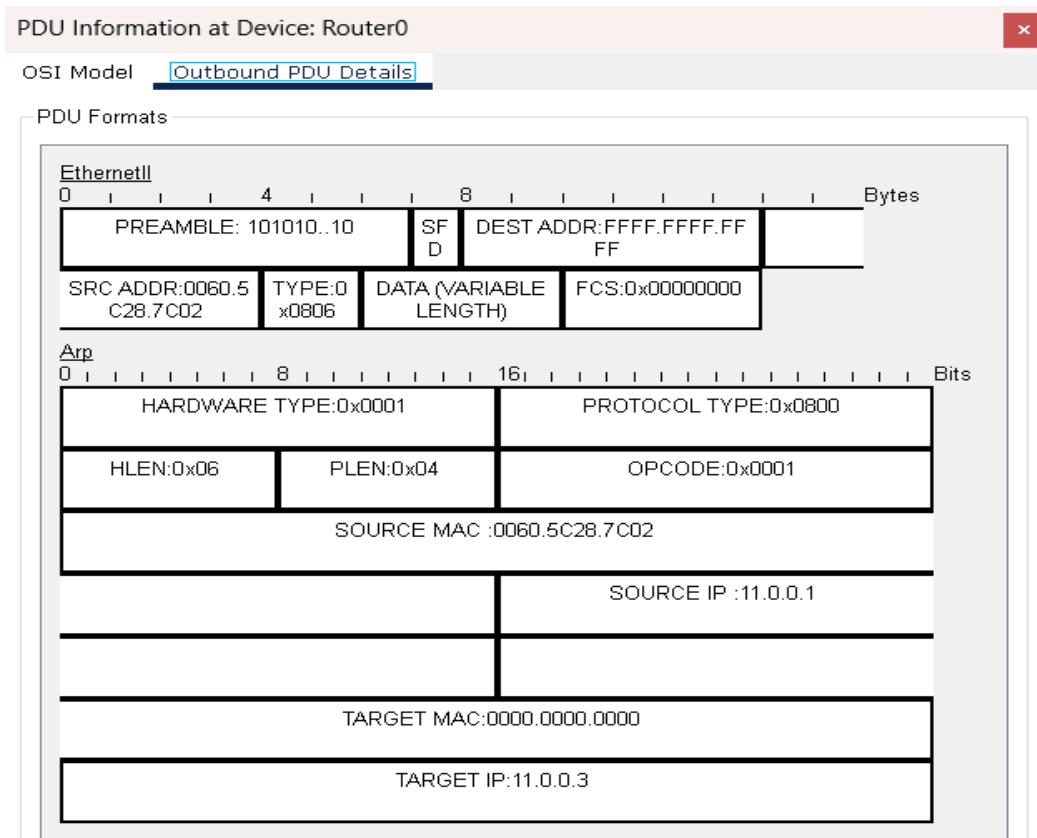


Fig: 2.10-ARP request to 11.0.0.0

- Here in Fig: 2.10 we can see the source is that router's default gateway of 11.0.0.0 network and the destination is same that is 11.0.0.3 because the 10.0.0.2 is looking for 11.0.0.3
  - In Fig 2.11, the ARP request is seen at another host which drops it because it is not the target.

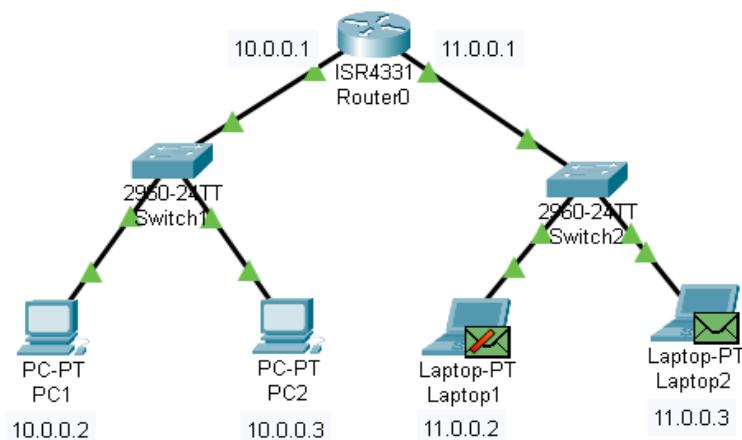


Fig: 2.11 – Packet drop at 11.0.0.2

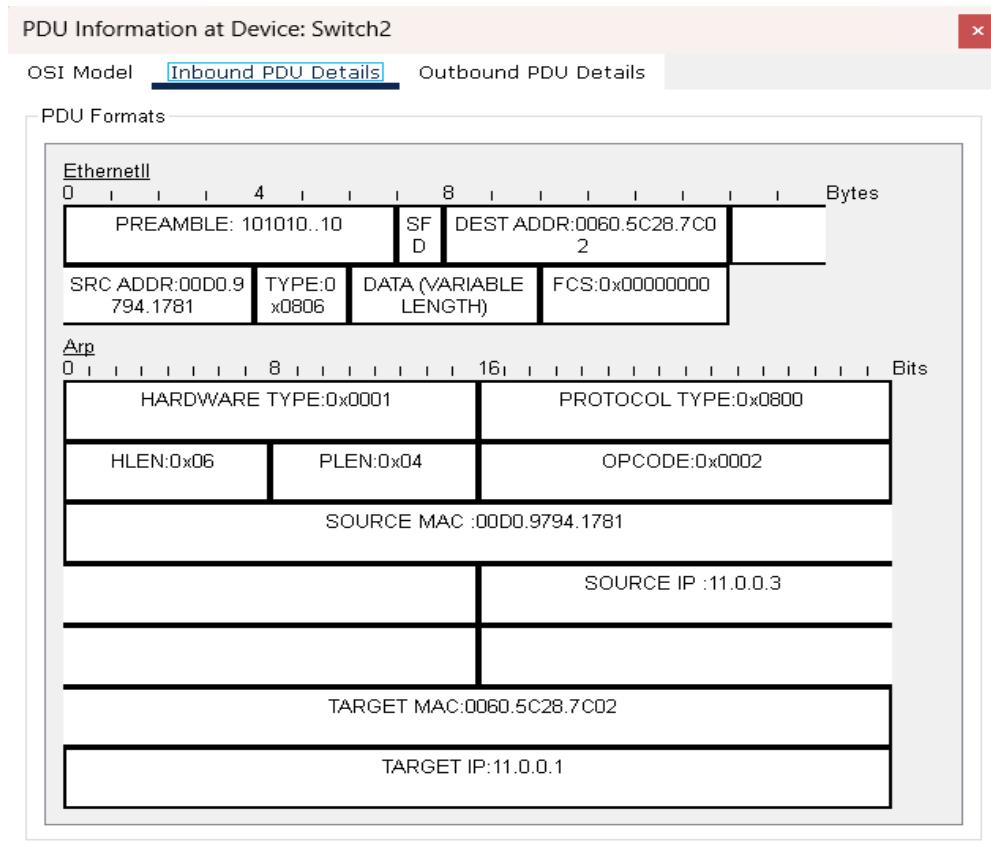


Fig: 2.12 – The ARP response from 11.0.0.3

- Fig 2.12 shows the ARP reply from the correct host (11.0.0.3). Now the router has the MAC address mapping.
- With the MAC address resolved, the ICMP request is sent successfully to the destination host (Fig 2.13).
- The source and destination IP addresses remain unchanged end-to-end, but the MAC addresses change hop by hop.
- The reply from the destination is an ICMP Echo Reply (Fig 2.14).
- Finally, Fig 2.15 confirms that the ICMP request succeeded.

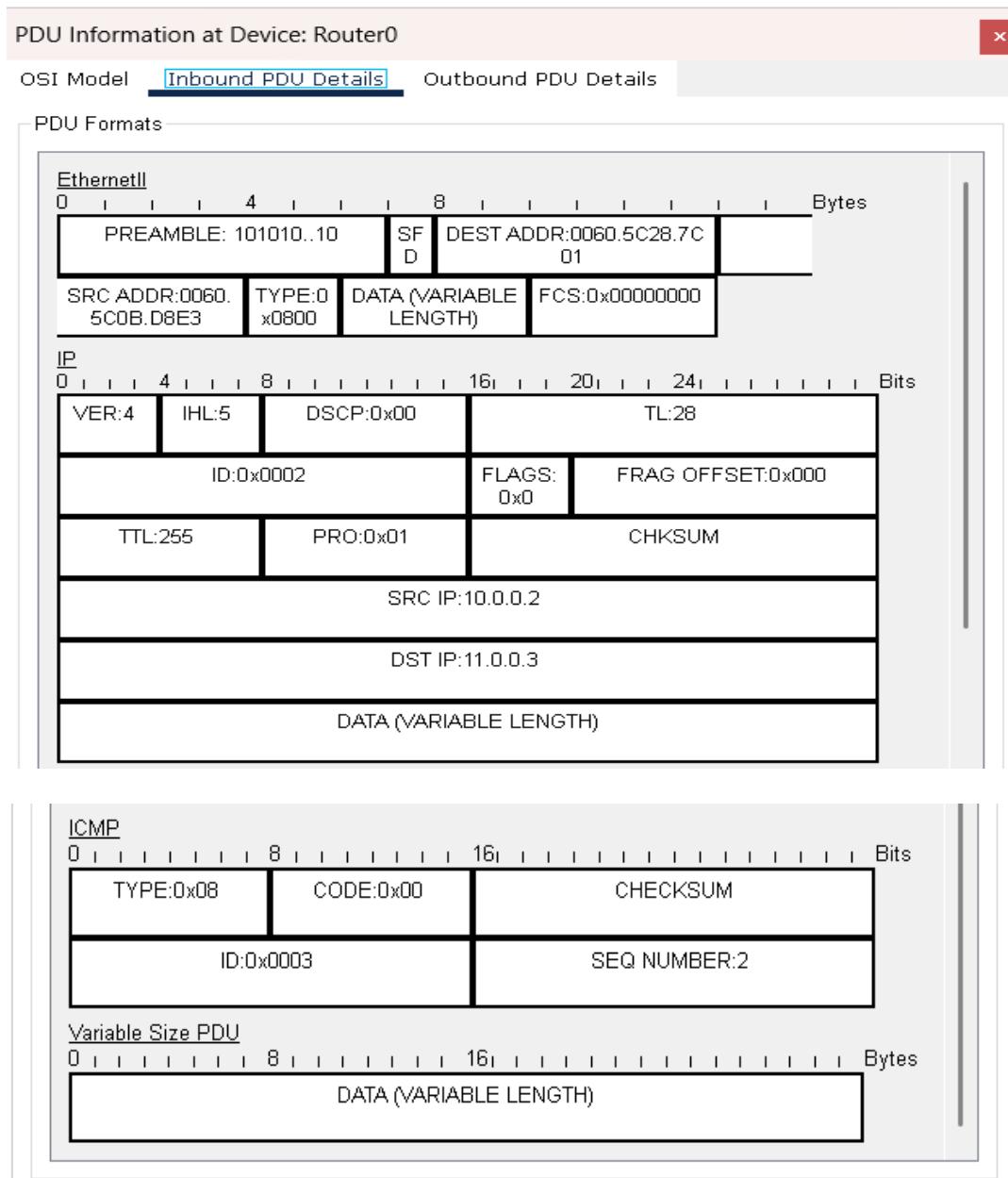


Fig: 2.13 – ICMP request details

- These are the details of ICMP request and In Fig. 2.14 we can see the details of the ICMP response or echo response

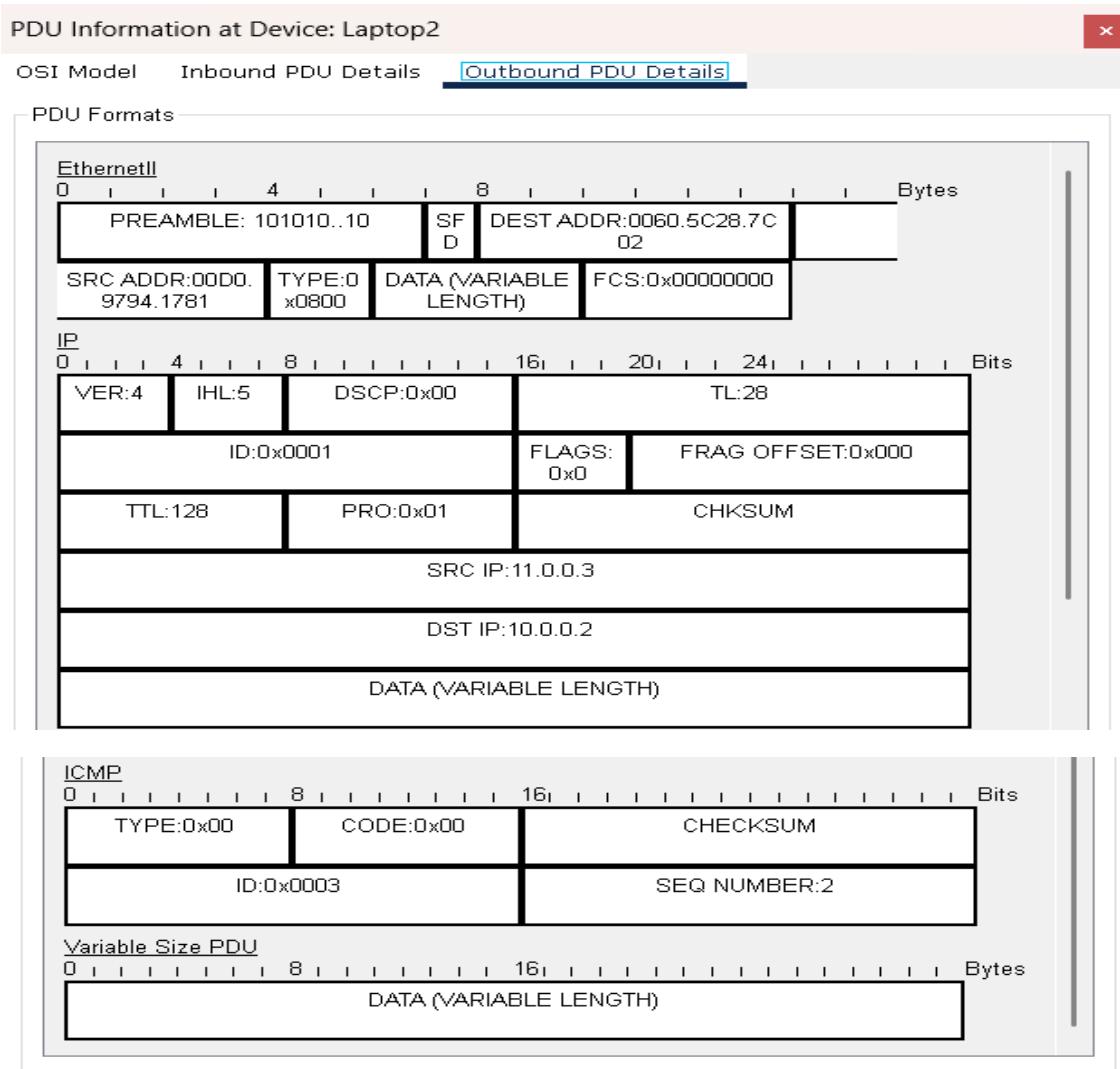


Fig: 2.14 – ICMP response

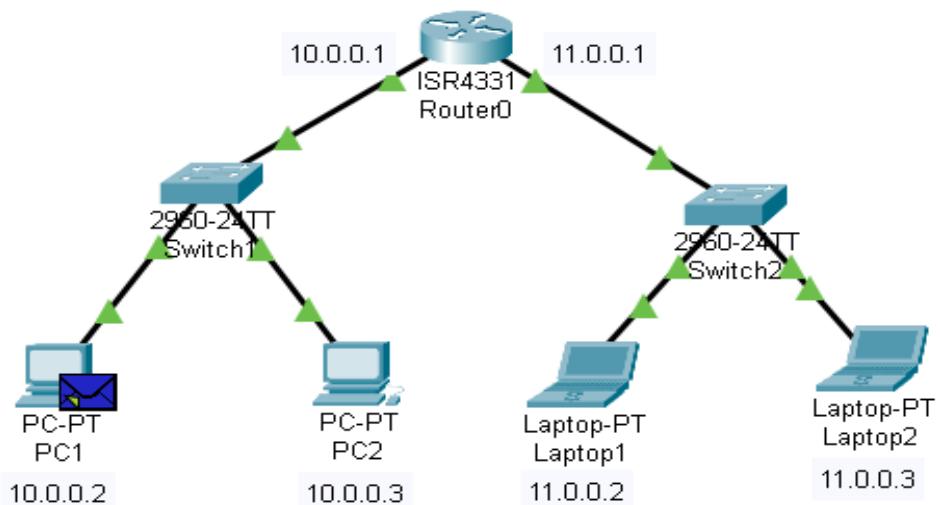


Fig: 2.15 The ICMP request is Succeeded

- This process illustrates how two networks communicate for the first time
- Initially, ARP caches and MAC address tables are empty.
- ARP broadcasts and replies populate the required tables.
- Once MAC addresses are known, ICMP communication succeeds.
- Subsequent communication occurs directly without repeated broadcasts.