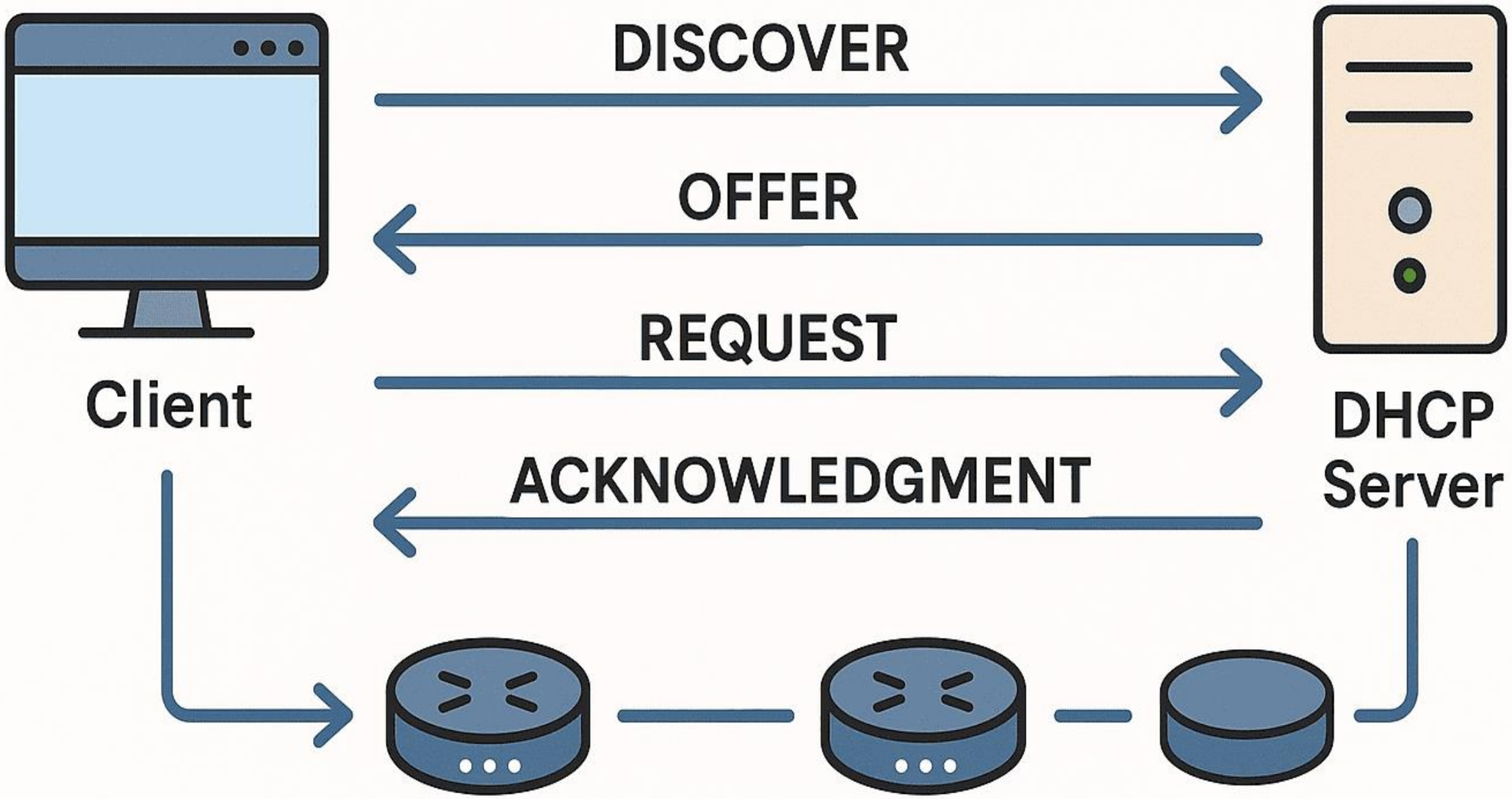
DHCP PACKET FLOW

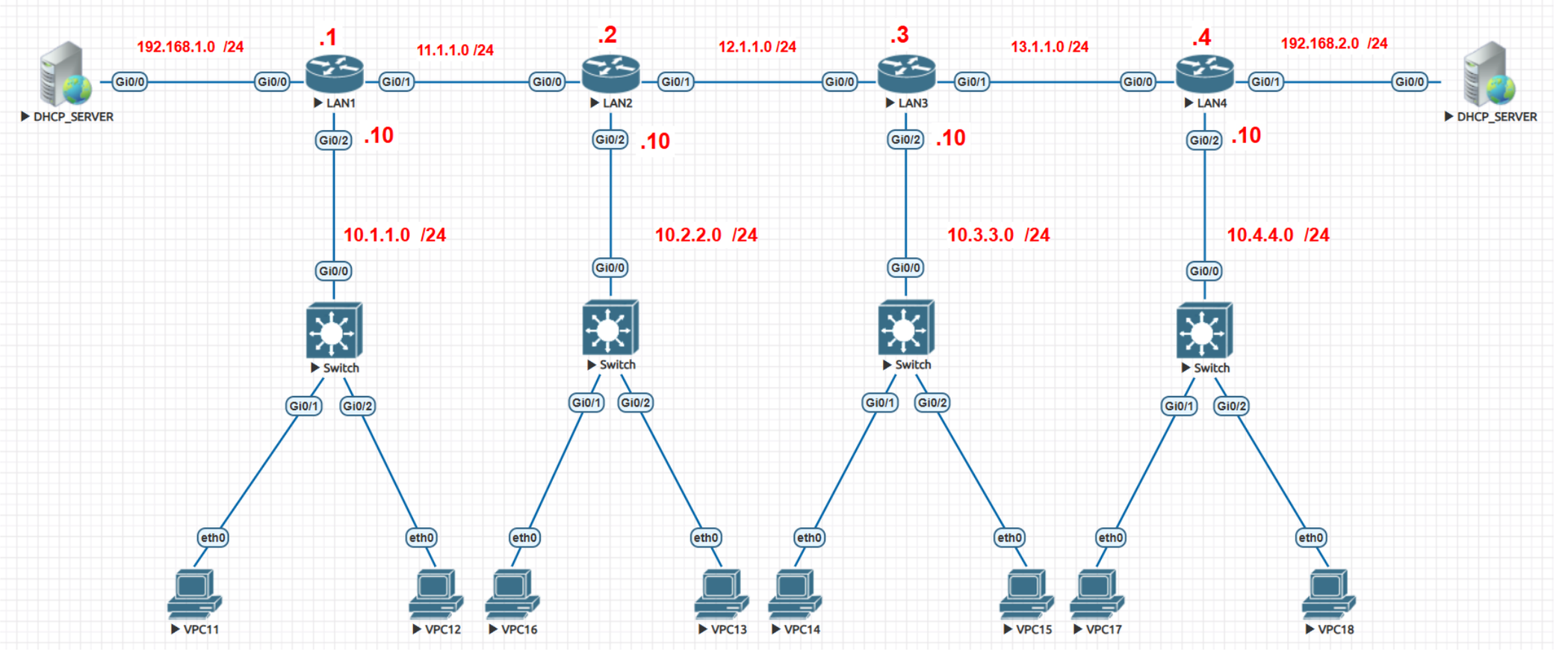


Dhcp and Relay Agent

- **DHCP** is a service that automatically gives IP addresses to devices on a network so they can connect and communicate.

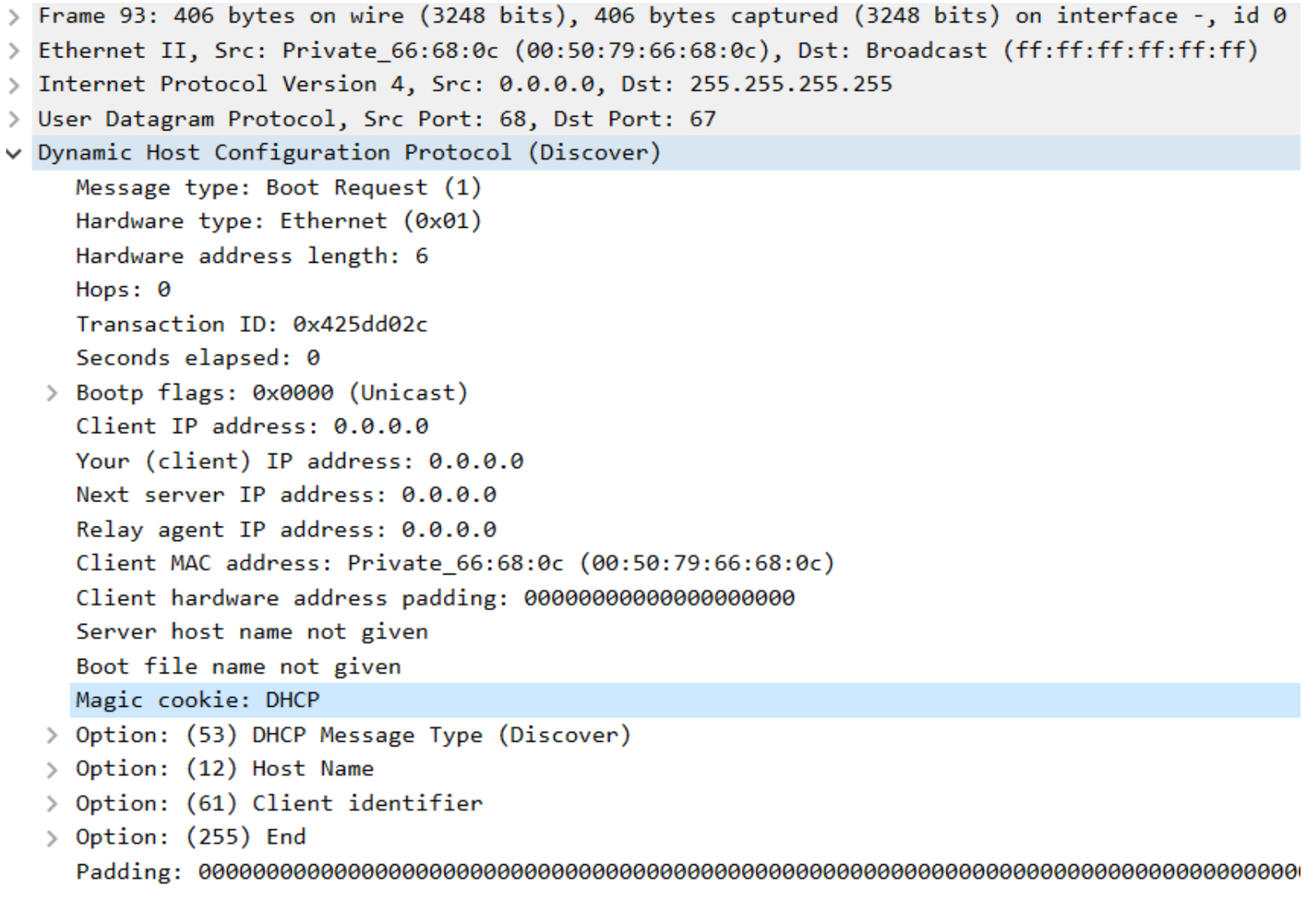
- **A DHCP relay agent** forwards DHCP messages between clients and a DHCP server when they are not on the same subnet.

TOPOLOGY

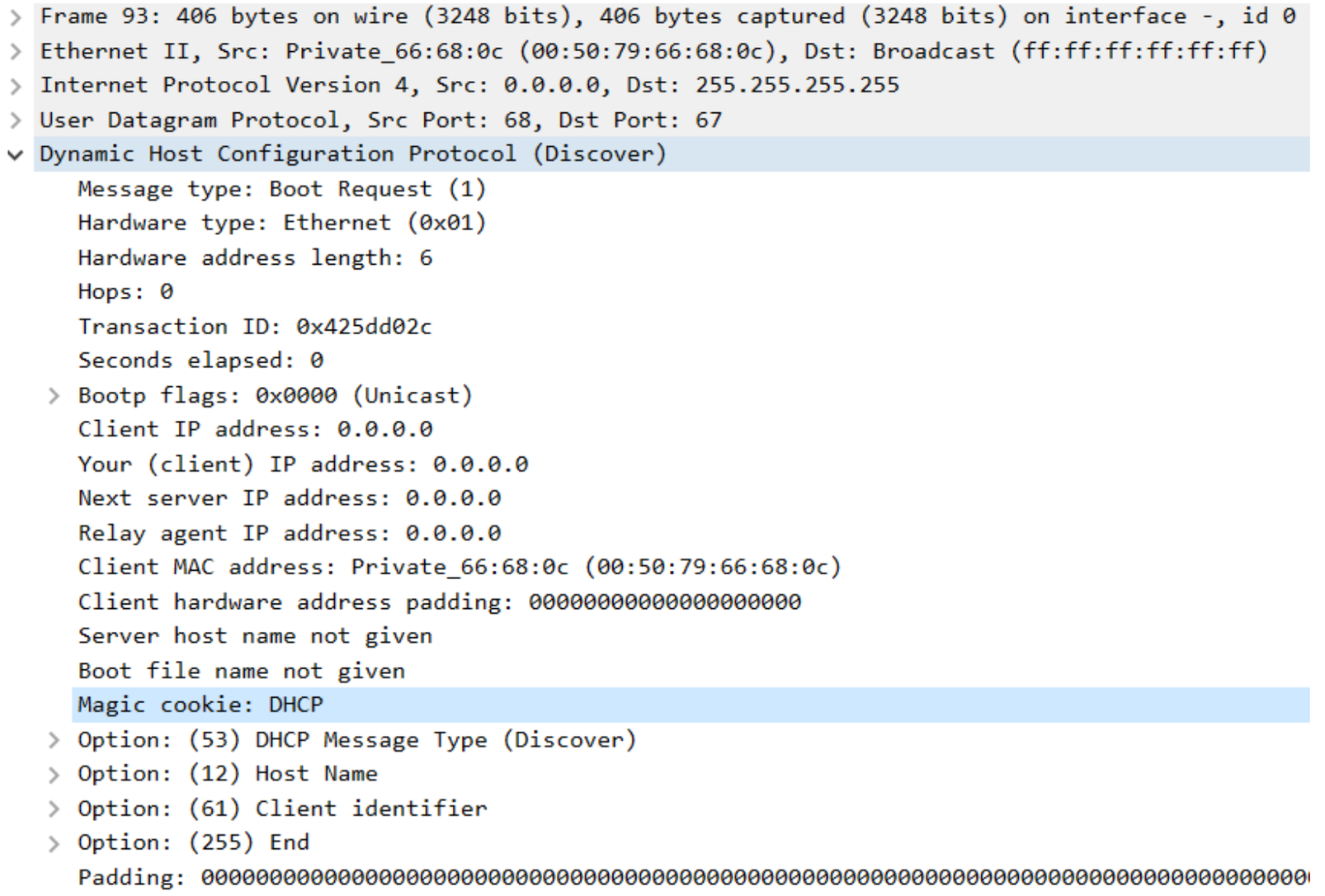

192.168.1.0 /24
.1
11.1.1.0 /24
.2
12.1.1.0 /24
.3
13.1.1.0 /24
.4
192.168.2.0 /24
DHCP_SERVER
LAN1
LAN2
LAN3
LAN4
DHCP_SERVER
Gi0/0
Gi0/1
Gi0/2
.10
10.1.1.0 /24
10.2.2.0 /24
10.3.3.0 /24
10.4.4.0 /24
Switch
eth0
VPC11
VPC12
VPC16
VPC13
VPC14
VPC15
VPC17
VPC18

What traffic is generated at the PC during the DHCP Discover phase?

During the DHCP Discover phase, the PC sends a broadcast message to find a DHCP server.



A switch forwards the same PDU to all devices within the same broadcast domain, except the port from which it was received.



What type of traffic does the DHCP relay agent generate after receiving a DHCP Discover (broadcast) message?

After receiving a DHCP Discover broadcast message from a PC, the DHCP relay agent sends a unicast message to the DHCP server.

```
> Frame 16: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:00 (50:00:00:02:00:00), Dst: 50:00:00:01:00:00 (50:00:00:01:00:00)
> Internet Protocol Version 4, Src: 10.1.1.10, Dst: 192.168.1.100
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0xa5691010
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (12) Host Name
  > Option: (61) Client identifier
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

Mac-address:
LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

What type of traffic does the DHCP Server generate after receiving a DHCP Discover (Unicast) message from DHCP Relay Agent?

After getting a DHCP Discover (unicast) message from the relay agent, the DHCP server sends a DHCP Offer as a unicast back to the relay agent.

```
177 261.236546    10.1.1.10           192.168.1.100       DHCP     406 DHCP Discover - Transaction ID 0x89433f50
178 261.245929    192.168.1.100       10.1.1.4            ICMP      70 Echo (ping) request  id=0x0003, seq=0/0, ttl=255 (no response found!)
179 262.238714    10.1.1.10           192.168.1.100       DHCP     406 DHCP Discover - Transaction ID 0x89433f50
180 262.340106    50:00:00:02:00:00   50:00:00:02:00:00   LOOP      60 Reply
181 262.555209    50:00:00:01:00:00   CDP/VTP/DTP/PAgP/UD… CDP     366 Device ID: DHCP_SERVER1  Port ID: GigabitEthernet0/0
182 262.755200    192.168.1.100       10.1.1.4            ICMP      70 Echo (ping) request  id=0x0003, seq=0/0, ttl=255 (no response found!)
```

```
> Frame 183: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:01:00:00 (50:00:00:01:00:00), Dst: 50:00:00:02:00:00 (50:00:00:02:00:00)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.1.1.10
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.1.1.4
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 000000
```

Mac-address:
LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

❓ Why does a DHCP server send a ping before offering an IP address?

i. A DHCP server sends a ping request before offering an IP address to check whether the IP is already in use on the network. This process is part of what's called ***Duplicate Address Detection (DAD).*** The relay agent generate a **proxy arp** to the local network.

ii. ***A dhcp server*** doesn't know about**:**

- ❑ Manually configured static IPs on clients.
- ❑ IPs assigned by a different DHCP server.
- ❑ The record is still correct, especially if the server is restarted or crashed.

Q. Why is the relay agent generated traffic the source port 67?

What type of traffic does the DHCP relay agent generate after receiving a DHCP Offer (Unicast) message from DHCP Server?

After receiving a DHCP Offer (Unicast) message from a Server, the DHCP relay agent sends a broadcast message to the local network.

```
> Ethernet II, Src: 50:00:00:02:00:02 (50:00:00:02:00:02), Dst: Private_66:68:0c (00:50:79:66:68:0c)
> Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.1.1.4
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.1.1.4
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 000000
```

❌ **ARP** can't be used to resolve IP to MAC at this stage because client doesn't have ip.

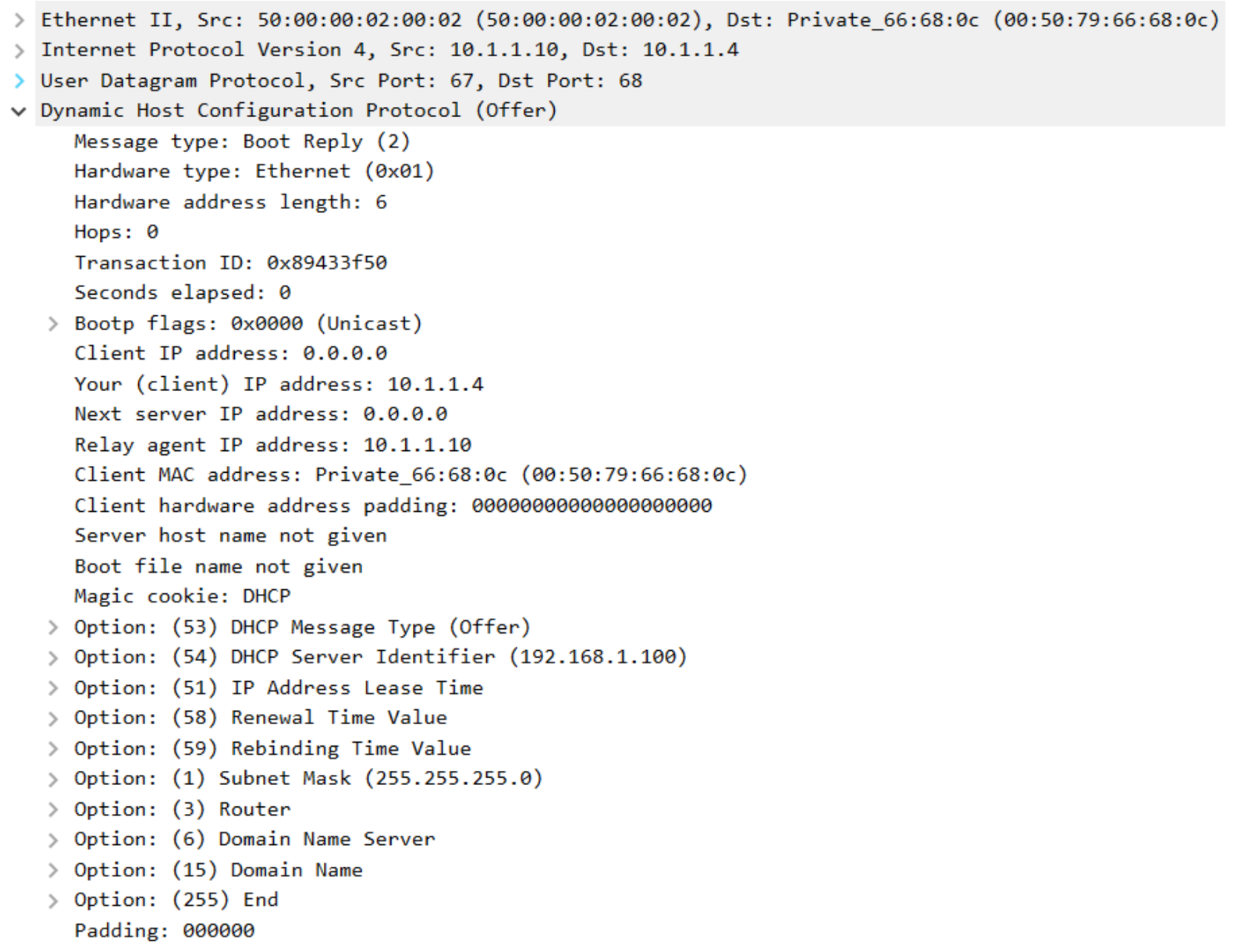
Mac-address:

LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

A switch forwards the same PDU to all devices within the same broadcast domain, except the port from which it was received.



What type of traffic does the PC generate after receiving a DHCP Offer (broadcast) message from Realy agent?

After receiving a DHCP Discover broadcast message of the Relay agent, the pc sends a Request (broadcast) message to the DHCP server.

```
> Ethernet II, Src: Private_66:68:0c (00:50:79:66:68:0c), Dst: 50:00:00:02:00:02 (50:00:00:02:00:02)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.1.1.4
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (50) Requested IP Address (10.1.1.4)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

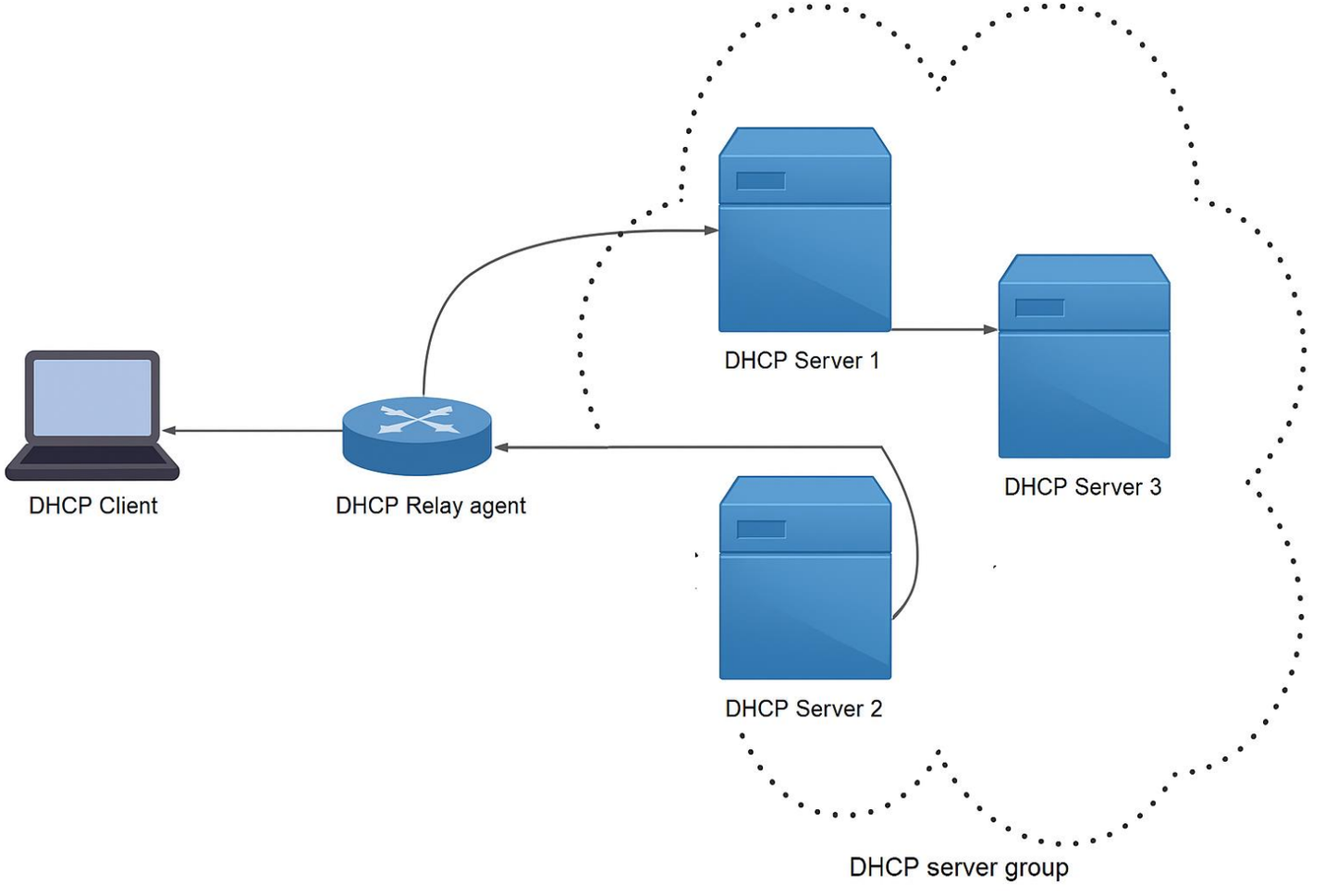
Mac-address:
LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

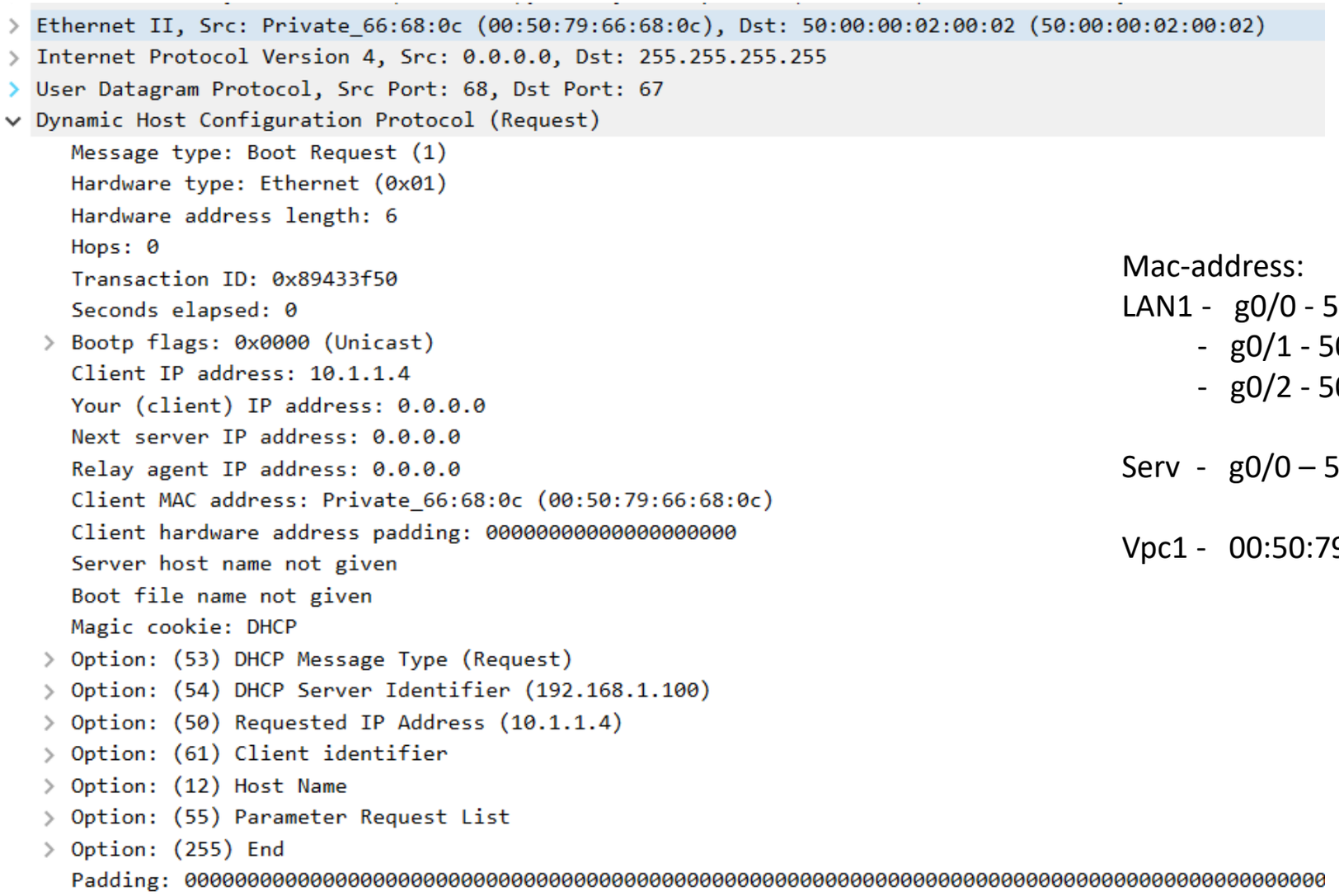
Vpc1 - 00:50:79:66:68:0c

Why the request message is broadcast?

Sent as a **broadcast** so that **all DHCP servers** know which dhcp offer was accepted.



A switch forwards the same PDU to all devices within the same broadcast domain, except the port from which it was received.



Mac-address:

LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

What type of traffic does the DHCP relay agent generate after receiving a DHCP Offer (broadcast) of the PC?

After receiving a DHCP Offer broadcast message of a PC, the DHCP relay agent sends a unicast message to the DHCP server.

```
> Frame 199: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface -, id 0
> Ethernet II, Src: 50:00:00:02:00:00 (50:00:00:02:00:00), Dst: 50:00:00:01:00:00 (50:00:00:01:00:00)
> Internet Protocol Version 4, Src: 10.1.1.10, Dst: 192.168.1.100
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.1.1.4
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (50) Requested IP Address (10.1.1.4)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000(
```

Mac-address:

LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

What type of traffic does the DHCP Server generate after receiving a DHCP Request (Unicast) message from DHCP Relay Agent?

After getting a DHCP Request(unicast) message from the relay agent, the DHCP server sends a DHCP *Ack* as a unicast back to the relay agent.

```
> Ethernet II, Src: 50:00:00:01:00:00 (50:00:00:01:00:00), Dst: 50:00:00:02:00:00 (50:00:00:02:00:00)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.1.1.10
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.1.1.4
    Your (client) IP address: 10.1.1.4
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 000000
```

Mac-address:
LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

What type of traffic does the DHCP relay agent generate after receiving a DHCP Ack (Unicast) message from DHCP Server?

After receiving a DHCP Offer (Unicast) message from a Server, the DHCP relay agent sends a broadcast message to the local network.

```
> Ethernet II, Src: 50:00:00:02:00:02 (50:00:00:02:00:02), Dst: Private_66:68:0c (00:50:79:66:68:0c)
> Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.1.1.4
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.1.1.4
    Your (client) IP address: 10.1.1.4
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 000000
```

Mac-address:

LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

A switch forwards the same PDU to all devices within the same broadcast domain, except the port from which it was received.

```
> Ethernet II, Src: 50:00:00:02:00:02 (50:00:00:02:00:02), Dst: Private_66:68:0c (00:50:79:66:68:0c)
> Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.1.1.4
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x89433f50
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.1.1.4
    Your (client) IP address: 10.1.1.4
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.1.10
    Client MAC address: Private_66:68:0c (00:50:79:66:68:0c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.1.100)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 000000
```

Mac-address:

LAN1 - g0/0 - 5000.0002.0000
- g0/1 - 5000.0002.0001
- g0/2 - 5000.0002.0002

Serv - g0/0 – 5000.0001.0000

Vpc1 - 00:50:79:66:68:0c

What type of traffic does the PC generate after receiving a DHCP Ack (broadcast) message from Realy agent?

After receiving a DHCP ACK message from the relay agent, the PC sends a GARP (Gratuitous ARP) Broadcast to check if the offered IP is already in use before accepting it.

28	25.937218	Private_66:68:0c	Broadcast	ARP	64 Gratuitous ARP for 10.1.1.4 (Request)
29	26.507358	50:00:00:07:00:02	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/50:00:00:07:00:00
30	26.590496	10.1.1.10	224.0.0.10	EIGRP	74 Hello
31	26.938423	Private_66:68:0c	Broadcast	ARP	64 Gratuitous ARP for 10.1.1.4 (Request)
32	27.938990	Private_66:68:0c	Broadcast	ARP	64 Gratuitous ARP for 10.1.1.4 (Request)

❓Why does the switch still treat the DHCP Offer as a broadcast, even though it knows the client's MAC address?

Because the DHCP Offer sent by the relay agent is a broadcast at Layer 2 (Ethernet) — not a unicast — and the switch just forwards it as-is.

Note: When more than one router is present between relay agent and dhcp server, it replaces the mac-addresses while traveling from relay to server or vice-versa.

DHCP SNOOPING

DHCP snooping is a security feature that protects your network from fake DHCP servers.

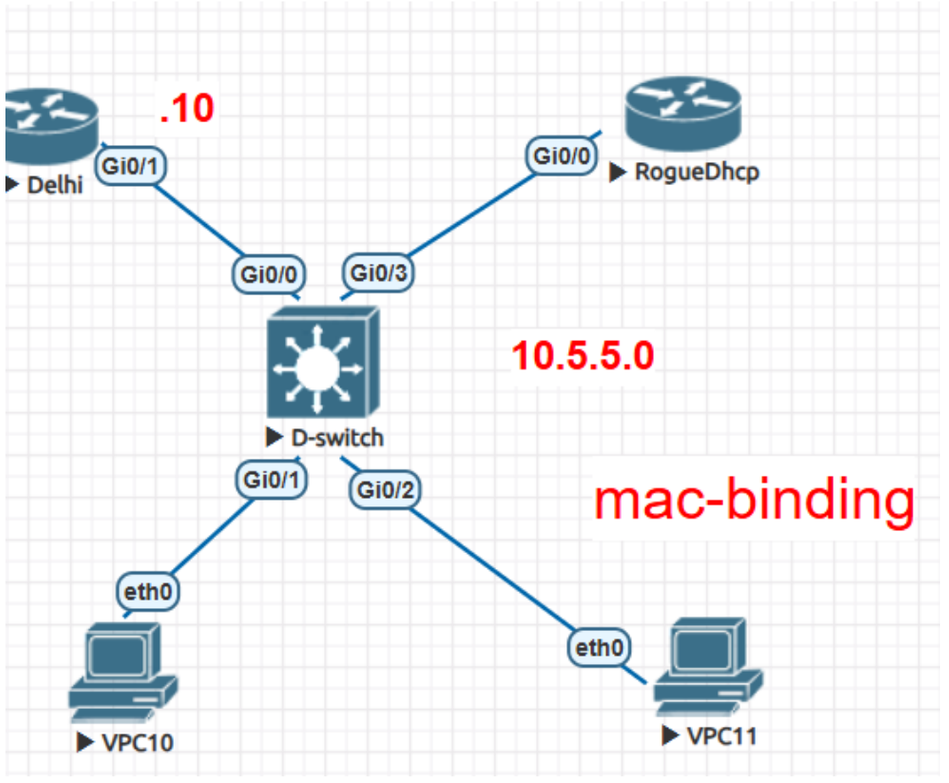
- ❑ It helps make sure that **only the real DHCP server** can give out IP addresses.
- ❑ The switch checks which ports are safe (trusted) and which ones are not (untrusted).

There are two types of ports:

- ❑ **Trusted ports**: These are usually connected to the real DHCP server (like an uplink to a router).
- ❑ **Untrusted ports**: These are ports where users plug in their devices (like computers). By default, all ports are untrusted.

Note: If a fake DHCP server is connected to an untrusted port, the switch will **block its messages**.

DHCP SNOOPING Packet Flow



Need to resolve: option 82

Switch(config)# no ip dhcp snooping information option

Switch(config)# interface g0/0
Switch(config-if)# ip dhcp snooping limit rate 20
Switch(config-if)# ip dhcp snooping trust