

Rohit Garg
2018A7PS0193G

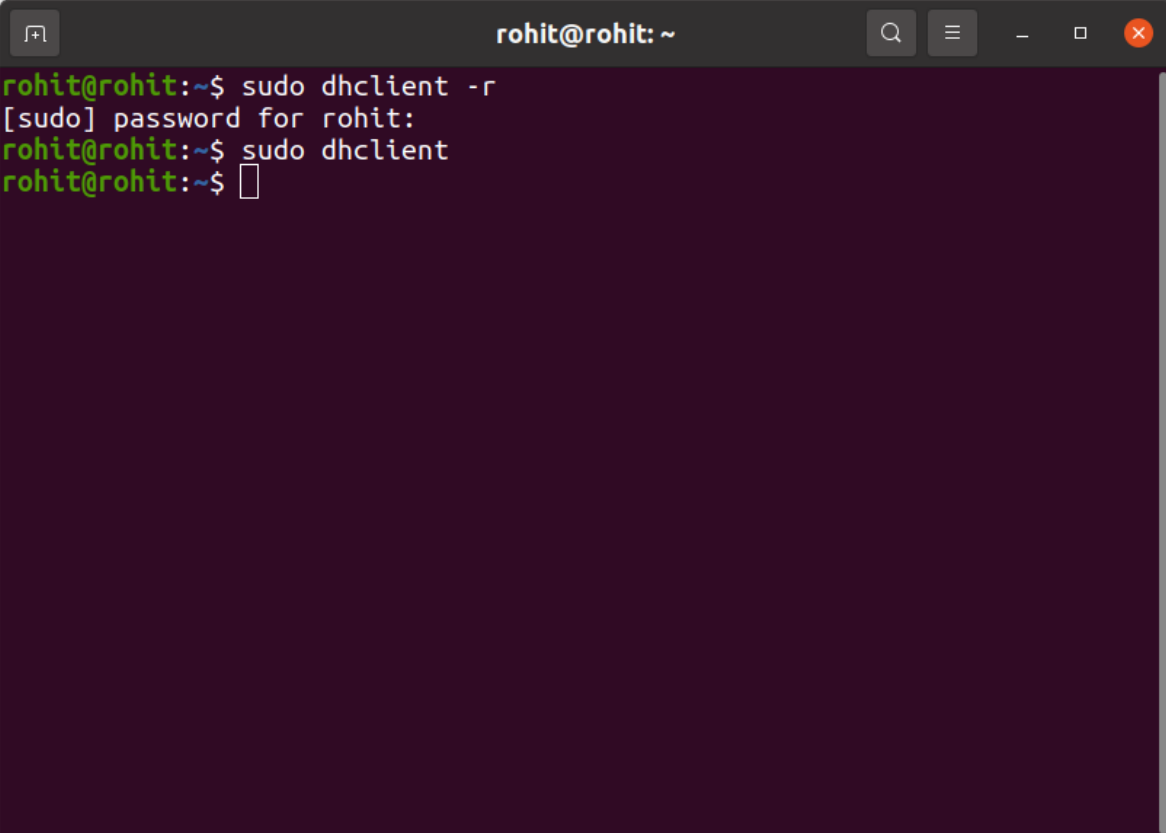
COMPUTER NETWORKS

CS F303

1. Show a round of execution of the DHCP protocol. Show DHCP Request (2 marks), Reply (2 marks), and ACK messages (2 marks) in that round. Find out IP addresses of the DHCP server (2 marks) and client (2 marks). Write the filter and show the output in a screenshot.

1.

In order to demonstrate the working of DHCP protocol, we instruct the host to obtain a network configuration, including a new IP address using `dhclient` command. Hence, to get issued a new address, we release the old IP address by typing '`sudo dhclient -r`' at the terminal. Now open Wireshark to start packet capture at LAN(wlo1 in my case). Now reissue IP address by typing '`sudo dhclient`' on terminal to get a new IP address. The IP address gets released and reissued after these commands.

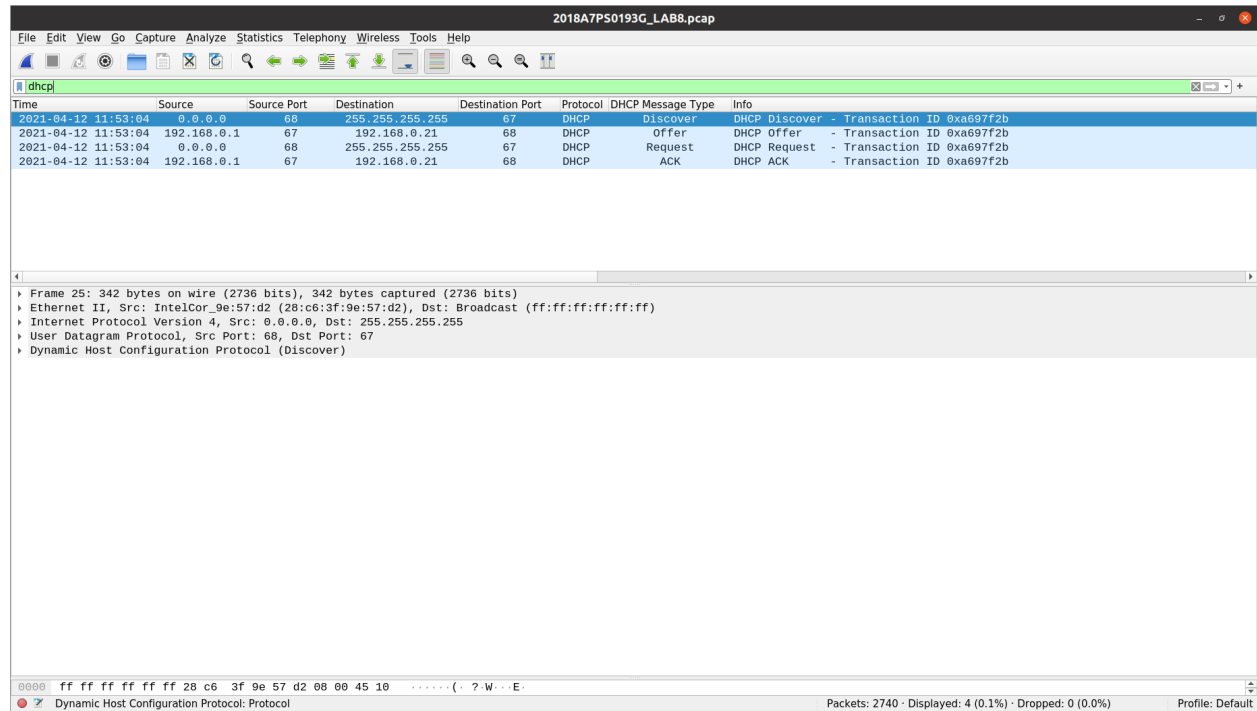
A screenshot of a terminal window titled 'rohit@rohit: ~'. The terminal shows the following commands and output:

```
rohit@rohit:~$ sudo dhclient -r
[sudo] password for rohit:
rohit@rohit:~$ sudo dhclient
rohit@rohit:~$
```

The terminal has a dark purple background and a light green prompt. The window has standard Linux window controls (minimize, maximize, close) and a search icon in the title bar.

DHCP uses UDP transport layer protocol and uses port numbers 67 and 68.

DHCP packets can be filtered out using **dhcp** filter.



The screenshot shows a Wireshark capture of a DHCP transaction. The filter bar at the top is set to 'dhcp'. The packet list shows four packets: a Discover (68 to 67), an Offer (67 to 68), a Request (68 to 67), and an ACK (67 to 68). The packet details pane for the first packet (Discover) is expanded, showing the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Discover) layers. The status bar at the bottom indicates 2740 packets, 4 displayed (0.1%), and 0 dropped (0.0%).

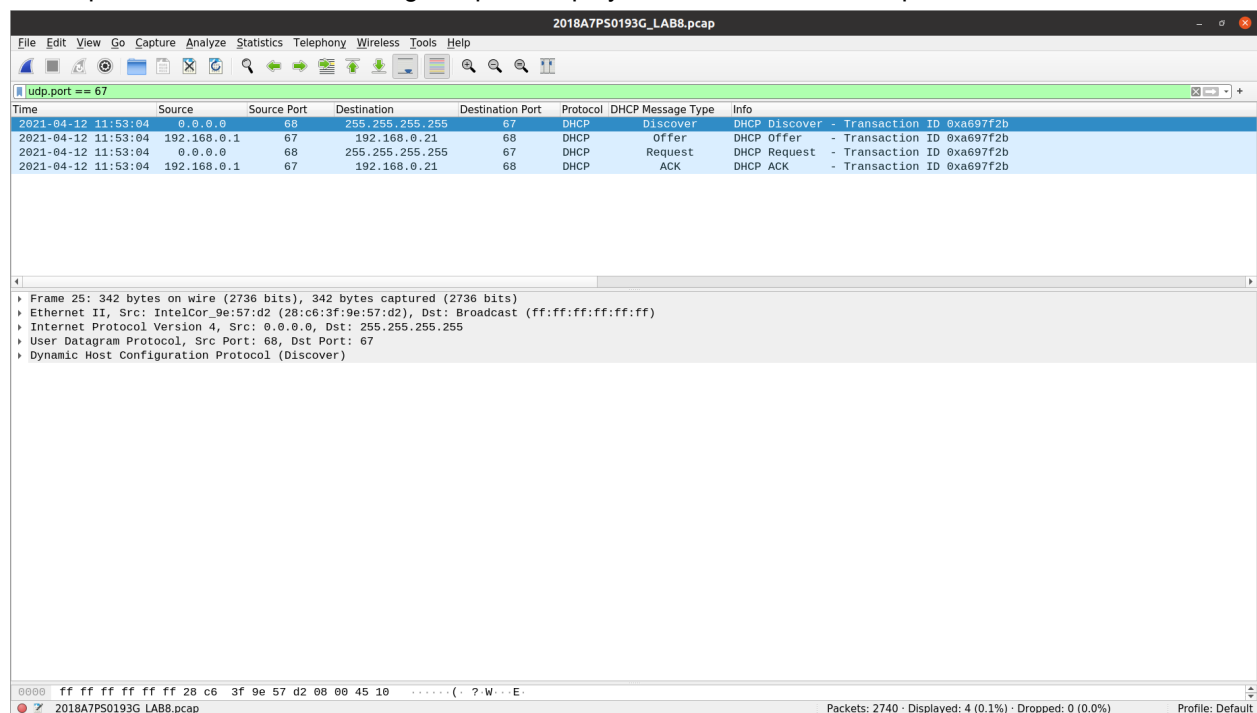
Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Discover	DHCP Discover - Transaction ID 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	Offer	DHCP Offer - Transaction ID 0xa697f2b
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Request	DHCP Request - Transaction ID 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	ACK	DHCP ACK - Transaction ID 0xa697f2b

Frame 25: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff 28 c6 3f 9e 57 d2 08 00 45 10(. ? W...E-
Dynamic Host Configuration Protocol: Protocol

Packets: 2740 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Note :Since DHCP server is listening on port 67, we can also use 'udp.port == 67' as a filter to filter out DHCP packets but we will be using 'dhcp' as display filter to filter out DHCP packets.



The screenshot shows the same Wireshark capture with the filter bar set to 'udp.port == 67'. The packet list now only shows the first packet (Discover) and the third packet (Request), as the Offer and ACK packets were filtered out. The packet details pane for the first packet is expanded, showing the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Discover) layers. The status bar at the bottom indicates 2740 packets, 4 displayed (0.1%), and 0 dropped (0.0%).

Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Discover	DHCP Discover - Transaction ID 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	Offer	DHCP Offer - Transaction ID 0xa697f2b
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Request	DHCP Request - Transaction ID 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	ACK	DHCP ACK - Transaction ID 0xa697f2b

Frame 25: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff 28 c6 3f 9e 57 d2 08 00 45 10(. ? W...E-
2018A7PS0193G_LAB8.pcap

Packets: 2740 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Discover messages can be filtered out using 'dhcp.option.dhcp == dhcp_message_type' display filter where message type can be 'discover', 'offer', 'request', 'ack'. For Example:-

The image shows a Wireshark packet capture window for the file '2018A7PS0193G_LAB8.pcap'. The display filter is set to 'dhcp.option.dhcp == discover'. The packet list shows a single packet at time 2021-04-12 11:53:04.0.0.0, source port 68, destination 255.255.255.255, protocol DHCP, message type Discover, with transaction ID 0xa697f2b.

The packet details pane shows the following structure:

- Frame 25: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
- Ethernet II, Src: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)
 - Message type: Boot Request (1)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xa697f2b
 - 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: 0.0.0.0
 - Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
 - Client hardware address padding: 00000000000000000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (Discover)
 - Option: (50) Requested IP Address (192.168.0.21)
 - Option: (12) Host Name
 - Option: (55) Parameter Request List
 - Option: (255) End
 - Padding: 00

The packet bytes pane shows the raw data: ff ff ff ff ff ff 28 c6 3f 9e 57 d2 00 00 45 10. The status bar indicates 2740 packets, 1 displayed (0.0%), 0 dropped (0.0%), and the profile is Default.

DHCP discover is the first request message packet sent by a client to the DHCP server. Client broadcasts a DISCOVER message in order to locate the DHCP server to request for a new IP address.

Ethernet II - Broadcast MAC address = ff:ff:ff:ff -> Since client doesn't have the IP address or the information about the server, hence, it has to broadcast to discover a DHCP server.

Source IP Address = 0.0.0.0 -> Client after `sudo dhclient -r` command releases its IP address and its IP address is set to 0.0.0.0.

Destination IP Address = 255.255.255.255 -> Broadcast IP Address

DHCP Message Type = Discover (1) since it is a discover message

DHCP Offer

DHCP Offer message is the reply message packet sent by the server to the client.

The image displays two screenshots of a Wireshark packet capture. The top screenshot shows a DHCP Discover message (Transaction ID: 0xa697f2b) from a client (0.0.0.0) to a server (192.168.0.1). The bottom screenshot shows the corresponding DHCP Offer message (Transaction ID: 0xa697f2b) from the server to the client, offering the IP address 192.168.0.21.

Packet 1: DHCP Discover

Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:04	0.0.0.0	65	255.255.255.255	67	DHCP	Discover	DHCP Discover - Transaction ID: 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	Offer	DHCP Offer - Transaction ID: 0xa697f2b
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Request	DHCP Request - Transaction ID: 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	ACK	DHCP ACK - Transaction ID: 0xa697f2b

Dynamic Host Configuration Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xa697f2b
- 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: 0.0.0.0
- Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Client hardware address padding: 00000000000000000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Discover)
- Option: (50) Requested IP Address (192.168.0.21)
- Option: (12) Host Name
- Option: (55) Parameter Request List
- Option: (255) End
- Padding: 00

Packet 2: DHCP Offer

Dynamic Host Configuration Protocol (Offer)

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xa697f2b
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 192.168.0.21
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Client hardware address padding: 00000000000000000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
- Length: 1
- DHCP: Offer (2)
- Option: (54) DHCP Server Identifier (192.168.0.1)
- Length: 4
- DHCP Server Identifier: 192.168.0.1
- Option: (51) IP Address Lease Time
- Length: 4
- IP Address Lease Time: (86400s) 1 day
- 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: (255) End

DHCP offer packet contains various details like :

Client IP address: Current IP address of the client

Your IP Address: The 'offered' IP address i.e. to be allocated to the client by DHCP server

DHCP Request

The image shows a Wireshark capture of a DHCP Request packet. The packet list at the top shows four packets: a Discover (1), an Offer (2), a Request (3), and an ACK (4). The selected packet is the Request (3), which is a Dynamic Host Configuration Protocol (Request) from source 192.168.0.1 to destination 192.168.0.21. The packet details pane shows the following structure:

- Dynamic Host Configuration Protocol (Request)
 - Message type: Boot Request (1)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xa697f2b
 - 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: 0.0.0.0
 - Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (Request)
 - Length: 1
 - DHCP: Request (3)
 - Option: (54) DHCP Server Identifier (192.168.0.1)
 - Length: 4
 - DHCP Server Identifier: 192.168.0.1
 - Option: (50) Requested IP Address (192.168.0.21)
 - Length: 4
 - Requested IP Address: 192.168.0.21
 - Option: (12) Host Name
 - Length: 5
 - Host Name: rohit
 - Option: (55) Parameter Request List
 - Length: 13
 - Parameter Request List Item: (1) Subnet Mask
 - Parameter Request List Item: (3) Broadcast Address

The packet bytes pane shows the raw data: 0000 ff ff ff ff ff ff 28 c6 3f 9e 57 d2 00 00 45 10 (. ? W E .

DHCP ACK

DHCP ACK is a unicast acknowledgement by the server to the client.

The image shows a Wireshark capture of a DHCP ACK packet. The packet list at the top shows four packets: a Discover (1), an Offer (2), a Request (3), and an ACK (4). The selected packet is the ACK (4), which is a Dynamic Host Configuration Protocol (ACK) from source 192.168.0.1 to destination 192.168.0.21. The packet details pane shows the following structure:

- Dynamic Host Configuration Protocol (ACK)
 - Message type: Boot Reply (2)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xa697f2b
 - Seconds elapsed: 0
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0
 - Your (client) IP address: 192.168.0.21
 - Next server IP address: 0.0.0.0
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (ACK)
 - Length: 1
 - DHCP: ACK (5)
 - Option: (54) DHCP Server Identifier (192.168.0.1)
 - Length: 4
 - DHCP Server Identifier: 192.168.0.1
 - Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (86400s) 1 day
 - Option: (58) Renewal Time Value
 - Length: 4
 - Renewal Time Value: (43200s) 12 hours
 - Option: (59) Rebinding Time Value
 - Option: (1) Subnet Mask (255.255.255.0)
 - Option: (3) Router
 - Option: (6) Domain Name Server
 - Option: (755) End

The packet bytes pane shows the raw data: 0000 28 c6 3f 9e 57 d2 ec 84 b4 ec 1c f0 00 00 45 00 (. ? W E .

In Packet Details Section, we can see details like, source and destination address. ACK message body also contains other information like IP Address Lease Time, Subnet Mask, Router (Default Gateway), Domain Name Server, and Domain Name,

Finding out Server IP Address

The server IP address of DHCP server can be identified using the server identifier located in the options section of DHCP ACK message. In this case, server IP address is 192.168.0.1

We can also apply it as filter 'dhcp.option.dhcp_server_id' to server IP address.

The image shows a Wireshark packet capture window titled '2018A7P50193G_LAB8.pcap'. The packet list on the left shows three packets. The selected packet is a DHCP ACK message (packet 2021-04-12 11:53:04). The packet details pane on the right shows the structure of the DHCP ACK message. The 'DHCP Server Identifier' field is highlighted, showing the value '192.168.0.1'. The packet bytes pane at the bottom shows the raw data of the packet, with the 'DHCP Server Identifier' field highlighted in blue.

Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	Offer	- Transaction ID 0xa697f2b
2021-04-12 11:53:04	0.0.0.0	68	255.255.255.255	67	DHCP	Request	- Transaction ID 0xa697f2b
2021-04-12 11:53:04	192.168.0.1	67	192.168.0.21	68	DHCP	ACK	- Transaction ID 0xa697f2b

Seconds elapsed: 0

- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 192.168.0.21
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (ACK)
 - Length: 1
 - DHCP: ACK (5)
- Option: (54) DHCP Server Identifier (192.168.0.1)
 - Length: 4
 - DHCP Server Identifier: 192.168.0.1
- Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (86400s) 1 day
- Option: (58) Renewal Time Value
 - Length: 4
 - Renewal Time Value: (43200s) 12 hours
- Option: (59) Rebinding Time Value
 - Length: 4
 - Rebinding Time Value: (75600s) 21 hours
- Option: (1) Subnet Mask (255.255.255.0)
 - Length: 4
 - Subnet Mask: 255.255.255.0
- Option: (3) Router
 - Length: 4
 - Router: 192.168.0.1
- Option: (6) Domain Name Server
 - Length: 4

0110 00 00 00 00 00 63 82 53 63 35 01 05 36 04 c0c- Sc5-6

Option 54: DHCP Server Identifier (dhcp.option.dhcp_server_id), 4 bytes

Packets: 2740 - Displayed: 3 (0.1%) - Dropped: 0 (0.0%) Profile: Default

The client's IP address can be identified using the Your Client IP under the DHCP ACK section. In this case, client's allocated IP address is 192.168.0.21. We can also apply it as filter 'dhcp.ip.your' to filter out client's IP address.

Note : dhcp.ip.client can also be used to filter out client's allocated IP address .

2. Show a round of execution of the ARP protocol. Show ARP Request (2 marks) and Reply (2 marks) messages in that round. Find the MAC address of the replier (2 marks). Write the filter and show the output in a screenshot.

```
rohit@rohit:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0          192.168.0.1     0.0.0.0          UG      0      0      0 wlo1
192.168.0.0      0.0.0.0         255.255.255.0    U        0      0      0 wlo1
rohit@rohit:~$ netstat -r -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags  MSS  Window  irtt Iface
0.0.0.0          192.168.0.1     0.0.0.0          UG      0    0        0 wlo1
192.168.0.0      0.0.0.0         255.255.255.0    U        0    0        0 wlo1
rohit@rohit:~$
```

```
rohit@rohit:~$ sudo arp -a
[sudo] password for rohit:
dsldevice.lan (192.168.0.1) at ec:84:b4:ec:1c:f0 [ether] on wlo1
rohit@rohit:~$ sudo arp -v
Address          HWtype  HWaddress      Flags Mask            Iface
dsldevice.lan    ether    ec:84:b4:ec:1c:f0 C                    wlo1
Entries: 1      Skipped: 0      Found: 1
rohit@rohit:~$ sudo arp -d dsldevice.lan
rohit@rohit:~$
```

```
rohit@rohit:~$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=7.58 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=8.00 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=4.40 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=2.86 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=4.77 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=4.78 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=3.14 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=3.88 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=4.27 ms
64 bytes from 192.168.0.1: icmp_seq=10 ttl=64 time=4.74 ms
64 bytes from 192.168.0.1: icmp_seq=11 ttl=64 time=4.70 ms
64 bytes from 192.168.0.1: icmp_seq=12 ttl=64 time=6.01 ms
64 bytes from 192.168.0.1: icmp_seq=13 ttl=64 time=5.18 ms
64 bytes from 192.168.0.1: icmp_seq=14 ttl=64 time=16.4 ms
64 bytes from 192.168.0.1: icmp_seq=15 ttl=64 time=5.61 ms
64 bytes from 192.168.0.1: icmp_seq=16 ttl=64 time=3.55 ms
64 bytes from 192.168.0.1: icmp_seq=17 ttl=64 time=3.16 ms
64 bytes from 192.168.0.1: icmp_seq=18 ttl=64 time=3.76 ms
64 bytes from 192.168.0.1: icmp_seq=19 ttl=64 time=4.48 ms
64 bytes from 192.168.0.1: icmp_seq=20 ttl=64 time=35.8 ms
```

```
--- 192.168.0.1 ping statistics ---
140 packets transmitted, 140 received, 0% packet loss, time 139198ms
rtt min/avg/max/mdev = 1.347/13.337/82.413/15.361 ms
rohit@rohit:~$
```

ARP Request

The need for an ARP request arises when a device wants to know the MAC address of the device to which the source wants to communicate with.

The screenshot shows a Wireshark interface with a packet capture file named 2018A7P50193C_LAB8.pcap. The main pane displays a list of network packets. Packet 24 is selected, which is an ARP request from CigShang_ec to IntelCor_9e. The details pane below shows the structure of the Ethernet II frame and the ARP protocol fields.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:00		CigShang_ec		Broadcast		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:01		CigShang_ec		Broadcast		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:02		CigShang_ec		Broadcast		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:03		CigShang_ec		Broadcast		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:04		IntelCor_9e		Broadcast		ARP		Who has 192.168.0.17? Tell 192.168.0.21
2021-04-12 11:53:04		CigShang_ec		IntelCor_9e:57:d2		ARP		192.168.0.1 is at ec:84:b4:ec:1c:f0
2021-04-12 11:53:04		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:04		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:09		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:09		CigShang_ec		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:14		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:14		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:19		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:19		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:24		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:24		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:29		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:29		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:34		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:34		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:39		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:39		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:44		CigShang_ec		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:44		IntelCor_9e		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2

Packet 24 Details:

- Ethernet II, Src: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
 - Type: ARP (0x8006)
 - Trailer: 000000000000000000000000b3f3014a
- Address Resolution Protocol (request)

Hex Dump:

```

0000  ff ff ff ff ff ff ff ff  ec 84 b4 ec 1c f0  08 06 00 01  ....

```

Status Bar: Packets: 2740 · Displayed: 59 (2.2%) · Dropped: 0 (0.0%) Profile: Default

ARP Reply

Wireshark - 2018A7P50193G_LAB8.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:34	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:34	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:39	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:39	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:44	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:44	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:49	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:49	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:54	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:54	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2
2021-04-12 11:53:59	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:59	IntelCor_9e...		CigShang_ec:1c:f0		ARP		192.168.0.21 is at 28:c6:3f:9e:57:d2

> Frame 1910: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

- Ethernet II, Src: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2), Dst: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
 - Destination: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
 - Source: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
 - Type: ARP (0x0806)
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
 - Sender IP address: 192.168.0.21
 - Target MAC address: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
 - Target IP address: 192.168.0.1

0000 ec 84 b4 ec 1c f0 28 c6 3f 9e 57 d2 08 06 00 01(? W

>> Address Resolution Protocol: Protocol

Packets: 2740 · Displayed: 59 (2.2%) · Dropped: 0 (0.0%) Profile: Default

MAC Address of the replier is the sender's MAC address in ARP Reply section which is **28:c6:3f:9e:57:d2**

arp.src.hw_mac can be used as a filter to find out replier's mac address.

The image shows a Wireshark packet capture window titled "2018A7P50193G_LAB8.pcap". The filter bar at the top is set to "arp.src.hw_mac". The packet list shows several ARP requests and replies. The selected packet is an ARP reply (Frame 1910) with the following details:

- Frame 1910: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2), Dst: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
- Destination: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
- Source: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Type: ARP (0x0806)
- Address Resolution Protocol (reply)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Sender IP address: 192.168.0.21
- Target MAC address: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
- Target IP address: 192.168.0.1

The packet bytes pane shows the raw data of the ARP reply packet:

```
0000  ec 84 b4 ec 1c f0 28 c6 3f 9e 57 d2 08 06 00 01  ....(.?..W....
0010  08 00 06 04 00 02 28 c6 3f 9e 57 d2 c0 a8 00 15  ....(.?..W....
0020  ec 84 b4 ec 1c f0 c0 a8 00 01  ....
```

The status bar at the bottom indicates: "Sender MAC address (arp.src.hw_mac), 6 bytes", "Packets: 2740 · Displayed: 59 (2.2%) · Dropped: 0 (0.0%)", and "Profile: Default".

3. Find the MAC address and the IP address of the Gateway router (2 marks). Write the filter and show the output in a screenshot.

We can find the IP address and MAC address of Gateway router using ARP request packets.

Type `arp.opcode == 1` and find out the sender's MAC address and IP address.

In my case,

MAC Address of Gateway Router is = `ec:84:b4:ec:1c:f0`

Filter for MAC Address of Gateway Router = `arp.src.hw_mac`

IP Address of Gateway Router is = `198.168.0.1`

Filter for IP Address of Gateway Router = `arp.src.proto_ip v4`

2018A7P50193G_LAB8.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: `arp.opcode == 1`

Time	Source	Source Port	Destination	Destination Port	Protocol	DHCP Message Type	Info
2021-04-12 11:53:03	CigShang_ec...		Broadcast		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:04	IntelCor_9e...		Broadcast		ARP		Who has 192.168.0.1? Tell 192.168.0.21
2021-04-12 11:53:04	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:09	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:14	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:19	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:24	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:29	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:34	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:39	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:44	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1
2021-04-12 11:53:49	CigShang_ec...		IntelCor_9e:57:d2		ARP		Who has 192.168.0.21? Tell 192.168.0.1

Frame 1909: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0), Dst: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)

- Destination: IntelCor_9e:57:d2 (28:c6:3f:9e:57:d2)
- Source: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)
- Type: ARP (0x0806)
- Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

- Hardware type: Ethernet
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)

Sender MAC address: CigShang_ec:1c:f0 (ec:84:b4:ec:1c:f0)

Sender IP address: 192.168.0.1

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.0.21

0000 28 c6 3f 9e 57 d2 ec 84 b4 ec 1c f0 00 06 00 01 (? W)

0010 08 00 06 04 00 01 ec 84 b4 ec 1c f0 c0 a8 00 01

0020 00 00 00 00 00 00 c0 a8 00 15 00 00 00 00 00 00

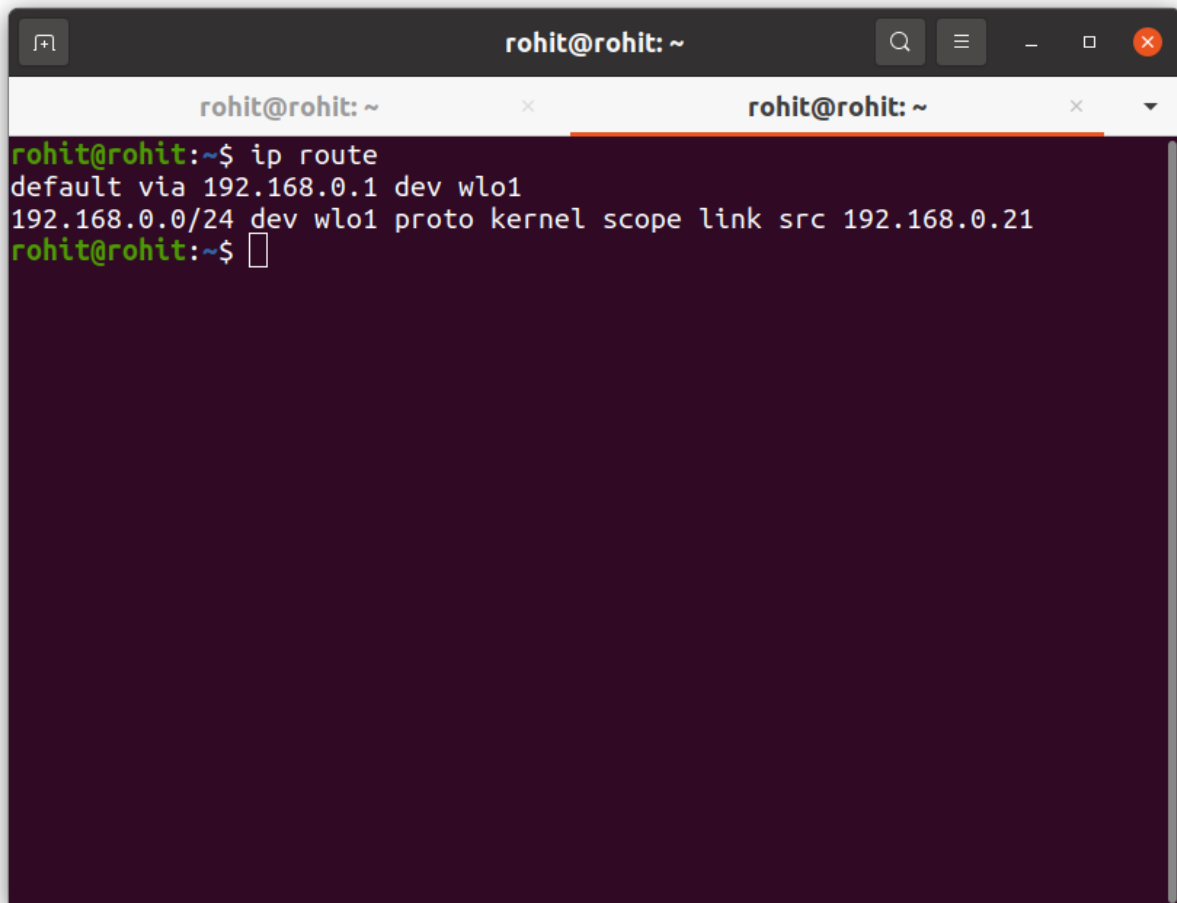
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Sender MAC address (arp.src.hw_mac), 6 bytes

Packets: 2740 · Displayed: 35 (1.3%) · Dropped: 0 (0.0%)

Profile: Default

These values can be verified using finding the router's IP and MAC using the terminal:



```
rohit@rohit: ~  
rohit@rohit:~$ ip route  
default via 192.168.0.1 dev wlo1  
192.168.0.0/24 dev wlo1 proto kernel scope link src 192.168.0.21  
rohit@rohit:~$
```

The image shows a terminal window with a dark purple background. The window title is 'rohit@rohit: ~'. The prompt is 'rohit@rohit:~\$'. The command 'ip route' has been executed, resulting in two lines of output: 'default via 192.168.0.1 dev wlo1' and '192.168.0.0/24 dev wlo1 proto kernel scope link src 192.168.0.21'. The prompt is now 'rohit@rohit:~\$' with a cursor.