

Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

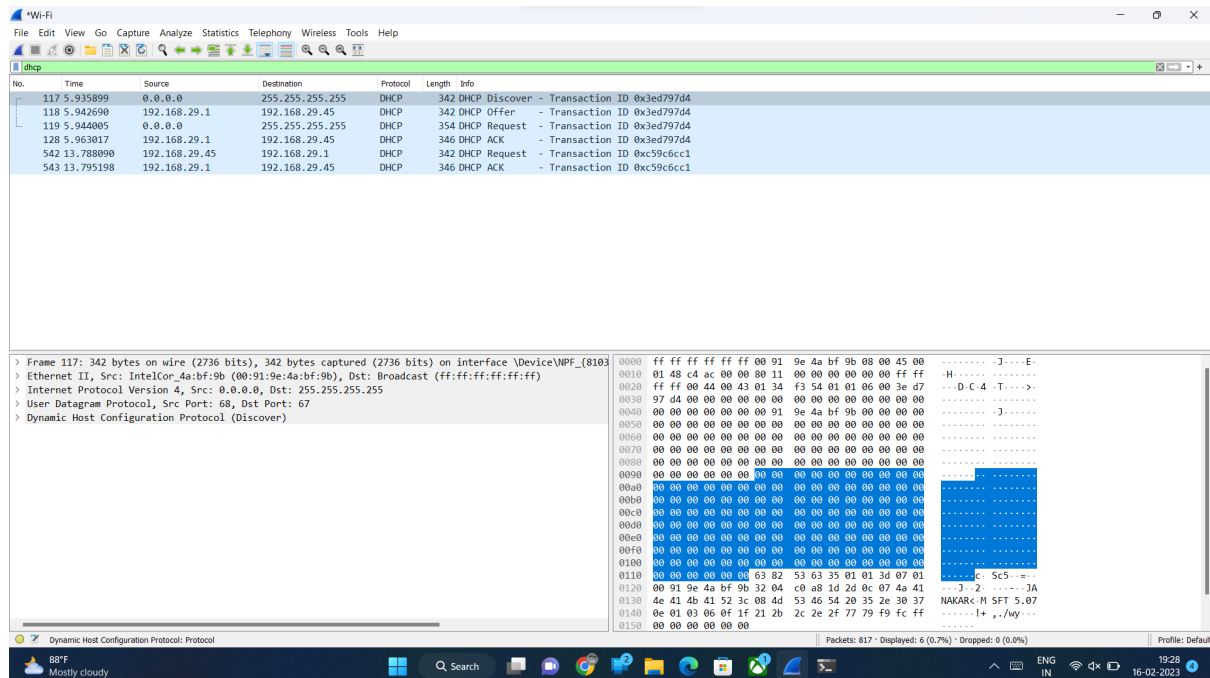
Name: Janakar Patel

Roll No: 20BIT061

Experiment 5:

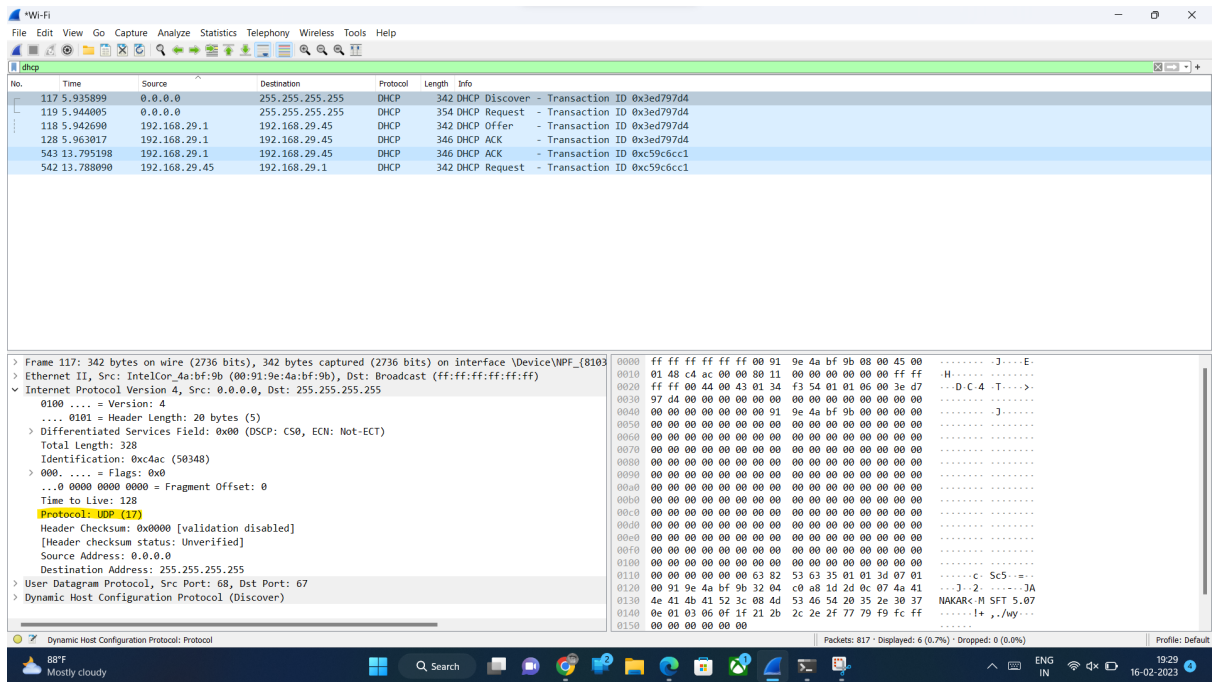
Aim: To understand the working of DHCP by using wire shark and packet tracer.

Software Tools required: - Wire-shark and Cisco packet tracer

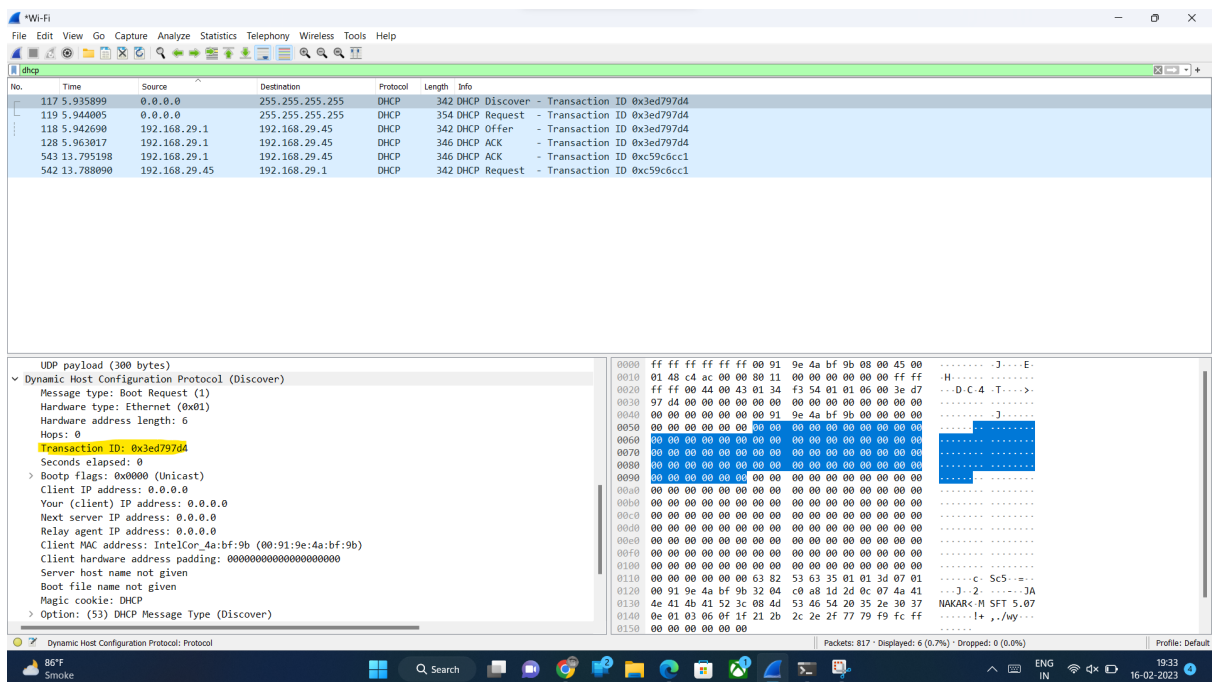


1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?

Ans: It is using UDP protocol.



- What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.
Ans:
Source IP address is 0.0.0.0
- What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.
Ans:
Destination IP address is 255.255.255.255
- What is the value in the transaction ID field of this DHCP Discover message?
Ans:
Transaction ID is 0x3ed797d4



5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?

Ans:

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_4a:bf:9b (00:91:9e:4a:bf:9b)
- 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: (61) Client Identifier
- Option: (50) Requested IP Address (192.168.29.45)
- Option: (12) Host Name
- Option: (60) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End
- Padding: 000000000000

Transaction ID (dhcp.id), 4 bytes

Packets: 817 · Displayed: 6 (0.7%) · Dropped: 0 (0.0%)

Profile: Default

6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?

Ans: Source and destination port number are interchange for both types of message.

Frame 117: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8103...}

Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

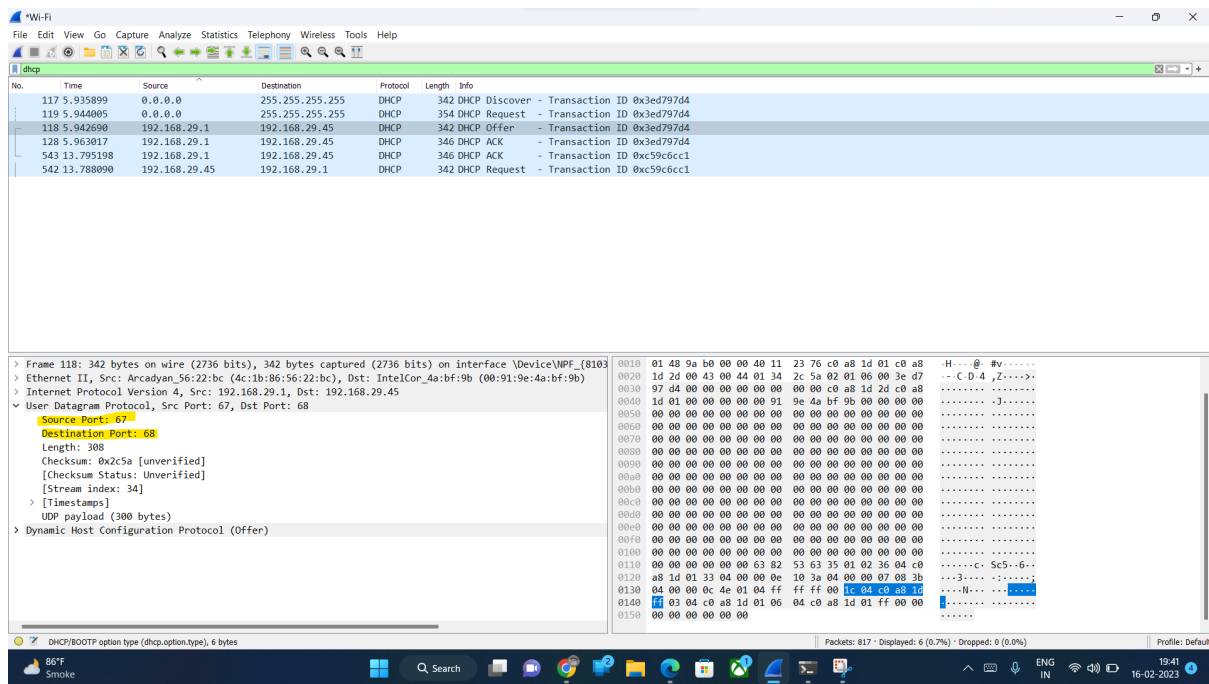
User Datagram Protocol, Src Port: 68, Dst Port: 67

- Source Port: 68
- Destination Port: 67
- Length: 308
- Checksum: 0xf354 [unverified]
- Checksum Status: Unverified
- Stream index: 33
- [Timestamp]
- UDP payload (300 bytes)
- Dynamic Host Configuration Protocol (Discover)

DHCP/BOOTP option type (dhcp.option.type), 1 byte

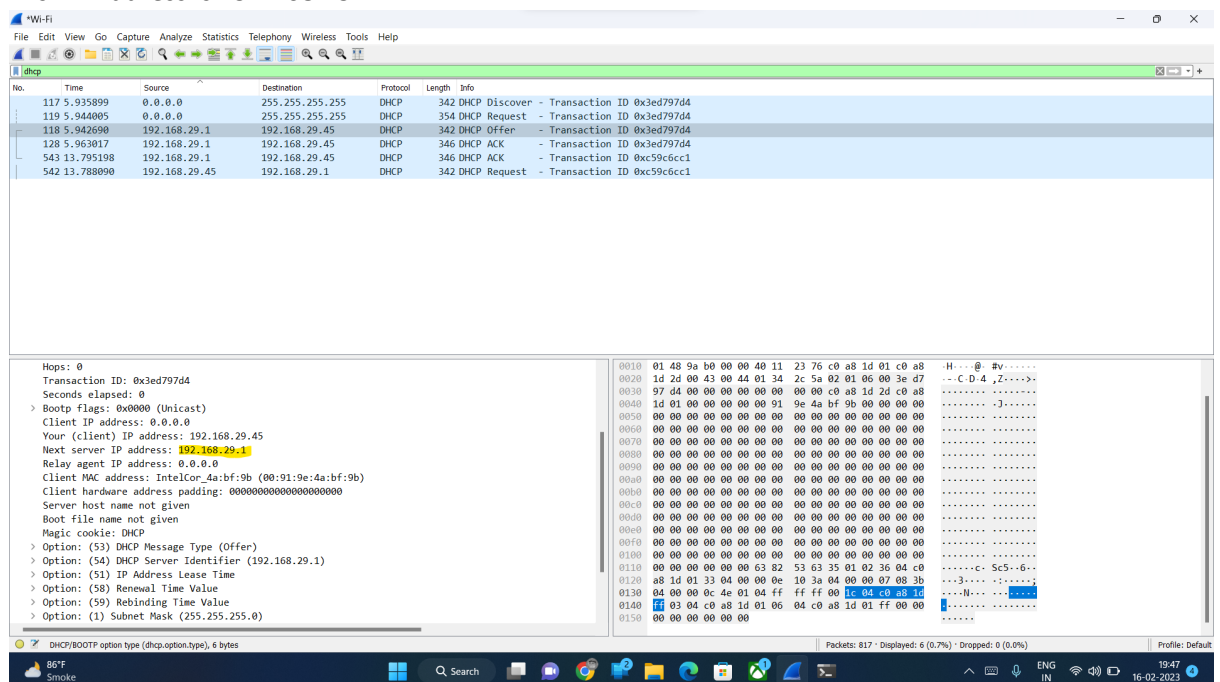
Packets: 817 · Displayed: 6 (0.7%) · Dropped: 0 (0.0%)

Profile: Default



7. What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.

Ans: IP Address is 192.168.29.1



8. What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [Hint: Look at your trace carefully. The answer to this question may differ from what you see in Figure 4.24 in the textbook. If you really want to dig into this, consult the [DHCP RFC](#), page 24.]

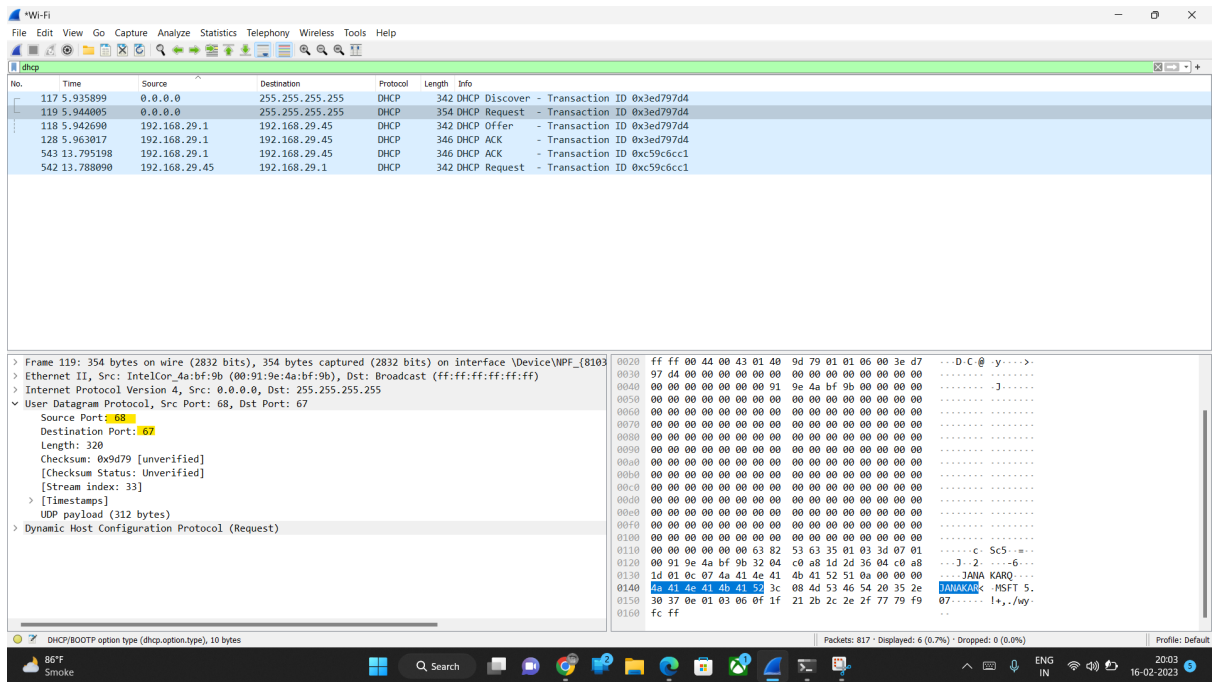
Ans: IP address is 192.168.29.45

Hops: 0
Transaction ID: 0x3ed797d4
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.29.45
Next server IP address: 192.168.29.1
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b)
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 (192.168.29.1)
> Option: (51) IP Address Lease Time
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
> Option: (1) Subnet Mask (255.255.255.0)

9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?
Ans:

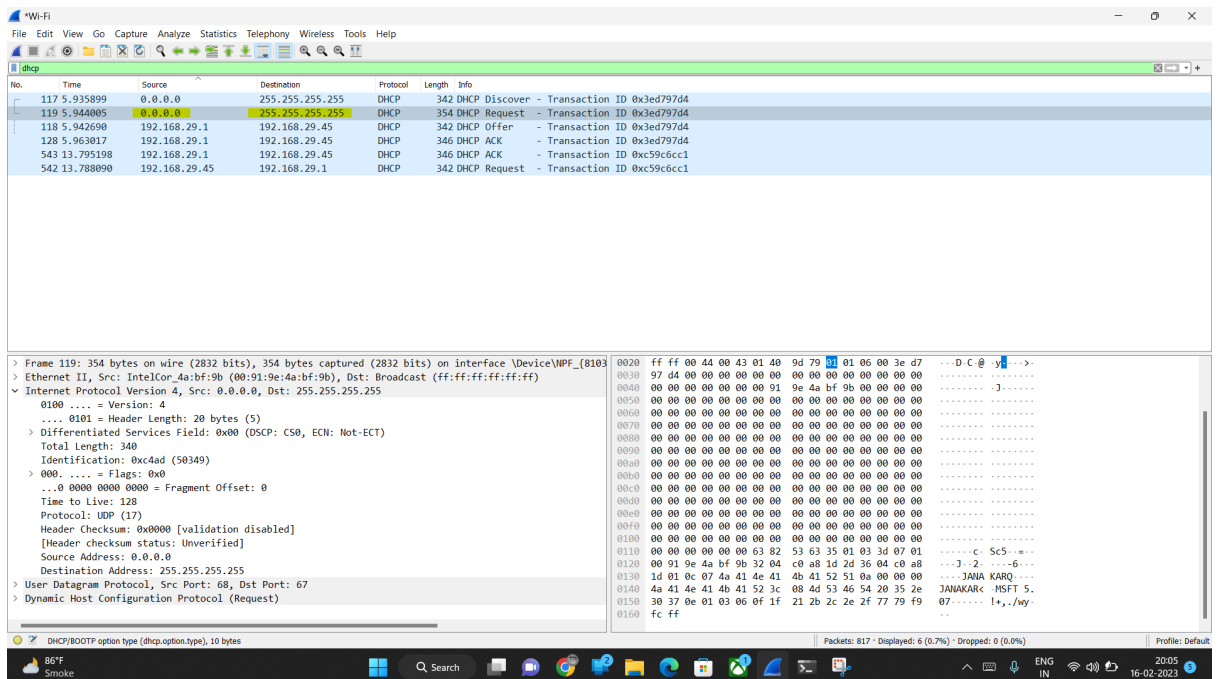
Your (client) IP address: 192.168.29.45
Next server IP address: 192.168.29.1
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier (192.168.29.1)
> 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: (28) Broadcast Address (192.168.29.255)
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (255) End
Padding: 0000000000000000

10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?
Ans: Source port is 68 and destination is 67



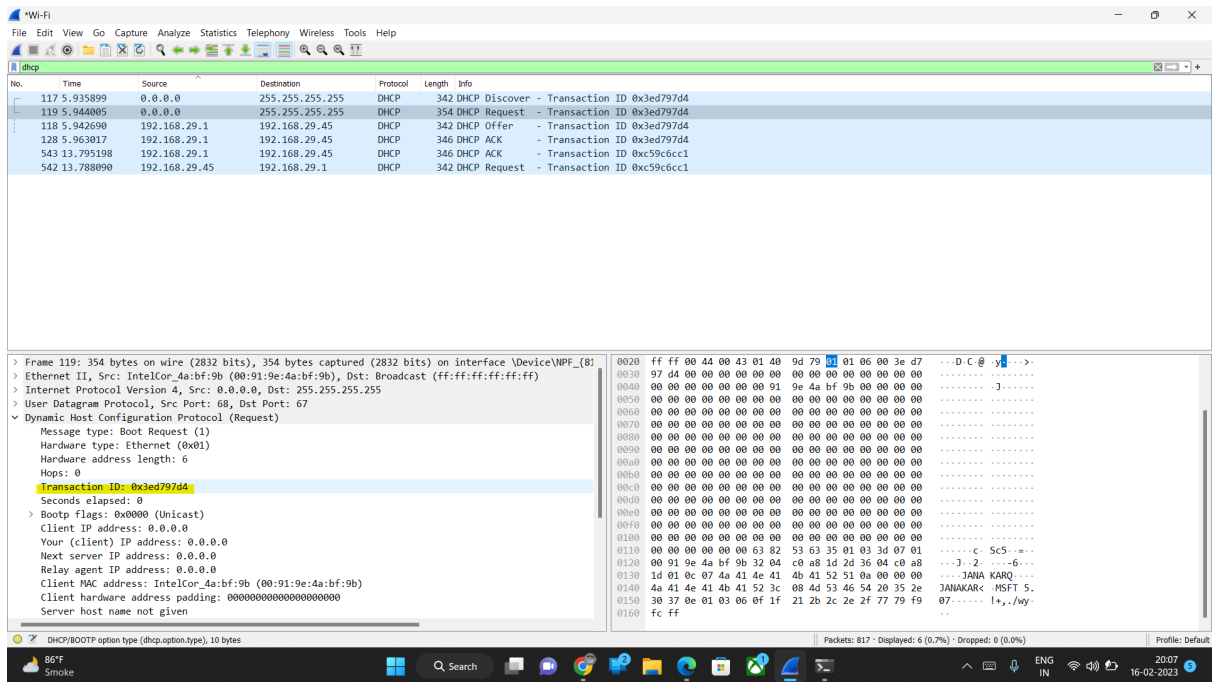
11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.
12. What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.

Ans:



13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?

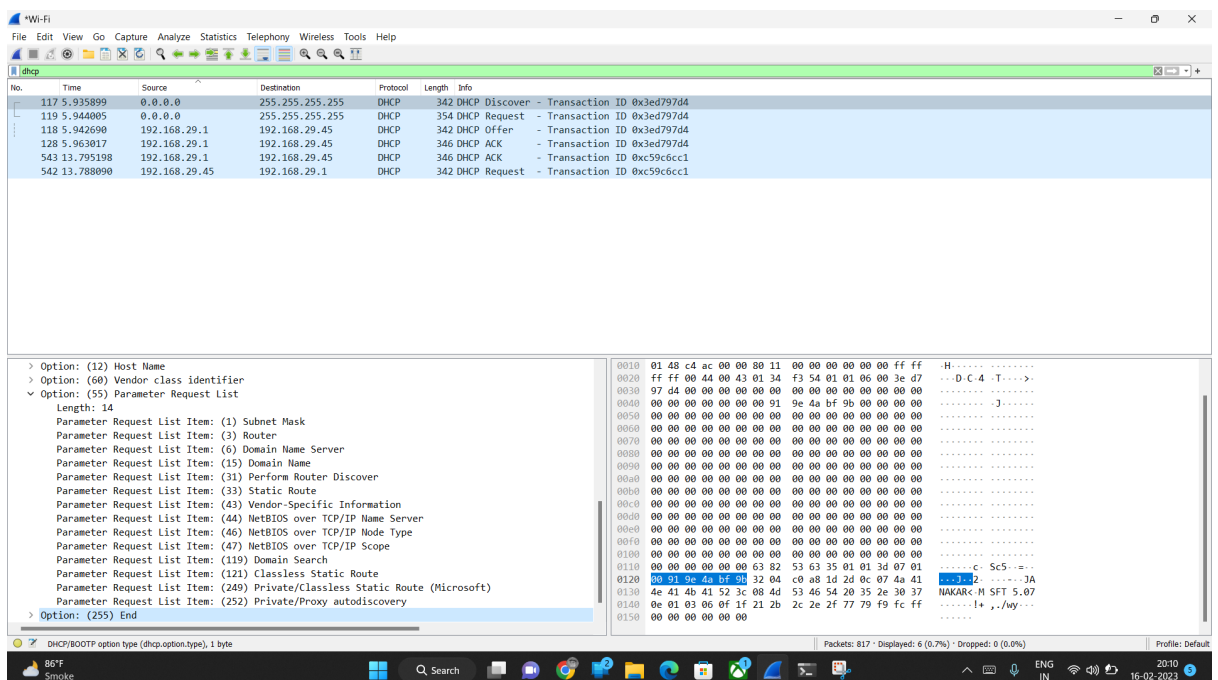
Ans: Transaction ID is 0x3ed797d4. Yes all the transaction ID is same

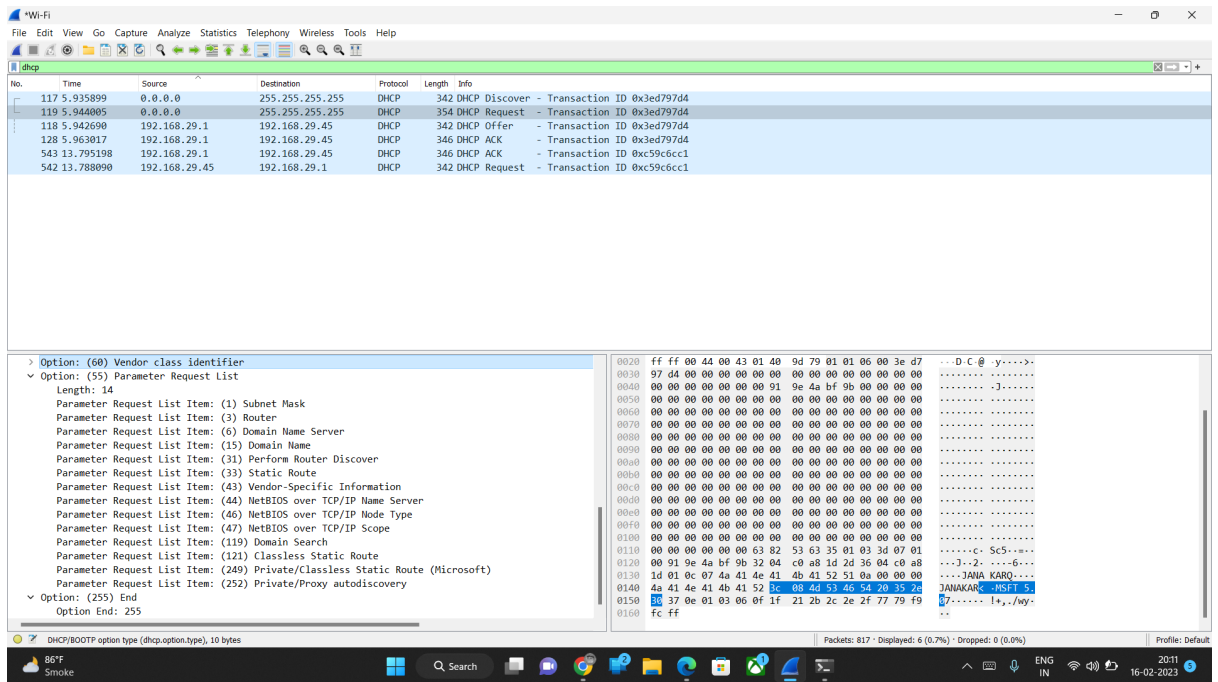


14. Now inspect the options field in the DHCP Discover message and take a close look at the “Parameter Request List”. The [DHCP RFC](#) notes that
- “The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number.”

What differences do you see between the entries in the ‘parameter request list’ option in this Request message and the same list option in the earlier Discover message?

Ans: There is no difference between the lists of discover and request message.

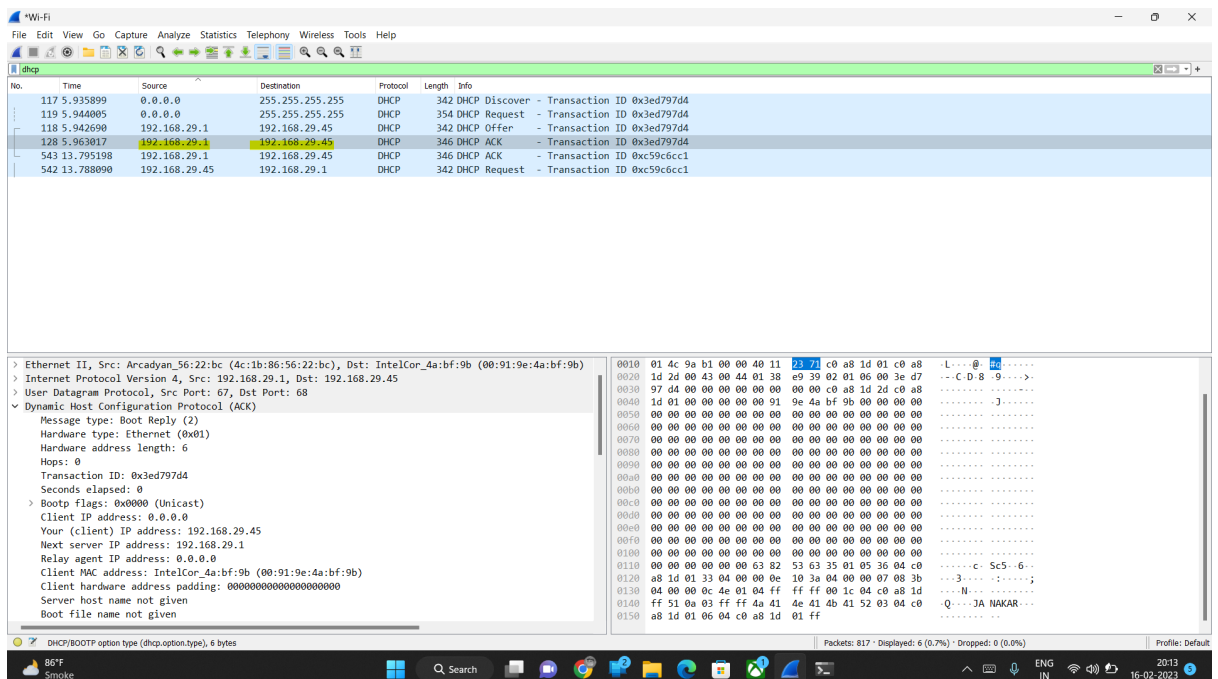




15. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

16. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.

Ans: The source IP Address is 192.168.29.1 and Destination IP address is 192.168.29.45



16. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?

Ans: IP address is 192.168.29.45

Wireshark packet capture showing DHCP transactions. The packet list shows a DHCP Discover (117), DHCP Request (119), DHCP Offer (118), DHCP ACK (128), and another DHCP Request (543). The packet details for the first DHCP Offer (118) are expanded, showing options like DHCP Message Type (ACK), DHCP Server Identifier (192.168.29.1), and IP Address Lease Time. The packet bytes pane shows the raw data of the DHCP Offer packet.

17. For how long a time (the so-called “lease time”) has the DHCP server assigned this IP address to the client?

Ans: It takes 1 hour time lease time.

Wireshark packet capture showing DHCP transactions. The packet list shows a DHCP Discover (117), DHCP Request (119), DHCP Offer (118), DHCP ACK (128), and another DHCP Request (543). The packet details for the first DHCP ACK (128) are expanded, showing options like DHCP Message Type (ACK), DHCP Server Identifier (192.168.29.1), and IP Address Lease Time (3600s) 1 hour. The packet bytes pane shows the raw data of the DHCP ACK packet.

18. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?

Ans: IP address is 192.198.29.1

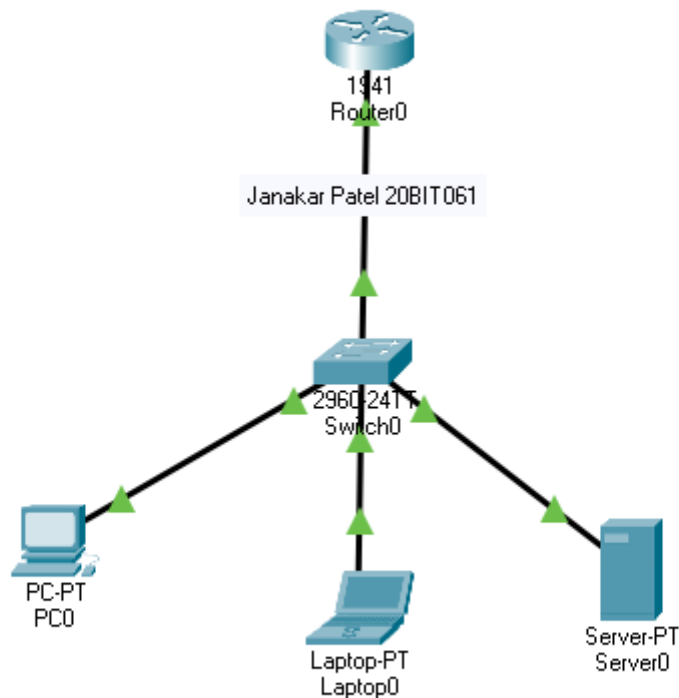
The image shows a Wireshark packet capture of DHCP traffic. The packet list at the top shows several DHCP packets. The selected packet is a DHCP Offer (342) with Transaction ID 0x3ed797d4. The packet details pane shows the following options:

- Length: 4
- Subnet Mask: 255.255.255.0
- Option: (28) Broadcast Address (192.168.29.255)
 - Length: 4
 - Broadcast Address: 192.168.29.255
- Option: (81) Client Fully Qualified Domain Name
 - Length: 10
 - Flags: 0x03, Server overrides, Server
 - A-RR result: 255
 - PTR-RR result: 255
 - Client name: JANAAR
- Option: (3) Router
 - Length: 4
 - Router: 192.168.29.1
- Option: (6) Domain Name Server
 - Length: 4
 - Domain Name Server: 192.168.29.1
- Option: (255) End
 - Option End: 255

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII representation shows the client name "JANAAR" and the router address "192.168.29.1".

Task 2: Configure a DHCP server in packet tracer by using the following link.

<https://www.youtube.com/watch?v=Pbu0rbCNJrA>



System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 2010 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB

CISCO1941/K9 platform with 524288 Kbytes of main memory

Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340

program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software

program load complete, entry point: 0x81000000, size: 0x2bb1c58

Self decompressing the image :

[OK]

Smart Init is enabled

smart init is sizing iomem

TYPE MEMORY_REQ

Onboard devices &

buffer pools 0x01E8F000

TOTAL: 0x01E8F000

Rounded IOMEM up to: 32Mb.

Using 6 percent iomem. [32Mb/512Mb]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#ip dhcp pool ABC-POOL

```
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.254
Router(dhcp-config)#dns-server 192.168.0.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#write memory
Building configuration...
[OK]
Router#
```

PC0

Physical Config Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display Name PC0

Interfaces FastEthernet0

Gateway/DNS IPv4

☒ DHCP

☐ Static

Default Gateway 192.168.0.254

DNS Server 192.168.0.1

Gateway/DNS IPv6

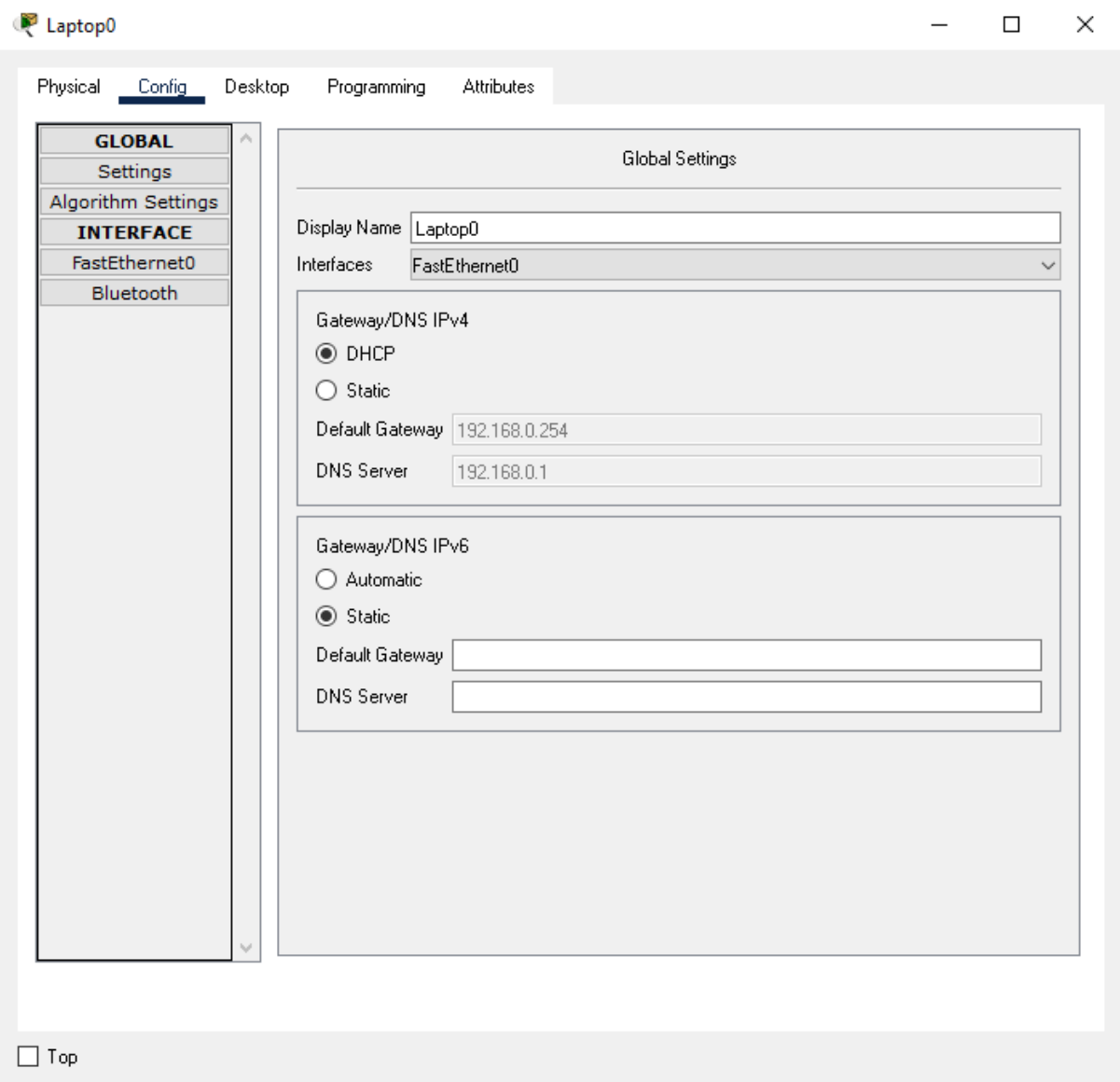
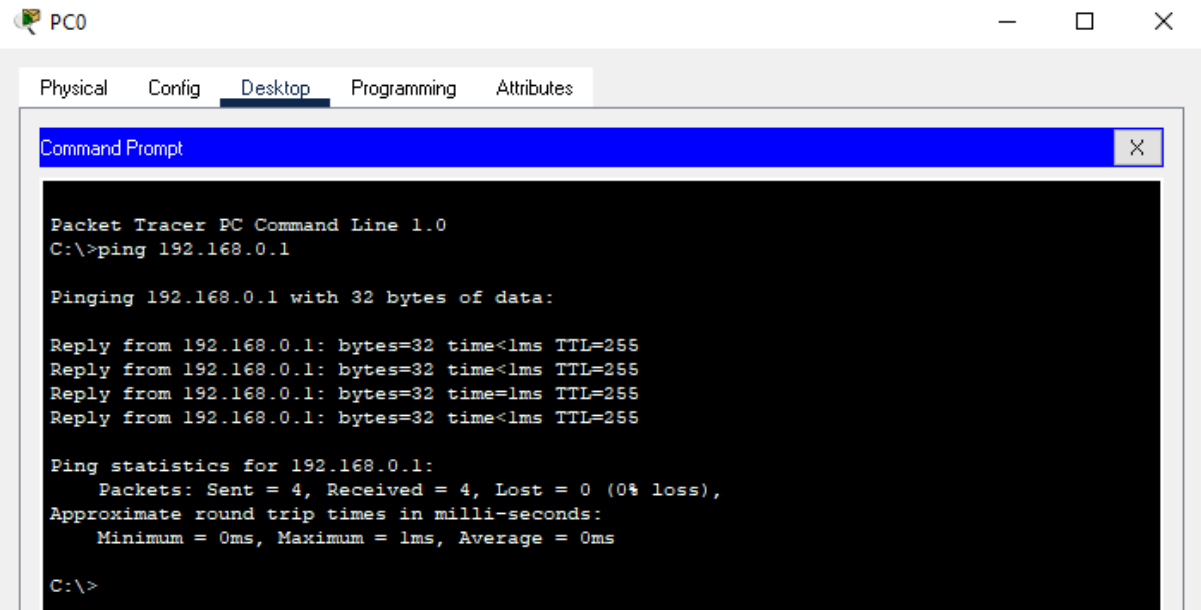
☐ Automatic

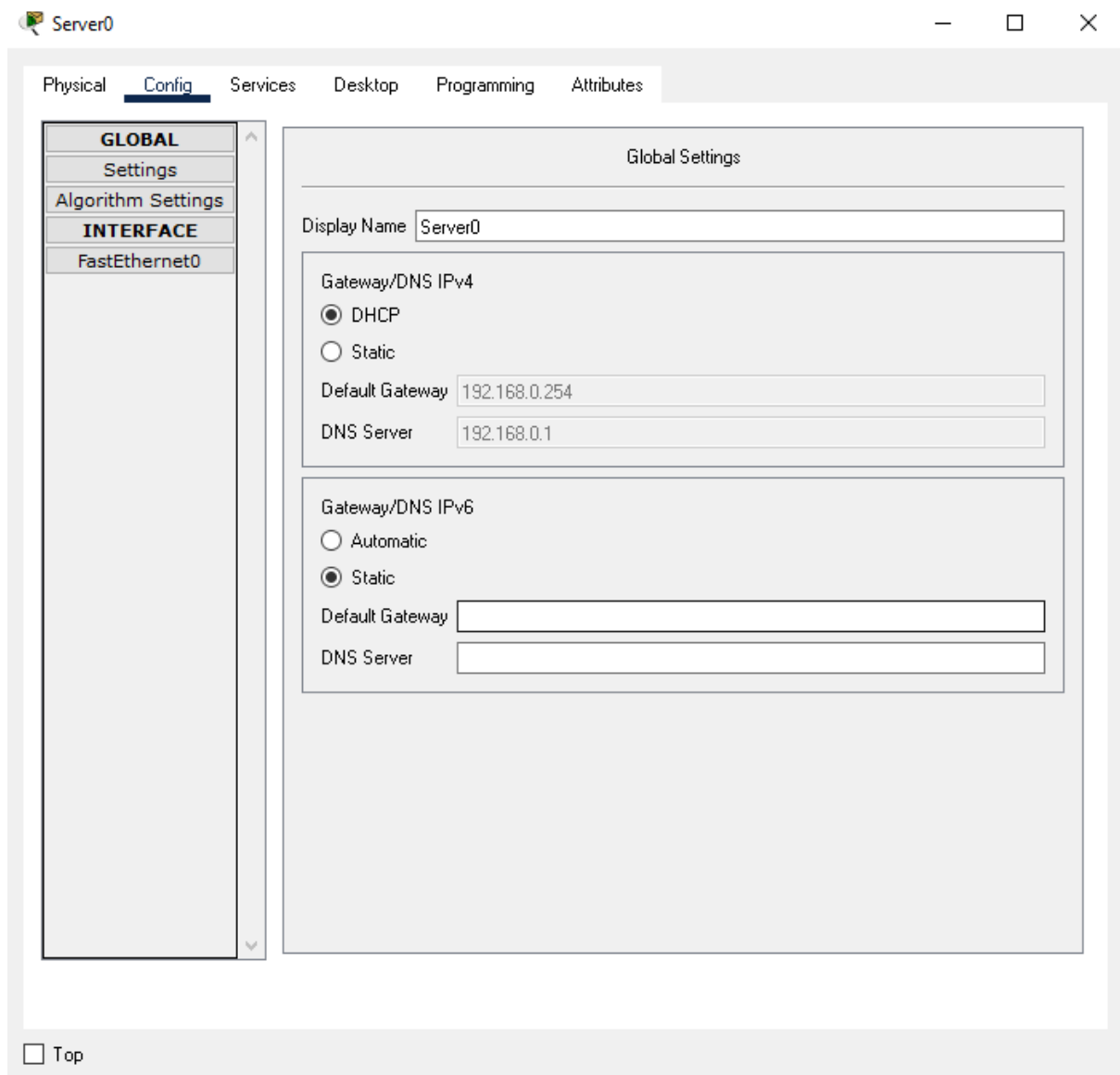
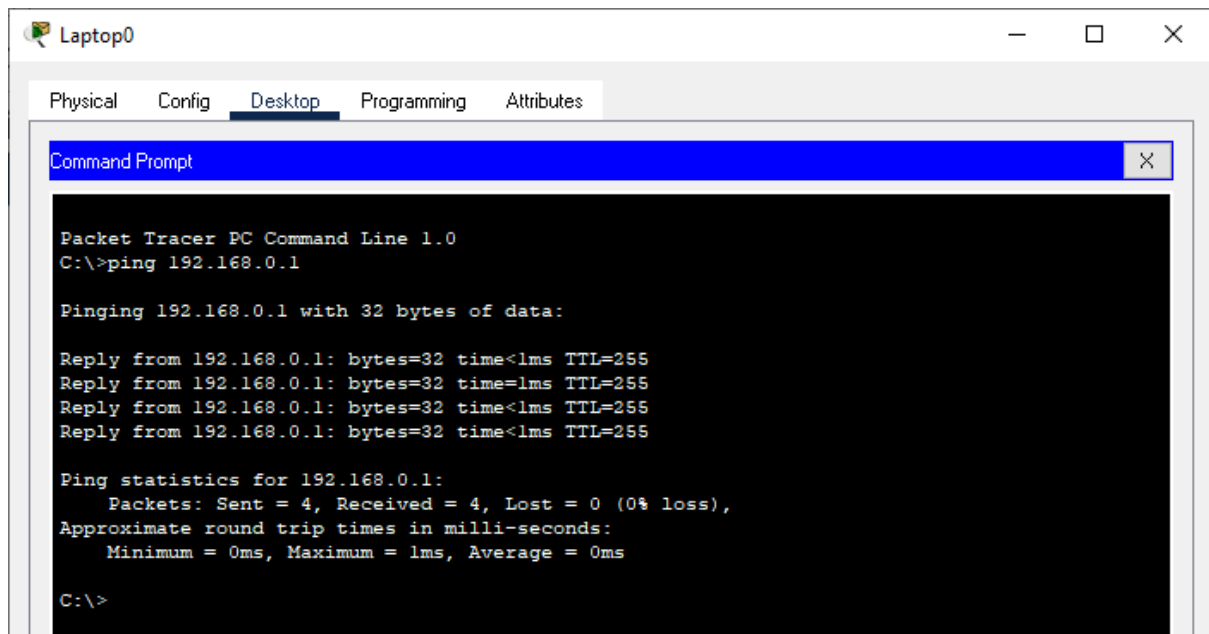
☒ Static

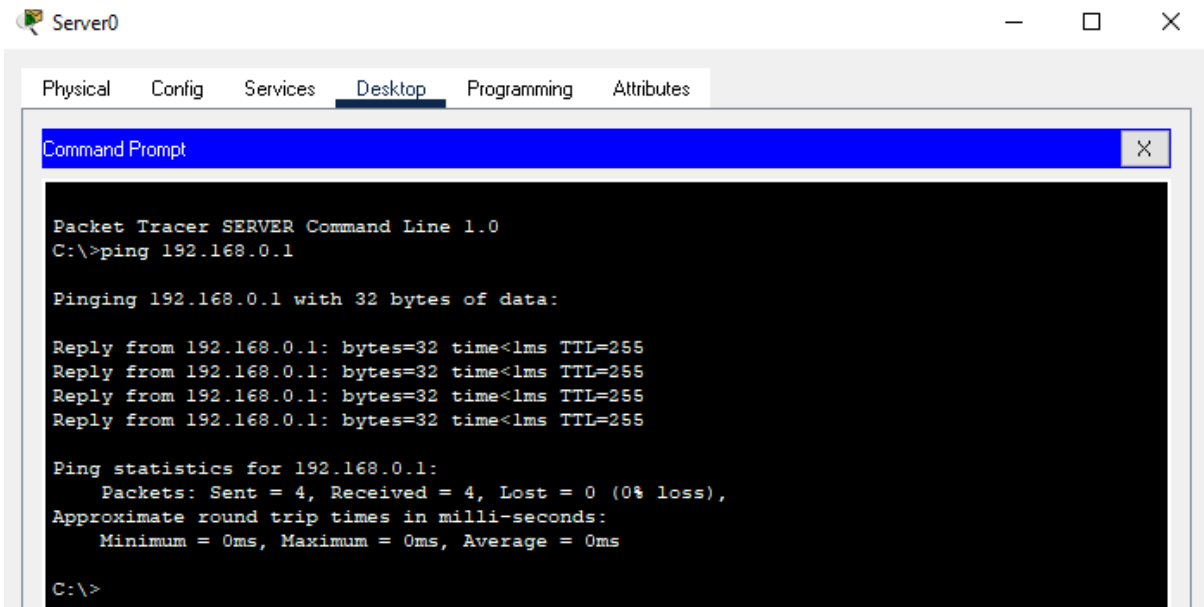
Default Gateway

DNS Server

☐ Top







```
Router>
```

```
Router>ping 192.168.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
Router>ping 192.168.0.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
Router>ping 192.168.0.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
Router>
```

