During tutorials prepare a short report of your activities and show it to your tutor.
Study the following **questions** and verify the correctness of the **answers** if given.
Be aware that the exam question might be directly related to the tutorial questions

Lecture 04 addendum tutorial:

Study the TCP Flow Graph that you obtained in Tutorial 4 (copy on Moodle) and answer the following questions:

1. Describe activities in frames 11, 13, 15
2. In the frame 32 why we have **Ack = 10043**
3. **Ack = 10043** has been repeated in many frames after the frame 32. What does it mean?
4. What is happening in the frame 86?
5. Are there any retransmissions occurring. In which frames?
6. Indicate frames related to the congestion control. What is happening after such frames have been received?

Group 10 Summary:

1. Frame11: The client choose an initial sequence number A and send TCP SYN message to the server
   Frame13: The server choose an initial sequence number and send TCP SYN-ACK message. The ACK number is set one more than the received sequence number A+1.
   Frame15: The client send a segment which length is 306

2. Ack num 10043 equals sequence number of frame31 8783 plus MSS 1260
   10043 = 8783 + 1260

3. The client doesn't accept the data with the beginning of 10043, and the Ack number of client remains 10043

4. There is a TCP fast retransmit procedure. If sender receives 3x2 ACKs for same data ("triple duplicate ACKs"), resend unACKed segment with smallest sequence number which is 10043

5. Frame 86 , Frame 121

6. Frame 86 , Frame 121: the receipt of three duplicate ACKs, When the congestion is detected, cwnd is typically halved, and the congestion- avoidance mode is entered

Group 4 Summary:

1. TCP 3-way handshake. The first two handshakes in the TCP three-way handshake between frame 11 and frame 13.
   Frame 11 sends a segment with seq 0 to the host with ip address 172.16.8.1 to the host with ip address 130.194.64.145.

Frame 13 is sent by the host with the ip address 130.194.64.145 to ack and seq to the host with the ip address 172.16.8.1.
HTTP connection gets GET command on frame 15

2. ACK=segment len+seq = Next sequence number
   Because the next sequence number of frame 31 is 10043, need the next sequence number is 10043 so the ACK for frame 32 is 10046.

3. Indicates that the data segment has been lost, 32 is the location where the data was lost, #1 represents the lost one, #2 means lost twice.

4. TCP Restransmission
   Frame 86 retransmits the packet with seq = 10043 ack = 643

5. 115,143,150,151,153,159,160,164,165,169,171,176,177,180,220,228,229,235,236,243,245,246,247,251,255,256.

6. When the sender continuously receives more than 3 identical acknowledgments, it means that the packet is lost, immediately uses fast retransmission, and enters the fast recovery state. After receiving these frames, ssthresh = cwnd / 2, and cwnd = ssthresh.

Group 5 Summary:

1. Describe activities in frames 11, 13, 15
   Frame 11 send a connection request from pc to server.
   Frame 13 send a connection response from server to pc.
   Frame 15 the pc sent a get request to server.

2. In the frame 32 why we have Ack = 10043
   8783+1260=10043

3. The datagram has been lost.

4. Retransmit the lost frame.

5. Yes, frame 86, 143, 150, 159, 160 frames.

6. 121, 122 (out of order). Adjust the congestion window.

Lecture 05 tutorial: Network Layer. Part 1.

Study the following questions. Verify the correctness of the sample and student group answers.

Question 1.
What is the fundamental difference between a router and a (link-layer) switch?

Answer (Group 6):
A router forwards a packet based on the packet's IP (layer 3) address. A link-layer switch forwards a packet based on the packet's MAC (layer 2) address.

Question 2.
What is the difference between routing and forwarding?

Answer (Group 6):
Forwarding is about moving a packet from a router's input port to the appropriate output port. Routing is about determining the end-to-routes between sources and destinations.

Question 3.
Do routers have IP addresses? If yes, how many?

Answer (Group 7):
Yes, it depends on the number of interfaces the router has. Each interface will be assigned a IP address. They must have at least two IP address.

Question 4.
Suppose Host A sends Host B a TCP segment encapsulated in an IP packet. When Host B receives the packet, how does the network layer in Host B know it should pass the payload of the IP packet to TCP rather than to UDP or to something else?

Answer (Group 7):
In the IPv4 header, there are 8 bit protocol field. if the protocol field is 6 indicating the transport protocol is TCP. if the protocol field is 17 indicating the transport protocol is UDP.

Question 5.
Explain the meaning of the following fields in the IPv4 header:

a. Total Length (TL)
b. Time to Live (TTL)

Answer (Group 8):

a. TL is the total length of the IP datagram. It includes the header and data. The picture above is the IP header. Because the field is 16 bits long, the theoretical maximum length of IP datagram is 65535 bytes. Since the length of the header is 20 bytes, the minimum total length is 20 bytes.

b. TTL is an 8 bit field. TTL is the maximum number of hops IP packet can forward in computer network. It ensures that datagram does not loop through the network forever. For example, when a routing loop is selected. When a router processes a datagram, the value of the TTL field is subtracted by 1. If the value of TTL is 0, Then the datagram is discarded and the router will send the ICMP time exceeded message to IP packet sender.

Question 6.
What does the Internet Corporation for Assigned Names and Numbers (ICANN) do?

Answer (Group 8):
ICANN mainly manages the assignment of both IP address, domain names and protocol parameter configuration. For example, It assigns and manages top-level domain names (such as ".com", ".info", ".name" etc. and authorizes private companies to become domain name registrars as well.

Question 7.
What is CIDR? What does **120.12.20.0/22** mean?

Answer (Group 9):
CIDR is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme. Instead of being limited to network identifiers (or "prefixes") of 8, 16 or 24 bits, CIDR currently uses prefixes anywhere from 13 to 27 bits. Thus, blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts. This allows for address assignments that much more closely fit an organization's specific needs.

In this case (120.12.20.0/22), the first 22 bits of the IP adress are used to identify the unique network leaving the remaining bits to identify the specific hosts.

Question 8.
Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix `223.1.17.0/24`. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form `a.b.c.d/x`) that satisfy these constraints.

Answer (Group 10):
Subnet with 12 interfaces : 223.1.17.176/28
Subnet with 60 interfaces : 223.1.17.192/26
Subnet with 90 interfaces : 223.1.17.0/25

Question 9.
Consider a subnet with prefix 128.119.40.128/26. Give an example of one IP address (of form xxx.xxx.xxx.xxx) that can be assigned to this network. Suppose an ISP owns the block of addresses of the form 128.119 .40.64/26. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. What are the prefixes (of form a.b.c.d/x) for the four subnets?

Answer (Group 9):
Binary: 10000000.01110111.00101000.10000000

An example IP address can be assigned to the above network：
Binary: 10000000.01110111.00101000.10000001
Decimal:128.119.40.129

Four subnets:

1. Binary: 10000000.01110111.00101000.01000000 / 28
Decimal:128.119.40.64/28

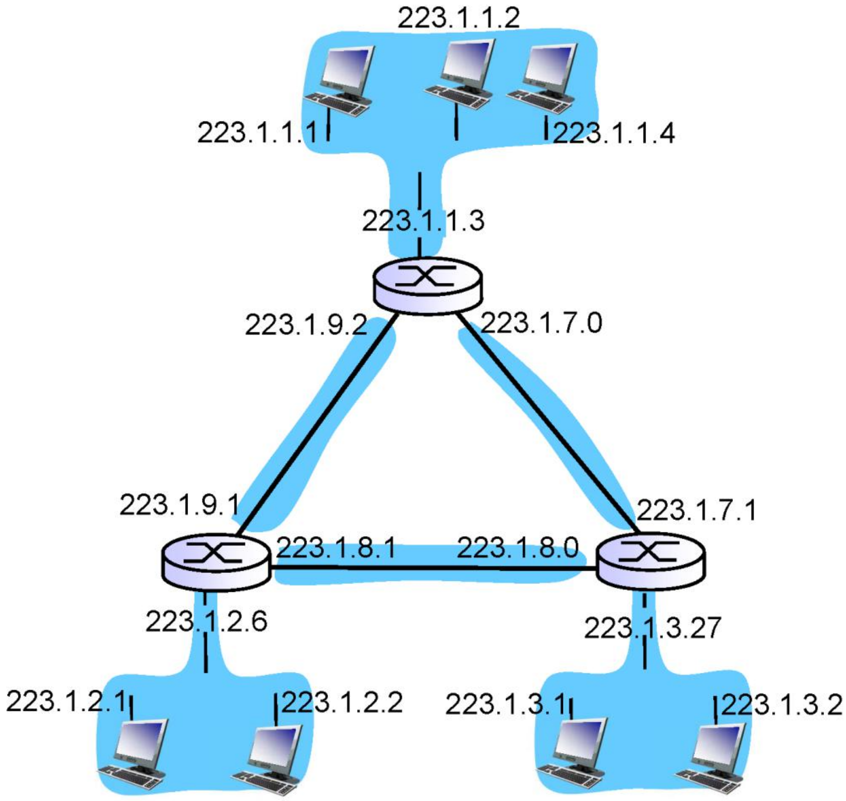
2. Binary: 10000000.01110111.00101000.01010000 / 28
Decimal:128.119.40.80/28

3. Binary: 10000000.01110111.00101000.01100000 / 28
Decimal:128.119.40.96/28

4. Binary: 10000000.01110111.00101000.01110000 / 28
Decimal:128.119.40.112/28

Each subnet contains 16 IPs, while 14 of them can be assigned with all 0s (net id) and all 1s (broadcast address) unavailable.

Question 10.
Consider the network **topology** shown in Slide 28:



Denote the three subnets **with hosts** (starting clockwise at 12:00) as Networks A, B, and C. Denote the subnets **without hosts** as Networks D, E, and F.

a) Assign network addresses to each of these six subnets, with the following constraints: All addresses must be allocated from 214.97.254/23; Subnet A should have enough addresses to support 250 interfaces; Subnet B should have enough addresses to support 120 interfaces; and Subnet C should have enough addresses to support 120 interfaces. Of course, subnets D, E and F should each be able to support two interfaces. For each subnet, the assignment should take the form a.b.c.d/x or a.b.c.d/x - e.f.g.h/y.

b) Using your answer to part (a), provide the forwarding tables (using longest prefix matching) for each of the three routers

Sample Answer:
From 214.97.254/23, possible assignments are

a) Subnet A: 214.97.255/24 (256 addresses)
Subnet B: 214.97.254.0/25 - 214.97.254.0/29 (128-8 = 120 addresses)
Subnet C: 214.97.254.128/25 (128 addresses)

Subnet D: 214.97.254.0/31 (2 addresses)
Subnet E: 214.97.254.2/31 (2 addresses)
Subnet F: 214.97.254.4/30 (4 addresses)

b) To simplify the solution, assume that no datagrams have router interfaces as ultimate destinations. Also, label D, E, F for the upper-right, bottom, and upper-left interior subnets, respectively.

Router 1

Longest Prefix Match	**Outgoing Interface**
11010110 01100001 11111111	Subnet A
11010110 01100001 11111110 0000000	Subnet D
11010110 01100001 11111110 000001	Subnet F

Router 2

Longest Prefix Match	**Outgoing Interface**
11010110 01100001 11111111 0000000	Subnet D
11010110 01100001 11111110 0	Subnet B
11010110 01100001 11111110 0000001	Subnet E

Alternative Answer (Group 10): Please verify!

Router2
Subnet D should be 11010110 01100001 11111110 00000000

Router3
11011000 01100001 11111110 1 Subnet C
11010110 01100001 11111110 00000001 Subnet E
11010110 01100001 11111110 000001 Subnet F

Question 11.
What are the

a. Private networks addresses,
b. Link-local addresses

Where are they used?

Answer (Group 2):
In the Internet addressing architecture, a private network is a network that uses private IP address space. Both, the IPv4 and the IPv6 specifications define private addressing ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Private IP address spaces were originally defined in an effort to delay IPv4 address exhaustion.

Private network addresses are not allocated to any specific organization and anyone may use these addresses without approval from a regional Internet registry. However, IP packets addressed from them cannot be routed through the public Internet.

In a computer network, a link-local address is a network address that is valid only for communications within the network segment or the broadcast domain that the host is connected to. Link-local addresses are most often assigned automatically through a process known as stateless address autoconfiguration or link-local address autoconfiguration.
Link-local addresses are not guaranteed to be unique beyond their network segment, therefore routers do not forward packets with link-local addresses.
Link-local addresses for IPv4 are defined in the address block 169.254.0.0/16 in CIDR notation. In IPv6, they are assigned the address block fe80::/10.

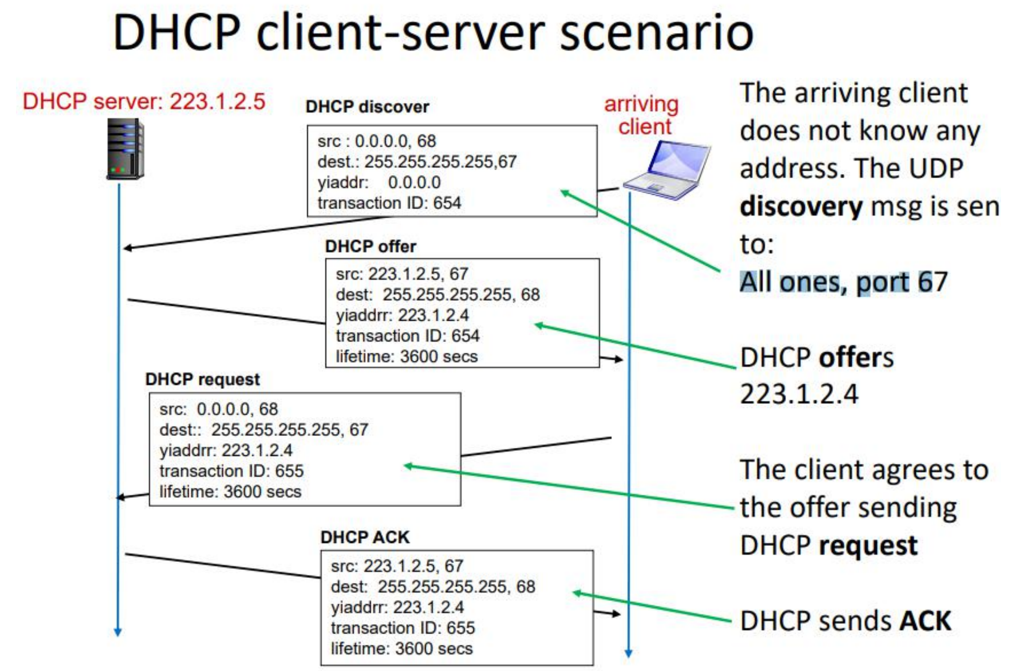
Question 12.
Describe the DHCP protocol. Use an example to demonstrate the main steps of the protocol

Answer (Group 3):
DHCP is built on server-client model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.
Suppose one client host wants to join a network, there will be four main steps:
the client broadcasts a DHCPDISCOVER message, which may include options that suggest values for the network address and lease duration. every host will receive this message, but only DHCP server will respond.

Each server may respond with a DHCPOFFER message that includes an available network address in the 'yiaddr' field (and other configuration parameters in DHCP options).

The client receives one or more DHCPOFFER messages from one or more servers, and client will only choose one server. The client broadcasts a DHCPREQUEST message to request configuration parameters from chosen server and tell other server it will not accept any other offer.

The chosen server responds with a DHCPACK message containing the configuration parameters for the requesting client. Other servers consider the DHCPREQUEST message as a rejection.



DHCP client-server scenario

DHCP discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

The arriving client does not know any address. The UDP **discovery** msg is sen to:
All ones, port 67

DHCP **offers** 223.1.2.4

The client agrees to the offer sending DHCP **request**

DHCP sends **ACK**

In this scenario:

Step1: Client broadcast a DHCP discover.

Src: port	0.0.0.0:68.
Dest: port	255.255.255.255:67

Step2: all server in the network will receive the DHCP discover. Only DHCP server will answer. In this scenario, DHCP server at 223.1.2.5 broadcast a DHCP offer with an available IP address in yiaddr(223.1.2.4).

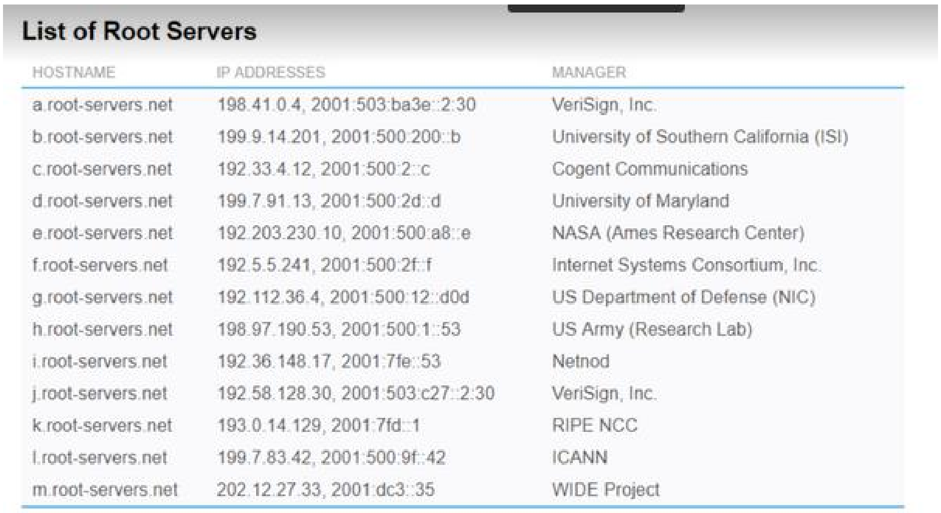
Step3: client broadcast the DHCP request and refuse other DHCP offer from other DHCP server.

Step4: DHCP server agree the request and broadcast a DHCP ack.

Question 13.
Where are the DNS root servers? (Slide 39)

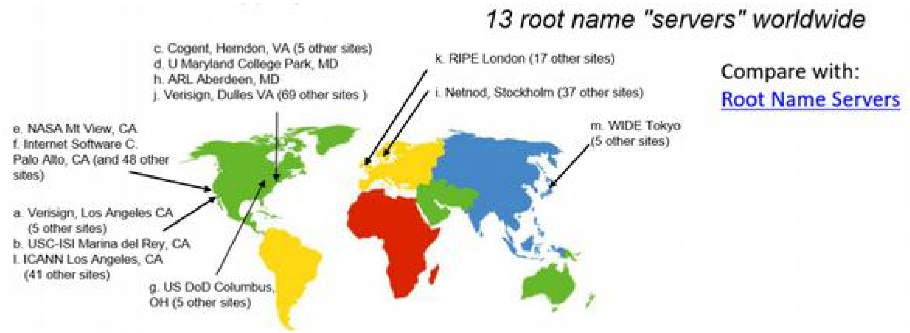
Go to: **http://root-servers.org** and http://www.iana.org/domains/root/servers **a**nd compile a short answer

Answer (Group 4):



List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project


13 root name "servers" worldwide
c. Cogent, Herndon, VA (5 other sites)
d. U Maryland College Park, MD
h. ARL Aberdeen, MD
j. Verisign, Dulles VA (69 other sites)
k. RIPE London (17 other sites)
i. Netnod, Stockholm (37 other sites)
Compare with:
Root Name Servers
e. NASA Mt View, CA
f. Internet Software C.
Palo Alto, CA (and 48 other sites)
m. WIDE Tokyo
(5 other sites)
a. Verisign, Los Angeles CA
(5 other sites)
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA
(41 other sites)
g. US DoD Columbus, OH (5 other sites)

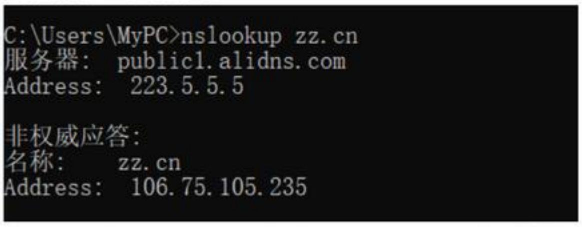
The root server is mainly used to manage the home directory of the Internet. There are only 13 root servers in the world, and one is the main root server in the United States. The remaining 12 are secondary root servers, 9 of which are in the United States, two in Europe, in the United Kingdom and Sweden, and one in Asia in Japan.
But I believe that there will be more DNS root servers in the world in the future.

Question 14.
Open the command window and practice using **nslookup** command

e.g.

```
app> nslookup  zz.cn
Server:  ns1.its.monash.edu.au
Address:  130.194.1.99
Non-authoritative answer:
Name:    zz.cn
Address:  211.100.61.67
```

Answer (Group 4):



```
C:\Users\MyPC>nslookup zz.cn
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
名称:    zz.cn
Address:  106.75.105.235
```

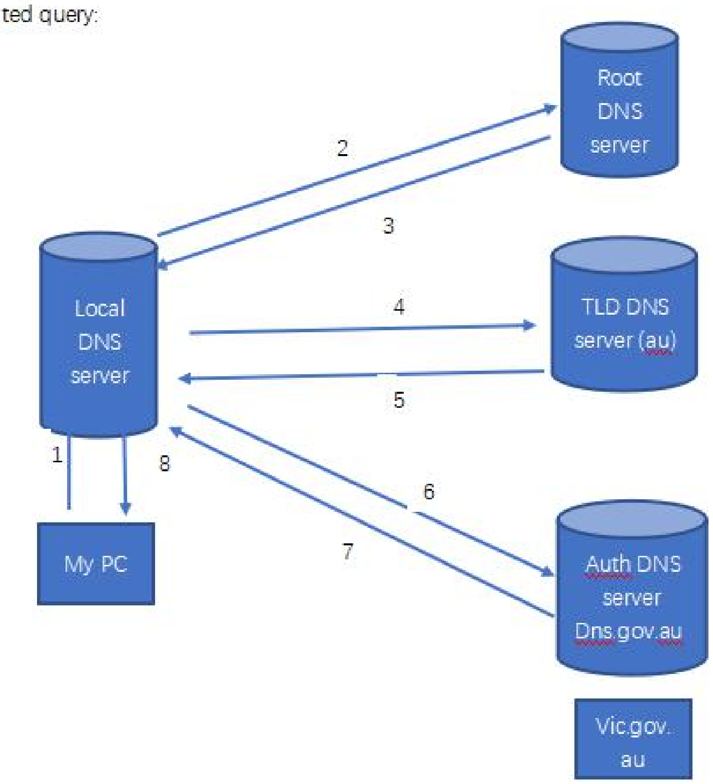
Nslookup (name server lookup) is used to query the DNS records, check whether the domain name resolution is normal, and use it to diagnose network problems when the network is faulty. From this we know the list of IP addresses of the zz.cn server group.

Question 15.

Assume that you try to access **vic.gov.au** and your local DNS server does not know the IP address. Draw diagrams similar to that in slides 42, 43 and 44 to demonstrate how the name resolution works using both the **iterated** and **recursive** query.

Answer (Group 5):

the iterated query:



1. My PC try to get access to URL= vic.gov.au and this URL => IP not in my address table. Then my PC sends DNS request to the local DNS server and URL => IP not available

2. Local server sends DNS request to the root server to get .au DNS server

3. Root DNS server knows the IP and return it to Local DNS server

4. Local server sends DNS request to the .au root server to get .gov.au DNS server

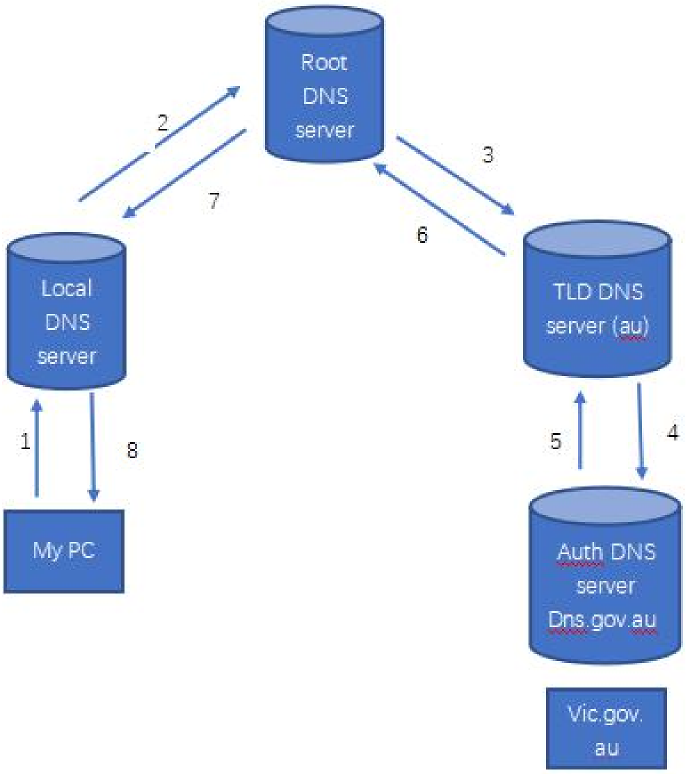
5. .au DNS server sends the IP back to the Local server

6. Local server sends DNS request to the .gov.au root server to get IP of vic.gov.au

7. .gov.au DNS server sends the IP back to the Local server

8. Local DNS server sends the IP back to the client computer

recursive query:



1. My PC try to get access to URL= vic.gov.au and this URL => IP not in my address table. Then my PC sends DNS request to the local DNS server and URL => IP not available

2. Local server sends DNS request to the root server to get IP of vic.gov.au

3. Root DNS server sends DNS request to the .au server to get IP of vic.gov.au

4. .au DNS server sends DNS request to the .gov.au server to get IP of vic.gov.au

5. .gov.au DNS server sends the IP back to the .au DNS server

6. .au DNS server sends the IP back to the root DNS server

7. Root DNS server sends the IP back to the local DNS server

8. Local DNS server sends the IP back to my PC

Wireshark: DHCP Experiment (optional)

In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). Enter "*ipconfig /release*". This command releases your current IP address, so that your host's IP address becomes : 0.0.0.0
2. Start up the Wireshark and begin packet capture.
3. Now go back to the Windows Command Prompt and enter "*ipconfig /renew*". This instructs your host to obtain a network configuration, including a new IP address e.g. 192.168.1.108
4. Wait until the "*ipconfig /renew*" has terminated. Then enter the same command "*ipconfig /renew*" again.
5. When the second *"ipconfig /renew"* terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
6. Finally, enter "*ipconfig /renew*" to again be allocated an IP address for your computer.
7. Stop Wireshark packet capture.

If you have problems with the recording the above wireshark traces, you can use pre-recorded **dhcp-ethereal-trace-1.pcap** available on Moodle.

Now let's take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter "bootp" and not "dhcp" in the filter.) We can see that the first *ipconfig* renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?
3. What is the link-layer (e.g., Ethernet) address of your host?
4. What values in the DHCP discover message differentiate this message from the DHCP request message?
5. What is the value of the Transaction-ID in each of the first four

(Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

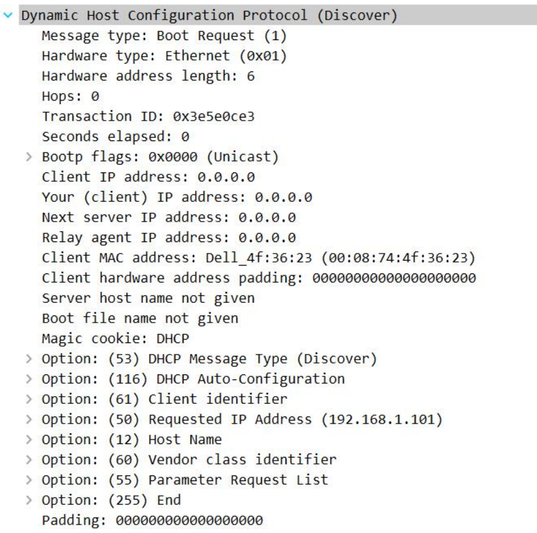
6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
7. What is the IP address of your DHCP server?
8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?
10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?
12. Explain the purpose of the lease time. How long is the lease time in your experiment?
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
14. Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets

Answers (Group 1):

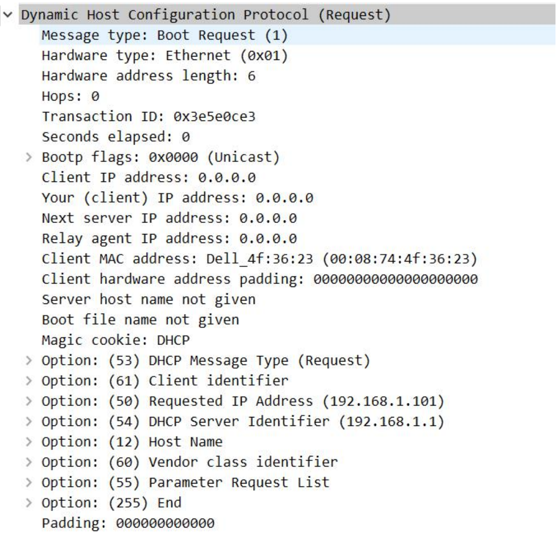
1. UDP

3. 00:08:74:4f:36:23

4. [See next page]



```
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    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: Dell_4f:36:23 (00:08:74:4f:36:23)
    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: (116) DHCP Auto-Configuration
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.101)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000000000
```



```
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    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: Dell_4f:36:23 (00:08:74:4f:36:23)
    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: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.101)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000
```

Option: (53) DHCP Message Type (**Discover**)   Option: (53) DHCP Message Type (**Request**)

Option: (116) DHCP Auto-Configuration   NULL

NULL   Option: (54) DHCP Sever Identifier (192.168.1.1)

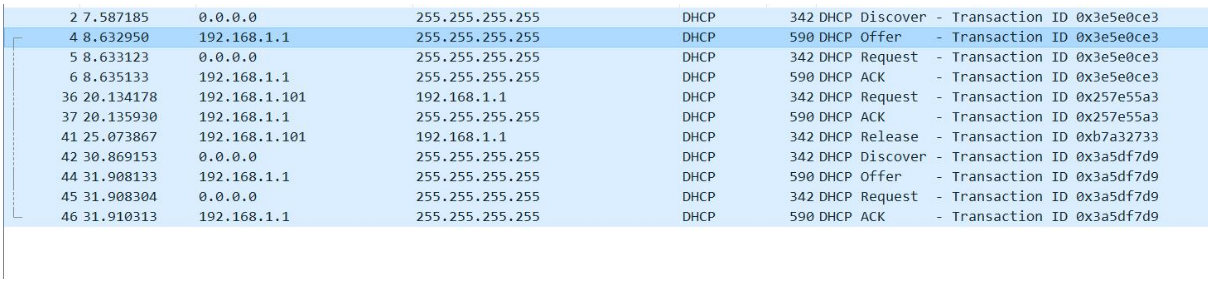
5. Transaction-ID of the first four messages (Discover/Offer/Request/ACK) is 0x3e5e0ce3.

   The Transaction-ID of the second set is 0x257e55a3

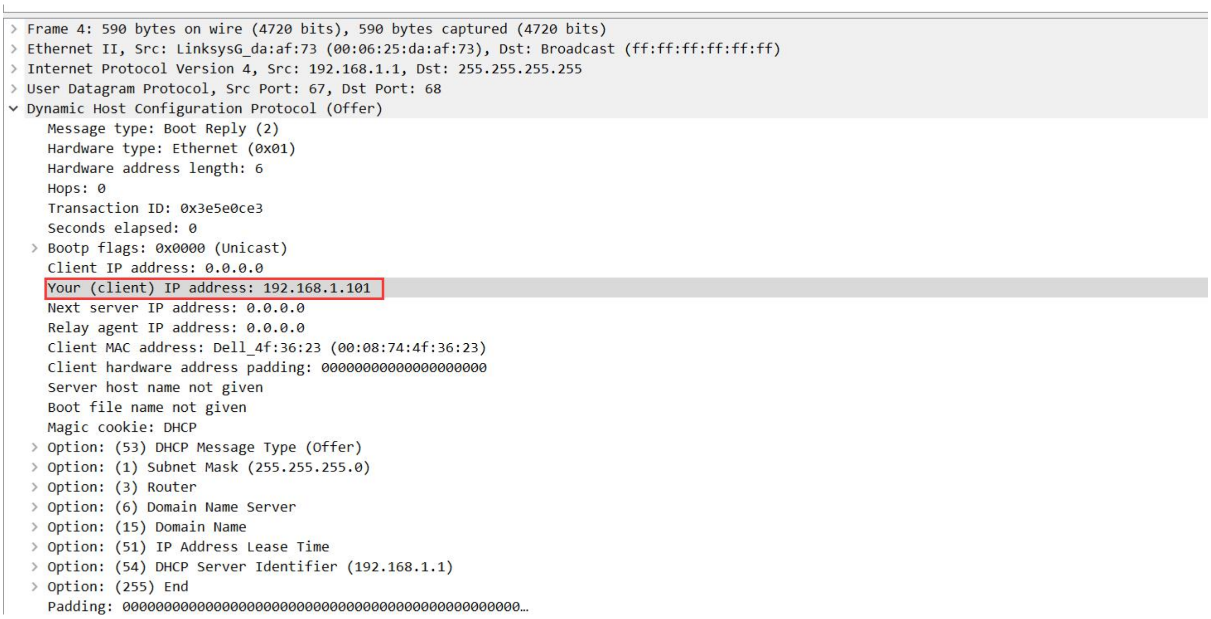
   Because the DHCP protocol is based on UDP, it is connectionless. And the client does not know the DHCP server's address, so the client broadcasts the DHCP discovery to look for the server. While the server can not ack the info to the client before it has an IP address, the server will broadcast the info, too. the Transaction-ID is designed for client and server to identify the corresponding context and get the corresponding info.

7. 192.168.1.1

8. 192.168.1.101. The first Offer indicates the offered DHCP address.



```
 2 7.587185   0.0.0.0         255.255.255.255   DHCP   342 DHCP Discover - Transaction ID 0x3e5e0ce3
 4 8.632950   192.168.1.1     255.255.255.255   DHCP   590 DHCP Offer    - Transaction ID 0x3e5e0ce3
 5 8.633123   0.0.0.0         255.255.255.255   DHCP   342 DHCP Request  - Transaction ID 0x3e5e0ce3
 6 8.635133   192.168.1.1     255.255.255.255   DHCP   590 DHCP ACK      - Transaction ID 0x3e5e0ce3
36 20.134178  192.168.1.101   192.168.1.1       DHCP   342 DHCP Request  - Transaction ID 0x257e55a3
37 20.135930  192.168.1.1     255.255.255.255   DHCP   590 DHCP ACK      - Transaction ID 0x257e55a3
41 25.073867  192.168.1.101   192.168.1.1       DHCP   342 DHCP Release  - Transaction ID 0xb7a32733
42 30.869153  0.0.0.0         255.255.255.255   DHCP   342 DHCP Discover - Transaction ID 0x3a5df7d9
44 31.908133  192.168.1.1     255.255.255.255   DHCP   590 DHCP Offer    - Transaction ID 0x3a5df7d9
45 31.908304  0.0.0.0         255.255.255.255   DHCP   342 DHCP Request  - Transaction ID 0x3a5df7d9
46 31.910313  192.168.1.1     255.255.255.255   DHCP   590 DHCP ACK      - Transaction ID 0x3a5df7d9
```



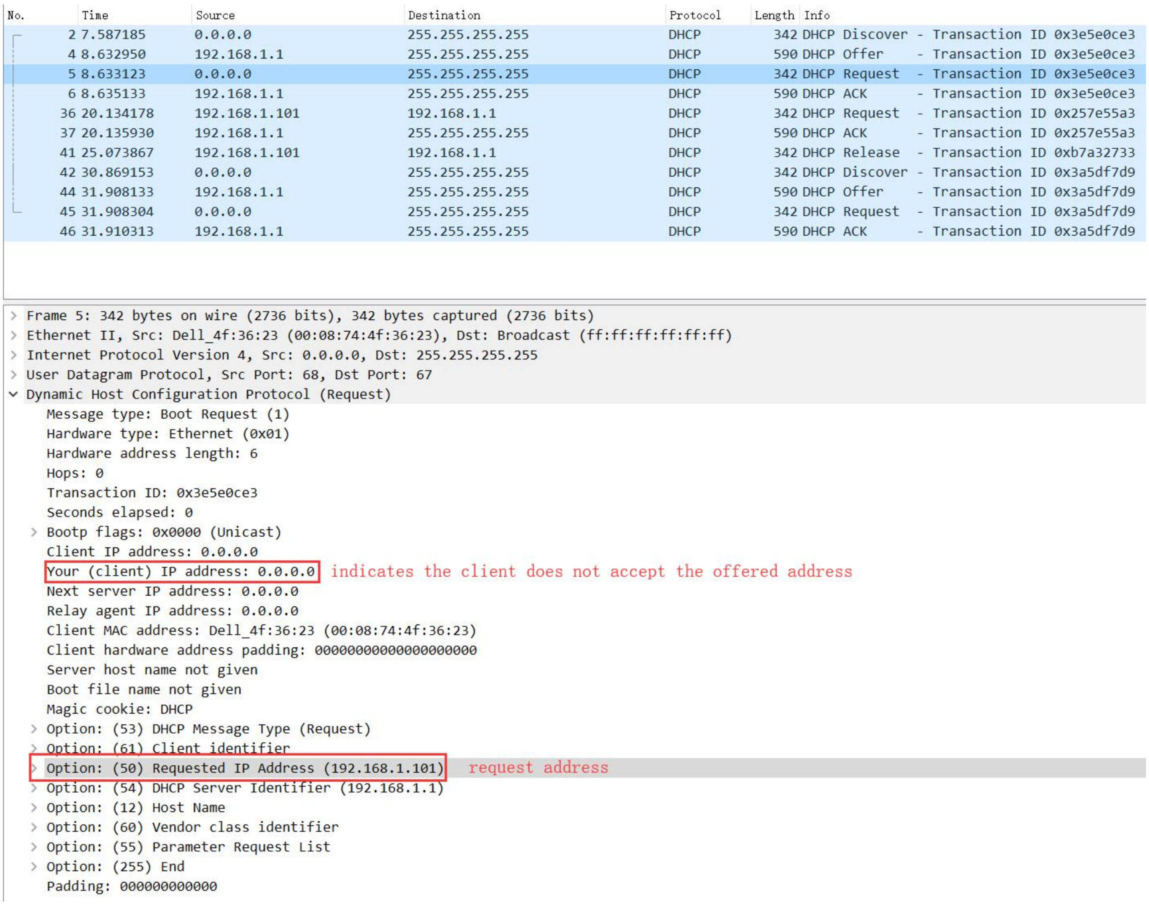
```
> Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    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: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (51) IP Address Lease Time
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

9. “Relay agent IP address: 0.0.0.0”. This indicates the absence of a relay agent.

No

10. To notify the client the net id and the router is the DHCP server.

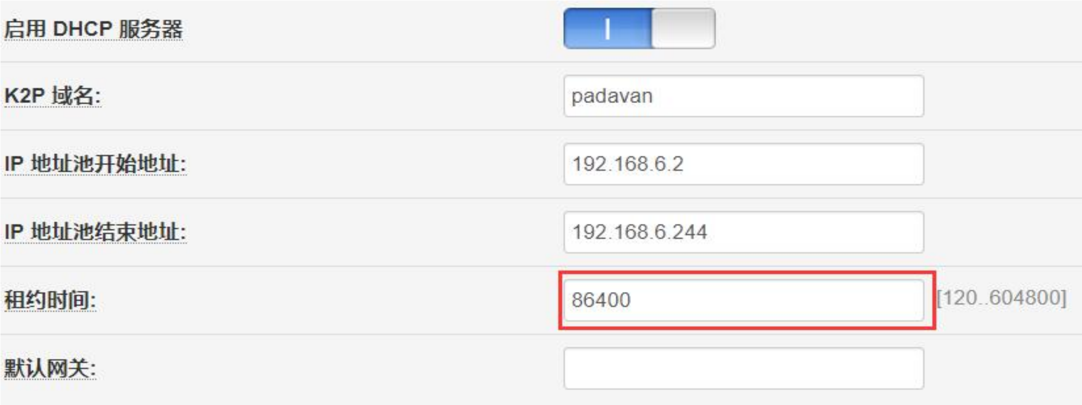
11. No.



```
No.   Time        Source          Destination        Protocol  Length Info
    2 7.587185    0.0.0.0         255.255.255.255    DHCP         342 DHCP Discover - Transaction ID 0x3e5e0ce3
    4 8.632950    192.168.1.1     255.255.255.255    DHCP         590 DHCP Offer    - Transaction ID 0x3e5e0ce3
    5 8.633123    0.0.0.0         255.255.255.255    DHCP         342 DHCP Request  - Transaction ID 0x3e5e0ce3
    6 8.635133    192.168.1.1     255.255.255.255    DHCP         590 DHCP ACK      - Transaction ID 0x3e5e0ce3
   36 20.134178   192.168.1.101   192.168.1.1        DHCP         342 DHCP Request  - Transaction ID 0x257e55a3
   37 20.135930   192.168.1.1     255.255.255.255    DHCP         590 DHCP ACK      - Transaction ID 0x257e55a3
   41 25.073867   192.168.1.101   192.168.1.1        DHCP         342 DHCP Release  - Transaction ID 0xb7a32733
   42 30.869153   0.0.0.0         255.255.255.255    DHCP         342 DHCP Discover - Transaction ID 0x3a5df7d9
   44 31.908133   192.168.1.1     255.255.255.255    DHCP         590 DHCP Offer    - Transaction ID 0x3a5df7d9
   45 31.908304   0.0.0.0         255.255.255.255    DHCP         342 DHCP Request  - Transaction ID 0x3a5df7d9
   46 31.910313   192.168.1.1     255.255.255.255    DHCP         590 DHCP ACK      - Transaction ID 0x3a5df7d9
```

```
> Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), 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
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0  indicates the client does not accept the offered address
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    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: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.101)  request address
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000
```

12. The duration for which a DHCP server loans an IP address to a DHCP client. In my router configuration, the DHCP lease is 86400s, a day.



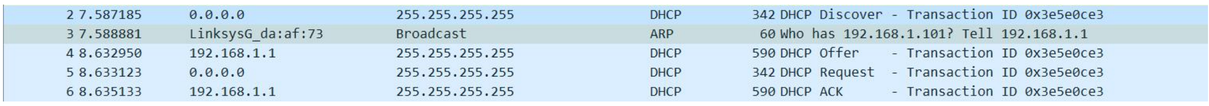
启用 DHCP 服务器	ON
K2P 域名:	padavan
IP 地址池开始地址:	192.168.6.2
IP 地址池结束地址:	192.168.6.244
租约时间:	86400 [120..604800]
默认网关:	

13. To notify the server the client is leaving now, and the assigned address can be recycled.

Yes, the server issues the release request, but does not respond to any message. In the following trace, we can see the server allocate the IP 192.168.1.101 again. This behavior shows the server indeed issued the release request.

If the release message is lost, the server will hold the assigned IP until the DHCP Lease is finished, and then release the IP and the server resource.

14.



```
    2 7.587185    0.0.0.0              255.255.255.255        DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
    3 7.588881    LinksysG_da:af:73    Broadcast              ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
    4 8.632950    192.168.1.1          255.255.255.255        DHCP      590 DHCP Offer    - Transaction ID 0x3e5e0ce3
    5 8.633123    0.0.0.0              255.255.255.255        DHCP      342 DHCP Request  - Transaction ID 0x3e5e0ce3
    6 8.635133    192.168.1.1          255.255.255.255        DHCP      590 DHCP ACK      - Transaction ID 0x3e5e0ce3
```

After the first DHCP discovery message, the router broadcast a ARP request to ensure there is no device in the network configured IP 192.168.1.101. Then the router offers the IP to the client.