Christopher Bazyani

Practical Cyber Security

Unit 3

Packet Sniffing – DHCP

**Capture a Trace**

Opening the supplied pcap file

Graphical user interface, text, application

Description automatically generated

**Inspect the Trace**

Looking at the third packet containing the DHCP exchange and exploring the bootstrap/DHCP protocol

Graphical user interface, application, Word

Description automatically generated

**Details of the DHCP messages**

**1. What are the two values of the BOOTP Message Type field?**

Boot Request (1) and Boot Reply (2)





**2. How long is the Transaction ID field? Say whether it is likely that concurrent DHCP operations done by different computers will happen to pick the same Transaction ID.**

It is 4 bytes long and there will be a collision in a relatively small number of DHCP operations until the number approaches 216.



**3. What is the name of the field that carries the IP address that is being assigned to the client? You will find this field filled in on the DHCP Ack, as that message is completing the assignment.**

It is the clients IP address field that carries the IP address being leased to the client.

Text

Description automatically generated

**4. What is the value of the Magic Cookie that stands for DHCP?**

0x63825363

Calendar

Description automatically generated

5. The first DHCP option is DHCP Message Type. What option value stands for this type?

Option value of 53 stands for DHCP Message Type.



**6. DHCP Requests will typically have a Client Identifier option. Look at the value of this option. How does it identify the client? Take a guess.**

Client Identifier to carry the Ethernet address of the client, but possible to use some other kind of identifier.

A screenshot of a text message

Description automatically generated with low confidence

**7. DHCP Acks will typically have a Server Identifier option. Look at the value of this option. How does it identify the server? Take a guess.**

Server Identifier to carry the IP address of the DHCP server.

A picture containing text

Description automatically generated

**8. What option value stands for the Requested IP Address option? And for the IP Address Lease. Time option?**

50 stands for Requested IP Address and the value of 51 stands for IP Address Lease Time.

A picture containing text

Description automatically generated

Text

Description automatically generated with low confidence

**9. How does the recipient of a DHCP message know that it has reached the last option?**

DHCP options is identified with a DHCP option called End with value 255.



**DHCP Message Addressing**

**1. What port number does the DHCP client use, and what port number does the DHCP server use? Ports matter because UDP messages are addressed using ports. Both of these port numbers are on the Request in the source and destination port fields (and you will also see them on the Ack).**

My computer uses UDP port 68 and the DHCP server uses UDP port 67.

Graphical user interface, text, application, chat or text message

Description automatically generated

**2. What source IP address is put on the Request message? It is a special value meaning “this host on this network” used for initialization.**

Source IP address is 0.0.0.0 and is a special address used during address initialization.



**3. What destination IP address is put on the Request message? It is also a reserved value designed to reach the DHCP server wherever it is on the local network.**

The destination IP address is 255.255.255.255. It is the broadcast address, which means the message is intended for all computers on the network.



**4. What source Ethernet address is put on the Request message, and what destination Ethernet address is put on the Request message? One of these addresses is a reserved address.**

Source Ethernet address is my computer’s Ethernet address, since that is already assigned to my NIC. The destination Ethernet address is ff:ff:ff:ff:ff:ff, the reserved broadcast Ethernet address, so that the packet reaches all computers on the local network.

A picture containing text

Description automatically generated

**5. How does a computer work out whether a DHCP message it receives is intended as a reply to its DHCP Request message, and not a reply to another computer? Hint: if you are not sure then go over the fields you inspected previously in Step 2 above.**

The Transaction ID for all DHCP messages in a single exchange is the same. As a result, a device searches for an Ack with a Transaction ID that fits the value it assigned to the earlier DHCP message, such as a Request.