Packets on the Network

Reading

30 minutes

Status | Incomplete

Introduction

We have spent some time exploring the makeup of a packet (the package that we use to send our user data across a network) from a theoretical perspective by detailing how we handle and wrap our user data at each layer of the OSI model.

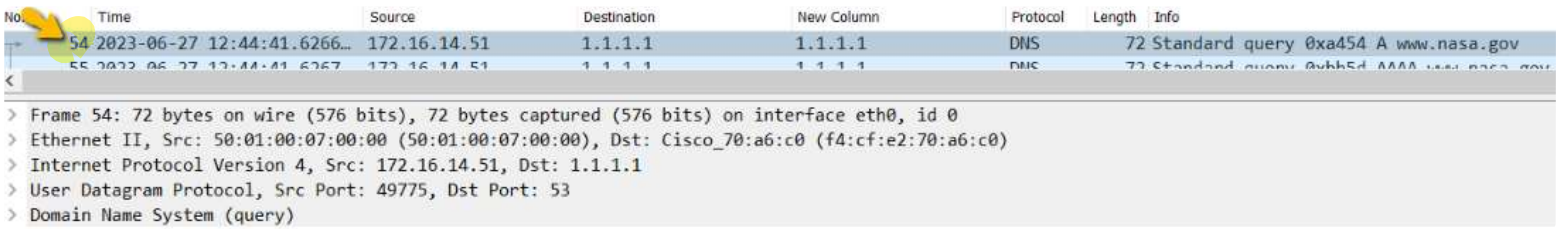
Now, let's look at how we can use this to help us understand what we see when we look at packets that we capture using a network sniffer software like Wireshark.

Reading

We are going to start by looking at a packet that has been created as part of a DNS request to view a website because the DNS protocol is a Layer 7 protocol and we will be able to investigate data that is associated with the most layers of the OSI model.

Note: A protocol in networking is a set of rules for formatting and processing data. You can think of it as a common language that computers use for communication. The DNS protocol stands for domain name system, and it allows computers to convert domain names like google.com to an IP address. This is why you can enter a domain name like facebook.com into a web browser, and your computer is able to find a web server associated with that domain.

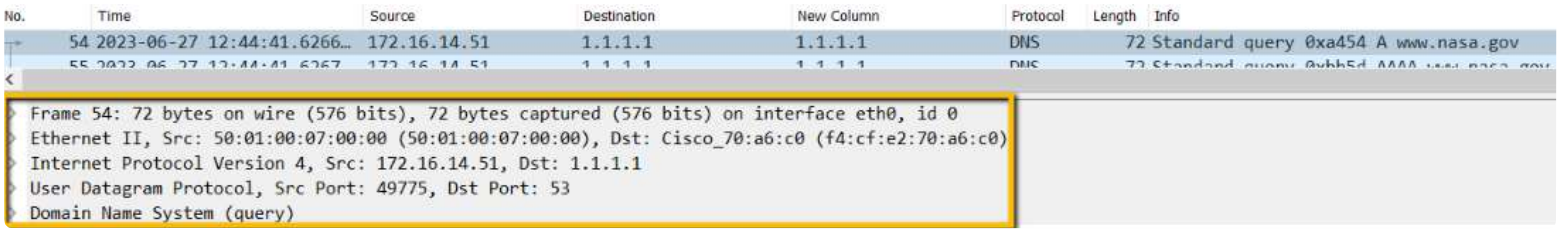
If DNS did not exist, you wouldn't actually be able to enter www.google.com and be taken there, you would have to remember Google's IP address and browse to that to get to Google's website instead. Converting a domain name to IP address is the purpose of DNS.



In this screen capture, we can see that we are looking at packet # 54. Let's start by getting some basics of the packet in question:

- **Time**: 2023-06-27 12:44 (captured on June 27, 2023 at 12:44pm)
- **Source**: 172.16.14.51 (the IPv4 address on the sending computer)
- **Destination**: 1.1.1.1 (the IPv4 address on the receiving computer)
- **Protocol**: DNS (this is a DNS request to get the IP address of the machine that is hosting a particular website)
- **Length**: 72 bytes (how long the packet is)
- **Info**: requesting an A record for the website 'www.nasa.gov' (looking for the IP address to go to the Nasa website)

This is already quite a lot of information regarding the purpose and content of this particular packet, and we got it all from the summary information that Wireshark has provided us with in our upper columns of data. Now, let's dive deeper by looking at the information available on the bottom portion of our screen. There are five sections to the data packet we are analyzing.



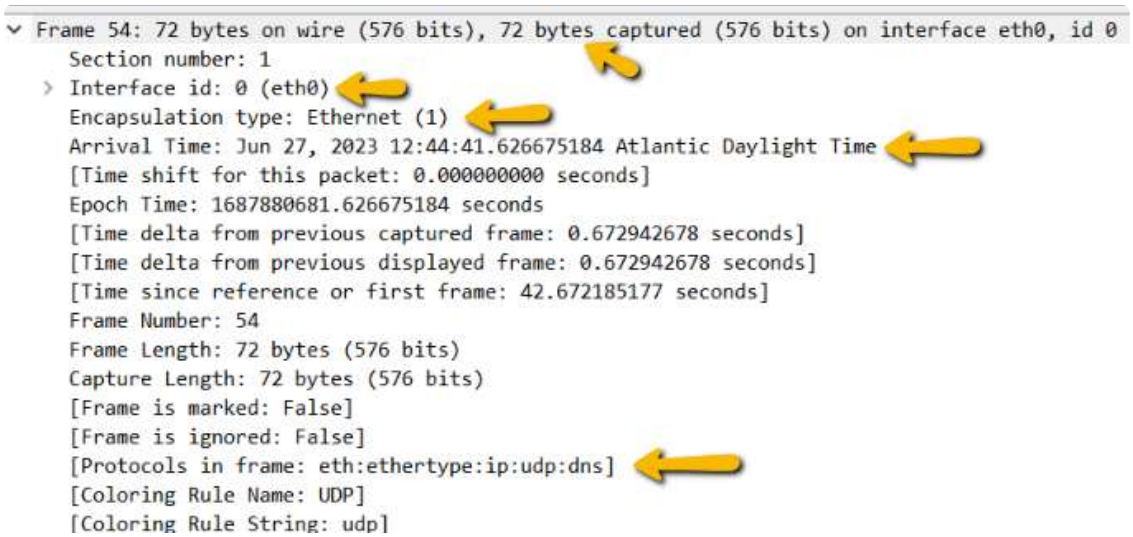
We will look at this content one section at a time in a little more detail, but first, let's look at it altogether. Each line represents a different set of information.

First thing to notice is the category headings:

Note: PDU = protocol data unit, a subsection of the overall data packet.

- **Frame**: *Layer 2 PDU* particulars, including a general description of the packet in question
- **Ethernet**: *Layer 2 PDU* protocol and its particulars, including MAC addresses for source and destination
- **Internet Protocol**: *Layer 3 PDU* protocol and its particulars, including IP addresses for source and destination
- **User Datagram Protocol**: *Layer 4 PDU* protocol (UDP) and its particulars, including port numbers
- **Domain Name System**: *Layer 7 PDU* protocol (DNS) and its particulars, including user data sent by the computer browser

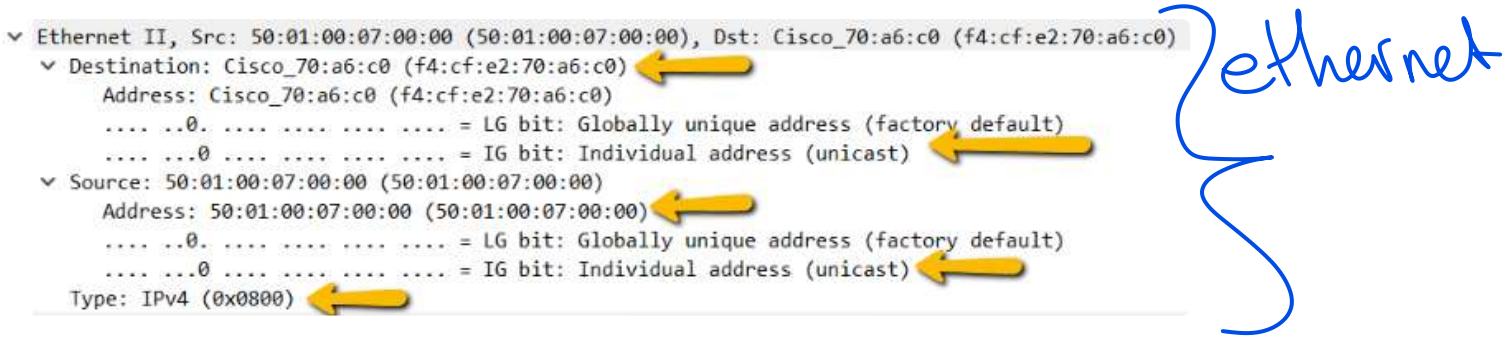
Now let's dive in a little deeper and look at some of the details in each category from above. We won't go over all of the details in every category, but there are a few items we may find useful later on that we can see. Let's take a look.



Frame category

Under the Frame category, we can see the following:

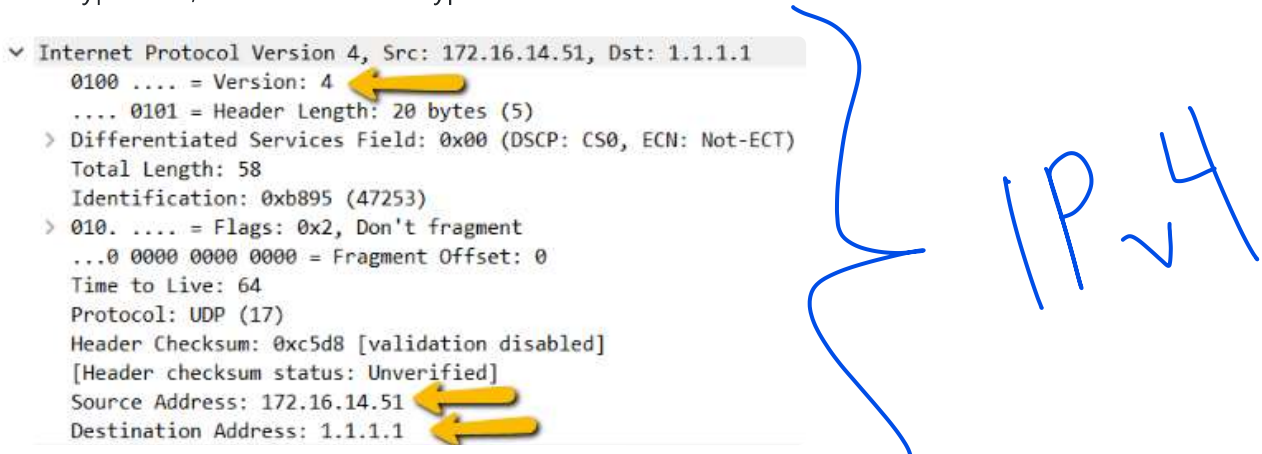
- Frame size, 72 bytes
- Interface id of the interface it was captured on, ***eth0*** (An interface is simply a component of the computer that allows it to connect to a network. One computer can have multiple interfaces, so this shows which interface is being used for this communication.)
- The encapsulation protocol at Layer 2, Ethernet
- The date and time it arrived on the interface and the timezone of the machine
- Protocols that are seen in this frame, Ethernet, IP, UDP, and DNS



Ethernet Category

Under the Ethernet category, we can see the following:

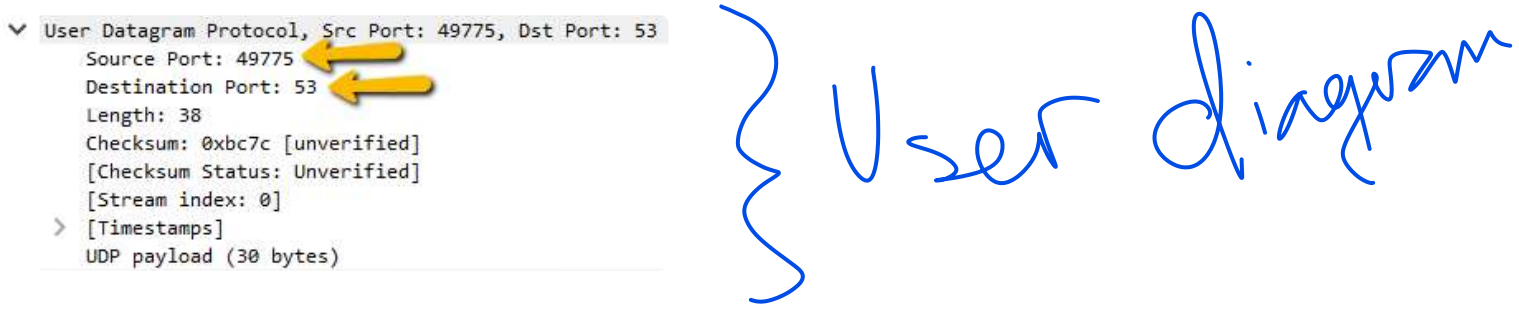
- Destination MAC address, (Remember, MAC addresses are used for local communications only, so this MAC address would be for the device in the immediate segment of the network that would be the next stop for the packet as it travels from the sending device toward the eventual intended receiving device)
- The second arrow points to a line specifying that it is unicast, this simply means that the destination MAC Address refers to a single interface (unique). The opposite would be anycast, which is a set of MAC Addresses
- Source MAC address, this is the MAC address for the immediate sending device, in this case, the originating source of the packet
- The next arrow shows that the Source MAC Address is also unicast. This means both MAC addresses are unicast, meaning they identify a single device each
- Type: IPv4, this identifies the type of IP address in use.



Internet Protocol Category

Under the Internet Protocol category, we can see the following:

- The version of IP being used, in this case, version 4
- Source address, of the sending machine
- Destination address, of the eventual receiving machine



Layer 4 User Datagram Protocol Category

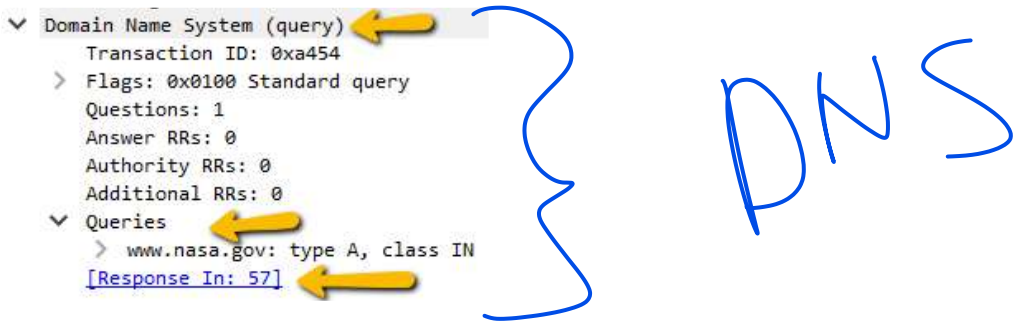
Under the Layer 4 User Datagram Protocol category, we can see the following:

- Source Port: the port that identifies the specific conversation and software associated with this conversation on the source device
- Destination Port: the port that identifies the specific software and individual conversation associated with this packet on the destination device

Note: You can think of a computer port as an entry point on the system. While an IP address identifies that computer system a message should be going to, a port number identifies the exact entry point that the message should be sent to (similar to how boats must dock at a particular port, computer messages must be sent to and from identified computer ports). For example, in this communication, the message is being sent from the device 172.16.14.51 from it's port 49775 and it's being sent to the device 1.1.1.1 on that device's port 53.

It's also important to note that each port typically responds to a specific type of service, for example, port 53 is typically used for DNS. Other common examples are port 80 which is typically used for http messages, and port 443 which is typically used for https. Every message will include a source and destination IP Address and their associated port numbers!

These are important because an IP address and a port number, together, identify a single conversation, or interchange, that is taking place on a specific device. This is called a socket. 2 Sockets, that's two combinations of an IP address and port number, identify a whole conversation, including the 2 devices participating in it.



Domain Name System Category

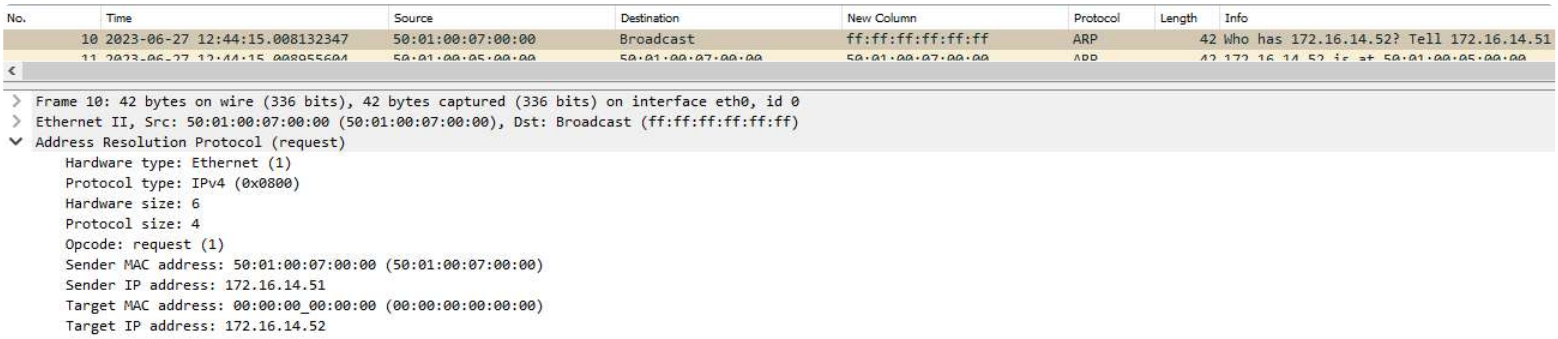
Under the Domain Name System category, we can see the following:

- The protocol at Layer 7 that is responsible for the User Data contained in the packet, in this case DNS. We can also see that is a query and not a response. Which means this message is requesting information from a DNS server related to a specific domain name.

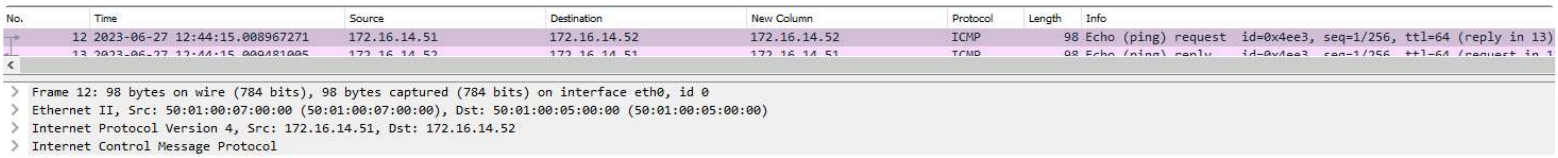
- The actual query that has been sent, in this case, a query to get the Type A record for the 'www.nasa.gov' website. This is a request to find the IP address for the 'www.nasa.gov' website
- What packet number (in Wireshark) the response to this request is found in, in this case, packet number 57

In the case of packet 54 that we have investigated in this example, because it carries the DNS protocol information, and DNS is a layer 7 protocol, we see header and user data from all the layers we have discussed. However, if the protocol that is the focus of the packet we are investigating is associated with layer 3 or 2, we would see fewer categories to investigate, as can be seen in the following examples.

ARP is a protocol that is associated with Layers 2 and 3 of the OSI model and is used by devices to learn the MAC address that is associated with a particular IP address that they wish to send information to.



ICMP is a protocol that is associated with Layer 3 of the OSI model and is used to aid in communicating traffic status information across the network. One of the types of traffic status that it is able to communicate is through the use of a ping, or echo request and reply, which will inform us of how long it takes for a request to travel across the network and a reply to get back. The longer this process takes, the more latency, or delay, there is that is being experienced on the network.



There are many protocols like these that are normally seen on our networks all the time. They are used for everyday tasks that make it possible for us to send communications reliably across our networks. The trick is to be able to identify when they are being used for normal network communication tasks, and when they are being used for other purposes that may support or aid a bad actor to achieve their nefarious goals.

Conclusion

Next, we will dive deeper into IP addresses and how to interpret and work with them.

✓ Mark Completed

Previous
Encapsulation Process Demonstration

Next
IP Addresses: Intro to IPv4

W01D2

Tue Jun 25

Lectures (1)

Work (15)

8 hrs + *1 hr stretch*

- Managing Linux Processes ✓
- *Fork vs Exec*
- *Adjusting Process Priority*
- Managing Linux Software ✓
- Linux Processes and Software ✓
- OSI layer models ✓
- The Encapsulation Process ✓
- Encapsulation Process Demonstration ✓
- Packets on the Network
- IP Addresses: Intro to IPv4
- IP Addresses: Intro to IPv6
- The Value of Group Work! ✓
- Addressing Scheme ✓
- AI Literacy Pre-Assessment ✓
- Introduction to AI ✓

W01D2 Schedule »