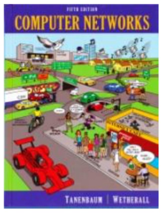
ICT1010 - Computer Networks

Lab Exercise – UDP



Objective

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss tolerating connections between applications on the Internet. Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. Both protocols send short packets of data, called datagrams. To look at the details of UDP (User Datagram Protocol). UDP is a transport protocol used throughout the Internet as an alternative to TCP when reliability is not required. UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. TCP has emerged as the dominant protocol used for the bulk of Internet connectivity owing to services for breaking large data sets into individual packets, checking for and resending lost packets and reassembling packets into the correct sequence. But these additional services come at a cost in terms of additional data overhead, and delays called latency.

In contrast, UDP just sends the packets, which means that it has much lower bandwidth overhead and latency. But packets can be lost or received out of order as a result, owing to the different paths individual packets traverse between sender and receiver. UDP is an ideal protocol for network applications in which perceived latency is critical such as gaming, voice and video communications, which can suffer some data loss without adversely affecting perceived quality. IWe will examine UDP in this lab.

Step 1: Capture a UDP Trace

There are many ways to cause your computer to send and receive UDP messages since UDP is widely used as a transport protocol. The easiest options are to:

- Do nothing but wait for a while. UDP is used for many “system protocols” that typically run in the background and produce small amounts of traffic, e.g., DHCP for IP address assignment and NTP for time synchronization.
- Use your browser to visit sites. UDP is used by DNS for resolving domain names to IP addresses, so visiting fresh sites will cause DNS traffic to be sent. Be careful not to visit unsafe sites; pick recommended sites or sites you know about but have not visited recently. Simply browsing the web is likely to cause a steady stream of DNS traffic.
- Start up a voice-over-IP call with your favorite client. UDP is used by RTP, which is the protocol commonly used to carry media samples in a voice or video call over the Internet.

1. Launch Wireshark by entering *Wireshark* in the *"ask my anything"* search box in Windows.

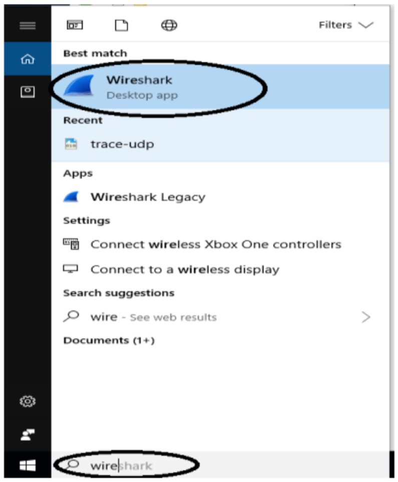
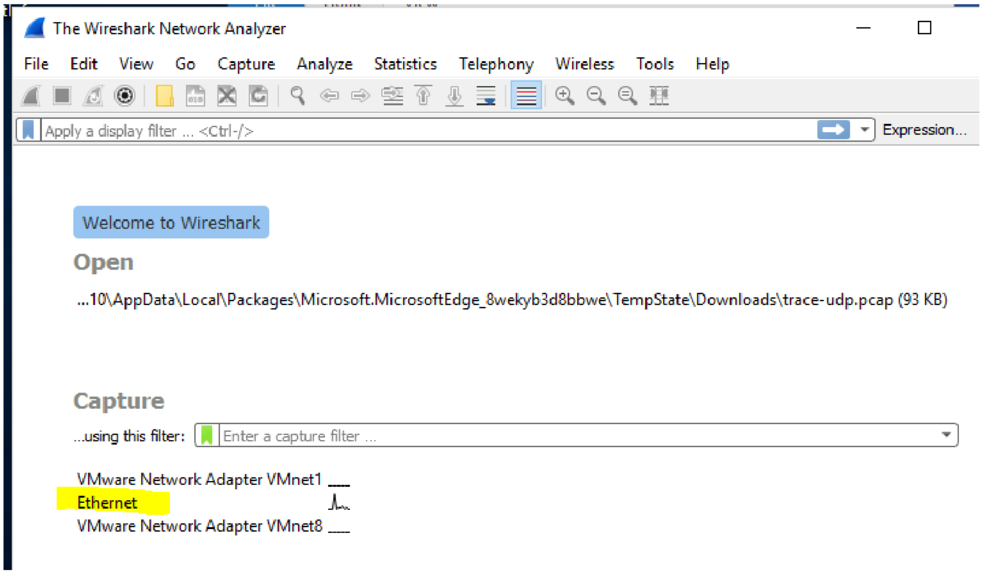


Figure 1: Starting Wireshark

2. Once Wireshark starts, select the *Ethernet interface.*

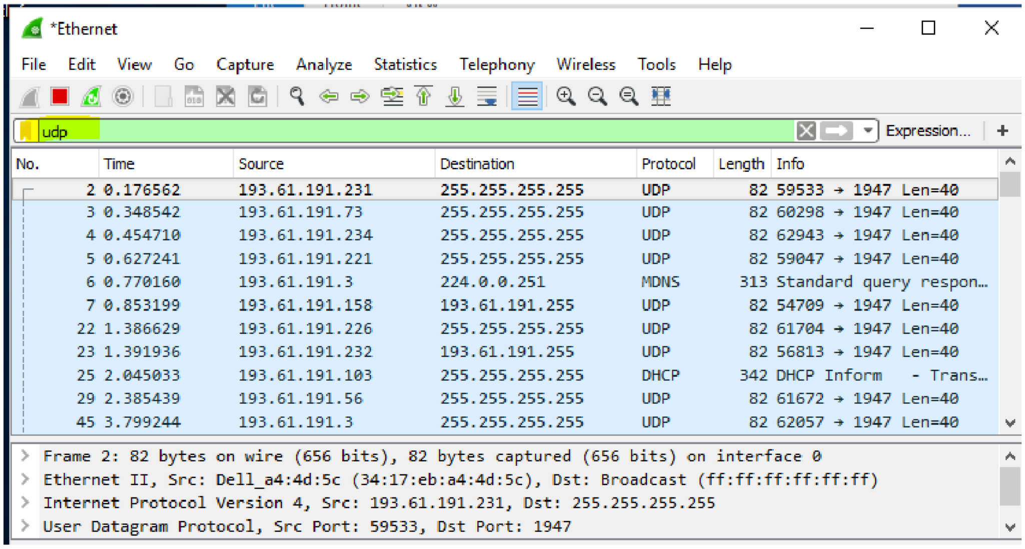

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
VMware Network Adapter VMnet1
Ethernet
VMware Network Adapter VMnet8

...10\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\trace-udp.pcap (93 KB)

Figure 2: Selecting the Ethernet Interface

3. Wireshark will automatically start capturing packets on the network.

   Now, enter a filter of **`udp`**. (This is shown below).


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.176562	193.61.191.231	255.255.255.255	UDP	82	59533 → 1947 Len=40
3	0.348542	193.61.191.73	255.255.255.255	UDP	82	60298 → 1947 Len=40
4	0.454710	193.61.191.234	255.255.255.255	UDP	82	62943 → 1947 Len=40
5	0.627241	193.61.191.221	255.255.255.255	UDP	82	59047 → 1947 Len=40
6	0.770160	193.61.191.3	224.0.0.251	MDNS	313	Standard query respon…
7	0.853199	193.61.191.158	193.61.191.255	UDP	82	54709 → 1947 Len=40
22	1.386629	193.61.191.226	255.255.255.255	UDP	82	61704 → 1947 Len=40
23	1.391936	193.61.191.232	193.61.191.255	UDP	82	56813 → 1947 Len=40
25	2.045033	193.61.191.103	255.255.255.255	DHCP	342	DHCP Inform - Trans…
29	2.385439	193.61.191.56	255.255.255.255	UDP	82	61672 → 1947 Len=40
45	3.799244	193.61.191.3	255.255.255.255	UDP	82	62057 → 1947 Len=40

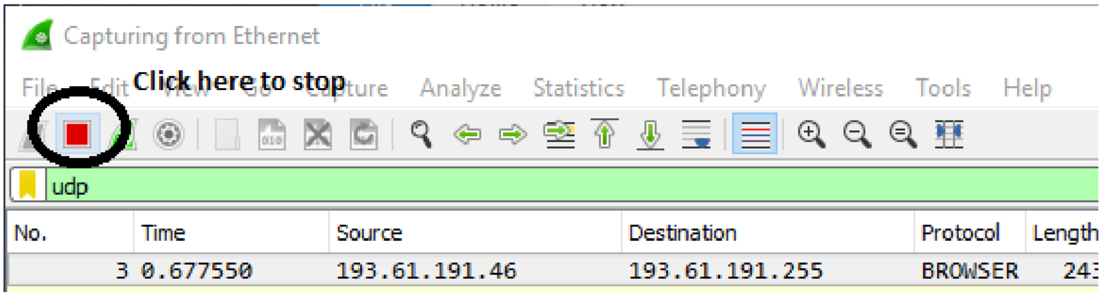
```
> Frame 2: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: Dell_a4:4d:5c (34:17:eb:a4:4d:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 193.61.191.231, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 59533, Dst Port: 1947
```

Figure 3: Setting up the capture options

4. When the capture is started, it will collect UDP traffic automatically.

5. Wait a little while (say 60 seconds) after you have stopped your activity to also observe any background UDP traffic. It is likely that you will observe a trickle of UDP traffic because system activity often uses UDP to communicate. We want to see some of this activity.

6. Use the Wireshark menus or buttons to stop the capture.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Click here to stop

udp

No.	Time	Source	Destination	Protocol	Length
3	0.677550	193.61.191.46	193.61.191.255	BROWSER	24

Figure 4: Stopping the capture

7. You should now have a trace with many UDP packets.

Step 2: Inspect the Trace

Different computers are likely to capture different kinds of UDP traffic depending on the network setup and local activity. Observe that the protocol column is likely to show multiple protocols, none of which is UDP. This is because the listed protocol is an application protocol layered on top of UDP. Wireshark gives the name of the application protocol, not the (UDP) transport protocol unless Wireshark cannot determine the application protocol. However, even if the packets are listed as an application protocol, they will have a UDP protocol header for us to study, following the IP and lower-layer protocol headers.

Select different packets in the trace (in the top panel) and browse the expanded UDP header (in the middle panel). You will see that it contains the following fields:

- Source Port, the port from which the UDP message is sent. It is given as a number and possibly a text name; names are given to port values that are registered for use with a specific application. ***List some of the source ports that you have identified?*** 53, 443, 5353

- Destination Port. This is the port number and possibly name to which the UDP message is destined. Ports are the only form of addressing in UDP. The computer is identified using the IP address in the lower IP layer.
List some of the destination ports that you have identified corresponding to the above source ports? 53, 5353, 50686

- Length. The length of the UDP message.
What is the typical length of of the UDP message that you have observed so far? 75 or 1399 bytes

  Note that UDP messages can be as large as roughly 64Kbytes but most often they are a few hundred bytes or less, typically around 100 bytes.

- Checksum. A checksum over the message that is used to validate its contents.
What is the value of the checksum field that you have observed? 0x1407

That is it! The UDP header has different values for different messages, but as you can see, it is short and sweet. The remainder of the message is the UDP payload that is normally identified the higher-layer protocol that it carries, e.g., DNS, or RTP.

Step 3: Understanding UDP Message Structure

The figure below shows the UDP message structure as you observed. It shows the position of the IP header, UDP header, and UDP payload. Within the UDP header, it shows the position and size of each UDP field. Note how the Length field gives the length of the UDP payload plus the UDP header. The checksum is 16 bits long and the UDP header is 8 bytes long.

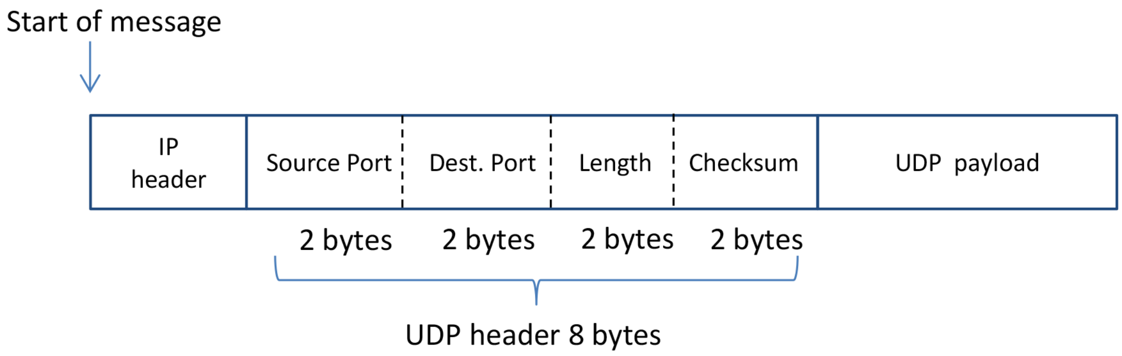


Figure 5: Structure of a UDP message

Step 4: Identifying UDP from IP header

The Protocol field in the IPv4 header is how IP knows that the next higher protocol layer is UDP.

What is the Protocol field value in the IPv4 header that indicates UDP is the higher layer protocol?

The protocol value is 17 (0x11)