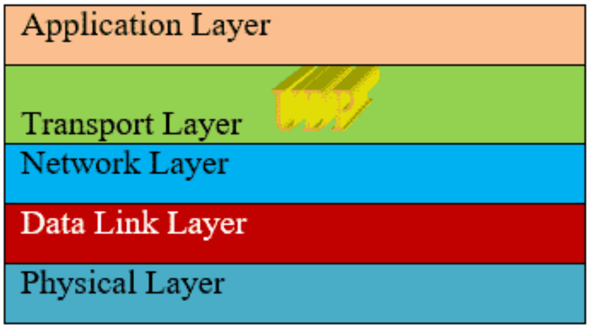
Wireshark

UDP Wireshark Analysis

3 years ago • by Bamdeb Ghosh

What is UDP?

User datagram protocol is another famous transport layer protocol than TCP. Below is the picture where UDP resides.



Intention of this article:

Intention of this article is to analysis UDP packet through Wireshark and understand UDP header practically. Difference between TCP and UDP can be read from internet.

Why UDP when we have TCP?

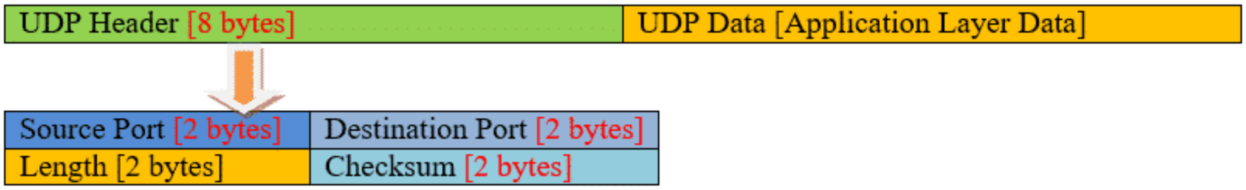
The basic reason is, UDP is a connection less protocol unlike TCP. So this feature makes UDP faster than TCP. But UDP suffers from the strong reliability unlike TCP. So, in conclusion when you can compromise some percentage in reliability but really wanted more speed, UDP is the transport layer protocol you should take.

To understand more on TCP please follow below link:

https://linuxhint.com/tcp_packet_capture_analysis/

UDP header:

UDP header is very simple and only 8 bytes.



UDP Header [8 bytes]	UDP Data [Application Layer Data]

Source Port [2 bytes]	Destination Port [2 bytes]
Length [2 bytes]	Checksum [2 bytes]

Source port: The source port number of the packet. Example: 4444.
Destination port: The destination port number of packet. Example: 51164.
Length: The length of UDP Data + UDP header.
Checksum: Checksum is present to detect error. Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

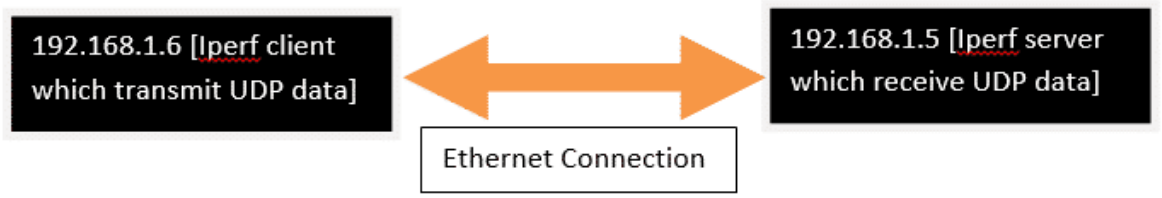
UDP Applications:

There are many protocols that use UDP. Here are some examples:

- DNS, DHCP, BOOTP, TFTP, RIP etc.
- Real time protocol which cannot tolerate delay.
- Used in some multicasting.

Packet Analysis:

Let's send some UDP date using Iperf network tool. **Here is the set up diagram used for generating udp data**


192.168.1.6 [Iperf client which transmit UDP data]
192.168.1.5 [Iperf server which receive UDP data]
Ethernet Connection

Here are the steps:

Step1: Start Wireshark.

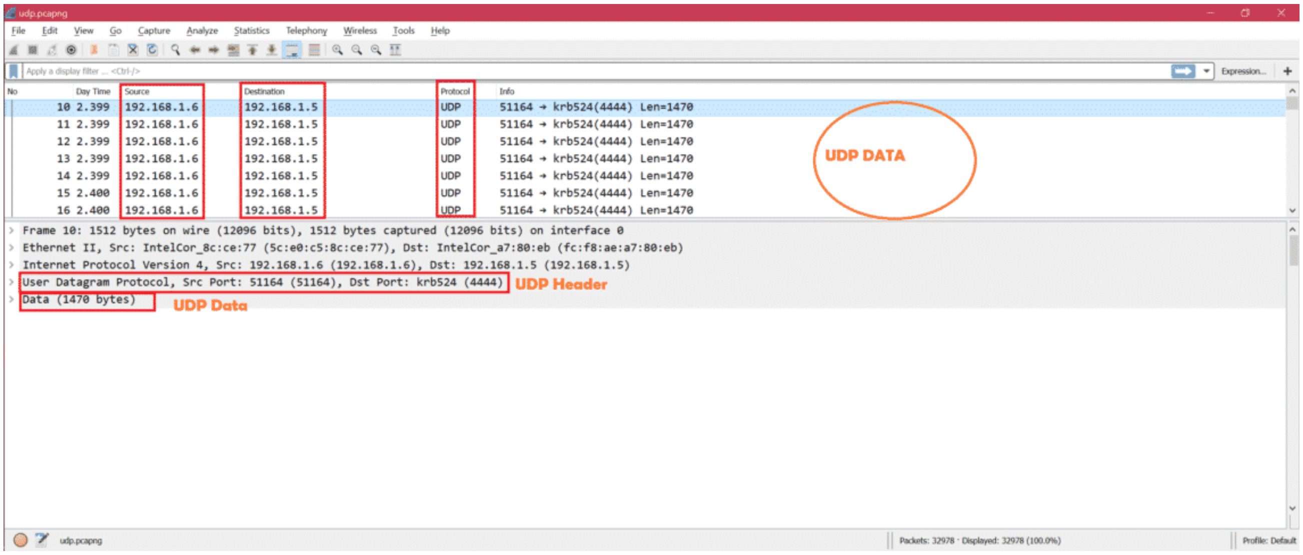
Step2: Run Iperf UDP server at 192.168.1.5 system.

Step3: Run Iperf UDP client at 192.168.1.6 system.

Step4: Stop Wireshark.

Step5: Analysis of captured packets

Here is the top level view of UDP packet in Wireshark.



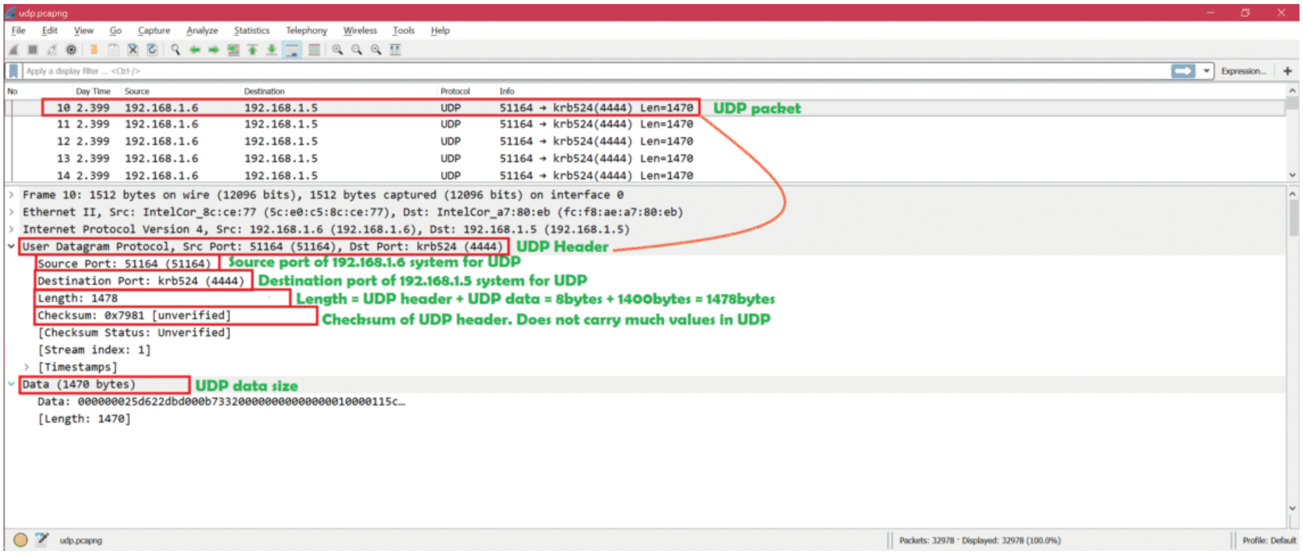
udp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
UDP DATA
UDP Header
UDP Data
udp.pcapng
Profile: Default

```
No   Day Time  Source       Destination   Protocol  Info
  10 2.399     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  11 2.399     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  12 2.399     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  13 2.399     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  14 2.399     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  15 2.400     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
  16 2.400     192.168.1.6  192.168.1.5   UDP       51164 → krb524(4444) Len=1470
```

```
> Frame 10: 1512 bytes on wire (12096 bits), 1512 bytes captured (12096 bits) on interface 0
> Ethernet II, Src: IntelCor_8c:ce:77 (5c:e0:c5:8c:ce:77), Dst: IntelCor_a7:80:eb (fc:f8:ae:a7:80:eb)
> Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.5 (192.168.1.5)
> User Datagram Protocol, Src Port: 51164 (51164), Dst Port: krb524 (4444)
> Data (1470 bytes)
```

```
Packets: 32978 · Displayed: 32978 (100.0%)
```

Now let's see inside UDP data packet. Here are the details of a UDP packet:


udp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
udp.pcapng
Packets: 32978 · Displayed: 32978 (100.0%)
Profile: Default

```
No   Day Time  Source        Destination    Protocol  Info
  10 2.399     192.168.1.6   192.168.1.5    UDP       51164 → krb524(4444) Len=1470
  11 2.399     192.168.1.6   192.168.1.5    UDP       51164 → krb524(4444) Len=1470
  12 2.399     192.168.1.6   192.168.1.5    UDP       51164 → krb524(4444) Len=1470
  13 2.399     192.168.1.6   192.168.1.5    UDP       51164 → krb524(4444) Len=1470
  14 2.399     192.168.1.6   192.168.1.5    UDP       51164 → krb524(4444) Len=1470

> Frame 10: 1512 bytes on wire (12096 bits), 1512 bytes captured (12096 bits) on interface 0
> Ethernet II, Src: IntelCor_8c:ce:77 (5c:e0:c5:8c:ce:77), Dst: IntelCor_a7:80:eb (fc:f8:ae:a7:80:eb)
> Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.5 (192.168.1.5)
v User Datagram Protocol, Src Port: 51164 (51164), Dst Port: krb524 (4444)
    Source Port: 51164 (51164)
    Destination Port: krb524 (4444)
    Length: 1478
    Checksum: 0x7981 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
v Data (1470 bytes)
    Data: 000000025d622dbd000b73320000000000000010000115c…
    [Length: 1470]
```

UDP packet

UDP Header

Source port of 192.168.1.6 system for UDP

Destination port of 192.168.1.5 system for UDP

Length = UDP header + UDP data = 8bytes + 1400bytes = 1478bytes

Checksum of UDP header. Does not carry much values in UDP

UDP data size

Note:

As UDP does not need any transport layer acknowledgement so evenif IPERF server is not running client will able send data unlike TCP.So always check in server side for UDP data.

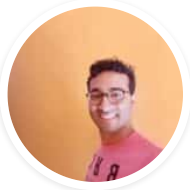
Summary:

Key points for UDP are:

1. There is no UDP connection frame exchange for UDP
2. There is no UDP transport layer ACK for UDP packet.
3. Depending upon application need one can go for UDP protocol to use.

#wireshark

ABOUT THE AUTHOR



Bamdeb Ghosh

Bamdeb Ghosh is having hands-on experience in Wireless networking domain.He's an expert in Wireshark capture analysis on Wireless or Wired Networking along with knowledge of Android, Bluetooth, Linux commands and python. Follow his site: wifisharks.com

View all posts

RELATED LINUX HINT POSTS

Using Wireshark to Examine FTP Traffic

A Guide to the Wireshark Command Line Interface “tshark”

Decrypting SSL/TLS Traffic with Wireshark

WireShark in-depth Tutorial

Why does Wireshark say no interfaces found

How to change time format in Wireshark

How to Use Wireshark to Search for a String in Packets

Linux Hint LLC, editor@linuxhint.com
1309 S Mary Ave Suite 210, Sunnyvale, CA
94087