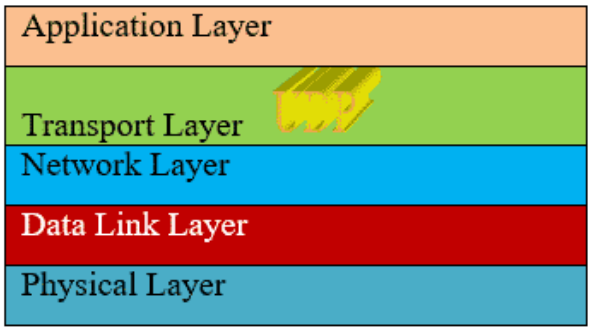
Wireshark

UDP Wireshark Analysis

4 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.

MY LATEST VIDEOS

Providing Audience Insights To T…

When Reddit was looking to better understand the diversity of its audience while protecting it…

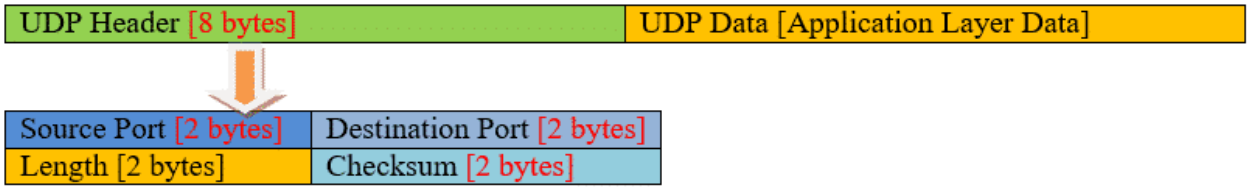
SPONSORED BY **QUANTCAST**

LEARN MORE

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.



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.

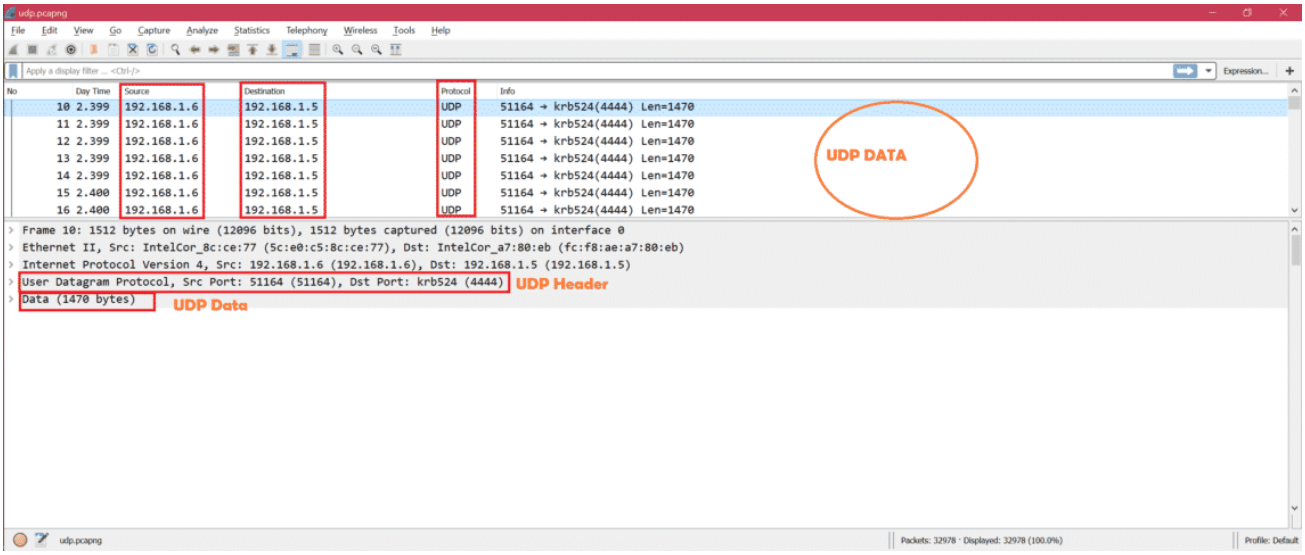
Packet Analysis:

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

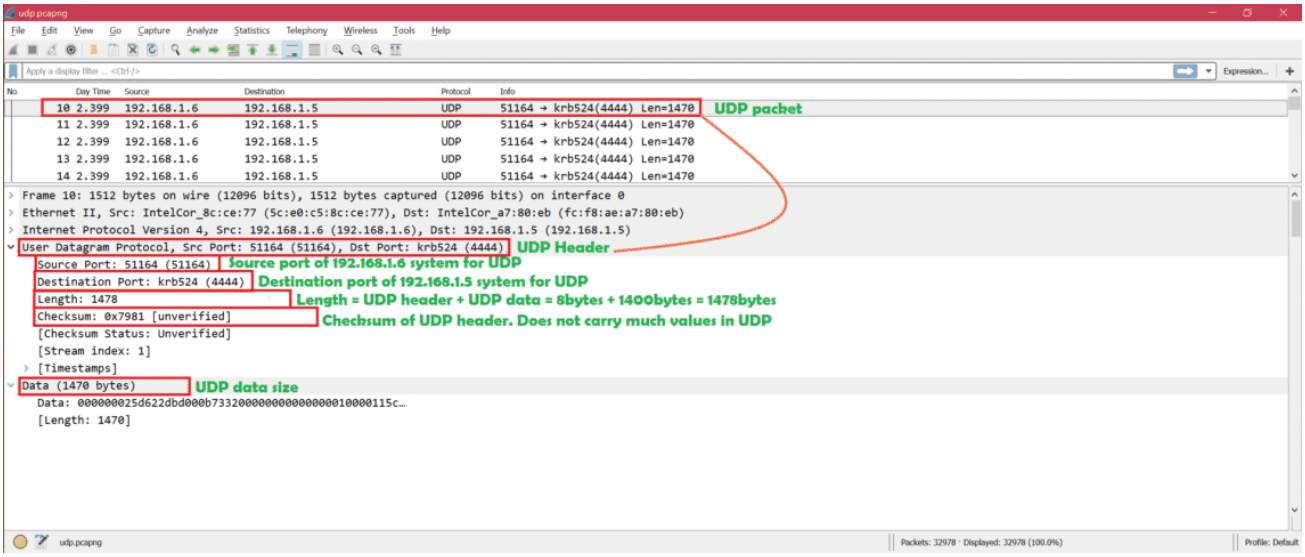
Here are the steps:

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.



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



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

- How to Extract a Video from Wireshark Capture
- ARP Spoofing Attack Analysis in Wireshark
- 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

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

Privacy Policy and Terms of Use

A RAPTIVE PARTNER SITE