

laboratory report

Title: TCP/UDP/RTCP Protocol Analysis

Time: 2021.12.22

Class: 2019211112

no: 2021523016

Name: 徐川峰

1.Purpose

Use Wireshark to familiarize yourself with the differences between UDP and TCP. Understand RTCP parameters.

2.Tool

Wireshark network packet analysis software.

3.Result

<1>UDP

(1) Wireshark

The screenshot shows the Wireshark interface with a list of network packets. The selected packet is a DNS query (Standard query) from 10.128.224.128 to 101.198.198.198. The packet details pane shows the following information:

- Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{1FC72E7F-14D8-46E3-9F11-7FC0197AA592}, id 0
- Ethernet II, Src: LiteonTe_f7:16:e9 (cc:b0:da:f7:16:e9), Dst: New43Cte_11:20:01 (74:85:c4:11:20:01)
- Internet Protocol Version 4, Src: 10.128.224.128, Dst: 101.198.198.198
- User Datagram Protocol, Src Port: 63176, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 74 85 c4 11 20 01 cc b0 da f7 16 e9 08 00 45 00 t... ..E-
0010 00 3a 4c e3 00 00 80 11 d6 42 0a 80 e0 80 65 c6 .:L....:B....
0020 c6 c6 f6 c8 00 35 00 20 6d 85 00 02 01 00 00 01 .....5m.....
0030 00 00 00 00 00 00 03 57 57 57 04 43 43 53 46 03 .....WMM-CCSF-
0040 45 44 55 00 00 01 00 01 EDU.....
```

(2) command line

```
无线局域网适配器 本地连接* 10:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 以太网 2:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    IPv6 地址 . . . . . : 2001:da8:215:3c01::4:dffa
    IPv6 地址 . . . . . : 2001:da8:215:3c01:f88a:9ea7:2525:39a8
    临时 IPv6 地址. . . . . : 2001:da8:215:3c01:69fb:519e:f30e:54f
    本地链接 IPv6 地址. . . . . : fe80::f88a:9ea7:2525:39a8%5
    IPv4 地址 . . . . . : 10.128.224.128
    子网掩码 . . . . . : 255.255.192.0
    默认网关 . . . . . : fe80::7685:c4ff:fe11:2001%5
                        10.128.192.1

隧道适配器 本地连接* 2:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap. {1FC72E7F-14DB-46E3-9F11-7FC0197AA592}:

    媒体状态 . . . . . : 媒体已断开连接
```

<2>TCP

(1) wireshark

The image shows a Wireshark capture of network traffic on the 'WLAN' interface. The packet list pane shows several packets, including a DNS query (73) and a TCP SYN packet (66) from 10.128.224.128 to 114.112.66.94. The packet details pane shows the selected packet (Frame 188) as a TCP segment with source port 59185 and destination port 80. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

(2) command line

```
正在 Ping www.a.shifen.com [2408:80f0:410c:1c:0:ff:b00e:347f] 具有 32 字节的数据:
来自 2408:80f0:410c:1c:0:ff:b00e:347f 的回复: 时间=27ms
来自 2408:80f0:410c:1c:0:ff:b00e:347f 的回复: 时间=110ms
来自 2408:80f0:410c:1c:0:ff:b00e:347f 的回复: 时间=30ms
来自 2408:80f0:410c:1c:0:ff:b00e:347f 的回复: 时间=32ms

2408:80f0:410c:1c:0:ff:b00e:347f 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 27ms, 最长 = 110ms, 平均 = 49ms
```

<3>RTCP

(1) wireshark

The image shows a Wireshark network capture interface. The top pane displays a list of captured packets, with several RTCP (Real-time Transport Control Protocol) packets highlighted. The middle pane shows the details of the selected packet, including the Receiver Report (RR) and the Source Description (SD). The bottom pane shows the raw packet data in hexadecimal and ASCII. A VLC media player window is overlaid on the right side of the Wireshark interface, displaying a video stream from the URL `rtsp://10.128.199.145:8554/test`. The video shows a street scene with cars and a bus.

4. Conclusion

- 1、TCP is connection-oriented, UDP is connection-less;
- 2、TCP ensures reliable transmission, UDP provides unreliable transmission
- 3、TCP transmits byte streams, UDP transmits segments;
- 4、When messages are sent, TCP ensures connection and checks time-out data while UDP just put data on the internet.
- 5、TCP connection is point-to-point while UDP connection is one-to-many or even many-to-many.
- 6、TCP has congestion control but UDP doesn't have.