TTL Introduction

TTL (Time To Live) is an important parameter in IP packet header. From TTL value, we can judge the current status of the IP layer.

TTL tells the router whether the packet should be dropped because it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet will be dropped. As TTL value will be deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of the routers which the packet passed through before it was dropped. When TTL becomes zero, the router will drop the packet and send an ICMP message to the sender of the packet.

Various causes will lead to packets transmission failure to the destination in a specific time period. For instance, wrong routing table configuration may cause packet endless loop. The solution is to drop the packet after a period of time and then send a message to the sender and let it decide whether to retransmit the packet. When this happens, the packet will be retransmitted at the router which is wrongly configured in the routing table. TTL value will be deducted by 1 upon each retransmission until TTL becomes zero when the packet is dropped by the router, which causes transmission error in the network.

Default TTL value varies depending on the difference of the operating system and transmission protocol. Here I listed the default TTL values in TCP and UDP under common operating systems in table 1:

Operating system	TCP	UDP
AIX	60	30
DEC Patchworks V5	30	30

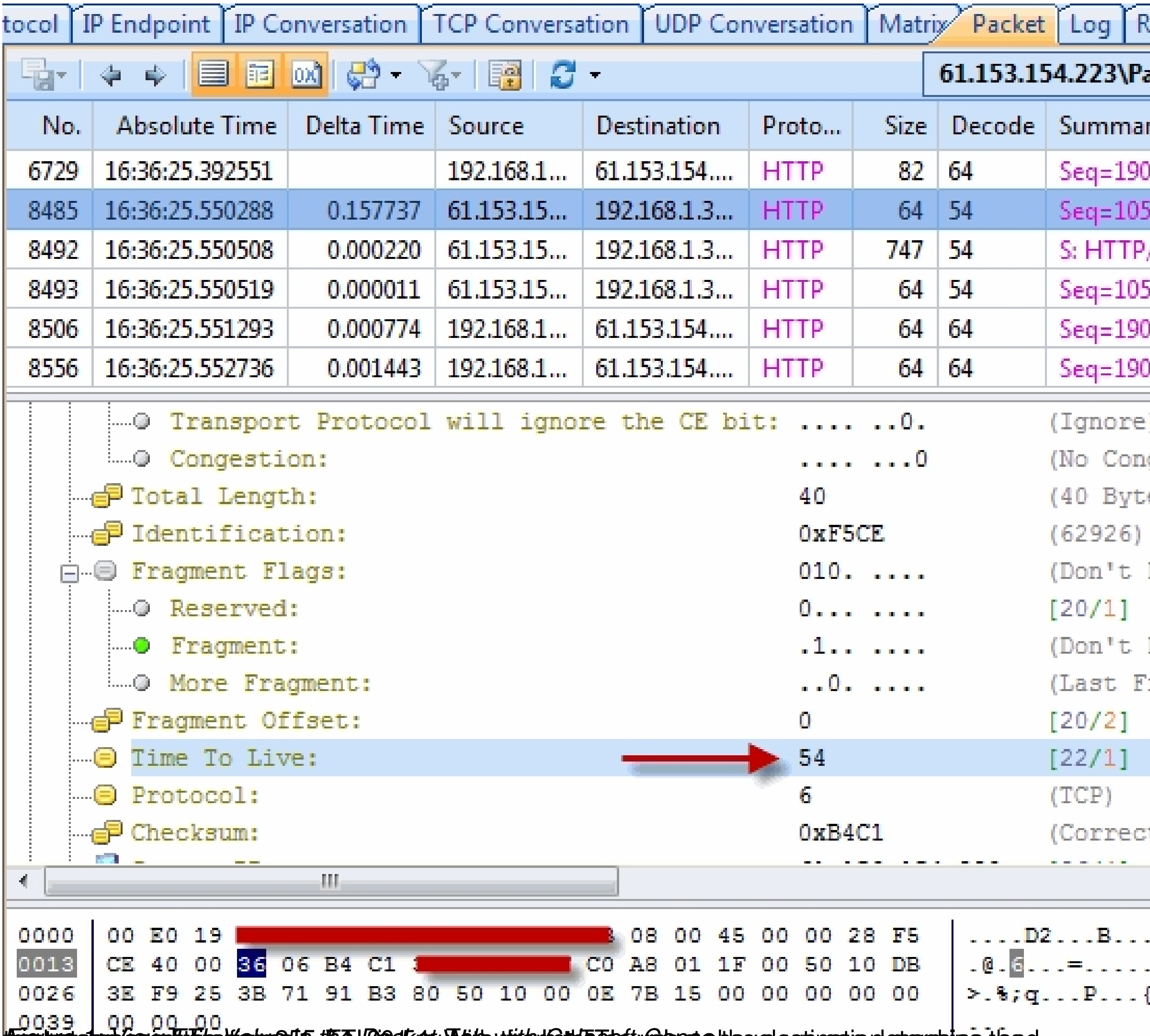
FreeBSD 2.1	64	64
HP/UX 9.0x	30	30
HP/UX 10.01	64	64
Irix 5.3	60	60
Irix 6.x	60	60
UNIX	255	255
Linux	64	64
MacOS/MacTCP 2.0.x	60	60
OS/2 TCP/IP 3.0	64	64
OSF/1 V3.2A	60	30
Solaris 2.x	255	255
SunOS 4.1.3/4.1.4	60	60
Ultrix V4.1/V4.2A	60	30
VMS/Multinet	64	64
VMS/TCPware	60	64
VMS/Wollongong 1.1.1.1	128	30
VMS/UCX (latest rel.)	128	128
MS Windows 95/98/NT 3.51	32	32
Windows NT 4.0/2000/XP/2003 Server	128	128

Table 1: Default TTL Value under Different Operating Systems

View TTL value of packets and analyze transmission error

When transmission error occurs in the network, we can view the TTL value of packets with a network analyzer and determine whether the error is resulted from wrong routing configuration or other possible reasons in combination of the above table.

Here I use Colasoft Capsa to view TTL of a packet.



No.	Absolute Time	Delta Time	Source	Destination	Proto...	Size	Decode	Summar
6729	16:36:25.392551		192.168.1...	61.153.154....	HTTP	82	64	Seq=190
8485	16:36:25.550288	0.157737	61.153.15...	192.168.1.3...	HTTP	64	54	Seq=105
8492	16:36:25.550508	0.000220	61.153.15...	192.168.1.3...	HTTP	747	54	S: HTTP/
8493	16:36:25.550519	0.000011	61.153.15...	192.168.1.3...	HTTP	64	54	Seq=105
8506	16:36:25.551293	0.000774	192.168.1...	61.153.154....	HTTP	64	64	Seq=190
8556	16:36:25.552736	0.001443	192.168.1...	61.153.154....	HTTP	64	64	Seq=190

```
Transport Protocol will ignore the CE bit:   .... ..0.   (Ignore
Congestion:                                  .... ...0   (No Con
Total Length:                                40          (40 Byt
Identification:                              0xF5CE      (62926)
Fragment Flags:                              010. ....   (Don't 
  Reserved:                                  0... ....   [20/1]
  Fragment:                                  .1.. ....   (Don't 
  More Fragment:                             ..0. ....   (Last F
Fragment Offset:                             0           [20/2]
Time To Live:                                54          [22/1]
Protocol:                                    6           (TCP)
Checksum:                                    0xB4C1      (Correc
```

```
0000  00 E0 19 [redacted] 08 00 45 00 00 28 F5   ....D2...B...
0013  CE 40 00 36 06 B4 C1 [redacted] C0 A8 01 1F 00 50 10 DB   .@.6...=.....
0026  3E F9 25 3B 71 91 B3 80 50 10 00 0E 7B 15 00 00 00 00 00   >.%;q...P...{
0039  00 00 00
```

[illegible]

Notice:

1. To determine how many routers a packet passed, you can deduct the TTL value of the packet you captured from the default TTL value of the source device.
2. If you don't know the default TTL value of the source device, you can use the default TTL value which is lager than and most close to the TTL value of the packet;
3. The peak TTL value is 255 as TTL field size is 1 byte.

Conclusion

If TTL value of the captured packets is too small, it indicate there may be a transmission error in the network. By checking the TTL value we can find out whether the network is normal or not.