Wireshark Developer and User Conference

Packet Trace Whispering

June 14th, 2011

Hansang Bae
Senior VP| Citi (f.k.a. Citigroup)
hansang@gmail.com

SHARKFEST **'11**
Stanford University
June 13-16, 2011

Packet Trace Whispering

June 14th, 2011

The video/audio recording made during the session will be made available on YouTube and www.lovemytool.com by the end of June.

On Youtube, just search for “hansangb wireshark”

Selective Packet Loss?

- After turning up a new international circuit, application developers cannot connect to the server.
- It’s not the network! Or is it?
- Easy to dismiss as packet loss at first glance.
- Use IP.ID to find additional clues.
- TCP guarantees delivery. What does that mean?
- Learn to pick up on key differences– Learn to ignore the background chatter.

C:\Traces\
g\Sharkfest 2011\b

Selective Packet Loss (con’t)?

```
cxi01-6509#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.70.3
Type of service [0]: 0x10
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10,
    timeout is 2 seconds:
Packet sent with a source address of 172.16.70.3
.....
Success rate is 0 percent (0/5)
```

```
cxi01-6509#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.70.3
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10,
    timeout is 2 seconds:
Packet sent with a source address of 172.16.70.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/
    avg/max = 72/73/76 ms
```

Selective Packet Loss (con't)?

```
cxi01-6509#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.70.3
Type of service [0]: 0x10
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10,
      timeout is 2 seconds:
Packet sent with a source address of 172.16.70.3
.....
Success rate is 0 percent (0/5)
```

```
cxi01-6509#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.70.3
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10,
      timeout is 2 seconds:
Packet sent with a source address of 172.16.70.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/
      avg/max = 72/73/76 ms
```

More Network Problems?

- Packet loss tend to be network infrastructure related.
- TCP SEQ is the same, but NEXT EXPECTED SEQ goes up. Is that OK?
- How does IP.ID help here? What does it prove?
- We can never be sure, but analysis can point us in the right direction.

pktloss.pcap

Don’t be so quick to judge

VTSlow.pcap

- Application response is slow.
- What are the usual suspects?
- There is a difference between SEND and RECEIVE window sizes.
- What does Stevens say?
- Not all “Windows Update” are the same.
- What should you not see? How do you fix it?
- Ultimately, whose fault is it?

Internet is the Internet, right?

- Customer sent us the trace but gave us little context
  - His application was encountering performance issues with an external vendor.
  - Vendor indicated that the issue was not on their end.
  - It was a “network/proxy issue”, or was it?

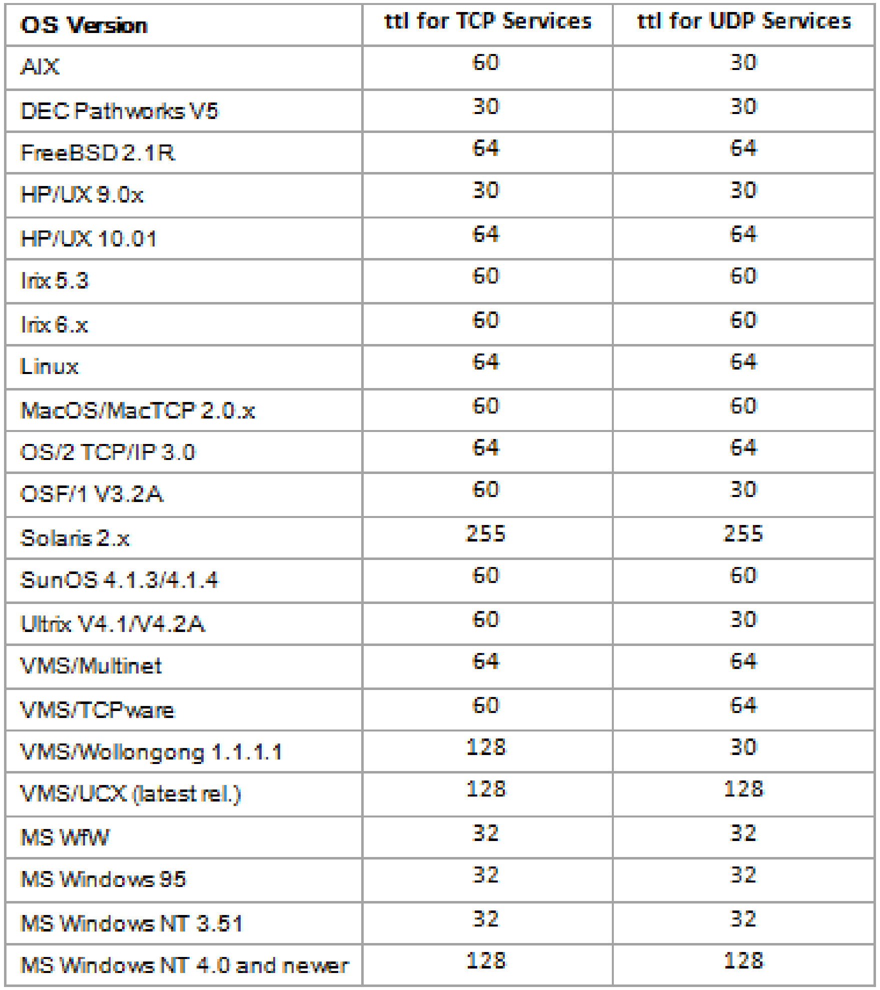
ExternalAppSlow.pcap

- Let’s examine the evidence…
- Sometimes, you have to look at the IP layer to ferret out the answer.
- Can we rule out packet loss?

Internet is the… (con’t)

TTL

- TTL is a field set by the originator of a packet.
- Created to prevent a packet from infinitely looping around networks/Internet.
- Value is decremented at every router hop.
- Can allow determination of how many hops a packet has traversed
- Provides some level of confidence as to whether 2 packets were originated by the same source and even allow passive stack fingerprinting.



OS Version	ttl for TCP Services	ttl for UDP Services
AIX	60	30
DEC Pathworks V5	30	30
FreeBSD 2.1R	64	64
HP/UX 9.0x	30	30
HP/UX 10.01	64	64
Irix 5.3	60	60
Irix 6.x	60	60
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 WfW	32	32
MS Windows 95	32	32
MS Windows NT 3.51	32	32
MS Windows NT 4.0 and newer	128	128