

SharkFest'17 US

Wireshark & Time Accurate Handling of Timing When Capturing Frames



Tuesday June 20, 2017
Thursday June 22, 2017

Werner Fischer
Principal Networking Consultant | avodaq AG

About me

- From Germany (sorry again for the accent)
- More than a decade Dual-CCIE (R/S, Security)
- Sniffer Certified Master
- Wireshark Certified Network Analyst
- VMware Certified Professional
- IPv6 Forum Certified Engineer (Gold)
- More than 20 years in the networking area



AGENDA

- Time basic
- Time Protocols
- NTP
- PTP
- Wrap-UP

Capture Files and other useful infos:

<http://goo.gl/LGNWo8>

Enterprise ToD Landscape

- Accurate/Secure/Reliable ToD for server/routers/applications for improved network operations and business operations
- Frequency and Time Synchronization



A Note on Terminology with Timing

- **Accuracy** – how close a measurement is to a true value
- **Precision** – how close repeated measurements are to each other
- **Frequency** – Reference signal drives circuits to a common standard
 - “10 Mhz is the same everywhere”
- **Phase** – making sure two systems understand when things start and stop- agree on milestones
 - “Everyone clapping together”

Precision Timing is essential

- Clock is the one of the most important component of any modern electrical system
- Network and applications also need accurate timing information to correlate all the events
 - Network Analysis
 - Application transactions
 - Data Forensics
 - Event-log analysis
- Timestamps mainly mandatory for compliance

Timing Challenge for up-to-date Networks

- Switches can forward the Frames in a matter of microseconds
- Ultra low latency switches for high frequency trading
- Some assumptions about the network
 - The transmission delays are almost constant over time (or at least change slowly)
 - The transmission delays are symmetrical between master and slave (i.e. time to travel from master to slave is the same as from slave to master)

Different Timestamps for different encapsulation

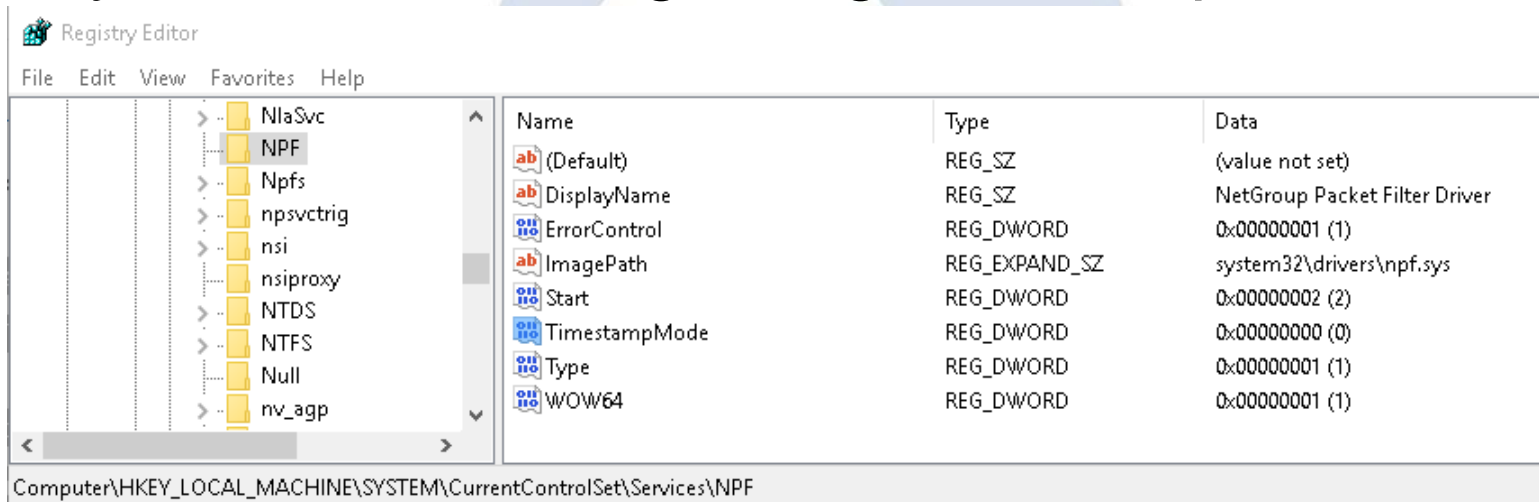
- frame.time
- prism.did.mactime
- radiotap.mactime
- ...

```
▼ Radiotap Header v0, Length 28
  Header revision: 0
  Header pad: 0
  Header length: 28
  > Present flags
    MAC timestamp: 169685850
  > Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
    ▼ USB URB
      [Source: host]
      [Destination: 1.1.0]
      URB id: 0x0000000ed896f00
      URB type: URB_SUBMIT ('S')
      URB transfer type: URB_CONTROL (0x02)
    > Endpoint: 0x80, Direction: IN
      Device: 1
      URB bus id: 1
      Device setup request: relevant (0)
      Data: not present ('<')
      URB sec: 1362459244
      URB usec: 273742
      URB status: Operation now in progress (-EINPROGRESS) (-115)
      URB length [bytes]: 40
      Data length [bytes]: 0
      [Response in: 2]
      Interval: 0
      Start frame: 0
      Copy of Transfer Flags: 0x0000200
      Number of ISO descriptors: 0
    > URB setup
```

```
▼ Frame 6: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits)
  Interface id: 0 (\Device\NPF_{4C3659F3-91DF-46A3-A615-EDA158651988})
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun 14, 2017 14:23:19.490510000 W. Europe Daylight T:
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1497442999.490510000 seconds
  [Time delta from previous captured frame: 0.003978000 seconds]
  [Time delta from previous displayed frame: 0.003978000 seconds]
  [Time since reference or first frame: 0.011334000 seconds]
```


WinPcap and Time

- Timestamp Mode adjusted by registry
<http://seclists.org/wireshark/2010/Aug/311>
- WinPcap is synchronized with the system clock only once, at the beginning of the capture !



Wireshark and Time Display Format

et: 0
t: 213

Option	Shortcut
Date and Time of Day (1970-01-01 01:02:03.123456)	Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)	
Time of Day (01:02:03.123456)	Ctrl+Alt+2
Seconds Since 1970-01-01	Ctrl+Alt+3
<input checked="" type="radio"/> Seconds Since Beginning of Capture	Ctrl+Alt+4
Seconds Since Previous Captured Packet	Ctrl+Alt+5
Seconds Since Previous Displayed Packet	Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456)	Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)	
UTC Time of Day (01:02:03.123456)	Ctrl+Alt+8
<input checked="" type="radio"/> Automatic (from capture file)	
Seconds	
Tenths of a second	
Hundredths of a second	
Milliseconds	
Microseconds	
Nanoseconds	
Display Seconds With Hours and Minutes	

AGENDA

- Time basic
- **Time Protocols**
- NTP
- PTP
- Wrap-UP



Different Time Sources available

- **NTP (Network Time Protocol)**
 - Several RFCs
 - time synchronization protocol for packet network
- **GPS (Global Position System)**
- **IRIG (And other serial timing protocols)**
- **PTP (Precision Timing Protocol)**
 - Defined in IEEE1588
 - Another time synchronization protocol for packet network

Different Time Scales

- The relationships in real time

local	2017-06-14 18:31:21	Wednesday	day 165	timezone UTC+2
UTC	2017-06-14 16:31:21	Wednesday	day 165	MJD 57918.68843
GPS	2017-06-14 16:31:39	week 1953	318699 s	cycle 1 week 0929 day 3
Loran	2017-06-14 16:31:48	GRI 9940	48 s until	next TOC 16:32:09 UTC
TAI	2017-06-14 16:31:58	Wednesday	day 165	37 leap seconds

- <http://www.leapsecond.com/java/gpsclock.htm>

AGENDA

- Time basic
- Time Protocols
- **NTP**
- PTP
- Wrap-UP

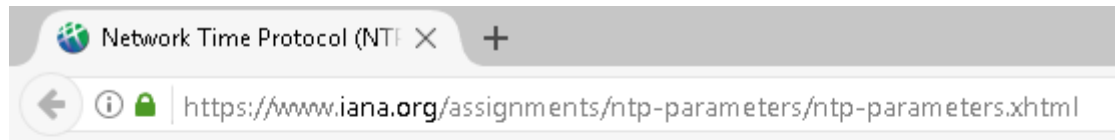


code.wireshark Code Review X +

https://code.wireshark.org/review/gitweb?p=wireshark.git;a=tree;f=epan/dissectors;h=546fcfb52b8c12020a81e3902d2111fe36a026e6;hb=HEAD

-rw-r--r--	59188	packet-ntp.c	blob history raw
-rw-r--r--	1239	packet-ntp.h	blob history raw

IANA and NTP Parameters



Network Time Protocol (NTP) Parameters

Created

2010-03-25

Last Updated

2016-03-31

Available Formats



XML



HTML



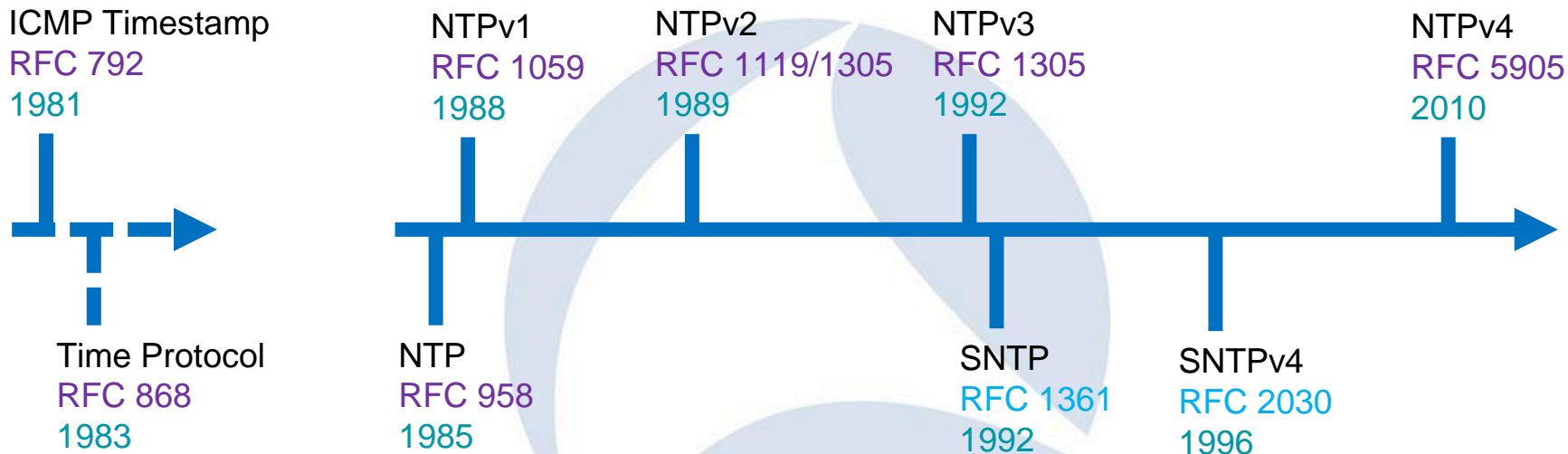
Plain text

Registries included below

- [NTP Reference Identifier Codes](#)
- [NTP Kiss-o'-Death Codes](#)
- [NTP Extension Field Types](#)

- Great resource for reference
- <https://www.iana.org/assignments/ntp-parameters/ntp-parameters.xhtml>

History of NTP



Useful (S)NTP RFCs – only for your reference

- **RFC 1305**
 - Network Time Protocol (Version 3) Specification, Implementation and Analysis
- **RFC 2030**
 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- **RFC 5905**
 - Network Time Protocol Version 4: Protocol and Algorithms Specification
- **RFC 5906**
 - Network Time Protocol Version 4: Autokey Specification
- **RFC 5907**
 - Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)
- **RFC 7821**
 - UDP Checksum Complement in the Network Time Protocol (NTP)
- **RFC 7822**
 - Network Time Protocol Version 4 (NTPv4) Extension Fields

NTP Pool Project

- <http://www.pool.ntp.org/en/>
- “ ...big virtual cluster of timeservers providing reliable easy to use NTP service for millions of clients ... ”

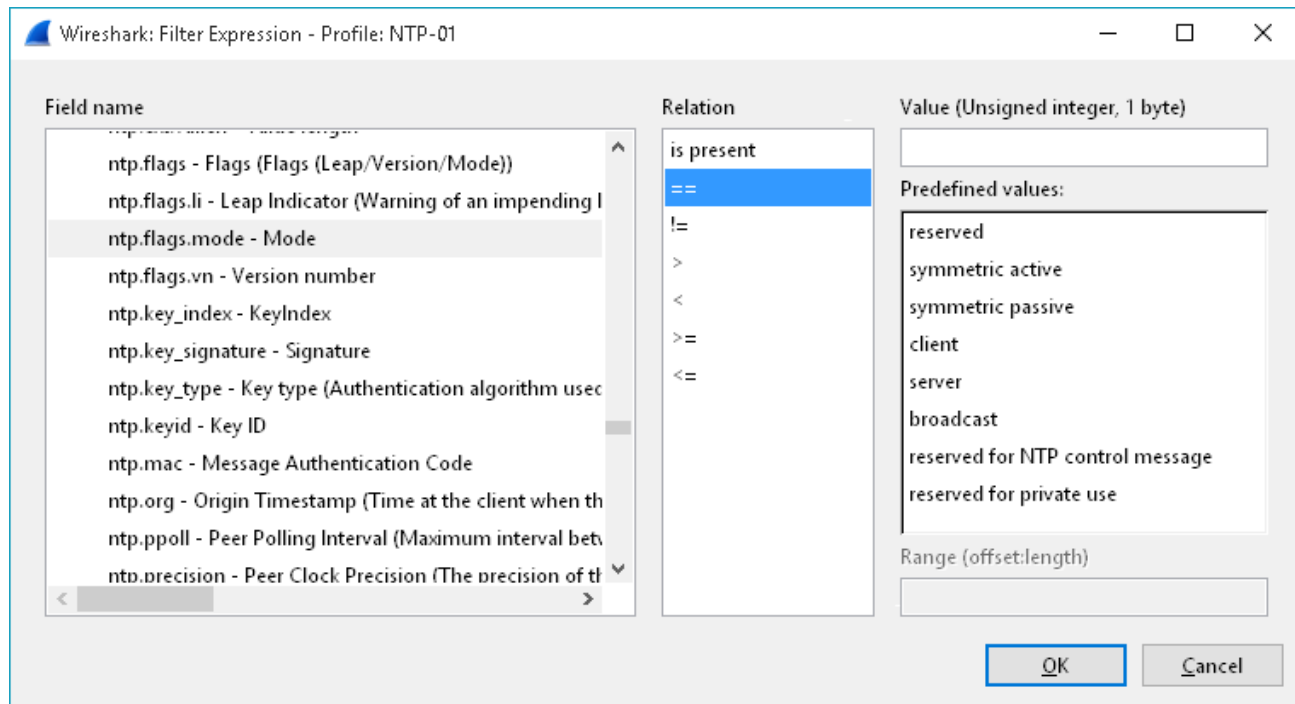
Active Servers

	Africa	34
	Antarctica	0
	Asia	268
	Europe	2789
	North America	939
	Oceania	100
	South America	46
	Global	3901
	All Pool Servers	4176

As of 2017-06-17

NTP Modes

- Peer
- Client
- Server
- Broadcast/
Multicast
- Control
- Private
Use

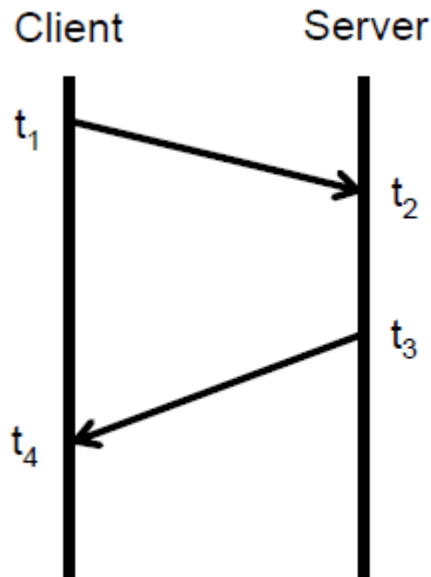


NTP Message Format

LI / VN / MODE	STRATUM
POLL	PRECISION
ROOT DELAY	
ROOT DISPERSION	
REFERENCE IDENTIFIER	
REFERENCE TIMESTAMP (64 bit scaled seconds)	
ORIGINATE TIMESTAMP	
RECEIVE TIMESTAMP	
TRANSMIT TIMESTAMP	

Basic NTP Time Information Exchange

• Client Request



ntpv4-ipv4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

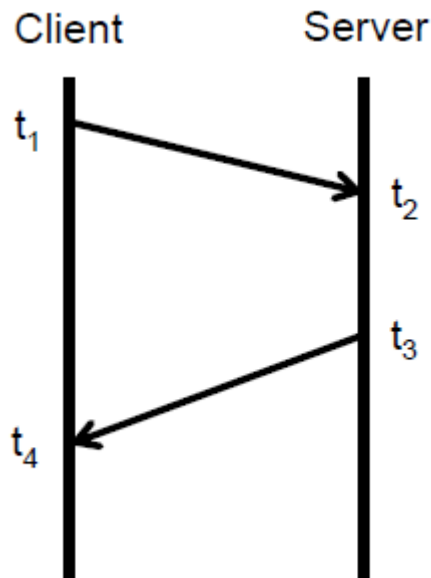
No.	Time	Source	Destination	Protocol	Info	Length	Flags
1	0.000000	2.2.2.1	2.2.2.2	NTP	NTP Version 4, client	90	
2	0.000431	2.2.2.2	2.2.2.1	NTP	NTP Version 4, server	90	

<

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Ethernet II, Src: aa:bb:cc:03:21:00 (aa:bb:cc:03:21:00), Dst: aa:bb:cc:03:22:00 (aa:bb:cc:03:22:00)
> Internet Protocol Version 4, Src: 2.2.2.1, Dst: 2.2.2.2
> User Datagram Protocol, Src Port: 123, Dst Port: 123
> Network Time Protocol (NTP Version 4, client)
> Flags: 0xe3, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 4, Mode: client
Peer Clock Stratum: unspecified or invalid (0)
Peer Polling Interval: 6 (64 sec)
Peer Clock Precision: 0.015625 sec
Root Delay: 0.0000 sec
Root Dispersion: 0.0000 sec
Reference ID: (Initialization)
Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Transmit Timestamp: May 3, 2011 12:03:19.157828000 UTC

Basic NTP Time Information Exchange

• Server Response



ntpv4-ipv4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info	Length
1	0.000000	2.2.2.1	2.2.2.2	NTP	NTP Version 4, client	90
2	0.000431	2.2.2.2	2.2.2.1	NTP	NTP Version 4, server	90

> Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Ethernet II, Src: aa:bb:cc:03:22:00 (aa:bb:cc:03:22:00), Dst: aa:bb:cc:03:21:00 (aa:bb:cc:03:21:00)
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 2.2.2.1
> User Datagram Protocol, Src Port: 123, Dst Port: 123
v Network Time Protocol (NTP Version 4, server)
 > Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
 Peer Clock Stratum: secondary reference (5)
 Peer Polling Interval: 6 (64 sec)
 Peer Clock Precision: 0.015625 sec
 Root Delay: 0.0000 sec
 Root Dispersion: 0.0315 sec
 Reference ID: 127.127.1.1
 Reference Timestamp: May 3, 2011 12:03:16.069718000 UTC
 Origin Timestamp: May 3, 2011 12:03:19.157828000 UTC
 Receive Timestamp: May 3, 2011 12:03:19.157718000 UTC
 Transmit Timestamp: May 3, 2011 12:03:19.157718000 UTC

Basic NTP Authentication

- MD5

```
Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
Origin Timestamp:   Jan  1, 1970 00:00:00.000000000 UTC
Receive Timestamp:  Jan  1, 1970 00:00:00.000000000 UTC
Transmit Timestamp: Oct  8, 2015 19:22:26.265421000 UTC
Key ID: 00000001
```

```
Message Authentication Code: 875f9463f635d24d42c00715a42e0f93
```

```
0000 00 1c 42 a6 21 1a 00 1c 42 71 99 e6 08 00 45 00  ..B.!... Bq....E.
0010 00 60 ed 45 40 00 40 11 37 0f 0a 00 01 1d 0a 00  .'.E@.@. 7.....
0020 01 1c 00 7b 00 7b 00 4c 16 96 e3 00 03 fa 00 01  ...{.{.L .....
0030 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
0050 00 00 d9 c1 40 f2 43 f2 a5 f6 00 00 00 01 87 5f  ...@.C. ....
0060 94 63 f6 35 d2 4d 42 c0 07 15 a4 2e 0f 93      .c.5.MB. ....
```

- SHA-1

```
Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
Origin Timestamp:   Jan  1, 1970 00:00:00.000000000 UTC
Receive Timestamp:  Jan  1, 1970 00:00:00.000000000 UTC
Transmit Timestamp: Oct  8, 2015 17:21:32.287131000 UTC
Key ID: 0000000c
```

```
Message Authentication Code: 6b944dce3f05510d206f615f36e900fa532594c8
```

```
0000 00 1c 42 a6 21 1a 00 1c 42 71 99 e6 08 00 45 00  ..B.!... Bq....E.
0010 00 64 8d 27 40 00 40 11 97 29 0a 00 01 1d 0a 00  .d.'@.@. ).....
0020 01 1c 00 7b 00 7b 00 50 16 9a e3 00 03 fa 00 01  ...{.{.P .....
0030 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
0050 00 00 d9 c1 24 9c 49 81 79 2f 00 00 00 0c 6b 94  ...$.I. y/...k.
0060 4d ce 3f 05 51 0d 20 6f 61 5f 36 e9 00 fa 53 25  M.?.Q. o a 6...S%
0070 94 c8      ..
```

NTP Timestamps

- NTP use 64 bit-Timestamps

- They consist of a 32-bit part for seconds and a 32-bit part for fractional second
- The time scale rolls over every 2^{32} seconds (136 years)
- Theoretical resolution of 2^{-32} seconds (233 picoseconds)
- It uses an epoch of 1 January 1900
- The first rollover occurs in 2036, prior to the UNIX year 2038 problem

```
Reference Timestamp: Jul 16, 2009 07:46:42.227275000 UTC
Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Transmit Timestamp: Jul 16, 2009 07:47:04.581275000 UTC
Key ID: 54040000
Message Authentication Code: 00000000000000000000000000000000

0000 00 19 b9 04 31 18 00 0a e4 c8 7a 64 08 00 45 00  ....1... ..zd..E.
0010 00 60 00 32 00 00 80 11 26 56 0a 00 00 04 0a 00  ..2... &v.....
0020 00 02 00 7b 00 7b 00 4c 5b 61 db 00 00 11 fa 00 00  ...{.L [a.....
0030 00 00 00 01 03 fe 00 00 00 00 00 ce 09 59 62 3a 2e  .....Yb:.
0040 b6 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..
0050 00 00 ce 09 59 78 94 ce 75 43 54 04 00 00 00 00 00  ...YX.. uCT.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Time.sec

Seconds

32 bit

Time.Frac

Fraction

32 bit

NTP and DHCP / DHCPv6

• IPv4 and DHCP

Option 42

• IPv6 and DHCPv6

- SNTP

dhcpv6.requested_option_code == 31

- NTP

dhcpv6.requested_option_code == 56

```
> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits)
> Ethernet II, Src: Vmware_9b:a1:5d (00:0c:29:9b:a1:5d), Dst: Vmware_38:f3:68 (00:0c:29:38:f3:68)
> Internet Protocol Version 6, Src: fe80::20c:29ff:fe9b:a15d, Dst: fe80::20c:29ff:fe38:f368
> User Datagram Protocol, Src Port: 547, Dst Port: 546
< DHCPv6
```

```
  Message type: Reply (7)
  Transaction ID: 0xf69b57
```

```
> Client Identifier
> Server Identifier
```

< NTP Server

```
  Option: NTP Server (56)
  Length: 61
  Value: 000100102a0100000000000000000000000000000010002010...
```

< NTP Server Address

```
  Suboption: NTP Server Address (1)
  Length: 16
  NTP Server Address: 2a01::1
```

< NTP Multicast Address

```
  Suboption: NTP Multicast Address (2)
  Length: 16
  NTP Multicast Address: ff05::101
```

< NTP Server FQDN

```
  Suboption: NTP Server FQDN (3)
  Length: 17
  NTP Server FQDN: ntp.example.com
```

< Option: (55) Parameter Request List

Length: 4

Parameter Request List Item: (1) Subnet Mask

Parameter Request List Item: (3) Router

Parameter Request List Item: (6) Domain Name Server

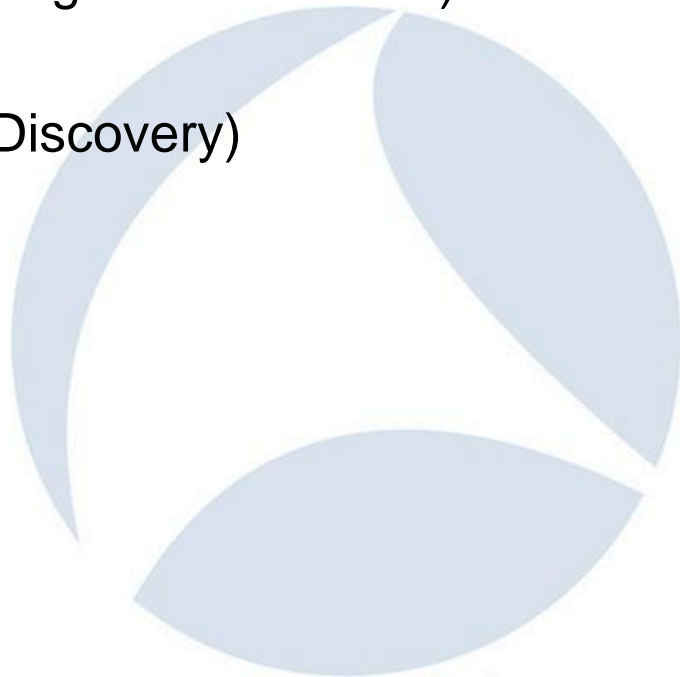
Parameter Request List Item: (42) Network Time Protocol Servers

> Option: (255) End

```
0000 00 0c 29 38 f3 68 00 0c 29 9b a1 5d 86 dd 60 00 ..)8.h.. )..]..`
0010 00 00 00 71 11 40 fe 80 00 00 00 00 00 00 02 0c ...q.@... ..
0020 29 ff fe 9b a1 5d fe 80 00 00 00 00 00 00 02 0c )....].. ..
0030 29 ff fe 38 f3 68 02 23 02 22 00 71 47 c1 07 f6 ).8.h.# ."qG...
0040 9b 57 00 01 00 0e 00 01 00 01 18 f0 0b 3f 00 0c .W.....?..
0050 29 38 f3 68 00 02 00 0e 00 01 00 01 18 ef 95 1b )8.h.... ..
0060 00 0c 29 9b a1 53 00 38 00 3d 00 01 00 10 2a 01 ...).S.8 .=....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 02 .....
0080 00 10 ff 05 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 01 01 00 03 00 11 03 6e 74 70 07 65 78 61 6d 70 .....n tp.examp
00a0 6c 65 03 63 6f 6d 00 le.com.
```

NTP and Multicast

- **IPv4 and IGMP**
(Internet Group Management Protocol)
- **IPv6 and MLD**
(Multicast Listener Discovery)



NTP and Multicast with IPv6

46	1111.944489	2001:6f8:900:8e6c:2013::132	ff05::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
47	1118.944227	fe80::46e4:d9ff:fee3:7754	ff02::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
48	1120.944103	2001:6f8:900:8e6c:2013::132	ff0e::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
49	1177.941269	2001:6f8:900:8e6c:2013::132	ff05::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
50	1183.940944	fe80::46e4:d9ff:fee3:7754	ff02::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
51	1184.940925	2001:6f8:900:8e6c:2013::132	ff0e::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
52	1243.937970	2001:6f8:900:8e6c:2013::132	ff05::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
53	1248.937753	2001:6f8:900:8e6c:2013::132	ff0e::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
54	1249.937669	fe80::46e4:d9ff:fee3:7754	ff02::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
55	1307.934788	2001:6f8:900:8e6c:2013::132	ff05::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
56	1313.934418	2001:6f8:900:8e6c:2013::132	ff0e::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
57	1313.934566	fe80::46e4:d9ff:fee3:7754	ff02::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
58	1372.931464	2001:6f8:900:8e6c:2013::132	ff05::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
59	1377.931213	2001:6f8:900:8e6c:2013::132	ff0e::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version
60	1377.931360	fe80::46e4:d9ff:fee3:7754	ff02::101	44:e4:d9:e3:77:54	33:33:00:00:01:01	NTP	110	NTP Version

FF02::101 means all NTP servers on the same link as the sender.

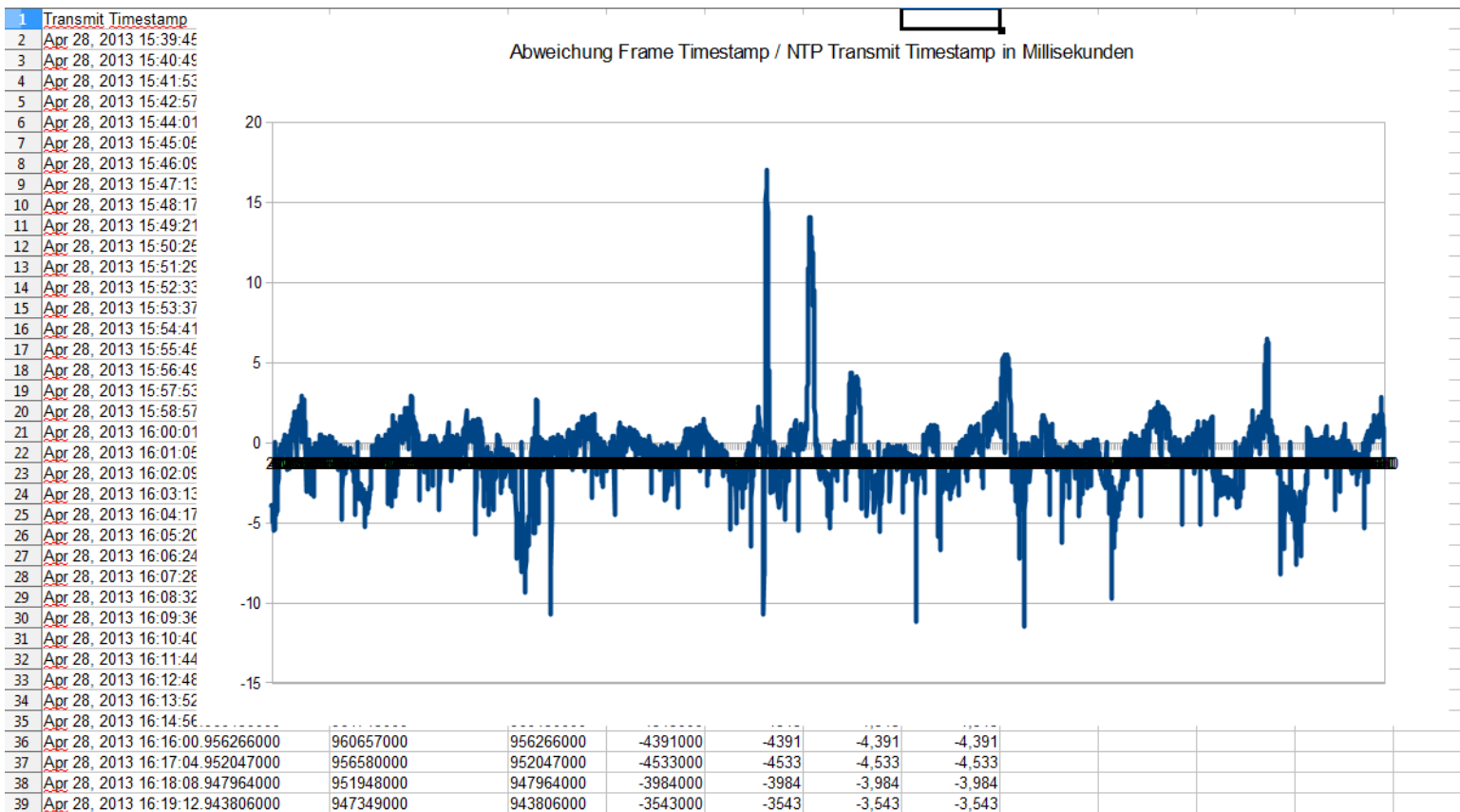
FF05::101 means all NTP servers in the same site as the sender.

FF0E::101 means all NTP servers in the Internet.

```
Frame 48: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on 0
Ethernet II, Src: 44:e4:d9:e3:77:54 (44:e4:d9:e3:77:54), Dst: 33:33:00:00:01:01 (33:33:00:00:01:01)
Internet Protocol Version 6, Src: 2001:6f8:900:8e6c:2013::132 (2001:6f8:900:8e6c:2013::132), Dst: ff0e::101 (ff0e::101)
  0110 .... = Version: 6
  .... 1110 0000 .... = Traffic class: 0x000000e0
  .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 56
  Next header: UDP (17)
  Hop limit: 255
  Source: 2001:6f8:900:8e6c:2013::132 (2001:6f8:900:8e6c:2013::132)
  Destination: ff0e::101 (ff0e::101)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
Network Time Protocol (NTP version 4, broadcast)
  Flags: 0x25
  Peer Clock Stratum: secondary reference (3)
  Peer Polling Interval: 6 (64 sec)
  Peer Clock Precision: 0,000000 sec
  Root Delay: 0,0555 sec
  Root Dispersion: 0,0323 sec
```

```
Frame 49: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on 0
Ethernet II, Src: 44:e4:d9:e3:77:54 (44:e4:d9:e3:77:54), Dst: 33:33:00:00:01:01 (33:33:00:00:01:01)
Internet Protocol Version 6, Src: 2001:6f8:900:8e6c:2013::132 (2001:6f8:900:8e6c:2013::132), Dst: ff05::101 (ff05::101)
  0110 .... = Version: 6
  .... 1110 0000 .... = Traffic class: 0x000000e0
  .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 56
  Next header: UDP (17)
  Hop limit: 255
  Source: 2001:6f8:900:8e6c:2013::132 (2001:6f8:900:8e6c:2013::132)
  Destination: ff05::101 (ff05::101)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
Network Time Protocol (NTP version 4, broadcast)
  Flags: 0x25
  Peer Clock Stratum: secondary reference (3)
  Peer Polling Interval: 6 (64 sec)
  Peer Clock Precision: 0,000000 sec
  Root Delay: 0,0555 sec
  Root Dispersion: 0,0332 sec
  Reference ID: 192.168.1.254
```

NTP Multicast versus frame.time



Time adjustment

- Time Shift for different capture file formats – sometimes needed
- File: “trace-over-1-week.converted-via-examine-into-pcap-format.pcap”

The screenshot displays the Wireshark interface with a packet capture file named "trace-over-1-week.converted-via-examine-into-pcap-format.pcap". The main pane shows a list of packets, with packet 9574 selected. The packet details pane shows the following information:

- Frame 9574: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
- Ethernet II, Src: Cisco_c6:83:d7 (00:14:1c:c6:83:d7), Dst: IPv4mcast
- Internet Protocol Version 4, Src: 192.168.5.254 (192.168.5.254), Dst: 224.0.1.1 (224.0.1.1)
- User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
- Network Time Protocol (NTP version 3, broadcast)
- Flags: 0x1d
- Peer Clock Stratum: secondary reference (3)
- Peer Polling Interval: 6 (64 sec)
- Peer Clock Precision: 0,000004 sec
- Root Delay: 0,0557 sec
- Root Dispersion: 0,0117 sec
- Reference ID: 192.168.1.254
- Reference Timestamp: May 5, 2013 17:43:38.628547000 UTC
- Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- Transmit Timestamp: May 5, 2013 17:50:16.598014000 UTC

The Time Shift dialog box is open, showing the following options:

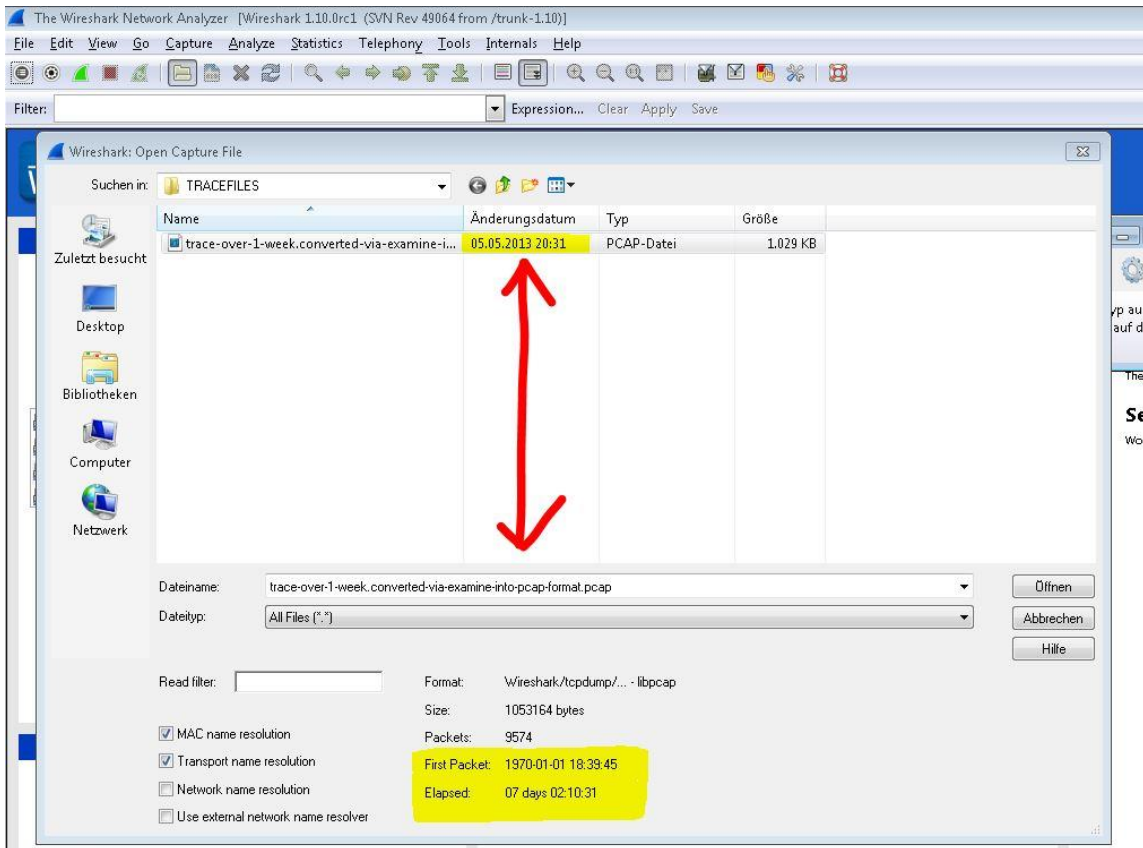
- Shift all packets
- Set packet to time
- Set packets to time and extrapolate

Under "Set packets to time and extrapolate", the following settings are shown:

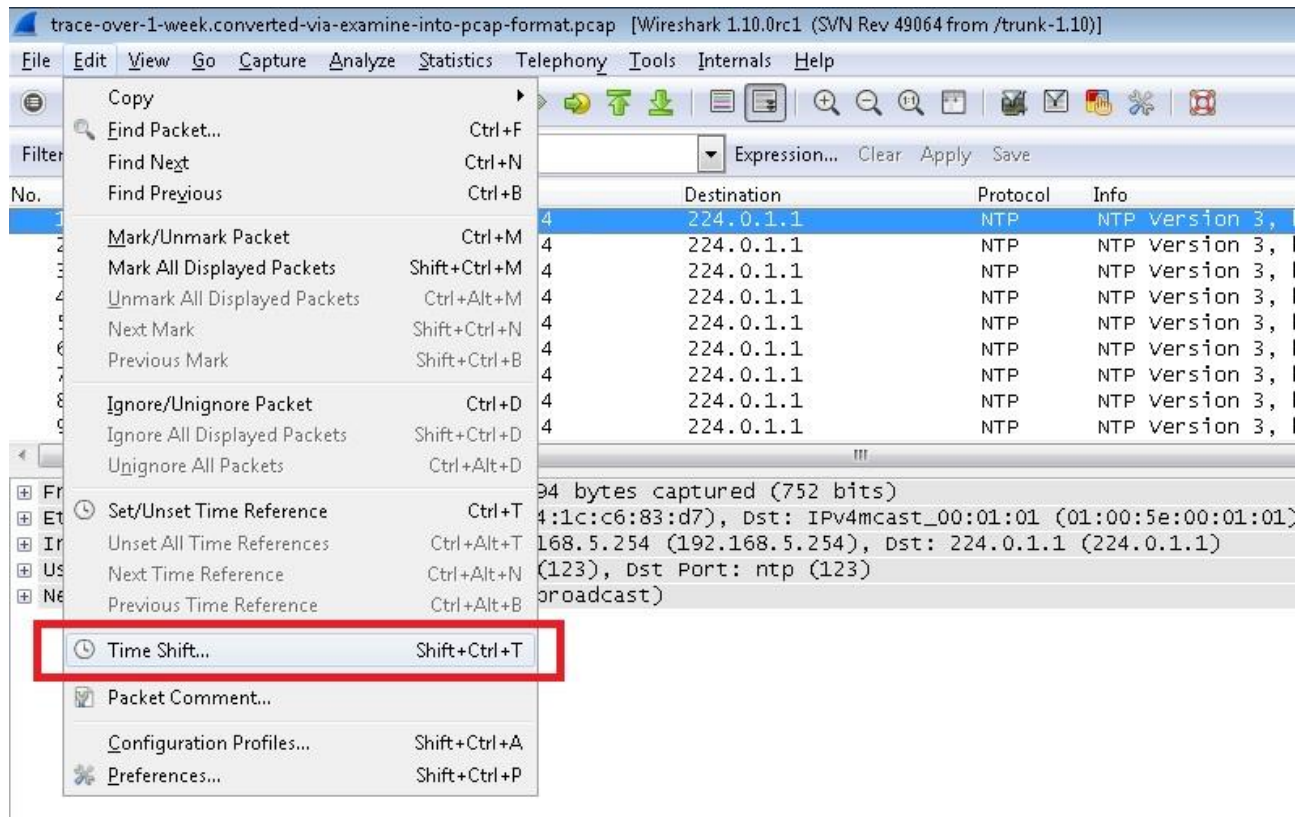
- Packet number: 1
- Set packet to time [YYYY-MM-DD] hh:mm:ss[.ddd]: 2013-04-28 15:39:45.099450000
- Packet number: 9574
- Set packet to time [YYYY-MM-DD] hh:mm:ss[.ddd]: 2013-05-05 17:50:16.598014000

The status bar at the bottom indicates the file size is 1053 KB and the profile is Default.

Time adjustment – Step 1



Time adjustment – Step 2



Time adjustment – Step 3

The image shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. Packet 1 is selected, and its details pane shows the following information:

- Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
- Ethernet II, Src: Cisco_C6:83:d7 (00:14:1c:c6:83:d7), Dst: IPv4mcast
- Internet Protocol Version 4, Src: 192.168.5.254 (192.168.5.254), Dst: 224.0.1.1 (224.0.1.1)
- User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
- Network Time Protocol (NTP Version 3, broadcast)
- Flags: 0x1d
- Peer Clock Stratum: secondary reference (3)
- Peer Polling Interval: 6 (64 sec)
- Peer Clock Precision: 0,000004 sec
- Root Delay: 0,0559 sec
- Root Dispersion: 0,0080 sec
- Reference ID: 192.168.1.254
- Reference Timestamp: May 5, 2013 17:43:38.628547000 UTC
- Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- Transmit Timestamp: Apr 28, 2013 15:39:45.099450000 UTC

The details pane for packet 9574 shows similar information, but with a different transmit timestamp: May 5, 2013 17:50:16.598014000 UTC.

The 'Wireshark: Time Shift' dialog box is open, showing the 'Set packets to time and extrapolate' option selected. The 'Packet number' field is set to 1. The 'Set packet to time' field is set to 2013-04-28 15:39:45.099450000. The 'Set packet to time' field is set to 2013-05-05 17:50:16.598014000.

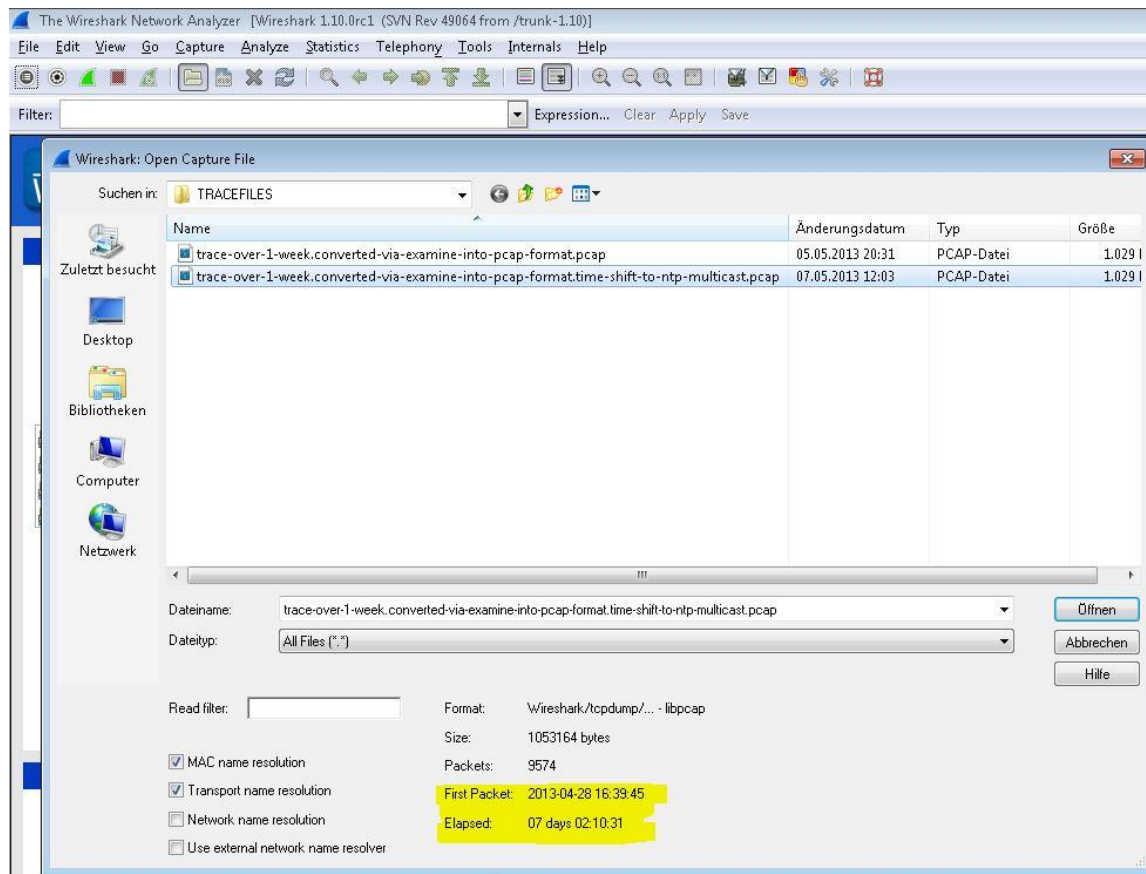
The packet list pane shows the following packets:

No.	LEN	Time	Source	Destination
1	94	0.000000000	192.168.5.254	224.0.1.1
2	94	63.995669000	192.168.5.254	224.0.1.1
3	94	63.995760000	192.168.5.254	224.0.1.1
4	94	63.995941000	192.168.5.254	224.0.1.1
5	94	63.996004000	192.168.5.254	224.0.1.1
6	94	63.996100000	192.168.5.254	224.0.1.1
7	94	63.996060000	192.168.5.254	224.0.1.1
8	94	63.994845000	192.168.5.254	224.0.1.1
9	94	63.995724000	192.168.5.254	224.0.1.1

The packet bytes pane shows the raw data for the selected packet:

```
0000 01 00 5e 00 01 01 00 14 1c c6 83 d7 08 00 45 c0 ..A.....E.
0010 00 4c 00 00 00 10 11 02 3a c0 a8 05 fe e0 00 .....{.8.....
0020 01 01 00 7b 00 7b 00 38 a9 93 1d 03 06 ee 00 00 .....{.8.....
0030 0e 50 00 00 02 0f c0 a8 01 fe d5 27 c1 02 1b a2 ..P.....
0040 3c 48 00 00 00 00 00 00 00 00 00 00 00 00 00 ..M.....
0050 00 00 05 27 c1 41 19 75 98 5c 0c a2 b8 48 .....Au...H
```


Time adjustment – Step 4



Time adjustment – Step 5

The image shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets, with packet 5840 selected. The packet details pane shows the following information:

- Encapsulation type: Ethernet (I)
- Arrival Time: May 3, 2013 00:27:35.990627000 Mitteleuropäis
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1367533655.990627000 seconds
- [Time delta from previous captured frame: 63.995872000 sec]
- [Time delta from previous displayed frame: 63.995872000 sec]
- [Time since reference or first frame: 373670.990627000 sec]
- Frame Number: 5840
- Frame Length: 94 bytes (752 bits)
- Capture Length: 94 bytes (752 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in Frame: eth:ip:udp:ntp]
- [Coloring rule Name: UDP]
- [Coloring rule string: udp]
- Ethernet II, Src: Cisco_c6:83:d7 (00:14:1c:c6:83:d7), Dst: IPv
- Internet Protocol Version 4, Src: 192.168.5.254 (192.168.5.254)
- User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
- Network Time Protocol (NTP version 3, broadcast)
- Flags: 0x1d
- Peer Clock Stratum: secondary reference (3)
- Peer Polling Interval: 6 (64 sec)
- Peer Clock Precision: 0,000004 sec
- Root Delay: 0,0597 sec
- Root Dispersion: 0,0061 sec
- Reference ID: 192.168.1.254
- Reference Timestamp: May 2, 2013 23:24:19.409702000 UTC
- origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
- Transmit Timestamp: May 2, 2013 23:27:36.392501000 UTC

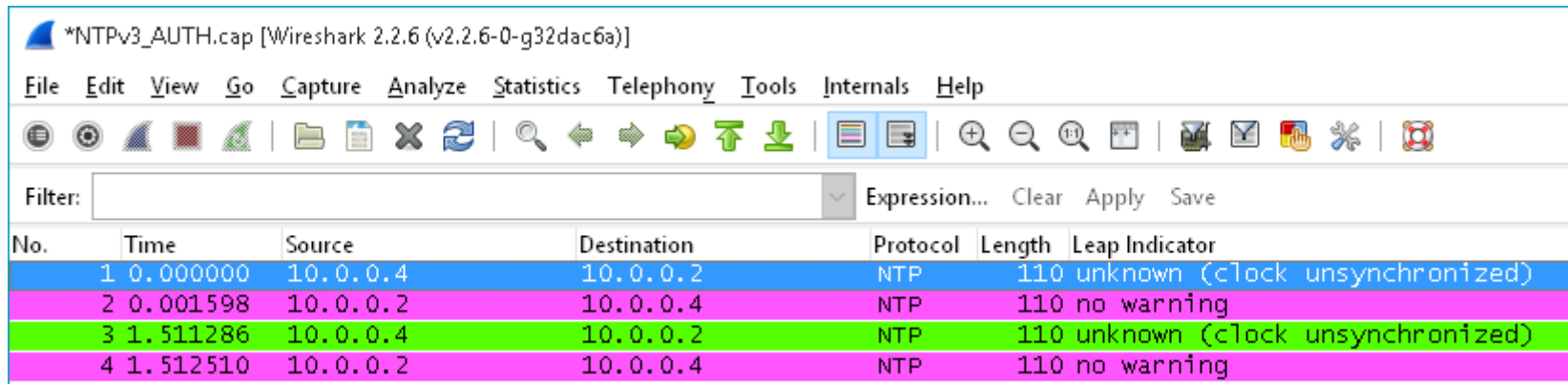
The packet bytes pane shows the raw hex and ASCII data for the selected packet.

The Summary pane on the right provides the following information:

- File:** Name: D:\TRACEFILES\trace-over-1-week.converted-via-examine-into-pcap-format.time-shift-to-ntp-multicast.pcap; Length: 1053164 bytes; Format: Wireshark/tcpdump/... - libpcap; Encapsulation: Ethernet; Packet size limit: 65535 bytes
- Time:** First packet: 2013-04-28 16:39:45; Last packet: 2013-05-05 18:50:16; Elapsed: 07 days 02:10:31
- Capture:** Interface: Dropped Packets Capture Filter Link type Packet size limit; unknown unknown unknown Ethernet 65535 bytes
- Display:** Display filter: none; Ignored packets: 0 (0,000%)
- Traffic:** Captured: 9574; Displayed: 9574; Displayed %: 100,000%; Marked: 0; Marked %: 0,000%
- Between first and last packet:** 612631,000 sec
- Avg. packets/sec:** 0,016
- Avg. packet size:** 94,000 bytes
- Bytes:** 899956; 899956; 100,000%; 0; 0,000%
- Avg. bytes/sec:** 1,469
- Avg. MBit/sec:** 0,000

NTP Coloring Rule

- Colors for various NTP message types



*NTPv3_AUTH.cap [Wireshark 2.2.6 (v2.2.6-0-g32dac6a)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Leap Indicator
1	0.000000	10.0.0.4	10.0.0.2	NTP	110	unknown (clock unsynchronized)
2	0.001598	10.0.0.2	10.0.0.4	NTP	110	no warning
3	1.511286	10.0.0.4	10.0.0.2	NTP	110	unknown (clock unsynchronized)
4	1.512510	10.0.0.2	10.0.0.4	NTP	110	no warning

- Wireshark Color Filters for NTP – useful!

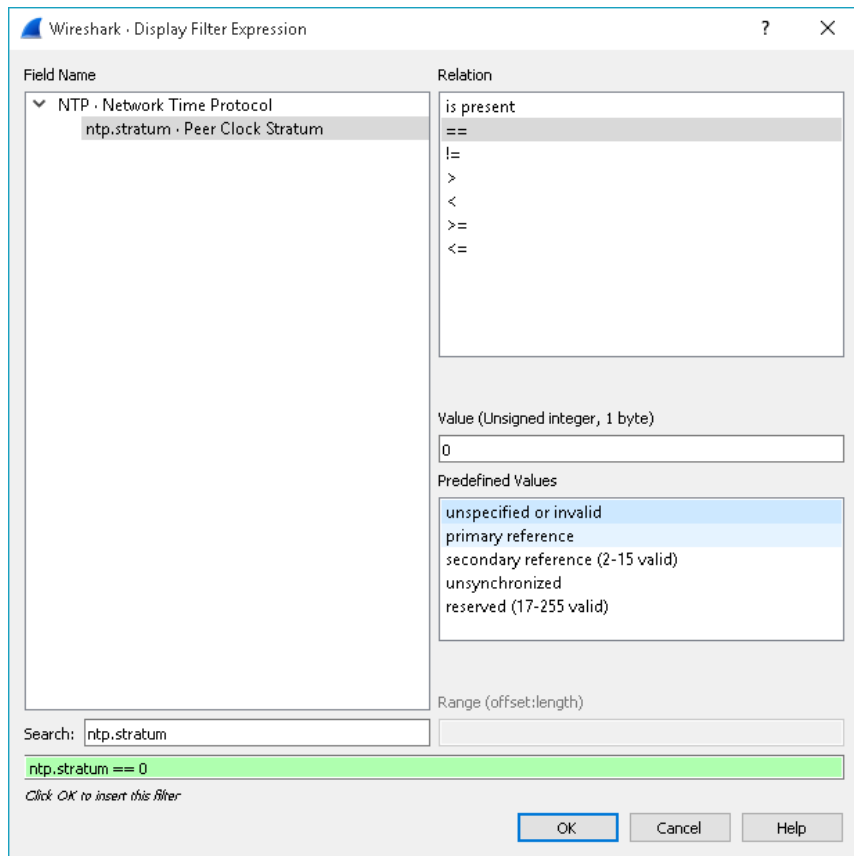
NTP Kiss-of-Death

- Kiss-of-Death packets are used by NTP servers to rate-limit NTP client requests that query too frequently
- Kiss of Death is a not a NTP protection protocol

```
Network Time Protocol (NTP Version 2, server)
  > Flags: 0xd4, Leap Indicator: unknown (clock unsynchronized), Version number:
Peer Clock Stratum: unspecified or invalid (0)
Peer Polling Interval: 4 (16 sec)
Peer Clock Precision: 0.015625 sec
Root Delay: 1.0000 sec
Root Dispersion: 1.0000 sec
Reference ID: Unidentified reference source 'RATE'
Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Origin Timestamp: Feb 7, 2036 06:28:15.999999000 UTC
Receive Timestamp: Feb 7, 2036 06:28:15.999999000 UTC
Transmit Timestamp: Feb 7, 2036 06:28:15.999999000 UTC
```

0000	00 25 64 a1 e8 25 c8 d3 a3 5e b7 55 08 00 45 b8	.%d..%.. ^.^..U..E.
0010	00 4c 00 00 40 00 3f 11 37 c8 c0 a8 81 65 c0 a8	.L..@.?. 7....e..
0020	00 6b 00 7b f9 c5 00 38 85 95 d4 00 04 fa 00 01	.k.{...8
0030	00 00 00 01 00 00 52 41 54 45 00 00 00 00 00 00RA TE.....
0040	00 00 ff ff ff ff ff ff ff 00 ff ff ff ff ff ff
0050	ff 00 ff ff ff ff ff ff ff 00

ntp.stratum - Peer Clock Stratum



- Stratum is a concept used in NTP and its value indicates the clocks location in the hierarchy
- While a lower stratum often indicates a more accurate clock
- BTW: 2^{256} seconds ?

ntp.refid - Reference ID

```
187  /* According to rfc, primary (stratum-0 and stratum-1) servers should set
188  * their Reference ID (4bytes field) according to following table:
189  */
190  static const struct {
191      const char *id;
192      const char *data;
193  } primary_sources[] = {
194      /* IANA / RFC 5905 */
195      { "GOES", "Geostationary Orbit Environment Satellite" },
196      { "GPS\0", "Global Position System" },
197      { "GAL\0", "Galileo Positioning System" },
198      { "PPS\0", "Generic pulse-per-second" },
199      { "IRIG", "Inter-Range Instrumentation Group" },
200      { "WWVB", "LF Radio WWVB Ft. Collins, CO 60 kHz" },
201      { "DCF\0", "LF Radio DCF77 Mainflingen, DE 77.5 kHz" },
202      { "HBG\0", "LF Radio HBG Prangins, HB 75 kHz" },
203      { "MSF\0", "LF Radio MSF Anthorn, UK 60 kHz" },
204      { "JJY\0", "LF Radio JJY Fukushima, JP 40 kHz, Saga, JP 60 kHz" },
205      { "LORC", "MF Radio LORAN C station, 100 kHz" },
206      { "TDF\0", "MF Radio Allouis, FR 162 kHz" },
207      { "CHU\0", "HF Radio CHU Ottawa, Ontario" },
208      { "WWV\0", "HF Radio WWV Ft. Collins, CO" },
209      { "WWVH", "HF Radio WWVH Kauai, HI" },
210      { "NIST", "NIST telephone modem" },
211      { "ACTS", "NIST telephone modem" },
212      { "USNO", "USNO telephone modem" },
213      { "PTB\0", "European telephone modem" },
214
215      /* Unofficial codes */
216      { "LOCL", "uncalibrated local clock" },
217      { "CESM", "calibrated Cesium clock" },
218      { "RBDN", "calibrated Rubidium clock" },
219      { "OMEG", "OMEGA radionavigation system" },
220      { "DCN\0", "DCN routing protocol" },
221      { "TSP\0", "TSP time protocol" },
222      { "DTS\0", "Digital Time Service" },
223      { "ATOM", "Atomic clock (calibrated)" },
224      { "VLF\0", "VLF radio (OMEGA,, etc.)" },
225      { "1PPS", "External 1 PPS input" },
226      { "FREE", "(Internal clock)" },
227      { "INIT", "(Initialization)" },
228      { "\0\0\0\0", "NULL" },
229      { NULL, NULL }
230  };
```

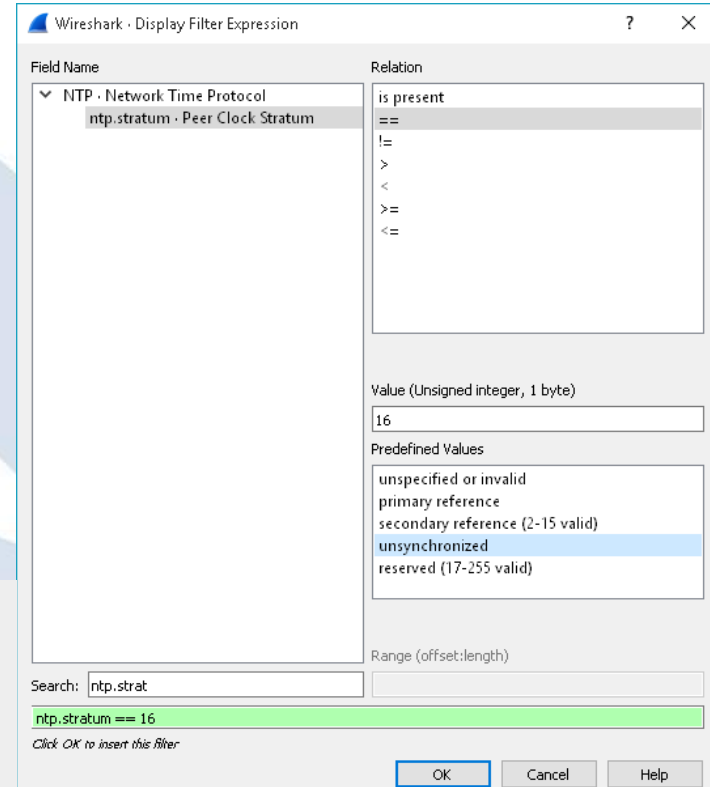
- Research in the source code – some interesting info
- Use a ASCII2HEX converter for your display filter 😊

packet-ntp.c

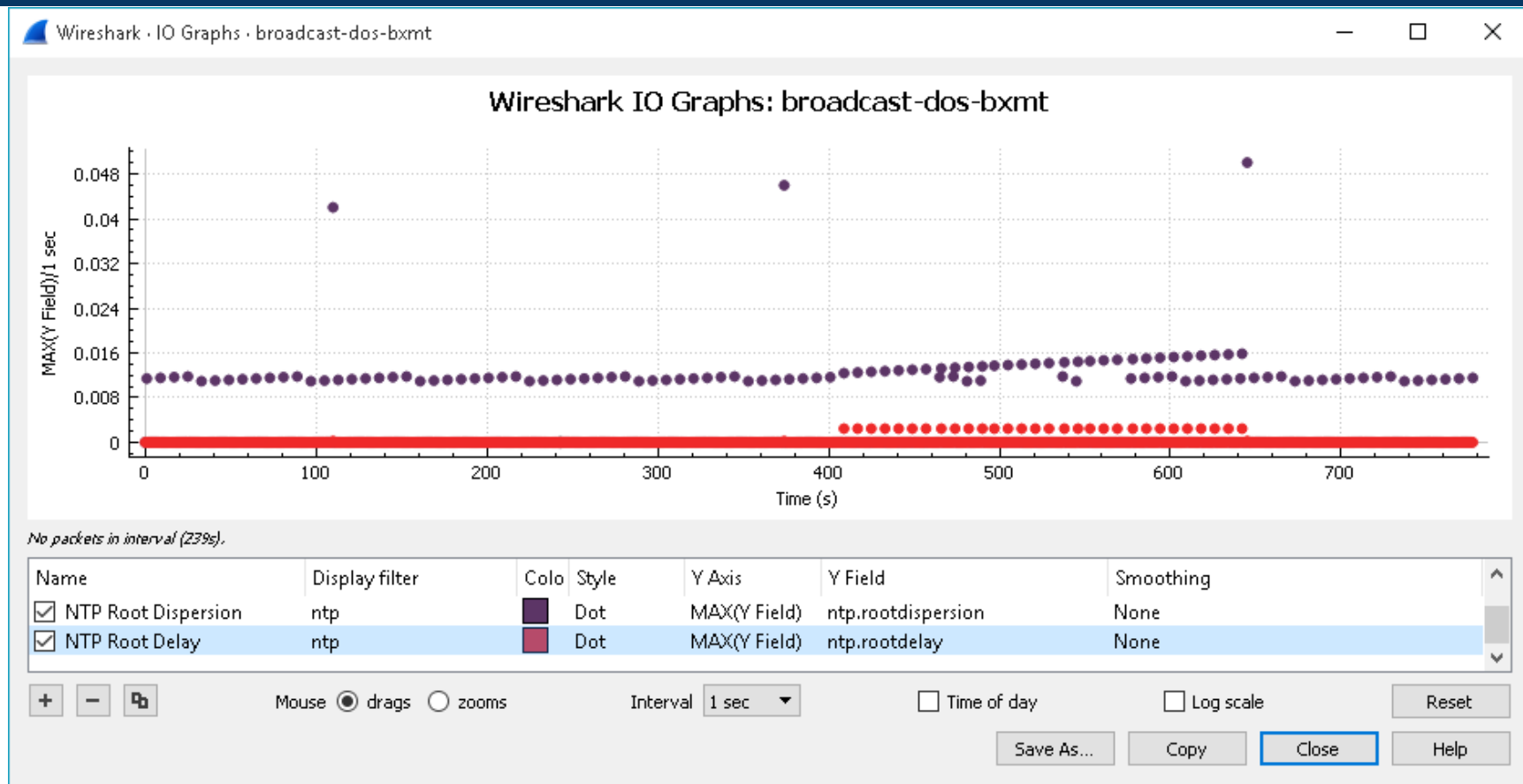
NTP Stratum

- Stratum levels define the distance from the reference clock
- A NTP server that is directly connected to a stratum-0 device is called a stratum-1 server
- NTP clients need some way of judging which time sources are likely to be the most accurate and preventing timing loops
- An NTP client synchronized from a Stratum 4 source would be a Stratum 5 device

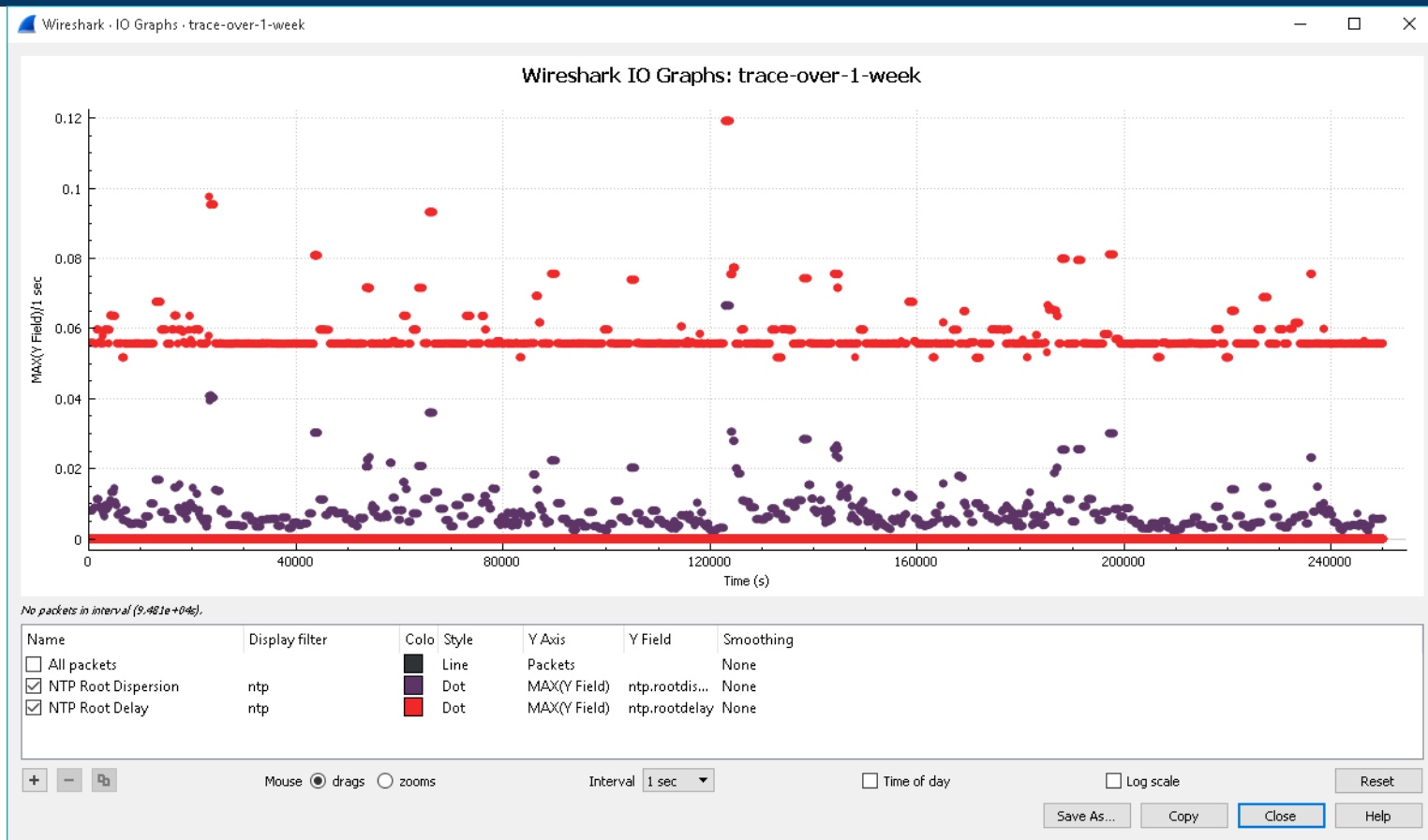
```
# ntpq -pn
      remote           refid       st t when poll reach  delay  offset  jitter
=====
*127.127.20.1    .GPS.             0 1  52  64  377   0.000   0.516   0.011
o127.127.22.0    .PPS.             0 1   3  16  377   0.000  -0.001   0.001
```



NTP Root Delay / Dispersion Monitoring / IO-Graph



NTP Root Delay / Dispersion Monitoring / IO-Graph



NTP Leap Seconds

- Leap seconds are scheduled to be inserted into or deleted from the UTC time scale in irregular intervals to keep the UTC time scale synchronized with the Earth rotation

▸ Network Time Protocol (NTP Version 4, server)

```
▸ Flags: 0x64, Leap Indicator: last minute of the day has 61 seconds, Version number: NTP Version 4, Mode: server
01.. .... = Leap Indicator: last minute of the day has 61 seconds (1)
..10 0... = Version number: NTP Version 4 (4)
100 = Mode: server (4)
```

▸ Network Time Protocol (NTP Version 4, symmetric active)

```
▸ Flags: 0xe1, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 4, Mode: symmetric active
11.. .... = Leap Indicator: unknown (clock unsynchronized) (3)
..10 0... = Version number: NTP Version 4 (4)
.... .001 = Mode: symmetric active (1)
```

```
Peer Clock Stratum: unspecified or invalid (0)
```

```
[9767716.320000] device br-lan entered promiscuous mode
[9890041.560000] Clock: inserting leap second 23:59:60 UTC
[24182566.210000] device br-lan left promiscuous mode
```

NTP Leap Seconds Smearing

- Workaround for systems get confused if the time is stepped back
- Duplicate timestamps can occur

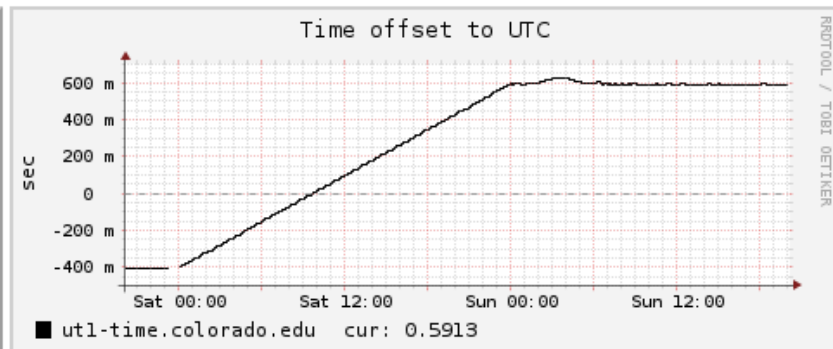
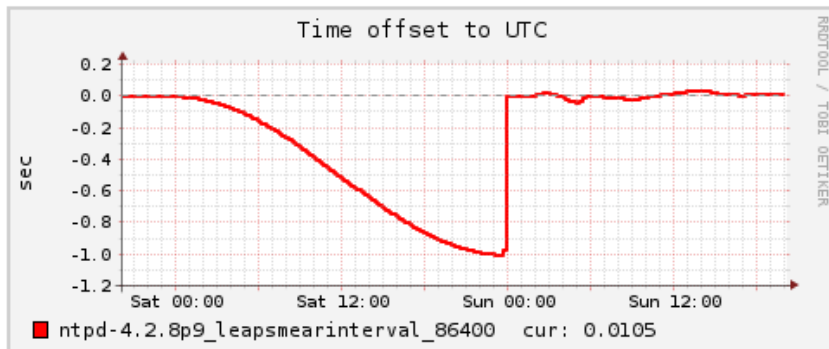
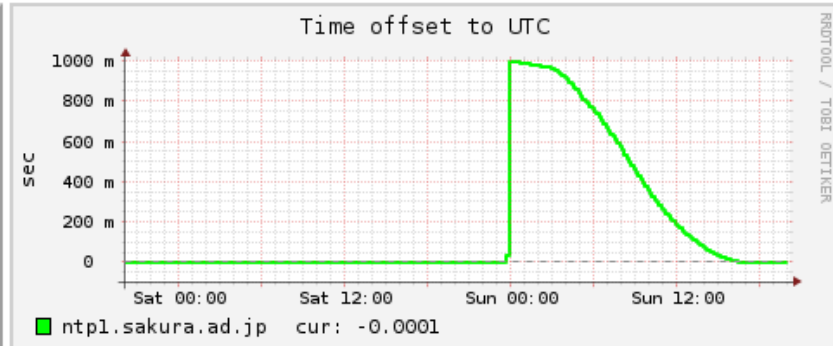
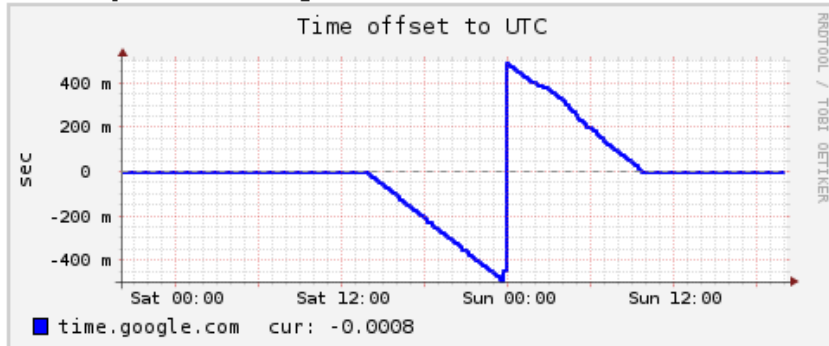
```
PS C:\Users\Administrator.LAB> w32tm.exe /query /status
Leap Indicator: 1(last minute has 59 seconds)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.1689984s
Root Dispersion: 11.9969834s
ReferenceId: 0x0D500C36 (source IP: 13.80.12.54)
Last Successful Sync Time: 31.12.2016 19:52:52
Source: time.windows.com,0x8
Poll Interval: 6 (64s)

PS C:\Users\Administrator.LAB>
```

NTP Leap Smearing Monitoring



Note: Leap smear monitoring has been finished at 2017-01-01T2000Z.



Watching NTP leap second with tshark

- `tshark -ni eth0 port 123 -R ntp.flags.mode==4 -Eheader=y -Tfields \`
`-e frame.time \`
`-e ntp.flags.li \`
`-e ntp.xmt`

```
frame.time ntp.flags.li ntp.xmt
Jun 30, 2015 14:48:01.772791000 1 d9:3d:1c:91:c6:04:86:7b
Jun 30, 2015 14:48:19.772441000 1 d9:3d:1c:a3:c5:e8:b2:2d
Jun 30, 2015 14:48:34.772810000 1 d9:3d:1c:b2:c5:fa:f6:4f
Jun 30, 2015 14:48:51.772300000 1 d9:3d:1c:c3:c5:d5:7d:c4
Jun 30, 2015 14:49:09.772914000 1 d9:3d:1c:d5:c5:fb:a2:93
```

Reference:

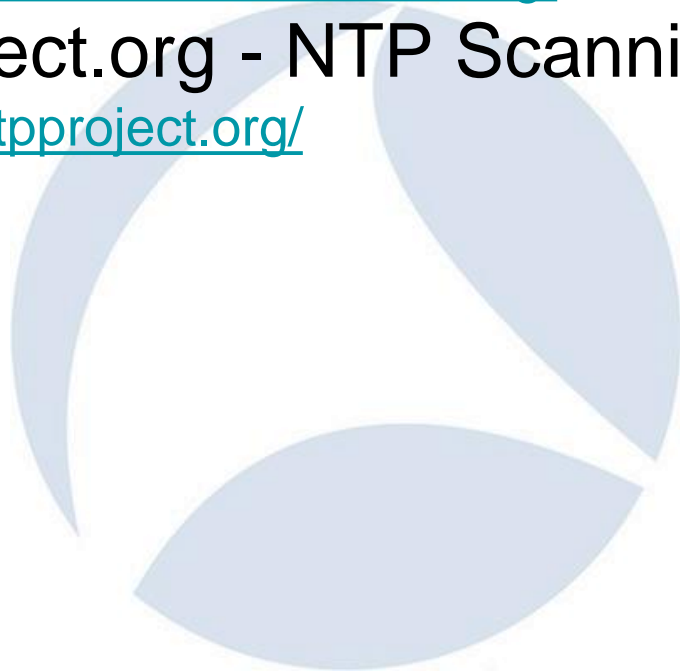
<http://www.theptpguy.net/posts/2015/06/30/watching-the-leap-second-with-tshark>

NTP to calibrate your capture file

- Tipp: Use Multicast NTP when possible
- Compare frame.time versus transmit timestamp
<https://isc.sans.edu/forums/diary/What+Time+Is+It+Using+NTP+Traffic+to+Calibrate+PCAP+Timestamps/21135/>

Public NTP Scanning Websites

- Open NTP Monitor (Mode 7) Scanning Project
 - <https://ntpmonitorscan.shadowserver.org/>
- OpenNTPProject.org - NTP Scanning Project
 - <http://www.openntpproject.org/>



NTP Mode 6

- Using Nmap – the easiest way 😊

- Mode 6

- `nmap -sU -pU:123 -Pn -n --script=ntp-info <IP>`

- ▼ Network Time Protocol (NTP Version 2, control)

- ▼ Flags: 0x16, Leap Indicator: no warning, Version number: NTP Version 2, Mode: reserved for NTP control message
 - 00.. = Leap Indicator: no warning (0)
 - ..01 0... = Version number: NTP Version 2 (2)
 -110 = Mode: reserved for NTP control message (6)
 - ▼ Flags 2: 0x02, Response bit: Request, Opcode: READVAR
 - 0... = Response bit: Request (0)
 - .0.. = Error bit: 0
 - ..0. = More bit: 0
 - ...0 0010 = Opcode: READVAR (2)

Sequence: 1

Status: 0x0000

AssociationID: 0

Offset: 0

Count: 0

NTP Mode 7

- Mode 7 with Nmap

- `nmap -sU -pU:123 -Pn -n --script=ntp-monlist <IP>`

- ▼ Network Time Protocol (NTP Version 2, private)

- ▼ Flags: 0x17, Response bit: Request, Version number: NTP Version 2, Mode: reserved for private use

- 0... = Response bit: Request (0)

- .0.. = More bit: 0

- ..01 0... = Version number: NTP Version 2 (2)

-111 = Mode: reserved for private use (7)

- ▼ Auth, sequence: 23

- 0... = Auth bit: 0

- .001 0111 = Sequence number: 23

- Implementation: XNTPD (3)

- Request code: MON_GETLIST_1 (42)

- 0000 = Err: No error (0x00)

- 0000 0000 0000 = Number of data items: 0

- 0000 = Reserved: 0x00

- 0000 0000 0000 = Size of data item: 0x0000

NTP Mode 7 - Replies

- ```

Network Time Protocol (NTP Version 2, control)
 Flags: 0x16, Leap Indicator: no warning, Version number: NTP Version 2, Mode: reserved for NTP control message
 00.. = Leap Indicator: no warning (0)
 ..01 0... = Version number: NTP Version 2 (2)
 110 = Mode: reserved for NTP control message (6)
 Flags 2: 0x82, Response bit: Response, Opcode: READVAR
 1... = Response bit: Response (1)
 .0.. = Error bit: 0
 ..0. = More bit: 0
 ...0 0010 = Opcode: READVAR (2)
 Sequence: 1
 Status: 0x0618, Leap Indicator: no warning, Clock Source: UDP/NTP, System Event Code: Unknown
 00.. = Leap Indicator: no warning (0)
 ..00 0110 = Clock Source: UDP/NTP (6)
 0001 = System Event Counter: 1
 1000 = System Event Code: Unknown (8)
 AssociationID: 0
 Offset: 0
 Count: 378
 Data
 > version="ntpd 4.2.8p9@1.3265-o Tue Dec 20 10:59:17 UTC 2016 (1)"
 > processor="mips"
 > system="Linux/4.4.14"
 > leap=0
 > stratum=3
 > precision=-17
 > rootdelay=57.997
 > rootdisp=44.302
 > refid=192.168.1.253
 > reftime=0xdceb9f7e.da5272e4
 > clock=0xdceba1ca.2b91884d
 > peer=64052
 > tc=10
 > mintc=3
 > offset=-1.389020
 > frequency=4.385
 > sys_jitter=1.700985
 > clk_jitter=1.085
 > clk_wander=0.034

Network Time Protocol (NTP Version 2, control)
 Flags: 0x16, Leap Indicator: no warning, Version number: NTP Version 2, Mode: reserved for NTP control message
 00.. = Leap Indicator: no warning (0)
 ..01 0... = Version number: NTP Version 2 (2)
 110 = Mode: reserved for NTP control message (6)
 Flags 2: 0x82, Response bit: Response, Opcode: READVAR
 1... = Response bit: Response (1)
 .0.. = Error bit: 0
 ..0. = More bit: 0
 ...0 0010 = Opcode: READVAR (2)
 Sequence: 1
 Status: 0x0600, Leap Indicator: no warning, Clock Source: UDP/NTP, System Event Code: unspecified
 00.. = Leap Indicator: no warning (0)
 ..00 0110 = Clock Source: UDP/NTP (6)
 0000 = System Event Counter: 0
 0000 = System Event Code: unspecified (0)
 AssociationID: 0
 Offset: 0
 Count: 213
 Data
 > system="cisco"
 > leap=0
 > stratum=2
 > rootdelay=59.27
 > rootdispersion=20.66
 > peer=62791
 > refid=131.234.137.64
 > reftime=0xDCEBA541.38C3A5FC
 > poll=10
 > clock=0xDCEBA931.25971874
 > phase=0.757
 > freq=-5.89
 > error=9.89

```

# NTP Control Clock Source / ntp.ctrl.sys\_status.clksrc

- Different Kind of sources for NTP available

Value (Unsigned integer, 2 bytes)

0

Predefined Values

unspecified or unknown

Calibrated atomic clock (e.g. HP 5061)

VLF (band 4) or LF (band 5) radio (e.g. OMEGA, WWVB)

HF (band 7) radio (e.g. CHU, MSF, WWV/H)

UHF (band 9) satellite (e.g. GOES, GPS)

local net (e.g. DCN, TSP, DTS)

UDP/NTP

UDP/TIME

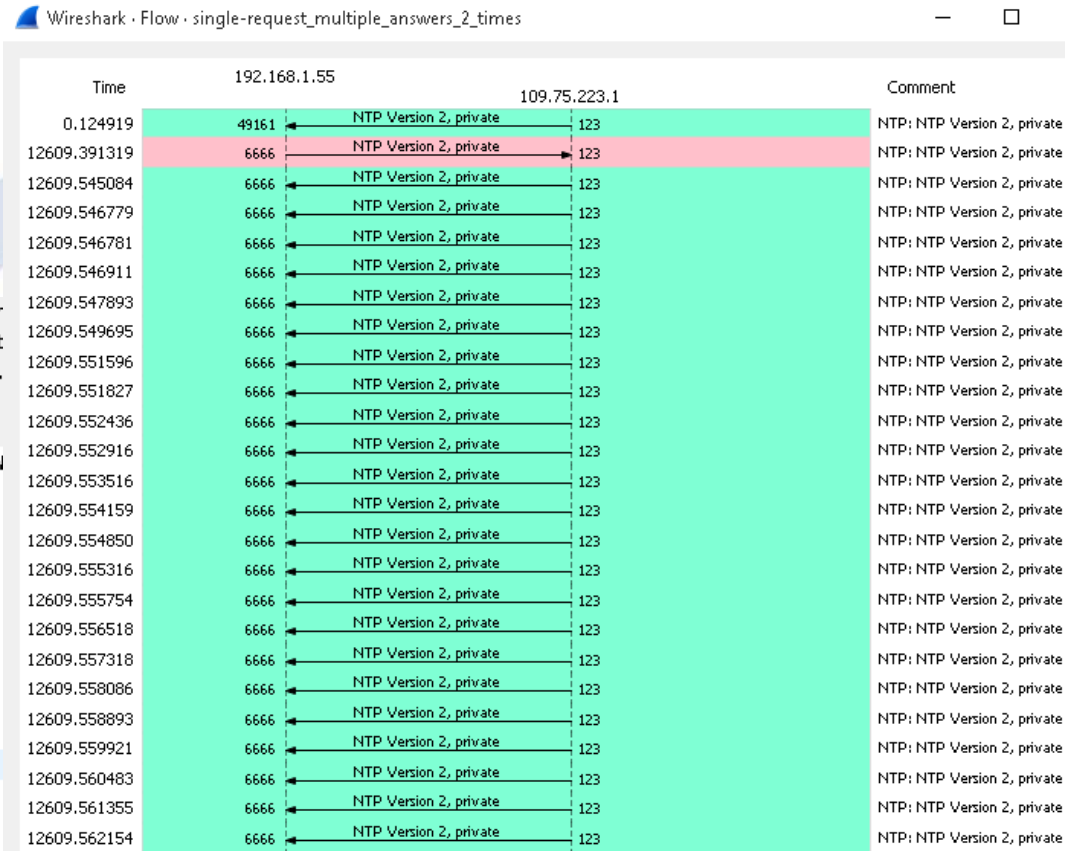
eyeball-and-wristwatch

telephone modem (e.g. NIST)

# NTP Amplification Attack / Reflection DDoS attacks

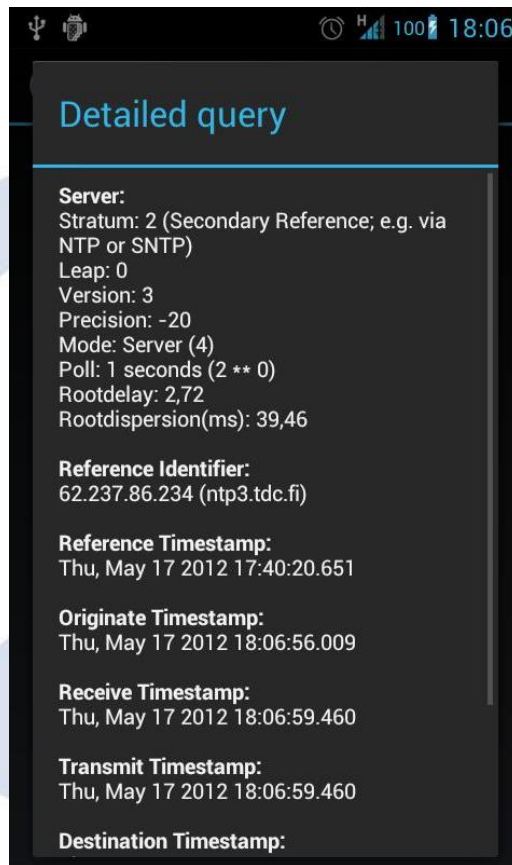
- One single request
- Flooding different Monlist items

```
> Frame 87: 482 bytes on wire (3856 bits), 482 bytes captured
> Ethernet II, Src: Cisco_05:9f:0b (00:50:73:05:9f:0b), Dst
> Internet Protocol Version 4, Src: 109.75.223.1, Dst: 192.
> User Datagram Protocol, Src Port: 123, Dst Port: 6666
▼ Network Time Protocol (NTP Version 2, private)
 > Flags: 0xd7, Response bit: Response, Version number: N
 > Auth, sequence: 215
 Implementation: XNTPD (3)
 Request code: MON_GETLIST_1 (42)
 0000 = Err: No error (0x00)
 0000 0000 0110 = Number of data items: 6
 0000 = Reserved: 0x00
 0000 0100 1000 = Size of data item: 0x0048
 > Monlist item: address: 217.7.239.199:35005
 > Monlist item: address: 31.19.17.89:40540
 > Monlist item: address: 109.234.60.27:123
 > Monlist item: address: 74.183.220.60:50177
 > Monlist item: address: 84.23.80.31:51254
 > Monlist item: address: 79.241.128.143:64345
```



# NTP APPs for your Smartphone

- Different kinds of APPs are available for different platforms
- Useful for checking your capture setup and results too 😊



# NTP Polling Intervals - RFCs and the Windows Way

| Windows version        | NTP.MAXPOLL:<br>Domain controllers | NTP.MAXPOLL:<br>Member /Standalone machines | NTP.MINPOLL:<br>Domain controllers | NTP.MINPOLL:<br>Member/Standalone machines |
|------------------------|------------------------------------|---------------------------------------------|------------------------------------|--------------------------------------------|
| Windows XP             | 15                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2003    | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Vista          | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2008    | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows 7              | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2008 R2 | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows 8              | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2012    | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows 8.1            | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2012 R2 | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows 10             | 10                                 | 15                                          | 6                                  | 10                                         |
| Windows Server 2016    | 10                                 | 15                                          | 6                                  | 10                                         |

- **RFC 1305**
  - NTP.MAXPOLL 1024 seconds, which was the maximum with NTPv3
- **RFC 5905**
  - poll intervals up to 36 hours

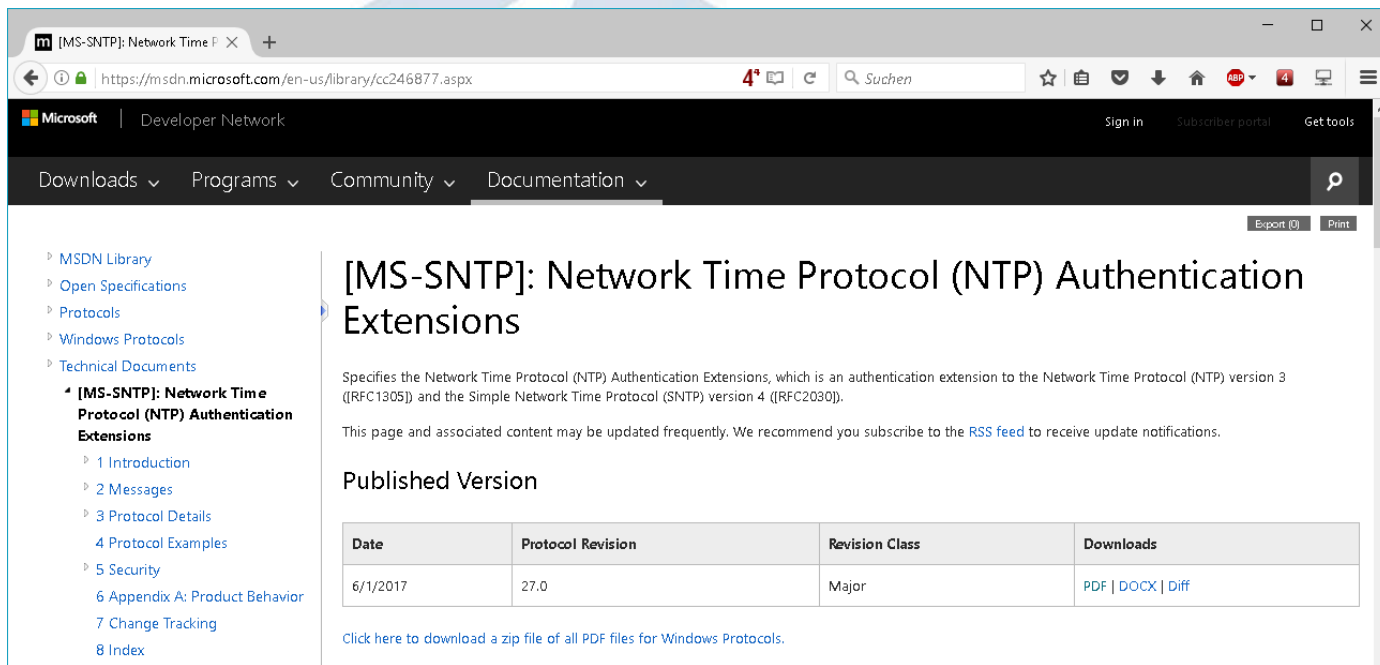
# Windows Accurate Time

- Is your Windows Capture Engine part of a domain?

The screenshot shows a web browser window displaying a Microsoft documentation page. The address bar shows the URL: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/windows-time-service/windows-2016-accurate-time>. The page header includes the Microsoft logo and navigation links for Technologies, Documentation, and Resources. Below the header is the Windows IT Center navigation bar with links for Explore, Docs, Downloads, Scripts, and Support. The breadcrumb trail reads: Docs / Windows Server / Identity and access. A search filter box is present. The main content area features the title "Windows Server 2016 Accurate Time" with a date of 2016-12-21, a reading time of 37 minutes, and contributor avatars. A sub-section titled "Applies To: Windows Server 2016" is visible. The "Introduction" section begins with the text: "Time synchronization accuracy in Windows Server 2016 has been improved substantially, while maintaining full backwards NTP compatibility with older Windows versions. Under reasonable operating conditions you can maintain a 1 ms accuracy with respect to UTC or better for Windows Server 2016 and Windows 10 Anniversary domain members. The following whitepaper discusses these topics as they relate to enabling accurate time:"

# MS-SNTP Extensions

- Microsoft has a custom authentication mechanism in their NTP implementation of the Windows Time Service



The screenshot shows a web browser window displaying the MSDN Library page for "[MS-SNTP]: Network Time Protocol (NTP) Authentication Extensions". The page title is "[MS-SNTP]: Network Time Protocol (NTP) Authentication Extensions". The URL is <https://msdn.microsoft.com/en-us/library/cc246877.aspx>. The page content includes a description of the Network Time Protocol (NTP) Authentication Extensions, which is an authentication extension to the Network Time Protocol (NTP) version 3 (RFC1305) and the Simple Network Time Protocol (SNTP) version 4 (RFC2030). The page also includes a section for the "Published Version" with a table showing the date, protocol revision, revision class, and download links.

**[MS-SNTP]: Network Time Protocol (NTP) Authentication Extensions**

Specifies the Network Time Protocol (NTP) Authentication Extensions, which is an authentication extension to the Network Time Protocol (NTP) version 3 (RFC1305) and the Simple Network Time Protocol (SNTP) version 4 (RFC2030).

This page and associated content may be updated frequently. We recommend you subscribe to the [RSS feed](#) to receive update notifications.

**Published Version**

| Date     | Protocol Revision | Revision Class | Downloads                                                         |
|----------|-------------------|----------------|-------------------------------------------------------------------|
| 6/1/2017 | 27.0              | Major          | <a href="#">PDF</a>   <a href="#">DOCX</a>   <a href="#">Diff</a> |

[Click here to download a zip file of all PDF files for Windows Protocols.](#)



# MS-SNTP Extensions - Wireshark

- Decoding with Wireshark not implemented yet ;-)

- Network Time Protocol (NTP Version 3, server)
  - Flags: 0x1c, Leap Indicator: no warning, Version number: NTP Version 3, Mode: server
  - Peer Clock Stratum: secondary reference (2)
  - Peer Polling Interval: 10 (1024 sec)
  - Peer Clock Precision: 0.015625 sec
  - Root Delay: 0.0313 sec
  - Root Dispersion: 0.0515 sec
  - Reference ID: 192.53.103.104
  - Reference Timestamp: May 15, 2017 08:17:12.726792000 UTC
  - Origin Timestamp: May 15, 2017 08:29:38.204909000 UTC
  - Receive Timestamp: May 15, 2017 08:29:38.226792000 UTC
  - Transmit Timestamp: May 15, 2017 08:29:38.226792000 UTC
- Extension
  - [Expert Info (Warning/Protocol): Extension length 0 < 8]
  - [Extension length 0 < 8]
  - [Severity level: Warning]
  - [Group: Protocol]

```
0000 ec f4 bb 1e 59 7e 20 4c 9e a6 5f 46 08 00 45 00 Y~ L .._F..E.
0010 00 94 5c d5 00 00 7e 11 44 23 0a c0 7e 0d 0a 80 ..\...~. D#...~...
0020 08 14 00 07 b0 00 80 15 b9 1c 02 0a fa 00 00 ...{.{..
0030 08 00 00 00 0d 2f c0 35 67 68 dc c3 e2 88 ba 0f /.5 gh.....
0040 14 6f dc c3 e5 72 34 74 f9 a7 dc c3 e5 72 3a 0f .o...r4tr:.
0050 14 6f dc c3 e5 72 3a 0f 14 6f b5 1d 00 00 01 00 .o...r:. .o.....
0060 00 00 7f 72 74 7f e2 ab d1 94 0f 01 c6 f4 8c 0d ...rt...
0070 03 30 0b 21 d5 85 b8 66 0d 4a 44 5c ef ec b6 ee .0!...f .JD\....
0080 26 1a cf 97 23 a9 2d 4f 03 09 fb b0 5f 82 28 63 &...#.-O_(c
0090 7e 68 e6 15 15 d4 3b 6c 6c 6d 92 46 0e bf 29 2a ~h....;l lm.F..)*
00a0 3a d3 ..
```

# MS-SNTP Extensions – MS Message Analyzer

| Name                | Value                                                                         | Bit Offset | Bit Length | Type                      |
|---------------------|-------------------------------------------------------------------------------|------------|------------|---------------------------|
| Leap                | no warning (0x00)                                                             | 0          | 2          | Leap                      |
| Version             | 3 (0x03)                                                                      | 2          | 3          | Byte                      |
| Mode                | server (0x04)                                                                 | 5          | 3          | Mode                      |
| Stratum             | secondary server(via NTP) (0x02)                                              | 8          | 8          | Stratum                   |
| Poll                | 10 (0x0A)                                                                     | 16         | 8          | SByte                     |
| Precision           | -6 (0xFA)                                                                     | 24         | 8          | SByte                     |
| RootDelay           | 2048 (0x00000800)                                                             | 32         | 32         | Int32                     |
| RootDispersion      | 3375 (0x00000D2F)                                                             | 64         | 32         | UInt32                    |
| ReferenceIdentifier | 192.53.103.104                                                                | 96         | 32         | Utility.IPv4Address       |
| ReferenceTimestamp  | 05.15.2017 10:17:12.7270000 +02:00 (0xDCC3E288BA0F146F)                       | 128        | 64         | UInt64                    |
| OriginateTimestamp  | 05.15.2017 10:29:38.2050000 +02:00 (0xDCC3E5723474F9A7)                       | 192        | 64         | UInt64                    |
| ReceiveTimestamp    | 05.15.2017 10:29:38.2270000 +02:00 (0xDCC3E5723A0F146F)                       | 256        | 64         | UInt64                    |
| TransmitTimestamp   | 05.15.2017 10:29:38.2270000 +02:00 (0xDCC3E5723A0F146F)                       | 320        | 64         | UInt64                    |
| ExtensionField      | ExtendedAuthenticator{KeyIdentifier=KeyIdentifierFlags{Rid=1519288320,Sign... | 384        | 576        | NTP.ExtendedAuthenticator |
| KeyIdentifier       | KeyIdentifierFlags{Rid=1519288320,Sign=0}                                     | 384        | 32         | NTP.KeyIdentifierFlags    |
| Rid                 | (10110101000111010000000000000000.) 1519288320 (0x5A8E8000)                   | 384        | 31         | Int32                     |
| Sign                | (.....0) (0x00000000)                                                         | 415        | 1          | Int32                     |
| Reserved            | 1 (0x01)                                                                      | 416        | 8          | Byte                      |
| Flags               | 0 (0x00)                                                                      | 424        | 8          | Byte                      |
| ClientHashIDHints   | 0 (0x00)                                                                      | 432        | 8          | Byte                      |
| SignatureHashID     | 0 (0x00)                                                                      | 440        | 8          | Byte                      |
| CryptoChecksum      | Blob{Data=binary[127,114,116,127,226,171,209,148,15,1,198,244,140,13,3,48,... | 448        | 512        | Utility.Blob              |
| Data                | binary[127,114,116,127,226,171,209,148,15,1,198,244,140,13,3,48,11,33,213,... | 448        | 512        | BinaryValue               |

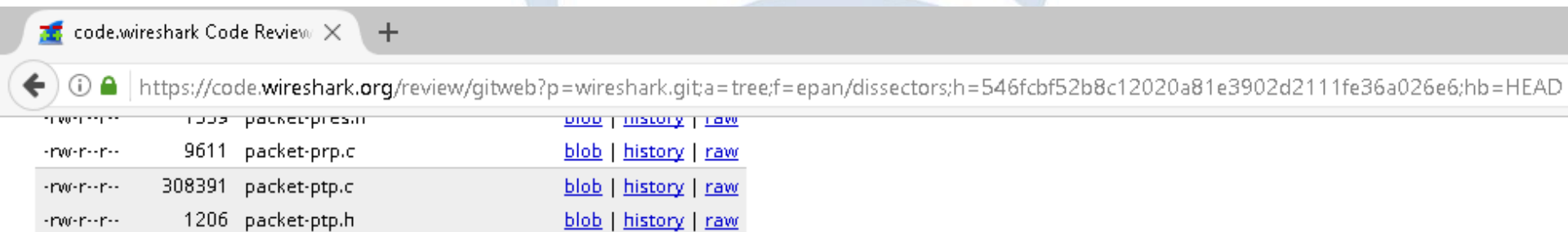
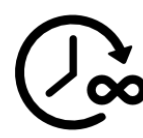
# Windows w32tm as a NTP client for testing

```
C:\Windows\system32\cmd.exe - w32tm.exe /stripchart /computer:192.168.0.107

C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>
C:\Users\wfischer>w32tm.exe /stripchart /computer:192.168.0.107
Tracking 192.168.0.107 [192.168.0.107:123].
The current time is 17.06.2017 14:11:35.
14:11:35 d:+00.00612579s o:+00.00122560s [*]
14:11:37 d:+00.00420193s o:+00.0010318s [*]
14:11:39 d:+00.00507323s o:+00.00070941s [*]
14:11:41 d:+00.00471529s o:+00.00045452s [*]
14:11:43 d:+00.00418638s o:+00.0011184s [*]
14:11:45 d:+00.00515372s o:+00.00068675s [*]
14:11:47 d:+00.00457182s o:+00.00049659s [*]
14:11:49 d:+00.00423317s o:+00.0015196s [*]
14:11:51 d:+00.00529866s o:+00.00076339s [*]
14:11:54 d:+00.00502840s o:+00.00043264s [*]
14:11:56 d:+00.00471392s o:+00.00045586s [*]
```

# AGENDA

- Time basic
- Time Protocols
- NTP
- **PTP**
- Wrap-UP



# IEEE 1588 Precision Time Protocol (PTP)

- IEEE 1588 Precision Time Protocol (PTP) is a highly accurate distributed time synchronization protocol for packet network
- IEEE 1588-2008, as known as IEEE 1588v2 or PTPv2 is the latest IEEE 1588 standard
  - Can direct map to Ethernet, or UDP IPv4.
  - Packet based timing distribution and synchronization.
  - Nanosecond to sub-microsecond accuracy
  - Low administrative effort, easy to manage and maintain
  - Low cost and low resource use, works on high-end or low-end device
  - Support redundant and fault-tolerant
  - No need to implement costly GPS or other dedicated timing network

# PTP Overview

- Peer-to-peer transparent clocks
- Time format
- Architectural choices
- Best master selection
- PTP profiles and conformance
- General optional features
- State configuration options
- Compatibility requirements
- Transport specific field
- Security
- Transport of cumulative frequency offset information

# Frequency and time Synchronization and Strategies

- Hierarchical architecture for clock and time distribution
- Accuracy better than NTP (from milliseconds to nanoseconds)
- Distribute Time to places where GPS would be impractical (e.g. DC)
- BMC (Best Master Clock) algorithm defines the "Grand Master" used to synchronize a clock domain

# PTPv2 Transport

- PTP over IPv4
- PTP over IPv6
- PTP over Ethernet
  - Note: 802.1AS over Ethernet (802.3) qualifies as a Profile of IEEE 1588-2008
- PTP over DeviceNET
- PTP over ControlNET
- PTP over IEC 61158 Type 10 (Fieldbus)



# PTP Packet/Frame Details

- Communication between master and slave use multicast group address
- Event messages use UDP Port 319
- General message use UDP port 320
- Above applies to both unicast and multicast
- IANA also reserved additional multicast address for PTP, currently it's not used
  - 224.0.1.130
  - 224.0.1.131
  - 224.0.1.132

# PTP addresses

| Ethernet and IP PTPv2 addressing (destination address)                                                     |                | IANA assignment    | Comments                                                                              |
|------------------------------------------------------------------------------------------------------------|----------------|--------------------|---------------------------------------------------------------------------------------|
| PTP primary for all except pdelay messages                                                                 | MAC (Ethernet) | 01-1B-19-00-00-00  | From OUI 00-1B-19 assigned to IEEE I&M Society TC9.                                   |
|                                                                                                            | IPv4           | 224.0.1.129        | Corresponds to PTPv1 default domain number.                                           |
|                                                                                                            | IPv6           | FF0X:0:0:0:0:0:181 | Value of X defines in section 2.7 of [RFC4291].                                       |
| PTP pdelay for pdelay messages<br><br>Note: might be used for all PTP messages in the scope of the address | MAC (Ethernet) | 01-80-C2-00-00-0E  | Allows transmission over Ethernet port blocked by any type of Spanning Tree Protocol. |
|                                                                                                            | IPv4           | 224.0.0.107        | TTL must be set to 1 and cannot be routed.                                            |
|                                                                                                            | IPv6           | FF02:0:0:0:0:0:6B  | HL must be set to 1 and cannot be routed.                                             |

# PTPv2 / General messages / Announce

```
> Frame 4: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 320, Dst Port: 320
▼ Precision Time Protocol (IEEE1588)
 > 0000 = transportSpecific: 0x0
 1011 = messageId: Announce Message (0xb)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 ▼ flags: 0x003c
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 1. = FREQUENCY_TRACEABLE: True
 1 = TIME_TRACEABLE: True
 1... = PTP_TIMESCALE: True
 1.. = PTP_UTC_REASONABLE: True
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Other Message (5)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
```

```
> Frame 17596: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▼ Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IeeeI&MS_00:00:00:00:00:00
 > Destination: IeeeI&MS_00:00:00 (01:1b:19:00:00:00)
 > Source: Meinberg_00:8f:ce (ec:46:70:00:8f:ce)
 Type: PTPv2 over Ethernet (IEEE1588) (0x88f7)
▼ Precision Time Protocol (IEEE1588)
 > 0000 = transportSpecific: 0x0
 1011 = messageId: Announce Message (0xb)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 ▼ flags: 0x003c
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 1. = FREQUENCY_TRACEABLE: True
 1 = TIME_TRACEABLE: True
 1... = PTP_TIMESCALE: True
 1.. = PTP_UTC_REASONABLE: True
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x011b190000000000
 SourcePortID: 1
 sequenceId: 38302
 control: Other Message (5)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
```

**01:1B:19:00:00:00**

for non-peer-delay measurement mechanism messages  
(Announce, Sync, Follow\_up, Delay\_Req, Delay\_Resp)

**01:80:C2:00:00:00:0E**

for peer-delay measurement mechanism messages  
(Pdelay\_Req, Pdelay\_Resp, Pdelay\_Resp\_Follow\_up)

# PTP ToD

- IEEE 1588v2 PTP is capable of frequency, phase and time-of-day synchronization
- Telecommunication industry requires the synchronization of frequency, phase and time-of-day
- Most of the applications in financial institute and data center networks are interested in Time-of-Day synchronization

# PTP – Wireshark Capture and Display Filter

- udp port 319 or udp port 320 or tcp port 319 or tcp port 320
- for PTP over Ethernet packets, specify:

"ether proto 0x88F7"

Capture filter for selected interfaces:

ether proto 0x88F7

Capture filter for selected interfaces:

udp port 319 or udp port 320 or tcp port 319 or tcp port 320



# PTP Clock Types

- **Ordinary Clock (OC)**
  - Has a single PTP port in a domain and maintains the timescale of the domain
- **Boundary Clock (BC)**
  - Has multiple PTP ports in a domain and maintains the timescale of the domain
- **Transparent Clock**
  - Measures the time taken for a PTP event message to transit the device
    - Peer-to-peer transparent clocks (P2P TC) provide corrections for the propagation delay of the link in addition to the transit time
    - End-to-end transparent clock (E2E TC)

# PTP Clock Types

- **Slave clock**

- A slave clock receives the time information from a master clock by synchronizing itself with the master clock. It does not redistribute the time to another clock

- **Grandmaster clock (GM)**

- A grandmaster clock is the highest-ranking clock within its PTP domain and is the primary reference source for all other PTP elements.

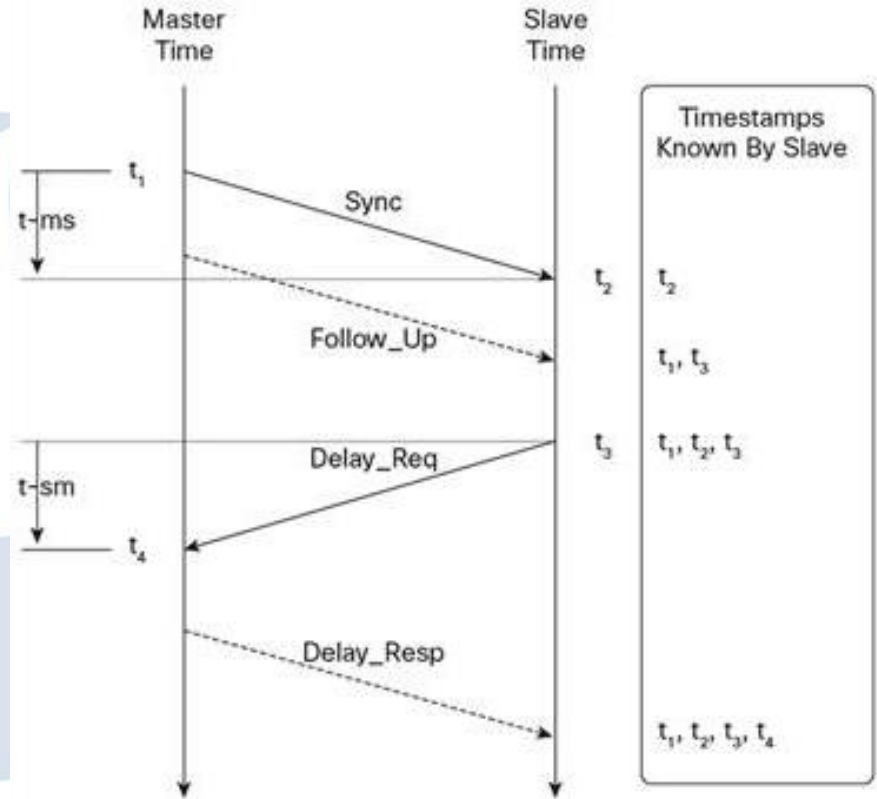
# PTP 1-step and 2-step clocks

- 1-step clock updates accurate timestamp ( $t_1$ ) in Sync message
- 2-step clock sends accurate timestamp ( $t_1$ ) in a Follow\_Up message
  - Simplify design while avoiding queuing noise
  - Ease integration of security extensions



# PTP Clock Synchronization Process

- Sync
- Follow Up
- Delay Request
- Delay Response



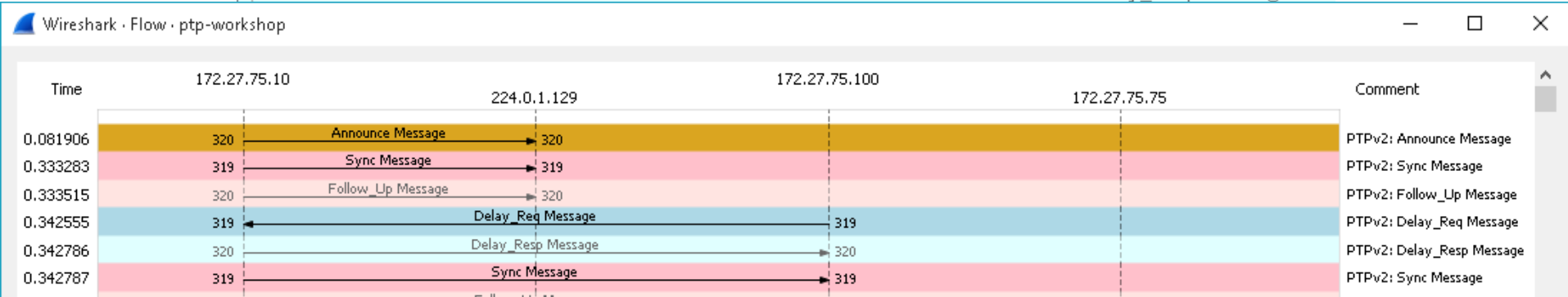
# PTP Clock Synchronization Process in Wireshark

ptp-workshop.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ptp

| No. | Time     | Source        | Destination   | Protocol | Info               |
|-----|----------|---------------|---------------|----------|--------------------|
| 4   | 0.081906 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Announce Message   |
| 12  | 0.333283 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Sync Message       |
| 13  | 0.333515 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Follow_Up Message  |
| 14  | 0.342555 | 172.27.75.100 | 172.27.75.10  | PTPv2    | Delay_Req Message  |
| 15  | 0.342786 | 172.27.75.10  | 172.27.75.100 | PTPv2    | Delay_Resp Message |



# PTPv2 Sync Message – verify by your own

- When was this?
- Was the capture engine in time sync?
  - Hint: Have a look at the originTimestamp and convert it

```
▼ Frame 12: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 Interface id: 0 (\Device\NPF_{BD5BE3FE-84FE-4398-A232-C6D212432BE8})
 Encapsulation type: Ethernet (1)
 Arrival Time: Mar 9, 2017 16:33:45.864628000 W. Europe Standard Time
```

```
originTimestamp (seconds): 1489073662
originTimestamp (nanoseconds): 870158024
```

```
> User Datagram Protocol, Src Port: 319, Dst Port: 319
▼ Precision Time Protocol (IEEE1588)
 ▼ 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 0000 = messageId: Sync Message (0x0)
 0010 = versionPTP: 2
 messageLength: 44
 subdomainNumber: 0
 ▼ flags: 0x0200
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0. = PTP_UNICAST: False
 1. = PTP_TWO_STEP: True
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670ffe008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Sync Message (0)
 logMessagePeriod: 0
 originTimestamp (seconds): 1489073662
 originTimestamp (nanoseconds): 870158024
```

```
0000 01 00 5e 00 01 81 ec 46 70 00 8f ce 08 00 45 00 ..^.....F p.....E.
0010 00 48 28 f7 40 00 05 11 74 07 ac 1b 4b 0a e0 00 .H(.@... t...K...
0020 01 81 01 3f 01 3f 00 34 10 18 00 02 00 2c 00 00 ...?.?.4
0030 02 00 00 00 00 00 00 00 00 00 00 00 00 00 ec 46
0040 70 ff fe 00 8f ce 00 01 95 9e 00 00 00 00 58 c1 p.....X.
0050 75 fe 33 dd 8e c8 u.3...
```

# PTPv2 Transmission

- **Mode:**
  - Unicast
  - Multicast
- **Rates:**
  - variable
- **Timeouts**
  - variable
- **TLV and Extensions**

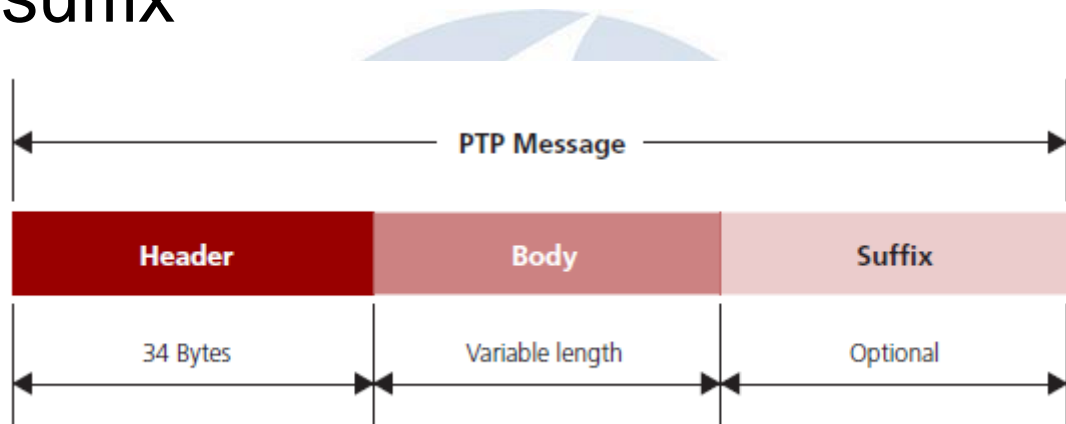


# PTP Grand Master (GM) selection

- GM-capable stations advertise that fact via ANNOUNCE messages
  - If station hears from station with “better” clock, does not send ANNOUNCE
- Settable “Priority” field can override clock quality
- MAC address is tie breaker
  - Bridges drop all inferior ANNOUNCE messages
- Forward only the best
  - Last one standing is Grand Master for the LAN
- GM is the root of the timing tree
- GM periodically sends the current time

# PTP Message Formats

- All PTP Messages consist of a header, body and optional suffix



# PTPv2 / General messages / Announce

```
> Frame 4: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 320, Dst Port: 320
▼ Precision Time Protocol (IEEE1588)
 > 0000 = transportSpecific: 0x0
 1011 = messageId: Announce Message (0xb)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 ▼ flags: 0x003c
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. .. = PTP_TWO_STEP: False
 0 .. = PTP_ALTERNATE_MASTER: False
 1. = FREQUENCY_TRACEABLE: True
 1 = TIME_TRACEABLE: True
 1... = PTP_TIMESCALE: True
 1.. = PTP_UTC_REASONABLE: True
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Other Message (5)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
```

IPv4

```
> Frame 17596: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▼ Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IeeeI&MS_00:00:00:00
 > Destination: IeeeI&MS_00:00:00 (01:1b:19:00:00:00)
 > Source: Meinberg_00:8f:ce (ec:46:70:00:8f:ce)
 Type: PTPv2 over Ethernet (IEEE1588) (0x88f7)
▼ Precision Time Protocol (IEEE1588)
 > 0000 = transportSpecific: 0x0
 1011 = messageId: Announce Message (0xb)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 ▼ flags: 0x003c
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. .. = PTP_TWO_STEP: False
 0 .. = PTP_ALTERNATE_MASTER: False
 1. = FREQUENCY_TRACEABLE: True
 1 = TIME_TRACEABLE: True
 1... = PTP_TIMESCALE: True
 1.. = PTP_UTC_REASONABLE: True
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 999
 control: Other Message (5)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
```

L2

# PTP Message Header

## • Common part of PTP Message Header

```
▼ Precision Time Protocol (IEEE1588)
 > 0000 = transportSpecific: 0x0
 0000 = messageId: Sync Message (0x0)
 0010 = versionPTP: 2
 messageLength: 44
 subdomainNumber: 0
 ▼ flags: 0x0200
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP_profile Specific 2: False
 ..0. .. = PTP_profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 1. = PTP_TWO_STEP: True
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0.. = PTP_LI_59: False
 0.. = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x6805cafffe39dabc
 SourcePortID: 1
 sequenceId: 387
 control: Sync Message (0)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
 originTimestamp (nanoseconds): 0
```

| Bits               |   |   |   |             |   |   |   | Octets | Offset |
|--------------------|---|---|---|-------------|---|---|---|--------|--------|
| 7                  | 6 | 5 | 4 | 3           | 2 | 1 | 0 |        |        |
| transportSpecific  |   |   |   | messageType |   |   |   | 1      | 0      |
| reserved           |   |   |   | versionPTP  |   |   |   | 1      | 1      |
| messageLength      |   |   |   |             |   |   |   | 2      | 2      |
| domainNumber       |   |   |   |             |   |   |   | 1      | 4      |
| reserved           |   |   |   |             |   |   |   | 1      | 5      |
| flags              |   |   |   |             |   |   |   | 2      | 6      |
| correctionField    |   |   |   |             |   |   |   | 8      | 8      |
| reserved           |   |   |   |             |   |   |   | 4      | 16     |
| sourcePortIdentity |   |   |   |             |   |   |   | 10     | 20     |
| sequenceId         |   |   |   |             |   |   |   | 2      | 30     |
| controlField       |   |   |   |             |   |   |   | 1      | 32     |
| logMessageInterval |   |   |   |             |   |   |   | 1      | 33     |

Source: IEEE 1588-2008, Table 18



# PTP Timestamps

- PTP use 80 bit-Timestamps

- They consist of a 48-bit part for seconds and a 32-bit part for nanosecond
- The time scale rolls over every  $2^{48}$  seconds (8.925.512 years)
- Theoretical resolution of  $2^{32}$  nanoseconds
- Timescale from TAI
  - also alternative timescale possible

```
control: Sync Message (0)
logMessagePeriod: 0
originTimestamp (seconds): 1489073662
originTimestamp (nanoseconds): 870158024
```

|      |                         |                         |                   |
|------|-------------------------|-------------------------|-------------------|
| 0000 | 01 00 5e 00 01 81 ec 46 | 70 00 8f ce 08 00 45 00 | ..^....F p.....E. |
| 0010 | 00 48 28 f7 40 00 05 11 | 74 07 ac 1b 4b 0a e0 00 | .H(.@... t...K... |
| 0020 | 01 81 01 3f 01 3f 00 34 | 10 18 00 02 00 2c 00 00 | ...?.?.4 .....    |
| 0030 | 02 00 00 00 00 00 00 00 | 00 00 00 00 00 00 ec 46 | .....F            |
| 0040 | 70 ff fe 00 8f ce 00 01 | 95 9e 00 00 00 00 58 c1 | p..... ..X.       |
| 0050 | 75 fe 33 dd 8e c8       |                         | u.3...            |

Time.sec  
Seconds  
48 bit

Time.Frac  
Nanoseconds  
32 bit

# PTPv2 Message Types

- Event messages (need to be accurately time stamped)
    - Sync
    - Delay\_Req
    - Pdelay\_Req
    - Pdelay\_Resp
  - General messages (not time stamped)
    - Follow\_Up
    - Delay\_Resp
    - Pdelay\_Resp\_Follow\_Up
    - Announce
    - Signaling and Management
- 

# PTPv2 Message Types

ptp.v2.flags.specific2 · PTP profile Specific 2  
ptp.v2.flags.timescale · PTP\_TIMESCALE  
ptp.v2.flags.timetraceable · TIME\_TRACEABLE  
ptp.v2.flags.twostep · PTP\_TWO\_STEP  
ptp.v2.flags.unicast · PTP\_UNICAST  
ptp.v2.flags.utcreasonable · PTP\_UTC\_REASONABLE  
ptp.v2.fu.preciseorigintimestamp.nanoseconds · preciseOriginTimestamp (nanoseconds)  
ptp.v2.fu.preciseorigintimestamp.seconds · preciseOriginTimestamp (seconds)  
ptp.v2.logmessageperiod · logMessagePeriod  
ptp.v2.messageid · messageId  
ptp.v2.messagelength · messageLength  
ptp.v2.mm.action · action  
ptp.v2.mm.AlternateMulticastSyncInterval · Alternate multicast sync interval  
ptp.v2.mm.announceReceiptTimeout · announceReceiptTimeout  
ptp.v2.mm.boundaryhops · boundaryHops

Value (Unsigned integer, 1 byte)

0xb

Predefined Values

Sync Message

Delay\_Req Message

Path\_Delay\_Req Message

Path\_Delay\_Resp Message

Follow\_Up Message

Delay\_Resp Message

Path\_Delay\_Resp\_Follow\_Up Message

Announce Message

Signalling Message

Management Message

**Event messages**

**General messages**

# PTP – Sync Message (0x0)

```
> Frame 12: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 319, Dst Port: 319
▼ Precision Time Protocol (IEEE1588)
 ▼ 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 0000 = messageId: Sync Message (0x0)
 0010 = versionPTP: 2
 messageLength: 44
 subdomainNumber: 0
 ▼ flags: 0x0200
 0... = PTP_SECURITY: False
 .0.. = PTP profile Specific 2: False
 ..0. = PTP profile Specific 1: False
 0.. = PTP_UNICAST: False
 1. = PTP_TWO_STEP: True
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP.UTC_REASONABLE: False
 0. = PTP.LI_59: False
 0 = PTP.LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffef008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Sync Message (0)
 logMessagePeriod: 0
 originTimestamp (seconds): 1489073662
 originTimestamp (nanoseconds): 870158024
```

## Sync Message Format

| Bits            |   |   |   |   |   |   |   | Octets | Offset |
|-----------------|---|---|---|---|---|---|---|--------|--------|
| 7               | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)   |   |   |   |   |   |   |   | 34     | 0      |
| originTimestamp |   |   |   |   |   |   |   | 10     | 34     |

IPv4

Event messages

# PTP - Delay\_Req Message (0x1)

```
> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:bf (ec:46:70:00:8f:bf), Dst: Meinberg_00:8f:ce (ec:46:70:00:8f:ce)
> Internet Protocol Version 4, Src: 172.27.75.100, Dst: 172.27.75.10
> User Datagram Protocol, Src Port: 319, Dst Port: 319
▼ Precision Time Protocol (IEEE1588)
 ▼ 0000 = transportSpecific: 0x0
 0 = V1 Compatibility: False
 0001 = messageId: Delay_Req Message (0x1)
 0010 = versionPTP: 2
 messageLength: 48
 subdomainNumber: 0
 ▼ flags: 0x0400
 0... .. = PTP_SECURITY: False
 .0... .. = PTP profile Specific 2: False
 ..0... .. = PTP profile Specific 1: False
 1... .. = PTP_UNICAST: True
 0... .. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... .. = PTP_TIMESCALE: False
 0... .. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fbf
 SourcePortID: 1
 sequenceId: 529
 control: Delay_Req Message (1)
 logMessagePeriod: 127
 originTimestamp (seconds): 1489073662
 originTimestamp (nanoseconds): 879479141
```

## Delay\_Req Message Format

| Bits            |   |   |   |   |   |   |   | Octets | Offset |
|-----------------|---|---|---|---|---|---|---|--------|--------|
| 7               | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)   |   |   |   |   |   |   |   | 34     | 0      |
| originTimestamp |   |   |   |   |   |   |   | 10     | 34     |

IPv4

Event messages

# PTP - Path\_Delay\_Req Message (0x2)

```
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: RichardH_00:09:ba (00:80:63:00:09:ba), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
▼ Precision Time Protocol (IEEE1588)
 ▼ 0000 = transportSpecific: 0x0
 ...0 = 802.1as conform: False
 0010 = messageId: Path_Delay_Req Message (0x2)
 0010 = versionPTP: 2
 messageLength: 54
 subdomainNumber: 0
 ▼ flags: 0x0000
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x008063ffff0009ba
 SourcePortID: 2
 sequenceId: 1118
 control: Other Message (5)
 logMessagePeriod: 15
 originTimestamp (seconds): 1169232201
 originTimestamp (nanoseconds): 474052852
```

Pdelay\_Req Message Format

| Bits            |   |   |   |   |   |   |   | Octets | Offset |
|-----------------|---|---|---|---|---|---|---|--------|--------|
| 7               | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)   |   |   |   |   |   |   |   | 34     | 0      |
| originTimestamp |   |   |   |   |   |   |   | 10     | 34     |
| reserved        |   |   |   |   |   |   |   | 10     | 44     |



L2

Event messages

# PTP - Path\_Delay\_Resp Message (0x3)

```
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: HonHaiPr_15:ad:ad (00:22:68:15:ad:ad), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
▼ Precision Time Protocol (IEEE1588)
 ▼ 0001 = transportSpecific: 0x1
 0011 = messageId: Path_Delay_Resp Message (0x3)
 0010 = versionPTP: 2
 messageLength: 54
 subdomainNumber: 0
 ▼ flags: 0x0000
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. .. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... .. = PTP_TIMESCALE: False
 0.. .. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x002268fffe15adad
 SourcePortID: 1
 sequenceId: 128
 control: Other Message (5)
 logMessagePeriod: 1
 requestreceiptTimestamp (seconds): 1273706546
 requestreceiptTimestamp (nanoseconds): 503340000
 requestingSourcePortIdentity: 0x005043fffe00101
 requestingSourcePortId: 0
```

## Pdelay\_Resp Message Format

| Bits                    |   |   |   |   |   |   |   | Octets | Offset |
|-------------------------|---|---|---|---|---|---|---|--------|--------|
| 7                       | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)           |   |   |   |   |   |   |   | 34     | 0      |
| receiveReceiptTimestamp |   |   |   |   |   |   |   | 10     | 34     |
| requestingPortIdentity  |   |   |   |   |   |   |   | 10     | 44     |



L2

Event messages

# PTP - Follow\_Up Message (0x8)

```
> Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: MeInberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 320, Dst Port: 320
√ Precision Time Protocol (IEEE1588)
 √ 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 1000 = messageId: Follow_Up Message (0x8)
 0010 = versionPTP: 2
 messageLength: 44
 subdomainNumber: 0
 √ flags: 0x0000
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 0.. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 0 = PTP_LI_61: False
 √ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Follow_Up Message (2)
 logMessagePeriod: 0
 preciseOriginTimestamp (seconds): 1489073662
 preciseOriginTimestamp (nanoseconds): 870210033
```

## Follow\_Up Message Format

| Bits                   |   |   |   |   |   |   |   | Octets | Offset |
|------------------------|---|---|---|---|---|---|---|--------|--------|
| 7                      | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)          |   |   |   |   |   |   |   | 34     | 0      |
| preciseOriginTimestamp |   |   |   |   |   |   |   | 10     | 34     |

IPv4

General messages



# PTP - Delay\_Resp Message (0x9)

```
> Frame 15: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: Meinberg_00:8f:bf (ec:46:70:00:8f:bf)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 172.27.75.100
> User Datagram Protocol, Src Port: 320, Dst Port: 320
```

## Precision Time Protocol (IEEE1588)

```
▼ 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 1001 = messageId: Delay_Resp Message (0x9)
 0010 = versionPTP: 2
 messageLength: 128
 subdomainNumber: 0
▼ flags: 0x0400
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP_profile Specific 2: False
 ..0. .. = PTP_profile Specific 1: False
 1.. .. = PTP_UNICAST: True
 0. = PTP_TWO_STEP: False
 0 = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 0 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP.UTC_REASONABLE: False
 0. = PTP.LI_59: False
 0 = PTP.LI_61: False
▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 529
 control: Delay_Resp Message (3)
 logMessagePeriod: 127
 receiveTimestamp (seconds): 1489073662
 receiveTimestamp (nanoseconds): 879482261
 requestingSourcePortIdentity: 0xec4670fffe008fbf
 requestingSourcePortId: 1
```

## Delay\_Resp Message Format

| Bits                   |   |   |   |   |   |   |   | Octets | Offset |
|------------------------|---|---|---|---|---|---|---|--------|--------|
| 7                      | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)          |   |   |   |   |   |   |   | 34     | 0      |
| receiveTimestamp       |   |   |   |   |   |   |   | 10     | 34     |
| requestingPortIdentity |   |   |   |   |   |   |   | 10     | 44     |

IPv4

General messages

# PTP - Path\_Delay\_Resp\_Follow\_Up Message (0xa)

```
> Frame 42: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
> Ethernet II, Src: Accedian_0a:14:a3 (00:15:ad:0a:14:a3), Dst: Fujitsu_1c:44:25 (00:e0:00:1c:44:25)
> Internet Protocol Version 4, Src: 192.168.1.74, Dst: 192.168.1.159
> User Datagram Protocol, Src Port: 320, Dst Port: 320
▼ Precision Time Protocol (IEEE1588)
 ▼ 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 1100 = messageId: Signalling Message (0xc)
 0010 = versionPTP: 2
 messageLength: 54
 subdomainNumber: 0
 ▼ flags: 0x0400
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 1.1. = PTP_UNICAST: True
 00. = PTP_TWO_STEP: False
 00. = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 00. = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0. = PTP_LI_59: False
 00. = PTP_LI_61: False
 ▼ correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x0015adfffe0a14a0
 SourcePortID: 1
 sequenceId: 21
 control: Other Message (5)
 logMessagePeriod: 127
 targetPortIdentity: 0x00e000fffe1c4425
 targetPortId: 1
 ▼ tlvType: Request unicast transmission (4)
 lengthField: 6
 1011 = messageType: Announce Message (0xb)
 ▼ logInterMessagePeriod: 1
 period: every 2 seconds
 rate: 0.5 packets/sec
 durationField: 300 seconds
```

## Pdelay\_Resp\_Follow\_Up Message Format

| Bits                    |   |   |   |   |   |   |   | Octets | Offset |
|-------------------------|---|---|---|---|---|---|---|--------|--------|
| 7                       | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)           |   |   |   |   |   |   |   | 34     | 0      |
| responseOriginTimestamp |   |   |   |   |   |   |   | 10     | 34     |
| requestingPortIdentity  |   |   |   |   |   |   |   | 10     | 44     |

IPv4

General messages

# PTP - Announce Message (0xb)

```
> Frame 4: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
> Ethernet II, Src: Meinberg_00:8f:ce (ec:46:70:00:8f:ce), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 172.27.75.10, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 320, Dst Port: 320
< Precision Time Protocol (IEEE1588)
 < 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 1011 = messageId: Announce Message (0xb)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 < flags: 0x003c
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP_profile Specific 2: False
 ..0. .. = PTP_profile Specific 1: False
 0.. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 0 .. = PTP_ALTERNATE_MASTER: False
 1. = FREQUENCY_TRACEABLE: True
 1 = TIME_TRACEABLE: True
 1... = PTP_TIMESCALE: True
 1. = PTP.UTC_REASONABLE: True
 0. = PTP.LI_59: False
 0 = PTP.LI_61: False
 < correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0xec4670fffe008fce
 SourcePortID: 1
 sequenceId: 38302
 control: Other Message (5)
 logMessagePeriod: 0
 originTimestamp (seconds): 0
 originTimestamp (nanoseconds): 0
 originCurrentUTCOffset: 37
 priority1: 128
 grandmasterClockClass: 6
 grandmasterClockAccuracy: The time is accurate to within 100 ns (0x21)
 grandmasterClockVariance: 13563
 priority2: 128
 grandmasterClockIdentity: 0xec4670fffe008fce
 localStepsRemoved: 0
 TimeSource: GPS (0x20)
```

## Announce Message Format

| Bits                    |   |   |   |   |   |   |   | Octets | Offset |
|-------------------------|---|---|---|---|---|---|---|--------|--------|
| 7                       | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)           |   |   |   |   |   |   |   | 34     | 0      |
| originTimestamp         |   |   |   |   |   |   |   | 10     | 34     |
| currentUtcOffset        |   |   |   |   |   |   |   | 2      | 44     |
| Reserved                |   |   |   |   |   |   |   | 1      | 46     |
| grandmasterPriority1    |   |   |   |   |   |   |   | 1      | 47     |
| grandmasterClockQuality |   |   |   |   |   |   |   | 4      | 48     |
| grandmasterPriority2    |   |   |   |   |   |   |   | 1      | 52     |
| grandmasterIdentity     |   |   |   |   |   |   |   | 8      | 53     |
| stepsRemoved            |   |   |   |   |   |   |   | 2      | 61     |
| timeSource              |   |   |   |   |   |   |   | 1      | 63     |

IPv4

General messages

# PTP - Signalling Message (0xc)

```
> Frame 42: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
> Ethernet II, Src: Accedian_0a:14:a3 (00:15:ad:0a:14:a3), Dst: Fujitsu_1c:44:25 (00:e0:00:1c:44:25)
> Internet Protocol Version 4, Src: 192.168.1.74, Dst: 192.168.1.159
> User Datagram Protocol, Src Port: 320, Dst Port: 320
< Precision Time Protocol (IEEE1588)
 < 0000 = transportSpecific: 0x0
 ...0 = V1 Compatibility: False
 1100 = messageId: Signalling Message (0xc)
 0010 = versionPTP: 2
 messageLength: 54
 subdomainNumber: 0
 < flags: 0x0400
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP profile Specific 2: False
 ..0. .. = PTP profile Specific 1: False
 1.1. = PTP_UNICAST: True
 00. = PTP_TWO_STEP: False
 00. = PTP_ALTERNATE_MASTER: False
 00. = FREQUENCY_TRACEABLE: False
 00. = TIME_TRACEABLE: False
 00. = PTP_TIMESCALE: False
 00. = PTP.UTC_REASONABLE: False
 00. = PTP.LI_59: False
 00. = PTP.LI_61: False
 < correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x0015adfffe0a14a0
 SourcePortID: 1
 sequenceId: 21
 control: Other Message (5)
 logMessagePeriod: 127
 targetPortIdentity: 0x00e000fffe1c4425
 targetPortId: 1
 < tlvType: Request unicast transmission (4)
 lengthField: 6
 1011 = messageType: Announce Message (0xb)
 < logInterMessagePeriod: 1
 period: every 2 seconds
 rate: 0.5 packets/sec
 durationField: 300 seconds
```

## Signalling Message Format

| Bits               |   |   |   |   |   |   |   | Octets | Offset |
|--------------------|---|---|---|---|---|---|---|--------|--------|
| 7                  | 6 | 5 | 4 | 3 | 2 | 1 | 0 |        |        |
| header (13.3)      |   |   |   |   |   |   |   | 34     | 0      |
| targetPortIdentity |   |   |   |   |   |   |   | 10     | 34     |
| One or more TLVs   |   |   |   |   |   |   |   | N      | 44     |

A Signaling message is used to transport a sequence of one or more TLV entities.

IPv4

General messages

# PTP - Management Message (0xd)

```
> Frame 4: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
> Ethernet II, Src: HewlettP_e0:06:d3 (b4:b5:2f:e0:06:d3), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)
> Internet Protocol Version 4, Src: 10.1.1.3.99, Dst: 224.0.1.129
> User Datagram Protocol, Src Port: 320, Dst Port: 320
> Precision Time Protocol (IEEE1588)
 < 0000 = transportSpecific: 0x0
 ... 0 = V1 Compatibility: False
 1101 = messageId: Management Message (0xd)
 0010 = versionPTP: 2
 messageLength: 64
 subdomainNumber: 0
 < flags: 0x0000
 0... .. = PTP_SECURITY: False
 .0.. .. = PTP_profile Specific 2: False
 ..0. = PTP_profile Specific 1: False
 0.. = PTP_UNICAST: False
 0. = PTP_TWO_STEP: False
 00 .. = PTP_ALTERNATE_MASTER: False
 0. = FREQUENCY_TRACEABLE: False
 00 = TIME_TRACEABLE: False
 0... = PTP_TIMESCALE: False
 0.. = PTP_UTC_REASONABLE: False
 0.. = PTP_LI_59: False
 0.. = PTP_LI_61: False
 < correction: 0.000000 nanoseconds
 correction: Ns: 0 nanoseconds
 correctionSubNs: 0.000000 nanoseconds
 ClockIdentity: 0x544debfffe35620e
 SourcePortID: 1
 sequenceId: 236
 control: Management Message (4)
 logMessagePeriod: 0
 targetPortIdentity: 0xfffffffffffff
 targetPortId: 65535
 startingBoundaryHops: 0
 boundaryHops: 0
 ... 0000 = action: GET (0)
 tlvType: Management (1)
 lengthField: 12
 managementId: TIME (8207)
 < data: 00000000000000000000
 current time (seconds): 0
 current time (nanoseconds): 0
```

## Management Message Format

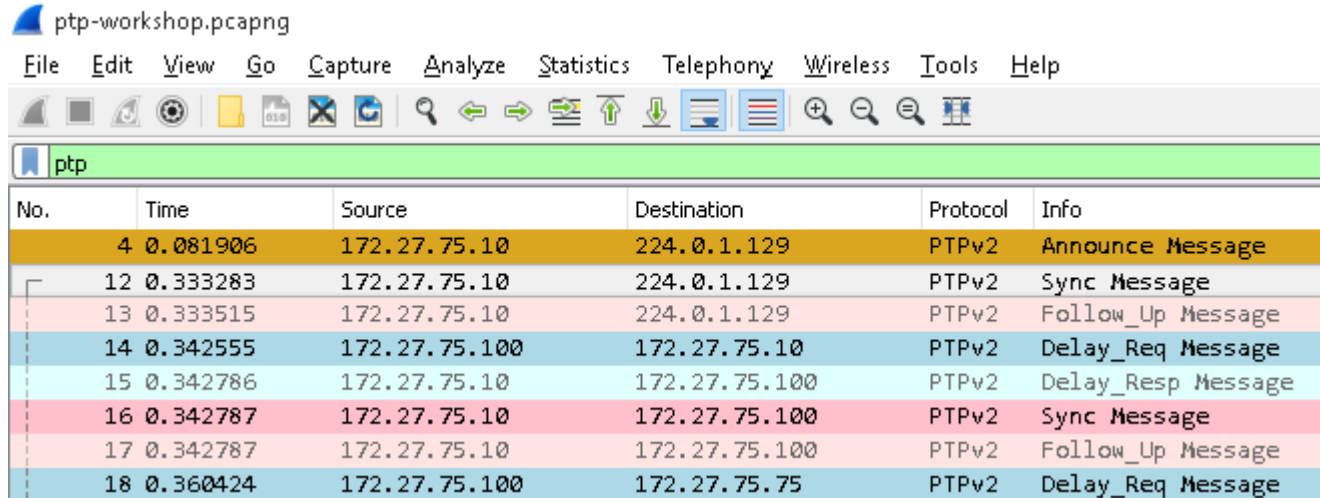
| Bits                 |   |   |   |             |   |   |   | Octets | Offset |
|----------------------|---|---|---|-------------|---|---|---|--------|--------|
| 7                    | 6 | 5 | 4 | 3           | 2 | 1 | 0 |        |        |
| header (13.3)        |   |   |   |             |   |   |   | 34     | 0      |
| targetPortIdentity   |   |   |   |             |   |   |   | 10     | 34     |
| startingBoundaryHops |   |   |   |             |   |   |   | 1      | 44     |
| boundaryHops         |   |   |   |             |   |   |   | 1      | 45     |
| Reserved             |   |   |   | actionField |   |   |   | 1      | 46     |
| Reserved             |   |   |   |             |   |   |   | 1      | 47     |
| managementTLV        |   |   |   |             |   |   |   | M      | 48     |

IPv4

General messages

# PTPv2 Coloring Rule

- Colors for various PTP message types



The screenshot shows the Wireshark interface with a capture file named 'ptp-workshop.pcapng'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. Below the toolbar, a green bar indicates the current filter is 'ptp'. The main display area shows a list of captured packets, each with a unique color background corresponding to its PTPv2 message type.

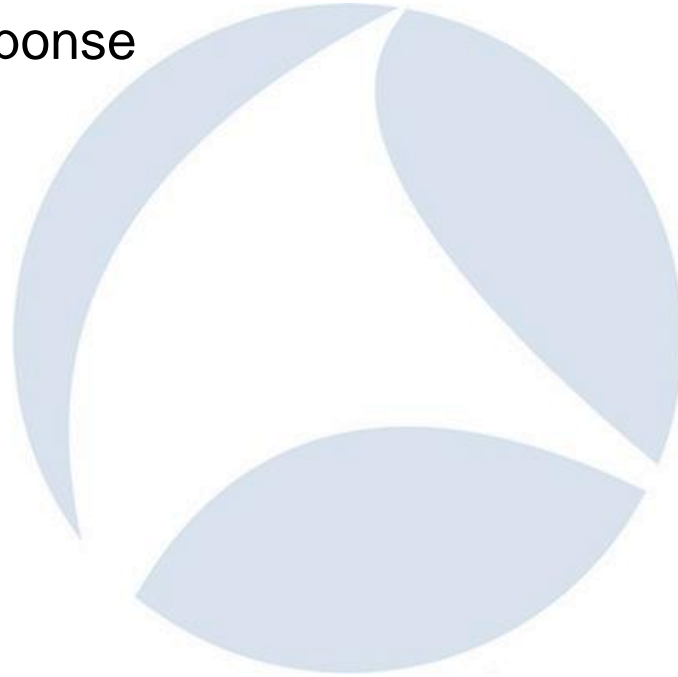
| No. | Time     | Source        | Destination   | Protocol | Info               |
|-----|----------|---------------|---------------|----------|--------------------|
| 4   | 0.081906 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Announce Message   |
| 12  | 0.333283 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Sync Message       |
| 13  | 0.333515 | 172.27.75.10  | 224.0.1.129   | PTPv2    | Follow_Up Message  |
| 14  | 0.342555 | 172.27.75.100 | 172.27.75.10  | PTPv2    | Delay_Req Message  |
| 15  | 0.342786 | 172.27.75.10  | 172.27.75.100 | PTPv2    | Delay_Resp Message |
| 16  | 0.342787 | 172.27.75.10  | 172.27.75.100 | PTPv2    | Sync Message       |
| 17  | 0.342787 | 172.27.75.10  | 172.27.75.100 | PTPv2    | Follow_Up Message  |
| 18  | 0.360424 | 172.27.75.100 | 172.27.75.75  | PTPv2    | Delay_Req Message  |

- Wireshark Color Filters for PTP (Tutorial)

- [https://www.iol.unh.edu/sites/default/files/knowledgebase/1588/Wire\\_shark\\_color\\_filters\\_tutorial.pdf](https://www.iol.unh.edu/sites/default/files/knowledgebase/1588/Wire_shark_color_filters_tutorial.pdf)

# PTP Delay measurement

- Path delay mechanisms
  - peer delay
  - delay request response



# PTP and QoS

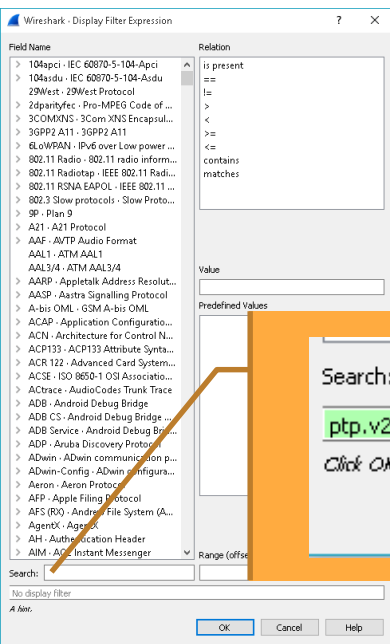
- For Carrier Ethernet Network (CEN), 1588v2 requires a dedicated CoS or even a dedicated EVC – with stringent requirements on Frame Loss Ratio, Frame Delay and Inter-frame Delay Variation
- For L3 - IPv4/v6 - the Traffic Classifier (DSCP) can be used for marking → Test with heavy Load also 😊



# PTPv2 / ptp.v2.an.grandmasterclockaccuracy

- Wireshark → Display Filter Expression

Apply a display filter ... <Ctrl-/> Express



Wireshark - Display Filter Expression

Field Name Relation Value

104apci - IEC 60870-5-104-Apcli  
104asdu - IEC 60870-5-104-Asdu  
29Mext - 29Mext Protocol  
2dparlyfec - Pro-MPEG Code of ...  
3COMXNS - 3Com XNS Encapsul...  
3GPP2 A11 - 3GPP2 A11  
6LoWPAN - IPv6 over Low power ...  
802.11 Radio - 802.11 radio inform...  
802.11 Radiotap - IEEE 802.11 Rad...  
802.11 RSNA EAPOL - IEEE 802.11 ...  
802.3 Slow protocols - Slow Proto...  
SP - Plan 9  
A21 - A21 Protocol  
AAF - AVTP Audio Format  
AAL1 - ATM AAL1  
AAL3/4 - ATM AAL3/4  
AARP - AppleTalk Address Resolut...  
AASP - Aastra Signalling Protocol  
A-bis OML - GSM A-bis OML  
ACAP - Application Configuratio...  
ACN - Architecture for Control N...  
ACP133 - ACP133 Attribute Synta...  
ACR122 - Advanced Card System...  
ACSE - ISO 9658-1 OJ Association...  
ACTrace - AudioCodes Trunk Trace  
ADB - Android Debug Bridge  
ADB CS - Android Debug Bridge ...  
ADB Service - Android Debug Br...  
ADP - Anuba Discovery Protoco...  
ADwin - ADwin communication p...  
ADwin-Config - ADwin configura...  
Aeron - Aeron Protocol  
AFP - Apple Filing Protocol  
AFS (R0) - Android File System (A...  
AgentX - AgentX  
AH - Authentication Header  
AIM - AOL Instant Messenger

is present  
==  
!=  
>  
<  
>=  
<=  
contains  
matches

Value

Predefined Values

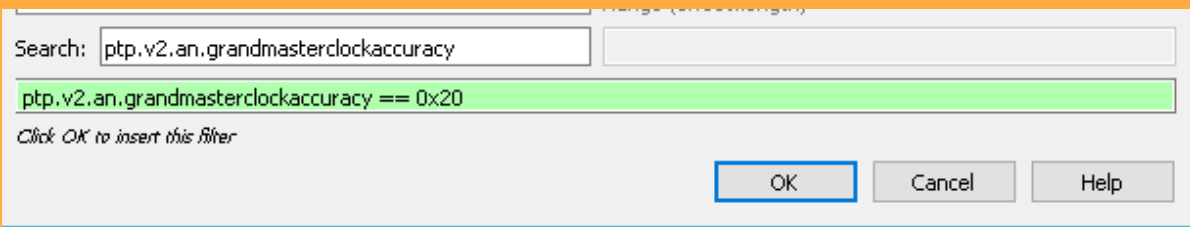
Search:

Range (offset)

No display filter

A filter

OK Cancel Help

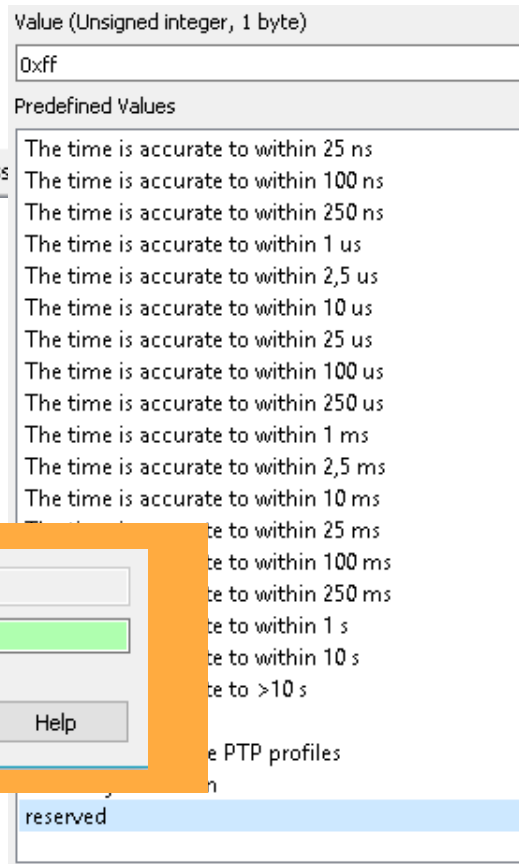


Search:

**ptp.v2.an.grandmasterclockaccuracy == 0x20**

Click OK to insert this filter

OK Cancel Help



Value (Unsigned integer, 1 byte)

0xff

Predefined Values

- The time is accurate to within 25 ns
- The time is accurate to within 100 ns
- The time is accurate to within 250 ns
- The time is accurate to within 1 us
- The time is accurate to within 2,5 us
- The time is accurate to within 10 us
- The time is accurate to within 25 us
- The time is accurate to within 100 us
- The time is accurate to within 250 us
- The time is accurate to within 1 ms
- The time is accurate to within 2,5 ms
- The time is accurate to within 10 ms
- The time is accurate to within 25 ms
- The time is accurate to within 100 ms
- The time is accurate to within 250 ms
- The time is accurate to within 1 s
- The time is accurate to within 10 s
- The time is accurate to >10 s

PTP profiles

reserved

# PTPv2 / ptp.v2.sig.tlv.tlv Type

- Request unicast transmission
  - Switch from Multicast to Unicast
  - Advantage from PTPv2 (PTPv1 only Multicast)

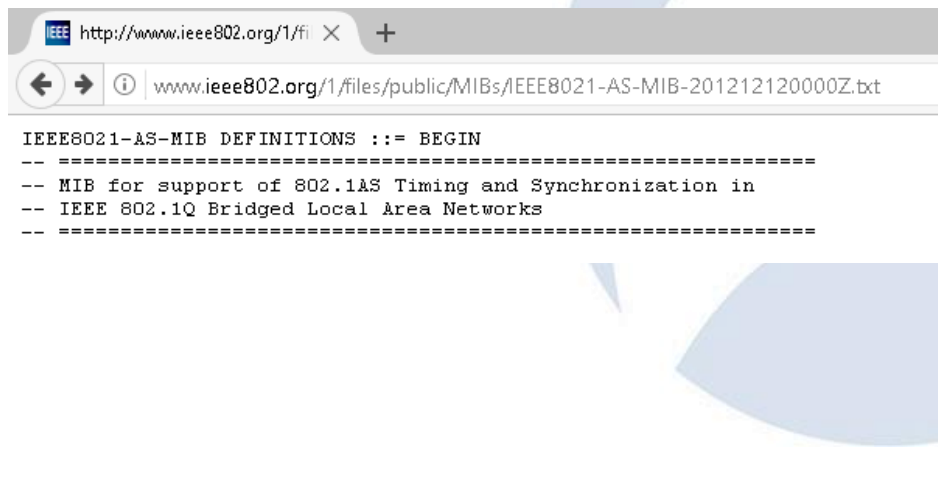
```
▼ tlvType: Request unicast transmission (4)
 lengthField: 6
 1011 = messageType: Announce Message (0xb)
 ▼ logInterMessagePeriod: 1
 period: every 2 seconds
 rate: 0.5 packets/sec
 durationField: 300 seconds
```

```
▼ tlvType: Grant unicast transmission (5)
 lengthField: 8
 1011 = messageType: Announce Message (0xb)
 ▼ logInterMessagePeriod: 1
 period: every 2 seconds
 rate: 0.5 packets/sec
 durationField: 300 seconds
 1 = renewalInvited: True
```

# PTPv2 / ptp.v2.an.tlvType

## • Demos:

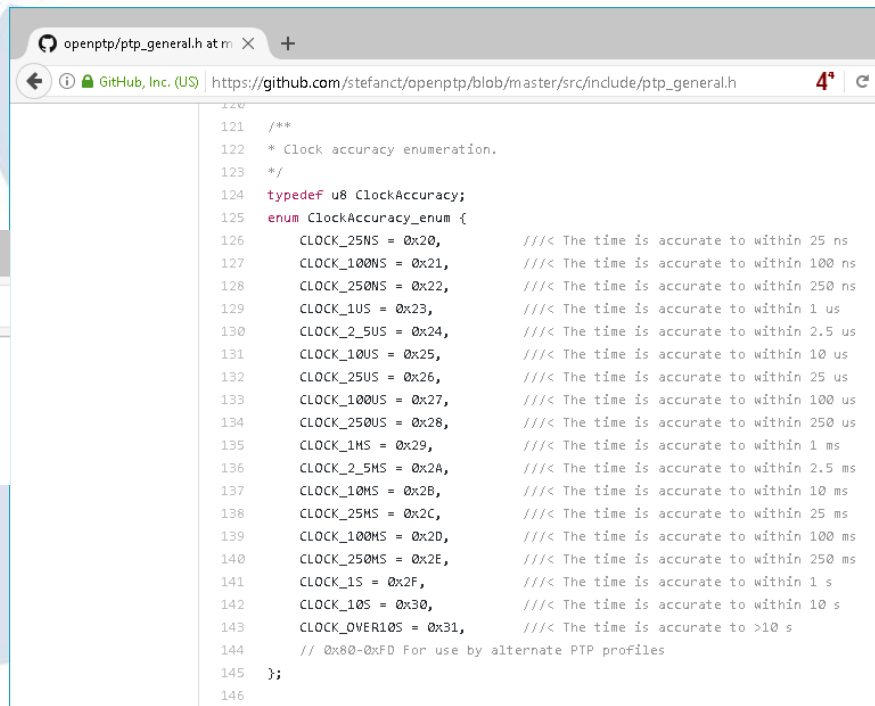
- Wireshark → Display Filter Expression
- Source on github for openptp
- IEEE MIB 802.1AS



http://www.ieee802.org/1/fi X +

www.ieee802.org/1/files/public/MIBs/IEEE8021-AS-MIB-201212120000Z.txt

```
IEEE8021-AS-MIB DEFINITIONS ::= BEGIN
--
-- =====
-- MIB for support of 802.1AS Timing and Synchronization in
-- IEEE 802.1Q Bridged Local Area Networks
-- =====
--
```



openptp/ptp\_general.h at m X +

GitHub, Inc. (US) https://github.com/stefanct/openptp/blob/master/src/include/ptp\_general.h 4 C

```
120
121 /**
122 * Clock accuracy enumeration.
123 */
124 typedef u8 ClockAccuracy;
125 enum ClockAccuracy_enum {
126 CLOCK_25NS = 0x20, ///< The time is accurate to within 25 ns
127 CLOCK_100NS = 0x21, ///< The time is accurate to within 100 ns
128 CLOCK_250NS = 0x22, ///< The time is accurate to within 250 ns
129 CLOCK_1US = 0x23, ///< The time is accurate to within 1 us
130 CLOCK_2_5US = 0x24, ///< The time is accurate to within 2.5 us
131 CLOCK_10US = 0x25, ///< The time is accurate to within 10 us
132 CLOCK_25US = 0x26, ///< The time is accurate to within 25 us
133 CLOCK_100US = 0x27, ///< The time is accurate to within 100 us
134 CLOCK_250US = 0x28, ///< The time is accurate to within 250 us
135 CLOCK_1MS = 0x29, ///< The time is accurate to within 1 ms
136 CLOCK_2_5MS = 0x2A, ///< The time is accurate to within 2.5 ms
137 CLOCK_10MS = 0x2B, ///< The time is accurate to within 10 ms
138 CLOCK_25MS = 0x2C, ///< The time is accurate to within 25 ms
139 CLOCK_100MS = 0x2D, ///< The time is accurate to within 100 ms
140 CLOCK_250MS = 0x2E, ///< The time is accurate to within 250 ms
141 CLOCK_1S = 0x2F, ///< The time is accurate to within 1 s
142 CLOCK_10S = 0x30, ///< The time is accurate to within 10 s
143 CLOCK_OVER10S = 0x31, ///< The time is accurate to >10 s
144 // 0x80-0xFD For use by alternate PTP profiles
145 };
146
```

# PTP Profiles

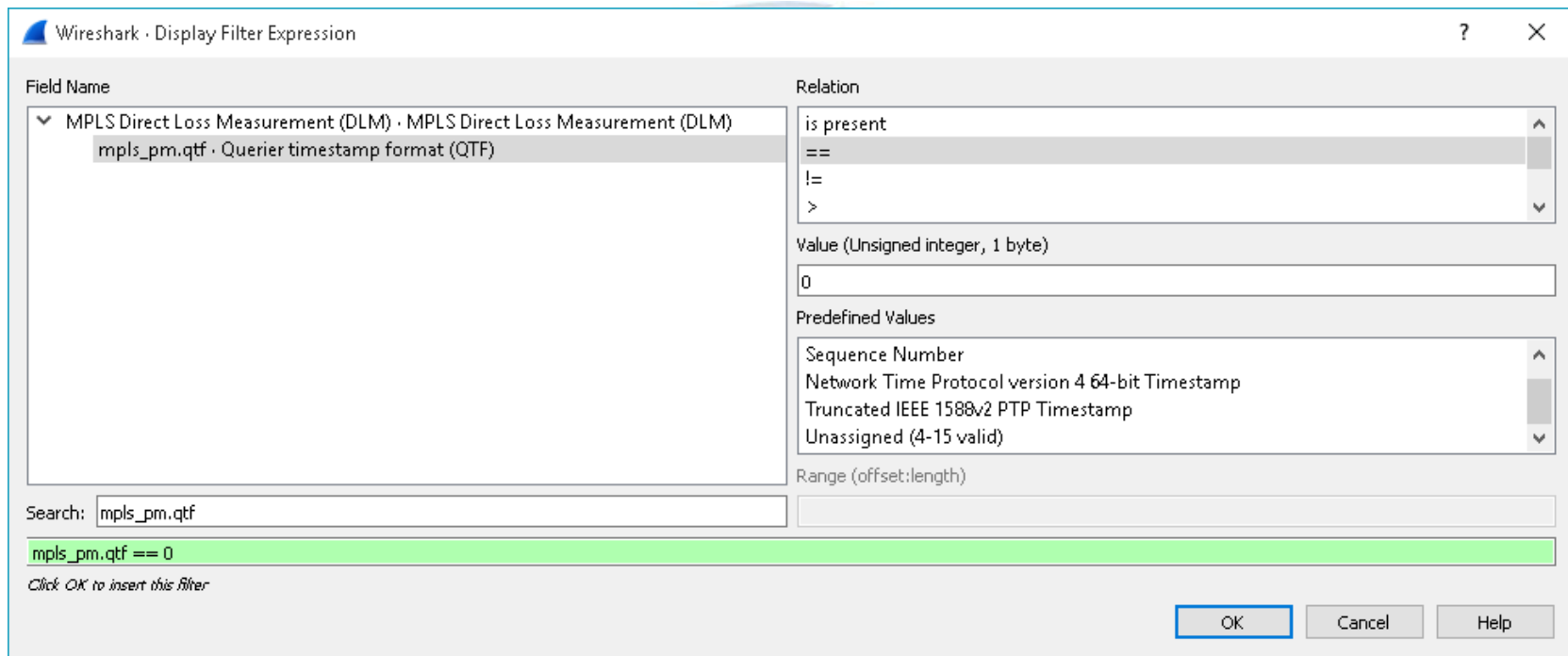
- **IEEE-C37.238 Power Profile**
  - for power system applications
- **IEEE 802.1AS-2011**
  - for audio and video applications
- **ITU-1 G.8265.1 Frequency Profile**
  - for frequency synchronization
- **ITU-T G.8275.1 Time and Phase Profile with full timing support (on new network)**
- **ITU-T G.8275.2 Time and Phase Profile with partial timing support (on existing network)**

# PTP Message Rates

- Different profiles have different message rates
  - G.8265.1
    - Announce message rate
      - Minimum rate: one packet every 16 seconds, Maximum rate: 8 packets per second, Default rate: one packet every 2 seconds
    - Sync message rate
      - Minimum rate: one packet every 16 seconds, Maximum rate: 128 packets per second
    - Delay\_Req/Delay\_Resp message rate
      - Minimum rate: one packet every 16 seconds, Maximum rate: 128 packets per second
  - G.8275.1
    - Announce message rate
      - 8 packets per seconds
    - Sync message rate
      - 16 packets per seconds
    - Delay\_Req/Delay\_Resp message rate
      - 16 packets per seconds

# MPLS Loss and Delay Measurement – RFC 6374

- Time, Time, Time ... also in the MPLS World



# NTP & PTP Comparison

| Criteria                  | NTP                              | PTP                                                                         |
|---------------------------|----------------------------------|-----------------------------------------------------------------------------|
| Peak time transfer error  | > 1ms                            | > 100 ns                                                                    |
| Primary error source      | Router                           | Router, Switches, Network Stack, Port contention                            |
| Implementation            | Hard- or Software Server/Clients | Hardware (mainly Master)<br>Software (Clients, Slaves)                      |
| Mode of operation         | Clients pull time from server    | Master push time to slave                                                   |
| On path support           | Non existent and not possible    | Not required, but possible through transparent clock (enhances performance) |
| Epoch                     | 0:00:00<br>1 January 1900        | 0:00:00<br>1 January 1970                                                   |
| Monitoring and Management | Exists (SNMP MIBs), Test Clients | Extensive inband metrics for monitoring and management                      |

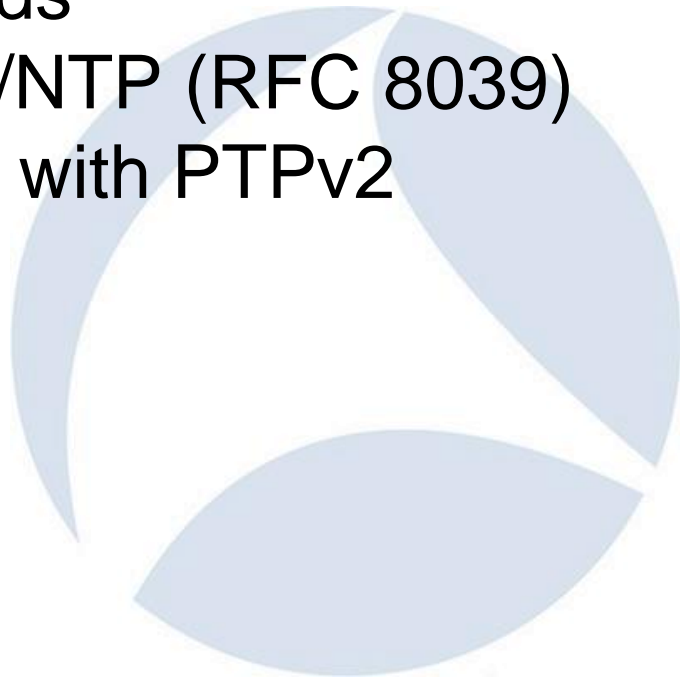
# Session Summary

- Highly accurate timing synchronization solution in sub-microsecond level can be done by IEEE 1588 PTP
  - IEEE 1588 PTPv2 and NTP are widely used timing synchronization protocols in the packet networks
  - Data center switches support PTP in hardware today
  - Delivery accurate timing information to client under heavy network load must be tested
  - PTPv2 solutions need to be carefully designed and reviewed before enabled in production network
- WIRESHARK is the tool for displaying the different time information, but remember the capture engine 😊**



# Future View

- Network Time Protocol Version 4 (NTPv4)  
Extension Fields
- Multipath PTP/NTP (RFC 8039)
- Authentication with PTPv2



# Please provide Session Feedback

- Use the guidebook app on your smartphone
- Fill out the required fields

The image displays two screenshots of a mobile application interface. The left screenshot shows the 'Details' page for a session titled '15: Wireshark & Time: Accurate Handling of Timing When Capturing Frames'. The session is scheduled for 'Dienstag, 20. Juni' from '16:15-17:30' at the location 'McKenna/Peter/Wright'. The difficulty is listed as 'Intermediate'. The description states: 'Sometimes an analysis task requires accurate handling of timing in capturing frames. Also, NTP and IEEE 1588 PTPv2 (Precision Time Protocol) are the most widely used time protocols for network synchronization. These standard protocols are used for time synchronization networking systems with accuracies ranging from micro to milliseconds, depending on different network environments. In this presentation, we will dig into problems rooted in time symptoms. Wireshark configuration profiles, display filters, and color rules can provide specific focus when you troubleshoot time issues.' At the bottom, there is a link to 'Zu meinem Zeitplan hinzufügen? Jetzt hinzufügen >'. The right screenshot shows the 'Web' page with a feedback form. Question 1 asks: 'On a scale of 1 to 10, how much did you enjoy this session? (Pflichtfeld) 10 being the highest.' Below this is a row of 10 buttons labeled 1 through 10. Question 2 asks: 'Please give any feedback you have for the presenter/conference (Pflichtfeld)'. Below this is a large text input field. At the bottom of the form is a blue button labeled 'Abschicken'. Navigation arrows and a refresh icon are visible at the bottom of the right screenshot.

# Slogan SharkFest 2017 from my party

## Spanning Tree of Network Analyst

1. Listen
2. Learn
3. Practice



Thank you for your attention !



SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017