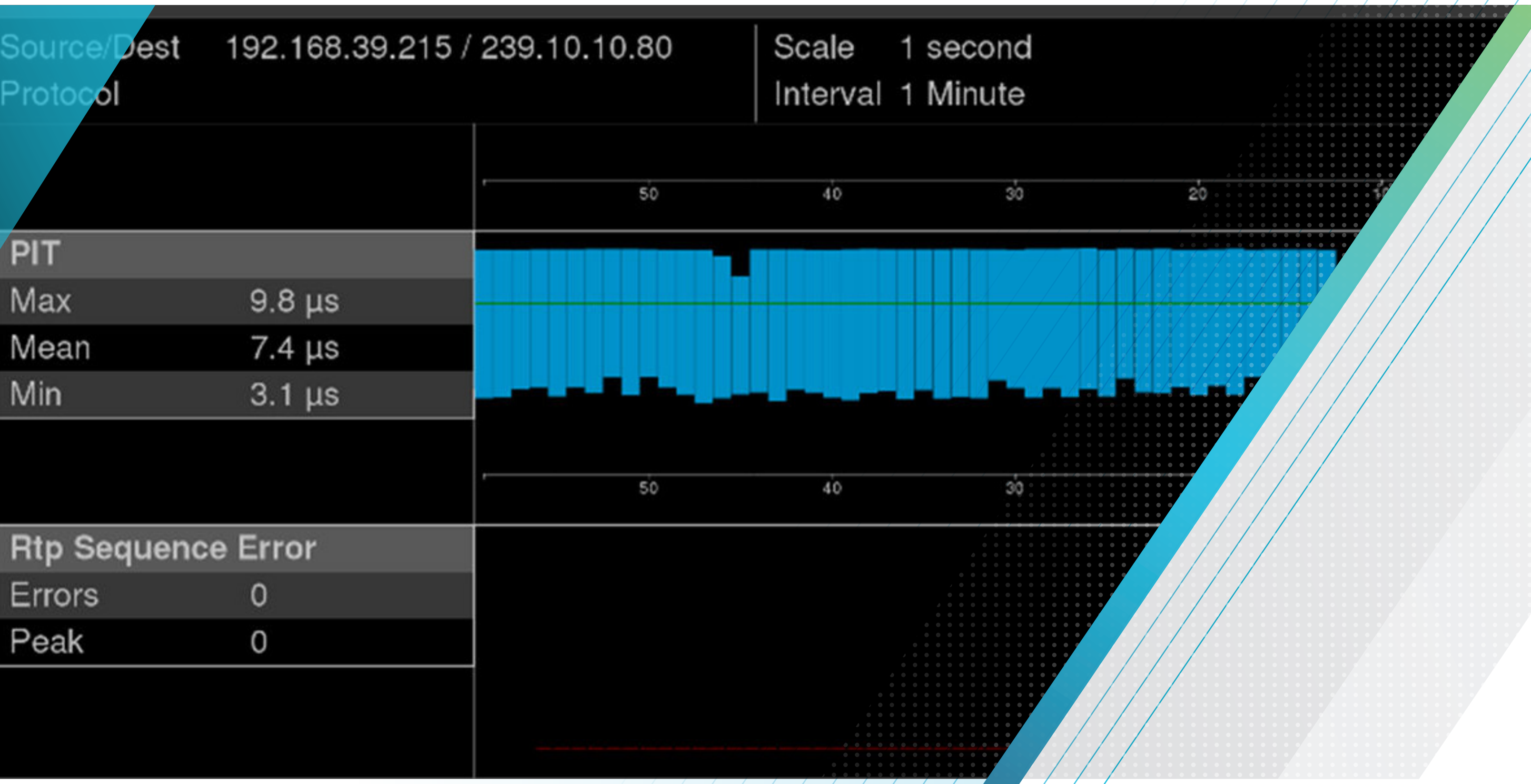
Diagnosing and Resolving Faults in an Operational IP Video Network

WHITE PAPER



Source/Dest 192.168.39.215 / 239.10.10.80
Protocol

Scale 1 second
Interval 1 Minute

PIT	
Max	9.8 µs
Mean	7.4 µs
Min	3.1 µs

Rtp Sequence Error	
Errors	0
Peak	0

Introduction

Deployment of IP Video networks in production and other operational applications exploits the ability to use Commercial Off-The-Shelf (COTS) IT-based infrastructure, which takes advantage of the economies of scale of the IT industry when compared with the relatively small broadcast industry. Additional advantages of reducing cabling cost and weight along with the much greater routing flexibility mean that in many parts of the World, trials, proofs of concept and early deployments of IP Video are already in place. Having said this, IP does bring with it technical challenges, including jitter; latency; the risk of dropped packets, an inherent lack of synchronicity along with asymmetry which results in different path delays upstream and downstream. Also, IP is a complex set of bi-directional protocols requiring a knowledge of both the source and destination before deployment. Another issue is that deploying IP for video production applications is effectively the collision of the two Worlds of video engineering and network engineering. Video engineers are used to and comfortable with the use of SDI, coax., patch panels, black burst and tri-level for timing and above all, signal quality. The challenge for the video engineer is to understand IT technology and impact of an IT infrastructure on the video. On the other hand, network engineers are familiar and comfortable with, IP Flows, Protocols, Network traffic, Router Configuration and Precision Time Protocol (PTP) and Network Time Protocol (NTP) for timing. The biggest difference however is that in most data center applications, lost data can be re-sent – this is not the case with high bitrate Video. The challenge for the network engineer is in understanding video technology and its impact on IT infrastructure. It is clear that the need is diagnostic monitoring and analysis tools that are usable by both video engineers and network engineers.

Video Engineer

- SDI, Analog, Audio and Patch Panels
- Black Burst and Tri Level Sync
- Importance of signal quality
- Challenge in understanding the IT technology and its impact on Video

Network Engineer

- IP Flows, Protocols, Network traffic, Router Configuration
- Precision Time Protocol
- Data can be resent - not the case with high bitrate Video
- Challenge in understanding video technology and its impact on IT infrastructure

What Problems Can Occur in IP Networks?

A lot of the issues that can cause problems in IP networks can be traced back to packet jitter. As will be explained in the next section, excessive packet jitter can lead to buffer overflows and underflows causing dropped packets and stalled data flows. Other problems that can be experienced are associated with the timing delay and asymmetry of PTP packet flows. In hybrid SDI and IP workflows, it is also necessary to ensure that the relationship between the SDI and IP video is consistent to enable seamless frame accurate switching. This can be achieved by measuring the relationship between the Black Burst/Tri-Level Sync and the PTP clock and making any necessary correction by skewing the SDI syncs with reference to the PTP clock.

WHAT CAUSES IP PACKET JITTER?

In any digital system, Jitter is any deviation from, or displacement of, the periodicity of the signal. In IP networks carrying constant bitrate data, jitter is the deviation from the periodicity of the packet arrival interval at a receiver. This can be caused by incorrect queueing or configuration issues, but assuming that the routers and switches are all configured and operating correctly, the most common cause of jitter is network congestion at router/switch interfaces.

A degree of jitter is inherent in any IP network due to its asynchronous nature. Obviously the application within a network element will likely require the data to be received in a non-bursty form and as a result, receiving devices adopt a de-jitter buffer. The application then receives the packets from the output of this buffer rather than directly, with packets flowing out of the buffer at a regular rate, smoothing out the variations in the timing of the packets flowing into the buffer.

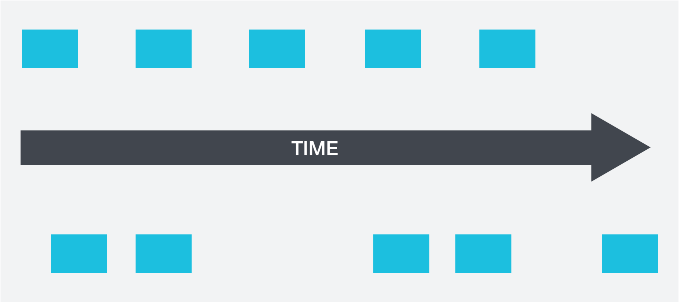


FIGURE 1. Packet jitter is deviation from the periodicity of the packet arrival interval.

WHAT CAN BE THE IMPACT OF EXCESSIVE JITTER?

In the previous section, we saw that packets flow out of a receiver's buffer at a steady rate. This is known as the "drain rate" of the buffer. Conversely the rate at which a buffer receives data is known as the "fill rate". Selecting the size of the buffer is important as if the buffer size is too small then if the drain rate exceeds the fill rate, then it is possible that too small a buffer could underflow, resulting in stalled packet flow. If the sink rate exceeds the drain rate, then at some point the buffer will overflow, resulting in packet loss. However, if the buffer size is too large, then the network element will introduce excessive latency. As can been seen in the above diagram, network jitter causes the packets to become non-periodic and as such the buffer fill rate will no longer be constant. As the jitter becomes greater, the aperiodicity becomes larger. At some point this aperiodicity will lead to the condition where the buffer's fill and drain rates become so uneven that the buffer will either underflow, leading to stalling or overflow, leading to packet loss.

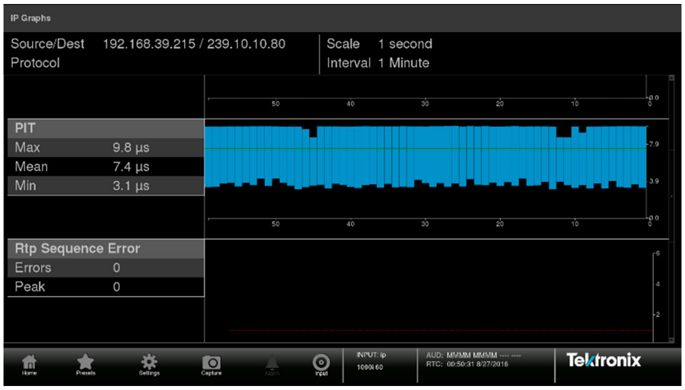
With the case of high bitrate video, either buffer underflow or buffer overflow will likely lead to impaired video. It should also be noted that port over subscription will of course also lead to packet loss.

Network Congestion → Excessive Jitter → Buffer Overflow → Packet Loss

FIGURE 2.

MEASURING JITTER IN REAL TIME PROTOCOL (RTP) NETWORKS

We have already seen that in networks carrying constant bitrate data, jitter is the deviation from periodicity at a receiver and as such, given an accurate clock in the receiver, jitter can be measured simply by measuring the time-stamps of the packet arrival times and plotting the inter-arrival intervals versus time.



IP Graphs

Source/Dest 192.168.39.215 / 239.10.10.80
Protocol

Scale 1 second
Interval 1 Minute

PIT	
Max	9.8 µs
Mean	7.4 µs
Min	3.1 µs

Rtp Sequence Error	
Errors	0
Peak	0

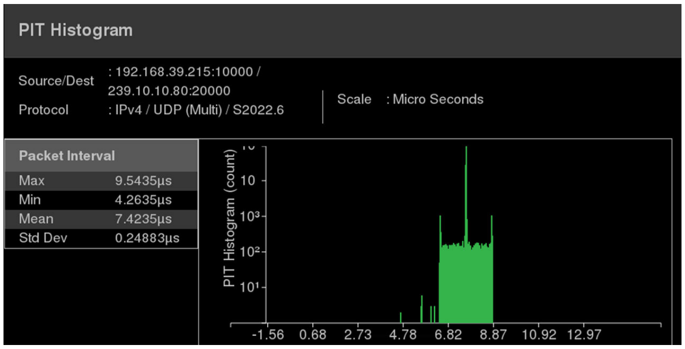
INPUT: ip
1080i 60

AUD: MMMM MMMM ---- ----
RTC: 00:50:31 8/27/2016

FIGURE 3. Packet inter-arrival intervals plotted versus time.

This method is useful to identify variances in jitter over time, but it is also useful to be able to plot the distribution of inter-arrival intervals versus frequency of occurrence as a histogram. We have also already seen that If the jitter value is so large that it causes packets to be received out of the range of the de-jitter buffer, then the out-of-range packets are dropped. Being able to identify outliers is an aid in identifying if the network jitter performance is either likely to or already the cause of packet loss.

This method is useful to identify variances in jitter over time, but it is also useful to be able to plot the distribution of inter-arrival intervals versus frequency of occurrence as a histogram. We have also already seen that If the jitter value is so large that it causes packets to be received out of the range of the de-jitter buffer, then the out-of-range packets are dropped. Being able to identify outliers is an aid in identifying if the network jitter performance is either likely to or already the cause of packet loss.



PIT Histogram

Source/Dest : 192.168.39.215:10000 / 239.10.10.80:20000
Protocol : IPv4 / UDP (Multi) / S2022.6

Scale : Micro Seconds

Packet Interval	
Max	9.5435µs
Min	4.2635µs
Mean	7.4235µs
Std Dev	0.24883µs

FIGURE 4. Packet inter-arrival intervals plotted versus frequency of occurrence.

With constant high-bitrate data, If the jitter distribution is extremely broad, it is likely that network congestion and hence network jitter magnitude is significant enough to cause packet loss. The corollary is that if the jitter distribution is narrow (as in the case shown above), and the system is experiencing packet loss, network congestion is unlikely to be the cause.

It might be assumed that that this distribution measurement could be used to estimate the buffer size needed to de-jitter the traffic flow, but it is important to consider that it takes no account of the ordering of the packet inter-arrival interval samples. In essence a series of packets with long inter-arrival intervals, will inevitably result in a corresponding burst of packets with short inter-arrival intervals. It is this burst of traffic, that can result in buffer overflow conditions and lost packets. This occurs if the sink rate exceeds the drain rate for a period of time that exceeds the length of the remaining buffer size, when represented in microseconds.

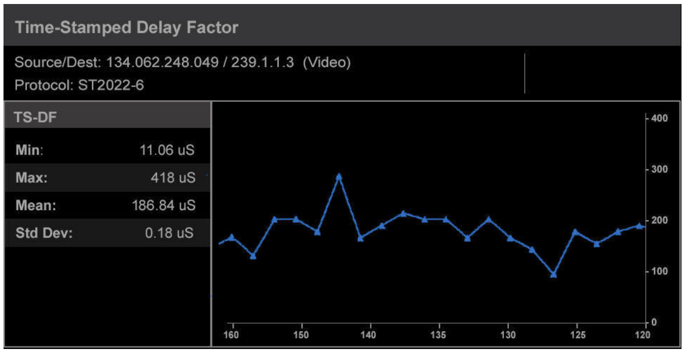
Burstiness leads to buffer overflow if:

sink rate > drain rate for Δ_T > remaining temporal buffer size

ESTABLISHING DE–JITTER BUFFER SIZE

We have already seen that merely measuring the packet inter-arrival times cannot realistically be used to predict the necessary de-jitter buffer size. There is however an alternative form of jitter measurement know as Delay Factor (DF) that can be used to establish de-jitter buffer sizes. Delay Factor is a temporal measurement, which in the case of high bitrate video is represented in microseconds, that indicates how much time is required to drain a virtual buffer at a network node. At any given time, the Delay Factor represents the temporal buffer size at that network node necessary to de-jitter the traffic flow.

One such form of DF measurement takes advantage of the fact that RTP carries time stamp information which is defined by RFC 3550 as reflecting the sampling instant of the first octet in the RTP data packet (the timestamp format being the same as that of NTP). This measurement is known as Time-Stamped Delay Factor or TS-DF, as defined by EBU Tech 3337. This method is in the public domain and is well suited to high bitrate media over RTP applications. TS-DF is based on correlating arrival times of network packets with the time-stamp field in the RTP header.



Time-Stamped Delay Factor

Source/Dest: 134.062.248.049 / 239.1.1.3 (Video)
Protocol: ST2022-6

TS-DF	
Min:	11.06 uS
Max:	418 uS
Mean:	186.84 uS
Std Dev:	0.18 uS

FIGURE 5. TS-DF represents temporal buffer size in microseconds.

The Time-stamped Delay Factor measurement is based on the Relative Transit Time defined in RFC 3550 (RTP: A Transport Protocol for Real-Time Applications). This is defined as the difference between a packet's RTP timestamp (held in the RTP header) and the receiver's clock at the time of arrival, measured in the same units. The TS-DF measurement period is 1 second. In this algorithm, the first packet at the start of the measurement period is considered to have no jitter and is used as a reference packet.

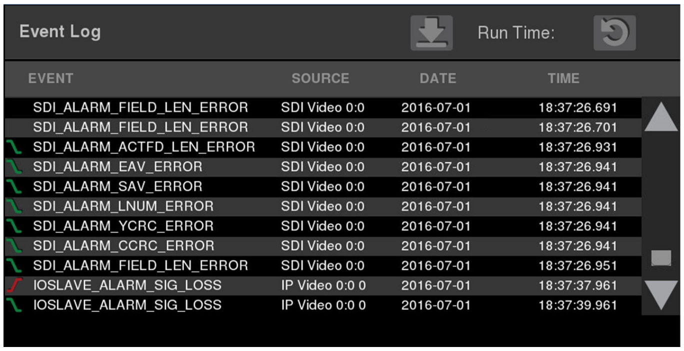
For each subsequent packet which arrives within the measurement period, the Relative Transit Time between this packet and the reference packet is calculated and at the end of the measurement period, the maximum and minimum values are extracted and the Time-stamped Delay Factor is calculated as:

$$\text{TS-DF} = D(\text{Max}) - D(\text{Min})$$

Unlike the jitter algorithm in RFC 3550, this algorithm does not use a smoothing factor and therefore gives a very accurate instantaneous result. The Tektronix hybrid SDI and IP media analysis platform implements both IP packet inter-arrival jitter measurements as well as the RTP specific TS-DF measurement.

ESTABLISHING ROOT CAUSE

Another consideration is to establish the root cause of video impairments. It is necessary to understand that if impairments are being experienced, whether IP errors are the root cause, or if some other fault is causing the impairment.

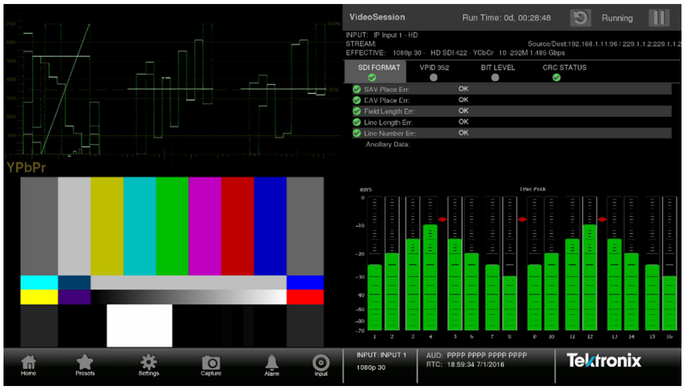

Event Log

Run Time:

EVENT	SOURCE	DATE	TIME
SDI_ALARM_FIELD_LEN_ERROR	SDI Video 0:0	2016-07-01	18:37:26.691
SDI_ALARM_FIELD_LEN_ERROR	SDI Video 0:0	2016-07-01	18:37:26.701
SDI_ALARM_ACTFD_LEN_ERROR	SDI Video 0:0	2016-07-01	18:37:26.931
SDI_ALARM_EAV_ERROR	SDI Video 0:0	2016-07-01	18:37:26.941
SDI_ALARM_SAV_ERROR	SDI Video 0:0	2016-07-01	18:37:26.941
SDI_ALARM_LNUM_ERROR	SDI Video 0:0	2016-07-01	18:37:26.941
SDI_ALARM_YCRC_ERROR	SDI Video 0:0	2016-07-01	18:37:26.941
SDI_ALARM_CCRC_ERROR	SDI Video 0:0	2016-07-01	18:37:26.941
SDI_ALARM_FIELD_LEN_ERROR	SDI Video 0:0	2016-07-01	18:37:26.951
IOSLAVE_ALARM_SIG_LOSS	IP Video 0:0 0	2016-07-01	18:37:37.961
IOSLAVE_ALARM_SIG_LOSS	IP Video 0:0 0	2016-07-01	18:37:39.961

FIGURE 6. Time-correlated Video and IP errors.

It is possible to establish whether packet errors are the root cause of video errors by correlating the time stamps of video errors with the time stamps of RTP packet errors.


VideoSession Run Time: 0d, 00:28:48 Running

INPUT: IP Input 1 - HD
STREAM: Source/Dest:192.168.1.11:96 / 229.1.1.2:229.1.1.2
EFFECTIVE: 1080p 30 - HD SDI 422 - YCbCr 10 -292M 1.485 Gbps

SDI FORMAT	VPID 352	BIT LEVEL	CRC STATUS
✓	●	●	✓

✓ SAV Place Err:	OK
✓ EAV Place Err:	OK
✓ Field Length Err:	OK
✓ Line Length Err:	OK
✓ Line Number Err:	OK
Ancillary Data:	

INPUT: INPUT 1
1080p 30

AUD: PPPP PPPP PPPP PPPP
RTC: 18:59:34 7/1/2016

FIGURE 7. Picture, Waveform Audio Bars and Error Log.

A video CRC error does not in itself confirm that the video is impaired and in addition to logging errors, it is desirable to use traditional monitoring methods such as picture and waveform displays as well as audio bars for confidence monitoring.

What is PTP?

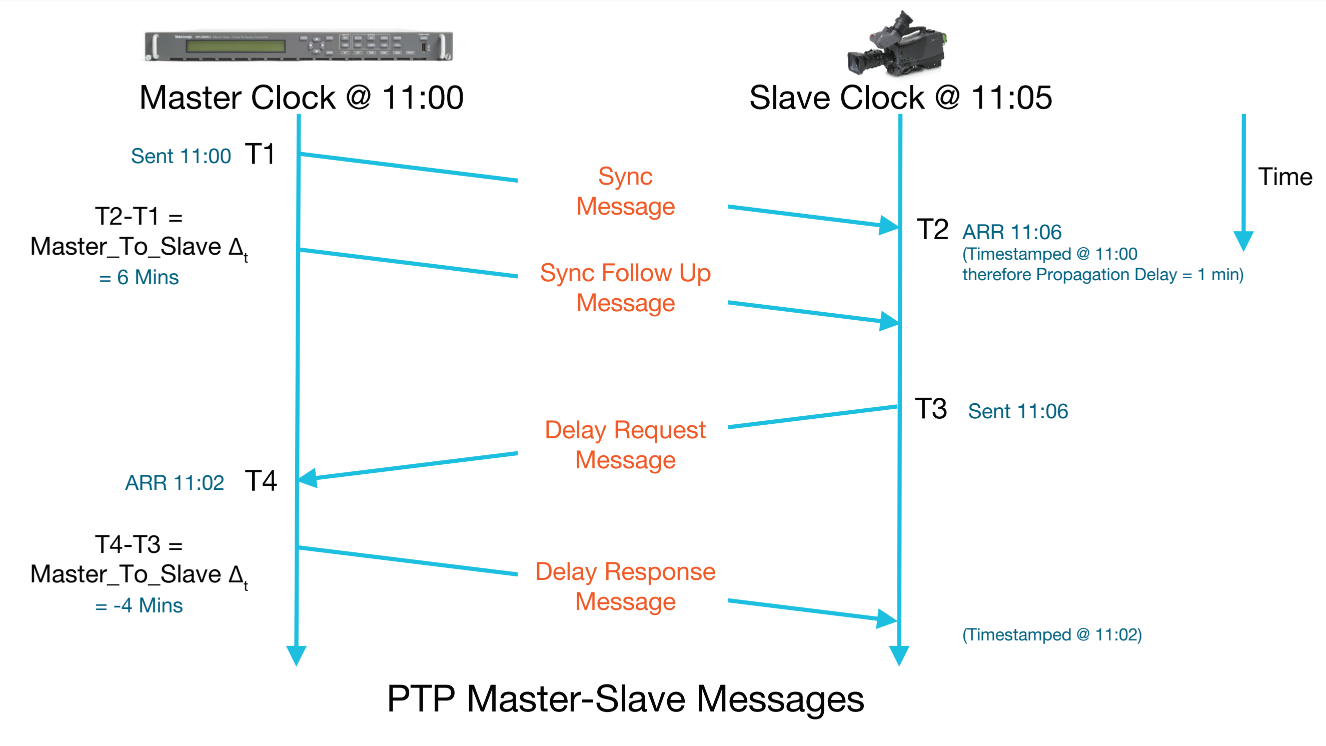
IP based networks can be considered to be asynchronous in that device clocks, at nodes distributed across the network have no inherent concept of system time. Precision Time Protocol (PTP: defined by IEEE 1588) is intended to synchronize the real-time clocks of different nodes on an Ethernet network. It should however be noted that PTP does not make the network itself synchronous (as is the case with Synchronous Ethernet also referred to as SyncE). The most recent version is IEEE 1588-2008, also known as PTP version 2 and SMPTE has developed a standard based on PTP version 2 specifically intended for broadcast video applications, known as SMPTE ST 2059.

The adoption of video over IP along with the use of PTP to synchronize the real-time clocks of different network nodes infers that any such network requires a network time server, in order to provide the PTP genlock functionality equivalent to that delivered by a Sync Pulse Generator (SPG) in SDI networks. Any logical grouping of clocks that are synchronized together are referred to as a PTP domain. Note that a clock in one domain may not be synchronized to clocks in another domain.

This PTP network time server is generally referred to as a PTP Grandmaster, with a device that derives its timing synchronization from PTP being referred to as a PTP Slave. A Master is a device that provides the time in a given PTP domain and a Slave is a device that synchronizes to a Master. A Grandmaster is a Master that is providing the ultimate source of clock synchronization in a network. In the context of broadcast applications, PTP Grandmasters are usually synchronized to GPS, GLONASS or both.

HOW IS TIME DERIVED IN A PTP NETWORK?

A network of Slave devices connected to a single Master is known as a domain and within any PTP domain there are a number of message types used to establish time within that network. Announce messages are used to establish the synchronization hierarchy and provide the clock status and clock criteria used to determine which clock becomes the Grandmaster. Sync and Follow-up messages are transmitted by the Grandmaster and are used by Slaves to derive the time. Delay Request messages are a request for timing information and are sent from the Slave to the Grandmaster in order to determine the reverse path propagation delay between the Slave and the Grandmaster. A Delay Response message is sent by the Grandmaster and contains the time of receipt of the Delay Request message by the Grandmaster.



Offset = (Master_To_Slave Δ_t – Slave_To_Master Δ_t)/2 **= 5 Mins**
Oneway Delay = (Master_To_Slave Δ_t + Slave_To_Master Δ_t)/2 **= 1 Min**

FIGURE 8. Deriving the Correct Time in a PTP Network.

As defined, PTP is a method for distributing time over a network, with a single Grandmaster providing the source of time, to synchronize one or more Slaves. The Grandmaster periodically transmits Sync and Follow up messages, which the slaves use to derive the time. In an ideal World the network delay could be programmed into each slave which could then be offset to the time in the received packet to derive the correct time. Such symmetry can only be relied upon in point-to-point IP links. Unfortunately, the path delay in switched/routed IP networks is variable at different network nodes and can also be asymmetric, in order to take account of this, the Slave devices must periodically send Delay Request messages to the Grandmaster. The Grandmaster accurately time stamps these messages on receipt and the time of receipt is sent back to the Slave in a Delay Response message.

Using the diagram above as a reference, the Slave is now able to calculate the difference between its own clock and that of the Grandmaster using the Master-to-Slave sync packet delay (T2-T1) and Slave-to-Master delay request packet-delay (T4-T3). The Offset (Slave Time – Master Time) = [(T2-T1)-(T4-T3)]/2. For the slave time to be absolutely correct, the propagation delay in both directions must be equal.

THE BEST MASTER CLOCK ALGORITHM

A fundamental component of PTP is the Best Master Clock Algorithm (BMCA) which runs on all clocks in the network. The BMCA is intended to provide resilience by allowing the most accurate clock to take over in the event that the current Grand Master is unable to continue:

- Loses GPS lock
- Becomes disconnected from the network
- Unable to act as Grand Master for any other reason

The selection of which clock is to become the Grandmaster is determined by the following BMCA criteria, listed in order of precedence:

1. Priority 1 Field (range 0-255, normally set to 255 for slaves and the lowest value <= 128 wins for masters)
2. Clock class (e.g. GPS locked or free running)
3. Clock accuracy
4. Clock variance (jitter and wander)
5. Priority 2 Field (range 0-255, normally set to 255 for slaves and the lowest value <= 128 wins for masters)
6. Tie-breaker is Clock Source Port ID (usually the Ethernet MAC address)

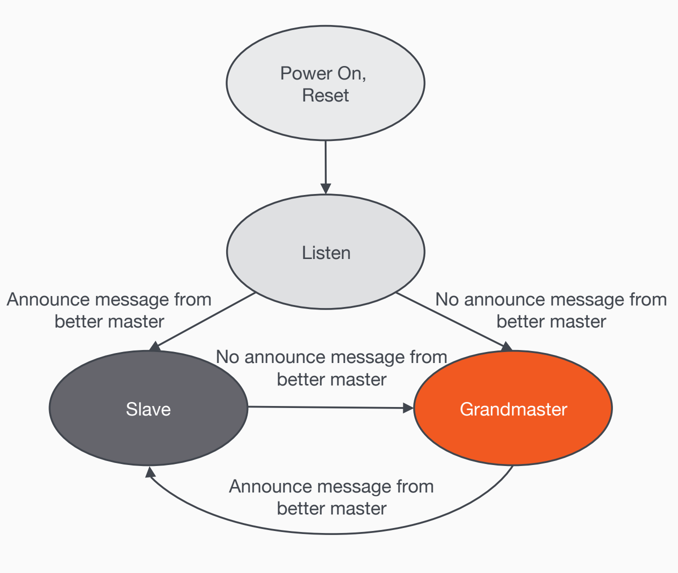

Power On, Reset
Listen
Announce message from better master
No announce message from better master
No announce message from better master
Slave
Grandmaster
Announce message from better master

FIGURE 9. Determining Master/Slave Clock State.

HOW IS IT POSSIBLE TO ENSURE THAT A BACKUP GRANDMASTER TAKES OVER IN THE EVENT OF FAILURE?

In order to establish an automatic main and backup Grandmaster fail over the Priority Two field is used to identify main and backup clocks between two or more otherwise identical redundant Grandmasters as follows:

- Main Grandmaster (Priority One Field = 128; Priority Two Field = 127)
- Backup Grandmaster (Priority One Field =128; Priority Two Field = 128)

If both identical Masters are locked to GPS, they will have the same clock quality, so the lowest Priority Two Field value will select which is the Grandmaster. If the Main clock loses GPS lock, then the Backup clock becomes the Better Master and will take over as Grandmaster.

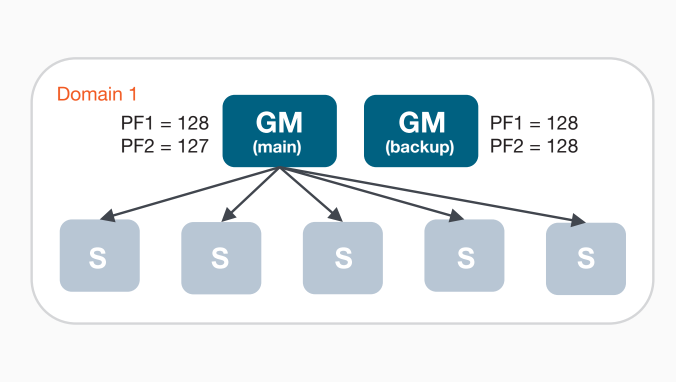


FIGURE 10. Configuration of Main/Backup Grandmasters for Automatic Failover.

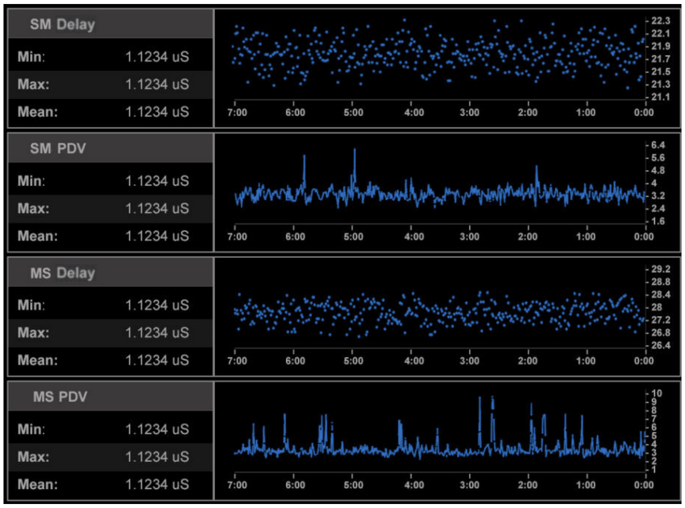
It is worth noting that if any GPS synchronized Master loses GPS lock, it will of course itself become free running and will be reliant upon its own internal local oscillator. However good this oscillator is, over an extended period of time it will drift, even if slightly relative to the GPS clock. Once GPS lock is re-acquired, unless the Master's local oscillator phase-lock loop (PLL) is driven slowly to re-synchronize with the GPS clock, then the system can suffer from what is known as "Sync Shock" when the Master's clock frequency suddenly changes. Whilst this may be acceptable in some IT applications, this of course is highly undesirable in a video production application. In the case of the SPG8000A, the "Stay Genlock" feature is designed specifically to avoid the problem of Sync Shock through careful control of the PLL.

In the case of live video production applications, a high degree of clock accuracy is required for synchronous video processing. A Grandmaster device such as the SPG8000A is locked to GPS (or GLONASS or both to provide greater constellation resilience), with the Grandmaster's local oscillator being phase-locked to the GPS reference.

With respect to time-stamping of packets, a dedicated hardware approach at the MAC or PHY layer is best used, to avoid variable latency in a software-based stack.

PTP MEASUREMENT AND MONITORING

When considering accurate PTP performance, it is important to understand whether the network is excessively asymmetric. That is, that the packet delay from the master to the slave device (M-S) is substantially different from the packet delay from the slave to the master (S-M). If the propagation delay in both directions is different, then the slave is offset to "correct" for this by adjusting its clock to a value of half the asymmetry. The clock's control loop adjusts the slave time to make the Master-to-Slave and Slave-to-Master propagation delays appear to be equal. If the asymmetry is excessive then the absolute clock value will not compensate accurately for either M-S or S-M packet delays.



SM Delay	
Min:	1.1234 uS
Max:	1.1234 uS
Mean:	1.1234 uS

SM PDV	
Min:	1.1234 uS
Max:	1.1234 uS
Mean:	1.1234 uS

MS Delay	
Min:	1.1234 uS
Max:	1.1234 uS
Mean:	1.1234 uS

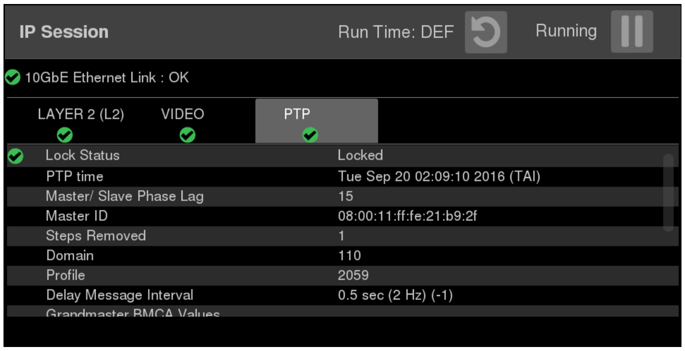
MS PDV	
Min:	1.1234 uS
Max:	1.1234 uS
Mean:	1.1234 uS

FIGURE 11. Measuring S-M/M-S packet delay asymmetry and packet delay variation.

Also to ensure clock accuracy, switches and routers need to account for their own queuing delays and as such need to be PTP aware. That is, they act either a transparent clock or a boundary clock, which in both cases account for their own queuing delays, but in different ways.

A Boundary clock receives PTP timing from the Grand Master, acting as a slave on one port. It uses this timing to phase lock its internal clock, which the device then to act as a PTP master and create new Sync and Announce messages on the output ports. In this way the queuing delay of the boundary clock is irrelevant since the PTP messages are newly time-stamped as they leave the device.

A switch operating in transparent clock mode measures the transit time of the PTP messages as they propagate through the switch. It then provides that time to the slave in the correction field of the PTP messages it carries. The slaves use this correction in the calculation of the offset and frequency. Since the delay in the switch is removed from the calculation result, the slave timing is this not affected by queuing delay within the switch.



✓ 10GbE Ethernet Link : OK

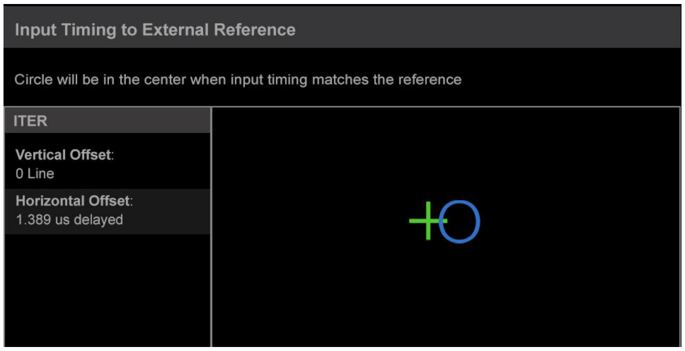
✓	Lock Status	Locked
	PTP time	Tue Sep 20 02:09:10 2016 (TAI)
	Master/ Slave Phase Lag	15
	Master ID	08:00:11:ff:fe:21:b9:2f
	Steps Removed	1
	Domain	110
	Profile	2059
	Delay Message Interval	0.5 sec (2 Hz) (-1)
	Grandmaster BMCA Values	

FIGURE 12. Monitoring PTP packet headers to ensure that devices are on the correct domain.

Devices in the same network should be on the same domain and it is vital that the BMCA priority levels are set correctly to both ensure that the correct best Master is chosen to be Grandmaster and that a suitable backup Master is chosen in the event of main Grandmaster failover.

HYBRID BLACK BURST/TRI–LEVEL AND PTP NETWORKS

For the foreseeable future, many video networks will use a combination of SDI and IP. In these cases, it is vital that the timing of the BB/Tri-Level is synchronous with the PTP if frame accurate switching is to be achieved.



Input Timing to External Reference

Circle will be in the center when input timing matches the reference

ITER

Vertical Offset: 0 Line

Horizontal Offset: 1.389 us delayed

FIGURE 13. Measuring the time relationship between BB/Tri-Level and PTP.

This can be achieved simply by measuring the timing relationship between PTP and Black Burst/Tri-Level and then adjusting the BB/Tri-Level to PTP offset in a hybrid SPG/PTP Grandmaster such as the Tektronix SPG8000A.

A FINAL CONSIDERATION

In live production applications, network experts may not be present on the production site and networking equipment also may not necessarily be in a location that is easily accessible.

FIGURE 14. Remote control ability enables on-location access to network expertise.

It is desirable that any diagnostic equipment should have the ability to be controlled remotely.

Summary

IP offers both opportunities and challenges to broadcasters in an environment where the worlds of Video Engineering and Network Engineering collide, it is essential that diagnostic monitoring and analysis tools are usable by both Video Engineers and Network Engineers

It is necessary to monitor jitter performance over time to avoid buffer overflows and consequent packet loss. Time-Stamped Delay Factor is a useful measurement for assisting with network provisioning as well as quickly identifying excessive jitter conditions that will lead to buffer issues. If network issues do occur is it is both necessary to determine the impact in terms of video errors, but also the impact in terms of picture impairment.

PTP provides the necessary synchronization required to use IP in live production workflows and monitoring timing stability is important. Finally, the transition to IP will be gradual and “Hybrid” SDI/IP workflows and hence hybrid diagnostic monitoring and analysis tools as well as hybrid Sync Pulse Generators/Grandmasters will be needed for the foreseeable future.

Contact Information:

Australia*	1 800 709 465
Austria	00800 2255 4835
Balkans, Israel, South Africa and other ISE Countries	+41 52 675 3777
Belgium*	00800 2255 4835
Brazil	+55 (11) 3759 7627
Canada	1 800 833 9200
Central East Europe / Baltics	+41 52 675 3777
Central Europe / Greece	+41 52 675 3777
Denmark	+45 80 88 1401
Finland	+41 52 675 3777
France*	00800 2255 4835
Germany*	00800 2255 4835
Hong Kong	400 820 5835
India	000 800 650 1835
Indonesia	007 803 601 5249
Italy	00800 2255 4835
Japan	81 (3) 6714 3010
Luxembourg	+41 52 675 3777
Malaysia	1 800 22 55835
Mexico, Central/South America and Caribbean	52 (55) 56 04 50 90
Middle East, Asia, and North Africa	+41 52 675 3777
The Netherlands*	00800 2255 4835
New Zealand	0800 800 238
Norway	800 16098
People's Republic of China	400 820 5835
Philippines	1 800 1601 0077
Poland	+41 52 675 3777
Portugal	80 08 12370
Republic of Korea	+82 2 6917 5000
Russia / CIS	+7 (495) 6647564
Singapore	800 6011 473
South Africa	+41 52 675 3777
Spain*	00800 2255 4835
Sweden*	00800 2255 4835
Switzerland*	00800 2255 4835
Taiwan	886 (2) 2656 6688
Thailand	1 800 011 931
United Kingdom / Ireland*	00800 2255 4835
USA	1 800 833 9200
Vietnam	12060128

*** European toll-free number. If not accessible, call:** +41 52 675 3777

Find more valuable resources at TEK.COM