Distributed Monitoring

Pervasive Visibility & Monitoring, Selective Drill-Down

Rony Kay

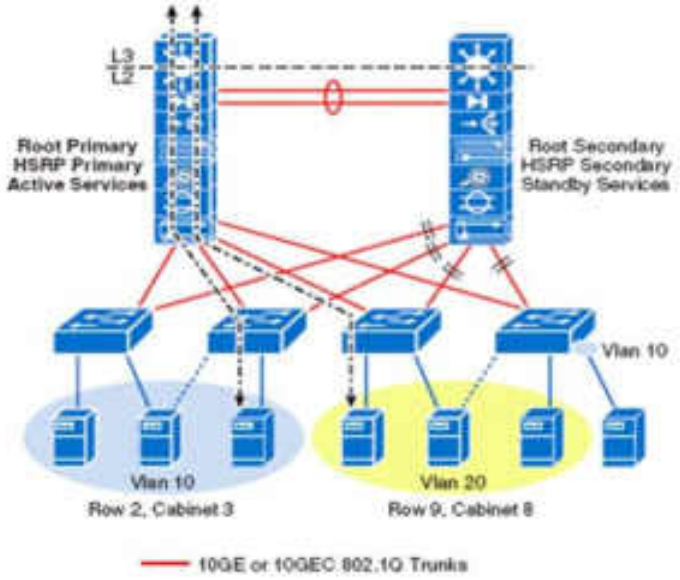
www.cpacket.com, 2012

Pervasive Visibility, Monitoring, and Drill Down

- cPacket delivers solutions for intelligent network visibility to enable efficient data-center and clouds operations
- Key market drivers include Data centers, clouds, virtualization, distributed storage, SaaS/PaaS, …

Simple Fact: More Complexity & Higher Speed

Complex Data Center Traffic



Traffic Jams and Accidents

- **Problem**: assure service quality and user experience
- **Solution**: pervasive visibility & proactive pre-instrumentation

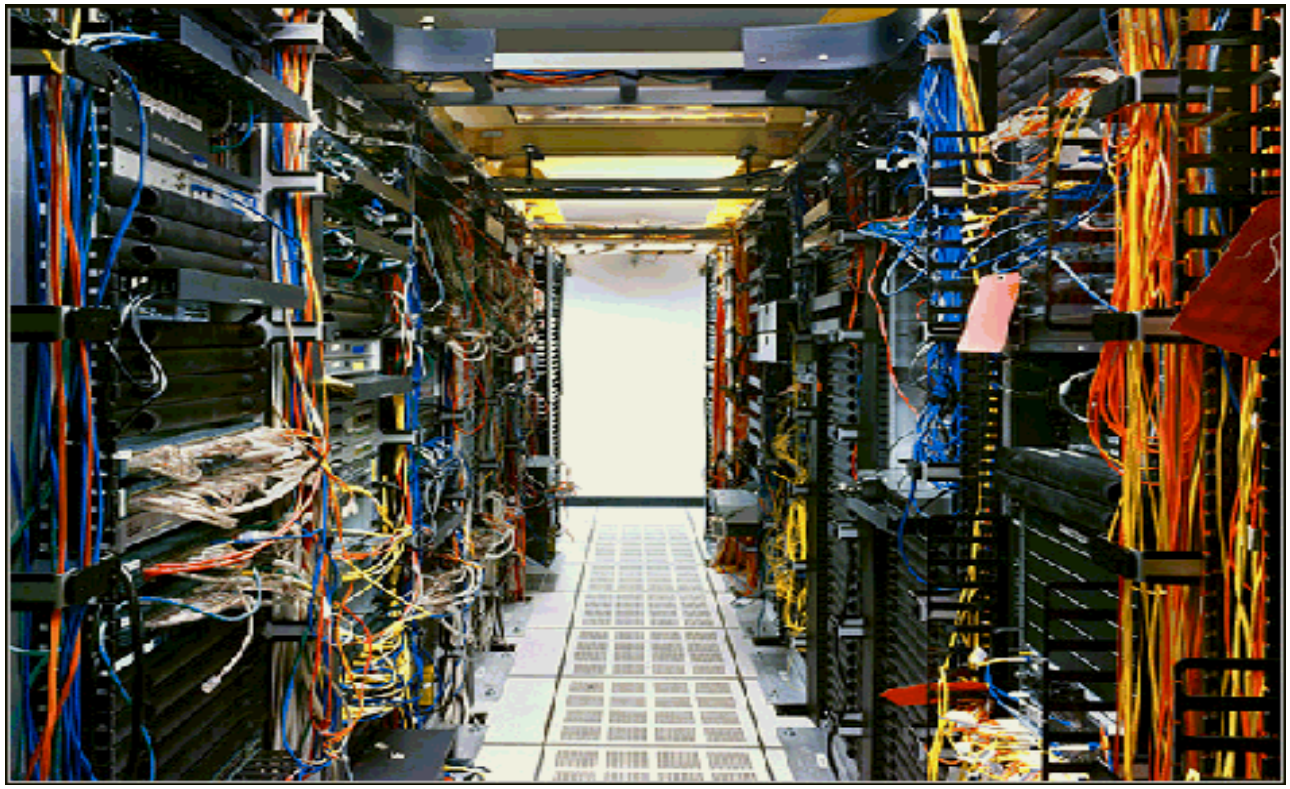
Presentation/Demo Context and Scope

- Wireshark is an effective protocol analysis tool (L2-L7)

- Protocol analysis should isolate the root-cause, e.g., is it the server, the client, or network ? … (or maybe the user)
  - BUT for network issues, it cannot pinpoint a specific hop in the path

- Trouble-shooting teams, YOU, operate in “cloudy” environment
  - Some murky **PROBLEM** statement, e.g., “ … sometimes my app is slow …”

But Where Do I Start Looking?



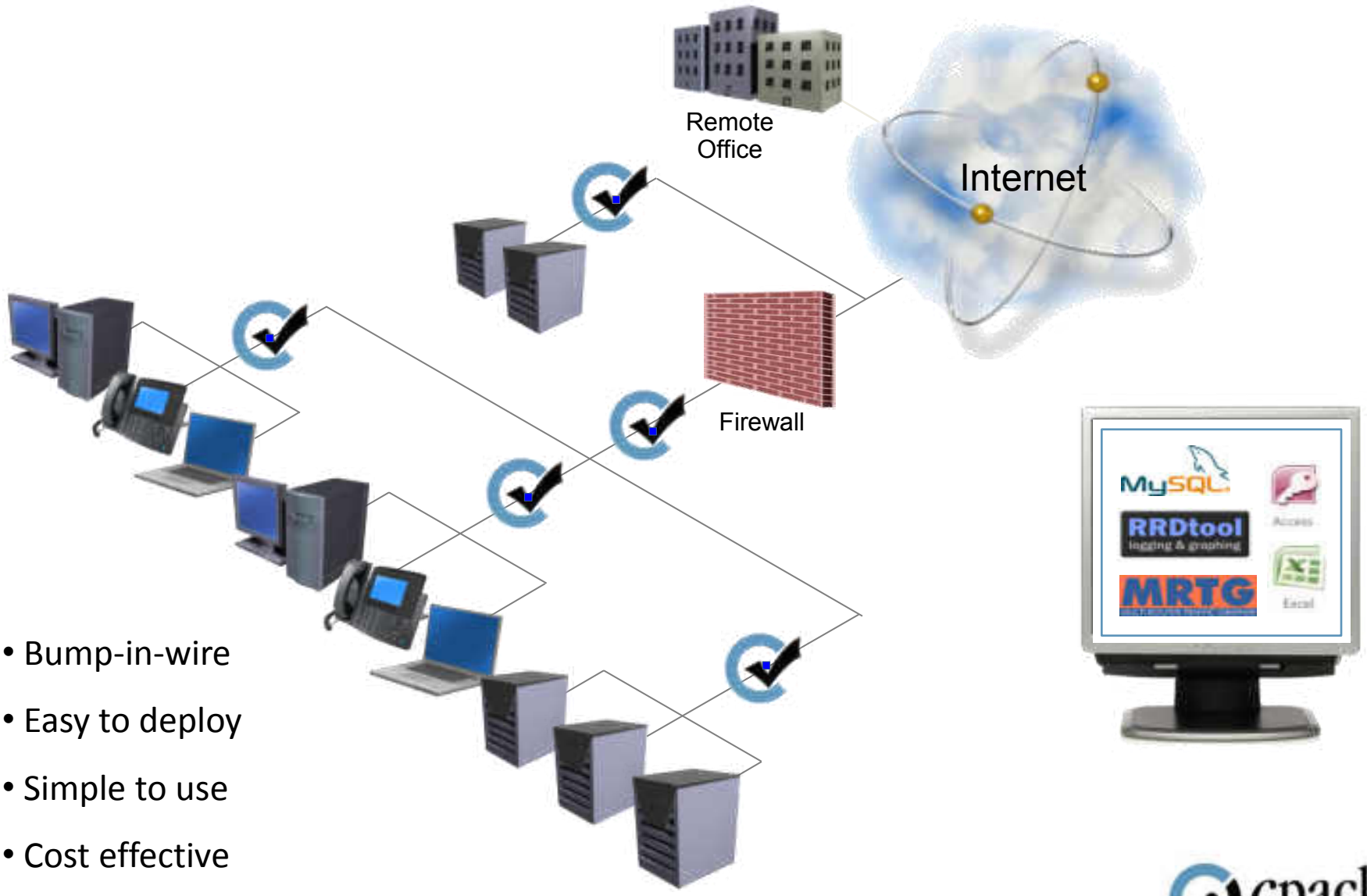
- **Protocol Analysis relies on access to RELEVANT data ,**
  BUT not too much and not too little

- Troubleshooting begins with a complaint, degraded user experience, or indication of negative impact on business ops
- Often the “intermittent” type of issues are not fully resolved due to lack of relevant data
- Significant **time, effort, and aggravation** are spent on getting relevant packets into Wireshark
  - Downloads, tickets, emails, cable runs, frantic phone calls, USB keys, …

Fundamental Scalability Gap

- Fact: deeper dive into protocols analysis requires an “expert”
- **The GAP: traffic volume and links number increase exponentially, while the number of experts does not keep up**
- The experts, YOU, need more efficient real-time visibility and more productive and immediate access to RELEVANT data
  - Suspected hot spots, health indicators, and specific packets trace

Vision: Pervasive Integrated Visibility



- Bump-in-wire
- Easy to deploy
- Simple to use
- Cost effective

Products and Network Intelligence Solutions

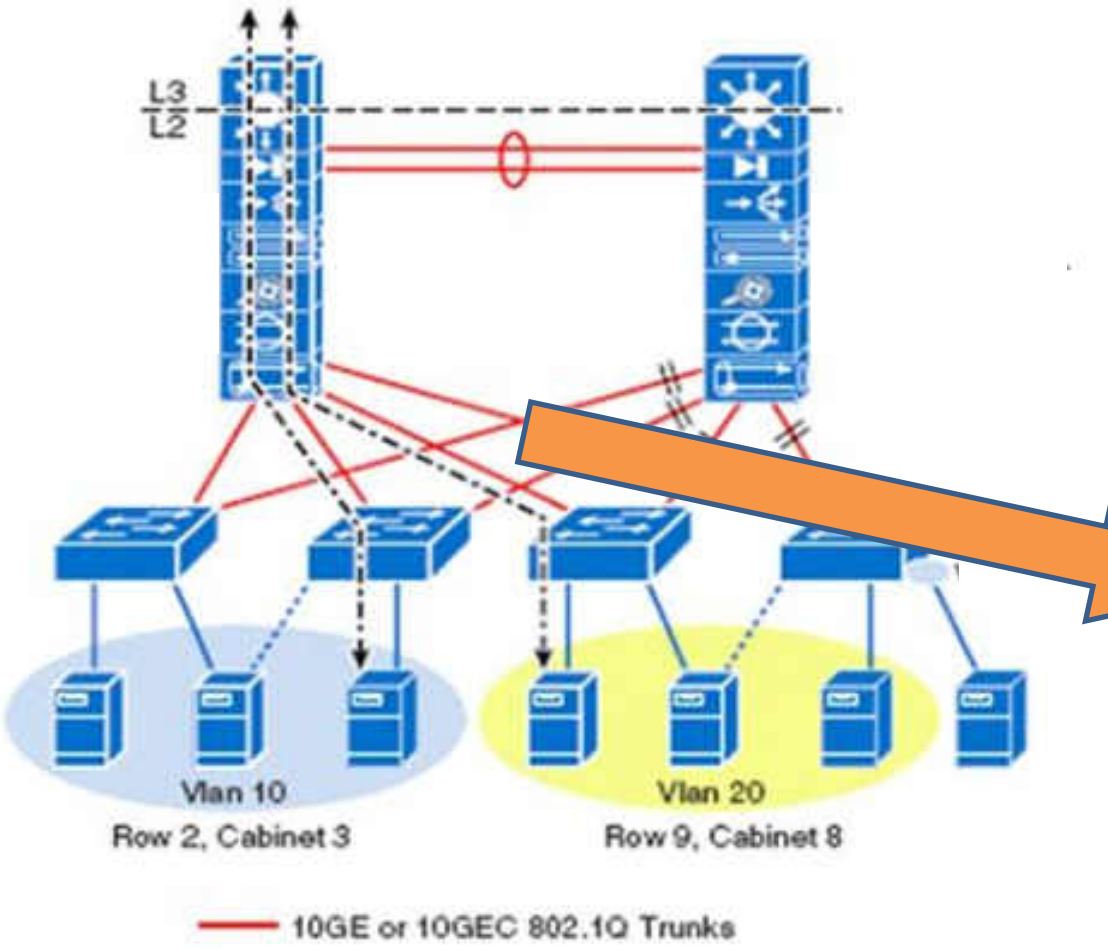
Standard Off-the-Shelf

Special Purpose Custom

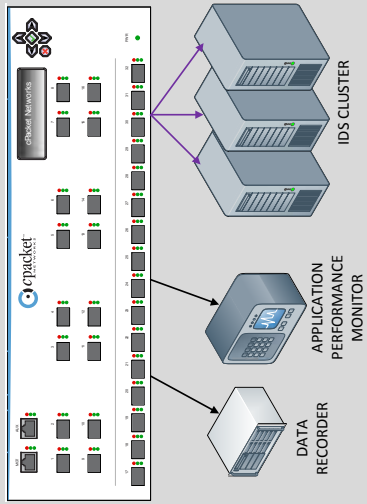
Versatile HW/SW architecture for a wide spectrum of intelligent Networking, including: visibility, monitoring, measurement

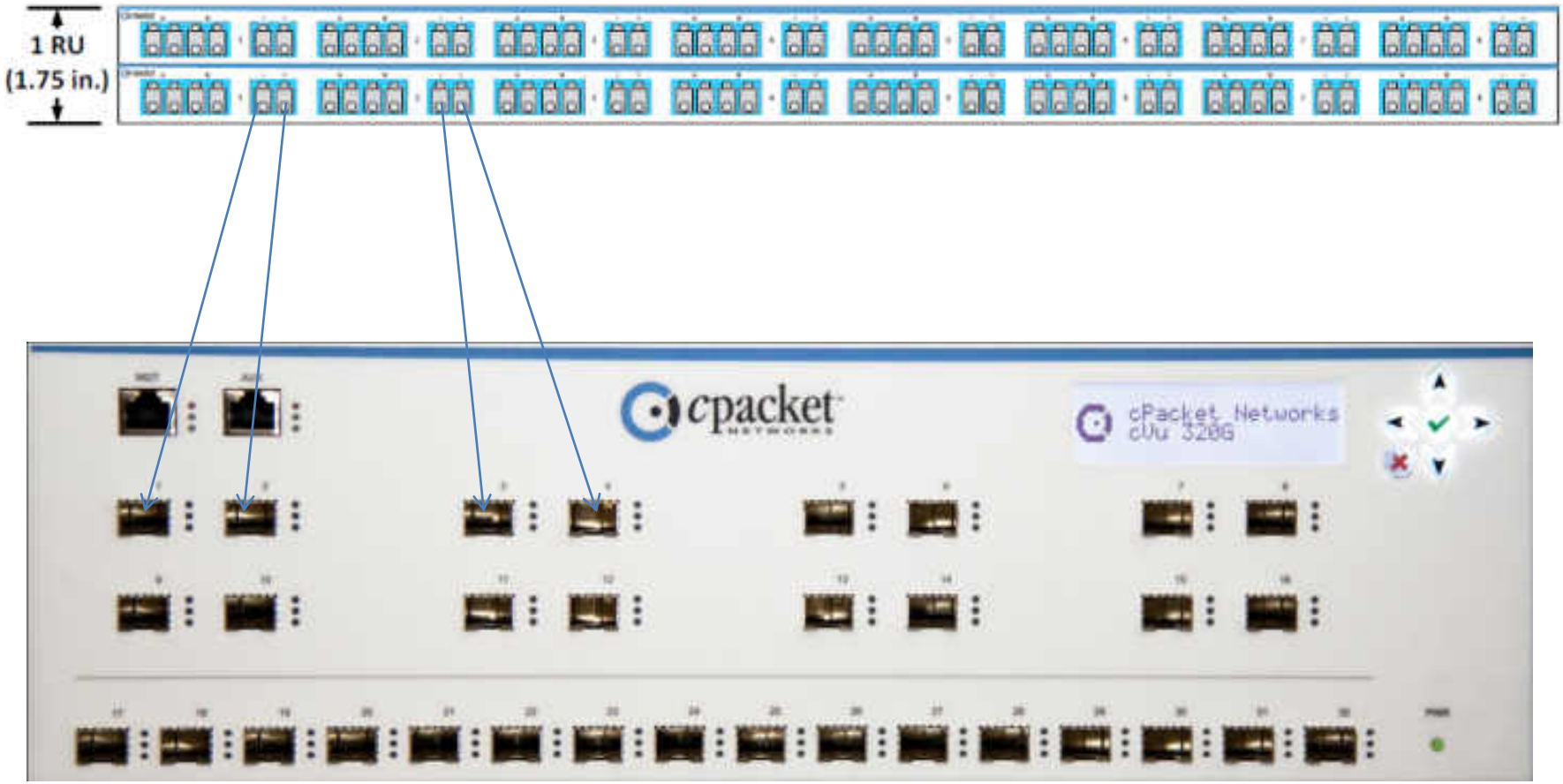
cVu device is an Intelligent Tools' Hub that feeds packets into tools AND also provides real-time Information

cVu Deployment Model



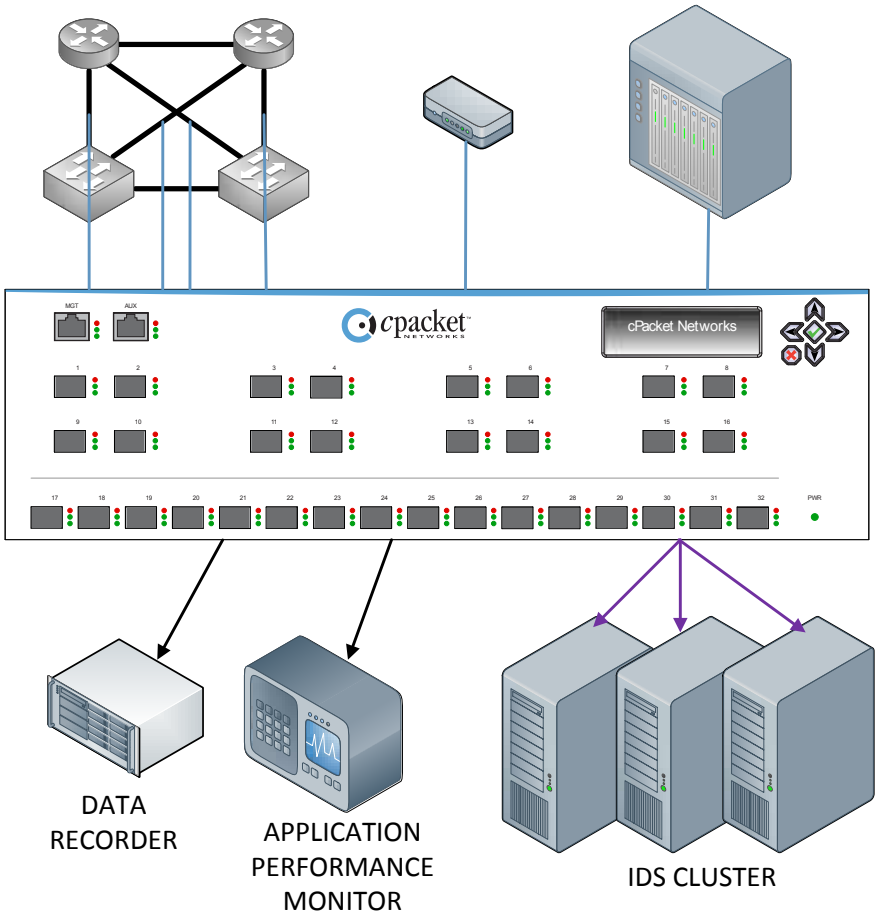
Orthogonal Monitoring
Performance, Capacity, Sec
Drill Down,
Trouble shooting




1 RU
(1.75 in.)
cpacket
cPacket Networks
cUu 3205

Serve as Centralized Tools' Hub

- Any-to-Any
  Many-to-One
  One-to-Many
- Filtering based on headers & payload L2-L7
- Granular built-in performance monitoring
- Automatic coherent flow balancing
- Accurate Time Stamping
- Triggers and alerts



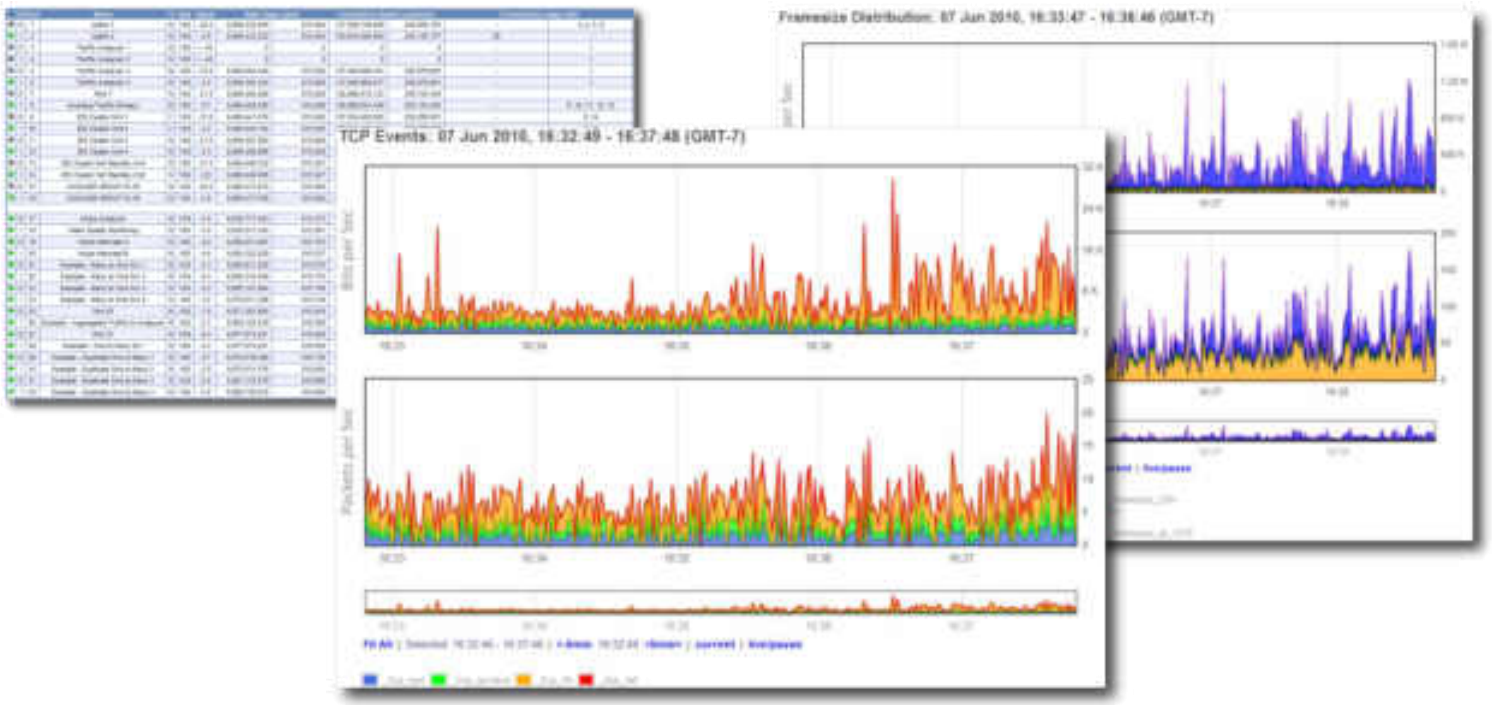
Standard Off-the-Shelf cVu Product Family

- **cVu 320G**

- **cVu 240G**

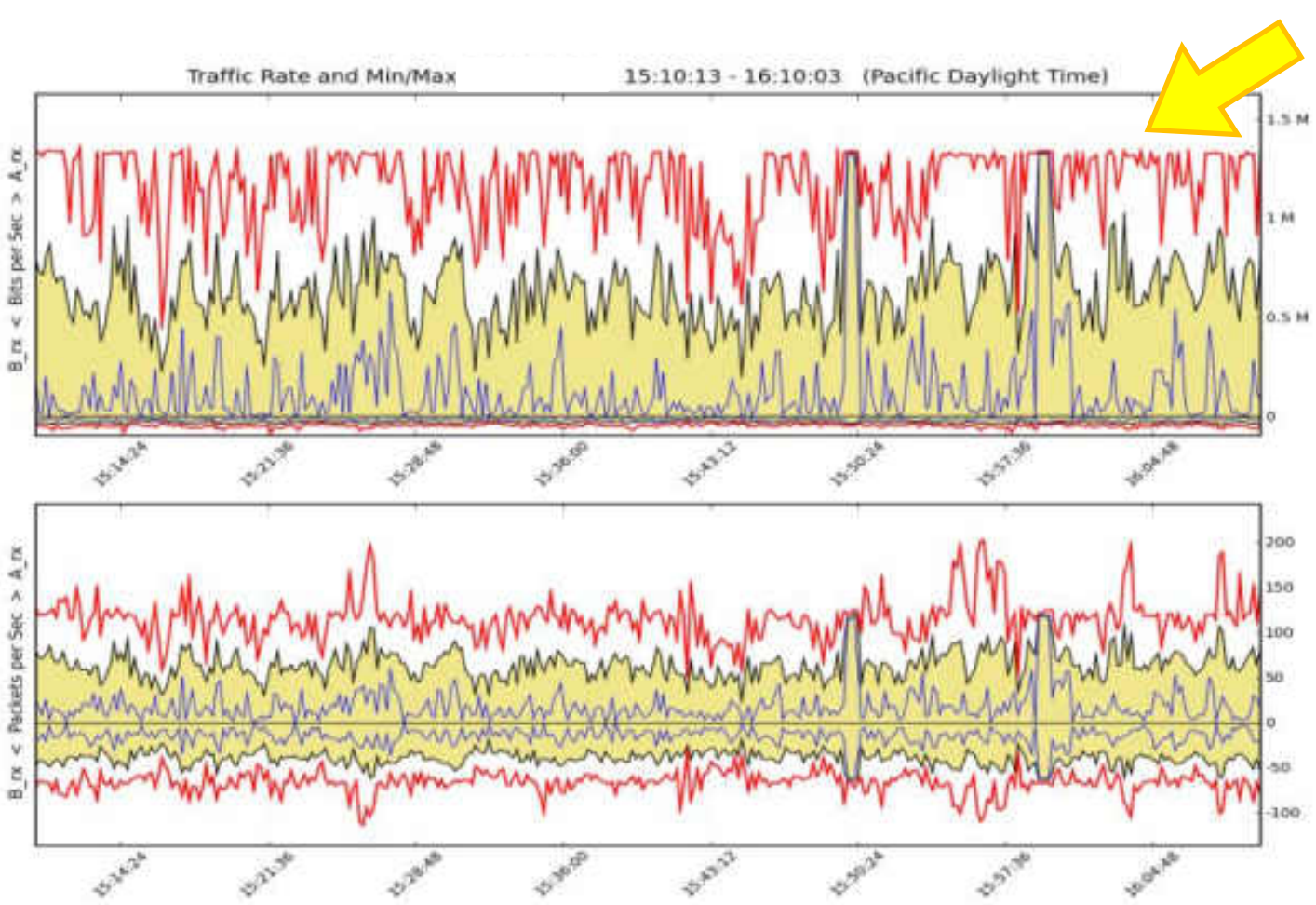
- **cVu 120G**

Granular Performance Counters and Graphs



- Accurate on-the fly analysis in real time
- Second by second counters and visualization
- Built-in ability to drill down on spikes and micro bursts

e.g. Averages (yellow) Mask Link Saturation (red)



* Yellow is average over 10 sec and Red is the max over 1 sec intervals

cVu Features and Smart Ports

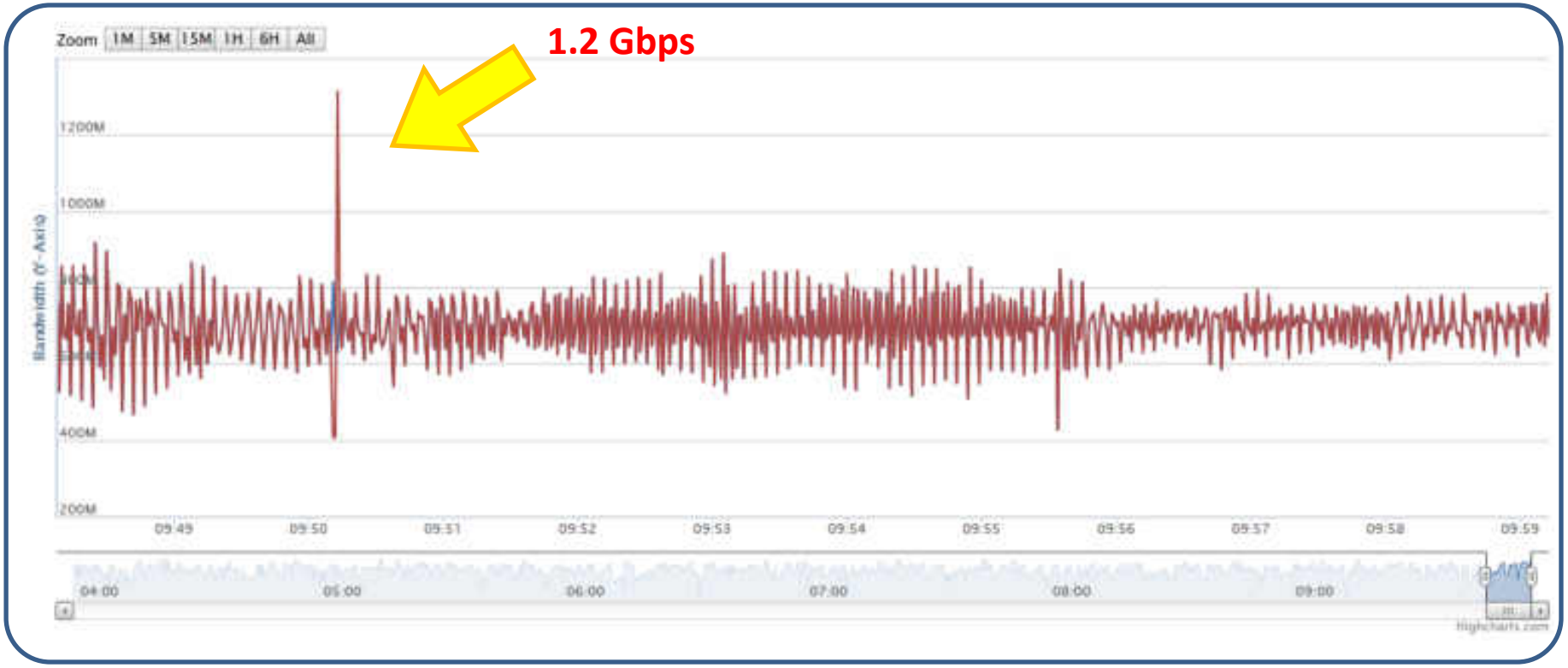
- Filtering base on Complete Packet Inspection (L2-L7)
  - Snap capture, extended capture, direct forwarding, tunnel forwarding …
- Performance monitoring
- Flow Balancing (… quick demo …)
- Packets Time stamping
- Built-in Spikes and Microburst detection
- Dynamic packet slicing of TCP payload
- Packet deduplication
- Tunnel Encapsulation - Decapsulation
- Stacking (modular build as you go)

Quick cVu 320G Demo

cVu Family is a Superset of Functionality

- Any-to-Any Aggregation, Replication and Flow Balancing
  - Enable Tool's Hub concept and broad coverage of multiple network links
- Enhanced distributed "situational-awareness" with real time performance monitoring and user-defined triggers
  - Automatic trigger and alerts based on thresholds and ratios
- Complete Packet Inspection (L2-L7) filtering
  - Selective forwarding and built-in snap capture

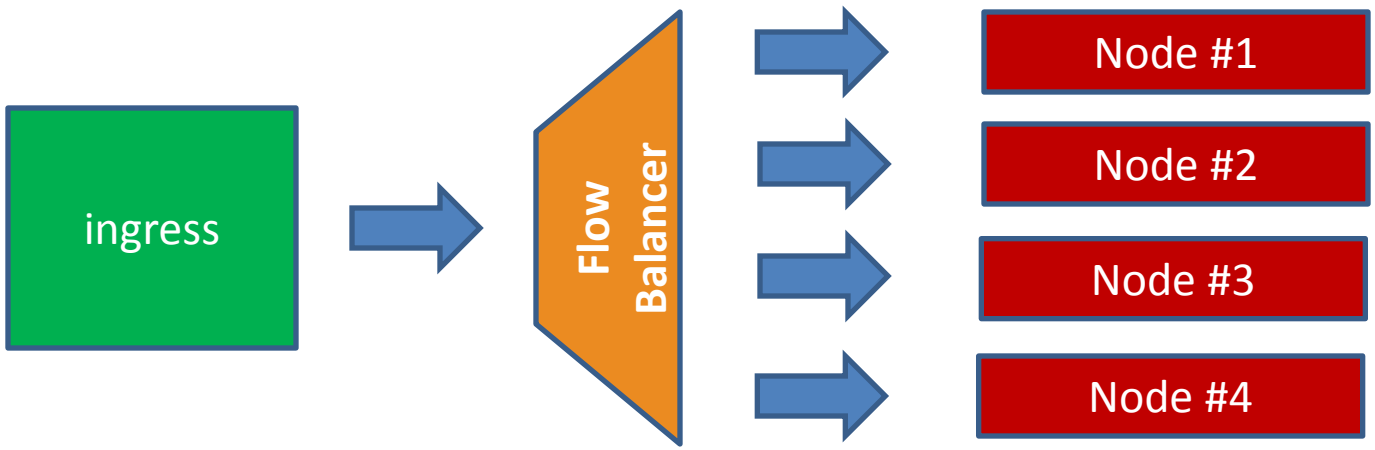
e.g. Spikes in Mixed 1G/10G Network



- The traffic spikes for a short duration over the planned capacity threshold (1Gbps), which can cause intermittent packet loss

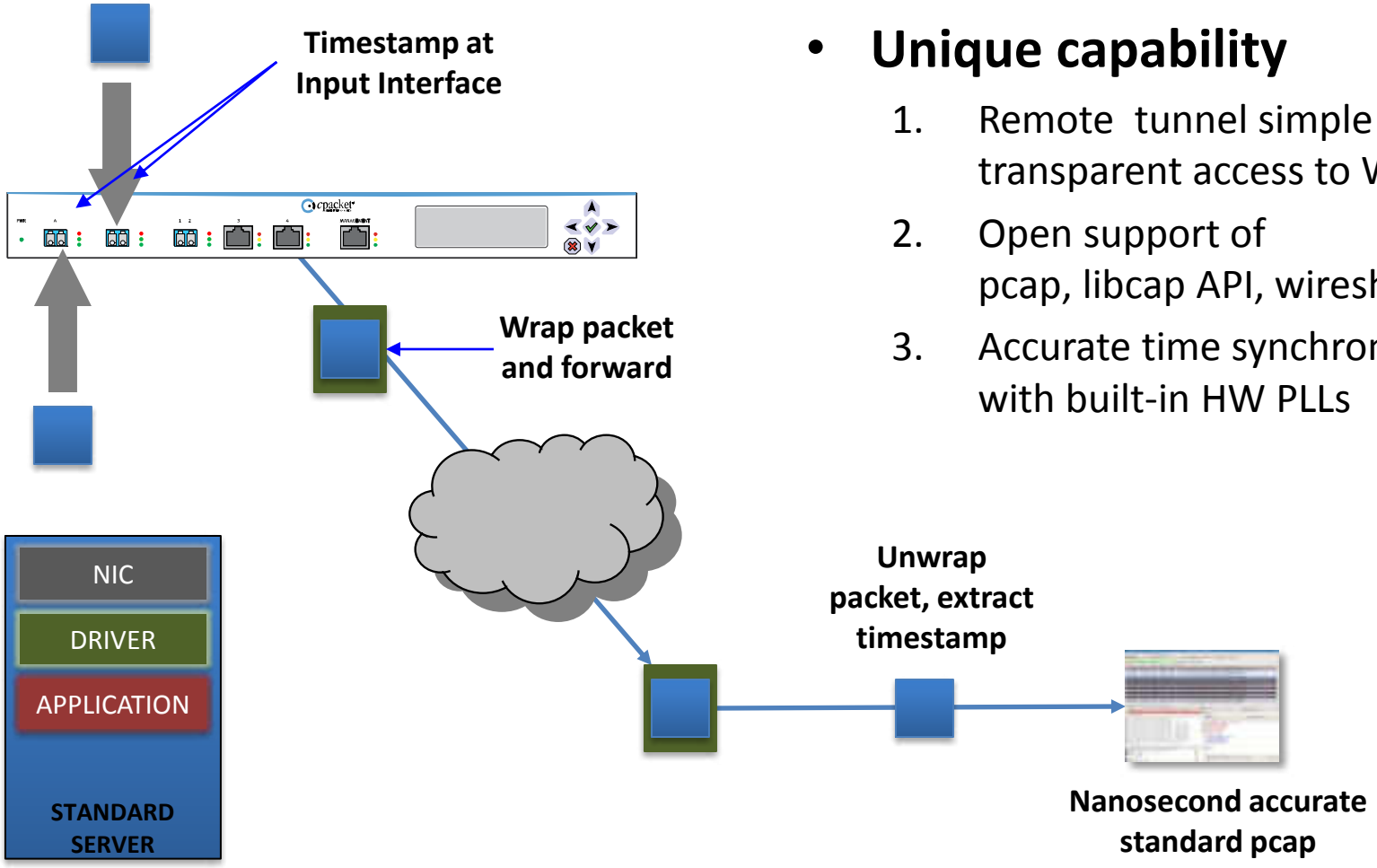
Simple to Use Coherent Flow Balancing

- Partition the incoming work load between cluster elements, while preserving full duplex ip.src <> ip.dst coherency



- Easy to use, simple, and flexible configurations

Cool Feature: Remote Forwarding & Tunneling

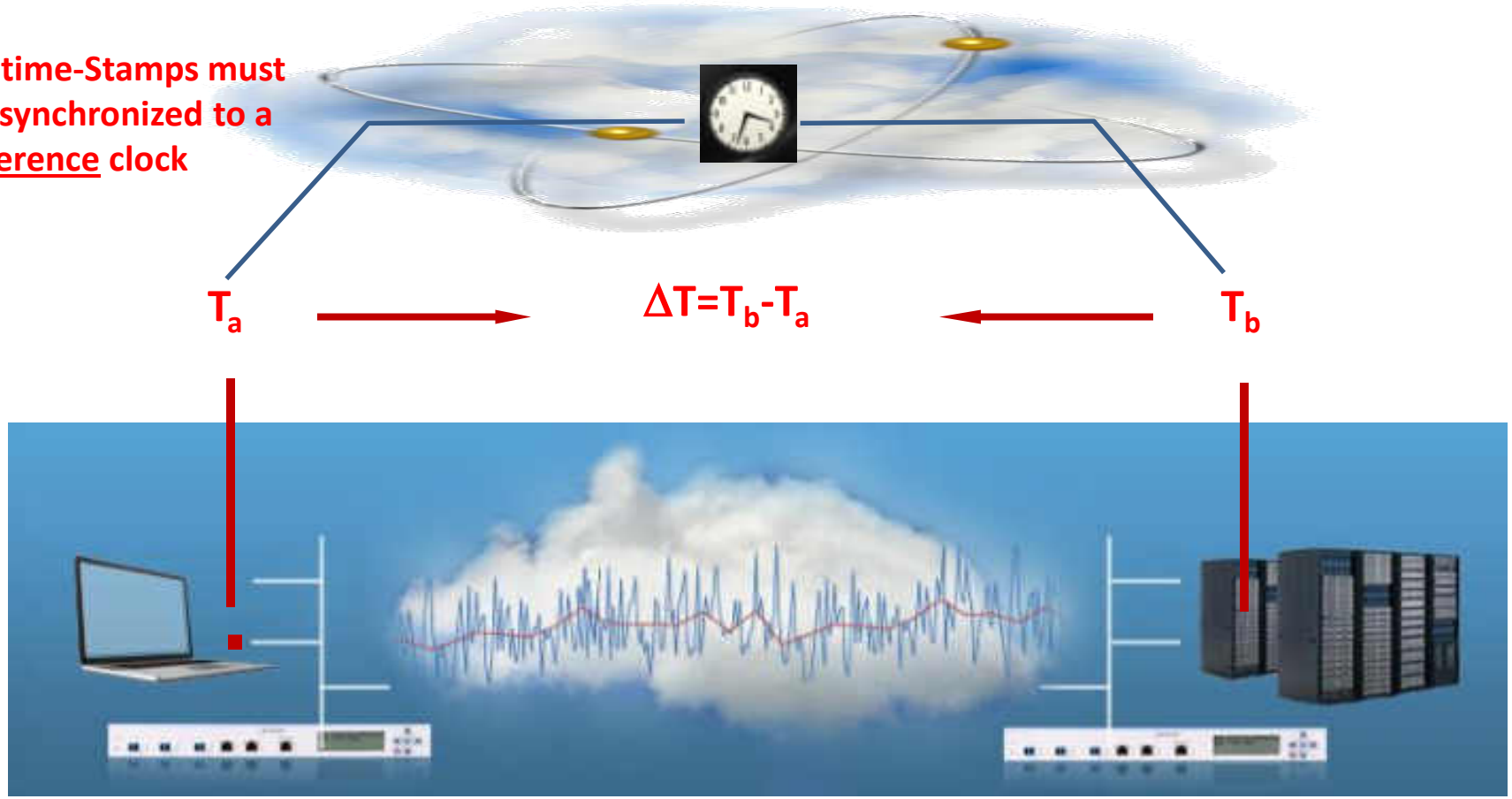


- **Unique capability**
  1. Remote tunnel simple transparent access to Wireshark
  2. Open support of pcap, libcap API, wireshark
  3. Accurate time synchronization with built-in HW PLLs

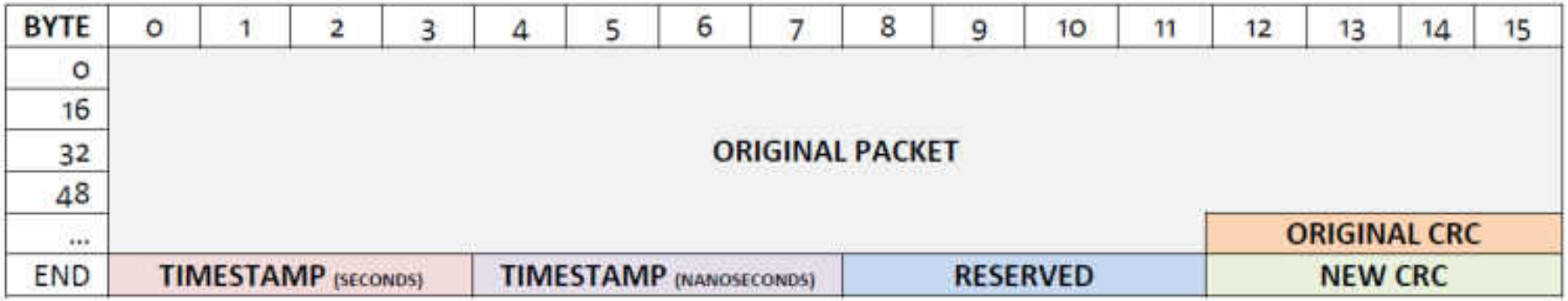
Enable any SW application to take advantage of HW time stamping at the wire

Time-stamping & One-Way Latency/Jitter

All time-Stamps must be synchronized to a reference clock

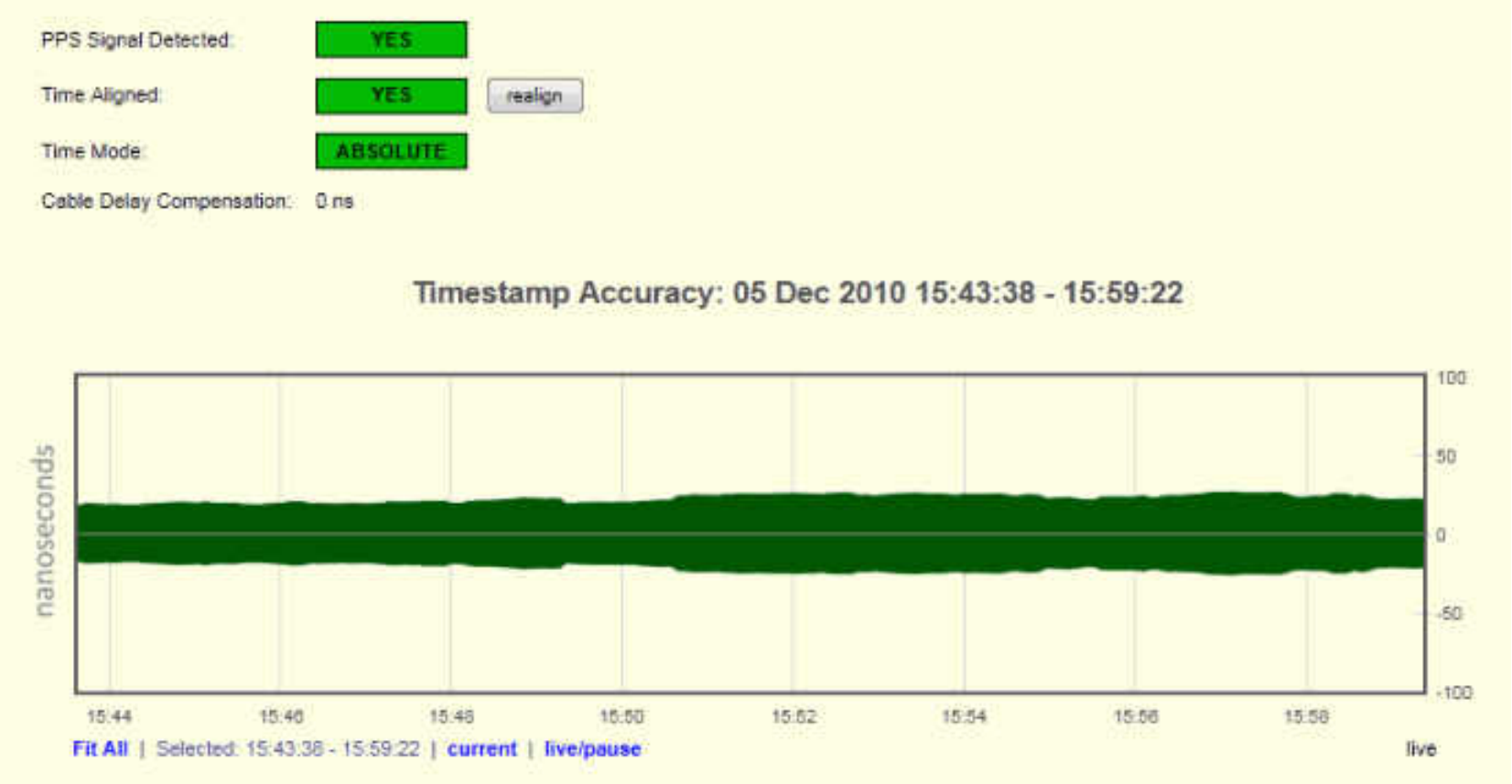


Open Time-Stamping Format - Wireshark Integration

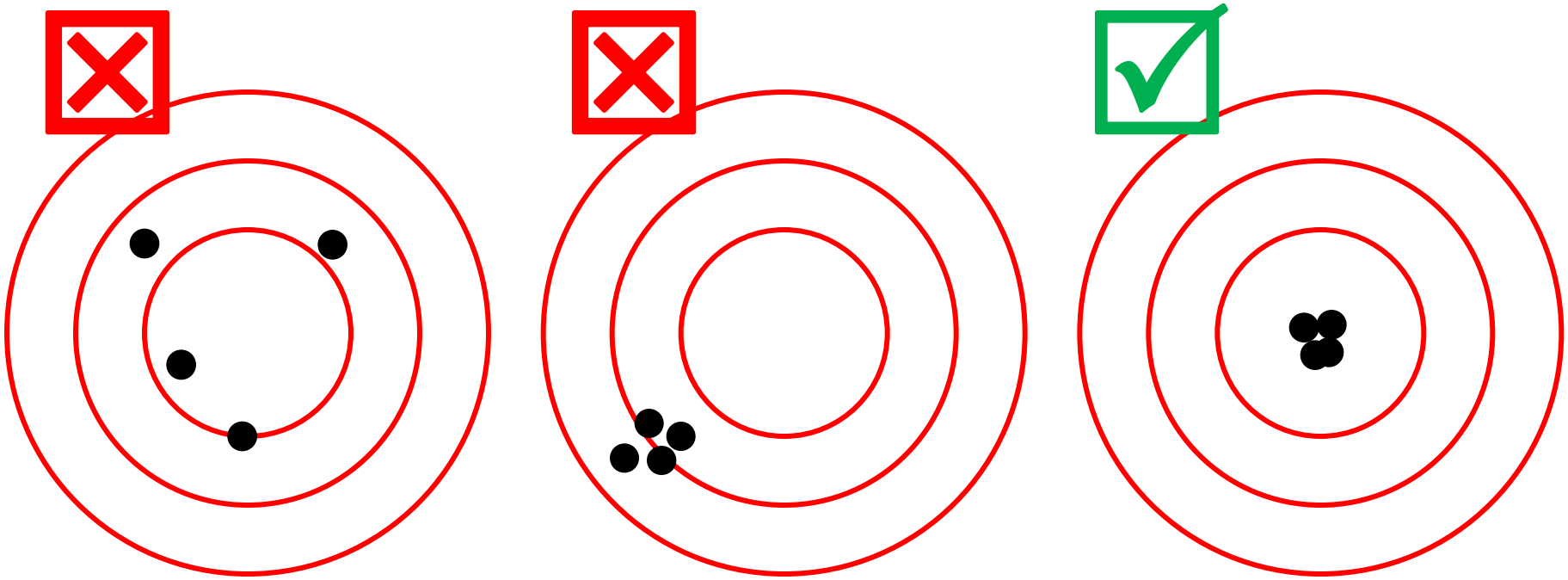


Title	Size	Description
ORIGINAL PACKET	X bytes	Original packet, including original CRC.
TIMESTAMP	8 bytes	8-byte timestamp, divided into two four-byte quantities. The first four bytes are the epoch time (in seconds) and the second four bytes are the fractional time (in nanoseconds). For both quantities, the most significant byte is first (as used by networks).
RESERVED	4 bytes	Reserved for future use.
NEW CRC (FCS)	4 bytes	The packet has a new CRC attached to the end as required by the Ethernet protocol.

Unique Real-Time Accuracy Diagnostics

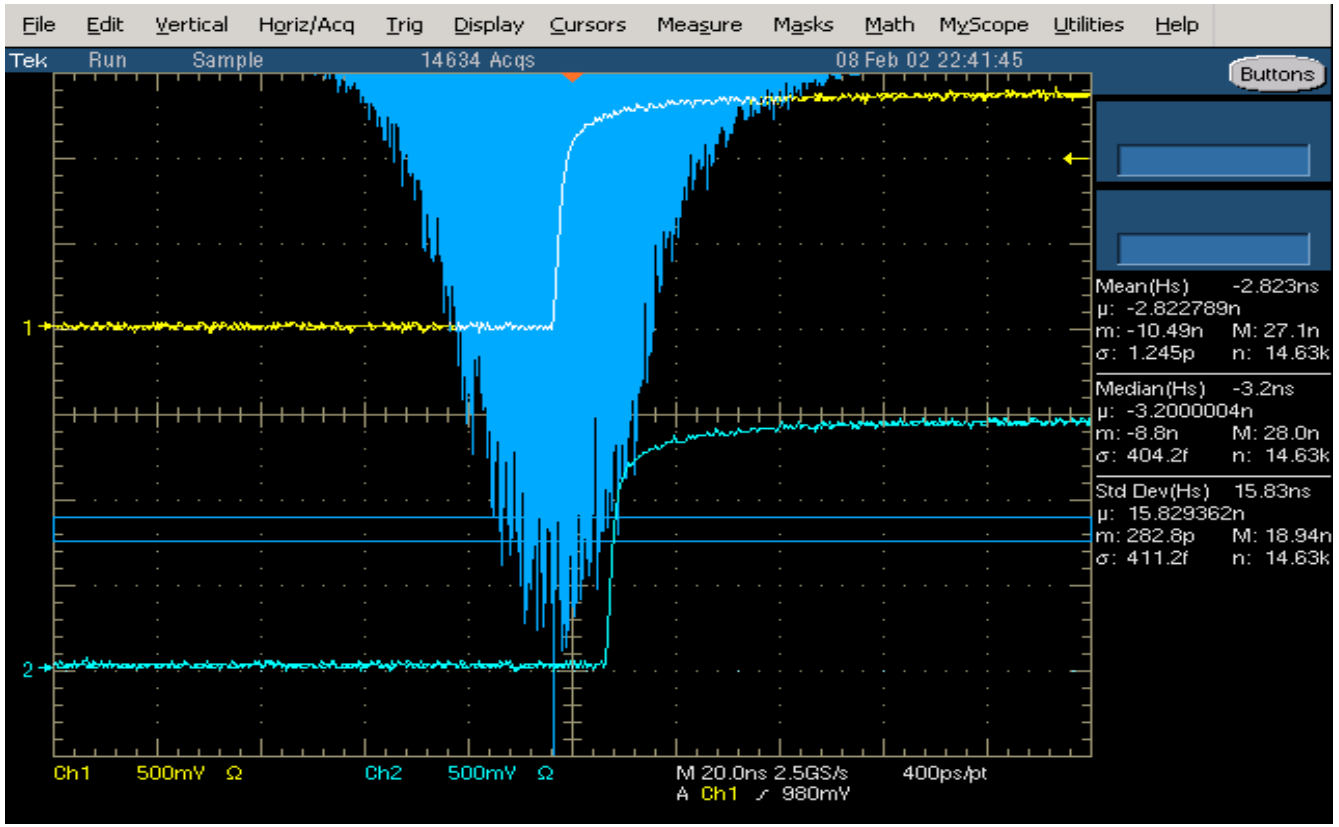


Avoid Surprises of (lack of) Accuracy and Precision



More info about Validation Methodology, see
www.cpacket.com/download

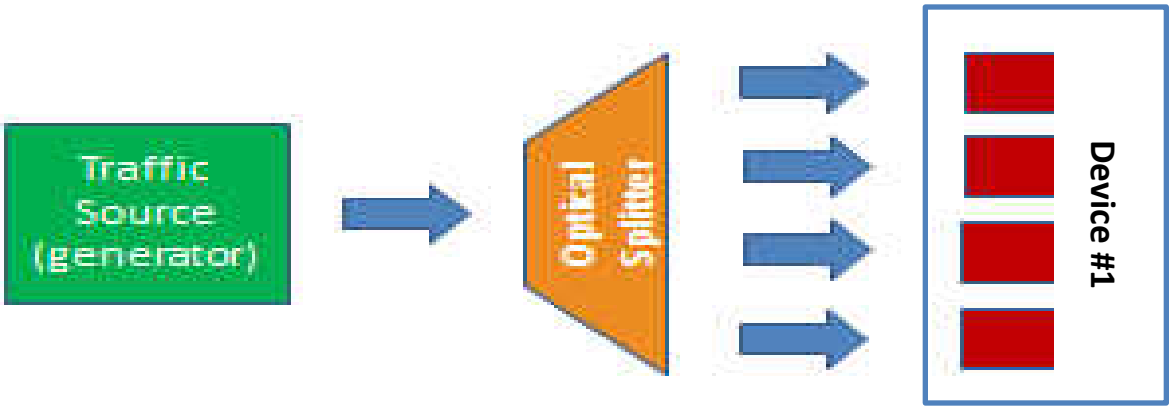
Comparison to Commercial GPS Jitter



- Histogram of discrepancies between two commercial GPS clocks:
  Avg = -2.8 ns, Median = -3.2 ns, **Std = 15.83 ns**

Test Consistency of Time-Stamping Engines

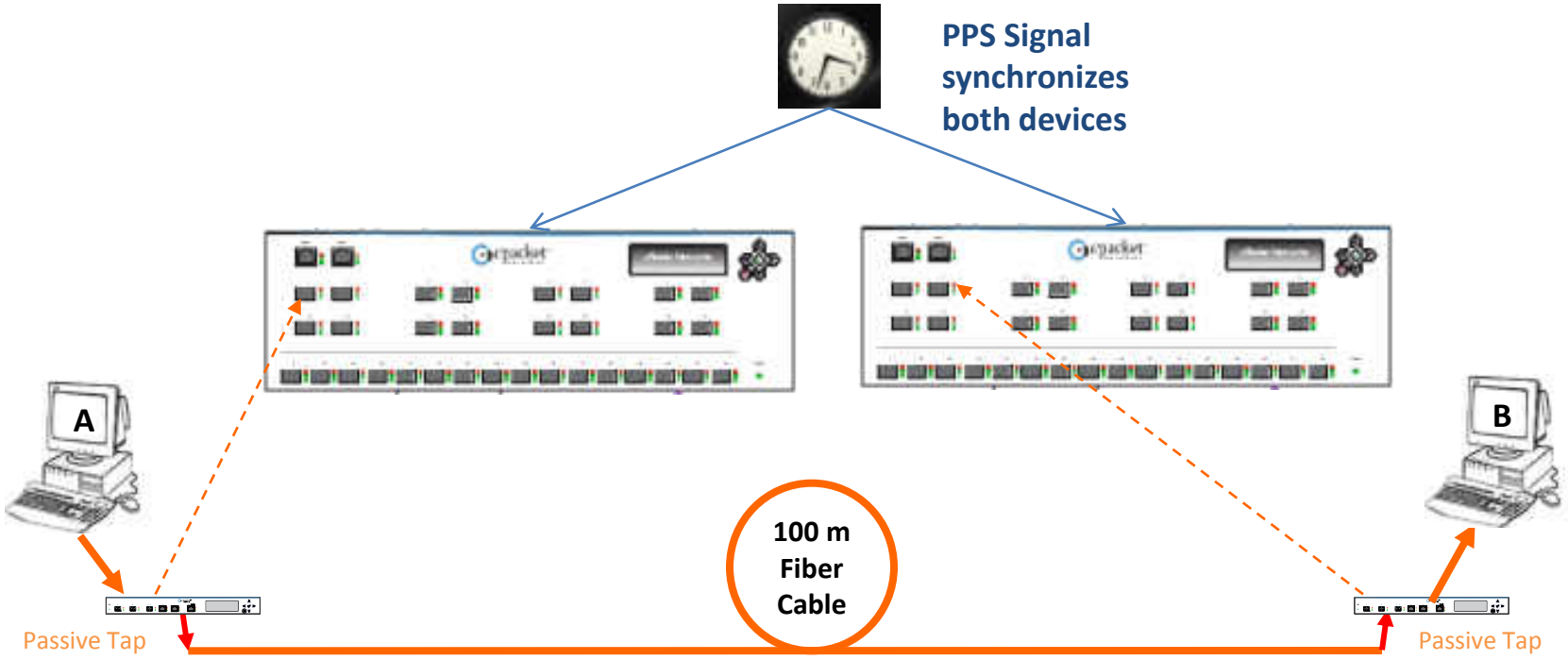
- Send traffic (e.g. laptop, tester)
- Use passive optical splitter to create “~simultaneous events”



- Capture the time-stamped packets
- Compare the time stamps in Wireshark (pcap) - are they consistent with the expected results

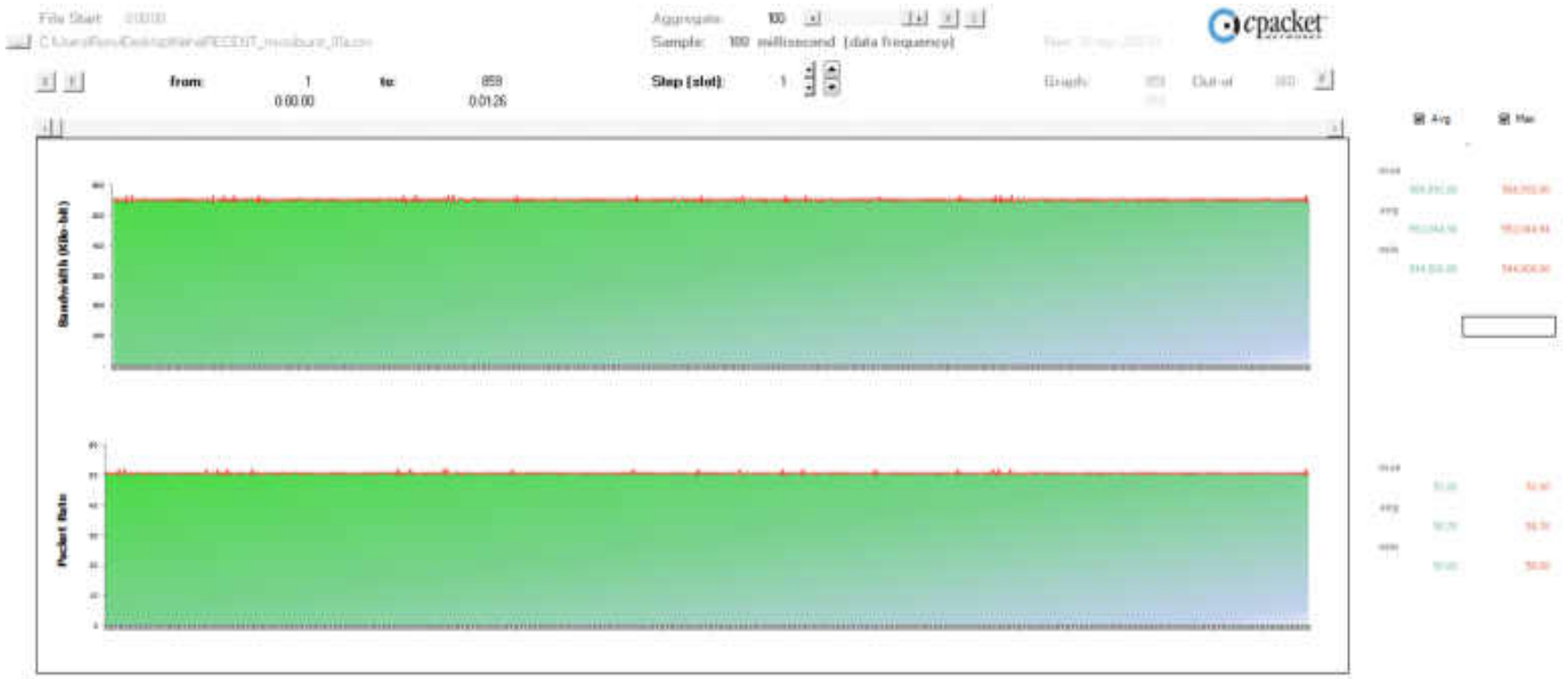
Confirm against a Known One-Way Reference

- Extend setup with fiber cable of a given length (~5 ns/meter)



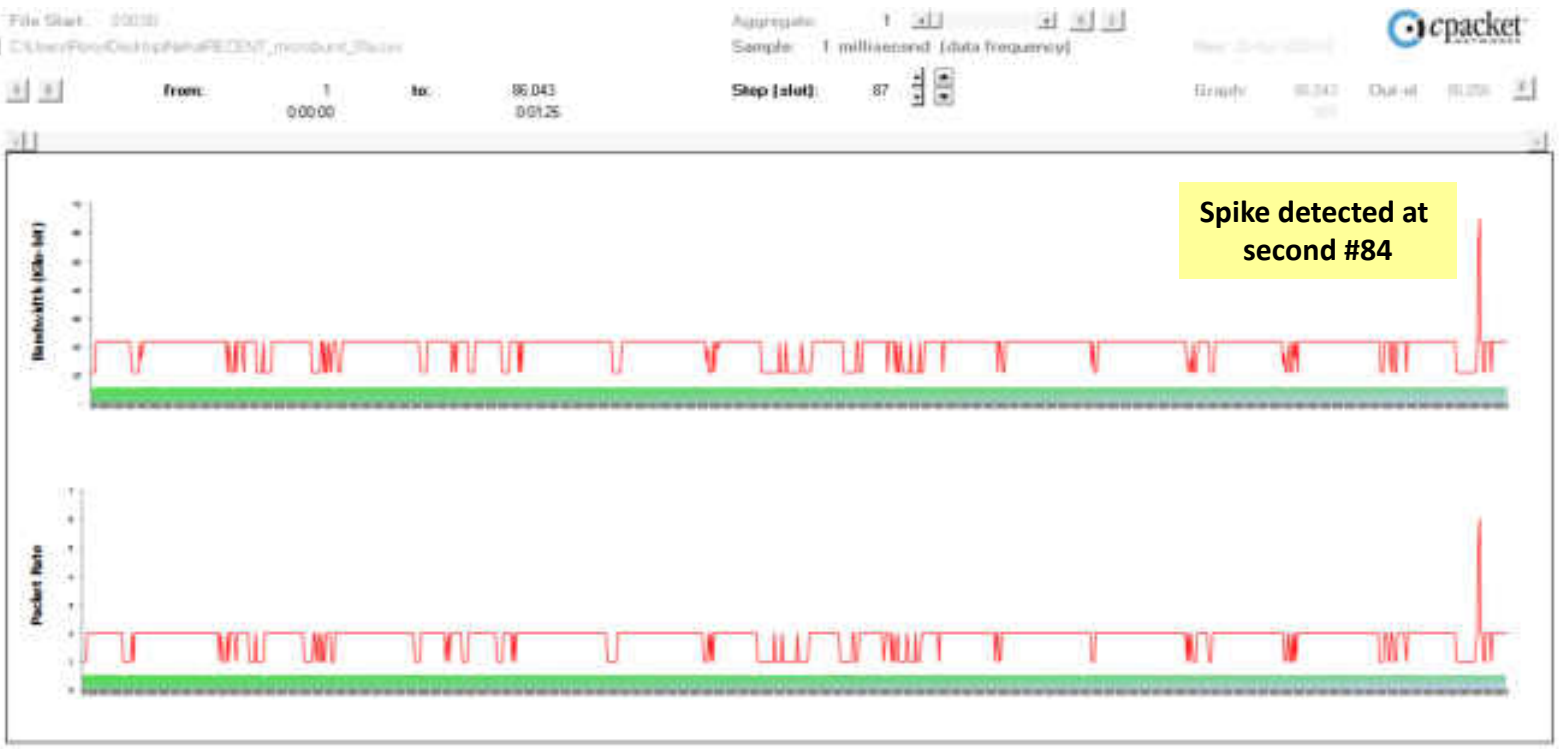
100 meters x 5 nanoseconds = ~500 nanoseconds (+/-?)

At one second the IPTV Stream Looks Stable



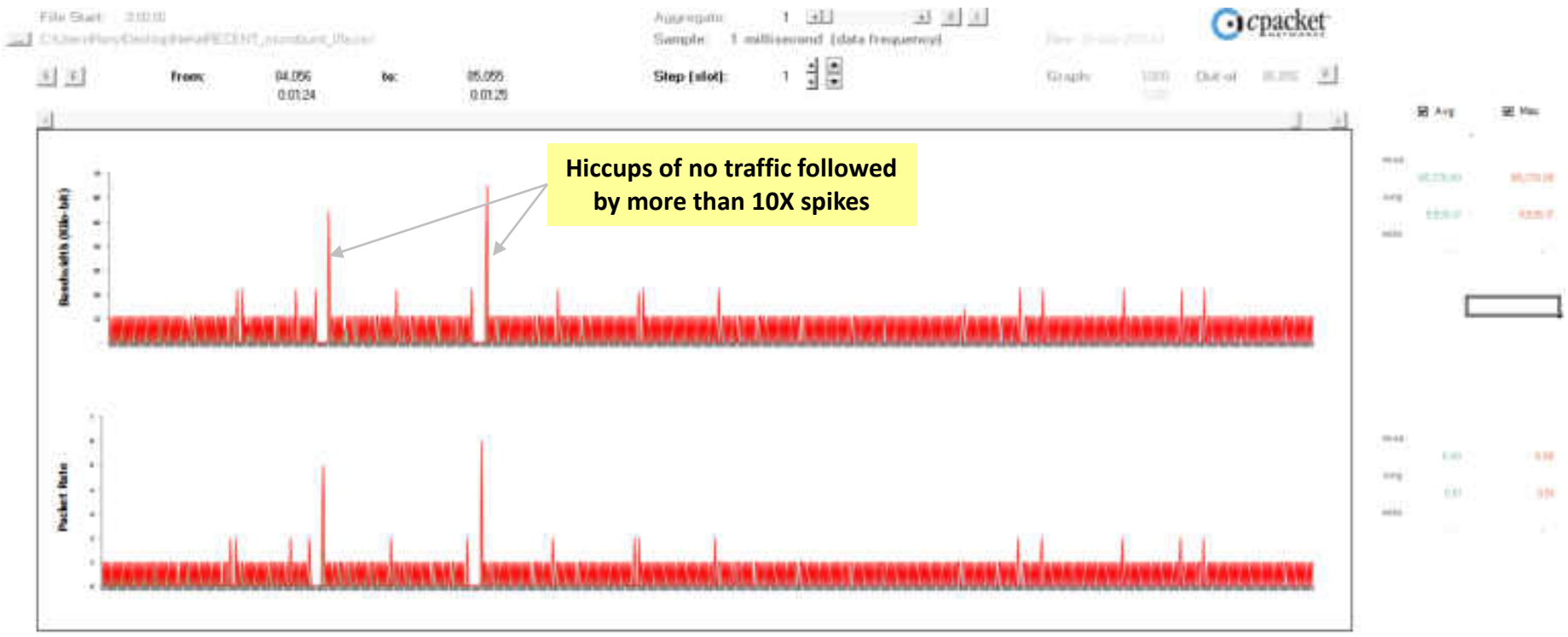
- At measurement frequency of once per second or even 10 times per second (*i.e.* **100 milliseconds**) traffic seems stable

Measurement at 1 millisecond Reveals a Spike



- The **red line** shows the performance **envelope** per 1 millisecond over duration of 86 seconds (1:26 minutes)

Root-cause of Hiccup at Second #84 (1:24-1:25)



- Traffic stopped for ~10 milliseconds period (hiccup) and encoder compensated with a **burst** of over **10X** of capcity constraints

If you cannot MEASURE, you cannot OPTIMIZE

High Frequency Trading Use Case

Centralized and Unified Red-Green Map

Automatic Alerts to Standard Collectors …

Millisecond Alert Log

```
2012-02-08T05:16:36Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:16:26Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:16:16Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:16:06Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:56Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:46Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:36Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:26Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:16Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:15:06Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:56Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:46Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:36Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:26Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:16Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:14:06Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:56Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:46Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:36Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:26Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:16Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:13:06Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:56Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:46Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:36Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:26Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:16Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:12:06Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:11:56Z: vlan_102 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
2012-02-08T05:11:56Z: vlan_112 max bps >= 2500000 for more than a millisecond | bps:(0, 0, 0) pps:(0,0,0)
```

NEW: Global Search Across ALL Smart Ports - cGREP

- Search across all the smart ports of cPacket virtual appliance for traffic profiles that match any header fields and payload content
- From a single template, the user drives a real time report of the matches in any link that is monitored by a cPacket smart port
- Effective for trouble shooting
- Unique enabler of path discovery based on custom heart beats

cPacket Objective

- Significant time, effort, and aggravation are spent on getting relevant packets into Wireshark
- cPacket delivers intelligent solutions for real-time visibility, proactive monitoring, and selective drill down (L2-L7)
- Enable efficient data center and network operations