

# SharkFest'17 US

## Designing a requirements based packet capture infrastructure



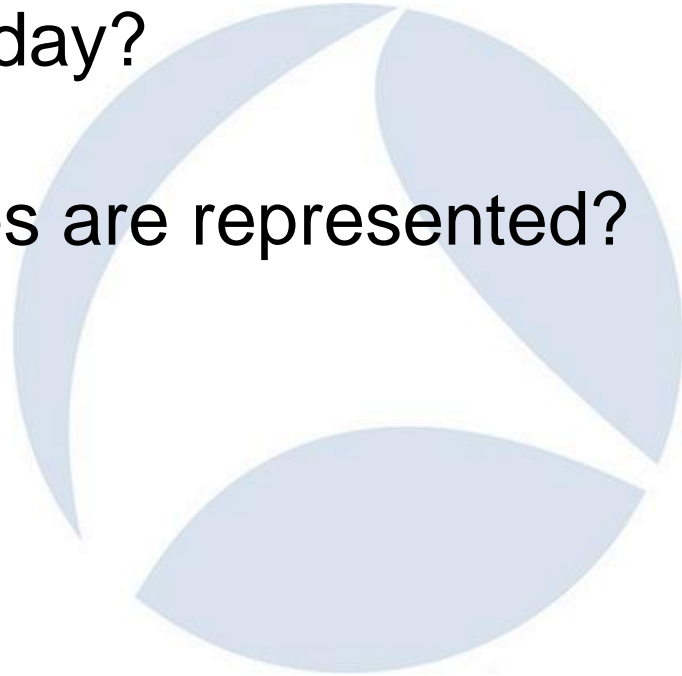
John Pittle

Distinguished Performance Consultant, Riverbed Professional Services

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

# Audience Profile

- Which IT teams / disciplines are represented in the session today?
- What industries are represented?



# Speaker Introduction

- App911 Emergency Troubleshooting Team Lead
- Technology Adoption Services Team Lead
- Consulting Practice Mentor
- Best Practices Contributor
- Program Owner – Riverbed Performance Management Workshop Series

# Premise

- We Love Packets!
- Many performance / availability issues can only be solved with packets and expert analysis
- Analysis is often delayed or deferred because we don't have the packets or the context we need at the time we need them
- Requirements based design of packet capture and analysis solutions can help ensure you get the funding needed to adequately support the business

# My Ask for This Session

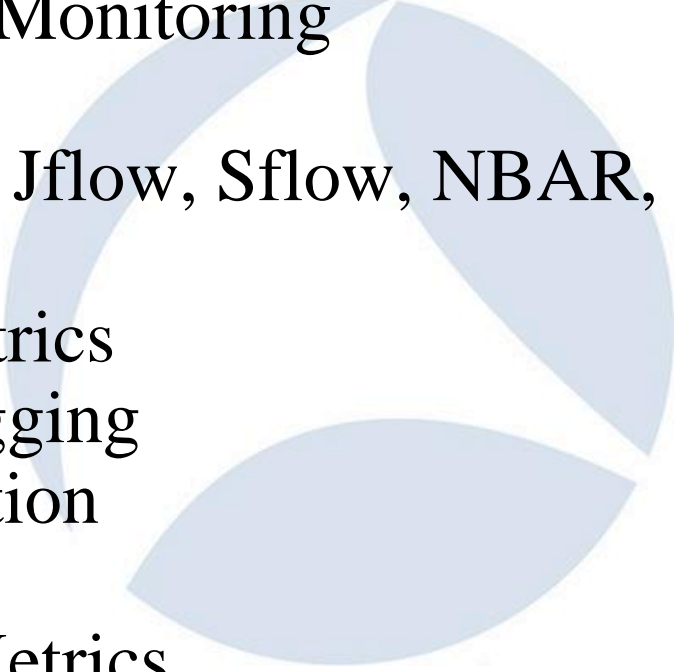
- Engage and Participate
- Share your experience
- Learn from your Peers
- Improve your Craft



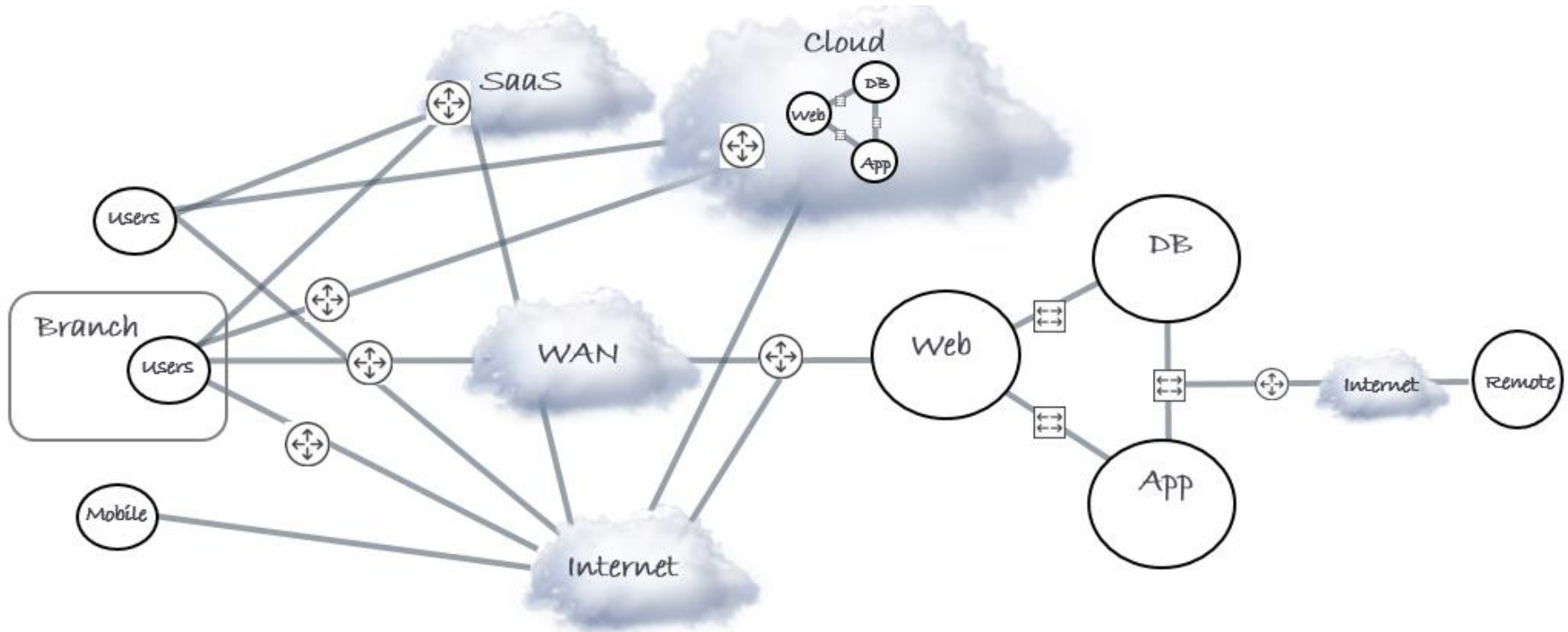
# Agenda

- Performance Management Landscape
- Packet Related Workflows & Technologies
- Requirements & Business Case Mechanics
- Gap & Risk Heat Maps
- Recommendations and Wrap-up

# Performance Management Landscape

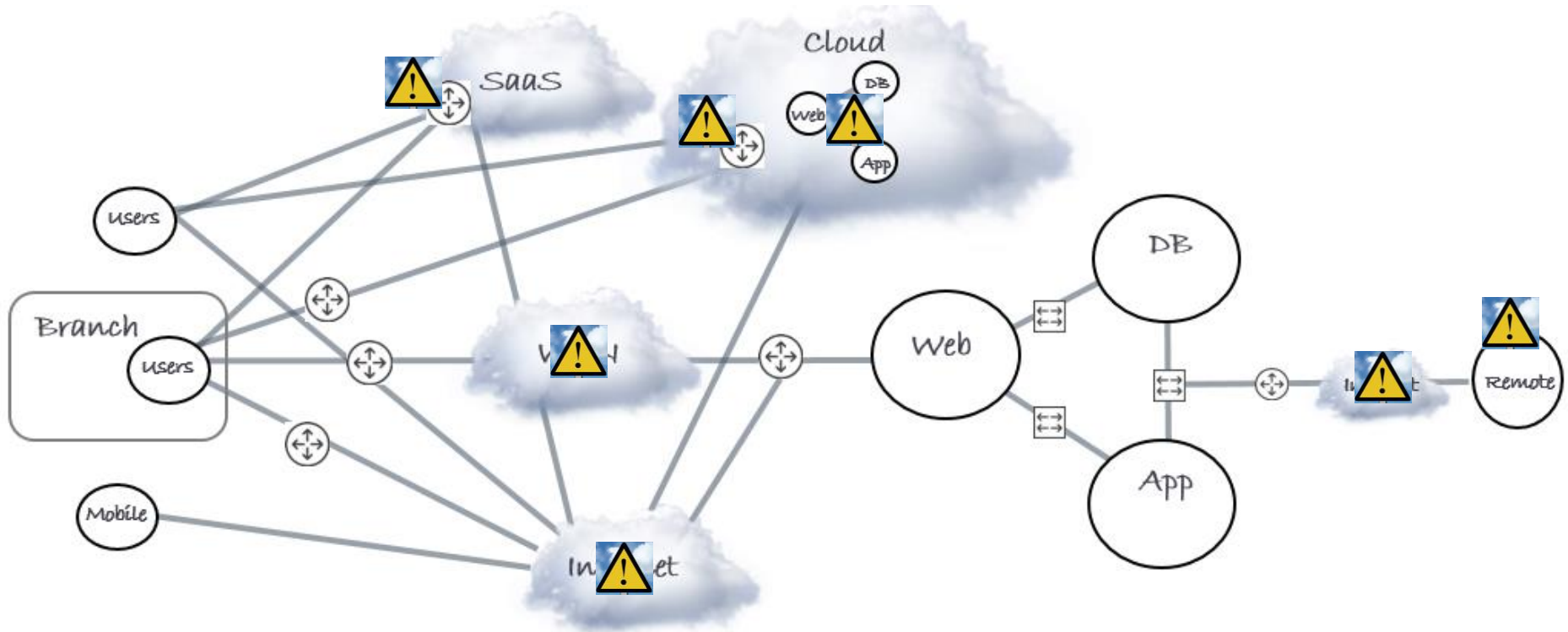
- End User Experience
  - User End Point Monitoring
  - Packets
  - Flow (NetFlow, Jflow, Sflow, NBAR, etc)
  - SNMP
  - Application Metrics
  - Application Logging
  - Javascript Injection
  - Host Metrics
  - Infrastructure Metrics
- 

# Hybrid Enterprise



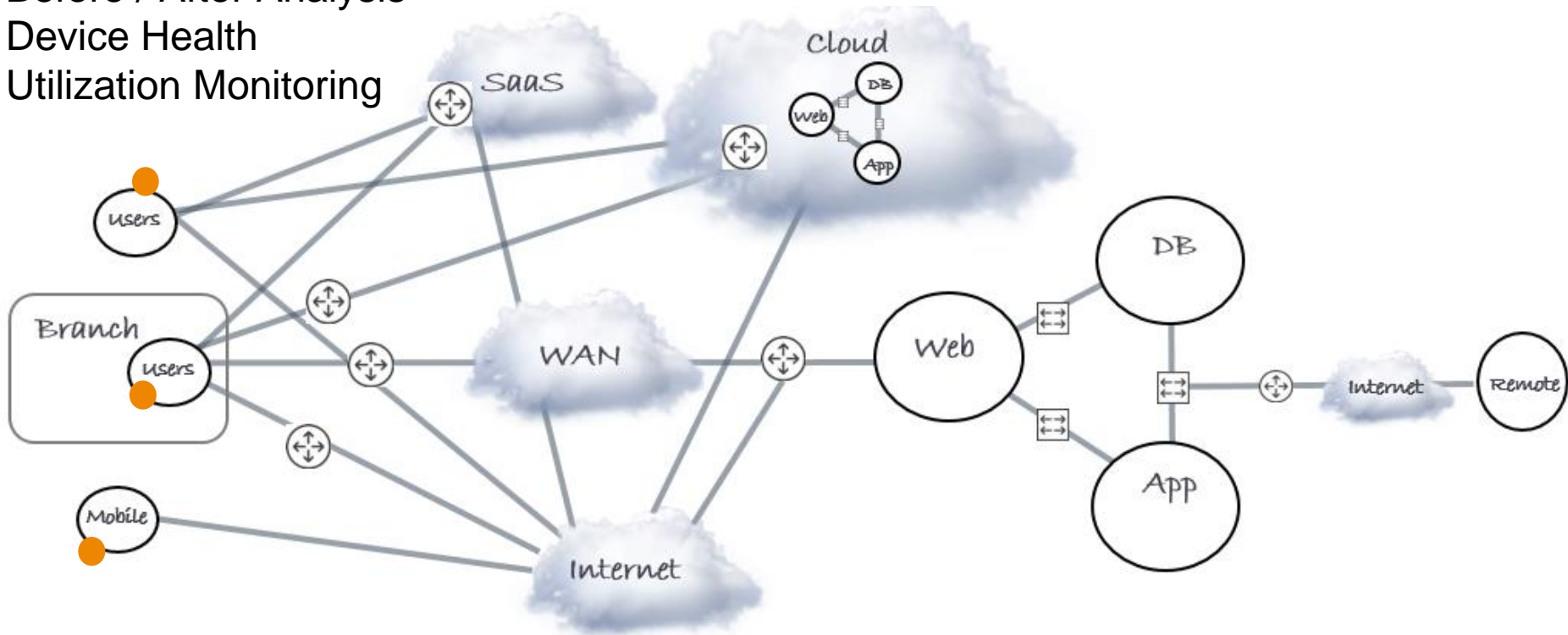


# Next Gen Challenges / Blind Spots

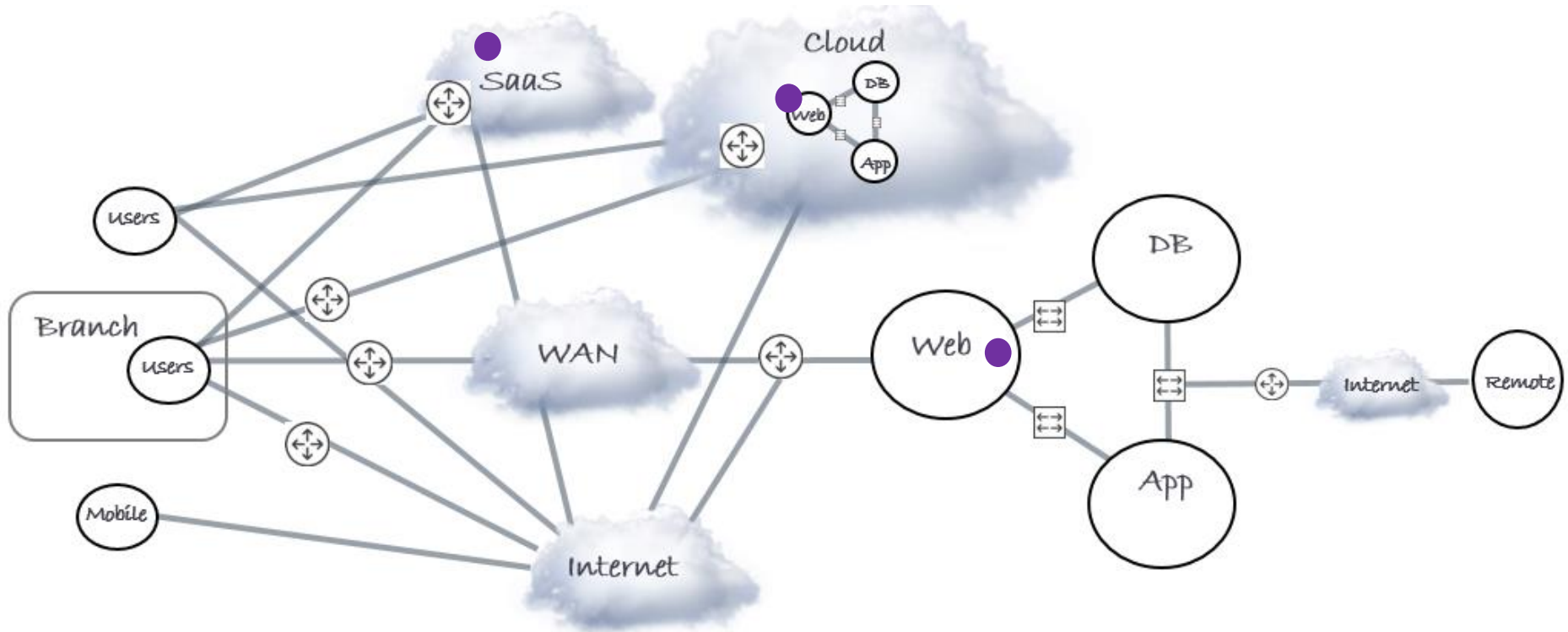


# User End Experience Monitoring

EUE Performance  
Before / After Analysis  
Device Health  
Utilization Monitoring



# Browser EUE - Javascript Injection

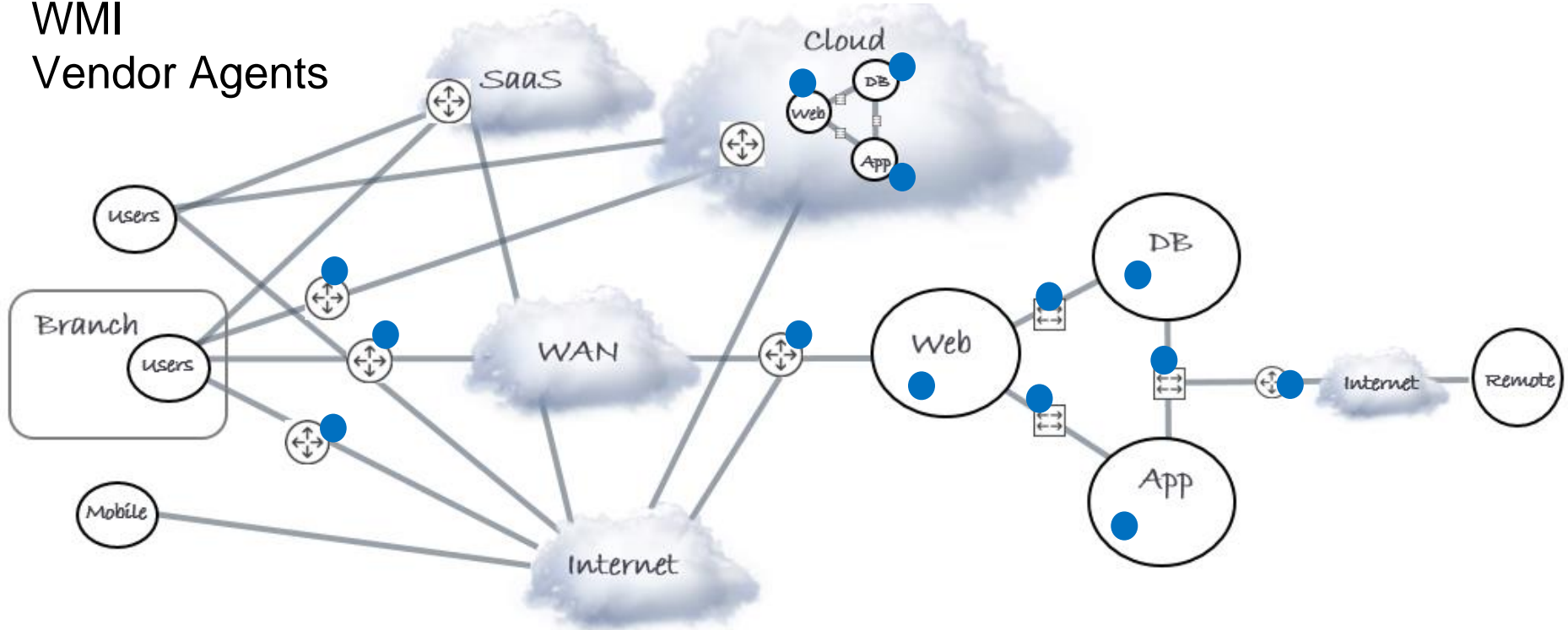


# Infrastructure Devices / Servers

SNMP

WMI

Vendor Agents



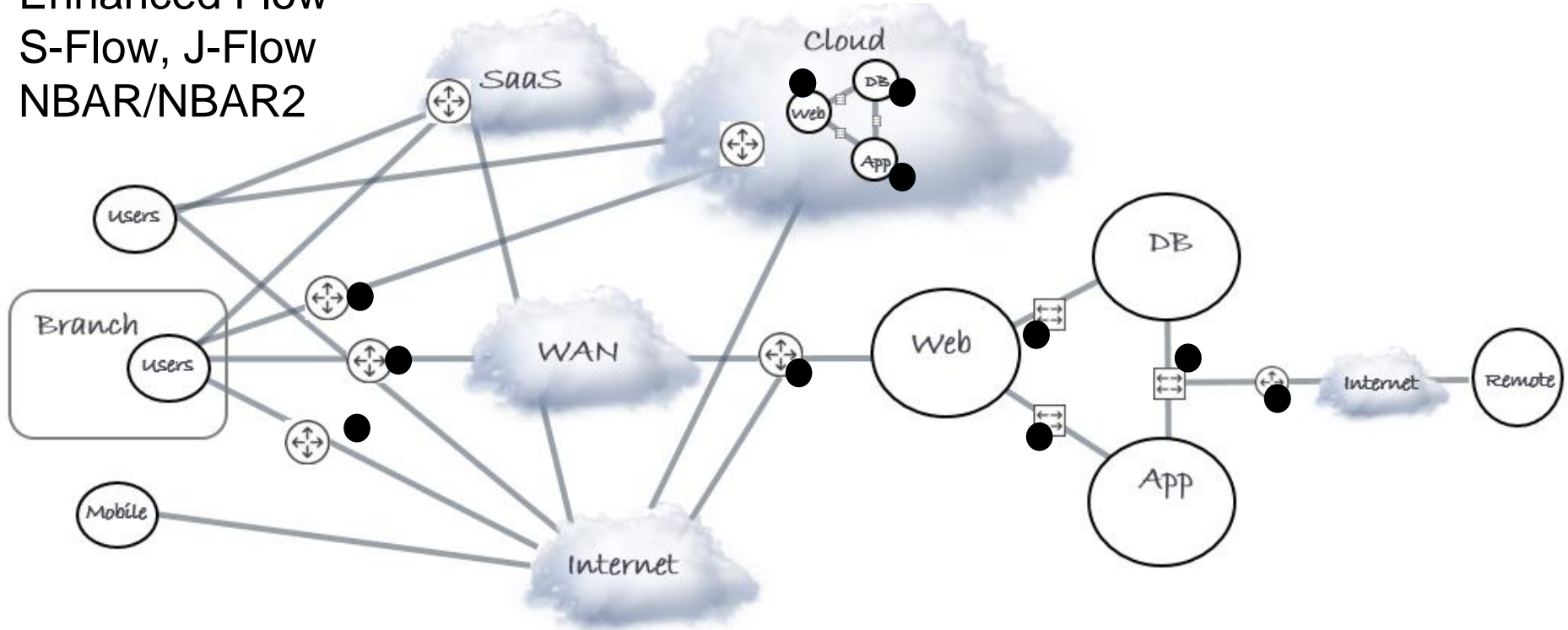
# Flow Records

Netflow

Enhanced Flow

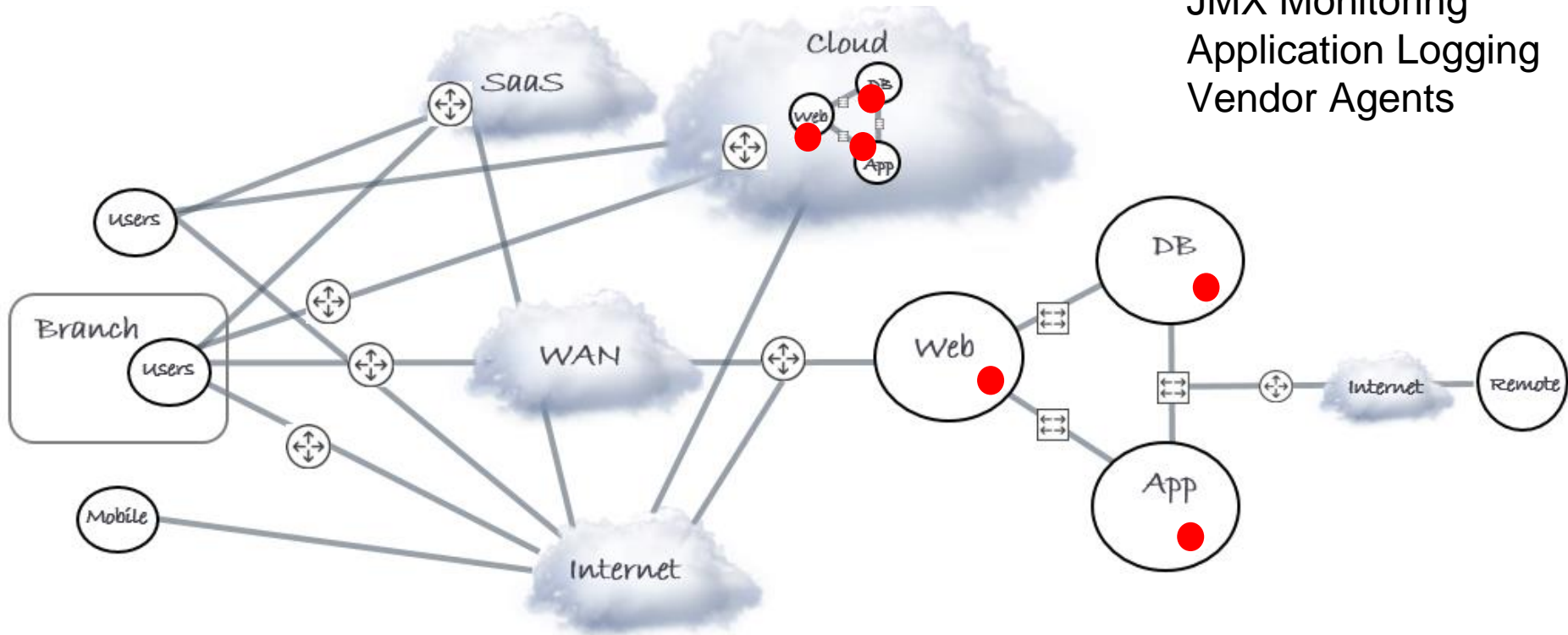
S-Flow, J-Flow

NBAR/NBAR2

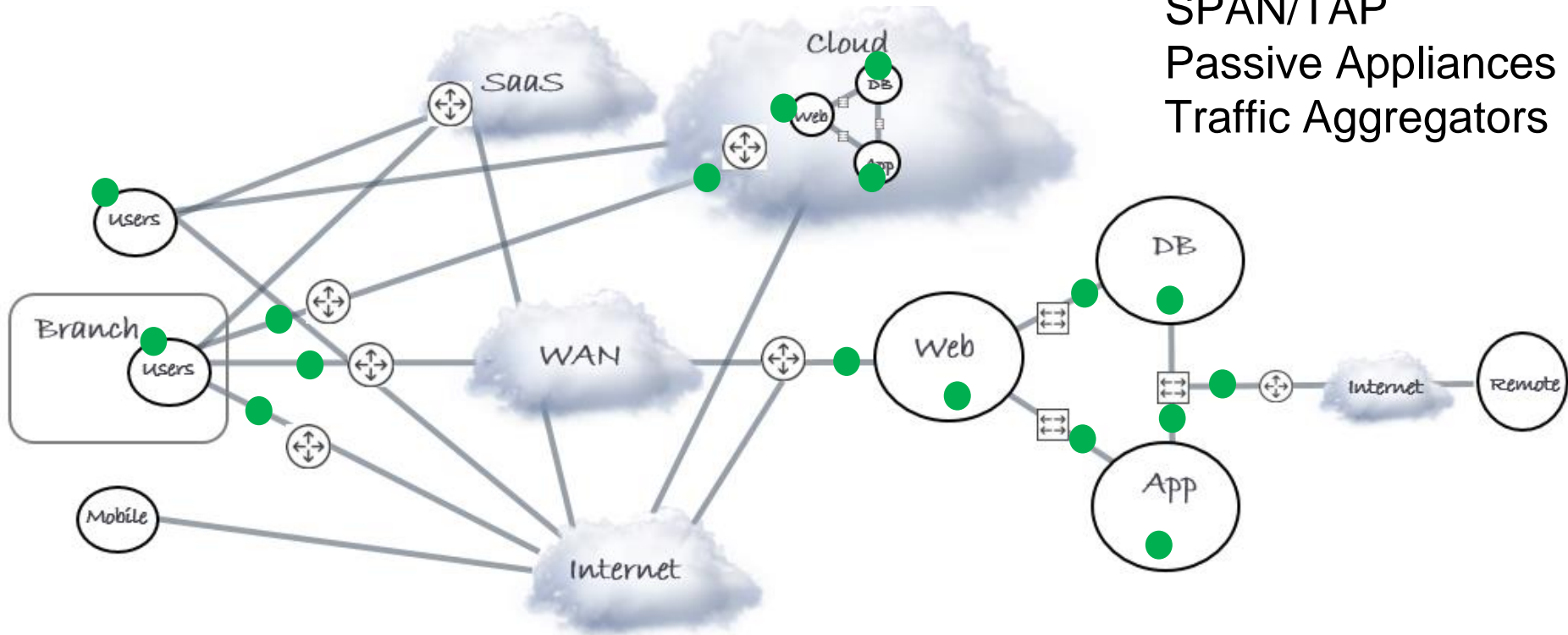


# Internal Application Components

Java / .NET Profiling  
JMX Monitoring  
Application Logging  
Vendor Agents



# Packet Capture / Collection

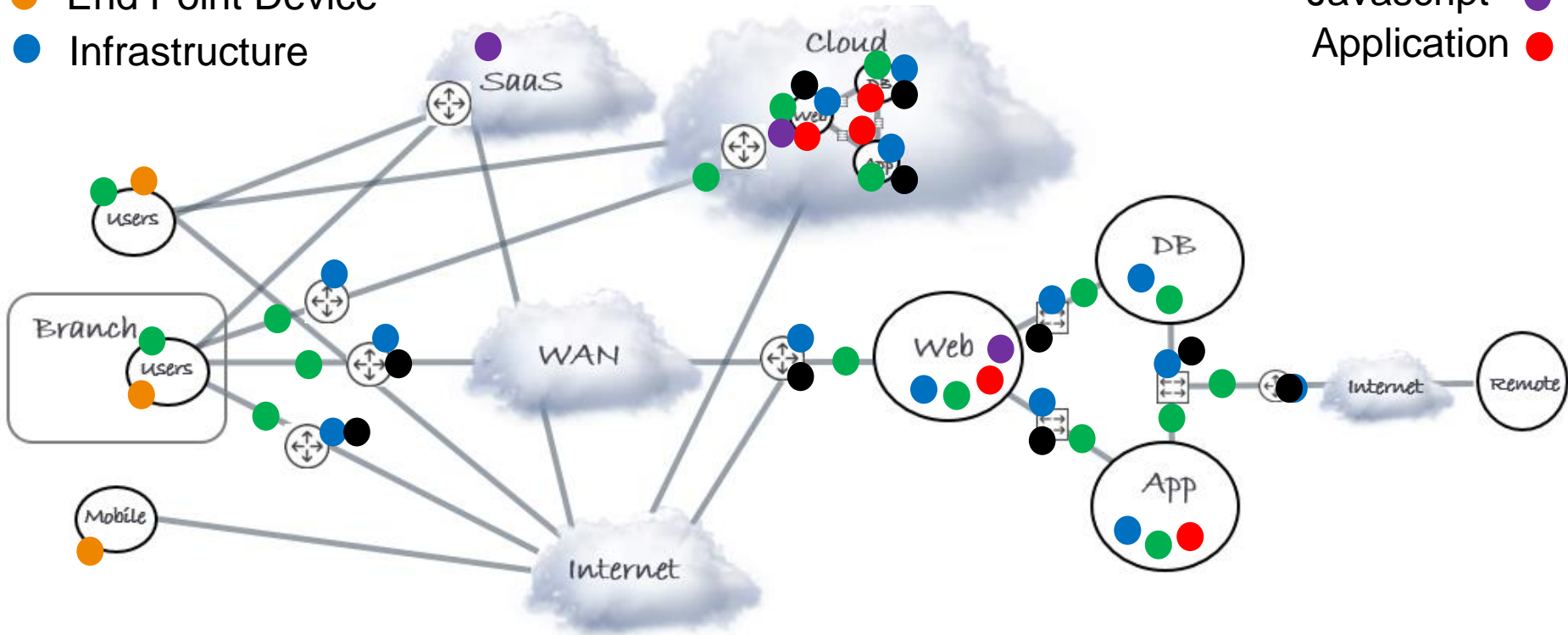


Host Captures  
SPAN/TAP  
Passive Appliances  
Traffic Aggregators

# Full End to End Visibility

- Packets
- End Point Device
- Infrastructure

- Flow
- Javascript
- Application






# Heard in the War Room...

- Link utilization is 80%, who's using the bandwidth?
- Server utilization is 85%, who's generating the load?
- Is user experience impacted?
- How long has it been going on?
- App ABC is slow, what infrastructure does it use?
- Who owns the fix?
- If device XYZ goes down, who's impacted?

# Heard in the CIO Staff Meeting

- Are we meeting our SLAs?
- Are customers happy?
- Is IT measurably contributing to company success?
- Are we investing in the right areas? How do we know?
- What's the impact if we \_\_\_\_\_?

# Holistic Performance Management

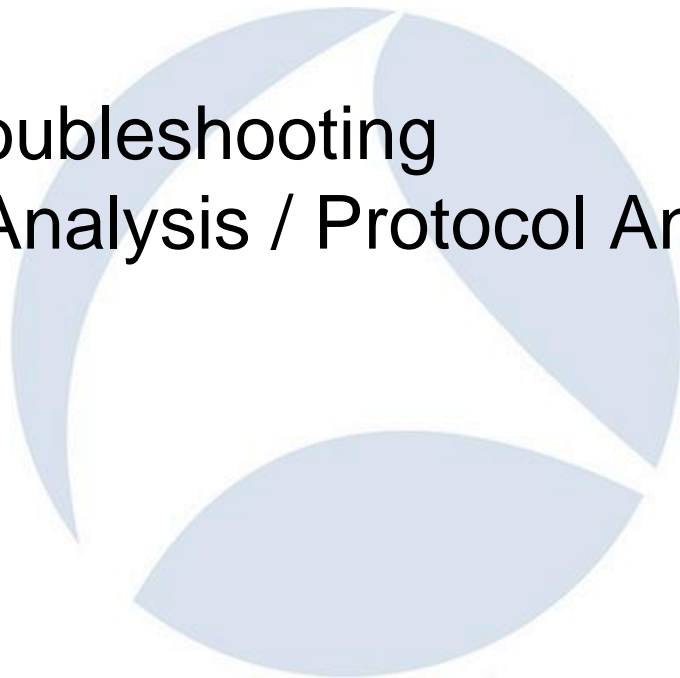
- A comprehensive, synergistic, holistic Performance Management strategy is needed to fully answer these questions
  - Packet based performance monitoring is a key part of that strategy
- 

# Questions / Discussion



# Packet Related Workflows & Technologies

- Capture
- Monitoring
- Triage and Troubleshooting
- Performance Analysis / Protocol Analysis
- Planning



# Packet Capture

- Host Based Captures
  - Network Devices with Capture Capability
  - Passive Appliances
  - SPAN/TAP Design
  - Packet Aggregation Design
  - Packet Aggregation Appliances
- 

# Manage Multiple Host Capture Agents

Capture Manager - Encryption Level: 1

On-Demand Capture | Continuous Capture | AppResponse Xpert | PathProbe

Capture Agents from (Dev Servers.agents)

Agent Name	Description	TCP Port	Agent Network Adapter	Filter	Status
server-dev-01		27401	6.1.136] eth0	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
apache-dev-01		27401	6.0.23] eth0	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux
face-tcserver-dev-01		27401	6.1.204] eth1	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
face-tcserver-dev-02		27401	6.0.84] eth0	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
strip-apache-dev-01		27401	6.0.64] eth0	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux
tcserver-dev-01		27401	6.1.21] eth1	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux

# Manage Multiple Host Agents

Capture Manager - Encryption Level: 1

On-Demand Capture | Continuous Capture | AppResponse Xpert | PathProbe

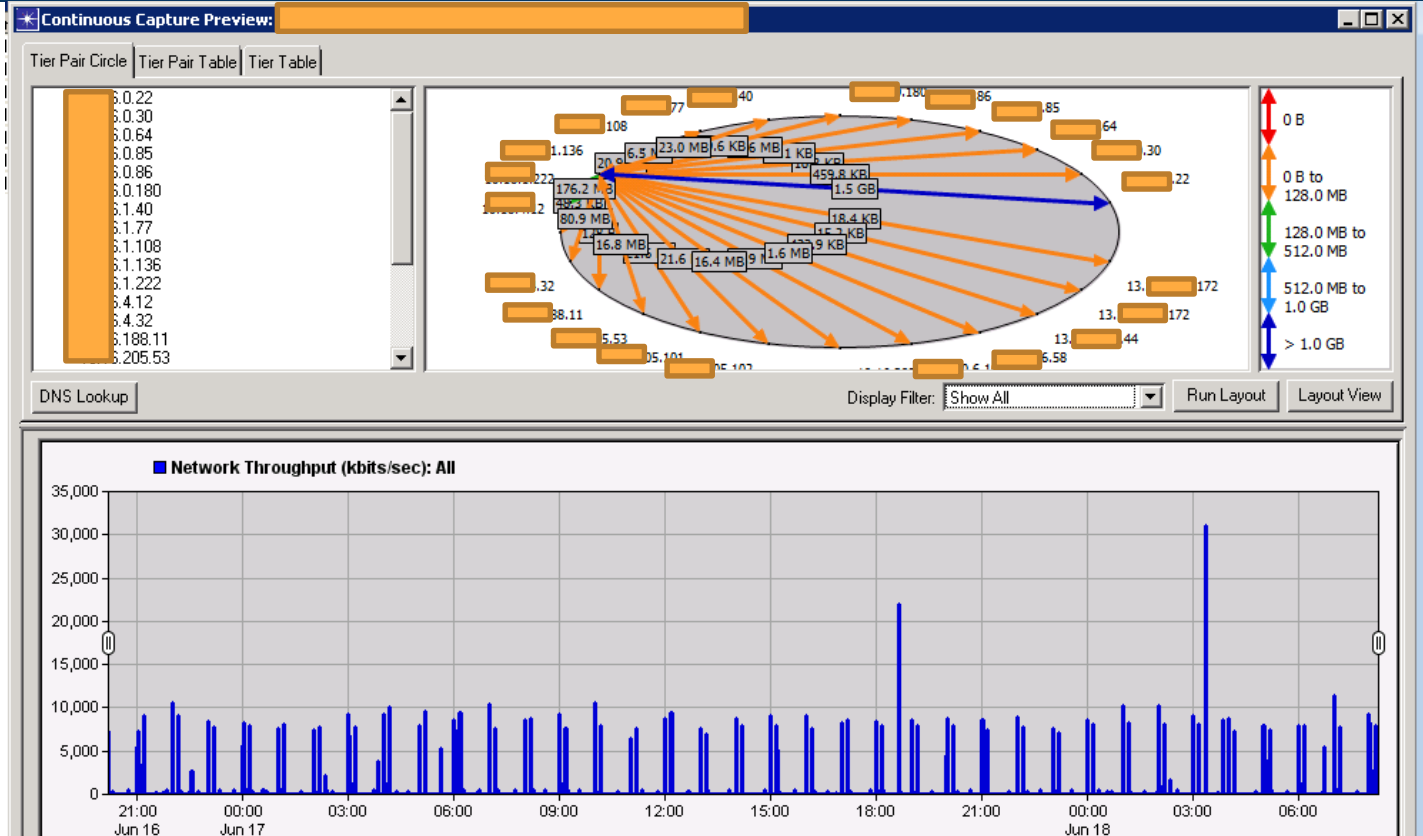
Capture Agents from (Dev Servers.agents)

Agent Name	Description	TCP Port	Agent Network Adapter	Filter	Status
tsserver-dev-01		27401	6.1.136] eth0	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
apache-dev-01		27401	6.0.23] eth0	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux
face-tcserver-dev-01		27401	6.1.204] eth1	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
face-tcserver-dev-02		27401	6.0.84] eth0	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
strip-apache-dev-01		27401	6.0.64] eth0	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux
tcserver-dev-01		27401	6.1.21] eth1	Default	0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux

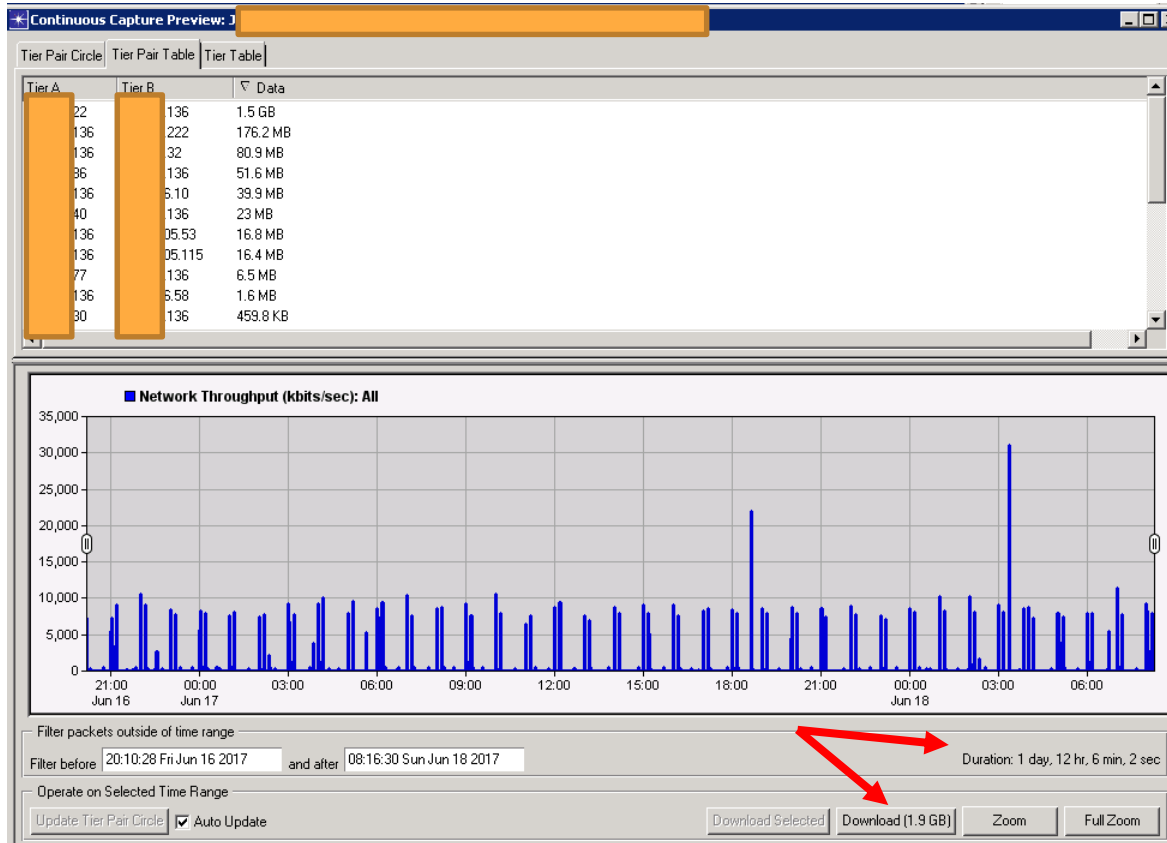
-- Capture Details --  
Name: Jun24  
Agent: [REDACTED]  
Capture time range: 20:10:28 Fri Jun 16 2017 to current  
Rolling buffer size: 2000 MB  
Promiscuous mode: True  
Maximum size of packet data to store: 65536 bytes  
Capture started by: jpittle  
Capture started from: [REDACTED]  
Filter: Default  
AppTransaction Xpert Packet Trace Warehouse repository size: 500 MB  
Agent network adapter [REDACTED]



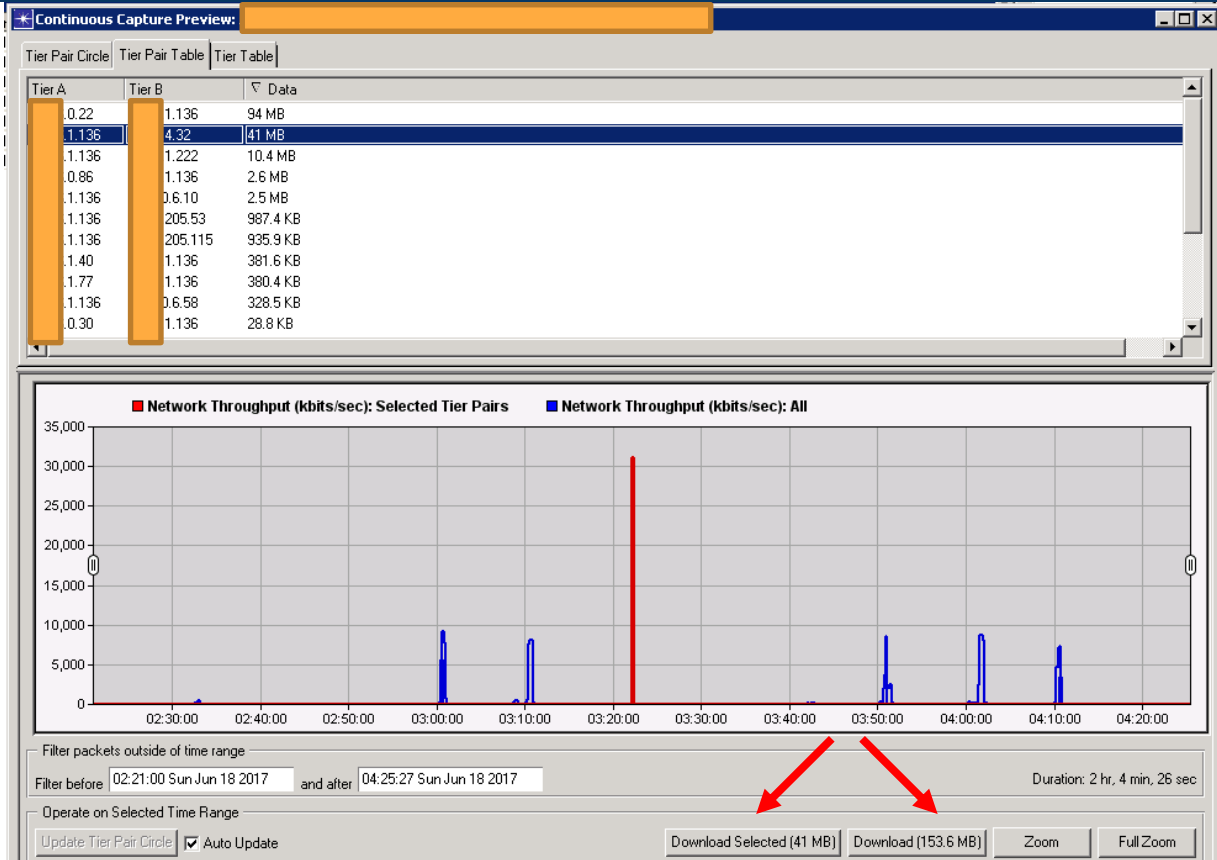
# Preview before downloading



# Preview before downloading



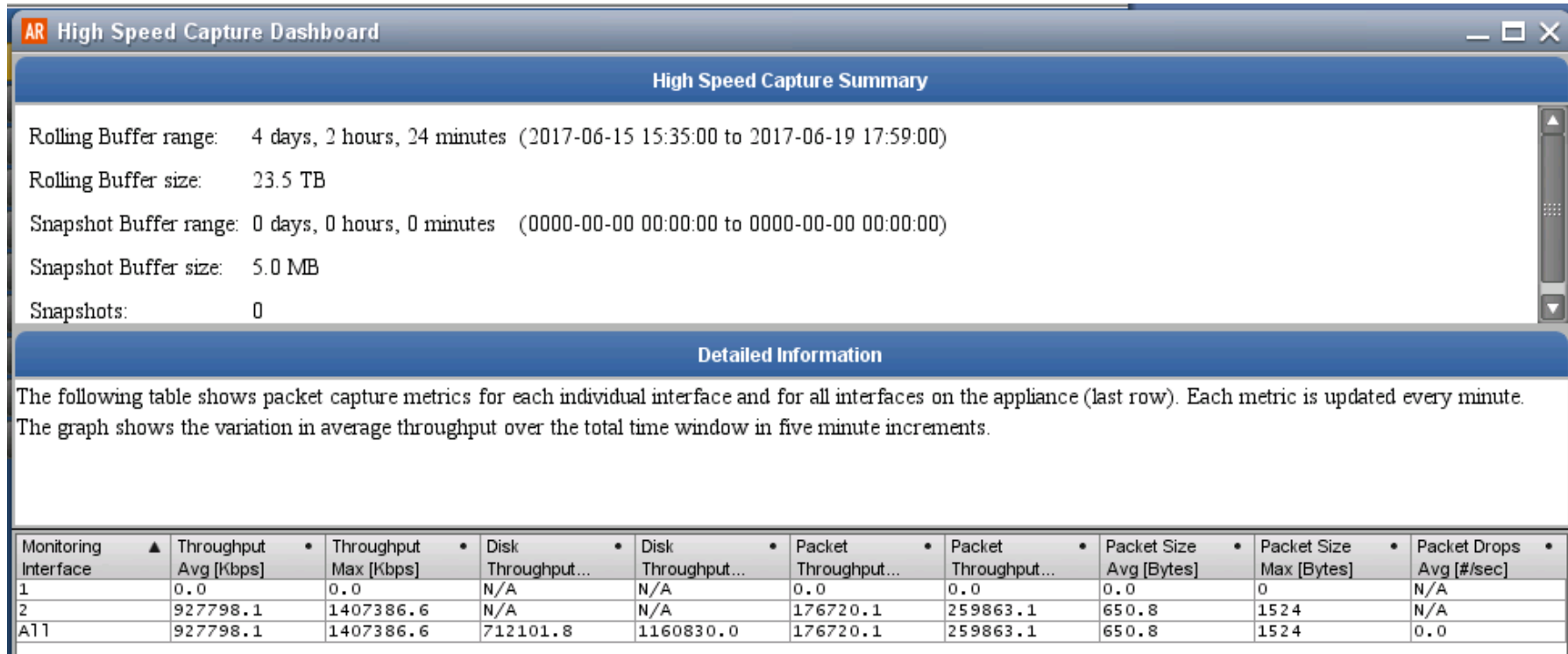
# Navigate to most relevant traffic before download



# Passive Appliances - Capture

- Always on, always analyzing performance
- All conversations, all the time, based on the traffic presented
- Capture packets into very large, indexed repository
- Packet Slicing and Filtering
- Byte Pattern Recognition
- Focused preview and selection of relevant conversations before download

# Passive Appliance - Continuous Capture



**AR High Speed Capture Dashboard**

### High Speed Capture Summary

Rolling Buffer range: 4 days, 2 hours, 24 minutes (2017-06-15 15:35:00 to 2017-06-19 17:59:00)  
Rolling Buffer size: 23.5 TB  
Snapshot Buffer range: 0 days, 0 hours, 0 minutes (0000-00-00 00:00:00 to 0000-00-00 00:00:00)  
Snapshot Buffer size: 5.0 MB  
Snapshots: 0

### Detailed Information

The following table shows packet capture metrics for each individual interface and for all interfaces on the appliance (last row). Each metric is updated every minute. The graph shows the variation in average throughput over the total time window in five minute increments.

Monitoring Interface	Throughput Avg [Kbps]	Throughput Max [Kbps]	Disk Throughput...	Disk Throughput...	Packet Throughput...	Packet Throughput...	Packet Size Avg [Bytes]	Packet Size Max [Bytes]	Packet Drops Avg [#/sec]
1	0.0	0.0	N/A	N/A	0.0	0.0	0.0	0	N/A
2	927798.1	1407386.6	N/A	N/A	176720.1	259863.1	650.8	1524	N/A
All	927798.1	1407386.6	712101.8	1160830.0	176720.1	259863.1	650.8	1524	0.0

# SPAN & TAP

- Engineered traffic feeds for performance and security tools
- SPAN design challenges
  - Device / traffic impacts
  - Full duplex over half duplex
  - Oversubscription
- TAP design challenges
  - Full duplex over half duplex
  - Managed vs. unmanaged TAPs
- Virtual TAPs for ESX

# Packet Aggregators

- Essential in large environments
  - Key Features:
    - Filtering, Splitting, Aggregating
    - Header modification
    - Scalability
    - De-dup
    - Flow generation
- 

# Questions / Comments

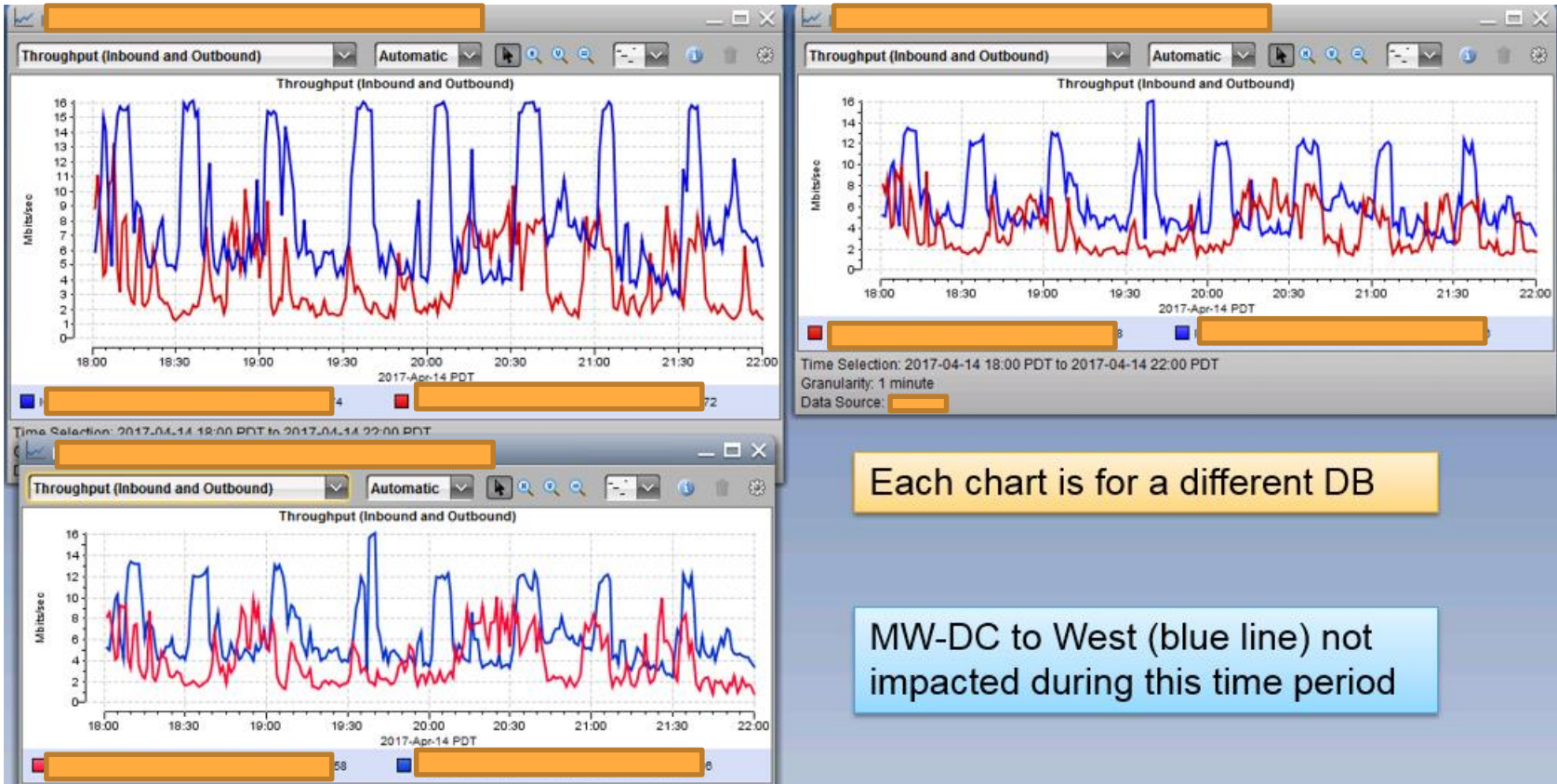




# Monitoring - Passive Appliances

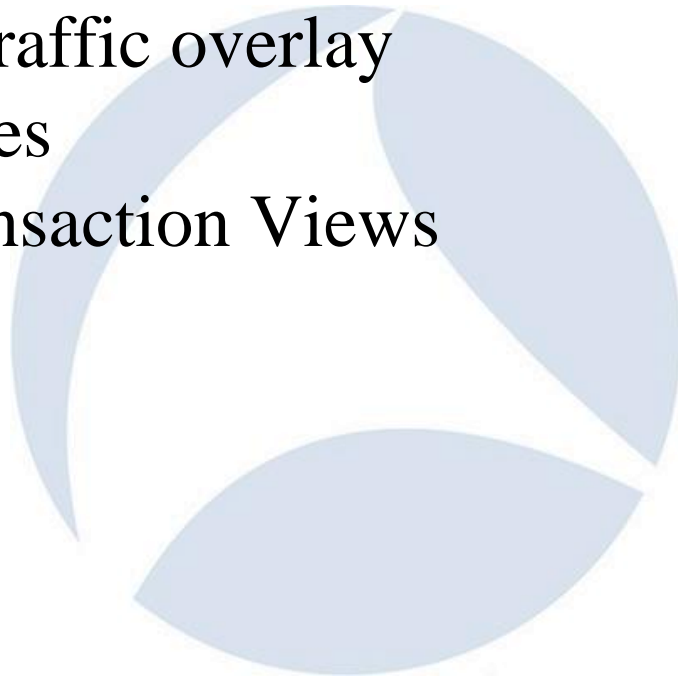
- Always on, always analyzing performance
- All conversations, all the time, based on the traffic presented
- Proactive alerting
- Baselineing and historical trends
- Quickly determine problem domain and download relevant packets when deeper dive is needed

# Real Time Views - Sample



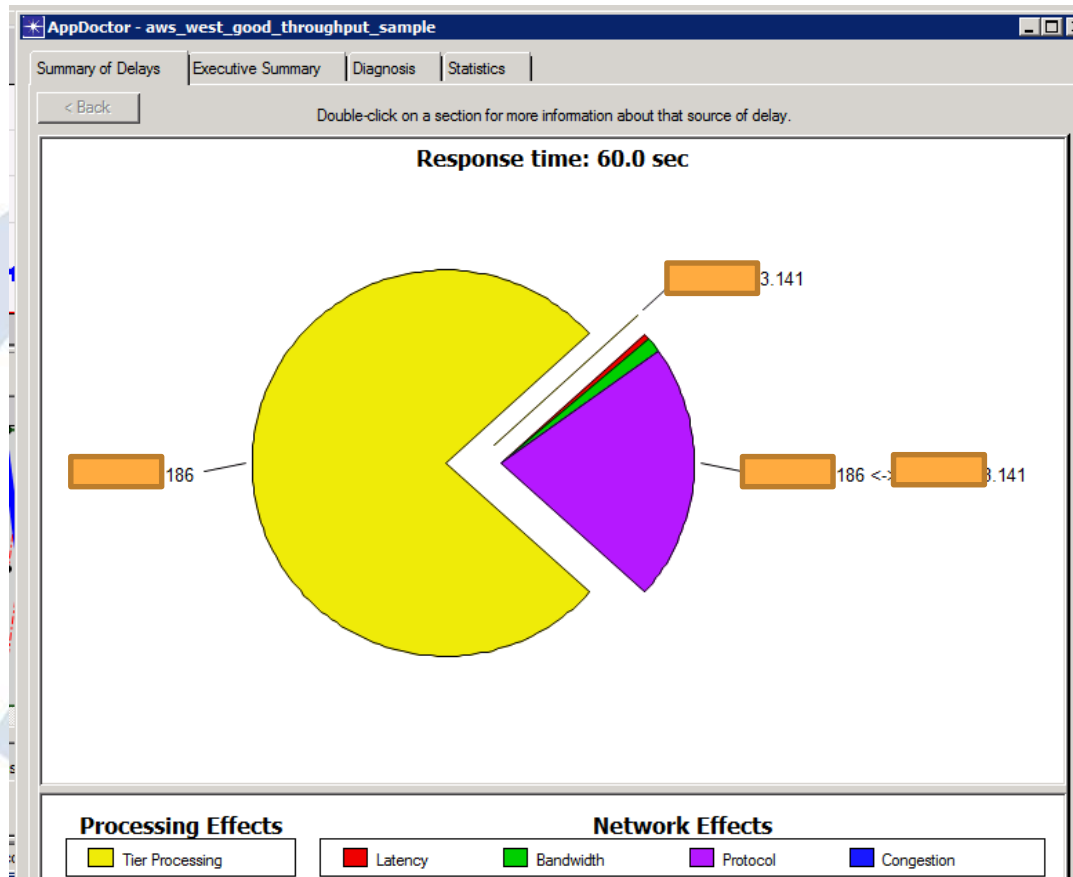
# Triage & Troubleshooting

- Automated Expert Analysis
- Key stats with traffic overlay
- Protocol Decodes
- End to End Transaction Views



# Expert Analysis Sample

- 1 minute sample
- Automated Summary of Delays Analysis



# Summary Statistics

- Some minor packet loss detected as reported by the 7 3ACK indicators
- Out of sequence packets are not necessarily expected, but we are using Internet transport so we should expect the unexpected

AppDoctor - west\_good\_throughput\_sample

Summary of Delays | Executive Summary | Diagnosis | Statistics

	Total	36	41
User Think Time (sec)	0.000000	0.000000	N/A
Effect of Processing (sec)	46.042246	45.999809	0.042437
Effect of Network (sec)	13.963628	N/A	N/A
Parallel Effects (sec)	0.000000	N/A	N/A

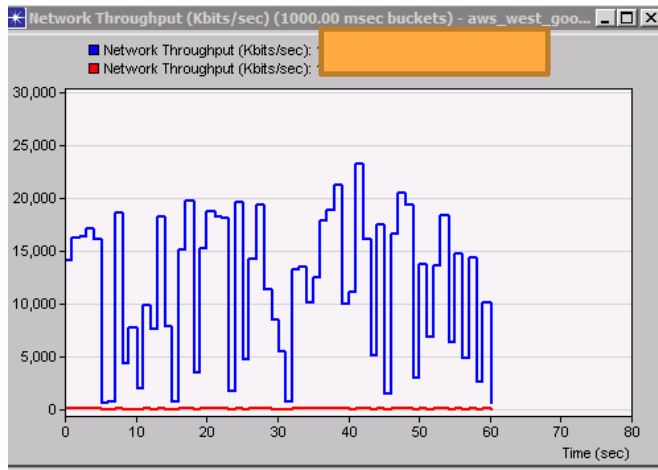
  

	Total	186 <->	1
Response Time (sec)	60.005874	60.005874	
Application Turns	46	46	
Application Messages	61,912	61,912	
Application Data (bytes)	84,520,800	84,520,800	
Average Application Message (bytes)	1,365.18	1,365.18	
Network Packets	69,166	69,166	
Network Data (bytes)	89,366,476	89,366,476	
Average Network Packet (bytes)	1,292.06	1,292.06	
Latency (ms)	N/A	7.10	
Effect of Latency (sec)	0.333812	0.333812	
Bandwidth (Kbps)	N/A	1,000,000.000	
Effect of Bandwidth (sec)	0.702963	0.702963	
Effect of Protocol (sec)	12.921820	12.921820	
Effect of Congestion (sec)	0.005034	0.005034	
Effect of Network Transfer (sec)	13.629817	13.629817	
Max Application Bytes Per Turn (A -> B)	N/A	16,086,279	
Max Application Bytes Per Turn (A <- B)	N/A	64	
Max Unacknowledged Data (A -> B) (bytes)	N/A	213,252	
Max Unacknowledged Data (A <- B) (bytes)	N/A	64	
Retransmissions	0	0	
Out of Sequence Packets	314	314	
Connection Resets	0	0	
TCP Frozen Window (sec)	0.000000	0.000000	
TCP Nagle's Algorithm (sec)	0.000000	0.000000	
TCP Triple-Duplicate ACK Loss Indications	7	7	

Export to Spreadsheet

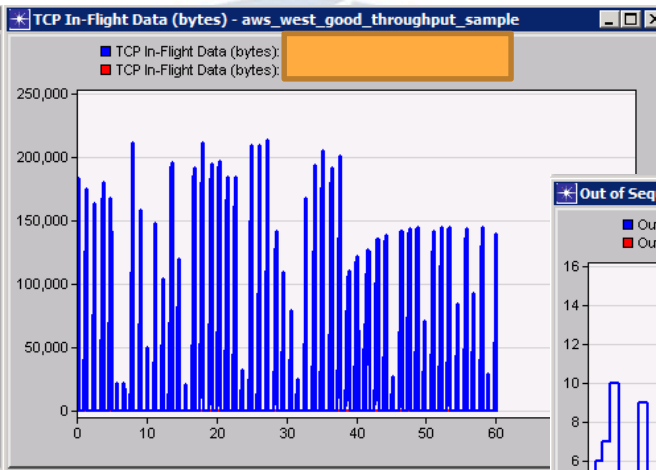
# Relevant Statistics

## Throughput

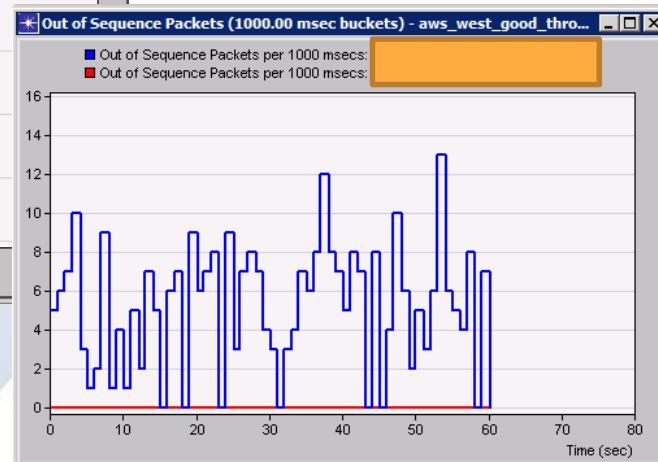


Microbursts of 18-23Mbps

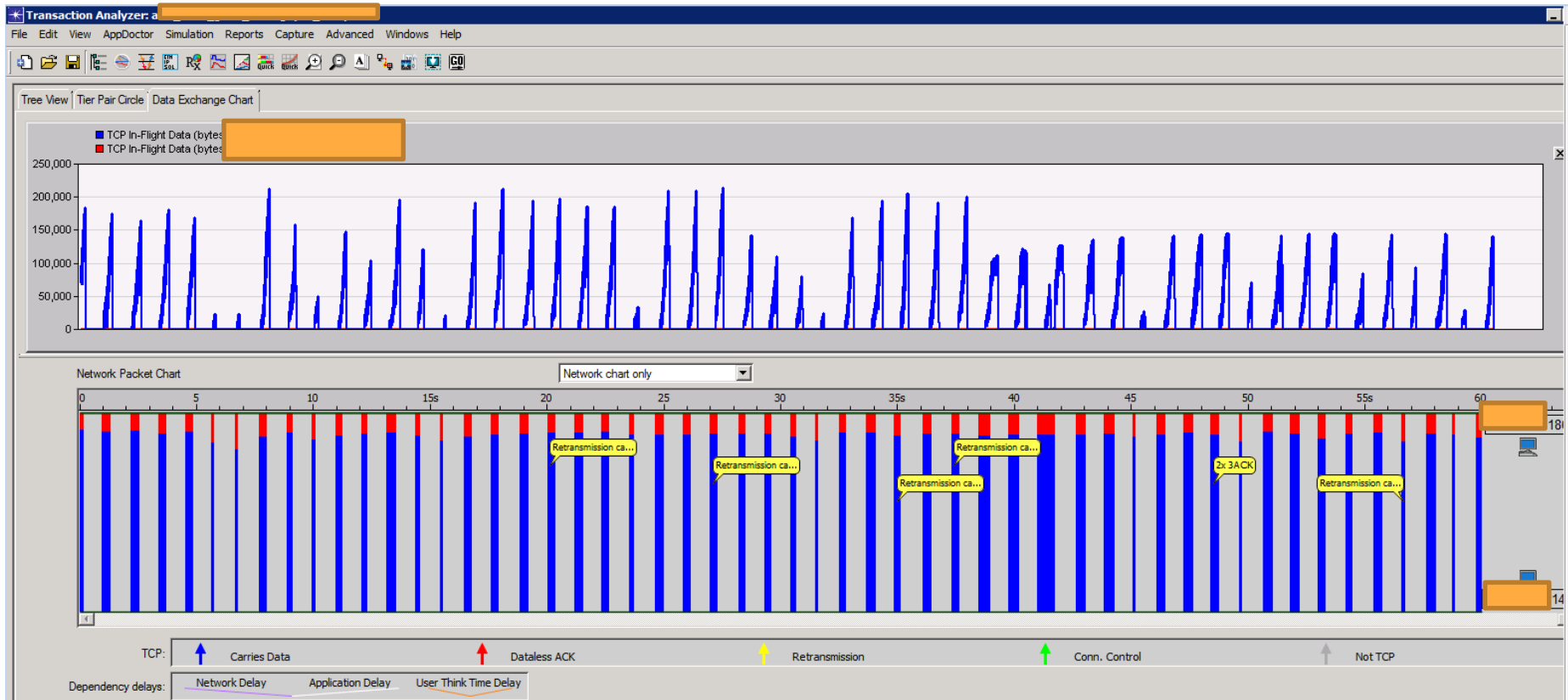
## Bytes in Flight



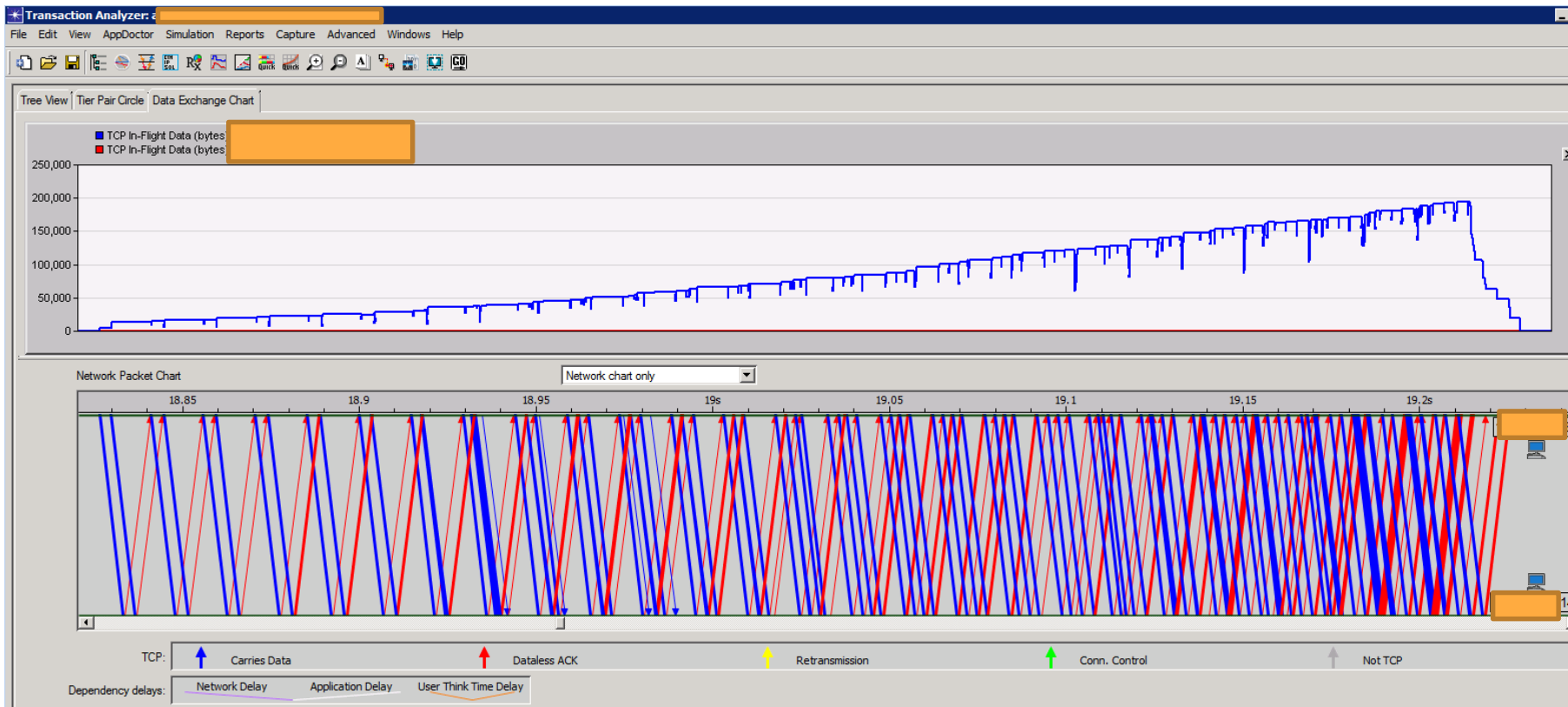
## Out of Sequence



# Packet Exchange vs. Bytes in Flight



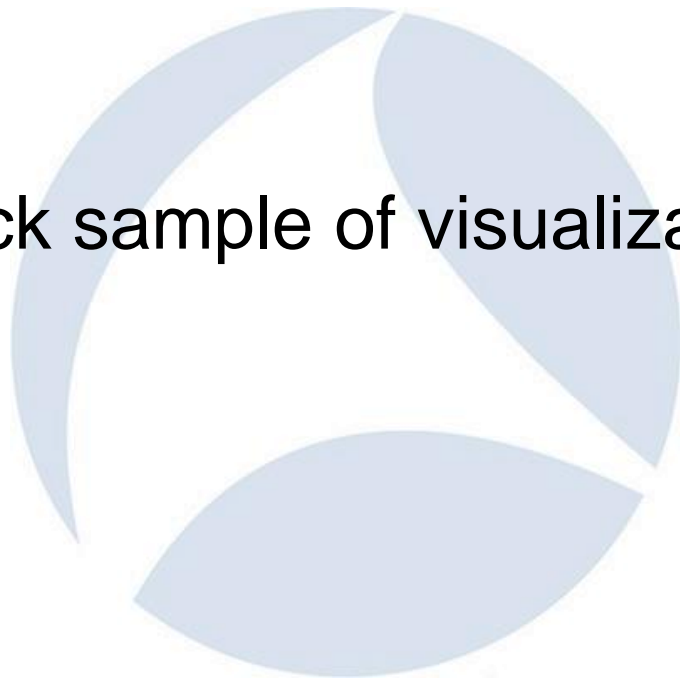
# 399ms burst drill down - 2.2 MB



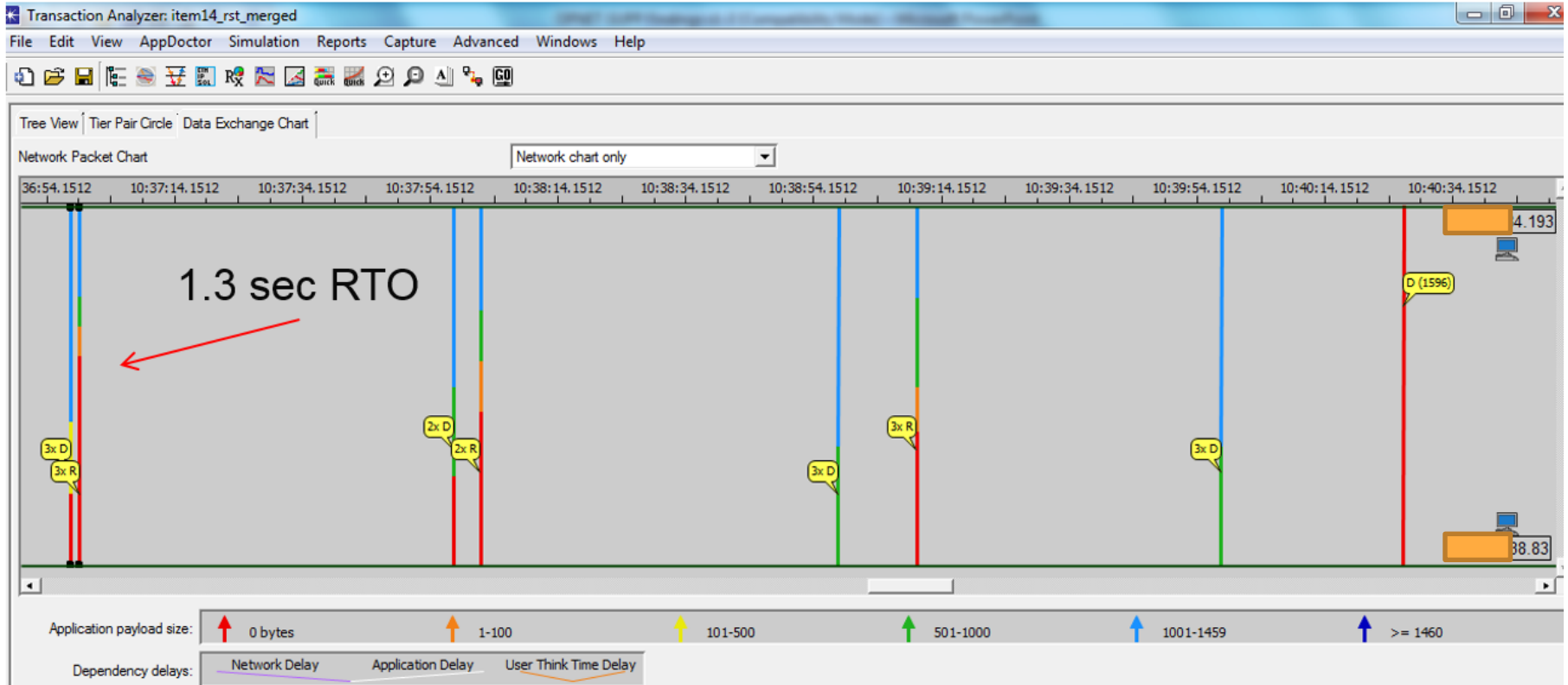


# Questions / Comments

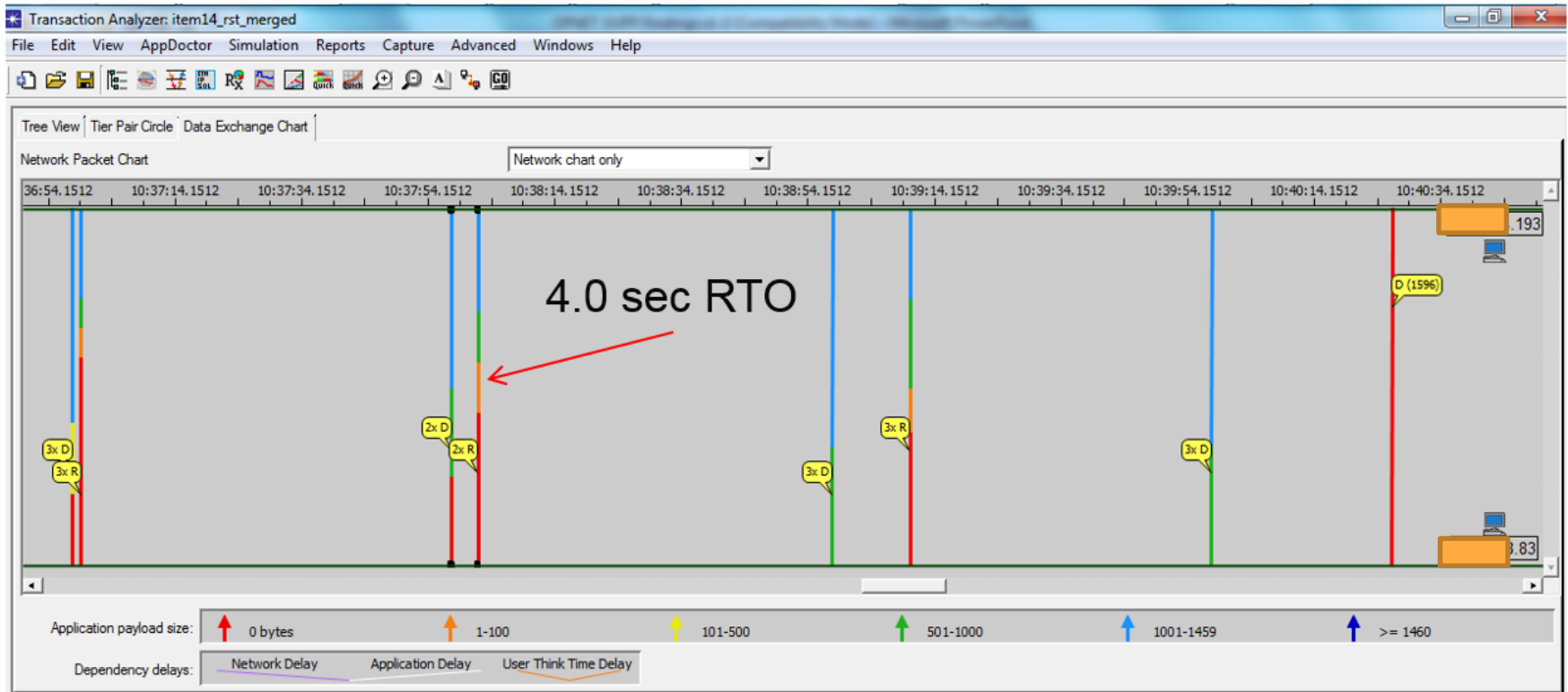
- Diagnosed TCP Slow Start on Idle without looking at decodes
- One more quick sample of visualization before we move on.....



# TCP RTO Visualization 1 of 4



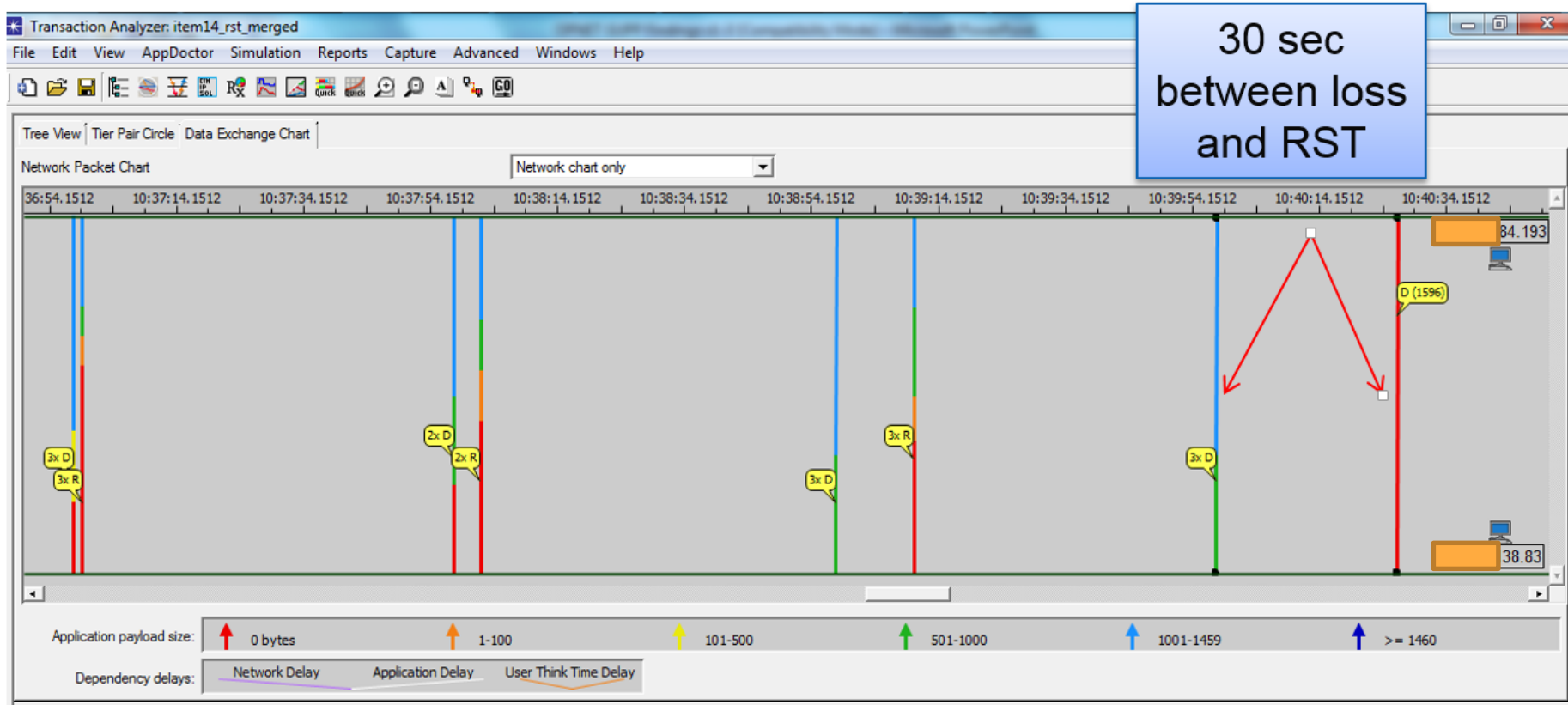
# TCP RTO Visualization 2 of 4



# TCP RTO Visualization 3 of 4



# TCP RTO Visualization 4 of 4



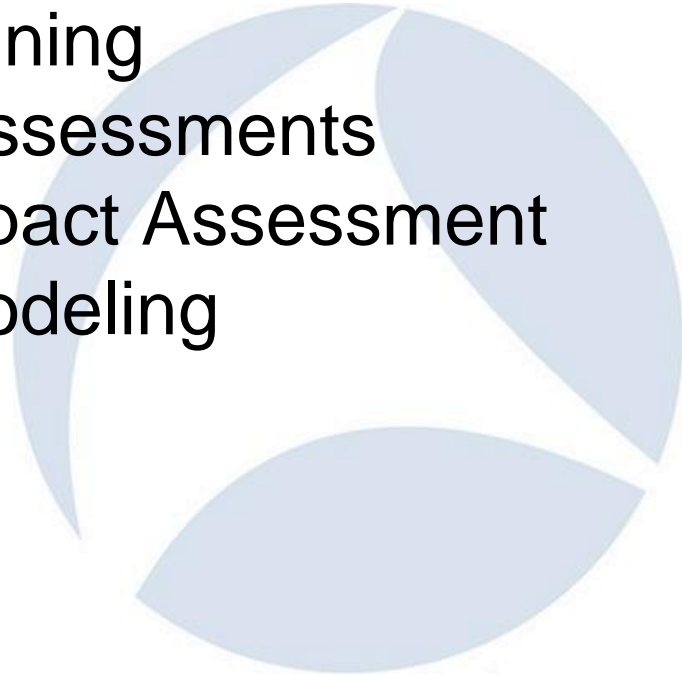
# Performance Analysis Workflows

- Dev Team Unit Testing
- Load Testing
- Pre-Deployment
- New Technology Assessments
- 3<sup>rd</sup> Party Software Qualification

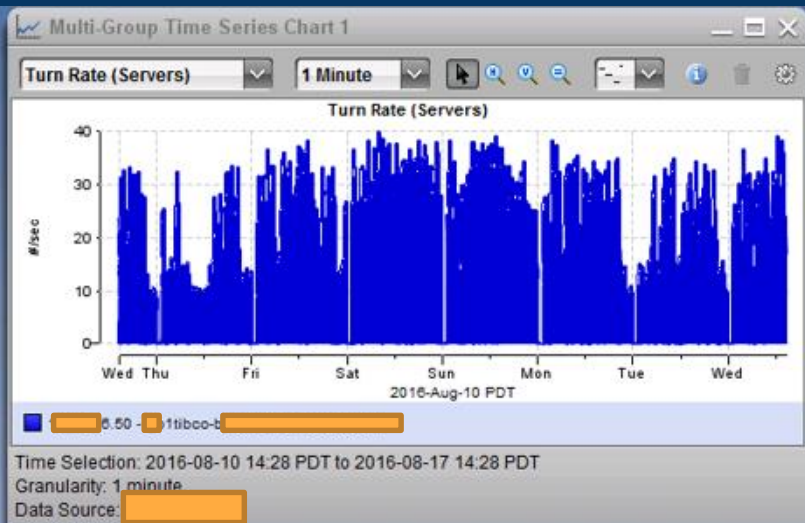
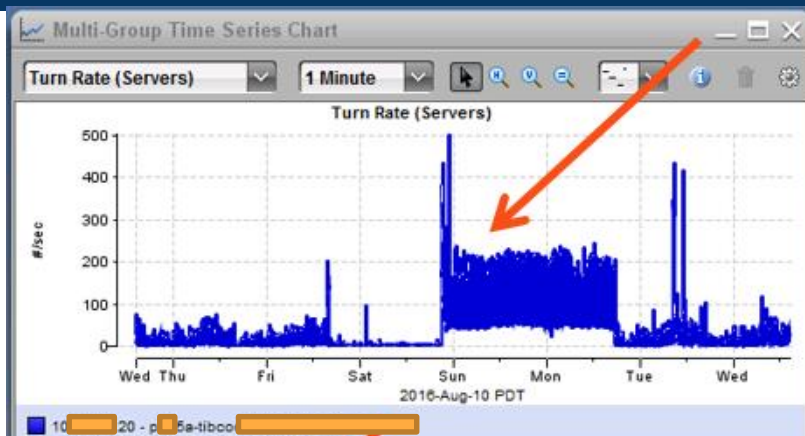


# Impact Assessments / Planning

- Capacity Planning
- Migration Planning
- Technology Assessments
- Bandwidth Impact Assessment
- End to End Modeling

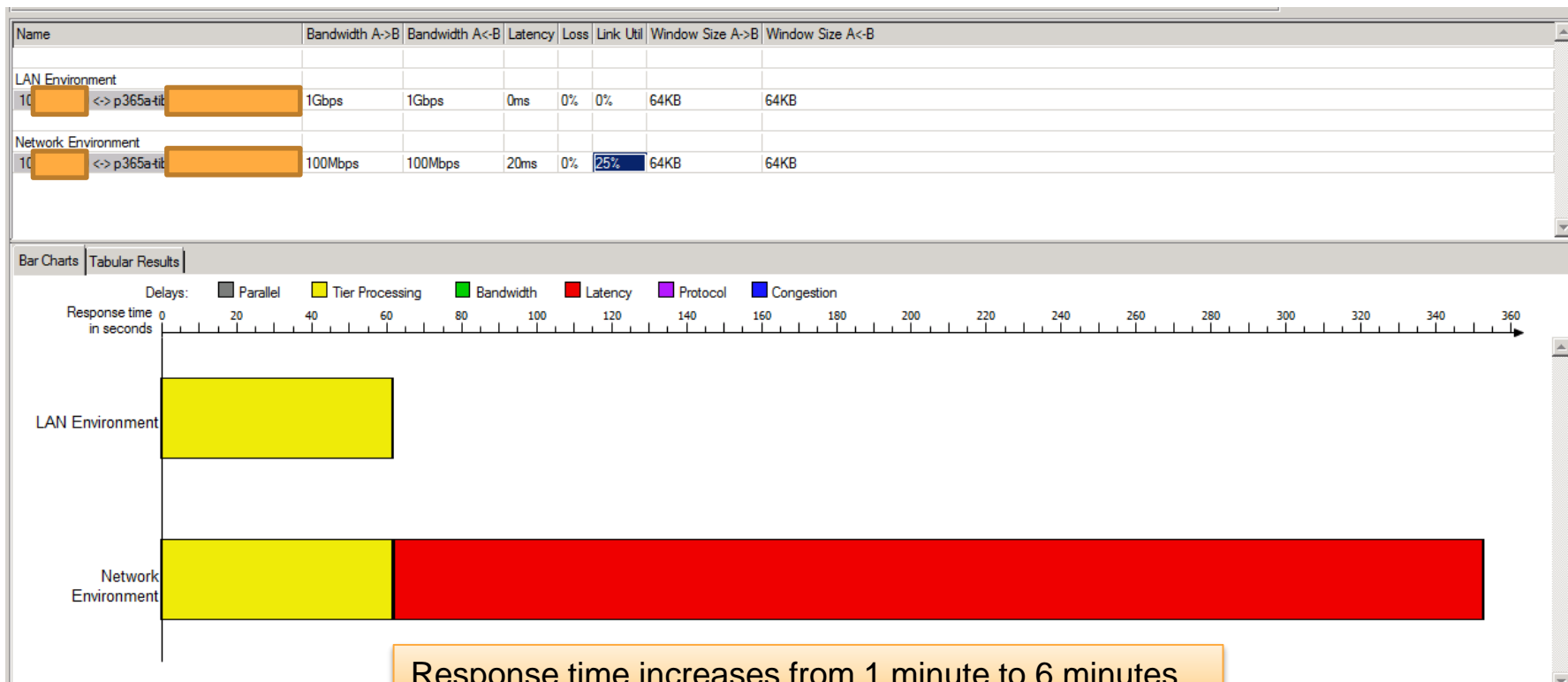


# Migration Planning - Latency Sensitive Conversations





# Impact of 40ms Round Trip Latency



# Questions / Discussion



# Requirements / Business Case

- Packets are an essential data source for Performance Management workflows
- Business leaders / budget owners seldom understand the importance
- They need your help to understand how visibility gaps are actually a risk to the business

# Troubleshooting in the Wild

- DB Replication Delays impact customer data visibility
- Claims Management Down
- Load Testing brings down production data center
- Call Center Stability Disruption
- eCommerce web page crash during checkout
- 2 hour outage of global eCommerce website
- Finance website crashes after super bowl commercial
- Global DNS Failover Troubleshooting

# Business Case

- Tie your requirements for packet based capabilities to key apps and key infrastructure services
- Characterize the business risk to your key apps & infrastructure
- Capture current state capabilities
- Identify gaps
- Identify risk to the business

# Types of Service Delivery Risks

- Poor app performance overall, can't meet SLAs
- App / Service is non-responsive
- Dependent system is down
- Can't complete key transactions
- Incomplete visibility
- Poorly performing infrastructure services are impacting everything

# Business Impact

- Customer Churn
  - Lost Revenue
  - Lost Productivity / Overtime Costs
  - Penalties / Fines
  - Missed Market Opportunities
- 

# Key Apps

- The most important apps to the business
- Characterize scope, scale, user community
- Identify business disruption when these apps are down or performing poorly
- Simple spreadsheet to capture key attributes



# Key App Attributes

	A	B	C	D	E	F	G
1							
2	<b>&lt;Customer&gt; Visibility Assessment - Key Apps</b>						
3	Enter details for up to 10 applications considered critical to the business						
4							
5		App #	App Name	App Technology	Primary BU	Business Use	Hosting Location
6		1					
7		2					
8		3					
9		4					



	A	B	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																
2	<b>&lt;Customer&gt; Visibility</b>															
3	Enter details for up to															
4			<b>Business Impact of Outage, (choose all that apply)</b>													
5	App #	Hosting Location	Est. # of outages last 90 days	Est. total minutes outage / impact last 90 days	Count of Registered Users	Peak Concurrent Users	Est. cost of outage /Hr (Low)	Est. cost of outage /Hr (Med)	Est. cost of outage /Hr (High)	Lost Revenue (Y/N)	Higher Costs (Y/N)	Lost Mktk Opportunity (Y/N)	Customer Sat (Y/N)	Other (Specify)		
6	1															
7	2															
8	3															
9	4															
10	5															



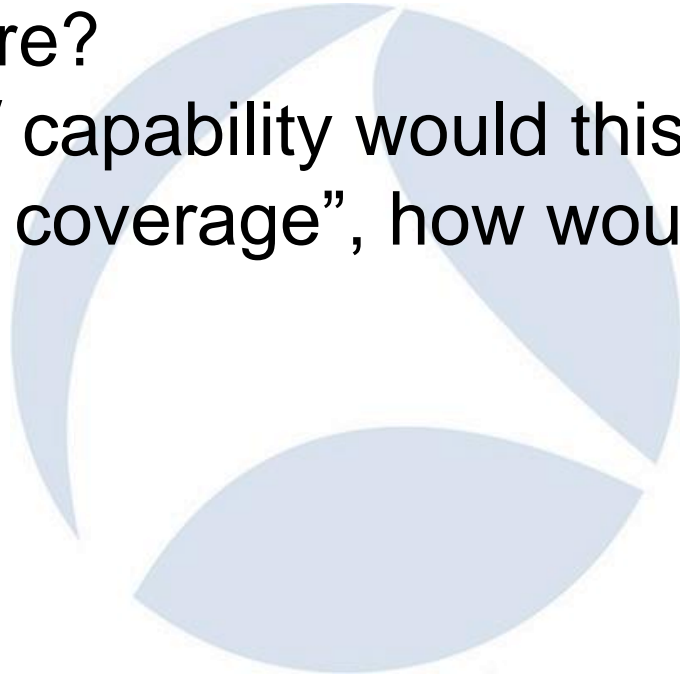
# Who has these details?

- Service Delivery Managers
- IT Business Office
- BU Owners
- Operations



# Current State Capture / Visibility Capabilities

- For each Key App - what is the most essential traffic to capture?
- What metrics / capability would this give you?
- If you had “full coverage”, how would you describe it?



# Heat Map Overview

- Simple Excel Spreadsheets with conditional formatting
- Visualize where we need coverage vs. where we have coverage
- Use color scheme to indicate risk
- Iterations of the heat map can be used to communicate a plan & cost estimates

# Current State – Packet Capture Coverage

Views	Key Applications Current State								
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance			
End User Experience	Red	Red	Red	Red	Red	Red	Grey	Grey	
Web to App Performance	Red	Red	Red	Red	Red	Red	Grey	Grey	
App to DB Performance	Yellow	Red	Red	Yellow	Red	Yellow	Grey	Grey	
App to Partner Systems	Grey	Red	Red	Grey	Red	Red	Grey	Grey	
App to SSO Performance	Red	Red	Red	Red	Red	Red	Grey	Grey	
	Green	Complete		Yellow	Some Risk		Grey	Not Applicable	
	Light Green	Partial		Red	Significant Risk				

# Current State / Future State Roadmap

- Where are my gaps / risks today?
  - What do I address first?
  - ...second?
  - ...third, and so on?
- 
- What would it take to reduce unplanned downtime for this app by 120 minutes per year?
  - What would that be worth to the business?

# Phase 1 – This Quarter

Views	Key Applications Roadmap Phase 1							
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	Red	Green	Green	Red	Red	Red	Grey	Grey
Web to App Performance	Red	Green	Green	Red	Red	Red	Grey	Grey
App to DB Performance	Yellow	Green	Green	Yellow	Red	Yellow	Grey	Grey
App to Partner Systems	Grey	Green	Green	Grey	Red	Red	Grey	Grey
App to SSO Performance	Red	Green	Green	Red	Red	Red	Grey	Grey
	Green	Complete		Yellow	Some Risk		Grey	Not Applicable
	Light Green	Partial		Red	Significant Risk			



# Phase 2 – Next Quarter

Views	Key Applications Roadmap Phase 2								
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance			
End User Experience	Complete	Complete	Complete	Complete	Complete	Significant Risk	Not Applicable	Not Applicable	
Web to App Performance	Complete	Complete	Complete	Complete	Complete	Significant Risk	Not Applicable	Not Applicable	
App to DB Performance	Complete	Complete	Complete	Complete	Complete	Some Risk	Not Applicable	Not Applicable	
App to Partner Systems	Not Applicable	Complete	Complete	Not Applicable	Complete	Significant Risk	Not Applicable	Not Applicable	
App to SSO Performance	Complete	Complete	Complete	Complete	Complete	Significant Risk	Not Applicable	Not Applicable	
	Complete	Complete			Some Risk		Not Applicable	Not Applicable	
	Partial				Significant Risk				

# Phase 3 – two Quarters out

Views	Key Applications Roadmap Phase 3								
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance			
End User Experience	Complete	Complete	Complete	Complete	Complete	Complete	Not Applicable	Not Applicable	
Web to App Performance	Complete	Complete	Complete	Complete	Complete	Complete	Not Applicable	Not Applicable	
App to DB Performance	Complete	Complete	Complete	Complete	Complete	Complete	Not Applicable	Not Applicable	
App to Partner Systems	Some Risk	Complete	Complete	Some Risk	Complete	Complete	Not Applicable	Not Applicable	
App to SSO Performance	Complete	Complete	Complete	Complete	Complete	Complete	Not Applicable	Not Applicable	
	Complete	Complete		Some Risk			Not Applicable	Not Applicable	
	Partial			Significant Risk					

# Alternate Phase 1

Views	Key Applications Roadmap Phase 1								
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance			
End User Experience	Green	Green	Green	Green	Green	Green	Grey	Grey	
Web to App Performance	Red	Red	Red	Red	Red	Red	Grey	Grey	
App to DB Performance	Yellow	Red	Red	Yellow	Red	Yellow	Grey	Grey	
App to Partner Systems	Grey	Red	Red	Grey	Red	Red	Grey	Grey	
App to SSO Performance	Green	Green	Green	Green	Green	Green	Grey	Grey	
	Green	Complete		Yellow	Some Risk		Grey	Not Applicable	
	Light Green	Partial		Red	Significant Risk				

# Comments / Discussion



# Key Infrastructure – Shared Services

- What are some key shared services in your environment?
- Degradation in these services will impact the entire environment



# Key Infrastructure – Shared Services

- DNS
  - NTP
  - Active Directory / LDAP
  - Single Sign-on
  - Email
  - Sharepoint Servers
  - VPN / Token Gateways
  - NAS Storage
  - VoIP and related infrastructure
  - Etc...
- 

# Current State – Critical Shared Services

	Critical Infrastructure Services					
	DNS	Global Load Balancer	AD/LDAP	Single Sign On (SSO)	Prod NetApp Filers	Local Load Balancers
Response Time	Yellow	Red	Light Green	Yellow	Red	Light Green
Transaction Rates	Green	Green	Green	Yellow	Light Green	Green
Connection Rates	Green	Green	Green	Yellow	Light Green	Green
Resource Utilization	Yellow	Green	Yellow	Green	Green	Yellow
Throughput Rates	Green	Green	Yellow	Yellow	Light Green	Green
Packet Loss / Retrans	Light Green	Green	Yellow	Yellow	Red	Green
Packet Captures	Yellow	Green	Red	Red	Red	Green
	Green	Complete		Yellow	Some Risk	
	Light Green	Partial		Red	Significant Risk	

# Questions / Comments





# General Recommendations

- Use passive appliances to get coverage for infrastructure shared services and all application edge traffic (EUE)
- Identify key apps where inter-tier packets are most beneficial and expand traffic feeds
- Leverage host based captures everywhere
- Add supplemental analysis capabilities on top of Wireshark

# Wrap-Up

- Packets are an essential component of your overall Performance Management capabilities
- Most companies have significant gaps in their packet capture and analysis workflows
- These gaps represent business risk and can be identified with a rationalized current state assessment tied to key apps and shared services
- Create a future state roadmap that shows the improvements and benefits of addressing gaps

# Thank You for your Participation!



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