SharkFest '17 Europe

Defining a Requirements Based Packet Capture Strategy

9 november 2017

John Pittle

Riverbed Technologies

#sf17eu • Estoril, Portugal • 7-10 november 2017

SharkFest '17 Europe

Alternate Title: Preparing to navigate Layer-8

9 november
2017

John Pittle

Riverbed Technologies

#sf17eu • Estoril, Portugal • 7-10 november 2017

Audience Profile

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

Speaker Introduction

- Team Lead: App911 Emergency Troubleshooting
- Team Lead: Technology Adoption Services
- Consulting Practice Mentor
- Best Practices Contributor
- Program Owner – Riverbed Performance Management Workshop Series
- Content Developer for Riverbed Performance Management Foundations Course

Speaker Introduction

- Team Lead: App911 Emergency Troubleshooting
- Team
- Cons
- Best
- Progr gement Work
- Cont Management Foundations Course

I Love solving complex performance problems with packets and performance tools

Session 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 and your Value to your Organization

Agenda

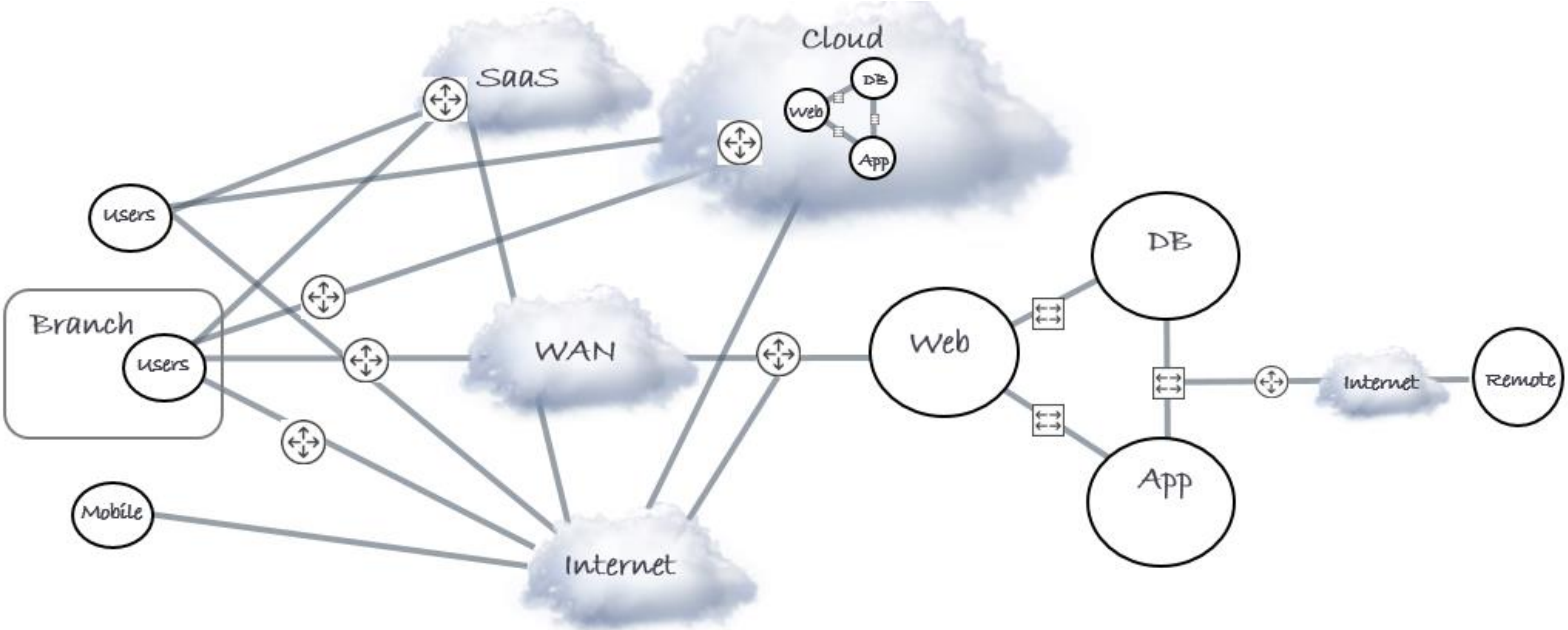
- Performance Management Landscape
- Packet Related Workflows & Technologies
- Requirements & Business Case Mechanics
- Gap & Risk Heat Maps
- Recommendations and Wrap-up

Performance Management Landscape

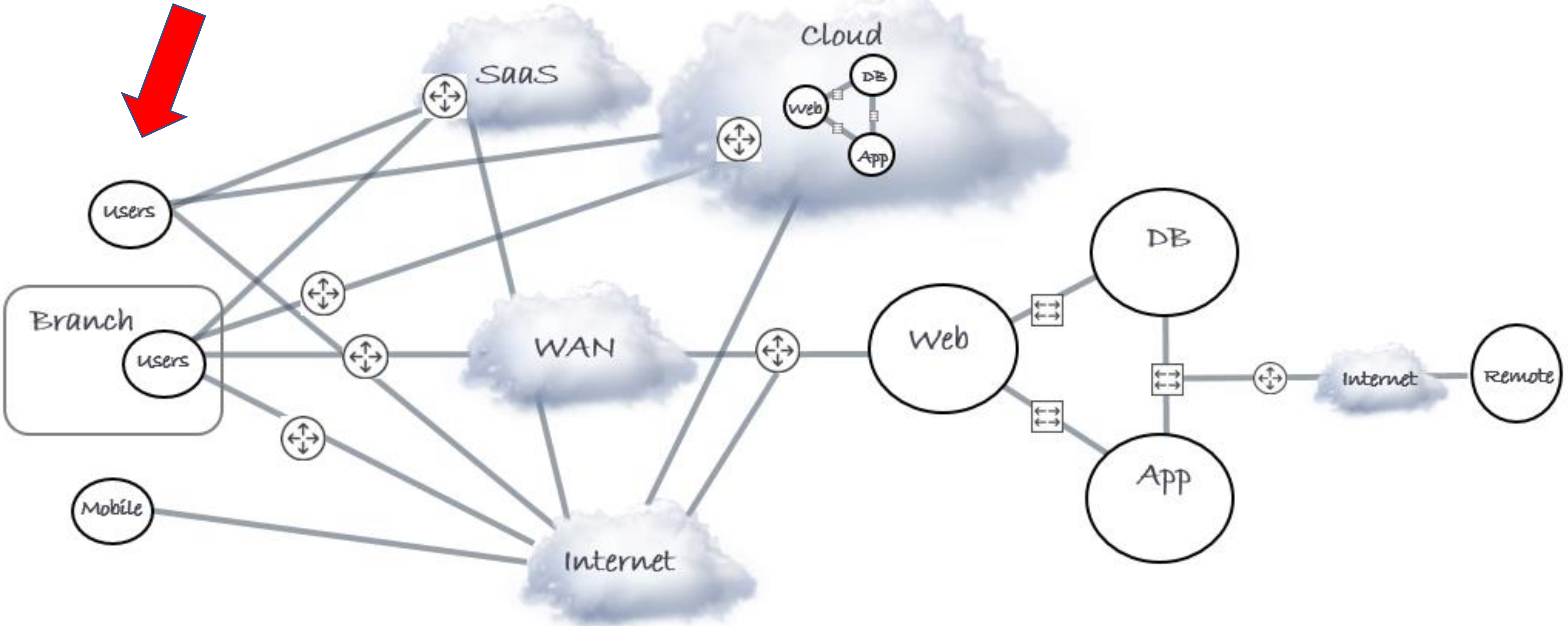
- End User Experience
- User End Point Monitoring
- Packets
- Flow (NetFlow, Jflow, Sflow, NBAR, etc)
- SNMP
- Application Metrics
- Application Logging
- Javascript Injection
- Host Metrics
- Infrastructure Metrics

Visibility and Instrumentation

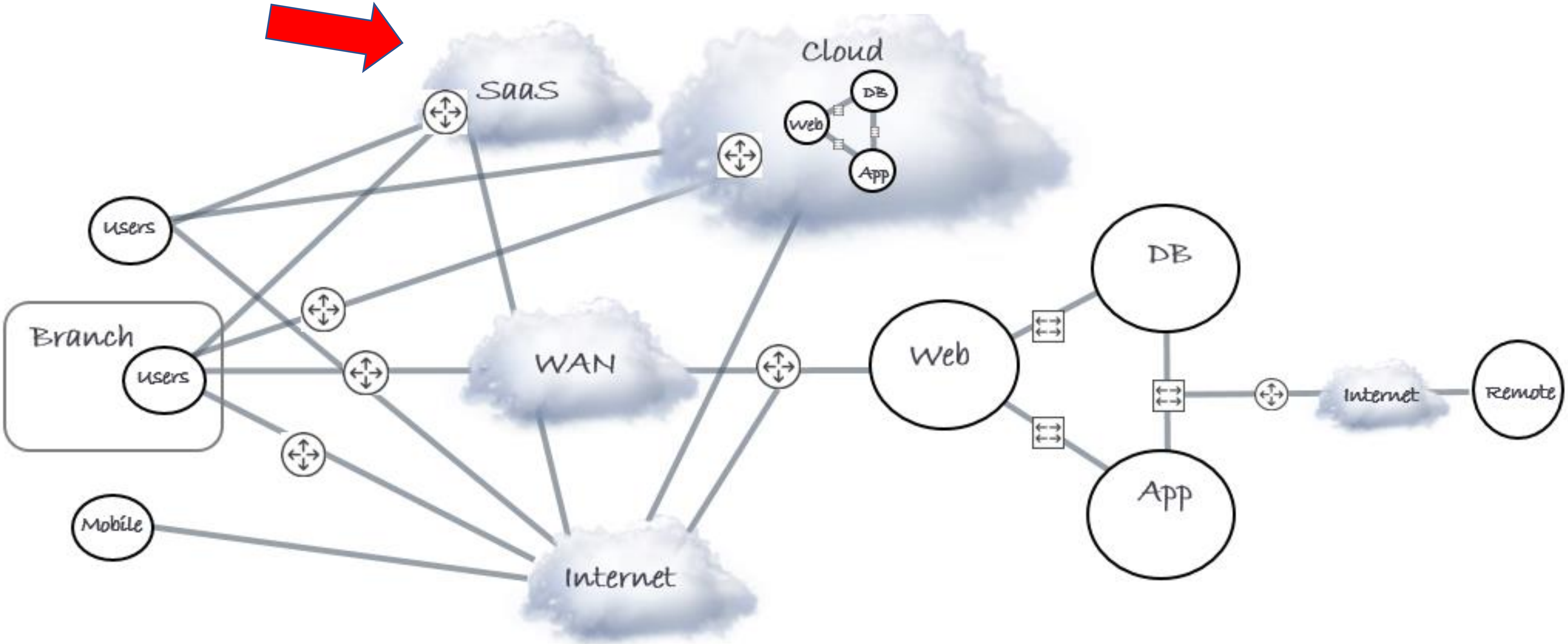
Hybrid Enterprise



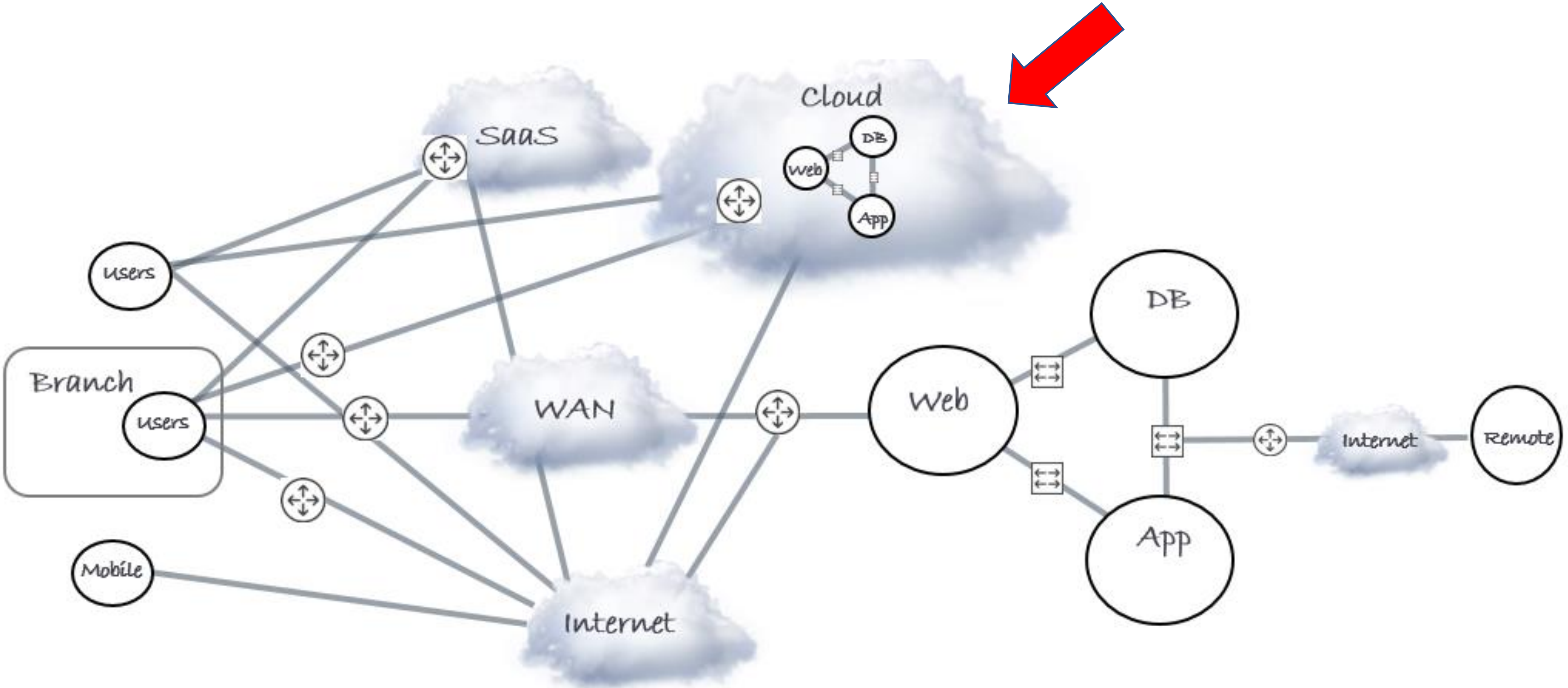
End User Devices & Locations



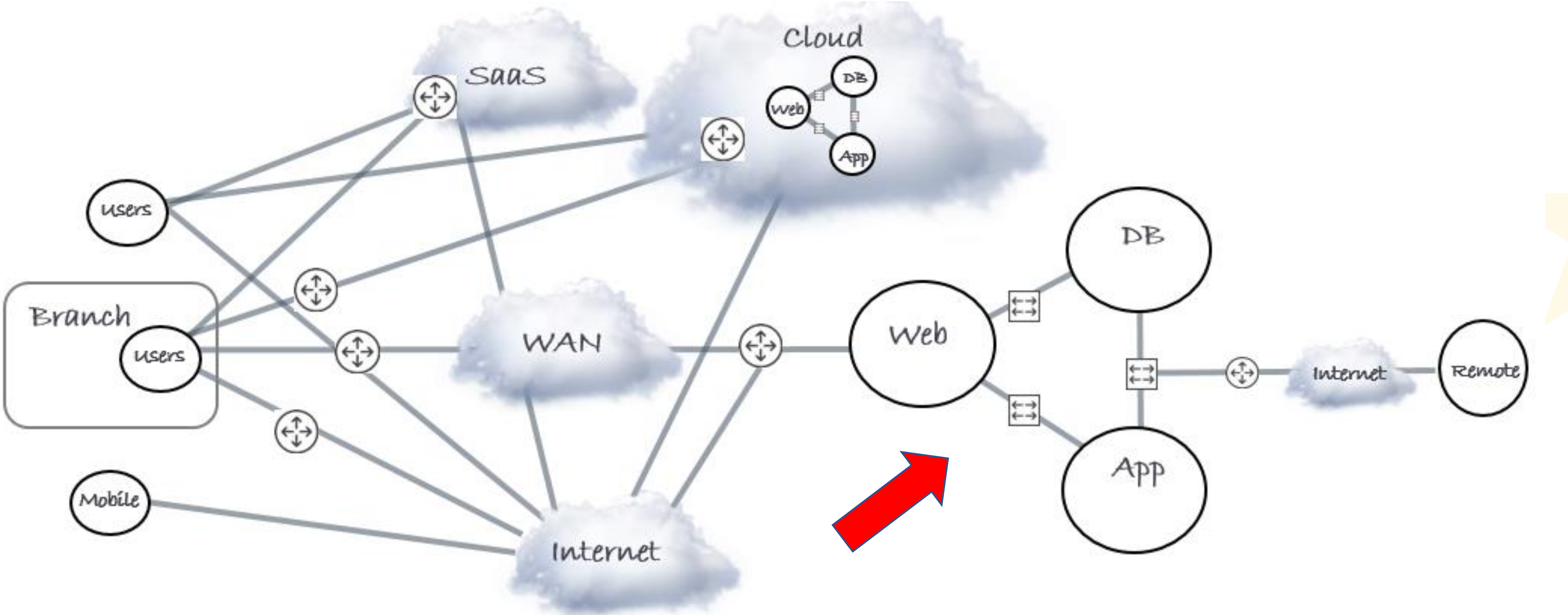
SaaS Applications



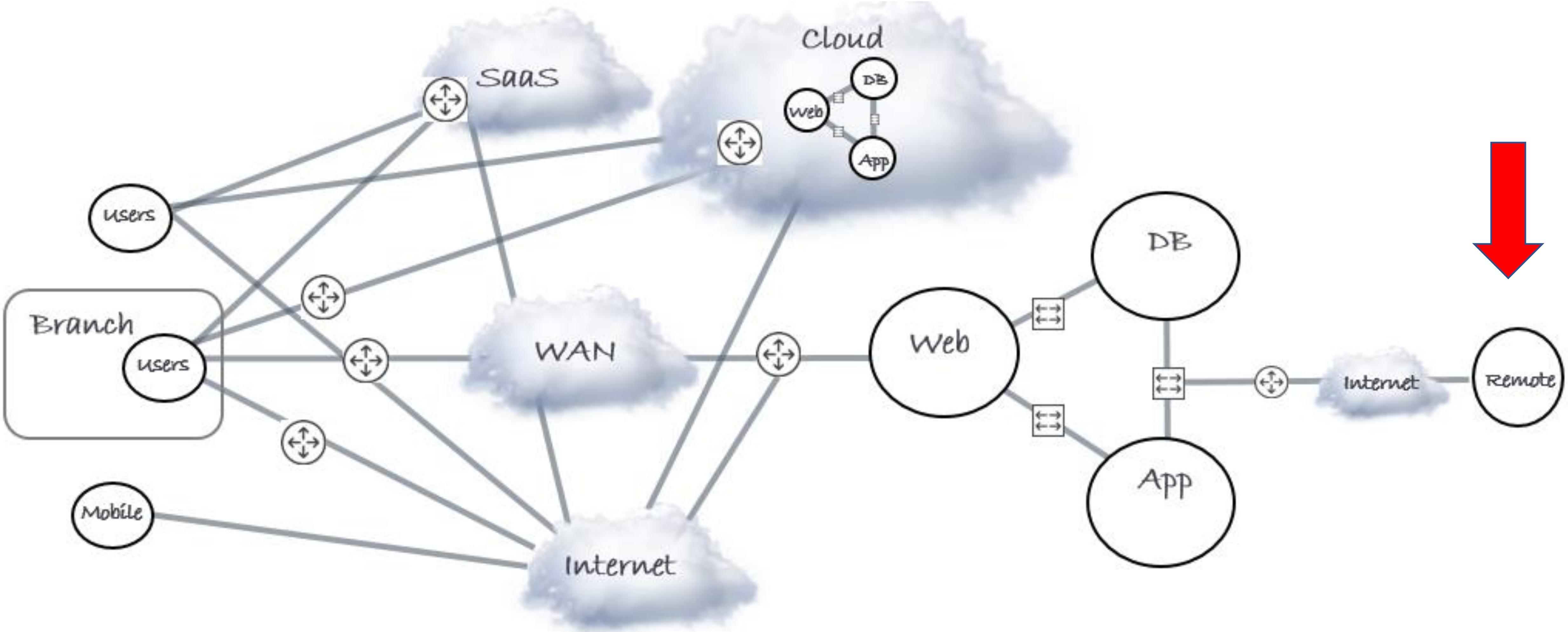
Cloud Hosting & Services



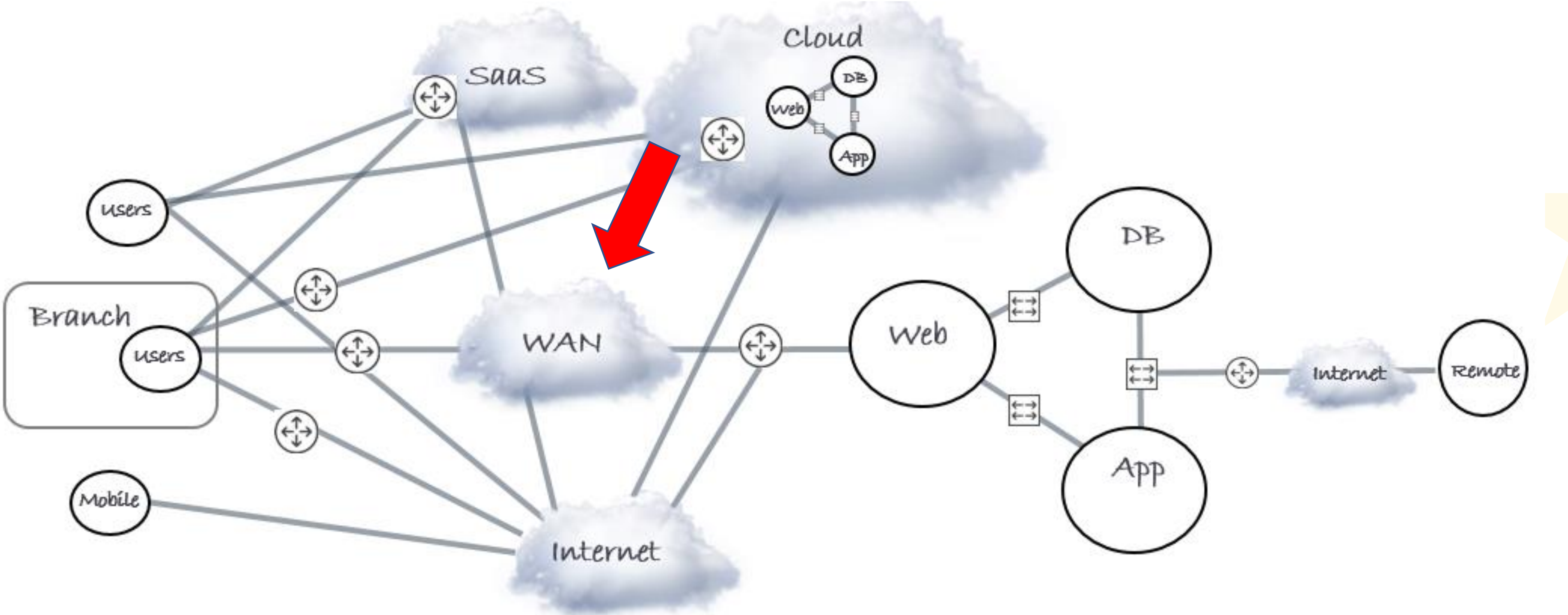
On-Prem Data Center(s)



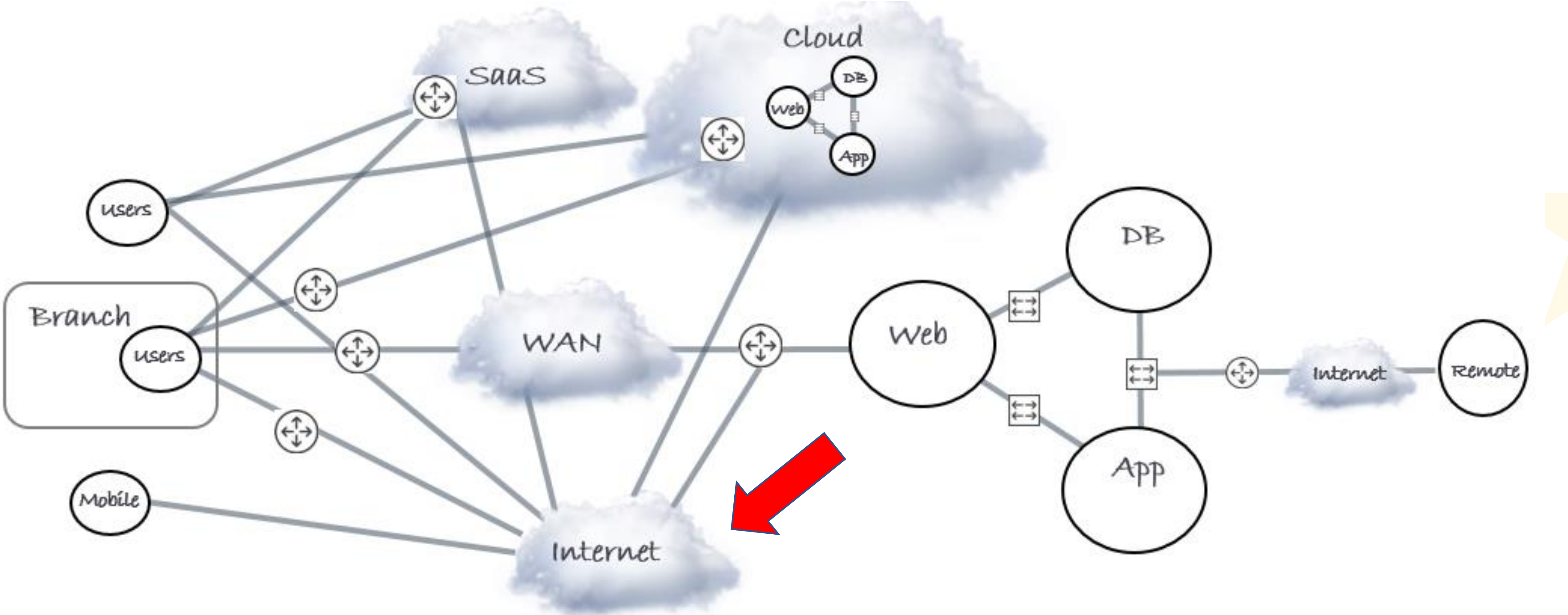
Business Partners



MPLS Provider(s)



Internet Transport(s)



Complex!

- How do we get performance visibility to all of this?

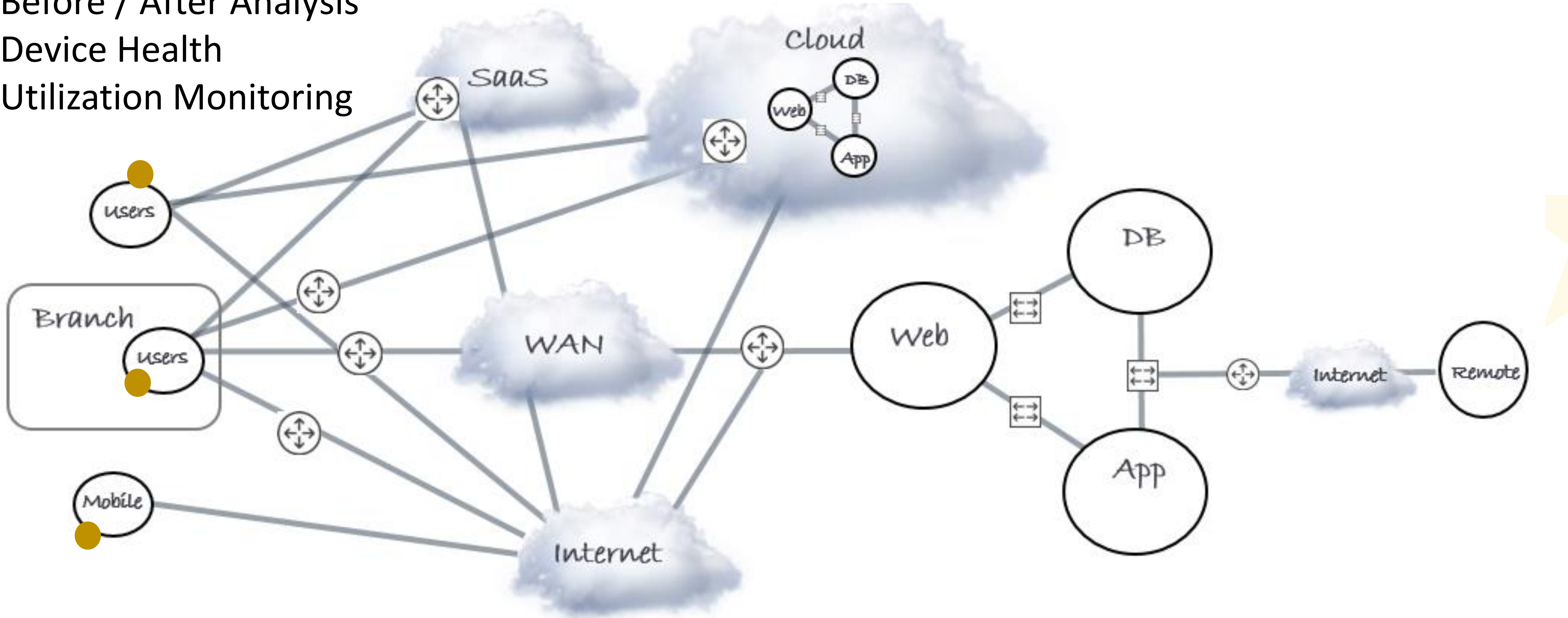
User End Point Device Monitoring

EUE Performance

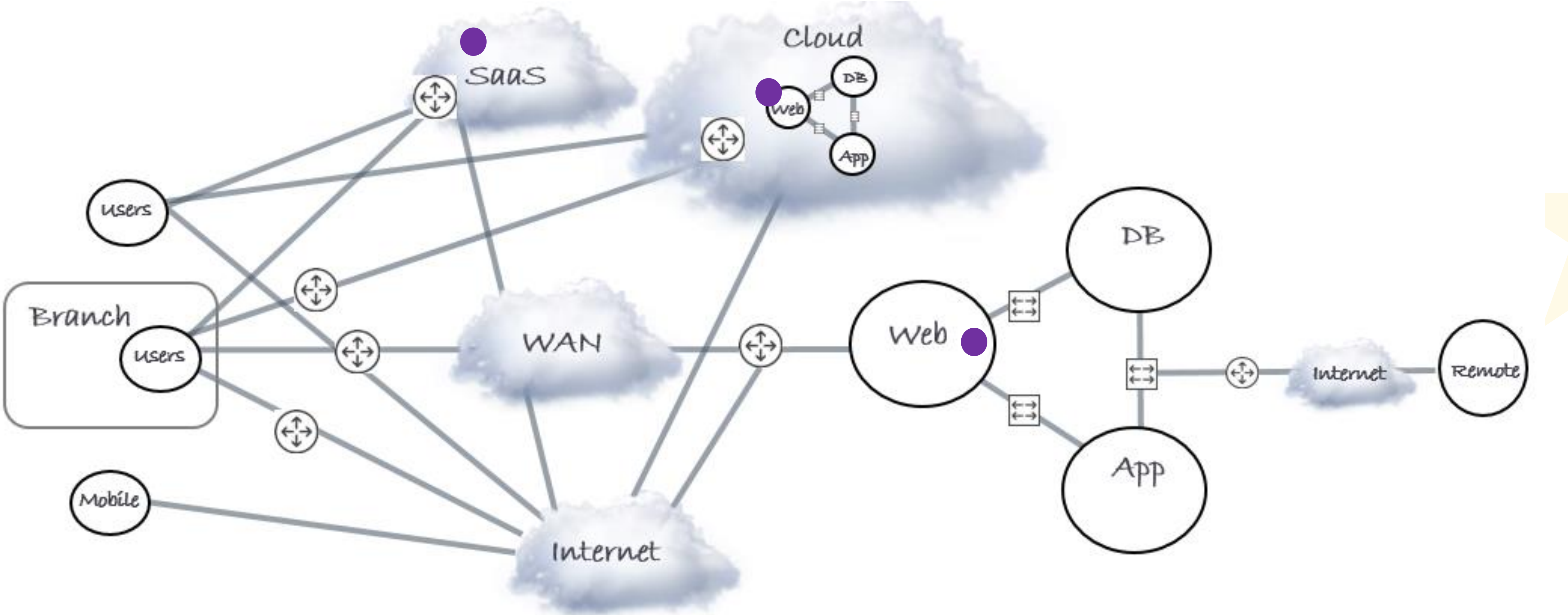
Before / After Analysis

Device Health

Utilization Monitoring

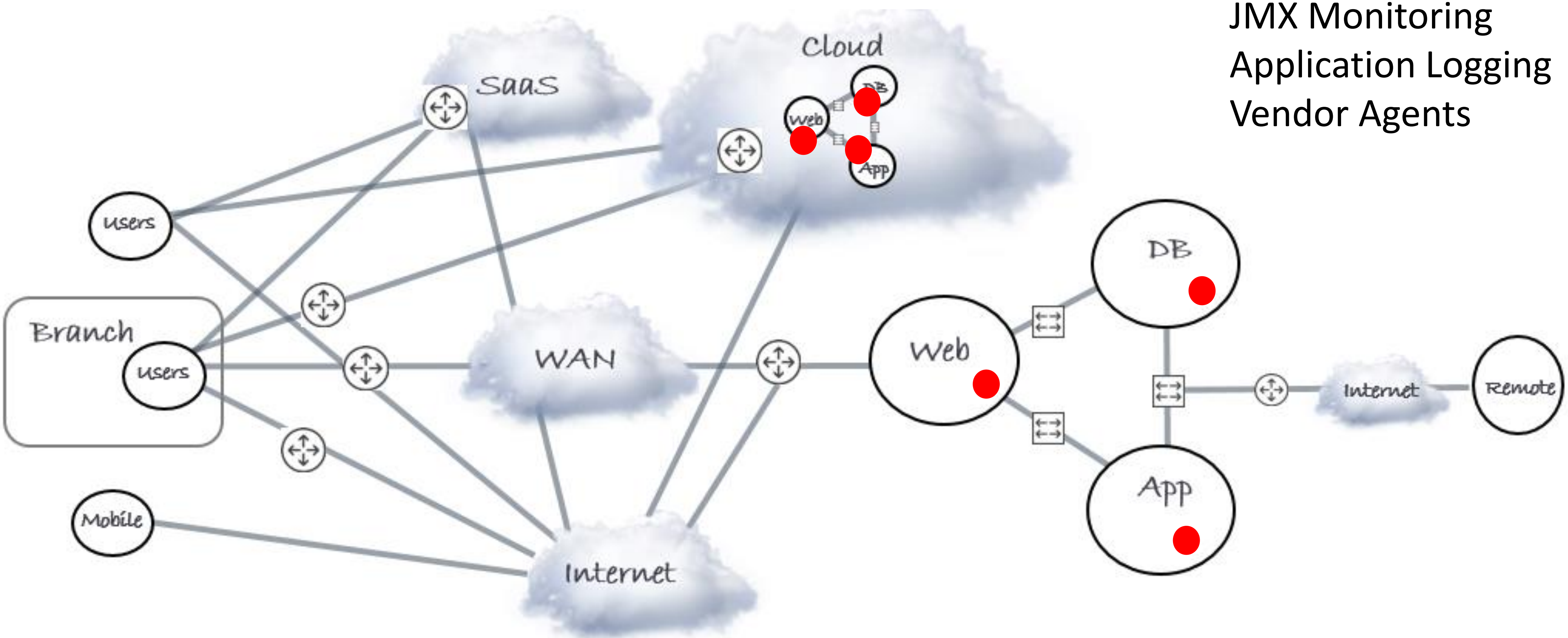


Browser EUE - Javascript Injection



Internal Application Components

Java / .NET Profiling
JMX Monitoring
Application Logging
Vendor Agents

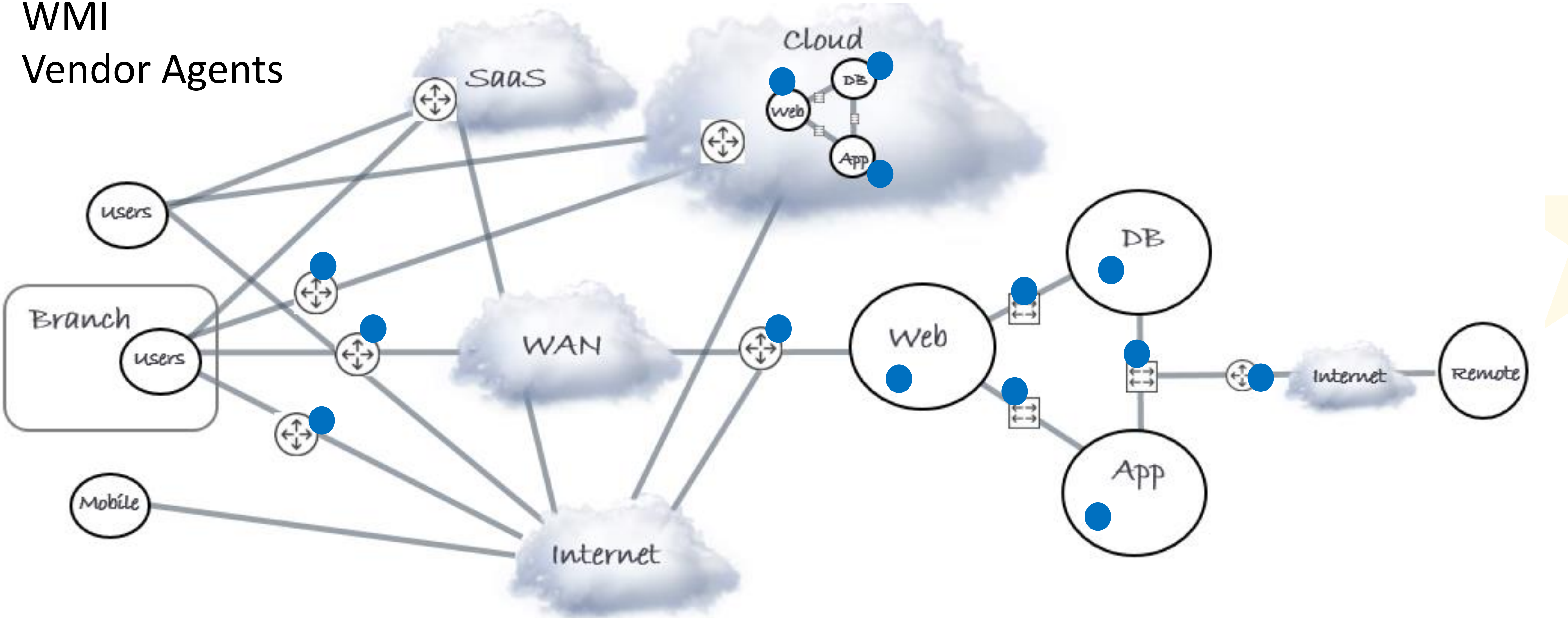


Infrastructure Devices / Servers

SNMP

WMI

Vendor Agents



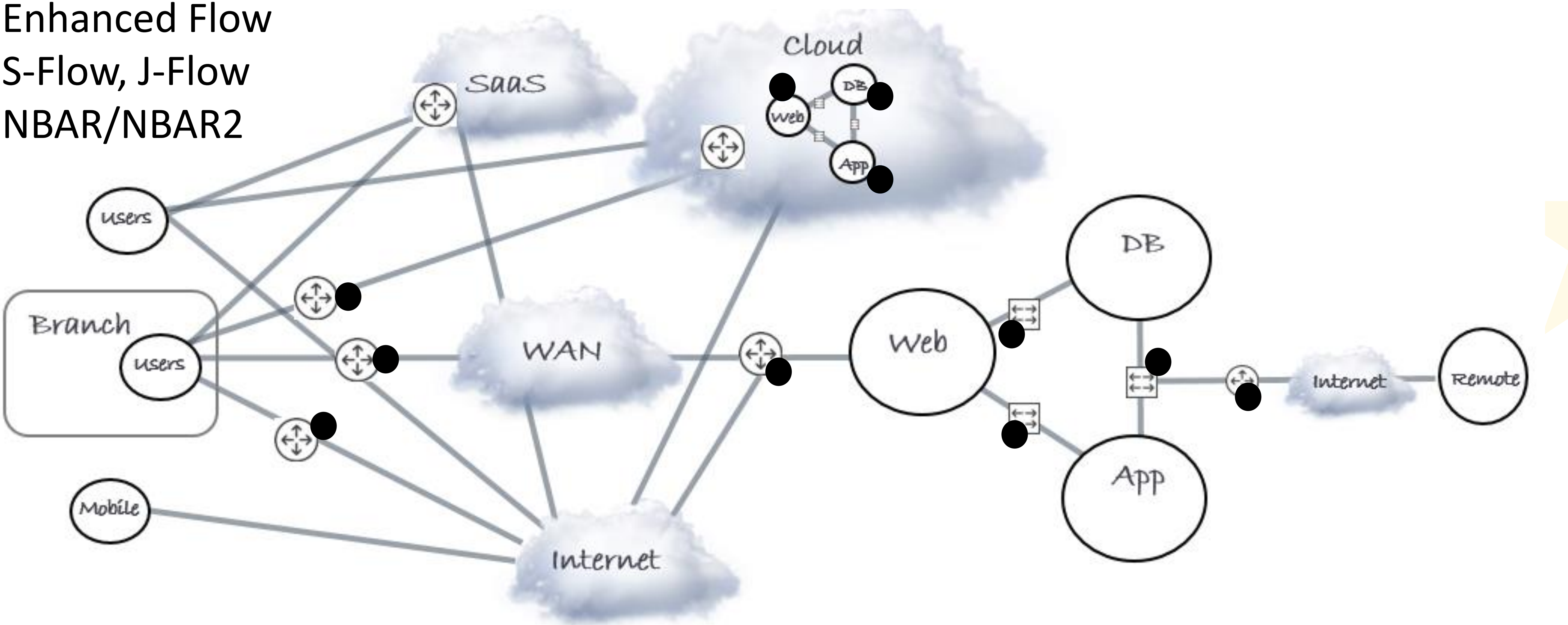
Flow Records

Netflow

Enhanced Flow

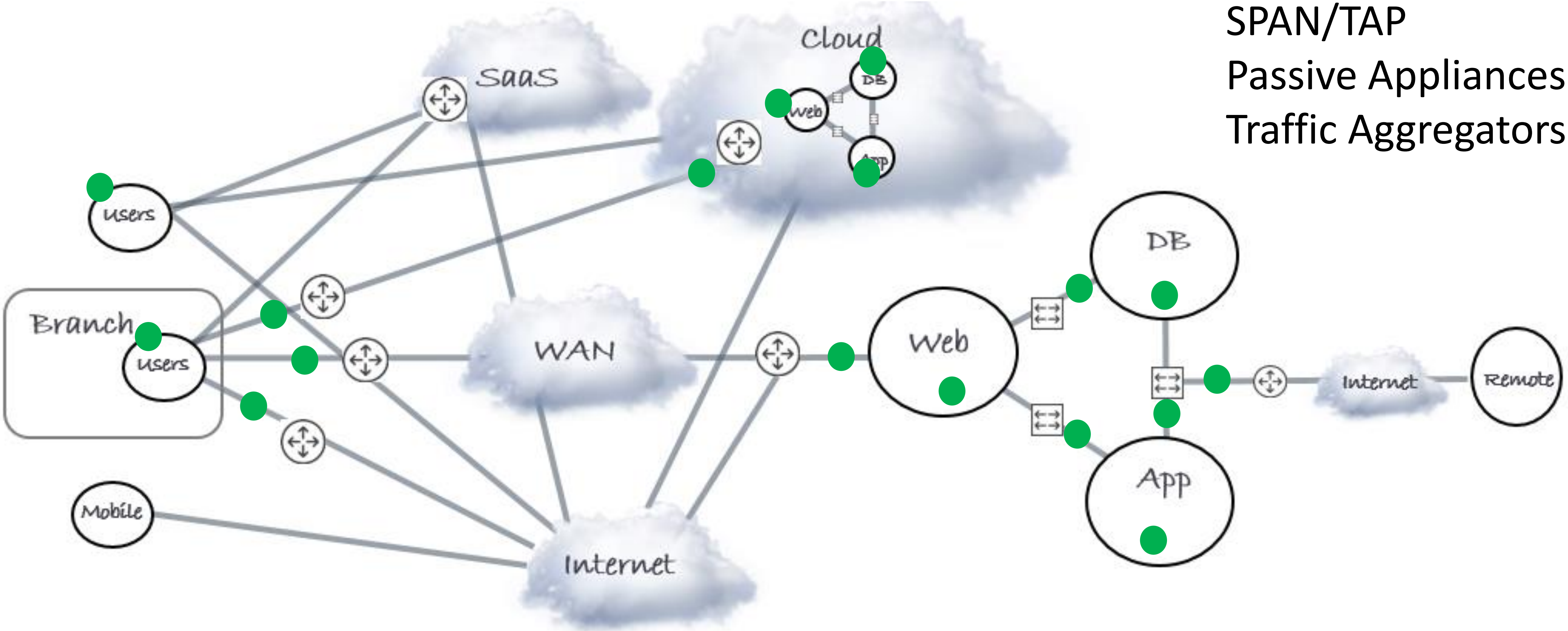
S-Flow, J-Flow

NBAR/NBAR2



Packet Capture / Collection

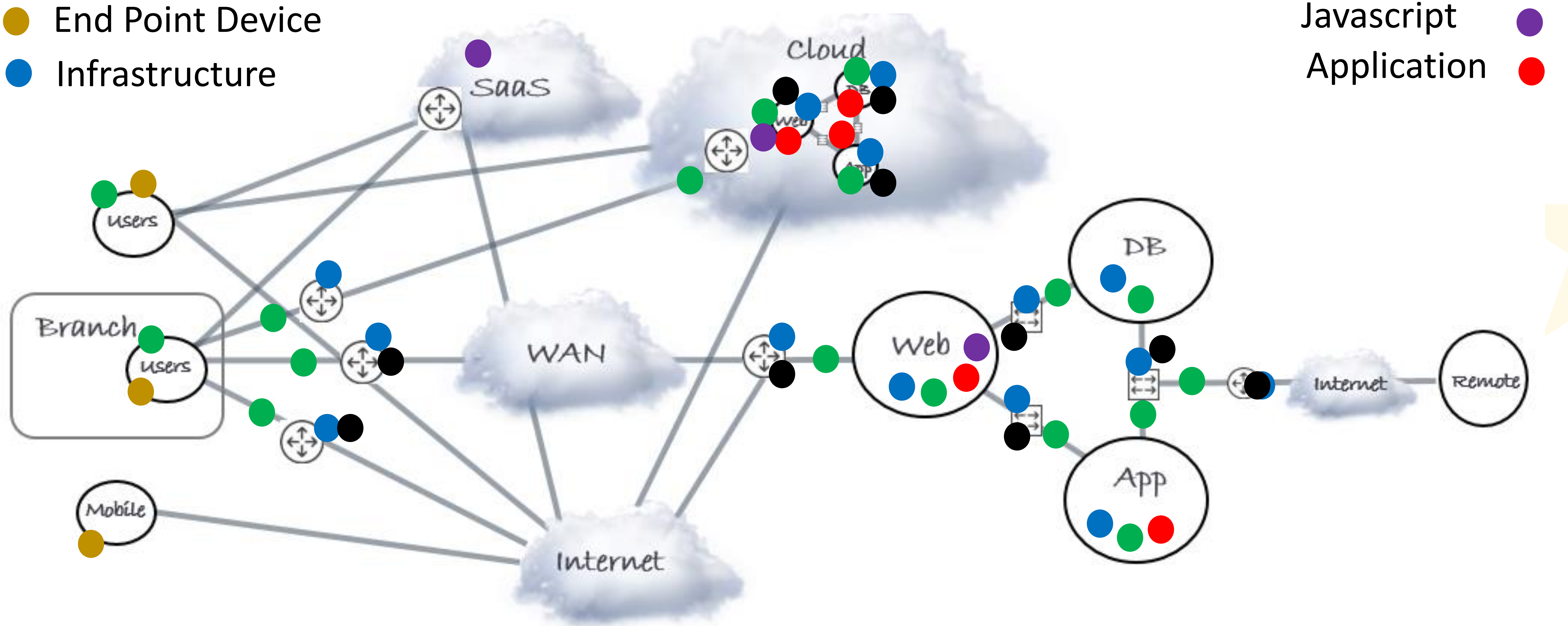
Host Captures
SPAN/TAP
Passive Appliances
Traffic Aggregators



Full End to End Visibility

- ● Packets
- ● End Point Device
- ● Infrastructure

- Flow ●
- Javascript ●
- Application ●



Heard in the War Room…

- Users are complaining!!
- App ABC is slow, what infrastructure does it use?
- Link utilization is 80%, who’s using the bandwidth?
- Server utilization is 85%, who’s generating the load?
- How long has it been going on?
- Management wants hourly status updates
- Who owns the fix?
- My area looks fine, it must be the Network

Heard in the War Room…

- Users are complaining!!
- Chaos is slow, what infrastructure Confusion
- Link utilization is 80%, who's using the bandwidth?
- Server u Unscheduled Overtime load?
- How lo
- Management wants hourly status updates
- Trust Issues ?
- e, it must be the Network Panic

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 ____________?

Heard in the CIO Staff Meeting

- Are we meeting our SLAs?
- A
- Is
  s
- A do we
  k
- What's the impact if we _____________?

How do we make the right investments to support the business today and in the future?

Complex Requirements!

How can we meet these complex requirements?

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

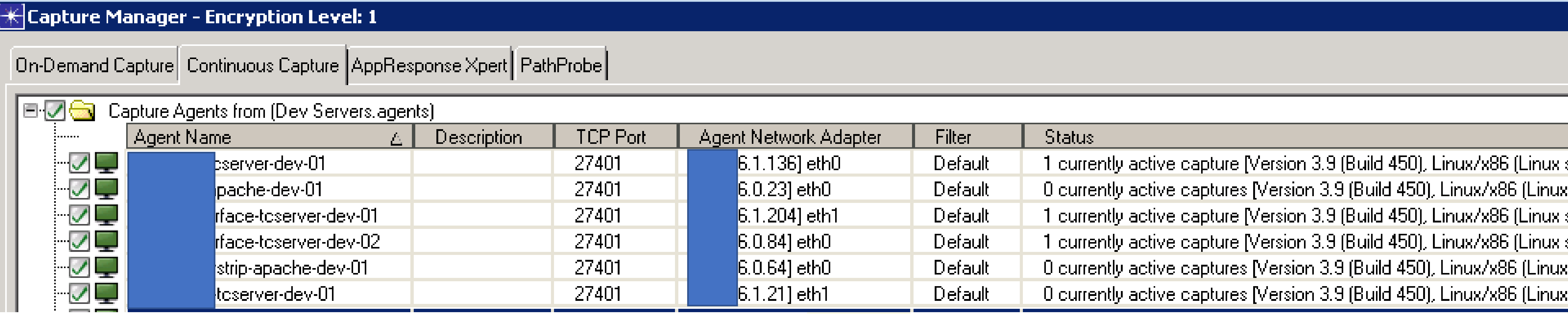
Packet Workflows & Technologies

- Capture
- Performance Monitoring
- Triage and Troubleshooting
- Pre-Release 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

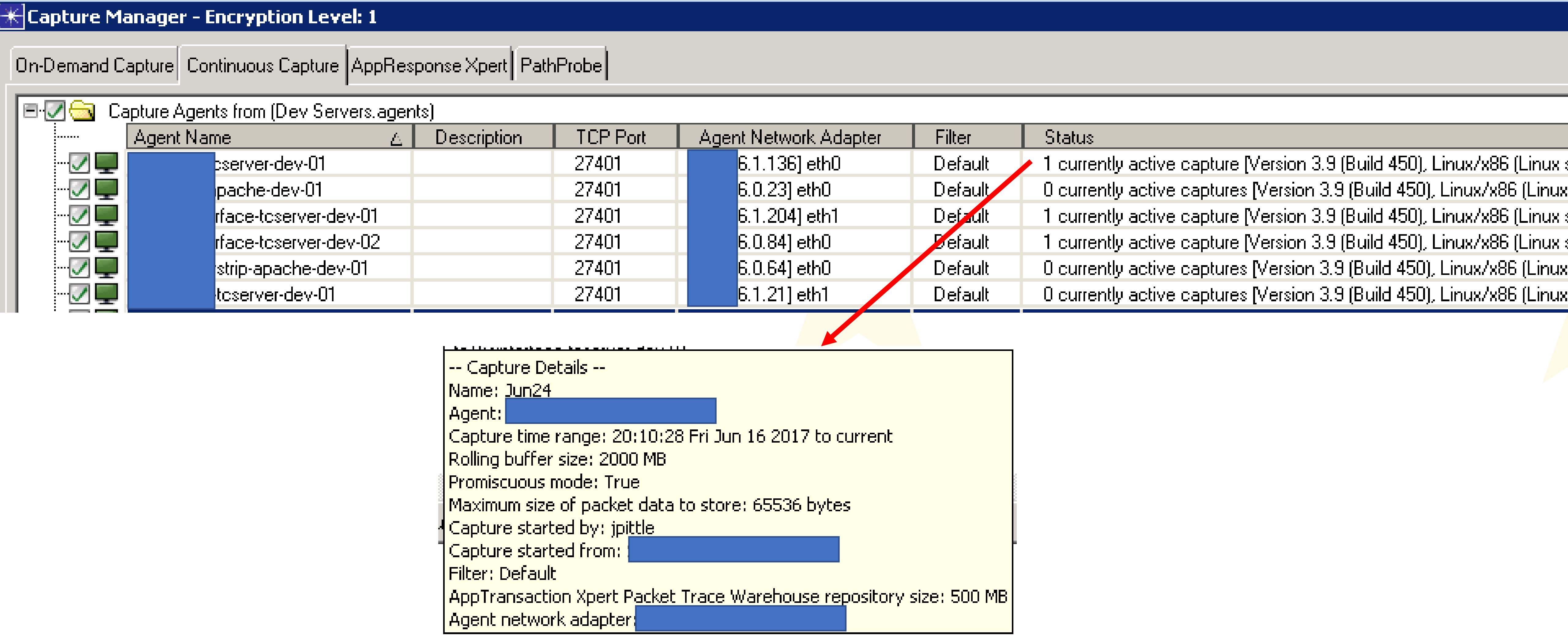


Capture Manager - Encryption Level: 1

☑ Capture Agents from (Dev Servers.agents)

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

Manage Multiple Host Agents



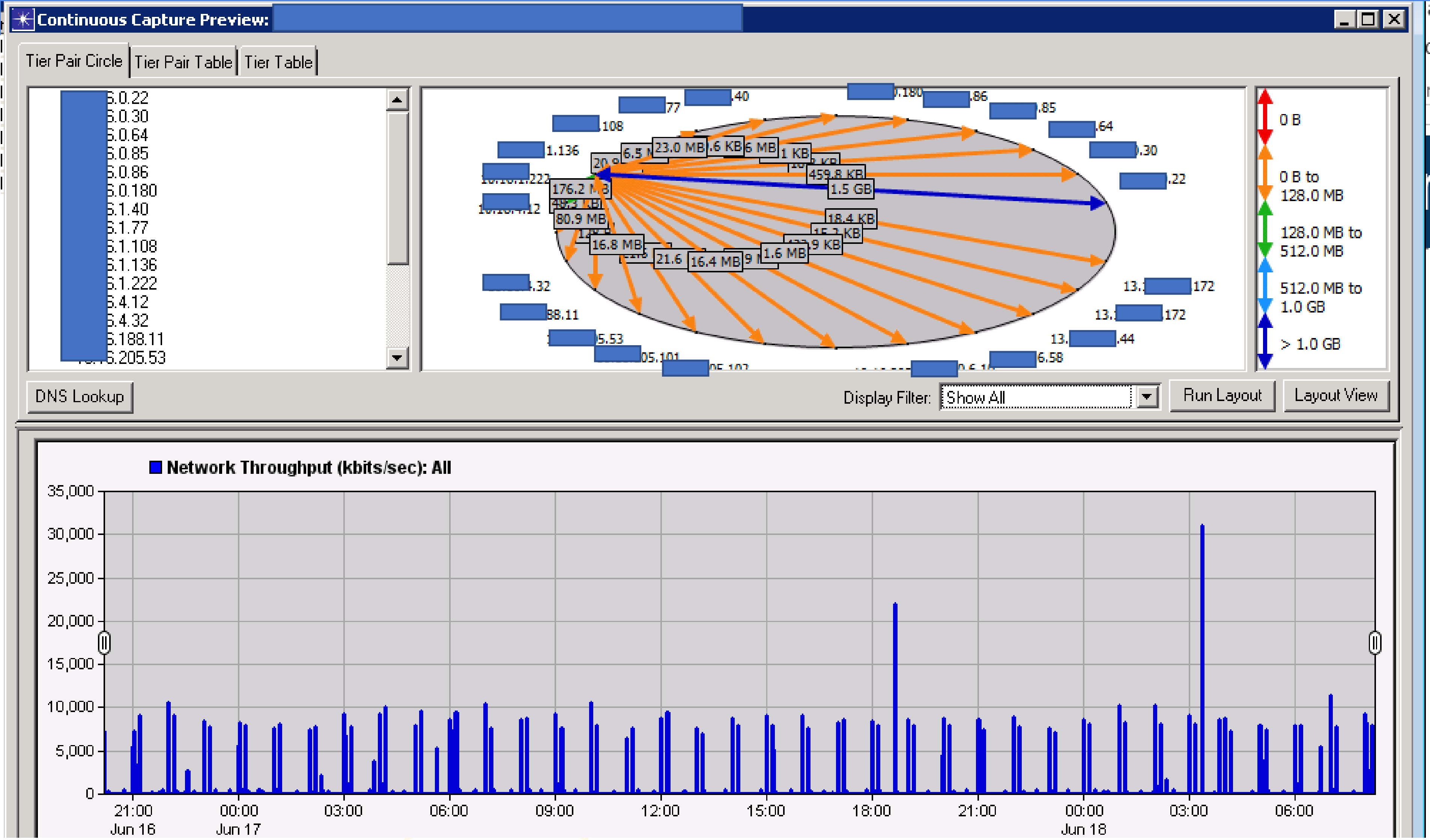
Capture Manager - Encryption Level: 1

☑ Capture Agents from (Dev Servers.agents)

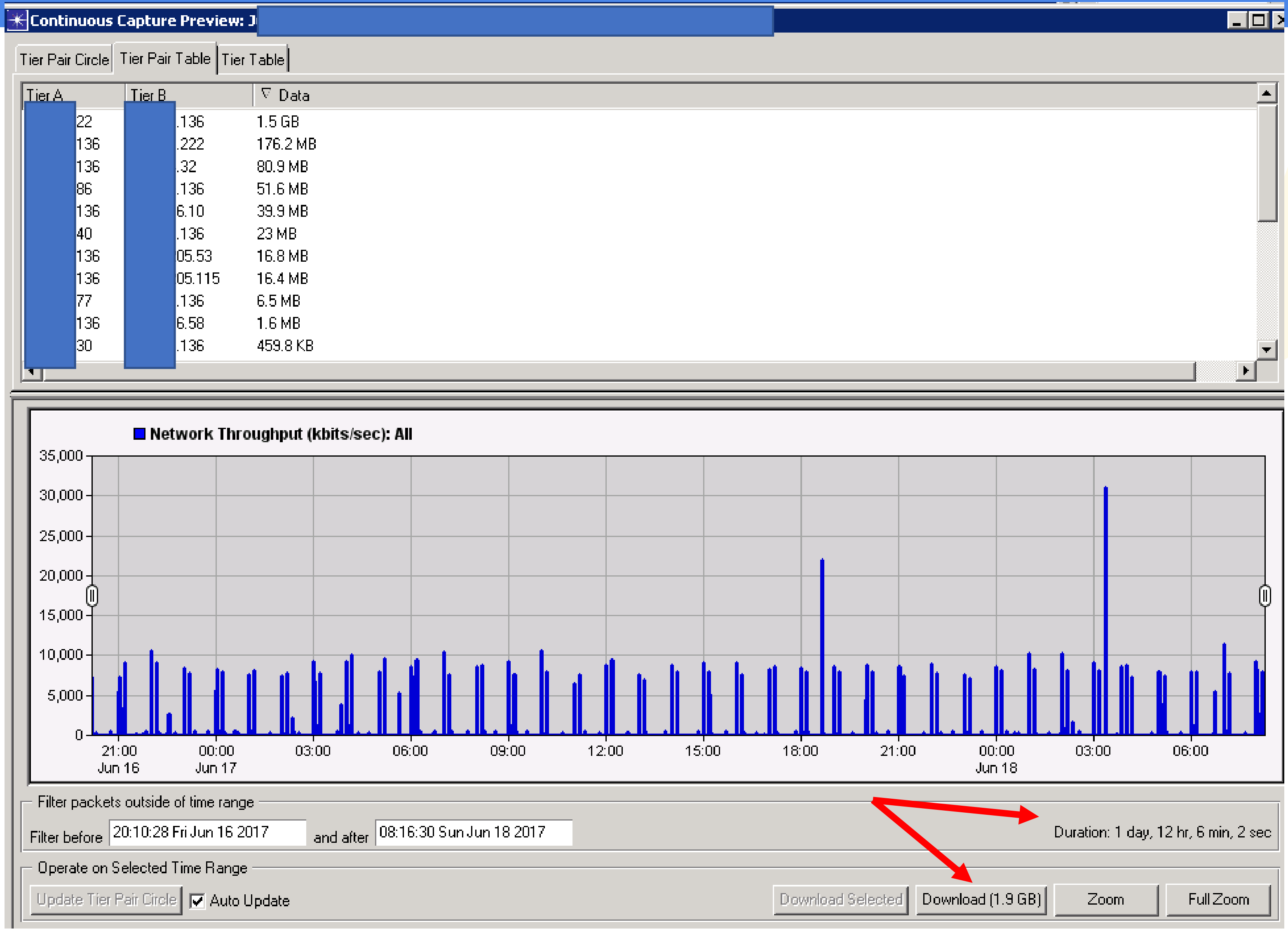
Agent Name	Description	TCP Port	Agent Network Adapter	Filter	Status
☑ [redacted]cserver-dev-01		27401	[redacted]6.1.136] eth0	Default	1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux
☑ [redacted]pache-dev-01		27401	[redacted]6.0.23] eth0	Default	0 currently active captures [Version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



Continuous Capture Preview: J[redacted]

Tier A	Tier B	▽ Data
[redacted]22	[redacted].136	1.5 GB
[redacted]136	[redacted].222	176.2 MB
[redacted]136	[redacted].32	80.9 MB
[redacted]86	[redacted].136	51.6 MB
[redacted]136	[redacted]6.10	39.9 MB
[redacted]40	[redacted].136	23 MB
[redacted]136	[redacted]05.53	16.8 MB
[redacted]136	[redacted]05.115	16.4 MB
[redacted]77	[redacted].136	6.5 MB
[redacted]136	[redacted]6.58	1.6 MB
[redacted]30	[redacted].136	459.8 KB

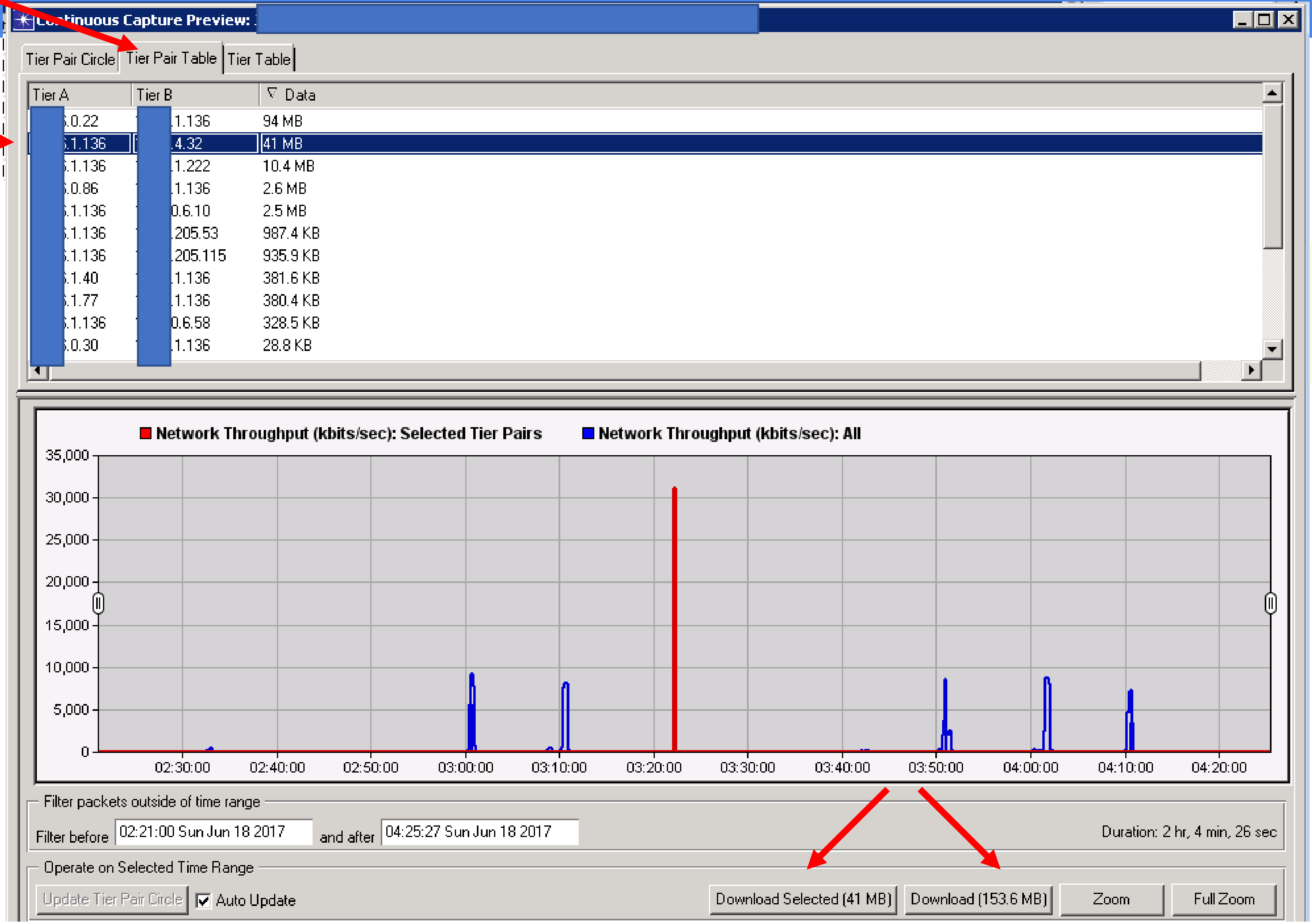
Filter packets outside of time range

Filter before 20:10:28 Fri Jun 16 2017 and after 08:16:30 Sun Jun 18 2017

Duration: 1 day, 12 hr, 6 min, 2 sec

Operate on Selected Time Range

Navigate to most relevant traffic before download



Continuous Capture Preview: [redacted]

Tier A	Tier B	Data
[redacted].0.22	[redacted]1.136	94 MB
[redacted].1.136	[redacted]4.32	41 MB
[redacted].1.136	[redacted]1.222	10.4 MB
[redacted].0.86	[redacted]1.136	2.6 MB
[redacted].1.136	[redacted]0.6.10	2.5 MB
[redacted].1.136	[redacted].205.53	987.4 KB
[redacted].1.136	[redacted].205.115	935.9 KB
[redacted].1.40	[redacted]1.136	381.6 KB
[redacted].1.77	[redacted]1.136	380.4 KB
[redacted].1.136	[redacted]0.6.58	328.5 KB
[redacted].0.30	[redacted]1.136	28.8 KB

Filter packets outside of time range

Filter before 02:21:00 Sun Jun 18 2017 and after 04:25:27 Sun Jun 18 2017

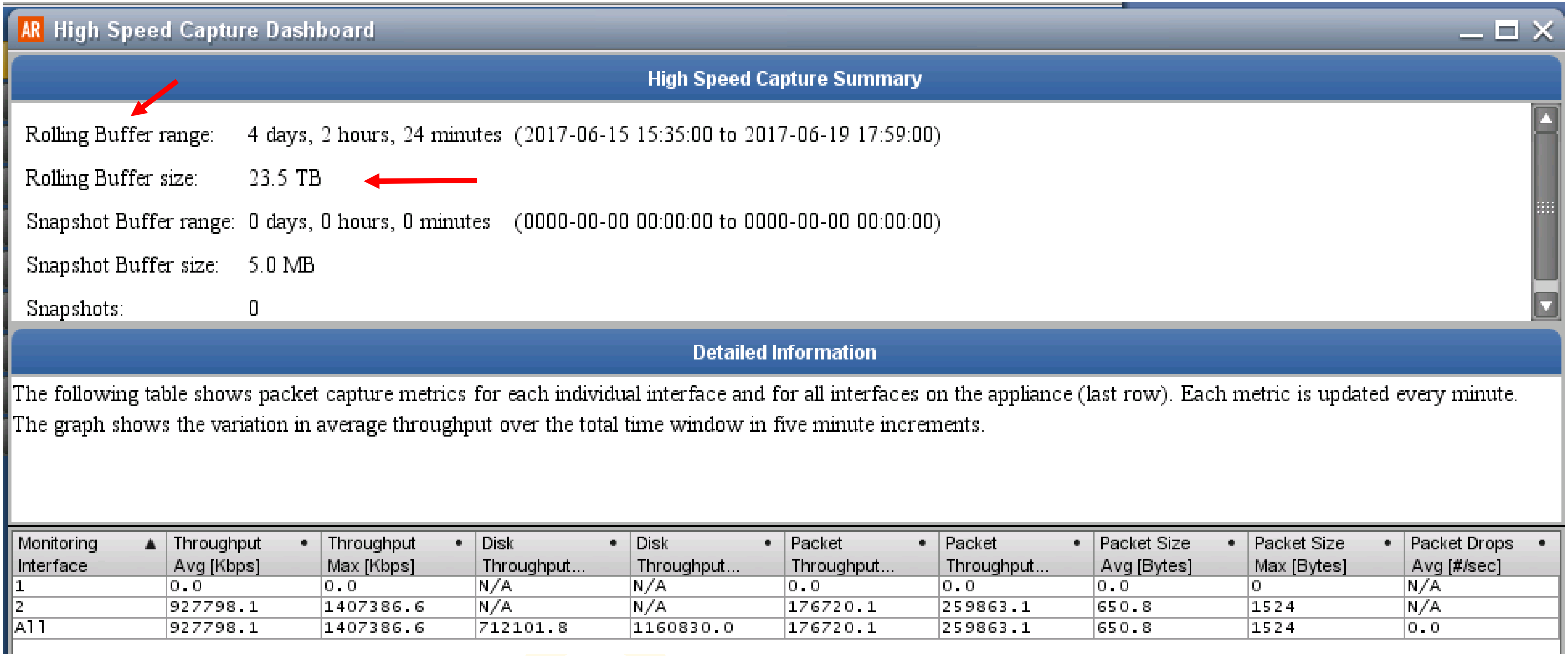
Duration: 2 hr, 4 min, 26 sec

Operate on Selected Time Range

Passive Appliances - Capture

- Always on…
- All packets, all the time, based on the traffic presented
- Capture packets into very large, indexed repository
- Packet Slicing and Filtering
- Preview and filter relevant conversations before downloading for analysis

Passive Appliance - Continuous Capture



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, Aggregating, Splitting
- Header / Layer modifications
- Time Stamps
- Packet De-duplication
- Flow generation
- Highly Scalable

Questions / Comments

Monitoring - Passive Appliances

- Always on, always analyzing app and network performance
- All conversations, all the time, based on the traffic presented
- Transaction level monitoring (Web, SOAP, SQL, etc.)
- TCP Level monitoring (Request / Response, Retrans, Congestion, In-flight, Windowing)
- Proactive alerting
- Baselining and historical trends
- Quickly determine problem domain; download relevant packets ***only when*** deeper dive is needed

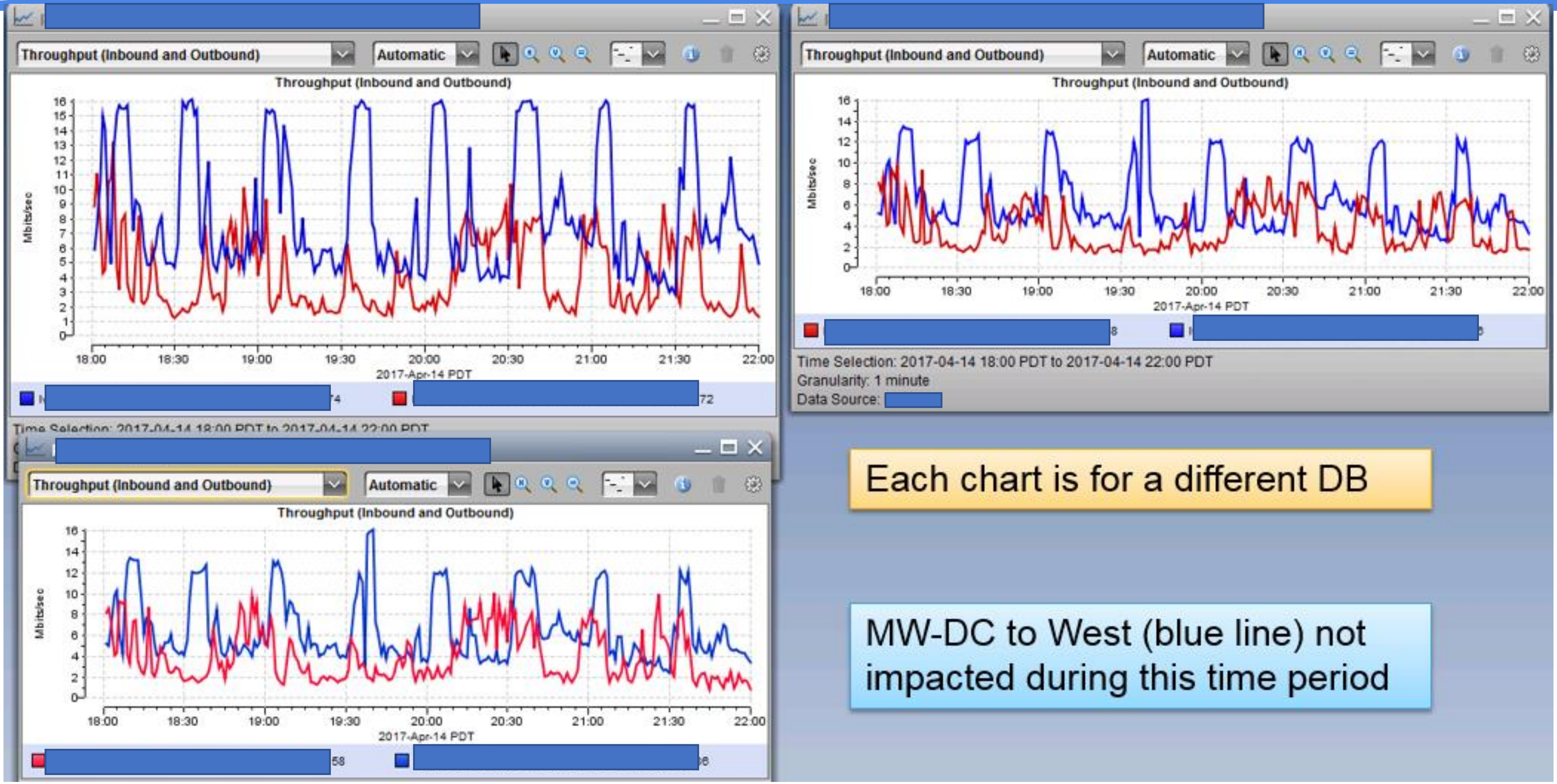
Triage & Troubleshooting

- Filter and isolate transactions of interest
- Utilize Automated Expert Analysis
- Overlay traffic with key performance statistics for visual correlation
- End to End Transaction views from multiple capture points
- Analyze performance indicators including protocol effects

Example: DB Cloud Replication

- DB instances in AWS East and AWS West
- Full mesh replication between AWS instances, and mirror instances in customer DC-1 / DC-2
- Replication delays between AWS East and DC-2
- DB used the technical term ‘LAG’
- Impact: Customer closes their data entry session; returns a few minutes later and is unable to see the latest updates (due to the LAG)

Real Time Views - Sample



[redacted]

🟦 [redacted] 🟥 [redacted]

Time Selection: 2017-04-14 18:00 PDT to 2017-04-14 22:00 PDT

[redacted]

🟥 [redacted] 🟦 [redacted]

Time Selection: 2017-04-14 18:00 PDT to 2017-04-14 22:00 PDT

Granularity: 1 minute

Data Source: [redacted]

[redacted]

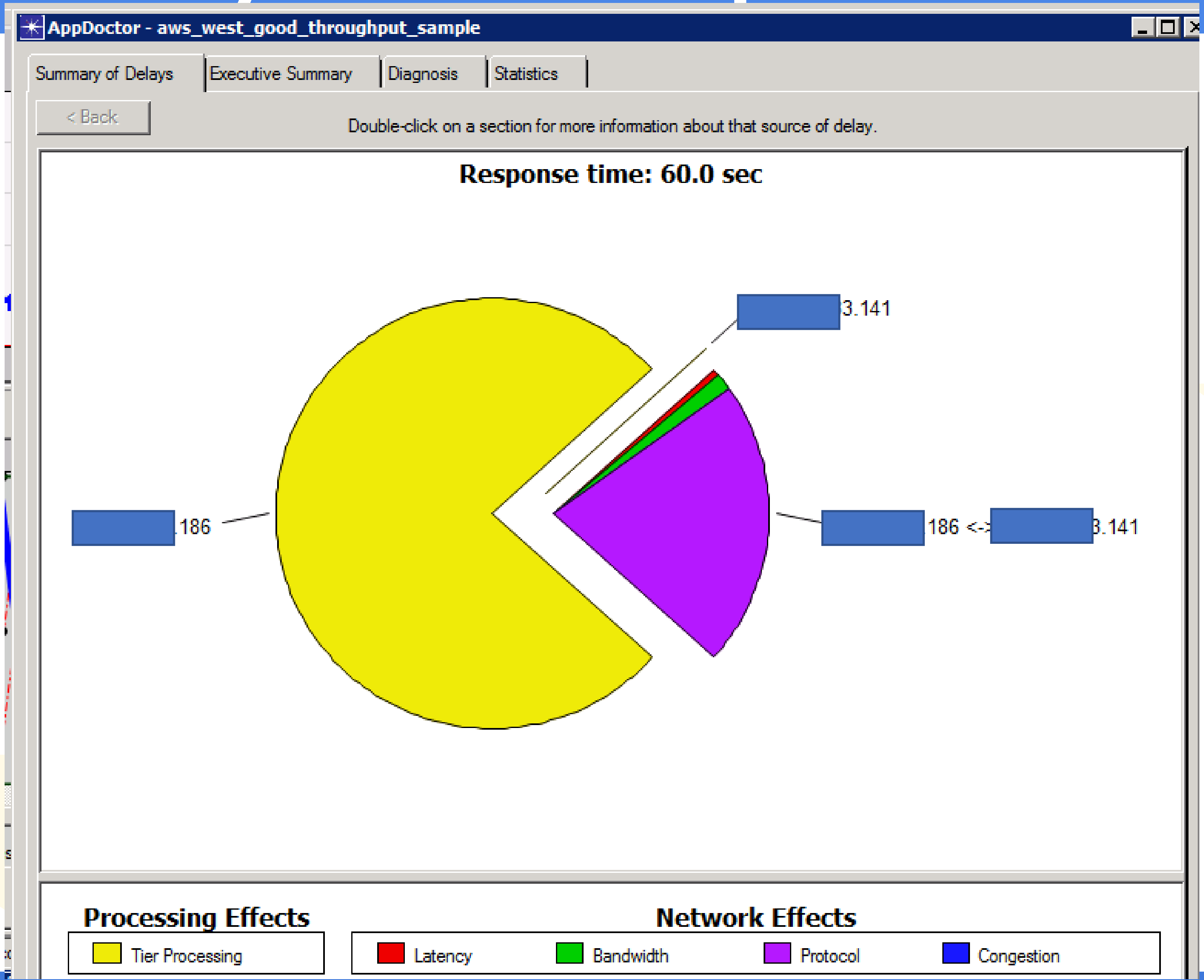
🟥 [redacted] 🟦 [redacted]

Each chart is for a different DB

MW-DC to West (blue line) not impacted during this time period

Expert Analysis Sample

- Download a 1 minute packet sample
- Chosen from appliance based on low throughput period
- Automated Summary of Delays Analysis



AppDoctor - aws_west_good_throughput_sample

Double-click on a section for more information about that source of delay.

Response time: 60.0 sec

Processing Effects

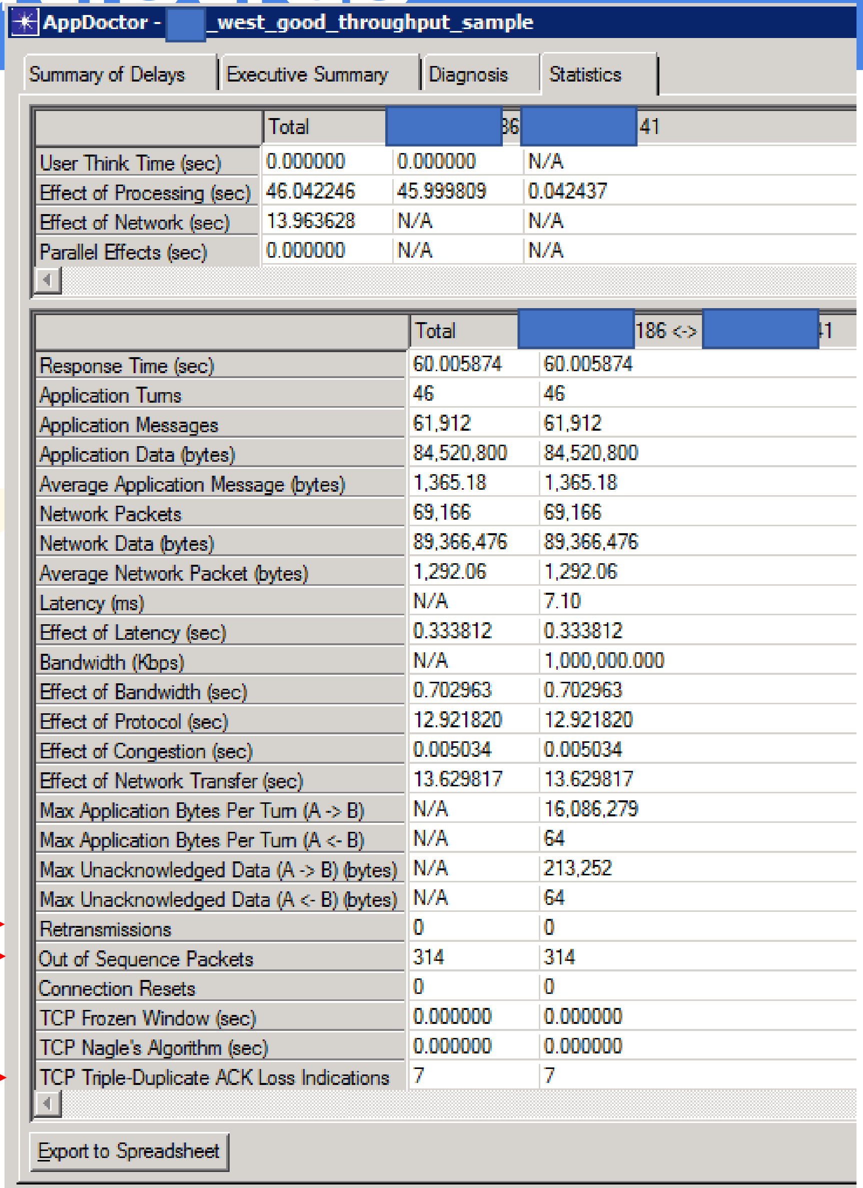
🟨 Tier Processing

Network Effects

🟥 Latency 🟩 Bandwidth 🟪 Protocol 🟦 Congestion

Summary Statistics

- 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



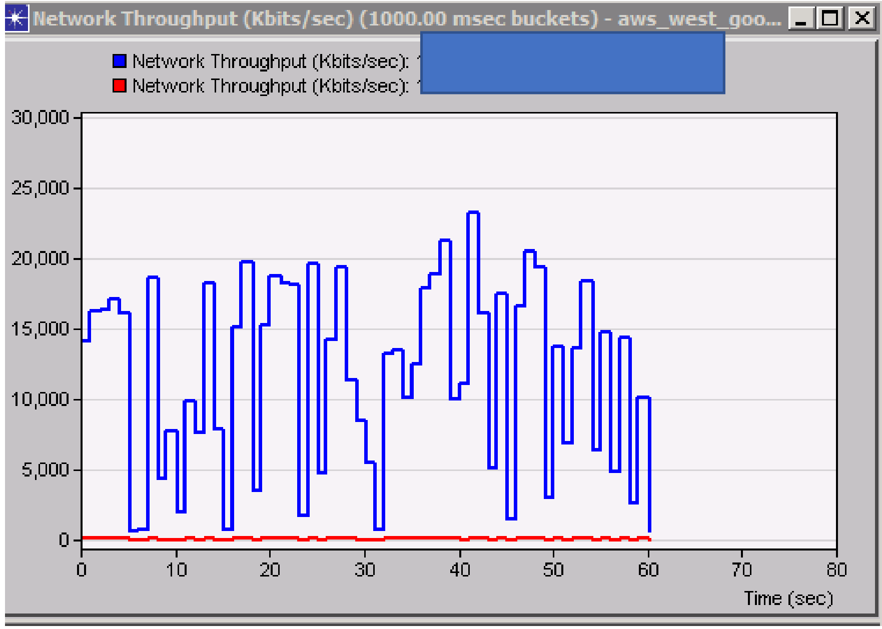
AppDoctor - [redacted] _west_good_throughput_sample

	Total	[redacted] 36	[redacted] 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	[redacted] 186 <-> [redacted] 41
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

Relevant Statistics

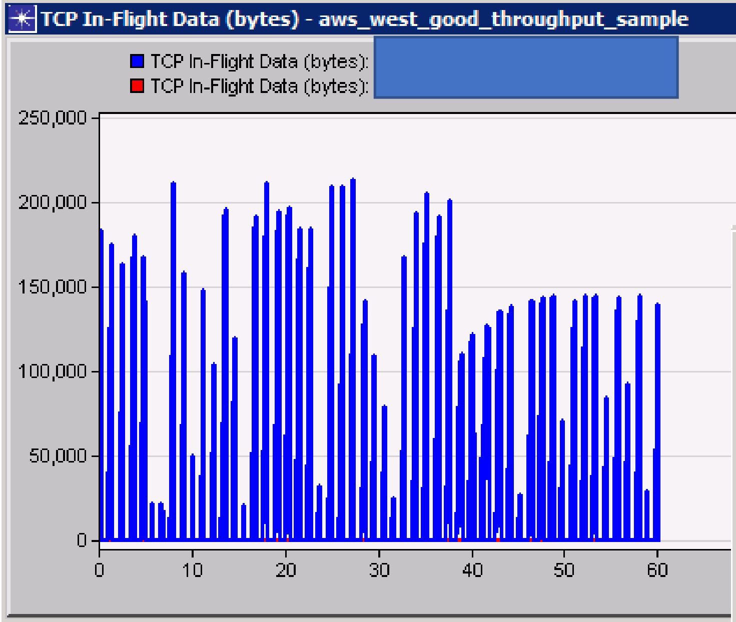
Throughput



Network Throughput (Kbits/sec) (1000.00 msec buckets) - aws_west_goo...

🟦 Network Throughput (Kbits/sec): [redacted]
🟥 Network Throughput (Kbits/sec): [redacted]

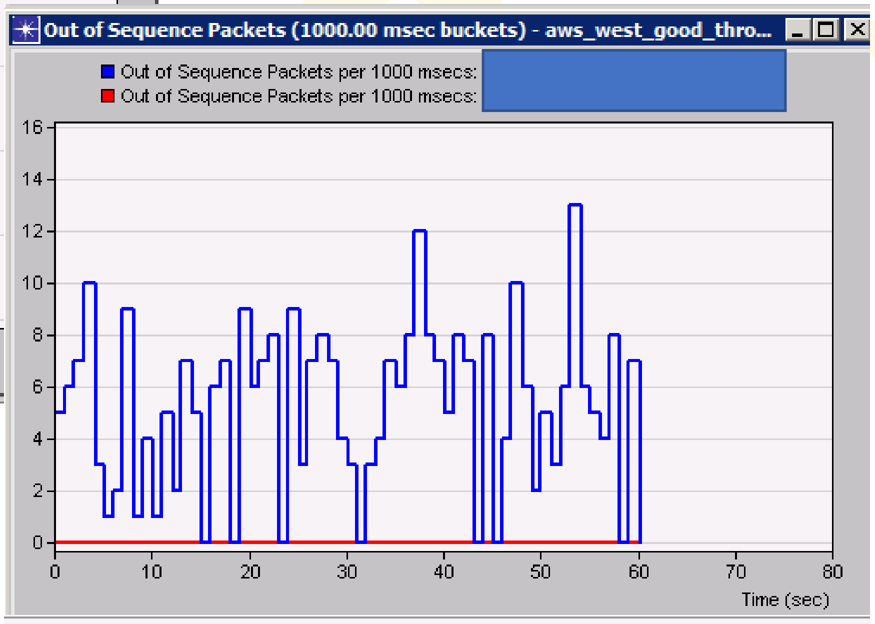
Bytes in Flight



TCP In-Flight Data (bytes) - aws_west_good_throughput_sample

🟦 TCP In-Flight Data (bytes): [redacted]
🟥 TCP In-Flight Data (bytes): [redacted]

Out of Sequence

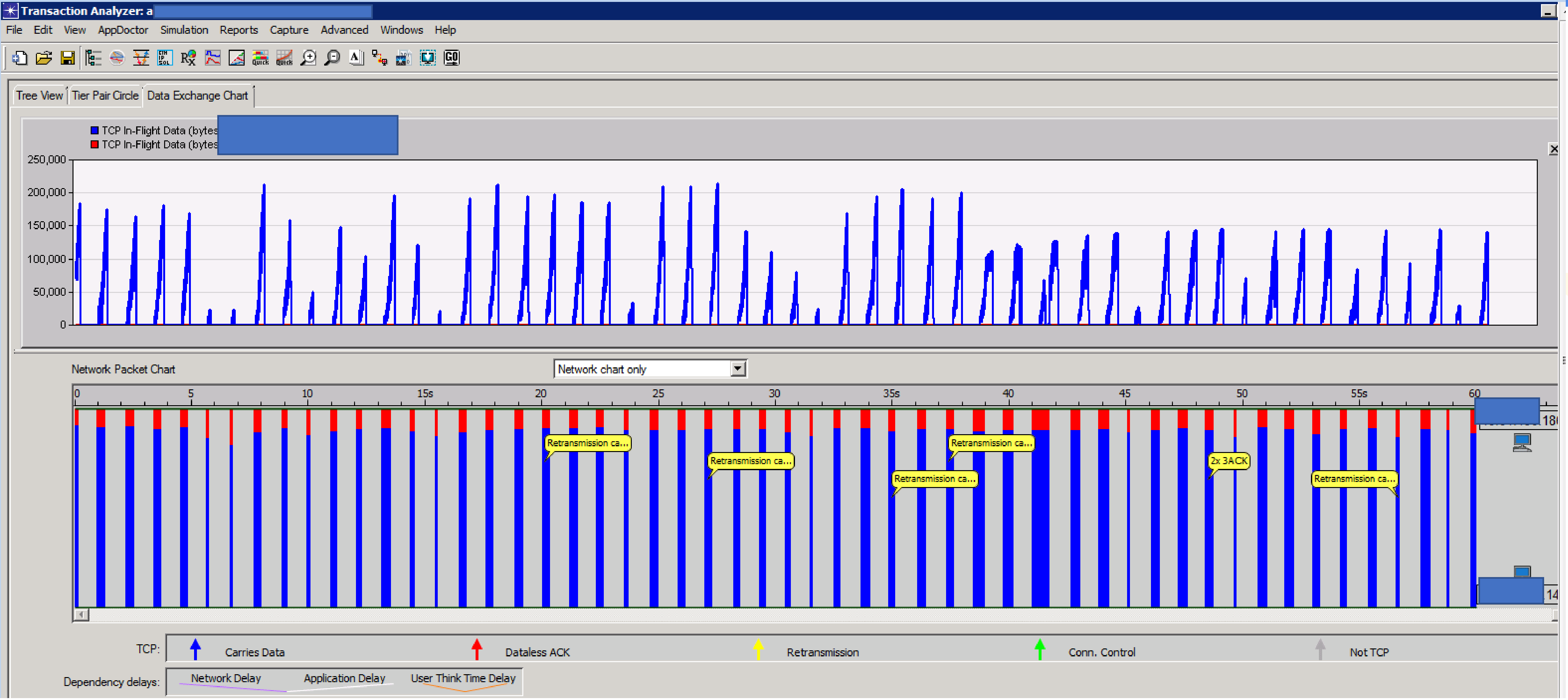


Out of Sequence Packets (1000.00 msec buckets) - aws_west_good_thro...

🟦 Out of Sequence Packets per 1000 msecs: [redacted]
🟥 Out of Sequence Packets per 1000 msecs: [redacted]

Microbursts of 18-23Mbps

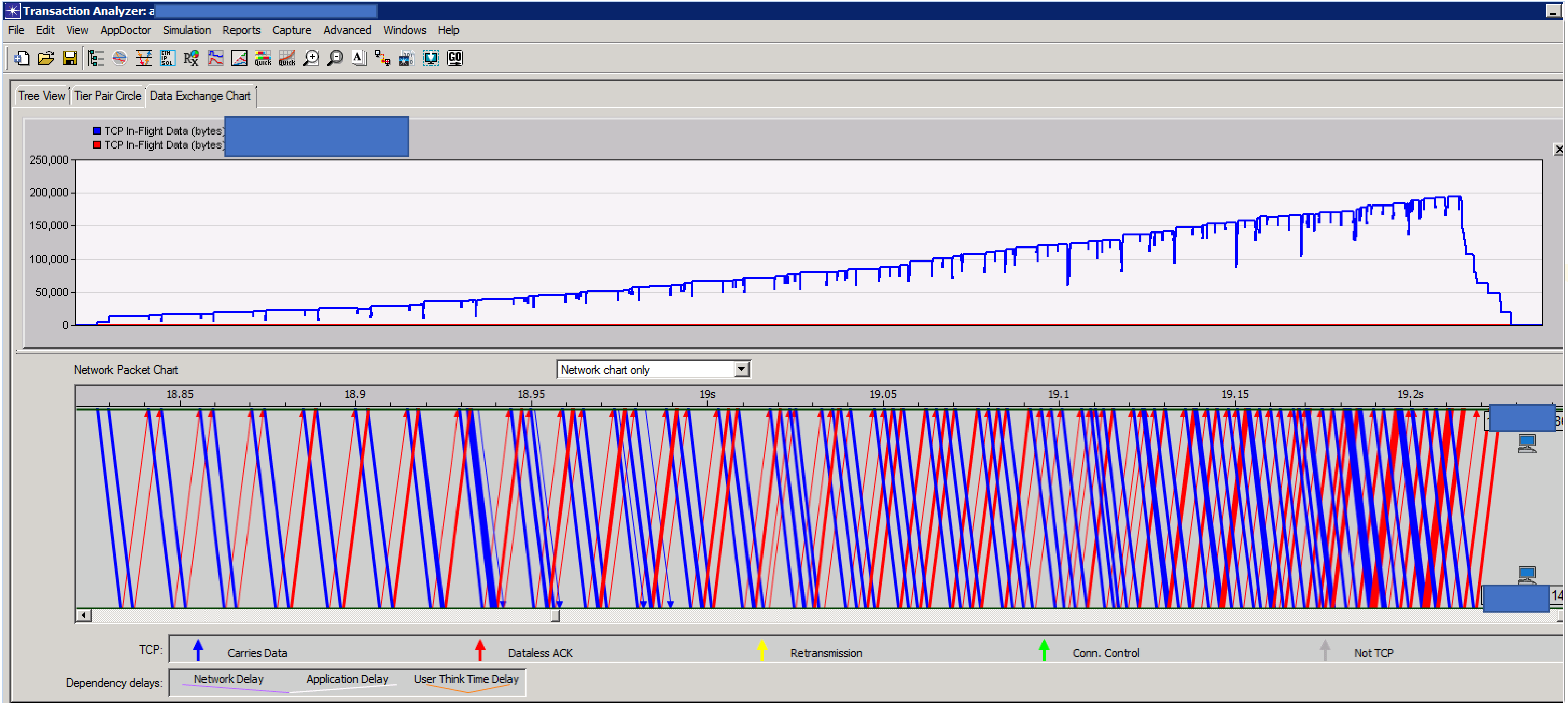
Packet Transfers vs. Bytes in Flight



Discussion

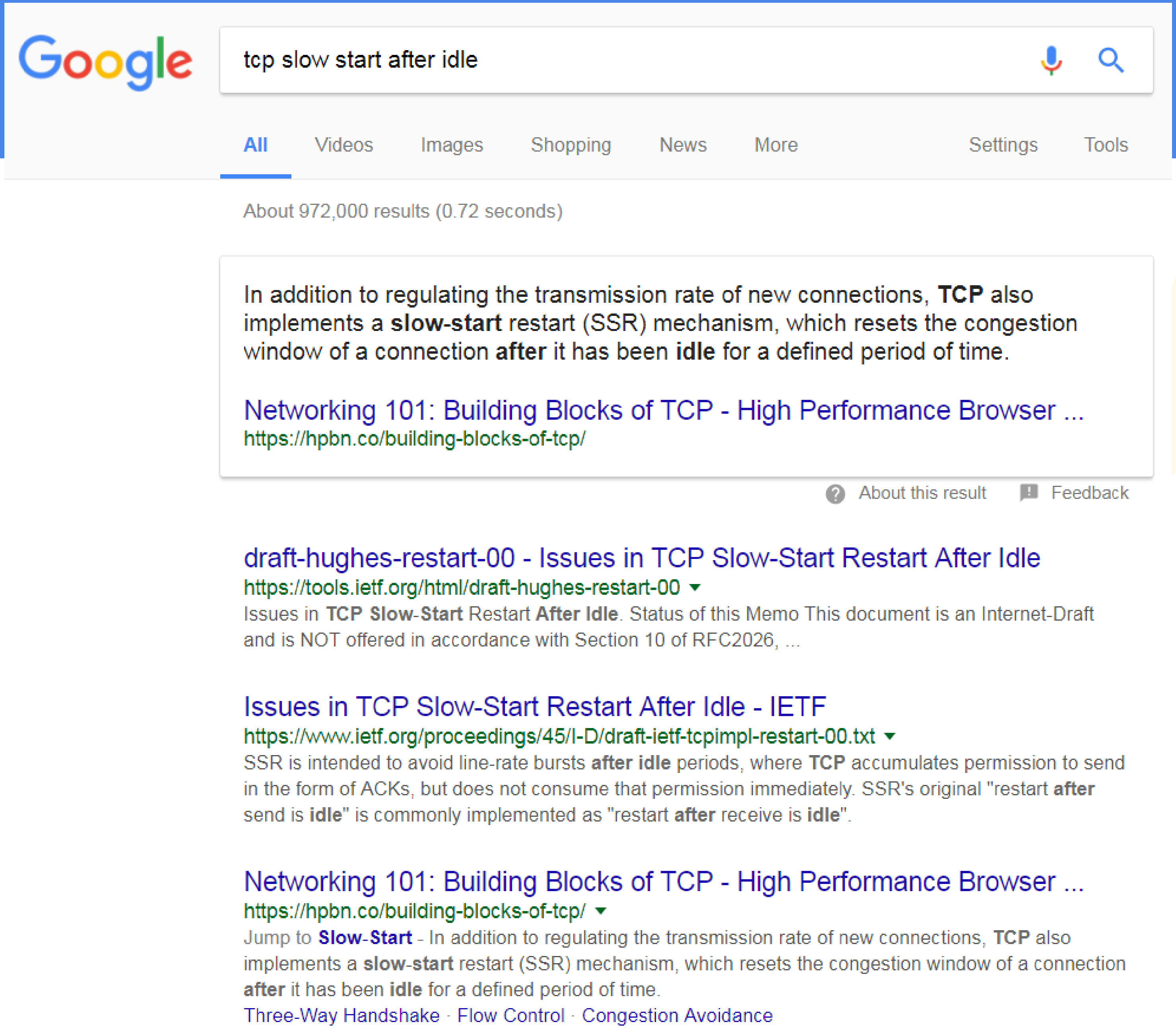
- What looks like continuous transfer on the appliance summary view, is actually short duration bursts of transmissions
- In 1 minute packet capture we can see dozens of start / stop packet exchange activity
- The top chart – “bytes in-flight” shows spikes and dips that correlate with the packet exchange activity
- Let’s drill down into one of the bursts of packet activity next…

399ms burst drill down - 2.2 MB



Discussion

- Deep dive into a 399ms burst
- Moved 2.2 MB of payload during this burst
- Top chart of bytes in flight looks a lot like TCP slow-start is playing a role
- Drill into other bursts show the exact same TCP slow-start behavior
- Not good for throughput…
- Linux admin reviewed and commented “hmm, looks like slow start on idle” is the default for these servers



About 972,000 results (0.72 seconds)

In addition to regulating the transmission rate of new connections, **TCP** also implements a **slow-start** restart (SSR) mechanism, which resets the congestion window of a connection **after** it has been **idle** for a defined period of time.

Networking 101: Building Blocks of TCP - High Performance Browser ...
https://hpbn.co/building-blocks-of-tcp/

draft-hughes-restart-00 - Issues in TCP Slow-Start Restart After Idle
https://tools.ietf.org/html/draft-hughes-restart-00
Issues in **TCP Slow-Start** Restart **After Idle**. Status of this Memo This document is an Internet-Draft and is NOT offered in accordance with Section 10 of RFC2026, ...

Issues in TCP Slow-Start Restart After Idle - IETF
https://www.ietf.org/proceedings/45/I-D/draft-ietf-tcpimpl-restart-00.txt
SSR is intended to avoid line-rate bursts **after idle** periods, where **TCP** accumulates permission to send in the form of ACKs, but does not consume that permission immediately. SSR's original "restart **after** send is **idle**" is commonly implemented as "restart **after** receive is **idle**".

Networking 101: Building Blocks of TCP - High Performance Browser ...
https://hpbn.co/building-blocks-of-tcp/
Jump to **Slow-Start** - In addition to regulating the transmission rate of new connections, **TCP** also implements a **slow-start** restart (SSR) mechanism, which resets the congestion window of a connection **after** it has been **idle** for a defined period of time.
Three-Way Handshake · Flow Control · Congestion Avoidance

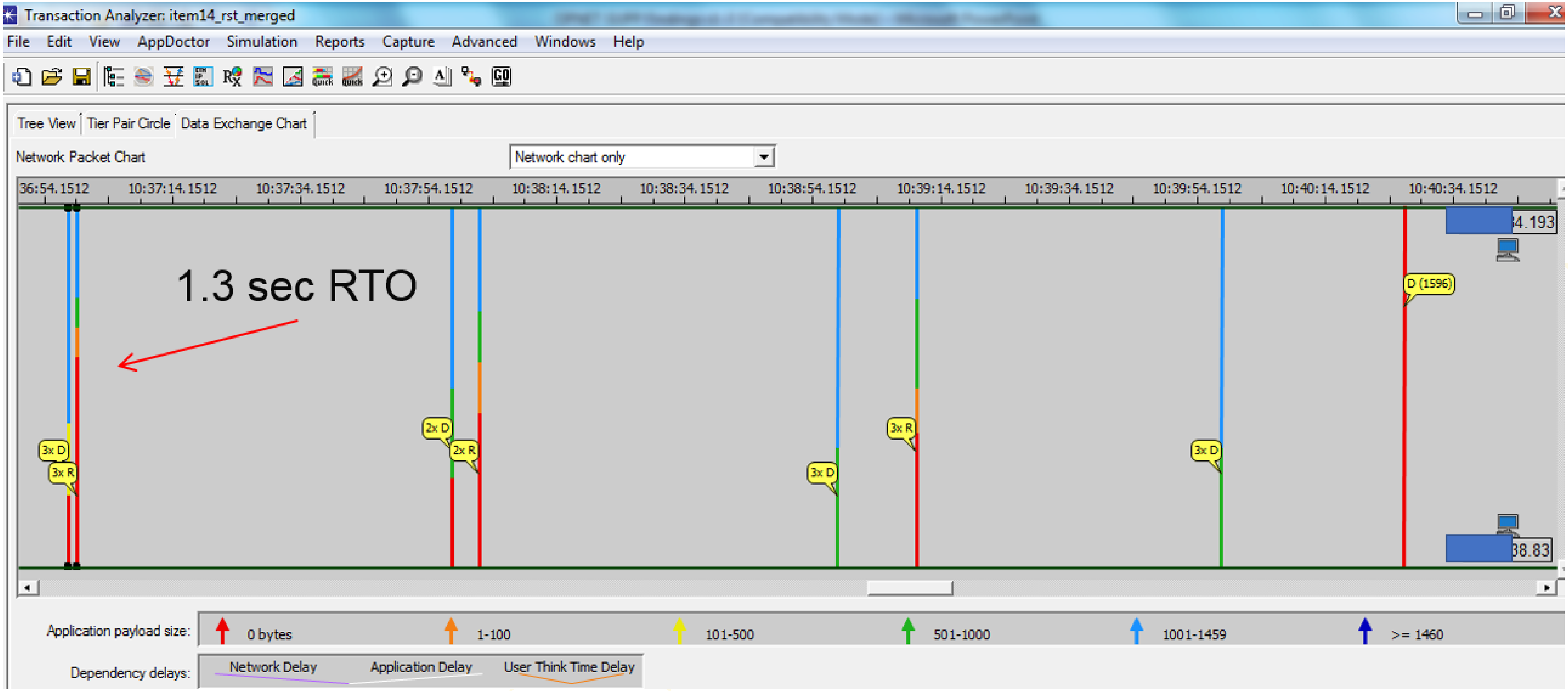
Questions / Comments

- Automated expert analysis can be a huge time saver when troubleshooting!
- Diagnosed TCP Slow Start on Idle without looking at decodes
- Packets don't Lie…., and pictures you paint with packets tell the true story
- One more quick sample of expert analysis visualization before we move on….

Background

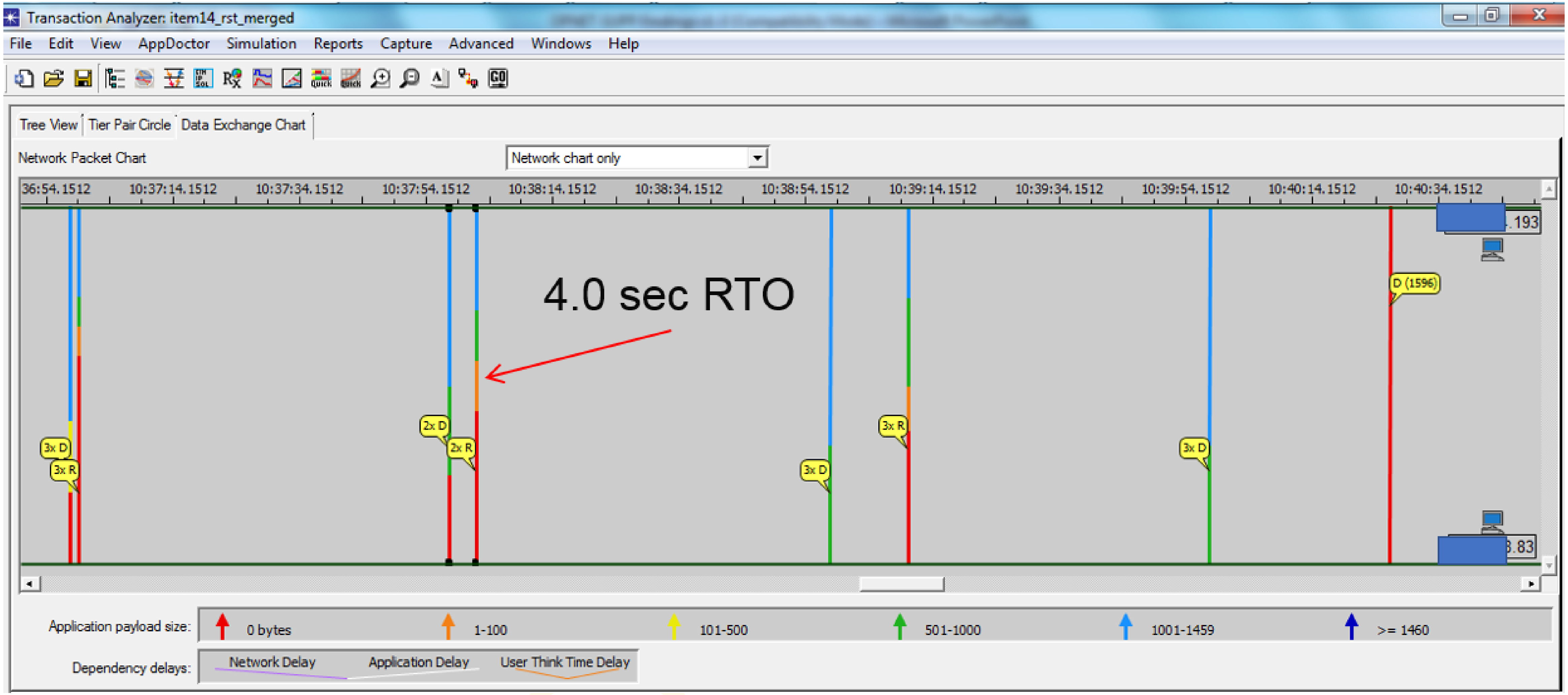
- Insurance company call center
- Reps have a variety of complaints:
  - Dropped calls
  - Screen pop not synchronized with call arrivals
  - CRM app session drops
- Reviewed packets from call center PCs and found periods of packet loss and retransmissions
- Next screens show visualization of TCP RTO affects which eventually lead to TCP RST

TCP RTO Visualization 1 of 4

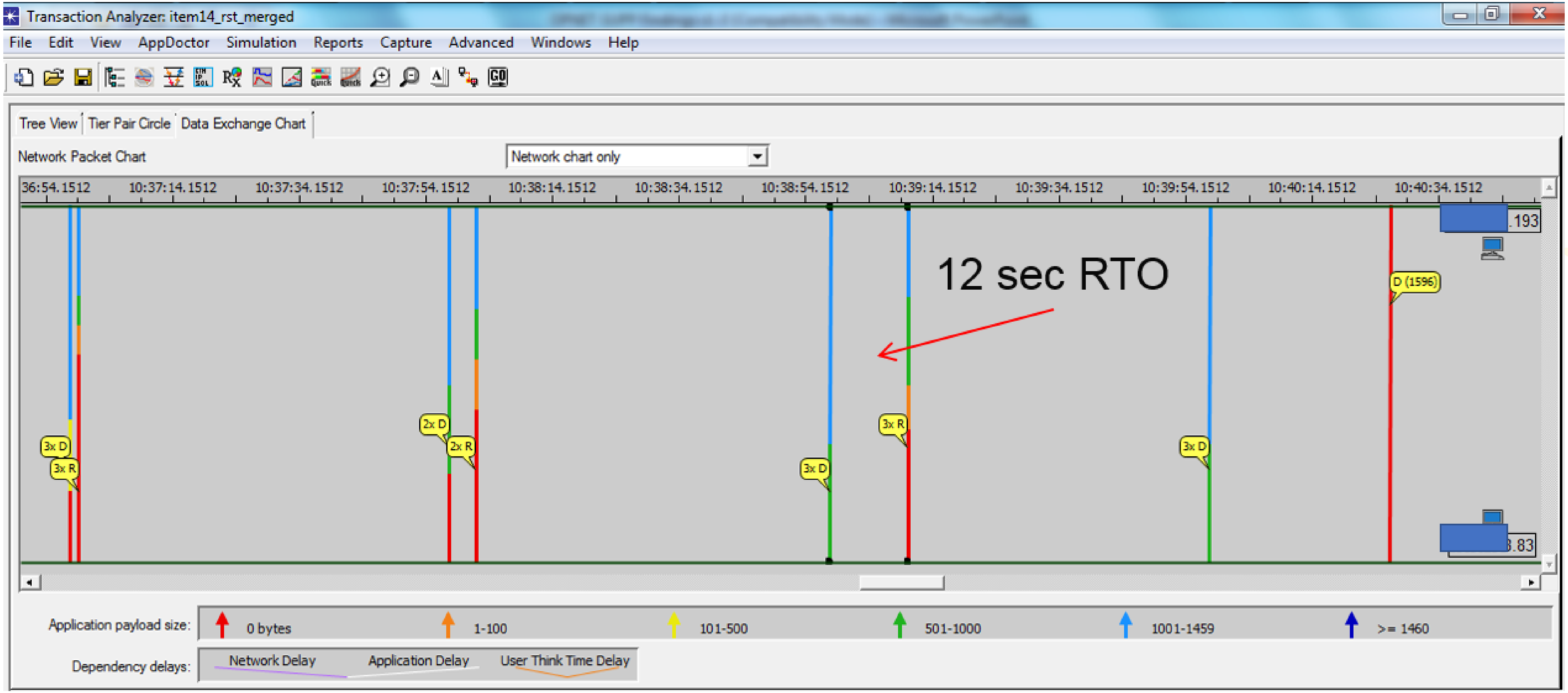


1.3 sec RTO

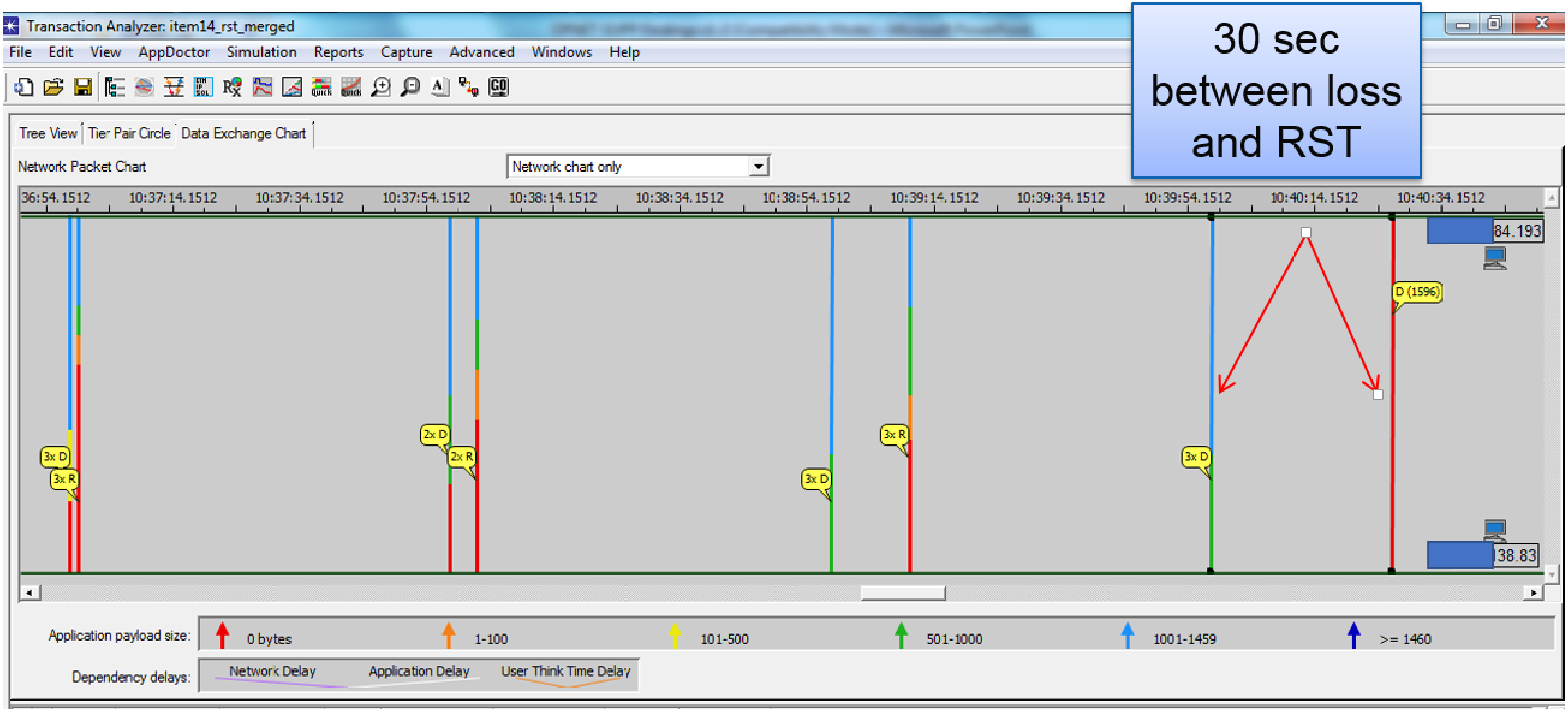
TCP RTO Visualization 2 of 4



TCP RTO Visualization 3 of 4



TCP RTO Visualization 4 of 4



30 sec between loss and RST

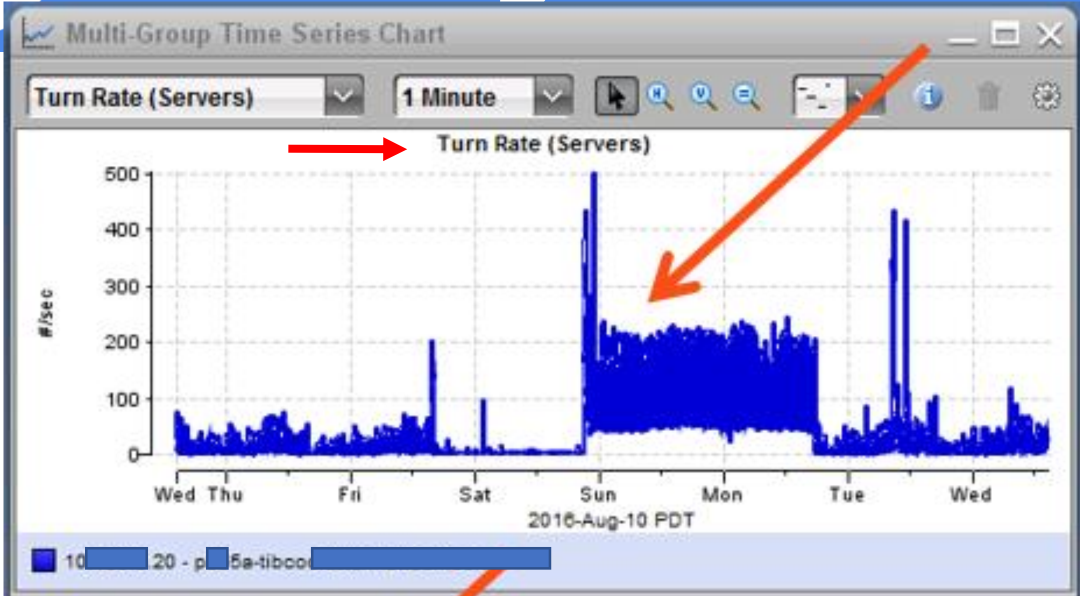
Performance Analysis Workflows

- Dev Team Unit Testing
- Load Testing
- Pre-Deployment Performance Assessment
- New Technology Assessments
- 3rd Party Software Qualification

Impact Assessments / Planning

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

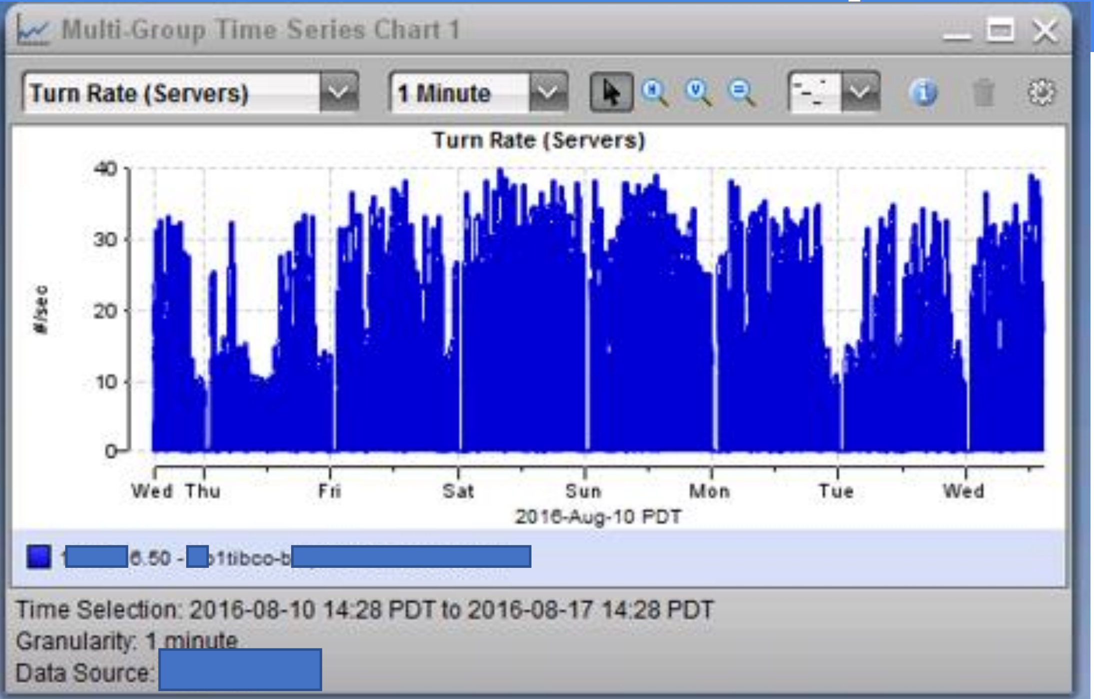
Pre-Migration Assessment Example



Multi-Group Time Series Chart

Turn Rate (Servers) · 1 Minute

10[redacted]20 - p[redacted]5a-tibco[redacted]



Multi-Group Time Series Chart 1

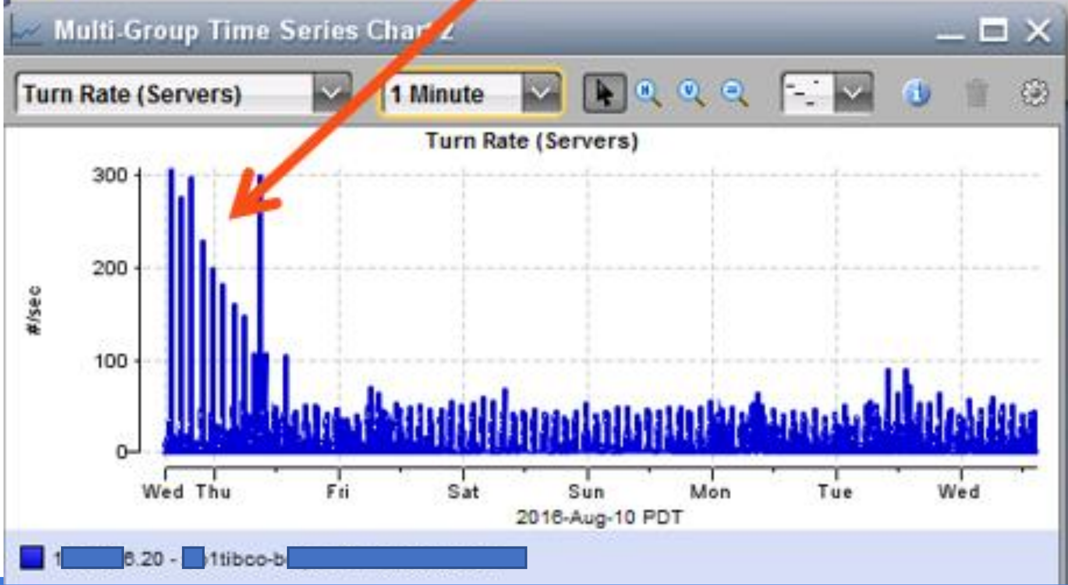
Turn Rate (Servers) · 1 Minute

1[redacted]6.50 - [redacted]1tibco-b[redacted]

Time Selection: 2016-08-10 14:28 PDT to 2016-08-17 14:28 PDT

Granularity: 1 minute

Data Source: [redacted]



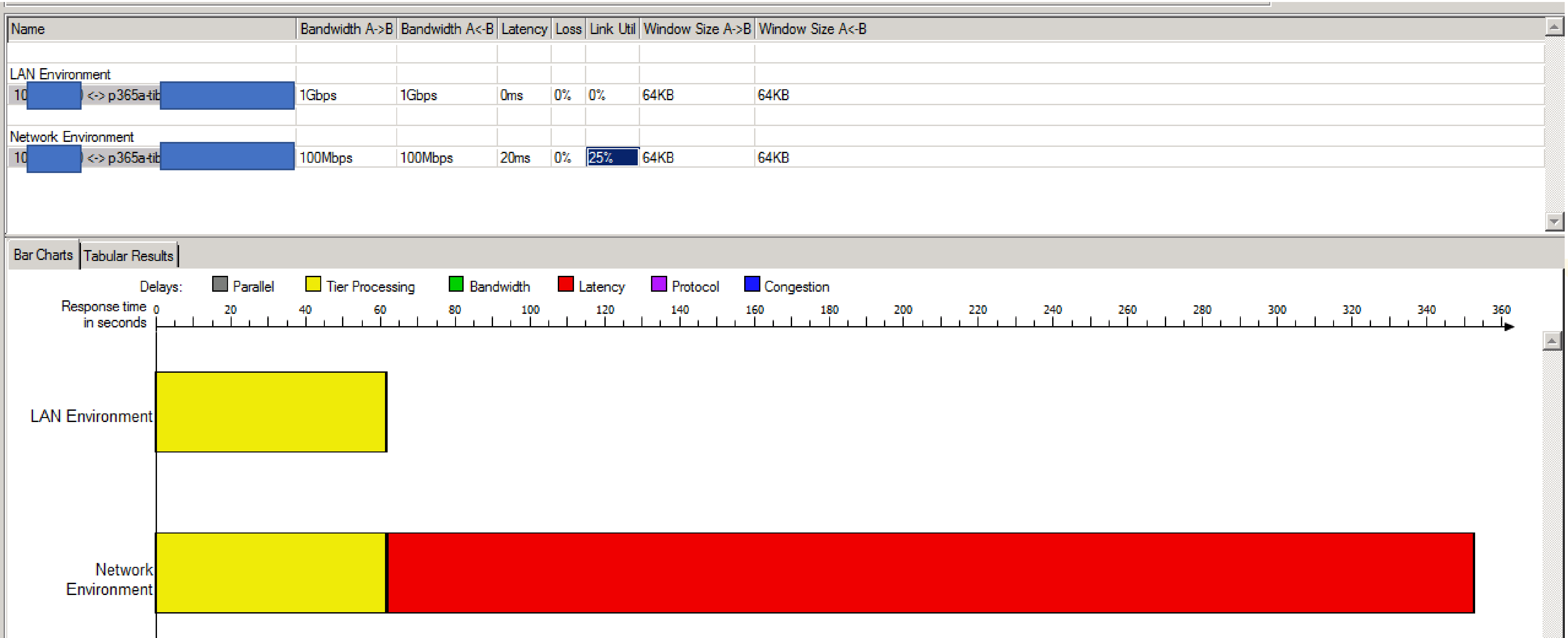
Multi-Group Time Series Chart 2

Turn Rate (Servers) · 1 Minute

1[redacted]6.20 - [redacted]1tibco-b[redacted]

Latency Sensitive Conversations

Impact of 40ms Round Trip Latency



Name	Bandwidth A->B	Bandwidth A<-B	Latency	Loss	Link Util	Window Size A->B	Window Size A<-B
LAN Environment							
10[redacted]) <-> p365a-tib[redacted]	1Gbps	1Gbps	0ms	0%	0%	64KB	64KB
Network Environment							
10[redacted]) <-> p365a-tib[redacted]	100Mbps	100Mbps	20ms	0%	25%	64KB	64KB

Response time increases from 1 minute to 6 minutes

Questions / Discussion

Time to Talk Money

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

Impact to the Business

- DB Replication Delays impact customer data visibility
- Claims Management Down
- Load Testing brings down production data center
- Call Center 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 Guidance

- 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

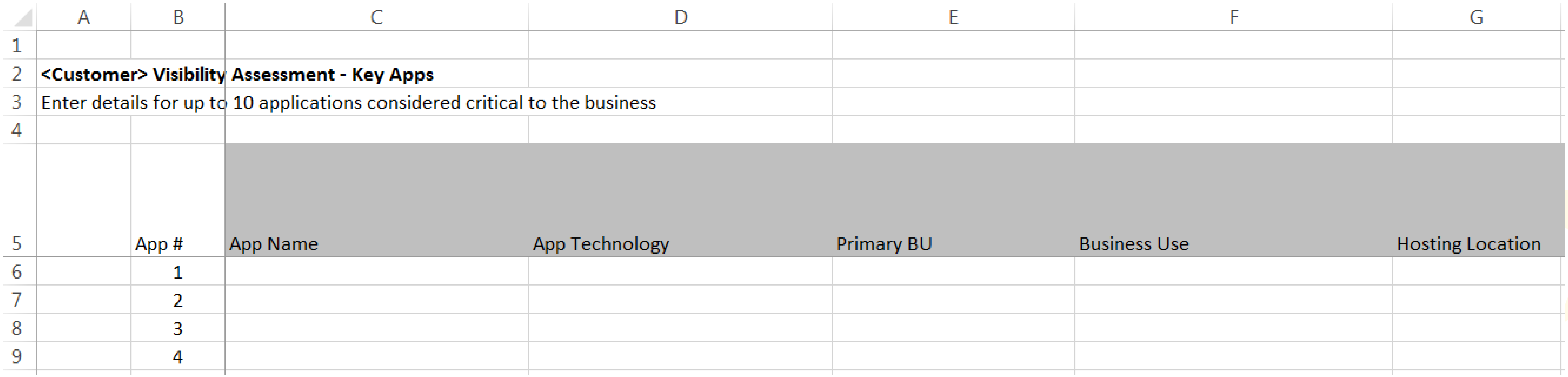
Business Impact

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

Identify Your 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

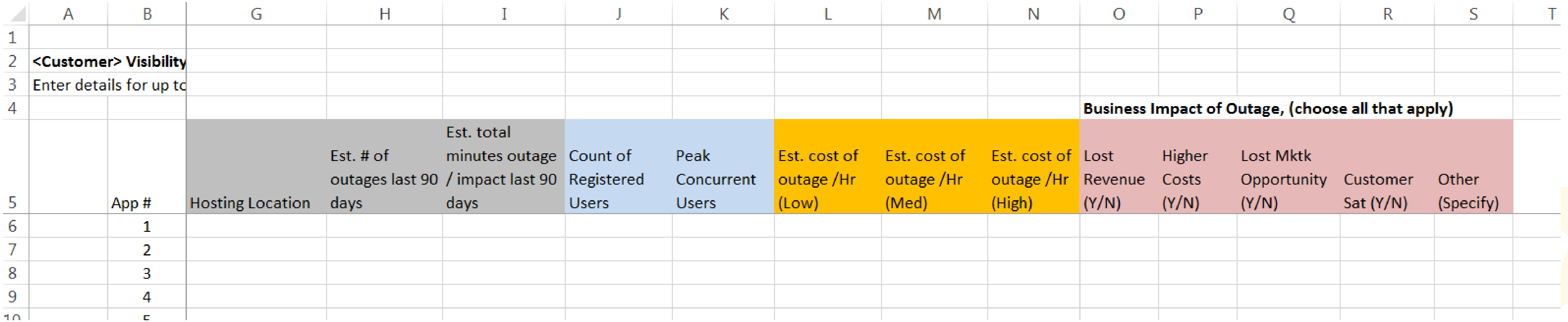


<Customer> Visibility Assessment - Key Apps

Enter details for up to 10 applications considered critical to the business

App #	App Name	App Technology	Primary BU	Business Use	Hosting Location
1					
2					
3					
4					

Additional Attributes



	A	B	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																
2	**<Customer> Visibility**															
3	Enter details for up tc															
4											**Business Impact of Outage, (choose all that apply)**					
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

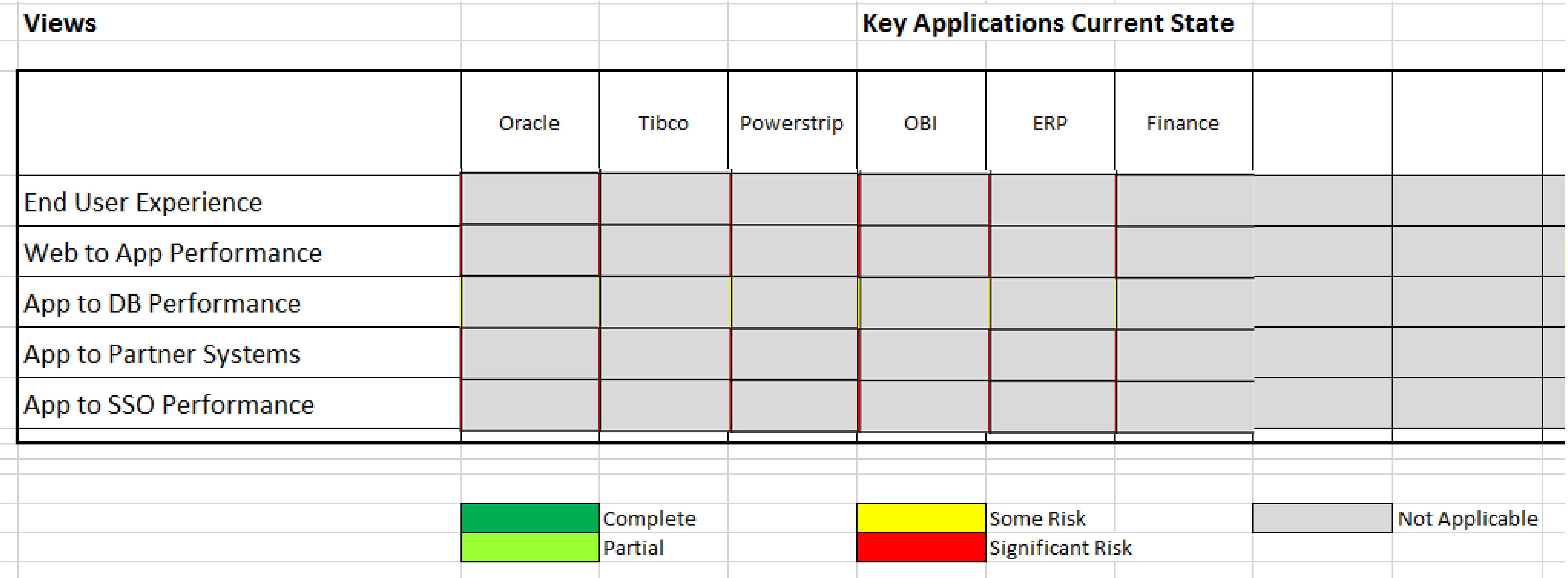
Current State: Capture / Visibility Capabilities

- 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?

Let’s use a Heat Map!

- Simple Excel Spreadsheets with conditional formatting
- Visualize where we have coverage vs. where we need 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

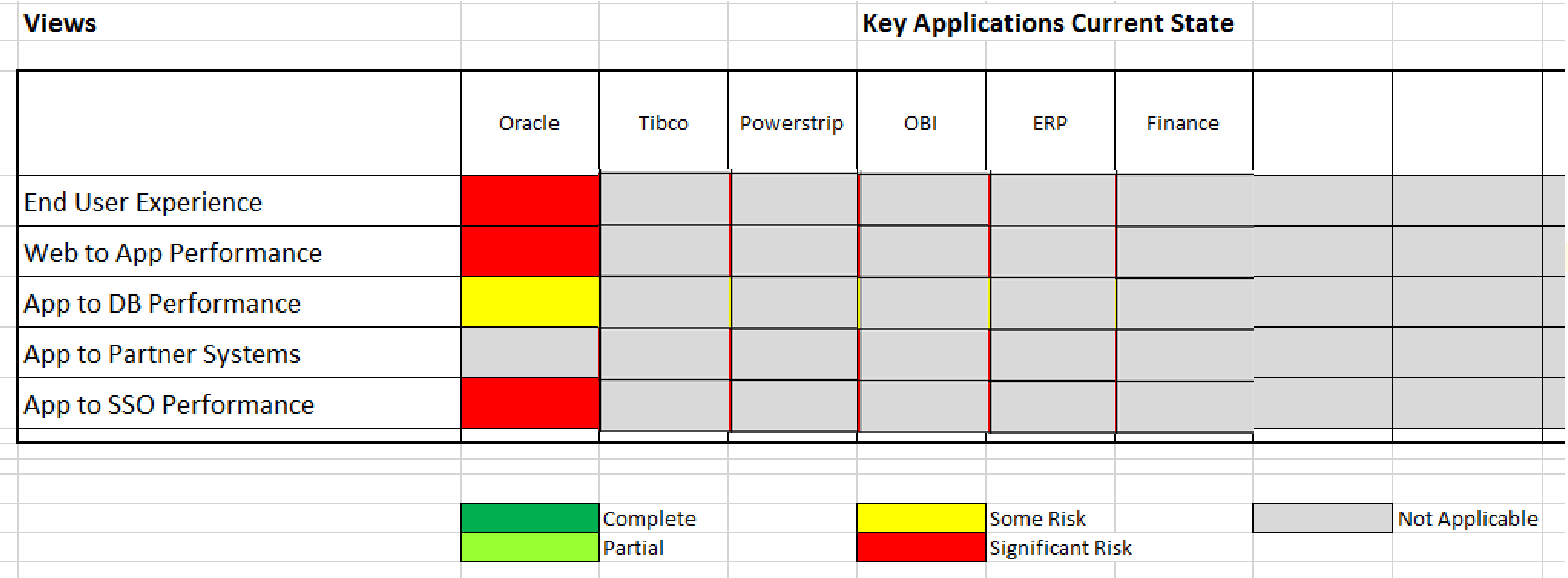


Views | **Key Applications Current State**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	▨	▨	▨	▨	▨	▨	▨	▨
Web to App Performance	▨	▨	▨	▨	▨	▨	▨	▨
App to DB Performance	▨	▨	▨	▨	▨	▨	▨	▨
App to Partner Systems	▨	▨	▨	▨	▨	▨	▨	▨
App to SSO Performance	▨	▨	▨	▨	▨	▨	▨	▨

🟩	Complete	🟨	Some Risk	▨	Not Applicable
🟩	Partial	🟥	Significant Risk		

Current State: Packet Capture Coverage

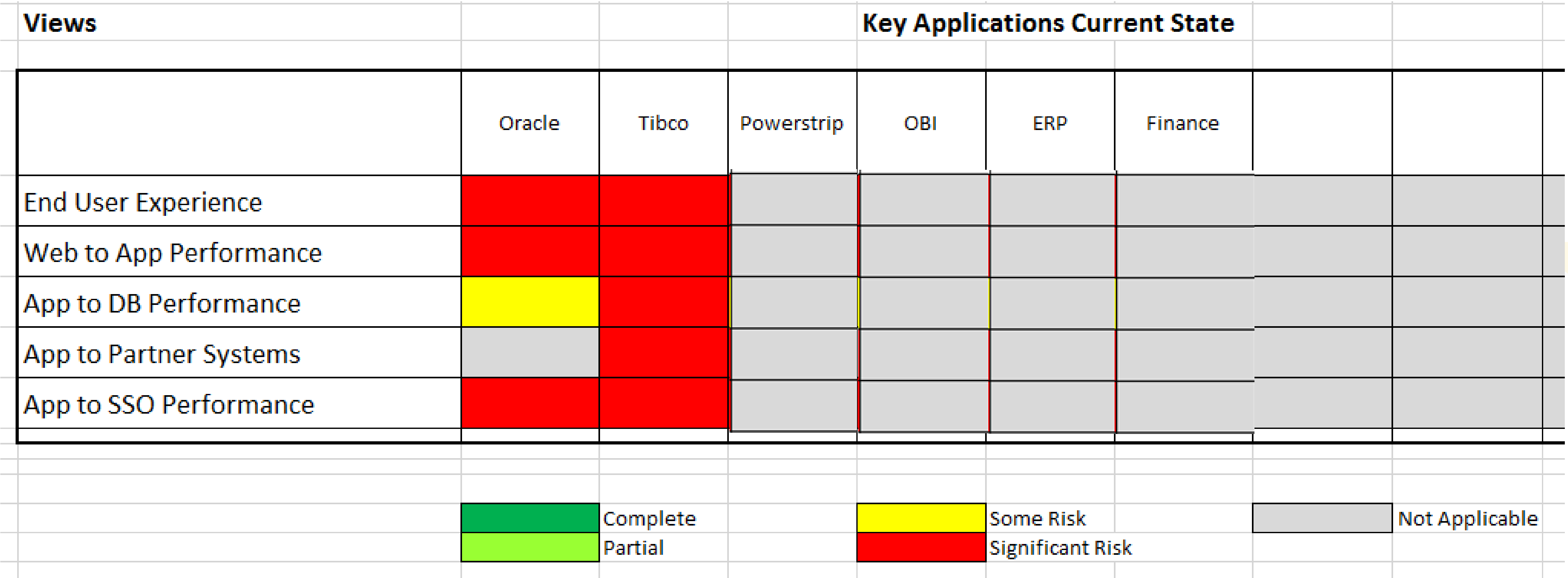


Views **Key Applications Current State**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜
Web to App Performance	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜
App to DB Performance	🟨	⬜	⬜	⬜	⬜	⬜	⬜	⬜
App to Partner Systems	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
App to SSO Performance	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜

🟩	Complete	🟨	Some Risk	⬜	Not Applicable
🟩	Partial	🟥	Significant Risk		

Current State: Packet Capture Coverage



Views | **Key Applications Current State**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜
Web to App Performance	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜
App to DB Performance	🟨	🟥	⬜	⬜	⬜	⬜	⬜	⬜
App to Partner Systems	⬜	🟥	⬜	⬜	⬜	⬜	⬜	⬜
App to SSO Performance	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜

🟩 Complete

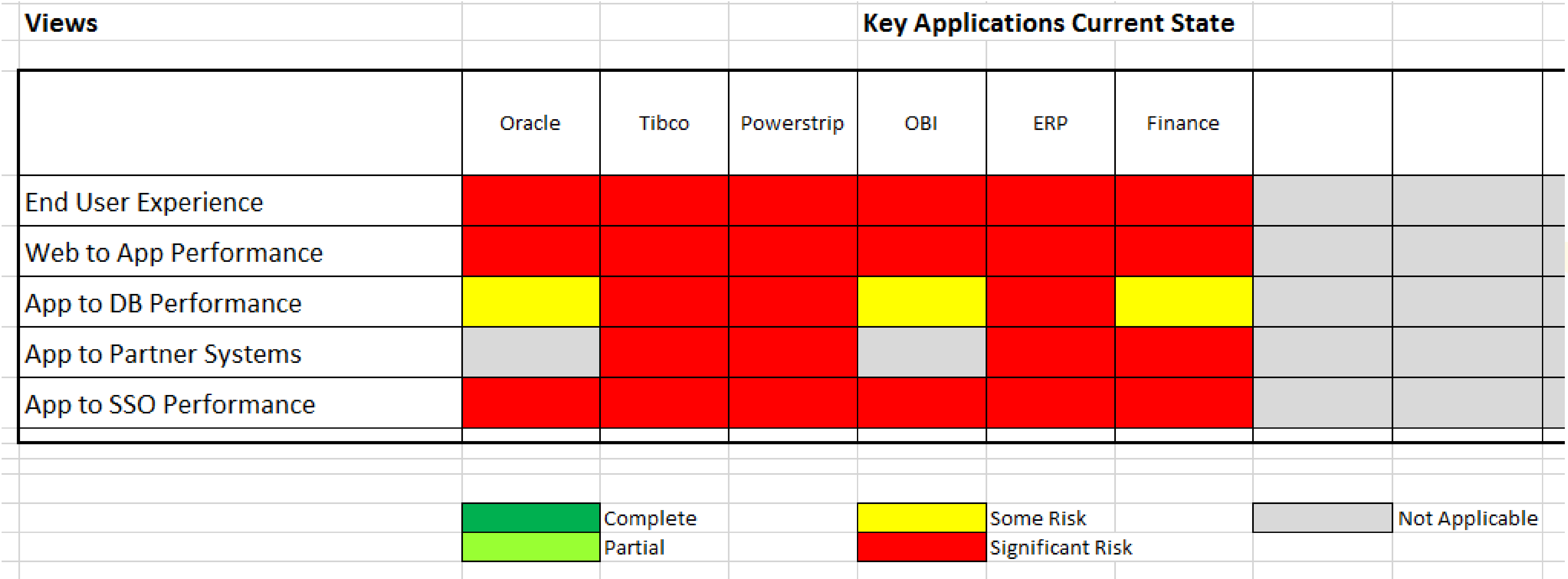
🟩 Partial

🟨 Some Risk

🟥 Significant Risk

⬜ Not Applicable

Current State: Packet Capture Coverage



Views **Key Applications Current State**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨
Web to App Performance	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨
App to DB Performance	🟨	🟥	🟥	🟨	🟥	🟨	▨	▨
App to Partner Systems	▨	🟥	🟥	▨	🟥	🟥	▨	▨
App to SSO Performance	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨

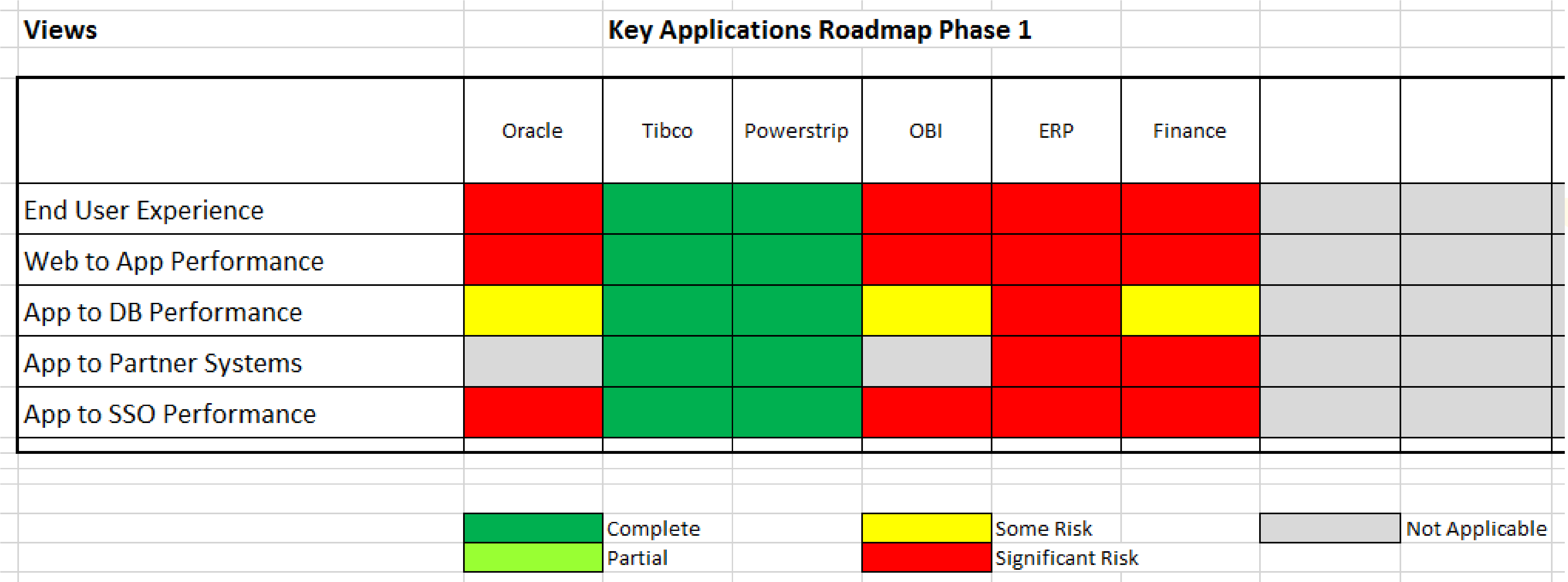
🟩	Complete	🟨	Some Risk	▨	Not Applicable
🟩	Partial	🟥	Significant Risk		

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



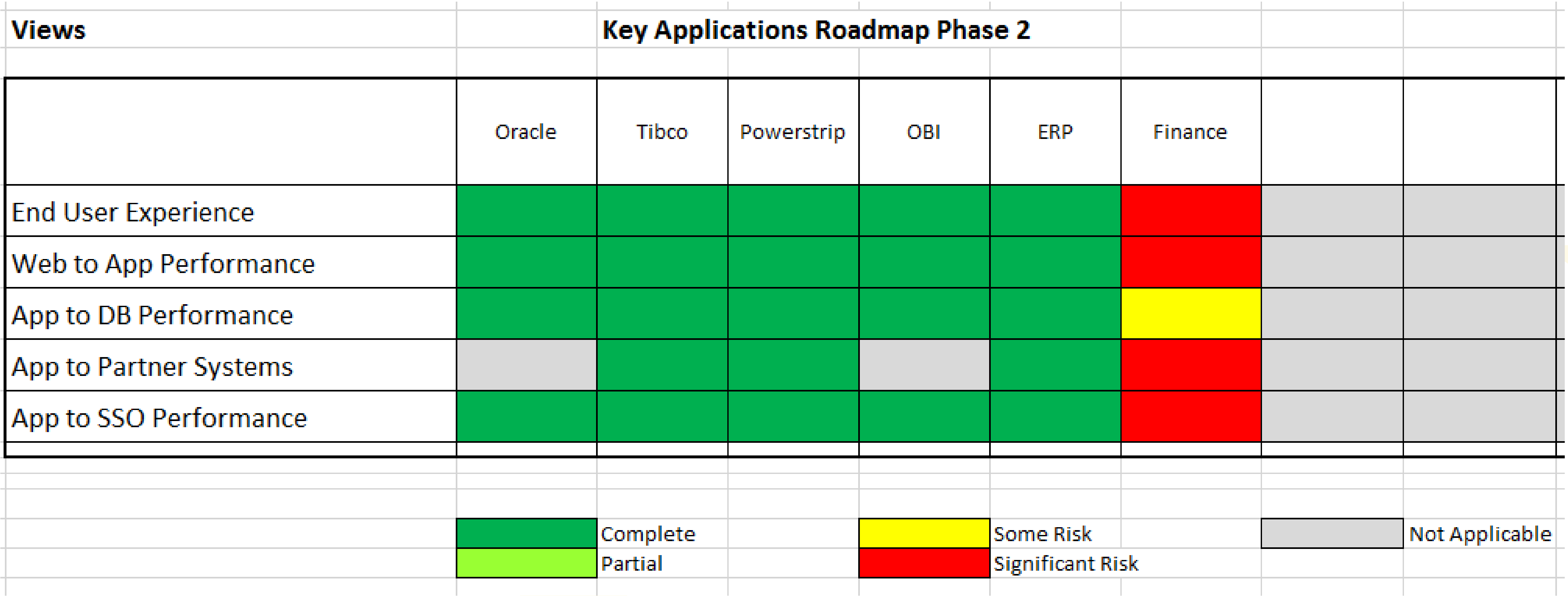
Views

Key Applications Roadmap Phase 1

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟥	🟩	🟩	🟥	🟥	🟥	⬜	⬜
Web to App Performance	🟥	🟩	🟩	🟥	🟥	🟥	⬜	⬜
App to DB Performance	🟨	🟩	🟩	🟨	🟥	🟨	⬜	⬜
App to Partner Systems	⬜	🟩	🟩	⬜	🟥	🟥	⬜	⬜
App to SSO Performance	🟥	🟩	🟩	🟥	🟥	🟥	⬜	⬜

🟩 Complete	🟨 Some Risk	⬜ Not Applicable
▨ Partial	🟥 Significant Risk	

Phase 2 – Next Quarter

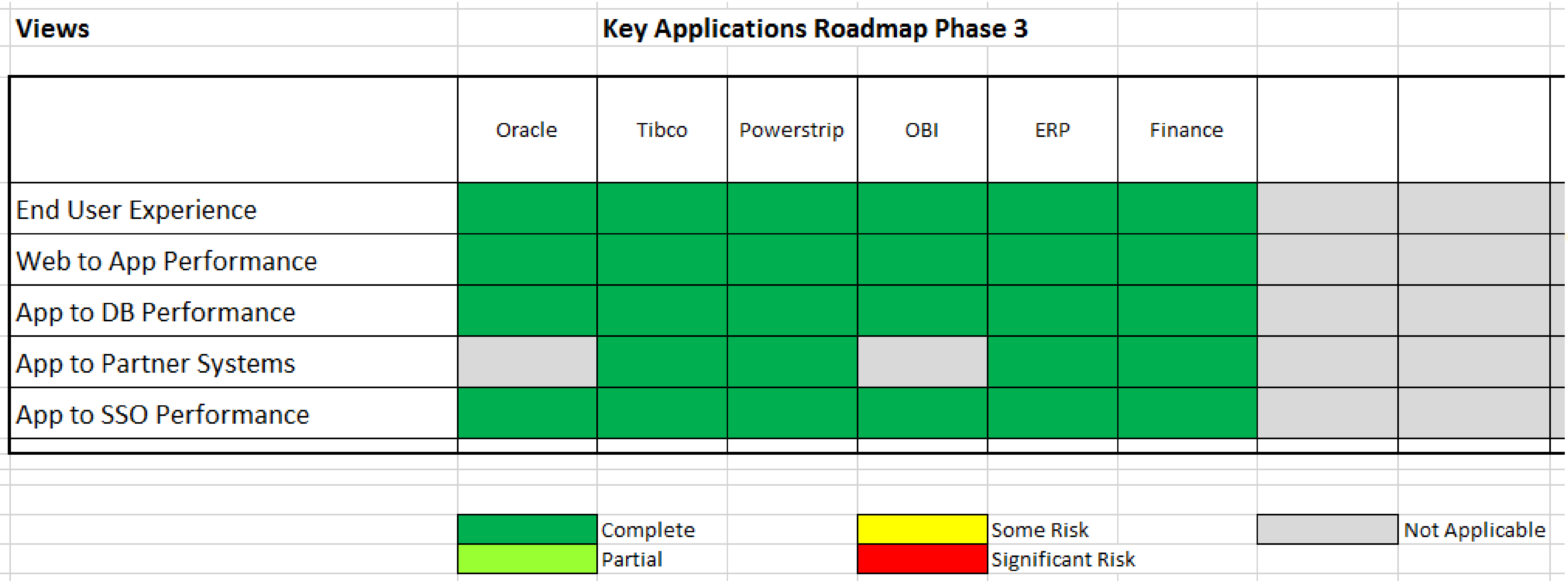


Views **Key Applications Roadmap Phase 2**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟩	🟩	🟩	🟩	🟩	🟥	⬜	⬜
Web to App Performance	🟩	🟩	🟩	🟩	🟩	🟥	⬜	⬜
App to DB Performance	🟩	🟩	🟩	🟩	🟩	🟨	⬜	⬜
App to Partner Systems	⬜	🟩	🟩	⬜	🟩	🟥	⬜	⬜
App to SSO Performance	🟩	🟩	🟩	🟩	🟩	🟥	⬜	⬜

🟩	Complete	🟨	Some Risk	⬜	Not Applicable
🟢	Partial	🟥	Significant Risk		

Phase 3 – two Quarters out



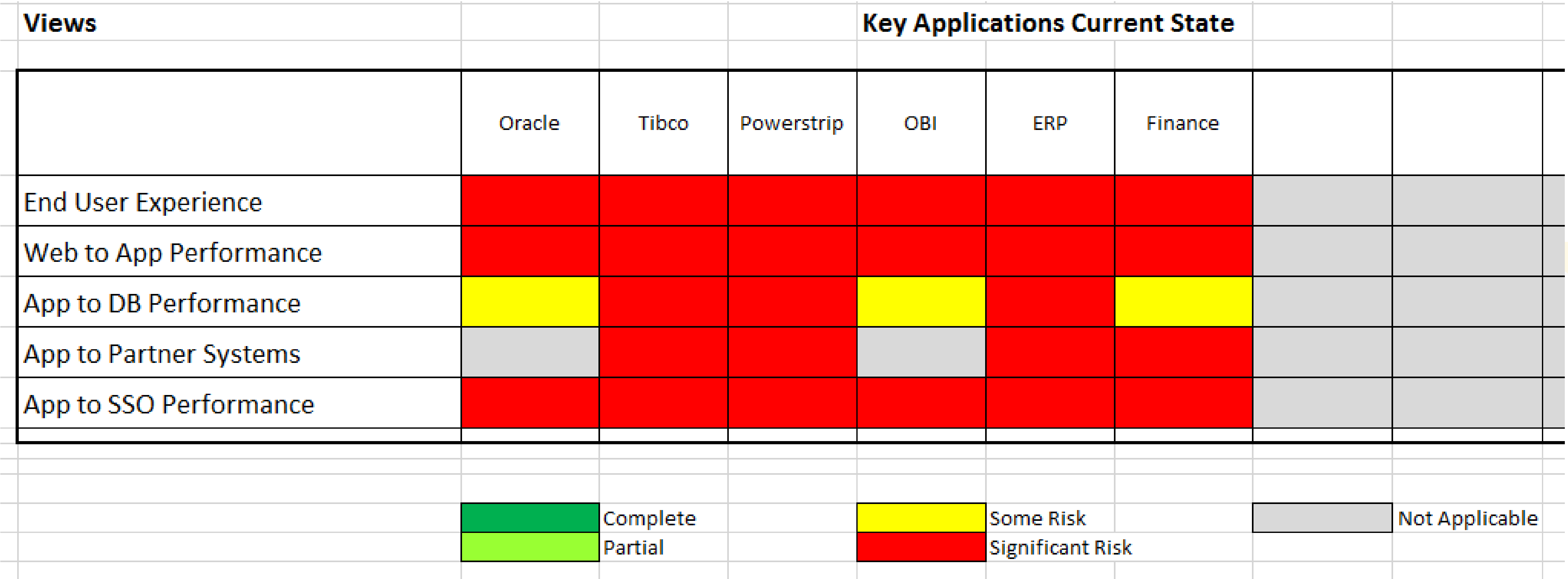
Views **Key Applications Roadmap Phase 3**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜
Web to App Performance	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜
App to DB Performance	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜
App to Partner Systems	⬜	🟩	🟩	⬜	🟩	🟩	⬜	⬜
App to SSO Performance	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜

🟩	Complete	🟨	Some Risk	⬜	Not Applicable
🟢	Partial	🟥	Significant Risk		

An Alternate Roadmap…

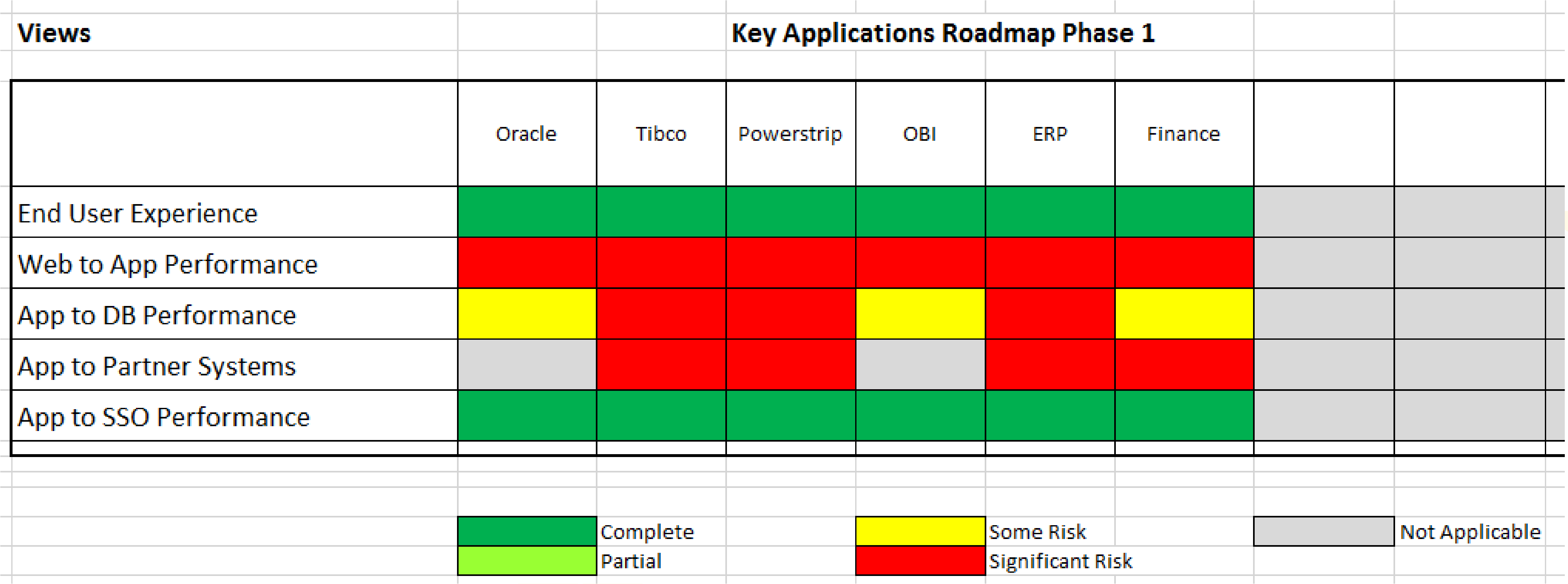
Current State: Packet Capture Coverage



Views				Key Applications Current State				
	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨
Web to App Performance	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨
App to DB Performance	🟨	🟥	🟥	🟨	🟥	🟨	▨	▨
App to Partner Systems	▨	🟥	🟥	▨	🟥	🟥	▨	▨
App to SSO Performance	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨

🟩 Complete		🟨 Some Risk		▨ Not Applicable
🟩 Partial		🟥 Significant Risk		

Alternate Phase 1



Views **Key Applications Roadmap Phase 1**

	Oracle	Tibco	Powerstrip	OBI	ERP	Finance		
End User Experience	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜
Web to App Performance	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜
App to DB Performance	🟨	🟥	🟥	🟨	🟥	🟨	⬜	⬜
App to Partner Systems	⬜	🟥	🟥	⬜	🟥	🟥	⬜	⬜
App to SSO Performance	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜

🟩	Complete	🟨	Some Risk	⬜	Not Applicable
🟢	Partial	🟥	Significant Risk		

Comments / Discussion

Key Infrastructure – Shared Services

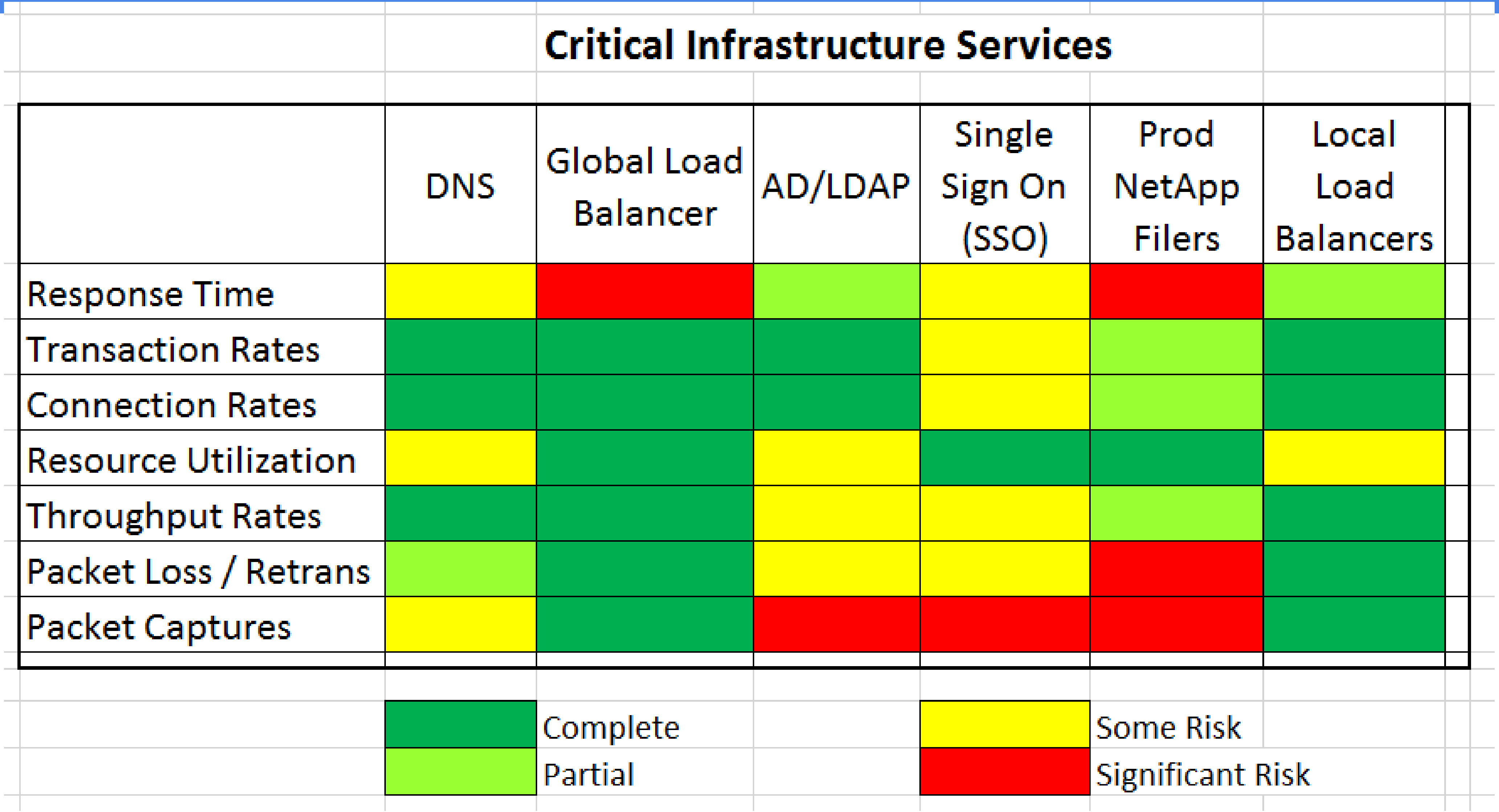
- What are some key shared services in your environment?

- 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	🟨	🟥	🟢	🟨	🟥	🟢
Transaction Rates	🟩	🟩	🟩	🟨	🟢	🟩
Connection Rates	🟩	🟩	🟩	🟨	🟢	🟩
Resource Utilization	🟨	🟩	🟨	🟩	🟩	🟨
Throughput Rates	🟩	🟩	🟨	🟨	🟢	🟩
Packet Loss / Retrans	🟢	🟩	🟨	🟨	🟥	🟩
Packet Captures	🟨	🟩	🟥	🟥	🟥	🟩

🟩	Complete	🟨	Some Risk
🟢	Partial	🟥	Significant Risk

Heat Map Demo

Questions / Comments

General Recommendations

- Leverage host based captures everywhere
- Use passive appliances to get coverage for infrastructure shared services and all application edge traffic (EUE)
- Add supplemental analysis capabilities on top of Wireshark

General Recommendations

- Identify key apps where inter-tier packets are most beneficial and expand traffic feeds
- Keep Management informed of current state and your recommended roadmap to increase visibility

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!