

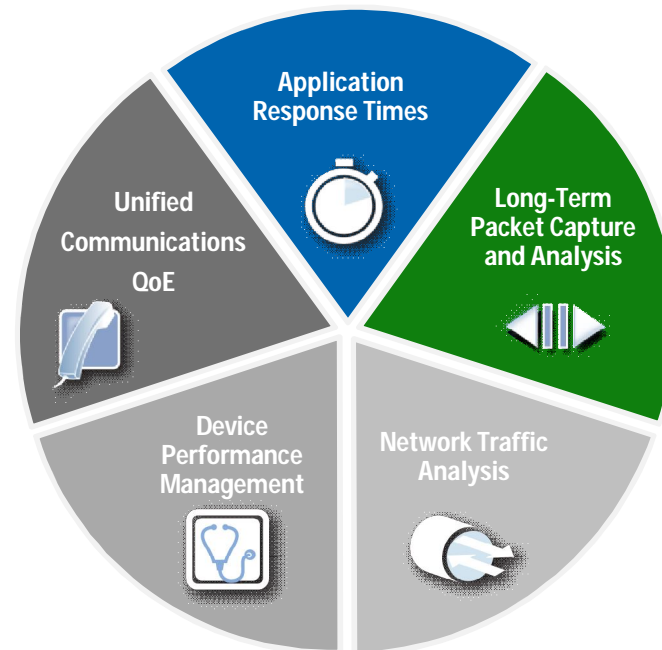
SuperAgent nie je AGENT!

Roman Tuchyňa, CSA

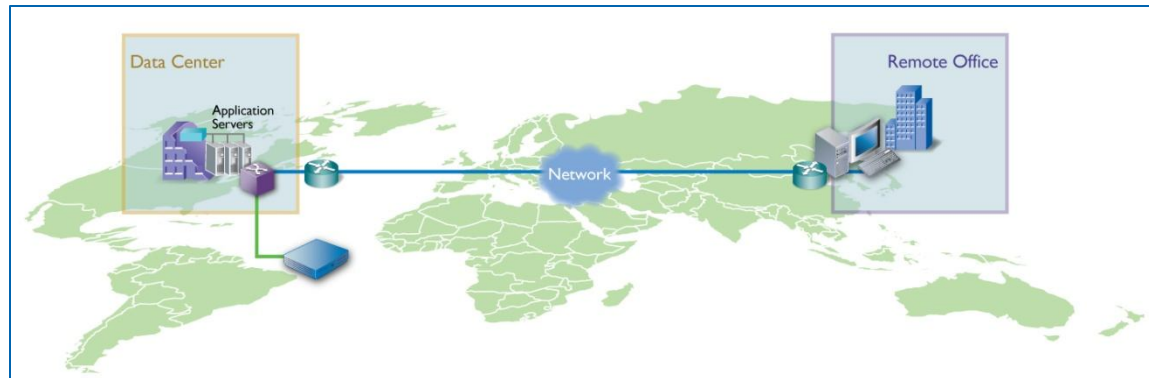
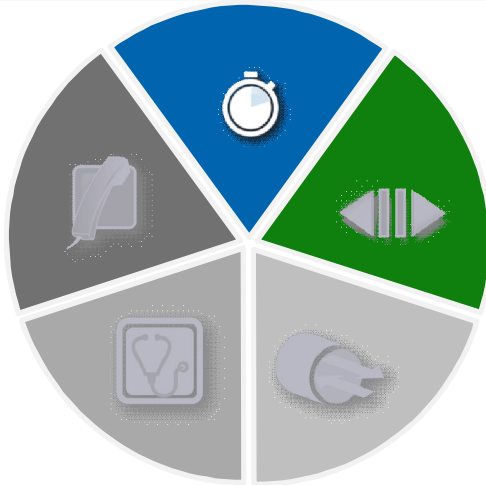
ca Forum

Bratislava
20. október

Complete Network Performance Management



Application Response Times

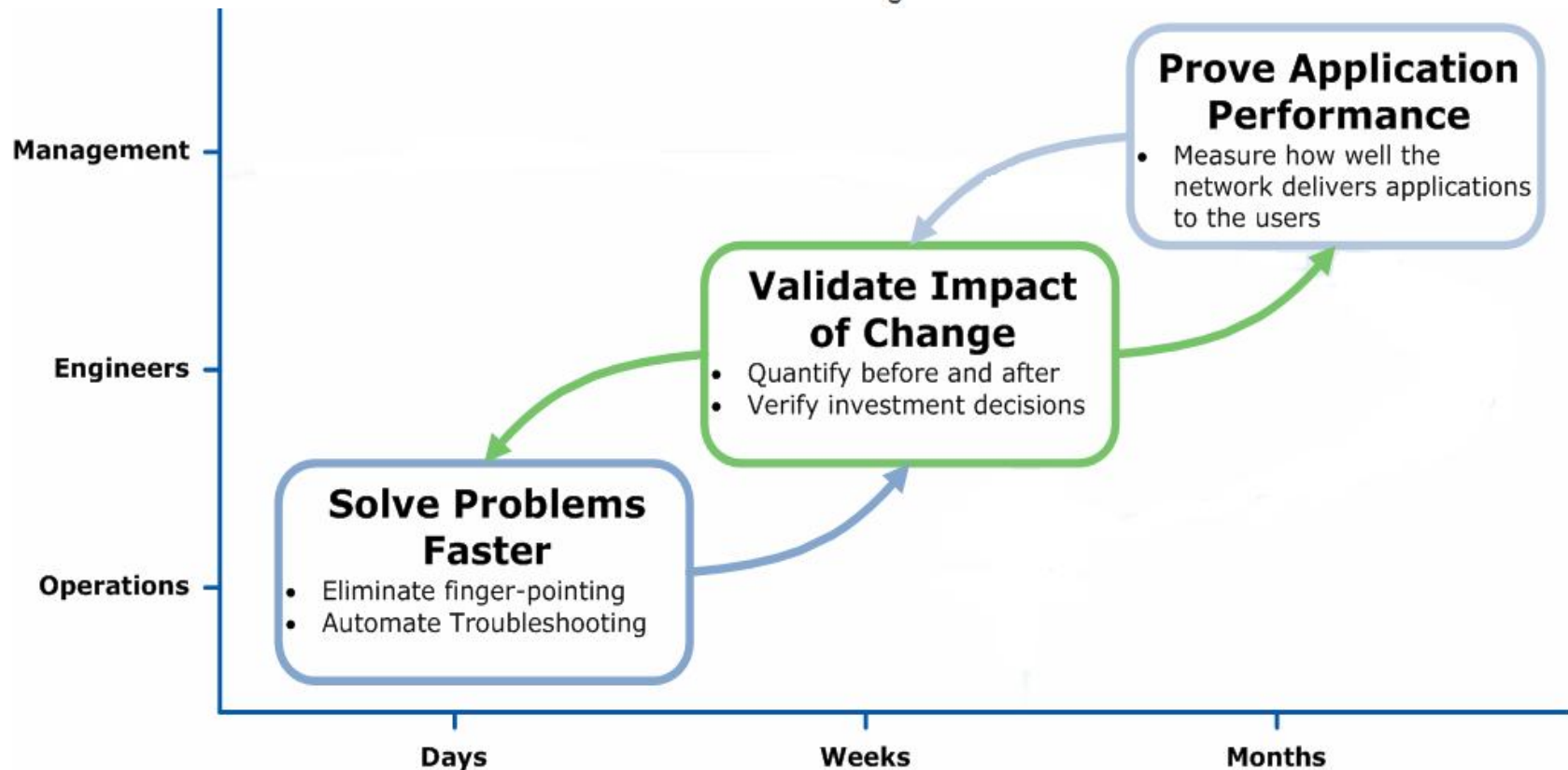


- **Application service level reporting down to packet details**
- **Unique WAN optimization monitoring**
- **Root cause analysis, problem isolation & automated investigations**
- **Passive appliance architecture requires no agents or probes**

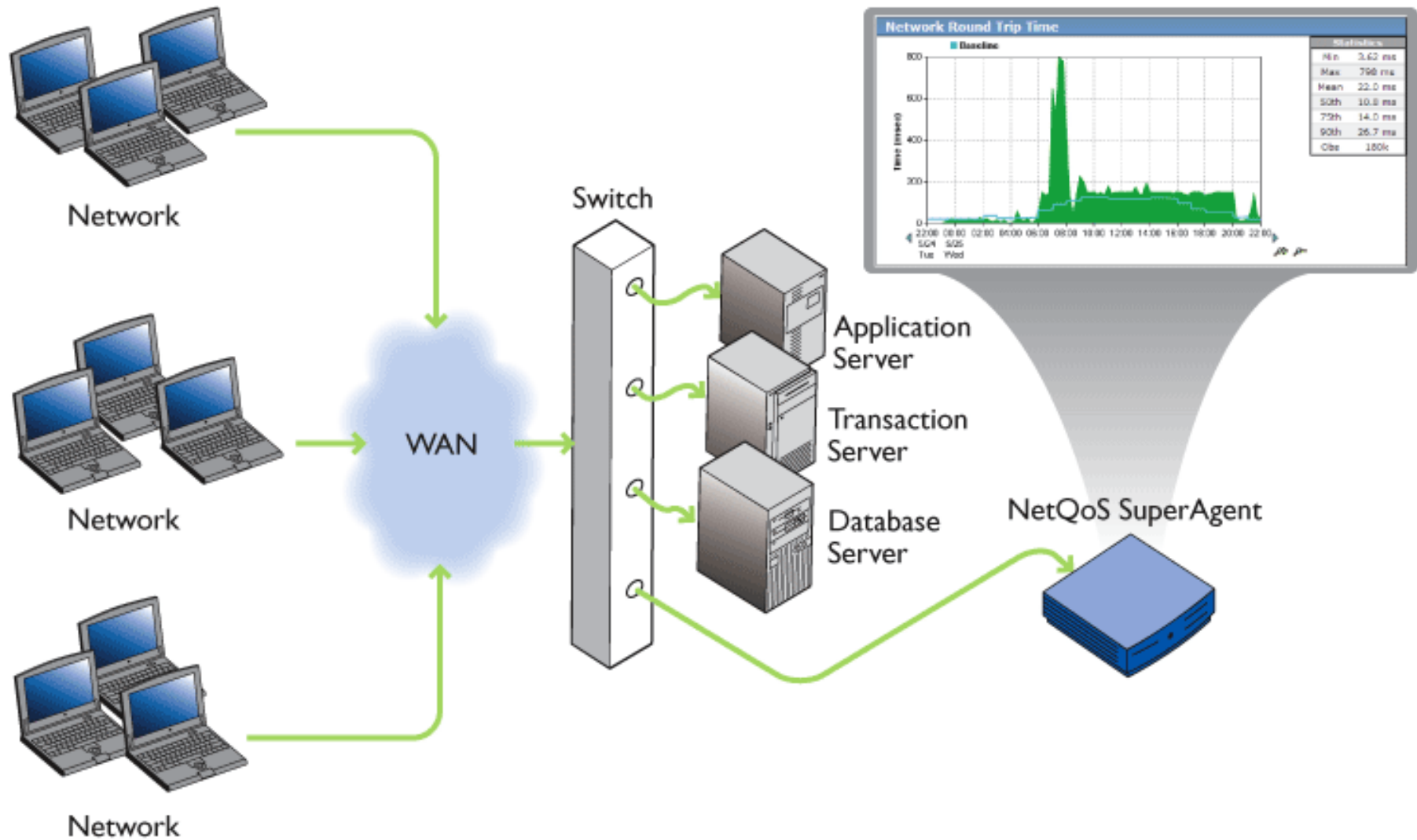
Performance by Network				
Network	Subnet	Transaction Time		Observations
		Wtd. Average: 2.46 sec	Average: 813.11 ms	
Pittsburgh PA	172.15.222.192/26	5.29 sec	482	
Nome AK	172.15.227.192/26	3.87 sec	248	
Vancouver	172.18.125.64/26	3.70 sec	1,636	
Baltimore MD	172.15.238.192/26	3.66 sec	89	
Singapore	172.15.92.128/26	3.65 sec	2,933,607	
SAP1	172.18.150.0/26	3.04 sec	476,415	
SAP3	172.18.125.0/26	3.03 sec	481,626	
SAP7	172.18.60.0/26	3.03 sec	477,049	
SAP8	172.18.150.64/26	3.02 sec	484,620	
SAP6	172.18.57.128/26	3.01 sec	480,685	



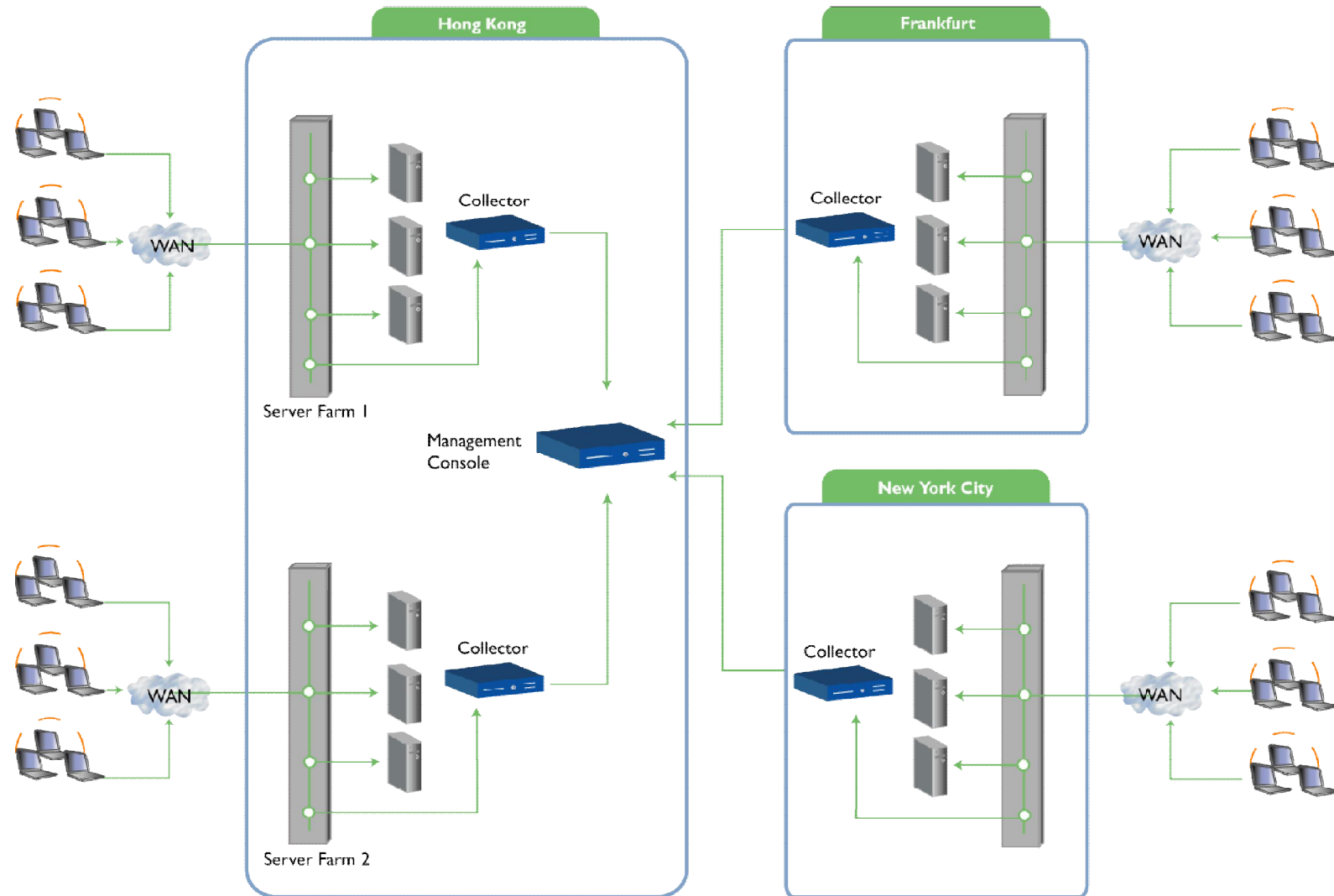
Value of End-to-End Monitoring

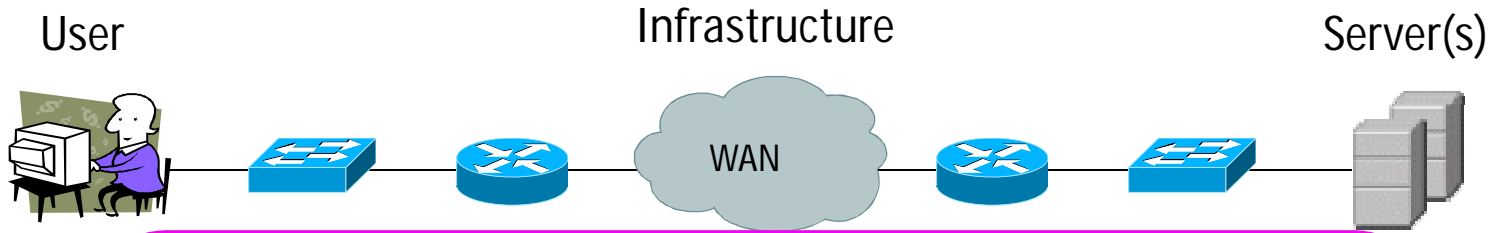


SuperAgent Architecture

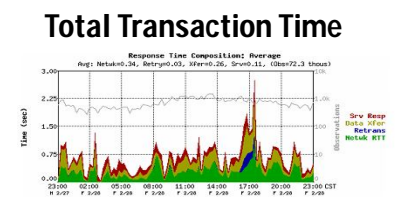
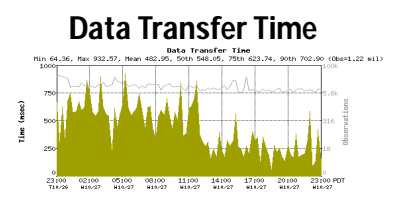
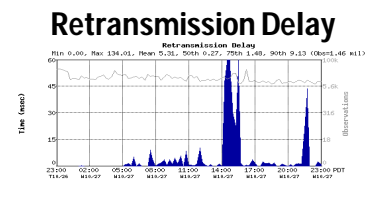
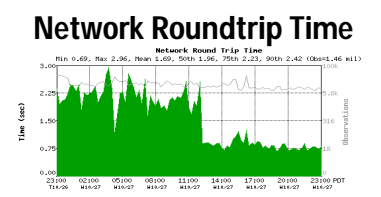
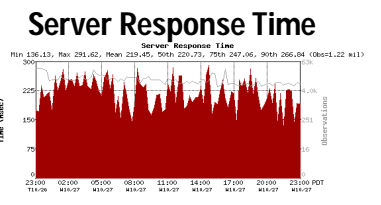


Scaling to the Most Demanding Networks



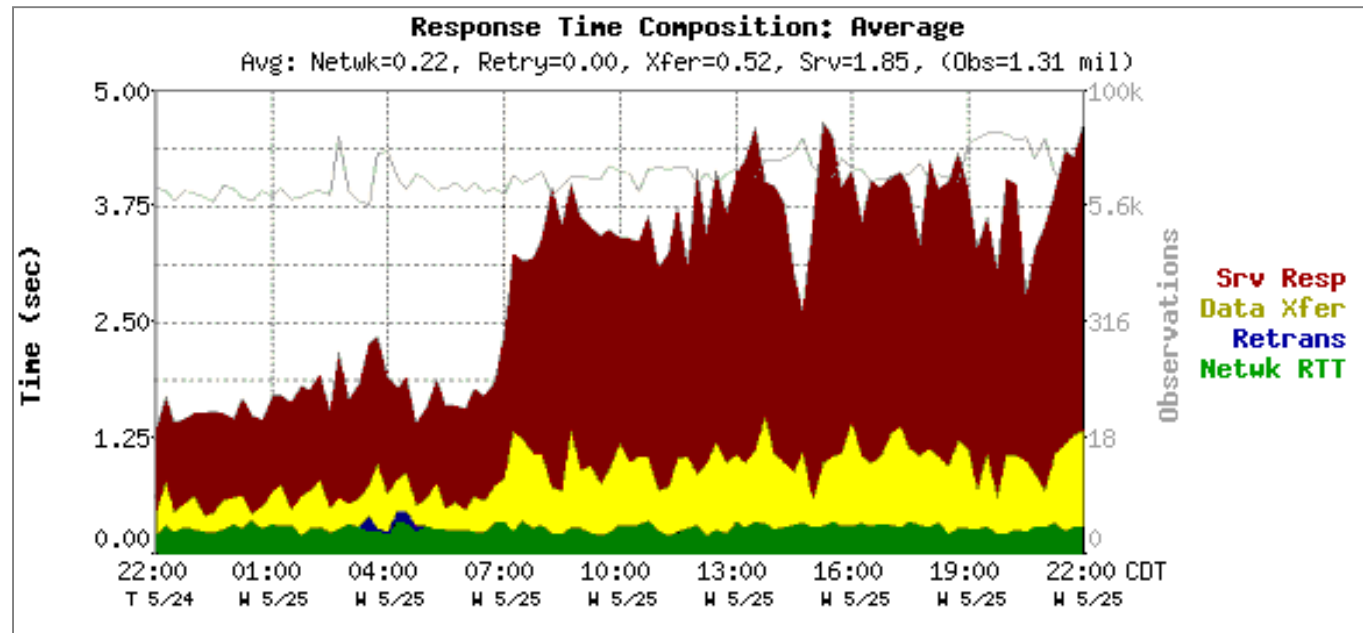


Web Transaction



Response Time Insight

Srv Resp
+
Data Xfer
+
Retrans
+
Network RTT
=

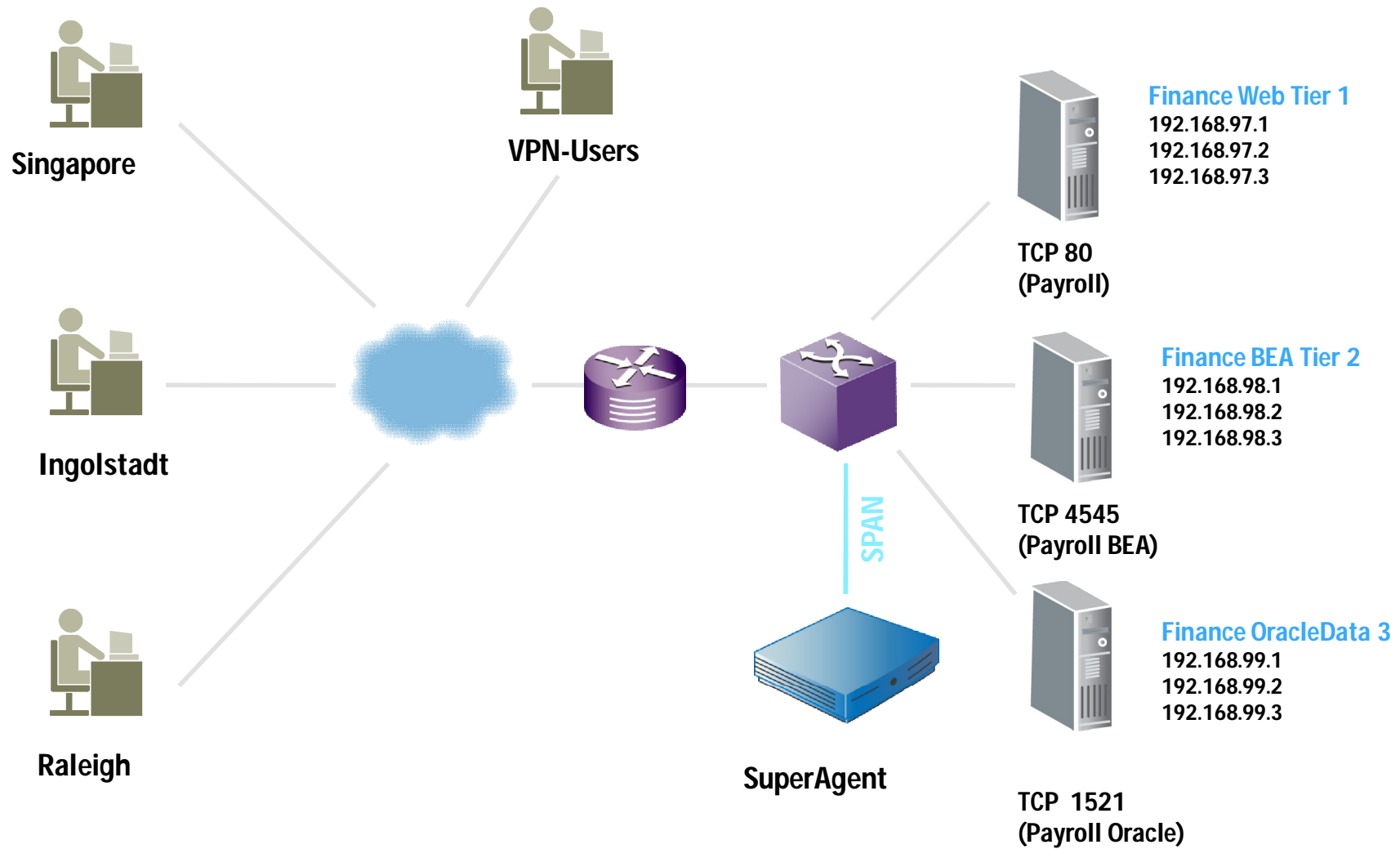


(grey line represents observed transactions over the given time interval)

Total Transaction Time

Total time for single TCP transaction across the network

SuperAgent Setup



Three Components

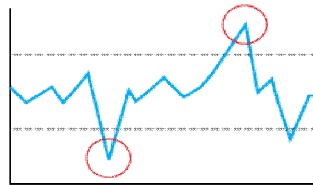
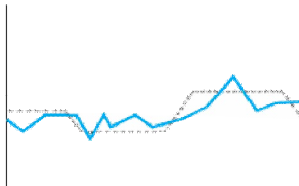
Application List								
SuperAgent monitors network traffic for the following Applications.								
You can modify more than one application at a time by checking selected applications and clicking an option in the grey header.								
<input type="text" value="payroll"/> <input type="button" value="Search"/> <input type="button" value="Clear"/>								
Application	TCP Ports	Type	Servers	Segments	Bytes	Last Seen		
Payroll	80	Standard		0	0	0	Never Seen	<input type="checkbox"/>
Payroll (bea) - Tier 2	4545	Standard		0	0	0	Never Seen	<input type="checkbox"/>
Payroll (oracle) - Tier 3	1521	Standard		0	0	0	Never Seen	<input type="checkbox"/>

Server List								
SuperAgent monitors network traffic for the following Servers.								
You can modify more than one server at a time by checking selected servers and clicking an option in the grey header.								
<input type="text" value="finance"/> <input type="button" value="Search"/> <input type="button" value="Clear"/>								
Server	Address	Type	Apps	Collection Device	Bytes	Last Seen		
Finance - BEA1 Tier 2	192.168.98.1	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - BEA2 Tier 2	192.168.98.2	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - BEA3 Tier 2	192.168.98.3	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - OracleDatabase1 Tier 3	192.168.99.1	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - OracleDatabase2 Tier 3	192.168.99.2	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - OracleDatabase3 Tier 3	192.168.99.3	Configured	0		0	Never Seen	<input type="checkbox"/>	
Finance - Web1 Tier 1	192.168.97.1	Configured	0		0	Never Seen	<input type="checkbox"/>	
			0		0	Never Seen	<input type="checkbox"/>	
			0		0	Never Seen	<input type="checkbox"/>	

Global Network Set						
Below is a list of all the networks in the above selected set.						
Network	Subnet	Regions	Network Type	Detect Servers		
San Jose - 10.200.5.0/24	10.200.5.1/32	0	T1	No	<input type="checkbox"/>	
Singapore - 10.19.1.0/24	10.19.1.0/32	0	T1	No	<input type="checkbox"/>	
Sydney - 10.30.9.0/24	10.30.9.1/32	0	T1	No	<input type="checkbox"/>	
Taipei -- 10.168.13.0/24	10.168.13.0/32	0	512K	No	<input type="checkbox"/>	
VPN Users -- 10.168.10.0/24	10.168.10.0/32	0	T1	No	<input type="checkbox"/>	

What we do with the Data

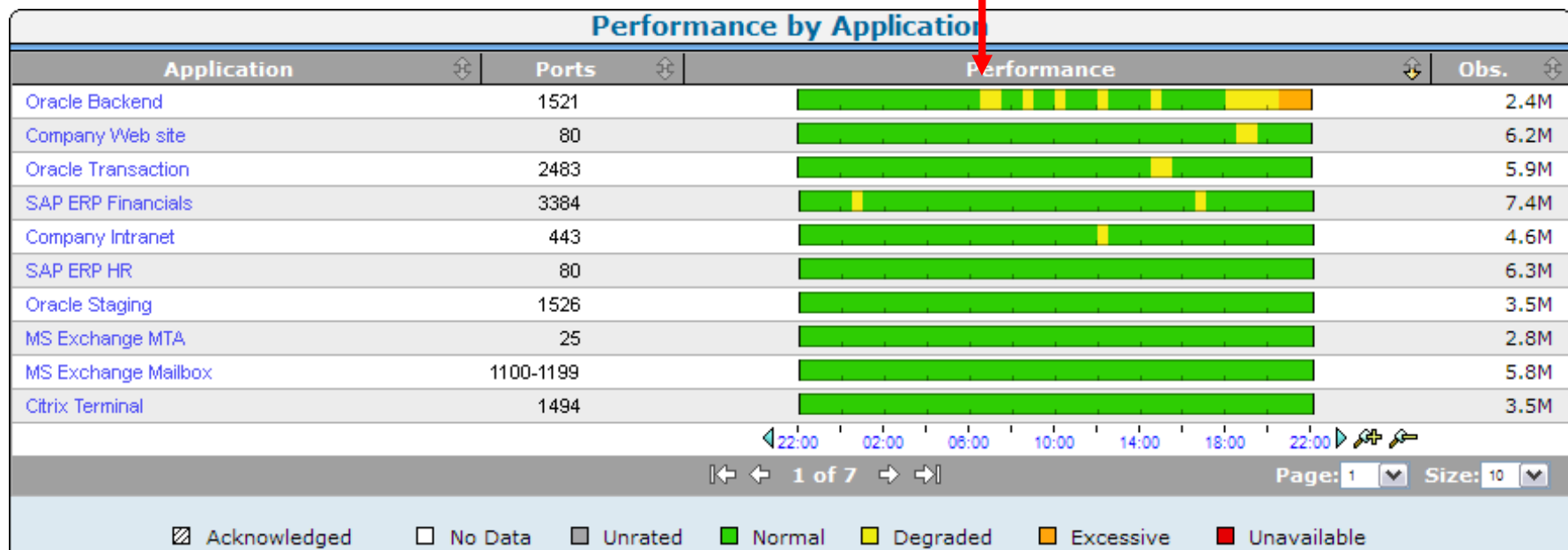
- Baselines normal performance
- Automatically computes thresholds to define Degraded & Excessive performance
- Classifies relative performance for all monitored networks, servers, & applications
- Launches appropriate, automated investigations when performance degrades



Interpretion

Recency:

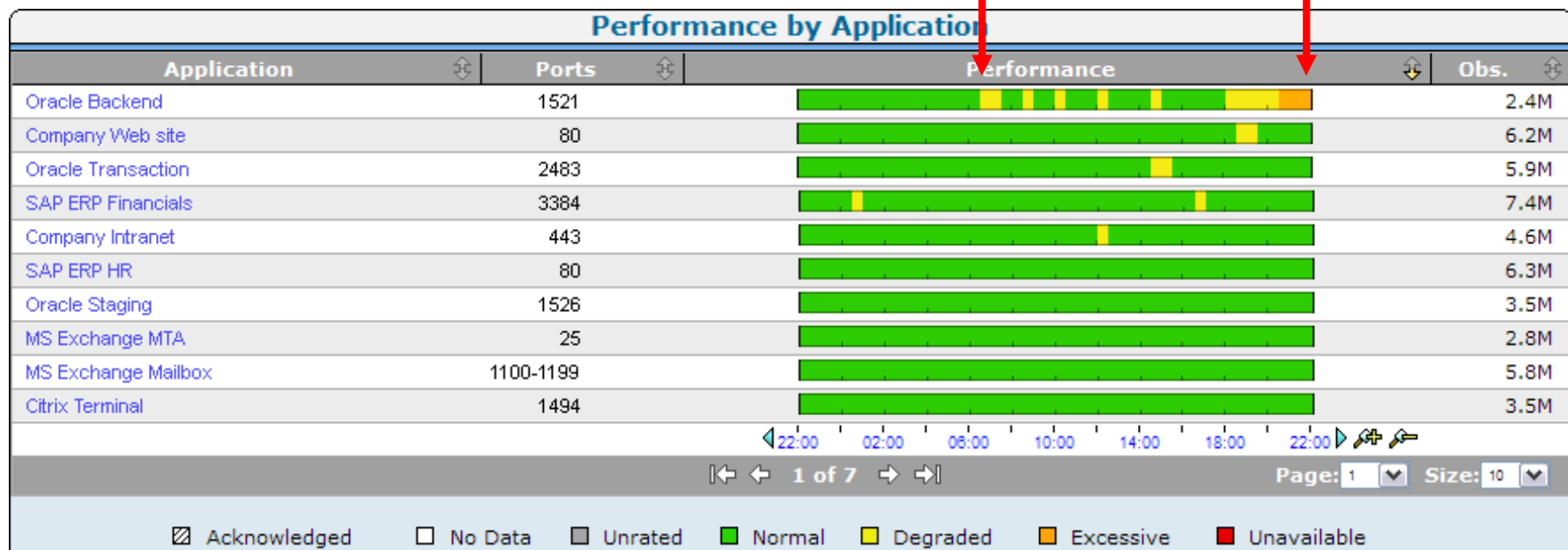
The problem first began shortly after 6:00 AM



Interpretation

Duration:

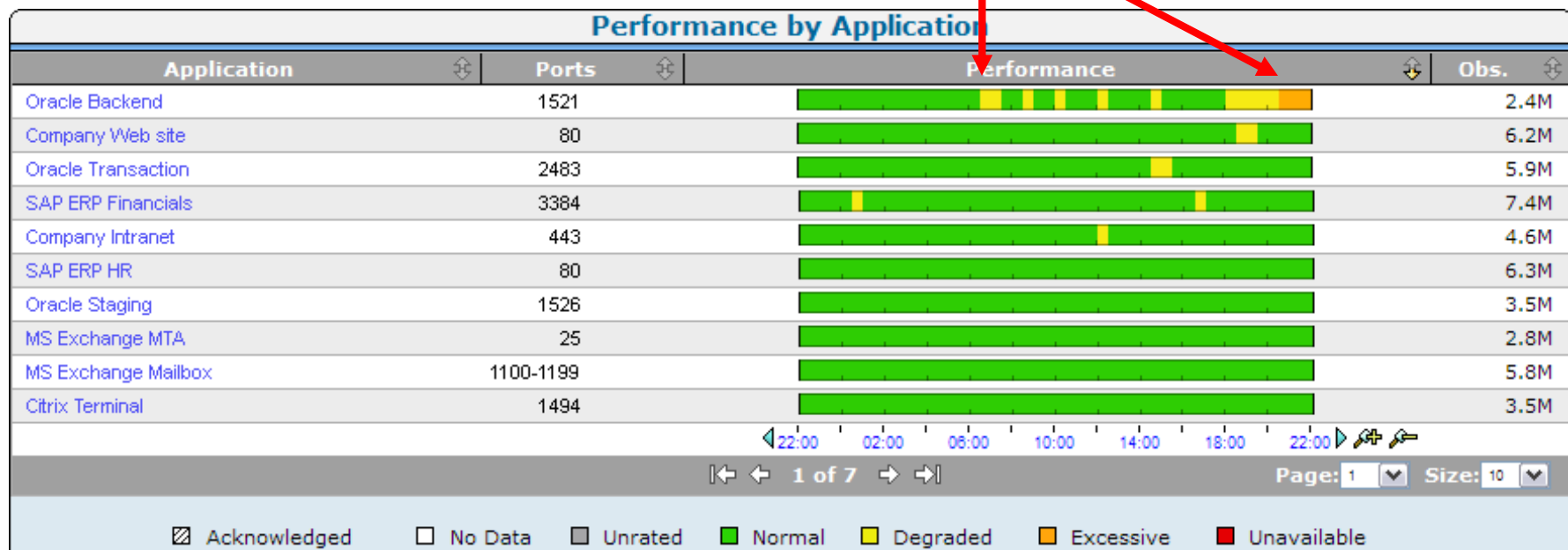
As of 10:00 PM, the problem has been ongoing for 16 hours



Interpretation

Severity:

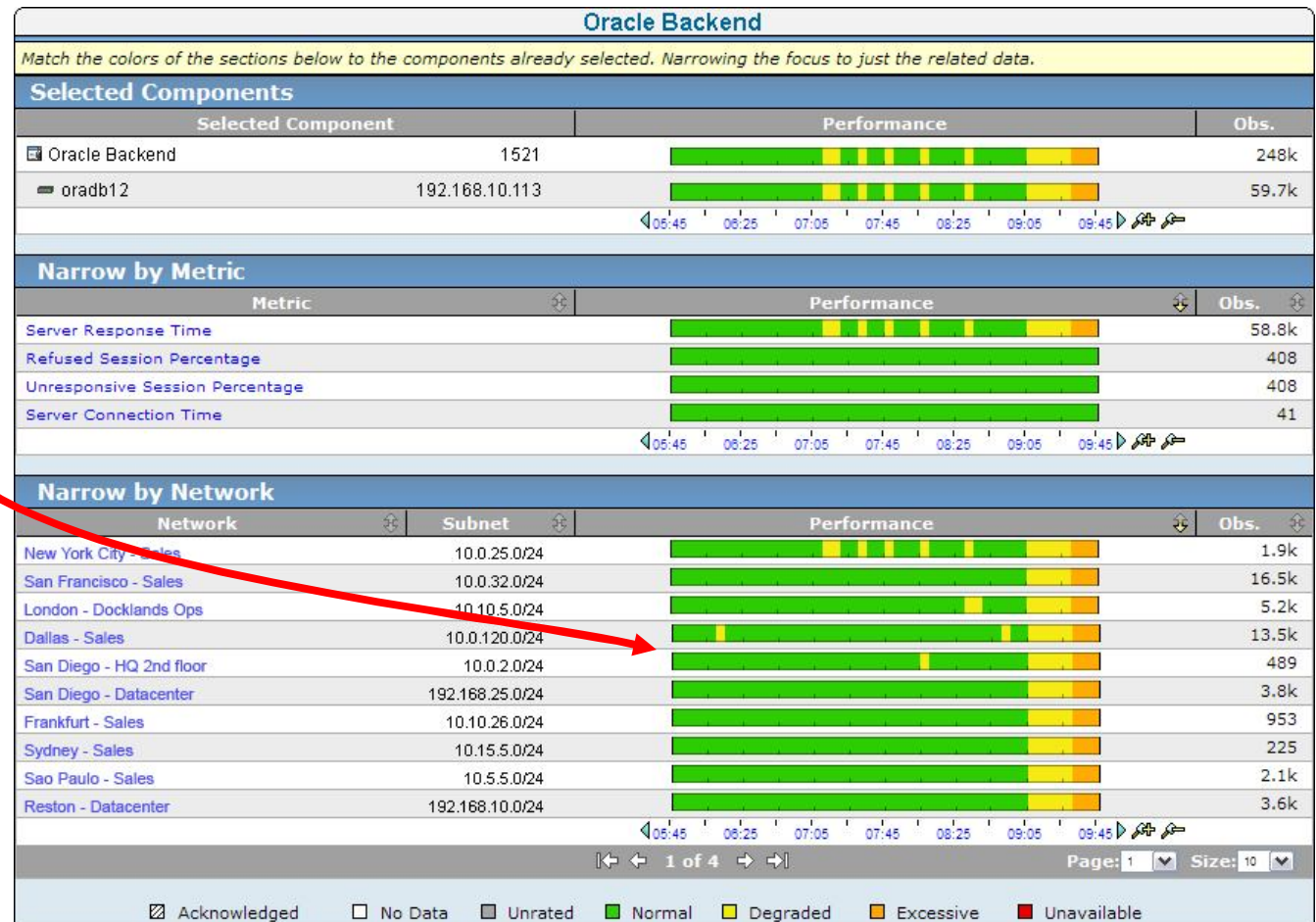
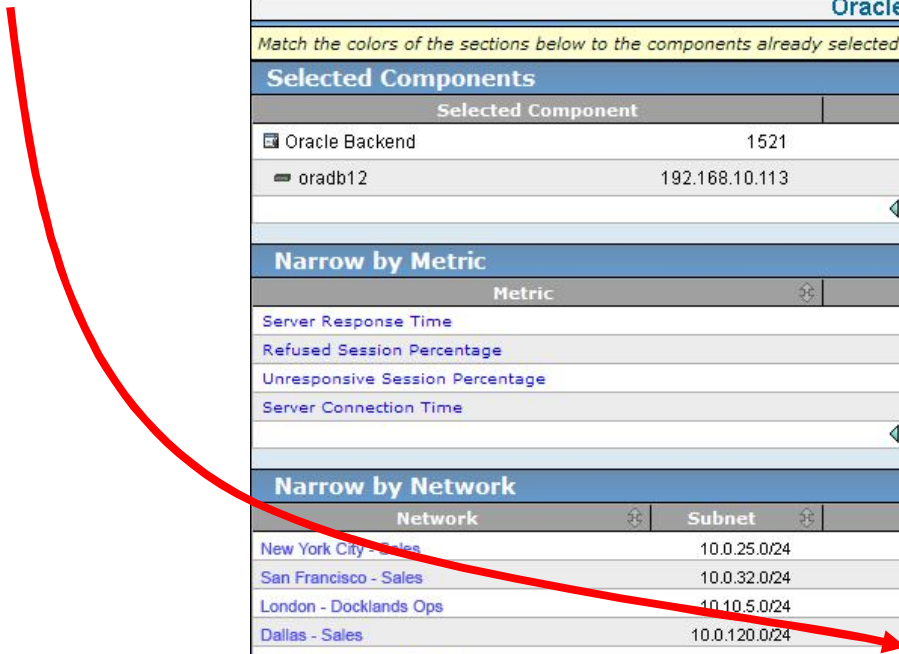
The problem started as a degraded issue and is now excessive



Interpretation

Pervasiveness:

The problem is effecting user across your network



Types of Actions

Incidents launch **actions**.

There are two types of actions:





- Investigations

- Perform the action of the engineer by proxy
- Perform the action immediately—at the time performance degradation is detected

- Notifications

- Alert that a threshold has been crossed
- Available via e-mail or SNMP trap

Available Investigations

Network Incident Response Actions				
Branch Office Investigation				
<i>Below is a list of all the actions for the selected Incident Response.</i>				
Action	Minimum Severity	Duration	Edit	Delete
Send Email Administrator1@Customer.com	Degraded	10 Minutes		
Trace route to network	Excessive	15 Minutes		

- Trace Route
 - Find multiple outbound paths; identify slowest hop
- SNMP Performance Query
 - Collect router and server performance data
- Application Connect Time
 - Time required to connect to the server
- Ping
 - Ping test of server response time
 - Ping test using range of packet sizes
- Packet Capture
 - Gather raw data for analysis in an external tool

From the Dashboard to the Root Cause

NetQoS // NetQoS Performance Center Help | Support | About | Sign Out rbmsel

Report Pages | My Pages | Demo | Management | Engineering | Operations | VMware vCenter

APD - Server Performance

Last day

Group: /Global Enterprise
◀ Day: 17 Apr 2009 CDT ▶

Application Performance Dashboard 17 Apr 2009 CDT

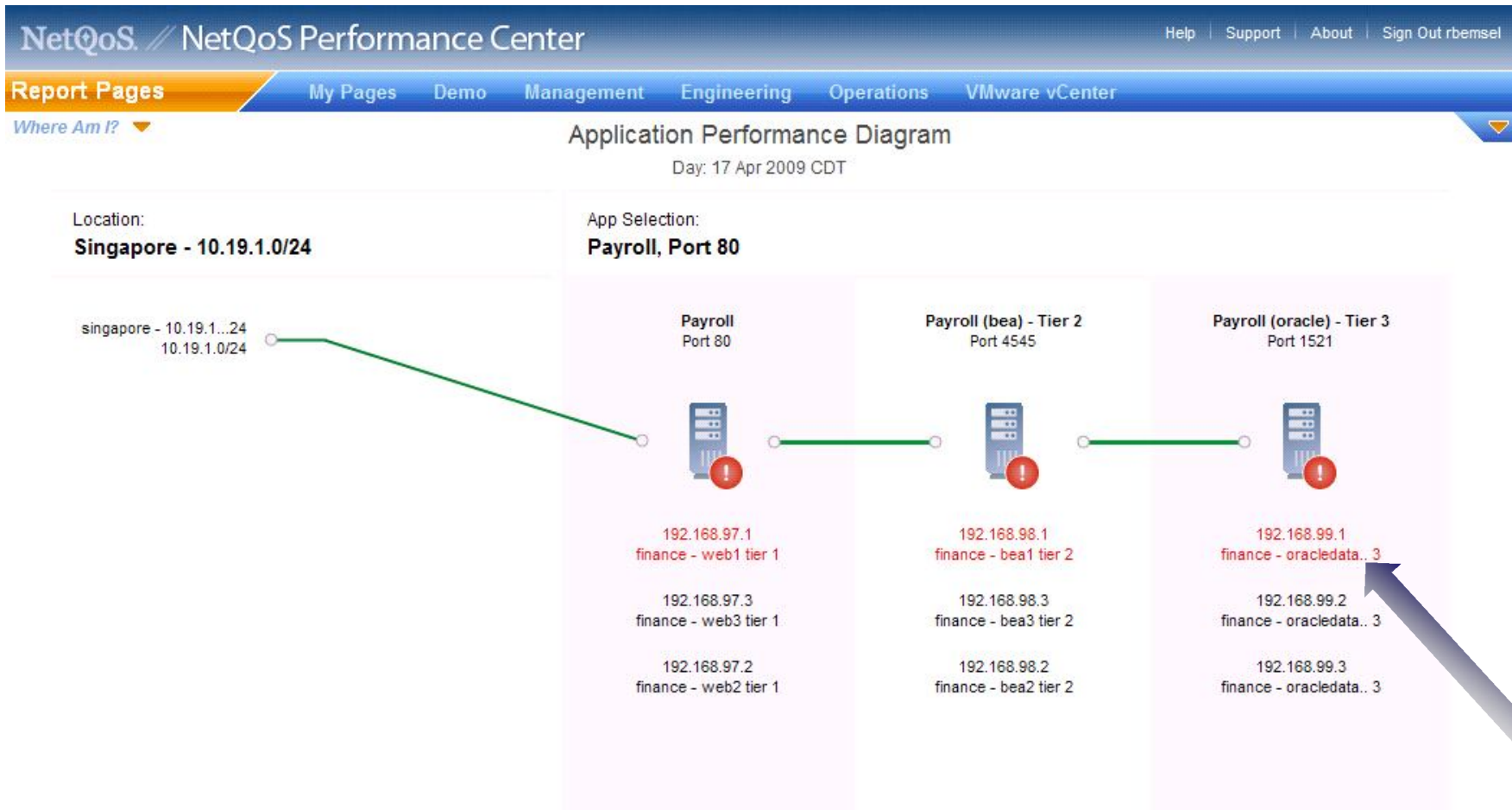
Selected Network Group: Oracle Infrastructure Full Screen

	Payroll	SAP	PeopleSoft
Calgary -- 10.16..24			
Johannesburg -- ...24			
Oaxaca -- 10.168..24			
Raleigh -- 10.16..24			
Singapore - 10.1..24			
Taipei -- 10.168..24			

Unrated Normal Problem

Search:

From the Dashboard to the Root Cause



From the Dashboard to the Root Cause

NetQoS // NetQoS Performance Center

Help | Support | About | Sign Out rbmsel

Report Pages

My Pages

Demo

Management

Engineering

Operations

VMware vCenter

Where Am I? ▾

Print Report | Email Report

Location:

Singapore - 10.19.1.0/24

App Selection:

Payroll , Port 80

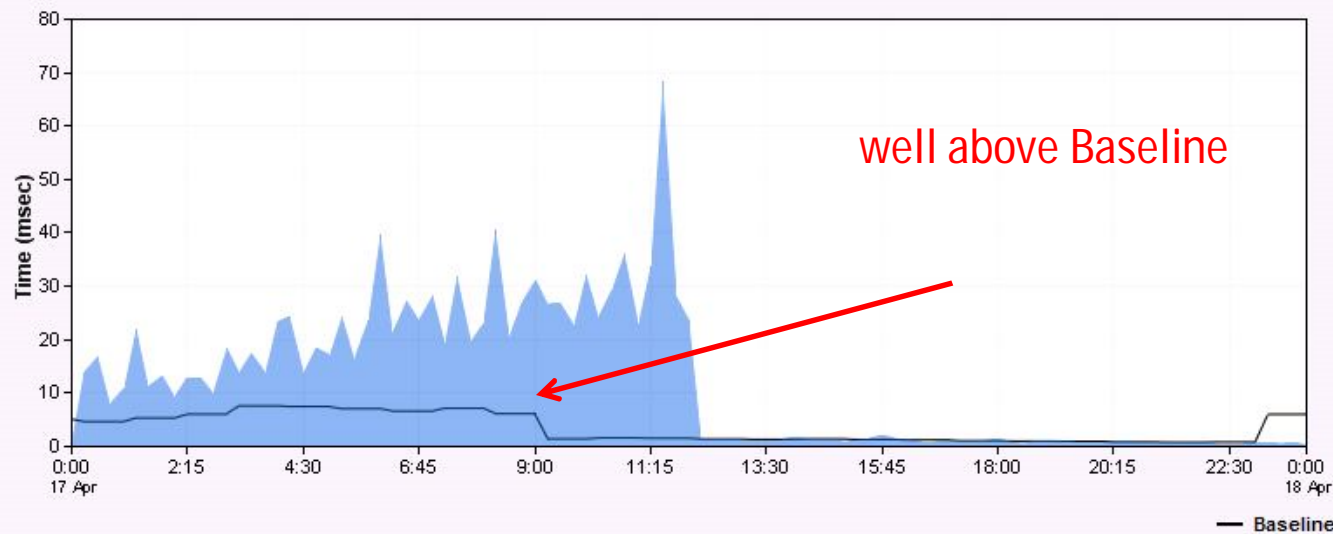
Server Response Time

17 Apr 2009 CDT

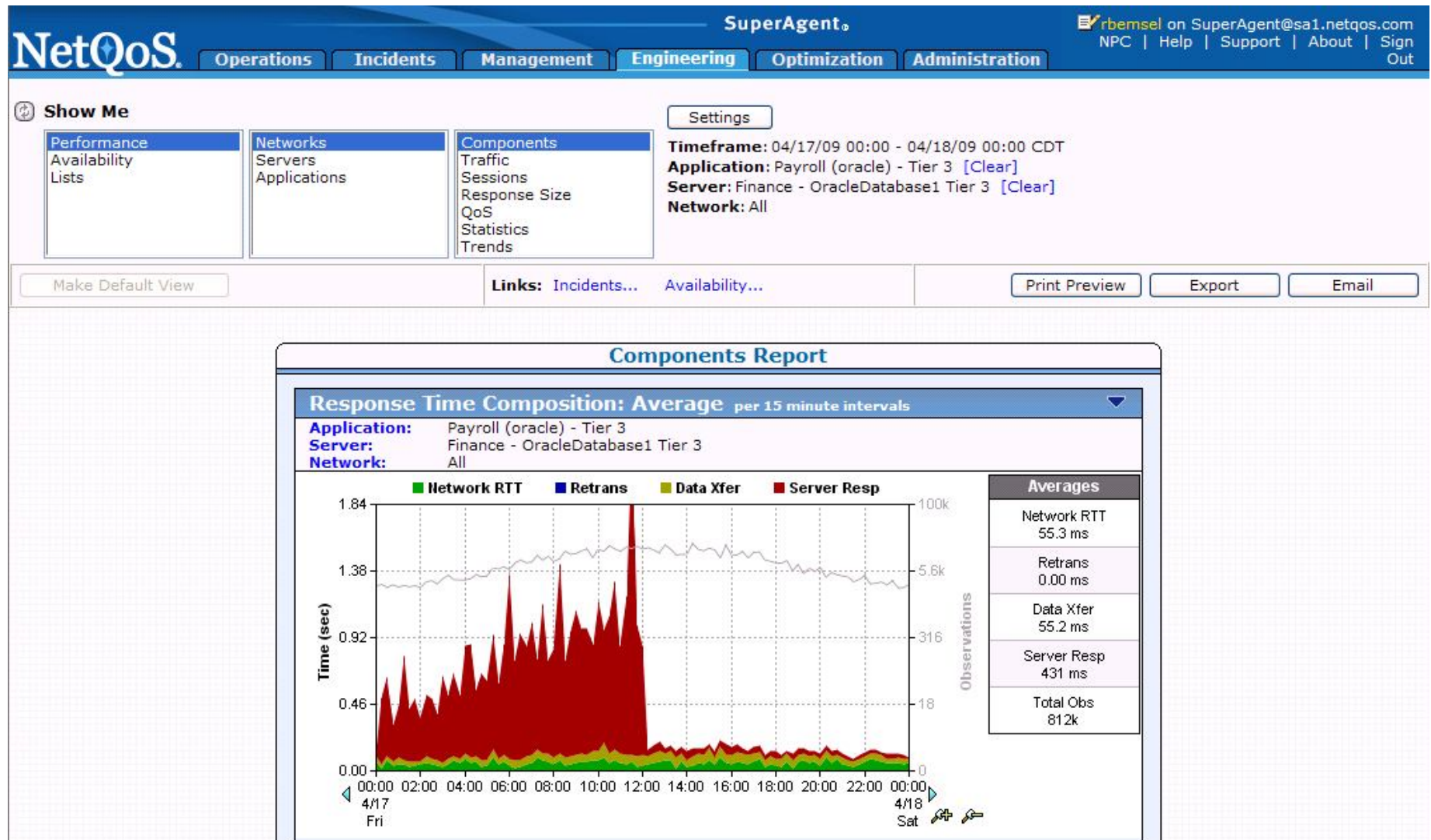
Application: Payroll (oracle) - Tier 3
Server: Finance - OracleDatabase1 Tier 3
Network: All

→ Advanced

Observations: 6.5M



From the Dashboard to the Root Cause



From the Dashboard to the Root Cause

NetQoS SuperAgent rbemsel on SuperAgent@sa1.netqos.com
NPC | Help | Support | About | Sign Out

Operations Incidents Management Engineering Optimization Administration

Show Me Settings

- Overview
- Applications
- Servers
- Networks
- Investigations

Timeframe: 04/17/09 00:00 - 04/18/09 00:00 CDT
Application: Payroll (oracle) - Tier 3 [Clear]
Server: Finance - OracleDatabase1 Tier 3 [Clear]
Network: All
Metric: All Relative Metrics

Incident State: Open and Closed
Minimum Severity: Degraded for 10 min
View By: Incident Lists

Make Default View Explore Find Incident Print Preview Export Email

Network Incidents

Insufficient Data or No Data Available to Produce Results.

Acknowledged
 No Data
 Unrated
 Normal
 Degraded
 Excessive
 Unavailable

Server Incidents

Incident #	Target	Application	Severity	Time	Duration	
6	Finance - OracleDatabase1 Tier 3 192.168.99.1	Payroll (oracle) - Tier 3	Closed	04/17/2009 09:00	4 hr	<input type="checkbox"/>

Acknowledged
 No Data
 Unrated
 Normal
 Degraded
 Excessive
 Unavailable

Server Incident #6

Incident Details

Number : #6	Time Frame : 04/17/2009 09:00 - 04/17/2009 13:00 CDT (4 hr)
Server : Finance - OracleDatabase1 Tier 3	Investigations : 2 related
Severity : Excessive	Status : Closed

Incident Investigations

Target	Investigation Type	Investigated On
View Finance - OracleDatabase1 Tier 3 192.168.99.1/10	Ping Sample	04/17/2009 09:05 CDT
View Finance - OracleDatabase1 Tier 3 192.168.99.1/10	SNMP Poll	04/17/2009 09:05 CDT

From the Dashboard to the Root Cause

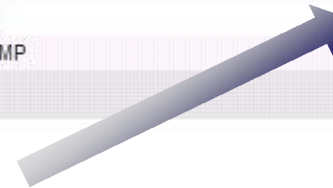
Investigations - All

17 Apr 2009 CDT

Target Type	Target	Investigation	Investigated On
Server	Finance - OracleDatabase1 Tier 3	Ping Response Time	04/17/09 09:05 CDT
Server	Finance - OracleDatabase1 Tier 3	Performance via SNMP	04/17/09 09:05 CDT

Search:

Show Top:



Ping Response Time Investigation

Server: Finance - OracleDatabase1 Tier 3 (192.168.99.1)
 Date: 04/17/2009 09:05 CDT
 Investigator: Collector 1 (1.0.1.1)

Server		Packets			Round Trip Time		
Name	Address	Sent	Received	Lost	Min	Max	Avg
Finance - OracleDatabase1 Tier 3	192.168.99.1	10	10	0	1 ms	2 ms	1 ms

Chart of Packet Response Times

Table of Packet Response Times

Table of Packet Response Times

Packet	Reply From	Size	Time To Live	Response Time
1	192.168.99.1	64	253	2 ms
2	192.168.99.1	64	253	2 ms
3	192.168.99.1	64	253	1 ms
4	192.168.99.1	64	253	2 ms
5	192.168.99.1	64	253	2 ms
6	192.168.99.1	64	253	2 ms
7	192.168.99.1	64	253	2 ms
8	192.168.99.1	64	253	2 ms
9	192.168.99.1	64	253	1 ms
10	192.168.99.1	64	253	2 ms

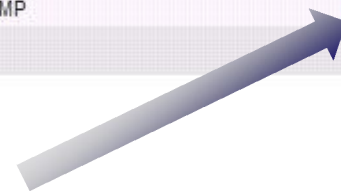
From the Dashboard to the Root Cause

Investigations - All

17 Apr 2009 CDT

Target Type	Target	Investigation	Investigated On
Server	Finance - OracleDatabase1 Tier 3	Ping Response Time	04/17/09 09:05 CDT
Server	Finance - OracleDatabase1 Tier 3	Performance via SNMP	04/17/09 09:05 CDT

Show Top: 10



Performance via SNMP Investigation

Server: Finance - OracleDatabase1 Tier 3 (192.168.99.1)
 Date: 04/17/2009 09:05 CDT
 Investigator: Collector 1 (1.0.1.1)

Device		Performance	
Name	Address	CPU	Memory
Finance - OracleDatabase1 Tier 3	192.168.99.1	52%	10.5%

Agent Name: Finance - OracleDatabase1 Tier 3
Description: Hardware: x86 Family 15 Model 2 Stepping 4 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
Up Since: 03/22/2009 06:43 CDT (03/22/2009 11:43 GMT)
Contact: DSS
Location: Finance - OracleDatabase1 Tier 3
Sampled Over: 60 seconds

Subsystem	Size	In Use	Free	% Free
Memory	1023.5 MB	107.4 MB	916.1 MB	89.5%
Hard Drive C: Label:Dell Server Serial Number c492b9fe	19.5 GB	7.5 GB	12.1 GB	61.7%
Hard Drive E: Label:New Volume Serial Number 6a2d7bd2	48.8 GB	bytes	48.8 GB	100.0%

Processor	In use over the last minute
1	90%
2	35%
3	31%
4	53%

Finance - OracleDatabase1 Tier 3 - Ethernet

	In	Out
IP Address	192.168.99.1	200.0 M
Physical Address	e2f89bf2298c5700	21.9 K
Status	Up	0
Speed	1.0 Gbit/s	30

Top CPU Processes

Id	Process	Memory	CPU
1020	backup.exe	87.9 MB	81.84%
1008	cctfmon.exe	7.9 MB	7.37%
1015	svchost.exe	6.7 MB	6.25%
1013	msdtc.exe	4.6 MB	4.32%
1003	ccEvtMgr.exe	123 KB	0.11%

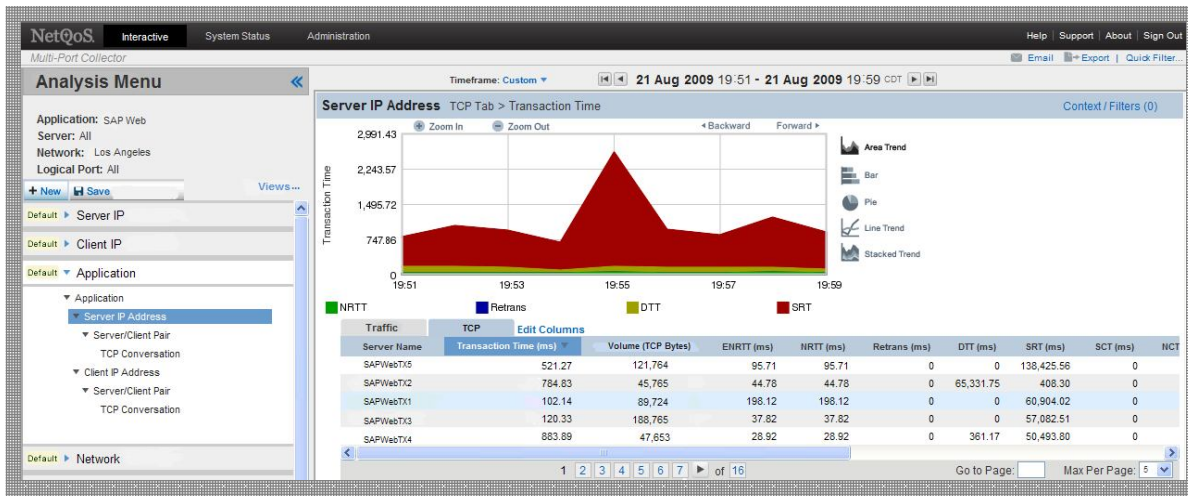
Top Memory Processes

Id	Process	Memory	CPU
1020	backup.exe	87.9 MB	81.84%
1008	cctfmon.exe	7.9 MB	7.37%
1015	svchost.exe	6.7 MB	6.25%
1013	msdtc.exe	4.6 MB	4.32%
1003	ccEvtMgr.exe	123 KB	0.11%

MultiPort Collector

Multi-Port Collector

- High-performance, port-dense Collector for APM solution.
- Interactive detailed session analysis.
- Performance and volume data at 1-min granularity.
- Complements higher-level reporting in the NPC dashboard.



Use Case

Performance Center Link to the Incidents Page

NetQoS SuperAgent. Operations Incidents Management Engineering Administration

Show Me: Overview, Applications, Servers, Networks, Investigations

Performance: Investigations, Compare, History

Settings: Application: SAP Web, Server: #96706, Network: Raleigh, Metric: All Server Metrics

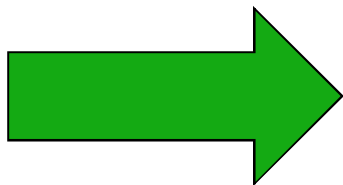
Links: Engineering Availability

Buttons: Make Default View, Explore, Acknowledge, Session Analysis, Print Preview, Export, Email

Server Incident #96706

Incident Details: Number: #96706, Server: SAPTX2, Severity: Excessive, Time Frame: 08/27/09 8:50 - 08/27/09 9:10 EST (20 min), Investigations: 1 related, Status: Closed

Select **Session Analysis** to drill to Multi-Port Collector with pre-filtered context



NetQoS Interactive System Status Administration

Multi-Port Collector

Analysis Menu: Application: SAP Web, Server: All, Network: Raleigh, Logical Port: All

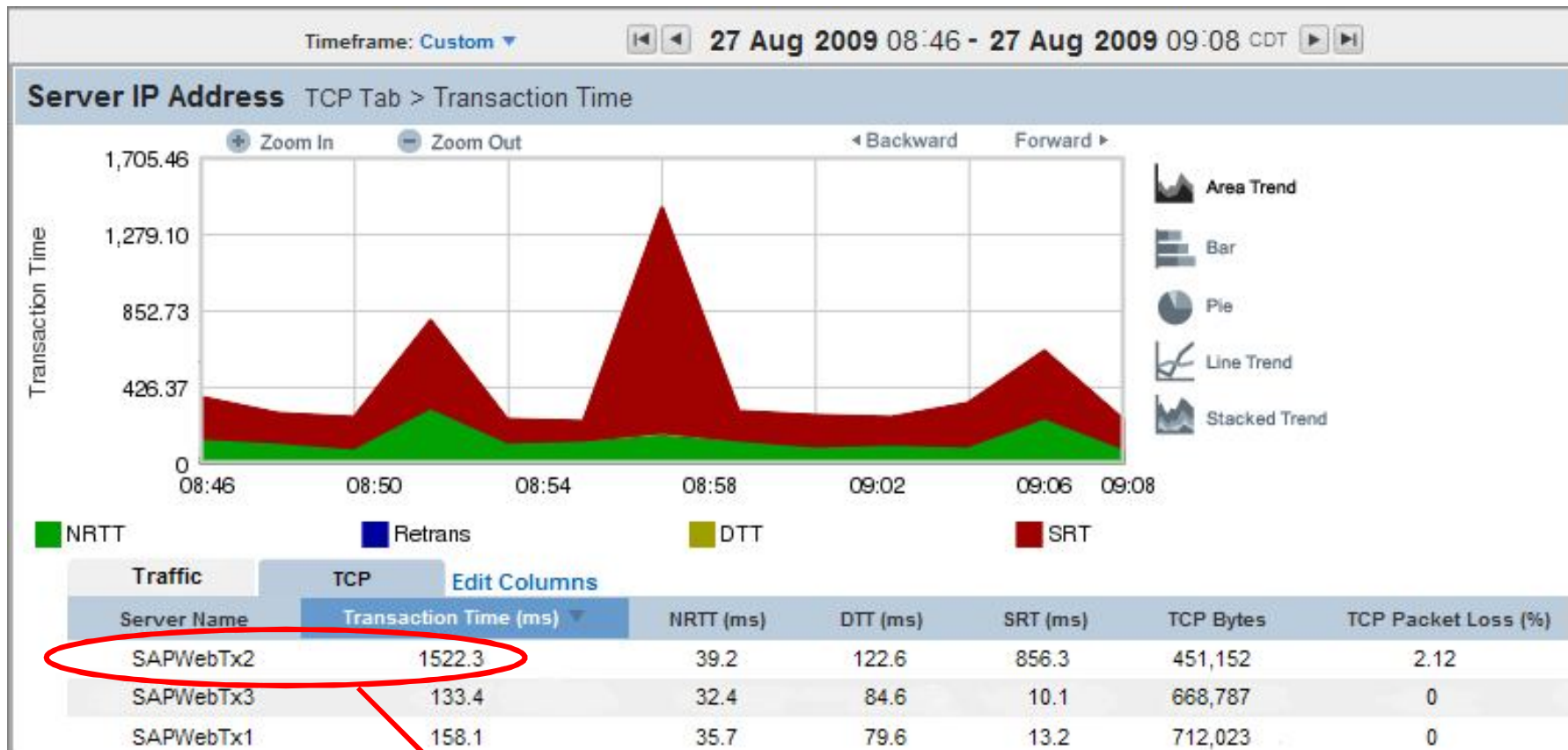
Server IP Address TCP Tab > Transaction Time

Timeframe: Custom 27 Aug 2009 08:46 - 27 Aug 2009 09:08 CDT

Transaction Time graph showing NRTT, Retrans, DTT, SRT

Traffic	TCP	Edit Columns							
Server Name	Transaction Time (ms)	Volume (TCP Bytes)	ENRIT (ms)	NRTT (ms)	Retrans (ms)	DTT (ms)	SRT (ms)	SCT (ms)	NCT
SAPWebTX5	521.27	121,764	95.71	95.71	0	0	138,425.56	0	
SAPWebTX2	784.83	45,765	44.78	44.78	0	65,331.75	408.30	0	
SAPWebTX1	102.14	89,724	198.12	198.12	0	0	60,904.02	0	
SAPWebTX3	120.33	188,765	37.82	37.82	0	0	57,082.51	0	
SAPWebTX4	883.89	47,653	28.92	28.92	0	361.17	50,493.80	0	

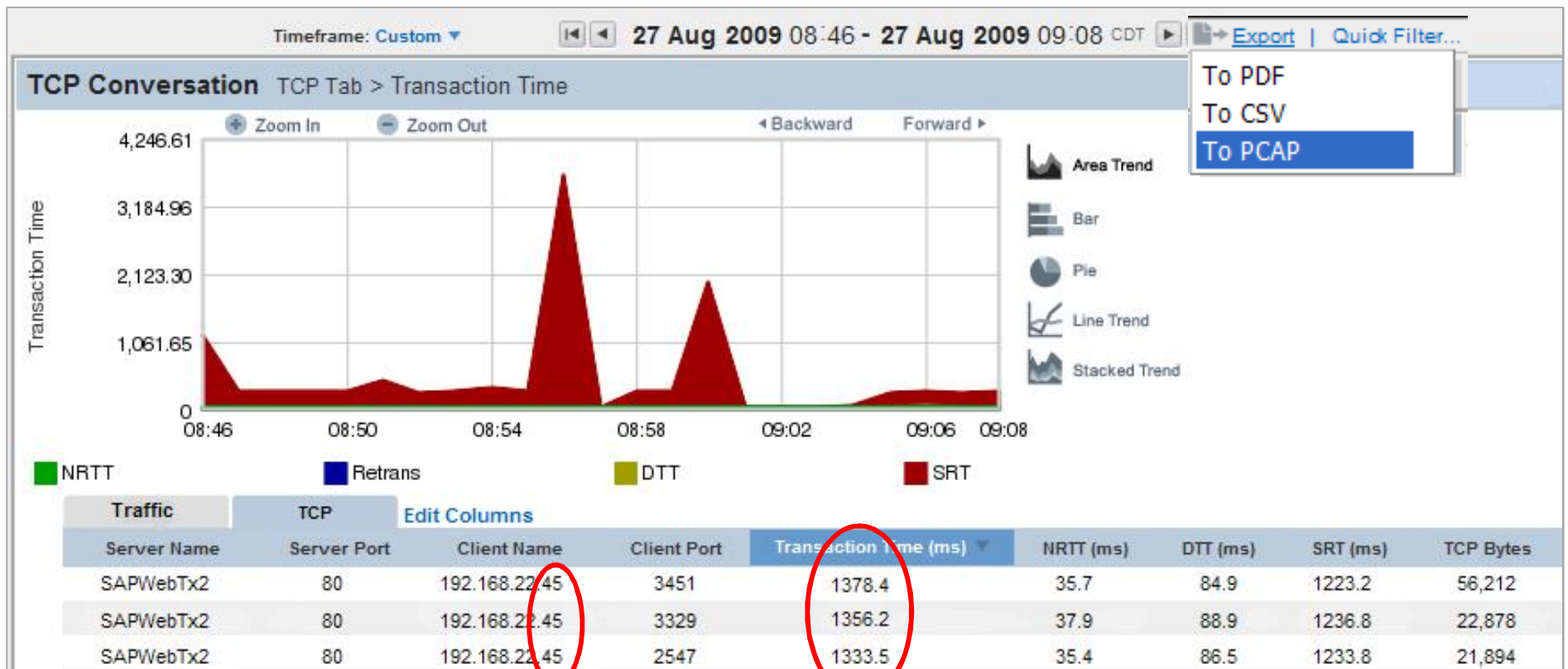
Application Performance by Server



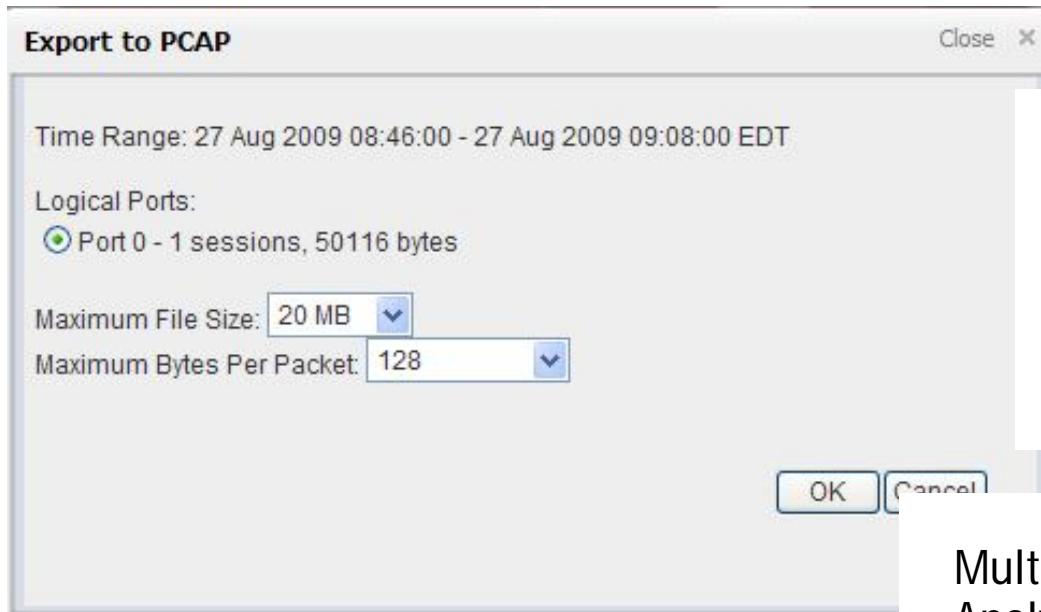
Drill Down and Apply As Filter
Apply As Filter

Locate the Worst-Performing Server

Performance for an Affected Client



Export Packets for Further Analysis



Multi-Hop
Analysis

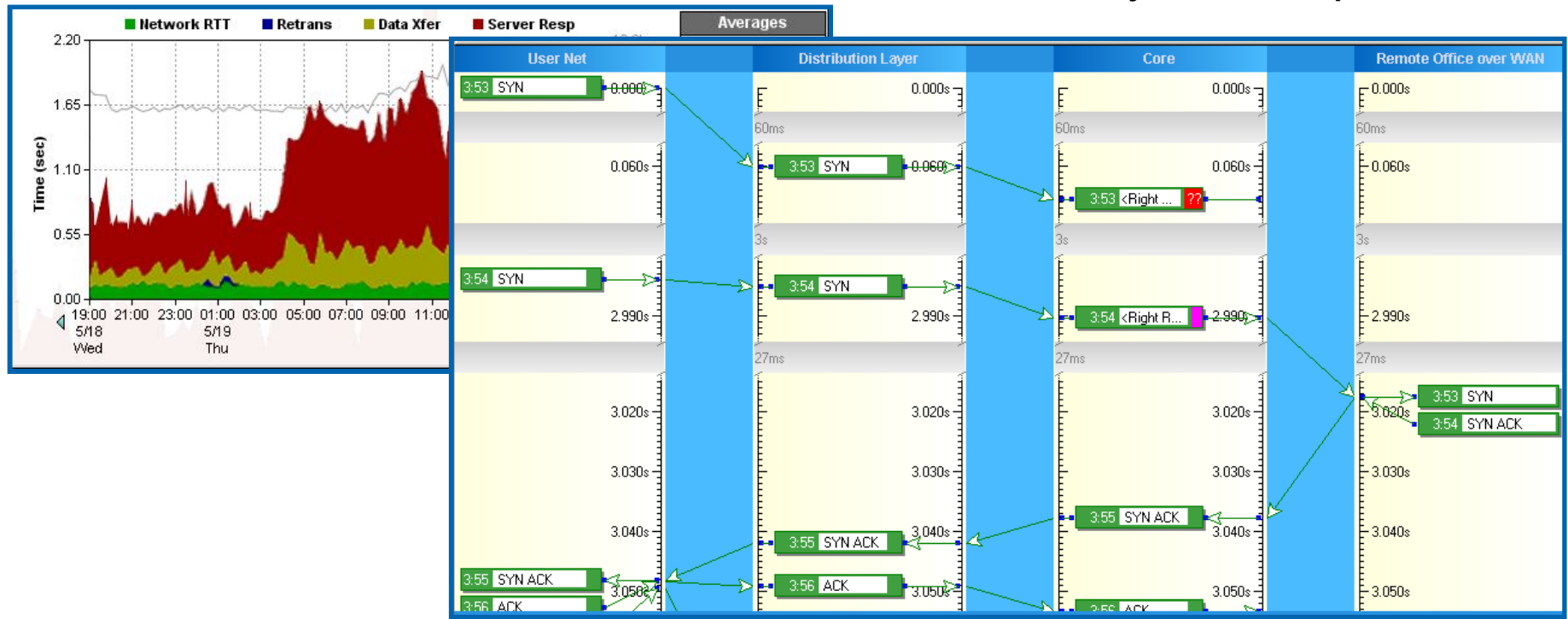
Connection
Dynamics

Long Term packet capture and analysis

Long-term Packet Capture



- > Retrospective packet analysis with stream reconstruction
- > Root cause analysis via automatic investigations
- > TiVo® for your network - storage up to 200 TB
- > Multi-hop analysis, connection dynamics, and 3-pane decode

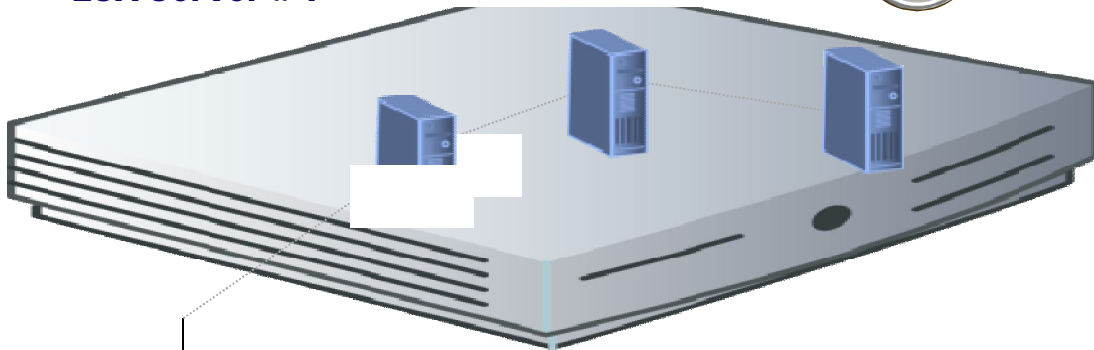


Virtual Collector

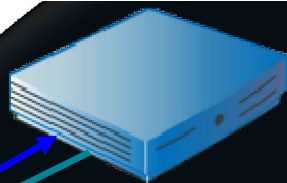
Monitoring Challenges



ESX Server #1



SuperAgent Collector

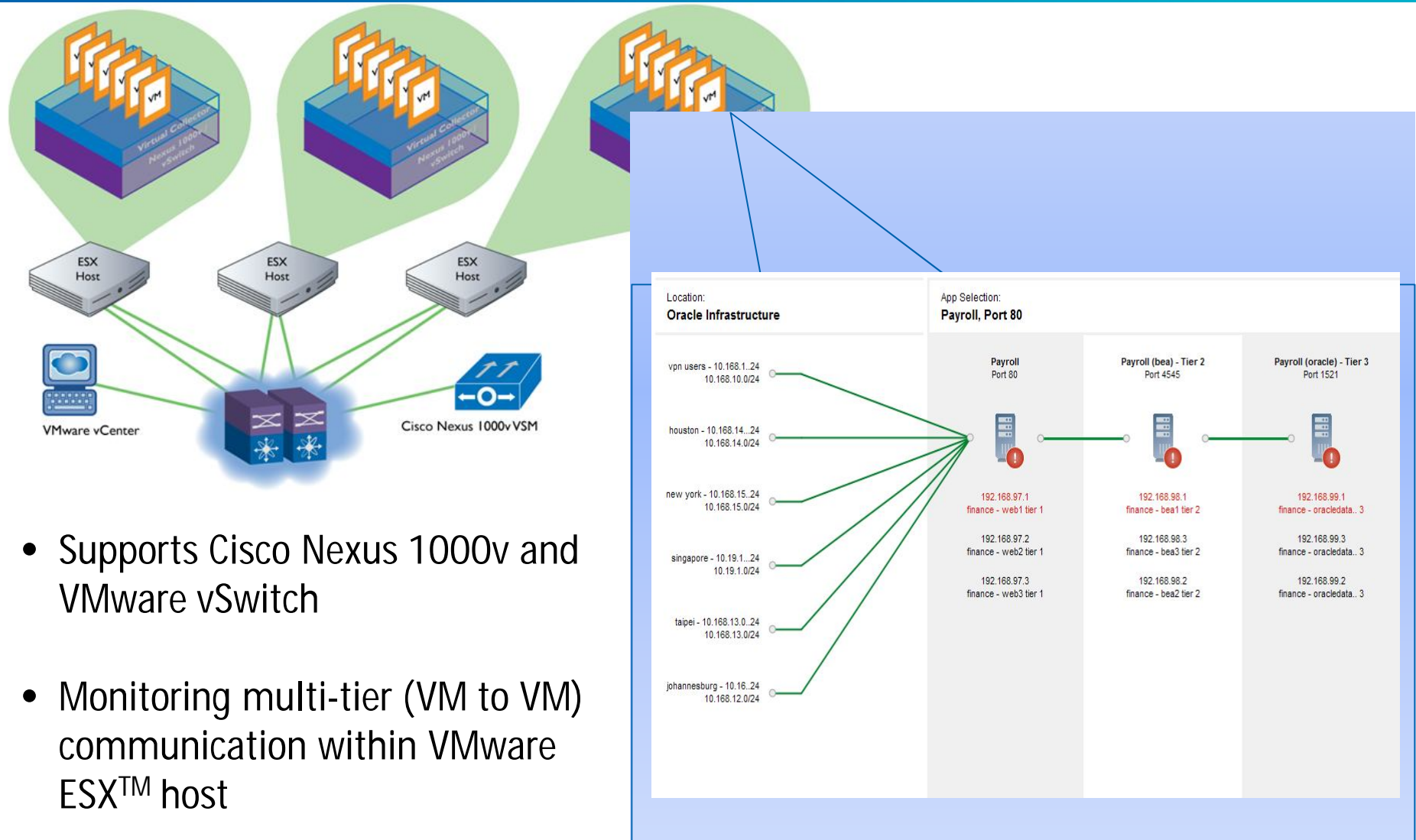


Data Center Switch



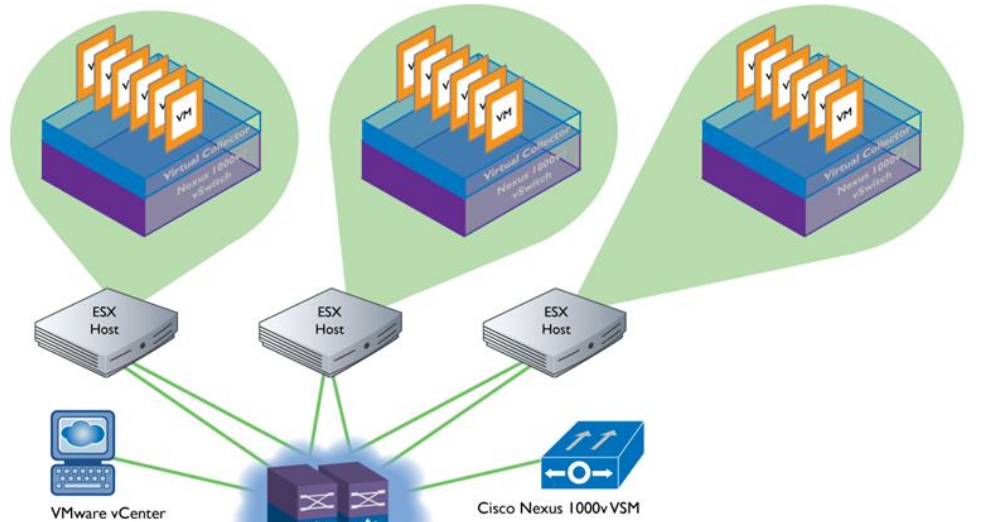
ESX Server #2

Response Time Virtual Collector

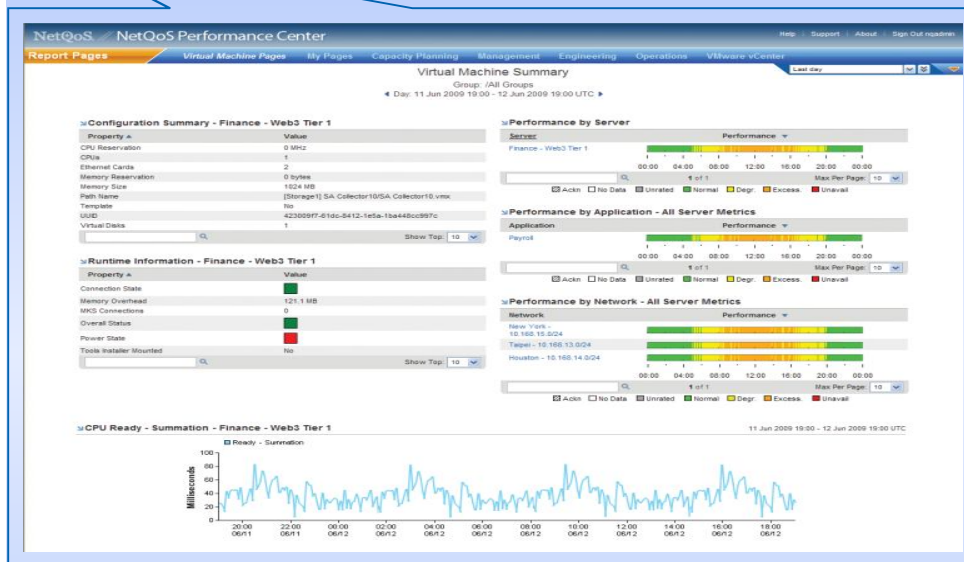


- Supports Cisco Nexus 1000v and VMware vSwitch
- Monitoring multi-tier (VM to VM) communication within VMware ESX™ host

VMware vCenter™ API Integration

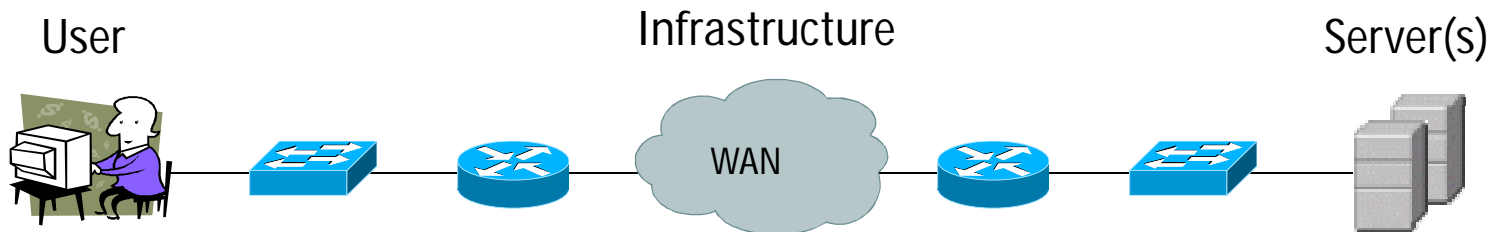


- NetQoS Performance Center response time views alongside VM device level information
- Trend reports highlight performance bottlenecks



Summary

Summary



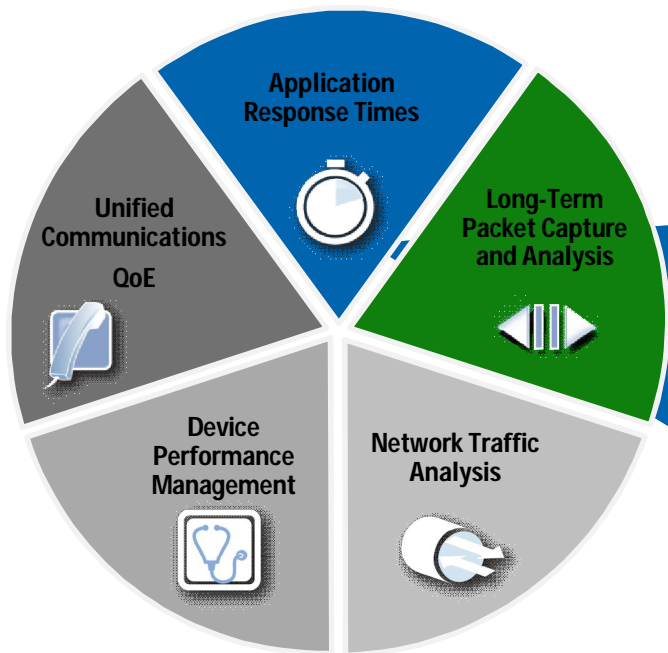
Solve performance problems faster by isolating the source to the application, server, or network.

- Understand normal performance through baselines
- Receive automatic alerts when performance degrades
- Quickly identify the source of performance problems
- Automatically gather diagnostic data through filtered packet captures, SNMP polling, and traceroutes

Mitigate risks from planned changes and unexpected events with before and after analysis.

Overall Dashboard

Overall Dashboard



- > Customizable, role-based access and reporting
- > Web console with top-down and drill-down navigation
- > Single interface for problem discovery down to root cause
- > Correlated key metrics for infrastructure planning and decision support
- > Third-party data integration



Thank you!