Infrastructure and Services Track

The Future of Network Management: *Over Niagara Falls in a Barrel*

Eric Siegel, Senior Analyst, Burton Group
esiegel@burtongroup.com

INTEROP®

BUSINESS. TECHNOLOGY.
ONE WEEK. ONE PLACE.

Agenda

- Overview
  - Challenges facing network management
  - Possible solutions
  - Tools
- Panel discussion with:
  - Gnanesh Dholakia, Senior Marketing Manager, CA (Concord, Spectrum, Wily)
    - www.ca.com/
  - Chris Greer, Network Analyst, Network Protocol Specialists
    - www.nps-llc.com/
  - Naresh Kannan, Business Strategy Director, Enterprise Performance Management, Fluke Networks
    - www.flukenetworks.com/
  - Terry Slattery, Founder and CTO, Netcordia
    - www.netcordia.com/

The Challenges

- Network is the new backplane
  - Network is now “inside” the transaction, not “outside”
- Multiservice
  - VoIP, videoconferencing, Web Services, transactions, IMs, file transfer, mail ... and all at different QoS levels
- Real-time
  - We can’t wait for a 5-minute poll cycle
- Opaque system elements
  - external network suppliers
  - encryption and “data reduction” data compression
- Constant change; loss of configuration information
  - We don’t know the effect of an element’s failure until it happens
  - Troubleshooters don’t know the production environment
- Test environment isn’t comprehensive
  - Subtle problems aren’t found during testing
- Many different organizations involved

from “The Big Book of Canada” by Christopher Moore; illus by Bill Slavin

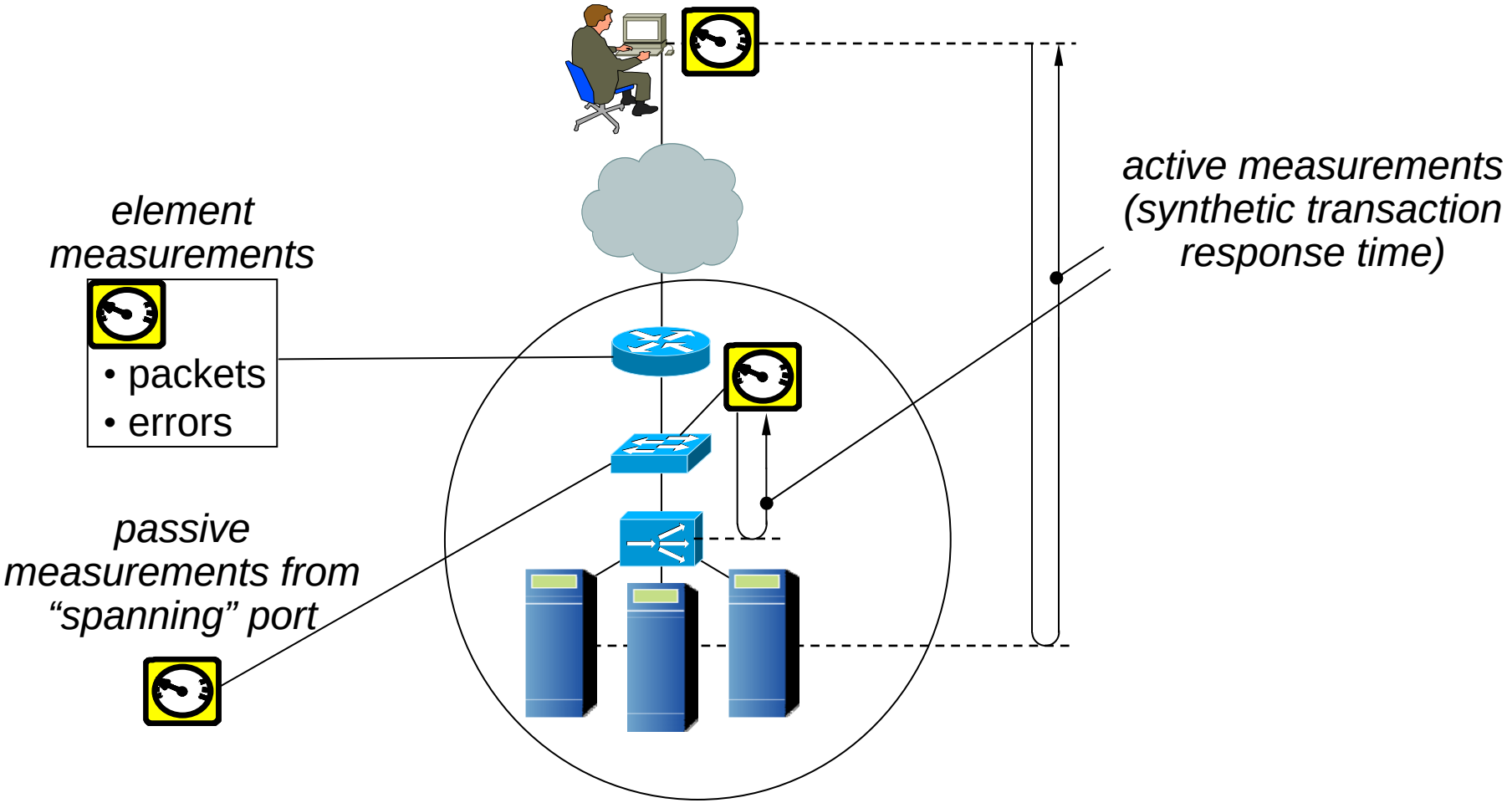
Solutions

- Good metrics and logs

... *leading to*...

- Quick incident management
- Detailed diagnostics for problem analysis

Measurement Types



Solutions: Good Metrics and Logs

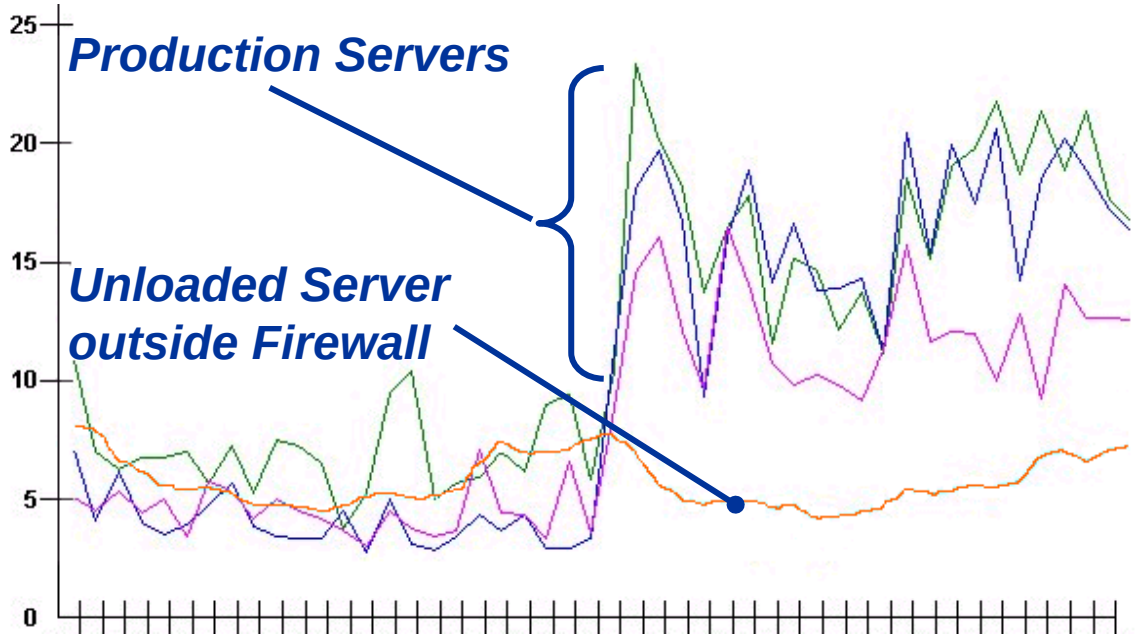
- Measure what is relevant, not just what is easy to measure
  - Which *services* are important to your users?
  - If a metric shows a problem exists, what else do you need to know?
- Clean up measurements
  - Remove erroneous measurements
  - Use percentiles or “geometric deviations”
    - Averages and standard deviations are usually *very* misleading!
  - Weight metrics appropriately
  - Set alarm thresholds appropriately
- Track configuration changes
- Ensure that applications provide usable alarms and logs
  - Applications should log errors they encounter
- Be sure measurement system is scalable
  - Use distributed measurement

Solutions: Quick Incident Management

- Daily audit to find problems before they grow
  - Configuration issues
  - Performance issues
- Design for “triage”
  - Identify “well-known” incidents (and the fix for them!)
  - Isolate to the responsible organization *quickly, credibly*
  - Involve everyone in planning incident responses
    - Network, Security, Servers, Middleware, Appliances
    - Create clear diagnostic demarcation points
    - Design the system for easy incident detection and triage
  - Avoid brittle solutions that must be re-designed because of minor changes to the environment
  - (example on next slide!)

Solutions: Triage Measurement

- Example: “network” *vs*. “server” triage
  - Using active measurements from outside server room

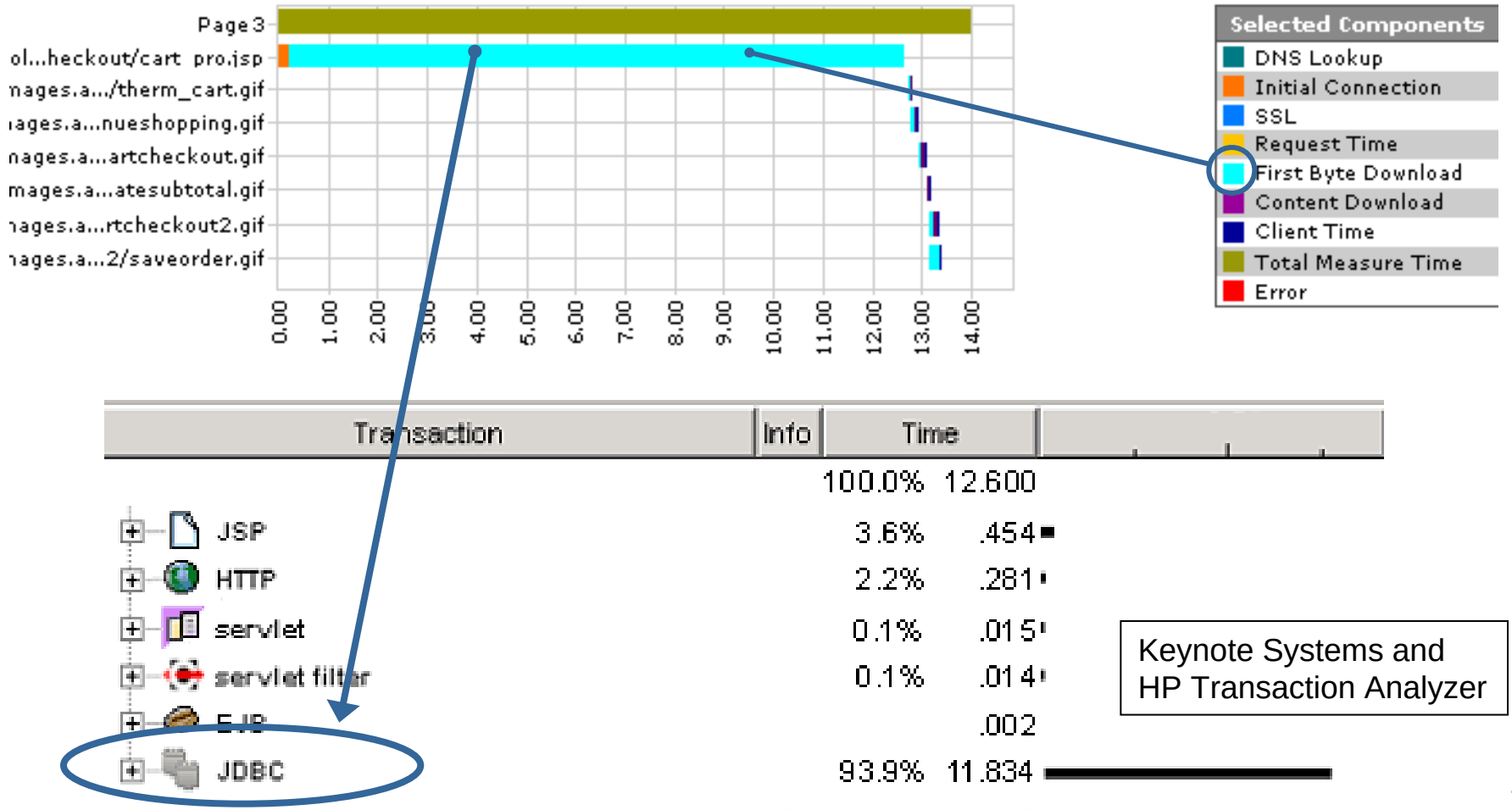


- Think of where *you* could use triage:
  - Internet access paths
  - DNS, DHCP, Identity database performance...

Solutions: Detailed Diagnostics

- Design systems and applications for diagnosis
  - Error logging and log analysis
  - "Dye tracing" of transactions
    - (example on next slide!)
    - Tools that programmers will understand
    - Can also provide summary metrics
  - "Root cause" tools
  - Remote "sniffing" and monitoring ("spanning") ports
- Configuration database and audit
- Arrange for outside diagnostics experts "on call"
  - Where will you find them?
  - When will you decide to call them?
  - How will visiting experts learn your system?

Solutions: Detailed Diagnostics



Keynote Systems and HP Transaction Analyzer

(*a small sample of*) Tools

- Measurement
  - Probes from Attachmate NetIQ, Brix, CA, Compuware ClientVantage, Fluke Networks, HP Internet Services and SiteScope, NetScout, Network Physics, Symphoniq TrueVue
    - Active probes: Cisco IP SLA ("SAA"), Juniper RPM; F5 monitors
    - "Agentless" (passive, server-side) web probes: CA (Wily) Customer Experience Manager, Compuware ClientVantage Agentless Monitoring, Coradiant TrueSight
  - Services from Gomez, Keynote
- Audit
  - CA (Wily) Introscope ChangeDetector, Netcordia NetMRI
- "Root Cause" analysis
  - CA Spectrum, EMC SMARTS, InfoVista VistaInsight for Networks
- Dye Tracing
  - CA (Wily), Compuware Vantage Analyzer, HP Transaction Analyzer, IBM Tivoli Composite Application Manager, Quest Software PerformaSure, Symphoniq TrueVue

Panel Discussion

- Panel discussion with:
  - Gnanesh Dholakia, Senior Marketing Manager, CA (Concord, Spectrum, Wily)
    - www.ca.com/
  - Chris Greer, Network Analyst, Network Protocol Specialists
    - www.nps-llc.com/
  - Naresh Kannan, Business Strategy Director, Enterprise Performance Management, Fluke Networks
    - www.flukenetworks.com/
  - Terry Slattery, Founder and CTO, Netcordia
    - www.netcordia.com/