



NetworkPhysics



network application

management

## ***Leveraging Infrastructure Data for Performance Management***

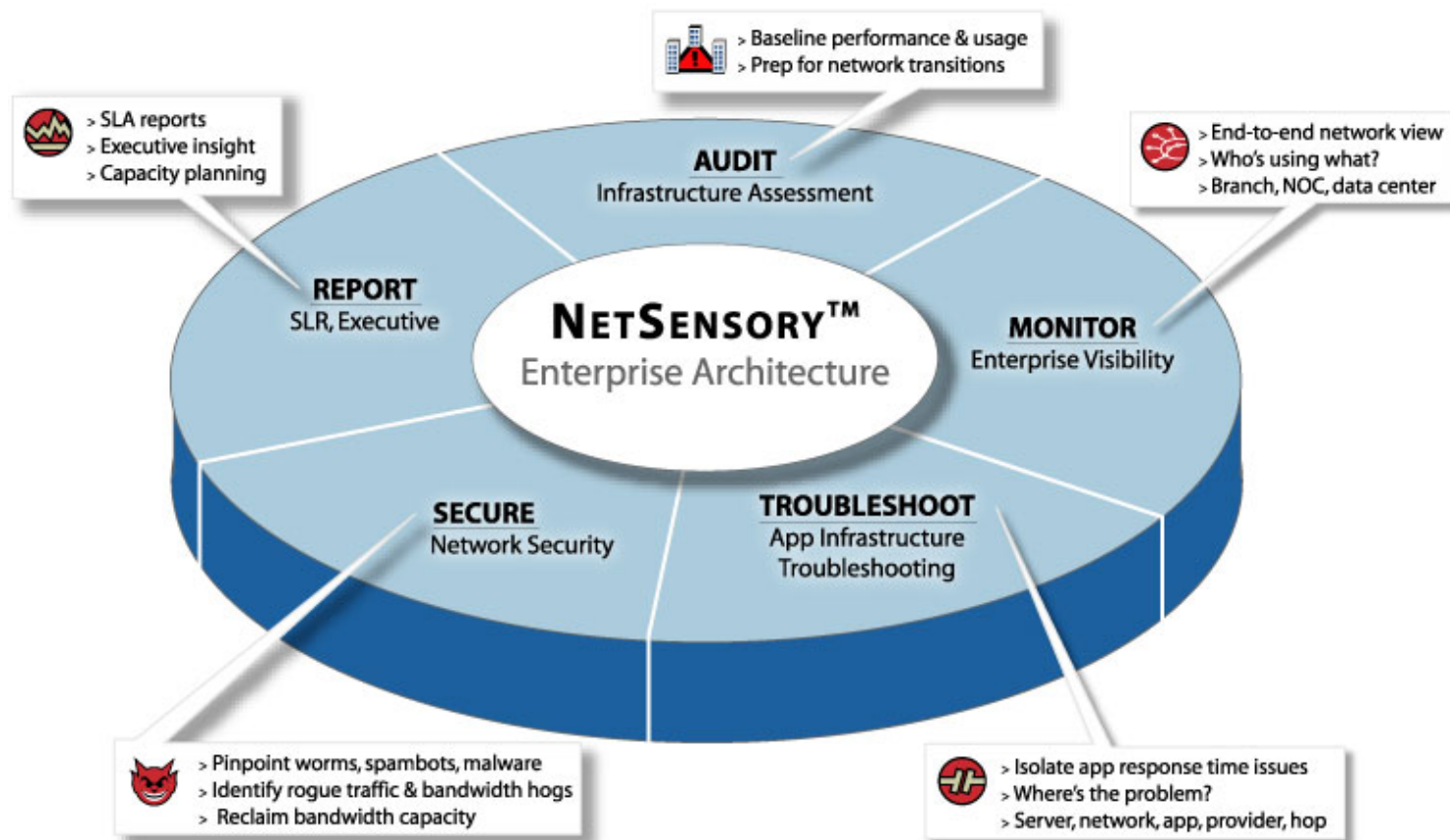
***Bob Quillin, VP Product Management, Network Physics***

***[bobq@networkphysics.com](mailto:bobq@networkphysics.com)***

***NetWorld+Interop 2005***

- **Brief company overview**

- Application management for the network team
- Enterprise scale, flow-based appliance product line



- **Key IP network building blocks found in every network**
  - TCP/IP
  - BGP protocol
  - Layer-3 routing
  - IP packets
- **Harvesting and analyzing this data can answer critical questions**



**What's really on my network? Who's doing what?**



**Do I have worms, viruses? Are they slowing down my apps?**

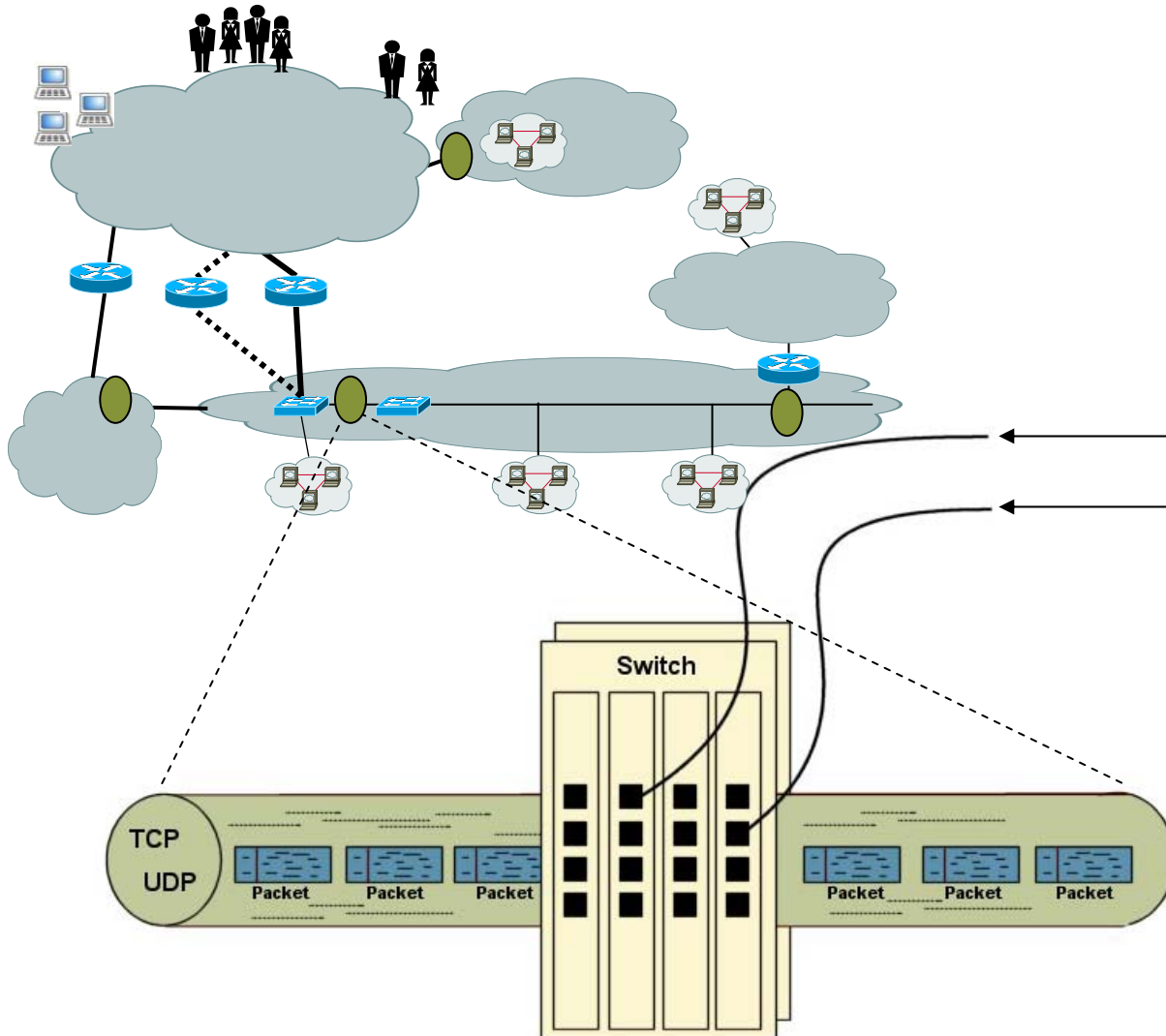


**The network is slow? Or is it? How do I find the truth?**



**Is rogue usage affecting my application response time?**

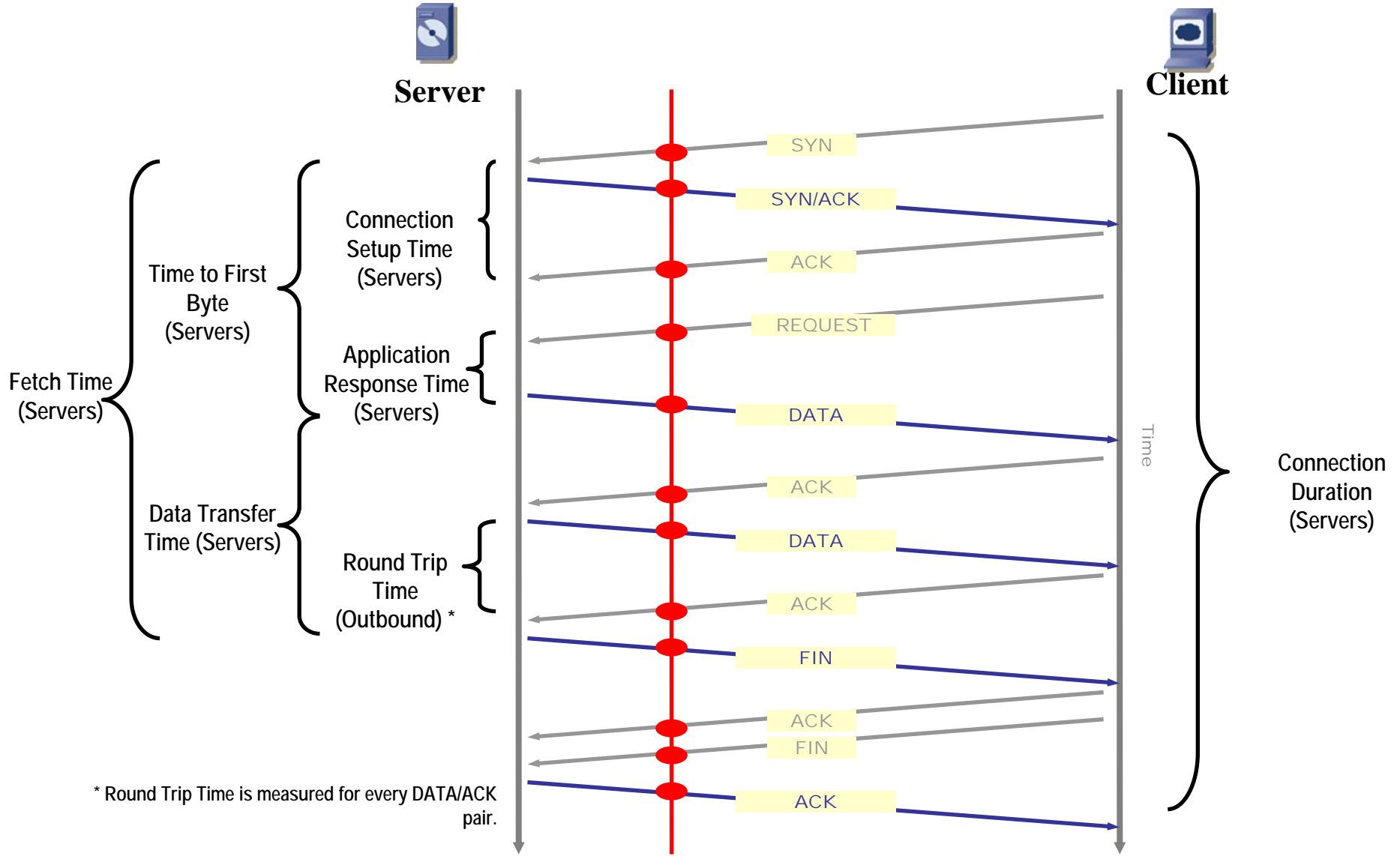
# Leveraging TCP/IP Application Flow Data

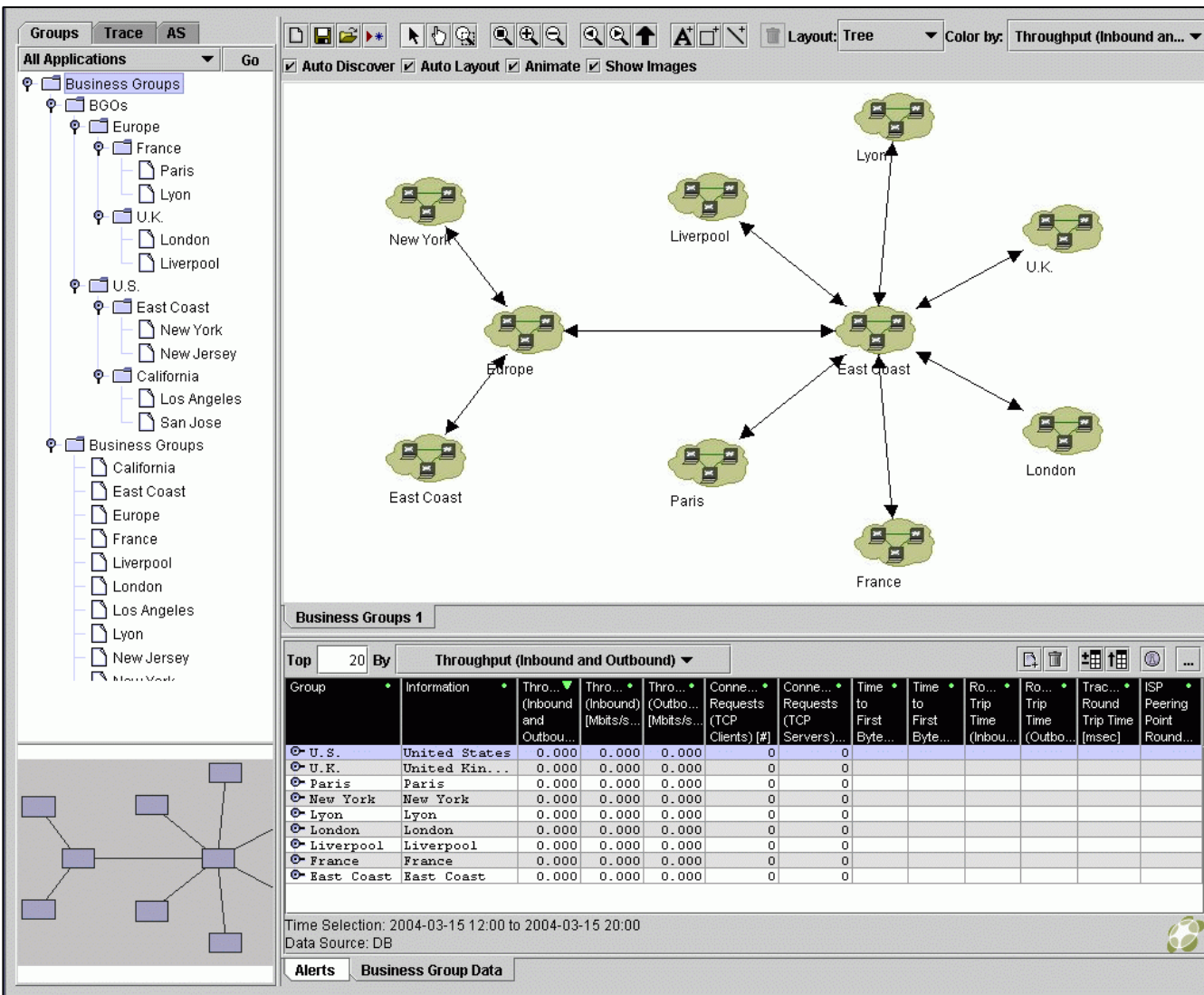


## Flow-Based Network Application Management

- **Flows = TCP, UDP connections**
  - End-to-end, Layer 4
  - Source, destination
  - Application or service port
- **Flow-based appliances monitor flows via switch spanning port or tap**
  - All traffic, all the time
- **Non-invasive: no agents, no SNMP, no polling, no synthetic transactions**
- **Inspect TCP, UDP flows in real-time to monitor performance, response time, utilization**
- **Deploy at major aggregation points to maximize flow visibility**

# Application Performance Metrics



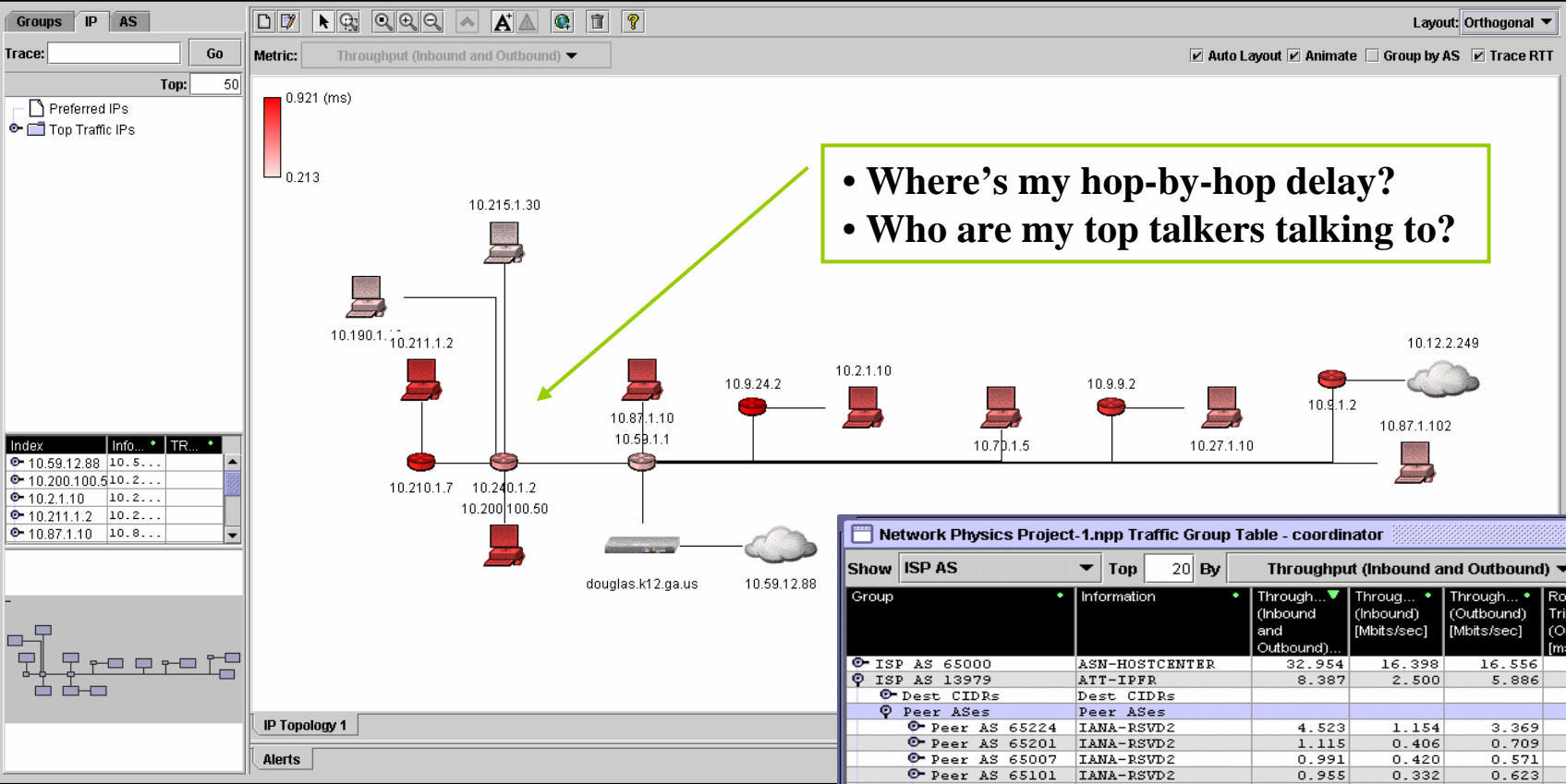



The screenshot displays the NetworkPhysics software interface. On the left is a tree view of 'Business Groups' including BGOs, Europe (France: Paris, Lyon; U.K.: London, Liverpool), U.S. (East Coast: New York, New Jersey; California: Los Angeles, San Jose), and another set of Business Groups (California, East Coast, Europe, France, Liverpool, London, Los Angeles, Lyon, New Jersey, New York). The main area shows a network diagram with nodes for New York, Liverpool, Lyon, U.K., East Coast, Paris, London, and France, all connected to a central 'East Coast' node. Below the diagram is a table titled 'Business Groups 1' showing throughput and connection metrics for various groups.

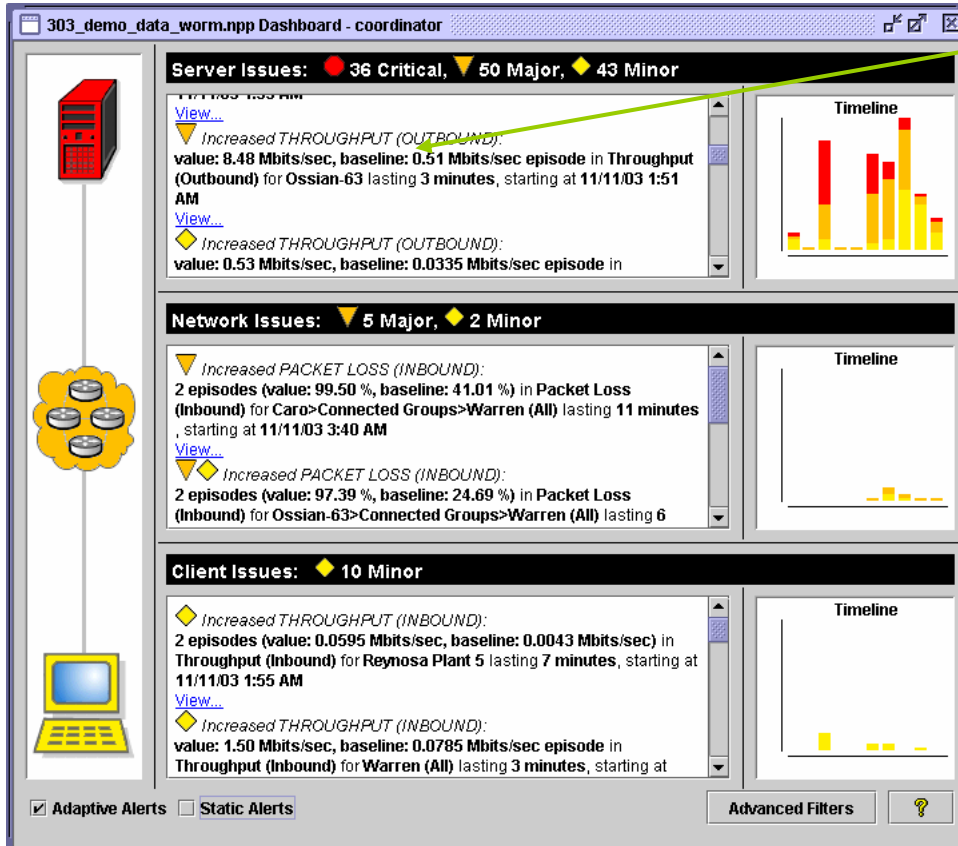
| Group      | Information   | Thro... (Inbound and Outbound) | Thro... (Inbound) [Mbits/s...] | Thro... (Outbound) [Mbits/s...] | Conne... Requests (TCP Clients) [#] | Conne... Requests (TCP Servers)... | Time to First Byte... | Time to First Byte... | Ro... Trip Time (Inbou...) | Ro... Trip Time (Outbo...) | Trac... Round Trip Time [msec] | ISP Peering Point Round... |
|------------|---------------|--------------------------------|--------------------------------|---------------------------------|-------------------------------------|------------------------------------|-----------------------|-----------------------|----------------------------|----------------------------|--------------------------------|----------------------------|
| U. S.      | United States | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| U. K.      | United Kin... | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| Paris      | Paris         | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| New York   | New York      | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| Lyon       | Lyon          | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| London     | London        | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| Liverpool  | Liverpool     | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| France     | France        | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |
| East Coast | East Coast    | 0.000                          | 0.000                          | 0.000                           | 0                                   | 0                                  |                       |                       |                            |                            |                                |                            |

Time Selection: 2004-03-15 12:00 to 2004-03-15 20:00  
Data Source: DB

- Real-time service topology
- View aggregate TCP/IP flow data between business entities
  - Application response time metrics
  - Connection metrics
  - Utilization & throughput metrics
- Integrated topology views
  - Service, traceroute IP, BGP
- Alert & metric visibility

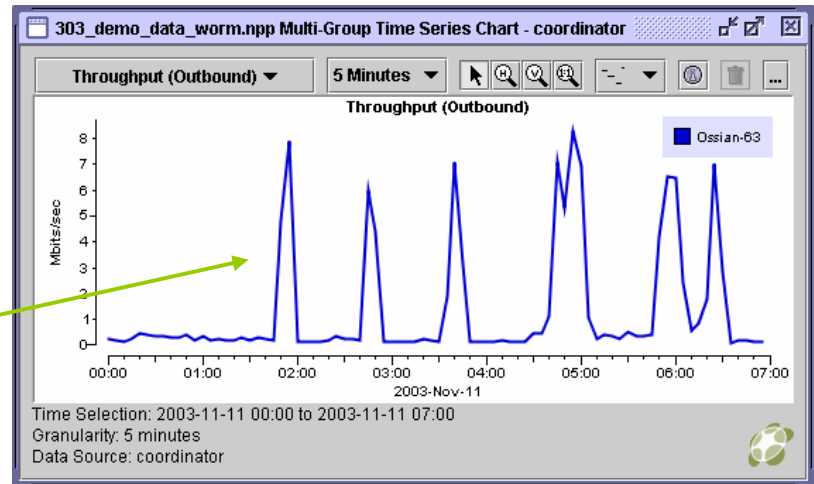


**Who are my ISPs peering with?  
Who's to blame for latency,  
packet loss, response time issues?**



Dashboard correlates performance & utilization data in real-time!

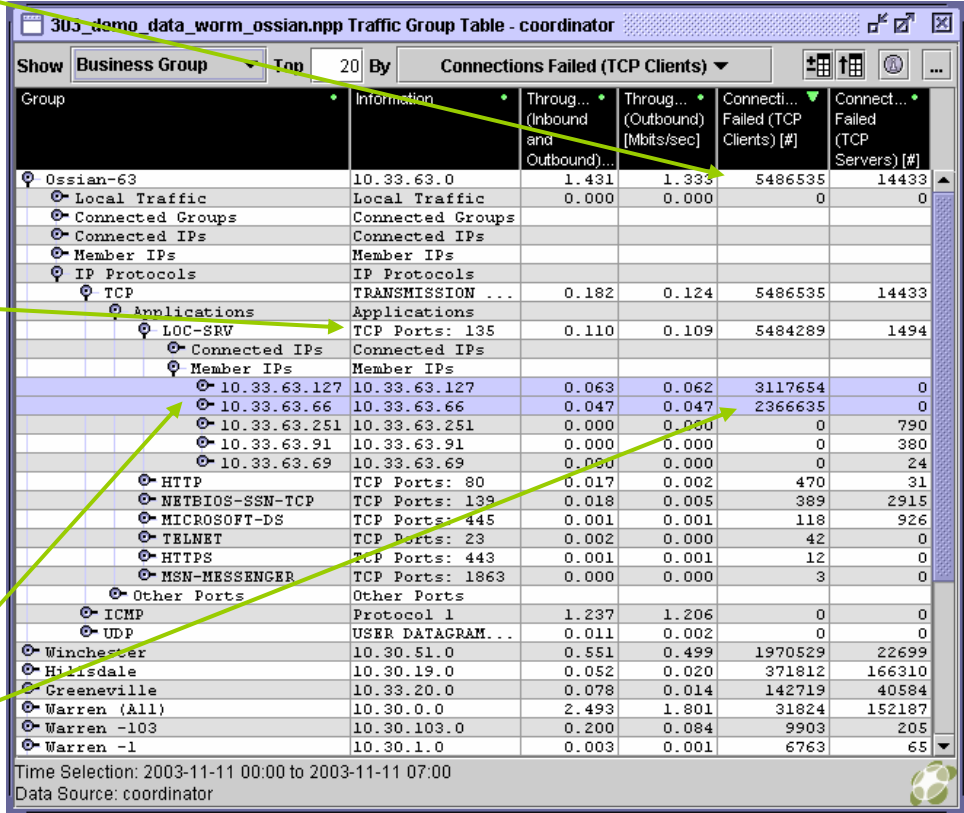
Time series of outbound throughput shows huge spikes in outbound traffic



A huge increase in failed TCP connections is a result of the worm trying to propagate itself through random subnets

Easily identify which applications are contributing to the failed connections. Port 135 is 1 of 2 well known ports used to propagate Blaster.

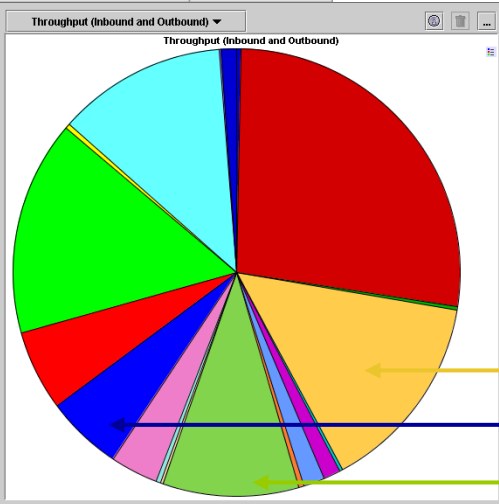
Drilling down to the members of the business group easily shows the 2 infected hosts trying to spread the worm.



| Group            | Information      | Through... (Inbound and Outbound)... | Through... (Outbound) [Mbits/sec] | Connecti... Failed (TCP Clients) [#] | Connect... Failed (TCP Servers) [#] |
|------------------|------------------|--------------------------------------|-----------------------------------|--------------------------------------|-------------------------------------|
| Ossiian-63       | 10.33.63.0       | 1.431                                | 1.333                             | 5486535                              | 14433                               |
| Local Traffic    | Local Traffic    | 0.000                                | 0.000                             | 0                                    | 0                                   |
| Connected Groups | Connected Groups |                                      |                                   |                                      |                                     |
| Connected IPs    | Connected IPs    |                                      |                                   |                                      |                                     |
| Member IPs       | Member IPs       |                                      |                                   |                                      |                                     |
| IP Protocols     | IP Protocols     |                                      |                                   |                                      |                                     |
| TCP              | TRANSMISSION ... | 0.182                                | 0.124                             | 5486535                              | 14433                               |
| Applications     | Applications     |                                      |                                   |                                      |                                     |
| LOC-SRV          | TCP Ports: 135   | 0.110                                | 0.109                             | 5484289                              | 1494                                |
| Connected IPs    | Connected IPs    |                                      |                                   |                                      |                                     |
| Member IPs       | Member IPs       |                                      |                                   |                                      |                                     |
| 10.33.63.127     | 10.33.63.127     | 0.063                                | 0.062                             | 3117654                              | 0                                   |
| 10.33.63.66      | 10.33.63.66      | 0.047                                | 0.047                             | 2366635                              | 0                                   |
| 10.33.63.251     | 10.33.63.251     | 0.000                                | 0.000                             | 0                                    | 790                                 |
| 10.33.63.91      | 10.33.63.91      | 0.000                                | 0.000                             | 0                                    | 380                                 |
| 10.33.63.69      | 10.33.63.69      | 0.000                                | 0.000                             | 0                                    | 24                                  |
| HTTP             | TCP Ports: 80    | 0.017                                | 0.002                             | 470                                  | 31                                  |
| NETBIOS-SSN-TCP  | TCP Ports: 139   | 0.018                                | 0.005                             | 389                                  | 2915                                |
| MICROSOFT-DS     | TCP Ports: 445   | 0.001                                | 0.001                             | 118                                  | 926                                 |
| TELNET           | TCP Ports: 23    | 0.002                                | 0.000                             | 42                                   | 0                                   |
| HTTPS            | TCP Ports: 443   | 0.001                                | 0.001                             | 12                                   | 0                                   |
| MSN-MESSENGER    | TCP Ports: 1863  | 0.000                                | 0.000                             | 3                                    | 0                                   |
| Other Ports      | Other Ports      |                                      |                                   |                                      |                                     |
| ICMP             | Protocol 1       | 1.237                                | 1.206                             | 0                                    | 0                                   |
| UDP              | USER DATAGRAM... | 0.011                                | 0.002                             | 0                                    | 0                                   |
| Winchester       | 10.30.51.0       | 0.551                                | 0.499                             | 1970529                              | 22699                               |
| Hillsdale        | 10.30.19.0       | 0.052                                | 0.020                             | 371812                               | 166310                              |
| Greeneville      | 10.33.20.0       | 0.078                                | 0.014                             | 142719                               | 40584                               |
| Warren (All)     | 10.30.0.0        | 2.493                                | 1.801                             | 31824                                | 152187                              |
| Warren -103      | 10.30.103.0      | 0.200                                | 0.084                             | 9903                                 | 205                                 |
| Warren -1        | 10.30.1.0        | 0.003                                | 0.001                             | 6763                                 | 65                                  |



| Group                  | Information            | Throughput (Inbound and Outbound) (Mbits/sec) |
|------------------------|------------------------|---|
| WB Internal networks   | WB Internal networks   | 56.450  |
| Local Traffic          | Local Traffic          | 0.014   |
| Connected Groups       | Connected Groups       |   |
| Connected IPs          | Connected IPs          |   |
| Member IPs             | Member IPs             |   |
| IP Protocols           | IP Protocols           |   |
| TCP                    | TCP                    |   |
| Applications           | Applications           |   |
| HTTP                   | HTTP                   |   |
| AOL                    | AOL                    |   |
| SMTP                   | SMTP                   |   |
| Real Networks          | Real Networks          |   |
| HTTPS-MAIN             | HTTPS-MAIN             |   |
| BitTorrent             | BitTorrent             |   |
| Windows Media Player   | Windows Media Player   |   |
| NETBIOS-SSN-TCP        | NETBIOS-SSN-TCP        |   |
| Open Flash Point Games | Open Flash Point Games |   |
| nCube License Manager  | nCube License Manager  |   |
| MICROSOFT-DS           | MICROSOFT-DS           |   |
| POP3                   | POP3                   |   |
| ica cytrix metaframe   | ica cytrix metaframe   |   |
| NNTTP                  | NNTTP                  |   |
| TELNET                 | TELNET                 |   |
| LDAP                   | LDAP                   |   |
| Gnutella-TCP           | Gnutella-TCP           |   |
| IBM MQ Series          | IBM MQ Series          |   |
| Domain Name Service    | Domain Name Service    |   |
| Tivoli                 | Tivoli                 |   |
| Other Ports            | Other Ports            |   |
| Other IP Protocols     | Other IP Protocols     |   |
| UDP                    | UDP                    |   |
| Internet               | Internet               |   |
| SAP Servers            | SAP Servers            |   |
| SF Center              | Server Farm Center ... | 14.364  |
| Other Group            | Other Group            | 3.079   |



Real Networks - Streaming Audio  
 Gnutella - Music Sharing  
 Flash Point - Games

## Business Problem

- Application and Security Services
  - Inability to isolate and identify non-business related traffic and the internal or external sources of that traffic.

| Real Networks   | Real Networks              |       |
|-----------------|----------------------------|-------|
| External IPs    | External IPs               |       |
| Internal IPs    | Internal IPs               |       |
| 10.130.198.244  | 10.130.198.244             | 0.249 |
| 64.157.128.162  | 10a-lvl3-ny22.rbn.com      | 0.249 |
| 10.130.69.46    | 10.130.69.46               | 0.131 |
| 10.130.152.173  | 10.130.152.173             | 0.122 |
| 209.247.111.152 | 10a-lvl3-tex13.rbn.com     | 0.110 |
| 64.156.70.80    | unknown.Level3.net         | 0.010 |
| 64.156.70.91    | unknown.Level3.net         | 0.002 |
| 217.163.2.201   | 217.163.2.201              | 0.000 |
| 10.130.89.74    | 10.130.89.74               | 0.051 |
| 205.188.216.25  | od-dtc3s-0.stream.aol.com  | 0.026 |
| 64.12.56.161    | demand3VIP1.stream.aol.com | 0.025 |

Internal Users IP Address  
 AOL Streaming Audio  
 Real Broadcast Network – rbn.com

## Network Drilldown

- Accounting and Security
  - Identify users of Real Networks streaming audio and to which sites they are connected in real-time.