The Ecosystem of Computer Networks

Ripe 46

Amsterdam, The Netherlands

September 2003

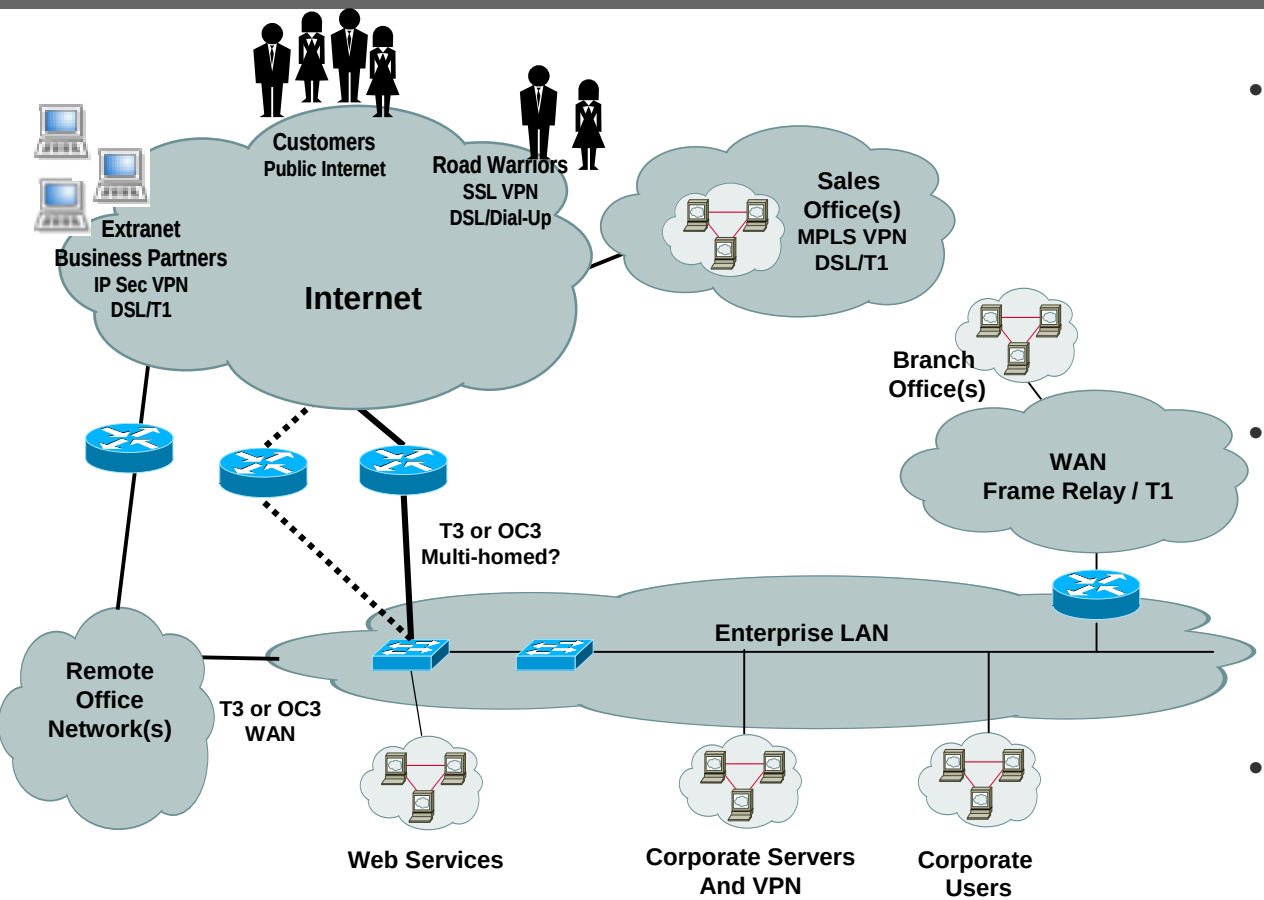
Silvia Veronese

Sveronese@networkphysics.com

Agenda

- Today’s IT challenges
- Introduction to Network Flow Analysis
- Nature of Network Congestion
- Case Studies
- Q&A

IT Challenge: The 3 C's



IT Goals

- Reduce complexity
- Enable change
- Manage costs

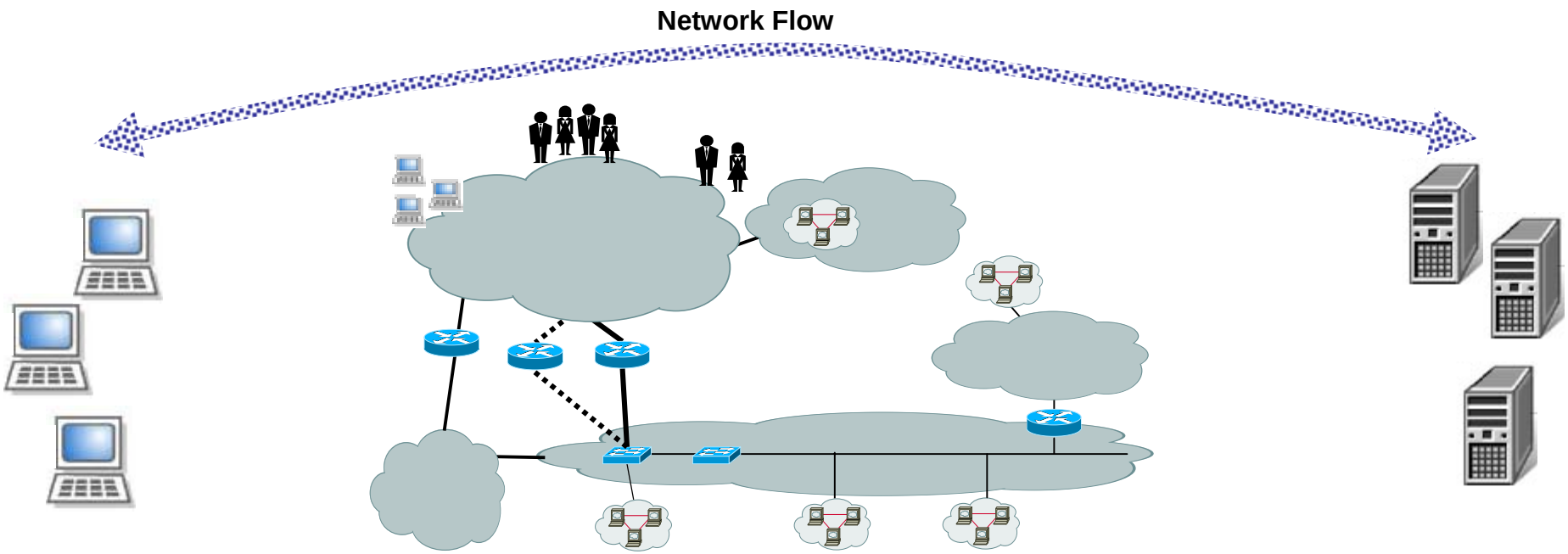
- **Complexity**
  - Sheer number of devices
  - Outsourced networks & services
  - Management silos
  - Network of networks
- **Change**
  - Economic & business change
  - Drives need for business agility
  - Business ecosystem
- **Cost**
  - Reducing capex & opex while meeting business goals
  - Spend less, manage more

Device-Based Management Can't Manage 3 C's

	Traditional Device-based Management Problems
Complexity	• **Management silos**: too much finger pointing across teams, too little answers • **Blind spots**: can't see or manage Internet, 3rd party networks, outsourced services
Change	• **Fear of network transitions**: network performance anxiety • **Hard-wired device mgmt:** breaks down w/ networks changes, migrations, moves
Cost	• **Escalating capex**: add/change services > add/change management • **Point tools proliferate:** single purpose probes, fragmented management

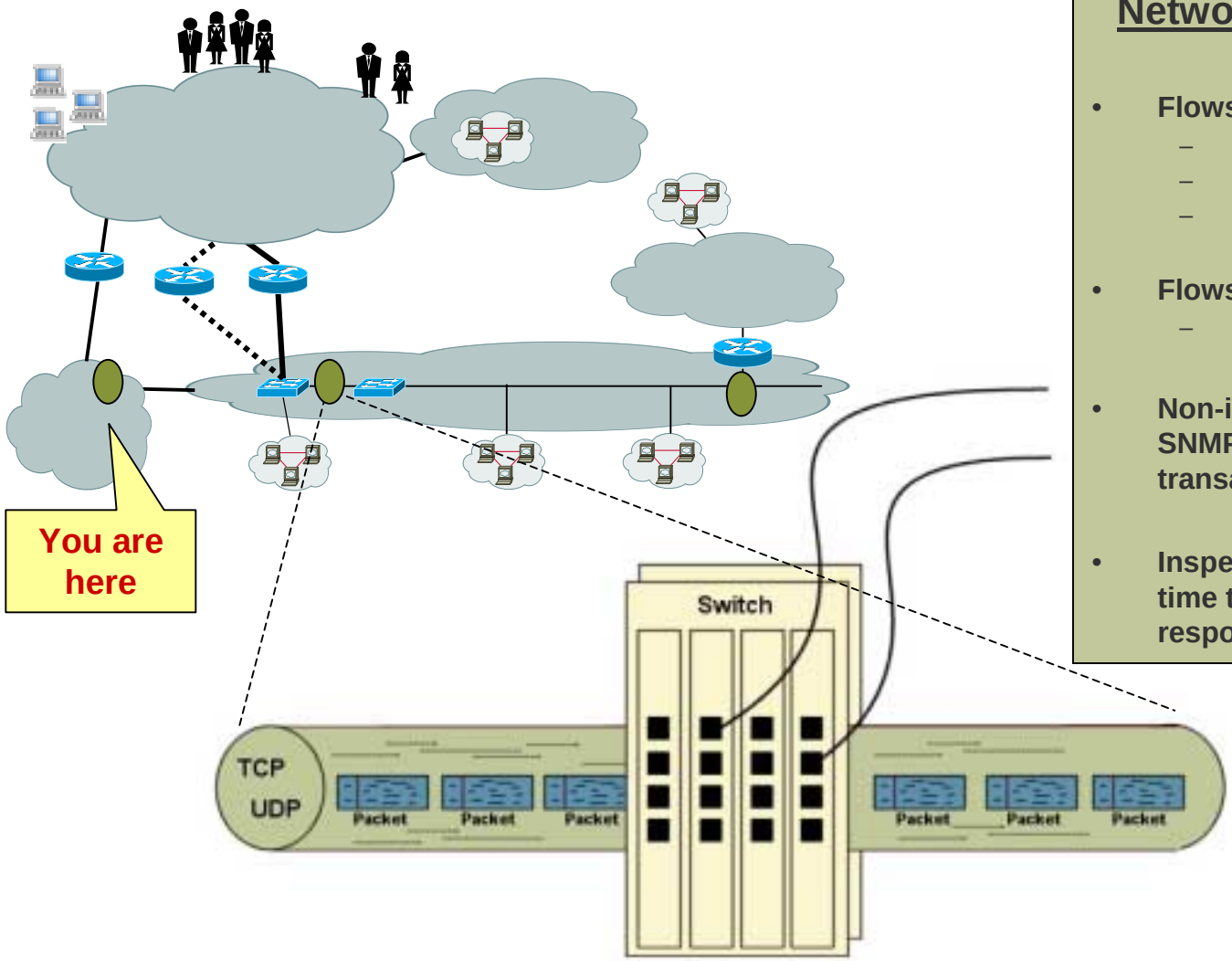
Flow-Based Management, Business Relevance

Manage actual network traffic flows, instead of devices → **Deliver object-relevant management of the most dynamic & complex networks**



- **Complexity:** Monitor end-to-end regardless of underlying complexity
- **Change:** Dynamically adapt to network changes
- **Cost:** Consolidate management to reduce cost

What are Network Flows?

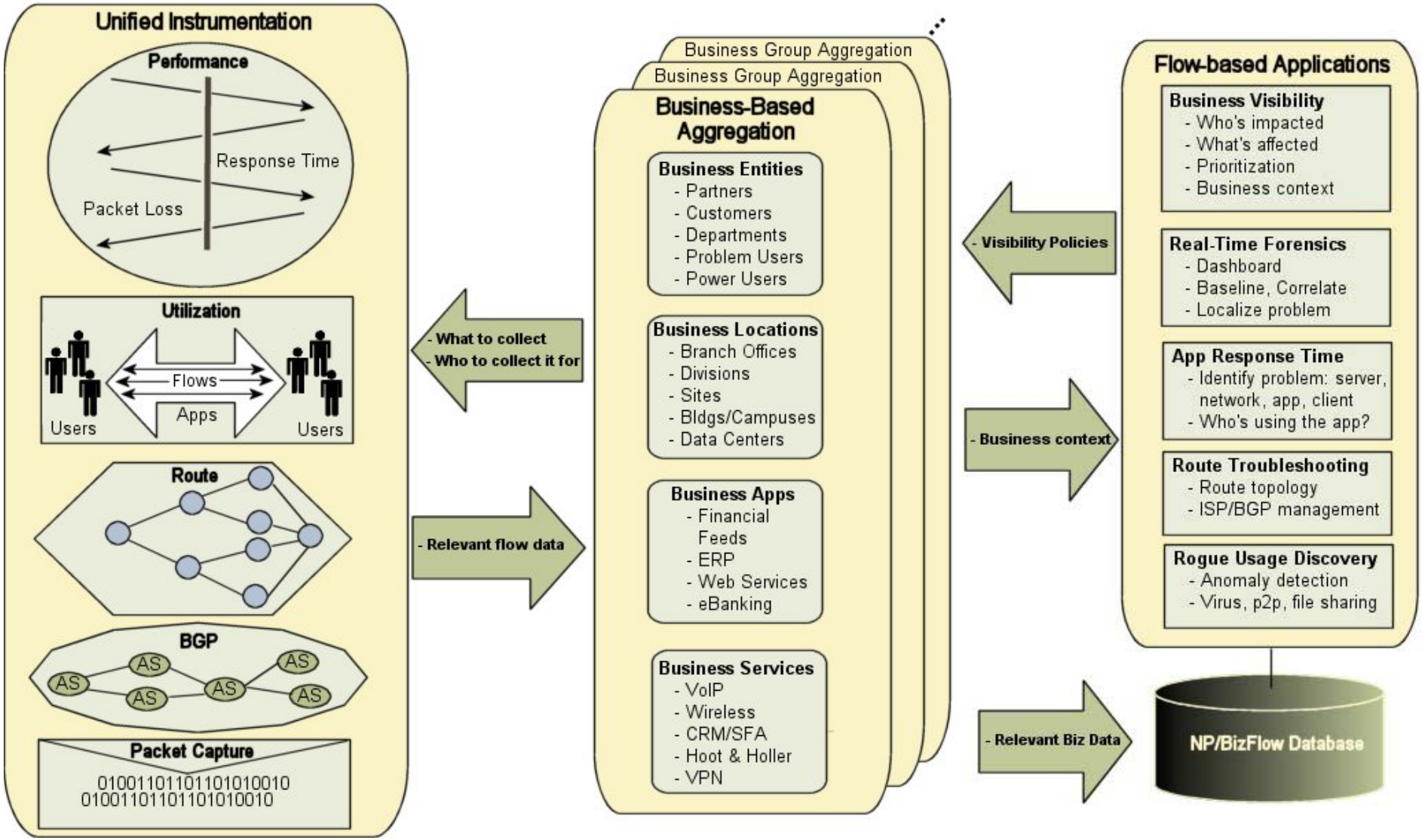


Network Traffic Flows 101

- **Flows = TCP, UDP connections**
  - End-to-end, Layer 4
  - Source, destination
  - Application or service port
- **Flows capture:**
  - 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**

Locate problems in the network using only what you can observe at ● !

What is Flow-Based Management?



Typical enterprise network profile

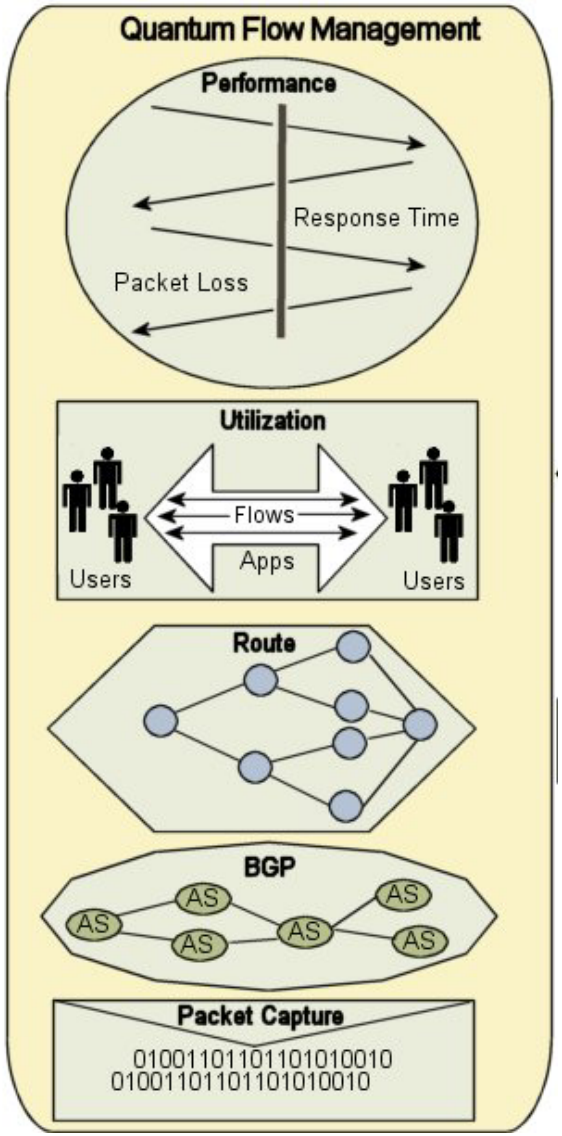
- **Average 200-300 Mb/s traffic**
- **90K flows/sec, 40K unique connected users/sec**
- **Experience 10% congestion episodes/sec, of which 30% are critical**
- **Sessions lasting 10 sec- 2min**
- **Financial value of each session may vary widely**
  - How much a session in a financial environment is worth?
  - How much a connection to Yahoo! is worth?
  - Where do you act first? CIO call, John Doe call?

- **Reduced IT human support**
- **Reduced IT infrastructure for troubleshooting**

- **Persistency of Network problems**
  - Congestions come and go in bursting mode.
  - When congestion occurs, it tends to occur repeatedly at specific “points” (I.e., specific bandwidth exchange points).

Apply the 8 seconds rule!

Today's challenges of intelligent data management



- **Real Time Data Acquisition**
  - Data is heterogeneous by nature. Patterns are fractal in nature and happen at all dimensions(packets, connections, flows)
- **Loss-less data compression.**
  - How can the system retain the information while reducing the size?
  - Effective pre-processing is the key to statistical accuracy and resolution.
- **Optimized clustering**
  - Average customer network will generate 90K convers/sec. In addition route, configuration, lookup information have to be correlated to the conversations in real-time
- **Pattern identification**
  - How do you close the gap between data generation and data comprehension?
  - What is the most appropriate data model ?

Accuracy relies on statistics: more traffic is better

What can we see?

IP packet headers

source IP address
destination IP address
TTL (time-to-live)
TOS (type-of-service):
    TCP, UDP, ICMP, etc.
…

TCP segment headers

Source, port number
Destination, port number
Flags:
    SYN
    FIN
    ACK
    RST
…

Data

e.g., HTTP stuff
(we note the total size, in bytes)

What can't we see?

Where packets have been

Where packets were delayed

Where packets got dropped

WHERE,
WHERE,
WHERE?

Extensive Suite of Metrics

- **Response Metrics**
  - Time to First Byte (ms)
  - Network Transfer Time (ms)
  - Server Response Time (ms)
  - Connection Duration (sec)
  - Round Trip Time (ms)

- **Client Metrics**
  - Time to Live (Hops)
  - Client Reset Rate (#/s)
  - Timeout Rate (#/s)
  - Client Request Rate (#/s)
  - Information (Hostname)

- **Throughput Metrics**
  - Inbound TCP Throughput (Mbps)
  - Inbound TCP Traffic (MB)
  - Inbound Packet Throughput (pps)
  - Inbound Packet Traffic (packets)
  - Inbound Throughput (Mbps)
  - Inbound Traffic (MB)
  - Outbound TCP Throughput (Mbps)
  - Outbound TCP Traffic (MB)
  - Outbound Packet Throughput (pps)
  - Outbound Packet Traffic (MB)
  - Outbound Throughput (Mbps)
  - Outbound Traffic (MB)
  - Connection Rate (#/s)
  - Connection Payload (KB)

- **Congestion Metrics**
  - Outbound Retrans (MB)
  - Outbound Packet Retrans (packets)
  - Outbound Retrans Rate (Mbps)
  - Outbound Packet Retrans Rate (pps)
  - Outbound Packet Loss (%)
  - Total Congestion Time (min)
  - Lossless Network Transfer Time

- **AS Metrics**
  - Trans-ISP RTT (ms)
  - ISP Peering Point RTT (ms)
  - Associated AS
  - Associate AS Description
  - Associated AS Information

For each IP address, subnet, business group, Autonomous System, Server, Client, etc.

Architecture

- Passive monitoring
- Does not require any network modification
- Does not rely on MIBs or other parameter polling mechanism
- Only one device is needed - does not require agents
- Collects data all the time - real-time and historical
- Database is included for long term analysis – Data is persistently stored.
- Includes a BGP Speaker, AS lookup, TCP/ICMP traceroutes
- Web server + Java app for data browsing

Business-Relevant Visibility

Virtualized: to maintain business service visibility regardless of network complexity

Show Business Groups Top 20

Group	Information	Total Outbound Throughput (kB/sec)	Total Inbound Throughput (kB/sec)
WB Internal networks		399.110	1269.264
Internet	Outside Addresses	313.118	1038.394
Exhange Servers	Burbank Exhcnag...	42.081	16.433
SF Left 2	Server Farm Left 2	24.097	156.263
Exchange 2000 Servers	Exhange 2000	19.359	17.768
SF Center	Server Farm Cen...	12.498	5.914
SAP Servers	SAP Subnet Virgina	11.751	18.600
World Secure West	World Secure SM...	8.840	4.379
B170	4000 Alameda	8.640	54.713
B154	Glass Building	6.434	39.100
AD Burbank	Domain controll...	5.462	4.123
AD Off Lot	AD off lot cont...	4.956	16.118
AD London	AD Lonon contro...	4.084	3.952
WHV Direct	WHV DIrect AOL	2.789	11.410
B2+3	Main Admin	2.727	16.104
SF Right	Server Farm Right	2.501	3.465
TCS MF	TCS Main Frame	1.857	32.259
RT&T	WB Internet	0.121	0.007

- **Feature: Business groups**
  - Business level visibility through data aggregation
- **Business critical apps**
  - SAP, Exchange
- **Important business units**
  - London, Burbank
  - Building 170, 154
- **Business networks**
  - Internet, Internal
- **Specific server farms**
  - Mainframe, SF L/R/C

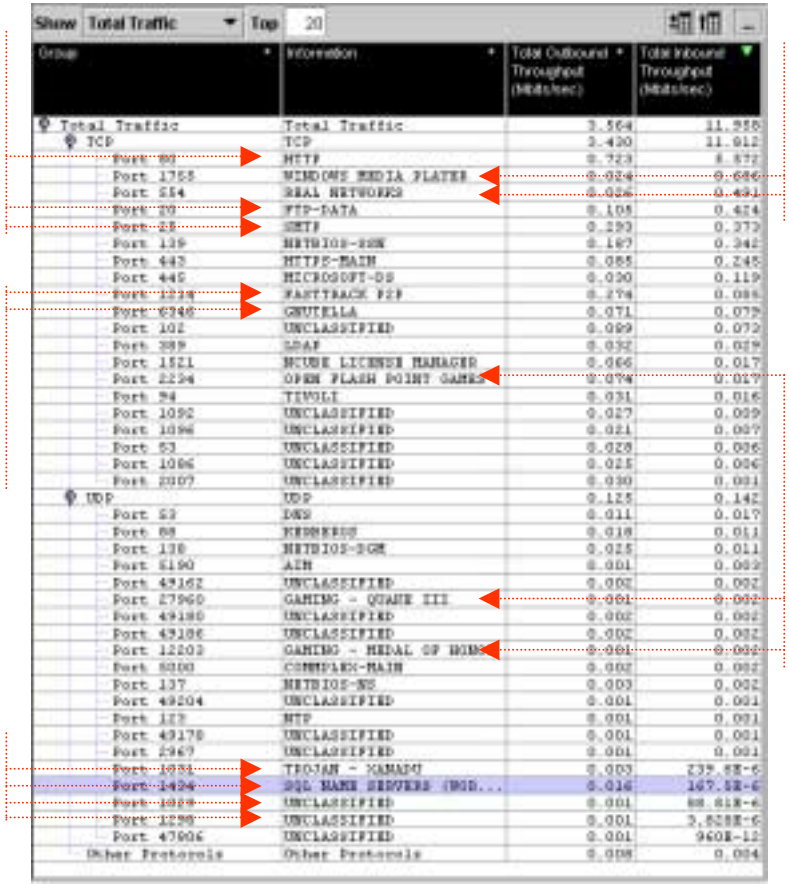
Baselining Application Usage

- Ports required for Firewall
- Determine which applications may need to be prioritized through the VPN
- Size of Internet Connection

- **Standard Services**
  - http
  - email
  - ftp

- **Peer-to-peer (P2P) apps**
  - Fasttrack-based apps (KazaA, Grokster, Morpheus)
  - Gnutella

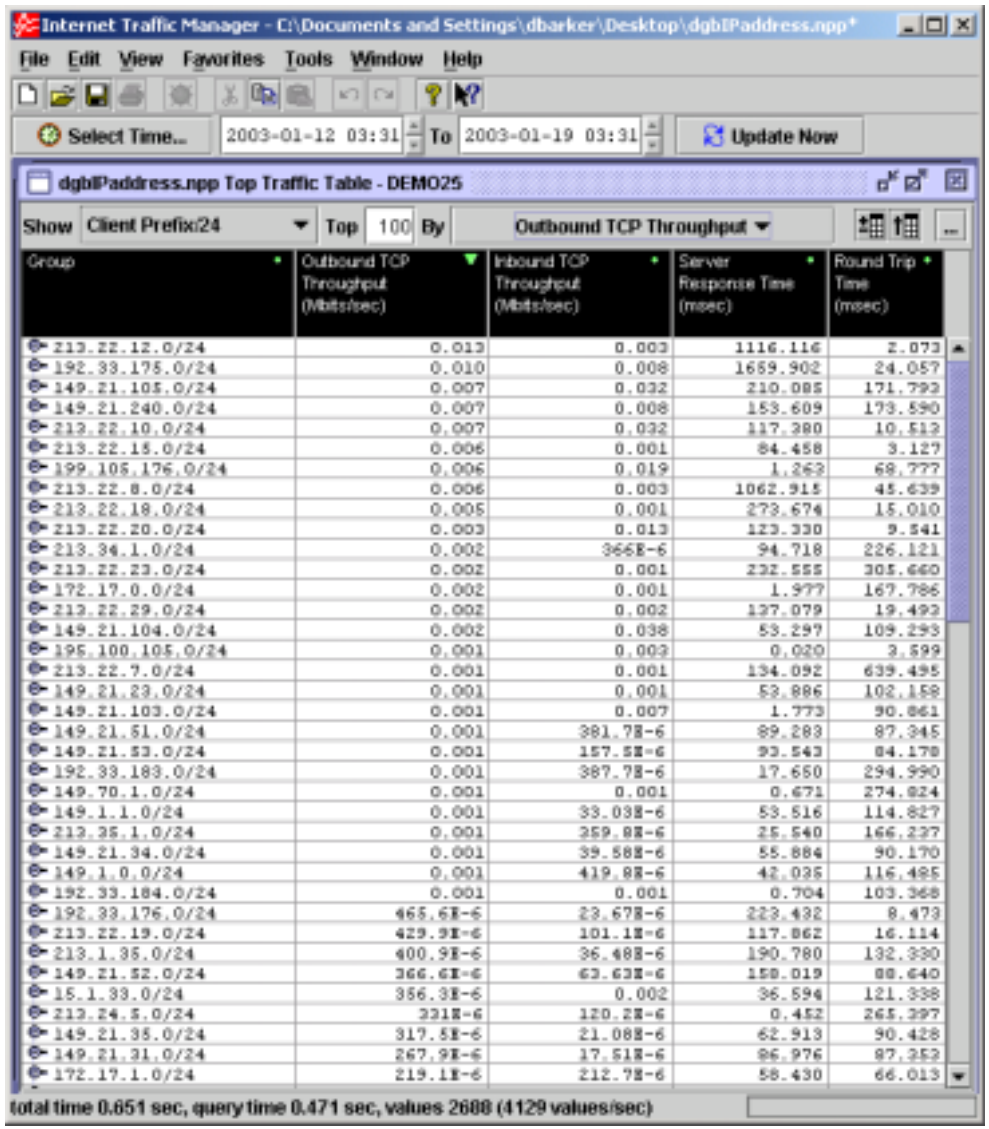
- **Internal Application Usage**



- **Streaming services**
  - Real
  - Windows Media Player

- **Gaming apps**
  - Operation Flashpoint
  - Quake III
  - Medal of Honor

Baselining All Users

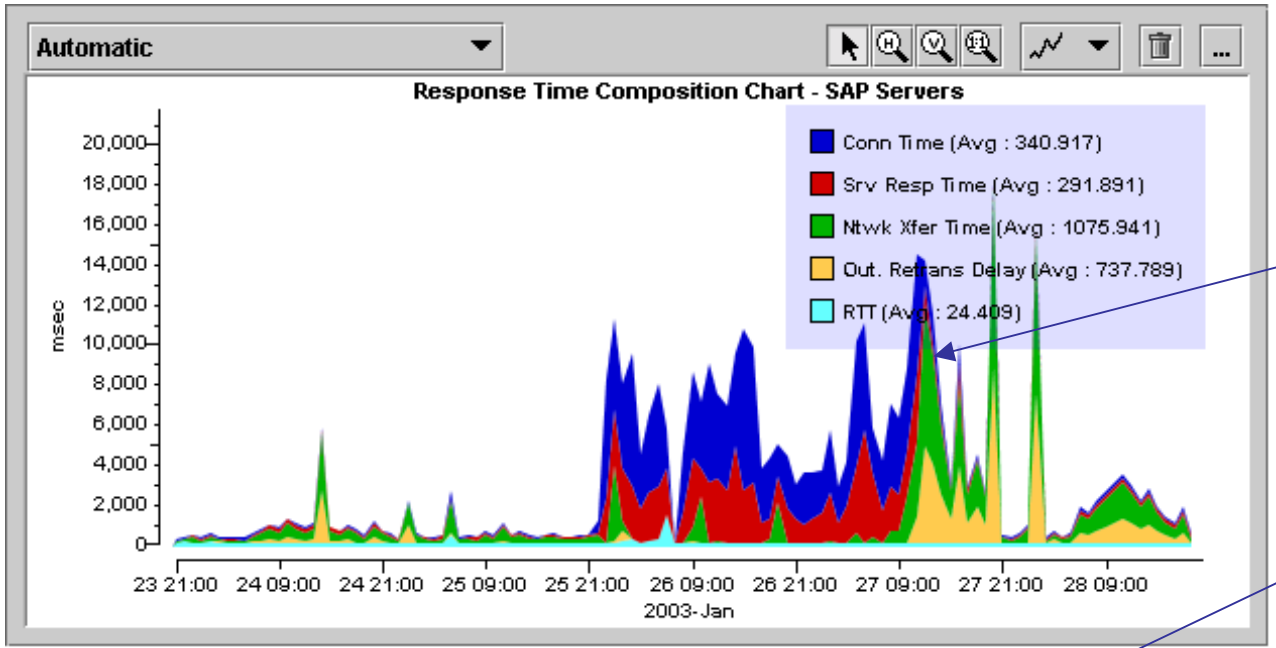


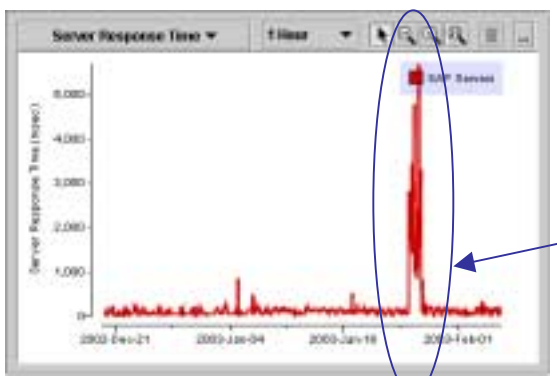
Group	Outbound TCP Throughput (Mbits/sec)	Inbound TCP Throughput (Mbits/sec)	Server Response Time (msec)	Round Trip Time (msec)
213.22.12.0/24	0.013	0.003	1116.116	2.073
192.33.175.0/24	0.010	0.008	1659.902	24.057
149.21.105.0/24	0.007	0.032	210.085	171.793
149.21.240.0/24	0.007	0.008	153.609	173.590
213.22.10.0/24	0.007	0.032	117.380	10.513
213.22.15.0/24	0.006	0.001	84.458	3.127
199.105.176.0/24	0.006	0.019	1.263	68.777
213.22.8.0/24	0.006	0.003	1062.915	45.639
213.22.18.0/24	0.005	0.001	273.674	15.010
213.22.20.0/24	0.003	0.013	123.330	9.541
213.34.1.0/24	0.002	366E-6	94.718	226.121
213.22.23.0/24	0.002	0.001	232.555	305.660
172.17.0.0/24	0.002	0.001	1.977	167.786
213.22.29.0/24	0.002	0.002	137.079	19.493
149.21.104.0/24	0.002	0.038	53.297	109.293
195.100.105.0/24	0.001	0.003	0.020	3.599
213.22.7.0/24	0.001	0.001	134.092	639.495
149.21.23.0/24	0.001	0.001	53.886	102.158
149.21.103.0/24	0.001	0.007	1.773	90.861
149.21.51.0/24	0.001	381.7E-6	89.283	87.345
149.21.53.0/24	0.001	157.5E-6	93.543	84.178
192.33.183.0/24	0.001	387.7E-6	17.650	294.990
149.70.1.0/24	0.001	0.001	0.671	274.024
149.1.1.0/24	0.001	33.03E-6	53.516	114.827
213.35.1.0/24	0.001	359.8E-6	25.540	166.237
149.21.34.0/24	0.001	39.58E-6	55.884	90.170
149.1.0.0/24	0.001	419.8E-6	42.035	116.485
192.33.184.0/24	0.001	0.001	0.704	103.368
192.33.176.0/24	465.6E-6	23.67E-6	223.432	8.473
213.22.19.0/24	429.9E-6	101.1E-6	117.862	16.114
213.1.35.0/24	400.9E-6	36.48E-6	190.780	132.330
149.21.52.0/24	366.6E-6	63.63E-6	159.019	88.640
15.1.33.0/24	356.3E-6	0.002	36.594	121.338
213.24.5.0/24	331E-6	120.2E-6	0.452	265.397
149.21.35.0/24	317.5E-6	21.08E-6	62.913	90.428
149.21.31.0/24	267.9E-6	17.51E-6	86.976	87.353
172.17.1.0/24	219.1E-6	212.7E-6	58.430	66.013

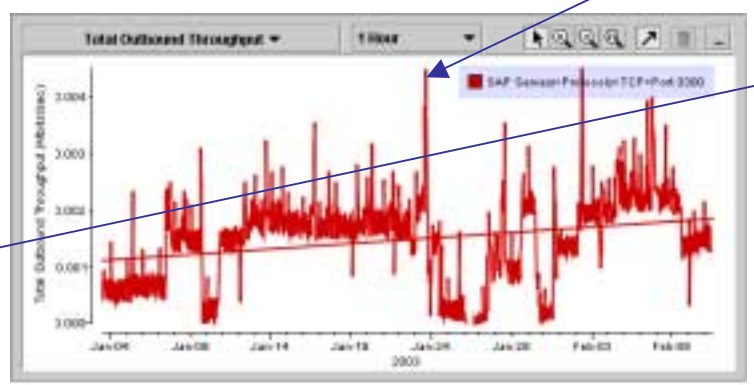
- **Security**
  - Detailed list of the subnets that need to allowed through the firewall.
- **Internet Connection**
  - Understand who is using the network and how much
  - May want to migrate remote offices with less traffic first!
- **Network Responsiveness**
  - Understand response times for remote offices as a baseline to measure VPN performance

Application Response Time Analysis

Unifying: across management silos, across disparate management systems

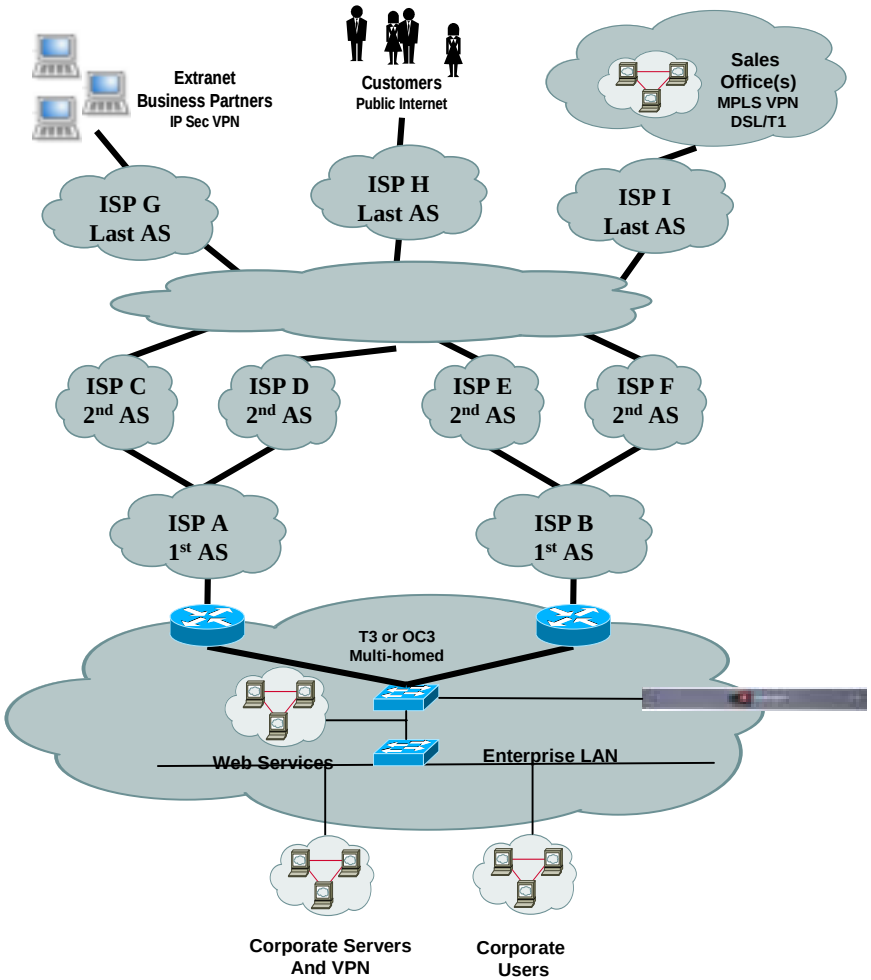






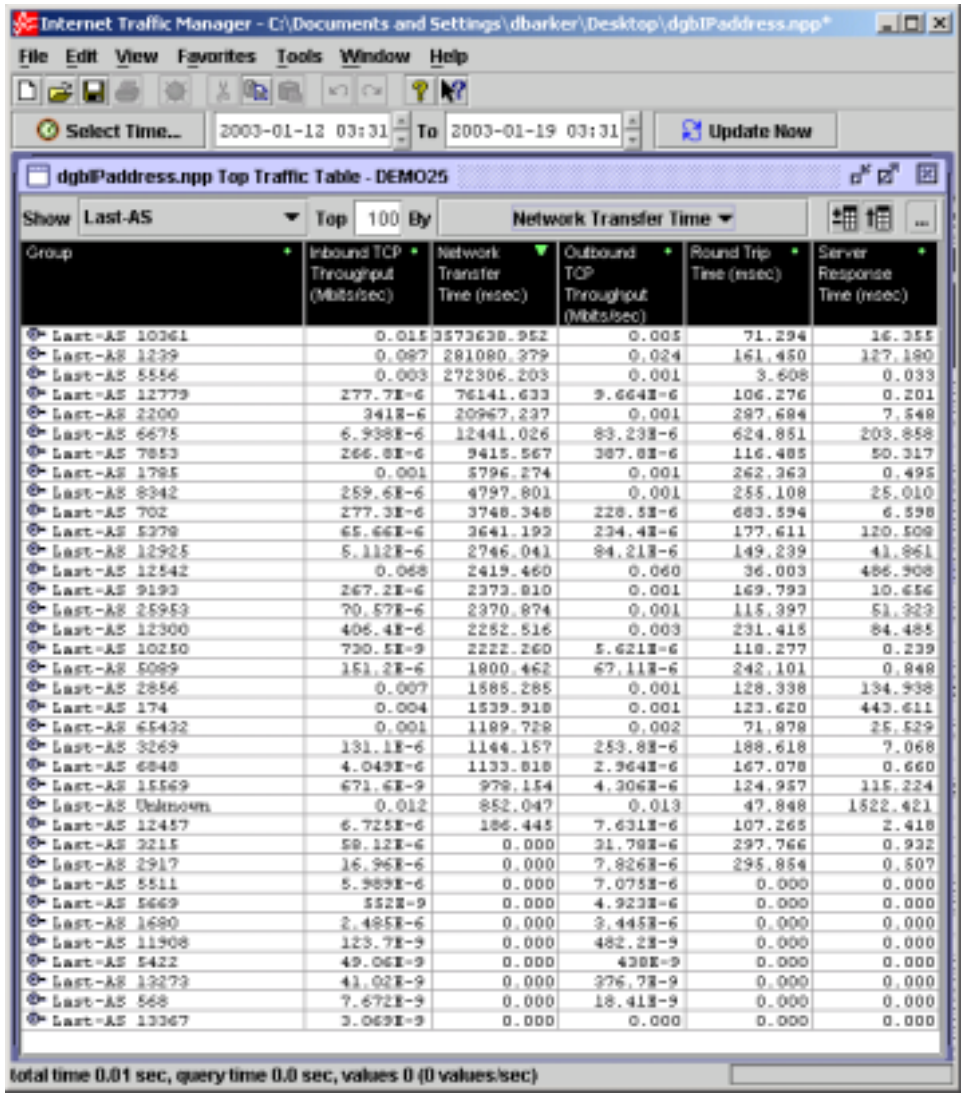
- **Feature: Response time composition analysis**
- **Troubleshoot SAP performance problems**
  - Isolate largest contributor to SAP response time delays
- **Monitor SAP usage trends month-to-month**
- **Identify major SAP application response time delays**

AS Information: Insight Into The Cloud



- **For each 1st, 2nd, and Last AS, we provide a unique set of statistics**
  - Utilization
  - End-to-End performance
  - Transit and peering latency
- **Only available by correlating Flows, BGP, and Traceroute Information**

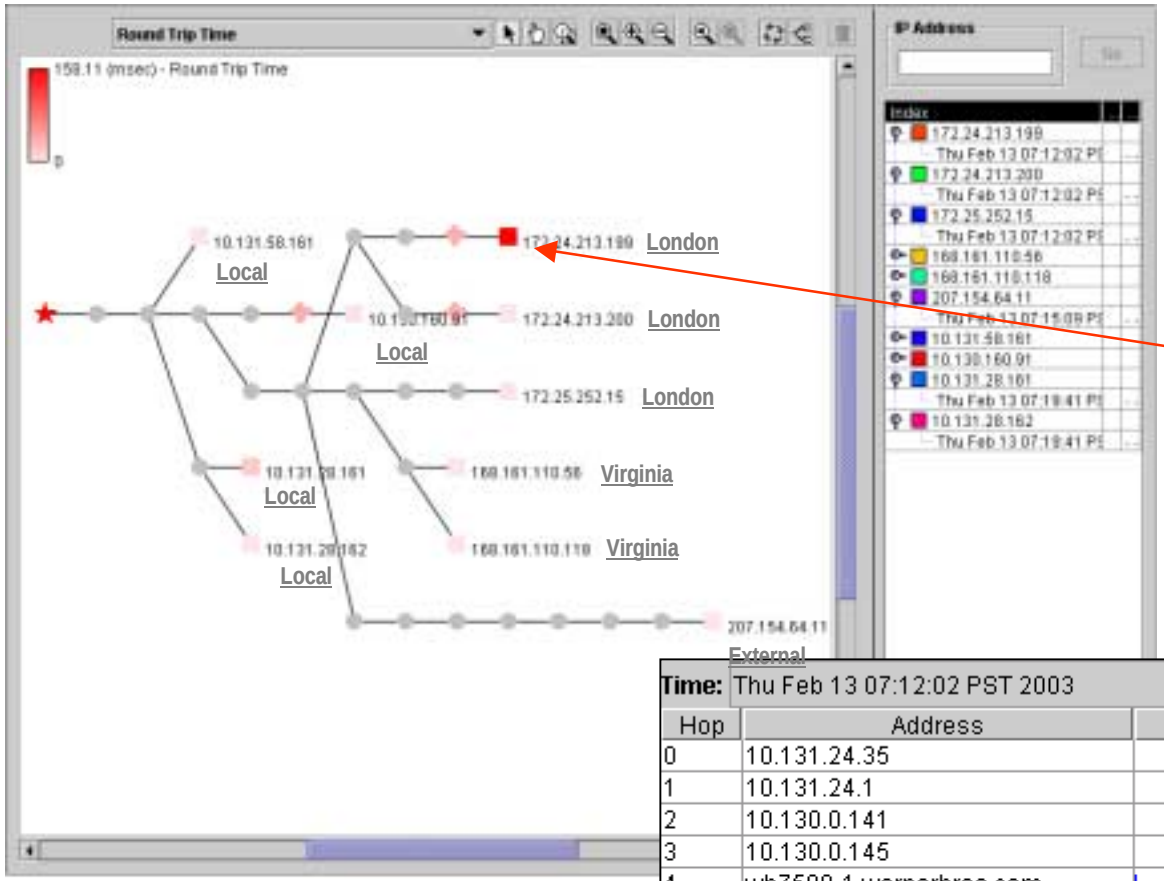
Measuring Service Provider Performance



Group	Inbound TCP Throughput (Mbits/sec)	Network Transfer Time (msec)	Outbound TCP Throughput (Mbits/sec)	Round Trip Time (msec)	Server Response Time (msec)
Last-AS 10361	0.015	3573630.952	0.005	71.294	16.355
Last-AS 1239	0.087	281080.379	0.024	161.450	127.180
Last-AS 5556	0.003	272306.203	0.001	3.608	0.033
Last-AS 12779	277.7E-6	76141.633	9.664E-6	106.276	0.201
Last-AS 2200	341E-6	20967.237	0.001	287.684	7.548
Last-AS 6675	6.938E-6	12441.026	83.23E-6	624.851	203.858
Last-AS 7853	266.8E-6	9415.567	387.8E-6	116.485	50.317
Last-AS 1795	0.001	5796.274	0.001	262.363	0.495
Last-AS 8342	259.6E-6	4797.801	0.001	255.108	25.010
Last-AS 702	277.3E-6	3748.348	228.5E-6	683.594	6.598
Last-AS 5379	65.66E-6	3641.193	234.4E-6	177.611	120.509
Last-AS 12925	5.112E-6	2746.041	84.21E-6	149.239	41.861
Last-AS 12542	0.068	2419.460	0.060	36.003	486.908
Last-AS 9193	267.2E-6	2373.810	0.001	169.793	10.656
Last-AS 25953	70.57E-6	2370.874	0.001	115.397	51.323
Last-AS 12300	406.4E-6	2252.516	0.003	231.415	84.485
Last-AS 10250	730.5E-9	2222.260	5.621E-6	118.277	0.239
Last-AS 5089	151.2E-6	1800.462	67.11E-6	242.101	0.848
Last-AS 2856	0.007	1585.285	0.001	128.338	134.938
Last-AS 174	0.004	1539.918	0.001	123.620	443.611
Last-AS 65432	0.001	1189.728	0.002	71.878	25.529
Last-AS 3269	131.1E-6	1144.157	253.8E-6	188.618	7.068
Last-AS 6848	4.049E-6	1133.818	2.964E-6	167.078	0.660
Last-AS 15569	671.6E-9	979.154	4.306E-6	124.957	115.224
Last-AS Unknown	0.012	852.047	0.013	47.848	1522.421
Last-AS 12457	6.725E-6	186.445	7.631E-6	107.265	2.418
Last-AS 3215	58.12E-6	0.000	31.78E-6	297.766	0.932
Last-AS 2917	16.96E-6	0.000	7.826E-6	295.854	0.507
Last-AS 5511	5.989E-6	0.000	7.075E-6	0.000	0.000
Last-AS 5669	552E-9	0.000	4.923E-6	0.000	0.000
Last-AS 1680	2.485E-6	0.000	3.445E-6	0.000	0.000
Last-AS 11908	123.7E-9	0.000	482.2E-9	0.000	0.000
Last-AS 5422	49.06E-9	0.000	430E-9	0.000	0.000
Last-AS 13273	41.02E-9	0.000	376.7E-9	0.000	0.000
Last-AS 568	7.672E-9	0.000	18.41E-9	0.000	0.000
Last-AS 13367	3.069E-9	0.000	0.000	0.000	0.000

- **Measure effectiveness of remote office and directly connected ISP's**
- **Thresholding can be used to alert users to any SLA violations.**
- **Validate efficiencies of ISP peers**
- **Grade performance of multiple ISP's**

Troubleshooting Inside the Cloud



Time: Thu Feb 13 07:12:02 PST 2003 ☑ **Lookup**

Hop	Address	RTT	ms	...
0	10.131.24.35		0.0	...
1	10.131.24.1		0.612	...
2	10.130.0.141		1.226	...
3	10.130.0.145		1.903	...
4	wb7500-1.warnerbros.com		2.387	...
5	168.161.218.129		2.905	...
6	168.161.48.48		2.123	...
7	172.25.199.163		120.857	...
8	10.140.8.2		120.62	...
9	172.25.252.15		119.874	...

- **Graphical network route analysis pinpoints hidden bottlenecks**
- **Identifies destinations with critical performance issues**
- **Measures hop-by-hop delay metrics to localize network latency problems**

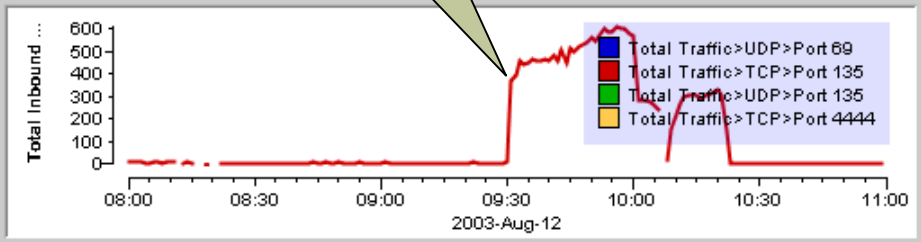
MS Blaster Worm

Detect the infection

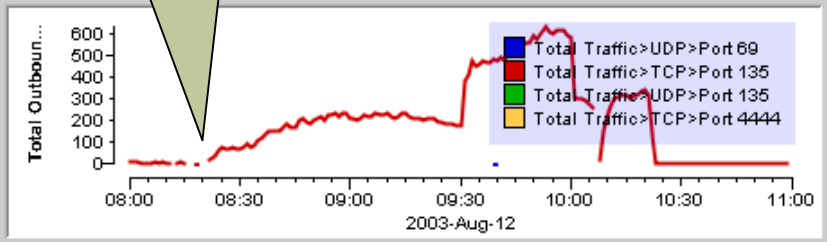
Where did it start?

Who is affected?

Virus affected Ports INBOUND TRAFFIC



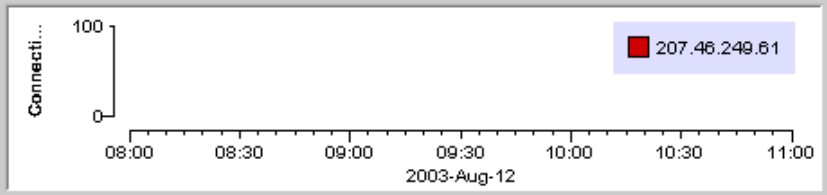
Virus affected Ports OUTBOUND TRAFFIC



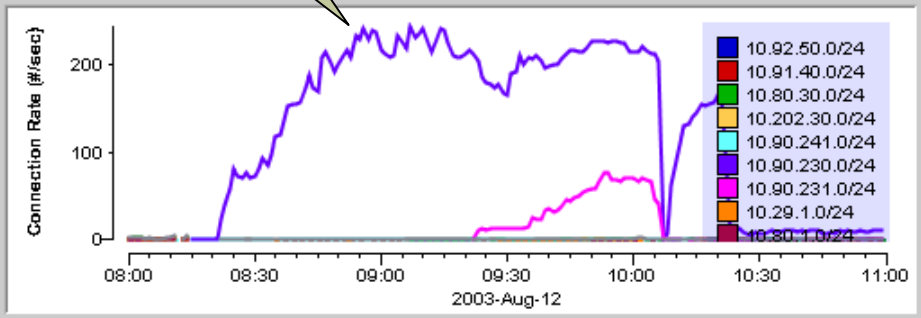
TRAFFIC to /24 subnets

Group	Connections (#)	Connection Rate...
10.90.230.0/24	1330832	123.225
10.90.231.0/24	110947	10.273
10.90.13.0/24	7230	0.669
	1530	0.142
	1270	0.118
	928	0.086

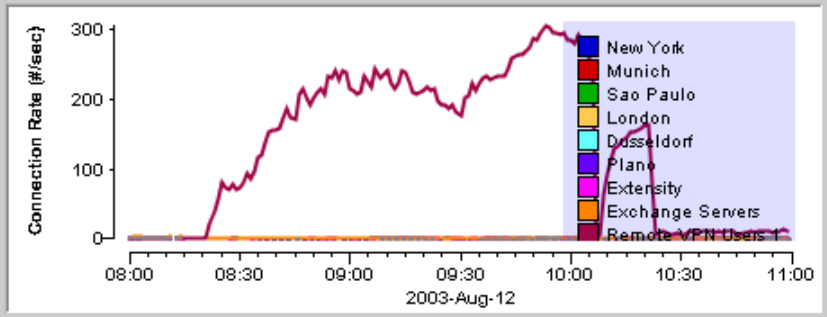
TRAFFIC to www.windowsupdate.com



Connection Rate for /24 Subnets



Connections Rate for Business Groups



Conclusions

- This is an interesting, but challenging problem (hardware and software)
- Capturing meaningful data is hard
- Make sense of them is even harder!

CREDITS

- SLAC (Stanford Linear Accelerator Center)
- Yahoo!
- Cisco
- Stanford and U. of Utah, DOE, DOD, National Labs.
- Staff of Network Physics

- We are looking for data/test sites and collaborators

Questions?

Silvia Veronese

NETWORK PHYSICS

Sveronese@networkphysics.com