Proactive Network Monitoring at The Depository Trust and Clearing Corporation

Raoul Farrell : DTCC
Nalini Elkins : Inside Products, Inc.

rfarrell@dtcc.com
Nalini.elkins@insidethestack.com

Session 7610

August 2, 2010

SHARE in Boston

Our SHARE Sessions – Boston

- Proactive Network Management at the DTCC
  Monday, August 2, 2010: 11:00 AM-12:00 PM

- TCP/IP Performance Management for Dummies
  Monday, August 2, 2010: 4:30 PM-5:45 PM

- AT-TLS Implementation and Diagnostics at U.S. Bank
  Wednesday, August 4, 2010: 11:00 AM-12:00 PM

- Best Practices for Certificate Management – (Panel)
  Thursday, August 5, 2010: 11:00 AM-12:00 PM

Agenda

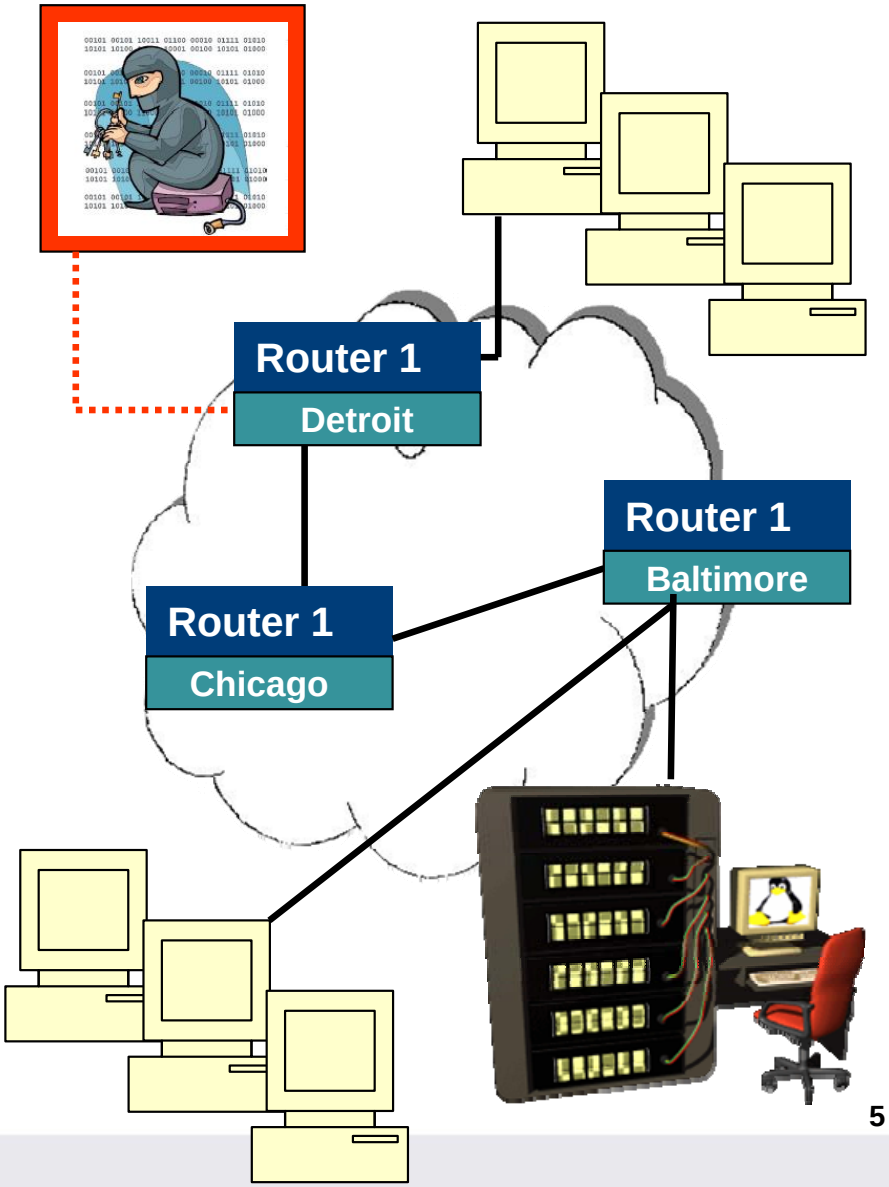
- Introduction to the DTCC
- Business requirements
- Network management needs and goals
- Proactive management
- Metrics used
- Processing of alerts and warnings
- Integration into our operational systems
- Results

Introduction to the DTCC

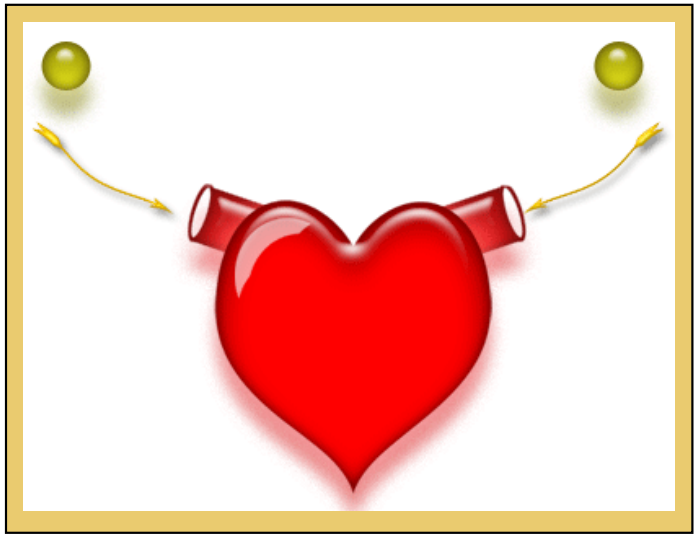
- The Depository Trust and Clearing Corporation (DTCC) is at the epicenter of the financial world.
- The business of the DTCC involves the safe transfer of securities ownership and settlement of trillions of dollars in trade obligations, under tight deadlines every day.
- At the same time, DTCC's primary mission is to protect and mitigate risk for its members. DTCC ensures the capacity, certainty and reliability required to clear and settle today's enormous trading volumes.

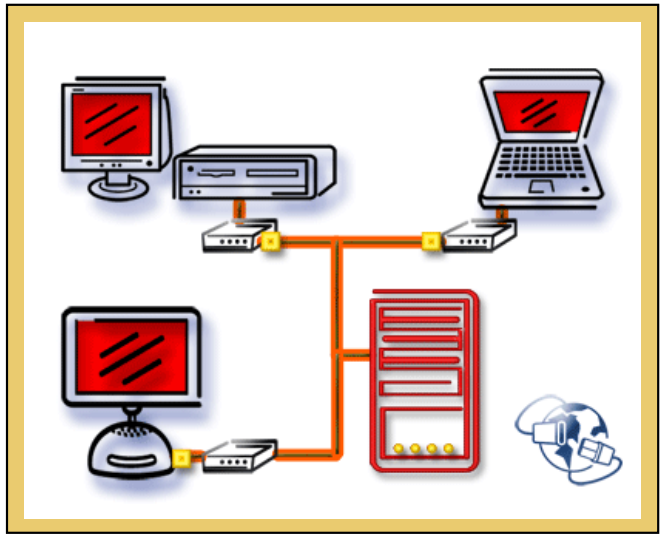
Business Requirements

- Interconnect the financial world…
- We are a service provider
- Close the markets…
- Do all this in a timely manner.
- And… run it as a business.
- Let's take each of the above and see the implications for network management.



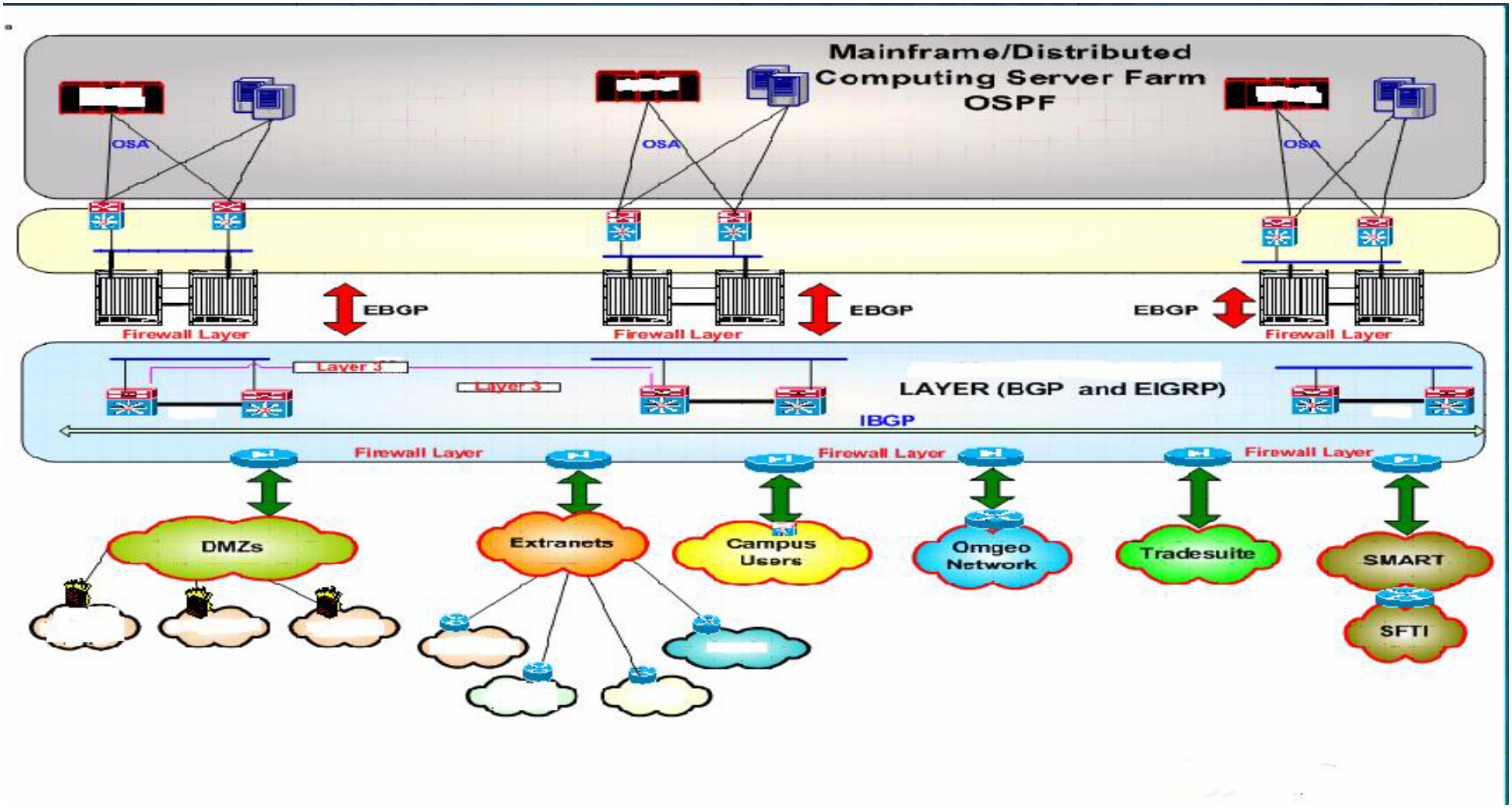
DTCC Interconnects the Financial World





- The network is at the heart of DTCC's business.

High Level Network Diagram

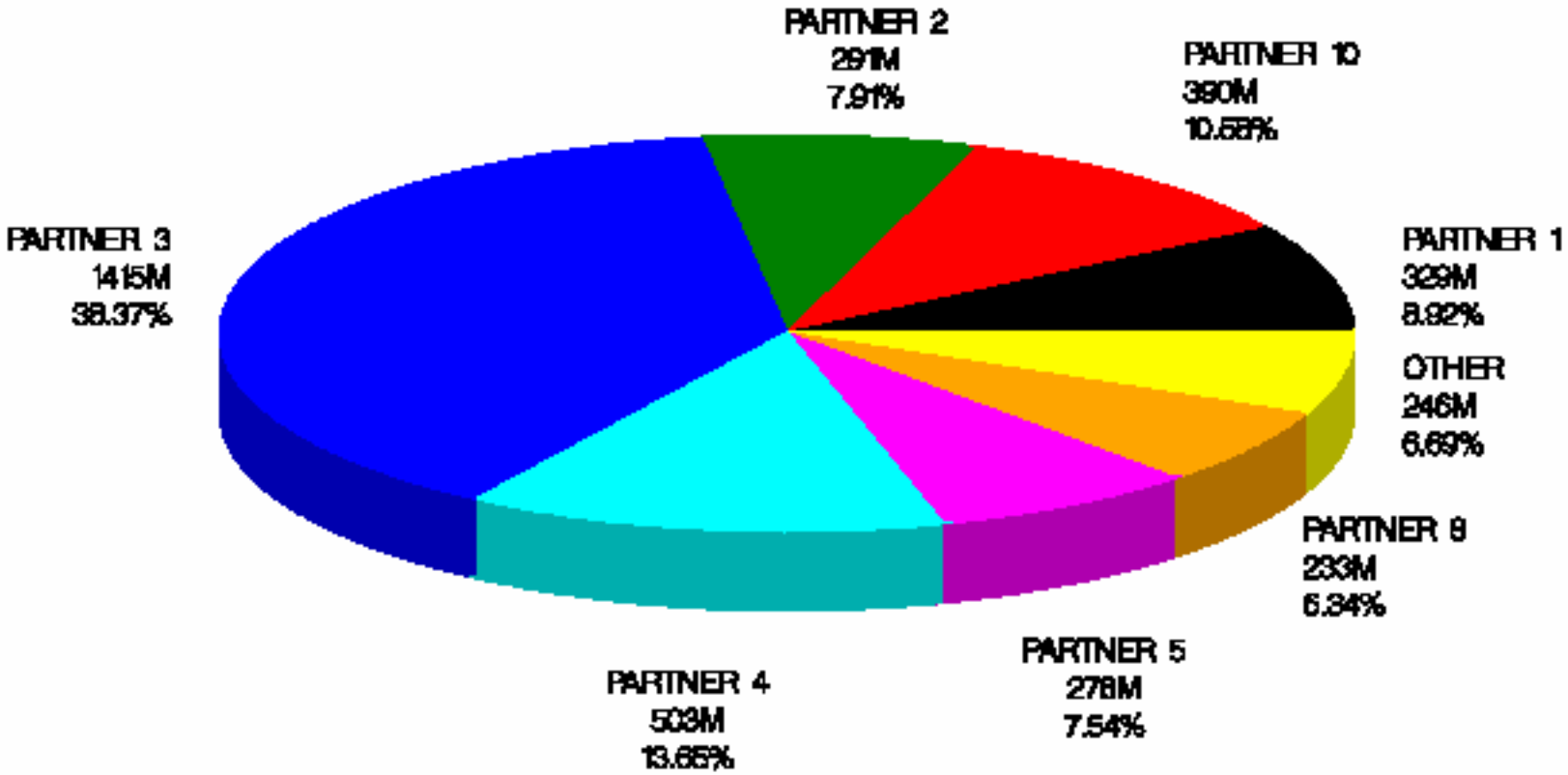


DTCC is a Service Provider

- What kind of service are we providing?
  - View by business partner
  - View by service (port)
  - Monitor availability
  - Monitor network response time
- How do we know if we are providing it?
  - Set thresholds
  - Define services
  - Get alerts
  - Monitor
- What do we do if there is a problem?

TOP PLAYERS -- TOTAL IP ACTIVITY -- JANUARY 5TH 2010

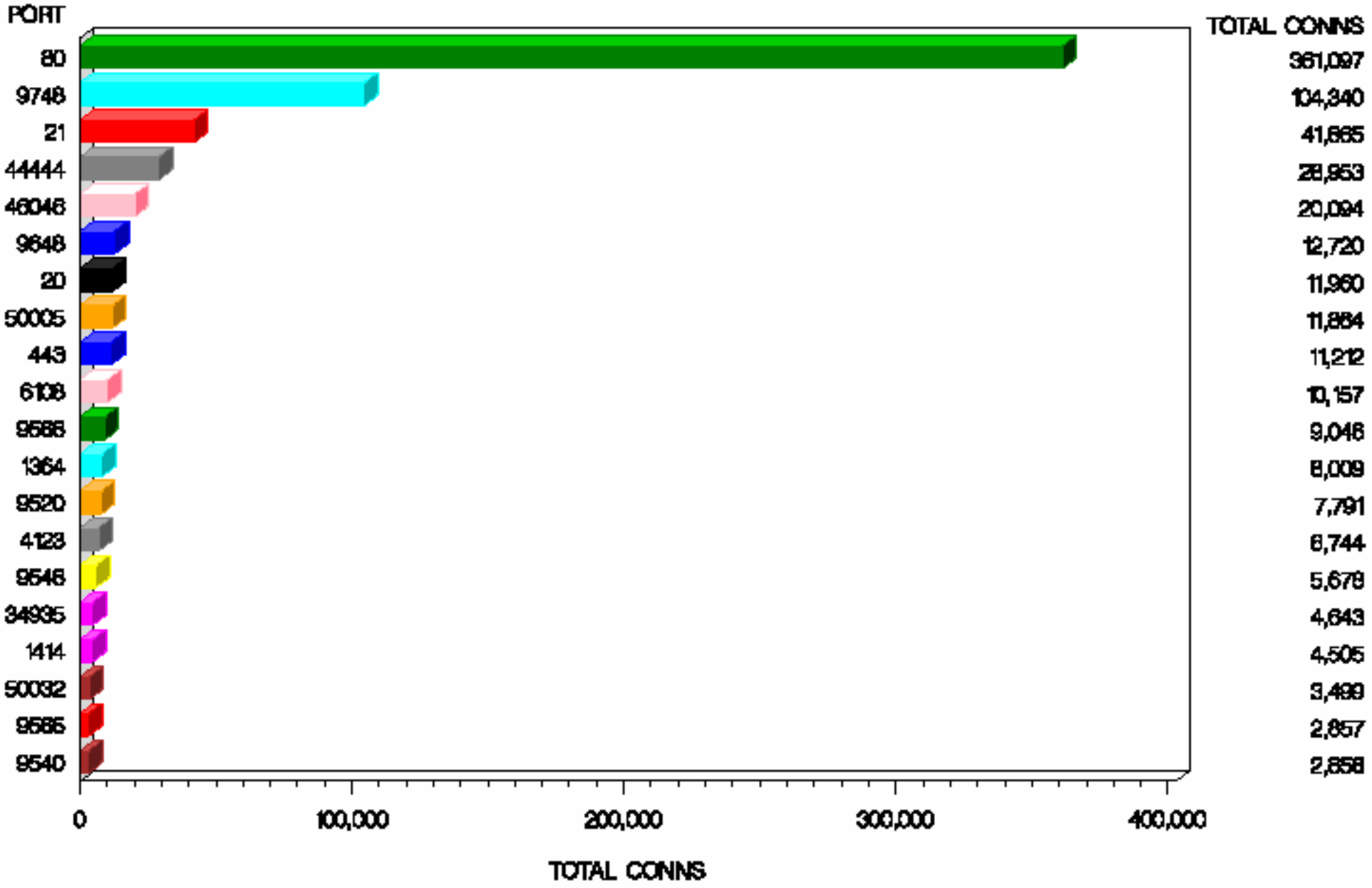
TCPSTACKID=



GRAPHICS BY NSP

TOP PORTS -- MAY 5TH 2009

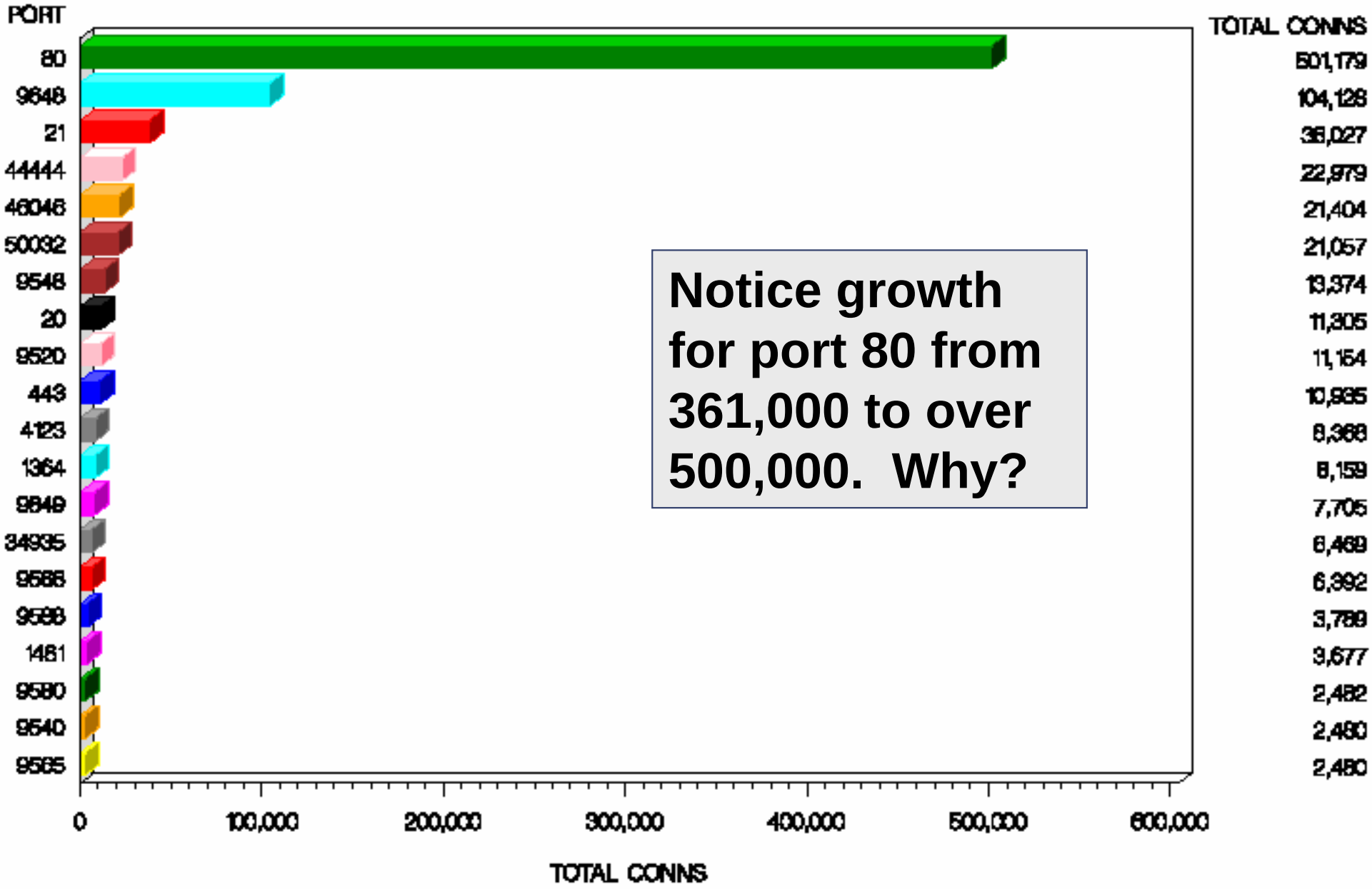
TCPSTACKID=



GRAPHICS BY NSP

TOP PORTS -- MARCH 5TH 2010

TCPSTACKID=



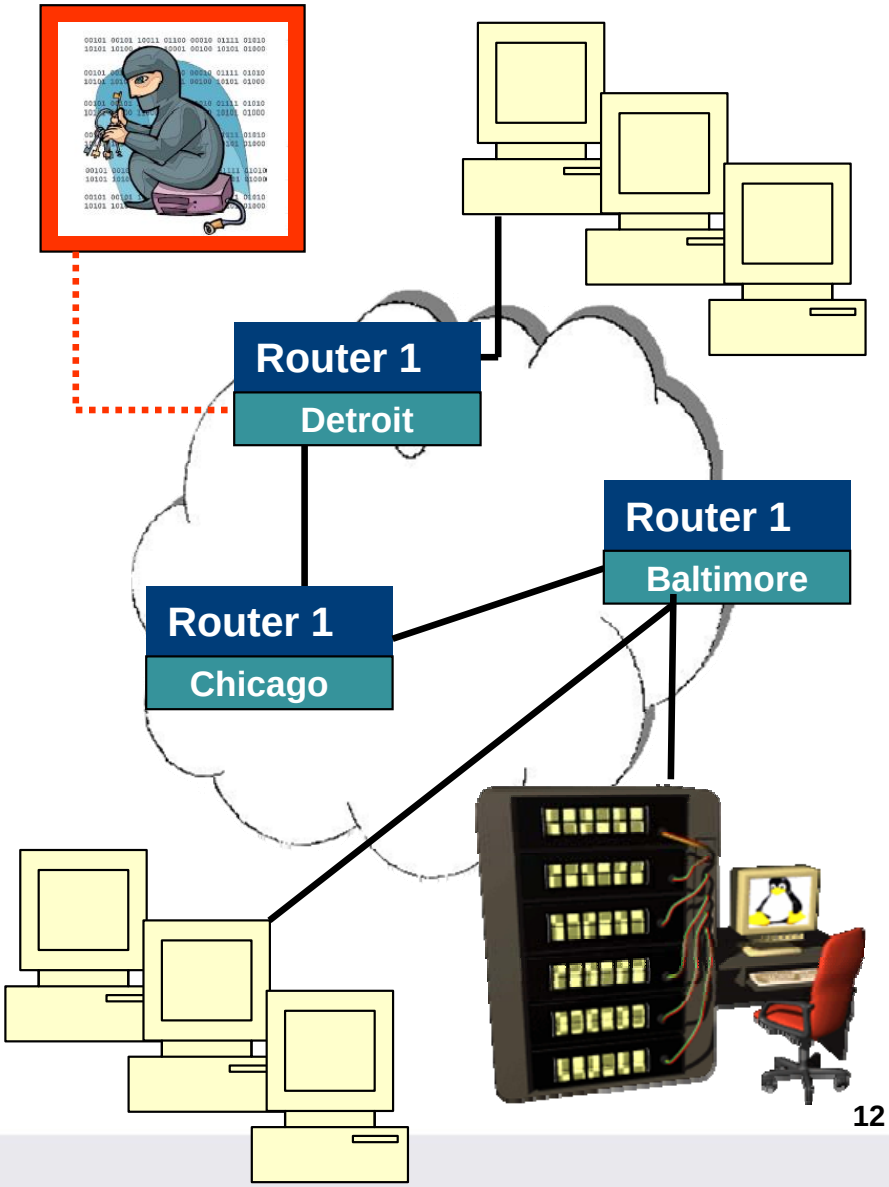
Notice growth for port 80 from 361,000 to over 500,000. Why?

GRAPHICS BY NSP

Keeping the Network Available

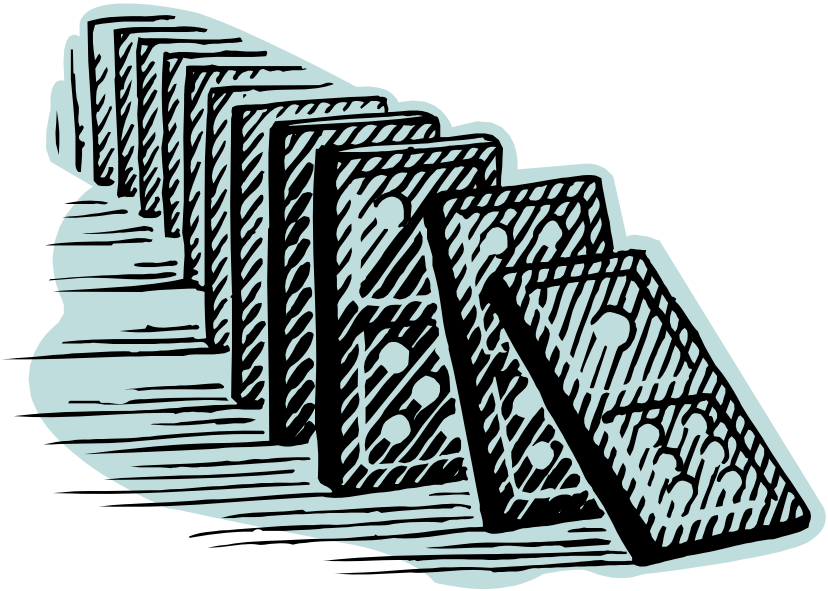
- Mainframes
- Routes
- Routers
- Servers
- Applications

- All have to be monitored in different ways.
- Fallback strategies devised.



Monitor Unavailability

- Metrics
  - Times unavailable.
  - Duration of unavailability.
  - Unavailable from where?



- Correlate unavailability with other resources.

- Can have domino effect (one resource going down impacts another).

Service Delivery Impact !!!

How we do Availability Checking

Group	Host Name	Source IP	Address Monitored	Available	Last Monitored
	192.168.1.231	127.0.0.1	192.168.1.103	No	2006-06-09 13:21:18.0
231Group	192.168.1.231	192.168.1.231	192.168.1.101	Yes	2006-06-09 13:22:19.0
232Group	192.168.1.232		192.168.1.101	Yes	2006-06-09 13:21:17.0

We use Availability Checker, a real-time monitor checking the availability of routers, switches, servers and any other networked devices that is in communication with the mainframe.

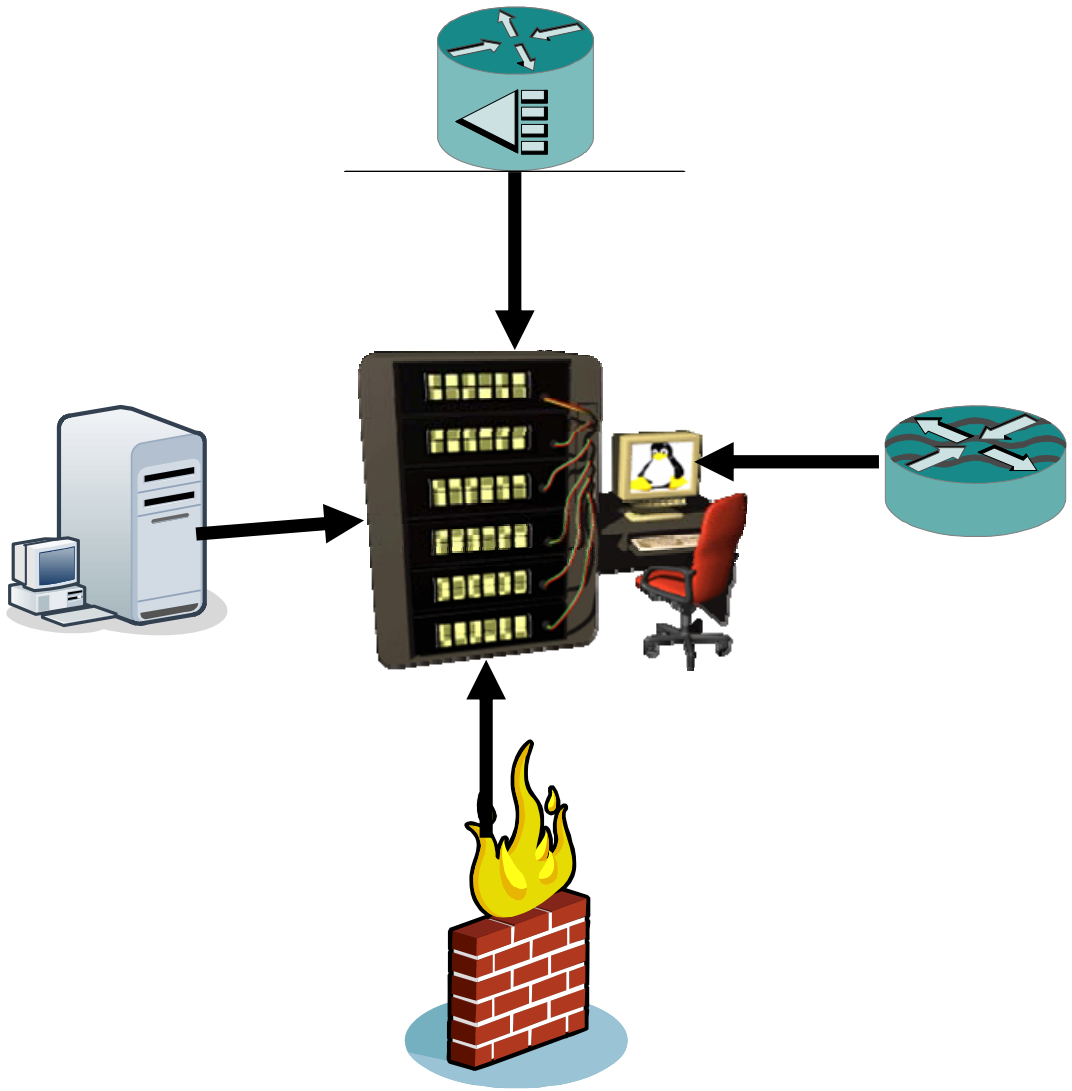
ICMP (Ping) is used to perform this activity. (Availability Checker requests are submitted to the Mainframe to Ping the remote device). Mainframe to End-device connectivity monitor generates SNMP Traps that are shipped to the NETCOOL Server. Unavailable Resource is considered a critical event.

This tool provides access to historical data about network device response time (Hourly, Daily, Weekly, Yearly) and unavailable resources.

What do we monitor?

- Routers,
- Switches,
- Firewalls, and
- Application servers.

- All must have connectivity to all mainframes.



How we do Application Checking

Group	Host Name	Source IP	Address Monitored	Local Port	Description
Dallas	Dallas1.9	172.29.122.223	172.29.122.222	21	FTP
New	Dallas1.9	172.29.122.222			

APPLICATION CHECKER

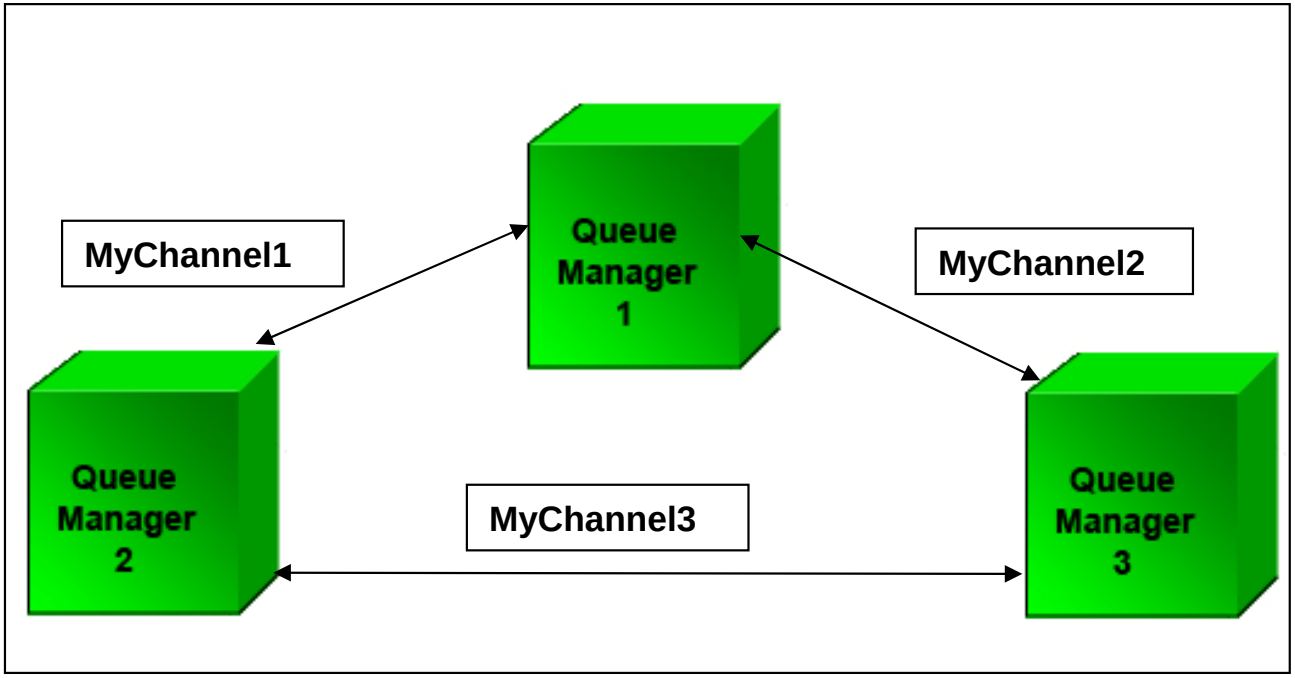
Available	Last Monitored	Response Time (Milliseconds)	Graph Last 24 Hours	Graph Last 7 Days	Graph Last 31 Days	Graph Last 365 Days
No	2010-05-02 06:55:34.0	625				
Yes	2010-05-02 06:55:33.0	750				

- We use Application Checker, a real-time monitor checking the availability of local or remote applications (TCP Ports) from the mainframe.
  - Mainframe to Application monitor generates SNMP Traps that are shipped to the NETCOOL Server. Traps are sent on Application state changes.
  - Unavailable Resources is considered a critical event.
  - Response time threshold exceeded generates warning traps.
- This tool provides access to historical data about network response time (Hourly, Daily, Weekly, and Yearly) and unavailable resources.

What do we monitor?

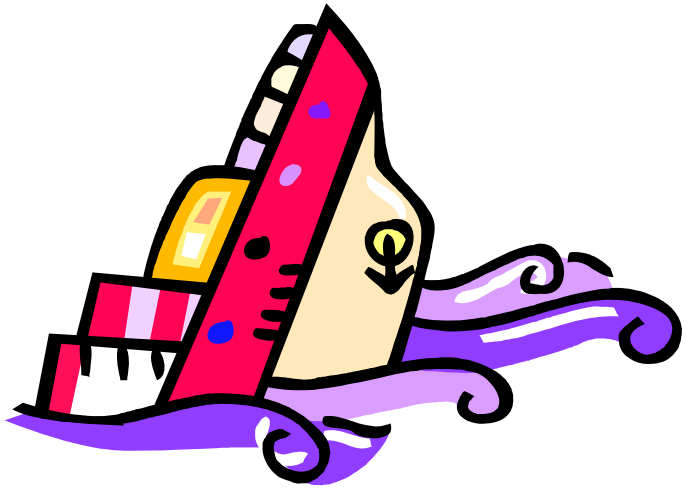
- MQSeries,
- DB2,
- FTP, and
- NDM

- Must be able to log on from all mainframes.



Test with Backup and Recovery

- Do availability / application checking before & after: Take a “snapshot”
  - Normal mode switch to backup data center
  - Disaster recovery drill



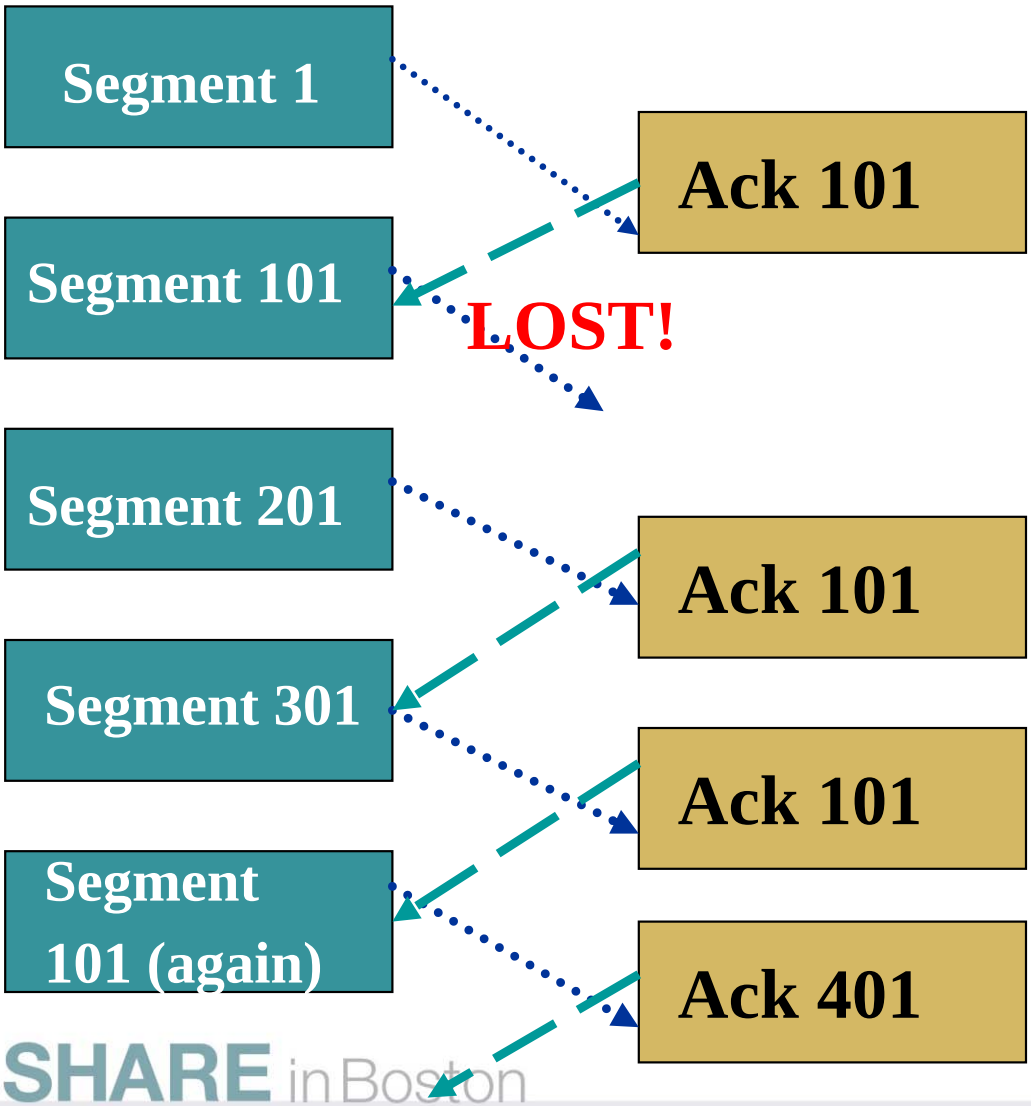
Monitor Response Time

- Network response time (round trip time)
- Round trip time = network degradation?
- Should round trip time average be used? Max? Round trip variance?
- Host / application response time (different group)

Network degradation can be:

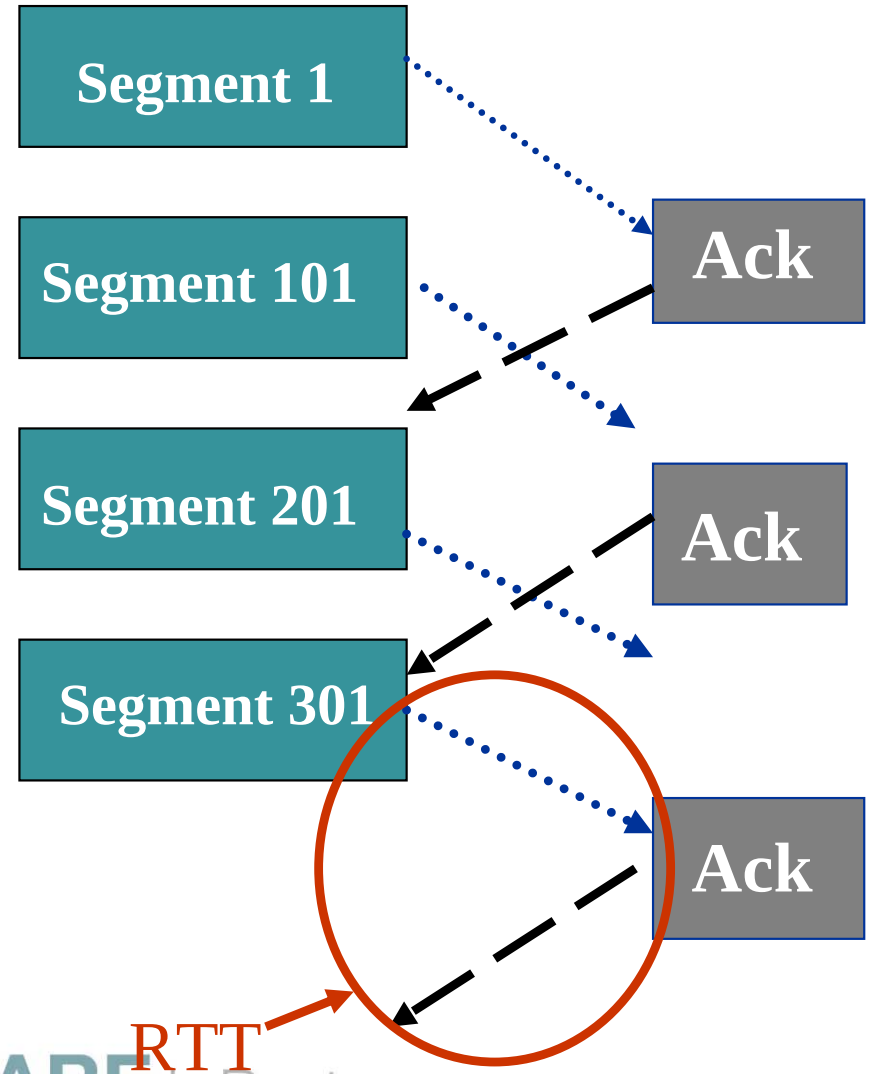
- **Retransmissions**
- **Duplicate acknowledgments**
- **Also signaled by congestion window**

What is a Duplicate ACK?



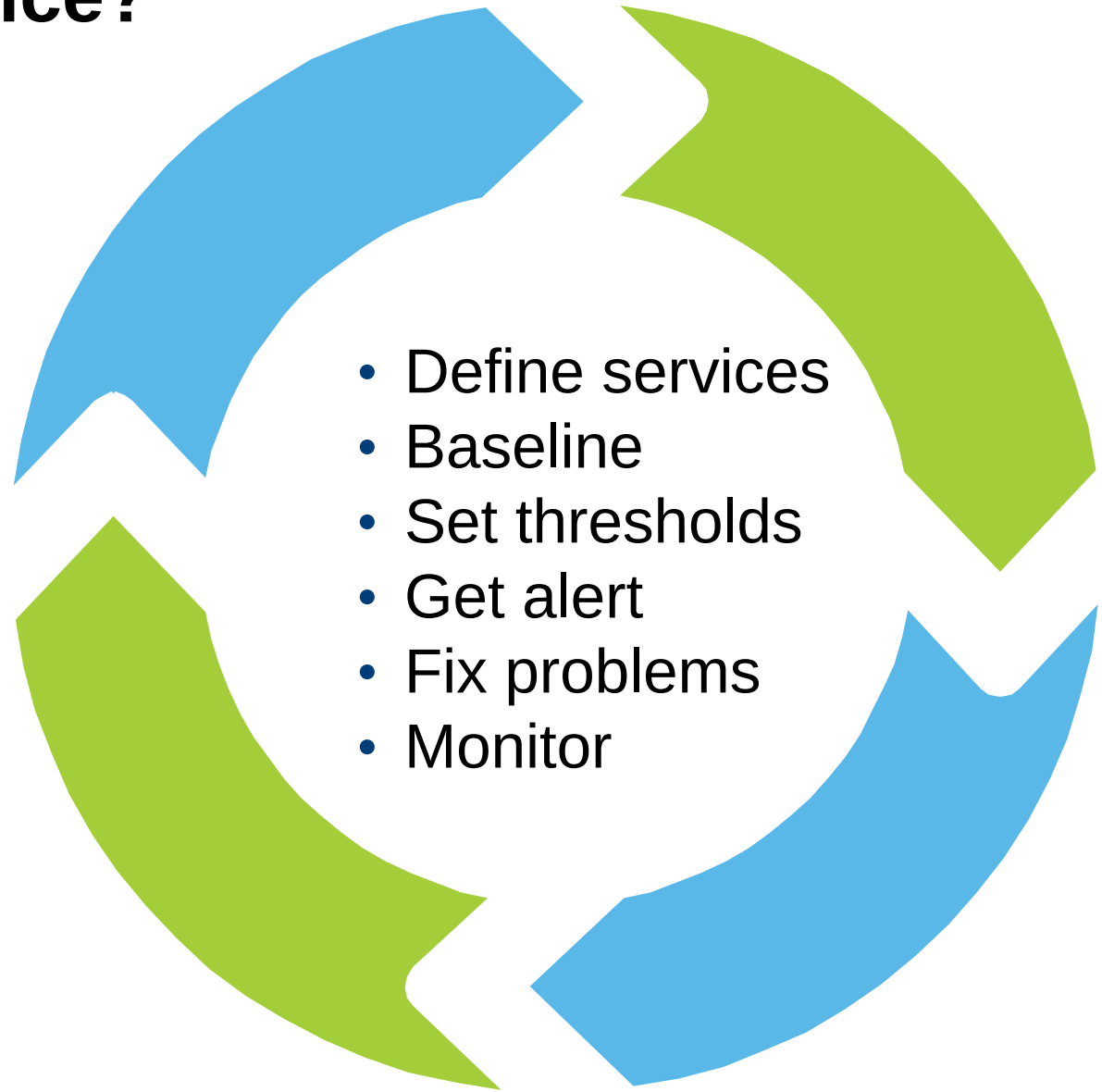
- Assume each segment has 100 bytes.
- Ack is for the next byte of data it is waiting for.
- A duplicate ack is sent when a packet is received and the sequence number indicates that it does not contain the byte you are waiting for.

Round Trip Time



- RTT is basically network time.
- RTT measures from the time the last character is sent to when the ACK comes back.
- This is similar to a PING except using the real data length used by the application and using TCP vs. ICMP.

How do we know if we are providing good service?



- Define services
- Baseline
- Set thresholds
- Get alert
- Fix problems
- Monitor

Create Baseline

- Baselining your network is a crucial task
- Problem areas: shift changes, weekends, red letter days
- Re-baselining with changes in topology

Set Thresholds

- Setting thresholds for a customer (Company A) is much different from another (Company B) whose profile is much different.

How do we set thresholds?

- Separate baseline data on a per client basis
  - Round trip time
  - Duplicate acknowledgments
  - Retransmissions
  - Bytes in / out

- Apply statistical measurements
  - Median
  - Maximum
  - 90th percentile

Sample Duplicate Ack Analysis

	Partner 1	Partner 2	Partner 3	Partner 4	Partner 5
Minimum	0	0	0	0	0
Median	1	1	1	1	1
90th percentile	3	1	24	14	11
95th percentile	3	2	40	34	40
98th percentile	6	8	747	98	319
99th percentile	11	164	902	288	648
Maximum	462	2,918	1,371	33,794	14,225
Suggested **Warning** Threshold	5	5	50	40	50
Suggested **Critical** Threshold	25	175	1,000	300	650

Produces Warning Definitions

- Each client is different
- Want to warn at different levels

Sample Client Configuration

```
IDENTIFIER                    Partner 1
  IP-ADDRESS4                 123.456.*.*
  IP-ADDRESS6                          NA
  LOCAL-PORT                            *
  REMOTE-PORT                           *
  MONITOR-INTERVAL                     60
  CONGESTION-WINDOW                  5000
  ROUND-TRIP-TIME                     250
  ROUND-TRIP-VARIANCE                2000
  BYTES-OUT                             -
  RETRANSMITS                           2
  CONNECTION-TERMINATED                 N
  DUPLICATE-ACKS                        4
  HUNG                                 10
  STATUS                           SYNSENT
  LOCAL-WINDOW-0                        1
  REMOTE-WINDOW-0                       1
  OUT-OF-ORDER                          0
```

Early Warning System

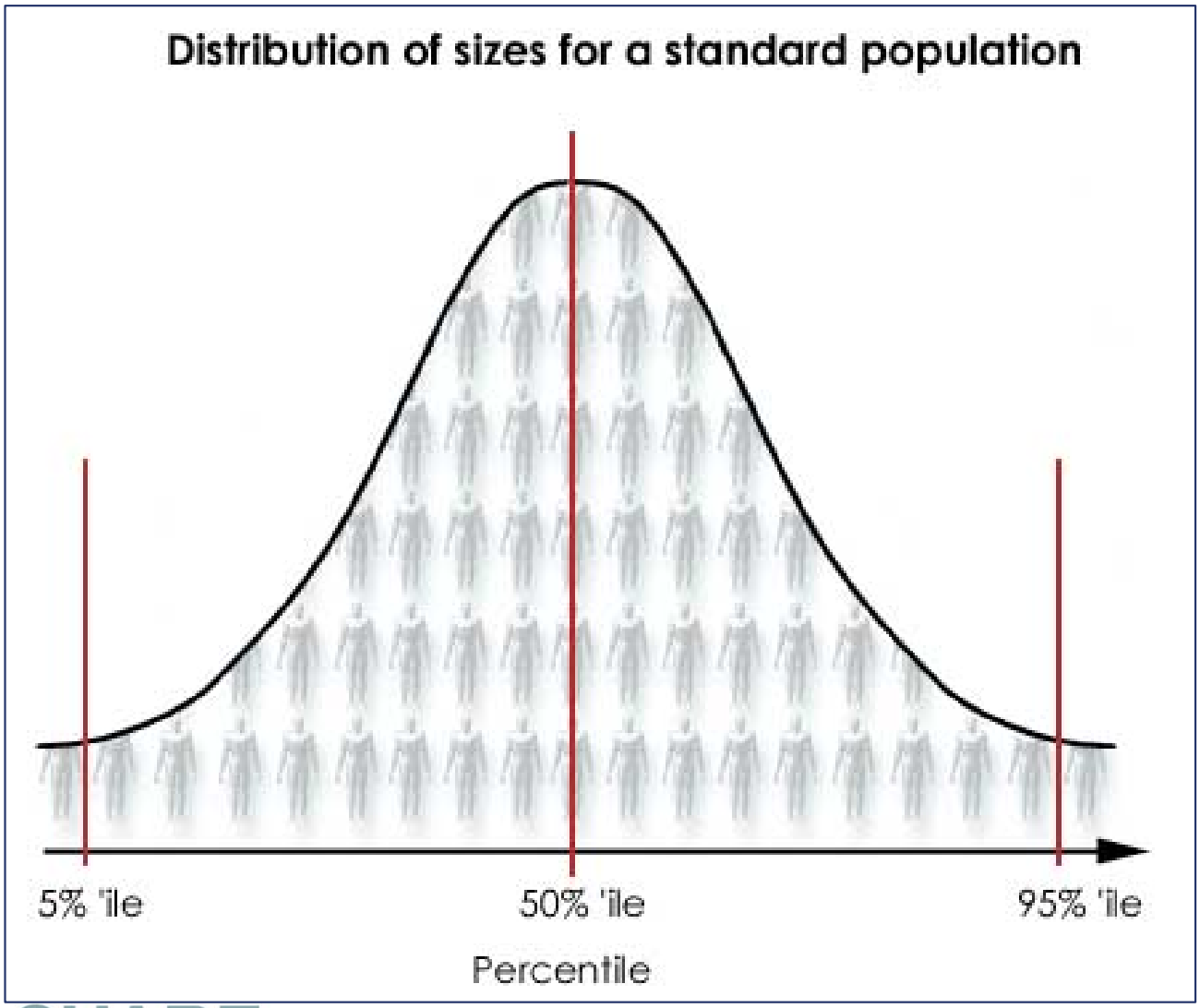
Inside Products, Inc.

Alerting Fundamentals

Don’t cry wolf but…

Don’t be asleep at the wheel

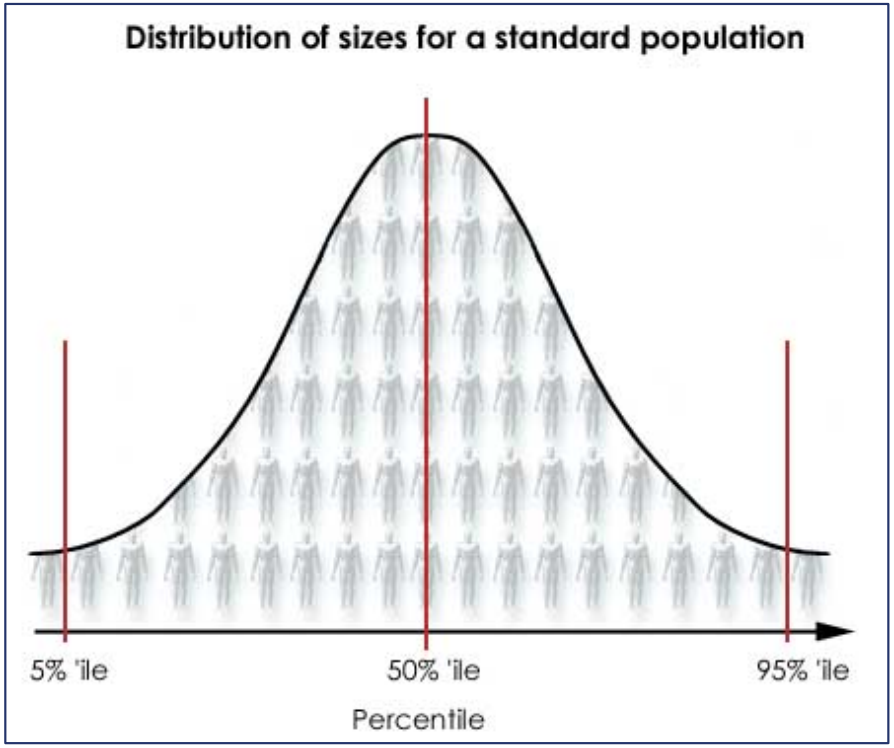
Some Words on Statistical Soundness



- Why these stats?
- 90th, 95th percentile show outliers

Sample Size

- Too little data is no good
- Garbage in, garbage out



- Example of Small Sample
- Only have 3 people all with a height of 5 feet, then graph will be very skewed.

How we got baseline data

- Connection Log (NMI)
- Can also use SMF records
- Data collection / manipulation / storage are quite large issues

Two Step Process

- First, figure out what you are providing currently, and deal with obvious problems.
- But second (once you know what is possible/reasonable), may want to negotiate with customers and get their agreement on what service they want/require.
- (For those which need higher capacity, you may be able to negotiate higher charges for providing it.) Then you have actual SLAs to measure against, not just internally generated SLOs (Service Level Objectives).

Getting Alerts

- Sample alerts

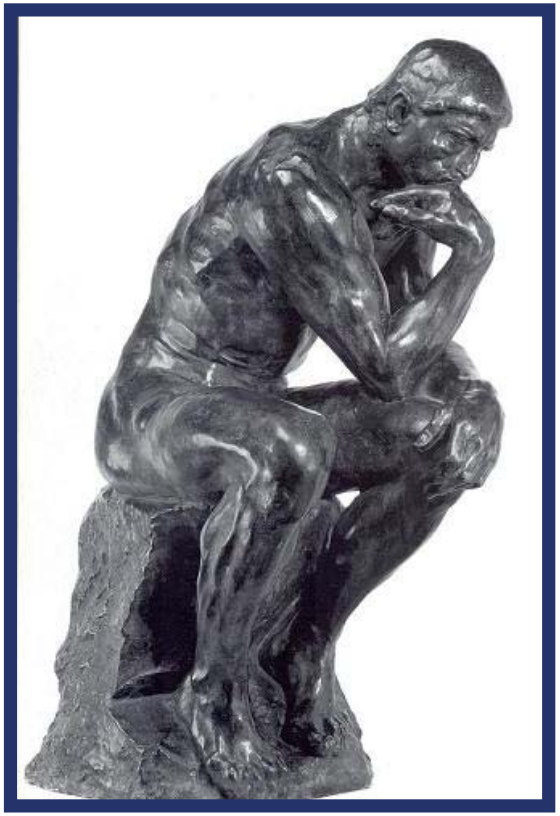
2010-06-07 01:30:17.12	**ITSWA201W**	**MY BANK**	**CON WINDOW**	**LT**	**5,000**
2010-06-07 01:30:57.14	**ITSWA205W**	**MY BANK**	**RETRANSMITS**	**GT**	**10**
2010-06-07 08:30:11.25	**ITSWA202W**	**MY BANK**	**RD TRIP TIME**	**GT**	**100**

- Alert correlation
  - Goal is to send to NetCool
  - SNMP traps
  - Correlate with other activity

What do we do if there is a problem?

- In depth analysis of problem area
  - What happened?
  - Why did it happen?

- Many groups may be involved
  - Network software & hardware support
  - Network operations
  - Customer Support Call Center
  - Business partner



Analysis of Top 50 Connections with Most Duplicate Acknowledgments

VERSION 1.3.1 INSIDE THE STACK
P001 - THE MOST TCP DUPLICATE ACKNOWLEDGMENTS CONNECTIONS
CONTAINS THE TOP 50 CONNECTIONS

aaa.bbb.ccc.ddd

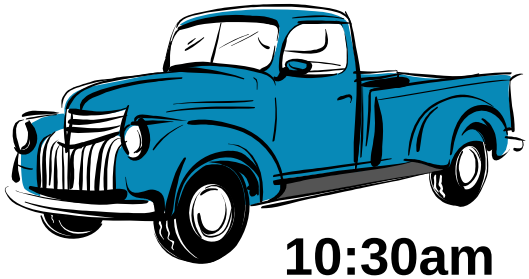
START DATE	START TIME	LOCAL PORT	REMOTE IP ADDRESS	REMOTE PORT	BYTES IN	BYTES OUT	ROUND TRIP TIME	ROUND TRIP VARIAN	RETRAN COUNT	DUP ACKS
2010-06-13	16:09:48	21553		20	0	851.6M	0	1	1,197	75,988
2010-06-13	12:37:49	20		62167	0	2.045B	329	48	20	56,865
2010-06-13	13:08:23	2440		20	0	421.8M	1	0	286	20,194
2010-06-13	17:06:48	28536		20	0	154.2M	1	0	167	10,931
2010-06-13	19:06:33	43439		20	0	162.5M	1	0	122	8,589
2010-06-13	20:06:41	50924		20	0	200.1M	1	1	87	7,840
2010-06-13	23:06:15	9311		20	0	127.9M	1	1	96	6,980
2010-06-13	21:06:42	58478		20	0	179.9M	1	1	79	6,929
2010-06-13	22:06:27	1548		20	0	146.6M	1	0	89	6,633
2010-06-13	18:06:30	35981		20	0	155.5M	1	0	74	6,019
2010-06-14	02:06:20	32165		20	0	139.4M	1	1	70	5,873
2010-06-14	03:06:20	39762		20	0	140.1M	1	0	67	5,643
2010-06-14	00:06:19	16938		20	0	126.8M	1	0	68	5,346
2010-06-14	01:06:19	24584		20	0	128.0M	2	1	59	5,041
2010-06-13	22:59:03	8357		1364	3,364	144.5M	259	183	7	3,477
2010-06-13	16:37:55	50032		36155	5.059M	24.70M	10	14	0	2,478
2010-06-13	09:07:24	50032		53630	114.7K	523.3K	52	49	0	1,671
2010-06-13	09:07:16	50032		61870	118.1K	499.7K	27	23	0	1,611
2010-06-13	22:36:53	5526		1364	3,360	61.91M	231	180	6	1,582
2010-06-13	20:01:53	50335		1372	3,732	115.1M	110	35	4	1,468
TOTALS					5.302M	5.327B			2,498	241.1K

In the future…

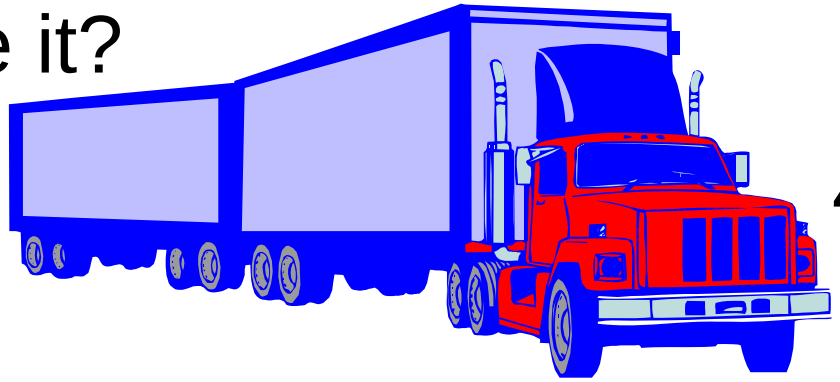
- The ability to distinguish the thresholds during different time periods. For instance:
  - Market hours
  - Non-Market hours
  - Special occasions (e.g. known heavy trading volume or information delivery days – days of the week, month, or year)
  - Special subsets of Market hours – e.g. Market Open (the first 15-30 minutes of the market day) or Market Close (the last 15 minutes of the market day)

DTCC Closes the Markets

- Times of the day call for extra capacity
- Do we have it?
- How do we measure it?



10:30am



4:00pm

DTCC Runs IT as a Business

- How?
- Run lean
- Constant tuning
- High availability