Traffic Management Systems An Impact Analyses

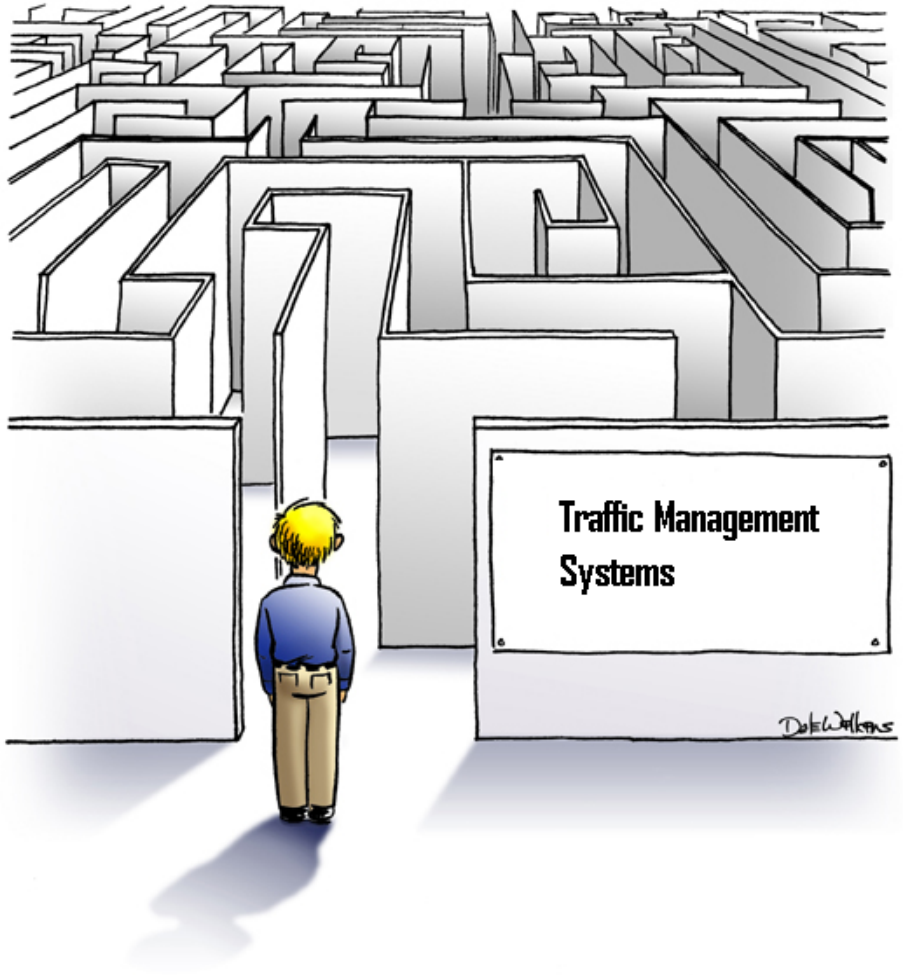
Mark Allen
Shuchi Muley

Agenda

- Problem Statement
- Approach
- Protocol Basics
- Data Sets
- Network Structure
- Data Analysis and Results
- Challenges
- Future Work
- Q & A

Problem Statement

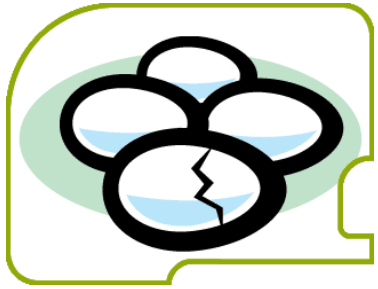
In the busy world of the Internet, users are pretty much able to derive any content they can imagine. With the limited amount of bandwidth available to ISPs, the growing concern they may have is regarding controlling the traffic to make improvements for efficiency. This project will serve as the analysis of the technical impacts of implementing a traffic management system.



Approach

- Categorize the Data (Know Your Network)
  - Web (HTTP/HTTPS)
  - FTP
  - Streaming Audio
  - Streaming Video

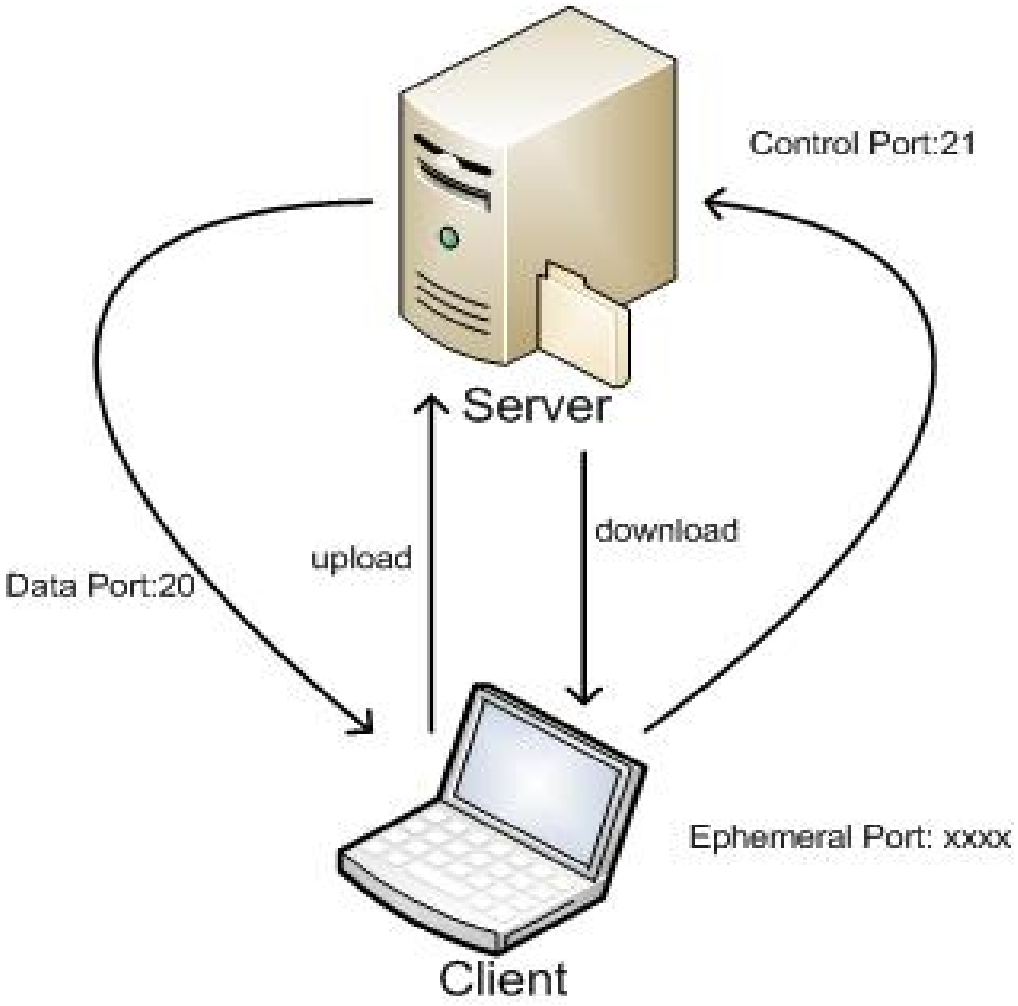
- Classify the Data (Know the Internet)
  - Legitimate
  - Illegitimate



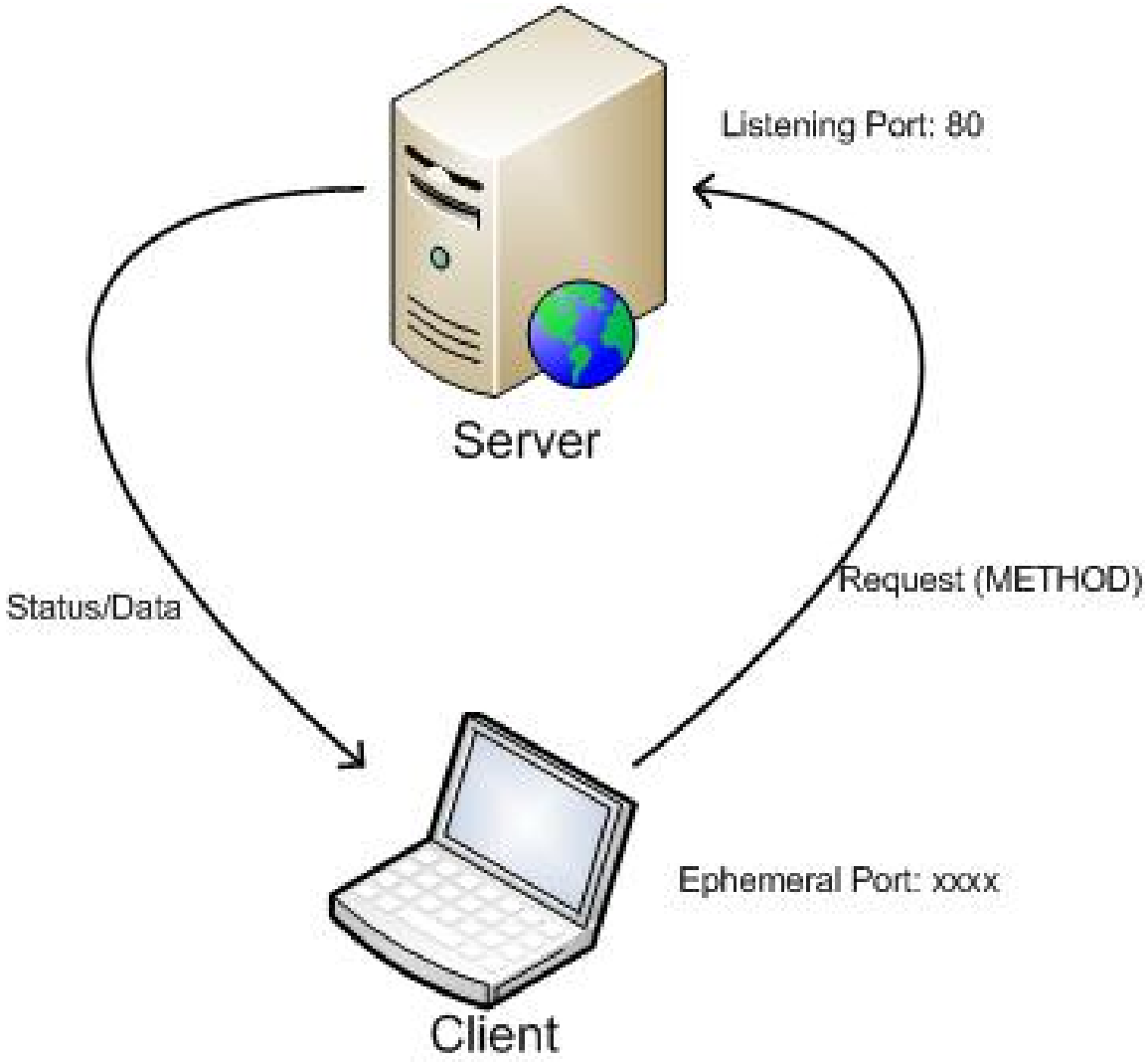
Traffic Management Systems

- Know how they work together
- Products:
  - Zeus Technology's Zeus Extensible Traffic Manager (ZXTM)
  - Secure Computing's Secure Web Smart Filter
  - ARA Network's Traffic Monitor

Protocol Basics - FTP

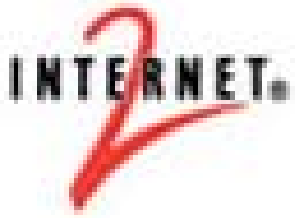


Protocol Basics - Web



Data Sets

- Two data sets from DatCat from the “Day In The Life”, or DITL, Internet Project
  - Collected from the Abilene Network Juniper T-640 routers (Internet2)
- Cities:
  - Atlanta, GA; Chicago, IL; Houston, TX; Kansas City, MO; Los Angeles, CA; New York, NY; Salt Lake City, UT



Data Sets

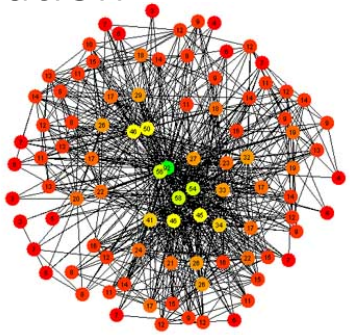
- 2007
  - Summary: NetFlow v5 data
  - Sampling ratio: 1/100
  - Anonymized: last 11 bits set to zero
  - Start Time: 2007-01-09 00:00 UTC (+0000)
  - End Time: 2007-01-11 00:00:01 UTC (+0000)
  - Duration: 2 days 00:00:01 (172801.0 s)

Data Sets

- 2008
  - Summary: NetFlow v5 data
  - Sampling ratio: 1/100
  - Anonymized: last 11 bits set to zero
  - Start Time 2008-03-19 00:00 UTC (+0000)
  - End Time 2008-03-20 00:00 UTC (+0000)
  - Duration 1 Day (86400.0 s)

Network Structure

- Many partners connecting to each other
  - Extremely high speed connections
  - Working together for fast application delivery
- Each partner has it's own Internet connection
- Should be able to see source and destination for one location juxtaposed in another location
  - Sampling and Anonymization

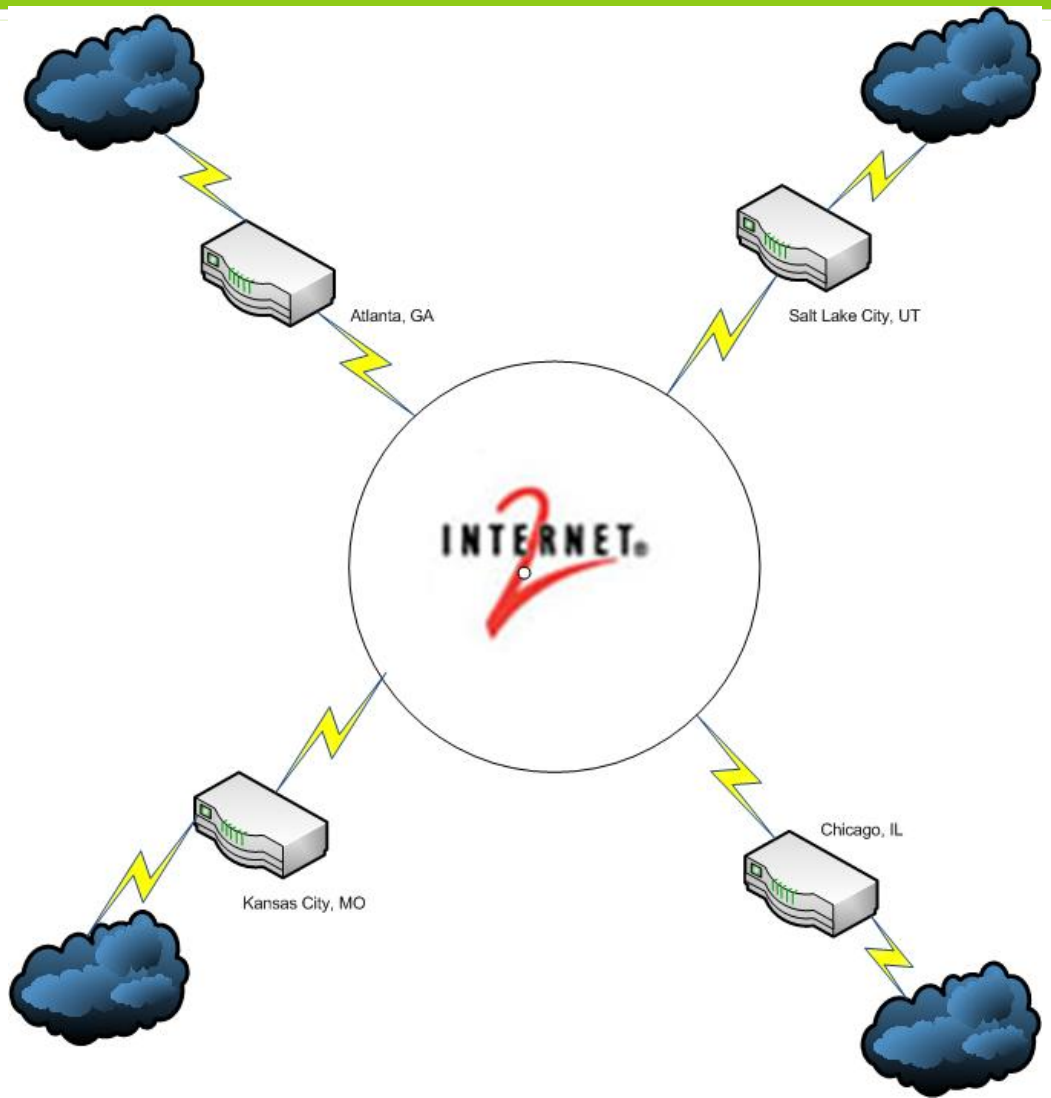


Network Structure

CONNECTORS

- 3ROX
- CENIC
- CIC OmniPoP
- Drexel University
- GPN
- Indiana GigaPoP
- KyRON
- LEARN
- LONI
- MAGPI
- MAX
- MCNC
- Merit Network
- MREN
- NOX
- NYSERNet
- Oregon Gigapop
- Pacific Northwest GigaPoP
- SoX
- University of Memphis
- University of New Mexico
- USF/FLR
- University of Utah/UEN

Network Structure



Data Analysis

FTP Analysis

- Filtered out the traffic
  - Port 21 – control traffic
  - Port 20 – data traffic
- Sorted the data
  - Bytes
  - Packets

PORT 21

Identified the major players between whom the communication was taking place.

sIP	dIP	sPort	dPort	Bytes	packets	sTime	eTime
163.221.8.0	21	193.233.8.0	50458	15000	10	2008/10/12T12:51:58.835	2008/10/12T12:52:33.402
163.221.8.0	21	193.233.8.0	50458	15000	10	2008/10/12T12:51:54.361	2008/10/12T12:52:33.060
128.113.24.0	21	193.233.8.0	63181	15620	11	2008/10/12T12:52:19.249	2008/10/12T12:52:50.711

Port 21

- Identified the bytes, and packets sent across these major IP's
- IP: 163.221.8.0
  - Packets: 1300
  - Bytes: 350,019
  - Duration: 3 hours

Port 21

- Results
  - Large amount of data transferred for a long time.
- Re-Analysis
  - Conversation on any other port?
- Results
  - Same results. No other conversation

Port 20

- Analyzed the data traffic for port 20
- Results
  - Conversation happened between a few IP addresses for a long time
- Re-Analysis
  - Conversation on any other port?

Other Conversation

- Conversation over port 21 and 80

130.14.24.0	**21**	**140.109.56.0**	**57889**	**1**	**52**
130.14.24.0	80	**140.109.56.0**	1493	1	507
130.14.24.0	80	**140.109.56.0**	1495	3	4500

Data Analysis

Web Analysis

sIP	Records
140.211.160.0	87472
130.14.24.0	68057
65.55.208.0	87982
128.30.48.0	207598
72.164.152.0	85542

Web Analyses

- Filtered the data to get more details

sIP	sPort	Bytes	Packets	Records
72.164.152.0	80	158698241	143738	85471
128.30.48.0	80	253913837	236503	204923
140.211.160.0	80	476931122	370825	85044

Web Analyses

- Picked up a few IP address serving as a Server and as a Client.

	Records	Packets	Bytes	Files
Total	535	582	405168	1
Pass	86	119	5282	
Fail	449	463	399886	

Web Analyses

- Re-Analyzed the data
- Web Analysis Results
  - Conversation happening on port 80 and port 443.
  - Data is anonymized, so cannot confirm.

Data Analysis

- FTP
  - Control Port
    - Lots of traffic
    - No Data
  - Data Port
    - Lots of Data
    - No Control
- Why?
  - Sampling/Anonymization

Data Analysis

- Web
  - Server with the most flows
  - Only used port 80
  - Looked for most bytes/packets as well
  - Looked for HTTPS-only servers
    - Need script to assist

Data Analysis

- Tangent
  - Port 443 on port 80 only server
  - 2 clients
    - What else were they doing?
    - Online Gaming?
    - Other?

Challenges

- Logistical
  - Focus/Tangents (AADD?)
  - Project Manager
  - Resource Availability
- Technical
  - Poor data set choice?
  - Anonymization
  - Sampling
  - Resource Skill Level

Future Work

- Continue to look at the network
  - Categorization of what we found and Streaming Audio and Streaming Video
- Look at the Internet
  - Classification of the data
- Investigate Traffic Manag
- Determine Impact of TM
- Finalize report
- Data Validation